Guide to the Algebra Ph.D Examination
At The University of Florida

Author: Joseph Anthony Ruffo

Disclaimer

This guide is intended to prepare students who plan to take the Algebra Ph.D Examination (based on MAS 6331 and MAS 6332) at the University of Florida. I found it best to prepare for the Ph.D Exam by focusing on three major areas from which problems typically appear: results discussed and proven in class, homework problems, and Ph.D Exam practice problems. This guide focuses on these three areas.

I have divided this guide into three sections: the Fall Semester (MAS 6311), the Spring Semester (MAS 6312), and Ph.D Exam practice problems. Each Semester first covers the topics from class, followed by the solutions to the associated homework problems. Proceeding the conclusion of the Spring Semester's materials, solutions to the majority of the Ph.D Exam practice problems are presented. Problems that appear to be skipped in this section were intentionally left unsolved either because the skipped problem was solved previously in the guide, or because the skipped problem involved material that was not covered when I took the 6000 Algebra sequence.

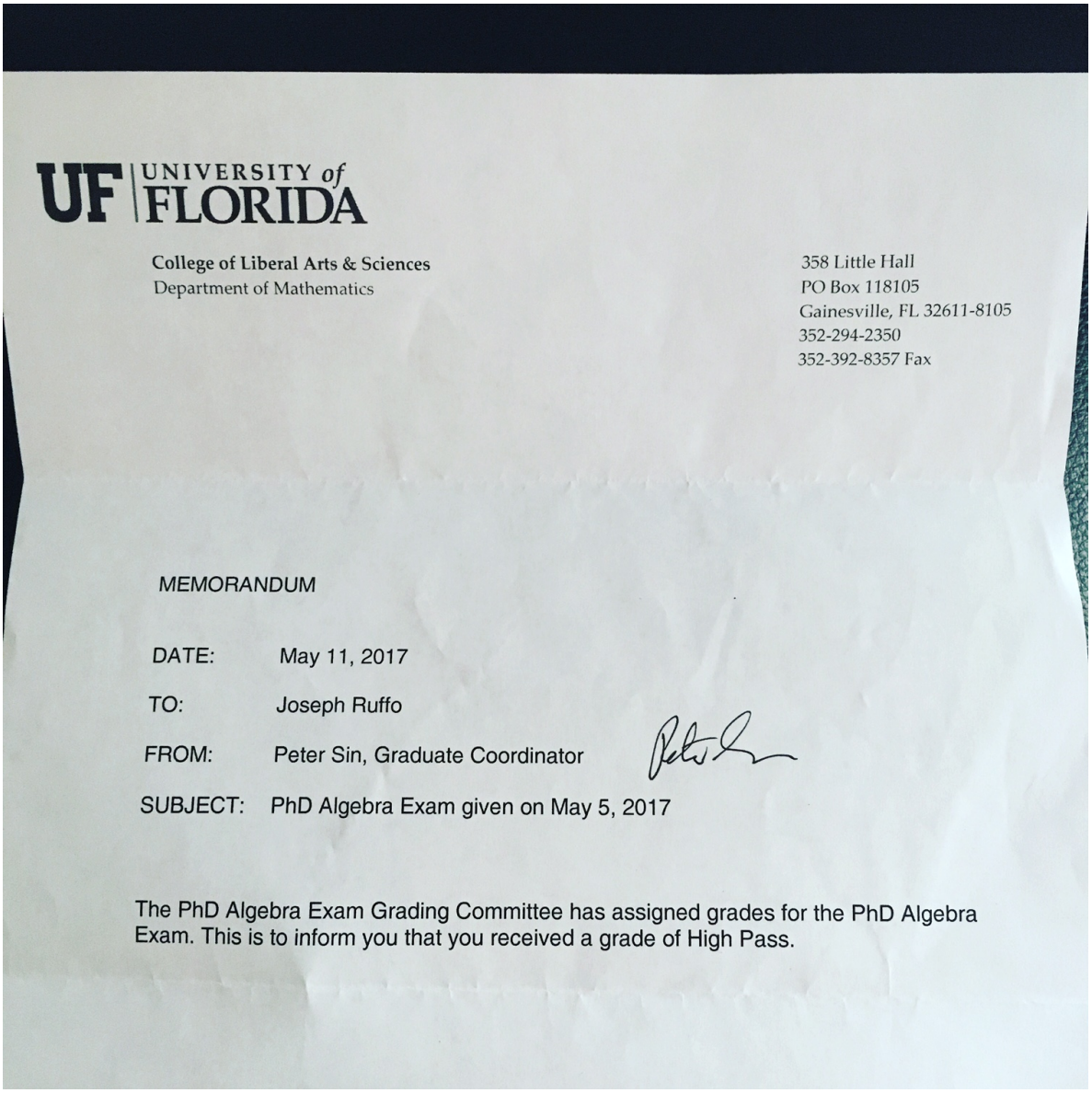
You will notice that both the Spring Semester's results from class and associated homework problems have received a much more comprehensive treatment than those from the Fall Semester's. This was due to timing; I prepared the Spring Semester's results gradually throughout the semester whereas I prepared the Fall Semester's results all at once in a rush to prepare for the Ph.D Exam. Therefore, I had more time to give attention to detail and eloquence in just about all of the problems from the Spring Semester. The reader should also be advised that there are a number of omitted proofs in this guide, all of which appear in the Fall Semester. Again, these were omitted due to timing issues. Furthermore, the reader should be aware of the small amount of material (mainly, material having to do with the Krull-Schmidt Theorem) that is missing from this guide. While this material has never shown up on a Ph.D Exam (hence rendering it all but irrelevant for this guide), it is my intention to fill in these gaps at a later date.

The proofs of results from class are mostly Dr. Turull's proofs; I have simply filled in the details so there is no ambiguity in any of his arguments. I have also provided proofs of claims made but not proven in class, as well as proofs of some supplemental results that were briefly mentioned in class. You can expect that almost all of these proofs are just about flawless. The proofs of the homework problems are (nearly) complete; I could not solve some of the more-challenging homework problems. You can expect to find occasional errors in these proofs and perhaps even much more efficient ways to solve these problems. The proofs of the Ph.D Exam practice problems are mostly accurate and, in my opinion, the majority of these results are about as efficient-solved as possible.

Finally, you will see certain problems repeated in the class notes, in the homework problems, and perhaps even in the Ph.D Exam practice problems. This is due to my own laziness in omitting repeated results. Remember: if a problem is repeated at least once, it likely means that it is a very appropriate problem for the Ph.D Exam. **In general, most solutions are certainly correct. However, many may have minor flaws or can be solved more efficiently, and a small number may have major gaps. Use and enjoy at your own risk.**

Why Use This Guide?

The proof is in the pudding:



UF UNIVERSITY of FLORIDA

College of Liberal Arts & Sciences
Department of Mathematics

358 Little Hall
PO Box 118105
Gainesville, FL 32611-8105
352-294-2350
352-392-8357 Fax

MEMORANDUM

DATE: May 11, 2017

TO: Joseph Ruffo

FROM: Peter Sin, Graduate Coordinator

SUBJECT: PhD Algebra Exam given on May 5, 2017

The PhD Algebra Exam Grading Committee has assigned grades for the PhD Algebra Exam. This is to inform you that you received a grade of High Pass.

Contents

Section I: Fall Semester 2016

Section II: Spring Semester 2017

Section III: Ph.D Exam Practice Problems

Section I: Fall Semester 2016

Topic 1: Preliminaries for Galois Theory

Definition. Let K be a field and let $0 \neq f(x) \in K[x]$. A ***splitting field*** for $f(x)$ over K is a field F such that F/K is a field extension and $f(x)$ may be written

$$f(x) = a \prod_{i=1}^{n} (x - \theta_i)$$

for some $a \in K^\times$ and $\theta_1, \ldots, \theta_n \in F$ where $F = K(\theta_1, \ldots, \theta_n)$.

Remark. In the situation of the above Definition, we have $[F : K] \leq \deg(f(x))!$.

Theorem. (Existence of Splitting Fields): Let K be a field and let $0 \neq f(x) \in K[x]$. Then there exists a splitting field for $f(x)$ over K.

Proof. Omitted. □

Theorem. (Uniqueness of Splitting Fields): Let K_1 and K_2 be fields and suppose that $\phi : K_1 \to K_2$ is an isomorphism of fields. Let $0 \neq f(x) \in K_1[x]$ and let $\phi(f(x))$ denote the polynomial in $K_2[x]$ that is obtained by applying ϕ to each of the coefficients of $f(x)$. Suppose that F_1 is a splitting field for $f(x)$ over K_1 and that F_2 is a splitting field for $\phi(f(x))$ over K_2. Then the isomorphism of fields $\phi : K_1 \to K_2$ may be extended to an isomorphism of fields $F_1 \to F_2$.

Proof. Omitted. □

Definition. Let F/K be a field extension and let $a \in F$. Then a is said to be ***algebraic*** over K if a is a root of some nonzero polynomial in $K[x]$. If a is not algebraic over K, then a is said to be ***transcendental*** over K. The field extension F/K is said to be ***algebraic*** if each element of F is algebraic over K. The field extension F/K is said to be ***transcendental*** if there is an element of F which is transcendental over K.

Definition. Let F/K be a field extension and let $a \in F$ be algebraic over K. Consider the natural ring homomorphism

$$\phi : K[x] \to K[a] \quad \text{by} \quad f(x) \mapsto f(a)$$

Then the ***minimum polynomial*** for a over K is a polynomial which generates the ideal $\ker \phi$ in $K[x]$.

Remark. In the situation of the above Definition, we may assert that the minimum polynomial for a over K is unique by stipulating that this polynomial be monic. We also have that the minimum polynomial for a over K is necessarily irreducible in $K[x]$.

Remark. In the situation of the above Definition, let $f(x) \in K[x]$ be the minimum polynomial for a over K. Then $[K(a) : K] = \deg(f(x))$.

Remark. Suppose that F/K is a field extension. If $[F : K] < \infty$, then F/K is an algebraic field extension. However, if F/K is an algebraic field extension it may not be the case that $[F : K] < \infty$. On the other hand, if F/K is a transcendental field extension then $[F : K] = \infty$. However, if $[F : K] = \infty$, it may not be the case that F/K is a transcendental field extension.

Proof. First, suppose that $[F : K] = n < \infty$ and let $0 \neq a \in F$. Then the set $\{1, a, a^2, \dots, a^n\}$ is a set of $n + 1$ nonzero elements of F and hence as $[F : K] = n$ it must be the case that $\{1, a, a^2, \dots, a^n\}$ is linearly dependent over K. Hence, there are elements $a_0, a_1, a_2, \dots, a_n \in K$ such that

$$a_n a^n + \cdots + a_2 a^2 + a_1 a + a_0 = 0$$

It now follows that $a \in F$ is algebraic over K. Since $a \in F$ was arbitrary, this shows that F/K is an algebraic field extension.

Next, consider the field extension $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{7}, \sqrt{11}, \dots)/\mathbb{Q}$. That is, consider the extension of $\mathbb{Q}$ that is given by adjoining the square root of each prime number to $\mathbb{Q}$. The degree of this extension is infinite but is clearly an algebraic extension.

Next, suppose that F/K is a transcendental field extension. Then there is an element $a \in F$ that is transcendental over K so that $[K(a) : K] = \infty$. This gives that

$$[F : K] = [F : K(a)][K(a) : K] = [F : K(a)] \cdot \infty = \infty$$

which shows that $[F : K] = \infty$.

Finally, consider the field extension $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{7}, \sqrt{11}, \dots)/\mathbb{Q}$ from the above. We know that this an extension is algebraic of infinite degree. In particular, this shows that an extension of infinite degree need not be transcendental. $\square$

Theorem. Let F/K be a field extension and define

$$A = \{a \in F : a \text{ is algebraic over } K\}$$

Then

(a): A is a subfield of F.

(b): A/K is an algebraic field extension.

(c): Any proper field extension B/A with $B \subseteq F$ is transcendental.

Proof. (a): First, note that $A \neq \emptyset$ as clearly $0 \in A$. Now, let $a, b \in A$. Then $[K(a) : K] < \infty$ and $[K(b) : K] < \infty$ so that surely $[K(a, b) : K(a)] < \infty$. Thus, we see

$$[K(a, b) : K] = [K(a, b) : K(a)][K(a) : K] < \infty$$

and hence $K(a, b)/K$ is an algebraic extension. Therefore, since $a - b, ab$, and a/b when $b \neq 0$ are elements of $K(a, b)$ it follows that $a - b, ab$, and a/b when $b \neq 0$ are algebraic

over K and are hence elements of A. We conclude that A is a field and clearly we have by the definition of A that $A \subseteq F$ so that A is a subfield of F. $\square$

Proof. (b): Let $a \in A$. Then a is algebraic over K by the definition of membership in A. Thus, as $a \in A$ was arbitrary we conclude that A/K is an algebraic field extension. $\square$

Proof. (c): Since A is properly contained in B, there is some element $b \in B - A$. For the sake of contradiction, suppose that b were algebraic over A. Then there is some

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in A[x] \quad \text{such that} \quad f(b) = 0$$

Now, notice by the above that $[K(a_{n-1}, \ldots, a_0, b) : K(a_{n-1}, \ldots, a_0)] \leq n$. Moreover, since $a_{n-1}, \ldots, a_0 \in A$ we obtain that

$$[K(a_{n-1}, \ldots, a_0) : K(a_{n-2}, \ldots, a_0)] < \infty$$

and

$$[K(a_{n-2}, \ldots, a_0) : K(a_{n-3}, \ldots, a_0)] < \infty$$

and so on. By the multiplicative nature of degrees, then, we conclude that

$$[K(b) : K] \leq K[(a_{n-1}, \ldots, a_0, b) : K] < \infty$$

and hence b is algebraic over K. However, this gives that $b \in A$ which is a contradiction. We conclude that b is transcendental over A and hence B/A is a transcendental field extension. This completes the proof. $\square$

Definition. Let E and F be fields. A ***field homomorphism*** from E to F is a map $\phi : E \to F$ such that ϕ is a ring homomorphism and $\phi(1_E) = 1_F$.

Definition. Let E and F be extension field of a field K. A ***K-homomorphism*** from E to F is a field homomorphism $\phi : E \to F$ such that $\phi(k) = k$ for each $k \in K$.

Theorem. Let E and F be fields and define

$$S = \{\sigma : E \to F : \sigma \text{ is a field homomorphism}\}$$

Then S is linearly independent over F.

Proof. Assume this is not the case. Then there are elements $\sigma_1, \ldots, \sigma_n \in S$ and elements $\lambda_1, \ldots, \lambda_n \in F^\times$ such that

$$\lambda_1\sigma_1 + \cdots + \lambda_n\sigma_n = 0$$

where n is a positive integer chosen to be as small as possible in a counterexample. Multiplying both sides of the above equality by λ_1^{-1} if necessary, we may further assume that $\lambda_1 = 1$ so that

$$\sigma_1 + \lambda_2\sigma_2 + \cdots + \lambda_n\sigma_n = 0$$

Since $\sigma_1 \neq 0$ as σ_1 is a field homomorphism, then, this gives that $n \geq 2$. Now, since $\sigma_1 \neq \sigma_2$ there is some $0 \neq a \in E$ such that $\sigma_1(a) \neq \sigma_2(a)$. Next, for all $b \in E$ we see

$$0 = \sigma_1(ab) + \lambda_2\sigma_2(ab) + \cdots + \lambda_n\sigma_n(ab) = \sigma_1(a)\sigma_1(b) + \lambda_2\sigma_2(a)\sigma_2(b) + \cdots + \lambda_n\sigma_n(a)\sigma_n(b)$$

and hence as $b \in E$ was arbitrary this gives that

$$\sigma_1(a)\sigma_1 + \lambda_2\sigma_2(a)\sigma_2 + \cdots + \lambda_n\sigma_n(a)\sigma_n = 0$$

Furthermore, as $a \neq 0$ we must have $\sigma_1(a) \neq 0$ and hence we may divide both sides of the above equality by $\sigma_1(a)$ to obtain

$$\sigma_1 + \left(\frac{\lambda_2\sigma_2(a)}{\sigma_1(a)}\right)\sigma_2 + \cdots + \left(\frac{\lambda_n\sigma_n(a)}{\sigma_1(a)}\right)\sigma_n = 0$$

Finally, subtracting equations now gives that

$$\left(\lambda_2 - \frac{\lambda_2\sigma_2(a)}{\sigma_1(a)}\right)\sigma_2 + \cdots + \left(\lambda_n - \frac{\lambda_n\sigma_n(a)}{\sigma_1(a)}\right)\sigma_n = 0$$

Moreover, notice that since $\sigma_1(a) \neq \sigma_2(a)$ we have

$$\lambda_2 - \frac{\lambda_2\sigma_2(a)}{\sigma_1(a)} = \lambda_2\left(1 - \frac{\sigma_2(a)}{\sigma_1(a)}\right) \neq 0$$

However, this contradicts our choice. This completes the proof. □

Corollary. Let E and F be field extensions of a field K and assume that $[E : K] < \infty$. Then the number of K-homomorphisms $E \to F$ is at most $[E : K]$.

Proof. Assume this is not the case. Let $[E : K] = n < \infty$ so that there are $n + 1$ K-homomorphisms $\sigma_1, \ldots, \sigma_{n+1} : E \to F$. Now, let $\{e_1, \ldots, e_n\} \subseteq E$ be a basis for E over K. Let $\mathrm{Res}(\sigma_i)$ denote the restriction of σ_i to the set $\{e_1, \ldots, e_n\}$ for each $i \in \{1, \ldots, n + 1\}$ and define

$$V = \{f : \{e_1, \ldots, e_n\} \to F\}$$

Then V is a vector space over F of dimension n and hence there are elements $\lambda_1, \ldots, \lambda_{n+1} \in F$ not all of which equal to 0 such that

$$\lambda_1\mathrm{Res}(\sigma_1) + \cdots + \lambda_{n+1}\mathrm{Res}(\sigma_{n+1}) = 0$$

However, since $\{e_1, \ldots, e_n\}$ is a basis for E over K it follows that every element of E is a K-linear combination of $\{e_1, \ldots, e_n\}$. In particular, this gives by the above equality that

$$\lambda_1\sigma_1 + \cdots + \lambda_{n+1}\sigma_{n+1} = 0$$

so that the set $\{\sigma_1, \ldots, \sigma_{n+1}\}$ is linearly dependent over F. However, this contradicts the previous Theorem. This completes the proof. □

Topic 2: Galois Theory; Calculating Galois Groups

Definition. Let F/K be a field extension. Then the ***Galois group*** of F/K, denoted $\mathrm{Gal}(F/K)$, is given by

$$\mathrm{Gal}(F/K) = \{\sigma : F \to F : \sigma \text{ is a field isomorphism and a } K\text{-homomorphism}\}$$

and is actually a group under function composition.

Definition. Let F/K be a field extension and $H \leq \mathrm{Gal}(F/K)$. Then the ***fixed field*** of H, denoted F^H, is given by

$$F^H = \{a \in F : \sigma(a) = a \text{ for all } \sigma \in H\}$$

and is actually a subfield of F containing K.

Theorem. Let K be a field and let $G \leq \mathrm{Aut}(K)$ be a finite subgroup of $\mathrm{Aut}(K)$. Then $\left[K : K^G\right] = |G|$.

Proof. Omitted. □

Definition. Let F/K be a field extension and let $G = \mathrm{Gal}(F/K)$. We say that F/K is a ***finite Galois extension*** if $[F : K] < \infty$ and $F^G = K$.

Theorem. (The Fundamental Theorem of Galois Theory): Let F/K be a finite Galois extension. Then there is a one-to-one correspondence between the intermediate fields of the extension F/K and the set of subgroups of $\mathrm{Gal}(F/K)$ that is given by for an intermediate field E of F/K we have $E \mapsto \mathrm{Gal}(F/E)$. Moreover, if $H \leq \mathrm{Gal}(F/K)$ we have $H = \mathrm{Gal}(F/F^H)$.

Furthermore, suppose that E, E_1, and E_2 are intermediate fields of the extension F/K. Then we also have

(a): $E_1 \supseteq E_2$ if and only if $\mathrm{Gal}(F/E_1) \subseteq \mathrm{Gal}(F/E_2)$.

(b): If $E_1 \supseteq E_2$, then $[E_1 : E_2] = [\mathrm{Gal}(F/E_2) : \mathrm{Gal}(F/E_1)]$.

(c): The extension F/E is Galois.

(d): The extension E/K is Galois if and only if $\mathrm{Gal}(F/E) \trianglelefteq \mathrm{Gal}(F/K)$. Moreover, if E/K is Galois then we have $\mathrm{Gal}(E/K) \simeq \mathrm{Gal}(F/K)/\mathrm{Gal}(F/E)$.

Proof. Omitted. □

Definition. Let K be a field. A function $\phi(x_1, \ldots, x_n) \in K(x_1, \ldots, x_n)$ is said to be ***symmetric*** if $\phi(x_{\sigma(1)}, \ldots, x_{\sigma(n)}) = \phi(x_1, \ldots, x_n)$ for each $\sigma \in S_n$. The ***elementary symmetric functions***, denoted $f_1, f_2, \ldots, f_n, f_{n+1}, \cdots \in K(x_1, \ldots, x_n)$, are defined as follows. We have

$$f_1 = \sum_{i=1}^{n} x_i \quad f_2 = \sum_{1 \leq i < j \leq n} x_i x_j \quad f_3 = \sum_{1 \leq i < j < k \leq n} x_i x_j x_k \quad \cdots \quad f_n = x_1 \cdots x_n$$

and $f_N = 0$ for each $N \geq n+1$.

Remark. The group S_n acts faithfully by automorphisms on the field $K(x_1, \ldots, x_n)$ by for $\sigma \in S_n$ and $\phi(x_1, \ldots, x_n) \in K(x_1, \ldots, x_n)$ we have

$$\sigma \cdot \phi(x_1, \ldots, x_n) = \phi(x_{\sigma(1)}, \ldots, x_{\sigma(n)})$$

Theorem. Let K be a field. Then field of symmetric functions in $x_1, \ldots, x_n$ over K is equal to $K(f_1, \ldots, f_n)$.

Proof. Define $E = K(x_1, \ldots, x_n)^{S_n}$ and note that by definition E is the field of symmetric functions over K in $x_1, \ldots, x_n$. Now, we know that

$$[K(x_1, \ldots, x_n) : E] = |S_n| = n!$$

Next, set $E_0 = K(f_1, \ldots, f_n) \subseteq E$ and define

$$f(X) = \prod_{i-1}^{n} (X - x_i) = X^n - f_1 X^{n-1} + f_2 X^{n-2} - f_3 X^{n-3} + \cdots + (-1)^n f_n \in E_0[X]$$

Clearly, the above polynomial gives that

$$[E_0(x_1) : E_0] \leq n$$

and

$$[E_0(x_1, x_2) : E_0(x_1)] \leq n - 1$$

and

$$[E_0(x_1, x_2, x_3) : E_0(x_1, x_2)] \leq n - 2$$

and so on. By the multiplicative nature of degrees, then, we conclude that

$$[E_0(x_1, \ldots, x_n) : E_0] \leq n(n-1)(n-2) \cdots 1 = n!$$

But note that clearly $E_0(x_1, \ldots, x_n) = K(x_1, \ldots, x_n)$ so that by the above we now have

$$[K(x_1, \ldots, x_n) : E_0] \leq n!$$

On the other hand, since we have the inclusion $E_0 \subseteq E \subseteq K(x_1, \ldots, x_n)$ and hence

$$[K(x_1, \ldots, x_n) : E_0] = [K(x_1, \ldots, x_n) : E][E : E_0] = n! \cdot [E : E_0] \geq n!$$

Therefore, we conclude that

$$[K(x_1, \ldots, x_n) : E_0] = n!$$

and hence by the above we obtain

$$n! = [K(x_1, \ldots, x_n) : E_0] = [K(x_1, \ldots, x_n) : E][E : E_0] = n! \cdot [E : E_0]$$

so that $[E : E_0] = 1$. We may now conclude that

$$K(x_1, \ldots, x_n)^{S_n} = E = E_0 = K(f_1, \ldots, f_n)$$

This completes the proof. $\square$

Definition. Let K be a field and let $0 \neq f(x) \in K[x]$. We say that $f(x)$ is ***separable*** if the roots of $f(x)$ in a splitting field for $f(x)$ over K are all distinct.

Theorem. Let K be a field and let $0 \neq f(x) \in K[x]$. Suppose that F is a splitting field for $f(x)$ over K and that $f(x)$ is separable. Then F/K is a finite Galois extension.

Proof. Assume this is false and choose a counterexample with $[F : K]$ as small as possible. If $[F : K] = 1$, then $F = K$ and hence F/K is a Galois extension so that we do not have a counterexample in this case. Therefore, we must have $[F : K] \geq 2$ so that $K \subsetneq F$. This implies that $f(x)$ has a root in F which is not in K and hence $f(x)$ is divisible by some irreducible polynomial $g(x) \in K[x]$ with $\deg(g(x)) = r \geq 2$. Let $\theta_1, \ldots, \theta_r \in F$ denote the roots of $g(x)$. In particular, since $g(x)$ divides $f(x)$ and as $f(x)$ is separable this implies that $\theta_1, \ldots, \theta_r$ are distinct.

Now, let $G = \mathrm{Gal}(F/K)$ and $H = \mathrm{Gal}(F/K(\theta_1))$ and notice that clearly

$$[F : K] = [F : K(\theta_1)][K(\theta_1) : K] \quad \text{so that} \quad [F : K(\theta_1)] = \frac{[F : K]}{[K(\theta_1) : K]}$$

Furthermore, since θ_1 is a root of the *irreducible* polynomial $g(x) \in K[x]$ it follows that $g(x)$ is the minimum polynomial for θ_1 over K so that

$$[K(\theta_1) : K] = \deg(g(x)) = r$$

and hence by the above equalities we obtain since $r \geq 2$ that

$$[F : K(\theta_1)] = \frac{[F : K]}{[K(\theta_1) : K]} = \frac{[F : K]}{r} < [F : K]$$

Furthermore, it is clear that F is a splitting field for the $f(x)$ over $K(\theta_1)$ since F is a splitting field for $f(x)$ over K and as θ_1 is a root of $g(x)$ and hence a root of $f(x)$. Thus, by our choice in counterexample it follows by the above inequality that $F/K(\theta_1)$ is a finite Galois extension so that in particular we obtain $|H| = |\mathrm{Gal}(F/K(\theta_1))| = [F : K(\theta_1)]$.

Next, recall that $g(x) \in K[x]$ is irreducible and that the roots of $g(x)$ are $\theta_1, \ldots, \theta_r$. Therefore, we have that $g(x)$ is the minimum polynomial for $\theta_1, \ldots, \theta_r$ over K. In particular, this gives that

$$K(\theta_1) \simeq \frac{K[x]}{(g(x))} \simeq K(\theta_i) \quad \text{for each} \quad i \in \{1, \ldots, r\}$$

By the above isomorphisms, it follows that there exist isomorphisms $K(\theta_1) \to K(\theta_i)$ which fix K and map $\theta_1 \mapsto \theta_i$ for each $i \in \{1, \ldots, r\}$. By the uniqueness of splitting fields, then, it follows that each of these isomorphisms can be extended to an isomorphism $\sigma_i : F \to F$ for each $i \in \{1, \ldots, r\}$. In particular, we have that $\sigma_1, \ldots, \sigma_r \in G$ and that $\sigma_i(\theta_1) = \theta_i$ for each $i \in \{1, \ldots, r\}$.

Finally, consider the left cosets $\sigma_1 H, \ldots, \sigma_r H$ of H in G. For the sake of contradiction, suppose that these cosets of H in G were not distinct. Then there exist $s, t \in \{1, \ldots, r\}$ with $s \neq t$ but $\sigma_s H = \sigma_t H$. Thus, there is some $\sigma \in H$ such that

$\sigma_s = \sigma_t \circ \sigma$. However, this gives since σ fixes $K(\theta_1)$ that

$$\theta_s = \sigma_s(\theta_1) = (\sigma_t \circ \sigma)(\theta_1) = \sigma_t(\sigma(\theta_1)) = \sigma_t(\theta_1) = \theta_t$$

which contradicts the fact that $\theta_s \neq \theta_t$ as $s \neq t$ and $\theta_1, \ldots, \theta_r$ are distinct. Hence, we conclude that the cosets $\sigma_1 H, \ldots, \sigma_r H$ of H in G are distinct. In particular, this gives

$$|G| = |H|[G : H] \geq |H|r = [F : K(\theta_1)][K(\theta_1) : K] = [F : K]$$

On the other hand, we have

$$|G| = |\mathrm{Gal}(F/K)| \leq [F : K]$$

and hence $|G| = [F : K]$. This shows that F/K is a finite Galois extension, which is a contradiction to our choice. This completes the proof. □

Theorem. Let K be a field with $\mathrm{char}(K) = 0$. Suppose that $f(x) \in K[x]$ is irreducible. Then $f(x)$ is separable.

Proof. For the sake of contradiction, suppose that $f(x)$ were not separable. Then in some splitting field F for $f(x)$ over K, there is an element $\theta \in F$ such that $f(x) = (x-\theta)^2 q(x)$ for some polynomial $q(x) \in K[x]$. Now, notice that

$$f'(x) = (x - \theta)^2 q'(x) + 2(x - \theta)q(x)$$

and hence the polynomials $f(x), f'(x) \in F[x]$ are divisible by the same irreducible factor $(x - \theta) \in F[x]$. Therefore, we see that $f(x)$ and $f'(x)$ are divisible by a common irreducible factor in $K[x]$. Now, recall that $f(x)$ is irreducible. By the previous observation, then, we see that $f(x)$ divides $f'(x)$. However, we have that

$$\deg(f'(x)) = \deg(f(x)) - 1 < \deg(f(x))$$

so that $f(x)$ cannot divide $f'(x)$ which is a contradiction. We conclude that $f(x)$ is separable, completing the proof. □

Corollary. Let K be a field with $\mathrm{char}(K) = 0$. Suppose that $0 \neq f(x) \in K[x]$ and that F is a splitting field for $f(x)$ over K. Then F/K is a finite Galois extension.

Proof. First, write

$$f(x) = a \prod_{i=1}^{k} g_i(x)^{n_i}$$

where $a \in K^\times$, $n_1, \ldots, n_k$ are positive integers, and $g_1(x), \ldots, g_k(x) \in K[x]$ are distinct, monic, irreducible polynomials. Now, let $h(x) = g_1(x) \cdots g_k(x)$ and notice that $f(x)$ and $h(x)$ share the same set of roots so that F is a splitting field for $h(x)$ over K as F is a splitting field for $f(x)$ over K. Furthermore, since $g_1(x), \ldots, g_k(x) \in K[x]$ are irreducible polynomials and as $\mathrm{char}(K) = 0$ it follows by the previous Theorem that $g_1(x), \ldots, g_k(x) \in K[x]$ are separable polynomials and hence it follows that $h(x) \in K[x]$ is a separable polynomial. Thus, since F is a splitting field for $h(x)$ over K we may now conclude by the second of the above previous Theorems that F/K is a finite Galois extension. This completes the proof. □

Definition. Let K be a field and $0 \neq f(x) \in K[x]$. Let F be a splitting field for $f(x)$ over K. Then the ***Galois group of*** $f(x)$ ***over*** K is $\mathrm{Gal}(F/K)$.

Theorem. Let K be a field and $0 \neq f(x) \in K[x]$ with $\deg(f(x)) = n \geq 1$ and let F be a splitting field for $f(x)$ over K. Let $G = \mathrm{Gal}(F/K)$ be the Galois group of $f(x)$ over K and let Γ denote the set of roots for $f(x)$ in a splitting field of $f(x)$ over K. Then

(a): The group G acts faithfully on the set Γ. In particular, we have that G is isomorphic to a subgroup of S_n.

(b): If $f(x)$ is irreducible and separable, then G acts transitively Γ. In particular, we have that n divides $|G|$.

(c): If $f(x)$ is separable and G acts transitively on Γ, then $f(x)$ is irreducible.

Proof. (a): Let $\theta \in \Gamma$ and $\sigma \in G$. Then since $f(\theta) = 0$, we have

$$0 = \sigma(0) = \sigma(f(\theta)) = f(\sigma(\theta))$$

so that $\sigma(\theta) \in \Gamma$ and hence G does indeed act on Γ. Now, suppose that $\sigma \in G$ is in the kernel of the action of G on Γ. In particular, we have that $\sigma(\theta) = \theta$ for each $\theta \in \Gamma$ so that σ fixes Γ. Moreover, recall that σ fixes K since $\sigma \in G$ and that $F = K(\Gamma)$ since F is a splitting field for $f(x)$ over K. Combining the previous two observations, we conclude that $\sigma \in G = \mathrm{Gal}(F/K)$ fixes $K(\Gamma) = F$ so that $\sigma = 1_F$. This result shows that the action of G on Γ is faithful and hence we obtain an injective group homomorphism $G \to S_n$. We may now conclude that also G is isomorphic to a subgroup of S_n by the First Isomorphism Theorem. $\square$

Proof. (b): Let $\theta_1, \theta_2 \in \Gamma$. Since $f(x) \in K[x]$ is irreducible and has θ_1, θ_2 as roots, it follows that $f(x)$ is the minimum polynomial for θ_1 and θ_2 over K. Hence, we obtain

$$K(\theta_1) \simeq \frac{K[x]}{(f(x))} \simeq K(\theta_2)$$

By the above isomorphism, it follows that there exists an isomorphism $K(\theta_1) \to K(\theta_2)$ which fixes K and maps $\theta_1 \mapsto \theta_2$. By the uniqueness of splitting fields, then, it follows that this isomorphism can be extended to an isomorphism $\sigma : F \to F$. In particular, we have that $\sigma \in G$ and that $\sigma(\theta_1) = \theta_2$. Thus, as $\theta_1, \theta_2 \in \Gamma$ were arbitrary it now follows that G acts transitively on Γ. Moreover, since G acts transitively on Γ we have by the Orbit-Stabilizer Theorem that $|\Gamma|$ divides $|G|$. But since $\deg(f(x)) = n$ and as $f(x)$ is separable by hypothesis, it follows that $|\Gamma| = n$ and hence n divides $|G|$. $\square$

Proof. (c): For the sake of contradiction, suppose that $f(x) \in K[x]$ were not irreducible. Then there are nonconstant polynomials $p(x), q(x) \in K[x]$ such that $f(x) = p(x)q(x)$. Now, let $\theta_1 \in F$ be a root of $p(x)$ and $\theta_2 \in F$ be a root of $q(x)$ so that clearly $\theta_1, \theta_2 \in \Gamma$. Since G acts transitively on Γ, there is some $\sigma \in G$ such that $\sigma(\theta_1) = \theta_2$. Now, let $m_1(x), m_2(x) \in K[x]$ be the minimum polynomials over K for θ_1, θ_2, respectively. Then we obtain that

$$0 = \sigma(0) = \sigma(m_1(\theta_1)) = m_1(\sigma(\theta_1)) = m_1(\theta_2)$$

By the above equality, we may now conclude that $m_1(x) = m_2(x)$.

Finally, recall that θ_1 is a root of $p(x)$ and that θ_2 is a root of $q(x)$. Therefore, we see that $m_1(x)$ divides $p(x)$ which divides $f(x)$ and that $m_2(x)$ divides $q(x)$ which divides $f(x)$. Therefore, the product $m_1(x)m_2(x)$ also divides $f(x)$. But since $m_1(x) = m_2(x)$ by the above, we may now conclude that in fact $m_1(x)^2$ divides $f(x)$. However, this implies that $f(x)$ is not separable which is a contradiction. We conclude that $f(x)$ is irreducible, completing the proof. $\square$

Definition. Let K be a field and $0 \neq f(x) \in K[x]$ with $\deg(f(x)) = n \geq 1$. Let F be a splitting field for $f(x)$ over K and write

$$f(x) = a \prod_{i=1}^{n} (x - \theta_i)$$

where $a \in K^\times$ and $\theta_1, \ldots, \theta_n \in F$. Define

$$\Delta = \prod_{1 \leq i < j \leq n} (\theta_i - \theta_j)$$

Then the ***discriminant*** D of $f(x)$ is given by $D = \Delta^2$.

Proposition. Adopting the same assumptions and notation as in the above Definition, we have that $D \in K$.

Proof. If $f(x)$ is not separable, then clearly $\Delta = 0$ so that

$$D = \Delta^2 = 0^2 = 0 \in K$$

If $f(x)$ is separable, then F/K is a finite Galois extension. Now let $\sigma \in \mathrm{Gal}(F/K)$ and recall that σ permutes the roots of $f(x)$ so that in particular we have $\sigma(\Delta) \in \{-\Delta, \Delta\}$. Thus, we obtain that

$$\sigma(D) = \sigma(\Delta^2) = (\sigma(\Delta))^2 = \Delta^2 = D$$

Thus, since $\sigma \in \mathrm{Gal}(F/K)$ was arbitrary and as F/K is a finite Galois extension the above equality shows that $D \in K$. $\square$

Proposition. Adopting the same assumptions and notation as in the above Definition, suppose that $f(x)$ is separable and that $\mathrm{char}(K) \neq 2$. Let Γ denote the set of roots of $f(x)$ in F. Then $\mathrm{Gal}(F/K) \subseteq A_\Gamma$ if and only if D is a square in K.

Proof. For the first direction, assume that $\mathrm{Gal}(F/K) \subseteq A_\Gamma$ and let $\sigma \in \mathrm{Gal}(F/K)$. By the previous inclusion, then, we have $\mathrm{sgn}(\sigma) = 1$ and hence

$$\sigma(\Delta) = \mathrm{sgn}(\sigma) \cdot \Delta = 1 \cdot \Delta = \Delta$$

Now, since $f(x)$ is separable we know that F/K is a finite Galois extension. Thus, since $\sigma \in \mathrm{Gal}(F/K)$ was arbitrary the above equality implies that $\Delta \in K$ and hence $D = \Delta^2$ is a square in K.

For the second direction, assume that D is a square in K. Now, since $f(x)$ is separable we know that $\Delta \neq 0$. Thus, since

$$\Delta^2 = D = (-\Delta)^2$$

we conclude that as D is a square in K that $\Delta \in K$. Finally, let $\sigma \in \mathrm{Gal}(F/K)$. Then since $\Delta \in K$, we have that

$$\Delta = \sigma(\Delta) = \mathrm{sgn}(\sigma) \cdot \Delta$$

so that $\mathrm{sgn}(\sigma) = 1$. In particular, this shows that $\sigma \in A_\Gamma$ and hence $\mathrm{Gal}(F/K) \subseteq A_\Gamma$. $\square$

Theorem. Let p be a prime number and let G be a transitive subgroup of S_p and assume that G contains a transposition. Then $G = S_p$.

Proof. Since G is a transitive subgroup of S_p, we have that p divides $|G|$ and hence by Cauchy's Theorem G contains an element σ of order p. In particular, since G is a subgroup of S_p it follows that σ is a p-cycle and hence we may write

$$\sigma = (a_1 \quad \cdots \quad a_p)$$

Now, let $\tau \in G$ be a transposition so that we may write $\tau = (b \quad c)$. Reordering if necessary, we may assume that $b = a_1$ and hence we now have that $c = a_N$ for some $N \in \{2, \ldots, p\}$. Moreover, notice that

$$\sigma^{N-1} = (a_1 \quad c \quad \cdots) \in G$$

is a p-cycle. Thus, without loss of generality we may assume that $\tau = (a_1 \quad a_2)$.

Finally, notice that by conjugation by powers of $\tau\sigma$ that $(a_1 \quad a_i) \in G$ for each $i \in \{2, \ldots, n\}$. Furthermore, by conjugating the resulting transpositions described in the previous sentence by powers of σ we see that G contains all transpositions in S_p. Therefore, since the transpositions of S_p generate S_p we conclude that $G = S_p$. This completes the proof. $\square$

Remark. If K is a field with $\mathrm{char}(K) \notin \{2, 3\}$ and $f(x) = x^3 + px + q \in K[x]$, then the discriminant D of $f(x)$ is such that $D = -4p^3 - 27q^2$.

Example. In what follows below, we let F denote the splitting field for $f(x)$ over $\mathbb{Q}$ and we let Γ denote the set of roots of $f(x)$ in F. In each case, calculate the Galois group of $f(x)$ over $\mathbb{Q}$ if

(a): $f(x) = x^4 - 2$.

(b): $f(x) = x^3 + x^2 - x - 1$.

(c): $f(x) = x^3 - 3x + 1$.

(d): $f(x) = x^5 - 4x + 2$.

(e): $f(x) = x^3 - 3$.

(f): $f(x) = (x^3 - 2)(x^2 - 3)$.

In Part (e), for each subgroup $H \leq \mathrm{Gal}(F/\mathbb{Q})$ find the fixed field F^H.

Proof. (a): Let $u = 2^{1/4}$ so that $\Gamma = \{u, -u, ui, -ui\}$. Thus, we see that $F = \mathbb{Q}(u, i)$ and since $\mathrm{char}(\mathbb{Q}) = 0$ we have that $F/\mathbb{Q}$ is a finite Galois extension so that

$$|\mathrm{Gal}(F/\mathbb{Q})| = [F : \mathbb{Q}] = [\mathbb{Q}(u, i) : \mathbb{Q}] = [\mathbb{Q}(u, i) : \mathbb{Q}(u)][\mathbb{Q}(u) : \mathbb{Q}]$$

Now, since $f(x)$ is irreducible over $\mathbb{Q}$ by Eisenstein's Criterion it follows that $f(x)$ is the minimum polynomial for u over $\mathbb{Q}$ so that

$$[\mathbb{Q}(u) : \mathbb{Q}] = \deg(f(x)) = 4$$

Furthermore, recall that $g(x) = x^2 + 1 \in \mathbb{Q}[x]$ is the minimum polynomial for i over $\mathbb{Q}$ and hence

$$[\mathbb{Q}(u, i) : \mathbb{Q}(u)] \leq [\mathbb{Q}(i) : \mathbb{Q}] = \deg(g(x)) = 2$$

so that $[\mathbb{Q}(u, i) : \mathbb{Q}(u)] \in \{1, 2\}$. However, we know that clearly $i \notin \mathbb{Q}(u)$ and thus it now follows that $[\mathbb{Q}(u, i) : \mathbb{Q}(u)] = 2$. Combining the previous results, then, we see

$$|\mathrm{Gal}(F/\mathbb{Q})| = [\mathbb{Q}(u, i) : \mathbb{Q}(u)][\mathbb{Q}(u) : \mathbb{Q}] = 2 \cdot 4 = 8$$

We will use this observation below.

Towards this end, by the above equality we may assert that $[F : \mathbb{Q}(i)] = 4$ and hence it follows by an argument similar to those presented above that $f(x)$ is the minimum polynomial for u over $\mathbb{Q}(i)$ so that in particular we obtain that $f(x)$ is irreducible over $\mathbb{Q}(i)$. Moreover, observe that $f(x)$ is separable by our above computation of the set Γ. Thus, it now follows that $\mathrm{Gal}(F/\mathbb{Q}(i))$ acts transitively on Γ. Therefore, there is some $\sigma \in \mathrm{Gal}(F/\mathbb{Q}(i)) \leq \mathrm{Gal}(F/\mathbb{Q})$ such that $\sigma(u) = iu$. Furthermore, we have since σ fixes $\mathbb{Q}(i)$ that $\sigma(i) = i$ and hence

$$\sigma(iu) = \sigma(i)\sigma(u) = i\sigma(u) = i \cdot iu = -u$$

and

$$\sigma(-u) = -\sigma(u) = -iu$$

and

$$\sigma(-iu) = -\sigma(iu) = -(-u) = u$$

Combining the previous results, we see that

$$(u \quad iu \quad -u \quad -iu) \in \mathrm{Gal}(F/\mathbb{Q})$$

Moreover, let $\tau : F \to F$ denote the complex conjugation map. Then clearly we have $\tau \in \mathrm{Gal}(F/\mathbb{Q})$ and hence it follows that $(iu \quad -iu) \in \mathrm{Gal}(F/\mathbb{Q})$.

Finally, let $\sigma_1 = (u \quad iu \quad -u \quad -iu) \in \mathrm{Gal}(F/\mathbb{Q})$ and $\sigma_2 = (iu \quad -iu) \in \mathrm{Gal}(F/\mathbb{Q})$. Then since $|\mathrm{Gal}(F/\mathbb{Q})| = 8$ by the above, we have that $\langle \sigma_1, \sigma_2 \rangle = \mathrm{Gal}(F/\mathbb{Q})$. Moreover, observe that $\sigma_1\sigma_2\sigma_1 = \sigma_2$ and hence we conclude that $\mathrm{Gal}(F/\mathbb{Q}) \simeq D_8$. □

Proof. (b): First, notice that

$$f(x) = x^3 + x^2 - x - 1 = x^2(x + 1) - 1(x + 1) = (x^2 - 1)(x + 1) = (x + 1)^2(x - 1)$$

and hence $\Gamma \subseteq \mathbb{Q}$. In particular, this gives that $F = \mathbb{Q}$ and hence

$$\mathrm{Gal}(F/\mathbb{Q}) = \mathrm{Gal}(\mathbb{Q}/\mathbb{Q}) = \{0\}$$

We conclude that $\mathrm{Gal}(F/\mathbb{Q})$ is trivial. □

Proof. (c): First, note that since

$$f(-1) = -1 + 3 + 1 = 3 \neq 0 \quad \text{and} \quad f(1) = 1 - 3 + 1 = -1 \neq 0$$

we have by the Rational Root Theorem that $f(x)$ has no roots in $\mathbb{Q}$. Therefore, since $f(x) \in \mathbb{Q}[x]$ is a polynomial of degree 3 over the field $\mathbb{Q}$ it follows that $f(x)$ is irreducible over $\mathbb{Q}$. Furthermore, since $\text{char}(\mathbb{Q}) = 0$ we see that $f(x)$ is separable over $\mathbb{Q}$ and thus $f(x)$ is an irreducible, separable polynomial over $\mathbb{Q}$ so that $\deg(f(x)) = 3$ divides $|\text{Gal}(F/\mathbb{Q})|$. Moreover, we know that $\text{Gal}(F/\mathbb{Q})$ is isomorphic to a subgroup of S_3. Therefore, it must be the case that $\text{Gal}(F/\mathbb{Q}) \in \{A_3, S_3\}$.

Finally, notice that the discriminant D of $f(x)$ is given by

$$D = -4(-3)^3 - 27(1)^2 = 81 = 9^2$$

so that D is a square in $\mathbb{Q}$. Therefore, it now follows that $\text{Gal}(F/\mathbb{Q}) \subseteq A_3$. But since $\text{Gal}(F/\mathbb{Q}) \in \{A_3, S_3\}$, this inclusion implies that $\text{Gal}(F/\mathbb{Q}) = A_3$. □

Proof. (d): First, we use elementary Calculus to show that $f(x)$ has exactly three real roots and exactly two non-real roots. Towards this end, notice that

$$f'(x) = 5x^4 - 4 \quad \text{so that} \quad f'(x) = 0 \quad \text{for} \quad x \in \left\{-(4/5)^{1/4}, (4/5)^{1/4}\right\}$$

These results give us good reason to investigate the evaluations

$$f(-2) < 0 \quad f(0) > 0 \quad f(1) < 0 \quad f(2) > 0$$

Thus, since $f(x)$ is clearly continuous on $\mathbb{R}$ we have by the Intermediate Value Theorem that there are elements $a_1 \in (-2, 0) \subseteq \mathbb{R}$, $a_2 \in (0, 1) \subseteq \mathbb{R}$, and $a_3 \in (1, 2) \subseteq \mathbb{R}$ such that $f(a_1) = f(a_2) = f(a_3) = 0$. Moreover, since $f'(x) = 0$ for exactly two real values of x it follows that $f(x)$ can have at most three distinct, real roots. By the previous result, we conclude that $f(x)$ has exactly three real roots and exactly two non-real roots. Let these two non-real roots of $f(x)$ be denoted $u_1, u_2 \in \mathbb{C}$. In particular, since non-real roots of polynomials in $\mathbb{Q}[x]$ come in complex conjugate pairs we have that $\overline{u_1} = u_2$.

We now prove the main result. Towards this end, notice that $f(x)$ is irreducible over $\mathbb{Q}$ by Eisenstein's Criterion. Since $\text{char}(\mathbb{Q}) = 0$, then, we see that $f(x)$ is separable over $\mathbb{Q}$ and hence $f(x)$ is an irreducible, separable polynomial over $\mathbb{Q}$ so that $\deg(f(x)) = 5$ divides $|\text{Gal}(F/\mathbb{Q})|$. Thus, since 5 is a prime number we have by Cauchy's Theorem that $\text{Gal}(F/\mathbb{Q})$ contains an element of order 5. But since $\text{Gal}(F/\mathbb{Q})$ is isomorphic to a subgroup of S_5, this observation implies that $\text{Gal}(F/\mathbb{Q})$ contains a 5-cycle.

Moreover, let $\tau : F \to F$ denote the complex conjugation map so that $\tau \in \text{Gal}(F/\mathbb{Q})$. Then since $f(x)$ has exactly three real roots and exactly two non-real roots u_1, u_2, it now follows that $\tau(u_1) = \overline{u_1} = u_2$ and that τ fixes the remaining three real roots of $f(x)$ since the complex conjugation map fixes $\mathbb{R}$. In particular, this observation implies that $(u_1 \quad u_2) \in \text{Gal}(F/\mathbb{Q})$ and hence $\text{Gal}(F/\mathbb{Q})$ contains a transposition. Combining the previous results, we conclude that $\text{Gal}(F/\mathbb{Q})$ is a subgroup of S_5 which contains a 5-cycle and a transposition. Since 5 is a prime number, then, we see that $\text{Gal}(F/\mathbb{Q}) = S_5$. □

Proof. (e): Let $u = 2^{1/3}$ so that $\Gamma = \{u, u\zeta, u\zeta^2\}$, where ζ is a primitive third root of unity. Thus, we see that $F = \mathbb{Q}(u, \zeta)$ and since $\text{char}(\mathbb{Q}) = 0$ we have that $F/\mathbb{Q}$ is a finite Galois extension so that

$$|\text{Gal}(F/\mathbb{Q})| = [F : \mathbb{Q}] = [\mathbb{Q}(u, \zeta) : \mathbb{Q}(\zeta)][\mathbb{Q}(\zeta) : \mathbb{Q}]$$

Now, let $g_3(x) \in \mathbb{Q}[x]$ denote the third cyclotomic polynomial over $\mathbb{Q}$. Then we know that $g_3(x)$ is the minimum polynomial for ζ over $\mathbb{Q}$ so that

$$[\mathbb{Q}(\zeta) : \mathbb{Q}] = \deg(g_3(x)) = \phi(3) = 2$$

Next, notice that since the polynomial $f(x) = x^3 - 2 \in \mathbb{Q}(\zeta)[x]$ is of degree 3 and has no roots in $\mathbb{Q}(\zeta)$ that $f(x)$ is irreducible over $\mathbb{Q}(\zeta)$. Therefore, we have that $f(x)$ is the minimum polynomial for u over $\mathbb{Q}(\zeta)$ so that

$$[\mathbb{Q}(u, \zeta) : \mathbb{Q}(\zeta)] = \deg(f(x)) = 3$$

Combining the previous results, then, we obtain

$$|\text{Gal}(F/\mathbb{Q})| = [F : \mathbb{Q}] = [\mathbb{Q}(u, \zeta) : \mathbb{Q}(\zeta)][\mathbb{Q}(\zeta) : \mathbb{Q}] = 3 \cdot 2 = 6$$

We will use this result below.

Next, recall that by the above computations we have that $f(x)$ is irreducible over $\mathbb{Q}(\zeta)$. Moreover, observe that $f(x)$ is separable by our above computation of the set Γ. Therefore, it follows that $\text{Gal}(F/\mathbb{Q}(\zeta))$ acts transitively on Γ and hence there is some $\sigma \in \text{Gal}(F/\mathbb{Q}(\zeta)) \leq \text{Gal}(F/\mathbb{Q})$ such that $\sigma(u) = u\zeta$. Furthermore, as σ fixes ζ we see

$$\sigma(u\zeta) = \zeta\sigma(u) = \zeta(u\zeta) = u\zeta^2$$

and

$$\sigma(u\zeta^2) = \zeta^2\sigma(u) = \zeta^2(u\zeta) = u\zeta^3 = u \cdot 1 = u$$

so that

$$(u \quad u\zeta \quad u\zeta^2) \in \text{Gal}(F/\mathbb{Q}(\zeta)) \leq \text{Gal}(F/\mathbb{Q})$$

Now, let $\tau : F \to F$ be the complex conjugation map so that $\tau \in \text{Gal}(F/\mathbb{Q})$. Then we know that $\tau(u) = u$ since $u \in \mathbb{R}$ and as σ fixes $\mathbb{R}$. But since $\tau(u\zeta) = \overline{u\zeta} = u\zeta^2$, it now follows that

$$(u\zeta \quad u\zeta^2) \in \text{Gal}(F/\mathbb{Q})$$

Finally, recall that $\text{Gal}(F/\mathbb{Q})$ is isomorphic to a subgroup of S_3. Moreover, notice by the above results that $\text{Gal}(F/\mathbb{Q})$ contains both a 3-cycle and a transposition. Since 3 is a prime number, then, we conclude that $\text{Gal}(F/\mathbb{Q}) = S_3$.

For each subgroup $H \leq \text{Gal}(F/\mathbb{Q}) = S_3$, we now find the fixed field F^H. Towards this end, note that the subgroups of $\text{Gal}(F/\mathbb{Q})$ are

$$\{\{(1_F)\}, \{(1_F), (u \quad u\zeta)\}, \{(1_F), (u, \quad u\zeta^2)\}, \{(1_F), (u\zeta \quad u\zeta^2)\},$$
$$\{(1_F), (u \quad u\zeta \quad u\zeta^2), (u \quad u\zeta^2 \quad u\zeta)\}, \text{Gal}(F/\mathbb{Q})\}$$

Now, note that by the Fundamental Theorem of Galois Theory we have

$$F^{\{(1_F)\}} = F \quad \text{and} \quad F^{\text{Gal}(F/\mathbb{Q})} = \mathbb{Q}$$

Moreover, we have by the above computations that

$$6 = |\mathrm{Gal}(F/\mathbb{Q})| = [F : \mathbb{Q}] = [F : \mathbb{Q}(\zeta)][\mathbb{Q}(\zeta) : \mathbb{Q}] = [F : \mathbb{Q}(\zeta)] \cdot 2$$

so that $[F : \mathbb{Q}(\zeta)] = 3$ and thus by the Fundamental Theorem of Galois Theory we see

$$|\mathrm{Gal}(F/\mathbb{Q}(\zeta))| = [F : \mathbb{Q}(\zeta)] = 3$$

It now follows by the Fundamental Theorem of Galois Theory that

$$F^{\{(1_F),(u \quad u\zeta \quad u\zeta^2),(u \quad u\zeta^2 \quad u\zeta)\}} = \mathbb{Q}(\zeta)$$

and so it remains to find the fixed fields of the extension $F/\mathbb{Q}$ corresponding to the three subgroups of $\mathrm{Gal}(F/\mathbb{Q})$ of order 2.

Towards this end, we first show that the fields $\mathbb{Q}(u), \mathbb{Q}(u\zeta), \mathbb{Q}(u\zeta^2)$ are each distinct. Indeed, suppose for the sake of contradiction that $\mathbb{Q}(u) = \mathbb{Q}(u\zeta)$. Then we have since $u\zeta \in \mathbb{Q}(u\zeta) = \mathbb{Q}(u)$ and as $1/u \in \mathbb{Q}(u)$ that

$$\zeta = u\zeta \cdot \frac{1}{u} \in \mathbb{Q}(u) \subseteq \mathbb{R}$$

which is a contradiction since $\zeta \notin \mathbb{R}$ as ζ is a primitive third root of unity. Using the same argument as presented above, we also obtain that $\mathbb{Q}(u) \neq \mathbb{Q}(u\zeta^2)$. Lastly, suppose that $\mathbb{Q}(u\zeta) = \mathbb{Q}(u\zeta^2)$. In this case, we see that $u\zeta^2 \in \mathbb{Q}(u\zeta^2) = \mathbb{Q}(u\zeta)$ and as $1/u\zeta \in \mathbb{Q}(u\zeta)$ this gives that

$$\zeta = u\zeta^2 \cdot \frac{1}{u\zeta} \in \mathbb{Q}(u\zeta)$$

and thus

$$u = u \cdot 1 = u \cdot \zeta^3 = u\zeta^2 \cdot \zeta \in \mathbb{Q}(u\zeta)$$

That is, we have $u, \zeta \in \mathbb{Q}(u\zeta)$ so that $\mathbb{Q}(u\zeta) = \mathbb{Q}(u, \zeta) = F$ which is clearly a contradiction. We conclude that the fields $\mathbb{Q}(u), \mathbb{Q}(u\zeta), \mathbb{Q}(u\zeta^2)$ are each distinct.

Finally, recall that by the Fundamental Theorem of Galois Theory that the set of subgroups of $\mathrm{Gal}(F/\mathbb{Q})$ are in a one-to-one correspondence with the intermediate fields of the extension $F/\mathbb{Q}$. Therefore, by the previous result it now follows that the three remaining subgroups of $\mathrm{Gal}(F/\mathbb{Q})$ for which we have not already calculated a fixed field correspond to the distinct intermediate fields $\mathbb{Q}(u), \mathbb{Q}(u\zeta), \mathbb{Q}(u\zeta^2)$ of the extension $F/\mathbb{Q}$. Now, notice that as $(1_F), (u \quad u\zeta) \in \{(1_F), (u \quad u\zeta)\} \leq \mathrm{Gal}(F/\mathbb{Q})$ fix $u\zeta^2$ it follows that

$$F^{\{(1_F),(u \quad u\zeta)\}} = \mathbb{Q}(u\zeta^2)$$

By the same reasoning, we also obtain that

$$F^{\{(1_F),(u, \quad u\zeta^2)\}} = \mathbb{Q}(u\zeta) \quad \text{and} \quad F^{\{(1_F),(u\zeta, \quad u\zeta^2)\}} = \mathbb{Q}(u)$$

This completes the proof. □

Proof. (f): Let $u = 2^{1/3}$ and $v = 3^{1/2}$ so that $\Gamma = \{u, u\zeta, u\zeta^2, -v, v\}$, where $\zeta = e^{2\pi i/3}$ is a primitive third root of unity. Thus, we see that $F = \mathbb{Q}(u, v, \zeta)$. Now, notice that

$$\zeta = e^{2\pi i/3} = \cos\left(\frac{2\pi}{3}\right) + i\sin\left(\frac{2\pi}{3}\right) = -\frac{1}{2} + i\frac{\sqrt{3}}{2} = -\frac{1}{2} + i\frac{v}{2}$$

Thus, it now follows that $\zeta \in \mathbb{Q}(v, i)$. In particular, this now gives that $F = \mathbb{Q}(u, v, \zeta) = \mathbb{Q}(u, v, i)$. Next, recall that the minimum polynomial for u over $\mathbb{Q}$ is $g(x) = x^3 - 2$. This gives that

$$[\mathbb{Q}(u) : \mathbb{Q}] = \deg(g(x)) = 3$$

Next, recall that the minimum polynomial for v over $\mathbb{Q}$ is $h(x) = x^2 - 3$ which gives that

$$[\mathbb{Q}(v) : \mathbb{Q}] = \deg(h(x)) = 2 \quad \text{so that} \quad [\mathbb{Q}(u, v) : \mathbb{Q}(u)] \leq 2$$

However, notice that clearly $v \notin \mathbb{Q}(u)$ and thus we have by the above inequality that $[\mathbb{Q}(u, v) : \mathbb{Q}(u)] = 2$. Finally, recall that the minimum polynomial for i over $\mathbb{Q}$ is $k(x) = x^2 + 1$ which gives that

$$[\mathbb{Q}(i) : \mathbb{Q}] = \deg(k(x)) = 2 \quad \text{so that} \quad [\mathbb{Q}(u, v, i) : \mathbb{Q}(u, v)] \leq 2$$

However, notice that clearly $\mathbb{Q}(u, v) \subseteq \mathbb{R}$ and thus $i \notin \mathbb{Q}(u, v)$ so that by the above inequality we obtain $[\mathbb{Q}(u, v, i) : \mathbb{Q}(u, v)] = 2$. Therefore, as $\text{char}(\mathbb{Q}) = 0$ we have that $F/\mathbb{Q}$ is a finite Galois extension so that by the above results we obtain

$$\begin{aligned}
|\text{Gal}(F/\mathbb{Q})| &= [F : \mathbb{Q}] \\
&= [\mathbb{Q}(u, v, i) : \mathbb{Q}] \\
&= [\mathbb{Q}(u, v, i) : \mathbb{Q}(u, v)][\mathbb{Q}(u, v) : \mathbb{Q}(u)][\mathbb{Q}(u) : \mathbb{Q}] \\
&= 2 \cdot 2 \cdot 3 \\
&= 12
\end{aligned}$$

We will use this result below.

Now, let $\sigma \in \text{Gal}(F/\mathbb{Q})$. Then σ permutes the roots of $f(x) = (x^3 - 2)(x^2 - 3)$. Furthermore, notice that the roots of $x^3 - 2$ are $u, u\zeta, u\zeta^2$ and that the roots of $x^2 - 3$ are $-v, v$. In particular, observe that the polynomials $x^3 - 2$ and $x^2 - 3$ share no common roots. Therefore, it now follows that σ permutes the roots of $x^3 - 2$ among themselves and that σ permutes the roots of $x^2 - 3$ among themselves. Thus, we see that $\sigma \in S_3 \times S_2$ and hence $\text{Gal}(F/\mathbb{Q}) \subseteq S_3 \times S_2$. But recall by the above that

$$|\text{Gal}(F/\mathbb{Q})| = 12 = 6 \cdot 2 = 3! \cdot 2! = |S_3 \times S_2|$$

so that by the previous inclusion we obtain that $\text{Gal}(F/\mathbb{Q}) = S_3 \times S_2$. $\square$

Topic 3: The Finite Field of Order p^n

Theorem. Let p be a prime number and let n be a positive integer. Then up to isomorphism, there is exactly one field of order p^n.

Remark. We will prove this result by first proving two Lemmas. After these Lemmas have been proven, we will then present a proof of the main result.

Lemma 1. Let K be a finite field with prime subfield P. Then $|K| = p^n$, where p is a prime number and $n = \dim_P(K)$. Furthermore, we have that K is a splitting field for the polynomial $f(x) = x^{p^n} - x \in P[x]$.

Proof. Let $\mathrm{char}(K) = p$. Since K is a finite field, we know that p is a prime number. Now, let $1_K \in K$ denote the multiplicative identity of K and define a map

$$\phi : \mathbb{Z} \to K \quad \text{by} \quad m \mapsto m \cdot 1_K$$

Clearly, we see ϕ is a ring homomorphism with $\ker \phi = \mathrm{char}(K)\mathbb{Z} = p\mathbb{Z}$. Thus, we have by the First Isomorphism Theorem for Rings that

$$\mathbb{Z}/p\mathbb{Z} = \mathbb{Z}/\ker\phi \simeq \phi(\mathbb{Z})$$

We claim that $\phi(\mathbb{Z}) = P$. Indeed, note that as P is a subfield of K that P must necessarily contain all elements of the form $m \cdot 1_K$ for each $m \in \mathbb{Z}$ so that $\phi(\mathbb{Z}) \subseteq P$. Moreover, since $\phi(\mathbb{Z}) \simeq \mathbb{Z}/p\mathbb{Z}$ and as p is a prime number it follows that $\phi(\mathbb{Z}) \subseteq K$ is a subfield of K. But since P contains no proper subfields of K and as $\phi(\mathbb{Z})$ is a subfield of K, we now have by the previous inclusion that $\phi(K) = P$. Finally, let $n = \dim_P(K)$. Then we have

$$|K| = |P|^{\dim_P(K)} = |P|^n = |\phi(\mathbb{Z})|^n = |\mathbb{Z}/p\mathbb{Z}|^n = p^n$$

This completes the proof of the first statement in the Lemma.

We now prove the second statement in the Lemma. Towards this end, first note that $|K^\times| = |K| - 1 = p^n - 1$. Now, let $a \in K$. If $a = 0$, then clearly $f(a) = 0$. If $a \neq 0$, then $a \in K^\times$ and hence by the previous observation we have

$$a^{p^n-1} = 1 \quad \text{so that} \quad a^{p^n} = a \quad \text{so that} \quad a^{p^n} - a = 0 \quad \text{so that} \quad f(a) = 0$$

Hence, if Γ denotes the set of roots of $f(x)$ then $K \subseteq \Gamma$. On the other hand, since $\deg(f(x)) = p^n$ we know that $|\Gamma| \leq p^n = |K|$. By the previous inclusion, then, we conclude that $K = \Gamma$ and hence it follows that K is a splitting field for $f(x)$ over P. $\square$

Lemma 2. Let F_1 and F_2 be finite fields with $|F_1| = |F_2|$. Then $F_1 \simeq F_2$.

Proof. Let P_1 and P_2 denote the prime subfields of F_1 and F_2, respectively. Since F_1 and F_2 are finite fields with $|F_1| = |F_2|$, it follows that $\mathrm{char}(F_1) = p = \mathrm{char}(F_2)$ where p is a prime number. Thus, by the proof of Lemma 1 it follows that $|F_1| = p^n = |F_2|$ for some positive integer n and that

$$P_1 \simeq \mathbb{Z}/p\mathbb{Z} \simeq P_2$$

Hence, there is an isomorphism of fields $\phi : P_1 \to P_2$. Now, consider the polynomial $f(x) = x^{p^n} - x \in P_1[x]$ and $g(x) = x^{p^n} - x \in P_2[x]$. By Lemma 1, we know that F_1 is a splitting field for $f(x)$ over P_1 and that F_2 is a splitting field for $g(x)$ over P_2. Moreover, notice that clearly $\phi(f(x)) = g(x)$. By the uniqueness of splitting fields, then, it follows that the isomorphism of fields $\phi : P_1 \to P_2$ may be extended to an isomorphism of fields $F_1 \to F_2$ so that $F_1 \simeq F_2$. This completes the proof. $\square$

Remark. We are now in a position to prove the main result.

Proof. Let p be a prime number and let n be a positive integer. Define $K = \mathbb{Z}/p\mathbb{Z}$. Then since p is a prime number, we know that K is a field. Now, consider the polynomial $f(x) = x^{p^n} - x \in K[x]$ and let F be a splitting field for $f(x)$ over K. Let $\Gamma \subseteq F$ denote the set of roots of $f(x)$. Notice that since clearly $\mathrm{char}(K) = p$, we have

$$f'(x) = p^n x^{p^n - 1} - 1 = 0 - 1 = -1$$

and hence it follows that $f(x)$ and $f'(x)$ are relatively prime polynomials so that $f(x)$ is separable. In particular, this gives that

$$|\Gamma| = \deg(f(x)) = p^n$$

We will use this observation below.

Next, let $a \in K$. By the same arguments as presented above, we have that $f(a) = 0$ so that $K \subseteq \Gamma$. Thus, we now obtain the inclusion $K \subseteq \Gamma \subseteq F$. Now, we claim that Γ is a field. Indeed, suppose that $a, b \in \Gamma$ so that

$$0 = f(a) = a^{p^n} - a \quad \text{so that} \quad a^{p^n} = a$$

and

$$0 = f(b) = b^{p^n} - b \quad \text{so that} \quad b^{p^n} = b$$

Furthermore, since $\mathrm{char}(K) = p$ it follows that $\mathrm{char}(F) = p$. Hence, we obtain by the above that

$$(a - b)^{p^n} = a^{p^n} - b^{p^n} = a - b$$

and

$$(ab)^{p^n} = a^{p^n} \cdot b^{p^n} = ab$$

and if $b \neq 0$

$$\left(\frac{a}{b}\right)^{p^n} = \frac{a^{p^n}}{b^{p^n}} = \frac{a}{b}$$

By the above results, then, we see that $f(a - b) = 0$, $f(ab) = 0$, and if $b \neq 0$ that $f(a/b) = 0$ so that $a - b, ab, a/b \in \Gamma$. We may now conclude that Γ is a field.

Finally, we may now assert by the above results and by the definition of Γ that Γ is a field extension of K such that $f(x) \in K[x]$ splits over Γ. However, recall the inclusion $K \subseteq \Gamma \subseteq F$ and that F is a splitting field for $f(x)$ over K. By the previous observation, then, we conclude that $F = \Gamma$ and hence

$$|F| = |\Gamma| = p^n$$

so that F is a field of order p^n. We may now conclude that for any prime number p and any positive integer n that there exists a field of order p^n. Moreover, we know by Lemma 2 that any two such fields must be isomorphic. This completes the proof. $\square$

Remark. By the results of the above Theorem, given a prime number p and a positive integer n we may denote *the* field of order p^n by $\mathbb{F}_{p^n}$.

Theorem. The map

$$\sigma : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n} \quad \text{by} \quad a \mapsto a^p$$

is an automorphism of $\mathbb{F}_{p^n}$. Moreover, we have that $\sigma \in \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ and $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ is a cyclic group with generator σ so that $\mathbb{F}_{p^n}/\mathbb{F}_p$ is a finite Galois extension.

Proof. Let $F = \mathbb{F}_{p^n}$ and note that clearly $\mathrm{char}(F) = p$. First, we show that σ is a field homomorphism. Towards this end, let $a, b \in F$. Then since $\mathrm{char}(F) = p$, we have

$$\sigma(a+b) = (a+b)^p = a^p + b^p = \sigma(a) + \sigma(b)$$

and

$$\sigma(ab) = (ab)^p = a^p b^p = \sigma(a)\sigma(b)$$

and

$$\sigma(1) = 1^p = 1$$

so that σ is a field homomorphism. Next, suppose that $a \in \ker \sigma$. Then

$$0 = \phi(a) = a^p$$

Since $a \in F$ and F has no zero divisors as F is a field, the above equality implies that $a = 0$ so that $\ker \sigma$ is trivial and hence σ is an injection. Thus, we see that in particular σ is an injection from the *finite* set F to itself so that σ must also be a surjection. We conclude that σ is an automorphism of $F = \mathbb{F}_{p^n}$.

Next, we show that $\sigma \in \mathrm{Gal}(F/\mathbb{F}_p)$. By the above result, it remains to prove that σ fixes $\mathbb{F}_p$. Indeed, suppose that $a \in \mathbb{F}^p$. Then we know by the arguments presented above that $a^p = a$ and hence

$$\sigma(a) = a^p = a$$

so that σ fixes $\mathbb{F}_p$. This shows that $\sigma \in \mathrm{Gal}(F/\mathbb{F}_p)$.

Finally, we show that $\mathrm{Gal}(F/\mathbb{F}_p)$ is generated by σ. Indeed, first notice that by previous arguments we may assert that

$$\begin{aligned} F^{\langle\sigma\rangle} &= \{a \in F : \sigma(a) = a\} \\ &= \{a \in F : a^p = a\} \\ &= \{a \in F : a \text{ is a root of } x^p - x \in \mathbb{F}_p[x]\} \\ &= \mathbb{F}_p \end{aligned}$$

and hence

$$|\sigma| = |\langle\sigma\rangle| = \left[F : F^{\langle\sigma\rangle}\right] = [F : \mathbb{F}_p] = [\mathbb{F}_{p^n} : \mathbb{F}_p] = \dim_{\mathbb{F}_p}(\mathbb{F}_{p^n}) = n$$

Therefore, we see that $\sigma \in \mathrm{Gal}(F/\mathbb{F}_p)$ is an element of $\mathrm{Gal}(F/\mathbb{F}_p)$ of order n. On the other hand, notice that by the same computation as above we have

$$|\mathrm{Gal}(F/\mathbb{F}_p)| \leq [F : \mathbb{F}_p] = n$$

Combining the previous two observations, then, we see that $\mathrm{Gal}(F/\mathbb{F}_p) = \langle \sigma \rangle$. We conclude that $\mathrm{Gal}(F/\mathbb{F}_p)$ is a cyclic group with generator σ. In particular, the above results show that

$$|\mathrm{Gal}(F/\mathbb{F}_p)| = |\langle \sigma \rangle| = n = [F : \mathbb{F}_p]$$

so that $\mathrm{Gal}(F/\mathbb{F}_p)$ is a finite Galois extension. □

Lemma. Suppose that m and n are positive integers and let p be a prime number. Then $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n}$ if and only if m divides n.

Proof. For the first direction, assume that $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n}$. Then

$$n = [\mathbb{F}_{p^n} : \mathbb{F}_p] = [\mathbb{F}_{p^n} : \mathbb{F}_{p^m}]\,[\mathbb{F}_{p^m} : \mathbb{F}_p] = [\mathbb{F}_{p^n} : \mathbb{F}_{p^m}] \cdot m$$

By the above equality, then, we conclude that m divides n. This completes the proof of the first direction.

For the second direction, assume that m divides n. First, recall by the above Theorem that $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ is a cyclic group of order n and hence contains a (unique) subgroup that corresponds to each positive positive divisor of its order. In particular, since m divides n it follows that $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ contains a subgroup H of order n/m. Moreover, by the above Theorem we may appeal to the Fundamental Theorem of Galois Theory to assert that

$$H = \mathrm{Gal}\left(\mathbb{F}_{p^n}/\mathbb{F}_{p^n}^H\right)$$

and

$$|G| = [\mathbb{F}_{p^n} : \mathbb{F}_p] \quad \text{and} \quad |H| = \left[\mathbb{F}_{p^n} : \mathbb{F}_{p^n}^H\right]$$

Thus, we obtain by the above that

$$\frac{n}{m} = |H| = \left[\mathbb{F}_{p^n} : \mathbb{F}_{p^n}^H\right] \quad \text{so that} \quad n = \left[\mathbb{F}_{p^n} : \mathbb{F}_{p^n}^H\right] \cdot m$$

However, recall that

$$n = |G| = [\mathbb{F}_{p^n} : \mathbb{F}_p] = \left[\mathbb{F}_{p^n} : \mathbb{F}_{p^n}^H\right]\left[\mathbb{F}_{p^n}^H : \mathbb{F}_p\right]$$

so that by the previous equality for n we now obtain

$$\left[\mathbb{F}_{p^n} : \mathbb{F}_{p^n}^H\right]\left[\mathbb{F}_{p^n}^H : \mathbb{F}_p\right] = \left[\mathbb{F}_{p^n} : \mathbb{F}_{p^n}^H\right] \cdot m \quad \text{so that} \quad m = \left[\mathbb{F}_{p^n}^H : \mathbb{F}_p\right]$$

Thus, we may now conclude that

$$\left|\mathbb{F}_{p^n}^H\right| = |\mathbb{F}_p|^{\left[\mathbb{F}_{p^n}^H : \mathbb{F}_p\right]} = |\mathbb{F}_p|^m = p^m$$

so that $\mathbb{F}_{p^n}^H = \mathbb{F}_{p^m}$ by the uniqueness of finite fields. Hence, we may now conclude that

$$\mathbb{F}_{p^m} = \mathbb{F}_{p^n}^H \subseteq \mathbb{F}_{p^n}$$

This completes the proof of the second direction. □

Theorem. Suppose that m and n are positive integers and that m divides n. Let p be a prime number and consider the field extension $\mathbb{F}_{p^n}/\mathbb{F}_{p^m}$ (which is actually a field extension by the above Lemma). Let $G = \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_{p^m})$ and let σ be the map as in the previous Theorem. Then $G = \langle \sigma^m \rangle$.

Proof. First, notice that

$$p^n = |\mathbb{F}_{p^n}| = |\mathbb{F}_{p^m}|^{[\mathbb{F}_{p^n}:\mathbb{F}_{p^m}]} = (p^m)^{[\mathbb{F}_{p^n}:\mathbb{F}_{p^m}]} = p^{m\cdot[\mathbb{F}_{p^n}:\mathbb{F}_{p^m}]}$$

and hence it follows that

$$[\mathbb{F}_{p^n} : \mathbb{F}_{p^m}] = \frac{n}{m}$$

Now, since $\mathbb{F}_{p^n}/\mathbb{F}_p$ is a finite Galois extension we know that $\mathbb{F}_{p^n}/\mathbb{F}_{p^m}$ is a finite Galois extension by the Fundamental Theorem of Galois Theory. This observation gives by the above that

$$|G| = [\mathbb{F}_{p^n} : \mathbb{F}_{p^m}] = \frac{n}{m}$$

Thus, since $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) = \langle \sigma \rangle$ and as $|\sigma| = n$ by the above Theorem we obtain by the above equality that

$$|\langle \sigma^m \rangle| = |\sigma^m| = \frac{|\sigma|}{m} = \frac{n}{m} = |G|$$

Finally, note that clearly $G \leq \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$. Moreover, recall that a finite cyclic group has a *unique* subgroup that corresponds to each positive divisor of its order. Thus, since G and $\langle \sigma^m \rangle$ are subgroups of the finite cyclic group $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ of order n/m we may now conclude that $G = \langle \sigma^m \rangle$. This completes the proof. $\square$

Topic 4: Cyclic and Cyclotomic Extensions

Definition. Let F/K be an algebraic field extension in the following definitions.

(a): An element $u \in F$ is ***separable*** if its minimum polynomial over K is separable.

(b): An element $u \in F$ is ***purely inseparable*** if its minimum polynomial over K is a power of a linear linear polynomial over a splitting field.

(c): The extension F/K is ***separable*** if every $u \in F$ is separable.

(d): The extension F/K is ***purely inseparable*** if every $u \in F$ is purely inseparable.

Theorem. Let F/K be an algebraic field extension. Then if $u, v \in F$ are separable over K, then the extension $K(u, v)/K$ is separable.

Proof. Let $f(x), g(x) \in K[x]$ denote the minimum polynomials over K for $u, v \in F$, respectively. Let E be a splitting field over $K(u, v)$ for the polynomial $f(x)g(x)$ so that E is also a splitting field for the polynomial $f(x)g(x)$ over K. Now, since u and v are separable it follows that $f(x)$ and $g(x)$ are separable polynomials and hence E/K is a finite Galois extension. Next, let $a \in E$ and define

$$\Gamma = \{\sigma(a) : \sigma \in \mathrm{Gal}(E/K)\}$$

and

$$p(x) = \prod_{\rho \in \Gamma} (x - \rho)$$

and note that $p(x)$ is clearly a separable polynomial. Moreover, since $1_E \in \mathrm{Gal}(E/K)$ we have that $a = 1_E(a) \in \Gamma$ and hence by the definition of $p(x)$ we see that $p(a) = 0$.

Next, recall that every element $\sigma \in \mathrm{Gal}(E/K)$ permutes Γ. Thus, it now follows by the definition of $p(x)$ that $\sigma(p(x)) = p(x)$ for each $\sigma \in \mathrm{Gal}(E/K)$ and since E/K is a finite Galois extension this observation implies that $p(x) \in K[x]$. We claim that $p(x)$ is irreducible in $K[x]$. Indeed, suppose that $q(x) \in K[x]$ is a nonconstant, monic polynomial which divides $p(x)$. Let ρ be a root of $q(x)$. Then since $q(x)$ divides $p(x)$, it follows that ρ is a root of $p(x)$ and hence $\rho \in \Gamma$. Now, since $q(x) \in K[x]$ it follows that since $q(x)$ has a root $\rho \in \Gamma$ that every element of Γ is a root of $q(x)$. Therefore, we see that $p(x)$ divides $q(x)$ and as $q(x)$ divides $p(x)$ this gives that $p(x) = q(x)$ so that $p(x)$ is irreducible. This completes the proof of our claim.

Finally, note that since $p(x)$ is a monic, irreducible polynomial in $K[x]$ which has a as a root it follows that $p(x)$ is the minimum polynomial for a over K. Since $p(x)$ is separable, then, we conclude that a is separable and as $a \in E$ was arbitrary this shows that E/K is a separable extension. It now follows that since $E \supseteq K(u, v)$ that $K(u, v)/K$ is a separable extension, completing the proof. $\square$

Theorem. Let F/K be an algebraic field extension. Then if $u, v \in F$ are purely inseparable over K, then the extension $K(u, v)/K$ is purely inseparable.

Proof. Let $a \in K(u,v)$ and let $f(x), g(x), h(x) \in K[x]$ denote the minimum polynomials over K for $a, u, v \in F$, respectively. Let E be a splitting field over $K(u,v,a)$ for the polynomial $f(x)g(x)h(x)$. Clearly, we have that E is also a splitting field for the polynomial $f(x)g(x)h(x)$ over K. Now, suppose that $b \in E$ is a root of $f(x)$. Then since a and b are roots of the same irreducible polynomial $f(x) \in K[x]$, we have that

$$K(a) \simeq \frac{K[x]}{(f(x))} \simeq K(b)$$

and hence as E is a splitting field for $f(x)g(x)h(x)$ over K it follows by the same argument presented multiple times above that there is some $\sigma \in \mathrm{Gal}(E/K)$ such that $\sigma(a) = b$. Now, since $\sigma \in \mathrm{Gal}(E/K)$ it follows that σ permutes the roots of the polynomials $g(x)$ and $h(x)$. But recall that since u and v are purely inseparable over K that u is the unique root of $g(x)$ and that v is the unique root of $h(x)$. Therefore, we have by the previous observation that $\sigma(a) = a$ and $\sigma(b) = b$.

Finally, note that as $\sigma \in \mathrm{Gal}(E/K)$ that σ fixes K and by the above we also have that σ fixes a and b. Therefore, we see that σ fixes $K(u,v)$. In particular, since $a \in K(u,v)$ this gives that

$$b = \sigma(a) = a$$

so that $b = a$. Thus, as b was as arbitrary root of $f(x)$ it now follows that a is the unique root of $f(x)$. Since $f(x)$ is the minimum polynomial for a over K, then, we may now conclude that a is purely inseparable over K. Since $a \in K(u,v)$ was arbitrary, we conclude that $K(u,v)/K$ is a purely inseparable extension. This completes the proof. $\square$

Definition. Let F/K be a finite Galois extension and let $\mathrm{Gal}(F/K) = \{\sigma_1, \ldots, \sigma_r\}$. Let $u \in F$. Then the ***norm*** of u with respect to F/K, denoted $N(u)$, is defined by

$$N(u) = \prod_{i=1}^{r} \sigma_i(u)$$

and the ***trace*** of u with respect to F/K, denoted $\mathrm{Tr}(u)$, is defined by

$$\mathrm{Tr}(u) = \sum_{i=1}^{r} \sigma_i(u)$$

Remark. For each $u \in F$, we have $N(u), \mathrm{Tr}(u) \in K$ so that N and Tr are maps $N : F \to K$ and $\mathrm{Tr} : F \to K$.

Remark. The map N from above is multiplicative. That is, for any $u, v \in F$ we have $N(uv) = N(u)N(v)$.

Remark. The map Tr from above is a K-linear map. That is, for any $k \in K$ and $u, v \in F$ we have $\mathrm{Tr}(ku + v) = k\mathrm{Tr}(u) + \mathrm{Tr}(v)$.

Definition. A field extension F/K is said to be ***cyclic*** if F/K is a finite Galois extension and $\mathrm{Gal}(F/K)$ is a cyclic group.

Theorem. Let F/K be a cyclic field extension and let $n = [F : K]$ and $\mathrm{Gal}(F/K) = \langle \sigma_0 \rangle$ for some $\sigma_0 \in \mathrm{Gal}(F/K)$. Let $u \in F$. Then

(a): $\mathrm{Tr}(u) = 0$ if and only if there is some $v \in F$ such that $u = v - \sigma_0(v)$.

(b): (Hilbert's Theorem 90): $N(u) = 1$ if and only if there is some $v \in F^\times$ such that $u = v\sigma_0(v)^{-1}$.

Proof. (a): Define a map

$$\phi : F \to F \quad \text{by} \quad v \mapsto v - \sigma_0(v)$$

Then it is immediate that ϕ is a well-defined K-linear map. Now, we claim that $\phi(F) \subseteq \ker \mathrm{Tr}$. Indeed, suppose that $x \in \phi(F)$ so that

$$x = \phi(w) = w - \sigma_0(w)$$

for some $w \in F$. Then since Tr is a K-linear map, we obtain

$$\begin{aligned}
\mathrm{Tr}(x) &= \mathrm{Tr}(w - \sigma_0(w)) \\
&= \mathrm{Tr}(w) - \mathrm{Tr}(\sigma_0(w)) \\
&= \sum_{i=1}^{n} \sigma_0^i(w) - \sum_{i=1}^{n} \sigma_0^i(\sigma_0(w)) \\
&= \sum_{i=1}^{n} [\sigma_0^i(w) - \sigma_0^{i+1}(w)] \\
&= (\sigma_0(w) - \sigma_0^2(w)) + (\sigma_0^2(w) - \sigma_0^3(w)) + \cdots + (\sigma_0^n(w) - \sigma_0^{n+1}(w)) \\
&= \sigma_0(w) - \sigma_0^{n+1}(w) \\
&= \sigma_0(w) - \sigma_0(w) \\
&= 0
\end{aligned}$$

which completes the proof of our claim.

Now, since $\mathrm{Tr} : F \to K$ is a K-linear map it follows that $\mathrm{Tr}(F)$ is a sub K-vector space over K so that $\mathrm{Tr}(F) \in \{\{0\}, K\}$. If $\mathrm{Tr}(F) = \{0\}$, then it follows that

$$1_F + \sigma_0 + \cdots + \sigma_0^{n-1} = 0$$

However, recall that the set $\{1_F, \sigma_0, \ldots, \sigma_0^{n-1}\}$ is linearly independent over F so that in particular we have $\mathrm{Tr}(F) \neq \{0\}$ so that $\mathrm{Tr}(F) = K$. Therefore, we see that $\dim_K(\ker \mathrm{Tr}) = n-1$. Moreover, we clearly have $\ker \phi = K$ so that $\dim_K(\phi(F)) = n-1$. By the previous two results, the inclusion $\phi(F) \subseteq \ker \mathrm{Tr}$ implies that $\phi(F) = \ker \mathrm{Tr}$.

Finally, suppose that $\mathrm{Tr}(u) = 0$. Then $u \in \ker \mathrm{Tr} = \phi(F)$ and hence there is some element $v \in F$ such that

$$u = \phi(v) = v - \sigma_0(v)$$

On the other hand, suppose that $u = v - \sigma_0(v)$ for some $v \in F$. Then $u = v - \sigma_0(v) = \phi(v)$ so that $u \in \phi(F) = \ker \mathrm{Tr}$. Thus, we obtain that $\mathrm{Tr}(u) = 0$. This completes the proof of both directions. $\square$

Proof. (b): For the first direction, assume that $N(u) = 1$. Since $\{1_F, \sigma_0, \ldots, \sigma_0^{n-1}\}$ is linearly independent over F, it follows that there is some $y \in F$ and some $v \in F^\times$ with

$$(u)y + (u\sigma_0(u))\sigma_0(y) + (u\sigma_0(u)\sigma_0^2(u))\sigma_0^2(y) + \cdots + (u\sigma_0(u)\cdots\sigma_0^{n-1}(u))\sigma_0^{n-1}(y) = v$$

However, recall by hypothesis that

$$1 = N(u) = \prod_{i=1}^{n} \sigma_0^i(u) = u\sigma_0(u)\cdots\sigma_0^{n-1}(u)$$

so that the above equality becomes

$$v = uy + u\sigma_0(u)\sigma_0(y) + u\sigma_0(u)\sigma_0^2(u)\sigma_0^2(y) + \cdots + \sigma_0^{n-1}(y)$$

and hence

$$\begin{aligned}
\sigma_0(v) &= \sigma_0(uy + u\sigma_0(u)\sigma_0(y) + u\sigma_0(u)\sigma_0^2(u)\sigma_0^2(y) + \cdots + \sigma_0^{n-1}(y)) \\
&= \sigma_0(u)\sigma_0(y) + \sigma_0(u)\sigma_0^2(u)\sigma_0^2(y) + \sigma_0(u)\sigma_0^2(u)\sigma_0^3(u)\sigma_0^3(y) \\
&+ \cdots + \sigma_0(u)\sigma_0^2(u)\cdots\sigma_0^{n-1}(u)\sigma_0^{n-1}(y) + \sigma_0^n(y) \\
&= \sigma_0(u)\sigma_0(y) + \sigma_0(u)\sigma_0^2(u)\sigma_0^2(y) + \sigma_0(u)\sigma_0^2(u)\sigma_0^3(u)\sigma_0^3(y) \\
&+ \cdots + \sigma_0(u)\sigma_0^2(u)\cdots\sigma_0^{n-1}(u)\sigma_0^{n-1}(y) + y
\end{aligned}$$

Left-multiplying both sides of the above equality by u, we obtain

$$\begin{aligned}
u\sigma_0(v) &= u\sigma_0(u)\sigma_0(y) + u\sigma_0(u)\sigma_0^2(u)\sigma_0^2(y) + u\sigma_0(u)\sigma_0^2(u)\sigma_0^3(u)\sigma_0^3(y) \\
&+ \cdots + u\sigma_0(u)\sigma_0^2(u)\cdots\sigma_0^{n-1}(u)\sigma_0^{n-1}(y) + uy \\
&= uy + u\sigma_0(u)\sigma_0(y) + u\sigma_0(u)\sigma_0^2(u)\sigma_0^2(y) + \cdots + u\sigma_0(u)\sigma_0^2(u)\cdots\sigma_0^{n-1}(u)\sigma_0^{n-1}(y) \\
&= v
\end{aligned}$$

Finally, recall that $N(u) = 1 \neq 0$ so that $0 \neq u \in F$ and hence as F is a field we have that u^{-1} exists in F. Thus, left-multiplying both sides of the above equality by u^{-1} gives $\sigma_0(v) = u^{-1}v$ which gives $u = v\sigma_0(v)^{-1}$, completing the proof of the first direction.

For the second direction, assume that $u = v\sigma_0(v)^{-1}$ for some $v \in F^\times$. Then we have since N is a multiplicative map that

$$\begin{aligned}
N(u) &= N\left(v\sigma_0(v)^{-1}\right) \\
&= N(v)N(\sigma_0(v)^{-1}) \\
&= N(v)N(\sigma_0(v^{-1})) \\
&= N(v)\prod_{i=1}^{n}\sigma_0^i(\sigma_0(v^{-1})) \\
&= N(v)\prod_{i=1}^{n}\sigma_0^{i+1}(v^{-1}) \\
&= N(v)\left[\sigma_0^2(v^{-1})\sigma_0^3(v^{-1})\cdots\sigma_0^{n-1}(v^{-1})\sigma_0^n(v^{-1})\sigma_0^{n+1}(v^{-1})\right] \\
&= N(v)\left[\sigma_0(v^{-1})\sigma_0^2(v^{-1})\cdots\sigma_0^{n-1}(v^{-1})\sigma_0^n(v^{-1})\right] \\
&= N(v)\left[\sigma_0(v)\sigma_0^2(v)\cdots\sigma_0^{n-1}(v)\sigma_0^n(v)\right]^{-1} \\
&= N(v)N(v)^{-1} \\
&= 1
\end{aligned}$$

This completes the proof of the second direction. □

Theorem. Let n be a positive integer and let K be a field which contains a primitive nth root of unity and F be an extension field of K. Then the following are equivalent.

(a): F is cyclic of degree d over K, where d divides n.

(b): F is a splitting field over K of a polynomial of the form $x^n - a \in K[x]$.

(c): F is a splitting field over K of an irreducible polynomial of the form $x^d - b \in K[x]$, where d divides n.

Proof. ((c) $\Rightarrow$ (b)): Let $v \in F$ be a root of $x^d - b$ so that $v^d = b$. Then the roots of $x^d - b$ are $v, v\eta, v\eta^2, \ldots, v\eta^{d-1}$, where η is a primitive dth root of unity. Moreover, since K contains a primitive nth root of unity and as d divides n it follows that $\eta \in K$. Therefore, since F is a splitting field for $x^d - b$ over K it follows that $F = K(v)$.

Now, let $a = b^{n/d} \in K$ and consider the polynomial $x^n - a \in K[x]$. By hypothesis, there is a primitive nth root of unity $\zeta \in K$. Now, notice that

$$(\zeta v)^n = \zeta^n v^n = 1 \cdot v^n = v^{d(n/d)} = b^{n/d} = a$$

and hence it follows that ζv is a root of $x^n - a$. Therefore, again using the fact that $\zeta \in K$ it now follows that $K(v) = F$ is a splitting field for $x^n - a$ over K.

((b) $\Rightarrow$ (a)): Let $u \in F$ be a root of $x^n - a$ so that $F = K(u)$. If $a = 0$, then $K = F$ and hence it follows that F/K is a cyclic extension of degree 1 which clearly divides n. Therefore, assume that $a \neq 0$ so that $u \neq 0$. Now, suppose that $\sigma \in \mathrm{Gal}(F/K)$. Then we know that σ permutes the roots of $x^n - a$ so that $\sigma(u) = \zeta u$, where $\zeta \in K$ is an nth root of unity.

Next, let R be the group of all nth roots of unity in $K^\times$ and observe that R is a cyclic group of order n. By the observations made in the above paragraph, then, we may assert that the map

$$\phi : \mathrm{Gal}(F/K) \to R \quad \text{by} \quad \sigma \mapsto \frac{\sigma(u)}{u}$$

is well-defined. Now, suppose that $v \in F$ is a root of $x^n - a$ so that $v = \zeta u$ for some $\zeta \in R \subseteq K^\times \subseteq K$. Then we obtain

$$\sigma(v) = \sigma(\zeta u) = \zeta\sigma(u) = \zeta u\frac{\sigma(u)}{u} = \zeta u\phi(\sigma) = v\phi(\sigma) \quad \text{for each} \quad \sigma \in \mathrm{Gal}(F/K)$$

By this result, then, we see that if $\sigma_1, \sigma_2 \in \mathrm{Gal}(F/K)$ that

$$\phi(\sigma_1 \circ \sigma_2) = \frac{(\sigma_1 \circ \sigma_2)(u)}{u} = \frac{\sigma_1(\sigma_2(u))}{u} = \frac{\sigma_1(u\phi(\sigma_2))}{u} = \frac{\sigma_1(u)}{u} \cdot \sigma_1(\phi(\sigma_2)) = \phi(\sigma_1)\phi(\sigma_2)$$

and hence ϕ is a group homomorphism.

Now, suppose that $\sigma \in \ker\phi$ so that

$$1 = \phi(\sigma) = \frac{\sigma(u)}{u} \quad \text{so that} \quad \sigma(u) = u$$

Therefore, we see that σ fixes u and since σ clearly fixes K we have that σ fixes $K(u) = F$ so that $\sigma = 1_F$. In particular, this shows that $\ker\phi$ is trivial so that since ϕ is a group homomorphism we have that ϕ is an injection. We may now conclude by the First Isomorphism Theorem that $\mathrm{Gal}(F/K)$ is isomorphic to a subgroup of the cyclic group R and hence $\mathrm{Gal}(F/K)$ is cyclic.

Finally, recall that the roots of $x^n - a$ are given by $u, u\zeta, u\zeta^2, \ldots, u\zeta^{n-1}$ where $\zeta \in K$ is a primitive nth root of unity. In particular, this observation shows that the roots of $x^n - a$ in the splitting field F for $x^n - a$ over K are all distinct so that $x^n - a$ is a separable polynomial. Hence, we conclude that F/K is a finite Galois extension. Since $\mathrm{Gal}(F/K)$ is a cyclic group by the above, then, we see that F/K is a cyclic extension. Moreover, suppose that d is the degree of the extension F/K. Since F/K is a finite Galois extension, we then have that

$$|\mathrm{Gal}(F/K)| = [F : K] = d$$

and since $\mathrm{Gal}(F/K)$ is isomorphic to a subgroup of the group R of order n it now follows by Lagrange's Theorem that d divides n.

((a) $\Rightarrow$ (c)): Since F/K is a cyclic extension, we have in particular that F/K is a finite Galois extension so that by hypothesis we have

$$|\mathrm{Gal}(F/K)| = [F : K] = d$$

Since $\mathrm{Gal}(F/K)$ is a cyclic group, there is some $\sigma \in \mathrm{Gal}(F/K)$ with $\mathrm{Gal}(F/K) = \langle\sigma\rangle$. Thus, the above observation gives that $\mathrm{Gal}(F/K) = \{1_F, \sigma, \ldots, \sigma^{d-1}\}$.

Now, by hypothesis there is some primitive nth root of unity in K and since d divides n this implies that there is a primitive dth root of unity $\eta \in K$. But since $\eta \in K$, we

have that $\tau(\eta) = \eta$ for each $\tau \in \mathrm{Gal}(F/K)$. This gives that

$$N(\eta) = \prod_{i=1}^{d} \sigma^i(\eta) = \prod_{i=1}^{d} \eta = \eta^d = 1$$

and hence by Hilbert's Theorem 90 there is some $w \in F^\times$ such that $w^{-1}\eta = \sigma(w^{-1})$. Thus, if we let $\alpha = w^{-1} \in F^\times$, then we have the equality $\sigma(\alpha) = \alpha\eta$.

Next, we show that $\alpha^d \in K$ by first showing that $\tau(\alpha^d) = \alpha^d$ for each $\tau \in \mathrm{Gal}(F/K)$. Indeed, we clearly have $1_F(\alpha^d) = \alpha^d$. Next, we have

$$\sigma(\alpha^d) = [\sigma(\alpha)]^d = (\alpha\eta)^d = \alpha^2\eta^d = \alpha^d \cdot 1 = \alpha^d$$

and

$$\sigma^2(\alpha^d) = \sigma(\sigma(\alpha^d)) = \sigma(\alpha^d) = \alpha^d$$

and so on so that $\sigma^i(\alpha^d) = \alpha^d$ for each $i \in \{1, \ldots, d\}$. This result shows that $\tau(\alpha^d) = \alpha^d$ for each $\tau \in \mathrm{Gal}(F/K)$ and since F/K is a finite Galois extension, this observation gives that $\alpha^d \in K$.

Now, let $b = \alpha^d$ define the polynomial $p(x) = x^d - b$ so that $p(x) \in K[x]$ by the above result. We will show that $p(x)$ is irreducible. Indeed, first note that clearly $1_F(\alpha) = \alpha$. Next, we have $\sigma(\alpha) = \alpha\eta$ and hence as $\eta \in K$ we have

$$\sigma^2(\alpha) = \sigma(\sigma(\alpha)) = \sigma(\alpha\eta) = \sigma(\alpha)\sigma(\eta) = \alpha\eta \cdot \eta = \alpha\eta^2$$

Inductively, then, we see that $\sigma^i(\alpha) = \alpha\eta^i$ for each $i \in \{1, \ldots, d\}$. In particular, we may now assert that $\sigma^i : K(\alpha) \to K(\alpha\eta^i)$ is a K-homomorphism which is an isomorphism such that $\sigma^i(\alpha) = \alpha\eta^i$ for each $i \in \{1, \ldots, d\}$. Thus, this result shows that $\alpha, \alpha\eta, \ldots, \alpha\eta^{d-1}$ all share the same minimum polynomial over K.

Next, suppose that $m(x) \in K[x]$ is the minimum polynomial for α over K. By the previous observation, we have that $\alpha, \alpha\eta, \ldots, \alpha\eta^{d-1}$ are distinct roots of $m(x)$ so that $\deg(m(x)) \geq d$ and hence

$$[K(\alpha) : K] = \deg(m(x)) \geq d$$

On the other hand, we have

$$d = [F : K] = [F : K(\alpha)][K(\alpha) : K]$$

and hence $[K(\alpha) : K] \leq d$. By the previous two inequalities, then, we have that $[K(\alpha) : K] = d$ so that

$$\deg(m(x)) = [K(\alpha) : K] = d$$

But recall that $p(x) \in K[x]$ is a monic polynomial of degree d and that

$$p(\alpha) = \alpha^d - b = \alpha^d - \alpha^d = 0$$

so that α is a root of $p(x)$. Therefore, since $m(x)$ is the minimum polynomial for α over K it now follows that $p(x) = m(x)$ and hence as $m(x)$ is irreducible we conclude that $p(x)$ is irreducible.

Finally, it remains to prove that F is a splitting field over K for $p(x) \in K[x]$. First, note that the roots of $p(x)$ are given by $\alpha, \alpha\eta, \ldots, \alpha\eta^{d-1}$ so that by the same arguments as presented above we have that $K(\alpha)$ is a splitting field for $p(x)$ over K. But note that

$$d = [F : K] = [F : K(\alpha)][K(\alpha) : K] = [F : K(\alpha)] \cdot d$$

so that $[F : K(\alpha)] = 1$ and hence $F = K(\alpha)$ so that F is a splitting field for $p(x)$ over K. This completes the proof. $\square$

Definition 1. Let n be a positive integer and consider $f(x) = x^n - 1 \in \mathbb{Q}[x]$. Let F be a splitting field for $f(x)$ over $\mathbb{Q}$. Then the field extension $F/\mathbb{Q}$ is called the ***cyclotomic extension of order*** n.

Theorem. Let $F/\mathbb{Q}$ be the cyclotomic extension of order n. Then $\mathrm{Gal}(F/\mathbb{Q})$ is abelian.

Proof. First, note that since $\mathrm{char}(\mathbb{Q}) = 0$ we have that $F/\mathbb{Q}$ is a finite Galois extension. Now, notice that the roots of $f(x) = x^n - 1$ are exactly $1, \zeta, \ldots, \zeta^{n-1}$ where ζ is a primitive nth root of unity and hence it follows that $F = \mathbb{Q}(\zeta)$. In particular, this observation shows that any element $\sigma \in \mathrm{Gal}(F/\mathbb{Q})$ is completely determined by the image of ζ under σ.

Now, fix any element $\sigma \in \mathrm{Gal}(F/\mathbb{Q})$. Then σ permutes the roots $1, \zeta, \ldots, \zeta^{n-1}$ of $f(x)$ so that $\sigma(\zeta) = \zeta^i$ for some $i \in \{1, \ldots, n\}$. By the same reasoning, we have that $\sigma^{-1}(\zeta) = \zeta^j$ for some $j \in \{1, \ldots, n\}$. Thus, we obtain

$$\zeta = 1_F(\zeta) = (\sigma^{-1} \circ \sigma)(\zeta) = \sigma^{-1}(\zeta^i) = \left[\sigma^{-1}(\zeta)\right]^i = (\zeta^j)^i = \zeta^{ij}$$

and as ζ is a primitive nth root of unity the above equality implies that $ij \equiv 1 \bmod n$. In particular, this gives that $\overline{i} \in \mathbb{Z}/n\mathbb{Z}$ is a unit of $\mathbb{Z}/n\mathbb{Z}$.

Next, define a map $\phi : \mathrm{Gal}(F/\mathbb{Q}) \to (\mathbb{Z}/n\mathbb{Z})^\times$ as follows. For any $\sigma \in \mathrm{Gal}(F/\mathbb{Q})$, we know by the above that $\sigma(\zeta) = \zeta^i$ for some $i \in \{1, \ldots, n\}$ and that $\overline{i} \in \mathbb{Z}/n\mathbb{Z}$ is a unit of $\mathbb{Z}/n\mathbb{Z}$; define $\phi(\sigma) = \overline{i}$. We will show that ϕ is well-defined. Towards this end, suppose that $\zeta^i = \sigma(\zeta) = \zeta^j$ and assume without loss of generality that $j \leq i$. Then by this equality, we obtain that

$$\zeta^j(\zeta^{i-j} - 1) = 0 \quad \text{so that} \quad \zeta^{i-j} = 1 \quad \text{so that} \qquad i - j \equiv 0 \bmod n$$

and hence

$$\overline{i} - \overline{j} = \overline{i - j} = \overline{0} \quad \text{so that} \quad \overline{i} = \overline{j}$$

The above equality shows that ϕ is a well-defined map.

Next, we show that ϕ is an injective group homomorphism. First, suppose that $\sigma_1, \sigma_2 \in \mathrm{Gal}(F/\mathbb{Q})$ and that $\sigma_1(\zeta) = \zeta^{i_1}$ and $\sigma_2(\zeta) = \zeta^{i_2}$. Then we have that

$$(\sigma_1 \circ \sigma_2)(\zeta) = \sigma_1(\sigma_2(\zeta)) = \sigma_1(\zeta^{i_2}) = [\sigma(\zeta)]^{i_2} = (\zeta^{i_1})^{i_2} = \zeta^{i_1 i_2}$$

and hence

$$\phi(\sigma_1 \circ \sigma_2) = \overline{i_1 i_2} = \overline{i_1} \cdot \overline{i_2} = \phi(\sigma_1)\phi(\sigma_2)$$

so that ϕ is a group homomorphism. Finally, let $\sigma \in \ker \phi$ and suppose that $\sigma(\zeta) = \zeta^i$. Then we obtain

$$\overline{1} = \phi(\sigma) = \overline{i}$$

so that $i \equiv 1 \mod n$ and hence we may write $i = nk + 1$ for some $k \in \mathbb{Z}$. Therefore, we see that since ζ is a primitive nth root of unity that

$$\sigma(\zeta) = \zeta^i = \zeta^{nk+1} = \zeta^{nk} \cdot \zeta = (\zeta^n)^k \cdot \zeta = 1^k \cdot \zeta = 1 \cdot \zeta = \zeta$$

Hence, we see that σ fixes ζ and as σ clearly fixes $\mathbb{Q}$ we have that σ fixes $\mathbb{Q}(\zeta) = F$. Thus, we conclude that $\sigma = 1_F$ so that $\ker \phi$ is trivial and as ϕ is a group homomorphism this gives that ϕ is an injection.

Finally, note that by the above results we obtain an injective group homomorphism $\phi : \mathrm{Gal}(F/\mathbb{Q}) \to (\mathbb{Z}/n\mathbb{Z})^\times$ so that by the First Isomorphism Theorem we see that $\mathrm{Gal}(F/\mathbb{Q})$ is isomorphic to a subgroup of $(\mathbb{Z}/n\mathbb{Z})^\times$. But since $(\mathbb{Z}/n\mathbb{Z})^\times$ is clearly an abelian group and as subgroups of abelian groups are abelian, this gives that $\mathrm{Gal}(F/\mathbb{Q})$ is abelian, completing the proof. $\square$

Corollary. Let $F/\mathbb{Q}$ be the cyclotomic extension of order n. Then

(a): $[F : \mathbb{Q}] = \phi(n)$, where ϕ is Euler's totient function. In particular, we have that $\mathrm{Gal}(F/\mathbb{Q}) \simeq (\mathbb{Z}/n\mathbb{Z})^\times$.

(b): If n is a prime number, then $\mathrm{Gal}(F/\mathbb{Q})$ is cyclic.

Proof. (a): Similarly as in the above proof, let ζ be a primitive nth root of unity so that $F = \mathbb{Q}(\zeta)$. Let $g_n(x) \in \mathbb{Q}[x]$ denote the nth cyclotomic polynomial. Then we know that $g_n(x)$ is irreducible over $\mathbb{Q}$ and has ζ as a root. Therefore, we see that $g_n(x)$ is the minimum polynomial for ζ over $\mathbb{Q}$ and hence

$$[F : \mathbb{Q}] = [\mathbb{Q}(\zeta) : \mathbb{Q}] = \deg(g_n(x)) = \phi(n)$$

Finally, recall by the above that $\phi : \mathrm{Gal}(F/\mathbb{Q}) \to (\mathbb{Z}/n\mathbb{Z})^\times$ is an injective group homomorphism. But by the above result and by elementary Group Theory, we know that

$$|\mathrm{Gal}(F/\mathbb{Q})| = \phi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times|$$

Therefore, we see that ϕ is an injection between two finite sets of the same cardinality so that ϕ must also be surjective. Hence, we conclude that ϕ is a group isomorphism so that $\mathrm{Gal}(F/\mathbb{Q}) \simeq (\mathbb{Z}/n\mathbb{Z})^\times$. $\square$

Proof. (b): By the proof of the above Theorem, we know that $\mathrm{Gal}(F/\mathbb{Q})$ is isomorphic to a subgroup of $(\mathbb{Z}/n\mathbb{Z})^\times$. Now, if n is a prime number then we know that $\mathbb{Z}/n\mathbb{Z}$ is a finite field and hence it follows that $(\mathbb{Z}/n\mathbb{Z})^\times$ is a cyclic group as the group of units of a finite field form a cyclic group. Thus, we see that $\mathrm{Gal}(F/\mathbb{Q})$ is isomorphic to a subgroup of the *cyclic* group $(\mathbb{Z}/n\mathbb{Z})^\times$ and hence $\mathrm{Gal}(F/\mathbb{Q})$ is cyclic. $\square$

Example. Let $F/\mathbb{Q}$ be the cyclotomic extension of order 8. Then $\mathrm{Gal}(F/\mathbb{Q})$ is of order 4 and is not cyclic.

Proof. First, we have by the above that

$$|\mathrm{Gal}(F/\mathbb{Q})| = [F : \mathbb{Q}] = \phi(8) = 4$$

so that $\mathrm{Gal}(F/\mathbb{Q})$ is of order 4. Next, we also know by the above that

$$\mathrm{Gal}(F/\mathbb{Q}) \simeq (\mathbb{Z}/8\mathbb{Z})^\times = \left\{\overline{1}, \overline{3}, \overline{5}, \overline{7}\right\}$$

Furthermore, notice that

$$(\overline{3})^2 = \overline{9} = \overline{1} \quad \text{and} \quad (\overline{5})^2 = \overline{25} = \overline{1}$$

so that $(\mathbb{Z}/8\mathbb{Z})^\times$ contains two distinct elements of order 2. In particular, this implies that $(\mathbb{Z}/8\mathbb{Z})^\times \simeq V_4$ and since V_4 is clearly not a cyclic group we see that $(\mathbb{Z}/8\mathbb{Z})^\times$ is not a cyclic group. Thus, since $\mathrm{Gal}(F/\mathbb{Q}) \simeq (\mathbb{Z}/8\mathbb{Z})^\times$ we conclude that $\mathrm{Gal}(F/\mathbb{Q})$ is not cyclic. This completes the proof. □

Example. Let $F/\mathbb{Q}$ be the cyclotomic extension of order 5. Determine $\mathrm{Gal}(F/\mathbb{Q})$ and all intermediate fields of the field extension $F/\mathbb{Q}$.

Proof. Since 5 is a prime number, we know that

$$\mathrm{Gal}(F/\mathbb{Q}) \simeq (\mathbb{Z}/5\mathbb{Z})^\times \simeq \mathbb{Z}/4\mathbb{Z}$$

so that $\mathrm{Gal}(F/\mathbb{Q})$ is the cyclic group of order 4. Next, we find the intermediate fields of the field extension $F/\mathbb{Q}$. Since $F/\mathbb{Q}$ is a finite Galois extension, it follows by the Fundamental Theorem of Galois Theory that the intermediate fields of $F/\mathbb{Q}$ are in a one-to-one correspondence with the set of subgroups of $\mathbb{Z}/4\mathbb{Z}$, which are exactly $\{0\}, \mathbb{Z}/2\mathbb{Z}$, and $\mathbb{Z}/4\mathbb{Z}$. Furthermore, we know that under the Galois correspondence we have

$$F \mapsto \mathrm{Gal}(F/F) \simeq \{0\}$$

and

$$\mathbb{Q} \mapsto \mathrm{Gal}(F/\mathbb{Q}) \simeq \mathbb{Z}/4\mathbb{Z}$$

Thus, there is exactly one intermediate field K of the extension $F/\mathbb{Q}$ with $\mathbb{Q} \subsetneq K \subsetneq F$.

Now, recall that $F = \mathbb{Q}(\zeta)$ where ζ is a primitive 5th root of unity. Furthermore, by the above observations we have

$$K \mapsto \mathrm{Gal}(F/K) = \mathrm{Gal}(\mathbb{Q}(\zeta)/K) \simeq \mathbb{Z}/2\mathbb{Z}$$

Thus, since $\mathbb{Z}/2\mathbb{Z}$ is the cyclic group of order 2 it follows that $\mathrm{Gal}(F/K) = \langle\sigma\rangle$ where $\sigma : \mathbb{Q}(\zeta) \to \mathbb{Q}(\zeta)$ is such that $|\sigma| = 2$. In particular, this implies that $\sigma^2(\zeta) = \zeta$ and hence we must have $\sigma(\zeta) = \zeta^4$. Next, recall that by the Fundamental Theorem of Galois Theory that $K = F^{\langle\sigma\rangle}$ and since $\langle\sigma\rangle = \{1_F, \sigma\}$ this gives observation gives that

$$K = F^{\langle\sigma\rangle} = \{u \in \mathbb{Q}(\zeta) : \sigma(u) = u\}$$

We now calculate K based on the above observation.

Towards this end, first let $u \in K$. Then $\sigma(u) = u$ since $u \in K$ and as σ fixes K and since $u \in \mathbb{Q}(\zeta)$, we may write

$$u = q_0 + q_1\zeta + q_2\zeta^2 + q_3\zeta^3 + q_4\zeta^4$$

for some $q_0, q_1, q_2, q_3, q_4 \in \mathbb{Q}$. Thus, by the definition of σ and as $\sigma(u) = u$ we obtain

$$\begin{aligned} q_0 + q_1\zeta + q_2\zeta^2 + q_3\zeta^3 + q_4\zeta^4 &= \sigma(q_0 + q_1\zeta + q_2\zeta^2 + q_3\zeta^3 + q_4\zeta^4) \\ &= q_0 + q_1\sigma(\zeta) + q_2\sigma(\zeta^2) + q_3\sigma(\zeta^3) + q_4\sigma(\zeta^4) \\ &= q_0 + q_1\zeta^4 + q_2\zeta^8 + q_3\zeta^{12} + q_4\zeta^{16} \\ &= q_0 + q_4\zeta + q_3\zeta^2 + q_2\zeta^3 + q_1\zeta^4 \end{aligned}$$

so that $q_1 = q_4$ and $q_2 = q_3$ so that

$$u = q_0 + q_1(\zeta + \zeta^4) + q_2(\zeta^2 + \zeta^3)$$

But as $\zeta^2 + \zeta^3 = (\zeta + \zeta^4)^2 - 2 \in \mathbb{Q}(\zeta + \zeta^4)$, the above equality gives that $u \in \mathbb{Q}(\zeta + \zeta^4)$ which gives that $K \subseteq \mathbb{Q}(\zeta + \zeta^4)$.

On the other hand, suppose that $u \in \mathbb{Q}(\zeta + \zeta^4)$. First, observe that

$$\sigma(\zeta + \zeta^4) = \sigma(\zeta) + \sigma(\zeta^4) = \zeta^4 + \zeta^{16} = \zeta^4 + \zeta = \zeta + \zeta^4$$

so that σ fixes $\zeta + \zeta^4$. Hence, as ζ also clearly fixes $\mathbb{Q}$ it now follows that $\sigma(u) = u$ which gives that $\mathbb{Q}(\zeta + \zeta^4) \subseteq K$. The previous results now show that $K = \mathbb{Q}(\zeta + \zeta^4)$. We conclude that the intermediate fields of the extension $F/\mathbb{Q}$ are exactly $F, \mathbb{Q}(\zeta + \zeta^4)$, and $\mathbb{Q}$. This completes the proof. $\square$

Topic 5: Algebraic Independence; Transcendence Bases

Definition. Let F/K be a field extension. A subset $S \subseteq F$ is said to be ***algebraically dependent*** if for some integer $n \geq 1$ there is a nonzero polynomial $f(x_1, \ldots, x_n) \in K[x_1, \ldots, x_n]$ with $f(s_1, \ldots, s_n) = 0$ for some distinct $s_1, \ldots, s_n \in S$. The set S from above is said to be ***algebraically independent*** if S is not algebraically dependent.

Theorem. Let F/K be a field extension. If $\{s_1, \ldots, s_n\} \subseteq F$ is algebraically independent over K, then $K(x_1, \ldots, x_n) \simeq K(s_1, \ldots, s_n)$.

Proof. First, define a map

$$\theta : K[x_1, \ldots, x_n] \to K[s_1, \ldots, s_n] \quad \text{by} \quad f(x_1, \ldots, x_n) \mapsto f(s_1, \ldots, s_n)$$

Then θ is clearly a well-defined surjective ring homomorphism. Moreover, suppose that $f(x_1, \ldots, x_n) \in \ker \theta$. Then

$$0 = \theta(f(x_1, \ldots, x_n)) = f(s_1, \ldots, s_n)$$

But since $\{s_1, \ldots, s_n\}$ is algebraically independent over K, it follows by the above equality that $f(x_1, \ldots, x_n) = 0$ and hence $\ker \theta$ is trivial which proves that θ is an injection. By the previous results, we see that θ is a ring isomorphism. Finally, by the uniqueness of fields of fractions θ may be extended to an isomorphism of fields $K(x_1, \ldots, x_n) \to K(s_1, \ldots, s_n)$ so that $K(x_1, \ldots, x_n) \simeq K(s_1, \ldots, s_n)$. $\square$

Definition. Let F/K be a field extension. Then a ***transcendence basis*** of F over K is a algebraically independent subset S of F over K which is maximal among all such.

Theorem. Let F/K be a field extension. Then there exists a transcendence basis for F over K.

Proof. First, define

$$\mathcal{S} = \{S \subseteq F : S \text{ is algebraically independent over } K\}$$

and note that $\emptyset \subseteq F$ is clearly algebraically independent over K so that $\emptyset \in \mathcal{S}$ and hence $\mathcal{S} \neq \emptyset$. Now, partially order $\mathcal{S}$ by inclusion of sets and let $\mathcal{C}$ be a nonempty chain in $\mathcal{S}$ and define

$$T = \bigcup_{S \in \mathcal{C}} S$$

We claim that $T \in \mathcal{S}$.

Indeed, first note that since each $S \in \mathcal{S}$ is such that $S \subseteq F$ we have that $T \subseteq F$. Now, for the sake of contradiction suppose that T were not algebraically independent. Then there is an integer $n \geq 1$ and a nonzero polynomial $f(x_1, \ldots, x_n) \in K[x_1, \ldots, x_n]$ such that $f(t_1, \ldots, t_n) = 0$ for some distinct elements $t_1, \ldots, t_n \in T$. But since $\mathcal{C}$ is a chain, it follows that there is some $S \in \mathcal{C}$ such that $\{t_1, \ldots, t_n\} \subseteq S$. However, since $f(t_1, \ldots, t_n) = 0$ it now follows that S is algebraically dependent which is a contradiction

as $S \in \mathcal{C}$. We conclude that $T \in \mathcal{S}$ so that T is clearly an upper bound for $\mathcal{C}$ in $\mathcal{S}$. By Zorn's Lemma, then, we conclude that there is a maximal element $S \in \mathcal{S}$.

Finally, note that by the definition of membership in $\mathcal{S}$ and as S is a maximal element of $\mathcal{S}$ we have that $S \subseteq F$ is an algebraically independent subset of F over K which is maximal among all algebraically independent subsets of F over K. By definition, then, we conclude that S is a transcendence basis for F over K. This completes the proof. $\square$

Theorem. Let F/K be a field extension and suppose that $S \subseteq F$ is algebraically independent over K and that $t \in F - S$. Then $S \cup \{t\} \subseteq F$ is algebraically independent over K if and only if the extension $K(S,t)/K(S)$ is transcendental.

Proof. For the first direction, suppose that $S \cup \{t\}$ is algebraically independent over K. For the sake of contradiction, suppose that the extension $K(S,t)/K(S)$ were not transcendental. In particular, this assumption implies that $t \in K(S,t)$ is algebraic over $K(S)$. Therefore, there is some nonzero polynomial $p(x)$ of the form

$$p(x) = x^n + \frac{q_{n-1}(s_1, \ldots, s_m)}{d_{n-1}(s_1, \ldots, s_m)} x^{n-1} + \cdots + \frac{q_0(s_1, \ldots, s_m)}{d_0(s_1, \ldots, s_m)} \in K(S)[x]$$

where

$$q_{n-1}(x_1, \ldots, x_m), \ldots, q_0(x_1, \ldots, x_m) \in K[x_1, \ldots, x_m]$$

and

$$0 \neq d_{n-1}(x_1, \ldots, x_m), \ldots, d_0(x_1, \ldots, x_m) \in K[x_1, \ldots, x_m]$$

and $s_1, \ldots, s_n \in S$ such that $p(t) = 0$. Clearing denominators in the above equality, then, we obtain a nonzero polynomial

$$r(x_1, \ldots, x_m, x) \in K[x_1, \ldots, x_m, x]$$

such that $r(s_1, \ldots, s_m, t) = 0$. However, this implies that $S \cup \{t\}$ is not algebraically independent over K which is a contradiction. We conclude that the extension $K(S,t)/K(S)$ is transcendental. This completes the proof of the first direction.

For the second direction, we will prove by contrapositive. Towards this end, suppose that $S \cup \{t\}$ is algebraically dependent over K. Then since S is algebraically independent over K, it follows that there is a nonzero polynomial $f(x_1, \ldots, x_m) \in K[x_1, \ldots, x_m]$ and elements $s_1, \ldots, s_{m-1} \in S$ such that $f(s_1, \ldots, s_{m-1}, t) = 0$. Now, if $f(x_1, \ldots, x_m)$ has degree in x_m equal to zero then it would follow that S is algebraically dependent over K which contradicts the fact that S is algebraically independent over K. Therefore, we see that $f(x_1, \ldots, x_m)$ has strictly positive degree in x_m.

Finally, notice that as $s_1, \ldots, s_{m-1} \in S$ and as $f(x_1, \ldots, x_m)$ has strictly positive degree in x_m we have $0 \neq f(s_1, \ldots, s_{m-1}, x_m) \in K(S)[x_m]$. Moreover, we have by the above that $f(s_1, \ldots, s_{m-1}, t) = 0$ so that t is algebraic over $K(S)$. In particular, this gives that $K(S,t)/K(S)$ is an algebraic field extension. This completes the proof of the second direction. $\square$

Topic 6: Some Problems From Field and Galois Theory

Example. Let K be a field. Then every element of $K(x)$ which is not in K is transcendental over K.

Proof. Suppose that $u \in K(x)$ is algebraic over K. If $u = 0$, then clearly $u \in K$. Therefore, assume that $u \neq 0$ so that we may write $u = f(x)/g(x)$ for some nonzero, relatively prime polynomials $f(x), g(x) \in K[x]$. Now, since $u \in K(x)$ is algebraic over K there is some irreducible polynomial $p(y) \in K[y]$ such that $p(u) = 0$. For definiteness, write

$$p(y) = \sum_{i=0}^{n} a_i y^i \quad \text{for some} \quad a_0, \ldots, a_n \in K \quad \text{with} \quad a_n \neq 0$$

Furthermore, since $p(y)$ is irreducible it follows that $a_0 \neq 0$. Next, since $p(u) = 0$ we see

$$0 = p(u) = \sum_{i=0}^{n} a_i \left(\frac{f(x)}{g(x)} \right)^i$$

so that by clearing denominators we obtain

$$a_0 g(x)^n + a_1 f(x) g(x)^{n-1} + \cdots + a_n f(x)^n = 0$$

Finally, notice that this equality implies that $f(x)$ divides $a_0 g(x)^n$ and that $g(x)$ divides $a_n f(x)^n$. But since $f(x)$ and $g(x)$ are relatively prime, these observations give that $f(x)$ divides a_0 and that $g(x)$ divides a_n. Thus, since a_0 and a_n are nonzero elements of K we obtain that $f(x), g(x) \in K$ so that $u = f(x)/g(x) \in K$. This completes the proof. $\square$

Example. Let F/K be a field extension and suppose that $u \in F$ is algebraic of odd degree over K. Then $u^2 \in F$ is algebraic of odd degree over K and $K(u) = K(u^2)$.

Proof. Note that we have the inclusion $K \subseteq K(u^2) \subseteq K(u)$ so that

$$[K(u) : K] = [K(u) : K(u^2)][K(u^2) : K]$$

Now, since $u \in F$ is algebraic of odd degree over K it follows by the above equality that $[K(u^2) : K] < \infty$ and that $[K(u^2) : K]$ must be odd or else $[K(u) : K]$ is even. In particular, this gives that $u^2 \in F$ is algebraic of odd degree over K.

Finally, consider the polynomial $f(x) = x^2 - u^2 \in K(u^2)[x]$. In particular, notice that $f(u) = u^2 - u^2 = 0$ which gives that

$$[K(u) : K(u^2)] = [K(u^2, u) : K(u^2)] \leq \deg(f(x)) = 2$$

so that $[K(u) : K(u^2)] \in \{1, 2\}$. However, if $[K(u) : K(u^2)] = 2$ then we have by the equality in the beginning of this proof that $[K(u) : K]$ is even which is a contradiction. We conclude that $[K(u) : K(u^2)] = 1$ so that $K(u) = K(u^2)$, completing the proof. $\square$

Example. Let F/K be a field extension. If $x^n - a \in K[x]$ is irreducible and $u \in F$ is a root of $x^n - a$ and m divides n, then the degree of u^m over K is n/m. What is the irreducible polynomial for u^m over K?

Proof. Since m divides m, we may define a polynomial $h(x) = x^{n/m} - a \in K[x]$. Now, notice that since u is a root of $x^n - a$ we have $u^n - a = 0$ so that $u^n = a$. This gives

$$h(u^m) = (u^m)^{n/m} - a = u^n - a = a - a = 0$$

so that $h(u^m) = 0$. Now, we claim that $h(x)$ is irreducible over K. Indeed, suppose for the sake of contradiction that $h(x) = h_1(x)h_2(x)$ for some nonconstant polynomials $h_1(x), h_2(x) \in K[x]$. Then we obtain

$$h_1(x^m)h_2(x^m) = h(x^m) = (x^m)^{n/m} = x^n - a$$

However, this implies that the polynomial $x^n - a \in K[x]$ is not irreducible which is a contradiction. We conclude that $h(x) \in K[x]$ is irreducible and since $h(u^m) = 0$ this implies that $h(x)$ is the irreducible polynomial for u^m over K and that

$$[K(u^m) : K] = \deg(h(x)) = \frac{n}{m}$$

This completes the proof. □

Example. If F/K is an algebraic field extension and D is an integral domain such that $K \subseteq D \subseteq F$, then D is a field.

Proof. Since D is an integral domain, it remains to prove that every nonzero element of D has an inverse in D. Towards this end, suppose that $0 \neq u \in D \subseteq F$. Then since F/K is an algebraic field extension, it follows that there is an irreducible polynomial $f(x) \in K[x]$ such that $f(u) = 0$. For definiteness, write

$$f(x) = \sum_{i=0}^{n} a_i x^i \quad \text{for some} \quad a_0, \ldots, a_n \in K$$

In particular, since $f(x)$ is irreducible it follows that $a_0 \neq 0$. Now, since $f(u) = 0$ we obtain that

$$0 = f(u) = a_0 + a_1 u + \cdots + a_n u^n$$

Next, let $c = -a_0 \in K$. Then since $a_0 \neq 0$, it follows that c is a nonzero element of the field K so that $c^{-1} \in K$. Thus, we see by the above equality that

$$c = -a_0 = a_1 u + \cdots a_n u^n = u(a_1 + \cdots + a_n a^{n-1})$$

so that by multiplying both sides of the above equality by c^{-1} we obtain

$$1 = u(a_1 + \cdots + a_n u^{n-1})c^{-1} = u(c^{-1}a_1 + \cdots + c^{-1}a_n u^{n-1})$$

Finally, as $c^{-1}, a_1, \ldots, a_n \in K \subseteq D$ and as $u \in D$ we see $c^{-1}a_1 + \cdots + c^{-1}a_n u^{n-1} \in D$. Moreover, by the above equality it follows that

$$u^{-1} = c^{-1}a_1 + \cdots + c^{-1}a_n u^{n-1} \in D$$

This completes the proof. □

Example. If $0 \leq d \in \mathbb{Q}$, then $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$ is a Galois extension.

Proof. Let $G = \mathrm{Gal}(\mathbb{Q}(\sqrt{d})/\mathbb{Q})$. If $\sqrt{d} \in \mathbb{Q}$, then we have $\mathbb{Q}(\sqrt{d}) = \mathbb{Q}$ so that G is trivial in this case and hence $\mathbb{Q}(\sqrt{d})^G = \mathbb{Q}$. Therefore, assume that $\sqrt{d} \notin \mathbb{Q}$. In this case, consider the polynomial $f(x) = x^2 - d \in \mathbb{Q}[x]$ and observe that since $\sqrt{d} \notin \mathbb{Q}$ we have that $f(x)$ is a polynomial of degree 2 in $\mathbb{Q}[x]$ with no roots in $\mathbb{Q}$ so that as $\mathbb{Q}$ is a field we have that $f(x)$ is irreducible over $\mathbb{Q}$. This gives that

$$[\mathbb{Q}(\sqrt{d}) : \mathbb{Q}] = \deg(f(x)) = 2$$

so that

$$|G| \leq [\mathbb{Q}(\sqrt{d}) : \mathbb{Q}] \leq 2$$

Now, since $f(x)$ is irreducible over $\mathbb{Q}$ and as $f(x)$ is clearly separable it follows that G acts transitively on the set of roots of $f(x)$. In particular, this implies that there is some $\sigma \in G$ such that $\sigma(\sqrt{d}) = -\sqrt{d}$.

Finally, we now have by the above inequality for $|G|$ and the previous result that $G = \{\tau, \sigma\}$ where $\tau : \mathbb{Q}(\sqrt{d}) \to \mathbb{Q}(\sqrt{d})$ is the identity map. Now, suppose $u \in \mathbb{Q}(\sqrt{d})^G$. Then since $\sqrt{d} \notin \mathbb{Q}$ but $d \in \mathbb{Q}$, it follows that we may write $u = p + q\sqrt{d}$ for some $p, q \in \mathbb{Q}$. Therefore, we see that since $u \in \mathbb{Q}(\sqrt{d})$ we have

$$p + q\sqrt{d} = u = \sigma(u) = \sigma(p + q\sqrt{d}) = p + q\sigma(\sqrt{d}) = p - q\sqrt{d}$$

and hence by the above equality we obtain that $q = -q$ so that $q = 0$ so that $u = p + q\sqrt{d} = p \in \mathbb{Q}$. By this result, then, we conclude that $\mathbb{Q}(\sqrt{d})^G = \mathbb{Q}$ so that $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$ is a Galois extension. This completes the proof. $\square$

Example. Let F/K be a field extension. If E is an intermediate field of the extension F/K such that E/K is Galois, F/E is Galois, and every $\sigma \in \mathrm{Gal}(E/K)$ is extendible to F, then F/K is Galois.

Proof. We have the tower of fields $K \subseteq E \subseteq F$. If $F = K$, then clearly F/K is Galois. Therefore, assume that $F \neq K$ so that $K \subsetneq F$. Let $u \in F - K$. In order to show that F/K is Galois, it suffices to show that there is some $\sigma \in \mathrm{Gal}(F/K)$ such that $\sigma(u) \neq u$.

Indeed, first suppose that $u \in E$ so that $u \in E - K$. Since E/K is Galois, there exists some $\tau \in \mathrm{Gal}(E/K)$ such that $\tau(u) \neq u$. By hypothesis, the map $\tau : E \to K$ can be extended to an element $\sigma \in \mathrm{Gal}(F/K)$. Therefore, since τ and σ agree on E and as $u \in E$ we have in particular that $\sigma(u) \neq u$. Secondly, suppose that $u \notin E$ so that $u \in F - E$. Since F/E is Galois, there is some element $\sigma \in \mathrm{Gal}(F/E) \leq \mathrm{Gal}(F/K)$ such that $\sigma(u) \neq u$. This completes the proof. $\square$

Example. Let K be a field. If $f(x) \in K[x]$ is a polynomial of degree n and if F is a splitting field for $f(x)$ over K, then $[F : K]$ divides $n!$.

Proof. Assume this is false. Among all counterexamples, choose one where $\deg(f(x)) = n$ is as small as possible. If $n = 0$, then $[F : K] = 1$ which divides $0! = 1$. If $n = 1$, then $[F : K] = 1$ which divides $1! = 1$. Therefore, we must have $\deg(f(x)) = n \geq 2$.

First, suppose that $f(x)$ is irreducible over K and let $u \in F$ be a root of $f(x)$. Then since $f(x) \in K[x]$ is irreducible and as $f(u) = 0$, we obtain

$$[K(u) : K] = \deg(f(x)) = n$$

Now, since u is a root of $f(x)$ it follows that we may write $f(x) = (x - u)g(x)$ for some polynomial $g(x) \in K[x]$ with $\deg(g(x)) = n - 1 < n$. Moreover, since F is a splitting field for $f(x)$ over K it follows that F is a splitting field for $g(x)$ over $K(u)$. By our choice, then, we have that $[F : K(u)]$ divides $(n-1)!$. Thus, we see by the above that

$$[F : K] = [F : K(u)][K(u) : K] = [F : K(u)] \cdot n$$

and since $[F : K(u)]$ divides $(n-1)!$ it now follows that $[F : K]$ divides $n \cdot (n-1)! = n!$. However, this is a contradiction to our choice.

Now, by the above we must have that $f(x)$ is not irreducible over K so that we may write $f(x) = g(x)h(x)$ for some polynomials $g(x), h(x) \in K[x]$ with

$$1 \leq \deg(g(x)), \deg(h(x)) \leq n - 1 < n$$

Let $m = \deg(g(x))$ and $k = \deg(h(x))$ so that

$$n = \deg(f(x)) = \deg(g(x)h(x)) = \deg(g(x)) + \deg(h(x)) = m + k$$

Next, let E be a splitting field for $g(x)$ over K. Then since $f(x) = g(x)h(x)$ and as F is a splitting field for $f(x)$ over K, it now follows that F is a splitting field for $h(x)$ over E. By our choice, then, we have that $[E : K]$ divides $m!$ and that $[F : E]$ divides $k!$. Finally, recall that $n = m + k$ so that $k = n - m$ and hence

$$\frac{n!}{m!k!} = \frac{n!}{m!(n-m)!} = \binom{n}{m} \in \mathbb{Z}$$

and hence $m!k!$ divides $n!$. But notice that

$$[F : K] = [F : E][E : K]$$

and hence $[F : K]$ divides $m!$ and $k!$ so that $[F : K]$ divides $m!k!$ which divides $n!$ so that $[F : K]$ divides $n!$. This final contradiction completes the proof. □

Example. Let K be a finite field. Then K is not algebraically closed.

Proof. Since K is finite, we may write $K = \{a_1, \ldots, a_n\}$. Now, define

$$p(x) = 1 + \prod_{i=1}^{n} (x - a_i) \in K[x]$$

In particular, notice that $p(x)$ is a nonconstant polynomial in $K[x]$. However, notice that by the definition of $p(x)$ that

$$p(a_i) = 1 + 0 = 1 \neq 0 \quad \text{for each} \quad i \in \{1, \ldots, n\}$$

In other words, we have exhibited a nonconstant polynomial $p(x) \in K[x]$ such that $p(x)$ has no roots in K. Thus, we conclude that K is not algebraically closed. This completes the proof. □

Example. Let F/K be a field extension and suppose that E is an intermediate field of the extension F/K.

(a): If $u \in F$ is separable over K, then u is separable over E.

(b): If F is separable over K, then F is separable over E and E is separable over K.

Proof. (a): Let $f(x) \in K[x]$ denote the minimum polynomial for u over K and let $g(x) \in E[x]$ denote the minimum polynomial for u over E. In particular, we see $f(x) \in K[x] \subseteq E[x]$ is a polynomial in $E[x]$ that has u as a root so that $g(x)$ divides $f(x)$. But since $u \in F$ is separable over K, it follows that $f(x)$ is a separable polynomial and since $g(x)$ divides $f(x)$ this gives that $g(x)$ is also a separable polynomial. Thus, we conclude that u is separable over E. $\square$

Proof. (b): Let $u \in F$. Since F is separable over K, we know that $u \in F$ is separable over K so that by Part (a) we see that u is separable over E. As $u \in F$ was arbitrary, this shows that F is separable over E. Finally, let $u \in E \subseteq F$. Since F is separable over K, it follows that u is separable over K. As $u \in E$ was arbitrary, this shows that E is separable over K. $\square$

Example. Let K be a field and let F be a splitting field for $f(x) \in K[x]$ over K. Suppose that $f(x)$ splits in F as $f(x) = (x - u_1)^{n_1} \cdots (x - u_k)^{n_k}$, where $u_1, \ldots, u_k$ are distinct and $n_1, \ldots, n_k$ are positive integers. Let $v_0, \ldots, v_k$ be the coefficients of the polynomial $g(x) = (x - u_1) \cdots (x - u_k)$ and let $E = K(v_0, \ldots, v_k)$. Show that $\mathrm{Gal}(F/E) = \mathrm{Gal}(F/K)$.

Proof. First, note that $K \subseteq K(v_0, \ldots, v_k) = E$ so that $\mathrm{Gal}(F/E) \leq \mathrm{Gal}(F/K)$. On the other hand, let $\sigma \in \mathrm{Gal}(F/K)$. Since F is a splitting field for $f(x)$ over K, then, it follows that σ permutes the roots $u_1, \ldots, u_k$ of $f(x)$. Therefore, we obtain that

$$\sigma(g(x)) = \sigma\left(\prod_{i=1}^{k}(x - u_i)\right) = \prod_{i=1}^{k}(x - u_i) = g(x)$$

Thus, we see that σ fixes $g(x)$ and hence σ must also fix the coefficients $v_0, \ldots, v_k$ of $g(x)$. Finally, recall that as $\sigma \in \mathrm{Gal}(F/K)$ that σ fixes K and since σ also fixes $v_0, \ldots, v_k$ by the above result we see that σ fixes $K(v_0, \ldots, v_k) = E$. We may now conclude that $\sigma \in \mathrm{Gal}(F/E)$ and hence $\mathrm{Gal}(F/K) \leq \mathrm{Gal}(F/K)$. We conclude that $\mathrm{Gal}(F/E) = \mathrm{Gal}(F/K)$, completing the proof. $\square$

Example. Let $f(x) \in \mathbb{R}[x]$ be an irreducible polynomial of degree 3 and let D be the discriminant of $f(x)$. Then $D > 0$ if and only if f has three real roots.

Proof. For the first direction, assume that $D > 0$ but that $f(x)$ did not have three real roots. Then it follows that $f(x)$ has two roots of the form $u_1 = a + bi$ and $u_2 = a - bi$

for some $a, b \in \mathbb{R}$ with $b \neq 0$. Now, we have

$$\begin{aligned}\Delta &= \prod_{1 \leq i < j \leq 3} (u_i - u_j) \\ &= (u_1 - u_2)(u_1 - u_3)(u_2 - u_3) \\ &= [(u_1 - a) - bi][(u_1 - a) + bi](2bi) \\ &= 2bi[(u_1 - a)^2 + b^2]\end{aligned}$$

so that

$$D = \Delta^2 = (2bi)^2[(u_1 - a)^2 + b^2] = -4b^2[(u_1 - a)^2 + b^2]^2$$

But since $b \neq 0$, the above equality implies that $D < 0$ which is a contradiction. We conclude that $f(x)$ has three real roots. This completes the proof of the first direction.

For the second direction, suppose that $f(x)$ has three real roots $u_1, u_2, u_3 \in \mathbb{R}$. By the above computation, we have

$$\Delta = (u_1 - u_2)(u_1 - u_3)(u_2 - u_3) \in \mathbb{R}$$

Moreover, since $\mathrm{char}(\mathbb{R}) = 0$ and as $f(x)$ is irreducible over $\mathbb{R}$ it follows that $f(x)$ is separable and hence $\Delta \neq 0$. Therefore, we obtain since $\Delta \in \mathbb{R}$ that $D = \Delta^2 > 0$. This completes the proof of the second direction. □

Example. Let K be a field and suppose that $f(x) \in K[x]$ is a monic, irreducible polynomial with $\deg(f(x)) \geq 2$ and that $f(x)$ is has a unique root in a splitting field over K. Then $\mathrm{char}(K) = p \neq 0$ and $f(x) = x^{p^n} - a$ for some integer $n \geq 1$ and some $a \in K$.

Proof. Let F be a splitting field for $f(x)$ over K and let $u \in F$ be the unique root of $f(x)$ so that $F = K(u)$. Furthermore, since $f(x) \in K[x]$ is monic and irreducible and has u as a root it follows that $f(x)$ is the minimum polynomial for u over K. But since u is the unique root of $f(x)$, it follows that $u \in F$ is purely inseparable so that $F/K = K(u)/K$ is a purely inseparable extension.

Next, for the sake of contradiction suppose that $\mathrm{char}(K) = 0$. In particular, since $f(x) \in K[x]$ is irreducible this assumption implies that $f(x)$ is separable. However, since $\deg(f(x)) \geq 2$ and as $f(x)$ has a unique root in F this is a contradiction. We conclude that $\mathrm{char}(K) = p \neq 0$. Finally, recall that $f(x)$ is the minimum polynomial for $u \in F$ and that F/K is a purely inseparable extension. Thus, since $\mathrm{char}(K) = p \neq 0$ it now follows that $f(x) = x^{p^n} - a \in K[x]$. Moreover, since $\deg(f(x)) \geq 2$ we must have $n \geq 1$ and since $x^{p^n} - a \in K[x]$ we have $a \in K$. This completes the proof. □

Example. Let K be a field and suppose that $f(x) \in K[x]$ is irreducible of degree $m \geq 1$ and that $\mathrm{char}(K)$ does not divide m. Then $f(x)$ is separable.

Proof. First, write

$$f(x) = \sum_{i=0}^{m} a_i x^i \quad \text{for some} \quad a_0, \ldots, a_m \in K$$

This gives that

$$f'(x) = \sum_{i=1}^{m} a_i x^{i-1} = m a_m x^{m-1} + (m-1) a_{m-1} x^{m-2} + \cdots + a_1$$

Finally, consider the coefficient ma_m of x^{m-1} in the above equality for $f'(x)$. In particular, since $\mathrm{char}(K)$ does not divide m it follows that $ma_m \neq 0$ so that $f'(x) \neq 0$. Thus, since $f(x) \in K[x]$ is an irreducible polynomial with $f'(x) \neq 0$ it now follows that $f(x)$ is separable. This completes the proof. $\square$

Example. Let K be a finite field and suppose that F/K is a finite dimensional field extension. Then the maps $N : F \to K$ and $\mathrm{Tr} : F \to K$ are surjective.

Proof. Let $[F : K] = n < \infty$. Since K is a finite field, then, we have that F is also a finite field so that F/K is a cyclic extension. Thus, we have that $|\mathrm{Gal}(F/K)| = [F : K] = n$ and there is some $\sigma \in \mathrm{Gal}(F/K)$ such that $\mathrm{Gal}(F/K) = \{1_F, \sigma, \ldots, \sigma^{n-1}\}$.

We first show that N is surjective. Towards this end, let $|K| = q$ so that $\sigma : F \to F$ is the map defined by $\sigma(a) = a^q$ for each $a \in F$. Now, suppose that $u \in F$. Then

$$N(u) = \prod_{i=0}^{n-1} \sigma^i(u) = \prod_{i=0}^{n-1} u^q = u^{\sum_{i=0}^{n-1} q^i} = u^{\frac{q^n-1}{q-1}}$$

Now, notice that since $[F : K] = n$ and as $|K| = q$ we have that $|F| = |K|^n = q^n$ so that $|F^\times| = q^n - 1$. Furthermore, since the multiplicative group of units of a finite field is cyclic there is some generator $u_0 \in F^\times$ of $F^\times$. In particular, observe that $|u_0| = q^n - 1$.

Next, by the above computation we have

$$N(u_0) = u_0^{\frac{q^n-1}{q-1}}$$

Now, suppose that $[N(u_0)]^z = 1$ for some positive integer z. Then by the above equality, we have that

$$1 = [N(u_0]^z = \left(u_0^{\frac{q^n-1}{q-1}}\right)^z = u_0^{\frac{z(q^n-1)}{q-1}}$$

In particular, we now have that $|u_0| = q^n - 1$ divides $\frac{z(q^n-1)}{q-1}$ so that $q-1$ divides z which gives that $q - 1 \leq z$. On the other hand, notice that since $|u_0| = q^n - 1$ that

$$[N(u_0)]^{q-1} = \left(u_0^{\frac{q^n-1}{q-1}}\right)^{q-1} = u_0^{q^n-1} = 1$$

By combining the previous results, we obtain that $|N(u_0)| = q - 1$. But recall that since $|K| = q$ that $|K^\times| = q - 1$ and hence it now follows that $K^\times = \langle N(u_0) \rangle$.

To complete the proof, let $a \in K$. If $a \in K^\times$, then by the above we have that $a \in K^\times = \langle N(u_0) \rangle \subseteq \mathrm{Im}(N)$. If $a = 0$, then $a = 0 = N(0) \in \mathrm{Im}(N)$. By the previous results, then, we conclude that $\mathrm{Im}(N) = K$ and hence $N : F \to K$ is a surjection.

Finally, we show that Tr is surjective. Towards this end, recall that $\mathrm{Tr} : F \to K$ is a K-linear map so that in particular we have that $\mathrm{Tr}(F)$ is a sub K-vector space over

K and thus $\mathrm{Tr}(F) \in \{\{0\}, K\}$. However, if $\mathrm{Tr}(F) = \{0\}$ we would then have by the definition of the trace map that

$$1_F + \sigma + \cdots + \sigma^{n-1} = 0$$

which is a contradiction since the set $\{1_F, \sigma, \ldots, \sigma^{n-1}\}$ is linearly independent over K. Thus, we conclude that $\mathrm{Tr}(F) = K$ so that $\mathrm{Tr} : F \to K$ is a surjection. $\square$

Example. Let p be a prime number and suppose that F/K is a cyclic extension of degree p^n. Suppose that L is an intermediate field of the extension F/K such that $F = L(u)$ for some $u \in F$ and that L/K is an extension of degree p^{n-1}. Then $F = K(u)$.

Proof. Since F/K is a cyclic extension of degree p^n, it follows that $\mathrm{Gal}(F/K)$ is a cyclic group of order p^n. Now, since p is a prime number it follows that the complete list of divisors of p^n is given by $1, p, \ldots, p^{n-1}, p^n$. Thus, since $\mathrm{Gal}(F/K)$ is a cyclic group of order p^n and as p is a prime number it follows that the complete list of subgroups of $\mathrm{Gal}(F/K)$ may be written

$$\mathrm{Gal}(F/F) \leq \mathrm{Gal}(F/L_{n-1}) \leq \cdots \leq \mathrm{Gal}(F/L_1) \leq \mathrm{Gal}(F/K)$$

with

$$|\mathrm{Gal}(F/F)| = 1 \quad |\mathrm{Gal}(F/L_{n-1})| = p \quad \cdots \quad |\mathrm{Gal}(F/L_1)| = p^{n-1} \quad |\mathrm{Gal}(F/K)| = p^n$$

and $L_1, \ldots, L_{n-1}$ are intermediate fields of the extension F/K with

$$K \subseteq L_1 \subseteq \cdots \subseteq L_{n-1} \subseteq F$$

Now, since $[F : K] = p^n$ and as $[L : K] = p^{n-1}$ we obtain

$$p^n = [F : K] = [F : L][L : K] = [F : L] \cdot p^{n-1}$$

so that $[F : L] = p$. Therefore, we see that $|\mathrm{Gal}(F/L)| = [F : L] = p$ so that $\mathrm{Gal}(F/L)$ is a subgroup of $\mathrm{Gal}(F/K)$ of order p. However, recall that a cyclic group has a *unique* subgroup for each positive divisor of its order. In particular, we have by this observation since $\mathrm{Gal}(F/L_{n-1})$ and $\mathrm{Gal}(F/L)$ are both subgroups of order p of the cyclic group $\mathrm{Gal}(F/K)$ that $\mathrm{Gal}(F/L_{n-1}) = \mathrm{Gal}(F/L)$ which gives that $L = L_{n-1}$ by the Fundamental Theorem of Galois Theory.

Finally, for the sake of contradiction suppose that $F \neq K(u)$. By the Fundamental Theorem of Galois Theory, we know that $K, L_1, \ldots, L_{n-1}, F$ is a complete list of the intermediate fields of the extension F/K. In particular, then, since $K(u) \neq F$ it now follows that $K(u) \in \{K, L_1, \ldots, L_{n-1}\}$. In any case, we obtain by the above tower of fields that $u \in L_{n-1}$ and hence by the above we obtain $F = L(u) = L_{n-1}(u) = L_{n-1}$. However, this gives by the above that

$$\mathrm{Gal}(F/L_{n-1}) = \mathrm{Gal}(F/F) \quad \text{so that} \quad p = |\mathrm{Gal}(F/L_{n-1})| = |\mathrm{Gal}(F/F)| = 1$$

which is a contradiction since p is a prime number. We conclude that $F = K(u)$. This completes the proof. $\square$

Example. Let K be a field with $\mathrm{char}(K) \neq 2$ and let n be an odd positive integer. Suppose that K contains a primitive nth root of unity. Then K also contains a primitive $2n$th root of unity.

Proof. Let $\zeta \in K$ be a primitive nth root of unity so that $\langle \zeta \rangle = \{1, \zeta, \ldots, \zeta^{n-1}\}$. Now, consider the element $-\zeta$. Since $\zeta \in K$ and as K is a field, we have that $-\zeta \in K$. Moreover, since ζ is a primitive nth root of unity we have that $\zeta^n = 1$ and hence

$$(-\zeta)^{2n} = [(-\zeta)^2]^n = \zeta^n = 1$$

so that $-\zeta$ is a $2n$th root of unity. Thus, it remains to prove that $-\zeta$ generates a subgroup of K of order $2n$. Indeed, since n is odd we have that $n-1$ is even and hence

$$\langle -\zeta \rangle = \{-\zeta, \zeta^2, -\zeta^3, \ldots, \zeta^{n-1}, -1, \zeta, -\zeta^2, \zeta^3, \ldots, -\zeta^{n-1}, 1\}$$

Finally, observe that since $\mathrm{char}(K) \neq 2$ that in particular we have

$$1 \neq -1, \zeta \neq -\zeta, \zeta^2 \neq -\zeta^2, \ldots, \zeta^{n-1} \neq -\zeta^{n-1}$$

so that by the above equality for $\langle -\zeta \rangle$ we obtain that $|\langle -\zeta \rangle| = n + n = 2n$. This completes the proof. $\square$

Example. Let n be an integer with $n \geq 3$ and suppose that ζ is a primitive nth root of unity over $\mathbb{Q}$. Then $[\mathbb{Q}(\zeta + \zeta^{-1}) : \mathbb{Q}] = \phi(n)/2$.

Proof. Since ζ is a primitive nth root of unity over $\mathbb{Q}$, we have $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \phi(n)$. Now, observe that we have the tower of fields $\mathbb{Q} \subseteq \mathbb{Q}(\zeta + \zeta^{-1}) \subseteq \mathbb{Q}(\zeta)$ and hence we now have

$$\phi(n) = [\mathbb{Q}(\zeta) : \mathbb{Q}] = [\mathbb{Q}(\zeta) : \mathbb{Q}(\zeta + \zeta^{-1})][\mathbb{Q}(\zeta + \zeta^{-1}) : \mathbb{Q}]$$

so that

$$[\mathbb{Q}(\zeta + \zeta^{-1}) : \mathbb{Q}] = \frac{\phi(n)}{[\mathbb{Q}(\zeta) : \mathbb{Q}(\zeta + \zeta^{-1})]}$$

Therefore, it remains to show that $[\mathbb{Q}(\zeta) : \mathbb{Q}(\zeta + \zeta^{-1})] = 2$.

Towards this end, first note that as $\mathbb{Q}(\zeta) = \mathbb{Q}(\zeta, \zeta + \zeta^{-1})$ that $[\mathbb{Q}(\zeta) : \mathbb{Q}(\zeta + \zeta^{-1})]$ is simply the degree of the minimum polynomial for ζ over $\mathbb{Q}(\zeta + \zeta^{-1})$. Now, since $n \geq 3$ and as ζ is a primitive nth root of unity it follows that $\zeta \notin \mathbb{Q}(\zeta + \zeta^{-1})$ and hence we see that $[\mathbb{Q}(\zeta) : \mathbb{Q}(\zeta + \zeta^{-1})] \geq 2$. Finally, consider the polynomial $p(x) \in \mathbb{Q}(\zeta + \zeta^{-1})[x]$ that is given by

$$p(x) = (\zeta + \zeta^{-1})x^2 - (\zeta + \zeta^{-1})^2 x + (\zeta + \zeta^{-1})$$

and observe that

$$\begin{aligned} p(\zeta) &= (\zeta + \zeta^{-1})\zeta^2 - (\zeta + \zeta^{-1})^2 \zeta + (\zeta + \zeta^{-1}) \\ &= (\zeta^3 + \zeta) - (\zeta^3 + 2\zeta + \zeta^{-1}) + (\zeta + \zeta^{-1}) \\ &= 0 \end{aligned}$$

In particular, we see that ζ is a root of the degree 2 polynomial $p(x) \in \mathbb{Q}(\zeta + \zeta^{-1})[x]$. It now follows that

$$[\mathbb{Q}(\zeta) : \mathbb{Q}(\zeta + \zeta^{-1})] \leq \deg(p(x)) = 2$$

and recalling $[\mathbb{Q}(\zeta) : \mathbb{Q}(\zeta + \zeta^{-1})] \geq 2$ by the above, we see $[\mathbb{Q}(\zeta) : \mathbb{Q}(\zeta + \zeta^{-1})] = 2$. $\square$

Topic 8: Free Groups; Generators and Relations

Definition. A ***category*** is a class $\mathcal{C}$ of objects $A, B, C, \ldots$ together with

(1): A class of disjoint sets, denoted $\mathrm{Hom}(A, B)$ for a given pair of objects A and B of $\mathcal{C}$. The elements of $\mathrm{Hom}(A, B)$ are called ***morphisms*** from A to B for each pair of objects A and B of $\mathcal{C}$;

(2): For each triple of objects A, B, C of $\mathcal{C}$, we have a function

$$\mathrm{Hom}(B, C) \times \mathrm{Hom}(A, B) \to \mathrm{Hom}(A, C) \quad \text{by} \quad (f, g) \mapsto f \circ g;$$

(3): For each object A of $\mathcal{C}$, we have the identity map $1_A \in \mathrm{Hom}(A, A)$;

all subject to

(a): (Associativity): For objects A, B, C, D of $\mathcal{C}$ and morphisms $f \in \mathrm{Hom}(A, B), g \in \mathrm{Hom}(B, C)$, and $h \in \mathrm{Hom}(C, D)$ we have $h \circ (g \circ f) = (h \circ g) \circ f$;

(b): (Identity): For objects A, B of $\mathcal{C}$ and a morphism $f \in \mathrm{Hom}(A, B)$ we have $1_B \circ f = f = f \circ 1_A$.

Definition. Let $\mathcal{C}$ be a category and let A, B be objects of $\mathcal{C}$ and $f \in \mathrm{Hom}(A, B)$ be a morphism of $\mathcal{C}$ from A to B. Then f is an ***equivalence*** if there is some $g \in \mathrm{Hom}(B, A)$ with $g \circ f = 1_A$ and $f \circ g = 1_B$.

Definition. Let $\mathcal{C}$ be a category. Then the ***opposite category*** of $\mathcal{C}$, denoted $\mathcal{C}^{\mathrm{op}}$, is the category whose objects are those of $\mathcal{C}$ and $\mathrm{Hom}_{\mathcal{C}^{\mathrm{op}}}(A, B) = \mathrm{Hom}_{\mathcal{C}}(B, A)$ for each pair of objects A, B of $\mathcal{C}$.

Definition. Let $\mathcal{C}$ be a category and let $(A_i)_{i \in I}$ be a family of objects of $\mathcal{C}$. A ***product*** for the family $(A_i)_{i \in I}$ is an object P of $\mathcal{C}$ together with a family of morphisms of $\mathcal{C}$ $(\pi_i : P \to A_i)_{i \in I}$ such that given any object B of $\mathcal{C}$ and any family of morphisms of $\mathcal{C}$ $(\phi_i : B \to A_i)_{i \in I}$ there exists a unique morphism $\phi : B \to P$ of $\mathcal{C}$ such that $\pi_i \circ \phi = \phi_i$ for each $i \in I$.

Theorem. Let $\mathcal{C}$ be a category and let $(A_i)_{i \in I}$ be a family of objects of $\mathcal{C}$. Let P_1 with $(\pi_{1,i} : P_1 \to A_i)_{i \in I}$ and P_2 with $(\pi_{2,i} : P_2 \to A_i)_{i \in I}$ be products for the family $(A_i)_{i \in I}$. Then P_1 and P_2 are equivalent in $\mathcal{C}$ and there is an equivalence $\theta : P_1 \to P_2$ of $\mathcal{C}$ such that $\pi_{2,i} \circ \theta = \pi_{1,i}$ for each $i \in I$.

Proof. Since P_1 with $(\pi_{1,i} : P_1 \to A_i)_{i \in I}$ is a product for the family $(A_i)_{i \in I}$, there exists a unique morphism $\phi : P_2 \to P_1$ of $\mathcal{C}$ such that $\pi_{1,i} \circ \phi = \pi_{2,i}$ for each $i \in I$. Since P_2 with $(\pi_{2,i} : P_2 \to A_i)_{i \in I}$ is a product for the family $(A_i)_{i \in I}$, there exists a unique morphism $\theta : P_1 \to P_2$ such that $\pi_{2,i} \circ \theta = \pi_{1,i}$ for each $i \in I$.

We claim that θ is an equivalence. Indeed, note that $\phi \circ \theta : P_1 \to P_1$ is a morphism of $\mathcal{C}$ and that

$$\pi_{1,i} \circ (\phi \circ \theta) = (\pi_{1,i} \circ \phi) \circ \theta = \pi_{2,i} \circ \theta = \pi_{1,i} = \pi_{1,i} \circ 1_{P_1} \quad \text{for each} \quad i \in I$$

But since P_1 is a product, the above equality gives us by uniqueness that $\phi \circ \theta = 1_{P_1}$. Similarly, note that $\theta \circ \phi : P_2 \to P_2$ is a morphism of $\mathcal{C}$ and that

$$\pi_{2,i} \circ (\theta \circ \phi) = (\pi_{2,i} \circ \theta) \circ \phi = \pi_{1,i} \circ \phi = \pi_{2,i} = \pi_{2,i} \circ 1_{P_2} \quad \text{for each} \quad i \in I$$

But since P_2 is a product, the above equality gives us by uniqueness that $\theta \circ \phi = 1_{P_2}$. Hence, it now follows that $\theta : P_1 \to P_2$ is an equivalence of $\mathcal{C}$ so that P_1 and P_2 are equivalent in $\mathcal{C}$. Moreover, recall that $\pi_{2,i} \circ \theta = \pi_{1,i}$ for each $i \in I$. This completes the proof. $\square$

Definition. Let $\mathcal{C}$ be a category and let $(A_i)_{i \in I}$ be a family of objects of $\mathcal{C}$. A ***coproduct*** for the family $(A_i)_{i \in I}$ is an object C of $\mathcal{C}$ together with a family of morphisms of $\mathcal{C}$ $(c_i : A_i \to C)_{i \in I}$ such that given any object D of $\mathcal{C}$ and any family of morphisms of $\mathcal{C}$ $(d_i : A_i \to D)_{i \in I}$ there exists a unique morphism $\theta : C \to D$ of $\mathcal{C}$ such that $\theta \circ c_i = d_i$ for each $i \in I$.

Theorem. Let $\mathcal{C}$ be a category and let $(A_i)_{i \in I}$ be a family of objects of $\mathcal{C}$. Let C_1 with $(c_{1,i} : A_i \to C_1)_{i \in I}$ and C_2 with $(c_{2,i} : A_i \to C_2)_{i \in I}$ be coproducts for the family $(A_i)_{i \in I}$. Then C_1 and C_2 are equivalent in $\mathcal{C}$ and there is an equivalence $\theta : C_1 \to C_2$ of $\mathcal{C}$ such that $\theta \circ c_{1,i} = c_{2,i}$ for each $i \in I$.

Proof. Since C_1 with $(c_{1,i} : A_i \to C_1)_{i \in I}$ is a coproduct for the family $(A_i)_{i \in I}$, there exists a unique morphism $\theta : C_1 \to C_2$ of $\mathcal{C}$ such that $\theta \circ c_{1,i} = c_{2,i}$ for each $i \in I$. Since C_2 with $(c_{2,i} : A_i \to C_2)_{i \in I}$ is a product for the family $(A_i)_{i \in I}$, there exists a unique morphism $\phi : C_2 \to C_1$ such that $\phi \circ c_{2,i} = c_{1,i}$ for each $i \in I$.

We claim that θ is an equivalence. Indeed, note that $\phi \circ \theta : C_1 \to C_1$ is a morphism of $\mathcal{C}$ and that

$$(\phi \circ \theta) \circ c_{1,i} = \phi \circ (\theta \circ c_{1,i}) = \phi \circ c_{2,i} = c_{1,i} = 1_{C_1} \circ c_{1,i} \quad \text{for each} \quad i \in I$$

But since C_1 is a coproduct, the above equality gives us by uniqueness that $\phi \circ \theta = 1_{C_1}$. Similarly, note that $\theta \circ \phi : C_2 \to C_2$ is a morphism of $\mathcal{C}$ and that

$$(\theta \circ \phi) \circ c_{2,i} = \theta \circ (\phi \circ c_{2,i}) = \theta \circ c_{1,i} = c_{2,i} = 1_{C_2} \circ c_{2,i} \quad \text{for each} \quad i \in I$$

But since C_2 is a coproduct, the above equality gives us by uniqueness that $\theta \circ \phi = 1_{C_2}$. Hence, it now follows that $\theta : C_1 \to C_2$ is an equivalence of $\mathcal{C}$ so that C_1 and C_2 are equivalent in $\mathcal{C}$. Moreover, recall that $\theta \circ c_{1,i} = c_{2,i}$ for each $i \in I$. This completes the proof. $\square$

Example. Let $(S_i)_{i \in I}$ be a family of sets and let

$$P = \left\{ f : I \to \bigcup_{i \in I} S_i : f(i) \in S_i \text{ for each } i \in I \right\}$$

together with the maps $(\pi_i : P \to S_i)_{i \in I}$ where $\pi_i(f) = f(i)$ for each $f \in P$ is a product for the family $(S_i)_{i \in I}$ in the category of sets whose objects are sets and whose morphisms are maps of sets.

Proof. Suppose that B is a set and that $(\phi_i : B \to S_i)_{i \in I}$ is a family of maps of sets. Define a map of sets

$$\phi : B \to P \quad \text{by} \quad \phi(b) : I \to \bigcup_{i \in I} S_i \quad \text{by} \quad \phi(b)(i) = \phi_i(b) \quad \text{for each} \quad b \in B, i \in I$$

It is immediate that ϕ is a well-defined map of sets. Now, notice that

$$(\pi_i \circ \phi)(b) = \pi_i(\phi(b)) = \phi(b)(i) = \phi_i(b) \quad \text{for each} \quad b \in B, i \in I$$

Therefore, it follows that $\pi_i \circ \phi = \phi_i$ for each $i \in I$. Next, suppose that $\theta : B \to P$ is a map of sets such that $\pi_i \circ \theta = \phi_i$ for each $i \in I$. Then we have

$$\theta(b)(i) = \pi_i(\theta(b)) = \phi_i(b) = \phi(b)(i) \quad \text{for each} \quad b \in B, i \in I$$

Hence, it now follows that $\theta(b) = \phi(b)$ for each $b \in B$ so that $\theta = \phi$. This result shows that ϕ is the unique map of sets such that $\pi_i \circ \phi = \phi_i$ for each $i \in I$. This completes the proof. □

Example. Let $\mathcal{G}$ be the category of groups whose objects are groups and whose morphisms are group homomorphisms. Then given two objects G_1 and G_2 of $\mathcal{G}$, the group $G_1 \times G_2$ together with the canonical projection homomorphisms $(\pi_i : G_1 \times G_2 \to G_i)_{i=1}^2$ is a product for $(G_i)_{i=1}^2$.

Proof. Suppose that H is a group and that $(\phi_i : H \to G_i)_{i=1}^2$ are group homomorphisms. Define a map

$$\phi : H \to G_1 \times G_2 \quad \text{by} \quad \phi(h) = (\phi_1(h), \phi_2(h)) \quad \text{for each} \quad h \in H$$

Clearly, we see that ϕ is a well-defined map. Furthermore, suppose that $h_1, h_2 \in H$. Then since ϕ_1 and ϕ_2 are group homomorphisms, we obtain

$$\begin{aligned}
\phi(h_1 h_2) &= (\phi_1(h_1 h_2), \phi_2(h_1 h_2)) \\
&= (\phi_1(h_1)\phi_1(h_2), \phi_2(h_1)\phi_2(h_2)) \\
&= (\phi_1(h_1), \phi_2(h_1))(\phi_1(h_2), \phi_2(h_2)) \\
&= \phi(h_1)\phi(h_2)
\end{aligned}$$

so that ϕ is a group homomorphism. Next, let $h \in H$. Then

$$(\pi_i \circ \phi)(h) = \pi_i(\phi(h)) = \pi_i(\phi_1(h), \phi_2(h)) = \phi_i(h) \quad \text{for each} \quad i \in \{1, 2\}$$

and hence $\pi_i \circ \phi = \phi_i$ for each $i \in \{1, 2\}$.

Finally, suppose that $\theta : H \to G_1 \times G_2$ is a group homomorphism such that $\pi_i \circ \theta = \phi_i$ for each $i \in \{1, 2\}$. Let $h \in H$. Then by the definition of π_1 and π_2, we see

$$\theta(h) = (\pi_1(\theta(h)), \pi_2(\theta(h)) = (\phi_1(h), \phi_2(h)) = \phi(h)$$

and hence $\theta = \phi$. This completes the proof. □

Example. Let $(S_i)_{i\in I}$ be a family of sets and let

$$C = \left\{ (s,i) \in \bigcup_{i\in I} S_i \times I : s \in S_i \right\}$$

together with the maps $(c_i : S_i \to C)_{i\in I}$ where $c_i(s) = (s,i)$ for each $s \in S_i$ is a coproduct for the family $(S_i)_{i\in I}$ in the category of sets whose objects are sets and whose morphisms are maps of sets.

Proof. Suppose that D is a set and that $(d_i : S_i \to D)_{i\in I}$ is a family of maps of sets. Define a map of sets

$$\theta : C \to D \quad \text{by} \quad \theta(s,i) = d_i(s) \quad \text{for each} \quad (s,i) \in C$$

It is immediate that θ is a well-defined map of sets. Now, notice that

$$(\theta \circ c_i)(s) = \theta(c_i(s)) = \theta(s,i) = d_i(s) \quad \text{for each} \quad i \in I, s \in S_i$$

Therefore, it follows that $\theta \circ c_i = d_i$ for each $i \in I$. Next, suppose that $\phi : C \to D$ is a map of sets such that $\phi \circ c_i = d_i$ for each $i \in I$. Then we have

$$\phi(s,i) = \phi(c_i(s)) = d_i(s) = \theta(s,i) \quad \text{for each} \quad (s,i) \in C$$

Hence, it now follows that $\phi = \theta$. This result shows that θ is the unique map of sets such that $c_i \circ \theta = d_i$ for each $i \in I$. This completes the proof. $\square$

Example. Let $\mathcal{A}$ be the category of abelian groups whose objects are abelian groups and whose morphisms are group homomorphisms. Then given two objects A_1 and A_2 of $\mathcal{A}$, the abelian group $A_1 \times A_2$ together with the canonical injection homomorphisms $(i_j : A_j \to A_1 \times A_2)_{j=1}^2$ is a coproduct for $(A_j)_{j=1}^2$.

Proof. Suppose that D is an abelian group and that $(d_j : A_j \to D)_{j=1}^2$ are group homomorphisms. Define a map

$$\theta : A_1 \times A_2 \to D \quad \text{by} \quad \theta(a_1,a_2) = d_1(a_1)d_2(a_2) \quad \text{for each} \quad (a_1,a_2) \in A_1 \times A_2$$

Clearly, we see that θ is a well-defined map. Furthermore, suppose that $(a,b),(c,d) \in A_1 \times A_2$. Then since d_1 and d_2 are group homomorphisms and as D is an abelian group, we obtain

$$\begin{aligned}
\theta((a,b)(c,d)) &= \theta(ac,bd) \\
&= d_1(ac)d_2(bd) \\
&= d_1(a)d_1(c)d_2(b)d_2(d) \\
&= [d_1(a)d_2(b)][d_1(c)d_2(d)] \\
&= \theta(a,b)\theta(c,d)
\end{aligned}$$

so that θ is a group homomorphism. Next, let $a \in A_1$. Then

$$(\theta \circ i_1)(a) = \theta(i_1(a)) = \theta(a,0) = d_1(a)d_2(0) = d_1(a)$$

so that $\theta \circ i_1 = d_1$. Similarly, let $b \in A_2$. Then

$$(\theta \circ i_2)(b) = \theta(i_2(b)) = \theta(0,b) = d_1(0)d_2(b) = d_2(b)$$

so that $\theta \circ i_2 = d_2$. Hence, we conclude that $\theta \circ i_j = d_j$ for each $j \in \{1, 2\}$.

Finally, suppose that $\phi : A_1 \times A_2 \to D$ is a group homomorphism such that $\phi \circ i_j = d_j$ for each $j \in \{1, 2\}$. Let $(a, b) \in A_1 \times A_2$. Then as ϕ is a group homomorphism, we see

$$\phi(a, b) = \phi((a, 0)(0, b)) = \phi(i_1(a)i_2(b)) = \phi(i_1(a))\phi(i_2(b)) = d_1(a)d_2(b) = \theta(a, b)$$

and hence $\phi = \theta$. This completes the proof. □

Example. Let $\mathcal{G}$ be the category of groups and consider the groups $G_1 = \mathbb{Z}/2\mathbb{Z}$ and $G_2 = \mathbb{Z}/3\mathbb{Z}$. Then the group $G_1 \times G_2$ together with the canonical injection homomorphisms $(i_j : G_j \to G_1 \times G_2)_{j=1}^2$ is not a coproduct for $(G_j)_{j=1}^2$.

Proof. For the sake of contradiction, suppose that the group $G_1 \times G_2$ together with $(i_j : G_j \to G_1 \times G_2)_{j=1}^2$ were a coproduct for $(G_j)_{j=1}^2$. Note that S_3 is a group and that

$$d_1 : G_1 \to S_3 \quad \text{by} \quad \overline{0} \mapsto (1) \quad \overline{1} \mapsto (1 \quad 2)$$

and

$$d_2 : G_2 \to S_3 \quad \text{by} \quad \overline{0} \mapsto (1) \quad \overline{1} \mapsto (1 \quad 2 \quad 3) \quad \overline{2} \mapsto (1 \quad 3 \quad 2)$$

are easily verified to be group homomorphisms. Since $G_1 \times G_2$ together with $(i_j : G_j \to G_1 \times G_2)_{j=1}^2$ is a coproduct for $(G_j)_{j=1}^2$, then, it follows that there exists a (unique) group homomorphism $\theta : G_1 \times G_2 \to S_3$ such that $\theta \circ i_j = d_j$ for each $j \in \{1, 2\}$. This gives

$$(1 \quad 2) = d_1(\overline{1}) = \theta(i_1(\overline{1})) = \theta(\overline{1}, \overline{0})$$

and

$$(1 \quad 2 \quad 3) = d_2(\overline{1}) = \theta(i_2(\overline{1})) = \theta(\overline{0}, \overline{1})$$

so that $\mathrm{Im}(\theta) \supseteq \{(1 \quad 2), (1 \quad 2 \quad 3)\}$. But since $S_3 = \langle (1 \quad 2), (1 \quad 2 \quad 3) \rangle$, it now follows that θ is a surjection. Moreover, notice that

$$|G_1 \times G_2| = 6 = |S_3|$$

and hence θ is a surjection between two finite sets of the same cardinality so that θ is also injective. Therefore, we conclude that θ is a group isomorphism which gives that $G_1 \times G_2 \simeq S_3$. However, since G_1 and G_2 are clearly abelian it follows that $G_1 \times G_2$ is abelian and since $G_1 \times G_2 \simeq S_3$ we obtain that S_3 is abelian which is a contradiction. This completes the proof. □

Definition. A ***concrete category*** is a category $\mathcal{C}$ together with a "function" σ that assigns to each object A of $\mathcal{C}$ a set $\sigma(A)$, called the ***underlying set*** of A, in such a way that

(1): Every morphism $A \to B$ of $\mathcal{C}$ is a function of the underlying sets $\sigma(A) \to \sigma(B)$;

(2): Given an object A of $\mathcal{C}$, the identity morphism $1_A \in \mathrm{Hom}(A, A)$ is the identity map on the set $\sigma(A)$;

(3): Composition of morphisms of $\mathcal{C}$ is composition of maps of sets.

Remark. If $\mathcal{C}$ is a concrete category and A is an object of $\mathcal{C}$, then we often denote A to be the underlying set of A.

Definition. Let $\mathcal{C}$ be a concrete category and let X be a set. Let F be an object of $\mathcal{C}$ and let $i : X \to F$ be a map of sets. We say that the pair (F, i) is ***free*** on X in $\mathcal{C}$ if given any object A of $\mathcal{C}$ and any map of sets $f : X \to A$, there exists a unique morphism $\overline{f} : F \to A$ of $\mathcal{C}$ such that $\overline{f} \circ i = f$ as maps of sets.

Theorem. Let $\mathcal{C}$ be a concrete category and let X be any set. Suppose that (F, i) and (F', i') are free on X in $\mathcal{C}$. Then there exists a unique equivalence $\phi : F \to F'$ of $\mathcal{C}$ such that $\phi \circ i = i'$.

Proof. Note that we have the following maps of sets

$$i : X \to F \quad \text{and} \quad i' : X \to F'$$

Now, since (F, i) is free on X in $\mathcal{C}$ there is a unique morphism $\phi : F \to F'$ of $\mathcal{C}$ such that $\phi \circ i = i'$. Similarly, since (F, i') is free on X in $\mathcal{C}$ there is a unique morphism $\psi : F' \to F$ of $\mathcal{C}$ such that $\psi \circ i' = i$. Next, notice that $\psi \circ \phi : F \to F$ is a morphism of $\mathcal{C}$ and that

$$(\psi \circ \phi) \circ i = \psi \circ (\phi \circ i) = \psi \circ i' = i = 1_F \circ i$$

Hence, since (F, i) is free on X in $\mathcal{C}$ the above equality gives us by uniqueness that $\psi \circ \phi = 1_F$. Similarly, notice that $\phi \circ \psi : F' \to F'$ is a morphism of $\mathcal{C}$ and that

$$(\phi \circ \psi) \circ i' = \phi \circ (\psi \circ i') = \phi \circ i = i' = 1_{F'} \circ i'$$

Hence, since (F', i') is free on X in $\mathcal{C}$ the above equality gives us by uniqueness that $\phi \circ \psi = 1'_F$. We conclude that $\phi : F \to F'$ is an equivalence of $\mathcal{C}$ such that $\phi \circ i = i'$. This completes the proof. $\square$

Theorem. Let $\mathcal{C}$ be a concrete category and let X and X' sets such that $|X| = |X'|$. Suppose that (F, i) is free on X in $\mathcal{C}$ and that (F', i') is free on X' in $\mathcal{C}$. Then F and F' are equivalent in $\mathcal{C}$.

Proof. Note that we have the following maps of sets

$$i : X \to F \quad \text{and} \quad i' : X' \to F'$$

Now, since $|X| = |X'|$ there is a bijection $f : X \to X'$ and a bijection $g : X' \to X$ such that $g \circ f = 1_X$ and $f \circ g = 1_{X'}$. Consider the maps

$$i' \circ f : X \to F' \quad \text{and} \quad i \circ g : X' \to F$$

Since (F, i) is free on X in $\mathcal{C}$, there is a a unique morphism $\phi : F \to F'$ of $\mathcal{C}$ such that $\phi \circ i = i' \circ f$. Similarly, since (F', i') is free on X' in $\mathcal{C}$ there is a unique morphism $\psi : F' \to F$ of $\mathcal{C}$ such that $\psi \circ i' = i \circ g$. Next, notice that $\psi \circ \phi : F \to F$ is a morphism of $\mathcal{C}$ and that

$$(\psi \circ \phi) \circ i = \psi \circ (\phi \circ i) = \psi \circ (i' \circ f) = (\psi \circ i') \circ f = (i \circ g) \circ f = i \circ (g \circ f) = i \circ 1_X = i = 1_F \circ i$$

Hence, since (F, i) is free on X in $\mathcal{C}$ the above equality gives us by uniqueness that $\psi \circ \phi = 1_F$. Similarly, notice that $\phi \circ \psi : F' \to F'$ is a morphism of $\mathcal{C}$ and that

$$(\phi \circ \psi) \circ i' = \phi \circ (\psi \circ i') = \phi \circ (i \circ g) = (\phi \circ i) \circ g = (i' \circ f) \circ g = i' \circ (f \circ g) = i' \circ 1_{X'} = i' = 1_{F'} \circ i'$$

Hence, since (F', i') is free on X' in $\mathcal{C}$ the above equality gives us by uniqueness that $\phi \circ \psi = 1_{F'}$. We conclude that $\phi : F \to F'$ is an equivalence of $\mathcal{C}$ so that F and F' are equivalent in $\mathcal{C}$, completing the proof. $\square$

Example. Let $\mathcal{G}$ be the category of all groups of order 1 and let X be a set. Then there are free objects of $\mathcal{G}$. However, if $\mathcal{G}$ is the category of finite groups then there are no free objects of $\mathcal{G}$.

Proof. Let G be a group of order 1 and define $i : X \to G$ by $i(x) = 1_G$ for each $x \in X$. Suppose that H is a group of order 1 that $f : X \to H$ is any map of sets. Clearly, we have $f(x) = 1_H$ for each $x \in X$. Now, define $\overline{f} : G \to H$ by $\overline{f}(1_G) = 1_H$. It is immediate that $\overline{f}$ is a well-defined group homomorphism. Moreover, suppose that $x \in X$. Then

$$(\overline{f} \circ i)(x) = \overline{f}(i(x)) = \overline{f}(1_G) = 1_H = f(x)$$

and hence $\overline{f} \circ i = f$. Finally, suppose that $\overline{g} : G \to H$ is a group homomorphism such that $\overline{g} \circ i = f$. Then since $\overline{g}$ is a group homomorphism, we have that necessarily $\overline{g}(1_G) = 1_H$ and hence $\overline{g} = \overline{f}$. This completes the proof. $\square$

Topic 8: Free Groups; Generators and Relations

Definition. Let X be a set.

(a): A ***word*** on X is a sequence of elements from the set $X \cup X^{-1} \cup \{1\}$, where

$$X^{-1} = \{x^{-1} : x \in X\}$$

and X, X^{-1}, and $\{1\}$ are disjoint sets such that almost all of the elements of the sequence are equal to 1. The sequence $(1, 1, 1, \dots)$ is called the ***empty word*** and is denoted 1. A ***reduced word*** on X is a word on X such that x and x^{-1} are never adjacent in the word for any $x \in X$ and any $x^{-1} \in X^{-1}$ and after the first 1 appears in the word all other elements in the word are equal to 1.

(b): Let w_1 and w_2 be two reduced words on X. Then the ***product*** of w_1 and w_2, denoted $w_1 w_2$, is obtained as follows. Suppose that

$$w_1 = a_1 a_2 \cdots a_n \quad \text{and} \quad w_2 = b_1 b_2 \cdots b_m$$

where $a_1, \dots, a_n, b_1, \dots, b_m \in X \cup X^{-1}$. Consider the word

$$a_1 a_2 \cdots a_n b_1 b_2 \cdots b_m$$

After canceling any occurrences of xx^{-1} and $x^{-1}x$ in the above word for $x \in X$ and $x^{-1} \in X^{-1}$, we obtain a reduced word which we denote as $w_1 w_2$ and call the product of w_1 and w_2.

Theorem. Let X be a set and let F denote the set of reduced words on X. Then F is a group with operation defined to be the product of reduced words. Furthermore, suppose that $i : X \to F$ is the "inclusion" map. Then (F, i) is free on X in the category of groups whose objects are groups and whose morphisms are group homomorphisms.

Proof. We prove the first statement in the above Theorem here. It is clear that the product of reduced words is a reduced words so that F is a nonempty set with an operation. Furthermore, we have that $1 \in F$ is the identity of F and that each element $w \in F$ has an inverse in F. Therefore, it remains to prove that the operation of product of reduced words is associative to complete the proof of the first statement in the Theorem.

Towards this end, for each $x \in X$ and each $\delta \in \{-1, 1\}$ define a map

$$|x^\delta| : F \to F \quad \text{by} \quad w \mapsto x^\delta w$$

Clearly, we have that $|x^\delta|$ is a well-defined map. Furthermore, we also have for each $x \in X$ and $\delta \in \{-1, 1\}$ that

$$|x^\delta| \circ |x^{-\delta}| = 1_F = |x^{-\delta}| \circ |x^\delta|$$

and hence $|x^\delta| : F \to F$ is a bijection so that $|x^\delta| \in S_F$.

Now, let F_0 be the subgroup of S_F generated by the set $\{|x|, |x^{-1}| : x \in X\}$ and define a map

$$\phi : F \to F_0 \quad \text{by} \quad x_1^{\epsilon_1} \cdots x_n^{\epsilon_n} \mapsto |x_1^{\epsilon_1}| \circ \cdots \circ |x_n^{\epsilon_n}|$$

Clearly, we see that ϕ is a well-defined map. Furthermore, we have $\phi(w_1w_2) = \phi(w_1) \circ \phi(w_2)$ for all $w_1, w_2 \in F$ so that ϕ is a homomorphism of sets with an operation. Moreover, observe that $(\phi(w))(1) = w$. Therefore, if $w_1, w_2 \in F$ and $\phi(w_1) = \phi(w_2)$ we obtain in particular that

$$w_1 = (\phi(w_1))(1) = (\phi(w_2))(1) = w_2$$

so that ϕ is an injection. Finally, since F_0 is a subgroup of the group S_F we have that the operation in F_0 is associative. Thus, as $\phi : F \to F_0$ is an injective homomorphism of sets with an operation by the above result we conclude that the operation in F is also associative. This completes the proof that F with operation defined to be product of reduced words is indeed a group.

We prove the second statement in the above Theorem here. Towards this end, let G be any group and suppose that $f : X \to G$ is any map of sets. Define a map

$$\overline{f} : F \to G \quad \text{by} \quad x_1^{\epsilon_1} \cdots x_n^{\epsilon_n} \mapsto f(x_1)^{\epsilon_1} \cdots f(x_n)^{\epsilon_n}$$

Clearly, we see that $\overline{f}$ is a well-defined group homomorphism. Now, let $x \in X$. Then

$$(\overline{f} \circ i)(x) = \overline{f}(i(x)) = \overline{f}(x) = f(x)$$

and hence $\overline{f} \circ i = f$.

Finally, suppose that $\overline{g} : F \to G$ is a group homomorphism such that $\overline{g} \circ i = f$ and let $x_1^{\epsilon_1} \cdots x_n^{\epsilon_n} \in F$. Then since $\overline{g}$ is a group homomorphism, we obtain

$$\begin{aligned}
\overline{g}(x_1^{\epsilon_1} \cdots x_n^{\epsilon_n}) &= \overline{g}(x_1^{\epsilon_1}) \cdots \overline{g}(x_n^{\epsilon_n}) \\
&= (\overline{g}(x_1))^{\epsilon_1} \cdots (\overline{g}(x_n))^{\epsilon_n} \\
&= (\overline{g}(i(x_1))^{\epsilon_1} \cdots (\overline{g}(i(x_n))^{\epsilon_n} \\
&= f(x_1)^{\epsilon_1} \cdots f(x_n)^{\epsilon_n} \\
&= \overline{f}(x_1^{\epsilon_1} \cdots x_n^{\epsilon_n})
\end{aligned}$$

and hence $\overline{g} = \overline{f}$. This completes the proof. □

Example. Let X be a set and let F be the free group on X. Then every nonidentity element of F has infinite order.

Proof. For a word $w \in F$, let $\text{len}(w)$ denote the length of the reduced word w. For the sake of contradiction, suppose that there is at least one nonidentity element in F of finite order. Then among all such nonidentity elements in F of finite order, we may choose one $w \in W$ with $\text{len}(w)$ as small as possible.

Suppose that $\text{len}(w) = 1$. Then $w = a$ for some $a \in X \cup X^{-1}$. Now, for any positive integer n we have

$$w^n = a^n = \underbrace{a \cdots a}_{n \text{ times}} \neq 1$$

which shows that w does not have finite order. Thus, we must have $\text{len}(w) \geq 2$. Suppose that $\text{len}(w) = 2$. Then $w = ab$ for some $a, b \in X \cup X^{-1}$ with $a \neq b^{-1}$ and $b \neq a^{-1}$. Now,

for any positive integer n we have

$$w^n = (ab)^n = \underbrace{(ab)\cdots(ab)}_{n \text{ times}} \neq 1$$

which shows that w does not have finite order. Thus, we must have $\text{len}(w) \geq 3$.

Now, since $\text{len}(w) \geq 3$ we can write $w = azb$ for some $a, b \in X \cup X^{-1}$ and some nonidentity element $z \in F$ with the first letter of z not equal to a^{-1} and the last letter of z not equal to b^{-1}. This gives that

$$\text{len}(w) = \text{len}(a) + \text{len}(z) + \text{len}(b) = 1 + \text{len}(z) + 1 = \text{len}(z) + 2$$

so that

$$\text{len}(z) = \text{len}(w) - 2 < \text{len}(w)$$

Thus, we have by our choice that z has infinite order so that $z^n \neq 1$ for any positive integer n.

Finally, recall that w is of finite order so that $w^m = 1$ for some positive integer m. If $b = a^{-1}$, this gives that

$$1 = w^m = (azb)^m = (aza^{-1})^m = \underbrace{(aza^{-1})\cdots(aza^{-1})}_{m \text{ times}} = az^m a^{-1}$$

and hence

$$z^m = a^{-1}a = 1$$

which is a contradiction since $z^n \neq 1$ for any positive integer n. Thus, we cannot have $b = a^{-1}$ and similarly we cannot have $a = b^{-1}$ and hence $b \neq a^{-1}$ and $a \neq b^{-1}$. However, this gives that

$$1 = w^m = (azb)^m = \underbrace{(azb)\cdots(azb)}_{m \text{ times}} \neq 1$$

which is obviously a contradiction. Hence, we conclude that every nonidentity element of F has infinite order. $\square$

Example. Let X be a set and let F be the free group on X. Let $Y \subseteq X$ and suppose that H is the smallest normal subgroup of F containing Y. Then F/H is a free group.

Proof. We will show that F/H is free on the set $X - Y$ in the category of groups whose objects are groups and whose morphisms are group homomorphisms. Towards this end, let $j : X - Y \to X$ and $i : X \to F$ denote the inclusion maps and let $\pi : F \to F/H$ denote the canonical projection map. Define $k = \pi \circ i \circ j : X - Y \to F/H$.

Now, suppose that G is a group and that $f : X - Y \to G$ is any map of sets. Next, define a map

$$g : X \to G \quad \text{by} \quad x \mapsto \begin{cases} f(x) & \text{if} \quad x \in X - Y \\ 1_G & \text{if} \quad x \in Y \end{cases}$$

In particular, we have by the definition of g that $g \circ j = f$. Moreover, since (F, i) is free on X it follows that there is a unique group homomorphism $\overline{g} : F \to G$ such that $\overline{g} \circ i = g$. Furthermore, let $y \in Y$. Then

$$\overline{g}(y) = \overline{g}(i(y)) = g(y) = 1_G$$

so that $Y \subseteq \ker \overline{g}$. But recall that H is the smallest normal subgroup of F containing Y. Therefore, since $\ker \phi$ is a normal subgroup of F containing Y by the previous result we see that $H \subseteq \ker \phi$. Hence, it now follows that there exists a unique group homomorphism $\overline{\overline{g}} : F/H \to G$ such that $\overline{\overline{g}} \circ \pi = \overline{g}$. Next, notice that

$$\overline{\overline{g}} \circ k = \overline{\overline{g}} \circ (\pi \circ i \circ j) = (\overline{\overline{g}} \circ \pi) \circ i \circ j = \overline{g} \circ i \circ j = (\overline{g} \circ i) \circ j = g \circ j = f$$

and hence $\overline{\overline{g}} \circ k = f$.

It remains to prove that $\overline{\overline{g}}$ is unique. Indeed, suppose that $\phi_1, \phi_2 : F/H \to G$ are group homomorphisms such that $\phi_1 \circ k = f = \phi_2 \circ k$. We claim that $\phi_1 \circ \pi \circ i = \phi_2 \circ \pi \circ i$. Towards this end, let $x \in X$. If $x \in X - Y$, then

$$(\phi_1 \circ \pi \circ i)(x) = \phi_1(\pi(i(x))) = \phi_1(\pi(i(j(x)))) = \phi_1(k(x)) = f(x)$$

and

$$(\phi_2 \circ \pi \circ i)(x) = \phi_2(\pi(i(x))) = \phi_2(\pi(i(j(x)))) = \phi_2(k(x)) = f(x)$$

If $x \in Y$, then

$$(\phi_1 \circ \pi \circ i)(x) = \phi_1(\pi(i(x))) = \phi_1(\pi(x)) = \phi_1(xH) = \phi_1(H) = 1_G$$

and

$$(\phi_2 \circ \pi \circ i)(x) = \phi_2(\pi(i(x))) = \phi_2(\pi(x)) = \phi_2(xH) = \phi_2(H) = 1_G$$

Thus, we conclude that $\phi_1 \circ \pi \circ i = \phi_2 \circ \pi \circ i$. Thus, as (F, i) is free on X the previous equality gives us by uniqueness that $\phi_1 \circ \pi = \phi_2 \circ \pi$. Finally, recall that π is a surjection and since $\phi_1 \circ \pi = \phi_2 \circ \pi$ this observation now gives that $\phi_1 = \phi_2$. We conclude that $\overline{\overline{g}}$ is unique and hence $(F/H, k)$ is free on $X - Y$ so that F/H is a free group. This completes the proof. □

Example. Solve the following.

(a): Define a *solvable group*.

(b): Prove that the homomorphic image of a solvable group is solvable.

(c): Prove that a free group is solvable if and only if it is the free group on at most one generator.

Proof. (a): Let G be a group. We say that G is ***solvable*** if there exists a sequence

$$\{1\} = H_0 \trianglelefteq H_1 \trianglelefteq \cdots \trianglelefteq H_r = G$$

where r is a positive integer and H_i/H_{i-1} is an abelian group for each $i \in \{1, \ldots, r\}$. □

Proof. (b): Let G be a solvable group and suppose that $\sigma : G \to H$ is a group homomorphism. We must show that $\sigma(G)$ is a solvable group. First, recall that the homomorphic

image of a group is a group so that $\sigma(G)$ is a group. Now, since G is solvable there is a sequence

$$\{1\} = H_0 \trianglelefteq H_1 \trianglelefteq \cdots \trianglelefteq H_r = G$$

where r is a positive integer and H_i/H_{i-1} is an abelian group for each $i \in \{1, \ldots, r\}$. Furthermore, we know that we may assume the above series is a composition series so that in addition we also have that H_i/H_{i-1} is a simple group for each $i \in \{1, \ldots, r\}$.

Now, fix any $m \in \{1, \ldots, r\}$. We will show that $\sigma(H_{m-1}) \trianglelefteq \sigma(H_m)$. Indeed, first note that since the homomorphic image of a group is a group and as $H_{m-1} \leq H_m$ we have $\sigma(H_{m-1}) \leq \sigma(H_m)$. Next, let $g \in \sigma(H_m)$ and $h \in \sigma(H_{m-1})$ so that there are elements $x \in H_m$ and $y \in H_{m-1}$ such that $\sigma(x) = g$ and $\sigma(y) = h$. Since $H_{m-1} \trianglelefteq H_m$ and we obtain that $xyx^{-1} \in H_{m-1}$ and hence

$$ghg^{-1} = \sigma(x)\sigma(y)(\sigma(x))^{-1} = \sigma(x)\sigma(y)\sigma(x^{-1}) = \sigma(xyx^{-1}) \in \sigma(H_{m-1})$$

We conclude that $\sigma(H_{m-1}) \trianglelefteq \sigma(H_m)$ and since $m \in \{1, \ldots, r\}$ was arbitrary, we now obtain the series

$$\{1\} = \sigma(H_0) \trianglelefteq \sigma(H_1) \trianglelefteq \cdots \trianglelefteq \sigma(H_r) = \sigma(G)$$

Thus, it remains to prove that $\sigma(H_i)/\sigma(H_{i-1})$ is abelian for each $i \in \{1, \ldots, r\}$.

Towards this end, again fix any $m \in \{1, \ldots, r\}$ and define a map

$$\phi : H_m/H_{m-1} \to \sigma(H_m)/\sigma(H_{m-1}) \quad \text{by} \quad xH_{m-1} \mapsto \sigma(x)\sigma(H_{m-1})$$

First, we show that ϕ is well-defined. Indeed, suppose that $xH_{m-1} = yH_{m-1}$ for some $x, y \in H_m$. This gives that $xy^{-1} \in H_{m-1}$ so that

$$\sigma(x)\sigma(y)^{-1} = \sigma(x)\sigma(y^{-1}) = \sigma(xy^{-1}) \in \sigma(H_{m-1})$$

so that $\sigma(x)\sigma(H_{m-1}) = \sigma(y)\sigma(H_{m-1})$ and hence

$$\phi(xH_{m-1}) = \sigma(x)\sigma(H_{m-1}) = \sigma(y)\sigma(H_{m-1}) = \phi(yH_{m-1})$$

so that ϕ is well-defined. Moreover, since σ is a group homomorphism it is easily verified that ϕ is also a group homomorphism.

Next, we show that ϕ is surjective. Towards this end, let $y \in \sigma(H_m)/\sigma(H_{m-1})$ so that $y = \sigma(x)\sigma(H_{m-1})$ for some $x \in H_m$. Then $xH_{m-1} \in H_m/H_{m-1}$ and

$$\phi(xH_{m-1}) = \sigma(x)\sigma(H_{m-1}) = y$$

so that ϕ is surjective. Secondly, notice that $\ker\phi$ is a normal subgroup of H_m/H_{m-1} so that since H_m/H_{m-1} is a simple group we have $\ker\phi \in \{\{1\}, H_m/H_{m-1}\}$. If $\ker\phi = H_m/H_{m-1}$, then by the First Isomorphism Theorem we obtain by the above that

$$\{1\} \simeq \sigma(H_m)/\sigma(H_{m-1})$$

so that $\sigma(H_m)/\sigma(H_{m-1})$ is abelian in this case. If $\ker\phi = \{1\}$, then by the First Isomorphism Theorem we obtain by the above that

$$H_m/H_{m-1} \simeq \sigma(H_m)/\sigma(H_{m-1})$$

so that $\sigma(H_m)/\sigma(H_{m-1})$ is abelian in this case as H_m/H_{m-1} is abelian. Thus, in all cases we see that $\sigma(H_m)/\sigma(H_{m-1})$ is abelian and as $m \in \{1, \ldots, r\}$ was arbitrary this

result shows that $\sigma(H_i)/\sigma(H_{i-1})$ is abelian for each $i \in \{1, \ldots, r\}$. By our observation made above, then, this completes the proof. $\square$

Proof. (c): For the first direction, suppose that F is a solvable free group. For the sake of contradiction, assume that F is a free group on a set X with $|X| \geq 2$. Now, since $|X| = 2$ there are distinct elements $x_1, x_2 \in F$. Let G be the free group on the set $\{x_1, x_2\}$ and let H be the free group on the (possibly empty) set $X - \{x_1, x_2\}$ so that $G \simeq F/H$. Now, notice that F/H is the homomorphic image of the canonical projection map $\pi : F \to F/H$ so that by Part (b) we have that F/H is a solvable group as F is a solvable group and hence as $G \simeq F/H$ we see that G is solvable.

Now, consider the group S_5 and recall that S_5 is not solvable. Let $\sigma_1 = (1 \quad 2) \in S_5$ and $\sigma_2 = (1 \quad 2 \quad 3 \quad 4 \quad 5) \in S_5$. Since 5 is a prime number, we see that $S_5 = \langle \sigma_1, \sigma_2 \rangle$. Next, define a map

$$f : \{x_1, x_2\} \to S_5 \quad \text{by} \quad x_1 \mapsto \sigma_1 \quad x_2 \mapsto \sigma_2$$

Recall that G is free on the set $\{x_1, x_2\}$ and so there is a unique group homomorphism

$$\overline{f} : G \to S_5 \quad \text{such that} \quad \overline{f}(x_1) = f(x_1) = \sigma_1 \quad \text{and} \quad \overline{f}(x_2) = f(x_2) = \sigma_2$$

Thus, we see that $\mathrm{Im}(\overline{f}) \supseteq \{\sigma_1, \sigma_2\}$ and as $S_5 = \langle \sigma_1, \sigma_2 \rangle$ we obtain that $\mathrm{Im}(G) = S_5$. In particular, then, we see that S_5 is a homomorphic image of the solvable group G so that by once again appealing to Part (b) we see that S_5 is solvable which is a contradiction. We conclude that F is a free group on at most one generator. This completes the proof of the first direction.

For the second direction, suppose that F is a free group on at most one generator. If F is a free group on zero generators, then F is trivial and hence solvable. If F is a free group on one generator, then $F \simeq \mathbb{Z}$ and since $\mathbb{Z}$ is a solvable group we conclude that F is solvable. Hence, we see in all cases that F is solvable. This completes the proof of the second direction. $\square$

Definition. Let X be a set and let R be a set of reduced words on X. Then the ***group*** G ***defined by generators*** X ***and relations*** R is the group F/N, where F is the free group on X and N is the smallest normal subgroup of F containing R.

Example. Show that the cyclic group of order 6 is the group defined by generators a, b and relations $a^2 = 1, b^3 = 1, a^{-1}b^{-1}ab = 1$.

Proof. Let $X = \{a, b\}$ and $R = \{a^2, b^3, a^{-1}b^{-1}ab\}$ and let F be the free group on X. Let N be the smallest normal subgroup of F such that $R \subseteq N$. By definition, we have that the group defined by generators X and relations R is F/N.

Now, define a map

$$f : X \to \mathbb{Z}/6\mathbb{Z} \quad \text{by} \quad a \mapsto \overline{3} \quad b \mapsto \overline{2}$$

Since F is free on X, there exists a unique group homomorphism $\overline{f} : F \to \mathbb{Z}/6\mathbb{Z}$ with

$$\overline{f}(a) = f(a) = \overline{3} \quad \text{and} \quad \overline{f}(b) = f(b) = \overline{2}$$

Furthermore, since $\overline{f}$ is a group homomorphism we see

$$\overline{f}(a^2) = \overline{f}(a) + \overline{f}(a) = \overline{3} + \overline{3} = \overline{6} = \overline{0}$$

and

$$\overline{f}(b^3) = \overline{f}(b) + \overline{f}(b) + \overline{f}(b) = \overline{2} + \overline{2} + \overline{2} = \overline{6} = \overline{0}$$

and

$$\begin{aligned}\overline{f}(a^{-1}b^{-1}ab) &= (\overline{f}(a))^{-1} + (\overline{f}(b))^{-1} + \overline{f}(a) + \overline{f}(b) \\ &= (\overline{3})^{-1} + (\overline{2})^{-1} + \overline{3} + \overline{2} \\ &= \overline{3} + \overline{4} + \overline{3} + \overline{2} \\ &= \overline{12} \\ &= \overline{0}\end{aligned}$$

By the above computations, then, we see that $R \subseteq \ker \overline{f}$. But recall that N is the smallest normal subgroup of F containing R. Therefore, since $\ker \overline{f}$ is a normal subgroup of F containing R by the previous result we conclude that $N \subseteq \ker \overline{f}$. In particular, this observation implies that there exists a unique group homomorphism $g : F/N \to \mathbb{Z}/6\mathbb{Z}$ with

$$g(aN) = \overline{f}(a) = \overline{3} \quad \text{and} \quad g(bN) = \overline{f}(b) = \overline{2}$$

Thus, we see that $\mathrm{Im}(g) \supseteq \{\overline{2}, \overline{3}\}$ and since $\mathbb{Z}/6\mathbb{Z} = \langle \overline{2}, \overline{3} \rangle$ we see that g is a surjection so that $|F/N| \geq |\mathbb{Z}/6\mathbb{Z}| = 6$.

Finally, we show that $|F/N| \leq 6$. Towards this end, we first show that any element $wN \in F/N$ has a representative of the form $a^i b^j$ for some $i \in \{0, 1\}$ and $j \in \{0, 1, 2\}$. Indeed, suppose that $wN \in F/N$. Then since $a^2, b^3 \in R \subseteq N$, we can choose a representative for wN of the form

$$a^{n_1} b^{n_2} a^{n_3} b^{n_4} \cdots a^{n_{r-1}} b^{n_r}$$

where $n_i \in \{0, 1\}$ for odd values of $i \in \{1, \ldots, r\}$ and $n_i \in \{0, 1, 2\}$ for even values of $i \in \{1, \ldots, r\}$. Now, among all such representatives for wN of the above form choose one where r is as small as possible. Suppose that $r \geq 3$. In this case, we have $n_1 = 1 = n_3$. This gives since $a^2, a^{-1}b^{-1}ab \in N$ that $ab^{n_2}aN = b^{n_2}N$. However, this contradicts the minimality of r. Therefore, we must have $r \leq 2$ and in particular we conclude that wN has a representative of the form $a^i b^j$ for some $i \in \{0, 1\}$ and $j \in \{0, 1, 2\}$. This gives that $|F/N| \leq 2 \cdot 3 = 6$. Combining the previous results, then, we conclude that

$$|F/N| = 6 = |\mathbb{Z}/6\mathbb{Z}|$$

so that g is a surjection between two finite sets of the same cardinality. This implies that g is a bijection and hence g is a group isomorphism and thus $F/N \simeq \mathbb{Z}/6\mathbb{Z}$. $\square$

Example. Show that S_3 is the group defined by the generators a, b and relations $a^2 = 1, b^3 = 1, abab = 1$.

Proof. Let $X = \{a, b\}$ and $R = \{a^2, b^3, abab\}$ and let F be the free group on X. Let N be the smallest normal subgroup of F such that $R \subseteq N$. By definition, we have that the group defined by generators X and relations R is F/N.

Now, define a map

$$f : X \to S_3 \quad \text{by} \quad a \mapsto (1 \quad 2) \quad b \mapsto (1 \quad 2 \quad 3)$$

Since F is free on X, there exists a unique group homomorphism $\overline{f} : F \to S_3$ with

$$\overline{f}(a) = f(a) = (1 \quad 2) \quad \text{and} \quad \overline{f}(b) = f(b) = (1 \quad 2 \quad 3)$$

Furthermore, since $\overline{f}$ is a group homomorphism we see

$$\overline{f}(a^2) = \overline{f}(a)\overline{f}(a) = (1 \quad 2)(1 \quad 2) = (1)$$

and

$$\overline{f}(b^3) = \overline{f}(b)\overline{f}(b)\overline{f}(b) = (1 \quad 2 \quad 3)(1 \quad 2 \quad 3)(1 \quad 2 \quad 3) = (1)$$

and

$$\begin{aligned} \overline{f}(abab) &= \overline{f}(a)\overline{f}(b)\overline{f}(a)\overline{f}(b) \\ &= (1 \quad 2)(1 \quad 2 \quad 3)(1 \quad 2)(1 \quad 2 \quad 3) \\ &= (1) \end{aligned}$$

By the above computations, then, we see that $R \subseteq \ker \overline{f}$. But recall that N is the smallest normal subgroup of F containing R. Therefore, since $\ker \overline{f}$ is a normal subgroup of F containing R by the previous result we conclude that $N \subseteq \ker \overline{f}$. In particular, this observation implies that there exists a unique group homomorphism $g : F/N \to S_3$ with

$$g(aN) = \overline{f}(a) = (1 \quad 2) \quad \text{and} \quad g(bN) = \overline{f}(b) = (1 \quad 2 \quad 3)$$

Thus, we see that $\mathrm{Im}(g) \supseteq \{(1 \quad 2), (1 \quad 2 \quad 3)\}$ and since $S_3 = \langle (1 \quad 2), (1 \quad 2 \quad 3) \rangle$ we see that g is a surjection so that $|F/N| \geq |S_3| = 3! = 6$.

Finally, we show that $|F/N| \leq 6$. Towards this end, we first show that any element $wN \in F/N$ has a representative of the form $a^i b^j$ for some $i \in \{0, 1\}$ and $j \in \{0, 1, 2\}$. Indeed, suppose that $wN \in F/N$. Then since $a^2, b^3 \in R \subseteq N$, we can choose a representative for wN of the form

$$a^{n_1} b^{n_2} a^{n_3} b^{n_4} \cdots a^{n_{r-1}} b^{n_r}$$

where $n_i \in \{0, 1\}$ for odd values of $i \in \{1, \ldots, r\}$ and $n_i \in \{0, 1, 2\}$ for even values of $i \in \{1, \ldots r\}$. Now, among all such representatives for wN of the above form choose one where r is as small as possible. Suppose that $r \geq 3$. In this case, we have $n_1 = 1 = n_3$. This gives since $a^2, abab \in N$ that $ab^{n_2}aN = b^{-n_2}N$. However, this contradicts the minimality of r. Therefore, we must have $r \leq 2$ and in particular we conclude that wN has a representative of the form $a^i b^j$ for some $i \in \{0, 1\}$ and $j \in \{0, 1, 2\}$. This gives that $|F/N| \leq 2 \cdot 3 = 6$. Combining the previous results, then, we conclude that

$$|F/N| = 6 = |S_3|$$

so that g is a surjection between two finite sets of the same cardinality. This implies that g is a bijection and hence g is a group isomorphism and thus $F/N \simeq S_3$. $\square$

Example. Show that Q_8 is the group defined by the generators a, b and relations $a^2 b^{-2} = 1, abab^{-1} = 1$.

Proof. Adopting all of the same notation and definitions as in the previous two Examples, the majority of the proof follows exactly as above. The difficult part is to show that $|F/N| \leq 8$, which we prove here. First, note that the relation $abab^{-1} = 1$ gives $aba = b$ and so

$$b^2 = (aba)^2 = (aba)(aba) = aba^2ba$$

Now, note that the relation $a^2b^{-2} = 1$ gives $a^2 = b^2$ and hence by the previous result we obtain

$$a^2 = b^2 = aba^2ba \quad \text{so that} \quad 1 = ba^2b = b(b^2)b = b^4$$

Therefore, by the relation $a^2 = b^2$ we also obtain

$$a^4 = (a^2)^2 = (b^2)^2 = b^4 = 1$$

Thus, the above results show that $a^4, b^4 \in N$. Furthermore, note that the relation $abab^{-1} = 1$ now gives that

$$ba = a^{-1}b = a^{-1} \cdot 1 \cdot b = a^{-1} \cdot a^4 \cdot b = a^3b \quad \text{so that} \quad b^{-1}a^3ba^{-1} = 1$$

Thus, the above result shows that $b^{-1}a^3ba^{-1} \in N$ so that $baN = a^3bN$. We will use the previous results below.

Towards this end, we first show that any element $wN \in F/N$ has a representative of the form a^ib^j for some $i \in \{0, 1, 2, 3\}$ and $j \in \{0, 1\}$. Indeed, suppose that $wN \in F/N$. Then since $a^4, b^4, a^2b^{-2} \in N$, we can choose a representative for wN of the form

$$a^{n_1}b^{n_2}a^{n_3}b^{n_4} \cdots a^{n_{r-1}}b^{n_r}$$

where $n_i \in \{0, 1, 2, 3\}$ for odd values of $i \in \{1, \ldots, r\}$ and $n_i \in \{0, 1\}$ for even values of $i \in \{1, \ldots, r\}$. Now, among all such representatives for wN of the above form choose one where r is as small as possible. Suppose that $r \geq 3$. In this case, we have $n_2 = 1$ and $n_3 \in \{1, 2, 3\}$. If $n_3 = 1$, then $n_3 - 1 = 0$ and thus we have since $baN = a^3bN$ that

$$a^{n_1}ba^{n_3}N = a^{n_1+3}ba^{n_3-1}N = a^{n_1+3}bN$$

which contradicts the minimality of r. Therefore, we must have $n_3 \in \{2, 3\}$. If $n_3 = 2$, then $n_3 - 2 = 0$ and thus we have since $baN = a^3bN$ that

$$a^{n_1}ba^{n_3}N = a^{n_1+3}ba^{n_3-1}N = a^{n_1+6}ba^{n_3-2}N = a^{n_1+6}bN$$

which contradicts the minimality of r. Therefore, we must have $n_3 = 3$ so that $n_3 - 3 = 0$ and thus we have since $baN = a^3bN$ that

$$a^{n_1}ba^{n_3}N = a^{n_1+3}ba^{n_3-1}N = a^{n_1+6}ba^{n_3-2}N = a^{n_1+9}ba^{n_3-3}N = a^{n_1+9}bN$$

which contradicts the minimality of r. Therefore, we must have $r \leq 2$ and in particular we conclude that wN has a representative of the form a^ib^j for some $i \in \{0, 1, 2, 3\}$ and $j \in \{0, 1\}$. This gives that $|F/N| \leq 4 \cdot 2 = 8$. Proceeding as in the previous Examples, this completes the proof. $\square$

Example. Let n be an integer with $n \geq 3$. Show that D_n is the group defined by the generators a, b and relations $a^n = 1, b^2 = 1, abab = 1$.

Proof. Let $X = \{a, b\}$ and $R = \{a^n, b^2, abab\}$ and let F be the free group on X. Let N be the smallest normal subgroup of F such that $R \subseteq N$. By definition, we have that the group defined by generators X and relations R is F/N.

Now, define a map

$$f : X \to D_n \quad \text{by} \quad a \mapsto r \quad b \mapsto s$$

Since F is free on X, there exists a unique group homomorphism $\overline{f} : F \to D_n$ with

$$\overline{f}(a) = f(a) = r \quad \text{and} \quad \overline{f}(b) = f(b) = s$$

Furthermore, since $\overline{f}$ is a group homomorphism we see

$$\overline{f}(a^n) = (\overline{f}(a))^n = r^n = 1$$

and

$$\overline{f}(b^2) = (\overline{f}(b))^2 = s^2 = 1$$

and

$$\begin{aligned}\overline{f}(abab) &= \overline{f}(a)\overline{f}(b)\overline{f}(a)\overline{f}(b) \\ &= rsrs \\ &= r(srs) \\ &= rr^{-1} \\ &= 1\end{aligned}$$

By the above computations, then, we see that $R \subseteq \ker \overline{f}$. But recall that N is the smallest normal subgroup of F containing R. Therefore, since $\ker \overline{f}$ is a normal subgroup of F containing R by the previous result we conclude that $N \subseteq \ker \overline{f}$. In particular, this observation implies that there exists a unique group homomorphism $g : F/N \to D_n$ with

$$g(aN) = \overline{f}(a) = r \quad \text{and} \quad g(bN) = \overline{f}(b) = s$$

Thus, we see that $\mathrm{Im}(g) \supseteq \{r, s\}$ and since $D_n = \langle r, s\rangle$ we see that g is a surjection so that $|F/N| \geq |D_n| = 2n$.

Finally, we show that $|F/N| \leq 2n$. Towards this end, we first show that any element $wN \in F/N$ has a representative of the form $a^i b^j$ for some $i \in \{0, 1, \ldots, n-1\}$ and $j \in \{0, 1\}$. Indeed, suppose that $wN \in F/N$. Then since $a^n, b^2 \in R \subseteq N$, we can choose a representative for wN of the form

$$a^{n_1} b^{n_2} a^{n_3} b^{n_4} \cdots a^{n_{r-1}} b^{n_r}$$

where $n_i \in \{0, 1, \ldots, n-1\}$ for odd values of $i \in \{1, \ldots, r\}$ and $n_i \in \{0, 1\}$ for even values of $i \in \{1, \ldots r\}$. Now, among all such representatives for wN of the above form choose one where r is as small as possible. Suppose that $r \geq 4$. In this case, we have $n_2 = 1 = n_4$. Now, note that the relation $abab = 1$ gives $bab = a^{-1}$ so that

$$a^{-2} = a^{-1} \cdot a^{-1} = (bab)(bab) = bab^2ab = ba \cdot 1 \cdot ab = ba^2b$$

so that

$$a^{-3} = a^{-1} \cdot a^{-2} = (bab)(ba^2b) = bab^2a^2b = ba \cdot 1 \cdot a^2b = ba^3b$$

Inductively, then, we conclude that

$$ba^m b = a^{-m} \quad \text{so that} \quad a^m b a^m b = 1$$

and hence $a^m b a^m b \in N$ so that $ba^m bN = a^{-m}N$ for each positive integer m. In particular, this gives that

$$ba^{n_3} bN = a^{-n_3}N$$

However, this contradicts the minimality of r. Thus, we must have $r \leq 3$. Suppose that $r = 3$. In this case, we have $n_2 = 1$. This gives since $b^2 \in R \subseteq N$ and by our above result that

$$ba^{n_3}N = ba^{n_3}b^2N = ba^{n_3}bbN = (ba^{n_3}b)bN = a^{-n_3}bN$$

However, this contradicts the minimality of r. Therefore, we must have $r \leq 2$ and in particular we conclude that wN has a representative of the form $a^i b^j$ for some $i \in \{0, 1, \ldots, n-1\}$ and $j \in \{0, 1\}$. This gives that $|F/N| \leq n \cdot 2 = 2n$. Combining the previous results, then, we conclude that

$$|F/N| = 2n = |D_n|$$

so that g is a surjection between two finite sets of the same cardinality. This implies that g is a bijection and hence g is a group isomorphism and thus $F/N \simeq D_n$. □

Example. Show that the group defined by the generators a, b and relations $a^2 = 1, b^3 = 1$ is infinite and nonabelian.

Proof. Let $X = \{a, b\}$ and $R = \{a^2, b^3\}$ and let F be the free group on X. Let N be the smallest normal subgroup of F such that $R \subseteq N$. By definition, we have that the group defined by generators X and relations R is F/N.

Before we begin, we prove that if $\theta : H \to K$ is a surjective group homomorphism and if K is nonabelian then H is nonabelian. Indeed, since K is nonabelian there are elements $k_1, k_2 \in K$ such that $k_1k_2 \neq k_2k_1$. Since θ is a surjection, there are elements $h_1, h_2 \in H$ such that $\theta(h_1) = k_1$ and $\theta(h_2) = k_2$. Now, suppose for the sake of contradiction that $h_1h_2 = h_2h_1$. Then as θ is a group homomorphism, we obtain

$$k_1k_2 = \theta(h_1)\theta(h_2) = \theta(h_1h_2) = \theta(h_2h_1) = \theta(h_2)\theta(h_1) = k_2k_1$$

so that $k_1k_2 = k_2k_1$ which is a contradiction. We conclude that $h_1h_2 \neq h_2h_1$ and in particular, this shows that H is nonabelian.

We now prove the main result. Towards this end, consider the elements $\sigma_1, \sigma_2 \in S_{\mathbb{Z}}$ given by

$$\sigma_1 = \cdots(-4 \quad -3)(-1 \quad 0)(2 \quad 3)\cdots$$

and

$$\sigma_2 = \cdots(-3 \quad -2 \quad -1)(0 \quad 1 \quad 2)(3 \quad 4 \quad 5)\cdots$$

Clearly, we have $\sigma_1^2 = (1) = \sigma_2^3$. Now, let $H = \langle \sigma_1\sigma_2 \rangle \subseteq S_{\mathbb{Z}}$ and define a map

$$f : X \to H \quad \text{by} \quad a \mapsto \sigma_1 \quad b \mapsto \sigma_2$$

Since F is free on X, there exists a unique group homomorphism $\overline{f} : F \to H$ with

$$\overline{f}(a) = f(a) = \sigma_1 \quad \text{and} \quad \overline{f}(b) = f(b) = \sigma_2$$

Furthermore, since $\overline{f}$ is a group homomorphism we see

$$\overline{f}(a^2) = (\overline{f}(a))^2 = \sigma_1^2 = (1)$$

and

$$\overline{f}(b^3) = (\overline{f}(b))^3 = \sigma_2^3 = (1)$$

By the above computations, then, we see that $R \subseteq \ker \overline{f}$. But recall that N is the smallest normal subgroup of F containing R. Therefore, since $\ker \overline{f}$ is a normal subgroup of F containing R by the previous result we conclude that $N \subseteq \ker \overline{f}$. In particular, this observation implies that there exists a unique group homomorphism $g : F/N \to H$ with

$$g(aN) = \overline{f}(a) = \sigma_1 \quad \text{and} \quad g(bN) = \overline{f}(b) = \sigma_2$$

Thus, we see that $\mathrm{Im}(g) \supseteq \{\sigma_1, \sigma_2\}$ and since $H = \langle \sigma_1, \sigma_2 \rangle$ we see that g is a surjection.

Now, notice that $(\sigma_1 \circ \sigma_2)(1) = 3$ but $(\sigma_2 \circ \sigma_1)(1) = 2$ so that in particular we have $\sigma_1 \circ \sigma_2 \neq \sigma_2 \circ \sigma_1$ and thus we see that H is a nonabelian group. Therefore, since g is a surjective group homomorphism we have by our preliminary result above that F/N is nonabelian. Finally, we claim that H is infinite. Indeed, consider the orbit $\mathcal{O}$ of $0 \in \mathbb{Z}$ in the action of H on $\mathbb{Z}$. Clearly, we have $\mathcal{O} = \mathbb{Z}$ by the definition of H. By the Orbit-Stablilzer Theorem, then, we obtain

$$\infty = |\mathbb{Z}| = |\mathcal{O}| = |H : \mathrm{Stab}_H(0)|$$

so that

$$|H| = \infty \cdot |\mathrm{Stab}_H(0)| = \infty$$

Therefore, since g is a surjection we obtain that $|F/N| \geq |H| = \infty$ so that F/N is infinite. We conclude that F/N is infinite and nonabelian, completing the proof. $\square$

Example. Let X be a set. Show that the free abelian group on X is isomorphic to the group defined by the generators X and relations $\{aba^{-1}b^{-1} = 1 : a, b \in X\}$. In particular, if $|X| = n < \infty$ then the group defined by the generators X and relations $\{aba^{-1}b^{-1} = 1 : a, b \in X\}$ is isomorphic to $\mathbb{Z}^n$.

Proof. Let $X = \{a, b\}$ and $R = \{aba^{-1}b^{-1} : a, b \in X\}$ and let F be the free group on X. Let N be the smallest normal subgroup of F such that $R \subseteq N$. By definition, we have that the group defined by generators X and relations R is F/N. If $X = \emptyset$, then both the free abelian group on X and F/N are trivial and hence isomorphic. Hence, we may assume that $X \neq \emptyset$.

We first show that F/N is the free abelian group on the set $Y = \{aN : a \in X\}$. To begin, we show that F/N is abelian. Towards this end, note that it suffices to show that $aNbN = bNaN$ for any $a, b \in X$ as this will imply that $w_1Nw_2N = w_2Nw_1N$ for any $w_1N, w_2N \in F/N$. Indeed, let $a, b \in X$. Then since $aba^{-1}b^{-1} \in N$, we have $abN = baN$ so that

$$aNbN = abN = baN = bNaN$$

Hence, we see that F/N is abelian.

Next, we show that Y is a nonempty basis for F/N. First, note that as $X \neq \emptyset$ we have $Y \neq \emptyset$. Now, suppose that $wN \in F/N$. Since $w \in F$, we have that $w = a_1^{n_1} \cdots a_m^{n_m}$ for some $a_1, \dots, a_m \in X$ and $n_1, \dots, n_m \in \mathbb{Z}$. Thus, since $a_1N, \dots, a_mN \in Y$ we obtain

$$wN = a_1^{n_1} \cdots a_m^{n_m} N = a_1^{n_1} N \cdots a_m^{n_m} N = (a_1N)^{n_1} \cdots (a_mN)^{n_m} \in \langle Y \rangle$$

Now, suppose that for some distinct elements $a_1N, \dots, a_mN \in Y$ and for some $n_1, \dots, n_m \in \mathbb{Z}$ we have

$$(a_1N)^{n_1} \cdots (a_mN)^{n_m} = N$$

so that

$$N = (a_1N)^{n_1} \cdots (a_mN)^{n_m} = a_1^{n_m} N \cdots a_m^{n_m} N = a_1^{n_1} \cdots a_m^{n_m} N$$

and hence $a_1^{n_1} \cdots a_m^{n_m} \in N$. Now, notice by the definition of N that we can write

$$N = \langle a^k b^\ell a^{-k} b^{-\ell} : a, b \in X, k, \ell \in \{0, 1, 2, \dots\} \rangle$$

In particular, this shows that if $w \in N$ then the exponent sum of each distinct letter in X appearing in the word w is equal to 0. Now, recall that $a_1^{n_1} \cdots a_m^{n_m} \in N$. By the previous observation, then, we have that the exponent sum of each distinct letter in X appearing in the word $a_1^{n_1} \cdots a_m^{n_m}$ is equal to 0. But recall that the elements $a_1N, \dots, a_mN \in Y$ are distinct so that $a_1, \dots, a_m \in X$ are distinct. Therefore, the exponent sum of a_j in the word $a_1^{n_1} \cdots a_m^{n_m}$ is equal to n_j and hence by the above we obtain that $n_j = 0$ for each $j \in \{1, \dots, m\}$. We conclude that F/N is the free abelian group on Y.

Finally, let G be the free abelian group on X. Now, notice that if $a, b \in X$ are distinct then $aN, bN \in Y$ are also distinct. On the other hand, if $aN, bN \in Y$ are distinct then $a, b \in X$ are also distinct. By these observations, then, we see that

$$|Y| = |\{aN : a \in X\} = |X|$$

Thus, by the result obtained above we see that G and F/N are both free abelian groups on sets of the same cardinality so that $F/N \simeq G$. Hence, as G is the free abelian group on X we conclude that F/N is isomorphic to free abelian group on X. In particular, suppose that $|X| = n < \infty$. In this case, the free abelian group on X is isomorphic to $\mathbb{Z}^n$. Therefore, by the above result we conclude that $F/N \simeq \mathbb{Z}^n$. $\square$

Topic 9: Indecomposability; Fitting's Lemma

Definition. Let G be a group. Then G is said to be ***indecomposable*** if G is nontrivial and G is not a direct sum of any two proper subgroups of G.

Example. The additive group $\mathbb{Q}$ is indecomposable.

Proof. Let H and K be any nontrivial, proper subgroups of $\mathbb{Q}$. Then there are nonzero elements $a_1/a_2 \in H$ and $b_1/b_2 \in K$. Now, notice that

$$a_1b_1 = b_1a_2 \cdot \frac{a_1}{a_2} \in H \quad \text{and} \quad a_1b_1 = a_1b_2 \cdot \frac{b_1}{b_2} \in K$$

so that $a_1b_1 \in H \cap K$. Furthermore, notice that since a_1/a_2 and b_1/b_2 are nonzero that necessarily a_1, b_1 are nonzero so that a_1b_1 is nonzero. By the previous result, then, we see $H \cap K \supsetneq \{0\}$. In particular, this shows that any two nontrivial, proper subgroups of $\mathbb{Q}$ intersect nontrivially so that $\mathbb{Q}$ cannot be a direct sum of any two proper subgroups of $\mathbb{Q}$. We conclude that the additive group $\mathbb{Q}$ is indecomposable. $\square$

Example. The group S_n is indecomposable for all $n \geq 2$.

Proof. If $n \in \{2, 3, 4\}$, the result is trivial, so assume that $n \geq 5$ and consider S_n. For the sake of contradiction, suppose that S_n were not indecomposable. Then there are nontrivial, proper subgroups H and K of S_n such that $S_n = H \oplus K$. Now, since $A_n \trianglelefteq S_n$ and as $S_n = H \oplus K$ it follows that $A_n \subseteq Z(S_n)$ or A_n has a nontrivial intersection with H or K. But recall that $n \geq 5$ so that in particular, we have that $Z(S_n)$ is trivial and that A_n is nontrivial. Therefore, we have $A_n \nsubseteq Z(S_n)$ and hence without loss of generality A_n must have a nontrivial intersection with H.

Next, since $H \trianglelefteq S_n$ as $S_n = H \oplus K$, we have that $H \cap A_n \trianglelefteq A_n$. But since $n \geq 5$, we have that A_n is simple so that $H \cap A_n \in \{\{1\}, A_n\}$. However, recall that $H \cap A_n$ is nontrivial so that by the previous observation we have $H \cap A_n = A_n$ so that $A_n \subseteq H$. But since H is a *proper* subgroup of S_n, we must have $H = A_n$ by the previous inclusion. This gives that

$$n! = |S_n| = |H \oplus K| = |H||K| = |A_n||K| = \frac{n!}{2}|K| \quad \text{so that} \quad |K| = 2$$

Furthermore, since $H = A_n$ and $H \cap K = \{1\}$ as $S_n = H \oplus K$ it now follows by the above calculation that $K = \{(1), \sigma\}$ for some $\sigma \in S_n - A_n$.

Finally, notice that since $\sigma \notin A_n$ that we have in particular that $\sigma \neq (1)$ and hence there are $a, b \in \{1, \ldots, n\}$ such that $\sigma(a) = b \neq a$. Furthermore, since $n \geq 5$ there is some $c \in \{1, \ldots, n\} - \{a, b\}$. This gives that

$$[(b \quad c)\sigma(b \quad c)^{-1}](a) = c \notin \{a, b\} = \{(1)(a), \sigma(a)\}$$

so that $(b \quad c)\sigma(b \quad c)^{-1} \notin \{(1), \sigma\} = K$. However, we have $K \trianglelefteq S_n$ as $S_n = H \oplus K$ and as $\sigma \in K$ we have $(b \quad c)\sigma(b \quad c)^{-1} \in K$ which is a contradiction. This final contradiction completes the proof. $\square$

Example. A nonzero homomorphic image of an indecomposable group need not be indecomposable.

Proof. Consider Q_8 and recall that the proper, nontrivial subgroups of Q_8 are precisely $\langle -1\rangle, \langle i\rangle, \langle j\rangle, \langle k\rangle$. Moreover, since each of these subgroups of Q_8 is cyclic it follows that each of these subgroups of Q_8 is abelian. Therefore, the direct sum of any two of these subgroups of Q_8 is abelian. However, notice that Q_8 is nonabelian as

$$ij = k \neq -k = ji$$

By combining the previous two observations, then, we see that Q_8 cannot be a direct sum of any two proper, nontrivial subgroups of Q_8 so that Q_8 is indecomposable.

Finally, consider the canonical projection map $\pi : Q_8 \to Q_8/\langle -1\rangle$ and notice that as π is a surjection we have

$$|\pi(Q_8)| = |Q_8/\langle -1\rangle| = \frac{8}{2} = 4 > 1$$

so that in particular $Q_8/\langle -1\rangle$ is a nonzero homomorphic image of the homomorphism π. However, notice that since every element of $Q_8/\langle -1\rangle$ is of order 2 and as $|Q_8/\langle -1\rangle| = 4$ it follows that $Q_8/\langle -1\rangle \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. In particular, this shows that the nonzero homomorphic image $Q_8/\langle -1\rangle$ of the indecomposable group Q_8 is not indecomposable. This completes the proof. $\square$

Definition. Let G be a group. Then G is said to satisfy the ***ascending chain condition (ACC)*** on subgroups if whenever

$$G_1 \subseteq G_2 \subseteq G_3 \subseteq \cdots \subseteq G_n \subseteq \cdots$$

is an increasing sequence of subgroups of G, there is a positive integer N such that $G_n = G_N$ for all $n \geq N$.

Remark. The definition for the ACC on normal subgroups, the definition for the descending chain condition (DCC) on subgroups, and the definition for the DCC on normal subgroups are defined analogously as in the formal Definition given above.

Example. Consider $\mathbb{Z}$. Then $\mathbb{Z}$ satisfies the ACC on subgroups but $\mathbb{Z}$ does satisfy the DCC on subgroups.

Proof. Since $\mathbb{Z}$ is a Noetherian ring, it is immediate that $\mathbb{Z}$ satisfies the ACC on subgroups. Now, for the element $2 \in \mathbb{Z}$ consider the subgroups of $\mathbb{Z}$ defined by $G_i = \langle 2^i\rangle$ for each $i \in \{1, 2, 3, \dots\}$. Then we obtain the properly decreasing chain

$$G_1 \supsetneq G_2 \supsetneq G_3 \supsetneq \cdots \supsetneq G_n \supsetneq \cdots$$

of subgroups of $\mathbb{Z}$. In particular, since this chain is properly decreasing it now follows that $\mathbb{Z}$ does not satisfy the DCC on subgroups. $\square$

Example. Let G be a group and let H and K be subgroups of G such that $G = H \oplus K$. Then if $N \trianglelefteq H$, we have $N \trianglelefteq G$. Therefore, if G satisfies the ACC or DCC on normal subgroups then so do H and K.

Proof. First, note that if $h \in K$ and $k \in K$ then as $H \trianglelefteq G$ and $K \trianglelefteq G$ as $G = H \oplus K$ we have

$$k^{-1}h^{-1}kh \in H \cap K$$

Furthermore, we have that $H \cap K = \{1\}$ as $G = H \oplus K$. This gives by the above result that $k^{-1}h^{-1}kh = 1$ and hence $hk = kh$.

We now prove the main result. Towards this end, let $g \in G$ and $n \in N$. As $G = H \oplus K$, there exist unique elements $h \in H$ and $k \in K$ such that $g = hk$. Furthermore, as $N \trianglelefteq H$ we see that if $n' = h^{-1}nh$ then $n' \in N$. Now, observe that

$$g^{-1}ng = (hk)^{-1}n(hk) = k^{-1}h^{-1}nhk = k^{-1}n'k$$

But by our preliminary result, we have since $n' \in N \trianglelefteq H$ and as $k \in K$ that $n'k = kn'$ so that

$$g^{-1}ng = k^{-1}n'k = k^{-1}kn' = n' \in N$$

We may now conclude that $N \trianglelefteq G$, completing the proof.

Finally, notice by the above result that it follows that any subgroup that is normal in H or K is normal in G. Therefore, if G satisfies the ACC or DCC on normal subgroups then so must H and K. This completes the proof. □

Theorem. Let G be a group that satisfies the ACC and DCC on normal subgroups. Then G is the direct sum of a finite number of indecomposable subgroups of G.

Proof. Omitted. □

Definition. Let G be a group and let $f : G \to G$ be an endomorphism of G. Then f is a ***normal endomorphism*** of G if

$$f(gag^{-1}) = gf(a)g^{-1} \quad \text{for all} \quad g, a \in G$$

Example. Let G be a group and let $f, g : G \to G$ be normal endomorphisms of G.

(a): $f \circ g : G \to G$ is a normal endomorphism of G.

(b): If $H \trianglelefteq G$, then $f(H) \trianglelefteq G$.

(c): If $f + g : G \to G$ is an endomorphism of G, then $f + g$ is a normal endomorphism of G.

Proof. (a): Let $a, h \in G$. Then since f and g are normal endomorphisms of G, we obtain

$$(f \circ g)(hah^{-1}) = f(g(hah^{-1})) = f(hg(a)h^{-1}) = hf(g(a))h^{-1} = h(f \circ g)(a)h^{-1}$$

This completes the proof. □

Proof. (b): Let $x \in f(H)$ and $k \in G$. As $x \in f(H)$, there is some $h \in H$ such that $x = f(h)$. Furthermore, as $H \trianglelefteq G$ we have that $khk^{-1} \in H$. Thus, we obtain since f is a normal endomorphism of G that

$$kxk^{-1} = kf(h)k^{-1} = f(khk^{-1}) \in f(H)$$

which shows that $f(H) \trianglelefteq G$. This completes the proof. □

Proof. (c): Let $a, h \in G$. Then since f and g are normal endomorphisms of G, we obtain

$$\begin{aligned}(f+g)(hah^{-1}) &= f(hah^{-1})g(hah^{-1}) \\ &= [hf(a)h^{-1}][hg(a)h^{-1}] \\ &= hf(a)g(a)h^{-1} \\ &= h(f+g)(a)h^{-1}\end{aligned}$$

This completes the proof. □

Lemma. Let G be a group that satisfies the ACC on normal subgroups and let $f : G \to G$ be an endomorphism of G. Then f is an automorphism of G if and only if f is an epimorphism.

Proof. If f is an automorphism of G, then f is an epimorphism. On the other hand, suppose that f is an epimorphism. Now, notice that

$$\{1\} \subseteq \ker f \subseteq \ker f^2 \subseteq \ker f^3 \subseteq \cdots \subseteq \ker f^n \subseteq \cdots$$

is an ascending sequence of normal subgroups of G. By hypothesis, then, there is some positive integer N such that $\ker f^N = \ker f^{N+1}$. Now, let $a \in \ker f$. Since f is an epimorphism, it follows that f^N is an epimorphism and hence there is some $g \in G$ such that $f^N(g) = a$. But notice that as $a \in \ker f$, we have

$$0 = f(a) = f(f^N(g)) = f^{N+1}(g) \quad \text{so that} \quad g \in \ker f^{N+1} = \ker f^N$$

Thus, we obtain that $a = f^N(g) = 0$ so that $\ker f$ is trivial. Since f is an endomorphism of G, then, we see that f is an injection and as f is an epimorphism we conclude that f is an automorphism of G. □

Lemma. Let G be a group that satisfies the DCC on normal subgroups and let $f : G \to G$ be a normal endomorphism of G. Then f is an automorphism of G if and only if f is a monomorphism.

Proof. If f is an automorphism of G, then f is a monomorphism. On the other hand, suppose that f is a monomorphism. Then since f is a normal endomorphism of G, it follows that

$$G \supseteq f(G) \supseteq f^2(G) \supseteq f^3(G) \supseteq \cdots \supseteq f^n(G) \supseteq \cdots$$

is a descending sequence of normal subgroups of G. By hypothesis, then, there is some positive integer N such that $f^N(G) = f^{N+1}(G)$. Now, let $g \in G$. Then there is some $a \in G$ such that $f^N(g) = f^{N+1}(a)$. Since f is a monomorphism, it follows that f^N is a monomorphism and hence

$$f^N(g) = f^{N+1}(a) = f^N(f(a)) \quad \text{so that} \quad f(a) = g$$

Thus, we obtain that f is a surjection and as f is a monomorphism we conclude that f is an automorphism of G. □

Lemma. (Fitting's Lemma): Let G be a group that satisfies both the ACC and DCC on normal subgroups and let $f : G \to G$ be a normal endomorphism of G. Then there is a integer $n \geq 1$ such that $G = \ker f^n \oplus f^n(G)$.

Proof. By the proofs of the previous two Lemmas, it follows that there is some integer $n \geq 1$ such that $\ker f^{n+m} = \ker f^n$ and $f^n(G) = f^{n+m}(G)$ for each integer $m \geq 0$. Furthermore, we know that $\ker f^n$ is clearly a normal subgroup of G and since f is a normal endomorphism of G we have that $f^n(G)$ is a normal subgroup of G.

Now, let $a \in \ker f^n \cap f^n(G)$. Since $a \in f^n(G)$, there is some $g \in G$ such that $f^n(g) = a$ and since $a \in \ker f^n$ this gives that

$$f^{2n}(g) = f^n(f^n(g)) = f^n(a) = 1 \quad \text{so that} \quad g \in \ker f^{2n} = \ker f^n$$

Thus, we see that $a = f^n(g) = 1$ and hence $\ker f^n \cap f^n(G) = \{1\}$.

Finally, let $g \in G$. Since $f^n(G) = f^{2n}(G)$, there is some $a \in G$ such that $f^{2n}(a) = f^n(g)$. Now, observe that

$$f^n(f^n(a)g^{-1}) = f^{2n}(a)f^n(g^{-1}) = f^n(g)f^n(g^{-1}) = f^n(g)(f^n(g))^{-1} = 1$$

so that $f^n(a)g^{-1} \in \ker f^n$ and hence

$$g(f^n(a))^{-1} = [f^n(a)g^{-1}]^{-1} \in \ker f^n$$

so that $g \in \ker f^n \cdot f^n(G)$. We conclude that $G = \ker f^n \oplus f^n(G)$. Combining the previous results, then, we obtain that $G = \ker f^n \oplus f^n(G)$. $\square$

Definition. Let G be a group and let $f : G \to G$ be an endomorphism of G. Then f is said to be ***nilpotent*** if there is some integer $n \geq 1$ such that $f^n(g) = 1$ for all $g \in G$.

Corollary. Let G be an indecomposable group that satisfies both the ACC and DCC on normal subgroups and let $f : G \to G$ be a normal endomorphism of G. Then either f is nilpotent or f is an automorphism of G.

Proof. By Fitting's Lemma, there is an integer $n \geq 1$ such that $G = \ker f^n \oplus f^n(G)$. But since G is indecomposable, we must have either $\ker f^n = \{1\}$ or $f^n(G) = \{1\}$. If $\ker f^n = \{1\}$, then f is a normal monomorphism of G and hence by a previous Lemma we see that f is an automorphism of G. If $f^n(G) = \{1\}$, then $f^n(g) = 1$ for all $g \in G$ and hence f is nilpotent. This completes the proof. $\square$

Fall Semester 2016 Homework Assignments

Homework 1: Page 240 #6, 7, 8

Problem 6. *Every element of $K(x_1, \ldots, x_n)$ which is not in K is transcendental over K.*

Proof. We will prove this result by contrapositive in the case where $n = 1$ and remark that the proof of the general case is similar. Towards this end, suppose that $u \in K(x)$ is algebraic over K. If $u = 0$, then clearly we have $u \in K$. So, assume that $u \neq 0$. Since $u \in K(x)$ and $u \neq 0$, we may write $u = f(x)/g(x)$ for some nonzero, relatively prime polynomials $f(x), g(x) \in K[x]$.

We desire to show that $u \in K$, which will establish the result. Since $u \in K(x)$ is algebraic over K, there exists an irreducible polynomial $p(y) \in K[y]$ so that $p(u) = 0$. Since $p(y) \in K[y]$, we may write

$$p(y) = \sum_{i=0}^{n} a_i y^i$$

where $a_i \in K$ for $i \in \{0, \ldots, n\}$. Clearly, we may assume that $a_n \neq 0$. Furthermore, since $p(y)$ is irreducible, we have that $a_0 \neq 0$. Now, note that

$$0 = p(u) = p(f(x)/g(x)) = \sum_{i=0}^{n} a_i (f(x)/g(x))^i$$

so that, after clearing denominators, we obtain

$$0 = \sum_{i=0}^{n} a_i f(x)^i g(x)^{n-i} = a_0 g(x)^n + a_1 f(x) g(x)^{n-1} + \cdots + a_n f(x)^n$$

Now, the previous equality implies that $f(x)$ divides $a_0 g(x)^m$ and that $g(x)$ divides $a_n f(x)^n$. But since $f(x)$ and $g(x)$ are relatively prime, these two observations imply that $f(x)$ divides a_0 and that $g(x)$ divides a_n. Since a_0 and a_n are nonzero elements of K, it now follows that since $f(x)$ divides a_0 and since $g(x)$ divides a_n that $f(x), g(x) \in K$. In particular, we now obtain

$$u = f(x)/g(x) \in K$$

This completes the proof. $\square$

Problem 7. *If v is algebraic over $K(u)$ for some $u \in F$ and v is transcendental over K, then u is algebraic over $K(v)$.*

Proof. Since v is algebraic over $K(u)$, there is a nonzero polynomial $z(x) \in K(u)[x]$ such that $z(v) = 0$. Since $z(x) \in K(u)[x]$, we may write

$$z(x) = \sum_{i=0}^{n} \frac{f_i(u)}{g_i(u)} x^i$$

where $f_i(x), g_i(x) \in K[x]$ and $g_i(u) \neq 0$ for all $i \in \{0, \ldots, n\}$. Notice that

$$0 = z(v) = \sum_{i=0}^{n} \frac{f_i(u)}{g_i(u)} v^i$$

so that, after clearing denominators, we obtain

$$0 = \sum_{i=0}^{n} h_i(u) v^i$$

where $h_i(x) = f_i(x) \prod_{k=0, k \neq i}^{n} g_i(x) \in K[x]$ for all $i \in \{0, \ldots, n\}$. Therefore, since $h_i(x) \in K[x]$, we may write

$$h_i(x) = \sum_{j=0}^{m} a_{ij} x^j$$

where $a_{ij} \in K$ for all $i \in \{0, \ldots, n\}$ and $j \in \{0, \ldots, m\}$. By the above, we now have

$$0 = \sum_{i=0}^{n} h_i(u) v^i = \sum_{i=0}^{n} \sum_{j=0}^{m} a_{ij} u^j v^i = \sum_{j=0}^{m} \left(\sum_{i=0}^{n} a_{ij} v^i \right) u^j$$

Clearly, we have

$$\sum_{i=0}^{n} a_{ij} v^i \in K(v)$$

for each $j \in \{0, \ldots, m\}$ so that if

$$\psi(x) = \sum_{j=0}^{m} \left(\sum_{i=0}^{n} a_{ij} v^i \right) x^j$$

then $\psi(x) \in K(v)[x]$ and $\psi(u) = 0$ by the above.

It remains to prove that $\psi(x) \neq 0$. For the sake of contradiction, suppose that $\psi(x) = 0$. In this case, we have

$$\sum_{i=0}^{n} a_{ij} v^i = 0$$

for all $j \in \{0, \ldots, m\}$. But since v is transcendental over K, this equality implies that $a_{ij} = 0$ for all $i \in \{0, \ldots, n\}$ and hence we obtain that $a_{ij} = 0$ for all $i \in \{0, \ldots, n\}$ and

$j \in \{0, \ldots, m\}$. This gives by the definition of $h_i(x)$ that $h_i(x) = 0$ for all $i \in \{0, \ldots, n\}$. But then

$$0 = h_i(x) = f_i(x) \prod_{k=0, k \neq i}^{n} g_i(x)$$

and since $g_i(x) \neq 0$, this implies that $f_i(x) = 0$ for all $i \in \{0, \ldots, n\}$. Hence, by the definition of $z(x)$ we obtain that $z(x) = 0$ which is a contradiction because $z(x)$ is nonzero. We conclude that $\psi(x) \in K(v)[x]$ is nonzero.

In conclusion, we have shown that $\psi(u) = 0$, where $\psi(x)$ is a nonzero polynomial in $K(v)[x]$. In particular, this shows that u is algebraic over $K(v)$. This completes the proof. $\square$

Problem 8. *If $u \in F$ is algebraic of odd degree over K, then so is u^2 and $K(u) = K(u^2)$.*

Proof. First, note that we clearly have the inclusion $K \subseteq K(u^2) \subseteq K(u)$ so that

$$[K(u) : K] = [K(u) : K(u^2)][K(u^2) : K]$$

In particular, since $[K(u) : K]$ is odd, the above equality shows that it cannot be the case that $[K(u) : K]$ is even. Hence, we have that $[K(u^2) : K]$ is odd. Furthermore, since $[K(u) : K] < \infty$ it follows by the above equality that $[K(u^2) : K] < \infty$, so that u^2 is algebraic over K. This completes the first part of the proof.

Now, let $p(x) = x^2 - u^2 \in K(u^2)[x]$. Note $\deg(p(x)) = 2$ and $p(u) = u^2 - u^2 = 0$. In particular, since $K(u, u^2) = K(u)$, this shows that

$$[K(u) : K(u^2)] = [K(u, u^2) : K(u^2)] = [K(u^2)(u) : K(u^2)] \leq \deg(p(x)) = 2$$

Thus, we have $[K(u) : K(u^2)] \in \{1, 2\}$. But if $[K(u) : K(u^2)] = 2$, then the equality at the beginning of the proof would imply that $[K(u) : K]$ is even, which is a contradiction. Hence, we must have $[K(u) : K(u^2)] = 1$ so that $K(u) = K(u^2)$. This completes the second part of the proof. $\square$

Homework 2: Page 240 #9, 13, 15

Problem 9. *If $x^n - a \in K[x]$ is irreducible and $u \in F$ is a root of $x^n - a$ and m divides n, then prove that the degree of u^m over K is n/m. What is the irreducible polynomial for u^m over K?*

Proof. Since m divides n, we may define $h(x) = x^{n/m} - a \in K[x]$. Notice that since u is a root of $x^n - a$ that we have

$$h(u^m) = (u^m)^{n/m} - a = u^n - a = 0$$

so that $h(u^m) = 0$. We claim that $h(x)$ is irreducible over K. For the sake of contradiction, suppose that $h(x)$ were reducible over K. Then we can write $h(x) = h_1(x)h_2(x)$ for some nonconstant polynomials $h_1(x), h_2(x) \in K[x]$. In this case, we have

$$h_1(x^m)h_2(x^m) = h(x^m) = (x^m)^{n/m} - a = x^n - a$$

which implies that $x^n - a$ is reducible over K since $h_1(x^m)$ and $h_2(x^m)$ are nonconstant polynomials in $K[x]$. This is a contradiction since $x^n - a$ is irreducible over K by hypothesis. Therefore, we conclude that $h(x)$ is irreducible over K.

Finally, since $h(x)$ is irreducible over K and since $h(u^m) = 0$, it follows that $h(x)$ is the irreducible polynomial for u^m over K. Furthermore, since $h(x) \in K[x]$ is a monic, irreducible polynomial with $h(u^m) = 0$, it follows that $h(x)$ is the minimum polynomial for u^m over K so that

$$[K(u^m) : K] = \deg(h(x)) = n/m$$

This shows that the degree of u^m over K is n/m, completing the proof. $\square$

Problem 13. *Consider the extension $\mathbb{Q}(u)/\mathbb{Q}$ generated by a real root u of $x^3 - 6x^2 + 9x + 3$. Express each of the following elements in terms of the basis $\{1, u, u^2\}$:*

(i): u^4

(ii): u^5

(iii): $3u^5 - u^4 + 2$

(iv): $(u+1)^{-1}$

(v): $(u^2 - 6u + 8)^{-1}$

Note: We remark that $x^3 - 6x^2 + 9x + 3$ is irreducible over $\mathbb{Q}$ by Eisenstein's Criterion. Furthermore, since u is a root of $x^3 - 6x^2 + 9x + 3$, it follows that

$$0 = u^3 - 6u^2 + 9u + 3 \quad \text{so that} \quad u^3 = 6u^2 - 9u - 3$$

Proof. (i): We have

$$\begin{aligned} u^4 &= u \cdot u^3 \\ &= u(6u^2 - 9u - 3) \\ &= 6u^3 - 9u^2 - 3u \\ &= 6(6u^2 - 9u - 3) - 9u^2 - 3u \\ &= 27u^2 - 57u - 18 \end{aligned}$$

□

Proof. (ii): We have

$$\begin{aligned} u^5 &= u \cdot u^4 \\ &= u(27u^2 - 57u - 18) \\ &= 27u^3 - 57u^2 - 18u \\ &= 27(6u^2 - 9u - 3) - 57u^2 - 18u \\ &= 105u^2 - 261u - 81 \end{aligned}$$

□

Proof. (iii): We have

$$\begin{aligned} 3u^5 - u^4 + 2 &= 3(105u^2 - 261u - 81) - (27u^2 - 57u - 18) + 2 \\ &= 288u^2 - 726u - 223 \end{aligned}$$

□

Proof. (iv): Using polynomial long division we obtain the equality

$$x^3 - 6x^2 + 9x + 3 = (x+1)(x^2 - 7x + 16) - 13$$

so that

$$0 = u^3 - 6u^2 + 9u + 3 = (u+1)(u^2 - 7u + 16) - 13$$

so that

$$13 = (u+1)(u^2 - 7u + 16)$$

so that

$$1 = \frac{1}{13}(u+1)(u^2 - 7u + 16)$$

so that

$$(u+1)^{-1} = \frac{1}{13}(u^2 - 7u + 16)$$

so that

$$(u+1)^{-1} = \frac{1}{13}u^2 - \frac{7}{13}u + \frac{16}{13}$$

□

Proof. (v): Using polynomial long division, we obtain the equality

$$x^3 - 6x^2 + 9x + 3 = (x^2 - 6x + 8)x + (x+3)$$

so that

$$0 = u^3 - 6u^2 + 9u + 3 = (u^2 - 6u + 8)u + (u+3)$$

so that

$$-u(u^2 - 6u + 8) = u + 3$$

Similarly, using polynomial long division, we obtain the equality

$$x^3 - 6x^2 + 9x + 3 = (x+3)(x^2 - 9x + 36) - 105$$

so that

$$0 = u^3 - 6u^2 + 9u + 3 = (u+3)(u^2 - 9u + 36) - 105$$

so that

$$105 = (u+3)(u^2 - 9u + 36)$$

so that

$$1 = \frac{1}{105}(u+3)(u^2 - 9u + 36)$$

so that

$$(u+3)^{-1} = \frac{1}{105}u^2 - \frac{9}{105}u + \frac{36}{105}$$

Thus, we obtain

$$1 = -u(u^2 - 6u + 8)(u+3)^{-1}$$

so that

$$\begin{aligned}
(u^2 - 6u + 8)^{-1} &= -u(u+3)^{-1} \\
&= -u\left(\frac{1}{105}u^2 - \frac{9}{105}u + \frac{36}{105}\right) \\
&= -\frac{1}{105}u^3 + \frac{9}{105}u^2 - \frac{36}{105}u \\
&= -\frac{1}{105}(6u^2 - 9u - 3) + \frac{9}{105}u^2 - \frac{36}{105}u \\
&= \frac{3}{105}u^2 - \frac{27}{105}u + \frac{3}{105}
\end{aligned}$$

□

Problem 15. *In the field $K(x)$, let $u = x^3/(x+1)$. Show that $K(x)$ is a simple extension of the field $K(u)$. What is $[K(x) : K(u)]$?*

Proof. Define $f(y) \in K(u)[y]$ by

$$f(y) = y^3 - uy - u = y^3 - \frac{x^3}{x+1}y - \frac{x^3}{x+1} = y^3 - \frac{x^3}{x+1}(y+1)$$

and note that

$$f(x) = x^3 - \frac{x^3}{x+1}(x+1) = x^3 - x^3 = 0$$

so that x is a root of $f(y)$.

We claim that $f(y)$ is irreducible over $K(u)$. First, we show that $f(y)$ is irreducible over $K[u]$. Towards this end, notice that $K[u]/(u) \simeq K$. Since K is a field, it now follows that (u) is a maximal ideal of $K[u]$ and hence a prime ideal of $K[u]$. Hence, since $f(y) = y^3 - uy - u$ and $u \in (u)$ but $u \notin (u)^2$, we have that $f(y)$ is irreducible over $K[u]$ by Eisenstein's Criterion. Since $K(u)$ is the field of fractions of $K[u]$, it now follows by Gauss' Lemma that $f(y)$ is irreducible over $K(u)$.

Now, by the above we have that $f(y)$ is a monic, irreducible polynomial in $K(u)[y]$ that has x as a root so that $f(y)$ is the minimum polynomial for x over $K(u)$. Furthermore, note that

$$u = \frac{x^3}{x+1} \in K(x)$$

so that $K(u)(x) = K(u, x) = K(x)$. This shows that $K(x)$ is a simple extension of $K(u)$ since $x \in K(x)$ and $K(u)(x) = K(x)$. Finally, combining the above results gives

$$[K(x) : K(u)] = [K(u)(x) : K(u)] = \deg(f(y)) = 3$$

This completes the proof. $\square$

Homework 3: Page 240 #10, 11, 17

Problem 10. *If F is algebraic over K and D is an integral domain such that $K \subseteq D \subseteq F$, then D is a field.*

Proof. Since D is an integral domain, it suffices to show that if $a \in D$ is a nonzero element of D then $a^{-1} \in D$. Towards this end, let $a \in D$ be a nonzero element of $D \subseteq F$. Since $a \in F$ and F/K is algebraic, it follows that there exists an irreducible polynomial $f(x) \in K[x]$ such that $f(a) = 0$. Let

$$f(x) = \sum_{i=0}^{n} b_i x^i$$

where $b_i \in K$ for $i \in \{0, \ldots, n\}$. Since $f(x)$ is irreducible, it follows that $b_0 \neq 0$.

Now, let $c = -b_0 \in K$. Since $b_0 \neq 0$ we have $c \neq 0$ so that $c^{-1} \in K$ exists. Notice that since $f(a) = 0$ we have

$$0 = f(a) = \sum_{i=0}^{n} b_i a^i = b_0 + b_1 a + \cdots + b_n a^n$$

which implies that

$$c = -b_0 = b_1 a + \cdots + b_n a^n = a(b_1 + \cdots + b_n a^{n-1})$$

Multiplying both sides of the above equality by c^{-1}, we obtain

$$1 = c^{-1}c = c^{-1}a(b_1 + \cdots + b_n a^{n-1}) = a(c^{-1}b_1 + \cdots + c^{-1}b_n a^{n-1})$$

By the above equality, it now follows that $a^{-1} = c^{-1}b_1 + \cdots + c^{-1}b_n a^{n-1}$. Furthermore, since $c^{-1}, b_1, \ldots, b_n \in K \subseteq D$ and since $a, \ldots, a^{n-1} \in D$ as $a \in D$, it follows that

$$a^{-1} = c^{-1}b_1 + \cdots + c^{-1}b_n a^{n-1} \in D$$

so that $a^{-1} \in D$. Since $a \in D$ was an arbitrary nonzero element of D, this completes the proof that D is a field. $\square$

Problem 11. *Give an example of a field extension $K \subseteq F$ such that $u, v \in F$ are transcendental over K, but $K(u, v) \neq K(x_1, x_2)$.*

Proof. Consider the field extension $\mathbb{Q}(\pi, \pi^2)/\mathbb{Q}$. We know that π is transcendental over $\mathbb{Q}$. We will show that π^2 is transcendental over $\mathbb{Q}$. For the sake of contradiction, suppose that π^2 were algebraic over $\mathbb{Q}$. Then there exists a nonzero polynomial $p(x) \in \mathbb{Q}[x]$ such that $p(\pi^2) = 0$. Let

$$p(x) = \sum_{i=0}^{n} a_i x^i$$

where $a_i \in \mathbb{Q}$ for $i \in \{0, \ldots, n\}$. Define $q(x) \in \mathbb{Q}[x]$ by

$$q(x) = \sum_{i=0}^{n} a_i x^{2i}$$

In particular, note that $q(x)$ is nonzero since $p(x)$ is nonzero. Now, notice that since $p(\pi^2) = 0$ we have

$$q(\pi) = \sum_{i=0}^{n} a_i \pi^{2i} = \sum_{i=0}^{n} a_i (\pi^2)^i = p(\pi^2) = 0$$

so that π is a root of the nonzero polynomial $q(x) \in \mathbb{Q}[x]$. This implies that π is algebraic over $\mathbb{Q}$ which is a contradiction. By this contradiction, it must be the case that π^2 is transcendental over $\mathbb{Q}$. Hence, we have that $\mathbb{Q}(\pi, \pi^2)/\mathbb{Q}$ is a field extension with $\pi, \pi^2 \in \mathbb{Q}(\pi, \pi^2)$ being transcendental over $\mathbb{Q}$.

Finally, notice that since $\pi^2 \in \mathbb{Q}(\pi)$ that $\mathbb{Q}(\pi, \pi^2) = \mathbb{Q}(\pi)$. In particular, this implies that the extension $\mathbb{Q}(\pi, \pi^2)/\mathbb{Q}$ has transcendence degree 1. On the other hand, clearly, the extension $\mathbb{Q}(x_1, x_2)/\mathbb{Q}$ has transcendence degree 2. Therefore, it cannot be the case that $\mathbb{Q}(\pi, \pi^2) \simeq \mathbb{Q}(x_1, x_2)$. This completes the proof. $\square$

Problem 17. *Find an irreducible polynomial f of degree 2 over the field $\mathbb{Z}_2$. Adjoin a root u of f to $\mathbb{Z}_2$ to obtain a field $\mathbb{Z}_2(u)$ of order 4. Use the same method to construct a field of order 8.*

Proof. Define $f(x) = x^2 + x + 1 \in \mathbb{Z}_2[x]$. Since $f(0) = 1 = f(1)$, it follows that $f(x)$ has no roots over $\mathbb{Z}_2$. Since $\mathbb{Z}_2$ is a field and since $f(x)$ is of degree 2, it now follows that $f(x)$ is irreducible over $\mathbb{Z}_2$.

Now, let u be a root of $f(x)$. Note that $f(x)$ is a monic, irreducible polynomial in $\mathbb{Z}_2[x]$ that has u as a root so that $f(x)$ is the minimum polynomial for u over $\mathbb{Z}_2$. As $\deg(f(x)) = 2$, it now follows that $\{1, u\}$ is a basis for $\mathbb{Z}_2(u)$ over $\mathbb{Z}_2$. Hence, we obtain

$$\mathbb{Z}_2(u) = \{a + bu : a, b \in \mathbb{Z}_2\} = \{0, 1, u, 1 + u\}$$

so that $\mathbb{Z}_2(u)$ is a field of order 4. This completes the first proof.

Define $g(x) = x^3 + x + 1 \in \mathbb{Z}_2[x]$. Since $f(0) = 1 = f(1)$, it follows that $g(x)$ has no roots over $\mathbb{Z}_2$. Since $\mathbb{Z}_2$ is a field and since $g(x)$ is of degree 3, it now follows that $g(x)$ is irreducible over $\mathbb{Z}_2$.

Now, let u be a root of $g(x)$. Note that $g(x)$ is a monic, irreducible polynomial in $\mathbb{Z}_2[x]$ that has u as a root so that $g(x)$ is the minimum polynomial for u over $\mathbb{Z}_2$. As $\deg(g(x)) = 3$, it follows that $\{1, u, u^2\}$ is a basis for $\mathbb{Z}_2(u)$ over $\mathbb{Z}_2$. Hence, we obtain

$$\mathbb{Z}_2(u) = \{a + bu + cu^2 : a, b, c \in \mathbb{Z}_2\} = \{0, 1, u, u^2, 1 + u, 1 + u^2, u + u^2, 1 + u + u^2\}$$

so that $\mathbb{Z}_2(u)$ is a field of order 8. This completes the second proof. $\square$

Homework 4: Page 255 #2, 4, 5

Problem 2. $\mathrm{Gal}(\mathbb{R}/\mathbb{Q})$ *is the identity group.*

Proof. Let $\sigma \in \mathrm{Gal}(\mathbb{R}/\mathbb{Q})$. First, we show that σ maps positive real numbers to positive real numbers. Towards this end, let $a \in \mathbb{R}$ be a positive real number. Then there exists a nonzero element $c \in \mathbb{R}$ such that $c^2 = a$. Since σ is an automorphism of $\mathbb{R}$, it follows that since $c \neq 0$ that $\sigma(c) \neq 0$ so that

$$\sigma(a) = \sigma(c^2) = \sigma(c)^2 > 0$$

This proves that σ maps positive real numbers to positive real numbers.

Next, we show that σ preserves order. Towards this end, let $a, b \in \mathbb{R}$ with $a < b$. Then we have that $b - a > 0$ so that by the above and since σ is an automorphism of $\mathbb{R}$ we obtain

$$\sigma(b) - \sigma(a) = \sigma(b - a) > 0$$

so that $\sigma(a) < \sigma(b)$. This proves that σ preserves order.

Finally, for the sake of contradiction, suppose that σ were not the identity map. Then there exists some $a \in \mathbb{R}$ such that $\sigma(a) \neq a$. Hence, it must be the case that either $a < \sigma(a)$ or $\sigma(a) < a$. First, suppose that $a < \sigma(a)$. Since $\mathbb{Q}$ is dense in $\mathbb{R}$, there exists an element $p \in \mathbb{Q}$ such that $a < p < \sigma(a)$. Since σ is the identity on $\mathbb{Q}$ and since σ preserves order, this gives

$$\sigma(a) < \sigma(p) = p < \sigma(a)$$

which is clearly a contradiction. Secondly, suppose that $\sigma(a) < a$. Since $\mathbb{Q}$ is dense in $\mathbb{R}$, there exists an element $q \in \mathbb{Q}$ such that $\sigma(a) < q < a$. Since σ is the identity on $\mathbb{Q}$ and since σ preserves order, this gives

$$\sigma(a) < q = \sigma(q) < \sigma(a)$$

which is clearly a contradiction. In any case, we obtain a contradiction so that σ is the identity map. This shows that $\mathrm{Gal}(\mathbb{R}/\mathbb{Q})$ is the identity group. $\square$

Problem 4. *What is the Galois group of* $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$ *over* $\mathbb{Q}$*?*

Proof. Let $G = \mathrm{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})/\mathbb{Q})$. First, note that $\sqrt{2}, \sqrt{3}$, and $\sqrt{5}$ are roots of the polynomials $x^2 - 2, x^2 - 3$, and $x^2 - 5$, respectively, in $\mathbb{Q}[x]$. Therefore, we have that

$$[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2 \quad [\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})] \leq 2 \quad [\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}) : \mathbb{Q}(\sqrt{2}, \sqrt{3})] \leq 2$$

We claim that $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$. For the sake of contradiction, suppose that $\sqrt{3} \in \mathbb{Q}(\sqrt{2})$. Then there are $a, b \in \mathbb{Q}$ such that $\sqrt{3} = a + b\sqrt{2}$. In particular, since $a \in \mathbb{Q}$, we must have $b \neq 0$. This equality gives

$$a^2 = (\sqrt{3} - b\sqrt{2})^2 = (3 + 2b^2) - 2b\sqrt{6}$$

so that

$$-2b\sqrt{6} = a^2 - 2b^2 - 3 \in \mathbb{Q}$$

which is a contradiction since $b \neq 0$. Thus, we see $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$. In particular, this gives

$$[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})] = 2$$

We claim that $\sqrt{5} \notin \mathbb{Q}(\sqrt{2}, \sqrt{3})$. For the sake of contradiction, suppose that $\sqrt{5} \in \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Then there are $a, b, c \in \mathbb{Q}$ such that $\sqrt{5} = a + b\sqrt{2} + c\sqrt{3}$. In particular, since $a \in \mathbb{Q}$, we must have that at least one of b or c is nonzero. This equality gives

$$a^2 = (\sqrt{5} - b\sqrt{2} - c\sqrt{3})^2 = (5 + 2b^2 + 3c^2) + 2bc\sqrt{6} - 2b\sqrt{10} - 2c\sqrt{15}$$

so that

$$2bc\sqrt{6} - 2b\sqrt{10} - 2c\sqrt{15} = a^2 - 2b^2 - 3c^2 - 5 \in \mathbb{Q}$$

which is a contradiction since at least one of b or c is nonzero. Thus, we see $\sqrt{5} \notin \mathbb{Q}(\sqrt{2}, \sqrt{3})$. In particular, this gives

$$[\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}) : \mathbb{Q}(\sqrt{2}, \sqrt{3})] = 2$$

Combining the above results, we now obtain

$$[\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}) : \mathbb{Q}(\sqrt{2}, \sqrt{3})][\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 8$$

Next, notice that $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$ is a splitting field for the polynomial

$$(x^2 - 2)(x^3 - 3)(x^2 - 5) \in \mathbb{Q}[x]$$

Since $\mathrm{char}(\mathbb{Q}) = 0$, it now follows that $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})/\mathbb{Q}$ is a finite Galois extension. In particular, combining this observation with the above result, we conclude that

$$|G| = [\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}) : \mathbb{Q}] = 8$$

so that $|G| = 8$.

Finally, let $\sigma \in G$ be a nonidentity element and note that σ is completely determined by the images of $\sqrt{2}, \sqrt{3}$, and $\sqrt{5}$. Now, since $x^2 - 2 \in \mathbb{Q}[x]$ has roots $\sqrt{2}$ and $-\sqrt{2}$ and since $\sigma \in G$, it follows that $\sigma(\sqrt{2}) \in \{\sqrt{2}, -\sqrt{2}\}$. By exactly the same reasoning, we have that $\sigma(\sqrt{3}) \in \{\sqrt{3}, -\sqrt{3}\}$ and $\sigma(\sqrt{5}) \in \{\sqrt{5}, -\sqrt{5}\}$. Hence, if $a \in \{\sqrt{2}, \sqrt{3}, \sqrt{5}\}$ then we must have

$$\sigma^2(a) = \sigma(\sigma(a)) = a$$

In particular, this shows that σ^2 fixes $\sqrt{2}, \sqrt{3}$, and $\sqrt{5}$ and so σ^2 fixes $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$ by the above observation. Thus, we obtain that σ^2 is the identity map on $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$ so that $|\sigma| = 2$. This argument shows that every nonidentity element of G is of order 2. Since $|G| = 8$, we obtain $G \simeq \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$. This completes the proof. $\square$

Problem 5. (a): *If* $0 \leq d \in \mathbb{Q}$*, then* $\mathbb{Q}(\sqrt{d})$ *is Galois over* $\mathbb{Q}$*.*
(b): $\mathbb{C}$ *is Galois over* $\mathbb{R}$*.*

Proof. (a): Let $G = \mathrm{Gal}(\mathbb{Q}(\sqrt{d}/\mathbb{Q})$. First, suppose that $\sqrt{d} \in \mathbb{Q}$. In this case, we obtain $\mathbb{Q}(\sqrt{d}) = \mathbb{Q}$ so that G is trivial. Hence, in this case, we see that $\mathbb{Q}(\sqrt{d})^G = \mathbb{Q}$ so that $\mathbb{Q}(\sqrt{d})$ is Galois over $\mathbb{Q}$.

Now, suppose that $\sqrt{d} \notin \mathbb{Q}$. Note that $x^2 - d$ is irreducible over $\mathbb{Q}$ in this case since $\sqrt{d} \notin \mathbb{Q}$. Furthermore, we have $(\sqrt{d})^2 - d = d - d = 0$ so that $\sqrt{d}$ is a root of $x^2 - d$. Hence, since $x^2 - d \in \mathbb{Q}[x]$ is a monic, irreducible polynomial that has $\sqrt{d}$ as a root, it follows that $x^2 - d$ is the minimum polynomial for $\sqrt{d}$ over $\mathbb{Q}$. This gives

$$[\mathbb{Q}(\sqrt{d}) : \mathbb{Q}] = \deg(x^2 - d) = 2$$

so that

$$|G| \leq [\mathbb{Q}(\sqrt{d}) : \mathbb{Q}] = 2$$

Since $x^2 - d$ is irreducible over $\mathbb{Q}$ and has roots $\sqrt{d}$ and $-\sqrt{d}$, we know that there exists an element $\sigma \in G$ such that $\sigma(\sqrt{d}) = -\sqrt{d}$. In particular, by combining the above results, we now have $G = \{\sigma_1, \sigma_2\}$, where σ_1 is the identity map on $\mathbb{Q}(\sqrt{d})$ and σ_2 is such that $\sigma_2(\sqrt{d}) = -\sqrt{d}$.

Finally, suppose that $a \in \mathbb{Q}(\sqrt{d})$ is fixed by every element of G. Since $a \in \mathbb{Q}(\sqrt{d})$, there are $p, q \in \mathbb{Q}$ such that $a = p + q\sqrt{d}$. Since a is fixed by every element of G, we have in particular that a is fixed by σ_2 so that

$$p + q\sqrt{d} = a = \sigma_2(a) = \sigma_2(p + q\sqrt{d}) = \sigma_2(p) + \sigma_2(q)\sigma_2(\sqrt{d}) = p + q(-\sqrt{d}) = p - q\sqrt{d}$$

so that $q = -q$. Thus, we obtain $q = 0$ so that

$$a = p + q\sqrt{d} = p \in \mathbb{Q}$$

This shows that $\mathbb{Q}(\sqrt{d})^G = \mathbb{Q}$ so that $\mathbb{Q}(\sqrt{d})$ is Galois over $\mathbb{Q}$, completing the proof. $\square$

Proof. (b): Let $G = \mathrm{Gal}(\mathbb{C}/\mathbb{R})$. First, note that $x^2 + 1$ is irreducible over $\mathbb{R}$ since $i \notin \mathbb{R}$. Furthermore, we have $(i)^2 + 1 = -1 + 1 = 0$ so that i is a root of $x^2 + 1$. Hence, since $x^2 + 1 \in \mathbb{R}[x]$ is a monic, irreducible polynomial that has i as a root, it follows that $x^2 + 1$ is the minimum polynomial for i over $\mathbb{R}$. This gives

$$[\mathbb{C} : \mathbb{R}] = 2$$

so that

$$|G| \leq |\mathbb{C} : \mathbb{R}| = 2$$

Recall that complex conjugation is an automorphism of $\mathbb{C}$ that fixes $\mathbb{R}$ so that complex conjugation is an element of G. By the above observation, we now have $G = \{\sigma_1, \sigma_2\}$, where σ_1 is the identity map on $\mathbb{C}$ and σ_2 is the complex conjugation map.

Finally, suppose that $a \in \mathbb{C}$ is fixed by every element of G. Since $a \in \mathbb{C}$, there are $p, q \in \mathbb{R}$ such that $a = p + qi$. Since a is fixed by every element of G, we have in

particular that a is fixed by σ_2 so that

$$p + qi = a = \sigma_2(a) = \sigma_2(p + qi) = \sigma_2(p) + \sigma_2(q)\sigma(i) = p + q(-i) = p - qi$$

so that $q = -q$. Thus, we obtain $q = 0$ so that

$$a = p + qi = p \in \mathbb{R}$$

This shows that $\mathbb{C}^G = \mathbb{R}$ so that $\mathbb{C}$ is Galois over $\mathbb{R}$, completing the proof. $\square$

Homework 5: Page 255 #6, 7, 8

Problem 6. *Let $f/g \in K(x)$ with $f/g \notin K$ and f, g relatively prime in $K(x)$ and consider the extension of K by $K(x)$.*

(a): *x is algebraic over $K(f/g)$ and $[K(x) : K(f/g)] = \max\{\deg(f), \deg(g)\}$.*

(b): *If $E \neq K$ is an intermediate field, then $[K(x) : E]$ is finite.*

(c): *The assignment $x \mapsto f/g$ induces a homomorphism $\sigma : K(x) \to K(x)$ such that $\phi(x)/\psi(x) \mapsto \phi(f/g)/\psi(f/g)$. σ is a K-automorphism of $K(x)$ if and only if $\max\{\deg(f), \deg(g)\} = 1$.*

(d): $\mathrm{Gal}(K(x)/K)$ *consists of all those automorphisms induced (as in (c)) by the assignment $x \mapsto (ax + b)/(cx + d)$, where $a, b, c, d \in K$ and $ad - bc \neq 0$.*

Proof. (a): First, define

$$\phi(y) = \frac{f(x)}{g(x)} g(y) - f(y)$$

Notice that $g(y), f(y) \in K[y] \subseteq K(f/g)[y]$ and that $f(x)/g(x) \in K(f/g)[y]$. This shows that $\phi(y) \in K(f/g)[y]$. Furthermore, we have

$$\phi(x) = \frac{f(x)}{g(x)} g(x) - f(x) = f(x) - f(x) = 0$$

so that $\phi(x) = 0$. For the sake of contradiction, suppose that $\phi(y) = 0$. In this case, we have that

$$0 = \frac{f(x)}{g(x)} g(y) - f(y)$$

so that

$$f(y) = \frac{f(x)}{g(x)} g(y)$$

which implies that $f(x)/g(x) \in K$. However, this contradicts the fact that $f/g \notin K$. Therefore, we have that $\phi(y) \neq 0$. We conclude that x is the root of a nonzero polynomial in $K(f/g)[y]$ so that x is algebraic over $K(f/g)$.

Now, we show that $\phi(y)$ is irreducible over $K(f/g)$. Recall that any element of $K(f/g)$ which is not in K is transcendental over K. Thus, as $f(x)/g(x) \in K(f/g)$ but $f(x)/g(x) \notin K$ by hypothesis, we see that $f(x)/g(x)$ is transcendental over K. This observation gives that we may write $z = f(x)/g(x)$ and consider z as an indeterminant. In this case, we have that

$$\phi(y) = \frac{f(x)}{g(x)} g(y) - f(y) = zg(y) - f(y) \in K(z)[y]$$

Finally, for the sake of contradiction, suppose that $\phi(y)$ were reducible in $K[z][y]$. Then as $\phi(y)$ is linear in z by the above, we can write

$$\phi(y) = (zg_0(y) - f_0(y))h(y)$$

where $g_0(y), f_0(y), h(y) \in K[y]$ and $h(y)$ is nonconstant and $g_0(y)h(y) = g(y)$ and $f_0(y)h(y) = f(y)$. But then $f(y)$ and $g(y)$ would fail to be relatively prime in $K[y]$,

which is a contradiction. Hence, we see that $\phi(y)$ is irreducible in $K[z][y]$. Since $K(z)$ is the field of fractions of $K[z]$, it now follows by Gauss' Lemma that $\phi(y)$ is irreducible in $K(z)[y] = K(f/g)[y]$. By the above, this now gives

$$[K(f/g, x) : K(f/g)] = \deg(\phi(y)) = \deg\left(\frac{f(x)}{g(x)}g(y) - f(y)\right) = \max\{\deg(f), \deg(g)\}$$

But since $f(x)/g(x) \in K(x)$, we have $K(f/g, x) = K(x)$ so that by the above equality we obtain

$$[K(x) : K(f/g)] = [K(f/g, x) : K(f/g)] = \max\{\deg(f), \deg(g)\}$$

This completes the proof. □

Proof. (b): Note that we have the tower of fields $K \subseteq E \subseteq K(x)$. Since $E \neq K$, there is an element $u \in E \subseteq K(x)$ with $u \notin K$. Therefore, we may write $u = f(x)/g(x)$ for some relatively prime polynomials $f(x), g(x) \in K[x]$.

Now, since $u \notin K$, we have that $f(x)/g(x) \notin K$. By the proof of Part (a), it follows that x is algebraic over $K(u)$. Furthermore, since $u = f(x)/g(x) \in K(x)$, we have that $K(u, x) = K(u)(x) = K(x)$. Thus, combining this observation with the fact that x is algebraic over $K(u)$, we obtain

$$[K(x) : K(u)] = [K(u, x) : K(u)] < \infty$$

Finally, since $u \in E$, we have the tower of fields $K \subseteq K(u) \subseteq E \subseteq K(x)$. By the above inequality, this observation gives

$$\infty > [K(x) : K(u)] = [K(x) : E][E : K(u)]$$

so that $[K(x) : E] < \infty$. This shows that $[K(x) : E]$ is finite, completing the proof. □

Proof. (c): First, define

$$\sigma : K(x) \to K(x) \quad \text{by} \quad \frac{\phi(x)}{\psi(x)} \mapsto \frac{\phi(f/g)}{\psi(f/g)}$$

It is clear that σ is a ring homomorphism and is the identity on K. Furthermore, we have $\phi(1) = 1$ so that σ is a field homomorphism and thus σ is a K-homomorphism. Since σ is not the zero map and since $K(x)$ is a field, it follows that σ is also injective. Therefore, we have that σ is a K-automorphism of $K(x)$ if and only if σ is surjective.

Finally, this gives that $\max\{\deg(f), \deg(g)\} = 1$ if and only if $[K(x) : K(f/g)] = 1$ (by Part (a)) if and only if $K(x) = K(f/g) = \sigma(K(x))$ if and only if σ is surjective if and only if σ is a K-automorphism of $K(x)$. This completes the proof. □

Proof. (d): Recall that the map in Part (c) is an injective K-homomorphism. Now, let $\sigma \in \mathrm{Gal}(K(x)/K)$. By Part (c), we have $\max\{\deg(f), \deg(g)\} = 1$ and so $f(x) = ax + b$ and $g(x) = cx + d$ for some $a, b, c, d \in K$. Since σ is an automorphism of $K(x)$, it follows that σ has an inverse. This implies that $ad - bc \neq 0$.

On the other hand, suppose that $\sigma : K(x) \to K(x)$ is defined by the assignment $x \mapsto (ax + b)/(cx + d)$ for some $a, b, c, d \in K$ with $ad - bc \neq 0$. By the observation

made at the beginning of this proof, it follows that σ is an injective K-homomorphism. Furthermore, we have that

$$\max\{\deg(ax+b), \deg(cx+d)\} = 1$$

By Part (c), then, we have that σ is a K-automorphism of $K(x)$ so that $\sigma \in \mathrm{Gal}(K(x)/K)$.

The above results show that $\mathrm{Gal}(K(x)/K)$ consists of the desired elements, completing the proof. $\square$

Problem 7. *Let* $\mathrm{char}(K) = 0$ *and* G *be the subset of* $\mathrm{Gal}(K(x)/K)$ *consisting of the three automorphisms induced (as in 6(c)) by* $x \mapsto x, x \mapsto 1/(1-x), x \mapsto (x-1)/x$. *Then* G *is a subgroup of* $\mathrm{Gal}(K(x)/K)$. *Determine the fixed field of* G.

Proof. Denote these three automorphisms of $K(x)$ by σ_1, σ_2, and σ_3, respectively. Simple algebra shows that

$$(\sigma_2 \circ \sigma_2)(x) = \sigma_2\left(\frac{1}{1-x}\right) = \frac{x-1}{x} = \sigma_3(x)$$

and

$$(\sigma_3 \circ \sigma_3)(x) = \sigma_3\left(\frac{x-1}{x}\right) = \frac{1}{1-x} = \sigma_2(x)$$

and

$$(\sigma_2 \circ \sigma_3)(x) = \sigma_2\left(\frac{x-1}{x}\right) = x = \sigma_1(x)$$

and

$$(\sigma_3 \circ \sigma_2)(x) = \sigma_3\left(\frac{1}{1-x}\right) = x = \sigma_1(x)$$

Since σ_1, σ_2, and σ_3 are completely determined by their images of x, the above calculations show that $\sigma_2 \circ \sigma_2 = \sigma_3$, $\sigma_3 \circ \sigma_3 = \sigma_2$, $\sigma_3 \circ \sigma_3 = \sigma_1$, and $\sigma_3 \circ \sigma_2 = \sigma_1$. In particular, the this shows that G is a group and hence G is a subgroup of $\mathrm{Gal}(K(x)/K)$.

Now, we show that $K(x)^G = \{f(x) + \sigma_2(f(x)) + \sigma_3(f(x)) : f(x) \in K(x)\}$. Towards this end, let D denote this latter set and let $g(x) \in K(x)^G$. Then we have by definition that $\sigma_2(g(x)) = g(x)$ and $\sigma_3(g(x)) = g(x)$. Since $\mathrm{char}(K) = 0$, we may define $f(x) \in K(x)$ by $f(x) = \frac{1}{3}g(x)$. Since $\frac{1}{3} \in K$, this gives by the previous observation that

$$\begin{aligned} f(x) + \sigma_2(f(x)) + \sigma_3(f(x)) &= \frac{1}{3}g(x) + \sigma_2\left(\frac{1}{3}g(x)\right) + \sigma_3\left(\frac{1}{3}g(x)\right) \\ &= \frac{1}{3}g(x) + \frac{1}{3}\sigma_2(g(x)) + \frac{1}{3}\sigma_3(g(x)) \\ &= \frac{1}{3}g(x) + \frac{1}{3}g(x) + \frac{1}{3}g(x) \\ &= g(x) \end{aligned}$$

so that $g(x) \in D$.

On the other hand, suppose that $f(x) \in K(x)$. Then by the above, we have

$$\sigma_1(f(x) + \sigma_2(f(x)) + \sigma_3(f(x))) = f(x) + \sigma_2(f(x)) + \sigma_3(f(x))$$

and

$$\begin{aligned} \sigma_2(f(x) + \sigma_2(f(x)) + \sigma_3(f(x))) &= \sigma_2(f(x)) + \sigma_2(\sigma_2(f(x))) + \sigma_2(\sigma_3(f(x))) \\ &= \sigma_2(f(x)) + \sigma_3(f(x)) + \sigma_1(f(x)) \\ &= f(x) + \sigma_2(f(x)) + \sigma_3(f(x)) \end{aligned}$$

and

$$\begin{aligned}\sigma_3(f(x)+\sigma_2(f(x))+\sigma_3(f(x))) &= \sigma_3(f(x))+\sigma_3(\sigma_2(f(x)))+\sigma_3(\sigma_3(f(x)))\\ &= \sigma_3(f(x))+\sigma_1(f(x))+\sigma_2(f(x))\\ &= f(x)+\sigma_2(f(x))+\sigma_3(f(x))\end{aligned}$$

so that $f(x)+\sigma_2(f(x))+\sigma_3(f(x)) \in K(x)^G$. Since $f(x) \in K(x)$ was arbitrary, the above shows that $f(x)+\sigma_2(f(x))+\sigma_3(f(x)) \in K(x)^G$ for all $f(x) \in K(x)$.

The above calculations prove that $K(x)^G = D$. This completes the proof. $\square$

Problem 8. *Assume* $\mathrm{char}(K) = 0$ *and let* G *be the subgroup of* $\mathrm{Gal}(K(x)/K)$ *that is generated by the automorphism induced by* $x \mapsto x+1$*. Then* G *is an infinite cyclic group. Determine the fixed field* E *of* G*. What is* $[K(x) : E]$*?*

Proof. First, define

$$\sigma : K(x) \to K(x) \quad \text{by} \quad x \mapsto x+1$$

Notice that

$$\sigma^2(x) = \sigma(\sigma(x)) = \sigma(x+1) = \sigma(x) + \sigma(1) = (x+1)+1 = x+2$$

and

$$\sigma^3(x) = \sigma(\sigma^2(x)) = \sigma(x+2) = \sigma(x) + \sigma(2) = (x+1)+2 = x+3$$

and

$$\sigma^4(x) = \sigma(\sigma^3(x)) = \sigma(x+3) = \sigma(x) + \sigma(3) = (x+1)+3 = x+4$$

Inductively, we obtain $\sigma^n(x) = x+n$ for all positive integers n. For the sake of contradiction, suppose that $|\sigma| = m < \infty$. Then by the above, this gives

$$x = \sigma^m(x) = x+m$$

so that $m \cdot 1 = m = 0$. However, this contradicts the fact that $\mathrm{char}(K) = 0$. Hence, we have $|\sigma| = \infty$ so that

$$|G| = |\langle \sigma \rangle| = |\sigma| = \infty$$

Hence, we have that G is an infinite cyclic group.

Now, as $G = \langle \sigma \rangle$, we can write

$$E = \{f(x) \in K(x) : \sigma^n(f(x)) = f(x), n \in \{0, 1, 2 \dots\}\}$$

First, suppose that $f(x) \in K[x]$ and $f(x) = f(x+1)$. We claim that such a polynomial $f(x)$ must be constant. For the sake of contradiction, suppose that $f(x)$ were not constant. Then we have $\deg(f(x)) = n \geq 1$. Write

$$f(x) = \sum_{i=0}^{n} a_i x^i$$

where $a_i \in K$ for $i \in \{0, \dots, n\}$. Since $f(x) = f(x+1)$, we have

$$\sum_{i=0}^{n} a_i x^i = f(x) = f(x+1) = \sum_{i=0}^{n} a_i (x+1)^i$$

Note that the coefficient of x^{n-1} on the left-hand side of the above equality is a_{n-1}. On the other hand, notice that

$$(x+1)^{n-1} = \sum_{i=0}^{n-1} \binom{n-1}{i} x^i$$

and

$$(x+1)^n = \sum_{i=0}^{n} \binom{n}{i} x^i$$

so that the coefficient of x^{n-1} on the right-hand side of the above equality is

$$a_{n-1}\binom{n-1}{n-1} + a_n\binom{n}{n-1} = a_{n-1} \cdot 1 + a_n \cdot n = na_n + a_{n-1}$$

Hence, combining the above results, we obtain

$$na_n + a_{n-1} = a_{n-1}$$

so that $na_n = 0$. But this is a contradiction as $n \geq 1$ and $\text{char}(K) = 0$. Therefore, such a polynomial $f(x)$ must be a constant polynomial.

Now, let $h(x) \in E$. Since $h(x) \in K(x)$, there are monic, relatively prime polynomials $f(x), g(x) \in K[x]$ with $g(x) \neq 0$ such that $h(x) = f(x)/g(x)$. Since $h(x) \in K(x)^G$, we have in particular that

$$h(x+1) = \sigma(h(x)) = h(x)$$

so that $h(x) = h(x+1)$. That is, we obtain

$$\frac{f(x)}{g(x)} = h(x) = h(x+1) = \frac{f(x+1)}{g(x+1)}$$

By the nature of $f(x)$ and $g(x)$, the above equality implies that $f(x) = f(x+1)$ and $g(x) = g(x+1)$. By the above result, it follows that $f(x)$ and $g(x)$ are constant polynomials. That is, we have $f(x), g(x) \in K$ so that $h(x) = f(x)/g(x) \in K$. As $h(x) \in E$ was arbitrary, this proves that $E \subseteq K$ and since we clearly also have $K \subseteq E$, we obtain that $E = K$.

Finally, recall that any element of $K(x)$ that is not in K is transcendental over K. Thus, as $x \in K(x)$ but $x \notin K$ and by the above result, we now have

$$[K(x) : E] = [K(x) : K] = \infty$$

This completes the proof. $\square$

Homework 6: Page 255 #12, 14

Problem 12. *If E is an intermediate field of the extension such that E is Galois over K, F is Galois over E, and every $\sigma \in \mathrm{Gal}(E/K)$ is extendible to F, then F is Galois over K.*

Proof. First, note that we have the tower of fields $K \subseteq E \subseteq F$. Let $u \in F - K$. In order to show that F is Galois over K, it suffices to show that there is some $\tau \in \mathrm{Gal}(F/K)$ such that $\tau(u) \neq u$.

If $u \in E$, then $u \in E - K$. Since E is Galois over K, there exists some $\sigma \in \mathrm{Gal}(E/K)$ such that $\sigma(u) \neq u$. By hypothesis, we have that σ can be extended to an element $\tau \in \mathrm{Gal}(F/K)$. Since τ agrees with σ on E and since $u \in E$, we have

$$\tau(u) = \sigma(u) \neq u$$

This proves the result in the case when $u \in E$.

If $u \notin E$, then $u \in F - E$. Since F is Galois over E, there is some $\tau \in \mathrm{Gal}(F/E)$ such that $\tau(u) \neq u$. But since $K \subseteq E \subseteq F$, we have $\mathrm{Gal}(F/E) \subseteq \mathrm{Gal}(F/K)$ so that $\tau \in \mathrm{Gal}(F/K)$. This proves the result in the case when $u \notin E$.

The above results show that if $u \in F - K$ then there is some $\tau \in \mathrm{Gal}(F/K)$ so that $\tau(u) \neq u$. Thus, we have that F is Galois over K, completing the proof. $\square$

Problem 14. *Let F be a finite dimensional Galois extension of K and let L and M be two intermediate fields.*

(a): $\mathrm{Gal}(F/LM) = \mathrm{Gal}(F/L) \cap \mathrm{Gal}(F/M)$.

(b): $\mathrm{Gal}(F/L \cap M) = \mathrm{Gal}(F/L) \vee \mathrm{Gal}(F/M)$.

(c): *What conclusion can be drawn if* $\mathrm{Gal}(F/L) \cap \mathrm{Gal}(F/M) = 1$ *?*

Note: Before we begin, we note that LM is the smallest field containing L and M and that $\mathrm{Gal}(F/L) \vee \mathrm{Gal}(F/M)$ is the smallest group containing $\mathrm{Gal}(F/L)$ and $\mathrm{Gal}(F/M)$. Furthermore, since F/K is a finite Galois extension, we observe that the Fundamental Theorem of Galois Theory (FTGT) applies to the extension F/K.

Proof. (a): First, note that $L, M \subseteq LM$ so that

$$\mathrm{Gal}(F/LM) \subseteq \mathrm{Gal}(F/L), \mathrm{Gal}(F/M)$$

and hence, we obtain

$$\mathrm{Gal}(F/LM) \subseteq \mathrm{Gal}(F/L) \cap \mathrm{Gal}(F/M)$$

Second, note that we clearly have

$$\mathrm{Gal}(F/L) \cap \mathrm{Gal}(F/M) \subseteq \mathrm{Gal}(F/L), \mathrm{Gal}(F/M)$$

so that, by FTGT, we obtain

$$F^{\mathrm{Gal}(F/L)}, F^{\mathrm{Gal}(F/M)} \subseteq F^{\mathrm{Gal}(F/L) \cap \mathrm{Gal}(F/M)}$$

Furthermore, by FTGT, we have $L = F^{\mathrm{Gal}(F/L)}$ and $M = F^{\mathrm{Gal}(F/M)}$ so that the above inclusion gives

$$L, M \subseteq F^{\mathrm{Gal}(F/L) \cap \mathrm{Gal}(F/M)}$$

Thus, we see that $F^{\mathrm{Gal}(F/L) \cap \mathrm{Gal}(F/M)}$ is a field containing L and M. It now follows that

$$LM \subseteq F^{\mathrm{Gal}(F/L) \cap \mathrm{Gal}(F/M)}$$

Thus, we obtain

$$\mathrm{Gal}(F/L) \cap \mathrm{Gal}(F/M) = \mathrm{Gal}\left(F/F^{\mathrm{Gal}(F/L) \cap \mathrm{Gal}(F/M)}\right) \subseteq \mathrm{Gal}(F/LM)$$

The above results show that $\mathrm{Gal}(F/LM) = \mathrm{Gal}(F/L) \cap \mathrm{Gal}(F/M)$. This completes the proof. $\square$

Proof. (b): First, notice that $L \cap M \subseteq L, M$. By FTGT, this gives

$$\mathrm{Gal}(F/L), \mathrm{Gal}(F/M) \subseteq \mathrm{Gal}(F/L \cap M)$$

so that $\mathrm{Gal}(F/L \cap M)$ is a group containing $\mathrm{Gal}(F/L)$ and $\mathrm{Gal}(F/M)$. Thus, we have

$$\mathrm{Gal}(F/L) \vee \mathrm{Gal}(F/M) \subseteq \mathrm{Gal}(F/L \cap M)$$

Second, by FTGT, we have $F^{\mathrm{Gal}(F/L \cap M)} = L \cap M$. Furthermore, we have

$$\mathrm{Gal}(F/L), \mathrm{Gal}(F/M) \subseteq \mathrm{Gal}(F/L) \vee \mathrm{Gal}(F/M)$$

so that, by FTGT, we obtain

$$F^{\mathrm{Gal}(F/L) \vee \mathrm{Gal}(F/M)} \subseteq F^{\mathrm{Gal}(F/L)}, F^{\mathrm{Gal}(F/M)}$$

By FTGT, we have $F^{\mathrm{Gal}(F/L)} = L$ and $F^{\mathrm{Gal}(F/M)} = M$ so that the above inclusion gives

$$F^{\mathrm{Gal}(F/L)\vee\mathrm{Gal}(F/M)} \subseteq L, M$$

Hence, by FTGT, this gives

$$F^{\mathrm{Gal}(F/L)\vee\mathrm{Gal}(F/M)} \subseteq L \cap M = F^{\mathrm{Gal}(F/L\cap M)}$$

By FTGT, the above inclusion gives

$$\mathrm{Gal}(F/L \cap M) \subseteq \mathrm{Gal}(F/L) \vee \mathrm{Gal}(F/M)$$

The above results show that $\mathrm{Gal}(F/L \cap M) = \mathrm{Gal}(F/L) \vee \mathrm{Gal}(F/M)$. This completes the proof. □

Proof. (c): Notice that by Part (a) and by the hypothesis of this part of the problem that we have

$$\mathrm{Gal}(F/LM) = \mathrm{Gal}(F/L) \cap \mathrm{Gal}(F/M) = 1$$

Thus, we obtain by this observation and by FTGT that

$$LM = F^{\mathrm{Gal}(F/LM)} = F^1 = F$$

so that $LM = F$. This establishes a desirable result. □

Homework 7: Page 267 #5, 8, 9

Problem 5. *If $f \in K[x]$ has degree n and F is a splitting field of f over K, then $[F : K]$ divides $n!$.*

Proof. Suppose this is false. Among all counterexamples, choose one where $\deg(f(x)) = n$ is as small as possible. If $n = 0$, then $[F : K] = 1$ which divides $1 = 0! = n!$. If $n = 1$, then $[F : K] = 1$ which divides $1 = 1! = n!$. Therefore, if $n \in \{0, 1\}$ we do not have a counterexample. By this observation, we must have that $\deg(f(x)) = n \geq 2$.

First, suppose that $f(x)$ is irreducible over K and let $u \in F$ be a root of $f(x)$. Since $f(x)$ is irreducible, we have

$$[K(u) : K] = \deg(f(x)) = n$$

Note that since u is a root of $f(x)$ that we can write $f(x) = (x - u)g(x)$ for some polynomial $g(x) \in K(u)[x]$ with $\deg(g(x)) = n - 1$. Since F is a splitting field for $f(x)$ over K, it follows that F is a splitting field for $g(x)$ over $K(u)$. Hence, by the inductive hypothesis, we see that $[F : K(u)]$ divides $(n - 1)!$. Therefore, by the above, we obtain

$$[F : K] = [F : K(u)][K(u) : K] = [F : K(u)] \cdot n$$

By the above equality and the fact that $[F : K(u)]$ divides $(n - 1)!$, it now follows that $[F : K]$ divides $n \cdot (n - 1)! = n!$. Hence, we do not have a counterexample if $f(x)$ is irreducible over K. By this observation, we must have that $f(x)$ is reducible over K.

Since $f(x)$ is reducible over K, we may write $f(x) = g(x)h(x)$ for some $g(x), h(x) \in K[x]$ with $1 \leq \deg(g(x)), \deg(h(x)) \leq n - 1$. Let $m = \deg(g(x))$ and $k = \deg(h(x))$. Then we have

$$n = \deg(f(x)) = \deg(g(x)h(x)) = \deg(g(x)) + \deg(h(x)) = m + k$$

Now, let E be a splitting field for $g(x)$ over K. Since F is a splitting field for $f(x)$ over K and since $f(x) = g(x)h(x)$, it follows that F is a splitting field for $h(x)$ over E. By the inductive hypothesis, then, we have that $[E : K]$ divides $m!$ and $[F : E]$ divides $k!$. Finally, since $n = m + k$ we have that $k = n - m$ so that

$$\frac{n!}{m!k!} = \frac{n!}{m!(n - m)!} = \binom{n}{m} \in \mathbb{Z}$$

Hence, we see that $m!k!$ divides $n!$. But since $[E : K]$ divides $m!$ and $[F : E]$ divides $k!$, we have that

$$[F : K] = [F : E][E : K]$$

divides $m!k!$ which divides $n!$ by the above result. Hence, we obtain that $[F : K]$ divides $n!$. This is the final contradiction, completing the proof. $\square$

Problem 8. *No finite field is algebraically closed.*

Proof. Let K be a finite field and write $K = \{a_1, \ldots, a_n\}$. Define

$$p(x) = 1 + \prod_{i=1}^{n} (x - a_i) \in K[x]$$

In particular, we have that $p(x)$ is nonconstant. Now, let $i \in \{1, \ldots, n\}$ and note that

$$p(a_i) = 1 + 0 = 1 \neq 0$$

so that a_i is not a root of $p(x)$. Since $i \in \{1, \ldots, n\}$ was arbitrary, this shows that $p(x)$ has no roots in $K = \{a_1, \ldots, a_n\}$. Hence, it cannot be the case that K is algebraically closed, as we have exhibited a nonconstant polynomial in $K[x]$ that has no root in K. This completes the proof. $\square$

Problem 9. *F is an algebraic closure of K if and only if F is algebraic over K and for every algebraic extension E of K there exists a K-monomorphism $E \to F$.*

Proof. For the first direction, suppose that F is an algebraic closure of K. By definition, we have that F is algebraic over K. Now, let E be an algebraic extension of K. If E is algebraically closed, then E is an algebraic closure of K. But since any two algebraic closures of K are K-isomorphic, it follows that there exists a K-monomorphism $E \to F$.

Now, assume that E is not algebraically closed. Let M be an algebraic closure of E and note that we have the tower of fields $K \subseteq E \subseteq M$. Since M is an algebraic closure of E, it follows that M/E is an algebraic extension. Since E/K is also an algebraic extension, it now follows that M/K is an algebraic extension. Since M is algebraically closed as M is an algebraic closure of E, it now follows that M is an algebraic closure of K. But since any two algebraic closures of K are K-isomorphic, it follows that there exists a K-monomorphism $M \to F$. By restricting this K-monomorphism to E, we see that there exists a K-monomorphism $E \to F$. This completes the proof of the first direction.

We now prove the second direction. Since F is algebraic over K, it remains to prove that F is algebraically closed in order to show that F is an algebraic closure of K. Towards this end, let M be an algebraic closure of F. Since M/F is an algebraic extension and since F/K is an algebraic extension, it now follows that M/K is an algebraic extension. By hypothesis, then, there exists a K-monomorphism $\sigma : M \to F$.

Now, since M/K is an algebraic extension and since M is algebraically closed, it follows that M is an algebraic closure of K so that every polynomial in $K[x]$ splits over M. Let $f(x) \in K[x]$ be any polynomial in $K[x]$. By the previous observation, we have that $f(x)$ splits over M. Thus, since $\sigma : M \to F$ is a monomorphism, it follows that $\sigma(f(x))$ splits over F. Furthermore, since σ is a K-homomorphism and since $f(x) \in K[x]$, we have that $\sigma(f(x)) = f(x)$. Combining the previous two observations, we have that $f(x)$ splits over F. Since $f(x) \in K[x]$ was an arbitrary polynomial and since F/K is an algebraic extension, it now follows that F is algebraically closed so that F is an algebraic closure of K. This completes the proof of the second direction. $\square$

Homework 8: Page 267 #12, 13, 14

Problem 12. *Let E be an intermediate field.*

(a): *If $u \in F$ is separable over K, then u is separable over E.*

(b): *If F is separable over K, then F is separable over E and E is separable over K.*

Proof. (a): Let $m_{K,u}(x)$ denote the minimum polynomial of u over K. Since $u \in F$ is separable over K, it follows that $m_{K,u}(x)$ is separable. Now, let $m_{E,u}(x)$ denote the minimum polynomial of u over E. Then since $K \subseteq E$, we have $m_{K,u}(x) \in K[x] \subseteq E[x]$. Furthermore, we clearly have $m_{K,u}(u) = 0$. The previous two observations imply that $m_{E,u}(x)$ divides $m_{K,u}(x)$. Hence, since $m_{K,u}(x)$ is separable, it now follows that $m_{E,u}(x)$ is separable. By definition, then, we have that u is separable over E. This completes the proof. $\square$

Proof. (b): Note that we have the tower of fields $K \subseteq E \subseteq F$. Now, let $u \in F$. Since F is separable over K, it follows that u is separable over K. By Part (a), this gives that u is separable over E. Since $u \in F$ was arbitrary, this shows that F is separable over E.

Finally, let $u \in E \subseteq F$. Since $u \in F$ and F is separable over K, it follows that u is separable over K. Since $u \in E$ was arbitrary, this shows that E is separable over K. $\square$

Problem 13. *Suppose $[F : K]$ is finite. Then the following conditions are equivalent:*

(i): *F is Galois over K.*

(ii): *F is separable over K and a splitting field of a polynomial $f \in K[x]$.*

(iii): *F is a splitting field over K of a polynomial $f \in K[x]$ whose irreducible factors are separable.*

Proof. (i $\Rightarrow$ ii): Since $[F : K]$ is finite, it follows that F/K is an algebraic extension. Thus, since F is Galois over K, it follows that F/K is an algebraic Galois extension so that F is separable over K and F is a splitting field over K of a set of polynomials $\{f_1(x), \ldots, f_n(x)\} \subseteq K[x]$. Define $f(x) = \prod_{i=1}^{n} f_i(x) \in K[x]$. Since $f_1(x), \ldots, f_n(x)$ split over F, it follows by the definition of $f(x)$ that $f(x)$ splits over F. Finally, we know that F is equal to K extended by the roots of $f_1(x), \ldots, f_n(x)$. However, again by the definition of $f(x)$, we have that the set of roots of $f(x)$ is equal to the set of roots of $f_1(x), \ldots, f_n(x)$. Therefore, we see that F is equal to K extended by the roots of $f(x)$. Combining the previous results, we have that F is a splitting field for the polynomial $f(x) \in K[x]$.

(i $\Rightarrow$ iii): By the first proof, we know that F is separable over K and a splitting field of a polynomial $f(x) \in K[x]$. Let $u_1, \ldots, u_n \in F$ be the roots of $f(x)$. By definition, we have that $F = K(u_1, \ldots, u_n)$. Now, let $f_1(x), \ldots, f_n(x) \in K[x]$ be the minimum polynomials of $u_1, \ldots, u_n$ over K, respectively. Since F is separable over K, it follows that $f_1(x), \ldots, f_n(x)$ are separable. Furthermore, since $f(u_1) = \cdots = f(u_n) = 0$, it follows that $f_1(x), \ldots, f_n(x)$ divide $f(x)$. Hence, since $f(x)$ splits over F, so must $f_1(x), \ldots, f_n(x)$. Now, define $g(x) = \prod_{i=1}^{n} f_i(x) \in K[x]$. In particular, note that the irreducible factors of $g(x)$ are $f_1(x), \ldots, f_n(x)$ and since $f_1(x), \ldots, f_n(x)$ are separable, it follows that $g(x)$ is a polynomial in $K[x]$ whose irreducible factors are separable. Furthermore, since $f_1(x), \ldots, f_n(x)$ split over F, it follows that $g(x)$ splits over F. Finally, note that the roots of $g(x)$ are the roots of $f_1(x), \ldots, f_n(x)$ and among these roots are $u_1, \ldots, u_n$. Combining the previous results, we see that $F = K(u_1, \ldots, u_n)$ is a splitting field of $g(x)$ over K.

(ii $\Rightarrow$ i): Note that F is a separable extension of K and that F is a splitting field of the set of polynomials $\{f(x)\}$ in $K[x]$. Thus, we have that F is Galois over K.

(iii $\Rightarrow$ ii): Clearly, it remains to prove that F is separable over K. Let $f(x) \in K[x]$ be a polynomial in $K[x]$ as in the hypothesis and let $f_1(x), \ldots, f_n(x) \in K[x]$ be the separable, irreducible factors of $f(x)$. Note that, by definition, F is equal to K extended by the roots of $f(x)$. Since the set of roots of $f(x)$ is equal to the set of roots of $f_1(x), \ldots, f_n(x)$, it now follows that F is a splitting field for the set of separable polynomials $\{f_1(x), \ldots, f_n(x)\} \subseteq K[x]$. It now follows that F is separable over K. $\square$

Problem 14. *If L and M are intermediate fields such that L is a finite dimensional Galois extension of K, then LM is finite dimensional and Galois over M and* $\mathrm{Gal}(LM/M) \simeq \mathrm{Gal}(L/L \cap M)$.

Proof. First, note that we have the tower of fields $K \subseteq L, M \subseteq F$. In order to prove that LM/M is a finite Galois extension, it suffices to show that LM/M is a finite extension and that LM is a splitting field over M of a separable polynomial in $M[x]$.

Note that since L/K is a finite Galois extension that there is a separable polynomial $f(x) \in K[x]$ with roots $u_1, \ldots, u_n \in L$ such that $L = K(u_1, \ldots, u_n)$. This gives that $L, M \subseteq M(u_1, \ldots, u_n)$. Since $M(u_1, \ldots, u_n)$ is a field containing L and M, it follows that $LM \subseteq M(u_1, \ldots, u_n)$. On the other hand, since $u_1, \ldots, u_n \in L$ we have that $M(u_1, \ldots, u_n) \subseteq LM$. The previous results show that $LM = M(u_1, \ldots, u_n)$ so that

$$[LM : M] = [M(u_1, \ldots, u_n) : M] < \infty$$

so that LM is finite dimensional over M. Furthermore, since $LM = M(u_1, \ldots, u_n)$ and $f(x) \in K[x] \subseteq M[x]$, it follows that LM is a splitting field for $f(x)$ over M since $u_1, \ldots, u_n$ are the roots of $f(x)$. Since $f(x)$ is separable, this shows that LM is Galois over M. In conclusion, we have that LM is finite dimensional and Galois over M.

Now, let $\sigma \in \mathrm{Gal}(LM/M)$. Since $L \subseteq LM$, we can restrict σ to L and denote this restriction as $\mathrm{Res}(\sigma) : L \to LM$. As LM/M is finite Galois, we have that LM/M is normal. Furthermore, since $L \subseteq LM$ and $\mathrm{Res}(\sigma)$ is an M-homomorphism, we have that $\mathrm{Res}(\sigma)$ is really a map $\mathrm{Res}(\sigma) : L \to L$. As σ fixes M and $K \subseteq M$, we have that σ fixes K so that by the previous result we obtain $\mathrm{Res}(\sigma) \in \mathrm{Gal}(L/K)$. Therefore, we have a map $\mathrm{Res} : \mathrm{Gal}(LM/M) \to \mathrm{Gal}(L/K)$, and it is clear that Res is a group homomorphism.

Now, recall that $LM = M(u_1, \ldots, u_n)$ so that $\sigma \in \mathrm{Gal}(LM/M)$ is completely determined by the images of $u_1, \ldots, u_n$. However, recall that $u_1, \ldots, u_n \in L$. These observations give that if $\mathrm{Res}(\sigma_1) = \mathrm{Res}(\sigma_2)$ for some $\sigma_1, \sigma_2 \in \mathrm{Gal}(LM/M)$, then we have $\sigma_1 = \sigma_2$. In particular, this shows that Res is an injection.

Finally, we prove that the image of Res is $\mathrm{Gal}(L/L \cap M)$. Towards this end, note that if $a \in L$ that a is fixed by all $\sigma \in \mathrm{Res}(\mathrm{Gal}(LM/M))$ if and only if a is fixed by all $\sigma \in \mathrm{Gal}(LM/M)$ if and only if $a \in M$ (since LM/M is Galois) if and only if $a \in L \cap M$. This proves that

$$L^{\mathrm{Res}(\mathrm{Gal}(LM/M))} = L \cap M$$

Thus, since $\mathrm{Res}(\mathrm{Gal}(LM/M)) \subseteq \mathrm{Gal}(L/K)$ and since L/K is a finite Galois extension, we have by FTGT and the above that

$$\mathrm{Res}(\mathrm{Gal}(LM/M)) = \mathrm{Gal}\left(L/L^{\mathrm{Res}(\mathrm{Gal}(LM/M))}\right) = \mathrm{Gal}(L/L \cap M)$$

Therefore, combining the above results, we have $\mathrm{Res} : \mathrm{Gal}(LM/M) \to \mathrm{Gal}(L/L \cap M)$ is an isomorphism so that $\mathrm{Gal}(LM/M) \simeq \mathrm{Gal}(L/L \cap M)$, completing the proof. $\square$

Homework 9: Page 276 #1, 2, 3

Problem 1. *Suppose $f \in K[x]$ splits in F as $f = (x-u_1)^{n_1} \cdots (x-u_k)^{n_k}$ (u_i distinct; $n_i \geq 1$). Let $v_0, \ldots, v_k$ be the coefficients of the polynomial $g = (x-u_1)\cdots(x-u_k)$ and let $E = K(v_0, \ldots, v_k)$.*

(a): *F is a splitting field of g over E.*

(b): *F is Galois over E.*

(c): $\mathrm{Gal}(F/E) = \mathrm{Gal}(F/K)$.

Note: We have the tower of fields $K \subseteq E \subseteq F$. By the definition of $f(x)$ and $g(x)$, we have that the roots of $f(x)$ and $g(x)$ are $u_1, \ldots, u_k \in F$. Since F is a splitting field for $f(x)$ over K, we have that $F = K(u_1, \ldots, u_k)$. We will use these observations below.

Proof. (a): We will first show that $E(u_1, \ldots, u_k) = F$. Note that since $E \subseteq F$ and since $u_1, \ldots, u_k \in F$ we have that

$$E(u_1, \ldots, u_k) \subseteq F(u_1, \ldots, u_k) = F$$

so that $E(u_1, \ldots, u_k) \subseteq F$. On the other hand, notice that

$$E(u_1, \ldots, u_k) = K(v_0, \ldots, v_k)(u_1, \ldots, u_k) = K(v_0, \ldots, v_k, u_1, \ldots, u_k) \supseteq K(u_1, \ldots, u_k) = F$$

so that $F \subseteq E(u_1, \ldots, u_k)$. The above results show that $E(u_1, \ldots, u_k) = F$.

Finally, note that since $g(x) \in E[x]$ and since $g(x)$ splits over F by the definition of $g(x)$, it now follows that F is a splitting field for $g(x)$ over E since the roots of $g(x)$ are $u_1, \ldots, u_k$. This completes the proof. $\square$

Proof. (b): Note that $g(x) \in E[x]$ is a separable polynomial by the definition of $g(x)$. Furthermore, by Part (a), we have that F is a splitting field for $g(x)$ over E. It now follows that F is Galois over E, completing the proof. $\square$

Proof. (c): First, note that $K \subseteq K(v_0, \ldots, v_k) = E$. Thus, we have $\mathrm{Gal}(F/E) \subseteq \mathrm{Gal}(F/K)$. On the other hand, let $\sigma \in \mathrm{Gal}(F/K)$. Note that we have

$$g(x) = (x-u_1)\cdots(x-u_k) = \prod_{i=1}^{k}(x-u_i)$$

Since F is a splitting field for $f(x)$ over K and since the roots of $f(x)$ are $u_1, \ldots, u_k$, it follows that $\sigma \in \mathrm{Gal}(F/K)$ permutes $u_1, \ldots, u_k$. Therefore, referring to the above equality, we see that $\sigma(g(x)) = g(x)$.

Finally, recall that $v_0, \ldots, v_k$ are the coefficients of $g(x)$ so that we may write

$$g(x) = \sum_{i=0}^{k} v_i x^i$$

Therefore, by the above result and this representation of $g(x)$, we obtain

$$\sum_{i=0}^{k} v_i x^i = g(x) = \sigma(g(x)) = \sigma\left(\sum_{i=0}^{k} v_i x^i\right) = \sum_{i=0}^{k} \sigma(v_i) x^i$$

By the above equality, we obtain $\sigma(v_i) = v_i$ for all $i \in \{0, \ldots, k\}$.

Finally, since $\sigma \in \mathrm{Gal}(F/K)$ we know that σ fixes K. Combining this observation with the previous result, we see that σ fixes $K(v_0, \ldots, v_k) = E$. Therefore, we have that $\sigma \in \mathrm{Gal}(F/E)$. Since $\sigma \in \mathrm{Gal}(F/K)$ was arbitrary, this gives that $\mathrm{Gal}(F/K) \subseteq \mathrm{Gal}(F/E)$. We conclude that $\mathrm{Gal}(F/E) = \mathrm{Gal}(F/K)$, completing the proof. $\square$

Problem 2. *Suppose K is a subfield of $\mathbb{R}$ (so that F may be taken to be a subfield of $\mathbb{C}$) and that f is irreducible of degree 3. Let D be the discriminant of f. Then*

(a): *$D > 0$ if and only if f has three real roots.*

(b): *$D < 0$ if and only if f has precisely one real root.*

Note: Since $f(x)$ is of degree 3, it follows by elementary Calculus that $f(x)$ has at least one real root. Denote this real root of $f(x)$ by u_1.

Proof. (a): For the first direction, suppose that $D > 0$. For the sake of contradiction, suppose that $f(x)$ did not have three real roots. Let $u_2, u_3 \in \mathbb{C} - \mathbb{R}$ denote the two nonreal roots of $f(x)$. Recall that since complex roots come in complex conjugate pairs that $\overline{u_2} = u_3$. Thus, we may write $u_2 = a + bi$ and $u_3 = a - bi$ for some $a, b \in \mathbb{R}$ with $b \neq 0$ since $u_2, u_3 \notin \mathbb{R}$. Now, note that

$$\begin{aligned}\Delta &= \prod_{1 \leq i < j \leq 3} (u_i - u_j) \\ &= (u_1 - u_2)(u_1 - u_3)(u_2 - u_3) \\ &= [(u_1 - a) - bi][(u_1 - a) + bi][2bi] \\ &= 2bi[(u_1 - a)^2 + b^2]\end{aligned}$$

so that

$$D = \Delta^2 = (2bi)^2[(u_1 - a)^2 + b^2]^2 = -4b^2[(u_1 - a)^2 + b^2]^2$$

But since $b \neq 0$, the above equality implies that $D < 0$, which is a contradiction. We conclude that $f(x)$ has three real roots.

For the second direction, suppose that $f(x)$ has three real roots $u_1, u_2, u_3 \in \mathbb{R}$. This gives by the above computation that

$$\Delta = (u_1 - u_2)(u_1 - u_3)(u_2 - u_3) \in \mathbb{R}$$

Furthermore, since $\text{char}(\mathbb{R}) = 0$ and $K \subseteq \mathbb{R}$, we have $\text{char}(K) = 0$. Since $f(x)$ is irreducible, this observation implies that $f(x)$ is separable. In particular, this gives that $\Delta \neq 0$. Hence, since $\Delta \in \mathbb{R}$ and since $\Delta \neq 0$, we have $D = \Delta^2 > 0$. □

Proof. (b): For the first direction, suppose that $D < 0$. For the sake of contradiction, suppose that $f(x)$ did not have exactly one real root. Then since $f(x)$ has at least one real root and since nonreal roots come in complex conjugate pairs, it follows that $f(x)$ has three real roots. By Part (a), it now follows that $D > 0$. However, this contradicts the fact that $D < 0$. We conclude that $f(x)$ has exactly one real root.

For the second direction, suppose that $f(x)$ has exactly one real root. Then the remaining two roots of $f(x)$ are nonreal and are thus complex conjugates. By Part (a), we saw in this situation that $D < 0$. This completes the proof. □

Problem 3. *Let f be a separable cubic with Galois group S_3 and roots $u_1, u_2, u_3 \in F$. Then the distinct intermediate fields of the extension of K by F are $F, K(\Delta), K(u_1), K(u_2), K(u_3), K$. The corresponding subgroups of the Galois group are $1, A_3, T_1, T_2, T_3, S_3$, where $T_i = \{(1), (j \quad k) : j \neq i \neq k\}$.*

Proof. Since $f(x)$ is separable, it is immediate that F/K is a finite Galois extension. Thus, by FTGT, there is a one-to-one correspondence from the intermediate fields of the extension F/K to the set of subgroups of $\mathrm{Gal}(F/K)$. Under this correspondence, we have that

$$F \mapsto \mathrm{Gal}(F/F) = 1$$

and

$$K \mapsto \mathrm{Gal}(F/K) = S_3$$

Furthermore, we also have

$$K(\Delta) \mapsto \mathrm{Gal}(F/K(\Delta)) = \mathrm{Gal}(F/K) \cap A_3 = S_3 \cap A_3 = A_3$$

We now show that $K(u_1) \mapsto T_1$. Towards this end, first note that since $\mathrm{Gal}(F/K) = S_3$ permutes the roots u_1, u_2, u_3 of $f(x)$ that there is some $\sigma \in \mathrm{Gal}(F/K)$ such that $\sigma(u_1) = u_1, \sigma(u_2) = u_2, \sigma(u_3) = u_2$. Since σ fixes K and u_1, we have that σ fixes $K(u_1)$ so that $\sigma \in \mathrm{Gal}(F/K(u_1))$. Hence, we obtain $(u_2 \quad u_3) = \sigma \in \mathrm{Gal}(F/K(u_1))$. Identifying $(2 \quad 3) \in S_3$ with $(u_2 \quad u_3)$, this result shows that

$$K(u_1) \mapsto \mathrm{Gal}(F/K(u_1)) = T_1$$

In a similar fashion, we also obtain that $K(u_2) \mapsto T_2$ and $K(u_3) \mapsto T_3$. This completes the proof. $\square$

Homework 10: Page 276 #10

Problem 10. *Determine the Galois groups of the following polynomials over the fields indicated:*

(a): $x^4 - 5$ *over* $\mathbb{Q}$*; over* $\mathbb{Q}(\sqrt{5})$*; over* $\mathbb{Q}(\sqrt{5}i)$*.*

(b): $(x^3 - 2)(x^2 - 3)(x^2 - 5)(x^2 - 7)$ *over* $\mathbb{Q}$*.*

(c): $x^3 - x - 1$ *over* $\mathbb{Q}$*; over* $\mathbb{Q}(\sqrt{23}i)$*.*

(d): $x^3 - 10$ *over* $\mathbb{Q}$*; over* $\mathbb{Q}(\sqrt{2})$*.*

(e): $x^5 - 6x + 3$ *over* $\mathbb{Q}$*.*

(f): $x^3 - 2$ *over* $\mathbb{Q}$*.*

(g): $(x^3 - 2)(x^2 - 5)$ *over* $\mathbb{Q}$*.*

Note: In all parts of this proof, we let $f(x)$ denote the given polynomial, Γ the set of roots of $f(x)$, F the splitting field of the given polynomial over the indicated base field, G the corresponding Galois group, and D the discriminant of $f(x)$. Furthermore, we also note that since every field involved in this problem is of characteristic 0 that $|G|$ is always equal to the dimension of F over the base field.

Proof. (a; over $\mathbb{Q}$): Let $u = 5^{1/4}$ so that $\Gamma = \{u, -u, iu, -iu\}$ which gives $F = \mathbb{Q}(u, i)$. Note that $f(x)$ is irreducible over $\mathbb{Q}$ by Eisenstein's Criterion and that u is a root of $f(x)$ so that

$$[\mathbb{Q}(u) : \mathbb{Q}] = \deg(f(x)) = 4$$

Now, note that $\mathbb{Q}(u) \subseteq \mathbb{R}$ and since $i \notin \mathbb{R}$ we have that $i \notin \mathbb{Q}(u)$ so that $x^2 + 1$ is the minimum polynomial for i over $\mathbb{Q}(u)$. This observation gives

$$[F : \mathbb{Q}(u)] = \deg(x^2 + 1) = 2$$

Hence, we obtain that

$$|G| = [F : \mathbb{Q}] = [F : \mathbb{Q}(u)][\mathbb{Q}(u) : \mathbb{Q}] = 4 \cdot 2 = 8$$

Now, the above calculation shows that $[F : \mathbb{Q}(i)] = 4$ since $[\mathbb{Q}(i) : \mathbb{Q}] = 2$. In particular, this implies that $f(x)$ is the minimum polynomial for u over $\mathbb{Q}(i)$. Hence, since iu is also a root of $f(x)$ there exists some element $\sigma \in \mathrm{Gal}(F/\mathbb{Q}(i)) \subseteq \mathrm{Gal}(F/\mathbb{Q})$ such that $\sigma(u) = iu$. Notice that since σ fixes i that

$$\sigma(iu) = \sigma(i)\sigma(u) = i(iu) = -u$$

and

$$\sigma(-u) = -\sigma(u) = -(iu) = -iu$$

and

$$\sigma(-iu) = -\sigma(i)\sigma(u) = -i(iu) = u$$

Hence, if $p_1 = (u \quad iu \quad -u \quad -iu)$, the above calculation shows that $p_1 \in G$. Furthermore, note that if $\tau : F \to F$ is the complex conjugation map that $\tau \in G$. In particular, this observation gives that if $p_2 = (iu \quad -iu)$, then $p_2 \in G$.

Combining the above results, we see that since $|G| = 8$ that $G = \langle p_1, p_2 \rangle$. Furthermore, note that

$$p_2 p_1 p_2^{-1} = p_1^{-1}$$

Hence, we obtain $G \simeq D_8$.

(a; over $\mathbb{Q}(\sqrt{5})$): We again have F and Γ as above. Notice that $x^2 - \sqrt{5} \in \mathbb{Q}(\sqrt{5})[x]$ and that u is a root of $x^2 - \sqrt{5}$. Now, for the sake of contradiction, suppose that $u \in \mathbb{Q}(\sqrt{5})$. Then we can write $u = a + b\sqrt{5}$ for some $a, b \in \mathbb{Q}$. By this equality, we obtain that

$$5b^2 = (b\sqrt{5})^2 = (u - a)^2 = u^2 - 2au + a^2 \notin \mathbb{Q}$$

which is a contradiction since $5b^2 \in \mathbb{Q}$ since $b \in \mathbb{Q}$. We conclude that $u \notin \mathbb{Q}(\sqrt{5})$ which implies that $x^2 - \sqrt{5}$ is the minimum polynomial for u over $\mathbb{Q}(\sqrt{5})$. This observation gives that

$$[\mathbb{Q}(\sqrt{5}, u) : \mathbb{Q}(\sqrt{5})] = \deg(x^2 - \sqrt{5}) = 2$$

However, we have $\sqrt{5} \in \mathbb{Q}(u)$ so that $\mathbb{Q}(\sqrt{5}, u) = \mathbb{Q}(u)$. Thus, we now have by the above equality that $[\mathbb{Q}(u) : \mathbb{Q}(\sqrt{5})] = 2$. Now, recall from the above that $[F : \mathbb{Q}(u)] = 2$. Thus, combining these results gives

$$|G| = [F : \mathbb{Q}(\sqrt{5})] = [F : \mathbb{Q}(u)][\mathbb{Q}(u) : \mathbb{Q}(\sqrt{5})] = 2 \cdot 2 = 4$$

Finally, let $\sigma \in G$. Notice that $x^2 - \sqrt{5} \in \mathbb{Q}(\sqrt{5})[x]$ and that the roots of $x^2 - \sqrt{5}$ are u and $-u$. Since σ must send roots of $x^2 - \sqrt{5}$ to roots of $x^2 - \sqrt{5}$, the previous observation gives that $\sigma(u) \in \{u, -u\}$. In particular, this shows that $\sigma \in G$ cannot be of order 4. Since $\sigma \in G$ was arbitrary, this shows that G has no elements of order 4. Thus, since $|G| = 4$ and G has no elements of order 4, it now follows that $G \simeq V_4$.

(a; over $\mathbb{Q}(\sqrt{5}i)$): We again have F and Γ as above. We claim that $\sqrt{5} \notin \mathbb{Q}(\sqrt{5}i)$. For the sake of contradiction, suppose that $\sqrt{5} \in \mathbb{Q}(\sqrt{5}i)$. Then there are $a, b \in \mathbb{Q}$ such that $\sqrt{5} = a + b\sqrt{5}i$. Dividing both sides of this equality by $\sqrt{5}$, we obtain $1 = a/\sqrt{5} + bi$ so that $a/\sqrt{5} = 1 - bi$. This equality implies that $b = 0$ so that $a = \sqrt{5}$ which is a contradiction since $a \in \mathbb{Q}$. We conclude that $\sqrt{5} \notin \mathbb{Q}(\sqrt{5}i)$. In a similar fashion, we also see that $u \notin \mathbb{Q}(\sqrt{5}i)$. The previous two observations imply that the minimum polynomial of u over $\mathbb{Q}(\sqrt{5}i)$ is $f(x)$ so that

$$[\mathbb{Q}(\sqrt{5}i, u) : \mathbb{Q}(\sqrt{5}i)] = \deg(f(x)) = 4$$

We claim that $\mathbb{Q}(\sqrt{5}i, u) = F$. On one hand, we have that $\sqrt{5}i = u \cdot u \cdot i \in F$ and since $u \in F$, this implies that $\mathbb{Q}(\sqrt{5}i, u) \subseteq F$. On the other hand, we have $u \in \mathbb{Q}(\sqrt{5}i, u)$ and since

$$i = \frac{1}{5} \cdot 5i = \frac{1}{5} \cdot u \cdot u \cdot \sqrt{5}i \in \mathbb{Q}(\sqrt{5}i, u)$$

we obtain $F \subseteq \mathbb{Q}(\sqrt{5}i, u)$. Hence, we see $F = \mathbb{Q}(\sqrt{5}i, u)$ so that by the above we have

$$|G| = [F : \mathbb{Q}(\sqrt{5}i)] = [\mathbb{Q}(\sqrt{5}i, u) : \mathbb{Q}(\sqrt{5}i)] = 4$$

Finally, the above proof shows that $f(x)$ is irreducible over $\mathbb{Q}(\sqrt{5}i)$. Hence, there exists some $\sigma \in G$ such that $\sigma(u) = iu$. Now, note that since $\sigma \in G$ we have that σ fixes $\sqrt{5}i$ so that

$$\sqrt{5}i = \sigma(\sqrt{5}i) = \sigma(u \cdot u \cdot i) = \sigma(u)\sigma(u)\sigma(i) = (iu)(iu)\sigma(i) = -u^2\sigma(i) = -\sqrt{5}\sigma(i)$$

Dividing both sides of this equality by $-\sqrt{5}$, we obtain $\sigma(i) = -i$ so that

$$\sigma(iu) = \sigma(i)\sigma(u) = (-i)(iu) = u$$

Since we also have

$$\sigma(-u) = -\sigma(u) = -(iu) = -iu$$

and

$$\sigma(-iu) = -\sigma(i)\sigma(u) = -(-i)(iu) = -u$$

the above calculations show that $(u \quad iu)(-u \quad -iu) \in G$ is an element of order 2.

Recall also by the above that there is some $\tau \in \mathrm{Gal}(F/\mathbb{Q}(i))$ such that $\tau(u) = iu$ and that $|\tau| = 4$. We claim that $\tau^2 \in G$. In order to prove this claim, it remains to show that τ^2 fixes $\sqrt{5}i$. Indeed, we have since τ fixes i that

$$\tau^2(u) = \tau(\tau(u)) = \tau(iu) = \tau(i)\tau(u) = i(iu) = -u$$

so that

$$\tau^2(\sqrt{5}i) = \tau^2(u \cdot u \cdot i) = \tau^2(u)\tau^2(u)\tau^2(i) = (-u)(-u)i = u^2 i = \sqrt{5}i$$

which shows that τ^2 fixes $\sqrt{5}i$. Hence, we obtain $\tau^2 \in G$. Since $|\tau| = 4$, it follows that $|\tau^2| = 2$. Furthermore, the above calculation shows that $\tau^2(u) = -u \neq iu$ so that τ is distinct from the element of order 2 in G exhibited above. In particular, this shows that G contains two distinct elements of order 2. Since $|G| = 4$, we conclude that $G \simeq V_4$. $\square$

Proof. (b): Let $u = 2^{1/3}$ and ζ be a primitive third root of unity so that

$$\Gamma = \{u, u\zeta, u\zeta^2, \sqrt{3}, -\sqrt{3}, \sqrt{5}, -\sqrt{5}, \sqrt{7}, -\sqrt{7}\}$$

Thus, we have $F = \mathbb{Q}(u, \sqrt{3}, \sqrt{5}, \sqrt{7}, \zeta)$. Note that $x^3 - 2$ is irreducible over $\mathbb{Q}$ by Eisenstein's Criterion and that u is a root of $x^3 - 2$ so that

$$[\mathbb{Q}(u) : \mathbb{Q}] = \deg(x^3 - 2) = 3$$

For the sake of contradiction, suppose that $\sqrt{3} \in \mathbb{Q}(u)$. Then there are $a, b \in \mathbb{Q}$ such that $\sqrt{3} = a + bu$. In particular, note that not both a and b can be equal to 0 by this equality. Squaring both sides of this equality gives that

$$3 = a^2 + 2abu + b^2u^2 \notin \mathbb{Q}$$

since not both a and b are equal to 0. However, this is a contradiction. Hence, we have $\sqrt{3} \notin \mathbb{Q}(u)$ so that

$$[\mathbb{Q}(u, \sqrt{3}) : \mathbb{Q}(u)] = 2$$

In a similar fashion, we obtain $\sqrt{5} \notin \mathbb{Q}(u, \sqrt{3})$ so that

$$[\mathbb{Q}(u, \sqrt{3}, \sqrt{5}) : \mathbb{Q}(u, \sqrt{3})] = 2$$

In a similar fashion, we obtain $\sqrt{7} \notin \mathbb{Q}(u, \sqrt{3}, \sqrt{5})$ so that

$$[\mathbb{Q}(u, \sqrt{3}, \sqrt{5}, \sqrt{7}) : \mathbb{Q}(u, \sqrt{3}, \sqrt{5})] = 2$$

Finally, since $\mathbb{Q}(u, \sqrt{3}, \sqrt{5}, \sqrt{7}) \subseteq \mathbb{R}$ and since $\zeta \notin \mathbb{R}$ it follows that $\zeta \notin \mathbb{Q}(u, \sqrt{3}, \sqrt{5}, \sqrt{7})$. Thus, the minimum polynomial for ζ over $\mathbb{Q}(u, \sqrt{3}, \sqrt{5}, \sqrt{7})$ is $x^2 + x + 1$ so that

$$[F : \mathbb{Q}(u, \sqrt{3}, \sqrt{5}, \sqrt{7})] = \deg(x^2 + x + 1) = 2$$

Combining the above results, we have

$$|G| = [F : \mathbb{Q}] = 3 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 48$$

Now, we know that G is isomorphic to a subgroup of S_9. Furthermore, notice that if $\sigma \in G$ that σ permutes the roots of each polynomial involved in the factorization of $f(x)$ among themselves since these polynomials share no common roots. Therefore, we have $G \subseteq S_3 \times S_2 \times S_2 \times S_2$. However, we also have

$$|G| = 48 = 6 \cdot 2 \cdot 2 \cdot 2 = |S_3| \cdot |S_2| \cdot |S_2| \cdot |S_2| = |S_3 \times S_2 \times S_2 \times S_2|$$

so that by the previous inclusion, we obtain $G \simeq S_3 \times S_2 \times S_2 \times S_2$. $\square$

Proof. (c; over $\mathbb{Q}$): First, note that by the Rational Root Theorem that $f(x)$ has no roots over $\mathbb{Q}$. Since $f(x) \in \mathbb{Q}[x]$ is of degree 3 and has no roots over $\mathbb{Q}$, it now follows that $f(x)$ is irreducible over $\mathbb{Q}$. Thus, since $\mathrm{char}(\mathbb{Q}) = 0$ we have that $f(x)$ is also separable so that $3 = \deg(f(x))$ divides $|G|$. Furthermore, we know that G is isomorphic to a subgroup of S_3. Therefore, since 3 divides $|G|$ this forces $G \in \{A_3, S_3\}$.

Finally, note that

$$D = -4(-1)^3 - 27(-1)^2 = 4 - 27 = -23 < 0$$

so that D cannot possibly be a square in $\mathbb{Q}$. In particular, this implies that $G \not\subseteq A_3$ so that by the above, we obtain $G \simeq S_3$.

(c; over $\mathbb{Q}(\sqrt{23}i)$): First, we show that $f(x)$ is irreducible over $\mathbb{Q}(\sqrt{23}i)$. For the sake of contradiction, suppose that $f(x)$ were reducible over $\mathbb{Q}(\sqrt{23}i)$. Since $f(x)$ is of degree 3, this implies that $f(x)$ has a root in $\mathbb{Q}(\sqrt{23}i)$. Let this root of $f(x)$ in $\mathbb{Q}(\sqrt{23}i)$ be denoted $a + b\sqrt{23}i$ for some $a, b \in \mathbb{Q}$. In particular, since $f(x)$ has no rational roots, it follows that $b \neq 0$ or else a would be a rational root of $f(x)$.

Now, let $g(x) \in \mathbb{Q}[x]$ be the minimum polynomial for $a + b\sqrt{23}i$ over $\mathbb{Q}$. Since $a + b\sqrt{23}i$ is a root of $f(x) \in \mathbb{Q}[x]$ it follows that $g(x)$ divides $f(x)$. Furthermore, since $b \neq 0$ it follows that $\deg(g(x)) = 2$. Therefore, we may write

$$f(x) = (x - c)g(x)$$

for some $c \in \mathbb{Q}$. However, this would imply that c is a rational root of $f(x)$ which is a contradiction since $f(x)$ has no rational roots. We conclude that $f(x)$ is irreducible over $\mathbb{Q}(\sqrt{23}i)$. Since we have by the above that $f(x)$ is also separable, we now have that $3 = \deg(f(x))$ divides $|G|$. Furthermore, we know that G is isomorphic to a subgroup of S_3. Therefore, since 3 divides $|G|$ this forces $G \in \{A_3, S_3\}$.

Finally, recall that

$$D = -23 = (\sqrt{23}i)^2$$

so that D is a square in $\mathbb{Q}(\sqrt{23}i)$. In particular, this implies that $G \subseteq A_3$ so that by the above, we obtain $G \simeq A_3$. $\square$

Proof. (d; over $\mathbb{Q}$): First, note that by the Rational Root Theorem that $f(x)$ has no roots over $\mathbb{Q}$. Since $f(x)$ is of degree 3, the same reasoning as above gives that $G \in \{A_3, S_3\}$. Finally, notice that

$$D = -4(0)^3 - 27(-10)^2 = -2700 < 0$$

so that D cannot possibly be a square in $\mathbb{Q}$. In particular, this implies that $G \not\subseteq A_3$ so that by the above, we obtain $G \simeq S_3$.

(d; over $\mathbb{Q}(\sqrt{2})$): Let $u = 10^{1/3}$ and ζ be a primitive third root of unity so that

$$\Gamma = \{u, u\zeta, u\zeta^2\}$$

For the sake of contradiction, suppose that $u \in \mathbb{Q}(\sqrt{2})$. Then we can write $u = a + b\sqrt{2}$ for some $a, b \in \mathbb{Q}$. By this equality, we obtain

$$2b^2 = (b\sqrt{2})^2 = (u-a)^2 = u^2 - 2au + a^2 \notin \mathbb{Q}$$

which is a contradiction since $2b^2 \in \mathbb{Q}$ since $b \in \mathbb{Q}$. Therefore, we have $u \notin \mathbb{Q}(\sqrt{2})$. Furthermore, since $\mathbb{Q}(\sqrt{2}) \subseteq \mathbb{R}$ and since $u\zeta, u\zeta^2 \notin \mathbb{R}$, it follows that $u\zeta, u\zeta^2 \notin \mathbb{Q}(\sqrt{2})$.

The above results show that $f(x)$ has no roots over $\mathbb{Q}(\sqrt{2})$. Since $f(x)$ is of degree 3, this implies that $f(x)$ is irreducible over $\mathbb{Q}(\sqrt{2})$. By the same reasoning as above, this implies that $G \in \{A_3, S_3\}$. As we saw above, we have $D = -2700$ which is not a square in $\mathbb{Q}(\sqrt{2})$. In particular, this implies that $G \not\subseteq A_3$ so that by the above, we obtain $G \simeq S_3$. $\square$

Proof. (e): First, note that by Eisenstein's Criterion that $f(x)$ is irreducible over $\mathbb{Q}$. By the same reasoning as above, we also have that $f(x)$ is separable. Furthermore, we know that G is isomorphic to a subgroup of S_5. Thus, by the previous result, we have that G is isomorphic to a transitive subgroup of S_5.

Now, using elementary Calculus, we see that $f(x)$ has exactly 3 real roots and exactly 2 nonreal roots. Denote these nonreal roots by u_1 and u_2 and note that since nonreal roots come in complex conjugate pairs that u_1 and u_2 are complex conjugates. Next, let $\tau : F \to F$ denote the complex conjugation map. Then we have $\tau \in G$. Furthermore, we know that τ permutes the roots of $f(x)$. But since τ is complex conjugation, it follows that τ fixes the 3 real roots of $f(x)$ and swaps u_1 and u_2. In other words, we have $(u_1 \quad u_2) \in G$. In particular, this shows that G contains a transposition.

Combining the above results, we have that G is isomorphic to a transitive subgroup of S_5 and that G contains a transposition. Since 5 is a prime number, this observation gives that $G \simeq S_5$. $\square$

Proof. (f): First, note that by Eisenstein's Criterion that $f(x)$ is irreducible over $\mathbb{Q}$. Since $f(x)$ is of degree 3, the same reasoning as above gives that $G \in \{A_3, S_3\}$. Finally, notice that

$$D = -4(0)^3 - 27(-2)^2 = -108 < 0$$

so that D cannot possibly be a square in $\mathbb{Q}$. In particular, this implies that $G \not\subseteq A_3$ so that by the above, we obtain $G \simeq S_3$. $\square$

Proof. (g): Let $u = 2^{1/3}$ and ζ be a primitive third root of unity so that

$$\Gamma = \{u, u\zeta, u\zeta^2, \sqrt{5}, -\sqrt{5}\}$$

Thus, we have $F = \mathbb{Q}(u, \sqrt{5}, \zeta)$. Recall from the above that $[\mathbb{Q}(u) : \mathbb{Q}] = 3$. For the sake of contradiction, suppose that $\sqrt{5} \in \mathbb{Q}(u)$. Then there are $a, b \in \mathbb{Q}$ such that $\sqrt{5} = a + bu$. In particular, note that not both a and b can be equal to 0 by this equality. Squaring both sides of this equality gives that

$$5 = a^2 + 2abu + b^2u^2 \notin \mathbb{Q}$$

since not both a and b are equal to 0. However, this is a contradiction. Hence, we have $\sqrt{5} \notin \mathbb{Q}(u)$ so that

$$[\mathbb{Q}(u, \sqrt{5}) : \mathbb{Q}(u)] = 2$$

Finally, since $\mathbb{Q}(u, \sqrt{5}) \subseteq \mathbb{R}$ and since $\zeta \notin \mathbb{R}$ it follows that $\zeta \notin \mathbb{Q}(u, \sqrt{5})$. Thus, the minimum polynomial for ζ over $\mathbb{Q}(u, \sqrt{5})$ is $x^2 + x + 1$ so that

$$[F : \mathbb{Q}(u, \sqrt{5})] = \deg(x^2 + x + 1) = 2$$

Combining the above results, we have

$$|G| = [F : \mathbb{Q}] = 3 \cdot 2 \cdot 2 = 12$$

Now, we know that G is isomorphic to a subgroup of S_5. Furthermore, notice that if $\sigma \in G$ that σ permutes the roots of each polynomial involved in the factorization of $f(x)$ among themselves since these polynomials share no common roots. Therefore, we have $G \subseteq S_3 \times S_2$. However, we also have

$$|G| = 12 = 6 \cdot 2 = |S_3| \cdot |S_2| = |S_3 \times S_2|$$

so that by the previous inclusion, we obtain $G \simeq S_3 \times S_2$. $\square$

Homework 11: Page 281 #6, 7, 8

Problem 6. *If $|K| = q$ and $(n, q) = 1$ and F is a splitting field of $x^n - 1$ over K, then $[F : K]$ is the least positive integer m such that $n\big|(q^m - 1)$.*

Proof. Let $[F : K] = m$ so that

$$|F| = |K|^{[F:K]} = |K|^m = q^m$$

Since $|F| = q^m$, it follows that $|F^\times| = q^m - 1$ so that every element of $F^\times$ is a root of the polynomial $x^{q^m-1} - 1 \in K[x]$. But since $x^{q^m-1} - 1$ can have at most $\deg(x^{q^m-1} - 1) = q^{m-1}$ roots, it follows that the set of roots of $x^{q^m-1} - 1$ is precisely equal to $F^\times$. Recall that $x^n - 1$ splits over F by hypothesis so that every root of $x^n - 1$ is in F. More specifically, since 0 is not a root of $x^n - 1$, we have that every root of $x^n - 1$ is in $F^\times$.

Now, since K is a finite field we have that $q = |K| = p^t$ for some prime number p and some positive integer t. More specifically, this gives that $\mathrm{char}(K) = p$ and

$$1 = (n, q) = (n, p^t)$$

Since p is prime, the above equality implies that p does not divide n. Furthermore, notice that the derivative of $x^n - 1$ is $nx^{n-1} \in K[x]$. Since p does not divide n and since $\mathrm{char}(K) = p$, this gives that $nx^{n-1} \neq 0$. Hence, it follows that the polynomial $x^n - 1$ and its derivative nx^{n-1} are relatively prime in $K[x]$ so that $x^n - 1$ is separable. In particular, this shows that $x^n - 1$ has only linear factors over $F^\times$. By the above, this gives that $x^n - 1$ divides $x^{q^m-1} - 1$ which implies that n divides $q^m - 1$.

We now prove that m is the least positive integer such that $n\big|(q^m - 1)$. If $m = 1$, then there is nothing to prove. So, assume that $m \geq 2$. For the sake of contradiction, suppose that there were some positive integer z with $z < m$ such that $n\big|(q^z - 1)$. Let L be a field extension of K with $[L : K] = z$. Then as F is a splitting field for $x^n - 1$ over K and since

$$[F : K] = m > z = [L : K]$$

it follows that $x^n - 1$ cannot split over L. Furthermore, as $n\big|(q^z - 1)$, we have that $x^n - 1 \in K[x] \subseteq L[x]$ divides $x^{q^z-1} - 1 \in K[x] \subseteq L[x]$ so that every root of $x^n - 1$ is a root of $x^{q^z-1} - 1$.

Notice that we have

$$|L| = |K|^{[L:K]} = |K|^z = q^z$$

In particular, using the same argument as presented above, this implies that the set of roots of $x^{q^z-1} - 1$ is precisely equal to $L^\times$. But recall that every root of $x^n - 1$ is a root of $x^{q^z-1} - 1$ so that every root of $x^n - 1$ is in $L^\times$. It now follows that $x^n - 1$ splits over L, which is a contradiction. This completes the proof. $\square$

Problem 7. *If $|K| = q$ and $f \in K[x]$ is irreducible, then f divides $x^{q^n} - x$ if and only if* $\deg f$ *divides n.*

Proof. For the first direction, assume that $f(x)$ divides $x^{q^n} - x$. Let a be a root of $f(x)$ in a splitting field for $f(x)$ over K. Since $f(x)$ divides $x^{q^n} - x$ and since a is a root of $f(x)$, it follows that a is a root of $x^{q^n} - x$ so that $a \in \mathbb{F}_{q^n}$. Furthermore, since $|K| = q$, we have that $K \subseteq \mathbb{F}_{q^n}$. Since $a \in \mathbb{F}_{q^n}$, this gives the tower of fields

$$K \subseteq K(a) \subseteq \mathbb{F}_{q^n}(a) = \mathbb{F}_{q^n}$$

Now, as $f(x) \in K[x]$ is irreducible and since a is a root of $f(x)$, it follows that

$$[K(a) : K] = \deg(f(x))$$

Thus, since $|K| = q$ we have that $n = [\mathbb{F}_{q^n} : K]$ so that

$$n = [\mathbb{F}_{q^n} : K] = [\mathbb{F}_{q^n} : K(a)][K(a) : K] = [\mathbb{F}_{q^n} : K(a)] \cdot \deg(f(x))$$

In particular, the above equality shows that $\deg(f(x))$ divides n, completing the proof of the first direction.

For the second direction, let $m = \deg(f(x))$ and assume that m divides n. Since m divides n, we have that $\mathbb{F}_{q^m} \subseteq \mathbb{F}_{q^n}$. Similarly as above, let a be a root of $f(x)$ in a splitting field for $f(x)$ over K so that

$$[K(a) : K] = \deg(f(x)) = m$$

so that

$$|K(a)| = |K|^{[K(a):K]} = |K|^m = q^m$$

By the uniqueness of finite fields, this gives that $K(a) = \mathbb{F}_{q^m}$ so that by the above we have the tower of fields $K \subseteq K(a) \subseteq \mathbb{F}_{q^n}$. In particular, we also have that $a \in K(a) \subseteq \mathbb{F}_{q^n}$ so that a is a root of the polynomial $x^{q^n} - x \in K[x]$.

Finally, note that since $f(x) \in K[x]$ is irreducible and has a as a root that $f(x)$ is the minimum polynomial for a over K. But since a is also a root of the polynomial $x^{q^n} - x \in K[x]$, we conclude that $f(x)$ divides $x^{q^n} - x$. This completes the proof of the second direction. $\square$

Problem 8. *If $|K| = p^r$ and $|F| = p^n$, then $r\big|n$ and $\mathrm{Gal}(F/K)$ is cyclic with generator ϕ given by $u \mapsto u^{p^r}$.*

Proof. Let $[F : K] = m$. Then we have

$$p^n = |F| = |K|^{[F:K]} = |K|^m = (p^r)^m = p^{rm}$$

so that $p^n = p^{rm}$ so that $n = rm$. In particular, this shows that $r\big|n$.

Now, define $\sigma : F \to F$ by $\sigma(a) = a^p$ for all $a \in F$. Then we know that we have $\mathrm{Gal}(F/\mathbb{F}_p) = \langle\sigma\rangle$. Since we have the tower of fields $\mathbb{F}_p \subseteq K \subseteq F$, we have

$$\mathrm{Gal}(F/K) \subseteq \mathrm{Gal}(F/\mathbb{F}_p) = \langle\sigma\rangle$$

Furthermore, since subgroups of cyclic groups are cyclic, it follows by the above that $\mathrm{Gal}(F/K)$ is cyclic.

Next, we know that

$$|\mathrm{Gal}(F/K)| = [F : K] = m$$

and

$$n = [F : \mathbb{F}_p] = |\mathrm{Gal}(F/\mathbb{F}_p)| = |\langle\sigma\rangle| = |\sigma|$$

The first of the above equalities shows that $\mathrm{Gal}(F/K)$ is a cyclic subgroup of order m of the cyclic group $\mathrm{Gal}(F/\mathbb{F}_p) = \langle\sigma\rangle$. On the other hand, recall that $n = rm$ so that $m = n/r$. Thus, by the second of the above equalities, we see that $\langle\sigma^r\rangle$ is a subgroup of $\mathrm{Gal}(F/\mathbb{F}_p)$ of order

$$\frac{|\sigma|}{r} = \frac{n}{r} = m$$

But since $\mathrm{Gal}(F/\mathbb{F}_p)$ is a cyclic group, it follows that each subgroup of $\mathrm{Gal}(F/\mathbb{F}_p)$ of a given order is unique. Combining this observation with the above results, we conclude that $\mathrm{Gal}(F/K) = \langle\sigma^r\rangle$.

Finally, let $\phi = \sigma^r : F \to F$. Let $a \in F$. Then we have

$$\phi(a) = \sigma^r(a) = \sigma^{r-1}(\sigma(a)) = \sigma^{r-1}(a^p) = \cdots = \sigma(a^{p^{r-1}}) = (a^{p^{r-1}})^p = a^{p^r}$$

so that $\phi : F \to F$ is indeed the map $u \mapsto u^{p^r}$. Since $\mathrm{Gal}(F/K) = \langle\sigma^r\rangle = \langle\phi\rangle$, this completes the proof. $\square$

Homework 12: Page 288 #5, 6, 7

Problem 5. *If* $\mathrm{char}(K) = p \neq 0$ *and* $a \in K$ *but* $a \notin K^p$*, then* $x^{p^n} - a \in K[x]$ *is irreducible for every* $n > 1$*.*

Proof. Let n be a positive integer with $n > 1$. Let F be a splitting field for $x^{p^n} - a$ over K and let $u_1, \ldots, u_{p^n} \in F$ denote the roots of $x^{p^n} - a$ so that $F = K(u_1, \ldots, u_{p^n})$ by the definition of F. Let $u \in \{u_1, \ldots, u_{p^n})$ and suppose that $z \in F$ is a root of $m_{K,u}(x)$. Note that since u is a root of $x^{p^n} - a$ that $m_{K,u}(x)$ divides $x^{p^n} - a$. In particular, since z is a root of $m_{K,u}(x)$ this observation implies that z is also a root of $x^{p^n} - a$. This gives

$$u^{p^n} - a = 0 = z^{p^n} - a$$

so that $u^{p^n} = z^{p^n}$ so that $u^{p^n} - z^{p^n} = 0$. Since $\mathrm{char}(K) = p$, it follows that $\mathrm{char}(F) = p$ so that we now have

$$(u - z)^{p^n} = u^{p^n} - z^{p^n} = 0$$

which implies that $z = u$. Since z was an arbitrary root of $m_{K,u}(x)$, it now follows that u is purely inseparable over K. Since $u \in \{u_1, \ldots, u_{p^n}\}$ was arbitrary, this now shows that F/K is a purely inseparable extension since $F = K(u_1, \ldots, u_{p^n})$.

Now, fix $u \in \{u_1, \ldots, u_{p^n}\}$. Since F/K is purely inseparable and since $\mathrm{char}(K) = p$, it follows that $m_{K,u}(x) = x^{p^r} - b \in K[x]$. As u is a root of $x^{p^n} - a$, we have that $m_{K,u}(x) = x^{p^r} - b$ divides $x^{p^n} - a$. In particular, this observation gives that $r \leq n$.

If $r = n$, then we have $m_{K,u}(x) = x^{p^n} - b$. Since u is a root of $m_{K,u}(x)$ and since u is a root of $x^{p^n} - a$, we have

$$u^{p^n} - b = 0 = u^{p^n} - a$$

so that $a = b$. Thus, we see $m_{K,u}(x) = x^{p^n} - a$. Since $m_{K,u}(x)$ is irreducible over K by definition, it now follows $x^{p^n} - a$ is irreducible over K. This completes the proof in the case when $r = n$.

For the sake of contradiction, suppose that $r < n$. Note that the equalities above imply the equalities $u^{p^r} = b$ and $u^{p^n} = a$. Since $r < n$, we can then write

$$a = u^{p^n} = (u^{p^r})^{p^{n-r}} = b^{p^{n-r}}$$

Now, recall that $b \in K$. Thus, since $r < n$ we have $n - r - 1 \geq 0$ so that $b^{p^{n-r-1}} \in K$. Hence, we obtain

$$a = b^{p^{n-r}} = (b^{p^{n-r-1}})^p \in K^p$$

which contradicts the fact that $a \notin K^p$. Hence, it cannot be the case that $r < n$ so that $r = n$. In this case, as we saw above, we obtain that $x^{p^n} - a$ is irreducible over K. This completes the proof. $\square$

Problem 6. *If $f \in K[x]$ is monic irreducible,* $\deg f \geq 2$*, and f has all its roots equal (in a splitting field), then* $\mathrm{char}(K) = p \neq 0$ *and $f = x^{p^n} - a$ for some $n \geq 1$ and $a \in K$.*

Proof. Let F be a splitting field for $f(x)$ over K and let $u \in F$ be the unique root of $f(x)$. By definition, we have that $F = K(u)$. Notice that as $f(x) \in K[x]$ is a monic, irreducible polynomial that has u as a root that $f(x) = m_{K,u}(x)$. Since $f(x)$ has a single root in F, it follows that $m_{K,u}(x) = f(x)$ is purely inseparable. Hence, we have that F/K is a purely inseparable extension since $F = K(u)$.

Now, for the sake of contradiction, suppose that $\mathrm{char}(K) = 0$. Then as $f(x)$ is irreducible, we have that $f(x)$ is separable. However, since $\deg(f(x)) \geq 2$ and since the only root of $f(x)$ is $u \in F$, it cannot be the case that $f(x)$ is separable. We conclude that $\mathrm{char}(K) = p \neq 0$ for some prime number p.

Finally, recall that $f(x)$ is the minimum polynomial for $u \in F$ and that F/K is a purely inseparable extension. Since $\mathrm{char}(K) = p \neq 0$, it follows that we have $f(x) = x^{p^n} - a \in K[x]$. Since $\deg(x^{p^n} - a) = \deg(f(x)) \geq 2$, we also have $n \geq 1$ and since $x^{p^n} - a \in K[x]$, we have $a \in K$. This completes the proof. $\square$

Problem 7. *Let F, K, S, P be as in Theorem 6.7 and suppose E is an intermediate field. Then*

(a): *F is purely inseparable over E if and only if $S \subseteq E$.*

(b): *If F is separable over E, then $P \subseteq E$.*

(c): *If $E \cap S = K$, then $E \subseteq P$.*

Note: Throughout these proofs, we have the tower of fields $K \subseteq S, P, E \subseteq F$.

Proof. (a): For the first direction, suppose that F/E is a purely inseparable extension and let $a \in S$. Since $a \in S$, we have by definition that a is separable over K so that $m_{K,a}(x) \in K[x]$ is a separable polynomial. Now, since F/E is purely inseparable, we have that $m_{E,a}(x) \in E[x]$ is purely inseparable. Since $m_{K,a}(x) \in K[x] \subseteq E[x]$ has a as a root, we must have that $m_{E,a}(x)$ divides $m_{K,a}(x)$. But since $m_{E,a}(x)$ is purely inseparable and since $m_{K,a}(x)$ is separable, it follows that $m_{E,a}(x)$ is linear so that $a \in E$. Since $a \in S$ was arbitrary, this proves that $S \subseteq E$. This completes the proof of the first direction.

For the second direction, suppose that $S \subseteq E$ and let $a \in F$. Since F/S is purely inseparable, we have that $m_{S,a}(x) \in S[x]$ is purely inseparable. Since $S \subseteq E$, we have that $m_{S,a}(x) \in S[x] \subseteq E[x]$. Hence, since $m_{S,a}(x) \in E[x]$ has a as a root, we must have that $m_{E,a}(x) \in E[x]$ divides $m_{S,a}(x)$. Since $m_{S,a}(x)$ is purely inseparable, it now follows that $m_{E,a}(x)$ is purely inseparable. Since $a \in F$ was arbitrary, this proves that F is purely inseparable over E. This completes the proof of the second direction. $\square$

Proof. (b): Let $a \in P$. Since $a \in P$, we have that $m_{K,a}(x)$ is purely inseparable. By the same argument as above, we have that $m_{E,a}(x)$ divides $m_{K,a}(x)$. Since F is separable over E, it follows that $m_{E,a}(x)$ is separable. But as $m_{K,a}(x)$ is purely inseparable and $m_{E,a}(x)$ divides $m_{K,a}(x)$, it follows that $m_{E,a}(x)$ is linear. In particular, this gives that $a \in E$. Since $a \in P$ was arbitrary, this proves that $P \subseteq E$. $\square$

Proof. (c): First, note that the set of separable elements of the extension E/K is equal to $E \cap S$ so that $E/E \cap S$ is a purely inseparable extension. But by hypothesis, we have that $E \cap S = K$ so that E/K is a purely inseparable extension. Now, let $a \in E$. Since E/K is purely inseparable, we have that a is purely inseparable over K. By definition, this gives that $a \in P$. Since $a \in E$ was arbitrary, this proves that $E \subseteq P$. $\square$

Homework 13: Page 288 #11, 12, 13

Problem 11. *If $f \in K[x]$ is irreducible of degree $m > 0$, and* $\mathrm{char}(K)$ *does not divides m, then f is separable.*

Proof. Since $f(x) \in K[x]$ is of degree $m > 0$, we can write

$$f(x) = a_m x^m + a_{m-1}x^{m-1} + \cdots + a_1 x + a_0$$

where $a_i \in K$ for $i \in \{0, \ldots, m\}$ so that

$$f'(x) = m a_m x^{m-1} + (m-1)a_{m-1}x^{m-2} + \cdots + a_1$$

In particular, consider the coefficient of x^{m-1} in $f'(x)$. This coefficient is ma_m and since $\mathrm{char}(K)$ does not divide m, it follows that $ma_m \neq 0$ so that $f'(x) \neq 0$. In particular, since $f(x) \in K[x]$ is irreducible, it follows that $f(x)$ is separable, completing the proof. $\square$

Problem 12. *F is purely inseparable over K if and only if F is algebraic over K and for any extension field E of F, the only K-monomorphism $F \to E$ is the inclusion map.*

Proof. For the first direction, assume that F is purely inseparable over K. By definition, we have that F is algebraic over K. Now, let E be a field extension of F so that we have the tower of fields $K \subseteq F \subseteq E$ and suppose that $\sigma : F \to E$ is a K-monomorphism. We will show that σ is the inclusion map.

Towards this end, let $a \in F$. Since F is purely inseparable over K, it follows that $m_{K,a}(x) = (x-a)^z$ for some positive integer $z \geq 1$. Now, since σ is a K-monomorphism and $m_{K,a}(x) \in K[x]$, we have that $\sigma(m_{K,a}(x)) = m_{K,a}(x)$. This gives

$$(x-a)^z = m_{K,a}(x) = \sigma(m_{K,a}(x)) = \sigma((x-a)^z) = (x-\sigma(a))^z$$

In particular, the above equality implies that $\sigma(a) = a$. Since $a \in F$ was arbitrary, this shows that $\sigma : F \to E$ is the inclusion map. This completes the proof of the first direction.

For the second direction, let E be an algebraic closure of K containing F so that we have the tower of fields $K \subseteq F \subseteq E$. For the sake of contradiction, suppose that F were not purely inseparable over K. Then there exists some $u \in F$ that is not purely inseparable over K. This implies that $m_{K,u}(x)$ is not purely inseparable. Now, let L be a splitting field for $m_{K,u}(x)$ over K such that $K \subseteq L \subseteq E$. Since $m_{K,u}(x)$ is not purely inseparable, there exists some root $v \in L$ of $m_{K,u}(x)$ such that $u \neq v$.

Next, note that there is some $\sigma \in \mathrm{Gal}(L/K)$ such that $\sigma(u) = v$. Furthermore, since E is an algebraic closure of L we see that the automorphism σ of L can be extended to an automorphism τ of E. In particular, since τ extends σ we have that $\tau \in \mathrm{Gal}(E/K)$. Finally, let $\mathrm{Res}(\tau) : F \to E$ denote the restriction of τ to F and note that $\mathrm{Res}(\tau)$ is a K-monomorphism $F \to E$ so that $\mathrm{Res}(\tau)$ is the inclusion map by hypothesis. In particular, since τ extends σ we now have

$$v = \sigma(u) = \mathrm{Res}(\tau)(u) = u$$

which contradicts the fact that $u \neq v$. Thus, we see F is purely inseparable over K. $\square$

Problem 13. (a): *The following conditions on a field K are equivalent:*

(i): *Every irreducible polynomial in $K[x]$ is separable.*

(ii): *Every algebraic closure $\overline{K}$ of K is Galois over K.*

(iii): *Every algebraic extension field of K is separable over K.*

(iv): *Either* $\mathrm{char}(K) = 0$ *or* $\mathrm{char}(K) = p$ *and* $K = K^p$.

(b): *Every finite field is perfect.*

Proof. (a): (i $\Rightarrow$ ii): Let $\overline{K}$ be an algebraic closure of K and note that $\overline{K}$ is an algebraic extension of K by definition. Now, since $\overline{K}$ is a splitting field for the set of irreducible polynomials in $K[x]$, it follows that $\overline{K}$ is a normal extension of K. Next, let $a \in \overline{K}$ and consider $m_{K,a}(x) \in K[x]$. Since $m_{K,a}(x) \in K[x]$ is irreducible, we have by hypothesis that $m_{K,a}(x)$ is separable so that a is separable. As $a \in \overline{K}$ was arbitrary, this shows that $\overline{K}$ is a separable extension of K. Finally, since $\overline{K}$ is a normal, separable extension of K, we have that $\overline{K}$ is Galois over K.

(ii $\Rightarrow$ iii): Let F be an algebraic extension of K and let $\overline{F}$ be an algebraic closure of F. Then we have the tower of fields $K \subseteq F \subseteq \overline{F}$. Since $\overline{F}$ is an algebraic extension of F by definition and since F is algebraic over K by hypothesis, we have that $\overline{F}$ is an algebraic extension of K. Hence, we have that $\overline{F}$ is an algebraic closure of K so that $\overline{F}$ is Galois over K by hypothesis. In particular, this implies that $\overline{F}$ is a separable extension of K. Finally, since $F \subseteq \overline{F}$ and since $\overline{F}$ is separable over K, we have that F is a separable extension of K.

(iii $\Rightarrow$ iv): Assume that $\mathrm{char}(K) \neq 0$ so that $\mathrm{char}(K) = p$ for some prime number p. Clearly, we have that $K^p \subseteq K$. On the other hand, let $a \in K$ and consider the polynomial $f(x) = x^p - a \in K[x]$. Let E be a splitting field for $f(x)$ over K and let $b \in E$ be a root of $f(x)$. Clearly, this gives that $b^p - a = 0$ so that $a = b^p$.

We now show that $b \in K$. Towards this end, notice that over E we have since $\mathrm{char}(K) = p$ that

$$f(x) = x^p - a = x^p - b^p = (x - b)^p$$

Since $f(x) \in K[x]$ and has b as a root, it follows that $m_{K,b}(x)$ divides $f(x)$. But recall that E is a splitting field for $f(x)$ over K so that E is an algebraic extension of K. By hypothesis, then, we have that E is separable over K. In particular, this implies that $m_{K,b}(x)$ is separable. But since $m_{K,b}(x)$ divides $f(x)$, we now have by the above equality that $m_{K,b}(x) = x - b \in K[x]$. Thus, we have that $b \in K$, as claimed. Finally, note that as $b \in K$ and $a = b^p$ that $a \in K^p$. As $a \in K$ was arbitrary, this gives that $K \subseteq K^p$ so that $K = K^p$.

(iv $\Rightarrow$ i): Let $f(x) \in K[x]$ be irreducible. If $\mathrm{char}(K) = 0$, then we have that $f(x)$ is separable since $f(x)$ is irreducible, completing the proof in this case. Now, assume that $\mathrm{char}(K) = p \neq 0$ for some prime number p. By hypothesis, we have that $K = K^p$. For the sake of contradiction, suppose that $f(x)$ is not separable. Since $f(x)$ is irreducible, this forces that $f'(x) = 0$. As $\mathrm{char}(K) = p$, this implies that $f(x)$ can be written

$$f(x) = a_n x^{pk_n} + a_{n-1} x^{pk_{n-1}} + \cdots + a_1 x^{pk_1} + a_0$$

where $a_i \in K$ for $i \in \{0, \ldots, n\}$ and $k_1, \ldots, k_n$ are positive integers. Since $K = K^p$, it follows that we may write $a_i = b_i^p$ for some $b_i \in K$ for each $i \in \{0, \ldots, n\}$. This implies that since $\text{char}(K) = p$ that

$$f(x) = b_n^p x^{pk_n} + b_{n-1}^p x^{pk_{n-1}} + \cdots + b_1^p x^{pk_1} + b_0^p = (b_n x^{k_n} + b_{n-1} x^{k_{n-1}} + \cdots + b_1 x^{k_1} + b_0)^p$$

However, since p is prime, we have $p \geq 2$ so that the above equality implies that $f(x)$ is irreducible over K which is a contradiction. We conclude that $f(x)$ is separable. $\square$

Proof. (b): Let K be a finite field. Since K is finite, we have that $\text{char}(K) = p$ for some prime number p. We claim that $K = K^p$. Clearly, as have that $K^p \subseteq K$. On the other hand, let $a \in K$. Since $\text{char}(K) = p$, it follows that $|K| = p^n$ for some positive integer n. Thus, since $a \in K$, this gives that $a^{p^n} = a$. Since $a^{p^{n-1}} \in K$, we have

$$a = a^{p^n} = (a^{p^{n-1}})^p \in K^p$$

so that $a \in K^p$. Hence, we have $K = K^p$ so that K is perfect. $\square$

Homework 14: Page 296 #2, 5, 7

Problem 2. *Let F be a finite dimensional extension of a finite field K. The norm N and the trace T (considered as maps $F \to K$) are surjective.*

Proof. Before beginning either proof, let $[F : K] = n$. Since F/K is a finite dimensional extension and as K is finite, it follows that F/K is a finite Galois extension and that $\mathrm{Gal}(F/K)$ is cyclic. Therefore, there is some $\sigma \in \mathrm{Gal}(F/K)$ such that $\mathrm{Gal}(F/K) = \{1, \sigma, \ldots, \sigma^{n-1}\}$.

We first show that N is surjective. Towards this end, first note that as K is a finite field that $|K| = p^m$ for some prime number p and some positive integer m. Let $q = p^m$. It follows that $\sigma : F \to F$ is defined by $\sigma(a) = a^q$ for all $a \in F$. Thus, if $u \in F$, we have

$$N(u) = \prod_{i=0}^{n-1} \sigma^i(u) = \prod_{i=0}^{n-1} u^{q^i} = u^{\sum_{i=0}^{n-1} q^i} = u^{\frac{q^n-1}{q-1}}$$

Now, since $[F : K] = n$ and as $|K| = q$, it follows that $|F| = q^n$ so that $|F^\times| = q^n - 1$. Since $F^\times$ is cyclic, there is a generator $u_0 \in F^\times$ of $F^\times$. By the above, we have in particular that

$$N(u_0) = u_0^{\frac{q^n-1}{q-1}}$$

Suppose that $[N(u_0)]^z = 1$ for some positive integer z. Then we have

$$1 = [N(u_0)]^z = \left(u_0^{\frac{q^n-1}{q-1}}\right)^z = u_0^{\frac{z(q^n-1)}{q-1}}$$

In particular, this equality implies that $|u_0| = q^n - 1$ divides $\frac{z(q^n-1)}{q-1}$ so that $q-1$ divides z. Since $q-1$ divides z, we have that $q - 1 \leq z$. On the other hand, we see that since $|u_0| = q^n - 1$ that

$$[N(u_0)]^{q-1} = \left(u_0^{\frac{q^n-1}{q-1}}\right)^{q-1} = u_0^{q^n-1} = 1$$

In particular, the above equality implies that $|N(u_0)| \leq q - 1$. By the above, this shows that $|N(u_0)| = q - 1$. Now, we have that $N(u_0) \in K$ is an element of order $q - 1$. Since $|K| = q$, we have that $|K^\times| = q - 1$. Thus, we have $K^\times = \langle N(u_0) \rangle$.

Finally, let $a \in K$. If $a = 0$, then $N(0) = 0 = a$. If $a \neq 0$, then $a \in K^\times$ so that by the above we have $a = [N(u_0)]^t$ for some nonnegative integer t. Since N is a multiplicative map, this gives

$$a = [N(u_0)]^t = N(u_0^t)$$

In particular, the previous results show that N is surjective.

We now show that T is surjective. Towards this end, recall that $T : F \to K$ is a K-linear map so that $T(F)$ is a sub K-vector space of K. In particular, this gives that $T(F) \in \{\{0\}, K\}$. If $T(F) = \{0\}$, it follows that

$$1 + \sigma + \cdots + \sigma^{n-1} = 0$$

which is a contradiction since the set $\{1, \sigma, \ldots, \sigma^{n-1}\}$ is linearly independent over F. Hence, we have $T(F) = K$ so that T is surjective. $\square$

Problem 5. *If F is a cyclic extension of K of degree p^n (p prime) and L is an intermediate field such that $F = L(u)$ and L is cyclic over K of degree p^{n-1}, then $F = K(u)$.*

Proof. Since F is a cyclic extension of K of order p^n, it follows that F is finite Galois over K and that $\mathrm{Gal}(F/K)$ is cyclic of order p^n. In particular, we note that FTGT applies to the extension F/K. Now, note that the divisors of p^n are exactly $1, p, \ldots, p^{n-1}, p^n$. Thus, since $\mathrm{Gal}(F/K)$ is cyclic of order p^n and p is a prime number, it follows that the subgroups of of $\mathrm{Gal}(F/K)$ can be written

$$\mathrm{Gal}(F/F) \subseteq \mathrm{Gal}(F/L_{n-1}) \subseteq \cdots \subseteq \mathrm{Gal}(F/L_1) \subseteq \mathrm{Gal}(F/K)$$

where $|\mathrm{Gal}(F/F)| = 1, |\mathrm{Gal}(F/L_{n-1})| = p, \ldots, |\mathrm{Gal}(F/L_1)| = p^{n-1}, |\mathrm{Gal}(F/K)| = p^n$, and $L_1, \ldots, L_{n-1}$ are intermediate fields of the extension F/K with

$$K \subseteq L_1 \subseteq \cdots \subseteq L_{n-1} \subseteq F$$

by FTGT.

Now, since $[F : K] = p^n$ and $[L : K] = p^{n-1}$, we have that

$$p^n = [F : K] = [F : L][L : K] = [F : L] \cdot p^{n-1}$$

so that $[F : L] = p$. By FTGT, this implies that $\mathrm{Gal}(F/L)$ is a subgroup of $\mathrm{Gal}(F/K)$ of order p. But since $\mathrm{Gal}(F/K)$ is a cyclic group, it follows that $\mathrm{Gal}(F/K)$ has a unique subgroup of order p so that $\mathrm{Gal}(F/L) = \mathrm{Gal}(F/L_{n-1})$ which implies that $L = L_{n-1}$. Thus, as $F = L(u)$, we now have $F = L_{n-1}(u)$.

Finally, for the sake of contradiction, suppose that $F \neq K(u)$. By FTGT, we know that $K, L_1, \ldots, L_{n-1}, F$ is a complete list of the intermediate fields of the extension F/K. Thus, since $K(u)$ is an intermediate field of F/K and since $F \neq K(u)$, it follows that $K(u) \in \{K, L_1, \ldots, L_{n-1}\}$. In any case, it follows by the above tower of fields that $u \in L_{n-1}$. Thus, we have $F = L_{n-1}(u) = L_{n-1}$ so that

$$p = |\mathrm{Gal}(F/L)| = |\mathrm{Gal}(F/L_{n-1})| = |\mathrm{Gal}(F/F)| = 1$$

which is clearly a contradiction since p is a prime number. We conclude that $F = K(u)$. This completes the proof. $\square$

Problem 7. *If n is an odd integer such that K contains a primitive nth root of unity and char$(K) \neq 2$, then K also contains a primitive $2n$th root of unity.*

Proof. Let $\zeta \in K$ be a primitive nth root of unity. Then

$$\langle \zeta \rangle = \{1, \zeta, \ldots, \zeta^{n-1}\}$$

Now, consider $-\zeta$. We claim that $-\zeta$ is a primitive $2n$th root of unity in K. First, note that since $\zeta \in K$ that $-\zeta \in K$. Furthermore, since ζ is an nth root of unity we have

$$(-\zeta)^{2n} = [(-\zeta)^2]^n = \zeta^n = 1$$

so that $-\zeta$ is a $2n$th root of unity.

It remains to prove that $-\zeta$ generates a group of order $2n$. Towards this end, note that since n is odd we have that $n-1$ is even so that

$$\langle -\zeta \rangle = \{-\zeta, \zeta^2, -\zeta^3, \ldots, \zeta^{n-1}, -1, \zeta, -\zeta^2, \zeta^3, \ldots, -\zeta^{n-1}, 1\}$$

Furthermore, since $\text{char}(K) \neq 2$, it follows that $-1 \neq 1, -\zeta \neq \zeta, \ldots, -\zeta^{n-1} \neq \zeta^{n-1}$. In particular, by the above equality, we now have $|\langle -\zeta \rangle| = 2n$ so that $-\zeta$ generates a group of order $2n$. Combining the above results, we see that $-\zeta \in K$ is a primitive $2n$th root of unity. This completes the proof. $\square$

Homework 15: Page 300 #1, 2, 3, 8, 9

Problem 1. *If $i \in \mathbb{Z}$, let $\overline{i}$ denote the image of i in $\mathbb{Z}_n$ under the canonical projection $\mathbb{Z} \to \mathbb{Z}_n$. Prove that $\overline{i}$ is a unit in the ring $\mathbb{Z}_n$ if and only if $(i, n) = 1$. Therefore the multiplicative group of units in $\mathbb{Z}_n$ has order $\phi(n)$.*

Proof. For the first direction, let $\overline{m}$ be a unit in $\mathbb{Z}_n$. Then there is some $\overline{z} \in \mathbb{Z}_n$ such that $\overline{z} \cdot \overline{m} = 1$. In particular, this shows that there is some $k \in \mathbb{Z}$ such that $mz = 1 + kn$. Thus, we have the equality

$$(z)m + (-k)n = 1$$

so that $(m, n) = 1$. This completes the proof of the first direction.

For the second direction, let $\overline{m} \in \mathbb{Z}_n$ and suppose that $(m, n) = 1$. Since $(m, n) = 1$, there exist $a, b \in \mathbb{Z}$ such that

$$(a)m + (b)n = 1$$

This equality gives that

$$am = 1 - bn$$

which implies that $\overline{a} \cdot \overline{m} = 1$. In particular, this implies that $\overline{m}$ is a unit in $\mathbb{Z}_n$.

By the above proof, we have that $\overline{m} \in \mathbb{Z}_n$ is a unit in $\mathbb{Z}_n$ if and only if $(m, n) = 1$. Since the number of positive integers that are relatively prime to n is precisely $\phi(n)$, we now have that $|\mathbb{Z}_n^\times| = \phi(n)$. This completes the proof. $\square$

Problem 2. *Establish the following properties of the Euler function ϕ.*
(a): *If p is prime and $n > 0$, then $\phi(p^n) = p^n(1 - 1/p) = p^{n-1}(p - 1)$.*
(b): *If $(m, n) = 1$, then $\phi(mn) = \phi(m)\phi(n)$.*
(c): *If $n = p_1^{k_1} \cdots p_r^{k_r}$ (p_i distinct primes, $k_i > 0$), then $\phi(n) = n(1-1/p_1)\cdots(1-1/p_r)$.*
(d): $\sum_{d|n} \phi(d) = n$.

Proof. (a): First, note that since p is prime the numbers that are not relatively prime to p^n are exactly the positive multiples of p. Since there are exactly $p^n/p = p^{n-1}$ positive multiples of p that are less than or equal to p^n, we now have

$$\phi(p^n) = p^n - p^{n-1} = p^{n-1}(p - 1) = p^n(1 - 1/p)$$

This completes the proof. □

Proof. (b): Since $(m, n) = 1$, we have by the Chinese Remainder Theorem that

$$\frac{\mathbb{Z}}{(mn)} = \frac{\mathbb{Z}}{(m)(n)} \simeq \frac{\mathbb{Z}}{(n)} \times \frac{\mathbb{Z}}{(m)}$$

Now, recall that $\phi(mn), \phi(m)$, and $\phi(n)$ are the number of units in the groups $\mathbb{Z}/(mn)$, $\mathbb{Z}/(m)$, and $\mathbb{Z}/(n)$, respectively. By the above isomorphism, we have that the number of units in $\mathbb{Z}/(mn)$ is equal to the number of units in $\mathbb{Z}/(n)$ multiplied by the number of units in $\mathbb{Z}/(m)$. Combining the previous two results, we obtain that $\phi(mn) = \phi(m)\phi(n)$. This completes the proof. □

Proof. (c): First, note that since the p_i are distinct primes that $p_1^{k_1}, \ldots, p_r^{k_r}$ are pairwise relatively prime. Thus, by Part (b) and Part (a), we obtain

$$\begin{aligned}
\phi(n) &= \phi(p_1^{k_1} \cdots p_r^{k_r}) \\
&= \phi(p_1^{k_1}) \cdots \phi(p_r^{k_r}) \\
&= p_1^{k_1}(1 - 1/p_1) \cdots p_r^{k_r}(1 - 1/p_r) \\
&= p_1^{k_1} \cdots p_r^{k_r}(1 - 1/p_1) \cdots (1 - 1/p_r) \\
&= n(1 - 1/p_1) \cdots (1 - 1/p_r)
\end{aligned}$$

This completes the proof. □

Proof. (d): Let $g_z(x)$ denote the zth cyclotomic polynomial over $\mathbb{Q}$ and consider the polynomial $x^n - 1 \in \mathbb{Q}[x]$. Then we have

$$n = \deg(x^n - 1) = \deg\left(\prod_{d|n} g_d(x)\right) = \sum_{d|n} \deg(g_d(x)) = \sum_{d|n} \phi(d)$$

This completes the proof. □

Problem 3. *Let ϕ be the Euler function.*

(a): *$\phi(n)$ is even for $n > 2$.*

(b): *Find all $n > 0$ such that $\phi(n) = 2$.*

Proof. (a): Let n be a positive integer with $n > 2$ and write $n = p_1^{k_1} \cdots p_r^{k_r}$, where $p_1 < \cdots < p_r$ are distinct primes and $k_1, \ldots, k_r$ are positive integers. First, consider if $n = 2^k$ for some positive integer k with $k \geq 2$. In this case, we have by the previous proof that

$$\phi(n) = \phi(2^k) = 2^{k-1}(2-1) = 2^{k-1}$$

Since $k \geq 2$, we have that $k - 1 \geq 1$ so that the above equality shows that $\phi(n)$ is even in this case.

Now, assume that n is not a power of 2. Then either $p_1 = 3$ or $p_2 = 3$. Furthermore, we have by the previous proof that

$$\phi(n) = \phi(p_1^{k_1} \cdots p_r^{k_r}) = p^{k_1-1}(p_1 - 1) \cdots p_r^{k_r-1}(p_r - 1)$$

By our previous observation, it must be the case that either $p_1 - 1 = 2$ or $p_2 - 1 = 2$. In either case, the above equality shows that 2 divides $\phi(n)$ so that $\phi(n)$ is even. Hence, in all cases, we conclude that $\phi(n)$ is even. $\square$

Proof. (b): Recall that if p is a prime number and n is a positive integer that $\phi(p^n) = p^{n-1}(p-1)$. In particular, if $p \geq 5$ then this equality shows that

$$\phi(p^n) \geq 5^{n-1}(5-1) \geq 4$$

This shows by the previous proof that if n is a positive integer that is divisible by a prime number greater than or equal to 5 that $\phi(n) > 2$ so that $\phi(n) \neq 2$. Thus, if $\phi(n) = 2$, we must have that $n = 2^m 3^k$ for some nonnegative integers m and k. Now, note the following:

If $m = 0 = k$, then $n = 1$ and so $\phi(n) \neq 2$.

If $m = 1$ and $k = 0$, then $n = 2$ and so $\phi(n) \neq 2$.

If $m = 0$ and $k = 1$, then $n = 3$ and so $\phi(n) = 2$.

If $m = 1 = k$, then $n = 6$ and so $\phi(n) = 2$.

If $m = 0$ and $k = 2$, then $n = 9$ and so $\phi(n) = 6 \neq 2$. In particular, this shows by the previous proof that $k \in \{0, 1\}$.

If $m = 2$ and $k = 0$, then $n = 4$ and so $\phi(n) = 2$.

If $m = 2$ and $k = 1$, then $n = 12$ and so $\phi(n) = 4 \neq 2$.

If $m = 3$ and $k = 0$, then $n = 8$ and so $\phi(n) = 4 \neq 2$. In particular, this shows by the previous proof that $m \in \{0, 1, 2\}$.

The previous results show that any positive integer candidate n such that $\phi(n) = 2$ is of the form $n = 2^m 3^k$, where $m \in \{0, 1, 2\}$ and $k \in \{0, 1\}$. Since we have tested all of these possibilities above, we conclude that the positive integers n such that $\phi(n) = 2$ are exactly $n = 3, 4, 6$. $\square$

Problem 8. *Let F_n be a cyclotomic extension of $\mathbb{Q}$ of order n.*

(a): *Determine* $\mathrm{Gal}(F_5/\mathbb{Q})$ *and all intermediate fields.*

(b): *Do the same for F_8.*

(c): *Do the same for F_7; if ζ is a primitive 7th root of unity what is the irreducible polynomial over $\mathbb{Q}$ of $\zeta + \zeta^{-1}$?*

Note: Before we begin, we note that $F_n/\mathbb{Q}$ is always a finite Galois extension so that FTGT applies the the extension $F_n/\mathbb{Q}$. We also know that $\mathrm{Gal}(F_n/\mathbb{Q}) \simeq \mathbb{Z}_n^\times$. Furthermore, if n is a prime number, then we know that $\mathrm{Gal}(F_n/\mathbb{Q})$ is a cyclic group. In this case, since $|\mathrm{Gal}(F_n/\mathbb{Q})| = |\mathbb{Z}_n^\times| = \phi(n)$ by the previously-established isomorphism, we obtain that $\mathrm{Gal}(F_n/\mathbb{Q}) \simeq \mathbb{Z}_{\phi(n)}$.

Proof. (a): First, note that since 5 is a prime number we have $\mathrm{Gal}(F_5/\mathbb{Q}) \simeq \mathbb{Z}_{\phi(5)} = \mathbb{Z}_4$.

We now find the intermediate fields of the extension $F_5/\mathbb{Q}$. By FTGT, we know that the intermediate fields of $F_5/\mathbb{Q}$ are in a bijective correspondence with the set of subgroups of $\mathbb{Z}_4$. Note that the subgroups of $\mathbb{Z}_4$ are exactly $\{0\}, \mathbb{Z}_2$, and $\mathbb{Z}_4$. Furthermore, we know that under the Galois correspondence we have

$$F_5 \mapsto \mathrm{Gal}(F_5/F_5) \simeq \{0\}$$

and

$$\mathbb{Q} \mapsto \mathrm{Gal}(F_5/\mathbb{Q}) \simeq \mathbb{Z}_4$$

Therefore, there is exactly one intermediate field K of the extension $F_5/\mathbb{Q}$ with $K \neq F_5$ and $K \neq \mathbb{Q}$.

Now, recall that $F_5 = \mathbb{Q}(\zeta)$, where ζ is a primitive 5th root of unity. By the above observations, we now have

$$K \mapsto \mathrm{Gal}(F_5/K) = \mathrm{Gal}(\mathbb{Q}(\zeta)/K) \simeq \mathbb{Z}_2$$

Since $\mathbb{Z}_2$ is a cyclic group of order 2, it now follows that $\mathrm{Gal}(\mathbb{Q}(\zeta)/K) = \langle\sigma\rangle$, where $\sigma : \mathbb{Q}(\zeta) \to \mathbb{Q}(\zeta)$ is such that $|\sigma| = 2$. In particular, this implies that $\sigma^2(\zeta) = \zeta$. Thus, since 5 is the smallest positive integer m such that $\zeta^m = 1$, we must have $\sigma(\zeta) = \zeta^4$. Finally, recall that by FTGT that K is the fixed field of $\langle\sigma\rangle$. But since $|\sigma| = 2$, we have $\langle\sigma\rangle = \{1, \sigma\}$. Combining these observations, we obtain that

$$K = \{u \in \mathbb{Q}(\zeta) : \sigma(u) = u\}$$

First, let $u \in K$. Then $\sigma(u) = u$ since $u \in K$ and

$$u = q_0 + q_1\zeta + q_2\zeta^2 + q_3\zeta^3 + q_4\zeta^4$$

for some $q_0, q_1, q_2, q_3, q_4 \in \mathbb{Q}$ since $u \in \mathbb{Q}(\zeta)$. By the definition of σ, we obtain

$$\begin{aligned}
q_0 + q_1\zeta + q_2\zeta^2 + q_3\zeta^3 + q_4\zeta^4 &= \sigma(q_0 + q_1\zeta + q_2\zeta^2 + q_3\zeta^3 + q_4\zeta^4) \\
&= q_0 + q_1\sigma(\zeta) + q_2\sigma(\zeta^2) + q_3\sigma(\zeta^3) + q_4\sigma(\zeta^4) \\
&= q_0 + q_1\zeta^4 + q_2\zeta^8 + q_3\zeta^{12} + q_4\zeta^{16} \\
&= q_0 + q_4\zeta + q_3\zeta^2 + q_2\zeta^3 + q_1\zeta^4
\end{aligned}$$

so that $q_1 = q_4$ and $q_2 = q_3$. Thus, we obtain

$$u = q_0 + q_1(\zeta + \zeta^4) + q_2(\zeta^2 + \zeta^3)$$

But since $\zeta^2 + \zeta^3 = (\zeta + \zeta^4)^2 - 2 \in \mathbb{Q}(\zeta + \zeta^4)$, we obtain $u \in \mathbb{Q}(\zeta + \zeta^4)$.

On the other hand, suppose that $u \in \mathbb{Q}(\zeta+\zeta^4)$. Then we can write $u = p+q(\zeta+\zeta^4)$ for some $p, q \in \mathbb{Q}$. By the definition of σ, we obtain

$$\begin{aligned}\sigma(u) &= \sigma(p + q(\zeta + \zeta^4)) \\ &= p + q(\sigma(\zeta) + \sigma(\zeta^4)) \\ &= p + q(\zeta^4 + \zeta^{16}) \\ &= p + q(\zeta + \zeta^4) \\ &= u\end{aligned}$$

so that $u \in K$. The previous results show that $K = \mathbb{Q}(\zeta + \zeta^4)$ so that the intermediate fields of the extension $F_5/\mathbb{Q}$ are $F_5, \mathbb{Q}(\zeta + \zeta^4)$, and $\mathbb{Q}$. This completes the proof. $\square$

Proof. (b): First, note that $\mathrm{Gal}(F_8/\mathbb{Q}) \simeq \mathbb{Z}_8^\times = \{1, 3, 5, 7\}$. Since $|3| = |5| = |7| = 2$, it follows that every nonidentity element of $\mathbb{Z}_8^\times$ is of order 2. Hence, we see

$$\mathrm{Gal}(F_8/\mathbb{Q}) \simeq \mathbb{Z}_8^\times \simeq V_4$$

so that $\mathrm{Gal}(F_8/\mathbb{Q}) \simeq V_4$.

We now find the intermediate fields of the extension $F_8/\mathbb{Q}$. By FTGT, we know that the intermediate fields of $F_8/\mathbb{Q}$ are in a bijective correspondence with the set of subgroups of V_4. Note that the subgroups of V_4 are exactly $\{0\}, S_1, S_2, S_3$, and V_4, where S_1, S_2, and S_3 are distinct subgroups of V_4 of order 2. Furthermore, we know that under the Galois correspondence we have

$$F_8 \mapsto \mathrm{Gal}(F_8/F_8) \simeq \{0\}$$

and

$$\mathbb{Q} \mapsto \mathrm{Gal}(F_8/\mathbb{Q}) \simeq V_4$$

Therefore, there are exactly three distinct intermediate fields K_1, K_2, and K_3 of the extension $F_8/\mathbb{Q}$ with $K_1, K_2, K_3 \neq F_5$ and $K_1, K_2, K_3 \neq \mathbb{Q}$.

Now, recall that $F_8 = \mathbb{Q}(\zeta)$, where ζ is a primitive 8th root of unity. By the above observations, we now have

$$K_1 \mapsto \mathrm{Gal}(F_8/K_1) = \mathrm{Gal}(\mathbb{Q}(\zeta)/K_1) \simeq S_1$$

and

$$K_2 \mapsto \mathrm{Gal}(F_8/K_2) = \mathrm{Gal}(\mathbb{Q}(\zeta)/K_2) \simeq S_2$$

and

$$K_3 \mapsto \mathrm{Gal}(F_8/K_3) = \mathrm{Gal}(\mathbb{Q}(\zeta)/K_3) \simeq S_3$$

Since S_1, S_2, and S_3 are cyclic groups of order 2, it now follows that $\mathrm{Gal}(\mathbb{Q}(\zeta)/K_1) = \langle\sigma_1\rangle, \mathrm{Gal}(\mathbb{Q}(\zeta)/K_2) = \langle\sigma_2\rangle$, and $\mathrm{Gal}(\mathbb{Q}(\zeta)/K_3) = \langle\sigma_3\rangle$, where $\sigma_1, \sigma_2, \sigma_3 : \mathbb{Q}(\zeta) \to \mathbb{Q}(\zeta)$ are such that $|\sigma_1| = |\sigma_2| = |\sigma_3| = 2$. In particular, this implies that $\sigma_1^2(\zeta) = \sigma_2^2(\zeta) = \sigma_3^2(\zeta) = \zeta$. Thus, since 8 is the smallest positive integer m such that $\zeta^m = 1$, we must

have without loss of generality that $\sigma_1(\zeta) = \zeta^3, \sigma_2(\zeta) = \zeta^5$, and $\sigma_3(\zeta) = \zeta^7$. Finally, recall that by FTGT that K_1, K_2, and K_3 are the fixed fields of $\langle\sigma_1\rangle, \langle\sigma_2\rangle$, and $\langle\sigma_3\rangle$, respectively. But since $|\sigma_1| = |\sigma_2| = |\sigma_3| = 2$, we have $\langle\sigma_1\rangle = \{1, \sigma_1\}, \langle\sigma_2\rangle = \{1, \sigma_2\}$, and $\langle\sigma_3\rangle = \{1, \sigma_3\}$. Combining these observations, we obtain that

$$K_1 = \{u \in \mathbb{Q}(\zeta) : \sigma_1(u) = u\}$$

and

$$K_2 = \{u \in \mathbb{Q}(\zeta) : \sigma_2(u) = u\}$$

and

$$K_3 = \{u \in \mathbb{Q}(\zeta) : \sigma_3(u) = u\}$$

First, let $u \in K_1$. Then $\sigma_1(u) = u$ since $u \in K_1$ and

$$u = q_0 + q_1\zeta + q_2\zeta^2 + q_3\zeta^3$$

for some $q_0, q_1, q_2, q_3 \in \mathbb{Q}$ since $u \in \mathbb{Q}(\zeta)$. By the definition of σ_1, we obtain

$$\begin{aligned} q_0 + q_1\zeta + q_2\zeta^2 + q_3\zeta^3 &= \sigma_1(q_0 + q_1\zeta + q_2\zeta^2 + q_3\zeta^3 + q_4\zeta^4) \\ &= q_0 + q_1\sigma_1(\zeta) + q_2\sigma_1(\zeta^2) + q_3\sigma_1(\zeta^3) \\ &= q_0 + q_1\zeta^3 + q_2\zeta^6 + q_3\zeta^9 \\ &= q_0 + q_1\zeta^3 - q_2\zeta^2 + q_3\zeta \\ &= q_0 + q_3\zeta + (-q_2)\zeta^2 + q_1\zeta^3 \end{aligned}$$

so that $q_1 = q_3$ and $q_2 = -q_2$. In particular, the latter of these two equalities implies that $q_2 = 0$. Thus, we obtain

$$u = q_0 + q_1(\zeta + \zeta^3)$$

so that $u \in \mathbb{Q}(\zeta + \zeta^3)$.

On the other hand, suppose that $u \in \mathbb{Q}(\zeta+\zeta^3)$. Then we can write $u = p+q(\zeta+\zeta^3)$ for some $p, q \in \mathbb{Q}$. By the definition of σ_1, we obtain

$$\begin{aligned} \sigma_1(u) &= \sigma_1(p + q(\zeta + \zeta^3)) \\ &= p + q(\sigma_1(\zeta) + \sigma_1(\zeta^3)) \\ &= p + q(\zeta^3 + \zeta^9) \\ &= p + q(\zeta + \zeta^3) \\ &= u \end{aligned}$$

so that $u \in K_1$. The previous results show that $K_1 = \mathbb{Q}(\zeta + \zeta^3)$.

Second, let $u \in K_2$. Then $\sigma_2(u) = u$ since $u \in K_2$ and

$$u = q_0 + q_1\zeta + q_2\zeta^2 + q_3\zeta^3$$

for some $q_0, q_1, q_2, q_3 \in \mathbb{Q}$ since $u \in \mathbb{Q}(\zeta)$. By the definition of σ_2, we obtain

$$\begin{aligned} q_0 + q_1\zeta + q_2\zeta^2 + q_3\zeta^3 &= \sigma_2(q_0 + q_1\zeta + q_2\zeta^2 + q_3\zeta^3 + q_4\zeta^4) \\ &= q_0 + q_1\sigma_2(\zeta) + q_2\sigma_2(\zeta^2) + q_3\sigma_2(\zeta^3) \\ &= q_0 + q_1\zeta^5 + q_2\zeta^{10} + q_3\zeta^{15} \\ &= q_0 - q_1\zeta + q_2\zeta^2 - q_3\zeta^3 \\ &= q_0 + (-q_1)\zeta + q_2\zeta^2 + (-q_3)\zeta^3 \end{aligned}$$

so that $q_1 = -q_1$ and $q_3 = -q_3$. In particular, these two equalities imply that $q_1 = 0 = q_3$. Thus, we obtain

$$u = q_0 + q_2\zeta^2$$

so that $u \in \mathbb{Q}(\zeta^2)$.

On the other hand, suppose that $u \in \mathbb{Q}(\zeta^2)$. Then we can write $u = p + q\zeta^2$ for some $p, q \in \mathbb{Q}$. By the definition of σ_2, we obtain

$$\begin{aligned} \sigma_2(u) &= \sigma_2(p + q\zeta^2) \\ &= p + q\sigma_2(\zeta^2) \\ &= p + q\zeta^{10} \\ &= p + q\zeta^2 \\ &= u \end{aligned}$$

so that $u \in K_2$. The previous results show that $K_2 = \mathbb{Q}(\zeta^2)$.

Third, let $u \in K_3$. Then $\sigma_3(u) = u$ since $u \in K_3$ and

$$u = q_0 + q_1\zeta + q_2\zeta^2 + q_3\zeta^3$$

for some $q_0, q_1, q_2, q_3 \in \mathbb{Q}$ since $u \in \mathbb{Q}(\zeta)$. By the definition of σ_3, we obtain

$$\begin{aligned} q_0 + q_1\zeta + q_2\zeta^2 + q_3\zeta^3 &= \sigma_3(q_0 + q_1\zeta + q_2\zeta^2 + q_3\zeta^3 + q_4\zeta^4) \\ &= q_0 + q_1\sigma_3(\zeta) + q_2\sigma_3(\zeta^2) + q_3\sigma_3(\zeta^3) \\ &= q_0 + q_1\zeta^7 + q_2\zeta^{14} + q_3\zeta^{21} \\ &= q_0 - q_1\zeta^3 - q_2\zeta^2 - q_3\zeta \\ &= q_0 + (-q_3)\zeta + (-q_2)\zeta^2 + (-q_1)\zeta^3 \end{aligned}$$

so that $q_1 = -q_3$ and $q_2 = -q_2$. In particular, the latter of these two equalities implies that $q_2 = 0$. Thus, we obtain

$$u = q_0 + q_1(\zeta - \zeta^3) = \mathbb{Q}(\zeta + \zeta^7)$$

so that $u \in \mathbb{Q}(\zeta + \zeta^7)$.

On the other hand, suppose that $u \in \mathbb{Q}(\zeta+\zeta^7)$. Then we can write $u = p+q(\zeta+\zeta^7)$ for some $p, q \in \mathbb{Q}$. By the definition of σ_1, we obtain

$$\begin{aligned}\sigma_1(u) &= \sigma_1(p + q(\zeta + \zeta^7)) \\ &= p + q(\sigma_1(\zeta) + \sigma_1(\zeta^7)) \\ &= p + q(\zeta^7 + \zeta^4 9) \\ &= p + q(\zeta + \zeta^7) \\ &= u\end{aligned}$$

so that $u \in K_3$. The previous results show that $K_3 = \mathbb{Q}(\zeta + \zeta^7)$.

In conclusion, we obtain that the intermediate fields of the extension $F_8/\mathbb{Q}$ are $F_8, \mathbb{Q}(\zeta + \zeta^3), \mathbb{Q}(\zeta^2), \mathbb{Q}(\zeta + \zeta^7)$, and $\mathbb{Q}$. This completes the proof. □

Proof. (c): First, note that since 7 is a prime number we have $\mathrm{Gal}(F_7/\mathbb{Q}) \simeq \mathbb{Z}_{\phi(7)} = \mathbb{Z}_6$.

We now find the intermediate fields of the extension $F_7/\mathbb{Q}$. By FTGT, we know that the intermediate fields of $F_7/\mathbb{Q}$ are in a bijective correspondence with the set of subgroups of $\mathbb{Z}_6$. Note that the subgroups of $\mathbb{Z}_6$ are exactly $\{0\}, S_1, S_2$, and V_4, where S_1 is a subgroup of $\mathbb{Z}_6$ of order 2 and S_2 is a subgroup of $\mathbb{Z}_6$ of order 3. Furthermore, we know that under the Galois correspondence we have

$$F_7 \mapsto \mathrm{Gal}(F_7/F_7) \simeq \{0\}$$

and

$$\mathbb{Q} \mapsto \mathrm{Gal}(F_7/\mathbb{Q}) \simeq \mathbb{Z}_6$$

Therefore, there are exactly two distinct intermediate fields K_1 and K_2 of the extension $F_7/\mathbb{Q}$ with $K_1, K_2 \neq F_7$ and $K_1, K_2 \neq \mathbb{Q}$.

Now, recall that $F_7 = \mathbb{Q}(\zeta)$, where ζ is a primitive 7th root of unity. By the above observations, we now have

$$K_1 \mapsto \mathrm{Gal}(F_7/K_1) = \mathrm{Gal}(\mathbb{Q}(\zeta)/K_1) \simeq S_1$$

and

$$K_2 \mapsto \mathrm{Gal}(F_7/K_2) = \mathrm{Gal}(\mathbb{Q}(\zeta)/K_2) \simeq S_2$$

Since S_1 and S_2 are cyclic groups of order 2 and 3, respectively, it now follows that $\mathrm{Gal}(\mathbb{Q}(\zeta)/K_1) = \langle\sigma_1\rangle$ and $\mathrm{Gal}(\mathbb{Q}(\zeta)/K_2) = \langle\sigma_2\rangle$, where $\sigma_1, \sigma_2 : \mathbb{Q}(\zeta) \to \mathbb{Q}(\zeta)$ are such that $|\sigma_1| = 2$ and $|\sigma_2| = 3$. In particular, this implies that $\sigma_1^2(\zeta) = \zeta = \sigma_2^3(\zeta)$. Thus, since 7 is the smallest positive integer m such that $\zeta^m = 1$, we must have that $\sigma_1(\zeta) = \zeta^6$ and $\sigma_2(\zeta) = \zeta^2$. Finally, recall that by FTGT that K_1 and K_2 are the fixed fields of $\langle\sigma_1\rangle$ and $\langle\sigma_2\rangle$, respectively. But since $|\sigma_1| = 2$ and $|\sigma_2| = 3$, we have $\langle\sigma_1\rangle = \{1, \sigma_1\}$ and $\langle\sigma_2\rangle = \{1, \sigma_2, \sigma_2^2\}$. Combining these observations, we obtain that

$$K_1 = \{u \in \mathbb{Q}(\zeta) : \sigma_1(u) = u\}$$

and

$$K_2 = \{u \in \mathbb{Q}(\zeta) : \sigma_2(u) = u = \sigma_2^2(u)\}$$

First, let $u \in K_1$. Then $\sigma_1(u) = u$ since $u \in K_1$ and

$$u = q_0 + q_1\zeta + q_2\zeta^2 + q_3\zeta^3 + q_4\zeta^4 + q_5\zeta^5 + q_6\zeta^6$$

for some $q_0, q_1, q_2, q_3, q_4, q_5, q_6 \in \mathbb{Q}$ since $u \in \mathbb{Q}(\zeta)$. By the definition of σ_1, we obtain

$$\begin{aligned} q_0 + q_1\zeta + q_2\zeta^2 + q_3\zeta^3 + q_4\zeta^4 + q_5\zeta^5 + q_6\zeta^6 &= \sigma_1(q_0 + q_1\zeta + q_2\zeta^2 + q_3\zeta^3 + q_4\zeta^4 + q_5\zeta^5 + q_6\zeta^6) \\ &= q_0 + q_1\sigma_1(\zeta) + q_2\sigma_1(\zeta^2) + q_3\sigma_1(\zeta^3) + q_4\sigma_1(\zeta^4) + q_5\sigma_1(\zeta^5) + q_6\sigma_1(\zeta^6) \\ &= q_0 + q_1\zeta^6 + q_2\zeta^{12} + q_3\zeta^{18} + q_4\zeta^{24} + q_5\zeta^{30} + q_6\zeta^{36} \\ &= q_0 + q_1\zeta^6 + q_2\zeta^5 + q_3\zeta^4 + q_4\zeta^3 + q_5\zeta^2 + q_6\zeta \\ &= q_0 + q_6\zeta + q_5\zeta^2 + q_4\zeta^3 + q_3\zeta^4 + q_2\zeta^5 + q_1\zeta^6 \end{aligned}$$

so that $q_1 = q_6, q_2 = q_5$, and $q_3 = q_4$. Thus, we obtain

$$u = q_0 + q_1(\zeta + \zeta^6) + q_2(\zeta^2 + \zeta^5) + q_3(\zeta^3 + \zeta^4)$$

But notice that

$$(\zeta + \zeta^6)^2 = \zeta^2 + 2\zeta^7 + \zeta^{12} = 2 + \zeta^2 + \zeta^5$$

so that

$$\zeta^2 + \zeta^5 = (\zeta + \zeta^6)^2 - 2 \in \mathbb{Q}(\zeta + \zeta^6)$$

and that

$$\begin{aligned} (\zeta + \zeta^6)^3 &= (\zeta + \zeta^6)(2 + \zeta^2 + \zeta^5) \\ &= 2\zeta + \zeta^3 + \zeta^6 + 2\zeta^6 + \zeta^8 + \zeta^{11} \\ &= 2\zeta + \zeta^3 + 3\zeta^6 + \zeta + \zeta^4 \\ &= 3\zeta + \zeta^3 + \zeta^4 + 3\zeta^6 \\ &= \zeta^3 + \zeta^4 + 3(\zeta + \zeta^6) \end{aligned}$$

so that

$$\zeta^3 + \zeta^4 = (\zeta + \zeta^6)^3 - 3(\zeta + \zeta^6) \in \mathbb{Q}(\zeta + \zeta^6)$$

The above results show that $u \in \mathbb{Q}(\zeta + \zeta^6)$.

On the other hand, suppose that $u \in \mathbb{Q}(\zeta + \zeta^6)$. Then we can write $u = p + q(\zeta + \zeta^6)$ for some $p, q \in \mathbb{Q}$. By the definition of σ_1, we obtain

$$\begin{aligned} \sigma_1(u) &= \sigma_1(p + q(\zeta + \zeta^6)) \\ &= p + q(\sigma_1(\zeta) + \sigma_1(\zeta^6)) \\ &= p + q(\zeta^6 + \zeta^{36}) \\ &= p + q(\zeta + \zeta^6) \\ &= u \end{aligned}$$

so that $u \in K_1$. The previous results show that $K_1 = \mathbb{Q}(\zeta + \zeta^6)$.

Second, let $u \in K_2$. Then $\sigma_2(u) = u = \sigma_2^2(u)$ since $u \in K_2$ and

$$u = q_0 + q_1\zeta + q_2\zeta^2 + q_3\zeta^3 + q_4\zeta^4 + q_5\zeta^5 + q_6\zeta^6$$

for some $q_0, q_1, q_2, q_3, q_4, q_5, q_6 \in \mathbb{Q}$ since $u \in \mathbb{Q}(\zeta)$. By the definition of σ_2, we obtain

$$\begin{aligned} q_0 + q_1\zeta + q_2\zeta^2 + q_3\zeta^3 + q_4\zeta^4 + q_5\zeta^5 + q_6\zeta^6 &= \sigma_2(q_0 + q_1\zeta + q_2\zeta^2 + q_3\zeta^3 + q_4\zeta^4 + q_5\zeta^5 + q_6\zeta^6) \\ &= q_0 + q_1\sigma_2(\zeta) + q_2\sigma_2(\zeta^2) + q_3\sigma_2(\zeta^3) + q_4\sigma_2(\zeta^4) + q_5\sigma_2(\zeta^5) + q_6\sigma_2(\zeta^6) \\ &= q_0 + q_1\zeta^2 + q_2\zeta^4 + q_3\zeta^6 + q_4\zeta^8 + q_5\zeta^{10} + q_6\zeta^{12} \\ &= q_0 + q_1\zeta^2 + q_2\zeta^4 + q_3\zeta^6 + q_4\zeta + q_5\zeta^3 + q_6\zeta^5 \\ &= q_0 + q_4\zeta + q_1\zeta^2 + q_5\zeta^3 + q_2\zeta^4 + q_6\zeta^5 + q_3\zeta^6 \end{aligned}$$

and

$$\begin{aligned} q_0 + q_1\zeta + q_2\zeta^2 + q_3\zeta^3 + q_4\zeta^4 + q_5\zeta^5 + q_6\zeta^6 &= \sigma_2^2(q_0 + q_1\zeta + q_2\zeta^2 + q_3\zeta^3 + q_4\zeta^4 + q_5\zeta^5 + q_6\zeta^6) \\ &= q_0 + q_1\sigma_2^2(\zeta) + q_2\sigma_2^2(\zeta^2) + q_3\sigma_2^2(\zeta^3) + q_4\sigma_2^2(\zeta^4) + q_5\sigma_2^2(\zeta^5) + q_6\sigma_2^2(\zeta^6) \\ &= q_0 + q_1\zeta^4 + q_2\zeta^8 + q_3\zeta^{12} + q_4\zeta^{16} + q_5\zeta^{20} + q_6\zeta^{24} \\ &= q_0 + q_1\zeta^4 + q_2\zeta + q_3\zeta^5 + q_4\zeta^2 + q_5\zeta^6 + q_6\zeta^3 \\ &= q_0 + q_2\zeta + q_4\zeta^2 + q_6\zeta^3 + q_5\zeta^4 + q_3\zeta^5 + q_5\zeta^6 \end{aligned}$$

so that $q_1 = q_4 = q_2$ and $q_3 = q_5 = q_6$. Thus, we obtain

$$u = q_0 + q_1(\zeta + \zeta^2 + \zeta^4) + q_2(\zeta^3 + \zeta^5 + \zeta^6)$$

But notice that

$$\begin{aligned} (\zeta + \zeta^2 + \zeta^4)^2 &= \zeta^2 + \zeta^3 + \zeta^5 + \zeta^3 + \zeta^4 + \zeta^6 + \zeta^5 + \zeta^6 + \zeta^8 \\ &= 2\zeta^3 + 2\zeta^5 + 2\zeta^6 + \zeta + \zeta^2 + \zeta^4 \end{aligned}$$

so that

$$\zeta^3 + \zeta^5 + \zeta^6 = \frac{1}{2}[(\zeta + \zeta^2 + \zeta^4)^2 - (\zeta + \zeta^2 + \zeta^4)] \in \mathbb{Q}(\zeta + \zeta^6)$$

The above results show that $u \in \mathbb{Q}(\zeta + \zeta^2 + \zeta^4)$.

On the other hand, suppose that $u \in \mathbb{Q}(\zeta + \zeta^2 + \zeta^4)$. Then we can write $u = p + q(\zeta + \zeta^2 + \zeta^4)$ for some $p, q \in \mathbb{Q}$. By the definition of σ_2, we obtain

$$\begin{aligned} \sigma_2(u) &= \sigma_2(p + q(\zeta + \zeta^2 + \zeta^4)) \\ &= p + q(\sigma_2(\zeta) + \sigma_2(\zeta^2) + \sigma_2(\zeta^4)) \\ &= p + q(\zeta^2 + \zeta^4 + \zeta^8) \\ &= p + q(\zeta + \zeta^2 + \zeta^4) \\ &= u \end{aligned}$$

and

$$\begin{aligned} \sigma_2^2(u) &= \sigma_2^2(p + q(\zeta + \zeta^2 + \zeta^4)) \\ &= p + q(\sigma_2^2(\zeta) + \sigma_2^2(\zeta^2) + \sigma_2^2(\zeta^4)) \\ &= p + q(\zeta^4 + \zeta^8 + \zeta^{16}) \\ &= p + q(\zeta + \zeta^2 + \zeta^4) \\ &= u \end{aligned}$$

so that $u \in K_2$. The previous results show that $K_2 = \mathbb{Q}(\zeta + \zeta^2 + \zeta^4)$.

In conclusion, we obtain that the intermediate fields of the extension $F_7/\mathbb{Q}$ are $F_7, \mathbb{Q}(\zeta + \zeta^6), \mathbb{Q}(\zeta + \zeta^2 + \zeta^4)$, and $\mathbb{Q}$. This completes the proof.

We now find the minimum polynomial over $\mathbb{Q}$ of $\zeta + \zeta^{-1} = \zeta + \zeta^6$. Towards this end, notice that since $1 + \zeta + \zeta^2 + \zeta^3 + \zeta^4 + \zeta^5 + \zeta^6 = 0$ we have

$$\zeta + \zeta^6 = -1 - \zeta^2 - \zeta^3 - \zeta^4 - \zeta^5$$

and

$$(\zeta + \zeta^6)^2 = 2 + \zeta^2 + \zeta^5$$

and

$$\begin{aligned}
(\zeta + \zeta^6)^3 &= (\zeta + \zeta^6)(2 + \zeta^2 + \zeta^5) \\
&= 2\zeta + \zeta^3 + \zeta^6 + 2\zeta^6 + \zeta^8 + \zeta^{11} \\
&= 2\zeta + \zeta^3 + \zeta^6 + 2\zeta^6 + \zeta + \zeta^4 \\
&= 3\zeta + \zeta^3 + \zeta^4 + 3\zeta^6 \\
&= 3(-1 - \zeta^2 - \zeta^3 - \zeta^4 - \zeta^5 - \zeta^6) + \zeta^3 + \zeta^4 + 3\zeta^6 \\
&= -3 - 3\zeta^2 - 2\zeta^3 - 2\zeta^4 - 3\zeta^5
\end{aligned}$$

so that

$$(\zeta + \zeta^6)^3 + (\zeta + \zeta^6)^2 - 2(\zeta + \zeta^6) - 1 = 0$$

Finally, define $p(x) \in \mathbb{Q}[x]$ by $p(x) = x^3 + x^2 - 2x - 1$. Note that by the above calculation we have that $\zeta + \zeta^{-1} = \zeta + \zeta^6$ is a root of $p(x)$. Futhermore, by the Rational Root Theorem, we have that $p(x)$ has no rational roots. Since $\deg(p(x)) = 3$, this observation implies that $p(x)$ is irreducible over $\mathbb{Q}$. Thus, since $p(x) \in \mathbb{Q}[x]$ is an irreducible, monic polynomial that has $\zeta + \zeta^{-1}$ as a root, it follows that $p(x)$ is the minimum polynomial for $\zeta + \zeta^{-1}$ over $\mathbb{Q}$. This completes the proof. $\square$

Problem 9. *If $n > 2$ and ζ is a primitive nth root of unity over $\mathbb{Q}$, then $[\mathbb{Q}(\zeta + \zeta^{-1}) : \mathbb{Q}] = \phi(n)/2$.*

Proof. As ζ is a primitive nth root of unity over $\mathbb{Q}$, we know that $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \phi(n)$. Now, note that we have the tower of fields $\mathbb{Q} \subseteq \mathbb{Q}(\zeta + \zeta^{-1}) \subseteq \mathbb{Q}(\zeta)$ so that

$$\phi(n) = [\mathbb{Q}(\zeta) : \mathbb{Q}] = [\mathbb{Q}(\zeta) : \mathbb{Q}(\zeta + \zeta^{-1})][\mathbb{Q}(\zeta + \zeta^{-1}) : \mathbb{Q}]$$

so that

$$[\mathbb{Q}(\zeta + \zeta^{-1}) : \mathbb{Q}] = \frac{\phi(n)}{[\mathbb{Q}(\zeta) : \mathbb{Q}(\zeta + \zeta^{-1})]}$$

Thus, the proof is complete if we show that $[\mathbb{Q}(\zeta) : \mathbb{Q}(\zeta + \zeta^{-1})] = 2$.

Now, note that $\mathbb{Q}(\zeta) = \mathbb{Q}(\zeta, \zeta + \zeta^{-1})$ so that $[\mathbb{Q}(\zeta) : \mathbb{Q}(\zeta + \zeta^{-1})]$ is the degree of the minimum polynomial for ζ over $\mathbb{Q}(\zeta + \zeta^{-1})$. Notice that $\zeta \notin \mathbb{Q}(\zeta + \zeta^{-1})$ since ζ is a primitive nth root of unity and $n > 2$ by hypothesis. In particular, this implies that $[\mathbb{Q}(\zeta) : \mathbb{Q}(\zeta + \zeta^{-1})] \geq 2$ so that the degree of the minimum polynomial for ζ over $\mathbb{Q}(\zeta + \zeta^{-1})$ is of degree at least 2.

Finally, consider the polynomial $p(x) \in \mathbb{Q}(\zeta + \zeta^{-1})[x]$ given by

$$p(x) = (\zeta + \zeta^{-1})x^2 - (\zeta + \zeta^{-1})^2 x + (\zeta + \zeta^{-1})$$

and note that

$$\begin{aligned} p(\zeta) &= (\zeta + \zeta^{-1})\zeta^2 - (\zeta + \zeta^{-1})^2\zeta + (\zeta + \zeta^{-1}) \\ &= (\zeta + \zeta^{-1})\zeta^2 - (\zeta^2 + \zeta^{-2} + 2)\zeta + (\zeta + \zeta^{-1}) \\ &= \zeta^3 + \zeta - \zeta^3 - \zeta^{-1} - 2\zeta + \zeta + \zeta^{-1} \\ &= 0 \end{aligned}$$

The above computation implies that the minimum polynomial for ζ over $\mathbb{Q}(\zeta + \zeta^{-1})$ must divide $p(x)$. But recall that the degree of the minimum polynomial for ζ over $\mathbb{Q}(\zeta + \zeta^{-1})$ is of degree at least 2 and that $p(x)$ is of degree 2. Hence, we conclude that the degree of the minimum polynomial for ζ over $\mathbb{Q}(\zeta + \zeta^{-1})$ is equal to 2 so that $[\mathbb{Q}(\zeta) : \mathbb{Q}(\zeta + \zeta^{-1})] = 2$. This completes the proof. $\square$

Homework 16: Page 317 #2, 3, 6

Problem 2. (a): *Use Zorn's Lemma to show that every field extension possesses a transcendence base.*

(b): *Show that every algebraically independent subset of F is contained in a transcendence base.*

Proof. (a): Let F/K be a field extension. Define

$$\mathcal{S} = \{S \subseteq F : S \text{ is algebraically independent over } K\}$$

and order $\mathcal{S}$ by for $S_1, S_2 \in \mathcal{S}$ we have $S_1 \geq S_2$ if and only if $S_1 \supseteq S_2$. Note that $\emptyset \subseteq F$ is algebraically independent over K so that $\emptyset \in \mathcal{S}$ which implies that $\mathcal{S} \neq \emptyset$.

Next, let $\mathcal{C}$ be a chain in $\mathcal{S}$. First, suppose that $\mathcal{C} = \emptyset$. Then $\emptyset \in \mathcal{S}$ is an upper bound for $\mathcal{C}$ in this case. Now, suppose that $\mathcal{C} \neq \emptyset$ and define

$$T = \bigcup_{S \in \mathcal{C}} S$$

We claim that T is an upper bound for $\mathcal{C}$ in $\mathcal{S}$. Clearly, by the definition of T, we have that T is an upper bound for $\mathcal{C}$. It remains to prove that $T \in \mathcal{S}$. We prove this below.

First, since each $S \in \mathcal{C}$ satisfies $S \subseteq F$, we have that $T \subseteq F$. We will now show that T is algebraically independent to establish that $T \in \mathcal{S}$. For the sake of contradiction, suppose that T were not algebraically independent. Then for some positive integer n there exists a nonzero polynomial $p(x_1, \ldots, x_n) \in K[x_1, \ldots, x_n]$ with $p(t_1, \ldots, t_n) = 0$ for some distinct $t_1, \ldots, t_n \in T$. In particular, this gives that the set $\{t_1, \ldots, t_n\}$ is algebraically dependent over K.

Now, by the definition of T, for each $i \in \{1, \ldots, n\}$ there exists some $S_i \in \mathcal{C}$ such that $t_i \in S_i$. But since $\mathcal{C}$ is a chain, there is some $S \in \{S_1, \ldots, S_n\}$ such that $t_1, \ldots, t_n \in S$. Furthermore, since $S \in \mathcal{C}$, we know that S is algebraically independent over K so that $\{t_1, \ldots, t_n\} \subseteq S$ is also algebraically independent over K. However, we have that $\{t_1, \ldots, t_n\}$ is algebraically dependent over K which is a contradiction.

By the above proof, we may use Zorn's Lemma to assert that there is a maximal element $S \in \mathcal{S}$. By definition, this $S \subseteq F$ is algebraically independent over K and is maximal among all such sets so that S is a transcendence basis of F over K. $\square$

Proof. (b): Let F/K be a field extension and suppose that $T \subseteq F$ is an algebraically independent subset of F over K. If F/K. As above, define

$$\mathcal{S} = \{S \subseteq F : S \text{ is algebraically independent over } K\}$$

By the above proof, we know that there is some maximal element $S \in \mathcal{S}$. In particular, by definition, we have that S is a transcendence base of F over K.

Now, since $T \subseteq F$ and T is algebraically independent over K, we have that $T \in \mathcal{S}$. But by the maximality of $S \in \mathcal{S}$ and since $T \in \mathcal{S}$, we have that $T \subseteq S$. Since S is a transcendence base of F over K, this completes the proof. $\square$

Problem 3. *Show that* $\{x_1, \ldots, x_n\}$ *is a transcendence base of* $K(x_1, \ldots, x_n)$.

Proof. We first show that $\{x_1, \ldots, x_n\}$ is algebraically independent over K. For the sake of contradiction, suppose that $\{x_1, \ldots, x_n\}$ were algebraically dependent over K. Then for some positive integer $m \in \{1, \ldots, n\}$ there exists a nonzero polynomial

$$p(z_1, \ldots, z_m) \in K[z_1, \ldots, z_m]$$

and distinct elements $y_1, \ldots, y_m \in \{x_1, \ldots, x_n\}$ such that

$$p(y_1, \ldots, y_m) = 0$$

Clearly, we have that $p(z_1, \ldots, z_m)$ cannot be a constant polynomial, or else we would have $p(y_1, \ldots, y_m) \neq 0$. Thus, since $p(z_1, \ldots, z_m)$ is a nonzero, nonconstant polynomial, at least one of the indeterminants $z_1, \ldots, z_m$ appears in $p(z_1, \ldots, z_m)$ so that at least one of the indeterminants $y_1, \ldots, y_m$ appears in $p(y_1, \ldots, y_m)$. However, this is impossible since $p(y_1, \ldots, y_m) = 0$. This contradiction allows us to conclude that $\{x_1, \ldots, x_n\}$ is algebraically independent.

Finally, note that since $\{x_1, \ldots, x_n\}$ is algebraically independent by the above we have that $K(x_1, \ldots, x_n)/K$ is a purely transcendental extension. In particular, this implies that $\{x_1, \ldots, x_n\}$ is a transcendence base of $K(x_1, \ldots, x_n)$ over K. $\square$

Problem 6. (a): *If S is a transcendence base of the field $\mathbb{C}$ of complex numbers over the field $\mathbb{Q}$ of rationals, show that S is infinite.*

(b): *Show that there are infinitely many distinct automorphisms of the field $\mathbb{C}$.*

(c): *Show that the transcendence degree of $\mathbb{C}/\mathbb{Q}$ is equal to $|\mathbb{C}|$.*

Proof. (a): For the sake of contradiction, suppose that S were finite. In this case, we may write $S = \{s_1, \ldots, s_n\}$, where $s_1, \ldots, s_n \in \mathbb{C}$ and n is a positive integer. Now, note that $\mathbb{Q}(s_1, \ldots, s_n)$ is equal to the set

$$\left\{ \frac{f(s_1, \ldots, s_n)}{g(s_1, \ldots, s_n)} : f(x_1, \ldots, x_n), g(x_1, \ldots, x_n) \in \mathbb{Q}[x_1, \ldots, x_n] \text{ and } g(x_1, \ldots, x_n) \neq 0 \right\}$$

Note that since $\mathbb{Q}$ is countable, it follows that $\mathbb{Q}[x_1, \ldots, x_n]$ is countable. Therefore, by the above, this observation implies that $\mathbb{Q}(s_1, \ldots, s_n)$ is countable. Since $\mathbb{Q}$ is countable and $\mathbb{C}$ is uncountable, this gives

$$|\mathbb{Q}(S)| = |\mathbb{Q}(s_1, \ldots, s_n)| = |\mathbb{Q}| < |\mathbb{C}|$$

In particular, the above inequality gives that $|\mathbb{Q}(S)| = \aleph_0$.

Finally, since S is a transcendence base of $\mathbb{C}$ over $\mathbb{Q}$, this implies that $\mathbb{C}/\mathbb{Q}(S)$ is an algebraic extension. Therefore, by the above, we have

$$|\mathbb{C}| \leq \aleph_0 |\mathbb{Q}(S)| = \aleph_0 \cdot \aleph_0 = \aleph_0$$

However, this is impossible since $\mathbb{C}$ is uncountable. Therefore, S must be infinite. □

Proof. (b): Let $\sigma : S \to S$ be a bijection. Since S is algebraically independent over $\mathbb{Q}$, it follows that σ extends to a $\mathbb{Q}$-homomorphism $\phi : \mathbb{Q}(S) \to \mathbb{Q}(S)$ which is an isomorphism. In particular, since $\phi : \mathbb{Q}(S) \to \mathbb{Q}(S)$ is an isomorphism of fields and since $\mathbb{C}$ is an algebraically closed extension field of $\mathbb{Q}(S)$, it follows that ϕ can be extended to an isomorphism of fields $\psi : \mathbb{C} \to \mathbb{C}$.

Finally, recall that S is infinite. Hence, there are infinitely many distinct bijections $S \to S$. By the above proof, each of these infinitely many distinct bijections $S \to S$ extends to an isomorphism of fields $\mathbb{C} \to \mathbb{C}$ so that there are infinitely many distinct isomorphisms $\mathbb{C} \to \mathbb{C}$. That is, there are infinitely many distinct automorphisms of the field $\mathbb{C}$. This completes the proof. □

Proof. (c): We know that

$$|S| \leq |\mathbb{Q}(S)| \leq |\mathbb{C}|$$

Furthermore, as was shown above, we have that $|S|$ is infinite. Therefore, by the above inequality, we see that $|S| \in \{\aleph_0, 2^{\aleph_0}\}$. If $|S| = \aleph_0$, then $|\mathbb{Q}(S)| = \aleph_0$ using the same argument as above. However, this gives the same contradiction as above. Therefore, we have that

$$|S| = 2^{\aleph_0} = |\mathbb{C}|$$

In particular, by definition, this implies that the transcendence degree of $\mathbb{C}/\mathbb{Q}$ is equal to $|\mathbb{C}|$. This completes the proof. □

Homework 17: Page 58 #1, 2, 3

Problem 1. *A* pointed set *is a pair* (S, x) *with* S *a set and* $x \in S$*. A morphism of pointed sets* $(S, x) \to (S', x')$ *is a triple* (f, x, x')*, where* $f : S \to S'$ *is a function such that* $f(x) = x'$*. Show that pointed sets form a category.*

Proof. Let the objects of $\mathcal{C}$ be the pointed sets. For objects (S, x) and (T, y) of $\mathcal{C}$, define

$$\hom((S, x), (T, y)) = \{f : S \to T : f(x) = y\}$$

For morphisms $f \in \hom((S, x), (T, y))$ and $g \in \hom((T, y), (U, z))$, define $g \circ f$ to be the composition of set maps. Note that for $f \in \hom((S, x), (T, y))$ and $g \in \hom((T, y), (U, z))$, we have that

$$g \circ f : S \to U \quad \text{and} \quad (g \circ f)(x) = g(f(x)) = g(y) = z$$

Therefore, we have that $g \circ f \in \hom((S, x), (U, z))$ by definition. Hence, we have a map

$$\hom((T, y), (U, z)) \times \hom((S, x), (T, y)) \to \hom((S, x), (U, z)) \quad \text{by} \quad (g, f) \mapsto g \circ f$$

Let (S, x) be an object of $\mathcal{C}$ and let $1_{(S,x)} : S \to S$ be the identity map. Then clearly, we have that $1_{(S,x)}(x) = x$ so that $1_{(S,x)} \in \hom((S, x), (S, x))$.

Now, let $(S, x), (T, y), (U, z), (V, w)$ be objects of $\mathcal{C}$ and suppose that

$$f \in \hom((S, x), (T, y)) \quad g \in \hom((T, y), (U, z)) \quad h \in \hom((U, z), (V, w))$$

Since the composition of set maps is associative, we obtain that $h \circ (g \circ f) = (h \circ g) \circ f$.

Finally, let $(S, x), (T, y)$ be objects of $\mathcal{C}$ and suppose that $f \in \hom((S, x), (T, y))$. Let $1_{(S,x)} : S \to S$ and $1_{(T,y)} : T \to T$ be the identity maps of S and T, respectively. Note that for any $s \in S$, we have

$$(1_{(T,y)} \circ f)(s) = 1_{(T,y)}(f(s)) = f(s)$$

and

$$(f \circ 1_{(S,x)})(s) = f(1_{(S,x)}(s)) = f(s)$$

Since $s \in S$ was arbitrary, the above shows that $1_{(T,y)} \circ f = f = f \circ 1_{(S,x)}$. This completes the proof that $\mathcal{C}$ is a category. $\square$

Problem 2. *If $f : A \to B$ is an equivalence in a category $\mathcal{C}$ and $g : B \to A$ is a morphism such that $g \circ f = 1_A, f \circ g = 1_B$, show that g is unique.*

Proof. Suppose that $h : B \to A$ is a morphism such that $h \circ f = 1_A, f \circ h = 1_B$. Since $\mathcal{C}$ is a category, we know that $1_A \circ g = g$ and $h \circ 1_B = h$. Furthermore, since $\mathcal{C}$ is a category, we know that the $(h \circ f) \circ g = h \circ (f \circ g)$. These observations give the equality

$$g = 1_A \circ g = (h \circ f) \circ g = h \circ (f \circ g) = h \circ 1_B = h$$

In particular, this shows that $h = g$ so that g is unique. $\square$

Problem 3. *In the category $\mathcal{G}$ of groups, show that the group $G_1 \times G_2$ together with the homomorphisms $\pi_1 : G_1 \times G_2 \to G_1$ and $\pi_2 : G_1 \times G_2 \to G_2$ is a product for $\{G_1, G_2\}$*

Proof. For definiteness, note that the objects of $\mathcal{G}$ are groups and for two objects H and K of $\mathcal{G}$, we have $\hom(H, K)$ is the set of all group homomorphisms $H \to K$.

Now, let G be an object of $\mathcal{G}$ and let $\phi_1 : G \to G_1$ and $\phi_2 : G \to G_2$ be morphisms of $\mathcal{G}$. Define $\phi : G \to G_1 \times G_2$ by $\phi(g) = (\phi_1(g), \phi_2(g))$ for all $g \in G$. Clearly, we have that ϕ is a well-defined map.

We now show that ϕ is a group homomorphism. Towards this end, let $g, h \in G$. Then since ϕ_1, ϕ_2 are group homomorphisms, we have that

$$\begin{aligned}
\phi(gh) &= (\phi_1(gh), \phi_2(gh)) \\
&= (\phi_1(g)\phi_1(h), \phi_2(g)\phi_2(h)) \\
&= (\phi_1(g), \phi_2(g))(\phi_1(h), \phi_2(h)) \\
&= \phi(g)\phi(h)
\end{aligned}$$

This proves that ϕ is a group homomorphism so that ϕ is a morphism of $\mathcal{G}$.

Furthermore, if $g \in G$, notice by the definition of π_1 and π_2 that

$$(\pi_1 \circ \phi)(g) = \pi_1(\phi(g)) = \pi_1((\phi_1(g), \phi_2(g)) = \phi_1(g)$$

and

$$(\pi_2 \circ \phi)(g) = \pi_2(\phi(g)) = \pi_2((\phi_1(g), \phi_2(g)) = \phi_2(g)$$

But since $g \in G$ was arbitrary, this shows $\pi_1 \circ \phi = \phi_1$ and $\pi_2 \circ \phi = \phi_2$.

Finally, suppose that $\theta : G \to G_1 \times G_2$ is a group homomorphism such that $\pi_1 \circ \theta = \phi_1$ and $\pi_2 \circ \theta = \phi_2$. In particular, we have that

$$\theta(g) = (\pi_1(\theta(g)), \pi_2(\theta(g))) = (\phi_1(g), \phi_2(g)) = \phi(g)$$

for all $g \in G$. Hence, we see that $\theta = \phi$ so that ϕ is unique. This completes the proof. $\square$

Homework 18: Page 58 #4; Page 63 #3, 4, 12, 13, 14

Problem 4. *In the category $\mathcal{A}$ of abelian groups, show that the group $A_1 \times A_2$, together with the homomorphisms $i_1 : A_1 \to A_1 \times A_2$ and $i_2 : A_2 \to A_1 \times A_2$ is a coproduct for $\{A_1, A_2\}$.*

Proof. For definiteness, note that the objects of $\mathcal{A}$ are abelian groups and for two objects H and K of $\mathcal{A}$, we have $\hom(H, K)$ is the set of all group homomorphisms $H \to K$.

Now, let D be an object of $\mathcal{A}$ and let $\phi_1 : A_1 \to D$ and $\phi_2 : A_2 \to D$ be morphisms of $\mathcal{A}$. Define $\phi : A_1 \times A_2 \to D$ by $\phi((a_1, a_2)) = \phi_1(a_1)\phi_2(a_2)$ for all $a_1 \in A_1$ and for all $a_2 \in A_2$. Clearly, we have that ϕ is a well-defined map.

We now show that ϕ is a group homomorphism. Towards this end, let $(a_1, a_2), (b_1, b_2) \in A_1 \times A_2$. Then since ϕ_1, ϕ_2 are group homomorphisms and since D is an abelian group, we have that

$$\begin{aligned}
\phi((a_1, a_2)(b_1, b_2)) &= \phi((a_1b_1, a_2b_2)) \\
&= \phi_1(a_1b_1)\phi_2(a_2b_2) \\
&= \phi_1(a_1)\phi_1(b_1)\phi_2(a_2)\phi_2(b_2) \\
&= [\phi_1(a_1)\phi_2(a_2)][\phi_1(b_1)\phi_2(b_2)] \\
&= \phi((a_1, b_1))\phi((a_2, b_2))
\end{aligned}$$

This proves that ϕ is a group homomorphism. Furthermore, note that since A_1 and A_2 are abelian groups that $A_1 \times A_2$ is an abelian group. Thus, ϕ is a morphism of $\mathcal{A}$.

Now, let e_1, e_2, and e denote the identities of A_1, A_2, and D, respectively. Let $a_1 \in A_1$. Then by the definition of i_1 and since ϕ_1 is a group homomorphism, we see

$$(\phi \circ i_1)(a_1) = \phi(i_1(a_1)) = \phi(a_1, e_2) = \phi_1(a_1)\phi_2(e_2) = \phi_1(a_1) \cdot e = \phi_1(a_1)$$

Similarly, let $a_2 \in A_2$. Then by the definition of i_2 and since ϕ_2 is a group homomorphism, we see

$$(\phi \circ i_2)(a_2) = \phi(i_2(a_2)) = \phi(e_1, a_2) = \phi_1(e_1)\phi_2(a_2) = e \cdot \phi_2(a_2) = \phi_2(a_2)$$

But since $a_1 \in A_1$ and $a_2 \in A_2$ were arbitrary, this shows $\phi \circ i_1 = \phi_1$ and $\phi \circ i_2 = \phi_2$.

Finally, suppose that $\theta : A_1 \times A_2 \to D$ is a group homomorphism such that $\theta \circ i_1 = \phi_1$ and $\theta \circ i_2 = \phi_2$. In particular, we have that

$$\theta((a_1, a_2)) = \theta((a_1, e_2)(e_1, a_2)) = \theta(i_1(a_1)i_2(a_2)) = \theta(i_1(a_1))\theta(i_2(a_2)) = \phi_1(a_1)\phi_2(a_2) = \phi((a_1, a_2))$$

for all $(a_1, a_2) \in A_1 \times A_2$. Hence, we see that $\theta = \phi$ so that ϕ is unique. This completes the proof. $\square$

Problem 3. *Let G be an (additive) abelian group with subgroups H and K. Show that $G \simeq H \oplus K$ if and only if there are homomorphisms*

$$\pi_1 : G \to H \quad \pi_2 : G \to K \quad i_1 : H \to G \quad i_2 : K \to G$$

such that

$$\pi_1 \circ i_1 = 1_H \quad \pi_2 \circ i_2 = 1_K \quad \pi_1 \circ i_2 = 0 \quad \pi_2 \circ i_1 = 0$$

and $i_1(\pi_1(x)) + i_2(\pi_2(x)) = x$ for all $x \in G$.

Proof. For the first direction, assume that $G \simeq H \oplus K$. Define π_1, π_2, i_1, i_2 in the usual way. Then π_1, π_2, i_1, i_2 are group homomorphisms. Now, let e denote the identity of G. Suppose that $h \in H$. Then we have

$$(\pi_1 \circ i_1)(h) = \pi_1(i_1(h)) = \pi_1(h, e) = h = 1_H(h)$$

Since $h \in H$ was arbitrary, this shows that $\pi_1 \circ i_1 = 1_H$. Similarly, we obtain that $\pi_2 \circ i_2 = 1_K$. Next, suppose that $k \in K$. Then we have

$$(\pi_1 \circ i_2)(k) = \pi_1(i_2(k)) = \pi_1((e, k)) = e = 0(k)$$

Since $k \in K$ was arbitrary, this shows that $\pi_1 \circ i_2 = 0$. Similarly, we obtain that $\pi_2 \circ i_1 = 0$. Finally, let $x \in G$. Then since $G \simeq H \oplus K$, there are unique elements $h \in H$ and $k \in K$ such that x may be identified with $(h, k) \in H \oplus K$. Hence, we have

$$\begin{aligned} i_1(\pi_1(x)) + i_2(\pi_2(x)) &= i_1(\pi_1(h, k)) + i_2(\pi_2(h, k)) \\ &= i_1(h) + i_2(k) \\ &= (h, e) + (e, k) \\ &= (h + e, e + k) \\ &= (h, k) \\ &= x \end{aligned}$$

This completes the proof of the first direction.

We now prove the second direction. Define $\phi : G \to H \oplus K$ by $\phi(g) = (\pi_1(g), \pi_2(g))$ for all $g \in G$. By the definition of π_1 and π_2, it follows that ϕ is a well-defined map. Now, let $g, h \in G$. Then since π_1 and π_2 are group homomorphisms, we have

$$\begin{aligned} \phi(g + h) &= (\pi_1(g + h), \pi_2(g + h)) \\ &= (\pi_1(g) + \pi_1(h), \pi_2(g) + \pi_2(h)) \\ &= (\pi_1(g), \pi_2(g)) + (\pi_1(h), \pi_2(h)) \\ &= \phi(g) + \phi(h) \end{aligned}$$

so that ϕ is a group homomomorphism.

Next, we show that ϕ is a surjection. Towards this end, let $(h, k) \in H \oplus K$. By the definition of i_1 and i_2, we have that $i_1(h) \in G$ and $i_2(k) \in G$. Set $g = i_1(h) + i_2(k) \in G$.

Then we have by the definition of ϕ, since π_1 and π_2 are group homomorphisms, and by hypothesis that

$$\begin{aligned}
\phi(g) &= \phi(i_1(h) + i_2(k)) \\
&= (\pi_1(i_1(h) + i_2(k)), \pi_2(i_1(h) + i_2(k))) \\
&= (\pi_1(i_1(h)) + \pi_1(i_2(k)), \pi_2(i_1(h)) + \pi_2(i_2(k))) \\
&= (1_H(h) + 0(k), 0(h) + 1_K(k)) \\
&= (h + e, e + k) \\
&= (h, k)
\end{aligned}$$

Hence, we see that ϕ is a surjection.

Finally, suppose that $x \in \ker \phi$ and let e denote the identity of G. Then we have

$$(e, e) = \phi(x) = (\pi_1(x), \pi_2(x))$$

which gives $\pi_1(x) = e = \pi_2(x)$. Combining this observation with our hypothesis for this direction, we have

$$x = i_1(\pi_1(x)) + i_2(\pi_2(x)) = i_1(e) + i_2(e) = (e, e) + (e, e) = (e + e, e + e) = (e, e)$$

so that $x \in G$ is identified with $(e, e) \in H \oplus K$. In particular, since $x \in \ker \phi$ was arbitrary, this shows that $\ker \phi$ is trivial. Thus, since ϕ is a group homomorphism, this implies that ϕ is an injection. Thus, we now have that ϕ is an isomorphism so that $G \simeq H \oplus K$. This completes the proof of the second direction. $\square$

Problem 4. *Give an example to show that the weak direct product is not a coproduct in the category of all groups.*

Proof. In the category of $\mathcal{G}$ of groups, consider the objects

$$G = \mathbb{Z}_2 = \{\overline{0}, \overline{1}\}$$

and

$$H = \mathbb{Z}_3 = \{\overline{0}, \overline{1}, \overline{2}\}$$

of $\mathcal{G}$.

Consider the weak direct product $(G \times H)^w$. In this case, since we are dealing only with the two groups G and H, we have that $(G \times H)^w = G \times H$. Define the group homomorphisms $i_1 : G \to G \times H$ and $i_2 : H \to G \times H$ in the usual way. We claim that the object $G \times H$ of $\mathcal{G}$ together with $\{i_1, i_2\}$ is not a coproduct in for $\{G, H\}$ in $\mathcal{G}$.

Indeed, for the sake of contradiction, suppose that the object $G \times H$ of $\mathcal{G}$ together with $\{i_1, i_2\}$ were a coproduct for $\{G, H\}$ in $\mathcal{G}$. Note that S_3 is an object of $\mathcal{G}$ and define

$$\phi_1 : G \to S_3 \quad \text{by} \quad \overline{0} \mapsto (1) \quad \overline{1} \mapsto (1 \quad 2)$$

and

$$\phi_2 : H \to S_3 \quad \text{by} \quad \overline{0} \mapsto (1) \quad \overline{1} \mapsto (1 \quad 2 \quad 3) \quad \overline{2} \mapsto (1 \quad 3 \quad 2)$$

Then it can easily be shown that ϕ_1 and ϕ_2 are group homomorphisms and are therefore morphisms of $\mathcal{G}$.

Now, since $G \times H$ together with $\{i_1, i_2\}$ is a coproduct and by the above result, there is a unique group homomorphism $\phi : G \times H \to S_3$ such that $\phi \circ i_1 = \phi_1$ and $\phi \circ i_2 = \phi_2$. Hence, we obtain

$$(1 \quad 2) = \phi_1(\overline{1}) = \phi(i_1(\overline{1})) = \phi((\overline{1}, \overline{0}))$$

and

$$(1 \quad 2 \quad 3) = \phi_2(\overline{1}) = \phi(i_2(\overline{1})) = \phi((\overline{0}, \overline{1}))$$

In particular, since $\langle (1 \quad 2), (1 \quad 2 \quad 3) \rangle = S_3$, this shows that ϕ is surjective. But since $|G \times H| = 6 = |S_3|$, we now have that ϕ is bijective. Since ϕ is a homomorphism, it now follows that ϕ is an isomorphism so that $G \times H \simeq S_3$.

However, note that since G and H are abelain that $G \times H$ is abelian. Furthermore, we know that S_3 is not abelian. These observations imply that $G \times H$ cannot be isomorphic to S_3, contradicting the above result. We conclude that $G \times H$ together with $\{i_1, i_2\}$ is not a coproduct for $\{G, H\}$ in $\mathcal{G}$. This shows that the weak direct product is not always a coproduct in the category $\mathcal{G}$ of all groups. $\square$

Problem 12. *A normal subgroup H of a group G is said to be a* ***direct factor*** *if there exists a normal subgroup K of G such that $G = H \times K$.*

(a): *If H is a direct factor of K and K is a direct factor of G, then H is normal in G.*

(b): *If H is a direct factor of G, then every homomorphism $H \to G$ may be extended to an endomorphism $G \to G$. However, a monomorphism $H \to G$ need not be extendible to an automorphism $G \to G$.*

Proof. (a): Since H is a direct factor of K, we have that $H \trianglelefteq K$ and there exists some $L \trianglelefteq K$ with $K = H \times L$. Since K is a direct factor of G, we have that $K \trianglelefteq G$ and there exists some $M \trianglelefteq G$ with $G = K \times M$. By the above, we now have $G = H \times L \times M$.

Define $\phi : H \times L \times M \to L \times M$ by $\phi(a, b, c) = (b, c)$ for all $(a, b, c) \in H \times L \times M$. Then ϕ is clearly a well-defined group homomorphism. Let e denote the identity of G. We will show that $\ker \phi = H \times \{e\} \times \{e\}$.

Towards this end, first suppose that $(a, b, c) \in \ker \phi$. Then we have

$$(b, c) = \phi((a, b, c)) = (e, e)$$

so that $b = e = c$. Hence, we have that

$$(a, b, c) = (a, e, e) \in H \times \{e\} \times \{e\}$$

On the other hand, suppose that $(a, e, e) \in H \times \{e\} \times \{e\}$. In this case, we have

$$\phi((a, e, e)) = (e, e)$$

so that $(a, e, e) \in \ker \phi$. The above results show that

$$H \simeq H \times \{e\} \times \{e\} = \ker \phi \trianglelefteq H \times L \times M = G$$

This completes the proof. $\square$

Proof. (b): Since H is a direct factor of G, we have that $H \trianglelefteq G$ and there exists some $K \trianglelefteq G$ with $G = H \times K$. Now, let $\phi : H \to H \times K$ be a group homomorphism. Define $\sigma : H \times K \to H \times K$ by $\sigma(h, k) = \phi(h)$ for all $(h, k) \in H \times K$. Then σ is clearly a well-defined map. Furthermore, if $(h_1, k_1), (h_2, k_2) \in H \times K$ then since ϕ is a group homomorphism we have that

$$\sigma((h_1, k_1)(h_2, k_2)) = \sigma((h_1h_2, k_1k_2)) = \phi(h_1h_2) = \phi(h_1)\phi(h_2) = \sigma((h_1, k_1))\sigma((h_2, k_2))$$

so that σ is a group homomorphism. Hence, $\sigma : G \to G$ is an endomorphism.

Finally, suppose that $h \in H$. Since $H \simeq H \times \{e\}$, we may identity $h \in H$ with $(h, e) \in H \times \{e\}$. Notice that by the definition of σ, we have

$$\sigma((h, e)) = \phi(h)$$

In particular, this shows that σ extends ϕ.

Consider the group $G = \mathbb{Z} \times \mathbb{Z}$. Let $H = \mathbb{Z} \times \{0\}$. Then by the above, we know that H is a normal subgroup of G. Furthermore, we have $H = \mathbb{Z} \times \{0\} \simeq \mathbb{Z}$ which gives that H is a direct factor of G.

Now, define $\phi : H \to G$ by $\phi(n, 0) = (2n, 2n)$ for all $(n, 0) \in H = \mathbb{Z} \times \{0\}$. Then ϕ is clearly a well-defined map. Furthermore, if $(n_1, 0), (n_2, 0) \in H$, then

$$\begin{aligned}
\phi((n_1, 0) + (n_2, 0)) &= \phi((n_1 + n_2, 0)) \\
&= (2(n_1 + n_2), 2(n_1 + n_2)) \\
&= (2n_1 + 2n_2, 2n_1 + 2n_2) \\
&= (2n_1, 2n_1) + (2n_2, 2n_2) \\
&= \phi((n_1, 0)) + \phi((n_2, 0))
\end{aligned}$$

so that ϕ is a group homomorphism. Furthermore, suppose that $(n_1, 0), (n_2, 0) \in H$ with $\phi((n_1, 0)) = \phi((n_2, 0))$. Then we have

$$(2n_1, 2n_1) = \phi((n_1, 0)) = \phi((n_2, 0)) = (2n_2, 2n_2)$$

which gives $2n_1 = 2n_2$ so that $n_1 = n_2$ so that $(n_1, 0) = (n_2, 0)$. In particular, this shows that ϕ is an injection. By the previous result, this shows that ϕ is a monomorphism.

For the sake of contradiction, suppose that ϕ could be extended to an automorphism $\sigma : G \to G$. Since σ is surjective, for the element $(1, 1) \in G$ there exists some $(n, m) \in G$ such that $\sigma((n, m)) = (1, 1)$. In this case, since σ is a group homomorphism, we have

$$\sigma((2n, 2m)) = \sigma((n, m) + (n, m)) = \sigma((n, m)) + \sigma((n, m)) = (1, 1) + (1, 1) = (2, 2)$$

However, since σ extends ϕ, we also have by the definition of ϕ that

$$(2, 2) = (2 \cdot 1, 2 \cdot 1) = \phi((1, 0)) = \sigma((1, 0))$$

In particular, the above results give

$$\sigma((2n, 2m)) = (2, 2) = \sigma((1, 0))$$

Since σ is injective, the above equality implies that $(2n, 2m) = (1, 0)$ so that $2n = 1$. However, since $n \in \mathbb{Z}$, this is impossible. We conclude that there is no extension of the monomorphism $\sigma : H \to G$ to an automorphism $G \to G$, completing the proof. $\square$

Problem 13. *Let $\{G_i : i \in I\}$ be a family of groups and $J \subseteq I$. The map*

$$\alpha : \prod_{j\in J} G_j \to \prod_{i\in I} G_i \quad \text{by} \quad (a_j)_{j\in J} \mapsto (b_i)_{i\in I}$$

where $b_j = a_j$ for $j \in J$ and $b_i = e_i$ (identity of G_i) for $i \notin J$, is a monomorphism of groups and

$$\prod_{i\in I} G_i \Big/ \alpha\left(\prod_{j\in J} G_j\right) \simeq \prod_{i\in I-J} G_i$$

Proof. Let $H = \prod_{j\in J} G_j$ and $G = \prod_{i\in I} G_i$. Let $(a_j)_{j\in J}, (b_j)_{j\in J} \in H$. Then we have

$$\alpha((a_j)_{j\in J}(b_j)_{j\in J}) = \alpha((a_jb_j)_{j\in J}) = \begin{cases} a_jb_j & \text{if } j \in J \\ e_i & \text{if } i \in I - J \end{cases}$$

On the other hand, since $e_ie_i = e_i$ for each $i \in I - J$, we have

$$\alpha((a_j)_{j\in J})\alpha((b_j)_{j\in J}) = \begin{cases} a_j & \text{if } j \in J \\ e_i & \text{if } i \in I - J \end{cases} \cdot \begin{cases} b_j & \text{if } j \in J \\ e_i & \text{if } i \in I - J \end{cases} = \begin{cases} a_jb_j & \text{if } j \in J \\ e_i & \text{if } i \in I - J \end{cases}$$

In particular, the above shows that

$$\alpha((a_j)_{j\in J}(b_j)_{j\in J}) = \alpha((a_j)_{j\in J})\alpha((b_j)_{j\in J})$$

so that α is a group homomorphism.

Now, suppose that $(a_j)_{j\in J} \in \ker\alpha$. Then we have

$$\alpha((a_j)_{j\in J}) = (e_i)_{i\in I}$$

Hence, by the definition of α, we have

$$(e_i)_{i\in I} = \alpha((a_j)_{j\in J}) = \begin{cases} a_j & \text{if } j \in J \\ e_i & \text{if } i \in I - J \end{cases}$$

In particular, the above shows that $(a_j)_{j\in J} = (e_j)_{j\in J}$. It now follows that $\ker\alpha$ is trivial. Since α is a group homomorphism, this observation shows that α is an injection so that α is a monomorphism.

Finally, let $K = \prod_{i\in I-J} G_i$ and define

$$\phi : G \to K \quad \text{by} \quad (a_i)_{i\in I} \mapsto (a_i)_{i\in I-J}$$

Clearly, ϕ is a well-defined map. Now, let $(a_i)_{i\in I}, (b_i)_{i\in I} \in G$. Then we have

$$\phi((a_i)_{i\in I}, (b_i)_{i\in I}) = \phi((a_ib_i)_{i\in I}) = (a_ib_i)_{i\in I-J} = (a_i)_{i\in I-J}(b_i)_{i\in I-J} = \phi((a_i)_{i\in I})\phi((b_i)_{i\in I})$$

so that ϕ is a group homomorphism. Furthermore, suppose that $(a_i)_{i\in I-J} \in K$ and define $(b_i)_{i\in I} \in G$ by

$$b_i = \begin{cases} a_i & \text{if } i \in I - J \\ e_i & \text{if } i \in J \end{cases}$$

Then we have $\phi((b_i)_{i\in I}) = (a_i)_{i\in I-J}$ so that ϕ is a surjection.

Now, we will show that $\ker \phi = \alpha(H)$. Towards this end, first suppose that $(a_i)_{i \in I} \in \ker \phi$. Then we have

$$(e_i)_{i \in I - J} = \phi((a_i)_{i \in I}) = (a_i)_{i \in I - J}$$

so that

$$a_i = \begin{cases} e_i & \text{if } i \in I - J \\ a_i & \text{if } i \in J \end{cases}$$

In particular, this shows that $(a_i)_{i \in I} \in \alpha(H)$. On the other hand, suppose that $(a_i)_{i \in I} \in \alpha(H)$. Then there is some $(b_j)_{j \in J} \in H$ so that $\alpha((b_j)_{j \in J}) = (a_i)_{i \in I}$. This gives

$$(a_i)_{i \in I} = \alpha((b_j)_{j \in J}) = \begin{cases} b_j & \text{if } j \in J \\ e_i & \text{if } i \in I - J \end{cases}$$

Therefore, we have

$$\phi((a_i)_{i \in I}) = (a_i)_{i \in I - J} = (e_i)_{i \in I - J}$$

so that $(a_i)_{i \in I} \in \ker \phi$. The above results prove that $\ker \phi = \alpha(H)$. Combining the previous results, we have by the First Isomorphism Theorem that $G/\alpha(H) \simeq K$. By the definition of G, H, and K, this completes the proof. $\square$

Problem 14. *Let $H_1 \trianglelefteq G_1$ and $H_2 \trianglelefteq G_2$ and give examples to show that each of the following statements may be false:*

(a): *$G_1 \simeq G_2$ and $H_1 \simeq H_2$ implies that $G_1/H_1 \simeq G_2/H_2$.*

(b): *$G_1 \simeq G_2$ and $G_1/H_1 \simeq G_2/H_2$ implies that $H_1 \simeq H_2$.*

(c): *$H_1 \simeq H_2$ and $G_1/H_1 \simeq G_2/H_2$ implies that $G_1 \simeq G_2$.*

Proof. (a): Let

$$G_1 = \mathbb{Z}_2 \times \mathbb{Z}_4 = G_2 \quad H_1 = \langle (1,0) \rangle \subseteq G_1 \quad H_2 = \langle (0,2) \rangle \subseteq G_2$$

Note that since the product of abelian groups is abelian, we have that G_1 and G_2 are abelian groups so that $H_1 \trianglelefteq G_1$ and $H_2 \trianglelefteq G_2$. Since $G_1 = G_2$, we have $G_1 \simeq G_2$ and as $|H_1| = 2 = |H_2|$, we have $H_1 \simeq \mathbb{Z}_2 \simeq H_2$ so that $H_1 \simeq H_2$.

Now, note that G_1/H_1 is a group of order 4 containing an element of order 4 so that $G_1/H_1 \simeq \mathbb{Z}_4$. On the other hand, note that G_2/H_2 is a group of order 4 all of whose nonidentity elements have order 2 so that $G_2/H_2 \simeq V_4$. In particular, the above shows that G_1/H_1 is not isomorphic to G_2/H_2. □

Proof. (b): Let

$$G_1 = \mathbb{Z}_2 \times \mathbb{Z}_4 = G_2 \quad H_1 = \mathbb{Z}_2 \times \langle 2 \rangle \subseteq G_1 \quad H_2 = \{0\} \times \mathbb{Z}_4 \subseteq G_2$$

Note that since the product of abelian groups is abelian, we have that G_1 and G_2 are abelian groups so that $H_1 \trianglelefteq G_1$ and $H_2 \trianglelefteq G_2$. Since $G_1 = G_2$, we have $G_1 \simeq G_2$ and as $|G_1/H_1| = 2 = |G_2/H_2|$, we have $G_1/H_1 \simeq \mathbb{Z}_2 \simeq G_2/H_2$ so that $G_1/H_1 \simeq G_2/H_2$.

Now, note that H_1 is a group of order 4 all of whose nonidentity elements have order 2 so that $H_1 \simeq V_4$. On the other hand, note that H_2 is a group of order 4 containing an element of order 4 so that $H_2 \simeq \mathbb{Z}_4$. In particular, the above shows that H_1 is not isomorphic to H_2. □

Proof. (c): Let

$$G_1 = \mathbb{Z}_2 \times \mathbb{Z}_4 \quad G_2 = \mathbb{Z}_8 \quad H_1 = \{0\} \times \mathbb{Z}_4 \subseteq G_1 \quad H_2 = \langle 2 \rangle \subseteq G_2$$

Note that since the product of abelian groups is abelian, we have that G_1 is an abelian group so that $H_1 \trianglelefteq G_1$. We also know that G_2 is cyclic and hence abelian so that $H_2 \trianglelefteq G_2$.

Now, note that H_1 is a group of order 4 containing an element of order 4 so that $H_1 \simeq \mathbb{Z}_4$. Since subgroups of cyclic groups are cyclic and since H_2 is a subgroup of order 4 of the cyclic group G_2, we have that $H_2 \simeq \mathbb{Z}_4$. Hence, we obtain $H_1 \simeq \mathbb{Z}_2 \simeq H_2$ so that $H_1 \simeq H_2$. Furthermore, since $|G_1/H_1| = 2 = |G_2/H_2|$, we have $G_1/H_1 \simeq \mathbb{Z}_2 \simeq G_2/H_2$ so that $G_1/H_1 \simeq G_2/H_2$.

However, notice that since 2 and 4 are not relatively prime we have that G_1 is not cyclic. On the other hand, we know that G_2 is cyclic. In particular, this observation shows that G_1 is not isomorphic to G_2. □

Homework 19: Page 68 #1, 2, 4

Problem 1. *Every nonidentity element in a free group F has infinite order.*

Proof. Let F be a free group on the set X. For the sake of contradiction, assume that F contains at least one nonidentity element of finite order. For an element $w \in F$, let $\text{len}(w)$ denote the length of the word w and let $w \in F$ be a nonidentity element of finite order m with $\text{len}(w)$ as small as possible.

If $\text{len}(w) = 1$, then $w = a$ for some $a \in X \cup X^{-1}$. In this case, we see that for each positive integer n we have

$$w^n = a^n = \underbrace{a \cdots a}_{n \text{ times}} \neq 1$$

In particular, this shows that w does not have finite order. Therefore, we may may assume that $\text{len}(w) \geq 2$.

If $\text{len}(w) = 2$, then $w = ab$ for some $a, b \in X \cup X^{-1}$. If $b = a^{-1}$, then

$$w = ab = aa^{-1} = 1$$

which contradicts the fact that w is a nonidentity element of F. Hence, we have $b \neq a^{-1}$. Similarly, we obtain $a \neq b^{-1}$. In particular, we now have for each positive integer n that

$$w^n = (ab)^n = \underbrace{(ab) \cdots (ab)}_{n \text{ times}} \neq 1$$

In particular, this shows that w does not have finite order. Therefore, we may assume that $\text{len}(w) \geq 3$.

Since $\text{len}(w) \geq 3$, we may write $w = azb$ for some $a, b \in X \cup X^{-1}$ and some nonidentity element $z \in F$ with the first letter of z not equal to a^{-1} and the last letter of z not equal to b^{-1}. Note that

$$\text{len}(w) = \text{len}(a) + \text{len}(z) + \text{len}(b) = 1 + \text{len}(z) + 1 = \text{len}(z) + 2$$

so that

$$\text{len}(z) = \text{len}(w) - 2 < \text{len}(w)$$

By the minimality of $\text{len}(w)$, the above equality implies that z cannot have finite order. This gives that $z^n \neq 1$ for each positive integer n.

Now, assume that $b = a^{-1}$. Then we have $w = azb = aza^{-1}$. Therefore, since $|w| = m$, we have

$$1 = w^m = (aza^{-1})^m = \underbrace{(aza^{-1}) \cdots (aza^{-1})}_{m \text{ times}} = az^m a^{-1}$$

so that

$$z^m = a^{-1}a = 1$$

However, this contradicts the fact that $z^n \neq 1$ for each positive integer n. Therefore, we must have $b \neq a^{-1}$. Similarly, we obtain $a \neq b^{-1}$. Since $|w| = m$, this gives

$$1 = a^m = (azb)^m = \underbrace{(azb) \cdots (azb)}_{m \text{ times}} \neq 1$$

which is obviously a contradiction. Hence, we conclude that every nonidentity element of F has infinite order. $\square$

Problem 2. *Show that the free group on the set $\{a\}$ is an infinite cyclic group, and hence isomorphic to $\mathbb{Z}$.*

Proof. Let F be the free group on the set $\{a\}$. Note that if $w \in F$ we have that $w = a^n$ for some integer n. Now, define

$$\phi : F \to \mathbb{Z} \quad \text{by} \quad a^n \mapsto n$$

Clearly, we have that ϕ is a well-defined map.

We now show that ϕ is a group homomorphism. Towards this end, let $x, y \in F$. Then $x = a^n$ and $y = a^m$ for some integers n and m so that

$$xy = a^n a^m = a^{n+m} \in F$$

Hence, we obtain

$$\phi(xy) = \phi(a^{n+m}) = n + m = \phi(a^n) + \phi(a^m) = \phi(x) + \phi(y)$$

This shows that ϕ is a group homomorphism.

Now, let $n \in \mathbb{Z}$. Let $x = a^n \in F$. Then we have

$$\phi(x) = \phi(a^n) = n$$

so that ϕ is a surjection.

Finally, suppose that $x \in \ker \phi$. Since $x \in F$, we may write $x = a^n$ for some integer n. This gives that

$$0 = \phi(x) = \phi(a^n) = n$$

Hence, we now have $x = a^n = a^0 = 1$. In particular, this shows that $\ker \phi$ is trivial. Since ϕ is a group homomorphism, this observation implies that ϕ is an injection.

By the above results, we have that ϕ is an isomorphism so that $F \simeq \mathbb{Z}$. In particular, since $\mathbb{Z}$ is an infinite cyclic group, this proves that F is an infinite cyclic group. $\square$

Problem 4. *Let F be the free group on the set X, and let $Y \subseteq X$. If H is the smallest normal subgroup of F containing Y, then F/H is a free group.*

Proof. We will show that F/H is free on the set $X-Y$ in the category of groups. Towards this end, let $j : X-Y \to X$ and $i : X \to F$ be the inclusion maps and let $\pi : F \to F/H$ be the canonical projection. Define $k = \pi \circ i \circ j$. Then we have $k : X - Y \to F/H$.

Now, let G be a group and let $f : X - Y \to G$ be a map of sets. Define $g : X \to G$ by $g(x) = f(x)$ for every $x \in X - Y$ and $g(y) = 1_G$ for every $y \in Y$, where 1_G denotes the identity of G. Since F is free on X, there exists a unique group homomorphism $\overline{g} : F \to G$ such that $\overline{g} \circ i = g$. Note that if $y \in Y$ then we have

$$\overline{g}(y) = \overline{g}(i(y)) = g(y) = 1_G$$

which shows that $Y \subseteq \ker(\overline{g})$ so that $\ker(\overline{g})$ is a normal subgroup of F containing Y. Hence, we have $H \subseteq \ker(\overline{g})$. In particular, this shows that there exists a group homomorphism $\overline{\overline{g}} : F/H \to G$ such that $\overline{\overline{g}} \circ \pi = \overline{g}$. The above results give that

$$\overline{\overline{g}} \circ k = \overline{\overline{g}} \circ \pi \circ i \circ j = \overline{g} \circ i \circ j = g \circ j = f$$

so that $\overline{\overline{g}} \circ k = f$.

It remains to prove that $\overline{\overline{g}}$ is unique. Suppose that $\phi_1, \phi_2 : F/H \to G$ are group homomorphisms such that $\phi_1 \circ k = f = \phi_2 \circ k$. Note that for $x \in X - Y$ we have

$$\phi_1(\pi(i(x))) = \phi_1(\pi(i(j(x)))) = \phi_1(k(x)) = \phi_2(k(x)) = \phi_2(\pi(i(j(x)))) = \phi_2(\pi(i(x)))$$

Furthermore, for $y \in Y$ we have since $Y \subseteq H$ and since ϕ_1 and ϕ_2 are group homomorphisms that

$$\phi_1(\pi(i(y))) = \phi_1(\pi(y)) = \phi_1(yH) = \phi(H) = 1_G$$

and

$$\phi_2(\pi(i(y))) = \phi_2(\pi(y)) = \phi_2(yH) = \phi(H) = 1_G$$

so that $\phi_1(\pi(i(y))) = \phi_2(\pi(i(y)))$. The above results show that $\phi_1(\pi(i(x)))) = \phi_2(\pi(i(x)))$ for all $x \in X$. Hence, we obtain $\phi_1 \circ \pi \circ i = \phi_2 \circ \pi \circ i$.

Now, notice that if $x \in X - Y$ we have

$$\phi_1(\pi(i(x))) = \phi_1(\pi(i(j(x)))) = \phi_1(k(x)) = f(x) = g(x)$$

Furthermore, for $y \in Y$, the above result gives

$$\phi_1(\pi(i(y))) = 1_G = g(y)$$

The above results show that $\phi_1(\pi(i(x))) = g(x)$ for all $x \in X$ so that $\phi_1 \circ \pi \circ i = g$. Since $\phi_1 \circ \pi \circ i = \phi_2 \circ \pi \circ i$ by the above, we now have

$$\phi_1 \circ \pi \circ i = g = \phi_1 \circ \pi \circ i$$

Furthermore, since the composition of group homomorphisms is a group homomorphism, we have $\phi_1 \circ \pi$ and $\phi_2 \circ \pi$ are group homomorphisms. Thus, since F is free on X, the above equality shows that $\phi_1 \circ \pi = \phi_2 \circ \pi$.

Finally, since π is a surjection, we obtain $\phi_1 = \phi_2$ since $\phi_1 \circ \pi = \phi_2 \circ \pi$. This proves that $\overline{\overline{g}}$ is unique and hence F/H is free on $X - Y$ in the category of groups. $\square$

Homework 20: Page 68 #6, 7, 8

Problem 6. *The cyclic group of order* 6 *is the group defined by generators* a, b *and relations* $a^2 = b^3 = a^{-1}b^{-1}ab = e$.

Proof. Let $X = \{a, b\}, R = \{a^2, b^3, a^{-1}b^{-1}ab\}$, and N be the smallest normal subgroup of F with $R \subseteq N$ where F is the free group on X. By definition, we have that the group defined by generators X and relations R is F/N.

Now, recall that $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$. Define

$$f : X \to \mathbb{Z}_6 \quad \text{by} \quad a \mapsto 3 \quad b \mapsto 2$$

Since F is free on X, there exists a unique group homomorphism $\overline{f} : F \to \mathbb{Z}_6$ such that

$$\overline{f}(a) = f(a) = 3 \quad \text{and} \quad \overline{f}(b) = f(b) = 2$$

Note that since $\overline{f}$ is a group homomorphism we have

$$\overline{f}(a^2) = \overline{f}(a) + \overline{f}(a) = 3 + 3 = 0$$

and

$$\overline{f}(b^3) = \overline{f}(b) + \overline{f}(b) + \overline{f}(b) = 2 + 2 + 2 = 0$$

and

$$\overline{f}(a^{-1}b^{-1}ab) = \overline{f}(a)^{-1} + \overline{f}(b)^{-1} + \overline{f}(a) + \overline{f}(b) = 3^{-1} + 2^{-1} + 3 + 2 = 3 + 4 + 3 + 2 = 0$$

In particular, the above shows that $R \subseteq \ker(\overline{f})$. Since $\ker(\overline{f})$ is a normal subgroup of F with $R \subseteq \ker(\overline{f})$, it follows by the definition of N that $N \subseteq \ker(\overline{f})$.

The above results show that there exists a group homomorphism $g : F/N \to \mathbb{Z}_6$ such that $g(aN) = 3$ and $g(bN) = 2$. Note that since $\mathbb{Z}_6 = \langle 2, 3 \rangle$ and since $2, 3 \in g(F/N)$ we have that g is a surjection. In particular, this gives that $|F/N| \geq |\mathbb{Z}_6| = 6$.

We will now show that $|F/N| \leq 6$. We claim that every element $wN \in F/N$ has a representative of the form $a^i b^j$ for some $i \in \{0, 1\}$ and $j \in \{0, 1, 2\}$. Indeed, let $wN \in F/N$. Since $a^2, b^3 \in N$, we can choose a representative for wN of the form

$$a^{n_1} b^{n_2} a^{n_3} b^{n_4} \cdots b^{n_r}$$

where $n_i \in \{0, 1\}$ for odd values of $i \in \{1, \ldots, r\}$ and $n_i \in \{0, 1, 2\}$ for even values of $i \in \{1, \ldots, r\}$.

Now, among all such representatives for wN of this form, choose one where r is as small as possible. First, suppose that $r \geq 3$. In this case, we have that $n_1 = 1 = n_3$. Notice that since $a^{-1}b^{-1}ab \in N$ and $a^2 \in N$, we have that

$$ab^{n_2}aN = b^{n_2}N$$

which contradicts the minimality of r. Hence, we must have $r \leq 2$ which shows that wN has a representative of the form $a^i b^j$ for some $i \in \{0, 1\}$ and $j \in \{0, 1, 2\}$. In particular, this gives that $|F/N| \leq 6$.

By the above results, we have that $|F/N| = 6 = |\mathbb{Z}_6|$. Since g is a surjection, this now gives that g is a bijection so that g is an isomorphism. Thus, we obtain $F/N \simeq \mathbb{Z}_6$. $\square$

Problem 7. *Show that the group defined by the generators a, b and relations $a^2 = e, b^3 = e$ is infinite and nonabelian.*

Proof. Let $X = \{a, b\}, R = \{a^2, b^3\}$, and N be the smallest normal subgroup of F with $R \subseteq N$ where F is the free group on X. By definition, we have that the group defined by the generators X and relations R is F/N.

Before we begin, we prove that if $\theta : H \to K$ is a surjective group homomorphism and if K is nonabelian then H is nonabelian. Indeed, since K is nonabelian, there exist $k_1, k_2 \in K$ such that $k_1k_2 \neq k_2k_1$. As θ is a surjection, there exist $h_1, h_2 \in H$ such that $\theta(h_1) = k_1$ and $\theta(h_2) = k_2$. Since θ is a group homomorphism, this gives

$$k_1k_2 = \theta(h_1)\theta(h_2) = \theta(h_1h_2)$$

and

$$k_2k_1 = \theta(h_2)\theta(h_1) = \theta(h_2h_1)$$

Hence, if $h_1h_2 = h_2h_1$ then the above results would imply that

$$k_1k_2 = \theta(h_1h_2) = \theta(h_2h_1) = k_2k_1$$

which is a contradiction since $k_1k_2 \neq k_2k_1$. Thus, we have $h_1h_2 \neq h_2h_1$ so that H is nonabelian. This proves the result.

We first show that F/N is nonabelian. Towards this end, recall that $D_6 = \langle r, s\rangle$ with $|r| = 3, |s| = 2$, and $srs = r^{-1}$. Define

$$f : X \to D_3 \quad \text{by} \quad a \mapsto s \quad b \mapsto r$$

Since F is free on X, there exists a unique group homomorphism $\overline{f} : F \to D_6$ such that

$$\overline{f}(a) = f(a) = s \quad \text{and} \quad \overline{f}(b) = f(b) = r$$

Note that since $\overline{f}$ is a group homomorphism we have

$$\overline{f}(a^2) = \overline{f}(a)\overline{f}(a) = s \cdot s = s^2 = 1$$

and

$$\overline{f}(b^3) = \overline{f}(b)\overline{f}(b)\overline{f}(b) = r \cdot r \cdot r = r^3 = 1$$

In particular, the above shows that $R \subseteq \ker(\overline{f})$. Since $\ker(\overline{f})$ is a normal subgroup of F with $R \subseteq \ker(\overline{f})$, it follows by the definition of N that $N \subseteq \ker(\overline{f})$.

The above results show that there exists a group homomorphism $g : F/N \to D_6$ such that $g(aN) = s$ and $g(bN) = r$. Note that since $D_6 = \langle r, s\rangle$ and since $r, s \in g(F/N)$ we have that g is a surjection. Furthermore, since $rs \neq sr$ we have that D_6 is nonabelian. Thus, by our preliminary result, the previous two observations give that F/N is nonabelian.

Finally, we show that F/N is infinite. Towards this end, consider $\sigma_1, \sigma_2 \in S_\infty$ given by $\sigma_1 = (3 \quad 4)(6 \quad 7)$ and $\sigma_2 = (1 \quad 2 \quad 3)(4 \quad 5 \quad 6)$. Clearly, we have $|\sigma_1| = 2$ and $|\sigma_2| = 3$. Let $H = \langle \sigma_1, \sigma_2\rangle \subseteq S_\infty$ and define

$$f : X \to H \quad \text{by} \quad a \mapsto \sigma_1 \quad b \mapsto \sigma_2$$

Since F is free on X, there exists a unique group homomorphism $\overline{f} : F \to H$ such that

$$\overline{f}(a) = f(a) = \sigma_1 \quad \text{and} \quad \overline{f}(b) = f(b) = \sigma_2$$

Note that since $\overline{f}$ is a group homomorphism we have

$$\overline{f}(a^2) = \overline{f}(a)\overline{f}(a) = \sigma_1 \cdot \sigma_1 = \sigma_1^2 = 1$$

and

$$\overline{f}(b^3) = \overline{f}(b)\overline{f}(b)\overline{f}(b) = \sigma_2 \cdot \sigma_2 \cdot \sigma_2 = \sigma_2^3 = 1$$

In particular, the above shows that $R \subseteq \ker(\overline{f})$. Since $\ker(\overline{f})$ is a normal subgroup of F with $R \subseteq \ker(\overline{f})$, it follows by the definition of N that $N \subseteq \ker(\overline{f})$.

The above results show that there exists a group homomorphism $g : F/N \to H$ such that $g(aN) = \sigma_1$ and $g(bN) = \sigma_2$. Note that since $H = \langle \sigma_1, \sigma_2 \rangle$ and since $\sigma_1, \sigma_2 \in g(F/N)$ we have that g is a surjection. In particular, this gives that $|F/N| \geq |H|$. However, we clearly have $|H| = \infty$ so that the previous inequality gives $|F/N| \geq \infty$. We conclude that F/N is infinite.

In conclusion, we have shown that F/N is an infinite, nonabelian group. This completes the proof. $\square$

Problem 7. *Show that the group defined by the generators a, b and relations $a^2 = e, b^3 = e$ is infinite and nonabelian.*

Proof. Let $X = \{a, b\}, R = \{a^2, b^3\}$, and N be the smallest normal subgroup of F with $R \subseteq N$ where F is the free group on X. By definition, we have that the group defined by the generators X and relations R is F/N.

Before we begin, we prove that if $\theta : H \to K$ is a surjective group homomorphism and if K is nonabelian then H is nonabelian. Indeed, since K is nonabelian, there exist $k_1, k_2 \in K$ such that $k_1k_2 \neq k_2k_1$. As θ is a surjection, there exist $h_1, h_2 \in H$ such that $\theta(h_1) = k_1$ and $\theta(h_2) = k_2$. Since θ is a group homomorphism, this gives

$$k_1k_2 = \theta(h_1)\theta(h_2) = \theta(h_1h_2)$$

and

$$k_2k_1 = \theta(h_2)\theta(h_1) = \theta(h_2h_1)$$

Hence, if $h_1h_2 = h_2h_1$ then the above results would imply that

$$k_1k_2 = \theta(h_1h_2) = \theta(h_2h_1) = k_2k_1$$

which is a contradiction since $k_1k_2 \neq k_2k_1$. Thus, we have $h_1h_2 \neq h_2h_1$ so that H is nonabelian. This proves the result.

We now prove the main result. Towards this end, consider $\sigma_1, \sigma_2 \in S_{\mathbb{Z}}$ given by

$$\sigma_1 = \cdots(-4 \quad -3)(-1 \quad 0)(2 \quad 3)\cdots$$

and

$$\sigma_2 = \cdots(-3 \quad -2 \quad -1)(0 \quad 1 \quad 2)(3 \quad 4 \quad 5)\cdots$$

Clearly, we have $|\sigma_1| = 2$ and $|\sigma_2| = 3$. Let $H = \langle \sigma_1, \sigma_2 \rangle \subseteq S_{\mathbb{Z}}$ and define

$$f : X \to H \quad \text{by} \quad a \mapsto \sigma_1 \quad b \mapsto \sigma_2$$

Since F is free on X, there exists a unique group homomorphism $\overline{f} : F \to H$ such that

$$\overline{f}(a) = f(a) = \sigma_1 \quad \text{and} \quad \overline{f}(b) = f(b) = \sigma_2$$

Note that since $\overline{f}$ is a group homomorphism we have

$$\overline{f}(a^2) = \overline{f}(a)\overline{f}(a) = \sigma_1 \cdot \sigma_1 = \sigma_1^2 = 1$$

and

$$\overline{f}(b^3) = \overline{f}(b)\overline{f}(b)\overline{f}(b) = \sigma_2 \cdot \sigma_2 \cdot \sigma_2 = \sigma_2^3 = 1$$

In particular, the above shows that $R \subseteq \ker(\overline{f})$. Since $\ker(\overline{f})$ is a normal subgroup of F with $R \subseteq \ker(\overline{f})$, it follows by the definition of N that $N \subseteq \ker(\overline{f})$.

The above results show that there exists a group homomorphism $g : F/N \to H$ such that $g(aN) = \sigma_1$ and $g(bN) = \sigma_2$. Note that since $H = \langle \sigma_1, \sigma_2 \rangle$ and since $\sigma_1, \sigma_2 \in g(F/N)$ we have that g is a surjection. Furthermore, note that $(\sigma_1 \circ \sigma_2)(1) = 3$ but $(\sigma_2 \circ \sigma_1)(1) = 2$ so that $\sigma_1\sigma_2 \neq \sigma_2\sigma_1$. In particular, this shows that H is nonabelian. By our preliminary result, then, this shows that F/N is nonabelian.

Now, since g is a surjection, we have that $|F/N| \geq |H|$. We claim that H is infinite. Indeed, consider the orbit $\mathcal{O}$ of $0 \in \mathbb{Z}$ in the action of H on $\mathbb{Z}$. In particular, we have that $\mathcal{O} = \mathbb{Z}$ by the definition of H. By the Orbit-Stabilizer Theorem, we have that

$$\infty = |\mathbb{Z}| = |\mathcal{O}| = |H : \mathrm{Stab}_H(0)|$$

so that

$$|H| = \infty \cdot |\mathrm{Stab}_H(0)| = \infty$$

By the above, this gives

$$|F/N| \geq |H| = \infty$$

so that $|F/N| = \infty$. In conclusion, we have shown that F/N is an infinite, nonabelian group. This completes the proof. $\square$

Problem 8. *The group defined by the generators a, b and relations $a^n = e$ (for a positive integer n with $n \geq 3$), $b^2 = e$, and $abab = e$ is the dihedral group D_{2n}.*

Proof. Let $X = \{a, b\}, R = \{a^n, b^2, abab\}$, and N be the smallest normal subgroup of F with $R \subseteq N$ where F is the free group on X. By definition, we have that the group defined by the generators X and relations R is F/N.

Now, recall that $D_{2n} = \langle r, s\rangle$ with $|r| = n, |s| = 2$, and $srs = r^{-1}$. Define

$$f : X \to D_{2n} \quad \text{by} \quad a \mapsto r \quad b \mapsto s$$

Since F is free on X, there exists a unique group homomorphism $\overline{f} : F \to D_{2n}$ such that

$$\overline{f}(a) = f(a) = r \quad \text{and} \quad \overline{f}(b) = f(b) = s$$

Note that since $\overline{f}$ is a group homomorphism we have

$$\overline{f}(a^n) = \overline{f}(a)^n = r^n = 1$$

and

$$\overline{f}(b^2) = \overline{f}(b)\overline{f}(b) = s \cdot s = s^2 = 1$$

and

$$\overline{f}(abab) = \overline{f}(a)\overline{f}(b)\overline{f}(a)\overline{f}(b) = rsrs = rr^{-1} = 1$$

In particular, the above shows that $R \subseteq \ker(\overline{f})$. Since $\ker(\overline{f})$ is a normal subgroup of F with $R \subseteq \ker(\overline{f})$, it follows by the definition of N that $N \subseteq \ker(\overline{f})$.

The above results show that there exists a group homomorphism $g : F/N \to D_{2n}$ such that $g(aN) = r$ and $g(bN) = s$. Note that since $D_{2n} = \langle r, s\rangle$ and since $r, s \in g(F/N)$ we have that g is a surjection. In particular, this gives that $|F/N| \geq |D_{2n}| = 2n$.

We will now show that $|F/N| \leq 2n$. We claim that every element $wN \in F/N$ has a representative of the form $a^i b^j$ for some $i \in \{0, 1, \ldots, n-1\}$ and $j \in \{0, 1\}$. Indeed, let $wN \in F/N$. Since $a^n, b^2 \in N$, we can choose a representative for wN of the form

$$a^{n_1} b^{n_2} a^{n_3} b^{n_4} \cdots b^{n_m}$$

where $n_i \in \{0, 1, \ldots, n-1\}$ for odd values of $i \in \{1, \ldots, m\}$ and $n_i \in \{0, 1\}$ for even values of $i \in \{1, \ldots, m\}$.

Now, among all such representatives for wN of this form, choose one where m is as small as possible. First, suppose that $m \geq 4$. In this case, we have that $n_2 = 1 = n_4$. Notice that since $abab \in N$ and $b^2 \in N$, we have that

$$ba^{n_3}bN = a^{n-n_3}N$$

which contradicts the minimality of m. Secondly, suppose that $m = 3$. In this case, we have that $n_2 = 1$. Notice that since $b^2 \in N$ and $abab \in N$, we have that

$$ba^{n_3}N = ba^{n_3}b^2N = ba^{n_3}bbN = a^{n-n_3}bN$$

which again contradicts the minimality of m. Hence, we must have $m \leq 2$ by the above results. This shows that wN has a representative of the form $a^i b^j$ for some $i \in \{0, 1, \ldots, n-1\}$ and $j \in \{0, 1\}$. In particular, this gives that $|F/N| \leq 2n$.

By the above results, we have that $|F/N| = 2n = |D_{2n}|$. Since g is a surjection, this now gives that g is a bijection so that g is an isomorphism. Thus, we obtain $F/N \simeq D_{2n}$. $\square$

Homework 21: Page 74 #3, 5, 9

Problem 3. *Let X be a set. Then the free abelian group on X is (isomorphic to) the group defined by the generators X and the relations $\{aba^{-1}b^{-1} = e : a, b \in X\}$.*

Proof. Let $R = \{aba^{-1}b^{-1} : a, b \in X\}$ and N be the smallest normal subgroup of F with $R \subseteq N$ where F is the free group on X. By definition, we have that the group defined by generators X and relations R is F/N. Note that if $X = \emptyset$, then both the free abelian group on X and F/N are trivial and hence isomorphic. Hence, we may assume $X \neq \emptyset$.

We first show that F/N is the free abelian group on the set $Y = \{aN : a \in X\}$. To show that F/N is abelian, it is enough to show that for any $a, b \in X$ we have $aNbN = bNaN$ as this will imply that $w_1Nw_2N = w_2Nw_1N$ for any $w_1N, w_2N \in F/N$. Indeed, note that since $aba^{-1}b^{-1} \in N$ we have

$$b^{-1}a^{-1}N = b^{-1}a^{-1}(aba^{-1}b^{-1})N = a^{-1}b^{-1}N$$

so that

$$abN = (b^{-1}a^{-1}N)^{-1} = (a^{-1}b^{-1}N)^{-1} = baN$$

so that

$$aNbN = abN = baN = bNaN$$

Hence, we have that F/N is abelian.

Now, note that since $X \neq \emptyset$ we have $Y \neq \emptyset$. Next, suppose that $wN \in F/N$. Since $w \in F$, we have that $w = a_1^{n_1} \cdots a_m^{n_m}$, for some $a_1, \ldots, a_m \in X$ and $n_1, \ldots, n_m \in \mathbb{Z}$. Hence, we obtain

$$wN = a_1^{n_1} \cdots a_m^{n_m} N = a_1^{n_1} N \cdots a_m^{n_m} N = (a_1N)^{n_1} \cdots (a_mN)^{n_m} \in \langle Y \rangle$$

Since $wN \in F/N$ was arbitrary, the above shows that $F/N = \langle Y \rangle$.

Finally, suppose that for some distinct elements $a_1N, \ldots, a_mN \in Y$ we have

$$(a_1N)^{n_1} \cdots (a_mN)^{n_m} = N$$

In this case, we have

$$N = (a_1N)^{n_1} \cdots (a_mN)^{n_m} = a_1^{n_1} N \cdots a_m^{n_m} N = a_1^{n_1} \cdots a_m^{n_m} N$$

so that $a_1^{n_1} \cdots a_m^{n_m} \in N$. We claim that $n_1 = \cdots = n_m = 0$.

Before proving this claim, note that by the definition of N we have

$$N = \langle a^k b^l a^{-k} b^{-l} : a, b \in X \text{ and } k, l \in \mathbb{N} \rangle$$

In particular, this observation implies that if $w \in N$ then the exponent sum of each distinct letter appearing in w is equal to 0.

By the above observation, since $a_1^{n_1} \cdots a_m^{n_m} \in N$, it follows that the exponent sum of each distinct letter appearing in $a_1^{n_1} \cdots a_m^{n_m}$ is equal to 0. However, recall that the elements $a_1N, \ldots, a_mN \in Y$ are distinct so that $a_1, \ldots, a_m$ are distinct. Therefore, for each $j \in \{1, \ldots, m\}$, the exponent sum of a_j is equal to n_j so that $n_j = 0$. This proves the claim that $n_1 = \cdots = n_m = 0$. We may now conclude that F/N is indeed the free abelian group on Y.

Now, let G be the free abelian group on X. Note that if $a, b \in X$ are distinct then the cosets aN and bN are also distinct. On the other hand, if aN and bN are distinct cosets for some $a, b \in X$, then a and b are also distinct. From these observations, it now follows that

$$|Y| = |\{xN : x \in X\}| = |X|$$

But since G is the free abelian group on X and F/N is the free abelian group on Y and $|X| = |Y|$ by the above equality, it now follows that $G \simeq F/N$. $\square$

Problem 5. *The direct sum of a family of free abelian groups is a free abelian group.*

Proof. Let $(A_i)_{i\in I}$ be a family of free abelian groups and let $X_i \subseteq A_i$ be a basis for A_i for each $i \in I$. Let $A = \bigoplus_{i\in I} A_i$. Note that since the direct sum of abelian groups is an abelian group, we have that A is an abelian group. Let X be the disjoint union of the X_i. Note that if $I = \emptyset$ then $X = \emptyset$. In this case, we have that A is trivial and hence A is the free abelian group on $X = \emptyset$. Therefore, we may assume that $I \neq \emptyset$.

First, we show that $A = \langle X \rangle$. Towards this end, let $a \in A$. Then there is some subset $\{i_1, \ldots, i_m\} \subseteq I$ such that

$$a = a_1 + \cdots + a_m$$

where $a_j \in A_{i_j}$ for each $j \in \{1, \ldots, m\}$. Now, for each $j \in \{1, \ldots, m\}$ since A_{i_j} is free on X_{i_j}, we know that a_j is equal to a finite $\mathbb{Z}$-linear combination of elements in X_{i_j}. Since $X_{i_j} \subseteq X$ for each $j \in \{1, \ldots, m\}$, we see by the above equality that a is equal to a finite $\mathbb{Z}$-linear combination of elements in X. In particular, this gives that $a \in \langle X \rangle$. Since $a \in A$ was arbitrary, this shows that $A = \langle X \rangle$.

We will use the above result to show that A is free on X in the category of abelian groups. Note that $X \neq \emptyset$ since $I \neq \emptyset$. Next, let $i : X \to A$ be the inclusion map. Let G be any abelian group let $f : X \to G$ be any map of sets. For each $j \in I$, define

$$f_j : X_j \to G \quad \text{by} \quad x \mapsto f(x)$$

so that f_j is the restriction of f to X_j. Since A_j is the free abelian group on X_j, there exists a unique group homomorphism

$$\overline{f}_j : A_j \to G \quad \text{with} \quad \overline{f}_j(x) = f_j(x) \quad \text{for all} \quad x \in X_j$$

In particular, note that by the definition of $\overline{f}_j$ that we have $\overline{f}_j$ is equal to f_j on X_j.

For each $j \in I$, let $i_j : A_j \to A$ be the canonical inclusion map. In particular, note that i_j is equal to i on X_j. Now, we know that A together with $(i_j)_{j\in I}$ is a coproduct for the family of abelian groups $(A_j)_{j\in I}$ in the category of abelian groups. Hence, since G is an abelian group and since $\left(\overline{f}_j : A_j \to G\right)_{j\in I}$ is a family of morphisms in the category of abelian groups, it follows that there is a unique group homomorphism

$$\phi : A \to G \quad \text{with} \quad \phi \circ i_j = \overline{f}_j$$

for each $j \in I$. It remains to show that $\phi \circ i = f$ and that ϕ is unique.

We show here that $\phi \circ i = f$. Towards this end, let $x \in X$. Then we have $x \in X_j$ for some $j \in I$. The above results give

$$(\phi \circ i)(x) = \phi(i(x)) = \phi(i_j(x)) = \overline{f}_j(x) = f_j(x) = f(x)$$

Since $x \in X$ was arbitrary, this shows that $\phi \circ i = f$.

Lastly, suppose that $\psi : A \to G$ is a group homomorphism such that $\psi \circ i = f$. Let $a \in A$. Since $A = \langle X \rangle$ by the above, there are distinct $x_1, \ldots, x_m \in X$ and $n_1, \ldots, n_m \in \mathbb{Z}$ such that we have

$$a = n_1 x_1 + \cdots + n_m x_m$$

Now, we have $x_1 \in X_{z_1}, \ldots, x_m \in X_{z_m}$ for some subset $\{z_1, \ldots, z_m\} \subseteq I$. By this observation, since ψ is a group homomorphism, and by the above results, we obtain

$$\begin{aligned}
\psi(a) &= \psi(n_1 x_1 + \cdots + n_m x_m) \\
&= n_1 \psi(x_1) + \cdots + n_m \psi(x_m) \\
&= n_1 \psi(i_{z_1}(x_1)) + \cdots + \psi(i_{z_m}(x_m)) \\
&= n_1 \psi(i(x_1)) + \cdots + n_m \psi(i(x_m)) \\
&= n_1 f(x_1) + \cdots + n_m f(x_m) \\
&= n_1 \phi(i(x_1)) + \cdots + n_m \phi(i(x_m)) \\
&= n_1 \phi(x_1) + \cdots + n_m \phi(x_m) \\
&= \phi(n_1 x_1 + \cdots + n_m x_m) \\
&= \phi(a)
\end{aligned}$$

Since $a \in A$ was arbitrary, this shows that $\psi = \phi$ so that ϕ is unique.

The above proof shows that A is a free object in the category of abelian groups. In particular, this shows that A is a free abelian group, completing the proof. $\square$

Problem 9. *Let G be a finitely generated abelian group in which no element (except 0) has finite order. Then G is a free abelian group.*

Proof. Since G is finitely generated, there exists a finite subset $X \subseteq G$ such that $G = \langle X \rangle$. If $X = \emptyset$, then G is trivial so that G is a free abelian group. Hence, we assume that $X \neq \emptyset$. Now, let $X = \{x_1, \ldots, x_n\}$. Let $Z = \bigoplus_{i=1}^{n} \mathbb{Z}$ and define a map

$$\phi : Z \to G \quad \text{by} \quad (m_1, \ldots, m_n) \mapsto m_1x_1 + \cdots + m_nx_n$$

Clearly, ϕ is a well-defined map. Now, let $(m_1, \ldots, m_n), (k_1, \ldots, k_n) \in Z$. Then

$$\begin{aligned}
\phi((m_1, \ldots, m_n) + (k_1, \ldots, k_n)) &= \phi((m_1 + k_1, \ldots, m_n + k_n)) \\
&= (m_1 + k_1)x_1 + \cdots + (m_n + k_n)x_n \\
&= (m_1x_1 + \cdots + m_nx_n) + (k_1x_1 + \cdots + k_nx_n) \\
&= \phi((m_1, \ldots, m_n)) + \phi((k_1, \ldots, k_n))
\end{aligned}$$

so that ϕ is a group homomorphism. Furthermore, suppose that $a \in G$. Then

$$a = m_1x_1 + \cdots + m_nx_n$$

for some $m_1, \ldots, m_n \in \mathbb{Z}$. Note that $(m_1, \ldots, m_n) \in Z$ and that

$$\phi((m_1, \ldots, m_n)) = m_1x_1 + \cdots + m_nx_n = a$$

so that ϕ is surjective. By the First Isomorphism Theorem, we have $Z/\ker\phi \simeq G$. If $\ker\phi$ is trivial, then we have $Z \simeq G$ so that G is a free abelian group of rank n since Z is a free abelian group of rank n. Therefore, we may assume that $\ker\phi$ is nontrivial.

Now, since $\ker\phi$ is a nontrivial subgroup of Z and since Z is clearly a free abelian group of rank n, it follows that there is a basis $\{y_1, \ldots, y_n\}$ for Z, some $r \in \{1, \ldots, n\}$, and positive integers $d_1, \ldots, d_r$ with $d_1 \big| d_2 \big| \cdots \big| d_r$ such that $\ker\phi$ is a free abelian group with basis $\{d_1y_1, \ldots, d_ry_r\}$. This gives

$$G \simeq Z/\ker\phi = \underbrace{\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}}_{n-r \text{ times}} \oplus \mathbb{Z}/(d_1) \oplus \cdots \oplus \mathbb{Z}/(d_r)$$

We wish to show that $d_1 = \cdots = d_r = 1$.

For the sake of contradiction, suppose that $d_1 \geq 2$. Since ϕ is a homomorphism and since $d_1y_1 \in \ker\phi$, we have

$$0 = \phi(d_1y_1) = d_1\phi(y_1)$$

Now, if $\phi(y_1) = 0$, then $y_1 \in \ker\phi$. Since $\{d_1y_1, \ldots, d_ry_r\}$ is a basis for $\ker\phi$, there exist $n_1, \ldots, n_r \in \mathbb{Z}$ such that

$$y_1 = n_1d_1y_1 + \cdots + n_rd_ry_r$$

Subtracting y_1 from both sides of this equality gives

$$0 = (n_1d_1 - 1)y_1 + \cdots + (n_rd_r)y_r$$

Since $\{y_1, \ldots, y_r\} \subseteq \{y_1, \ldots, y_n\}$ and since $\{y_1, \ldots, y_n\}$ is a basis for the free abelian group Z, the above equality implies that

$$n_1d_1 - 1 = \cdots = n_rd_r = 0$$

In particular, we have $n_1 d_1 - 1 = 0$ so that $n_1 d_1 = 1$. Since $n_1 \in \mathbb{Z}$, this forces $d_1 \in \{-1, 1\}$. However, we know that d_1 is not negative so that $d_1 = 1$. But this contradicts the fact that $d_1 \geq 2$. We conclude that $\phi(y_1) \neq 0$ and so $\phi(y_1)$ is a nonidentity element of G.

By hypothesis, we have since $\phi(y_1)$ is a nonidentity element of G that $\phi(y_1)$ has infinite order. However, recall that $0 = d_1\phi(y_1)$. This implies that $\phi(y_1)$ has order at most d_1. In particular, we now have that $\phi(y_1)$ has finite order which contradicts the fact that $\phi(y_1)$ has infinite order. We conclude that $d_1 = 1$.

In exactly the same fashion as above, we obtain $d_1 = \cdots = d_r = 1$ so that

$$(d_1) = \cdots = (d_r) = \mathbb{Z}$$

By the above, this gives

$$G \simeq \underbrace{\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}}_{n-r \text{ times}} \oplus \underbrace{\mathbb{Z}/\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/\mathbb{Z}}_{r \text{ times}} \simeq \underbrace{\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}}_{n-r \text{ times}}$$

This shows that G is a free abelian group of rank $n - r$, completing the proof. $\square$

Homework 22: Page 74 #12; Page 81 #9, 11

Problem 12. *Let F be the free (not necessarily abelian) group on a set X and G the free group on a set Y. Let F' be the subgroup of F* generated *by $\{aba^{-1}b^{-1} : a, b \in F\}$ and similarly for G'.*

(a): *$F' \trianglelefteq F, G' \trianglelefteq G$, and $F/F', G/G'$ are abelian.*

(b): *F/F' is a free abelian group of rank $|X|$; G/G' is a free abelian group of rank $|Y|$.*

(c): *$F \simeq G$ if and only if $|X| = |Y|$.*

Proof. (a): We prove that $F' \trianglelefteq F$. Let $C = \{aba^{-1}b^{-1} : a, b \in F\}$ so that $F' = \langle C \rangle$. We claim that F' is characteristic in F. Indeed, let $\sigma \in \mathrm{Aut}(F)$ and $a, b \in F$ so that $aba^{-1}b^{-1} \in C$ is an arbitrary element of C. Since σ is a group homomorphism, we have

$$\sigma(aba^{-1}b^{-1}) = \sigma(a)\sigma(b)\sigma(a)^{-1}\sigma(b)^{-1} \in C$$

In other words, σ maps elements of C to elements of C. Since σ is a bijection, this implies that σ maps the generators of F' bijectively onto themselves. This gives that $\sigma(F') = F'$ so that F' is characteristic in F. In particular, we now have $F' \trianglelefteq F$. In exactly the same fashion, we obtain that $G' \trianglelefteq G$.

We now prove that F/F' is abelian. Towards this end, let $aF', bF' \in F/F'$. Then since $aba^{-1}b^{-1} \in F'$, we have

$$a^{-1}b^{-1}F' = a^{-1}b^{-1}(aba^{-1}b^{-1})F' = a^{-1}b^{-1}F'$$

so that

$$aF'bF' = abF' = (b^{-1}a^{-1}F')^{-1} = (a^{-1}b^{-1}F')^{-1} = baF' = bF'aF'$$

Since $aF', bF' \in F/F'$ were arbitrary, this shows that F/F' is abelian. In exactly the same fashion, we obtain that G/G' is abelian. $\square$

Proof. (b): We prove that F/F' is a free abelian group of rank $|X|$. Let C be as above. Recall that $F' \trianglelefteq F$ and $F' = \langle C \rangle$. Let N be the smallest normal subgroup of F containing the set $\{xyx^{-1}y^{-1} : x, y \in X\}$. Note that F' necessarily contains the set $\{xyx^{-1}y^{-1} : x, y \in X\}$ and since $F' \trianglelefteq G$, this implies that $N \subseteq F'$. On the other hand, note that N must necessarily contain C. Since $F' = \langle C \rangle$, this implies that $F' \subseteq N$. The above arguments show that $F' = N$.

Since $F' = N$, we know by the proof of Problem 3 that F/F' is the free abelian group on the set $\{xF' : x \in X\}$. In this same problem, we also saw that $|\{xF' : x \in X\}| = |X|$. Hence, we obtain that F/F' is a free abelian group of rank $|X|$. In exactly the same fashion, we obtain that G/G' is a free abelian group of rank $|Y|$. $\square$

Proof. (c): For the first direction, assume that $F \simeq G$. Then there exists an isomorphism $\phi : F \to G$. Define

$$\psi : F \to G/G' \quad \text{by} \quad a \mapsto \phi(a)G'$$

Clearly, we have that ψ is a well-defined map. Let $a, b \in F$. Furthermore, since ϕ is a group homomorphism, we have

$$\psi(ab) = \phi(ab)G' = \phi(a)\phi(b)G' = \phi(a)G'\phi(b)G' = \psi(a)\psi(b)$$

so that ψ is a group homomorphism. Next, let C be as above and suppose that $aba^{-1}b^{-1} \in C$. Then since ϕ is a group homomorphism and since G/G' is abelian, we have that

$$\begin{aligned}
\psi(aba^{-1}b^{-1}) &= \phi(aba^{-1}b^{-1})G' \\
&= \phi(a)\phi(b)\phi(a)^{-1}\phi(b)^{-1}G' \\
&= \phi(a)G'\phi(b)G'\phi(a)^{-1}G'\phi(b)^{-1}G' \\
&= \phi(a)G'\phi(a)^{-1}G\phi(b)G'\phi(b)^{-1}G' \\
&= \phi(a)\phi(a)^{-1}\phi(b)\phi(b)^{-1}G' \\
&= 1G' \\
&= G'
\end{aligned}$$

In particular, the above shows that $C \subseteq \ker\psi$ so that by the definition of F' we have $F' \subseteq \ker\psi$. Therefore, if $\pi : F \to F/F'$ is the canonical projection map, then the above shows that there exists a group homomorphism $\theta : F/F' \to G/G'$ such that $\theta \circ \pi = \psi$.

We claim that θ is an isomorphism. Since θ is a group homomorphism, it remains to prove that θ is a bijection. First, suppose that $aF', bF' \in F/F'$ and $\theta(aF') = \theta(bF')$. Then we have

$$\phi(a)G' = \psi(a) = \theta(\pi(a)) = \theta(aF') = \theta(bF') = \theta(\pi(b)) = \psi(b) = \phi(b)G'$$

In particular, the above equality implies that there is some $c \in G'$ so that $\phi(a) = \phi(b)c$. Since $c \in G' \subseteq G$ and ϕ is a surjection, there exists some $d \in F$ so that $c = \phi(d)$. Note that since ϕ is an isomorphism that ϕ maps F' bijectively onto G'. Thus, since $c \in G'$, it now follows that in fact $d \in F'$. Furthermore, as ϕ is a group homomorphism, we have

$$\phi(a) = \phi(b)c = \phi(b)\phi(d) = \phi(bd)$$

Since ϕ is an injection, the above equality implies that $a = bd$. Since $d \in F'$, we now have that

$$aF' = bdF' = bF'$$

In particular, this shows that θ is an injection.

Next, let $aG' \in G/G'$. Since $a \in G$ and since ϕ is a surjection, there exists some $b \in F$ such that $\phi(b) = a$. Then we have $bF' \in F/F'$ and

$$aG' = \phi(b)G' = \psi(b) = \theta(\pi(b)) = \theta(bF')$$

so that θ is a surjection.

The above results show that θ is an isomorphism so that $F/F' \simeq G/G'$. Recall by the above we have that F/F' is a free abelian group of rank $|X|$ and G/G' is a free abelian group of rank $|Y|$. Since $F/F' \simeq G/G'$, this observation implies that $|X| = |Y|$.

For the second direction, assume that $|X| = |Y|$. Recall that F is the free group on X and G is the free group on Y. That is, F is free on X in the category of groups and G is free on Y in the category of groups. Since $|X| = |Y|$, this implies that there exists an equivalence $\phi : F \to G$. Since equivalences in the category of groups are isomorphisms, this gives that ϕ is an isomorphism so that $F \simeq G$. This completes the proof. $\square$

Problem 9. *How many subgroups of order p^2 does the abelian group $\mathbb{Z}_{p^3} \oplus \mathbb{Z}_{p^2}$ have?*

Proof. Let $G = \mathbb{Z}_{p^3} \oplus \mathbb{Z}_{p^2}$. Suppose that H is a subgroup of G of order p^2. Since the direct sum of abelian groups is an abelian group, we have that G is an abelian group. Since subgroups of abelian groups are abelian, we have that H is an abelian group of order p^2. Hence, by the Fundamental Theorem of Finitely Generated Abelian Groups, it must be the case that either $H \simeq \mathbb{Z}_p \oplus \mathbb{Z}_p$ or $H \simeq \mathbb{Z}_{p^2}$. In particular, this shows that every subgroup of G of order p^2 is isomorphic to either $\mathbb{Z}_p \oplus \mathbb{Z}_p$ or $\mathbb{Z}_{p^2}$.

Firstly, we count the number of subgroups of G that are isomorphic to $\mathbb{Z}_p \oplus \mathbb{Z}_p$. Recall that, up to isomorphism, there is exactly one group of order p. Therefore, in this case, such a subgroup of G must be of the form $H \oplus K$, where H is a subgroup of $\mathbb{Z}_{p^3}$ of order p and K is a subgroup of $\mathbb{Z}_{p^2}$ of order p. Since $\mathbb{Z}_{p^3}$ is cyclic and since p divides $p^3 = |\mathbb{Z}_{p^3}|$, it follows that $\mathbb{Z}_{p^3}$ has exactly one subgroup of order p, namely $\langle p^2 \rangle$. By the same reasoning, we also have that $\mathbb{Z}_{p^2}$ has exactly one subgroup of order p, namely $\langle p \rangle$. Hence, there is exactly one subgroup of G of order p^2 that is isomorphic to $\mathbb{Z}_p \oplus \mathbb{Z}_p$, namely $\langle p^2 \rangle \oplus \langle p \rangle$.

Secondly, we count the number of subgroups of G that are isomorphic to $\mathbb{Z}_{p^2}$. Since $\mathbb{Z}_{p^2}$ is cyclic, this task is equivalent to finding the number of cyclic subgroups of G of order p^2. Note that every cyclic subgroup of G of order p^2 is generated by some element $(a, b) \in G$ of order p^2. Furthermore, we know that for $(a, b) \in G$, we have

$$|\langle (a, b) \rangle| = |(a, b)| = \operatorname{lcm}(|a|, |b|)$$

Hence, we must first find the number of elements $(a, b) \in G$ such that $\operatorname{lcm}(|a|, |b|) = p^2$.

Towards this end, suppose that $(a, b) \in G$ with $\operatorname{lcm}(|a|, |b|) = p^2$. By Lagrange's Theorem, since $a \in \mathbb{Z}_{p^3}$, we have $|a| \in \{1, p, p^2, p^3\}$. Similarly, since $b \in \mathbb{Z}_{p^2}$, we have $|b| \in \{1, p, p^2\}$. We now arrive at the following distinct possibilities for $|a|$ and $|b|$ such that $\operatorname{lcm}(|a|, |b|) = p^2$. These are

$$|a| \in \{1, p, p^2\} \text{ and } |b| = p^2 \quad \text{or} \quad |a| = p^2 \text{ and } |b| \in \{1, p\}$$

Now, let ϕ denote Euler's totient function. Note that since $\mathbb{Z}_{p^2}$ and $\mathbb{Z}_{p^3}$ are cyclic groups that the number of elements of order p in both of these groups is equal to $\phi(p) = p - 1$. By the same reasoning, the number of elements of order p^2 in both $\mathbb{Z}_{p^2}$ and $\mathbb{Z}_{p^3}$ is equal to $\phi(p^2) = p^2 - p$. Hence, the first case for $|a|$ and $|b|$ gives

$$[1 + \phi(p) + \phi(p^2)] \cdot \phi(p^2) = [1 + (p - 1) + (p^2 - p)] \cdot (p^2 - p) = p^2 \cdot (p^2 - p) = p^4 - p^3$$

elements of order p^2 in G of the first type. Similarly, the second case for $|a|$ and $|b|$ gives

$$\phi(p^2) \cdot [1 + \phi(p)] = (p^2 - p) \cdot [1 + (p - 1)] = (p^2 - p) \cdot p = p^3 - p^2$$

elements of order p^2 in G of the second type. Thus, there are exactly

$$(p^4 - p^3) + (p^3 - p^2) = p^4 - p^2$$

distinct elements of order p^2 in G.

Finally, note that each element of order p^2 in G generates a cyclic subgroup of G of order p^2. In each of these cyclic subgroups, however, there are exactly $\phi(p^2) = p^2 - p$

elements of order p^2 that will generate the same cyclic subgroup. Therefore, there are

$$\frac{p^4 - p^2}{\phi(p^2)} = \frac{(p^2 + p)(p^2 - p)}{(p^2 - p)} = p^2 + p$$

distinct cyclic subgroups of G of order p^2.

Combining the above results, we have that there are exactly $1 + (p^2 + p) = p^2 + p + 1$ subgroups of G of order p^2. This completes the proof. $\square$

Problem 11. *Let G, H, and K be finitely generated abelian groups.*
(a): *If $G \oplus G \simeq H \oplus H$, then $G \simeq H$.*
(b): *If $G \oplus H \simeq G \oplus K$, then $H \simeq K$.*
(c): *If G_1 is a free abelian group of rank $\aleph_0$, then $G_1 \oplus \mathbb{Z} \oplus \mathbb{Z} \simeq G_1 \oplus \mathbb{Z}$, but $\mathbb{Z} \oplus \mathbb{Z} \not\simeq \mathbb{Z}$.*

Proof. (a): By the Fundamental Theorem of Finitely Generated Abelian Groups, since G and H are finitely generated abelian groups, we can write

$$G \simeq \bigoplus_{i=1}^{r} \mathbb{Z}_{m_i} \oplus \bigoplus_{i=1}^{a} \mathbb{Z}$$

and

$$H \simeq \bigoplus_{i=1}^{s} \mathbb{Z}_{n_i} \oplus \bigoplus_{i=1}^{b} \mathbb{Z}$$

where $m_1, \ldots, m_r$ is a unique (possibly empty) list of positive integers with $m_1 > 1$ and $m_1 \big| \cdots \big| m_r$ and a is a nonnegative integer; $n_1, \ldots, n_s$ is a unique (possibly empty) list of positive integers with $n_1 > 1$ and $n_1 \big| \cdots \big| n_s$ and b is a nonnegative integer.

Now, note that after rearrangement, we have

$$G \oplus G \simeq \mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_1} \oplus \cdots \oplus \mathbb{Z}_{m_r} \oplus \mathbb{Z}_{m_r} \oplus \bigoplus_{i=1}^{2a} \mathbb{Z}$$

and

$$H \oplus H \simeq \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_1} \oplus \cdots \oplus \mathbb{Z}_{n_s} \oplus \mathbb{Z}_{n_s} \oplus \bigoplus_{i=1}^{2b} \mathbb{Z}$$

Since $G \oplus G \simeq H \oplus H$, we have by the above that

$$\mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_1} \oplus \cdots \oplus \mathbb{Z}_{m_r} \oplus \mathbb{Z}_{m_r} \oplus \bigoplus_{i=1}^{2a} \mathbb{Z} \simeq \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_1} \oplus \cdots \oplus \mathbb{Z}_{n_s} \oplus \mathbb{Z}_{n_s} \oplus \bigoplus_{i=1}^{2b} \mathbb{Z}$$

Now, we know that the direct sum of two finitely generated abelian groups is a finitely generated abelian group. Hence, since G is a finitely generated abelian group, we have that $G \oplus G$ is a finitely generated abelian group. By the uniqueness portion of the Fundamental Theorem of Finitely Generated Abelian Groups, the above gives

$$r = s, \quad 2a = 2b, \quad m_i = n_i \text{ for all } i \in \{1, \ldots, r\}$$

Clearly, the fact that $2a = 2b$ gives $a = b$. We may now conclude that

$$G \simeq \bigoplus_{i=1}^{r} \mathbb{Z}_{m_i} \oplus \bigoplus_{i=1}^{a} \mathbb{Z} = \bigoplus_{i=1}^{s} \mathbb{Z}_{n_i} \oplus \bigoplus_{i=1}^{b} \mathbb{Z} \simeq H$$

so that $G \simeq H$. This completes the proof. $\square$

Proof. (b): By the Fundamental Theorem of Finitely Generated Abelian Groups, since G, H, and K are finitely generated abelian groups, we can write

$$G \simeq \bigoplus_{i=1}^{r} \mathbb{Z}_{p_i^{m_i}} \oplus \bigoplus_{i=1}^{a} \mathbb{Z}$$

and

$$H \simeq \bigoplus_{i=1}^{s} \mathbb{Z}_{q_i^{n_i}} \oplus \bigoplus_{i=1}^{b} \mathbb{Z}$$

and

$$K \simeq \bigoplus_{i=1}^{t} \mathbb{Z}_{z_i^{k_i}} \oplus \bigoplus_{i=1}^{c} \mathbb{Z}$$

where $p_1^{m_1}, \ldots, p_r^{m_r}$ is a unique (possibly empty) list of powers of prime numbers up to the order of its members, $m_1, \ldots, m_r$ are positive integers, and a is a nonnegative integer; $q_1^{n_1}, \ldots, q_s^{n_s}$ is a unique (possibly empty) list of powers of prime numbers up to the order of its members, $n_1, \ldots, n_s$ are positive integers, and b is a nonnegative integer; $z_1^{k_1}, \ldots, z_t^{k_t}$ is a unique (possibly empty) list of powers of prime numbers up to the order of its members, $k_1, \ldots, k_t$ are positive integers, and c is a nonnegative integer.

Now, note that after rearrangement, we have

$$G \oplus H \simeq \bigoplus_{i=1}^{r} \mathbb{Z}_{p_i^{m_i}} \oplus \bigoplus_{i=1}^{s} \mathbb{Z}_{q_i^{n_i}} \oplus \bigoplus_{i=1}^{a+b} \mathbb{Z}$$

and

$$G \oplus K \simeq \bigoplus_{i=1}^{r} \mathbb{Z}_{p_i^{m_i}} \oplus \bigoplus_{i=1}^{t} \mathbb{Z}_{z_i^{k_i}} \oplus \bigoplus_{i=1}^{a+c} \mathbb{Z}$$

Since $G \oplus H \simeq G \oplus K$, we have by the above that

$$\bigoplus_{i=1}^{r} \mathbb{Z}_{p_i^{m_i}} \oplus \bigoplus_{i=1}^{s} \mathbb{Z}_{q_i^{n_i}} \oplus \bigoplus_{i=1}^{a+b} \mathbb{Z} \simeq \bigoplus_{i=1}^{r} \mathbb{Z}_{p_i^{m_i}} \oplus \bigoplus_{i=1}^{t} \mathbb{Z}_{z_i^{k_i}} \oplus \bigoplus_{i=1}^{a+c} \mathbb{Z}$$

Now, we know that the direct sum of two finitely generated abelian groups is a finitely generated abelian group. Hence, since G and H are finitely generated abelian groups, we have that $G \oplus H$ is a finitely generated abelian group. By the uniqueness portion of the Fundamental Theorem of Finitely Generated Abelian Groups, the above gives that the lists $p_1^{m_1}, \ldots, p_r^{m_r}, q_1^{n_1}, \ldots, q_s^{n_s}$ and $p_1^{m_1}, \ldots, p_r^{m_r}, z_1^{k_1}, \ldots, z_t^{k_t}$ are the same up to order and that $a + b = a + c$. In particular, we now have that the lists $q_1^{n_1}, \ldots, q_s^{n_s}$ and $z_1^{k_1}, \ldots, z_t^{k_t}$ are the same up to order and that $b = c$. We may now conclude that

$$H \simeq \bigoplus_{i=1}^{s} \mathbb{Z}_{q_i^{n_i}} \oplus \bigoplus_{i=1}^{b} \mathbb{Z} \simeq \bigoplus_{i=1}^{t} \mathbb{Z}_{z_i^{k_i}} \oplus \bigoplus_{i=1}^{c} \mathbb{Z} \simeq K$$

so that $H \simeq K$. This completes the proof. $\square$

Proof. (c): Let $G = G_1 \oplus \mathbb{Z} \oplus \mathbb{Z}$ and $H = G_1 \oplus \mathbb{Z}$. Since the direct sum of free abelian groups is a free abelian group, we have that G and H are free abelian groups. Furthermore, we have that G is a free abelian group of rank

$$\aleph_0 + 1 + 1 = \aleph_0$$

and that H is a free abelian group of rank

$$\aleph_0 + 1 = \aleph_0$$

In other words, we have that G and H are free abelian groups of the same rank. Hence, we obtain $G \simeq H$ so that

$$G_1 \oplus \mathbb{Z} \oplus \mathbb{Z} = G \simeq H = G_1 \oplus \mathbb{Z}$$

so that $G_1 \oplus \mathbb{Z} \oplus \mathbb{Z} \simeq G_1 \oplus \mathbb{Z}$.

Finally, note that $\mathbb{Z} \oplus \mathbb{Z}$ is clearly a free abelian group of rank 2 and that $\mathbb{Z}$ is clearly a free abelian group of rank 1. We know that two free abelian groups are isomorphic if and only if they have the same rank. Hence, it cannot be the case that $\mathbb{Z} \oplus \mathbb{Z}$ is isomorphic to $\mathbb{Z}$ since $\mathbb{Z} \oplus \mathbb{Z}$ is a free abelian group of rank 2 but $\mathbb{Z}$ is a free abelian group of rank 1. We conclude that $\mathbb{Z} \oplus \mathbb{Z} \not\simeq \mathbb{Z}$. This completes the proof. $\square$

Homework 23: Page 81 #12, 14, 15

Problem 12. (a): *What are the elementary divisors of the group $\mathbb{Z}_2 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_{35}$; what are its invariant factors? Do the same for $\mathbb{Z}_{26} \oplus \mathbb{Z}_{42} \oplus \mathbb{Z}_{49} \oplus \mathbb{Z}_{200} \oplus \mathbb{Z}_{1000}$.*

(b): *Determine up to isomorphism all abelian groups of order 64. Do the same for order 96.*

(c): *Determine all abelian groups of order n for $n \leq 20$.*

Proof. (a): Let $G = \mathbb{Z}_2 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_{35}$. Then

$$G \simeq \mathbb{Z}_2 \oplus \mathbb{Z}_9 \oplus (\mathbb{Z}_5 \oplus \mathbb{Z}_7) = \mathbb{Z}_2 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_7$$

so that the elementary divisors of G are $\{2, 3^2, 5, 7\}$. Furthermore, the invariant factors of G are $\{2 \cdot 3^2 \cdot 5 \cdot 7\} = \{630\}$.

Let $H = \mathbb{Z}_{26} \oplus \mathbb{Z}_{42} \oplus \mathbb{Z}_{49} \oplus \mathbb{Z}_{200} \oplus \mathbb{Z}_{1000}$. Then

$$\begin{aligned} H &\simeq (\mathbb{Z}_2 \oplus \mathbb{Z}_{13}) \oplus (\mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_7) \oplus (\mathbb{Z}_8 \oplus \mathbb{Z}_{25}) \oplus (\mathbb{Z}_8 \oplus \mathbb{Z}_{125}) \\ &\simeq \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_8 \oplus \mathbb{Z}_8 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_{25} \oplus \mathbb{Z}_{125} \oplus \mathbb{Z}_7 \oplus \mathbb{Z}_{49} \oplus \mathbb{Z}_{13} \end{aligned}$$

so that the elementary divisors of H are $\{2, 2, 2^3, 2^3, 3, 5^2, 5^3, 7, 7^2, 13\}$. Furthermore, the invariant factors of H are $\{2, 2, 2^3 \cdot 5^2 \cdot 7, 2^3 \cdot 3 \cdot 5^3 \cdot 7^2 \cdot 13\} = \{2, 2, 1400, 1911000\}$. $\square$

Proof. (b): Let G be an abelian group of order $64 = 2^6$. Then G is isomorphic to one of the following groups:

$$\mathbb{Z}_{64} \quad \mathbb{Z}_{32} \oplus \mathbb{Z}_2 \quad \mathbb{Z}_{16} \oplus \mathbb{Z}_4 \quad \mathbb{Z}_{16} \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \quad \mathbb{Z}_8 \oplus \mathbb{Z}_8 \quad \mathbb{Z}_8 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_2 \quad \mathbb{Z}_8 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$$

$$\mathbb{Z}_4 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_4 \quad \mathbb{Z}_4 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \quad \mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \quad \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$$

Let H be an abelian group of order $96 = 2^5 \cdot 3$. First note that any abelian group of order 2^5 is isomorphic to one of the following groups:

$$\mathbb{Z}_{32} \quad \mathbb{Z}_{16} \oplus \mathbb{Z}_2 \quad \mathbb{Z}_8 \oplus \mathbb{Z}_4 \quad \mathbb{Z}_8 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \quad \mathbb{Z}_4 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_2$$

$$\mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \quad \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$$

Furthermore, any abelian group of order 3 is isomorphic to $\mathbb{Z}_3$. Combining the previous two results, we conclude that H is isomorphic to one of the following groups:

$$\mathbb{Z}_{96} \quad \mathbb{Z}_{16} \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \quad \mathbb{Z}_8 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_3 \quad \mathbb{Z}_8 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \quad \mathbb{Z}_4 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3$$

$$\mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \quad \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3$$

$\square$

Proof. (c): Let G be an abelian group of order n, where $n \leq 20$.

If $n = 1$, then G is the trivial group.

If $n \in \{2, 3, 5, 7, 11, 13, 17, 19\}$, then $G \simeq \mathbb{Z}_n$ since in this case n is prime.

If $n = 4$, then

$$G \simeq \mathbb{Z}_4 \quad \text{or} \quad G \simeq \mathbb{Z}_2 \oplus \mathbb{Z}_2$$

If $n = 6$, then $G \simeq \mathbb{Z}_6$.

If $n = 8$, then

$$G \simeq \mathbb{Z}_8 \quad \text{or} \quad G \simeq \mathbb{Z}_4 \oplus \mathbb{Z}_2 \quad \text{or} \quad G \simeq \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$$

If $n = 9$, then

$$G \simeq \mathbb{Z}_9 \quad \text{or} \quad G \simeq \mathbb{Z}_3 \oplus \mathbb{Z}_3$$

If $n = 10$, then $G \simeq \mathbb{Z}_{10}$.

If $n = 12$, then

$$G \simeq \mathbb{Z}_{12} \quad \text{or} \quad G \simeq \mathbb{Z}_3 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$$

If $n = 14$, then $G \simeq \mathbb{Z}_{14}$.

If $n = 15$, then $G \simeq \mathbb{Z}_{15}$.

If $n = 16$, then

$$G \simeq \mathbb{Z}_{16} \quad \text{or} \quad G \simeq \mathbb{Z}_8 \oplus \mathbb{Z}_2 \quad \text{or} \quad G \simeq \mathbb{Z}_4 \oplus \mathbb{Z}_4$$
$$\text{or} \quad G \simeq \mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \quad \text{or} \quad G \simeq \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$$

If $n = 18$, then

$$G \simeq \mathbb{Z}_{18} \quad \text{or} \quad G \simeq \mathbb{Z}_3 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$$

If $n = 20$, then

$$G \simeq \mathbb{Z}_{20} \quad \text{or} \quad G \simeq \mathbb{Z}_5 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$$

This completes the proof. $\square$

Problem 14. *If H is a subgroup of a finite abelian group G, then G has a subgroup that is isomorphic to G/H.*

Proof. Since G is a *finite* abelian group, by the Fundamental Theorem of Finitely Generated Abelian Groups, we can write

$$G \simeq \mathbb{Z}_{m_1} \oplus \cdots \oplus \mathbb{Z}_{m_r}$$

where $m_1, \ldots, m_r$ is a unique (possibly empty) list of positive integers with $m_1 > 1$ and $m_1 \big| \cdots \big| m_r$. Now, let G^* be the set

$$G^* = \{\phi : G \to \mathbb{C}^\times : \phi \text{ is a group homomorphism}\}$$

and define an operation on G^* by for $\phi_1, \phi_2 \in G^*$ we have $\phi_1\phi_2 : G \to \mathbb{C}^\times$ defined by $(\phi_1\phi_2)(g) = \phi_1(g)\phi_2(g)$ for all $g \in G$.

Note that for $\phi_1, \phi_2 \in G^*$ and $g, h \in G$ we have since ϕ_1 and ϕ_2 are group homomorphisms and since $\mathbb{C}^\times$ is an abelian group that

$$\begin{aligned}(\phi_1\phi_2)(gh) &= \phi_1(gh)\phi_2(gh) \\ &= \phi_1(g)\phi_1(h)\phi_2(g)\phi_2(h) \\ &= [\phi_1(g)\phi_2(g)][\phi_1(h)\phi_2(h)] \\ &= (\phi_1\phi_2)(g)(\phi_1\phi_2)(h)\end{aligned}$$

so that $\phi_1\phi_2 : G \to \mathbb{C}^\times$ is a group homomorphism. In particular, this shows that the operation on G^* defined above is indeed an operation on G^*. Next, since $\mathbb{C}^\times$ is a group, we have that multiplication in $\mathbb{C}^\times$ is associative which implies that the operation on G^* defined above is associative. Note that the trivial group homomorphism $G \to \mathbb{C}^\times$ is an identity of G^*. Finally, let $\phi \in G^*$ and consider the map $\theta : G \to \mathbb{C}^\times$ defined by $\theta(g) = \phi(g)^{-1}$ for all $g \in G$. Since ϕ is a group homomorphism and since $\mathbb{C}^\times$ is an abelian group, it follows that θ is a group homomorphism so that $\theta \in G^*$. Finally, it now follows that θ is the inverse of ϕ. The above results show that G^* is a group.

Now, let R_i denote the group of n_ith roots of unity and let $t_i \in \mathbb{Z}_{n_i}$ be a generator of $\mathbb{Z}_{n_i}$ for $i \in \{1, \ldots, r\}$. Notice that each R_i is the cyclic group of order n_i so that $R_i \simeq \mathbb{Z}_{n_i}$ for each $i \in \{1, \ldots, r\}$. Next, define a map

$$\psi : G^* \to R_1 \times \cdots \times R_r \quad \text{by} \quad \phi \mapsto (\phi(t_1), \ldots, \phi(t_r))$$

It can be shown that ψ is an isomorphism so that $G^* \simeq R_1 \times \cdots \times R_r$. Combining the above results gives

$$G^* \simeq R_1 \times \cdots \times R_r \simeq \mathbb{Z}_{n_1} \oplus \cdots \oplus \mathbb{Z}_{n_r} \simeq G$$

so that $G \simeq G^*$. In particular, since G was an arbitrary finite abelian group, the above proof shows that any finite abelian group K is isomorphic to K^*, where K^* is defined in an analogous fashion to G^* as defined above.

To finish the proof, let H be a subgroup of G. Since G is an abelian group we know that $H \trianglelefteq G$ so that G/H is indeed a group. Now, define $(G/H)^*$ analogously as G^* as defined above and let

$$A = \{\phi \in G^* : H \subseteq \ker \phi\}$$

It can be shown that A is a group and that $(G/H)^* \simeq A$. Furthermore, since G/H is a finite abelian group as G is a finite abelian group, the previous observation gives that $G/H \simeq (G/H)^*$. Combining all of the previous results, we obtain

$$G/H \simeq (G/H)^* \simeq A \subseteq G^* \simeq G$$

In particular, this shows that $G/H \simeq A$ and that A is isomorphic to a subgroup of G. Thus, we have that G/H is isomorphic to a subgroup of G, completing the proof. $\square$

Problem 15. *Every finite subgroup of $\mathbb{Q}/\mathbb{Z}$ is cyclic.*

Proof. Let G be a finite subgroup of $\mathbb{Q}/\mathbb{Z}$. Then for some positive integer n, we can write

$$G = \langle \{q_i + \mathbb{Z} : q_i \in \mathbb{Q}, i \in \{1, \dots, n\}\} \rangle$$

Furthermore, for each $i \in \{1, \dots, n\}$ we can write $q_i = a_i/b_i$ for some $a_i, b_i \in \mathbb{Z}$ such that $b_i \neq 0$.

Now, let $m = b_1 \cdots b_n$ and let $g \in G$. We claim that $g \in \langle 1/m + \mathbb{Z} \rangle$. Towards this end, note that by the above we can write

$$g = (q_1 + \mathbb{Z})^{m_1} + \cdots + (q_n + \mathbb{Z})^{m_n}$$

where $m_1, \dots, m_n \in \mathbb{Z}$. This gives

$$\begin{aligned}
g &= (m_1 q_1 + \mathbb{Z}) + \cdots + (m_n q_n + \mathbb{Z}) \\
&= (m_1 q_1 + \cdots + m_n q_n) + \mathbb{Z} \\
&= \left(m_1 \cdot \frac{a_1}{b_1} + \cdots + m_n \cdot \frac{a_n}{b_n} \right) + \mathbb{Z} \\
&= \left(\frac{m_1 \cdot a_1 \cdot b_2 \cdots b_n}{b_1 \cdots b_n} + \cdots + \frac{m_n \cdot a_n \cdot b_1 \cdots b_{n-1}}{b_1 \cdots b_n} \right) + \mathbb{Z} \\
&= \left(\frac{m_1 \cdot a_1 \cdot b_2 \cdots b_n + \cdots + m_n \cdot a_n \cdot b_1 \cdots b_{n-1}}{b_1 \cdots b_n} \right) + \mathbb{Z} \\
&= \left(\frac{m_1 \cdot a_1 \cdot b_2 \cdots b_n + \cdots + m_n \cdot a_n \cdot b_1 \cdots b_{n-1}}{m} \right) + \mathbb{Z} \\
&= \left[(m_1 \cdot a_1 \cdot b_2 \cdots b_n + \cdots + m_n \cdot a_n \cdot b_1 \cdots b_{n-1}) \cdot \frac{1}{m} \right] + \mathbb{Z} \\
&= (1/m + \mathbb{Z})^{m_1 \cdot a_1 \cdot b_2 \cdots b_n + \cdots + m_n \cdot a_n \cdot b_1 \cdots b_{n-1}} \\
&\in \langle 1/m + \mathbb{Z} \rangle
\end{aligned}$$

Since $g \in G$ was arbitrary, this shows that $G \subseteq \langle 1/m + \mathbb{Z} \rangle$. Finally, note that $\langle 1/m + \mathbb{Z} \rangle$ is a cyclic group. Since subgroups of cyclic groups are cyclic, we may now conclude that G is cyclic since G is a subgroup of $\langle 1/m + \mathbb{Z} \rangle$. This completes the proof. $\square$

Homework 24: Page 87 #2, 3, 4

Problem 2. *S_n is indecomposable for all $n \geq 2$.*

Proof. Consider if $n = 2$. Since $|S_2| = 2$, it follows that there is no nontrivial, proper subgroup of S_2. Hence, S_2 is indecomposable.

Consider if $n = 3$. For the sake of contradiction, suppose that $S_3 = H \times K$, where H and K are nontrivial, proper subgroups of S_3. Note that the only normal subgroups of S_3 are $\{1\}, A_3$, and S_3. Since H and K are necessarily normal in S_3 and since H and K are nontrivial, proper subgroups of S_3, it follows that $H = A_3 = K$. But then

$$6 = |S_3| = |H \times K| = |H| \cdot |K| = |A_3| \cdot |A_3| = 3 \cdot 3 = 9$$

which is obviously a contradiction. Hence, S_3 is indecomposable.

Consider if $n = 4$. For the sake of contradiction, suppose that $S_4 = H \times K$, where H and K are nontrivial, proper subgroups of S_4. We know that

$$V = \{(1), (1 \quad 2)(3 \quad 4), (1 \quad 3)(2 \quad 4), (1 \quad 4)(2 \quad 3)\}$$

is a normal subgroup of S_4 of order 4. Furthermore, note that the only normal subgroups of S_4 are $\{1\}, V, A_4$, and S_4. Since H and K are necessarily normal in S_4 and since H and K are nontrivial, proper subgroups of S_4, it follows that $H, K \in \{V, A_4\}$. However, any choice of H and K give a contradiction similar to the one presented above. Hence, S_4 is indecomposable.

Consider if $n \geq 5$. For the sake of contradiction, suppose that $S_n = H \times K$, where H and K are nontrivial, proper subgroups of S_n. Now, since $n \geq 5$, we know that $Z(S_n)$ is trivial. Since A_n is normal in S_n and since $S_n = H \times K$, it must be the case that either $A_n \subseteq Z(S_n)$ or A_n has a nontrivial intersection with either H or K. Since $n \geq 5$, we have that A_n is nontrivial. Hence, as $Z(S_n)$ is trivial, it cannot be the case that $A_n \subseteq Z(S_n)$. Therefore, without loss of generality, we may assume that A_n has a nontrivial intersection with H.

Now, since H is necessarily normal in S_n it follows that $H \cap A_n \trianglelefteq A_n$. But since $n \geq 5$ we have that A_n is simple. Therefore, we have $H \cap A_n \in \{\{1\}, A_n\}$. But since $H \cap A_n \neq \{1\}$, we have $H \cap A_n = A_n$ so that $A_n \subseteq H$. Since H is a subgroup of S_n, this implies that $H \in \{A_n, S_n\}$. However, we know that H is proper in S_n so that $H = A_n$. Hence, we have

$$n! = |S_n| = |H \times K| = |H| \cdot |K| = |A_n| \cdot |K| = \frac{n!}{2} \cdot |K|$$

so that $|K| = 2$. Furthermore, since necessarily $H \cap K = \{1\}$ and since $H = A_n$, it follows that $K = \{(1), \sigma\}$, where $\sigma \notin A_n$.

Finally, since $\sigma \neq (1)$, there are $a, b \in \{1, \ldots, n\}$ such that $\sigma(a) = b \neq a$. Since $n \geq 5$, there is some $c \in \{1, \ldots, n\}$ such that $c \notin \{a, b\}$. Hence, we have

$$[(b \quad c)\sigma(b \quad c)^{-1}](a) = c \notin \{a, b\} = \{(1)(a), \sigma(a)\}$$

so that $(b \quad c)\sigma(b \quad c)^{-1} \notin \{(1), \sigma\} = K$. However, this is a contradiction as $\sigma \in K$ and necessarily $K \trianglelefteq G$. Hence, S_n is indecomposable for all $n \geq 5$.

In conclusion, we have shown that S_n is indecomposable for all $n \geq 2$. This completes the proof. $\square$

Problem 3. *The additive group $\mathbb{Q}$ is indecomposable.*

Proof. Let H and K be any nontrivial, proper subgroups of $\mathbb{Q}$. Since H and K are nontrivial, there exist nonidentity elements $a \in H$ and $b \in K$. Note that since a and b are nonidentity elements of $\mathbb{Q}$ that we can write

$$a = \frac{a_1}{a_2} \quad \text{and} \quad b = \frac{b_1}{b_2}$$

for some nonzero integers a_1, a_2, b_1, b_2. Since H is a group and $a \in H$, we have

$$a_1 b_1 = b_1 a_2 \cdot \frac{a_1}{a_2} = b_1 a_2 \cdot a \in H$$

Similarly, since K is a group and $b \in K$, we have

$$a_1 b_1 = a_1 b_2 \cdot \frac{b_1}{b_2} = a_1 b_2 \cdot b \in K$$

Hence, we have $a_1 b_1 \in H \cap K$. Furthermore, since a_1 and b_1 are nonzero integers, it follows that $a_1 b_1$ is a nonzero integer. Therefore, we have that $H \cap K \neq \{0\}$.

The above result shows that any two nontrivial, proper subgroups of $\mathbb{Q}$ intersect nontrivially so that $\mathbb{Q}$ is not a direct product of any two of its proper subgroups. This proves that the additive group $\mathbb{Q}$ is indecomposable. $\square$

Problem 4. *A nontrivial homomorphic image of an indecomposable group need not be indecomposable.*

Proof. Consider $Q_8 = \{1, -1, i, -i, j, -j, k, -k\}$. First, note that the proper, nontrivial subgroups of Q_8 are $\langle -1 \rangle, \langle i \rangle, \langle j \rangle$, and $\langle k \rangle$. Furthermore, since each of these subgroups is cyclic, it follows that each of these subgroups is abelian. Now, for the sake of contradiction, suppose that Q_8 were not indecomposable. Then $Q_8 = H \times K$, where H and K are nontrivial, proper subgroups of Q_8. Since the direct product of abelian groups is abelian, it follows by the above that Q_8 is abelian. However, we have

$$ij = k \neq -k = ji$$

which shows that Q_8 is nonabelian. This contradiction permits us to conclude that Q_8 is indecomposable.

Next, note that $\langle -1 \rangle = Z(Q_8) \trianglelefteq Q_8$. Hence, we have that $Q_8/\langle -1 \rangle$ is a group. Now, consider the canonical projection homomorphism $\pi : Q_8 \to Q_8/\langle -1 \rangle$. Since π is surjective and since $|Q_8/\langle -1 \rangle| = 8/2 = 4 > 1$, we have that $Q_8/\langle -1 \rangle$ is a nontrivial homomorphic image of the indecomposable group Q_8.

However, we see that since $|Q_8/\langle -1 \rangle| = 4$ and since every nonidentity element of $Q_8/\langle -1 \rangle$ is of order 2 that $Q_8/\langle -1 \rangle \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$. In particular, this shows that the group $Q_8/\langle -1 \rangle$ is not indecomposable. This completes the proof that the nontrivial homomorphic image of an indecomposable group need not be indecomposable. $\square$

Homework 25: Page 87 #6, 7, 8

Problem 6. *Let H, K be normal subgroups of a group G such that $G = H \times K$.*

(a): *If N is a normal subgroup of H, then N is normal in G.*

(b): *If G satisfies the ACC or DCC on normal subgroups, then so do H and K.*

Proof. (a): We first show that for all $h \in H$ and $k \in K$ we have that $hk = kh$. Indeed, since $H \trianglelefteq G$ and $K \trianglelefteq G$, we have

$$k^{-1}h^{-1}kh \in H \cap K$$

However, since $G = H \times K$, we have that $H \cap K = 1$ so that $k^{-1}h^{-1}kh = 1$ which gives $hk = kh$, as desired.

Now, we prove the main result. Towards this end, let $g \in G$ and $n \in N$. Since $G = H \times K$, there exist elements $h \in H$ and $k \in K$ such that $g = hk$. Hence, since $N \trianglelefteq H$, we obtain

$$g^{-1}ng = (hk)^{-1}n(hk) = k^{-1}h^{-1}nhk = k^{-1}n'k$$

for some $n' \in N$. In particular, since $n' \in N \subseteq H$, we have by our preliminary result that $n'k = kn'$. Hence, by the above equality, this gives

$$g^{-1}ng = k^{-1}n'k = k^{-1}kn' = n' \in N$$

Since $g \in G$ and $n \in N$ were arbitrary, this shows that $N \trianglelefteq G$, completing the proof. $\square$

Proof. (b): First, suppose that G satisfies the ACC on normal subgroups. We will show that H satisfies the ACC on normal subgroups. For the sake of contradiction, suppose that H did not satisfy the ACC on normal subgroups. Then there exists an increasing sequence of normal subgroups

$$H_1 \subseteq H_2 \subseteq \cdots \subseteq H_n \subseteq \cdots$$

of H such that for any positive integer n_0 there exists some positive integer $n > n_0$ with $H_n \neq H_{n_0}$. Note that by Part (a), we have that the above sequence of normal subgroups of H is a sequence of normal subgroups of G. Since G satisfies the ACC on normal subgroups, it follows that there exists a positive integer n_0 such that $H_n = H_{n_0}$ for all positive integers $n \geq n_0$. However, this contradicts the above. We conclude that H satisfies the ACC on normal subgroups. In exactly the same fashion, we see that H also satisfies the DCC on normal subgroups.

Since the result of Part (a) also applies to the subgroup K of G, the same argument as presented above shows that K satisfies the ACC and DCC on normal subgroups. This completes the proof. $\square$

Problem 7. *If f and g are endomorphisms of a group G, then $f+g$ need not be an endomorphism.*

Proof. Consider $G = S_3$. Let $a = (1 \quad 2 \quad 3) \in S_3$ and $b = (1 \quad 3 \quad 2) \in G$ and define

$$f : G \to G \quad \text{by} \quad x \mapsto axa^{-1}$$

and

$$g : G \to G \quad \text{by} \quad x \mapsto bxb^{-1}$$

Let $x, y \in G$. Then

$$f(xy) = axya^{-1} = (axa^{-1})(aya^{-1}) = f(x)f(y)$$

so that f is an endomorphism of G. In exactly the same fashion, we obtain that g is an endomorphism of G.

Now, let $x = (1 \quad 2) \in G$ and $y = (1 \quad 3) \in G$. Note that

$$xy = (1 \quad 2)(1 \quad 3) = (1 \quad 3 \quad 2) = b$$

Hence, we obtain

$$(f+g)(xy) = (f+g)(b) = f(b)g(b) = (aba^{-1})(bbb^{-1}) = aba^{-1}b$$

Notice that

$$aba^{-1}b = (1 \quad 2 \quad 3)(1 \quad 3 \quad 2)(1 \quad 2 \quad 3)^{-1}(1 \quad 3 \quad 2) = (1 \quad 2 \quad 3) = a$$

so that by the above we have $(f+g)(xy) = a$. Furthermore, we have

$$(f+g)(x)(f+g)(y) = f(x)g(x)f(y)g(y) = (axa^{-1})(bxb^{-1})(aya^{-1})(byb^{-1})$$

In the same way as above, we obtain

$$axa^{-1} = (2 \quad 3) \quad bxb^{-1} = (1 \quad 3) \quad aya^{-1} = (1 \quad 2) \quad byb^{-1} = (2 \quad 3)$$

so that

$$(f+g)(x)(f+g)(y) = (2 \quad 3)(1 \quad 3)(1 \quad 2)(2 \quad 3) = (1 \quad 3 \quad 2) = b$$

Finally, we clearly have that $a \neq b$. By the above, we now have

$$(f+g)(xy) = a \neq b = (f+g)(x)(f+g)(y)$$

In particular, this proves that $f+g$ is not an endomorphism of G despite the fact that f and g are endomorphisms of G. This completes the proof. $\square$

Problem 8. *Let f and g be normal endomorphisms of a group G.*

(a): *fg is a normal endomorphism.*

(b): *$H \trianglelefteq G$ implies $f(H) \trianglelefteq G$.*

(c): *If $f+g$ is an endomorphism, then it is normal.*

Proof. (a): Let $h, k \in G$. Since f and g are normal endomorphisms of G, we have

$$(fg)(hkh^{-1}) = f(g(hkh^{-1})) = f(hg(k)h^{-1}) = hf(g(k))h^{-1} = h(fg)(k)h^{-1}$$

This shows that fg is a normal endomorphism of G. □

Proof. (b): Let $g \in G$ and $n \in f(H)$. Then there is some $h \in H$ with $n = f(h)$. Note that since $H \trianglelefteq G$ we have $ghg^{-1} \in H$. Therefore, since f is a normal endomorphism of G, we now have

$$gng^{-1} = gf(h)g^{-1} = f(ghg^{-1}) \in f(H)$$

This shows that $f(H) \trianglelefteq G$. □

Proof. (c): Let $h, k \in G$. Since f and g are normal endomorphisms of G, we have

$$\begin{aligned}(f+g)(hkh^{-1}) &= f(hkh^{-1})g(hkh^{-1}) \\ &= [hf(k)h^{-1}][hg(k)h^{-1}] \\ &= hf(k)g(k)h^{-1} \\ &= h(f+g)(k)h^{-1}\end{aligned}$$

Since $f+g$ is an endomorphism of G, this shows that $f+g$ is a normal endomorphism of G, completing the proof. □

Section II: Spring Semester 2017

Topic 1: Localization; Local Rings

Definition. Let R be a commutative ring, possibly without identity. A ***multiplicative set*** in R is a nonempty subset S of R such that for all $s_1, s_2 \in S$ we have $s_1 s_2 \in S$.

Example. The set of all nonzero elements of an integral domain

Proof. This follows from the fact that the product of two nonzero elements of an integral domain is again a nonzero element since integral domains have no zero divisors. □

Example. The set of units in a commutative ring with 1.

Proof. This follows from the fact that the product of two units in a commutative ring with 1 is again a unit. □

Example. The set of elements of a commutative ring with 1 that are not zero divisors.

Proof. Let S be this set and let $a, b \in S$. If $a = 0$ or $b = 0$, then $ab = 0 \in S$. Therefore, assume that a and b are nonzero. Since a and b are nonzero and since a and b are not zero divisors, we have that ab is nonzero. Now, suppose that $abc = 0$ for some $c \in R$. Then $a(bc) = 0$ and since a is not a zero divisor and $a \neq 0$, this equality implies that $bc = 0$. Since b is not a zero divisor and $b \neq 0$, this equality implies that $c = 0$. We conclude that ab is not a zero divisor so that $ab \in S$. □

Example. Any ideal of R.

Proof. This follows from the fact that any ideal of R is closed under multiplication. □

Example. If P is a prime ideal of R, then $R - P$ is a multiplicative set.

Proof. Let $a, b \in R - P$. Since P is a prime ideal and $a, b \notin P$, we have that $ab \notin P$ so that $ab \in R - P$. □

Example. The set of positive powers of an element $r \in R$.

Proof. This follows from the fact that the product of any two positive powers of an $r \in R$ is again a positive power of the element $r \in R$. □

Theorem. Let S be a multiplicative set in a commutative ring R. The relation $\sim$ on $R \times S$ by $(r, s) \sim (r', s')$ if and only if there is some $s'' \in S$ such that $s''(rs' - r's) = 0$ is an equivalence relation on $R \times S$. If R has no zero divisors and $0 \notin S$, then $(r, s) \sim (r', s')$ if and only if $rs' - r's = 0$.

Proof. That $\sim$ is a reflexive and symmetric relation is easily verified. Now, suppose that $(r, s) \sim (r', s')$ and $(r', s') \sim (r'', s'')$. Then there are $s_1, s_2 \in S$ such that

$$s_1(rs' - r's) = 0 \quad \text{and} \quad s_2(r's'' - r''s') = 0$$

so that

$$s_1rs' = s_1r's \quad \text{and} \quad s_2r's'' = s_2r''s'$$

Note that $s_1s_2s' \in S$ and

$$s_1s_2s'(rs'' - r''s) = (s_1rs')s_2s'' - (s_2r''s')s_1s = (s_1r's)s_2s'' - (s_2r's'')s_1s = 0$$

Thus, we have $(r, s) \sim (r'', s'')$ so that $\sim$ is transitive. The above results show that $\sim$ is an equivalence relation on $R \times S$.

Finally, suppose that R has no zero divisors and $0 \notin S$. Then $(r, s) \sim (r', s')$ if and only if there is some $s'' \in S$ such that $s''(rs' - r's) = 0$ if and only if $rs' - rs = 0$ since $s'' \neq 0$ as $0 \notin S$ and since R has no zero divisors. □

Notation. Denote the equivalence class of (r, s) by r/s.

Remark. $r/s \sim r's'$ if and only if there is some $s'' \in S$ such that $s''(rs' - r's) = 0$.

Proof. This is immediate by the definition of the relation $\sim$, completing the proof. □

Remark. For all $r \in R$ and $s, t \in S$, we have $r/s = tr/ts$.

Proof. Let $s' \in S$ be any element of S and note that

$$0 = s' \cdot 0 = s'(rts - rts) = s'(rts - trs)$$

so that $r/s = tr/ts$. □

Notation. Let $S^{-1}R$ denote the set of equivalence classes.

Definition. The set $S^{-1}R$ is called the ***localization*** of R with respect to S.

Theorem. Let R be a commutative ring and let S be a multiplicative set in R. Then
(a): $S^{-1}R$ is a commutative ring with 1 with addition

$$\frac{r}{s} + \frac{r'}{s'} = \frac{rs' + r's}{ss'}$$

and multiplication

$$\frac{r}{s} \cdot \frac{r'}{s'} = \frac{rr'}{ss'}$$

for all $r/s, r'/s' \in S^{-1}R$.
(b): If R is a nonzero ring with no zero divisors and $0 \notin S$, then $S^{-1}R$ is an integral domain.
(c): If R is a nonzero ring with no zero divisors and $S = R - \{0\}$, then $S^{-1}R$ is a field.

Proof. (a): We first establish that addition and multiplication as defined above are well-defined in $S^{-1}R$. Towards this end, let $r/s, r'/s' \in S^{-1}R$ and suppose that $r/s = r_1/s_1$ and $r'/s' = r_2/s_2$. We must show that $r/s + r'/s' = r_1/s_1 + r_2/s_2$ and $rr'/ss' = r_1r_2/s_1s_2$. That is, we must show that

$$\frac{rs' + r's}{ss'} = \frac{r_1s_2 + r_2s_1}{s_1s_2} \quad \text{and} \quad \frac{rr'}{ss'} = \frac{r_1r_2}{s_1s_2}$$

Since $r/s = r_1/s_1$ and $r'/s' = r_2/s_2$ there exist $z_1, z_2 \in S$ such that

$$z_1(rs_1 - r_1s) = 0 \quad \text{and} \quad z_2(r's_2 - r_2s') = 0$$

so that

$$z_1rs_1 = z_1r_1s \quad \text{and} \quad z_2r's_2 = z_2r_2s'$$

Note that $z_1z_2 \in S$ and

$$z_1z_2[(rs' + r's)s_1s_2] = (z_1rs_1)z_2s's_2 + (z_2r's_2)z_1ss_1 = (z_1r_1s)z_2s's_2 + (z_2r_2s')z_1ss_1$$

and

$$z_1z_2[(r_1s_2 + r_2s_1)ss'] = (z_1r_1s)z_2s's_2 + (z_2r_2s')z_1ss_1 = z_1z_2[(rs' + r's)s_1s_2]$$

so that

$$z_1z_2[(rs' + r's)s_1s_2 - (r_1s_2 + r_2s_1)ss'] = 0$$

which proves that addition as defined above is well-defined in $S^{-1}R$. Next, we have

$$z_1z_2(rr's_1s_2 - r_1r_2ss') = (z_1rs_1)z_2r's_2 - (z_2r_2s')z_1r_1s = (z_1r_1s)z_2r's_2 - (z_2r's_2)z_1r_1s = 0$$

which proves that multiplication as defined above is well-defined in $S^{-1}R$.

Finally, that $S^{-1}R$ is a commutative ring follows from the fact that R is a commutative ring. Now, let $r/s \in S^{-1}R$. Note that $s/s \in S^{-1}R$ and

$$\frac{r}{s} \cdot \frac{s}{s} = \frac{rs}{ss} = \frac{r}{s}$$

which shows that $S^{-1}R$ has identity, completing the proof. □

Proof. (b): By Part (a), we know that $S^{-1}R$ is a commutative ring with additive identity $0/z$ and multiplicative identity z/z for any $z \in S$. For the sake of contradiction, suppose that $z/z = 0/z$. Then there is some $s \in S$ such that

$$s(zz - 0) = 0$$

so that $sz^2 = 0$. However, since $sz^2 \in S$, we now have that $0 \in S$ which contradicts the fact that $0 \notin S$. Hence, the additive identity of $S^{-1}R$ does not equal the multiplicative identity of $S^{-1}R$.

Lastly, we show $S^{-1}R$ has no zero divisors. Towards this end, let $r/s, r'/s' \in S^{-1}R$ and suppose that

$$\frac{0}{s} = \frac{r}{s} \cdot \frac{r'}{s'} = \frac{rr'}{ss'}$$

Then there is some $s'' \in S$ such that

$$s''(0 - rr's) = 0$$

so that $rr'ss'' = 0$. Since R has no zero divisors, this equality implies that either $rr' = 0$ or $ss'' = 0$. But since $ss'' \in S$ and $0 \notin S$, we have $ss'' \neq 0$ so that $rr' = 0$. Since R has no zero divisors, this equality implies that either $r = 0$ or $r' = 0$ so that either r/s or r'/s' is the zero element of $S^{-1}R$. This proves that $S^{-1}R$ has no zero divisors and hence $S^{-1}R$ is an integral domain. □

Proof. (c): Since $0 \notin S$, we have by Part (b) that $S^{-1}R$ is an integral domain. Therefore, it remains to prove that each nonzero element of $S^{-1}R$ has a multiplicative inverse in $S^{-1}R$. Towards this end, let $r/s \in S^{-1}R$ be a nonzero element of $S^{-1}R$ so that $r \neq 0$. Thus, we have $r \in R - \{0\} = S$ which implies that $s/r \in S^{-1}R$. Finally, note that

$$\frac{r}{s} \cdot \frac{s}{r} = \frac{rs}{sr} = \frac{rs}{rs}$$

That is, the element $s/r \in S^{-1}R$ is the multiplicative inverse of $r/s \in S^{-1}R$. □

Theorem. Let S be a multiplicative set in a commutative ring R. Then

(a): The map $\phi_S : R \to S^{-1}R$ by $\phi_S(r) = rs/s$ for any $s \in S$ is a well-defined ring homomorphism and for any $s \in S$, we have that $\phi_S(s)$ is a unit of $S^{-1}R$.

(b): If $0 \notin S$ and S has no zero divisors, then ϕ_S is injective.

(c): If R has identity and S consists of units, then ϕ_S is an isomorphism.

Proof. (a): Let $r \in R$ and note that $rs/s = rz/z$ for any $s, z \in S$. Thus, we see that ϕ_S is a well-defined map. Next, that ϕ_S is a ring homomorphism is easily verified. Finally, let $s \in S$ and note that

$$\phi_S(s) = \frac{ss}{s} = \frac{s^2}{s}$$

Now, note that $s^2 \in S$ so that $s/s^2 \in S^{-1}R$. Furthermore, note that

$$\frac{s^2}{s} \cdot \frac{s}{s^2} = \frac{s^3}{s^3}$$

That is, the element $s/s^2 \in S^{-1}R$ is the multiplicative inverse of $s^2/s = \phi_S(s)$ so that $\phi_S(s)$ is a unit of $S^{-1}R$. □

Proof. (b): Since ϕ_S is a ring homomorphism, it suffices to show that the kernel of ϕ_S is trivial to establish that ϕ_S is injective. Towards this end, suppose that $r \in \ker \phi_S$ and let $s \in S$ be any element of S. Then

$$\frac{0}{s} = \phi_S(r) = \frac{rs}{s}$$

Hence, there is some $s' \in S$ such that

$$s'(0 - rss) = 0$$

so that $rs^2s' = 0$. Now, note that $s^2s' \in S$ and since $0 \notin S$ we have $s^2s' \neq 0$. Since S has no zero divisors, the equality $rs^2s' = 0$ forces $r = 0$. Thus, we see $\ker \phi_S$ is trivial and hence ϕ_S is an injection. □

Proof. (c): Since S consists of units, we have in particular that $0 \notin S$ and that S has no zero divisors. Therefore, by Part (a) and Part (b) of this Theorem, it follows that ϕ_S is an injective ring homomorphism and so it remains to prove that ϕ_S is a surjection. Towards this end, let $r/s \in S^{-1}R$. Since $s \in S$ and S consists of units, we have that s^{-1} exists in R. Thus, we have $rs^{-1} \in R$ and

$$\phi_S(rs^{-1}) = \frac{rs^{-1} \cdot s}{s} = \frac{r}{s}$$

so that ϕ_S is surjective. This completes the proof. $\square$

Theorem. Let R be a commutative ring and S be a multiplicative set in R. Then given any pair (T, ψ), where T is a commutative ring with identity and $\psi : R \to T$ is a ring homomorphism such that $\psi(S)$ consists of units of T, then there is a unique ring homomorphism $\theta : S^{-1}R \to T$ such that $\theta \circ \phi_S = \psi$, where $\phi_S : R \to S^{-1}R$ is defined as in the previous lecture.

Proof. Define $\theta : S^{-1}R \to T$ by $\theta(r/s) = \psi(r)\psi(s)^{-1}$ for all $r/s \in S^{-1}R$. To see that θ is well-defined, suppose that $r/s, r'/s' \in S^{-1}R$ and $r/s = r'/s'$. By definition, there exists some $s'' \in S$ such that $s''(rs' - r's) = 0$ so that $s''rs' = s''r's$. Applying ψ to both sides of the previous equality, we have since ψ is a ring homomorphism that

$$\psi(s'')\psi(r)\psi(s') = \psi(s''rs') = \psi(s''r's) = \psi(s'')\psi(r')\psi(s)$$

Since $s, s', s'' \in S$, we have that $\psi(s), \psi(s'), \psi(s'') \in T$ are units of T. Thus, left-multiplying the above equality by $\psi(s'')^{-1}$ gives that $\psi(r)\psi(s') = \psi(r')\psi(s)$. Hence, we now obtain

$$\theta(r/s) = \psi(r)\psi(s)^{-1} = \psi(r')\psi(s')^{-1} = \theta(r'/s')$$

which proves that θ is well-defined. Furthermore, since ψ is a ring homomorphism, it easily follows by the definition of θ that θ is a ring homomorphism.

Now, let $r \in R$ and fix $s \in S$. Then since ψ is a ring homomorphism we obtain

$$(\theta \circ \phi_S)(r) = \theta(\phi_S(r)) = \theta(rs/s) = \psi(rs)\psi(s)^{-1} = \psi(r)\psi(s)\psi(s)^{-1} = \psi(r)$$

Since $r \in R$ was arbitrary, the above equality proves that $\theta \circ \phi_S = \psi$.

Finally, suppose that $g : S^{-1}R \to T$ is a ring homomorphism with $g \circ \phi_S = \psi$. Let $r/s \in S^{-1}R$ and note that

$$\frac{r}{s} = \frac{r}{s} \cdot \frac{s^2}{s^2} = \frac{rs}{s} \cdot \frac{s}{s^2} = \phi_S(r) \cdot \phi_S(s)^{-1}$$

Thus, since g and ϕ_S are ring homomorphisms and since $g \circ \phi_S = \psi$, we have

$$\begin{aligned} g(r/s) &= g\left(\phi_S(r)\phi_S(s)^{-1}\right) \\ &= g\left(\phi_S(r)\phi_S\left(s^{-1}\right)\right) \\ &= g(\phi_S(r))g\left(\phi_S(s^{-1})\right) \\ &= g(\phi_S(r))g(\phi_S(s))^{-1} \\ &= \psi(r)\psi(s)^{-1} \\ &= \theta(r/s) \end{aligned}$$

Since $r/s \in S^{-1}R$ was arbitrary, the above equality proves that $g = \theta$. This establishes the uniqueness of θ as stated in this Theorem. □

Note. For the remainder of this lecture, we assume that R is a commutative ring with identity and that S is a multiplicative set in R.

Definition. If I is an ideal of R, then the set

$$S^{-1}I = \{i/s : i \in I, s \in S\}$$

is called the ***extension*** of I in $S^{-1}R$.

Remark. $S^{-1}I$ is an ideal of $S^{-1}I$ containing $\phi_S(I)$.

Proof. First, note that $S^{-1}I \neq \emptyset$ since $I \neq \emptyset$ and $S \neq \emptyset$. Now, let $i/s, i'/s' \in S^{-1}I$ and note that

$$\frac{i}{s} - \frac{i'}{s'} = \frac{is' - i's}{ss'} \in S^{-1}I$$

since $is - i's \in I$ as I is an ideal of R and since $ss' \in S$. Thus, we see $S^{-1}I$ is a subgroup of $S^{-1}R$ under addition. Next, let $r/s \in S^{-1}R$ and $i/z \in S^{-1}I$. Then

$$\frac{r}{s} \cdot \frac{i}{z} = \frac{ri}{sz} \in S^{-1}I$$

since $ri \in I$ as I is an ideal of R and since $sz \in R$. The above results show that $S^{-1}I$ is an ideal of $S^{-1}R$. Finally, let $r/s \in \phi_S(I)$. Then there is some $i \in I$ such that

$$\frac{r}{s} = \phi_S(i) = \frac{is}{s} \in S^{-1}I$$

since $is \in I$ as I is an ideal of R. This shows that $S^{-1}I$ contains $\phi_S(I)$. □

Proposition. (a): For an ideal I of R, we have $S^{-1}I = S^{-1}R$ if and only if $S \cap I \neq \emptyset$.

(b): Every ideal J of $S^{-1}R$ is of the form $S^{-1}I$, where $I = \phi_S^{-1}(J)$.

(c): If P is a prime ideal of R and $S \cap P = \emptyset$, then $S^{-1}P$ is a prime ideal of $S^{-1}R$ and $\phi_S^{-1}(S^{-1}P) = P$.

Proof. (a): For the first direction, assume that $S^{-1}I = S^{-1}R$. Then there is some $i \in I$ and some $s \in S$ such that $i/s = s/s$. Hence, there is some $s' \in S$ such that $s'(is - s^2) = 0$ so that $iss' = s^2s'$. Note that since I is an ideal that the left-hand side of this equality

is in I and that the right-hand side of this equality is clearly in S. Therefore, we have $iss' \in S \cap I$ so that $S \cap I \neq \emptyset$.

For the second direction, assume that $S \cap I \neq \emptyset$. Let $i \in S \cap I$. Then $i/i \in S^{-1}I$ so that $S^{-1}I$ is an ideal of $S^{-1}R$ containing the multiplicative identity of $S^{-1}R$. Therefore, we have $S^{-1}I = S^{-1}R$. □

Proof. (b): Let J be an ideal of $S^{-1}R$ and let $I = \phi_S^{-1}(J)$. We show that $J = S^{-1}I$. First, let $r/s \in J$. Then since J is an ideal of $S^{-1}R$ and $s^2/s \in S^{-1}R$, we have

$$\phi_S(r) = \frac{rs}{s} = \frac{s^2}{s} \cdot \frac{r}{s} \in J$$

so that $r \in \phi_S^{-1}(J) = I$. In particular, this shows that $r/s \in S^{-1}I$. On the other hand, let $r/s \in S^{-1}I$. Then we have $r \in I = \phi_S^{-1}(J)$ so that

$$\frac{rs}{s} = \phi_S(r) \in J$$

Hence, since J is an ideal and since $1/s \in S^{-1}R$ as R has identity, this gives

$$\frac{r}{s} = \frac{s}{s} \cdot \frac{r}{s} = \frac{1}{s} \cdot \frac{rs}{s} \in J$$

so that $r/s \in J$. The above results complete the proof. □

Proof. (c): We know that $S^{-1}P$ is an ideal of $S^{-1}R$ since P is an ideal of R. Now, since $S \cap P = \emptyset$ we have by Part (a) of this proposition that $S^{-1}P \neq S^{-1}R$. Next, suppose that $r/s, r'/s' \in S^{-1}R$ and

$$\frac{rr'}{ss'} = \frac{r}{s} \cdot \frac{r'}{s'} \in S^{-1}P$$

Then there is some $i/z \in S^{-1}P$ such that $rr'/ss' = i/z$. Thus, there is some $s'' \in S$ such that $s''(rr'z - iss') = 0$ so that $rr'zs'' = iss's'' \in P$ since $i \in P$ and P is an ideal. Now, since P is a prime ideal, the above gives that either $rr' \in P$ or $zs'' \in P$. However, we know that $zs'' \in S$ and since $S \cap P = \emptyset$, we cannot have $zs'' \in P$. Hence, we must have $rr' \in P$. Again since P is a prime ideal, this forces either $r \in P$ or $r' \in P$. That is, we have either $r/s \in S^{-1}P$ or $r'/s' \in S^{-1}P$ so that $S^{-1}P$ is a prime ideal of $S^{-1}R$.

Finally, we show that $\phi_S^{-1}(S^{-1}P) = P$. Towards this end, let $a \in \phi_S^{-1}(S^{-1}P)$ and fix any $s \in S$. Then we have

$$\frac{as}{s} = \phi_S(a) \in S^{-1}P$$

Thus, there is some $i/z \in S^{-1}P$ such that $as/s = i/z$. Therefore, there is some $s' \in S$ such that $s'(asz - is) = 0$ so that $aszs' = iss' \in P$ since $i \in P$ and P is an ideal. Since P is a prime ideal, the fact that $aszs' \in P$ implies that $a \in P$ or $szs' \in P$. However, we know that $szs' \in S$ and since $S \cap P = \emptyset$, we have $szs' \notin P$ so that $a \in P$.

On the other hand, let $a \in P$ and again fix any $s \in S$. Then $as \in P$ as P is an ideal and thus

$$\phi_S(a) = \frac{as}{s} \in S^{-1}P$$

so that $a \in \phi_S^{-1}(S^{-1}P)$. The above results show that $\phi_S^{-1}(S^{-1}P) = P$. □

Definition. Let R be a commutative ring with 1 and let P be a prime ideal of R. Then the ***localization*** of R at P, denoted R_P, is $(R-P)^{-1}R$. If I is an ideal of R, then $I_P = (R-P)^{-1}I$ is called the ideal I ***localized*** at P.

Theorem. Let R be a commutative ring with 1 and P a prime ideal of R. Then

(a): There is a one-to-one correspondence between the set of all prime ideals of R contained in P and the set of all prime ideals of R_P.

(b): The ideal P_P of R_P is the unique maximal ideal of R_P.

Proof. (a): Let $S = R - P$. First, suppose that Q is a prime ideal of R with $Q \subseteq P$. Since $Q \subseteq P$, we have that $Q \cap S = \emptyset$. Since Q is a prime ideal of R, by Proposition 1 from the previous lecture we have that Q_P is a prime ideal of R_P and $Q = \phi_S^{-1}(Q_P)$.

On the other hand, suppose that Q is a prime ideal of R_P. Since the inverse homomorphic image of a prime ideal is a prime ideal, we see that $\phi_S^{-1}(Q)$ is a prime ideal of R. Furthermore, since Q is an ideal of R_P we know by Proposition 1 from the previous lecture that $Q = S^{-1}\phi_S^{-1}(Q)$. Thus, since Q is a prime ideal of R_P, we now have in particular that

$$S^{-1}\phi_S^{-1}(Q) = Q \neq R_P = S^{-1}R$$

Thus, since $\phi_S^{-1}(Q)$ is an ideal of R, appealing once again to Proposition 1 from the previous lecture gives

$$(R-P) \cap \phi_S^{-1}(Q) = S \cap \phi_S^{-1}(Q) = \emptyset$$

The above equality gives $\phi_S^{-1}(Q) \subseteq P$. Hence, combining the previous results, we see that $\phi_S^{-1}(Q)$ is a prime ideal of R with $\phi_S^{-1}(Q) \subseteq P$.

The previous results show that there is a one-to-one correspondence between the set of all prime ideals of R contained in P and the set of all prime ideals of R_P. $\square$

Proof. (b): Let $S = R - P$. First, note that since P is a prime ideal of R and since $P \cap S = \emptyset$ we have by Proposition 1 from the previous lecture that P_P is a prime ideal of R_P. In particular, this gives $P_P \neq R_P$. Now, suppose that I is an ideal of R_P and $I \not\subseteq P_P$. Since I is an ideal of R_P, we have by Proposition 1 from the previous lecture that $I = J_P$ for some ideal J of R. Hence, we have $J_P = I \not\subseteq P_P$. Finally, note that for ideals M and N of R that $M \subseteq N$ implies that $M_P \subseteq N_P$. Since $J_P \not\subseteq P_P$, this implies that $J \not\subseteq P$ so that

$$S \cap J = (R-P) \cap J \neq \emptyset$$

Thus, since J is an ideal of R and since $S \cap J \neq \emptyset$, we have by Proposition 1 from the previous lecture that $I = J_P = R_P$. In particular, this shows that P_P is the unique maximal ideal of R_P. $\square$

Definition. A ***local ring*** is a commutative ring with 1 which has a unique maximal ideal.

Theorem. If R be a commutative ring with $1 \neq 0$, then the following are equivalent:

(a): R is a local ring.

(b): There is some proper ideal M of R such that all nonunits of R are contained in M.

(c): The nonunits of R form an ideal of R.

Proof. (a $\Rightarrow$ b): Suppose that R is a local ring and let M be the unique maximal ideal of R. Since M is a maximal ideal of R, we have $M \neq R$ so that M is a proper ideal of R. Now, let $a \in R$ be a nonunit of R. Then the ideal (a) is a proper ideal of R and is hence contained in some maximal ideal of R. But since M is the unique maximal ideal of R, this gives

$$a \in (a) \subseteq M$$

so that all nonunits of R are contained in M.

(b $\Rightarrow$ c): Let M be a proper ideal of R such that all nonunits of R are contained in M. On the other hand, let $m \in M$. If m were a unit of R, then

$$M \supseteq (m) = R$$

which contradicts the fact that M is properly contained in R. Hence, it must be the case that m is a nonunit of R. Thus, we see that M is exactly the set of nonunits of R so that the nonunits of R form an ideal of R since M is an ideal of R.

(c $\Rightarrow$ a): Let M denote the set of nonunits of R. By hypothesis, we have that M is an ideal of R. Furthermore, since $1 \in R$ is a unit of R we have that $1 \notin M$ so that $M \neq R$. Now, if I is an ideal of R with $I \not\subseteq M$, then there is some $i \in I$ such that $i \notin M$. Since $i \notin M$, we have that i is a unit of R and thus

$$I \supseteq (i) = R$$

so that $I = R$ and so M is the unique maximal ideal of R so that R is a local ring. $\square$

Example. Consider $\mathbb{Z}$ and let p be a prime number. Then $\mathbb{Z}_{(p)}$ is equal to the set $\{a/b : a, b \in \mathbb{Z}, p \text{ does not divide } b\}$. The unique maximal ideal of $\mathbb{Z}_{(p)}$ is all fractions with denominator not divisible by p and numerator divisible by p.

Proof. Note that by definition we have

$$\mathbb{Z}_{(p)} = (\mathbb{Z} - (p))^{-1}\mathbb{Z}$$

Thus, we see $\mathbb{Z}_{(p)}$ is the set of all fractions with numerators in $\mathbb{Z}$ and denominators in $\mathbb{Z} - (p)$. This completes the proof of the first claim made above.

Finally, let P denote the ideal of $\mathbb{Z}_{(p)}$ generated by the element $p = p/1 \in \mathbb{Z}_{(p)}$. We claim that P is the unique maximal ideal of $\mathbb{Z}_{(p)}$. Towards this end, first note that clearly $P \neq \mathbb{Z}_{(p)}$. Next, suppose that I is an ideal of $\mathbb{Z}_{(p)}$ with $I \not\subseteq P$. Since $\mathbb{Z}$ is a PID and $0 \notin \mathbb{Z} - (p)$, we have that $\mathbb{Z}_{(p)}$ is a PID. In particular, we may now write $I = (c)$ for some $c \in \mathbb{Z}_{(p)}$. Note that since $I \not\subseteq P$ we must have $c \notin P$ or else $I = (c) \subseteq P$.

Now, let $c = a/b$ for some $a, b \in \mathbb{Z}$. Since $a/b = c \notin P$, it follows that p does not divide a. Hence, we have $b/a \in \mathbb{Z}_{(p)}$. In particular, this shows that $c = a/b$ is a unit in $\mathbb{Z}_{(p)}$ so that $I = (c) = \mathbb{Z}_{(p)}$. This shows that P is the unique maximal ideal of $\mathbb{Z}_{(p)}$. $\square$

Example. The ***p-adic integers***, denoted $\mathbb{Z}_p$, where p is a prime number are defined as follows. Let $R_i = \mathbb{Z}/p^i\mathbb{Z}$ for $i \in \{1, 2, \dots\}$ and $\pi_i : R_i \to R_{i-1}$ for $i \in \{2, 3, \dots\}$ be the natural projection. Then

$$\mathbb{Z}_p = \left\{ f : \{1, 2, \dots\} \to \bigcup_{i \in \{1,2\dots\}} R_i : f(i) \in R_i \text{ if } i \geq 1 \text{ and } \pi_i(f(i)) = f(i-1) \text{ if } i \geq 2 \right\}$$

Define $+$ and $\cdot$ on $\mathbb{Z}_p$ componentwise. Then $\mathbb{Z}_p$ is a commutative ring with identity and in fact $\mathbb{Z}_p$ is an integral domain. There is a natural ring homomorphism

$$\mathbb{Z} \to \mathbb{Z}_p \quad \text{by} \quad a \mapsto (a + p^i\mathbb{Z})_{i \in \{1,2,\dots\}}$$

Note that this ring homomorphism has a trivial kernel and therefore this map is an injection. Hence, we may consider $\mathbb{Z} \subseteq \mathbb{Z}_p$, which shows that the cardinality of $\mathbb{Z}_p$ is at least countably infinite. It turns out that $\mathbb{Z}_p$ is uncountable.

Finally, note that every nonunit of $\mathbb{Z}_p$ is contained in the maximal ideal $p\mathbb{Z}_p$ of $\mathbb{Z}_p$ so that $p\mathbb{Z}_p$ is the unique maximal ideal of $\mathbb{Z}_p$. This shows that $\mathbb{Z}_p$ is a local ring. The field of fractions of $\mathbb{Z}_p$ is denoted $\mathbb{Q}_p$ and is called the field of ***p-adic numbers***.

Proof. That $\mathbb{Z}_p$ is a ring is easily verified. Furthermore, since $\mathbb{Z}/p^i\mathbb{Z}$ is a commutative ring with identity for each $i \in \{1, 2, \dots\}$, it now follows that $\mathbb{Z}_p$ is a commutative ring with identity. We will prove that $\mathbb{Z}_p$ is an integral domain when we discuss discrete valuation rings.

Next, we clearly see that the map $\mathbb{Z} \to \mathbb{Z}_p$ defined above is a ring homomorphism. We can see that the kernel of this homomorphism by noting that if $a \in \mathbb{Z}$ is in the kernel of the above map then p^i divides a for all $i \in \{1, 2, \dots\}$ and thus $a = 0$. Hence, this map is injective so that $\mathbb{Z}_p$ contains an isomorphic copy of $\mathbb{Z}$. That is, we may consider $\mathbb{Z} \subseteq \mathbb{Z}_p$ so that the cardinality of $\mathbb{Z}_p$ is at least countably infinite. That $\mathbb{Z}_p$ is uncountable will not be proven here.

Next, we prove that $p\mathbb{Z}_p$ is a maximal ideal of $\mathbb{Z}_p$. Indeed, consider the map

$$\mathbb{Z}_p \to \mathbb{Z}/p\mathbb{Z} \quad \text{by} \quad (a_1 + p\mathbb{Z}, a_2 + p^2\mathbb{Z}, \dots) \mapsto a_1 + p\mathbb{Z}$$

This map is easily seen to be a surjective ring homomorphism. We claim that the kernel of this map is $p\mathbb{Z}_p$. Indeed, if $\alpha = (a_1 + p\mathbb{Z}, a_2 + p^2\mathbb{Z}, \dots) \in p\mathbb{Z}_p$ then in particular p divides a_1 so that $a_1 + p\mathbb{Z}$ is the zero element of $\mathbb{Z}/p\mathbb{Z}$. Hence, we see that α is in the kernel of the above map. On the other hand, suppose that $\alpha = (a_1 + p\mathbb{Z}, a_2 + p^2\mathbb{Z}, \dots)$ is in the kernel of the above map. Then p must divide a_1. By the definition of a_2, it now follows that p also divides a_2. Inductively, we see that p divides a_i for all $i \in \{1, 2, \dots\}$ so that $\alpha \in p\mathbb{Z}_p$. This completes the proof of our claim. Lastly, note that by the First Isomorphism Theorem for Rings the above results show that $\mathbb{Z}_p/p\mathbb{Z}_p \simeq \mathbb{Z}/p\mathbb{Z}$. Furthermore, since $\mathbb{Z}/p\mathbb{Z}$ is a field as p is a prime number, this shows that $p\mathbb{Z}_p$ is a maximal ideal of $\mathbb{Z}_p$, as claimed.

Finally, we prove that every nonunit of $\mathbb{Z}_p$ is contained in $p\mathbb{Z}_p$. We will prove this by contrapositive. Towards this end, suppose that $\alpha = (a_1, a_2, \dots) \in \mathbb{Z}_p$ is not in $p\mathbb{Z}_p$. Since $\alpha \notin p\mathbb{Z}_p$, then in particular p does not divide a_1 so that $a_1 + p\mathbb{Z}$ is a nonzero element

of $\mathbb{Z}/p\mathbb{Z}$ and since $\mathbb{Z}/p\mathbb{Z}$ is a field, this implies that $a_1 + p\mathbb{Z}$ is a unit of $\mathbb{Z}/p\mathbb{Z}$. Let $b_1 + p\mathbb{Z} \in \mathbb{Z}/p\mathbb{Z}$ be the inverse of $a_1 + p\mathbb{Z}$. Inductively, using Number Theory concepts, we can construct an element $\beta = (b_1, b_2, \dots) \in \mathbb{Z}_p$ such that β is the inverse of α. This shows that α is a unit of $\mathbb{Z}_p$. In particular, since $\alpha \notin p\mathbb{Z}_p$ was arbitrary, we conclude that every element not in $p\mathbb{Z}_p$ is a unit of $\mathbb{Z}_p$ so that $p\mathbb{Z}_p$ contains all nonunits of $\mathbb{Z}_p$.

The previous results show that $p\mathbb{Z}$ is a maximal ideal (hence a proper ideal) of $\mathbb{Z}_p$ which contains all nonunits of $\mathbb{Z}_p$. This implies that $p\mathbb{Z}_p$ is the unique maximal ideal of $\mathbb{Z}_p$ so that $\mathbb{Z}_p$ is a local ring. This completes the proof. $\square$

Topic 2: Short Exact Sequences

Notation. Let R be a ring. Then $\mathcal{M}(R)$ denotes the category of R-modules.

Definition. Let R be a ring. A sequence

$$\cdots \longrightarrow A_i \xrightarrow{f_i} A_{i+1} \xrightarrow{f_{i+1}} \cdots \longrightarrow A_n \xrightarrow{f_n} A_{n+1} \xrightarrow{f_{n+1}} \cdots$$

where the A_i are objects of $\mathcal{M}(R)$ and the f_i are morphisms of $\mathcal{M}(R)$ is ***exact*** if $\mathrm{Im}(f_i) = \ker(f_{i+1})$ whenever f_i and f_{i+1} are both defined.

Example. Let A be a module and let B be a submodule of A. Then the sequence

$$0 \longrightarrow B \xrightarrow{i} A \xrightarrow{\pi} A/B \longrightarrow 0$$

is exact.

Proof. Note that the maps $0 \to B, i, \pi$, and $A/B \to 0$ are morphisms. Now, note that $\mathrm{Im}(0 \to B) = \{0\} = \ker(i)$. Next, we have $\mathrm{Im}(i) = B = \ker(\pi)$. Finally, we have $\mathrm{Im}(\pi) = A/B = \ker(A/B \to 0)$. $\square$

Definition. A ***short*** exact sequence is an exact sequence of the form

$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$$

Example. Let R be a ring and let A and B be objects of $\mathcal{M}(R)$. Then

$$0 \longrightarrow A \xrightarrow{i} A \oplus B \xrightarrow{\pi} B \longrightarrow 0$$

is a short exact sequence.

Proof. Note that the maps $0 \to A, i, \pi$, and $B \to 0$ are morphisms. Now, note that $\mathrm{Im}(0 \to A) = \{0\} = \ker(i)$. Next, we have $\mathrm{Im}(i) = A = \ker(\pi)$. Finally, we have $\mathrm{Im}(\pi) = B = \ker(B \to 0)$. $\square$

Theorem. (The Short Five Lemma): Let R be any ring and let

$$\begin{tikzcd}
0 \arrow[r] & A \arrow[r, "f"] \arrow[d, "\alpha"] & B \arrow[r, "g"] \arrow[d, "\beta"] & C \arrow[r] \arrow[d, "\gamma"] & 0 \\
0 \arrow[r] & A' \arrow[r, "f'"] & B' \arrow[r, "g'"] & C' \arrow[r] & 0
\end{tikzcd}$$

be a commutative diagram with short exact rows. Then

(a): If α and γ are monomorphisms, then β is a monomorphism.

(b): If α and γ are epimorphisms, then β is an epimorphism.

(c): If α and γ are isomorphisms, then β is an isomorphisms.

Proof. (a): Since β is an R-module homomorphism, it suffices to prove that $\ker(\beta)$ is trivial to establish that β is an injection. Towards this end, let $b \in \ker(\beta)$ so that $\beta(b) = 0$. Since the diagram commutes, this gives

$$\gamma(g(b)) = g'(\beta(b)) = g'(0) = 0$$

so that $g(b) \in \ker(\gamma)$. Since γ is an injection, this implies that $g(b) = 0$ and thus $b \in \ker(g) = \mathrm{Im}(f)$ since the first row of the diagram is exact. Hence, there is some $a \in A$ such that $f(a) = b$. Since the diagram commutes, we have that

$$f'(\alpha(a)) = \beta(f(a)) = \beta(b) = 0$$

so that $\alpha(a) \in \ker(f')$. By the diagram, we know that f' is an injection which implies that $\alpha(a) = 0$ since $\alpha(a) \in \ker(f')$. Thus, we have $a \in \ker(\alpha)$ and since α is an injection, this implies that $a = 0$. Thus, we now have

$$0 = f(0) = f(a) = b$$

We conclude that β is injective so that β is a monomorphism, completing the proof. $\square$

Proof. (b): Let $b' \in B'$ and let $c' = g'(b') \in C'$. Since γ is a surjection, there is some $c \in C$ such that $\gamma(c) = c'$. By the diagram, we know that g is a surjection so there is some $b \in B$ such that $g(b) = c$. Since the diagram commutes, we have that

$$g'(\beta(b)) = \gamma(g(b)) = \gamma(c) = c' = g'(b')$$

Since g' is an R-module homomorphism, we now have

$$0 = g'(b') - g'(\beta(b)) = g'(b' - \beta(b))$$

so that $b' - \beta(b) \in \ker(g') = \mathrm{Im}(f')$ since the second row of the diagram is exact. Thus, there is some $a' \in A'$ such that $f'(a') = b' - \beta(b)$. Since α is a surjection, there is some $a \in A$ such that $\alpha(a) = a'$. Thus, we have since the diagram commutes that

$$b' - \beta(b) = f'(a') = f'(\alpha(a)) = \beta(f(a))$$

so that since β is an R-module homomorphism we have

$$b' = \beta(f(a)) + \beta(b) = \beta(f(a) + b)$$

We conclude that β is surjective so that β is an epimorphism, completing the proof. $\square$

Proof. (c): This is immediate by the results from Part (a) and Part (b). $\square$

Definition. Two short exact sequences are ***isomorphic*** if there exist α, β, γ as in the lemma which are isomorphisms.

Remark. When this happens, then $\alpha^{-1}, \beta^{-1}, \gamma^{-1}$ are also isomorphisms in the same way.

Proof. By hypothesis, it remains to prove that the diagram

$$\begin{tikzcd}
0 \arrow[r] & A' \arrow[r, "f'"] \arrow[d, "\alpha^{-1}"] & B' \arrow[r, "g'"] \arrow[d, "\beta^{-1}"] & C' \arrow[r] \arrow[d, "\gamma^{-1}"] & 0 \\
0 \arrow[r] & A \arrow[r, "f"] & B \arrow[r, "g"] & C \arrow[r] & 0
\end{tikzcd}$$

commutes. Towards this end, first note that by hypothesis we have $f' \circ \alpha = \beta \circ f$ and $g' \circ \beta = \gamma \circ g$. By the first of these equalities, we have

$$f' = f' \circ \alpha \circ \alpha^{-1} = \beta \circ f \circ \alpha^{-1}$$

so that

$$\beta^{-1} \circ f' = \beta^{-1} \circ \beta \circ f \circ \alpha^{-1} = f \circ \alpha^{-1}$$

By the second of these equalities, we have that

$$g = \gamma^{-1} \circ \gamma \circ g = \gamma^{-1} \circ g' \circ \beta$$

so that

$$g \circ \beta^{-1} = \gamma^{-1} \circ g' \circ \beta \circ \beta^{-1} = \gamma^{-1} \circ g'$$

This shows that the above diagram commutes, completing the proof. □

Theorem. Let R be a ring and suppose that

$$\begin{tikzcd}
0 \arrow[r] & A_1 \arrow[r, "f"] & B \arrow[r, "g"] & A_2 \arrow[r] & 0
\end{tikzcd}$$

is a short exact sequence of R-modules. Then the following are equivalent:

(a): There is an R-module homomorphism $h : A_2 \to B$ such that $g \circ h = 1_{A_2}$.

(b): There is an R-module homomorphism $k : B \to A_1$ such that $k \circ f = 1_{A_1}$.

(c): The short exact sequence

$$\begin{tikzcd}
0 \arrow[r] & A_1 \arrow[r, "f"] & B \arrow[r, "g"] & A_2 \arrow[r] & 0
\end{tikzcd}$$

is isomorphic (with identity maps on A_1 and A_2) to the short exact sequence

$$\begin{tikzcd}
0 \arrow[r] & A_1 \arrow[r, "i_1"] & A_1 \oplus A_2 \arrow[r, "\pi_2"] & A_2 \arrow[r] & 0
\end{tikzcd}$$

Proof. (a $\Rightarrow$ c): Define

$$\phi : A_1 \oplus A_2 \to B \quad \text{by} \quad (a_1, a_2) \mapsto f(a_1) + h(a_2)$$

Since f and h are both R-module homomorphisms, it is easily verified that ϕ is an R-module homomorphism. We will now show that the diagram

$$\begin{tikzcd}
0 \arrow[r] & A_1 \arrow[r, "i_1"] \arrow[d, "1_{A_1}"] & A_1 \oplus A_2 \arrow[r, "\pi_2"] \arrow[d, "\phi"] & A_2 \arrow[r] \arrow[d, "1_{A_2}"] & 0 \\
0 \arrow[r] & A_1 \arrow[r, "f"] & B \arrow[r, "g"] & A_2 \arrow[r] & 0
\end{tikzcd}$$

commutes, or that $f = f \circ 1_{A_1} = \phi \circ i_1$ and that $g \circ \phi = 1_{A_2} \circ \pi_2 = \pi_2$.

To prove the first equality, let $a_1 \in A_1$. Then

$$(\phi \circ i_1)(a_1) = \phi(i_1(a_1)) = \phi((a_1, 0)) = f(a_1) + h(0) = f(a_1) + 0 = f(a_1)$$

so that $f = \phi \circ i_1$. To prove the second equality, first note that since the second row of the diagram is exact that $\ker(g) = \mathrm{Im}(f)$. Now, let $(a_1, a_2) \in A_1 \oplus A_2$. Then

$$\begin{aligned}
(g \circ \phi)((a_1, a_2)) &= g(\phi((a_1, a_2))) \\
&= g(f(a_1) + h(a_2)) \\
&= g(f(a_1)) + g(h(a_2)) \\
&= 0 + 1_{A_2}(a_2) \\
&= a_2 \\
&= \pi_2((a_1, a_2))
\end{aligned}$$

so that $g \circ \phi = \pi_2$. The above results show that the diagram is commutative. Since 1_{A_1} and 1_{A_2} are clearly isomorphisms, we have by the Short Five Lemma that ϕ is an isomorphism. This completes the proof.

(b $\Rightarrow$ c): Define

$$\psi : B \to A_1 \oplus A_2 \quad \text{by} \quad b \mapsto (k(b), g(b))$$

Since k and g are both R-module homomorphisms, it is easily verified that ψ is an R-module homomorphism. We will now show that the diagram

$$\begin{tikzcd}
0 \arrow[r] & A_1 \arrow[r, "f"] \arrow[d, "1_{A_1}"] & B \arrow[r, "g"] \arrow[d, "\psi"] & A_2 \arrow[r] \arrow[d, "1_{A_2}"] & 0 \\
0 \arrow[r] & A_1 \arrow[r, "i_1"] & A_1 \oplus A_2 \arrow[r, "\pi_2"] & A_2 \arrow[r] & 0
\end{tikzcd}$$

commutes, or that $i_1 = i_1 \circ 1_{A_1} = \psi \circ f$ and that $\pi_2 \circ \psi = 1_{A_2} \circ g = g$.

To prove the first equality, first note that since the first row of the diagram is exact that $\ker(g) = \mathrm{Im}(f)$. Now, let $a_1 \in A_1$. Then

$$\begin{aligned}
(\psi \circ f)(a_1) &= \psi(f(a_1)) \\
&= (k(f(a_1)), g(f(a_1))) \\
&= (1_{A_1}(a_1), 0) \\
&= (a_1, 0) \\
&= i_1(a_1)
\end{aligned}$$

so that $i_1 = \psi \circ f$. To prove the second equality, let $b \in B$. Then

$$(\pi_2 \circ \psi)(b) = \pi_2(\psi(b)) = \pi_2((k(b), g(b)) = g(b)$$

so that $\pi_2 \circ \psi = g$. The above results show that the diagram is commutative. Since 1_{A_1} and 1_{A_2} are clearly isomorphisms, we have by the Short Five Lemma that ψ is an isomorphism. This completes the proof.

(c $\Rightarrow$ a and b): By hypothesis, we have the commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & A_1 \arrow[r, "i_1"] \arrow[d, "1_{A_1}"] & A_1 \oplus A_2 \arrow[r, "\pi_2"] \arrow[d, "\phi"] & A_2 \arrow[r] \arrow[d, "1_{A_2}"] & 0 \\
0 \arrow[r] & A_1 \arrow[r, "f"] & B \arrow[r, "g"] & A_2 \arrow[r] & 0
\end{tikzcd}$$

where the first and second rows are exact and $\phi : A_1 \oplus A_2 \to B$ is an R-module isomorphism. Since the diagram is commutative, we have $f = f \circ 1_{A_1} = \phi \circ i_1$ and $g \circ \phi = 1_{A_2} \circ \pi_2 = \pi_2$. In particular, the first of these equalities gives

$$\phi^{-1} \circ f = \phi^{-1} \circ \phi \circ i_1 = i_1$$

so that $\phi^{-1} \circ f = i_1$.

Now, define $h : A_2 \to B$ by $h = \phi \circ i_2$ and define $k : B \to A_1$ by $\pi_1 \circ \phi^{-1}$. Since the defined composition of R-module homomorphisms is an R-module homomorphism, it follows that h and k are R-module homomorphisms. Furthermore, since $\pi_1 \circ i_1 = 1_{A_1}$ and $\pi_2 \circ i_2 = 1_{A_2}$, we obtain the equalities

$$g \circ h = g \circ \phi \circ i_2 = \pi_2 \circ i_2 = 1_{A_2}$$

and

$$k \circ f = \pi_1 \circ \phi^{-1} \circ f = \pi_1 \circ i_1 = 1_{A_1}$$

This completes the proof. $\square$

Note. In Turull's proof of (a $\Rightarrow$ c) he shows that $B = A_1' \oplus A_2'$, where $A_1' = f(A_1) \subseteq B$ and $A_2' = h(A_2) \subseteq B$.

Proof. Define $A_1' = f(A_1) \subseteq B$ and $A_2' = h(A_2) \subseteq B$. We will show that $B = A_1' + A_2'$ and that $A_1' \cap A_2' = \{0\}$. First, suppose that $b \in B$. We claim that $b - h(g(b)) \in \ker(g)$. Indeed, since $g \circ h = 1_{A_2}$, we have since g is an R-module homomorphism that

$$g(b - h(g(b)) = g(b) - g(h(g(b))) = g(b) - (g \circ h)(g(b)) = g(b) - 1_{A_2}(g(b)) = g(b) - g(b) = 0$$

so that $b - h(g(b)) \in \ker(g)$, as claimed. But since we have a short exact sequence, we have that $\ker(g) = \mathrm{Im}(f) = A_1'$ so that $b - h(g(b)) \in A_1'$. Furthermore, we clearly have $h(g(b)) \in \mathrm{Im}(h) = A_2'$. Combining the previous two results gives

$$b = (b - h(g(b)) + h(g(b)) \in A_1' + A_2'$$

Therefore, we have $B = A_1' + A_2'$.

Finally, suppose that $b \in A_1' \cap A_2'$. Since $b \in A_1' = f(A_1)$, there is some $a_1 \in A_1$ such that $b = f(a_1)$. Since $b \in A_2' = h(A_2)$, there is some $a_2 \in A_2$ such that $b = h(a_2)$. Applying g to both sides of the first of these equalities gives since $\ker(g) = \mathrm{Im}(f)$ as we have an exact sequence that

$$g(b) = g(f(a_1)) = 0$$

Since $g \circ h = 1_{A_2}$, applying g to both sides of the second of the above equalities gives

$$0 = g(b) = g(h(a_2)) = 1_{A_2}(a_2) = a_2$$

Thus, since h is an R-module homomorphism we have $b = h(a_2) = h(0) = 0$. This shows that $A_1' \cap A_2' = \{0\}$. The above results show that $B = A_1' \oplus A_2'$. $\square$

Definition. We say that a short exact sequence

$$0 \longrightarrow A_1 \xrightarrow{f} B \xrightarrow{g} A_2 \longrightarrow 0$$

is a ***split*** short exact sequence if it satisfies the conditions of the above theorem.

Note. In Turull's proof of (b $\Rightarrow$ c) from Theorem 1 of the previous lecture he shows that $B = \mathrm{Im}(f) \oplus \ker(k)$.

Proof. First, let $b \in B$. We claim that $b - f(k(b)) \in \ker(k)$. Indeed, notice that since k is an R-module homomorphism and since $k \circ f = 1_{A_1}$ we have

$$k(b - f(k(b)) = k(b) - k(f(k(b))) = k(b) - (k \circ f)(k(b)) = k(b) - 1_{A_1}(k(b)) = k(b) - k(b) = 0$$

which shows that $b - f(k(b)) \in \ker(k)$. Since we clearly have $f(k(b)) \in \mathrm{Im}(f)$, this gives

$$b = f(k(b)) + (b - f(k(b)) \in \mathrm{Im}(f) + \ker(k)$$

so that $B = \mathrm{Im}(f) + \ker(k)$.

Finally, suppose that $b \in \mathrm{Im}(f) \cap \ker(k)$. Since $b \in \mathrm{Im}(f)$, there is some $a_1 \in A_1$ such that $f(a_1) = b$. Since $b \in \ker(k)$, we have that $k(b) = 0$. Hence, since $k \circ f = 1_{A_1}$ we obtain

$$0 = k(b) = k(f(a_1)) = 1_{A_1}(a_1) = a_1$$

so that

$$b = f(a_1) = f(0) = 0$$

which shows $\mathrm{Im}(f) \cap \ker(k) = \{0\}$. The above results prove that $B = \mathrm{Im}(f) \oplus \ker(k)$. $\square$

Topic 3: Projective and Injective Modules

Definition. A module P is ***projective*** if given any diagram of modules and module homomorphisms of the form

$$\begin{tikzcd} & P \arrow[d, "f"] & \\ A \arrow[r, "g"] & B \arrow[r] & 0 \end{tikzcd}$$

with exact row there exists a module homomorphism $h : P \to A$ such that the diagram

$$\begin{tikzcd} & P \arrow[d, "f"] \arrow[dl, "h"'] & \\ A \arrow[r, "g"] & B \arrow[r] & 0 \end{tikzcd}$$

commutes.

Theorem. Let R be a ring with 1. Let F be a free R-module. Then F is projective.

Proof. Let S be a set such that $i : S \to F$ is a map of sets that makes F a free R-module and suppose that

$$\begin{tikzcd} & F \arrow[d, "f"] & \\ A \arrow[r, "g"] & B \arrow[r] & 0 \end{tikzcd}$$

is a diagram of R-modules and R-module homomorphisms with exact row. We must show that there is an R-module homomorphism $\beta : F \to A$ such that $g \circ \beta = f$.

Towards this end, first define a map of sets $\alpha : S \to A$ as follows. Let $s \in S$. Then $f(i(s)) \in B$. Now, note that g is a surjection since the above row is exact. Hence, there is some $a \in A$ such that $g(a) = f(i(s))$. Define $\alpha(s) = a$ and note that by construction we have $g \circ \alpha = f \circ i$.

Finally, since F is a free R-module there exists a (unique) R-module homomorphism $\beta : F \to A$ such that $\beta \circ i = \alpha$. Hence, we obtain since $g \circ \alpha = f \circ i$ that

$$g \circ \beta \circ i = g \circ \alpha = f \circ i$$

But recall that $f : F \to B$ is an R-module homomorphism. Furthermore, since the defined composition of R-module homomorphisms is an R-module homomorphism, we have that $g \circ \beta : F \to B$ is an R-module homomorphism. Thus, the above equality gives by uniqueness since F is a free R-module that $g \circ \beta = f$ which shows that F is projective. This completes the proof. $\square$

Corollary. Let R be a ring with 1. Then every R-module is a homomorphic image of a projective R-module.

Proof. Let A be an R-module and let $X \subseteq A$ is a set of generators for A. Let F be a the free R-module on X. Let $i : X \to F$ be a map of sets that makes F free on X and let $f : X \to A$ be the inclusion map. Since F is free on X, there is a (unique) R-module homomorphism $\overline{f} : F \to A$ such that $\overline{f} \circ i = f$. Now, let $x \in X$ and notice that

$$x = f(x) = \overline{f}(i(x)) \in \operatorname{Im}\left(\overline{f}\right)$$

Since $x \in X$ was arbitrary, this shows that $X \subseteq \operatorname{Im}\left(\overline{f}\right)$. But as X is a generating set for A, this inclusion now gives $A \subseteq \operatorname{Im}\left(\overline{f}\right)$. Since we clearly have $\operatorname{Im}\left(\overline{f}\right) \subseteq A$, the previous result gives $\operatorname{Im}\left(\overline{f}\right) = A$ so that A is the homomorphic image of the free R-module F. But since F is a free R-module, we have by the previous Theorem that F is projective as an R-module so that A is the homomorphic image of the projective R-module F. Since A was an arbitrary R-module, this completes the proof. $\square$

Example. Every $\mathbb{R}$-module is projective.

Proof. Since $\mathbb{R}$ is a field, we know that any $\mathbb{R}$-module can be considered as a vector space over $\mathbb{R}$ and hence any $\mathbb{R}$-module is a free $\mathbb{R}$-module. Since every free $\mathbb{R}$-module is projective by the previous Corollary, then, we conclude every $\mathbb{R}$-module is projective. $\square$

Example. Consider the ring $\mathbb{Z}$. Then $\mathbb{Z}$ is projective as a $\mathbb{Z}$-module and $\{0\}$ is projective as a $\mathbb{Z}$-module. However, we see that $\mathbb{Z}/2\mathbb{Z}$ is not projective as a $\mathbb{Z}$-module but is projective as a $\mathbb{Z}/2\mathbb{Z}$-module.

Proof. Since $\{1\} \subseteq \mathbb{Z}$ is a basis for $\mathbb{Z}$ over $\mathbb{Z}$, it follows that $\mathbb{Z}$ is a free $\mathbb{Z}$-module and hence projective as a $\mathbb{Z}$-module. Similarly, since $\{\overline{1}\} \subseteq \mathbb{Z}/2\mathbb{Z}$ is a basis for $\mathbb{Z}/2\mathbb{Z}$ over $\mathbb{Z}/2\mathbb{Z}$, it follows that $\mathbb{Z}/2\mathbb{Z}$ is a free $\mathbb{Z}/2\mathbb{Z}$-module and hence projective as a $\mathbb{Z}/2\mathbb{Z}$-module. Since $\emptyset \subseteq \{0\}$ is a basis for $\{0\}$ over $\mathbb{Z}$, it follows that $\{0\}$ is a free $\mathbb{Z}$-module and hence projective as a $\mathbb{Z}$-module.

It remains to show that $\mathbb{Z}/2\mathbb{Z}$ is not projective as a $\mathbb{Z}$-module. For the sake of contradiction, suppose that $\mathbb{Z}/2\mathbb{Z}$ were projective as a $\mathbb{Z}$-module. Consider the diagram $\mathbb{Z}$-modules and maps

$$\begin{tikzcd}
 & \mathbb{Z}/2\mathbb{Z} \arrow[d, "i"] & \\
\mathbb{Z}/4\mathbb{Z} \arrow[r, "g"] & \mathbb{Z}/2\mathbb{Z} \arrow[r] & 0
\end{tikzcd}$$

where i is the identity map and $g : \mathbb{Z}/4\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$ is the canonical projection. Then we have that g is a surjective $\mathbb{Z}$-module homomorphism and hence the above diagram is a diagram of $\mathbb{Z}$-modules and $\mathbb{Z}$-module homomorphisms with exact row. Therefore, since $\mathbb{Z}/2\mathbb{Z}$ is projective as a $\mathbb{Z}$-module there is a $\mathbb{Z}$-module homomorphism $h : \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/4\mathbb{Z}$ such that $g \circ h = i$.

Now, since $|h(\overline{1})|$ must divide $|\overline{1}| = 2$ as h is an $\mathbb{Z}$-module homomorphism, it follows that $|h(\overline{1})| \in \{1, 2\}$ so that $h(\overline{1}) \in \{\overline{0}, \overline{2}\}$. If $h(\overline{1}) = \overline{0}$, then we obtain

$$\overline{0} = g(\overline{0}) = g(h(\overline{1})) = i(\overline{1}) = \overline{1}$$

which is a contradiction. Therefore, it must be the case that $h(\overline{1}) = \overline{2}$. But recall that $g \circ h = i$ so that this result gives

$$\overline{1} = i(\overline{1}) = g(h(\overline{1})) = g(\overline{2})$$

Thus, since g is a $\mathbb{Z}$-module homomorphism we have

$$\overline{0} = \overline{1} + \overline{1} = g(\overline{1}) + g(\overline{1}) = g(\overline{1} + \overline{1}) = g(\overline{2}) = \overline{1}$$

which is a contradiction. We conclude that $\mathbb{Z}/2\mathbb{Z}$ is not projective as a $\mathbb{Z}$-module, completing the proof. $\square$

Theorem. Let R be a ring with 1 and let P be an R-module. Then the following are equivalent:

(a): P is projective.

(b): Every short exact sequence

$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} P \longrightarrow 0$$

splits.

(c): There is a free R-module F and an R-module K such that $F \simeq K \oplus P$.

Proof. (a $\Rightarrow$ b): Note we have the diagram of R-modules and R-module homomorphisms

$$\begin{tikzcd} & & & P \arrow[d, "1_P"] & \\ 0 \arrow[r] & A \arrow[r, "f"] & B \arrow[r, "g"] & P \arrow[r] & 0 \end{tikzcd}$$

with exact row. Since P is projective, there is an R-module homomorphism $h : P \to B$ such that $g \circ h = 1_P$. Therefore, the given short exact sequence splits.

(b $\Rightarrow$ c): Since every module is the homomorphic image of a free module, there exists a free R-module F and a surjective R-module homomorphism $g : F \to P$. Let $K = \ker(g)$ and $i : K \to F$ be the inclusion map. Since g is a surjection, it follows that the sequence

$$0 \longrightarrow K \xrightarrow{i} F \xrightarrow{g} P \longrightarrow 0$$

is a short exact sequence. By hypothesis, this short exact sequence splits. In other words, we obtain $F \simeq K \oplus P$.

(c $\Rightarrow$ a): Let $a : S \to F$ be a map of sets that makes F free. Let $\pi : F \to P$ denote the canonical projection and $i : P \to F$ denote the canonical inclusion. Now, we prove

the main result. Towards this end, suppose that we are given the diagram of R-modules and R-module homomorphisms

$$\begin{tikzcd} & P \arrow[d, "f"] & \\ A \arrow[r, "g"] & B \arrow[r] & 0 \end{tikzcd}$$

with exact row. Define a map $b : S \to A$ as follows. Let $s \in S$. Then $f(\pi(a(s))) \in B$. Since the above row is exact, we have that g is a surjection and hence there is some $c \in A$ such that $g(c) = f(\pi(a(s)))$. Define $b(s) = c$. By construction, then, we see that $g \circ b = f \circ \pi \circ a$.

Now, since $b : S \to A$ is a map of sets and since F is free it follows that there exists a unique R-module homomorphism $h_1 : F \to A$ such that $h_1 \circ a = b$. Define $h_2 : P \to A$ by $h_2 = h_1 \circ i$. Since the defined composition of R-module homomorphisms is an R-module homomorphism, it follows that h_2 is an R-module homomorphism. We will show that $g \circ h_2 = f$.

Towards this end, first notice that by the above results we have

$$f \circ \pi \circ a = g \circ b = g \circ h_1 \circ a$$

Therefore, since F is free we have by uniqueness that $f \circ \pi = g \circ h_1$. Furthermore, since $\pi \circ i = 1_P$ the previous equality and the above results give

$$f = f \circ 1_P = f \circ \pi \circ i = g \circ h_1 \circ i = g \circ h_2$$

which proves that $g \circ h_2 = f$. We conclude that P is projective. $\square$

Proposition. Let R be a ring with 1. A direct sum of R-modules $\bigoplus_{i \in I} P_i$ is projective if and only if P_i is projective for each $i \in I$.

Proof. For the first direction, assume that the direct sum of R-modules $\bigoplus_{i \in I} P_i$ is projective and fix any $j \in I$. Let $\pi : \bigoplus_{i \in I} P_i \to P_j$ denote the canonical projection and $i : P_j \to \bigoplus_{i \in I} P_i$ denote the canonical inclusion. Now, assume we are given the diagram of R-modules and R-module homomorphisms

$$\begin{tikzcd} & P_j \arrow[d, "f"] & \\ A \arrow[r, "g"] & B \arrow[r] & 0 \end{tikzcd}$$

with exact row. Note that since the defined composition of R-module homomorphisms is an R-module homomorphism that we have $f \circ \pi : \bigoplus_{i \in I} P_i \to B$ is an R-module homomorphism. Therefore, since $\bigoplus_{i \in I} P_i$ is projective, this implies that there exists an R-module homomorphism $h_1 : \bigoplus_{i \in I} P_i \to A$ such that $g \circ h_1 = f \circ \pi$.

Finally, define $h_2 : P_j \to A$ by $h_2 = h_1 \circ i$. Since the defined composition of R-module homomorphisms is an R-module homomorphism, we have that h_2 is an R-module

homomorphism. Furthermore, since $\pi \circ i = 1_{P_j}$ we see that

$$g \circ h_2 = g \circ h_1 \circ i = f \circ \pi \circ i = f \circ 1_{P_j} = f$$

which shows that $g \circ h_2 = f$. We conclude that P_j is projective. Since $j \in I$ was arbitrary, this completes the proof of the first direction.

For the second direction, assume that P_i is projective for each $i \in I$. Then for each $i \in I$ there exists a free R-module F_i such that P_i is isomorphic to a direct summand of F_i. Since the direct sum of a family of free R-modules is a free R-module, we have that $\bigoplus_{i \in I} F_i$ is a free R-module. Furthermore, since each P_i is isomorphic to a direct summand of F_i, it now follows that $\bigoplus_{i \in I} P_i$ is isomorphic to a direct summand of $\bigoplus_{i \in I} F_i$. Therefore, since $\bigoplus_{i \in I} F_i$ is a free R-module, this implies that $\bigoplus_{i \in I} P_i$ is projective. This completes the proof of the second direction. $\square$

Note. Informally, projective means commutative the diagram

$$\begin{tikzcd}
 & P \arrow[dl, dotted, "h"'] \arrow[d, "f"] & \\
A \arrow[r, "g"] & B \arrow[r] & 0
\end{tikzcd}$$

with exact row. Informally, injective will mean "reversing" all of the arrows in the above commutative diagram and replacing the projective module P with the injective module I. That is, injective will mean the commutative diagram

$$\begin{tikzcd}
 & I & \\
A \arrow[ur, dotted, "h"] & B \arrow[l, "g"] \arrow[u, "f"] & 0 \arrow[l]
\end{tikzcd}$$

with exact row. Equivalently, since we prefer to read these diagrams left-to-right and up-to-down, injective will mean the commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & A \arrow[r, "g"] \arrow[d, "f"] & B \\
 & I \arrow[ur, dotted, "h"] &
\end{tikzcd}$$

with exact row.

Note. It was mentioned in class to know an example of a projective module that is not a free module. We claim that $\mathbb{Z}/2\mathbb{Z}$ and $\mathbb{Z}/3\mathbb{Z}$ are projective $\mathbb{Z}/6\mathbb{Z}$-modules but are not free $\mathbb{Z}/6\mathbb{Z}$-modules.

Proof. First, note that $\mathbb{Z}/2\mathbb{Z}$ and $\mathbb{Z}/3\mathbb{Z}$ are $\mathbb{Z}/6\mathbb{Z}$-modules. Furthermore, clearly, we have that $\mathbb{Z}/6\mathbb{Z}$ is a free $\mathbb{Z}/6\mathbb{Z}$-module. Since $\mathbb{Z}/6\mathbb{Z} \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$ as 2 and 3 are relatively prime integers, it now follows that both $\mathbb{Z}/2\mathbb{Z}$ and $\mathbb{Z}/3\mathbb{Z}$ are projective $\mathbb{Z}/6\mathbb{Z}$-modules since $\mathbb{Z}/6\mathbb{Z}$ is a free $\mathbb{Z}/6\mathbb{Z}$-module by the previous observation.

Now, recall that any free $\mathbb{Z}/6\mathbb{Z}$-module is isomorphic to a direct sum of copies of $\mathbb{Z}/6\mathbb{Z}$. Therefore, if F is a free $\mathbb{Z}/6\mathbb{Z}$-module it must be the case that

$$|F| \geq |\mathbb{Z}/6\mathbb{Z}| = 6$$

Since $|\mathbb{Z}/2\mathbb{Z}| = 2 < 6$ and $|\mathbb{Z}/3\mathbb{Z}| = 3 < 6$, then, it now follows that $\mathbb{Z}/2\mathbb{Z}$ is not a free $\mathbb{Z}/6\mathbb{Z}$-module and that $\mathbb{Z}/3\mathbb{Z}$ is not a free $\mathbb{Z}/6\mathbb{Z}$-module. This completes the proof. $\square$

Note. Throughout this lecture, we assume that R is a ring with 1.

Definition. Let J be an R-module. Then J is ***injective*** if given any diagram of R-modules and R-module homomorphisms

$$\begin{tikzcd} 0 \arrow[r] & A \arrow[r, "g"] \arrow[d, "f"] & B \\ & J & \end{tikzcd}$$

with exact row there exists an R-module homomorphism $h : B \to J$ such that the diagram

$$\begin{tikzcd} 0 \arrow[r] & A \arrow[r, "g"] \arrow[d, "f"] & B \arrow[dl, "h"] \\ & J & \end{tikzcd}$$

commutes.

Lemma. An R-module J is injective if and only if for any left ideal L of R any R-module homomorphism $\phi : L \to J$ can be extended to an R-module homomorphism $R \to J$.

Proof. For the first direction, assume that J is an injective R-module. Let L be a left ideal of R and suppose that $\phi : L \to R$ is an R-module homomorphism. Now, let $i : L \to R$ be the inclusion map. Then i is an injective R-module homomorphism and thus we obtain the diagram of R-modules and R-module homomorphisms

$$\begin{tikzcd} 0 \arrow[r] & L \arrow[r, "i"] \arrow[d, "\phi"] & R \\ & J & \end{tikzcd}$$

with exact row. Since J is injective, then, it follows that there exists an R-module homomorphism $h : R \to J$ such that $h \circ i = \phi$. But since $i : L \to R$ is the inclusion map, it now follows by the previous equality that the R-module homomorphism $h : R \to J$ extends ϕ. This completes the proof of the first direction.

For the second direction, suppose that we are given the following diagram of R-modules and R-module homomorphisms

$$\begin{tikzcd} 0 \arrow[r] & A \arrow[r, "g"] \arrow[d, "f"] & B \\ & J & \end{tikzcd}$$

with exact row. Now, let $\mathcal{S}$ denote the collection of all pairs (C, h), where C is a submodule of B containing $\mathrm{Im}(g)$ and $h : C \to J$ is an R-module homomorphism such that $h \circ g = f$. First, note that since the R-module homomorphic image of an R-module is an R-module, we have that $\mathrm{Im}(g)$ is a submodule of B clearly containing $\mathrm{Im}(g)$. Furthermore, note that since g is injective as the above row is exact and since the defined composition of R-module homomorphisms is an R-module homomorphism that $f \circ g^{-1} : \mathrm{Im}(g) \to J$ is an R-module homomorphism with

$$\left(f \circ g^{-1}\right) \circ g = f \circ g^{-1} \circ g = f \circ 1_A = f$$

In particular, the above result shows that $(\mathrm{Im}(g), f \circ g^{-1}) \in \mathcal{S}$ so that $\mathcal{S} \neq \emptyset$.

Next, define for $(C_1, h_1), (C_2, h_2) \in \mathcal{S}$ that $(C_1, h_1) \leq (C_2, h_2)$ if and only if $C_1 \subseteq C_2$ and $h_2\big|_{C_1} = h_1$. It is easily verified that $\leq$ is a partial ordering on $\mathcal{S}$. Now, let $\mathcal{C}$ be a nonempty chain in $\mathcal{S}$. Let C be the union of the first coordinates of the elements of $\mathcal{C}$. Then since $\mathcal{C}$ is a chain, it follows that C is a submodule of B that clearly contains $\mathrm{Im}(g)$ since the first coordinate of each element in $\mathcal{C}$ contains $\mathrm{Im}(g)$. Let $h : C \to J$ be defined as follows. For an element $c \in C$ if $(C_1, h_1) \in \mathcal{C}$ with $c \in C_1$, define $h(c) = h_1(c)$. Then h is a well-defined R-module homomorphism by the definition of the partial ordering $\leq$ on $\mathcal{S}$. The previous results show that $(C, h) \in \mathcal{S}$. Thus, we see that (C, h) is clearly an upper bound for $\mathcal{C}$ in $\mathcal{S}$. Hence, by Zorn's Lemma we may conclude that there is some maximal element $(H, h) \in \mathcal{S}$.

We claim that $H = B$. Indeed, for the sake of contradiction suppose that $H \neq B$. Since $H \subseteq B$ but $H \neq B$, it follows that there is some $b \in B$ with $b \notin H$. Now, define

$$L = \{r \in R : rb \in H\}$$

We show that L is a left ideal of R. First, note that $0 \in R$ and $0 \cdot b = 0 \in H$ since H is an R-module. This result shows that $0 \in L$ so that $L \neq \emptyset$. Next, suppose that $r_1, r_2 \in L$. Then $r_1 b, r_2 b \in H$. Note that $r_1 - r_2 \in R$ since R is a ring and that $r_1 b - r_2 b \in H$ since H is a module with $r_1 b, r_2 b \in H$. Hence, we obtain

$$(r_1 - r_2)b = r_1 b - r_2 b \in H$$

so that $r_1 - r_2 \in L$ which shows that L is a subgroup of R under addition. Finally, let $r \in L$ and $s \in R$. Since $r \in L$ we have $rb \in H$ and since H is an R-module and $s \in R$, we now have $s(rb) \in H$. Thus, we obtain since $sr \in R$ as R is a ring and since

$$(sr)b = s(rb) \in H$$

that $sr \in L$ which completes the proof that L is a left ideal of R.

Now, define a map

$$\psi : L \to J \quad \text{by} \quad r \mapsto h(rb)$$

We claim that ψ is a well-defined R-module homomorphism. First, to see that ψ is well-defined note that if $r \in L$ then $rb \in H$ by the definition of L. Therefore, for any $r \in L$ we have that $h : H \to J$ is defined at rb since $rb \in H$. By the definition of ψ as presented above, this proves that ψ is a well-defined map.

Finally, suppose that $s \in R$ and $r_1, r_2 \in L$. Since L is a left ideal of R and $r_1 \in L$, it follows that $sr_1 \in L$ and since $r_2 \in L$ we now have that $sr_1 + r_2 \in L$ since L is closed under addition. Furthermore, since $r_1, r_2 \in L$ we have by the definition of L that $r_1b, r_2b \in H$ by the definition of L so that h is defined at r_1b and r_2b. Similarly, since $sr_1 \in L$ by the previous observation we have by the definition of L that $sr_1b \in H$ so that h is defined at sr_1b. Thus, by the definition of ψ and since h is an R-module homomorphism we obtain that

$$\begin{aligned}
\psi(sr_1 + r_2) &= h((sr_1 + r_2)b) \\
&= h(sr_1b + r_2b) \\
&= h(sr_1b) + h(r_2b) \\
&= sh(r_1b) + h(r_2b) \\
&= s\psi(r_1) + \psi(r_2)
\end{aligned}$$

which shows that ψ is an R-module homomorphism. By hypothesis, then, we have that ψ can be extended to an R-module homomorphism $k : R \to J$. In particular, since k extends ψ, we have by the definition of ψ that for all $r \in L$ we have $k(r) = \psi(r) = h(rb)$.

Now, since R has 1 we may define $c = k(1)$. Define a map $\overline{h} : H + Rb \to J$ by $\overline{h}(a + rb) = h(a) + rc$ for all $a \in H$ and $r \in R$. We claim that $\overline{h} : H + Rb \to J$ is a well-defined R-module homomorphism that extends h.

To see that $\overline{h}$ is well-defined, first note that if $a + rb \in H + Rb$ that $h(a) \in J$ since h maps H into J. Furthermore, we have that $rc \in J$ since k maps R into J and $c = k(1)$ and J is an ideal so that $rc \in J$. Thus, since J is an ideal and $h(a), rc \in J$ we have that

$$\overline{h}(a + rb) = h(a) + rc \in J$$

so that $\overline{h}$ actually does map $H + Rb$ into J.

Next, suppose that $a + rb, a' + r'b \in H + Rb$ and $a + rb = a' + r'b$. By this equality, then, we obtain

$$a - a' = r'b - rb = (r' - r)b$$

and since $a, a' \in H$ and H is a module, it follows that $a - a' \in H$ so that by $(r' - r)b \in H$. By the definition of L, then, this shows that $r' - r \in L$. Now, note that by the definition of $\overline{h}$, the definition of h, the definition of k, the definition of ψ, since h and k are

R-module homomorphisms, and since k is equal to ψ on L we obtain

$$\begin{aligned}
\overline{h}(a+rb)-\overline{h}(a'+r'b) &= [h(a)+rc]-[h(a')+r'c] \\
&= [h(a)-h(a')]-[(r'-r)c] \\
&= h(a-a')-(r'-r)k(1) \\
&= h(a-a')-k((r'-r)\cdot 1) \\
&= h(a-a')-k(r'-r) \\
&= h(a-a')-\psi(r'-r) \\
&= h(a-a')-h((r'-r)b) \\
&= h((a-a')-(r'-r)b) \\
&= h((a-a')-(r'b-rb)) \\
&= h((a-a')-(a-a')) \\
&= h(0) \\
&= 0
\end{aligned}$$

The above shows that $\overline{h}(a+rb)=\overline{h}(a'+r'b)$ so that $\overline{h}$ is well-defined.

To see that $\overline{h}$ is an R-module homomorphism, let $a+rb, a'+r'b \in H+Rb$ and $s \in R$. Since $a \in H$ and H is an R-module, it follows that $sa \in H$ and hence $sa+a' \in H$ since H is an R-module. Furthermore, we have $sr+r' \in R$ since R is a ring and $s, r, r' \in R$. Hence, this shows that

$$(sa+a')+(sr+r')b \in H+Rb$$

Hence, by the definition of $\overline{h}$, the definition of h, and since h is an R-module homomorphism we obtain

$$\begin{aligned}
\overline{h}(s(a+rb)+(a'+r'b)) &= \overline{h}((sa+a')+(sr+r')b) \\
&= h(sa+a')+(sr+r')c \\
&= [sh(a)+h(a')]+[s(rc)+r'c] \\
&= s[h(a)+rc]+[h(a')+r'c] \\
&= s\overline{h}(a+rb)+\overline{h}(a'+r'b)
\end{aligned}$$

The above shows that $\overline{h}$ is an R-module homomorphism.

To see that $\overline{h}$ extends h, let $a \in H$. Then

$$a = a+0 = a+0b \in H+Rb$$

and hence by the definition of $\overline{h}$ we obtain

$$\overline{h}(a) = \overline{h}(a+0b) = h(a)+0c = h(a)+0 = h(a)$$

so that $\overline{h}$ extends h.

To complete the proof, note that $H+Rb$ is a submodule of B containing $\mathrm{Im}(g)$ since H contains $\mathrm{Im}(g)$ and $H \subseteq H+Rb$. Furthermore, as was shown above, we have that

$\overline{h}$ is an R-module homomorphism such that $\overline{h} \circ g = f$ since $h \circ g = f$ and $\overline{h}$ extends h. This shows that $(H + Rb, \overline{h}) \in \mathcal{S}$. Furthermore, we have that $H \subseteq H + Rb$ and $\overline{h}\big|_H = h$ by the above results. In particular, we now have $(H, h) \leq (H + Rb, \overline{h})$. But since H is properly contained in $H + Rb$ since $b \notin H$ and R has identity, this contradicts the maximality of $(H, h) \in \mathcal{S}$. We conclude that $H = B$ and hence $h : B \to J$ is an R-module homomorphism such that $h \circ g = f$. This completes the proof that J is an injective R-module. □

Definition. An abelian group D is said to be ***divisible*** if for any $y \in D$ and for any nonzero $n \in \mathbb{Z}$ there is some $x \in D$ such that $y = nx$.

Example. $\mathbb{Z}$ is not divisible but $\mathbb{Q}$ is divisible. The trivial group is divisible. $\mathbb{Z}/2\mathbb{Z}$ is not divisible. $\mathbb{R}$ is divisible.

Proof. To see that $\mathbb{Z}$ is not divisible, consider the element $y = 3 \in \mathbb{Z}$. Then for the nonzero integer $n = 5 \in \mathbb{Z}$, clearly, there is no $x \in \mathbb{Z}$ such that $y = nx$ so that $\mathbb{Z}$ is not divisible. To see that $\mathbb{Q}$ is divisible, let $y = a/b \in \mathbb{Q}$ and $n \in \mathbb{Z}$ be nonzero. Then $x = a/nb \in \mathbb{Q}$ and

$$y = \frac{a}{b} = n \cdot \frac{a}{nb} = nx$$

so that $\mathbb{Q}$ is divisible.

To see that the trivial group $\{0\}$ is divisible, let $y \in \{0\}$ and $n \in \mathbb{Z}$ be nonzero. Then we have $y = 0$ and for the element $x = 0 \in \{0\}$ we have

$$y = 0 = n0 = nx$$

so that the trivial group $\{0\}$ is divisible.

To see that $\mathbb{Z}/2\mathbb{Z}$ is not divisible, consider the element $y = \overline{1} \in \mathbb{Z}/2\mathbb{Z}$. Then for the nonzero integer $n = 2 \in \mathbb{Z}$, we have that $nx = \overline{0}$ for all $x \in \mathbb{Z}/2\mathbb{Z}$. In particular, this shows that there is no $x \in \mathbb{Z}/2\mathbb{Z}$ such that $y = nx$ so that $\mathbb{Z}/2\mathbb{Z}$ is not divisible.

To see that $\mathbb{R}$ is divisible, let $y \in \mathbb{R}$ and $n \in \mathbb{Z}$ be nonzero. Then $x = y/n \in \mathbb{R}$ and

$$y = n \cdot \frac{y}{n} = nx$$

so that $\mathbb{R}$ is divisible. □

Lemma. An abelian group is divisible if and only if it is injective as a $\mathbb{Z}$-module.

Proof. For the first direction, let A be a divisible abelian group. Since A is an abelian group, we have that A is a $\mathbb{Z}$-module. Therefore, we know that A is injective as a $\mathbb{Z}$-module if and only if for any left ideal I of $\mathbb{Z}$ any $\mathbb{Z}$-module homomorphism $f : I \to A$ can be extended to a $\mathbb{Z}$-module homomorphism $h : \mathbb{Z} \to A$. We will use this equivalence to show that A is an injective $\mathbb{Z}$-module.

Towards this end, let I be a left ideal of $\mathbb{Z}$ and suppose that $f : I \to A$ is a $\mathbb{Z}$-module homomorphism. Since $\mathbb{Z}$ is a PID, there is some element $n \in \mathbb{Z}$ such that $I = (n)$. If

$n = 0$, then clearly

$$I = (n) = (0) = \{0\}$$

and the remainder of the proof is trivial in this case. Therefore, assume that $n \neq 0$ and note that the $\mathbb{Z}$-module homomorphism $f : I \to A$ is really the $\mathbb{Z}$-module homomorphism $f : (n) \to A$. Now, notice that clearly $f(n) \in A$ and since A is divisible and $n \in \mathbb{Z}$ is nonzero it follows that there is some $a \in A$ such that $f(n) = na$.

Finally, define a map $h : \mathbb{Z} \to A$ by $h(1) = a$. Then it is easily verified that h is a $\mathbb{Z}$-module homomorphism. Furthermore, suppose that $z \in I = (n)$. Then there is some $k \in \mathbb{Z}$ such that $z = kn$. Hence, we obtain since h and f are $\mathbb{Z}$-module homomorphisms and as $f(n) = na$ and $h(1) = a$ that

$$h(z) = h(kn) = h(kn \cdot 1) = knh(1) = kna = k(na) = kf(n) = f(kn) = f(z)$$

Since $z \in I$ was arbitrary, this shows that h extends f. We conclude that A is an injective $\mathbb{Z}$-module, completing the proof of the first direction.

For the second direction, let A be an abelian group so that A is a $\mathbb{Z}$-module and suppose that A is injective as a $\mathbb{Z}$-module. Let $y \in A$ and let $n \in \mathbb{Z}$ be nonzero. Note that since $\{n\} \subseteq (n)$ is a basis over $\mathbb{Z}$ for the ideal (and hence $\mathbb{Z}$-module) (n) it follows that (n) is free $\mathbb{Z}$-module.

Now, let $i : \{n\} \to (n)$ be the inclusion map and define $g : \{n\} \to A$ by $g(n) = y$. Then since (n) is a free $\mathbb{Z}$-module and since A is a $\mathbb{Z}$-module, it follows that there exists a (unique) $\mathbb{Z}$-module homomorphism $f : (n) \to A$ such that $f \circ i = g$. In other words, we have that $f : (n) \to A$ is a $\mathbb{Z}$-module homomorphism such that

$$f(n) = f(i(n)) = g(n) = y$$

We will use the fact that $f(n) = y$ in what follows.

Now, since (n) is a left ideal of $\mathbb{Z}$ and since A is an injective $\mathbb{Z}$-module, it follows that the above $\mathbb{Z}$-module homomorphism $f : (n) \to A$ can be extended to a $\mathbb{Z}$-module homomorphism $h : \mathbb{Z} \to A$. Finally, let $a = h(1) \in A$. Then since h extends f and as h is a $\mathbb{Z}$-module homomorphism, we have that

$$y = f(n) = h(n) = h(n \cdot 1) = nh(1) = na$$

so that $y = na$. Since $y \in A$ and the nonzero element $n \in \mathbb{Z}$ were arbitrary, this shows that A is divisible. This completes the proof of the second direction. $\square$

Lemma. Every abelian group may be embedded in a divisible abelian group.

Proof. Let A be an abelian group. Then A is a $\mathbb{Z}$-module and hence is the homomorphic image of a free $\mathbb{Z}$-module. In other words, there exists a free $\mathbb{Z}$-module F and a surjective $\mathbb{Z}$-module homomorphism $h : F \to A$. Let $K = \ker(h)$. Then by the First Isomorphism Theorem for Modules, we obtain that $F/K \simeq A$.

Now, since F is a free $\mathbb{Z}$-module, it follows that F is isomorphic to a direct sum of copies of $\mathbb{Z}$. Let D denote a direct sum of copies of $\mathbb{Q}$ where the number of copies of $\mathbb{Q}$ in this direct sum is equal to the number of copies of $\mathbb{Z}$ involved in the direct sum to

which F is isomorphic. Since $\mathbb{Q}$ is divisible and since the direct sum of divisible groups is divisible, it follows that D is divisible.

Finally, since $\mathbb{Z} \subseteq \mathbb{Q}$ and by the above results it follows that there is an embedding $f : F \to D$. The embedding f induces an isomorphism that yields $F/K \simeq f(F)/f(K)$. Combining the above results, we obtain

$$A \simeq F/K \simeq f(F)/f(K) \subseteq D/f(K)$$

which shows that A can be embedded in the abelian group $D/f(K)$. But note that $D/f(K)$ is the homomorphic image of the canonical projection map $\pi : D \to D/f(K)$. Since D is divisible and since the homomorphic image of a divisible group is divisible, then, we conclude that $D/f(K)$ is divisible. By the above result, we conclude that A can be embedded in the divisible group $D/f(K)$. This completes the proof. $\square$

Remark. Let A be an R-module. Then $\mathrm{Hom}_R(R, A)$ is an R-module under $(r\phi)(s) = \phi(sr)$ for all $\phi \in \mathrm{Hom}_R(R, A)$ and for all $r, s \in R$ and $\mathrm{Hom}_R(R, A) \simeq A$ as R-modules.

Proof. We first prove that $\mathrm{Hom}_R(R, A)$ is an R-module. Indeed, notice that $\mathrm{Hom}_R(R, A)$ is clearly an abelian group under addition and that if $r \in R$ and $\phi \in \mathrm{Hom}_R(R, A)$ then $r\phi \in \mathrm{Hom}_R(R, A)$. Furthermore, all of the module axioms are also easily verified with the exception of the axiom $r_1(r_2\phi) = (r_1r_2)\phi$ for all $r_1, r_2 \in R$ and $\phi \in \mathrm{Hom}_R(R, A)$. We prove this here. Towards this end, let $r_1, r_2, s \in R$ and $\phi \in \mathrm{Hom}_R(R, A)$. Then by definition, we see

$$[r_1(r_2\phi)]\,(s) = (r_2\phi)(sr_1) = \phi(sr_1r_2) = [(r_1r_2)\phi](s)$$

which shows that $r_1(r_2\phi) = (r_1r_2)\phi$. This completes the proof that $\mathrm{Hom}_R(R, A)$ is an R-module.

Secondly, we prove that $\mathrm{Hom}_R(R, A) \simeq A$ as R-modules. First, note that since R has identity we may define a map

$$\psi : \mathrm{Hom}_R(R, A) \to A \quad \text{by} \quad \phi \mapsto \phi(1)$$

We claim that ψ is an R-module isomorphism. Indeed, let $r \in R$ and $\phi_1, \phi_2 \in \mathrm{Hom}_R(R, A)$. Then by the definition of ψ and the definition of the action of R on $\mathrm{Hom}_R(R, A)$, we see

$$\begin{aligned}
\psi(r\phi_1 + \phi_2) &= (r\phi_1 + \phi_2)(1) \\
&= (r\phi_1)(1) + \phi_2(1) \\
&= \phi_1(1 \cdot r) + \phi_2(1) \\
&= \phi_1(r \cdot 1) + \phi_2(1) \\
&= r\phi_1(1) + \phi_2(1) \\
&= r\psi(\phi_1) + \psi(\phi_2)
\end{aligned}$$

which proves that ψ is an R-module homomorphism.

Next, we show that ψ is an injection. Since ψ is an R-module homomorphism, it suffices to prove that $\ker(\psi)$ is trivial to establish that ψ is an injection. Towards this

end, suppose that $\phi \in \ker(\psi)$. Then by the definition of ψ, we have $0 = \psi(\phi) = \phi(1)$. Now, let $r \in R$. Then since ϕ is an R-module homomorphism, we obtain

$$\phi(r) = \phi(r \cdot 1) = r\phi(1) = r \cdot 0 = 0$$

Since $r \in R$ was arbitrary, the above equality shows that ϕ is the zero map and as $\phi \in \ker(\psi)$ was arbitrary, this shows that $\ker(\psi)$ is trivial and hence ψ is an injection.

Finally, we show that ψ is a surjection. Towards this end, let $a \in A$. Define a map $\phi : R \to A$ by $\phi(1) = a$. Then it is easily verified that ϕ is an R-module homomorphism so that $\phi \in \mathrm{Hom}_R(R, A)$. Furthermore, by the definition of ψ we have

$$\psi(\phi) = \phi(1) = a$$

so that ψ is a surjection.

The above results show that $\psi : \mathrm{Hom}_R(R, A) \to A$ is an R-module isomorphism so that $\mathrm{Hom}_R(R, A) \simeq A$ as R-modules. This completes the proof. $\square$

Proposition. Let R be a ring with 1 and A an R-module. Then A can be embedded in an injective R-module.

Proof. Since A is a module, we have in particular that A is an additive abelian group and hence A is a $\mathbb{Z}$-module. Since any $\mathbb{Z}$-module can be embedded in an injective $\mathbb{Z}$-module, there exists an injective $\mathbb{Z}$-module J and an injective $\mathbb{Z}$-module homomorphism $f : A \to J$. Now, define a map

$$\overline{f} : \mathrm{Hom}_{\mathbb{Z}}(R, A) \to \mathrm{Hom}_{\mathbb{Z}}(R, J) \quad \text{by} \quad \phi \mapsto f \circ \phi$$

We claim that $\overline{f}$ is a well-defined injective group homomorphism.

First, note that if $\phi \in \mathrm{Hom}_{\mathbb{Z}}(R, A)$ then $f \circ \phi : R \to J$ and $f \circ \phi$ is a $\mathbb{Z}$-module homomorphism since the defined composition of $\mathbb{Z}$-module homomorphisms is a $\mathbb{Z}$-module homomorphism. This shows that $\overline{f}$ is well-defined. Next, let $\phi_1, \phi_2 \in \mathrm{Hom}_{\mathbb{Z}}(R, A)$ and $r \in R$. Then since f is a $\mathbb{Z}$-module homomorphism we have

$$\begin{aligned}
\left[\overline{f}(\phi_1 + \phi_2)\right](r) &= [f \circ (\phi_1 + \phi_2)](r) \\
&= f((\phi_1 + \phi_2)(r)) \\
&= f(\phi_1(r) + \phi_2(r)) \\
&= f(\phi_1(r)) + f(\phi_2(r)) \\
&= (f \circ \phi_1)(r) + (f \circ \phi_2)(r) \\
&= \overline{f}(\phi_1)(r) + \overline{f}(\phi_2)(r) \\
&= \left[\overline{f}(\phi_1) + \overline{f}(\phi_2)\right](r)
\end{aligned}$$

and thus $\overline{f}(\phi_1 + \phi_2) = \overline{f}(\phi_1) + \overline{f}(\phi_2)$ so that $\overline{f}$ is a group homomorphism. Finally, suppose that $\overline{f}(\phi_1) = \overline{f}(\phi_2)$ for some $\phi_1, \phi_2 \in \mathrm{Hom}_{\mathbb{Z}}(R, A)$ and let $r \in R$. By the definition of $\overline{f}$ we have since $\overline{f}(\phi_1)(r) = \overline{f}(\phi_2)(r)$ that $(f \circ \phi_1)(r) = (f \circ \phi_2)(r)$ so that $f(\phi_1(r)) = f(\phi_2(r))$. But since f is an injection, this gives that $\phi_1(r) = \phi_2(r)$ and since $r \in R$ was arbitrary, this proves that $\phi_1 = \phi_2$. Therefore, we have that $\overline{f}$ is an injection.

Next, we show that $\overline{f}$ is an R-module homomorphism. First, note that $\mathrm{Hom}_{\mathbb{Z}}(R, A)$ is an R-module with action defined by for $r, s \in R$ and $\phi \in \mathrm{Hom}_{\mathbb{Z}}(R, A)$ we have $(r\phi)(s) = \phi(sr)$. Similarly, note that $\mathrm{Hom}_{\mathbb{Z}}(R, J)$ is an R-module with action defined by for $r, s \in R$ and $\phi \in \mathrm{Hom}_{\mathbb{Z}}(R, J)$ we have $(r\phi)(s) = \phi(sr)$.

Now, recall that $\overline{f}$ is a group homomorphism. Finally, let $\phi \in \mathrm{Hom}_{\mathbb{Z}}(R, A)$ and let $r, s \in R$. Then we have

$$[\overline{f}(r\phi)](s) = [f \circ (r\phi)](s) = f((r\phi)(s)) = f(\phi(sr))$$

and

$$[r\overline{f}(\phi)](s) = \overline{f}(\phi)(sr) = (f \circ \phi)(sr) = f(\phi(sr))$$

and thus $\overline{f}(r\phi) = r\overline{f}(\phi)$. We conclude that $\overline{f}$ is an R-module homomorphism.

Recall that $A \simeq \mathrm{Hom}_R(R, A)$ as R-modules. Furthermore, it is clear that $\mathrm{Hom}_R(R, A)$ is an R-submodule of $\mathrm{Hom}_{\mathbb{Z}}(R, A)$. By the above results, then, it remains to prove that $\mathrm{Hom}_{\mathbb{Z}}(R, J)$ is an injective R-module to establish the main result.

Towards this end, let L be a left ideal of R and suppose that $g : L \to \mathrm{Hom}_{\mathbb{Z}}(R, J)$ is an R-module homomorphism. Define a map

$$h : L \to J \quad \text{by} \quad r \mapsto g(r)(1)$$

We claim that h is a $\mathbb{Z}$-module homomorphism. Since h is a map from an additive abelian group into an additive abelian group, it suffices to show that h is a group homomorphism to establish that h is a $\mathbb{Z}$-module homomorphism. Towards this end, let $r, s \in R$. Then since g is an R-module homomorphism, we have

$$h(r + s) = g(r + s)(1) = [g(r) + g(s)](1) = g(r)(1) + g(s)(1) = h(r) + h(s)$$

so that h is a $\mathbb{Z}$-module homomorphism. Hence, since L is an injective $\mathbb{Z}$-module it follows that h can be extended to a $\mathbb{Z}$-module homomorphism $t : R \to J$.

Now, define a map

$$\tau : R \to \mathrm{Hom}_{\mathbb{Z}}(R, J) \quad \text{by} \quad r \mapsto \tau(r) : R \to J \quad \text{by} \quad s \mapsto t(sr)$$

We claim that τ is an R-module homomorphism. First, we show that τ maps R into $\mathrm{Hom}_{\mathbb{Z}}(R, J)$. Let $r \in R$. In order to show that $\tau(r) \in \mathrm{Hom}_{\mathbb{Z}}(R, J)$, it suffices to show that $\tau(r) : R \to J$ is a group homomorphism by the previous reasoning. Let $s_1, s_2 \in R$. Then since t is a $\mathbb{Z}$-module homomorphism, we have

$$\tau(r)(s_1 + s_2) = t((s_1 + s_2)r) = t(s_1r + s_2r) = t(s_1r) + t(s_2r) = \tau(r)(s_1) + \tau(r)(s_2)$$

so that $\tau(r) \in \mathrm{Hom}_{\mathbb{Z}}(R, J)$. Next, let $r_1, r_2, s \in R$. Then since t is a $\mathbb{Z}$-module homomorphism, we have

$$\begin{aligned}
[\tau(r_1 + r_2)](s) &= t(s(r_1 + r_2)) \\
&= t(sr_1 + sr_2) \\
&= t(sr_1) + t(sr_2) \\
&= \tau(r_1)(s) + \tau(r_2)(s) \\
&= [\tau(r_1) + \tau(r_2)](s)
\end{aligned}$$

and thus $\tau(r_1 + r_2) = \tau(r_1) + \tau(r_2)$ so that τ is a group homomorphism. Finally, let $a, r, s \in R$. Then

$$[a\tau(r)](s) = \tau(r)(sa) = t(sar) = [\tau(ar)](s)$$

and thus $\tau(ar) = a\tau(r)$. Combining the previous results, we conclude that τ is an R-module homomorphism.

Finally, we show that τ extends g. Towards this end, let $r \in L$ and $s \in R$. Since L is a left ideal of R, we have that $sr \in L$. Therefore, since t extends h we have

$$\tau(r)(s) = t(sr) = h(sr)$$

and since g is an R-module homomorphism we have

$$g(r)(s) = g(r)(1 \cdot s) = [sg(r)](1) = g(sr)(1) = h(sr)$$

and thus $\tau(r) = g(r)$ so that τ extends g.

Combining the previous results, we conclude that $\mathrm{Hom}_{\mathbb{Z}}(R, J)$ is an injective R-module. Thus, the injective R-module homomorphism $\overline{f} : \mathrm{Hom}_{\mathbb{Z}}(R, A) \to \mathrm{Hom}_{\mathbb{Z}}(R, J)$ embeds the R-isomorphic copy $\mathrm{Hom}_R(R, A) \subseteq \mathrm{Hom}_{\mathbb{Z}}(R, A)$ of A into the injective R-module $\mathrm{Hom}_{\mathbb{Z}}(R, J)$. This completes the proof. $\square$

Theorem. Let R be a ring with 1 and

$$0 \longrightarrow A \xrightarrow{\phi} B \xrightarrow{\psi} C$$

be an exact sequence of R-modules and D be any R-module. Then

$$0 \longrightarrow \mathrm{Hom}_R(D, A) \xrightarrow{\overline{\phi}} \mathrm{Hom}_R(D, B) \xrightarrow{\overline{\psi}} \mathrm{Hom}_R(D, C)$$

is an exact sequence of abelian groups.

Proof. First note that $\mathrm{Hom}_R(D, A), \mathrm{Hom}_R(D, B)$, and $\mathrm{Hom}_R(D, C)$ are clearly abelian groups. Next, if $\alpha \in \mathrm{Hom}_R(D, A)$ and $\beta \in \mathrm{Hom}_R(D, B)$ then we define $\overline{\phi}(\alpha) = \phi \circ \alpha$ and $\overline{\psi}(\beta) = \psi \circ \beta$.

Now, we verify that $\overline{\phi}$ is a group homomorphism and remark that the proof that $\overline{\psi}$ is a group homomorphism is identical to the one we present below for $\overline{\phi}$. Towards this end, let $\alpha, \beta \in \mathrm{Hom}_R(D, A)$. Then since ϕ is an R-module homomorphism we have

$$\overline{\phi}(\alpha + \beta) = \phi \circ (\alpha + \beta) = (\phi \circ \alpha) + (\phi \circ \beta) = \overline{\phi}(\alpha) + \overline{\phi}(\beta)$$

so that $\overline{\phi}$ is a group homomorphism. Similarly, we see that $\overline{\psi}$ is a group homomorphism.

Next, we show that $\ker(\overline{\phi})$ is trivial. Towards this end, let $\alpha \in \ker(\overline{\phi})$. In this case, we have that $\overline{\phi}(\alpha) = \phi \circ \alpha : D \to B$ is the zero map so that for all $d \in D$ we have

$$0 = (\phi \circ \alpha)(d) = \phi(\alpha(d))$$

But since the above sequence is exact, it follows that ϕ is an injection and hence $\ker(\phi)$ is trivial. By the above equality, then, we obtain that $\alpha(d) = 0$ for all $d \in D$ which implies that $\alpha : D \to B$ is the zero map. We conclude that $\ker(\overline{\phi})$ is trivial.

Finally, we show that $\mathrm{Im}(\overline{\phi}) = \ker(\overline{\psi})$. First, let $\beta \in \mathrm{Im}(\overline{\phi})$. Then there is some $\alpha \in \mathrm{Hom}_R(D, A)$ such that $\overline{\phi}(\alpha) = \beta$ so that $\phi \circ \alpha = \beta$. Therefore, we obtain since the above sequence is exact that

$$\overline{\psi}(\beta) = \overline{\psi}(\phi \circ \alpha) = \psi \circ (\phi \circ \alpha) = (\psi \circ \phi) \circ \alpha = 0$$

The above equality proves that $\beta \in \ker(\overline{\psi})$. On the other hand, let $\beta \in \ker(\overline{\psi})$. Then

$$0 = \overline{\psi}(\beta) = \psi \circ \beta$$

and thus $\mathrm{Im}(\beta) \subseteq \ker(\psi) = \mathrm{Im}(\phi)$ since the above sequence is exact. Now, recall that ϕ is an injection as the above sequence is exact. In particular, this implies that $\phi : A \to \phi(A)$ is an R-module isomorphism. Therefore, since $\mathrm{Im}(\beta) \subseteq \mathrm{Im}(\phi)$ we see $\phi^{-1} \circ \beta : D \to A$ is a well-defined R-module homomorphism so that $\phi^{-1} \circ \beta \in \mathrm{Hom}_R(D, A)$. Therefore, we now have

$$\overline{\phi}(\phi^{-1} \circ \beta) = \phi \circ (\phi^{-1} \circ \beta) = (\phi \circ \phi^{-1}) \circ \beta = \beta$$

and thus $\beta \in \mathrm{Im}(\overline{\phi})$. Combining the previous results, we conclude that $\mathrm{Im}(\overline{\phi}) = \ker(\overline{\psi})$ so that the above sequence is an exact sequence of abelian groups. $\square$

Theorem. Let R be a ring with 1 and

$$A \xrightarrow{\phi} B \xrightarrow{\psi} C \longrightarrow 0$$

be an exact sequence of R-modules and D be any R-module. Then

$$0 \longrightarrow \mathrm{Hom}_R(C, D) \xrightarrow{\overline{\psi}} \mathrm{Hom}_R(B, D) \xrightarrow{\overline{\phi}} \mathrm{Hom}_R(A, D)$$

is an exact sequence of abelian groups.

Proof. First note that $\mathrm{Hom}_R(C, D), \mathrm{Hom}_R(B, D)$, and $\mathrm{Hom}_R(A, D)$ are clearly abelian groups. Next, if $\alpha \in \mathrm{Hom}_R(C, D)$ and $\beta \in \mathrm{Hom}_R(B, D)$ then we define $\overline{\psi}(\alpha) = \alpha \circ \psi$ and $\overline{\phi}(\beta) = \beta \circ \phi$.

Now, we verify that $\overline{\psi}$ is a group homomorphism and remark that the proof that $\overline{\phi}$ is a group homomorphism is identical to the one we present below for $\overline{\psi}$. Towards this end, let $\alpha, \beta \in \mathrm{Hom}_R(C, D)$. Then since we have

$$\overline{\psi}(\alpha + \beta) = (\alpha + \beta) \circ \psi = (\alpha \circ \psi) + (\beta \circ \psi) = \overline{\psi}(\alpha) + \overline{\psi}(\beta)$$

so that $\overline{\psi}$ is a group homomorphism. Similarly, we see that $\overline{\phi}$ is a group homomorphism.

Next, we show that $\ker(\overline{\psi})$ is trivial. Towards this end, let $\alpha \in \ker(\overline{\psi})$. In this case, we have that

$$0 = \overline{\psi}(\alpha) = \alpha \circ \psi$$

and hence as the above sequence is exact we now have $C = \mathrm{Im}(\psi) \subseteq \ker(\alpha)$. But note that $\alpha : C \to D$ and thus α is the zero map. We conclude that $\ker(\overline{\psi})$ is trivial.

Finally, we show that $\mathrm{Im}(\overline{\psi}) = \ker(\overline{\phi})$. First, let $\alpha \in \mathrm{Im}(\overline{\psi})$. Then there is some $\beta \in \mathrm{Hom}_R(C, D)$ such that $\overline{\psi}(\beta) = \alpha$ so that $\beta \circ \psi = \alpha$. Therefore, we obtain since the above sequence is exact that

$$\overline{\phi}(\alpha) = \overline{\phi}(\beta \circ \psi) = (\beta \circ \psi) \circ \phi = \beta \circ (\psi \circ \phi) = 0$$

On the other hand, let $\alpha \in \ker(\overline{\phi})$. Then

$$0 = \overline{\phi}(\alpha) = \alpha \circ \phi$$

and thus we obtain since the above sequence is exact that

$$\ker(\psi) = \operatorname{Im}(\phi) \subseteq \ker(\alpha)$$

so that $\ker(\psi) \subseteq \ker(\alpha)$. This observation implies that there exists an R-module homomorphism $\beta : B/\ker(\psi) \to D$ defined by $\beta(b + \ker(\psi)) = \alpha(b)$ for all $b + \ker(\psi) \in B/\ker(\psi)$. Now, as the above row is exact we have that ψ is a surjection and hence by the First Isomorphism Theorem for Modules we obtain an R-module isomorphism $\gamma : B/\ker(\psi) \to C$ defined by $\gamma(b + \ker(\psi)) = \psi(b)$ for all $b + \ker(\psi) \in B/\ker(\psi)$. Therefore, we see $\beta \circ \gamma^{-1} : C \to D$ is a well-defined R-module homomorphism so that $\beta \circ \gamma^{-1} \in \operatorname{Hom}_R(C, D)$. Therefore, we now have by the definition of γ^{-1} that

$$\overline{\psi}(\beta \circ \gamma^{-1}) = (\beta \circ \gamma^{-1}) \circ \psi = \beta \circ (\gamma^{-1} \circ \psi) = \beta$$

thus $\beta \in \operatorname{Im}(\overline{\psi})$. Combining the previous results, we conclude that $\operatorname{Im}(\overline{\psi}) = \ker(\overline{\phi})$ so that the above sequence is an exact sequence of abelian groups. $\square$

Example. Consider the short exact sequence of $\mathbb{Z}$-modules

$$0 \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow \mathbb{Z}/4\mathbb{Z} \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow 0$$

where the map $\mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/4\mathbb{Z}$ is inclusion and the map $\mathbb{Z}/4\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$ is projection. In particular, by Theorem 1 above we see by taking $D = \mathbb{Z}/2\mathbb{Z}$ that

$$0 \longrightarrow \operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z}) \longrightarrow \operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/4\mathbb{Z}) \longrightarrow \operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z})$$

is an exact sequence of abelian groups. We remark that all of the above Homs are of order 2.

Proof. That the first and last Homs are of order 2 is immediate. That the middle Hom is of order 2 follows from the fact that a nonzero $\mathbb{Z}$-module homomorphism $\mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/4\mathbb{Z}$ must map the nonidentity element of $\mathbb{Z}/2\mathbb{Z}$ to the unique element of order 2 in $\mathbb{Z}/4\mathbb{Z}$ by order considerations. This completes the proof. $\square$

Definition. Let R be a ring with 1 and let A be a left R-module. Define $A^* = \operatorname{Hom}_R(A, R)$. Then A^* is a right R-module by for $\phi \in A^*$, $r \in R$, and $a \in A$ we have $(\phi r)(a) = \phi(a)r$. We call A^* the ***dual module*** of A.

Proof. We clearly have that A^* is an abelian group under addition. To see that we have a right action of R on A^*, let $\phi \in A^*$, $r \in R$, $s \in R$, and $a_1, a_2 \in A$. Then since ϕ is a

left R-module homomorphism, we have

$$\begin{aligned}(\phi r)(sa_1 + a_2) &= \phi(sa_1 + a_2)r \\ &= [\phi(sa_1) + \phi(a_2)]r \\ &= [s\phi(a_1) + \phi(a_2)]r \\ &= s\phi(a_1)r + \phi(a_2)r \\ &= s(\phi r)(a_1) + (\phi r)(a_2)\end{aligned}$$

and thus $\phi r \in A^*$ so that we have a right action of R on A^*.

Next, suppose that $\phi_1, \phi_2 \in A^*$, $r \in R$, and $a \in A$. Then

$$\begin{aligned}[(\phi_1 + \phi_2)r]\,(a) &= (\phi_1 + \phi_2)(a)r \\ &= [\phi_1(a) + \phi_2(a)]r \\ &= \phi_1(a)r + \phi_2(a)r \\ &= (\phi_1 r)(a) + (\phi_2 r)(a) \\ &= [\phi_1 r + \phi_2 r](a)\end{aligned}$$

and thus $(\phi_1 + \phi_2)r = \phi_1 r + \phi_2 r$. Next, let $\phi \in A^*$, $r, s \in R$, and $a \in A$. Then

$$\begin{aligned}[\phi(r + s)]\,(a) &= \phi(a)(r + s) \\ &= \phi(a)r + \phi(a)s \\ &= (\phi r)(a) + (\phi s)(a) \\ &= [\phi r + \phi s](a)\end{aligned}$$

and thus $\phi(r + s) = \phi r + \phi s$. Finally, let $\phi \in A$, $r, s \in R$, and $a \in A$. Then

$$[(\phi r)s]\,(a) = (\phi r)(a)s = \phi(a)rs = [\phi(rs)](a)$$

and thus $(\phi r)s = \phi(rs)$. We conclude that A^* is a right R-module. □

Remark. If R is commutative, then A and A^* are R-modules.

Proof. This is immediate, since we assume that A is a left R-module (hence an R-module since R is commutative) and since we have that A^* is a right R-module (hence an R-module since R is commutative). □

Remark. Let A and B be left R-modules and suppose that $\phi : A \to B$ is a left R-module homomorphism. Then the map $\phi^* : B^* \to A^*$ defined by $\phi^*(\psi) = \psi \circ \phi$ for all $\psi \in B^*$ is a right R-module homomorphism.

Proof. To see that ϕ^* is well-defined, note that if $\psi \in B^*$ that $\phi^*(\psi) = \psi \circ \phi : A \to R$ and $\psi \circ \phi$ is a left R-module homomorphism since the defined composition of left R-module homomorphisms is a left R-module homomorphism. Thus, the map ϕ^* is well-defined.

To see that ϕ^* is a right R-module homomorphism, let $\psi_1, \psi_2 \in \mathrm{Hom}_R(B, R)$, $r \in R$, and $a \in A$. Then

$$\begin{aligned}
[\phi^*(\psi_1 r + \psi_2)]\,(a) &= [(\psi_1 r + \psi_2) \circ \phi](a) \\
&= [\psi_1 r + \psi_2](\phi(a)) \\
&= (\psi_1 r)(\phi(a)) + \psi_2(\phi(a)) \\
&= \psi_1(\phi(a))r + \psi_2(\phi(a)) \\
&= (\psi_1 \circ \phi)(a)r + (\psi_2 \circ \phi)(a) \\
&= \phi^*(\psi_1)(a)r + \phi^*(\psi_2)(a) \\
&= [\phi^*(\psi_1)r](a) + \phi^*(\psi_2)(a) \\
&= [\phi^*(\psi_1)r + \phi^*(\psi_2)](a)
\end{aligned}$$

and thus $\phi^*(\psi_1 r + \psi_2) = \phi^*(\psi_1)r + \phi^*(\psi_2)$. We may now conclude that ϕ^* is indeed a right R-module homomorphism. $\square$

Notation. For $a \in A$ and $f \in A^*$, we write $\langle a, f \rangle = f(a)$.

Theorem. Let R be a ring with 1 and let A be a free left R-module of finite rank n. Then A^* is a free right R-module of rank n.

Proof. Let $X \subseteq A$ be a basis for A over R and define the dual basis $X^* \subseteq A^*$ as follows. Let $X^* = \{f_x : x \in X\}$, where $f_x : A \to R$ is defined by for $y \in X$ we have

$$f_x(y) = \delta_{x,y} 1 = \begin{cases} 1 & \text{if } x = y \\ 0 & \text{if } x \neq y \end{cases}$$

We remark that by the definition of f_x we have $f_x \in A^*$ for each $x \in X$.

Next, we show that X^* as defined in the previous lecture is linearly independent. Towards this end, assume that $\sum_{x \in X} f_x r_x = 0$ for some $r_x \in R$. Let $y \in X$. Then we have by the definition of the action of R on A^* that

$$0 = 0(y) = \left(\sum_{x \in X} f_x r_x \right)(y) = \sum_{x \in X} (f_x r_x)(y) = \sum_{x \in X} f_x(y) r_x = f_y(y) r_y = 1 \cdot r_y = r_y$$

Thus, since $y \in X$ was arbitrary we conclude that $r_x = 0$ for each $x \in X$ so that X^* is linearly independent.

Finally, we show that X^* spans A^*. Towards this end, let $f \in A^*$. Then f is a map $f : A \to R$ and so $f(x) \in R$ for each $x \in X \subseteq A$. Therefore, we have

$$\sum_{x \in X} f_x f(x) \in \mathrm{span}\{f_x : x \in X\} = \mathrm{span} X^*$$

Furthermore, suppose that $y \in X$. Then we have by the definition of the action of R on A^* that

$$\left(\sum_{x \in X} f_x f(x) \right)(y) = \sum_{x \in X} (f_x f(x))(y) = \sum_{x \in X} f_x(y) f(x) = f_y(y) f(y) = 1 \cdot f(y) = f(y)$$

Thus, since $y \in X$ was arbitrary and since X is a basis for A it now follows that

$$f = \sum_{x \in X} f_x f(x) \in \text{span} X^*$$

Since $f \in A^*$ was arbitrary, we conclude that X^* spans A^*. Combining the previous two results, we conclude that X^* is a basis for A^*. $\square$

Theorem. Let R be a nonzero ring with 1. Let A be a left R-module. For each $a \in A$, define $\theta(a) : A^* \to R$ by for $f \in A^*$ we have $\theta(a)(f) = f(a)$. Then $\theta : A \to A^{**}$ is a left R-module homomorphism. If A is a free left R-module of finite rank, then θ is an isomorphism.

Proof. First, we show that θ is well-defined. Towards this end, let $a \in A$ and $f \in A^*$. Since $f \in A^*$ we know that $f : A \to R$ and hence $\theta(a)(f) = f(a) \in R$ so that indeed $\theta(a) : A^* \to R$. Now, we show that $\theta(a) : A^* \to R$ is a right R-module homomorphism. Towards this end, let $f_1, f_2 \in A^*$. Then

$$\theta(a)(f_1 + f_2) = (f_1 + f_2)(a) = f_1(a) + f_2(a) = \theta(a)(f_1) + \theta(a)(f_2)$$

so that $\theta(a)$ is a group homomorphism. Furthermore, if $f \in A^*$ and $r \in R$ then we have by the definition of the action of R on A^* that

$$\theta(a)(fr) = (fr)(a) = f(a)r = \theta(a)(f)r$$

so that $\theta(a)$ is a right R-module homomorphism. By the previous results, we may now conclude that $\theta(a) \in \text{Hom}_R(A^*, R) = A^{**}$ and thus $\theta : A \to A^{**}$ is a well-defined.

Now, let $a_1, a_2 \in A$ and $f \in A^*$. As f is a left R-module homomorphism, we see

$$\theta(a_1 + a_2)(f) = f(a_1 + a_2) = f(a_1) + f(a_2) = \theta(a_1)(f) + \theta(a_2)(f) = [\theta(a_1) + \theta(a_2)](f)$$

and thus $\theta(a_1 + a_2) = \theta(a_1) + \theta(a_2)$ so that θ is a group homomorphism. Finally, let $a \in A$, $r \in R$, and $f \in A^*$. Then since f is a left R-module homomorphism, we obtain

$$[\theta(ra)(f)] = f(ra) = rf(a) = r\theta(a)(f) = [r\theta(a)](f)$$

and thus $\theta(ra) = r\theta(a)$ so that θ is a left R-module homomorphism.

We now prove the second statement in the above Theorem. First, note that by the above results we need only show that $\theta : A \to A^{**}$ is a bijection assuming the hypothesis that A is a free left R-module of finite rank. Towards this end, suppose that A is a free left R-module of finite rank. Then we know that A^* is a free right R-module of finite rank with basis X^* as defined above. By the same reasoning, we know that A^{**} is a free left R-module of finite rank with basis X^{**}. For definiteness, we remark that these bases are defined by

$$X^* = \{f_x : x \in X\} \subseteq A^* \quad \text{where} \quad f_x : A \to R \quad \text{is given by} \quad f_x(y) = \delta_{x,y} 1$$

and

$$X^{**} = \{g_x : x \in X\} \subseteq A^{**} \quad \text{where} \quad g_x : A^* \to R \quad \text{is given by} \quad g_x(f_y) = \delta_{x,y} 1$$

We will use these observations to show that θ is a surjection.

Towards this end, let $x \in X$. Then we have that $\theta(x) : A^* \to R$ and for each $f_y \in X^*$ we have

$$\theta(x)(f_y) = f_y(x) = \delta_{x,y}1 = g_x(f_y)$$

Since the above equality holds for each element f_y in the basis X^* for A^*, it now follows that $\theta(x) = g_x$ for each $x \in X$. Therefore, we have $\mathrm{Im}(\theta) \supseteq \{g_x : x \in X\} = X^{**}$ and since X^{**} is a basis for A^{**} it now follows that $\theta : A \to A^{**}$ is surjective.

Finally, we show that θ is an injection. Since θ is a left R-module homomorphism, it suffices to show that $\ker\theta$ is trivial to establish that θ is an injection. Towards this end, let $a \in \ker\theta$ so that $\theta(a) : A^* \to R$ is the zero map. Since $a \in A$ and as X is a basis for A over R, it follows that we can write $a = \sum_{x\in X} r_x x$ for some $r_x \in R$.

Now, let $f_y \in X^*$. Then since $\theta(a) : A^* \to R$ is the zero map and as f_y is a left R-module homomorphism, we obtain

$$\begin{aligned}
0 = \theta(a)(f_y) &= f_y(a) \\
&= f_y\left(\sum_{x\in X} r_x x\right) \\
&= \sum_{x\in X} f_y(r_x x) \\
&= \sum_{x\in X} r_x f_y(x) \\
&= f_y(y) r_y \\
&= 1 \cdot r_y \\
&= r_y
\end{aligned}$$

Since $f_y \in X^*$ was arbitrary, it now follows that $r_x = 0$ for each $x \in X$ so that

$$a = \sum_{x\in X} r_x x = \sum_{x\in X} 0x = 0$$

and hence $\ker\theta$ is trivial so that θ is an injection. Combining the previous results, we have that θ is a left R-module isomorphism. This completes the proof. $\square$

Topic 4: Tensor Products

Definition. Let R be a nonzero ring with 1. Let A be a right R-module and B be a left R-module. A map $f : A \times B \to C$ is called a ***middle linear map*** if C is an abelian group and

$$f(a_1 + a_2, b) = f(a_1, b) + f(a_2, b)$$

and

$$f(a, b_1 + b_2) = f(a, b_1) + f(a, b_2)$$

and

$$f(ar, b) = f(a, rb)$$

for all $a, a_1, a_2 \in A$, $b, b_1, b_2 \in B$, and $r \in R$.

We denote the ***category of middle linear maps*** by $\mathcal{M}(A, B)$ whose objects are middle linear maps with domain $A \times B$ and the morphisms from $f_1 : A \times B \to C$ to $f_2 : A \times B \to D$ are the group homomorphisms $g : C \to D$ such that $g \circ f_1 = f_2$.

Remark. From the above, we have that $\mathcal{M}(A, B)$ is indeed a category.

Proof. This is easy but tedious to check. We will not prove this here. □

Definition. Let $\mathcal{C}$ be a category. An object I of $\mathcal{C}$ is said to be a ***universal object*** of $\mathcal{C}$ if for each object C of $\mathcal{C}$ there exists a unique morphism $I \to C$ of $\mathcal{C}$.

Definition. Let R be a nonzero ring with 1. Let A be a left R-module and B be a right R-module. The ***tensor product*** of A and B is a universal object of $\mathcal{M}(A, B)$. We denote the abelian group that is the target space of the tensor product of A and B by $A \otimes_R B$ and we denote the image of $(a, b) \in A \times B$ under the tensor product by $a \otimes_R b$. In other words, we have $(a, b) \mapsto a \otimes_R b$ under the tensor product.

Remark. When we say (C, α) is an object of $\mathcal{M}(A, B)$, we mean that C is an abelian group and $\alpha : A \times B \to C$ is a middle linear map.

Remark. It can be helpful to think of the tensor product of A and B as follows. Suppose that $g : A \times B \to A \otimes_R B$ is the tensor product of A and B. Since g is a universal object of $\mathcal{M}(A, B)$, it follows that given any object f of $\mathcal{M}(A, B)$ there exists a unique morphism $\phi : g \to f$ of $\mathcal{M}(A, B)$. That is, given any middle linear map $f : A \times B \to C$ where C is an abelian group there exists a unique group homomorphism $\phi : A \otimes_R B \to C$ such that $\phi \circ g = f$.

Theorem. With the same assumptions from the previous lecture, the tensor product always exists.

Proof. Let F be the free abelian group on the set $A \times B$ and let S be the subgroup of F generated by the elements

$$(a_1 + a_2, b) - (a_1, b) - (a_2, b) \in F \quad (a, b_1 + b_2) - (a, b_1) - (a, b_2) \in F \quad (ar, b) - (a, rb) \in F$$

for all $a, a_1, a_2 \in A$, $b, b_1, b_2 \in B$, and $r \in R$. Since F is abelian, we may define the abelian group $C = F/S$. Now, define a map

$$\beta : A \times B \to C \quad \text{by} \quad (a, b) \mapsto (a, b) + S$$

By the definition of C, it is easily verified that β is a well-defined middle linear map. Therefore, we have that (C, β) is an object of $\mathcal{M}(A, B)$.

We claim that (C, β) is a universal object of $\mathcal{M}(A, B)$. Towards this end, suppose that (D, γ) is any object of $\mathcal{M}(A, B)$. We must show that there is a unique group homomorphism $\overline{\phi} : C \to D$ such that $\overline{\phi} \circ \beta = \gamma$. First, note that $\gamma : A \times B \to D$ is a map of sets and that D is an abelian group. Therefore, since F is the free abelian group on the set $A \times B$ it now follows that there exists a (unique) group homomorphism $\phi : F \to D$ such that $\phi(a, b) = \gamma(a, b)$ for all $(a, b) \in A \times B$.

Now, we claim that $S \subseteq \ker \phi$. Note that in order to establish this claim, we need only show that the generators of S are in $\ker \phi$. Indeed, notice that since γ is an object of $\mathcal{M}(A, B)$ that γ is a middle linear map. Furthermore, recall that ϕ is a group homomorphism. Thus, by the previous two observations and since $\phi(a, b) = \gamma(a, b)$ for all $(a, b) \in A \times B$ we obtain

$$\begin{aligned}
\phi((a_1 + a_2, b) - (a_1, b) - (a_2, b)) &= \phi(a_1 + a_2, b) - \phi(a_1, b) - \phi(a_2, b) \\
&= \gamma(a_1 + a_2, b) - \gamma(a_1, b) - \gamma(a_2, b) \\
&= [\gamma(a_1, b) + \gamma(a_2, b)] - \gamma(a_1, b) - \gamma(a_2, b) \\
&= 0
\end{aligned}$$

for all $a_1, a_2 \in A$ and $b \in B$. Similarly, we obtain that the other two types of generators of S are also in $\ker \phi$. Thus, we have $S \subseteq \ker \phi$.

Next, note that as $S \subseteq \ker \phi$ that there is a group homomorphism $\overline{\phi} : F/S \to D$ such that $\overline{\phi}((a, b) + S) = \phi(a, b)$ for all $(a, b) \in A \times B$. But since $C = F/S$ and as $\phi(a, b) = \gamma(a, b)$ for all $(a, b) \in A \times B$, we now have that $\overline{\phi} : C \to D$ is a group homomorphism such that $\overline{\phi}((a, b) + S) = \gamma(a, b)$ for all $(a, b) \in A \times B$. Furthermore, suppose that $(a, b) \in A \times B$. Then

$$\overline{\phi}(\beta(a, b)) = \overline{\phi}((a, b) + S) = \gamma(a, b)$$

and thus $\overline{\phi} \circ \beta = \gamma$.

Finally, we show that $\overline{\phi}$ is unique. Towards this end, suppose that $\overline{\psi} : C \to D$ is a group homomorphism such that $\overline{\psi} \circ \beta = \gamma$. In order to show that $\overline{\psi} = \overline{\phi}$, it suffices to show that $\overline{\psi}((a, b) + S) = \overline{\phi}((a, b) + S)$ for all $(a, b) \in A \times B$ since F is the free abelian group on the set $A \times B$. Indeed, suppose that $(a, b) \in A \times B$. Then we have

$$\overline{\psi}((a, b) + S) = \overline{\psi}(\beta(a, b)) = \gamma(a, b) = \phi(a, b) = \overline{\phi}((a, b) + S)$$

Therefore, we conclude that $\overline{\psi} = \overline{\phi}$ and hence $\overline{\phi}$ is unique.

The above results prove that (C, β) is a universal object in $\mathcal{M}(A, B)$. By the definition of the tensor product, then, we conclude that the tensor product always exists. This completes the proof. $\square$

Definition. Let R be a ring with 1. Let A, A' be right R-modules and B, B' be left R-modules. Let $f : A \to A'$ and $g : B \to B'$ be right and left R-module homomorphisms, respectively. Then there is a unique group homomorphism $f \otimes_R g : A \otimes_R B \to A' \otimes_R B'$ such that $(f \otimes_R g)(a \otimes_R b) = f(a) \otimes_R g(b)$ for all $a \in A$ and $b \in B$. The map $f \otimes_R g$ is called the ***tensor product*** of f and g.

Proof. Define a map

$$\mu : A \times B \to A' \otimes_R B' \quad \text{by} \quad (a, b) \mapsto f(a) \otimes_R g(b)$$

Clearly, we see that μ is well-defined. We also claim that μ is a middle linear map. We will verify the first of the three middle linear map axioms and remark that the remaining two are as easily proven as the first. Indeed, suppose that $a_1, a_2 \in A$ and $b \in B$. Then since f is a right R-module homomorphism, we obtain

$$\begin{aligned}
\mu(a_1 + a_2, b) &= f(a_1 + a_2) \otimes_R g(b) \\
&= [f(a_1) + f(a_2)] \otimes_R g(b) \\
&= [f(a_1) \otimes_R g(b)] + [f(a_2) \otimes_R g(b)] \\
&= \mu(a_1, b) + \mu(a_2, b)
\end{aligned}$$

Similarly, the remaining two middle linear map axioms are proven by relying on the fact that f is a right R-module homomorphism and g is a left R-module homomorphism.

The above results show that $(A' \otimes_R B', \mu)$ is an object of $\mathcal{M}(A, B)$. Therefore, by the definition of the tensor product there exists a unique group homomorphism $f \otimes_R g : A \otimes_R B \to A' \otimes_R B'$ such that $(f \otimes_R g)(a \otimes_R b) = \mu(a, b) = f(a) \otimes_R g(b)$ for all $a \in A$ and $b \in B$. This completes the proof. □

Definition. Let R and S be rings with 1. Then an R, S***-bimodule*** is an abelian group A with a left R-module structure and a right S-module structure such that $(ra)s = r(as)$ for all $a \in A$, $r \in R$, and $s \in S$.

Remark. If R is commutative, then every R-module can be viewed as an R, R-bimodule.

Proof. This is immediate. □

Theorem. Let A be an S, R-bimodule and let B be a left R-module. Then $A \otimes_R B$ is a left S-module.

Proof. By definition, we have that $A \otimes_R B$ is an abelian group under addition. We now define a left S-module structure on $A \otimes_R B$. Towards this end, let $s \in S$ and define a map

$$\mu : A \times B \to A \otimes_R B \quad \text{by} \quad (a, b) \mapsto (sa) \otimes_R b$$

Since A is an S, R-bimodule, we see that μ is well-defined. We claim that μ is a middle linear map. Similarly as with the above, we will verify the third of the middle linear map

axioms and remark that the remaining two are as easily proven as the third. Indeed, suppose that $a \in A$, $b \in B$, and $r \in R$. Then since A is an S, R-bimodule, we have

$$\mu(ar, b) = (s(ar)) \otimes_R b = ((sa)r) \otimes_R b = (sa) \otimes_R rb = \mu(a, rb)$$

Similarly, the remaining two middle linear map axioms are proven by relying on the fact that A is an S, R-bimodule.

The above results show that $(\mu, A \otimes_R B)$ is an object of $\mathcal{M}(A, B)$. Therefore, by the definition of the tensor product there exists a (unique) group homomorphism $s\cdot : A \otimes_R B \to A \otimes_R B$ such that $s \cdot (a \otimes_R b) = \mu(a, b) = (sa) \otimes_R b$ for all $a \in A$ and $b \in B$. Since $s \in S$ was arbitrary, we may now conclude that for any $s \in S$ we obtain a (unique) group homomorphism $s\cdot : A \otimes_R B \to A \otimes_R B$ such that $s \cdot (a \otimes_R b) = (sa) \otimes_R b$ for all $a \in A$ and $b \in B$.

We claim that the above results provide a left S-module structure on $A \otimes_R B$. Indeed, suppose that $s \in S$ and $u \in A \otimes_R B$. By the above, there is a (unique) group homomorphism $s\cdot : A \otimes_R B \to A \otimes_R B$ such that $s \cdot (a \otimes_R b) = (sa) \otimes_R b$ for all $a \in A$ and $b \in B$. Furthermore, since $u \in A \otimes_R B$ we can write $u = \sum_{i=1}^n a_i \otimes_R b_i$ for some $a_1, \ldots, a_n \in A$ and $b_1, \ldots, b_n \in B$. Now, define $s \cdot u$ to be the element

$$s \cdot u = \sum_{i=1}^n s \cdot (a_i \otimes_R b_i) \in A \otimes_R B$$

We now show that this action is well-defined. Towards this end, suppose that

$$\sum_{i=1}^n a_i \otimes_R b_i = u = \sum_{i=1}^m c_i \otimes_R d_i$$

for some $c_1, \ldots, c_m \in A$ and $d_1, \ldots, d_m \in B$. Then since $s\cdot$ is a group homomorphism, we obtain

$$\begin{aligned} 0 = 0 \otimes_R 0 = (s0) \otimes_r 0 &= s \cdot (0 \otimes_R 0) \\ &= s \cdot \left(\sum_{i=1}^n a_i \otimes_R b_i - \sum_{i=1}^m c_i \otimes_R d_i \right) \\ &= s \cdot \sum_{i=1}^n a_i \otimes_R b_i - s \cdot \sum_{i=1}^m c_i \otimes_R d_i \end{aligned}$$

and hence

$$s \cdot \sum_{i=1}^n a_i \otimes_R b_i = s \cdot \sum_{i=1}^m c_i \otimes_R d_i$$

which shows that the action of s on u is well-defined. Since $s \in S$ and $u \in A \otimes_R B$ were arbitrary, it now follows that we have a well-defined left action of S on $A \otimes_R B$.

Finally, we prove that the above left action of S on $A \otimes_R B$ satisfies the three left module axioms by relying on the existence of the above (unique) group homomorphism for each $s \in S$. We will prove the first two of these three axioms and remark that the

remaining one is similarly-proven. First, let $u_1, u_2 \in A \otimes_R B$ and $s \in S$. Then since $s\cdot$ is a group homomorphism, we have

$$s \cdot (u_1 + u_2) = s \cdot u_1 + s \cdot u_2$$

Next, let $u \in A \otimes_R B$ and write $u = \sum_{i=1}^n a_i \otimes_R b_i$ for some $a_1, \dots, a_n \in A$ and $b_1, \dots b_n \in B$ and let $s_1, s_2 \in S$ and write $s = s_1 + s_2 \in S$. Then since $s\cdot, s_1\cdot$, and $s_2\cdot$ are group homomorphisms, by the properties of $s\cdot, s_1\cdot$, and $s_2\cdot$, and since A is an S, R-bimodule, we have

$$\begin{aligned}
(s_1 + s_2) \cdot u &= s \cdot \sum_{i=1}^n a_i \otimes_R b_i \\
&= \sum_{i=1}^n s \cdot (a_i \otimes_R b_i) \\
&= \sum_{i=1}^n (sa_i) \otimes_R b_i \\
&= \sum_{i=1}^n [(s_1 + s_2)a_i] \otimes_R b_i \\
&= \sum_{i=1}^n (s_1 a_i + s_2 a_i) \otimes_R b_i \\
&= \sum_{i=1}^n [((s_1 a_i) \otimes_R b_i) + ((s_2 a_i) \otimes_R b_i)] \\
&= \sum_{i=1}^n (s_1 a_i) \otimes_R b_i + \sum_{i=1}^n (s_2 a_i) \otimes_R b_i \\
&= \sum_{i=1}^n s_1 \cdot (a_i \otimes_R b_i) + \sum_{i=1}^n s_2 \cdot (a_i \otimes_R b_i) \\
&= s_1 \cdot \sum_{i=1}^n a_i \otimes_R b_i + s_2 \cdot \sum_{i=1}^n a_i \otimes_R b_i \\
&= s_1 \cdot u + s_2 \cdot u
\end{aligned}$$

As has been mentioned previously, the remaining left module axiom is similarly-proven as the above. This completes the proof that $A \otimes_R B$ is a left S-module. □

Example. Let F be a field and suppose that V and W are vector spaces over F. Then $V \otimes_F W$ is a vector space over F. Furthermore, we have that $\dim_F(V \otimes_F W) = \dim_F(V) \cdot \dim_F(W)$.

Proof. Note that since F is a field and as V and W are vector spaces over F that V and W are both F, F-bimodules. Therefore, it now follows that $V \otimes_F W$ is an F-module and hence $V \otimes_F W$ is a vector space over F since F is a field. We now prove the second

statement. Towards this end, let $(v_i)_{i\in I} \subseteq V$ and $(w_j)_{j\in J} \subseteq W$ be bases over F for V and W, respectively. We claim that $(v_i \otimes_F w_j)_{(i,j)\in I\times J}$ is a basis for $V \otimes_F W$ over F.

First, we show that $(v_i \otimes_F w_j)_{(i,j)\in I\times J}$ spans $V \otimes_F W$. Towards this end, let $v \in V$ and $w \in W$ and consider $v \otimes_F w$. Since $v \in V$ and $(v_i)_{i\in I}$ is a basis for V over F, we have that $v = \sum_{i\in I} f_i v_i$ for some $(f_i)_{i\in I} \subseteq F$ with only finitely many of these elements of F not equal to 0. Similarly, since $w \in W$ and $(w_j)_{j\in J}$ is a basis for W over F, we have that $w = \sum_{j\in J} f_j w_j$ for some $(f_j)_{j\in J} \subseteq F$ with only finitely many of these elements of F not equal to 0. Now, let $g : V \times W \to V \otimes_F W$ be the tensor product. In particular, since F is a field we know that g is an F-bilinear map. Thus, we obtain

$$\begin{aligned}
v \otimes_F w &= g(v, w) \\
&= g\left(\sum_{i\in I} f_i v_i, \sum_{j\in J} f_j w_j\right) \\
&= \sum_{i\in I} g\left(f_i v_i, \sum_{j\in J} f_j w_j\right) \\
&= \sum_{i\in I}\sum_{j\in J} g(f_i v_i, f_j w_j) \\
&= \sum_{i\in I}\sum_{j\in J} f_i g(v_i, f_j w_i) \\
&= \sum_{i\in I}\sum_{j\in J} f_i f_j g(v_i, w_i) \\
&= \sum_{(i,j)\in I\times J} [f_i f_j g(v_i, w_j)] \\
&= \sum_{(i,j)\in I\times J} [f_i f_j (v_i \otimes w_j)]
\end{aligned}$$

which shows that any elementary tensor in $V \otimes_F W$ is an F-linear combination of elements from $(v_i \otimes_F w_j)_{(i,j)\in I\times J}$. Hence, since every element of $V \otimes_F W$ is a finite sum of elementary tensors from $V \otimes_F W$ it now follows that $(v_i \otimes_F w_j)_{(i,j)\in I\times J}$ spans $V \otimes_F W$.

Next, we show that $(v_i \otimes_F w_j)_{(i,j)\in I\times J}$ is linearly independent. Towards this end, suppose that

$$\sum_{(i,j)\in I\times J} [f_{ij}(v_i \otimes_F w_j)] = 0$$

for some $(f_{ij})_{(i,j)\in I\times J} \subseteq F$ with only finitely many of these elements of F not equal to 0. Now, let $(\alpha_k)_{k\in I}$ and $(\beta_l)_{l\in J}$ be the maps $V \to F$ and $W \to F$, respectively, defined by

$$\alpha_k(v_i) = \delta_{k,i}1 \quad \beta_l(w_j) = \delta_{l,j}1$$

for all $i, k \in I$ and $j, l \in J$. Clearly, we have that $\alpha_k : V \to F$ and $\beta_l : W \to F$ are F-linear transformations for each $k \in I$ and $l \in J$. Therefore, there exists a (unique)

F-linear transformation

$$(\alpha_k \otimes_F \beta_l) : V \otimes_F W \to F \otimes_F F \quad \text{such that} \quad (\alpha_k \otimes_F \beta_l)(v \otimes_F w) = \alpha_k(v) \otimes_F \beta_l(w)$$

for all $k \in I$, $l \in J$, $v \in V$, and $w \in W$. Fixing any $k \in I$ and $l \in J$, we obtain since $\alpha_k \otimes_F \beta_l$ is an F-linear transformation that

$$\begin{aligned}
0 &= (\alpha_k \otimes_F \beta_l)(0) \\
&= (\alpha_k \otimes_F \beta_l)\left(\sum_{(i,j)\in I\times J} [f_{ij}(v_i \otimes_F w_j)]\right) \\
&= \sum_{(i,j)\in I\times J} [(\alpha_k \otimes_F \beta_l)(f_{ij}(v_i \otimes_F w_j))] \\
&= \sum_{(i,j)\in I\times J} [f_{ij}(\alpha_k \otimes_F \beta_l)(v_i \otimes_F w_j)] \\
&= \sum_{(i,j)\in I\times J} [f_{ij}(\alpha_k(v_i) \otimes_F \beta_l(w_j))] \\
&= f_{kl}(\alpha_k(v_k) \otimes_F \beta_l(w_l)) \\
&= f_{kl}(1 \otimes_F 1) \\
&= f_{kl}
\end{aligned}$$

Therefore, since $k \in I$ and $l \in J$ were arbitrary, we conclude that $f_{ij} = 0$ for all $(i,j) \in I \times J$ and hence $(v_i \otimes_F w_j)_{(i,j)\in I\times J}$ is linearly independent. By the previous two results, we may now conclude that $(v_i \otimes_F w_j)_{(i,j)\in I\times J}$ is a basis for $V \otimes_F W$ over F.

Finally, note that since $(v_i \otimes_F w_j)_{(i,j)\in I\times J}$ is a linearly independent set that each element of $(v_i \otimes_F w_j)_{(i,j)\in I\times J}$ is necessarily distinct. Therefore, since $(v_i \otimes_F w_j)_{(i,j)\in I\times J}$ is a basis for $V \otimes_F W$ over F we may now conclude that

$$\begin{aligned}
\dim_F(V \otimes_F W) &= |(v_i \otimes_F w_j)_{(i,j)\in I\times J}| \\
&= |I| \cdot |J| \\
&= |(v_i)_{i\in I}| \cdot |(w_j)_{j\in J}| \\
&= \dim_F(V) \cdot \dim_F(W)
\end{aligned}$$

This completes the proof. □

Example. We have $\mathbb{Z}_2 \otimes \mathbb{Z}_2 \simeq \mathbb{Z}_2$ and $\mathbb{Z}_2 \otimes \mathbb{Z}_3 \simeq 0$.

Proof. We simply list the elements of $\mathbb{Z}_2 \otimes \mathbb{Z}_2$ and $\mathbb{Z}_2 \otimes \mathbb{Z}_3$. For $\mathbb{Z}_2 \otimes \mathbb{Z}_2$, we have

$$\overline{0} \otimes \overline{0} = 0 \quad \overline{0} \otimes \overline{1} = 0 \quad \overline{1} \otimes \overline{0} = 0 \quad \overline{1} \otimes \overline{1} = 1$$

Therefore, we see that $\mathbb{Z}_2 \otimes \mathbb{Z}_2$ is a group of order 2 so that $\mathbb{Z}_2 \otimes \mathbb{Z}_2 \simeq \mathbb{Z}_2$. Finally, for $\mathbb{Z}_2 \otimes \mathbb{Z}_3$, we have

$$\overline{0} \otimes \overline{0} = 0 \quad \overline{0} \otimes \overline{1} = 0 \quad \overline{0} \otimes \overline{2} = 0 \quad \overline{1} \otimes \overline{0} = 0$$

and

$$\overline{1} \otimes \overline{1} = \overline{1} \otimes \overline{4} = \overline{1} \otimes 4\overline{1} = 4\overline{1} \otimes \overline{1} = \overline{4} \otimes \overline{1} = \overline{0} \otimes \overline{1} = 0$$

and

$$\overline{1} \otimes \overline{2} = \overline{1} \otimes 2\overline{1} = 2\overline{1} \otimes \overline{1} = \overline{2} \otimes \overline{1} = \overline{0} \otimes \overline{1} = 0$$

Therefore, we see that every element of $\mathbb{Z}_2 \otimes \mathbb{Z}_3$ is equal to the zero element of $\mathbb{Z}_2 \otimes \mathbb{Z}_3$ so that $\mathbb{Z}_2 \otimes \mathbb{Z}_3 \simeq 0$. This completes the proof. $\square$

Example. (Tensor products distribute over direct sums) Let R be a ring with 1 and let M, M' be right R-modules and N, N' be left R-modules. Then

$$(M \oplus M') \otimes_R N \simeq (M \otimes_R N) \oplus (M' \otimes_R N)$$

and

$$M \otimes_R (N \oplus N') \simeq (M \otimes_R N) \oplus (M \otimes_R N)$$

Proof. We will prove the first statement and remark that the proof of the second statement is analogous to that of the first. Towards this end, define a map

$$f : (M \oplus M') \times N \to (M \otimes_R N) \oplus (M' \otimes_R N) \quad \text{by} \quad ((m, m'), n) \mapsto (m \otimes_R n, m' \otimes_R n)$$

It is easily verified that f is a middle linear map. Therefore, by the definition of the tensor product there exists a (unique) group homomorphism

$$\phi : (M \oplus M') \otimes_R N \to (M \otimes_R N) \oplus (M' \otimes_R N)$$

such that

$$\phi((m, m') \otimes_R n) = f((m, m'), n) = (m \otimes_R n, m' \otimes_R n) \quad \text{for all} \quad m \in M, m' \in M', n \in N$$

On the other hand, define

$$g : M \times N \to (M \oplus M') \otimes_R N \quad \text{by} \quad (m, n) \mapsto (m, 0) \otimes_R n$$

and

$$h : M' \times N \to (M \oplus M') \otimes_R N \quad \text{by} \quad (m', n) \mapsto (0, m') \otimes_R n$$

It is easily verified that both g and h are middle linear maps. Therefore, by the definition of the tensor product there exist (unique) group homomorphisms

$$\psi : M \otimes_R N \to (M \oplus M') \otimes_R N$$

such that

$$\psi(m \otimes_R n) = g(m, n) = (m, 0) \otimes_R n \quad \text{for all} \quad m \in M, n \in N$$

and

$$\gamma : M' \otimes_R N \to (M \oplus M') \otimes_R N$$

such that

$$\gamma(m', n) = h(m', n) = (0, m') \otimes_R n \quad \text{for all} \quad m' \in M', n \in N$$

In turn, the group homomorphisms ψ and γ give a group homomorphism

$$\theta : (M \otimes_R N) \oplus (M' \otimes_R N) \to (M \oplus M') \otimes_R N$$

such that

$$\theta(m\otimes_R n_1, m'\otimes_R n_2) = (m,0)\otimes_R n_1 + (0,m')\otimes_R n_2 \quad \text{for all} \quad m \in M, m' \in M', n_1, n_2 \in N$$

Finally, it is easily verified that the maps ϕ and θ are inverses of one another. In particular, we now have that the group homomorphism

$$\phi : (M \oplus M') \otimes_R N \to (M \otimes_R N) \oplus (M' \otimes_R N)$$

is bijective and hence a group isomorphism. We conclude that

$$(M \oplus M') \otimes_R N \simeq (M \otimes_R N) \oplus (M' \otimes_R N)$$

This completes the proof. □

Example. We have $(\mathbb{Z} \times \mathbb{Z}) \otimes (\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}) \simeq \underbrace{\mathbb{Z} \times \cdots \times \mathbb{Z}}_{\text{6 times}}$.

Proof. This is immediate, since $\otimes$ distributes over direct sums by the above proof and since, clearly, we have $\mathbb{Z} \otimes \mathbb{Z} \simeq \mathbb{Z}$. □

Example. Let R be a ring with identity and suppose that

$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$$

is a short exact sequence of left R-modules and left R-module homomorphisms. Suppose that D is a right R-module. Show that the sequence

$$D \otimes_R A \xrightarrow{1_D \otimes_R f} D \otimes_R B \xrightarrow{1_D \otimes_R g} D \otimes_R C \longrightarrow 0$$

of tensor products is exact. That is, show

(a): $\mathrm{Im}(1_D \otimes_R g) = D \otimes_R C$.

(b): $\mathrm{Im}(1_D \otimes_R f) \subseteq \ker(1_D \otimes_R g)$.

(c): $\ker(1_D \otimes_R g) \subseteq \mathrm{Im}(1_D \otimes_R f)$.

Proof. (a): In order to show that $\mathrm{Im}(1_D \otimes_R g) = D \otimes_R C$, it suffices to show that each elementary tensor in $D \otimes_R C$ is in the image of $1_D \otimes_R g$ since the elementary tensors in $D \otimes_R C$ generate $D \otimes_R C$. Towards this end, suppose that $d \otimes_R c \in D \otimes_R C$ is an elementary tensor in $D \otimes_R C$. Since the given sequence is a short exact sequence, we know that g is a surjection and hence as $c \in C$ there is some $b \in B$ such that $g(b) = c$. Now, notice that $d \otimes_R b \in D \otimes_R B$ and that

$$(1_D \otimes_R g)(d \otimes_R b) = 1_D(d) \otimes_R g(b) = d \otimes_R c$$

and hence $d \otimes_R c \in \mathrm{Im}(1_D \otimes_R g)$. By our previous observation, this completes the proof that $\mathrm{Im}(1_D \otimes_R g) = D \otimes_R C$. □

Proof. (b): Suppose $u \in \mathrm{Im}(1_D \otimes_R f)$. Then there is some $\sum_{i=1}^n d_i \otimes_R a_i \in D \otimes_R A$ with

$$\begin{aligned} u &= (1_D \otimes_R f)\left(\sum_{i=1}^n d_i \otimes_R a_i\right) \\ &= \sum_{i=1}^n [(1_D \otimes_R f)(d_i \otimes_R a_i)] \\ &= \sum_{i=1}^n [1_D(d_i) \otimes_R f(a_i)] \\ &= \sum_{i=1}^n [d_i \otimes_R f(a_i)] \end{aligned}$$

where the above equalities are justified by the fact that $1_D \otimes_R f$ is a group homomorphism and by the definition of the map $1_D \otimes_R f$. Now, since the given sequence is a short exact sequence we know that $\mathrm{Im} f = \ker g$ and hence by the above equality for u we obtain

$$\begin{aligned} (1_D \otimes_R g)(u) &= (1_D \otimes_R g)\left(\sum_{i=1}^n [d_i \otimes_R f(a_i)]\right) \\ &= \sum_{i=1}^n [(1_D \otimes_R g)(d_i \otimes_R f(a_i)] \\ &= \sum_{i=1}^n [1_D(d_i) \otimes_R g(f(a_i))] \\ &= \sum_{i=1}^n [d_i \otimes_R g(f(a_i))] \\ &= \sum_{i=1}^n d_i \otimes_R 0 \\ &= 0 \end{aligned}$$

where the above equalities are justified by the fact that $1_D \otimes_R g$ is a group homomorphism and by the definition of the map $1_D \otimes_R g$. Thus, by the above result we conclude that $u \in \ker(1_D \otimes_R g)$. This completes the proof. $\square$

Proof. (c): First, recall the canonical projection map

$$\pi : D \otimes_R B \to \frac{D \otimes_R B}{\mathrm{Im}(1_D \otimes_R f)}$$

Furthermore, we have the map

$$1_D \otimes_R g : D \otimes_R B \to D \otimes_R C$$

and by the result of Part (b) we know that $\mathrm{Im}(1_D \otimes_R f) \subseteq \ker(1_D \otimes_R g)$. By these observations and by the definition of π, then, there is a (unique) group homomorphism

$$\alpha : \frac{D \otimes_R B}{\mathrm{Im}(1_D \otimes_R f)} \to D \otimes_R C$$

such that

$$\begin{aligned}\alpha(\pi(d \otimes_R b)) &= \alpha((d \otimes_R b) + \mathrm{Im}(1_D \otimes_R f)) \\ &= (1_D \otimes_R g)(d \otimes_R b) \\ &= 1_D(d) \otimes_R g(b) \\ &= d \otimes_R g(b)\end{aligned}$$

for each $d \in D$ and $b \in B$. We claim that α is a group isomorphism. Towards this end, note that it remains to show that α is a bijection to establish that α is a group isomorphism. We will accomplish this task by exhibiting a two-sided inverse β of α.

Indeed, first let $c \in C$ and $d \in D$. By the same reasoning as above, we know that g is a surjection and hence there is some $b \in B$ such that $g(b) = c$. Now, define a map

$$\mu : D \times C \to \frac{D \otimes_R B}{\mathrm{Im}(1_D \otimes_R f)} \quad \text{by} \quad (d, c) \mapsto \pi(d \otimes_R b)$$

First, we show that μ is well-defined. Towards this end, suppose that $g(b') = c$ for some other $b' \in B$. In this case, we have $g(b) = c = g(b')$ so that since g is a group homomorphism we have

$$0 = g(b) - g(b') = g(b - b')$$

so that $b - b' \in \ker g = \mathrm{Im} f$ since the given sequence is a short exact sequence. Hence, there is some $a \in A$ such that $f(a) = b - b'$ so that $b = b' + f(a)$. Now, notice that

$$d \otimes_R f(a) = 1_D(d) \otimes_R f(a) = (1_D \otimes_R f)(d \otimes_R a) \quad \text{so that} \quad d \otimes_R f(a) \in \mathrm{Im}(1_D \otimes_R f)$$

and thus

$$\pi(d \otimes_R f(a)) = (d \otimes_R f(a)) + \mathrm{Im}(1_D \otimes_R f) = \mathrm{Im}(1_D \otimes_R f)$$

Therefore, we see since π is a group homomorphism that

$$\begin{aligned}\pi(d \otimes_R b) &= \pi(d \otimes_R (b' + f(a))) \\ &= \pi(d \otimes_R b' + d \otimes_R f(a)) \\ &= \pi(d \otimes_R b') + \pi(d \otimes_R f(a)) \\ &= ((d \otimes_R b') + \mathrm{Im}(1_D \otimes_R f)) + \mathrm{Im}(1_D \otimes_R f) \\ &= (d \otimes_R b') + \mathrm{Im}(1_D \otimes_R f) \\ &= \pi(d \otimes_R b')\end{aligned}$$

and hence it now follows that μ is a well-defined map.

Next, we show that μ is a middle linear map. First, suppose that $d_1, d_2 \in D$ and $c \in C$. Let $b \in B$ be such that $g(b) = c$. Then by the definition of μ and since π is a

group homomorphism, we obtain

$$\begin{aligned}\mu(d_1 + d_2, c) &= \pi((d_1 + d_2) \otimes_R b) \\ &= \pi(d_1 \otimes_R b + d_2 \otimes_R b) \\ &= \pi(d_1 \otimes_R b) + \pi(d_2 \otimes_R b) \\ &= \mu(d_1, c) + \mu(d_2, c)\end{aligned}$$

Secondly, suppose that $d \in D$ and $c_1, c_2 \in C$. Let $b_1, b_2 \in B$ be such that $g(b_1) = c_1$ and $g(b_2) = c_2$. Since g is a group homomorphism, this gives that

$$c_1 + c_2 = g(b_1) + g(b_2) = g(b_1 + b_2)$$

Thus, by the same reasoning as presented above we obtain

$$\begin{aligned}\mu(d, c_1 + c_2) &= \pi(d \otimes_R (b_1 + b_2)) \\ &= \pi(d \otimes_R b_1 + d \otimes_R b_2) \\ &= \pi(d \otimes_R b_1) + \pi(d \otimes_R b_2) \\ &= \mu(d, b_1) + \mu(d, b_2)\end{aligned}$$

Thirdly, suppose that $d \in D, c \in C$, and $r \in R$. Let $b \in B$ be such that $g(b) = c$. Moreover, since g is a left R-module homomorphism we see

$$rc = rg(b) = g(rb)$$

Thus, by the same reasoning as presented above we obtain

$$\begin{aligned}\mu(dr, c) &= \pi(dr \otimes_R b) \\ &= \pi(d \otimes_R rb) \\ &= \mu(d, rc)\end{aligned}$$

Combining the previous results, then, we see that μ is a middle linear map and hence there exists a (unique) group homomorphism

$$\beta : D \otimes_R C \to \frac{D \otimes_R B}{\mathrm{Im}(1_D \otimes_R f)}$$

such that if $d \in D$ and $c \in C$ with $g(b) = c$ for some $b \in B$ we have

$$\beta(d \otimes_R c) = \mu(d \otimes_R c) = \pi(d \otimes_R b)$$

We claim that β is a two-sided inverse of α.

First, we show that $\alpha \circ \beta = 1_{D \otimes_R C}$. By the same reasoning as presented above, it suffices to show that the maps involved in the previous equality agree on the elementary tensors of $D \otimes_R C$. Indeed, suppose that $d \otimes_R c \in D \otimes_R C$ is an elementary tensor of

$D \otimes_R C$ and let $b \in B$ be such that $g(b) = c$. Then

$$\begin{aligned}(\alpha \circ \beta)(d \otimes_R c) &= \alpha(\beta(d \otimes_R c)) \\ &= \alpha(\pi(d \otimes_R b)) \\ &= d \otimes_R g(b) \\ &= d \otimes_R c \\ &= 1_{D \otimes_R C}(d \otimes_R c)\end{aligned}$$

so that $\alpha \circ \beta = 1_{D \otimes_R C}$. Secondly, we show that $\beta \circ \alpha = 1_{D \otimes_R B/\mathrm{Im}(1_D \otimes_R f)}$. By the same reasoning as presented above, it suffices to show that the maps involved in the previous equality agree on the elementary tensors of $D \otimes_R B/\mathrm{Im}(1_D \otimes_R f)$. Indeed, suppose that $(d \otimes_R b) + \mathrm{Im}(1_D \otimes_R f) \in D \otimes_R B/\mathrm{Im}(1_D \otimes_R f)$ is an elementary tensor of $D \otimes_R B/\mathrm{Im}(1_D \otimes_R f)$. Then

$$\begin{aligned}(\beta \circ \alpha)((d \otimes_R b) + \mathrm{Im}(1_D \otimes_R f)) &= \beta(\alpha((d \otimes_R b) + \mathrm{Im}(1_D \otimes_R f))) \\ &= \beta(\alpha(\pi(d \otimes_R b))) \\ &= \beta(d \otimes_R g(b)) \\ &= \beta(d \otimes_R b) \\ &= \pi(d \otimes_R b) \\ &= (d \otimes_R b) + \mathrm{Im}(1_D \otimes_R f)\end{aligned}$$

so that $\beta \circ \alpha = 1_{D \otimes_R B/\mathrm{Im}(1_D \otimes_R f)}$. Combining the previous results, then, we see that β is a two-sided inverse of α. In particular, by our observation made above this gives that α is a group isomorphism.

Finally, recall that by Part (a) we have that $\mathrm{Im}(1_D \otimes_R g) = D \otimes_R C$. In particular, this gives by the First Isomorphism Theorem that

$$\frac{D \otimes_R B}{\ker(1_D \otimes_R g)} \simeq D \otimes_R C$$

But recall that

$$\alpha : \frac{D \otimes_R B}{\mathrm{Im}(1_D \otimes_R f)} \to D \otimes_R C$$

is an isomorphism by the above result. Therefore, we obtain

$$\frac{D \otimes_R B}{\ker(1_D \otimes_R g)} \simeq D \otimes_R C \simeq \frac{D \otimes_R B}{\mathrm{Im}(1_D \otimes_R f)}$$

and hence we conclude that $\ker(1_D \otimes_R g) = \mathrm{Im}(1_D \otimes_R f)$. This completes the proof. $\square$

Topic 5: Commutative Algebra; Hilbert's Basis Theorem

Theorem. Let R be a commutative ring with 1 and let S be a multiplicative set in R and I an ideal of R such that $S \cap I = \emptyset$. Then there is a prime ideal P of R maximal among those containing I and disjoint from S.

Proof. Let $\mathcal{S}$ denote the collection of all ideals of R containing I that have an empty intersection with S. Note that clearly we have $I \in \mathcal{S}$ by hypothesis so that $\mathcal{S} \neq \emptyset$. Now, define a partial order on $\mathcal{S}$ by for $J_1, J_2 \in \mathcal{S}$ we have $J_1 \leq J_2$ if and only if $J_1 \subseteq J_2$. Next, let $\mathcal{C}$ be a nonempty chain in $\mathcal{S}$ and define

$$J = \bigcup_{C \in \mathcal{C}} C$$

Notice that since $\mathcal{C}$ is a chain and since each $C \in \mathcal{C}$ is an ideal of R we have that J is an ideal of R. Furthermore, since each $C \in \mathcal{C}$ contains I we have that J also contains I and as each $C \in \mathcal{C}$ has an empty intersection with S we have that J also has an empty intersection with S. By the previous results, we see that $J \in \mathcal{S}$ and as J is clearly an upper bound for $\mathcal{C}$ we have by Zorn's Lemma that there is a maximal element $P \in \mathcal{S}$.

Now, by the definition of membership in $\mathcal{S}$ it follows that the proof will be complete once we establish that P is a *prime* ideal of R. Towards this end, first note that since $S \cap P = \emptyset$ and as $S \neq \emptyset$ since S is a multiplicative set in R we must have that $P \neq R$. Next, for the sake of contradiction suppose there were elements $a, b \in R$ such that $ab \in P$ but $a, b \notin P$. In this case, we see that $Ra + P$ and $Rb + P$ are ideals of R which properly contain P since R has 1 and $a, b \notin P$. Furthermore, we also have that $Ra + P$ and $Rb + P$ contain I since P contains I as $P \in \mathcal{S}$. Therefore, by the maximality of $P \in \mathcal{S}$ and by the definition of $\mathcal{S}$ it follows that it must be the case that there exist elements $r_1, r_2 \in R$ and $p_1, p_2 \in P$ such that

$$r_1 a + p_1, r_2 b + p_2 \in S$$

Since S is a multiplicative set, then, we have

$$(r_1 a + p_1)(r_2 b + p_2) \in S$$

and since P is an ideal of R with $ab, p_1, p_2 \in P$ we have as R is commutative that

$$(r_1 a + p_1)(r_2 b + p_2) = r_1 r_2 ab + r_1 p_2 + r_2 p_1 + p_1 p_2 \in P$$

However, the previous two results show that

$$(r_1 a + p_1)(r_2 b + p_2) \in S \cap P$$

which contradicts the fact that $S \cap P = \emptyset$ since $P \in \mathcal{S}$. We conclude that P is a prime ideal of R, completing the proof. $\square$

Definition. Let R be a commutative ring with 1 and I an ideal of R. The ***radical*** of I is the intersection of all prime ideals of R containing I and is denoted $\mathrm{Rad}(I)$.

Theorem. Let R be a commutative ring with 1 and I be an ideal of R. Then

$$\mathrm{Rad}(I) = \{r \in R : r^n \in I \text{ for some } n \geq 1\}$$

Proof. First, let $r \in \mathrm{Rad}(I)$. For the sake of contradiction, suppose that for every $n \geq 1$ we have $r^n \notin I$. Now, define $S = \{r^n : n \geq 1\}$ and notice that S is a multiplicative set in R. Furthermore, we have by our assumption that $S \cap I = \emptyset$. Therefore, there is a prime ideal P of R such that $P \supseteq I$ and $S \cap P = \emptyset$. But since P is a prime ideal of R containing I, it follows that $\mathrm{Rad}(I) \subseteq P$ and hence $r \in P$ since $r \in \mathrm{Rad}(I)$. However, we also clearly have that $r \in S$ and thus $r \in S \cap P$ so that $S \cap P \neq \emptyset$ which is a contradiction. We conclude that there is some $n \geq 1$ such that $r^n \in I$.

On the other hand, suppose that $r \in R$ and $r^n \in I$ for some $n \geq 1$. Let P be a prime ideal of R with $P \supseteq I$. In this case, we have $r^n \in I \subseteq P$ and since P is a prime ideal of R it now follows that $r \in P$. Since P was an arbitrary prime ideal of R containing I, we now have by definition that $r \in \mathrm{Rad}(I)$. This completes the proof. $\square$

Lemma. (Nakayama's Lemma) Let R be a commutative ring with 1 and J an ideal of R. Then the following are equivalent:

(i): J is contained in every maximal ideal of R.

(ii): For all $j \in J$, we have that $1 - j$ is a unit of R.

(iii): If A is a finitely generated R-module such that $JA = A$, then $A = 0$.

(iv): If B is an R-submodule of a finitely generated R-module A such that $A = JA + B$, then $A = B$.

Proof. (i $\Rightarrow$ ii): For the sake of contradiction, suppose there were some $j \in J$ such that $1 - j$ were not a unit of R. In this case, then, the ideal $(1 - j)$ must be contained in some maximal ideal M of R so that

$$1 - j \in (1 - j) \subseteq M$$

Therefore, there is some $m \in M$ such that $1 - j = m$ and thus $1 = j + m$. But by hypothesis, we have that $J \subseteq M$ so that $j \in J \subseteq M$. Thus, we obtain that $1 = j + m \in M$ since $j, m \in M$. However, this implies that $M = R$ which contradicts the fact that $M \neq R$ since M is a maximal ideal of R. We conclude that $1 - j$ is a unit of R for every $j \in J$.

(ii $\Rightarrow$ iii): For the sake of contradiction, suppose that $A \neq 0$. Since A is finitely generated, we can choose a generating set $\{a_1, \ldots, a_n\} \subseteq A$ with n as small as possible. In particular, since $A \neq 0$ we have $n \geq 1$ and $a_1 \neq 0$. Now, since $a_1 \in A = JA$, since A is generated by $\{a_1, \ldots, a_n\}$, and since J is an ideal of R it follows that we may write

$$a_1 = j_1 a_1 + \cdots + j_n a_n$$

for some $j_1, \ldots, j_n \in J$. By the above equality, we obtain the equality

$$(1 - j_1)a_1 = a_1 - j_1 a_1 = j_2 a_2 + \cdots + j_n a_n$$

Furthermore, by hypothesis, we have that $1 - j_1$ is a unit of R since $j_1 \in J$. Therefore, left-multiplying both sides of the above equality by $(1 - j_1)^{-1}$ implies that a_1 is an R-linear combination of $a_2, \ldots, a_n$. By this observation and since $\{a_1, \ldots, a_n\}$ generates A, it now follows that in fact $\{a_2, \ldots, a_n\}$ generates A. However, this contradicts the minimality of n. We conclude that $A = 0$.

(iii $\Rightarrow$ iv): Let A be a finitely generated R-module and let $B \subseteq A$ be an R-submodule of A such that $A = JA + B$. We claim that $J(A/B) = A/B$. Towards this end, first suppose that $x \in J(A/B)$. Then there exist elements $j_1, \ldots, j_n \in J$ and elements $a_1 + B, \ldots, a_n + B \in A/B$ such that

$$\begin{aligned} x &= j_1(a_1 + B) + \cdots + j_n(a_n + B) \\ &= (j_1 a_1 + B) + \cdots + (j_n a_n + B) \\ &= (j_1 a_1 + \cdots + j_n a_n) + B \end{aligned}$$

Now, notice that $j_1 a_1 + \cdots + j_n a_n \in JA$. Therefore, since $A = JA + B$ and as

$$(j_1 a_1 + \cdots + j_n a_n) + 0 \in JA + B$$

it follows that there is some $a \in A$ such that

$$a = (j_1 a_1 + \cdots + j_n a_n) + 0 = j_1 a_1 + \cdots + j_n a_n$$

and thus

$$j_1 a_1 + \cdots + j_n a_n = a \in A$$

so that

$$x = (j_1 a_1 + \cdots + j_n a_n) + B = a + B \in A/B$$

On the other hand, suppose that $x \in A/B$. Then there is some $a \in A$ such that $x = a + B$. Since $a \in A$ and as $A = JA + B$, it follows that there are $j_1, \ldots, j_n \in J$, $a_1, \ldots, a_n \in A$, and $b \in B$ such that

$$a = (j_1 a_1 + \cdots + j_n a_n) + b$$

and as $b \in B$ we obtain

$$\begin{aligned} x &= a + B \\ &= ((j_1 a_1 + \cdots + j_n a_n) + b) + B \\ &= (j_1 a_1 + \cdots + j_n a_n) + B \\ &= (j_1 a_1 + B) + \cdots + (j_n a_n + B) \\ &= j_1(a_1 + B) + \cdots + j_n(a_n + B) \\ &\in J(A/B) \end{aligned}$$

The previous results allow us to conclude that $J(A/B) = A/B$. Finally, notice that since A is a finitely generated R-module that A/B is a finitely generated R-module. Therefore, by hypothesis we have since $J(A/B) = A/B$ that $A/B = 0$ and hence $A = B$.

(iv $\Rightarrow$ i): Let M be a maximal ideal of R. First, suppose that $M \neq JR + M$. Since $JR + M$ is an ideal of R that clearly properly contains M and as M is a maximal ideal of R, it now follows that $JR + M = R$. Now, note that R is a finitely generated R-module since R has identity and hence $\{1\} \subseteq R$ is a finite generating set for R. Furthermore,

note that M is an R-submodule of R since M is an ideal of R. By hypothesis, then, the previous two observations imply that $R = M$ which is a contradiction since $M \neq R$ as M is a maximal ideal of R. Therefore, we conclude that $M = JR + M$ and hence as R has identity we have

$$J \subseteq JR + M = M$$

so that $J \subseteq M$. As the maximal ideal M of R was arbitrary, this completes the proof. $\square$

Proposition. Let R be a commutative local ring. Then every finitely generated projective R-module is a free R-module.

Proof. Let M be the unique maximal ideal of R and suppose that P is a finitely generated projective R-module. Since P is a finitely generated R-module, we know that P is the homomorphic image of a finitely generated free R-module. Among all such finitely generated free R-modules, choose one F with the smallest number of generators. Let n be this number of generators and let $x_1, \ldots, x_n \in F$ be a basis for F over R.

Now, let $\pi : F \to P$ be a surjective R-module homomorphism and let $K = \ker \pi$. Then we obtain the short exact sequence

$$0 \longrightarrow K \xrightarrow{\ i\ } F \xrightarrow{\ \pi\ } P \longrightarrow 0$$

where i is the inclusion map. Since P is a projective R-module, it follows that the above short exact sequence splits so that $F \simeq K \oplus P$. Therefore, there is an R-submodule P' of F such that $F = K \oplus P'$ and $P' \simeq P$.

For the sake of contradiction, suppose that $K \not\subseteq MF$. Then there is some $k \in K$ such that $k \notin MF$. Since $k \in K \subseteq F$ and as $x_1, \ldots, x_n \in F$ is a basis for F over R, it follows that there are $r_1, \ldots, r_n \in R$ such that $k = r_1x_1 + \cdots + r_nx_n$. Now, if $r_1, \ldots, r_n \in M$ then by the previous equality it would follow that $k \in MF$ which contradicts the fact that $k \notin MF$. Therefore, there is some $i \in \{1, \ldots, n\}$ such that $r_i \notin M$. Without loss of generality, assume that $r_1 \notin M$.

Next, note that since $r_1x_1 + \cdots + r_nx_n = k \in K = \ker \pi$ we have since π is an R-module homomorphism that

$$0 = \pi(k) = \pi(r_1x_1 + \cdots + r_nx_n) = \pi(r_1x_1) + \cdots + \pi(r_nx_n) = r_1\pi(x_1) + \cdots + r_n\pi(x_n)$$

and thus

$$r_1\pi(x_1) = -r_2\pi(x_2) - \cdots - r_n\pi(x_n) = \pi(-r_2x_2) + \cdots + \pi(-r_nx_n)$$

Now, since $r_1 \notin M$ and as M is the unique maximal ideal of R it follows that r_1 is a unit of R. Therefore, by left-multiplying the above equality by r_1^{-1} it follows that since π is an R-module homomorphism that $\pi(x_1) \in \pi(Rx_2 + \cdots + Rx_n)$. But recall that F is a free R-module with basis $\{x_1, \ldots, x_n\}$ and that $\pi : F \to P$ is a surjective R-module homomorphism. By these two observations, then, we see that

$$P = \pi(F) = \pi(Rx_1 + \cdots + Rx_n)$$

and as $\pi(x_1) \in \pi(Rx_2 + \cdots + Rx_n)$ it now follows that

$$P = \pi(Rx_1 + \cdots + Rx_n) = \pi(Rx_2 + \cdots + Rx_n)$$

However, the above equality implies that P is the homomorphic image of a finitely generated free R-module with a basis of cardinality strictly less than n, contradicting the minimality of n. We conclude that $K \subseteq MF$.

To complete the proof, notice that clearly $MF + P' \subseteq F$ since F is an R-module and $M \subseteq R$ and as $P' \subseteq F$. On the other hand, by our above result we have that

$$F = K + P' \subseteq MF + P'$$

and thus $F = MF + P'$. Finally, note that since M is the unique maximal ideal of R that M is trivially contained in every maximal ideal of R. Thus, since $F = MF + P'$, since F is a finitely generated R-module, and as P' is an R-submodule of F we have by Nakayama's Lemma that $F = P'$. Therefore, we obtain $P \simeq P' = F$ and since F is a free R-module we conclude that P is a free R-module. This completes the proof. $\square$

Theorem. (Hilbert's Basis Theorem) Let R be a commutative Noetherian ring with 1. Then $R[x_1, \ldots, x_n]$ is Noetherian.

Proof. Inductively, it follows that it suffices to prove the result for $R[x]$. Towards this end, let I be an ideal of $R[x]$. We must show that I is finitely generated. First, for each integer $n \geq 0$ define

$$I_n = \{r \in R : r \text{ is the leading coefficient of some } f(x) \in I \text{ with } \deg(f(x)) = n\} \cup \{0\}$$

We claim that I_n is an ideal of R for each integer $n \geq 0$.

Indeed, fix any integer $n \geq 0$. First, note that $0 \in I_n$ so that $I_n \neq \emptyset$. Now, suppose that $r_1, r_2 \in I_n$. If $r_1 = 0 = r_2$, then clearly $r_1 - r_2 \in I_n$. If $r_1 \neq 0$ and $r_2 = 0$, then clearly $r_1 - r_2 \in I_n$. If $r_1 = 0$ and $r_2 \neq 0$, note that there is some polynomial $f(x) \in I$ with $\deg(f(x)) = n$ with leading coefficient r_2. By this observation, it is immediate that $-f(x) \in I$ since I is an ideal of $R[x]$ and $\deg(-f(x)) = n$ with leading coefficient $-r_2$ so that

$$r_1 - r_2 = 0 - r_2 = -r_2 \in I_n$$

Finally, suppose that $r_1 \neq 0$ and $r_2 \neq 0$. If $r_1 - r_2 = 0$, then $r_1 - r_2 \in I$. Therefore, assume that $r_1 - r_2 \neq 0$. Since $r_1 \neq 0$ and $r_2 \neq 0$ are elements of I_n, it follows that there exist polynomials $f(x), g(x) \in I$ with $\deg(f(x)) = n = \deg(g(x))$ with leading coefficients r_1, r_2, respectively. By this observation, it is immediate that $f(x) - g(x) \in I$ since I is an ideal of $R[x]$ and since $r_1 - r_2 \neq 0$ we have $\deg(f(x) - g(x)) = n$ with leading coefficient $r_1 - r_2$ so that $r_1 - r_2 \in I_n$. Therefore, we may now conclude that I_n is a subgroup of $R[x]$ under addition.

Now, let $s \in R$ and $r \in I_n$. If $r = 0$, then $sr = 0 \in I_n$. Therefore, assume that $r \neq 0$. If $sr = 0$, then clearly $sr \in I_n$. Therefore, assume that $sr \neq 0$. Since $r \neq 0$ is an element of I_n, there is some polynomial $f(x) \in I$ with $\deg(f(x)) = n$ with leading coefficient r. By this observation, it is immediate that $sf(x) \in I$ since I is an ideal of $R[x]$ and since $sr \neq 0$ we have $\deg(sf(x)) = n$ with leading coefficient sr so that $sr \in I_n$. The previous results show that I_n is an ideal of $R[x]$ and since the integer $n \geq 0$ was arbitrary, we may now conclude that I_n is an ideal of $R[x]$ for each integer $n \geq 0$.

Next, again fix any integer $n \geq 0$. We claim that $I_n \subseteq I_{n+1}$. Indeed, suppose that $r \in I_n$. If $r = 0$, then clearly $r \in I_{n+1}$. Therefore, assume that $r \neq 0$. Since $r \neq 0$ is an element of I_n, there is some polynomial $f(x) \in I$ with $\deg(f(x)) = n$ with leading coefficient r. By this observation, it is immediate that $xf(x) \in I$ since I is an ideal of $R[x]$ and since $r \neq 0$ we have $\deg(xf(x)) = n + 1$ with leading coefficient r so that $r \in I_{n+1}$. The previous result shows that $I_n \subseteq I_{n+1}$ and since the integer $n \geq 0$ was arbitrary, we now obtain the ascending chain of ideals of R

$$I_0 \subseteq I_1 \subseteq I_2 \subseteq \cdots \subseteq I_n \subseteq \cdots$$

Therefore, since R is Noetherian it follows that there exists some integer $t \geq 0$ such that for all $n \geq t$ we have $I_n = I_t$.

Again by the observation that R is Noetherian, it follows that for each I_i there exist elements $r_{i,1}, \ldots, r_{i,\alpha_i} \in I_i$ such that $I_i = (r_{i,1}, \ldots, r_{i,\alpha_i})$ with $r_{i,j} \neq 0$ for all integers $i \geq 0$ and all integers $1 \leq j \leq \alpha_i$. Furthermore, it follows that since each $r_{i,j}$ is a nonzero element of I_i that there exist polynomials $f_{i,j}(x) \in I$ with $\deg(f_{i,j}(x)) = i$ with leading coefficient $r_{i,j}$ for all integers $i \geq 0$ and all integers $1 \leq j \leq \alpha_i$.

We claim that the ideal I of $R[x]$ is generated by the set

$$A = \{f_{i,j}(x) : i \in \{0, \ldots, t\}, j \in \{1, \ldots, \alpha_i\}\}$$

Towards this end, let J be the ideal of $R[x]$ generated by A. First note that we clearly have $A \subseteq I$ so that $J \subseteq I$ as I is an ideal of $R[x]$. For the sake of contradiction, suppose that $I \neq J$. In this case, there is a polynomial $g(x) \in I - J$ which can be chosen to be of smallest possible degree among all of the polynomials in $I - J$. For definiteness, let $\deg(g(x)) = n$ and let a be the leading coefficient of $g(x)$ so that $a \in I_n$ by definition.

First, suppose that $n \geq t$. In this case, we have $I_n = I_t$ by the above. Therefore, we have that $a \in I_n = I_t = (r_{t,1}, \ldots, r_{t,\alpha_t})$ and hence there exist elements $s_1, \ldots, s_{\alpha_t} \in R$ such that $a = s_1 r_{t,1} + \cdots + s_{\alpha_t} r_{t,\alpha_t}$. Now, consider the polynomial

$$h(x) = s_1 f_{t,1}(x) + \cdots + s_{\alpha_t} f_{t,\alpha_t}(x)$$

Notice that $\deg(f_{t,1}(x)), \ldots, \deg(f_{t,\alpha_t}(x)) = t$ and that the leading coefficient of $h(x)$ is a. These observations imply that $\deg(h(x)) = t$. Also, we see that $h(x) \in J$ since J is an ideal of $R[x]$ and $f_{t,1}(x), \ldots, f_{t,\alpha_t}(x) \in A \subseteq J$. Furthermore, since J is an ideal of $R[x]$ and $h(x) \in J$ we have that $x^{n-t}h(x)$ is a polynomial in J of degree n with leading coefficient a. Therefore, we see that since $g(x)$ is a polynomial of degree n with leading coefficient a and as I is an ideal with $g(x) \in I$ and $x^{n-t}h(x) \in J \subseteq I$ that $g(x) - x^{n-t}h(x)$ is a polynomial in I of degree at most $n - 1$. By the minimality of n, then, we conclude that $g(x) - x^{n-t}h(x) \in J$. But since $x^{n-t}h(x) \in J$, this implies that $g(x) \in J$ since J is an ideal which is a contradiction.

The above result now forces $n < t$. In this case, we have $a \in I_n = (r_{n,1}, \ldots, r_{n,\alpha_n})$ and hence there exists elements $s_1, \ldots, s_n \in R$ such that $a = s_1 r_{n,1} + \cdots + s_{\alpha_n} r_{n,\alpha_n}$. Similarly as above, consider the polynomial

$$h(x) = s_1 f_{n,1}(x) + \cdots + s_{\alpha_n} f_{n,\alpha_n}(x)$$

Notice that $\deg(f_{n,1}(x)), \ldots, \deg(f_{n,\alpha_n}(x)) = n$ and that the leading coefficient of $h(x)$ is a. These observations imply that $\deg(h(x)) = n$. Also, we see that $h(x) \in J$ since J is an ideal of $R[x]$ and $f_{n,1}(x), \ldots, f_{n,\alpha_n}(x) \in A \subseteq J$. Therefore, we see since $h(x)$ is a polynomial in $J \subseteq I$ of degree n with leading coefficient a, since $g(x) \in I$, and as I is an ideal that $g(x) - h(x)$ is a polynomial in I of degree at most $n-1$. By the minimality of n, then, we conclude that $g(x) - h(x) \in J$. But since $h(x) \in J$, this implies that $g(x) \in J$ since J is an ideal which is a contradiction.

In any case, we obtain a contradiction by assuming that $I \neq J$. Therefore, we conclude that $I = J = (A)$ and since A is finite we conclude that I is finitely generated. As I was an arbitrary ideal of $R[x]$, this completes the proof the $R[x]$ is Noetherian. $\square$

Topic 6: Ring Extensions; Integral Closure

Definition. Let S be a commutative ring with identity and R a subring of S containing the identity of S. In this situation, we say that S is an ***extension ring*** of R.

Definition. Let S be an extension ring of a ring R and let $s \in S$. We say that s is ***integral*** over R if there is some monic polynomial $f(x) \in R[x]$ (so that $f(x) \neq 0$ by the stipulation that $f(x)$ be monic) such that $f(s) = 0$. We say that S is an ***integral extension*** of R if every element in S is integral over R.

Example. We have that $\sqrt{2} \in \mathbb{C}$ is integral over $\mathbb{Z}$ and that $1/\sqrt{2} \in \mathbb{C}$ is integral over $\mathbb{Q}$ but that $1/\sqrt{2} \in \mathbb{C}$ is not integral over $\mathbb{Z}$.

Proof. Note that $\mathbb{C}$ is clearly an extension ring of the rings $\mathbb{Z}$ and $\mathbb{Q}$.

Now, let $f(x) = x^2 - 2 \in \mathbb{Z}[x]$. Then $f(x)$ is a monic polynomial in $\mathbb{Z}[x]$ such that $f(\sqrt{2}) = (\sqrt{2})^2 - 2 = 0$ so that $\sqrt{2} \in \mathbb{C}$ is integral over $\mathbb{Z}$.

Next, let $g(x) = x^2 - 1/2 \in \mathbb{Q}[x]$. Then $g(x)$ is a monic polynomial in $\mathbb{Q}[x]$ such that $g(1/\sqrt{2}) = (1/\sqrt{2})^2 - 1/2 = 0$ so that $1/\sqrt{2} \in \mathbb{C}$ is integral over $\mathbb{Q}$.

Lastly, we remark that we will not prove here that $1/\sqrt{2} \in \mathbb{C}$ is not integral over $\mathbb{Z}$. Nonetheless, consider the polynomial $h(x) = 2x^2 - 1 \in \mathbb{Z}[x]$. In this case, we see that $h(1/\sqrt{2}) = 2(1/\sqrt{2})^2 - 1 = 0$ so that $1/\sqrt{2} \in \mathbb{C}$ is *algebraic* over $\mathbb{Z}$.

However, notice that while $h(x)$ is a polynomial in $\mathbb{Z}[x]$ such that $h(1/\sqrt{2}) = 0$ that it does not follow by the existence of $h(x)$ that $1/\sqrt{2} \in \mathbb{C}$ is integral over $\mathbb{Z}$ since $h(x)$ is not a monic polynomial in $\mathbb{Z}[x]$. $\square$

Theorem. Let S be an extension ring of a ring R. Let $s \in S$. Then the following are equivalent:

(i): s is integral over R.

(ii): $R[s]$ is finitely generated as an R-module.

(iii): There is a subring T of S containing $R[s]$ which is finitely generated an an R-module.

(iv): There is an $R[s]$-submodule B of S which is finitely generated as an R-module and whose annihilator in $R[s]$ is zero.

Proof. (i $\Rightarrow$ ii): Since s is integral over R, there is a monic polynomial $f(x) \in R[x]$ such that $f(s) = 0$. Let $n = \deg(f(x))$. We claim that $\{1, s, s^2, \ldots, s^{n-1}\}$ generate $R[s]$ as an R-module. Towards this end, suppose that $z \in R[s]$. Then there is some $g(x) \in R[x]$ such that $z = g(s)$. Now, note that R has identity and that the leading coefficient of $f(x)$ is a unit of R as the leading coefficient of $f(x)$ is 1 as $f(x)$ is monic. By these observations, we may use the Division Algorithm to write $g(x) = f(x)q(x) + r(x)$ for some $q(x), r(x) \in R[x]$ with $\deg(r(x)) < \deg(f(x)) = n$. Thus, as $f(s) = 0$ we see

$$z = g(s) = f(s)q(s) + r(s) = 0 + r(s) = r(s)$$

Therefore, since $\deg(r(x)) < n$ and $r(x) \in R[x]$ it now follows that z is an R-linear combination of $1, s, s^2, \ldots, s^{n-1}$. Since $z \in R[s]$ was arbitrary, we conclude that $R[s]$ is finitely generated as an R-module.

(ii $\Rightarrow$ iii): Let $T = R[s]$. Then T is a subring of S containing $R[s]$. Furthermore, since $R[s]$ is finitely generated as an R-module by hypothesis it follows directly by the definition of T that T is finitely generated as an R-module.

(iii $\Rightarrow$ iv): Let $B = T$. Since T is a subring of S containing $R[s]$, it is immediate by the definition of B that B is an $R[s]$-submodule of S. Furthermore, since T is a finitely generated R-module it follows by the definition of B that B is a finitely generated R-module. Finally, notice that we have $1 \in R[s] \subseteq T = B$. We will use this observation to show that the annihilator of B in $R[s]$ is zero. Towards this end, suppose that $u \in R[s]$ is in the annihilator of B. Since $1 \in B$, this implies that $u = u1 = 0$ and hence the annihilator of B in $R[s]$ is zero.

(iv $\Rightarrow$ i): Let $\{b_1, \ldots, b_n\} \subseteq B$ be a finite set of R-generators for B. Since B is an $R[s]$-submodule of S, it follows that $sb_i \in B$ for each $i \in \{1, \ldots, n\}$. Thus, we may write

$$sb_i = r_{i,1}b_1 + \cdots + r_{i,n}b_n \quad \text{for some} \quad r_{i,1}, \ldots, r_{i,n} \in R \quad \text{for each} \quad i \in \{1, \ldots, n\}$$

We then obtain the equations

$$\begin{aligned}
&(r_{1,1} - s)b_1 + r_{1,2}b_2 + \cdots + r_{1,n}b_n = 0 \\
&r_{2,1}b_1 + (r_{2,2} - s)b_2 + \cdots + r_{2,n}b_n = 0 \\
&\vdots \\
&r_{n,1}b_1 + r_{n,2}b_2 + \cdots + (r_{n,n} - s)b_n = 0
\end{aligned}$$

Now, let

$$M = \begin{bmatrix} r_{1,1} - s & r_{1,2} & \cdots & r_{1,n} \\ r_{2,1} & r_{2,2} - s & \cdots & r_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ r_{n,1} & r_{n,2} & \cdots & r_{n,n} - s \end{bmatrix}$$

Then by the above collection of equations, we have

$$M \begin{bmatrix} b_1 \\ \vdots \\ b_n \end{bmatrix} = \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix}$$

By facts from Linear Algebra, there is another matrix N such that $NM = \det(M)I$. Therefore, we obtain by the above that

$$\begin{bmatrix} \det(M)b_1 \\ \vdots \\ \det(M)b_n \end{bmatrix} = \det(M)I \begin{bmatrix} b_1 \\ \vdots \\ b_n \end{bmatrix} = NM \begin{bmatrix} b_1 \\ \vdots \\ b_n \end{bmatrix} = N \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix}$$

and hence $\det(M)b_i = 0$ for all $i \in \{1, \ldots, n\}$. Now, notice that $\det(M) \in R[s]$. Furthermore, since $\det(M)b_i = 0$ for all $i \in \{1, \ldots, n\}$ and since $b_1, \ldots, b_n \in B$ generate B as an R-module it now follows that $\det(M) \in R[s]$ is in the annihilator of B.

By the above results, we have by hypothesis that $\det(M) = 0$. It now follows that there is some polynomial $d(x) \in R[x]$ with $\deg(d(x)) = n$ and leading coefficient either 1 or -1 such that $d(s) = 0$. If the leading coefficient of $d(x)$ is 1, then $d(x)$ is a monic polynomial in $R[x]$ such that $d(s) = 0$ so that s is integral over R. If the leading coefficient of $d(x)$ is -1, then $-d(x)$ is a monic polynomial in $R[x]$ such that $-d(s) = -0 = 0$ so that s is integral over R. This completes the proof. □

Corollary. Suppose S is an extension ring of a ring R and that $s \in S$ is integral over R. Then $R[s]$ is an integral extension of R.

Proof. Since $s \in S$ is integral over R, we have by the previous Theorem that there is a subring T of S containing $R[s]$ which is finitely generated as an R-module. Now, let $t \in R[s] \subseteq T$. Then T is a subring of S containing $R[t]$ and T is finitely generated as an R-module. Appealing once again to the previous Theorem, this shows t is integral over R. Since $t \in R[s]$ was arbitrary, this shows that $R[s]$ is an integral extension of R. □

Corollary. Suppose that T/S is an integral extension and that S/R is an integral extension. Then T/R is an integral extension.

Proof. Let $t \in T$. Since T/S is an integral extension, there is some monic polynomial $f(x) \in S[x]$ such that $f(t) = 0$. For definiteness, write

$$f(x) = x^k + a_{k-1}x^{k-1} + \cdots + a_1 x + a_0 \in S[x]$$

Now, since $a_0, \ldots, a_{k-1} \in S$ and as S/R is an integral extension we know that there is some n_i such that $R[a_i]$ is generated as an R-module by $\{1, a_i, a_i^2, \ldots, a_i^{n_i-1}\}$ for each $i \in \{0, \ldots, k-1\}$. Therefore, we see $R[a_0, \ldots, a_{k-1}]$ is generated as an R-module by

$$\left\{1, a_0, \ldots, a_0^{n_0-1}, \ldots, a_{k-1}, \ldots, a_{k-1}^{n_{k-1}-1}\right\}$$

We will use this observation below.

Towards this end, consider $R[a_0, \ldots, a_{k-1}, t]$ and recall that $f(t) = 0$. By this observation, it follows that $R[a_0, \ldots, a_{k-1}, t]$ is generated as an R-module by the above set of generators for $R[a_0, \ldots, a_{k-1}]$ multiplied by the elements from $\{1, t, t^2, \ldots, t^{k-1}\}$. Since this set of generators is clearly finite, we see $R[a_0, \ldots, a_{k-1}, t]$ is a subring of T that is finitely generated as an R-module. Furthermore, we have that $R[a_0, \ldots, a_{k-1}, t] \supseteq R[t]$. By the Theorem from the previous lecture, we conclude that t is integral over R and hence T/R is an integral extension, completing the proof. □

Corollary. Let S be an extension ring of a ring R. Let $\hat{R}$ be the set of elements of S which are integral over R. Then $\hat{R}$ is a subring of S and $\hat{R}$ is an integral extension of R which contains every subring of S that is integral over R. Furthermore, if S is an integral domain then $\hat{R}$ is an integral domain.

Proof. First, note that clearly $0 \in S$ is integral over R so that $0 \in \hat{R}$ and hence $\hat{R} \neq \emptyset$. Now, suppose that $s, t \in \hat{R}$. Since s is integral over R as $s \in \hat{R}$, we know that $R[s]/R$ is an integral extension. Similarly, since t is integral over R as $t \in \hat{R}$ it is immediate

that t is integral over $R[s]$ and hence $R[s,t]/R[s]$ is an integral extension. Now, as $R[s,t]/R[s]$ and $R[s]/R$ are both integral extensions it follows by the previous Corollary that $R[s,t]/R$ is an integral extension. In particular, we may now assert that since clearly $s-t, st \in R[s,t]$ that $s-t$ and st are integral over R. Thus, by definition we see that $s-t, st \in \hat{R}$ and hence $\hat{R}$ is a subring of S.

Next, we show that $\hat{R}$ is an integral extension of R. First, suppose that $r \in R$. Then we have $f(x) = x - r \in R[x]$ is a monic polynomial in $R[x]$ with $f(r) = r - r = 0$ so that r is integral over R. In particular, this shows by definition that $R \subseteq \hat{R}$. Furthermore, note that the identity of S is in R since S is an extension ring of R. Therefore, since $R \subseteq \hat{R}$ it now follows that R contains the identity of $\hat{R}$. Since $\hat{R}$ is a ring by the above, we may now conclude that $\hat{R}$ is an extension ring of R. Finally, note that any element of $\hat{R}$ is integral over R by definition. Thus, we conclude that $\hat{R}/R$ is an integral extension.

Next, we show that $\hat{R}$ contains every subring of S that is integral over R. Towards this end, suppose that T is a subring of S such that T is an integral extension of R. Let $t \in T$. Since T is integral over R, we see that t is integral over R so that $t \in \hat{R}$ by definition. This observation shows that $T \subseteq \hat{R}$ so that $\hat{R}$ contains every subring of S that is integral over R.

Finally, suppose that S is an integral domain. Since $\hat{R}$ is a subring of S by the above, we see that $\hat{R}$ is a commutative ring. Furthermore, note that $\hat{R}$ has identity (namely, the identity of S) by the above and that this identity is not equal to 0 or else S would not be an integral domain. Lastly, it is immediate that $\hat{R}$ contains no zero divisors since $\hat{R} \subseteq S$ and as S contains no zero divisors as S is an integral domain. We conclude that $\hat{R}$ is an integral domain. □

Definition. The ring $\hat{R}$ from the above Corollary is called the ***integral closure*** of R in S.

Remark. Let R' denote the integral closure of $\hat{R}$, where $\hat{R}$ is as above. Then $R' = \hat{R}$.

Proof. By the above Corollaries, we know that $R'/\hat{R}$ and $\hat{R}/R$ are integral extensions so that R'/R is an integral extension. Appealing to the above Corollary, we know that $\hat{R}$ contains every subring of S that is integral over R. Therefore, since R' is a subring of S that is integral over R by the previous observation we see that $R' \subseteq \hat{R}$. Since we also clearly have $\hat{R} \subseteq R'$, this shows that $R' = \hat{R}$. □

Definition. Consider the ring extension $\mathbb{C}/\mathbb{Z}$. The elements of $\mathbb{C}$ which are integral over $\mathbb{Z}$ are called the ***algebraic integers***.

Example. The elements $\sqrt{2}, 1 + 3\sqrt{2} \in \mathbb{C}$ are algebraic integers.

Proof. To see that $\sqrt{2} \in \mathbb{C}$ is integral over $\mathbb{Z}$, consider the polynomial $f(x) = x^2 - 2 \in \mathbb{Z}[x]$. Then $f(x)$ is a monic polynomial in $\mathbb{Z}[x]$ with

$$f(\sqrt{2}) = (\sqrt{2})^2 - 2 = 0$$

and hence $\sqrt{2} \in \mathbb{C}$ is integral over $\mathbb{Z}$ so that $\sqrt{2}$ is an algebraic integer.

To see that $1+3\sqrt{2} \in \mathbb{C}$ is integral over $\mathbb{Z}$, consider the polynomials $g(x) = x - 1 \in \mathbb{Z}[x]$ and $h(x) = x^2 - 18 \in \mathbb{Z}[x]$. Then $g(x)$ and $h(x)$ are monic polynomials in $\mathbb{Z}[x]$ with

$$g(1) = 1 - 1 = 0 \quad \text{and} \quad h(3\sqrt{2}) = (3\sqrt{2})^2 - 18 = 18 - 18 = 0$$

and hence $1, 3\sqrt{2} \in \mathbb{C}$ are integral over $\mathbb{Z}$. Finally, we know that the elements of $\mathbb{C}$ which are integral over $\mathbb{Z}$ form a subring of $\mathbb{C}$ by the above Corollary. Therefore, since both $1, 3\sqrt{2} \in \mathbb{C}$ are integral over $\mathbb{Z}$ we see that their sum $1+3\sqrt{2} \in \mathbb{C}$ must also be integral over $\mathbb{Z}$ so that $1+3\sqrt{2} \in \mathbb{C}$ is an algebraic integer. This completes the proof. $\square$

Definition. Let S/R be a ring extension. Then S/R is called ***integrally closed*** (or we say that R is ***integrally closed in*** S) if $\hat{R} = R$.

More specifically, an integral domain R is said to be ***integrally closed*** if R is integrally closed in the field of fractions of R. We remark that if we say R is integrally closed without mentioning any other ring, then it is assumed that R is an integral domain and that R is integrally closed in the field of fractions of R.

Example. Consider $\mathbb{Z}$. Then $\mathbb{Z}$ is integrally closed. However, we see that $\mathbb{Z}$ is not integrally closed in $\mathbb{C}$.

Proof. First, we show that $\mathbb{Z}$ is integrally closed which means we must show that $\mathbb{Z}$ is integrally closed in the field of fractions $\mathbb{Q}$ of $\mathbb{Z}$. Towards this end, suppose that $a/b \in \mathbb{Q}$ is integral over $\mathbb{Z}$ and note that we may take a and b to be relatively prime integers. Now, by definition there is a monic polynomial $f(x) \in \mathbb{Z}[x]$ such that $f(a/b) = 0$. For definiteness, write

$$f(x) = x^n + c_{n-1}x^{n-1} + \cdots + c_1 x + c_0$$

so that

$$0 = f\left(\frac{a}{b}\right) = \frac{a^n}{b^n} + c_{n-1}\frac{a^{n-1}}{b^{n-1}} + \cdots + c_1\frac{a}{b} + c_0$$

Multiplying both sides of the above equality by b^n, we obtain

$$0 = a^n + c_{n-1}a^{n-1}b + \cdots + c_1 ab^{n-1} + c_0 b^n$$

so that

$$a^n = b(-c_{n-1}a^{n-1} - \cdots - c_1 ab^{n-2} - c_0 b^{n-1})$$

and hence b divides a^n. But as a and b are relatively prime integers, it follows that $b \in \{-1, 1\}$ and so either $a/b = a/1 = a \in \mathbb{Z}$ or $a/b = a/(-1) = -a \in \mathbb{Z}$. We conclude that $\mathbb{Z}$ is integrally closed in the field of fractions $\mathbb{Q}$ of $\mathbb{Z}$ so that $\mathbb{Z}$ is integrally closed.

Secondly, we show that $\mathbb{Z}$ is not integrally closed in $\mathbb{C}$. Indeed, recall by Example 1 that $\sqrt{2} \in \mathbb{C}$ is integral over $\mathbb{Z}$ but that clearly $\sqrt{2} \notin \mathbb{Z}$. In particular, this shows that $\mathbb{Z}$ is not integrally closed in $\mathbb{C}$. $\square$

Example. Let F be a field and consider the ideal $(X^2 - Y^3) \subseteq F[X, Y]$. Let $R = F[X, Y]/(X^2 - Y^3)$ and let x and y denote the class of X and Y, respectively, in R. Then $x/y \notin R$ but x/y is integral over R so that R is not integrally closed.

Proof. We begin by showing that $X^2 - Y^3$ is irreducible in $F[X,Y] = F[Y][X]$. Towards this end, we first show that $X^2 - Y^3$ is irreducible in $F(Y)[X]$. Indeed, note that $X^2 - Y^3$ is of degree 2 in $F(Y)[X]$, that $F(Y)$ is a field, and that $X^2 - Y^3$ clearly has no roots in $F(Y)$. By the previous observations, we see $X^2 - Y^3$ is irreducible in $F(Y)[X]$. Furthermore, note that the coefficients of $X^2 - Y^3 \in F[Y][X]$ are 1 and $-Y^3$ and are hence relatively prime in $F[Y]$ so that $X^2 - Y^3$ is a primitive polynomial in $F[Y][X]$. Thus, since $F(Y)$ is the field of fractions of $F[Y]$ we may now conclude by Gauss' Lemma that $X^2 - Y^3$ is irreducible in $F[Y][X] = F[X,Y]$.

By the above, we know that $X^2 - Y^3$ is an irreducible element of $F[X,Y]$ and hence $X^2 - Y^3$ is a prime element of $F[X,Y]$ since $F[X,Y]$ is a clearly a UFD. Therefore, we see that $(X^2 - Y^3)$ is a prime ideal of $F[X,Y]$ so that $R = F[X,Y]/(X^2 - Y^3)$ is an integral domain as $F[X,Y]$ is clearly commutative. We remark that the field of fractions of R consists of all elements of the form

$$\frac{f(X,Y) + (X^2 - Y^3)}{g(X,Y) + (X^2 - Y^3)} \quad \text{for some} \quad f(X,Y), g(X,Y) \in F[X,Y]$$

We now prove the main result.

Towards this end, we first show that $x/y \notin R$. For the sake of contradiction, suppose that $x/y \in R$. First, note that

$$\frac{x}{y} = \frac{X + (X^2 - Y^3)}{Y + (X^2 - Y^3)}$$

and since $x/y \in R$ it follows that there is some $f(X,Y) \in F[X,Y]$ such that

$$\frac{X + (X^2 - Y^3)}{Y + (X^2 - Y^3)} = f(X,Y) + (X^2 - Y^3)$$

However, the above equality implies that

$$\frac{X}{Y} - f(X,Y) \in (X^2 - Y^3)$$

which is clearly impossible. We conclude that $x/y \notin R$.

Next, we show that x/y is integral over R. Indeed, first note that

$$\begin{aligned}
\left(\frac{x}{y}\right)^2 &= \left[\frac{X + (X^2 - Y^3)}{Y + (X^2 - Y^3)}\right]^2 \\
&= \frac{X^2 + (X^2 - Y^3)}{Y^2 + (X^2 - Y^3)} \\
&= \frac{[X^2 - (X^2 - Y^3)] + (X^2 - Y^3)}{Y^2 + (X^2 - Y^3)} \\
&= \frac{Y^3 + (X^2 - Y^3)}{Y^2 + (X^2 - Y^3)} \\
&= Y + (X^2 - Y^3) \\
&= y
\end{aligned}$$

Therefore, if we define the polynomial

$$f(z) = z^2 - y \in R[z]$$

then we see that $f(z)$ is a monic polynomial in $R[z]$ and that, by the above, we also have

$$f\left(\frac{x}{y}\right) = \left(\frac{x}{y}\right)^2 - y = y - y = 0$$

Thus, combining the previous results shows that x/y is integral over R but that $x/y \notin R$. In particular, this shows that R is not integrally closed. This completes the proof. $\square$

Example. The integral closure $\hat{\mathbb{Z}}$ of $\mathbb{Z}$ in $\mathbb{Q}(i)$ is $\mathbb{Z}[i]$, the ***ring of Gaussian integers***.

Proof. Let $\hat{\mathbb{Z}}$ denote the integral closure of $\mathbb{Z}$ in $\mathbb{Q}(i)$ and let $f(x) = x^2 + 1 \in \mathbb{Z}[x]$. Then $f(x)$ is a monic polynomial in $\mathbb{Z}[x]$ and

$$f(i) = i^2 + 1 = -1 + 1 = 0$$

so that $i \in \mathbb{Q}(i)$ is integral over $\mathbb{Z}$. In particular, this shows that $\mathbb{Z}[i]$ is subring of $\mathbb{Q}(i)$ such that $\mathbb{Z}[i]$ is an integral extension of $\mathbb{Z}$. By the above Corollary, then, we obtain the inclusion $\mathbb{Z}[i] \subseteq \hat{\mathbb{Z}}$.

On the other hand, suppose for the sake of contradiction that there were some $a+bi \in \mathbb{Q}(i)$ such that $a+bi \in \hat{\mathbb{Z}}$ but $a+bi \notin \mathbb{Z}[i]$. Now, if $b = 0$ then $a = a+bi \in \hat{\mathbb{Z}}$ but $a = a+bi \notin \mathbb{Z}[i]$. In particular, these observations show that $a \in \mathbb{Q} - \mathbb{Z}$ is in $\hat{\mathbb{Z}}$. However, it follows that this would contradict the results from Example 2 above. Therefore, it must be the case that $b \neq 0$. Furthermore, note that by adding or subtracting elements from $\hat{\mathbb{Z}}$ and since $\hat{\mathbb{Z}}$ is a subring of $\mathbb{Q}(i)$ that we may assume $|a|, |b| < 1$. We will use both of these observations below.

Now, note that since $a + bi \in \hat{\mathbb{Z}}$ that $a + bi$ is a zero of a monic polynomial in $\mathbb{Z}[x]$ and thus $\overline{a + bi} = a - bi$ is also a zero of the same monic polynomial since $b \neq 0$ and as nonreal roots of polynomials in $\mathbb{Z}[x]$ come in complex conjugate pairs. Therefore, we see that since $\hat{\mathbb{Z}}$ is a ring that

$$2a = (a + bi) + (a - bi) \in \hat{\mathbb{Z}} \quad \text{and} \quad 2bi = (a + bi) - (a - bi) \in \hat{\mathbb{Z}}$$

Next, note that since $i \in \hat{\mathbb{Z}}$ by the above we have since $\hat{\mathbb{Z}}$ is a ring that $-i \in \hat{\mathbb{Z}}$ and hence by the same reasoning and since $2bi \in \hat{\mathbb{Z}}$ we see that

$$2b = -2bi^2 = (2bi)(-i) \in \hat{\mathbb{Z}}$$

Therefore, we obtain that $2a, 2b \in \hat{\mathbb{Z}}$. In addition, by the same reasoning as presented above we have

$$(a + bi)(a - bi) = a^2 + b^2 \in \hat{\mathbb{Z}}$$

We will use these observations below.

Finally, note that since $a, b \in \mathbb{Q}$ that clearly $2a, 2b, a^2 + b^2 \in \mathbb{Q}$. Thus, by our above result we may now conclude that $2a, 2b, a^2 + b^2 \in \mathbb{Q}$ are in $\hat{\mathbb{Z}}$ and hence it follows

by Example 2 above that $2a, 2b, a^2 + b^2 \in \mathbb{Z}$. But since $|a|, |b| < 1$, as $b \neq 0$, and as $2a, 2b \in \mathbb{Z}$ it now follows that

$$0 < a^2 + b^2 \leq \frac{1}{2}$$

which is clearly impossible since $a^2+b^2 \in \mathbb{Z}$. We may now conclude by this contradiction that $\hat{\mathbb{Z}} \subseteq \mathbb{Z}[i]$ and hence $\hat{\mathbb{Z}} = \mathbb{Z}[i]$, completing the proof. □

Theorem. (The Lying-Over Theorem) Let S be an integral extension of R and let P be a prime ideal of R. Then there is a prime ideal Q of S such that $Q \cap R = P$.

Proof. Since P is a prime ideal of R, we know that $R - P$ is a multiplicative subset of R and hence $R - P$ is a multiplicative subset of S. Furthermore, note that clearly $0 \notin R-P$ so that the zero ideal of S has an empty intersection with $R-P$. In particular, this shows that there is an ideal Q of S maximal among all of the ideals of S that have an empty intersection with $R-P$. Moreover, we know that this ideal Q is a prime ideal of S and since Q has an empty intersection with $R - P$ it follows that $Q \cap R \subseteq P$.

For the sake of contradiction, suppose that $Q \cap R \neq P$. By the previous inclusion and since $P \subseteq R$, this assumption implies that there is some element $u \in P$ such that $u \notin Q$. Now, note that $Q + Su$ is an ideal of S which properly contains Q since $u \notin Q$ and S has identity. Hence, by the maximality of Q we conclude that there is some $c \in (Q + Su) \cap (R - P)$ and so there exist elements $q \in Q$ and $s \in S$ such that $q + su = c \in (Q + Su) \cap (R - P)$.

Now, since $s \in S$ and as S is an integral extension of R there is a monic polynomial $f(x) \in R[x]$ such that $f(s) = 0$. For definiteness, write

$$f(x) = x^n + r_{n-1}x^{n-1} + \cdots + r_0 \in R[x]$$

so that

$$0 = f(s) = s^n + r_{n-1}s^{n-1} + \cdots + r_0$$

Multiplying both sides of the above equality by u^n gives

$$0 = s^n u^n + r_{n-1}s^{n-1}u^n + \cdots + r_0 u^n = (su)^n + r_{n-1}(su)^{n-1}u + \cdots + r_0 u^n$$

Notice that since the sum on the right-hand side of the equality is equal to 0 that this sum is in Q. Furthermore, since $c = su + q$ we have $su = c - q$. Thus, since $q \in Q$ and as Q is an ideal of S it now follows by the previous observations, the above equality, and the Binomial Theorem that if we define

$$v = c^n + r_{n-1}c^{n-1}u + \cdots + r_0 u^n$$

then $v \in Q$. Furthermore, since $c, r_{n-1}, \ldots, r_0, u \in R$ it follows by the definition of v that $v \in R$ so that $v \in Q \cap R \subseteq P$. In addition, since $u \in P$ and $v \in P$ by the previous result we have by the definition of v that $c^n \in P$ and since P is a prime ideal this implies that $c \in P$. However, this contradicts the fact that $c \notin P$. We conclude that $Q \cap R = P$ and since Q is a prime ideal of S, this completes the proof. □

Definition. In the situation of the above Theorem, we say that a prime ideal Q of S ***lies over*** a prime ideal P of R if $Q \cap R = P$.

Corollary. In the situation of the above Theorem, if I is any ideal of S such that $I \cap R \subseteq P$, then the prime ideal Q of S can be chosen such that $I \subseteq Q$.

Proof. Since $I \cap R \subseteq P$, we see $I \cap (R - P) = \emptyset$ and as Q is maximal among all ideals of S that have an empty intersection with $R - P$, it follows that $I \subseteq Q$. $\square$

Theorem. Let S be an integral extension of R and let Q be a prime ideal of S lying over a prime ideal P of R. Then Q is a maximal ideal of S if and only if P is a maximal ideal of R.

Proof. For the first direction, assume that Q is a maximal ideal of S lying over the prime ideal P of R so that $Q \cap R = P$. Since P is a proper ideal of R as P is a prime ideal of R, it follows that there is some maximal ideal M of R such that $P \subseteq M$. Now, since M is a maximal ideal of R we have in particular that M is a prime ideal of R. Moreover, we have $Q \cap R = P \subseteq M$. By these observations and the above Corollary, it now follows that there is a prime ideal Q_1 of S such that $Q_1 \cap R = M$ and $Q \subseteq Q_1$.

Now, since Q_1 is a prime ideal of S we have in particular that $Q_1 \neq S$. Therefore, since $Q \subseteq Q_1$ and as Q is a maximal ideal of S this implies that $Q = Q_1$. By the above results, this now gives

$$P = Q \cap R = Q_1 \cap R = M$$

so that $P = M$. Thus, since M is a maximal ideal of R we conclude that P is a maximal ideal of R. This completes the proof of the first direction.

For the second direction, assume that P is a maximal ideal of R and that Q is a prime ideal of S lying over P so that $Q \cap R = P$. Since Q is a proper ideal of S as Q is a prime ideal of S, it follows that there is some maximal ideal M_0 of S such that $Q \subseteq M_0$. Since $Q \cap R = P$, this inclusion gives

$$P = Q \cap R \subseteq M_0 \cap R$$

Furthermore, note that $1 \notin M_0 \cap R$ since M_0 is a maximal ideal of S. In particular, since R and S share the same identity as S is a ring extension of R this implies that $M_0 \cap R$ is a proper ideal of R which contains the maximal ideal P of R. Therefore, we have that $M_0 \cap R = P$ so that

$$M_0 \cap R = P = Q \cap R$$

We will use this observation below.

For the sake of contradiction, assume that $Q \neq M_0$. Since $Q \subseteq M_0$, this assumption implies that there is some $s \in M_0$ such that $s \notin Q$. Now, since $s \in S$ and as S is an integral extension of R there is a monic polynomial $g(x) \in R[x]$ such that $g(s) = 0 \in Q$. By this observation, it follows that we can choose a polynomial $f(x) \in R[x]$ of smallest degree such that $f(s) \in Q$. For definiteness, write

$$f(x) = x^n + r_{n-1}x^{n-1} + \cdots + r_0 \in R[x]$$

so that

$$s^n + r_{n-1}s^{n-1} + \cdots + r_0 = f(s) \in Q \subseteq M_0$$

Now, since $s \in M_0$ and as M_0 is an ideal the above result forces $r_0 \in M_0$ and hence $r_0 \in M_0 \cap R = Q \cap R$. Therefore, we see that

$$s(s^{n-1} + r_{n-1}s^{n-2} + \cdots + r_1) = s^n + r_{n-1}s^{n-1} + \cdots + r_1 s = f(s) - r_0 \in Q$$

But since Q is a prime ideal of S and $s \notin Q$, the previous result implies that

$$s^{n-1} + r_{n-1}s^{n-2} + \cdots + r_1 \in Q$$

However, this implies that if we define the polynomial

$$h(x) = x^{n-1} + r_{n-1}x^{n-2} + \cdots r_1 \in R[x]$$

then $h(x)$ is of strictly smaller degree than $f(x)$ and $h(s) \in Q$ which is a contradiction. We conclude that $Q = M_0$ and since M_0 is a maximal ideal of S, we have that Q is a maximal ideal of S. This completes the proof of the second direction. $\square$

Topic 7: Fractional Ideals; Dedekind Domains

Definition. A ***fractional ideal*** of a domain R is a nonzero R-submodule I of its field of fractions such that $aI \subseteq R$ for some nonzero $a \in R$.

Remark. In the situation of Definition 1, we set K to be the field of fractions of R. Furthermore, throughout the next few lectures we will assume that R is a domain with field of fractions K.

Remark. Every nonzero finitely generated R-submodule of K is a fractional ideal.

Proof. Let I be a nonzero finitely generated R-submodule of K. Clearly, it remains to prove the existence of a nonzero element $b \in R$ such that $bI \subseteq R$. Now, since I is a finitely generated R-submodule of K there is a finite number of elements

$$\frac{a_1}{b_1}, \dots, \frac{a_n}{b_n} \in I \subseteq F$$

where $b_1, \dots, b_n \neq 0$ which generate I as an R-module so that we may write

$$I = R\frac{a_1}{b_1} + \cdots + R\frac{a_n}{b_n}$$

Let $b = b_1 \cdots b_n$. Since clearly $b_1, \dots, b_n \in R$, we have $b \in R$ and as R is an integral domain and $b_1, \dots, b_n \neq 0$ we have $b \neq 0$. Furthermore, we have by the above that

$$bI = b\left(R\frac{a_1}{b_1} + \cdots + R\frac{a_n}{b_n}\right) = R(b_2 \cdots b_n a_1) + \cdots + R(b_1 \cdots b_{n-1} a_n) \subseteq R$$

We conclude that I is a fractional ideal of R. $\square$

Remark. Let I be a fractional ideal of R so that there is some nonzero $a \in R$ with $aI \subseteq R$. Then I and aI are isomorphic as R-modules.

Proof. It is immediate that aI is an R-module since I is an R-module. Now, define

$$\phi : I \to aI \quad \text{by} \quad i \mapsto ai$$

Clearly, we see that ϕ is well-defined. We claim that ϕ is an R-module isomorphism. Towards this end, first let $i_1, i_2 \in I$ and $r \in R$. Then since R is commutative and as $a, r \in R$, we have

$$\begin{aligned}
\phi(ri_1 + i_2) &= a(ri_1 + i_2) \\
&= a(ri_1) + ai_2 \\
&= (ar)i_1 + ai_2 \\
&= (ra)i_1 + ai_2 \\
&= r(ai_1) + ai_2 \\
&= r\phi(i_1) + \phi(i_2)
\end{aligned}$$

so that ϕ is an R-module homomorphism. Next, we show that ϕ is an injection. Since ϕ is an R-module homomorphism, it suffices to show that $\ker\phi$ is trivial to establish that ϕ is an injection. Towards this end, let $i \in \ker\phi$. Then

$$0 = \phi(i) = ai$$

Thus, since R is an integral domain we have by the above equality that either $a = 0$ or $i = 0$. But since $a \neq 0$, we obtain $i = 0$ and hence $\ker\phi$ is trivial so that ϕ is an injection. Finally, let $ai \in aI$. Then clearly $i \in I$ and $\phi(i) = ai$ so that ϕ is a surjection. We conclude that ϕ is an R-module isomorphism so that I and aI are isomorphic as R-modules. □

Example. The fractional ideals of $\mathbb{Z}$ are $q\mathbb{Z}$ for $q \in \mathbb{Q}, q \neq 0$.

Proof. Let I be a fractional ideal of $\mathbb{Z}$. Then I is a nonzero $\mathbb{Z}$-submodule of $\mathbb{Q}$ and there is some nonzero $a \in \mathbb{Z}$ such that $aI \subseteq \mathbb{Z}$. Now, notice that aI is a nonzero $\mathbb{Z}$-submodule of $\mathbb{Z}$ so that aI is a nonzero ideal of $\mathbb{Z}$. Thus, since $\mathbb{Z}$ is a PID there is some nonzero $b \in \mathbb{Z}$ such that $aI = (b)$. Let $q = b/a \in \mathbb{Q}$ and notice that since $a, b \in \mathbb{Z}$ are nonzero that $q \in \mathbb{Q}$ is nonzero. Furthermore, we claim that $I = q\mathbb{Z}$.

Indeed, first let $i \in I$. Then $ai \in aI = (b)$ and so there is some $n \in \mathbb{Z}$ such that $ai = nb$. Thus, we obtain

$$i = \frac{nb}{a} = \frac{b}{a}n \in \frac{b}{a}\mathbb{Z} = q\mathbb{Z}$$

On the other hand, let $qn \in q\mathbb{Z}$. Notice that since $aI = (b)$, we have $I = \frac{1}{a}(b)$. By this observation, we obtain

$$qn = \frac{b}{a}n = \frac{1}{a}nb \in \frac{1}{a}(b) = I$$

and thus $I = q\mathbb{Z}$.

Now, let $q \in \mathbb{Q}, q \neq 0$ and consider $q\mathbb{Z}$. Since $q \in \mathbb{Q}$ is nonzero, we see that $q\mathbb{Z}$ is a nonzero $\mathbb{Z}$-submodule of $\mathbb{Q}$. Next, since $q \in \mathbb{Q}$ is nonzero, there are nonzero elements $a, b \in \mathbb{Z}$ such that $q = b/a$. Therefore, we obtain since $b \in \mathbb{Z}$ that

$$a(q\mathbb{Z}) = a\left(\frac{b}{a}\mathbb{Z}\right) = b\mathbb{Z} \subseteq \mathbb{Z}$$

Thus, since $a \in \mathbb{Z}$ is nonzero the above result shows that $q\mathbb{Z}$ is a fractional ideal of $\mathbb{Z}$. We conclude that the fractional ideals of $\mathbb{Z}$ are $q\mathbb{Z}$ for $q \in \mathbb{Q}, q \neq 0$. □

Definition. If I and J are fractional ideals of R, then IJ is defined to be the R-submodule of K generated by ij for $i \in I$ and $j \in J$. In other words, we have

$$IJ = \left\{ \sum_{i=1}^{n} a_i b_i : a_i \in I, b_i \in J \text{ for } i \in \{1, \ldots, n\} \right\}$$

Theorem. The fractional ideals of R form a monoid with identity R under multiplication.

Proof. Let I and J be fractional ideals of R. Then I and J are nonzero R-submodules of K and there are nonzero elements $a, b \in R$ such that $aI, bJ \subseteq R$. Now, note that since K is a field and as I and J are nonzero R-submodules of K we have that IJ is a nonzero R-submodule of K. Furthermore, since $a, b \in R$ are nonzero elements of R and as R is an integral domain we have that $ab \in R$ is a nonzero element of R and

$$(ab)IJ = (aI)(bJ) \subseteq R$$

The above results show that IJ is a fractional ideal of R.

Next, note that if I, J, K are fractional ideals of R then we clearly have $I(JK) = (IJ)K$ so that the above operation is associative. Finally, let I be a fractional ideal of R. We claim that $RI = I = IR$. Towards this end, let $x = \sum_{j=1}^{n} r_j i_j \in RI$. Since I is an R-module, we have $r_1 i_1, \ldots, r_n i_n \in I$ so that $x = \sum_{j=1}^{n} r_j i_j \in I$. On the other hand, suppose that $x \in I$. Then as R has identity, we have $x = 1x \in RI$. We conclude that $RI = I$. Similarly, we also have $IR = I$ and hence R is an identity. Combining the previous results, we see the fractional ideals of R form a monoid with identity R. $\square$

Definition. A fractional ideal I of R is ***invertible*** if I is invertible as an element of the monoid of fractional ideals of R.

Definition. If I is a fractional ideal of R, we define

$$I^{-1} = \{a \in K : aI \subseteq R\}$$

Remark. The set I^{-1} from Definition 4 is a fractional ideal of R.

Proof. First, we show that I^{-1} is a nonzero R-submodule of K. Notice that since I is a fractional ideal of R, there is some nonzero $a \in R \subseteq K$ such that $aI \subseteq R$ so that $a \in I^{-1}$ which shows that I^{-1} is both nonempty and nonzero. Next, suppose that $a, b \in I^{-1}$. Then $a - b \in K$ and $aI, bI \subseteq R$ so that

$$(a - b)I = aI - bI \subseteq R$$

so that $a - b \in I^{-1}$ which shows that I^{-1} is an abelian subgroup of K under addition since K is a field.

Now, define an action of R on I^{-1} by multiplication. To see that this is indeed an action of R on I^{-1}, let $a \in I^{-1}$ and $r \in R$. It is immediate that $ra \in K$. Now, since $a \in I^{-1}$ we have $aI \subseteq R$ and since $r \in R$, this gives

$$(ra)I = r(aI) \subseteq rR = R$$

and thus $ra \in I^{-1}$ so that this is indeed an action of R on I^{-1}. Finally, it is easily verified that the module axioms hold so that by the above results we have that I^{-1} is a nonzero R-submodule of K.

Finally, note that as I is a fractional ideal of R that I is nonzero and so there is some nonzero element $b \in I$. Since $b \in I \subseteq K$ is nonzero, we can write $b = c/d$ for some nonzero elements $c, d \in R$. Thus, since I is an R-submodule of K and as $d \in R$ we have

$$c = d\frac{c}{d} \in I$$

and hence $c \in I \cap R$ is a nonzero element of $I \cap R$. We claim that $cI^{-1} \subseteq R$. Towards this end, let $a \in I^{-1}$. Then $aI \subseteq R$ by definition and hence

$$ca = ac \in aI \subseteq R$$

so that as $a \in I^{-1}$ was arbitrary we have $cI^{-1} \subseteq R$. In particular, since $c \in R$ is nonzero this inclusion completes the proof that I^{-1} is a fractional ideal of R. □

Remark. If I is invertible, then I^{-1} is the inverse of I.

Proof. Since I is invertible, there is some fractional ideal J of R such that $JI = R$. Now, let $j \in J$. Then $j \in K$ and if $i \in I$ we have

$$ji \in JI = R$$

so that $jI \subseteq R$ which shows that $j \in I^{-1}$. On the other hand, notice that since I^{-1} is a fractional ideal of R by the above proof and as R is an identity in the monoid of fractional ideals of R we have

$$I^{-1} = RI^{-1} = (JI)I^{-1} = J(II^{-1})$$

Now, we claim that $II^{-1} \subseteq R$. Indeed, let $\sum_{i=1}^{n} a_i b_i \in II^{-1}$. In order to show that $\sum_{i=1}^{n} a_i b_i \in R$, it suffices to show that each summand in this sum is in R since R is a ring. Towards this end, consider $a_1 b_1$. Since $b_1 \in I^{-1}$, we have that $b_1 I \subseteq R$ so that since $a_1 \in I$ we have

$$a_1 b_1 = b_1 a_1 \in b_1 I \subseteq R$$

so that $a_1 b_1 \in R$. We conclude that $\sum_{i=1}^{n} a_i b_i \in R$ and hence $II^{-1} \subseteq R$, as claimed. Finally, we now have by the above results and since J is an R-submodule of K that

$$I^{-1} = J(II^{-1}) \subseteq JR = J$$

and thus $J = I^{-1}$. This completes the proof. □

Example. If R is a PID, then every fractional ideal of R is invertible.

Proof. Let R be a PID and suppose that I is a fractional ideal of R. By definition, there is some nonzero $a \in R$ such that $aI \subseteq R$. As follows by the same arguments presented in proofs from the previous lecture, we have that aI is a nonzero ideal of R and hence since R is a PID there is some nonzero $b \in R$ such that $aI = (b)$ so that $I = \frac{1}{a}(b)$.

Next, since $b \in R$ is nonzero it follows that we may define define $J = \frac{a}{b}R$. In particular, since a is nonzero we see by the definition of J that J is a nonzero R-submodule of K. Moreover, notice that since $a \in R$ we have

$$bJ = b\left(\frac{a}{b}R\right) = aR \subseteq R$$

and since $b \in R$ is nonzero it follows by the above inclusion and the previous observation that J is a fractional ideal of R.

Finally, we show that J is the inverse of I. Indeed, by the above results we have

$$JI = \left(\frac{a}{b}R\right)\left(\frac{1}{a}(b)\right) = \frac{1}{b}R(b) = R$$

The above equality shows that J is the inverse of I in the monoid of fractional ideals of R and hence I is invertible. This completes the proof. $\square$

Example. Let K be a field and let (x, y) be the ideal generated by x and y in $K[x, y]$. Then we have

$$(x, y)^{-1}(x, y) \subseteq (x, y)$$

In particular, since $(x, y) \neq K[x, y]$ we see (x, y) is not an invertible ideal of $K[x, y]$.

Proof. First, recall by definition that

$$(x, y)^{-1} = \{r \in K(x, y) : r(x, y) \subseteq K[x, y]\}$$

We claim that $(x, y)^{-1} \subseteq K[x, y]$. Towards this end, let $r \in (x, y)^{-1}$. If $r = 0$, then clearly $r \in K[x, y]$. Therefore, assume that $r \neq 0$. Notice that since $K(x, y)$ is a field, we have in particular that $K(x, y)$ is a UFD. Therefore, since $r \in K(x, y)$ is nonzero it follows that we may write $r = \epsilon p_1^{n_1} \cdots p_m^{n_m}$ where ϵ is a unit of $K[x, y]$, $p_1, \ldots, p_m$ are prime elements of $K[x, y]$, $n_1, \ldots, n_m \in \mathbb{Z}$, and $p_1, \ldots, p_m$ are pairwise relatively prime.

Now, since $r \in (x, y)^{-1}$ we have $r(x, y) \subseteq K[x, y]$ so that in particular we obtain $rx, ry \in r(x, y) \subseteq K[x, y]$. Furthermore, note that since clearly

$$\frac{K[x, y]}{(x)} \simeq K[y] \quad \text{and} \quad \frac{K[x, y]}{(y)} \simeq K[x]$$

and as $K[y]$ and $K[x]$ are clearly integral domains that the ideals (x) and (y) are prime ideals of $K[x, y]$ and hence x and y are prime elements of $K[x, y]$. By the previous observations, it follows that if x is relatively prime to $p_1, \ldots, p_m$ that $n_1, \ldots, n_m \geq 0$ and if y is relatively prime to $p_1, \ldots, p_m$ that $n_1, \ldots, n_m \geq 0$. Moreover, it must be the case that at least one of these situations holds.

Finally, since at least one of the previously-described situations must hold we conclude that $n_1, \ldots, n_m \geq 0$. In other words, we now have

$$r = \epsilon p_1^{n_1} \cdots p_m^{n_m} \in K[x, y]$$

and since $r \in (x, y)^{-1}$ was arbitrary this shows that $(x, y)^{-1} \subseteq K[x, y]$. This gives

$$(x, y)^{-1}(x, y) \subseteq K[x, y](x, y) = (x, y)$$

which establishes the first result. In addition, note that since clearly $1 \in K[x, y]$ but $1 \notin (x, y)$ that $(x, y) \neq K[x, y]$. Thus, since $K[x, y]$ is the identity of the monoid of fractional ideals of $K[x, y]$ and as $(x, y)^{-1}(x, y) \neq K[x, y]$ by the above inclusion it follows that (x, y) is not an invertible ideal of $K[x, y]$. This completes the proof. $\square$

Lemma. Let $I_1, \ldots, I_n$ be nonzero ideals of an integral domain R.

(a): The product $I_1 \cdots I_n$ is an invertible ideal of R if and only if I_j is an invertible ideal of R for each $j \in \{1, \ldots, n\}$.

(b): If $P_1 \cdots P_m = Q_1 \cdots Q_n$, where $P_1, \ldots, P_m, Q_1, \ldots, Q_n$ are prime ideals of R and each of $P_1, \ldots, P_m$ is invertible, then $m = n$ and after reindexing if necessary we have $Q_i = P_i$ for each $i \in \{1, \ldots, m\}$.

Proof. (a): For the first direction, assume that $I_1 \cdots I_n$ is an invertible ideal of R and let J be the inverse of $I_1 \cdots I_n$ in the monoid of fractional ideals of R so that $JI_1 \cdots I_n = R$. Now, fix any $j \in \{1, \ldots, n\}$ and consider the ideal I_j. Notice that I_j and $JI_1 \cdots I_{j-1} I_{j+1} \cdots I_n$ are clearly a fractional ideals of R and that by the above we have

$$(JI_1 \cdots I_{j-1} I_{j+1} \cdots I_n) I_j = JI_1 \cdots I_n = R$$

We conclude that I_j is an invertible ideal of R and as $j \in \{1, \ldots, n\}$ was arbitrary this completes the proof of the first direction.

For the second direction, assume that $I_1, \ldots, I_n$ are invertible ideals of R and let $I_1^{-1}, \ldots, I_n^{-1}$ be the respective inverses of $I_1, \ldots, I_n$ in the monoid of fractional ideals of R so that $I_j I_j^{-1} = R$ for each $j \in \{1, \ldots, n\}$. Then we clearly have that $I_1 \cdots I_n$ is a fractional ideal of R and that

$$(I_1 \cdots I_n)(I_1^{-1} \cdots I_n^{-1}) = (I_1 I_1^{-1}) \cdots (I_n I_n^{-1}) = R \cdots R = R$$

By the above equality, we conclude that $I_1^{-1} \cdots I_n^{-1}$ is the inverse of $I_1 \cdots I_n$ in the monoid of fractional ideals of R so that $I_1 \cdots I_n$ is an invertible ideal of R. This completes the proof of the second direction. □

Proof. (b): We will prove this by induction on m. If $m = 0$ then

$$R = P_1 \cdots P_m = Q_1 \cdots Q_n$$

But since $Q_1, \ldots, Q_n$ are prime ideals of R, we have in particular that $Q_1, \ldots, Q_n$ are properly contained in R so that $Q_1 \cdots Q_n$ must also be properly contained in R. By the above equality, then, we conclude that $n = 0$ and so the desired result holds in this case.

Now, assume that $m \geq 1$. After reordering $P_1, \ldots, P_m$ if necessary, assume that P_1 is minimal among the ideals $P_1, \ldots, P_m$ and note that

$$Q_1 \cdots Q_n = P_1 \cdots P_m \subseteq P_1$$

For the sake of contradiction, suppose that $Q_i \not\subseteq P_1$ for each $i \in \{1, \ldots, n\}$. In this case, there are elements $q_i \in Q_i - P_1$ for each $i \in \{1, \ldots, n\}$ and hence by the above inclusion we have that

$$q_1 \cdots q_n \in Q_1 \cdots Q_n \subseteq P_1$$

But since P_1 is a prime ideal of R, it now follows that since $q_1 \cdots q_n \in P_1$ that there is some $j \in \{1, \ldots, n\}$ such that $q_j \in P_1$. However, this contradicts the fact that $q_j \in Q_j - P_1$. Thus, after reordering $Q_1, \ldots, Q_n$ if necessary, we have that $Q_1 \subseteq P_1$.

Similarly as above, notice that

$$P_1 \cdots P_m = Q_1 \cdots Q_n \subseteq Q_1$$

Thus, by the same argument as presented above that allowed us to conclude that $Q_1 \subseteq P_1$ we have that $P_j \subseteq Q_1$ for some $j \in \{1, \ldots, m\}$. Thus, by the above result we now have

$$P_j \subseteq Q_1 \subseteq P_1$$

and since P_1 was chosen to be minimal among $P_1, \ldots, P_m$ it follows by the above inclusion that $P_j = P_1$. Combining the previous inclusions, we now obtain

$$P_1 = P_j \subseteq Q_1 \subseteq P_1$$

and hence $Q_1 = P_1$.

Finally, recall that by hypothesis we have that P_1 is an invertible ideal of R so that $P_1^{-1}P_1 = R$. But since $P_1 = Q_1$, this gives $P_1^{-1}Q_1 = R$. Thus, we obtain

$$\begin{aligned} P_2 \cdots P_m &= RP_2 \cdots P_m \\ &= (P_1^{-1}P_1)P_2 \cdots P_m \\ &= P_1^{-1}(P_1 \cdots P_m) \\ &= P_1^{-1}(Q_1 \cdots Q_n) \\ &= (P_1^{-1}Q_1)Q_2 \cdots Q_n \\ &= RQ_2 \cdots Q_n \\ &= Q_2 \cdots Q_n \end{aligned}$$

By induction, the above equality completes the proof. □

Definition. A ***Dedekind domain*** is an integral domain R such that every nonzero ideal of R that is properly contained in R is a product of a finite number of prime ideals of R.

Theorem. Let R be a Dedekind domain. Then every nonzero prime ideal of R is invertible and maximal.

Proof. Let P be a nonzero prime ideal of R. We first show that P is a maximal ideal of R. For the sake of contradiction, suppose that P were not a maximal ideal of R. Then there is some $a \in R$ with $a \notin P$ with $P + aR \neq R$. Now, notice that $P + a^2R \subseteq P + aR \neq R$. Furthermore, we have that $P + aR$ and $P + a^2R$ are clearly nonzero ideals of R since P is a nonzero ideal of R. Therefore, since R is Dedekind there are prime ideals $P_1, \ldots, P_m$ and $Q_1, \ldots, Q_n$ of R such that $P + aR = P_1 \cdots P_m$ and $P + a^2R = Q_1 \cdots Q_n$.

Next, let $\pi : R \to R/P$ be the canonical projection map. Then since π is a surjective ring homomorphism with $\ker \pi = P$, we have that

$$\begin{aligned} \pi(P_1) \cdots \pi(P_m) &= \pi(P_1 \cdots P_m) \\ &= \pi(P + aR) \\ &= \pi(P) + \pi(aR) \\ &= 0 + \pi(a)\pi(R) \\ &= \pi(a)R/P \\ &= (\pi(a)) \end{aligned}$$

so that

$$\begin{aligned}\pi(Q_1)\cdots\pi(Q_n) &= \pi(Q_1\cdots Q_n)\\ &= \pi(P+a^2R)\\ &= \pi(P)+\pi(a^2R)\\ &= 0+\pi(a^2)\pi(R)\\ &= \pi(a^2)R/P\\ &= (\pi(a^2))\\ &= (\pi(a))^2\\ &= (\pi(P_1)\cdots\pi(P_m))^2\\ &= \pi(P_1)^2\cdots\pi(P_m)^2\end{aligned}$$

which gives the equality

$$\pi(Q_1)\cdots\pi(Q_n) = \pi(P_1)^2\cdots\pi(P_m)^2$$

Now, we have since P is a prime ideal of R that R/P is an integral domain. In addition, since $a \notin P$ it follows that $\pi(a) \neq 0$ so that the ideal $(\pi(a))$ is nonzero. Thus, since $(\pi(a))$ is a nonzero principal ideal of the integral domain R/P it follows that $(\pi(a))$ is an invertible ideal of R/P so that $(\pi(a))^2$ is also an invertible ideal of R/P. Furthermore, notice that

$$\ker\pi = P \subseteq P + aR = P_1\cdots P_m \subseteq P_1,\ldots,P_m$$

and

$$\ker\pi = P \subseteq P + a^2R = Q_1\cdots Q_n \subseteq Q_1,\ldots,Q_n$$

so that

$$\ker\pi = P \subseteq P_1,\ldots,P_m,Q_1,\ldots,Q_n$$

Hence, by the above result and since $P_1,\ldots,P_m$ and $Q_1,\ldots,Q_n$ are prime ideals of R we see $\pi(P_1),\ldots,\pi(P_m),\pi(Q_1),\ldots,\pi(Q_n)$ are prime ideals of R/P. Moreover, recall that

$$(\pi(a))^2 = \pi(Q_1)\cdots\pi(Q_n)$$

is an invertible ideal of R/P so that $\pi(Q_1),\ldots,\pi(Q_n)$ are invertible ideals of R/P by the Lemma from the previous lecture. Therefore, since $\pi(Q_1),\ldots,\pi(Q_n),\pi(P_1),\ldots,\pi(P_m)$ are prime ideals of R/P, since $\pi(Q_1),\ldots,\pi(Q_n)$ are invertible ideals of R/P, and since

$$\pi(Q_1)\cdots\pi(Q_n) = \pi(P_1)^2\cdots\pi(P_m)^2$$

we again have by the Lemma from the previous lecture that $n = 2m$ and after reindexing if necessary we have

$$\pi(Q_1)=\pi(Q_2)=\pi(P_1) \quad \pi(Q_3)=\pi(Q_4)=\pi(P_2) \quad \cdots \quad \pi(Q_{2m-1})=\pi(Q_{2m})=\pi(P_m)$$

We will use these equalities below.

Towards this end, recall that

$$\ker\pi = P \subseteq P_1,\ldots,P_m,Q_1,\ldots,Q_n$$

By this observation and the previous results, we obtain the equalities

$$Q_1 = Q_2 = P_1 \quad Q_3 = Q_4 = P_2 \quad \cdots \quad Q_{2m-1} = Q_{2m} = P_m$$

so that

$$P + a^2R = Q_1 \cdots Q_n = P_1^2 \cdots P_m^2 = (P_1 \cdots P_m)^2 = (P + aR)^2$$

This gives that

$$P \subseteq P + a^2R = (P + aR)^2 \subseteq P^2 + aR$$

We will use this result to show that $P = P^2 + aP$. First, note that we clearly have $P^2 + aP \subseteq P$. On the other hand, let $p \in P$. Then $p \in P^2 + aR$ by the above inclusion so that there are elements $c \in P^2 \subseteq P$ and $r \in R$ such that $p = c + ar$. Thus, we obtain $ar = p - c \in P$ so that either $a \in P$ or $r \in P$ since P is a prime ideal of R. But since $a \notin P$, we have $r \in P$ and hence $ar \in aP$. Since $c \in P^2$, this gives that $p = c + ar \in P^2 + aP$ and hence $P = P^2 + aP$.

Now, we have $P = P^2 + aP = P(P + aR)$. Suppose that P is an invertible ideal of R and let P^{-1} denote the inverse of P in the monoid of fractional ideals of R so that $P^{-1}P = R$. Then we now have

$$R = P^{-1}P = P^{-1}(P(P + aR)) = (P^{-1}P)(P + aR) = R(P + aR) = P + aR$$

which contradicts the fact that $P + aR \neq R$. Therefore, we conclude that any nonzero invertible prime ideal of R is a maximal ideal of R.

Next, suppose that P is a nonzero prime ideal of R and let $c \in P$ be nonzero. Then $(c) \subseteq P$ is a nonzero principal ideal of R and hence is an invertible ideal of R. Now, since P is a prime ideal we have $P \neq R$ so that since $(c) \subseteq P$ we have $(c) \neq R$. Therefore, since R is Dedekind there are prime ideals $P_1, \ldots, P_n$ of R with $(c) = P_1 \cdots P_n$ and since (c) is an invertible ideal of R it follows that $P_1, \ldots, P_n$ are invertible ideals of R.

Finally, note that we have $P_1 \cdots P_n = (c) \subseteq P$ and since P is a prime ideal of R it follows by previously-presented arguments that there is some $N \in \{1, \ldots, n\}$ with $P_N \subseteq P$. Now, since P_N is an invertible prime ideal of R so that by our first result above we have that P_N is a maximal ideal of R. But recall that P is a prime ideal of R so that in particular we have $P \neq R$. Thus, since P_N is a maximal ideal of R and $P_N \subseteq P$ we must have $P = P_N$ and hence P is an invertible and maximal ideal of R since P_N is an invertible and maximal ideal of R. This completes the proof. $\square$

Lemma. Let I be a fractional ideal of an integral domain R. Then if $f \in \mathrm{Hom}_R(I, R)$ and $a, b \in I$ we have $af(b) = bf(a)$.

Proof. Let $a = r_1/s_1$ and $b = r_2/s_2$ for some $r_1, r_2, s_1, s_2 \in R$ where $s_1 \neq 0$ and $s_2 \neq 0$. Since $f \in \mathrm{Hom}_R(I, R)$, then, we obtain

$$\begin{aligned} s_1 s_2 a f(b) &= s_1 s_2 \frac{r_1}{s_1} f\left(\frac{r_2}{s_2}\right) \\ &= s_2 r_1 f\left(r_2 \cdot \frac{1}{s_2}\right) \\ &= s_2 r_1 r_2 f\left(\frac{1}{s_2}\right) \\ &= r_1 r_2 f\left(\frac{s_2}{s_2}\right) \\ &= r_1 r_2 f(1) \\ &= f(r_1 r_2) \end{aligned}$$

By the same reasoning, we have

$$\begin{aligned} f(r_1 r_2) &= f\left(r_1 r_2 \cdot \frac{s_1}{s_1}\right) \\ &= s_1 r_2 f\left(\frac{r_1}{s_1}\right) \\ &= s_1 r_2 \cdot \frac{s_2}{s_2} f\left(\frac{r_1}{s_1}\right) \\ &= s_1 s_2 \frac{r_2}{s_2} f\left(\frac{r_1}{s_1}\right) \\ &= s_1 s_2 b f(a) \end{aligned}$$

Combining the previous results, we obtain $s_1 s_2 a f(b) = s_1 s_2 b f(a)$. Thus, since R is an integral domain we may cancel the term $s_1 s_2$ on both sides of this equality to obtain $a f(b) = b f(a)$. This completes the proof. □

Lemma. Let R be an integral domain. Then every invertible fractional ideal of R is finitely generated as an R-module.

Proof. Let I be an invertible fractional ideal of R and let J be an inverse of I in the monoid of fractional ideals of R so that $JI = R$. Now, we have $1 \in R = JI$ so that we may write $1 = j_1 i_1 + \cdots + j_n i_n$ for some $j_1, \ldots, j_n \in J$ and $i_1, \ldots, i_n \in I$. We claim that $I = (i_1, \ldots i_n)$. Clearly, we have that $(i_1, \ldots, i_n) \subseteq I$ since $i_1, \ldots, i_n \in I$ and as I is an ideal of R. On the other hand, let $x \in I$. Then we have $xj_1, \ldots, xj_n \in IJ = JI = R$ and since $1 = j_1 i_1 + \cdots + j_n i_n$, we also have $x = xj_1 i_1 + \cdots xj_n i_n$. Combining the previous results, we obtain

$$x = xj_1 i_1 + \cdots + xj_n i_n = (xj_1) i_1 + \cdots + (xj_n) i_n \in (i_1, \ldots, i_n)$$

and hence we conclude that $I = (i_1, \ldots, i_n)$ so that I is finitely generated as an R-module. This completes the proof. □

Theorem. Let R be an integral domain and I a fractional ideal of R. Then I is invertible if and only if I is a projective R-module.

Proof. For the first direction, suppose that I is an invertible fractional ideal of R. Let J be an inverse of I in the monoid of fractional ideals of R so that $JI = R$. Thus, we may write $1 = \sum_{i=1}^{n} a_i b_i$ for some $a_1, \ldots, a_n \in J$ and $b_1, \ldots, b_n \in I$. Furthermore, by the above Lemma we know that $I = (b_1, \ldots, b_n)$. Now, let F be a free R-module with basis $\{e_1, \ldots, e_n\}$ and define

$$\pi : F \to I \quad \text{by} \quad \sum_{i=1}^{n} \lambda_i e_i \mapsto \sum_{i=1}^{n} \lambda_i b_i$$

Since $I = (b_1, \ldots, b_n)$, it is immediate that π is a surjective R-module homomorphism. This observation gives that

$$0 \longrightarrow \ker \pi \xrightarrow{\ i\ } F \xrightarrow{\ \pi\ } I \longrightarrow 0$$

where i is the inclusion map is a short exact sequence of R-modules.

Now, define

$$\zeta : I \to F \quad \text{by} \quad c \mapsto \sum_{i=1}^{n} (ca_i) e_i$$

Clearly, we have that ζ is a well-defined R-module homomorphism. Moreover, observe that if $c \in I$ then we have

$$(\pi \circ \zeta)(c) = \pi(\zeta(c)) = \pi\left(\sum_{i=1}^{n} (ca_i) e_i\right) = \sum_{i=1}^{n} (ca_i) b_i = c \sum_{i=1}^{n} a_i b_i = c \cdot 1 = c$$

so that $\pi \circ \zeta = 1_I$. Therefore, we see that our short exact sequence above splits so that $F \simeq \ker \pi \oplus I$. In particular, since I is a direct summand of the free R-module F it follows that I is a projective R-module. This completes the proof of the first direction.

For the second direction, suppose that I is a projective R-module and let $(b_j)_{j \in J}$ be a set of generators for I. Let F be a free R-module with basis $(e_j)_{j \in J}$ and let $\pi : F \to I$ be the R-module homomorphism defined by $\pi(e_j) = b_j$ for each $j \in J$. Since the set of generators $(b_j)_{j \in J}$ for I is in the image of π, it follows that π is a surjection. Therefore, since P is a projective R-module, it follows by an argument that has been showcased several times in previous lectures there is an R-module homomorphism $\zeta : I \to F$ such that $\pi \circ \zeta = 1_I$.

Now, let $\pi_j : F \to R$ be the jth canonical projection map and note that since the defined composition of R-module homomorphisms is an R-module homomorphism that $\pi_j \circ \zeta : I \to R$ is an R-module homomorphism for each $j \in J$. Next, let $b \in I$ with $b \neq 0$. Then since $\pi_j \circ \zeta$ is an R-module homomorphism, we have by a Lemma from the previous lecture that

$$c \cdot \frac{\pi_j(\zeta(b))}{b} = \frac{c\pi_j(\zeta(b))}{b} = \frac{b\pi_j(\zeta(c))}{b} = \pi_j(\zeta(c)) \in R \quad \text{for each} \quad c \in I, j \in J$$

In particular, the above result shows that

$$\frac{\pi_j(\zeta(b))}{b} I \subseteq R$$

and hence

$$\frac{\pi_j(\zeta(b))}{b} \in I^{-1}$$

for each nonzero element $b \in I$ and each $j \in J$.

Finally, notice that since $\pi \circ \zeta = 1_I$ we have that

$$\begin{aligned} b &= 1_I(b) \\ &= (\pi \circ \zeta)(b) \\ &= \pi(\zeta(b)) \\ &= \sum_{j \in J} \pi_j(\zeta(b)) b_j \\ &= \sum_{j \in J_0} \pi_j(\zeta(b)) b_j \end{aligned}$$

for all $b \in I$ and where J_0 is some finite subset of J. Hence, by the above equality we have that

$$1 = \frac{1}{b} \cdot \sum_{j \in J_0} \pi_j(\zeta(b)) b_j = \sum_{j \in J_0} \frac{\pi_j(\zeta(b))}{b} b_j$$

which shows that $1 \in I^{-1}I$ by the above result. Hence, we now have that $R \subseteq I^{-1}I$. On the other hand, recall that $J^{-1}J \subseteq R$ for any fractional ideal J of R so that $I^{-1}I \subseteq R$. We conclude that $I^{-1}I = R$ and hence I is invertible in the monoid of fractional ideals of R so that I is invertible. This completes the proof. $\square$

Definition. A ***discrete valuation ring*** (abbreviated DVR) is a PID that has exactly one nonzero prime ideal.

Lemma. Let R be a Noetherian integrally closed integral domain and suppose that R has a unique nonzero prime ideal P. Then R is a DVR.

Note: We will prove several facts before proving the main result. Furthermore, we remark that since P is the unique nonzero prime ideal of R and since any maximal ideal of R is a prime ideal of R that P is the unique maximal ideal of R.

Fact 1. Let K be the field of fractions of R and let I be any fractional ideal of R. Define the set

$$\overline{I} = \{a \in K : aI \subseteq I\}$$

Then $\overline{I} = R$.

Proof. Since I is a fractional ideal of R, we have in particular that I is an R-submodule of K so that $R \subseteq \overline{I}$. We now prove the reverse inclusion. Towards this end, we first

show that $\overline{I}$ is a subring of K. Indeed, since $R \subseteq \overline{I}$ we have that $\overline{I} \neq \emptyset$. Next, let $a, b \in \overline{I}$ so that $aI, bI \subseteq I$. Then we have

$$(a-b)I = aI - bI \subseteq I$$

so that $a - b \in \overline{I}$. Furthermore, we have

$$(ab)I = a(bI) \subseteq aI \subseteq I$$

so that $ab \in \overline{I}$ and hence $\overline{I}$ is a subring of K.

Next, we show that $\overline{I}$ is a fractional ideal of R. First, note that since $R \subseteq \overline{I}$ we have that $\overline{I}$ is nonzero. Now, suppose that $a \in \overline{I}$ and $r \in R$. Then since I is an R-submodule of K and $r \in R$, we have

$$(ra)I = r(aI) \subseteq rI \subseteq I$$

so that $ra \in \overline{I}$. In particular, since I is an R-submodule of K it follows by this result that $\overline{I}$ is an R-submodule of K. Finally, note that since I is a fractional ideal of R that there is some nonzero element $r \in R$ with $rI \subseteq R$. Furthermore, since I is a fractional ideal of R we have in particular that I is nonzero and hence there is a nonzero element $i \in I$. Now, we have that $ri \in rI \subseteq R$ and since r and i are nonzero it follows that $ri \neq 0$. Let $a \in \overline{I}$ so that $aI \subseteq I$. In particular, we have since $i \in I$ that $ai \in aI \subseteq I$ and hence $r(ai) \in rI \subseteq R$. The previous results now give that

$$(ri)a = r(ia) = r(ai) \in R$$

and since $a \in \overline{I}$ was arbitrary, we conclude that $(ri)\overline{I} \subseteq R$. Thus, since $ri \in R$ is nonzero we may now conclude that $\overline{I}$ is a fractional ideal of R.

Finally, note that since $\overline{I}$ is a fractional ideal of R that $\overline{I}$ is isomorphic as an R-module to an ideal of R. Since R is Noetherian, then, it follows that $\overline{I}$ is finitely generated as an R-module. Thus, since $\overline{I}$ is a subring of K which is finitely generated as an R-module it follows that every element of $\overline{I}$ is integral over R. But since R is integrally closed, this observation implies that $\overline{I} \subseteq R$. We may now conclude that $\overline{I} = R$. $\square$

Fact 2. We have $R \subsetneq P^{-1}$.

Proof. Let $\mathcal{F}$ denote the set of all ideals J of R such that $J \neq 0$ and $R \subsetneq J^{-1}$. We claim that $\mathcal{F}$ is nonempty. Towards this end, first note that since P is nonzero we may choose a nonzero element $a \in P$ and define $J = (a)$ so that J is an ideal of R with $J \neq 0$. Now, since P is a prime ideal of R we have in particular that $P \neq R$ and hence it follows that as $a \in P$ that $(a) = J \subseteq P \neq R$. Therefore, we see that a is not a unit of R so that $\frac{1}{a} \notin R$. On the other hand, notice that since $J = (a)$ we clearly have $\frac{1}{a}J \subseteq R$ and hence we see that $\frac{1}{a} \in J^{-1}$. Thus, we obtain that $\frac{1}{a} \notin R$ but $\frac{1}{a} \in J^{-1}$ and since clearly $R \subseteq J^{-1}$ as J is an ideal of R this result shows that $R \subsetneq J^{-1}$. Therefore, we have that $J \in \mathcal{F}$ so that $\mathcal{F} \neq \emptyset$. This completes the proof of our claim and since R is Noetherian, it now follows that there is a maximal element $M \in \mathcal{F}$.

We now show that M is a prime ideal of R. For the sake of contradiction, suppose that $M = R$. In this case, we have that $M^{-1} = R^{-1} = R$ which contradicts the fact that $R \subsetneq M^{-1}$. Therefore, we see that $M \neq R$. Next, suppose that $a, b \in R$ with $ab \in M$

and $a \notin M$. As $R \subsetneq M^{-1}$, there is some element $c \in M^{-1} - R$. Now, since $c \in M^{-1}$ we have $cM \subseteq R$ and hence as $ab \in M$ we have $c(ab) \in cM \subseteq R$. Thus, it now follows that $bc(aR + M) \subseteq R$ so that $bc \in (aR + M)^{-1}$. Notice that $aR + M \supsetneq M$ as $a \notin M$ and as R has 1. In particular, this shows by the maximality of $M \in \mathcal{F}$ that $R = (aR + M)^{-1}$ so that $bc \in (aR + M)^{-1} = R$.

Finally, note that since $bc \in R$ and as $cM \subseteq R$ that $c(bR + M) \subseteq R$ which gives that $c \in (bR + M)^{-1}$. Thus, since $c \notin R$ it follows by the maximality of $M \in \mathcal{F}$ that $bR + M = M$ and hence $b \in M$. We may now conclude that M is a prime ideal of R. But recall that P is the unique nonzero prime ideal of R. Therefore, since M is a nonzero prime ideal of R we see that $M = P$ and hence $R \subsetneq M^{-1} = P^{-1}$. □

Fact 3. We have that P is an invertible ideal of R.

Proof. Since $P \subseteq R$ is an ideal of R, it follows that $1 \in P^{-1}$ and hence $P \subseteq PP^{-1}$. Furthermore, since clearly $PP^{-1} \subseteq R$ it follows that PP^{-1} is an ideal of R. Therefore, since P is a maximal ideal of R the inclusion $P \subseteq PP^{-1}$ implies that either $PP^{-1} = P$ or $PP^{-1} = R$. Suppose that $PP^{-1} = P$. In this case, then, we have that $P^{-1} \subseteq \overline{P}$. But recall by Fact 2 that $R \subsetneq P^{-1}$ so that we now obtain the inclusion $R \subsetneq P^{-1} \subseteq \overline{P}$. In particular, we may now conclude that $\overline{P} \neq R$. However, this contradicts Fact 1. Therefore, we conclude that $PP^{-1} = R$ and hence P is an invertible ideal of R. □

Fact 4. We have that $\bigcap_{n=1}^{\infty} P^n = \{0\}$.

Proof. Let $I = \bigcap_{n=1}^{\infty} P^n$ and for the sake of contradiction, suppose that $I \neq \{0\}$. Now, since the intersection of ideals is an ideal it follows that I is an ideal of R and since $I \neq \{0\}$ we see that I is a fractional ideal of R. We claim that $P^{-1} \subseteq \overline{I}$. Indeed, let $a \in P^{-1}$ so that $aP \subseteq R$ and note that we must show $aI \subseteq I$ in order to conclude that $a \in \overline{I}$. Towards this end, let $b \in I$ so that $b \in P^n$ for each integer $n \geq 1$ and fix an integer $N \geq 1$. In order to prove that $aI \subseteq I$, it will suffice to show that $ab \in P^N$ since the fixed integer $N \geq 1$ is arbitrary.

Now, since $b \in P^{N+1}$ it follows that b is equal to a finite sum of elements of the form $p_1 p_2 \cdots p_{N+1}$ where $p_1, p_2, \ldots, p_{N+1} \in P$. Therefore, in order to show that $ab \in P^N$ it suffices to show that a multiplied by any element of the form in the previous sentence is in P^N. Indeed, let $p_1, p_2, \ldots p_{N+1} \in P$ and consider the element $p_1 p_2 \cdots p_{N+1} \in P^{N+1}$. Notice that $ap_1 \in aP \subseteq R$ so that $ap_1 \in R$. Therefore, since P^N is an ideal of R and as clearly $p_2 \cdots p_{N+1} \in P^N$ we obtain

$$ap_1 p_2 \cdots p_{N+1} = (ap_1) p_2 \cdots p_{N+1} \in P^N$$

By our previous observations, this completes the proof of our claim that $P^{-1} \subseteq \overline{I}$.

Finally, recall by Fact 2 that $R \subsetneq P^{-1}$. By the above result, we now obtain the inclusion $R \subsetneq P^{-1} \subseteq \overline{I}$. In particular, this inclusion shows that $\overline{I} \neq R$. However, this contradicts Fact 1. Therefore, we conclude that $\bigcap_{n=1}^{\infty} P^n = I = \{0\}$. □

Fact 5. We have that P is a principal ideal of R.

Proof. First, recall that P is nonzero. For the sake of contradiction, suppose that $P = P^2$. Then by this assumption and by Fact 4, we see

$$\{0\} \neq P = \bigcap_{n=1}^{\infty} P^n = \{0\}$$

which is clearly a contradiction. Therefore, we see that $P \neq P^2$ and since clearly $P^2 \subseteq P$ this result shows that $P \subsetneq P^2$. Hence, there is some element $\pi \in P - P^2$. Now, notice that since $\pi \in P$ we have $\pi P^{-1} \subseteq R$ so that πP^{-1} is an ideal of R.

Now, for the sake of contradiction suppose that $\pi P^{-1} \subseteq P$. Since P is an invertible ideal of R by Fact 3, we have that $P^{-1}P = R$. By the previous inclusion, then, we see

$$\pi R = \pi(P^{-1}P) = (\pi P^{-1}) \cdot P \subseteq P \cdot P = P^2$$

so that $\pi R \subseteq P^2$. However, since R has 1 and $\pi \in P \subseteq R$ this implies that

$$\pi = \pi \cdot 1 \in \pi R \subseteq P^2$$

which contradicts the fact that $\pi \notin P^2$. Therefore, we conclude that $\pi P^{-1} \nsubseteq P$.

Finally, recall that πP^{-1} is an ideal of R and that P is a maximal ideal of R. Therefore, since $\pi P^{-1} \nsubseteq P$ it must be the case that $\pi P^{-1} = R$. Again using the fact that $P^{-1}P = R$, we obtain by this equality that

$$\pi R = \pi(P^{-1}P) = (\pi P^{-1}) \cdot P = R \cdot P = RP = P$$

so that $P = \pi R$. Hence, we see that P is principal. This completes the proof. □

Proof. We prove the main result here. Note that by hypothesis, we need only show that R is a PID to conclude that R is a DVR. Towards this end, let I be an ideal of R and for the sake of contradiction suppose that I is not principal so that $\{0\} \neq I \neq R$. Now, since P is the unique maximal ideal of R and as I is a proper ideal of R it follows that $I \subseteq P$. Furthermore, if $I \subseteq P^n$ for each integer $n \geq 1$ then

$$\{0\} \neq I \subseteq \bigcap_{n=1}^{\infty} P^n$$

which contradicts Fact 4. Therefore, since $I \subseteq P$ it follows that there exists an integer $n_0 \geq 1$ such that $I \subseteq P^{n_0}$ but $I \nsubseteq P^{n_0+1}$.

Now, since $I \nsubseteq P^{n_0+1}$ there is some element $a \in I - P^{n_0+1}$. Furthermore, if π is as in the proof of Fact 5 then by the same proof we know that $P = \pi R$ so that $P^{n_0} = \pi^{n_0} R$ and $P^{n_0+1} = \pi^{n_0+1} R$. Thus, we now have that $a \in I \subseteq P^{n_0} = \pi^{n_0} R$ and hence there is some $u \in R$ such that $a = \pi^{n_0} u$. For the sake of contradiction, suppose that $u \in P$. Then $u \in P = \pi R$ so that $u = \pi r$ for some $r \in R$. By the above results, this gives

$$a = \pi^{n_0} u = \pi^{n_0} \cdot \pi r = \pi^{n_0+1} r \in \pi^{n_0+1} R = P^{n_0+1}$$

which contradicts the fact that $a \notin P^{n_0+1}$. Therefore, we conclude that $a \notin P$.

Finally, note that since $a \notin P$ and as P is the unique maximal ideal of R that a is a unit of R. Therefore, since $a = \pi^{n_0} u$ it now follows a and π^{n_0} are associate elements

of R and hence a and π^{n_0} generate the same ideal of R. Thus, by the above results and since $a \in I$ this gives that

$$\pi^{n_0} R = aR \subseteq I \subseteq P^{n_0} = \pi^{n_0} R$$

Therefore, the above inclusions are actually equalities so that $I = \pi^{n_0} R$ and hence I is a principal ideal of R. However, this contradicts our assumption that I is not principal. We conclude that every ideal of R is principal and hence R is a PID. By our initial observation, then, this completes the proof. $\square$

Topic 8: Affine Varieties; Hilbert's Nullstellensatz

Theorem. (Noether's Normalization Lemma) Let R be an integral domain which is a finitely generated extension of a field K and let $r < \infty$ be the transcendence degree of the field extension F/K, where F is the field of fractions of R. Then there is an algebraically independent subset $\{t_1, \ldots, t_r\}$ of R such that R is integral over $K[t_1, \ldots, t_r]$.

Note: We have the inclusion $K \subseteq R \subseteq F$.

Proof. Assume this is false and let n be the smallest number of generators for R as a ring extension of K. Then $n \geq r$ so that among all counterexamples, we may choose one with $n - r$ as small as possible. Now, let $u_1, \ldots, u_n \in R$ be such that $R = K[u_1, \ldots, u_n]$. If the set $\{u_1, \ldots, u_n\}$ is algebraically independent over K, then we clearly have no counterexample. Therefore, the set $\{u_1, \ldots, u_n\}$ is algebraically dependent over K and hence there exists a dependence relation

$$\sum_{(i_1,\ldots,i_n)\in I} k_{i_1,\ldots,i_n} u_1^{i_1} \cdots u_n^{i_n}$$

where I is a nonempty, finite subset of $\underbrace{\mathbb{N} \times \cdots \times \mathbb{N}}_{n \text{ times}}$ and $k_{i_1,\ldots,i_n} \in K^\times$ for each element $(i_1, \ldots, i_n) \in I$.

Now, let $c \in \mathbb{Z}$ be larger than every component i_s which appears in any element $(i_1, \ldots, i_n) \in I$ and for each $(i_1, \ldots, i_n) \in I$ define $f(i_1, \ldots, i_n) = \sum_{\ell=1}^{n} i_\ell c^{\ell-1} \in \mathbb{N}$. Then f is a map $f : I \to \mathbb{N}$. Furthermore, notice that f is an injective function on the nonempty, finite set I and hence since $f : I \to \mathbb{N}$ it follows that there is some unique element $(j_1, \ldots, j_n) \in I$ such that $f(j_1, \ldots, j_n)$ gives the maximum value of f.

Next, for each $i \in \{2, \ldots, n\}$ define $v_i = u_i - u_1^{c^{i-1}}$ so that $u_i = v_i + u_1^{c^{i-1}}$. Then by the above dependence relation, we obtain the equality

$$k_{j_1,\ldots,j_n} u_1^{j_1 + cj_2 + c^2 j_3 + \cdots + c^{n-1} j_n} + g(u_1, v_2, v_3, \ldots, v_n) = 0$$

where $g(x_1, \ldots, x_n) \in K[x_1, \ldots, x_n]$ has degree in x_1 strictly less than $f(j_1, \ldots, j_n)$. Furthermore, since $k_{j_1,\ldots,j_n} \in K^\times$ we may divide both sides of the above equality by $k_{j_1,\ldots,j_n}$ so that u_1 is a root of the *monic* polynomial

$$x^{j_1 + cj_2 + c^2 j_3 + \cdots + c^{n-1} j_n} + \frac{1}{k_{j_1,\ldots,j_n}} g(x, v_2, v_3, \ldots, v_n) \in K[v_2, \ldots, v_n][x]$$

In particular, this shows that u_1 is integral over $K[v_2, \ldots, v_n]$.

Finally, notice by our choice of counterexample that the Theorem holds for the ring extension $K[v_2, \ldots, v_n]$ of K. Therefore, there are elements $t_1, \ldots, t_r \in K[v_2, \ldots, v_n]$ such that the set $\{t_1, \ldots, t_r\}$ is algebraically independent over K and $K[v_2, \ldots, v_n]$ is integral over $K[t_1, \ldots, t_r]$. Furthermore, recall that u_1 is integral over $K[v_2, \ldots, v_n]$ so that by the above we have that $K[u_1, v_2, \ldots, v_n]$ is integral over $K[t_1, \ldots, t_r]$. Also, note that by the definition of $v_2, \ldots, v_n$ we clearly have that $u_1, u_2, \ldots, u_n$ are integral over $K[u_1, v_2, \ldots, v_n]$. Thus, we conclude that $K[u_1, \ldots, u_n]$ is integral over $K[t_1, \ldots, t_r]$ so

that since $R = K[u_1, \ldots, u_n]$ we have that R is integral over $K[t_1, \ldots, t_r]$. This final contradiction completes the proof. $\square$

Definition. Let F/K be a field extension. For a subsets $S \subseteq K[x_1, \ldots, x_n]$, define

$$V(S) = \{(a_1, \ldots, a_n) \in F^n : \text{ for all } f \in S \text{ we have } f(a_1, \ldots, a_n) = 0\}$$

Then we call $V(S)$ an ***algebraic set*** or an ***affine*** K***-variety***.

Definition. Let F/K be a field extension. For subsets $Y \subseteq F^n$, define

$$J(Y) = \{f \in K[x_1, \ldots, x_n] : f(a_1, \ldots, a_n) = 0 \text{ for all } (a_1, \ldots, a_n) \in Y\}$$

Remark. The set $J(Y)$ from the above definition is an ideal of $K[x_1, \ldots, x_n]$.

Proof. Note that the zero polynomial in $K[x_1, \ldots, x_n]$ is clearly in $J(Y)$ so that in particular we have $J(Y) \neq \emptyset$. Next, let $f(x_1, \ldots, x_n), g(x_1, \ldots, x_n) \in J(Y)$ and $(a_1, \ldots, a_n) \in Y$. Then by definition, we have

$$f(a_1, \ldots, a_n) = 0 = g(a_1, \ldots, a_n)$$

so that

$$(f - g)(a_1, \ldots, a_n) = f(a_1, \ldots, a_n) - g(a_1, \ldots, a_n) = 0 - 0 = 0$$

so that $(f - g)(x_1, \ldots, x_n) \in J(Y)$ so that $J(Y)$ is a subgroup of $K[x_1, \ldots, x_n]$ under addition. Finally, let $f(x_1, \ldots, x_n) \in J(Y), g(x_1, \ldots, x_n) \in K[x_1, \ldots, x_n]$, and $(a_1, \ldots, a_n) \in Y$ so that $f(a_1, \ldots, a_n) = 0$ by definition. Then we obtain

$$(gf)(a_1, \ldots, a_n) = g(a_1, \ldots, a_n)f(a_1, \ldots, a_n) = g(a_1, \ldots, a_n) \cdot 0 = 0$$

so that $(fg)(x_1, \ldots, x_n) \in J(Y)$. We conclude that $J(Y)$ is an ideal of $K[x_1, \ldots, x_n]$. $\square$

Remark. We have that F^n and $\emptyset$ are algebraic sets.

Proof. First, let $S = \emptyset$. Then by definition, we have

$$V(S) = \{(a_1, \ldots, a_n) \in F^n : \text{ for all } f \in S \text{ we have } f(a_1, \ldots, a_n) = 0\} = F^n$$

so that F^n is an algebraic set. Secondly, let $S \subseteq K[x_1, \ldots, x_n]$ be such that the polynomial $1 \in S$. Then by definition, we have

$$V(S) = \{(a_1, \ldots, a_n) \in F^n : \text{ for all } f \in S \text{ we have } f(a_1, \ldots, a_n) = 0\} = \emptyset$$

so that $\emptyset$ is an algebraic set. $\square$

Remark. If $(A_i)_{i \in I}$ is a collection of algebraic sets, then $\bigcap_{i \in I} A_i$ is an algebraic set.

Proof. Since A_i is an algebraic set, there is some set $S_i \subseteq K[x_1, \ldots, x_n]$ such that $A_i = V(S_i)$ for each $i \in I$. We claim that $\bigcap_{i \in I} A_i = V\left(\bigcup_{i \in I} S_i\right)$.

Towards this end, first let $(a_1, \ldots, a_n) \in \bigcap_{i \in I} A_i$ and let $f(x_1, \ldots, x_n) \in \bigcup_{i \in I} S_i$ so that $f(x_1, \ldots, x_n) \in S_j$ for some $j \in I$. Now, we have in particular that $(a_1, \ldots, a_n) \in A_j$ since $(a_1, \ldots, a_n) \in \bigcap_{i \in I} A_i$. Thus, since $A_j = V(S_j)$ and $f(x_1, \ldots, x_n) \in S_j$ we obtain

that $f(a_1, \ldots, a_n) = 0$. Since $f(x_1, \ldots, x_n) \in \bigcup_{i \in I} S_i$ was arbitrary, it now follows that $(a_1, \ldots, a_n) \in V\left(\bigcup_{i \in I} S_i\right)$.

On the other hand, let $(a_1, \ldots, a_n) \in V\left(\bigcup_{i \in I} S_i\right)$ so that $f(a_1, \ldots, a_n) = 0$ for each $f(x_1, \ldots, x_n) \in \bigcup_{i \in I} S_i$. Now, fix any element $j \in I$ and let $f(x_1, \ldots, x_n) \in S_j \subseteq \bigcup_{i \in I} S_i$ so that by our previous observation we have $f(a_1, \ldots, a_n) = 0$. Thus, since $f(x_1, \ldots, x_n) \in S_j$ was arbitrary it now follows that $(a_1, \ldots, a_n) \in V(S_j) = A_j$. Finally, recall that the fixed element $j \in I$ was arbitrary and so we conclude that $(a_1, \ldots, a_n) \in \bigcap_{i \in I} A_i$. This completes the proof that $\bigcap_{i \in I} A_i = V\left(\bigcup_{i \in I} S_i\right)$ and hence $\bigcap_{i \in I} A_i$ is an algebraic set. □

Remark. If $S_1, S_2 \subseteq K[x_1, \ldots, x_n]$, then $V(S_1) \cup V(S_2) = V(S_1 S_2)$.

Proof. Before we begin, note that if either $S_1 = \emptyset$ or $S_2 = \emptyset$ then either $V(S_1) = F^n$ or $V(S_2) = F^n$. Furthermore, notice that in this case we also have $S_1 S_2 = \emptyset$ so that $V(S_1 S_2) = F^n$. Hence, we obtain

$$V(S_1) \cup V(S_2) = F^n = V(S_1 S_2)$$

so that the result is true in this case. Therefore, assume that $S_1 \neq \emptyset$ and $S_2 \neq \emptyset$.

First, let $(a_1, \ldots, a_n) \in V(S_1) \cup V(S_2)$ and assume without loss of generality that $(a_1, \ldots, a_n) \in V(S_1)$ so that $f(a_1, \ldots, a_n) = 0$ for each $f(x_1, \ldots, x_n) \in S_1$. Now, let $h(x_1, \ldots, x_n) \in S_1 S_2$ so that we may write

$$h(x_1, \ldots, x_n) = f(x_1, \ldots, x_n) g(x_1, \ldots, x_n)$$

for some $f(x_1, \ldots, x_n) \in S_1$ and $g(x_1, \ldots, x_n) \in S_2$. In particular, since $f(x_1, \ldots, x_n) \in S_1$ we have by our initial observation that $f(a_1, \ldots, a_n) = 0$ so that

$$h(a_1, \ldots, a_n) = f(a_1, \ldots, a_n) g(a_1, \ldots, a_n) = 0 \cdot g(a_1, \ldots, a_n) = 0$$

Thus, since $h(x_1, \ldots, x_n) \in S_1 S_2$ was arbitrary we may now conclude by the above equality that $(a_1, \ldots, a_n) \in V(S_1 S_2)$.

On the other hand, let $(a_1, \ldots, a_n) \in V(S_1 S_2)$ so that $h(a_1, \ldots, a_n) = 0$ for each $h(x_1, \ldots, x_n) \in S_1 S_2$. Now, assume that $(a_1, \ldots, a_n) \notin V(S_2)$ so that there is some polynomial $g(x_1, \ldots, x_n) \in S_2$ such that $g(a_1, \ldots, a_n) \neq 0$ and fix any polynomial $f(x_1, \ldots, x_n) \in S_1$. Then clearly, we have

$$h(x_1, \ldots, x_n) = f(x_1, \ldots, x_n) g(x_1, \ldots, x_n) \in S_1 S_2$$

so that by our initial observation we obtain

$$0 = h(a_1, \ldots, a_n) = f(a_1, \ldots, a_n) g(a_1, \ldots, a_n)$$

Thus, by the above equality we must have $f(a_1, \ldots, a_n) = 0$ since $g(a_1, \ldots, a_n) \neq 0$ and since $f(x_1, \ldots, x_n) \in S_1$ was arbitrary the above equality also shows that $(a_1, \ldots, a_n) \in V(S_1) \subseteq V(S_1) \cup V(S_2)$. This completes the proof. □

Question. If I is an ideal of $K[x_1, \ldots, x_n]$ and $I \neq K[x_1, \ldots, x_n]$, then $V(I) \neq \emptyset$? In general, the answer to this question is no.

For example, let $K = \mathbb{R} = F$ and consider the ideal $I = (f(x,y)) \subseteq \mathbb{R}[x,y]$ of $\mathbb{R}[x,y]$ where $f(x,y) = x^2 + y^2 + 1$. In particular, notice that $f(x,y)$ is an irreducible element of $\mathbb{R}[x,y]$ and since $\mathbb{R}[x,y]$ is a UFD as $\mathbb{R}$ is a field this implies that $f(x,y)$ is a prime element of $\mathbb{R}[x,y]$. Therefore, the ideal $I = (f(x,y))$ is a prime ideal of $\mathbb{R}[x,y]$ so that in particular we have $I \neq \mathbb{R}[x,y]$. On the other hand, however, notice that the equation

$$f(x,y) = x^2 + y^2 + 1 = 0$$

clearly has no solutions in $\mathbb{R}^2$ and thus we have that $V(I) = V((f(x,y))) = \emptyset$.

Remark. In the context of Question 1, if F is an algebraically closed field then the answer to Question 1 is yes. We state this formally as follows.

Theorem. (Lemma for Hilbert's Nullstellensatz): Let F be an algebraically closed extension field of a field K and I an ideal of $K[x_1, \ldots, x_n]$ such that $I \neq K[x_1, \ldots, x_n]$. Then $V(I) \neq \emptyset$ over F^n.

Remark. If I is an ideal of $K[x_1, \ldots, x_n]$ such that $I \neq K[x_1, \ldots, x_n]$ and $(a_1, \ldots, a_n) \in V(I)$, then there is a ring homomorphism

$$\phi_{(a_1,\ldots,a_n)} : K[x_1, \ldots, x_n]/I \to F$$

which is the identity map on K/I.

Proof. Define a map

$$\phi : K[x_1, \ldots, x_n] \to F \quad \text{by} \quad f(x_1, \ldots, x_n) \mapsto f(a_1, \ldots, a_n)$$

and note that ϕ is clearly a ring homomorphism. Now, suppose $f(x_1, \ldots, x_n) \in I$. Then since $(a_1, \ldots, a_n) \in V(I)$, we have by definition that $f(a_1, \ldots, a_n) = 0$. In particular, we now have that $f(x_1, \ldots, x_n) \in \ker \phi$ and since $f(x_1, \ldots, x_n) \in I$ was arbitrary we obtain that $I \subseteq \ker \phi$. Hence, there exists a (unique) ring homomorphism

$$\phi_{(a_1,\ldots,a_n)} : K[x_1, \ldots, x_n]/I \to F$$

such that

$$\phi_{(a_1,\ldots,a_n)}(f(x_1, \ldots, x_n) + I) = \phi(f(x_1, \ldots, x_n)) \quad \text{for each} \quad f(x_1, \ldots, x_n) \in K[x_1, \ldots, x_n]$$

In particular, suppose that $a + I \in K/I \subseteq K[x_1, \ldots, x_n]/I$. Then we have

$$\phi_{(a_1,\ldots,a_n)}(a + I) = \phi(a) = a$$

so that $\phi_{(a_1,\ldots,a_n)}$ is the identity map on K/I. This completes the proof. $\square$

Remark. Conversely, suppose that I is an ideal of $K[x_1, \ldots, x_n]$ such that $I \neq K[x_1, \ldots, x_n]$ and that

$$\phi : K[x_1, \ldots, x_n]/I \to F$$

is a ring homomorphism such that ϕ is the identity on K/I. Then the element

$$(\phi(x_1 + I), \ldots, \phi(x_n + I)) \in F^n$$

is an element of $V(I)$.

Proof. Let $f(x_1, \ldots, x_n) \in I \subseteq K[x_1, \ldots, x_n]$. Then since $f(x_1, \ldots, x_n) \in I$ we have

$$f(x_1, \ldots, x_n) + I = I$$

so that

$$\phi(f(x_1, \ldots, x_n) + I) = \phi(I) = 0$$

Furthermore, since the ring homomorphism ϕ is the identity on K/I we obtain

$$\phi(f(x_1, \ldots, x_n) + I) = f(\phi(x_1 + I), \ldots, \phi(x_n + I))$$

Combining the above equalities now gives

$$f(\phi(x_1 + I), \ldots, \phi(x_n + I)) = \phi(f(x_1, \ldots, x_n) + I) = 0$$

Thus, since $f(x_1, \ldots, x_n) \in I$ was arbitrary the above equality shows that

$$(\phi(x_1 + I), \ldots, \phi(x_n + I)) \in V(I)$$

This completes the proof. □

Proof. (Lemma for Hilbert's Nullstellensatz): Since $I \neq K[x_1, \ldots, x_n]$ is an ideal of $K[x_1, \ldots, x_n]$, it follows that there is some maximal ideal M of $K[x_1, \ldots, x_n]$ such that $I \subseteq M$. Furthermore, since $I \subseteq M$ it is immediate that $V(M) \subseteq V(I)$. Therefore, it suffices to show that $V(M) \neq \emptyset$ in order to conclude that $V(I) \neq \emptyset$.

Towards this end, define $R = K[x_1, \ldots, x_n]/M$ and note that since M is a maximal ideal of $K[x_1, \ldots, x_n]$ that R is a field. Let $\pi : K[x_1, \ldots, x_n] \to R$ be the canonical projection map. Now, note that we clearly have $\ker \pi \cap K = \{0\}$ and hence it follows that $\pi(K) \simeq K$ so that $\pi(K)$ is a field as K is a field. Furthermore, recall that $R = K[x_1, \ldots, x_n]/M$ so that

$$R = \pi(K)[x_1 + M, \ldots, x_n + M]$$

which shows that R is a finitely generated ring extension of $\pi(K)$. Moreover, recall that R and $\pi(K)$ are fields so that $R/\pi(K)$ is a field extension. Therefore, we may let $r < \infty$ denote the transcendence degree of R over $\pi(K)$. Combining the previous two observations, we may appeal to Noether's Normalization Lemma to assert that there is an algebraically independent subset $\{t_1, \ldots, t_r\} \subseteq R$ of R over $\pi(K)$ such that R is integral over $S = \pi(K)[t_1, \ldots, t_r]$.

Next, let $M_0 \subseteq S$ be the ideal of S generated by the set $\{t_1, \ldots, t_r\}$. Then since the set $\{t_1, \ldots, t_r\}$ is algebraically independent over $\pi(K)$, it follows that

$$S/M_0 = \pi(K)[t_1, \ldots, t_r]/(t_1, \ldots, t_r) \simeq \pi(K) \simeq K$$

Thus, since K is a field it now follows that M_0 is a maximal ideal of S. Combining the previous results, we now have that R/S is an integral ring extension and that M_0 is a maximal ideal of S. Therefore, by the Lying-Over Theorem it follows that there is a maximal ideal N of R such that $N \cap S = M_0$.

Finally, recall that R is a field so that the only ideals of R are $\{0\}$ and R. Therefore, since N is a maximal ideal of R we have in particular that $N \neq R$ so that $N = \{0\}$.

Therefore, we now have

$$(t_1, \ldots, t_r) = M_0 = N \cap S = \{0\} \cap S = \{0\}$$

so that $r = 0$. That is, the transcendence degree of R over $\pi(K)$ so that R is an integral extension of $\pi(K)$. But since R and $\pi(K)$ are fields, it now follows that R is an algebraic extension of $\pi(K)$. Thus, since F is algebraically closed it now follows that there is a ring homomorphism $\phi : R \to F$ that is the "identity" on K. That is, we have that M is an ideal of $K[x_1, \ldots, x_n]$ such that $\phi : K[x_1, \ldots, x_n]/M \to F$ is a ring homomorphism which is the "identity" on K so that by Remark 7 above we have that $V(M) \neq \emptyset$. By our initial observation, this completes the proof. $\square$

Theorem. (Hilbert's Nullstellensatz): Let F be an algebraically closed extension field of a field K and I an ideal of $K[x_1, \ldots, x_n]$. Then $J(V(I)) = \mathrm{Rad}(I)$.

Proof. Before we begin, suppose that $I = K[x_1, \ldots, x_n]$. Then by the Lemma for Hilbert's Nullstellensatz, we have that $V(I) = \emptyset$ so that $J(V(I)) = K[x_1, \ldots, x_n]$. On the other hand, note that we clearly have $\mathrm{Rad}(I) = K[x_1, \ldots, x_n]$ in this case and hence we see that

$$J(V(I)) = K[x_1, \ldots, x_n] = \mathrm{Rad}(I)$$

so that the result is true in this case. Therefore, assume that $I \neq K[x_1, \ldots, x_n]$.

First, suppose that $f(x_1, \ldots, x_n) \in \mathrm{Rad}(I)$. Then there is an integer $m \geq 1$ such that $f(x_1, \ldots, x_n)^m \in I$. Now, let $(a_1, \ldots, a_n) \in V(I)$ so that $g(a_1, \ldots, a_n) = 0$ for each $g(x_1, \ldots, x_n) \in I$. Then since $f(x_1, \ldots, x_n)^m \in I$, we have that

$$\underbrace{f(a_1, \ldots, a_n) \cdots f(a_1, \ldots, a_n)}_{m \text{ times}} = f(a_1, \ldots, a_n)^m = 0$$

By the above equality, then, it follows that $f(a_1, \ldots, a_n) = 0$. Thus, since $(a_1, \ldots, a_n) \in V(I)$ was arbitrary it now follows that $f(x_1, \ldots, x_n) \in J(V(I))$ and hence we conclude that $\mathrm{Rad}(I) \subseteq J(V(I))$.

Secondly, suppose that $f(x_1, \ldots, x_n) \in J(V(I))$ so that $f(a_1, \ldots, a_n) = 0$ for all $(a_1, \ldots, a_n) \in V(I)$. For simplicity, write $f(x_1, \ldots, x_n) = f$. If $f = 0$, then clearly $f \in J(V(I))$ so assume that $f \neq 0$. Next, consider the ring $K[x_1, \ldots, x_n, y]$ and let L be the ideal of $K[x_1, \ldots, x_n, y]$ generated by I and the polynomial $yf - 1 \in K[x_1, \ldots, x_n, y]$. We claim that $V_{n+1}(L) = \emptyset$. Indeed, suppose for the sake of contradiction that there were some element $(a_1, \ldots, a_n, b) \in F^{n+1}$ that were an element of $V_{n+1}(L)$. Notice that since $(a_1, \ldots, a_n, b) \in V_{n+1}(L)$ we clearly have by the definition of L that $(a_1, \ldots, a_n) \in V(I)$

so that $f(a_1, \ldots, a_n) = 0$. Thus, since $yf - 1 \in L$ we have that

$$\begin{aligned} 0 &= (yf-1)(a_1, \ldots, a_n, b) \\ &= (yf)(a_1, \ldots, a_n, b) - 1 \\ &= bf(a_1, \ldots, a_n) - 1 \\ &= b \cdot 0 - 1 \\ &= -1 \\ &\neq 0 \end{aligned}$$

which is clearly a contradiction. Thus, we have that $V_{n+1}(L) = \emptyset$ so that by the Lemma for Hilbert's Nullstellensatz we obtain $L = K[x_1, \ldots, x_n, y]$.

Now, since $L = K[x_1, \ldots, x_n, y]$ we have in particular that $1 \in L$ since we clearly have $1 \in K[x_1, \ldots, x_n, y]$. Therefore, there are elements $f_1, \ldots, f_{t-1} \in I$ and $g_1, \ldots, g_t \in K[x_1, \ldots, x_n, y]$ such that

$$1 = \sum_{i=1}^{t-1} g_i f_i + g_t \cdot (yf - 1)$$

Next, consider the map $K[x_1, \ldots, x_n, y] \to K(x_1, \ldots, x_n)$ that is defined by $x_i \mapsto x_i$ and $y \mapsto 1/f$. Clearly, this map is a well-defined ring homomorphism since $f \neq 0$. Moreover, note that this ring homomorphism maps 1 to 1. Therefore, applying this ring homomorphism to both sides of the above equality gives

$$\begin{aligned} 1 &= \sum_{i=1}^{t-1} g\left(x_1, \ldots, x_n, \frac{1}{f}\right) f_i(x_1, \ldots, x_n) + g_t\left(x_1, \ldots, x_n, \frac{1}{f}\right) \cdot \left(\frac{1}{f} \cdot f - 1\right) \\ &= \sum_{i=1}^{t-1} g\left(x_1, \ldots, x_n, \frac{1}{f}\right) f_i(x_1, \ldots, x_n) + g_t\left(x_1, \ldots, x_n, \frac{1}{f}\right) \cdot (1 - 1) \\ &= \sum_{i=1}^{t-1} g\left(x_1, \ldots, x_n, \frac{1}{f}\right) f_i(x_1, \ldots, x_n) + 0 \\ &= \sum_{i=1}^{t-1} g\left(x_1, \ldots, x_n, \frac{1}{f}\right) f_i(x_1, \ldots, x_n) \end{aligned}$$

Now, notice that there is clearly an integer $m \geq 1$ such that

$$f^m g_i\left(x_1, \ldots, x_n, \frac{1}{f}\right) \in K[x_1, \ldots, x_n] \quad \text{for each} \quad i \in \{1, \ldots, t-1\}$$

Therefore, multiplying both sides of the equality established above by f^m and recalling that $f_i(x_1, \ldots, x_n) \in I$ for each $i \in \{1, \ldots, t-1\}$ we obtain since I is an ideal of

$K[x_1, \ldots, x_n]$ that

$$\begin{aligned} f^m &= f^m \sum_{i=1}^{t-1} g\left(x_1, \ldots, x_n, \frac{1}{f}\right) f_i(x_1, \ldots, x_n) \\ &= \sum_{i=1}^{t-1} \left[f^m g\left(x_1, \ldots, x_n, \frac{1}{f}\right)\right] f_i(x_1, \ldots, x_n) \\ &\in I \end{aligned}$$

so that $f^m \in I$. Thus, we conclude that $f \in \mathrm{Rad}(I)$ so that $J(V(I)) \subseteq \mathrm{Rad}(I)$ and hence $J(V(I)) = \mathrm{Rad}(I)$. This completes the proof. $\square$

Topic 9: Noncommutative Algebra; Simple Rings and Modules

Remark. In what follows, when we say that R is a ring we mean that R is an associative ring but that R is not necessarily commutative and that R is not necessarily a ring with identity.

Definition. Let R be a ring and let A be a (left) R-module. We say that A is ***simple*** or that A is ***irreducible*** if $RA \neq \{0\}$ and A contains no proper, nontrivial R-submodule. We say that R is ***simple*** if $R^2 \neq \{0\}$ and R has no proper, nontrivial (two-sided) ideal.

Example. Every field is a simple ring.

Proof. Let F be a field. Then $1 \in F$ and $1 \neq 0$. Thus, we have

$$0 \neq 1 = 1 \cdot 1 \in F^2$$

so that $F^2 \neq \{0\}$. Finally, suppose that I is an ideal of F. Then since F is a field, we have $I \in \{\{0\}, F\}$. In particular, this shows that F contains no proper, nontrivial two-sided ideal. We conclude that F is simple. $\square$

Example. Let $V \neq \{0\}$ be a vector space over a field F and let $(e_i)_{i \in I}$ be a basis for V over F. For $i, j \in I$, define a map

$$e_{i,j} : V \to V \quad \text{by} \quad \sum_{\ell \in I} \lambda_\ell e_\ell \mapsto \lambda_j e_i$$

so that for $i, j \in I$ we have $e_{i,j} \in \operatorname{End}_F(V)$. We show that for $i, j, k, \ell \in I$ we have

$$e_{i,j} \circ e_{k,\ell} = \begin{cases} e_{i,\ell} & \text{if} \quad j = k \\ 0 & \text{if} \quad j \neq k \end{cases}$$

Indeed, first suppose that $j = k$ and let $\sum_{z \in I} \lambda_z e_z \in V$. Then

$$\begin{aligned}
(e_{i,j} \circ e_{k,\ell}) \left(\sum_{z \in I} \lambda_z e_z \right) &= (e_{i,j} \circ e_{j,\ell}) \left(\sum_{z \in I} \lambda_z e_z \right) \\
&= e_{i,j} \left(e_{j,\ell} \left(\sum_{z \in I} \lambda_z e_z \right) \right) \\
&= e_{i,j}(\lambda_\ell e_j) \\
&= \lambda_\ell e_{i,j}(e_j) \\
&= \lambda_\ell e_{i,j}(1 \cdot e_j) \\
&= \lambda_\ell (1 \cdot e_i) \\
&= \lambda_\ell e_i \\
&= e_{i,\ell} \left(\sum_{z \in I} \lambda_z e_z \right)
\end{aligned}$$

and hence we conclude that $e_{i,j} \circ e_{k,\ell} = e_{i,\ell}$. On the other hand, suppose that $j \neq k$ and let $\sum_{z \in I} \lambda_z e_z \in V$. Then

$$\begin{aligned}(e_{i,j} \circ e_{k,\ell}) \left(\sum_{z \in I} \lambda_z e_z \right) &= e_{i,j} \left(e_{k,\ell} \left(\sum_{z \in I} \lambda_z e_z \right) \right) \\ &= e_{i,j}(\lambda_\ell e_k) \\ &= \lambda_\ell e_{i,j}(e_k) \\ &= \lambda_\ell (0 \cdot e_i) \\ &= 0\end{aligned}$$

and hence we conclude that $e_{i,j} \circ e_{k,\ell} = 0$. This completes the proof of our claim.

Theorem. Let $V \neq \{0\}$ be a vector space over a field F and let $(e_i)_{i \in I}$ be a basis for V over F. For $i, j \in I$, define $e_{i,j} \in \mathrm{End}_F(V)$ as in the previous lecture and let R be the set of all F-linear combinations of the $e_{i,j}$ for $i, j \in I$. Then R is a simple ring.

Proof. First, we show that R is a ring. Clearly, we have that R is an abelian group under addition. Furthermore, it follows by the results from the previous lecture that R is closed under function composition. Finally, recall that function composition is an associative operation and note that the distributivity axiom clearly holds for R. We conclude that R is a ring in the sense of the Remark from the previous lecture.

Next, we show that $R^2 \neq \{0\}$. Towards this end, note that since $V \neq \{0\}$ that there is some $i \in I$ and hence there is some element e_i in the basis $(e_i)_{i \in I}$ for V over F. Moreover, since e_i is in the basis $(e_i)_{i \in I}$ for V over F it is immediate that $e_i \neq 0$. Now, consider the map $e_{i,i} : V \to V$. By definition, we have

$$e_{i,i}(e_i) = e_{i,i}(1 \cdot e_i) = e_i \neq 0$$

and hence $e_{i,i}$ is a nonzero element of R. Thus, by the results from the previous lecture we now obtain that

$$0 \neq e_{i,i} = e_{i,i} \circ e_{i,i} \in R^2$$

so that $R^2 \neq \{0\}$.

Finally, we show that R has no proper, nontrivial two-sided ideal. Towards this end, let J be a two-sided ideal of R with $J \neq \{0\}$. Since $J \neq \{0\}$, there is some $f \in J$ with $f \neq 0$. Now, we have that $f : V \to V$ is a nonzero map so that in particular f must map some element e_j in the basis $(e_i)_{i \in I}$ for V over F to a nonzero element of V and thus there is some $i \in I$ such that the ith coordinate of $f(e_j)$ is nonzero. Let $a \in F$ denote the ith coordinate of $f(e_j)$ so that by the previous observation we have $a \neq 0$. Moreover, since e_i is in the basis $(e_i)_{i \in I}$ for V over F it follows that $e_i \neq 0$ so that $ae_i \neq 0$ as $a \neq 0$.

Now, we claim that $e_{i,i} \circ f \circ e_{j,j}$ is a nonzero element of J. Indeed, note that by the above we have

$$(e_{i,i} \circ f \circ e_{j,j})(e_j) = e_{i,i}(f(e_{j,j}(e_j))) = e_{i,i}(f(e_j)) = ae_i \neq 0$$

so that $e_{i,i} \circ f \circ e_{j,j}$ is nonzero. Furthermore, since $f \in J$, since $e_{i,i}, e_{j,j} \in R$, and as J is a two-sided ideal of R it now follows that $e_{i,i} \circ f \circ e_{j,j}$ is a nonzero element of J. This completes the proof of our claim. Note that by this result, it follows that $e_{i,j} \in J$.

To complete the proof, let $i', j' \in I$. Then since $e_{i,j} \in J$ by the above, since $e_{i',i}, e_{j,j'} \in R$, and as J is a two-sided ideal of R it follows that $e_{i',i} \circ e_{i,j} \circ e_{j,j'} \in J$. Moreover, we have by the results from the previous lecture that

$$e_{i',i} \circ e_{i,j} \circ e_{j,j'} = e_{i',i} \circ (e_{i,j} \circ e_{j,j'}) = e_{i',i} \circ e_{i,j'} = e_{i',j'}$$

and hence we conclude by the above that $e_{i',j'} \in J$. Thus, since $i', j' \in I$ were arbitrary it now follows that $e_{i',j'} \in J$ for all $i', j' \in I$ so that by the definition of R we conclude that $J = R$. This result proves that R contains no proper, nontrivial two-sided ideal so that R. This completes the proof that R is a simple ring. □

Remark. Furthermore, we have that V is a simple R-module.

Proof. Before we begin, note that V is clearly an R-module. Now, first note that since $V \neq \{0\}$ there is a nonzero element e_i in the basis $(e_i)_{i \in I}$ for V over F. Clearly, we have that $e_i \in V$. Furthermore, consider the element $e_{i,i} \in R$. Then we have $e_{i,i}(e_i) = e_i \neq 0$ and hence it follows since $e_i \in V$ that $RV \neq \{0\}$.

Finally, let W be a nontrivial R-submodule of V. Then there is some nonzero element $a \in W$. Now, fix any $z \in I$. We claim that $e_z \in W$. Towards this end, first note that since $a \in W \subseteq V$ we may write $a = \sum_{s \in I} \lambda_s e_s$ for some $(\lambda_s)_{s \in I} \subseteq F$ and since a is nonzero it follows that there is some $r \in I$ such that $\lambda_r \neq 0$. Furthermore, since W is an R-module and $e_{z,r} \in R$ and $a \in W$ we have $e_{z,r}(a) \in W$. But notice that

$$e_{z,r}(a) = e_{z,r}\left(\sum_{s \in I} \lambda_s e_s\right) = \lambda_r e_z$$

and since $\lambda_r \in F$ is nonzero and F is a field, we may multiply both sides of the above equality by λ_r^{-1} to obtain since $e_{z,r}(a) \in W$ that

$$e_z = \lambda_r^{-1} e_{z,r}(a) \in W$$

Thus, since $z \in I$ was arbitrary it now follows that $(e_i)_{i \in I} \subseteq W \subseteq V$. But since $(e_i)_{i \in I}$ is a basis for V over F, it now follows that $W = V$. This result proves that V contains no proper, nontrivial R-submodule. This completes the proof that V is a simple R-module. □

Remark. In particular, if V is a finite dimensional vector space over F then $R = \mathrm{End}_F(V)$ is a simple ring and V is a simple R-module.

Proof. By the previous two results, we know that R is a simple ring and that V is a simple R-module so that it remains to prove that $R = \mathrm{End}_F(V)$. This fact follows from the hypothesis that V is finite dimensional over F, completing the proof. □

Lemma. (Schur's Lemma): Let R be a ring and let A be a simple R-module. Then:

(a): If $f : A \to B$ is a nonzero R-module homomorphism, then f is injective.

(b): If $g : B \to A$ is a nonzero R-module homomorphism, then g is surjective.

(c): Let $D = \mathrm{End}_R(A)$. Then D is a division ring.

Proof. (a): Since f is an R-module homomorphism, it suffices to show that $\ker f = \{0\}$ to establish that f is an injection. Towards this end, recall that $\ker f$ is an R-submodule of A and since A is a simple R-module this gives that $\ker f \in \{\{0\}, A\}$. But since f is nonzero, it now follows that $\ker f = \{0\}$ so that f is an injection. □

Proof. (b): Recall that $\mathrm{Im}(g)$ is an R-submodule of A and since A is a simple R-module, this gives that $\mathrm{Im}(g) \in \{\{0\}, A\}$. But since g is nonzero, it now follows that $\mathrm{Im}(g) = A$ so that g is a surjection. □

Proof. (c): Clearly, we have that D is ring. Furthermore, since $A \neq \{0\}$ as A is a simple R-module it follows that the identity map $1_A \in D$ is a nonzero element of D so that $D \neq \{0\}$ and 1_A is an identity of D. Finally, let $f \in D$ with $f \neq 0$. Then $f : A \to A$ is a nonzero R-module homomorphism so that by the results of Part (a) and Part (b) above, we have that f is an R-module automorphism. Therefore, we have that $f^{-1}\mathrm{End}_R(A) = D$ and hence f is a unit of D. Combining the previous results, we conclude that D is a division ring. □

Theorem. (Jacobson's Density Theorem): Let R be a ring and let A be a simple R-module. Let $D = \mathrm{End}_R(A)$. Let $v_1, \ldots, v_n \in A$ and $u_1, \ldots, u_n \in A$ and suppose that the set $\{v_1, \ldots, v_n\}$ is linearly independent over D. Then there is some $r \in R$ such that $rv_i = u_i$ for each $i \in \{1, \ldots, n\}$.

Note: We prove this Theorem in three parts. Before we begin the proofs of these three parts, we set up the situation as follows. Assume the desired result is false. Among all counterexamples, pick one with n is as small possible and among all such counterexamples, pick one where there are as few nonzero u_i as possible.

Step 1. Exactly one of the $u_1, \ldots, u_n$ (say u_n) is nonzero.

Proof. If $u_i = 0$ for each $i \in \{1, \ldots, n\}$, then we clearly have no counterexample. For the sake of contradiction, suppose that this is false. By the previous observation, then, it follows without loss of generality that $u_{n-1} \neq 0$ and $u_n \neq 0$. Now, by our choice it follows that there are $r_1, r_2 \in R$ such that $r_1 v_i = 0$ for each $i \in \{1, \ldots, n-1\}$ and $r_1 v_n = u_n$ and $r_2 v_i = u_i$ for $i \in \{1, \ldots, n-1\}$ and $r_2 v_n = 0$. Finally, fix $z \in \{1, \ldots, n-1\}$. Then by the above results, we have

$$(r_1 + r_2)v_z = r_1 v_z + r_2 v_z = 0 + r_2 v_z = r_2 v_z = u_z$$

and

$$(r_1 + r_2)v_n = r_1 v_n + r_2 v_n = r_1 v_n + 0 = r_1 v_n = u_n$$

Hence, by the above results we conclude that $(r_1 + r_2)v_i = u_i$ for each $i \in \{1, \ldots, n\}$. But since $r_1 + r_2 \in R$ as $r_1, r_2 \in R$, this contradicts our choice. We may now conclude that there is exactly one of $u_1, \ldots, u_n$ that is nonzero and without loss of generality, we may assume that this nonzero element is u_n, completing the proof. □

Step 2. Let $I = \mathrm{Ann}(v_1, \ldots, v_{n-1}) = \{r \in R : rv_i = 0 \text{ for } i \in \{1, \ldots, n-1\}\}$. Then $Iv_n = \{0\}$.

Proof. First, note that I is a left ideal of R. Now, we claim that Iv_n is an R-submodule of A. Towards this end, notice that since A is an R-module with $v_n \in A$ and as $I \subseteq R$ we have that $Iv_n \subseteq A$. Furthermore, we clearly have that Iv_n is a subgroup A under addition. Finally, let $r \in R$ and $iv_n \in Iv_n$. Now, since I is an ideal of R and $r \in R$ and $i \in I$ we have $ri \in R$. Thus, we obtain

$$r(iv_n) = (ri)v_n \in Iv_n$$

and hence Iv_n is an R-submodule of A.

Now, since A is a simple R-module it follows by the above result that $Iv_n \in \{\{0\}, A\}$. For the sake of contradiction, suppose that $Iv_n = A$. Then since $u_n \in A$, there is some $i \in I \subseteq R$ such that $iv_n = u_n$. However, since $u_1, \ldots, u_{n-1} = 0$ by the above it follows that this contradicts our choice. Therefore, we conclude that $Iv_n = \{0\}$. □

Step 3. The Theorem holds.

Proof. Note that since the set $\{v_1, \ldots, v_n\}$ is linearly independent over D that we have in particular that $v_n \neq 0$. Now, recall that $Iv_n = \{0\}$. For the sake of contradiction, suppose that $I = R$. Then we have $Rv_n = \{0\}$ by the above. Furthermore, notice that since $v_n \neq 0$ that $\mathbb{Z}v_n$ is a nontrivial R-submodule of A. Therefore, since A is a simple R-module it follows that $\mathbb{Z}v_n = A$. However, since A is a simple R-module we have

$$\{0\} \neq RA = R(\mathbb{Z}v_n) = Rv_n = \{0\}$$

which is clearly a contradiction. Therefore, we obtain that $I \neq R$. That is, we have

$$\{r \in R : rv_i = 0 \text{ for } i \in \{1, \ldots, n-1\}\} = \mathrm{Ann}(v_1, \ldots, v_{n-1}) = I \neq R$$

and hence in particular we see that $n \geq 2$.

Let $I_0 = \mathrm{Ann}(v_1, \ldots, v_{n-2})$. We claim that $I_0 v_{n-1} = A$. Indeed, first notice that since $I_0 \subseteq R$ and $v_{n-1} \in A$ we have that since A is an R-module that $I_0 v_{n-1} \subseteq A$. On the other hand, let $a \in A$. Then by the minimality of n, it follows that there is some $r \in R$ such that $rv_1 = 0, \ldots, rv_{n-2} = 0, rv_{n-1} = a$. In particular, we see that $r \in \mathrm{Ann}(v_1, \ldots, v_{n-2}) = I_0$ and hence $a = rv_{n-1} \in I_0 v_{n-1}$. Combining the previous results, we see that $I_0 v_{n-1} = A$. Thus, we may define a map

$$\theta : A \to A \quad \text{by} \quad iv_{n-1} \mapsto iv_n$$

We show that $\theta \in D$.

First, we show that θ is well-defined. Towards this end, suppose that $i_1 v_{n-1} = i_2 v_{n-1}$ for some $i_1, i_2 \in I_0$. Clearly, this equality gives that $(i_1 - i_2)v_{n-1} = 0$ and hence it now follows that $i_1 - i_2 \in I$. Now, recall that $Iv_n = \{0\}$ by Step 2. Therefore, we obtain since $i_1 - i_2 \in I$ that $(i_1 - i_2)v_n = 0$ so that $i_1 v_n = i_2 v_n$. Thus, we have

$$\theta(i_1 v_n) = i_1 v_n = i_2 v_n = \theta(i_2 v_n)$$

so that θ is well-defined. Furthermore, it is clear that $\theta : A \to A$ is an R-module homomorphism and hence $\theta \in D$.

Finally, let $j \in I_0 \subseteq R$. Then we have since $\theta \in D$ that

$$j(\theta(v_{n-1}) - v_n) = j\theta(v_{n-1}) - jv_n = \theta(jv_{n-1}) - jv_n = jv_n - jv_n = 0$$

Thus, we conclude by minimality that the set $\{v_1, \ldots, v_{n-2}, \theta(v_{n-1}) - v_n\}$ is linearly dependent over D. However, this implies that the set $\{v_1, \ldots, v_n\}$ is linearly dependent over D which is a contradiction. This completes the proof. $\square$

Topic 10: The Wedderburn-Artin Theorems; The Jacobson Radical

Definition. Let R be a ring and let A be a (left) R-module. Then A is said to be ***faithful*** if the (left) annihilator $\text{Ann}(A)$ is such that $\text{Ann}(A) = \{0\}$.

Definition. Let R be a ring. Then R is said to be (left) ***primitive*** if there exists a faithful, simple (left) R-module.

Theorem. (Wedderburn-Artin Theorem Part I): Let R be a left-Artinian ring. Then the following conditions on R are equivalent.

(i): R is simple.

(ii): R is primitive.

(iii): R is isomorphic to $\text{End}_D(V)$ for some division ring D and some finite dimension vector space V over D.

(iv): R is isomorphic to the ring of all $n \times n$ matrices over a division ring D.

Proof. (iii $\Rightarrow$ iv) and (iv $\Rightarrow$ iii): One can believe that both of these implications are true, even though one needs to be careful about exactly on what sides the multiplications of matrices occurs.

(i $\Rightarrow$ ii): Assume that R is a simple ring and define the set $I = \{r \in R : Rr = 0\}$. We claim that I is an ideal of R. Towards this end, note that we clearly have $0 \in I$ so that $I \neq \emptyset$. Now, let $r_1, r_2 \in I$ so that $Rr_1 = 0 = Rr_2$. Thus, we obtain that

$$R(r_1 - r_2) = Rr_1 - Rr_2 = 0 - 0 = 0$$

so that $r_1 - r_2 \in I$ and hence I is a subgroup of R under addition. Finally, let $r \in I$ and $s \in R$. Since $r \in I$, we have that $Rr = 0$. Therefore, we obtain

$$R(sr) = (Rs)r = Rr = 0$$

and

$$R(rs) = (Rr)s = 0s = 0$$

so that $sr, rs \in I$. By the above results, we conclude that I is a two-sided ideal of R. Since R is simple, then, we have that $I \in \{\{0\}, R\}$. Suppose that $I = R$. Then we have by the definition of I that $R^2 = \{0\}$. However, since R is simple we have $R^2 \neq \{0\}$. Hence, we conclude that $I = \{0\}$.

Now, note that since R is left-Artinian there is a minimal left ideal I_0 of R. We claim that I_0 is a simple R-module. First, note that since I_0 is an ideal of R we have that I_0 is an R-module. Now, suppose that J is a nontrivial R-submodule with $J \subseteq I$. Then J is a nontrivial ideal of R with $J \subseteq I$ and as I is a minimal ideal of R, it now follows that $J = I$.

Finally, we claim that $\text{Ann}(I_0) = \{0\}$. For the sake of contradiction, suppose that $\text{Ann}(I_0) \neq \{0\}$. Then since $\text{Ann}(I_0)$ is a two-sided ideal of R and as $\text{Ann}(I_0) \neq \{0\}$, we have that since R is simple that $\text{Ann}(I_0) = R$ so that $Ru = 0$ for each $u \in I_0 \subseteq R$. Now, since I_0 is a minimal ideal of R we have in particular that $I_0 \neq \{0\}$ so that there is some

nonzero $u \in I_0$. By the previous observation, we have that $Ru = 0$ and hence $u \in I$ which implies that $I \neq \{0\}$. However, this contradicts the fact that $I = \{0\}$. Thus, we conclude that $\mathrm{Ann}(I_0) = \{0\}$ so that $RI_0 \neq \{0\}$. Combining the above results, then, we see that I_0 is a simple R-module. Moreover, since $\mathrm{Ann}(I_0) = \{0\}$ we have that I_0 is a faithful R-module. Therefore, we see R is primitive.

(ii $\Rightarrow$ iii)): Let V be a faithful, simple (left) R-module and define $D = \mathrm{End}_R(V)$. By Schur's Lemma, we have that D is a division ring and we know that V is a (left) vector space over D.

Before we prove the main result, we show that V cannot be infinite dimensional over D. For the sake of contradiction, suppose that V were infinite dimensional over D so that there exists a countably infinite linearly independent subset $(v_i)_{i=1}^{\infty} \subseteq V$ of V over D. Now, we claim that

$$\mathrm{Ann}_R(v_1) \supsetneq \mathrm{Ann}_R(v_1, v_2) \supsetneq \cdots \supsetneq \mathrm{Ann}_R(v_1, \ldots, v_n) \supsetneq \cdots$$

is a strictly decreasing sequence of (left) ideals of R.

First, notice that $\mathrm{Ann}_R(v_1, \ldots, v_n)$ is clearly an ideal of R for each integer $n \geq 1$ and $\mathrm{Ann}_R(v_1, \ldots, v_{n-1}) \supseteq \mathrm{Ann}_R(v_1, \ldots, v_n)$ for each integer $n \geq 2$. Therefore, it remains to prove that the above inclusions are strict. Indeed, suppose for the sake of contradiction that $\mathrm{Ann}_R(v_1) = \mathrm{Ann}_R(v_1, v_2)$. By Jacobson's Density Theorem, there is some $r \in R$ such that $rv_1 = 0$ and $rv_2 = v_1$. By the first of these equalities, we have that $r \in \mathrm{Ann}_R(v_1) = \mathrm{Ann}_R(v_1, v_2)$ so that $rv_2 = 0$. However, recall that v_1 is in the linearly independent subset $(v_i)_{i=1}^{\infty}$ of V over D so that in particular we have $v_1 \neq 0$ so that by the above results we have

$$0 \neq v_1 = rv_2 = 0$$

which is a contradiction. Therefore, it now follows that each of the above inclusions are strict which completes the proof of our claim. However, the existence of the above strictly decreasing sequence of (left) ideals of R contradicts the fact that R is left-Artinian. We conclude that V must be finite dimensional over D.

Now, since V is finite dimensional over D there is some basis $\{v_1, \ldots, v_n\}$ for V over D. Next, define a map

$$\psi : R \to \mathrm{End}_D(V) \quad \text{by} \quad \psi(r) : V \to V \quad \text{by} \quad \psi(r)(v) = rv \quad \text{for each} \quad r \in R, v \in V$$

First, we show that ψ is well-defined. Towards this end, let $r \in R, v_1, v_2 \in V$, and $\theta \in D = \mathrm{End}_R(V)$. Then we have

$$\begin{aligned}
\psi(r)(\theta v_1 + v_2) &= \psi(r)(\theta(v_1) + v_2) \\
&= r(\theta(v_1) + v_2) \\
&= r\theta(v_1) + rv_2 \\
&= \theta(rv_1) + rv_2 \\
&= \theta(\psi(r)(v_1)) + \psi(r)(v_2) \\
&= \theta\psi(r)(v_1) + \psi(r)(v_2)
\end{aligned}$$

so that $\psi(r) \in \mathrm{End}_D(V)$ and hence ψ is a well-defined map.

Next, we show that ψ is a ring isomorphism. Towards this end, let $r_1, r_2 \in R$ and $v \in V$. Then we have

$$\psi(r_1 + r_2)(v) = (r_1 + r_2)v = r_1 v + r_2 v = \psi(r_1)(v) + \psi(r_2)(v) = (\psi(r_1) + \psi(r_2))(v)$$

so that $\psi(r_1 + r_2) = \psi(r_1) + \psi(r_2)$ and

$$\psi(r_1 r_2)(v) = (r_1 r_2)v = r_1(r_2 v) = r_1 \psi(r_2)(v) = \psi(r_1)(\psi(r_2)(v)) = (\psi(r_1) \circ \psi(r_2))(v)$$

so that $\psi(r_1 r_2) = \psi(r_1) \circ \psi(r_2)$ and hence ψ is a ring homomorphism.

Next, we show that ψ is injective. Towards this end, note that since ψ is a ring homomorphism that it suffices to show that $\ker \psi$ is trivial to establish that ψ is an injection. Indeed, let $r \in \ker \psi$ so that $\psi(r) : V \to V$ is the zero map. In other words, we have that

$$rv = \psi(r)(v) = 0 \quad \text{for each} \quad v \in V$$

so that $r \in \mathrm{Ann}_R(V)$. But recall that V is a faithful R-module so that $\mathrm{Ann}_R(V) = \{0\}$ and hence $r = 0$ so that $\ker \psi$ is trivial and hence ψ is an injection.

Finally, we show that ψ is a surjection. Towards this end, let $\theta \in \mathrm{End}_D(V)$. Since $\{v_1, \ldots, v_n\}$ is a basis for V over D, it follows that θ is completely determined by the images of $v_1, \ldots, v_n$ under θ. Now, since V is a simple R-module and as $\{v_1, \ldots, v_n\}$ is a linearly independent subset of V over D as $\{v_1, \ldots, v_n\}$ is a basis for V over D we have by Jacobson's Density Theorem that there is some $r \in R$ such that $rv_i = \theta(v_i)$ for each $i \in \{1, \ldots, n\}$. Now, notice that

$$\psi(r)(v_i) = rv_i = \theta(v_i) \quad \text{for each} \quad i \in \{1, \ldots, n\}$$

so that by the above observation we have $\psi(r) = \theta$ and so ψ is a surjection. We may now conclude that ψ is a ring isomorphism and hence $R \simeq \mathrm{End}_D(V)$. As D is a division ring, then, this completes the proof of this implication.

(iii $\Rightarrow$ i): Assume that $R \simeq \mathrm{End}_D(V)$, where D is a division ring and V is a finite dimensional vector space over D. We will show that $\mathrm{End}_D(V)$ is a simple ring. Towards this end, first note that since V is finite dimensional over D that there is some basis $\{v_1, \ldots, v_n\} \subseteq V$ for V over D. For $i, j \in \{1, \ldots, n\}$, define

$$e_{i,j} : V \to V \quad \text{by} \quad \sum_{k=1}^{n} d_k v_k \mapsto d_j v_i$$

and let S be the set of all D-linear combinations of the $e_{i,j}$. Then by previous results, we know that S is a simple ring and since V is finite dimensional over D we have $S = \mathrm{End}_D(V)$ so that $S \simeq R$ so that R is simple. This completes the proof. $\square$

Proposition. Let R be a simple, left-Artinian ring. Then R has a simple module and any two simple R-modules are isomorphic.

Proof. Since R is a simple, left-Artinian ring, we have by the Wedderburn-Artin Theorem that R is primitive and hence R has a simple module. Now, since R is left-Artinian there is a minimal (left) ideal I of R and in particular since I is an ideal of R we have that I is an R-module.

We claim that I is a simple R-module. Towards this end, consider $\mathrm{Ann}(I)$. Then $\mathrm{Ann}(I)$ is a two-sided ideal of R so that since R is simple we have $\mathrm{Ann}(I) \in \{\{0\}, R\}$. Suppose that $\mathrm{Ann}(I) = R$. Then we have $RI = \{0\}$. Now, once again appealing to the Wedderburn-Artin Theorem we see that R has identity so that by the above we have $I = 1I = \{0\}$. However, recall that I is a minimal ideal of R so that in particular we have $I \neq \{0\}$ which is a contradiction. Thus, we conclude that $\mathrm{Ann}(I) = \{0\}$ and since I is a minimal left ideal of R it now follows that I is a simple R-module.

Next, let A be a simple R-module. We claim that there is some $a \in A$ such that $Ia \neq \{0\}$. Indeed, for the sake of contradiction suppose that $Ia = \{0\}$ for each $a \in A$ so that $IA = \{0\}$ and hence $I \subseteq \mathrm{Ann}(A)$. Now, recall that A is a simple R-module so that in particular we have $RA \neq \{0\}$. Moreover, we have that $\mathrm{Ann}(A)$ is a two-sided ideal of R so that since R is simple we have $\mathrm{Ann}(A) \in \{\{0\}, R\}$. However, since $RA \neq \{0\}$ it now follows that $\mathrm{Ann}(A) = \{0\}$. Therefore, by the above result we have $I \subseteq \mathrm{Ann}(A) = \{0\}$ so that $I = \{0\}$. But recall that $I \neq \{0\}$, which is a contradiction. We conclude that there is some $a \in A$ such that $Ia \neq \{0\}$.

Finally, define a map

$$\phi : I \to A \quad \text{by} \quad i \mapsto ia$$

and note that since $I \subseteq R$ and as A is an R-module we have that ϕ is a well-defined map. Moreover, let $i_1, i_2 \in I$ and $r \in R$. Then

$$\phi(ri_1 + i_2) = (ri_1 + i_2)a = (ri_1)a + i_2a = r(i_1a) + i_2a = r\phi(i_1) + \phi(i_2)$$

so that ϕ is an R-module homomorphism. Furthermore, note that

$$\phi(I) = Ia \neq \{0\}$$

by the above so that ϕ is a nonzero R-module homomorphism. Therefore, since I and A are simple R-modules it follows by Schur's Lemma that ϕ is bijective and hence ϕ is an R-module isomorphism so that $I \simeq A$. This completes the proof. $\square$

Definition. Let R be a ring. We define the ***Jacobson radical*** of R, denoted $J(R)$, to be the intersection of the annihilators of all the simple (left) R-modules.

Definition. Let R be a ring. We say that R is ***semisimple*** if the Jacobson radical $J(R)$ of R is such that $J(R) = \{0\}$.

Remark. Let R be a ring. Then every simple R-module is isomorphic to R/I for some maximal ideal I of R.

Proof. Let A be a simple R-module. Then we have in particular that $RA \neq \{0\}$ and hence there is some $a \in A$ such that $Ra \neq \{0\}$. Now, define a map

$$\phi : R \to A \quad \text{by} \quad r \mapsto ra$$

Then ϕ is clearly an R-module homomorphism. Next, we show that ϕ is a surjection. Towards this end, recall that since ϕ is an R-module homomorphism that $\phi(R)$ is an R-submodule of A. Therefore, since A is a simple R-module it follows that $\phi(R) \in \{\{0\}, A\}$.

Suppose that $\phi(R) = \{0\}$. Then we have

$$\{0\} \neq Ra = \phi(R) = \{0\}$$

which is clearly a contradiction. Hence, we conclude that $\phi(R) = A$ and so that ϕ is a surjection. By the First Isomorphism Theorem for Modules, then, we conclude that $A \simeq R/I$ where $I = \ker \phi$.

Next, we show that I is a maximal ideal of R. Towards this end, suppose that J is an ideal of R with $I \subseteq J \subseteq R$ and that $J \neq I$. In particular, this implies that there is some $a \in J - I = J - \ker \phi$. By this observation and by the same reasoning as presented above, we now have that $\phi(J)$ is an R-submodule of A and since A is a simple R-module this gives that $\phi(J) = A$. But recall that $\phi(R) = A$ so that we now have $\phi(J) = \phi(R)$.

Finally, for the sake of contradiction suppose that $R \neq J$. Then since $J \subseteq R$, this implies that there is some $r \in R - J$ so that clearly we have $\phi(r) \in \phi(R)$. We claim that $\phi(r) \notin \phi(J)$. For the sake of contradiction, suppose that $\phi(r) \in \phi(J)$ so that there is some $j \in J$ with $\phi(r) = \phi(j)$. Then since ϕ is an R-module homomorphism, this gives

$$0 = \phi(r) - \phi(j) = \phi(r - j)$$

so that $r - j \in \ker \phi = I \subseteq J$. Therefore, since $j \in J$ and as J is an ideal of R this implies that $r \in J$ which is a contradiction. We conclude that $R = J$ and hence I is a maximal ideal of R such that $A \simeq R/I$. This completes the proof. $\square$

Remark. We limit our study of the Jacobson radical to the case where R is both left-Artinian and left-Noetherian.

Definition. Let R be a ring and let I be an ideal of R. Then I is ***nilpotent*** if for some integer $n \geq 1$, we have $I^n = \{0\}$.

Theorem. Let R be a ring which is both left-Artinian and left-Noetherian. Then $J(R)$ is a nilpotent ideal of R and contains every nilpotent ideal of R.

Proof. Suppose that I is a nilpotent ideal of R and let A be a simple R-module. Then since $I \subseteq R$ and as A is an R-module we have $IA \subseteq A$ so that IA is an R-submodule of A. Since A is a simple R-module, then, it follows that $IA \in \{\{0\}, A\}$. Suppose that $IA = A$ so that $I^m A = A$ for each positive integer m. Recall that I is a nilpotent ideal of R so that there is some integer $n \geq 1$ such that $I^n = \{0\}$. By the previous observation, then, we have

$$A = I^n A = \{0\}A = \{0\}$$

However, since A is a simple R-module we have in particular that $A \neq \{0\}$ which contradicts the above equality. We conclude that $IA = \{0\}$ and hence $I \subseteq \mathrm{Ann}(A)$. Therefore, since A was an arbitrary simple R-module we conclude that $I \subseteq J(R)$.

By the above result, it remains to prove that $J(R)$ is a nilpotent ideal of R. Towards this end, note that since R is both left-Artinian and left-Noetherian that there is a maximal chain of left ideals of R

$$J(R) = I_0 \supsetneq I_1 \supsetneq I_2 \supsetneq \cdots \supsetneq I_n = \{0\}$$

Now, fix any $N \in \{0, 1, \ldots, n-1\}$ and consider the quotient I_N/I_{N+1} as an R-module. Then since the above chain of left ideals of R is maximal, it follows that either I_N/I_{N+1} is a simple R-module or that R acts trivially on I_N/I_{N+1}.

Suppose first that I_N/I_{N+1} is a simple R-module. Then by the definition of $J(R)$, we have that $J(R) \subseteq \mathrm{Ann}(I_N/I_{N+1})$ so that $J(R)(I_N/I_{N+1}) = \{0\}$. If R acts trivially on I_N/I_{N+1}, then since $J(R) \subseteq R$ we clearly have $J(R)(I_N/I_{N+1}) = \{0\}$. In either case, then, we see that $J(R)(I_N/I_{N+1}) = \{0\}$ so that $J(R)I_N \subseteq I_{N+1}$. Furthermore, since $N \in \{0, 1, \ldots, n-1\}$ was arbitrary this result shows that $J(R)I_i \subseteq I_{i+1}$ for each $i \in \{0, 1, \ldots, n-1\}$.

Finally, let $J = J(R)$. Then by the above, we have that

$$J = I_0 \subseteq I_0$$

so that

$$J^2 = JJ \subseteq JI_0 \subseteq I_1$$

so that

$$J^3 = JJ^2 \subseteq JI_1 \subseteq I_2$$

Continuing this process, then, we see that

$$J^{n+1} = JJ^n \subseteq JI_{n-1} \subseteq I_n = \{0\}$$

and hence $J^{n+1} = \{0\}$ so that $J = J(R)$ is nilpotent. This completes the proof. □

Theorem. (Wedderburn-Artin Theorem Part II): Let R be a ring. Then the following conditions on R are equivalent.

(i): R is a nonzero, semisimple, left-Artinian ring.

(ii): R is a direct product of a finite positive number of simple ideals, each of which is isomorphic to the endomorphism ring of a nonzero, finite dimensional vector space over a division ring.

(iii): There are division rings $D_1, \ldots, D_t$ and integers $n_1, \ldots, n_t, t \geq 1$ such that R is isomorphic to $\mathrm{Mat}_{n_1}(D_1) \times \cdots \times \mathrm{Mat}_{n_t}(D_t)$.

Proof. (ii ⇒ iii) and (iii ⇒ ii): One can believe that both of these implications are true, even though one needs to be careful about exactly on what sides the multiplications of matrices occurs.

(ii ⇒ i): By hypothesis, we may write

$$R = \mathrm{End}_{D_1}(V_1) \oplus \cdots \oplus \mathrm{End}_{D_t}(V_t)$$

where t is an integer with $t \geq 1$ and V_i is a nonzero, finite dimensional vector space over the division ring D_i for each $i \in \{1, \ldots, t\}$. Clearly, we have that R is a nonzero ring. Furthermore, notice that since V_i is finite dimensional over D_i that $\mathrm{End}_{D_i}(V_i)$ is a left-Artinian ring for each $i \in \{1, \ldots, t\}$. Therefore, since the direct sum of a finite number of left-Artinian rings is a left-Artinian ring it now follows that R is left-Artinian.

By the above results, it remains to prove that R is semisimple. Towards this end, let $\pi_i : R \to \mathrm{End}_{D_i}(V_i)$ denote the canonical projection map for each $i \in \{1, \ldots, t\}$. Now,

fix any $N \in \{1, \ldots, t\}$. Define for $\theta \in R$ and $v \in V_N$ we have $\theta v = \pi_N(\theta)(v)$. Then this defines an action of R on V_N so that V_i may be considered as an R-module for each $i \in \{1, \ldots, t\}$. Furthermore, since V_i is a simple $\mathrm{End}_{D_i}(V_i)$-module it follows that V_i is a simple R-module for each $i \in \{1, \ldots, t\}$. In particular, this implies that

$$J(R) \subseteq \bigcap_{i=1}^{t} \mathrm{Ann}_R(V_i)$$

We will use this result below.

Towards this end, fix any $N \in \{1, \ldots, t\}$. We claim that $\mathrm{Ann}_R(V_N) = \ker(\pi_N)$. Towards this end, suppose first that $\theta \in \mathrm{Ann}_R(V_N)$. Then

$$0 = \theta v = \pi_N(\theta)(v) \quad \text{for each} \quad v \in V_N$$

In other words, we see $\pi_N(\theta) : V_N \to V_N$ is the zero map so that $\theta \in \ker(\pi_N)$. On the other hand, suppose that $\theta \in \ker(\pi_N)$. Then $\pi_N(\theta) : V_N \to V_N$ is the zero map so that

$$0 = \pi_N(\theta)(v) = \theta v \quad \text{for each} \quad v \in V_N$$

In other words, we see $\theta V_N = \{0\}$ so that $\theta \in \mathrm{Ann}_R(V_N)$. Thus, since $N \in \{1, \ldots, t\}$ was arbitrary we conclude that $\mathrm{Ann}_R(V_i) = \ker(\pi_i)$ for each $i \in \{1, \ldots, n\}$. Therefore, by the above we now have

$$J(R) \subseteq \bigcap_{i=1}^{t} \ker(\pi_i)$$

Moreover, if $\theta \in \ker(\pi_i)$ for each $i \in \{1, \ldots, t\}$ then $\theta = 0$ so that by the above inclusion we have $J(R) \subseteq \{0\}$. We conclude that $J(R) = \{0\}$ and hence R is primitive. $\square$

Lemma. Let R be a left-Artinian ring and suppose that V is a simple R-module. Then $R/\mathrm{Ann}_R(V)$ is a left-Artinian, simple ring.

Proof. First, note that since R is left-Artinian and as the homomorphic image of a left-Artinian ring is a left-Artinian ring we have that $R/\mathrm{Ann}_R(V)$ is a left-Artinian ring. Now, we claim that $R/\mathrm{Ann}_R(V)$ is a primitive ring. Towards this end, note that since V is an R-module we have that V is an $R/\mathrm{Ann}_R(V)$-module with action defined by for $r + \mathrm{Ann}_R(V) \in R/\mathrm{Ann}_R(V)$ and $v \in V$ we have $(r + \mathrm{Ann}_R(V))v = rv$. Now, since V is a simple R-module it follows that V is a simple $R/\mathrm{Ann}_R(V)$-module. Furthermore, suppose that $r + \mathrm{Ann}_R(V) \in \mathrm{Ann}_{R/\mathrm{Ann}_R(V)}(V)$ so that

$$0 = (r + \mathrm{Ann}_R(V))v = rv \quad \text{for each} \quad v \in V$$

Then by the above equality, we see that $r \in \mathrm{Ann}_R(V)$ so that $r + \mathrm{Ann}_R(V) = \mathrm{Ann}_R(V)$ and hence $\mathrm{Ann}_{R/\mathrm{Ann}_R(V)}(V)$ is trivial so that V is a faithful $R/\mathrm{Ann}_R(V)$-module.

Finally, note by the above results that V is a faithful, simple $R/\mathrm{Ann}(V)$-module so that $R/\mathrm{Ann}(V)$ is a left-Artinian, primitive ring. By the Wedderburn-Artin Theorem Part I, then, we conclude that $R/\mathrm{Ann}(V)$ is a simple ring. This completes the proof. $\square$

Proof. (Continued; (i $\Rightarrow$ ii)): Let R be a nonzero, semisimple, left-Artinian ring. Suppose that $V_1, \ldots, V_n$ are simple R-modules with $\mathrm{Ann}(V_i) \neq \mathrm{Ann}(V_j)$ for any $i, j \in \{1, \ldots, n\}$ with $i \neq j$. Define $P_i = \mathrm{Ann}(V_i)$ for each $i \in \{1, \ldots, n\}$. Then by the above Lemma, we have that R/P_i is a simple ring and hence by the Fourth Isomorphism Theorem for Rings it follows that P_i is a maximal ideal of R for each $i \in \{1, \ldots, n\}$. Moreover, since R/P_i is a simple ring we have in particular that $(R/P_i)^2 \neq P_i$ and hence $R^2 \nsubseteq P_i$ for each $i \in \{1, \ldots, n\}$. By the previous two observations, we conclude that $P_i + P_j = R$ for $i, j \in \{1, \ldots, n\}$ with $i \neq j$ and that $R^2 + P_i = R$ for $i \in \{1, \ldots, n\}$.

Next, if $n = 1$ then the result is clearly true so suppose that $n \geq 2$. Define the map

$$\phi : R \to R/P_1 \times \cdots \times R/P_n \quad \text{by} \quad r \mapsto (r + P_1, \ldots, r + P_n)$$

and note that ϕ is clearly a ring homomorphism. Recall that $P_i + P_j = R$ for $i, j \in \{1, \ldots, n\}$ with $i \neq j$ so that

$$P_i + \prod_{j \in \{1, \ldots, n\}, j \neq i} (P_i + P_j) = R \quad \text{for each} \quad i \in \{1, \ldots, n\}$$

Now, expanding the above product we see that every summand is contained in P_i except for those summands which are contained in

$$P_1 \cdots P_{i-1} P_{i+1} \cdots P_n \subseteq P_1 \cap \cdots \cap P_{i-1} \cap P_{i+1} \cap \cdots \cap P_n \quad \text{for each} \quad i \in \{1, \ldots, n\}$$

and hence by the above we have

$$P_i + P_1 \cap \cdots \cap P_{i-1} \cap P_{i+1} \cap \cdots \cap P_n = R \quad \text{for each} \quad i \in \{1, \ldots, n\}$$

Thus, by the proof of the Chinese Remainder Theorem it now follows that ϕ is surjective.

Next, we know that

$$P_1 \supseteq P_1 \cap P_2 \supseteq P_1 \cap P_2 \cap P_3 \supseteq \cdots \supseteq P_1 \cap \cdots \cap P_n$$

Now, for the sake of contradiction suppose that $P_1 = P_1 \cap P_2$. Recall that $P_1 + P_2 = R$ and that $R^2 + P_1 = R$. Furthermore, we clearly have $P_1 = P_1 \cap P_2 \subseteq P_2$ and that $P_1 P_2, P_2 P_1 \subseteq P_1$. Hence, we obtain

$$\begin{aligned}
R &= R^2 + P_1 \\
&= (P_1 + P_2)^2 + P_1 \\
&= P_1^2 + P_1 P_2 + P_2 P_1 + P_2^2 + P_1 \\
&\subseteq P_1 + P_1 + P_1 + P_2^2 + P_1 \\
&= P_1 + P_2^2 \\
&\subseteq P_2 + P_2^2 \\
&= P_2
\end{aligned}$$

which implies that $P_2 = R$. However, this is a contradiction since P_2 is a maximal ideal of R so that in particular we have $P_2 \neq R$. Therefore, we conclude that $P_1 \neq P_1 \cap P_2$

which gives the strict inclusion $P_1 \supsetneq P_1 \cap P_2$. Thus, it now follows that we obtain the strictly decreasing sequence of ideals of R

$$P_1 \supsetneq P_1 \cap P_2 \supsetneq P_1 \cap P_2 \cap P_3 \supsetneq \cdots \supsetneq P_1 \cap \cdots \cap P_n$$

Therefore, since R is Artinian it now follows that $n < \infty$ and hence the set of annihilators of simple R-modules is finite.

Finally, let $P_1, \ldots, P_n$ be the finite number of distinct annihilators of the simple R-modules. Since R is semisimple, it follows that $P_1 \cap \cdots \cap P_n = \{0\}$. But recall that clearly $\ker \phi = P_1 \cap \cdots \cap P_n$ and hence by the previous result it now follows that $\ker \phi$ is trivial. Since ϕ is as surjective ring homomorphism, then, it now follows that ϕ is a ring isomorphism so that $R \simeq R/P_1 \times \cdots \times R/P_n$. Moreover, recall by the above Lemma that $R/P_1, \ldots, R/P_n$ are left-Artinian, simple rings. Thus, by the Wedderburn-Artin Theorem Part I we may now conclude that R/P_i is isomorphic to $\mathrm{End}_{D_i}(V_i)$ for some division ring D_i and some finite dimensional vector space V_i over D_i for each $i \in \{1, \ldots, n\}$. Thus, combining the previous two results we obtain the isomorphism

$$R \simeq R/P_1 \times \cdots \times R/P_n \simeq \mathrm{End}_{D_1}(V_1) \times \cdots \times \mathrm{End}_{D_n}(V_n)$$

Furthermore, as $R/P_1, \ldots, R/P_n$ are simple rings we have in particular $R/P_1, \ldots, R/P_n$ are nonzero rings and hence it follows by the above that $V_1, \ldots, V_n$ are nonzero, finite dimensional vector spaces over the division rings $D_1, \ldots, D_n$, respectively. This completes the proof. □

Proposition. Let R be a left-Artinian ring with identity 1_R and let M be a simple R-module. Then M is a unital R-module.

Proof. Let $\phi : R \to \mathrm{End}_{\mathbb{Z}}(M)$ denote the representation homomorphism and let $D = \mathrm{End}_R(M)$ which is a division ring by Schur's Lemma as M is a simple R-module. Furthermore, once again using the fact that M is a simple R-module and as R is left-Artinian it follows by the Wedderburn-Artin Theorem Part I that $\phi(R) = \mathrm{End}_D(M)$ and that M is finite dimensional over D. Now, note that clearly $1_M \in \mathrm{End}_D(M) = \phi(R)$ is an identity of $\phi(R)$. On the other hand, we have that $\phi(1_R)$ is an identity of $\phi(R)$. By the uniqueness of multiplicative identities, then, we have that $1_M = \phi(1_R)$. Finally, let $m \in M$. Then by the previous result, we have

$$1_R \cdot m = \phi(1_R)(m) = 1_M(m) = m$$

and since $m \in M$ was arbitrary the above equality shows that M is a unital R-module. This completes the proof. □

Corollary. If R is a left-Artinian ring with identity, then $J(R)$ is the intersection of the annihilators of all the simple unital left R-modules.

Proof. First, note that since R is a left-Artinian ring with identity we have by the previous result that if M is a simple R-module then M is a unital R-module. Thus, since $J(R)$ is equal to the intersection of all the annihilators of the simple R-modules and since each simple R-module is a unital R-module it now follows that $J(R)$ is the intersection of the annihilators of all the simple unital left R-modules. □

Topic 11: Algebras

Definition. Let K be a field. Then a ***(unital) algebra*** or a ***K-algebra*** is a ring A with identity together with an injective ring homomorphism $\phi : K \to Z(A)$ such that $\phi(1)$ is the identity of A. In particular, if A is a division ring we say that A is a ***division algebra*** over K.

Remark. $Z(A)$ contains a "copy" of K.

Proof. Since $\phi : K \to Z(A)$ is an *injective* ring homomorphism, this is immediate. □

Remark. A is a vector space over K.

Proof. Since A is a ring, we have that A is in particular an abelian group under addition. Now, define an action of K on A by for $k \in K$ and $a \in A$ we have $ka = \phi(k)a$. Clearly, this gives a well-defined action of K on A since ϕ maps K into A and as A is closed under multiplication since A is a ring. Also, since ϕ is a ring homomorphism it follows that this action of K on A satisfies the vector space axioms and hence A is a vector space over K. □

Remark. If A is finite dimensional over K, then A is both left-Artinian and left-Noetherian and right-Artinian and right-Noetherian.

Proof. We will show that A is left-Artinian and remark that the proof of the fact that A is left-Noetherian and right-Artinian and right-Noetherian are similar. Towards this end, suppose that

$$I_1 \supseteq I_2 \supseteq I_3 \supseteq \cdots \supseteq I_n \supseteq \cdots$$

is a decreasing chain of left ideals of A. Now, since A is a finite dimensional vector space over K it follows that the ideal I_i of A is a finite dimensional vector space over K for each $i \in \{1, 2, \dots\}$. Therefore, there must exist a positive integer N such that for all $n \geq N$ we have that $I_n = I_N$. We conclude that A is left-Artinian. □

Remark. If M is a unital left A-module, then M is naturally a vector space over K. If $\rho : A \to \mathrm{End}_{\mathbb{Z}}(M)$ is the representation homomorphism, then $\rho(A) \subseteq \mathrm{End}_K(M)$. Furthermore, we have $\mathrm{Id}_M K \subseteq \mathrm{End}_A(M)$.

Proof. First, we show that M is naturally a vector space over K. Indeed, first note that since M is a unital A-module that M is in particular an abelian group under addition. Now, define an action of K on M by for $k \in K$ and $m \in M$ we have $km = \phi(k)m$. Clearly, this gives a well-defined action of K on M since ϕ maps K into A and as M is a unital left A-module. Also, since ϕ is a ring homomorphism it follows that this action of K on M satisfies the vector space axioms and hence M is a vector space over K.

Secondly, we show that $\rho(A) \subseteq \mathrm{End}_K(M)$. Indeed, fix any $a \in A$ and first note that since ρ maps A into $\mathrm{End}_{\mathbb{Z}}(M)$ that $\rho(a)$ is an additive homomorphism. Next, notice

that if $k \in K$ and $m \in M$ we have since $\phi(K) \subseteq Z(A)$ that

$$\rho(a)(km) = a(km) = a(\phi(k)m) = (a\phi(k))m = (\phi(k)a)m = (ka)m = k(am) = k\rho(a)(m)$$

Combining the above results, then, we see that $\rho(a) \in \mathrm{End}_K(M)$ and as $a \in A$ was arbitrary we conclude $\rho(A) \subseteq \mathrm{End}_K(M)$.

Thirdly, we show that $\mathrm{Id}_M K \subseteq \mathrm{End}_A(M)$. Indeed, fix any element $k \in K$ and let $a \in A$ and $m_1, m_2 \in M$. Then we have

$$\begin{aligned}
(\mathrm{Id}_M k)(am_1 + m_2) &= \mathrm{Id}_M(am_1 + m_2)k \\
&= (am_1 + m_2)k \\
&= (am_1)k + m_2 k \\
&= a(m_1 k) + m_2 k \\
&= a(\mathrm{Id}_M(m_1)k) + \mathrm{Id}_M(m_2)k \\
&= a(\mathrm{Id}_M k)(m_1) + (\mathrm{Id}_M k)(m_2)
\end{aligned}$$

so that $\mathrm{Id}_M k \in \mathrm{End}_A(M)$ and as $k \in K$ was arbitrary we conclude $\mathrm{Id}_M K \subseteq \mathrm{End}_A(M)$. This completes the proof. □

Theorem. Let A be a semisimple finite dimensional algebra over a field K. Then $A \simeq \mathrm{Mat}_{n_1}(D_1) \times \cdots \times \mathrm{Mat}_{n_t}(D_t)$ where $n_1, \ldots, n_t$ are positive integers and $D_1, \ldots, D_t$ are division algebras over K.

Proof. Omitted. □

Example. Let G be a finite group and let K be a field. Then the group ring KG is an algebra over K.

Proof. We remark that the group ring KG has a vector space structure over K that is given by for $k \in K$ and $\sum_{g \in G} \lambda_g g \in KG$ we have

$$k\left(\sum_{g \in G} \lambda_g g\right) = \sum_{g \in G} (k\lambda_g) g$$

This completes the proof. □

Theorem. (Maschke's Theorem): Let G be a finite group and let K be a field. Then the group ring KG (which is an algebra over K by the above) is semisimple if and only if $\mathrm{char}(K)$ does not divide $|G|$.

Note: Before we begin the proof of either direction, we set up the situation as follows. Let $M = KG$ and consider M as a left KG-module. Let $\phi : KG \to \mathrm{End}_{\mathbb{Z}}(M)$ be the representation homomorphism. Then by Remark 4 above, we know that $\phi(KG) \subseteq \mathrm{End}_K(M)$ and hence we see that ϕ is a map $\phi : KG \to \mathrm{End}_K(M)$. Furthermore, for

$f \in \mathrm{End}_K(M)$ let $\mathrm{Tr}(f)$ denote the trace of f. Then for each $g \in G$, we have

$$\mathrm{Tr}(\phi(g)) = \begin{cases} |G|1_K & \text{if} \quad g = 1_G \\ 0 & \text{if} \quad g \neq 1_G \end{cases}$$

We will use these observations in the proofs of both directions.

Proof. For the first direction, suppose that $\mathrm{char}(K)$ does not divide $|G|$. For the sake of contradiction, suppose that KG is not semisimple so that $J(KG) \neq \{0\}$. Therefore, there is some nonzero element $r \in J(KG)$. Since r is nonzero and by multiplying by some element of G and of $K^\times$ if necessary, we can further assume that r may be written $r = 1_G + \sum_{g \in G - \{1_G\}} \lambda_g g$. Now, since KG is an algebra over K and as KG is finite dimensional over K as G is finite we have by Remark 3 above that in particular KG is left-Artinian and left-Noetherian. Thus, by a result from a previous lecture we have that $J(KG)$ is nilpotent. In particular, this implies since $r \in J(KG)$ that r is nilpotent. By this observation, it follows that $\mathrm{Tr}(\phi(r)) = 0$. On the other hand, as Tr and ϕ are both in particular K-linear maps we have by the above Note that

$$\begin{aligned}
\mathrm{Tr}(\phi(r)) &= \mathrm{Tr}\left(\phi\left(1_G + \sum_{g \in G - \{1_G\}} \lambda_g g\right)\right) \\
&= \mathrm{Tr}\left(\phi(1_G) + \phi\left(\sum_{g \in G - \{1_G\}} \lambda_g g\right)\right) \\
&= \mathrm{Tr}\left(\phi(1_G) + \sum_{g \in G - \{1_G\}} \phi(\lambda_g g)\right) \\
&= \mathrm{Tr}\left(\phi(1_G) + \sum_{g \in G - \{1_G\}} \lambda_g \phi(g)\right) \\
&= \mathrm{Tr}(\phi(1_G)) + \mathrm{Tr}\left(\sum_{g \in G - \{1_G\}} \lambda_g \phi(g)\right) \\
&= \mathrm{Tr}(\phi(1_G)) + \sum_{g \in G - \{1_G\}} \mathrm{Tr}(\lambda_g \phi(g)) \\
&= \mathrm{Tr}(\phi(1_G)) + \sum_{g \in G - \{1_G\}} \lambda_g \mathrm{Tr}(\phi(g)) \\
&= \mathrm{Tr}(\phi(1_G)) + 0 \\
&= |G|1_K
\end{aligned}$$

Therefore, we now have $0 = \mathrm{Tr}(\phi(r)) = |G|1_K$ which implies that $\mathrm{char}(K)$ divides $|G|$. However, this is a contradiction. We conclude that KG is semisimple, completing the proof of the first direction.

For the second direction, we will prove by contrapositive. Towards this end, suppose that $\mathrm{char}(K)$ divides $|G|$. Consider the element $c = \sum_{g \in G} g \in KG$. Clearly, we have $c \in Z(KG)$. Furthermore, since $\mathrm{char}(K)$ divides $|G|$ we obtain

$$c^2 = \left(\sum_{g \in G} g \right)^2 = |G| \sum_{g \in G} g = |G|c = 0$$

so that $c^2 = 0$. By the previous results, then, we see that $KGc = KGcKG$ is a nonzero, nilpotent, two-sided ideal of KG. Furthermore, we know that KG is left-Artinian and left-Noetherian by the above so that $J(KG)$ contains every nilpotent ideal of KG and hence $J(KG) \supseteq KGc \supsetneq \{0\}$ so that $J(KG) \neq \{0\}$. Thus, we see that KG is not semisimple. This completes the proof of the second direction. $\square$

Corollary. Let G be a finite group and let K be a field with $\mathrm{char}(K) = 0$. Then $KG \simeq \mathrm{Mat}_{n_1}(D_1) \times \cdots \times \mathrm{Mat}_{n_t}(D_t)$, where $n_1, \ldots, n_t$ are positive integers are $D_1, \ldots, D_t$ are finite dimensional division algebras over K.

Proof. Since G is a finite group, we know that KG is a finite dimensional algebra over K. Moreover, since $\mathrm{char}(K) = 0$ we know that in particular $\mathrm{char}(K)$ does not divide $|G|$ so that by Maschke's Theorem we have that KG is semisimple. By Theorem 1 from the previous lecture, then, we conclude that $KG \simeq \mathrm{Mat}_{n_1}(D_1) \times \cdots \times \mathrm{Mat}_{n_t}(D_t)$, where $n_1, \ldots, n_t$ are positive integers are $D_1, \ldots, D_t$ are finite dimensional division algebras over K. This completes the proof. $\square$

Definition. An algebra A over a field K is called ***central simple*** if A is simple (as a ring) and $Z(A) = 1_A K$.

Remark. If A is any algebra over a field K, we have $1_A K \subseteq Z(A)$.

Proof. Let $k \in K$ and $a \in A$. Then we have since $\phi(K) \subseteq Z(A)$ that

$$\begin{aligned}
(1_A k)a &= 1_A(ka) \\
&= 1_A(\phi(k)a) \\
&= 1_A(a\phi(k)) \\
&= (1_A a)\phi(k) \\
&= (a1_A)\phi(k) \\
&= a(1_A\phi(k)) \\
&= a(1_A k)
\end{aligned}$$

and hence $1_A k \in Z(A)$ so that $1_A K \subseteq Z(A)$. $\square$

Example. If K is a field, then K is a central simple algebra over K.

Proof. Since K is a field, we have in particular that K is a simple ring. Furthermore, since K is a field we have in particular that $Z(K) = K = 1_K K$, completing the proof. $\square$

Example. Let $\mathbb{H} = \{a + bi + cj + dk : a, b, c, d \in \mathbb{R}\}$ subject to the relations $i^2 = -1, j^2 = -1, k^2 = -1, ij = k = -ji$. Then $\mathbb{H}$ is called the ***Quaternion Algebra***. We have that $\mathbb{H}$ is a central simple algebra over $\mathbb{R}$ and $\mathbb{H}$ is a division algebra over $\mathbb{R}$.

Proof. First, note that $\mathbb{H}$ is clearly an algebra over $\mathbb{R}$. Next, we have that $\mathbb{H}^2 \neq \{0\}$. Moreover, suppose that I is a nontrivial two-sided ideal of $\mathbb{H}$. Then since I contains a nonzero element, it follows that I contains the identity of $\mathbb{H}$ and since I is an ideal of $\mathbb{H}$ this implies that $I = \mathbb{H}$. Therefore, we see that $\mathbb{H}$ is a simple ring. Finally, by the relations above we must have that $Z(\mathbb{H}) = \mathbb{R} = 1_{\mathbb{H}}\mathbb{R}$. It now follows that $\mathbb{H}$ is a central simple algebra over $\mathbb{R}$.

Finally, we show that $\mathbb{H}$ is a division ring. Towards this end, suppose that $a + bi + cj + dk \in \mathbb{H}$. Then by the above relations, we have

$$(a + bi + cj + dk)(a - bi - cj - dk) = a^2 + b^2 + c^2 + d^2$$

Now, suppose that $a + bi + cj + dk \in \mathbb{H}$ is a nonzero element of $\mathbb{H}$. Then clearly, we have $a^2 + b^2 + c^2 + d^2 \neq 0$ so that we may define

$$\frac{a - bi - cj - dk}{a^2 + b^2 + c^2 + d^2} \in \mathbb{H}$$

Furthermore, we have by the above that

$$\frac{a - bi - cj - dk}{a^2 + b^2 + c^2 + d^2} \cdot (a + bi + cj + dk) = \frac{a^2 + b^2 + c^2 + d^2}{a^2 + b^2 + c^2 + d^2} = 1$$

and

$$(a + bi + cj + dk) \cdot \frac{a - bi - cj - dk}{a^2 + b^2 + c^2 + d^2} = \frac{a^2 + b^2 + c^2 + d^2}{a^2 + b^2 + c^2 + d^2} = 1$$

so that

$$(a + bi + cj + dk)^{-1} = \frac{a - bi - cj - dk}{a^2 + b^2 + c^2 + d^2} \in \mathbb{H}$$

and thus $\mathbb{H}$ is a division ring. Since $\mathbb{H}$ is an algebra over $\mathbb{R}$, then, we may now conclude that $\mathbb{H}$ is a division algebra over $\mathbb{R}$. $\square$

Remark. Let A and B be algebras over a field K. Then $A \otimes_K B$ is an algebra over K with multiplication given by

$$(a \otimes_K b)(a' \otimes_K b') = (aa') \otimes_K (bb')$$

for all $a, a' \in A$ and $b, b' \in B$.

Proof. We first sketch a proof that the above multiplication is well-defined. Towards this end, fix $a \in A$ and $b \in B$ and define a map

$$b_1 : A \times B \to A \otimes_K B \quad \text{by} \quad (a', b') \mapsto (aa') \otimes_K (bb')$$

Then b_1 is a well-defined K-bilinear map. Therefore, there exists a (unique) group homomorphism

$$\phi_{(a,b)} : A \otimes_K B \to A \otimes_K B \quad \text{such that} \quad a' \otimes_K b' \mapsto b_1(a', b') = (aa') \otimes_K (bb')$$

Thus, since the fixed elements $a \in A$ and $b \in B$ were arbitrary it now follows that for any $(a, b) \in A \times B$ there exists a group homomorphism $\phi_{(a,b)} : A \otimes_K B \to A \otimes_K B$ such that $\phi_{(a,b)}(a' \otimes_K b') = (aa') \otimes_K (bb')$ for all $a' \in A$ and $b' \in B$.

Finally, define a map

$$b_2 : A \times B \to \mathrm{Hom}_K(A \otimes_K B, A \otimes_K B) \quad \text{by} \quad (a, b) \mapsto \phi_{(a,b)}$$

Then b_2 is a well-defined K-bilinear map. Therefore, there exists a (unique) group homomorphism

$$\psi : A \otimes_K B \to \mathrm{Hom}_K(A \otimes_K B, A \otimes_K B) \quad \text{such that} \quad a \otimes_K b \mapsto b_2(a, b) = \phi_{(a,b)}$$

Now, for $\alpha, \beta \in A \otimes_K B$ define the product $\alpha \cdot \beta = \psi(\alpha)(\beta)$. Then this is the product as defined above and hence the multiplication is well-defined.

We now show that $A \otimes_K B$ is an algebra over K. First, note that by the above results we have that $A \otimes_K B$ is a ring with identity $1_A \otimes_K 1_B$. Now, since A and B are algebras over K we have in particular that A and B are vector spaces over K and hence $A \otimes_K B$ is a vector space over K. Let $\lambda \in K$. We claim that $\lambda(1_A \otimes_K 1_B) \in Z(A \otimes_K B)$. Indeed, first note that $\lambda(1_A \otimes_K 1_B) = (\lambda 1_A) \otimes_K 1_B$. Furthermore, suppose that $a \in A$ and $b \in B$. Then by the previous observation, we have

$$(\lambda(1_A \otimes_K 1_B))(a \otimes_K b) = ((\lambda 1_A) \otimes_K 1_B)(a \otimes_K b) = ((\lambda 1_A)a) \otimes_K (1_B b)$$

and

$$(a \otimes_K b)(\lambda(1_A \otimes_K 1_B)) = (a \otimes_K b)((\lambda 1_A) \otimes_K 1_B) = (a(\lambda 1_A)) \otimes_K (b 1_B)$$

Now, notice that since A is an algebra over K that

$$(\lambda 1_A)a = \lambda(1_A a) = \lambda a$$

and

$$a(\lambda 1_A) = (a\lambda)1_A = (\lambda a)1_A = \lambda(a 1_A) = \lambda a$$

Moreover, we clearly have $1_B b = b = b 1_B$ and hence by combining the previous results we obtain that $(\lambda(1_A \otimes_K 1_B))(a \otimes_K b) = (a \otimes_K b)(\lambda(1_A \otimes_K 1_B))$ so that $\lambda(1_A \otimes_K 1_B) \in Z(A \otimes_K B)$. Therefore, if we define

$$\phi : K \to Z(A \otimes_K B) \quad \text{by} \quad \lambda \mapsto \lambda(1_A \otimes_K 1_B)$$

then by the above results we see that ϕ is a well-defined injective ring homomorphism such that $\phi(1_K) = 1_{A \otimes_K B}$. We conclude that $A \otimes_K B$ is an algebra over K. $\square$

Theorem. Let A be a central simple algebra over K and let B be a simple algebra over K. Then $A \otimes_K B$ is a simple algebra over K.

Proof. First, we show that $(A \otimes_K B)^2 \neq \{0\}$. Indeed, note that since A and B are in particular simple rings we have $A^2 \neq \{0\}$ and $B^2 \neq \{0\}$. Therefore, there is some $a \in A$ such that $a^2 \neq 0$ and there is some $b \in B$ such that $b^2 \neq 0$. Now, notice that $a \otimes_K b \in A \otimes_K B$ so that $(a \otimes_K b)^2 \in (A \otimes_K B)^2$. Furthermore, since $a^2, b^2 \neq 0$ we have

$$(a \otimes_K b)^2 = (a \otimes_K b)(a \otimes_K b) = a^2 \otimes_K b^2 \neq 0$$

and hence $(A \otimes_K B)^2 \neq \{0\}$.

Next, we show that $A \otimes_K B$ contains no proper, nontrivial, two-sided ideals. Towards this end, let I be a nontrivial, two-sided ideal of $A \otimes_K B$. Now, since B is an algebra over K we know that B is a vector space over K. Therefore, there is some basis $Y \subseteq B$ for B over K. Similarly, since A is an algebra over K we know that A is a vector space over K. By the previous observations, then, there is some nonzero element $u \in I$ that can be written $u = \sum_{i=1}^{n} a_i \otimes_K y_i$ where $a_1, \ldots, a_n \in A, y_1, \ldots, y_n \in Y$, and n is chosen to be as small as possible. In particular, since u is nonzero we have $n \geq 1$.

Now, by the minimality of n it follows that $a_1 \neq 0$. Therefore, since A has identity we see that Aa_1A is a nontrivial, two-sided ideal of A and since A is a simple ring we conclude that $Aa_1A = A$. Thus, since A has identity there are $r_1, \ldots, r_t, s_1, \ldots, s_t \in A$ such that $1_A = \sum_{i=1}^{t}(r_i a_1 s_i)$. Next, define

$$v = \sum_{j=1}^{t}[(r_j \otimes_K 1_B)u(s_j \otimes_K 1_B)]$$

Then since I is a two-sided ideal of $A \otimes_K B$ and as $u \in I$, we have by the above definition of v that $v \in I$. Moreover, we have by the definition of the tensor product that

$$\begin{aligned}
v &= \sum_{j=1}^{t}[(r_j \otimes_K 1_B)u(s_j \otimes_K 1_B)] \\
&= \sum_{j=1}^{t}\left[(r_j \otimes_K 1_B)\left(\sum_{i=1}^{n}(a_i \otimes_K y_i)\right)(s_j \otimes_K 1_B)\right] \\
&= \sum_{i=1}^{n}\left[\left(\sum_{j=1}^{t}(r_j a_i s_j)\right) \otimes_K y_i\right] \\
&= \sum_{j=1}^{t}(r_j a_1 s_j \otimes_K y_1) + \sum_{i=2}^{n}\left[\left(\sum_{j=1}^{t}(r_j a_i s_j)\right) \otimes_K y_i\right] \\
&= \sum_{j=1}^{t}(r_j a_1 s_j) \otimes_K y_1 + \sum_{i=2}^{n}\left[\left(\sum_{j=1}^{t}(r_j a_i s_j)\right) \otimes_K y_i\right] \\
&= 1_A \otimes_K y_1 + \sum_{i=2}^{n}\left[\left(\sum_{j=1}^{t}(r_j a_i s_j)\right) \otimes_K y_i\right]
\end{aligned}$$

Now, for each $i \in \{2, \ldots, n\}$ define $\overline{a_i} = \sum_{j=1}^{t}(r_j a_i s_j)$ so that by the above we see

$$v = 1_A \otimes_K y_1 + \sum_{i=2}^{n} \overline{a_i} \otimes_K y_i \in I$$

We will use this result below.

Now, fix any $a \in A$. Then since I is an ideal of $A \otimes_K B$ and as $v \in I$ we have that the element $w = (a \otimes_K 1_B)v - v(a \otimes_K 1_B) \in I$. Moreover, notice that

$$\begin{aligned} w &= (a \otimes_K 1_B)v - v(a \otimes_K 1_B) \\ &= 0 + \sum_{i=2}^{n} [(a\overline{a_i} - \overline{a_i}a) \otimes_K y_i] \\ &= \sum_{i=2}^{n} [(a\overline{a_i} - \overline{a_i}a) \otimes_K y_i] \end{aligned}$$

Since $w \in I$, then, we have by the above equality and by our choice that $w = 0$ and hence it follows that $a\overline{a_i} = \overline{a_i}a$ for each $i \in \{2, \ldots, n\}$. Thus, since $a \in A$ was arbitrary and as A is central simple we obtain $\overline{a_i} \in Z(A) = K$ for each $i \in \{2, \ldots, n\}$ so that

$$b = y_1 + \sum_{i=2}^{n} \overline{a_i} y_i$$

is a nonzero K-linear combination of elements from the basis Y for B over K. In particular, this gives that $b \neq 0$.

Finally, by the above results we may now assert that

$$\begin{aligned} v &= 1_A \otimes_K y_1 + \sum_{i=2}^{n} [\overline{a_i} \otimes_K y_i] \\ &= 1_A \otimes_K y_1 + \sum_{i=2}^{n} [1_A \otimes_K \overline{a_i} y_i] \\ &= 1_A \otimes_K \left(y_1 + \sum_{i=2}^{n} \overline{a_i} y_i \right) \\ &= 1_A \otimes_K b \end{aligned}$$

Furthermore, since b is nonzero by the above and as B has identity we have that BbB is a nontrivial two-sided ideal of B so that since B is in particular a simple ring we have $BbB = B$. Therefore, there are elements $b_1, \ldots, b_k, c_1, \ldots, c_k \in B$ such that

$$1_B = \sum_{i=1}^{k} b_i b c_i$$

Now, since I is an ideal of $A \otimes_K B$ and as $v \in I$ we have

$$\sum_{i=1}^{k} [(1_A \otimes_K b_i)v(1_A \otimes_A c_i)] \in I$$

But notice that

$$\begin{aligned}\sum_{i=1}^{k}[(1_A \otimes_K b_i)v(1_A \otimes_A c_i)] &= \sum_{i=1}^{k}[(1_A \otimes_K b_i)(1_A \otimes_K b)(1_A \otimes_A c_i)] \\ &= \sum_{i=1}^{k}[1_A \otimes_K b_i b c_i] \\ &= 1_A \otimes_K \left(\sum_{i=1}^{k} b_i b c_i\right) \\ &= 1_A \otimes_K 1_B\end{aligned}$$

and hence the identity element $1_A \otimes_K 1_B$ of $A \otimes_K B$ is in the ideal I of $A \otimes_K B$ so that $I = A \otimes_K B$. Therefore, we see that $A \otimes_K B$ contains no proper, nontrivial, two-sided ideals. This completes the proof that $A \otimes_K B$ is a simple ring and hence $A \otimes_K B$ is a simple algebra over K. □

Definition. If A is an algebra, we define the op-***algebra*** of A, denoted A^{op}, to be the set A together with the vector space structure of A and multiplication $*$ given by $a * b = ba$ for all $a, b \in A$.

Definition. Let A and B be algebras over a field K. An ***algebra homomorphism*** is a map $\phi : A \to B$ that is both a ring homomorphism and a K-module homomorphism.

Theorem. Let A be a central simple finite dimensional algebra over a field K. Then $A \otimes_K A^{\text{op}} \simeq \text{End}_K(M)$, where M is A viewed as a vector space over K.

Proof. First, define two maps

$$\phi_\ell : A \to \text{End}_K(M) \quad \text{by} \quad \phi_\ell(a) : M \to M \quad \text{by} \quad \phi_\ell(a)(m) = am$$

and

$$\phi_r : A \to \text{End}_K(M) \quad \text{by} \quad \phi_r(a) : M \to M \quad \text{by} \quad \phi_r(a)(m) = ma$$

for all $a \in A$ and $m \in M$. Then it is easily verified $\phi_\ell : A \to \text{End}_K(M)$ and that $\phi_r : A^{\text{op}} \to \text{End}_K(M)$ are algebra homomorphisms. Furthermore, every element of the image of ϕ_ℓ commutes with every element of the image of ϕ_r. Now, set

$$m : A \times A^{\text{op}} \to \text{End}_K(M) \quad \text{by} \quad m(a, b) = \phi_\ell(a) \circ \phi_r(b)$$

for all $a \in A$ and $b \in A^{\text{op}}$. Then m is a K-bilinear map and hence there exists a (unique) K-linear map

$$\phi : A \otimes_K A^{\text{op}} \to \text{End}_K(M) \quad \text{such that} \quad \phi(a \otimes_K b) = \phi_\ell(a) \circ \phi_r(b)$$

for all $a \in A$ and $b \in A^{\text{op}}$.

Finally, since ϕ is K-linear and as

$$\phi((a \otimes_K b)(a' \otimes_K b')) = \phi((aa') \otimes_K (bb')) = \phi(a \otimes_K b) \circ \phi(a' \otimes_K b')$$

for all $a, a' \in A$ and $b, b' \in B$ we see that ϕ is in fact an algebra homomorphism. Moreover, notice that $\phi(1_A \otimes_K 1_{A^{\mathrm{op}}}) = \mathrm{Id}_M \neq 0$ since M is in particular a simple ring so that $M \neq 0$. In particular, this implies that $\phi : A \otimes_K A^{\mathrm{op}} \to \mathrm{End}_K(M)$ is a nonzero map so that $\ker \phi \neq A \otimes_K A^{\mathrm{op}}$. But by the previous Theorem, we have since A is a central simple algebra over K that $A \otimes_K A^{\mathrm{op}}$ is a simple algebra over K so that in particular $A \otimes_K A^{\mathrm{op}}$ is a simple ring. Therefore, since $\ker \phi \neq A \otimes_K A^{\mathrm{op}}$ it follows that $\ker \phi$ is trivial so that since ϕ is an algebra homomorphism we have that ϕ is an injection. Thus, we see that since A is finite dimensional over K that

$$\dim_K(A \otimes_K A^{\mathrm{op}}) = (\dim(A))^2 < \infty$$

and

$$\dim_K(\mathrm{End}_K(M)) = (\dim_K(M))^2 = (\dim_K(A))^2 < \infty$$

and hence ϕ is a surjection. Thus, we conclude that $\phi : A \otimes_K A^{\mathrm{op}} \to \mathrm{End}_K(M)$ is an algebra isomorphism so that $A \otimes_K A^{\mathrm{op}} \simeq \mathrm{End}_K(M)$. This completes the proof. $\square$

Spring Semester 2017 Homework Problems

Homework 1: Page 121 #12; Page 134 #17; Page 140 #3, 4

Problem 12. *An element of a ring is called* ***nilpotent*** *if $a^n = 0$ for some n. Prove that in a commutative ring $a + b$ is nilpotent if a and b are. Show that this result may be false if R is not commutative.*

Proof. Let R be a commutative ring and suppose that $a, b \in R$ are nilpotent. Then there exist positive integers n and m such that $a^n = 0$ and $b^m = 0$. Without loss of generality, assume that $n \geq m$ and let $z = 2n$. Since R is a commutative ring, we have by the Binomial Theorem that

$$(a+b)^z = c_0 a^z + c_1 a^{z-1} b + \cdots + c_n a^{z-n} b^n + \cdots + c_{z-1} a b^{z-1} + c_z b^z$$

for some $c_0, \ldots, c_z \in \mathbb{Z}$. By the definition of z, we have $z - i \geq n$ for all $i \in \{0, \ldots, n\}$. Thus, by the above equality, this observation gives that $(a+b)^z = 0$. In particular, this proves that $a + b$ is nilpotent.

Finally, we show that the above result need not be true if R is not commutative. Indeed, let R denote the ring of all 2×2 matrices with entries in $\mathbb{Z}$ and observe that R is not commutative. Now, consider

$$A = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \in R$$

and

$$B = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} \in R$$

Clearly, we have $A^2 = 0 = B^2$ so that A and B are nilpotent elements of R. However, notice that

$$A + B = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

so that $A + B$ is the 2×2 identity matrix. Thus, we have

$$(A+B)^n = A + B \neq 0$$

for all positive integers n. In particular, the above results show that $A+B$ is not nilpotent despite the fact that A and B are both nilpotent. This completes the proof. $\square$

Problem 17. *Let $f : R \to S$ be an epimorphism of rings with kernel K.*

(a): *If P is a prime ideal in R that contains K, then $f(P)$ is a prime ideal in S.*

(b): *If Q is a prime ideal in S, then $f^{-1}(Q)$ is a prime ideal in R that contains K.*

(c): *There is a one-to-one correspondence between the set of all prime ideals in R that contain K and the set of all prime ideals in S, given by $P \mapsto f(P)$.*

(d): *If I is an ideal in a ring R, then every prime ideal in R/I is of the form P/I, where P is a prime ideal in R that contains I.*

Proof. (a): First, we show that $f(P)$ is an ideal in S. Towards this end, let $s_1, s_2 \in f(P)$. Then there exist $r_1, r_2 \in P$ such that $f(r_1) = s_1$ and $f(r_2) = s_2$. Since P is an ideal in R, it follows that $r_1 - r_2 \in P$. But since f is a ring homomorphism, we now have

$$s_1 - s_2 = f(r_1) - f(r_2) = f(r_1 - r_2) \in f(P)$$

This shows that $f(P)$ is a subgroup of S under addition. Finally, let $s \in S$ and $s' \in f(P)$. Then there exists some $r' \in P$ such that $f(r') = s'$. Since f is a surjection, there exists some $r \in R$ such that $f(r) = s$. Since P is an ideal in R, we have that $rr' \in P$. Thus, since f is a ring homomorphism, we obtain

$$ss' = f(r)f(r') = f(rr') \in f(P)$$

Similarly, we obtain $s's \in f(P)$. The above results show that $f(P)$ is an ideal in S.

Now, as P is a prime ideal in R we have $P \neq R$ so that $f(P) \neq S$. Suppose that $s_1 s_2 \in f(P)$ for some $s_1, s_2 \in S$. Since $s_1 s_2 \in f(P)$, there is some $r \in P$ such that $f(r) = s_1 s_2$. Furthermore, since f is surjective, there are $r_1, r_2 \in R$ such that $f(r_1) = s_1$ and $f(r_2) = s_2$. Finally, note that since f is a ring homomorphism we have

$$f(r_1 r_2 - r) = f(r_1)f(r_2) - f(r) = s_1 \cdot s_2 - s_1 s_2 = s_1 s_2 - s_1 s_2 = 0$$

so that $r_1 r_2 - r \in K \subseteq P$. But as $r \in P$, we now have $r_1 r_2 \in P$. Since P is a prime ideal in R, this forces either $r_1 \in P$ or $r_2 \in P$ so that either $s_1 = f(r_1) \in f(P)$ or $s_2 = f(r_2) \in f(P)$. This completes the proof that $f(P)$ is a prime ideal in S. $\square$

Proof. (b): First, we show that $f^{-1}(Q)$ is an ideal in R containing K. Towards this end, let $r_1, r_2 \in f^{-1}(Q)$ so that $f(r_1), f(r_2) \in Q$. Since Q is an ideal in S, it follows that $f(r_1) - f(r_2) \in Q$. But since f is a ring homomorphism, we now have

$$f(r_1 - r_2) = f(r_1) - f(r_2) \in Q$$

so that $r_1 - r_2 \in f^{-1}(Q)$. This shows that $f^{-1}(Q)$ is a subgroup of R under addition. Finally, let $r \in R$ and $s \in f^{-1}(Q)$ so that $f(s) \in Q$. Since Q is an ideal in S and as f is a ring homomorphism, we have

$$f(rs) = f(r)f(s) \in Q$$

so that $rs \in f^{-1}(Q)$. Similarly, we obtain $sr \in f^{-1}(Q)$. The above results show that $f^{-1}(Q)$ is an ideal in R. Lastly, let $r \in K$. Then $f(r) = 0 \in Q$ since Q is an ideal. Thus, we have $r \in f^{-1}(Q)$ so that $K \subseteq f^{-1}(Q)$.

Now, as Q is a prime ideal in S we have $Q \neq S$ so that $f^{-1}(Q) \neq R$. Suppose that $r_1 r_2 \in f^{-1}(Q)$ for some $r_1, r_2 \in R$. Since $r_1 r_2 \in f^{-1}(Q)$, we have $f(r_1 r_2) \in Q$. But since f is a ring homomorphism, we have

$$f(r_1)f(r_2) = f(r_1 r_2) \in Q$$

Since Q is a prime ideal in S, the above shows that either $f(r_1) \in Q$ or $f(r_2) \in Q$. In other words, we have either $r_1 \in f^{-1}(Q)$ or $r_2 \in f^{-1}(Q)$. This completes the proof that $f^{-1}(Q)$ is a prime ideal in S containing K. □

Proof. (c): Let $\mathcal{A}$ denote the set of all prime ideals in R that contain K and let $\mathcal{B}$ denote the set of all prime ideals in S. Define $\Phi : \mathcal{A} \to \mathcal{B}$ by $\Phi(P) = f(P)$ for all $P \in \mathcal{A}$. By Part (a), it follows that Φ is a well-defined map. Similarly, define $\Psi : \mathcal{B} \to \mathcal{A}$ by $\Psi(Q) = f^{-1}(Q)$ for all $Q \in \mathcal{B}$. By Part (b), it follows that Ψ is a well-defined map. Finally, notice that Ψ is a two-sided inverse of Φ so that Φ is a bijection. In other words, we have shown that there is a one-to-one correspondence between $\mathcal{A}$ and $\mathcal{B}$ given by $P \mapsto f(P)$. This completes the proof. □

Proof. (d): Consider the canonical projection map $\pi : R \to R/I$ and recall that π is an epimorphism of rings with kernel I. By Part (c), there is a one-to-one correspondence between the set of all prime ideals in R that contain I and the set of all prime ideals in R/I given by $P \mapsto \pi(P)$.

Now, let Q be a prime ideal in R/I. By the previous observation, there is a (unique) prime ideal P of R containing I such that $P \mapsto Q$. However, we have by the definition of this correspondence and by the definition of π that $P \mapsto \pi(P) = P/I$. Hence, we obtain $Q = P/I$. This completes the proof. □

Problem 3. *Let R be the subring $\{a + b\sqrt{10} : a, b \in \mathbb{Z}\}$ of the field of real numbers.*

(a): *The map $N : R \to \mathbb{Z}$ given by $a + b\sqrt{10} \mapsto (a + b\sqrt{10})(a - b\sqrt{10}) = a^2 - 10b^2$ is such that $N(uv) = N(u)N(v)$ for all $u, v \in R$ and $N(u) = 0$ if and only if $u = 0$.*

(b): *u is a unit in R if and only if $N(u) = \pm 1$.*

(c): *$2, 3, 4 + \sqrt{10}$, and $4 - \sqrt{10}$ are irreducible elements of R.*

(d): *$2, 3, 4 + \sqrt{10}$, and $4 - \sqrt{10}$ are not prime elements of R.*

Proof. (a): Let $u = a + b\sqrt{10}$ and $v = c + d\sqrt{10}$ be elements of R. Note that

$$N(u) = a^2 - 10b^2$$

and

$$N(v) = c^2 - 10d^2$$

so that

$$N(u)N(v) = (a^2 - 10b^2)(c^2 - 10d^2) = a^2c^2 - 10a^2d^2 - 10b^2c^2 + 100b^2d^2$$

Furthermore, we have

$$uv = (a + b\sqrt{10})(c + d\sqrt{10}) = (ac + 10bd) + (ad + bc)\sqrt{10}$$

so that

$$N(uv) = (ac + 10bd)^2 - 10(ad + bc)^2 = a^2c^2 - 10a^2d^2 - 10b^2c^2 + 100b^2d^2 = N(u)N(v)$$

We now prove the second result. Towards this end, let $u = a + b\sqrt{10} \in R$. For the first direction, assume that $N(u) = 0$ so that

$$0 = N(u) = a^2 - 10b^2$$

which gives

$$a^2 = 10b^2$$

Hence, we have $a = \pm b\sqrt{10}$. But since $a, b \in \mathbb{Z}$, this forces $b = 0$ and since $a^2 = 10b^2$, we now also have $a = 0$. Thus, we obtain $u = a + b\sqrt{10} = 0$.

For the second direction, assume that $u = 0$. In this case, we have $a = 0 = b$ so that

$$N(u) = a^2 - 10b^2 = 0$$

This completes the proof. □

Proof. (b): For the first direction, assume that $u = a + b\sqrt{10} \in R$ is a unit in R. Then there exists some $v \in R$ such that $uv = 1$. By Part (a), we have

$$1 = 1^2 = N(1) = N(uv) = N(u)N(v)$$

But since $N(u), N(v) \in \mathbb{Z}$, the above equality now forces $N(u) = \pm 1$. This completes the proof of the first direction.

For the second direction, assume that $N(u) = \pm 1$. First, suppose that $N(u) = 1$. Define $v = a - b\sqrt{10} \in R$. Then we have

$$1 = N(u) = N(a + b\sqrt{10}) = a^2 - 10b^2 = (a + b\sqrt{10})(a - b\sqrt{10}) = uv$$

so that $v \in R$ is the inverse of u. This shows that u is a unit in R. Secondly, suppose that $N(u) = -1$. Define $v = -a + b\sqrt{10} \in R$. Then we have

$$-1 = N(u) = N(a + b\sqrt{10}) = a^2 - 10b^2 = (a + b\sqrt{10})(a - b\sqrt{10}) = u \cdot -v$$

Multiplying both sides of the above equality by -1, we obtain $1 = uv$ so that $v \in R$ is the inverse of u. This shows that u is a unit in R. This completes the proof of the second direction. □

Proof. (c): For the sake of contradiction, suppose that 2 were not irreducible in R. Then there exist nonzero, nonunits $u, v \in R$ such that $2 = uv$. By Part (a), we now have

$$4 = 2^2 = N(2) = N(uv) = N(u)N(v)$$

Since u and v are nonunits, Part (b) gives that $N(u), N(v) \neq \pm 1$. Hence, by the above equality, we now have $N(u) = \pm 2$.

First, suppose that $N(u) = 2$. Since $u \in R$, we can write $u = a + b\sqrt{10}$ for some $a, b \in \mathbb{Z}$. This gives

$$2 = N(u) = N(a + b\sqrt{10}) = a^2 - 10b^2$$

which forces a^2 to be congruent to 2 modulo 10. However, this is not possible. We conclude that $N(u) \neq 2$. Similarly, we obtain that $N(u) \neq -2$. But this is a contradiction. Therefore, we have that 2 is an irreducible element in R.

Using analogous arguments, we conclude that $3, 4+\sqrt{10}$, and $4-\sqrt{10}$ are irreducible elements of R. This completes the proof. □

Proof. (d): First, note that

$$3 \cdot 2 = 6 = (4 + \sqrt{10})(4 - \sqrt{10})$$

Now, for the sake of contradiction, suppose that 2 were a prime element of R. By the above equality, it must be the case that either 2 divides $4 + \sqrt{10}$ or 2 divides $4 - \sqrt{10}$ in R. If 2 divides $4 + \sqrt{10}$ in R, then there is some $u \in R$ such that $4 + \sqrt{10} = 2u$. By Part (a), this gives

$$6 = 4^2 - 10 = N(4 + \sqrt{10}) = N(2u) = N(2)N(u) = 2^2 \cdot N(u) = 4N(u)$$

By the above equality, we now have that 4 divides 6 in $\mathbb{Z}$ which is clearly a contradiction. Thus, it cannot be the case that 2 divides $4 + \sqrt{10}$ in R. Similarly, we obtain that 2 cannot divide $4 - \sqrt{10}$ in R. But this is a contradiction. Therefore, we have that 2 is not a prime element in R.

Using analogous arguments, we conclude that $3, 4+\sqrt{10}$, and $4-\sqrt{10}$ are not prime elements of R. This completes the proof. □

Problem 4. *Show that in the integral domain of Exercise 3 every element can be factored into a product of irreducibles, but this factorization need not be unique.*

Proof. Let R be the integral domain of Exercise 3 and let $u \in R$ be a nonzero, nonunit. We show by induction on $|N(u)|$ that u can be factored into a product of irreducibles of R. Since u is a nonzero, nonunit, it follows by the previous problem that $|N(u)| \geq 2$.

For the base case, assume that $|N(u)| = 2$ and write $u = vw$ for some $v, w \in R$. Then by the previous problem, we have

$$2 = |N(u)| = |N(vw)| = |N(v)N(w)| = |N(v)||N(w)|$$

so that either $N(v) = \pm 1$ or $N(w) = \pm 1$. By the previous problem, this implies that either v or w is a unit in R and hence $u = vw$ is itself irreducible, completing the proof of the base case.

Finally, assume that u is not irreducible. Then we can write $u = vw$ for some nonunits $v, w \in R$ and since $u = vw$ is nonzero, we also have that v and w are nonzero. Hence, since $v, w \in R$ are nonzero, nonunits, we have by the previous problem that $|N(v)|, |N(w)| \geq 2$. Furthermore, we have by the previous problem that

$$|N(u)| = |N(vw)| = |N(v)N(w)| = |N(v)||N(w)|$$

Thus, since $|N(v)|, |N(w)| \geq 2$, the above equality implies that $|N(v)| < |N(u)|$ and $|N(w)| < |N(u)|$. By the induction hypothesis, it now follows that both v and w can be factored into a product of irreducibles of R so that $u = vw$ can be factored into a product of irreducibles of R. This completes the proof of the first part of this problem.

Consider the element $6 \in R$ and note that

$$2 \cdot 3 = 6 = (4 + \sqrt{10})(4 - \sqrt{10})$$

By the previous problem, we know that $2, 3, 4+\sqrt{10}$, and $4-\sqrt{10}$ are irreducible elements of R. Hence, the above equality shows that the factorization of the element $6 \in R$ into irreducible elements of R need not be unique. $\square$

Homework 2: Page 148 #6, 10, 12, 14, 15, 16

Problem 6. *Let S be a multiplicative subset of an integral domain R such that $0 \notin S$. If R is a principal ideal domain, then so is $S^{-1}R$.*

Proof. Let R be a PID. We begin by noting that since R is an integral domain and $0 \notin S$ that $S^{-1}R$ is an integral domain.

Next, let J be an ideal of $S^{-1}R$. Since J is an ideal of $S^{-1}R$, we have that $J = S^{-1}I$ where $I = \phi_S^{-1}(J)$. Since the inverse homomorphic image of an ideal is an ideal, we have that I is an ideal of R. Since R is a PID, there is some $r \in R$ with $I = (r)$.

Now, fix any $s \in S$. We claim that $J = (rs/s)$. First, suppose that $a \in J = S^{-1}I$. Then $a = i/z$ for some $i \in I$ and $z \in S$. Since $i \in I = (r)$, there is some $b \in r$ so that $i = br$. As $b \in R$ and $z \in S$ we have $b/z \in S^{-1}R$ so that

$$a = \frac{i}{z} = \frac{br}{z} = \frac{br}{z} \cdot \frac{s}{s} = \frac{b}{z} \cdot \frac{rs}{s} \in \left(\frac{rs}{s}\right)$$

On the other hand, suppose that $a \in (rs/s)$. Then there is some $b/z \in S^{-1}R$ such that

$$a = \frac{b}{z} \cdot \frac{rs}{s}$$

Notice that $bsr \in (r) = I$ and that $zs \in S$ as $z, s \in S$ and S is a multiplicative set. Hence, we now have

$$a = \frac{b}{z} \cdot \frac{rs}{s} = \frac{bsr}{zs} \in S^{-1}I = J$$

We conclude that $J = (rs/s)$ so that J is principal. As J was an arbitrary ideal of $S^{-1}R$, this shows that $S^{-1}R$ is a PID. $\square$

Problem 10. *Let R be an integral domain and for each maximal ideal M (which is also prime, of course), consider R_M as a subring of the quotient field of R. Show that $\cap R_M = R$, where the intersection is taken over all maximal ideals M of R.*

Proof. First, suppose that $r/1 \in R$. Let M be a maximal ideal of R. Since M is a maximal ideal of R, we have that $M \neq R$. In particular, this implies that $1 \notin M$ since M is an ideal and thus $1 \in R - M$. Hence, we have $r/1 \in (R-M)^{-1}R = R_M$. Since M was an arbitrary maximal ideal of R, this shows that $r/1 \in \cap R_M$.

On the other hand, suppose that $r/s \in \cap R_M$. In particular, note that $r \in R$ and $s \in R - M$ for every maximal ideal M of R so that s is not in any maximal ideal of R. Now, suppose that $a \in R$ is a nonunit of R. Then the ideal (a) of R is a proper ideal of R and hence (a) is contained in some maximal ideal of R. In particular, this shows that if $a \in R$ is a nonunit of R then $a \in (a)$ is contained in some maximal ideal of R. The contrapositive of this statement gives that if $a \in R$ is not in any maximal ideal of R then a is a unit of R. Hence, since s is not in any maximal ideal of R we have that s is a unit of R so that $s^{-1} \in R$. Thus, since $r, s^{-1} \in R$, we obtain

$$\frac{r}{s} = r \cdot s^{-1} \in R$$

so that $r/s \in R$. This completes the proof. $\square$

Problem 12. *A commutative ring with identity is local if and only if for all $r, s \in R$, $r + s = 1$ implies r or s is a unit.*

Proof. Let R be a commutative ring with identity. For the first direction, assume that R is a local ring and let M be the unique maximal ideal of R. Suppose $r, s \in R$ and $r + s = 1$. For the sake of contradiction, assume that neither r nor s is a unit. Then the ideals (r) and (s) are proper ideals of R. Hence, there are maximal ideals M_1 and M_2 of R such that $(r) \subseteq M_1$ and $(s) \subseteq M_2$. But since M is the unique maximal ideal of R, it follows that $M_1 = M = M_2$ so that $(r) \subseteq M$ and $(s) \subseteq M$. This gives

$$r \in (r) \subseteq M \quad \text{and} \quad s \in (s) \subseteq M$$

Hence, we have $r, s \in M$. Since M is an ideal, we now have

$$1 = r + s \in M$$

so that $M = R$. However, this is a contradiction since M is a maximal ideal of R so that $M \neq R$. Thus, either r or s is a unit.

For the second direction, assume that for all $r, s \in R$, if $r + s = 1$ we have r or s is a unit. For the sake of contradiction, assume that R is not local. Then there exist distinct maximal ideals M_1 and M_2 of R. Now, note that $M_1 + M_2$ is an ideal of R since M_1 and M_2 are ideals of R. Furthermore, notice that

$$M_1 \subseteq M_1 + M_2 \subseteq R$$

Since M_1 is a maximal ideal of R, this inclusion implies that either $M_1 + M_2 = M_1$ or $M_1 + M_2 = R$. But since M_1 and M_2 are distinct ideals of R, we have $M_1 + M_2 \neq M_1$ so that $M_1 + M_2 = R$. Thus, since $1 \in R = M_1 + M_2$ there exists some $r \in M_1$ and some $s \in M_2$ such that $r + s = 1$. By hypothesis, then, either r or s is a unit. Without loss of generality, assume that r is a unit. Since $r \in M_1$ is a unit and M_1 is an ideal, this implies that $M_1 = R$. However, this contradicts the fact that $M_1 \neq R$ since M_1 is a maximal ideal of R. We conclude that R is local. $\square$

Problem 14. *If M is a maximal ideal in a commutative ring R with identity and n is a positive integer, then the ring R/M^n has a unique prime ideal and therefore is local.*

Proof. Let n be a positive integer. By a previous homework, we know that the prime ideals of R/M^n are of the form I/M^n, where I is a prime ideal of R with $M^n \subseteq I$. Now, let J be a prime ideal of R/M^n. Then by the previous observation, we may write $J = I/M^n$ for some prime ideal I of R with $M^n \subseteq I$.

We now prove that $M \subseteq I$. Towards this end, let $m \in M$. Since $m \in M$, we have

$$\underbrace{m \cdot m \cdots m}_{n \text{ times}} \in M^n \subseteq I$$

But since I is a prime ideal, the above observation implies that $m \in I$ so that $M \subseteq I$. Finally, observe that we now have

$$M \subseteq I \subseteq R$$

Since M is a maximal ideal of R, the above inclusion implies that $I = M$ or $I = R$. But since I is a prime ideal of R, we have that $I \neq R$ so that $I = M$. Thus, we have

$$J = I/M^n = M/M^n$$

Since J was an arbitrary prime ideal of R/M^n, we may now conclude that M/M^n is the unique prime ideal of R/M^n. In particular, since maximal ideals are prime ideals, this result gives that M/M^n is the unique maximal ideal of R/M^n so that R/M^n is a local ring. This completes the proof. $\square$

Problem 15. *In a commutative ring R with identity the following conditions are equivalent:*

(a): *R has a unique prime ideal.*

(b): *Every nonunit is nilpotent.*

(c): *R has a minimal prime ideal which contains all zero divisors. Also, all nonzero, nonunits of R are zero divisors.*

Proof. (a $\Rightarrow$ b): Suppose that R has a unique prime ideal P and let $a \in R$ be a nonunit. If $a = 0$, then we clearly have that a is nilpotent. Therefore, assume that $a \neq 0$. Since $a \in R$ is a nonunit, it follows that the ideal (a) is a proper ideal of R and hence (a) is contained in some maximal ideal of R. But since maximal ideals are prime ideals and since P is the unique prime ideal of R, it follows that P is the unique maximal ideal of R so that $(a) \subseteq P$. Hence, we have $a \in (a) \subseteq P$.

Define $S = \{a^n : n \in \{1, 2, \dots\}\}$ and note that S is a multiplicative set in R so that $S^{-1}R$ is a commutative ring with identity. Now, for the sake of contradiction, suppose that $S^{-1}R$ were not the zero ring. Then since $S^{-1}R$ is a commutative ring with identity and $S^{-1}R$ is not the zero ring, there is a maximal (hence prime) ideal Q of $S^{-1}R$. Since Q is an ideal of $S^{-1}R$, we know that $Q = S^{-1}\phi_S^{-1}(Q)$. But since the inverse homomorphic image of a prime ideal is a prime ideal and since P is the unique prime ideal of R, we have that $\phi_S^{-1}(Q) = P$ so that $Q = S^{-1}P$. In particular, since $a \in P$ and $a \in S$, we have that $a/a \in S^{-1}P = Q$ so that Q contains the multiplicative identity of $S^{-1}R$. Since Q is an ideal of $S^{-1}R$, this now implies that $Q = S^{-1}R$. But this contradicts the fact that $Q \neq S^{-1}R$ since Q is a prime ideal of $S^{-1}R$. Therefore, we see $S^{-1}R$ is the zero ring.

Finally, since $S^{-1}R$ is the zero ring with identity, it follows that the additive identity of $S^{-1}R$ is equal to the multiplicative identity of $S^{-1}R$ so that $a/a = 0/a$. Therefore, there is some $s \in S$ such that $s(a^2 - 0) = 0$ so that $sa^2 = 0$. But since $s \in S$ there is some $n \in \{1, 2, \dots\}$ such that $s = a^n$. Hence, we have that

$$0 = sa^2 = a^n \cdot a^2 = a^{n+2}$$

so that $a \in R$ is nilpotent.

(b $\Rightarrow$ c): Suppose that every nonunit in R is nilpotent. Let I denote the set of all zero divisors of R together with 0. We claim that I is a prime ideal of R. Towards this end, first note that $0 \in I$ so that $I \neq \emptyset$. Next, let $a, b \in I$. If $a - b = 0$, then clearly $a - b \in I$, so assume that $a - b \neq 0$. Note that any element of I is either a zero divisor or 0 so that every element of I is a nonunit of R. Thus, since $a, b \in I$ we have that a and b are nonunits of R. Hence, by hypothesis, it now follows that a and b are nilpotent. By a previous homework problem, we have that $a - b$ is nilpotent since a and b are nilpotent. Since $a - b \neq 0$ and $a - b$ is nilpotent, this implies that $a - b$ is a zero divisor so that $a - b \in I$. Thus, we see I is a subgroup of R under addition.

Next, let $r \in R$ and $a \in I$. We must show that $ra \in I$. If $ra = 0$, then $ra \in I$. Therefore, assume that $ra \neq 0$. Note that $a \neq 0$ or else $ra = 0$ and since $a \in I$, this implies that a is a zero divisor. Hence, there is some $c \in R$ with $c \neq 0$ such that $ca = 0$.

Multiplying both sides of this equality by r gives $c(ra) = 0$. Since $c \neq 0$, this equality implies that ra is a zero divisor of R and hence $ra \in I$. The above results show that I is an ideal of R.

To see that I is a prime ideal of R, suppose that $ab \in I$ for some $a, b \in R$. If $a = 0$ or $b = 0$, then $a \in I$ or $b \in I$. Therefore, assume that $a \neq 0$ and $b \neq 0$. Now, since $ab \in I$, we have that $ab = 0$ or ab is a zero divisor of R. First, suppose that $ab = 0$. Since $a \neq 0$ and $b \neq 0$, this equality implies that a is a zero divisor of R and hence $a \in I$. Secondly, suppose that ab is a zero divisor of R. Then there is some nonzero $c \in R$ such that $cab = 0$. First, suppose that $ca = 0$. Then since $c \neq 0$ this equality implies that a is a zero divisor of R and hence $a \in I$. If $ca \neq 0$, note that

$$(ca)b = cab = 0$$

so that b is a zero divisor of R and hence $b \in I$. The above results show that I is a prime ideal of R.

By the above results, we have that the set I of zero divisors of R together with 0 forms a prime ideal of R. Clearly, then, this implies that I is the minimal prime ideal of R which contains all zero divisors. Finally, suppose that $a \in R$ is a nonzero, nonunit. By hypothesis, this implies that a is nilpotent. Since a is a nonzero, nilpotent element of R, this implies that a is a zero divisor.

(c $\Rightarrow$ a): Let Q be the minimal prime ideal of R which contains all zero divisors and let P be a prime ideal of R. We will show that $P = Q$. Towards this end, let $a \in P$. If a is a unit of R, then $P = R$ which contradicts the fact that P is a prime ideal of R. Therefore, it must be the case that a is a nonunit of R. If $a = 0$, then clearly $a \in Q$. If $a \neq 0$, then a is a nonzero, nonunit of R so that by hypothesis we see a is a zero divisor so that $a \in Q$. On the other hand, we have $Q \subseteq P$ by the minimality of Q. The above results show that $P = Q$, which proves that R has a unique prime ideal. $\square$

Problem 16. *Every nonzero homomorphic image of a local ring is local.*

Proof. Let R be a local ring with unique maximal ideal M and suppose that $\phi : R \to S$ is a nonzero ring homomorphism. We must show that $\phi(R)$ is a local ring. First, note that by the First Isomorphism Theorem for Rings we have $\phi(R) \simeq R/\ker\phi$. Furthermore, since ϕ is a nonzero ring homomorphism, it follows that $\ker\phi \neq R$ so that $\ker\phi$ is a proper ideal of R. Therefore, we have that $\ker\phi$ is contained in some maximal ideal of R. But since M is the unique maximal ideal of R, this observation gives $\ker\phi \subseteq M$.

We show that $M/\ker\phi$ is the unique maximal ideal of $R/\ker\phi$. First, since M is an ideal of R containing $\ker\phi$, it follows that $M/\ker\phi$ is an ideal of $R/\ker\phi$. Furthermore, we see that $M \neq R$ as M is a maximal ideal of R, which implies that $M/\ker\phi \neq R/\ker\phi$. Now, suppose that $I/\ker\phi$ is an ideal of $R/\ker\phi$ with $I/\ker\phi \not\subseteq M/\ker\phi$. Then there is some $i + \ker\phi \in I/\ker\phi$ such that $i + \ker\phi \notin M/\ker\phi$. In particular, this implies that $i \in I$ but $i \notin M$. Now, since M is the unique maximal ideal of R, it follows that all of the nonunits of R are contained in M. But since $i \notin M$, this implies that i must be a unit of R. Finally, recall that there is a one-to-one correspondence between the set of ideals of $R/\ker\phi$ and the set of ideals of R that contain $\ker\phi$. In particular, since $I/\ker\phi$ is an ideal of $R/\ker\phi$, we have that I is an ideal of R. Thus, since $i \in I$ is a unit and I is an ideal of R, this implies that $I = R$ so that $I/\ker\phi = R/\ker\phi$.

The above results prove that $M/\ker\phi$ is the unique maximal ideal of $R/\ker\phi$ so that $R/\ker\phi$ is a local ring. Since $\phi(R) \simeq R/\ker\phi$, we conclude that $\phi(R)$ is a local ring, completing the proof. $\square$

Homework 3: Page 157 #10, 11; Page 165 #1

Problem 10. (a): *If F is a field then every nonzero element of $F[[x]]$ is of the form $x^k u$ with $u \in F[[x]]$ a unit.*

(b): *$F[[x]]$ is a principal ideal domain whose only ideals are $0, F[[x]] = (1) = (x^0)$, and (x^k) for each $k \geq 1$.*

Proof. (a): Let $\sum_{i=0}^{\infty} a_i x^i \in F[[x]]$ be a nonzero element of $F[[x]]$. If $a_0 \neq 0$, then $a_0 \in F$ is a unit of F since F is a field. Thus, in this case, we have that $\sum_{i=0}^{\infty} a_i x^i \in F[[x]]$ is a unit of $F[[x]]$. Now, let $u = \sum_{i=0}^{\infty} a_i x^i \in F[[x]]$. Then $u \in F[[x]]$ is a unit of $F[[x]]$ by the previous observation. Furthermore, we have

$$\sum_{i=0}^{\infty} a_i x^i = u = 1 \cdot u = x^0 u$$

which completes the proof in the case when $a_0 \neq 0$.

Now, suppose that $a_0 = 0$. Define $J = \{j \in \{1, 2, \dots, \} : a_j \neq 0\}$. Since $\sum_{i=0}^{\infty} a_i x^i$ is a nonzero element of $F[[x]]$ and $a_0 = 0$, it follows that $a_j \neq 0$ for some $j \in \{1, 2, \dots\}$. In particular, this shows that $J \neq \emptyset$. Thus, since J is a nonempty set of positive integers, it now follows that there exist some minimal element $k \in J$. In particular, by the definition of J, we have that $a_k \neq 0$ so that $a_k \in F$ is a unit since F is a field. Now, let $u = \sum_{i=k}^{\infty} a_i x^{i-k} \in F[[x]]$. Then $u \in F[[x]]$ is a unit of $F[[x]]$ since $a_k \in F$ is a unit of F. Furthermore, by the minimality of k, we have

$$\sum_{i=0}^{\infty} a_i x^i = \sum_{i=k}^{\infty} a_i x^i = x^k \cdot \sum_{i=k}^{\infty} a_i x^{i-k} = x^k u$$

which completes the proof in the case when $a_0 = 0$ and hence in all cases. □

Proof. (b): Since F is a field, it is immediate that $F[[x]]$ is an integral domain. Therefore, it remains to prove that every ideal of $F[[x]]$ is principal. Towards this end, let I be an ideal of $F[[x]]$. If $I = 0$, then I is clearly principal. If $I = F[[x]]$, then $I = (1) = (x^0)$ so that I is principal. Therefore, assume that I is a nonzero, proper ideal of $F[[x]]$.

Since I is a proper ideal of $F[[x]]$, it follows that I contains no units of $F[[x]]$. Thus, it follows by Part (a) of this problem that every nonzero element of $I \subseteq F[[x]]$ is of the form $x^m u$ for some integer $m \geq 1$ and some unit $u \in F[[x]]$. Let $k \geq 1$ be the smallest of these integers. We claim that $I = (x^k)$.

First, let $z \in I$. If $z = 0$ then clearly $z \in (x^k)$. Therefore, assume that z is a nonzero element of I. Then $z = x^m u$ for some unit $u \in F[[x]]$ and some positive integer m. By the minimality of k, we have that $k \leq m$ so that $m - k \geq 0$. Thus, we have

$$z = x^m u = x^k x^{m-k} u = (x^{m-k} u) x^k \in (x^k)$$

The above results show that $I \subseteq (x^k)$. On the other hand, note that there is some $z \in I$ such that $z = x^k u$ for some unit u of $F[[x]]$ by the definition of k. Since u is a unit, we may multiply both sides of this equality by u^{-1} to obtain

$$x^k = u^{-1} z \in I$$

since I is an ideal and $z \in I$. Thus, since $x^k \in I$ and I is an ideal we have $(x^k) \subseteq I$. The above results show that $I = (x^k)$ for some $k \geq 1$.

We have shown that every ideal of $F[[x]]$ is principal so that $F[[x]]$ is a PID. Furthermore, we have also shown that the only ideals of $F[[x]]$ are $0, F[[x]] = (1) = (x^0)$, and (x^k) for each $k \geq 1$. This completes the proof. $\square$

Problem 11. *Let $\mathcal{C}$ be the category with objects all commutative rings with identity and morphisms all ring homomorphisms $f : R \to S$ such that $f(1_R) = 1_S$. Then the polynomial ring $\mathbb{Z}[x_1, \ldots, x_n]$ is a free object on the set $\{x_1, \ldots, x_n\}$ in the category $\mathcal{C}$.*

Proof. Let $i : \{x_1, \ldots, x_n\} \to \mathbb{Z}[x_1, \ldots, x_n]$ be the inclusion map. Let R be an object of $\mathcal{C}$ so that R is a commutative ring with identity and let $f : \{x_1, \ldots, x_n\} \to R$ be any map. We must show that there exists a unique morphism $\overline{f} : \mathbb{Z}[x_1, \ldots, x_n] \to R$ of $\mathcal{C}$ such that $\overline{f} \circ i = f$. In other words, we must show that there exists a unique ring homomorphism $\overline{f} : \mathbb{Z}[x_1, \ldots, x_n] \to R$ such that $\overline{f}$ maps the multiplicative identity of $\mathbb{Z}[x_1, \ldots, x_n]$ to the multiplicative identity of R and $\overline{f} \circ i = f$.

Consider the map $g : \mathbb{Z} \to R$ by $g(n) = n \cdot 1$ for all $n \in \mathbb{Z}$. Clearly, we see that g is a ring homomorphism that maps the multiplicative identity of $\mathbb{Z}$ to the multiplicative identity of R. Furthermore, note that $f(x_1), \ldots, f(x_n) \in R$. Since both $\mathbb{Z}$ and R are commutative rings with identity, the previous two observations give the existence of a unique ring homomorphism $\overline{f} : \mathbb{Z}[x_1, \ldots, x_n] \to R$ such that $\overline{f}$ extends g and $\overline{f}(x_i) = f(x_i)$ for all $i \in \{1, \ldots, n\}$.

Now, notice that since $\overline{f}$ extends g that $\overline{f}$ maps the multiplicative identity of $\mathbb{Z}[x_1, \ldots, x_n]$ to the multiplicative identity of R since g maps the multiplicative identity of $\mathbb{Z}$ to the multiplicative identity of R and as the multiplicative identity of $\mathbb{Z}$ is the multiplicative identity of $\mathbb{Z}[x_1, \ldots, x_n]$. Next, let $z \in \{x_1, \ldots, x_n\}$. Then by the above we have that

$$(\overline{f} \circ i)(z) = \overline{f}(i(z)) = \overline{f}(z) = f(z)$$

Since $z \in \{x_1, \ldots, x_n\}$ was arbitrary, this shows that $\overline{f} \circ i = f$. Finally, that $\overline{f}$ is the unique morphism of $\mathcal{C}$ such that $\overline{f} \circ i = f$ follows from the fact that $\overline{f}$ is unique in the way described above. This completes the proof. $\square$

Problem 1. (a): *If D is an integral domain and c is an irreducible element in D, then $D[x]$ is not a principal ideal domain by considering the ideal (x, c).*

(b): *$\mathbb{Z}[x]$ is not a principal ideal domain.*

(c): *If F is a field and $n \geq 2$, then $F[x_1, \ldots, x_n]$ is not a principal ideal domain.*

Proof. (a): For the sake of contradiction, suppose that $D[x]$ were a PID. Let $c \in D$ be an irreducible element of D and consider the ideal (x, c) of $D[x]$. Since $D[x]$ is a PID, there exists some element $f(x) \in D[x]$ such that $(x, c) = (f(x))$. In particular, we have $c \in (x, c) = (f(x))$ and thus there is some polynomial $g(x) \in D[x]$ such that $c = f(x)g(x)$. Now, since D is an integral domain and since $c \neq 0$ since c is irreducible, we have that

$$0 = \deg(c) = \deg(f(x)g(x)) = \deg(f(x)) + \deg(g(x))$$

This implies that $\deg(f(x)) = 0 = \deg(g(x))$. In other words, we see that $f(x)$ and $g(x)$ are constant polynomials so that $f(x), g(x) \in D$. Thus, since $c = f(x)g(x)$ and as c is irreducible, this implies that either $f(x)$ or $g(x)$ is a unit in D.

If $f(x)$ is a unit in D, then $(x, c) = (f(x)) = D$. Hence, we have $1 \in D = (x, c)$ and thus there exist elements $r_1, r_2 \in D$ such that $1 = r_1 x + r_2 c$. Clearly, this equality implies that $r_1 = 0$ so that

$$1 = r_1 x + r_2 c = 0 + r_2 c = r_2 c$$

The above equality implies that c is a unit in D. But since c is irreducible in D, it cannot be the case that c is a unit in D.

By the above contradiction, we must have that $g(x)$ is a unit in D. Thus, since $c = f(x)g(x)$ and $g(x)$ is a unit in D it now follows that c and $f(x)$ are associates in D and hence generate the same ideal in D. Therefore, we have

$$x \in (x, c) = (f(x)) = (c)$$

so that $x = dc$ for some $d \in D$. However, since $c, d \in D$, this implies that $x = dc \in D$ which is clearly impossible. We conclude that $D[x]$ is not a PID. $\square$

Proof. (b): We can rephrase the result of Part (a) of this problem as follows. If D is an integral domain that contains at least one irreducible element, then $D[x]$ is not a principal ideal domain. Now, notice that $\mathbb{Z}$ is clearly an integral domain and that $2 \in \mathbb{Z}$ is an irreducible element of $\mathbb{Z}$. By the previously-mentioned result, we conclude that $\mathbb{Z}[x]$ is not a PID. $\square$

Proof. (c): Let $n \geq 2$. We first show that x_1 is irreducible in $F[x_1]$. Towards this end, first note that x_1 is clearly a nonzero, nonunit of $F[x_1]$. Now, suppose $x_1 = f(x_1)g(x_1)$ for some $f(x_1), g(x_1) \in F[x_1]$. Since F is a field, we have

$$1 = \deg(x_1) = \deg(f(x_1)g(x_1)) = \deg(f(x_1)) + \deg(g(x_1))$$

By the above equality, it follows that either $\deg(f(x_1)) = 0$ or $\deg(g(x_1)) = 0$. Without loss of generality, assume that $\deg(f(x_1)) = 0$. Then $f(x_1) \in F[x_1]$ is a constant polynomial so that $f(x_1) \in F$. Furthermore, note that since $0 \neq x_1 = f(x_1)g(x_1)$ we

have that $f(x_1) \neq 0$. Hence, since $f(x_1)$ is a nonzero element of the field F it follows that $f(x_1)$ is a unit in F and hence a unit in $F[x_1]$. In particular, this shows that x_1 is irreducible in $F[x_1]$ which clearly implies that x_1 is irreducible in $F[x_1, \ldots, x_{n-1}]$.

We now prove the main result. First, note that as F is a field that that $F[x_1, \ldots, x_{n-1}]$ is an integral domain. Furthermore, by the above result, we have that the element $x_1 \in F[x_1, \ldots, x_{n-1}]$ is an irreducible element of $F[x_1, \ldots, x_{n-1}]$. By Part (a) of this problem, then, we have

$$F[x_1, \ldots, x_{n-1}][x_n] = F[x_1, \ldots, x_n]$$

is not a principal ideal domain. This completes the proof. $\square$

Homework 4: Page 179 #11, 12, 15

Problem 11. (a): *If A is a module over a commutative ring R and $a \in A$, then $\mathcal{O}_a = \{r \in R : ra = 0\}$ is an ideal of R. If $\mathcal{O}_a \neq 0$, a is said to be a* ***torsion element*** *of A.*

(b): *If R is an integral domain, then the set $T(A)$ of all torsion elements of A is a submodule of A. ($T(A)$ is called the* ***torsion submodule****).*

(c): *Show that (b) may be false for a commutative ring R, which is not an integral domain.*

In (d)—(f) R is an integral domain.

(d): *If $f : A \to B$ is an R-module homomorphism, then $f(T(A)) \subseteq T(B)$; hence the restriction f_T of f to $T(A)$ is an R-module homomorphism $T(A) \to T(B)$.*

(e): *If*

$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C$$

is an exact sequence of R-modules, then so is

$$0 \longrightarrow T(A) \xrightarrow{f_T} T(B) \xrightarrow{g_T} T(C)$$

(f): *If $g : B \to C$ is an R-module epimorphism, then $g_T : T(B) \to T(C)$ need not be an epimorphism.*

Proof. (a): First, note that $0 \in \mathcal{O}_a$ so that $\mathcal{O}_a \neq \emptyset$. Now, let $r_1, r_2 \in \mathcal{O}_a$ so that we have $r_1 a = 0 = r_2 a$. This gives

$$0 = 0 - 0 = r_1 a - r_2 a = (r_1 - r_2)a$$

and since $r_1 - r_2 \in R$, the above equality shows that $r_1 - r_2 \in \mathcal{O}_a$. Finally, suppose that $s \in \mathcal{O}_a$ and let $r \in R$. Since $s \in \mathcal{O}_a$, it follows that $sa = 0$. Hence, multiplying both sides of this equality by r gives $0 = r(sa) = (rs)a$. Since $rs \in R$, this equality shows that $rs \in \mathcal{O}_a$. We conclude that $\mathcal{O}_a$ is an ideal of R. □

Proof. (b): For definiteness, note that we can write

$$T(A) = \{a \in A : ra = 0 \text{ for some nonzero } r \in R\}$$

Now, we prove the main result. First, note that $1 \neq 0$ since R is an integral domain. Since A is a module, we have $0 \in A$. Thus, since $1 \cdot 0 = 0$ this shows that $0 \in T(A)$ so that $T(A) \neq \emptyset$. Next, suppose that $a_1, a_2 \in T(A)$. Then there are nonzero elements $r_1, r_2 \in R$ such that $r_1 a_1 = 0 = r_2 a_2$. Since r_1 and r_2 are nonzero elements of the integral domain R, it follows that $r_1 r_2$ is also a nonzero element of R. Furthermore, we have

$$r_1 r_2 (a_1 - a_2) = (r_1 r_2)a_1 - (r_1 r_2)a_2 = r_2(r_1 a_1) - r_1(r_2 a_2) = r_2 \cdot 0 - r_2 \cdot 0 = 0 - 0 = 0$$

so that by the previous observation we obtain $a_1 - a_2 \in T(A)$. The above results show that $T(A)$ is a subgroup of A under addition.

Finally, let $r \in R$ and $a \in T(A)$. Since $a \in T(A)$, there is some nonzero $s \in R$ such that $sa = 0$. Thus, we obtain

$$s(ra) = r(sa) = r \cdot 0 = 0$$

Since $s \in R$ is nonzero, the above equality shows that $ra \in T(A)$. We conclude that $T(A)$ is a submodule of A. $\square$

Proof. (c): Let $R = \mathbb{Z}/6\mathbb{Z}$ and let $A = R$. Note that R is a commutative ring but is not an integral domain, since for the nonzero elements $\overline{2}$ and $\overline{3}$ in R we have $\overline{2} \cdot \overline{3} = \overline{0}$. Furthermore, as any ring is a module over itself, we have $A = R$ is a module over R.

We claim that $T(A)$ is not a submodule. Towards this end, once again consider the elements $\overline{2}$ and $\overline{3}$ of R. By the equality presented above, we see that $\overline{2}, \overline{3} \in T(A)$. However, note that $\overline{2} + \overline{3} = \overline{5} \notin T(A)$ since $a \cdot \overline{5} \neq \overline{0}$ for any nonzero element $a \in R$. This argument shows that $T(A)$ is not closed under addition and hence cannot be a subgroup of A under addition. In particular, this shows that $T(A)$ is not a submodule of A. $\square$

Proof. (d): Let $f : A \to B$ be an R-module homomorphism and let $a \in T(A)$. Then there is some nonzero $r \in R$ such that $ra = 0$. Since f is an R-module homomorphism, this gives that

$$0 = f(0) = f(ra) = rf(a)$$

Since $r \in R$ is nonzero and as $f(a) \in B$, the above equality shows that $f(a) \in T(B)$. Since $a \in T(A)$ was arbitrary, the above proof shows that $f(T(A)) \subseteq T(B)$. $\square$

Proof. (e): By the previous Parts of this problem, we know that $f_T : T(A) \to T(B)$ and $g_T : T(B) \to T(C)$ are R-module homomorphisms. Therefore, it remains to prove that $\mathrm{Im}(f_T) = \ker(g_T)$ and that $\ker(f_T)$ is trivial. By hypothesis, note that we have $\mathrm{Im}(f) = \ker(g)$ and that $\ker(f)$ is trivial. We will use these facts below.

First, let $b \in \mathrm{Im}(f_T)$. Then $b \in \mathrm{Im}(f_T) \subseteq \mathrm{Im}(f) = \ker(g)$ and $b \in \mathrm{Im}(f_T) \subseteq T(B)$. Hence, we have $b \in T(B)$ and since g is equal to g_T on $T(B)$, the above results give

$$g_T(b) = g(b) = 0$$

so that $b \in \ker(g_T)$.

On the other hand, let $b \in \ker(g_T)$. Then $b \in \ker(g_T) \subseteq \ker(g) = \mathrm{Im}(f)$ and $b \in \ker(g_T) \subseteq T(B)$. Since $b \in \mathrm{Im}(f)$, there is some $a \in A$ such that $f(a) = b$ and since $b \in T(B)$ there is some nonzero $r \in R$ such that $rb = 0$. We claim that $a \in T(A)$. Indeed, note that since $f(a) = b$ and since f is an R-module homomorphism we have

$$f(ra) = rf(a) = rb = 0$$

and thus $ra \in \ker(f)$. But since $\ker(f)$ is trivial, this shows that $ra = 0$ and since r is nonzero, we conclude that $a \in T(A)$. Hence, since f is equal to f_T on $T(A)$, the above results give

$$b = f(a) = f_T(a)$$

so that $b \in \mathrm{Im}(f_T)$. Combining the previous two results shows that $\mathrm{Im}(f_T) = \ker(g_T)$.

Finally, since $\ker(f_T) \subseteq \ker(f)$ and as $\ker(f)$ is trivial, this inclusion implies that $\ker(f_T)$ is trivial. This completes the proof. $\square$

Proof. (f): Let $B = \mathbb{Z}$ and let $C = \mathbb{Z}/5\mathbb{Z}$. Note that clearly B is a $\mathbb{Z}$-module and since C is an abelian group, it follows that C is a $\mathbb{Z}$-module. Furthermore, since $\mathbb{Z}$ is an integral domain, we have by Part (b) of this problem that $T(B)$ an $T(C)$ are indeed submodules of B and C, respectively.

Now, since $\mathbb{Z}$ has no zero divisors, it follows that $T(B) = \{0\}$. Next, notice that if $a + 5\mathbb{Z} \in \mathbb{Z}/5\mathbb{Z}$ then $5 \in \mathbb{Z}$ is a nonzero element of $\mathbb{Z}$ and

$$5(a + 5\mathbb{Z}) = 5a + 5\mathbb{Z} = 0 + 5\mathbb{Z}$$

which implies that $a+5\mathbb{Z} \in T(C)$. Since $a+5\mathbb{Z} \in \mathbb{Z}/5\mathbb{Z}$ was arbitrary, this result proves that $T(C) = \mathbb{Z}/5\mathbb{Z}$.

Finally, define

$$g : \mathbb{Z} \to \mathbb{Z}/5\mathbb{Z} \quad \text{by} \quad a \mapsto a + 5\mathbb{Z}$$

and note that g is clearly a surjective $\mathbb{Z}$-module homomorphism and hence $g : B \to C$ is a $\mathbb{Z}$-module epimorphism. On the other hand, notice that by Part (d) and the above we have $g_T : T(B) \to T(C)$ is the map $g_T : \{0\} \to \mathbb{Z}/5\mathbb{Z}$. Therefore, since

$$|\{0\}| = 1 < 5 = |\mathbb{Z}/5\mathbb{Z}|$$

it cannot be the case that the map $g_T : T(B) \to T(C)$ is a surjection. We conclude that $g_T : T(B) \to T(C)$ is not an epimorphism. This completes the proof. $\square$

Problem 12. *(The Five Lemma) Let*

$$\begin{tikzcd}
A_1 \arrow[r, "f"] \arrow[d, "\alpha_1"] & A_2 \arrow[r, "g"] \arrow[d, "\alpha_2"] & A_3 \arrow[r, "h"] \arrow[d, "\alpha_3"] & A_4 \arrow[r, "k"] \arrow[d, "\alpha_4"] & A_5 \arrow[d, "\alpha_5"] \\
B_1 \arrow[r, "f'"] & B_2 \arrow[r, "g'"] & B_3 \arrow[r, "h'"] & B_4 \arrow[r, "k'"] & B_5
\end{tikzcd}$$

be a commutative diagram of R-modules and R-module homomorphisms, with exact rows. Prove that:

(a): *α_1 is an epimorphism and α_2, α_4 monomorphisms imply that α_3 is a monomorphism.*

(b): *α_5 is a monomorphism and α_2, α_4 epimorphisms imply that α_3 is an epimorphism.*

Proof. (a): Since α_3 is an R-module homomorphism, it suffices to prove that $\ker(\alpha_3)$ is trivial to establish that α_3 is monomorphism. Towards this end, let $a_3 \in \ker(\alpha_3)$. Then $\alpha(a_3) = 0$ so that since the diagram commutes we have

$$\alpha_4(h(a_3)) = h'(\alpha_3(a_3)) = h'(0) = 0$$

and thus $h(a_3) \in \ker(\alpha_4)$. But since α_4 is a monomorphism, this implies that $h(a_3) = 0$ so that $a_3 \in \ker(h) = \mathrm{Im}(g)$ since the first row of the diagram is exact. Thus, there is some $a_2 \in A_2$ such that $g(a_2) = a_3$. Now, since the diagram commutes we have

$$g'(\alpha_2(a_2)) = \alpha_3(g(a_2)) = \alpha_3(a_3) = 0$$

Thus, we see $\alpha_2(a_2) \in \ker(g') = \mathrm{Im}(f')$ since the second row of the diagram is exact. Thus, there is some $b_1 \in B_1$ such that $f'(b_1) = \alpha_2(a_2)$. Now, since α_1 is surjective, there is some $a_1 \in A_1$ such that $\alpha_1(a_1) = b_1$. By the above result and since the diagram commutes, we obtain

$$\alpha_2(f(a_1)) = f'(\alpha_1(a_1)) = f'(b_1) = \alpha_2(a_2)$$

Since α_2 is an injection, the above equality implies that $f(a_1) = a_2$ so that $a_2 \in \mathrm{Im}(f) = \ker(g)$. Therefore, we have $a_3 = g(a_2) = 0$. We conclude that $\ker(\alpha_3)$ is trivial so that α_3 is a monomorphism. $\square$

Proof. (b): Let $b_3 \in B_3$. Then $h'(b_3) \in B_4$ and since α_4 is an epimorphism, this implies that there is some $a_4 \in A_4$ such that $\alpha_4(a_4) = h'(b_3)$. Furthermore, note that $h'(b_3) \in \mathrm{Im}(h') = \ker(k')$ since the second row of the diagram is exact. By the previous two results and since the diagram is commutative, we have

$$\alpha_5(k(a_4)) = k'(\alpha_4(a_4)) = k'(h'(b_3)) = 0$$

Since α_5 is injective, the above equality implies that $k(a_4) = 0$ so that $a_4 \in \ker(k) = \mathrm{Im}(h)$ since the first row of the diagram is exact. Thus, there is some $a_3 \in A_3$ such that $h(a_3) = a_4$. Hence, since the diagram commutes and by the above, we have

$$h'(\alpha_3(a_3)) = \alpha_4(h(a_3)) = \alpha_4(a_4) = h'(b_3)$$

Thus, since h' is an R-module homomorphism, the above equality gives

$$0 = h'(\alpha_3(a_3)) - h'(b_3) = h'(\alpha_3(a_3) - b_3)$$

so that $\alpha_3(a_3) - b_3 \in \ker(h') = \mathrm{Im}(g')$ since the second row of the diagram is exact. Thus, there is some $b_2 \in B_2$ such that $g'(b_2) = \alpha_3(a_3) - b_3$. Since α_2 is surjective, there is some $a_2 \in A_2$ such that $\alpha(a_2) = b_2$. Since the diagram commutes, this gives

$$\alpha_3(g(a_2)) = g'(\alpha_2(a_2)) = g'(b_2) = \alpha_3(a_3) - b_3$$

Thus, since α_3 is an R-module homomorphism, the above equality gives

$$\alpha_3(a_3 - g(a_2)) = \alpha_3(a_3) - \alpha_3(g(a_2)) = b_3$$

We conclude that α_3 is a surjection and hence an epimorphism. $\square$

Problem 15. *If $f : A \to B$ and $g : B \to A$ are R-module homomorphisms such that $g \circ f = 1_A$, then $B = \mathrm{Im}(f) \oplus \ker(g)$.*

Proof. We must show that $B = \mathrm{Im}(f) + \ker(g)$ and that $\mathrm{Im}(f) \cap \ker(g) = \{0\}$. First, let $b \in B$. We claim that $b - f(g(b)) \in \ker(g)$. Towards this end, note that since $g \circ f = 1_A$ we have since g is an R-module homomorphism that

$$\begin{aligned} g(b - f(g(b)) &= g(b) - g(f(g(b))) \\ &= g(b) - (g \circ f)(g(b)) \\ &= g(b) - 1_A(g(b)) \\ &= g(b) - g(b) \\ &= 0 \end{aligned}$$

so that $b - f(g(b)) \in \ker(g)$, as claimed. Now, note that clearly $f(g(b)) \in \mathrm{Im}(f)$ so that combining this observation with the previous result gives

$$b = f(g(b)) + (b - f(g(b)) \in \mathrm{Im}(f) + \ker(g)$$

The above result shows that $B = \mathrm{Im}(f) + \ker(g)$.

Finally, suppose that $b \in \mathrm{Im}(f) \cap \ker(g)$. Since $b \in \mathrm{Im}(f)$, there is some $a \in A$ such that $b = f(a)$. Since $b \in \ker(g)$, we have $g(b) = 0$. Thus, since $g \circ f = 1_A$ we now have

$$0 = g(b) = g(f(a)) = 1_A(a) = a$$

so that $a = 0$. Thus, as f is an R-module homomorphism, we have

$$b = f(a) = f(0) = 0$$

so that $b = 0$. This shows that $\mathrm{Im}(f) \cap \ker(g) = \{0\}$. Since $B = \mathrm{Im}(f) + \ker(g)$, we conclude that $B = \mathrm{Im}(f) \oplus \ker(g)$. $\square$

Homework 5: Page 189 #4, 7, 12, 13

Problem 4. *Let R be a principal ideal domain, A a unitary left R-module, and $p \in R$ a prime. Let $pA = \{pa : a \in A\}$ and $A[p] = \{a \in A : pa = 0\}$.*

(a): *$R/(p)$ is a field.*

(b): *pA and $A[p]$ are submodules of A.*

(c): *A/pA is a vector space over $R/(p)$, with $(r + (p))(a + pA) = ra + pA$.*

(d): *$A[p]$ is a vector space over $R/(p)$, with $(r + (p))a = ra$.*

Proof. (a): Since $p \in R$ is a prime, it follows that (p) is a nonzero prime ideal. Since a nonzero prime ideal in a PID is a maximal ideal and since R is a PID, it now follows that (p) is a maximal ideal of R. Hence, we conclude that $R/(p)$ is a field since (p) is a maximal ideal of R. □

Proof. (b): We first show that pA is a submodule of A. Towards this end, first note that $0 \in A$ as A is a module and $0 = p \cdot 0 \in pA$ so that $pA \neq \emptyset$. Next, let $x, y \in pA$. Then there are $a_1, a_2 \in A$ such that $x = pa_1$ and $y = pa_2$. Note that $a_1 - a_2 \in A$ since A is a module and that

$$x - y = pa_1 - pa_2 = p(a_1 - a_2) \in pA$$

so that pA is a subgroup of A under addition. Finally, let $r \in R$ and $x \in pA$. Then there is some $a \in A$ such that $x = pa$. Since A is a module, we have $ra \in A$ and hence

$$rx = r(pa) = p(ra) \in pA$$

which completes the proof that pA is a submodule of A.

Secondly, we show that $A[p]$ is a submodule of A. Towards this end, first note that $0 \in A$ since A is a module and $p \cdot 0 = 0$ so that $0 \in A[p]$ so that $A[p] \neq \emptyset$. Next, let $x, y \in A[p]$. Note that $x - y \in A$ since $x, y \in A$ and A is a module and that $px = 0 = py$ since $x, y \in A[p]$. Therefore, we see

$$0 = 0 - 0 = px - py = p(x - y)$$

so that $x - y \in A[p]$ so that $A[p]$ is a subgroup of A under addition. Finally, let $r \in R$ and $x \in A[p]$. Since A is a module and $x \in A$ we have $rx \in A$ and as $x \in A[p]$ we have $px = 0$ and hence

$$p(rx) = r(px) = r \cdot 0 = 0$$

so that $rx \in A[p]$. The above results show that $A[p]$ is a submodule of A. □

Proof. (c): We begin by noting that A/pA is an abelian group under addition. To see that the multiplication as defined above is well-defined, suppose that $a + pA, b + pA \in A/pA$ and $r + (p), s + (p) \in R/(p)$ with $a + pA = b + pA$ and $r + (p) = s + (p)$. By the first of these equalities, we have that $a - b \in pA$ and by the second of these equalities, we have that $r - s \in (p)$. Since $a - b \in pA$ and pA is a module, we have that $s(a - b) \in pA$. Since $r - s \in (p)$, there is some $k \in R$ such that $r - s = kp$. Hence, we have $ka \in A$ since A is a module so that

$$(r - s)a = (kp)a = p(ka) \in pA$$

Hence, since $s(a-b), (r-s)a \in pA$ and as pA is a module we obtain

$$ra - sb = ra - sa + sa - sb = (r-s)a + s(a-b) \in pA$$

so that

$$(r+(p))(a+pA) = ra + pA = sb + pA = (s+(p))(b+pA)$$

which shows that multiplication as defined above is indeed well-defined. That A/pA meets the remaining requirements to be a vector space over $R/(p)$ is easily verified. $\square$

Proof. (d): We begin by noting that $A[p]$ is an abelian group. To see that the multiplication as defined above is well-defined, suppose that $r+(p), s+(p) \in R/(p)$ with $r+(p) = s+(p)$ and let $a \in A[p]$. Since $r+(p) = s+(p)$, we have that $r-s \in (p)$ and since $a \in A[p]$, we have that $pa = 0$. Since $r-s \in (p)$, there is some $k \in R$ such that $r-s = kp$. Hence, we obtain

$$ra - sa = (r-s)a = (kp)a = k(pa) = k \cdot 0 = 0$$

so that

$$(r+(p))a = ra = sa = (s+(p))a$$

which shows that multiplication as defined above is indeed well-defined. That $A[p]$ meets the remaining requirements to be a vector space over $R/(p)$ is easily verified. $\square$

Problem 7. *If G is a nontrivial group that is not cyclic of order 2, then G has a nonidentity automorphism.*

Proof. Let G be a nontrivial group that is not cyclic of order 2. Recall $\mathrm{Inn}(G) \simeq G/Z(G)$. In particular, this observation implies that $\mathrm{Inn}(G)$ is nontrivial if $Z(G) \neq G$ and hence G has a nonidentity automorphism in this case. On the other hand, suppose that $Z(G) = G$. In this case, it follows that G is abelian. Now, consider the map

$$\phi : G \to G \quad \text{by} \quad g \mapsto -g$$

Since G is abelian, we have that

$$\phi(g+h) = -(g+h) = -h-g = (-h)+(-g) = (-g)+(-h) = \phi(g)+\phi(h)$$

so that ϕ is a group homomorphism. Next, suppose that $g \in \ker(g)$ so that we have $-g = \phi(g) = 0$ which implies that $g = 0$ so that $\ker(g)$ is trivial. Since g is a group homomorphism, then, it now follows that g is an injection. Finally, suppose $g \in G$. Then we have $-g \in G$ and

$$\phi(-g) = -(-g) = g$$

so that g is a surjection. The above results show that ϕ is an automorphism of G.

Next, note that the automorphism ϕ of G from above is a nontrivial automorphism of G unless $g = -g$ for every $g \in G$. In other words, the automorphism ϕ of G from above is a nontrivial automorphism of G unless every nonidentity element of G has order 2. Therefore, it remains to prove the result for the case when every nonidentity element of G has order 2.

Now, since G is an abelian group it follows that G is a $\mathbb{Z}$-module. Furthermore, note that $\mathbb{Z}$ is a PID and that the element $2 \in \mathbb{Z}$ is a prime element of $\mathbb{Z}$. Therefore, by Part (d) of this problem we see that

$$G[2] = \{g \in G : 2g = 0\}$$

is a vector space over $\mathbb{Z}/2\mathbb{Z}$. But since every nonidentity element of g has order 2, it follows by the definition of $G[2]$ that $G[2] = G$. Combining the previous observation with this result, we see that G is a vector space over $\mathbb{Z}/2\mathbb{Z}$.

Finally, note that as G is a vector space over $\mathbb{Z}/2\mathbb{Z}$ that by hypothesis we have

$$2 < |G| = |\mathbb{Z}/2\mathbb{Z}|^{\dim_{\mathbb{Z}/2\mathbb{Z}}(G)} = 2^{\dim_{\mathbb{Z}/2\mathbb{Z}}(G)}$$

which implies that $\dim_{\mathbb{Z}/2\mathbb{Z}}(G) \geq 2$. Therefore, if X is a basis for G over $\mathbb{Z}/2\mathbb{Z}$ then there exist distinct elements $g, h \in X$. Furthermore, as X is a basis for G over $\mathbb{Z}/2\mathbb{Z}$ it follows that every element of G is a finite sum of elements in X. These observations imply that we may define a map ψ first on X by

$$g \mapsto h \quad h \mapsto g \quad k \mapsto k \quad \text{if} \quad k \in X - \{g, h\}$$

and then extend ψ to a map $\psi : G \to G$ by defining $\sum_{i=1}^{n} g_i \mapsto \sum_{i=1}^{n} \psi(g_i)$ under ψ. By the definition of ψ, is readily verified that ψ is an automorphism of G and is hence a nonidentity automorphism of G since $\psi(g) = h \neq g$. This completes the proof. $\square$

Problem 12. *If F is a free module over a ring with identity such that F has a basis of finite cardinality $n \geq 1$ and another basis of cardinality $n+1$, then F has a basis of cardinality m for every $m \geq n$, where m is a positive integer.*

Proof. Let R be a ring with identity and let F be a free R-module with basis of finite cardinality $n \geq 1$ and another basis of cardinality $n+1$. For the sake of contradiction, suppose that the conclusion to this problem were false. Among all positive integers m with $m \geq n$, choose the smallest positive integer m such that F does not have a basis of cardinality m. By hypothesis, if $m \in \{n, n+1\}$ then F has a basis of cardinality m and hence we do not have a counterexample in this case. Thus, we must have $m \geq n+2$.

Now, since the free R-module F has bases of finite cardinalities n and $n+1$, we have that

$$\bigoplus_{i=1}^{n} R \simeq F \simeq \bigoplus_{i=1}^{n+1} R$$

so that

$$\bigoplus_{i=1}^{n} R \simeq \bigoplus_{i=1}^{n+1} R$$

Furthermore, by the minimality of m, we know that the free R-module F must have a basis of finite cardinality $m-1$ so that we also have

$$F \simeq \bigoplus_{i=1}^{m-1} R$$

Finally, note that since $m \geq n+2$ we have that $m-(n+1) \geq 1$. By this observation and since

$$\bigoplus_{i=1}^{n} R \simeq \bigoplus_{i=1}^{n+1} R$$

we obtain

$$F \simeq \bigoplus_{i=1}^{m-1} R = \bigoplus_{i=1}^{m-(n+1)} R \oplus \bigoplus_{i=1}^{n} R \simeq \bigoplus_{i=1}^{m-(n+1)} R \oplus \bigoplus_{i=1}^{n+1} R = \bigoplus_{i=1}^{m} R$$

so that

$$F \simeq \bigoplus_{i=1}^{m} R$$

which implies that F has a basis of cardinality m. However, this is a contradiction. We conclude that F has a basis of cardinality m for every $m \geq n$, completing the proof. $\square$

Problem 13. *Let K be a ring with identity and F a free K-module with an infinite denumerable basis $\{e_1, e_2, \dots\}$. Then $R = \mathrm{Hom}_K(F, F)$ is a ring by a previous exercise. If n is any positive integer, then the free left R-module R has a basis of n elements; that is, as an R-module, $R \simeq R \oplus \cdots \oplus R$ for any finite number of summands.*

Proof. Let n be a positive integer. Note that by the previous exercise mentioned in the problem we have that R is a ring with identity. We now prove the main result.

If $n = 1$, then since R has identity it follows that $\{1\} \subseteq R$ is a basis for R over R. Therefore, we see that R has a basis of n elements in this case so that $R \simeq R$.

If $n = 2$, consider the subset $\{f_1, f_2\} \subseteq R$ where f_1 and f_2 are defined as follows. For each positive integer m, define

$$f_1(e_{2m}) = e_m \qquad f_2(e_{2m-1}) = e_m$$

and f_1 and f_2 are equal to 0 for any other e_i for which f_1 and f_2 have not already been defined as above. Now, suppose that $g_1 f_1 + g_2 f_2 = 0$ for some $g_1, g_2 \in R$. Then evaluating both sides of this equality at each e_i shows that $g_1(e_i) = g_2(e_i) = 0$ for each $i \in \{1, 2, \dots\}$ so that $g_1 = g_2 = 0$. In particular, this shows that $\{f_1, f_2\}$ is linearly independent over R. Finally, suppose that $g \in R$. Define $g_1, g_2 \in R$ by for each positive integer m

$$g_1(e_m) = g(e_{2m}) \quad g_2(e_m) = g(e_{2m-1})$$

Let m be a positive integer. Then

$$\begin{aligned}(g_1 f_1 + g_2 f_2)(e_{2m}) &= g_1 f_1(e_{2m}) + g_2 f_2(e_{2m}) \\ &= g_1(e_m) + g_2(0) \\ &= g(e_{2m}) + 0 \\ &= g(e_{2m})\end{aligned}$$

and

$$\begin{aligned}(g_1 f_1 + g_2 f_2)(e_{2m-1}) &= g_1 f_1(e_{2m-1}) + g_2 f_2(e_{2m-1}) \\ &= g_1(0) + g_2(e_m) \\ &= 0 + g(e_{2m-1}) \\ &= g(e_{2m-1})\end{aligned}$$

which shows that $g = g_1 f_1 + g_2 f_2$. Since $g \in R$ was arbitrary, the above results prove that $\{f_1, f_2\}$ spans R. We conclude that $\{f_1, f_2\}$ is a basis for R over R. Therefore, we see that R has a basis of n elements in this case so that $R \simeq R \oplus R$.

If $n = 3$, consider the subset $\{f_1, f_2, f_3\} \subseteq R$ where f_1, f_2, and f_3 are defined as follows. For each positive integer m, define

$$f_1(e_{3m}) = e_m \quad f_2(e_{3m-1}) = e_m \quad f_3(e_{3m-2}) = e_m$$

and f_1, f_2, and f_3 are equal to 0 for any other e_i for which f_1, f_2, and f_3 have not already been defined as above. Now, suppose that $g_1 f_1 + g_2 f_2 + g_3 f_3 = 0$ for some $g_1, g_2, g_3 \in R$. Then evaluating both sides of this equality at each e_i shows that $g_1(e_i) = g_2(e_i) = g_3(e_i) = 0$ for each $i \in \{1, 2, \dots\}$ so that $g_1 = g_2 = g_3 = 0$. In particular, this shows

that $\{f_1, f_2, f_3\}$ is linearly independent over R. Finally, suppose that $g \in R$. Define $g_1, g_2, g_3 \in R$ by for each positive integer m

$$g_1(e_m) = g(e_{3m}) \quad g_2(e_m) = g(e_{3m-1}) \quad g_3(e_m) = g(e_{3m-2})$$

Let m be a positive integer. Then

$$\begin{aligned}(g_1f_1 + g_2f_2 + g_3f_3)(e_{3m}) &= g_1f_1(e_{3m}) + g_2f_2(e_{3m}) + g_3f_3(e_{3m}) \\ &= g_1(e_m) + g_2(0) + g_3(0) \\ &= g(e_{3m}) + 0 + 0 \\ &= g(e_{3m})\end{aligned}$$

and

$$\begin{aligned}(g_1f_1 + g_2f_2 + g_3f_3)(e_{3m-1}) &= g_1f_1(e_{3m-1}) + g_2f_2(e_{3m-1}) + g_3f_3(e_{3m-1}) \\ &= g_1(0) + g_2(e_m) + g_3(0) \\ &= 0 + g(e_{3m-1}) + 0 \\ &= g(e_{3m-1})\end{aligned}$$

and

$$\begin{aligned}(g_1f_1 + g_2f_2 + g_3f_3)(e_{3m-2}) &= g_1f_1(e_{3m-2}) + g_2f_2(e_{3m-2}) + g_3f_3(e_{3m-2}) \\ &= g_1(0) + g_2(0) + g_3(e_m) \\ &= 0 + 0 + g(e_{3m-2}) \\ &= g(e_{3m-2})\end{aligned}$$

which shows that $g = g_1f_1 + g_2f_2 + g_3f_3$. Since $g \in R$ was arbitrary, the above results prove that $\{f_1, f_2, f_3\}$ spans R. We conclude that $\{f_1, f_2, f_3\}$ is a basis for R over R. Therefore, we see that R has a basis of n elements in this case so that $R \simeq R \oplus R \oplus R$.

If $n \geq 4$, we can define a subset $\{f_1, \ldots, f_n\} \subseteq R$ analogously as above and conclude that $\{f_1, \ldots, f_n\}$ is a basis for R over R. Therefore, we see that R has a basis with n elements in this case so that

$$R \simeq \underbrace{R \oplus \cdots \oplus R}_{n \text{ times}}$$

This completes the proof. $\square$

Homework 6: Page 198 #2, 3, 5

Problem 2. *Let R be a ring with identity. An R-module A is injective if and only if for every left ideal L of R and R-module homomorphism $g : L \to A$, there exists $a \in A$ such that $g(r) = ra$ for every $r \in L$.*

Proof. For the first direction, suppose that A is an injective R-module. Let L be a left ideal of R and let $g : L \to A$ be an R-module homomorphism. Let $i : L \to R$ denote the inclusion map. Then since i is clearly an injective R-module homomorphism, we have the following diagram of R-modules and R-module homomorphisms

$$\begin{tikzcd} 0 \arrow[r] & L \arrow[r, "i"] \arrow[d, "g"] & R \\ & A & \end{tikzcd}$$

with exact row. Since A is an injective R-module, then, there exists an R-module homomorphism $h : R \to A$ such that $h \circ i = g$. Finally, note that since R has 1 we may define $a = h(1) \in A$.

To complete the proof, let $r \in L$. Then we have since $h \circ i = g$ and since h is an R-module homomorphism that

$$g(r) = h(i(r)) = h(r) = h(r \cdot 1) = rh(1) = ra$$

Since $r \in L$ was arbitrary, this completes the proof of the first direction.

We now prove the second direction. Towards this end, let A be an R-module. Recall that A is injective if and only if for any left ideal L of R any R-module homomorphism $g : L \to A$ can be extended to an R-module homomorphism $R \to A$. In order to prove A is injective, then, we will use this equivalence. Accordingly, let L be any left ideal of R and suppose that $g : L \to A$ is an R-module homomorphism. By hypothesis, there exists an element $a \in A$ such that $g(r) = ra$ for every $r \in L$.

Finally, define $\psi : R \to A$ by $\psi(r) = ra$ for each $r \in R$. Since A is an R-module and $a \in A$, it follows that $ra \in A$ for each $r \in R$ so that ψ is a well-defined map. Next, we show that ψ is an R-module homomorphism. Towards this end, let $s, r_1, r_2 \in R$. Then $sr_1 + r_2 \in R$ since R is a ring. Thus, by the definition of ψ we obtain

$$\psi(sr_1 + r_2) = (sr_1 + r_2)a = sr_1a + r_2a = s\psi(r_1) + \psi(r_2)$$

so that ψ is an R-module homomorphism. Furthermore, if $r \in L$ then by the definition of R and by the above we have $\psi(r) = ra = g(r)$. In particular, this shows that the R-module homomorphism $\psi : R \to A$ extends g. We conclude that A is injective, completing the proof of the second direction. $\square$

Problem 3. *Every vector space over a division ring D is both a projective and an injective D-module.*

Proof. Let D be a division ring and suppose that J is a vector space over D. We first show that J is a projective D-module. Indeed, note that as J is a vector space over D that J is a free D-module. Since D is a division ring, we clearly have that D has 1 so that any free D-module is a projective D-module. Since J is a free D-module, then, we conclude that J is a projective D-module.

Secondly, we show that J is an injective D-module. Recall that J is injective if and only if for any left ideal L of D any D-module homomorphism $g : L \to J$ can be extended to a D-module homomorphism $D \to J$. In order to prove J is injective, then, we will use this equivalence. Accordingly, let L be any left ideal of D and suppose that $g : L \to J$ is an R-module homomorphism. Note that as D is a division ring and since L is a left ideal of D, it follows that $L \in \{\{0\}, D\}$.

If $L = \{0\}$, then the D-module homomorphism $g : L \to J$ is really the D-module homomorphism $g : \{0\} \to J$. Since g is a D-module homomorphism, we know that $g(0) = 0$. Now, define $h : D \to J$ by $h(d) = 0$ for all $d \in D$. Then we clearly have that h is a D-module homomorphism and $h(0) = 0 = g(0)$ so that h extends g. In this case, then, we conclude that J is an injective D-module.

Finally, if $L = D$ then the D-module homomorphism $g : L \to J$ is really the D-module homomorphism $g : D \to J$. In this case, since the D-module homomorphism g is already defined on all of D, we conclude that J is an injective D-module. This completes the proof. $\square$

Problem 5. *$\mathbb{Q}$ is not a projective $\mathbb{Z}$-module.*

Proof. For the sake of contradiction, suppose that $\mathbb{Q}$ were a projective $\mathbb{Z}$-module. Then there is a free $\mathbb{Z}$-module F and a $\mathbb{Z}$-module K such that $F \simeq K \oplus \mathbb{Q}$. Let $i : \mathbb{Q} \to F$ denote the canonical inclusion map. In particular, we know that i is a $\mathbb{Z}$-module homomorphism. Furthermore, we clearly have that $\ker(i)$ is trivial which implies that for the nonzero element $1 \in \mathbb{Q}$ we have $i(1) \neq 0$.

Now, since F is a free $\mathbb{Z}$-module there is a nonempty basis X for F over $\mathbb{Z}$. Since $i(1) \in F$ and as $i(1) \neq 0$, then, it follows for some positive integer n we can write

$$i(1) = \sum_{i=1}^{n} a_i e_i$$

for some unique elements $a_1, \ldots, a_n \in \mathbb{Z}$ and for some unique elements $e_1, \ldots, e_n \in X$. Define $N = 1 + \max_{i \in \{1,\ldots,n\}} |a_i|$ and note that $N \in \mathbb{Z}$. Furthermore, it is clear by the definition of N that $N \neq 0$. We will use this fact below.

Recall that $i : \mathbb{Q} \to F$ is a $\mathbb{Z}$-module homomorphism. Therefore, since $N \in \mathbb{Z}$ and since $N \neq 0$ we have by the above that

$$\sum_{i=1}^{n} a_i e_i = i(1) = i\left(\frac{N}{N}\right) = i\left(N \cdot \frac{1}{N}\right) = Ni\left(\frac{1}{N}\right)$$

Since $N \neq 0$, we may divide both sides of the above equality by N to obtain

$$\frac{1}{N} \sum_{i=1}^{n} a_i e_i = i\left(\frac{1}{N}\right)$$

But since i maps $\mathbb{Q}$ into F, we now have

$$\sum_{i=1}^{n} \frac{a_i}{N} e_i = \frac{1}{N} \sum_{i=1}^{n} a_i e_i = i\left(\frac{1}{N}\right) \in F$$

Therefore, as F is a free $\mathbb{Z}$-module the above result shows that $a_i/N \in \mathbb{Z}$ for each $i \in \{1, \ldots, n\}$. In other words, we conclude that N divides $a_1, \ldots, a_n$.

Finally, recall that $N = 1 + \max_{i \in \{1,\ldots,n\}} |a_i|$ so that $N > |a_i|$ for each $i \in \{1, \ldots, n\}$. But since N divides $a_1, \ldots, a_n$, this observation implies that $a_1 = \cdots = a_n = 0$ so that

$$i(1) = \sum_{i=1}^{n} a_i e_i = \sum_{i=1}^{n} 0 \cdot e_i = 0$$

which gives $i(1) = 0$. However, this is a contradiction to our previous observation that $i(1) \neq 0$. This completes the proof. $\square$

Homework 7: Page 198 #7, 8, 9

Problem 7. *Without using Lemma 3.9 prove that:*

(a): *Every homomorphic image of a divisible abelian group is divisible.*

(b): *Every direct summand of a divisible abelian group is divisible.*

(c): *A direct sum of divisible abelian groups is divisible.*

Proof. (a): Let A be a divisible abelian group and let $\phi : A \to B$ be a group homomorphism. First, note that since the homomorphic image of a group is a group and since A is abelian it is immediate that $\phi(A)$ is an abelian group. Next, let $y \in \phi(A)$ and let $n \in \mathbb{Z}$ be nonzero. Since $y \in \phi(A)$, there is some $x \in A$ such that $\phi(x) = y$. Furthermore, since $x \in A$ and as A is divisible it follows that there is some $z \in A$ such that $x = nz$. Finally, note that since ϕ is a group homomorphism we have

$$y = \phi(x) = \phi(nz) = \phi(\underbrace{z + \cdots + z}_{n \text{ times}}) = \underbrace{\phi(z) + \cdots + \phi(z)}_{n \text{ times}} = n\phi(z)$$

so that $y = n\phi(z)$. But since $z \in A$, it follows that $\phi(z) \in \phi(A)$. By the previous equality, then, we conclude that $\phi(A)$ is divisible. This completes the proof. $\square$

Proof. (b): Let A be a divisible abelian group and let B be a direct summand of A. Since B is a direct summand of the abelian group A, it follows that B is an abelian group. Now, let $\pi : A \to B$ denote the canonical projection map. Then we know that π is a surjective group homomorphism. Furthermore, since A is divisible we know by Part (a) of this problem that the homomorphic image $\pi(A)$ is divisible. But since π is surjective, we have that $\pi(A) = B$ and hence we conclude that B is divisible. $\square$

Proof. (c): Let $(A_i)_{i \in I}$ be any collection of divisible abelian groups. Since the direct sum of any number of abelian groups is an abelian group, we have that $\bigoplus_{i \in I} A_i$ is an abelian group. Next, let $(y_i)_{i \in I} \in \bigoplus_{i \in I} A_i$ and let $n \in \mathbb{Z}$ be nonzero. Since $y_i \in A_i$ and since A_i is divisible, it follows that there exists some element $x_i \in A_i$ such that $y_i = nx_i$ for each $i \in I$. Finally, notice that $(x_i)_{i \in I} \in \bigoplus_{i \in I} A_i$ and that

$$(y_i)_{i \in I} = (nx_i)_{i \in I} = n(x_i)_{i \in I}$$

so that $(y_i)_{i \in I} = n(x_i)_{i \in I}$. We conclude that $\bigoplus_{i \in I} A_i$ is divisible. $\square$

Problem 8. *Every torsion-free divisible abelian group D is a direct sum of copies of the rationals $\mathbb{Q}$.*

Proof. First, let $y \in D$ and let $n \in \mathbb{Z}$ be nonzero. Since D is divisible, it follows that there is some $x \in D$ such that $y = nx$. We claim that this $x \in D$ is unique. Indeed, suppose that $x' \in D$ is such that $y = nx'$ so that $nx = y = nx'$. Hence, we have

$$0 = nx - nx' = n(x - x')$$

Now, note that $x - x' \in D$ since $x, x' \in D$ and D is a group. Therefore, since $n(x - x') = 0$, since $n \in \mathbb{Z}$ is nonzero, and since D is torsion-free we conclude that $x - x' = 0$ so that $x = x'$. This completes the proof of our claim that $x \in D$ is the unique element of D such that $y = nx$. In particular, this result shows that for any $y \in D$ and any nonzero $n \in \mathbb{Z}$ there exists a unique element $x \in D$ such that $y = nx$. By uniqueness, then, this element $x \in D$ can be written $x = \left(\frac{1}{n}\right) y$.

We now define an action of $\mathbb{Q}$ on D as follows. Let $y \in D$ and $\frac{m}{n} \in \mathbb{Q}$ and define $\frac{m}{n} y = m \left(\frac{1}{n}\right) y$. By the previous result, this definition does indeed define an action of $\mathbb{Q}$ on D. We claim that this definition makes D into a vector space over $\mathbb{Q}$. Towards this end, first note that by hypothesis D is an abelian group and that we have an action of $\mathbb{Q}$ on D as defined above. Therefore, it remains to prove that this action of $\mathbb{Q}$ on D satisfies the vector space axioms. We will prove the first of these axioms and remark that the remaining vector space axioms are similarly-proven.

Towards this end, let $\frac{m}{n} \in \mathbb{Q}$ and $y_1, y_2 \in D$. Then we have

$$\begin{aligned}
\frac{m}{n}(y_1 + y_2) &= m \left[\left(\frac{1}{n} \right) (y_1 + y_2) \right] \\
&= m \left[\left(\frac{1}{n} \right) y_1 + \left(\frac{1}{n} \right) y_2 \right] \\
&= m \left(\frac{1}{n} \right) y_1 + m \left(\frac{1}{n} \right) y_2 \\
&= \frac{m}{n} y_1 + \frac{m}{n} y_2
\end{aligned}$$

As has been previously-stated, the remaining vector space axioms are proven similarly to the one proven above. We conclude that D is a vector space over $\mathbb{Q}$.

To complete the proof, recall that any vector space over a division ring is free over that ring. In our case in this problem, we have shown that D is a vector space over the division ring $\mathbb{Q}$ and hence D is a free $\mathbb{Q}$-module by the previous observation. Thus, it follows that D is isomorphic to a direct sum of copies of $\mathbb{Q}$. This completes the proof. $\square$

Problem 9. (a): *If D is an abelian group with torsion subgroup D_t, then D/D_t is torsion-free.*

(b): *If D is divisible, then so is D_t, whence $D = D_t \oplus E$, with E torsion-free.*

Proof. (a): We must show that the torsion subgroup of D/D_t is trivial to establish that D/D_t is torsion-free. Towards this end, suppose that $gD_t \in D/D_t$ is in the torsion subgroup of D/D_t. Then there exists a nonzero element $n \in \mathbb{Z}$ such that $(gD_t)^n = D_t$. That is, we have

$$D_t = (gD_t)^n = g^n D_t$$

so that $g^n \in D_t$. Thus, there exists a nonzero element $m \in \mathbb{Z}$ such that $(g^n)^m = 0$. That is, we have

$$0 = (g^n)^m = g^{nm}$$

Finally, note that since both n and m are nonzero elements of $\mathbb{Z}$ that nm is a nonzero element of $\mathbb{Z}$. Therefore, by the above equality we have that $g \in D_t$. We conclude that $gD_t = D_t$ since $g \in D_t$. Since gD_t in the torsion subgroup of D/D_t was arbitrary, we conclude that the torsion subgroup of D/D_t is trivial which shows that D/D_t is torsion-free, completing the proof. $\square$

Proof. (b): First, note that since any subgroup of an abelian group is abelian, we have that the subgroup D_t of the abelian group D is also abelian. Now, let $y \in D_t$ and $n \in \mathbb{Z}$ be nonzero. Since $y \in D_t$, there is some nonzero integer $m \in \mathbb{Z}$ such that $my = 0$. Furthermore, since $y \in D_t \subseteq D$ and as D is divisible there is some $x \in D$ such that $y = nx$. We claim that $x \in D_t$. Indeed, since $my = 0$ and as $y = nx$ we have that

$$0 = my = mnx$$

Finally, note that since both n and m are nonzero elements of $\mathbb{Z}$ that mn is a nonzero element of $\mathbb{Z}$. Therefore, by the above equality we have that $x \in D_t$. Since $y = nx$ and $x \in D_t$, this shows that D_t is divisible.

To prove the second statement, let $i : D_t \to D$ denote the inclusion map and $\pi : D \to D/D_t$ denote the canonical projection map. Clearly, we have that i is an injective $\mathbb{Z}$-module homomorphism and π is a surjective $\mathbb{Z}$-module homomorphism. Therefore, we have that

$$0 \longrightarrow D_t \xrightarrow{\ i\ } D \xrightarrow{\ \pi\ } D/D_t \longrightarrow 0$$

is a short exact sequence of $\mathbb{Z}$-modules and $\mathbb{Z}$-module homomorphisms.

Now, let $1_{D_t} : D_t \to D_t$ be the identity map so that 1_{D_t} is a $\mathbb{Z}$-module homomorphism. Thus, the following is a diagram of $\mathbb{Z}$-modules and $\mathbb{Z}$-module homomorphisms

$$\begin{tikzcd} 0 \arrow[r] & D_t \arrow[r, "i"] \arrow[d, "1_{D_t}"] & D \\ & D_t & \end{tikzcd}$$

with exact row. Now, note that by the proof of the first statement in Part (b) we have that D_t is a divisible abelian group and hence D_t is an injective $\mathbb{Z}$-module. Therefore,

there is a $\mathbb{Z}$-module homomorphism $\phi : D \to D_t$ such that $\phi \circ i = 1_{D_t}$. Hence, the short exact sequence above splits so that $D \simeq D_t \oplus D/D_t$.

To complete the proof, let $E = D/D_t$. Then by Part (a) of this problem, we have that E is torsion-free. By the previous result, then, we have that $D \simeq D_t \oplus E$, where E is torsion-free. This completes the proof. $\square$

Homework 8: Page 198 #4, 10, 11

Problem 4. (a): *For each prime p, $\mathbb{Z}(p^\infty)$ is a divisible group.*

(b): *No nonzero finite abelian group is divisible.*

(c): *No nonzero free abelian group is divisible.*

(d): *$\mathbb{Q}$ is a divisible abelian group.*

Proof. (a): We first show that $\mathbb{Z}(p^\infty)$ is q-divisible for each prime number $q \in \mathbb{Z}$ distinct from p. Towards this end, let $q \in \mathbb{Z}$ be a prime number distinct from p and let

$$y = \frac{a}{p^k} + \mathbb{Z} \in \mathbb{Z}(p^\infty)$$

Since p and q are distinct primes, it follows that $(p^k, q) = 1$ and hence there exist elements $z_1, z_2 \in \mathbb{Z}$ such that $z_1 p^k + z_2 q = 1$. Multiplying both sides of this equality by a gives $az_1 p^k + az_2 q = a$ so that $az_2 q = a - az_1 p^k$. Now, define

$$x = \frac{az_2}{p^k} + \mathbb{Z} \in \mathbb{Z}(p^\infty)$$

and note that by the above equality we have

$$q\left(\frac{az_2}{p^k}\right) = \frac{az_2 q}{p^k} = \frac{a - az_1 p^k}{p^k} = \frac{a}{p^k} - \frac{az_1 p^k}{p^k} = \frac{a}{p^k} - az_1$$

Therefore, since we clearly have $az_1 \in \mathbb{Z}$ the above equality gives

$$qx = q\left(\frac{az_2}{p^k} + \mathbb{Z}\right) = q\left(\frac{az_2}{p^k}\right) + \mathbb{Z} = \frac{a}{p^k} - az_1 + \mathbb{Z} = \frac{a}{p^k} + \mathbb{Z} = y$$

and thus $y = qx$. The above results that $\mathbb{Z}(p^\infty)$ is q-divisible for each prime number $q \in \mathbb{Z}$ distinct from p.

Next, we show that $\mathbb{Z}(p^\infty)$ is p-divisible. Towards this end, let

$$y = \frac{a}{p^k} + \mathbb{Z} \in \mathbb{Z}(p^\infty)$$

and define

$$x = \frac{a}{p^{k+1}} + \mathbb{Z} \in \mathbb{Z}(p^\infty)$$

Then we have

$$px = p\left(\frac{a}{p^{k+1}} + \mathbb{Z}\right) = p\left(\frac{a}{p^{k+1}}\right) + \mathbb{Z} = \frac{pa}{p^{k+1}} + \mathbb{Z} = \frac{a}{p^k} + \mathbb{Z} = y$$

and thus $y = px$. The above results show that $\mathbb{Z}(p^\infty)$ is p-divisible.

Combining the previous results, we may now assert that $\mathbb{Z}(p^\infty)$ is r-divisible for each prime number $r \in \mathbb{Z}$ which implies that $\mathbb{Z}(p^\infty)$ is r^k-divisible for each prime number r and each nonnegative integer k. Finally, since any nonzero element $n \in \mathbb{Z}$ can be written as a product of powers of prime numbers and since $\mathbb{Z}(p^\infty)$ is r^k-divisible for each prime number r and each nonnegative integer k it now follows that $\mathbb{Z}(p^\infty)$ is divisible. This completes the proof. $\square$

Proof. (b): Let A be a nonzero finite abelian group. For the sake of contradiction, suppose that A were divisible. Since A is nonzero, there exists some element $a \in A - \{0\}$. Furthermore, since A is finite we have that $|A| \in \mathbb{Z}$ is a nonzero element of $\mathbb{Z}$. Therefore, since A is divisible there is some element $b \in A$ such that $a = |A|b$. Now, since $b \in A$ it follows that $|b|$ divides $|A|$ and hence $|A|b = 0$. But then

$$a = |A|b = 0$$

which contradicts the fact that $a \in A - \{0\}$. We conclude that A is not divisible. $\square$

Proof. (c): Let A be a nonzero free abelian group. For the sake of contradiction, suppose that A were divisible. Since A is a nontrivial free abelian group, it follows that A can be written $A = \bigoplus_{i \in I} \mathbb{Z}$, where I is some nonempty index set. Now, since A is divisible it must be the case that each direct summand in the above direct sum is divisible. But since I is nonempty, this implies that $\mathbb{Z}$ is a divisible group which is clearly a contradiction. We conclude that A is not divisible. $\square$

Proof. (d): Let $y \in \mathbb{Q}$ and let $n \in \mathbb{Z}$ be nonzero. Since $y \in \mathbb{Q}$ we can write $y = \frac{a}{b}$ for some $a, b \in \mathbb{Z}$ with $b \neq 0$. Now, notice that $nb \neq 0$ since n and b are nonzero elements of $\mathbb{Z}$. Therefore, if we define $x = \frac{a}{nb}$ we have that $x \in \mathbb{Q}$. Furthermore, note that

$$y = \frac{a}{b} = n \cdot \frac{a}{nb} = nx$$

so that $y = nx$. Thus, since $y \in \mathbb{Q}$ was arbitrary we conclude that $\mathbb{Q}$ is divisible. $\square$

Problem 10. *Let p be a prime and D a divisible abelian p-group. Then D is a direct sum of copies of $\mathbb{Z}(p^\infty)$.*

Proof. If D is trivial, then we are done. Therefore, assume that D is a nontrivial divisible abelian p-group. We first show that D has a subgroup isomorphic to $\mathbb{Z}(p^\infty)$. Towards this end, first note that since p clearly divides $|D|$ we have by Cauchy's Theorem that there exist an element $x_1 \in D$ of order p. Since D is divisible and since $p \in \mathbb{Z}$ is nonzero, there exists an element $x_2 \in D$ such that $x_1 = px_2$. Similarly, since D is divisble and since $p \in \mathbb{Z}$ is nonzero, there exists an element $x_3 \in D$ such that $x_2 = px_3$. Inductively, we obtain a sequence $x_1, x_2, x_3, \dots$ of elements of D with the property that for each positive integer n we have $x_n = px_{n+1}$.

Now, let $H = \langle x_1, x_2, x_3, \dots \rangle \subseteq D$. We claim that $H \simeq \mathbb{Z}(p^\infty)$. Towards this end, define a map

$$\phi : H \to \mathbb{Z}(p^\infty) \quad \text{by} \quad x_n \mapsto \frac{1}{p^n} + \mathbb{Z} \quad \text{for each positive integer } n$$

It can be shown that this map is an isomorphism so that $H \simeq \mathbb{Z}(p^\infty)$, as claimed. Notice that since the nontrivial divisible abelian p-group D was arbitrary that this result implies that any nontrivial divisible abelian p-group contains a subgroup isomorphic to $\mathbb{Z}(p^\infty)$. We will use this observation at the end of the proof.

Next, let $\mathcal{S}$ denote the collection of all subgroups of D that are isomorphic to $\mathbb{Z}(p^\infty)$ and let $\mathcal{T}$ denote the collection of all subsets $\mathcal{X} \subseteq \mathcal{S}$ such that the sum of the elements in $\mathcal{X}$ is direct. Note that $\{H\} \subseteq \mathcal{S}$ is a subset of $\mathcal{S}$ by the above result and that the sum of the elements in $\{H\}$ is clearly direct. In particular, this shows that $\{H\} \in \mathcal{T}$ so that $\mathcal{T} \neq \emptyset$. Define a partial ordering $\leq$ on $\mathcal{T}$ by for if $\mathcal{X}_1, \mathcal{X}_2 \in \mathcal{T}$ then $\mathcal{X}_1 \leq \mathcal{X}_2$ if and only if $\mathcal{X}_1 \subseteq \mathcal{X}_2$.

Now, let $\mathcal{C}$ be a nonempty chain in $\mathcal{T}$ and let $\mathcal{D}$ be the union of the elements of $\mathcal{C}$. Then clearly $\mathcal{D} \subseteq \mathcal{S}$ since each element of $\mathcal{C}$ is a subset of $\mathcal{S}$. Furthermore, since $\mathcal{C}$ is a chain it follows that the sum of the elements in $\mathcal{D}$ is direct since the sum of the elements in each element in $\mathcal{C}$ is direct. It now follows that $\mathcal{D} \in \mathcal{T}$ so that $\mathcal{D}$ is clearly an upper bound for $\mathcal{C}$ in $\mathcal{T}$. By the previous results, we may apply Zorn's Lemma to assert that there exists a maximal element $\mathcal{X} \in \mathcal{T}$.

Note that since $\mathcal{X} \in \mathcal{T}$ that each element of $\mathcal{X}$ is isomorphic to $\mathbb{Z}(p^\infty)$ and that the sum of the elements of $\mathcal{X}$ is direct by the definition of $\mathcal{T}$. Define

$$H = \sum_{X \in \mathcal{X}} X = \bigoplus_{X \in \mathcal{X}} X$$

In particular, since each element of $\mathcal{X}$ is isomorphic to $\mathbb{Z}(p^\infty)$ and since $\mathbb{Z}(p^\infty)$ is divisible, it follows that each element of $\mathcal{X}$ is divisible. Since the direct sum of divisible groups is a divisible group, then, we have by the definition of H that H is a divisible group.

We also claim that H is a direct summand of D. Indeed, since H is a divisible group by the above argument we see that H is an injective $\mathbb{Z}$-module. Furthermore, since H is a subgroup of the abelian group D we have that H is a $\mathbb{Z}$-submodule of the $\mathbb{Z}$-module

D. By the previous two observations, we may conclude that H is a direct summand of D. Therefore, may we write $D = H \oplus K$ for some subgroup K of D.

We claim that K must be the trivial subgroup of D. By way of contradiction, suppose that K were a nontrivial subgroup of D. Since D is a p-group, this implies that K is a nontrivial p-group. Furthermore, note that K is a direct summand of the divisible group D so that K is a divisible group. Combining the previous observations, we see that K is a nontrivial divisible abelian p-group.

Recall that any nontrivial divisible abelian p-group contains a subgroup isomorphic to $\mathbb{Z}(p^\infty)$ by the argument presented at the beginning of this proof. Since K is a nontrivial divisible abelian p-group, then, it must be the case that K contains a subgroup P such that $P \simeq \mathbb{Z}(p^\infty)$. This implies that $P \in \mathcal{S}$ and since $\mathcal{X} \subseteq \mathcal{S}$ as $\mathcal{X} \in \mathcal{T}$, we have that $\mathcal{X} \cup \{P\} \subseteq \mathcal{S}$. In addition, it follows by the above that the sum of the elements in $\mathcal{X} \cup P$ is direct. Combining the previous two observations, we conclude that $\mathcal{X} \cup \{P\} \in \mathcal{T}$. However, this contradicts the maximality of $\mathcal{X} \in \mathcal{T}$ since $\mathcal{X} \subsetneq \mathcal{X} \cup \{P\}$ as $P \notin \mathcal{X}$. We conclude that K is the trivial subgroup of D, as claimed.

Finally, recall that $D = H \oplus K$. But since K is the trivial subgroup of D, it follows that we may now write $D = H$. By the definition of H, we have that H is a direct sum of subgroups of D that are isomorphic to $\mathbb{Z}(p^\infty)$. Therefore, since $D = H$ this completes the proof. $\square$

Problem 11. *Every divisible abelian group is a direct sum of copies of the rationals* $\mathbb{Q}$ *and copies of* $\mathbb{Z}(p^\infty)$ *for various primes* p.

Proof. Suppose that D be a divisible abelian group. Then by a previous exercise, we may write $D = D_t \oplus E$, where D_t is the torsion subgroup of D and E is a torsion-free subgroup of D. In particular, since D_t and E are direct summands of the divisible group D it follows that D_t and E are also divisible groups by a previous exercise. We will use this fact below.

Now, recall that since D is an abelian group that the torsion subgroup D_t of D is a direct sum of p-groups for various primes p. Thus, since D_t is divisible it follows that each direct summand in this direct sum is also divisible by a previous exercise. In other words, we see that each direct summand of D is divisible p-group. Hence, by the previous exercise we have that each direct summand of D_t is a direct sum of copies of $\mathbb{Z}(p^\infty)$ for various primes p.

Finally, since E is a torsion-free divisible group we have once again by a previous exercise that E is isomorphic to a direct sum of copies of $\mathbb{Q}$. Combining the previous results, we see that $D = D_t \oplus E$ is a direct sum of copies of $\mathbb{Z}(p^\infty)$ for various primes p (these direct summands come from the decomposition of D_t described previously) and copies of $\mathbb{Q}$ (these direct summands come from the decomposition of E described previously). This completes the proof. $\square$

Homework 9: Page 206 #2, 3, 5

Problem 2. *If A and B are abelian groups and m, n integers such that $mA = 0 = mB$, then every element of* $\mathrm{Hom}(A, B)$ *has order dividing* (m, n).

Proof. Let $z = (m, n)$. Suppose that $\phi \in \mathrm{Hom}(A, B)$ so that $\phi : A \to B$ is a group homomorphism and let $a \in A$. By hypothesis, we have that $ma = 0$ so that $|a|$ divides m. Now, recall that the order of the homomorphic image of an element of finite order must divide the order of that element. Thus, since $a \in A$ is an element of finite order by the equality $ma = 0$, this observation gives that $|\phi(a)|$ divides $|a|$. Therefore, as $|a|$ divides m this implies that $|\phi(a)|$ divides m.

On the other hand, since $\phi(a) \in B$ we have by hypothesis that $n\phi(a) = 0$ so that $|\phi(a)|$ divides n. Therefore, we have shown that $|\phi(a)|$ divides m and n so that $|\phi(a)|$ divides $(m, n) = z$.

Finally, since the element $a \in A$ above was arbitrary we may now conclude that $|\phi(a)|$ divides z for all $a \in A$ so that $z\phi(a) = 0$ for all $a \in A$. Since this equality holds for all $a \in A$, we may conclude that $|\phi|$ divides z. As $\phi \in \mathrm{Hom}(A, B)$ was arbitrary, this completes the proof. $\square$

Problem 3. *Let* $\pi : \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$ *be the canonical epimorphism. The induced map*

$$\overline{\pi} : \mathrm{Hom}(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}) \to \mathrm{Hom}(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z})$$

is the zero map. Since $\mathrm{Hom}(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z}) \neq 0$, $\overline{\pi}$ *is not an epimorphism.*

Proof. Let $\phi \in \mathrm{Hom}(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z})$. We will show that $\overline{\pi}(\phi) : \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$ is the zero homomorphism. For the sake of contradiction, suppose $\overline{\pi}(\phi)$ were not the zero homomorphism. Then it must be the case that $\overline{\pi}(\phi)(\overline{1}) = \overline{1}$. Now, by the definition of $\overline{\pi}$ we have that

$$\overline{1} = \overline{\pi}(\phi)(\overline{1}) = (\pi \circ \phi)(\overline{1}) = \pi(\phi(\overline{1}))$$

Next, note since $\pi : \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$ is the canonical epimorphism it follows that for an element $m \in \mathbb{Z}$ we have $\pi(m) = \overline{1}$ if and only if m is an odd integer. By the above equality, then, it must be the case that $\phi(\overline{1}) \in \mathbb{Z}$ is an odd integer. Since $\phi(\overline{1})$ is an odd integer, this implies that $\phi(\overline{1}) \in \mathbb{Z}$ is a nonzero element of $\mathbb{Z}$ since 0 is an even integer. Thus, since any nonzero element of $\mathbb{Z}$ has infinite order we may now conclude that $|\phi(\overline{1})| = \infty$.

Finally, note that since $\phi : \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}$ is a group homomorphism and since $\overline{1} \in \mathbb{Z}/2\mathbb{Z}$ is an element of $\mathbb{Z}/2\mathbb{Z}$ of finite order 2 it follows that $\infty = |\phi(\overline{1})|$ divides $|\overline{1}| = 2$ which is clearly absurd. We may now conclude that $\overline{\pi}(\phi) : \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$ is the zero map. Since $\phi \in \mathrm{Hom}(\mathbb{Z}/2\mathbb{Z})$ was arbitrary, the above result shows that $\overline{\pi} : \mathrm{Hom}(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}) \to \mathrm{Hom}(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z})$ is the zero map.

We remark that since $\overline{\pi} : \mathrm{Hom}(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}) \to \mathrm{Hom}(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z})$ is the zero map we have $|\mathrm{Im}(\overline{\pi})| = 1$ and since $|\mathrm{Hom}(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z})| = 2 > 1 = |\mathrm{Im}(\overline{\pi})|$ it now follows that $\overline{\pi}$ is not surjective and hence $\overline{\pi}$ is not an epimorphism. This completes the proof $\square$

Problem 5. *Let R be a ring with identity; then there is a* ring *isomorphism* $\mathrm{Hom}_R(R,R) \simeq R^{\mathrm{op}}$ *where* Hom_R *denotes left R-module homomorphisms. In particular, if R is commutative, then there is a ring isomorphism* $\mathrm{Hom}_R(R,R) \simeq R$.

Proof. For definiteness, let $\circ$ denote composition of maps and let $*$ denote the multiplicative operation in R^{op}. Now, since R has identity we may define a map

$$\psi : \mathrm{Hom}_R(R,R) \to R^{\mathrm{op}} \quad \text{by} \quad \alpha \mapsto \alpha(1)$$

By the definition of ψ, we have that ψ is a well-defined map. Next, let $\alpha, \beta \in \mathrm{Hom}_R(R,R)$. Then we have

$$\psi(\alpha+\beta) = (\alpha+\beta)(1) = \alpha(1) + \beta(1) = \psi(\alpha) + \psi(\beta)$$

so that ψ is a group homomorphism. Now, let $\beta(1) = r \in R$. Then we have by the definition of multiplication in R^{op} and since α is an R-module homomorphism that

$$\begin{aligned}
\psi(\alpha \circ \beta) &= (\alpha \circ \beta)(1) \\
&= \alpha(\beta(1)) \\
&= \alpha(r) \\
&= \alpha(r \cdot 1) \\
&= r\alpha(1) \\
&= \alpha(1) * r \\
&= \alpha(1) * \beta(1) \\
&= \psi(\alpha) * \psi(\beta)
\end{aligned}$$

We may now conclude that ψ is a ring homomorphism.

It remains to prove that ψ is a bijection. First, we prove that ψ is injective. Since ψ is a ring homomorphism, it suffices to show that $\ker(\psi)$ is trivial to establish that ψ is an injection. Towards this end, suppose that $\alpha \in \ker(\psi)$. Then

$$0 = \psi(\alpha) = \alpha(1)$$

Now, let $r \in R$. Then since α is an R-module homomorphism, we obtain

$$\alpha(r) = \alpha(r \cdot 1) = r\alpha(1) = r0 = 0 * r = 0$$

and since $r \in R$ was arbitrary, this shows that α is the zero map. We conclude that $\ker(\psi)$ is trivial and hence ψ is an injection.

Finally, suppose that $r \in R^{\mathrm{op}}$. Define a map $\alpha : R \to R$ by $\alpha(1) = r$. It is easily verified that α is an R-module homomorphism so that $\alpha \in \mathrm{Hom}_R(R,R)$. Furthermore, notice that

$$\psi(\alpha) = \alpha(1) = r$$

and thus ψ is a surjection. The previous results show that ψ is a ring isomorphism so that $\mathrm{Hom}_R(R,R) \simeq R^{\mathrm{op}}$.

We remark that if R is commutative, then clearly $R^{\mathrm{op}} = R$. Thus, by the above results we conclude that if R is a commutative ring then $R = R^{\mathrm{op}} \simeq \mathrm{Hom}_R(R,R)$ so that there is a ring isomorphism $\mathrm{Hom}_R(R,R) \simeq R$. This completes the proof. $\square$

Homework 10: Page 206 #8, 9, 10

Problem 8. *If R has an identity and we denote the left R-module R by ${}_RR$ and the right R-module R by R_R, then $({}_RR)^* \simeq R_R$ and $(R_R)^* \simeq {}_RR$.*

Proof. We will prove that $({}_RR)^* \simeq R_R$ and remark that the proof that $(R_R)^* \simeq {}_RR$ is analogous. Towards this end, first note that since R has 1 we may define a map

$$\psi : ({}_RR)^* \to R_R \quad \text{by} \quad \phi \mapsto \phi(1)$$

Notice that as $\phi : {}_RR \to R$ for all $\phi \in ({}_RR)^*$ it follows that ψ is a well-defined map. We claim that ψ is a right R-module isomorphism. Indeed, let $\phi_1, \phi_2 \in ({}_RR)^*$. Then

$$\psi(\phi_1 + \phi_2) = (\phi_1 + \phi_2)(1) = \phi_1(1) + \phi_2(1) = \psi(\phi_1) + \psi(\phi_2)$$

Furthermore, if $r \in R$ and $\phi \in ({}_RR)^*$ we have

$$\psi(\phi r) = (\phi r)(1) = \phi(1)r = \psi(\phi)r$$

By the previous two results, we have that ψ is a right R-module homomorphism.

It remains to prove that ψ is a bijection. First, we prove that ψ is injective. Since ψ is a right R-module homomorphism, it suffices to show that $\ker(\psi)$ is trivial to establish that ψ is an injection. Towards this end, suppose that $\phi \in \ker(\psi)$. Then

$$0 = \psi(\phi) = \phi(1)$$

Now, let $r \in R$. Then since ϕ is a left R-module homomorphism, we obtain

$$\phi(r) = \phi(r \cdot 1) = r\phi(1) = r0 = 0$$

and since $r \in R$ was arbitrary, this shows that ϕ is the zero map. We conclude that $\ker(\psi)$ is trivial and hence ψ is an injection.

Finally, suppose that $r \in R_R$. Define a map $\phi : {}_RR \to R$ by $\phi(1) = r$. It is easily verified that ϕ is a left R-module homomorphism so that $\phi \in ({}_RR)^*$. Furthermore, notice

$$\psi(\phi) = \phi(1) = r$$

and thus ψ is a surjection. The previous results show that ψ is a right R-module isomorphism so that $({}_RR)^* \simeq R_R$. As previously-mentioned, the proof that $(R_R)^* \simeq {}_RR$ is analogous to the one presented above. This completes the proof. $\square$

Problem 9. *For any homomorphism $f : A \to B$ of left R-modules the diagram*

$$\begin{tikzcd} A \arrow[r, "\theta_A"] \arrow[d, "f"] & A^{**} \arrow[d, "f^*"] \\ B \arrow[r, "\theta_B"] & B^{**} \end{tikzcd}$$

is commutative, where θ_A, θ_B are as in Theorem 4.12 and f^* is the map induced on $A^{**} = \mathrm{Hom}_R(\mathrm{Hom}_R(A, R), R)$ by the map $\overline{f} : \mathrm{Hom}_R(B, R) \to \mathrm{Hom}_R(A, R)$.

Proof. For definiteness, note that we must show $f^* \circ \theta_A = \theta_B \circ f$. We also point out that

$$\theta_A : A \to A^{**} \quad \text{by} \quad \theta_A(a) : A^* \to R \quad \text{by} \quad \theta_A(a)(g) = g(a)$$

and

$$\theta_B : B \to B^{**} \quad \text{by} \quad \theta_B(b) : B^* \to R \quad \text{by} \quad \theta_B(b)(g) = g(b)$$

and

$$\overline{f} : B^* \to A^* \quad \text{by} \quad \overline{f}(\phi) = \phi \circ f : A \to R$$

and

$$f^* : A^{**} \to B^{**} \quad \text{by} \quad f^*(\psi) = \psi \circ \overline{f} : B^* \to R$$

Now, let $a \in A$. By the above definitions, we have

$$(f^* \circ \theta_A)(a) = f^*(\theta_A(a)) = \theta_A(a) \circ \overline{f} : B^* \to R$$

and

$$(\theta_B \circ f)(a) = \theta_B(f(a)) : B^* \to R$$

To complete the proof, let $g \in B^*$. Then by the above definitions, we have

$$(\theta_A(a) \circ \overline{f})(g) = \theta_A(a)(\overline{f}(g)) = \theta_A(a)(g \circ f) = (g \circ f)(a) = g(f(a))$$

and

$$(\theta_B(f(a)))(g) = g(f(a))$$

Since $g \in B^*$ was arbitrary, the previous two results show that $\theta_A \circ \overline{f} = \theta_B(f(a))$ and therefore by our initial two results we obtain

$$(f^* \circ \theta_A)(a) = \theta_A(a) \circ \overline{f} = \theta_B(f(a)) = (\theta_B \circ f)(a)$$

Since $a \in A$ was arbitrary, the above result shows that $f^* \circ \theta_A = \theta_B \circ f$. Thus, by our initial observation the diagram commutes. This completes the proof. $\square$

Problem 10. *Let $F = \sum_{x \in X} \mathbb{Z}x$ be a free $\mathbb{Z}$-module with infinite basis X. Then $\{f_x : x \in X\}$ (Theorem 4.11) does not form a basis of F^*.*

Proof. First, note that

$$F^* = \mathrm{Hom}_{\mathbb{Z}}(F, \mathbb{Z}) = \mathrm{Hom}_{\mathbb{Z}}\left(\sum_{x \in X} \mathbb{Z}x, \mathbb{Z}\right) \simeq \prod_{x \in X} \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}x, \mathbb{Z})$$

But since we clearly have $\mathbb{Z}x \simeq \mathbb{Z}$ for each $x \in X$ and since $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, \mathbb{Z}) \simeq \mathbb{Z}$, we obtain

$$\prod_{x \in X} \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}x, \mathbb{Z}) \simeq \prod_{x \in X} \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, \mathbb{Z}) \simeq \prod_{x \in X} \mathbb{Z} \simeq \prod_{x \in X} \mathbb{Z}x$$

Therefore, combining the previous two results shows that

$$F^* \simeq \prod_{x \in X} \mathbb{Z}x$$

and thus there exists an isomorphism $\phi : F^* \to \prod_{x \in X} \mathbb{Z}x$.

Now, for the sake of contradiction suppose that $\{f_x : x \in X\}$ were a basis for F^*. Note that for each $y \in X$ we have by the definition of the isomorphism ϕ that

$$\phi(f_y) = \begin{cases} x & \text{if } x = y \\ 0 & \text{if } x \neq y \end{cases} \qquad \text{for each } x, y \in X$$

Furthermore, since $\{f_x : x \in X\}$ is a basis for F^* and as ϕ is an isomorphism it follows that $\{\phi(f_y) : y \in X\}$ is a basis for $\prod_{x \in X} \mathbb{Z}x$ and hence must span $\prod_{x \in X} \mathbb{Z}x$. Therefore, for the element

$$(x)_{x \in X} \in \prod_{x \in X} \mathbb{Z}x$$

there is a finite $\mathbb{Z}$-linear combination of elements from $\{\phi(f_y) : y \in X\}$ that is equal to the element $(x)_{x \in X}$.

Finally, note that any finite $\mathbb{Z}$-linear combination of elements from $\{\phi(y) : y \in X\}$ must be equal to 0 in all but finitely many coordinates by the above equality. Therefore, since $(x)_{x \in X}$ is a finite $\mathbb{Z}$-linear combination of elements from $\{\phi(y) : y \in X\}$ it now follows that $(x)_{x \in X}$ is equal to 0 in all but finitely many coordinates. However, this is clearly a contradiction since X is infinite. We conclude that $\{f_x : x \in X\}$ does not form a basis for F^*, completing the proof. $\square$

Homework 11: Page 216 #2, 3, 7

Problem 2. *Let A and B be abelian groups.*

(a): *For each $m > 0$, $A \otimes \mathbb{Z}_m \simeq A/mA$.*

(b): $\mathbb{Z}_m \otimes \mathbb{Z}_n \simeq \mathbb{Z}_c$, *where $c = (m, n)$.*

(c): *Describe $A \otimes B$, when A and B are finitely generated.*

Note: We will be informal in the discussion in Part (c) to avoid obfuscating the point.

Proof. (a): Let $m > 0$ and define a map

$$f : A \times \mathbb{Z}_m \to A/mA \quad \text{by} \quad (a, \overline{z}) \mapsto za + mA$$

We show that f is well-defined. Towards this end, suppose that $(a_1, \overline{z_1}) = (a_2, \overline{z_2})$ for some $(a_1, \overline{z_1}), (a_2, \overline{z_2}) \in A \times \mathbb{Z}_m$. Then clearly $a_1 = a_2$ and $\overline{z_1} = \overline{z_2}$. Since $\overline{z_1} = \overline{z_2}$, it follows that

$$\overline{0} = \overline{z_1} - \overline{z_2} = \overline{z_1 - z_2}$$

so that m divides $z_1 - z_2$. Now, since $a_1 = a_2$ we can write $a_1 = a_2 = a \in A$. Furthermore, since m divides $z_1 - z_2$ we have $(z_1 - z_2)a \in mA$. Hence, we obtain

$$\begin{aligned} f(a_1, \overline{z_1}) - f(a_2, \overline{z_2}) &= f(a, \overline{z_1}) - f(a, \overline{z_2}) \\ &= (z_1 a + mA) - (z_2 a + mA) \\ &= (z_1 - z_2)a + mA \\ &= mA \end{aligned}$$

In particular, the above result shows that $f(a_1, \overline{z_1}) - f(a_2, \overline{z_2})$ is equal to the identity element of A/mA so that $f(a_1, \overline{z_1}) = f(a_2, \overline{z_2})$ which shows that f is well-defined. Furthermore, it is easily verified that f is a middle linear map and hence there exists a (unique) group homomorphism $\phi : A \otimes \mathbb{Z}_m \to A/mA$ such that $\phi \circ g = f$, where $g : A \times \mathbb{Z}_m \to A \otimes \mathbb{Z}_m$ is the tensor product.

Now, note that if $a \in A$ and $\overline{z} \in \mathbb{Z}_m$ we have since $\phi \circ g = f$ that

$$\phi(a \otimes \overline{z}) = \phi(g(a, \overline{z})) = f(a, \overline{z}) = za + mA$$

and

$$a \otimes \overline{z} = a \otimes z\overline{1} = g(a, z\overline{1}) = g(za, \overline{1}) = za \otimes \overline{1}$$

In particular, the second of the above equalities shows if $a \in A$ and $\overline{z} \in \mathbb{Z}_m$ then we have $a \otimes \overline{z} = b \otimes \overline{1}$ for some $b \in A$. Therefore, since $A \otimes \mathbb{Z}_m$ is generated by the elements of the form $a \otimes \overline{z}$ where $a \in A$ and $\overline{z} \in \mathbb{Z}_m$ it now follows that any element in $A \otimes \mathbb{Z}_m$ is a finite sum of elements of the form $b \otimes \overline{1}$ where $b \in A$. In addition, note that if $a_1, a_2 \in A$ and if $a = a_1 + a_2 \in A$ then

$$(a_1 \otimes \overline{1}) + (a_2 \otimes \overline{1}) = g(a_1, \overline{1}) + g(a_2, \overline{1}) = g(a_1 + a_2, \overline{1}) = (a_1 + a_2) \otimes \overline{1} = a \otimes \overline{1}$$

Inductively, the above equality shows that any finite sum of elements of the form $b \otimes \overline{1}$ where $b \in A$ and $\overline{1} \in \mathbb{Z}_m$ is again an element of the same form. By our previous observation, then, we may now conclude that every element of $A \otimes \mathbb{Z}_m$ is of the form $b \otimes \overline{1}$ for some $b \in A$.

Next, we show that ϕ is an injection by using the above results. Since ϕ is a group homomorphism, it suffices to show that $\ker \phi$ is trivial to establish that ϕ is an injection. Towards this end, suppose that $x \in \ker \phi$. By the above result, we may write $x = b \otimes \overline{1}$ for some $b \in A$. Therefore, since $b \otimes \overline{1} = x \in \ker \phi$ and by the first of the above equalities we obtain

$$mA = \phi(x) = \phi(b \otimes \overline{1}) = 1b + mA = b + mA$$

and hence $b \in mA$. Thus, there is some $c \in A$ such that $b = mc$. Appealing to the second of the above equalities, then, we obtain

$$x = b \otimes \overline{1} = mc \otimes \overline{1} = c \otimes \overline{m} = c \otimes \overline{0} = 0$$

and hence $\ker \phi$ is trivial. We conclude that ϕ is an injection.

Finally, we show that ϕ is a surjection. Since $\phi \circ g = f$, it suffices to show that f is a surjection to establish that ϕ is a surjection. Towards this end, let $a + mA \in A/mA$. Then clearly $(a, \overline{1}) \in A \times \mathbb{Z}_m$ and

$$f(a, \overline{1}) = 1a + mA = a + mA$$

so that f is a surjection. We conclude that ϕ is a surjection. Combining the previous results, we see that ϕ is a group isomorphism so that $A \otimes \mathbb{Z}_m \simeq A/mA$. $\square$

Proof. (b): First, note that since $\mathbb{Z}_m$ is an abelian group and as $n > 0$ that by the result of Part (a) we have $\mathbb{Z}_m \otimes \mathbb{Z}_n \simeq \mathbb{Z}_m/n\mathbb{Z}_m$. We claim that $\mathbb{Z}_m/n\mathbb{Z}_m \simeq \mathbb{Z}_c$, where $c = (m, n)$. Towards this end, define a map

$$\phi : \mathbb{Z}_m \to \mathbb{Z}_c \quad \text{by} \quad z + m\mathbb{Z} \mapsto z + c\mathbb{Z}$$

First, we show that ϕ is well-defined. Towards this end, suppose that $z_1 + m\mathbb{Z} = z_2 + m\mathbb{Z}$ for some $z_1 + m\mathbb{Z}, z_2 + m\mathbb{Z} \in \mathbb{Z}_m$. In this case, we have $z_1 - z_2 \in m\mathbb{Z}$ and hence there is some $z \in \mathbb{Z}$ such that $z_1 - z_2 = mz$. But since $c = (m, n)$, it follows that there is some $k \in \mathbb{Z}$ such that $m = ck$ and hence $z_1 - z_2 = mz = ckz$. This gives

$$\phi(z_1 + m\mathbb{Z}) - \phi(z_2 + m\mathbb{Z}) = (z_1 + c\mathbb{Z}) - (z_2 + c\mathbb{Z}) = (z_1 - z_2) + c\mathbb{Z} = ckz + c\mathbb{Z} = c\mathbb{Z}$$

In particular, the above result shows that $\phi(z_1 + m\mathbb{Z}) - \phi(z_2 + m\mathbb{Z})$ is equal to the identity element of $\mathbb{Z}_c$ so that $\phi(z_1 + m\mathbb{Z}) = \phi(z_2 + m\mathbb{Z})$ which shows that ϕ is well-defined.

Next, note that by the definition of ϕ it is clear that ϕ is a surjective group homomorphism. We claim that $\ker \phi = n\mathbb{Z}_m$. Towards this end, first let $z + m\mathbb{Z} \in \ker \phi \subseteq \mathbb{Z}_m$. Then we have

$$c\mathbb{Z} = \phi(z + m\mathbb{Z}) = z + c\mathbb{Z}$$

so that $z \in c\mathbb{Z}$. Therefore, there is some $k \in \mathbb{Z}$ such that $z = ck$. Now, since $c = (m, n)$, there exist elements $z_1, z_2 \in \mathbb{Z}$ such that $z_1 m + z_2 n = c$. Thus, combining the previous

results now gives

$$\begin{aligned} z + m\mathbb{Z} &= ck + m\mathbb{Z} \\ &= (z_1 m + z_2 n)k + m\mathbb{Z} \\ &= (mz_1 k + nz_2 k) + m\mathbb{Z} \\ &= nz_2 k + m\mathbb{Z} \\ &= n(z_2 k + m\mathbb{Z}) \\ &\in n\mathbb{Z}_m \end{aligned}$$

so that $z + m\mathbb{Z} \in n\mathbb{Z}_m$. On the other hand, let $n(z + m\mathbb{Z}) \in n\mathbb{Z}_m$. Since $c = (m, n)$, there is some $k \in \mathbb{Z}$ such that $n = ck$. Hence, by the definition of ϕ we obtain

$$\phi(n(z + m\mathbb{Z})) = \phi(nz + m\mathbb{Z}) = nz + c\mathbb{Z} = ckz + c\mathbb{Z} = c\mathbb{Z}$$

so that $n(z+m\mathbb{Z}) \in \ker\phi$. The previous results now show that $\ker\phi = n\mathbb{Z}_m$. Therefore, by the previous results and by the First Isomorphism Theorem we have

$$\mathbb{Z}_m/n\mathbb{Z}_m = \mathbb{Z}_m/\ker\phi \simeq \mathbb{Z}_c$$

Finally, combining the previous results now shows that

$$\mathbb{Z}_m \otimes \mathbb{Z}_n \simeq \mathbb{Z}_m/n\mathbb{Z}_m \simeq \mathbb{Z}_c$$

so that $\mathbb{Z}_m \otimes \mathbb{Z}_n \simeq \mathbb{Z}_c$. This completes the proof. □

Proof. (c): Suppose that A and B are finitely generated abelian groups. Then by the Fundamental Theorem of Finitely Generated Abelian Groups, we can write

$$A \simeq \mathbb{Z}_{n_1} \oplus \cdots \oplus \mathbb{Z}_{n_r} \oplus \bigoplus_{i=1}^{n_0} \mathbb{Z}$$

and

$$B \simeq \mathbb{Z}_{m_1} \oplus \cdots \oplus \mathbb{Z}_{m_s} \oplus \bigoplus_{i=1}^{m_0} \mathbb{Z}$$

We discuss $A \otimes B$ based on the above and the previous results of this problem.

By the result of Part (a), it follows that given any abelian group C we have $C \otimes \mathbb{Z} \simeq C$ and $\mathbb{Z} \otimes C \simeq C$. Also, recall that $\otimes$ distributes over $\oplus$. Therefore, by Part (b) and by noting the above decompositions of A and B we see that $A \otimes B$ is the direct sum of:

- $\mathbb{Z}_{(n_i, m_j)}$ for each pair $(i, j) \in \{1, \ldots, r\} \times \{1, \ldots, s\}$.
- m_0 copies of each of the $\mathbb{Z}_{n_i}$ for each $i \in \{1, \ldots, r\}$.
- n_0 copies of each of the $\mathbb{Z}_{m_j}$ for each $j \in \{1, \ldots, s\}$.
- $n_0 m_0$ copies of $\mathbb{Z}$.

This completes our discussion. □

Problem 3. *If A is a torsion abelian group and $\mathbb{Q}$ the (additive) group of rationals, then*

(a): $A \otimes \mathbb{Q} = 0$.

(b): $\mathbb{Q} \otimes \mathbb{Q} \simeq \mathbb{Q}$.

Proof. (a): Let $a \in A$ and $r \in \mathbb{Q}$. We claim that $a \otimes r = 0$. Towards this end, first note that since $a \in A$ and as A is torsion that there exists a nonzero element $n \in \mathbb{Z}$ such that $na = 0$. Furthermore, since n is a nonzero element of $\mathbb{Z}$ we have that $\frac{r}{n} \in \mathbb{Q}$. Therefore, if $g : A \times \mathbb{Q} \to A \otimes \mathbb{Q}$ is the tensor product then

$$a \otimes r = g(a, r) = g\left(a, n\frac{r}{n}\right) = g\left(na, \frac{r}{n}\right) = g\left(0, \frac{r}{n}\right) = 0 \otimes \frac{r}{n} = 0$$

The above equality establishes our claim.

Finally, recall that $A \otimes \mathbb{Q}$ is generated by the elements of the form $a \otimes r$ where $a \in A$ and $r \in \mathbb{Q}$. But by our previous result, we know that any element of this form is equal to 0 and hence the group generated by these elements must also be equal to 0. By the previous observation, then, we conclude that $A \otimes \mathbb{Q} = 0$. $\square$

Proof. (b): First, we show that if $\frac{a}{b}, \frac{c}{d} \in \mathbb{Q}$ then $\frac{a}{b} \otimes \frac{c}{d} = \frac{ac}{bd} \otimes 1$. Indeed, note that

$$\frac{a}{b} \otimes \frac{c}{d} = \frac{ad}{bd} \otimes \frac{c}{d} = d\frac{a}{bd} \otimes \frac{c}{d} = \frac{a}{bd} \otimes d\frac{c}{d} = \frac{a}{bd} \otimes c\frac{d}{d} = c\frac{a}{bd} \otimes \frac{d}{d} = \frac{ac}{bd} \otimes 1$$

The above equality establishes our claim. In particular, since $\mathbb{Q} \otimes \mathbb{Q}$ is generated by the elements of the form $\frac{a}{b} \otimes \frac{c}{d}$ where $\frac{a}{b}, \frac{c}{d} \in \mathbb{Q}$ it now follows that $\mathbb{Q} \otimes \mathbb{Q}$ is generated by the elements of the form $r \otimes 1$ where $r \in \mathbb{Q}$. Hence, we may now assert that every element of $\mathbb{Q} \otimes \mathbb{Q}$ is a finite sum of elements of the form $r \otimes 1$ where $r \in \mathbb{Q}$. Furthermore, suppose that $r_1, r_2 \in \mathbb{Q}$. Then we have

$$(r_1 \otimes 1) + (r_2 \otimes 1) = (r_1 + r_2) \otimes 1$$

Inductively, the above equality shows that any finite sum of elements of the form $r \otimes 1$ where $r \in \mathbb{Q}$ is again an element of the same form. By our previous observation, then, we may now conclude that any element of $\mathbb{Q} \otimes \mathbb{Q}$ is of the form $r \otimes 1$ for some $r \in \mathbb{Q}$.

Now, define a map

$$f : \mathbb{Q} \times \mathbb{Q} \to \mathbb{Q} \quad \text{by} \quad (r, s) \mapsto rs$$

It is easily verified that f is a middle linear map and hence there exists a (unique) group homomorphism $\phi : \mathbb{Q} \otimes \mathbb{Q} \to \mathbb{Q}$ such that $\phi \circ g = f$, where $g : \mathbb{Q} \times \mathbb{Q} \to \mathbb{Q} \otimes \mathbb{Q}$ is the tensor product. We will claim that ϕ is a bijection.

First, we show that ϕ is an injection. Since ϕ is a group homomorphism, it suffices to show that $\ker \phi$ is trivial to establish that ϕ is an injection. Towards this end, let $x \in \ker \phi$. By the above result, we may write $x = r \otimes 1$ for some $r \in \mathbb{Q}$. Therefore, since $r \otimes 1 = x \in \ker \phi$ we obtain

$$0 = \phi(x) = \phi(r \otimes 1) = \phi(g(r, 1)) = f(r, 1) = r \cdot 1 = r$$

and hence

$$x = r \otimes 1 = 0 \otimes 1 = 0$$

We conclude that $\ker \phi$ is trivial so that ϕ is an injection.

Finally, we show that ϕ is a surjection. Since $\phi \circ g = f$, it suffices to show that f is a surjection to establish that ϕ is a surjection. Towards this end, let $r \in \mathbb{Q}$. Then clearly $(r, 1) \in \mathbb{Q} \times \mathbb{Q}$ and

$$f(r, 1) = r \cdot 1 = r$$

so that f is a surjection. We conclude that ϕ is a surjection. Combining the previous results, we see that ϕ is a group isomorphism so that $\mathbb{Q} \otimes \mathbb{Q} \simeq \mathbb{Q}$. $\square$

Problem 7. *The usual injection $\alpha : \mathbb{Z}_2 \to \mathbb{Z}_4$ is a monomorphism of abelian groups. Show that $1 \otimes \alpha : \mathbb{Z}_2 \otimes \mathbb{Z}_2 \to \mathbb{Z}_2 \otimes \mathbb{Z}_4$ is the zero map.*

Proof. Before we begin, we remark that $\alpha : \mathbb{Z}_2 \to \mathbb{Z}_4$ is the map defined by $\overline{0} \mapsto \overline{0}$ and $\overline{1} \mapsto \overline{2}$. Therefore, it is clear that α is indeed a monomorphism of abelian groups.

Now, recall that the map $1 \otimes \alpha : \mathbb{Z}_2 \otimes \mathbb{Z}_2 \to \mathbb{Z}_2 \otimes \mathbb{Z}_4$ is given by $(1 \otimes \alpha)(a \otimes b) = 1(a) \otimes \alpha(b)$ for all $a, b \in \mathbb{Z}_2$. Furthermore, recall by the definition of α we have $\alpha(\overline{0}) = \overline{0}$ and $\alpha(\overline{1}) = \overline{2}$. Therefore, we obtain

$$(1 \otimes \alpha)(\overline{0} \otimes \overline{0}) = 1(\overline{0}) \otimes \alpha(\overline{0}) = \overline{0} \otimes \overline{0} = 0$$

and

$$(1 \otimes \alpha)(\overline{1} \otimes \overline{0}) = 1(\overline{1}) \otimes \alpha(\overline{0}) = \overline{1} \otimes \overline{0} = 0$$

and

$$(1 \otimes \alpha)(\overline{0} \otimes \overline{1}) = 1(\overline{0}) \otimes \alpha(\overline{1}) = \overline{0} \otimes \overline{2} = 0$$

and

$$(1 \otimes \alpha)(\overline{1} \otimes \overline{1}) = 1(\overline{1}) \otimes \alpha(\overline{1}) = \overline{1} \otimes \overline{2} = \overline{1} \otimes 2\overline{1} = 2\overline{1} \otimes \overline{1} = \overline{0} \otimes \overline{1} = 0$$

The above equalities reveal that $1 \otimes \alpha$ maps every possible element of $\mathbb{Z}_2 \otimes \mathbb{Z}_2$ to the zero element of $\mathbb{Z}_2 \otimes \mathbb{Z}_4$. Thus, we conclude that $1 \otimes \alpha : \mathbb{Z}_2 \otimes \mathbb{Z}_2 \to \mathbb{Z}_2 \otimes \mathbb{Z}_4$ is the zero map. This completes the proof. $\square$

Homework 12: Page 216 #9, 10, 11

Problem 9. (a): *If I is a right ideal of a ring R with identity and B a left R-module, then there is a group isomorphism $R/I \otimes_R B \simeq B/IB$, where IB is the subgroup of B generated by all elements rb with $r \in I, b \in B$.*

(b): *If R is commutative with identity and I, J are ideals of R, then there is an R-module isomorphism $R/I \otimes_R R/J \simeq R/(I+J)$.*

Proof. (a): First, define a map

$$f : R/I \times B \to B/IB \quad \text{by} \quad (r+I, b) \mapsto rb + IB$$

Note that since B is a left R-module that f is indeed a map. Next, we show that f is well-defined. Towards this end, suppose that $(r_1 + I, b_1) = (r_2 + I, b_2)$ for some $(r_1 + I, b_1), (r_2 + I, b_2) \in R/I \times B$. Clearly, this gives $r_1 + I = r_2 + I$ so that $r_1 - r_2 \in I$ and that $b_1 = b_2$ so that we may write $b_1 = b_2 = b \in B$. Now, since $r_1 - r_2 \in I$ and $b \in B$ we have $(r_1 - r_2)b \in IB$ and hence

$$\begin{aligned} f(r_1 + I, b_1) - f(r_2 + I, b_2) &= f(r_1 + I, b) - f(r_2 + I, b) \\ &= (r_1 b + IB) - (r_2 b + IB) \\ &= (r_1 - r_2)b + IB \\ &= IB \end{aligned}$$

In particular, the above result shows that $f(r_1 + I, b_1) - f(r_2 + I, b_2)$ is equal to the identity element of B/IB so that $f(r_1 + I, b_1) = f(r_2 + I, b_2)$ which shows that f is well-defined. Furthermore, it is easily verified that f is a middle linear map and hence there exists a (unique) group homomorphism $\phi : R/I \otimes_R B \to B/IB$ such that $\phi((r+I) \otimes_R b) = f(r+I, b) = rb + IB$ for all $r + I \in R/I$ and $b \in B$.

Now, let $r_1 + I, r_2 + I \in R/I$ and $b_1, b_2 \in B$. Let $b = r_1 b_1 + r_2 b_2$. Then since B is a left R-module, we have that $b \in B$. Furthermore, as R has identity we have that

$$\begin{aligned} ((r_1 + I) \otimes_R b_1) + ((r_2 + I) \otimes_R b_2) &= ((1+I)r_1 \otimes_R b_1) + ((1+I)r_2 \otimes_R b_2) \\ &= ((1+I) \otimes_R r_1 b_1) + ((1+I) \otimes_R r_2 b_2) \\ &= (1+I) \otimes_R (r_1 b_1 + r_2 b_2) \\ &= (1+I) \otimes_R b \end{aligned}$$

Inductively, this equality shows that any finite sum of elements of the form $(r+I) \otimes_R b$ where $r + I \in R/I$ and $b \in B$ is of the form $(1+I) \otimes_R c$ where $c \in B$. Therefore, since every element of $R/I \otimes_R B$ is a finite sum of elements of the form $(r+I) \otimes_R b$ where $r + I \in R/I$ and $b \in B$ it now follows that every element of $R/I \otimes_R B$ is of the form $(1+I) \otimes_R c$ where $c \in B$.

Next, we show that ϕ is an injection. Towards this end, suppose that $x \in \ker \phi$. By the previous observation, we may write $x = (1+I) \otimes_R b$ where $b \in B$. Now, since $x \in \ker \phi$ we have

$$IB = \phi(x) = \phi((1+I) \otimes_R b) = 1b + IB = b + IB$$

so that $b \in IB$. Therefore, we may write $b = \sum_{j=1}^{n} i_j b_j$ for some $i_1, \ldots, i_n \in I$ and $b_1, \ldots, b_n \in B$. This gives

$$\begin{aligned}
x &= (1+I) \otimes_R b \\
&= (1+I) \otimes_R \left(\sum_{j=1}^{n} i_j b_j \right) \\
&= \sum_{j=1}^{n} [(1+I) \otimes_R i_j b_j] \\
&= \sum_{j=1}^{n} [(1+I) i_j \otimes_R b_j] \\
&= \sum_{j=1}^{n} [(1 \cdot i_j + I) \otimes_R b_j] \\
&= \sum_{j=1}^{n} [(i_j + I) \otimes_R b_j] \\
&= \sum_{j=1}^{n} (I \otimes_R b_j) \\
&= I \otimes_R \left(\sum_{j=1}^{n} b_j \right) \\
&= 0
\end{aligned}$$

and hence $x = 0$ so that $\ker \phi$ is trivial. We conclude that ϕ is an injection.

Finally, we show that ϕ is a surjection. As follows by observing the arguments of the previous homework, it suffices to show that f is an surjection in order to conclude that ϕ is a surjection. Towards this end, let $b + IB \in B/IB$. As R has identity, we have $(1+I, b) \in R/I \times B$ and

$$f(1+I, b) = 1b + IB = b + IB$$

so that f is a surjection. Therefore, we conclude that ϕ is a surjection and hence ϕ is a group isomorphism so that $R/I \otimes_R B \simeq B/IB$. $\square$

Proof. (b): Before we begin, we remark that since R is commutative we have that $R/I \otimes_R R/J$ is an R-module. Furthermore, it is also clear that $(R/J)/(I(R/J))$ is an R-module.

We now prove the main result. Towards this end, note that we can view R/J as a left R-module and so by Part (a) there exists a (unique) group isomorphism

$$\phi : R/I \otimes_R R/J \to \frac{R/J}{I(R/J)}$$

where ϕ is defined as in Part (a). Next, we show that ϕ is an R-module isomorphism. Towards this end, note that by our initial observation at the beginning of this problem and since ϕ is a group isomorphism that we need only show ϕ preserves the R-module structure to establish that ϕ is an R-module isomorphism.

Indeed, suppose that $r_1 + I \in R/I$ and $r_2 + J \in R/J$ and let $s \in R$. Then by the definition of ϕ from Part (a), we have

$$\begin{aligned}\phi(s((r_1 + I) \otimes_R (r_2 + J))) &= \phi((s(r_1 + I)) \otimes_R (r_2 + J)) \\ &= \phi((sr_1 + I) \otimes_R (r_2 + J)) \\ &= (sr_1(r_2 + J)) + I(R/J)\end{aligned}$$

and

$$\begin{aligned}s\phi((r_1 + I) \otimes_R (r_2 + J)) &= s[(r_1(r_2 + J)) + I(R/J)] \\ &= (sr_1(r_2 + J)) + I(R/J)\end{aligned}$$

Hence, by the above result it now follows that ϕ preserves the R-module structure. We may now conclude that

$$\phi : R/I \otimes_R R/J \to \frac{R/J}{I(R/J)}$$

is an R-module isomorphism.

Next, we claim that $I(R/J) = (I + J)/J$. Indeed, first let $x \in I(R/J)$. Then

$$x = \sum_{k=1}^{n} (i_k(r_k + J))$$

for some $i_1, \ldots, i_n \in I$ and $r_1 + J, \ldots, r_n + J \in R/J$. Since I is an ideal of R and $i_k \in I$, we have $i_k r_k \in I$ for each $k \in \{1, \ldots, n\}$. Furthermore, since J is an ideal we have $0 \in J$. Combining the previous two observations, then, we see that

$$(i_k r_k + 0) + J \in (I + J)/J$$

for each $k \in \{1, \ldots, n\}$. Thus, since $(I + J)/J$ is clearly closed under addition we obtain

$$x = \sum_{k=1}^{n} (i_k(r_k + J)) = \sum_{k=1}^{n} (i_k r_k + J) = \sum_{k=1}^{n} ((i_k r_k + 0) + J) \in (I + J)/J$$

On the other hand, let $x \in (I + J)/J$. Then $x = (i + j) + J$ for some $i \in I$ and $j \in J$. Thus, since R has identity and as $j \in J$ we have

$$x = (i + j) + J = i + J = i \cdot 1 + J = i(1 + J) \in I(R/J)$$

The previous two results show that $I(R/J) = (I + J)/J$, as claimed.

Finally, note that by the Third Isomorphism Theorem for Modules we have

$$\frac{R/J}{(I + J)/J} \simeq \frac{R}{I + J}$$

as R-modules. Combining the previous results, then, we conclude that

$$R/I \otimes_R R/J \simeq \frac{R/J}{I(R/J)} = \frac{R/J}{(I + J)/J} \simeq \frac{R}{I + J}$$

with each of the above isomorphisms being isomorphisms of R-modules. Thus, we conclude that $R/I \otimes_R R/J \simeq R/(I+J)$ as R-modules and hence there is an R-module isomorphism $R/I \otimes_R R/J \simeq R/(I+J)$. This completes the proof. $\square$

Problem 10. *If R, S are rings, A a right R-module, B an R, S-bimodule, and C a left S-module and D is an abelian group, define a* middle linear map *to be a map $f : A \times B \times C \to D$ such that*

(i): $f(a + a', b, c) = f(a, b, c) + f(a', b, c)$

(ii): $f(a, b + b', c) = f(a, b, c) + f(a, b', c)$

(iii): $f(a, b, c + c') = f(a, b, c) + f(a, b, c')$

(iv): $f(ar, b, c) = f(a, rb, c)$ *for* $r \in R$

(v): $f(a, bs, c) = f(a, b, sc)$ *for* $s \in S$

Then:

(a): *The map $i : A \times B \times C \to (A \otimes_R B) \otimes_S C$ given by $(a, b, c) \mapsto (a \otimes_R b) \otimes_S c$ is middle linear.*

(b): *The middle linear map i is* universal*; that is, given a middle linear map $g : A \times B \times C \to D$, there exists a unique group homomorphism $\overline{g} : (A \otimes_R B) \otimes_S C \to D$ such that $\overline{g} \circ i = g$.*

(c): *The map $j : A \times B \times C \to A \otimes_R (B \otimes_S C)$ given by $(a, b, c) \mapsto a \otimes_R (b \otimes_S c)$ is also a universal middle linear map.*

(d): $(A \otimes_R B) \otimes_S C \simeq A \otimes_R (B \otimes_S C)$.

Proof. (a): We will verify that i is middle linear by verifying (i) through (v) as in the statement of this problem one-by-one. Towards this end, let $a, a' \in A$, $b, b' \in B$, $c, c' \in C$, $r \in R$, and $s \in S$ for all parts of what follows.

To verify (i), we have

$$i(a + a', b, c) = [(a + a') \otimes_R b] \otimes_S c = [(a \otimes_R b) + (a' \otimes_R b)] \otimes_S c$$

and

$$i(a, b, c) + i(a', b, c) = [(a \otimes_R b) \otimes_S c] + [(a' \otimes_R b) \otimes_S c] = [(a \otimes_R b) + (a' \otimes_R b)] \otimes_S c$$

which verifies (i).

To verify (ii), we have

$$i(a, b + b', c) = [(a \otimes_R (b + b')] \otimes_S c = [(a \otimes_R b) + (a \otimes_R b')] \otimes_S c$$

and

$$i(a, b, c) + i(a, b', c) = [(a \otimes_R b) \otimes_S c] + [(a \otimes_R b') \otimes_S c] = [(a \otimes_R b) + (a \otimes_R b')] \otimes_S c$$

which verifies (ii).

To verify (iii), we have

$$i(a, b, c + c') = (a \otimes_R b) \otimes_S (c + c')$$

and

$$i(a, b, c) + i(a, b, c') = [(a \otimes_R b) \otimes_S c] + [(a \otimes_R b) \otimes_S c'] = (a \otimes_R b) \otimes_S (c + c')$$

which verifies (iii).

To verify (iv), we have

$$i(ar, b, c) = (ar \otimes_R b) \otimes_S c = (a \otimes_R rb) \otimes_S c = i(a, rb, c)$$

which verifies (iv).

To verify (v), we have

$$i(a, bs, c) = (a \otimes_R bs) \otimes_S c = [(a \otimes_R b)s] \otimes_S c = (a \otimes_R b) \otimes_S sc = i(a, b, sc)$$

which verifies (v). We conclude that i is a middle linear map. □

Proof. (b): Suppose that $g : A \times B \times C \to D$ is a middle linear map. Define a map

$$h : (A \otimes_R B) \times C \to D \quad \text{by} \quad ((a \otimes_R b), c) \mapsto g(a, b, c)$$

Now, note that $A \otimes_R B$ is a right S-module and that C is a left S-module. Furthermore, since g is a middle linear map in the above sense, it follows that h is a well-defined middle linear map in the usual sense. By the previous two observations and the definition of the tensor product, then, there exists a unique group homomorphism $\overline{g} : (A \otimes_R B) \otimes_S C \to D$ such that $\overline{g}((a \otimes_R b) \otimes_S c) = h((a \otimes_R b), c)$ for all $a \in A$, $b \in B$, and $c \in C$.

Finally, notice that by recalling the definition of i we have that

$$\overline{g}(i(a, b, c)) = \overline{g}((a \otimes_R b) \otimes_S c)$$

for all $a \in A$, $b \in B$, and $c \in C$. In addition, recall by the definition of h and by the above result that

$$\overline{g}((a \otimes_R b) \otimes_S c) = h((a \otimes_R b), c) = g(a, b, c)$$

for all $a \in A$, $b \in B$, and $c \in C$. Hence, combining the previous two observations gives

$$\overline{g}(i(a, b, c)) = g(a, b, c)$$

for all $a \in A$, $b \in B$, and $c \in C$ and hence $\overline{g} \circ i = g$. Furthermore, we see that $\overline{g}$ is unique in the desired sense of this part of the problem by noting the above equalities. Thus, by the above results we may conclude that there exists a unique group homomorphism $\overline{g} : (A \otimes_R B) \otimes_S C \to D$ such that $\overline{g} \circ i = g$. This completes the proof. □

Proof. (c): This result follows by arguments symmetric to those presented above that were used established Part (a) and Part (b). □

Proof. (d): Note by Part (b) and Part (c) that $((A \otimes_R B) \otimes_S C, i)$ and $(A \otimes_R (B \otimes_S C), j)$ are universal objects in the category of all middle linear maps $f : A \times B \times C \to D$, where D is an abelian group and a middle linear map is defined in the above sense. Since any two universal objects in a category are equivalent, then, it follows that there exists a group isomorphism $(A \otimes_R B) \otimes_S C \to A \otimes_R (B \otimes_S C)$ and thus we may now conclude that $(A \otimes_R B) \otimes_S C \simeq A \otimes_R (B \otimes_S C)$. This completes the proof. □

Problem 11. *Let A, B, C be modules over a commutative ring R.*

(a): *The set $\mathcal{L}(A, B; C)$ of all R-bilinear maps $A \times B \to C$ is an R-module with $(f + g)(a, b) = f(a, b) + g(a, b)$ and $(rf)(a, b) = rf(a, b)$.*

(b): *Each one of the following R-modules is isomorphic to $\mathcal{L}(A, B; C)$:*

(i): $\mathrm{Hom}_R(A \otimes_R B, C)$.

(ii): $\mathrm{Hom}_R(A, \mathrm{Hom}_R(B, C))$.

(iii): $\mathrm{Hom}_R(B, \mathrm{Hom}_R(A, C))$.

Proof. (a): We first show that $\mathcal{L}(A, B; C)$ is an abelian group under addition. Towards this end, note that since the zero map $A \times B \to C$ is clearly an R-bilinear map we have $\mathcal{L}(A, B; C) \neq \emptyset$. Next, suppose that $f, g \in \mathcal{L}(A, B; C)$. Then as $f, g \in \mathcal{L}(A, B; C)$, we have that

$$\begin{aligned}(f + g)(a_1 + a_2, b) &= f(a_1 + a_2, b) + g(a_1 + a_2, b) \\ &= [f(a_1, b) + f(a_2, b)] + [g(a_1, b) + g(a_2, b)] \\ &= [f(a_1, b) + g(a_1, b)] + [f(a_2, b) + g(a_2, b)] \\ &= (f + g)(a_1, b) + (f + g)(a_2, b)\end{aligned}$$

and

$$\begin{aligned}(f + g)(a, b_1 + b_2) &= f(a, b_1 + b_2) + g(a, b_1 + b_2) \\ &= [f(a, b_1) + f(a, b_2)] + [g(a, b_1) + g(a, b_2)] \\ &= [f(a, b_1) + g(a, b_1)] + [f(a, b_2) + g(a, b_2)] \\ &= (f + g)(a, b_1) + (f + g)(a, b_2)\end{aligned}$$

and

$$\begin{aligned}(f + g)(ra, b) &= f(ra, b) + g(ra, b) \\ &= [rf(a, b)] + [rg(a, b)] \\ &= r[f(a, b) + g(a, b)] \\ &= r(f + g)(a, b)\end{aligned}$$

and

$$\begin{aligned}(f + g)(a, rb) &= f(a, rb) + g(a, rb) \\ &= [rf(a, b)] + [rg(a, b)] \\ &= r[f(a, b) + g(a, b)] \\ &= r(f + g)(a, b)\end{aligned}$$

for all $a, a_1, a_2 \in A$, $b, b_1, b_2 \in B$, and $r \in R$. By the previous results, we may now conclude that $f + g \in \mathcal{L}(A, B; C)$ and hence $\mathcal{L}(A, B; C)$ is closed under addition.

Finally, note that an additive identity of $\mathcal{L}(A, B; C)$ is the zero map $A \times B \to C$. Furthermore, given any element $f \in \mathcal{L}(A, B; C)$ we see that the map $-f : A \times B \to C$ defined by $(-f)(a, b) = -f(a, b)$ for all $a \in A$ and $b \in B$ is an R-bilinear map since f is an R-bilinear map and is clearly an additive inverse of f. We conclude that $\mathcal{L}(A, B; C)$ is a group under addition. Lastly, it follows that $\mathcal{L}(A, B; C)$ is an abelian group under addition since C is an abelian group under addition as C is an R-module.

Next, we show that the action of R on $\mathcal{L}(A, B; C)$ defined above is indeed an action. Towards this end, suppose that $f \in \mathcal{L}(A, B; C)$. Then as $f \in \mathcal{L}(A, B; C)$ and as R is commutative, we have that

$$\begin{aligned}(rf)(a_1 + a_2, b) &= r[f(a_1 + a_2, b)] \\ &= r[f(a_1, b) + f(a_2, b)] \\ &= r[f(a_1, b)] + r[f(a_2, b)] \\ &= (rf)(a_1, b) + (rf)(a_2, b)\end{aligned}$$

and

$$\begin{aligned}(rf)(a, b_1 + b_2) &= r[f(a, b_1 + b_2)] \\ &= r[f(a, b_1) + f(a, b_2)] \\ &= r[f(a, b_1)] + r[f(a, b_2)] \\ &= (rf)(a, b_1) + (rf)(a, b_2)\end{aligned}$$

and

$$\begin{aligned}(rf)(sa, b) &= r[f(sa, b)] \\ &= r[s[f(a, b)]] \\ &= (rs)[f(a, b)] \\ &= (sr)[f(a, b)] \\ &= s[r[f(a, b)]] \\ &= s(rf)(a, b)\end{aligned}$$

and

$$\begin{aligned}(rf)(a, sb) &= r[f(a, sb)] \\ &= r[s[f(a, b)]] \\ &= (rs)f(a, b) \\ &= (sr)f(a, b) \\ &= s[r[f(a, b)]] \\ &= s(rf)(a, b)\end{aligned}$$

for all $a, a_1, a_2 \in A$, $b, b_1, b_2 \in B$, and $r, s \in R$. By the previous results, we may now conclude that $rf \in \mathcal{L}(A, B; C)$ and hence we do have a left action of R on $\mathcal{L}(A, B; C)$.

Finally, we show that this left action of R on $\mathcal{L}(A, B; C)$ satisfies the three module axioms. First, let $r \in R$ and $f, g \in \mathcal{L}(A, B; C)$. Then

$$\begin{aligned}[r(f + g)]\,(a, b) &= r[(f + g)(a, b)] \\ &= r[f(a, b) + g(a, b)] \\ &= r[f(a, b)] + r[g(a, b)] \\ &= (rf)(a, b) + (rg)(a, b) \\ &= (rf + rg)(a, b)\end{aligned}$$

for all $a \in A$ and $b \in B$ so that $r(f+g) = rf+rg$. Next, let $r, s \in R$ and $f \in \mathcal{L}(A, B; C)$. Then if $z = r + s \in R$ we have

$$\begin{aligned}
[(r+s)f]\,(a,b) &= (zf)(a,b) \\
&= z[f(a,b)] \\
&= (r+s)[f(a,b)] \\
&= r[f(a,b)] + s[f(a,b)] \\
&= (rf)(a,b) + (sf)(a,b) \\
&= (rf+sf)(a,b)
\end{aligned}$$

for all $a \in A$ and $b \in B$ so that $(r+s)f = rf+sf$. Next, let $r, s \in R$ and $f \in \mathcal{L}(A, B; C)$. Then if $g = sf$, we have $g \in \mathcal{L}(A, B; C)$ and

$$\begin{aligned}
[r(sf)]\,(a,b) &= (rg)(a,b) \\
&= r[g(a,b)] \\
&= r[(sf)(a,b)] \\
&= r[s[f(a,b)]] \\
&= (rs)[f(a,b)] \\
&= [(rs)f](a,b)
\end{aligned}$$

for all $a \in A$ and $b \in B$ so that $r(sf) = (rs)f$. The previous results show that $\mathcal{L}(A, B; C)$ is an R-module, completing the proof. □

Proof. (b, (i)): Let $g : A \times B \to A \otimes_R B$ be the tensor product of A and B and define

$$\psi : \mathrm{Hom}_R(A \otimes_R B, C) \to \mathcal{L}(A, B; C) \quad \text{by} \quad f \mapsto f \circ g$$

It is easily verified that ψ is actually a map. Next, we show that ψ is an R-module homomorphism. Towards this end, let $f_1, f_2 \in \mathrm{Hom}_R(A \otimes_R B, C)$. Then

$$\begin{aligned}
[\psi(f_1+f_2)]\,(a,b) &= [(f_1+f_2) \circ g](a,b) \\
&= (f_1+f_2)(g(a,b)) \\
&= f_1(g(a,b)) + f_2(g(a,b)) \\
&= (f_1 \circ g)(a,b) + (f_2 \circ g)(a,b) \\
&= [\psi(f_1)](a,b) + [\psi(f_2)](a,b) \\
&= [\psi(f_1) + \psi(f_2)](a,b)
\end{aligned}$$

for all $a \in A$ and $b \in B$ so that $\psi(f_1+f_2) = \psi(f_1) + \psi(f_2)$. Furthermore, let $r \in R$ and $f \in \mathrm{Hom}_R(A \otimes_R B, C)$. Then

$$[\psi(rf)](a,b) = [(rf) \circ g](a,b) = (rf)(g(a,b)) = r[f(g(a,b))]$$

and

$$[r\psi(f)](a,b) = r[[\psi(f)](a,b)] = r[(f \circ g)(a,b)] = r[f(g(a,b))]$$

for all $a \in A$ and $b \in B$ so that $\psi(rf) = r\psi(f)$. The previous two results show that ψ is an R-module homomorphism.

Next, we show that ψ is injective. Towards this end, suppose that $f \in \ker \psi$ so that $\psi(f) : A \times B \to C$ is the zero map. Let $a \in A$ and $b \in B$. Then by the definition of ψ, we obtain

$$f(a \otimes_R b) = f(g(a, b)) = [\psi(f)](a, b) = 0$$

It now follows by the above equality that $f : A \otimes_R B \to C$ is the zero map and hence $\ker \psi$ is trivial so that ψ is an injection.

Finally, we show that ψ is surjective. Towards this end, suppose that $\phi \in \mathcal{L}(A, B; C)$. In particular, we have that $\phi : A \times B \to C$ is a middle linear map and hence by the definition of the tensor product there is a (unique) group homomorphism $\overline{\phi} : A \otimes_R B \to C$ such that $\overline{\phi} \circ g = \phi$. Furthermore, since $\overline{\phi} \circ g = \phi$ and as $\phi \in \mathcal{L}(A, B; C)$ we have

$$\begin{aligned}
\overline{\phi}(r(a \otimes_R b)) &= \overline{\phi}(r(g(a, b))) \\
&= \overline{\phi}(g(ra, b)) \\
&= \phi(ra, b) \\
&= r[\phi(a, b)] \\
&= r[\overline{\phi}(g(a, b))] \\
&= r[\overline{\phi}(a \otimes_R b)]
\end{aligned}$$

for all $a \in A$, $b \in B$, and $r \in R$. In particular, it now follows by the above equality together with the fact that $\overline{\phi}$ is a group homomorphism shows that $\overline{\phi} : A \otimes_R B \to C$ is an R-module homomorphism and hence $\overline{\phi} \in \mathrm{Hom}_R(A \otimes_R B, C)$. Thus, we may apply ψ to $\overline{\phi}$ to obtain by the above results that

$$\psi(\overline{\phi}) = \overline{\phi} \circ g = \phi$$

and hence ψ is surjective. The previous results prove that ψ is an R-module isomorphism so that $\mathrm{Hom}_R(A \otimes_R B, C) \simeq \mathcal{L}(A, B; C)$. This completes the proof. $\square$

Proof. (b, (ii)): Define

$$\psi : \mathrm{Hom}_R(A, \mathrm{Hom}_R(B, C)) \to \mathcal{L}(A, B; C) \quad \text{by} \quad \psi(f) : A \times B \to C$$

where

$$\psi(f) : A \times B \to C \quad \text{by} \quad (a, b) \mapsto [f(a)](b)$$

It is easily verified that ψ is actually a map. Next, we show that ψ is an R-module homomorphism. Towards this end, let $f_1, f_2 \in \mathrm{Hom}_R(A, \mathrm{Hom}_R(B, C))$. Then

$$\begin{aligned}
[\psi(f_1 + f_2)]\,(a, b) &= [(f_1 + f_2)(a)](b) \\
&= [f_1(a) + f_2(a)](b) \\
&= [f_1(a)](b) + [f_2(a)](b) \\
&= [\psi(f_1)](a, b) + [\psi(f_2)](a, b) \\
&= [\psi(f_1) + \psi(f_2)](a, b)
\end{aligned}$$

for all $a \in A$ and $b \in B$ so that $\psi(f_1 + f_2) = \psi(f_1) + \psi(f_2)$. Furthermore, let $r \in R$ and $f \in \mathrm{Hom}_R(A, \mathrm{Hom}_R(B, C))$. Then

$$[\psi(rf)]\,(a, b) = [(rf)(a)](b) = [r[f(a)]](b) = r[[f(a)](b)]$$

and

$$[r\psi(f)](a, b) = r[[\psi(f)](a, b)] = r[[f(a)](b)]$$

for all $a \in A$ and $b \in B$ so that $\psi(rf) = r\psi(f)$. The previous two results show that ψ is an R-module homomorphism.

Next, we show that ψ is injective. Towards this end, suppose that $f \in \ker \psi$ so that $\psi(f) : A \times B \to C$ is the zero map. Let $a \in A$ and $b \in B$. Then by the definition of ψ, we obtain

$$[f(a)](b) = [\psi(f)](a, b) = 0$$

Since $b \in B$ was arbitrary, this shows that $f(a) : B \to C$ is the zero map. Since $a \in A$ was arbitrary, we may now conclude that $f : A \to \mathrm{Hom}_R(B, C)$ is the zero map. We conclude that $\ker \psi$ is trivial and hence ψ is an injection.

Finally, we show that ψ is surjective. Towards this end, suppose that $\phi \in \mathcal{L}(A, B; C)$. Define a map

$$f : A \to \mathrm{Hom}_R(B, C) \quad \text{by} \quad f(a) : A \to \mathrm{Hom}_R(B, C)$$

where

$$f(a) : B \to C \quad \text{by} \quad b \mapsto \phi(a, b)$$

We will show that $f \in \mathrm{Hom}_R(A, \mathrm{Hom}_R(B, C))$. First, we show that f maps A into $\mathrm{Hom}_R(B, C)$. Towards this end, let $a \in A$, $b_1, b_2 \in B$, and $r \in R$. Then

$$\begin{aligned}
[f(a)]\,(rb_1 + b_2) &= \phi(a, rb_1 + b_2) \\
&= \phi(a, rb_1) + \phi(a, b_2) \\
&= r[\phi(a, b_1)] + \phi(a, b_2) \\
&= r[[f(a)](b_1)] + [f(a)](b_2)
\end{aligned}$$

and hence $f(a) \in \mathrm{Hom}_R(B, C)$ so that f does indeed map A into $\mathrm{Hom}_R(B, C)$.

Next, we show that f is an R-module homomorphism. Indeed, notice that

$$\begin{aligned}
[f(ra_1 + a_2)]\,(b) &= \phi(ra_1 + a_2, b) \\
&= \phi(ra_1, b) + \phi(a_2, b) \\
&= r[\phi(a_1, b)] + \phi(a_2, b) \\
&= r[[f(a_1)](b)] + [f(a_2)](b)
\end{aligned}$$

and

$$[rf(a_1) + f(a_2)](b) = [rf(a_1)](b) + [f(a_2)](b) = r[[f(a_1)](b)] + [f(a_2)](b)$$

for all $a_1, a_2 \in A$, $b \in B$, and $r \in R$ so that $f(ra_1 + a_2) = rf(a_1) + f(a_2)$. Hence, we see that f is an R-module homomorphism so that $f \in \mathrm{Hom}_R(A, \mathrm{Hom}_R(B, C))$.

Finally, note that since $f \in \mathrm{Hom}_R(A, \mathrm{Hom}_R(B, C))$ we can apply ψ to f to obtain

$$[\psi(f)](a, b) = f(a)(b) = \phi(a, b)$$

for all $a \in A$ and $b \in B$ so that $\psi(f) = \phi$. We conclude that ψ is surjective. The previous results prove that ψ is an R-module isomorphism so that $\mathrm{Hom}_R(A, \mathrm{Hom}_R(B, C)) \simeq \mathcal{L}(A, B; C)$. This completes the proof. $\square$

Proof. (b, (iii)): Define

$$\psi : \mathrm{Hom}_R(B, \mathrm{Hom}_R(A, C)) \to \mathcal{L}(A, B; C) \quad \text{by} \quad \psi(f) : A \times B \to C$$

where

$$\psi(f) : A \times B \to C \quad \text{by} \quad (a, b) \mapsto [f(b)](a)$$

By arguments symmetric to those presented in the proof of Part (b, (ii)), it follows that ψ is an R-module isomorphism so that $\mathrm{Hom}_R(B, \mathrm{Hom}_R(A, C)) \simeq \mathcal{L}(A, B; C)$. This completes the proof. $\square$

Homework 13: Page 394 #3, 5, 6A.

Problem 3. *Let R be a Noetherian local ring with maximal ideal M. If the ideal M/M^2 in R/M^2 is generated by $\{a_1 + M^2, \dots, a_n + M^2\}$, then the ideal M is generated in R by $\{a_1, \dots, a_n\}$.*

Proof. First, note that as $\{a_1 + M^2, \dots, a_n + M^2\} \subseteq M/M^2$ we have $a_1, \dots, a_n \in M$. Let $A = \{a_1, \dots, a_n\}$ so that $A \subseteq M$ and let J be the ideal of R generated by A. Since $A \subseteq M$ and as M is an ideal, we have $J \subseteq M$.

Now, we claim that $J + M^2 = M + M^2$. Indeed, first note that since $J \subseteq M$ we see $J + M^2 \subseteq M + M^2$. On the other hand, suppose that $m + a \in M + M^2$ and consider the element $m + M^2 \in M/M^2$. Since M/M^2 in R/M^2 is generated by the set $\{a_1 + M^2, \dots, a_n + M^2\}$, it follows that there are elements $r_1 + M^2, \dots, r_n + M^2 \in R/M^2$ such that

$$\begin{aligned} m + M^2 &= (r_1 + M^2)(a_1 + M^2) + \cdots + (r_n + M^2)(a_n + M^2) \\ &= (r_1 a_1 + M^2) + \cdots + (r_n a_n + M^2) \\ &= (r_1 a_1 + \cdots + r_n a_n) + M^2 \end{aligned}$$

and hence $m = r_1 a_1 + \cdots + r_n a_n + b$ for some $b \in M^2$. Now, since J is the ideal of R generated by $A = \{a_1, \dots, a_n\}$ we have that $r_1 a_1 + \cdots + r_n a_n \in J$. Thus, we obtain since $b + a \in M^2$ as $b, a \in M^2$ and M^2 is an ideal that

$$m + a = (r_1 a_1 + \cdots + r_n a_n + b) + a = (r_1 a_1 + \cdots + r_n a_n) + (b + a) \in J + M^2$$

We conclude that $J + M^2 = M + M^2$.

Next, we show that $(J + M^2)/J = M(M/J)$. Towards this end, first let $(j + a) + J \in (J + M^2)/J$. Then since $j \in J$, this gives

$$(j + a) + J = a + j + J = a + J$$

Furthermore, since $a \in M^2$ it follows that there are elements $m_1, m_1', \dots, m_k, m_k' \in M$ such that $a = m_1 m_1' + \cdots + m_k m_k'$ and thus

$$\begin{aligned} (j + a) + J &= a + J \\ &= (m_1 m_1' + \cdots + m_k m_k') + J \\ &= (m_1 m_1' + J) + \cdots + (m_k m_k' + J) \\ &= m_1(m_1' + J) + \cdots + m_k(m_k' + J) \\ &\in M(M/J) \end{aligned}$$

On the other hand, suppose that

$$m_1(m_1' + J) + \cdots + m_k(m_k' + J) \in M(M/J)$$

Then

$$\begin{aligned} m_1(m_1' + J) + \cdots + m_k(m_k' + J) &= (m_1 m_1' + J) + \cdots + (m_k m_k' + J) \\ &= (m_1 m_1' + \cdots + m_k m_k') + J \\ &= (0 + (m_1 m_1' + \cdots m_k m_k')) + J \\ &\in (J + M^2)/J \end{aligned}$$

since clearly $0 \in J$ and $m_1 m_1' + \cdots + m_k m_k' \in M^2$. We conclude $(J + M^2)/J = M(M/J)$.

Next, notice that since clearly $M^2 \subseteq M$ we have $M + M^2 = M$. By the previous results, then, we obtain

$$M\left(\frac{M}{J}\right) = \frac{J + M^2}{J} = \frac{M + M^2}{J} = \frac{M}{J}$$

Furthermore, suppose that $m \in M$. If $1 - m$ is not a unit of R, it follows that the ideal $(1 - m)$ is contained in some maximal ideal of R. But since M is the unique maximal ideal of R, we have that $1 - m \in (1 - m) \subseteq M$ so that $1 \in M$ as $m \in M$. However, this implies that $M = R$ which contradicts the fact that M is a maximal ideal of R. We conclude that $1 - m$ is a unit of R for each $m \in M$.

Finally, notice that since R is Noetherian and as M is an ideal of R we have that M is finitely generated. By this observation, it follows that M/J is finitely generated as an R-module. By the above results, we may appeal to Nakayama's Lemma to assert that $M/J = 0$ and hence $M = J$. Since $J = (A) = (a_1, \ldots, a_n)$, this equality implies that the ideal M is generated by $A = \{a_1, \ldots, a_n\}$ in R. This completes the proof. $\square$

Problem 5. *Let R be a commutative ring with identity and J an ideal that is contained in every maximal ideal of R. Let A be a finitely generated R-module and $f : C \to A$ an R-module homomorphism. Then f induces a homomorphism $\overline{f} : C/JC \to A/JA$ in the usual way. Show that if $\overline{f}$ is an epimorphism, then f is an epimorphism.*

Proof. First, we establish the existence of the map $\overline{f}$ described in the statement of this problem. Towards this end, we begin by proving that $f(JC) \subseteq JA$. Indeed, let $j_1c_1 + \cdots + j_nc_n \in JC$. Then since $f : C \to A$ is an R-module homomorphism, we have

$$f(j_1c_1 + \cdots + j_nc_n) = f(j_1c_1) + \cdots + f(j_nc_n) = j_1f(c_1) + \cdots + j_nf(c_n) \in JA$$

This result shows that $f(JC) \subseteq JA$. In particular, we now have that $JC \subseteq f^{-1}(JA)$.

Now, let $\pi : A \to A/JA$ denote the canonical projection map and consider the map $\pi \circ f : C \to A/JA$. We claim that $f^{-1}(JA) = \ker(\pi \circ f)$. Indeed, first let $x \in f^{-1}(JA)$. Then there is some element $z \in JA$ such that $f(x) = z$ and hence

$$(\pi \circ f)(x) = \pi(f(x)) = \pi(z) = z + JA = JA$$

The above equality shows that $x \in \ker(\pi \circ f)$. On the other hand, suppose that $x \in \ker(\pi \circ f)$. In this case, then, we have

$$JA = (\pi \circ f)(x) = \pi(f(x)) = f(x) + JA$$

so that $f(x) \in JA$ and hence $x \in f^{-1}(JA)$. We conclude that $f^{-1}(JA) = \ker(\pi \circ f)$ so that by our previous result, we now have $JC \subseteq f^{-1}(JA) = \ker(\pi \circ f)$. This observation implies that there exists a (unique) group homomorphism $\overline{f} : C/JC \to A/JA$ where

$$\overline{f}(c + JC) = (\pi \circ f)(c) \quad \text{for each} \quad c + JC \in C/JC$$

Thus, if $c + JC \in C/CJ$ we see that

$$\overline{f}(c + JC) = (\pi \circ f)(c) = \pi(f(c)) = f(c) + JA$$

Therefore, we have that $\overline{f} : C/JC \to A/JA$ is defined by

$$\overline{f}(c + JC) = f(c) + JA \quad \text{for each} \quad c + JC \in C/JC$$

We now prove the main result.

Towards this end, suppose that the group homomorphism $\overline{f} : C/JC \to A/JA$ is an epimorphism. We must show that $f : C \to A$ is an epimorphism. Since f is an R-module homomorphism, it remains to prove that f is a surjection. In order to prove this, notice that it suffices to show that $f(C) = A$. Now, by the definition of $\overline{f}$ and since $\overline{f}$ is surjective we have the equalities

$$A/JA = \overline{f}(C/JC) = f(C)/JA$$

We will use this observation below.

We claim that $A = f(C) + JA$. Indeed, first suppose that $a \in A$. Then by our above result, we have $a + JA \in A/JA = f(C)/JA$ and hence there is some $c \in C$ such that $a + JA = f(c) + JA$. This implies that $a = f(c) + z$ for some element $z \in JA$. Thus, we obtain

$$a = f(c) + z \in f(C) + JA$$

On the other hand, suppose that $f(c) + z \in f(C) + JA$. Then by our above result, we have since $z \in JA$ that

$$(f(c) + z) + JA = f(c) + JA \in f(C)/JA = A/JA$$

and hence there is some $a \in A$ such that

$$(f(c) + z) + JA = a + JA$$

But since $z \in JA$, we now have

$$f(c) + JA = (f(c) + z) + JA = a + JA$$

and hence there is some $w \in JA$ with $f(c) = a + w$. But recall that A is an R-module and since $J \subseteq R$, we now observe that $z, w \in A$. Thus, since we also have $a \in A$ we see

$$f(c) + z = (a + w) + z \in A$$

The previous results show that $A = f(C) + JA$.

To complete the proof, recall that R is a commutative ring with identity, that J is an ideal that is contained in every maximal ideal of R, and that A is a finitely generated R-module. Furthermore, since $f : C \to A$ is an R-module homomorphism, it follows that $f(C)$ is an R-submodule of A. Thus, by the previous observations and since $A = f(C) + JA$ we may appeal to Nakayama's Lemma to assert that $A = f(C)$. Therefore, the map $f : C \to A$ is a surjection and hence f is an epimorphism. This completes the proof. $\square$

Problem 6. (a): *Let R be a commutative ring with identity. If every ideal of R can be generated by a finite or denumerable subset, then the same is true of $R[x]$.*

Note. In this problem, we intend "countable" to mean countably infinite and *not* finite.

Proof. Let I be an ideal of $R[x]$. Similarly as in the proof of Hilbert's Basis Theorem, define for each integer $n \geq 0$ the set

$$I_n = \{r \in R : r \text{ is the leading coefficient of some } f(x) \in I \text{ with } \deg(f(x)) = n\} \cup \{0\}$$

Then we know that I_n is an ideal of R for each integer $n \geq 0$ by the proof of Hilbert's Basis Theorem.

Now, fix any integer $i \geq 0$. Since I_i is an ideal of R, we have by hypothesis that I_i is either finitely generated or countably generated. First, suppose that I_i is finitely generated. Then there are elements $r_{i,1}, \dots, r_{i,\alpha_i} \in R$ with $r_{i,j} \neq 0$ such that $I_i = (r_{i,1}, \dots, r_{i,\alpha_i})$ and polynomials $f_{i,1}(x), \dots, f_{i,\alpha_i}(x) \in I$ such that $\deg(f_{i,j}(x)) = i$ and the leading coefficient of $f_{i,j}(x)$ is $r_{i,j}$ for each $j \in \{1, \dots, \alpha_i\}$. Secondly, suppose that I_i is countably generated. Then there are elements $r_{i,1}, r_{i,2}, \dots \in R$ with $r_{i,j} \neq 0$ such that $I_i = (r_{i,1}, r_{i,2}, \dots)$ and polynomials $f_{i,1}(x), f_{i,2}(x), \dots \in I$ such that $\deg(f_{i,j}(x)) = i$ and the leading coefficient of $f_{i,j}(x)$ is $r_{i,j}$ for each $j \in \{1, 2, \dots\}$.

Next, define the sets

$$F = \{i \in \{0, 1, \dots\} : I_i \text{ is finitely generated}\}$$

and

$$C = \{i \in \{0, 1, \dots\} : I_i \text{ is countably generated}\}$$

and

$$A = \{f_{i,j}(x) : i \in F, j \in \{1, \dots, \alpha_i\}\} \quad B = \{f_{i,j}(x) : i \in C, j \in \{1, 2, \dots\}\}$$

Clearly, we see that $F \cup C = \{0, 1, \dots\}$ and that $F \cap C = \emptyset$. Furthermore, it is immediate that $A \cup B$ is either a finite or countable subset of $I \subseteq R[x]$. Now, let J be the ideal of $R[x]$ generated by $A \cup B$. Since we have $A \cup B \subseteq I$ and I is an ideal, we have that $J \subseteq I$. For the sake of contradiction, suppose that $I \neq J$. In this case, there is a polynomial $g(x) \in I - J$ which can be chosen to be of smallest possible degree among all of the polynomials in $I - J$. For definiteness, let $\deg(g(x)) = n$ and let a be the leading coefficient of $g(x)$ so that $a \in I_n$ by definition.

First, suppose that $n \in F$. In this case, we have $I_n = (r_{n,1}, \dots, r_{n,\alpha_n})$. Therefore, since $a \in I_n$ there exist elements $s_1, \dots, s_{\alpha_n} \in R$ such that $a = s_1 r_{n,1} + \cdots + s_{\alpha_n} r_{n,\alpha_n}$. Now, consider the polynomial

$$h(x) = s_1 f_{n,1}(x) + \cdots + s_{\alpha_n} f_{n,\alpha_n}(x)$$

Notice that $\deg(f_{n,1}(x)), \dots, \deg(f_{n,\alpha_n}(x)) = n$ and that the leading coefficient of $h(x)$ is a. These observations imply that $\deg(h(x)) = n$. Also, we see that $h(x) \in J$ since J is an ideal of $R[x]$ and $f_{n,1}(x), \dots, f_{n,\alpha_n}(x) \in A \subseteq J$. Therefore, we see that since $g(x)$ is a polynomial of degree n with leading coefficient a and as I is an ideal with $g(x) \in I$ and $h(x) \in J \subseteq I$ that $g(x) - h(x)$ is a polynomial in I of degree at most $n - 1$. By

the minimality of n, then, we conclude that $g(x) - h(x) \in J$. But since $h(x) \in J$, this implies that $g(x) \in J$ since J is an ideal which is a contradiction.

The above result now forces $n \in C$. In this case, we have $a \in I_n = (r_{n,1}, r_{n,2}, \dots)$ and hence there is some finite subset $\{r_{n,n_1}, \dots, r_{n,n_k}\} \subseteq \{r_{n,1}, r_{n,2}, \dots\}$ and elements $s_{n_1}, \dots, s_{n_k} \in R$ such that $a = s_{n_1} r_{n,n_1} + \cdots + s_{n_k} r_{n,n_k}$. Now, consider the polynomial

$$h(x) = s_{n_1} f_{n,n_1}(x) + \cdots + s_{n_k} f_{n,n_k}(x)$$

Notice that $\deg(f_{n,n_1}(x)), \dots, \deg(f_{n,n_k}(x)) = n$ and that the leading coefficient of $h(x)$ is a. These observations imply that $\deg(h(x)) = n$. Also, we see that $h(x) \in J$ since J is an ideal of $R[x]$ and $f_{n,n_1}(x), \dots, f_{n,n_k}(x) \in B \subseteq J$. Therefore, we see that since $g(x)$ is a polynomial of degree n with leading coefficient a and as I is an ideal with $g(x) \in I$ and $h(x) \in J \subseteq I$ that $g(x) - h(x)$ is a polynomial in I of degree at most $n - 1$. By the minimality of n, then, we conclude that $g(x) - h(x) \in J$. But since $h(x) \in J$, this implies that $g(x) \in J$ since J is an ideal which is a contradiction.

In any case, we obtain a contradiction by assuming that $I \neq J$. Therefore, we conclude that $I = J = (A \cup B)$ and since $A \cup B$ is either finite or countable we conclude that I is either finitely or countably generated. As I was an arbitrary ideal of $R[x]$, this completes the proof. $\square$

Homework 14: Page 400 #1, 2, 3

Problem 1. *Let S be an integral extension ring of R and suppose R and S are integral domains. Then S is a field if and only if R is a field.*

Proof. For the first direction, assume that S is a field. Since R is an integral domain, it remains to prove that every nonzero element of R has a multiplicative inverse in R. Towards this end, let $r \in R$ be a nonzero element of R. Since $r \in R \subseteq S$ and as S is a field, it follows that $r^{-1} \in S$. Furthermore, since S is an integral extension of R and $r^{-1} \in S$ it follows that there is a monic polynomial $f(x) \in R[x]$ such that $f(r^{-1}) = 0$. For definiteness, write

$$f(x) = x^n + c_{n-1}x^{n-1} + \cdots + c_1 x + c_0 \in R[x]$$

so that

$$\begin{aligned} 0 &= f(r^{-1}) \\ &= (r^{-1})^n + c_{n-1}(r^{-1})^{n-1} + \cdots + c_1(r^{-1}) + c_0 \\ &= r^{-n} + c_{n-1}r^{-n+1} + \cdots + c_1 r^{-1} + c_0 \end{aligned}$$

Multiplying both sides of this equality by r^{n-1}, we obtain

$$0 = r^{-1} + c_{n-1} + \cdots + c_1 r^{n-2} + c_0 r^{n-1}$$

so that

$$r^{-1} = -(c_{n-1} + \cdots + c_1 r^{n-2} + c_0 r^{n-1})$$

Now, notice that since R is a ring that each of the summands on the right-hand side of the above equality is in R. By this observation and again appealing to the fact that R is a ring, we see that the right-hand side of the above equality is in R so that $r^{-1} \in R$. This shows that R is a field, completing the proof of the first direction.

For the second direction, assume that R is a field. Since S is an integral domain, it remains to prove that every nonzero element of S has a multiplicative inverse in S. Towards this end, let $s \in S$ be a nonzero element of S. Since S is an integral extension of R and as $s \in S$, it follows that $R[s]$ is finitely generated as an R-module and since R is a field this implies that $R[s]$ is a finite-dimensional vector space over R. Now, consider the map

$$f : R[s] \to R[s] \quad \text{by} \quad z \mapsto sz$$

Clearly, we see that f is well-defined. We claim that f is an R-linear transformation. Indeed, suppose that $z_1, z_2 \in R[s]$ and $r \in R$. Then since $r \in R \subseteq S$ and $s \in S$ and as S is commutative, we obtain

$$\begin{aligned} f(rz_1 + z_2) &= s(rz_1 + z_2) \\ &= s(rz_1) + sz_2 \\ &= (sr)z_1 + sz_2 \\ &= (rs)z_1 + sz_2 \\ &= r(sz_1) + sz_2 \\ &= rf(z_1) + f(z_2) \end{aligned}$$

which shows that f is an R-linear transformation.

We claim that f is an injection. Since f is an R-linear transformation, it suffices to show that $\ker f$ is trivial to establish that f is an injection. Towards this end, let $z \in \ker f$. Then $0 = f(z) = sz$. Now, recall that S is an integral domain, that s is a nonzero element of S, and that $z \in \ker f \subseteq R[s] \subseteq S$. By these observations and the previous equality, then, we see that $z = 0$ so that $\ker f$ is trivial. We may now conclude that f is an injection.

Finally, note that since f is an injective R-linear transformation on the finite-dimensional R-vector space $R[s]$ and as any injective linear transformation on a finite-dimensional vector space is surjective we conclude that f is a surjection. Therefore, as $1 \in R \subseteq R[s]$ it follows that there is some element $z \in R[s] \subseteq S$ such that

$$1 = f(z) = zs$$

By the above equality, we conclude that $s^{-1} = z \in S$ and hence S is a field. This completes the proof of the second direction. $\square$

Problem 2. *Let R be an integral domain. If the quotient field F of R is integral over R, then R is a field.*

Proof. Since F is a field, it is immediate that F is an integral domain. Furthermore, since F is integral over R we have that F is an integral extension ring of R. These observations show that the hypotheses of the previous problem are satisfied. Therefore, since F is a field we may conclude by the previous problem that R is also a field. $\square$

Problem 3. *Let R be an integral domain with quotient field F. If $0 \neq a \in R$ and $1/a \in F$ is integral over R, then a is a unit of R.*

Proof. Since $1/a \in F$ is integral over R, there is a monic polynomial $f(x) \in R[x]$ such that $f(1/a) = 0$. For definiteness, write

$$f(x) = x^n + c_{n-1}x^{n-1} + \cdots + c_1 x + c_0 \in R[x]$$

so that

$$\begin{aligned} 0 &= f\left(\frac{1}{a}\right) \\ &= \left(\frac{1}{a}\right)^n + c_{n-1}\left(\frac{1}{a}\right)^{n-1} + \cdots + c_1\left(\frac{1}{a}\right) + c_0 \\ &= \frac{1}{a^n} + c_{n-1}\frac{1}{a^{n-1}} + \cdots + c_1\frac{1}{a} + c_0 \end{aligned}$$

Multiplying both sides of the above equality by a^n, we obtain

$$0 = 1 + c_{n-1}a + \cdots + c_1 a^{n-1} + c_0 a^n$$

so that

$$1 = -c_{n-1}a - \cdots - c_1 a^{n-1} - c_0 a^n = a(-c_{n-1} - \cdots - c_1 a^{n-2} - c_0 a^{n-1})$$

Now, notice that since R is a ring that each of the summands on the right-hand side of the above equality is in R. By this observation and appealing to the fact that R is a ring, we see that the term in parentheses on the right-hand side of the above equality is in R. Finally, note by the above equality and by the previous observation we have

$$a^{-1} = -c_{n-1} - \cdots - c_1 a^{n-2} - c_0 a^{n-1} \in R$$

so that a is a unit of R. This completes the proof. $\square$

Homework 15: Page 400 #6, 8, 10

Problem 6. *If S is an integral extension of R, then $S[x_1, \ldots, x_n]$ is an integral extension ring of $R[x_1, \ldots, x_n]$.*

Proof. Recall that the subring of $S[x_1, \ldots, x_n]$ generated by the elements of $S[x_1, \ldots, x_n]$ which are integral over $R[x_1, \ldots, x_n]$ is an integral extension of $R[x_1, \ldots, x_n]$. Now, since S is integral over R we see that S is clearly integral over $R[x_1, \ldots, x_n]$. In addition, it is immediate that $x_1, \ldots, x_n$ are integral over $R[x_1, \ldots, x_n]$ since $x_1, \ldots, x_n \in R[x_1, \ldots, x_n]$. By our previous observation, then, this shows that the subring of $S[x_1, \ldots, x_n]$ generated by S and $x_1, \ldots, x_n$ is integral over $R[x_1, \ldots, x_n]$. But notice that the subring of $S[x_1, \ldots, x_n]$ generated by S and $x_1, \ldots, x_n$ is simply $S[x_1, \ldots, x_n]$ so that $S[x_1, \ldots, x_n]$ is integral over $R[x_1, \ldots, x_n]$. This completes the proof. $\square$

Problem 8. *Every UFD is integrally closed.*

Proof. Let R be a UFD with field of fractions F and suppose that $\alpha \in F$ is integral over R. Since $\alpha \in F$ and as R is a UFD, it follows that we can write $\alpha = a/b$ for some $a, b \in R$ where no irreducible element of R divides both a and b. Furthermore, since α is integral over R there is some monic polynomial $f(x) \in R[x]$ such that $f(\alpha) = 0$. For definiteness, write

$$f(x) = x^n + r_{n-1}x^{n-1} + \cdots + r_0$$

so that

$$0 = f(\alpha) = f\left(\frac{a}{b}\right) = \left(\frac{a}{b}\right)^n + r_{n-1}\left(\frac{a}{b}\right)^{n-1} + \cdots + r_0 = \frac{a^n}{b^n} + r_{n-1}\frac{a^{n-1}}{b^{n-1}} + \cdots + r_0$$

Multiplying both sides of this equality by b^n, we obtain

$$0 = a^n + r_{n-1}a^{n-1}b + \cdots + r_0 b^n$$

so that

$$a^n = b(-r_{n-1}a^{n-1} - \cdots - r_0 b^{n-1})$$

Now, as the term in the parenthesis on the right-hand side of the above equality is clearly in R it now follows that b divides a^n in R.

Next, suppose for the sake of contradiction that there were some irreducible element $d \in R$ such that d divides b. Since irreducible elements in a UFD are prime, it follows that d is a prime element of R. Furthermore, since d divides b and b divides a^n it follows that d divides a^n. Thus, since d is a prime element of R we see that d also divides a as d divides a^n. We now see that d divides both a and b. But as $d \in R$ is irreducible, this contradicts the fact that no irreducible element of R divides both a and b.

Finally, notice by the above contradiction that no irreducible element of R divides $b \in R$ so that b must be either 0 or a unit of R since R is a UFD. However, we know that $b \neq 0$ since the set of denominators in the field of fractions of an integral domain does not include 0. Therefore, we see that b is a unit of R and hence b^{-1} exists in R. This gives since $a \in R$ that

$$\alpha = \frac{a}{b} = ab^{-1} \in R$$

In particular, the above result shows that any element of F which is integral over R is in R so that R is integrally closed. This completes the proof. $\square$

Problem 10. *Let S be a ring extension of R.*

(a): *If $I \neq S$ is an ideal of S, then $I \cap R \neq R$ and $I \cap R$ is an ideal of R.*

(b): *If Q is a prime ideal of S, then $Q \cap R$ is a prime ideal of R.*

Proof. (a): Since $I \neq S$ is an ideal of S, it follows the that $1_S \notin I$ so that, clearly, we have $1_S \notin I \cap R$. On the other hand, since S is an extension ring of R we know that $1_S \in R$. Combining the previous two observations, we conclude that $I \cap R \neq R$.

Next, we show that $I \cap R$ is an ideal of R. Towards this end, note that since R is a subring of S we have in particular that R is a subgroup of S under addition so that R and S share the same additive identity 0. Therefore, since I is an ideal of S we have that $0 \in I \cap R$ so that $I \cap R \neq \emptyset$. Next, let $r_1, r_2 \in I \cap R$. Since $r_1, r_2 \in I$ and as I is an ideal we have $r_1 - r_2 \in I$ and as $r_1, r_2 \in R$ and R is a ring we have $r_1 - r_2 \in R$. Thus, we obtain $r_1 - r_2 \in I \cap R$ so that $I \cap R$ is a subgroup of R under addition.

Finally, let $i \in I \cap R$ and $r \in R$. Then we have $r \in R \subseteq S$ and since I is an ideal of S with $i \in I$, we see $ri \in I$. Furthermore, since R is a ring and $r, i \in R$ we have $ri \in R$. Combining the previous results, we see $ri \in I \cap R$. This completes the proof that $I \cap R$ is an ideal of R. $\square$

Proof. (b): Since Q is a prime ideal of S, we have in particular that $Q \neq S$ so that by Part (a) we see $Q \cap R \neq R$. Again appealing to Part (a), we also see that $Q \cap R$ is an ideal of R since Q is an ideal of R. Finally, suppose that $a, b \in R$ are elements of R such that $ab \in Q \cap R$. Since $ab \in Q$ and Q is a prime ideal of S, it follows that $a \in Q$ or $b \in Q$. Without loss of generality, assume that $a \in Q$. Thus, since also $a \in R$ we see $a \in Q \cap R$ which shows that $Q \cap R$ is a prime ideal of R. This completes the proof. $\square$

Homework 16: Page 377 #1, 2, 3

Problem 1. *The ring R of all 2×2 matrices*

$$\begin{bmatrix} a & b \\ 0 & c \end{bmatrix}$$

such that a is an integer and b, c are rational is not left Noetherian.

Proof. Define for each nonnegative integer n the set

$$I_n = \left\{ \begin{bmatrix} 0 & \frac{m}{2^n} \\ 0 & 0 \end{bmatrix} : m \in \mathbb{Z} \right\} \subseteq R$$

We first verify that I_n is a left ideal of R for each nonnegative integer n. Towards this end, fix a nonnegative integer n. Clearly, we have that $I_n \neq \emptyset$. Now, suppose that

$$A = \begin{bmatrix} 0 & \frac{m_1}{2^n} \\ 0 & 0 \end{bmatrix} \in I_n \quad \text{and} \quad B = \begin{bmatrix} 0 & \frac{m_2}{2^n} \\ 0 & 0 \end{bmatrix} \in I_n$$

and notice that since $m_1 - m_2 \in \mathbb{Z}$ we have

$$A - B = \begin{bmatrix} 0 & \frac{m_1}{2^n} \\ 0 & 0 \end{bmatrix} - \begin{bmatrix} 0 & \frac{m_2}{2^n} \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & \frac{m_1}{2^n} - \frac{m_2}{2^n} \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & \frac{m_1 - m_2}{2^n} \\ 0 & 0 \end{bmatrix} \in R$$

and thus I_n is a subgroup of R under addition. Next, let

$$A = \begin{bmatrix} 0 & \frac{m}{2^n} \\ 0 & 0 \end{bmatrix} \in I_n \quad \text{and} \quad B = \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \in R$$

Then we have since $am \in \mathbb{Z}$ that

$$BA = \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \begin{bmatrix} 0 & \frac{m}{2^n} \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & \frac{am}{2^n} \\ 0 & 0 \end{bmatrix} \in I_n$$

By the previous results, we conclude that I_n is a left ideal of R for each nonnegative integer n.

Next, we show that $I_n \subsetneq I_{n+1}$ for each nonnegative integer n. Towards this end, fix a nonnegative integer n and suppose that

$$A = \begin{bmatrix} 0 & \frac{m}{2^n} \\ 0 & 0 \end{bmatrix} \in I_n$$

Then we have since $2m \in \mathbb{Z}$ that

$$A = \begin{bmatrix} 0 & \frac{m}{2^n} \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & \frac{2m}{2^{n+1}} \\ 0 & 0 \end{bmatrix} \in I_{n+1}$$

so that $I_n \subseteq I_{n+1}$. To see that this containment is proper, consider the element

$$A = \begin{bmatrix} 0 & \frac{1}{2^{n+1}} \\ 0 & 0 \end{bmatrix} \in I_{n+1}$$

We claim that $A \notin I_n$. Indeed, suppose for the sake of contradiction that $A \in I_n$ so that for some $m \in \mathbb{Z}$ we have

$$\begin{bmatrix} 0 & \frac{1}{2^{n+1}} \\ 0 & 0 \end{bmatrix} = A = \begin{bmatrix} 0 & \frac{m}{2^n} \\ 0 & 0 \end{bmatrix}$$

so that

$$\frac{1}{2^{n+1}} = \frac{m}{2^n}$$

so that

$$m = \frac{2^n}{2^{n+1}} = \frac{1}{2} \notin \mathbb{Z}$$

which contradicts the fact that $m \in \mathbb{Z}$. We conclude that $I_n \subsetneq I_{n+1}$ for each nonnegative integer n.

Combining the above results, we obtain the ascending chain of left ideals of R

$$I_0 \subsetneq I_1 \subsetneq \cdots \subsetneq I_n \subsetneq \cdots$$

Furthermore, since each of the above inclusions is proper we conclude that there does not exist an integer $N \geq 0$ such that $I_n = I_N$ for all $n \geq N$. In particular, this shows that R does not satisfy the ascending chain condition on left ideals so that R is not left Noetherian. $\square$

Problem 2. *If I is a nonzero ideal in a PID R, then the ring R/I is both Noetherian and Artinian.*

Proof. We first show that R/I is Noetherian. Towards this end, let $\overline{J}$ be an ideal of R/I. Note that since $\overline{J}$ is an ideal of R/I we have that $\overline{J}$ is an R/I-submodule of R/I. By the Fourth Isomorphism Theorem for Modules, then, there is an R-submodule J of R with $I \subseteq J$ such that $\overline{J} = J/I$. Now, since J is an R-submodule of R it follows that J is an ideal of R and hence J is a finitely generated ideal of R since R is a PID. Therefore, we see that the ideal $J/I = \overline{J}$ is a finitely generated ideal of R/I. Since $\overline{J}$ was an arbitrary ideal of R/I, we conclude that R/I is Noetherian.

Lastly, we show that R/I is Artinian. Towards this end, suppose that

$$\overline{J_0} \supseteq \overline{J_1} \supseteq \cdots \supseteq \overline{J_n} \supseteq \cdots$$

is a descending chain of ideals of R/I. By the same reasoning as presented above, it follows that for each nonnegative integer n there is an ideal J_n of R with $I \subseteq J_n$ such that $\overline{J_n} = J_n/I$. Now, since R is a PID and as J_n is an ideal of R there is an element $a_n \in R$ such that $J_n = (a_n)$ for each nonnnegative integer n. Similarly, since R is a PID and as I is a nonzero ideal of R there is a nonzero element $a \in R$ such that $I = (a)$.

If a is a unit of R, then we have

$$R = (a) = I \subseteq J_n$$

so that $J_n = R$ for each nonnegative integer n. Therefore, for each nonnegative integer n we have

$$\overline{J_n} = J_n/I = R/I = J_0/I = \overline{J_0}$$

Thus, we see R/I satisfies the descending chain condition on ideals and is hence Artinian in this case. Therefore, we may assume that a is a nonunit of R and since a is also nonzero we now have that a is a nonzero, nonunit of R. Hence, since R is a PID and therefore a UFD we see in particular that a is divisible by only finitely many irreducible elements of R. We will use this observation below.

Now, since $I \subseteq J_n$ we have by the above observations that

$$a \in (a) = I \subseteq J_n = (a_n)$$

so that a_n divides a for each nonnegative integer n. Furthermore, notice that the above descending chain of ideals of R/I can be written

$$J_0/I \supseteq J_1/I \supseteq \cdots \supseteq J_n/I \supseteq \cdots$$

so that we have the descending chain of ideals of R

$$J_0 \supseteq J_1 \supseteq \cdots \supseteq J_n \supseteq \cdots$$

Suppose that for some nonnegative integer N we have that $a_N = 0$. In this case, we would have

$$\{0\} = (0) = (a_N) = J_N \supseteq J_n$$

and hence $J_n = \{0\} = J_N$ which implies that

$$\overline{J_n} = J_n/I = J_N/I = \overline{J_N}$$

for each nonnegative integer $n \geq N$. Thus, we see R/I satisfies the descending chain condition on ideals and is hence Artinian in this case. Therefore, we may assume that $a_n \neq 0$ for each nonnegative integer n.

Next, notice that if a_n is a unit of R for each nonnegative integer n that $J_n = (a_n) = R$ for each nonnegative integer n and hence

$$J_n = R = J_0$$

which implies that

$$\overline{J_n} = J_n/I = J_0/I = \overline{J_0}$$

Thus, we see R/I satisfies the descending chain condition on ideals and is hence Artinian in this case. Therefore, we may assume that there is some a_N such that a_N is not a unit of R for some nonnegative integer N. In particular, this shows that for each nonnegative integer $n \geq N$ we have

$$R \neq (a_N) = J_N \supseteq J_n = (a_n)$$

so that a_n is not a unit of R. By the above results, we have that a_n is a nonzero, nonunit of R for each nonnegative integer $n \geq N$. Therefore, since R is a PID and hence a UFD we have that a_n can be written as a product of irreducible elements of R in a way that is unique up to order and associates for each nonnegative integer $n \geq N$.

Finally, recall that a_n divides a so that the irreducible divisors of a_n divide a for each nonnegative integer $n \geq N$. But recall from the above that only finitely many irreducible elements of R can divide a. Thus, it now follows that there is some nonnegative integer $K \geq N$ such that for each nonnegative integer $n \geq K$ we have that a_n and a_K are divisible by precisely the same irreducible elements of R. Again appealing to the fact that R is a UFD, this observation shows that a_n and a_K are associates for each nonnegative integer $n \geq K$. Therefore, since a_n and a_K are associates it follows that a_n and a_K generate the same ideal of R so that

$$J_n = (a_n) = (a_K) = J_K$$

for each nonnegative integer $n \geq K$. Thus, we obtain

$$\overline{J_n} = J_n/I = J_K/I = \overline{J_K}$$

for each nonnegative integer $n \geq K$. Thus, we see R/I satisfies the descending chain condition on ideals and is hence Artinian in this case. In all cases, then, we conclude that R/I is Artinian. This completes the proof. $\square$

Problem 3. *Let S be a multiplicative subset of a commutative Noetherian ring R with identity. Then the ring $S^{-1}R$ is Noetherian.*

Proof. Recall that a ring T is Noetherian if and only if every ideal of T is finitely generated. We will use this equivalence below.

Towards this end, let J be an ideal of $S^{-1}R$. Since J is an ideal of $S^{-1}R$, we have that $J = S^{-1}I$ where $I = \phi_S^{-1}(J)$. Since the inverse homomorphic image of an ideal is an ideal, we have that I is an ideal of R. Since R is Noetherian, then, we have that I is a finitely generated ideal of R so that $I = (r_1, \ldots, r_n)$ for some $r_1, \ldots, r_n \in R$.

Now, fix any $s \in S$. We claim that

$$J = \left(\frac{r_1 s}{s}, \ldots, \frac{r_n s}{s}\right)$$

First, suppose that $a \in J = S^{-1}I$. Then $a = i/z$ for some $i \in I$ and $z \in S$. Since $i \in I = (r_1, \ldots, r_n)$, there are elements $b_1, \ldots, b_n \in R$ so that $i = b_1 r_1 + \cdots + b_n r_n$. As $b_1, \ldots, b_n \in R$ and $z \in S$ we have $b_1/z, \ldots, b_n/z \in S^{-1}R$ so that

$$\begin{aligned}
a &= \frac{i}{z} \\
&= \frac{b_1 r_1 + \cdots + b_n r_n}{z} \\
&= \frac{b_1 r_1}{z} + \cdots + \frac{b_n r_n}{z} \\
&= \frac{b_1 r_1}{z} \cdot \frac{s}{s} + \cdots + \frac{b_n r_n}{z} \cdot \frac{s}{s} \\
&= \frac{b_1}{z} \cdot \frac{r_1 s}{s} + \cdots + \frac{b_n}{z} \cdot \frac{r_n s}{s} \\
&\in \left(\frac{r_1 s}{s}, \ldots, \frac{r_n s}{s}\right)
\end{aligned}$$

On the other hand, suppose that

$$a \in \left(\frac{r_1 s}{s}, \ldots, \frac{r_n s}{s}\right)$$

Then there are $b_1/z_1, \ldots, b_n/z_n \in S^{-1}R$ such that

$$a = \frac{b_1}{z_1} \cdot \frac{r_1 s}{s} + \cdots + \frac{b_n}{z_n} \cdot \frac{r_n s}{s}$$

Now, notice that

$$(b_1 z_2 \cdots z_n s) r_1, \ldots, (b_n z_1 \cdots z_{n-1} s) r_n \in (r_1, \ldots, r_n) = I$$

so that as I is an ideal of R we have

$$(b_1 z_2 \cdots z_n s) r_1 + \cdots + (b_n z_1 \cdots z_{n-1} s) r_n \in I$$

Furthermore, we have $z_1 \cdots z_n s \in S$ as $z_1, \ldots, z_n, s \in S$ and S is a multiplicative set. Hence, we now have

$$a = \frac{b_1}{z_1} \cdot \frac{r_1 s}{s} + \cdots + \frac{b_n}{z_n} \cdot \frac{r_n s}{s} = \frac{(b_1 z_2 \cdots z_n s) r_1 + \cdots + (b_n z_1 \cdots z_{n-1} s) r_n}{z_1 \cdots z_n s} \in S^{-1} I = J$$

We conclude that

$$J = \left(\frac{r_1 s}{s}, \ldots, \frac{r_n s}{s} \right)$$

so that J is finitely generated. Therefore, by our observation made at the start of this proof we see that $S^{-1}R$ is Noetherian. $\square$

Homework 17: Page 377 #4, 5, 7

Problem 4. *Let R be a commutative ring with identity. If an ideal I of R is not finitely generated, then there is an infinite properly ascending chain of ideals*

$$J_1 \subsetneq J_2 \subsetneq \cdots$$

such that $J_k \subseteq I$ for all k. The union of the J_k need not be I.

Proof. Let $x_1 \in I$. Since I is not finitely generated, there is some element $x_2 \in I - (x_1)$. Furthermore, if $(x_1, x_2) = (x_1)$ then we would have $x_2 \in (x_1, x_2) = (x_1)$ which is a contradiction. Therefore, we have that $(x_1) \subsetneq (x_1, x_2)$. Similarly, since I is not finitely generated, there is some element $x_3 \in I - (x_1, x_2)$ and by the same reasoning as above we have that $(x_1, x_2) \subsetneq (x_1, x_2, x_3)$. Inductively, we obtain elements $x_1, x_2, x_3, \cdots \in I$ such that $(x_1, \dots x_n) \subsetneq (x_1, \dots, x_{n+1})$ for each positive integer n.

Now, for each positive integer n let $J_n = (x_1, \dots, x_n)$. By the above, we obtain the infinite properly ascending chain of ideals

$$J_1 \subsetneq J_2 \subsetneq J_3 \subsetneq \cdots$$

Furthermore, it is immediate by the definition of J_n that $J_n \subseteq I$ for each positive integer n. This completes the proof of the first statement in this problem.

Finally, let R be a commutative ring with identity and consider the polynomial ring $R[x_1, x_2, \dots]$ in infinitely many indeterminants $x_1, x_2, \dots$. Let $I = (x_1, x_2, \dots)$ and notice that, clearly, we have that I is an ideal of $R[x_1, x_2, \dots]$ which is not finitely generated. Now, let $J_1 = \{0\}$ and $J_n = (x_2, \dots, x_n)$ for each integer $n \geq 2$. Notice that by the definition of each J_n, we have the infinite properly ascending chain of ideals

$$J_1 \subsetneq J_2 \subsetneq J_3 \subsetneq \cdots$$

and that $J_n \subseteq I$ for each positive integer n.

Lastly, we claim that $\bigcup_{n=1}^{\infty} J_n \neq I$. First, note that clearly $x_1 \in (x_1, x_2, \dots) = I$. For the sake of contradiction, suppose that $x_1 \in \bigcup_{n=1}^{\infty} J_n$ so that there is some integer $N \geq 1$ with $x_1 \in J_N$. If $N = 1$, then

$$x_1 \in J_N = J_1 = \{0\}$$

which is clearly a contradiction. Therefore, we have $N \geq 2$ so that

$$x_1 \in J_N = (x_2, \dots, x_N)$$

which is clearly a contradiction. We conclude that $x_1 \in I$ but $x_1 \notin \bigcup_{n=1}^{\infty} J_n$ so that $\bigcup_{n=1}^{\infty} J_n \neq I$. This completes the proof of the second statement in this problem. $\square$

Problem 5. *Every homomorphic image of a left Noetherian or Artinian ring is left Noetherian or Artinian, respectively.*

Proof. Let $\phi : R \to S$ be a ring homomorphism for both parts of this proof.

First, suppose that R is left Noetherian and let

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$$

be an ascending chain of left ideals of $\phi(R)$. Since the inverse ring homomorphic image of a left ideal is a left ideal, we have that $\phi^{-1}(I_n)$ is a left ideal of R for each positive integer n. Thus, by the above inclusions and the previous observation we see that

$$\phi^{-1}(I_1) \subseteq \phi^{-1}(I_2) \subseteq \phi^{-1}(I_3) \subseteq \cdots$$

is an ascending chain of left ideals of R. Thus, since R is left Noetherian there is some positive integer N such that $\phi^{-1}(I_n) = \phi^{-1}(I_N)$ for each positive integer $n \geq N$.

We claim that $I_n = I_N$ for each positive integer $n \geq N$. Towards this end, fix a positive integer $n \geq N$ and let $i \in I_n \subseteq \phi(R)$. Then there is some $r \in R$ such that $\phi(r) = i$ so that

$$r \in \phi^{-1}(i) \subseteq \phi^{-1}(I_n) = \phi^{-1}(I_N)$$

and thus $i = \phi(r) \in I_N$. On the other hand, let $i \in I_N \subseteq \phi(R)$. Then there is some $r \in R$ such that $\phi(r) = i$ so that

$$r \in \phi^{-1}(i) \subseteq \phi^{-1}(I_N) = \phi^{-1}(I_n)$$

and thus $i = \phi(r) \in I_n$. We conclude that $I_n = I_N$ and since the fixed positive integer $n \geq N$ was arbitrary, this shows that $\phi(R)$ is Noetherian.

The proof that $\phi(R)$ is left Artinian if R is left Artinian follows by a symmetric version of the proof given above that was used to show that $\phi(R)$ is left Noetherian if R is left Noetherian. This completes the proof. $\square$

Problem 7. *An Artinian integral domain is a field.*

Proof. Let R be an Artinian integral domain. Since R is an integral domain, it remains to prove that every nonzero element of R has an inverse in R. Towards this end, let $a \in R$ be a nonzero element of R and notice that

$$(a) \supseteq (a^2) \supseteq (a^3) \supseteq \cdots$$

is a descending chain of ideals of R. Thus, since R is Artinian there is some positive integer N such that $(a^n) = (a^N)$ for each positive integer $n \geq N$. In particular, we have $(a^{N+1}) = (a^N)$ so that

$$a^N \in (a^N) = (a^{N+1})$$

and hence there is some $r \in R$ such that $a^N = ra^{N+1}$. Therefore, we have

$$0 = a^N - ra^{N+1} = a^N - a^{N+1}r = a^N(1 - ar)$$

Now, since R is an integral domain the above equality implies that either $a^N = 0$ or $1 - ar = 0$. However, since a is nonzero and R is an integral domain it follows that $a^N \neq 0$. Therefore, we see that $1 - ar = 0$ so that $ar = 1$. Since $r \in R$, this shows that $a^{-1} = r \in R$ so that a has an inverse in R. We conclude that R is a field. $\square$

Homework 18: Page 407 #1, 2, 3

Problem 1. *The ideal generated by* 3 *and* $1+\sqrt{5}i$ *in the subdomain* $\mathbb{Z}[\sqrt{5}i]$ *of* $\mathbb{C}$ *is invertible.*

Proof. Let $I = (3, 1+\sqrt{5}i) \subseteq \mathbb{Z}[\sqrt{5}i]$ and $J = (3, 1-\sqrt{5}i) \subseteq \mathbb{Z}[\sqrt{5}i]$ and note that I and J are clearly fractional ideals of $\mathbb{Z}[\sqrt{5}i]$. We claim that $IJ = (3)$. To establish the inclusion $IJ \subseteq (3)$, first recall that IJ is generated by all elements of the form ab where $a \in I$ and $b \in J$. In order to prove that $IJ \subseteq (3)$, then, it suffices to show that $ab \in (3)$ for all $a \in I$ and $b \in J$. Towards this end, let $a \in I$ and $b \in J$. Then

$$a = 3a_1 + a_2(1+\sqrt{5}i) \quad b = 3b_1 + b_2(1-\sqrt{5}i) \quad \text{for some} \quad a_1, a_2, b_1, b_2 \in \mathbb{Z}[\sqrt{5}i]$$

and hence

$$\begin{aligned} ab &= [3a_1 + a_2(1+\sqrt{5}i)][3b_1 + b_2(1-\sqrt{5}i)] \\ &= 9a_1b_1 + 3a_1b_2(1-\sqrt{5}i) + 3a_2b_1(1+\sqrt{5}i) + a_2b_2(1+\sqrt{5}i)(1-\sqrt{5}i) \\ &= 9a_1b_1 + 3a_1b_2(1-\sqrt{5}i) + 3a_2b_1(1+\sqrt{5}i) + 6a_2b_2 \\ &= (3a_1b_1 + a_1b_2(1-\sqrt{5}i) + a_2b_1(1+\sqrt{5}i) + 2a_2b_2)3 \\ &\in (3) \end{aligned}$$

so that by our previous observation, we obtain $IJ \subseteq (3)$.

On the other hand, to establish the inclusion $(3) \subseteq IJ$ it suffices to show that $3 \in IJ$ since IJ is an ideal of $\mathbb{Z}[\sqrt{5}i]$. Towards this end, first notice that we clearly have $1+\sqrt{5}i \in I$, $1-\sqrt{5}i \in J$, $3 \in I$, and $3 \in J$. Therefore, we see

$$6 = (1+\sqrt{5}i)(1-\sqrt{5}i) \in IJ \quad \text{and} \quad 9 = 3 \cdot 3 \in IJ$$

so that

$$3 = 9 - 6 \in IJ$$

so that by our previous observation, we obtain $(3) \subseteq IJ$ and thus $IJ = (3)$. This establishes our claim.

Now, recall that a nonzero principal ideal in an integral domain is invertible. Thus, since clearly (3) is a nonzero principal ideal in the integral domain $\mathbb{Z}[\sqrt{5}i]$ we have by this observation that (3) is an invertible ideal of $\mathbb{Z}[\sqrt{5}i]$ and therefore by our above result we have that $IJ = (3)$ is an invertible ideal of $\mathbb{Z}[\sqrt{5}i]$. Finally, recall that a product of nonzero ideals in an integral domain is invertible if and only if each ideal involved in the product is invertible. Therefore, since I and J are clearly nonzero ideals in the integral domain $\mathbb{Z}[\sqrt{5}i]$ such that IJ is an invertible ideal of $\mathbb{Z}[\sqrt{5}i]$ we may now conclude that $I = (3, 1+\sqrt{5}i)$ is an invertible ideal of $\mathbb{Z}[\sqrt{5}i]$, completing the proof. $\square$

Problem 2. *An invertible ideal in an integral domain that is a local ring is principal.*

Proof. Let R be an integral domain that is a local ring with unique maximal ideal M and suppose that $I \subseteq R$ is an invertible ideal of R. Then there exists a fractional ideal J of R such that $IJ = R$. Since R has identity, we have that $1 \in R = IJ$ and hence we may write $1 = \sum_{k=1}^{n} i_k j_k$ for some $i_1, \ldots, i_n \in I$ and $j_1, \ldots, j_n \in J$. We claim that $I = (i_1, \ldots, i_n)$. Clearly, we have $(i_1, \ldots, i_n) \subseteq I$ as $i_1, \ldots, i_n \in I$. On the other hand, let $x \in I$ and note that $xj_1, \ldots, xj_n \in IJ = R$. Thus, since $1 = \sum_{k=1}^{n} i_k j_k$ we see that

$$x = x \cdot 1 = x \sum_{k=1}^{n} i_k j_k = \sum_{k=1}^{n} x i_k j_k = \sum_{k=1}^{n} (x j_k) i_k \in (i_1, \ldots, i_n)$$

We conclude that $I = (i_1, \ldots, i_n)$, as claimed.

Now, note if $i_1 j_1, \ldots, i_n j_n \in M$ then $1 = \sum_{k=1}^{n} i_k j_k \in M$ which implies that $M = R$. However, since M is a maximal ideal of R we have $M \neq R$. Therefore, we may assume without loss of generality that $i_1 j_1 \notin M$. Thus, as $i_1 j_1 \in IJ = R$ but $i_1 j_1 \notin M$ we have $i_1 j_1 \in R - M$ and since M is the unique maximal ideal of R this implies that $i_1 j_1$ is a unit of R. Therefore, if we define $u = i_1 j_1 \in R$ then we have $1 = u^{-1} i_1 j_1$.

Finally, we claim that $I = (u^{-1} i_1)$. First, note that since $i_1 \in I$ and $u^{-1} \in R$ we have since I is an ideal of R that $u^{-1} i_1 \in I$ so that $(u^{-1} i_1) \subseteq I$. On the other hand, let $y \in I$. Then since $j_1 \in J$ and $JI = IJ = R$, we have $j_1 y \in JI = R$. Similarly, we have $i_1 j_1, \ldots, i_n j_n \in IJ = R$. Combining the previous two observations, we obtain

$$i_1 j_1 j_1 y = (i_1 j_1)(j_1 y) \in R \quad i_2 j_2 j_1 y = (i_2 j_2)(j_1 y) \in R \quad \cdots \quad i_n j_n j_1 y = (i_n j_n)(j_1 y) \in R$$

Therefore, we have

$$\begin{aligned} y &= y \cdot 1 \\ &= y \sum_{k=1}^{n} i_k j_k \\ &= \sum_{k=1}^{n} i_k j_k y \\ &= \sum_{k=1}^{n} i_k j_k (1 \cdot y) \\ &= \sum_{k=1}^{n} i_k j_k (u^{-1} i_1 j_1 \cdot y) \\ &= \sum_{k=1}^{n} (i_k j_k j_1 y) u^{-1} i_1 \\ &\in (u^{-1} i_1) \end{aligned}$$

We conclude that $I = (u^{-1} i_1)$ and hence I is principal. This completes the proof. $\square$

Problem 3. *If I is an invertible ideal in an integral domain R and S is a multiplicative set in R with $0 \notin S$, then $S^{-1}I$ is invertible in $S^{-1}R$.*

Proof. Let K be the field of fractions of R. Since $0 \notin S$ and R is an integral domain, we have that $S^{-1}R$ is an integral domain and clearly the field of fractions of $S^{-1}R$ is K. Now, as I is an invertible ideal of R, there exists a fractional ideal J of R such that $IJ = R$. We claim that $S^{-1}I$ and $S^{-1}J$ are fractional ideals of $S^{-1}R$.

Indeed, first note that since J is a fractional ideal of R that J is nonzero so that there is some nonzero element $j \in J$. Therefore, fixing any $s \in S$ shows that $j/s \in S^{-1}J$ is a nonzero element of $S^{-1}J$ so that $S^{-1}J$ is nonzero. Furthermore, suppose that $j/s \in S^{-1}J$ and $r/s' \in S^{-1}R$. Then $rj \in J$ since J is an R-submodule of K and $s's \in S$ since $s, s' \in S$ and S is a multiplicative subset of R. These observations give

$$\frac{r}{s'} \cdot \frac{j}{s} = \frac{rj}{s's} \in S^{-1}J$$

Thus, by the above results and since J is an R-submodule of K we conclude that $S^{-1}J$ is a nonzero $S^{-1}R$-submodule of K. Finally, note that since J is a fractional ideal of R that there is some nonzero element $r \in R$ such that $rJ \subseteq R$. Again fixing any $s \in S$, we have since $r \in R$ is nonzero that $r/s \in S^{-1}R$ is nonzero. Moreover, if $j/s' \in S^{-1}J$ then $rj \in rJ \subseteq R$ and $ss' \in S$ since $s, s' \in S$ and S is a multiplicative subset of R. These observations give

$$\frac{r}{s} \cdot \frac{j}{s'} = \frac{rj}{ss'} \in S^{-1}R$$

Thus, we now have that r/s is a nonzero element of $S^{-1}R$ with $(r/s)S^{-1}J \subseteq S^{-1}R$. We may now conclude that $S^{-1}J$ is a fractional ideal of $S^{-1}R$. In exactly the same fashion, we also see that $S^{-1}I$ is a fractional ideal of $S^{-1}R$.

Next, we show that $(S^{-1}I)(S^{-1}J) = S^{-1}R$. First, suppose that

$$\sum_{k=1}^{n} \left(\frac{i_k}{s_k} \cdot \frac{j_k}{s'_k} \right) \in (S^{-1}I)(S^{-1}J)$$

Then $i_1 j_1, \ldots, i_n j_n \in IJ = R$ and $s_1 s'_1, \ldots, s_k s'_k \in S$ since S is a multiplicative subset of R and $s_1, \ldots, s_n, s'_1, \ldots, s'_k \in S$. Thus, we obtain

$$\sum_{k=1}^{n} \left(\frac{i_k}{s_k} \cdot \frac{j_k}{s'_k} \right) = \sum_{k=1}^{n} \frac{i_k j_k}{s_k s'_k} \in S^{-1}R$$

On the other hand, suppose that $r/s \in S^{-1}R$. Since $r \in R = IJ$, we may write $r = \sum_{k=1}^{n} i_k j_k$ for some $i_1, \ldots, i_n \in I$ and $j_1, \ldots, j_n \in J$. Now, since I is an invertible ideal in R we have in particular that I is an ideal of R so that since $s \in S \subseteq R$ we have $si_1, \ldots, si_n \in I$. Thus, we obtain

$$\frac{r}{s} = \frac{\sum_{k=1}^{n} i_k j_k}{s} = \sum_{k=1}^{n} \frac{i_k j_k}{s} = \sum_{k=1}^{n} \left(\frac{i_k j_k}{s} \cdot \frac{s}{s} \right) = \sum_{k=1}^{n} \left(\frac{s i_k}{s} \cdot \frac{j_k}{s} \right) \in (S^{-1}I)(S^{-1}J)$$

so that $(S^{-1}I)(S^{-1}J) = S^{-1}R$. Finally, as $S^{-1}J$ is a fractional ideal of $S^{-1}R$ with $(S^{-1}I)(S^{-1}J) = S^{-1}R$ we see that $S^{-1}J$ is an inverse of $S^{-1}I$ in the monoid of fractional ideals of $S^{-1}R$ so that $S^{-1}I$ is invertible in $S^{-1}R$. This completes the proof. $\square$

Homework 19: Page 407 #4, 5, 6

Problem 4. *Let R be any ring with identity and P an R-module. Then P is projective if and only if there exist sets $(a_i)_{i\in I} \subseteq P$ and $(f_i)_{i\in I} \subseteq \mathrm{Hom}_R(P,R)$ such that for all $a \in P$, $a = \sum_{i\in I} f_i(a)a_i$.*

Proof. For the first direction, assume that P is a projective R-module and let $(a_i)_{i\in I} \subseteq P$ be a set of generators for P. Let ζ and $(\pi_i)_{i\in I}$ be defined as in the proof of the Theorem from class and define $f_i = \pi_i \circ \zeta$ for each $i \in I$. Then $(f_i)_{i\in I} \subseteq \mathrm{Hom}_R(P,R)$. Furthermore, if $a \in P$ then we know from the proof of the same Theorem from class that $a = \sum_{i\in I} f_i(a)a_i$. This completes the proof of the first direction.

For the second direction, let P be an R-module and assume that there are sets $(a_i)_{i\in I} \subseteq P$ and $(f_i)_{i\in I} \subseteq \mathrm{Hom}_R(P,R)$ such that for all $a \in P$ we have $a = \sum_{i\in I} f_i(a)a_i$. Let F be a free R-module with basis $(e_i)_{i\in I}$ and define

$$\pi : F \to P \quad \text{by} \quad e_i \mapsto a_i \quad \text{for each} \quad i \in I$$

Notice that by hypothesis we have that each element of P is an R-linear combination of elements from the set $(a_i)_{i\in I}$ which implies that $(a_i)_{i\in I}$ generates the ideal P of R. Therefore, by recalling the defintion of π we have that π is a surjective R-module homomorphism so that

$$0 \longrightarrow \ker\pi \xrightarrow{\ i\ } F \xrightarrow{\ \pi\ } P \longrightarrow 0$$

where i is the inclusion map is a short exact sequence of R-modules and R-module homomorphisms. Now, define

$$\zeta : P \to F \quad \text{by} \quad c \mapsto \sum_{i\in I} f_i(c)e_i$$

and observe that ζ is clearly a well-defined R-module homomorphism. Furthermore, since the defined composition of R-module homomorphisms is an R-module homomorphism we see that $\pi \circ \zeta : P \to P$ is an R-module homomorphism.

We claim that $\pi \circ \zeta : P \to P$ is the identity map. Towards this end, let $c \in P$. Then since $f_i(c) \in R$ for each $i \in I$, since π is an R-module homomorphism, and by hypothesis we see that

$$\begin{aligned}
(\pi \circ \zeta)(c) &= \pi(\zeta(c)) \\
&= \pi\left(\sum_{i\in I} f_i(c)e_i\right) \\
&= \sum_{i\in I} \pi(f_i(c)e_i) \\
&= \sum_{i\in I} f_i(c)\pi(e_i) \\
&= \sum_{i\in I} f_i(c)a_i \\
&= c
\end{aligned}$$

which proves that $\pi \circ \zeta : P \to P$ is the identity map.

Finally, note that by our previous results and since $\pi \circ \zeta$ is an R-module homomorphism that the short exact sequence from the above splits. Therefore, we have that $F \simeq \ker \pi \oplus P$. In particular, since P is a direct summand of the free R-module F it now follows that P is a projective R-module. This completes the proof of the second direction and hence completes the proof. $\square$

Problem 5. *A discrete valuation ring R is Noetherian and integrally closed.*

Proof. Firstly, note that since R is a discrete valuation ring we have in particular that R is a PID and hence every ideal of R is finitely generated. Thus, we see that R is Noetherian. Secondly, note that since R is a discrete valuation ring we have in particular that R is a PID and hence R is a UFD. Furthermore, recall that by a previous homework that a UFD is integrally closed. Thus, we see that R is integrally closed. This completes the proof. $\square$

Problem 6. (a): *If every nonzero prime ideal in an integral domain R is invertible, then R is Dedekind.*

(b): *If R is a Noetherian integral domain in which every maximal ideal is invertible, then R is Dedekind.*

Note: Suppose that every nonzero prime ideal of R is invertible. Since every invertible ideal is finitely generated, it follows by this assumption that every prime ideal of R is finitely generated and hence R is Noetherian. Moreover, since every maximal ideal is a prime ideal it now follows that every maximal ideal of R is invertible. In other words, by assuming the hypotheses of (a) we see that the hypotheses of (b) are satisfied. Thus, it suffices to prove (b) in order to prove parts (a) and (b). We do this below.

Proof. For the sake of contradiction, suppose that R is not Dedekind and let $\mathcal{F}$ denote the set of nonzero proper ideals of R which are not a product of a finite number of prime ideals of R. Now, since R is an integral domain but R is not Dedekind it follows that there exists a nonzero proper ideal of R which is not a product of a finite number of prime ideals of R so that $\mathcal{F} \neq \emptyset$. Thus, since R is Noetherian it follows that there exists a maximal element $I \in \mathcal{F}$.

Since $I \in \mathcal{F}$, we have that I is a proper ideal of R so that $I \subseteq M$ for some maximal ideal M of R. Since M is a maximal ideal of R, we have by hypothesis that M is an invertible ideal of R so that $M^{-1}M = R$. Thus, by the previous inclusion we now have

$$M^{-1}I = M^{-1} \cdot I \subseteq M^{-1} \cdot M = M^{-1}M = R$$

so that $M^{-1}I \subseteq R$. Therefore, we see that $M^{-1}I$ is an ideal of R. We will use this observation below.

Now, for the sake of contradiction suppose that $I = M^{-1}I$. Again using the invertibility of M, this equality implies that $I = MI$. Now, consider the localized ring R_M and recall that M_M is the unique maximal ideal of R_M. Since $I = MI$, we see $I_M = M_M I_M$. Furthermore, since R is Noetherian and as I is an ideal of R it follows that I is finitely generated so that I_M is also finitely generated. Thus, since $I_M = M_M I_M$ and as M_M is the unique maximal ideal of R_M we may now appeal to Nakayama's Lemma to assert that $I_M = 0$. However, this implies that $I = 0$ which is a contradiction since $I \in \mathcal{F}$. We conclude that $I \neq M^{-1}I$.

Finally, note that since M is an ideal of R that $1 \in M^{-1}$. In particular, this shows that $I \subseteq M^{-1}I$ and since $I \neq M^{-1}I$ we obtain the strict inclusion $I \subsetneq M^{-1}I$. Now, if $M^{-1}I = R$ then again using the invertibility of M this equality implies that $I = M$ so that I is a product of a finite number of maximal (hence prime) ideals of R. However, this contradicts the fact that $I \in \mathcal{F}$. Therefore, we see $M^{-1}I \neq R$. Combining the previous results, we see that $M^{-1}I$ is a nonzero proper ideal of R which properly contains I. By the maximality of $I \in \mathcal{F}$, then, it follows that there are prime ideals $P_1, \ldots, P_n$ of R such that $M^{-1}I = P_1 \cdots P_n$. Again using the invertibility of M, the above equality implies that $I = MP_1 \cdots P_n$. Since M is a maximal (hence prime) ideal of R, then , the previous equality implies that I is the product of a finite number of prime ideals of R. However, this contradicts the fact that $I \in \mathcal{F}$. We conclude that R is Dedekind. $\square$

Homework 20: Page 407 #7, 9, 10

Problem 7. *If S is a multiplicative subset of a Dedekind domain R (with $1 \in S, 0 \notin S$), then $S^{-1}R$ is a Dedekind domain.*

Proof. First, note that since R is a Dedekind domain we have that R is an integral domain and since $0 \notin S$ it follows by this observation that $S^{-1}R$ is an integral domain. Now, recall that an integral domain T is a Dedekind domain if and only if every nonzero ideal in T is invertible. We will use this equivalence to prove that the integral domain $S^{-1}R$ is a Dedekind domain.

Towards this end, let J be a nonzero ideal in $S^{-1}R$ and recall that $J = S^{-1}\phi_S^{-1}(J)$. Before continuing with the proof of the main result, we show that every element of J is of the form j/s for some $j \in J \cap R$ and some $s \in S$. Indeed, let $a \in J = S^{-1}\phi_S^{-1}(J)$ so that $a = j/s$ for some $j \in \phi_S^{-1}(J) \subseteq R$ and $s \in S$. Now, since $j \in \phi_S^{-1}(J)$ it follows that $\phi_S(j) \in J$. But by the definition of ϕ_S and since $1 \in S$, we have that

$$j = \frac{j}{1} = \frac{j}{1} \cdot \frac{s}{s} = \frac{js}{s} = \phi_S(j) \in J$$

so that $j \in J$ and hence $j \in J \cap R$. This result establishes that every element of J is of the previously-described form. We will use this fact below.

Towards this end, note that as J is a nonzero ideal in $S^{-1}R$ that $J \cap R$ is a nonzero ideal in R. Since R is Dedekind, then, it follows that $J \cap R$ is an invertible ideal in R so that there is some fractional ideal I of R such that $I(J \cap R) = R$. Now, we claim that $(S^{-1}I)J = S^{-1}(I(J \cap R))$. First, let $x \in (S^{-1}I)J$. Then we can write

$$x = \sum_{k=1}^{n} \frac{i_k}{s_k} \cdot a_k$$

for some $i_1, \ldots, i_n \in I, s_1, \ldots, s_n \in S$, and $a_1, \ldots, a_n \in J$. By our above result, we know that $a_k = j_k/s'_k$ for some $j_k \in J \cap R$ and $s'_k \in S$ for each $k \in \{1, \ldots, n\}$. Thus, we have that $i_1 j_1, \ldots, i_n j_n \in I(J \cap R)$. Furthermore, since S is a multiplicative subset of R we have that $s_1 s'_1, \ldots, s_n s'_n \in S$. Combining the previous two observations, we obtain

$$\frac{i_1 j_1}{s_1 s'_1}, \ldots, \frac{i_n j_n}{s_n s'_n} \in S^{-1}(I(J \cap R))$$

so that by recalling the above equality we have

$$x = \sum_{k=1}^{n} \frac{i_k}{s_k} \cdot \frac{j_k}{s'_k} = \sum_{k=1}^{n} \frac{i_k j_k}{s_k s'_k} \in S^{-1}(I(J \cap R))$$

Thus, we see that $x \in S^{-1}(I(J \cap R))$. On the other hand, let $x \in S^{-1}(I(J \cap R))$. Then we can write

$$x = \frac{\sum_{k=1}^{n} i_k j_k}{s} = \sum_{k=1}^{n} \frac{i_k j_k}{s}$$

for some $i_1, \ldots, i_n \in I, j_1, \ldots, j_n \in J \cap R$, and $s \in S$. Now, notice that clearly $i_1/s, \ldots, i_n/s \in S^{-1}I$. Thus, as $1 \in S$ we have by recalling the above equality that

$$x = \sum_{k=1}^{n} \left(\frac{i_k j_k}{s} \cdot \frac{s}{s} \right) = \sum_{k=1}^{n} \left(\frac{i_k}{s} \cdot \frac{j_k s}{s} \right) = \sum_{k=1}^{n} \left(\frac{i_k}{s} \cdot \frac{j_k}{1} \cdot \frac{s}{s} \right) = \sum_{k=1}^{n} \left(\frac{i_k}{s} \cdot j_k \right) \in (S^{-1}I)J$$

Thus, we see that $x \in (S^{-1}I)J$. We conclude that $(S^{-1}I)J = S^{-1}(I(J \cap R))$.

Finally, recall that $I(J \cap R) = R$ so that by our above result we obtain that

$$(S^{-1}I)J = S^{-1}(I(J \cap R)) = S^{-1}R$$

By the above equality and since $S^{-1}I$ is a fractional ideal of $S^{-1}R$ as I is a fractional ideal of R, we conclude that $S^{-1}I$ is an inverse of J in the monoid of fractional ideals of $S^{-1}R$ so that J is an invertible ideal in $S^{-1}R$. Since J was an arbitrary nonzero ideal in $S^{-1}R$, this result shows that $S^{-1}R$ is Dedekind, completing the proof. $\square$

Problem 9. *If a Dedekind domain R has only a finite number of nonzero prime ideals $P_1, \ldots, P_n$, then R is a PID.*

Proof. Since R is Dedekind and as $P_1, \ldots, P_n$ are nonzero prime ideals of R, it follows that $P_1, \ldots, P_n$ are maximal ideals of R. Moreover, since any maximal ideal of R is clearly a prime ideal of R it now follows that $P_1, \ldots, P_n$ are the maximal ideals of R. Next, suppose that I is an ideal of R. We will show that I is principal.

If I is the zero ideal of R, then I is clearly principal. Therefore, assume that I is nonzero so that I is a nonzero ideal of the Dedekind domain R which implies that I is an invertible ideal in R. Thus, there is some fractional ideal J of R such that $IJ = R$. Now, as $P_1, \ldots, P_n$ are maximal ideals of R we have in particular that $P_1, \ldots, P_n \neq R$ and since $IJ = R$ it follows that for each $k \in \{1, \ldots, n\}$ there are elements $i_k \in I$ and $j_k \in J$ such that $i_k j_k \notin P_k$.

Now, it follows by arguments from class and from previous homeworks that for each $k \in \{1, \ldots, n\}$ the maximal ideal P_k cannot contain the intersection of the maximal ideals $P_1, \ldots, P_{k-1}, P_{k+1}, \ldots, P_n$. Therefore, for each $k \in \{1, \ldots, n\}$ there is an element $u_k \in P_1 \cap \cdots \cap P_{k-1} \cap P_{k+1} \cap \cdots \cap P_n$ such that $u_k \notin P_k$. Next, define $v = u_1 j_1 + \cdots + u_n j_n$. Recall that clearly $u_1, \ldots, u_n \in R$ and since J is a fractional ideal of R we have in particular that J is an R-module. By these observations and since $j_1, \ldots, j_n \in J$, it now follows by the definition of v that $v \in J$ and hence vI is an ideal in R.

We claim that vI is not contained in any maximal ideal of R. For the sake of contradiction, suppose that vI were contained in some maximal ideal of R. Then since $P_1, \ldots, P_n$ are the maximal ideals of R, we may assume without loss of generality that $vI \subseteq P_1$. Therefore, since $i_1 \in I$ we have that $vi_1 \in vI \subseteq P_1$. Now, notice that by the definition of v we have

$$vi_1 = (u_1 j_1 + \cdots + u_n j_n) i_1 = u_1 j_1 i_1 + \cdots + u_n j_n i_1$$

Furthermore, we have that $j_2 i_1, \ldots, j_n i_1 \in JI = IJ = R$ and that $u_2, \ldots, u_n \in P_1$. Thus, since P_1 is an ideal of R we see that $u_2 j_2 i_1, \ldots, u_n j_n i_1 \in P_1$ so that

$$u_2 j_2 i_1 + \cdots + u_n j_n i_1 \in P_1$$

and since $vi_1 \in P_1$ we now have by the above equality that $u_1 j_1 i_1 \in P_1$. However, recall that $u_1 \notin P_1$ and $j_1 i_1 \notin P_1$ so that since P_1 is a prime ideal of R we have that $u_1 j_1 i_1 \notin P_1$ which contradicts the fact that $u_1 j_1 i_1 \in P_1$. Hence, we conclude that vI is not contained in any maximal ideal of R.

Finally, note that since the ideal vI of R is not contained in any maximal ideal of R that $vI = R$. Thus, we have $I = \frac{1}{v} R = \left(\frac{1}{v}\right)$ so that I is principal. We conclude that R is a PID, completing the proof. $\square$

Problem 10. *If I is a nonzero ideal in a Dedekind domain R, then R/I is an Artinian ring.*

Proof. (Version 1): First, note that since R is Dedekind that R is Noetherian. Therefore, since the ring homomorphic image of a Noetherian ring is a Noetherian ring it follows that R/I is a Noetherian ring.

Next, let A be a nonzero prime ideal of R/I. We claim that A is a maximal ideal of R. Towards this end, suppose that B is an ideal of R/I with $A \subseteq B \subseteq R/I$. Since A is a nonzero prime ideal of R/I, we know by a previous homework problem that $A = P/I$ for some nonzero prime ideal P of R with $I \subseteq P$. Similarly, since B is an ideal of R/I we know by the Fourth Isomorphism Theorem for Rings that $B = J/I$ for some ideal J of R with $I \subseteq J$.

Now, since P is a prime ideal of R and as R is Dedekind it follows that P is a maximal ideal of R. Furthermore, observe that since $A \subseteq B \subseteq R/I$ we have by the above that $P/I \subseteq J/I \subseteq R/I$ so that we obtain the inclusion $P \subseteq J \subseteq R$. Thus, since P is a maximal ideal of R and as J is an ideal of R the previous inclusion implies that either $J = P$ or $J = R$. Therefore, we see that since $B = J/I$ that either $B = P/I = A$ or $B = R/I$ and hence we conclude that A is a maximal ideal of R/I.

Finally, note that by the above results we have that R/I is a Noetherian ring in which every nonzero prime ideal of R/I is a maximal ideal of R/I. This observation implies that R/I is an Artinian ring, completing the proof. $\square$

Proof. (Version 2): Recall that an integral domain S is a Dedekind domain if and only if every proper ideal in S is uniquely a product of a finite number of prime ideals. We will use this equivalence to prove this problem.

Before we prove the main result, we show that I is contained in at most a finite number of distinct ideals of R. If $I = R$, then the result is immediate. Therefore, assume that $I \neq R$ so that I is a nonzero proper ideal of R and suppose that $J \subseteq R$ is an ideal of R with $I \subseteq J$. Clearly, we know that R is an ideal of R containing I so we may assume that J is a proper ideal of R. Now, since I is a nonzero proper ideal of the Dedekind domain R it follows that there are distinct nonzero prime ideals $P_1, \ldots, P_m$ of R such that $I = P_1^{n_1} \cdots P_m^{n_m}$ where $n_1, \ldots, n_m$ are positve integers. Similarly, since J is a nonzero proper ideal of the Dedekind domain R it follows that there are distinct nonzero prime ideals $Q_1, \ldots, Q_s$ of R such that $J = Q_1^{k_1} \cdots Q_s^{k_s}$ where $k_1, \ldots, k_s$ are positive integers.

Next, notice that we now have the inclusion

$$P_1^{n_1} \cdots P_m^{n_m} = I \subseteq J = Q_1^{k_1} \cdots Q_s^{k_s} \subseteq Q_1, \ldots, Q_s$$

Therefore, as has been shown multiple times in previous lectures and in previous homeworks we know that since $Q_1, \ldots, Q_s$ are prime ideals of R that there are elements $P_{t_1}, \ldots, P_{t_s} \in \{P_1, \ldots, P_m\}$ such that

$$P_{t_1} \subseteq Q_1 \quad \cdots \quad P_{t_s} \subseteq Q_s$$

Furthermore, since every nonzero prime ideal in a Dedekind domain is maximal and as the prime ideals $Q_1, \ldots, Q_s$ are clearly proper ideals of R it follows by the above inclusions that $Q_1 = P_{t_1}, \ldots, Q_s = P_{t_s}$ and since $Q_1, \ldots, Q_s$ are distinct it follows that $P_{t_1}, \ldots, P_{t_s}$ are distinct. Combining the previous results, we now have

$$P_1^{n_1} \cdots P_m^{n_m} = I \subseteq J = Q_1^{k_1} \cdots Q_s^{k_s} = P_{t_1}^{k_1} \cdots P_{t_s}^{k_s}$$

Furthermore, note that since $J = P_{t_1}^{k_1} \cdots P_{t_s}^{k_s}$ and as $\{P_{t_1}, \ldots, P_{t_s}\} \subseteq \{P_1, \ldots, P_m\}$ that we can clearly write $J = P_1^{\alpha_1} \cdots P_m^{\alpha_m}$ for some nonnegative integers $\alpha_1, \ldots, \alpha_m$ where not all of $\alpha_1, \ldots, \alpha_m$ are equal to 0 as $J \neq R$. Thus, by the above inclusion we now obtain the inclusion

$$P_1^{n_1} \cdots P_m^{n_m} = I \subseteq J = P_1^{\alpha_1} \cdots P_m^{\alpha_m}$$

Therefore, by the above inclusion it now follows since R is Dedekind that $0 \leq \alpha_i \leq n_i$ for each $i \in \{1, \ldots, m\}$ and where not all of $\alpha_1, \ldots, \alpha_m$ are equal to 0 as $J \neq R$. Thus, taking into account the ideal R of R containing I we conclude that I can be contained in at most $(n_1 + 1) \cdots (n_m + 1)$ ideals of R. That is, we see I can be contained in at most a finite number of ideals of R.

We now prove the main result. Towards this end, let

$$B_1 \supseteq B_2 \supseteq \cdots \supseteq B_n \supseteq \cdots$$

be a descending chain of ideals of R/I. Recall that by the Fourth Isomorphism Theorem for Rings that there are ideals $A_1, A_2, \ldots$ of R with $I \subseteq A_1, I \subseteq A_2, \ldots$ such that $B_1 = A_1/I, B_2 = A_2/I, \ldots$. Hence, by the above we obtain the inclusion

$$A_1/I \supseteq A_2/I \supseteq \cdots \supseteq A_n/I \supseteq \cdots$$

which implies the inclusion

$$A_1 \supseteq A_2 \supseteq \cdots \supseteq A_n \supseteq \cdots$$

Finally, recall that the ideal I of R can be contained in at most a finite number of ideals of R. Therefore, since $I \subseteq A_1, I \subseteq A_2, \ldots$ it follows by the last inclusion above that there is an integer $N \geq 1$ such that $A_n = A_N$ for each integer $n \geq N$. Hence, for each integer $n \geq N$ we have

$$B_n = A_n/I = A_N/I = B_N$$

so that R/I satisfies the descending chain condition on ideals. We conclude that R/I is Artinian, completing the proof. $\square$

Homework 21: Page 413 #3, 8, 9

Note: We assume in this Homework that F is an algebraically closed extension field of a field K.

Problem 3. *There is a one-to-one inclusion-reversing correspondence between the set of affine K-varieties in F^n and the set of radical ideals of $K[x_1, \ldots, x_n]$.*

Proof. Before we begin, recall that an ideal I of a ring R is a radical ideal of R if $I = \mathrm{Rad}(I)$. Furthermore, we prove two Lemmas below before proving the main result.

Lemma 1. If A is an affine K-variety in F^n, then $V(J(A)) = A$.

Proof. First, note that since A is an affine K-variety in F^n we have that $A = V(S)$ for some subset $S \subseteq K[x_1, \ldots, x_n]$. Therefore, we must show that $V(J(V(S))) = V(S)$.

Towards this end, first let $(a_1, \ldots, a_n) \in V(J(V(S)))$ so that $f(a_1, \ldots, a_n) = 0$ for all $f(x_1, \ldots, x_n) \in J(V(S))$. Now, let $f(x_1, \ldots, x_n) \in S$. We claim that $f(x_1, \ldots, x_n) \in J(V(S))$. Towards this end, let $(b_1, \ldots, b_n) \in V(S)$ so that $g(b_1, \ldots, b_n) = 0$ for all $g(x_1, \ldots, x_n) \in S$. Therefore, since $f(x_1, \ldots, x_n) \in S$ we have that $f(b_1, \ldots, b_n) = 0$ and since $(b_1, \ldots, b_n) \in V(S)$ was arbitrary this result shows that $f(x_1, \ldots, x_n) \in J(V(S))$. Thus, by our initial observation we now have that $f(a_1, \ldots, a_n) = 0$ and since $f(x_1, \ldots, x_n) \in S$ was arbitrary this shows that $(a_1, \ldots, a_n) \in V(S)$. We now have the inclusion $V(J(V(S))) \subseteq V(S)$.

On the other hand, let $(a_1, \ldots, a_n) \in V(S)$ and let $f(x_1, \ldots, x_n) \in J(V(S))$ so that $f(b_1, \ldots, b_n) = 0$ for all $(b_1, \ldots, b_n) \in V(S)$. Therefore, since $(a_1, \ldots, a_n) \in V(S)$ we have that $f(a_1, \ldots, a_n) = 0$ and since $f(x_1, \ldots, x_n) \in J(V(S))$ was arbitrary this result shows that $(a_1, \ldots, a_n) \in V(J(V(S))$. We now have the inclusion $V(S) \subseteq V(J(V(S)))$. We conclude that $V(J(V(S))) = V(S)$ so that $V(J(A)) = A$. $\square$

Lemma 2. If a subset $S \subseteq K[x_1, \ldots, x_n]$ is such that $J(V(S)) = S$, then S is a radical ideal of $K[x_1, \ldots, x_n]$.

Proof. First, note that since $J(V(S))$ is an ideal of $K[x_1, \ldots, x_n]$ and as $S = J(V(S))$ we have that S is an ideal of $K[x_1, \ldots, x_n]$. Therefore, by Hilbert's Nullstellensatz we obtain that

$$\mathrm{Rad}(S) = J(V(S)) = S$$

so that $S = \mathrm{Rad}(S)$ and hence S is a radical ideal of $K[x_1, \ldots, x_n]$. $\square$

We now prove the main result. Towards this end, let $\mathcal{K}$ denote the set of affine K-varieties in F^n and let $\mathcal{R}$ denote the set of radical ideals of $K[x_1, \ldots, x_n]$. Define

$$f : \mathcal{K} \to \mathcal{R} \quad \text{by} \quad A \mapsto J(A)$$

We show that f is well-defined. Towards this end, let $A \in \mathcal{K}$ so that A is an affine K-variety in F^n. Now, we claim that $J(V(f(A))) = f(A)$. Indeed, since A is an affine K-variety of F^n we have by Lemma 1 above that $V(J(A)) = A$ so that

$$J(V(f(A))) = J(V(J(A)) = J(A) = f(A)$$

which completes the proof of our claim. By Lemma 2, this result shows that $f(A)$ is a radical ideal of $K[x_1, \ldots, x_n]$ and so $f(A) \in \mathcal{R}$ so that f is a well-defined map.

On the other hand, define

$$g : \mathcal{R} \to \mathcal{K} \quad \text{by} \quad I \mapsto V(I)$$

Notice that if I is a radical ideal of $K[x_1, \ldots, x_n]$, then we clearly have that $V(I)$ is an affine K-variety in F^n. Therefore, we see that f is well-defined a map.

Now, we show that $f \circ g = 1_{\mathcal{R}}$ and $g \circ f = 1_{\mathcal{K}}$. Indeed, first let $I \in \mathcal{R}$. Then since I is a radical ideal of $K[x_1, \ldots, x_n]$ and by Hilbert's Nullstellensatz, we have

$$I = \mathrm{Rad}(I) = J(V(I))$$

Therefore, we obtain

$$(f \circ g)(I) = f(g(I)) = f(V(I)) = J(V(I)) = I$$

so that $f \circ g = 1_{\mathcal{R}}$. Secondly, let $A \in \mathcal{K}$. By the same reasoning as above, we have $V(J(A)) = A$. Therefore, we obtain

$$(g \circ f)(A) = g(f(A)) = g(J(A)) = V(J(A)) = A$$

so that $g \circ f = 1_{\mathcal{K}}$. Combining the previous two results, then, we see that f and g are inverses of one another so that there is a one-to-one correspondence between $\mathcal{K}$ and $\mathcal{R}$.

Finally, we show that this one-to-one correspondence is inclusion-reversing. Towards this end, suppose that $I_1, I_2 \in \mathcal{R}$ and $I_1 \subseteq I_2$. Now, let $(a_1, \ldots, a_n) \in V(I_2)$. Then $f(a_1, \ldots, a_n) = 0$ for all $f(x_1, \ldots, x_n) \in I_2$. Next, let $g(x_1, \ldots, x_n) \in I_1 \subseteq I_2$ so that by the previous observation we have $g(a_1, \ldots, a_n) = 0$. Thus, as $g(x_1, \ldots, x_n) \in I_1$ was arbitrary it follows that $(a_1, \ldots, a_n) \in V(I_1)$ and hence

$$g(I_2) = V(I_2) \subseteq V(I_1) = g(I_1)$$

so that $g(I_2) \subseteq g(I_1)$.

On the other hand, suppose that $A_1, A_2 \in \mathcal{K}$ and $A_1 \subseteq A_2$. Now, let $f(x_1, \ldots, x_n) \in J(A_2)$. Then $f(a_1, \ldots, a_n) = 0$ for all $(a_1, \ldots, a_n) \in A_2$. Next, let $(b_1, \ldots, b_n) \in A_1 \subseteq A_2$ so that by the previous observation we have $f(b_1, \ldots, b_n) = 0$. Thus, as $(b_1, \ldots, b_n) \in A_2$ was arbitrary it follows that $f(x_1, \ldots, x_n) \in J(A_1)$ and hence

$$f(A_2) = J(A_2) \subseteq J(A_1) = f(A_1)$$

so that $f(A_2) \subseteq f(A_2)$. We conclude that the above one-to-one correspondence is inclusion-reversing. This completes the proof. $\square$

Problem 8. *A nonempty K-variety V in F^n is* ***irreducible*** *provided that whenever $V = W_1 \cup W_2$ with W_1, W_2 being K-varieties in F^n, either $V = W_1$ or $V = W_2$.*

(a): *Prove that V is irreducible if and only if $J(V)$ is a prime ideal in $K[x_1, \ldots, x_n]$.*

(b): *Let $F = \mathbb{C}$ and $S = \{x^2 - 2y^2\}$. Then $V(S)$ is irreducible as a $\mathbb{Q}$-variety but not as an $\mathbb{R}$-variety.*

Proof. (a): For the first direction, assume that V is an irreducible K-variety in F^n. Now, we know that $J(V)$ is an ideal of $K[x_1, \ldots, x_n]$. We claim that $J(V) \neq K[x_1, \ldots, x_n]$. For the sake of contradiction, suppose that $J(V) = K[x_1, \ldots, x_n]$. Then $1 \in K[x_1, \ldots, x_n] = J(V)$. Now, since $V \neq \emptyset$ there is some element $(a_1, \ldots, a_n) \in V$ and since $1 \in J(V)$ we now have $1(a_1, \ldots, a_n) = 0$. However, this gives

$$0 \neq 1 = 1(a_1, \ldots, a_n) = 0$$

which is clearly a contradiction. Therefore, we have $J(V) \neq K[x_1, \ldots, x_n]$.

Now, suppose that $f(x_1, \ldots, x_n), g(x_1, \ldots, x_n) \in K[x_1, \ldots, x_n]$ such that the product $f(x_1, \ldots, x_n)g(x_1, \ldots x_n) \in J(V)$. Next, define the sets

$$W_1 = V \cap V(\{f(x_1, \ldots, x_n)\}) \quad \text{and} \quad W_2 = V \cap V(\{g(x_1, \ldots, x_n)\})$$

We claim that $V = W_1 \cup W_2$. Towards this end, first let $(a_1, \ldots, a_n) \in V$. Then since $f(x_1, \ldots, x_n)g(x_1, \ldots, x_n) \in J(V)$ we have that

$$0 = (fg)(a_1, \ldots, a_n) = f(a_1, \ldots, a_n)g(a_1, \ldots, a_n)$$

so that by the above equality we have either $f(a_1, \ldots a_n) = 0$ or $g(a_1, \ldots, a_n) = 0$. Without loss of generality, assume that $f(a_1, \ldots, a_n) = 0$. Then we have $(a_1, \ldots, a_n) \in V(\{f(x_1, \ldots, x_n)\})$ and since $(a_1, \ldots, a_n) \in V$ this gives that

$$(a_1, \ldots, a_n) \in V \cap V(\{f(x_1, \ldots, x_n)\}) = W_1 \subseteq W_1 \cup V_2$$

On the other hand, suppose that $(a_1, \ldots, a_n) \in W_1 \cup W_2$ and without loss of generality assume that $(a_1, \ldots, a_n) \in W_1 = V \cap V(\{f(x_1, \ldots, x_n)\})$. Then clearly we have that $(a_1, \ldots, a_n) \in V$. Combining the above results, then, we have that $V = W_1 \cup W_2$.

Finally, note that since the intersection of K-varieties is a K-variety that we have by the definition of W_1 and W_2 that W_1 and W_2 are K-varieties. Therefore, since $V = W_1 \cup W_2$ and V is an irreducible K-variety in F^n it follows that either $V = W_1$ or $V = W_2$. Without loss of generality, assume that $V = W_1$. Then we have

$$V = W_1 = V \cap V(\{f(x_1, \ldots, x_n)\})$$

Now, let $(a_1, \ldots, a_n) \in V$. Then by the above, we have that

$$(a_1, \ldots, a_n) \in V \cap V(\{f(x_1, \ldots, x_n)\}) \subseteq V(\{f(x_1, \ldots, x_n)\})$$

so that $f(a_1, \ldots, a_n) = 0$. Thus, since $(a_1, \ldots, a_n) \in V$ was arbitrary this shows that $f(x_1, \ldots, x_n) \in J(V)$. Therefore, we conclude that $J(V)$ is a prime ideal of $K[x_1, \ldots, x_n]$. This completes the proof of the first direction.

For the second direction, let V be a nonempty K-variety in F^n such that $J(V)$ is a prime ideal of $K[x_1, \ldots, x_n]$ and suppose that W_1 and W_2 are K-varieties in F^n such

that $V = W_1 \cup W_2$. Suppose that $V \neq W_1$. We claim that $J(V) = J(W_2)$. Indeed, first note that since $V = W_1 \cup W_2$ that we have $W_2 \subseteq W_1 \cup W_2 = V$ so that by the first problem in this homework we have $J(V) \subseteq J(W_2)$.

On the other hand, suppose that $g(x_1, \ldots, x_n) \in J(W_2)$. Now, since we have $W_1 \subseteq W_1 \cup W_2 = V$ appealing again to the first problem in this homework gives that $J(V) \subseteq J(W_1)$. Moreover, appealing once again to the first problem in this homework we have since $V \neq W_1$ that $J(V) \neq J(W_1)$ and hence by the previous inclusion this implies that there is some element $f(x_1, \ldots, x_n) \in J(W_1) - J(V)$. We claim that $f(x_1, \ldots, x_n)g(x_1, \ldots, x_n) \in J(V) = J(W_1 \cup W_2)$. Indeed, suppose that $(a_1, \ldots, a_n) \in W_1 \cup W_2$. If $(a_1, \ldots, a_n) \in W_1$, then $f(a_1, \ldots, a_n) = 0$ since $f(x_1, \ldots, x_n) \in J(W_1)$ and hence we have

$$(fg)(a_1, \ldots, a_n) = f(a_1, \ldots, a_n)g(a_1, \ldots, a_n) = 0 \cdot g(a_1, \ldots, a_n) = 0$$

so that $f(x_1, \ldots, x_n)g(x_1, \ldots, x_n) \in J(W_1 \cup W_2) = J(V)$ in this case. If $(a_1, \ldots, a_n) \in W_2$, then $g(a_1, \ldots, a_n) = 0$ since $g(x_1, \ldots, x_n) \in J(W_2)$ and hence we have

$$(fg)(a_1, \ldots, a_n) = f(a_1, \ldots, a_n)g(a_1, \ldots, a_n) = f(a_1, \ldots, a_n) \cdot 0 = 0$$

so that $f(x_1, \ldots, x_n)g(x_1, \ldots, x_n) \in J(W_1 \cup W_2) = J(V)$ in this case and hence in all cases. Therefore, since $f(x_1, \ldots, x_n) \notin J(V)$ and as $J(V)$ is a prime ideal of $K[x_1, \ldots, x_n]$ it now follows that $g(x_1, \ldots, x_n) \in J(V)$. We may now conclude that $J(V) = J(W_2)$.

Finally, recall that if A is a K-variety we have that $V(J(A)) = A$. Therefore, since V and W_2 are K-varieties we obtain

$$V = V(J(V)) = V(J(W_2)) = W_2$$

so that $V = W_2$. We conclude that V is an irreducible K-variety, completing the proof of the second direction. $\square$

Proof. (b): Let $f(x, y) = x^2 - 2y^2$ and let $K \in \{\mathbb{Q}, \mathbb{R}\}$. Before we prove either statement involved in this part of the problem, we show that $J(V(S)) = (f(x, y))$. Towards this end, first let $g(x, y) \in J(V(S))$. Then we have $g(a, b) = 0$ for all $(a, b) \in V(S) = V(\{f(x, y)\})$. In other words, we see that every zero of $f(x, y)$ is a zero of $g(x, y)$. Therefore, there exists a polynomial $h(x, y) \in K[x, y]$ such that $g(x, y) = h(x, y)f(x, y)$ so that $g(x, y) \in (f(x, y))$. On the other hand, let $g(x, y) \in (f(x, y))$ so that there is some polynomial $h(x, y) \in K[x, y]$ such that $g(x, y) = h(x, y)f(x, y)$. Let $(a, b) \in V(S) = V(\{f(x, y)\})$. Then $f(a, b) = 0$ so that by the above equality for $g(x, y)$ we have

$$g(a, b) = h(a, b)f(a, b) = h(a, b) \cdot 0 = 0$$

and hence $g(x, y) \in J(V(S))$. We conclude that $J(V(S)) = (f(x, y))$.

Next, we show that $f(x, y)$ is irreducible in $\mathbb{Q}[x, y]$ but that $f(x, y)$ is reducible in $\mathbb{R}[x, y]$. Indeed, note that as

$$f(x, y) = x^2 - 2y^2 = \left(x - \sqrt{2}y\right)\left(x + \sqrt{2}y\right)$$

and as $\sqrt{2} \in \mathbb{R} - \mathbb{Q}$ it follows that $f(x, y)$ is irreducible in $\mathbb{Q}[x, y]$ but that $f(x, y)$ is reducible in $\mathbb{R}[x, y]$.

Now, we show that $V(S)$ is irreducible as a $\mathbb{Q}$-variety. Indeed, first note that as $V(S)$ is clearly a nonempty $\mathbb{Q}$-variety in $\mathbb{C}^n$ by the first part of this problem it suffices to show that $J(V(S)) = (f(x, y))$ is a prime ideal of $\mathbb{Q}[x, y]$. Towards this end, note that since $f(x, y)$ is irreducible in $\mathbb{Q}[x, y]$ by the above and since $\mathbb{Q}[x, y]$ is a UFD as $\mathbb{Q}$ is a field it follows that $f(x, y)$ is a prime element of $\mathbb{Q}[x, y]$. Thus, the ideal $(f(x, y)) = J(V(S))$ is a prime ideal of $\mathbb{Q}[x, y]$. By the above observation, then, we conclude that $V(S)$ is irreducible as a $\mathbb{Q}$-variety.

Finally, we show that $V(S)$ is not irreducible as an $\mathbb{R}$-variety. Indeed, note that by the above we have that $f(x, y)$ is reducible in $\mathbb{R}[x, y]$. Therefore, since $\mathbb{R}[x, y]$ is a UFD as $\mathbb{R}$ is a field it follows that $f(x, y)$ is not a prime element of $\mathbb{R}[x, y]$. Thus, the ideal $(f(x, y)) = J(V(S))$ is not a prime ideal of $\mathbb{R}[x, y]$. By the first part of this problem, then, we see that $V(S)$ is not irreducible as an $\mathbb{R}$-variety. This completes the proof. $\square$

Problem 9. *Every nonempty K-variety in F^n may be written uniquely as a finite union $V_1 \cup \cdots \cup V_k$ of affine K-varieties in F^n such that $V_j \nsubseteq V_i$ for $i \neq j$ and V_i is irreducible.*

Proof. First, we show that every nonempty K-variety in F^n can be written as a finite union of affine K-varieties in F^n. For the sake of contradiction, suppose there were a nonempty K-variety V in F^n for which this desired result is not true. Clearly, if V is an irreducible K-variety then the result is true. Therefore, it must be the case that V is not an irreducible K-variety. Since V is a nonempty K-variety that is not an irreducible K-variety, it follows that there are K-varieties V_1 and V_2 such that $V = V_1 \cup V_1'$ but $V \neq V_1$ and $V \neq V_1'$. Therefore, it follows that V_1 and V_1' are nonempty K-varieties which are both properly contained in V.

Now, if the desired result is true for both of the nonempty K-varieties V_1 and V_1' then it follows that the desired result would be true for V. However, this is a contradiction. Therefore, without loss of generality it must be the case that the desired result fails for V_1 so that by the same reasoning as presented above it follows that there is a nonempty K-variety V_2 which is properly contained in V_1 such that the desired result fails for V_2. Continuing in this fashion, we obtain the properly descending chain of K-varieties

$$V \supsetneq V_1 \supsetneq V_2 \supsetneq \cdots \supsetneq V_m \supsetneq \cdots$$

Therefore, by the first problem in this homework we obtain the properly ascending chain of ideals of $K[x_1, \ldots, x_n]$ given by

$$J(V) \subsetneq J(V_1) \subsetneq J(V_2) \subsetneq \cdots \subsetneq J(V_m) \subsetneq \cdots$$

Now, note that since K is a field we have in particular that K is Noetherian. Therefore, by Hilbert's Basis Theorem it follows that $K[x_1, \ldots, x_n]$ is Noetherian. However, this contradicts the existence of the above properly ascending chain of ideals of $K[x_1, \ldots, x_n]$. We conclude that every nonempty K-variety in F^n may be written as a finite union $V_1 \cup \cdots \cup V_k$ of affine K-varieties in F^n.

To complete the proof, let V be a nonempty K-variety in F^n. By the above, there is a finite number of irreducible affine K-varieties $W_1, \ldots, W_m$ in F^n such that $V = W_1 \cup \cdots \cup W_m$. Now, suppose that $W_j \subseteq W_i$ for some $i, j \in \{1, \ldots, m\}$ with $i \neq j$. Then by the inclusion $W_j \subseteq W_i$, it follows that we may delete the K-variety W_j from the union involved in the above equality for V. Continuing in this fashion, we obtain that V may be written $V = V_1 \cup \cdots \cup V_k$ where $V_1, \ldots, V_k$ are irreducible affine K-varieties in F^n such that $V_j \nsubseteq V_i$ for each $i, j \in \{1, \ldots, k\}$ with $i \neq j$.

Finally, we show that the union $V = V_1 \cup \cdots \cup V_k$ is unique. Indeed, suppose that we have $V = Z_1 \cup \cdots \cup Z_m$ where $Z_1, \ldots, Z_m$ are irreducible affine K-varieties in F^n such that $Z_j \nsubseteq Z_i$ for each $i, j \in \{1, \ldots, m\}$ with $i \neq j$. Now, fix any $r \in \{1, \ldots, k\}$. Then since $V = Z_1 \cup \cdots \cup Z_m$, we have

$$V_r = V \cap V_r = (Z_1 \cup \cdots \cup Z_m) \cap V_r = (Z_1 \cap V_r) \cup \cdots \cup (Z_m \cap V_r)$$

But recall that V_r is irreducible so that by the above equality and since the union of K-varieties is a K-variety, there is some $s \in \{1, \ldots, m\}$ such that $V_r = Z_s \cap V_r \subseteq Z_s$ and hence $V_r \subseteq Z_s$. On the other hand, by the exact same argument as presented above

there is some $t \in \{1, \ldots, k\}$ such that $Z_s \subseteq V_t$. Combining the previous two inclusions, then, we obtain the inclusion $V_r \subseteq Z_s \subseteq V_t$ and hence $r = t$. Therefore, we now have the inclusions $V_r \subseteq Z_s$ and $Z_s \subseteq V_r$ so that $V_r = Z_s$. Thus, since the fixed element $r \in \{1, \ldots, k\}$ was arbitrary it now follows that the union $V = V_1 \cup \cdots \cup V_k$ is unique. This completes the proof. $\square$

Homework 22: Page 424 #3

Problem 3. *Let V be an infinite dimensional vector space over a division ring D.*

(a): *If F is the set of all $\theta \in \mathrm{End}_D(V)$ such that $\mathrm{Im}(\theta)$ is finite dimensional, then F is a proper ideal of $\mathrm{End}_D(V)$. Therefore $\mathrm{End}_D(V)$ is not simple.*

(b): *F is itself a simple ring.*

(c): *F is contained in every nonzero ideal of $\mathrm{End}_D(V)$.*

(d): *$\mathrm{End}_D(V)$ is not (left) Artinian.*

Proof. (a): First, we show that F is a two-sided ideal of $\mathrm{End}_D(V)$. Towards this end, note that the zero map $V \to V$ is an element of $\mathrm{End}_D(V)$ and that the image $\{0\}$ of the zero map is clearly a finite dimensional vector space over D. Thus, the zero map $V \to V$ is in F so that $F \neq \emptyset$. Next, let $\theta_1, \theta_2 \in F$ so that $\mathrm{Im}(\theta_1)$ and $\mathrm{Im}(\theta_2)$ are finite dimensional vector spaces over D so that $\dim_D(\mathrm{Im}(\theta_1)) < \infty$ and $\dim_D(\mathrm{Im}(\theta_2)) < \infty$.

Now, consider the element $\theta_1 - \theta_2$ and note that since $\theta_1, \theta_2 \in \mathrm{End}_D(V)$ and as $\mathrm{End}_D(V)$ is a ring we have that $\theta_1 - \theta_2 \in \mathrm{End}_D(V)$. Moreover, recall that the image of a vector space under a linear transformation is a vector space and that the difference of vector spaces is a vector space. Thus, it follows by these observations that $\mathrm{Im}(\theta_1 - \theta_2)$ and $\mathrm{Im}(\theta_1) - \mathrm{Im}(\theta_2)$ are vector spaces over D. Furthermore, since we clearly have $\mathrm{Im}(\theta_1 - \theta_2) \subseteq \mathrm{Im}(\theta_1) - \mathrm{Im}(\theta_2)$ we obtain by the previous results that

$$\begin{aligned}
\dim_D(\mathrm{Im}(\theta_1 - \theta_2)) &\leq \dim_D(\mathrm{Im}(\theta_1) - \mathrm{Im}(\theta_2)) \\
&= \dim_D(\mathrm{Im}(\theta_1) + \mathrm{Im}(\theta_2)) \\
&= \dim_D(\mathrm{Im}(\theta_1)) + \dim_D(\mathrm{Im}(\theta_2)) - \dim_D(\mathrm{Im}(\theta_1) \cap \mathrm{Im}(\theta_2)) \\
&\leq \dim_D(\mathrm{Im}(\theta_1)) + \dim_D(\mathrm{Im}(\theta_2)) \\
&< \infty
\end{aligned}$$

Thus, we now have that $\mathrm{Im}(\theta_1 - \theta_2)$ is a finite dimensional vector space over D so that $\theta_1 - \theta_2 \in F$. We conclude that F is a subgroup of $\mathrm{End}_D(V)$ under addition.

Finally, let $\phi \in \mathrm{End}_D(V)$ and $\theta \in F$ so that $\dim_D(\mathrm{Im}(\theta)) < \infty$. We claim that $\phi \circ \theta \in F$ and that $\theta \circ \phi \in F$. Indeed, first note that since the defined composition of linear transformations is a linear transformation we have that $\phi \circ \theta \in \mathrm{End}_D(V)$. Now, consider $\mathrm{Im}(\phi \circ \theta)$ and note that we clearly have $\mathrm{Im}(\phi \circ \theta) = \mathrm{Im}\left(\phi\big|_{\mathrm{Im}(\theta)}\right)$. Furthermore, recall that the image of a vector space under a linear transformation is a vector space so that $\mathrm{Im}(\phi \circ \theta) = \mathrm{Im}\left(\phi\big|_{\mathrm{Im}(\theta)}\right)$ is a vector space over D. Therefore, combining the previous results gives that

$$\begin{aligned}
\dim_D(\mathrm{Im}(\phi \circ \theta)) &= \dim_D\left(\mathrm{Im}\left(\phi\big|_{\mathrm{Im}(\theta)}\right)\right) \\
&= \dim_D(\mathrm{Im}(\theta)) - \dim_D\left(\ker\left(\phi\big|_{\mathrm{Im}(\theta)}\right)\right) \\
&\leq \dim_D(\mathrm{Im}(\theta)) \\
&< \infty
\end{aligned}$$

Thus, we now have that $\text{Im}(\phi \circ \theta)$ is a finite dimensional vector space over D so that $\phi \circ \theta \in F$. Secondly, note by the same reasoning as presented above we have $\theta \circ \phi \in \text{End}_D(V)$ and that $\text{Im}(\theta \circ \phi)$ and $\text{Im}(\theta)$ are vector spaces over D. Furthermore, we clearly have that $\text{Im}(\theta \circ \phi) \subseteq \text{Im}(\theta)$. Therefore, combining the previous results gives that

$$\dim_D(\text{Im}(\theta \circ \phi)) \leq \dim_D(\text{Im}(\theta)) < \infty$$

Thus, we now have that $\text{Im}(\theta \circ \phi)$ is a finite dimensional vector space over D so that $\theta \circ \phi \in F$. We conclude that F is a two-sided ideal of $\text{End}_D(V)$.

Next, we show that F is properly contained in $\text{End}_D(V)$. Towards this end, recall that V is an infinite dimensional vector space over D so that $\dim_D(V) = \infty$. Moreover, we clearly have that $1_V \in \text{End}_D(V)$ and that $\text{Im}(1_V) = V$. Therefore, combining the previous results gives that

$$\dim_D(\text{Im}(1_V)) = \dim_D(V) = \infty$$

so that $1_V \notin F$. Thus, as $1_V \in \text{End}_D(V)$ but $1_V \notin F$ we obtain by the above result that F is a proper ideal of $\text{End}_D(V)$.

Lastly, we show that $\text{End}_D(V)$ is not a simple ring. Towards this end, we first show that F is nonzero. Indeed, fix any element a in a basis E for V over D and define a map

$$\theta : V \to V \quad \text{by} \quad e \mapsto \begin{cases} a & \text{if} \quad e = a \\ 0 & \text{if} \quad e \neq a \end{cases} \quad \text{for each} \quad e \in E$$

Now, note that clearly $\theta \in \text{End}_D(F)$ and since a is an element of a basis E for V over D we have $a \neq 0$ so that $\theta(a) = a \neq 0$. In particular, these observations show that θ is a nonzero element of $\text{End}_D(F)$. Moreover, we have that

$$\dim_D(\text{Im}(\theta)) = \dim_D((a)) = 1 < \infty$$

Combining the previous results, then, we see that θ is a nonzero element of F so that $F \neq \{0\}$. Therefore, we may now combine this result with the above result to conclude that F is a proper, nontrivial two-sided ideal of $\text{End}_D(V)$ so that $\text{End}_D(V)$ is not simple. This completes the proof. $\square$

Proof. (b): We begin by showing that F is a ring. Towards this end, first note that by the proof in Part (a) that F is a two-sided ideal of $\text{End}_D(V)$ shows that F an abelian group under addition. Next, suppose that $\theta_1, \theta_2 \in F$ so that in particular we have $\dim_D(\text{Im}(\theta_1)) < \infty$ and consider $\theta_1 \circ \theta_2$. By the same reasoning as presented in Part (a), we have that $\theta_1 \circ \theta_2 \in \text{End}_D(V)$ and that $\text{Im}(\theta_1 \circ \theta_2)$ is a vector space over D. Moreover, we clearly have that $\text{Im}(\theta_1 \circ \theta_2) \subseteq \text{Im}(\theta_1)$. Thus, combining the previous results gives

$$\dim_D(\text{Im}(\theta_1 \circ \theta_2)) \leq \dim_D(\text{Im}(\theta_1)) < \infty$$

Thus, we now have that $\text{Im}(\theta_1 \circ \theta_2)$ is a finite dimensional vector space over D so that $\theta_1 \circ \theta_2 \in F$ and hence F is closed under function composition. Furthermore, recall that function composition is an associative operation and note that the distributivity axiom clearly holds for F. We conclude that F is a ring.

Next, we show that $F^2 \neq \{0\}$. Indeed, consider the map $\theta : V \to V$ as defined in Part (a) and recall that $\theta \in F$ so that $\theta \circ \theta \in F^2$. Moreover, we have that

$$(\theta \circ \theta)(a) = \theta(\theta(a)) = \theta(a) = a \neq 0$$

and hence $\theta \circ \theta$ is a nonzero element of F^2 so that $F^2 \neq \{0\}$.

Finally, we show that F has no nontrivial, proper two-sided ideals. Towards this end, let J be a nontrivial two-sided ideal of F so that there is some nonzero element in F. Now, let $(e_i)_{i \in I}$ be a basis for V over D and for $i, j \in I$ define $e_{i,j} \in \mathrm{End}_D(V)$ and $R \subseteq \mathrm{End}_D(V)$ as in class. Then since there is some nonzero element in the two-sided ideal J of F and since clearly $R \subseteq F$, it follows that $R \subseteq J$. Now, suppose that $\theta \in F$. Then since $\mathrm{Im}(\theta)$ is a finite dimensional vector space over D, it follows that θ is a finite D-linear combination of elements $e_{i,j} \in \mathrm{End}_D(V)$. In particular, this shows that $\theta \in R \subseteq J$ and hence it follows that $F \subseteq J$. Furthermore, since $J \subseteq F$ as J is an ideal of F we may now conclude that $J = F$ and thus F contains no nontrivial, proper two-sided ideals. By the above results, then, we conclude that F is a simple ring. This completes the proof. □

Proof. (c): Let I be a nonzero two-sided ideal of $\mathrm{End}_D(V)$. Then since I is a two-sided ideal of $\mathrm{End}_D(V)$ and as F is a two-sided ideal of $\mathrm{End}_D(V)$ by Part (a), we have that IF is a two-sided ideal of $\mathrm{End}_D(V)$. But recall that F is a ring by Part (b) and that we clearly have $IF \subseteq F$ so that by the previous observation, we now have that IF is a two-sided ideal of F. Therefore, since F is a simple ring by Part (b) it follows that $IF \in \{\{0\}, F\}$.

Now, we claim that $IF \neq \{0\}$. Towards this end, note that since I is in particular nonzero there is some nonzero element $\phi \in I$. That is, we have that $\phi : V \to V$ is a nonzero map so that there is some element a in a basis E for V over D such that $\phi(a) \neq 0$. Next, define

$$\theta : V \to V \quad \text{by} \quad e \mapsto \begin{cases} a & \text{if} \quad e = a \\ 0 & \text{if} \quad e \neq a \end{cases} \quad \text{for each} \quad e \in E$$

Now, note that by the same reasoning as presented in Part (a) we have that $\theta \in F$. Therefore, we have that $\phi \circ \theta \in IF$ and

$$(\phi \circ \theta)(a) = \phi(\theta(a)) = \phi(a) \neq 0$$

In particular, the above results show that $\phi \circ \theta$ is a nonzero element of IF so that $IF \neq \{0\}$. Therefore, by the above observation we have that $IF = F$. This gives that

$$F = IF \subseteq I$$

and hence $F \subseteq I$. Thus, as I was an arbitrary nonzero ideal of $\mathrm{End}_D(V)$ this completes the proof. □

Proof. (d): Let E be a basis for V over D. Now, since V is an infinite dimensional vector space over V it follows that $|E| = \infty$ and so there is some countably infinite

subset $(e_i)_{i=1}^{\infty} \subseteq E$. Next, fix a positive integer n and consider the map $\theta_{1,\dots,n} : V \to V$ that is defined as follows. We have

$$\theta_{1,\dots,n}(e_i) = 0 \quad \text{for each} \quad i \in \{1, \dots, n\}$$

and

$$\theta_{1,\dots,n}(e_j) = e_j \quad \text{for each} \quad j \in \{n+1, n+2, \dots\}$$

and

$$\theta_{1,\dots,n}(e) = 0 \quad \text{for each} \quad e \in E - (e_i)_{i=1}^{\infty}$$

By the above definition, it is immediate that $\theta_{1,\dots,n} \in \mathrm{End}_D(V)$ and hence $(\theta_{1,\dots,n})$ is a left ideal of $\mathrm{End}_D(V)$. Thus, since the fixed positive integer n was arbitrary we have that $(\theta_{1,\dots,n})$ is a left ideal of $\mathrm{End}_D(V)$ for each positive integer n. We claim that

$$(\theta_1) \supsetneq (\theta_{1,2}) \supsetneq (\theta_{1,2,3}) \supsetneq \cdots \supsetneq (\theta_{1,\dots,n-1}) \supsetneq (\theta_{1,\dots,n}) \supsetneq \cdots$$

is a properly descending chain of left ideals of $\mathrm{End}_D(V)$.

Towards this end, we first show $(\theta_1) \supsetneq (\theta_{1,2})$. To begin, we show that $\theta_{1,2} \in (\theta_1)$. Indeed, define a map

$$\phi : V \to V \quad \text{by} \quad e_2 \mapsto 0 \quad \text{and} \quad e \mapsto e \quad \text{for each} \quad e \in E - \{e_2\}$$

Clearly, we have that $\phi \in \mathrm{End}_D(V)$ so that $\phi \circ \theta_1 \in (\theta_1)$. Moreover, notice that

$$(\phi \circ \theta_1)(e_1) = \phi(\theta_1(e_1)) = \phi(0) = 0 = \theta_{1,2}(e_1)$$

and

$$(\phi \circ \theta_1)(e_2) = \phi(\theta_1(e_2)) = \phi(e_2) = 0 = \theta_{1,2}(e_2)$$

and

$$(\phi \circ \theta_1)(e_z) = \phi(\theta_1(e_z)) = \phi(e_z) = e_z = \theta_{1,2}(e_z) \quad \text{for each} \quad z \in \{3, 4, \dots\}$$

and

$$(\phi \circ \theta_1)(e) = \phi(\theta_1(e)) = \phi(0) = 0 = \theta_{1,2}(e) \quad \text{for each} \quad e \in E - (e_i)_{i=1}^{\infty}$$

By the above results, then, we conclude that $\theta_{1,2} = \phi \circ \theta_1 \in (\theta_1)$. Therefore, since (θ_1) is a left ideal of $\mathrm{End}_D(V)$ we obtain that $(\theta_{1,2}) \subseteq (\theta_1)$ and hence $(\theta_1) \supseteq (\theta_{1,2})$. Finally, we show that this inclusion is strict. For the sake of contradiction, suppose that $(\theta_1) = (\theta_{1,2})$. Then we clearly have $\theta_1 \in (\theta_1) = (\theta_{1,2})$ and hence there is some element $\phi \in \mathrm{End}_D(V)$ such that $\theta_1 = \phi \circ \theta_{1,2}$. Furthermore, recall that e_2 is in a basis E for V over D so that we have in particular that $e_2 \neq 0$. Therefore, we obtain that

$$0 \neq e_2 = \theta_1(e_2) = (\phi \circ \theta_{1,2})(e_2) = \phi(\theta_{1,2}(e_2)) = \phi(0) = 0$$

which is clearly a contradiction. Thus, we obtain by the above that $(\theta_1) \supsetneq (\theta_{1,2})$.

Finally, by a similar argument as presented above we may now assert that we have the strict inclusion $(\theta_{1,\dots,n-1}) \supsetneq (\theta_{1,\dots,n})$ for each integer $n \geq 2$. This gives that

$$(\theta_1) \supsetneq (\theta_{1,2}) \supsetneq (\theta_{1,2,3}) \supsetneq \cdots \supsetneq (\theta_{1,\dots,n-1}) \supsetneq (\theta_{1,\dots,n}) \supsetneq \cdots$$

is a properly descending chain of left ideals of $\mathrm{End}_D(V)$. In particular, the existence of the above properly descending chain of left ideals of $\mathrm{End}_D(V)$ shows that $\mathrm{End}_D(V)$ is not (left) Artinian. This completes the proof. $\square$

Homework 23: Page 424 #4, 5, 6

Problem 4. *Let V be a vector space over a division ring D. A subring R of $\mathrm{End}_D(V)$ is said to be n-**fold transitive** if for every $k \in \{1, \ldots, n\}$ and every linearly independent subset $\{v_1, \ldots, v_k\}$ of V and every arbitrary subset $\{u_1, \ldots, u_k\}$ of V, there exists $\theta \in R$ such that $\theta(v_i) = u_i$ for $i \in \{1, \ldots, k\}$.*

(a): *If R is one-fold transitive, then R is primitive.*

(b): *If R is two-fold transitive, then R is dense in $\mathrm{End}_D(V)$.*

Proof. (a): To begin, note that V is an R-module with action defined by for $\theta \in R$ and $v \in V$ we have $\theta v = \theta(v)$. Now, we claim that V is a faithful, simple (left) R-module. First, we show that V is a faithful R-module. Towards this end, suppose that $\phi \in \mathrm{Ann}(V)$ so that $0 = \phi v = \phi(v)$ for each $v \in V$. In particular, this shows that $\phi : V \to V$ is the zero map and hence as $\phi \in \mathrm{Ann}(V)$ was arbitrary we conclude that $\mathrm{Ann}(V) = \{0\}$ so that V is a faithful R-module.

Next, we show that V is a simple R-module. Indeed, since R is one-fold transitive it follows that $\dim_D(V) \geq 1$ so that in particular we have that V is nonzero and hence there is a nonzero element $v \in V$. Now, notice that since v is nonzero that the set $\{v\}$ is clearly a linearly independent subset of V. Therefore, since R is one-fold transitive there is some $\theta \in R$ such that $\theta(v) = v$ and hence

$$\theta v = \theta(v) = v \neq 0$$

In particular, the above equality shows that $\theta v \in RV$ is a nonzero element of RV so that $RV \neq \{0\}$.

Finally, let $W \subseteq V$ be a nonzero R-submodule of V. Then there is some nonzero element $w \in W$. Now, let $v \in V$. If $v = 0$, then since W is an R-module we clearly have $v = 0 \in W$. If $v \neq 0$, first note that since $w \in W \subseteq V$ is nonzero that the set $\{w\}$ is clearly a linearly independent subset of V. Thus, since R is one-fold transitive there is some $\theta \in R$ such that $\theta(w) = v$ so that since W is an R-module we obtain that

$$v = \theta(w) = \theta w \in RW \subseteq W$$

In any case, we see that $v \in W$ and since $v \in V$ was arbitrary we may now conclude that $V \subseteq W$. But since $W \subseteq V$, we see that $W = V$ and hence V is a simple R-module. Combining the above results, we obtain that V is a faithful, simple R-module so that R is primitive. $\square$

Proof. (b): Let $\Delta = \mathrm{End}_R(V)$. First, we show that R is a dense subring of $\mathrm{End}_\Delta(V)$. Before we begin, we remark that $R \subseteq \mathrm{End}_\Delta(V)$ so that R is indeed a subring of $\mathrm{End}_\Delta(V)$ Now, we claim that Δ is a division ring. Towards this end, note that since R is two-fold transitive that R is clearly one-fold transitive. Therefore, by the proof of Part (a) we have that V is a simple R-module so that by Schur's Lemma we have that $\mathrm{End}_R(V) = \Delta$ is a division ring. Moreover, recall that V is a (left) Δ-module so that since Δ is a division ring we see that V is a (left) vector space over Δ.

Now, let n be a positive integer and let $\{v_1, \ldots, v_n\}$ be a linearly independent subset of V over Δ and let $\{u_1, \ldots, u_n\}$ be any arbitrary subset of V. We must find an element $\theta \in R$ such that $\theta(v_i) = u_i$ for each $i \in \{1, \ldots, n\}$. Towards this end, recall once again by the proof of Part (a) we have that V is a simple R-module. Thus, by Jacobson's Density Theorem there is some element $\theta \in R$ such that $\theta(v_i) = u_i$ for each $i \in \{1, \ldots, n\}$. We conclude that R is a dense subring of $\mathrm{End}_\Delta(V)$.

Next, let $Z = \{\beta_d : d \in D\}$ where for each $d \in D$ we have β_d is the map defined by

$$\beta_d : V \to V \quad \text{by} \quad v \mapsto dv$$

and note that since V is a vector space over D that β_d is a well-defined map for each $d \in D$. We claim that $Z = \Delta$. Towards this end, first let $\beta_d \in Z$ and let $v_1, v_2 \in V$ and $\theta \in R \subseteq \mathrm{End}_D(V)$. Then we obtain that

$$\begin{aligned}
\beta_d(\theta v_1 + v_2) &= \beta_d(\theta(v_1) + v_2) \\
&= d(\theta(v_1) + v_2) \\
&= d\theta(v_1) + dv_2 \\
&= \theta(dv_1) + dv_2 \\
&= \theta(\beta_d(v_1)) + dv_2 \\
&= \theta\beta_d(v_1) + \beta_d(v_2)
\end{aligned}$$

so that $\beta_d \in \mathrm{End}_R(V)$ and hence we see that $Z \subseteq \Delta$.

On the other hand, let $\phi \in \Delta = \mathrm{End}_R(V)$ and let $v \in V$ be a nonzero element of V. Now, since R is two-fold transitive it follows that $\dim_D(V) \geq 2$. Therefore, since $v \in V$ is nonzero it follows that there is some $d \in D$ such that $\{v, dv\}$ is a linearly independent subset of V. Since R is two-fold transitive and as $\phi(v) \in V$, then, there is some $\theta \in R \subseteq \mathrm{End}_D(V)$ such that $\theta(v) = v$ and $\theta(dv) = \phi(v)$. Thus, we obtain that

$$\begin{aligned}
\phi(v) &= \phi(\theta(v)) \\
&= \phi(\theta v) \\
&= \theta\phi(v) \\
&= \theta(\phi(v)) \\
&= \theta(\theta(dv)) \\
&= \theta(d\theta(v)) \\
&= d\theta(\theta(v)) \\
&= d\theta(v) \\
&= dv \\
&= \beta_d(v)
\end{aligned}$$

Furthermore, we have that

$$\phi(0) = 0 = d0 = \beta_d(0)$$

Combining the above results, we see that $\phi = \beta_d \in Z$ and hence we see that $\Delta \subseteq Z$. We conclude that $Z = \Delta$.

Next, we show that $D \simeq Z$. Towards this end, define a map

$$\psi : D \to Z \quad \text{by} \quad d \mapsto \beta_d$$

Clearly, we see that ψ is a well-defined map. Furthermore, we claim that ψ is a ring isomorphism. Towards this end, let $d_1, d_2 \in D$ and let $v \in V$. Then

$$\psi(d_1 + d_2)(v) = \beta_{d_1+d_2}(v) = (d_1 + d_2)v = d_1 v + d_2 v = \beta_{d_1}(v) + \beta_{d_2}(v) = (\beta_{d_1} + \beta_{d_2})(v)$$

and hence we see that

$$\psi(d_1 + d_2) = \beta_{d_1} + \beta_{d_2} = \psi(d_1) + \psi(d_2)$$

and

$$\psi(d_1 d_2)(v) = \beta_{d_1 d_2}(v) = (d_1 d_2)v = d_1(d_2 v) = d_1 \beta_{d_2}(v) = \beta_{d_1}(\beta_{d_2}(v)) = (\beta_{d_1} \circ \beta_{d_2})(v)$$

and hence we see that

$$\psi(d_1 d_2) = \beta_{d_1} \circ \beta_{d_2} = \psi(d_1) \circ \psi(d_2)$$

which proves that ψ is a ring homomorphism.

Next, we show that ψ is a bijection. First, we show that ϕ is an injection. Towards this end, note that since ψ is a ring homomorphism that it suffices to prove that $\ker \psi$ is trivial to establish that ψ is an injection. Now, let $d \in \ker \psi$ so that $\psi(d) = \beta_d$ is the zero map $V \to V$. That is, we have that

$$0 = \beta_d(v) = dv \quad \text{for each} \quad v \in V$$

For the sake of contradiction, suppose that d were nonzero. Then since D is a division ring and as $d \in D$ is nonzero, we may left-multiply both sides of the above equality by d^{-1} to obtain

$$0 = d^{-1}0 = d^{-1}(dv) = (d^{-1}d)v = 1v = v \quad \text{for each} \quad v \in V$$

However, this implies that $V = \{0\}$ which is a contradiction as $\dim_D(V) \geq 2$ by the above. Therefore, we have that $d = 0$ and hence $\ker \psi$ is trivial so that ψ is an injection. Finally, let $\beta_d \in Z$. Then clearly $d \in D$ and $\psi(d) = \beta_d$ so that ψ is a surjection. Combining the above results, then, we see that ψ is a ring isomorphism so that $D \simeq Z$.

To complete the proof, recall by the above that R is a dense subring of $\mathrm{End}_\Delta(V)$. Notice that by the previous two results we have that $\Delta = Z \simeq D$ so that $\Delta \simeq D$. Thus, by the initial observation made at the beginning of this paragraph we conclude that R is a dense subring of $\mathrm{End}_D(V)$. This completes the proof. $\square$

Problem 5. *If R is a primitive ring such that for all $a, b \in R$, we have $a(ab - ba) = (ab - ba)a$, then R is a division ring.*

Proof. Since R is a primitive ring, there is a faithful, simple R-module V. Now, since V is a simple R-module we have by Schur's Lemma that $\mathrm{End}_R(V)$ is a division ring. Recall that V is an vector space over $\mathrm{End}_R(V)$. We claim that $\dim_{\mathrm{End}_R(V)}(V) = 1$. For the sake of contradiction, suppose that $\dim_{\mathrm{End}_R(V)}(V) \neq 1$. If $\dim_{\mathrm{End}_R(V)}(V) = 0$, then we have $V = \{0\}$. But as V is a simple R-module, we have in particular that $V \neq \{0\}$ which is a contradiction. Thus, we see that $\dim_{\mathrm{End}_R(V)}(V) \geq 2$ and so there is an $\mathrm{End}_R(V)$-linearly independent subset $\{v_1, v_2\}$ of V.

Now, since V is a simple R-module and as $\{v_1, v_2\}$ is an $\mathrm{End}_R(V)$-linearly independent subset of V we may appeal to Jacobson's Density Theorem to assert that there is some $a \in R$ such that $av_1 = v_1$ and $av_2 = 0$. By the same reasoning, there is some $b \in R$ such that $bv_1 = 0$ and $bv_2 = v_1$. Thus, we see

$$a(ab - ba)v_2 = a^2bv_2 - abav_2 = a^2(bv_2) - ab(av_2) = a^2v_1 - ab0 = a(av_1) = av_1 = v_1$$

and

$$(ab - ba)av_2 = (ab - ba)0 = 0$$

so that by hypothesis we have

$$v_1 = a(ab - ba)v_2 = (ab - ba)av_2 = 0$$

However, recall that the subset $\{v_1, v_2\}$ of V is linearly independent so that in particular we have $v_1 \neq 0$ which contradicts the above equality and thus $\dim_{\mathrm{End}_R(V)}(V) = 1$.

Finally, since V is a faithful, simple R-module it follows that R is isomorphic to $\mathrm{End}_R(V)^{\mathrm{op}}$ by the above result. Furthermore, we have that $\mathrm{End}_R(V)^{\mathrm{op}}$ is a division ring as $\mathrm{End}_R(V)$ is a division ring. Thus, we conclude that R is a division ring. This completes the proof. $\square$

Problem 6. *If R is a primitive ring with identity and $e \in R$ is such that $e^2 = e \neq 0$, then:*

(a): *eRe is a subring of R, with identity e.*

(b): *eRe is primitive.*

Proof. (a): First, note that as $e \in R$ we have $eee \in eRe$ so that $eRe \neq \emptyset$. Next, let $er_1e, er_2e \in eRe$. Then as R is a ring, we have $r_1 - r_2 \in R$ and $r_1 + r_2 = r_2 + r_1$ so that

$$er_1e - er_2e = e(r_1 - r_2)e \in eRe$$

and

$$er_1e + er_2e = e(r_1 + r_2)e = e(r_2 + r_1)e = er_2e + er_1e$$

and hence we conclude that R is an abelian group under addition. Furthermore, since R is a ring and as $e, r_1, r_2 \in R$ we have that $r_1e^2r_2 \in R$ so that

$$(er_1e)(er_2e) = er_1e^2r_2e = e(r_1e^2r_2)e \in eRe$$

and hence eRe is closed under multiplication. Moreover, since R is a ring it follows that multiplication in eRe is associative and that the distributivity axiom holds for eRe. Thus, we conclude that eRe is a subring of R.

Finally, we show that e is an identity of eRe. Towards this end, let $ere \in eRe$. Then we have by hypothesis that

$$e(ere) = e^2re = ere$$

and

$$(ere)e = ere^2 = ere$$

so that e is an identity of eRe. This completes the proof. □

Proof. (b): Since R is primitive, there is a faithful, simple (left) R-module V. We claim that eV is a faithful, simple (left) eRe-module. First, we show that eV is an eRe-module. Towards this end, first note that $0 \in V$ as V is an R-module so that $0 = e0 \in eV$ so that $eV \neq \emptyset$. Next, let $ev_1, ev_2 \in V$. Then since V is an R-module, we have $v_1 - v_2 \in V$ and $v_1 + v_2 = v_2 + v_1$ so that

$$ev_1 - ev_2 = e(v_1 - v_2) \in eV$$

and

$$ev_1 + ev_2 = e(v_1 + v_2) = e(v_2 + v_1) = ev_2 + ev_1$$

and hence we conclude that eV is an abelian group under addition. Furthermore, suppose that $ere \in eRe$ and $ev \in eV$. Then since V is an R-module, we have since $re^2 \in R$ as R is a ring that $re^2v \in V$ and hence

$$(ere)ev = ere^2v = e(re^2v) \in eV$$

which shows that eRe acts on eV. The remaining module axioms are proven by continuing to use the fact that V is an R-module. We conclude that eV is an eRe-module.

Next, we show that eV is a faithful eRe-module. Towards this end, suppose that $ere \in \mathrm{Ann}_{eRe}(eV)$. Then we have by hypothesis that

$$0 = (ere)(ev) = ere^2v = erev = (ere)v \quad \text{for each} \quad v \in V$$

Now, recall that V is a faithful R-module so that $\mathrm{Ann}_R(V) = \{0\}$. Furthermore, since R is a ring we have $ere \in R$ and hence by the above equality we have that $ere \in \mathrm{Ann}_R(V) = \{0\}$ so that $ere = \{0\}$. Thus, since $ere \in \mathrm{Ann}_{eRe}(eV)$ was arbitrary we conclude that $\mathrm{Ann}_{eRe}(eV) = \{0\}$ and hence eV is a faithful eRe-module.

Finally, we show that eV is a simple eRe-module. Before we prove this result, we first show that $eV \neq \{0\}$. For the sake of contradiction, suppose that $eV = \{0\}$. Then we have since $e \in R$ that $e \in \mathrm{Ann}_R(V)$. But recall that $\mathrm{Ann}_R(V) = \{0\}$ and hence $e = 0$, which contradicts the fact that $e \neq 0$. Therefore, we see that $eV \neq \{0\}$ so that there is some nonzero element $ev \in eV$. Furthermore, since R has identity we have by hypothesis that

$$e = e^2 = ee = e1e \in eRe$$

and hence by hypothesis we obtain

$$0 \neq ev = e^2v = eev = e(ev) \in (eRe)(eV)$$

so that $(eRe)(eV) \neq \{0\}$.

Lastly, suppose that $W \subseteq eV$ is a nontrivial eRe-submodule of eV. Then there is some nonzero element $w \in W \subseteq eV$ so that $w = ev$ for some $v \in V$. In particular, since $e \in R, v \in V$, and as V is an R-module we have that $w = ev \in V$ is a nonzero element of V. Therefore, since R has identity we have that Rw is a nontrivial R-submodule of V so that since V is a simple R-module we obtain that $Rw = V$. Thus, we obtain by hypothesis that

$$(eRe)w = (eRe)(ev) = eRe^2v = eRev = eRw = eV$$

so that $(eRe)w = eV$. But recall that W is an eRe-module so that since $w \in W$ we have that $(eRe)w \subseteq W$. Combining this observation with the previous result, we obtain

$$W \supseteq (eRe)w = eV$$

and since $W \subseteq eV$ we conclude that $W = eV$. Combining the above results, we see that eV is a faithful, simple eRe-module. Therefore, we have that eRe is a primitive ring. This completes the proof. $\square$

Homework 24: Page 433 #7, 8, 9

Problem 7. *If R is the ring of all rational numbers with odd denominators, then $J(R)$ consists of all rational numbers with even numerator and odd denominator.*

Proof. Before we begin, we prove the following Lemma.

Lemma. Let R be a nonzero ring with identity. Then $J(R)$ is equal to the intersection of the maximal (left) ideals of R.

Proof. First, suppose that $x \in J(R)$ and let M be a maximal (left) ideal of R. Then as M is a maximal ideal of R, it follows by the Fourth Isomorphism Theorem for Rings that the R-module R/M is a contains no proper, nontrivial ideals of R. Furthermore, for the sake of contradiction suppose that $R(R/M)$ is trivial. Then since R has identity, we have that

$$R/M = 1(R/M) = M$$

so that $R \subseteq M$ so that $M = R$. However, this is a contradiction since M is a maximal ideal of R and hence in particular we have $M \neq R$. Thus, we conclude that $R(R/M) \neq \{0\}$ so that R/M is a simple R-module. Thus, since $x \in J(R)$ we have $x(R/M) = M$ so that $xR \subseteq M$. Hence, as $1 \in R$ we obtain

$$x = x \cdot 1 \in xR \subseteq M$$

On the other hand, suppose that x is in every maximal ideal of R and let A be a simple R-module. Now, since A is a simple R-module we have in particular that $A \neq \{0\}$ so that there is some nonzero element $a \in A$.

We claim that $\mathrm{Ann}(a)$ is a maximal ideal of R. Towards this end, define a map

$$\phi : R \to A \quad \text{by} \quad r \mapsto ra$$

Then ϕ is clearly an R-module homomorphism. Moreover, since R has identity we have that ϕ is a surjection and it is immediate that $\ker \phi = \mathrm{Ann}(a)$. Thus, by the First Isomorphism Theorem for Modules we obtain that $R/\mathrm{Ann}(a) \simeq A$. Finally, note that since A is a simple R-module and as $R/\mathrm{Ann}(a) \simeq A$ that in particular $R/\mathrm{Ann}(a)$ contains no proper, nontrivial ideals of R so that by the Fourth Isomorphism Theorem for Rings we conclude that $\mathrm{Ann}(a)$ is a maximal ideal of R.

Finally, recall that x is in every maximal ideal of R. Moreover, notice that by the above results that $\mathrm{Ann}(a)$ is a maximal ideal of R for each nonzero element $a \in A$. By the above result, then, we have that $xa = 0$ for each nonzero $a \in A$ and since clearly $x0 = 0$ we conclude that $xA = \{0\}$ so that $x \in \mathrm{Ann}(A)$. Since A was an arbitrary simple R-module, we conclude that $x \in J(R)$, completing the proof of the Lemma. $\square$

We now prove the main result. Let $S \subseteq R$ denote the set of all rational numbers with even numerators and odd denominators. Then clearly, we have $S = (2)$. We claim that S is the unique maximal ideal of R.

Towards this end, recall that it suffices to show that S is a proper ideal of R and that S contains all nonunits of R. Indeed, first note that since $1/1 \in R$ but clearly

$1/1 \notin S$ we have that S is properly contained in R. Next, suppose that $a/b \in R$ is a nonunit of R and for the sake of contradiction suppose that $a/b \notin S$. If $a/b = 0$, then this is a contradiction since clearly $0 \in S$. Therefore, we have $a/b \neq 0$.

Now, since $a/b \in S \subseteq R$ is a nonunit of R it follows that the inverse b/a of a/b in $\mathbb{Q}$ (which exists since $a/b \neq 0$) is not in R. In particular, this implies that the denominator a of b/a is even. Furthermore, since $a/b \in R$ we have that the denominator b of a/b is odd. Combining the previous two results, we see that $a/b \in S$ which is a contradiction. Therefore, we have that $a/b \in S$ and hence S is a proper ideal of R which contains all nonunits of R so that S is the unique maximal ideal of R.

Finally, since R has identity $1/1$ we have by the above Lemma that $J(R)$ is equal to the intersection of the maximal ideals of R. But since S is the unique maximal ideal of R, we conclude that $J(R) = S$. This completes the proof. $\square$

Problem 8. *Let R be the ring of all upper triangular $n \times n$ matrices over a division ring D. Find $J(R)$ and prove that $R/J(R)$ is isomorphic to the direct product $D \times \cdots \times D$ (n factors).*

Proof. Before we begin, we prove the following Lemma.

Lemma. Let R be a nonzero ring with identity and let I be an ideal of R with $I \subseteq J(R)$. Then $J(R/I) = J(R)/I$.

Proof. Recall by the previous Lemma that $J(R/I)$ is equal to the intersection of the maximal ideals of R/I and that $J(R) \supseteq I$ is equal to the intersection of the maximal ideals of R which contain I. Now, let M be a maximal ideal of R/I. Then by the Fourth Isomorphism Theorem for Rings, there is a maximal ideal N of R such that $I \subseteq N$ and $M = N/I$. Furthermore, since N is a maximal ideal of R we have by the observation made at the beginning of this proof that $J(R) \subseteq N$. Thus, we obtain that

$$J(R)/I \subseteq N/I = M$$

and hence since M was an arbitrary maximal ideal of R/I the above inclusion gives that $J(R)/I \subseteq J(R/I)$. On the other hand, let M be a maximal ideal of R such that $I \subseteq M$. Then by the Fourth Isomorphism Theorem for Rings, the ideal M/I is a maximal ideal of R/I. Thus, we have by the observation made at the beginning of this proof that $J(R/I) \subseteq M/I$ and since M was an arbitrary maximal ideal of R such that $I \subseteq M$ we may now conclude that $J(R/I) \subseteq J(R)/I$. This completes the proof of the Lemma. $\square$

We now prove the main result. Towards this end, let Z be the set of all upper triangular $n \times n$ matrices over D whose elements contain only zeros along their main diagonal. We claim that $J(R) = Z$. Clearly, we have that Z is an ideal of R and that $Z^n = \{0\}$ so that Z is a nilpotent ideal of R. Thus, we have that $Z \subseteq J(R)$. Next, define a map $\phi : R \to D^n$ that sends each upper triangular matrix in R to its main diagonal. Clearly, we see that ϕ is a surjective ring homomorphism with $\ker \phi = Z$ so that $R/Z \simeq D^n$ by the First Isomorphism Theorem for Rings.

Now, by the above results we have that Z is an ideal of R with $Z \subseteq J(R)$ and that $R/Z \simeq D^n$. In other words, we have that

$$R/Z \simeq D^n = \underbrace{D \times \cdots \times D}_{n \text{ times}} = \underbrace{\mathrm{Mat}_1(D) \times \cdots \times \mathrm{Mat}_1(D)}_{n \text{ times}}$$

and thus it follows that R/Z is a semisimple ring by the Wedderburn-Artin Theorem Part II. Therefore, we have $J(R/Z) = \{0\}$ so that by the above Lemma we obtain that

$$J(R)/Z = J(R/Z) = \{0\}$$

and hence we conclude that $J(R) = Z$. Finally note that since $J(R) = Z$, we now obtain

$$R/J(R) = R/Z \simeq D^n = \underbrace{D \times \cdots \times D}_{n \text{ times}}$$

This completes the proof. $\square$

Problem 9. *A PID R is semisimple if and only if R is a field or R contains an infinite number of distinct nonassociate irreducible elements.*

Proof. First, suppose that R is semisimple so that $J(R) = \{0\}$. For the sake of contradiction, suppose that R is not a field but only contains a finite number of distinct nonassociate irreducible elements, say $p_1, \ldots, p_n$. In particular, since $p_1, \ldots, p_n$ are irreducible elements of R we have that $p_1, \ldots, p_n \neq 0$.

Next, since R is a PID we know that the irreducible elements of R are exactly the prime elements of R and hence $p_1, \ldots, p_n$ are the distinct nonassociate prime elements of R. We claim that $(p_1), \ldots, (p_n)$ are precisely the nonzero prime ideals of R. Indeed, first notice that the ideals $(p_1), \ldots, (p_n)$ are nonzero prime ideals of R since $p_1, \ldots, p_n$ are prime elements of R. On the other hand, suppose that P is a nonzero prime ideal of R. Then since R is a PID, it follows that $P = (p)$ for some element $p \in R$. In particular, we have since P is nonzero that $p \neq 0$ and hence p is a prime element of R so that $p \in \{p_1, \ldots, p_n\}$ or p is associate to p_N for some $N \in \{1, \ldots, n\}$. Since associate elements generate the same ideal, then, we see in either case that $P = (p)$ is equal to one of $(p_1), \ldots, (p_n)$. Therefore, we conclude that $(p_1), \ldots, (p_n)$ are exactly the nonzero, prime ideals of R. Furthermore, recall that the nonzero prime ideals in a PID are precisely the maximal ideals. By the above result, then, we conclude that $(p_1), \ldots, (p_n)$ are exactly the maximal ideals of R.

Finally, recall by the first Lemma above that $J(R)$ is equal to the intersection of the maximal ideals of R. By the above result, then, we have that

$$J(R) = \bigcap_{i=1}^{n} (p_i)$$

and hence

$$p_1 \cdots p_n \in \bigcap_{i=1}^{n} (p_i) = J(R)$$

Moreover, recall that $p_1, \ldots, p_n$ are nonzero elements of R and since R is in particular an integral domain as R is a PID it follows that $p_1 \cdots p_n \neq 0$. However, this implies by the above that $J(R) \neq \{0\}$ which contradicts the fact that $J(R) = \{0\}$. We conclude that either R is a field or that R contains an infinite number of distinct nonassociate irreducible elements. This completes the proof of the first direction.

For the second direction, suppose first that R is a field. Let A be a simple R-module. Then since $\mathrm{Ann}(A)$ is an ideal of R and as R is a field, it follows that $\mathrm{Ann}(A) \in \{\{0\}, R\}$. However, if $\mathrm{Ann}(A) = R$ it follows that $RA = \{0\}$ which contradicts the fact that $RA \neq \{0\}$ since A is a simple R-module. Thus, we see that $\mathrm{Ann}(A) = \{0\}$ and since A was an arbitrary simple R-module it now follows that $J(R) = \{0\}$ so that R is primitive in this case.

Secondly, suppose that R has an infinite number of distinct nonassociate irreducible (hence prime, by the same reasoning as above) elements. Now, let $r \in R$ be a nonzero element of R. If r is a unit of R, we have that $(r) = R$. Therefore, if $r \in J(R)$ it follows

that $J(R) \supseteq (r) = R$ so that $J(R) = R$. However, recall that $J(R)$ is equal to the intersection of the maximal ideals of R which are in particular properly contained in R so that $J(R) \neq R$. Therefore, we conclude that $J(R)$ does not contain any units of R.

Next, suppose that $r \in R$ is a nonzero nonunit of R and recall that as R is a PID we have that R is a UFD so that since r is a nonzero nonunit of R it follows that only a finite number of prime elements of R can divide r. But since R has an infinite number of distinct nonassociate prime elements, it now follows that there is some prime element $p \in R$ such that p does not divide r so that $r \notin (p)$. Moreover, recall that the nonzero prime ideals in a PID are precisely the maximal ideals. Therefore, we have since p is a prime element of the PID R that (p) is a nonzero prime ideal of R and hence (p) is a maximal ideal of R. Thus, we see that (p) is a maximal ideal of R such that $r \notin (p)$.

Finally, let $r \in R$ be a nonzero element of R. If r is a unit, then $r \notin J(R)$ by the above. If r is a nonunit, then there is a maximal ideal M of R such that $r \notin M$. But since $J(R)$ is equal to the intersection of the maximal ideals of R and as M is a maximal ideal of R with $r \notin M$ we have that $r \notin J(R)$. Thus, we conclude that $J(R)$ contains no nonzero elements of R so that $J(R) = \{0\}$ and hence R is semisimple. This completes the proof. $\square$

Homework 25: #3, 4, 11

Problem 3. *A nonzero commutative semisimple left-Artinian ring is a direct product of fields.*

Proof. Since R is a nonzero semisimple left-Artinian ring we have by the Wedderburn-Artin Theorem Part II that

$$R \simeq \mathrm{Mat}_{n_1}(D_1) \times \cdots \times \mathrm{Mat}_{n_t}(D_t)$$

where $n_1, \ldots, n_t, t$ are positive integers and $D_1, \ldots, D_t$ are division rings. Furthermore, since R is commutative it follows by the above that $\mathrm{Mat}_{n_i}(D_i)$ is a commutative ring for each $i \in \{1, \ldots, t\}$. Therefore, since $\mathrm{Mat}_z(D)$ is a noncommutative ring for any integer $z \geq 2$ and any division ring D we must have that $n_1, \ldots, n_t = 1$ and hence

$$R \simeq \mathrm{Mat}_{n_1}(D_1) \times \cdots \times \mathrm{Mat}_{n_t}(D_t) = \mathrm{Mat}_1(D) \times \cdots \times \mathrm{Mat}_1(D_t) = D_1 \times \cdots \times D_t$$

Finally, note by the same reasoning as above that $D_1, \ldots, D_t$ are commutative rings and hence $D_1, \ldots, D_t$ are commutative division rings so that $D_1, \ldots, D_t$ are fields. Therefore, we see that R is the direct product of the fields $D_1, \ldots, D_t$. This completes the proof. $\square$

Problem 4. *Determine up to isomorphism all semisimple rings of order 1008. How many of them are commutative?*

Proof. Let R be a semisimple ring of order $1008 = 2^4 \cdot 3^2 \cdot 7$. Notice that since $|R| = 1008 > 1$ we have that R is nonzero and since $|R| = 1008 < \infty$ it is immediate that R is a left-Artinian ring. Since R is semisimple, then, we have by the Wedderburn-Artin Theorem Part II that

$$R \simeq \mathrm{Mat}_{n_1}(D_1) \times \cdots \times \mathrm{Mat}_{n_t}(D_t)$$

where $n_1, \ldots, n_t, t$ are positive integers and $D_1, \ldots, D_t$ are division rings. Also, since R is finite it follows by the above that $D_1, \ldots, D_t$ are finite. Thus, we see $D_1, \ldots, D_t$ are in particular finite division rings so that $D_1, \ldots, D_t$ are finite fields. Also, as $D_1, \ldots, D_t$ are finite fields we know that $|D_1|, \ldots, |D_t|$ are positive integer powers of prime numbers and that $D_1, \ldots, D_t$ are determined up to isomorphism by their respective orders.

Now, recall that given a positive integer m and a finite field D that $|\mathrm{Mat}_m(D)| = |D|^{m^2}$. Thus, by the above isomorphism we have

$$\begin{aligned} 2^4 \cdot 3^2 \cdot 7 = 1008 &= |R| \\ &= |\mathrm{Mat}_{n_1}(D_1) \times \cdots \times \mathrm{Mat}_{n_t}(D_t)| \\ &= |\mathrm{Mat}_{n_1}(D_1)| \cdots |\mathrm{Mat}_{n_t}(D_t)| \\ &= |D_1|^{n_1^2} \cdots |D_t|^{n_t^2} \end{aligned}$$

Let $\mathbb{F}_q$ denote the finite field of order q. Then by combining all of the above observations, we obtain the following:

The possible products of matrix rings whose orders contribute to the factor of 2^4 in $|R| = 1008$ are exactly the following:

- $M_2(\mathbb{F}_2)$
- $M_1(\mathbb{F}_{16}) = \mathbb{F}_{16}$
- $M_1(\mathbb{F}_4) \times M_1(\mathbb{F}_4) = \mathbb{F}_4 \times \mathbb{F}_4$
- $M_1(\mathbb{F}_4) \times M_1(\mathbb{F}_2) \times M_1(\mathbb{F}_2) = \mathbb{F}_4 \times \mathbb{F}_2 \times \mathbb{F}_2$
- $M_1(\mathbb{F}_2) \times M_1(\mathbb{F}_2) \times M_1(\mathbb{F}_2) \times M_1(\mathbb{F}_2) = \mathbb{F}_2 \times \mathbb{F}_2 \times \mathbb{F}_2 \times \mathbb{F}_2$

The possible products of matrix rings whose orders contribute to the factor of 3^2 in $|R| = 1008$ are exactly the following:

- $M_1(\mathbb{F}_9) = \mathbb{F}_9$
- $M_1(\mathbb{F}_3) \times M_1(\mathbb{F}_3) = \mathbb{F}_3 \times \mathbb{F}_3$

The possible products of matrix rings whose orders contribute to the factor of 7 in $|R| = 1008$ are exactly the following:

- $M_1(\mathbb{F}_7) = \mathbb{F}_7$

Finally, recall that $M_2(\mathbb{F}_2)$ is clearly not a commutative ring but that the fields $\mathbb{F}_{16}, \mathbb{F}_4, \mathbb{F}_3$, and $\mathbb{F}_3$ are in particular commutative rings. Moreover, recall that the product

of commutative rings is a commutative ring if and only if each factor in the product is a commutative ring. Combining the above results, then, we conclude that R is isomorphic to one of the following rings, each of which that we indicate to be either commutative or noncommutative:

- $M_2(\mathbb{F}_2) \times \mathbb{F}_9 \times \mathbb{F}_7$ (noncommutative)
- $M_2(\mathbb{F}_2) \times \mathbb{F}_3 \times \mathbb{F}_3 \times \mathbb{F}_7$ (noncommutative)
- $\mathbb{F}_{16} \times \mathbb{F}_9 \times \mathbb{F}_7$ (commutative)
- $\mathbb{F}_{16} \times \mathbb{F}_3 \times \mathbb{F}_3 \times \mathbb{F}_7$ (commutative)
- $\mathbb{F}_8 \times \mathbb{F}_2 \times \mathbb{F}_9 \times \mathbb{F}_7$ (commutative)
- $\mathbb{F}_8 \times \mathbb{F}_2 \times \mathbb{F}_3 \times \mathbb{F}_3 \times \mathbb{F}_7$ (commutative)
- $\mathbb{F}_4 \times \mathbb{F}_4 \times \mathbb{F}_9 \times \mathbb{F}_7$ (commutative)
- $\mathbb{F}_4 \times \mathbb{F}_4 \times \mathbb{F}_3 \times \mathbb{F}_3 \times \mathbb{F}_7$ (commutative)
- $\mathbb{F}_4 \times \mathbb{F}_2 \times \mathbb{F}_2 \times \mathbb{F}_9 \times \mathbb{F}_7$ (commutative)
- $\mathbb{F}_4 \times \mathbb{F}_2 \times \mathbb{F}_2 \times \mathbb{F}_3 \times \mathbb{F}_3 \times \mathbb{F}_7$ (commutative)
- $\mathbb{F}_2 \times \mathbb{F}_2 \times \mathbb{F}_2 \times \mathbb{F}_2 \times \mathbb{F}_9 \times \mathbb{F}_7$ (commutative)
- $\mathbb{F}_2 \times \mathbb{F}_2 \times \mathbb{F}_2 \times \mathbb{F}_2 \times \mathbb{F}_3 \times \mathbb{F}_3 \times \mathbb{F}_7$ (commutative)

The above is the complete list of the 10 isomorphism classes of semisimple rings of order 1008. In particular, by the above we see that exactly 8 of these 10 isomorphism classes are commutative. This completes the proof. $\square$

Problem 11. *Let R be the ring of 2×2 matrices over an infinite field.*

(a): *R has an infinite number of distinct proper left ideals, any two of which are isomorphic as left R-modules.*

(b): *There are infinitely many distinct pairs (B, C) such that B and C are minimal left ideals of R and $R = B \oplus C$.*

Proof. (a): Let F be an infinite field and let $R = \mathrm{Mat}_2(F)$. For $h, k \in F^\times$, define

$$I_h = \left\{ \begin{bmatrix} ah & 0 \\ bh & 0 \end{bmatrix} : a, b \in F \right\} \quad \text{and} \quad J_k = \left\{ \begin{bmatrix} 0 & ak \\ 0 & bk \end{bmatrix} : a, b \in F \right\}$$

Now, fix any $h, k \in F^\times$. Then I_h and J_k are clearly left ideals of R. Furthermore, notice that the identity matrix in R is clearly in neither I_h nor I_k so that I_h and I_k are properly contained in R. Finally, define $\mathcal{I} = \{I_h : h \in F^\times\}$ and $\mathcal{J} = \{J_k : k \in F^\times\}$ and let $\mathcal{A} = \mathcal{I} \cup \mathcal{J}$. Recall that F is an infinite field so that in particular $F^\times$ is infinite. Hence, it now follows that $\mathcal{I}$ and $\mathcal{J}$ are infinite so that $\mathcal{A} = \mathcal{I} \cup \mathcal{J}$ is also infinite.

Next, we show that any two elements of $\mathcal{A}$ are isomorphic as left R-modules. Indeed, suppose that $I, J \in \mathcal{A}$. First, suppose that not both I and J lie in either $\mathcal{I}$ or $\mathcal{J}$. Without loss of generality, assume that $I \in \mathcal{I}$ and $J \in \mathcal{J}$ so that $I = I_h$ for some $h \in F^\times$ and $J = J_k$ for some $k \in F^\times$. Define a map

$$\phi : I \to J \quad \text{by} \quad \begin{bmatrix} ah & 0 \\ bh & 0 \end{bmatrix} \mapsto \begin{bmatrix} 0 & ak \\ 0 & bk \end{bmatrix}$$

Then ϕ is clearly a well-defined surjective R-module homomorphism. Furthermore, suppose that $A \in \ker \phi$ so that $A \in \ker \phi \subseteq I$ so that we may write

$$A = \begin{bmatrix} ah & 0 \\ bh & 0 \end{bmatrix} \quad \text{for some} \quad a, b \in F$$

This gives that

$$\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} = \phi(A) = \phi\left(\begin{bmatrix} ah & 0 \\ bh & 0 \end{bmatrix} \right) = \begin{bmatrix} 0 & ak \\ 0 & bk \end{bmatrix}$$

so that $ak = 0 = bk$. Therefore, since $k \in F^\times$ and as F is in particular an integral domain as F is a field we may now conclude by the previous equalities that $a = 0 = b$ and hence

$$A = \begin{bmatrix} ah & 0 \\ bh & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

so that $\ker \phi$ is trivial. Thus, since ϕ is an R-module homomorphism we conclude that ϕ is injective. Combining the previous results, we see that ϕ is an R-module isomorphism so that $I \simeq J$. If $I, J \in \mathcal{I}$ or $I, J \in \mathcal{J}$, then an argument similar to the one presented above that allowed us to conclude that $I \simeq J$ gives once again that $I \simeq J$. Hence, in all cases we see for $I, J \in \mathcal{A}$ we have $I \simeq J$.

Finally, note by the above results that $\mathcal{A}$ is an infinite collection of distinct proper left ideals of R and that any two elements of $\mathcal{A}$ are isomorphic as left R-modules. This completes the proof. $\square$

Proof. (b): Before we prove the main result, we show that $\mathcal{A}$ consists of minimal left ideals of R. Indeed, let $I \in \mathcal{A}$ and first suppose that $I \in \mathcal{I}$ so that $I = I_h$ for some $h \in F^\times$. Now, notice that clearly $I \neq \{0\}$. Next, suppose that J is an ideal of R such that $\{0\} \subseteq J \subseteq I$ and suppose that $J \neq \{0\}$. Since J is a nonzero ideal of R and as $J \subseteq I$, it follows that there is some nonzero element in J which can be written

$$\begin{bmatrix} ah & 0 \\ bh & 0 \end{bmatrix} \quad \text{for some} \quad a, b \in F \quad \text{with not both} \quad a, b = 0$$

Now, let

$$\begin{bmatrix} ch & 0 \\ dh & 0 \end{bmatrix} \in I$$

If $a \in F$ is nonzero, then a^{-1} exists in F as F is a field and hence we have

$$\begin{bmatrix} ca^{-1} & 0 \\ da^{-1} & 0 \end{bmatrix} \in R$$

so that since J is a left ideal of R we have

$$\begin{bmatrix} ch & 0 \\ dh & 0 \end{bmatrix} = \begin{bmatrix} ca^{-1} & 0 \\ da^{-1} & 0 \end{bmatrix} \begin{bmatrix} ah & 0 \\ bh & 0 \end{bmatrix} \in J$$

If $a = 0$, then by the above we have that $b \in F$ is nonzero so that b^{-1} exists in F as F is a field and hence we have

$$\begin{bmatrix} 0 & cb^{-1} \\ 0 & db^{-1} \end{bmatrix} \in R$$

so that since J is a left ideal of R we have

$$\begin{bmatrix} ch & 0 \\ dh & 0 \end{bmatrix} = \begin{bmatrix} 0 & cb^{-1} \\ 0 & db^{-1} \end{bmatrix} \begin{bmatrix} 0 & 0 \\ bh & 0 \end{bmatrix} = \begin{bmatrix} 0 & cb^{-1} \\ 0 & db^{-1} \end{bmatrix} \begin{bmatrix} ah & 0 \\ bh & 0 \end{bmatrix} \in J$$

Thus, we now have $I \subseteq J$ and as $J \subseteq I$ we obtain $J = I$. It now follows that I is a minimal left ideal of R in the case when $I \in \mathcal{I}$. If $I \in \mathcal{J}$, then an argument similar to the one presented above shows that I is a minimal left ideal of R. We may now conclude that $\mathcal{A}$ consists of minimal left ideals of R.

We now prove the main result. Towards this end, fix any $B \in \mathcal{I}$ and $C \in \mathcal{J}$ so that $B = I_h$ for some $h \in F^\times$ and $C = J_k$ for some $k \in F^\times$. We claim that $R = B \oplus C$. Towards this end, first notice that by the definition of membership in $\mathcal{I}$ and $\mathcal{J}$ that clearly $B \cap C = \{0\}$. Next, let

$$\begin{bmatrix} n_1 & n_2 \\ n_3 & n_4 \end{bmatrix} \in R$$

Now, since $h, k \in F^\times$ we have in particular that h^{-1} and k^{-1} exist in F. Furthermore, we clearly have $n_1h^{-1}, n_3h^{-1} \in F$ and $n_2k^{-1}, n_4k^{-1} \in F$ as F is a field. Thus, we have

$$\begin{bmatrix} n_1 & 0 \\ n_3 & 0 \end{bmatrix} = \begin{bmatrix} (n_1h^{-1})h & 0 \\ (n_3h^{-1})h & 0 \end{bmatrix} \in B$$

and

$$\begin{bmatrix} 0 & n_2 \\ 0 & n_4 \end{bmatrix} = \begin{bmatrix} 0 & (n_2k^{-1})k \\ 0 & (n_4k^{-1})k \end{bmatrix} \in C$$

so that

$$\begin{bmatrix} n_1 & n_2 \\ n_3 & n_4 \end{bmatrix} = \begin{bmatrix} n_1 & 0 \\ n_3 & 0 \end{bmatrix} + \begin{bmatrix} 0 & n_2 \\ 0 & n_4 \end{bmatrix} \in B + C$$

We may now conclude that $R = B + C$. Combining the previous results, then, we have that $R = B \oplus C$.

Finally, by the above results we have that for each pair (B, C) where $B \in \mathcal{I}$ and $C \in \mathcal{J}$ we have that $R = B \oplus C$. Furthermore, recall that $\mathcal{A} = \mathcal{I} \cup \mathcal{J}$ is infinite and that each element of $\mathcal{A}$ is a minimal left ideal of R. Combining all of the previous results, then, we conclude that there are infinitely many distinct pairs (B, C) such that B and C are minimal left ideals of R and $R = B \oplus C$. This completes the proof. $\square$

Homework 26: Page 462 #2, 3, 4

Problem 2. *If A and B are central simple algebras over a field K, then so is $A \otimes_K B$.*

Proof. Before we prove the main result, we show that $Z(A \otimes_K B) = Z(A) \otimes_K Z(B)$. Towards this end, first suppose that $z \in Z(A \otimes_K B)$ and write $z = \sum_{i=1}^n a_i \otimes_K b_i$ for some $a_1, \ldots, a_n \in A$ and $b_1, \ldots, b_n \in B$ and we may assume without loss of generality that $a_1, \ldots, a_n$ are linearly independent over K and that $b_1, \ldots, b_n$ are linearly independent over K. Now, fix any element $a \in A$. Then since $z \in Z(A \otimes_K B)$, we have that

$$\begin{aligned}
0 &= z(a \otimes_K 1_B) - (a \otimes_K 1_B)z \\
&= \sum_{i=1}^n [(a_i \otimes_K b_i)(a \otimes_K 1_B)] - \sum_{i=1}^n [(a \otimes_K 1_B)(a_i \otimes_K b_i)] \\
&= \sum_{i=1}^n (a_i a \otimes_K b_i) - \sum_{i=1}^n (a a_i \otimes_K b_i) \\
&= \sum_{i=1}^n [(a_i a \otimes_K b_i) - (a a_i \otimes_K b_i)] \\
&= \sum_{i=1}^n [(a_i a - a a_i) \otimes_K b_i]
\end{aligned}$$

Furthermore, recall that $b_1, \ldots, b_n$ are linearly independent over K. By the above equality, then, we conclude that $a_i a - a a_i = 0$ so that $a_i a = a a_i$ for each $i \in \{1, \ldots, n\}$. Thus, since $a \in A$ was arbitrary this shows that $a_i \in Z(A)$ for each $i \in \{1, \ldots, n\}$. Now, by using the same argument that was presented above we may also conclude that $b_i \in Z(B)$ for each $i \in \{1, \ldots, n\}$.

Combining the previous results, then, we see that $a_i \otimes_K b_i \in Z(A) \otimes_K Z(B)$ for each $i \in \{1, \ldots, n\}$ so that

$$z = \sum_{i=1}^n a_i \otimes_K b_i \in Z(A) \otimes_K Z(B)$$

On the other hand, suppose that $z \in Z(A) \otimes_K Z(B)$ and write $z = \sum_{i=1}^n a_i \otimes_K b_i$ for some $a_1, \ldots, a_n \in Z(A)$ and $b_1, \ldots, b_n \in Z(B)$. Now, let $a \otimes_K b \in A \otimes_K B$. Then since

$a_1, \ldots, a_n \in Z(A)$ and $b_1, \ldots, b_n \in Z(B)$, we obtain

$$\begin{aligned} z(a \otimes_K b) &= \sum_{i=1}^{n} [(a_i \otimes_k b_i)(a \otimes_K b)] \\ &= \sum_{i=1}^{n} (a_i a \otimes_K b_i b) \\ &= \sum_{i=1}^{n} (a a_i \otimes_K b b_i) \\ &= \sum_{i=1}^{n} [(a \otimes_K b)(a_i \otimes_K b_i)] \\ &= (a \otimes_K b) z \end{aligned}$$

Therefore, we see that z commutes with each elementary tensor of $A \otimes_K B$ so that since every element of $A \otimes_K B$ is a finite sum of elementary tensors of $A \otimes_K B$ we obtain that $z \in Z(A \otimes_K B)$. By the above results, then, we see that $Z(A \otimes_K B) = Z(A) \otimes_K Z(B)$.

Finally, recall that since A is a central simple algebra over K and as B is a central simple algebra over K so that B is in particular a simple algebra over K that we have $A \otimes_K B$ is a simple algebra over K. Therefore, it remains to prove that $Z(A \otimes_K B) = K$ to complete the proof. Indeed, since A and B are central simple algebras over K we have that $Z(A) = K = Z(B)$. Thus, by our preliminary result above we obtain

$$Z(A \otimes_K B) = Z(A) \otimes_K Z(B) = K \otimes_K K = K$$

We conclude that $Z(A \otimes_K B) = K$, completing the proof. $\square$

Problem 3. *Let D be a division ring and F a subfield. If $d \in D$ commutes with every element of F, then the subdivision ring $F[d]$ generated by F and d (the intersection of all subdivision rings of D containing F and d) is a subfield.*

Proof. Notice that in order to prove that $F[d]$ is a field that it remains to show that $F[d]$ is commutative. Towards this end, suppose that $x, y \in F[d]$ so that we may write

$$x = \sum_{i=0}^{n} a_i d^i \quad \text{and} \quad y = \sum_{i=0}^{m} b_i d^i \quad \text{for some} \quad a_1, \ldots, a_n, b_1, \ldots, b_m \in F$$

Now, since F is a field we have in particular that F is commutative. Moreover, recall by hypothesis that d commutes with every element of F. By these observations, then, it now follows by the above equalities for x and y that

$$xy = \sum_{i=0}^{n} a_i d^i \cdot \sum_{i=0}^{m} b_i d^i = \sum_{i=0}^{n+m} \left(\sum_{j=0}^{i} a_i b_{i-j} \right) d^i = \sum_{i=0}^{m} b_i d^i \cdot \sum_{i=0}^{n} a_i d^i = yx$$

so that $xy = yx$. Therefore, since $x, y \in F[d]$ were arbitrary this shows that $F[d]$ is commutative. By our observation made at the beginning of this proof, then, we conclude that $F[d]$ is a field and hence $F[d]$ is a subfield of D. This completes the proof. $\square$

Problem 4. *If D is a division ring, then D contains a maximal subfield.*

Proof. First, let $\mathcal{S}$ denote the collection of all commutative subrings with identity of D. Then $Z(D) \subseteq D$ is clearly a commutative subring with identity of D so that $Z(D) \in \mathcal{S}$ and hence $\mathcal{S} \neq \emptyset$. Now, partially order $\mathcal{S}$ by inclusion of sets and let $\mathcal{C}$ be a nonempty chain in $\mathcal{S}$. Define

$$J = \bigcup_{C \in \mathcal{C}} C$$

Then since $\mathcal{C}$ is a chain and as each $C \in \mathcal{C}$ is a subring with identity of D, we see that J is a subring with identity of D. Moreover, since each $C \in \mathcal{C}$ is commutative it is immediate by the definition of J that J is commutative. Therefore, we see that J is a commutative subring with identity of D so that $J \in \mathcal{S}$ is clearly an upper bound for $\mathcal{C}$. By Zorn's Lemma, we conclude that there is a maximal element $F \in \mathcal{S}$.

Finally, we show that F is a maximal subfield of D. Indeed, first note that as $F \in \mathcal{S}$ we see that F is a commutative subring with identity of the division ring D so that F is a field and hence F is a subfield of D. We claim that F is a maximal subfield of D. Towards this end, suppose that K is a subfield of D with $F \subseteq K$. Then we have in particular that K is a commutative subring with identity of D and hence $K \in \mathcal{S}$. By the maximality of $F \in \mathcal{S}$, then, we conclude that $K = F$. We conclude that F is a maximal subfield of D and hence D contains a maximal subfield. This completes the proof. $\square$

Section III: Ph.D Exam Practice Problems

Part 1: Randoms from Group Theory

Problem 1. *Suppose that G is a finite group.*

(a): *Prove that if G is nilpotent, and H is any proper subgroup, then H is a proper subgroup of its normalizer.*

(b): *Use (a) to prove that G is nilpotent if and only if it is isomorphic to a finite direct product of p-groups.*

Proof. (a): Since G is nilpotent, there exists a series of normal subgroups of G

$$\{1\} = N_0 \subseteq N_1 \subseteq \cdots \subseteq N_r = G$$

where r is a nonnegative integer and $N_i/N_{i-1} \subseteq Z(G/N_{i-1})$ for each $i \in \{1, \ldots, r\}$. Now, since H is a proper subgroup of G, we have that $N_0 \subseteq H$ and $N_r = G \nsubseteq H$. Therefore, there is some index $k \in \{0, \ldots, r-1\}$ such that $N_k \subseteq H$ but $N_{k+1} \nsubseteq H$.

Now, by the above, we have

$$N_{k+1}/N_k \subseteq Z(G/N_k) \subseteq N_{G/N_k}(H/N_k) = N_G(H)/N_k$$

In particular, since $N_k \subseteq H \subseteq N_G(H)$, we have that $N_{k+1} \subseteq N_G(H)$.

Finally, suppose for the sake of contradiction that $H = N_G(H)$. By the previous inclusion, this gives $N_{k+1} \subseteq N_G(H) = H$. However, this contradicts the fact that $N_{k+1} \nsubseteq H$. Therefore, we have $H \neq N_G(H)$. In particular, since every group is a subgroup of its normalizer, it now follows that H is a proper subgroup of its normalizer. $\square$

Proof. (b): For the first direction, assume that G is nilpotent. If G is trivial, then G is clearly isomorphic to a finite direct product of p-groups. So, assume that G is nontrivial and let $p_1, \ldots, p_n$ be a complete list of the distinct prime numbers dividing $|G|$, where n is a positive integer. For each $i \in \{1, \ldots, n\}$, let $P_i \in \mathrm{Syl}_{p_i}(G)$.

Now, fix $m \in \{1, \ldots, n\}$. Since P_m is a Sylow p_m-subgroup of G, it follows that $N_G(N_G(P_m)) = N_G(P_m)$. If $N_G(P_m)$ were a proper subgroup of G, then by the above, we have that $N_G(P_m)$ is a proper subgroup of $N_G(N_G(P_m))$ which is not the case since $N_G(N_G(P_m)) = N_G(P_m)$. Hence, $N_G(P_m) = G$ so that $P_m \triangleleft G$. Since $m \in \{1, \ldots, n\}$ was arbitrary, it follows that $P_1, \ldots, P_n \trianglelefteq G$.

Next, define $H = \prod_{i=1}^n P_i$. Then H is a group since $P_1, \ldots, P_n \trianglelefteq G$. Furthermore, clearly, we have

$$|H| \leq \prod_{i=1}^n |P_i|$$

On the other hand, we have that $|P_i|$ divides $|H|$ for each $i \in \{1, \ldots, n\}$ by Lagrange's Theorem. In particular, since the orders of $P_1, \ldots, P_n$ are pairwise relatively prime, we

have that $\prod_{i=1}^{n} |P_i|$ divides $|H|$. But by the above inequality, this gives

$$|H| = \prod_{i=1}^{n} |P_i| = |G|$$

Hence, since $H \subseteq G$, this gives that $G = H$.

Finally, fix $m \in \{1, \ldots, n\}$. For the sake of contradiction, assume that there were some nonidentity element x of G in the intersection

$$P_m \cap \prod_{i=1, i \neq m}^{n} P_i$$

Since the above product is a group, it follows by Lagrange's Theorem that $|x| > 1$ must divide $|P_m|$ and the order of the above product. Now, note that since the orders of $P_1, \ldots, P_{m-1}, P_{m+1}, \ldots, P_n$ are pairwise relatively prime, we have

$$\left| \prod_{i=1, i \neq m}^{n} P_i \right| = \prod_{i=1, i \neq m}^{n} |P_i|$$

Now, since $|P_m|$ is a positive power of the prime p_m, it follows that $|x|$ is a positive power of the prime p_m. However, p_m does not divide the order of the above product so that $|x|$ cannot divide the order of the above product. This is a contradiction. Therefore, we conclude that

$$P_m \cap \prod_{i=1, i \neq m}^{n} P_i = 1$$

Since $m \in \{1, \ldots, n\}$ was arbitrary, combining the previous results gives that G is equal to the (finite) direct product of $P_1, \ldots, P_n$. Since $P_1, \ldots, P_n$ are p-groups, this completes the proof of the first direction.

Conversely, assume that G is isomorphic to a finite direct product of p-groups, say

$$G = \bigoplus_{i=1}^{n} G_i$$

It is immediate that

$$Z_1(G) = Z(G) = \bigoplus_{i=1}^{n} Z(G_i) = \bigoplus_{i=1}^{n} Z_1(G_i)$$

Similarly, we have

$$Z_2(G) = \frac{G}{Z(G)} = \bigoplus_{i=1}^{n} \frac{G_i}{Z(G_i)} = \bigoplus_{i=1}^{n} Z_2(G_i)$$

Inductively, for each positive integer m, we obtain

$$Z_m(G) = \bigoplus_{i=1}^{n} Z_m(G_i)$$

Now, since G_i is a p-group we have that G_i is nilpotent for each $i \in \{1, \ldots, n\}$. Hence, for each $i \in \{1, \ldots, n\}$, we may define r_i to be the nilpotency class of G_i. Set $r = \max\{r_1, \ldots, r_n\}$. Then we have by the above that

$$Z_r(G) = \bigoplus_{i=1}^{n} Z_r(G_i) = \bigoplus_{i=1}^{n} G_i = G$$

Hence, we conclude that G is nilpotent. This completes the proof of the second direction. $\square$

Problem 2. (a): *Show that A_5 is simple.*
(b): *Use (a) to show that S_n is not solvable for $n \geq 5$.*

Proof. (a): First, note that the cycle types of elements in A_5 are

$$(1,1,1,1,1) \quad (2,2,1) \quad (3,1,1) \quad (5)$$

Now, note the following:

There is 1 element of the cycle type $(1,1,1,1,1)$.
There are $\frac{5\cdot4\cdot3\cdot2}{2\cdot2\cdot2} = 15$ elements of the cycle type $(2,2,1)$.
There are $\frac{5\cdot4\cdot3}{3} = 20$ elements of the cycle type $(3,1,1)$.
There are $\frac{5\cdot4\cdot3\cdot2\cdot1}{5} = 24$ elements of the cycle type (5).

Recall that a conjugacy class of S_5 that is contained in A_5 splits evenly into two distinct A_5 conjugacy classes if and only if the cycle type of the elements in that conjugacy class consist of distinct odd positive integers. Therefore, by the above, we have that H_1, H_2, H_3, H_4, H_5 are the distinct conjugacy classes of A_5, where H_1 corresponds to the elements of A_5 of the $(1,1,1,1,1)$ cycle type, H_2 corresponds to the elements of A_5 of the $(2,2,1)$ cycle type, H_3 corresponds to the elements of A_5 of the $(3,1,1)$ cycle type, and H_4 and H_5 correspond to the elements of A_5 of the (5) cycle type. Thus, by the above, we have

$$|H_1| = 1 \quad |H_2| = 15 \quad |H_3| = 20 \quad |H_4| = 12 = |H_5|$$

Now, for the sake of contradiction, suppose that A_5 were not simple. Then there exists a nontrivial, proper, normal subgroup H of A_5. Before continuing with the proof, we prove that if N is a normal subgroup of a group G and K is a conjugacy class of G then either $K \subseteq N$ or $K \cap N = \emptyset$. Indeed, suppose that $N \trianglelefteq G$ and that $K \cap N \neq \emptyset$. Then there is some $x \in K \cap N$. Note that for every $g \in G$ we have $gxg^{-1} \in N$ since $N \trianglelefteq G$. That is, N contains all conjugates of x so that $K \subseteq N$, as desired.

We now apply this result to the above normal subgroup N to assert that N is a (disjoint) union of conjugacy classes of A_5. In particular, this implies that $|N|$ is a sum of the orders of some subset of $H_1, \ldots, H_5$. But we also know by Lagrange's Theorem that $|N|$ divides $|A_5| = 60 = 2^2 \cdot 3 \cdot 5$. Furthermore, since N is nontrivial and properly contained in A_5, it follows that $|N| \neq 1$ and $|N| \neq |A_5| = 60$. However, note that no sum of $|H_1|, \ldots, |H_5|$ that is not equal to 1 or 60 can divide $|A_5|$. This is a contradiction. Therefore, we conclude that there is no such subgroup N as above so that A_5 is simple by definition. $\square$

Proof. (b): Using induction, we can show that A_n is simple for each integer $n \geq 5$ by utilizing the above result as proof of the base case.

Now, let $n \geq 5$ be an integer and consider S_n. Note that since A_n is of index 2 in S_n that A_n is the largest proper, normal subgroup of S_n. Furthermore, by the above result, we know that A_n is simple so that the only proper, normal subgroup of A_n is

$\{1\}$. Finally, suppose that

$$\{1\} = N_0 \trianglelefteq N_1 \trianglelefteq \cdots \trianglelefteq N_r = S_n$$

is a subnormal series of S_n such that N_i/N_{i-1} is abelian for each $i \in \{1, \ldots, r\}$.

If A_n did not appear in the above subnormal series, then by the above argument, we know that $N_m/N_{m-1} = S_n/\{1\}$ for some $m \in \{1, \ldots, r\}$. However, this would imply that S_n is abelian which is not the case since $n \geq 5$. Therefore, we conclude that A_n must appear in the above subnormal series. However, by the same argument as just presented, this would imply that A_n is abelian, which is not the case since $n \geq 5$.

By the above contradictions, we conclude that no such subnormal series of S_n exists. In particular, this implies that S_n is not solvable, completing the proof. $\square$

Problem 3. *A proper subgroup M of G is maximal if whenever $M \leq H \leq G$, we have $H = M$ or $H = G$. Suppose that G is a finite group has only one maximal subgroup. Prove that G is cyclic of prime power order.*

Proof. Let M be the unique maximal subgroup of G. Since M is properly contained in G, there is some element $g \in G - M$. Now, let $H = \langle g \rangle$. For the sake of contradiction, suppose that $H \neq G$. In particular, this implies that H is a proper subgroup of G so that there is some maximal subgroup K of G such that $H \subseteq K$. But since M is the unique maximal subgroup of G, it follows that $K = M$ so that

$$g \in \langle g \rangle = H \subseteq M$$

However, this contradicts the fact that $g \in G - M$. Thus, we conclude that $\langle g \rangle = H = G$ so that G is a cyclic group.

We now show that G has prime power order. For the sake of contradiction, suppose that $|G|$ were not the power of a prime. Let $p_1, \ldots, p_n$ be a complete list of the distinct prime numbers dividing $|G|$. Then by our assumption, we have that $n \geq 2$.

Now, for each $i \in \{1, \ldots, n\}$ let $P_i \in \mathrm{Syl}_{p_i}(G)$. Since $n \geq 2$, it follows that for each $i \in \{1, \ldots, n\}$ that P_i is a proper subgroup of G so that P_i is contained in some maximal subgroup K_i of G. But since M is the unique maximal subgroup of G, it follows that $K_i = M$ so that $P_i \subseteq M$ for each $i \in \{1, \ldots, n\}$. Hence, we obtain the inclusion

$$\prod_{i=1}^{n} P_i \subseteq M$$

In particular, by order considerations, note that since $P_1, \ldots, P_n$ pairwise intersect in only the identity. Therefore, we have

$$|M| \geq \left| \prod_{i=1}^{n} P_i \right| = \prod_{i=1}^{n} |P_i| = |G|$$

Thus, since $M \subseteq G$, it now follows that $|M| = |G|$ so that $M = G$. However, this contradicts the fact that M is properly contained in G. We conclude that there is only one prime number dividing $|G|$ so that G is of prime power order. $\square$

Problem 4. *Suppose that F is a free group on the alphabet X, and that Y is a subset of X. Let H be the least normal subgroup of F containing Y. Prove that F/H is a free group.*

Proof. We will show that F/H is free on the set $X-Y$ in the category of groups. Towards this end, let $j : X-Y \to X$ and $i : X \to F$ be the inclusion maps and let $\pi : F \to F/H$ be the canonical projection. Define $k = \pi \circ i \circ j$. Then we have $k : X - Y \to F/H$.

Now, let G be a group and let $f : X - Y \to G$ be a map of sets. Define $g : X \to G$ by $g(x) = f(x)$ for every $x \in X - Y$ and $g(y) = 1_G$ for every $y \in Y$, where 1_G denotes the identity of G. Since F is free on X, there exists a unique group homomorphism $\overline{g} : F \to G$ such that $\overline{g} \circ i = g$. Note that if $y \in Y$ then we have

$$\overline{g}(y) = \overline{g}(i(y)) = g(y) = 1_G$$

which shows that $Y \subseteq \ker(\overline{g})$ so that $\ker(\overline{g})$ is a normal subgroup of F containing Y. Hence, we have $H \subseteq \ker(\overline{g})$. In particular, this shows that there exists a group homomorphism $\overline{\overline{g}} : F/H \to G$ such that $\overline{\overline{g}} \circ \pi = \overline{g}$. The above results give that

$$\overline{\overline{g}} \circ k = \overline{\overline{g}} \circ \pi \circ i \circ j = \overline{g} \circ i \circ j = g \circ j = f$$

so that $\overline{\overline{g}} \circ k = f$.

It remains to prove that $\overline{\overline{g}}$ is unique. Suppose that $\phi_1, \phi_2 : F/H \to G$ are group homomorphisms such that $\phi_1 \circ k = f = \phi_2 \circ k$. Note that for $x \in X - Y$ we have

$$\phi_1(\pi(i(x))) = \phi_1(\pi(i(j(x)))) = \phi_1(k(x)) = \phi_2(k(x)) = \phi_2(\pi(i(j(x)))) = \phi_2(\pi(i(x)))$$

Furthermore, for $y \in Y$ we have since $Y \subseteq H$ and since ϕ_1 and ϕ_2 are group homomorphisms that

$$\phi_1(\pi(i(y))) = \phi_1(\pi(y)) = \phi_1(yH) = \phi(H) = 1_G$$

and

$$\phi_2(\pi(i(y))) = \phi_2(\pi(y)) = \phi_2(yH) = \phi(H) = 1_G$$

so that $\phi_1(\pi(i(y))) = \phi_2(\pi(i(y)))$. The above results show that $\phi_1(\pi(i(x)))) = \phi_2(\pi(i(x)))$ for all $x \in X$. Hence, we obtain $\phi_1 \circ \pi \circ i = \phi_2 \circ \pi \circ i$.

Now, notice that if $x \in X - Y$ we have

$$\phi_1(\pi(i(x))) = \phi_1(\pi(i(j(x)))) = \phi_1(k(x)) = f(x) = g(x)$$

Furthermore, for $y \in Y$, the above result gives

$$\phi_1(\pi(i(y))) = 1_G = g(y)$$

The above results show that $\phi_1(\pi(i(x))) = g(x)$ for all $x \in X$ so that $\phi_1 \circ \pi \circ i = g$. Since $\phi_1 \circ \pi \circ i = \phi_2 \circ \pi \circ i$ by the above, we now have

$$\phi_1 \circ \pi \circ i = g = \phi_1 \circ \pi \circ i$$

Furthermore, since the composition of group homomorphisms is a group homomorphism, we have $\phi_1 \circ \pi$ and $\phi_2 \circ \pi$ are group homomorphisms. Thus, since F is free on X, the above equality shows that $\phi_1 \circ \pi = \phi_2 \circ \pi$.

Finally, since π is a surjection, we obtain $\phi_1 = \phi_2$ since $\phi_1 \circ \pi = \phi_2 \circ \pi$. This proves that $\overline{\overline{g}}$ is unique and hence F/H is free on $X - Y$ in the category of groups. $\square$

Problem 5. *Let G be the group defined by two generators a and b, with relations $a^2 = b^3 = e$. Prove that it is infinite and nonabelian.*

Proof. Let $X = \{a, b\}, R = \{a^2, b^3\}$, and N be the smallest normal subgroup of F with $R \subseteq N$ where F is the free group on X. By definition, we have that the group defined by the generators X and relations R is F/N.

Before we begin, we prove that if $\theta : H \to K$ is a surjective group homomorphism and if K is nonabelian then H is nonabelian. Indeed, since K is nonabelian, there exist $k_1, k_2 \in K$ such that $k_1k_2 \neq k_2k_1$. As θ is a surjection, there exist $h_1, h_2 \in H$ such that $\theta(h_1) = k_1$ and $\theta(h_2) = k_2$. Since θ is a group homomorphism, this gives

$$k_1k_2 = \theta(h_1)\theta(h_2) = \theta(h_1h_2)$$

and

$$k_2k_1 = \theta(h_2)\theta(h_1) = \theta(h_2h_1)$$

Hence, if $h_1h_2 = h_2h_1$ then the above results would imply that

$$k_1k_2 = \theta(h_1h_2) = \theta(h_2h_1) = k_2k_1$$

which is a contradiction since $k_1k_2 \neq k_2k_1$. Thus, we have $h_1h_2 \neq h_2h_1$ so that H is nonabelian. This proves the result.

We now prove the main result. Towards this end, consider $\sigma_1, \sigma_2 \in S_{\mathbb{Z}}$ given by

$$\sigma_1 = \cdots(-4 \quad -3)(-1 \quad 0)(2 \quad 3)\cdots$$

and

$$\sigma_2 = \cdots(-3 \quad -2 \quad -1)(0 \quad 1 \quad 2)(3 \quad 4 \quad 5)\cdots$$

Clearly, we have $|\sigma_1| = 2$ and $|\sigma_2| = 3$. Let $H = \langle \sigma_1, \sigma_2 \rangle \subseteq S_{\mathbb{Z}}$ and define

$$f : X \to H \quad \text{by} \quad a \mapsto \sigma_1 \quad b \mapsto \sigma_2$$

Since F is free on X, there exists a unique group homomorphism $\overline{f} : F \to H$ such that

$$\overline{f}(a) = f(a) = \sigma_1 \quad \text{and} \quad \overline{f}(b) = f(b) = \sigma_2$$

Note that since $\overline{f}$ is a group homomorphism we have

$$\overline{f}(a^2) = \overline{f}(a)\overline{f}(a) = \sigma_1 \cdot \sigma_1 = \sigma_1^2 = 1$$

and

$$\overline{f}(b^3) = \overline{f}(b)\overline{f}(b)\overline{f}(b) = \sigma_2 \cdot \sigma_2 \cdot \sigma_2 = \sigma_2^3 = 1$$

In particular, the above shows that $R \subseteq \ker(\overline{f})$. Since $\ker(\overline{f})$ is a normal subgroup of F with $R \subseteq \ker(\overline{f})$, it follows by the definition of N that $N \subseteq \ker(\overline{f})$.

The above results show that there exists a group homomorphism $g : F/N \to H$ such that $g(aN) = \sigma_1$ and $g(bN) = \sigma_2$. Note that since $H = \langle \sigma_1, \sigma_2 \rangle$ and since $\sigma_1, \sigma_2 \in g(F/N)$ we have that g is a surjection. Furthermore, we see that $S_{\mathbb{Z}}$ is nonabelian since for $(1 \quad 2), (1 \quad 2 \quad 3) \in S_{\mathbb{Z}}$ we have

$$(1 \quad 2)(1 \quad 2 \quad 3) = (2 \quad 3) \neq (1 \quad 3) = (1 \quad 2 \quad 3)(1 \quad 2)$$

By our preliminary result, then, this shows that F/N is nonabelian.

Now, since g is a surjection, we have that $|F/N| \geq |H|$. We claim that H is infinite. Indeed, consider the orbit $\mathcal{O}$ of $0 \in \mathbb{Z}$ in the action of H on $\mathbb{Z}$. In particular, we have that $\mathcal{O} = \mathbb{Z}$ by the definition of H. By the Orbit-Stabilizer Theorem, we have that

$$\infty = |\mathbb{Z}| = |\mathcal{O}| = |H : \mathrm{Stab}_H(0)|$$

so that

$$|H| = \infty \cdot |\mathrm{Stab}_H(0)| = \infty$$

By the above, this gives

$$|F/N| \geq |H| = \infty$$

so that $|F/N| = \infty$. In conclusion, we have shown that F/N is an infinite, nonabelian group. This completes the proof. $\square$

Problem 6. *Suppose that G is a finite solvable group. Prove that there is a sequence*

$$\{1\} = G_0 \leq G_1 \leq \cdots \leq G_r = G$$

of subgroups of G, so that each G_{i-1} is normal in G_i and G_i/G_{i-1} is cyclic.

Proof. Since G is solvable, there exists a sequence

$$\{1\} = N_0 \trianglelefteq N_1 \trianglelefteq \cdots \trianglelefteq N_m = G \qquad \text{(A)}$$

such that N_i/N_{i-1} is abelian for each $i \in \{1, \ldots, m\}$. We claim that (A) can be made into a composition series.

If (A) is already a composition series, then we are done. If (A) is not a composition series, then there is at least one factor of (A) that is not simple. Let N_z/N_{z-1} be a factor of (A) that is not simple for some $z \in \{1, \ldots, m\}$. Then there exists a nontrivial, proper, normal subgroup of N_z/N_{z-1}, say

$$H/N_{z-1} \trianglelefteq N_z/N_{z-1}$$

By the Fourth Isomorphism Theorem, the above gives $N_{z-1} \trianglelefteq H \trianglelefteq N_z$. Furthermore, since N_z/N_{z-1} is an abelian group and since subgroups of abelian groups are abelian, we have that H/N_{z-1} is an abelian group. In addition, we have by the Third Isomorphism Theorem that

$$N_z/H \simeq \frac{N_z/N_{z-1}}{H/N_{z-1}}$$

Therefore, we have that N_z/H is isomorphic to a quotient of the abelian group N_z/N_{z-1} so that N_z/H is abelian. Thus, we obtain a new subnormal series

$$\{1\} = N_0 \trianglelefteq N_1 \trianglelefteq \cdots \trianglelefteq N_{z-1} \trianglelefteq H \trianglelefteq N_z \trianglelefteq \cdots \trianglelefteq N_m = G \qquad \text{(B)}$$

such that each factor of (B) is abelian.

Now, if (B) is not a composition series, then we can repeat the above process to obtain a new subnormal series with abelian factors in the same way we obtained (B) from (A). Since G is finite, this process must eventually terminate in a composition series, say

$$\{1\} = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_r = G \qquad \text{(C)}$$

such that G_i/G_{i-1} is abelian for each $i \in \{1, \ldots, r\}$. In particular, note that as G is finite we have that G_i/G_{i-1} is a finite, abelian, simple group for each $i \in \{1, \ldots, r\}$.

We will now show that a finite, abelian, simple group must necessarily be cyclic. Towards this end, let A be such a group. If A is trivial, then clearly A is cyclic. Therefore, suppose that A is not trivial and let $x \in A$ be a nonidentity element. Since A is abelian, we have that $\langle x \rangle \trianglelefteq A$. But since $x \in A$ is a nonidentity element, we have that $\langle x \rangle$ is a nontrivial, normal subgroup of A. Since A is simple, this forces $\langle x \rangle = A$ so that A is cyclic, as claimed.

By the above proof, it follows that G_i/G_{i-1} is cyclic for each $i \in \{1, \ldots, r\}$. We conclude that (C) is a sequence satisfying the conclusion of this problem. This completes the proof. $\square$

Problem 7. (a): *Define* solvable group.

(b): *Prove that the homomorphic image of a solvable group is solvable.*

(c): *Prove that a free group is solvable if and only if it is the free group on at most one generator.*

Proof. (a): Let G be a group. We say that G is ***solvable*** if there exists a sequence

$$\{1\} = H_0 \trianglelefteq H_1 \trianglelefteq \cdots \trianglelefteq H_r = G$$

where r is a positive integer and H_i/H_{i-1} is abelian for each $i \in \{1, \ldots, r\}$. □

Proof. (b): Let G be a solvable group and suppose that $\sigma : G \to \sigma(G)$ is a group homomorphism. We must show that $\sigma(G)$ is solvable.

First, note that $\sigma(G)$ is a group since the homomorphic image of a group is a group. Now, since G is solvable, there exists a sequence

$$\{1\} = H_0 \trianglelefteq H_1 \trianglelefteq \cdots \trianglelefteq H_r = G$$

where r is a positive integer and H_i/H_{i-1} is abelian for each $i \in \{1, \ldots, r\}$. By a previous result, we can assume that the above sequence forms a composition series so that we may also assume that H_i/H_{i-1} is simple for each $i \in \{1, \ldots, r\}$.

Now, fix $m \in \{1, \ldots, r\}$. By the above, we have $H_{m-1} \trianglelefteq H_m$. We will show that $\sigma(H_{m-1}) \trianglelefteq \sigma(H_m)$. Towards this end, first note that as the homomorphic image of a group is a group that $\sigma(H_{m-1})$ and $\sigma(H_m)$ are groups. Furthermore, since $H_{m-1} \subseteq H_m$, we have that $\sigma(H_{m-1}) \subseteq \sigma(H_m)$ and thus we obtain $\sigma(H_{m-1}) \leq \sigma(H_m)$.

Next, let $g \in \sigma(H_m)$ and $h \in \sigma(H_{m-1})$. Then there exists some $x \in H_m$ and some $y \in H_{m-1}$ such that $g = \sigma(x)$ and $h = \sigma(y)$. Furthermore, since $H_{m-1} \trianglelefteq H_m$, we have that $xyx^{-1} \in H_{m-1}$. Therefore, since σ is a homomorphism, we obtain

$$ghg^{-1} = \sigma(x)\sigma(y)[\sigma(x)]^{-1} = \sigma(x)\sigma(y)\sigma(x^{-1}) = \sigma(xyx^{-1}) \in \sigma(H_{m-1})$$

This shows that $\sigma(H_{m-1}) \trianglelefteq \sigma(H_m)$, as claimed.

Next, we show that $\sigma(H_m)/\sigma(H_{m-1})$ is abelian. Towards this end, define

$$\phi : H_m/H_{m-1} \to \sigma(H_m)/\sigma(H_{m-1})$$

by $\phi(xH_{m-1}) = \sigma(x)\sigma(H_{m-1})$ for all $xH_{m-1} \in H_m/H_{m-1}$. To see that ϕ is well-defined, suppose that $x_1H_{m-1}, x_2H_{m-1} \in H_m/H_{m-1}$ with $x_1H_{m-1} = x_2H_{m-1}$. In this case, we have by $x_2^{-1}x_1 \in H_{m-1}$ so that $\sigma(x_2^{-1}x_1) \in \sigma(H_{m-1})$. But since σ is a group homomorphism, this gives that $\sigma(x_2)^{-1}\sigma(x_1) \in \sigma(H_{m-1})$ so that

$$\phi(x_1H_{m-1}) = \sigma(x_1)\sigma(H_{m-1}) = \sigma(x_2)\sigma(H_{m-1}) = \phi(x_2H_{m-1})$$

In particular, this shows that ϕ is well-defined.

Now, let $y \in \sigma(H_m)/\sigma(H_{m-1})$. Then $y = \sigma(x)\sigma(H_{m-1})$ for some $x \in H_m$. Notice that $xH_{m-1} \in H_m/H_{m-1}$ and

$$\phi(xH_{m-1}) = \sigma(x)\sigma(H_{m-1}) = y$$

so that ϕ is surjective.

Finally, notice that $\ker\phi$ is a normal subgroup of H_m/H_{m-1}. Since H_m/H_{m-1} is simple, it now follows that $\ker\phi \in \{\{1\}, H_m/H_{m-1}\}$. If $\ker\phi = \{1\}$, then the above results and the First Isomorphism Theorem give

$$H_m/H_{m-1} \simeq \sigma(H_m)/\sigma(H_{m-1})$$

In this case, since H_m/H_{m-1} is abelian, we obtain that $\sigma(H_m)/\sigma(H_{m-1})$ is abelian. If $\ker\phi = H_m/H_{m-1}$, then the above results and the First Isomorphism Theorem give

$$\{1\} \simeq \sigma(H_m)/\sigma(H_{m-1})$$

In this case, since $\{1\}$ is abelian, we obtain that $\sigma(H_m)/\sigma(H_{m-1})$ is abelian. In all cases, then, we see that $\sigma(H_m)/\sigma(H_{m-1})$ is abelian, as claimed.

Since $m \in \{1, \ldots, r\}$ was arbitrary, we obtain

$$\{1\} = \sigma(H_0) \trianglelefteq \sigma(H_1) \trianglelefteq \cdots \trianglelefteq \sigma(H_r) = \sigma(G)$$

where $\sigma(H_i)/\sigma(H_{i-1})$ is abelian for each $i \in \{1, \ldots, r\}$. By definition, the existence of the above sequence shows that $\sigma(G)$ is solvable. This completes the proof. $\square$

Proof. (c): For the first direction, suppose that F is a solvable free group. For the sake of contradiction, assume that F is a free group on the set $X = \{x_1, \ldots, x_n\}$ for some positive integer $n \geq 2$. Now, let G be the free group on the set $\{x_1, x_2\}$ and let H be the free group on the (possibly empty) set $\{x_3, \ldots, x_n\}$. It is clear that $G \simeq F/H$. Furthermore, since F is solvable and since quotients of solvable groups are solvable, we have that G is also solvable.

Now, consider the symmetric group S_5 and recall that S_5 is not solvable. Let $\sigma_1 = (1 \quad 2) \in S_5$ and $\sigma_2 = (1 \quad 2 \quad 3 \quad 4 \quad 5) \in S_5$ and note that $S_5 = \langle \sigma_1, \sigma_2 \rangle$. Define

$$f : \{x_1, x_2\} \to S_5 \quad \text{by} \quad x_1 \mapsto \sigma_1 \quad \text{and} \quad x_2 \mapsto \sigma_2$$

Since G is free on the set $\{x_1, x_2\}$ in the category of groups, there exists a group homomorphism $\overline{f} : G \to S_5$ such that $\overline{f}(x_1) = f(x_1) = \sigma_1$ and $\overline{f}(x_2) = f(x_2) = \sigma_2$.

Now, note that since $S_5 = \langle \sigma_1, \sigma_2 \rangle$ and since $\overline{f}(x_1) = \sigma_1$ and $\overline{f}(x_2) = \sigma_2$ we have that $\overline{f}$ is a surjection. Hence, we have that S_5 is the homomorphic image of G. In particular, since G is solvable and since homomorphic images of solvable groups are solvable, this observation implies that S_5 is solvable. However, this is a contradiction. We conclude that F is a free group on at most one generator, completing the proof of the first direction.

For the second direction, suppose that F is a free group on at most one generator. If F is a free group on the set $X = \emptyset$, then F is trivial and hence solvable. If F is the free group on the set $X = \{x\}$, then $F \simeq \mathbb{Z}$. Since $\mathbb{Z}$ is a solvable group, this implies that F is solvable. This completes the proof of the second direction. $\square$

Problem 8. *Let G be a group; call $g \in G$ a* non-generator *if, for each subset X of G so that $X \cup \{g\}$ generates G, then, in fact, X itself generates G. Let* $\mathrm{Fr}(G)$ *denote the set of all non-generators of G.*

(a): *Prove that* $\mathrm{Fr}(G)$ *is a subgroup of G.*

(b): *Show that* $\mathrm{Fr}(G)$ *is the intersection of all maximal subgroups of G.*

Proof. (a): Let X be a subset of G such that $X \cup \{1\}$ generates G. In this case, we have

$$G = \langle X \cup \{1\} \rangle = \langle X \rangle$$

Thus, we see that $1 \in \mathrm{Fr}(G)$. In particular, this implies that $\mathrm{Fr}(G) \neq \emptyset$.

Now, let $x, y \in \mathrm{Fr}(G)$. We will show that $xy^{-1} \in \mathrm{Fr}(G)$. Let X be a subset of G such that $X \cup \{xy^{-1}\}$ generates G. In this case, we have

$$G = \langle X \cup \{xy^{-1}\} \rangle = \langle \langle X \cup \{x\} \rangle \cup \{y^{-1}\} \rangle = \langle \langle X \cup \{x\} \rangle \cup \{y\} \rangle$$

The above shows that $X \cup \{x\}$ is a subset of G so that $(X \cup \{x\}) \cup \{y\}$ generates G. Since $y \in \mathrm{Fr}(G)$, this implies that $X \cup \{x\}$ generates G. Therefore, X is a subset of G such that $X \cup \{x\}$ generates G. Since $x \in \mathrm{Fr}(G)$, this implies that X generates G. Thus, we obtain that $xy^{-1} \in \mathrm{Fr}(G)$. In particular, the above results prove that $\mathrm{Fr}(G)$ is a subgroup of G. $\square$

Proof. (b): Before we begin, note that if G has no maximal subgroups then the intersection of all maximal subgroups of G is simply G itself. We then have $\mathrm{Fr}(G) = G$ which completes the proof in this case. We now assume that G has maximal subgroups.

First, let $g \in \mathrm{Fr}(G)$ and let M be a maximal subgroup of G. For the sake of contradiction, assume that $g \notin M$. In this case, since M is a group, we have

$$M = \langle M \rangle \subseteq \langle M \cup \{g\} \rangle \subseteq G$$

But since $g \notin M$, we know that $M \neq \langle M \cup \{g\} \rangle$. Hence, by the maximality of M and this observation, we have that $\langle M \cup \{g\} \rangle = G$. However, recall that $g \in \mathrm{Fr}(G)$. Thus, we now conclude that since M is a group that $M = \langle M \rangle = G$, which contradicts the fact that M is properly contained in G since M is a maximal subgroup of G. Therefore, $g \in M$ and since M was an arbitrary maximal subgroup of G, this implies that g is in the intersection of all maximal subgroups of G.

Secondly, let g be in the intersection of all maximal subgroups of G. For the sake of contradiction, suppose that $g \notin \mathrm{Fr}(G)$. Then there exists a subset $X \subseteq G$ such that $\langle X \cup \{g\} \rangle = G$ but X does not generate G. Therefore, there is some proper subgroup A of G such that $X \subseteq A$. Define

$$\mathcal{S} = \{H \leq G : X \subseteq H \text{ and } g \notin H\}$$

and order $\mathcal{S}$ by inclusion of sets. Note that if $g \in A$ then since $X \subseteq A$ and $X \cup \{g\}$ generates G, we have as A is a group that $A = \langle A \rangle = G$. However, this contradicts that A is properly contained in G. In particular, we have that $A \leq G, X \subseteq A$, and $g \notin A$ so that $A \in \mathcal{S}$. Notice that this gives $\mathcal{S} \neq \emptyset$.

Now, let $\mathcal{C}$ be a chain in $\mathcal{S}$. If $\mathcal{C} = \emptyset$, then $A \in \mathcal{S}$ is an upper bound for $\mathcal{C}$ in $\mathcal{S}$. If $\mathcal{C} \neq \emptyset$ define

$$J = \bigcup_{C \in \mathcal{C}} C$$

It follows by the definition of J that J is an upper bound for $\mathcal{C}$. It is also immediate that since $X \subseteq C$ and $g \notin C$ for every $C \in \mathcal{C}$, we have that $X \subseteq J$ and $g \notin J$. We will now show that J is a group. Towards this end, first note that we clearly have $J \neq \emptyset$. Now, let $x, y \in J$. Then $x \in C_1$ and $y \in C_2$ for some $C_1, C_2 \in \mathcal{C}$. Since $\mathcal{C}$ is a chain, we may assume without loss of generality that $C_1 \subseteq C_2$. In this case, we have that $x, y \in C_2$ and since C_2 is a group, we have

$$xy^{-1} \in C_2 \subseteq J$$

Hence, it follows that J is a group. The above results show that $J \in \mathcal{S}$ so that J is an upper bound for $\mathcal{C}$ in $\mathcal{S}$. By Zorn's Lemma, there is some maximal element $M \in \mathcal{S}$.

Now, since $M \in \mathcal{S}$, we have that M is a subgroup of G such that $X \subseteq M$ and $g \notin M$. Furthermore, since $g \in G$ but $g \notin M$, we have that $M \neq G$. Suppose now that N is a subgroup of G such that $M \subseteq N \subseteq G$ and $M \neq N$. By the maximality of M, we have that $N \notin \mathcal{S}$. But since N is a subgroup of G and $X \subseteq M \subseteq N$, this forces that $g \in N$. Hence, as $X \cup \{g\}$ generates G, as $X \subseteq N$, and as N is a group, we have

$$N = \langle N \rangle = G$$

In particular, this shows that M is a maximal subgroup of G so that $g \in M$. However, this contradicts the fact that $g \notin M$. We conclude that $g \in \mathrm{Fr}(G)$.

The above arguments show that $\mathrm{Fr}(G)$ is equal to the intersection of all maximal subgroups of G. $\square$

Part 2: Spring Semester 2017

Problem 9. *Suppose that R is a principal ideal domain. Prove that any submodule of a free R-module is free.*

Proof. Let M be a free R-module and let W be an R-submodule of M. Since M is a free R-module, there exists a basis $B \subseteq M$ for M. Let $\mathcal{C}$ denote the collection of all pairs (A, C), where $A \subseteq B$ and C is a basis for $\operatorname{span}\{A\} \cap W$. Note that since $\emptyset \subseteq B$ and $\emptyset$ is a basis for $\{0\} = \operatorname{span}\{\emptyset\} \cap W$ we have that $(\emptyset, \emptyset) \in \mathcal{C}$ so that $\mathcal{C} \neq \emptyset$. Order $\mathcal{C}$ by for $(A_1, C_1), (A_2, C_2) \in \mathcal{C}$ we have $(A_1, C_1) \leq (A_2, C_2)$ if and only if $A_1 \subseteq A_2$ and $C_1 \subseteq C_2$. Clearly, this defines a partial ordering on $\mathcal{C}$.

Now, let J be a chain in $\mathcal{C}$. If $J = \emptyset$, then $(\emptyset, \emptyset) \in \mathcal{C}$ is an upper bound for J. Therefore, assume that $J \neq \emptyset$. Note that

$$\mathcal{J} = \left(\bigcup_{x \in J} \pi_1(x), \bigcup_{x \in J} \pi_2(x) \right)$$

is clearly an upper bound for J. We will show that $\mathcal{J} \in \mathcal{C}$.

Towards this end, first note that since $\pi_1(x) \subseteq B$ for each $x \in J$ we have that $\bigcup_{x \in J} \pi_1(x) \subseteq B$. Since J is a chain, we have that $\bigcup_{x \in J} \pi_2(x)$ is linearly independent. Now, let $v \in \operatorname{span}\left\{\bigcup_{x \in J} \pi_1(x)\right\} \cap W$. Then it follows that there exists some $x \in J$ such that $v \in \operatorname{span}\{\pi_1(x)\} \cap W$. Since $x \in J$, we know that $\pi_2(x)$ is a basis for $\operatorname{span}\{\pi_1(x)\} \cap W$. Thus, we obtain

$$v \in \operatorname{span}\{\pi_2(x)\} \subseteq \operatorname{span}\left\{ \bigcup_{x \in J} \pi_2(x) \right\}$$

The above results show that $\bigcup_{x \in J} \pi_2(x)$ is a basis for $\operatorname{span}\left\{\bigcup_{x \in J} \pi_1(x)\right\} \cap W$. Combining the above results, we obtain $\mathcal{J} \in \mathcal{C}$. By Zorn's Lemma, there exists some maximal element $(A, C) \in \mathcal{C}$.

For the sake of contradiction, suppose that $A \neq B$. Since $A \subseteq B$, this implies that there is some $e \in B$ such that $e \notin A$. Define $S_0 = \operatorname{span}\{A\}$ and $S = \operatorname{span}\{A \cup \{e\}\}$. Let $\pi : S \to R$ denote the map that assigns to each element of S its coordinate at e and note that π is an R-module homomorphism with $\ker \pi = S_0$. Now, since $(A, C) \in \mathcal{C}$, we know that $S_0 \cap W$ is free with basis C. Furthermore, since π is an R-module homomorphism we have that $\pi(S \cap W)$ is an R-submodule of R since $S \cap W$ is an R-submodule of W. Since R is a principal ideal domain, this implies that $\pi(S \cap W)$ is a free R-module.

Now, we have since $\ker \pi = S_0$ and since clearly $S_0 \subseteq S$ that

$$S \cap W \cap \ker \pi = S \cap W \cap S_0 = S_0 \cap W$$

is a free R-module. This implies that $S \cap W$ is isomorphic to $S_0 \cap W \oplus \pi(S \cap W)$. Thus, we can extend the basis C to a basis for $S \cap W$. However, this contradicts the maximality of $(A, C) \in \mathcal{C}$. We conclude that $A = B$ and $W = W \cap \operatorname{span}\{A\}$ so that W is a free R-module. This completes the proof. $\square$

Problem 14. *Give an example of a projective module which is not free. Explain.*

Proof. We claim that $\mathbb{Z}/2\mathbb{Z}$ and $\mathbb{Z}/3\mathbb{Z}$ are projective $\mathbb{Z}/6\mathbb{Z}$-modules but are not free $\mathbb{Z}/6\mathbb{Z}$-modules. First, we show that $\mathbb{Z}/2\mathbb{Z}$ and $\mathbb{Z}/3\mathbb{Z}$ are actually $\mathbb{Z}/6\mathbb{Z}$-modules. We will accomplish this task by proving a more general result. This result is:

Lemma. If A is an abelian group and $n > 0$ an integer such that $na = 0$ for all $a \in A$, then A is a $\mathbb{Z}/n\mathbb{Z}$-module.

Indeed, define an action of $\mathbb{Z}/n\mathbb{Z}$ on A by for $\overline{k} \in \mathbb{Z}/n\mathbb{Z}$ and $a \in A$ we have $\overline{k}a = ka$. We claim that this action of $\mathbb{Z}/n\mathbb{Z}$ on A is well-defined. Towards this end, suppose that $\overline{k_1} = \overline{k_2}$ for some $\overline{k_1}, \overline{k_2} \in \mathbb{Z}/n\mathbb{Z}$. Then we have

$$\overline{0} = \overline{k_1} - \overline{k_2} = \overline{k_1 - k_2}$$

and hence n divides $k_1 - k_2$. Therefore, there is some $m \in \mathbb{Z}$ such that $k_1 - k_2 = mn$ so that $k_1 = mn + k_2$. Now, since $a \in A$ we have by hypothesis that $na = 0$. Therefore, we obtain

$$\overline{k_1}a = k_1 a = (mn + k_2)a = mna + k_2 a = m(na) + k_2 a = m(0) + k_2 a = k_2 a = \overline{k_2}a$$

so that the above action of $\mathbb{Z}/n\mathbb{Z}$ on A is indeed well-defined. The verification of the module axioms is straightforward, completing the proof of the Lemma.

Now, we prove the main result. Towards this end, notice that $\mathbb{Z}/2\mathbb{Z}$ is an abelian group such that $6a = 0$ for all $a \in \mathbb{Z}/2\mathbb{Z}$. Similarly, notice that $\mathbb{Z}/3\mathbb{Z}$ is an abelian group such that $6a = 0$ for all $a \in \mathbb{Z}/3\mathbb{Z}$. Hence, by the above Lemma we have that $\mathbb{Z}/2\mathbb{Z}$ and $\mathbb{Z}/3\mathbb{Z}$ are indeed $\mathbb{Z}/6\mathbb{Z}$-modules.

Next, notice that $\mathbb{Z}/6\mathbb{Z}$ is clearly a free $\mathbb{Z}/6\mathbb{Z}$-module. In addition, since $\mathbb{Z}/6\mathbb{Z} \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$ as 2 and 3 are relatively prime integers it now follows that both $\mathbb{Z}/2\mathbb{Z}$ and $\mathbb{Z}/3\mathbb{Z}$ are projective $\mathbb{Z}/6\mathbb{Z}$-modules since $\mathbb{Z}/6\mathbb{Z}$ is a free $\mathbb{Z}/6\mathbb{Z}$-module.

Now, recall that any free $\mathbb{Z}/6\mathbb{Z}$-module is isomorphic to a direct sum of copies of $\mathbb{Z}/6\mathbb{Z}$. Therefore, if F is a free $\mathbb{Z}/6\mathbb{Z}$-module it must be the case that

$$|F| \geq |\mathbb{Z}/6\mathbb{Z}| = 6$$

Since $|\mathbb{Z}/2\mathbb{Z}| = 2 < 6$ and $|\mathbb{Z}/3\mathbb{Z}| = 3 < 6$, then, it now follows that $\mathbb{Z}/2\mathbb{Z}$ is not a free $\mathbb{Z}/6\mathbb{Z}$-module and that $\mathbb{Z}/3\mathbb{Z}$ is not a free $\mathbb{Z}/6\mathbb{Z}$-module. This completes the proof that $\mathbb{Z}/2\mathbb{Z}$ and $\mathbb{Z}/3\mathbb{Z}$ are projective $\mathbb{Z}/6\mathbb{Z}$-modules but are not free $\mathbb{Z}/6\mathbb{Z}$-modules. $\square$

Problem 16. *Let R be a ring with identity. Prove that a direct product of left R-modules is injective if and only if each factor is injective.*

Note: Recall that if S is a ring with identity that an S-module J is injective if and only if for any left ideal L of S any S-module homomorphism $L \to J$ can be extended to an S-module homomorphism $S \to J$. We will use this equivalence in the proof of both directions below.

Proof. For the first direction, suppose that $(J_i)_{i\in I}$ is a collection of left R-modules such that $\bigoplus_{i\in I} J_i$ is an injective R-module. Let L be a left ideal of R and for each $k \in I$ suppose that $\phi_k : L \to J_k$ is an R-module homomorphism. Define

$$\phi : L \to \bigoplus_{i\in I} J_i \quad \text{by} \quad a \mapsto (\phi_k(a))_{k\in I}$$

Now, since ϕ_k is an R-module homomorphism for each $k \in I$ it follows that ϕ is an R-module homomorphism. Hence, as $\bigoplus_{i\in I} J_i$ is an injective R-module by hypothesis it now follows that ϕ can be extended to an R-module homomorphism $\psi : R \to \bigoplus_{i\in I} J_i$.

Next, for each $k \in I$ let $\pi_k : \bigoplus_{i\in I} J_i \to J_k$ denote the canonical projection map and note that π_k is an R-module homomorphism. For each $k \in I$, let $\psi_k = \pi_k \circ \psi$. In particular, note that $\psi_k : R \to J_k$ is an R-module homomorphism for each $k \in I$ since the defined composition of R-module homomorphisms is an R-module homomorphism.

Finally, fix any $k \in I$. We claim that ψ_k extends ϕ_k. Towards this end, suppose that $a \in L$. Then since $\psi : R \to \bigoplus_{i\in I} J_i$ extends $\phi : L \to \bigoplus_{i\in I} J_i$, we have that

$$\psi_k(a) = (\pi_k \circ \psi)(a) = \pi_k(\psi(a)) = \pi_k(\phi(a)) = \pi_k(\phi_k(a)_{k\in I}) = \phi_k(a)$$

Thus, since $a \in L$ was arbitrary it now follows that ψ_k extends ϕ_k. We may now conclude that J_k is an injective R-module and since $k \in I$ was arbitrary, this completes the proof of the first direction.

For the second direction, suppose that $(J_i)_{i\in I}$ is a collection of injective left R-modules. Let L be a left ideal of R and suppose that $\phi : L \to \bigoplus_{i\in I} J_i$ is an R-module homomorphism. For each $k \in I$, let $\pi_k : \bigoplus_{i\in I} J_i \to J_k$ denote the canonical projection map and note that π_k is an R-module homomorphism. We also observe that

$$\phi(a) = (\pi_k(\phi(a)))_{k\in I} \quad \text{for each} \quad a \in L$$

This fact will be used below.

Now, for each $k \in I$ let $\phi_k = \pi_k \circ \phi$. In particular, notice that $\phi_k : L \to J_k$ is an R-module homomorphism for each $k \in I$ since the defined composition of R-module homomorphisms is an R-module homomorphism. Therefore, since J_k is an injective R-module by hypothesis it follows that for each $k \in I$ there exists an R-module homomorphism $\psi_k : R \to J_k$ extending ϕ_k.

Finally, define a map

$$\psi : R \to \bigoplus_{i\in I} J_i \quad \text{by} \quad r \mapsto (\psi_k(r))_{k\in I}$$

Now, since ψ_k is an R-module homomorphism for each $k \in I$ it follows that ψ is an R-module homomorphism. Furthermore, we claim that ψ extends ϕ. Towards this end, suppose that $a \in L$. Then since $\psi_k : R \to J_k$ extends $\phi_k : L \to J_k$ for each $k \in I$ and by our observation made above, we see

$$\psi(a) = (\psi_k(a))_{k\in I} = (\phi_k(a))_{k\in I} = ((\pi_k \circ \phi)(a))_{k\in I} = (\pi_k(\phi(a)))_{k\in I} = \phi(a)$$

Thus, since $a \in L$ was arbitrary it now follows that ψ extends ϕ. We may now conclude that $\bigoplus_{i\in I} J_i$ is an injective R-module, completing the proof of the second direction. $\square$

Problem 17. *Suppose that R is a commutative ring with identity. If A and B are projective R-modules, prove that $A \otimes_R B$ is also projective.*

Proof. Before we begin, we prove that the tensor product of two free R-modules is free. Indeed, suppose that C and D are free R-modules. Since C and D are free R-modules, it follows that $C \simeq \bigoplus_{i \in I} R$ and $D \simeq \bigoplus_{j \in J} R$ where I and J are nonempty index sets with each of the above isomorphims being an isomorphim of R-modules. Therefore, since tensor products distribute over direct sums and since $R \otimes_R R \simeq R$ we obtain

$$\begin{aligned} C \otimes_R B &= \left(\bigoplus_{i \in I} R \right) \otimes_R \left(\bigoplus_{j \in J} R \right) \\ &\simeq \bigoplus_{i \in I} \left(R \otimes_R \left(\bigoplus_{j \in J} R \right) \right) \\ &\simeq \bigoplus_{i \in I} \left(\bigoplus_{j \in J} (R \otimes_R R) \right) \\ &= \bigoplus_{(i,j) \in I \times J} (R \otimes_R R) \\ &\simeq \bigoplus_{(i,j) \in I \times J} R \end{aligned}$$

with each of the above isomorphisms being an isomorphism of R-modules since R is commutative. Therefore, we see $C \otimes_R B \simeq \bigoplus_{(i,j) \in I \times J} R$ as R-modules. Thus, as $I \times J$ is nonempty as both I and J are nonempty we conclude that $C \otimes_R B$ is a free R-module.

Now, we prove the main result. Towards this end, first note that as A and B are projective R-modules there are free R-modules F_1 and F_2 and R-modules K_1 and K_2 such that $F_1 \simeq K_1 \oplus A$ and $F_2 \simeq K_2 \oplus B$. Furthermore, notice that since tensor products distribute over direct sums that we have

$$\begin{aligned} F_1 \otimes_R F_2 &\simeq (K_1 \oplus A) \otimes_R (K_2 \oplus B) \\ &\simeq [K_1 \otimes_R (K_2 \oplus B)] \oplus [A \otimes_R (K_2 \oplus B)] \\ &\simeq [(K_1 \otimes_R K_2) \oplus (K_1 \otimes_R B)] \oplus [(A \otimes_R K_2) \oplus (A \otimes_R B)] \\ &= [(K_1 \otimes_R K_2) \oplus (A \otimes_R K_2) \oplus (K_1 \otimes_R B)] \oplus (A \otimes_R B) \end{aligned}$$

with each of the above isomorphisms being an isomorphism of R-modules since R is commutative. Now, note that

$$(K_1 \otimes_R K_2) \oplus (A \otimes_R K_2) \oplus (K_1 \otimes_R B)$$

is an R-module since each direct summand in the above direct sum is an R-module as R is commutative. Therefore, we see that since

$$F_1 \otimes_R F_2 \simeq [(K_1 \otimes_R K_2) \oplus (A \otimes_R K_2) \oplus (K_1 \otimes_R B)] \oplus (A \otimes_R B)$$

and as $F_1 \otimes_R F_2$ is a free R-module by our preliminary result that $A \otimes_R B$ is a projective R-module. This completes the proof. $\square$

Problem 19. *Suppose* $(m, n) = 1$. *Compute* $\mathbb{Z}_m \otimes_{\mathbb{Z}} \mathbb{Z}_n$. *Justify your answer.*

Proof. We will denote $\otimes_{\mathbb{Z}}$ as $\otimes$ for simplicity throughout this proof. Now, we prove a more general result before proving the main result. This result is:

Lemma. Let A be an abelian group. Then for each $m > 0$, we have $A \otimes \mathbb{Z}_m \simeq A/mA$. In particular, this result implies that $\mathbb{Z}_m \otimes \mathbb{Z}_n \simeq \mathbb{Z}_c$, where $c = (m, n)$.

Indeed, let $m > 0$ and define a map

$$f : A \times \mathbb{Z}_m \to A/mA \quad \text{by} \quad (a, \overline{z}) \mapsto za + mA$$

We show that f is well-defined. Towards this end, suppose that $(a_1, \overline{z_1}) = (a_2, \overline{z_2})$ for some $(a_1, \overline{z_1}), (a_2, \overline{z_2}) \in A \times \mathbb{Z}_m$. Then clearly $a_1 = a_2$ and $\overline{z_1} = \overline{z_2}$. Since $\overline{z_1} = \overline{z_2}$, it follows that

$$\overline{0} = \overline{z_1} - \overline{z_2} = \overline{z_1 - z_2}$$

so that m divides $z_1 - z_2$. Now, since $a_1 = a_2$ we can write $a_1 = a_2 = a \in A$. Furthermore, since m divides $z_1 - z_2$ we have $(z_1 - z_2)a \in mA$. Hence, we obtain

$$\begin{aligned} f(a_1, \overline{z_1}) - f(a_2, \overline{z_2}) &= f(a, \overline{z_1}) - f(a, \overline{z_2}) \\ &= (z_1 a + mA) - (z_2 a + mA) \\ &= (z_1 - z_2)a + mA \\ &= mA \end{aligned}$$

In particular, the above result shows that $f(a_1, \overline{z_1}) - f(a_2, \overline{z_2})$ is equal to the identity element of A/mA so that $f(a_1, \overline{z_1}) = f(a_2, \overline{z_2})$ which shows that f is well-defined. Furthermore, it is easily verified that f is a middle linear map and hence there exists a (unique) group homomorphism $\phi : A \otimes \mathbb{Z}_m \to A/mA$ such that $\phi \circ g = f$, where $g : A \times \mathbb{Z}_m \to A \otimes \mathbb{Z}_m$ is the tensor product.

Now, note that if $a \in A$ and $\overline{z} \in \mathbb{Z}_m$ we have since $\phi \circ g = f$ that

$$\phi(a \otimes \overline{z}) = \phi(g(a, \overline{z})) = f(a, \overline{z}) = za + mA$$

and

$$a \otimes \overline{z} = a \otimes z\overline{1} = g(a, z\overline{1}) = g(za, \overline{1}) = za \otimes \overline{1}$$

In particular, the second of the above equalities shows if $a \in A$ and $\overline{z} \in \mathbb{Z}_m$ then we have $a \otimes \overline{z} = b \otimes \overline{1}$ for some $b \in A$. Therefore, since $A \otimes \mathbb{Z}_m$ is generated by the elements of the form $a \otimes \overline{z}$ where $a \in A$ and $\overline{z} \in \mathbb{Z}_m$ it now follows that any element in $A \otimes \mathbb{Z}_m$ is a finite sum of elements of the form $b \otimes \overline{1}$ where $b \in A$. In addition, note that if $a_1, a_2 \in A$ and if $a = a_1 + a_2 \in A$ then

$$(a_1 \otimes \overline{1}) + (a_2 \otimes \overline{1}) = g(a_1, \overline{1}) + g(a_2, \overline{1}) = g(a_1 + a_2, \overline{1}) = (a_1 + a_2) \otimes \overline{1} = a \otimes \overline{1}$$

Inductively, the above equality shows that any finite sum of elements of the form $b \otimes \overline{1}$ where $b \in A$ and $\overline{1} \in \mathbb{Z}_m$ is again an element of the same form. By our previous observation, then, we may now conclude that every element of $A \otimes \mathbb{Z}_m$ is of the form $b \otimes \overline{1}$ for some $b \in A$.

Next, we show that ϕ is an injection by using the above results. Since ϕ is a group homomorphism, it suffices to show that $\ker\phi$ is trivial to establish that ϕ is an injection. Towards this end, suppose that $x \in \ker\phi$. By the above result, we may write $x = b \otimes \overline{1}$ for some $b \in A$. Therefore, since $b \otimes \overline{1} = x \in \ker\phi$ and by the first of the above equalities we obtain

$$mA = \phi(x) = \phi(b \otimes \overline{1}) = 1b + mA = b + mA$$

and hence $b \in mA$. Thus, there is some $c \in A$ such that $b = mc$. Appealing to the second of the above equalities, then, we obtain

$$x = b \otimes \overline{1} = mc \otimes \overline{1} = c \otimes \overline{m} = c \otimes \overline{0} = 0$$

and hence $\ker\phi$ is trivial. We conclude that ϕ is an injection.

Finally, we show that ϕ is a surjection. Since $\phi \circ g = f$, it suffices to show that f is a surjection to establish that ϕ is a surjection. Towards this end, let $a + mA \in A/mA$. Then clearly $(a, \overline{1}) \in A \times \mathbb{Z}_m$ and

$$f(a, \overline{1}) = 1a + mA = a + mA$$

so that f is a surjection. We conclude that ϕ is a surjection. Combining the previous results, we see that ϕ is a group isomorphism so that $A \otimes \mathbb{Z}_m \simeq A/mA$.

We now prove the second part of the Lemma. Towards this end, note that since $\mathbb{Z}_m$ is an abelian group and as $n > 0$ that by the result of the first part of the Lemma we have $\mathbb{Z}_m \otimes \mathbb{Z}_n \simeq \mathbb{Z}_m/n\mathbb{Z}_m$. We claim that $\mathbb{Z}_m/n\mathbb{Z}_m \simeq \mathbb{Z}_c$, where $c = (m, n)$. Towards this end, define a map

$$\phi : \mathbb{Z}_m \to \mathbb{Z}_c \quad \text{by} \quad z + m\mathbb{Z} \mapsto z + c\mathbb{Z}$$

First, we show that ϕ is well-defined. Towards this end, suppose that $z_1 + m\mathbb{Z} = z_2 + m\mathbb{Z}$ for some $z_1 + m\mathbb{Z}, z_2 + m\mathbb{Z} \in \mathbb{Z}_m$. In this case, we have $z_1 - z_2 \in m\mathbb{Z}$ and hence there is some $z \in \mathbb{Z}$ such that $z_1 - z_2 = mz$. But since $c = (m, n)$, it follows that there is some $k \in \mathbb{Z}$ such that $m = ck$ and hence $z_1 - z_2 = mz = ckz$. This gives

$$\phi(z_1 + m\mathbb{Z}) - \phi(z_2 + m\mathbb{Z}) = (z_1 + c\mathbb{Z}) - (z_2 + c\mathbb{Z}) = (z_1 - z_2) + c\mathbb{Z} = ckz + c\mathbb{Z} = c\mathbb{Z}$$

In particular, the above result shows that $\phi(z_1 + m\mathbb{Z}) - \phi(z_2 + m\mathbb{Z})$ is equal to the identity element of $\mathbb{Z}_c$ so that $\phi(z_1 + m\mathbb{Z}) = \phi(z_2 + m\mathbb{Z})$ which shows that ϕ is well-defined.

Next, note that by the definition of ϕ it is clear that ϕ is a surjective group homomorphism. We claim that $\ker\phi = n\mathbb{Z}_m$. Towards this end, first let $z + m\mathbb{Z} \in \ker\phi \subseteq \mathbb{Z}_m$. Then we have

$$c\mathbb{Z} = \phi(z + m\mathbb{Z}) = z + c\mathbb{Z}$$

so that $z \in c\mathbb{Z}$. Therefore, there is some $k \in \mathbb{Z}$ such that $z = ck$. Now, since $c = (m, n)$, there exist elements $z_1, z_2 \in \mathbb{Z}$ such that $z_1 m + z_2 n = c$. Thus, combining the previous

results now gives

$$\begin{aligned} z + m\mathbb{Z} &= ck + m\mathbb{Z} \\ &= (z_1 m + z_2 n)k + m\mathbb{Z} \\ &= (mz_1 k + nz_2 k) + m\mathbb{Z} \\ &= nz_2 k + m\mathbb{Z} \\ &= n(z_2 k + m\mathbb{Z}) \\ &\in n\mathbb{Z}_m \end{aligned}$$

so that $z + m\mathbb{Z} \in n\mathbb{Z}_m$. On the other hand, let $n(z + m\mathbb{Z}) \in n\mathbb{Z}_m$. Since $c = (m, n)$, there is some $k \in \mathbb{Z}$ such that $n = ck$. Hence, by the definition of ϕ we obtain

$$\phi(n(z + m\mathbb{Z})) = \phi(nz + m\mathbb{Z}) = nz + c\mathbb{Z} = ckz + c\mathbb{Z} = c\mathbb{Z}$$

so that $n(z+m\mathbb{Z}) \in \ker\phi$. The previous results now show that $\ker\phi = n\mathbb{Z}_m$. Therefore, by the previous results and by the First Isomorphism Theorem we have

$$\mathbb{Z}_m/n\mathbb{Z}_m = \mathbb{Z}_m/\ker\phi \simeq \mathbb{Z}_c$$

Finally, combining the previous results now shows that

$$\mathbb{Z}_m \otimes \mathbb{Z}_n \simeq \mathbb{Z}_m/n\mathbb{Z}_m \simeq \mathbb{Z}_c$$

so that $\mathbb{Z}_m \otimes \mathbb{Z}_n \simeq \mathbb{Z}_c$. This completes the proof of second part of the Lemma.

Now, we consider $\mathbb{Z}_m \otimes \mathbb{Z}_n$ when $(m, n) = 1$. By the above Lemma, it follows that

$$\mathbb{Z}_m \otimes \mathbb{Z}_n \simeq \mathbb{Z}_{(m,n)} = \mathbb{Z}_1 = \mathbb{Z}/\mathbb{Z} \simeq 0$$

and hence $\mathbb{Z}_m \otimes \mathbb{Z}_n \simeq 0$. This completes the proof. $\square$

Problem 26. *Suppose that R is a ring with identity, and that every short exact sequence of unital R-modules splits. Prove that every unital R-module is isomorphic to a direct sum of simple R-submodules.*

Proof. Let A be a unital R-module. If A is the zero R-module, then the desired result is immediate. Therefore, assume that A is a nonzero unital R-module.

We first show that if B is an R-submodule of A and if C is an R-submodule of B, then C is a direct summand of B. Towards this end, first note that C is an R-submodule of the R-submodule B of A so that C is an R-submodule of A. Therefore, we have the short exact sequence of unital R-modules

$$0 \longrightarrow C \xrightarrow{\ i\ } A \xrightarrow{\ \pi\ } A/C \longrightarrow 0$$

where i is the inclusion map and π is the canonical projection map. By hypothesis, the above short exact sequence splits so that $A \simeq C \oplus A/C$. Therefore, we may write $A = C \oplus D$ where D is an R-submodule of A with $D \simeq A/C$. This now gives since $C \subseteq B \subseteq A$ that

$$B = B \cap A = B \cap (C \oplus D) = (B \cap C) \oplus (B \cap D) = C \oplus (B \cap D)$$

and hence C is a direct summand of B, as claimed. We will use this result below.

Next, we show that A contains a simple R-submodule. Towards this end, first note that since A is nonzero that there is a nonzero element $a \in A$. Now, let $\mathcal{S}$ denote the collection of all R-submodules of A which do not contain a. Since the zero R-submodule of A does not contain a since a is nonzero, we have that the zero R-submodule of A is in $\mathcal{S}$ so that $\mathcal{S} \neq \emptyset$. Now, partially order $\mathcal{S}$ by inclusion of sets and let $\mathcal{C}$ be a nonempty chain in $\mathcal{S}$. Let C be the union of the elements in $\mathcal{C}$ and note that since each element in $\mathcal{C}$ is an R-submodule of A which does not contain a and as $\mathcal{C}$ is a chain that C is an R-submodule of A that does not contain a. Therefore, we see that $C \in \mathcal{S}$ is clearly an upper bound for $\mathcal{C}$. By Zorn's Lemma, then, we conclude that there is a maximal element $B \in \mathcal{S}$.

Next, note that by the same argument as presented above we have that $A = B \oplus C$ for some R-submodule C of A. We claim that C is a simple R-submodule of A. Towards this end, first note that since A is a unitary R-module and $C \subseteq A$, we have that C is a unitary R-submodule of A. Furthermore, note that as $a \notin B$ as $B \in \mathcal{S}$ but $a \in A = B \oplus C$ we have that C is nonzero. Thus, we see that C is a nonzero unital R-submodule of A.

By the above results, it remains to prove that C contains no nonzero, proper R-submodules to establish that C is a simple R-submodule of A. For the sake of contradiction, suppose there were some nonzero, proper R-submodule D of C. Note that as D is an R-submodule of C which is an R-submodule of A, we have by our above result that there is some R-submodule E of C with $C = D \oplus E$. In particular, notice that since D is a proper R-submodule of C and since $C = D \oplus E$ that necessarily E is nonzero. Next, notice that we now have

$$A = B \oplus C = B \oplus D \oplus E$$

Furthermore, since D and E are nonzero we see that both $B \oplus D$ and $B \oplus E$ are R-submodules of A which both properly contain B. By the maximality of $B \in \mathcal{S}$, then, it must be the case that $a \in B \oplus D$ and $a \in B \oplus E$. Therefore, we may write

$$b + d = a = b' + e \quad \text{for some} \quad b, b' \in B, d \in D, e \in E$$

so that

$$0 = a - a = (b + d) - (b' + e) = (b - b') + d - e \in B \oplus D \oplus E$$

By the above equality, we now have $b - b' = 0$, $d = 0$, and $e = 0$ so that

$$b = b + 0 = b + d = a$$

However, this gives that $a = b \in B$ which is a contradiction since $a \notin B$. We conclude that C is a simple R-submodule of A so that A contains a simple R-submodule. We remark that by the same argument just presented above that any nonzero R-module E contains a simple R-submodule S and that S is a direct summand of E. We will use this observation below.

Towards this end, let $\mathcal{T}$ denote the set of collections of simple R-submodules of A such that the R-submodule of A generated by the elements in each collection in $\mathcal{T}$ is direct. By the above, we know that A contains a simple R-submodule and so it follows that $\mathcal{T} \neq \emptyset$. Now, partially order $\mathcal{T}$ by inclusion of sets and let $\mathcal{C}$ be a nonempty chain in $\mathcal{T}$. Let $\mathcal{E}$ be the union of the elements in $\mathcal{C}$ and note that since each element in $\mathcal{C}$ is a collection of simple R-submodules of A that $\mathcal{E}$ is a collection of simple R-submodules of A. Moreover, since $\mathcal{C}$ is a chain it follows by arguments presented in previous homeworks that the R-submodule of A generated by the elements in $\mathcal{E}$ is direct. Therefore, we see that $\mathcal{E} \in \mathcal{T}$ is clearly an upper bound for $\mathcal{C}$. By Zorn's Lemma, then, we conclude that there is a maximal element $\mathcal{D} \in \mathcal{T}$. For definiteness, let $\mathcal{D} = (S_i)_{i \in I}$ where S_i is a simple R-submodule of A for each $i \in I$.

Finally, let D be the R-submodule of A generated by the collection $\mathcal{D} = (S_i)_{i \in I}$ so that D is a direct sum of simple R-submodules of A. By the same argument as presented above, we have that $A = D \oplus E$ for some R-submodule E of A. For the sake of contradiction, suppose that E were not the zero R-submodule of A. Then by our above remark, we have that E contains a simple R-submodule S and that S is a direct summand of E. Since S is a direct summand of E, since E is nonzero, and since $A = D \oplus E$, it follows that $S \notin \mathcal{D}$ and that the R-submodule of A generated by the collection $\mathcal{D} \cup \{S\}$ is direct. The previous two observations show that $\mathcal{D} \cup \{S\} \in \mathcal{T}$ but $\mathcal{D} \cup \{S\} \supsetneq \mathcal{D}$ which contradicts the maximality of $\mathcal{D} \in \mathcal{T}$. We conclude that E is the zero R-submodule of A so that

$$A = D \oplus E = D = \bigoplus_{i \in I} S_i$$

Since S_i is a simple R-module for each $i \in I$, this completes the proof. $\square$

Problem 27. *Suppose that R is a ring with identity, A a unital right R-module, B a unital left R-module, and C is an abelian group. Let $\mathcal{M}(R)$ denote the category of right R-modules and $\mathcal{A}$ be the category of abelian groups. Then the abelian groups $\mathrm{Hom}_{\mathcal{M}(R)}(A, \mathrm{Hom}_{\mathcal{A}}(B, C))$ and $\mathrm{Hom}_{\mathcal{A}}(A \otimes_R B, C)$ are naturually isomorphic. Prove this, explaining what is meant by "naturally isomorphic."*

Proof. Define

$$\psi : \mathrm{Hom}_{\mathcal{A}}(A \otimes_R B, C) \to \mathrm{Hom}_{\mathcal{M}(R)}(A, \mathrm{Hom}_{\mathcal{A}}(B, C))$$

by for each $f \in \mathrm{Hom}_{\mathcal{A}}(A \otimes_R B, C)$ we have

$$\psi(f) : A \to \mathrm{Hom}_{\mathcal{A}}(B, C)$$

is defined for each $a \in A$ by

$$[\psi(f)](a) : B \to C \quad \text{by} \quad [[\psi(f)](a)](b) = f(a \otimes_R b) \quad \text{for each} \quad b \in B$$

We claim that ψ is a group isomorphism.

First, we show that ψ is actually a map. To establish this result, we must show that $[\psi(f)](a) : B \to C$ is a group homomorphism for each $f \in \mathrm{Hom}_{\mathcal{A}}(A \otimes_R B, C)$ and $a \in A$ and that $\psi(f) : A \to \mathrm{Hom}_{\mathcal{A}}(B, C)$ is a right R-module homomorphism for each $f \in \mathrm{Hom}_{\mathcal{A}}(A \otimes_R B, C)$.

Towards this end, let $f \in \mathrm{Hom}_{\mathcal{A}}(A \otimes_R B, C)$, $a \in A$, and $b_1, b_2 \in B$. Then since f is a group homomorphism, we obtain

$$\begin{aligned}
[[\psi(f)](a)]\,(b_1 + b_2) &= f(a \otimes_R (b_1 + b_2)) \\
&= f((a \otimes_R b_1) + (a \otimes_R b_2)) \\
&= f(a \otimes_R b_1) + f(a \otimes_R b_2) \\
&= [[\psi(f)](a)](b_1) + [[\psi(f)](a)](b_2)
\end{aligned}$$

and thus $[\psi(f)](a) \in \mathrm{Hom}_{\mathcal{A}}(B, C)$. Next, let $f \in \mathrm{Hom}_{\mathcal{A}}(A \otimes_R B, C)$, $a_1, a_2 \in A$, $b \in B$, and $r \in R$. Then since f is a group homomorphism, we obtain

$$\begin{aligned}
[[\psi(f)]\,(a_1 r + a_2)](b) &= f((a_1 r + a_2) \otimes_R b) \\
&= f((a_1 r \otimes_R b) + (a_2 \otimes_R b)) \\
&= f(a_1 r \otimes_R b) + f(a_2 \otimes_R b) \\
&= f(a_1 \otimes_R rb) + f(a_2 \otimes_R b)
\end{aligned}$$

and

$$\begin{aligned}
[[\psi(f)](a_1)r + [\psi(f)](a_2)]\,(b) &= [[\psi(f)](a_1)r](b) + [[\psi(f)](a_2)](b) \\
&= [[\psi(f)](a_1)](rb) + [[\psi(f)](a_2)](b) \\
&= f(a_1 \otimes_R rb) + f(a_2 \otimes_R b)
\end{aligned}$$

and thus $[\psi(f)](a_1 r + a_2) = [\psi(f)](a_1)r + [\psi(f)](a_2)$. In particular, this result shows that $\psi(f) \in \mathrm{Hom}_{\mathcal{M}(R)}(A, \mathrm{Hom}_{\mathcal{A}}(B, C))$. Combining the previous results, we conclude that ψ is indeed a map.

Next, we show that ψ is a group homomorphism. Towards this end, let $f_1, f_2 \in \mathrm{Hom}_{\mathcal{A}}(A \otimes_R B, C)$, $a \in A$, and $b \in B$. Then

$$\begin{aligned}[[\psi(f_1 + f_2)]\,(a)](b) &= (f_1 + f_2)(a \otimes_R b) \\ &= f_1(a \otimes_R b) + f_2(a \otimes_R b)\end{aligned}$$

and

$$\begin{aligned}[[\psi(f_1) + \psi(f_2)](a)]\,(b) &= [[\psi(f_1)](a) + [\psi(f_2)](a)](b) \\ &= [[\psi(f_1)](a)](b) + [[\psi(f_2)](a)](b) \\ &= f(a \otimes_R b) + f(a \otimes_R b)\end{aligned}$$

and thus $\psi(f_1 + f_2) = \psi(f_1) + \psi(f_2)$ so that ψ is a group homomorphism.

By the above results, it remains to prove that ψ is a bijection. First, we show that ψ is an injection. Since ψ is a group homomorphism, it suffices to show that $\ker \psi$ is trivial to establish that ψ is an injection. Towards this end, suppose that $f \in \ker \psi$. Then $\psi(f) : A \to \mathrm{Hom}_{\mathcal{A}}(B, C)$ is the zero map so that $[\psi(f)](a) : B \to C$ is the zero map for each $a \in A$ so that $[[\psi(f)](a)](b) = 0$ for each $b \in B$. In other words, we see

$$0 = [[\psi(f)](a)](b) = f(a \otimes_R b)$$

for each $a \in A$ and $b \in B$. Therefore, we conclude that $f : A \otimes_R B \to C$ is the zero map and hence $\ker \psi$ is trivial so that ψ is an injection.

Finally, we prove that ψ is a surjection. Towards this end, suppose that $g \in \mathrm{Hom}_{\mathcal{M}(R)}(A, \mathrm{Hom}_{\mathcal{A}}(B, C))$. By definition, we have that $g : A \to \mathrm{Hom}_{\mathcal{A}}(B, C)$ is a right R-module homomorphism and $g(a) : B \to C$ is a group homomorphism for each $a \in A$. Now, define a map

$$h : A \times B \to C \quad \text{by} \quad h(a, b) = [g(a)](b) \quad \text{for each} \quad a \in A, b \in B$$

It is easily verified that h is a middle linear map by using the facts that $g : A \to \mathrm{Hom}_{\mathcal{A}}(B, C)$ is a right R-module homomorphism and $g(a) : B \to C$ is a group homomorphism for each $a \in A$. By the definition of the tensor product, then, there exists a (unique) group homomorphism $f : A \otimes_R B \to C$ such that $f(a \otimes_R b) = h(a, b) = [g(a)](b)$ for each $a \in A$ and $b \in B$. In other words, we have that $f \in \mathrm{Hom}_{\mathcal{A}}(A \otimes_R B, C)$ and

$$[[\psi(f)](a)](b) = f(a \otimes_R b) = [g(a)](b) \quad \text{for each} \quad a \in A \quad b \in B$$

so that $\psi(f) = g$. We conclude that ψ is a surjection. Combining the previous results, we see ψ is a group isomorphism so that $\mathrm{Hom}_{\mathcal{M}(R)}(A, \mathrm{Hom}_{\mathcal{A}}(B, C))$ and $\mathrm{Hom}_{\mathcal{A}}(A \otimes_R B, C)$ are isomorphic.

As we saw in the above proof, all we had to do was "follow our noses" by defining maps in an expected (or canonical) manner in order to establish the desired isomorphism. This is what is meant by "naturally isomorphic." $\square$

Problem 28. *Suppose that R is a ring with identity. For each left R-module A, $\mathrm{Hom}_{\mathcal{M}(R)}(R, A)$ is naturally R-isomorphic to A. Prove this, and explain what the "natural" part is all about.*

Proof. Since R has identity, we may define a map

$$\psi : \mathrm{Hom}_{\mathcal{M}(R)}(R, A) \to A \quad \text{by} \quad \psi(\phi) = \phi(1) \quad \text{for each} \quad \phi \in \mathrm{Hom}_{\mathcal{M}(R)}(R, A)$$

Clearly, we see that ψ is a well-defined map. We claim that ψ is a left R-module isomorphism. Indeed, let $r \in R$ and $\phi_1, \phi_2 \in \mathrm{Hom}_{\mathcal{M}(R)}(R, A)$. Then by the definition of ψ and the definition of the action of R on $\mathrm{Hom}_{\mathcal{M}(R)}(R, A)$, we see

$$\begin{aligned}
\psi(r\phi_1 + \phi_2) &= (r\phi_1 + \phi_2)(1) \\
&= (r\phi_1)(1) + \phi_2(1) \\
&= \phi_1(1 \cdot r) + \phi_2(1) \\
&= \phi_1(r \cdot 1) + \phi_2(1) \\
&= r\phi_1(1) + \phi_2(1) \\
&= r\psi(\phi_1) + \psi(\phi_2)
\end{aligned}$$

which proves that ψ is a left R-module homomorphism.

Next, we show that ψ is an injection. Since ψ is a left R-module homomorphism, it suffices to prove that $\ker \psi$ is trivial to establish that ψ is an injection. Towards this end, suppose that $\phi \in \ker \psi$. Then by the definition of ψ, we have $0 = \psi(\phi) = \phi(1)$. Now, let $r \in R$. Then since ϕ is a left R-module homomorphism, we obtain

$$\phi(r) = \phi(r \cdot 1) = r\phi(1) = r \cdot 0 = 0$$

Since $r \in R$ was arbitrary, the above equality shows that ϕ is the zero map and as $\phi \in \ker \psi$ was arbitrary, this shows that $\ker \psi$ is trivial and hence ψ is an injection.

Finally, we show that ψ is a surjection. Towards this end, let $a \in A$. Define a map

$$\phi : R \to A \quad \text{by} \quad \phi(r) = ra \quad \text{for each} \quad r \in R$$

We claim that ϕ is a left R-module homomorphism. Indeed, suppose that $r_1, r_2, s \in R$. Then since A is a left R-module we obtain

$$\phi(sr_1 + r_2) = (sr_1 + r_2)a = (sr_1)a + r_2a = s(r_1a) + r_2a = s\phi(r_1) + \phi(r_2)$$

so that ϕ is a left R-module homomorphism. In other words, we see $\phi \in \mathrm{Hom}_{\mathcal{M}(R)}(R, A)$ and so we may apply ψ to ϕ to obtain

$$\psi(\phi) = \phi(1) = 1a = a$$

so that ψ is a surjection. Combining the above results shows $\psi : \mathrm{Hom}_{\mathcal{M}(R)}(R, A) \to A$ is a left R-module isomorphism so that $\mathrm{Hom}_{\mathcal{M}(R)}(R, A)$ is R-isomorphic to A.

As we saw in the above proof, all we had to do was "follow our noses" by defining maps in an expected (or canonical) manner in order to establish the desired isomorphism. This is what is meant by "naturally isomorphic." $\square$

Problem 29. *Suppose that R is a ring with identity. Prove that*

$$\mathrm{Hom}_{\mathcal{A}}\left(B, \prod_{i\in I} A_i\right) \simeq \prod_{i\in I} \mathrm{Hom}_{\mathcal{A}}(B, A_i)$$

as right R-modules, for all left R-modules B, and all abelian groups A_i for $i \in I$.

Proof. Let $\mathcal{M}(R)$ denote the category of right R-modules. Since B is a left R-module, we have in particular that B is an abelian group. Furthermore, as A_i is an abelian group for each $i \in I$ it follows that $\mathrm{Hom}_{\mathcal{A}}(B, A_i)$ is a right R-module with action defined by for all $\phi \in \mathrm{Hom}_{\mathcal{A}}(B, A_i)$, $b \in B$, and $r \in R$ we have $(\phi r)(b) = \phi(rb)$ for each $i \in I$. In particular, we see that $(\mathrm{Hom}_{\mathcal{A}}(B, A_i))_{i\in I}$ is a family of objects of $\mathcal{M}(R)$.

We use the **fact from Category Theory** that $\prod_{i\in I} \mathrm{Hom}_{\mathcal{A}}(B, A_i)$ together with the family of right R-module homomorphisms $\left(\pi_i : \prod_{i\in I} \mathrm{Hom}_{\mathcal{A}}(B, A_i) \to \mathrm{Hom}_{\mathcal{A}}(B, A_i)\right)_{i\in I}$ (where π_i is the canonical projection map for each $i \in I$) is a product for the family of objects $(\mathrm{Hom}_{\mathcal{A}}(B, A_i))_{i\in I}$ of $\mathcal{M}(R)$.

Now, since A_i is an abelian group for each $i \in I$ it follows that $\prod_{i\in I} A_i$ is an abelian group and hence $\mathrm{Hom}_{\mathcal{A}}\left(B, \prod_{i\in I} A_i\right)$ is an object of $\mathcal{M}(R)$. For each $i \in I$, define a map

$$\psi_i : \mathrm{Hom}_{\mathcal{A}}\left(B, \prod_{i\in I} A_i\right) \to \mathrm{Hom}_{\mathcal{A}}(B, A_i) \quad \text{by} \quad f \mapsto \phi_i \circ f$$

where $\phi_i : \prod_{i\in I} A_i \to A_i$ is the canonical projection map for each $i \in I$. First, we show that ψ_i is well-defined for each $i \in I$. Towards this end, fix any $j \in I$ and suppose that $f \in \mathrm{Hom}_{\mathcal{A}}\left(B, \prod_{i\in I} A_i\right)$. Then $f : B \to \prod_{i\in I} A_i$ is a group homomorphism. Furthermore, we know that $\phi_j : \prod_{i\in I} A_i \to A_j$ is a group homomorphism. Therefore, since the defined composition of group homomorphisms is a group homomorphism we see that $\phi_j \circ f : B \to A_j$ is a group homomorphism so that

$$\psi_j(f) = \phi_j \circ f \in \mathrm{Hom}_{\mathcal{A}}(B, A_j)$$

In particular, this shows that ψ_j is well-defined and since $j \in I$ was arbitrary, we may now conclude that ψ_i is well-defined for each $i \in I$.

Next, we show that ψ_i is a right R-module homomorphism for each $i \in I$. Towards this end, again fix any $j \in I$. Let $f_1, f_2 \in \mathrm{Hom}_{\mathcal{A}}\left(B, \prod_{i\in I} A_i\right)$, $r \in R$, and $b \in B$. Then since ϕ_j is a group homomorphism, we obtain

$$\begin{aligned}
[\psi_j(f_1 r + f_2)]\,(b) &= [\phi_j \circ (f_1 r + f_2)](b) \\
&= \phi_j((f_1 r + f_2)(b)) \\
&= \phi_j((f_1 r)(b) + f_2(b)) \\
&= \phi_j(f_1(rb) + f_2(b)) \\
&= \phi_j(f_1(rb)) + \phi_j(f_2(b)) \\
&= (\phi_j \circ f_1)(rb) + (\phi_j \circ f_2)(b) \\
&= [\psi_j(f_1)](rb) + [\psi_j(f_2)](b)
\end{aligned}$$

and

$$[\psi_j(f_1)r + \psi_j(f_2)](b) = [\psi_j(f_1)r](b) + [\psi_j(f_2)](b) = [\psi_j(f_1)](rb) + [\psi_j(f_2)](b)$$

and thus $\psi_j(f_1 r + f_2) = \psi_j(f_1)r + \psi_j(f_2)$ so that ψ_j is a right R-module homomorphism. Hence, as $j \in I$ was arbitrary we conclude $(\psi_i : \mathrm{Hom}_{\mathcal{A}}\left(B, \prod_{i\in I} A_i\right) \to \mathrm{Hom}_{\mathcal{A}}(B, A_i))_{i\in I}$ is a family of morphisms of $\mathcal{M}(R)$.

By the previous results, we may now assert that since $\prod_{i\in I} \mathrm{Hom}_{\mathcal{A}}(B, A_i)$ together with $\left(\pi_i : \prod_{i\in I} \mathrm{Hom}_{\mathcal{A}}(B, A_i) \to \mathrm{Hom}_{\mathcal{A}}(B, A_i)\right)_{i\in I}$ is a product for the family of objects $(\mathrm{Hom}_{\mathcal{A}}(B, A_i))_{i\in I}$ of $\mathcal{M}(R)$ that there exists a (unique) right R-module homomorphism

$$\psi : \mathrm{Hom}_{\mathcal{A}}\left(B, \prod_{i\in I} A_i\right) \to \prod_{i\in I} \mathrm{Hom}_{\mathcal{A}}(B, A_i)$$

such that $\pi_i \circ \psi = \psi_i$ for each $i \in I$. Thus, in order to establish that $\mathrm{Hom}_{\mathcal{A}}\left(B, \prod_{i\in I} A_i\right) \simeq \prod_{i\in I} \mathrm{Hom}_{\mathcal{A}}(B, A_i)$ as right R-modules it remains to prove that ψ is a bijection.

First, we prove that ψ is injective. Since ψ is a right R-module homomorphism, it suffices to show that $\ker \psi$ is trivial to establish that ψ is an injection. Towards this end, suppose that $f \in \ker \psi$ so that $\psi(f)$ is equal to the zero element of $\prod_{i\in I} \mathrm{Hom}_{\mathcal{A}}(B, A_i)$. Now, note that $\psi(f) = (\pi_i(\psi(f)))_{i\in I}$ so that by the previous observation we see that $\pi_i(\psi(f)) : B \to A_i$ is the zero map for each $i \in I$. Finally, let $b \in B$ and note that since $f(b) = (\phi_i(f(b)))_{i\in I}$, since $\pi_i \circ \psi = \psi_i$ for each $i \in I$, and by our previous observation that we have

$$\begin{aligned} f(b) &= (\phi_i(f(b)))_{i\in I} \\ &= ((\phi_i \circ f)(b))_{i\in I} \\ &= ([\psi_i(f)](b))_{i\in I} \\ &= ([(\pi_i \circ \psi)(f)](b))_{i\in I} \\ &= ([\pi_i(\psi(f))](b))_{i\in I} \\ &= (0)_{i\in I} \end{aligned}$$

Thus, since $b \in B$ was arbitrary we see that $f : B \to \prod_{i\in I} A_i$ is the zero map. We may now conclude that $\ker \psi$ is trivial and hence ψ is an injection.

Lastly, we prove that ψ is surjective. Indeed, suppose $(f_i)_{i\in I} \in \prod_{i\in I} \mathrm{Hom}_{\mathcal{A}}(B, A_i)$ so that $f_i : B \to A_i$ is a group homomorphism for each $i \in I$. Define a map

$$g : B \to \prod_{i\in I} A_i \quad \text{by} \quad b \mapsto (f_i(b))_{i\in I}$$

In particular, since $f_i : B \to A_i$ is a group homomorphism for each $i \in I$ it is easily verified that g is a well-defined group homomorphism so that $g \in \mathrm{Hom}_{\mathcal{A}}\left(B, \prod_{i\in I} A_i\right)$. Therefore, we may apply ψ to g.

We claim that $\psi(g) = (f_i)_{i\in I}$. Towards this end, notice that $\psi(g) = (\pi_i(\psi(g)))_{i\in I}$. Thus, in order to show that $\psi(g) = (f_i)_{i\in I}$ it follows we must show $\pi_i(\psi(g)) : B \to A_i$ is the same map as $f_i : B \to A_i$ for each $i \in I$. Towards this end, fix any $j \in I$ and let

$b \in B$. Then since $\pi_i \circ \psi = \psi_i$ for each $i \in I$, we have

$$\begin{aligned}
[\pi_j(\psi(g))]\,(b) &= [(\pi_j \circ \psi)(g)](b) \\
&= [\psi_j(g)](b) \\
&= (\phi_j \circ g)(b) \\
&= \phi_j(g(b)) \\
&= \phi_j((f_i(b))_{i\in I}) \\
&= f_j(b)
\end{aligned}$$

and thus $\pi_j(\psi(g)) = f_j$. Since $j \in I$ was arbitrary, we may now conclude that $\psi(g) = (f_i)_{i\in I}$ so that ψ is a surjection. By the above results, we see that ψ is a right R-module isomorphism so that $\mathrm{Hom}_{\mathcal{A}}\left(B, \prod_{i\in I} A_i\right) \simeq \prod_{i\in I} \mathrm{Hom}_{\mathcal{A}}(B, A_i)$ as right R-modules. This completes the proof. $\square$

Problem 31. *Suppose that R and S are rings with identity. Let A be an S, R-bimodule, and B a left R-module. Prove that $A \otimes_R B$ has a unique scalar multiplication making it a left S-module, so that $s(a \otimes_R b) = sa \otimes_R b$, for each $s \in S$, $a \in A$, and $b \in B$.*

Proof. By definition, we have that $A \otimes_R B$ is an abelian group under addition. We now define a left S-module structure on $A \otimes_R B$. Towards this end, let $s \in S$ and define

$$\mu : A \times B \to A \otimes_R B \quad \text{by} \quad (a, b) \mapsto (sa) \otimes_R b$$

Since A is an S, R-bimodule, we see that μ is a well- defined map. We claim that μ is a middle linear map. Towards this end, first let $a_1, a_2 \in A$ and $b \in B$. Then

$$\begin{aligned}
\mu(a_1 + a_1, b) &= (s(a_1 + a_2)) \otimes_R b \\
&= (sa_1 + sa_2) \otimes_R b \\
&= [(sa_1) \otimes_R b] + [(sa_2) \otimes_R b] \\
&= \mu(a_1, b) + \mu(a_2, b)
\end{aligned}$$

Next, let $a \in A$ and $b_1, b_2 \in B$. Then

$$\begin{aligned}
\mu(a, b_1 + b_2) &= (sa) \otimes_R (b_1 + b_2) \\
&= [(sa) \otimes_R b_1] + [(sa) \otimes_R b_2] \\
&= \mu(a, b_1) + \mu(a, b_2)
\end{aligned}$$

Finally, let $a \in A, b \in B$, and $r \in R$. Then since A is an S, R-bimodule, we have

$$\begin{aligned}
\mu(ar, b) &= (s(ar)) \otimes_R b \\
&= ((sa)r) \otimes_R b \\
&= (sa) \otimes_R rb \\
&= \mu(a, rb)
\end{aligned}$$

The previous results show that μ is a middle linear map. Hence, by the definition of the tensor product there exists a unique group homomorphism $s\cdot : A \otimes_R B \to A \otimes_R B$ such that $s \cdot (a \otimes_R b) = \mu(a, b) = (sa) \otimes_R B$ for all $a \in A$ and $b \in B$. Since $s \in S$ was arbitrary, this show that for each $s \in S$ we obtain a unique group homomorphism $s\cdot : A \otimes_R B \to A \otimes_R B$ such that $s \cdot (a \otimes_R b) = \mu(a, b) = (sa) \otimes_R B$ for all $a \in A$ and $b \in B$. We will use this observation below.

Towards this end, we claim that the above results give a left S-module structure on $A \otimes_R B$. Indeed, let $s \in S$. Then by the above, there is a unique group homomorphism $s\cdot : A \otimes_R B \to A \otimes_R B$ such that $s \cdot (a \otimes_R b) = \mu(a, b) = (sa) \otimes_R B$ for all $a \in A$ and $b \in B$. Now, let $u \in A \otimes_R B$. Then we may write $u = \sum_{i=1}^n a_i \otimes_R b_i$ for some $a_1, \ldots, a_n \in A$ and $b_1, \ldots, b_n \in B$. Define

$$s \cdot u = \sum_{i=1}^n s \cdot (a_i \otimes_R b_i) \in A \otimes_R B$$

In order to see that this action is indeed well-defined, suppose that

$$\sum_{i=1}^{n} a_i \otimes_R b_i = u = \sum_{i=1}^{m} c_i \otimes_R d_i$$

for some $c_1, \ldots, c_m \in A$ and $d_1, \ldots, d_m \in B$. Then since $s\cdot$ is a group homomorphism, we obtain

$$\begin{aligned} 0 = 0 \otimes_R 0 = (s0) \otimes_r 0 &= s \cdot (0 \otimes_R 0) \\ &= s \cdot \left(\sum_{i=1}^{n} a_i \otimes_R b_i - \sum_{i=1}^{m} c_i \otimes_R d_i \right) \\ &= s \cdot \sum_{i=1}^{n} a_i \otimes_R b_i - s \cdot \sum_{i=1}^{m} c_i \otimes_R d_i \end{aligned}$$

and hence

$$s \cdot \sum_{i=1}^{n} a_i \otimes_R b_i = s \cdot \sum_{i=1}^{m} c_i \otimes_R d_i$$

which shows that the action of S on $A \otimes_R B$ is well-defined.

Finally, we prove that the above left action of S on $A \otimes_R B$ satisfies the four left module axioms. First, let $u_1, u_2 \in A \otimes_R B$ and $s \in S$. Then since $s\cdot$ is a group homomorphism, we have

$$s \cdot (u_1 + u_2) = s \cdot u_1 + s \cdot u_2$$

Next, let $u \in A \otimes_R B$ and write $u = \sum_{i=1}^{n} a_i \otimes_R b_i$ for some $a_1, \ldots, a_n \in A$ and $b_1, \ldots b_n \in B$ and let $s_1, s_2 \in S$ and write $s = s_1 + s_2 \in S$. Then since $s\cdot, s_1\cdot$, and $s_2\cdot$ are group homomorphisms, by the properties of $s\cdot, s_1\cdot$, and $s_2\cdot$, and since A is an

S, R-bimodule, we have

$$\begin{aligned}
(s_1 + s_2) \cdot u &= s \cdot \sum_{i=1}^{n} a_i \otimes_R b_i \\
&= \sum_{i=1}^{n} s \cdot (a_i \otimes_R b_i) \\
&= \sum_{i=1}^{n} (sa_i) \otimes_R b_i \\
&= \sum_{i=1}^{n} [(s_1 + s_2)a_i] \otimes_R b_i \\
&= \sum_{i=1}^{n} (s_1 a_i + s_2 a_i) \otimes_R b_i \\
&= \sum_{i=1}^{n} [((s_1 a_i) \otimes_R b_i) + ((s_2 a_i) \otimes_R b_i)] \\
&= \sum_{i=1}^{n} (s_1 a_i) \otimes_R b_i + \sum_{i=1}^{n} (s_2 a_i) \otimes_R b_i \\
&= \sum_{i=1}^{n} s_1 \cdot (a_i \otimes_R b_i) + \sum_{i=1}^{n} s_2 \cdot (a_i \otimes_R b_i) \\
&= s_1 \cdot \sum_{i=1}^{n} a_i \otimes_R b_i + s_2 \cdot \sum_{i=1}^{n} a_i \otimes_R b_i \\
&= s_1 \cdot u + s_2 \cdot u
\end{aligned}$$

Next, let $u \in A \otimes_R B$ and write $u = \sum_{i=1}^{n} a_i \otimes_R b_i$ for some $a_1, \ldots, a_n \in A$ and $b_1, \ldots, b_n \in B$ and let $s_1, s_2 \in S$. Then since $s_1 \cdot$ and $s_2 \cdot$ are group homomorphisms, by

the properties of $s_1\cdot$ and $s_2\cdot$, and since A is an S, R-bimodule, we have

$$\begin{aligned}
s_1 \cdot (s_2 \cdot u) &= s_1 \cdot \left(s_2 \cdot \sum_{i=1}^{n} a_i \otimes_R b_i \right) \\
&= s_1 \cdot \sum_{i=1}^{n} s_2 \cdot (a_i \otimes_R b_i) \\
&= s_1 \cdot \sum_{i=1}^{n} (s_2 a_i) \otimes_R b_i \\
&= \sum_{i=1}^{n} s_1 \cdot ((s_2 a_i) \otimes_R b_i) \\
&= \sum_{i=1}^{n} (s_1(s_2 a_i)) \otimes_R b_i \\
&= \sum_{i=1}^{n} ((s_1 s_2) a_i) \otimes_R b_i \\
&= \sum_{i=1}^{n} s_1 s_2 \cdot (a_i \otimes_R b_i) \\
&= s_1 s_2 \cdot \sum_{i=1}^{n} a_i \otimes_R b_i \\
&= (s_1 s_2) \cdot u
\end{aligned}$$

Finally, let $u \in A \otimes_R B$ and write $u = \sum_{i=1}^{n} a_i \otimes_R b_i$ for some $a_1, \ldots, a_n \in A$ and $b_1, \ldots, b_n \in B$. Then since $1\cdot$ is a group homomorphism, by the properties of $1\cdot$, and since A is an S, R-bimodule, we have

$$1 \cdot u = 1 \cdot \sum_{i=1}^{n} a_i \otimes_R b_i = \sum_{i=1}^{n} 1 \cdot (a_i \otimes_R b_i) = \sum_{i=1}^{n} (1 a_i) \otimes_R b_i = \sum_{i=1}^{n} a_i \otimes_R b_i = u$$

By the above results, we conclude that $A \otimes_R B$ has a unique scalar multiplication making it a left S-module with the properties as outlined in the statement of this problem. This completes the proof. $\square$

Problem 32. *Let R be a commutative ring with identity, and suppose that B is an R-module, and I is an ideal of R. Prove that $R/I \otimes_R B \simeq B/IB$, where IB is the R-submodule of B generated by all elements of the form rb, with $r \in I, b \in B$.*

Proof. First, define a map

$$f : R/I \times B \to B/IB \quad \text{by} \quad (r+I, b) \mapsto rb + IB$$

Note that since B is an R-module that f is indeed a map. Next, we show that f is well-defined. Towards this end, suppose that $(r_1 + I, b_1) = (r_2 + I, b_2)$ for some $(r_1 + I, b_1), (r_2 + I, b_2) \in R/I \times B$. Clearly, this gives $r_1 + I = r_2 + I$ so that $r_1 - r_2 \in I$ and that $b_1 = b_2$ so that we may write $b_1 = b_2 = b \in B$. Now, since $r_1 - r_2 \in I$ and $b \in B$ we have $(r_1 - r_2)b \in IB$ and hence

$$\begin{aligned} f(r_1 + I, b_1) - f(r_2 + I, b_2) &= f(r_1 + I, b) - f(r_2 + I, b) \\ &= (r_1 b + IB) - (r_2 b + IB) \\ &= (r_1 - r_2)b + IB \\ &= IB \end{aligned}$$

In particular, the above result shows that $f(r_1 + I, b_1) - f(r_2 + I, b_2)$ is equal to the identity element of B/IB so that $f(r_1 + I, b_1) = f(r_2 + I, b_2)$ which shows that f is well-defined. Furthermore, since R is commutative it is easily verified that f is an R-bilinear map and hence by the definition of the tensor product there exists a (unique) R-module homomorphism $\phi : R/I \otimes_R B \to B/IB$ such that $\phi((r+I) \otimes_R b) = f(r+I, b) = rb + IB$ for all $r + I \in R/I$ and $b \in B$.

Now, let $r_1 + I, r_2 + I \in R/I$ and $b_1, b_2 \in B$. Let $b = r_1 b_1 + r_2 b_2$. Then since B is an R-module, we have that $b \in B$. Furthermore, as R has identity we have that

$$\begin{aligned} ((r_1 + I) \otimes_R b_1) + ((r_2 + I) \otimes_R b_2) &= (r_1(1 + I) \otimes_R b_1) + (r_2(1 + I) \otimes_R b_2) \\ &= ((1 + I) \otimes_R r_1 b_1) + ((1 + I) \otimes_R r_2 b_2) \\ &= (1 + I) \otimes_R (r_1 b_1 + r_2 b_2) \\ &= (1 + I) \otimes_R b \end{aligned}$$

Inductively, this equality shows that any finite sum of elements of the form $(r + I) \otimes_R b$ where $r + I \in R/I$ and $b \in B$ is of the form $(1 + I) \otimes_R c$ where $c \in B$. Therefore, since every element of $R/I \otimes_R B$ is a finite sum of elements of the form $(r + I) \otimes_R b$ where $r + I \in R/I$ and $b \in B$ it now follows that every element of $R/I \otimes_R B$ is of the form $(1 + I) \otimes_R c$ where $c \in B$.

Next, we show that ϕ is an injection. Towards this end, suppose that $x \in \ker \phi$. By the previous observation, we may write $x = (1 + I) \otimes_R b$ where $b \in B$. Now, since $x \in \ker \phi$ we have

$$IB = \phi(x) = \phi((1 + I) \otimes_R b) = 1b + IB = b + IB$$

so that $b \in IB$. Therefore, we may write $b = \sum_{j=1}^{n} i_j b_j$ for some $i_1, \ldots, i_n \in I$ and $b_1, \ldots, b_n \in B$. This gives

$$\begin{aligned}
x &= (1+I) \otimes_R b \\
&= (1+I) \otimes_R \left(\sum_{j=1}^{n} i_j b_j \right) \\
&= \sum_{j=1}^{n} [(1+I) \otimes_R i_j b_j] \\
&= \sum_{j=1}^{n} [i_j (1+I) \otimes_R b_j] \\
&= \sum_{j=1}^{n} [(i_j \cdot 1 + I) \otimes_R b_j] \\
&= \sum_{j=1}^{n} [(i_j + I) \otimes_R b_j] \\
&= \sum_{j=1}^{n} (I \otimes_R b_j) \\
&= I \otimes_R \left(\sum_{j=1}^{n} b_j \right) \\
&= 0
\end{aligned}$$

and hence $x = 0$ so that $\ker \phi$ is trivial. We conclude that ϕ is an injection.

Finally, we show that ϕ is a surjection. Towards this end, let $b + IB \in B/IB$. Then clearly $(1+I) \otimes_R b \in R/I \otimes_R B$ and

$$\phi((1+I) \otimes_R b) = 1b + IB = b + IB$$

so that ϕ is a surjection. By the above results, we conclude that ϕ is an R-module isomorphism so that $R/I \otimes_R B \simeq B/IB$ as R-modules. This completes the proof. $\square$

Problem 33. *Suppose that R is a commutative ring with identity. Let $F(m)$ and $F(n)$ be the free R-modules on m and n generators, respectively. Prove that if $F(m) \simeq F(n)$, then $m = n$.*

Proof. Since $F(m)$ and $F(n)$ are the free R-modules on m and n generators, respectively, we know that $F(m) \simeq \bigoplus_{i=1}^{m} R$ and $F(n) \simeq \bigoplus_{i=1}^{n} R$. For simplicity, we will write $F(m) \simeq R^m$ and $F(n) \simeq R^n$. Since $F(m) \simeq F(n)$ by hypothesis, it follows that there is an R-module isomorphism $\phi : R^m \to R^n$.

Now, since R is a commutative ring with identity there exists some maximal ideal I of R and as I is an ideal of R it follows that IR^n is an ideal of R^n. Therefore, we may consider the canonical projection map $\pi : R^n \to R^n/IR^n$. In particular, we have that π is a surjective R-module homomorphism. Thus, as the defined composition of R-module homomorphisms is an R-module homomorphism we see that $\pi \circ \phi : R^m \to R^n/IR^n$ is an R-module homomorphism.

We claim that $\ker(\pi \circ \phi) = IR^m$. Towards this end, first suppose that $x \in \ker(\pi \circ \phi)$. In this case, we obtain

$$IR^n = (\pi \circ \phi)(x) = \pi(\phi(x)) = \phi(x) + IR^n$$

and thus $\phi(x) \in IR^n$. Therefore, there are $i_1, \ldots, i_k \in I$ and $s_1, \ldots, s_k \in R^n$ such that

$$\phi(x) = \sum_{j=1}^{k} i_j s_j$$

Now, since $\phi : R^m \to R^n$ is a surjection and as $s_1, \ldots, s_k \in R^n$ it follows that there are elements $r_1, \ldots, r_k \in R^m$ such that $\phi(r_1) = s_1, \ldots, \phi(r_k) = s_k$. Thus, we obtain since ϕ is an R-module isomorphism and as $i_1, \ldots, i_k \in I \subseteq R$ that

$$\phi(x) = \sum_{j=1}^{k} i_j s_j = \sum_{j=1}^{k} i_j \phi(r_j) = \sum_{j=1}^{k} \phi(i_j r_j) = \phi\left(\sum_{j=1}^{k} i_j r_j\right)$$

Hence, as ϕ is an injection the above equality implies that $x = \sum_{j=1}^{n} i_j r_j$. Furthermore, recall that $r_1, \ldots, r_k \in R^m$. By the previous equality, this observation now gives

$$x = \sum_{j=1}^{k} i_j r_j \in IR^m$$

On the other hand, suppose that $x \in IR^m$. Then there are $i_1, \ldots, i_k \in I$ and $r_1, \ldots, r_k \in R^m$ such that $x = \sum_{j=1}^{k} i_j r_j$. Thus, we obtain since ϕ is an R-module isomorphism and

as $i_1, \ldots, i_k \in I \subseteq R$ that

$$\begin{aligned}(\pi \circ \phi)(x) &= \pi(\phi(x)) \\ &= \pi\left(\phi\left(\sum_{j=1}^{k} i_j r_j\right)\right) \\ &= \pi\left(\sum_{j=1}^{k} \phi(i_j r_j)\right) \\ &= \pi\left(\sum_{j=1}^{k} i_j \phi(r_j)\right) \\ &= \sum_{j=1}^{k} i_j \phi(r_j) + IR^n\end{aligned}$$

But since $\phi(r_j) \in R^n$ for each $j \in \{1, \ldots, k\}$ it now follows that $\sum_{j=1}^{k} i_j \phi(r_j) \in IR^n$. Thus, we obtain by the above equality that

$$(\pi \circ \phi)(x) = \sum_{j=1}^{k} i_j \phi(r_j) + IR^n = IR^n$$

so that $x \in \ker(\pi \circ \phi)$. The previous result now give $\ker(\pi \circ \phi) = IR^n$.

Next, note that since π and ϕ are surjections and since the defined composition of two surjections is a surjection we have that $\pi \circ \phi$ is a surjection. Combining the previous results, we now have by the First Isomorphism Theorem for Modules that

$$R^m/IR^m = R^m/\ker(\pi \circ \phi) \simeq R^n/IR^n$$

as R-modules. We will use this fact below.

Now, notice that by the results of the previous problem we have

$$R/I \otimes_R R^m \simeq R^m/IR^m \quad R/I \otimes_R R^n \simeq R^n/IR^n$$

where the above isomoprhisms are isomorphisms of R-modules. Therefore, as $R^m/IR^m \simeq R^n/IR^n$ as R-modules by the above observation we obtain

$$R/I \otimes_R R^m \simeq R^m/IR^m \simeq R^n/IR^n \simeq R/I \otimes_R R^n$$

where the above isomorphisms are isomorphisms of R-modules. Therefore, we have that $R/I \otimes_R R^m \simeq R/I \otimes_R R^n$ as R-modules.

Next, we claim that $R/I \otimes_R R^m \simeq (R/I)^m$ as R-modules. Indeed, note that since the tensor product distributes over direct sums and as clearly $R/I \otimes_R R \simeq R/I$ we have

$$\begin{aligned} R/I \otimes_R R^m &= R/I \otimes_R \underbrace{(R \oplus \cdots \oplus R)}_{m \text{ times}} \\ &\simeq \underbrace{(R/I \otimes_R R) \oplus \cdots \oplus (R/I \otimes_R R)}_{m \text{ times}} \\ &\simeq \underbrace{R/I \oplus \cdots \oplus R/I}_{m \text{ times}} \\ &= (R/I)^m \end{aligned}$$

where the above isomorphisms are isomorphisms of R-modules. Therefore, we have that $R/I \otimes_R R^m \simeq (R/I)^m$ as R-modules. In exactly the same fashion, we have that $R/I \otimes_R R^n \simeq (R/I)^n$ as R-modules. Combining the previous two results with the result from the above, we now have

$$(R/I)^m \simeq R/I \otimes_R R^m \simeq R/I \otimes_R R^n \simeq (R/I)^n$$

where the above isomorphisms are isomorphisms of R-modules. Therefore, we have that $(R/I)^m \simeq (R/I)^n$ as R-modules.

Finally, note that since $(R/I)^m \simeq (R/I)^n$ as R-modules it follows that we also have $(R/I)^m \simeq (R/I)^n$ as R/I-modules. But recall that I is a maximal ideal of R. Thus, as R is a commutative ring with identity it follows that R/I is a field and hence $(R/I)^m$ and $(R/I)^n$ are finite dimensional vector spaces of dimensions m and n, respectively, over the field R/I. But recall that two finite dimensional vector spaces over a field are isomorphic if and only if they are of the same dimension over that field. Therefore, since $(R/I)^m$ and $(R/I)^n$ are R/I-isomorphic vector spaces over the field R/I of finite dimensions m and n, respectively, it now follows that these dimensions must be equal so that $m = n$. This completes the proof. $\square$

Problem 34. *Suppose that R is a commutative ring with identity, and that I is an ideal of R. Define the radical $\sqrt{I}$, and prove that $\sqrt{I}$ is the intersection of all prime ideals of R that contain I.*

Proof. In the situation of the statement of this problem, we define the ***radical*** of I, denoted $\sqrt{I}$, to be the set

$$\sqrt{I} = \{r \in R : r^n \in I \text{ for some } n \in \{1, 2, \dots\}\}$$

We now show that $\sqrt{I}$ equal to the intersection of all prime ideals of R that contain I.

First, suppose that $r \in \sqrt{I}$. Then $r^n \in I$ for some $n \in \{1, 2, \dots\}$. Now, let P be a prime ideal of R with $I \subseteq P$. In this case, we have $r^n \in I \subseteq P$ so that $r^n \in P$. But since P is a prime ideal of R with $r^n \in P$ we have that $r \in P$. Thus, as P was an arbitrary prime ideal of R containing I this shows that r is in the intersection of all prime ideals of R that contain I.

On the other hand, suppose that $r \in R$ is in the intersection of all prime ideals of R that contain I. For the sake of contradiction, suppose that $r \notin \sqrt{I}$. Then for each $n \in \{1, 2, \dots\}$ we have that $r^n \notin I$. Now, consider the set

$$S = \{r^n : n \in \{1, 2, \dots\}\}$$

and note that S is clearly a multiplicative subset of R. Moreover, since $r^n \notin I$ for each $n \in \{1, 2, \dots\}$ we have that $I \cap S = \emptyset$. Therefore, there exists an ideal P of R containing I that is maximal among all ideals of R containing I which have an empty intersection with S. In addition, we know that this ideal P is a prime ideal of R. Therefore, since P is a prime ideal of R containing I we have that $r \in P$ since r is in the intersection of all prime ideals of R that contain I. However, this would imply that $r \in P \cap S$ since clearly $r \in S$ which contradicts the fact that P has an empty intersection with S. We conclude that $r \in \sqrt{I}$ and hence we have that the radical $\sqrt{I}$ of I is equal to the intersection of all prime ideals of R containing I. This completes the proof. $\square$

Problem 43. *Let R be a commutative ring with identity, which satisfies the ascending chain condition on prime ideals. Must R be Noetherian? Prove, or else give a counterexample.*

Proof. We claim that this statement is false. Indeed, let F be a field and consider the polynomial ring $F[x_1, x_2, \dots]$ in infinitely many indeterminants $x_1, x_2, \dots$. Define

$$R = \frac{F[x_1, x_2, \dots]}{(x_1^2, x_2^2, \dots)}$$

Since F is a field, we clearly have that R is a commutative ring with identity. We claim that R satisfies the ascending chain condition on prime ideals but is not Noetherian.

In order to show that R satisfies the ascending chain condition on prime ideals, it will clearly suffice to show that R has a unique prime ideal. Towards this end, let P be a prime ideal of R and recall that the set of nilpotent elements of a commutative ring with identity is equal to the intersection of the prime ideals of that ring. Now, note that

$$\overline{x_n}^2 = (x_n + (x_1^2, x_2^2, \dots))^2 = x_n^2 + (x_1^2, x_2^2, \dots) = (x_1^2, x_2^2, \dots)$$

so that $\overline{x_n}$ is a nilpotent element of R for each positive integer n. Thus, we now have that $\overline{x_1}, \overline{x_2}, \dots$ are nilpotent elements of R so that by our above observation we have $\overline{x_1}, \overline{x_2}, \dots \in P$ as P is a prime ideal of R. Therefore, since P is an ideal of R we obtain that $(\overline{x_1}, \overline{x_2}, \dots) \subseteq P$.

Now, notice that clearly $R/(\overline{x_1}, \overline{x_2}, \dots) \simeq F$. Therefore, since F is a field it now follows that $(\overline{x_1}, \overline{x_2}, \dots)$ is a maximal ideal of R. Moreover, since P is a prime ideal of R we have in particular that $P \neq R$. Hence, as $(\overline{x_1}, \overline{x_2}, \dots) \subseteq P$ and since $(\overline{x_1}, \overline{x_2}, \dots)$ is a maximal ideal of R it now follows that $P = (\overline{x_1}, \overline{x_2}, \dots)$. Since P was an arbitrary prime ideal of R, we may now assert that the unique prime ideal of R is $(\overline{x_1}, \overline{x_2}, \dots)$ and hence R clearly satisfies the ascending chain condition on prime ideals.

Finally, we show that R not Noetherian. Towards this end, recall that R is Noetherian if and only if every ideal of R is finitely generated. However, note that the ideal $(\overline{x_1}, \overline{x_2}, \dots)$ of R is clearly not finitely generated. We conclude, therefore, that R is not Noetherian. Since R satisfies the ascending chain condition on prime ideals but as R is not Noetherian, this completes the proof of our claim. $\square$

Problem 44. *Prove that an Artinian commutative ring R with identity has only a finite number of prime ideals, and that each one is a maximal ideal.*

Proof. We first show that any prime ideal of R is a maximal ideal of R. Towards this end, recall that the ring homomorphic image of an Artinian ring is an Artinian ring. Now, consider the canonical projection map $\pi : R \to R/P$ and recall that π is a surjective ring homomorphism. By our previous observation, then, we see that R/P is an Artinian ring since R is an Artinian ring by hypothesis. Moreover, since P is a prime ideal of R we have that R/P is an integral domain. Combining the previous results, then, we conclude that R/P is an Artinian integral domain and is hence a field by a previous homework. Thus, since R/P is a field we see that the prime ideal P of R is in fact a maximal ideal of R.

To complete the proof, it remains to show that there are only finitely many prime ideals of R. Towards this end, note that it suffices to show that R has only finitely many maximal ideals since each prime ideal of R is a maximal ideal of R by the above result. Now, for the sake of contradiction assume that R had infinitely many maximal ideals. Then there are distinct maximal ideals $M_1, M_2, \ldots$ of R. For each positive integer n, let $I_n = M_1 \cdots M_n$. Clearly, we have that I_n is an ideal of R and that

$$I_n = M_1 \cdots M_n \supseteq M_1 \cdots M_n M_{n+1} = I_{n+1}$$

for each positive integer n so that we have the descending chain of ideals of R

$$I_1 \supseteq I_2 \supseteq I_3 \supseteq \cdots$$

Therefore, since R is Artinian there is a positive integer N such that $I_n = I_N$ for each integer $n \geq N$.

Now, by the above we have in particular that

$$M_1 \cdots M_N = I_N = I_{N+1} = M_1 \cdots M_{N+1}$$

and hence

$$M_1 \cdots M_N = M_1 \cdots M_{N+1} \subseteq M_{N+1}$$

Finally, recall that M_{N+1} is a maximal ideal of R and hence a prime ideal of R. By arguments from previous lectures, this observation together with the above inclusion imply that there is some $K \in \{1, \ldots, N\}$ with $M_K \subseteq M_{N+1}$. Furthermore, since M_{N+1} is a maximal ideal of R we have in particular that $M_{N+1} \neq R$. Therefore, by the previous inclusion and since M_K is a maximal ideal of R we see $M_K = M_{N+1}$. However, this is a contradiction as $K \in \{1, \ldots, N\}$ and as $M_1, M_2, \ldots$ are distinct maximal ideals of R. This completes the proof. $\square$

Part 3: Fall Semester 2016

Problem 60. *Let Θ_p be the pth cyclotomic polynomial over the field $\mathbb{Q}$, where p is a prime number. Outline an argument which shows that the Galois group of the splitting field of Θ_p over $\mathbb{Q}$ is cyclic of order $p-1$. (Clearly identify the results you need for the argument).*

Proof. The **first result** we require is the following:

Let n be a positive integer and let $g_n(x)$ denote the nth cyclotomic polynomial over $\mathbb{Q}$. Then we have

$$x^n - 1 = \prod_{d|n} g_d(x)$$

In our case, since p is prime, this result gives that

$$\Theta_p(x) = \frac{x^p - 1}{\prod_{d|p, d<p} g_d(x)} = \frac{x^p - 1}{g_1(x)}$$

But since $g_1(x) = x - 1$ we have that

$$\Theta_p(x) = \frac{x^p - 1}{x - 1} = \frac{(x-1)(x^{p-1} + x^{p-2} + \cdots + x + 1)}{x - 1} = x^{p-1} + x^{p-2} + \cdots + x + 1$$

Now, let ζ be a primitive pth root of unity. Then the roots of $\Theta_p(x)$ are $\zeta, \zeta^2, \ldots, \zeta^{p-1}$. Therefore, we see that $\mathbb{Q}(\zeta)$ is a splitting field for $\Theta_p(x)$ over $\mathbb{Q}$. Let G denote the Galois group of the splitting field of $\Theta_p(x)$ over $\mathbb{Q}$. Then by the above, we have that $G = \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$. Furthermore, since $\mathbb{Q}(\zeta)$ is a splitting field for $\Theta_p(x)$ over $\mathbb{Q}$ and since $\mathrm{char}(\mathbb{Q}) = 0$, we have that $\mathbb{Q}(\zeta)/\mathbb{Q}$ is a finite Galois extension so that $|G| = [\mathbb{Q}(\zeta) : \mathbb{Q}]$.

The **second result** we require is the following:

If q is a prime number, then the polynomial

$$x^{q-1} + x^{q-2} + \cdots + x + 1$$

is irreducible over $\mathbb{Z}$.

In our case, since p is prime, this result gives that $\Theta_p(x)$ is irreducible over $\mathbb{Z}$. But since $\mathbb{Q}$ is the field of fractions of $\mathbb{Z}$, it follows by Gauss' Lemma that $\Theta_p(x)$ is irreducible over $\mathbb{Q}$. Hence, since $\Theta_p(x) \in \mathbb{Q}[x]$ is a monic, irreducible polynomial and has ζ as a root, it follows that $\Theta_p(x)$ is the minimum polynomial for ζ over $\mathbb{Q}$. Combining the above results, then, we obtain

$$|G| = [\mathbb{Q}(\zeta) : \mathbb{Q}] = \deg(\Theta_p(x)) = p - 1$$

This shows that G has order $p-1$. So, it remains to prove that G is cyclic.

The **third result** we require is the following:

Let K be a field and let n be a positive integer such that $\mathrm{char}(K)$ *does not divide n. Suppose that F is a splitting field for the polynomial $x^n - 1$ over K. Then* $\mathrm{Gal}(F/K)$ *is isomorphic to a subgroup of $\mathbb{Z}_n^\times$.*

In our case, consider the polynomial $x^p - 1 \in \mathbb{Q}[x]$. Note that the roots of $x^p - 1$ are $1, \zeta, \zeta^2, \ldots, \zeta^{p-1}$ so that $\mathbb{Q}(\zeta)$ is a splitting field for $x^p - 1$ over $\mathbb{Q}$. Since $\mathrm{char}(\mathbb{Q}) = 0$, we clearly have that $\mathrm{char}(\mathbb{Q})$ does not divide p. By the above result, then, we have that $G = \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ is isomorphic to a subgroup of $\mathbb{Z}_p^\times$. However, as has been established above, we know that

$$|G| = p - 1 = |\mathbb{Z}_p^\times|$$

Therefore, we conclude that G is isomorphic to $\mathbb{Z}_p^\times$. But since p is prime, we know that $\mathbb{Z}_p$ is a field. Hence, as $\mathbb{Z}_p^\times$ is a finite subgroup of $\mathbb{Z}_p^\times$ and since finite subgroups of the group of units of a field are cyclic, it follows that $\mathbb{Z}_p^\times$ is cyclic. Hence, we conclude that G is cyclic. This completes the proof. $\square$

Problem 61. *Compute the Galois groups of the splitting fields of the following polynomials, over* $\mathbb{Q}$*:*

(a): $p(x) = x^5 - 2$.

(b): $p(x) = x^3 - 3x + 3$.

Proof. (a): Let G be the Galois group of $p(x)$ over $\mathbb{Q}$ and let Γ be the set of roots of $p(x)$. Let $u = 2^{1/5}$ and let ζ be a primitive fifth root of unity. Then we have

$$\Gamma = \{u, u\zeta, u\zeta^2, u\zeta^3, u\zeta^4\}$$

Thus, we see that $\mathbb{Q}(u, \zeta)$ is a splitting field of $p(x)$ over $\mathbb{Q}$.

Now, since ζ is a primitive fifth root of unity, it follows that

$$1 + \zeta + \zeta^2 + \zeta^3 + \zeta^4 = 0$$

so that ζ is a root of $x^4 + x^3 + x^2 + x + 1 \in \mathbb{Q}[x]$. Since 5 is prime, it follows that $x^4 + x^3 + x^2 + x + 1$ is irreducible over $\mathbb{Q}$. Thus, since $x^4 + x^3 + x^2 + x + 1 \in \mathbb{Q}[x]$ is a monic, irreducible polynomial and has ζ as a root, it follows that $x^4 + x^3 + x^2 + x + 1$ is the minimum polynomial for ζ over $\mathbb{Q}$. Therefore, we have

$$[\mathbb{Q}(\zeta) : \mathbb{Q}] = \deg(x^4 + x^3 + x^2 + x + 1) = 4$$

Now, $p(x)$ is irreducible over $\mathbb{Q}$ by Eisenstein's Criterion. Thus, since $p(x) \in \mathbb{Q}[x]$ is a monic, irreducible polynomial and has u as a root, it follows that $p(x)$ is the minimum polynomial for u over $\mathbb{Q}$. Therefore, we have

$$[\mathbb{Q}(u) : \mathbb{Q}] = \deg(p(x)) = 5$$

Notice that

$$[\mathbb{Q}(u, \zeta) : \mathbb{Q}(\zeta)][\mathbb{Q}(\zeta) : \mathbb{Q}] = [\mathbb{Q}(u, \zeta) : \mathbb{Q}] = [\mathbb{Q}(u, \zeta) : \mathbb{Q}(u)][\mathbb{Q}(u) : \mathbb{Q}]$$

Thus, by the above computations, we see that 4 and 5 both divide $[\mathbb{Q}(u, \zeta) : \mathbb{Q}]$ so that 20 divides $[\mathbb{Q}(u, \zeta) : \mathbb{Q}]$. Finally, notice that we clearly have $[\mathbb{Q}(u, \zeta) : \mathbb{Q}(\zeta)] \leq 5$. Therefore, we have

$$[\mathbb{Q}(u, \zeta) : \mathbb{Q}] = [\mathbb{Q}(u, \zeta) : \mathbb{Q}(\zeta)][\mathbb{Q}(\zeta) : \mathbb{Q}] = 4[\mathbb{Q}(u, \zeta) : \mathbb{Q}(\zeta)] \leq 4 \cdot 5 = 20$$

But since 20 divides $[\mathbb{Q}(u, \zeta) : \mathbb{Q}]$, it now follows that $[\mathbb{Q}(u, \zeta) : \mathbb{Q}] = 20$.

Now, we have by definition that $G = \mathrm{Gal}(\mathbb{Q}(u, \zeta)/\mathbb{Q})$. Since $p(x) \in \mathbb{Q}[x]$ is irreducible and since $\mathrm{char}(\mathbb{Q}) = 0$, it follows that $p(x)$ is separable. Thus, we obtain that $\mathbb{Q}(u, \zeta)/\mathbb{Q}$ is a finite Galois extension. It now follows by this observation and the above result that

$$|G| = |\,\mathrm{Gal}(\mathbb{Q}(u, \zeta)/\mathbb{Q})| = [\mathbb{Q}(u, \zeta) : \mathbb{Q}] = 20$$

Now, it follows by the above computations that $[\mathbb{Q}(u, \zeta) : \mathbb{Q}(u)] = 4$. Therefore, the minimum polynomial for ζ over $\mathbb{Q}(u)$ is $x^4 + x^3 + x^2 + x + 1$, which implies that $x^4 + x^3 + x^2 + x + 1$ is irreducible over $\mathbb{Q}(u)$. Notice that $\zeta, \zeta^2, \zeta^3, \zeta^4$ are the roots of $x^4 + x^3 + x^2 + x + 1$. Therefore, since $x^4 + x^3 + x^2 + x + 1$ is irreducible over $\mathbb{Q}(u)$, for each $i \in \{1, 2, 3, 4\}$, there is a $\mathbb{Q}(u)$-homomorphism $\sigma_i : \mathbb{Q}(u, \zeta) \to \mathbb{Q}(u, \zeta)$ which is

an isomorphism such that $\sigma_i(\zeta) = \zeta^i$. In particular, note that $\{\sigma_1, \sigma_2, \sigma_3, \sigma_4\} \subseteq G$. Let $H_1 = \{\sigma_1, \sigma_2, \sigma_3, \sigma_4\}$.

Similarly, it follows by the above computations that $[\mathbb{Q}(u, \zeta) : \mathbb{Q}(\zeta)] = 5$. Therefore, the minimum polynomial for u over $\mathbb{Q}(\zeta)$ is $p(x)$, which implies that $p(x)$ is irreducible over $\mathbb{Q}(\zeta)$. Recall that Γ as defined above is the set of roots of $p(x)$. Therefore, since $p(x)$ is irreducible over $\mathbb{Q}(\zeta)$, for each $i \in \{0, 1, 2, 3, 4\}$, there is a $\mathbb{Q}(\zeta)$-homomorphism $\tau_i : \mathbb{Q}(u, \zeta) \to \mathbb{Q}(u, \zeta)$ which is an isomorphism such that $\tau_i(u) = u\zeta^i$. In particular, note that $\{\tau_0, \tau_1, \tau_2, \tau_3, \tau_4\} \subseteq G$. Let $H_2 = \{\tau_0, \tau_1, \tau_2, \tau_3, \tau_4\}$.

Now, note that H_1 is a group since the above shows that $H_1 = \mathrm{Gal}(\mathbb{Q}(u, \zeta)/\mathbb{Q}(u))$. Similarly, we see that H_2 is a group since the above shows that $H_2 = \mathrm{Gal}(\mathbb{Q}(u, \zeta)/\mathbb{Q}(\zeta))$.

By the definition of H_1, it follows that H_1 is isomorphic to $\mathbb{Z}_5^\times$, which is a cyclic group since 5 is a prime number. We claim that H_1 is not normal in G. Indeed, suppose to the contrary that $H_1 \trianglelefteq G$. Then by the Fundamental Theorem of Galois Theory, it follows that $\mathbb{Q}(u)/\mathbb{Q}$ is a finite Galois extension. Therefore, $\mathbb{Q}(u)$ is a splitting field of a polynomial in $\mathbb{Q}[x]$. However, this is not possible. Therefore, we conclude that H_1 is not normal in G.

Next, notice that since $|H_2| = 5$ we have that $H_2 \in \mathrm{Syl}_5(G)$. Furthermore, we know that $n_5(G)$ is congruent to 1 modulo 5 and that $n_5(G)$ divides $2^2 = 4$. Therefore, we have that $n_5(G) = 1$ so that $H_2 \trianglelefteq G$.

Finally, note that $H_1 \cap H_2 = \{1\}$ since H_1 is a group of order 4 and H_2 is a group of order 5. Therefore, we obtain

$$|H_1H_2| = \frac{|H_1||H_2|}{|H_1 \cap H_2|} = \frac{4 \cdot 5}{1} = 20 = |G|$$

Therefore, we have that $G = H_1H_2$.

The above results show that $G = H_2 \rtimes H_1$, where H_1 is a cyclic group of order 4 and H_2 is a cyclic group of order 5. This completes the proof. $\square$

Proof. (b): Let G be the Galois group of $p(x)$ over $\mathbb{Q}$. By the Rational Root Theorem, the only possible rational roots of $p(x)$ are 3 and -3. However, notice that $p(3) \neq 0$ and $p(-3) \neq 0$. Therefore, $p(x)$ has no rational roots and since $\deg(p(x)) = 3$, it now follows that $p(x)$ is irreducible over $\mathbb{Q}$. Furthermore, since $\mathrm{char}(\mathbb{Q}) = 0$ and $p(x)$ is irreducible over $\mathbb{Q}$, we have that $p(x)$ is separable.

Now, we know that G is isomorphic to a subgroup of S_3. In addition, since $p(x)$ is irreducible over $\mathbb{Q}$ and is separable, we have that $3 = \deg(p(x))$ divides $|G|$. Therefore, we have that $G \in \{A_3, S_3\}$. Finally, note that the discriminant D of $p(x)$ is

$$D = -4(-3)^3 - 27(3)^2 = 27(4) - 27(9) < 0$$

Thus, D cannot be the square of an element in $\mathbb{Q}$. Since $p(x)$ is separable, this observation implies that G is not contained in A_3. Therefore, G is isomorphic to S_3. $\square$

Problem 62. *Suppose that F is a finite Galois extension of the field K. If* $\mathrm{Gal}(F/K)$ *has order pq, where $p < q$ are distinct primes, and p does not divide $q-1$, prove that F has two subfields F_p and F_q, which are stable under the action of* $\mathrm{Gal}(F/K)$*, such that:*

(a): $F_p \cap F_q = K$.

(b): F_p *and* F_q *generate* F.

(c): $\mathrm{Gal}(F_p/K)$ *is cyclic of order p and* $\mathrm{Gal}(F_q/K)$ *is cyclic of order q.*

Proof. Let $G = \mathrm{Gal}(F/K)$. Let $H_p \in \mathrm{Syl}_p(G)$ and $H_q \in \mathrm{Syl}_q(G)$. Now, we know that $n_q(G)$ is congruent to 1 modulo q and $n_q(G)$ divides p. Since $n_q(G)$ divides the prime p, we have $n_q(G) \in \{1, p\}$. But $n_q(G)$ is congruent to 1 modulo q and since $p < q$, it cannot be the case that $n_q(G) = p$. Therefore, $n_q(G) = 1$.

We also know that $n_p(G)$ is congruent to 1 modulo p and $n_p(G)$ divides q. Since $n_p(G)$ divides the prime q, we have $n_p(G) \in \{1, q\}$. Suppose that $n_p(G) = q$. Then by the above, we have that q is congruent to 1 modulo p. In particular, this implies that $q-1$ is congruent to 0 modulo p so that p divides $q-1$. However, we have by hypothesis that p does not divide $q-1$. Therefore, $n_q(G) = 1$.

Now, since $|G| = pq$, we have that $|H_p| = p$ and $|H_q| = q$. Note that since $|H_p| = p$ and p is prime, we have that H_p contains $p-1$ elements of order p. Furthermore, these are the only elements of G of order p, as if there were another element of G of order p not among these $p-1$ elements, then this element would generate a Sylow p-subgroup of G distinct from H_p, contradicting the fact that H_p is the only Sylow p-subgroup of G. Similarly, since $|H_q| = q$ and q is prime, we have that H_q contains $q-1$ elements of order q. By the same reasoning as above, these are the only elements of G of order q.

Now, with the identity of G, we have accounted for

$$(p-1) + (q-1) + 1 = p + q - 1$$

elements of G. Since $p < q$, we have that $p - 1 < q$. Furthermore, since p is prime, we have that $p \geq 2$. Therefore, we have

$$p + q - 1 = (p-1) + q < q + q = 2q \leq pq = |G|$$

Thus, we may now conclude that there is some nonidentity element of G that is neither of order p nor q. But since $|G| = pq$, by Lagrange's Theorem, this element must have order pq. In other words, G is a cyclic group since $|G| = pq$.

Since G is cyclic, it follows that for each positive divisor of $|G|$ we have that G has exactly one subgroup of that order. Thus, since $|G| = pq$ and p and q are primes, it follows that the subgroups of G are exactly $\{1\}, H_p, H_q$, and G. Now, since F/K is a finite Galois extension, by the Fundamental Theorem of Galois Theory, there is a bijective correspondence between the subgroups of G and the intermediate fields of the extension F/K. Thus, the intermediate fields of the extension F/K are exactly K, F_p, F_q, and F, where $F_p \mapsto H_p$ and $F_q \mapsto H_q$ under this correspondence. We will now prove that F_p and F_q meet all of the requirements of this problem.

By the Fundamental Theorem of Galois Theory, we know that $H_p = \mathrm{Gal}(F/F_p)$ and $H_q = \mathrm{Gal}(F/F_q)$. Since G is cyclic, it follows that every subgroup of G is normal in G. Thus, we have $H_p \trianglelefteq G$ and $H_q \trianglelefteq G$. Therefore, F_p and F_q are stable under the action of G. Furthermore, by the Fundamental Theorem of Galois Theory, the normality of H_p and H_q in G give

$$\mathrm{Gal}(F_p/K) \simeq \frac{G}{H_p}$$

and

$$\mathrm{Gal}(F_q/K) \simeq \frac{G}{H_q}$$

Thus, since G is cyclic, it now follows that $\mathrm{Gal}(F_p/K)$ and $\mathrm{Gal}(F_q/K)$ are cyclic. Furthermore, we have by the above that

$$|\,\mathrm{Gal}(F_p/K)| = \frac{pq}{p} = q$$

and

$$|\,\mathrm{Gal}(F_q/K)| = \frac{pq}{q} = p$$

Now, note $F_p \cap F_q$ is a field since the intersection of fields is a field. Furthermore, $F_p \cap F_q$ is an intermediate field of the extension F/K since F_p and F_q are intermediate fields of F/K. By the above observations, we have that $F_p \cap F_q \in \{K, F_p, F_q, F\}$.

Note that this intersection is necessarily properly contained in F since both F_p and F_q are properly contained in F. In particular, we have that $F_p \cap F_q \neq F$. For the sake of contradiction, assume that $F_p \subseteq F_q$. By the Fundamental Theorem of Galois Theory, this would imply that $H_q \subseteq H_p$. However, this is not possible since H_q is a group of prime order q and H_p is a group of prime order p. Therefore, F_p cannot be contained in F_q. Similarly, F_q cannot be contained in F_p. Therefore, we have that $F_p \cap F_q \notin \{F_p, F_q\}$. Thus, we conclude that $F_p \cap F_q = K$.

Finally, since F_p and F_q are subfields of F, we have that F_p and F_q generate a subfield of F containing both F_p and F_q. By the above, the only subfields of F containing both F_p and F_q is F itself. Therefore, F_p and F_q generate F. This completes the proof. $\square$

Problem 63. *Prove than an automorphism of the real field is necessarily the identity.*

Proof. Clearly, the identity map $\mathbb{R} \to \mathbb{R}$ is an automorphism of $\mathbb{R}$. On the other hand, suppose that $\sigma : \mathbb{R} \to \mathbb{R}$ is an automorphism of $\mathbb{R}$. First, we show that σ maps positive real numbers to positive real numbers. Towards this end, let $a \in \mathbb{R}$ be such that $a > 0$. Then there is some nonzero $b \in \mathbb{R}$ such that $a = b^2$. In particular, since $b \neq 0$ and since σ is an automorphism of $\mathbb{R}$, we have that $\sigma(b) \neq 0$. Therefore, since σ is an automorphism and by this result, we obtain

$$\sigma(a) = \sigma(b^2) = [\sigma(b)]^2 > 0$$

This proves that σ maps positive real numbers to positive real numbers.

Now, we show that σ preserves the order structure on $\mathbb{R}$. Towards this end, let $a, b \in \mathbb{R}$ be such that $a < b$. Then $b - a > 0$ so that by the above result and since σ is an autmomorphism, we obtain

$$0 < \sigma(b - a) = \sigma(b) - \sigma(a)$$

This inequality implies that $\sigma(a) < \sigma(b)$. Since $a, b \in \mathbb{R}$ were arbitrary real numbers with $a < b$, the above shows that σ preserves the order structure on $\mathbb{R}$.

Now, we show that σ is the identity on $\mathbb{N}$. First note that since σ is an automorphism we have that $\sigma(0) = 0$. Now, let $n \in \mathbb{N}$ be nonzero. Since σ is an automorphism, we have that $\sigma(1) = 1$. Thus, we obtain

$$\sigma(n) = \sigma(\underbrace{1 + \cdots + 1}_{\text{n times}}) = \sum_{i=1}^{n} \sigma(1) = \sum_{i=1}^{n} 1 = n$$

This proves our claim.

Now, we show that σ is the identity on $\mathbb{Q}$. First, let $p \in \mathbb{Q}$ be positive. Then for some nonzero $a, b \in \mathbb{N}$ we can write

$$p = \frac{a}{b} = ab^{-1}$$

But since $a, b \in \mathbb{N}$ and since σ is an automorphism, we now have by the above that

$$\sigma(p) = \sigma(ab^{-1}) = \sigma(a)\sigma(b^{-1}) = \sigma(a)[\sigma(b)]^{-1} = a(b)^{-1} = ab^{-1} = p$$

This proves that σ is the identity on the positive rationals. Lastly, let $p \in \mathbb{Q}$ be negative. Then $-p$ is a positive rational number. By the above and since σ is an automorphism, we now have

$$\sigma(-p) = -\sigma(p) = -(p) = -p$$

Thus, since $\sigma(0) = 0$, we have shown that σ is the identity on $\mathbb{Q}$.

Finally, for the sake of contradiction, suppose that σ were not the identity map. Then there exists some $a \in \mathbb{R}$ such that $\sigma(a) \neq a$. Since we have $a \neq \sigma(a)$, it must be the case that either $a < \sigma(a)$ or $\sigma(a) < a$.

First, suppose that $a < \sigma(a)$. Since $\mathbb{Q}$ is dense in $\mathbb{R}$, there is some $p \in \mathbb{Q}$ such that $a < p < \sigma(a)$. Since $p \in \mathbb{Q}$, we have by the above that $\sigma(p) = p$. Hence, since $a < p$, we

have by the above that

$$\sigma(a) < \sigma(p) = p$$

However, this contradicts the fact that $\sigma(a) > p$.

Secondly, suppose that $\sigma(a) < a$. Since $\mathbb{Q}$ is dense in $\mathbb{R}$, there is some $p \in \mathbb{Q}$ such that $\sigma(a) < p < a$. Since $p \in \mathbb{Q}$, we have by the above that $\sigma(p) = p$. Hence, since $p < a$, we have by the above that

$$p = \sigma(p) < \sigma(a)$$

However, this contradicts the fact that $\sigma(a) < p$. Therefore, we conclude that $\sigma(a) = a$ for every $a \in \mathbb{R}$. That is, σ is the identity map on $\mathbb{R}$. Since σ was an arbitrary automorphism of $\mathbb{R}$, this shows that an automorphism of the real field is necessarily the identity. $\square$

Problem 64. *Let F be a finite field extension of K, and $G = \mathrm{Gal}(F/K)$. Denote $(\cdot)'$ the Galois correspondences $E \mapsto E'$ and $H \mapsto H'$, mapping intermediate subfields to subgroups of G and back.*

(a): *If E is an intermediate subfield which is invariant under all automorphisms in G, then show that E' is normal in G.*

(b): *If H is a normal subgroup of G, then prove that $\sigma(H') = H'$, for each $\sigma \in G$.*

Proof. (a): First, note that

$$E' = \mathrm{Gal}(F/E) = \{\sigma \in G : \sigma(e) = e \text{ for all } e \in E\}$$

Now, let $\tau \in G$. By hypothesis, we have that $\tau(E) = E$. Therefore, the above observations give

$$\begin{aligned}
\tau E' \tau^{-1} &= \{\tau\sigma\tau^{-1} : \sigma \in E'\} \\
&= \{\tau\sigma\tau^{-1} : \sigma \in G \text{ and } \sigma(e) = e \text{ for all } e \in E\} \\
&= \{\phi \in G : \tau^{-1}(\phi(\tau(e))) = e \text{ for all } e \in E\} \\
&= \{\phi \in G : \phi(\tau(e)) = \tau(e) \text{ for all } e \in E\} \\
&= \{\phi \in G : \phi \in \mathrm{Gal}(F/\tau(E))\} \\
&= \mathrm{Gal}(F/\tau(E)) \\
&= \mathrm{Gal}(F/E) \\
&= E'
\end{aligned}$$

Since $\tau \in G$ was arbitrary, the above shows that E' is normal in G. □

Proof. (b): First, note that since H is a subgroup of $G = \mathrm{Gal}(F/K)$ that there is some intermediate field E of F/K such that $H = \mathrm{Gal}(F/E)$. Therefore, by the Galois correspondence, we have that $H' = E$. By this observation, it follows that we must show that $\sigma(E) = E$ for all $\sigma \in G$. Towards this end, let $\sigma \in G$. Since $H \trianglelefteq G$, we obtain

$$\begin{aligned}
\mathrm{Gal}(F/\sigma(E)) &= \{\tau \in G : \tau(\sigma(e)) = \sigma(e) \text{ for all } e \in E\} \\
&= \{\tau \in G : \sigma^{-1}(\tau(\sigma(e))) = e \text{ for all } e \in E\} \\
&= \{\tau \in G : \sigma^{-1}\tau\sigma \in \mathrm{Gal}(F/E)\} \\
&= \{\tau \in G : \sigma^{-1}\tau\sigma \in H\} \\
&= \{\tau \in G : \tau \in \sigma H \sigma^{-1}\} \\
&= \sigma H \sigma^{-1} \\
&= H \\
&= \mathrm{Gal}(F/E)
\end{aligned}$$

Thus, we have $\mathrm{Gal}(F/\sigma(E)) = \mathrm{Gal}(F/E)$. This implies that $\sigma(E)$ and E both map to the same subgroup of G under the Galois correspondence. But since the Galois correspondence is always injective, this observation implies that $\sigma(E) = E$. This completes the proof. □

Problem 65. (a): *Define: splitting field of a polynomial.*

(b): *Assuming the existence and uniqueness of splitting fields, up to isomorphism over the base field, prove this:*

Let F be a finite extension of K. Then F is a splitting field for some polynomial if and only if every irreducible polynomial over K, having a root in F, factors completely over F.

Proof. (a): Let K be a field and let $f(x) \in K[x]$ be a nonzero polynomial. A ***splitting field*** for $f(x)$ over K is a field F such that F is an extension of K and $f(x)$ splits into linear factors over F

$$f(x) = a\prod_{i=1}^{n}(x - u_i)$$

where $a \in K^\times, u_1, \ldots, u_n \in F$, and $F = K(u_1, \ldots, u_n)$. □

Proof. (b): Let F be a finite extension of K. For the first direction, assume that F is a splitting field for some polynomial $f(x) \in K[x]$. Suppose that $p(x) \in K[x]$ is irreducible and that $p(x)$ has a root in F. Let $u_1, \ldots, u_n$ denote the roots of $f(x)$ and write

$$f(x) = a\prod_{i=1}^{n}(x - u_i)$$

for some $a \in K^\times$. We also have by definition that $F = K(u_1, \ldots, u_n)$.

Now, let $\overline{K}$ be an algebraic closure of K with $\overline{K} \supseteq F$ and suppose that $\sigma : F \to \overline{K}$ is an injective K-homomorphism. We will show that $\sigma(F) = F$. Towards this end, note that as $f(x) \in K[x]$ and as σ is a K-homomorphism we have that $\sigma(f(x)) = f(x)$, where $\sigma(f(x))$ is interpreted as the polynomial obtained by applying σ to each of the coefficients of $f(x)$. By the above representation of $f(x)$ and since σ is injective, it follows that σ permutes $u_1, \ldots, u_n$. Therefore, since σ fixes K, we have

$$\sigma(F) = \sigma(K(u_1, \ldots, u_n)) = K(u_1, \ldots, u_n) = F$$

The above shows that F/K is a normal extension. Therefore, since $p(x) \in K[x]$ is irreducible and has a root in F, it follows that $p(x)$ factors completely over F.

For the second direction, assume that every irreducible polynomial over K, having a root in F, factors completely over F. Since F is a finite extension of K, we can write $F = K(u_1, \ldots, u_n)$ for some $u_1, \ldots, u_n \in F$. For each $i \in \{1, \ldots, n\}$, let $m_{K,u_i}(x) \in K[x]$ denote the minimum polynomial for u_i over K. In particular, since for each $i \in \{1, \ldots, n\}$ we have $m_{K,u_i}(x)$ is irreducible over K with a root $u_i \in F$, it follows by hypothesis that $m_{K,u_i}(x)$ factors completely over F. Define

$$f(x) = \prod_{i=1}^{n} m_{K,u_i}(x) \in K[x]$$

We claim that F is a splitting field for $f(x)$ over K. Towards this end, let E be a splitting field for $f(x)$ over K. Then E is equal to K extended by the roots of $f(x)$, and

among these roots are $u_1, \ldots, u_n$. Since $F = K(u_1, \ldots, u_n)$, we obtain the inclusion

$$K \subseteq F \subseteq E$$

Finally, note that since $m_{K,u_i}(x)$ factors completely over F for each $i \in \{1, \ldots, n\}$, it follows by the definition of $f(x)$ that $f(x)$ factors completely over F. By the above inclusion and since E is a splitting field for $f(x)$ over K, it follows that $F = E$ so that F is a splitting field for $f(x)$ over K. This completes the proof. $\square$

Problem 66. *Use the notions of formal derivatives to show that, if $f(x)$ is an irreducible polynomial over the field K then it has repeated roots in the splitting field if and only if the characteristic of K is $p > 0$, and $f(x) = g(x^p)$ for some $g(x) \in K[x]$.*

Proof. Let $f(x) \in K[x]$ be an irreducible polynomial and let F be a splitting field for $f(x)$ over K. For the first direction, suppose that $f(x)$ has repeated roots in F. For the sake of contradiction, assume that $\text{char}(K) = 0$. Then since $f(x)$ is irreducible, it follows that $f(x)$ is separable. Therefore, the roots of $f(x)$ in F are distinct, which contradicts the fact that $f(x)$ has repeated roots in F. Thus, it must be the case that $\text{char}(K) = p > 0$ for some prime number p.

Now, since $f(x)$ has repeated roots in F, we have that $f(x)$ is not separable. Thus, if $f'(x)$ denotes the derivative of $f(x)$, then $f'(x) = 0$ since $f(x)$ is irreducible. Since $f(x) \in K[x]$, we can write

$$f(x) = \sum_{i=0}^{n} a_i x^i$$

where $a_0, \ldots, a_n \in K$. Since $f'(x) = 0$, we now have

$$0 = f'(x) = \sum_{i=1}^{n} i a_i x^{i-1}$$

Thus, we obtain $ia_i = 0$ for each $i \in \{1, \ldots, n\}$. Now, let

$$J = \{j \in \{1, \ldots, n\} : a_j \neq 0\}$$

Then we have

$$0 = f'(x) = \sum_{j \in J} j a_j x^{j-1}$$

Now, since $\text{char}(K) = p$, by the above equality, and since $a_j \neq 0$ for each $j \in J$, we have that p divides j for each $j \in J$. Therefore, for each $j \in J$, there exists a positive integer z_j such that $j = pz_j$. Thus, we obtain

$$f(x) = \sum_{i=0}^{n} a_i x^i = a_0 + \sum_{i=1}^{n} a_i x^i = a_0 + \sum_{j \in J} a_j x^j = a_0 + \sum_{j \in J} a_j x^{pz_j} = a_0 + \sum_{j \in J} a_j (x^p)^{z_j}$$

The above shows that $f(x) = g(x^p)$, where

$$g(x) = \sum_{j \in J} a_j x^{z_j} \in K[x]$$

This completes the proof of the first direction.

For the second direction, assume that $\text{char}(K) = p > 0$ and $f(x) = g(x^p)$ for some $g(x) \in K[x]$. Let

$$g(x) = \sum_{i=0}^{n} a_i x^i$$

where $a_0, \ldots, a_n \in K$. Thus, we obtain

$$f(x) = g(x^p) = \sum_{i=0}^{n} a_i (x^p)^i = \sum_{i=0}^{n} a_i x^{pi}$$

Since $\mathrm{char}(K) = p$, we have

$$f'(x) = \sum_{i=1}^{n} pia_i x^{pi-1} = \sum_{i=1}^{n} 0x^{pi-1} = 0$$

Thus, $f'(x) = 0$. Since $f(x)$ is irreducible, it now follows that $f(x)$ is not separable so that $f(x)$ has a repeated root in F. This completes the proof. $\square$

Problem 67. *Let p be a prime number.*

(a): *Prove that if a subgroup H of S_p, the symmetric group on p letters, contains a p-cycle and a transposition, then $H = S_p$.*

(b): *If $p(x)$ is an irreducible polynomial over $\mathbb{Q}$, of degree p, having exactly two non-real roots, then show that the Galois group of the splitting field of $p(x)$ is S_p.*

Proof. (a): Let $\sigma \in H$ be a p-cycle and let $\tau \in H$ be a transposition. Write

$$\sigma = (a_1 \quad a_2 \quad \cdots \quad a_p)$$

and

$$\tau = (b \quad c)$$

Now, we have that $b \in \{a_1, \ldots, a_p\}$. We may renumber the $a_1, \ldots, a_p$ so that $b = a_1$. Since $b \neq c$ and since $b = a_1$, we have that $c \in \{a_2, \ldots, a_p\}$ so that $c = a_i$ for some $i \in \{2, \ldots, p\}$. Notice that

$$\sigma^{i-1} = (a_1 \quad c \quad \cdots \quad)$$

and that σ^{i-1} is a p-cycle. Therefore, we may assume without loss that $\tau = (a_1 \quad a_2)$.

Now, notice that

$$\tau\sigma = (a_1 \quad a_2)(a_1 \quad a_2 \quad \cdots \quad a_p) = (a_2 \quad a_3 \quad \cdots \quad a_p) \in H$$

Thus, we have

$$(\tau\sigma)(a_1 \quad a_2)(\tau\sigma)^{-1} = (a_2 \quad a_3 \quad \cdots \quad a_p)(a_1 \quad a_2)(a_2 \quad a_3 \quad \cdots \quad a_p)^{-1} = (a_1 \quad a_3) \in H$$

Similarly, we have

$$(\tau\sigma)(a_1 \quad a_3)(\tau\sigma)^{-1} = (a_2 \quad a_3 \quad \cdots \quad a_p)(a_1 \quad a_3)(a_2 \quad a_3 \quad \cdots \quad a_p)^{-1} = (a_1 \quad a_4) \in H$$

Continuing this process, we obtain that $(a_1 \quad a_i) \in H$ for all $i \in \{2, \ldots, p\}$.

Now, notice that

$$\sigma(a_1 \quad a_2)\sigma^{-1} = (a_1 \quad a_2 \quad \cdots \quad a_p)(a_1 \quad a_2)(a_1 \quad a_2 \quad \cdots \quad a_p)^{-1} = (a_2 \quad a_3) \in H$$

Similarly, we have

$$\sigma(a_2 \quad a_3)\sigma^{-1} = (a_1 \quad a_2 \quad \cdots \quad a_p)(a_2 \quad a_3)(a_1 \quad a_2 \quad \cdots \quad a_p)^{-1} = (a_3 \quad a_4) \in H$$

Continuing this process, we obtain that

$$(a_1 \quad a_2), (a_2, \quad a_3), \ldots, (a_{p-1} \quad a_p) \in H$$

Finally, by repeating this process for each transposition $(a_1 \quad a_i)$ for each $i \in \{2, \ldots, p\}$, we obtain that H contains all transpositions of S_p. Since the transpositions of S_p generate S_p and since H contains all transpositions of S_p, it now follows that $H = S_p$. $\square$

Proof. (b): Let $p(x) \in \mathbb{Q}[x]$ be irreducible of degree p with exactly two non-real roots u_1 and u_2, let F be a splitting field for $p(x)$ over K, and let G be the Galois group of the splitting field of $p(x)$.

Since $\text{char}(\mathbb{Q}) = 0$ and since $p(x)$ is irreducible over $\mathbb{Q}$, it follows that $p(x)$ is separable. Therefore, since $p(x)$ is irreducible over $\mathbb{Q}$ and is separable, it follows that $p = \deg(p(x))$ divides $|G|$. Since p is a prime number dividing $|G|$, it follows by Cauchy's

Theorem that G contains an element of order p. But since G is isomorphic to a subgroup of S_p, it now follows that G contains a p-cycle.

Now, since F is a splitting field for $p(x)$ over $\mathbb{Q}$, we have that $F \subseteq \mathbb{C}$. Consider the map $\tau : F \to F$ given by complex conjugation. Since $F \subseteq \mathbb{C}$, it follows that τ is indeed a map. Furthermore, we know that since τ is complex conjugation that $\tau \in \mathrm{Gal}(F/\mathbb{Q}) = G$.

Next, note that since non-real roots of polynomials over $\mathbb{Q}$ are complex conjugates of one another that we have $\tau(u_1) = u_2$. Also, since $p(x)$ has no other non-real roots, it follows that $\tau(u) = u$ for every root u of $p(x)$ with $u \neq u_1$ and $u \neq u_2$ since τ is complex conjugation and hence fixes $\mathbb{R}$. Therefore, we conclude that $(u_1 \quad u_2) \in G$.

We have shown that G contains a p-cycle and the transposition $(u_1 \quad u_2)$. By the first part of this problem, then, we conclude that $G = S_p$. $\square$

Problem 68. *Prove that any finite subgroup of the multiplicative group of nonzero elements of a field is cyclic.*

Proof. Let F be a field and suppose that G is a finite subgroup of the multiplicative group of nonzero elements of F. If G is the trivial group, then G is clearly cyclic.

Otherwise, let $p_1, \ldots, p_n$ be a complete list of the distinct primes dividing $|G|$ and for each $i \in \{1, \ldots, n\}$, let $P_i \in \mathrm{Syl}_{p_i}(G)$. Since G is a subset of a field, it follows that G is abelian. Therefore, G is nilpotent so that G is the internal direct product of its distinct Sylow subgroups. That is,

$$G = \bigoplus_{i=1}^{n} P_i$$

Now, for the sake of contradiction, assume that G were not cyclic. By the above, this implies that there exist some $m \in \{1, \ldots, n\}$ such that P_m is not cyclic. By Lagrange's Theorem, then, it follows that every element of P_m has order dividing $|P_m|/p_m$. Therefore, every element of G has order dividing $|G|/p_m$. More specifically, since G is a subgroup of the multiplicative group of nonzero elements of F, this implies that $g^{|G|/p_m} = 1$ for every $g \in G$.

Consider the polynomial

$$f(x) = x^{|G|/p_m} - 1 \in F[x]$$

Since F is a field, it follows that $f(x)$ has at most $\deg(f(x)) = |G|/p_m$ roots in F. However, by the above observation, we know that every element of $G \subseteq F$ is a root of $f(x)$. Therefore, $f(x)$ has at least $|G| > |G|/p_m$ roots in F. This contradicts the fact that $f(x)$ has at most $|G|/p_m$ roots in F. Therefore, we conclude that G is a cyclic group. $\square$

Problem 69. *Prove that for each prime number p and positive integer n there is (up to isomorphism) one field of order p^n. Your proof should include an argument which shows that the order of a finite field is necessarily the power of a prime number.*

Proof. We first show that the order of a finite field is necessarily the power of a prime number. Towards this end, let K be a finite field and let $1_K \in K$ denote the multiplicative identity of K. Let $\text{char}(K) = p$. Then p is a prime number since the characteristic of any finite field is equal to a prime number.

Now, define a map

$$\phi : \mathbb{Z} \to K$$

by $\phi(n) = n \cdot 1_K$ for all $n \in \mathbb{Z}$. Clearly, ϕ is a well-defined mapping of $\mathbb{Z}$ into K. We will show that ϕ is a field homomorphism. Towards this end, let $n, m \in \mathbb{Z}$. Then we have

$$\phi(n+m) = (n+m) \cdot 1_K = n \cdot 1_K + m \cdot 1_K = \phi(n) + \phi(m)$$

and

$$\phi(nm) = (nm) \cdot 1_K = (n \cdot 1_K)(m \cdot 1_K) = \phi(n)\phi(m)$$

Finally, note that

$$\phi(1) = 1 \cdot 1_K = 1_K$$

Thus, ϕ is a field homomorphism, as claimed. Finally, since $\text{char}(K) = p$, we have

$$\begin{aligned} \ker \phi &= \{n \in \mathbb{Z} : \phi(n) = 0\} \\ &= \{n \in \mathbb{Z} : n \cdot 1_K = 0\} \\ &= \{n \in \mathbb{Z} : p \text{ divides } n\} \\ &= \{n \in \mathbb{Z} : n \in p\mathbb{Z}\} \\ &= p\mathbb{Z} \end{aligned}$$

Thus, by the First Isomorphism Theorem for Rings, we have that $\mathbb{Z}/p\mathbb{Z}$ is isomorphic to a subfield S of K.

Now, let P denote the prime subfield of K. Then P is a subfield of K containing no proper subfields. In particular, notice that P must contain all elements of the form $n \cdot 1_K$ for all $n \in \mathbb{Z}$. This implies that $S \subseteq P$. But since S is a field and P contains no proper subfields, this implies that $P = S$ so that the prime subfield of K is isomorphic to $\mathbb{Z}/p\mathbb{Z}$.

Finally, note that since P is a subfield of K that K is a finite dimensional vector space over P. So, we may write

$$[K : P] = n < \infty$$

Therefore, we obtain

$$|K| = |P|^{[K:P]} = |P|^n = |\mathbb{Z}/p\mathbb{Z}|^n = (p)^n = p^n$$

This shows that $|K| = p^n$ for some prime number p and positive integer n.

We now prove that any two finite fields of the same cardinality are isomorphic by proving an additional result about the field K above. To begin, let $p(x) = x^{p^n} - x \in K[x]$.

We claim that K is a splitting field for $p(x)$ over P. Indeed, note that since $|K| = p^n$ we have $|K^\times| = p^n - 1$. Hence, since $K^\times$ is a group, this implies that $a^{p^n-1} = 1$ for every $a \in K^\times$. Therefore, we see that $a^{p^n} = a$ for every $a \in K$. That is, every element of K is a root of $p(x)$. But since $p(x)$ can have at most p^n roots and $|K| = p^n$, this shows that K is precisely equal to the set of roots of $p(x)$. It now follows that K is a splitting field for $p(x)$ over P.

Now, suppose that F_1 and F_2 are finite fields such that $|F_1| = |F_2|$. Let P_1 and P_2 denote the prime subfields of F_1 and F_2, respectively. Since $|F_1| = |F_2|$ and F_1 and F_2 are finite, it follows that $\mathrm{char}(F_1) = \mathrm{char}(F_2)$. Hence, by the above, it follows that P_1 and P_2 are isomorphic. To complete the proof, suppose that $|F_1| = n = |F_2|$. Then by the above, we know that F_1 is a splitting field for the polynomial $x^n - x$ over P_1 and F_2 is a splitting field for the polynomial $x^n - x$ over P_2. By the uniqueness of splitting fields, then, we obtain that F_1 and F_2 are isomorphic.

Finally, let p be a prime and let n be a positive integer. We will show that there exists a field F of order p^n. Once this is established, by the above results, we will have proven that the desired result. To begin, let $K = \mathbb{Z}/p\mathbb{Z}$. Since p is a prime number, it follows that K is a field. Let $p(x) = x^{p^n} - x \in K[x]$ and let F be a splitting field for $p(x)$ over K. Note that, clearly, $\mathrm{char}(F) = \mathrm{char}(K) = p$.

Now, if $p'(x)$ denotes the derivative of $p(x)$, then we have by the above that

$$p'(x) = p^n x^{p^n-1} - 1 = 0 - 1 = -1$$

Hence, it follows that $p(x)$ and $p'(x)$ are relatively prime which implies that $p(x)$ is a separable polynomial. In particular, if Γ denotes the set of roots of $p(x)$, then

$$|\Gamma| = \deg(p(x)) = p^n$$

Furthermore, since F is a splitting field for $p(x)$ over K, we clearly have that $\Gamma \subseteq F$.

We will prove that Γ is a field. Towards this end, let $a, b \in \Gamma$. By the definition of membership in Γ, we have

$$0 = p(a) = a^{p^n} - a$$

and

$$0 = p(b) = b^{p^n} - b$$

so that $a^{p^n} = a$ and $b^{p^n} = b$. Now, note that since $\mathrm{char}(F) = p$, we have

$$(a-b)^{p^n} = a^{p^n} - b^{p^n} = a - b$$

so that $p(a-b) = 0$ so that $a - b \in \Gamma$. Next, we see

$$(ab)^{p^n} = a^{p^n} b^{p^n} = ab$$

so that $p(ab) = 0$ so that $ab \in \Gamma$. Finally, if $b \neq 0$, we have

$$\left(\frac{a}{b}\right)^{p^n} = \frac{a^{p^n}}{b^{p^n}} = \frac{a}{b}$$

so that $p(a/b) = 0$ so that $a/b \in \Gamma$. The above results show that Γ is a field. In particular, note that Γ is a field and that $p(x)$ splits over Γ.

Finally, let $a \in K$. Since $|K| = p$, it follows by the above that $a^p = a$. Therefore,

$$a^{p^2} = (a^p)^p = (a)^p = a^p = a$$

Continuing this process, we obtain $a^{p^n} = a$ so that $a \in \Gamma$. Since $a \in K$ was arbitrary and by the above, we now obtain the inclusion

$$K \subseteq \Gamma \subseteq F$$

But since F is a splitting field for $p(x)$ over K and $p(x)$ splits over Γ, the above inclusion implies that $F = \Gamma$ so that

$$|F| = |\Gamma| = p^n$$

This completes the proof. $\square$

Problem 70. *Consider the polynomial over the field $\mathbb{F}_2$ of two elements: $g(x) = x^4 + x^3 + x^2 + x + 1$.*

(a): *Prove that $g(x)$ is irreducible over $\mathbb{F}_2$.*

(b): *Let F be a splitting field for $g(x)$ over $\mathbb{F}_2$, and let $u \in F$ be a root of $g(x)$. Factor $g(x)$ into irreducibles over $\mathbb{F}_2(u)$.*

(c): *Show that $F = \mathbb{F}_2(u)$.*

(d): *Find the Galois group $\mathrm{Gal}(F/\mathbb{F}_2)$.*

Proof. (a): First, note that $g(0) = 1 \neq 0$ and $g(1) = 1 \neq 0$. Therefore, $g(x)$ has no roots in $\mathbb{F}_2$ and hence has no linear factors over $\mathbb{F}_2$. Now, for the sake of contradiction, assume that $g(x)$ can be factored as the product of two quadratics in $\mathbb{F}_2[x]$. Then we can write

$$g(x) = (x^2 + ax + b)(x^2 + cx + d) = x^4 + (a + c)x^3 + (b + d + ac)x^2 + (ad + bc)x + bd$$

where $a, b, c, d \in \mathbb{F}_2$. It follows immediately that $b = d = 1$. Thus, the condition $b + d + ac = 1$ now implies that $ac = 1$ so that $a = c = 1$. However, this would give that $a + c = 0$, which contradicts the condition that $a + c = 1$. We conclude that $g(x)$ cannot be factored into two quadratics over $\mathbb{F}_2$. Since $\deg(g(x)) = 4$, the above results prove that $g(x)$ is irreducible over $\mathbb{F}_2$. $\square$

Proof. (b): Since u is a root of $g(x)$, we have the equality

$$0 = g(u) = u^4 + u^3 + u^2 + u + 1$$

Now, consider the polynomial $f(x) \in \mathbb{F}_2(u)[x]$ given by

$$f(x) = (x - u)(x - u^2)(x - u^3)(x - u^4) = x^4 + ax^3 + bx^2 + cx + d$$

where $a, b, c, d \in \mathbb{F}_2$. We claim that $f(x) = g(x)$.

First, we have

$$a = -\sum_{i=1}^{4} u^i = -(u + u^2 + u^3 + u^4)$$

But note that by the above equality we have

$$u + u^2 + u^3 + u^4 = -1 = 1$$

Therefore, we have that $a = -(1) = -1 = 1$.

Secondly, we have

$$b = \sum_{1 \leq i < j \leq 4} u^i u^j = u^3 + u^4 + u^5 + u^5 + u^6 + u^7$$

But note that by the above equality we have

$$u^3 + u^4 + u^5 + u^6 + u^7 = 0$$

and that

$$u^5 = -(u + u^2 + u^3 + u^4) = -(1) = -1 = 1$$

Therefore, we have that $b = 0 + 1 = 1$.

Thirdly, we have

$$c = -\sum_{1 \leq i < j < k \leq 4} u^i u^j u^k = -(u^6 + u^7 + u^8 + u^9)$$

But note that by the above equality we have

$$u^5 + u^6 + u^7 + u^8 + u^9 = 0$$

so that, by the above computation of u^5, we have

$$u^6 + u^7 + u^8 + u^9 = -u^5 = -(1) = -1 = 1$$

Therefore, we have that $c = -(1) = -1 = 1$.

Fourthly, note that by the above computation of u^5, we have

$$d = u^{10} = (u^5)^2 = (1)^2 = 1$$

Therefore, we have shown that $a = b = c = d = 1$. In turn, this implies that $f(x) = g(x)$. Thus, we obtain that

$$g(x) = f(x) = (x - u)(x - u^2)(x - u^3)(x - u^4)$$

which is clearly the factorization of $g(x)$ into irreducibles over $\mathbb{F}_2(u)$. □

Proof. (c): By definition, we know that F is equal to $\mathbb{F}_2$ extended by the roots of $g(x)$. Since u is a root of $g(x)$, we obtain the inclusion

$$\mathbb{F}_2 \subseteq \mathbb{F}_2(u) \subseteq F$$

But by the above, we see that $f(x)$ splits over $\mathbb{F}_2(u)$. Therefore, by the above inclusion, we obtain $F = \mathbb{F}_2(u)$. □

Proof. (d): Let $g'(x)$ denote the derivative of $g(x)$. Then we have

$$g'(x) = 4x^3 + 3x^2 + 2x + 1 = x^2 + 1 \neq 0$$

Therefore, since $g(x)$ is an irreducible polynomial in $\mathbb{F}_2[x]$ and $g'(x) \neq 0$, it follows that $g(x)$ is separable. Thus, we now have that F is a splitting field of a separable polynomial in $\mathbb{F}_2[x]$ so that $F/\mathbb{F}_2$ is a finite Galois extension. In particular, this gives

$$|\operatorname{Gal}(F/\mathbb{F}_2)| = [F : \mathbb{F}_2]$$

Now, by the above, $g(x)$ is a monic, irreducible polynomial over $\mathbb{F}_2$ that has u as a root so that $g(x)$ is the minimum polynomial for u over $\mathbb{F}_2$. Therefore, we obtain

$$|\operatorname{Gal}(F/\mathbb{F}_2)| = [F : \mathbb{F}_2] = [\mathbb{F}_2(u) : \mathbb{F}_2] = \deg(g(x)) = 4$$

Finally, notice that since $[F : \mathbb{F}_2] = 4$ that

$$|F| = |\mathbb{F}_2|^4 = 2^4$$

So, we may assume that $F = \mathbb{F}_{2^4}$. Furthermore, we know that $\operatorname{Gal}(\mathbb{F}_{2^4}/\mathbb{F}_2)$ is cyclic. Therefore, combining the above results, we have that $\operatorname{Gal}(F/\mathbb{F}_2)$ is cyclic of order 4. We conclude that $\operatorname{Gal}(F/\mathbb{F}_2)$ is isomorphic to $\mathbb{Z}_4$. □

Problem 71. *Let F/K be a cyclic extension of fields with finite Galois group $\langle\sigma\rangle$.*

(a): *State the Hilbert Theorem 90 in multiplicative form.*

(b): *Suppose $[F:K]=n$ is relatively prime to the characteristic of K, and K contains a primitive nth root of unity. Prove that there exists $\alpha\in K$ such that $F=K(\alpha)$ and $m_{K,\alpha}(x)$ (i.e., the irreducible polynomial of α over K) is x^n-a for some $a\in K$.*

Proof. (a): ***Hilbert's Theorem 90***: Let F/K be a cyclic extension of fields and let $\sigma\in\mathrm{Gal}(F/K)$ be a generator for $\mathrm{Gal}(F/K)$. Suppose that $[F:K]=n$ for some positive integer n so that

$$\mathrm{Gal}(F/K)=\langle\sigma\rangle=\{1,\sigma,\ldots,\sigma^{n-1}\}$$

Let $N_K^F:F\to K$ be the norm map defined by

$$N_K^F(u)=\prod_{i=0}^{n-1}\sigma^i(u)$$

for all $u\in F$. Let $u\in F$. Then $N_K^F(u)=1$ if and only if there exists an element $v\in F^\times$ such that $u=v[\sigma(v)]^{-1}$. □

Proof. (b): Since F/K is a cyclic extension, we have that F/K is a finite Galois extension. Therefore, we have

$$|\mathrm{Gal}(F/K)|=[F:K]=n$$

Since $\mathrm{Gal}(F/K)=\langle\sigma\rangle$, the above gives that $\mathrm{Gal}(F/K)=\{1,\sigma,\ldots,\sigma^{n-1}\}$.

Now, let $\zeta\in K$ be a primitive nth root of unity. Since $\zeta\in K$, we have that $\tau(\zeta)=\zeta$ for all $\tau\in\mathrm{Gal}(F/K)$. Therefore, by the above, we have

$$N_K^F(\zeta)=\prod_{i=0}^{n-1}\sigma^i(\zeta)=\prod_{i=0}^{n-1}\zeta=\zeta^n=1$$

Thus, by Hilbert's Theorem 90, there exists some $w\in F^\times$ such that $\zeta=w[\sigma(w)]^{-1}$. That is, since σ is an automorphism, we have $w^{-1}\zeta=\sigma(w^{-1})$. Therefore, if $\alpha=w^{-1}\in F^\times$, we have the equality $\sigma(\alpha)=\alpha\zeta$.

We claim that $\alpha^n\in K$. To prove this claim, we first show that α^n is fixed by every element of $\mathrm{Gal}(F/K)$. Towards this end, first note that clearly $1(\alpha^n)=\alpha^n$. Next, as σ is an automorphism and by the above, we have

$$\sigma(\alpha^n)=[\sigma(\alpha)]^n=(\alpha\zeta)^n=\alpha^n\zeta^n=\alpha^n\cdot 1=\alpha^n$$

By the same reasoning and by this equality, we also have

$$\sigma^2(\alpha^n)=\sigma(\sigma(\alpha^n))=\sigma(\alpha^n)=\alpha^n$$

Repeating this argument, we obtain that $\sigma^i(\alpha^n)=\alpha^n$ for all $i\in\{0,\ldots,n-1\}$. Therefore, α^n is fixed by every element of $\mathrm{Gal}(F/K)$, as claimed. Since F/K is a finite Galois extension, then, this result shows that $\alpha^n\in K$.

Now, define $a=\alpha^n$ and $p(x)=x^n-a$. Then $p(x)\in K[x]$ since $a\in K$. Furthermore, we have that

$$p(\alpha)=\alpha^n-a=\alpha^n-\alpha^n=0$$

so that α is a root of $p(x)$. In particular, this observation gives that $\alpha, \alpha\zeta, \alpha\zeta^2, \ldots, \alpha\zeta^{n-1}$ are the distinct roots of $p(x)$.

We will now show that $p(x)$ is the minimum polynomial of α over K. Towards this end, first note that $1(\alpha) = \alpha$. Next, we have $\sigma(\alpha) = \alpha\zeta$. Next, since σ is an automorphism and as $\zeta \in K$, we have

$$\sigma^2(\alpha) = \sigma(\sigma(\alpha)) = \sigma(\alpha\zeta) = \sigma(\alpha)\sigma(\zeta) = \alpha\zeta \cdot \zeta = \alpha\zeta^2$$

Repeating this argument, we obtain that $\sigma^i(\alpha) = \alpha\zeta^i$ for each $i \in \{0, \ldots, n-1\}$.

Now, fix $m \in \{0, \ldots, n-1\}$. By the above, we see that $\sigma^m : K(\alpha) \to K(\alpha\zeta^m)$ is a K-homomorphism which is an isomorphism such that $\sigma^m(\alpha) = \alpha\zeta^m$. Therefore, α and $\alpha\zeta^m$ share the same minimum polynomial over K. But since $m \in \{0, \ldots, n-1\}$ was arbitrary, it follows that the distinct elements $\alpha, \alpha\zeta, \alpha\zeta^2, \ldots, \alpha\zeta^{n-1}$ all share the same minimum polynomial over K.

Now, let $m_{K,\alpha}(x) \in K[x]$ denote the minimum polynomial of α over K. By the above, we have that $\alpha, \alpha\zeta^2, \ldots, \alpha\zeta^{n-1}$ are distinct roots of $m_{K,\alpha}(x)$. Therefore, we have that $\deg(m_{K,\alpha}(x)) \geq n$. On the other hand, we have that

$$n = [F : K] = [F : K(\alpha)][K(\alpha) : K]$$

In particular, this equality implies that $[K(\alpha) : K] \leq n$. Therefore, we have by the above and by this observation that

$$n \geq [K(\alpha) : K] = \deg(m_{K,\alpha}(x)) \geq n$$

Hence, we obtain $[K(\alpha) : K] = n$ which implies that $\deg(m_{K,\alpha}(x)) = n$. But recall that $p(x) \in K[x]$ is a monic polynomial of degree n with roots $\alpha, \alpha\zeta, \alpha\zeta^2, \ldots, \alpha\zeta^{n-1}$. Combining the above results, then, it follows that $p(x)$ is the minimum polynomial of α over K. Finally, since $p(x)$ is the minimum polynomial of α over K, we have that

$$m_{K,\alpha}(x) = p(x) = x^n - a$$

Furthermore, note that

$$n = [F : K] = [F : K(\alpha)][K(\alpha) : K] = [F : K(\alpha)] \cdot n$$

Therefore, we have $[F : K(\alpha)] = 1$ so that $F = K(\alpha)$. This completes the proof. $\square$

Problem 72. (a): *Define* algebraic closure.

(b): *Prove that every field has an algebraic closure, and argue that if $\overline{K}$ is an algebraic closure of K, then $\overline{K}$ is countable, if K is finite, while $|\overline{K}| = |K|$ otherwise.*

Proof. (a): Let F be a field. We say that F is ***algebraically closed*** if every nonconstant polynomial $f(x) \in F[x]$ has a root in F.

Let K be a field. We say that a field extension $\overline{K}$ of K is an ***algebraic closure*** of K if $\overline{K}$ is algebraically closed and if $\overline{K}/K$ is an algebraic extension. □

Proof. (b): Let S be a set such that $K \subseteq S$ with $|S| > \aleph_0|K|$. Define

$$\mathcal{R} = \{L \subseteq S : L \text{ is an algebraic extension of } K\}$$

Then $\mathcal{R}$ is partially ordered by for $L_1, L_2 \in \mathcal{R}$ we have $L_2 \geq L_1$ if and only if $L_2 \supseteq L_1$. Note that since $K \subseteq S$ and K is an algebraic extension of K we have $K \in \mathcal{R}$ so that $\mathcal{R} \neq \emptyset$. Now, let $\mathcal{C}$ be a chain in $\mathcal{R}$. If $\mathcal{C} = \emptyset$, then $K \in \mathcal{R}$ is an upper bound for $\mathcal{C}$. If $\mathcal{C} \neq \emptyset$, define

$$J = \bigcup_{L \in \mathcal{C}} L$$

Since $\mathcal{C}$ is a chain, it follows that J is a field. By definition, $L \subseteq S$ for each $L \in \mathcal{C}$. Therefore, we have $J \subseteq S$. Furthermore, since each $L \in \mathcal{C}$ is algebraic over K, it follows that J is also algebraic over K. Thus, we see that $J \in \mathcal{R}$ and that J is clearly an upper bound for $\mathcal{C}$. The above results show that we may use Zorn's Lemma to assert that there is some maximal element $\overline{K} \in \mathcal{R}$.

We claim that $\overline{K}$ is an algebraic closure of K. It is immediate by the definition of $\mathcal{R}$ and since $\overline{K} \in \mathcal{R}$ that $\overline{K}/K$ is an algebraic extension. So, it remains to prove that $\overline{K}$ is algebraically closed.

For the sake of contradiction, suppose that $\overline{K}$ were not algebraically closed. Then there is some nonconstant polynomial $f(x) \in \overline{K}[x]$ such that $f(x)$ has no root in $\overline{K}$. It now follows that there is some algebraic extension $F = \overline{K}(u)$ of $\overline{K}$, where u is a root of $f(x)$ with $u \notin \overline{K}$. Since $F/\overline{K}$ is an algebraic extension and $\overline{K}/K$ is an algebraic extension, it follows that F/K is an algebraic extension. Therefore, we obtain the inequality

$$|F - \overline{K}| \leq |F| \leq \aleph_0|K| < |S|$$

Thus, we also have

$$|\overline{K}| \leq |F| < |S|$$

Furthermore, note that

$$|S| = |(S - \overline{K}) \cup \overline{K}| = |S - \overline{K}| + |\overline{K}|$$

By the second inequality above, we have $|\overline{K}| < |S|$. By the above equality and since S is infinite, then, we have

$$|S| = |S - \overline{K}|$$

Thus, by the first inequality above, we have

$$|F - \overline{K}| < |S - \overline{K}|$$

Thus, there is an injection $\theta : F \to S$ such that $\theta(a) = a$ for every $a \in \overline{K}$.

Now, we can make $\theta(F)$ into a field by defining for all $a, b \in F$ that

$$\theta(a)\theta(b) = \theta(ab)$$

and

$$\theta(a) + \theta(b) = \theta(a + b)$$

Since θ is the identity on $\overline{K}$, we have that $\theta(F)$ is a field extension of $\overline{K}$. Furthermore, we have by the above that $\theta : F \to \theta(F)$ is a $\overline{K}$-homomorphism which is an isomorphism.

Since $\theta : F \to \theta(F)$ is an isomorphism of fields and since F/K is an algebraic extension, it now follows that $\theta(F)/K$ is an algebraic extension. Since we also have $\theta(F) \subseteq S$, we may now conclude that $\theta(F) \in \mathcal{R}$. Finally, note that $F \neq \overline{K}$ since if $F = \overline{K}$, then the root u of $f(x)$ would be in $\overline{K}$ which is not the case since $f(x)$ has no roots in $\overline{K}$. Therefore, we have $\theta(F) \neq \overline{K}$. But since $\theta(F) \supseteq \overline{K}$ and $\theta(F) \neq \overline{K}$ and $\theta(F) \in \mathcal{R}$, this contradicts the maximality of $\overline{K} \in \mathcal{R}$. Therefore, $f(x)$ must have a root in $\overline{K}$ so that $\overline{K}$ is algebraically closed. This completes the first part of the problem.

We now prove the second part of the problem. Let K be a field and let $\overline{K}$ be an algebraic closure of K. We will prove this problem for each case of the cardinality of K. Before we begin, we show that $\overline{K}$ cannot be finite, independent of the cardinality of K. Towards this end, suppose that F is a finite field and write $F = \{a_1, \ldots, a_n\}$. Define

$$p(x) = 1 + \prod_{i=1}^{n}(x - a_i) \in F[x]$$

and note that in particular $p(x)$ is a nonconstant polynomial in $F[x]$. Clearly, we have $p(a_i) = 1 + 0 = 1 \neq 0$ for each $i \in \{1, \ldots, n\}$. Thus, we have exhibited a nonconstant polynomial $p(x) \in F[x]$ such that $p(x)$ has no roots in F. By definition, then, it now follows that F is not algebraically closed. Since F was an arbitrary finite field, this proves that every finite field fails to be algebraically closed. In particular, as $\overline{K}$ is algebraically closed, it now follows that $\overline{K}$ cannot be finite.

Now, suppose that K is finite and let $a \in \overline{K}$. Since $\overline{K}/K$ is an algebraic extension, we know that a is a root of some nonzero polynomial in $K[x]$. For each positive integer n, let P_n denote the collection of all polynomials of degree n over K. Since K is finite, it follows that P_n is finite for each positive integer n. Furthermore, we know that a polynomial of degree n over a field can have at most n roots. Combining the above results and noting that $\overline{K} \supseteq K$, we have that

$$|K| \leq |\overline{K}| \leq \sum_{n=1}^{\infty} n|P_n|$$

Note that the right-hand side of the above inequality is countably infinite. Thus, by this inequality and as $\overline{K}$ is not finite, we conclude that $\overline{K}$ is countably infinite.

Finally, suppose that K is infinite and let $a \in \overline{K}$. Since $\overline{K}/K$ is an algebraic extension, we know that a is a root of some nonzero polynomial in $K[x]$. For each positive integer n, let P_n denote the collection of all polynomials of degree n over K. Note that

P_n is infinite of the same cardinality as K for each positive integer n. Furthermore, we know that a polynomial of degree n over a field can have at most n roots. Combining the above results and noting that $\overline{K} \supseteq K$, we have that

$$|K| \leq |\overline{K}| \leq \sum_{n=1}^{\infty} n|P_n|$$

Note that the right-hand side of the above inequality is infinite of the same cardinality as K since P_n is infinite of the same cardinality as K for each positive integer n. Hence, by the above inequality, we conclude that $\overline{K}$ is infinite of the same cardinality as K. $\square$