11.2.9 Given a linear \( \varphi : V \to V \) such that \( \varphi(W) \subseteq W \), show \( \varphi \) induces linear \( \varphi|W : W \to W \) and \( \bar{\varphi} : V/W \to V/W \):

**Solution.** That \( \varphi|W \) is a linear map \( W \to W \) follows from the definition of subspace. The map \( \bar{\varphi} \) is \( \varphi(v + W) = \varphi(v) + W \), which is well-defined since

\[
 v + W = v' + W \Rightarrow v - v' \in W \Rightarrow \varphi(v - v') \in W \Rightarrow \varphi(v) + W = \varphi(v') + W.
\]

The linearity of \( \bar{\varphi} \) follows from that of \( \varphi \).

If \( \varphi|W \) and \( \bar{\varphi} \) are nonsingular, show that \( \varphi \) is nonsingular:

**Solution.**

Suppose \( \varphi(v) = 0 \). The definition of \( \bar{\varphi} \) shows that \( \bar{\varphi}(v + W) = 0 \). Since \( \bar{\varphi} \) is nonsingular, \( v + W = 0 \) in \( V/W \) and thus \( v \in W \). Since \( \varphi|W \) is nonsingular, \( \varphi(v) = 0 \) and \( v \in W \) imply \( v = 0 \).

The converse holds if \( \dim V < \infty \):

**Solution.** For a finite-dimensional space, a nonsingular linear map is an automorphism. Since \( V \) has finite dimension, so do \( W \) and \( V/W \). We suppose \( \varphi \) is nonsingular. Evidently \( \varphi|W \) is nonsingular; suppose now \( \bar{\varphi}(v + W) = 0 \). From the definition of \( \bar{\varphi} \) we conclude that \( (\varphi) \in W \), and since \( \varphi|W \) is an automorphism there is a \( w \in W \) such that \( \varphi(w) = \varphi(v) \). Then \( \varphi(v - w) = 0 \), and as \( \varphi \) is nonsingular, \( v - w = 0 \), i.e. \( v = w \) and then \( v \in W \). It follows that \( v + W = 0 \) in \( V/W \), as required.

The last statement is false in the infinite-dimensional case: Consider \( V = \mathbb{K}^\mathbb{N} \), \( \varphi((v_i)) = (w_i) \) with \( w_0 = 0 \), \( w_i = v_{i-1} \) for \( i > 0 \). Then the set \( W \) of \( (v_i) \) such that \( v_0 = 0 \) is a subspace of \( V \) stable under \( \varphi \). Furthermore \( \varphi \) is nonsingular, but \( \bar{\varphi} \) is identically 0.

11.2.11 Given \( \varphi : V \to V \) such that \( \varphi^2 = \varphi \), (a) Show \( \text{Im}(\varphi) \cap \text{Ker}(\varphi) = 0 \):

**Solution.** Suppose \( v \in \text{Im}(\varphi) \cap \text{Ker}(\varphi) \). Then \( \varphi(v) = 0 \) and \( v = \varphi(w) \) for some \( w \in V \); consequently

\[
 v = \varphi(w) = \varphi^2(w) = \varphi(v) = 0
\]

as required.

(b) Show that \( V = \text{Im}(\varphi) \oplus \text{Ker}(\varphi) \):
Solution. We have shown $\text{Im}(\varphi) \cap \text{Ker}(\varphi) = 0$, so by the recognition theorem for direct sums we need only show $V = \text{Im}(\varphi + \text{Ker}(\varphi))$. In fact for any $v \in V$, $v = \varphi(v) + (v - \varphi(v))$; clearly $\varphi(v) \in \text{Im}(\varphi)$ and

$$
\varphi(v - \varphi(v)) = \varphi(v) - \varphi^2(v) = \varphi(v) - \varphi(v) = 0
$$

shows that $v - \varphi(v) \in \text{Ker}(\varphi)$.

(c) Show that $V$ has a basis for which the matrix of $\varphi$ is diagonal, with all diagonal entries equal to 0 or 1:

Solution. Pick a basis $\{v_i\}_{i \in I}$ of $\text{Im}(\varphi)$ and $\{w_j\}_{j \in J}$ of $\text{Ker}(\varphi)$. By part (b) we know that $\{v_i, w_j\}_{i \in I, j \in J}$ is a basis of $V$. Since $\varphi(v_i) = v_i$ and $\varphi_j(w_j) = 0$ for all $i$ and $j$, the matrix of $\varphi$ is diagonal, with 1s and 0s on the diagonal.

11.3.3 $V$ is a vector space of finite dimension, $S \subseteq V^*$ is a subset of the dual. (a) Show $\text{Ann}(S)$ is a subspace of $V$:

Solution. If $v, w \in \text{Ann}(S)$ then $v(x) = w(x) = 0$ for all $x \in S$, and consequently $(av + bw)(x) = av(x) + bw(x) = 0$ for all $x \in S$ and scalars $a, b$. It follows that $av + bw \in \text{Ann}(S)$.

(b) If $W_1, W_2 \subseteq V^*$ are subspaces, show $\text{Ann}(W_1 + W_2) = \text{Ann}(W_1) \cap \text{Ann}(W_2)$ and $\text{Ann}(W_1 \cap W_2) = \text{Ann}(W_1) + \text{Ann}(W_2)$:

Solution. Since $W_1 \subseteq W_1 + W_2$ and $W_2 \subseteq W_1 + W_2$, $\text{Ann}(W_1 + W_2) \subseteq \text{Ann}(W_1)$ and $\text{Ann}(W_1 + W_2) \subseteq \text{Ann}(W_2)$, so finally $\text{Ann}(W_1 + W_2) \subseteq \text{Ann}(W_1) \cap \text{Ann}(W_2)$. Conversely if $v \in \text{Ann}(W_1) \cap \text{Ann}(W_2)$ and $x \in W_1, y \in W_2$ then $v(x) = v(y) = 0$ and thus $v(x + y) = 0$. Since $x$ and $y$ were arbitrary, $v \in \text{Ann}(W_1 + W_2)$. Notice that this part doesn’t require $V$ to have finite dimension.

For the second equality we first choose a basis $x_1, \ldots, x_r$ of $W_1 \cap W_2$, and extend it to bases $x_1, \ldots, x_r, y_1, \ldots, y_s$ of $W_1$ and $x_1, \ldots, x_r, z_1, \ldots, z_s$ of $W_2$. Then the set of $x_1, \ldots, x_r, y_1, \ldots, y_s, z_1, \ldots, z_s$ is independent (check this!), and may be extended to a basis $x_1, \ldots, x_r, y_1, \ldots, y_s, z_1, \ldots, z_s, w_1, \ldots, w_u$ of $V^*$. If we identify $V^{**} \simeq V$, we see that there is a basis

$$
x_1^\vee, \ldots, x_r^\vee, y_1^\vee, \ldots, y_s^\vee, z_1^\vee, \ldots, z_s^\vee, w_1^\vee, \ldots, w_u^\vee
$$

of $V$ for which the dual basis of $V^*$ is $x_1, \ldots, x_r, y_1, \ldots, y_s, z_1, \ldots, z_s, w_1, \ldots, w_u$.

By (a), an element

$$
v = \sum_i a_i x_i^\vee + \sum_j b_j y_j^\vee + \sum_k c_k z_k^\vee + \sum_\ell d_\ell w_\ell^\vee
$$

of $V$ is in $\text{Ann}(W_1 \cap W_2)$ if and only if $a_i = 0$ for all $i$. If this is so, $v = v_1 + v_2$.
where
\[ v_1 = \sum_j b_j y_j^\vee \in \text{Ann}(W_1), \quad v_2 = \sum_k c_k z_k^\vee + \sum_\ell d_\ell w_\ell^\vee \in \text{Ann}(W_2). \]

Since \( v \) was arbitrary, \( \text{Ann}(W_1 \cap W_2) \subseteq \text{Ann}(W_1) + \text{Ann}(W_2) \). For the reverse inclusion it suffices to show \( \text{Ann}(W_1) \subseteq \text{Ann}(W_1 \cap W_2) \) and \( \text{Ann}(W_2) \subseteq \text{Ann}(W_1 \cap W_2) \), but this follows from \( W_1 \cap W_2 \subseteq W_1 \) and \( W_1 \cap W_2 \subseteq W_2 \).

(c) With the same notation, show \( W_1 = W_2 \) if and only if \( \text{Ann}(W_1) = \text{Ann}(W_2) \):

**Solution.** It suffices to show the if part. By part (b) the hypothesis implies that \( \text{Ann}(W_1 \cap W_2) = \text{Ann}(W_1 + W_2) \). We first claim that if \( W \subseteq W' \subseteq V^* \) and \( \text{Ann}(W) = \text{Ann}(W') \) then \( W = W' \). If not, there is a \( v \in W' \setminus W \). Let \( x_1, \ldots, x_r \) be a basis of \( W \); since \( v \not\in W \) the set \( x_1, \ldots, x_r, v \) is independent and may be extended to a basis of \( V^* \). Then the element \( v^\vee \) of the dual basis of \( V \) vanishes on \( W \) but not on \( W' \), and so \( \text{Ann}(W) \neq \text{Ann}(W') \).

Applying this to the spaces \( W_1 \cap W_2 \subseteq W_1 + W_2 \subseteq V^* \) we see that in fact \( W_1 \cap W_2 = W_1 + W_2 \subseteq V^* \) and consequently \( W_1 = W_2 \).

(d) Show \( \text{Ann}(S) = \text{Ann}(\text{Span}(S)) \):

**Solution.** Clearly \( \text{Ann}(\text{Span}(S)) \subseteq \text{Ann}(S) \). If \( v \in \text{Ann}(S) \) then \( s(v) = 0 \) for all \( s \in S \) and thus \( \sum_i a_i s_i(v) = 0 \) if \( s_i \in S \). Thus \( v \in \text{Ann}(\text{Span}(S)) \).

(e) If \( \{v_1, \ldots, v_n\} \) is a basis of \( V \) and \( S = \{v_1^*, \ldots, v_k^*\} \), show \( \text{Ann}(S) = \text{Span}(v_{k+1}, \ldots, v_n) \):

**Solution.** If \( v = \sum_i a_i v_i \) then \( v_i^*(v) = a_i \), so \( v \in \text{Ann}(S) \) if and only if \( a_1 = \cdots = a_k = 0 \), i.e. \( v \in \text{Span}(v_{k+1}, \ldots, v_n) \).

**11.3.4** If \( V \) has infinite dimension with basis \( A \) and \( A^* = \{v^* \mid v \in A\} \), show that \( A^* \) does not span \( V^* \):

**Solution.** Let \( v^* \in V \) be such that \( v^*(v) = 1 \) for all \( v \in A \) (there is a unique \( v^* \) with this property). If \( v^* \in \text{Span}(A^*) \), there is a finite set \( T \subseteq A^* \) such that \( v^* \in \text{Span}(T) \). For \( v \in A^* \setminus T \) we then have \( v^*(v) = 0 \), a contradiction. Therefore \( v^* \not\in \text{Span}(A^*) \).

**11.4.3** If \( R \) is commutative with 1 and \( A \) is an \( n \times n \) matrix such that \( Ax = 0 \), \( x = (x_1 \ x_2 \cdots x_n)^T \), show that \( \text{det}(A) x_i = 0 \) for all \( i \):

**Solution.** Write \( A \) in block form as \( A = (v_1 \ v_2 \cdots v_n) \) with column vectors \( v_i \in R^n \). Then \( Ax = \sum_i x_i v_i = 0 \), and
\[ \det(v_1 \ v_2 \cdots 0 \cdots v_n) = 0 \]
where the 0 is in column \( i \). Since the determinant is a linear function of its
columns, we may write this

\[ \sum_j x_j \det A_j = 0 \]

where \( A_j \) is the matrix obtained by replacing the \( i \)th column with the \( j \)th. If \( j \neq i \) then \( A_j \) has two identical columns, and then \( \det(A_j) = 0 \). When \( j = i \), \( A_i = A \), so the equation says that \( x_i \det(A) = 0 \).

12.1.4 Suppose \( R \) is an integral domain, \( M \) is an \( R \)-module, \( N \) is a submodule of rank \( r \), and \( M/N \) has rank \( s \); show \( M \) has rank \( r + s \):

**Solution.** There are independent elements \( n_1, \ldots, n_r \in N \) such that \( N' = \sum_i Rn_i \) is free and \( N/N' \) is torsion, and elements \( m_1, \ldots, m_s \in M \) such that \( m_1 + N, \ldots, m_s + N \) are independent in \( M/N \), \( M'' = \sum_j R(m_j + N) \subseteq M/N \) is free and \( (M/N)/M'' \) is torsion. We will show that \( n_1, \ldots, n_r, m_1, \ldots, m_s \) is an independent set and that if \( M' = \sum_j Rm_j + N' \) then \( M/M' \) is torsion; this will show that the rank of \( M \) is \( r + s \).

Suppose \( \sum_i a_im_i + \sum_j b_jn_j = 0 \). Then \( \sum_i b_i(m_i + N) = 0 \), and we see that \( b_i = 0 \) for all \( i \). Then \( \sum_j b_jn_j = 0 \), and it follows that \( b_j = 0 \) for all \( j \).

Suppose now \( m \in M \) is nonzero. There is a nonzero \( r \in R \) such that \( r(m + N) \in M'' \), and if we write \( r(m + N) = \sum_j a_j(m_j + N) \) then \( rm - \sum_j a_jm_j \in N \). There is then a nonzero \( s \in R \) such that

\[ s(rm - \sum_i a_im_i) = N' \]

and it follows that \( srm \in M' \). Since \( R \) is an integral domain \( rs \neq 0 \) and we have show that \( M/M' \) is torsion.

12.1.13 Suppose \( R \) is a PID and \( M \) is a finitely generated \( R \)-module; describe \( M/\text{Tor}(M) \):

**Solution.** We first observe that for any family \( \{M_i\}_{i \in I} \) of \( R \)-modules and \( M = \bigoplus_i M_i \),

\[ \text{Tor}(M) = \bigoplus_i \text{Tor}(M_i). \]

In fact for \( (m_i) \in M, r \in R \) we have \( r(m_i) = 0 \) if and only if \( rm_i = 0 \), from which it follows that \( \text{Tor}(M) \subseteq \bigoplus_i \text{Tor}(M_i) \). Suppose now \( (m_i) \in \bigoplus_i \text{Tor}(M_i) \) is nonzero. There is a finite set \( J \subseteq I \) such that \( i \notin J \) implies \( m_i = 0 \). For \( i \in J \) choose nonzero \( r_i \in R \) such that \( r_im_i = 0 \) for \( i \notin J \); then if \( r = \prod_{i \in J} r_i \), \( rm_i = 0 \) for all \( i \in J \) and thus \( r(m_i) = 0 \). Since \( R \) is an integral domain, \( r \neq 0 \). Thus \( (m_i) \in \text{Tor}(M) \).

If \( d \) is a nonzero element of \( R \), \( \text{Tor}(R/(d)) = R/(d) \), while \( \text{Tor}(R) = 0 \). If finally
\[ M \cong \bigoplus_i R/(d_i) \oplus R^n \text{ with } d_i \neq 0, \]
\[ \text{Tor}(M) = \bigoplus_i \text{Tor}(R/(d_i)) \oplus \text{Tor}(R)^n \cong R^n. \]

12.2.4 Show that two 3 \times 3 matrices (coefficients in a field) with the same minimal and characteristic polynomials are similar:

**Solution.** Suppose \( A \) and \( B \) are 3 \times 3 matrices with characteristic polynomial \( \Phi \), and minimal polynomial \( m \).

1. If \( m \) has degree 3, it is the only invariant factor for \( A \) and \( B \), and so they are similar.
2. If \( m \) has degree 2 there is a linear polynomial \( f \) such that \( fm = \Phi \). Then \( A \), \( B \) both have \( f \), \( m \) for invariant divisors, and are similar.
3. If \( m \) is linear, \( \Phi = f^3 \) and both \( A \), \( B \) have invariant factors \( f \), \( f \), \( f \). So they are similar.

Give a counterexample for 4 \times 4 matrices:

**Solution.** Let \( \ell = X - a \) be any linear polynomial; there are 4 \times 4 matrices \( A \), \( B \) such that \( A \) has invariant factors \( \ell \), \( \ell \), \( \ell^2 \) and \( B \) has invariant factors \( \ell^2 \), \( \ell^2 \). Then \( A \) and \( B \) both have minimal polynomial \( \ell^2 \) and characteristic polynomial \( \ell^4 \), but are not similar since their invariant factors are different.

12.2.7 Find the eigenvalues of the matrix

\[
\begin{pmatrix}
0 & 1 & 0 & 0 \\
0 & 0 & 1 & 0 \\
0 & 0 & 0 & 1 \\
1 & 0 & 0 & 0
\end{pmatrix}
\]

**Solution.** Observe that the matrix is the transpose of the companion matrix of \( X^4 - 1 \), and so has the same characteristic polynomial, namely \( X^4 - 1 \). The problem does not specify the field! There are two cases: (a) If the field has characteristic 0 or \( p \) with \( p \) odd, the characteristic polynomial has 4 distinct roots \( \pm 1, \pm i \) where \( i \) is a root of \( X^2 + 1 \) in some extension of the field of degree 1 or 2. (b) if the field has characteristic 2, the characteristic polynomial is \((X - 1)^4\) which has 1 as a fourfold root.

12.2.8 Show that the characteristic polynomial of the companion matrix of a polynomial \( f(x) \) is \( f(x) \) itself:
Solution. Say \( f(x) = a_0 + a_1 x + \cdots + x^n \), so the characteristic polynomial is

\[
\begin{vmatrix}
 x & 0 & a_0 \\
-1 & x & 0 & a_1 \\
0 & -1 & x & 0 & a_2 \\
\vdots & \ddots & \ddots & \ddots & \ddots \\
 & & & & -1 & a_{n-1} + x
\end{vmatrix}
\]

The assertion is clear if \( n = 1 \), so we use induction on \( n \). Using the cofactor expansion for the first row, we see this is

\[
\begin{vmatrix}
 x & 0 & a_1 \\
-1 & x & 0 & a_2 \\
\vdots & \ddots & \ddots & \ddots \\
 & & & & -1 & a_{n-1} + x
\end{vmatrix} = x \begin{vmatrix}
 x & 0 \\
-1 & x \\
\vdots & \ddots \\
 & & -1 & a_{n-1} + x
\end{vmatrix} + (-1)^{n+1}a_0 \begin{vmatrix}
 0 & -1 & x & 0 \\
\vdots & \ddots & \ddots & \ddots \\
 & & & & -1
\end{vmatrix}
\]

The first term is \( x \) times the characteristic polynomial of the companion matrix of \( a_1 + a_2 x + \cdots + x^{n-1} \), which by induction is that polynomial itself. The second determinant is upper triangular, equal to \((-1)^{n-1}\). The assertion follows.

12.2.10 Find all similarity classes of \( 6 \times 6 \) matrices over \( \mathbb{Q} \) with minimal polynomial \( (X + 2)^2(X - 1) \).

Solution. It suffices to find the possible invariant factors that yield this minimal polynomial. The characteristic polynomial has degree six and the last invariant factor has degree three, so the degrees of the others must add up to three. Here’s how the possibilities break down:

- If there’s only one other invariant factor, it’s necessarily equal to \((X + 2)^2(X - 1)\). The rational canonical form is

  \[
  \begin{pmatrix}
  0 & 0 & 4 \\
  1 & 0 & 0 \\
  0 & 1 & -3
  \end{pmatrix}
  \begin{pmatrix}
  0 & 0 & 4 \\
  1 & 0 & 0 \\
  0 & 1 & -3
  \end{pmatrix}
  \]

  (entries not indicated are 0).

- If there are two other invariant factors, they have degrees one and two and successively divide each other (and \((X + 2)^2(X - 1)\) as well). The possibilities are

  1. \( X - 1, (X - 1)(X + 2), (X + 2)^2(X - 1) \)
  2. \( X + 2, (X - 1)(X + 2), (X + 2)^2(X - 1) \)
3. $X + 2, (X + 2)^2, (X + 2)^2(X - 1)$

The corresponding rational canonical forms are

$$
\begin{pmatrix}
1 & 0 & 2 \\
0 & 0 & 4 \\
1 & 0 & 0
\end{pmatrix},
\begin{pmatrix}
1 & 1 & 0 \\
0 & 0 & 4 \\
1 & 0 & 0
\end{pmatrix},
\begin{pmatrix}
1 & 0 & 1 \\
0 & 0 & 4 \\
1 & 0 & 0
\end{pmatrix}
$$

• If there are three other invariant factors they are all linear and equal. The possibilities are

1. $X - 1, X - 1, X - 1, (X + 2)^2(X - 1)$
2. $X + 2, X + 2, X + 2, (X + 2)^2(X - 1)$

and the rational canonical forms are

$$
\begin{pmatrix}
1 & 1 & 0 \\
0 & 0 & 4 \\
1 & 0 & 0
\end{pmatrix},
\begin{pmatrix}
-2 & 0 & 2 \\
0 & 0 & 4 \\
1 & 0 & 0
\end{pmatrix},
\begin{pmatrix}
-2 & 0 & -4 \\
0 & 0 & 4 \\
1 & 0 & 0
\end{pmatrix}
$$

12.2.11 Find all similarity classes of $6 \times 6$ matrices over $\mathbb{Q}$ with characteristic polynomial $(X^4 - 1)(X^2 - 1)$:

Solution. Since $(X^4 - 1)(X^2 - 1) = (X^2 + 1)(X + 1)(X - 1)^2$ is the irreducible factorization in $\mathbb{Q}[X]$, the possible invariant factors are

• $(X^4 - 1)(X^2 - 1)$
• $(X + 1)(X - 1), (X^2 + 1)(X + 1)(X - 1)$
• $X + 1, (X^2 + 1)(X + 1)(X - 1)^2$
• $X - 1, (X^2 + 1)(X + 1)^2(X - 1)$

The corresponding rational canonical forms, in order, are

$$
\begin{pmatrix}
0 & 1 & 0 \\
1 & 0 & -1 \\
1 & 0 & 0
\end{pmatrix},
\begin{pmatrix}
0 & 1 & 0 \\
1 & 0 & 0 \\
1 & 0 & 0
\end{pmatrix}
$$
12.3.22 If $A \in M_{n \times n}(\mathbb{C})$ satisfies $A^3 - A = 0$, then $A$ is diagonalizable.

**Solution.** The minimal polynomial divides $X^3 - X = X(X + 1)(X - 1)$, and since all elementary divisors must divide this, the elementary divisors are all linear. This implies that $A$ is diagonalizable: if $(X - a)$ is one of the elementary divisors, the corresponding summand of $\mathbb{C}^n$ is $\mathbb{C}[X]/(X - a) \cong \mathbb{C}$ and has dimension one.

Is this true over an arbitrary field?

**Solution.** It’s false for a field of characteristic 2, for then the minimal polynomial factors $X(X + 1)^2$. If, say, this is both the minimal and characteristic polynomial (so that $n = 3$) the Jordan decomposition is a block of size one with eigenvalue 0, and a block of size two with eigenvalue one. Note, however, that if the characteristic is $p \neq 2$, the situation is the same as for $\mathbb{C}$.

12.3.23 There is no $A \in M_{3 \times 3}(\mathbb{Q})$ with $A^8 = I$ but $A^4 \neq I$.

**Solution.** The condition is that the minimal polynomial divides $X^8 - 1$ but not $X^4 - 1$. Since $X^8 - 1 = (X^4 - 1)(X^4 + 1)$, this means that every irreducible factor of the minimal polynomial divides $X^4 + 1$. Since the latter is irreducible over $\mathbb{Q}$, the minimal polynomial must then have degree at least four, which is absurd for a $3 \times 3$ matrix.

12.3.31 A nilpotent matrix is similar to a block diagonal matrix whose blocks have 1s on the first superdiagonal and 0s elsewhere.

**Solution.** If $A$ is nilpotent, say $A^k = 0$, then $Av = \lambda v$ implies $0 = A^k v = \lambda^k v$, so if $v \neq 0$ then $\lambda = 0$. In other words, 0 is the only eigenvalue of $A$. Since the eigenvalues are all in the field, $A$ is similar to a matrix in Jordan normal form, and this has the asserted type.

13.1.4 The map $a + b\sqrt{2} \mapsto a - b\sqrt{2}$ is an isomorphism of $\mathbb{Q}(\sqrt{2})$ with itself.
Solution. Say $\varphi(a+b\sqrt{2}) = a-b\sqrt{2}$. This is evidently a bijection. Furthermore

$$
\varphi((a + b\sqrt{2}) + (c + d\sqrt{2})) = \varphi((a + c) + (b + d)\sqrt{2})
$$

$$
= (a + c) - (b + d)\sqrt{2} = (a - b\sqrt{2}) + (c - d\sqrt{2})
$$

$$
= \varphi(a + b\sqrt{2}) + \varphi(c + d\sqrt{2})
$$

and

$$
\varphi((a + b\sqrt{2})(c + d\sqrt{2})) = \varphi((ac + 2bd) + (ad + bc)\sqrt{2})
$$

$$
= (ac + 2bd) - (ad + bc)\sqrt{2}
$$

$$
= (a - b\sqrt{2})(c - d\sqrt{2})
$$

$$
= \varphi(a + b\sqrt{2})\varphi(c + d\sqrt{2}).
$$

13.1.7 The polynomial $X^3 - nX + 2$ is irreducible in $\mathbb{Q}[X]$ if $n \neq -1, 3, 5$.

Solution. If it’s not irreducible it must have a linear factor, and thus a root in $\mathbb{Q}$. Since it’s monic, root in $\mathbb{Q}$ is integral and divides the constant term 2. So it suffices to substitute $X = \pm 1, \pm 2$ and see what this says about $n$:

1. $1^3 - n + 2 = 0 \Rightarrow n = 3$
2. $(-1)^3 - n(-1) + 2 = 0 \Rightarrow n = -1$
3. $2^3 - 2n + 2 = 0 \Rightarrow n = 5$
4. $(-2)^3 - (-2)n + 2 = 0 \Rightarrow n = 3$.

13.2.4 Find the degree over $\mathbb{Q}$ of $2 + \sqrt{3}$ and $1 + 2^{1/3} + 2^{2/3}$.

Solution. $2 + \sqrt{3}$ is a root of $(X - 2)^2 - 3 = 0$, so it has degree at most 2. If it had degree 1 then $\sqrt{3} \in \mathbb{Q}$, which is absurd.

Let $\alpha = 1 + 2^{1/3} + 2^{2/3}$. This is contained in $\mathbb{Q}(2^{1/3})$ which has degree 3 over $\mathbb{Q}$, so the degree of $\alpha$ is either 1 or 3. If it has degree 1, then $\alpha$ and $\alpha^2$ are in $\mathbb{Q}$. Then

$$
1 + 0 \cdot 2^{1/3} + 0 \cdot 2^{2/3} = 1
$$

$$
1 + 1 \cdot 2^{1/3} + 1 \cdot 2^{2/3} = \alpha
$$

$$
5 + 4 \cdot 2^{1/3} + 3 \cdot 2^{2/3} = \alpha^2
$$

say that $(1, 2^{1/3}, 2^{2/3})$ is a solution of a $3 \times 3$ system with matrix $\begin{pmatrix} 0 & 1 & 1 \\ 1 & 1 & 1 \\ 5 & 4 & 3 \end{pmatrix}$ and whose known side is entirely rational. Since the matrix is rational and
invertible (in fact it has determinant 1), this implies that $2^{1/3}$ and $2^{2/3}$ are rational, which is false. Thus $\alpha$ has degree 3.

13.2.7 Show that $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$. Conclude that $[\mathbb{Q}(\sqrt{2} + \sqrt{3} : \mathbb{Q}] = 4$. Find an irreducible polynomial satisfied by $\sqrt{2} + \sqrt{3}$.

Solution. Since $\sqrt{2}, \sqrt{3} \in \mathbb{Q}(\sqrt{2}, \sqrt{3})$ we have $\sqrt{2} + \sqrt{3} \in \mathbb{Q}(\sqrt{2}, \sqrt{3})$ and thus $\mathbb{Q}(\sqrt{2} + \sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3})$.

To show the reverse inclusion it’s actually easier to show first that $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$. First, $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ and $\sqrt{3}$ is a root of a quadratic with coefficients in $\mathbb{Q}(\sqrt{2})$ (in fact in $\mathbb{Q}$) so the degree of $\sqrt{3}$ over $\mathbb{Q}(\sqrt{2})$ is either 1 or 2. If it’s 1, $\sqrt{3} = a + b\sqrt{2}$ with $a, b \in \mathbb{Q}$. Squaring this yields $3 = a^2 + 2ab^2 + 4b^2\sqrt{2}$, which forces $ab = 0$ since $\sqrt{2} \notin \mathbb{Q}$. But if $a = 0$, $\sqrt{3}/2$ is rational and if $b = 0$, $\sqrt{3}$ is rational. Thus $\sqrt{3}$ has degree 2 over $\mathbb{Q}(\sqrt{2})$ and it follows that $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$. Now 1, $\sqrt{2}$ is a basis of $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$, and 1, $\sqrt{3}$ is a basis of $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}(\sqrt{2})$, so 1, $\sqrt{2}$, $\sqrt{3}$, $\sqrt{6}$ is a basis of $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$.

Since $\mathbb{Q}(\alpha) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3})$, $\alpha = \sqrt{2} + \sqrt{3}$ has degree 1, 2 or 4 over $\mathbb{Q}$, and $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ if and only if its degree is 4. If it has degree 1, $\sqrt{2} + \sqrt{3}$ is rational and so is $(\sqrt{2} + \sqrt{3})^2 = 5 + 2\sqrt{6}$, implying that $\sqrt{6}$ is rational. If $\alpha = \sqrt{2} + \sqrt{3}$ has degree 2, then 1, $\alpha$ and $\alpha^2$ must be linearly dependent over $\mathbb{Q}$. But $a + b\alpha + c\alpha^2 = 0$ is

$$(a + 5c) + b\sqrt{2} + b\sqrt{3} + 2c\sqrt{6} = 0$$

which implies $a = b = c = 0$ since 1, $\sqrt{2}$, $\sqrt{3}$, $\sqrt{6}$ are linearly independent over $\mathbb{Q}$. Therefore $\alpha$ has degree 4 over $\mathbb{Q}$, and $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$.

Since $\alpha$ has degree 4 over $\mathbb{Q}$ it’s enough to find a monic polynomial of degree 4 in $\mathbb{Q}[X]$ of which $\alpha$ is a root. In fact the characteristic polynomial of the map $\mathbb{Q}(\alpha) \to \mathbb{Q}(\alpha)$ given by $x \mapsto \alpha x$ is such a polynomial, and if we use the basis 1, $\sqrt{2}$, $\sqrt{3}$, $\sqrt{6}$ the matrix is

$$\begin{pmatrix}
0 & 2 & 3 & 0 \\
1 & 0 & 0 & 3 \\
1 & 0 & 0 & 2 \\
0 & 1 & 1 & 0
\end{pmatrix}$$

and the polynomial is

$$\Phi(X) = \begin{vmatrix}
-X & 2 & 3 & 0 \\
1 & -X & 0 & 3 \\
1 & 0 & -X & 2 \\
0 & 1 & 1 & -X
\end{vmatrix}.$$