ALGEBRA EXERCISES, PhD EXAMINATION LEVEL

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.

2. (a) Show that A_5 is simple.

   (b) Use (a) to show that S_n is not solvable for $n \geq 5$.

3. A proper subgroup M of a group G is maximal if whenever $M \leq H \leq G$, we have $H = M$ or $H = G$. Suppose that G is a finite group and G has only one maximal subgroup. Prove that G is cyclic of prime power order.

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. (Hint: Show it's free on the alphabet $X \setminus Y$.)

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 non-abelian.

   (Hint: Exhibit a non-abelian, infinite homomorphic image of G; there is one inside $PSL(2, \mathbf{Z})$, which is the group of 2 by 2 matrices with integer entries and determinant 1, modulo its center.)

6. Suppose that G is a finite solvable group. Prove that there is a sequence $G = G_0 \geq G_1 \geq \cdots \geq G_k = \{e\}$ of subgroups of G, so that each G_{i+1} is normal in G_i and G_i/G_{i+1} is cyclic.

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.

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 $Fr(G)$ denote the set of all non-generators of G.
   (a) Prove that $Fr(G)$ is a subgroup of G.
   (b) Show that $Fr(G)$ is the intersection of all maximal (proper) subgroups of G. (Careful with Zorn's Lemma!)

9. Suppose that R is a principal ideal domain. Prove that any submodule of a free R-module is free.

10. Prove that an abelian group is injective if and only if it is divisible.

11. Prove that every abelian group G can be embedded as a subgroup of a divisible abelian group.

12. Let G be an abelian group. Prove that G has a subgroup $d(G)$ which is divisible and contains all divisible subgroups of G, and, moreover, that $d(G)$ is a summand of G, such that $G/d(G)$ has no nontrivial divisible subgroups.

13. Suppose that R is a ring with identity.
    (a) Prove that each free left R-module is projective.
    (b) Prove that a left R-module P is projective if and only if each short exact sequence of left R-modules below splits

$$0 \to A \to B \to P \to 0.$$

You may use the fact that every left R-module is a homomorphic image of a free one.

14. Give an example of a projective module which is not free. Explain.

15. Let R be a ring with identity. Prove that a direct sum of left R-modules is projective if and only if each summand is projective.

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.

17. Suppose that A is a commutative ring with identity. If P and Q are projective A-modules, prove that $P \otimes_A Q$ is also projective.

18. Suppose that R is a principal ideal domain and F is its field of fractions. For any torsion-free R-module M, prove that $M \otimes_R F$ is the injective hull of M. (You may use any results about injective and flat modules over a PID; please identify them clearly.)

19. Suppose $(m, n) = 1$. Compute $\mathbf{Z}_m \otimes_{\mathbf{Z}} \mathbf{Z}_n$. Justify your answer.

20. Apply the Wedderburn-Artin Theorem to characterize the left Artinian rings R with identity for which $r^3 = r$, for each $r \in R$.

21. Prove that there are (up to ring isomorphism) only 12 semisimple rings of order 1008, of which only two are not commutative.

22. Suppose that G is a finite group and K is a field. Prove:

(a) If the characteristic of K does not divide $|G|$, then $K[G]$, the group algebra over K, is a semisimple left Artinian ring. (You may use that $K[G]$ is a ring with identity, and the Wedderburn-Artin Theorem in all its glory.

(b) Show that if the characteristic of K does divide the order of G, then the Jacobson radical of $K[G]$ is nontrivial.

23. State and prove the Jacobson Density Theorem.

24. Let R be a ring with identity, and suppose that $J(R)$ denotes the Jacobson radical of R. Prove that the following conditions are equivalent:

    (a) $R/J(R)$ is a division ring.

    (b) R has exactly one maximal right ideal.

    (c) All the nonunits of R are contained in a proper two sided ideal.

    (d) The nonunits of R form a two sided ideal.

    (e) For each $r \in R$, either r or $1 - r$ is a unit.

    (f) For each $r \in R$, either r or $1 - r$ is right invertible.

25. Let R be a ring with identity, and J be an indecomposable injective left R-module, and $S = \mathrm{End}_R(J)$. Prove that S satisfies condition (e) of the previous problem. (Hint: Recall that an injective module J is indecomposable if and only if every two nonzero submodules of J have nontrivial intersection.)

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.

27. Suppose that R is a ring with identity, M is a unital right R-module, N a unital left R-module, and G is an abelian group. **Mod-R** denotes

the category of right R-modules, while **Ab** stands for the category of abelian groups. Then the abelian groups

$$\mathrm{Hom}_{\mathbf{Mod-R}}(M, \mathrm{Hom}_{\mathbf{Ab}}(N,G)) \text{ and } \mathrm{Hom}_{\mathbf{Ab}}(M \otimes_R N, G)$$

are naturally isomorphic. Prove this, explaining what is meant by "naturally isomoprhic".

28. Suppose that R is a ring with identity. For each left R-module M, $\mathrm{Hom}_{\mathbf{R-Mod}}(R, M)$ is naturally R-isomorphic to M. Prove this, and explain what the "natural" part is all about.

29. Suppose that R is a ring with identity. Prove that

$$\mathrm{Hom}_{\mathbf{Ab}}(B, \Pi_{i \in I} G_i) = \Pi_{i \in I} \mathrm{Hom}_{\mathbf{Ab}}(B, G_i),$$

as right R-modules, for all left R-modules B and all abelian groups G_i ($i \in I$). You may use resources from category theory; if so, outline your argument so that it is clear which theorems you are appealing to.

30. Let R be a ring with identity.
    (a) Define *flat* left R-module.
    (b) Prove that a free left R-module is flat.

31. Suppose that R and S are rings with identity. Let ${}_SA_R$ be an S-R-bimodule, and B be a left R-module. Prove that $A \otimes_R B$ has a unique scalar multiplication making it a left S-module, so that $s(a \otimes b) = sa \otimes b$, for each $s \in S$, $a \in A$, and $b \in B$.

32. Let A be a commutative ring with identity, and suppose that M is an A-module, and I is an ideal of A. Prove that

$$(A/I) \otimes_A M \cong M/IM,$$

where IM is the submodule generated by all elements of the form xb, with $x \in I$, $b \in M$.

33. Suppose that A is a commutative ring with identity. Let $F(m)$ and $F(n)$ be the free modules on m and n generators, respectively. Prove that if $F(m) \cong F(n)$, then $m = n$.

34. Suppose that A is a commutative ring with identity, and that J is an ideal of A. Define the radical $\sqrt{J}$, and prove that $\sqrt{J}$ is the intersection of all the prime ideals of A that contain J.

35. Prove Nakayama's Lemma: let A be a commutative ring with identity. Let M be a finitely generated A-module, and I be an ideal of A, contained in the Jacobson radical $J(A)$ of A. Show that if $IM = M$ then $M = \{0\}$.

36. Let A be a commutative ring with identity, and S be a multiplicative system of A.

    (a) Briefly define: the ring of fractions $S^{-1}A$; module of fractions $S^{-1}M$. (Don't prove anything; simply spell out what's what.)

    (b) Prove that $S^{-1}(\cdot)$ is a covariant functor which carries short exact sequences of A-modules to short exact sequences of $S^{-1}A$-modules.

37. Let A be a commutative ring with identity. For each multiplicative system S of A, prove that $S^{-1}A$ is a flat A-module.

38. Let A be a commutative ring with identity. For each multiplicative system S of A, prove that the contraction $Q \mapsto Q \cap A$ is an order isomorphism from $Spec(S^{-1}A)$ onto the subset of $Spec(A)$ consisting of all prime ideals P of A which are disjoint from S.

39. Let F be a field; prove that the ring of formal power series $F[[T]]$ is a discrete valuation ring.

40. Give an outline of the proof of the following: if A is an integral domain and a subring of a field K, then the integral closure of A in K is the intersection of all the valuation subrings of K that contain A. Your outline should explain how the valuation rings in question are obtained.

41. Let A be a commutative ring with identity. A is *von Neumann regular* if for each $a \in A$ there exists an $x \in A$ such that $a^2x = a$. Let $n(A) = \sqrt{\{0\}}$. Prove that the following are equivalent for A:

    (a) A is von Neumann regular.

    (b) Every principal ideal of A is generated by an idempotent.

    (c) Every prime ideal of A is maximal.

    (d) $n(A) = \{0\}$ and $Spec(A)$ is a Hausdorff space.

42. Suppose that A is a commutative ring with identity, and that I is an ideal of A containing a regular element. Prove that I is projective (as an A-module) if and only if I is invertible (as a fractional ideal of its classical ring of fractions).

43. Let A be a commutative ring with identity, which satisfies the ascending chain condition on prime ideals. Must A be Noetherian? Prove, or else give a counterexample.

44. Prove that an Artinian commutative ring A with identity has only a finite number of prime ideals, and that each one is a maximal ideal.

45. Let A be a commutative ring with identity. Prove that if A is Artinian then it is Noetherian. (Hint: Use the preceding exercise, and show the question can be reduced to considering finite dimensional vector spaces over the residue fields of A.)

46. Suppose that A is a commutative ring with identity, and M is an A-module. Show that the following are equivalent:

   (a) M is flat over A.
   (b) M_P is flat over A_P, for each prime ideal P of A.
   (c) M_Q is flat over A_Q, for each maximal ideal Q of A.

   (Note: Clearly state the facts about localization which are needed here.)

47. Prove Noether's Normalization Lemma: If K is an infinite field field and A is a finitely generated K-algebra, then A is integral over K, or else one can choose $\{ x_1, x_2, \cdots, x_n \}$ and an index r, with $1 \leq r \leq n$, so that $A = K[x_1, x_2, \cdots, x_n]$, and

   (a) $\{ x_1, x_2, \cdots, x_r \}$ is algebraically independent over K, and
   (b) A is integral over $K[x_1, x_2, \cdots, x_r]$.

48. Suppose that A is a subring of the commutative ring B with 1. If B is integral over A, prove that every homomorphism f of A into the algebraically closed field L admits an extension to a homomorphism $g : B \to L$.

49. State and prove the Hilbert Basis Theorem.

50. Let k be a field; $A = k[T_1, T_2, \cdots, T_n]$ stands for the polynomial ring in n indeterminates.

   (a) Define: the *affine variety* associated with an ideal I of A.
   (b) The affine varieties are the closed subsets of a topology on k^n; accepting this, prove that the closed subsets of k^n satisfy the descending chain condition.

51. If A is a commutative ring with identity which is Noetherian, then prove that $A[[T]]$, the ring of formal power series, is also Noetherian.

52. State and prove the Hilbert Nullstellensatz.

53. Let A be an integral domain.

    (a) In terms of valuations, define *discrete valuation ring*.

    (b) Prove that a valuation ring A is discrete if and only if it is a principal ideal domain.

54. Let A be an integral domain.

    (a) Define: *invertible fractional ideal* of A.

    (b) Prove that A is an Dedekind domain if and only if every nonzero fractional ideal is invertible. (Hint: Do it first in the local case, and then use localization to complete the proof.)

55. Let A be a local Noetherian commutative ring with identity, and M be a finitely generated A-module. Prove that M is flat if and only if it is free.

56. Prove that the lattice of all ideals of a Dedekind domain is distributive. (Hint: Localize!)

57. Use the group algebra to establish the existence of a valuation ring of Krull dimension one which is not discrete. (Outline any relevant construction clearly, and state all pertinent facts.)

58. Using the primary decomposition of ideals in Noetherian rings, prove that if A is a Dedekind domain then every nonzero ideal is expressible as a product of prime ideals. (Hint: Show at some point that if Q is a primary ideal in a Noetherian ring, with $\sqrt{Q}$ maximal, then Q is a power of its radical.)

59. Among the following integral domains, decide which ones are Dedekind domains, and give a brief explanation.

    (a) $\mathbf{Z}[T]$, the polynomial ring over the integers, in one variable.
    (b) $\mathbf{Z}[\sqrt{-5}] = \{\, a + b\sqrt{-5} \,:\, a, b \in \mathbf{Z} \,\}$.
    (c) The ring $k[[T]]$ of all formal power series in one variable, over the field k.
    (d) $k[T_1, T_2]$, the polynomial ring in two variables, over the field k.

60. Let Θ_p be the p-th cyclotomic polynomial over the field $\mathbf{Q}$, where p is a prime number. Outline an argument which shows that the Galois group of the splitting field of Θ_p over $\mathbf{Q}$ is cyclic of order $p-1$. (Clearly identify the results you need for the argument.)

61. Compute the Galois groups of the splitting fields of the following polynomials, over $\mathbf{Q}$:

    (a) $p(T) = T^5 - 2$; (ingredients: a little Sylow Theory, semidirect products,...?)
    (b) $p(T) = T^3 - 3T + 3$; (how many real roots?)

62. Suppose that E is a finite Galois extension of the field F. If $\mathrm{Gal}(E/F)$ has order pq, where $p < q$ are distinct primes, and p does not divide $q-1$, prove that E has two subfields E_p and E_q, which are stable under the action of $\mathrm{Gal}(E/F)$, such that $E_p \cap E_q = F$, E_p and E_q generate E, and $\mathrm{Gal}(E_p/F)$ (resp. $\mathrm{Gal}(E_q/F)$) is cyclic of order p (resp. q).

63. Prove that an automorphism of the real field is necessarily the identity.

64. Let E be a finite field extension of F, and $G = \mathrm{Gal}(E/F)$. Denote by $(\cdot)'$ the Galois correspondences $L \to L'$ and $H \to H'$, mapping intermediate subfields to subgroups of G and back.

(a) If L is an intermediate subfield which is invariant under all the automorphisms of G, then show that L' is normal in G.

(b) If H is a normal subgroup of G, then prove that $gH' = H'$, for each $g \in G$.

65. (a) Define: splitting field of a polynomial.

(b) Assuming existence and uniqueness of splitting fields, up to isomorphism over the base field, prove this: *Let E be a finite extension of F. Then E is a splitting field for some polynomial if and only if every irreducible polynomial over F, having a root in E, factors completely over E.*

66. Use the notions of formal derivatives to show that, if $f(T)$ is an irreducible polynomial over the field F then it has repeated roots in the splitting field if and only if the characteristic of F is $p > 0$, and $f(T) = g(T^p)$, for some $g(T) \in F[T]$.

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 $p(T)$ is an irreducible polynomial over $\mathbf{Q}$, of degree p, having exactly two non-real roots, then show that the Galois group of the splitting field of $p(T)$ is S_p.

68. Prove that any finite subgroup of the multiplicative group of nonzero elements of a field is cyclic.

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.

70. Consider the polynomial over the field $\mathbf{F}_2$ of two elements: $g(x) = x^4 + x^3 + x^2 + x + 1$.

(a) Prove that $g(x)$ is irreducible over $\mathbf{F}_2$.

(b) Let K be a splitting field for $g(x)$ over $\mathbf{F}_2$, and let $r \in K$ be a root of $g(x)$. Factor $g(x)$ into irreducibles over $\mathbf{F}_2(r)$.

(c) Show that $K = \mathbf{F}_2(r)$.

(d) Find the Galois group $\mathrm{Gal}(K/\mathbf{F}_2)$.

71. Let K/k be a cyclic extension of fields with finite Galois group $< \sigma >$.

(a) State the Hilbert Theorem 90 in the multiplicative form.

(b) Suppose $[K : k] = n$ is relatively prime to the characteristic of k, and k contains a primitive n-th root of unity. Prove that there exists $\alpha \in K$ such that $K = k(\alpha)$ and $Irr(\alpha, k, x)$ (i.e., the irreducible polynomial of α over k) is $x^n - a$ for some $a \in k$.

72. (a) Define: *algebraic closure*.

(b) Prove that every field has an algebraic closure, and argue that if E is an algebraic closure of F, then $|E|$ is countable, if F is finite, while $|E| = |F|$, otherwise.