Homework #01, due 1/20/10 = 9.1.2, 9.1.4, 9.1.6, 9.1.8, 9.2.3

Additional problems for study: 9.1.1, 9.1.3, 9.1.5, 9.1.13, 9.2.1, 9.2.2, 9.2.4, 9.2.5, 9.2.6, 9.3.2, 9.3.3

9.1.1 (This problem was not assigned except for study, but it’s useful for the next problem.) Let $p$ and $q$ be polynomials in $\mathbb{Z}[x, y, z]$, where

$p = p(x, y, z) = 2x^2y - 3xy^3z + 4y^2z^5$
$q = q(x, y, z) = 7x^2 + 5x^2y^3z^4 - 3x^2z^3$

(a) Write each of $p$ and $q$ as a polynomial in $x$ with coefficients in $\mathbb{Z}[y, z]$.

$p = (2y)x^2 - (3y^3z)x + 4y^2z^5$
$q = (7 + 5y^3z^4 - 3z^3)x^2$

(b) Find the degree of each of $p$ and $q$.

$\text{deg}(p) = 7 \quad \text{deg}(q) = 9$

(c) Find the degree of $p$ and $q$ in each of the three variables $x, y,$ and $z$.

$\text{deg}_x(p) = 2 \quad \text{deg}_x(q) = 2$
$\text{deg}_y(p) = 3 \quad \text{deg}_y(q) = 3$
$\text{deg}_z(p) = 5 \quad \text{deg}_z(q) = 4$

(d) Compute $pq$ and find the degree of $pq$ in each of the three variables $x, y,$ and $z$.

$pq = (2x^2y - 3xy^3z + 4y^2z^5)(7x^2 + 5x^2y^3z^4 - 3x^2z^3)$

$= 2x^2y(7x^2 + 5x^2y^3z^4 - 3x^2z^3)$
$- 3xy^3z(7x^2 + 5x^2y^3z^4 - 3x^2z^3)$
$+ 4y^2z^5(7x^2 + 5x^2y^3z^4 - 3x^2z^3)$

$= 2x^2y7x^2 + 2x^2y5x^2y^3z^4 - 2x^2y3x^2z^3$
$- 3xy^3z7x^2 - 3xy^3z5x^2y^3z^4 + 3xy^3z3x^2z^3$
\[ + 4y^2z^5x^2 + 4y^2z^5x^2y^3z^4 - 4y^2z^5x^2z^3 \]
\[ = 14x^4y + 10x^4y^4z^4 - 6x^4yz^3 \]
\[ - 21x^3y^3z - 15x^3y^6z^5 + 9x^3y^3z^4 \]
\[ + 28x^2y^2z^5 + 20x^2y^5z^9 - 12x^2y^2z^8 \]
\[ \deg_x(pq) = 2 + 2 = 4 \quad \deg_y(pq) = 3 + 3 = 6 \quad \deg_z(pq) = 5 + 4 = 9 \]

(e) Write \( pq \) as a polynomial in the variable \( z \) with coefficients in \( \mathbb{Z} \).
\[ pq = 14x^4y - (21x^3y^3)z - (6x^4y^3)z^3 + (10x^4y^4 + 9x^3y^3)z^4 \]
\[ + (28x^2y^2 - 15x^3y^6)z^5 - (12x^2y^2)z^8 + (20x^2y^5)z^9 \]

9.1.2 Repeat the preceding exercise under the assumption that the coefficients of \( p \) and \( q \) are in \( \mathbb{Z}/3\mathbb{Z} \). Let \( p \) and \( q \) be polynomials in \( \mathbb{Z}/3\mathbb{Z}[x, y, z] \), where
\[ p = p(x, y, z) = 2x^2y + y^2z^5 \]
\[ q = q(x, y, z) = x^2 + 2x^2y^3z^4 \]

(a) Write each of \( p \) and \( q \) as a polynomial in \( x \) with coefficients in \( \mathbb{Z}/3\mathbb{Z}[y, z] \).

We need only reduce the coefficients modulo 3, which gives us
\[ p = (\overline{2}y)x^2 + y^2z^5 \]
\[ q = (\overline{1} + \overline{2}y^3z^4)x^2 \]

(b) Find the degree of each of \( p \) and \( q \).
\[ \deg(p) = 7 \quad \deg(q) = 9 \]

(c) Find the degree of \( p \) and \( q \) in each of the three variables \( x \), \( y \), and \( z \).
\[ \deg_x(p) = 2 \quad \deg_x(q) = 2 \]
\[ \deg_y(p) = 2 \quad \deg_y(q) = 3 \]
\[ \deg_z(p) = 5 \quad \deg_z(q) = 4 \]
(d) Compute $pq$ and find the degree of $pq$ in each of the three variables $x$, $y$, and $z$.

$$pq = (2x^2y + y^2z^5)(x^2 + 2x^2y^3z^4)$$

$$= 2x^2y(x^2 + 2x^2y^3z^4) + y^2z^5(x^2 + 2x^2y^3z^4)$$

$$= 2x^2y(x^2) + 2x^2y(2x^2y^3z^4) + y^2z^5x^2 + y^2z^5(2x^2y^3z^4)$$

$$= 2x^4y + x^4y^4z^4 + x^2y^2z^5 + 2x^2y^5z^9$$

$$\deg_x(pq) = 2 + 2 = 4 \quad \deg_y(pq) = 3 + 3 = 6 \quad \deg_z(pq) = 5 + 4 = 9$$

(e) Write $pq$ as a polynomial in the variable $z$ with coefficients in $\mathbb{Z}/3\mathbb{Z}[x,y]$.

$$pq = 2x^4y + x^4y^4z^4 + x^2y^2z^5 + 2x^2y^5z^9$$

9.1.4 Prove that the ideals $(x)$ and $(x,y)$ are prime ideals in $\mathbb{Q}[x,y]$ but only the latter ideal is a maximal ideal.

To show $(x)$ is a prime ideal of $\mathbb{Q}[x,y]$, we must assume $pq \in (x)$, where $p,q \in \mathbb{Q}[x,y]$, and show that either $p \in (x)$ or $q \in (x)$. Suppose $p = a_n(y)x^n + \cdots + a_1(y)x + a_0(y)$ and $q = b_m(y)x^m + \cdots + b_1(y)x + b_0(y)$, where $a_n(y), \ldots, a_0(y), b_m(y), \ldots, b_0(y) \in \mathbb{Q}[y]$. Then $pq$ has exactly one term with $x$-degree 0, namely the polynomial $a_0(y)b_0(y) \in \mathbb{Q}[y]$.

From the assumption $pq \in (x)$ we know there is some polynomial $s \in \mathbb{Q}[x,y]$ such that $pq = sx$. Note that every (non-zero) term in $sx$ has $x$ as a factor, hence its $x$-degree is at least 1. Hence every nonzero term in $pq$ has degree at least 1. It therefore follows from $pq = sx$ that $a_0b_0 = 0$.

Now $\mathbb{Q}$ is an integral domain, hence $\mathbb{Q}[y]$ is also an integral domain by Prop. 9.2, so from $a_0b_0 = 0$ we conclude that either $a_0 = 0$ or $b_0 = 0$. If $a_0 = 0$ then every term of $p$ has $x$ as a factor, hence $p$ is equal to $x$ multiplied by some polynomial, so $p \in (x)$. Similarly, if $b_0 = 0$, then $q \in (x)$. This shows that $p$ or $q$ is in $(x)$, so $(x)$ is prime.
To show \((x, y)\) is a prime ideal of \(\mathbb{Q}[x, y]\), we must assume \(pq \in (x, y)\), where \(p, q \in \mathbb{Q}[x, y]\), and show that either \(p \in (x, y)\) or \(q \in (x, y)\). From \(pq \in (x, y)\) we get \(pq = sx + ty\) for some polynomials \(s, t \in \mathbb{Q}[x, y]\). This means that the constant term of \(pq\) is 0, because \(sx + ty\) is a polynomial in which every term either has \(x\) as a factor or has \(y\) as a factor. Let \(a_0 \in \mathbb{Q}\) be the constant term of \(p\) and let \(b_0 \in \mathbb{Q}\) be the constant term of \(q\). Then \(a_0 b_0 = 0\), so either \(a_0 = 0\) or \(b_0 = 0\). But if \(a_0 = 0\) then every term of \(p\) has either \(x\) or \(y\) (or both) as a factor, and this implies that \(p \in (x, y)\). Similarly, if \(b_0 = 0\) then \(q \in (x, y)\). This shows that \((x, y)\) is prime.

Define a function \(\varphi : \mathbb{Q} \to \mathbb{Q}[x, y]/(x, y)\) by \(\varphi(q) = q + (x, y)\) for every \(q \in \mathbb{Q}\). It is easy to show that \(\varphi\) preserves \(+\) and \(\cdot\) and is therefore a ring homomorphism. Note that \(\varphi\) sends each rational \(q\) to the set of polynomials in \(\mathbb{Q}[x, y]\) which have constant term equal to \(q\). Now every polynomial in \(\mathbb{Q}[x, y]\) has a constant term, so \(\varphi\) is onto. Furthermore, polynomials with distinct constant terms are distinct, so \(\varphi\) is injective. These considerations show that \(\mathbb{Q}[x, y]/(x, y)\) is isomorphic to \(\mathbb{Q}\). But \(\mathbb{Q}\) is a field, so the ideal \((x, y)\) is a maximal ideal by Prop. 7.12 (which says, if \(R\) a commutative ring then an ideal \(M\) is maximal if and only if \(R/M\) is a field).

One the other hand, \((x)\) is not a maximal ideal because (as we will show) it is a proper subset of the maximal ideal \((x, y)\). We have \((x) \subseteq (x, y)\) since \(\{x\} \subseteq \{x, y\}\). To show the inclusion is proper it is enough to note that \(y \in (x, y)\) but \(y \notin (x)\) because the \(x\)-degree of \(y\) is 0 but the \(x\)-degree of every polynomial in \((x)\) is at least 1 (and not 0).

9.1.6 Prove that \((x, y)\) is not a principal ideal in \(\mathbb{Q}[x, y]\).

Let us suppose, to the contrary, that \((x, y) = (p)\) for some polynomial \(p \in \mathbb{Q}[x, y]\). Then, since \(x, y \in (x, y) = (p)\), there are \(s, t \in \mathbb{Q}[x, y]\) such that \(x = sp\) and \(y = tp\). Then \(0 = \deg_y(x) = \deg_y(s) + \deg_y(p)\), so \(0 = \deg_y(p)\), and \(0 = \deg_x(y) = \deg_x(t) + \deg_x(p)\), so \(0 = \deg_x(p)\). From \(0 = \deg_y(p) = \deg_x(p)\) we get \(\deg(p) = 0\) and \(p \in \mathbb{Q}\). But \(p \in (x) = (x, y)\), so \(p = fx + gy\) for some \(f, g \in \mathbb{Q}[x, y]\), so \(\deg(p) = \deg(fx + gy) = \deg(fx) + \deg(gy) = \deg(f) + \deg(g)\).
\[
\min(\deg(f) + \deg(x), \deg(g) + \deg(y)) = \min(\deg(f) + 1, \deg(g) + 1) \geq 1,
\]
contradicting \( \deg(p) = 0 \).

**9.1.8** Let \( F \) be a field and let \( R = F[x, x^2 y, x^3 y^2, \ldots, x^n y^{n-1}, \ldots] \) be a subring of the polynomial ring \( F[x, y] \).

(a) Prove that the field of fractions of \( R \) and \( F[x, y] \) are the same.

Just as a review, we note that Th. 7.15 says, if \( R \) is a commutative ring, \( \emptyset \neq D \subseteq R, 0 \notin D, D \) is closed under \( \cdot \), and \( D \) contains no 0-divisors, then there is a *ring of quotients* \( Q = D^{-1}R \supseteq R \) such that

1. \( Q \) is a commutative ring with 1,
2. \( D \subseteq Q^\times \),
3. \( Q = \{ d^{-1}r | d \in D, r \in R \} \),
4. if \( D \) is a set of units in \( S \supseteq R \), a commutative ring with 1 extending \( R \), then \( Q \) is isomorphic to a subring \( Q' \) of \( S \) extending \( R \), i.e., \( Q \cong Q' \) and \( R \subseteq Q' \subseteq S \).

If \( R \) is an integral domain, then \( D = R - \{0\} \) has the needed properties and \( D^{-1}R \) is a field, called the *field of quotients* of \( R \).

If \( F \) is a field, then the polynomial ring \( F[x, y] \) is an integral domain, so \( F[x, y] \) has a field of fractions obtained by choosing \( D = F[x, y] - \{0\} \). Let \( Q_1 \) be the field of fractions of \( F[x, y] \). Then

\[
R = F[x, x^2 y, x^3 y^2, \ldots, x^n y^{n-1}, \ldots] \subseteq F[x, y] \subseteq Q_1 = D^{-1}F[x, y]
\]

By Th. 7.15, there is a subring \( Q_2 \) of \( Q_1 \) which is isomorphic to the field of quotients of \( R \), so

\[
R = F[x, x^2 y, x^3 y^2, \ldots, x^n y^{n-1}, \ldots] \subseteq Q_2 \subseteq Q_1
\]

and we need only show \( Q_1 \subseteq Q_2 \).

Note that \( x \in R \) so \( x \in Q_2 \). Also, \( 0 \neq x, x^2 y \in R \) so \( x, x^2 y \in Q_2 \), but \( x \) is a unit of \( Q_2 \), so \( y = (x^{-1})^2 x^2 y \in Q_2 \). From \( x, y \in Q_2 \) we get

\[
F[x, y] \subseteq Q_2.
\]
Consider an arbitrary element $d^{-1}p \in Q_1$, where $0 \neq d \in F[x,y]$ and $p \in F[x,y]$. Then $d, p \in Q_2$ and $d \neq 0$ and $Q_2$ is a field, so $pd^{-1} = \frac{p}{d} \in Q_2$. This shows $Q_1 \subseteq Q_2$, completing the proof that $Q_1 = Q_2$.

(b) Prove that $R$ contains an ideal that is not finitely generated.

For every $n \in \mathbb{Z}^+$ let $G_n := \{x, \ldots, x^ny^{n-1}\}$, and let $\langle G_n \rangle$ be the closure of $G_n$ under multiplication. Then a polynomial $f \in F[x,y]$ belongs to $\mathbb{F}[x,x^2y,x^3y^2,\ldots,x^ny^{n-1}]$ if and only if $f$ is a linear combination of a finite subset of $\langle G_n \rangle$, that is, there is a finite set of monomials $M \subseteq \langle G_n \rangle$ and a finite set of coefficients $\alpha_m \in F$, $m \in M$, such that $f = \sum_{m \in M} \alpha_m m$.

For every $f \in \mathbb{F}[x,y]$ let $r(f) = \deg_x(f) - \deg_y(f)$. Note that if $m \in G_n$ then $r(m) = 1$. If $f, g \in \mathbb{F}[x,y]$ then

$$r(fg) = \deg_x(fg) - \deg_y(fg) = \deg_x(f) + \deg_x(g) - (\deg_y(f) + \deg_y(g)) = \deg_x(f) - \deg_y(f) + \deg_x(g) - \deg_y(g) = r(f) + r(g)$$

Therefore, for every $m \in \langle G_n \rangle$, either $m \in G_n$ and $r(m) = 1$, or else $r(m) > 1$ (because $m$ is a nontrivial product of two or more monomials from $G_n$).

Claim $x^{n+1}y^n \notin \mathbb{F}[x,\ldots,x^ny^{n-1}]$.

Proof Suppose, to the contrary, that $x^{n+1}y^n \in \mathbb{F}[x,\ldots,x^ny^{n-1}]$. Then there is a finite set of monomials $M \subseteq \langle G_n \rangle$ and a finite set of coefficients $\alpha_m \in F$, $m \in M$, such that $x^{n+1}y^n = \sum_{m \in M} \alpha_m m$. Now two polynomials in $\mathbb{F}[x,y]$ are equal if and only if they have the same coefficients. In this case, this means that $x^{n+1}y^n$ is one of the monomials in $M$, say $x^{n+1}y^n = m \in M$, and its coefficient is $\alpha_m = 1$, and all the other coefficients are 0. Now $m \in M \subseteq \langle G_n \rangle$, but $r(m) = r(x^{n+1}y^n) = 1$, so in fact $m \in G_n$. However, this is a contradiction because $x^{n+1}y^n \notin G_n$. 
$R$ is an ideal of itself, so by the following claim $R$ contains an ideal (itself) that is not finitely generated.

Claim $R$ is not finitely generated.

Proof Suppose, to the contrary, that $G \subseteq R$ is a finite set of generators of $R$. Now $R$ is the union of a chain of subrings since

$$R = F[x, x^2y, \cdots , x^n y^{n-1}, \cdots ] = \bigcup_{n \in \mathbb{Z}^+} F[x, \cdots , x^n y^{n-1}].$$

Each element of $G$ is in one of the subrings $F[x, \cdots , x^n y^{n-1}] \subseteq R$, $n = 1, 2, 3, \cdots$. For each element of $G$, choose such a subring containing that element. There are only finitely many such subrings since $G$ is finite, and one of them, say $F[x, \cdots , x^N y^{N-1}]$ for some $N \in \mathbb{Z}^+$, contains all the others (because every finite subset of a linearly ordered set has a maximum element). Thus $G \subseteq F[x, \cdots , x^N y^{N-1}]$, so, since $G$ generates $R$, we have $R \subseteq F[x, \cdots , x^N y^{N-1}]$, but $F[x, \cdots , x^N y^{N-1}] \subseteq R$, so $F[x, \cdots , x^N y^{N-1}] = R$. We now have a contradiction since, by the claim above, $x^{N+1} y^N \notin F[x, \cdots , x^N y^{N-1}]$.

9.2.3 Let $f(x)$ be a polynomial in $F[x]$. Prove that $F[x]/(f(x))$ is a field if and only if $f(x)$ is irreducible. [Use Proposition 7, Section 8.2]

We note that Prop. 8.7 says, “Every nonzero prime ideal in a PID is maximal”. The proof actually shows that, in an integral domain, prime ideals are maximal among principal ideals. In a PID, all ideals are principal, so prime ideals are maximal.

We assume (although it is not explicitly mentioned in the text of the problem) that $F$ is a field. Then $F[x]$ is a Euclidean domain, hence $F[x]$ is a PID, so by Prop. 8.7, prime ideals in $F[x]$ are maximal. Prop. 7.14 says that, in a commutative ring, every maximal ideal is prime. Therefore,

(1) in $F[x]$ an ideal is prime if and only if it is maximal.
Now complete the proof as follows—

\[ F[x]/(f(x)) \] is a field

\[ \iff (f(x)) \text{ is a maximal ideal of } F[x] \quad \text{Prop. 7.12, below} \]

\[ \iff (f(x)) \text{ is a prime ideal of } F[x] \quad \text{see (1) above} \]

\[ \iff f(x) \text{ is prime in } F[x] \quad \text{Def. (2), p. 284} \]

\[ \iff f(x) \text{ is irreducible in } F[x] \quad \text{Prop. 8.11, below} \]

Prop. 7.12 says, “If \( R \) is a commutative ring then an ideal \( M \) is maximal if and only if \( R/M \) is a field.” Prop. 8.11 says, “In a PID a nonzero element is a prime if and only if it is irreducible.”

---

Homework #02, due 1/27/10 = 9.4.1, 9.4.2, 9.4.5, 9.4.6, 9.4.7.

Additional problems recommended for study: 9.4.4, 9.4.9, 9.4.11, 9.4.13, 9.4.17

9.4.1 Determine whether the following polynomials are irreducible in the rings indicated. For those that are reducible, determine their factorization into irreducibles. The notation \( \mathbb{F}_p \) denotes the finite field \( \mathbb{Z}/p\mathbb{Z} \), \( p \) a prime.

9.4.1(a) \( x^2 + x + 1 \) in \( \mathbb{F}_2[x] \)

By Prop. 9.10 the quadratic polynomial \( p(x) = x^2 + x + 1 \) is irreducible in \( \mathbb{F}_2[x] \) if and only if \( p(x) \) has no root in \( \mathbb{F}_2 \). This we check by substituting all the elements of the field \( \mathbb{F}_2 \) (there are only 0 and 1) into \( p(x) \) and calculating the result \textit{modulo} 2, as follows: \( p(0) = 0^2 + 0 + 1 = 1 \neq 0 \) and \( p(1) = 1^2 + 1 + 1 = 1 + 1 + 1 = 1 \neq 0 \). Since \( p(x) \) has no roots in \( \mathbb{F}_2 \), \( p(x) \) is irreducible.

9.4.1(b) \( x^3 + x + 1 \) in \( \mathbb{F}_3[x] \).

By Prop. 9.10 the cubic polynomial \( q(x) = x^3 + x + 1 \) is irreducible in \( \mathbb{F}_3[x] \) if and only if \( p(x) \) has no root in \( \mathbb{F}_3 \). This we check by substituting all the elements of the field \( \mathbb{F}_3 \) (there are only 0, 1, and 2) into \( p(x) \) and calculating the result \textit{modulo} 3, as follows: \( p(0) = 0^3 + 0 + 1 = 1 \neq 0 \),
\( p(1) = 1^3 + 1 + 1 = 1 + 1 + 1 = 0, \) and \( p(2) = 2^3 + 2 + 1 = 8 + 2 + 1 = 11 \neq 0. \) Since \( p(x) \) has root 1 in \( \mathbb{F}_2, \) \( p(x) \) has linear factor \( x - 1 \) and factorization \( p(x) = (x - 1)(x^2 + x - 1) = (x + 2)(x^2 + x + 2) \) (note \(-1 = 2 \mod 3\)).

**9.4.1(c)** \( x^4 + 1 \) in \( \mathbb{F}_5[x]. \)

Let \( p(x) = x^4 + 1. \) By Prop. 9.10 we can show that \( p(x) \) has no linear factor by substituting the elements 0, 1, 2, 3, 4 of \( \mathbb{F}_5 \) in \( p(x) \) and calculating modulo 5: \( p(0) = 1 \neq 0, \) \( p(1) = 1^4 + 1 = 2 \neq 0, \) \( p(2) = 2^4 + 1 = 17 = 2 \neq 0, \) \( p(3) = 3^4 + 1 = 82 = 2 \neq 0, \) and \( p(4) = 4^4 + 1 = 256 + 1 = 257 = 2 \neq 0. \) It remains to consider factorizations into monic quadratic polynomials.

Suppose \( p(x) = (x^2 + ax + b)(x^2 + cx + d) \) where \( a, b, c, d \in \mathbb{F}_5. \) Then
\[
x^4 + 1 = p(x) = x^4 + (a + c)x^3 + (b + ac + d)x^2 + (ad + bc)x + bd
\]
so \( 0 = a + c, 0 = b + ac + d, 0 = ad + bc, \) and \( 1 = bd. \) From \( 0 = a + c \) we have \( c = -a, \) so \( 0 = b + a(-a) + d \) and \( 0 = ad + b(-a), \) so \( a^2 = b + d \) and \( ab = ad. \)

If \( a \neq 0 \) then \( b = d \) by cancellation from \( ad = ab, \) so \( a^2 = 2b \) and \( b^2 = 1 \) from \( a^2 = b + d \) and \( 1 = bd. \) Now \( 1^2 = 1, 2^2 = 4, 3^2 = 9 = 4, \) \( 4^2 = 1, \) so \( b \) is 1 or 4. But then either \( a^2 = 2 \) or \( a^2 = 2(4) = 8 = 3, \) and neither of these equations has a solution in \( \mathbb{F}_5 \) (since \( 1^2 = 1, 2^2 = 4, 3^2 = 4, 4^2 = 1). \) On the other hand, if \( a = 0 \) then \( 0^2 = 0 = b + d, \) so \( b = -d, \) so \( b^2 = -bd = -1 = 4, \) so \( b = 2, d = -2, a = 0, c = 0, \) giving a factorization
\[
p(x) = x^4 + 1 = (x^2 + 2)(x^2 - 2) = (x^2 + 2)(x^2 + 3).
\]
Thus \( p(x) \) is a reducible polynomial in \( \mathbb{F}_5[x]. \)

**9.4.1(d)** \( x^4 + 10x^2 + 1 \) in \( \mathbb{Z}[x]. \)

This polynomial has no real-valued roots, since \( x^4 \geq 0 \) and \( x^2 \geq 0 \) for all \( x \in \mathbb{R}, \) hence \( x^4 + 10x^2 + 1 \geq 1 \) for all \( x \in \mathbb{R}. \) This shows, by Prop. 9.10, that \( x^4 + 10x^2 + 1 \) has no linear factors in \( \mathbb{Z}[x]. \) We consider factoring \( x^4 + 10x^2 + 1 \) into quadratic polynomials. If \( a, b, c, d \in \mathbb{Z} \) and
\[
x^4 + 10x^2 + 1 = (x^2 + ax + b)(x^2 + cx + d)
\]
\[ = x^4 + (a + c)x^3 + (b + ac + d)x^2 + (ad + bc)x + bd \]

then \( 0 = a + c, b + ac + d = 10, ad + bc = 0, \) and \( bd = 1. \) From \( 0 = a + c \)
we get \( c = -a, \) so, by \( ad + bc = 0 \) we have \( ad - ab = 0, \) hence \( a = 0 \) or \( d = b. \)

If \( a = 0 \) then \( c = 0 \) and the factorization becomes

\[ x^4 + 10x^2 + 1 = (x^2 + b)(x^2 + d) = x^4 + (b + d)x^2 + bd \]

so \( b + d = 10 \) and \( bd = 1. \) These equations have no solution in \( \mathbb{Z}. \)
Indeed, we have either \( b = d = 1 \) or \( b = d = -1 \) by \( bd = 1, \) and neither choice satisfies the equation \( b + d = 10. \)

If \( a \neq 0 \) then \( b = d \) and the factorization becomes

\[ x^4 + 10x^2 + 1 = (x^2 + ax + b)(x^2 - ax + b) \]

\[ = x^4 + (2b - a^2)x^2 + b^2 \]

where \( 2b = a^2 + 10 \) and \( b^2 = 1. \) From \( 2b = a^2 + 10 \geq 10 \) we get \( b \geq 5, \)
but from \( b^2 = 1 \) we get \( b = \pm 1, \) a contradiction. Thus there is no factorization into quadratic factors, and \( x^4 + 10x^2 + 1 \) is irreducible over \( \mathbb{Z}[x]. \)

---

**9.4.2** Prove that the following polynomials are irreducible in \( \mathbb{Z}[x]. \)

**9.4.2(a)** \( x^4 - 4x^3 + 6 \)

This polynomial is irreducible by Eisenstein’s Criterion, since the prime \( 2 \) does not divide the leading coefficient, does divide all the coefficients of the low order terms, namely \(-4, 0, 0, \) and \( 6, \) but the square of \( 2 \) does not divide the constant \( 6. \)

**9.4.2(b)** \( x^6 + 30x^5 - 15x^3 + 6x - 120 \)

The coefficients of the low order terms are \( 30, 0, -15, 0, 6, \) and \(-120. \) These numbers are divisible by the prime \( 3, \) but \( 3^2 = 9 \) does not divide \(-120 = -2^3 \cdot 3 \cdot 5, \) so the polynomial is irreducible by Eisenstein’s Criterion.

**9.4.2(c)** \( x^4 + 6x^3 + 4x^2 + 2x + 1 \) [Substitute \( x - 1 \) for \( x. \)]
Let \( p(x) = x^4 + 6x^3 + 4x^2 + 2x + 1 \). Then to calculate \( p(x - 1) \) we first note that
\[
\begin{align*}
(x - 1)^4 &= x^4 - 4x^3 + 6x^2 - 4x + 1 \\
6(x - 1)^3 &= 6x^3 - 18x^2 + 18x - 6 \\
4(x - 1)^2 &= 4x^2 - 8x + 4 \\
2(x - 1) &= 2x - 2 \\
1 &= 1
\end{align*}
\]
Then we add these up and get
\[
p(x - 1) = (x - 1)^4 + 6(x - 1)^3 + 4(x - 1)^2 + 2(x - 1) + 1 \\
= x^4 + 2x^3 - 8x^2 + 8x - 2
\]
Now \( x^4 + 2x^3 - 8x^2 + 8x - 2 \) is irreducible by Eisenstein’s Criterion, since the prime 2 divides all the lower order coefficients, but \( 2^2 = 4 \) does not divide the constant \(-2\). Any factorization of \( p(x) \) would provide a factorization of \( p(x - 1) \) as well, since if \( p(x) = a(x)b(x) \) then \( x^4 + 2x^3 - 8x^2 + 8x - 2 = p(x - 1) = a(x - 1)b(x - 1) \), contradicting the irreducibility of \( p(x - 1) \). Therefore \( p(x) \) is itself irreducible in \( \mathbb{Z}[x] \).

**9.4.2(d)** \( \frac{(x+2)^p-2^p}{x} \), where \( p \) is an odd prime, in \( \mathbb{Z}[x] \).

To express \( \frac{(x+2)^p-2^p}{x} \) as a polynomial we expand \( (x + 2)^p \) according to the binomial theorem. The final constant \( 2^p \) cancels with \( -2^p \), so every remaining term has \( x \) as a factor, which we cancel, leaving
\[
x^{p-1} + 2 \binom{p}{1} x^{p-2} + 2^2 \binom{p}{2} x^{p-3} + \cdots + 2^{p-1} \binom{p}{p-1}
\]
Every lower order coefficient in this polynomial has the form
\[
2^k \binom{p}{k} x^{p-k-1} = 2^k \cdot p \cdot (p - 1) \cdots (p - k - 1)
\]
with \( 0 < k < p \). Each lower order coefficient has \( p \) as a factor but does not have \( p^2 \) as a factor, so the polynomial is irreducible by Eisenstein’s Criterion.
9.4.5 Find all the monic irreducible polynomials of degree \( \leq 3 \) in \( \mathbb{F}_2[x] \), and the same in \( \mathbb{F}_3[x] \).

All the monic linear (degree 1) polynomials \( x - a \) are irreducible. For \( \mathbb{F}_2 \) these irreducible linear polynomials are \( x \) and \( x - 1(= x + 1) \). For \( \mathbb{F}_3 \) these irreducible linear polynomials are \( x, x - 1(= x + 2) \), and \( x - 2(= x + 1) \).

In \( \mathbb{F}_2[x] \) the only (monic) quadratic polynomials are \( x^2, x^2 + 1, x^2 + x, \) and \( x^2 + x + 1 \). Obviously, \( x^2 \) and \( x^2 + x \) are reducible since \( x^2 = xx \) and \( x^2 + x = x(x + 1) \). Less obviously, \( x^2 + 1 \) has 1 as a root, which leads to the factorization \( x^2 + 1 = (x + 1)(x + 1) \). Finally, \( x^2 + x + 1 \) has no root in \( \mathbb{F}_2 \) since \( 1^2 + 1 + 1 = 1 \neq 0 \) and \( 0^2 + 0 + 1 = 1 \neq 0 \), so, because it is quadratic, it is irreducible.

In \( \mathbb{F}_3[x] \) the nine monic quadratic polynomials are \( x^2, x^2 + 1, x^2 + 2, x^2 + x, x^2 + 2x, x^2 + x + 1, x^2 + 2x + 1, x^2 + x + 2, \) and \( x^2 + 2x + 2 \). Obviously, \( x^2, x^2 + x, \) and \( x^2 + 2x \) are reducible. Since the remaining polynomials \( x^2 + 1, x^2 + 2, x^2 + x + 1, x^2 + 2x + 1, x^2 + x + 2, \) and \( x^2 + 2x + 2 \) are quadratic, they are reducible if and only if they have a root in \( \mathbb{F}_3 \), so we check each of them for roots:

\[
\begin{array}{cccc}
x^2 + 1 & 0^2 + 1 = 1 & 1^2 + 1 = 2 & 2^2 + 1 = 2 \\
x^2 + 2 & 0^2 + 2 = 2 & 1^2 + 2 = 0 & 2^2 + 2 = 0 \\
x^2 + x + 1 & 0^2 + 0 + 1 = 1 & 1^2 + 1 + 1 = 0 & 2^2 + 2 + 1 = 1 \\
x^2 + 2x + 1 & 0^2 + 2 \cdot 0 + 1 = 1 & 1^2 + 2 \cdot 1 + 1 = 1 & 2^2 + 2 \cdot 2 + 1 = 0 \\
x^2 + x + 2 & 0^2 + 0 + 2 = 2 & 1^2 + 1 + 2 = 1 & 2^2 + 2 + 2 = 2 \\
x^2 + 2x + 2 & 0^2 + 2 \cdot 0 + 2 = 2 & 1^2 + 2 \cdot 1 + 2 = 2 & 2^2 + 2 \cdot 2 + 2 = 1 \\
\end{array}
\]

Since \( x^2 + 2 \) has 1 and 2 as roots, we get the factorization \( x^2 + 2 = (x - 1)(x - 2) = (x + 2)(x + 1) \). Since \( x^2 + x + 1 \) has 1 as a (multiple) root, we get a factorization \( x^2 + x + 1 = (x - 1)(x - 1) = (x + 2)(x + 2) \). Finally, \( x + 2x + 1 = (x + 1)(x + 1) \). The remaining polynomials, which are the only irreducible quadratic polynomials in \( \mathbb{F}_3[x] \), are \( x^2 + 1 \) (used below), \( x^2 + x + 2 \), and \( x^2 + 2x + 2 \).

There are quite a few monic cubic polynomials, so I thought it best to write some code in GAP to do the computations. The following GAP
code computes, counts, and prints the irreducible cubic polynomials over the field $\mathbb{F}_p$, for $p$ ranging over the first 12 primes.

```
irrcubic:=function(p)
local f,c,t,roots,irr;
  f:=function(c,p)
  end;
  t:=Tuples([0..p-1],4);
  roots:=Set(Filtered(t,c->f(c,p)=0),c->[1..3]);
  irr:=Difference(Tuples([0..p-1],3),roots);
  Print("The number of irreducible monic cubic ");
  Print("polynomials over F_","p"," is\t",Size(irr));
  # Print("The irreducible monic cubic ");
  # Print("polynomials over F_","p"," are\n");
  # for c in irr do
  #   # if c[1]=1 then Print(" + x^2");fi;
  #   # if c[1] in [2..p-1] then Print(" + ",c[1],"x^2");fi;
  #   # if c[2]=1 then Print(" + x");fi;
  #   # if c[2] in [2..p-1] then Print(" + ",c[2],"x");fi;
  #   # if c[3]=1 then Print(" + 1");fi;
  #   # if c[3] in [2..p-1] then Print(" + ",c[3]);fi;
  #   Print("\n");
  # od;
  Print("\n");
  return irr;
end;
LogTo("roots.output");
for p in Primes{[1..12]} do
  irrcubic(p);
od;
```

Running the GAP code without printing the polynomials produces the data in the following table, which shows the number $n_p$ of irreducible
monic cubic polynomials over $\mathbb{F}_p$ for the first 12 primes.

<table>
<thead>
<tr>
<th>$p$</th>
<th>2</th>
<th>3</th>
<th>5</th>
<th>7</th>
<th>11</th>
<th>13</th>
<th>17</th>
<th>19</th>
<th>23</th>
<th>29</th>
<th>31</th>
<th>37</th>
</tr>
</thead>
<tbody>
<tr>
<td>$n_p$</td>
<td>2</td>
<td>8</td>
<td>40</td>
<td>112</td>
<td>440</td>
<td>728</td>
<td>1632</td>
<td>2280</td>
<td>4048</td>
<td>8120</td>
<td>9920</td>
<td>16872</td>
</tr>
</tbody>
</table>

By uncommenting the Print commands we get lists of irreducible monic cubic polynomials. The 2 irreducible monic cubic polynomials in $\mathbb{F}_2[x]$ are

$$x^3 + x + 1 \quad x^3 + x^2 + 1$$

The 8 irreducible monic cubic polynomials over $\mathbb{F}_3[x]$ are

$$x^3 + 2x + 1 \quad x^3 + x^2 + 2x + 1$$
$$x^3 + 2x + 2 \quad x^3 + 2x^2 + 1$$
$$x^3 + x^2 + 2 \quad x^3 + 2x^2 + x + 1$$
$$x^3 + x^2 + x + 2 \quad x^3 + 2x^2 + 2x + 2$$

The 40 irreducible monic cubic polynomials over $\mathbb{F}_5$ are

$$x^3 + x + 1 \quad x^3 + 2x^2 + 2x + 2$$
$$x^3 + x + 4 \quad x^3 + 2x^2 + 2x + 3$$
$$x^3 + 2x + 1 \quad x^3 + 2x^2 + 4x + 2$$
$$x^3 + 2x + 4 \quad x^3 + 2x^2 + 4x + 4$$
$$x^3 + 3x + 2 \quad x^3 + 3x^2 + 2$$
$$x^3 + 3x + 3 \quad x^3 + 3x^2 + 4$$
$$x^3 + 4x + 2 \quad x^3 + 3x^2 + x + 1$$
$$x^3 + 4x + 3 \quad x^3 + 3x^2 + x + 2$$
$$x^3 + x^2 + 1 \quad x^3 + 3x^2 + 2x + 2$$
$$x^3 + x^2 + 2 \quad x^3 + 3x^2 + 2x + 3$$
$$x^3 + x^2 + x + 3 \quad x^3 + 3x^2 + 4x + 1$$
$$x^3 + x^2 + x + 4 \quad x^3 + 3x^2 + 4x + 3$$
$$x^3 + x^2 + 3x + 1 \quad x^3 + 4x^2 + 3$$
9.4.6 Construct fields of each of the following orders: (a) 9, (b) 49, (c) 8, (d) 81. (you may exhibit these as \( F[x]/(f(x)) \) for some \( F \) and \( f \)). [Use Exercises 2 and 3 in Section 2.]

By Exer. 9.2.3, \( F[x]/(f(x)) \) is a field when \( f \in F[x] \) is irreducible, and by Exer. 9.2.2, \( F[x]/(f(x)) \) has \( q^n \) elements if \( |F| = q \) and \( \deg(f) = n \).

(a) To get a field of order 9, we choose \( F = \mathbb{F}_3 \) so that \( q = |\mathbb{F}_3| = 3 \), and we choose an irreducible quadratic, so that \( n = 2 \) and the order of the field \( F[x]/(f(x)) \) is \( q^n = 3^2 = 9 \), as desired. For \( f \) we may use \( x^2 + 1 \), which is an irreducible quadratic polynomial in \( \mathbb{F}_3[x] \) by Exer. 9.4.5, solved above.

(b) To get a field of order 49, we choose \( F = \mathbb{F}_7 \) so that \( q = |\mathbb{F}_7| = 7 \), and we let \( f \) be any irreducible quadratic in \( \mathbb{F}_7[x] \). Then \( n = 2 \) and the order of the field \( F[x]/(f(x)) \) is \( q^n = 7^2 = 49 \). One choice that works is \( f(x) = x^2 + 1 \). By the way, the quadratic irreducible polynomials in \( \mathbb{F}_7[x] \) are

\[
\begin{align*}
\text{9.4.6} & \quad \text{Construct fields of each of the following orders: (a) 9, (b) 49, (c) 8, (d) 81. (you may exhibit these as } F[x]/(f(x)) \text{ for some } F \text{ and } f. \text{[Use Exercises 2 and 3 in Section 2.]} \\
& \quad \text{By Exer. 9.2.3, } F[x]/(f(x)) \text{ is a field when } f \in F[x] \text{ is irreducible, and by Exer. 9.2.2, } F[x]/(f(x)) \text{ has } q^n \text{ elements if } |F| = q \text{ and } \deg(f) = n. \\
& \quad \text{(a) To get a field of order 9, we choose } F = \mathbb{F}_3 \text{ so that } q = |\mathbb{F}_3| = 3, \text{ and we choose an irreducible quadratic, so that } n = 2 \text{ and the order of the field } F[x]/(f(x)) \text{ is } q^n = 3^2 = 9, \text{ as desired. For } f \text{ we may use } x^2 + 1, \text{ which is an irreducible quadratic polynomial in } \mathbb{F}_3[x] \text{ by Exer. 9.4.5, solved above.} \\
& \quad \text{(b) To get a field of order 49, we choose } F = \mathbb{F}_7 \text{ so that } q = |\mathbb{F}_7| = 7, \text{ and we let } f \text{ be any irreducible quadratic in } \mathbb{F}_7[x]. \text{ Then } n = 2 \text{ and the order of the field } F[x]/(f(x)) \text{ is } q^n = 7^2 = 49. \text{ One choice that works is } f(x) = x^2 + 1. \text{ By the way, the quadratic irreducible polynomials in } \mathbb{F}_7[x] \text{ are} \\
\end{align*}
\]
\[ \begin{align*}
&x^2 + 4x + 1 & x^2 + 4x + 5 & x^2 + 4x + 6 \\
x^2 + 5x + 2 & x^2 + 5x + 3 & x^2 + 5x + 5 \\
x^2 + 6x + 3 & x^2 + 6x + 4 & x^2 + 6x + 6 \\
\end{align*} \]

(c) To get a field of order 8, we choose \( F = \mathbb{F}_2 \) so that \( q = |\mathbb{F}_2| = 2 \), and we choose an irreducible cubic polynomial \( f \) in \( \mathbb{F}_2[x] \), so that \( n = 3 \) and the order of the field \( F[x]/(f(x)) \) is \( q^n = 2^3 = 8 \). For \( f \) we may use \( x^3 + x + 1 \) or \( x^3 + x^2 + 1 \) (the two irreducible monic cubics in \( \mathbb{F}_2[x] \), as shown above).

(d) To get a field of order 81, we choose \( F = \mathbb{F}_3 \) so that \( q = |\mathbb{F}_3| = 3 \), and we choose an irreducible quartic polynomial \( f \) in \( \mathbb{F}_3[x] \), so that \( n = 4 \) and the order of the field \( F[x]/(f(x)) \) is \( q^n = 3^4 = 81 \). Let \( f(x) = x^4 + x + 2 \). Then \( f \) has no linear factors because it has no roots in \( \mathbb{F}_3 \), since \( 0^4 + 0 + 2 = 2, 1^4 + 1 + 2 = 1, \) and \( 2^4 + 2 + 2 = 2 \).

Suppose \( f(x) = (x^2 + ax + b)(x^2 + cx + d) \) where \( a, b, c, d \in \mathbb{F}_3 \). Then

\[ x^4 + x + 2 = x^4 + (a + c)x^3 + (b + ac + d)x^2 + (ad + bc)x + bd, \]

which implies that \( 0 = a + c, 0 = b + ac + d, 1 = ad + bc, \) and \( 2 = bd \). From \( 0 = a + c \) we have \( c = -a \). Substituting \(-a\) for \( c \) in the equations

\[ 0 = b + ac + d \text{ and } 1 = ad + bc \]

(and simplifying) yields \( a^2 = b + d \) and \( 1 = a(d - b) \). By the latter equation, \( a = a^2(d - b) \), so by \( a^2 = b + d \)

we have \( a = (d - b)(b + d) = d^2 - b^2 \). From \( bd = 1 \) we know \( b \neq 0 \) and \( d \neq 0 \). The only nonzero element that is a square in \( \mathbb{F}_3 \) is 1, since \( 1^2 = 1 \) and \( 2^2 = 1 \) in \( \mathbb{F}_3 \). Therefore \( a = b^2 - d^2 = 1 - 1 = 0 \), but then \( 1 = a(d - b) = 0(d - b) = 0 \), a contradiction. This shows that \( f \) is actually irreducible, so \( \mathbb{F}_3[x]/(f) \) is a field with 81 elements in it.

\[ \textbf{9.4.7} \] Show that \( \mathbb{R}[x]/(x^2 + 1) \) is isomorphic to the field of complex numbers.

Let \( p(x) = x^2 + 1 \) and let \( P = (x^2 + 1) \) be the principal ideal of \( \mathbb{R}[x] \) generated by \( p(x) \). Obviously \( p(x) \) has no real roots since, for every \( r \in \mathbb{R} \), \( r^2 + 1 \geq 1 \). Since \( p(x) \) is quadratic and has no real roots, \( p(x) \) is irreducible in \( \mathbb{R}[x] \) by Prop. \textbf{9.10}. Therefore \( \mathbb{R}[x]/P \) is a field by Exer. \textbf{9.2.3} (or the upcoming Prop. \textbf{9.15}). The element \( \pi = x + P \in \mathbb{R}[x]/P \) is a solution to \( x^2 = -1 \) and plays the same role
as the imaginary $i = \sqrt{-1}$ in $\mathbb{C}$, because $x^2 = (x + P)^2 = x^2 + P = x^2 - (x^2 + 1) + P = -1 + P$.

The elements of $\mathbb{R}[x]/P$ are cosets of the form $a + bx + P$, $a, b \in \mathbb{R}$. Define a map $\varphi : \mathbb{R}[x]/P \to \mathbb{C}$ by $\varphi(a + bx + P) = a + b\sqrt{-1}$. To show $\varphi$ is well-defined, let us assume that $a + bx + P = c + dx + P$ for some $a, b, c, d \in \mathbb{R}$. Then $a - c + (b - d)x \in P$, hence $a - c + (b - d)x = p(x)q(x)$ for some $q(x) \in \mathbb{R}[x]$. If $b - d \neq 0$ then

$$1 = \deg(a - c + (b - d)x) = \deg(p(x)q(x))$$
$$= \deg(p(x)) + \deg(q(x)) = 2 + \deg(q(x)) \geq 2,$$

a contradiction, so $b = d$. But then $a - c \in P$, hence $a - c = p(x)q'(x)$ for some $q'(x) \in \mathbb{R}[x]$. If $a - c \neq 0$ then $0 = \deg(a - c) = \deg(p(x)q'(x)) = \deg(p(x)) + \deg(q'(x)) = 2 + \deg(q'(x)) \geq 2$, a contradiction, so $a = c$. Thus, each element of $\mathbb{R}[x]/P$ has the form $a + bx + P$ for uniquely determined reals $a, b \in \mathbb{R}$. Next are calculations that show $\varphi$ is a ring homomorphism because it preserves differences and products.

$$\varphi((a + bx + P) - (c + dx + P))$$
$$= \varphi((a - c) + (b - d)x + P)$$
$$= (a - c) + (b - d)\sqrt{-1}$$
$$= (a + b\sqrt{-1}) - (c + d\sqrt{-1})$$
$$= \varphi(a + bx + P) - \varphi(c + dx + P)$$
$$\varphi((a + bx + P)(c + dx + P))$$
$$= \varphi((a + bx)(c + dx) + P)$$
$$= \varphi(ac + (ad + bc)x + bdx^2 + P)$$
$$= \varphi(ac + (ad + bc)x + bdx^2 + (-bd)(x^2 + 1) + P)$$
$$= \varphi(ac + (ad + bc)x + bdx^2 - bdx^2 - bd + P)$$
$$= \varphi(ac - bd + (ad + bc)x + P)$$
$$= ac - bd + (ad + bc)\sqrt{-1}$$
$$= ac + (ad + bc)\sqrt{-1} + bd(\sqrt{-1})^2$$
Finally, to see that $\varphi$ is injective, we note that kernel of $\varphi$ is trivial since if $\varphi(a + bx + P) = 0$ then $a + b\sqrt{-1} = 0$, hence $a = b = 0$, so $a + bx + P = P = 0 \in \mathbb{R}[x]/P$.

---

**Homework #03**, due 2/3/10 = 9.4.3, 9.4.8, 9.4.14, 9.4.18 (use 9.4.17), 9.5.2.

Additional problems recommended for study: 9.4.10, 9.4.12, 9.4.16, 9.4.20, 9.5.1, 9.5.3, 9.5.4, 9.5.7

**9.4.3** Show that the polynomial $(x - 1)(x - 2) \cdots (x - n) - 1$ is irreducible over $\mathbb{Z}[n]$ for all $n \geq 1$. [If the polynomial factors consider the values of the factors at $x = 1, 2, \ldots, n$.]

Let $p(x) = (x-1)(x-2) \cdots (x-n)-1$. To show that $p(x)$ is irreducible in $\mathbb{Z}[x]$ for all $n \geq 1$, we assume $p(x) = a(x)b(x)$ for some (wlog monic) polynomials $a(x), b(x) \in \mathbb{Z}[x]$, and we will show this factorization is trivial.

For all $k \in \{1, \cdots , n\}$ we have $p(k) = -1 = a(k)b(k)$ so, since $a(k)$ and $b(k)$ are integers, they both must be 1 or $-1$, and they can’t have the same sign, so $a(x) \neq b(x)$. Thus we have $1 = (a(k))^2 = (b(k))^2$ for all $k \in \{1, \cdots , n\}$. Since deg($p$) = $n$ = deg($a(x)$) + deg($b(x)$), the degrees of $a(x)$ and $b(x)$ cannot both be strictly larger than $\frac{n}{2}$, so we may assume one of them has degree no more than $\frac{n}{2}$. We assume wlog that deg($a(x)$) $\leq \frac{n}{2}$, hence deg($a^2(x)$) $\leq n$. Therefore $p(x) + a^2(x)$ is a polynomial of degree $n$ that has roots 1, $\cdots$, $n$. These are distinct roots, so by Prop. 9.9 $p(x) + a^2(x)$ has $n$ distinct linear factors $x-1, x-2, \ldots, x-n$. Now $p(x) + a^2(x)$ has factor $x-1$, so $p(x) + a^2(x) = (x-1)q_1(x)$ for some $q_1(x) \in \mathbb{Z}[x]$, but $p(x) + a^2(x)$ has roots 2, $\cdots$, $n$ and these aren’t roots of $x-1$, so they’re roots of $q_1(x)$, so $q_1(x)$ has a linear factor $x-2$, hence $q_1(x) = (x-2)q_2(x)$, and so on. Thus

$$p(x) + a^2(x) = (x-1)q_1(x)$$
\[ (x - 1)(x - 2)q_2(x) = \cdots = (x - 1)(x - 2) \cdots (x - n) = p(x) + 1 \]

Note the final equation gives \( a^2(x) = 1 \), so the degree of \( a^2(x) \) is actually 0, hence \( a(x) \) is a constant in \( \mathbb{Z} \) whose square is 1, so \( a(x) = \pm 1 \) and \( p(x) = \mp b(x) \). Therefore the factorization is trivial.

**9.4.8** Prove that \( K_1 = \mathbb{F}_{11}[x]/(x^2 + 1) \) and \( K_2 = \mathbb{F}_{11}/(y^2 + 2y + 2) \) are both fields with 121 elements. Prove that the map which sends the element \( p(\overline{x}) \) of \( K_1 \) to the element \( p(\overline{y} + 1) \) of \( K_2 \) (where \( p \) is any polynomial with coefficients in \( \mathbb{F}_{11} \)) is well-defined and gives a ring (hence field) isomorphism from \( K_1 \) onto \( K_2 \).

First we note that \( x^2 + 1 \) is quadratic and has no roots in the ground field \( \mathbb{F}_{11} \) since, calculating modulo 11, we have

\[
\begin{align*}
(0)^2 + 1 &= 1 \\
(1)^2 + 1 &= 2 \\
(2)^2 + 1 &= 5 \\
(3)^2 + 1 &= 10 \\
(4)^2 + 1 &= 6 \\
(5)^2 + 1 &= 2 \\
(6)^2 + 1 &= 4 \\
(7)^2 + 1 &= 6 \\
(8)^2 + 1 &= 10 \\
(9)^2 + 1 &= 5 \\
(10)^2 + 1 &= 2 
\end{align*}
\]

It follows by Prop. 9.10 that \( x^2 + 1 \) is irreducible in \( \mathbb{F}_{11}[x] \). The elements of the quotient field \( K_1 = \mathbb{F}_{11}[x]/(x^2 + 1) \) are \( ax + b + P \), where \( P = (x^2 + 1) \) and \( a, b \in \mathbb{F}_{11} \).

By Exer. 9.2.3, \( F[x]/(f(x)) \) is a field when \( f \in F[x] \) is irreducible, and by Exer. 9.2.2, \( F[x]/(f(x)) \) has \( q^n \) elements if \( |F| = q \) and \( \deg(f) = n \). In this case we have \( F = \mathbb{F}_{11} \) so \( q = 11 \), and \( f(x) = x^2 + 1 \) so \( n = 2 \), and the number of elements in \( K_1 \) is therefore \( q^n = 11^2 = 121 \). (Part of the proof goes like this: if \( a + bx + P = c + dx + P \) for some \( a, b, c, d \in \mathbb{F}_{11} \), then \( a - c + (b - d)x \in P \), hence \( a - c + (b - d)x = p(x)q(x) \) for some \( q(x) \in \mathbb{F}_{11}[x] \). If \( b - d \neq 0 \) then

\[
1 = \deg(a - c + (b - d)x) = \deg(p(x)q(x)) = \deg(p(x)) + \deg(q(x)) = 2 + \deg(q(x)) \geq 2,
\]
a contradiction, so \( b = d \). But then \( a - c \in P \), hence \( a - c = pq(x)q'(x) \) for some \( q'(x) \in \mathbb{F}_{11}[x] \). If \( a - c \neq 0 \) then \( 0 = \text{deg}(a - c) = \text{deg}(pq(x)q'(x)) = \text{deg}(p(x)) + \text{deg}(q'(x)) = 2 + \text{deg}(q'(x)) \geq 2 \), a contradiction, so \( a = c \). Thus, each element of \( \mathbb{F}_{11}[x]/P \) has the form \( a + bx + P \) for uniquely determined \( a, b \in \mathbb{F}_{11} \).

Define a map \( \varphi \) from \( \mathbb{F}_{11}[x] \) to \( \mathbb{F}_{11}[y] \) by \( \varphi(p(x)) = p(y + 1) \) for every \( p(x) \in \mathbb{F}_{11}[x] \). Then \( \varphi \) is a ring homomorphism because

\[
\varphi(p(x)q(x)) = p(y + 1)q(y + 1) = \varphi(p(x))\varphi(q(x))
\]

\[
\varphi(p(x) + q(x)) = p(y + 1) + q(y + 1) = \varphi(p(x)) + \varphi(q(x))
\]

The map \( \varphi \) can be described as “substitute \( y + 1 \) for \( x \)”. This map has an inverse \( \varphi^{-1} \) which may be described as “substitute \( x - 1 \) for \( y \)”, that is, for all \( q(y) \in \mathbb{F}_{11}[y] \) we let \( \psi(q(y)) = q(x - 1) \), so that

\[
\psi(\varphi(p(x))) = \psi(p(y + 1)) = p((x - 1) + 1) = p(x) \quad \text{and} \quad \varphi(\psi(q(y))) = \varphi(q(x - 1)) = q((y + 1) - 1) = q(y),
\]

so \( \psi = \varphi^{-1} \). This shows that \( \varphi \) is actually a ring isomorphism. Note that \( \varphi(x^2 + 1) = (y + 1)^2 + 1 = y^2 + 2y + 2 \). Corresponding elements in isomorphic rings generate corresponding ideals, so the image of the principal ideal \( (x^2 + 1) \subseteq \mathbb{F}_{11}[x] \) under \( \varphi \) is the ideal \( (y^2 + 2y + 1) \subseteq \mathbb{F}_{11}[y] \). Consequently the quotients by corresponding ideals are isomorphic, so

\[
K_1 = \mathbb{F}_{11}[x]/(x^2 + 1) \cong \mathbb{F}_{11}/(y^2 + 2y + 2) = K_2.
\]

9.4.14 Factor each of the two polynomials \( x^8 - 1 \) and \( x^6 - 1 \) into irreducibles over each of the following rings. (a) \( \mathbb{Z} \) (b) \( \mathbb{Z}/2\mathbb{Z} \) (c) \( \mathbb{Z}/3\mathbb{Z} \).

(a) \( \mathbb{Z} \): First we note that

\[
x^8 - 1 = (x^4)^2 - 1 = (x^4 + 1)(x^4 - 1)
\]

\[
= (x^4 + 1)(x^2 + 1)(x^2 - 1)
\]

\[
= (x^4 + 1)(x^2 + 1)(x + 1)(x - 1)
\]

Next we show that the factors \( x^4 + 1, x^2 + 1, x + 1, \) and \( x - 1 \) are all irreducible in \( \mathbb{Z}[x] \). In Example (3), p. 310, following Cor. 14 in Section 9.4, the polynomial \( p(x) = x^4 + 1 \in \mathbb{Z}[x] \) was shown to be irreducible in two steps. First, by the Eisenstein Criterion, applied with
prime 2 to the polynomial $p(x+1) = (x+1)^4+1 = x^4+4x^3+6x^2+4x+2$, we know that $p(x+1)$ is irreducible in $\mathbb{Z}[x]$. Second, if there were a nontrivial factorization $p(x) = a(x)b(x)$, with $a(x), b(x) \in \mathbb{Z}[x]$, $1 \leq \deg(a(x)) < 4$, and $1 \leq \deg(b(x)) < 4$, then we would have $p(x+1) = a(x+1)b(x+1)$ where $1 \leq \deg(a(x+1)) < 4$ and $1 \leq \deg(b(x+1)) < 4$, contradicting the irreducibility of $p(x+1)$. The factor $x^2+1$ has no roots in $\mathbb{Z}$ and is quadratic, hence is irreducible by Prop. 9.10. Finally, the linear factors $x+1$ and $x-1$ are irreducible.

A factorization of $x^6 - 1$ into irreducibles in $\mathbb{Z}[x]$ is

$$x^6 - 1 = (x^3)^2 - 1 = (x^3 + 1)(x^3 - 1) = (x^2 - x + 1)(x + 1)(x^2 + x + 1)(x - 1)$$

The linear factors $x+1$ and $x-1$ are irreducible. Let $p(x) = x^2 - x + 1$. Then

$$p(x+1) = (x+1)^2 - (x+1) + 1 = x^2 + 2x + 1 - x - 1 + 1 = x^2 + x + 1$$
$$p(x+2) = (x+2)^2 - (x+2) + 1 = x^2 + 4x + 4 - x - 2 + 1 = x^2 + 3x + 3$$

Now $x^2 + 3x + 3$ is irreducible in $\mathbb{Z}[x]$ by the Eisenstein Criterion, since prime 3 does not divide the leading coefficient 1, but does divide the lower order coefficients (3 and 3), and its square $3^2 = 9$ does not divide the constant 3. If $p(x)$ had a nontrivial factorization into nonconstant polynomials, say $p(x) = a(x)b(x)$, this would yield a nontrivial factorization $p(x+2) = a(x+2)b(x+2)$, contradicting the irreducibility of $p(x+2)$, so $p(x)$ is irreducible. A nontrivial factorization of $p(x+1)$, say $p(x+1) = c(x)d(x)$, would yield a nontrivial factorization $p(x+2) = c(x+1)d(x+1)$, contradicting the irreducibility of $p(x+2)$, so $p(x+1)$ is also irreducible. This shows that the two quadratic factors in the factorization of $x^6 - 1$ are irreducible in $\mathbb{Z}[x]$. 
(b): \( \mathbb{Z}/2\mathbb{Z} \). This ring is the 2-element field \( \mathbb{F}_2 \), whose only elements are 0 and 1, and in which we have \(-1 = 1\), so the previous factorizations can be written

\[
\begin{align*}
x^8 - 1 &= (x^4 + 1)(x^2 + 1)(x + 1)(x + 1) \\
x^6 - 1 &= (x^2 + x + 1)(x + 1)(x^2 + x + 1)(x + 1)
\end{align*}
\]

Note that \((x + 1)(x + 1) = x^2 + 2x + 1 = x^2 + 1\), and \((x^2 + 1)(x^2 + 1) = x^4 + 2x^2 + 1 = x^4 + 1\), so we can continue to factor \(x^8 - 1\), obtaining

\[
x^8 - 1 = (x^4 + 1)(x^2 + 1)(x + 1)(x + 1) = (x + 1)^8
\]

On the other hand, \(x^2 + x + 1\) is irreducible in \( \mathbb{F}_2[x] \), so a factorization of \(x^6 - 1\) into irreducibles over \( \mathbb{Z}/2\mathbb{Z} \) is the same as it was over \( \mathbb{Z} \), namely

\[
x^6 - 1 = (x^2 + x + 1)(x + 1)(x^2 + x + 1)(x + 1)
\]

GAP that confirms these results:

```gap
gap> r:=PolynomialRing(GF(2),["x"]);
gap> x:=IndeterminatesOfPolynomialRing(r)[1];
gap> Factors(x^8-1);Factors(x^6-1);
[ x+Z(2)^0, x+Z(2)^0, x+Z(2)^0, x+Z(2)^0,
  x+Z(2)^0, x+Z(2)^0, x+Z(2)^0, x+Z(2)^0 ]
[ x+Z(2)^0, x+Z(2)^0, x^2+x+Z(2)^0, x^2+x+Z(2)^0 ]
```

(c): \( \mathbb{Z}/3\mathbb{Z} \). This ring is the 3-element field \( \mathbb{F}_3 \), in which \(-1 = 2\). The factorizations of \(x^8 - 1\) and \(x^6 - 1\) into irreducibles are

\[
\begin{align*}
x^8 - 1 &= (x + 1)(x + 2)(x^2 + 1)(x^2 + x + 2)(x^2 + 2x + 2) \\
x^6 - 1 &= (x + 1)(x + 1)(x + 1)(x + 2)(x + 2)(x + 2)
\end{align*}
\]

These results were obtained by the following calculation in GAP:

```gap
gap> r:=PolynomialRing(GF(3),["x"]);
gap> IndeterminatesOfPolynomialRing(r);
[ x ]
```
\texttt{gap> x:=IndeterminatesOfPolynomialRing(r)[1]; x}
\texttt{gap> Factors(x^8-1);Factors(x^6-1);
[ x+Z(3)^0, x-Z(3)^0, x^2+Z(3)^0, x^2+x-Z(3)^0, x^2-x-Z(3)^0 ]
[ x+Z(3)^0, x+Z(3)^0, x+Z(3)^0, x-Z(3)^0, x-Z(3)^0, x-Z(3)^0 ]}

\textbf{9.4.18} Show that $6x^5 + 14x^3 - 21x + 35$ and $18x^5 - 30x^2 + 120x + 360$ are irreducible in $\mathbb{Q}[x]$.

We may use Exer. 9.4.17, which is the extended version of the Eisenstein Criterion that was proved in class.

Let $p(x) = 6x^5 + 14x^3 - 21x + 35$. Then $p(x)$ is irreducible in $\mathbb{Z}[x]$ by Eisenstein’s Criterion using prime 7, which does not divide the leading coefficient 6, does divide the remaining coefficients 14, -21, and 35, but its square $7^2 = 49$ does not divide the constant 35. Suppose $p(x)$ is reducible in $\mathbb{Q}[x]$, say $p(x) = A(x)B(x)$ for some $A(x), B(x) \in \mathbb{Q}[x]$. Note that $\mathbb{Q}$ is the field of fractions of $\mathbb{Z}$, so by Prop. 9.5 (Gauss’s Lemma) there are rationals $r, s \in \mathbb{Q}$ such that $p(x) = rA(x)sB(x)$, $rA(x) \in \mathbb{Z}[x]$, and $sB(x) \in \mathbb{Z}[x]$, contradicting the irreducibility of $p(x)$ in $\mathbb{Z}[x]$.

Let $q(x) = 18x^5 - 30x^2 + 120x + 360$. Then $q(x)$ is irreducible by Eisenstein’s Criterion using prime 5, which does not divide the leading coefficient 18, does divide the remaining coefficients -30, 120, and 360, but $5^2 = 25$ does not divide the constant 360. By Prop. 9.5 (Gauss’s Lemma), $q(x)$ is also irreducible in $\mathbb{Q}[x]$, as was argued for $p(x)$ above.

\textbf{9.5.2} For each of the fields in Exercise 6 of Section 4 exhibit a generator for the cyclic multiplicative group of nonzero elements.

Exer. 9.4.6 asks for fields of order (a) 9, (b) 49, (c) 8, and (d) 81, exhibited in the form $F[x]/(f(x))$ where $F$ is a field and $f \in F[x]$.

(a) For a field $F[x]/(f(x))$ of order 9, let $F = \mathbb{F}_3$ and let $f$ be the irreducible quadratic polynomial $f(x) = x^2 + 1 \in \mathbb{F}_3[x]$. The elements $F[x]/(f(x))$ have the form $ax + b + (f)$, where $a, b \in \{0, 1, 2\}$. The multiplicative group of $F[x]/(f(x))$ is generated by $x + 2 + (f)$, as is shown in the table of calculations below, where we write simply “$ax + b$”
instead of “$ax+b+(f)$”. With this notational convention, observe that in $F[x]/(f(x))$ we have $x^2 + 1 = 0$ (more precisely, $x^2 + 1 + (f) = (f)$), so $x^2 = -1 = 2$.

$$(x + 2)^1 = x + 2$$

$$(x + 2)^2 = x^2 + 4x + 4 = 2 + x + 1 = x$$

$$(x + 2)^3 = (x + 2)x = x^2 + 2x = 2x + 2$$

$$(x + 2)^4 = (2x + 2)(x + 2) = 2x^2 + 6x + 4 = 2(2) + 1 = 2$$

$$(x + 2)^5 = 2(x + 2) = 2x + 1$$

$$(x + 2)^6 = (2x + 1)(x + 2) = 2x^2 + 5x + 2 = 2(2) + 2x + 2 = 2x$$

$$(x + 2)^7 = 2x(x + 2) = 2x^2 + 4x = 2(2) + x = x + 1$$

$$(x + 2)^8 = (x + 1)(x + 2) = x^2 + 3x + 2 = 2 + 2 = 1$$

(b) To get a field $F[x]/(f(x))$ of order 49, we choose $F = \mathbb{F}_7$ so that $q = |\mathbb{F}_7| = 7$, and we let $f$ be any one of the 21 monic irreducible quadratic polynomials in $\mathbb{F}_7[x]$. Then $n = 2$ and the order of $F[x]/(f(x))$ is $q^n = 7^2 = 49$. The 21 monic irreducible quadratic polynomials in $\mathbb{F}_7[x]$ are organized in the following table according to the 7 linear substitutions, “substitute $x + n$ for $x$”.

<table>
<thead>
<tr>
<th>$\varphi(x)$</th>
<th>$x^2 + 1$</th>
<th>$x^2 + 2$</th>
<th>$x^2 + 4$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\varphi(x + 1)$</td>
<td>$x^2 + 2x + 2$</td>
<td>$x^2 + 2x + 3$</td>
<td>$x^2 + 2x + 5$</td>
</tr>
<tr>
<td>$\varphi(x + 2)$</td>
<td>$x^2 + 4x + 5$</td>
<td>$x^2 + 4x + 6$</td>
<td>$x^2 + 4x + 1$</td>
</tr>
<tr>
<td>$\varphi(x + 3)$</td>
<td>$x^2 + 6x + 3$</td>
<td>$x^2 + 6x + 4$</td>
<td>$x^2 + 6x + 6$</td>
</tr>
<tr>
<td>$\varphi(x + 4)$</td>
<td>$x^2 + x + 3$</td>
<td>$x^2 + x + 4$</td>
<td>$x^2 + x + 6$</td>
</tr>
<tr>
<td>$\varphi(x + 5)$</td>
<td>$x^2 + 3x + 5$</td>
<td>$x^2 + 3x + 6$</td>
<td>$x^2 + 3x + 1$</td>
</tr>
<tr>
<td>$\varphi(x + 6)$</td>
<td>$x^2 + 5x + 2$</td>
<td>$x^2 + 5x + 3$</td>
<td>$x^2 + 5x + 5$</td>
</tr>
</tbody>
</table>

Claim: $\mathbb{F}_7/(x^2 + 1)$ is generated by $x + 3 = x + 3 + (x^2 + 1)$. From $x^2 + 1 = 0$ we have $x^2 = -1 = 6$, so we can derive a rule for raising $x + 3$ to powers in $\mathbb{F}_7/(x^2 + 1)$. If $ax + b$ is a power of $x + 3$, we get the next power as follows:

$$(ax + b)(x + 3) = ax^2 + (3a + b)x + 3b = (3a + b)x + (6a + 3b)$$
Using GAP, I computed the powers of $x + 3$, and obtained these results, which prove that $x + 3$ is indeed a generator.

$$(x + 3)^1 = x + 3$$
$$(x + 3)^2 = 6x + 1$$
$$(x + 3)^3 = 5x + 4$$
$$(x + 3)^5 = x + 2$$
$$(x + 3)^7 = 5x + 3$$
$$(x + 3)^9 = 3x + 2$$
$$(x + 3)^{11} = x + 5$$
$$(x + 3)^{13} = 3x + 6$$
$$(x + 3)^{15} = 4x + 2$$
$$(x + 3)^{17} = 2x + 6$$
$$(x + 3)^{19} = 3x + 1$$
$$(x + 3)^{21} = 2x + 4$$
$$(x + 3)^{23} = 5x + 6$$
$$(x + 3)^{25} = 6x + 4$$
$$(x + 3)^{27} = 2x + 3$$
$$(x + 3)^{29} = 6x + 5$$
$$(x + 3)^{31} = x + 4$$
$$(x + 3)^{33} = 4x + 5$$
$$(x + 3)^{35} = 6x + 2$$
$$(x + 3)^{37} = 4x + 1$$
$$(x + 3)^{39} = 3x + 5$$
$$(x + 3)^{41} = 5x + 1$$
$$(x + 3)^{43} = 4x + 6$$
$$(x + 3)^{45} = 5x + 3$$

$$(x + 3)^4 = 5x$$
$$(x + 3)^6 = 5x + 5$$
$$(x + 3)^8 = 3$$
$$(x + 3)^{10} = 4x + 3$$
$$(x + 3)^{12} = x$$
$$(x + 3)^{14} = x + 1$$
$$(x + 3)^{16} = 2$$
$$(x + 3)^{18} = 5x + 2$$
$$(x + 3)^{20} = 3x$$
$$(x + 3)^{22} = 3x + 3$$
$$(x + 3)^{24} = 6$$
$$(x + 3)^{26} = x + 6$$
$$(x + 3)^{28} = 2x$$
$$(x + 3)^{30} = 2x + 2$$
$$(x + 3)^{32} = 4$$
$$(x + 3)^{34} = 3x + 4$$
$$(x + 3)^{36} = 6x$$
$$(x + 3)^{38} = 6x + 6$$
$$(x + 3)^{40} = 5$$
$$(x + 3)^{42} = 2x + 5$$
$$(x + 3)^{44} = 4x$$
$$(x + 3)^{46} = 4x + 4$$
\[(x + 3)^{47} = 2x + 1 \quad (x + 3)^{48} = 1\]
\[(x + 3)^{49} = x + 3\]

(c) For a field \( F[x]/(f(x)) \) of order 8, let \( F = \mathbb{F}_2 \) and let \( f \) be the irreducible cubic polynomial \( f(x) = x^3 + x + 1 \in \mathbb{F}_2[x] \). The multiplicative group of \( \mathbb{F}_3[x]/(x^3 + x + 1) \) has 7 elements, and since 7 is prime it follows that every non-zero element of the field will generate the multiplicative group. In particular, \( x \) generates, as is explicitly shown by the following calculations. First note that since \( x^3 + x + 1 = 0 \), we get \( x^3 = -x - 1 = x + 1 \) (all modulo 2), so
\[
\begin{align*}
x^1 &= x \\
x^2 &= x^2 \\
x^3 &= x + 1 \\
x^4 &= x^2 + x \\
x^5 &= x^3 + x^2 = x^2 + x + 1 \\
x^6 &= x^3 + x^2 + x = x^2 + 1 \\
x^7 &= x^3 + x^2 = x + 1 + x + 1
\end{align*}
\]

(d) For a field \( F[x]/(f(x)) \) of order 81, let \( F = \mathbb{F}_3 \) and let \( f \) be the irreducible quartic polynomial \( f(x) = x^4 + x + 2 \in F[x] \) (shown to be irreducible in Exer. 9.4.6(d)). Let \( P = (f) \subseteq F[x] \). The elements \( F[x]/(f(x)) \) have the form \( ax^3 + bx^2 + cx + d + P \), where \( a, b, c, d \in \{0, 1, 2\} \). The multiplicative group of \( F[x]/(f(x)) \) is generated by \( x + P \). The 80 powers of \( x + P \) are shown in the table below, which has only \( “ax^3 + bx^2 + cx + d” \) instead of \( “ax^3 + bx^2 + cx + d + P” \).

\[
\begin{align*}
x^1 &= x & x^{41} &= 2x \\
x^2 &= x^2 & x^{42} &= 2x^2 \\
x^3 &= x^3 & x^{43} &= 2x^3 \\
x^4 &= 2x + 1 & x^{44} &= x + 2
\end{align*}
\]
\[ x^5 = 2x^2 + x \]
\[ x^6 = 2x^3 + x^2 \]
\[ x^7 = x^3 + x + 2 \]
\[ x^8 = x^2 + x + 1 \]
\[ x^9 = x^3 + x^2 + x \]
\[ x^{10} = x^3 + x^2 + 2x + 1 \]
\[ x^{11} = x^3 + 2x^2 + 1 \]
\[ x^{12} = 2x^3 + 1 \]
\[ x^{13} = 2x + 2 \]
\[ x^{14} = 2x^2 + 2x \]
\[ x^{15} = 2x^3 + 2x^2 \]
\[ x^{16} = 2x^3 + x + 2 \]
\[ x^{17} = x^2 + 2 \]
\[ x^{18} = x^3 + 2x \]
\[ x^{19} = 2x^2 + 2x + 1 \]
\[ x^{20} = 2x^3 + 2x^2 + x \]
\[ x^{21} = 2x^3 + x^2 + x + 2 \]
\[ x^{22} = x^3 + x^2 + 2 \]
\[ x^{23} = x^3 + x + 1 \]
\[ x^{24} = x^2 + 1 \]
\[ x^{25} = x^3 + x \]
\[ x^{26} = x^2 + 2x + 1 \]
\[ x^{27} = x^3 + 2x^2 + x \]
\[ x^{28} = 2x^3 + x^2 + 2x + 1 \]
\[ x^{29} = x^3 + 2x^2 + 2x + 2 \]
\[ x^{45} = x^2 + 2x \]
\[ x^{46} = x^3 + 2x^2 \]
\[ x^{47} = 2x^3 + 2x + 1 \]
\[ x^{48} = 2x^2 + 2x + 2 \]
\[ x^{49} = 2x^3 + 2x^2 + 2x \]
\[ x^{50} = 2x^3 + 2x^2 + x + 2 \]
\[ x^{51} = 2x^3 + x^2 + 2 \]
\[ x^{52} = x^3 + 2 \]
\[ x^{53} = x + 1 \]
\[ x^{54} = x^2 + x \]
\[ x^{55} = x^3 + x^2 \]
\[ x^{56} = x^3 + 2x + 1 \]
\[ x^{57} = 2x^2 + 1 \]
\[ x^{58} = 2x^3 + x \]
\[ x^{59} = x^2 + x + 2 \]
\[ x^{60} = x^3 + x^2 + 2x \]
\[ x^{61} = x^3 + 2x^2 + 2x + 1 \]
\[ x^{62} = 2x^3 + 2x^2 + 1 \]
\[ x^{63} = 2x^3 + 2x + 2 \]
\[ x^{64} = 2x^2 + 2 \]
\[ x^{65} = 2x^3 + 2x \]
\[ x^{66} = 2x^2 + x + 2 \]
\[ x^{67} = 2x^3 + x^2 + 2x \]
\[ x^{68} = x^3 + 2x^2 + x + 2 \]
\[ x^{69} = 2x^3 + x^2 + x + 1 \]
\[ x^{30} = 2x^3 + 2x^2 + x + 1 \quad x^{70} = x^3 + x^2 + 2x + 2 \]
\[ x^{31} = 2x^3 + x^2 + 2x + 2 \quad x^{71} = x^3 + 2x^2 + x + 1 \]
\[ x^{32} = x^3 + 2x^2 + 2 \quad x^{72} = 2x^3 + x^2 + 1 \]
\[ x^{33} = 2x^3 + x + 1 \quad x^{73} = x^3 + 2x + 2 \]
\[ x^{34} = x^2 + 2x + 2 \quad x^{74} = 2x^2 + x + 1 \]
\[ x^{35} = x^3 + 2x^2 + 2x \quad x^{75} = 2x^3 + x^2 + x \]
\[ x^{36} = 2x^3 + 2x^2 + 2x + 1 \quad x^{76} = x^3 + x^2 + x + 2 \]
\[ x^{37} = 2x^3 + 2x^2 + 2x + 2 \quad x^{77} = x^3 + x^2 + x + 1 \]
\[ x^{38} = 2x^3 + 2x^2 + 2 \quad x^{78} = x^3 + x^2 + 1 \]
\[ x^{39} = 2x^3 + 2 \quad x^{79} = x^3 + 1 \]
\[ x^{40} = 2 \quad x^{80} = 1 \]

---

**Homework #04, due 2/10/10 = 10.1.1, 10.1.8, 10.1.9, 10.1.10.**

Additional problems recommended for study: 10.1.2, 10.1.3, 10.1.4, 10.1.5, 10.1.6, 10.1.7, 10.1.11, 10.1.12, 10.1.15

10.1.1 Assume $R$ is a ring with 1 and $M$ is a left $R$-module. Prove that $0m = 0$ and $(-1)m = -m$ for all $m \in M$.

Let $m \in M$. Since $M$ is a group with identity element 0, we have $0 = 0 + 0$ and $0 + 0m = 0m$. Then $0 + 0m = 0m = (0 + 0)m = 0m + 0m$ by the module axiom $(r + s)m = rm + sm$. Since $M$ is a group, we can cancel $0m$ from both sides, leaving $0 = 0m$.

Since $R$ is a ring with 1, we have $0 = 1 + (-1)$, so $0m = (1 + (-1))m = 1m + (-1)m$, but $1m = m$ by one of the module axioms and $0m = 0$ by the first part of this problem, so $0 = m + (-1)m$. By adding $-m$ to both sides we get $-m = (-1)m$.

10.1.8 Assume $R$ is a ring with 1 and $M$ is a left $R$-module. An element $m$ of the $R$-module $M$ is called a torsion element if $rm = 0$ for
some nonzero element $r \in R$. The set of torsion elements is denoted by

$$\text{Tor}(M) := \{m \in M | rm = 0 \text{ for some nonzero } r \in R\}$$

(a) Prove that if $R$ is an integral domain then $\text{Tor}(M)$ is a submodule of $M$ (called the torsion submodule of $M$).

Note that, by hypothesis, $R$ is commutative, has 1, and has no zero divisors. Also, for every $r \in R$ we have $0 + r0 = r0 = r(0+0) = r0 + r0$, so, cancelling $r0$ from both sides leaves $0 = r0$.

Let $m, n \in \text{Tor}(M)$. Then there are nonzero $r, s \in R$ such that $rm = 0 = sn$. Since $R$ is an integral domain and neither $r$ nor $s$ is zero, we conclude that $rs \neq 0$. Then $m + n \in \text{Tor}(M)$ because

$$rs(m + n) = (rs)m + (rs)n$$
$$= (sr)m + (rs)n \quad \text{by a module axiom}$$
$$= s(rm) + r(sn) \quad \text{since } rm = 0 = sn$$
$$= s0 + r0 \quad \text{proved above}$$
$$= 0 + 0$$
$$= 0$$

This shows $\text{Tor}(M)$ is closed under $+$. Also, for every $t \in R$ we have

$$r(tm) = (rt)m \quad \text{by a module axiom}$$
$$= (tr)m \quad \text{R is commutative}$$
$$= t(rm)$$
$$= t0 \quad \text{since } rm = 0$$
$$= 0 \quad \text{proved above}$$

so $tm \in \text{Tor}(M)$. Since $\text{Tor}(M)$ is closed under $+$ and the action of $R$, it is a submodule.

(b) Give an example of a ring $R$ and an $R$-module $M$ such that $\text{Tor}(M)$ is not a submodule of $M$. [Consider the torsion elements in the $R$-module $R$.]
Let $R = \mathbb{Z}/6\mathbb{Z}$ and $n = n + 6\mathbb{Z}$ for every $n \in \mathbb{Z}$. Then
\[
2 \cdot 3 = (2 + 6\mathbb{Z})(3 + 6\mathbb{Z}) = 2 \cdot 3 + 6\mathbb{Z} = 6 + 6\mathbb{Z} = 6\mathbb{Z} = 0.
\]
This equation implies that if we consider $R$ as a module over itself, we have $3 \in \text{Tor}(R)$, but we also have $3 \cdot 2 = 0$, so $2 \in \text{Tor}(M)$ as well. Note that $2 + 3 = 5$ and $5 \notin \text{Tor}(M)$ because $1 \cdot 5 = 5 \neq 0$, $2 \cdot 5 = 4 \neq 0$, $3 \cdot 5 = 3 \neq 0$, $4 \cdot 5 = 2 \neq 0$, and $5 \cdot 5 = 1 \neq 0$. Thus 2 and 3 are in $\text{Tor}(M)$, but their sum is not in $\text{Tor}(M)$. This shows that $\text{Tor}(M)$ is not a submodule.

(c) If $R$ has zero divisors show that every nonzero $R$-module has nonzero torsion elements.

Assume $R$ is a commutative ring with 1 and with zero divisors, say $rs = 0$ where $r, s \in R$ and $r \neq 0 \neq s$. Assume $M$ is a nonzero $R$-module. Since $M$ is not the zero module, we may choose some $m \in M$ with $m \neq 0$. If $sm = 0$, then $m \in \text{Tor}(M)$ since $s \neq 0$, and we’re done, so assume $sm \neq 0$. Then
\[
r(sm) = (rs)m \quad \text{module axiom}
\]
\[
= 0m \quad \text{since } rs = 0
\]
\[
= 0 \quad \text{by 10.1.1 above}
\]
Since $r \neq 0$, this shows that $sm \in \text{Tor}(M)$. Either way, we have a nonzero element in $\text{Tor}(M)$.

10.1.9 Assume $R$ is a ring with 1 and $M$ is a left $R$-module. If $N$ is a submodule of $M$, the annihilator of $N$ in $R$ is defined to be $\{ r \in R | rn = 0 \text{ for all } n \in N \}$. Prove that the annihilator of $N$ in $R$ is a 2-sided ideal of $R$.

Let $\text{Ann}_R(N) \subseteq R$ be the annihilator of $N$ in $R$. Assume $r \in \text{Ann}_R(N)$ and let $s \in R$. We wish to show $sr \in \text{Ann}_R(N)$ and $rs \in \text{Ann}_R(N)$. For every $n \in N$ we have $(sr)n = s(rn) = s \cdot 0 = 0$, so $sr \in \text{Ann}_R(N)$. Also, for every $n \in N$, $sn \in N$ since $n \in N$ and $N$ is a submodule, so $(rs)n = r(sn) = 0$ since $r \in \text{Ann}_R(N)$. So far we have shown that $\text{Ann}_R(N)$ is closed under multiplication by elements of $R$, both on the left and on the right. To complete the proof we need to show...
$\text{Ann}_R(N)$ is closed under $+$. Let $r, s \in \text{Ann}_R(N)$. Then for all $n \in N$, we have $rn = sn = 0$, so $(r + s)n = rn + sn = 0 + 0 = 0$. Therefore $r + s \in \text{Ann}_R(N)$.

**10.1.10** Assume $R$ is a ring with 1 and $M$ is a left $R$-module. If $I$ is an ideal of $R$, the annihilator of $I$ in $M$ is defined to be $\{m \in M | am = 0 \text{ for all } a \in I\}$. Prove that the annihilator of $I$ in $M$ is a submodule of $M$.

Let $\text{Ann}_M(I)$ be the annihilator of $I$ in $M$. We will show $\text{Ann}_M(I)$ is closed under $-$ and closed under the action of elements in $R$. Let $m, n \in \text{Ann}_M(I)$. Then, for all $a \in I$, $am = an = 0$, so $a(m - n) = am - an = 0 - 0 = 0$. This shows $m - n \in \text{Ann}_M(I)$. Let $r \in R$. Then $rm \in \text{Ann}_M(I)$ because, for every $a \in I$, we have $ar \in I$ since $I$ is an ideal, so $(ar)m = 0$ since $m \in \text{Ann}_M(I)$, hence $a(rm) = 0$ by a module axiom.

Homework #05, due 2/17/10 = 10.3.1, 10.3.4, 10.3.5, 10.3.7, 10.3.15

Additional problems recommended for study: 10.2.1, 10.2.2, 10.2.3, 10.2.5, 10.2.6, 10.2.10, 10.2.11, 10.3.2, 10.3.9, 10.3.12, 10.3.13, 10.3.14.

**10.3.1** Assume $R$ is a ring with 1 and $M$ is a left $R$-module. Prove that if $A$ and $B$ are sets with the same cardinality, then the free modules $F(A)$ and $F(B)$ are isomorphic.

Since $A$ and $B$ have the same cardinality there exists a bijection $f : A \to B$. Since $f$ is a bijection its inverse is also a bijection and $f^{-1} : B \to A$. By Th. 10.6 the free modules $F(A)$ and $F(B)$ have the universal mapping property. Let us apply this property to $f$. Note that the range of $f$ is $B$ since $f$ is surjective, and $B$ is a subset of the free module $F(B)$. Thus we have another function (which we call $g$) that maps $A$ into $F(B)$ and is equal to $f$ on all elements of $A$, that is, $g : A \to F(B)$ and $g(a) = f(a)$ for all $a \in A$. By the universal mapping property there is a unique $R$-module homomorphism $\varphi : F(A) \to F(B)$.
which extends \( g \) (and \( f \)), that is, \( f(a) = g(a) = \varphi(a) \) for all \( a \in A \). By the same reasoning, with \( A \) and \( B \) interchanged and \( f \) replaced by \( f^{-1} \), we get another \( R \)-module homomorphism \( \psi : F(B) \to F(A) \) extending \( f^{-1} \). The composition of \( R \)-module homomorphisms is again an \( R \)-module homomorphism, so we obtain the \( R \)-module homomorphism \( \psi \circ \varphi : F(A) \to F(A) \). For every \( a \in A \), \((\psi \circ \varphi)(a) = \psi(\varphi(a)) = \psi(f(a))\), but \( f(a) \in B \) and \( \psi \) extends \( f^{-1} \), so \( \psi(f(a)) = f^{-1}(f(a)) = a \). This shows that \( \psi \circ \varphi \) is an extension of the identity map \( \iota : A \to F(A) \) which sends every element of \( A \) to itself, that is, \( \iota(a) = a \) for every \( a \in A \).

Now, by the universal mapping property, \( \iota \) has a unique extension to an \( R \)-module homomorphism from \( F(A) \) to itself. The identity map from \( F(A) \) to \( F(A) \) is an \( R \)-module homomorphism of \( F(A) \) onto itself, and by the universal mapping property of \( F(A) \) it is the only \( R \)-module homomorphism of \( F(A) \) onto itself. However, we found that \( \psi \circ \varphi \) is a homomorphism of \( F(A) \) onto itself that extends the identity map on \( A \), so \( \psi \circ \varphi \) must therefore be the identity map from \( F(A) \) to \( F(A) \). Similarly, \( \varphi \circ \psi \) is the identity map from \( F(B) \) to \( F(B) \). Thus \( \varphi \) and \( \psi \) are \( R \)-module homomorphisms between \( F(A) \) and \( F(B) \), and they are inverses of each other, so they are both injective and surjective, and are therefore isomorphisms between \( F(A) \) and \( F(B) \). Thus \( F(A) \cong F(B) \) whenever \( |A| = |B| \).

10.3.4 An \( R \)-module \( M \) is called a torsion module if for each \( m \in M \) there is a nonzero element \( r \in R \) such that \( rm = 0 \), where \( r \) may depend on \( m \) (i.e., \( M = \operatorname{Tor}(M) \) in the notation of Exercise 8 of Section 10.1). Prove that every finite abelian group is a torsion \( \mathbb{Z} \)-module. Give an example of an infinite abelian group that is a torsion \( \mathbb{Z} \)-module.

Let \( M \) be a finite abelian group, so that \( M \) is also a \( \mathbb{Z} \)-module. Let \( n \) be the order of \( M \), that is, \( n = |M| \in \mathbb{Z}^+ \). Then, for every \( a \in M \), the order of \( a \) divides the order \( n \) of the abelian group \( M \), so \( na = 0 \). Since \( n \in \mathbb{Z} \) and \( na \) is the result of the action of \( n \) on \( a \) in the module \( M \), we have \( a \in \operatorname{Tor}(M) \) for every \( a \in M \), so \( M \subseteq \operatorname{Tor}(M) \). The opposite inclusion holds trivially, so \( M = \operatorname{Tor}(M) \).
Let \( M = \prod_{i \in \mathbb{Z}^+} \mathbb{Z}/2\mathbb{Z} \). Thus \( M \) is the direct product of countably many copies of the 2-element cyclic group \( \mathbb{Z}/2\mathbb{Z} \). \( M \) is an infinite abelian group whose cardinality is the same as the set of real numbers. Every element of \( M \) has order 2, so \( 2 \cdot m = 0 \) for every \( m \in M \), so \( \text{Tor}(M) = M \).

10.3.5 Let \( R \) be an integral domain. Prove that every finitely generated torsion \( R \)-module has a nonzero annihilator, i.e., there is a nonzero \( r \in R \) such that \( rm = 0 \) for all \( m \in M \)—here \( r \) does not depend on \( m \) (the annihilator of a module was defined in Exercise 9 of Section 10.1). Give an example of a torsion \( R \)-module whose annihilator is the zero ideal.

Assume \( M \) is a finitely generated torsion \( R \)-module. Then there is a finite set \( A \subseteq M \) of nonzero elements such that \( M = RA \). Let \( A = \{a_1, \cdots, a_n\} \), \( n \in \omega \). Since \( M \) is a torsion module, there exist nonzero elements \( r_1, \cdots, r_n \in R \) such that \( r_1a_1 = 0, r_2a_2 = 0, \ldots, r_na_n = 0 \). Let \( q = r_1 \cdots r_n \). Consider an arbitrary element \( m \in M \). Since \( M = RA \), there are ring elements \( s_1, \cdots, s_n \in R \) such that \( m = s_1a_1 + \cdots + s_na_n \). Let \( 1 \leq i \leq n \). Since \( R \) is an integral domain, \( R \) is commutative, so \( q = pr_i \) where \( p \) is the product of all the other factors \( r_j \) with \( j \neq i \). Then \( qa_i = (pr_i)a_i = p(r_ia_i) = p0 = 0 \). This shows \( qa_1 = qa_2 = \cdots = qa_n = 0 \), so we have

\[
qm = q(s_1a_1 + \cdots + s_na_n)
= q(s_1a_1) + \cdots + q(s_na_n) \quad \text{module axiom}
= (qs_1)a_1 + \cdots + (qs_n)a_n \quad \text{module axiom}
= (s_1q)a_1 + \cdots + (s_nq)a_n \quad \text{since } R \text{ is commutative}
= s_1(qa_1) + \cdots + s_n(qa_n) \quad \text{module axiom}
= s_1(0) + \cdots + s_n(0) \quad \text{shown above}
= 0 + \cdots + 0
= 0
\]

Since \( m \) was an arbitrary element of \( M \), we have shown that \( qm = 0 \) for every \( m \in M \). Finally, we observe that \( q \) is nonzero because \( r_i \neq 0 \).
and the product on nonzero elements in the integral domain $R$ cannot be zero.

For an example of a torsion $R$-module whose annihilator is the zero ideal, let $R = \mathbb{Z}$, and let $M$ be the direct sum of the finite cyclic groups $\mathbb{Z}/n\mathbb{Z}$ with $2 \leq n \in \mathbb{Z}^+$, so

$$M = \bigoplus_{2 \leq n \in \mathbb{Z}^+} \mathbb{Z}/n\mathbb{Z}.$$  

Let $m \in M$. Then there are $k \in \mathbb{Z}^+$ and $a_1, \ldots, a_k \in \mathbb{Z}$ such that $m = (a_1 + 2\mathbb{Z}, \ldots, a_k + k\mathbb{Z}, 0, 0, 0, \ldots)$, so $k! \cdot m = 0$, so $m \in \text{Tor}(M)$. Then $M$ is a torsion module, but no element of $\mathbb{Z}$ annihilates every element of $M$, for if $k \in \mathbb{Z}^+$ then $k \cdot (\ldots, 1 + (k+1)\mathbb{Z}, 0, 0, \ldots) \neq 0$.

10.3.7 Assume $R$ is a ring with 1 and $M$ is a left $R$-module. Let $N$ be a submodule of $M$. Prove that if both $M/N$ and $N$ are finitely generated, then so is $M$.

$N$ is a finitely generated $R$-module, so there is a finite subset $A \subseteq N$ such that $N = RA$. $M/N$ is also a finitely generated $R$-module. The elements of $M/N$ have the form $b + N$ with $b \in M$, so there is a finite subset $B \subseteq M$ such that $M/N = R\{b + N|b \in B\}$. Let $A = \{a_1, \ldots, a_n\}$ and $B = \{b_1, \ldots, b_k\}$. Then

$$N = \{r_1a_1 + \cdots + r_na_n|b_1, \ldots, r_n \in R\}$$
$$M/N = \{s_1(b_1 + N) + \cdots + s_k(b_k + N)|s_1, \ldots, s_k \in R\}$$
$$= \{s_1b_1 + \cdots + s_kb_k + N|s_1, \ldots, s_k \in R\}$$

We will show $M = R(A \cup B)$. Let $m \in M$. Then $m + N \in M/N$, so by the second equation above there exist $s_1, \ldots, s_k \in R$ such that $m + N = s_1b_1 + \cdots + s_kb_k + N$. Now $m \in m + N$, so $m \in s_1b_1 + \cdots + s_kb_k + N$, so by the first equation above there exist $r_1, \ldots, r_n \in R$ such that $m = s_1b_1 + \cdots + s_kb_k + r_1a_1 + \cdots + r_na_n \in R(A \cup B)$, as was to be shown. Now $A \cup B$ is finite because both $A$ and $B$ are finite, so $M$ is therefore finitely generated by the finite set $A \cup B$. 

10.3.15 An element $e \in R$ is called a **central idempotent** if $e^2 = e$ and $er = re$ for all $r \in R$. If $e$ a central idempotent in $R$, prove that $M = eM \oplus (1 - e)M$. [Recall Exercise 14 in Section 10.1.]

We wish to show that $eM$ and $(1 - e)M$ are submodules and that $M$ is the internal direct sum of the two submodules $eM$ and $(1 - e)M$.

To see that $eM$ is a submodule, first note that $em_1 + em_2 = e(m_1 + m_2) \in eM$ for all $m_1, m_2 \in M$, so $eM$ is closed under addition. To see that $eM$ is closed under the action of $R$, let $m \in M$ and $r \in R$. Then, using the fact that $e$ is in the center and hence $er = re$, we have $r(em) = (re)m = (er)m = e(rm) \in eM$.

The proof that $(1 - e)M$ is also closed under addition is essentially the same, namely, $(1 - e)m_1 + (1 - e)m_2 = (1 - e)(m_1 + m_2) \in (1 - e)M$ for all $m_1, m_2 \in M$. Next we show that $(1 - e)M$ is closed under the action of $R$. Let $m \in M$ and $r \in R$. Then, using the fact that $e$ is in the center and hence $er = re$, we have

$$r((1 - e)m) = r((1 - e))m = (r1 - re)m = (1r - er)m = ((1 - e)r)m = (1 - e)(rm) \in (1 - e)M$$

Next we show $eM \cap (1 - e)M = \{0\}$. Let $m \in eM \cap (1 - e)M$. Then there are $m_1, m_2 \in M$ such that $m = em_1 = (1 - e)m_2$, so

$$m = em_1 = e^2m_1 = (ee)m_1 = e(em_1) = e((1 - e)m_2) = e(1 - e)m_2 = (e1 - e^2)m_2$$

$$e = e^2$$

$$em_1 = (1 - e)m_2$$
\[= (e - e)m_2\]
\[e = e^2\]
\[= 0m_2\]
\[= 0.\]

It therefore follows by Prop. 10.5 that \(M \cong eM \oplus (1 - e)M\).

---

Homework #06, due 2/24/10 = 10.2.9, 10.2.10, 10.3.12, 10.3.13, 10.3.14

Additional problems recommended for study: 10.3.18, 10.3.19, 10.3.20, 10.3.21, 10.3.22, 10.3.23, 10.3.24

10.2.9 Let \(R\) be a commutative ring. Prove that \(\text{Hom}_R(R, M)\) and \(M\) are isomorphic as left \(R\)-modules. [Show that each element of \(\text{Hom}_R(R, M)\) is determined by its value on the identity of \(R\).]

Let 1 be the identity of \(R\). (The hint suggests that such an element exists, so we assume \(R\) is a commutative ring with 1.) First note that \(\text{Hom}_R(R, M)\) is indeed an \(R\)-module by Prop. 10.2(2), for which we need the commutativity of \(R\). We wish to show \(\text{Hom}_R(R, M) \cong M\).

For every \(\varphi \in \text{Hom}_R(R, M)\), let \(\Psi(\varphi) = \varphi(1)\). This defines a map \(\Psi\) from \(\text{Hom}_R(R, M)\) to \(M\). For \(\Psi\) to be an \(R\)-module homomorphism, we must check \(\Psi(\varphi + \psi) = \Psi(\varphi) + \Psi(\psi)\) and \(\Psi(r\varphi) = r\Psi(\varphi)\) for all \(\varphi, \psi \in \text{Hom}_R(R, M)\) and all \(r \in R\).

\[
\Psi(\varphi + \psi) = (\varphi + \psi)(1) \quad \text{def of } \Psi
\]
\[
= \varphi(1) + \psi(1) \quad \text{def of } + \text{ in } \text{Hom}_R(R, M)
\]
\[
= \Psi(\varphi) + \Psi(\psi) \quad \text{def of } \Psi
\]

\[
\Psi(r\varphi) = (r\varphi)(1) \quad \text{def of } \Psi
\]
\[
= r(\varphi(1)) \quad \text{def of action of } R \text{ on } \text{Hom}_R(R, M)
\]
\[
= r\Psi(\varphi) \quad \text{def of } \Psi
\]

If \(\Psi(\varphi) = \Psi(\psi)\), then \(\varphi(1) = \psi(1)\) by the definition of \(\Psi\), so, for all \(r \in R\), \(\varphi(r) = \varphi(r1) = r\varphi(1) = r\psi(1) = \psi(r1) = \psi(r)\), which shows \(\varphi = \psi\). Thus \(\Psi\) is injective.
For surjectivity of $\Psi$, start with an arbitrary $m \in M$. Define a map $\xi_m$ by $\xi_m(r) = rm$ for all $r \in R$. Then $\xi_m$ is an $R$-module homomorphism of $R$ to $M$ because

$$\xi_m(r + s) = (r + s)m \quad \text{def of } \xi_m$$

$$= rm + sm \quad \text{module axiom}$$

$$= \xi_m(r) + \xi_m(s) \quad \text{def of } \xi_m$$

$$\xi_m(rs) = (rs)m \quad \text{def of } \xi_m$$

$$= r(sm) \quad \text{module axiom}$$

$$= r\xi_m(s) \quad \text{def of } \xi_m$$

Finally, we have $\Psi(\xi_m) = \xi_m(1) = 1m = m$, and this holds for all $m \in M$, so $\Psi$ is surjective.

**10.2.10** Let $R$ be a commutative ring. Prove that $\text{Hom}_R(R, R)$ and $R$ are isomorphic as rings.

As in the previous problem, we assume $R$ is a ring with 1. By Exer. **10.2.9** above, $\text{Hom}_R(R, R)$ and $R$ are isomorphic as left $R$-modules via the isomorphism $\Psi$, which is defined for every $\varphi \in \text{Hom}_R(R, R)$ by $\Psi(\varphi) = \varphi(1)$. $\text{Hom}_R(R, R)$ is closed under composition, and is a ring under the + of $\text{Hom}_R(R, R)$ together with $\circ$. To show $\text{Hom}_R(R, R)$ and $R$ are isomorphic as rings we must show that composition in $\text{Hom}_R(R, R)$ is mapped to multiplication in $R$.

Define $\Psi$ and $\xi$ as above, but with $R$ in place of $M$, so the definitions are $\Psi(\varphi) = \varphi(1)$ and $\xi_m(r) = rm$ with $\varphi \in \text{Hom}_R(R, R)$ and $r, m \in R$. It was shown above that $\Psi$ is a bijection, hence its inverse is surjective. It was proved above that the inverse of $\Psi$ is the map $\xi$ that sends $m \in R$ to $\xi_m \in \text{Hom}_R(R, R)$, so $\varphi = \xi_{\varphi(1)}$ and $\psi = \xi_{\psi(1)}$. Then

$$\Psi(\varphi \circ \psi) = \Psi(\xi_{\varphi(1)} \circ \xi_{\psi(1)}) \quad \text{Psi and } \xi \text{ are inverses}$$

$$= (\xi_{\varphi(1)} \circ \xi_{\psi(1)})(1) \quad \text{def of } \Psi$$

$$= \xi_{\varphi(1)}(\xi_{\psi(1)}(1)) \quad \text{def of } \circ$$

$$= \xi_{\varphi(1)}(1\psi(1)) \quad \text{def of } \xi_{\psi(1)}$$

$$= (1\psi(1))\varphi(1) \quad \text{def of } \xi_{\varphi(1)}$$
\[
\begin{align*}
= \psi(1)\varphi(1) \\
= \Psi(\psi)\Psi(\varphi) & \text{ def of } \Psi \\
= \Psi(\varphi)\Psi(\psi) & \text{ } R \text{ is commutative}
\end{align*}
\]

10.3.12 Let \( R \) be a commutative ring and let \( A, B \) and \( M \) be \( R \)-modules. Prove the following isomorphisms of \( R \)-modules.

(a) \( \text{Hom}_R(A \times B, M) \cong \text{Hom}_R(A, M) \times \text{Hom}_R(B, M) \)

(b) \( \text{Hom}_R(M, A \times B) \cong \text{Hom}_R(M, A) \times \text{Hom}_R(M, B) \)

First some observations on both parts. Since \( R \) is a commutative ring, it follows by Prop. 10.2 that \( \text{Hom}_R(A, M), \text{Hom}_R(B, M), \text{Hom}_R(M, A), \text{Hom}_R(M, B), \text{Hom}_R(A \times B, M) \), and \( \text{Hom}_R(M, A \times B) \) are \( R \)-modules, so \( \text{Hom}_R(A, M) \times \text{Hom}_R(B, M) \) and \( \text{Hom}_R(M, A) \times \text{Hom}_R(M, B) \) are also \( R \)-modules (since they are direct products of \( R \)-modules).

(a) An arbitrary element of \( \text{Hom}_R(A, M) \times \text{Hom}_R(B, M) \) is an ordered pair \((\alpha_1, \beta_1)\) consisting of \( \alpha_1 \in \text{Hom}_R(A, M) \) and \( \beta_1 \in \text{Hom}_R(B, M) \). Given an arbitrary pair of module homomorphisms

\[
(\alpha_1, \beta_1) \in \text{Hom}_R(A, M) \times \text{Hom}_R(B, M),
\]

define a map \( \Psi(\alpha_1, \beta_1) : A \times B \to M \) by \( \Psi(\alpha_1, \beta_1)(a, b) = \alpha_1(a) + \beta_1(b) \) for all \( a \in A \) and all \( b \in B \). We show now that \( \Psi(\alpha_1, \beta_1) \in \text{Hom}_R(A \times B, M) \). For all \( a_1, a_2 \in A, b_1, b_2 \in B, \) and \( r \in R \) we have

\[
\begin{align*}
\Psi(\alpha_1, \beta_1)((a_1, b_1) + (a_2, b_2)) &= \Psi(\alpha_1, \beta_1)(a_1 + a_2, b_1 + b_2) & \text{def of } + \text{ in } A \times B \\
&= \alpha_1(a_1 + a_2) + \beta_1(b_1 + b_2) & \text{def of } \Psi \\
&= (\alpha_1(a_1) + \alpha_1(a_2)) + (\beta_1(b_1) + \beta_1(b_2)) & \alpha_1, \beta_1 \text{ are } R\text{-module homs} \\
&= \alpha_1(a_1) + \beta_1(b_1) + \alpha_1(a_2) + \beta_1(b_2) & \text{properties of } + \\
&= \Psi(\alpha_1, \beta_1)(a_1, b_1) + \Psi(\alpha_1, \beta_1)(a_2, b_2) & \text{def of } \Psi \\
\Psi(\alpha_1, \beta_1)(r(a_1, b_1)) &= \Psi(\alpha_1, \beta_1)(ra_1, rb_1) & \text{def of action of } R \text{ on } A \times B
\end{align*}
\]
\[ \alpha_1(r\alpha_1) + \beta_1(r\beta_1) \quad \text{def of } \Psi \]
\[ = r\alpha_1(a_1) + r\beta_1(b_1) \quad \alpha_1, \beta_1 \text{ are } R\text{-module homs} \]
\[ = r(\alpha_1(a_1) + \beta_1(b_1)) \quad \text{module axiom} \]
\[ = r\Psi(\alpha_1, \beta_1)(a_1, b_1) \quad \text{def of } \Psi \]

This shows that \( \Psi : \Hom_R(A, M) \times \Hom_R(B, M) \rightarrow \Hom_R(A \times B, M) \).

Now we must show that \( \Psi \) is itself an \( R \)-module homomorphism from the \( R \)-module \( \Hom_R(A, M) \times \Hom_R(B, M) \) to the \( R \)-module \( \Hom_R(A \times B, M) \). Let \( \alpha_1, \alpha_2 \in \Hom_R(A, M) \) and \( \beta_2, \beta_1 \in \Hom_R(A, M) \), so that we have

\[ (\alpha_1, \beta_1), (\alpha_2, \beta_2) \in \Hom_R(A, M) \times \Hom_R(B, M) \]

We wish to show

(1) \( \Psi((\alpha_1, \beta_1) + (\alpha_2, \beta_2)) = \Psi(\alpha_1, \beta_1) + \Psi(\alpha_2, \beta_2) \)

and

(2) \( \Psi(r(\alpha_1, \beta_1)) = r\Psi(\alpha_1, \beta_1) \)

For all \( a \in A, b \in B, \) and \( r \in R \) we have

\[ \Psi((\alpha_1, \beta_1) + (\alpha_2, \beta_2))(a, b) \]
\[ = \Psi(\alpha_1 + \alpha_2, \beta_1 + \beta_2)(a, b) \quad \text{def of + in } \Hom_R(A, M) \times \Hom_R(B, M) \]
\[ = ((\alpha_1 + \alpha_2)(a), (\beta_1 + \beta_2)(b)) \quad \text{def of } \Psi \]
\[ = (\alpha_1(a) + \alpha_2(a), \beta_1(b) + \beta_2(b)) \quad \text{def of + in } \Hom_R(A, M) \text{ and } \Hom_R(B, M) \]
\[ = (\alpha_1(a), \beta_1(b)) + (\alpha_2(a), \beta_2(b)) \quad \text{def of + in } A \times B \]
\[ = \Psi(\alpha_1, \beta_1)(a, b) + \Psi(\alpha_2, \beta_2)(a, b) \quad \text{def of } \Psi \]

This calculation shows that (1) holds. For (2) we have

\[ \Psi(r(\alpha_1, \beta_1))(a, b) \]
\[ = \Psi(r\alpha_1, r\beta_1)(a, b) \quad \text{def of } R\text{-action on } \Hom_R(A, M) \times \Hom_R(B, M) \]
\[ = ((r\alpha_1)(a), (r\beta_1)(b)) \quad \text{def of } \Psi \]
\[ = (r(\alpha_1(a)), r(\beta_1(b))) \quad \text{def of } R\text{-action on } \Hom_R(A, M) \text{ and on } \Hom_R(B, M) \]
\[ = r(\alpha_1(a), \beta_1(b)) \quad \text{def of } R\text{-action on } A \times B \]
\[ r \Psi(\alpha_1, \beta_1)(a, b) \quad \text{def of } \Psi \]

Finally we must show \( \Psi \) is a bijection.

To show \( \Psi \) is injective, assume \( \Psi(\alpha_1, \beta_1) = \Psi(\alpha_2, \beta_2) \) where \( \alpha_1, \alpha_2 \in \text{Hom}_R(A, M) \) and \( \beta_2, \beta_1 \in \text{Hom}_R(A, M) \). We must show \( (\alpha_1, \beta_1) = (\alpha_2, \beta_2) \). First note that for all \( a \in A \) and \( b \in B \), we have \( \Psi(\alpha_1, \beta_1)(a, b) = \Psi(\alpha_2, \beta_2)(a, b) \), hence \( \alpha_1(a) + \beta_1(b) = \alpha_2(a) + \beta_2(b) \) by the definition of \( \Psi \). In particular, for every \( a \in A \) we have \( \alpha_1(a) + \beta_1(0) = \alpha_2(a) + \beta_2(0) \), but \( \beta_1(0) = \beta_2(0) = 0 \) since \( \beta_1 \) and \( \beta_2 \) are module homomorphisms, so we have \( \alpha_1(a) = \alpha_2(a) \) for all \( a \in A \), which tells us that \( \alpha_1 = \alpha_2 \). Similarly, for every \( b \in B \) we have \( \beta_1(b) = \alpha_1(0) + \beta_1(b) = \alpha_2(0) + \beta_2(b) = \beta_2(b) \), so \( \beta_1 = \beta_2 \). From \( \alpha_1 = \alpha_2 \) and \( \beta_1 = \beta_2 \) we get \( (\alpha_1, \beta_1) = (\alpha_2, \beta_2) \).

To show \( \Psi \) is surjective, consider an arbitrary \( \varphi \in \text{Hom}_R(A \times B, M) \). Define \( \varphi_1 : A \to M \) by \( \varphi_1(a) = \varphi(a, 0) \) for all \( a \in A \), and define \( \varphi_2 : B \to M \) by \( \varphi_2(b) = \varphi(0, b) \). Then \( \varphi_1 \) and \( \varphi_2 \) are \( R \)-module homomorphisms, so \( \varphi_1 \in \text{Hom}_R(A, M) \) and \( \varphi_2 \in \text{Hom}_R(B, M) \). For all \( a \in A \) and \( b \in B \),

\[
\Psi(\varphi_1, \varphi_2)(a, b) \\
= \varphi_1(a) + \varphi_2(b) \quad \text{def of } \Psi \\
= \varphi(a, 0) + \varphi(0, b) \quad \text{def of } \varphi_1 \text{ and } \varphi_2 \\
= \varphi((a, 0) + (0, b)) \quad \varphi \text{ is a module homomorphism} \\
= \varphi(a, b) \quad \text{def of } + \text{ in } A \times B
\]

This calculation shows that \( \Psi(\varphi_1, \varphi_2) = \varphi \).

(b) We will define a map

\[ \Phi : \text{Hom}_R(M, A) \times \text{Hom}_R(M, B) \to \text{Hom}_R(M, A \times B) \]

as follows. First, for an arbitrary pair \( (\alpha_1, \beta_1) \in \text{Hom}_R(M, A) \times \text{Hom}_R(M, B) \), where \( \alpha_1 \in \text{Hom}_R(M, A) \) and \( \beta_1 \in \text{Hom}_R(M, B) \), let \( \Phi(\alpha_1, \beta_1) \) be the map from \( M \) to \( A \times B \) defined for all \( x \in M \) by \( \Phi(\alpha_1, \beta_1)(x) = (\alpha_1(x), \beta_1(x)) \). We show now that \( \Phi(\alpha_1, \beta_1) \) is actually an \( R \)-module homomorphism from \( M \) to the \( R \)-module \( A \times B \). For all
\( x, y \in M \) and \( r \in R \) we have

\[
\Phi(\alpha_1, \beta_1)(x + y) = (\alpha_1(x + y), \beta_1(x + y)) \quad \text{def of } \Phi
\]
\[
= (\alpha_1(x) + \alpha_1(y), \beta_1(x) + \beta_1(y)) \quad \alpha_1, \beta_1 \text{ are } R\text{-module homs}
\]
\[
= (\alpha_1(x), \beta_1(x)) + (\alpha_1(y), \beta_1(y)) \quad \text{def + of in } A \times B
\]
\[
= \Phi(\alpha_1, \beta_1)(x) + \Phi(\alpha_1, \beta_1)(y) \quad \text{def of } \Phi
\]

\[
\Phi(\alpha_1, \beta_1)(rx) = (r\alpha_1(x), r\beta_1(x)) \quad \alpha_1, \beta_1 \text{ are } R\text{-module homs}
\]
\[
= r(\alpha_1(x), \beta_1(x)) \quad \text{def of action of } R \text{ on } A \times B
\]
\[
= r\Phi(\alpha_1, \beta_1)(x) \quad \text{def of } \Phi
\]

so \( \Phi(\alpha_1, \beta_1) \) is an \( R\)-module homomorphism from \( M \) into \( A \times B \).

Now we must show that \( \Phi \) is itself an \( R\)-module homomorphism from the \( R\)-module \( \text{Hom}_R(M, A) \times \text{Hom}_R(M, B) \) to the \( R\)-module \( \text{Hom}_R(M, A \times B) \). Let \( \alpha_1, \alpha_2 \in \text{Hom}_R(M, A) \) and \( \beta_2, \beta_1 \in \text{Hom}_R(M, B) \), so that we have

\[
(\alpha_1, \beta_1), (\alpha_2, \beta_2) \in \text{Hom}_R(M, A) \times \text{Hom}_R(M, B)
\]

We wish to show

\[
\Phi((\alpha_1, \beta_1) + (\alpha_2, \beta_2)) = \Phi(\alpha_1, \beta_1) + \Phi(\alpha_2, \beta_2)
\]

and

\[
\Phi(r(\alpha_1, \beta_1)) = r\Phi(\alpha_1, \beta_1)
\]

For every \( x \in M \) and \( r \in R \) we have

\[
\Phi((\alpha_1, \beta_1) + (\alpha_2, \beta_2))(x)
\]
\[
= \Phi(\alpha_1 + \alpha_2, \beta_1 + \beta_2)(x) \quad \text{def of + in } \text{Hom}_R(M, A) \times \text{Hom}_R(M, B)
\]
\[
= ((\alpha_1 + \alpha_2)(x), (\beta_1 + \beta_2)(x)) \quad \text{def of } \Phi
\]
\[
= (\alpha_1(x) + \alpha_2(x), \beta_1(x) + \beta_2(x)) \quad \text{def of + in } \text{Hom}_R(M, A) \text{ and } \text{Hom}_R(M, B)
\]
\[
= (\alpha_1(x), \beta_1(x)) + (\alpha_2(x), \beta_2(x)) \quad \text{def of + in } A \times B
\]
\[ \Phi(\alpha_1, \beta_1)(x) + \Phi(\alpha_2, \beta_2)(x) \quad \text{def of } \Phi \]

\[ \Phi(r(\alpha_1, \beta_1))(x) \]
\[ = \Phi(r\alpha_1, r\beta_1)(x) \quad \text{def of } R\text{-action on } \text{Hom}_R(M, A) \times \text{Hom}_R(M, B) \]
\[ = ((r\alpha_1)(x), (r\beta_1)(x)) \quad \text{def of } \Phi \]
\[ = (r(\alpha_1(x)), r(\beta_1(x))) \quad \text{def of } R\text{-action on } \text{Hom}_R(M, A), \text{ and } \text{Hom}_R(M, B) \]
\[ = r(\alpha_1(x), \beta_1(x)) \quad \text{def of } R\text{-action on } A \times B \]
\[ = r\Phi(\alpha_1, \beta_1)(x) \quad \text{def of } \Phi \]

Finally, we show \( \Phi \) is bijective.

To show \( \Phi \) is injective, assume \( \Phi(\alpha_1, \beta_1) = \Phi(\alpha_2, \beta_2) \) where \( \alpha_1, \alpha_2 \in \text{Hom}_R(A, M) \) and \( \beta_2, \beta_1 \in \text{Hom}_R(B, M) \). Then for all \( x \in M \) we have \( \Phi(\alpha_1, \beta_1)(x) = \Phi(\alpha_2, \beta_2)(x) \), hence \( (\alpha_1(x), \beta_1(x)) = (\alpha_2(x), \beta_2(x)) \), hence \( \alpha_1(x) = \alpha_2(x) \) and \( \beta_1(x) = \beta_2(x) \). This shows \( \alpha_1 = \alpha_2 \) and \( \beta_1 = \beta_2 \), so \( (\alpha_1, \alpha_2) = (\beta_1, \beta_2) \).

To show \( \Psi \) is surjective, consider an arbitrary \( \varphi \in \text{Hom}_R(M, A \times B) \). Let \( \pi_1 \) and \( \pi_2 \) be the \( R \)-module homomorphisms that project \( A \times B \) onto \( A \), and \( B \), respectively: \( \pi_1 : A \times B \to A \) and \( \pi_2 : A \times B \to B \). Then for all \( x \in M \) we have
\[ \Psi(\pi_1 \circ \varphi, \pi_2 \circ \varphi)(x) = ((\pi_1 \circ \varphi)(x), (\pi_2 \circ \varphi)(x)) \quad \text{def of } \Phi \]
\[ = (\pi_1(\varphi(x)), \pi_2(\varphi(x))) \quad \text{def of } \circ \]
\[ = \varphi(x) \quad \text{def of } \pi_1 \text{ and } \pi_2 \]

so \( \Psi(\pi_1 \circ \varphi, \pi_2 \circ \varphi) = \varphi \).

10.3.13 Let \( R \) be a commutative ring and let \( F \) be a free \( R \)-module of finite rank. Prove the following isomorphism of \( R \)-modules:
\[ \text{Hom}_R(F, R) \cong F \]

Assume \( M \) is free module of finite rank \( n < \omega \) and let \( X = \{x_1, \ldots, x_n\} \subseteq F \) be a free basis for \( F \). Every \( R \)-module homomorphism \( \varphi \in \text{Hom}_R(F, R) \) obviously determines a map \( f : X \to R \), where \( f(x) = \varphi(x) \in R \) for every \( x \in X \). Conversely, since \( X \) is a free basis, every function
\( f : X \to R \) determines a unique \( R \)-module homomorphism \( \varphi : F \to R \) extending \( f \).

Let \( \Psi \) be the map that sends each \( R \)-module homomorphism \( \varphi \in \text{Hom}_R(F, R) \) to \( \varphi(x_1)x_1 + \cdots + \varphi(x_n)x_n \in F \), so

\[
\Psi(\varphi) = \varphi(x_1)x_1 + \cdots + \varphi(x_n)x_n
\]

To see that \( \Psi \) is surjective, consider an arbitrary element of \( F \), which has the form \( a_1x_1 + \cdots + a_nx_n \) for some \( a_1, \ldots, a_n \in R \). Define \( f : X \to R \) by setting \( f(x_i) = a_i \) for \( 1 \leq i \leq n \), and let \( \varphi \) be the unique \( R \)-module homomorphism extending \( f \). Then

\[
\Psi(\varphi) = \varphi(x_1)x_1 + \cdots + \varphi(x_n)x_n = f(x_1)x_1 + \cdots + f(x_n)x_n = a_1x_1 + \cdots + a_nx_n.
\]

To see that \( \Psi \) is injective, suppose \( \Psi(\varphi) = \Psi(\psi) \). Then \( \varphi(x_1)x_1 + \cdots + \varphi(x_n)x_n = \psi(x_1)x_1 + \cdots + \psi(x_n)x_n \), but \( X \) is a free basis, so representations of elements as linear combinations of elements of \( X \) are unique, hence \( \varphi(x_1) = \psi(x_1), \ldots, \varphi(x_n) = \psi(x_n) \), so \( \varphi = \psi \) because \( R \)-module homomorphisms that agree on the free basis \( X \) must be the same by uniqueness. Finally, the following calculations show \( \Psi \) is a homomorphism.

\[
\Psi(\varphi) + \Psi(\psi) = (\varphi(x_1)x_1 + \cdots + \varphi(x_n)x_n) + (\psi(x_1)x_1 + \cdots + \psi(x_n)x_n)
\]

\[
= (\varphi(x_1)x_1 + \psi(x_1)x_1) + \cdots + (\varphi(x_n)x_n + \psi(x_n)x_n)
\]

\[
= (\varphi(x_1) + \psi(x_1))x_1 + \cdots + (\varphi(x_n) + \psi(x_n))x_n
\]

\[
= \Psi(\varphi + \psi)
\]

\[
\Psi(r\varphi) = ((r\varphi)(x_1))x_1 + \cdots + ((r\varphi)(x_n))x_n \quad \text{def of } \Psi
\]

\[
= (r\varphi(x_1))x_1 + \cdots + (r\varphi(x_n))x_n \quad \text{def of action of } R \text{ on } \text{Hom}
\]

\[
= r(\varphi(x_1)x_1) + \cdots + r(\varphi(x_n)x_n) \quad \text{module axiom}
\]
\[ = r(\varphi(x_1)x_1 + \cdots + \varphi(x_n)x_n) \quad \text{module axiom} \]
\[ = r(\Psi(\varphi)) \quad \text{def of } \Psi \]

**10.3.14** Let \( R \) be a commutative ring and let \( F \) be the free \( R \)-module of rank \( n \). Prove that \( \text{Hom}_R(F, M) \cong M \times \cdots \times M \) (\( n \) times). [Use Exercise 9 in Section 10.2 and Exercise 12.]

By (repeated or inductive use of) Exer. 10.3.12(a) above,

\[ \text{Hom}_R(R \times \cdots \times R, M) \cong \text{Hom}_R(R, M) \times \cdots \times \text{Hom}_R(R, M) \]

and by Exer. 10.2.9 above, \( \text{Hom}_R(R, M) \) and \( M \) are isomorphic as left \( R \)-modules, so

\[ \text{Hom}_R(R^n, M) \cong M \times \cdots \times M \]

However, \( R^n \) is the free \( R \)-module of rank \( n \), so \( F = R^n \), hence

\[ \text{Hom}_R(F, M) \cong M \times \cdots \times M \]

Homework #07, due 3/3/10 = 12.1.1, 12.1.2, 12.1.3, 10.3.18, 12.1.10

Additional problems recommended for study: 12.1.4, 12.1.5, 12.1.6, 12.1.7, 12.1.8, 12.1.9

**12.1.1** Let \( M \) be a module over the integral domain \( R \).

(a) Suppose \( x \) is a nonzero torsion element in \( M \). Show that \( x \) and 0 are “linearly dependent.” Conclude that the rank of \( \text{Tor}(M) \) is 0, so that in particular any torsion \( R \)-module has rank 0.

(b) Show that the rank of \( M \) is the same as the rank of the (torsion free) quotient \( M/\text{Tor}(M) \).

(a) Since \( x \) is a nonzero torsion element of \( M \), there exists some nonzero \( r \in R \) such that \( rx = 0 \). The rank of a module over an integral domain is the maximum number of linearly independent elements. A set of elements of a module is linearly dependent if some linear combination of them is 0, and yet not all of the coefficients are 0. The
equation $rx = 0$ is just such an example; a linear combination of the elements in \{x\} is 0, and yet not all coefficients are 0 (because $r \neq 0$), so it shows that \{x\} is not a linear independent set whenever $x$ is a torsion element. Every element in a torsion module is a torsion element, so a torsion module cannot have a linearly independent 1-element set, so the largest set of linearly independent elements is the empty set, so the rank of a torsion module is 0. In particular, the rank of the torsion submodule $\text{Tor}(M)$ of $M$ is 0.

(b) Let $N = \text{Tor}(M)$ be the torsion submodule of $M$. Suppose the rank of $M$ is $n$ and \{x_1, \cdots, x_n\} is a linearly independent set of elements of $M$. Suppose \{x_1 + N, x_2 + N, \cdots, x_n + N\} is not linearly independent in the quotient module $M/N$. Then there are coefficients $r_1, \cdots, r_n \in R$, not all zero, such that $r_1(x_1 + N) + \cdots + r_n(x_n + N) = N$. This implies $r_1x_1 + \cdots + r_n x_n \in N$, so $r_1x_1 + \cdots + r_n x_n$ is a torsion element. There is some nonzero $s \in R$ such that $s(r_1x_1 + \cdots + r_n x_n) = 0$, hence $sr_1x_1 + \cdots + sr_n x_n = 0$. But, since there is at least one nonzero coefficient, say $r_i \neq 0$, and $s \neq 0$, we get $sr_i \neq 0$ because $R$ is an integral domain. Since not all the coefficients $sr_1, \cdots, sr_n$ are zero and $sr_1x_1 + \cdots + sr_n x_n = 0$, we conclude that \{x_1, \cdots, x_n\} is linearly dependent, contradicting the hypothesis. This shows that \{x_1 + N, x_2 + N, \cdots, x_n + N\} is linearly independent, so the rank of the quotient $M/N$ is at least $n$.

The rank of $M/N$ cannot be more than $n$, because if we consider an arbitrary set of $n + 1$ elements of $M/N$, say $y_1 + N, \ldots, y_{n+1} + N$ with $y_1, \cdots, y_{n+1} \in M$, then \{y_1, \cdots, y_{n+1}\} is linearly dependent since $M$ has rank $n$, so $r_1y_1 + \cdots + r_{n+1}y_{n+1} = 0$ for some $r_1, \cdots, r_{n+1} \in R$, not all zero, hence

$$N = 0 + N$$
$$= r_1y_1 + \cdots + r_{n+1}y_{n+1} + N$$
$$= r_1y_1 + N + \cdots + r_{n+1}y_{n+1} + N$$
$$= r_1(y_1 + N) + \cdots + r_{n+1}(y_{n+1} + N)$$

which shows that \{y_1 + N, \cdots, y_{n+1} + N\} is linearly dependent in $M/N$. Therefore the ranks of $M$ and $M/\text{Tor}(M)$ are the same.
12.1.2 Let $M$ be a module over the integral domain $R$.

(a) Suppose that $M$ has rank $n$ and $x_1, x_2, \ldots, x_n$ is any maximal set of linearly independent elements of $M$. Let $N = Rx_1 + \cdots + Rx_n$ be the submodule generated by $x_1, x_2, \ldots, x_n$. Prove that $N$ is isomorphic to $R^n$ and that the quotient $M/N$ is a torsion $R$-module (equivalently, the elements $x_1, \ldots, x_n$ are linearly independent and for any $y \in M$ there is a nonzero element $r \in R$ such that $ry$ can be written as a linear combination $r_1x_1 + \cdots + r_nx_n$ of the $x_i$).

(b) Prove conversely that if $M$ contains a submodule $N$ that is free of rank $n$ (i.e., $N \cong R^n$) such that the quotient $M/N$ is a torsion $R$-module then $M$ has rank $n$. [Let $y_1, y_2, \ldots, y_{n+1}$ be any $n+1$ elements of $M$. Use the fact that $M/N$ is torsion to write $r_iy_i$ as a linear combination of a basis for $N$ for some nonzero elements $r_1, \ldots, r_{n+1}$ of $R$. Use an argument as in the proof of Proposition 3 to see that the $r_iy_i$, and hence also the $y_i$, are linearly dependent.]

(a) This proof proceeds by a direct construction of an isomorphism from $R^n$ to $N$ (rather than an appeal to theorems of Chapter 10).

Define $\varphi : R^n \to N$ by $\varphi(r_1, \ldots, r_n) = r_1x_1 + \cdots + r_nx_n$ for all $r_1, \ldots, r_n \in R$. Then $\varphi$ is obviously surjective, just by the definition of $N$. To show $\varphi$ is injective, assume there are two elements of $R^n$, $(r_1, \ldots, r_n)$ and $(s_1, \ldots, s_n)$, such that $\varphi(r_1, \ldots, r_n) = \varphi(s_1, \ldots, s_n)$. Then $r_1x_1 + \cdots + r_nx_n = s_1x_1 + \cdots + s_nx_n$ by the definition of $\varphi$, so $(r_1 - s_1)x_1 + \cdots + (r_n - s_n)x_n = 0$ by module arithmetic. But then $r_1 - s_1 = 0, \ldots, r_n - s_n = 0$ by the linear independence of $\{x_1, \ldots, x_n\}$, so $r_1 = s_1, \ldots, r_n = s_n$, hence $(r_1, \ldots, r_n) = (s_1, \ldots, s_n)$. Thus $\varphi$ is injective.

To check $\varphi$ is a module homomorphism, consider two arbitrary elements $(r_1, \ldots, r_n), (s_1, \ldots, s_n) \in R^n$. Then

$$
\varphi\left((r_1, \ldots, r_n) + (s_1, \ldots, s_n)\right) = \varphi(r_1 + s_1, \ldots, r_n + s_n) \quad \text{def of } + \text{ in } R^n
$$
\[
= (r_1 + s_1)x_1 + \cdots + (r_n + s_n)x_n \quad \text{def of } \varphi \\
= (r_1 x_1 + \cdots + r_n x_n) + (s_1 x_1 + \cdots + s_n x_n) \quad \text{module arithmetic} \\
= \varphi(r_1, \cdots, r_n) + \varphi(s_1, \cdots, s_n) \quad \text{def of } \varphi
\]

and, for all \( r \in R \),
\[
\varphi\left(r(r_1, \cdots, r_n)\right) \\
= \varphi(rr_1, \cdots, rr_n) \quad \text{def of action of } R \text{ on } R^n \\
= (rr_1)x_1 + \cdots + (rr_n)x_n \quad \text{def of } \varphi \\
= r(r_1 x_1 + \cdots + r_n x_n) \quad \text{module arithmetic} \\
= r\varphi(r_1, \cdots, x_n) \quad \text{def of } \varphi
\]

Now we show that the quotient \( M/N \) is a torsion \( R \)-module. We need to show every nonzero element of the quotient is torsion because it can be annihilated by a nonzero element of \( R \). Let \( y + N \in M/N \) where \( y \in M \) and \( y \notin N \), so that \( y + N \) is nonzero in \( M/N \). Note that, in particular, \( y \notin \{x_1, \cdots, x_n\} \). Since \( \{x_1, \cdots, x_n\} \) is a maximal linear independent set, the strictly larger set \( \{y, x_1, \cdots, x_n\} \) must be linearly dependent, so there are coefficients \( s, r_1, \cdots, r_n \in R \), not all zero, such that \( sy + r_1 x_1 + \cdots + r_n x_n = 0 \). We cannot have \( s = 0 \), otherwise \( r_1 x_1 + \cdots + r_n x_n = 0 \) and one of the coefficients \( r_1, \cdots, r_n \) is nonzero, contradicting the linear independence of \( \{x_1, \cdots, x_n\} \). But then we have \( sy = -r_1 x_1 - \cdots - r_n x_n \in N \), hence \( sy + N = s(y + N) = N \), i.e., \( s(y + N) \) is zero in the quotient \( M/N \).

**(b)** Assume \( M \) contains a submodule \( N \) that is free of rank \( n \) (i.e., \( N \cong R^n \)) and the quotient \( M/N \) is a torsion \( R \)-module. We will show that \( M \) has rank \( n \).

Since \( N \) has rank \( n \), it contains a maximal linearly independent subset \( X = \{x_1, \cdots, x_n\} \subseteq N \). Then \( X \) is also a linearly independent subset of \( M \) with cardinality \( n \), so the rank of \( M \) has to be at least \( n \).

We need only show that the rank of \( M \) can be at most \( n \). To that end, let \( y_1, y_2, \cdots, y_{n+1} \) be any \( n + 1 \) elements of \( M \). We want to show these elements are linearly dependent. The images \( y_1, y_2, \cdots, y_{n+1} \) in
the quotient module \( M/N \) are
\[ y_1 + N, y_2 + N, \ldots, y_{n+1} + N. \]
Since \( M/N \) is torsion, each of these elements has a nonzero element of \( R \) that annihilates it, that is, there are nonzero \( r_1, \ldots, r_{n+1} \in R \) such that
\[ r_1y_1 + N = r_2y_2 + N = \cdots = r_{n+1}y_{n+1} + N = N. \]
Note that if \( y_i \) is already in \( N \), we can use any nonzero \( r_i \in R \), and if \( y_i \) is not in \( N \), we use the fact that \( y_i + N \) is torsion in \( M/N \). Therefore we have \( \{r_1y_1, r_2y_2, \ldots, r_{n+1}y_{n+1}\} \subseteq N. \)

Let
\[ Y := \{r_1y_1, r_2y_2, \ldots, r_{n+1}y_{n+1}\}. \]

By a theorem proved in class\(^1\), the submodule of \( N \) generated by \( Y \) is free and has rank no more than the rank \( n \) of \( N \). Since \( Y \) has more than \( n \) elements, \( Y \) is linearly dependent, so there are coefficients \( s_1, s_2, \ldots, s_{n+1} \in R \), not all zero, such that
\[ s_1(r_1y_1) + s_2(r_2y_2) + \cdots + s_{n+1}(r_{n+1}y_{n+1}) = 0. \]

By module arithmetic, this equation says
\[ (s_1r_1)y_1 + (s_2r_2)y_2 + \cdots + (s_{n+1}r_{n+1})y_{n+1} = 0. \]
Note that not all the coefficients \( s_1r_1, s_2r_2, \ldots, s_{n+1}r_{n+1} \) are zero, because we know that some \( s_i \) is not zero and that all the \( r_i \) are not zero, hence \( s_i r_i \neq 0 \) because \( R \) is an integral domain. This shows that any set \( Y \subseteq M \) with \( n + 1 \) elements is linearly dependent, completing the proof that the rank of \( M \) is \( n \).

**12.1.3** Let \( R \) be an integral domain and let \( A \) and \( B \) be \( R \)-modules of ranks \( m \) and \( n \), respectively. Prove that the rank of \( A \oplus B \) is \( m + n \).
[Use the previous exercise.]

Let \( M = A \oplus B \). According to the meaning of \( \oplus \) in the text, this could mean that \( M \) is the external direct product of \( A \) and \( B \), i.e., \( M = A \times B \). However, I prefer to assume that \( A \) and \( B \) are submodules of \( M \) and

---

\(^1\)Th. Assume \( R \) is a P.I.D., \( M \) is a free module over \( R \) with finite rank \( n \), and \( N \) is a submodule of \( M \). Then \( N \) is a free submodule of \( M \) with rank no more than \( n \).
$M$ is the internal direct product of $A$ and $B$. This is also expressed by $M = A \oplus B$. This assumption implies that $A \cap B = \{0\}$.

Since the rank of $A$ is $m$, there is a maximal (in the submodule $A$) linearly independent subset $X = \{x_1, \cdots, x_m\} \subseteq A$. Similarly, since the rank $B$ is $n$, there is a maximal (in $B$) linearly independent subset $Y = \{y_1, \cdots, y_n\} \subseteq B$. Let $A_1 = Rx_1 + \cdots + Rx_m$ and $B_1 = Ry_1 + \cdots + Ry_n$. Then $A/A_1$ and $B/B_1$ are torsion modules by Exer. 12.1.2(a).

**Claim 1.** $X \cup Y$ is linearly independent in $M$.

**Proof:** Suppose some linear combination of elements of $X \cup Y$ is zero, say

$$r_1x_1 + \cdots + r_mx_m + s_1y_1 + \cdots + s.ny_n = 0$$

where $r_1, \cdots, r_m, s_1, \cdots, s_n \in R$. Let $z = r_1x_1 + \cdots + r_mx_m$. Then $z \in A_1 \subseteq A$, and $z = -s_1y_1 - \cdots - s.ny_n$ by (3), so $z \in B_1 \subseteq B$ as well. Then $z \in A \cap B = \{0\}$, so $z = 0$. Therefore $r_1 = \cdots = r_m = 0$ by the linear independence of $\{x_1, \cdots, x_m\}$, and $s_1 = \cdots = s_n = 0$ by the linear independence of $\{y_1, \cdots, y_n\}$. Thus all the coefficients in (3) are zero. This completes the proof of the Claim.

Let $M_1 = A_1 \oplus B_1$. Then $M_1$ is isomorphic to $R^{m+n}$ by Exer. 12.1.2(a), and is thus a free $R$-module of rank $m + n$.

**Claim 2.** $M/M_1$ is torsion.

**Proof:** Assume $0 \neq w \in M$. Then, since $M = A \oplus B$, there are unique $a \in A$ and $b \in B$ such that $w = a + b$. Now $A/A_1$ is torsion, so some nonzero $r \in R$ annihilates $a + A_1$, that is, $r(a + A_1) = A_1$, so $ra \in A_1$. Similarly, $B/B_1$ is torsion, so there is some nonzero $s \in R$ such that $sb \in B_1$. Note that $rs = sr$ since $R$ is an integral domain and hence is commutative. Then we have $rsz = rs(a + b) = rsa + rsb = s(ra) + r(sb) \in A_1 + B_1 = M_1$. Note that $rs$ is nonzero since $R$ is an integral domain and $s \neq 0 \neq r$. Thus $rs(z + M_1) = rsz + M_1 = M_1$, so $z + M_1$ is annihilated by the nonzero $rs \in R$.

It follows from Claims 1 and 2 by Exer. 12.1.2(b) that the rank of $M$ is $m + n$. 
10.3.18 Let \( R \) be a Principal Ideal Domain and let \( M \) be an \( R \)-module that is annihilated by the proper, nonzero ideal \( (a) \). Let \( a = p_1^{\alpha_1}p_2^{\alpha_2} \cdots p_k^{\alpha_k} \) be the unique factorization of \( a \) into distinct prime powers in \( R \). Let \( M_i \) be the annihilator of \( p_i^{\alpha_i} \), i.e., \( M_i \) is the set \( \{ m \in M | p_i^{\alpha_i}m = 0 \} \) — called the \( p_i \)-primary component of \( M \). Prove that

\[
M = M_1 \oplus M_2 \oplus \cdots \oplus M_k
\]

This problem, assigned after covering Section 12.1, can be solved by the Primary Decomposition Theorem 12.7. By the way, for a prime \( p \in \mathbb{Z} \), the \( p \)-primary component of a finite abelian group is the subgroup of elements whose order is a power of \( p \) (p. 142). In Exer. 10.3.22, if \( p \) is a prime in the PID \( R \), the \( p \)-primary component of a torsion \( R \)-module is the set of elements annihilated by some positive power of \( p \).

Exer. 10.3.18 follows directly as a special case of part of Th. 12.7, (the Primary Decomposition Theorem), which states that if \( R \) is a PID, \( M \) is a nonzero torsion \( R \)-module with nonzero annihilator \( a = up_1^{\alpha_1} \cdots p_n^{\alpha_n} \), where \( u \in R^{\times} \) is a unit of \( R \) and \( p_1, \ldots, p_n \in R \) are distinct primes of \( R \), and \( N_i = \{ x \in M | p_i^{\alpha_i}x = 0 \} \), 1 \( \leq \) \( i \) \( \leq \) \( n \), then \( N_i \) is a submodule of \( M \) with annihilator \( p_i^{\alpha_i} \), \( N_i \) is the \( p_i \)-primary component of \( M \), and \( M = N_1 \oplus \cdots \oplus N_n \). The remaining part of Th. 12.7 is that if \( M \) is finitely generated then \( N_i \) is the direct sum of finitely many cyclic modules whose annihilators are divisors of \( p_i^{\alpha_i} \).

12.1.10 For \( p \) a prime in the P.I.D. \( R \) and \( N \) an \( R \)-module prove that the \( p \)-primary component of \( N \) is a submodule of \( N \) and prove that \( N \) is the direct sum of its \( p \)-primary components (there need not be finitely many of them).

There may be infinitely many \( p \)-primary components, perhaps one for every prime in \( R \). The proof cannot be completed unless \( N \) is assumed to be a torsion module.

\( N \) may not be finitely generated, so we have a situation in which various elements could be annihilated by arbitrarily large powers of a given prime \( p \in R \). Let \( N_p \) be the \( p \)-primary component of \( M \), i.e., the set of elements annihilated by a positive power of \( p \). Suppose \( x, y \in N_p \). Then
for some positive powers \( p^m \) and \( p^n \), with \( m, n \in \mathbb{Z}^+ \), we have \( p^m x = 0 = p^n y \). Then \( p^{m+n}(x-y) = p^{m+n}x - p^{m+n}y = p^n(p^m x) - p^n(p^m y) = 0 \), so \( x - y \in N_p \). If \( r \in R \), then \( p^n(rx) = r(p^m x) = r0 = 0 \) since \( R \) is commutative, so \( N_p \) is closed under the action of \( R \). Thus the \( p \)-primary component \( N_p \) of \( N \) is a submodule of \( N \). To show

\[
N = \bigoplus_{\text{prime } p \in R} N_p
\]

we must show, for an arbitrary prime \( q \in R \), that

\[
N_q \cap \bigoplus_{\text{prime } p \in R, p \neq q} N_p = \{0\}
\]

and that every element of \( N \) is the sum of elements in \( p \)-primary components (for which we need to assume \( N \) is torsion).

For (5), suppose \( x \in N_q \) and

\[
x \in \bigoplus_{\text{prime } p \in R, p \neq q} N_p.
\]

Then \( 0 = q^n x \) for some \( n \in \mathbb{Z}^+ \), and \( x \) is a finite sum of elements, each of which is annihilated by a positive power of a prime of \( R \) distinct from \( q \). Let \( r \) be the product of these prime power annihilators. By some simple module computations (actually carried out in the solution to Exer. 10.3.5 above), we get \( rx = 0 \). Since all the prime divisors of \( r \) are distinct from \( q \), the greatest common divisor of \( q^n \) and \( r \) is 1. Since \( R \) is a PID, there exist some \( s, t \in R \) such that \( 1 = sq^n + tr \). Hence \( x = 1x = (sq^n + tr)x = sq^n x + trx = s(q^n x) + t(rx) = s0 + t0 = 0 \), as desired.

Assume \( N \) is torsion, and let \( x \) be an arbitrary element of \( N \). Then \( x \) is annihilated by some nonzero \( r \in R \), so \( rx = 0 \). Since \( R \) is a PID, it is also a UFD, so \( r \) has a unique factorization into a finite product of finite powers of primes of \( R \), say \( r = p_1^{a_1} \cdots p_n^{a_n} \), where \( p_1, \ldots, p_n \) are distinct primes and \( a_1, \ldots, a_n \) are non-negative integers. We show next by induction on \( n \) that

\[
x \in N_{p_1} \oplus \cdots \oplus N_{p_n}
\]
If \( n = 1 \) then \( x \) is annihilated by a power of \( p_1 \) since \( r = p_1^{a_1} \) and 
\[ 0 = r x = p_1^{a_1} x, \quad \text{so} \quad x \in N_{p_1}. \]
Now we assume (7) holds for \( n \), and we will prove it for \( n + 1 \). Suppose \( r x = 0 \) where 
\[ r = p_1^{a_1} \cdots p_n^{a_n} p_{n+1}^{a_{n+1}}, \]
where \( p_1, \ldots, p_{n+1} \) are distinct primes in \( R \) and \( a_1, \ldots, a_{n+1} \) are non-negative integers. Then 
\[ 0 = r x = p_1^{a_1} \cdots p_n^{a_n} (p_{n+1}^{a_{n+1}} x) \]
so by the inductive hypothesis we have 
\[ p_{n+1}^{a_{n+1}} x \in N_{p_1} \oplus \cdots \oplus N_{p_n} \]  
(8)
We also have 
\[ 0 = r x = p_{n+1}^{a_{n+1}} (p_1^{a_1} \cdots p_n^{a_n} x) \]
since \( R \) is commutative, so 
\[ p_1^{a_1} \cdots p_n^{a_n} x \in N_{p_{n+1}} \]  
(9)
Notice that \( p_{n+1}^{a_{n+1}} \) and \( p_1^{a_1} \cdots p_n^{a_n} \) have no common factors and their greatest common divisor is 1. Hence there are \( s, t \in R \) such that 
\[ 1 = sp_{n+1}^{a_{n+1}} + tp_1^{a_1} \cdots p_n^{a_n}. \]
Multiplying both sides by \( x \), we get 
\[ x = sp_{n+1}^{a_{n+1}} x + t p_1^{a_1} \cdots p_n^{a_n} x \in (N_{p_1} \oplus \cdots \oplus N_{p_n}) \oplus N_{p_{n+1}} \]
by (8) and (9). This completes the proof of (7), which implies that \( x \) is in 
\[ \bigoplus_{\text{prime } p \in R} N_p, \]
as desired.

---

Homework #08, due 3/10/10 = 12.1.4, 12.1.5, 12.1.6, 12.1.7, 12.1.8, 12.1.9

12.1.4 Let \( R \) be an integral domain, let \( M \) be an \( R \)-module and let \( N \) be a submodule of \( M \). Suppose \( M \) has rank \( n \), \( N \) has rank \( r \) and the quotient \( M/N \) has rank \( s \). Prove that \( n = r + s \). [Let \( x_1, x_2, \cdots, x_s \) be elements of \( M \) whose images in \( M/N \) are a maximal set of independent elements and let \( x_{s+1}, x_{s+2}, \cdots, x_{s+r} \) be a maximal set of independent elements in \( N \). Prove that \( x_1, x_2, \cdots, x_{s+r} \) are linearly independent in \( M \) and that for any elements \( y \in M \) there is a nonzero element \( r \in R \) such that \( r y \) is a linear combination of these elements. Then use Exercise 12.1.2.]

Note first that the authors are using “\( r \)” with two quite different meanings, both as an integer and as an element of \( R \). Following the hint,
let \( x_1, x_2, \ldots, x_s \in M \) be elements whose images in \( M/N \) are a maximal set of independent elements and let \( x_{s+1}, x_{s+2}, \ldots, x_{s+r} \in N \) be a maximal set of independent elements in \( N \).

**Claim:** \( x_1, x_2, \ldots, x_{s+r} \) are linearly independent in \( M \).

Suppose \( a_1, \ldots, a_{s+r} \in R \) and

\[
(10) \quad a_1 x_1 + \cdots + a_s x_s + a_{s+1} x_{s+1} + \cdots + a_{s+r} x_{s+r} = 0.
\]

Note that \( x_{s+1}, x_{s+2}, \ldots, x_{s+r} \in N \), hence

\[
(11) \quad a_{s+1} x_{s+1} + \cdots + a_{s+r} x_{s+r} + N = N,
\]

so, applying to both sides of (10) the canonical module homomorphism that sends \( y \in M \) to the coset \( y + N \), we obtain

\[
(12) \quad a_1 x_1 + N + \cdots + a_s x_s + N = N,
\]

hence

\[
(13) \quad a_1(x_1 + N) + \cdots + a_s(x_s + N) = N,
\]

but we chose \( x_1, x_2, \ldots, x_s \in M \) so that \( x_1 + N, x_2 + N, \ldots, x_s + N \in M/N \) are independent elements, so from (13) we conclude that

\[
(14) \quad a_1 = \cdots = a_s = 0.
\]

Substituting these values back into (10) produces

\[
(15) \quad a_{s+1} x_{s+1} + \cdots + a_{s+r} x_{s+r} = 0.
\]

Since we chose independent elements \( x_{s+1}, x_{s+2}, \ldots, x_{s+r} \in N \), it follows that

\[
(16) \quad a_{s+1} = \cdots = a_{s+r} = 0.
\]

We have proved that (14) and (16) follow from (10), completing the proof of the Claim.

Let \( y \in M \). Then \( y + N \in M/N \). We chose \( x_1, x_2, \ldots, x_s \in M \) so that \( x_1 + N, x_2 + N, \ldots, x_s + N \in M/N \) is a maximal set of \( s \) independent elements, so the \( s+1 \) elements \( y + N, x_1 + N, x_2 + N, \ldots, x_s + N \in M/N \)
cannot be independent. There are coefficients $b, a_1, \cdots, a_s \in R$, not all zero, such that

$$\tag{17} b(y + N) + a_1(x_1 + N) + \cdots + a_s(x_s + N) = N,$$

which implies

$$\tag{18} z := by + a_1x_1 + \cdots + a_sx_s \in N.$$

Now if $b = 0$ then

$$\tag{19} a_1(x_1 + N) + \cdots + a_s(x_s + N) = N,$$

hence $a_1 = \cdots = a_s = 0$ by the independence of $x_1 + N, \cdots, x_s + N$, contradicting our assumption that not all coefficients are zero, so $b \neq 0$. (We could have used Exer. 12.1.2(a) here, as is done in the next paragraph.)

Let $L := Rx_{s+1} + Rx_{s+2} + \cdots + Rx_{s+r}$. Then $L$ is a submodule of $N$. Since $\{x_{s+1}, x_{s+2}, \cdots, x_{s+r}\} \subseteq N$ is a maximal set of independent elements in $N$, by Exer. 12.1.2(a) the quotient $N/L$ is torsion. Applying this to $z \in N$, we conclude there is some nonzero $c \in R$ such that $c(z + L) = L$, hence $cz \in L$. By the definitions of $z$ and $L$ this gives us

$$cz = c(by + a_1x_1 + \cdots + a_sx_s)$$
$$= cby + ca_1x_1 + \cdots + ca_sx_s$$
$$\in L = Rx_{s+1} + Rx_{s+2} + \cdots + Rx_{s+r}$$

which implies the existence of coefficients $a_{s+1}, \cdots, a_{s+r} \in R$ such that

$$\tag{20} cby + ca_1x_1 + \cdots + ca_sx_s = a_{s+1}x_{s+1} + \cdots + a_{s+r}x_{s+r}.$$

Let $r = cb$. Then $r \neq 0$ because $c \neq 0, b \neq 0$, and $R$ is an integral domain. From (20) we get

$$ry = -ca_1x_1 - \cdots - ca_sx_s + a_{s+1}x_{s+1} + \cdots + a_{s+r}x_{s+r},$$

which implies

$$\tag{21} ry \in Rx_1 + \cdots + Rx_s + Rx_{s+1} + \cdots + Rx_{s+r}.$$
We have shown that for every \( y \in M \) there is some nonzero \( r \in R \) such that (21), which says that the quotient module

\[
M/(Rx_1 + \cdots + Rx_s + Rx_{s+1} + \cdots + Rx_{s+r})
\]

is torsion. It follows by Exer. 12.1.2(b) that \( M \) has rank \( s + r \). By assumption, \( M \) has rank \( n \), so \( n = s + r \).

**12.1.5** Let \( R = \mathbb{Z}[x] \) and let \( M = (2, x) \) be the ideal generated by 2 and \( x \), considered as a submodule of \( R \). Show that \( \{2, x\} \) is not a basis of \( M \). [Find a nontrivial \( R \)-linear dependence between these two elements.] Show that the rank of \( M \) is 1 but that \( M \) is not free of rank 1 (cf. Exercise 12.1.2).

Since \( R \) contains (a copy of) \( \mathbb{Z} \), the submodule \( M \) of \( R \) generated by \( x \) and 2 contains all multiples of \( x \), and all sums of such multiples, so it contains all polynomials with constant 0. But \( M \) also contains all multiples of 2, hence all even integers, and these can be constants in polynomials in \( M \), so \( M \) consists of those polynomials in \( \mathbb{Z}[x] \) whose constant is even.

The two elements 2 and \( x \) of the \( R \)-module \( \mathbb{Z}[x] \) satisfy the relation \( x \cdot 2 + (-2)x = 0 \), where \( x \) and \(-2\) are coefficients in the ring \( \mathbb{Z}[x] \), so the set \( \{2, x\} \) is not independent. In fact, no 2-element subset \( \{p, q\} \subseteq M \) can be independent, since \( q \cdot p + (-p)q = 0 \). Note that \( p \) and \( q \) can’t both be zero, otherwise \( \{p, q\} \) has only one element, so the coefficients in the relation \( q \cdot p + (-p)q = 0 \) are not both zero. Thus the rank of \( M \) cannot be 2. Now the singleton subset \( \{2\} \) of \( M \) is independent, for if \( r \in R \) and \( r \cdot 2 = 0 \), then \( r = 0 \). So the rank of \( M \) is at least 1. This shows the rank of \( M \) is 1.

To show \( M \) is not free of rank 1, we need assume otherwise and get a contradiction. Suppose there is a single polynomial \( p(x) \in M \) such that \( M = Rp(x) \). Note that \( Rp(x) \) is simply the ideal \( (p(x)) \) of \( \mathbb{Z}[x] = R \) generated by \( p(x) \). Then \( (2, x) = (p(x)) \) so there are polynomials \( q(x), s(x) \in \mathbb{Z}[x] = R \) such that \( 2 = p(x)q(x) \) and \( x = p(x)s(x) \). From \( 2 = p(x)q(x) \) it follows that these two polynomials are actually both constants, i.e., \( p(x) = p \in \mathbb{Z} \) and \( q(x) = q \in \mathbb{Z} \), hence \( 2 = pq \) and
\[ x = ps(x) \]. From \( 2 = pq \) we get \( \{p, q\} \subseteq \{\pm 1, \pm 2\} \). If \( p \) were \( \pm 1 \) then every polynomial would be a multiple of \( p \), contrary to the assumption that \( (p) = (2, x) \neq \mathbb{Z}[x] = R \). Therefore \( p \) is \( \pm 2 \), so by \( x = ps(x) \) we have \( x = \pm 2s(x) \), hence the coefficient of \( x \) (which is 1) is equal to the coefficient of \( x \) in the polynomial \( \pm 2s(x) \), but that coefficient is a multiple of 2, so again we have a contradiction. (This is the proof that \( (2, x) \) is a non-principal ideal of \( \mathbb{Z}[x] \).) This shows that \( M \) cannot be free of rank 1.

**12.1.6** Show that if \( R \) is an integral domain and \( M \) is any nonprincipal ideal of \( R \) then \( M \) is torsion free of rank 1 but is not a free \( R \)-module.

For every nonzero \( m \in M \subseteq R \), there is no nonzero \( r \in R \) such that \( rm = 0 \), because \( R \) is an integral domain and has no zero divisors. This shows that every submodule \( M \) of \( R \) (treated as \( R \)-modules) is torsion free.

Every submodule \( M \subseteq R \) has rank at least 1, for if \( m \in M \), then \( \{m\} \) is an independent set because if \( rm = 0 \) with \( r \in R \), then \( r = 0 \), as was just observed.

No submodule \( M \subseteq R \) has rank 2, for if nonzero \( m_1, m_2 \in M \) are distinct, then the equation \( m_1m_2 + (-m_2)m_1 = 0 \) shows that \( \{m_1, m_2\} \) is not independent.

If a submodule \( M \) is free of rank 1, then there is some generator \( g \in R \) such that \( M = Rg = (g) \), hence \( M \) is a principal ideal of \( R \). Therefore, if \( M \) is a nonprincipal ideal of \( R \), then \( M \) is a torsion free submodule of \( R \) with rank 1, but \( M \) is not free of rank 1.

**12.1.7** Let \( R \) be any ring, let \( A_1, A_2, \ldots, A_m \) be \( R \)-modules and let \( B_i \) be a submodule \( A_i \), \( 1 \leq i \leq m \). Prove that

\[
(A_1 \oplus A_2 \oplus \cdots \oplus A_m) / (B_1 \oplus B_2 \oplus \cdots \oplus B_m) 
\cong (A_1/B_1) \oplus (A_2/B_2) \oplus \cdots \oplus (A_m/B_m)
\]

No solution given here.

**12.1.8** Let \( R \) be a P.I.D., let \( B \) be a torsion \( R \)-module, and let \( p \) be a prime in \( R \). Prove that if \( pb = 0 \) for some nonzero \( b \in B \), then \( \text{Ann}(B) \subseteq (p) \).
We assume $R$ is a PID, $B$ is a torsion $R$-module, $p$ is prime in $R$, $pb = 0$, and $0 \neq b \in B$, and will show $\text{Ann}(B) \subseteq (p)$. Let $r \in \text{Ann}(B)$. This means that $\forall a \in B$, $ra = 0$. In particular, $rb = 0$. Since $R$ is a PID, there is some $d \in R$ such that $(r, p) = (d)$. Then $p \in (r, p) = (d)$, so $d | p$, so there is some $q \in R$ such that $dq = p$. But $p$ is prime in $R$, so either $p | d$ or $p | q$. \textbf{Case 1.} Suppose first that $p | d$. Then $(d) \subseteq (p) = (d)$, so $(p) = (d)$. In this case we have $r \in (r, p) = (d) = (p)$ so $p | r$ and $r \in (p)$, as desired. \textbf{Case 2} Suppose $p | q$. Then there is some $u \in R$ such that $pu = q$. But we saw earlier that $dq = p$, so we now have $p = dq = d(pu) = p(du)$, hence $1 = du$ by cancellation. (This implies that $d$ and $u$ are units of $R$.) Now $d \in (r, p)$, so there are $s, t \in R$ such that $d = rs + pt$. Then

\[
(22) \quad db = (rs + pt)b = s(rb) + t(pb) = s0 + t0 = 0 + 0 = 0,
\]

so $b = 1b = (du)b = u(db) = u0 = 0$, contradicting $b \neq 0$. This means that the second case cannot occur, so we’re done.

\textbf{12.1.9} Give an example of an integral domain $R$ and a nonzero torsion $R$-module $M$ such that $\text{Ann}(M) = 0$. Prove that if $N$ is a finitely generated torsion $R$-module then $\text{Ann}(N) \neq 0$.

Exer. 10.3.5 is essentially the same as this problem. Here’s a copy of my earlier solution to that problem, edited a little: \textbf{10.3.5} says, “Let $R$ be an integral domain. Prove that every finitely generated torsion $R$-module has a nonzero annihilator, \textit{i.e.}, there is a nonzero $r \in R$ such that $rm = 0$ for all $m \in M$—here $r$ does not depend on $m$ (the annihilator of a module was defined in Exer. 10.1.9). Give an example of a torsion $R$-module whose annihilator is the zero ideal.”

Solution: Assume $N$ is a finitely generated torsion $R$-module. Then there is a finite set $A \subseteq N$ of nonzero elements such that $N = RA$. Let $A = \{a_1, \ldots, a_k\}$, $k \in \omega$. Since $N$ is a torsion module, there exist nonzero elements $r_1, \ldots, r_k \in R$ such that $r_1a_1 = 0$, $r_2a_2 = 0$, \ldots, $r_ka_k = 0$. Let $q = r_1 \cdot \ldots \cdot r_k$. Consider an arbitrary element $n \in N$. Since $N = RA$, there are ring elements $s_1, \ldots, s_k \in R$ such that $n = s_1a_1 + \cdots + s_ka_k$. Let $1 \leq i \leq k$. Since $R$ is an integral domain, $R$ is commutative, so $q = pr_i$ where $p$ is the product of all the
other factors \( r_j \) with \( j \neq i \). Then \( qa_i = (pr_i)a_i = p(r_i a_i) = p0 = 0 \). This shows \( qa_1 = qa_2 = \cdots = qa_k = 0 \), so we have

\[
qn = q(s_1a_1 + \cdots + s_ka_k)
= q(s_1a_1) + \cdots + q(s_ka_k) \quad \text{module axiom}
= (qs_1)a_1 + \cdots + (qs_ka_k) \quad \text{module axiom}
= (s_1q)a_1 + \cdots + (s_ka_k) \quad \text{since } R \text{ is commutative}
= s_1(qa_1) + \cdots + s_k(qa_k) \quad \text{module axiom}
= s_1(0) + \cdots + s_k(0) \quad \text{shown above}
= 0 + \cdots + 0
= 0
\]

Since \( n \) was an arbitrary element of \( N \), we have shown that \( qn = 0 \) for every \( n \in N \). Finally, we observe that \( q \) is nonzero because \( r_i \neq 0 \) and the product of nonzero elements in the integral domain \( R \) cannot be zero.

For an example of a torsion \( R \)-module whose annihilator is the zero ideal, let \( R = \mathbb{Z} \), and let \( M \) be the direct sum of the finite cyclic groups \( \mathbb{Z}/k\mathbb{Z} \) with \( 2 \leq k \in \mathbb{Z}^+ \), so

\[
M = \bigoplus_{2 \leq k \in \mathbb{Z}^+} \mathbb{Z}/k\mathbb{Z}.
\]

Let \( m \in M \). Then there are \( k \in \mathbb{Z}^+ \) and \( a_1, \ldots, a_k \in \mathbb{Z} \) such that \( m = (a_1 + 2\mathbb{Z}, \ldots, a_k + k\mathbb{Z}, 0, 0, 0, \cdots) \), so \( k! \cdot m = 0 \), so \( m \in \text{Tor}(M) \). Then \( M \) is a torsion module, but no element of \( \mathbb{Z} \) annihilates every element of \( M \), for if \( k \in \mathbb{Z}^+ \) then \( k \cdot (\ldots, 1 + (k+1)\mathbb{Z}, 0, 0, \cdots) \neq 0 \).

---

Homework #09, due 3/24/10 = 12.2.2, 12.2.3, 12.2.4, 12.2.7, 12.2.8

12.2.2 Let \( M \) be as is Lemma 19. Prove that the minimal polynomial of \( M \) is the least common multiple of the minimal polynomials of \( A_1, \ldots, A_k \).
In Lemma 19, $F$ is a field and $M$ is the block diagonal matrix
\[
M = \begin{pmatrix}
A_1 & 0 & \cdots & 0 \\
0 & A_2 & \cdots & 0 \\
\vdots & \vdots & \ddots & \vdots \\
0 & 0 & \cdots & A_k
\end{pmatrix}
\]
where $A_1, \cdots, A_k$ are square matrices with entries in $F$. It follows from the definition of matrix multiplication that for any positive integer $n \in \mathbb{Z}^+$, we have
\[
M^n = \begin{pmatrix}
A_1^n & 0 & \cdots & 0 \\
0 & A_2^n & \cdots & 0 \\
\vdots & \vdots & \ddots & \vdots \\
0 & 0 & \cdots & A_k^n
\end{pmatrix}
\]
and for any scalar $a \in F$, we have
\[
aM = \begin{pmatrix}
aA_1 & 0 & \cdots & 0 \\
0 & aA_2 & \cdots & 0 \\
\vdots & \vdots & \ddots & \vdots \\
0 & 0 & \cdots & aA_k
\end{pmatrix}
\]
so for any polynomial $p(x) \in F[x],$
\[
p(M) = \begin{pmatrix}
p(A_1) & 0 & \cdots & 0 \\
0 & p(A_2) & \cdots & 0 \\
\vdots & \vdots & \ddots & \vdots \\
0 & 0 & \cdots & p(A_k)
\end{pmatrix}
\]
Therefore $p(x)$ annihilates $M$ if and only if $p(x)$ annihilates all the matrices $A_1, \cdots, A_k$. In particular, the minimum polynomial $m_M(x)$ annihilates $M$, hence annihilates all the matrices $A_1, \cdots, A_k$, and therefore is a multiple of each of the minimum polynomials $m_{A_1}(x), \cdots, m_{A_k}(x)$. (The minimum polynomial of a matrix $A$ divides every polynomial that annihilates $A$, since otherwise the nonzero remainder upon division by the minimum polynomial $m_A(x)$ would be a polynomial annihilating $A$ but with smaller degree than $m_A(x)$, contradicting the definition of $m_A(x)$.) Therefore, to obtain $m_M(x)$, we simply choose, among all the common multiples of the minimum polynomials of $A_1, \cdots, A_k$, the
one with smallest degree, but that is, by definition, the least common multiple of $m_{A_1}(x), \ldots, m_{A_k}(x)$.

**12.2.3** Prove that two $2 \times 2$ matrices over $F$ which are not scalar matrices are similar if and only if they have the same characteristic polynomial.

Let $A$ be a $2 \times 2$ matrix over $F$. Then $A$ determines a linear transformation $T$ of the vector space $V = F^2$, and $T$ determines an $F[x]$-module called in class “$V[T]$” (vs. just “$V$”), as a reminder that multiplication by $x$ acts the same as applying $T$.

The characteristic polynomial $c_A(x)$ is quadratic (since $A$ is $2 \times 2$), and is the product of the invariant factors of $V[T]$. The invariant factors have degree 1 or more and the largest invariant factor is the minimal polynomial $m_A(x)$.

One possibility is that the only invariant factor is $c_A(x) = m_A(x) = x^2 + a_1x + a_0$. In this case $A$ is similar to the companion matrix $\begin{pmatrix} 0 & -a_0 \\ 1 & -a_1 \end{pmatrix}$.

The only other possibility is that $c_A(x)$ is not the minimal polynomial, but instead is the product of the minimal polynomial with the smaller invariant factors. Since $c_A(x)$ is quadratic, the only way this can happen is that there are two linear invariant factors. Since the invariant factors are linear and monic, the only way one of them can divide another is that they are equal to each other, so $m_A(x) = x - b$ and $c_A(x) = (x - b)^2$. The matrix $A$ is similar to the block diagonal matrix whose blocks are the companion matrices for the invariant factors $x - b$ and $x - b$, namely $(b)$ and $(b)$, so $A$ is similar to the scalar matrix $S = \begin{pmatrix} b & 0 \\ 0 & b \end{pmatrix} = bI$. But for scalar matrices, similarity is equality, since for any $2 \times 2$ matrix $P$ we have $PSP^{-1} = PbIP^{-1} = bPIP^{-1} = bI = S$. Thus $A$ is a scalar matrix.

Suppose $A$ and $B$ are $2 \times 2$ matrices but are not scalar matrices. Then, as was shown above, the rational canonical form of $A$ is the companion
matrix \( \begin{pmatrix} 0 & -a_0 \\ 1 & -a_1 \end{pmatrix} \), where \( c_A(x) = m_A(x) = x^2 + a_1x + a_0 \) and the rational canonical form of \( B \) is the companion matrix \( \begin{pmatrix} 0 & -b_0 \\ 1 & -b_1 \end{pmatrix} \), where \( c_B(x) = m_B(x) = x^2 + b_1x + b_0 \). Now \( A \) and \( B \) are similar if and only if they have the same rational canonical form, so \( A \) and \( B \) are similar if and only if
\[
\begin{pmatrix} 0 & -a_0 \\ 1 & -a_1 \end{pmatrix} = \begin{pmatrix} 0 & -b_0 \\ 1 & -b_1 \end{pmatrix},
\]
which is obviously equivalent to the equality of their characteristic polynomials.

**12.2.4** Prove that two \( 3 \times 3 \) matrices over \( F \) are similar if and only if they have the same characteristic and the same minimal polynomials. Give an explicit counterexample to this assertion for \( 4 \times 4 \) matrices.

Let \( A \) be a \( 3 \times 3 \) matrix over \( F \). Then \( A \) determines a linear transformation \( T \) of the vector space \( V = F^3 \), and \( T \) determines an \( F[x] \)-module called \( V[T] \) (see comments above on this notation).

The characteristic polynomial \( c_A(x) \) is cubic (since \( A \) is \( 3 \times 3 \)), and is the product of the invariant factors of \( V[T] \). The invariant factors have degree 1 or more and the largest invariant factor is the minimal polynomial \( m_A(x) \). The degree of the minimal polynomial is 1, 2 or 3.

**Case 1.** \( m_A(x) \) has degree 3. Since \( c_A(x) \) is cubic and is divisible by the cubic invariant factor \( m_A(x) \), there can be no other invariant factors, hence the only invariant factor is \( c_A(x) = m_A(x) = x^3 + a_2x^2 + a_1x + a_0 \).

In this case \( A \) is similar to the companion matrix \( \begin{pmatrix} 0 & 0 & -a_0 \\ 1 & 0 & -a_1 \\ 0 & 1 & -a_2 \end{pmatrix} \).

**Case 2.** \( m_A(x) \) has degree 1, say \( m_A(x) = x - b \). The other invariant factors must be at least linear and must divide \( m_A(x) \), so they are all linear. Each invariant factor divides the next and all of them are monic, so they are all the same. Hence \( c_A(x) = (x - b)^3 \). The rational canonical form of \( A \) is the block diagonal matrix with three blocks of
the form \((b)\), namely
\[
\begin{pmatrix}
  b & 0 & 0 \\
  0 & b & 0 \\
  0 & 0 & b
\end{pmatrix}
\]

**Case 3.** \(m_A(x)\) has degree 2. In this case there must be one other linear invariant factor
\[
a_1(x) = x - b,
\]
and the minimal polynomial must be the second invariant factor \(a_2(x) = m_A(x)\), but this second factor is divisible by \(a_1(x)\), so we have
\[
a_2(x) = m_A(x) = (x - b)(x - c) = x^2 - (b + c)x + bc,
\]
and finally
\[
c_A(x) = a_1(x)a_2(x) = (x - b)^2(x - c).
\]
The rational canonical form in this case has a block of the form \((b)\), and then a block that is the companion matrix of \(m_A(x)\), namely
\[
\begin{pmatrix}
  b & 0 & 0 \\
  0 & 0 & -bc \\
  0 & 1 & b + c
\end{pmatrix}
\]
If two \(3 \times 3\) matrices \(A\) and \(B\) have the same minimal and characteristic polynomials, then they both fall into exactly one of the cases examined above, and in each case the rational canonical forms of \(A\) and \(B\) are determined by the coefficients of their minimal and characteristic polynomials, so that \(A\) and \(B\) will have the same rational canonical forms (and hence are similar) if and only if their characteristic and minimal polynomials are the same.

For an explicit counterexample among \(4 \times 4\) matrices we look for matrices \(A\) and \(B\) such that \(A\) has invariant factors \(x - 1, \ x - 1, \) and \((x - 1)^2 = m_A(x)\), hence \(c_A(x) = (x - 1)^4\), while \(B\) has invariant factors
\((x - 1)^2\) and \((x - 1)^2 = m_B(x)\), with \(c_B(x) = (x - 1)^4\). For example,

\[
A = \begin{pmatrix}
1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 \\
0 & 0 & 0 & -1 \\
0 & 0 & 1 & 2
\end{pmatrix}
\]

\[
B = \begin{pmatrix}
0 & -1 & 0 & 0 \\
1 & 2 & 0 & 0 \\
0 & 0 & 0 & -1 \\
0 & 0 & 1 & 2
\end{pmatrix}
\]

Then \(A\) and \(B\) have the same characteristic and minimal polynomials, and yet are not similar because they have distinct rational canonical forms (and are already in rational canonical form).

**12.2.7** Determine the eigenvalues of the matrix

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

We calculate the characteristic polynomial directly,

\[
\det(xI - A) = \begin{vmatrix}
x & -1 & 0 & 0 \\
0 & x & -1 & 0 \\
0 & 0 & x & -1 \\
-1 & 0 & 0 & x
\end{vmatrix}
= x \begin{vmatrix}
x & -1 & 0 \\
0 & x & -1 \\
0 & 0 & x
\end{vmatrix} - (-1) \begin{vmatrix}
0 & -1 & 0 \\
0 & x & -1 \\
-1 & 0 & x
\end{vmatrix}
= x \begin{vmatrix}
x & -1 & 0 \\
0 & x & -1 \\
0 & 0 & x
\end{vmatrix} + \begin{vmatrix}
0 & -1 & 0 \\
0 & x & -1 \\
-1 & 0 & x
\end{vmatrix}
= x^4 - 1 = (x^2 + 1)(x - 1)(x + 1)
\]

which shows that the eigenvalues are \(\pm 1, \pm \sqrt{-1}\).
12.2.8 Verify that the characteristic polynomial of the companion matrix

\[ C = \begin{pmatrix}
0 & 0 & 0 & \cdots & 0 & -a_0 \\
1 & 0 & 0 & \cdots & 0 & -a_1 \\
0 & 1 & 0 & \cdots & 0 & -a_2 \\
\vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\
0 & 0 & 0 & \cdots & 1 & -a_{n-1}
\end{pmatrix} \]

is \( x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \).

The characteristic polynomial of \( C \) is the determinant of the matrix

\[ xI - C = \begin{pmatrix}
x & 0 & 0 & \cdots & 0 & a_0 \\
-1 & x & 0 & \cdots & 0 & a_1 \\
0 & -1 & x & \cdots & 0 & a_2 \\
\vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\
0 & 0 & 0 & \cdots & -1 & x + a_{n-1}
\end{pmatrix} \]

The determinant of \( xI - C \) is unchanged if we add multiples of rows in \( xI - C \) to other rows in \( xI - C \) (see Prop. 11.22). Here is \( xI - C \) with the second row multiplied by \( x \), the third row multiplied by \( x^2 \), \( \ldots \), and row \( n \) multiplied by \( x^{n-1} \):

\[ \begin{pmatrix}
x & 0 & 0 & \cdots & 0 & a_0 \\
x \cdot x & x^2 & 0 & \cdots & 0 & a_1x \\
0 & -x^2 & x^3 & \cdots & 0 & a_2x^2 \\
\vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\
0 & 0 & 0 & \cdots & -x^{n-1} & x^n + a_{n-1}x^{n-1}
\end{pmatrix} \]

Let \( p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \), and add rows 2 through \( n \) of the matrix above to the first row of matrix \( xI - C \), obtaining

\[ D = \begin{pmatrix}
0 & 0 & 0 & \cdots & 0 & p(x) \\
-1 & x & 0 & \cdots & 0 & a_1 \\
0 & -1 & x & \cdots & 0 & a_2 \\
\vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\
0 & 0 & 0 & \cdots & x & a_{n-2} \\
0 & 0 & 0 & \cdots & -1 & x + a_{n-1}
\end{pmatrix} \]
Now \( xI - C \) and \( D \) have the same determinant. If we compute the determinant of \( D \) by expanding along the first row, we get

\[
\det D = (-1)^{n-1} p(x) \det E
\]

where \( E \) is the square matrix with \( n - 1 \) rows and columns, \(-1\) on the diagonal, and \( x \) on the superdiagonal:

\[
E = \begin{pmatrix}
-1 & x & 0 & \cdots & 0 \\
0 & -1 & x & \cdots & 0 \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
0 & 0 & 0 & \cdots & x \\
0 & 0 & 0 & \cdots & -1
\end{pmatrix}
\]

The determinant of \( E \) is unchanged by adding \( x \) times the first column to the second column. This operation eliminates the \( x \) in the second column, and the new second column can now be used to eliminate the \( x \) in the third column, and so on. The result is that the determinant of \( E \) is the same as the determinant of a \((n - 1) \times (n - 1)\) matrix with \(-1\) on the diagonal, whose determinant is \((-1)^{n-1}\). Thus we have \( \det E = (-1)^{n-1} \), so by (23) we have

\[
\det D = (-1)^{n-1} p(x) \det E = (-1)^{n-1} p(x)(-1)^{n-1} = p(x),
\]
as desired.

---

Homework #10, due 3/31/10 = 12.2.9, 12.2.10, 12.2.11, 12.3.1,

Additional problems recommended for study: 12.2.1, 12.2.5, 12.2.6, 12.2.12-18, 12.2.21-26

12.2.9 Find the rational canonical forms of

\[
\begin{pmatrix}
0 & -1 & -1 \\
0 & 0 & 0 \\
-1 & 0 & 0
\end{pmatrix}, \quad \begin{pmatrix}
c & c & -1 \\
0 & c & 1 \\
-1 & 1 & c
\end{pmatrix}, \quad \begin{pmatrix}
422 & 465 & 15 & -30 \\
-420 & -462 & -15 & 30 \\
840 & 930 & 32 & -60 \\
-140 & -155 & -5 & 12
\end{pmatrix}.
\]
12.2.9(a) Let

\[ A = \begin{pmatrix} 0 & -1 & -1 \\ 0 & 0 & 0 \\ -1 & 0 & 0 \end{pmatrix} \]

Compute the characteristic polynomial \( c_A(x) \in F[x] \) by expansion down the first column:

\[
c_A(x) = \det (xI - A) = \det \begin{pmatrix} x & 1 & 1 \\ 0 & x & 0 \\ 1 & 0 & x \end{pmatrix}
\]

\[
= x \det \begin{pmatrix} x & 0 \\ 0 & x \end{pmatrix} + \det \begin{pmatrix} 1 & 1 \\ x & 0 \end{pmatrix}
\]

\[
= x^3 - x = x(x-1)(x+1)
\]

The characteristic polynomial is the product of the invariant factors of \( A \), by Prop. 12.20. Suppose \( A \) has more than one invariant factor, say \( a_1(x), \ldots, a_m(x) \in \mathbb{Q}[x] \), where \( a_1(x) | \ldots | a_m(x) \) and \( m \geq 2 \). If a linear polynomial \( x + b \) divides one of the invariant factors besides the last one, say \( x + b \) divides \( a_i(x) \) with \( i < m \), then \( (x+b)^2 \) must divide \( c_A(x) \) since \( a_i(x) | a_m(x) \), so, for some \( p(x), q(x) \in F[x] \),

\[
c_A(x) = a_1(x) \cdots a_i(x) \cdots a_m(x)
\]

\[
= a_1(x) \cdots p(x)(x+b) \cdots q(x)(x+b)
\]

In this case the characteristic polynomial is \( x(x-1)(x+1) \), which has only linear factors, so none of them can divide any “earlier” invariant factors, i.e., there is only one invariant factor, and it is both the characteristic polynomial and minimal polynomial of \( A \). Thus

\[
c_A(x) = m_A(x) = x(x-1)(x+1) = x^3 - x,
\]

and the rational canonical form of \( A \) is the companion matrix of \( x^3 - x \), namely

\[
\begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}
\]
12.2.9(b) Let

\[ A = \begin{pmatrix} c & c & -1 \\ 0 & c & 1 \\ -1 & 1 & c \end{pmatrix} \]

Then the characteristic polynomial of \( A \) can be factored into distinct linear factors:

\[
c_A(x) = \det(xI - A)
= \det \begin{pmatrix} x - c & 0 & 1 \\ 0 & x - c & -1 \\ 1 & -1 & x - c \end{pmatrix}
= (x - c) \det \begin{pmatrix} x - c & -1 \\ -1 & x - c \end{pmatrix} + \det \begin{pmatrix} 0 & 1 \\ x - c & -1 \end{pmatrix}
= (x - c)((x - c)^2 - 1) - (x - c)
= (x - c)((x - c)^2 - 2)
= (x - c)(x - c + \sqrt{2})(x - c - \sqrt{2})
= x^3 - 3cx^2 + (3c^2 - 2)x - c^3 + 2c
\]

As argued above, since the characteristic polynomial is the product of distinct linear polynomials, the minimal and characteristic polynomials are the same and are the sole invariant factor of \( A \). So the rational canonical form of \( A \) is the companion matrix of the characteristic polynomial \( c_A(x) \) of \( A \), namely

\[
\begin{pmatrix} 0 & c^3 - 2c \\ 1 & 2 - 3c^2 \\ 0 & 3c \end{pmatrix}
\]

12.2.9(c) Let

\[
A = \begin{pmatrix} 422 & 465 & 15 & -30 \\ -420 & -462 & -15 & 30 \\ 840 & 930 & 32 & -60 \\ -140 & -155 & -5 & 12 \end{pmatrix}
\]
The Smith normal form is
\[
\begin{pmatrix}
1 & 0 & 0 & 0 \\
0 & x - 2 & 0 & 0 \\
0 & 0 & x - 2 & 0 \\
0 & 0 & 0 & (x - 2)(x + 3)
\end{pmatrix}
\]
so the invariant factors are \(a_1 = x - 2\), \(a_2 = x - 2\), and \(a_2 = (x - 2)(x + 3) = x^2 + x - 6\). The companion matrices for these polynomials are \((2)\), \((2)\), and \(\begin{pmatrix} 0 & 6 \\ 1 & -1 \end{pmatrix}\), respectively, so the rational canonical form for \(A\) is
\[
\begin{pmatrix}
2 & 0 & 0 & 0 \\
0 & 2 & 0 & 0 \\
0 & 0 & 0 & 6 \\
0 & 0 & 1 & -1
\end{pmatrix}
\]

12.2.10 Find all similarity classes of 6\(\times\)6 matrices over \(\mathbb{Q}\) with minimal polynomial \((x + 2)^2(x - 1)\) (it suffices to give all lists of invariant factors and write out some of their corresponding matrices.)

First we review some facts that put limits on the possible lists of invariant factors for \(A\). The characteristic polynomial \(c_A(x)\) of a 6\(\times\)6 matrix \(A\) has degree 6 and \(c_A(x)\) is divisible by the cubic minimal polynomial \(m_A(x) = (x + 2)^2(x - 1)\), which is the “last” and largest invariant factor. Now \(c_A(x)\) is the product of the invariant factors, and the remaining invariant factors (besides \(m_A(x)\)) must divide \(m_A(x)\) and have degree at least 1, so \(c_A(x)\) is the product of \(m_A(x)\) and three linear factors that divide \(m_A(x)\). The possible lists of invariant factors for \(A\) are:

\[
\begin{array}{ccc}
(24) & (x + 2)^2(x - 1) & (x + 2)^2(x - 1) \\
(25) & x + 2 & (x + 2)^2 & (x + 2)^2(x - 1) \\
(26) & x + 2 & (x + 2)(x - 1) & (x + 2)^2(x - 1) \\
(27) & x - 1 & (x + 2)(x - 1) & (x + 2)^2(x - 1) \\
(28) & x + 2 & x + 2 & (x + 2)^2(x - 1) \\
(29) & x - 1 & x - 1 & x - 1 & (x + 2)^2(x - 1)
\end{array}
\]
The corresponding characteristic polynomials are
\[(x + 2)^4(x - 1)^2\] in case (24)
\[(x + 2)^5(x - 1)\] in case (25)
\[(x + 2)^4(x - 1)^2\] in case (26)
\[(x + 2)^3(x - 1)^3\] in case (27)
\[(x + 2)^5(x - 1)\] in case (28)
\[(x + 2)^2(x - 1)^4\] in case (29)

Note that in the pairs of cases (24)(27) and (25)(28), there exist pairs of dissimilar $6 \times 6$ matrices with the same minimal and characteristic polynomials. The polynomials that occur in the lists above as potential invariant factors, together with their companion matrices, are listed next.

\[(x + 2)^2(x - 1) = x^3 + 3x^2 - 4\]
\[
\begin{bmatrix}
0 & 0 & 4 \\
0 & 1 & 0 \\
0 & 1 & -3
\end{bmatrix}
\]

\[(x + 2)^2 = x^2 + 4x + 4\]
\[
\begin{bmatrix}
0 & -4 \\
1 & -4
\end{bmatrix}
\]

\[(x + 2)(x - 1) = x^2 + x - 2\]
\[
\begin{bmatrix}
0 & 2 \\
1 & -1
\end{bmatrix}
\]
\[x + 2\]
\[x - 1\]
\[
\begin{bmatrix}
-2 \\
1
\end{bmatrix}
\]

Finally, rational canonical forms for the six cases:

\[
\begin{pmatrix}
0 & 0 & 4 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & -3 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 4 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & -3
\end{pmatrix}
\] case (24)
12.2.11 Find all similarity classes of $6 \times 6$ matrices over $\mathbb{C}$ with characteristic polynomial $(x^4 - 1)(x^2 - 1)$. 

$$\begin{pmatrix} -2 & 0 & 0 & 0 & 0 & 0 \\ 0 & -4 & 0 & 0 & 0 & 0 \\ 0 & 1 & -4 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 4 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 - 3 \end{pmatrix}$$ case (25)

$$\begin{pmatrix} -2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & 0 \\ 0 & 1 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 4 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 - 3 \end{pmatrix}$$ case (26)

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & 0 \\ 0 & 1 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 4 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 - 3 \end{pmatrix}$$ case (27)

$$\begin{pmatrix} -2 & 0 & 0 & 0 & 0 & 0 \\ 0 & -2 & 0 & 0 & 0 & 0 \\ 0 & 0 & -2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 4 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 - 3 \end{pmatrix}$$ case (28)

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 4 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & - 3 \end{pmatrix}$$ case (29)
First we factor the characteristic polynomial over $\mathbb{C}$.
\[ c_A(x) = (x^4 - 1)(x^2 - 1) \]
\[ = (x^2 - 1)(x^2 + 1)(x - 1)(x + 1) \]
\[ = (x - 1)(x + 1)(x - \sqrt{-1})(x + \sqrt{-1})(x - 1)(x + 1) \]
\[ = (x - 1)^2(x + 1)^2(x - \sqrt{-1})(x + \sqrt{-1}) \]

The problem is then to give all lists of invariant factors whose product is $c_A(x)$. Every linear polynomial that divides $c_A(x)$ (or any of the invariant factors) must also divide the minimum polynomial $m_A(x)$. The various possibilities for $m_A(x)$ arise from linear factors that appear in $c_A(x)$ with powers higher than 1. So $m_A(x)$ and the remaining invariant factors are one of the following possibilities:

(30) \((x - 1)^2(x + 1)^2(x - \sqrt{-1})(x + \sqrt{-1})\)

(31) \((x - 1)(x + 1)^2(x - \sqrt{-1})(x + \sqrt{-1}) \quad x - 1\)

(32) \((x - 1)^2(x + 1)(x - \sqrt{-1})(x + \sqrt{-1}) \quad x + 1\)

(33) \((x - 1)(x + 1)(x - \sqrt{-1})(x + \sqrt{-1}) \quad (x - 1)(x + 1)\)

For each of these cases we compute polynomials and companion matrices.

**Case (30)** The polynomial
\[ c_A(x) = (x - 1)^2(x + 1)^2(x - \sqrt{-1})(x + \sqrt{-1}) \]
\[ = (x^4 - 1)(x^2 - 1) \]
\[ = x^6 - x^4 - x^2 + 1 \]

has companion matrix
\[
\begin{pmatrix}
0 & 0 & 0 & 0 & 0 & -1 \\
1 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 1 \\
0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 1 \\
0 & 0 & 0 & 0 & 1 & 0
\end{pmatrix}
\]
and this matrix is a representative of the similarity class.

**Case (31)** The polynomial

\[(x - 1)(x + 1)^2(x - \sqrt{-1})(x + \sqrt{-1})\]

\[= (x^2 - 1)(x + 1)(x^2 + 1)\]

\[= (x^4 - 1)(x + 1)\]

\[= x^5 + x^4 - x - 1\]

has companion matrix

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

and the other invariant factor is \(x - 1\), which has companion matrix (1), so a representative in rational canonical form of the similarity class in this case is

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

**Case (32)** The polynomial

\[(x - 1)^2(x + 1)(x - \sqrt{-1})(x + \sqrt{-1})\]

\[= (x^2 - 1)(x - 1)(x^2 + 1)\]

\[= (x^4 - 1)(x - 1)\]

\[= x^5 - x^4 - x + 1\]
has companion matrix
\[
\begin{pmatrix}
0 & 0 & 0 & 0 & -1 \\
1 & 0 & 0 & 0 & 1 \\
0 & 1 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 1 & 1
\end{pmatrix}
\]

and the other invariant factor is \(x + 1\), which has companion matrix \((-1)\), so a representative in rational canonical form of the similarity class in this case is
\[
\begin{pmatrix}
-1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & -1 \\
0 & 1 & 0 & 0 & 0 & 1 \\
0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 1
\end{pmatrix}
\]

**Case** (33) The polynomial
\[
(x - 1)(x + 1)(x - \sqrt{-1})(x + \sqrt{-1}) = (x^2 - 1)(x^2 + 1) = x^4 - 1
\]
has companion matrix
\[
\begin{pmatrix}
0 & 0 & 0 & 1 \\
1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 \\
0 & 0 & 1 & 0
\end{pmatrix}
\]

and \((x - 1)(x + 1) = x^2 - 1\) has companion matrix
\[
\begin{pmatrix}
0 & 1 \\
1 & 0
\end{pmatrix}
\]
so a representative in rational canonical form of the similarity class in this case is

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

12.3.1 Suppose the vector space \( V \) is the direct sum of cyclic \( F[x] \)-modules whose annihilators are \((x + 1)^2\), \((x - 1)(x^2 + 1)^2\), \((x^4 - 1)\), and \((x + 1)(x^2 - 1)\). Determine the invariant factors and elementary divisors for \( V \).

Let us first assume that \( F = \mathbb{Q} \). That way the polynomial \( x^2 + 1 \) is prime/irreducible. (Otherwise we could consider doing this problem over \( \mathbb{C} \), but then \( x^2 + 1 \) is the product of two linear factors.) \( V \) is assumed to be the direct sum of four cyclic \( F[x] \)-modules, three of which may be further decomposed into sums as follows:

\[
\begin{align*}
(34) & \quad F[x]/((x - 1)(x^2 + 1)^2) \cong F[x]/(x - 1) \oplus F[x]/((x^2 + 1)^2) \\
(35) & \quad F[x]/(x^4 - 1) \cong F[x]/(x - 1) \oplus F[x]/(x + 1) \oplus F[x]/(x^2 + 1) \\
(36) & \quad F[x]/((x + 1)(x^2 - 1)) \cong F[x]/((x + 1)^2) \oplus F[x]/(x - 1)
\end{align*}
\]

so the list of elementary divisors of \( V \) is \( x - 1, x - 1, x - 1, x + 1, (x + 1)^2, (x + 1)^2, x^2 + 1, (x^2 + 1)^2 \). The minimal polynomial must be the product of the elementary divisors with the highest powers, so the invariant factors are

\[
m_A(x) = (x - 1)(x + 1)^2(x^2 + 1)^2
\]

\[
a_2 = (x - 1)(x + 1)^2(x^2 + 1)
\]

\[
a_1 = (x - 1)(x + 1)
\]

Now we solve the problem again, under the assumption on \( F \) (made at the beginning of Section 12.2) that all the polynomials involved can be factored into linear polynomials. This is certainly true if we assume
$F = \mathbb{C}$. Two of the decompositions given above can be extended using the factorization $x^2 + 1 = (x - \sqrt{-1})(x + \sqrt{-1})$. First, instead of (34), we note that $F[x]/((x - 1)(x^2 + 1)^2)$ is isomorphic to

$$F[x]/(x - 1) \oplus F[x]/((x + \sqrt{-1})^2) \oplus F[x]/((x - \sqrt{-1})^2)$$

and instead of (35), we note that $F[x]/(x^4 - 1)$ is isomorphic to

$$F[x]/(x - 1) \oplus F[x]/(x + 1) \oplus F[x]/(x + \sqrt{-1}) \oplus F[x]/(x - \sqrt{-1})$$

so the list of elementary divisors of $V$ is

$$x - 1 \quad x - 1 \quad x - 1$$

$$x + 1 \quad (x + 1)^2 \quad (x + 1)^2$$

$$x + \sqrt{-1} \quad (x + \sqrt{-1})^2$$

$$x - \sqrt{-1} \quad (x - \sqrt{-1})^2$$

and the invariant factors are

$$m_A(x) = (x - 1)(x + 1)^2(x - \sqrt{-1})^2(x + \sqrt{-1})^2$$

$$a_2 = (x - 1)(x + 1)^2(x + \sqrt{-1})(x - \sqrt{-1})$$

$$a_1 = (x - 1)(x + 1)$$

---

Homework #11, due 4/7/10 = 13.1.1, 13.1.2, 13.1.3, 13.2.1, 13.2.2

Additional problems recommended for study: 13.1.4, 13.1.5, 13.1.6, 13.1.7, 13.1.8

**13.1.1** Show that $p(x) = x^3 + 9x + 6$ is irreducible in $\mathbb{Q}[x]$. Let $\theta$ be a root of $p(x)$. Find the inverse of $1 + \theta$ in $\mathbb{Q}(\theta)$.

The prime 3 does not divide the leading term of the polynomial $x^3 + 9x + 6$, does divide the remaining coefficients 0, 9, and 6, but its square $3^2$ does not divide the constant term 6. Therefore $p(x)$ is irreducible in $\mathbb{Q}[x]$ by the Eisenstein criterion.

By Th. 13.6, $\mathbb{Q}(\theta) \cong \mathbb{Q}[x]/(p)$, so to find the inverse of $1 + \theta$ in $\mathbb{Q}(\theta)$ it is enough to compute the inverse of $1 + x$ in the quotient $\mathbb{Q}[x]/(p)$.  

---


To do this, use the Euclidean algorithm to find a linear combination of $p(x)$ and $1 + x$ that equals 1. First divide $x + 1$ into $x^3 + 9x + 6$, get quotient $x^2 - x + 10$ and remainder $-4$, so that

$$x^3 + 9x + 6 = (x + 1)(x^2 - x + 10) + (-4)$$

It follows that

$$1 = -\frac{1}{4}(x^3 + 9x + 6) + \frac{1}{4}(x^2 - x + 10)(x + 1)$$

By the hypothesis on $\theta$, $\theta^3 + 9\theta + 6 = 0$, so substituting $\theta$ for $x$ in the previous equation gives

$$1 = \frac{1}{4}(\theta^2 - \theta + 10)(\theta + 1)$$

hence

$$(\theta + 1)^{-1} = \frac{1}{4}(\theta^2 - \theta + 10) \in \mathbb{Q}(\theta).$$

13.1.2 Show that $x^3 - 2x - 2$ is irreducible over $\mathbb{Q}$ and let $\theta$ be a root. Compute $(1 + \theta)(1 + \theta + \theta^2)$ and $\frac{1 + \theta}{1 + \theta + \theta^2}$ in $\mathbb{Q}(\theta)$.

First observe that the prime 2 does not divide the leading coefficient of $x^3 - 2x - 2$ (which is 1), does divide all the other coefficients (which are 0, −2, and −2), but $2^2$ does not divide the constant $-2$ of $x^3 - 2x - 2$, so $x^3 - 2x - 2$ is irreducible over $\mathbb{Q}$ by the Eisenstein criterion.

Since $\theta$ is a root of $x^3 - 2x - 2$, we know $\theta^3 - 2\theta - 2 = 0$, hence $\theta^3 = 2\theta + 2$, so

$$(1 + \theta)(1 + \theta + \theta^2) = (1 + \theta + \theta^2) + (\theta + \theta^2 + \theta^3)$$

$$= 1 + 2\theta + 2\theta^2 + \theta^3$$

$$= 1 + 2\theta + 2\theta^2 + (2\theta + 2)$$

$$= 3 + 4\theta + 2\theta^2$$

We will compute $\frac{1 + \theta}{1 + \theta + \theta^2}$ by first computing the inverse of $1 + \theta + \theta^2$. By Th. 13.6, $\mathbb{Q}(\theta) \cong \mathbb{Q}[x]/(x^3 - 2x - 2)$, so to find the inverse of $1 + \theta + \theta^2$ in $\mathbb{Q}(\theta)$ it is enough to compute the inverse of $1 + x + x^2$ in the quotient $\mathbb{Q}[x]/(x^3 - 2x - 2)$. To do this, use the Euclidean algorithm to find a
linear combination of $x^3 - 2x - 2$ and $1 + x + x^2$ that equals 1; we need to find polynomials $p(x), q(x) \in \mathbb{Q}[x]$ such that

(37) \[(x^3 - 2x - 2)p(x) + (x^2 + x + 1)q(x) = 1.\]

Then $\frac{(x^2 + x + 1)q(x)}{1}$ in $\mathbb{Q}[x]/(x^3 - 2x - 2)$, so the inverse of $1 + \theta + \theta^2$ is $q(\theta)$.

Now such polynomials exist because $x^3 - 2x - 2$ is irreducible, hence prime, and $1 + x + x^2$ has smaller degree (2 vs. 3), so $x^3 - 2x - 2$ and $1 + x + x^2$ are relatively prime, and $\mathbb{Q}[x]$ is a Euclidean domain, so the greatest common divisor of $x^3 - 2x - 2$ and $1 + x + x^2$, namely, 1, is a linear combination of these two polynomials.

Use the Euclidean algorithm: divide $x^2 + x + 1$ into $x^3 - 2x - 2$, get quotient $x - 1$ and remainder $-2x - 1$, so that

(38) \[x^3 - 2x - 2 = (x^2 + x + 1)(x - 1) + (-2x - 1),\]

which implies

(39) \[-2x - 1 = x^3 - 2x - 2 - (x^2 + x + 1)(x - 1).\]

Next we divide $x^2 + x + 1$ by the remainder $-2x - 1$, obtaining quotient $-\frac{1}{2}x - \frac{1}{4}$ and remainder $\frac{3}{4}$, so that

(40) \[x^2 + x + 1 = (-2x - 1)(-\frac{1}{2}x - \frac{1}{4}) + \frac{3}{4},\]

From (40) we get

\[
\frac{3}{4} = x^2 + x + 1 - \left( -2x - 1 \right) \left( -\frac{1}{2}x - \frac{1}{4} \right)
\]

so by substituting according to (39) and simplifying we get

\[
\frac{3}{4} = x^2 + x + 1 - \left( x^3 - 2x - 2 \right) \left( -\frac{1}{2}x - \frac{1}{4} \right)
\]

\[
= x^2 + x + 1 - \left( x^3 - 2x - 2 \right) \left( -\frac{1}{2}x - \frac{1}{4} \right) + \left( x^2 + x + 1 \right) \left( -2x - 1 \right) \left( -\frac{1}{2}x - \frac{1}{4} \right)
\]

\[
= x^2 + x + 1 + \left( x^3 - 2x - 2 \right) \left( \frac{1}{2}x + \frac{1}{4} \right) - \left( x^2 + x + 1 \right) \left( -2x - 1 \right) \left( \frac{1}{2}x + \frac{1}{4} \right)
\]

\[
= \left( x^3 - 2x - 2 \right) \left( \frac{1}{2}x + \frac{1}{4} \right) + \left( x^2 + x + 1 \right) \left( 1 - \left( -2x - 1 \right) \left( \frac{1}{2}x + \frac{1}{4} \right) \right)
\]

Multiplying both sides by $4/3$ gives

\[
1 = \frac{4}{3} \left( x^3 - 2x - 2 \right) \left( \frac{1}{2}x + \frac{1}{4} \right) + \left( x^2 + x + 1 \right) \left( 1 - \left( -2x - 1 \right) \left( \frac{1}{2}x + \frac{1}{4} \right) \right)
\]
\[ (x^3 - 2x - 2) \frac{1}{3} (2x + 1) + (x^2 + x + 1) \frac{1}{3} (-2x^2 + x + 5) \]

Substitute \( \theta \) for \( x \), note that \( \theta^3 - 2\theta - 2 = 0 \) since \( \theta \) is a root of \( x^3 - 2x - 2 \), and get

\[ 1 = (\theta^2 + \theta + 1) \frac{1}{3} (-2\theta^2 + \theta + 5) \]

Therefore \( (1 + \theta + \theta^2)^{-1} = \frac{1}{3} (-2\theta^2 + \theta + 5) \). To compute \( \frac{1 + \theta}{1 + \theta + \theta^2} \), multiply this answer by \( 1 + \theta \):

\[
(1 + \theta)(1 + \theta + \theta^2)^{-1} = (1 + \theta)\left(\frac{1}{3} (-2\theta^2 + \theta + 5)\right)
= \frac{1}{3} (-2\theta^2 + \theta + 5 + (-2\theta^2 + \theta + 5)\theta)
= \frac{1}{3} (-2\theta^2 + \theta + 5 - 2\theta^3 + \theta^2 + 5\theta)
= \frac{1}{3} (-2\theta^3 - \theta^2 + 6\theta + 5)
\]

**13.1.3** Show that \( x^3 + x + 1 \) is irreducible over \( \mathbb{F}_2 \) and let \( \theta \) be a root. Compute the powers of \( \theta \) in \( \mathbb{F}_2(\theta) \).

Since \( x^3 + x + 1 \) is cubic, it would have a linear factor (and hence a root) if it were reducible, so to show it is irreducible it is enough to show it has no roots in \( \mathbb{F}_2 \), but this is an easy calculation (where \( =_2 \) is equality modulo 2): \( 0^3 + 0 + 1 = 1 \neq 0 \), \( 1^3 + 1 + 1 = 3 =_2 1 \neq 0 \), and \( 2^3 + 2 + 1 = 11 =_2 1 \neq 0 \).

Since \( \theta \) is a root of \( x^3 + x + 1 \) (in some extension field of \( \mathbb{F}_2 \)), we have

Since \( \theta^3 + \theta + 1 = 0 \), so \( \theta^3 = -1 - \theta =_2 1 + \theta \). Then the powers of \( \theta \) are

\[
\theta^0 = 1
\theta^1 = \theta
\theta^2
\theta^3 = 1 + \theta
\theta^4 = \theta + \theta^2
\theta^5 = \theta^2 + \theta^3 = 1 + \theta + \theta^2
\theta^6 = \theta + \theta^2 + \theta^3 = \theta + \theta^2 + 1 + \theta = 1 + \theta^2
\theta^7 = \theta + \theta^3 = \theta + 1 + \theta = 1
\]

\]
13.2.1 Let $\mathbb{F}$ be a finite field of characteristic $p$. Prove that $|\mathbb{F}| = p^n$ for some positive integer $n$.

$\mathbb{F}$ has ground field generated by the unit element $1_\mathbb{F}$. Since the characteristic is $p$, this ground field is (isomorphic to) $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Since $\mathbb{F}$ is an extension field of $\mathbb{F}_p$, it is a vector space over $\mathbb{F}_p$, but it is finite, so it must be a finite dimensional vector space, therefore isomorphic to a direct power of the ground field $\mathbb{F}$, which has cardinality $p$, so the cardinality of $\mathbb{F}$ must therefore be a power of $p$.

13.2.2 Let $g(x) = x^2 + x - 1$ and let $h(x) = x^3 - x + 1$. Obtain fields of 4, 8, 9, and 27 elements by adjoining a root of $f(x)$ to the field $F$ where $f(x) = g(x)$ or $h(x)$ and $F = \mathbb{F}_2$ or $\mathbb{F}_3$. Write down the multiplication tables for the fields with 4 and 9 elements and show that the nonzero elements form a cyclic group.

The polynomials $g(x)$ and $h(x)$ have low enough degree (2 or 3) that if one of them were reducible it would have to have a linear factor, hence a root in the ground field. We prove that they are both irreducible over both $\mathbb{F}_2$ and $\mathbb{F}_3$ by checking that neither of them has a root in either $\mathbb{F}_2$ or $\mathbb{F}_3$. In $\mathbb{F}_2$,

$g(0) = 0^2 + 0 - 1 = 1 \neq 0 \quad h(0) = 0^3 - 0 + 1 = 1 \neq 0$
$g(1) = 1^2 + 1 - 1 = 1 \neq 0 \quad h(1) = 1^3 - 1 + 1 = 1 \neq 0$

while in $\mathbb{F}_3$,

$g(0) = 0^2 + 0 - 1 = 2 \neq 0 \quad h(0) = 0^3 - 0 + 1 = 1 \neq 0$
$g(1) = 1^2 + 1 - 1 = 1 \neq 0 \quad h(1) = 1^3 - 1 + 1 = 1 \neq 0$
$g(2) = 2^2 + 2 - 1 = 2 \neq 0 \quad h(2) = 2^3 - 2 + 1 = 1 \neq 0$

4-element field. We get a field $K$ with 4 elements by adding a root of the quadratic polynomial $g(x) = x^2 + x - 1$ to the field $\mathbb{F}_2$. This gives an extension of degree 2, so the size of the extension field is $|\mathbb{F}_2|^2 = 2^2 = 4$. For an extension $K/\mathbb{F}_2$ in which $g(x)$ has root $\alpha$, we let $K = \mathbb{F}_2[x]/(g(x))$ and $\alpha = \overline{x} = x + (g(x))$. Note that $\alpha^2 = 1 - \alpha = 1 + \alpha$ (because the ground field of $K$ is $\mathbb{F}_2$). The nonzero elements of $K$ form a cyclic group generated by $\alpha$, whose elements are $\alpha, \alpha^2 = 1 + \alpha, and
\[ \alpha^3 = \alpha + \alpha^2 = \alpha + 1 + \alpha = 1. \] The multiplication table for elements of \( K \) is

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
<th>( \alpha )</th>
<th>1 + ( \alpha )</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>( \alpha )</td>
<td>1 + ( \alpha )</td>
</tr>
<tr>
<td>( \alpha )</td>
<td>0</td>
<td>( \alpha )</td>
<td>1 + ( \alpha )</td>
<td>1 + ( \alpha )</td>
</tr>
<tr>
<td>1 + ( \alpha )</td>
<td>0</td>
<td>1 + ( \alpha )</td>
<td>1 + ( \alpha )</td>
<td>( \alpha )</td>
</tr>
</tbody>
</table>

**8-element field.** We get a field \( K \) with 8 elements by adding a root of the cubic polynomial \( h(x) = x^3 - x + 1 \) to the field \( \mathbb{F}_2 \). This gives an extension of degree 3, so the size of the extension field is \( |\mathbb{F}_2|^3 = 2^3 = 8 \). Let \( K = \mathbb{F}_2[x]/(h(x)) \) and \( \theta = \overline{x} = x + (h(x)) \). Then \( \theta^3 - \theta + 1 = 0 \) so \( \theta^3 = \theta - 1 = 1 + \theta \) (because the ground field of \( K \) is \( \mathbb{F}_2 \)). The nonzero elements of \( K \) form a cyclic group generated by \( \theta \), whose elements are \( \theta, \theta^2, \theta^3 = 1 + \theta, \theta^4 = \theta + \theta^2, \theta^5 = \theta^2 + \theta^3 = 1 + \theta + \theta^2, \theta^6 = \theta + \theta^2 + \theta^3 = \theta + \theta^2 + 1 + \theta = 1 + \theta^2 \), and \( \theta^7 = \theta + \theta^3 = \theta + 1 + \theta = 1 \). The multiplication table for elements of \( K \) is

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>( \theta )</th>
<th>( \theta^2 )</th>
<th>1 + ( \theta )</th>
<th>( \theta + \theta^2 )</th>
<th>1 + ( \theta + \theta^2 )</th>
<th>1 + ( \theta + \theta^2 + 1 + \theta )</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>( \theta )</td>
<td>0</td>
<td>( \theta )</td>
<td>( \theta^2 )</td>
<td>1 + ( \theta )</td>
<td>( \theta + \theta^2 )</td>
<td>1 + ( \theta + \theta^2 )</td>
<td>1 + ( \theta + \theta^2 + 1 + \theta )</td>
</tr>
<tr>
<td>( \theta^2 )</td>
<td>0</td>
<td>( \theta^2 )</td>
<td>1 + ( \theta )</td>
<td>( \theta + \theta^2 )</td>
<td>1 + ( \theta + \theta^2 )</td>
<td>1 + ( \theta + \theta^2 + 1 + \theta )</td>
<td>1 + ( \theta + \theta^2 + 1 + \theta )</td>
</tr>
<tr>
<td>1 + ( \theta )</td>
<td>0</td>
<td>1 + ( \theta )</td>
<td>( \theta + \theta^2 )</td>
<td>1 + ( \theta + \theta^2 )</td>
<td>1 + ( \theta + \theta^2 )</td>
<td>1 + ( \theta + \theta^2 )</td>
<td>1 + ( \theta + \theta^2 )</td>
</tr>
<tr>
<td>( \theta + \theta^2 )</td>
<td>0</td>
<td>( \theta + \theta^2 )</td>
<td>1 + ( \theta + \theta^2 )</td>
<td>1 + ( \theta + \theta^2 )</td>
<td>1 + ( \theta + \theta^2 )</td>
<td>1 + ( \theta + \theta^2 )</td>
<td>1 + ( \theta + \theta^2 )</td>
</tr>
<tr>
<td>1 + ( \theta + \theta^2 )</td>
<td>0</td>
<td>1 + ( \theta + \theta^2 )</td>
<td>1 + ( \theta + \theta^2 )</td>
<td>1 + ( \theta + \theta^2 )</td>
<td>1 + ( \theta + \theta^2 )</td>
<td>1 + ( \theta + \theta^2 )</td>
<td>1 + ( \theta + \theta^2 )</td>
</tr>
<tr>
<td>1 + ( \theta + \theta^2 + 1 + \theta )</td>
<td>0</td>
<td>1 + ( \theta + \theta^2 + 1 + \theta )</td>
<td>1 + ( \theta + \theta^2 + 1 + \theta )</td>
<td>1 + ( \theta + \theta^2 + 1 + \theta )</td>
<td>1 + ( \theta + \theta^2 + 1 + \theta )</td>
<td>1 + ( \theta + \theta^2 + 1 + \theta )</td>
<td>1 + ( \theta + \theta^2 + 1 + \theta )</td>
</tr>
</tbody>
</table>

**9-element field.** We get a field \( K \) with 9 elements by adding a root of the quadratic polynomial \( g(x) = x^2 + x - 1 \) to the field \( \mathbb{F}_3 \). This gives an extension of degree 2, so the size of the extension field is \( |\mathbb{F}_3|^2 = 3^2 = 9 \). For an extension \( K/\mathbb{F}_3 \) in which \( g(x) \) has root \( \theta \), we let \( K = \mathbb{F}_3[x]/(g(x)) \) and \( \theta = \overline{x} = x + (g(x)) \). Note that \( \theta^2 = 1 - \theta = 1 + 2\theta \) (because the ground field of \( K \) is \( \mathbb{F}_3 \)). The nonzero elements of \( K \) form a cyclic group generated by \( \theta \), whose elements are the powers of \( \theta \), namely, \( \theta, \theta^2 = 1 + 2\theta, \theta^3 = \theta + 2\theta^2 = \theta + 2 + 4\theta = 2 + 2\theta, \theta^4 = 2\theta + 2\theta^2 = \theta + 2 + 4\theta = 2, \theta^5 = 2\theta, \theta^6 = 2\theta^2 = 2 + 4\theta = 2 + \theta, \theta^7 = 2\theta + \theta^2 = 2\theta + 1 + 2\theta = 1 + \theta, \) and \( \theta^8 = \theta + \theta^2 = \theta + 1 + 2\theta = 1 \).
The multiplication table for elements of $K$ is

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
<th>$\theta$</th>
<th>$1 + 2\theta$</th>
<th>$2 + 2\theta$</th>
<th>$2\theta$</th>
<th>$2 + \theta$</th>
<th>$1 + \theta$</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>$\theta$</td>
<td>$1 + 2\theta$</td>
<td>$2 + 2\theta$</td>
<td>$2\theta$</td>
<td>$2 + \theta$</td>
<td>$1 + \theta$</td>
</tr>
<tr>
<td>$\theta$</td>
<td>0</td>
<td>$\theta$</td>
<td>$1 + 2\theta$</td>
<td>$2 + 2\theta$</td>
<td>$2\theta$</td>
<td>$2 + \theta$</td>
<td>$1 + \theta$</td>
<td>1</td>
</tr>
<tr>
<td>$1 + 2\theta$</td>
<td>0</td>
<td>$1 + 2\theta$</td>
<td>$2 + 2\theta$</td>
<td>$2\theta$</td>
<td>$2 + \theta$</td>
<td>$1 + \theta$</td>
<td>1</td>
<td>$\theta$</td>
</tr>
<tr>
<td>$2 + 2\theta$</td>
<td>0</td>
<td>$2 + 2\theta$</td>
<td>$2\theta$</td>
<td>$2 + \theta$</td>
<td>$1 + \theta$</td>
<td>1</td>
<td>$\theta$</td>
<td>$1 + 2\theta$</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>$2\theta$</td>
<td>$2 + \theta$</td>
<td>$1 + \theta$</td>
<td>1</td>
<td>$\theta$</td>
<td>$1 + 2\theta$</td>
<td>$2 + 2\theta$</td>
</tr>
<tr>
<td>$2\theta$</td>
<td>0</td>
<td>$2\theta$</td>
<td>$2 + \theta$</td>
<td>$1 + \theta$</td>
<td>1</td>
<td>$\theta$</td>
<td>$1 + 2\theta$</td>
<td>$2 + 2\theta$</td>
</tr>
<tr>
<td>$2 + \theta$</td>
<td>0</td>
<td>$2 + \theta$</td>
<td>$1 + \theta$</td>
<td>1</td>
<td>$\theta$</td>
<td>$1 + 2\theta$</td>
<td>$2 + 2\theta$</td>
<td>2</td>
</tr>
<tr>
<td>$1 + \theta$</td>
<td>0</td>
<td>$1 + \theta$</td>
<td>1</td>
<td>$\theta$</td>
<td>$1 + 2\theta$</td>
<td>$2 + 2\theta$</td>
<td>2</td>
<td>$2\theta$</td>
</tr>
</tbody>
</table>

27-element field. We get a field $K$ with 27 elements by adding a root of the cubic polynomial $h(x) = x^3 - x + 1$ to the field $\mathbb{F}_3$. This gives an extension of degree 3, so the size of the extension field is $|\mathbb{F}_3|^3 = 3^3 = 27$. Let $K = \mathbb{F}_3[x]/(h(x))$ and $\theta = \overline{x} = x + (h(x))$. Then $\theta^3 - \theta + 1 = 0$ so $\theta^3 = \theta - 1 = 2 + \theta$ (because the ground field of $K$ is $\mathbb{F}_3$). The nonzero elements of $K$ form a cyclic group of order 26 generated by $\theta$, whose elements are

$\theta$,
$\theta^2$,
$\theta^3 = 2 + \theta$,
$\theta^4 = 2\theta + \theta^2$,
$\theta^5 = 2\theta^2 + \theta^3 = 2 + \theta + 2\theta^2$,
$\theta^6 = 2\theta + \theta^2 + 2\theta^3 = 2\theta + \theta^2 + 4 + 2\theta = 1 + \theta + \theta^2$,
$\theta^7 = \theta + \theta^2 + \theta^3 = \theta + \theta^2 + 2 + \theta = 2 + 2\theta + \theta^2$,
$\theta^8 = 2\theta + 2\theta^2 + \theta^3 = 2\theta + 2\theta^2 + 2 + \theta = 2 + 2\theta^2$,
$\theta^9 = 2\theta + 2\theta^3 = 2\theta + 4 + 2\theta = 1 + \theta$,
$\theta^{10} = \theta + \theta^2$,
$\theta^{11} = \theta^2 + \theta^3 = 2 + \theta + \theta^2$,
$\theta^{12} = 2\theta + \theta^2 + \theta^3 = 2\theta + \theta^2 + 2 + \theta = 2 + \theta^2$,
\[ \varpi^{13} = 2\varpi + \varpi^3 = 2\varpi + 2 + \varpi = 2, \]
\[ \varpi^{14} = 2\varpi, \]
\[ \varpi^{15} = 2\varpi^2, \]
\[ \varpi^{16} = 2\varpi^3 = 4 + 2\varpi = 1 + 2\varpi, \]
\[ \varpi^{17} = \varpi + 2\varpi^2, \]
\[ \varpi^{18} = \varpi^2 + 2\varpi^3 = \varpi^2 + 4 + 2\varpi = 1 + 2\varpi + \varpi^2, \]
\[ \varpi^{19} = \varpi + 2\varpi^2 + \varpi^3 = \varpi + 2\varpi^2 + 2 + \varpi = 2 + 2\varpi + 2\varpi^2, \]
\[ \varpi^{20} = 2\varpi + 2\varpi^2 + 2\varpi^3 = 2\varpi + 2\varpi^2 + 4 + 2\varpi = 1 + \varpi + 2\varpi^2, \]
\[ \varpi^{21} = \varpi + \varpi^2 + 2\varpi^3 = \varpi + \varpi^2 + 4 + 2\varpi = 1 + \varpi^2, \]
\[ \varpi^{22} = \varpi + \varpi^3 = \varpi + 2 + \varpi = 2 + 2\varpi, \]
\[ \varpi^{23} = 2\varpi + 2\varpi^2, \]
\[ \varpi^{24} = 2\varpi^2 + 2\varpi^3 = 2\varpi^2 + 4 + 2\varpi = 1 + 2\varpi + 2\varpi^2, \]
\[ \varpi^{25} = \varpi + 2\varpi^2 + 2\varpi^3 = \varpi + 2\varpi^2 + 4 + 2\varpi = 1 + 2\varpi^2, \]
\[ \varpi^{26} = \varpi + 2\varpi^3 = \varpi + 4 + 2\varpi = 1. \]

This list of powers of \( \varpi \) is a form of multiplication table for \( K \). For example, to multiply \( 1 + \varpi \) and \( 2 + 2\varpi + 2\varpi^2 \) we note that \( \varpi^9 = 1 + \varpi \) and \( \varpi^{19} = 2 + 2\varpi + 2\varpi^2 \), hence

\[(1 + \varpi)(2 + 2\varpi + 2\varpi^2) = \varpi^9\varpi^{19} = \varpi^{28} = \varpi^2.\]

---

Homework #12, due 4/14/10 = \textbf{13.2.3, 13.2.4, 13.2.5, 13.2.7, 13.2.11} 
Additional problems recommended for study: \textbf{13.2.8, 13.2.10, 13.2.13, 13.2.14, 13.2.16, 13.2.17, 13.2.19, 13.2.20, 13.2.21} 

\textbf{13.2.3} Determine the minimal polynomial over \( \mathbb{Q} \) for the element \( 1 + i \). 
Let \( \alpha = 1 + i \). Noting \( i^2 = -1 \), we have

\[ \alpha^2 = (1 + i)^2 = 1^2 + i^2 + 2 \cdot 1 \cdot i = 1 - 1 + 2i = 2i = 2(\alpha - 1) \]
so $\alpha$ is a root of $x^2 - 2x + 2 \in \mathbb{Q}[x]$. This polynomial is irreducible by the Eisenstein criterion using prime 2, and it is monic, so it is the minimal polynomial of its roots, one of which is $\alpha$.

**13.2.4** Determine the degree over $\mathbb{Q}$ of $2 + \sqrt{3}$ and of $1 + \sqrt{2} + \sqrt{4}$.

First we note that $\mathbb{Q}(2 + \sqrt{3}) = \mathbb{Q}(\sqrt{3})$ and $\sqrt{3} \notin \mathbb{Q}$ so the degree of the extension $\mathbb{Q}(2 + \sqrt{3})$ cannot be 1, hence is 2 or more. But it cannot be more than 2, because $2 + \sqrt{3}$ satisfies the equation $(x - 2)^2 = 3$ and is therefore a root of the monic quadratic polynomial $x^2 - 4x + 1$. The degree of $\mathbb{Q}(2 + \sqrt{3})$ over $\mathbb{Q}$ is therefore 2, and the minimal polynomial of $2 + \sqrt{3}$ over $\mathbb{Q}$ is $x^2 - 4x + 2$.

Let $\beta = 1 + \sqrt{2} + \sqrt{4}$ and $\alpha = \sqrt{2}$. Notice that $\beta \in \mathbb{Q}(\alpha)$ because $\beta = 1 + \alpha + \alpha^2$, so we have $\mathbb{Q} \subseteq \mathbb{Q}(\beta) \subseteq \mathbb{Q}(\alpha)$. By “degree multiply” we have $[\mathbb{Q}(\alpha) : \mathbb{Q}(\beta)][\mathbb{Q}(\beta) : \mathbb{Q}] = [\mathbb{Q}(\alpha) : \mathbb{Q}]$. But $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$ since $\alpha$ is a root of the monic irreducible polynomial $x^3 - 2 \in \mathbb{Q}[x]$, so $[\mathbb{Q}(\beta) : \mathbb{Q}]$ divides 3. Therefore $[\mathbb{Q}(\beta) : \mathbb{Q}]$ must be either 1 or 3. To show it is 3, assume, to the contrary, that $[\mathbb{Q}(\beta) : \mathbb{Q}] = 1$. Then $\beta \in \mathbb{Q}$, and

\[
\beta^2 = (1 + \alpha + \alpha^2)^2 = 1 + \alpha^2 + \alpha^4 + 2\alpha + 2\alpha^2 + 2\alpha^3 = 1 + \alpha^2 + 2\alpha + 2\alpha^2 + 4 = 5 + 4\alpha + 3\alpha^2
\]

so

\[
\beta^2 - 3\beta = 5 + 4\alpha + 3\alpha^2 - 3(1 + \alpha + \alpha^2) = 2 + \alpha
\]

hence

\[
\alpha = \beta^2 - 3\beta - 2 \in \mathbb{Q}(\beta) = \mathbb{Q}
\]

which contradicts the fact that $\alpha \notin \mathbb{Q}$. Of course, these calculations also allow us to proceed slightly differently. We have $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$ so we need only show $\mathbb{Q}(\alpha) = \mathbb{Q}(\beta)$, but this follows from equations
derived above, namely, \( \beta = 1 + \alpha + \alpha^2 \in \mathbb{Q}(\alpha) \) and \( \alpha = \beta^2 - 3\beta - 2 \in \mathbb{Q}(\beta) \).

13.2.5 Let \( F = \mathbb{Q}(i) \). Prove that \( x^3 - 2 \) and \( x^3 - 3 \) are irreducible over \( F \).

[A more general theorem was proved in class that includes this problem as a special case. The problem could be solved by an appeal to this theorem, but the solution presented below essentially repeats the proof of the general theorem.]

Let \( \alpha = \sqrt[3]{2} \). Then \( \alpha \notin \mathbb{Q} \) and \( \alpha \) is a root of \( x^3 - 2 \in \mathbb{Q}[x] \). Since the monic irreducible cubic polynomial \( x^3 - 2 \in \mathbb{Q}[x] \) is irreducible by Eisenstein (via prime 2), it is the minimal polynomial of \( \alpha \) over \( \mathbb{Q} \). Therefore

(41) \[ [\mathbb{Q}(\alpha) : \mathbb{Q}] = 3 \]

Also, \( F \) is a quadratic extension of \( \mathbb{Q} \) since \( i \notin \mathbb{Q} \) and the degree of \( i \) is 2, because \( i \) is the root of the monic irreducible quadratic polynomial \( x^2 + 1 \) (so \( x^2 + 1 \) is the minimal polynomial of \( i \) over \( \mathbb{Q} \)). Thus

(42) \[ [F : \mathbb{Q}] = 2 \]

Consider the extension field \( K = \mathbb{Q}(\alpha, i) \) of \( \mathbb{Q} \). Now \( K \) has subfield \( F \), so by Corollary 13.15 and (42), \( [K : \mathbb{Q}] \) is divisible by 2. Similarly, \( K \) has subfield \( \mathbb{Q}(\alpha) \), so by Corollary 13.15 and (41), \( [K : \mathbb{Q}] \) is divisible by 3. Since \( [K : \mathbb{Q}] \) is divisible by both 2 and 3, and these two numbers are relatively prime, we have

(43) \[ [K : \mathbb{Q}] \geq 6 \]

Now \( \mathbb{Q} \) is contained in the extension field \( F \), so by Corollary 13.10 the minimal polynomial of \( \alpha \) over \( F \) must divide the minimal polynomial of \( \alpha \) over \( \mathbb{Q} \), hence \( m_{\alpha,F} | m_{\alpha,\mathbb{Q}} \). From above we know that \( m_{\alpha,\mathbb{Q}} = x^3 - 2 \), so

(44) \[ \deg(m_{\alpha,F}) \leq \deg(m_{\alpha,\mathbb{Q}}) = 3. \]
The degree of $F(\alpha)$ over $F$ is the degree of $m_{\alpha, F}$, and $K = F(\alpha)$, so by (43) and Th. 13.14 ("degrees multiply"), we have

$$6 \leq [K : \mathbb{Q}] = \deg(m_{\alpha, F})[F : \mathbb{Q}] = 2 \deg(m_{\alpha, F}),$$

hence

(45) \hspace{1cm} 3 \leq \deg(m_{\alpha, F}).

From (44) and (46) we have

(46) \hspace{1cm} 3 = \deg(m_{\alpha, F}) = [K : F] = F(\alpha) : F].

By (46) and the fact, established above, that $m_{\alpha, F}|x^3 - 2$, we have $m_{\alpha, F} = x^3 - 2$. Minimal polynomials are irreducible, so $x^3 - 2$ is irreducible over $F$.

Exactly the same argument also shows that $x^3 - 3$ is irreducible over $F$. This time, let $\beta = \sqrt[3]{3} \notin \mathbb{Q}$. Then $\beta$ is a root of $x^3 - 3 \in \mathbb{Q}[x]$. The monic irreducible cubic polynomial $x^3 - 3 \in \mathbb{Q}[x]$ is irreducible over $\mathbb{Q}$ by Eisenstein, this time using prime 3, so $x^3 - 3$ is the minimal polynomial of $\beta$ over $\mathbb{Q}$, $[\mathbb{Q}(\beta) : \mathbb{Q}] = 3$, etc.

13.2.7 Prove that $\mathbb{Q}(\sqrt{2} + \sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ [one inclusion is obvious; for the other consider $(\sqrt{2} + \sqrt{3})^2$, etc.] Find an irreducible polynomial satisfied by $\sqrt{2} + \sqrt{3}$.

Clearly, $\sqrt{2} + \sqrt{3} \in \mathbb{Q}(\sqrt{2}, \sqrt{3})$, so $\mathbb{Q}(\sqrt{2} + \sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Let $\alpha = \sqrt{2} + \sqrt{3}$. Then $\alpha^2 = 2 + 3 + 2\sqrt{2}\sqrt{3}$, so $\sqrt{2}\sqrt{3} = \frac{1}{2}(\alpha^2 - 5) \in \mathbb{Q}(\alpha)$. It follows that $\alpha\sqrt{2}\sqrt{3} - 2\alpha \in \mathbb{Q}(\alpha)$, but

$$\alpha\sqrt{2}\sqrt{3} - 2\alpha = (\sqrt{2} + \sqrt{3})\sqrt{2}\sqrt{3}$$

$$= 2\sqrt{3} + 3\sqrt{2} - 2\sqrt{2} - 2\sqrt{3}$$

$$= \sqrt{2}$$

so $\sqrt{2} \in \mathbb{Q}(\alpha)$, which implies that $\sqrt{3} = \alpha - \sqrt{2} \in \mathbb{Q}(\alpha)$. From these last two statements we get $\mathbb{Q}(\sqrt{2}, \sqrt{3}) \subseteq \mathbb{Q}(\alpha)$, as desired.

13.2.11(a) Let $\sqrt{3 + 4i}$ denote the square root of the complex number $3 + 4i$ that lies in the first quadrant and let $\sqrt{3 - 4i}$ denote the
square root of $3 - 4i$ that lies in the fourth quadrant. Prove that $[\mathbb{Q}(\sqrt{3 + 4i} + \sqrt{3 - 4i}) : \mathbb{Q}] = 1$. (b) Determine the degree of the extension $\mathbb{Q}(\sqrt{1 + \sqrt{-3}} + \sqrt{1 - \sqrt{-3}})$ over $\mathbb{Q}$.

(a) Conjugation is an isomorphism of the complex field $\mathbb{C}$ onto itself. The conjugate of $a + bi$ is $a - bi$. This map takes numbers in the first quadrant to numbers in the fourth, and numbers in the fourth quadrant to numbers in the first. It is a field isomorphism, and therefore takes square roots to square roots. In particular, since $\sqrt{3 + 4i}$ is a square root of $3 + 4i$, its conjugate is a square root of the conjugate $3 - 4i$ of $3 + 4i$. Furthermore, since $\sqrt{3 + 4i}$ is the square root of $3 + 4i$ in the first quadrant, its conjugate is the square root of $3 - 4i$ in the fourth quadrant, which is, by definition, $\sqrt{3 - 4i}$. Thus $\sqrt{3 + 4i}$ and $\sqrt{3 - 4i}$ are conjugates of each other. The sum of a complex number and its conjugate is a real number, so $\sqrt{3 + 4i} + \sqrt{3 - 4i} \in \mathbb{R}$. Next, note that

$$\begin{align*}
(\sqrt{3 + 4i} + \sqrt{3 - 4i})^2 &= (3 + 4i) + (3 - 4i) + 2\sqrt{3 + 4i}\sqrt{3 - 4i} \\
&= 6 + 2\sqrt{(3 + 4i)(3 - 4i)} \\
&= 6 + 2\sqrt{3^2 - 4^2i^2 + 12i - 12i} \\
&= 6 + 2\sqrt{9 + 16} \\
&= 6 + 2\sqrt{25} \\
&= 16
\end{align*}$$

so $\sqrt{3 + 4i} + \sqrt{3 - 4i} = 4 \in \mathbb{Q}$. It follows that $\mathbb{Q}(\sqrt{3 + 4i} + \sqrt{3 - 4i}) = \mathbb{Q}$, so $[\mathbb{Q}(\sqrt{3 + 4i} + \sqrt{3 - 4i}) : \mathbb{Q}] = 1$.

13.2.11(b) Repeating the opening remarks of part (a), we conclude that $\sqrt{1 + \sqrt{-3}} + \sqrt{1 - \sqrt{-3}} \in \mathbb{R}$. Now calculate:

$$\begin{align*}
\left(\sqrt{1 + \sqrt{-3}} + \sqrt{1 - \sqrt{-3}}\right)^2 &= (1 + \sqrt{-3}) + (1 - \sqrt{-3}) + 2\sqrt{1 + \sqrt{-3}}\sqrt{1 - \sqrt{-3}} \\
&= 2 + 2\sqrt{(1 + \sqrt{-3})(1 - \sqrt{-3})}
\end{align*}$$
\[ = 2 + 2\sqrt{1^2 - \sqrt{-3}^2} \]
\[ = 2 + 2\sqrt{1 + 3} \]
\[ = 2 + 2\sqrt{4} \]
\[ = 6 \]

so
\[ \sqrt{1 + \sqrt{-3}} + \sqrt{1 - \sqrt{-3}} = \pm\sqrt{6} \]
hence
\[ \mathbb{Q}\left(\sqrt{1 + \sqrt{-3}} + \sqrt{1 - \sqrt{-3}}\right) = \mathbb{Q}\left(\sqrt{6}\right) \]
and the degree of \( \mathbb{Q}\left(\sqrt{6}\right) \) over \( \mathbb{Q} \) is 2, so the degree of the extension \( \mathbb{Q}\left(\sqrt{1 + \sqrt{-3}} + \sqrt{1 - \sqrt{-3}}\right) \) over \( \mathbb{Q} \) is also 2.

Homework #13, due 4/21/10 = 13.2.12, 13.3.1, 13.3.2, 13.3.4, 13.4.1, 13.4.2

Additional problems recommended for study: 13.3.3, 13.3.5, 13.4.3, 13.4.4, 13.4.5, 13.4.6

13.2.12 Suppose the degree of the extension \( K/F \) is a prime \( p \). Show that any subfield \( E \) of \( K \) containing \( F \) is either \( K \) or \( F \).

By the theorem that “degrees multiply”, we have
\[ (47) \quad p = [K : F] = [K : E][E : F] \]
so \([E : F]\) is a positive integer that divides the prime \( p \), and therefore must be equal to 1 or \( p \). If \([E : F] = 1\) then \( E = F \). If \([E : F] = p\) then \([K : E] = 1\) by (47), so \( K = F \). Thus either \( K = E \) or \( F = E \).

13.3.1 Prove that it is impossible to construct the regular 9-gon.

The angles in a regular 9-gon are all equal to \( \frac{360^\circ}{9} = 40^\circ \). Angles can be bisected with compass and straightedge, so if a 9-gon could be constructed, then one of its angles could be bisected, producing a 20° angle, from which it would be possible to construct \( \cos(20^\circ) \). However,
by the proof of Th. 13.24(II), \( \cos(20^\circ) \) is not constructible. In fact, 
\( 20^\circ \) has degree 3 over \( \mathbb{Q} \) because \( 2 \cos(20^\circ) \) satisfies the irreducible cubic polynomial \( x^3 - 3x - 1 \).

13.3.2 Prove that Archimedes’ construction actually trisects the angle \( \theta \). [Note that isosceles triangles in Figure 5 to prove that \( \beta = \gamma = 2\alpha \).]

Refer to Figure 5 in the text. Let \( O \) be the center of the circle of radius 1. Let \( P \) be the point outside the circle and lying on a diameter of the circle. Let \( X \) and \( Y \) be the points on the circle such that \( P, X, \) and \( Y \) are collinear, and \( X \) is between \( P \) and \( Y \). By hypothesis, \( PX = 1 \). Let \( \alpha = \angle XPO, \beta = \angle YXO, \gamma = \angle XYO \), and let \( \theta \) be the angle between the diameter \( PO \) and the radius \( OY \), such that \( \theta \) is an exterior angle of \( \triangle PYO \).

Then, by the pons asinorum, \( \alpha = \angle XPO = \angle XOP \) because \( \triangle PXO \) is isosceles with base \( PO \). Note that \( \beta \) is an exterior angle of \( \triangle PXO \) and is therefore equal to the sum of the two remote interior angles, which are \( \angle XPO \) and \( \angle XOP \). These two angles are both equal to \( \alpha \), so \( \beta = 2\alpha \).

By the pons asinorum, \( \beta = \angle YXO = \angle XYO = \gamma \) because \( \triangle XOY \) is isosceles with base \( XY \). Note that since \( \theta \) is an exterior angle of \( \triangle PYO \), we have \( \theta = \gamma + \alpha = \beta + \alpha = 2\alpha + \alpha = 3\alpha \).

13.3.4 The construction of the regular 7-gon amounts to the constructibility of \( \cos(2\pi/7) \). We shall see later (Section 14.5 and Exercise 2 of Section 14.7) that \( \alpha = \cos(2\pi/7) \) satisfies the equation \( x^3 + x^2 - 2x - 1 = 0 \). Use this to prove that the regular 7-gon is not constructible by straightedge and compass.

If \( p(x) = x^3 + x^2 - 2x - 1 \) can be factored over \( \mathbb{Q} \), then by Gauss’s Lemma it can be factored over \( \mathbb{Z} \), and hence has a root in \( \mathbb{Z} \) which must divide 1. But \( p(1) = -1 \neq 0 \) and \( p(-1) = 1 \neq 0 \), so \( p(x) = x^3 + x^2 - 2x - 1 \) is irreducible over \( \mathbb{Q} \). Consequently its roots (including \( \alpha \)) have degree 3 over \( \mathbb{Q} \) and therefore do not lie in an finite dimensional extension of \( \mathbb{Q} \) whose dimension is a power of 2, and hence \( \alpha \) is not constructible.

13.4.1 Determine the splitting field and its degree over \( \mathbb{Q} \) for \( x^4 - 2 \).
To find the roots of $x^4 - 2$, factor it:

$$x^4 - 2 = (x^2 + \sqrt{2})(x^2 - \sqrt{2}) = (x + \sqrt[4]{2}i)(x - \sqrt[4]{2}i)(x + \sqrt{2})(x - \sqrt{2})$$

The roots of $x^4 - 2$ are therefore $-\sqrt[4]{2}i$, $\sqrt[4]{2}i$, $-\sqrt{2}$, and $\sqrt{2}$, so the splitting field is

$$F := \mathbb{Q}(\sqrt[4]{2}i, -\sqrt{2}i, \sqrt{2}, -\sqrt{2})$$

Obviously

$$F = \mathbb{Q}(\sqrt[4]{2}i, \sqrt{2}) = \mathbb{Q}(i, \sqrt{2})$$

Note that $i$ is not in $\mathbb{Q}(\sqrt{2})$ because the latter field is contained in the real numbers $\mathbb{R}$, but $i \notin \mathbb{R}$. So the extension obtained by adding $i$ to $\mathbb{Q}(\sqrt{2})$ is a proper extension and therefore has degree at least 2. On the other hand, $i$ is a root of the quadratic polynomial $x^2 + 1 \in \mathbb{Q}(\sqrt{2})[x]$, so the degree can also not be any more than 2, and therefore is exactly 2. Thus

$$[\mathbb{Q}(i, \sqrt{2}) : \mathbb{Q}(\sqrt{2})] = 2.$$ 

We also know that

$$[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 4$$

because $\sqrt{2}$ is a root of the polynomial $x^4 - 2$ which is irreducible over $\mathbb{Q}$ by Eisenstein, using prime 2. We therefore have (by the "degrees multiply" theorem)

$$[F : \mathbb{Q}] = [\mathbb{Q}(i, \sqrt{2}) : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2 \cdot 4 = 8$$

so the degree of the splitting field $F$ over $\mathbb{Q}$ is 8.

**13.4.2** Determine the splitting field and its degree over $\mathbb{Q}$ for $x^4 + 2$.

The roots of $x^4 + 2$ are $\frac{\pm(1+i)}{\sqrt{2}}$, so the splitting field of $x^4 + 2$ is

$$F := \mathbb{Q}\left(\frac{1+i}{\sqrt{2}}, \frac{1-i}{\sqrt{2}}, \frac{-1+i}{\sqrt{2}}, \frac{-1-i}{\sqrt{2}}\right).$$

We must compute its degree over $\mathbb{Q}$. Let $\alpha = \frac{1+i}{\sqrt{2}}$. Then, using the first two of the roots, we get $\sqrt{2} \in F$ because

$$\sqrt{2} = \left(\frac{1}{2} \left(\frac{2}{\sqrt{2}}\right)\right)^{-1} = \left(\frac{1}{2} \left(\frac{1+i}{\sqrt{2}} + \frac{1-i}{\sqrt{2}}\right)\right)^{-1} \in F.$$
We then conclude that $i \in F$ because
$$i = \alpha \sqrt{2} - 1 \in F.$$ 
Therefore we now know that $\mathbb{Q}(\sqrt{2}, i) \subseteq F$, but the opposite inclusion is obvious, so
$$F = \mathbb{Q}(\sqrt{2}, i),$$
and $[F : \mathbb{Q}] = 8$, as was shown in the previous problem.

Homework #14, due 4/28/10 = 14.1.1, 14.1.2, 14.1.3, 14.1.4, 14.2.1, 14.2.2,
Additional problems recommended for study: 13.4.3, 13.4.4, 13.4.5, 13.4.6, 14.1.5, 14.1.6, 14.1.7, 14.1.8, 14.1.9, 14.2.4, 14.2.5, 14.2.6, 14.2.7, 14.2.8, 14.2.10, 14.2.12, 14.2.14

14.1.1(a) Show that if the field $K$ is generated over $F$ by the elements $\alpha_1, \ldots, \alpha_n$ then an automorphism $\sigma$ of $K$ fixing $F$ is uniquely determined by $\sigma(\alpha_1), \ldots, \sigma(\alpha_n)$. In particular show that an automorphism fixes $K$ if and only if it fixes a [i.e., every] set of generators for $K$.

Except for some minor notational changes, the following proof works for an arbitrary (and possibly infinite) set of generators of $K$ over $F$.

Assume $K = F(\alpha_1, \ldots, \alpha_n)$ and $\sigma$ is an automorphism of $K$ fixing $F$. To show $\sigma$ is uniquely determined by $\sigma(\alpha_1), \ldots, \sigma(\alpha_n)$, assume that $\tau$ is some other automorphism of $K$ that fixes $F$ and agrees with $\sigma$ on the generators, i.e.

(48) \hspace{1cm} \sigma(\alpha_1) = \tau(\alpha_1), \ldots, \sigma(\alpha_n) = \tau(\alpha_n).

Let $E := \{\beta \in K | \sigma(\beta) = \tau(\beta)\}$ be the set of elements of $K$ on which $\tau$ and $\sigma$ agree. We show that $E$ is a field containing $F$ and every $\alpha_i$.

First we note that $\alpha_1, \ldots, \alpha_n \in E$ by (48), and $F \subseteq E$ because $\tau$ and $\sigma$ are both the identity function on elements of $F$, so if $\beta \in F$ then $\beta = \tau(\beta) = \sigma(\beta)$. Suppose $\beta, \gamma \in E$. Then $\beta \gamma^{-1} \in E$ because

$$\sigma(\beta \gamma^{-1}) = \sigma(\beta)\sigma(\gamma)^{-1} \hspace{1cm} \sigma \text{ is an automorphism}$$
$$= \tau(\beta)\tau(\gamma)^{-1} \hspace{1cm} \beta, \gamma \in E$$
\[ \tau(\beta \gamma^{-1}) \quad \tau \text{ is an automorphism} \]
and \( \beta \pm \gamma \in E \) because
\[
\sigma(\beta \pm \gamma) = \sigma(\beta) \pm \sigma(\gamma) \quad \sigma \text{ is an automorphism}
= \tau(\beta) \pm \tau(\gamma) \quad \beta, \gamma \in E
= \tau(\beta \pm \gamma) \quad \tau \text{ is an automorphism}
\]
Since \( E \) is a field containing \( F \) and \( \alpha_1, \ldots, \alpha_n \), we have \( K = F(\alpha_1, \ldots, \alpha_n) \subseteq E \), but by definition we have \( E \subseteq K \), so \( E = K \). This means that \( \sigma \) and \( \tau \) agree on every element in their domain \( K \), and are therefore the same function.

If an automorphism fixes \( K \) then it obviously fixes every subfield \( F \) of \( K \) and every set of generators of \( K \) over \( F \).

Conversely, for every set \( A \subseteq K \) of generators and every subfield \( F \), if an automorphism \( \sigma \) fixes \( F \) and \( A \) then it agrees on \( A \) with the identity function on \( K \), which is an automorphism of \( K \) fixing \( F \). By what was proved above, it follows that the \( \sigma \) and the identity function on \( K \) must be the same.

14.1.1(b) Let \( G \leq \text{Gal}(K/F) \) be a subgroup of the Galois group of the extension \( K/F \) and suppose \( \sigma_1, \ldots, \sigma_k \) are generators for \( G \). Show that the subfield \( E/F \) is fixed by \( G \) if and only if it is fixed by the generators \( \sigma_1, \ldots, \sigma_k \).

One direction is trivial, for if \( G \) fixes \( E/F \) then all its elements fix \( E/F \), including the generators \( \sigma_1, \ldots, \sigma_k \). We therefore need only assume \( E/F \) is fixed by the generators \( \sigma_1, \ldots, \sigma_k \) and show that \( E/F \) is fixed by \( G \). Let \( H \) be the set of elements of \( G \) that fix \( E/F \), that is,
\[
H = \{ g \in G | \forall \beta \in E (g(\beta) = \beta) \}.
\]
Then the generators are in \( H \) because, by hypothesis, they fix \( E/F \). We show now that \( H \) is closed under the group operations. Let \( g, h \in H \), that is, \( g \) and \( h \) fix \( E/F \). Then, for every \( \beta \in E \),
\[
(g \circ h)(\beta) = g(h(\beta))
\]
\[ g(\beta) = \beta \quad \text{since } g \text{ fixes } E/F \]

so \( g \circ h \in E \), and \( g^{-1} \in H \) because

\[
g^{-1}(\beta) = g^{-1}(g(\beta)) \quad \text{since } g \text{ fixes } E/F
\]

\[ = (g^{-1} \circ g)(\beta) = 1(\beta) = \beta \]

We have shown that \( H \) is a subgroup of \( G \) that contains the generators of \( G \), so \( G = H \). By the definition of \( H \), we conclude \( G \) fixes \( E/F \).

**14.1.2** Let \( \tau \) be the map \( \tau : \mathbb{C} \rightarrow \mathbb{C} \) defined by \( \tau(a + bi) = a - bi \) (complex conjugation). Prove that \( \tau \) is an automorphism of \( \mathbb{C} \).

First note that \( \tau \) behaves properly with respect to addition and subtraction because

\[
\tau((a + bi) + (c + di)) = \tau(a + c + (b + d)i)
\]

\[ = a + c - (b + d)i \]

\[ = a - bi + c - di \]

\[ = \tau(c + di) + \tau(c + di) \]

and

\[
\tau((a + bi) - (c + di)) = \tau(a + c - (b + d)i)
\]

\[ = a + c + (b + d)i \]

\[ = a + bi + c + di \]

\[ = \tau(a - bi) + \tau(c - di) \]

For multiplication, we have

\[
\tau((a + bi)(c + di)) = \tau(ac - bd + (bc + ad)i)
\]

\[ = ac - bd - (bc + ad)i \]

\[ = (a - bi)(c - di) \]

\[ = \tau(a + bi)\tau(c + di) \]
For quotients, first note that
\[ \tau \left( \frac{a + bi}{c + di} \right) = \tau \left( \frac{(a + bi)(c - di)}{(c + di)(c - di)} \right) \]
\[ = \tau \left( \frac{(ac + bd) + (bc - ad)i}{c^2 + d^2} \right) = \frac{(ac + bd) + (ad - bc)i}{c^2 + d^2} \]
but we also have
\[ \frac{\tau(a + bi)}{\tau(c + di)} = \frac{a - bi}{c - di} = \frac{(a - bi)(c + di)}{(c - di)(c + di)} = \frac{(ac + bd) + (ad - bc)i}{c^2 + d^2} \]
so
\[ \tau \left( \frac{a + bi}{c + di} \right) = \frac{\tau(a + bi)}{\tau(c + di)}. \]
Note that \( \tau \) is its own inverse (\( \tau^{-1} = \tau \) because \( \tau \circ \tau \) is the identity function on \( \mathbb{C} \)), and hence is bijective. Therefore \( \tau \) is an automorphism of \( \mathbb{C} \).

**14.1.3** Determine the fixed field of complex conjugation on \( \mathbb{C} \).

Let \( \tau \) be complex conjugation, as in the previous problem. Certainly \( \tau \) fixes \( \mathbb{R} \), for if \( a \in \mathbb{R} \) then \( \tau(a) = \tau(a + 0i) = a - 0i = a \). Suppose \( a, b \in \mathbb{R} \) and \( a + bi \) is fixed by \( \tau \). Then \( \tau(a + bi) = a - bi = a + bi \), so \( 0 = 2bi \), hence \( b = 0 \), hence \( a + bi = a \in \mathbb{R} \). Thus the fixed field of \( \tau \) is \( \mathbb{R} \).

**14.1.4** Prove that \( \mathbb{Q}(\sqrt{2}) \) and \( \mathbb{Q}(\sqrt{3}) \) are not isomorphic.

Assume, to the contrary, that there is some \( \sigma \) which is an isomorphism from \( \mathbb{Q}(\sqrt{2}) \) onto \( \mathbb{Q}(\sqrt{3}) \). Then \( \sigma(1) = 1 \) and, more generally, \( \sigma(q) = q \) for all \( q \in \mathbb{Q} \). Consider the element \( \sigma(\sqrt{2}) \in \mathbb{Q}(\sqrt{3}) \). Since \( \mathbb{Q}(\sqrt{3}) \) is a quadratic extension of \( \mathbb{Q} \) and has basis \( \{1, \sqrt{3}\} \), there are \( a, b \in \mathbb{Q} \) such that \( \sigma(\sqrt{2}) = a + b\sqrt{3} \). Squaring both sides and using the hypothesis that \( \sigma \) is an isomorphism, we get
\[ 2 = \sigma(2) = \sigma(\sqrt{2})^2 = (\sigma(\sqrt{2}))^2 = (a + b\sqrt{3})^2 = a^2 + 2ab\sqrt{3} + 3b^2. \]
If \( ab \neq 0 \) then, since \( a, b \in \mathbb{Q} \),
\[ \sqrt{3} = \frac{2 - a^2 - 3b^2}{2ab} \in \mathbb{Q}. \]
But this is a contradiction, so \( ab = 0 \), hence \( a = 0 \) or \( b = 0 \). If \( a = 0 \) then, by (49), \( 2 = 3b^2 \), which implies that \( \sqrt{\frac{2}{3}} = b \in \mathbb{Q} \), a contradiction. If \( b = 0 \), then (49) implies \( \sqrt{2} = a \in \mathbb{Q} \), again a contradiction. This shows no such isomorphism \( \sigma \) can exist, hence \( \mathbb{Q}(\sqrt{2}) \not\cong \mathbb{Q}(\sqrt{3}) \).

14.2.1 Determine the minimal polynomial over \( \mathbb{Q} \) for the element \( \sqrt{2} + \sqrt{5} \).

Let \( p = 2 \) and \( q = 5 \) and \( \alpha = \sqrt{p} + \sqrt{q} \). Then \( \alpha^2 = p + q + 2\sqrt{pq} \), so

\[
4pq = (\alpha^2 - (p + q))^2 = \alpha^4 - 2\alpha^2(p + q) + (p^2 + 2pq + q^2)
\]

so

\[
0 = \alpha^4 - 2\alpha^2(p + q) + (p - q)^2
\]

With \( p = 2 \) and \( q = 5 \), we get \( 0 = \alpha^4 - 14\alpha^2 + 9 \) and the minimal polynomial of \( \alpha \) is \( x^4 - 14x^2 + 9 \).

14.2.2 Determine the minimal polynomial over \( \mathbb{Q} \) for the element \( 1 + \sqrt[3]{2} + \sqrt[3]{4} \).

Let \( p = 2 \) and \( \alpha = 1 + \sqrt[3]{p} + \sqrt[3]{p^2} \). Then \( \alpha - 1 = \sqrt[3]{p} + \sqrt[3]{p^2} \), so, cubing both sides, we have

\[
\alpha^3 - 3\alpha^2 + 3\alpha - 1 = (\alpha - 1)^3 = p(1 + \sqrt[3]{p})^3
\]

\[
= p(1 + 3\sqrt[3]{p} + 3\sqrt[3]{p^2} + p)
\]

\[
= p(1 + 3(\alpha - 1) + p)
\]

\[
= p(p - 2 + 3\alpha)
\]

\[
= p^2 - 2p + 3p\alpha
\]

It follows that

\[
\alpha^3 - 3\alpha^2 + 3(1-p)\alpha - (p-1)^2 = 0.
\]

The minimal polynomial of \( \alpha \) over \( \mathbb{Q} \) is

\[
x^3 - 3x^2 + 3(1-p)x - (p-1)^2.
\]

With \( p = 2 \) we conclude that the minimal polynomial of \( \alpha \) over \( \mathbb{Q} \) is

\[
x^3 - 3x^2 - 3x - 1
\]