SOLUTIONS to DUMMIT'S *ABSTRACT ALGEBRA*

A Solutions Manual of Dubious Quality

Kyle Mickelson

Last updated: June 4th, 2025

Contents

❋ Introduction to Groups

1.1 Basic Axioms and Examples

Exercise 1.1.1. Determine which of the following binary operations are associative:
(a) the operation $*$ on $\mathbb{Z}$ defined by $a * b = a - b$
(b) the operation $*$ on $\mathbb{R}$ defined by $a * b = a + b + ab$
(c) the operation $*$ on $\mathbb{Q}$ defined by $a * b = \frac{a+b}{5}$
(d) the operation $*$ on $\mathbb{Z} \times \mathbb{Z}$ defined by $(a, b) * (c, d) = (ad + bc, ad)$
(e) the operation $*$ on $\mathbb{Q} - \{0\}$ defined by $a * b = \frac{a}{b}$.

Proof. (a) Note that under this operation $1*(2*3) = 1*-1 = 2$ while $(1*2)*3 = -4$, so that clearly the operation $*$ is not associatibve on $\mathbb{Z}$.

(b) Let $a, b, c \in \mathbb{R}$ and observe that

$$\begin{aligned} a * (b * c) &= a * (b + c + bc) \\ &= a + b + c + bc + ab + ac + abc \\ &= (a + b + ab) + c + c(a + b + ab) \\ &= (a + b + ab) * c \\ &= (a * b) * c \end{aligned}$$

and hence $*$ on $\mathbb{R}$ is associative.

(c) Note that under this operation we have

$$1 * (0 * -1/5) = 1 * (\frac{-1/5}{5}) = \frac{1 - 1/25}{5} = \frac{24}{5}$$

$$(1 * 0) * -1/5 = 1/5 * -1/5 = \frac{0}{5} = 0$$

and hence $*$ on $\mathbb{Q}$ cannot be associative.

(d) Let $a, b, c, d, e, f \in \mathbb{Z}$ be arbitrary. We may observe that

$$\begin{aligned} (a, b) * ((c, d) * (e, f)) &= (a, b) * (cf + de, df) \\ &= (adf + bcf + bde, bdf) \\ &= ((ad + bc)f + (bd)e, (bd)f) \\ &= (ad + bc, bd) * (e, f) \\ &= ((a, b) * (c, d)) * (e, f) \end{aligned}$$

and hence $*$ is associative on $\mathbb{Z} \times \mathbb{Z}$.

(e) Finally, note that under this binary operation we have

$$2 * (3 * 2) = 2 * \frac{3}{2} = \frac{2}{\frac{3}{2}} = \frac{4}{3}$$

$$(2 * 3) * 2 = \frac{2}{3} * 2 = \frac{\frac{2}{3}}{2} = \frac{1}{3}$$

and hence the operation $*$ is not associative on $\mathbb{Q} \setminus \{0\}$. ■

Exercise 1.1.2. Decide which of the binary operations in the preceding exercise are commutative.

Proof. For part (a), taking $a = 1$ and $b = 2$ gives that $a - b = -1$ and $b - a = 1$, so that the binary operation $*$ in part (a) is certainly not commutative.

For part (b), the operation $*$ is commutative via the commutativity of addition and multiplication in $\mathbb{R}$, as

$$a * b = a + b + ab = b + a + ba = b * a$$

for all $a, b \in \mathbb{R}$.

For part (c), the operation $*$ is once again commutative by the property of commutativity of addition in $\mathbb{Q}$, as

$$a * b = \frac{a + b}{5} = \frac{b + a}{5} = b * a$$

for all $a, b \in \mathbb{Q}$.

For part (d), the operation $*$ is once again commutative by commutativity of addition in $\mathbb{Z}$, as we have that

$$(a, b) * (c, d) = (ad + bc, bd) = (cb + da, db) = (c, d) * (a, b)$$

for all $a, b, c, d \in \mathbb{Z}$.

Finally, for part (e) we have

$$1 * 2 = \frac{1}{2} \neq 2 = \frac{2}{1} = 2 * 1$$

so that $*$ on $\mathbb{Q} \setminus \{0\}$ is certainly not a commutative binary operation. ■

Exercise 1.1.3. Prove that addition of residue classes in $\mathbb{Z}/n\mathbb{Z}$ is associative (you may assume it is well defined).

Proof. We take integers a, b, c and consider the residue classes modulo n, which we denote by $\overline{a}$, $\overline{b}$, and $\overline{c}$, respectively. We observe that

$$(\overline{a}+\overline{b})+\overline{c}=\overline{(a+b)}+\overline{c}=\overline{(a+b)+c}=\overline{a+(b+c)}=\overline{a}+\overline{(b+c)}=\overline{a}+(\overline{b}+\overline{c})$$

where the third equality holds by the associativity of addition in $\mathbb{Z}$. ■

Exercise 1.1.4. Prove that multiplication of residue classes in $\mathbb{Z}/n\mathbb{Z}$ is associative (you may assume it is well defined).

Proof. We take integers a, b, c and consider the residue classes modulo n, which we denote by $\overline{a}$, $\overline{b}$, and $\overline{c}$, respectively. We observe that

$$(\overline{a}\cdot\overline{b})\cdot\overline{c}=\overline{(ab)}\cdot\overline{c}=\overline{(a\cdot b)\cdot c}=\overline{a\cdot(b\cdot c)}=\overline{a}\cdot\overline{(b\cdot c)}=\overline{a}\cdot(\overline{b}\cdot\overline{c})$$

where the third equality holds by the associativity of multiplication in $\mathbb{Z}$. ■

Exercise 1.1.5 Prove for all $n > 1$ that $\mathbb{Z}/n\mathbb{Z}$ is not a group under multiplication of residue classes.

Proof. Suppose $n > 1$. Then the set $\mathbb{Z}/n\mathbb{Z}$ contains at least 2 elements. Namely, $\overline{0}$ is one such element. Note that under multiplication, the identity element for $\mathbb{Z}/n\mathbb{Z}$ must be $\overline{1}$. However, note that there is no integer x for which $0 \cdot x = 1$, and therefore the element $\overline{0} \in \mathbb{Z}/n\mathbb{Z}$ cannot have an inverse. Thus, $(\mathbb{Z}/n\mathbb{Z}, \cdot)$ is not a group. ■

Exercise 1.1.6.

Exercise 1.1.7.

Exercise 1.1.8. Let $G = \{z \in \mathbb{C} \mid z^n = 1 \text{ for some } n \in \mathbb{Z}\}$.
(a) Prove that G is a group under multiplication (called the group of *roots of unity* in $\mathbb{C}$).
(b) Prove that G is not a group under addition.

Proof. (a) Let $G = \{z \in \mathbb{C} : z^n = 1,\ n \in \mathbb{Z}^+\}$. First we show closure, let $x, y \in G$, such that $x^n = 1$ and $y^m = 1$. Then $(xy)^{nm} = x^{mn}y^{mn} = (x^n)^m(y^m)^n = 1^m1^n = 1$, and hence $xy \in G$. The identity element of G is 1 trivially. G also contains inverses of all elements, as if $z^n = 1 \implies z^{-n} = (z^{-1})^n = 1$, and hence $z^{-1} \in G$. Associativity follows from the associativity of multiplication in $\mathbb{C}$.

(b) To show that G is not a group under addition, note that G under addition does not have an identity element, as $0^n \neq 1$ for any $n \in \mathbb{Z}^+$. Therefore G is not a group under addition. ■

Exercise 1.1.9.

Exercise 1.1.10.

Exercise 1.1.11.

Exercise 1.1.12.

Exercise 1.1.13.

Exercise 1.1.14.

Exercise 1.1.15.

Exercise 1.1.16. Let x be an element of G. Prove that $x^2 = 1$ if and only if $|x|$ is either 1 or 2.

Proof. Let $x \in G$. Suppose $x^2 = 1$. Then we see that either x is of order 2 (by definition) or that $x = 1$. Conversely, suppose $|x|$ is 1 or 2. Then by definition, $x^2 = 1$, as desired. ∎

Exercise 1.1.17.

Exercise 1.1.18.

Exercise 1.1.19. Let $x \in G$ and let $a, b \in \mathbb{Z}^+$.
(a) Prove that $x^{a+b} = x^a x^b$ and $(x^a)^b = x^{ab}$.
(b) Prove that $(x^a)^{-1} = x^{-a}$.
(c) Establish part (a) for arbitrary integers a and b (positive, negative, or zero).

Proof. (a) Let $x \in G$ and $a, b \in \mathbb{Z}^+$. See $x^{a+b} = x^a x^b$ by exponent rules. Also, $(x^a)^b = x^{ab}$ by the same.

(b) By the result proven in second half part (a), substituting $b = -1$, we can see that $(x^a)^{-1} = x^{-a}$.

(c) By the rules of exponents, which are satisfied for any arbitrary integers a and b, the above hold similarly. ∎

Exercise 1.1.20. For $x \in G$, show that x and x^{-1} have the same order.

Proof. Suppose G is a group and $x \in G$. Since G is closed under inverses, $x^{-1} \in G$. Either $|x| = \infty$ or $|x| = n < \infty$. If $|x| = \infty$, we claim that $|x^{-1}| = \infty$ also. To show this, assume, for contradiction, that $|x| = \infty$ and $|x^{-1}| = n < \infty$. Then we know:

$$(x^{-1})^n = 1 \implies x^{-n} = 1 \iff x^n = 1$$

Which is a contradiction to $|x| = \infty$. Therefore, if $|x| = \infty$, we have $|x^{-1}| = \infty$ also. The same is true for x^{-1} without loss of generality. From this, we may now only consider the cases where both $|x|$ and $|x^{-1}|$ are finite.

Now let $|x| = n < \infty$ and $|x^{-1}| = m < \infty$, and suppose $n < m$. We may write:

$$x^n = 1 \iff x^{-n} = (x^{-1})^n = 1$$

But we assumed m was the least positive integer for which $(x^{-1})^m = 1$, so this is a contradiction; hence $n \geq m$. But if this is the case, then:

$$(x^{-1})^m = 1 \implies x^{-m} = 1 \iff x^m = 1$$

Which is a contradiction to n being the least positive integer for which $x^n = 1$. Therefore $n \leq m$; hence we may conclude that $n = m$, and so $|x| = |x^{-1}|$. ■

Exercise 1.1.21. Let G be a finite group and let x be an element of G of order n. Prove that if n is odd, then $x = (x^2)^k$ for some k.

Proof. Let $x \in G$ where G is finite and $|x| = n$. Suppose n is odd. Then $n = 2m+1$ for some $m \in \mathbb{N}_{\geq 0}$. Now, $x^n = x^{2m+1} = x^{2m}x = (x^2)^m x = 1$. Applying x to the right of both sides, we find $(x^2)^m x^2 = x \implies (x^2)^{m+1} = x$. Set $k = m+1$ and now we see that $x = (x^2)^k$ for some integer $k \geq 1$ as desired. ■

Exercise 1.1.22. If x and g are elements of the group G, prove that $|x| = |gxg^{-1}|$. Deduce that $|ab| = |ba|$ for all $a, b \in G$.

Proof. Let $x, g \in G$, and suppose $|x| = n$ and $|g^{-1}xg| = m$. Then $x^n = 1$ and $(g^{-1}xg)^m = 1$. Then we see $(g^{-1})^m x^m g^m = g^{-m}x^{m-n}x^n g^m = g^{-m}x^{m-n}g^m = 1$. Applying g to the right of the previous equation, find $x^{m-n}g^m = g^m \implies x^{m-n} = 1 \implies x^n = x^m$ Hence we see that $x^n = x^m = 1$ so $n = m$. In the case where the order of x is infinite, note that the order of $g^{-1}xg$ must also be infinite, as if $|g^{-1}xg| = k$, then $(g^{-1}xg)^k = 1 \implies x^k = 1$, but this contradicts the infinite order of x. Thus if $|x| = \infty$, then $|g^{-1}xg| = \infty$. Hence we have proved that $|x| = |g^{-1}xg|$. Substituting $x = a$ and $g = ab$, we can also use the above to deduce that $|ab| = |ba|$, where $a, b \in G$. ■

Exercise 1.1.23. Suppose $x \in G$ and $|x| = n < \infty$. If $n = st$ for $s, t \in \mathbb{Z}^+$, prove $|x^s| = t$.

Proof. Suppose $x \in G$ and $|x| = n$. Then $x^n = 1$, to which $x^n = x^{st} = 1$, and so $(x^s)^t = 1$. We will show that t is the smallest integer to force this relation. Since n is the smallest such integer for which $x^n = 1$, it follows that if $t' < t$, and $n = st$, then:

$$st' < st = n \iff (x^s)^{t'} \neq 1$$

And so t is the smallest such positive integer; hence $|x^s| = t$. ■

Exercise 1.1.24. If a and b are commuting elements of G, prove that $(ab)^n = a^n b^n$ for all $n \in \mathbb{Z}$.

Proof. Take $a, b \in G$ as above. In the $n = 1$ case, note $(ab)^1 = a^1 b^1$ trivially holds. Suppose it holds for the nth case; so we have $(ab)^n = a^n b^n$. Then:

$$\begin{aligned}(ab)^{n+1} &= (ab)^n(ab) \\ &= a^n b^n (ab) \\ &= a^n b^n (ba) \\ &= a^n b^{n+1} a \\ &= a^n a b^{n+1} \\ &= a^{n+1} b^{n+1}\end{aligned}$$

Which follows since we assumed a and b were commuting elements, and so a necessarily commutes with any power of b, since $b^n = b \cdots b$. Therefore, by induction, we may conclude that the relation holds. ■

Exercise 1.1.25. Prove that if $x^2 = 1$ for all $x \in G$ then G is abelian.

Proof. Let G be a group and suppose $x^2 = 1$ for all $x \in G$. Let $x, y \in G$. Then the product xy is also in G, and by our hypothesis $(xy)^2 = 1$ must hold. However this is equivalent to:

$$xyxy = 1 \implies yxy = x^{-1} \implies xy = y^{-1}x^{-1}$$

Noting that $x = x^{-1}$ and $y = y^{-1}$, we may substitute these values into the above:

$$xy = y^{-1}x^{-1} = yx$$

So $xy = yx$ for all $x, y \in G$. Therefore, we may write G is an abelian group. ■

Exercise 1.1.26. Assume H is a nonempty subset of $(G, \star)$ which is closed under the binary operation on G and is closed under inverses, i.e., for all h and $k \in H$, hk and $h^{-1} \in H$. Prove that H is a group under the operation $\star$ restricted to H (such a subset is called a *subgroup* of G)

Proof. Suppose $H \subset G$, $H \neq \emptyset$, also that $h, k \in H \implies hk, h^{-1} \in H$ (closed under inverses and closed under binary operation of G). We see that the group operation of G restricted to H is necessarily associative. Also, since H is closed under inverses, we know $h, h^{-1} \in H$, and by closure of group operation, $hh^{-1} = 1 \in H$, so H contains the identity element of G. Hence, since H is equipped with an associative binary operation, contains inverses, and contains an identity element, H is necessarily a group by the group axioms as desired (call such a subset a subgroup of G) ∎

Exercise 1.1.27. Prove that if x is an element of the group G, then $\{x^n \mid n \in \mathbb{Z}\}$ is a subgroup of G.

Proof. Let G be a group and $x \in G$. Consider $\langle x \rangle = \{x^n \mid n \in \mathbb{Z}\}$. Note that for $n = 1$, we recover $x^1 = x \in \langle x \rangle$, so clearly $\langle x \rangle \neq \emptyset$. Now suppose $x^n, x^m \in \langle x \rangle$. Then:

$$x^n \cdot x^m = x^{m+n}$$

Letting $m + n = k$, clearly $k \in \mathbb{Z}$, and so $x^k \in \langle x \rangle$. Therefore $\langle x \rangle$ is closed under the binary operation on G. Further, note that if $x^n \in \langle x \rangle$, then $x^{-n} \in \langle x \rangle$, and so $\langle x \rangle$ is closed under inverses. By Exercise 1.1.26, $\langle x \rangle \leq G$ as desired. ∎

Exercise 1.1.28. Let $(A, \star)$ and $(B, \diamond)$ be groups and let $A \times B$ be their direct product (as defined in Example 6). Verify all the group axioms for $A \times B$:
(a) prove that the associative law holds: for all $(a_i, b_i) \in A \times B$, $i = 1, 2, 3$

$$(a_1, b_1)[(a_2, b_2)(a_3, b_3)] = [(a_1, b_1)(a_2, b_2)](a_3, b_3)$$

(b) prove that $(1, 1)$ is the identity of $A \times B$, and
(c) prove that the inverse of (a, b) is (a^{-1}, b^{-1}).

Proof. Let $(A, \star)$ and $(B, \diamond)$ be groups, with $A \times B$ their direct product. So we have $A \times B = \{(a, b) : a \in A, b \in B\}$, with component-wise operations. We can immediately see that the identity in $A \times B$ is the ordered pair consisting of the identity of A and B, $(1_A, 1_B)$. Let $c \in A$, and $d \in B$, then $(c, d) \cdot (1_A, 1_B) = (c \cdot 1_A, d \cdot 1_B) = (c, d)$. Additionally, the group operation is associative, as if we let $(a, b), (a', b'), (a'', b'') \in A \times B$, then we see:

$$[(a, b)(a', b')](a'', b'') = [(a \star a', b \diamond b')](a'', b'') = (a \star a' \star a'', b \diamond b' \diamond b'') =$$

$$(a, b)[(a' \star a'', b' \diamond b'')] = (a, b)[(a', b')(a'', b'')]$$

Finally, note that this direct product group contains inverses, where $(a, b)^{-1} = (a^{-1}, b^{-1})$ as expected. Therefore the group $A \times B$ satisfies all of the group axioms. ∎

Exercise 1.1.29. Prove that $A \times B$ is an abelian group if and only if both A and B are abelian.

Proof. Suppose $A \times B$ is an abelian group. Then:

$$(a, b) \cdot (a', b') = (aa', bb') = (a'a, b'b) = (a', b') \cdot (a, b)$$

And in particular, it must be the case that $aa' = a'a$ for all $a, a' \in A$ and $bb' = b'b$ for all $b, b' \in B$, which is precisely the same as both A and B being abelian groups. ∎

Exercise 1.1.30. Prove that $(a, 1)$ and $(1, b)$ of $A \times B$ commute and deduce that the order of (a, b) is the least common multiple of $|a|$ and $|b|$.

Proof. Take the group $A \times B$ and consider the elements $(a, 1)$ and $(1, b)$. Note:

$$(a, 1) \cdot (1, b) = (a \cdot 1, 1 \cdot b) = (a, b) = (1 \cdot a, b \cdot 1) = (1, b) \cdot (a, 1)$$

So that the above elements commute. Clearly $|(a, 1)| = |a|$ and $|(1, b)| = |b|$. By the results of [[DF-1.1-24]], we may write that:

$$|(a, 1) \cdot (1, b)| = |(a, b)| = |a| \cdot |b|$$

Which is the desired relation. ∎

Exercise 1.1.31. Prove that any finite group G of even order contains an element of order 2.

Proof. Let G be a finite group and suppose G is of even order. Now consider the subset of G defined as $t(G) = \{g \in G \mid g \neq g^{-1}\}$. The identity of G is not in $t(G)$, since $1 = 1^{-1} = 1$ trivially.

Observe that if $x \in t(G)$ then $|x| \neq 2$. Furthermore, since [[DF-1.1-20]] states that $|x| = |x^{-1}|$, it must be the case that $x^{-1} \in t(G)$ as well, for $|x^{-1}| \neq 2$. Therefore, each element of $t(G)$ must also have its inverse in $t(G)$, and since inverses are unique, it must be the case that there are an even number of elements in $t(G)$.

Now consider $G \setminus t(G) = \{g \in G \mid g = g^{-1}\}$. We know $1 \in G \setminus t(G)$. However, it must be the case that $|G \setminus t(G)| + |t(G)| = |G|$. We assumed G was of even order, and we know $|t(G)|$ is even, which forces $|G \setminus t(G)|$ to be even as well. Therefore there must exist at least one element $x \in G \setminus t(G)$ in addition to $1 \in G \setminus t(G)$. Since $x \neq 1$, it must be the case that $x = x^{-1}$, or equivalently, $x^2 = 1$, to which $|x| = 2$. ∎

Exercise 1.1.32. If x is an element of finite order n in G, prove that the elements $1, x, x^2, \ldots, x^{n-1}$ are all distinct. Deduce that $|x| \leq |G|$.

Proof. Let G be a group and let $x \in G$ such that $|x| = n$. If $n = 1$, then x is the identity and so vacuously satisfies the hypothesis, so assume $n > 1$. Now take $i, j \in \{1, \ldots, n-1\}$ such that $i \neq j$. Assume, for contradiction, that $x^i = x^j$. Then:

$$x^i = x^j \iff x^{i-j} = 1$$

To which we must have $i - j = 0$, or equivalently, $i = j$, a contradiction. In particular, this means that $1, x, x^2, \ldots, x^{n-1}$ are distinct.

In particular, we may write that if $|x| > |G|$, then there would be some x^i for $i \in \{1, \ldots, n-1\}$ for which $x^i \notin G$, a contradiction to the closure of G by group axioms. So we may deduce $|x| \leq |G|$. ■

Exercise 1.1.33. Let x be an element of finite order n in G.
(a) Prove that if n is odd then $x^i \neq x^{-i}$ for all $i = 1, 2, \ldots, n-1$.
(b) Prove that if $n = 2k$ and $1 \leq i < n$ then $x^i = x^{-i}$ if and only if $i = k$.

Proof. (a) Let x be an element of finite order n in G. Suppose that n is odd and suppose by way of contradiction that $x^i = x^{-i}$ for all $i = 1, 2, ..., n-1$. Then applying x^i to the right of both sides, we obtain $x^i x^i = 1 \implies x^{2i} = 1$. This implies that the order of x is even, hence a contradiction. Thus we conclude that $x^i \neq x^{-i}$ for all $i = 1, 2, ..., n-1$.

(b) Let $n = 2k$ and $1 \leq i < n$. Suppose $x^i = x^{-i}$. Then applying x^i to the right of both sides, we find $x^i x^i = 1 \implies x^{2i} = 1$. Therefore $n = 2i$, but because $n = 2k$, we can see that $2i = 2k \implies i = k$. Conversely suppose that $i = k$. Then $x^n = x^{2i} = 1 \implies x^i = x^{-i}$ for $1 \leq i < n$. Therefore we conclude that if $n = 2k$ and $1 \leq i < n$ then $x^i = x^{-i} \iff i = k$ as desired. ■

Exercise 1.1.34. If x is an element of infinite order in G, prove that the elements x^n, $n \in \mathbb{Z}$ are all distinct.

Proof. Let $x \in G$ and $|x| = \infty$. Suppose that the elements x^n with $n \in \mathbb{Z}$ are not distinct. Then $x^i = x^j \implies x^i x^{-j} = x^{i-j} = 1$. Then we can see that $|x| = i - j$, contradicting the infinite order of x. Thus a contradiction. Hence all of the elements x^n with $n \in \mathbb{Z}$ are distinct as desired. ■

Exercise 1.1.35. If x is an element of finite order n in G, use the Division Algorithm to show that *any* integral power of x equals one of the elements in the set $\{1, x, x^2, \ldots, x^{n-1}\}$ (so these are all the distinct elements of the cyclic subgroup (cf. Exercise 27 above) of G generated by x.)

Proof. Let $x \in G$ be an element of finite order, $|x| = n < \infty$. We will prove that any integral power of x is equal to one of the elements in the set $\{1, x, x^2, \ldots, x^{n-1}\}$ (the elements of the cyclic subgroup of G generated by x). Let $m = qn + r$ where $0 \leq r < n$. Then $m - r = qn$, so we have $x^{qn} = x^{m-r} \implies (x^n)^q = x^m x^{-r} \implies (1)^q = 1 = x^m x^{-r}$. Hence we have that $x^r = x^m$, and since $0 \leq r < n$, we know that r ranges from $1, 2, \ldots, n-1$. Since $m \in \mathbb{Z}$ was arbitrary, we can see that any integral power of x, say x^m, is equivalent to some element of $\{1, x, x^2, \ldots, x^{n-1}\}$, an element of the cyclic subgroup of G generated by x. ∎

Exercise 1.1.36. Assume $G = \{1, a, b, c\}$ is a group of order 4 with identity 1. Assume also that G has no elements of order 4. Use cancellation laws to show that there is a unique group table for G. Deduce that G is abelian.

Proof. Let $G = \{1, a, b, c\}$ be a group of order 4 with identity 1. Suppose that G has no elements of order 4. Hence by Problem 1.1.32, we know that the elements of G have order ≤ 3. By Problem 1.1.31, we know that since G is finite and has an even order of 4, that G contains an element of order 2. This element of order 2 cannot be the identity 1 by definition. Without loss of generality assume it is $a \in G$. Then $a^2 = 1$. Since G is a group, then $a \in G$ has an inverse $a^{-1} \in G$, which is either b or c. Assume without loss of generality that $a^{-1} = b$. Then $ab = ba = 1$. By Problem 1.1.20, we know that an element and its inverse have the same order, and hence the order of $b \in G$ is also 2. Now the element $c \in G$ must also have an inverse, and since $b = a^{-1}$ and the inverse of an element is unique, then the only option is that $a = c^{-1}$. Thus $ac = ca = 1$. Therefore again $|c| = 2$ because $|c^{-1}| = |a| = 2$ as previously established. Therefore, every non-identity element in G has order 2, and thus by Problem 1.1.25, we can conclude that G is in fact abelian (and consequently the group has a unique symmetric group table by Exercise 1.1.10). ∎

1.2 Dihedral Groups

1.3 Symmetric Groups

1.4 Matrix Groups

1.5 The Quaternion Group

1.6 Homomorphisms and Isomorphisms

Exercise 1.6.1. Let $\varphi : G \to H$ be a homomorphism. (a) Prove that $\varphi(x^n) = \varphi(x)^n$ for all $n \in \mathbb{Z}^+$. (b) Do part (a) for $n = -1$ and deduce that $\varphi(x^n) = \varphi(x)^n$ for all $n \in \mathbb{Z}$.

Proof. (a) Let $\varphi : G \to H$ be a homomorphism. For the base case, $n = 1$, we see that $\varphi(x^1) = \varphi(x)^1$ indeed holds. Now suppose it holds for the nth case, $n \in \mathbb{Z}^+$, so $\varphi(x^n) = \varphi(x)^n$. Now see

$$\varphi(x^{n+1}) = \varphi(x^n x) = \varphi(x^n)\varphi(x) = \varphi(x)^n\varphi(x) = \varphi(x)^{n+1}$$

since $\varphi(xy) = \varphi(x)\varphi(y)$ for all $x, y \in G$, in particular for $x^n, x \in G$. Hence the relation holds for the $n+1$th case and therefore the equality is shown to hold by induction for all $n \in \mathbb{Z}^+$.

(b) Now we will prove that the above holds for all $n \in \mathbb{Z}$. For the base case, we have $n = -1$. We see

$$\varphi(xx^{-1}) = \varphi(1_G) = 1_H = \varphi(x)\varphi(x^{-1})$$

Hence we see $\varphi(x)\varphi(x^{-1}) = 1_H \implies \varphi(x)^{-1} = \varphi(x^{-1})$. Thus it holds for the $n = -1$ case. Given the result proved in the first part of the problem, we can deduce that the equality holds for all $n \in \mathbb{Z}$. ∎

Exercise 1.6.2. If $\varphi : G \to H$ is an isomorphism, prove that $|\varphi(x)| = |x|$ for all $x \in G$. Deduce that any two isomorphic groups have the same number of elements of order n for each $n \in \mathbb{Z}^+$. Is this result true if φ is only assumed to be a homomorphism?

Proof. Let $\varphi : G \to H$ be an isomorphism. Suppose $x \in G$ and that $|x| = k$. Then $x^k = 1$, and thus we see that $\varphi(x^k) = \varphi(1_G) = 1_H$. But by Problem 1.6.1, we know that $\varphi(x^k) = \varphi(x)^k$, and hence we have $\varphi(x)^k = 1_H$. Therefore we see that $|\varphi(x)| \leq k$. If $|\varphi(x)| < k$ was strict, then $\varphi(x)^l = 1_H$ implies $\varphi(x^l) = 1_H$ and so $x^l = 1_G$ since φ is an isomorphism, which is a contradiction for we assumed $|x| = k > l$. Thus $|\varphi(x)| = k$, as desired.

If $x \in G$ such that $|x| = \infty$, suppose that $|\varphi(x)| = k < \infty$. Then $\varphi(x)^k = 1_H$ by definition. However, note that $\varphi(x)^k = \varphi(x^k) = 1_H = \varphi(1_G)$ due to φ being an isomorphism. Then $\varphi(x^k) = \varphi(1_G) \implies x^k = 1_G$. Hence a contradiction to the infinite order of x. Therefore, if the order of x is infinite, the order of $\varphi(x)$ is infinite also.

Since the choice of x was arbitrary, we can conclude that $|x| = |\varphi(x)|$ for all $x \in G$. From this we can also deduce that any two isomorphic groups have the same number of elements of order n for each $n \in \mathbb{Z}^+$. Also this result does not hold if φ is only assumed to be a homomorphism, as then φ may not be an injection. ■

Exercise 1.6.3. If $\varphi : G \to H$ is an isomorphism, prove that G is abelian if and only if H is abelian. If $\varphi : G \to H$ is a homomorphism, what additional conditions on φ (if any) are sufficient to ensure that if G is abelian, then so is H?

Proof. Let $\varphi : G \to H$ be an isomorphism. Suppose that G is abelian. Let $x, y \in G$, so we know $xy = yx$. Then $\varphi(xy) = \varphi(x)\varphi(y)$, but since $\varphi(xy) = \varphi(yx)$, we see that $\varphi(x)\varphi(y) = \varphi(y)\varphi(x)$, and thus H is abelian. Conversely, suppose that H is abelian. Then let $\varphi(x), \varphi(y) \in H$. So we have

$$\varphi(x)\varphi(y) = \varphi(y)\varphi(x) \implies \varphi(xy) = \varphi(yx) \implies xy = yx$$

Hence G is abelian. Therefore G is abelian if and only if H is abelian.

Additionally, if φ is only assumed to be a homomorphism, then surjectivity of φ is enough to ensure that if G is abelian then H is abelian. Injectivity of φ is needed to show that if H is abelian then G is abelian. ■

Exercise 1.6.4. Prove that the multiplicative groups $\mathbb{R}\setminus\{0\}$ and $\mathbb{C}\setminus\{0\}$ are not isomorphic.

Proof. In $(\mathbb{R} - \{0\}, \times)$ we have $|1| = 1$, $|-1| = 2$ with all other $x \in \mathbb{R} - \{0\}$ having infinite order. Let $x \in \mathbb{R} - \{0\}$ such that $x \neq 1, -1$. Suppose $|x| = k < \infty$. Then $x^k = 1$ for some $n \in \mathbb{Z}^+$. Since $x \neq 1, -1$, the only option is that $n = 0$, a contradiction. Therefore every $x \neq 1, -1$ element of $(\mathbb{R} - \{0\}, \times)$ has infinite order. However $i \in \mathbb{C} - \{0\}$ has order 4. Thus there is no isomorphism between these two groups by Problem 1.6.2. ■

Exercise 1.6.5. Prove that the additive groups $\mathbb{R}$ and $\mathbb{Q}$ are not isomorphic.

Proof. No bijection exists between the countably infinite set $\mathbb{Q}$ and the uncountably infinite set $\mathbb{R}$. Thus the two groups $(\mathbb{Q}, +)$ and $(\mathbb{R}, +)$ cannot be isomorphic. ■

Exercise 1.6.6. Prove that the additive groups $\mathbb{Z}$ and $\mathbb{Q}$ are not isomorphic.

Proof. Suppose an isomorphism φ exists such that $\varphi : (\mathbb{Z}, +) \to (\mathbb{Q}, +)$. Note that $\mathbb{Z} = \langle \pm 1 \rangle$. As such, $x = \pm \sum_{k=1}^{n} 1$ for any $x \in \mathbb{Z}$. Thus, $\varphi(x) = \varphi(\pm \sum_{k=1}^{n} 1) = \pm \sum_{k=1}^{n} \varphi(1)$. Since φ is a surjection, for any $q \in \mathbb{Q}$, $q = \varphi(x)$, where $x \in \mathbb{Z}$. Thus we have shown $\mathbb{Q} = \langle \pm\varphi(1) \rangle$. Let $q \in \mathbb{Q}$, then $q = n\varphi(1)$ for some $n \in \mathbb{Z}$ by definition of a generator. Since the set $\mathbb{Q}$ is closed under multiplication, then $\frac{1}{r} \cdot q \in \mathbb{Q}$, where $r \neq 0, 1$. But this implies that $\mathbb{Q} \neq \langle \pm\varphi(1) \rangle$, as $\frac{1}{r} \neq n$ for $n \in \mathbb{Z}$. Thus a contradiction. Hence no isomorphism exists between $(\mathbb{Z}, +)$ and $(\mathbb{Q}, +)$ as desired. ∎

Exercise 1.6.7. Prove that D_8 and Q_8 are not isomorphic.

Proof. We know that D_8 is generated by the elements r and s with orders 4 and 2, respectively. We also know that Q_8 is generated by the elements i and j which both have order 4 since $i^2 = -1$ implies $i^4 = 1$. Similarly for j, we have $j^4 = 1$. In particular, there can exist no isomorphism since the generators have different orders for these groups. ∎

Exercise 1.6.8. Prove that if $n \neq m$, S_n and S_m are not isomorphic.

Proof. Suppose $S_n \cong S_m$ where $m \neq n$. Then by definition of isomorphism, we know that a bijection exists between the groups. Therefore they must have the same order. We know that $|S_m| = m!$ and $|S_n| = n!$. Since $m \neq n$, we know that $m! \neq n!$, hence a contradiction. Therefore if $m \neq n$, then S_m is not isomorphic to S_n as desired. ∎

Exercise 1.6.9.

Exercise 1.6.10.

Exercise 1.6.11.

Exercise 1.6.12.

Exercise 1.6.13. Let G and H be groups and let $\varphi : G \to H$ be a homomorphism. Prove that the image of φ, $\varphi(G)$, is a subgroup of H (cf. Exercise 26 of Section 1). Prove that if φ is injective then $G \cong \varphi(G)$.

Proof. Let $\varphi : G \to H$ be a homomorphism. Clearly $\varphi(G) \subseteq H$. It is trivial to verify that $\varphi(G)$ is closed under the binary operation inherited from H and further that the operation is associative. The identity of H lies in $\varphi(G)$ since $\varphi(1_G) = 1_H$ holds always. What remains is closure under inverses. Suppose $h \in \varphi(G)$. Then there exists $g \in G$ such that $\varphi(g) = h$. Now $h^{-1} = \varphi(g)^{-1} = \varphi(g^{-1})$ so that $h^{-1} \in \varphi(G)$ as well.

Now if φ is injective, then $G/\ker\varphi = G \cong \varphi(G)$ by the first isomorphism theorem. (You'll see this later, don't worry about it). ■

Exercise 1.6.14. Let G and H be groups and let $\varphi : G \to H$ be a homomorphism. Define the kernel of φ to be $\{g \in G \mid \varphi(g) = 1_H\}$ (so the kernel is the set of elements in G which map to the identity of H, i.e., is the fiber over the identity of H). Prove that the kernel of φ is a subgroup (cf. Exercise 26 of Section 1) of G. Prove that φ is injective if and only if the kernel of φ is the identity subgroup of G.

Proof. Let G and H be groups and $\varphi : G \to H$ be a homomorphism. Define $\ker\varphi = \{g \in G : \varphi(g) = 1_H\}$. We can see that $\varphi(1_G) = 1_H$ trivially, so $1_G \in \ker\varphi$. Now let $x, y \in \ker\varphi$. Then $\varphi(x) = 1_H$ and $\varphi(y) = 1_H$, and $\varphi(x)\varphi(y) = \varphi(xy) = 1_H \cdot 1_H = 1_H$, and so $xy \in \ker\varphi$. Finally $\varphi(y^{-1}) = \varphi(y)^{-1} = (1_H)^{-1} = 1_H$, and hence $y^{-1} \in \ker\varphi$. Therefore since $\ker\varphi \subseteq G$, we conclude that $\ker\varphi$ is a subgroup of G by Problem 1.1.26.

Furthermore, suppose that φ is injective. Then let $x \in \ker\varphi$. By definition, $\varphi(x) = 1_H$, but $\varphi(1_G) = 1_H$, so by injectivity we know that $x = 1_G$. Since the choice of x was arbitrary, we conclude that $\ker\varphi = \{1_G\}$. Conversely, suppose that $\ker\varphi = \{1_G\}$. Then let $x, y \in G$ and suppose $\varphi(x) = \varphi(y) \implies \varphi(y)^{-1}\varphi(x) = \varphi(y^{-1})\varphi(x) = 1_H$, so then since φ is a homomorphism, $\varphi(y^{-1}x) = 1_H$, but since this implies that $y^{-1}x \in \ker\varphi$, we know that $y^{-1}x = 1_G \implies x = y$, an injection by definition. Therefore φ is injective $\iff \ker\varphi = \{1_G\}$ as desired. ■

Exercise 1.6.15. Define a map $\pi : \mathbb{R}^2 \to \mathbb{R}$ by $\pi((x, y)) = x$. Prove that π is a homomorphism and find the kernel of π (cf. Exercise 14).

Proof. Define $\pi : \mathbb{R}^2 \to \mathbb{R}$ by $\pi((x, y)) = x$. Let $(x, y), (x', y') \in \mathbb{R}^2$. Hence $\pi((x, y)) = x$ and $\pi((x', y') = x'$. Then define their product as $(xx', yy') \in \mathbb{R}^2$. Now we see that $\pi((x, y)(x', y')) = \pi((xx', yy') = xx' = \pi((x, y))\pi((x', y'))$. Therefore π is a homomorphism by definition. We can see that $\ker\pi = \{(x, y) \in \mathbb{R}^2 : \pi((x, y)) = 0\}$ which is the y-axis in $\mathbb{R}^2$. ■

Exercise 1.6.16. Let A and B be groups and let G be their direct product, $A \times B$. Prove that the maps $\pi_1 : G \to A$ and $\pi_2 : G \to B$ defined by $\pi_1(a, b) = a$ and $\pi_2(a, b) = b$ are homomorphisms and find their kernels (cf. Exercise 14).

Proof. Let A and B be groups with $G = A \times B$. Suppose there exist maps $\pi_1 : G \to A$ and $\pi_2 : G \to B$ defined by $\pi_1((a, b)) = a$ and $\pi_2((a, b)) = b$. Let $(a, b), (a', b') \in G$. Then $\pi_1((aa', bb')) = aa' = \pi_1((a, b))\pi_1((a', b'))$, so π_1 is a homomorphism, and by the same logic, π_2 is also. We note that $\ker\pi_1 = \{(a, b) \in G : \pi_1((a, b)) = 0\}$, which equivalent to all $(0, b) \in G$. Therefore we conclude that $\ker\pi_1 = \{(0, b) \in G\}$ and $\ker\pi_2 = \{(a, 0) \in G\}$. ■

Exercise 1.6.17. Let G be any group. Prove that the map from G to itself defined by $g \mapsto g^{-1}$ is a homomorphism if and only if G is abelian.

Proof. Let G be a group. Suppose $\varphi : G \to G$ defined by $\varphi(x) = x^{-1}$ for any $x \in G$ is a homomorphism. Let $x, y \in G$. Then we know that $\varphi(xy) = \varphi(x)\varphi(y) = x^{-1}y^{-1}$, however by definition this map sends xy to $(xy)^{-1} = y^{-1}x^{-1}$. In particular then, we know that $\varphi(xy) = y^{-1}x^{-1} = x^{-1}y^{-1} \implies xy = yx$. Since the choice of $x, y \in G$ was arbitrary, G is therefore an abelian group by definition. Conversely, suppose that G is an abelian group. Then we know that $xy = yx$ for any $x, y \in G$. Define a map $\varphi : G \to G$ by $\varphi(x) = x^{-1}$. Then we know that $\varphi(xy) = (xy)^{-1} = y^{-1}x^{-1}$ and $\varphi(yx) = (yx)^{-1} = x^{-1}y^{-1}$. In particular, since $xy = yx$, we see that $\varphi(yx) = \varphi(x)\varphi(y) = \varphi(y)\varphi(x) = \varphi(xy)$, and so by definition φ is a homomorphism. ■

Exercise 1.6.18. Let G be any group. Prove that the map from G to itself defined by $g \mapsto g^2$ is a homomorphism if and only if G is abelian.

Proof. Let G be a group. Suppose that the map $\varphi : G \to G$ defined by $\varphi(x) = x^2$ for all $x \in G$ is a homomorphism. Then $\varphi(xy) = \varphi(x)\varphi(y) = x^2y^2$. But since $(xy)^2 = x^2y^2 \implies (xy)(xy) = x^2y^2 \implies x(yx)y = x^2y^2 \implies x(xy)y = x^2y^2$. Hence $xy = yx$ and G is an abelian group. Conversely suppose that G is an abelian group. Then in particular we know that for $x, y \in G$, $xy = yx$. Define a map $\varphi : G \to G$ by $\varphi(x) = x^2$. Then since $(xy)^2 = x^2y^2$, we see $\varphi(xy) = (xy)^2 = x^2y^2 = \varphi(x)\varphi(y)$. Therefore φ is a homomorphism as desired. ■

Exercise 1.6.19.

Exercise 1.6.20. Let G be a group and let $\mathrm{Aut}(G)$ be the set of all isomorphisms from G onto G. Prove that $\mathrm{Aut}(G)$ is a group under function composition (called the automorphism group of G and the elements of $\mathrm{Aut}(G)$ are called automorphisms of G).

Proof. Let $\mathrm{Aut}(G)$ be the set of all isomorphisms from G onto G. We can show that $\mathrm{Aut}(G)$ is a group with the binary operation as function composition, which we know to be associative. Further, the identity element of this group is the trivial isomorphism, defined by $g \mapsto g$. Also, by definition of a bijection, every isomorphism has an inverse and thus all elements of $\mathrm{Aut}(G)$ have an inverse. Therefore the $\mathrm{Aut}(G)$ is a group as desired. ■

Exercise 1.6.21. Prove that for each fixed nonzero $k \in \mathbb{Q}$ the map from $\mathbb{Q}$ to itself defined by $q \mapsto kq$ is an automorphism of $\mathbb{Q}$ (cf. Exercise 20).

Proof. Let $k \in \mathbb{Q}$ such that k is fixed and nonzero. Consider the map $\varphi : \mathbb{Q} \to \mathbb{Q}$ defined by $\varphi(q) = kq$ for all $q \in \mathbb{Q}$. Let $q, p \in \mathbb{Q}$. Then $\varphi(q+p) = k(q+p) = kq+kp =$

$\varphi(q)+\varphi(p)$ and so φ is a homomorphism. Now suppose $\varphi(q) = \varphi(p) \implies kq = kp$. Since $k \neq 0$, we see that this implies $p = q$, and hence φ is injective. Again, since $k \neq 0$, we also know that $\frac{q}{k} \in \mathbb{Q}$. Then $\varphi(\frac{q}{k}) = k \cdot \frac{q}{k} = q \in \mathbb{Q}$, and hence φ is surjective. Therefore φ is a bijective homomorphism from $\mathbb{Q}$ to itself, and by definition φ is an automorphism of $\mathbb{Q}$ as desired. ■

Exercise 1.6.22. Let A be an abelian group and fix some $k \in \mathbb{Z}$. Prove that the map $a \mapsto a^k$ is a homomorphism from A to itself. If $k = -1$ prove that this homomorphism is an isomorphism (i.e., is an automorphism of A).

Proof. Let A be an abelian group and $k \in \mathbb{Z}$ be fixed. Suppose there exists a map $\varphi : A \to A$ defined by $\varphi(a) = a^k$. Let $a, b \in A$. Then because A is abelian, we see that $\varphi(ab) = (ab)^k = a^k b^k = \varphi(a)\varphi(b)$. Therefore φ is a homomorphism. Additionally, suppose $k = -1$. Then since A is abelian, φ is a homomorphism by Problem 1.6.17. Then since $\varphi(a) = \varphi(b) \implies a^{-1} = b^{-1} \implies a = b$ by uniqueness of inverses, we can see that φ is injective. Further, $b \in A \implies b = a^{-1}$ for some $a \in A$. Then since A is a group, $b \in A$. Thus φ is surjective, and hence an isomorphism. Therefore in the case where $k = -1$, we conclude that φ is an automorphism of A as desired. ■

Exercise 1.6.23. Let G be a finite group which possesses an automorphism σ (cf. Exercise 20) such that $\sigma(g) = g$ if and only if $g = 1$. If σ^2 is the identity map from G to G, prove that G is abelian (such an automorphism σ is called fixed point free of order 2). [Show that every element of G can be written in the form $x^{-1}\sigma(x)$ and apply σ to such an expression.]

Proof. Let G be a finite group and let $\sigma \in \text{Aut}(G)$ defined by $\sigma(g) = g \iff g = 1$ (a permutation which fixes only the identity element of G). Let a subset of G be $H = \{x^{-1}\sigma(x) : x \in G\} \subseteq G$. Define $\varphi : G \to H$ by $\varphi(x) = x^{-1}\sigma(x)$, so $1_G \in H$ because $\varphi(1_G) = 1_G^{-1}\sigma(1_G) = 1_G$. Now let $x, y \in G$ such that $x, y \neq 1$ and suppose that $\varphi(x) = \varphi(y)$, so we now have that $x^{-1}\sigma(x) = y^{-1}\sigma(y) \implies yx^{-1} = \sigma(y)\sigma(x)^{-1} \implies yx^{-1} = \sigma(y)\sigma(x^{-1}) = \sigma(yx^{-1})$, and since $\sigma(g) = g \iff g = 1$, we have $yx^{-1} = 1 \implies y = x$, and hence φ is an injection by definition, so $|G| \leq |H|$, but since $H \subseteq G \implies |G| \geq |H|$, we have that $|G| = |H| \implies G = H$. Hence every element $x \in G$ can be rewritten in the form $x = x^{-1}\sigma(x)$. Now let $z \in G$ so there is an $x \in G$ such that $z = x^{-1}\sigma(x)$. Now $\sigma(z) = \sigma(x)^{-1}x = (x^{-1}\sigma(x))^{-1} = z^{-1}$, so $\sigma(z) = z^{-1}$. Now let $w \in G$ so $\sigma(zw) = w^{-1}z^{-1}$ but also $\sigma(zw) = \sigma(z)\sigma(w) = z^{-1}w^{-1}$ because $\sigma \in \text{Aut}(G)$. Thus $w^{-1}z^{-1} = z^{-1}w^{-1} \implies wz = zw$ and this holds for all $z, w \in G$, hence G is abelian as desired. ■

Exercise 1.6.24. Let G be a finite group and let x and y be distinct elements of order 2 in G that generate G. Prove that $G \cong D_{2n}$, where $n = |xy|$. [See Exercise 6 in Section 2.]

Proof. Let G be a finite group and $x, y \in G$ distinct elements such that $|x| = |y| = 2$ that generate G. Let $t = xy$. Then by Problem 1.2.6, we know that $tx = xt^{-1}$. Suppose $n = |xy|$. Then we can see that x and t satisfy the same relations as s and r in D_{2n}, as $G = \langle x, t \mid x^2 = t^n = 1, tx = xt^{-1}\rangle$. Hence since x and $t = xy$ are generators for the group G and satisfy the same relations as the generators r and s in D_{2n}, we conclude that $G \cong D_{2n}$ as desired. ∎

Exercise 1.6.25. Let $n \in \mathbb{Z}^+$, let r and s be the usual generators of D_{2n} and let $\theta = 2\pi/n$.
(a) Prove that the matrix $\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$ is the matrix of the linear transformation which rotates the x, y plane about the origin in a counterclockwise direction by θ radians.
(b) Prove that the map $\varphi : D_{2n} \to \mathrm{GL}_2(\mathbb{R})$ defined by

$$\varphi(r) = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \text{ and } \varphi(s) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

extends to a homomorphism of D_{2n} into $\mathrm{GL}_2(\mathbb{R})$.
(c) Prove that the homomorphism φ in part (b) is injective.

Proof. (a) We have the matrix $\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$ and we would like to show that it is the matrix of the linear transformation which rotates the xy-plane about the origin CCW by θ radians. Take the standard ordered basis for $\mathbb{R}^2$, $\vec{e}_1 = \binom{1}{0}$ and $\vec{e}_2 = \binom{0}{1}$. Then performing matrix multiplication, we find that the basis vectors transform into the following:

$$\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} \cos\theta \\ \sin\theta \end{pmatrix}$$

$$\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} -\sin\theta \\ \cos\theta \end{pmatrix}$$

This transformation is clearly linear and we can see that the transformed basis vectors do indeed rotate the plane CCW by θ radians.

(b) Suppose that there exists a map $\varphi : D_{2n} \to GL_2(\mathbb{R})$ defined on generators by:

$$\varphi(r) = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}, \ \varphi(s) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

To prove that this map extends to a homomorphism, we need to show that the generators satisfy the same relations. First, we know that group presentation for $D_{2n} = \langle s, r \mid s^2 = e^n = 1, rs = sr^{-1}\rangle$. Now we see that:

$$\varphi(s)^2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

and that:

$$\varphi(r)^n = \begin{pmatrix}\cos\theta & -\sin\theta\\ \sin\theta & \cos\theta\end{pmatrix}\begin{pmatrix}\cos\theta & -\sin\theta\\ \sin\theta & \cos\theta\end{pmatrix}\cdots =$$

$$\begin{pmatrix}\cos^2\theta-\sin^2\theta & 2\cos\theta\sin\theta\\ 2\cos\theta\sin\theta & \cos^2\theta-\sin^2\theta\end{pmatrix}\cdots = \begin{pmatrix}\cos n\theta & \sin n\theta\\ \sin n\theta & \cos n\theta\end{pmatrix}$$

Using trigonometric identities. Then since we know that $\theta = 2\pi/n$, we can see that:

$$\begin{pmatrix}\cos n\theta & \sin n\theta\\ \sin n\theta & \cos n\theta\end{pmatrix} = \begin{pmatrix}\cos 2\pi & \sin 2\pi\\ \sin 2\pi & \cos 2\pi\end{pmatrix} = \begin{pmatrix}\cos n\theta & \sin n\theta\\ \sin n\theta & \cos n\theta\end{pmatrix} = \begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$$

So this relation holds as well. Now for the final relation, we find:

$$\varphi(r)\varphi(s) = \begin{pmatrix}\cos\theta & -\sin\theta\\ \sin\theta & \cos\theta\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix} = \begin{pmatrix}-\sin\theta & \cos\theta\\ \cos\theta & \sin\theta\end{pmatrix}$$

And then we compute:

$$\varphi(s)\varphi(r)^{-1} = \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}\cos\theta & \sin\theta\\ -\sin\theta & \cos\theta\end{pmatrix} = \begin{pmatrix}-\sin\theta & \cos\theta\\ \cos\theta & \sin\theta\end{pmatrix}$$

Therefore the generators $\varphi(s)$ and $\varphi(r)$ in $GL_2(\mathbb{R})$ satisfy the same relations as the generators r and s in D_{2n}, and hence the map φ is indeed a homomorphism between the two groups.

(c) Now we would like to prove that the homomorphism φ is injective. Suppose $\varphi(a) = \varphi(b)$, with $a, b \in D_{2n}$. Then $a = s^k r^i$ and $b = s^h r^j$ for $k, h \in \{0, 1\}$ and $0 \le i, j \le n-1$. Hence since φ is a homomorphism, we see that:

$$\varphi(a) = \varphi(s^k r^i) = \varphi(s)^k\varphi(r)^i = \varphi(s)^h\varphi(r)^j = \varphi(s^h r^j) = \varphi(b)$$

$$\implies \varphi(s)^k\varphi(r)^i = \varphi(s)^h\varphi(r)^j$$

$$\implies \varphi(s)^{h-k} = \varphi(r)^{i-j}$$

But from the relations in the presentation for $GL_2(\mathbb{R})$, we know that $\varphi(s) \neq \varphi(r)^i$ for any i, so $h - k = 0 \implies h = k$. But then we see that:

$$\varphi(r)^{i-j} = 1 \implies \varphi(r)^i = \varphi(r)^j \implies i = j$$

Thus we have shown that $h = k$ and $i = j$ and so by the homomorphism we conclude that $a = s^k r^i = s^h r^j = b$. Hence $\varphi(a) = \varphi(b) \implies a = b$, so by definition φ is an injection as desired. ■

Exercise 1.6.26. Let i and j be the generators of Q_8 described in Section 5. Prove that the map φ from Q_8 to $\mathrm{GL}_2(\mathbb{C})$ defined on generators by

$$\varphi(i) = \begin{pmatrix} \sqrt{-1} & 0 \\ 0 & \sqrt{-1} \end{pmatrix} \quad \text{and} \quad \varphi(j) = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

extends to a homomorphism. Prove that φ is injective.

Proof. Let $Q_8 = \langle i, j \rangle$. Suppose that there exists a map $\varphi : Q_8 \to GL_2(\mathbb{C})$ defined on generators by:

$$\varphi(i) = \begin{pmatrix} \sqrt{-1} & 0 \\ 0 & \sqrt{-1} \end{pmatrix}, \quad \varphi(j) = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

We know that if $\varphi(i)$ and $\varphi(j)$ satisfy the same relations as the generators $i, j \in Q_8$, then φ extends to a homomorphism. We know that a presentation $Q_8 = \langle i, j \mid i^4 = 1, i^2 = j^2, ij = ji^{-1} \rangle$. First we see that:

$$\varphi(i)^4 = (\begin{pmatrix} \sqrt{-1} & 0 \\ 0 & \sqrt{-1} \end{pmatrix}\begin{pmatrix} \sqrt{-1} & 0 \\ 0 & \sqrt{-1} \end{pmatrix})^2 = (\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix})^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$\varphi(j)^2 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = (\begin{pmatrix} \sqrt{-1} & 0 \\ 0 & \sqrt{-1} \end{pmatrix})^2 = \varphi(i)^2$$

And finally we see that:

$$\varphi(i)\varphi(j) = \begin{pmatrix} \sqrt{-1} & 0 \\ 0 & \sqrt{-1} \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & -\sqrt{-1} \\ \sqrt{-1} & 0 \end{pmatrix}$$

$$\varphi(j)\varphi(i)^{-1} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} \sqrt{-1} & 0 \\ 0 & \sqrt{-1} \end{pmatrix} = \begin{pmatrix} 0 & -\sqrt{-1} \\ \sqrt{-1} & 0 \end{pmatrix}$$

And hence we can see that $\varphi(i)\varphi(j) = \varphi(j)\varphi(i)^{-1}$. Therefore we have shown that the generators $\varphi(i), \varphi(j)$ for $GL_2(\mathbb{C})$ satisfy the same relations as the generators i, j for G. Hence φ is indeed a homomorphism. Additionally, we see that $\ker \varphi = \{1\}$ because $i, i^{-1} = -i, j, j^{-1} = -j, ij, (ij)^{-1} = ji \notin \ker \varphi$, and these are all of the elements in Q_8. Hence φ is injective. ∎

1.7 Group Actions

Exercise 1.7.1.

Exercise 1.7.2.

Exercise 1.7.3.

Exercise 1.7.4.

Exercise 1.7.5.

Exercise 1.7.6.

Exercise 1.7.7.

Exercise 1.7.8.

Exercise 1.7.9.

Exercise 1.7.10.

Exercise 1.7.11.

Exercise 1.7.12.

Exercise 1.7.13.

Exercise 1.7.14.

Exercise 1.7.15.

Exercise 1.7.16.

Exercise 1.7.17.

Exercise 1.7.18.

Exercise 1.7.19.

Exercise 1.7.20.

Exercise 1.7.21.

Exercise 1.7.22.

Exercise 1.7.23.

※ Subgroups

2.1 Definition and Examples

Exercise 2.1.1. In each case, prove that the specified subset is a subgroup of the given group:

Proof. (a) Consider $A = \{\lambda + \lambda i \mid \lambda \in \mathbb{R}\}$. Note that $0 \in \mathbb{R}$, and so $0 + 0i \in A$, to which $A \neq \emptyset$. Suppose $a, b \in A$, where $a = \lambda + \lambda i$ and $b = \mu + \mu i$. We have:

$$(\lambda + \lambda i) + (-\mu - \mu i) = \lambda + \lambda i - \mu - \mu i = (\lambda - \mu) + (\lambda - \mu)i \in A$$

Since $\lambda - \mu \in \mathbb{R}$. Therefore $ab^{-1} \in A$, and so by the subgroup criterion, $A \leq \mathbb{C}$ under addition.

(b) XX

(c) XX

(d) Fix $n \in \mathbb{Z}^+$. Take $Q' = \{a/b \in \mathbb{Q} \mid \gcd(b, n) = 1\}$. Clearly $Q' \subset \mathbb{Q}$. Note that $0/1 = 0 \in \mathbb{Q}$, and we have $1 \mid n$ trivially, and so $0 \in Q'$, to which $Q' \neq \emptyset$. Now suppose a/b and a'/b' are elements of Q'. Then we have:

$$\frac{a}{b} - \frac{a'}{b'} = \frac{ab' - a'b}{bb'} \in Q'$$

Which follows from the multiplicative property of the greatest common divisor function, equivalently, $\gcd(b, n) = 1$ and $\gcd(b', n) = 1$ implies $\gcd(bb', n) = 1$; hence $Q' \leq \mathbb{Q}$ by the subgroup criterion.

(e) Consider $R' = \{a \in \mathbb{R} \mid a \neq 0,\ a^2 \in \mathbb{Q}\}$ as a subset of the multiplicative group $\mathbb{R} \setminus \{0\}$. Note that $1 \in \mathbb{R}$ satisfies $1^2 = 1 \in \mathbb{Q}$, and so $1 \in R'$, to which $R' \neq \emptyset$. Now suppose that $x, y \in R'$. Then:

$$(xy^{-1})^2 = (x \cdot \frac{1}{y})^2 = (\frac{x}{y})^2 = \frac{x^2}{y^2}$$

And since x and y are contained in R', then we know $x^2, y^2 \in \mathbb{Q}$, to which their quotient necessarily is also in $\mathbb{Q}$. Equivalently, $xy^{-1} \in R'$, and so $R' \leq \mathbb{R} \setminus \{0\}$ by the subgroup criterion. ∎

Exercise 2.1.2. In each prove that the specified subset is not a subgroup of the given group.

a.) the set of 2-cycles of S_n for $n \geq 3$.

b.) the set of reflections in D_{2n} for $n \geq 3$.

c.) for n a composite integer such that $n > 1$ and G a group containing an element of order n, the set $\{x \in G \mid |x| = n\} \cup \{1\}$.

d.) the set of positive and negative odd integers in $\mathbb{Z}$ together with 0.

e.) the set of real numbers whose square is a rational number under addition.

Proof. (a) Take the case where $n = 3$. Note that in S_3, there are three 2-cycles. Consider their subset, $\{(1\ 2), (1\ 3), (2\ 3)\}$. Note that:

$$(1\ 2)(1\ 3) = (1\ 3\ 2)$$

And so this subset is not closed under the group operation, and hence not a subgroup of S_n for any $n \geq 3$, for these permutations are guaranteed to exist for all such S_n.

(b) Let $n \geq 3$, and consider D_{2n}. Let S denote the subset of D_{2n} consisting of all reflections. Note we have s and sr^{n+1} as elements in this subset. However:

$$(s)(sr^{n+1}) = ssr^{n+1} = r^{n+1} = r^n r = r \notin S$$

And so S is not closed under the group operation and cannot be a subgroup of D_{2n}.

(c) We will prove that the outlined subset cannot be a subgroup by example, which will show that it need not hold generally. Take $G = \mathbb{C} \setminus \{0\}$, and pick $n = 4$, which is a composite number greater than 1. Note that $i \in \mathbb{C} \setminus \{0\}$ satisfies $|i| = 4$. Now take:

$$\{z \in \mathbb{C} \setminus \{0\} \mid |z| = 4\} \cup \{1\} = \{1, i, -i\}$$

To see that the above subset is not a subgroup of $\mathbb{C} \setminus \{0\}$, take:

$$i \cdot i = i^2 = (\sqrt{-1})^2 = -1$$

And note that -1 has order 2 in $\mathbb{C} \setminus \{0\}$, and so the above subset cannot be a subgroup of the given group for it is not closed under the group operation.

(d) Take 3 and 5, which are both odd integers and therefore in the provided subset. Note we have $5 - 3 = 2$, which is an even integer, and so clearly this subset is not a subgroup.

(e) Consider $R' = \{x \in \mathbb{R} \mid x^2 \in \mathbb{Q}\} \subset \mathbb{R}$. Note that $\sqrt{2}$ satisfies $\sqrt{2}^2 = 2 \in \mathbb{Q}$, to which $\sqrt{2} \in R'$. Also $2 \in \mathbb{R}$ satisfies $2^2 = 4 \in \mathbb{Q}$, and so again $2 \in R'$. However, if we take these elements sum, we find:

$$(2 + \sqrt{2})^2 = 6 + 4\sqrt{2} = 6 + \sqrt{32} \notin \mathbb{Q}$$

To which this subset R' is not closed under addition; hence not a subgroup of $\mathbb{R}$. ∎

Exercise 2.1.3. Show that the following subsets of the dihedral group D_8 are actually subgroups:
1.) $\{1, r^2, s, sr^2\}$
2.) $\{1, r^2, sr, sr^3\}$

Proof. (a) This set is clearly non-empty, and so it suffices to show that the subset is closed under inverses and the group operation.

$$r^2 \cdot s = r^2 s = sr^{-2} = sr^2 \in A$$

$$r^2 \cdot sr^2 = r^2 sr^2 = sr^{-2} r^2 = s \in A$$

$$s \cdot sr^2 = ssr^2 = r^2 \in A$$

And clearly the product of the identity with any other element of the subset is also in the subset. Therefore this subset is closed under the group operation. Also note that $(r^2)^{-1} = r^2$, $s^{-1} = s$, and $(sr^2)^{-1} = r^{-2}s^{-1} = r^{-2}s = sr^2$, so that this subset is closed under inverses. Therefore $A \leq D_8$.

(b) This subset is again non-empty, and we can take the products of each element:

$$r^2 \cdot sr = r^2 sr = sr^{-2} r = sr \in A$$

$$r^2 \cdot sr^3 = r^2 sr^3 = sr^{-2} r^3 = sr \in A$$

$$sr \cdot sr^3 = srsr^3 = r^{-1} ssr^3 = r^{-1} r^3 = r^2 \in A$$

And again the identity composed with any element stays within the subset A, so that A is closed under the group operation. Further, note $(r^2)^{-1} = r^{-2} = r^2$, $(sr)^{-1} = r^{-1}s^{-1} = r^{-1}s = sr$, and $(sr^3)^{-1} = r^{-3}s^{-1} = r^{-3}s = sr^3$, and so A is also closed under inverses. Therefore $A \leq D_8$. ■

Exercise 2.1.4. Give an explicit example of a group G and an infinite subset H of G that is closed under the group operation but is not a subgroup of G.

Proof. Consider the multiplicative group $\mathbb{Q} \setminus \{0\}$. Note that $\mathbb{Z} \setminus \{0\} \subset \mathbb{Q} \setminus \{0\}$. Furthermore, if we take $a, b \in \mathbb{Z} \setminus \{0\}$, then it must the case that $ab \in \mathbb{Z} \setminus \{0\}$, and so this infinite subset is closed under the group operation of multiplication. However, this subset is clearly not closed under inverses, and so cannot be a subgroup of $\mathbb{Q} \setminus \{0\}$. An easy example of this is taking $2 \in \mathbb{Z} \setminus \{0\}$ and noting that $1/2 \notin \mathbb{Z} \setminus \{0\}$. ■

Exercise 2.1.5. Prove that G cannot have a subgroup H with $|H| = n - 1$, where $n = |G| > 2$.

Proof. Let G be a group with $|G| = n > 2$. Assume, for contradiction, that $H \leq G$ such that $|H| = n - 1$. Then there must exist some non-identity element $x \in G$ for which $x \notin H$. If $|x| \neq 2$, then it must be the case that $x \neq x^{-1}$, and so $x^{-1} \in H$, which would mean $x \in H$ since H is closed under inverses, a contradiction; hence $|x| = 2$ must hold. Note then that the subset $\langle x \rangle = \{1, x\}$ is a subgroup of G.

Now, observe that $H \cup \langle x \rangle = G$, and since G is a subgroup of itself, in particular $H \cup \langle x \rangle$ is a subgroup of G. However, by [[DF-2.1-8]], the set $H \cup \langle x \rangle$ is a subgroup of G if and only if either $\langle x \rangle \subseteq H$ or $H \subseteq \langle x \rangle$ holds true. Since we assumed $x \notin H$, clearly $\langle x \rangle \nsubseteq H$. Therefore it must be the case that $H \subseteq \langle x \rangle$. However, the only two elements of $\langle x \rangle$ are the identity and x itself, and since H must contain the identity of G, either $H = \{1\}$ or $H = \langle x \rangle$.

But if $H = \{1\}$, then $|H| = 1$, which is a contradiction to our assumption that $n > 2$, as $|H| = n - 1 = 1$ implies $n = 2$. Therefore we have $H = \langle x \rangle$, which is also a contradiction for we assumed $x \notin H$. Given this, we may conclude that a group G with $|G| = n > 2$ cannot have a subgroup H of order $|H| = n - 1$. ∎

Exercise 2.1.6. Let G be an abelian group. Prove that $\{g \in G \mid |g| < \infty\}$ is a subgroup of G (called the torsion subgroup of G). Give an explicit example where this set is not a group when G is non-abelian.

Proof. Let G be an abelian group. Consider $T(G) = \{g \in G \mid |g| < \infty\}$. Note that the identity of G has order 1, and therefore $1 \in T(G)$, so that $T(G) \neq \emptyset$. Now suppose $x, y \in T(G)$. We may write $|x| = n$ and $|y| = m$, where $m, n \in \mathbb{Z}^+$. Note that since an element and its inverse have the same order, we have $|y^{-1}| = m$ as well. Observe:

$$(xy^{-1})^{mn} = x^{mn}(y^{-1})^{mn} = (x^n)^m((y^{-1})^m)^n = 1 \cdot 1 = 1$$

To which we may write that the element xy^{-1} must have finite order, as it cannot possibly have infinite order; hence $xy^{-1} \in T(G)$, and so by the subgroup criterion, the torsion subgroup $T(G)$ is a subgroup of G.

Consider the infinite dihedral group D_∞, which is a non-abelian group. Note that sr and sr^2 are elements of D_∞ that both have order 2. However:

$$(sr)(sr^2) = srsr^2 = srr^{-2}s = sr^{-1}s = rss = r$$

And clearly $|r| = \infty$, to which we may write that the subset $T(D_\infty)$ as defined above is indeed not a subgroup. ∎

Exercise 2.1.7. Fix some $n \in \mathbb{Z}$ with $n > 1$. Find the torsion subgroup of $\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. Show that the set of elements of infinite order together with the identity is not a subgroup of this direct product.

Proof. Choose $n \in \mathbb{Z}$ with $n > 1$. Then consider $T(\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z})$. Note that every element of $\mathbb{Z}$ is of infinite order except the identity. Also, each element of $\mathbb{Z}/n\mathbb{Z}$ is of finite order. Therefore the torsion subgroup of this direct product is:

$$T(\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}) = \{(0, \overline{a}) \mid \overline{a} \in \mathbb{Z}/n\mathbb{Z}\}$$

To show that the set of elements of infinite order together with the identity is not a subgroup, consider the elements $(1, \overline{0})$ and $(-1, \overline{0})$, which are both of infinite order. Taking their product:

$$(1, \overline{0}) \cdot (-1, \overline{0}) = (1 - 1, \overline{0}) = (0, \overline{0})$$

Which is, in fact, an element of finite order. Therefore the set in question cannot be closed under the group operation. ∎

Exercise 2.1.8. Let H and K be subgroups of G. Prove that $H \cup K$ is a subgroup if and only if either $H \subseteq K$ or $K \subseteq H$.

Proof. Let G be a group, with $H, K \leq G$. For the forward direction, suppose $H \cup K \leq G$. Let $x, y \in H \cup K$. Without loss of generality, let $x \in H$ and $y \in K$. We know that the product xy must also be an element of $H \cup K$, and so either $xy \in H$ or $xy \in K$ or $xy \in H \cap K$.

In the case where $xy \in H$, then clearly we may apply the inverse of x to this element to obtain $x^{-1}(xy) = y \in H$, to which $K \subseteq H$. On the other hand, if $xy \in K$, then we may apply the inverse of y to obtain $(xy)y^{-1} = x \in K$, to which $H \subseteq K$. If $xy \in H \cap K$, then $xy \in H$ and $xy \in K$, to which $x^{-1}(xy) = y \in H$ and $(xy)y^{-1} = x \in K$, so necessarily $K = H$; hence, in any case, $H \subseteq K$ or $K \subseteq H$ must hold.

Conversely, suppose that $H \subseteq K$ or $K \subseteq H$ holds. Without loss of generality, let $K \subseteq H$. Then $H \cup K = H$ trivially holds, and since we assumed H to be a subgroup of G, we may write that $H \cup K$ is a subgroup of G ∎

Exercise 2.1.9. Let $G = GL(n, F)$, where F is any field. Define:

$$SL(n, F) = \{A \in GL(n, F) \mid \det(A) = 1\}$$

Prove that $SL(n, F) \leq GL(n, F)$.

Proof. Consider the subset $SL(n, F)$ of the $GL(n, F)$ defined in the problem. Note that the $n \times n$ identity matrix, $\mathcal{I}_n$, satisfies $\det(\mathcal{I}_n) = 1$ trivially, to which $\mathcal{I}_n \in SL(n, F)$, and so $SL(n, F) \neq \emptyset$.

Now suppose $A, B \in SL(n, F)$. We have $\det(A) = \det(B) = 1$. First recall that the determinant of the inverse of a matrix is equal to the reciprocal of the determinant of the matrix. With this, we can see:

$$\det(AB^{-1}) = \det(A)\det(B^{-1}) = \det(A) \cdot \frac{1}{\det(B)} = 1 \cdot \frac{1}{1} = 1$$

By the multiplicative property of the determinant function. Given the above, we may write that the matrix product $AB^{-1} \in SL(n, F)$. By the subgroup criterion, this is sufficient for $SL(n, F) \leq GL(n, F)$. ∎

Exercise 2.1.10.
a.) Prove that if H and K are subgroups of G then so is their intersection $H \cap K$.
b.) Prove that the intersection of an arbitrary nonempty collection of subgroups of G is again a subgroup of G.

Proof. (a) Let G be a group and suppose $H, K \leq G$. Consider $H \cap K \subseteq G$. Note that $1 \in H$ and $1 \in K$, and so $1 \in H \cap K$ which implies $H \cap K \neq \emptyset$. Now suppose $x, y \in H \cap K$. Then $x, y \in H$ and $x, y \in K$, and since both H and K are subgroups, we know $xy^{-1} \in H$ and $xy^{-1} \in K$ must hold; equivalently, we have $xy^{-1} \in H \cap K$. Thus, by the subgroup criterion, $H \cap K \leq G$.

(b) Let G be a group and suppose that $\{H_i \mid i \in \mathcal{I}\}$ is a nonempty collection of subgroups of G, for some index set $\mathcal{I}$. Now consider their intersection, $\bigcap_{i \in \mathcal{I}} H_i \subseteq G$. Note that since $H_i \leq G$ for all $i \in \mathcal{I}$, and the collection is nonempty, we have $1 \in H_i$ for all $i \in \mathcal{I}$, to which $1 \in \bigcap_{i \in \mathcal{I}} H_i$ and so $\bigcap_{i \in \mathcal{I}} H_i \neq \emptyset$. Now suppose $x, y \in \bigcap_{i \in \mathcal{I}} H_i$. Then $x, y \in H_i$ for all $i \in \mathcal{I}$, and since each H_i is a subgroup of G, we must have closure under the group operation and inverses, to which $xy^{-1} \in H_i$ for all $i \in \mathcal{I}$. This is equivalent to $xy^{-1} \in \bigcap_{i \in \mathcal{I}} H_i$ and so by the subgroup criterion, we have shown $\bigcap_{i \in \mathcal{I}} H_i \leq G$. ■

Exercise 2.1.11. Let A and B be groups. Prove that the following sets are subgroups of the direct product $A \times B$.
a.) $\{(a, 1) \mid a \in A\}$
b.) $\{(1, b) \mid b \in B\}$
c.) $\{(a, a) \mid a \in A\}$

Proof. (a) Since A was assumed to be a group, $1 \in A$, and so $(1, 1) \in \{(a, 1) \mid a \in A\}$, to which the subset is non-empty. Take $(x, 1)$ and $(y, 1)$ in this group, where $x, y \in A$. Note that $y^{-1} \in A$ by closure under inverses, and so $(y^{-1}, 1) \in \{(a, 1) \mid a \in A\}$. Therefore:

$$(x, 1) \cdot (y^{-1}, 1) = (xy^{-1}, 1) \in \{(a, 1) \mid a \in A\}$$

And therefore by the subgroup criterion, $\{(a, 1) \mid a \in A\} \leq A \times B$.

(b) Refer to the results of part (a) and note that by symmetry we may easily find that $\{(1, b) \mid b \in B\} \leq A \times B$.

(c) Take $\{(a, a) \mid a \in A\}$ as a subset of $A \times A$. The element $(1, 1)$ is in this subset, and so it is non-empty. Furthermore, the inclusion of (y, y) implies (y^{-1}, y^{-1}) is an element of this subset, to which:

$$(x, x) \cdot (y^{-1}, y^{-1}) = (xy^{-1}, xy^{-1})$$

Which is trivially an element of the desired subset; appeal to the subgroup criterion to note that $\{(a, a) \mid a \in A\} \leq A \times A$. ■

Exercise 2.1.12. Let A be an abelian group and fix some $n \in \mathbb{Z}$. Prove that the following sets are subgroups:
a.) $\{a^n \mid a \in A\}$
b.) $\{a \in A \mid a^n = 1\}$

Proof. (a) Fix $n \in \mathbb{Z}$. Let A be an abelian group. Consider $A' = \{a^n \mid a \in A\} \subseteq A$. Note that the identity of A satisfies $1^n = 1$ for any n; hence $1 \in A'$. Now suppose $x, y \in A'$. Then we may write:

$$x^n(y^{-1})^n = (xy^{-1})^n \implies xy^{-1} \in A'$$

Which follows since $xy^{-1} \in A$ and A is abelian, to which we may pull out the above powers of x and y^{-1}. Thus, by the subgroup criterion, $A' \leq A$.

(b) Now consider $A'' = \{a \in A \mid a^n = 1\} \subseteq A$. Clearly $1 \in A$ satisfies containment in A'', for $1^n = 1$ for any n. Suppose $x, y \in A''$. Then we know that $x^n = y^n = 1$. Furthermore, we may also obtain $y^{-n} = 1$. Note:

$$x^n = 1 \implies x^n y^{-n} = 1 \iff (xy^{-1})^n = 1$$

And the above is the criterion for $xy{-}1 \in A''$; hence we may appeal to the subgroup criterion to write that $A'' \leq A$. ■

Exercise 2.1.13. Let H be a subgroup of the additive group of rational numbers with the property that $1/x \in H$ for every nonzero element x of H. Prove that $H = 0$ or $\mathbb{Q}$.

Proof. Let $H \leq \mathbb{Q}$ such that if $x \neq 0$ and $x \in H$, then $1/x \in H$. We know that $H \subseteq \mathbb{Q}$, as it is a subgroup. Let $a/b \in \mathbb{Q}$ be arbitrary. Suppose there exists some nonzero $x \in H$. Then, by construction, we have $1/x \in H$. Since H is closed under addition, it must be the case that:

$$\sum_{i=1}^{x} \frac{1}{x} = \frac{1}{x} + \cdots + \frac{1}{x} = \frac{x}{x} = 1$$

So that we necessarily have $1 \in H$. Since $b \in \mathbb{Z}$, we can write $\sum_{i=1}^{b} 1 = b$, again since H is closed under addition. The construction of H implies $1/b \in H$. Now we may take:

$$\sum_{i=1}^{a} \frac{1}{b} = \frac{1}{b} + \cdots + \frac{1}{b} = \frac{a}{b}$$

And so we have $a/b \in H$. But $a/b \in \mathbb{Q}$ was arbitrary, and so the above procedure shows that if H possesses a nonzero element x, then it must be the case that $\mathbb{Q} \subseteq H$, to which $H = \mathbb{Q}$ follows.

On the other hand, if there exists no nonzero element $x \in H$, then only $0 \in H$, and we may write that $H = \{0\}$, so that H is the trivial subgroup. ■

Exercise 2.1.14. Show that $\{x \in D_{2n} \mid x^2 = 1\}$ is not a subgroup of D_{2n}, where $n \geq 3$.

Proof. Let $n \geq 3$ and consider the group D_{2n} and the subset $S = \{x \in D_{2n} \mid x^2 = 1\}$. We will show that $S \not\leq D_{2n}$. To do this, take the elements $sr, sr^2 \in D_{2n}$, which are guaranteed to exist for $n \geq 3$. Note that $|sr| = |sr^2| = 2$, and so $sr, sr^2 \in S$.

If $S \leq D_{2n}$ held, then it would have to be the case that $(sr)(sr^2) \in S$, for subgroups are closed under the binary operation of the group restricted to the subgroup. But:

$$(sr)(sr^2) = srsr^2 = srr^{-2}s = sr^{-1}s = rss = r \notin S$$

For clearly $|r| \neq 2$. Therefore, we have shown that S cannot be a subgroup of D_{2n} for all $n \geq 3$. ■

Exercise 2.1.15. Let $H_1 \leq H_2 \leq \cdots$ be an ascending chain of subgroups of G. Prove that $\bigcup_{i=1}^{\infty} H_i$ is a subgroup of G.

Proof. Let G be a group and suppose $H_1 \leq H_2 \leq \cdots$ is an ascending chain whereby each $H_i \leq G$. Now consider their infinite union $\bigcup_{i=1}^{\infty} H_i$. Note that even if each H_i were trivial, we would still have $1 \in \bigcup_{i=1}^{\infty} H_i$, to which $\bigcup_{i=1}^{\infty} H_i \neq \emptyset$.

Now suppose $a, b \in \bigcup_{i=1}^{\infty} H_i$. Then we may write that for some i and j, we have $a \in H_i$ and $b \in H_j$. Either $i = j$, in which case both a and b belong to this subgroup, or we have, without loss of generality, $i < j$, to which we may write that $a \in H_j$ also. Since $H_j \leq G$, it is clear that $ab^{-1} \in H_j$, to which $ab^{-1} \in \bigcup_{i=1}^{\infty} H_i$. Therefore, by the subgroup criterion, we have $\bigcup_{i=1}^{\infty} H_i \leq G$. ■

Exercise 2.1.16. Let $n \in \mathbb{Z}^+$ and let $\mathbb{F}$ be a field. Prove that the set $\{(a_{ij}) \in GL(n, \mathbb{F}) \mid a_{ij} = 0\ , i > j\}$ is a subgroup of $GL(n, \mathbb{F})$.

Proof. Fix $n \in \mathbb{Z}^+$ and choose a field $\mathbb{F}$. Let $U = \{(a_{ij}) \in GL(n, \mathbb{F}) \mid a_{ij} = 0\ , i > j\}$. Note that the $n \times n$ identity matrix, $\mathcal{I}_n = (a_{ij})$, satisfies the criterion that $a_{ij} = 0$ for all $i > j$ trivially, to which $\mathcal{I}_n \in U$.

Now suppose $(a_{ij}), (b_{ij}) \in U$. Then, in particular, (b_{ij}) defines an upper triangular matrix. We know that the inverse of an upper triangular matrix is again, an upper triangular matrix; hence $(b_{ij})^{-1}$ is an upper triangular matrix. The matrix product of two upper triangular matrices is again an upper triangular matrix, so we may write $(a_{ij})(b_{ij})^{-1} \in U$, to which U satisfies the subgroup criterion; hence $U \leq GL(n, \mathbb{F})$. ■

2.2 Centralizers and Normalizers, Stabilizers and Kernels

Exercise 2.2.1. Prove that $C_G(A) = \{g \in G \mid g^{-1}ag = a, \ \forall a \in A\}$.

Proof. Let G be a group and $A \subset G$ such that $A \neq \emptyset$. Suppose $x \in C_G(A)$. In particular, we have that:

$$xax^{-1} = a \iff ax^{-1} = x^{-1}a \iff a = x^{-1}ax$$

Implying $x \in \{g \in G \mid g^{-1}ag = a, \ \forall a \in A\}$, so we necessarily have that for arbitrary x, to which $C_G(A) \subseteq \{g \in G \mid g^{-1}ag = a, \ \forall a \in A\}$. Given that the above provides the implication both ways, this is equivalent to set equality. ■

Exercise 2.2.2. Prove that $C_G(Z(G)) = G$ and deduce $N_G(Z(G)) = G$.

Proof. Let G be a group. We immediately know that $C_G(Z(G)) \leq G$. Now suppose $x \in G$. Then we know $xg = gx$ for all $g \in Z(G)$, since elements of $Z(G)$ commute with all elements of G. We may multiply the above equation on the right by x^{-1} to find we have $xgx^{-1} = g$, to which $x \in C_G(Z(G))$. Since $x \in G$ was arbitrary, $G \subseteq C_G(Z(G))$, to which the reverse containment follows immediately since $C_G(Z(G)) \leq G$; hence, we have $C_G(Z(G)) = G$.

Given that, in general, we have $Z(G) \leq C_G(A) \leq N_G(A) \leq G$, we can take the result found above to write that if $C_G(Z(G)) = G$, then since $C_G(Z(G)) \leq N_G(Z(G))$, it follows that $G \leq N_G(Z(G))$, to which we obtain $N_G(Z(G)) = G$. ■

Exercise 2.2.3. Prove that if A and B are subsets of G with $A \subseteq B$, then $C_G(B)$ is a subgroup of $C_G(A)$.

Proof. Let G be a group and suppose $A, B \subseteq G$ with $A \subseteq B$. Suppose $x \in C_G(B)$. Then, in particular, $xbx^{-1} = b$ for all $b \in B$. Since each $a \in A$ satisfies $a \in B$, this necessarily means that $xax^{-1} = a$ for all such $a \in A$, to which $x \in C_G(A)$. Therefore, we have shown $C_G(B) \subseteq C_G(A)$. Since centralizers are subgroups, $C_G(B)$ is closed under products and inverses with respect to the inherited group operation of G, which is shared by $C_G(A)$, and thus we may conclude $C_G(B) \leq C_G(A)$. ■

Exercise 2.2.4. For each S_3, D_8, and Q_8, compute the centralizers of each element and find the center of each group.

Proof. First we determine S_3. Each of the 2-cycles in S_3 form a cyclic subgroup of order 2 in S_3. Since, in general, a 2-cycle is in its own centralizer, this implies that each cyclic subgroup of order 2 must divide the order of the centralizer, by

Lagrange's Theorem. Therefore, either their centralizer has order 2 or 6. In this manner, take $(1\ 2) \in S_3$. We know $\{\iota, (1\ 2)\} \leq C_{S_3}((1\ 2))$. We can see clearly:

$$(1\ 2\ 3)(1\ 2)(1\ 2\ 3)^{-1} = (1\ 2\ 3)(1\ 2)(1\ 3\ 2) = (2\ 3)$$

Which implies that $(1\ 2\ 3) \notin C_{S_3}((1\ 2))$. Hence $|C_{S_3}((1\ 2))| \neq 6$, to which it must be the case that $|C_{S_3}((1\ 2))| = 2$, and so $C_{S_3}((1\ 2)) = \{\iota, (1\ 2)\}$ must hold. A similar argument as the above shows that $C_{S_3}((1\ 3)) = \{\iota, (1\ 3)\}$ and $C_{S_3}((2\ 3)) = \{\iota, (2\ 3)\}$. For the 3-cycles, we can see:

$$(1\ 2\ 3)(1\ 3\ 2)(1\ 2\ 3)^{-1} = (1\ 2\ 3)(1\ 3\ 2)(1\ 3\ 2) = (1\ 3\ 2)$$

And so $(1\ 2\ 3) \in C_{S_3}((1\ 3\ 2))$. Similarly:

$$(1\ 3\ 2)(1\ 3\ 2)(1\ 3\ 2)^{-1} = (1\ 3\ 2)(1\ 3\ 2)(1\ 2\ 3) = (1\ 3\ 2)$$

To whcih $(1\ 3\ 2) \in C_{S_3}((1\ 3\ 2))$. In the above discussion,, we showed that the 3-cycles do not commute with the 2-cycles, and hence $C_{S_3}((1\ 3\ 2)) = \{\iota, (1\ 3\ 2), (1\ 2\ 3)\}$, and likewise $C_{S_3}((1\ 2\ 3)) = \{\iota, (1\ 2\ 3), (1\ 3\ 2)\}$. Since $Z(S_3)$ is a subgroup of any centralizer of S_3, it follows that $Z(S_3) = \{\iota\}$ since the identity permutation is the only common element in each centralizer.

Second, we determine D_8. Note that $x \in C_{D_8}(r)$ if and only if $xr = rx$. Since r and s do not commute, we know $s \notin C_{D_8}(r)$. Since powers of r commute, $r \in C_{D_8}(r)$, and since $C_{D_8}(r)$ is a subgroup, if $sr^i \in C_{D_8}(r)$, then $sr^ir^{-i} = s \in C_{D_8}(r)$, a contradiction. Therefore $C_{D_8}(r) = \{1, r, r^2, r^3\}$. We can arrive at a similar conclusion for r^3, and so $C_{D_8}(r^3) = \{1, r, r^2, r^3\}$. If we consider r^2, note that $sr^2s = ssr^{-2} = r^{-2} = r^2$, so necessarily we have $s \in C_{D_8}(r^2)$. But powers of r commute, and so $r \in C_{D_8}(r^2)$. Since r and s generate D_8, it must be the case that $C_{D_8}(r^2) = D_8$. Now consider $C_{D_8}(s)$. We showed above that s does not commute with r, but does commute with r^2, to which $s, r^2 \in C_{D_8}(s)$, and by closure $sr^2 \in C_{D_8}(s)$. Therefore we may write $C_{D_8}(s) = \{1, r^2, s, sr^2\}$. For $C_{D_8}(sr)$, note $ssrs = rs = sr^{-1}$, so $s \notin C_{D_8}(sr)$. Also, $rsrr^{-1} = rs = sr^{-1}$, and so $r \notin C_{D_8}(sr)$. Also, since $C_{D_8}(r^2) = D_8$, it must be the case that $r^2 \in C_{D_8}(sr)$. Therefore $C_{D_8}(sr) = \{1, r^2\}$. The case for the element sr^3 is identical and so $C_{D_8}(sr^3) = \{1, r^2\}$. What remains is to determine $C_{D_8}(sr^2)$, and since necessarily $r^2 \in C_{D_8}(sr^2)$, by closure $s \in C_{D_8}(sr^2)$. But $rsr^2r^{-1} = rsr = rr^{-1}s = s$, and so $r \notin C_{D_8}(sr^2)$. Therefore we conclude $C_{D_8}(sr^2) = \{1, r^2, s, sr^2\}$. From the results above, we can easily find $Z(D_8) = \{1, r^2\}$.

Third, we consider Q_8. First, we determine $C_{Q_8}(-1)$. Since $i \cdot -1 \cdot -i = i^2 = -1$, and similarly for each j and k, we know that $C_{Q_8}(-1) = Q_8$. Now consider $C_{Q_8}(i)$. We clearly have $1, -1 \in C_{Q_8}(i)$, and also:

$$i \cdot i \cdot -i = i^2 \cdot -i = -1 \cdot -i = i$$

And so $i \in C_{Q_8}(i)$, and by closure $-i \in C_{Q_8}(i)$ also. Note that j and k do not commute with i, and so we are done, with $C_{Q_8}(i) = \{\pm 1, \pm i\}$. Note that replacing i with $-i$ in the above equation shows that $C_{Q_8}(i) = C_{Q_8}(-i)$. The above reasoning holds true again for both j and k, and so we may write $C_{Q_8}(j) = C_{Q_8}(-j) = \{\pm 1, \pm j\}$ as well as $C_{Q_8}(k) = C_{Q_8}(-k) = \{\pm 1, \pm k\}$. Therefore, the center of Q_8 must be in each of the centralizers above, to which $Z(Q_8) = \{\pm 1\}$. ∎

Exercise 2.2.5. Show the specified group G and subgroup A of G satisfies $C_G(A) = A$ and $N_G(A) = G$.
a.) $G = S_3$ and $A = \{(1), (1\ 2\ 3), (1\ 3\ 2)\}$.
b.) $G = D_8$ and $A = \{1, r^2, s, sr^2\}$.
c.) $G = D_{10}$ and $A = \{1, r, r^2, r^3, r^4\}$.

Proof. (a) Note that $(1\ 2\ 3)(1\ 3\ 2) = (1\ 3\ 2)(1\ 2\ 3) = (1)$, and so $(1\ 2\ 3), (1\ 3\ 2) \in C_{S_3}(A)$. Therefore $A \leq C_{S_3}(A)$. Since $|A| = 3$ and $|S_3| = 6$, Lagrange's Theorem permits either $C_{S_3}(A) = A$ or $C_{S_3}(A) = S_3$. However:

$$(1\ 2)(1\ 2\ 3)(1\ 2) = (1\ 3\ 2)$$

And hence $(1\ 2) \notin C_{S_3}(A)$, to which $C_{S_3}(A) \neq S_3$ and thus $C_{S_3}(A) = A$. Note that we have $C_{S_3}(A) \leq N_{S_3}(A)$, and so $A \leq N_{S_3}(A)$. Again by Lagrange's Theorem, either $N_{S_3}(A) = A$ or $N_{S_3}(A) = S_3$. Our equation above shows that $(1\ 2) \in N_{S_3}(A)$, and hence $N_{S_3}(A) = S_3$ follows.

(b) We know $Z(D_8) = \{1, r^2\}$, and so $\{1, r^2\} \leq C_{D_8}(A)$. Since $sr^2s = ssr^{-2} = r^2$ and $ssr^2s = r^2s = sr^{-2} = sr^2$, we have $s \in C_{D_8}(A)$, and by closure $sr^2 \in C_{D_8}(A)$, to which $A \leq C_{D_8}(A)$. Lagrange's Theorem permits $C_{D_8}(A) = A$ or $C_{D_8}(A) = D_8$. Since:

$$rsr^{-1} = r^2s = sr^2 \neq s$$

We know $r \notin C_{D_8}(A)$, to which it must be the case that $C_{D_8}(A) \neq D_8$ and so $C_{D_8}(A) = A$. Now we know $A \leq N_{D_8}(A)$. The above equation shows that r fixes A under conjugation, since $sr^2 \in A$, and hence $r \in N_{D_8}(A)$, to which it must be the case that $N_{D_8}(A) = D_8$.

(c) Clearly rotations commute, in other words $r \cdot r^i \cdot r^{-1} = r^i$ for each possible i, and so we have $A \leq C_{D_{10}}(A)$. Lagrange's Theorem states that since $|D_{10}| = 10$, and $|A| = 5$, either $C_{D_{10}}(A) = A$ or $C_{D_{10}}(A) = D_{10}$. Note that:

$$srs = ssr^{-1} = r^{-1} \neq r$$

To which $s \notin C_{D_{10}}(A)$ and so $C_{D_{10}}(A) = A$ is forced. Now we have $A \leq N_{D_{10}}(A)$. The above equation shows $srs = r^{-1} = r^4 \in A$, and so $s \in N_{D_{10}}(A)$, and so it must be the case that $N_{D_{10}}(A) = D_{10}$ ∎

Exercise 2.2.6. Let H be a subgroup of G.
a,) Show that $H \leq N_G(H)$. Give an example to show that this is not necessarily true if H is not a subgroup.
b.) Show that $H \leq C_G(H)$ if and only if H is abelian.

Proof. (a) Let G be a group and suppose $H \leq G$. Consider $N_G(H) \leq G$. We can clearly see that since H is closed under the group operation, $hHh^{-1} = H$ for all $h \in H$, so H fixes elements of H. This is equivalent to $H \subseteq N_G(H)$. Since H is, in particular, a subgroup, it follows that $H \leq N_G(H)$.

Any example works, for if H is not a subgroup of G, then it cannot possibly be a subgroup of $N_G(H)$. Explicitly, we could take $G = D_6$ and consider $H = \{s, r\}$, clearly not a subgroup of D_6. Then:

$$r \cdot s \cdot r^{-1} = rsr^{-1} = rrs = r^2 s = sr^{-2} = sr^2 \notin H$$

And so $H \not\subset N_G(H)$, and thus cannot possibly satisfy $H \leq N_G(H)$.

(b) Let $H \leq G$. Suppose $H \leq C_G(H)$. Let $x, y \in H$. We know $xax^{-1} = a$ for all $a \in H$. In particular, since $y \in H$, we have $xyx^{-1} = y$ to which $xy = yx$ for all $x, y \in H$. Thus, H is abelian. Conversely, suppose H is an abelian subgroup of G. Then $xy = yx$ for all $x, y \in H$, and so $xyx^{-1} = y$ also holds, which is equivalent to $x \in C_G(H)$. But $y \in C_G(H)$ as well for $yxy^{-1} = x$. Thus $H \subseteq C_G(H)$, to which H being a subgroup of G implies $H \leq C_G(H)$. ■

Exercise 2.2.7. Let $n \in \mathbb{Z}$ with $n \geq 3$. Prove the following:
a.) $Z(D_{2n}) = 1$ if n is odd.
b.) $Z(D_{2n}) = \{1, r^k\}$ if $n = 2k$.

Proof. (a) Suppose we have $n \in \mathbb{Z}$ with $n \geq 3$, and n an odd intege. Suppose $s^k r^i \in Z(D_{2n})$, where $0 \leq k < 2$ and $1 \leq i \leq n$ are fixed. Taking an arbitrary element $s^h r^j \in D_{2n}$, we see:

$$s^k r^i s^h r^j r^{-i} s^{-k} = s^{k+h} r^{j-2i} s^{-k} = s^{2k+h} r^{2i-j}$$

Hence, in order for the two elements to commute, it must be the case that $2k+h = h$ and $2i - j = j$. Rearranging, we find $2k = 0 \implies k = 0$, and $2i = 2j \implies i = j$. However, this implies $s^k r^i$ commutes with only those elements that contain r^j, a contradiction to $s^k r^i \in Z(D_{2n})$. Thus no such element exists, and so $Z(D_{2n})$ is trivial. ■

(b) Suppose instead that we have $n \in \mathbb{Z}$ with $n \geq 3$ such that $n = 2k$ for some integer k. Now assume $s^k r^i \in Z(D_{2n})$. TO-DO ■

Exercise 2.2.8. Let $G = S_n$, fix an $i \in \{1, 2, \ldots, n\}$ and let $G_i = \{\sigma \in G \mid \sigma(i) = i\}$. Use group actions to prove that G_i is a subgroup of G. Find $|G_i|$.

Proof. Take G and fix an i as outlined in the problem. Let G act on the set of indices $\{1, 2, \ldots, n\}$ by $\sigma \cdot i = \sigma(i)$ for all $\sigma \in G$. Note first that the identity permutation in S_n fixes all indices, in particular $\iota \cdot i = \iota(i) = i$ for any i. Hence $\iota \in G_i$, to which $G_i \neq \emptyset$. Now suppose $\sigma_1, \sigma_2 \in G_i$. We know:

$$(\sigma_1 \circ \sigma_2^{-1}) \cdot i = \sigma_1 \cdot (\sigma_2^{-1} \cdot i) = \sigma_1 \cdot \sigma_2^{-1}(i) = \sigma_1 \cdot i = \sigma_1(i) = i$$

To which we may write that $\sigma_1 \circ \sigma_2^{-1} \in G_i$; hence by the subgroup criterion, we can say that $G_i \leq G$. In order to find $|G_i|$, we would like to determine the number of permutations in G that act to fix i. First recall that $|S_n| = n!$. In terms of counting, a permutation that fixes i removes at least one index, and thus such a permutation would act on the set of $n-1$ indices, $\{1, 2, \ldots, n-1\}$. Therefore, in this way, we can see that $|G_i| = |S_{n-1}| = (n-1)!$. ∎

Exercise 2.2.9. For any subgroup H of G and any nonempty subset A of G, define $N_H(A)$ to be the set $\{h \in H \mid hAh^{-1} = A\}$. Show that $N_H(A) = N_G(A) \cap H$ and deduce that $N_H(A)$ is a subgroup of H.

Proof. Let G be a group, $H \leq G$, and $A \subseteq G$ such that $A \neq \emptyset$. Take the set $N_H(A)$ as defined in the problem. Suppose $x \in N_H(A)$. We have $x \in H$ by construction, and also $xAx^{-1} = A$, to which it necessarily follows that $x \in N_G(A)$ and $x \in H$, or equivalently, $x \in N_G(A) \cap H$; hence we may write $N_H(A) \subseteq N_G(A) \cap H$.

For the converse, suppose $x \in N_G(A) \cap H$. Then $xAx^{-1} = A$ and $x \in H$, to which the construction of the set $N_H(A)$ permits $x \in N_H(A)$, and so $N_G(A) \cap H \subseteq N_H(A)$. Therefore we have $N_H(A) = N_G(A) \cap H$.

We know that the intersection of two subgroups of a group is again a subgroup of the given group. In this manner, we know that $N_A(H) \leq G$, for both $N_G(A) \leq G$ and $H \leq G$. Note additionally that $N_H(A) \subseteq H$, to which $N_H(A) \leq H$. ∎

Exercise 2.2.10. Let H be a subgroup of order 2 in G. Show that $N_G(H) = C_G(H)$. Deduce that if $N_G(H) = G$, then $H \leq Z(G)$.

Proof. Let G be a group and $H \leq G$ such that $|H| = 2$. Given that H contains the identity, there is one non-identity element of H, call it h. Now suppose $x \in N_G(H)$. Then we may write that $xHx^{-1} = H$, or equivalently $xH = Hx$. In particular, we may have $x1 = 1x$, which trivially holds, $xh = 1x$, $x1 = xh$, or $xh = hx$. In the case where $xh = 1x$, which is equivalent to $xh = x$, the left cancellation law implies $h = 1$, which contradicts our assumption that $h \neq 1$. The same holds in the case where $x1 = xh$.

Therefore we are left with $x1 = 1x$ or $xh = hx$. The first equation implies $x1x^{-1} = 1$. The second is equivalent to $xhx^{-1} = h$. Therefore, $xhx^{-1} = h$ for all

$h \in H$, namely the identity and h. This is sufficient criterion for $x \in C_G(H)$, and so $N_G(H) \leq C_G(H)$. But we know that $C_G(H) \leq N_G(H)$ holds in general; hence $N_G(H) = C_G(H)$. ■

Given the above result, if we had $N_G(H) = G$, then $C_G(H) = G$ as well, so if $g \in G$, then $ghg^{-1} = h$, or equivalently, $gh = hg$ for all $h \in H$. In particular, this means that H is abelian, and so by [[DF-2.2-6]], $H \leq Z(G)$. ■

Exercise 2.2.11. Prove that $Z(G) \leq N_G(A)$ for any subset A of G.

Proof. Take G a group and $A \subseteq G$ with $A \neq \emptyset$. Suppose $x \in Z(G)$. Then $xg = gx$ for all $g \in G$, to which $xgx^{-1} = g$. In particular, for any $a \in A$, we have $xax^{-1} = a$, and so $x \in C_G(A)$. In general, $C_G(A) \leq N_G(A)$, and so $x \in N_G(A)$. Since $x \in Z(G)$ was arbitrary, we have $Z(G) \subseteq N_G(A)$, and since $Z(G) \leq G$, it must be the case that $Z(G) \leq N_G(A)$. ■

Exercise 2.2.12. Let R be the set of all polynomials with integer coefficients in the independent variables x_1, x_2, x_3, x_4; i.e. $R = \mathbb{Z}[x_1, x_2, x_3, x_4]$.

a.) Let $p(x_1, x_2, x_3, x_4)$ be the polynomial above, let $\sigma = (1\ 2\ 3\ 4)$ and $\tau = (1\ 2\ 3)$. Compute $\sigma \cdot p$, $\tau \cdot (\sigma \cdot p)$, $(\tau \circ \sigma) \cdot p$, and $(\sigma \circ \tau) \cdot p$.

b.) Prove that these definitions give a left group action of S_4 on R.

c.) Exhibit all permutations in S_4 that stabilize x_4, and prove that they form a subgroup isomorphic to S_3.

d.) Exhibit all permutations in S_4 that stabilize the element $x_1 + x_2$ and prove that they form an abelian subgroup of order 4.

e.) Exhibit all permutations in S_4 that stabilize the element $x_1x_2 + x_3x_4$ and prove that they form a subgroup isomorphic to the dihedral group of order 8.

f.) Show that the permutations in S_4 that stabilize the element $(x_1 + x_2)(x_3 + x_4)$ are exactly the same as those found in part (e).

Proof. (a) Let $p(x_1, x_2, x_3, x_4) = 12x_1^5x_2^7x_4 - 18x_2^3x_3 + 11x_1^6x_2x_3^3x_4^{23}$ be as in the problem description. Taking the map from the description, we may find:

$$\sigma \cdot p = 12x_2^5x_3^7x_1 - 18x_3^3x_4 + 11x_2^6x_3x_4^3x_1^{23}$$

$$\tau \cdot (\sigma \cdot p) = 12x_3^5x_1^7x_2 - 18x_1^3x_4 + 11x_3^6x_1x_4^3x_2^{23}$$

$$(\tau \circ \sigma) \cdot p = 12x_3^5x_1^7x_2 - 18x_1^3x_4 + 11x_3^6x_1x_4^3x_2^{23}$$

$$(\sigma \circ \tau) \cdot p = 12x_3^5x_4^7x_1 - 18x_4^3x_2 + 11x_3^6x_4x_2^3x_1^{23}$$

Which are all of the required calculations.

(b) Let S_4 act on R defined by $(\sigma, p(x_1, x_2, x_3, x_4)) \mapsto p(x_{\sigma(1)}, x_{\sigma(2)}, x_{\sigma(3)}, x_{\sigma(4)})$ for all $\sigma \in S_4$ and $p(x_1, x_2, x_3, x_4) \in R$. Take $\sigma_1, \sigma_2 \in S_4$, and $p \in R$. Then:

$$\sigma_1 \cdot (\sigma_2 \cdot p) = \sigma_1 \cdot p(x_{\sigma_2(1)}, x_{\sigma_2(2)}, x_{\sigma_2(3)}, x_{\sigma_2(4)})$$

$$= p(x_{(\sigma_1\circ\sigma_2)(1)}, x_{(\sigma_1\circ\sigma_2)(2)}, x_{(\sigma_1\circ\sigma_2)(3)}, x_{(\sigma_1\circ\sigma_2)(4)})$$
$$= (\sigma_1 \circ \sigma_2) \cdot p$$

So that the first condition for a group action is met. Now note that for any $p \in R$, taking the identity permutation $\iota \in S_4$ we find:

$$\iota \cdot p = p(x_{\iota(1)}, x_{\iota(2)}, x_{\iota(3)}, x_{\iota(4)})$$
$$= p(x_1, x_2, x_3, x_4) = p$$

And so the second condition is also met. Therefore, the map defined above satisfies the requirements to be a group action of S_4 on the set R.

(c) We would like to take all permutations in S_4 that stabilize the element $x_4 \in R$. In essence, we would like to determine $(S_4)_{x_4}$. Clearly $\sigma \in (S_4)_{x_4}$ if and only if $\sigma \cdot x_4 = x_{\sigma(4)} = x_4$, so that σ must fix 4. Proceeding in this manner, we find:

$$(S_4)_{x_4} = \{\iota, (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)\}$$

And, since $(S_4)_{x_4} \leq S_4$, we know that in particular $(S_4)_{x_4}$ is a group. This fact, along with that $|(S_4)_{x_4}| = 6$, in addition to $(S_4)_{x_4}$ clearly being non-abelian, allows us to conclude that $(S_4)_{x_4}$ must be isomorphic to S_3. Therefore $(S_4)_{x_4} \cong S_3$.

(d) Now we would like to take all $\sigma \in S_4$ that stabilize $x_1 + x_2 \in R$. Equivalently, we want to find $(S_4)_{x_1+x_2}$. In order for $\sigma \in (S_4)_{x_1+x_2}$, we need to have the relation that $\sigma \cdot x_1 + x_2 = x_{\sigma(1)} + x_{\sigma(2)} = x_1 + x_2$ or $x_2 + x_1$. Hence, either 1 and 2 are fixed, or they are swapped. The permutations which satisfy this criterion are:

$$(S_4)_{x_1+x_2} = \{\iota, (1\ 2), (3\ 4), (1\ 2)(3\ 4)\}$$

The identity permutation trivially commutes with all other elements of $(S_4)_{x_1+x_2}$. Now, note that $(1\ 2)(3\ 4) = (3\ 4)(1\ 2)$ since disjoint cycles commute. Further, we have $(1\ 2)(1\ 2)(3\ 4) = (3\ 4)$ and $(1\ 2)(3\ 4)(1\ 2) = 3\ 4)$ so that the permutations $(1\ 2)(3\ 4)$ and $(1\ 2)$ also commute. Finally, note that $(3\ 4)$ and $(1\ 2)(3\ 4)$ also commute for the same reason as the previous case. Therefore we may conclude that $(S_4)_{x_1+x_2}$, is an abelian subgroup of order 4.

(e) The permutations of S_4 that stabilize the element $x_1x_2 + x_3x_4 \in R$ are precisely those that either swap 1 and 2 while fixing 3 and 4, swap 3 and 4 whiile fixing 1 and 2, or swap both pairs simultaneously, or fix all of them. We can find:

$$(S_4)_{x_1x_2+x_3x_4} = \{\iota, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3), (1\ 2), (3\ 4), (1\ 3\ 2\ 4), (1\ 4\ 2\ 3)\}$$

Now, in order to prove that $(S_4)_{x_1x_2+x_3x_4}$ is isomorphic to D_8, we will have to construct a map. Take $\Phi : (S_4)_{x_1x_2+x_3x_4} \longrightarrow D_8$ defined explicitly by:

$$\Phi(\iota) = 1,\ \Phi((1\ 3\ 2\ 4)) = r,\ \Phi((1\ 2)(3\ 4)) = r^2,\ \Phi((1\ 4\ 2\ 3)) = r^3$$

$$\Phi((1\ 4)(2\ 3)) = s,\ \Phi((1\ 2)) = sr,\ \Phi((1\ 3)(2\ 4)) = sr^2,\ \Phi((3\ 4)) = sr^3$$

This mapping is clearly injective and surjective, and is thus a bijection between the groups. Furthermore, it can be checked that Φ is a group homomorphism. First, note that $\Phi(1\ 3\ 2\ 4)^4 = 1$ and $\Phi((1\ 4)(2\ 3))^2 = 1$, Additionally, we can see:

$$\Phi((1\ 3\ 2\ 4))\Phi((1\ 4)(2\ 3)) = \Phi((1\ 4)(2\ 3))\Phi((1\ 3\ 2\ 4))^{-1}$$

So that the relations of $r, s \in D_{2n}$, specifically $rs = sr^{-1}$, are satisfied by Φ. The rest of the homomorphism follows. Therefore, we have constructed an isomorphism; hence $(S_4)_{x_1x_2+x_3x_4} \cong D_8$.

(f) Now we would like to take the permutations in S_4 which stabilize the element $(x_1 + x_2)(x_3 + x_4) \in R$. Note $(x_1 + x_2)(x_3 + x_4) = x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4$. In particular, we want to determine $(S_4)_{(x_1+x_2)(x_3+x_4)}$, which can be found:

$$\{\iota, (1\ 2), (3\ 4), (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3), (1\ 3\ 2\ 4), (1\ 4\ 2\ 3)\}$$

Note that $(S_4)_{(x_1+x_2)(x_3+x_4)} = (S_4)_{x_1x_2+x_3x_4}$ that we found in part (e). The stabilizers of these elements contain precisely the same permutations in S_4. ■

Exercise 2.2.13. Let n be a positive integer and let $R = \mathbb{Z}[x_1, x_2, x_3, x_4]$. For each $\sigma \in S_n$, define a map $\sigma : R \longrightarrow R$ by $\sigma \cdot p(x_1, \dots, x_n) = p(x_{\sigma(1)}, \dots, x_{\sigma(n)})$. Prove that this defines a left group action of S_n on R.

Proof. Take $n \in \mathbb{Z}^+$ and consider $R = \mathbb{Z}[x_1, x_2, x_3, x_4]$ with the mapping defined above. Note first that for any $p(x_1, \dots, x_n) \in R$, arbitrarily letting p be of degree m, with $a_i \in \mathbb{Z}$ for $1 \leq i \leq m$, and letting $r_j \in \mathbb{Z}_{\geq 0}$ for $1 \leq j \leq n$, we have:

$$\begin{aligned}
\iota \cdot p(x_1, \dots, x_n) &= \iota \cdot \sum_{i=1}^{m} a_i \prod_{j=1}^{n} x_j^{r_j} \\
&= \sum_{i=1}^{m} a_i \prod_{j=1}^{n} x_{\iota(j)}^{r_j} \\
&= \sum_{i=1}^{m} a_i \prod_{j=1}^{n} x_j^{r_j} \\
&= p(x_1, \dots, x_n)
\end{aligned}$$

Which follows since $\iota(i) = i$ for any $1 \leq i \leq n$. And so the first condition for a group action holds. Now take any permutations $\sigma, \tau \in S_n$ and letting $p(x_1, \dots, x_n) \in R$

be arbitrary once more, note that:

$$\begin{aligned}
\sigma \cdot (\tau \cdot p(x_1, \dots, x_n)) &= \sigma \cdot (\tau \cdot \sum_{i=1}^{m} a_i \prod_{j=1}^{n} x_j^{r_j}) \\
&= \sigma \cdot \sum_{i=1}^{m} a_i \prod_{j=1}^{n} x_{\tau(j)}^{r_j} \\
&= \sum_{i=1}^{m} a_i \prod_{j=1}^{n} x_{\sigma(\tau(j))}^{r_j} \\
&= \sum_{i=1}^{m} a_i \prod_{j=1}^{n} x_{(\sigma\circ\tau)(j)}^{r_j} \\
&= (\sigma \circ \tau) \cdot \sum_{i=1}^{m} a_i \prod_{j=1}^{n} x_j^{r_j} \\
&= (\sigma \circ \tau) \cdot p(x_1, \dots, x_n)
\end{aligned}$$

To which the second condition for a group action holds. Therefore, we may refer to the definition of a group action to conclude that the mapping defined above imparts a left group action of S_n on the set R. ■

Exercise 2.2.14. Let $H(F)$ be the Heisenberg group over the field F. Determine which matrices lie in the center of $H(F)$ and prove that $Z(H(F))$ is isomorphic to the additive group F.

Proof. Consider $H(F)$, and suppose we have a matrix $X \in Z(H(F))$. Let X be given by:

$$X = \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}$$

Where $a, b, c \in F$. If we take another arbitrary matrix $Y \in H(F)$, then $Y \in Z(H(F))$ only when $XY \in Z(H(F))$. This occurs precisely when:

$$XY = \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & d & e \\ 0 & 1 & f \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a+d & b+af+e \\ 0 & 1 & c+f \\ 0 & 0 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & a+d & b+dc+e \\ 0 & 1 & c+f \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & d & e \\ 0 & 1 & f \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} = YX$$

Note that $XY = YX$ only when $b + af + e = b + dc + e$, equivalently only if $af = dc$. Since $a, c \in F$ were fixed by virtue of our choice of X, this relation must hold for any such $d, f \in F$, or for any such $Y \in H(F)$, to which it must be the case that $a = 0$ and $c = 0$. Therefore, we may write:

$$Z(H(F)) = \{\begin{pmatrix} 1 & 0 & a \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \mid a \in F\}$$

Now we would like to show $Z(H(F)) \cong F$, where F is taken as an additive group. Construct a map $\Phi : F \longrightarrow Z(H(F))$ defined, for each $a \in F$, by:

$$\Phi(a) = \begin{pmatrix} 1 & 0 & a \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

We will show that Φ is a group homomorphism. To do this, take $x, y \in F$ and note that:

$$\Phi(x+y) = \begin{pmatrix} 1 & 0 & x+y \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & x \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 & y \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \Phi(x)\Phi(y)$$

So that we have shown Φ is a group homomorphism. Further, we can see that Φ is clearly injective, as well as surjective. Therefore Φ is an isomorphism and we may write $Z(H(F)) \cong F$. ■

2.3 Cyclic Groups and Cyclic Subgroups

Exercise 2.3.1 Find all subgroups of $Z_{45} = \langle x \rangle$, giving a generator for each. Describe the containments between these subgroups.

Proof. We will determine the subgroups of Z_{45}. The positive divisors of 45 are as follows: $1, 3, 5, 9, 15$, and 45. Therefore, we have subgroups corresponding to $\langle 1 \rangle$, $\langle 3 \rangle$, $\langle 5 \rangle$, $\langle 9 \rangle$, $\langle 15 \rangle$, and $\langle 45 \rangle$. The subgroup $\langle 1 \rangle$ is of order 45 and is generated by 1. The subgroup $\langle 3 \rangle$ is of order 15 and is generated by 3. The subgroup $\langle 5 \rangle$ is of order 9 and is generated by 5. The subgroup $\langle 9 \rangle$ is of order 5 and is generated by 9. The subgroup $\langle 15 \rangle$ is of order 3 and is generated by 15. Finally, the subgroup $\langle 45 \rangle$ is of order 1 and is generated by 45.

For containment, we may write that $\langle x \rangle \leq \langle y \rangle$ if and only if $y \mid x$. Hence we have the following: $\langle 45 \rangle \leq \langle 9 \rangle \leq \langle 3 \rangle \leq \langle 1 \rangle$, $\langle 45 \rangle \leq \langle 15 \rangle \leq \langle 3 \rangle \leq \langle 1 \rangle$, and finally we have $\langle 45 \rangle \leq \langle 15 \rangle \leq \langle 5 \rangle \leq \langle 1 \rangle$. ∎

Exercise 2.3.2 If x is an element of a finite group G and $|x| = |G|$, prove that $G = \langle x \rangle$. Give an explicit example to show that this need not be the case if G is an infinite group.

Proof. Let G be a finite group and suppose $x \in G$ such that $|x| = |G|$. Since x generates a cyclic subgroup of G, we immediately have $\langle x \rangle \leq G$. Now suppose $g \in G$. Then, since $|G| = |x|$, and $\langle x \rangle \leq G$, it must be the case that $g = x^a$ for some $0 \leq a \leq |G|$. But this means $g \in \langle x \rangle$, to which $G \leq \langle x \rangle$; hence we may conclude that $\langle x \rangle = G$.

To show that the above need not hold if G is infinite, take $G = \mathbb{Z}$ and $x = 2$. Then clearly $|2| = |\mathbb{Z}| = \infty$, however $\langle 2 \rangle = 2\mathbb{Z} \neq \mathbb{Z}$. ∎

Exercise 2.3.3 Find all generators for $\mathbb{Z}/48\mathbb{Z}$.

Proof. An element $x \in \mathbb{Z}/48\mathbb{Z}$ is a generator for this group if and only if $\gcd(48, x) = 1$, which follows from Proposition 6(2). We know $48 = 2^4 \cdot 3$. Euler's phi function allows us to see that there are $\varphi(48) = 16$ coprime integers to 48, to which there are 16 generators for $\mathbb{Z}/48\mathbb{Z}$. These coprime integers are 1, 5, 7, 11, 13, 17, 19, 23, 25, 29, 31, 35, 37, 41, 43, and 47. These are precisely the generators for $\mathbb{Z}/48\mathbb{Z}$. ∎

Exercise 2.3.4 Find all generators for $\mathbb{Z}/202\mathbb{Z}$.

Proof. We first note that $202 = 2 \cdot 101$. The number of coprime positive integers less than 101 is given by Euler's phi function, and permits $\varphi(101) = 100$. Thus, there are 100 coprime integers less than 101. By Proposition 6(2), these coprime integers are precisely the generators of $\mathbb{Z}/202\mathbb{Z}$. These generators are precisely those odd integers between 0 and 202, not including 101 itself, of which there are 100. ■

Exercise 2.3.5 Find the number of generators for $\mathbb{Z}/49000\mathbb{Z}$.

Proof. By Proposition 6(2), there are exactly $\varphi(49000)$ generators for the group $\mathbb{Z}/49000\mathbb{Z}$. Note that $49000 = 2^3 \cdot 5^3 \cdot 7^2$. Euler's phi function allows us to see that:

$$\varphi(49000) = 2^{3-1}(2-1)5^{3-1}(5-1)7^{2-1}(7-1) = 2^2 \cdot 5^2 \cdot 4 \cdot 7 \cdot 6 = 16800$$

Therefore there are exactly 16800 generators for the group $\mathbb{Z}/49000\mathbb{Z}$. ■

Exercise 2.3.6

Exercise 2.3.7

Exercise 2.3.8

Exercise 2.3.9

Exercise 2.3.10

Exercise 2.3.11

Exercise 2.3.12 Prove that the following groups are not cyclic:
a.) $Z_2 \times Z_2$.
b.) $Z_2 \times \mathbb{Z}$
c.) $\mathbb{Z} \times \mathbb{Z}$

Proof. (a) This group consists of four elements, namely $(\overline{0}, \overline{0}), (\overline{0}, \overline{1}), (\overline{1}, \overline{0})$, and $(\overline{1}, \overline{1})$. For the cyclic subgroup generated by the identity, we recover the identity. Otherwise, we may take the cyclic subgroup generated by each of the other three elements and note:

$$\langle(\overline{0}, \overline{1})\rangle = \{(\overline{0}, \overline{0}), (\overline{0}, \overline{1})\}$$

$$\langle(\overline{1}, \overline{0})\rangle = \{(\overline{0}, \overline{0}), (\overline{1}, \overline{0})\}$$

$$\langle(\overline{1}, \overline{1})\rangle = \{(\overline{0}, \overline{0}), (\overline{1}, \overline{1})\}$$

And clearly none of the above sets are equal to $Z_2 \times Z_2$. Therefore there can be no such one element that generates the whole group, to which $Z_2 \times Z_2$ is non-cyclic.

(b) Assume, for contradiction, that $Z_2 \times \mathbb{Z}$ is a cyclic group. Clearly this group is infinite, and so by Theorem 4(2), we must have $Z_2 \times \mathbb{Z} \cong \mathbb{Z}$. However, note that the cyclic subgroup generated by the element $(\overline{1}, 0)$ is finite. This can be seen by composing the element with itself, in particular, $|(\overline{1}, 0)| = 2$. Since $Z_2 \times \mathbb{Z} \cong \mathbb{Z}$, it follows that $\mathbb{Z}$ must have a cyclic subgroup of order 2; however it is clear that it does not. Hence $Z_2 \times \mathbb{Z} \ncong \mathbb{Z}$, to which $Z_2 \times \mathbb{Z}$ is a non-cyclic group.

(c) Suppose, for contradiction, that the group $\mathbb{Z}\times\mathbb{Z}$ is cyclic. By definition, there exists some element (a, b) for which $\langle(a, b)\rangle = \mathbb{Z}\times\mathbb{Z}$. This necessitates $|(a, b)| = \infty$. In particular, there exists some positive integers n and m for which $(a, b)^n = (0, 1)$ and $(a, b)^m = (1, 0)$. Equivalently, we have $(a^n, b^n) = (0, 1)$, to which $a^n = 0$, and $(a^m, b^m) = (1, 0)$, to which $b^m = 0$. However this implies:

$$(a, b)^{mn} = (a^{mn}, b^{mn}) = ((a^n)^m, (b^m)^n) = (0, 0)$$

To which $|(a, b)| \leq mn < \infty$ since $mn \in \mathbb{Z}^+$; a contradiction to the element (a, b) having infinite order. Therefore we may conclude that $\mathbb{Z} \times \mathbb{Z}$ is non-cyclic. ∎

Exercise 2.3.13 Prove that the following pairs of groups are not isomorphic:
a.) $\mathbb{Z} \times Z_2$ and $\mathbb{Z}$.
b.) $\mathbb{Q} \times Z_2$ and $\mathbb{Q}$.

Proof. (a) In part (b) of [[DF-2.3-12]], we showed that $\mathbb{Z}\times Z_2$ was not a cyclic group. In particular, Theorem 4(2) permits us to write that $\mathbb{Z} \times Z_2 \ncong \mathbb{Z}$, which follows since all infinite cyclic groups are isomorphic to $\mathbb{Z}$.

(b) Let $\langle x\rangle = Z_2$. Note that $(0, x) \in \mathbb{Q} \times Z_2$ has finite order, in particular, it has order 2; hence the cyclic subgroup formed by this element is $\langle(0, x)\rangle \leq \mathbb{Q} \times Z_2$. There is no such cyclic subgroup of order 2 in the group $\mathbb{Q}$. Since isomorphisms preserve such subgroup structures, we may write $\mathbb{Q} \times Z_2 \ncong \mathbb{Q}$. ∎

Exercise 2.3.14

Exercise 2.3.15 Prove that $\mathbb{Q} \times \mathbb{Q}$ is not cyclic.

Proof. Assume, for contradiction, that $\mathbb{Q} \times \mathbb{Q}$ is a cyclic group. In this manner, we may write that there exists some element, say (p, q), for which $\langle(p, q)\rangle = \mathbb{Q} \times \mathbb{Q}$. Thus there exists integers a and b, where $a \neq b$, for which:

$$(p, q)^a = (1, 0) \text{ and } (p, q)^b = (1, 1)$$

Note then that $(p, q)^a = (ap, aq)$ and $(p, q)^b = (bp, bq)$. We may then write that $ap = 1$ and $bp = 1$ hold simultaneously. But this implies $p = 1/a$ and $p = 1/b$, so $1/a = 1/b$, or $a = b$. This is a contradiction for we assumed $a \neq b$; hence no such element (p, q) exists, and thus the group $\mathbb{Q} \times \mathbb{Q}$ is not cyclic. ∎

Exercise 2.3.16

Exercise 2.3.17

Exercise 2.3.18

Exercise 2.3.19

Exercise 2.3.20 Let p be a prime and $n \in \mathbb{Z}^+$. Show that if x is an element of the group G such that $x^{p^n} = 1$ then $|x| = p^m$ for some $m \leq n$.

Proof. Let G be a group, p a prime, and $n \in \mathbb{Z}^+$. Suppose $x \in G$ such that $x^{p^n} = 1$. We immediately have, by virtue of Proposition 3, that $|x| \mid p^n$. Thus, we may write that $|x| \cdot k = p^n$ for some $k \in \mathbb{Z}$. Since the order of an element is a positive integer, this implies:

$$|x| = \frac{p^n}{k} \in \mathbb{Z}^+$$

But, since p^n is a power of a prime p, and k divides p^n, we must have $k = p^a$ for some $a \leq n$, equivalently, k must also be some prime power of p. The requirement that $a \leq n$ comes from $|x| \in \mathbb{Z}^+$. Our above equation becomes:

$$|x| = \frac{p^n}{p^a} = p^{n-a}$$

Note $n - a > 0$. Setting $m = n - a$, and taking account of the fact that $|x| = p^{n-a}$, it is then clear that $|x| = p^m$, where $m \leq n$. ■

Exercise 2.3.21

Exercise 2.3.22

Exercise 2.3.23

Exercise 2.3.24

Exercise 2.3.25 Let G be a cyclic group of order n and let k be an integer relatively prime to n. Prove that the map $x \mapsto x^k$ is surjective. Use Lagrange's Theorem to prove that the same is true for any finite group of order n.

Proof. Let G be a cyclic group of order n, denoted by $G = \langle x \rangle$. Let $k \in \mathbb{Z}$ such that $\gcd(n, k) = 1$. By Proposition 6(2) we know that $G = \langle x^k \rangle$. Construct a map

$\varphi : G \to G$ defined by $\varphi(x) = x^k$ for all $x \in G$. To prove that φ is surjective, suppose $y \in G$. Since $\langle x^k \rangle = G$, we may write $y = (x^k)^a$ for some $a \in \mathbb{Z}$. Note:

$$y = (x^k)^a = \varphi(x)^a \in G$$

To which $G \subseteq \varphi(G)$, and since the reverse containment is trivial, we may write that $G = \varphi(G)$; hence the map φ is surjective by definition. ■

Exercise 2.3.26 Let Z_n be a cyclic group of order n and for each integer a let:

$$\sigma_a : Z_n \to Z_n \text{ by } \sigma_a(x) = x^a \text{ for all } x \in Z_n$$

a.) Prove that σ_a is an automorphism of Z_n if and only if a is relatively prime to n.
b.) Prove that $\sigma_a = \sigma_b$ if and only if $a \equiv b \mod n$.
c.) Prove that every automorphism of Z_n is equal to σ_a for some a.
d.) Prove that $\sigma_a \circ \sigma_b = \sigma_{ab}$. Deduce that the map $\overline{a} \mapsto \sigma_a$ is an automorphism of $(\mathbb{Z}/n\mathbb{Z})^\times$ onto the automorphism group of Z_n.

Proof. (a) Consider Z_n and take the map σ_a defined for each $a \in \mathbb{Z}$ as above. Suppose $\sigma_a \in \text{Aut}(Z_n)$. Then σ_a is an isomorphism, and so by definition maps generators to generators. In this case, if $Z_n = \langle x \rangle$, then $\sigma_a(x) = x^a$ must satisfy $\langle x^a \rangle = Z_n$. By Proposition 6(2), this implies $\gcd(a, n) = 1$.

Conversely, suppose $\gcd(a, n) = 1$. Let $x^i, x^j \in Z_n$, where $i, j \in \mathbb{Z}$. Then:

$$\sigma_a(x^i x^j) = \sigma_a(x^{i+j}) = x^{a(i+j)} = x^{ai+aj} = x^{ai}x^{aj} = (x^j)^a(x^j)^a = \sigma_a(x^i)\sigma_a(x^j)$$

And hence the mapping σ_a is a group homomorphism from Z_n onto Z_n. Furthermore, by [[DF-2.3-25]], the map σ_a is surjective. Now assume $\sigma_a(x^i) = \sigma_a(x^j)$. Then:

$$(x^i)^a = (x^j)^a \iff x^{ia-ja} = 1 \iff x^{a(i-j)} = 1 \iff \sigma_a(x^{i-j}) = 1$$

But since σ_a is a group homomorphism, the above implies $x^{i-j} = 1$, to which $x^i = x^j$ and so the map σ_a is injective. Thus σ_a is an isomorphism from Z_n onto Z_n, equivalently, $\sigma_a \in \text{Aut}(Z_n)$.

(b) Now suppose $\sigma_a = \sigma_b$. Then $\sigma_a(x) = \sigma_b(x)$ for each $x \in Z_n$, Take some $k \in \mathbb{Z}$ and consider $x^k \in Z_n$. Then we know $\sigma_a(x^k) = \sigma_b(x^k)$, which permits us to write:

$$(x^k)^a = (x^k)^b \iff x^{ka} = x^{kb} \iff x^{ka-kb} = 1 \iff x^{k(a-b)} = 1 = x^n$$

But since $x^n = 1$, we must have $k(a - b) = n$, or $a - b \mid n$, which is precisely equivalent to $a \equiv b \mod n$. This proves the implication in both directions, and thus completes the proof.

(c) Suppose we have some arbitrary $\tau \in \text{Aut}(Z_n)$. Then τ is an isomorphism from Z_n onto Z_n, and so in particular τ must map generators of Z_n to generators of Z_n. In Proposition 6(2), we identifed the generators of Z_n as those elements x^a for integers a for which $\gcd(a, n) = 1$. Thus, if τ is not the trivial isomorphism, i.e. $\tau(x) \neq x$ for all $x \in Z_n$, then τ maps $x \mapsto x^a$ for some such integer a. Therefore $\tau = \sigma_a$ as desired.

(d) Take $x \in Z_n$ and let $a, b \in \mathbb{Z}$. Then we can observe:

$$(\sigma_a \circ \sigma_b)(x) = \sigma_a(\sigma_b(x)) = \sigma_a(x^b) = (x^b)^a = x^{ab} = \sigma_{ab}(x)$$

Since x was arbitrary, the above holds for all of Z_n, and hence $\sigma_a \circ \sigma_b = \sigma_{ab}$.

Construct a mapping $\psi : (\mathbb{Z}/n\mathbb{Z})^\times \longrightarrow \text{Aut}(Z_n)$ defined by $\psi(\overline{a}) = \sigma_a$ for each residue class $\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^\times$. Note that the group $(\mathbb{Z}/n\mathbb{Z})^\times$ consists of all those residue classes $\overline{a}$ for which $\gcd(a, n) = 1$. Taking $\overline{a}, \overline{b} \in (\mathbb{Z}/n\mathbb{Z})^\times$, we can see that:

$$\psi(\overline{ab}) = \sigma_{ab} = \sigma_a \circ \sigma_b = \psi(\overline{a})\psi(\overline{b})$$

Which follows from the proof above. This shows that ψ is a group homomorphism. From part (b), we know that ψ is injective, and from part (c), we have ψ is surjective; hence a bijection. Therefore, ψ is an isomorphism, to which we may write $(\mathbb{Z}/n\mathbb{Z})^\times \cong \text{Aut}(Z_n)$. This shows that $\text{Aut}(Z_n)$ is an abelian group of order $\varphi(n)$, where φ is Euler's phi function. ■

2.4 Subgroups Generated by Subsets of a Group

Exercise 2.4.1 Prove that if H is a subgroup of G then $\langle H\rangle = H$.

Proof. Let G be a group and $H \leq G$. Consider H as a subset of G, and note:

$$\langle H\rangle = \bigcap_{H\subseteq\Theta,\ \Theta\leq G} \Theta$$

Since H was assumed to be a subgroup, and $H \subseteq H$ holds trivially, we may write:

$$\langle H\rangle = (\bigcap_{H\subseteq\Theta,\ \Theta\leq G} \Theta) \cap H = H$$

Which follows since for any such $\Theta \leq G$, if $H \subseteq \Theta$, then $\Theta \cap H = H$. Thus the subgroup of G generated by a subgroup H is the subgroup H itself. ■

Exercise 2.4.2 Prove that if A is a subset of B then $\langle A\rangle \leq \langle B\rangle$. Give an example where $A \subseteq B$ with $A \neq B$ but $\langle A\rangle = \langle B\rangle$.

Proof. Let G be a group, and $A, B \subseteq G$. Suppose A is contained in B. If we have some element $x \in \langle A\rangle$, then $x = a_1^{\epsilon_1}a_2^{\epsilon_2}a_3^{\epsilon_3}\cdots$ for some $a_i \in A$ and $\epsilon_i = \pm 1$ for each i. However, since $A \subseteq B$, each of the a_i also satisfy $a_i \in B$, to which $x \in \langle B\rangle$; hence we have $\langle A\rangle \leq \langle B\rangle$.

For an example where $A \subseteq B$ with $A \neq B$, but $\langle A\rangle = \langle B\rangle$, consider the group D_8. Take $A = \{1, r\}$ and $B = \{1, r, r^2, r^3\}$. Note $A \subseteq B$, and $A \neq B$. However, we clearly have $\langle A\rangle = \langle B\rangle$. ■

Exercise 2.4.3 Prove that if H is an abelian subgroup of a group G then $\langle H, Z(G)\rangle$ is abelian. Give an explicit example of an abelian subgroup of H of a group G such that $\langle H, C_G(H)\rangle$ is not abelian.

Proof. Let G be a group and $H \leq G$ such that H is abelian. Suppose $x, y \in \langle H, Z(G)\rangle$, with $x = a_1^{\epsilon_1}a_2^{\epsilon_2}\cdots a_n^{\epsilon_n}$ for some $n \in \mathbb{Z}$ and $y = b_1^{\epsilon_1}b_2^{\epsilon_2}\cdots b_m^{\epsilon_m}$ for some $m \in \mathbb{Z}$, where each of the $a_i, b_j \in H \cup Z(G)$ for all $1 \leq i \leq n$ and $1 \leq j \leq m$.

Since H is abelian, and elements of $Z(G)$ commute with all $h \in H$, it follows that the elements of any finite product of elements from H and $Z(G)$ commute. Hence we are permitted to write:

$$xy = a_1^{\epsilon_1}a_2^{\epsilon_2}\cdots a_n^{\epsilon_n}b_1^{\epsilon_1}b_2^{\epsilon_2}\cdots b_m^{\epsilon_m} = b_1^{\epsilon_1}b_2^{\epsilon_2}\cdots b_m^{\epsilon_m}a_1^{\epsilon_1}a_2^{\epsilon_2}\cdots a_n^{\epsilon_n} = yx$$

Since each of the a_i commutes with all other $a_{j\neq i}$, and b_i, and identically so with each b_j. This shows that the subgroup $\langle H, Z(G)\rangle$ is abelian. ■

Exercise 2.4.4 Prove that if H is a subgroup of G then H is generated by the set $H \setminus \{1\}$.

Proof. Let G be a group and $H \leq G$. If $H = \{1\}$, then $H \setminus \{1\} = \emptyset$. Note that we have $\langle \emptyset \rangle = \{1\}$, where the identity 1 has been defined as the empty word consisting of elements of H. In this case, we have $\langle H \setminus \{1\} \rangle = H$.

Now assume $H \neq \{1\}$. Note that $\langle H \setminus \{1\} \rangle \subseteq H$ since $H \leq G$. Since H is non-trivial, there exists some $h \in H \setminus \{1\}$ for which $h \neq 1$. However this implies $h^{-1} \in H \setminus \{1\}$. Hence $1 = hh^{-1} \in \langle H \setminus \{1\} \rangle$. But then any $h' \in H$ also satisfies $h' \in \langle H \setminus \{1\} \rangle$, to which $H \subseteq \langle H \setminus \{1\} \rangle$, and hence $\langle H \setminus \{1\} \rangle = H$. ■

Exercise 2.4.5 Prove that the subgrou generated by any two distinct elements of order 2 in S_3 is all of S_3.

Proof. Every transposition clearly has order 2 in S_n, in particular in S_3. Moreover, the only non-transposition elements of S_3 are (1 2 3) and (1 3 2), each of which has order 3. Thus we need only show that any two distinct transpositions generate S_3. This is easy, however, for the only transpositions are (1 2), (2 3), and (1 3). So let $a, b, c \in \{1, 2, 3\}$ with $a \neq b$ and $a \neq c$ and $b \neq c$. Then note that:

$$(a\ b)(a\ b) = (1)$$

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

$$(b\ c) = (b\ c)$$

$$(a\ b)(b\ c) = (a\ c\ b)$$

$$(b\ c)(a\ b) = (a\ b\ c)$$

$$(a\ b)(b\ c)(a\ b) = (a\ c)$$

Hence $\langle (a\ b), (b\ c) \rangle = S_3$ clearly holds. ■

Exercise 2.4.6

Exercise 2.4.7

Exercise 2.4.8

Exercise 2.4.9

Exercise 2.4.10

Exercise 2.4.11

Exercise 2.4.12

Exercise 2.4.13

Exercise 2.4.14 A group H is called *finitely generated* if there is a finite set A such that $H = \langle A \rangle$.
(a) Prove that every finite group is finitely generated.
(b) Prove that $\mathbb{Z}$ is finitely generated.
(c) Prove that every finitely generated subgroup of the additive group $\mathbb{Q}$ is cyclic. [If H is a finitely generated subgroup of $\mathbb{Q}$, show that $H \leq \langle \frac{1}{k} \rangle$ where k is the product of all the denominators which appear in a set of generators for H.]
(d) Prove that $\mathbb{Q}$ is not finitely generated.

Proof. (a) If G is a finite group then $G = \langle G \rangle$ is a finite set of generators for G.

(b) It is clear that $\mathbb{Z} = \langle 1 \rangle$ since any $n \in \mathbb{Z}^+$ may be writen $n = \sum_{i=1}^{n} 1$ and similarly we may write $-n = \sum_{i=1}^{n}(-1)$.

(c) Suppose H is a finitely generated subgroup of $\mathbb{Q}$, say with $H = \langle q_1, \ldots, q_n \rangle$ with $q_i \in \mathbb{Q}$ for each $i \in \{1, \ldots, n\}$. We may write $q_i = a_i/b_i$ for each i, with all of the $b_i \neq 0$, and a_i, b_i integers. Let $k = b_1 \cdots b_n$. We claim that:

$$H = \langle \frac{1}{b_1 \cdots b_n} \rangle = \langle \frac{1}{k} \rangle$$

Note that if $m \in H$ then $m = \sum_{i=1}^{n} q_i$ and hence

$$m = \frac{a_1}{b_1} + \cdots + \frac{a_n}{b_n}$$

Multiplying both sides of the above equation by $b_1 \cdots b_n$ yields:

$$(b_1 \cdots b_n)m = a_1 b_2 \cdots b_n + a_2 b_1 b_3 \cdots b_n + \cdots + a_n b_1 \cdots b_{n-1}$$

Dividing now by $b_1 \cdots b_n$ gives us:

$$m = \left(\frac{1}{b_1 \cdots b_n} \right) (a_1 b_2 \cdots b_n + a_2 b_1 b_3 \cdots b_n + \cdots + a_n b_1 \cdots b_{n-1})$$

In particular, we have written m as a sum of $1/k$, hence $m \in \langle 1/k \rangle$; since $m \in H$ was arbitrary, this suffices to show that $H \subseteq \langle 1/k \rangle$, and since the reverse inclusion is trivial, we have set equality; hence $H = \langle 1/k \rangle$ is cyclic.

(d) If we assume $\mathbb{Q}$ is finitely generated, then since $\mathbb{Q}$ is a subgroup of $\mathbb{Q}$, we may refer to part (c) above to write that $\mathbb{Q}$ is cyclic, say with generator a/b. Note, however, that this would imply $n(a/b) = 0/1$ for some $n \in \mathbb{Z}^+$, and hence that $na = 0$, hence that $a = 0$ since n is positive. Clearly, however, $0/b$ does not generate $\mathbb{Q}$, for instance since no sum of $0/b$ is equal to $1/1 = 1$; this is a contradiction, so that $\mathbb{Q}$ is certainly not finitely generated. ■

Exercise 2.4.15 Exhibit a proper subgroup of $\mathbb{Q}$ which is not cyclic.

Proof. Consider the following subset of $\mathbb{Q}$:

$$\mathbb{Z}_{(2)} = \{a/b \mid a, b \in \mathbb{Z}, b \neq 0, 2 \nmid b\}$$

We first show that $\mathbb{Z}_{(2)}$ is a subgroup of $\mathbb{Q}$. Observe that if $a/b, c/d \in \mathbb{Z}_{(2)}$ we have that $2 \nmid b, d$, and hence $2 \nmid bd$. In particular, we have:

$$\frac{a}{b} - \frac{c}{d} = \frac{ad - bc}{bd} \in \mathbb{Z}_{(2)}$$

since clearly $ad - bc \in \mathbb{Z}$ and $bd \in \mathbb{Z} \setminus \{0\}$ since $b, d \neq 0$. This shows that $\mathbb{Z}_{(2)}$ is a subgroup of $\mathbb{Q}$ by the subgroup criterion. If $\mathbb{Z}_{(2)}$ was cyclic, say with generator a/b, then since $0/1 \in \mathbb{Z}_{(2)}$ since $2 \nmid 1$, we would require that there exist $n \in \mathbb{Z}^+$ such that:

$$n\left(\frac{a}{b}\right) = \frac{0}{1} \iff \frac{a}{b} + \cdots + \frac{a}{b} = \frac{na}{b} = \frac{0}{1} \iff na = 0$$

and of course one of n or a must be zero; hence $a = 0$; but clearly $0/b$ does not generate $\mathbb{Z}_{(2)}$, since for instance $1 \in \mathbb{Z}_{(2)}$ and no sum of $0/b$ will equal 1. Moreover, $\mathbb{Z}_{(2)}$ is proper since $1/2 \notin \mathbb{Z}_{(2)}$. ■

Exercise 2.4.16

Exercise 2.4.17

Exercise 2.4.18

Exercise 2.4.19 A nontrivial abelian group A is called divisible if for each element $a \in A$ and each nonzero integer k there is an element $x \in A$ such that $x^k = a$.
a.) Prove that the additive group of rational numbers, $\mathbb{Q}$, is divisible.
b.) Prove that no finite abelian group is divisible.

Proof. (a) Consider the additive group $\mathbb{Q}$. Let $q \in \mathbb{Q}$ be arbitrary. Then we may write:

$$q = \frac{a}{b}$$

Where $a, b \in \mathbb{Z}$ and $b \neq 0$. Written in additive notation, we may consider the element $1/b \in \mathbb{Q}$ and write that adding $1/b$ to itself a times grants:

$$\sum_{i=1}^{a} \frac{1}{b} = \frac{1}{b} + \cdots + \frac{1}{b} = \frac{a}{b}$$

Equivalently in multiplicative notation, we have $(1/b)^a = a/b = q$. This shows that any element in $\mathbb{Q}$ has a kth root in $\mathbb{Q}$, so that $\mathbb{Q}$ is by definition a divisible group.

(b) Let A be an arbitrary finite abelian group. Assume, for contradiction, that A is divisible. Let $|A| = k$. By definition of a divisible group, $A \neq \{1\}$, so we may pick $a \in A$ for which $a \neq 1$. We know that there exists an element $x \in A$ for which $x^k = a$. Let $|x| = n$. Lagrange's Theorem states that $|x| \mid |G|$, or $n \mid k$, to which $k = nm$ for some $m \in \mathbb{Z}$. Note:

$$x^k = a \iff x^{nm} = a \iff (x^n)^m = 1^m = 1 = a$$

And so we must have $a = 1$, which is a contradiction since we assumed that $a \neq 1$. Therefore no such finite abelian group A is divisible. ■

Exercise 2.4.20 Prove that if A and B are nontrivial abelian groups, then $A \times B$ is divisible if and only if both A and B are divisible groups.

Proof. Let A and B be non-trivial abelian groups. Suppose $A \times B$ is divisible. Then for any element $(a, b) \in A \times B$, and each $k \in \mathbb{Z} \setminus \{0\}$, we can be assured that there exists an element $(x, y) \in A \times B$ for which:

$$(a, b) = (x, y)^k \iff (a, b) = (x^k, y^k)$$

In particular, if and only if we have $a = x^k$ and $b = y^k$, where $a, x \in A$ and $b, y \in B$, i.e., both A and B are divisible groups. This suffices to show both directions of the implication and so we are done. ■

2.5 The Lattice of Subgroups of a Group

Exercise 2.5.1

Exercise 2.5.1

Exercise 2.5.1

Exercise 2.5.1

Exercise 2.5.1

Exercise 2.5.1

Exercise 2.5.1

Exercise 2.5.1

Exercise 2.5.1

Exercise 2.5.1

❈ Quotient Groups and Homomorphisms

3.1 Definitions and Examples

Exercise 3.1.1 Let $\varphi : G \to H$ be a homomorphism and let E be a subgroup of H. Prove that $\varphi^{-1}(E) \leq G$. Deduce that $\ker \varphi \leq G$.

Proof. Let $\varphi : G \to H$ be a group homomorphism, and $E \leq H$. Consider the preimage of E under φ, the set $\varphi^{-1}(E)$. Since $E \leq H$, we must have $\varphi(1_G) = 1_H \in E$, to which $1 \in \varphi^{-1}(E)$, so that $\varphi^{-1}(E) \neq \emptyset$. Now suppose $x, y \in \varphi^{-1}(E)$, so by construction of the preimage we have $\varphi(x), \varphi(y) \in E$. Since E is closed under products and inverses, it follows that:

$$\varphi(x)\varphi(y)^{-1} \in E$$

But since φ is a homomorphism, the above is equivalent to the following expression:

$$\varphi(xy^{-1}) \in E$$

These two facts suffice to show that $\varphi^{-1}(E) \leq G$ by the subgroup criterion.

Taking $E = \{1\}$, the trivial subgroup of H, and referring to the result above, we find that $\varphi^{-1}(E) = \varphi^{-1}(\{1\}) \leq G$, but note:

$$\varphi^{-1}(\{1\}) = \{g \in G \mid \varphi(g) = 1\} = \ker \varphi$$

And so we trivially recover that $\ker \varphi \leq G$. ■

Exercise 3.1.2 Let $\varphi : G \to H$ be a homomorphism of groups with kernel K and let $a, b \in \varphi(G)$. Let $X \in G/K$ be the fiber above a and let Y be the fiber above b. Fix an element u of X. Prove that if $XY = Z$ in the quotient group G/K and w is any member of Z, then there is some $v \in Y$ such that $uv = w$.

Proof. Let $\varphi : G \to H$ be a group homomorphism with $\ker \varphi = K$. Let $a, b \in \varphi(G)$, $X = \varphi^{-1}(a)$, and $Y = \varphi^{-1}(b)$. Fix $u \in X$. Suppose we have $XY = Z$, for some $Z \in G/K$. Let $w \in Z$. We know from Proposition 2(1) that:

$$X = \{uk \mid k \in K\} = uK$$

Similarly for Z, we may rewrite the above with w instead of u, $Z = wK$. Therefore, we may rewrite the equation $XY = Z$ as:

$$uK \cdot Y = wK \implies Y = u^{-1}K \cdot wK \implies Y = u^{-1}wK$$

Which follows from Proposition 5(1). We then have $u^{-1}w \in Y$. Let v denote $u^{-1}w$. Then $v = u^{-1}w \implies uv = w$, which is the desired relation. ■

Exercise 3.1.3 Let A be an abelian group and let B be a subgroup of A. Prove that A/B is abelian. Give an example of a non-abelian group G containing a proper normal subgroup N such that G/N is abelian.

Proof. Let A be an abelian group, and $B \leq A$. Any subgroup of an abelian group is normal, and so $B \trianglelefteq A$, to which A/B is a group by Theorem 6(1). Let $xB, yB \in A/B$. Then:

$$xByB = xyB = (xy)B = (yx)B = yxB = yBxB$$

Which follows since $xy = yx$ for all $x, y \in A$, since A is abelian, and the operation carried out in the parentheses above is carried out in A. This suffices to show that A/B is abelian.

For an example, take $G = Q_8$, which is a non-abelian group. Take $N = \langle \pm 1 \rangle$, where N is a proper subgroup of Q_8, and in particular is normal in Q_8 as per the discussion in the text; i.e., since $Z(Q_8) = \langle \pm 1 \rangle$. We saw that $Q_8/\langle \pm 1 \rangle \cong V_4$, and clearly the Klein 4-group, V_4, is abelian, to which $Q_8/\langle \pm 1 \rangle$ is abelian. ■

Exercise 3.1.4 Prove that in the quotient group G/N, $(gN)^\alpha = g^\alpha N$ for all $\alpha \in \mathbb{Z}$.

Proof. Let G/N be a quotient group, and $\alpha \in \mathbb{Z}$ arbitrary. Now note that:

$$(gN)^\alpha = \prod_{i=1}^{\alpha} gN = (\prod_{i=1}^{\alpha} g)N = g^\alpha N$$

Which follows from the results of Proposition 5(1-2). ■

Exercise 3.1.5 Use the preceding exercise to prove that the order of the element gN in G/N is n, where n is the smallest positive integer such that $g^n \in N$. Give an example to show that the order of gN in G/N may be strictly smaller than the order of g in G.

Proof. Let n be the smallest positive integer for which $g^n \in N$. We would like to show that $|gN| = n$. Note that in [[DF-3.1-4]] we saw $(gN)^n = g^n N = N$, since $g^n \in N$; hence we may write that $|gN| \leq n$. Assume, for contradiction, that $|gN| < n$. Then there is some $m < n$ such that $m \in \mathbb{Z}^+$ and $(gN)^m = N$. But note:

$$(gN)^m = g^m N \neq N$$

Which follows since $g^m \notin N$, for we assumed that n was the smallest positive integer for which $g^n \in N$. Thus $|gN| \geq n$, to wich we may write $|gN| = n$. In the case where no such n exists in our hypothesis, it follows that no positive integer exists such that $g^n \in N$, to which we may never have $(gN)^n = N$, and so $|gN| = \infty$.

For the desired example, take $G = D_8$ and $N = \langle r^2 \rangle$. We have seen before that $\langle r^2 \rangle \trianglelefteq D_8$, to which $D_8/\langle r^2 \rangle$ is a group. Consider the coset with representative r.

Note that $r\langle r^2\rangle = \{r, r^3\}$. As we saw in the proof above, the order of $r\langle r^2\rangle$ is n, where n is the smallest positive integer for which $r^n \in \langle r^2\rangle$. We can immediately see that $n = 2$ in this case, to which $|r\langle r^2\rangle| = 2$. However in the ambient group D_8, we know that $|r| = 4$. Thus we have the order of $r\langle r^2\rangle$ strictly less than the order of r as desired. ■

Exercise 3.1.6 Define $\varphi : \mathbb{R}^\times \to \{\pm 1\}$ by letting $\varphi(x)$ be x divided by the absolute value of x. Describe the fibers of φ and prove that φ is a homomorphism.

Proof. Define $\varphi : \mathbb{R}^\times \to \{\pm 1\}$ by $\varphi(x) = x/|x|$. The fibers of φ are:

$$\varphi^{-1}(1) = \{x \in \mathbb{R}^\times \mid x/|x| = 1\} = \{x \in \mathbb{R}^\times \mid x > 0\} = \mathbb{R}_{>0}$$

And:

$$\varphi^{-1}(-1) = \{x \in \mathbb{R}^\times \mid x/|x| = -1\} = \{x \in \mathbb{R}^\times \mid x < 0\} = \mathbb{R}_{<0}$$

In other words, φ distinguishes positive and negative nonzero real numbers. Let $x, y \in \mathbb{R}^\times$. Then:

$$\varphi(xy) = \frac{xy}{|xy|} = \frac{x}{|x|} \cdot \frac{y}{|y|} = \varphi(x)\varphi(y)$$

To which φ is a homomorphism from $\mathbb{R}^\times$ to $\{\pm 1\}$. ■

Exercise 3.1.7

Exercise 3.1.8

Exercise 3.1.9

Exercise 3.1.10

Exercise 3.1.11

Exercise 3.1.12

Exercise 3.1.13

Exercise 3.1.14

Exercise 3.1.15

Exercise 3.1.16

Exercise 3.1.17

Exercise 3.1.18

Exercise 3.1.19

Exercise 3.1.20

Exercise 3.1.21

Exercise 3.1.22

Exercise 3.1.23

Exercise 3.1.24 Prove that if $N \trianglelefteq G$ and H is any subgroup of G then $N \cap H \trianglelefteq H$.

Proof. Let G be a group $H \leq G$. Suppose $N \trianglelefteq G$. We know that the intersection of two subgroups of G is again a subgroup of G, so $N \cap H \leq G$, and furthermore we know that $N \cap H \subseteq H$, to which $N \cap H \leq H$ follows.

To prove normality, let $x \in H$ be arbitrary. Then xkx^{-1} where $k \in N \cap H$, in particular $k \in N$ and $k \in H$, and since we assumed $x \in H$, we have closure under products and inverses and so $xkx^{-1} \in H$. But this means $xN \cap Hx^{-1} \subseteq N \cap H$ for any $x \in H$, which by Theorem 6(5) is sufficient condition for $N \cap H \trianglelefteq H$. ∎

Exercise 3.1.25

Exercise 3.1.26

Exercise 3.1.27 Let N be a finite subgroup of a group G. Show that $gNg^{-1} \subseteq N$ if and only if $gNg^{-1} = N$. Deduce that $N_G(N) = \{g \in G \mid gNg^{-1} \subseteq N\}$.

Proof. Let G be a group and $N \leq G$ such that N is finite. Let $g \in G$ and suppose $gNg^{-1} \subseteq N$. Let $n \in N$. Since N is a subgroup, there exists an inverse $n^{-1} \in N$. By assumption, we have $gn^{-1}g^{-1} = k$ for some $k \in N$. Observe:

$$gn^{-1}g^{-1} = k \iff gn^{-1}g^{-1}k^{-1} = 1 \iff k^{-1} = gng^{-1}$$

And clearly $k^{-1} \in N$ since N is closed under inverses. In particular, the above shows that $n \in gNg^{-1}$, and so we have shown $N \subseteq gNg^{-1}$, to which $gNg^{-1} = N$. For the converse statement, suppose we have $gNg^{-1} = N$. It is then trivially the case that $gNg^{-1} \subseteq N$, and so we are done. ∎

Exercise 3.1.28

Exercise 3.1.29

Exercise 3.1.30

Exercise 3.1.31

Exercise 3.1.32

Exercise 3.1.33

Exercise 3.1.34

Exercise 3.1.35

Exercise 3.1.36 Prove that if $G/Z(G)$ is cyclic then G is abelian.

Proof. Let G be a group. Suppose $G/Z(G)$ is cyclic. Let $x \in G$ and $G/Z(G) = \langle xZ(G) \rangle$. Take an arbitrary $g \in G$. Then since the left cosets of $Z(G)$ in G partition G, we may write $g \in gZ(G)$, i.e., g is in some left coset. By assumption:

$$gZ(G) = (xZ(G))^{\alpha} = x^{\alpha}Z(G)$$

for some $\alpha \in \mathbb{Z}$. But note that the above occurs if and only if:

$$x^{-\alpha}gZ(G) = Z(G) \iff x^{-\alpha}g \in Z(G)$$

However, then we may write:

$$g = 1 \cdot g = x^{\alpha-\alpha}g = x^{\alpha}(x^{-\alpha}g) \iff g = x^{\alpha}z$$

Where $z = x^{-\alpha}g \in Z(G)$. This means we may write any element of G as a product of some power of x and some element in $Z(G)$. But then if we have another element $h \in G$ such that $h \neq g$, we may write $h = x^{\beta}w$ for some $w \in Z(G)$ and $\beta \in \mathbb{Z}$ as well. Then:

$$gh = x^{\alpha}zx^{\beta}w = x^{\alpha}zwx^{\beta} = x^{\alpha}wzx^{\beta} = x^{\alpha}wx^{\beta}z = wx^{\alpha+\beta}z = wx^{\beta+\alpha}z =$$

$$= x^{\beta}wx^{\alpha}z = hg$$

Which follows since $z, w \in Z(G)$ and so commute with all elements of G, and x^{α}, x^{β} both commute as powers of x. Hence, we have shown G is abelian. ∎

Exercise 3.1.37

Exercise 3.1.38

Exercise 3.1.39

Exercise 3.1.40 Let G be a group, let N be a normal subgroup of G and let $\overline{G} = G/N$. Prove that $\overline{x}$ and $\overline{y}$ commute in $\overline{G}$ if and only if $x^{-1}y^{-1}xy \in N$.

Proof. Let G be a group and $N \trianglelefteq G$. Then $\overline{G} = G/N$ is a group. Suppose $\overline{x}$ and $\overline{y}$ commtue in $\overline{G}$, i.e., we have $\overline{xy} = \overline{yx}$. Equivalently:

$$xNyN = yNxN \iff xyN = yxN \iff x^{-1}y^{-1}xyN = N \iff x^{-1}y^{-1}xy \in N$$

Where the above manipulations follow from Proposition 5(1) and 5(2), in addition to Theorem 4(5). In particular, this shows the proof in both directions and so we are done. ∎

Exercise 3.1.41 Let G be a group. Prove that $N = \langle x^{-1}y^{-1}xy \mid x, y \in G\rangle$ is a normal subgroup of G and G/N is abelian. (N is called the commutator of G).

Proof. Let G be a group and $N = \langle x^{-1}y^{-1}xy \mid x, y \in G\rangle$. We know that N is a subgroup of G, for N is the subgroup generated by elements of the form $x^{-1}y^{-1}xy$ for any $x, y \in G$. To show $N \trianglelefteq G$, let $x \in N$. Take an arbitrary $g \in G$. Note that $x^{-1}g^{-1}xg \in N$ by construction. Since N is a subgroup, it is closed under products, to which:

$$x \cdot x^{-1}g^{-1}xg = g^{-1}xg \in N$$

Which is equivalent to $gxg^{-1} \in N$, and so $gNg^{-1} \subseteq N$ for all $g \in G$, which by Theorem 6(5) allows us to write that $N \trianglelefteq G$.

Given the above, we know that G/N is a group. To show that G/N is abelian, note that by [[DF-3.1-40]], if $x^{-1}y^{-1}xy \in N$ then $xNyN = yNxN$. But in our above construction, we trivially have $x^{-1}y^{-1}xy \in N$ for any $x, y \in G$, to which any $xNyN = yNxN$ and so the quotient group G/N is abelian. ■

Exercise 3.1.42 Assume both H and K are normal subgroups of G with $H \cap K = 1$. Prove that $xy = yx$ for all $x \in H$ and $y \in K$.

Proof. Let G be a group and suppose $H, K \trianglelefteq G$ such that $H \cap K = \{1\}$. Let $x \in H$ and $y \in K$ such that $x, y \neq 1$. By closure of subgroups, $x^{-1} \in H$ and $y^{-1} \in K$. Since $gHg^{-1} \subseteq H$ for all $g \in G$ by Theorem 6(5), we may take $g = y^{-1}$ and note that $y^{-1}xy \in H$. Clearly then the product of x^{-1} and $y^{-1}xy$ will be an element of H also, i.e., we have $x^{-1}y^{-1}xy \in H$.

But note that we also have $gKg^{-1} \subseteq K$ for all $g \in G$, and so take $g = x^{-1}$ and repeat the above to find that we must have $x^{-1}y^{-1}xy \in K$. However, this mea ■

Exercise 3.1.43 Assume $\mathcal{P} = \{A_i \mid i \in I\}$ is any partition of G with the property that $\mathcal{P}$ is a group under the "quotient operation" defined as follows: to compute the product of A_i with A_j take any element a_i of A_i and let A_iA_j be the element of $\mathcal{P}$ containing a_ia_j (this operation is assumed to be well-defined). Prove that the element of $\mathcal{P}$ that contains the identity of G is a normal subgroup of G and the elements of $\mathcal{P}$ are the cosets of this subgroup (so $\mathcal{P}$ is just a quotient group of G in the usual sense).

Proof. Let G be a group and take $\mathcal{P} = \{A_i \mid i \in I\}$ a partition of G such that $\mathcal{P}$ is a group under the "quotient operation" defined in the problem. Since $\mathcal{P}$ is a partition of G, one set A_j contains the identity of G. Let $A_i \in \mathcal{P}$ be such a subset.

First we will show that A_i must be a subgroup of G. Clearly $A_i \subseteq G$. If $1 \in A_i$ is the only element of A_i, then A_i is the trivial subgroup. So let $x \in A_i$ such that

$x \neq 1$. If we had $x^{-1} \in A_j \neq A_i$, then:

$$x^{-1} \cdot x \in A_j A_i$$

But we know that $x^{-1} \cdot x = 1 \in A_i$. This means that $A_j A_i = A_i$, to which $x^{-1} \in A_i$. Thus A_i is closed under inverses. Now let $y \in A_i$. By the definition of the operation in the problem, we know:

$$x \cdot y \in A_i A_i = A_i$$

And so A_i is closed under products also. Therefore $A_i \leq G$. Now we will show that $A_i \trianglelefteq G$. Take any $g \in G$, which is contained in some $A_j \in \mathcal{P}$. Then:

$$g = g \cdot 1 \in A_j A_i$$

But also we have:

$$g = 1 \cdot g \in A_i A_j$$

And since $\mathcal{P}$ is a partition of G, it follows that $A_i A_j \cap A_j A_i = \emptyset$. But since $g \in A_i A_j \cap A_j A_i$, we know that $A_i A_j \cap A_j A_i \neq \emptyset$. Thus it must be the case that $A_i A_j = A_j A_i$. In particular, this means that $g A_i = A_i g$ for all $g \in G$. By Theorem 6(3), this is equivalent to $A_i \trianglelefteq G$.

Now we will show that the elements of $\mathcal{P}$ are simply the cosets of this subgroup. By Proposition 4, the cosets of A_i in G form a partition of G, which is $\mathcal{P}$. We have also have, for some $A_j, A_k \in \mathcal{P}$, the following:

$$A_j A_i = A_k A_i \iff A_j = A_k$$

Which follows since $A_j \cap A_k = \emptyset$ for all $j \neq k$ since $\mathcal{P}$ is a partition of G. Essentially, if $u \in A_j$ and $v \in A_k$ are two representatives satisfying the above, then it must be the case that $A_j = A_k$, i.e., u and v are both in one subset. This suffices to show that each element of $\mathcal{P}$ is simply a coset of A_i in G. ■

3.2 More on Cosets and Lagrange's Theorem

Exercise 3.2.1 Which of the following are permissible orders for subgroups of a group of order 120: 1, 2, 5, 7, 9, 15, 60, 240? For each permissible order give the corresponding index.

Proof. We know that $120 = 2^3 \cdot 3 \cdot 5$, and that by Lagrange's Theorem, a subgroup of a group with order 120 must have its order a positive divisor of 120. Note that the divisors of 120 are: 1, 2, 5, 6, 8, 10, 12, 15, 24, 48, 60, and 120. Therefore we may write that 1, 2, 5, 15, and 60 are all possible orders from the problem. In order, we have index 120, index 60, index 25, index 8, and index 2. ∎

Exercise 3.2.2

Exercise 3.2.3

Exercise 3.2.4 Show that if $|G| = pq$ for some primes p and q not necessarily distinct, then either G is abelian or $Z(G) = 1$.

Proof. Let G be a group such that $|G| = pq$. We will first consider the case where $p = q$, i.e., the case where $|G| = p^2$. In this case, consider the center of G, the subgroup $Z(G)$, which we know to be a normal subgroup of G. Since $Z(G) \trianglelefteq G$, then we know $G/Z(G)$ is a subgroup of G, and so by Lagrange's Theorem, we have $|G/Z(G)| \mid p^2$. Since p is a prime, we may have $|G/Z(G)| = 1, p$, or p^2. If $|G/Z(G)| = 1$, then it must be the case that $G = Z(G)$, to which G is abelian. If $|G/Z(G)| = p$, then we know by Corollary 10 that $G/Z(G) \cong Z_p$. By [[DF-3.1-36]]. this fact implies that G is abelian. Finally, if $|G/Z(G)| = p^2$, then $G = G/Z(G)$ and so $Z(G) = 1$.

Alternatively, consider the case where $p \neq q$. By Theorem 12, Sylow's Theorem, since $p \nmid q$ and since both p and q are prime, we may write that there exist $P, Q \leq G$ for which $|P| = p$ and $|Q| = q$. Then by Proposition 13:

$$|PQ| = \frac{|P| \cdot |Q|}{|P \cap Q|} \leq pq$$

But note that if $x \in P \cap Q$, it must be the case that $|x| \mid p$ and $|x| \mid q$ by Lagrange's Theorem, and since we have $p \nmid q$ and $q \nmid p$, it follows that $|x| = 1$ is required, to which $P \cap Q = \{1\}$. Thus the above shows $|PQ| = |G|$, and so $G = PQ$. In particular, we have PQ is a group, and so Proposition 14 states $PQ = QP$.

Given the above, note that since $|P| = p$ and $|Q| = q$ both primes, Corollary 10 provides us with $P \cong Z_p$ and $Q \cong Z_q$. So let $P = \langle x \rangle$ and $Q = \langle y \rangle$. Then if

$g, h \in G$, since $G = PQ$, we may write $g = x^a y^b$ and $h = x^{a'} y^{b'}$ for appropriately chosen indices $1 \le a, a' \le p$ and $1 \le b, b' \le q$. Then:

$$gh = x^a y^b x^{a'} y^{b'} = x^a x^{a'} y^b y^{b'} = x^{a+a'} y^{b+b'} = x^{a'} y^{b'} x^a y^b = hg$$

Which follows since $PQ = QP$ as we saw above, so that any x^a and y^b commute. The above shows that G is an abelian group. ∎

Exercise 3.2.5 Let H be a subgroup of G and fix some element $g \in G$.
a.) Prove that gHg^{-1} is a subgroup of G of the same order as H.
b.) Deduce that if $n \in \mathbb{Z}^+$ and H is the unique subgroup of G of order n, then $H \trianglelefteq G$.

Proof. (a) Let $H \le G$ and fix $g \in G$. Consider the set $gHg^{-1} \subseteq G$. Note that since $1 \in H$, we trivially have $g \cdot 1 \cdot g^{-1} = gg^{-1} = 1 \in gHg^{-1}$ which implies $gHg^{-1} \neq \emptyset$. Now suppose $x, y \in gHg^{-1}$. Then $x = ghg^{-1}$ and $y = gkg^{-1}$ for $h, k \in H$. Now:

$$xy^{-1} = ghg^{-1}(gkg^{-1})^{-1} = ghg^{-1}gk^{-1}g = ghk^{-1}g^{-1}$$

Since $H \le G$, H is closed under products and inverses, and so $h, k \in H$ implies $hk^{-1} \in H$, which given the above shows $xy^{-1} \in gHg^{-1}$. By the subgroup criterion, we may write $gHg^{-1} \le G$.

Now construct a map $\varphi : H \to gHg^{-1}$. We will show that φ is a bijection. First, if we have $x \in gHg^{-1}$, then clearly $x = ghg^{-1}$ for some $h \in H$, to which $\varphi(h) = x$ and so φ is surjective. Additionally, if $ghg^{-1} = gkg^{-1}$, then clearly we may multiply the inverse of g ont he right and g on the left to obtain $h = k$, to which φ is injective; hence a bijection to which $|H| = |gHg^{-1}|$ as desired.

(b) Now let $n \in \mathbb{Z}^+$ and suppose H is the unique subgroup of G of order n. By part (a) above, we know $gHg^{-1} \le G$ and $|H| = |gHg^{-1}| = n$. But since we assumed H was unique, it follows that $H = gHg^{-1}$ which implies $Hg = gH$, which is equivalent to $H \trianglelefteq G$. ∎

Exercise 3.2.6 Let $H \le G$ and let $g \in G$. Prove that if the right coset Hg equals some left coset of H in G then it equals the left coset gH and g must be in $N_G(H)$.

Proof. Let G be a group and $H \le G$. Take $g \in G$ and suppose $Hg = xH$, with $x \in G$, i.e., for some left coset of H in G. Then:

$$Hg = xH \iff x^{-1}Hg = H \iff x^{-1}g \in H$$

Where the final part above follows since $1 \in H$. Now, since we took xH as a coset of H in G, and we showed above that $x^{-1}g \in H$, we may write:

$$x(x^{-1}g) = xx^{-1}g = g \in xH$$

But then $g \in xH$ implies that $xH = gH$, to which $Hg = gH$, equivalently $H = gHg^{-1}$, the definition of $g \in N_G(H)$. ∎

Exercise 3.2.7 Let $H \leq G$ and define a relation $\sim$ on G by $a \sim b$ if and only if $b^{-1}a \in H$. Prove that $\sim$ is an equivalence relation and describe the equivalence class of each $a \in G$. Use this to prove Proposition 4.

Proof. Let G be a group and $H \leq G$. Take $\sim$ as defined in the problem description. First, take $a \in G$. Then we know that $a^{-1}a = 1 \in H$, to which $a \sim a$, and so the relation is reflexive.

Now take $b \in G$. Suppose $a \sim b$. Then $b^{-1}a \in H$, and since H is closed under inverses, it follows that $(b^{-1}a)^{-1} = a^{-1}(b^{-1})^{-1} = a^{-1}b \in H$; hence $b \sim a$. Thus the relation is symmetric.

Now take $c \in G$ also. Suppose $a \sim b$ and $b \sim c$. Then $b^{-1}a, c^{-1}b \in H$. Since H is closed under products, we know:

$$(c^{-1}b)(b^{-1}a) = c^{-1}bb^{-1}a = c^{-1}a \in H$$

And so $a \sim c$. Thus the relation is transitive, and so is an equivalence relation on G. The equivalence class of any $a \in G$ is as follows:

$$[a]_\sim = \{g \in G \mid g^{-1}a \in H\} = \{g \in G \mid aH = gH\} = aH$$

i.e., the equivalence class is precisely the left coset of H in G that contains a. ■

Exercise 3.2.8 Prove that if H and K are finite subgroups of G whose orders are relatively prime, then $H \cap K = 1$.

Proof. Let G be a group and $H, K \leq G$ be finite subgroups. Suppose the orders of H and K are relatively prime. Let $|H| = n$ and $|K| = m$. We know that the set $H \cap K$ is a subgroup of both H and K. By Lagrange's Theorem, we have $|H \cap K| \mid n$ and $|H \cap K| \mid m$. But then $|H \cap K|$ is a common divisor of n and m, and since we assumed the greatest common divisor of n and m was 1, it follows that $|H \cap K| = 1$. This is equivalent to $H \cap K = \{1\}$ as desired. ■

Exercise 3.2.9

Exercise 3.2.10

Exercise 3.2.11

Exercise 3.2.12

Exercise 3.2.13

Exercise 3.2.14

Exercise 3.2.15

Exercise 3.2.16 Use Lagrange's Theorem in the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^\times$ to prove Fermat's Little Theorem: if p is a prime then $a^p \equiv a \mod p$ for all $a \in \mathbb{Z}$.

Proof. Let $a \in \mathbb{Z}$ be arbitrary, and consider the group $(\mathbb{Z}/p\mathbb{Z})^\times$, with p a prime. If $a = p$, then we know $p^p \equiv p \mod p$ holds trivially, so assume $a \neq p$. Since p is a prime, we must have $\gcd(a, p) = 1$. This is a sufficient condition for $\overline{a} \in (\mathbb{Z}/p\mathbb{Z})^\times$. By Corollary 9, we know that:

$$\overline{a}^{|(\mathbb{Z}/p\mathbb{Z})^\times|} = 1 \implies \overline{a}^{\varphi(p)} = \overline{a}^{p-1} = 1$$

Where φ is Euler's phi-function, and $\varphi(p) = p - 1$ follows since p is prime. But note that:

$$\overline{a}^{p-1} = 1 \iff \overline{a}^p\overline{a}^{-1} = 1 \iff \overline{a}^p = \overline{a}$$

Note that in $(\mathbb{Z}/p\mathbb{Z})^\times$, equality is equivalent to congruence modulo p. Given this, the above implies:

$$a^p \equiv a \mod p$$

Which is the desired relation. This suffices to prove Fermat's Little Theorem. ∎

Exercise 3.2.17

Exercise 3.2.18

Exercise 3.2.19

Exercise 3.2.20

Exercise 3.2.21

Exercise 3.2.22

Exercise 3.2.23

3.3 The Isomorphism Theorems

3.4 Composition Series and the HÃűlder Program

Exercise 3.4.1 Prove that if G is an abelian simple group then $G \cong Z_p$ for some prime p (do not assume that G is finite).

Proof. Suppose G is a simple abelian group. In an abelian group, all subgroups are normal, and since G is simple, this implies that the only subgroups of G are thus 1 and G itself. Assume $G \neq 1$. Then there exists some non-identity element $x \in G$. We have $\langle x \rangle \leq G$ always, and since $\langle x \rangle$ is a subgroup of G either we have $G = \langle x \rangle$ or $\langle x \rangle = 1$. Since $x \neq 1$, we have $\langle x \rangle \neq 1$, and so $\langle x \rangle = G$ must hold, to which G is cyclic.

There are two cases: either $|G| = n < \infty$ or $|G| = \infty$. If G is infinite, then clearly $|x| = \infty$ since G is generated by x. From Proposition 6(1) in Chapter 2 Section 3, we know that $G = \langle x^a \rangle$ if and only if $a = \pm 1$. However, note that for any $m \neq \pm 1$, we have $\langle x^m \rangle \leq G$, and since there are no non-trivial subgroups, this forces $\langle x^m \rangle = G$, so that $m = \pm 1$, a contradiction.

Thus $|G| = n < \infty$ for some $n \in \mathbb{Z}^+$. Once more, we have that $\langle x^m \rangle = G$ for any $m \in \mathbb{Z}^+$, and by Proposition 6(2) in Chapter 2 Section 3, this means that $\gcd(m, n) = 1$. In particular, n is a positive integer relatively prime to all other positive integers except 1, and so must be a prime, $n = p$, for some prime p. Thus $G \cong Z_p$, which was the desired statement. ■

Exercise 3.4.2 Exhibit all 3 composition series for Q_8 and all 7 composition series for D_8. List the composition factors in each case.

Proof. Take Q_8. The three composition series for Q_8 are as follows:

$$1 \leq \langle -1 \rangle \leq \langle -i \rangle \leq Q_8$$

Where the composition factors are $\langle -1 \rangle$, $\langle -i \rangle / \langle -1 \rangle$, and $Q_8 / \langle -i \rangle$. Then:

$$1 \leq \langle -1 \rangle \leq \langle -j \rangle \leq Q_8$$

Where the composition factors are $\langle -1 \rangle$, $\langle -j \rangle / \langle -1 \rangle$, and $Q_8 / \langle -j \rangle$. Finally:

$$1 \leq \langle -1 \rangle \leq \langle -k \rangle \leq Q_8$$

Where the composition factors are $\langle -1 \rangle$, $\langle -k \rangle / \langle -1 \rangle$, and $Q_8 / \langle -k \rangle$.

Now take D_8. The first of the seven composition series for D_8 is:

$$1 \leq \langle s \rangle \leq \langle s, r^2 \rangle \leq D_8$$

With composition factors $\langle s \rangle$, $\langle s, r^2 \rangle / \langle s \rangle$, and $D_8 / \langle s, r^2 \rangle$. The next is:

$$1 \leq \langle r^2 \rangle \leq \langle r \rangle \leq D_8$$

With composition factors $\langle r^2 \rangle$, $\langle r \rangle / \langle r^2 \rangle$, and $D_8 / \langle r \rangle$. Third, we have:

$$1 \leq \langle r^2 \rangle \leq \langle s, r^2 \rangle \leq D_8$$

With composition factors $\langle r^2 \rangle$, $\langle s, r^2 \rangle / \langle r^2 \rangle$, and $D_8 / \langle s, r^2 \rangle$. Fourth, we have:

$$1 \leq \langle sr \rangle \leq \langle sr, sr^3 \rangle \leq D_8$$

With composition factors $\langle sr \rangle$, $\langle sr, sr^3 \rangle / \langle sr \rangle$, and $D_8 / \langle sr, sr^3 \rangle$. Fifth, we have:

$$1 \leq \langle sr^3 \rangle \leq \langle sr, sr^3 \rangle \leq D_8$$

With composition factors $\langle sr^3 \rangle$, $\langle sr, sr^3 \rangle / \langle sr^3 \rangle$, and $D_8 / \langle sr, sr^3 \rangle$. Sixth, we have:

$$1 \leq \langle sr^2 \rangle \leq \langle s, sr^2 \rangle \leq D_8$$

With composition factors $\langle sr^2 \rangle$, $\langle s, sr^2 \rangle / \langle sr^2 \rangle$, and $D_8 / \langle s, sr^2 \rangle$. Finally, we have:

$$1 \leq \langle s \rangle \leq \langle s, sr^2 \rangle \leq D_8$$

With composition factors $\langle s \rangle$, $\langle s, sr^2 \rangle / \langle s \rangle$, and $D_8 / \langle s, sr^2 \rangle$. In each of the above 7 cases, we clearly have $N_{i+1}/N_i \cong Z_2$. ■

Exercise 3.4.3

Exercise 3.4.4

Exercise 3.4.5 Prove that subgroups and quotient groups of a solvable group are solvable.

Proof. Let G be a group and suppose G is solvable. Then there exists a chain of subgroups

$$1 = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_s = G$$

of G for which G_{i+1}/G_i is abelian for $0 \leq i < s$. Let $N \trianglelefteq G$, so that G/N is a quotient group of G. From the lattice isomorphism theorem, we know that there is a bijection between the set of subgroups A of G containing N onto the set of subgroups of A/N in G/N.

Since we have an ascending chain of containment for the G_i, it follows that since $N \trianglelefteq G$ we must have $N \subseteq G_k$ for some $0 \leq k < n$. Fix this index k, which permits us to write that $N \subseteq G_i$ for all $i \geq k$, i.e., ensures that N is contained in each successive subgroup, and so satisfies the hypothesis of the lattice isomorphism theorem.

In particular, by Theorem 20(5), for all $k \leq i < n$, we have that $G_i \trianglelefteq G$ if and only if $G_i/N \trianglelefteq G/N$, so now G_i/N is normal in G/N. Furthermore, we know that $G_i \trianglelefteq G_{i+1}$ if and only if $G_i/N \trianglelefteq G_{i+1}/N$ by Theorem 20(1). Thus, we may set $G_{k-1} = N$ and write that:

$$1 = N/N \trianglelefteq G_k/N \trianglelefteq \cdots \trianglelefteq G_s/N = G/N$$

Now, since $G_i \leq G_{i+1}$, and $G_i, G_{i+1} \trianglelefteq G$ for any i by assumption, we may invoke the results of the third isomorphism theorem to write:

$$(G_{i+1}/N)/(G_i/N) \cong G_{i+1}/G_i$$

Which suffices to show that $(G_{i+1}/N)/(G_i/N)$ is abelian, since the above isomorphism maps this group to G_{i+1}/G_i which was abelian by assumption. Therefore we have shown G/N is a solvable group.

Now we will prove that every subgroup of a solvable group is solvable. Let $H \leq G$ where G is as above, with the same chain of subgroups. So we have:

$$1 = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_s = G$$

Where each G_{i+1}/G_i is abelian for $0 \leq i < s$. Recall that in [[DF-3.1-24]] we showed that if $N \trianglelefteq G$, and $H \leq G$, then $N \cap H \trianglelefteq H$. Using this fact we can see:

$$1 = G_0 \cap H \trianglelefteq G_1 \cap H \trianglelefteq \cdots \trianglelefteq G_s \cap H = G \cap H = H$$

So in particular we have each $G_i \cap H \trianglelefteq H$ for all i, since by assumption we took $G_i \trianglelefteq G$ for each i. Additionally, since $G_i \trianglelefteq G_{i+1}$, and the intersection of two subgroups of G is again a siubgroup of G, we know that $G_i \cap H \leq G_{i+1} \cap H$. To show that this containment is normal, notte that $G_i \trianglelefteq G_{i+1}$ implies $G_{i+1} \leq N_G(G_i)$, and we know $G_{i+1} \cap H \leq N_G(G_i)$. Thus $G_i \cap H \trianglelefteq G_{i+1} \cap H$ for each $0 \leq i < s$. Now to prove that H is solvable it suffices to show that $(G_{i+1} \cap H)/(G_i \cap H)$ is abelian for all i.

To prove this, note that we have $G_{i+1} \cap H$ and G_i as subgroups of $G/$ Since we found above that $G_{i+1} \cap H \leq N_G(G_i)$, we may invoke the second isomorphism theorem to write that:

$$\frac{(G_{i+1} \cap H)G_i}{G_i} \cong \frac{G_{i+1} \cap H}{(G_{i+1} \cap H) \cap G_i} = \frac{G_{i+1} \cap H}{G_i \cap H}$$

But note that by the lattice isomorphism theorem, since $G_i \trianglelefteq G$ by assumption, and we saw $(G_{i+1} \cap H)G_i \subseteq G_{i+1}$, it follows that:

$$\frac{G_{i+1} \cap H}{G_i \cap H} \cong \frac{(G_{i+1} \cap H)G_i}{G_i} \leq G_{i+1}/G_i$$

To which the factor $(G_{i+1} \cap H)/(G_i \cap H)$ is a isomorphic to a subgroup of an abelian group, and since subgroups of abelian groups are isomorphic, it must also be abelian for each $0 \leq i < s$. Therefore H is by definition solvable. ■

Exercise 3.4.6

Exercise 3.4.7

Exercise 3.4.8

Exercise 3.4.9

Exercise 3.4.10

Exercise 3.4.11

Exercise 3.4.12

3.5 Transpositions and the Alternating Group

※ Group Actions

4.1 Group Actions and Permutation Representations

Exercise 4.1.1

Exercise 4.1.2

Exercise 4.1.3

Exercise 4.1.4

Exercise 4.1.5

Exercise 4.1.6

Exercise 4.1.7 Let G be a transitive permutation group on the finite set A. A *block* is a nonempty subset B of A such that for all $\sigma \in G$ either $\sigma(B) = B$ or $\sigma(B) \cap B = \varnothing$ (here $\sigma(B)$ is the set $\{\sigma(b) \mid b \in B\}$).
(a) Prove that if B is a block containing the element a of A, then the set G_B defined by $\{\sigma \in G \mid \sigma(B) = B\}$ is a subgroup of G containing G_a.
(b) Show that if B is a block and $\sigma_1(B), \sigma_2(B), \ldots, \sigma_n(B)$ are all distinct images of B under the elements of G, then these form a partition of A.
(c) A (transitive) group G on a set A is said to be *primitive* if the only blocks in A are the trivial ones: the sets of size 1 and A itself. Show that S_4 is primitive on $A = \{1, 2, 3, 4\}$. Show that D_8 is not primitive as a permutation group on the four vertices of a square.
(d) Prove that the transitive group G is primitive on A if and only if for each $a \in A$, the only subgroups of G containing G_a are G_a and G (i.e., G_a is a *maximal* subgroup of G, cf. Exercise 16, Section 2.4). [Use part (a).]

Proof. (a) Since the identity element of G fixes B, we know that $1 \in G_B \neq \varnothing$. If $\sigma, \tau \in G_B$ then $\sigma(B) = B$ and $\tau(B) = B$. In particular, we have that:

$$\tau^{-1}(B) = \tau^{-1}(\tau(B)) = (\tau^{-1}\tau)B = (1)B = B$$

and hence $\tau^{-1}(B) = B$ holds. Now it is clear that $\sigma\tau^{-1}(B) = \sigma(\tau^{-1}(B)) = \sigma(B) = B$;

hence $\sigma\tau^{-1} \in G_B$ and so $G_B \leq G$ by the subgroup criterion. If we assume that $\sigma \in G_a$, then $\sigma(a) = a$. Since B is a block, and $a \in \sigma(B) \cap B$, we require $\sigma(B) = B$. Thus $\sigma \in G_B$, to which $G_a \leq G_B$.

(b) Take B a block. Set $\Sigma = \{\sigma(B) \mid \sigma \in G\}$. Since B is a block, $B \neq \emptyset$, so there exists some $b \in B$. Now, for any $a \in A$, since G is transitive, there exists $\sigma \in G$ for which $\sigma(b) = a$. Since $b \in B$, we have $a = \sigma(b) \in \sigma(B)$; hence each element of A is contained in some element of Σ. Now suppose $\sigma \neq \tau$. If $\sigma(B) \cap \tau(B) \neq \emptyset$, then there exists an element $a \in \sigma(B) \cap \tau(B)$. Then there exists $b, c \in B$ such that $\sigma(b) = a$ and $\tau(c) = a$. Then $\tau^{-1}\sigma(b) = c$ holds, and $b, c \in B$ this means that $\tau^{-1}\sigma(B) = B$ since B is a block. Thus $\sigma(B) = \tau(B)$. In particular, for any $\sigma, \tau \in G$, either $\sigma(B)$ and $\tau(B)$ are disjoint or equal; hence the set Σ partitions A.

(c) We show that S_4 is primitive on $\{1, 2, 3, 4\}$. A non-trivial block B for S_4 contains either two or three elements of A. For generality, we take $A = \{a, b, c, d\}$. If B contains three elements, without loss of generality, say $B = \{a, b, c\}$, then the permutation $\sigma = (a\ b\ c\ d) \in S_4$ gives $\sigma(B) = \{b, c, d\}$, and clearly $B \cap \sigma(B) = \{b, c\}$ is neither all of B nor $\emptyset$; this is a contradiction to B being a block. If, on the other hand, B has two elements, say $B = \{a, b\}$, then the permutation $\tau = (a\ b\ c) \in S_4$ gives $\tau(B) = \{b, c\}$ and clearly $B \cap \tau(B) = \{b\}$ is neither all of B nor $\emptyset$; once more, a contradiction, since B is a block. Thus S_4 has no non-trivial blocks on A; hence is primitive.

Now consider D_8 acting on the four vertices of a square. $A = \{1, 2, 3, 4\}$ as vertices of the square labeled in a clockwise fashion. Considered as a permutation group, we may write $D_8 = \langle (1\ 2\ 3\ 4), (2\ 4) \rangle$. We claim that $\Delta = \{2, 4\}$ is a block for D_8. To do this, we must show that for each $\sigma \in D_8$, either $\sigma(\Delta) = \Delta$ or $\sigma(\Delta) \cap \Delta = \emptyset$. It suffices to show this on the generators for D_8:

$$(1\ 2\ 3\ 4)\Delta = \{1, 3\}$$

$$(2\ 4)\Delta = \{2, 4\}$$

Clearly $(1\ 2\ 3\ 4)\Delta \cap \Delta = \emptyset$ and $(2\ 4)\Delta = \Delta$. Hence Δ is a non-trivial block for D_8; hence this action is not primitive.

(d) For a fixed $a \in A$, we claim that there is a bijection between blocks of G containing a and subgroups of G containing G_a. Referring to part (a) above, we know that given a block Δ containing a, we have that G_Δ is a subgroup of G containing G_a. Conversely, given a subgroup H of G containing G_a, we claim that the set

$$\mathrm{Orb}_H(a) = \{\sigma(a) \mid \sigma \in H \mid\}$$

is a block for G containing a. To see this, note first that $(1) \in \mathrm{Orb}_H(a) \neq \varnothing$ since $(1) \in H$ and $(1)(a) = a$ always. Now if $\sigma \in G$ then either $\sigma \in H$ or $\sigma \notin H$. If $\sigma \in H$ then $\sigma(\mathrm{Orb}_H(a)) = \mathrm{Orb}_H(a)$. If $\sigma \notin H$ then $\sigma(\tau(a)) \notin \mathrm{Orb}_H(a)$ for any $\tau \in H$ since $\sigma\tau \notin H$, for if this were the case then since $\tau \in H$ we would have $\sigma\tau\tau^{-1} = \sigma \in H$, a contradiction. Hence $\sigma(\mathrm{Orb}_H(a)) \cap \mathrm{Orb}_H(a) = \varnothing$ holds; thus $\mathrm{Orb}_H(a)$ is a block for G.

Define a map Ψ from the blocks of G containing a to the subgroups of G containing G_a which takes $B \mapsto G_B$. Define a map Φ from the subgroups of G containing G_a to the blocks of G containing a which takes $H \mapsto \mathrm{Orb}_H(a)$. We claim that Ψ and Φ are inverses to one another.

To see this, given a block Δ containing a, we have the following set:

$$\Phi(\Psi(\Delta)) = \Phi(G_\Delta) = \mathrm{Orb}_{G_\Delta}(a) = \{\sigma(a) \mid \sigma \in G_\Delta\}$$

Set $\Delta' = \mathrm{Orb}_{G_\Delta}(a)$. We claim $\Delta = \Delta'$. Take any $b \in \Delta$. Since G is transitive, we know there exists $\sigma \in G$ such that $\sigma(a) = b$. Since $a \in \Delta$ by assumption, and Δ is a block and $b \in \Delta \cap \sigma(\Delta) \neq \varnothing$, we require $\Delta = \sigma(\Delta)$. Thus $\sigma \in G_\Delta$, and hence $b = \sigma(a) \in \Delta'$, to which $\Delta \subseteq \Delta'$. For the reverse containment, if $b \in \Delta'$ then $b = \sigma(a)$ for some $\sigma \in G_\Delta$, and so we have that $\sigma(\Delta) = \Delta$, and hence $b \in \sigma(\Delta) = \Delta$ means $\Delta' \subseteq \Delta$; thus we have equality.

Given a subgroup H of G containing G_a, we have:

$$\Psi(\Phi(H)) = \Psi(\mathrm{Orb}_H(a)) = G_{\mathrm{Orb}_H(a)}$$

Set $H' = G_{\mathrm{Orb}_H(a)}$. We claim $H = H'$. If $\sigma \in H$ then for any $\tau(a) \in \mathrm{Orb}_H(a)$ we have $\sigma(\tau(a)) = \sigma\tau(a) \in \mathrm{Orb}_H(a)$ since $\sigma\tau \in H$ by closure. Thus $\sigma(\mathrm{Orb}_H(a)) = \mathrm{Orb}_H(a)$ holds, to which $\sigma \in H'$ and hence $H \subseteq H'$. For the reverse containment, if $\sigma \in H'$ then $\sigma(\mathrm{Orb}_H(a)) = \mathrm{Orb}_H(a)$ and so in particular for $a = (1)(a) \in \mathrm{Orb}_H(a)$ we have $\sigma(a) \in \mathrm{Orb}_H(a)$, which means $\sigma \in H$; hence $H' \subseteq H$, giving us the equality.

Thus the maps Ψ and Φ above are inverses to one another, and so we have a bijection between the blocks of G containing a and the subgroups of G containing G_a.

Now if G is primitive then G has no non-trivial blocks, and in particular no non-trivial blocks containing a. Thus the only blocks containing a are $\{a\}$ and A itself. But $\Psi(\{a\}) = G_{\{a\}} = G_a$ and $\Psi(A) = G_A = G$; hence the only subgroups of G containing G_a are G_a and G itself; thus G_a is a maximal subgroup of G.

Conversely, if G_a is a maximal subgroup of G, then $\Phi(G_a) = \mathrm{Orb}_{G_a}(a) = \{a\}$ and $\Phi(G) = \mathrm{Orb}_G(a) = A$ are the only blocks of G containing a; hence G is primitive on A. ■

Exercise 4.1.8

Exercise 4.1.9

Exercise 4.1.10

4.2 Groups Acting on Themselves by Left Multiplication–Cayley's Theorem

4.3 Groups Acting on Themselves by Conjugation–The Class Equation

4.4 Automorphisms

Exercise 4.4.1 If $\sigma \in \text{Aut}(G)$ and φ_g is conjugation by g prove $\sigma\varphi_g\sigma^{-1} = \varphi_{\sigma(g)}$. Deduce that $\text{Inn}(G) \trianglelefteq \text{Aut}(G)$.

Proof. Let G be a group and $g \in G$. Suppose $\sigma \in \text{Aut}(G)$ and φ_g is conjugation by g. Let $h \in G$ be arbitrary. Then:

$$(\sigma\varphi_g\sigma^{-1})(h) = \sigma(\varphi_g(\sigma^{-1}(h))$$

Now, since $\sigma \in \text{Aut}(G)$, σ is a bijection, so it follows that there exists some $k \in G$ for which $\sigma^{-1}(h) = k$, equivalently, $\sigma(k) = h$. Thus:

$$\sigma(\varphi_g(\sigma^{-1}(h)) = \sigma(\varphi_g(k)) = \sigma(gkg^{-1}) = \sigma(g)\sigma(k)\sigma(g)^{-1} = \sigma(g)h\sigma(g)^{-1}$$

But then note that the above is precisely the same as $\sigma\varphi_g\sigma^{-1} = \varphi_{\sigma(g)}$, and since the above holds for all $h \in G$, it follows that this equality of mappings holds also.

Given the above proof, we may note that for all $g \in G$, we the corresponding conjugation map $\varphi_g \in \text{Inn}(G)$, and that these conjugation maps completely characterize the group of inner automorphisms $\text{Inn}(G)$. Thus, for any $\sigma \in \text{Aut}(G)$, we have:

$$\sigma\text{Inn}(G)\sigma^{-1} = \text{Inn}(G)$$

Since any map of the form $\varphi_{\sigma(g)}$ is again a conjugation by a fixed element of G, and so is in the group of inner automorphisms of G. The above is sufficient condition to write $\text{Inn}(G) \trianglelefteq \text{Aut}(G)$. ∎

Exercise 4.4.2 Prove that if G is an abelian group of order pq, where p and q are distinct primes, then G is cyclic.

Proof. Let G be an abelian group. Suppose $|G| = pq$, where p and q are distinct primes. By Cauchy's Theorem, since $p \mid |G|$ and $q \mid |G|$, it follows that there exists elements x and y in G for which $|x| = p$ and $|y| = q$. Now we will consider their prodict.

$$(xy)^{pq} = x^{pq}y^{pq} = (x^p)^q(y^q)^p = 1^q1^p = 1 \cdot 1 = 1$$

And so $|xy| \leq pq$. To prove that $|xy| = pq$, take some $k < pq$ and note that k must be some multiple of both p and q in order to satisfy $(xy)^k = 1$, but since $k < pq$, this is impossible; hence $|xy| = pq$ and so $\langle xy \rangle \leq G$ implies $\langle xy \rangle = G$ since $|G| = |xy|$. Thus G is cyclic. ∎

Exercise 4.4.3 Prove that under any automorphism of D_8, r has at most 2 possible images and s has at most 4 possible images. Deduce that $|\text{Aut}(D_8)| \leq 8$.

Proof. Consider the group D_8, and take some $\sigma \in \text{Aut}(D_8)$. Since $\sigma : D_8 \to D_8$ is an isomorphism, it follows that $|x| = |\sigma(x)|$ for all $x \in D_8$. If we consider $r \in D_8$, which has $|r| = 4$, then since the only elements of D_8 that satisfy $|x| = 4$ are $x = r$ and $x = r^3$, it follows that either $\sigma(r) = r$ or $\sigma(r) = r^3$. Thus, r has at most 2 possible images under automorphism.

To show the second part of the problem, we will first prove that $Z(G)$ char G. So take a group G and $\phi \in \text{Aut}(G)$. Then we know $Z(G) \cong \phi(Z(G))$, so that necessarily $\phi(Z(G)) \leq Z(\phi(G))$, i.e., the image of the center of G is a subgroup of the center of the image of G. Now suppose $y \in Z(\phi(G))$. Then, since ϕ is surjective, we have $y = \phi(x)$ for some $x \in G$. Since $y = \phi(x) \in Z(\phi(G))$ it follows that, for any $\phi(z) \in \phi(G)$, we have:

$$\phi(z)\phi(x) = \phi(x)\phi(z) \iff \phi(zx) = \phi(xz)$$

Which follows since ϕ is a group isomorphism. Now, since ϕ is a bijection, it is injective, and so we have:

$$\phi(zx) = \phi(xz) \implies zx = xz$$

For all $z \in G$. This means that $x \in Z(G)$, to which $Z(\phi(G)) \leq \phi(Z(G))$, and so $Z(\phi(G)) = \phi(Z(G))$ and so we have $\phi(Z(G)) = Z(G)$, i.e., $Z(G)$ char G.

For $s \in D_8$, note that $|s| = 2$, and we have s, r^2, sr, sr^2, and sr^3 as the only elements of D_8 also of order 2. However, it is impossible for $\sigma(s) = r^2$, since $s \notin Z(D_8)$ and $r^2 \in Z(D_8)$, we may not have $\sigma(s) = r^2$. Thus s has at most 4 possible images under automorphism.

Since, by definition of an isomorphim, we must have any automorphism of D_8 mapping generators to generators, and $\langle s, r \rangle = D_8$, there are a total of 2 elements to which r can be mapped and 4 elements to which s can be mapped, and thus there are at most 8 bijective mappings in $\text{Aut}(D_8)$, to which $|\text{Aut}(D_8)| \leq 8$. ■

Exercise 4.4.4 Use arguments similar to those in the preceding exercise to show that $|\text{Aut}(Q_8)| \leq 24$.

Proof. Consider the group Q_8. Note that $|1| = 1$, $|-1| = 2$, and the elements $\pm i, \pm j$ and $\pm k$ each have order 4. If $\phi \in \text{Aut}(Q_8)$, then ϕ preserves order and so we may not change either 1 or -1. Note that ϕ must satisfy:

$$\phi(-1) = -1$$

And since both $i^2 = -1$ and $(-i)^2 = -1$, it follows that we may map i to either itself or $-i$. This holds additionally for both j and k. Since each of i, j, and k each generate a cyclic subgroup, their images under ϕ must also generate these subgroups, and so we may not interchange any of the i and j and k. Thus for each of the three letters i and j and k, we have 2 options, and so there are $3 \cdot 2 \cdot 2 \cdot 2 = 24$ options for mappings. Thus $|\text{Aut}(Q_8)| \leq 24$. ■

Exercise 4.4.5

Exercise 4.4.6 Prove that characteristic subgroups are normal. Given an example of a normal subgroup that is not characteristic.

Proof. Let G be a group and $H \leq G$. Suppose H char G. Then, if $\sigma \in \text{Aut}(G)$, we know that by definition $\sigma(H) = H$. In particular, conjugation by a fixed $g \in G$ is an automorphism of G, and so fixes H also. Let ϕ_g be any such conjugation. Then:

$$\varphi_g(H) = gHg^{-1} = H$$

Which holds for all $g \in G$ by H being characteristic in G. The above is equivalent to $gH = Hg$ for all $g \in G$, to which $H \trianglelefteq G$. ■

Exercise 4.4.7 If H is the unique subgroup of a given order in a group G prove H is characteristic in G.

Proof. Let G be a group and $H \leq G$ such that $|H| = n$ for some $n \in \mathbb{Z}^+$. Suppose H is the unique subgroup of G of order n. Now take an arbitrary $\sigma \in \text{Aut}(G)$. Then we know that σ preserves subgroups and orders, and so in particular we must have $H \cong \sigma(H)$. In particular, this means that $|\sigma(H)| = n$ also. But since $\sigma : G \to G$ is an isomorphism, we have $\sigma(H) \leq G$. By assumption H was the unique subgroup of order n of G, and so we necessarily have $H = \sigma(H)$. Therefore, by definition, we have H char G. ■

Exercise 4.4.8

Exercise 4.4.9

Exercise 4.4.10

Exercise 4.4.11

Exercise 4.4.12 Let G be a group of order 3825. Prove that if H is a normal subgroup of order 17 in G then $H \leq Z(G)$.

Proof. Let G be a group with $|G| = 3825 = 3^2 \cdot 5^2 \cdot 17$. Suppose $H \trianglelefteq G$ with $|H| = 17$. Since 17 is prime, we know that $H \cong Z_{17}$, to which H is necessarily abelian, and so $H \leq C_G(H)$. By Lagrange's Theorem, this implies that 17 divides $|C_G(H)|$. By Corollary 14, since $H \trianglelefteq G$, we have $G/C_G(H)$ isomorphic to some subgroup of $\mathrm{Aut}(H)$. Given that 17 divides $|C_G(H)|$ and $H \leq C_G(H)$, we may have $|G/C_G(H)| = 1, 3, 5, 9, 15, 25, 45, 51, 85, 153$, or 225.

However, note that by Proposition 17(1), since $|H| = 17$ is an odd prime, we have $\mathrm{Aut}(H)$ is cyclic and of order 16. Since $|G/C_G(H)|$ divides $|\mathrm{Aut}(H)| = 16$ by Lagrange's Theorem, it is clear that $|G/C_G(H)| = 1$ is the only valid option from the above. This implies $G = C_G(H)$, to which $H \leq Z(G)$. ■

Exercise 4.4.13 Let G be a group of order 203. Prove that if H is a normal subgroup of order 7 in G then $H \leq Z(G)$. Deduce that G is abelian in this case.

Proof. Let G be a group with $|G| = 203 = 7 \cdot 29$. Suppose $H \trianglelefteq G$ such that $|H| = 7$. Since 7 is prime, it follows that $H \cong Z_7$, to which H is abelian and hence $H \leq C_G(H)$. Thus 7 divides $|C_G(H)|$, so $|C_G(H)| \geq 7$, and so either $|C_G(H)| = 7$, 29, or 203.

By Corollary 14, H being normal in G implies $G/C_G(H)$ is isomorphic to some subgroup of $\mathrm{Aut}(H)$. Further, by Proposition 17(1), we know that since 7 is an odd prime, $|\mathrm{Aut}(H)| = 6$. Thus $|G/C_G(H)|$ divides 6. and so given our above discussion we have $|G/C_G(H)| = 1$ or 29; it follows that $|G/C_G(H)| = 1$. Thus $G = C_G(H)$ and so $H \leq Z(G)$.

From the above, we may deduce $|Z(G)| \geq 7$, to which $|Z(G)| = 7, 29$, or 203. If $|Z(G)| = 7$, then $|G/Z(G)| = 29$, which is prime, and so $G/Z(G) \cong Z_{29}$. By [[DF-3.1-36]], this implies G is abelian. If instead we had $|Z(G)| = 29$, then $|G/Z(G)| = 7$, again a prime, so again $G/Z(G) \cong Z_p$, and so again by the same result G is abelian. Finally, if $|Z(G)| = 203$, then clearly $|G/Z(G)| = 1$, and so $G = Z(G)$, implying that G is abelian. Hence we have deduced that, in any case, our G above is abelian. ■

Exercise 4.4.14 Let G be a group of order 1575. Prove that if H is a normal subgroup of order 9 in G then $H \leq Z(G)$.

Proof. Let G be a group with $|G| = 1575 = 3^2 \cdot 5^2 \cdot 7$. By Corollary 9 in the chapter, we may write that since $|H| = 9 = 3^2$, H is abelian. Then, either H is cyclic or H is the elementary abelian group of order 9. First we will consider the case where H is cyclic, i.e., $H \cong Z_9$. This implies $H \leq C_G(H)$, and so 9 divides $|C_G(H)|$. By Corollary 14, since $H \trianglelefteq G$, we have $G/C_G(H)$ isomorphic to some subgroup of $\mathrm{Aut}(H)$. Since H is cyclic, Proposition 17(1) permits $|\mathrm{Aut}(H)| = 3(3-1) = 6$. Thus we must have $|G/C_G(H)|$ divides 2. But since $|C_G(H)| \geq 9$, we know that either $|G/C_G(H)| = 1, 5, 7, 25, 35$, or 175. Clearly then $|G/C_G(H)| = 1$, to which $G = C_G(H)$, and so $H \leq Z(G)$.

Now consider the case where H is the elementary abelian group of order 9. In this case, we have $H \cong Z_3 \times Z_3$, and so $|\text{Aut}(H)| = 3(3-1)^2(3+1) = 48$. Since H is abelian, we have $H \leq C_G(H)$, so 9 divides $|C_G(H)|$ and $|C_G(H)| \geq 9$. Proposition 17(1) again permits us to write that $G/C_G(H)$ is isomorphic to a subgroup of $\text{Aut}(H)$. Thus $|G/C_G(H)|$ divides 48. But since 9 divides $|C_G(H)|$, we are left with $|G/C_G(H)| = 1, 5, 7, 25, 35$, or 175 as above. The only valid order that divides 48 is 1, and so $|G/C_G(H)| = 1$, to which $G = C_G(H)$, equivalently, $H \leq Z(G)$. ■

Exercise 4.4.15

Exercise 4.4.16

Exercise 4.4.17

Exercise 4.4.18

Exercise 4.4.19

Exercise 4.4.20

4.5 The Sylow Theorems

Exercise 4.5.1 Prove that if $P \in \mathrm{Syl}_p(G)$ and H is a subgroup of G containing P then $P \in \mathrm{Syl}_p(H)$. Give an example to show that, in general, a Sylow p-subgroup of a subgroup of G need not be a Sylow p-subgroup of G.

Proof. Let G be a group and p a prime such that $|G| = p^\alpha m$ for some $\alpha \geq 0$ where $p \nmid m$. Suppose $P \in \mathrm{Syl}_p(G)$ and $P \leq H \leq G$. We know that $|P| = p^\alpha$, and so by Lagrange's Theorem, we have $p^\alpha \mid |H|$, and since $H \leq G$, $|H| \mid p^\alpha m$ also. Let $|H| = p^\alpha k$ for some $k \in \mathbb{Z}^+$. If $k = 0$, then $P = H$, and so we trivially have that H is the unique Sylow p-subgroup of H, and so $P = H \in \mathrm{Syl}_p(H)$. So assume $k > 1$. In this case, since $p^\alpha k \mid p^\alpha m$, it must follow that $k \mid m$. But this means that $p \nmid k$, and so since $P \leq H$ with $|P| = p^\alpha$, $P \in \mathrm{Syl}_p(H)$ by definition.

We will now produce an example to show that a Sylow p-subgroup of a subgroup of G need not be a Sylow p-subgroup of G itself. Consider $G = Z_{12}$ and $H = Z_6$, where $Z_6 \leq Z_{12}$. Note that $|G| = 2^2 \cdot 3$ and $2 \nmid 3$. Set $P = Z_2$ where $|Z_2| = 2^1$, which is by definition a Sylow 2-subgroup of H, since $|H| = 2^1 \cdot 3$. However, P is not a Sylow 2-subgroup of G since a Sylow 2-subgroup of G would require order $2^2 = 4$. ■

Exercise 4.5.2 Prove that if H is a subgroup of G and $Q \in \mathrm{Syl}_p(H)$ then $gQg^{-1} \in \mathrm{Syl}_p(gHg^{-1})$ for all $g \in G$.

Proof. Let G be a finite group, p a prime. Suppose $H \leq G$ and $Q \in \mathrm{Syl}_p(H)$. Let $|H| = p^\alpha m$, where $p \nmid m$, so $|Q| = p^\alpha$. We know that $H \cong gHg^{-1}$ for all $g \in G$ by Corollary 14. Similarly for Q, we know $Q \cong gQg^{-1}$ for all g. In particular, this implies $|gHg^{-1}| = p^\alpha m$ and $|gQg^{-1}| = p^\alpha$. But then, since it is clear that $gQg^{-1} \leq gHg^{-1}$ since $Q \leq H$, and so by definition, gQg^{-1} is a Sylow p-subgroup of gHg^{-1}, and so $gQg^{-1} \in \mathrm{Syl}_p(gHg^{-1})$ for all $g \in G$. ■

Exercise 4.5.3 Use Sylow's Theorem to prove Cauchy's Theorem.

Proof. Let G be a finite group and $p \mid |G|$, where p is a prime. Since $|G| > 1$, following because p is a prime and divides $|G|$, we know that there exists an element $x \in G$ for which $x \neq 1$. If $|G| = p^\alpha$ for any $\alpha \geq 1$, then we know that $|x|$ divides p^α by Lagrange's Theorem, so that $|x| = p^\beta$ for some $1 \leq \beta \leq \alpha$. But then p divides the order of x, and so $|x| = pk$, where $k = p^{\beta-1}$. By Proposition 2.5(2), we know that:

$$|x^{p^{\beta-1}}| = \frac{p^\beta}{\gcd(p^\beta, p^{\beta-1})} = \frac{p^\beta}{p^{\beta-1}} = p$$

And so we have our element of order p. So we may assume that $|G| = p^\alpha m$ for some $m \in \mathbb{Z}^+$ such that $p \nmid m$, i.e., the order of G is not only a power of p. Now, by Theorem 18(1), we have $\text{Syl}_p(G) \neq \emptyset$, to which $P \in \text{Syl}_p(G)$, where $|P| = p^\alpha$. Since $\alpha \geq 1$, there exists $x \in P$ for which $x \neq 1$, and we know that $|x|$ divides p^α. But then we are in the same position as the preceding paragraph, and so again we produce an element of order p. ■

Exercise 4.5.4

Exercise 4.5.5

Exercise 4.5.6

Exercise 4.5.7

Exercise 4.5.8

Exercise 4.5.9

Exercise 4.5.10

Exercise 4.5.11

Exercise 4.5.12

Exercise 4.5.13 Prove that a group of order 56 has a normal Sylow p-subgroup for some prime p dividing its order.

Proof. Let G be a group and $|G| = 56 = 2^3 \cdot 7$. By Sylow's Theorem, we may write that $n_7(G) = 1 + 7k$ for some $k \geq 0$. Further, $n_7(G) \mid 2^3 = 8$, and so we have permissible values of k being $k = 0$ or $k = 1$. In the case where $k = 0$, we have $n_7(G) = 1$, to which there is a unique Sylow 7-subgroup that is normal by Corollary 20.

Now tale $k = 1$. We have $n_7(G) = 1 + 7 = 8$ distinct Sylow 7-subgroups. Note that each of these subgroups is cyclic. Thus each Sylow 7-subgroup has 6 non-identity elements and the intersection of all of the 8 subgroups is trivial, to which there are a total of $8 \cdot 6 = 48$ elements of order 7 in G. By Theorem 18(1), we know $\text{Syl}_2(G) \neq \emptyset$, so we have at least one Sylow 2-subgroup of G. But since this Sylow 2-subgroup has order $2^3 = 8$, and $48 + 8 = 56$, there can be no other Sylow 2-subgroup since then the number of elements would surpass $|G| = 56$. Thus there is only one Sylow 2-subgroup of G and so by Corollary 20, it is normal in G. ■

Exercise 4.5.14 Prove that a group of order 312 has a normal Sylow p-subgroup for some prime p dividing 312.

Proof. Let G be a group with $|G| = 312 = 2^3 \cdot 3 \cdot 13$. By Sylow's Theorem, we know that $n_{13}(G) = 1 + 13k$ for some $k \geq 0$, and that $n_{13}(G) \mid 2^3 \cdot 3 = 24$. Clearly the only permissible value for k is $k = 0$, so then $n_{13}(G) = 1$ and so there is a unique Sylow 13-subgroup of G and it is normal in G by Corollary 20. ■

Exercise 4.5.15 Prove that a group of order 351 has a normal Sylow p-subgroup for some prime p dividing its order.

Proof. Let G be a group with $|G| = 351 = 3^3 \cdot 13$. Sylow's Theorem tells us that $n_{13}(G) = 1+13k$ for some $k \geq 0$, and that $n_{13}(G)$ divides $3^3 = 27$. Note then that the only permissible values for k are $k = 0$ or $k = 2$. In the case where $k = 0$, we have a unique Sylow 13-subgroup, which is normal by Corollary 20. So consider the case where $k = 2$, so we have 27 Sylow 13-subgroups of G. Note that if $H \in \text{Syl}_{13}(G)$, then $H \cong Z_{13}$ since 13 is prime. Since each Sylow 13-subgroup is cyclic, their intersection must be trivial, to which there are 27 distinct Sylow 13-subgroups of G, each with 12 non-identity elements. But then there are $12 \cdot 27 = 324$ elements of order 13 in G. Since $\text{Syl}_3(G) \neq \emptyset$, we know there must be at least one Sylow 3-subgroup of G, with 26 non-identity elements. Since $324 + 27 = 351$, there can only be one such Sylow 3-subgroup, and so again by Corollary 20, this Sylow 3-subgroup is normal in G. ∎

Exercise 4.5.16

Exercise 4.5.17 Prove that if $|G| = 105$ then G has a normal Sylow 5-subgroup and a normal Sylow 7-subgroup.

Proof. Let G be a group with $|G| = 105 = 3 \cdot 5 \cdot 7$. Assume, for contradiction, that G does not contain a normal Sylow 5-subgroup and a normal Sylow 7-subgroup. Now by Sylow's Theorem, $n_5(G) = 1 + 5k$, where $k \geq 0$, and $n_5(G) \mid 3 \cdot 7 = 21$. This forces either $k = 0$ or $k = 4$. If $k = 0$, then $n_5(G) = 1$, and so we have a normal Sylow 5-subgroup, contradictory to our assumption. Thus $k = 4$, so we have 21 Sylow 5-subgroups, each of which are cyclic since 5 is prime, and so each of whose intersection is trivial. Thus we have $5 - 1 = 4$ non-identity elements in each cyclic subgroup, and 21 subgroups, to which we have $4 \cdot 21 = 84$ elements of order 5 in G.

Similarly, we have $n_7(G) = 1 + 7h$, where $h \geq 0$, and $n_7(G) \mid 3 \cdot 5 = 15$. This forces either $h = 0$ or $h = 2$, and since we have no normal Sylow 7-subgroups, it follows that $h = 2$, so we have 15 Sylow 7-subgroups, each of which are cyclic since 7 is prime, and each of which contain 6 non-identity elements. Thus we have $6 \cdot 15 = 90$ elements of order 7 in G. Since we have 84 elements of order 5, we have that $90 + 84 > |G| = 105$, which is a contradiction. Therefore we may conclude that if $|G| = 105$, then G must have a normal Sylow 7-subgroup and a normal Sylow 5-subgroup. ∎

Exercise 4.5.18

Exercise 4.5.19

Exercise 4.5.20

Exercise 4.5.21

Exercise 4.5.22

Exercise 4.5.23

Exercise 4.5.24

Exercise 4.5.25

Exercise 4.5.26

Exercise 4.5.27

Exercise 4.5.28

Exercise 4.5.29

Exercise 4.5.30

Exercise 4.5.31

Exercise 4.5.32 Let P be a Sylow p-subgroup of H and let H be a subgroup of K. If $P \trianglelefteq H$ and $H \trianglelefteq K$, prove that P is normal in K. Deduce that if $P \in \mathrm{Syl}_p(G)$ and $H = N_G(P)$, then $N_G(H) = H$ (in words: *normalizers of Sylow p-subgroups are self-normalizing*).

Proof. Let $P \in \mathrm{Syl}_p(H)$ and $H \leq K$. Suppose $P \trianglelefteq H$ and $H \trianglelefteq K$. Then, by Corollary 20 we know that P char H, to which we may invoke the results of [[DF-4.4-8]], to write that $P \trianglelefteq K$.

Now take $P \in \mathrm{Syl}_p(G)$ and denote $H = N_G(P)$. Since $P \trianglelefteq H$ by construction, as well as $H \trianglelefteq N_G(H)$, it follows by the above result that $P \trianglelefteq N_G(H)$. However this means that if $x \in N_G(H)$, then $xPx^{-1} = P$. Note that this also implies $x \in H = N_G(P)$, to which $N_G(H) \leq H$, and hence $N_G(H) = H$. ■

Exercise 4.5.33 Let P be a normal Sylow p-subgroup of G and let H be any subgroup of G. Prove that $P \cap H$ is the unique Sylow p-subgroup of H.

Proof. Let G be a group, $P \in \mathrm{Syl}_p(G)$ such that $P \trianglelefteq G$, and $H \leq G$. First, let $|G| = p^\alpha m$, where $p \nmid m$. Then $|P| = p^\alpha$. Since $H \leq N_G(P) = G$, it follows from the second isomorphism theorem that $PH \leq G$, $P \cap H \trianglelefteq H$, and $P \trianglelefteq PH$. By [[DF-4.5-1]], since $P \leq PH \leq G$, and $P \in \mathrm{Syl}_p(G)$, it follows that $P \in \mathrm{Syl}_p(PH)$. Thus, by definition, $|PH| = p^\alpha n$, where $p \nmid n$. But then:

$$|PH| = \frac{|P| \cdot |H|}{|P \cap H|} = p^\alpha n \iff \frac{|H|}{|P \cap H|} = n$$

Now, since $P \cap H \leq P$, we know by Lagrange's Theorem that $|P \cap H| = p^\beta$, for some $1 \leq \beta \leq \alpha$. This implies that:

$$|H| = |P \cap H| \cdot n = p^\beta n$$

By definition, we then have $P \cap H \in \mathrm{Syl}_p(H)$. Furthermore, since we saw above that $P \cap H \trianglelefteq H$, it follows from Corollary 20 that $P \cap H$ is the unique Sylow p-subgroup of H. ■

Exercise 4.5.34 Let $P \in \mathrm{Syl}_p(G)$ and assume $N \trianglelefteq G$. Use the conjugacy part of Sylow's Theorem to prove that $P \cap N$ is a Sylow p-subgroup of N. Deduce that PN/N is a Sylow p-subgroup of G/N.

Proof. Let G be a group, $P \in \mathrm{Syl}_p(G)$, and $N \trianglelefteq G$. Let $|G| = p^\alpha m$, with $p \nmid m$. Then $|P| = p^\alpha$, and since $P \cap N \leq P$, by Lagrange's Theorem $P \cap N$ divides p^α, to which $|P \cap N| = p^\beta$ for some $1 \leq \beta \leq \alpha$. Since $P \leq N_G(N) = G$, the second isomorphism theorem allows us to write that $PN \leq G$. Furthermore, since $P \leq PN \leq G$, it follows from [[DF-4.5-1]] that $P \in \mathrm{Syl}_p(PN)$. Thus $|PN| = p^\alpha n$, for some $p \nmid n$. But then:

$$|PN| = \frac{|P| \cdot |N|}{|P \cap N|} = p^\alpha n \iff |N| = p^\beta n$$

Therefore, since $P \cap N \leq N$, and $|P \cap N| = p^\beta$, $P \cap N$ is by definition a Sylow p-subgroup of N.

Now note that, with our above hypothesis, $PN/N \leq G/N$ clearly holds by the lattice isomorphism theorem. If we let $|G|$ be as above, the order of G/N is seen to be:

$$|G/N| = \frac{|G|}{|N|} = \frac{p^\alpha m}{p^\beta n} = p^{\alpha-\beta} k$$

Where $k = m/n$ is some integer. But then since:

$$|PN/N| = \frac{|P| \cdot |N|}{|P \cap N| \cdot |N|} = \frac{|P|}{|P \cap N|} = \frac{p^\alpha}{p^\beta} = p^{\alpha-\beta}$$

We may refer to the definition of a Sylow p-subgroup of G/N to write that $PN/N \in \mathrm{Syl}_p(G/N)$ as desired. ∎

Exercise 4.5.35

Exercise 4.5.36

Exercise 4.5.37

Exercise 4.5.38

Exercise 4.5.39

Exercise 4.5.40

Exercise 4.5.41

Exercise 4.5.42

Exercise 4.5.43

Exercise 4.5.44

Exercise 4.5.45

Exercise 4.5.46

Exercise 4.5.47

Exercise 4.5.48

Exercise 4.5.49

Exercise 4.5.50

Exercise 4.5.51

Exercise 4.5.52

Exercise 4.5.53

Exercise 4.5.54

Exercise 4.5.55

Exercise 4.5.56

4.6 The Simplicity of A_n

Exercise 4.6.1

Exercise 4.6.2

Exercise 4.6.3

Exercise 4.6.4

Exercise 4.6.5

Exercise 4.6.6

Exercise 4.6.7

Exercise 4.6.8

❊ Direct and Semidirect Products and Abelian Groups

5.1 Direct Products

Exercise 5.1.1

Exercise 5.1.2

Exercise 5.1.3

Exercise 5.1.4

Exercise 5.1.5

Exercise 5.1.6

Exercise 5.1.7

Exercise 5.1.8

Exercise 5.1.9

Exercise 5.1.10

Exercise 5.1.11

Exercise 5.1.12

Exercise 5.1.13

Exercise 5.1.14

Exercise 5.1.15

Exercise 5.1.16

Exercise 5.1.17

Exercise 5.1.18

5.2 The Fundamental Theorem of Finitely Generated Abelian Groups

Exercise 5.2.1

Exercise 5.2.2

Exercise 5.2.3

Exercise 5.2.4

Exercise 5.2.5

Exercise 5.2.6

Exercise 5.2.7

Exercise 5.2.8

Exercise 5.2.9

Exercise 5.2.10

Exercise 5.2.11

Exercise 5.2.12

Exercise 5.2.13

Exercise 5.2.14

Exercise 5.2.15

Exercise 5.2.16

5.3 Table of Groups of Small Order

Exercise 5.3.1

5.4 Recognizing Direct Products

Exercise 5.4.1

Exercise 5.4.2

Exercise 5.4.3

Exercise 5.4.4

Exercise 5.4.5

Exercise 5.4.6

Exercise 5.4.7

Exercise 5.4.8

Exercise 5.4.9

Exercise 5.4.10

Exercise 5.4.11

Exercise 5.4.12

Exercise 5.4.13

Exercise 5.4.14

Exercise 5.4.15

Exercise 5.4.16

Exercise 5.4.17

Exercise 5.4.18

Exercise 5.4.19

Exercise 5.4.20

5.5 Semidirect Products

Exercise 5.5.1

Exercise 5.5.2

Exercise 5.5.3

Exercise 5.5.4

Exercise 5.5.5

Exercise 5.5.6

Exercise 5.5.7

Exercise 5.5.8

Exercise 5.5.9

Exercise 5.5.10

Exercise 5.5.11

Exercise 5.5.12

Exercise 5.5.13

Exercise 5.5.14

Exercise 5.5.15

Exercise 5.5.16

Exercise 5.5.17

Exercise 5.5.18

Exercise 5.5.19

Exercise 5.5.20

Exercise 5.5.21

Exercise 5.5.22

Exercise 5.5.23

Exercise 5.5.24

Exercise 5.5.25

※ Further Topics in Group Theory

6.1 p-groups, Nilpotent Groups, and Solvable Groups

6.2 Applications in Groups of Medium Order

6.3 A Word on Free Groups

※ Introduction to Rings

7.1 Basic Definitions and Examples

Exercise 7.1.1

Exercise 7.1.2

Exercise 7.1.3

Exercise 7.1.4

Exercise 7.1.5

Exercise 7.1.6

Exercise 7.1.7 The *center* of a ring R is $\{z \in R \mid zr = rz \text{ for all } r \in R\}$ (i.e., is the set of all elements which commute with every element of R). Prove that the center of a ring is a subring that contains the identity. Prove that the center of a division ring is a field.

Proof. Let R be a ring with identity. We shall denote the center of R by $Z(R)$. Since the identity 1 commutes with every element of R automatically, we know that $1 \in Z(R)$ and hence $Z(R) \neq \emptyset$. Now take $a, b \in Z(R)$. Then

$$(a-b)r = ar - br = ra - rb = r(a-b)$$

$$(ab)r = a(br) = a(rb) = (ar)b = (ra)b = r(ab)$$

which follows since $ra = ar$ and $br = rb$ for all $r \in R$ since a and b commute with all elements of R. The above equations show that $a - b \in Z(R)$ and $ab \in Z(R)$, and hence that $Z(R)$ is a subring of R.

Now let D be a division ring. Then $Z(D)$ is a subring of D, and in particular is a ring in its own right. Moreover, $Z(D)$ is a commutative ring, and every non-zero element has a multiplicative inverse, i.e., is a unit, since D is a division ring. Hence $Z(D)$ is a field. ■

Exercise 7.1.8 Describe the center of the real Hamilton Quaternions $\mathbb{H}$. Prove that $\{a + bi \mid a, b \in \mathbb{R}\}$ is a subring of $\mathbb{H}$ which is a field but is not contained in the center of $\mathbb{H}$.

Proof. Take $\alpha \in Z(\mathbb{H})$, letting $\alpha = x + yi + zj + wk$. We know that α must commute with every element of $\mathbb{H}$, in particular we require $\alpha i = i\alpha$. Thus the two values

$$\alpha i = (x + yi + zj + wk)i = xi + yi^2 + zji + wki = -y + xi - wj - zk$$

$$i\alpha = i(x + yi + zj + wk) = xi + yi^2 + zij + wik = -y + xi - wj + zk$$

must agree. However, note that

$$-y + xi - wj - zk = -y + xi - wj + zk \iff -zk = zk$$

which occurs if and only if $z = 0$. Thus we have $\alpha = x + yi + wk$. But α must also commute with j, as $\alpha j = j\alpha$, and so we require that the two values

$$\alpha j = (x + yi + wk)j = xj + yij + wkj = -wi + xj + yk$$

$$j\alpha = j(x + yi + wk) = xj + yji + wjk = wi + xj - yk$$

agree. But note that

$$-wi + xj + yk = wi + xj - yk \iff -wi + yk = wi - yk \iff 2wi = 2yk$$

but this implies that $2w = 2y = 0$ since the components of i and k must agree. Hence we have that $y = w = 0$ as well, and so $\alpha = x$ must hold. Since any real number commutes with any real quaternion, as can easily be seen, this suffices to prove that $Z(\mathbb{H}) = \mathbb{R}$.

Now consider the subset $A = \{a + bi \mid a, b \in \mathbb{R}\}$ of $\mathbb{H}$. Note that $0 \in A$ so that $A \neq \emptyset$, and moreover if $a + bi, c + di \in A$ then

$$(a + bi) - (c + di) = a + bi - c - di = (a - c) + (b - d)i \in A$$

$$(a + bi)(c + di) = ac + adi + bci + bdi^2 = (ac - bd) + (ad + bc)i \in A$$

and so A is a subring of $\mathbb{H}$. We have commutativity of multiplication in A since

$$(c + di)(a + bi) = ca + cbi + dai + dbi^2 = (ac - bd) + (ad + bc)i$$

agrees with the value for $(a + bi)(c + di)$. For inverses under multiplication, note that

$$(a + bi)\left(\frac{a - bi}{a^2 + b^2}\right) = \frac{a^2 - abi + abi - b^2i^2}{a^2 + b^2} = \frac{a^2 + b^2}{a^2 + b^2} = 1$$

and clearly

$$\frac{a - bi}{a^2 + b^2} = \frac{a}{a^2 + b^2} - \frac{b}{a^2 + b^2}i \in A$$

as well. Hence every non-zero element of A has a multiplicative inverse, which since multiplication in A is commutative means that A is a field. Clearly, also, A is not contained in $Z(\mathbb{H})$ since $Z(\mathbb{H}) = \mathbb{R}$ and $A \not\subseteq \mathbb{R}$, for instance via $i \in A$. ■

Exercise 7.1.9 For a fixed element $a \in R$ define $C(a) = \{r \in R \mid ra = ar\}$. Prove that $C(a)$ is a subring of R containing a. Prove that the center of R is the intersection of the subrings $C(a)$ over all $a \in R$.

Proof. Fix $a \in R$. Since R has an identity, we know that $1a = a1$ and hence $1 \in C(a)$ to which $C(a) \neq \varnothing$. Now take $x, y \in C(a)$. Then observe that

$$(x - y)a = xa - ya = ax - ay = a(x - y)$$

$$(xy)a = x(ya) = x(ay) = (xa)y = (ax)y = a(xy)$$

and so we have $x - y, xy \in C(a)$, to which $C(a)$ is a subring of R. Moreover, since $aa = aa$ trivially holds, we have $a \in C(a)$.

Now consider the center $Z(R)$ of R. We claim that

$$Z(R) = \bigcap_{a \in R} C(a)$$

If $r \in Z(R)$ then $ra = ar$ for all $a \in R$ and so $r \in C(a)$ for all $a \in R$, meaning we have $Z(R) \subseteq \bigcap_{a \in R} C(a)$. For the reverse inclusion, if $r \in \bigcap_{a \in R} C(a)$ then $ra = ar$ for all $a \in R$, meaning obviously that $r \in Z(R)$. ■

Exercise 7.1.10 Prove that if D is a division ring then $C(a)$ is a division ring for all $a \in D$ (cf. the preceding exercise).

Proof. Let D be a division ring and take any $a \in D$. From Exercise 7.1.9 above we know that $C(a)$ is a subring of D, in particular a ring itself. What remains is to prove that every non-zero element of $C(a)$ is a unit. Take any $r \in C(a)$ and note that $r^{-1} \in D$ must exist. Since we know $ar = ra$, we can multiply on the left by r^{-1} to obtain $r^{-1}ar = r^{-1}ra = a$. Now multiplying on the right by r^{-1} gives us that $r^{-1}arr^{-1} = ar^{-1}$, and so of course $r^{-1}a = ar^{-1}$, proving that $r^{-1} \in C(a)$, and hence that $C(a)$ is a dvision ring. ■

Exercise 7.1.11 Prove that if R is an integral domain and $x^2 = 1$ for some $x \in R$ then $x = \pm 1$.

Proof. Let R be an integral domain and suppose $x^2 = 1$ for some $x \in R$. Then we have

$$x^2 - 1 = (x - 1)(x + 1) = 0$$

and since R is an integral domain either $x - 1 = 0$ or $x + 1 = 0$ must hold. In the first case we have $x = 1$ and in the second case we have $x = -1$, so that $x = \pm 1$ must hold, as desired. ■

Exercise 7.1.12 Prove that any subring of a field which contains the identity is an integral domain.

Proof. Let F be a field and suppose R is a subring of F with $1 \in R$. Assume $ab = 0$ for some $a, b \in R$. Since fields have no zero divisors, and since the multiplication $ab = 0$ must also hold in F, we know that either $a = 0$ or $b = 0$, and hence the same must hold in R. Hence R has no zero divisors, and since $1 \in R$, we know that R is an integral domain. ∎

Exercise 7.1.13 An element x in R is called *nilpotent* if $x^m = 0$ for some $m \in \mathbb{Z}^+$.
(a) Show that if $n = a^k b$ for some integers a and b then $\overline{ab}$ is a nilpotent element of $\mathbb{Z}/n\mathbb{Z}$.
(b) If $a \in \mathbb{Z}$ is an integer, show that the element $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$ is nilpotent if and only if every prime divisor of n is also a divisor of a. In particular, determine the nilpotent elements of $\mathbb{Z}/72\mathbb{Z}$ explicitly.
(c) Let R be the ring of functions from a nonempty set X to a field F. Prove that R contains no nonzero nilpotent elements.

Proof. (a) Suppose $n = a^k b$ for some $a, b \in \mathbb{Z}$, and some $k \in \mathbb{Z}^+$. Then we have

$$(ab)^k = a^k b^k = (a^k b) b^{k-1} = n b^{k-1}$$

In particular, we can see that

$$(ab)^k = n b^{k-1} \equiv 0 \pmod{n}$$

and so $\overline{ab}$ is a nilpotent element of $\mathbb{Z}/n\mathbb{Z}$.

(b) Suppose $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$ is nilpotent. Then there exists $k \in \mathbb{Z}^+$ such that $\overline{a}^k = \overline{0}$. In other words, $a^k = nb$ for some $b \in \mathbb{Z}$. In particular, any prime divisor p of n must divide nb, and hence must also divide a^k. But then p must also divide either a or a^{k-1}, and similarly either a or a^{k-2}, and all the way until we reach a. In other words, every prime divisor of n must also divide a.

Take $n = \prod_{i=1}^m p_i^{r_i}$ as the prime factorization of n. For the converse, suppose every prime divisor of n divides a, that is $p_i \mid a$ for all $i \in \{1, \dots, m\}$. In particular, we have that

$$a = (p_1 \cdots p_m) b$$

for some integer b. Now set $k = \max\{r_1, \dots, r_m\}$. Then we have that

$$a^k = (p_1^k \cdots p_m^k) b^k$$

Clearly $p_i^{r_i}$ divides a^k for all $i \in \{1, \dots, m\}$ since $r_i \leq k$ for all such i. In particular, this means that n divides a^k, and hence that $\overline{a}^k = \overline{0}$ in $\mathbb{Z}/n\mathbb{Z}$, which means that $\overline{a}$ is nilpotent.

Using what we have proved above, consider $n = 72$. The prime factorization of 72 is $72 = 2^3 \cdot 3^2$. Thus the prime factors of 72 are simply 2 and 3. By the proof above, the nilpotent elements of $\mathbb{Z}/72\mathbb{Z}$ are those elements $\overline{a}$ where a is an integer between 0 and 71 divisible by both 2 and 3. Explicitly, can see that any such integer divisible by 2 and 3 must have 6 as a divisor, and so the nilpotent elements are of the form $6k$ as k ranges. Computing, we find:

$$\{0, 6, 12, 18, 24, 30, 36, 42, 48, 54, 60, 66\}$$

to be the set of nilpotent elements of $\mathbb{Z}/72\mathbb{Z}$ (when taken modulo 72).

(c) Let X be a set such that $X \neq \varnothing$ and let F be a field. Let R be the ring of functions from X to F. Assume, for contradiction, that R has a nilpotent element, say $f : X \to F$. Then $f^k = 0$, the zero map, for some $k \in \mathbb{Z}^+$. However, if this is the casse, note that

$$f^k(x) = f(x)^k$$

since multplication in the ring of functions R is defined this way. Since $f^k = 0$ we know that $f(x)^k = 0$ for all $x \in X$, and since F is a field, hence an integral domain, we know that $f(x) = 0$ must hold for all $x \in X$, which means that $f = 0$ is the zero function. Hence R has no non-zero nilpotent elements. ∎

Exercise 7.1.14 Let x be a nilpotent element of the commutative ring R (cf. the preceding exercise).
(a) Prove that x is either zero or a zero divisor.
(b) Prove that rx is nilpotent for all $r \in R$.
(c) Prove that $1 + x$ is a unit in R.
(d) Deduce that the sum of a nilpotent element and a unit is a unit.

Proof. (a) Suppose $x \in R$ is a nilpotent element. Take $k \in \mathbb{Z}^+$ to be the integer minimal with respect to the property that $x^k = 0$ in R. If $x = 0$ then we are done, so assume $x \neq 0$. Then $x^k = x^{k-1}x = 0$ and since $x^{k-1} \neq 0$, as we assumed k was minimal with respect to the property above, this shows that x is a zero divisor in R.

(b) Let $r \in R$ be arbitrary. Since x is nilpotent, there exists $k \in \mathbb{Z}^+$ for which $x^k = 0$. Now note that $(rx)^k = r^k x^k = r^k 0 = 0$ where the second equality holds since R is a commutative ring. In particular, this shows that rx is nilpotent.

(c) Once again, since x is nilpotent, there exists $k \in \mathbb{Z}^+$ such that $x^k = 0$. There are two cases: either k is even or k is odd. If k is even, note that

$$(1 + x)(-x^{k-1} + x^{k-2} - \cdots - x + 1) = -x^{k-1} + x^{k-2} - \cdots - x + 1 - x^k + x^{k-1} - \cdots - x^2 + x$$

$$= -x^k + (-x^{k-1} + x^{k-1}) + (-x^{k-2} + x^{k-2}) + \cdots + (-x + x) + 1$$
$$= 1$$

to which the element $-x^{k-1} + x^{k-2} - \cdots - x + 1 \in R$ makes $1 + x$ into a unit, as it is a multiplicative inverse, as can easily be seen by performing the multiplication on the left instead.

Now we turn to the case where k is odd. We observe that

$$(1 + x)(x^{k-1} - x^{k-2} + \cdots - x + 1) = x^{k-1} - x^{k-2} + \cdots - x + 1 + x^k - x^{k-1} + \cdots - x^2 + x$$
$$= x^k + (x^{k-1} - x^{k-1}) + (-x^{k-2} + x^{k-2}) + \cdots + (-x + x) + 1$$
$$= 1$$

once more because $x^k = 0$ holds. Performing the multiplication on the left instead of the right as we did above yields the same result; we have shown that in either case $1 + x$ is a unit in R.

(d) Let x be a nilpotent element of R and let y be a unit in R. We claim that $x + y$ is a unit in R. Since y is a unit we know that $y^{-1} \in R$. By part (b) above, since x is nilpotent and $y^{-1} \in R$ we have that xy^{-1} is nilpotent. Now, by part (c), we know that $1 + xy^{-1}$ is a unit. Now observe that

$$x + y = (xy^{-1} + 1)y$$

and since both y and $xy^{-1} + 1$ are units, and the product of two units is once more a unit since $R^\times$ is closed under multiplication, we have that $x + y$ is a unit, as desired. ■

Exercise 7.1.15 A ring R is called a *Boolean ring* if $a^2 = a$ for all $a \in R$. Prove that every Boolean ring is commutative.

Proof. Let R be a Boolean ring and take $x, y \in R$. Since $x + y \in R$ we require $(x + y)^2 = x + y$ since R is Boolean. Performing the multiplication, we get

$$(x + y)^2 = x^2 + xy + yx + y^2 = x + xy + yx + y$$

where the second equality follows since $x^2 = x$ and $y^2 = y$. Now from our initial observation above, we require that

$$x + y = x + xy + yx + y \iff xy + yx = 0$$

which of course occurs if and only if $xy = -(yx)$. However, note that $(-1)^2 = -1$ must hold, and since $(-1)^2 = 1$, we need $-1 = 1$ to hold in R. In other words, the above equation implies that $xy = -(yx) = yx$, and hence that multiplication in R is commutative. ■

Exercise 7.1.16 Prove that the only Boolean ring that is an integral domain is $\mathbb{Z}/2\mathbb{Z}$.

Proof. Suppose B is a Boolean ring that is an integral domain. Clearly 0 and 1 are elements of B, so that $|B| \geq 2$. Suppose $x \in B$ such that $x \neq 0, 1$. Then observe that since $x + 1 \in B$ we require $(x+1)^2 = x + 1$ as B is a Boolean ring. Performing the multiplication yields

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

where the second equality follows since $x^2 = x$. From our initial observation, we now require that

$$x + 2x + 1 = x + 1 \iff 2x = 0$$

Clearly $2 \neq 0$, and since B is an integral domain, the above equation on the right implies that $x = 0$, contrary to our assumption that $x \neq 0$. Thus no such element $x \in B$ exists, and so $|B| = 2$. Since rings are, in particular, additive abelian groups, and the only such group of order 2 is $\mathbb{Z}/2\mathbb{Z}$, we require that $B = \mathbb{Z}/2\mathbb{Z}$. ∎

Exercise 7.1.17 Let R and S be rings. Prove that the direct product $R \times S$ is a ring under componentwise addition and multiplication. Prove that $R \times S$ is commutative if and only if both R and S are commutative. Prove that $R \times S$ has an identity if and only if both R and S have an identity.

Proof. Let R and S be rings. Clearly $R \times S$ is an abelian group under componentwise addition. We also have associativity induced by the associativity of the multiplication operation in both R and S, since for instance

$$[(r,s)(r',s')](r'',s'') = (rr',ss')(r'',s'') = (rr'r'',ss's'')$$

$$(r,s)[(r',s')(r'',s'')] = (r,s)(r'r'',s's'') = (rr'r'',ss's'')$$

and the two values above agree. To check the distributive law, we see

$$[(r,s)+(r',s')](r'',s'') = (r+r',s+s')(r'',s'')$$

$$= (rr''+r'r'',ss''+s's'')$$

$$= (r,s)(r'',s'') + (r',s')(r'',s'')$$

which follows by the distributivity of the rings R and S once more. The check for the other distributive law is identical to the above, and we shall omit it.

Now assume both R and S are commutative. Then if $r, r' \in R$ and $s, s' \in S$ we have $rr' = r'r$ and $ss' = s's$. This gives that

$$(r,s)(r',s') = (rr',ss') = (r'r,s's) = (r',s')(r,s)$$

and hence $R \times S$ is commutative. Conversely, if $R \times S$ is commutative then we clearly have commutativity in both R and S, respectively.

Now assume both R and S have an identity, say 1_R and 1_S, respectively. Then, for any $r \in R$ and $s \in S$, we have

$$(1_R, 1_S)(r, s) = (1_R r, 1_S s) = (r, s) = (r1_R, s1_S) = (r, s)(1_R, 1_S)$$

and hence $(1_R, 1_S)$ is an identity for $R \times S$. Conversely, it can easily be shown that if $R \times S$ has an identity, say (a, b), then a is an identity for R and b is an identity for S. ∎

Exercise 7.1.18 Prove that $\{(r, r) \mid r \in R\}$ is a subring if $R \times R$.

Proof. Let $D = \{(r, r) \mid r \in R\}$. To prove the claim, note that $0 \in R$ and hence $(0, 0) \in D$ holds, to which $D \neq \varnothing$. Now take $x, y \in D$, letting $x = (r, r)$ and $y = (s, s)$ for $r, s \in R$. We have

$$x - y = (r, r) - (s, s) = (r - s, r - s) \in D$$

$$xy = (r, r)(s, s) = (rs, rs) \in D$$

and hence D is closed under subtraction and multiplication. Therefore D is a subring of $R \times R$. ∎

Exercise 7.1.19 Let I be any nonempty index set and let R_i be a ring for each $i \in I$. Prove that the direct product $\prod_{i \in I} R_i$ is a ring under componentwise addition and multiplication.

Proof. If I is an index set and R_i is a ring for each $i \in I$, then clearly $\prod_{i \in I} R_i$ is an abelian group under componentwise addition, the direct product of the underlying additive abelian groups R_i, as we have seen before. We show that componentwise multiplication is associative:

$$\begin{aligned}
(c_1, c_2, \ldots) &= (a_1 b_1, a_2 b_2, \ldots)(c_1, c_2, \ldots) \\
&= ((a_1 b_1) c_1, (a_2 b_2) c_2, \ldots) \\
&= (a_1 (b_1 c_1), a_2 (b_2 c_2), \ldots) \\
&= (a_1, a_2, \ldots)(b_1 c_1, b_2 c_2, \ldots) \\
&= (a_1, a_2, \ldots)[(b_1, b_2, \ldots)(c_1, c_2, \ldots)]
\end{aligned}$$

where the third line above follows from the second given the assumed associativity of multiplication in each ring R_i. For the distributive laws, we have:

$$\begin{aligned}(c_1, c_2, \ldots) &= (a_1 + b_1, a_2 + b_2, \ldots)(c_1, c_2, \ldots)\\ &= ((a_1 + b_1)c_1, (a_2 + b_2)c_2, \ldots)\\ &= (a_1c_1 + b_1c_1, a_2c_2 + b_2c_2, \ldots)\\ &= (a_1c_1, a_2c_2, \ldots) + (b_1c_1, b_2c_2, \ldots)\\ &= (a_1, a_2, \ldots)(c_1, c_2, \ldots) + (b_1, b_2, \ldots)(c_1, c_2, \ldots)\end{aligned}$$

The third one line follows from the second by the assumpiton that the distributive law holds in each component ring R_i. The other distributive law is proved in an entirely analagous fashion, and hence shall be omitted for brevity. We conclude that $\prod_{i\in I} R_i$ is a ring under the operations of componentwise addition and componentwise multiplication. ■

Exercise 7.1.20 Let R be the collection of sequences $(a_1, a_2, a_3, \ldots)$ of integers $a_1, a_2, a_3, \ldots$ where all but finitely many of the a_i are 0 (called the *direct sum* of infinitely many copies of $\mathbb{Z}$). Prove that R is a ring under componentwise addition and multiplication which does not have an identity.

Proof. Let R be as defined in the problem description. Taking $I = \mathbb{N}$ and letting $R_i = \mathbb{Z}$ for all $i \in I$, we can see that R is a subset of the direct product ring $\prod_{i\in I} R_i$ of Exercise 7.1.19 previously. We shall show that R is a subring of $\prod_{i\in \mathbb{I}} R_i$ which does not have an identity. Note that if $(a_1, a_2, \ldots)$ and $(b_1, b_2, \ldots)$ are elements of R, then

$$(a_1, a_2, \ldots) - (b_1, b_2, \ldots) = (a_1 - b_1, a_2 - b_2, \ldots) \in R$$

since by assumption $(a_1, a_2, \ldots)$ has finitely many non-zero components, as does $(b_1, b_2, \ldots)$, and so too must their difference $(a_1 - b_1, a_2 - b_2, \ldots)$. Similarly,

$$(a_1, a_2, \ldots)(b_1, b_2, \ldots) = (a_1b_1, a_2b_2, \ldots) \in R$$

holds for the same reason. Since $(0, 0, 0, \ldots) \in R$, we know that $R \neq \varnothing$, and hence the above conditions suffice to show that R is a subring, hence a ring, of $\prod_{i\in I} R_i$.

If R did have an identity, then it would have to be that inherited from $\prod_{i\in I} R_i$, which is clearly $(1, 1, 1, \ldots)$, the infinite sequence consisting of only the identity elements of each copy of $\mathbb{Z}$. However, it is clear that $(1, 1, 1, \ldots) \notin R$, for none of its components are 0. Hence R has no identity. ■

Exercise 7.1.21

Exercise 7.1.22 Given an example of an infinite Boolean ring.

Proof. Consider the set of natural numbers $\mathbb{N}$. Note that $\mathcal{P}(\mathbb{N})$ is an infinite set, as there are infinitely many subsets of $\mathbb{N}$. From Exercise 7.1.21 above, we know that since $\mathbb{N} \neq \emptyset$, then $\mathcal{P}(\mathbb{N})$ is a ring with addition given by symmetric difference and multiplication given by intersection. From part (b) of Exercise 7.1.21, this ring is Boolean. ∎

Exercise 7.1.23

Exercise 7.1.24

Exercise 7.1.25

Exercise 7.1.26 Let K be a field. A discrete valuation on K is a function $\nu : K^\times \to \mathbb{Z}$ satisfying:

(i) $\nu(ab) = \nu(a) + \nu(b)$ (i.e., ν is a homomorphism from the multiplicative group of nonzero elements of K to $\mathbb{Z}$),

(ii) ν is surjective, and

(iii) $\nu(x + y) \geq \min\{\nu(x), \nu(y)\}$ for all $x, y \in K^\times$ with $x + y \neq 0$.

The set $R = \{x \in K^\times \mid \nu(x) \geq 0\} \cup \{0\}$ is called the valuation ring of ν.

(a) Prove that R is a subring of K which contains the identity. (In general, a ring R is called a discrete valuation ring if there is some field K and some discrete valuation ν on K such that R is the valuation ring of ν.)

(b) Prove that for each nonzero element $x \in K$ either x or x^{-1} is in R.

(c) Prove that an element x is a unit in R if and only if $\nu(x) = 0$.

Proof. (a) Clearly we have $R \subseteq K$ by construction. We prove that R is a subgroup of K under addition. Clearly $0 \in R$ so that $R \neq \emptyset$. Suppose $x, y \in R$. Then $\nu(x), \nu(y) \geq 0$. Note $\nu(x - y) \geq \min\{\nu(x), \nu(-y)\}$ by condition (ii). To show $\nu(x - y) \geq 0$ we need only prove that $\nu(-y) \geq 0$. We make the quick remark that by condition (i) we have:

$$0 = \nu(1) = \nu(-1 \cdot -1) = \nu(-1) + \nu(-1)$$

which implies $\nu(-1) = -\nu(-1)$, and thus $\nu(-1) = 0$ is forced. With this in mind, we have:

$$\nu(-y) = \nu(-1 \cdot y) = \nu(-1) + \nu(y) = \nu(y) \geq 0$$

since $y \in R$. Therefore we have $\nu(-y) \geq 0$ and so $-y \in R$ follows. Thus by the above we have $\nu(x - y) \geq 0$, and so $x - y \in R$. By the subgroup criterion, R is a subgroup of K. Now we prove that R is closed under multiplication. Suppose $x, y \in R$. Then $\nu(x), \nu(y) \geq 0$. We have $\nu(xy) = \nu(x) + \nu(y) \geq 0$ and so $xy \in R$ as well. Hence R is a subring of K, with identity as noted above.

(b) Let $x \in K^\times$. Either $\nu(x) \geq 0$ or $\nu(x) < 0$. We know that

$$0 = \nu(1) = \nu(xx^{-1}) = \nu(x) + \nu(x^{-1})$$

which implies $\nu(x) = -\nu(x^{-1})$. Thus if $\nu(x) < 0$ we have $\nu(x^{-1}) > 0$ and so $x^{-1} \in R$ while $x \notin R$. In the other case, if $\nu(x) \geq 0$ then $\nu(x^{-1}) \leq 0$, and so if the inequality is strict we have $x \in R$ while $x^{-1} \notin R$. If $\nu(x) = \nu(x^{-1}) = 0$ then both $x, x^{-1} \in R$.

(c) Suppose $x \in R$ is a unit. That is, there exists $y \in R$ for which $xy = yx = 1$. Thus $\nu(x) + \nu(y) = 0$ by condition (i) and so $\nu(x) = -\nu(y)$, but since $x, y \in R$ we have $\nu(x), \nu(y) \geq 0$ and so $\nu(x) = 0$ is required. Conversely, if $\nu(x) = 0$, then by part (b) we have $x, x^{-1} \in R$ so that clearly x is a unit in R. ■

Exercise 7.1.27 A specific example of a discrete valuation ring (cf. the preceding exercise) is obtained when p is a prime and $K = \mathbb{Q}$ and

$$\nu_p : \mathbb{Q}^\times \to \mathbb{Z} \text{ by } \nu_p(\frac{a}{b}) = \alpha \text{ where } \frac{a}{b} = p^\alpha \frac{c}{d} \;\; p \nmid c \text{ and } p \nmid d$$

>Prove that the corresponding valuation ring R is the ring of all rational numbers whose denominators are relatively prime to p. Describe the units of this valuation ring.

Proof. With valuation ν_p defined above, we may recall that the valuation ring of ν_p on $\mathbb{Q}$ as: $R = \{x \in \mathbb{Q}^\times \mid \nu_p(x) \geq 0\} \cup \{0\}$. Suppose $a/b \in \mathbb{Q}$ where $p \nmid b$. Some power of p, perhaps p^0, divides a, and so we may write $a = p^\alpha c$ for some $\alpha \geq 0$ and $c \in \mathbb{Z}$ such that $p \nmid c$. Then

$$\frac{a}{b} = p^\alpha \frac{c}{b}$$

which implies that $\nu_p(a/b) = \alpha \geq 0$. Thus $a/b \in R$. In particular, every rational number with denominator relatively prime to p is contained in R. We show the converse. Suppose $a/b \in R$. Without loss of generality, we may assume that a/b is in lowest terms, i.e., that a and b share no common factors. Then $\nu_p(a/b) = \alpha \geq 0$, and so there exist $c, d \in \mathbb{Z}$ such that $p \nmid c, d$ and:

$$\frac{a}{b} = p^\alpha \frac{c}{d}$$

Multiplying out the above equation, we obtain:

$$ad = p^\alpha bc$$

In particular, since d is not divisible by p, it follows that $p^\alpha \mid a$. If $\alpha = 0$ then $a = d$ and $b = c$ and $p \nmid a, b$ by the construction of the valuation. Otherwise, $\alpha > 1$ and since $p \mid a$ the assumption that a and b share no common factors implies $p \nmid b$. In either case, the denominator of a/b and p are relatively prime, proving the reverse inclusion above.

Recall from Exercise 7.1.26 that the units of R are those $x \in \mathbb{Q}^\times$ for which $\nu_p(x) = 0$. As mentioned above, if $x = a/b$ and $\nu_p(a/b) = 0$ then (assuming lowest terms; no common factors):

$$\frac{a}{b} = p^0 \frac{c}{d} \implies c = a, b = d$$

and so $p \nmid a, b$. Thus the units of R are those elements of $\mathbb{Q}^\times$ for which the numerator and denominator are relatively prime to p. ■

Exercise 7.1.28 Let R be a ring with $1 \neq 0$. A nonzero element a is called a left zero divisor in R if there is a nonzero element $x \in R$ such that $ax = 0$. Symmetrically, $b \neq 0$ is a right zero divisor if there is a nonzero $y \in R$ such that $yb = 0$ (so a zero divisor is an element which is either a left or a right zero divisor). An element $u \in R$ has a left inverse in R if there is some $s \in R$ such that $su = 1$. Symmetrically, v has a right inverse if $vt = 1$ for some $t \in R$.
(a) Prove that u is a unit if and only if it has both a right and a left inverse (i.e., u must have a two-sided inverse).
(b) Prove that if u has a right inverse then u is not a right zero divisor.
(c) Prove that if u has more than one right inverse then u is a left zero divisor.
(d) Prove that if R is a finite ring then every element that has a right inverse is a unit (i.e., has a two-sided inverse).

Proof. (a) If $u \in R$ is a unit then there exists $b \in R \setminus \{0\}$ such that $bu = ub = 1$. In particular, b is both a right and a left inverse for u by definition. Conversely, if u has a left inverse b and a right inverse c, then:

$$b = b \cdot 1 = b \cdot uc = b(uc) = (bu)c = 1 \cdot c = c$$

so that $b = c$ is required. In particular, u has a 2-sided inverse, and hence is a unit.

(b) Suppose u has a right inverse $b \in R \setminus \{0\}$. This means $ub = 1$. Now suppose, for contradiction, that u is a right zero divisor. Then there exists $\lambda \in R \setminus \{0\}$ such that $u\lambda = 0$. Now observe:

$$b = b \cdot 1 + b \cdot 0 = b(1 + 0) = b(1 + u\lambda) = b + bu\lambda = b + \lambda$$

Subtracting both sides of the above equation by b, we obtain $\lambda = 0$. This is a contradiction. Therefore u is not a right zero divisor.

(c) Let b be a right inverse of an element $u \in R \setminus \{0\}$. Suppose b' is another right inverse for u such that $b \neq b'$. We have $ub = 1$ and $ub' = 1$. Observe:

$$u(b - b') = ub - ub' = 1 - 1 = 0$$

Since $b \neq b'$ by assumption, we know $b - b' \neq 0$. Therefore u is a left zero divisor in R, specifically for the non-zero element $b - b' \in R$.

(d) Let R be a finite ring, Suppose $u \in R$ has a right inverse, say b. From part (a) above we know that this fact implies u is not a right zero divisor. In particular, there exists no element $x \in R \setminus \{0\}$ for which $xu = 0$. As such, the multiplication map $\varphi : R \to R$ defined by $\varphi(x) = xu$ for all $x \in R$ is injective (if $\varphi(y) = 0$ then $yu = 0$ and so $y = 0$ is forced). Since R is finite, this map φ is surjective as well. Thus there exists some $y \in R \setminus \{0\}$ for which $\varphi(y) = 1$, so that $yu = 1$. In other words, u has a left inverse y. In particular, u has both a left and right inverse, and so by part (a) above u is a unit, and so $y = b$ is a 2-sided inverse for u, as desired. ■

Exercise 7.1.29 Let A be any commutative ring with identity $1 \neq 0$. Let R be the set of all group homomorphisms of the additive group A to itself with addition defined as pointwise addition of functions and multiplication defined as function composition. Prove that these operations make R into a ring with identity. Prove that the units of R are the group automorphisms of A (cf. Exercise 20, Section 1.6).

Proof. Let A be a commutative ring with $1 \neq 0$, with R the set of group homomorphisms from A to itself. If f and g are group homomorphisms of A into itself, then $f + g$ is also such a homomorphism (likewise $g + f$ by the commutativty of addition in A). Associativity follows from the associativity of addition in A. Inverses are given by $-f$ for all such $f \in R$. The additive identity of R is the trivial homomorphism of A into itself. These facts ensure that $(R, +)$ is an abelian group. Associativity of function composition is a direct consequence of the associativity of composition of group homomorphisms. The rest is pretty clear.

Note that the units of R are group homomorphisms which have 2-sided inverses as per Exercise 7.1.28(a). A group homomorphism with a 2-sided inverse is a bijection, thus an isomorphism from A to itself. These are precisely the automorphisms of A. Conversely, any such automorphism is clearly a unit in R. This completely characterizes the units in this ring R. ■

Exercise 7.1.30 Let $A = \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} \times \cdots$ be the direct product of copies of $\mathbb{Z}$ indexed by the positive integers (so A is a ring under componentwise addition and multiplication) and let R be the ring of all group homomorphisms from A to itself as described in the preceding exercise. Let φ be the element of R defined by $\varphi(a_1, a_2, a_3, \ldots) = (a_2, a_3, \ldots)$. Let ψ be the element of R defined by $\psi(a_1, a_2, a_3, \ldots) = (0, a_1, a_2, a_3, \ldots)$.
(a) Prove that $\varphi\psi$ is the identity of R but $\psi\varphi$ is not the identity of R (i.e., ψ is a right inverse for φ but not a left inverse).
(b) Exhibit infinitely many right inverses for φ.
(c) Find a nonzero element π of R such that $\varphi\pi = 0$ but $\pi\varphi \neq 0$. >(d) Prove that there is no nonzero element $\lambda \in R$ such that $\lambda\varphi = 0$ (i.e., φ is a left zero divisor but not a right zero divisor).

Proof. (a) First we show directly that $\varphi\psi$ is the identity of R. To do this, note:

$$\varphi(\psi(a_1, a_2, a_3, \ldots)) = \varphi(0, a_1, a_2, a_3, \ldots) = (a_1, a_2, a_3, \ldots)$$

for any such element of A; thus ψ is a right inverse for φ. To see that $\psi\varphi$ is not the identity, note:

$$\psi(\varphi(a_1, a_2, a_3, \ldots)) = \psi(a_2, a_3, \ldots) = (0, a_2, a_3, \ldots)$$

and so clearly $\psi\varphi$ does not fix every element of A; hence ψ is not a left inverse for φ.

(b) Define $\Psi_a(a_1, a_2, a_3, \ldots) = (a, a_1, a_2, a_3, \ldots)$ for all $a \in \mathbb{Z}$. The collection $\{\Psi_a\}_{a\in\mathbb{Z}}$ is infinite. It is clear that each such Ψ_a is a group homomorphism of A. Also, we have:

$$\varphi(\Psi_a(a_1, a_2, a_3, \ldots)) = \varphi(a, a_1, a_2, a_3, \ldots) = (a_1, a_2, a_3, \ldots)$$

and so $\varphi\Psi_a$ fixes all elements of A, to which $\varphi\Psi_a = 1$, and so Ψ_a are right inverses for φ, and there are infinitely many.

(c) Consider π defined by $\pi(a_1, a_2, a_3, \ldots) = (a_1, 0, 0, \ldots)$, the projection onto the first component of A, which is clearly a group homomorphism of A, and so lies in R. We have $\pi \neq 0$, and clearly:

$$\varphi(\pi(a_1, a_2, a_3, \ldots)) = \varphi(a_1, 0, 0, \ldots) = (0, 0, 0, \ldots) = 0$$

so that π is a right zero divisor of φ. We also have:

$$\pi(\varphi(a_1, a_2, a_3, \ldots)) = \pi(a_2, a_3, \ldots) = (a_2, 0, 0, \ldots) \neq 0$$

and so $\pi\varphi \neq 0$ holds. In particular, π is not a left zero divisor for φ.

(d) To rule out the existence of a non-zero element $\lambda \in R$ for which $\lambda\varphi = 0$; equivalently, to prove that φ is not a right zero divisor, refer to Exercise 7.1.28(b). Since in part (b) above we exhibited infinitely many right inverse for φ, this exercise asserts that φ is not a right zero divisor, which is the desired statement. Thus no such λ exists. ∎

7.2 Examples: Polynomial Rings, Matrix Rings, and Group Rings

Exercise 7.2.1

Exercise 7.2.2

Exercise 7.2.3

Exercise 7.2.4

Exercise 7.2.5

Exercise 7.2.6

Exercise 7.2.7

Exercise 7.2.8

Exercise 7.2.9

Exercise 7.2.10

Exercise 7.2.11

Exercise 7.2.12

Exercise 7.2.13

7.3 Ring Homomorphisms and Quotient Rings

Exercise 7.3.1. Prove that the rings $2\mathbb{Z}$ and $3\mathbb{Z}$ are not isomorphic.

Proof. ■

Exercise 7.3.2

Exercise 7.3.3

Exercise 7.3.4

Exercise 7.3.5

Exercise 7.3.6

Exercise 7.3.7

Exercise 7.3.8

Exercise 7.3.9

Exercise 7.3.10

Exercise 7.3.11

Exercise 7.3.12

Exercise 7.3.13

Exercise 7.3.14

Exercise 7.3.15

Exercise 7.3.16

Exercise 7.3.17

Exercise 7.3.18

Exercise 7.3.19

Exercise 7.3.20

Exercise 7.3.21

Exercise 7.3.22. Let a be an element of the ring R.
(a) Prove that $\{x \in R \mid ax = 0\}$ is a right ideal and $\{y \in R \mid ya = 0\}$ is a left ideal (called respectively the right and left *annihilators* of a in R).
(b) Prove that if L is a left ideal of R then $\{x \in R \mid xa = 0 \text{ for all } a \in L\}$ is a two-sided ideal (called the left *annihilator* of L in R).

Proof. (a) Fix $a \in R$ and let $A_r = \{x \in R \mid ax = 0\}$. Note $A_r \neq \varnothing$ since $a0 = 0$ means $0 \in A_r$. Now, if $x, x' \in A$ then $ax = 0$ and $ax' = 0$, and hence by the distributive property we have $a(x - x') = ax - ax' = 0 - 0 = 0$ to whuch $x - x' \in A_r$. Thus A_r is a subgroup of R. Let $r \in R$ be arbitrary; we have $a(xr) = (ax)r = 0r = 0$ and hence $xr \in A_r$, meaning that $A_rR \subseteq A_r$ and so A_r is a right ideal of R.

Let $A_l = \{y \in R \mid ya = 0\}$. Then $0a = 0$ so $0 \in A_l \neq \varnothing$, and again if $y, y' \in A_l$ then $(y - y')a = ya - y'a = 0 - 0 = 0$ via the distributive property, giving $y - y' \in A_l$. If $r \in R$ then $(ry)a = r(ya) = r0 = 0$ and so $RA_l \subseteq A_l$, and A_l is a left ideal of R.

(b) Let L be a left ideal of R. Let $\text{Ann}(L) = \{x \in R \mid xa = 0 \text{ for all } a \in L\}$. We know that $0a = 0$ for all $a \in R$ and so $0 \in \text{Ann}(L) \neq \emptyset$. Taking $x, x' \in \text{Ann}(L)$ means $xa = 0$ and $x'a = 0$ for all $a \in L$, and so $(x - x')a = xa - x'a = 0$ gives $x - x' \in \text{Ann}(L)$, proving that $\text{Ann}(L)$ is a subgroup of R by the subgroup criterion.

Now let $r \in R$ be arbitrary and suppose $x \in \text{Ann}(L)$. Then $(rx)a = r(xa) = r0 = 0$ proves that $rx \in \text{Ann}(L)$ and hence that $R\text{Ann}(L) \subseteq \text{Ann}(L)$. Similarly, we have that $(xr)a = x(ra) = 0$ since $ra \in L$ since L was assumed a left ideal of R, and x kills every element of L. Thus $xr \in \text{Ann}(L)$ proves that $\text{Ann}(L)R \subseteq \text{Ann}(L)$. Therefore we may conclude that $\text{Ann}(L)$ is a two-sided ideal of R, as desired. ■

Exercise 7.3.23

Exercise 7.3.24

Exercise 7.3.25

Exercise 7.3.26

Exercise 7.3.27

Exercise 7.3.28

Exercise 7.3.29. Let R be a commutative ring. Recall (cf. Exercise 13, Section 1) that an element $x \in R$ is nilpotent if $x^n = 0$ for some $n \in \mathbb{Z}^+$. Prove that the set of all nilpotent elements form an ideal — called the *nilradical* of R and denoted by $\mathfrak{N}(R)$. [Use the Binomial Theorem to show $\mathfrak{N}(R)$ is called under addition.]

Proof. We must prove that $\mathfrak{N}(R)$ is a additive subgroup of R which is closed under multiplication, and we must show that $x\mathfrak{N}(R) \subseteq \mathfrak{N}(R)$ for all $x \in R$.

First we show that $\mathfrak{N}(R)$ is closed under multiplication. Take $x, y \in \mathfrak{N}(R)$, so that there exists $n, m \in \mathbb{Z}^+$ for which $x^n = 0$ and $y^m = 0$. Clearly we have

$$(xy)^n = x^n y^n = 0y^n = 0$$

and hence $xy \in \mathfrak{N}(R)$ holds.

Now we prove closure under addition: by the Binomial Theorem, Exercise 7.3.25, we have that

$$\begin{aligned}
(x + y)^{n+m} &= \sum_{i=0}^{n+m} \binom{n+m}{i} x^i y^{n+m-i} \\
&= \sum_{i=0}^{n+m} \binom{n+m}{i} x^i y^n y^m y^{-i} \\
&= \sum_{i=0}^{n+m} \binom{n+m}{i} x^i y^n 0 y^m y^{-i} \\
&= 0
\end{aligned}$$

Hence $x + y \in \mathfrak{N}(R)$ holds. Closure under additive inverses is trivial to see; thus $\mathfrak{N}(R)$ is an additive subgroup of R which is closed under multiplication.

Finally, if $r \in R$ and $x \in \mathfrak{N}(R)$, with $n \in \mathbb{Z}^+$ such that $x^n = 0$, then clearly $(rx)^n = r^n x^n = r^n 0 = 0$ holds, to which $rx \in \mathfrak{N}(R)$; hence $\mathfrak{N}(R)$ is an ideal of R. ■

Exercise 7.3.30. Prove that if R is a commutative ring and $\mathfrak{N}(R)$ is its nilradical (cf. the preceding exercise) then zero is the only nilpotent element of $R/\mathfrak{N}(R)$ i.e., prove that $\mathfrak{N}(R/\mathfrak{N}(R)) = 0$.

Proof. If $\overline{x}$ is a nilpotent element of $R/\mathfrak{N}(R)$ then there exists $n \in \mathbb{Z}^+$ for which $(\overline{x})^n = \overline{0}$, so equivalently $\overline{x^n} = \overline{0}$, hence $x^n \in \mathfrak{N}(R)$. Thus x^n lies in the nilradical of R, hence is a nilpotent element of R. Thus there exists $m \in \mathbb{Z}^+$ for which $(x^n)^m = 0$. But since $(x^n)^m = x^{nm}$, this means for $k = nm$ we have $x^k = 0$. Therefore x is a nilpotent element of R, hence lies in the nilradical, hence $\overline{x} = \overline{0}$. Thus the only nilpotent element of $R/\mathfrak{N}(R)$ is zero. ■

Exercise 7.3.31. Prove that the elements $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ and $\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$ are nilpotent elements of $M_2(\mathbb{Z})$ whose sum is not nilpotent (note that these two matrices do not commute). Deduce that the set of nilpotent elements in the noncommutative ring $M_2(\mathbb{Z})$ is not an ideal.

Proof. We just need to show that some power of the two matrices above equals the zero matrix. So for the first, we note that

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}^2 = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

and for the second matrix, we have

$$\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}^2 = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

Thus these two matrices are indeed nilpotents in $M_2(\mathbb{Z})$. Note that

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

We claim that the matrix on the right hand side of the above equation is not nilpotent in $M_2(\mathbb{Z})$. To see this, observe that

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \mathcal{I}_2$$

where $\mathcal{I}_2$ is the 2×2 identity matrix. Now, for any $n \in \mathbb{Z}^+$, either n is even or n is odd. If n is even, then $n = 2k$ for some k, and so

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^n = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^{2k} = \left(\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^2\right)^k = \mathcal{I}_2^k = \mathcal{I}_2 \neq O$$

In the other case, when n is odd, we have $n = 2k+1$ for some k, and so

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^n = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^{2k+1} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^{2k} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \mathcal{I}_2 \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \neq O$$

Therefore, in any case, the sum of the two matrices in the problem description is not nilpotent; hence the nilradical of a noncommutative ring need not be closed under addition, hence is not necessarily an ideal. ■

Exercise 7.3.32. Let $\varphi : R \to S$ be a homomorphism of rings. Prove that if x is a nilpotent element of R then $\varphi(x)$ is a nilpotent in S.

Proof. If x is a nilpotent element of R then there exists $n \in \mathbb{Z}^+$ such that $x^n = 0$. Since φ is a ring homomorphism, we know $\varphi(x)^n = \varphi(x^n) = \varphi(0) = 0$; hence $\varphi(x)$ is a nilpotent element of S. ■

Exercise 7.3.33

Exercise 7.3.34

Exercise 7.3.35

Exercise 7.3.36. Show that if I is the ideal of all polynomials in $\mathbb{Z}[x]$ with zero constant term then $I^m = \{a_n x^n + a_{n+1}x^{n+1} + \cdots + a_{n+m}x^{n+m} \mid a_i \in \mathbb{Z}, m \geq 0\}$ is the set of polynomials whose first nonzero term has degree at least n.

Proof. One inclusion is immediate and the other follows quite easily. ■

Exercise 7.3.37. An ideal N is called *nilpotent* if N^n is the zero ideal for some $n \geq 1$. Prove that the ideal $p\mathbb{Z}/p^m\mathbb{Z}$ is a nilpotent ideal in the ring $\mathbb{Z}/p^m\mathbb{Z}$.

Proof. Note that $(p\mathbb{Z}/p^m\mathbb{Z})^m = p^m\mathbb{Z}/p^m\mathbb{Z} = 0$. In other words, since we may equivalently write (p) for the ideal $p\mathbb{Z}/p^m\mathbb{Z}$, it is obvious that $(p)^m = (p^m) = (0)$ since the integer p^m is clearly congruent to 0 modulo p^m. ■

7.4 Properties of Ideals

Exercise 7.4.1.

Exercise 7.4.2.

Exercise 7.4.3.

Exercise 7.4.4. Assume R is commutative. Prove that R is a field if and only if 0 is a maximal ideal.

Proof. For the forward direction, assume R is a field. The, since R is commutative, we know (via Proposition 9(2)) the only ideals of R are 0 and R. Since $0 \neq R$ and the only ideals containing 0 are 0 and R (indeed these are the only ideals of R), 0 is by definition of a maximal ideal.

Conversely, if 0 is a maximal ideal, and I is any non-zero, proper ideal of R, then there exists some element $x \in I$, and $0x = 0 \in I$ by ideal properties of I, hence I is an ideal containing 0, hence $I = 0$ or $I = R$ holds since 0 is maximal. But I is both non-zero and proper by assumption; contradiction. ∎

Exercise 7.4.5. Prove that if M is an ideal such that R/M is a field then M is a maximal ideal (do not assume R is commutative).

Proof. Let M be an ideal of R and suppose R/M is a field. Suppose that I is an ideal of R containing M. If $M = I$ we are done, so assume $M \neq I$, so $M \subset I$. Then there exists some $x \in I$ such that $x \notin M$.

Since, in particular, we have $x \in I \subseteq R$, passing to the quotient we have the equivalence class $\overline{x} \in R/M$, and we know that $\overline{x} \neq \overline{0}$ since $x \notin M$. Thus $\overline{x}$ is a non-zero element of a field, hence has a multiplicative inverse $\overline{y} \in R/M$ such that $\overline{xy} = \overline{1}$, to which $\overline{1 - xy} = \overline{0}$. This means that $1 - xy \in M$ holds. Since $M \subset I$, we also have $1 - xy \in I$.

Since $x \in I$ by our assumption above, and since I is an ideal of R, we know that $xy \in I$ by closure. Note, however, that $1 - xy$ and xy both lie in I, and so too must their sum: $xy + (1 - xy) = xy + 1 - xy = 1 \in I$. Thus $I = R$ holds.

Therefore the only ideals of R which contain M are M itself and R; in other words, M is a maximal ideal of R, as desired. ∎

Exercise 7.4.6. Prove that R is a division ring if and only if its only left ideals are (0) and R. (The analogous result holds when "left" is replaced by "right.")

Proof. If R is a division ring, and I is some non-zero left ideal of R, then there exists some non-zero element $x \in I$. Since R is a division ring, x has a non-zero inverse, say given by y. Thus $yx = 1 \in I$ by closure under left multiplication. Hence $I = R$ holds.

Conversely, assume the only left ideals of R are (0) and R itself. For any nonzero element $x \in R$, we know (x) is an ideal of R. Hence either $(x) = (0)$ or $(x) = R$. The former case is impossible for we took $x \neq 0$. Thus $(x) = R$ holds. In particular, since $1 \in R$, there exists some $y \in R$ such that $yx = 1$ holds. This y is precisely a multiplicative inverse for x; since x was arbitrary in R, we conclude that R is a division ring. ■

Exercise 7.4.7. Let R be a commutative ring with 1. Prove that the principal ideal generated by x in the polynomial ring $R[x]$ is a prime ideal if and only if R is an integral domain. Prove that (x) is a maximal ideal if and only if R is a field.

Proof. Let R be a commutative ring with 1 and consider the polynomial ring $R[x]$. If the ideal (x) of $R[x]$ is a prime ideal, then $R[x]/(x) \cong R$ is an integral domain, adn conversely. Similarly, the ideal (x) is maximal if and only if $R[x]/(x) \cong R$ is a field, giving the statement. ■

Exercise 7.4.8 Let R be an integral domain. Prove that $(a) = (b)$ for some elements $a, b \in R$, if and only if $a = uh$ for some unit u of R.

Proof. Let R be an integral domain and suppose $(a) = (b)$ with $a, b \neq 0$. Then there exists some $r \in R$ for which $ra = b$. Likewise, there exists some $s \in R$ such that $a = sb$. Now, substituting, we have that $r(sb) = b$, and hence that $(rs)b = b$. Subtracting yields

$$(rs)b - b = 0 \iff (rs - 1)b = 0$$

and since R is an integral domain, and $b \neq 0$ by assumption, we require $rs = 1$. We can perform an analagous computation with a, noting that $a = sb$ implies $a = s(ra)$ and so

$$(sr)a - a = 0 \iff (sr - 1)a = 0$$

and since $a \neq 0$ in the integral domain R, we have $sr - 1 = 0$, so $sr = 1$. But the fact that $rs = sr = 1$ means that s and r are inverses, units, and so $a = ub$ must hold, where we have taken $u = s$, a unit. ■

Exercise 7.4.9 Let R be the ring of all continuous functions on $[0, 1]$ and let I be the collection of all functions $f(x)$ in R with $f(1/3) = f(1/2) = 0$. Prove that I is an ideal of R but is not a prime ideal.

Proof. Let $f(x)$ in R be arbitrary, and suppose that $g(x) \in I$. Consider the product $f(x)g(x)$. Evaluating at $x = 1/3$ we obtain that

$$f(1/3)g(1/3) = f(1/3) \cdot 0 = 0$$

$$f(1/2)g(1/2) = f(1/2) \cdot 0 = 0$$

and hence $f(x)g(x) \in I$ must hold. A similar computation shows that I is closed by multiplication of elements of R on the right; in particular, I is an ideal of the ring R.

Now we show that I is not a prime ideal of R by example. Consider $f(x) = x - 1/3$ and $g(x) = x - 1/2$, both of which are clearly elements of R, since they are polynomials, which are necessarily continuous on $[0, 1]$. Note that

$$f(x)g(x) = (x - 1/3)(x - 1/2)$$

and clearly evaluating gives $f(1/3)g(1/3) = 0 \cdot (1/3 - 1/2) = 0$ and $f(1/2)g(1/2) = (1/2 - 1/3) \cdot 0 = 0$. In particular, the product $f(x)g(x) \in I$, however neither $f(x)$ nor $g(x)$ lie in I, as $f(1/3) = 0 \neq f(1/2) = 1/2 - 1/3$. Likewise for $g(x)$. Therefore I cannot be a prime ideal of R. ■

Exercise 7.4.10 Assume R is commutative. Prove that if P is a prime ideal of R and P contains no zero divisors then R is an integral domain.

Proof. Let R be a commutative ring and suppose P is a prime ideal of R which contains no zero divisors. Assume, for contradiction, that $a \in R \setminus \{0\}$ is a zero divisor. Then there exists $b \in R \setminus \{0\}$ such that $ab = 0$. Since P contains 0, as all ideals must, and $ab = 0 \in P$, the fact that P is prime forces either $a \in P$ or $b \in P$. If $a \in P$ then this is a contradiction, for we assumed P contained no zero divisors. Thus it must be the case that $b \in P$, which again is a contradiction, for b is also a zero divisor. Hence no such zero divisors may exist in R, which suffices to prove that R is an integral domain. ■

Exercise 7.4.11 Assume R is commutative. Let I and J be ideals of R and assume P is a prime ideal of R that contains IJ (for example, if P contains $I \cap J$). Prove either I or J is contained in P.

Proof. Let R be a commutative ring with ideals I and J and prime ideal P. Suppose $IJ \subseteq P$. Let $ab \in IJ$ where $a \in I$ and $b \in J$. Then $ab \in P$, and hence either $a \in P$ or $b \in P$.

Without loss of generality, we consider the case where $a \in P$ and $b \notin P$. Since P is, in particular, an ideal of R, we know that $ra \in P$ for all $r \in R$, and hence all $r \in J \subseteq R$. However, this means that for any $c \in J \setminus \{0\}$ we have $ac \in IJ \subseteq P$ which means either $a \in P$ or $c \in P$. Since we already know that $a \in P$, we require $c \notin P$. Since $c \in J \setminus \{0\}$ was arbitrary, this means that P contains no elements of J besides 0.

Now fix any $c \in J$ and let $n \in I$ be arbitrary. Then $nc \in IJ \subseteq P$ and so either $n \in P$ or $c \in P$. Since $c \in J$ we know from above that $c \notin P$, and so we require $n \in P$. Since $n \in I$ was arbitrary, this suffices to prove that $I \subseteq P$.

A completely analagous process deals with the second case above where $a \notin P$ and $b \in P$, in which case we find that $J \subseteq P$ with P not containing I. Hence the statement is proved. ■

Exercise 7.4.12

Exercise 7.4.13 Let $\varphi : R \to S$ be a homomorphism of commutative rings.
(a) Prove that if P is a prime ideal of S then either $\varphi^{-1}(P) = R$ or $\varphi^{-1}(P)$ is a prime ideal of R. Apply this to the special case when R is a subring of S and φ is the inclusion homomorphism to deduce that if P is a prime ideal of S then $P \cap R$ is either R or a prime ideal of R.
(b) Prove that if M is a maximal ideal of S and φ is surjective then $\varphi^{-1}(M)$ is a maximal ideal of R. Give an example to show that this need not be the case if φ is not surjective.

Proof. (a) Suppose P is a prime ideal of S. We know from Exercise 7.3.24(a) that $\varphi^{-1}(P)$ is an ideal of R. If $\varphi^{-1}(P) = R$ then we are done, so assume this is not the case. Suppose $ab \in \varphi^{-1}(P)$ for elements $a, b \in R$. Then $\varphi(ab) = \varphi(a)\varphi(b) \in P$ and so either $\varphi(a) \in P$ or $\varphi(b) \in P$. In the first case we have that $\varphi(b) \notin P$ and hence that $b \notin \varphi^{-1}(P)$ and $a \in \varphi^{-1}(P)$. A similar computation shows that if $\varphi(a) \notin P$ and $\varphi(b) \in P$ then $a \notin \varphi^{-1}(P)$ and $b \in \varphi^{-1}(P)$. In particular, $\varphi^{-1}(P)$ is a prime ideal of R.

Now assume $R \subseteq S$ and that $\varphi : R \to S$ is the inclusion ring homomorphism. If P is a prime ideal of S, then from Exercise 7.3.24(a) and our above work we have that $P \cap R$ is a prime ideal of R.

(b) Suppose M is a maximal ideal of S and that φ is surjective. Since M is in particular a prime ideal, part (a) above gives that $\varphi^{-1}(M) = R$ or $\varphi^{-1}(M)$ is a prime ideal of R. So assume $\varphi^{-1}(M)$ is a prime ideal of R, and assume I is some ideal of R. containing $\varphi^{-1}(M)$. From Exercise 7.3.24(b) the surjectivity of φ gives that $\varphi(I)$ is an ideal of S, and we necessarily ahev that $M \subseteq \varphi(I)$ in S. Since M is maximal, we require $M = \varphi(I)$, and hence $I = \varphi^{-1}(M)$. Thus $\varphi^{-1}(M)$ is a maximal ideal of R.

For an example to show that this need not be the case when φ is not surjective, consider the inclusion ring homomorphism $\varphi : \mathbb{Q} \to \mathbb{Q}[x]$. Clearly φ is not surjective, since for instance no elements of $\mathbb{Q}$ map to x. Note that (x) is a maximal ideal of $\mathbb{Q}[x]$ since $\mathbb{Q}[x]/(x) \cong \mathbb{Q}$ is a field. However, we have that $\varphi^{-1}((x)) = \varnothing$, clearly not a maximal ideal of $\mathbb{Q}$, and not even an ideal. ■

Exercise 7.4.14

Exercise 7.4.15

Exercise 7.4.16

Exercise 7.4.17

Exercise 7.4.18

Exercise 7.4.19 Let R be a finite commutative ring with identity. Prove that every prime ideal of R is a maximal ideal.

Proof. Let R be such a finite commutative ring with 1 and suppose P is a prime ideal of R. Then R/P is an integral domain, and since R is finite so too must be R/P. Recall from Corollary 3 in Section 7.1 that any finite integral domain is a field, and so R/P must be a field, and hence P must be maximal. ■

Exercise 7.4.20.

Exercise 7.4.21.

Exercise 7.4.22.

Exercise 7.4.23. Prove that in a Boolean ring (cf. Exercise 15, Section 1) every prime ideal is a maximal ideal.

Proof. Let B be a Boolean ring and let P be a prime ideal of B. To prove that P is a maximal ideal of B, we show that the integral domain B/P is a field. So suppose $\overline{x} \in B/P$.

Recall that $x^2 = x$ holds in B since it is Boolean, hence $x^2 - x = 0$, to which $x(x-1) = 0$ holds in B. Descending to the quotient ring, we require that

$$\overline{x}(\overline{x-1}) = \overline{0}$$

hold in B/P. Since B/P is an integral domain, either $\overline{x} = \overline{0}$ or $\overline{x-1} = \overline{0}$. If $\overline{x} \neq \overline{0}$ is non-zero then $\overline{x-1} = \overline{0}$ must hold, to which $\overline{x} = \overline{1}$.

In particular, the ring B/P contains only two elements, hence must be isomorphic to the field $\mathbb{Z}/2\mathbb{Z}$, which means that P is a maximal ideal. ■

Exercise 7.4.24. Prove that in a Boolean ring every finitely generated ideal is principal.

Proof. TBD. ■

Exercise 7.4.25.

Exercise 7.4.26.

Exercise 7.4.27.

Exercise 7.4.28.

Exercise 7.4.29.

Exercise 7.4.30.

Exercise 7.4.31.

Exercise 7.4.32.

Exercise 7.4.33.

Exercise 7.4.34.

Exercise 7.4.35.

Exercise 7.4.36.

Exercise 7.4.37.

Exercise 7.4.38.

Exercise 7.4.39.

Exercise 7.4.40. Assume R is commutative. Prove that the following are equivalent: (see also Exercises 13 and 14 in Section 1)
(i) R has exactly one prime ideal
(ii) every element of R is either nilpotent or a unit
(iii) $R/\mathfrak{N}(R)$ is a field (cf. Exercise 29, Section 3).

Proof. (i) $\implies$ (ii). Any element $x \in R$ is either a unit or a non-unit. If x is a unit, we are done, so assume x is a non-unit. Then we know that the ideal (x) is a proper ideal of R, since $(x) \neq (1) = R$, and hence by Proposition 11 we know (x) is contained in a maximal ideal of R, say $\mathfrak{m}$. But $\mathfrak{m}$ is also a prime ideal, and there is exactly one prime ideal of R, so it follows that $\mathfrak{m}$ is the unique prime ideal of R.

However, since the nilradical of R is equal to the intersection of all prime ideals of R, via Exercise 7.4.26, we know that $\mathfrak{N}(R) = \mathfrak{m}$, and hence that $x \in \mathfrak{N}(R)$, so that x is a nilpotent element of R.

(ii) $\implies$ (iii). We want to prove that $R/\mathfrak{N}(R)$ is a field; to do so, we shall prove that every non-zero element of R has a multiplicative inverse. So let $\overline{x} \in R/\mathfrak{N}(R)$ be some non-zero element. By assumption of (ii), the representative element x is nilpotent or a unit in R. In the former case, we have $x \in \mathfrak{N}(R)$, and hence that $\overline{x} = \overline{0}$ in $R/\mathfrak{N}(R)$, so this is impossible. Thus x must be a unit in R, so there exists $y \in R \setminus \{0\}$ for which $xy = 1$. Descending to the quotient, we get that $\overline{xy} = \overline{1}$. Thus $\overline{y}$ is an inverse for $\overline{x}$ in $R/\mathfrak{N}(R)$, hence this ring is a field.

(iii) $\implies$ (i). If $R/\mathfrak{N}(R)$ is a field, then $\mathfrak{N}(R)$ is a maximal ideal, hence a prime ideal. We claim that $\mathfrak{N}(R)$ is the unique prime ideal of R. Assume we have some other prime ideal P of R. Since the nilradical is contained in the intersection of all prime ideals of R, we require that $\mathfrak{N}(R) \subseteq P$, but since $\mathfrak{N}(R)$ is maximal, this means $\mathfrak{N}(R) = P$. Thus R has exactly one prime ideal. ∎

Exercise 7.4.41. A proper ideal Q of the commutative ring R is called *primary* if whenever $ab \in Q$ and $a \notin Q$ then $b^n \in Q$ for some positive integer n. (Note that the symmetry between a and b in this definition implies that if Q is a primary ideal and $ab \in Q$ with neither a nor b in Q, then a positive power of a and a positive power of b both lie in Q.) Establish the following facts about primary ideals.
(a) The primary ideals of $\mathbb{Z}$ are 0 and (p^n) where p is a prime and n is a positive integer.
(b) Every prime ideal of R is a primary ideal.
(c) An ideal Q of R is primary if and only if every zero divisor in R/Q is a nilpotent element of R/Q.
(d) If Q is a primary ideal then rad(Q) is a prime ideal (cf. Exercise 30).

Proof. (a) TBD.

(b) Let P be a prime ideal of R. Suppose $ab \in P$ with $a \notin P$. By definition of a prime ideal, either a or b lies in P, and since a does not lie in P, we require that $b \in P$; hence P is a primary ideal.

(c) Suppose Q is a primary ideal of R and let $\overline{x} \neq \overline{0}$ be a zero divisor of R/Q. Since $\overline{x}$ is a zero divisor, there exists some non-zero $\overline{y}$ in R/Q such that $\overline{xy} = \overline{0}$, which means that $xy \in Q$. Since $xy \in Q$, and $y \notin Q$ (by the assumption that $\overline{y} \neq \overline{0}$), the fact that Q is primary means $x^n \in Q$ for some $n \in \mathbb{Z}^+$. But this means $\overline{x}$ is a nilpotent element of R/Q, since $\overline{x}^n = \overline{0}$. Thus every zero divisor in R/Q is nilpotent.

Conversely, if every zero divisor in R/Q is nilpotent, and we have $ab \in Q$ with $a \notin Q$, then $\overline{b}$ is a zero divisor in R/Q since $\overline{ab} = \overline{0}$ with $\overline{a} \neq \overline{0}$, hence $\overline{b}$ nilpotent, so $\overline{b}^n = \overline{0}$ for some $n \in \mathbb{Z}^+$, hence $b^n \in Q$; therefore Q is a primary ideal, proving the converse statement.

(d) Suppose Q is a primary ideal. Our claim is that rad(Q) is a prime ideal. So suppose $xy \in \text{rad}(Q)$. Then there exists $n \in \mathbb{Z}^+$ such that $(xy)^n = x^n y^n \in Q$. There are two cases: either both of x^n and y^n lie in Q, or at least one of them does not. In the former case, that is, when $x^n, y^n \in Q$, then clearly $x, y \in \text{rad}(Q)$ holds.

Thus we consider the latter case: assume that $x^n \notin Q$. Since Q is a primary ideal, there exists some $m \in \mathbb{Z}^+$ for which $(y^n)^m = y^{nm} \in Q$, which means $y \in \text{rad}(Q)$.

The case where $y^n \notin Q$ is dealt with in an entirely symmetric argument, and yields that $x \in \text{rad}(Q)$.

In particular, in all cases above, we have either $x \in \text{rad}(Q)$ or $y \in \text{rad}(Q)$. This means, by definition, that $\text{rad}(Q)$ is a prime ideal of R. ■

7.5 Rings of Fractions

Exercise 7.5.1.

Exercise 7.5.2.

Exercise 7.5.3. Let F be a field. Prove that F contains a unique smallest subfield F_0 and that F_0 is isomorphic to either $\mathbb{Q}$ or $\mathbb{Z}/p\mathbb{Z}$ for some prime p (F_0 is called the *prime subfield* of F). [See Exercise 26, Section 3.]

Proof. Take F a field. We know, in particular, that F is a commutative ring with identity $1 \neq 0$. As such, Exercise 7.3.26 applies, wherein we met a ring homomorphism $\phi : \mathbb{Z} \to F$ defined by $\phi(n) = n$ for all integers n. There are two cases: either ϕ is injective or ϕ is not injective.

In the latter case, we know that $\ker \phi$ is an ideal of $\mathbb{Z}$, hence of the form $n\mathbb{Z}$ for some n. It thus follows by the first isomorphism theorem for rings that $\mathbb{Z}/n\mathbb{Z} \cong \phi(\mathbb{Z})$, where $\phi(\mathbb{Z})$ is a subring of the field F, hence $\phi(Z)$ is an integral domain, hence $n\mathbb{Z}$ is a prime ideal of $\mathbb{Z}$, hence $n = p$ for some prime p (since all prime ideals of $\mathbb{Z}$ are of this form). Now $F_0 := \phi(\mathbb{Z}) \cong \mathbb{Z}/p\mathbb{Z}$ is a subfield of F, and is indeed the unique smallest subfield of F for the only subfield of F_0 is itself.

In the former case, that is, when ϕ is injective, we have that $\mathbb{Z} \cong \phi(\mathbb{Z})$, so that $\mathbb{Z}$ is isomorphic to a subring of the field F. Since $\mathbb{Z}$ is an integral domain with field of fractions $\mathbb{Q}$, Corollary 16 applies, so the subring of F generated by $\phi(\mathbb{Z})$ is isomorphic to $\mathbb{Q}$, hence $F_0 := \mathbb{Q}$ is a subfield of F, and is indeed the unique smallest subfield by the universal property in Theorem 15. ∎

Exercise 7.5.4. Prove that any subfield of $\mathbb{R}$ must contain $\mathbb{Q}$.

Proof. If F is a subfield of $\mathbb{R}$ then F is, in particular, a field. Thus by Exercise 7.5.3 above, F contains a unique smallest subfield F_0. Indeed, we know that $F_0 \not\cong \mathbb{Z}/p\mathbb{Z}$ for some prime p since if this were the case then $F_0 \subseteq \mathbb{R}$, which would mean $\mathbb{R}$ has elements of finite order, for instance 1, which is clearly absurd. Thus $F_0 \cong \mathbb{Q}$, and so F must contain (an isomorphic copy of) $\mathbb{Q}$. ∎

Exercise 7.5.5.

Exercise 7.5.6.

7.6 The Chinese Remainder Theorem

Exercise 7.6.1.

Exercise 7.6.2.

Exercise 7.6.3.

Exercise 7.6.4.

Exercise 7.6.5.

Exercise 7.6.6.

Exercise 7.6.7.

Exercise 7.6.8. Suppose for every pair of indices i, j with $i \leq j$ there is a map $\rho_{ij} : A_i \longrightarrow A_j$ such that the following hold:

i. $\rho_{jk} \circ \rho_{ij} = \rho_{ik}$ whenever $i \leq j \leq k$.

ii. $\rho_{ii} = 1$ for all $i \in I$.

Let B be the disjoint union of all the A_i. Define a relation $\sim$ on B by

$$a \sim b \;\text{ if and only if there exists } k \text{ with } i, j \leq k \text{ and } \rho_{ik}(a) = \rho_{jk}(b),$$

for $a \in A_i$ and $b \in A_j$.

(a) Show that $\sim$ is an equivalence relation on B. (The set of equivalence classes is called the direct or inductive limit of the directed system $\{A_i\}$, and is denoted $\varinjlim A_i$. In the remaining parts of this exercise let $A = \varinjlim A_i$.)

(b) Let $\overline{x}$ denote the class of x in A and define $\rho_i : A_i \longrightarrow A$ by $\rho_i(a) = \overline{a}$. Show that if each ρ_{ij} is injective, then so is ρ_i for all i (so we may then identify each A_i as a subset of A).

(c) Assume all ρ_{ij} are group homomorphisms. For $a \in A_i$, $b \in A_j$ show that the operation

$$\overline{a} + \overline{b} = \overline{\rho_{ik}(a) + \rho_{jk}(b)}$$

where k is any index with $i, j \leq k$, is well defined and makes A into an abelian group. Deduce that the maps ρ_i in (b) are group homomorphisms from A_i to A.

(d) Show that if all A_i are commutative rings with 1 and all ρ_{ij} are ring homomorphisms that send 1 to 1, then A may likewise be given the structure of a commutative ring with 1 such that all ρ_i are ring homomorphisms.

(e) Under the hypotheses in (c) prove that the direct limit has the following universal property: if C is any abelian group such that for each $i \in I$ there is a homomorphism $\varphi_i : A_i \longrightarrow C$ with $\varphi_i = \varphi_j \circ \rho_{ij}$ whenever $i \leq j$, then there is a unique homomorphism $\varphi : A \longrightarrow C$ such that $\varphi \circ \rho_i = \varphi_i$ for all i.

Proof. (a) We prove that $\sim$ is reflexive first. Take $a \in A_i$ and note that $\rho_{ii} : A_i \longrightarrow A_i$ is the identity on A_i by construction, and hence $\rho_{ii}(a) = \rho_{ii}(a)$ trivially holds, where we have taken $k = i$ and $i, i \leq k$ holds trivially. For symmetry, suppose

$a \sim b$ where $a \in A_i$ and $b \in A_j$. Then there exists an index k such that $i, j \leq k$ and $\rho_{ik}(a) = \rho_{jk}(b)$. It is obvious that we may take the same k to get $b \sim a$.

Lastly, we show that $\sim$ is transitive; assume $a \sim b$ and $b \sim c$ where $a \in A_i$, $b \in A_j$, and $c \in A_k$. By assumption, there exists an index p such that $i, j \leq p$ and $\rho_{ip}(a) = \rho_{jp}(b)$, and also there exists some index q such that $j, k \leq q$ and $\rho_{jq}(b) = \rho_{kq}(c)$. Since I is a directed set, given both $p, q \in I$ there exists some index P such that $p, q \leq P$. In particular, we now have that $j \leq p \leq P$ and that $j \leq q \leq P$, which, means that

$$(\rho_{pP} \circ \rho_{jp})(b) = \rho_{jP}(b)$$

$$(\rho_{qP} \circ \rho_{jq})(b) = \rho_{jP}(b)$$

from condition (ii) in the problem statement. Now since $i \leq p \leq P$ and $k \leq q \leq P$ must hold as well, condition (ii) once again gives

$$(\rho_{pP} \circ \rho_{ip})(a) = \rho_{iP}(a)$$

$$(\rho_{qP} \circ \rho_{kp})(c) = \rho_{kP}(c)$$

Now we use the four equalities above, combined with our equalities obtained from $a \sim b$ and $b \sim c$ to get the following string of relations

$$\begin{aligned}
\rho_{iP}(a) &= (\rho_{pP} \circ \rho_{ip})(a) \\
&= (\rho_{pP} \circ \rho_{jp})(b) \\
&= \rho_{jP}(b) \\
&= (\rho_{qP} \circ \rho_{jq})(b) \\
&= (\rho_{qP} \circ \rho_{kq})(c) \\
&= \rho_{kP}(c)
\end{aligned}$$

Therefore, since $i, k \leq P$ and we have that $\rho_{iP}(a) = \rho_{kP}(c)$, we may finally write that $a \sim c$, so that $\sim$ is transitive. With the three facts checked above, $\sim$ is an equivalence relation on B, as desired.

(b) Define $\rho_i : A_i \to \varinjlim A_i$ for all $i \in I$. Suppose that $\rho_{ij} : A_i \to A_j$ is injective for all $i, j \in I$. To prove that each ρ_i is injective, assume $\rho_i(a) = \rho_i(b)$ for $a, b \in A_i$. Then, in particular, $\overline{a} = \overline{b}$ so that a and b lie in the same coset under $\sim$ and hence $a \sim b$. Thus there exists an index k such that $i \leq k$ and $\rho_{ik}(a) = \rho_{ik}(b)$. The injectivity of ρ_{ik} was assumed, and thus $a = b$. Therefore ρ_i is injective.

(c) Define a binary operation for all $a \in A_i$ and $b \in A_j$ as follows:

$$+ : \varinjlim A_i \times \varinjlim A_i \to \varinjlim A_i$$

$$(\overline{a}, \overline{b}) := \overline{a} + \overline{b} \longmapsto \overline{\rho_{ik}(a) + \rho_{jk}(b)}$$

for any index k with $i, j \leq k$. We show that $+$ is well defined. So let $c \in A_i$ and $d \in A_j$ and assume that $(\overline{a}, \overline{b}) = (\overline{c}, \overline{d})$. Then $a \sim b$ and $b \sim d$ must hold, and hence there exists some indices p and q for which $i, j \leq p$ and $i, j \leq q$ with $\rho_{ip}(a) = \rho_{ip}(c)$ and $\rho_{jp}(b) = \rho_{jq}(d)$. Since the ρ_{ij} are group homomorphisms for all $i, j \in I$ we necessarily have that $\rho_{ip}(a - c) = 0$ and that $\rho_{jq}(d - b) = 0$.

Since I is a directed set, given $p, q \in I$ there exists some index k such that $p, q \leq k$. In particular, we know have $i \leq p \leq k$, and hence $\rho_{pk} \circ \rho_{ip} = \rho_{ik}$. Observe that

$$\begin{aligned}
\rho_{ik}(a) - \rho_{ik}(c) &= \rho_{ik}(a - c) \\
&= (\rho_{pk} \cdot \rho_{ip})(a - c) \\
&= \rho_{pk}(\rho_{ip}(a - c)) \\
&= \rho_{pk}(0) \\
&= 0
\end{aligned}$$

where the last line follows since ρ_{pk} is a group homomorphism, so must take the identity of A_i to the identity of A_k. In a completely analagous fashion, we have $j \leq q \leq k$, and hence $\rho_{qk} \circ \rho_{jq} = \rho_{jk}$, which allows us to see that

$$\begin{aligned}
\rho_{jk}(d) - \rho_{jk}(b) &= \rho_{jk}(d - b) \\
&= (\rho_{qk} \circ \rho_{jq})(d - b) \\
&= \rho_{qk}(\rho_{jq}(d - b)) \\
&= \rho_{qk}(0) \\
&= 0
\end{aligned}$$

Now we can use the two equaitons above to get $\rho_{ik}(a) - \rho_{ik}(c) = \rho_{jk}(d) - \rho_{jk}(b)$, which necessarily implies that $\rho_{ik}(a) + \rho_{jk}(b) = \rho_{ik}(c) + \rho_{jk}(d)$. Since this equality takes place in the group A_k, it is required by the well definition shown in part (b) that

$$\overline{\rho_{ik}(a) + \rho_{jk}(b)} = \overline{rho_{ik}(c) + \rho_{jk}(d)}$$

and hence the binary operation $+$ is well defined on the direct limit of $\{A_i\}$.

Using the binary operation above, it is easy to see how the direct limit forms a group. We have

$$\begin{aligned}
\overline{a} + (\overline{b} + \overline{c}) &= \overline{a} + \overline{\rho_{ik}(b) + \rho_{jk}(c)} \\
&= \overline{\rho_{lp}(a) + \rho_{kp}(\rho_{ik}(b) + \rho_{jk}(c))} \\
&= \overline{\rho_{lp}(a) + \rho_{ip}(b) + \rho_{jp}(c)} \\
&= \overline{\rho_{kp}(\rho_{lk}(a) + \rho_{ik}(b)) + \rho_{jp}(c)} \\
&= \overline{\rho_{lk}(a) + \rho_{jk}(b)} + \overline{c} \\
&= (\overline{a} + \overline{b}) + \overline{c}
\end{aligned}$$

where we have let k be an index with $i, j \leq k$ in the first line, and in the second line we have let p be an index for which $k \leq p$. From these, we have $i \leq k \leq p$ and so we get $\rho_{kp} \circ \rho_{ik} = \rho_{ip}$ and likewise since $j \leq k \leq p$ we have $\rho_{kp} \circ \rho_{jk} = \rho_{jp}$. Thus the operation is associative. Closure under inverses is easy, for $a \in A_i$ consider $-a_i \in A_i$. We get

$$\overline{a} + \overline{-a} = \overline{\rho_{ik}(a) + \rho_{ik}(-a)} = \overline{\rho_{ik}(a) - \rho_{ik}(a)} = \overline{0}$$

which follows given that ρ_{ik} is a group homomorphism. The existence of an identity element is also easily seen, simply by taking the identity the identity common to all of the A_i, which is 0. Therefore we may conclude that

$$\varinjlim A_i$$

with the binary operation + defined above forms a group, which is also abelian since each of the A_i is abelian, as can be easily seen.

With the above in mind, we can deduce that the maps from part (b) above,

$$\rho_i : A \to \varinjlim A_i$$

taking a to $\overline{a}$ are group homomorphisms, since $\rho_i(a + b) = \overline{a + b} = \overline{a} + \overline{b}$ since $a, b \in A_i$.

(d) Now assume that $\rho_{ij} : A_i \to A_j$ is a ring homomorphism for all $i, j \in I$. Given our results from part (c) above, we need only provide a multiplication map. Define, for all $a \in A_i$ and $b \in A_j$, the map

$$\cdot : \varinjlim A_i \times \varinjlim A_i \longrightarrow \varinjlim A_i$$

$$(\overline{a}, \overline{b}) := \overline{a} \cdot \overline{b} \longmapsto \overline{\rho_{ik}(a)\rho_{jk}(b)}$$

where k is any index such that $i, j \leq k$. We show that the map defined above is well defined. To this end, suppose that $(\overline{a}, \overline{b}) = (\overline{c}, \overline{d})$ for $a, c \in A_i$ and $b, d \in A_j$. Then $a \sim c$ and $b \sim d$ is implied, and thus there exists p and q in I for which $\rho_{ip}(a) = \rho_{ip}(c)$ and $\rho_{jq}(b) = \rho_{jq}(d)$.

Now, once again since I is a directed set, given $p, q \in I$ we have some index k such that $p, q \leq k$. Now since $i \leq p \leq k$ and $j \leq q \leq k$ we get $\rho_{pk} \circ \rho_{ip} = \rho_{ik}$ and $\rho_{qk} \circ \rho_{jq} = \rho_{jk}$. Our two equations now become

$$\rho_{ik}(a) = (\rho_{pk} \circ \rho_{ip})(a) = (\rho_{pk} \circ \rho_{ip})(c) = \rho_{ik}(c)$$

$$\rho_{jk}(b) = (\rho_{qk} \circ \rho_{jq})(b) = (\rho_{qk} \circ \rho_{jq})(d) = \rho_{jk}(d)$$

Which, upon multiplying together using the underlying ring structure of A_k, gives

$$\rho_{ik}(a)\rho_{jk}(b) = \rho_{ik}(c)\rho_{jk}(d)$$

and hence

$$\overline{\rho_{ik}(a)\rho_{jk}(b)} = \overline{\rho_{ik}(c)\rho_{jk}(d)}$$

which means that our multiplication map $\cdot$ is well defined, as desired. The check that $\cdot$ is associative is trivial, simply perform a similar procedure as we did in part (c). Likewise, the check that $\cdot$ and $+$ satisfy the distributive laws follows right from the underlying ring structure of the A_i.

In particular, the maps ρ_i from part (b), which we showed were group homomorphisms in part (c), now have the structure of ring homomorphisms from the multiplication we defined above.

$$\rho_i(ab) = \overline{ab} = \overline{a} \cdot \overline{b} = \rho_i(a)\rho_i(b)$$

which was the desired statement.

(e) We prove the universal property. Let C be an abelian group. Suppose that for each $i \in I$ we have homomorphism of groups $\varphi_i : A_i \to C$ with $\varphi_i = \varphi_j \circ \rho_{ij}$ whenever $i \leq j$. Consider the map

$$\varphi : \varinjlim A_i \to C$$

such that $\varphi \circ \rho_i = \varphi_i$ for all i. From part (b), for all $i \in I$ we have

$$\rho_i : A_i \to \varinjlim A_i$$

defined by $\rho_i(a) = \overline{a}$, each of which are group homomorphisms under the assumptions in part (c). As such, we may compose

We check to make sure that φ is well defined. This follows since if $a \in A_i$ and $b \in A_j$ with $\overline{a} = \overline{b}$, then $a \sim b$ and so there exists an index k such that $i, j \leq k$ and $\rho_{ik}(a) = \rho_{jk}(b)$. This means that

$$\varphi_i(a) = (\varphi_k \circ \rho_{ik})(a) = (\varphi_k \circ \rho_{jk})(b) = \varphi_j(b)$$

and thus $\varphi(\overline{a}) = \varphi_i(a) = \varphi_j(b) = \varphi(\overline{b})$, to which φ is well defined. Now let $a \in A_i$ and $b \in A_j$ be arbitrary, Then we can find that

$$\begin{aligned}
\varphi(\overline{a} + \overline{b}) &= \varphi(\overline{\rho_{ik}(a) + \rho_{jk}(b)}) \\
&= \varphi_k(\rho_{ik}(a) + \rho_{jk}(b)) \\
&= (\varphi_k \circ \rho_{ik})(a) + (\varphi_k \circ \rho_{jk})(b) \\
&= \varphi_i(a) + \varphi_j(b) \\
&= \varphi(\overline{a}) + \varphi(\overline{b})
\end{aligned}$$

where the first line follows from the proof of part (c), and the fourth follows from the third line due to the construction of the φ_i maps. In particular, φ is a group homomorphism. The uniqueness of φ is a consequence of the uniqueness of the maps ρ_{ij} and ρ_i as defined for all $i, j \in I$. ∎

Exercise 7.6.9.

Exercise 7.6.10.

Exercise 7.6.11.

※ Euclidean Domains, Principal Ideal Domains, and Unique Factorization Domains

8.1 Euclidean Domains

Exercise 8.1.1 For each of the following five pairs of integers a and b, determine their greatest common divisor d and write d as a linear combination $ax + by$ of a and b.
(a) $a = 20$, $b = 13$.
(b) $a = 69$, $b = 372$.
(c) $a = 11391$, $b = 5673$.
(d) $a = 507885$, $b = 60808$.
(e) $a = 91442056588823$, $b = 779086434385541$ (the Euclidean Algorithm requires only 7 steps for these integers).

Proof. ■

Exercise 8.1.2

Exercise 8.1.3 Let R be a Euclidean Domain. Let m be the minimum integer in the set of norms of nonzero elements of R. Prove that every nonzero element of R of norm m is a unit. Deduce that a nonzero element of norm zero (if such an element exists) is a unit.

Proof. Take R a Euclidean Domain with norm N. Suppose $x \in R \setminus \{0\}$ has norm m. Since R is, in particular, an integral domain, we have that $1 \in R$, and since clearly $1 \neq 0$, we invoke the Division Algorithm inherent to R to write that there exists non-zero elements $q, r \in R$ such that

$$1 = qx + r$$

with $r = 0$ or with $N(r) < N(x) = m$. By assumption, m was the minimum norm of non-zero elements of R, and hence $r = 0$ is required. Thus $1 = qx$ for some non-zero $q \in R$. Hence x is a unit.

Using the above, clearly if there exists a non-zero element of R having norm equal to 0, then since 0 is the minimum integer automatically, then the element is a unit. ■

Exercise 8.1.4 Let R be a Euclidean Domain.
(a) Prove that if $(a, b) = 1$ and a divides bc, then a divides c. More generally, show that if a divides bc with nonzero a, b then $\frac{a}{(a,b)}$ divides c.
(b) Consider the Diophantine Equation $ax + by = N$ where a, b and N are integers and a, b are nonzero. Suppose x_0, y_0 is a solution: $ax_0 + by_0 = N$. Prove that the full set of

solutions to this equation is given by

$$x = x_0 + m\frac{b}{(a,b)}, \qquad y = y_0 - m\frac{a}{(a,b)}$$

as m ranges over the integers. [If x, y is a solution to $ax + by = N$, show that $a(x - x_0) = b(y_0 - y)$ and use (a).]

Proof. (a)

(b) ∎

Exercise 8.1.5

Exercise 8.1.6

Exercise 8.1.7

Exercise 8.1.8

Exercise 8.1.9

Exercise 8.1.10

Exercise 8.1.11

Exercise 8.1.12

8.2 Principal Ideal Domains (P.I.D.s)

Exercise 8.2.1

Exercise 8.2.2

Exercise 8.2.3

Exercise 8.2.4

Exercise 8.2.5

Exercise 8.2.6

Exercise 8.2.7

Exercise 8.2.8

8.3 Unique Factorization Domains (U.F.D.s)

Exercise 8.3.1

Exercise 8.3.2

Exercise 8.3.3

Exercise 8.3.4

Exercise 8.3.5

Exercise 8.3.6

Exercise 8.3.7

Exercise 8.3.8

Exercise 8.3.9

Exercise 8.3.10

Exercise 8.3.11

❈ Polynomial Rings

9.1 Definitions and Basic Properties

Exercise 9.1.1

Exercise 9.1.2

Exercise 9.1.3

Exercise 9.1.4

Exercise 9.1.5

Exercise 9.1.6

Exercise 9.1.7

Exercise 9.1.8

Exercise 9.1.9

Exercise 9.1.10

Exercise 9.1.11

Exercise 9.1.12

Exercise 9.1.13

Exercise 9.1.14

Exercise 9.1.15

Exercise 9.1.16

Exercise 9.1.17

Exercise 9.1.18

9.2 Polynomial Rings over Fields I

Exercise 9.2.1

Exercise 9.2.2

Exercise 9.2.3

Exercise 9.2.4

Exercise 9.2.5

Exercise 9.2.6

Exercise 9.2.7

Exercise 9.2.8

Exercise 9.2.9

Exercise 9.2.10

Exercise 9.2.11

Exercise 9.2.12

Exercise 9.2.13

9.3 Polynomial Rings that are Unique Factorization Domains

Exercise 9.3.1

Exercise 9.3.2

Exercise 9.3.3

Exercise 9.3.4

Exercise 9.3.5

9.4 Irreducibility Criteria

Exercise 9.4.1

Exercise 9.4.2

Exercise 9.4.3

Exercise 9.4.4

Exercise 9.4.5

Exercise 9.4.6

Exercise 9.4.7

Exercise 9.4.8

Exercise 9.4.9

Exercise 9.4.10

Exercise 9.4.11

Exercise 9.4.12

Exercise 9.4.13

Exercise 9.4.14

Exercise 9.4.15

Exercise 9.4.16

Exercise 9.4.17

Exercise 9.4.18

Exercise 9.4.19

Exercise 9.4.20

9.5 Polynomial Rings over Fields II

Exercise 9.5.1

Exercise 9.5.2

Exercise 9.5.3

Exercise 9.5.4

Exercise 9.5.5

Exercise 9.5.6

Exercise 9.5.7

9.6 Polynomial Rings in Several Variables over a Field and GrÃűbner Bases

※ Introduction to Module Theory

10.1 Basic Definitions and Examples

Exercise 10.1.1 Prove that $0m = 0$ and $(-1)m = -m$ for all $m \in M$.

Proof. Let $m \in M$ be arbitrary. For any $r \in R$, note that we have

$$0m = (r - r)m = rm - rm = 0$$

Similarly, we may observe

$$(-1)m = (1 \cdot -1)m = 1(-m) = -m$$

which suffices to show the desired relations. ■

Exercise 10.1.2 Prove that $R^\times$ and M satisfy the two axioms in Section 1.7 for a group action of the multiplicative group $R^\times$ on the set M.

Proof. Let $r, s \in R^\times$ and take $m \in M$. Then we trivially have

$$(rs)m = r(sm)$$

which follows by definition of the R-module M. The fact that $1 \cdot m = m$ once more follows from the definition of M. ■

Exercise 10.1.3 Assume that $rm = 0$ for some $r \in R$ and some $m \in M$ with $m \neq 0$. Prove that r does not have a left inverse (i.e. there is no $s \in R$ such that $sr = 1$).

Proof. Assume, for contradiction, that r has a left inverse, say $s \in R$. Then, since $1 \cdot m = m$ for all $m \in M$ by construction of M, we see

$$m = 1m = (sr)m = s(rm) = s0 = 0$$

which follows since $rs = 1$ by assumption. The above is a contradiction, for we assumed that $m \neq 0$. ■

Exercise 10.1.4 Let M be the module R^n described in Example 3 and let $I_1, I_2, \ldots, I_n$ be the left ideals of R. Prove that the following are submodules of M:
(a) $\{(x_1, x_2, \ldots, x_n) \mid x_i \in I_i\}$
(b) $\{(x_1, x_2, \ldots, x_n) \mid x_i \in R \text{ and } x_1 + x_2 + \cdots + x_n = 0\}$

Proof. (a) Denote $N = \{(x_1, x_2, \ldots, x_n) \mid x_i \in I_i\}$. First note that $0 \in I_i$ for all $1 \leq i \leq n$ by definition of ideals of R. This implies that $0 = (0, \ldots, 0) \in N$, to which $N \neq \varnothing$. Now let $x, y \in N$ and $r \in R$. Take $x = (x_1, \ldots, x_n)$ and

$y = (y_1, \dots, y_n)$. We know $x_i, y_i \in I_i$ for all $1 \le i \le n$ by construction of N. Since each I_i is a left ideal of R, this implies $ry_i \in I_i$ for all $1 \le i \le n$ also. By closure of each I_i under addition, we then have $x_i + ry_i \in I_i$ for each $1 \le i \le n$. In particular, we have $x + ry \in N$. The submodule criterion guarantees that N is an R-submodule of M.

(b) Denote $N = \{(x_1, x_2, \dots, x_n) \mid x_i \in R \text{ and } x_1 + x_2 + \cdots + x_n = 0\}$. Since $0 + \cdots + 0 = 0$ trivially holds, and $0 \in R$, we know $(0, \dots, 0) \in N$, to which $N \neq \emptyset$. Now take $x, y \in N$ and let $r \in R$ be arbitrary. Note

$$\sum_{j=1}^{n}(x_j + ry_j) = \sum_{j=1}^{n} x_j + \sum_{j=1}^{n} ry_j = \sum_{j=1}^{n} x_j + r\sum_{j=0}^{n} y_j = 0 + r0 = 0$$

following by the assumption that $x, y \in N$. Therefore, we can see that indeed $x + ry \in N$. The submodule criterion then guarantees that N is an R-submodule of M. ■

Exercise 10.1.5 For any left ideal I of R define

$$IM = \{\sum_{\text{finite}} a_i m_i \mid a_i \in I,\ m_i \in M\}$$

to be the collection of all finite sums of elements of the form am where $a \in I$ and $m \in M$. Prove that IM is a submodule of M.

Proof. Let R be a ring with identity and M a left R-module. Let I be some left ideal of R. Define $IM = \{\sum_{\text{finite}} a_i m_i \mid a_i \in I,\ m_i \in M\}$. First we prove that IM is a subgroup of M considered as an additive group. Let $x, y \in IM$. Then $x = \sum_{i=1}^{k} a_i m_i$ and $y = \sum_{i=1}^{h} b_i n_i$ for $a_i, b_i \in I$ and $m_i, n_i \in M$, and some $k, h \in \mathbb{Z}^+$. Without loss of generality assume $k > h$. Define $b_i = 0$ and $n_i = 0$ for all $h < i \le k$. Then

$$x - y = \sum_{i=1}^{k} a_i m_i - \sum_{j=1}^{h} b_j n_j = \sum_{i=1}^{k}(a_i - b_i)(m_i - n_i)$$

and since $a_i - b_i \in I$ by properties of the ideal I, and $m_i - n_i \in M$ by closure of M under subtraction, this implies $x - y$ is a finite sum of elements of I and M, to which $x - y \in IM$. The subgroup criterion guarantees that $IM \le M$ as an additive group. To prove IM is an R-submodule of M, we need only show that IM is closed under the action of ring elements from R. So let $r \in R$ be arbitrary and $x \in IM$ as before.

$$rx = r\sum_{i=1}^{k} a_i m_i = \sum_{i=1}^{k} r(a_i m_i) = \sum_{i=1}^{k}(ra_i)m_i$$

and since I is closed under left multiplication by elements of R, this means $ra_i \in I$ for all $1 \le i \le k$, and so necessarily $rx \in IM$. ■

Exercise 10.1.6 Show that the intersection of any nonempty collection of submodules of an R-module is a submodule.

Proof. Let M be an R-module, and $\mathcal{N}$ be a nonempty collection of R-submodules of M. Consider the set $\bigcap_{S\in\mathcal{N}} S$. Since each $S \in \mathcal{N}$ is an R-submodule of M, $S \leq M$ as additive groups. The intersection of any nonempty collection of subgroups of M is once more a subgroup of M, following from Exericse 2.1.10(b), and thus $\bigcap_{S\in\mathcal{N}} S \leq M$ follows. What remains is to show that $\bigcap_{S\in\mathcal{N}} S$ is closed under the action of ring elements from R. Let $x \in \bigcap_{S\in\mathcal{N}} S$ and $r \in R$ be arbitrary. In particular, $x \in S$ for all $S \in \mathcal{N}$. Since each S is an R-submodule, we know $rx \in S$ for all $S \in \mathcal{N}$, implying $rx \in \bigcap_{S\in\mathcal{N}} S$ as well. ■

Exercise 10.1.7 Let $N_1 \subseteq N_2 \subseteq \cdots$ be an ascending chain of submodules of M. Prove that $\bigcup_{i=1}^{\infty} N_i$ is a submodule of M.

Proof. Take M an R-module and $N_1 \subseteq N_2 \subseteq \cdots$ a chain of submodules of M. Consider the set $\bigcup_{i=1}^{\infty} N_i$. Since each N_i is an R-submodule of M, each $N_i \leq M$ as an additive group. By Exercise 2.1.8, [[DF-2.1-8]], we know $H \cup K$ is a subgroup of a group G if and only if either $H \subseteq K$ or $K \subseteq H$. It is a simple induction to extend this to the arbitrary case where $N_1 \cup N_2$ is a subgroup of M since $N_1 \subseteq N_2$. Similarly, we have $\bigcup_{i=1}^{n} N_i \subseteq N_{n+1}$ and so $\bigcup_{i=1}^{n+1} N_i$ is a subgroup. With this induction, we have $\bigcup_{i=1}^{\infty} N_i \leq M$ is a subgroup. Now let $r \in R$ and $x \in \bigcup_{i=1}^{\infty} N_i$. Then $x \in N_i$ for some $i \in \mathbb{N}$. In particular, $rx \in N_i$ by closure under N_i of the action of R. Thus $rx \in \bigcup_{i=1}^{\infty} N_i$. Thus we have proved $\bigcup_{i=1}^{\infty} N_i$ is an R-submodule of M. ■

Exercise 10.1.8 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

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

(a) Prove that if R is an integral domain then $\mathrm{Tor}(M)$ is a submodule of M (called the torsion submodule of M).
(b) Give an example of a ring R and an R-module M such that $\mathrm{Tor}(M)$ is not a submodule.
(c) If R has zero divisors show that every nonzero R-module has nonzero torsion elements.

Proof. (a) Let M be an R-module. Suppose R is an integral domain, meaning that R is a commutative ring with identity and R has no zero divisors. To show that the set $\mathrm{Tor}(M)$ is an R-submodule of M, we need only prove that $\mathrm{Tor}(M) \neq \emptyset$ and that $\mathrm{Tor}(M)$ contains $x + ry$ for all $x, y \in \mathrm{Tor}(M)$ and $r \in R$. Note that $0 \in \mathrm{Tor}(M)$ trivially holds, for if $r \in R$ such that $r \neq 0$, then $r0 = 0$. Now take $x, y \in \mathrm{Tor}(M)$

and $r \in R$. Since x and y are torsion elements, there exist nonzero $s, t \in R$ for which $sx = 0$ and $ty = 0$. Now we may note

$$st(x + ry) = (st)x + (st)ry = (ts)x + s(rt)y = t(sx) + sr(ty) = t0 + sr0 = 0$$

also, we may be assired that $st \neq 0$, for neither s, t are equal to 0 and R is an integral domain. The element $st \in R$ above implies $x + ry$ is a torsion element, and thus $x + ry \in \text{Tor}(M)$. The submodule criterion guarantees that $\text{Tor}(M)$ is an R-submodule of M.

(b) We give an example of a ring R for which $\text{Tor}(M)$ is not an R-submodule of M. Based on part (a), we look for a ring with zero divisors. Consider the ring $\mathbb{Z}/6\mathbb{Z}$ as an $\mathbb{Z}/6\mathbb{Z}$-module over itself. Note that $2, 3 \in \mathbb{Z}/6\mathbb{Z}$ are both nonzero ring elements whose product is $2 \cdot 3 = 6 = 0$; in particular $\mathbb{Z}/6\mathbb{Z}$ is not an integral domain.

Consider $\text{Tor}(\mathbb{Z}/6\mathbb{Z})$. We can easily find that $0, 2, 3, 4 \in \text{Tor}(\mathbb{Z}/6\mathbb{Z})$; see this by considering $3 \cdot 2 = 2 \cdot 3 = 0$ and $4 \cdot 3 = 3 \cdot 4 = 0$. However $1, 5 \notin \text{Tor}(\mathbb{Z}/6\mathbb{Z})$. Thus $\text{Tor}(\mathbb{Z}/6\mathbb{Z}) = \{0, 2, 3, 4\}$. We can see that $\text{Tor}(\mathbb{Z}/6\mathbb{Z}) \not\leq \mathbb{Z}/6\mathbb{Z}$ as an additive subgroup, since $2, 3 \in \text{Tor}(\mathbb{Z}/6\mathbb{Z})$ implies $2 + 3 = 5 \in \text{Tor}(\mathbb{Z}/6\mathbb{Z})$, which is clearly not the case. Therefore $\text{Tor}(\mathbb{Z}/6\mathbb{Z})$ cannot be an $\mathbb{Z}/6\mathbb{Z}$-submodule of $\mathbb{Z}/6\mathbb{Z}$.

(c) Let R be a ring with zero divisors. Suppose M is any nonzero R-module. Let $a \in R$ be a zero divisor, say with $b \in R$ such that $b \neq 0$ and $ab = 0$. Now take some nonzero $x \in M$. Since M is closed under the action of ring elements from R, we know $bx \in M$. If it is the case that $bx = 0$, then $x \in \text{Tor}(M)$ follows since $b \neq 0$. If $bx \neq 0$, then once more under closure of this action,

$$a(bx) = (ab)x = 0x = 0 \in M$$

and since $a \neq 0$ by assumption, it follows that $bx \in \text{Tor}(M)$. In either case, we have shown containment of a nonzero element of M in $\text{Tor}(M)$. In other words, M has a nonzero torsion element. ■

Exercise 10.1.9 If N is a submodule of M, the annihilator of N in R is defined to be

$$\{a \in R \mid an = 0 \text{ for all } n \in N\}$$

Prove that the annihilator of N in R is a 2-sided ideal of R.

Proof. Let $\text{Ann}_R(N)$ denote the annihilator of N in R. First we show that $\text{Ann}_R(N)$ is an additive subgroup of R. Note that $0 \in R$ satisfies $0n = 0$ for all $n \in N$ and hence $0 \in \text{Ann}_R(N) \neq \varnothing$. Now let $a, b \in \text{Ann}_R(N)$. Then

$$(a - b)n = an - bn = 0 + 0 = 0$$

for all $n \in N$ and so $a - b \in \text{Ann}_R(N)$. Thus $\text{Ann}_R(N)$ is a subgroup of R by the subgroup criterion. Now let $r \in R$ be arbitrary and take $a \in \text{Ann}_R(N)$. Then

$$(ra)n = r(an) = r0 = 0$$

for all $n \in N$ and hence $ra \in \text{Ann}_R(N)$. Similarly,

$$(ar)n = a(rn) = 0$$

since by assumption N is am R-submodule and so $rn \in N$, and by assumption $an = 0$ for all $n \in N$, in particular rn. Thus $\text{Ann}_R(N)$ is a 2-sided ideal of R, as desired. ∎

Exercise 10.1.10 If I is a right ideal of R, the annihilator of I in M is defined to be

$$\{m \in M \mid am = 0 \text{ for all } a \in I\}$$

Prove that the annihilator of I in M is a submodule of M.

Proof. Let $\text{Ann}_M(I)$ denote the annihilator of I in M. First we show that $\text{Ann}_M(I)$ is an additive subgroup of M. Note that $0 \in M$ satisfies $a0 = 0$ for all $a \in I$ and hence $0 \in \text{Ann}_M(I) \neq \emptyset$. Now suppose $m, n \in \text{Ann}_M(I)$. Then since $am = 0$ and $an = 0$ for all $a \in I$, we know that

$$a(m - n) = am - an = 0 - 0 = 0$$

for all $a \in I$. Thus $m - n \in \text{Ann}_M(I)$ and so $\text{Ann}_M(I)$ is a subgroup of M. Now let $r \in R$ be arbitrary and take $m \in \text{Ann}_M(I)$. Then

$$a(rm) = (ar)m = 0$$

since $ar \in I$ as I is a right ideal of R, and by assumption m annihilates all elements of I. Thus $rm \in \text{Ann}_M(I)$ and so $\text{Ann}_M(I)$ is an R-submodule of M, as desired. ∎

Exercise 10.1.11 Let M be the abelian group (i.e., $\mathbb{Z}$-module) $\mathbb{Z}/24\mathbb{Z} \times \mathbb{Z}/15\mathbb{Z} \times \mathbb{Z}/50\mathbb{Z}$.
(a) Find the annihilator of M in $\mathbb{Z}$ (i.e., a generator for this principal ideal).
(b) Let $I = 2\mathbb{Z}$. Describe the annihilator of I in M as a direct product of cyclic groups.

Proof. (a) We claim that $\text{Ann}_{\mathbb{Z}}(M) = (\text{lcm}(24, 15, 50) = (600)$. We have that $24 = 2^3 \cdot 3$, $15 = 3 \cdot 5$, and $50 = 2 \cdot 5^2$, and so clearly the least common multiple of 24, 15, and 50 is $2^3 \cdot 3 \cdot 5^2 = 600$. To prove this, observe that if $n \in \text{Ann}_{\mathbb{Z}}(M)$ then $nm = 0$ for all $m \in M$; in particular, for $m = (1, 1, 1)$. Thus we require that $n(1, 1, 1) = (n, n, n) = 0$, and hence that $n \equiv 0 \pmod{24}$, $n \equiv 0 \pmod{15}$, and $n \equiv 0 \pmod{50}$. In particular, n is divisible by each of 24, 15, and 50, and so must be divisible by the least common multiple 600, to which $n \in (600)$; hence

$\mathrm{Ann}_{\mathbb{Z}}(M) \subseteq (600)$. For the reverse containment, take $n \in (600)$ and note that $n(x, y, z) = (nx, ny, nz) = 0$ in M for any $x \in \mathbb{Z}/24\mathbb{Z}$, $y \in \mathbb{Z}/15\mathbb{Z}$, and $z \in \mathbb{Z}/50\mathbb{Z}$; this follows since n is congruent to 0 in each of $\mathbb{Z}/24\mathbb{Z}$, $\mathbb{Z}/15\mathbb{Z}$, and $\mathbb{Z}/50\mathbb{Z}$ since n is a multiple of each 24, 15, and 50; thus $(600) \subseteq \mathrm{Ann}_{\mathbb{Z}}(M) = (600)$, and so we have set equality.

(b) Let $I = 2\mathbb{Z}$. We claim that $\mathrm{Ann}_M(I) = \langle 12 \rangle \times \langle 0 \rangle \times \langle 25 \rangle$. If $m \in \mathrm{Ann}_M(I)$ then $am = 0$ for all $a \in I$, and in particular $2m = 0$. Thus if we write $m = (x, y, z)$ for $x \in \mathbb{Z}/24\mathbb{Z}$, $y \in \mathbb{Z}/15\mathbb{Z}$, and $z \in \mathbb{Z}/50\mathbb{Z}$, then $2m = (2x, 2y, 2z) = 0$ which implies that $2x \equiv 0 \pmod{24}$, $2y \equiv 0 \pmod{15}$, and $2z \equiv 0 \pmod{50}$; hence x must be divisible by $2^2 \cdot 3$, y must be divisible by $3 \cdot 5$, and z must be divisible by 5^2, since, respectively, $24 \mid 2x$, $15 \mid 2y$, and $50 \mid 2z$ is required. These requirements mean that x is a multiple of $2^2 \cdot 3 = 12$, y is a multiple of $3 \cdot 5 = 15$, and z is a multiple of $5^2 = 25$, and hence that $x \in \langle 12 \rangle$, $y \in \langle 15 \rangle = \langle 0 \rangle$, and $z \in \langle 25 \rangle$. Hence $m \in \langle 12 \rangle \times \langle 0 \rangle \times \langle 25 \rangle$, which proves that $\mathrm{Ann}_M(I) \subseteq \langle 12 \rangle \times \langle 0 \rangle \times \langle 25 \rangle$. For the reverse containment, note that if $m = (x, y, z) \in \langle 12 \rangle \times \langle 0 \rangle \times \langle 25 \rangle$ then $x \equiv 0, 12 \pmod{24}$, $y \equiv 0 \pmod{15}$, and $z \equiv 0, 25 \pmod{50}$. In any of these cases for x, y, z, we know that $a \in I$ has the form $a = 2k$ for some $k \in \mathbb{Z}$, so that $am = (2k)m = (2kx, 2ky, 2kz) = (0, 0, 0)$ since $24 \mid 2kx$ and $50 \mid 2kz$ since x is a multiple of 12 and z a multiple of 25. Therefore $m \in \mathrm{Ann}_M(I)$ holds, and we have our desired equality. ■

Exercise 10.1.12

Exercise 10.1.13 Let I be an ideal of R. Let M' be the subset of elements a of M that are annihilated by some power, I^k, of the ideal I, where the power may depend on a. Prove that M' is a submodule of M. [Use Exercise 7.]

Proof. Let M_k denote the subset of M consisting of elements a of M annihilated by I^k. That is, for an integer $k \geq 1$, set $M_k = \mathrm{Ann}_M(I^k)$ in the notation of the preceding exercises. We claim that $M_k \subseteq M_{k+1}$ for all $k \geq 1$. To this end, suppose $m \in M_k$. Then m is annihilated by I^k. Note that any $r \in I^{k+1} = II^k$ may be written $r = s's$ for $s' \in I$ and $s \in I^k$. Then $rm = (s's)m = s'(sm) = s'0 = 0$ holds since m is annihilated by I^k; hence m is annihilated by I^{k+1}, proving our claim.

Now we have an ascending chain of submodules $M_1 \subseteq M_2 \subseteq \cdots \subseteq M_k \subseteq \cdots$, and by Exercise 10.1.7 we know that $\bigcup_{k=1}^{\infty} M_k$ is a submodule of M. Note, however, that this submodule is precisely M' as defined in the problem description; hence M' is a submodule of M. ■

Exercise 10.1.14 Let z be an element of the center of R, i.e., $zr = rz$ for all $r \in R$. Prove that zM is a submodule of M, where $zM = \{zm \mid m \in M\}$. Show that if R is the ring of

2×2 matrices over a field and e is the matrix with a 1 in position $1,1$ and zeros elsewhere then eR is not a left R-submodule (where $M = R$ is considered as a left R-module as in Example 1)–in this case the matrix e is not in the center of R.

Proof. Let R be a ring and $z \in Z(R)$. Let M be an R-module. We prove that zM is an R-submodule of M. First note that $0 \in M$ satisfies $z0 = 0 \in zM$ and so $zM \neq \varnothing$. Now suppose $a, b \in zM$. Then there exist $m, n \in M$ such that $a = zm$ and $b = zn$. Now we have

$$a - b = zm - zn = z(m - n)$$

and since $m - n \in M$ by closure, it follows that $a - b \in zM$. Thus zM is a subgroup of M by the subgroup criterion. Now let $r \in R$ be arbitrary and assume $a \in zM$. Then $a = zm$ for some $m \in M$ and

$$ra = r(zm) = (rz)m = (zr)m = z(rm)$$

since z commutes with all elements of R. Since $rm \in M$ by closure, we have that $ra \in zM$, proving that zM is an R-submodule of M.

Now let F be a field and $R = M_2(F)$. Let e be the matrix with a 1 in the first row first column and zeros elsewhere. Then

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}$$

and so we can easily verify that

$$eR = \{\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \mid a, b \in F\}$$

Now we aim to show that eR is not an R-submodule of R considered as a left R-module over itself. To do this, we must find some $r \in R$ for which $ra \notin eR$ for some $a \in eR$. Consider

$$\begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ a & b \end{pmatrix} \notin eR$$

therefore eR is not closed under multiplication by elements of R on the left, and so cannot be a left R-submodule of R. In particular, the converse statement to what we proved above asserts that since eR is not a left R-submodule, then e is not in $Z(R)$. ■

Exercise 10.1.15 If M is a finite abelian group then M is naturally a $\mathbb{Z}$-module. Can this action be extended to make M into a $\mathbb{Q}$-module.

Proof. Take $M = \mathbb{Z}/6\mathbb{Z}$. Note $\mathbb{Z}/6\mathbb{Z}$ is a $\mathbb{Z}$-module. Assume, for contradiction, that $\mathbb{Z}/6\mathbb{Z}$ is a $\mathbb{Q}$-module. Then, for any $x \in \mathbb{Z}/6\mathbb{Z}$, we have

$$x = 1 \cdot x = (\frac{6}{6}) \cdot x = \frac{1}{6} \cdot 6x) = \frac{1}{6} \cdot 0 = 0$$

which follows since $1 \in \mathbb{Q}$ satisfies $1 \cdot x = x$ for all $x \in \mathbb{Z}/6\mathbb{Z}$, and $6/6 = 1$ clearly holds. However we know $6 \cdot x = 6x \in \mathbb{Z}/6\mathbb{Z}$ is 0. Since there are clearly non-zero elements of $\mathbb{Z}/6\mathbb{Z}$, we have a contradiction. ∎

Exercise 10.1.16

Exercise 10.1.17 Let T be the shift operator on the vector space V and let $e_1, \ldots, e_n$ be the usual basis vectors described in the example of $F[x]$-submodules. If $m \geq n$ find $(a_m x^m + a_{m-1}x^{m-1} + \cdots + a_0)e_n$.

Proof. Take $m \geq n$. Then we can rewrite the polynomial as

$$a_m x^m + a_{m-1}x^{m-1} + \cdots + a_n x^n + \cdots + a_0$$

With T as the shift operator, we can now see that

$$(a_m T^m + a_{m-1}T^{m-1} + \cdots + a_n T^n + \cdots + a_0)(e_n)$$
$$= a_m T^m(e_n) + \cdots + a_n T^n(e_n) + \cdots + a_0 e_n$$
$$= a_m(0, \ldots, 0) + \cdots + a_n(1, 0, \ldots, 0) + \cdots + a_0(0, \ldots, 1)$$
$$= (a_n, a_{n+1}, \ldots, a_1, a_0)$$

so that applying the shift operator T to the nth standard vector e_n gives us the coefficients of the polynomial up to the nth coefficient. ∎

Exercise 10.1.18 Let $F = \mathbb{R}$, let $V = \mathbb{R}^2$ and let T be the linear transformation from V to V which is rotation clockwise about the origin by $\pi/2$ radians. Show that V and 0 are the only $F[x]$-submodules for this T.

Proof. Suppose W is an $\mathbb{R}$-subspace of V that is not equal to V or 0. Then $\dim_{\mathbb{R}}(W) = 1$ and so $W = \operatorname{span}(v)$ for some $v \in V \setminus \{0\}$. Let $v = (a, b)$.

Note that $T(1, 0) = (0, 1)$ and $T(0, 1) = (-1, 0)$. Now we can see that

$$T(v) = T(a, b) = (-b, a)$$

To see that $(-b, a) \notin W$, we need to show that (a, b) and $(-b, a)$ are not multiples of one another. Suppose this was the case for some $\lambda \in \mathbb{R}$. Then $\lambda(a, b) = (-b, a)$ implies $\lambda a = -b$ and $\lambda b = a$, so that $\lambda^2 b = -b$ and hence $\lambda^2 = -1$. But then $\lambda = \sqrt{-1} \notin \mathbb{R}$, a contradiction. Hence $(-b, a) = T(v) \notin W$ and so W is not T-stable, and hence is not an $F[x]$-submodule of V. Therefore the only $F[x]$-submodules of V are 0 and V itself. ∎

Exercise 10.1.19 Let $F = \mathbb{R}$, let $V = \mathbb{R}^2$ and let T be the linear transformation from V to V which is projection onto the y-axis. Show that V, 0, the x-axis and the y-axis are the only $F[x]$-submodules for this T.

Proof. Consider $\mathbb{R}^2$ as an $\mathbb{R}$-vector space. Consider the projection linear transformation $T : \mathbb{R}^2 \to \mathbb{R}^2$ defined by $T(x, y) = (x, 0)$ for all $(x, y) \in \mathbb{R}^2$. From the correspondence given in the text, $\mathbb{R}^2$ becomes an $\mathbb{R}[x]$-module where the element x acts on $\mathbb{R}^2$ as T. In particular, the T-invariant subspaces of $\mathbb{R}^2$ as an $\mathbb{R}$-vector space are precisely the $\mathbb{R}[x]$-submodules of $\mathbb{R}^2$.

We trivially have that $0 = \{0\}$, the trivial subspace of $\mathbb{R}^2$, is T-invariant. Likewise for $\mathbb{R}^2$ itself as a subspace. Let $U_x = \{(x, 0) \in \mathbb{R}^2 \mid x \in \mathbb{R}\}$ and $U_y = \{(0, y) \in \mathbb{R}^2 \mid y \in \mathbb{R}\}$. Letting $(a, 0) \in U_x$ and $(0, b) \in U_y$ be arbitrary, we find

$$T(a, 0) = (a, 0) \in U_x \text{ and } T(0, b) = (0, 0) \in U_y$$

so that indeed $T(U_x) \subseteq U_x$ and $T(U_y) \subseteq U_y$ hold. Thus U_x, the x-axis, and U_y, the y-axis, are both T-invariant subspaces of $\mathbb{R}^2$; hence U_x and U_y are $\mathbb{R}[x]$-submodules of $\mathbb{R}^2$.

If U was some other T-invariant subspace of $\mathbb{R}^2$ such that $U \neq U_x, U_y$, then U would be equal to some line in the plane, say $U = \{(x, y) \in \mathbb{R}^2 \mid y = \lambda x\}$ for some $\lambda \in \mathbb{R} \setminus \{0\}$. Let $(x, y) \in U$ such that $(x, y) \neq (0, 0)$ be arbitrary. Then $T(x, y) = (x, 0)$. By the T-invariant assumption, we then have $(x, 0) \in U$, but this implies $0 = \lambda x$, and since $x \neq 0$, this means $\lambda = 0$. This is a contradiction, for then $U = U_x$, the x-axis. ∎

Exercise 10.1.20 Let $F = \mathbb{R}$, let $V = \mathbb{R}^2$ and let T be the linear transformation from V to V which is rotation clockwise about the origin by π radians. Show that every subspace of V is an $F[x]$-submodule for this T.

Proof. Suppose W is an $\mathbb{R}$-subspace that is not 0 or V. Then W is 1-dimensional and so $W = \operatorname{span}(v)$ for some $v \in V \setminus \{0\}$. Let $v = (a, b)$ and $\lambda \in \mathbb{R}$. First we may note that $T(1, 0) = (-1, 0)$ and $T(0, 1) = (0, -1)$. Now:

$$T(\lambda v) = (-\lambda a, -\lambda b) = -(\lambda a, \lambda b) \in W$$

by closure. Hence $T(W) \subseteq W$ and so W is an $F[x]$-submodule of V. ∎

Exercise 10.1.21 Let $n \in \mathbb{Z}^+$, $n > 1$ and let R be the ring of $n \times n$ matrices with entries from a field F. Let M be the set of $n \times n$ matrices with arbitrary elements of F in the first column and zeros elsewhere. Show that M is a submodule of R when R is considered as a left module over itself, but M is not a submodule of R when R is considered as a right R-module.

Proof. Let R and M be as in the problem description. It is trivial to verify that M is an additive subgroup of R. What remains is to check whether the action of R on M remains in M. Take an arbitary matrix from R and one from M. Upon multiplication of R by M on the left, we can see that:

$$\begin{pmatrix} x_{11} & x_{21} & \cdots & x_{n1} \\ x_{21} & x_{22} & \cdots & x_{n2} \\ \vdots & \vdots & \ddots & \vdots \\ x_{n1} & x_{n2} & \cdots & x_{nn} \end{pmatrix} \begin{pmatrix} a_1 & 0 & \cdots & 0 \\ a_2 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ a_n & 0 & \cdots & 0 \end{pmatrix} = \begin{pmatrix} \sum_{i=1}^n x_{i1}a_i & 0 & \cdots & 0 \\ \sum_{i=1}^n x_{i2}a_i & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ \sum_{i=1}^n x_{in}a_i & 0 & \cdots & 0 \end{pmatrix}$$

and clearly the above matrix lies in M as well. This implies that M is an R-submodule of R considered as a left R-module over itself. However, note that performing the same procedure on the right gives

$$\begin{pmatrix} a_1 & 0 & \cdots & 0 \\ a_2 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ a_n & 0 & \cdots & 0 \end{pmatrix} \begin{pmatrix} x_{11} & x_{21} & \cdots & x_{n1} \\ x_{21} & x_{22} & \cdots & x_{n2} \\ \vdots & \vdots & \ddots & \vdots \\ x_{n1} & x_{n2} & \cdots & x_{nn} \end{pmatrix} = \begin{pmatrix} a_1x_{11} & a_1x_{21} & \cdots & a_1x_{n1} \\ a_2x_{11} & a_2x_{21} & \cdots & a_2x_{n1} \\ \vdots & \vdots & \ddots & \vdots \\ a_nx_{11} & a_nx_{21} & \cdots & a_nx_{n1} \end{pmatrix}$$

and clearly the matrix above does not lie in M for all values of x_{ij} above, and hence does not lie in M for all matrices in R. Thus M is not an R-submodule of R considered as a right R-module over itself. ∎

Exercise 10.1.22 Suppose that A is a ring with identity 1_A that is a unital left R-module satisfying $r \cdot (ab) = (r \cdot a)b = a(r \cdot b)$ for all $r \in R$ and $a, b \in A$. Prove that the map $f : R \to A$ defined by $f(r) = r \cdot 1_A$ is a ring homomorphism mapping 1_R to 1_A and that $f(R)$ is contained in the center of A. Conclude that A is an R-algebra and that the R-module structure on A induced by its algebra structure is precisely the original R-module structure.

Proof. First we prove that $f : R \to A$ defined by $f(r) = r \cdot 1_A$ for all $r \in R$ is a ring homomorphism. Let $r, s \in R$. By the R-module structure of A, we have

$$f(r+s) = (r+s) \cdot 1_A = r \cdot 1_A + s \cdot 1_A = f(r) + f(s)$$

Similarly, we can find that

$$f(rs) = rs \cdot 1_A = rs \cdot 1_A 1_A = r(s \cdot 1_A)1_A = (r \cdot 1_A)(s \cdot 1_A) = f(r)f(s)$$

which follows by the assumption that $r \cdot (ab) = (r \cdot a)b = a(r \cdot b)$. Finally,

$$f(1_R) = 1_R \cdot 1_A = 1_A$$

follows from the fact that R is a unital ring, so that $1_R \cdot a = a$ for all $a \in A$ since A is an R-module. Therefore f is a ring homomorphism that maps the identity of R to that of A.

Now we show that $f(R)$ lies in the center of A. To do this, take $a \in f(R)$. We show that a commutes with all of A. Let $a = f(r)$ for some $r \in R$. Then, for arbitrary $b \in A$, we have

$$ab = f(r)b = (r \cdot 1_A)b = 1_A(r \cdot b) = 1_A(r \cdot (b1_A))$$

$$= 1_A((r \cdot b)1_A) = 1_A(b(r \cdot 1_A)) = 1_A b(r \cdot 1_A) = bf(r) = ba$$

which follows from several applications of the assumptions of structure of the R-module A as well as the fact that $b = 1_A b = 1_A b$ for all $b \in A$. Thus we have shown a lies in the center of A, to which $f(R)$ is a subset.

The map f above suffices to make A into an R-algebra. The natural R-module structure on A induced by its algebra structure is

$$r \cdot a = a \cdot r = f(r)a = (r \cdot 1_A)a = 1_A(r \cdot a) = r \cdot a$$

which is simply the original R-module structure in our assumption. Conversely, if A is an R-algebra, then A is a unital ring that is also a left R-module satisfying $r \cdot (ab) = (r \cdot a)b = a(r \cdot b)$ for all $r \in R$ and $a, b \in A$ since $f(R)$ is contained in the center of A. Thus we have shown an if and only if statement describing how a ring A satisfying the above permits a natural R-algebra structure. This suffices to show an equivalent definition of an R-algebra. ■

Exercise 10.1.23 Let A be the direct product ring $\mathbb{C} \times \mathbb{C}$. Let τ_1 denote the identity map on $\mathbb{C}$ and let τ_2 denote complex conjugation. For any pair $p, q \in \{1, 2\}$ (not necessarily distinct) define

$$f_{p,q} : \mathbb{C} \to \mathbb{C} \times \mathbb{C} \text{ by } f_{p,q}(z) = (\tau_p(z), \tau_q(z))$$

(a) Prove that each $f_{p,q}$ is an injective ring homomorphism, and that they all agree on the subfield $\mathbb{R}$ of $\mathbb{C}$. Deduce that A has four distinct $\mathbb{C}$-algebra structures. Explicitly give the action $z \cdot (u, v)$ of a complex number z on an ordered pair in A in each case.

(b) Prove that if $f_{p,q} \neq f_{p',q'}$ then the identity map on A is not a $\mathbb{C}$-algebra homomorphism from A considered as a $\mathbb{C}$-algebra via $f_{p,q}$ to A considered as a $\mathbb{C}$-algebra via $f_{p',q'}$ (although the identity is an $\mathbb{R}$-algebra homomorphism.

(c) Prove that for any pair p, q there is some ring isomorphism from A to itself such that A is isomorphic as a $\mathbb{C}$-algebra via $f_{p,q}$ to A considered as a $\mathbb{C}$-algebra via $f_{1,1}$ (the "natural" $\mathbb{C}$-algebra structure on A).

Proof. (a) Let $p, q \in \{1, 2\}$ be arbitrary, and let $z, w \in \mathbb{C}$. Then we may observe

$$f_{p,q}(z + w) = (\tau_p(z + w), \tau_q(z + w))$$

$$= (\tau_p(z) + \tau_p(w), \tau_q(z) + \tau_q(w))$$

$$= (\tau_p(z), \tau_q(z)) + (\tau_p(w), \tau_q(w))$$

$$= f_{p,q}(z) + f_{p,q}(w)$$

Similarly, we may find

$$f_{p,q}(zw) = (\tau_p(zw), \tau_q(zw)) = (\tau_p(z)\tau_p(w), \tau_q(z)\tau_q(w))$$
$$= (\tau_p(z), \tau_q(z)) \cdot (\tau_p(w), \tau_q(w))$$
$$= f_{p,q}(z) \cdot f_{p,q}(w)$$

Where both of the above derivations follow since the identity map and complex conjugation both are additive and multiplicative maps. The above suffices to show that each $f_{p,q}$ is a ring homomorphism. To show injectivity, we need only note that $\ker f_{p,q} = \{0\}$. This follows for if we have $z \in \ker f_{p,q}$, then it must be the case that $(\tau_p(z), \tau_q(z)) = (0, 0)$, so that $\tau_p(z) = 0$ and $\tau_q(z) = 0$. But if $p = 1$ then $\tau_p(z) = z$, so $z = 0$, and if $p = 2$ then $\tau_p(z) = \overline{z}$, so $\overline{z} = 0$. In either case, it must be that $z = 0$. Therefore each $f_{p,q}$ is injective. It is clear that $f_{p,q}(r) = (\tau_p(r), \tau_q(r)) = (r, r)$ for all $r \in \mathbb{R}$, so that each map $f_{p,q}$ agree on the subfield $\mathbb{R}$ of $\mathbb{C}$. This can be seen for both the identity and complex conjugation fix $\mathbb{R}$.

Each of the injective ring homomorphism $f_{p,q}$ above make $\mathbb{C} \times \mathbb{C}$ into a $\mathbb{C}$-algebra. Taking $(u, v) \in \mathbb{C} \times \mathbb{C}$ and $z \in \mathbb{C}$, the action of z on (u, v) is given by

$$z \cdot (u, v) = \left\{ \begin{array}{ll} (zu, zv) & \text{if } p = q = 1 \\ (\overline{z}u, zv), & \text{if } p = 2, q = 1 \\ (zu, \overline{z}v), & \text{if } p = 1, q = 2 \\ (\overline{z}u, \overline{z}v), & \text{if } p = q = 2 \end{array} \right\} \tag{1}$$

which completely characterizes the actions of any complex number on an element of $\mathbb{C} \times \mathbb{C}$.

(b) Suppose $f_{p,q} \neq f_{p',q'}$. We show that the identity map $\iota : \mathbb{C} \times \mathbb{C} \to \mathbb{C} \times \mathbb{C}$ is not a $\mathbb{C}$-algebra homomorphism. This follows since

$$\iota(f_{p,q}(z)(u, v)) = f_{p',q'}(z)\iota(u, v) = f_{p',q'}(z)(u, v)$$

must be satisfied for a $\mathbb{C}$-algebra homomorphism, however since $f_{p,q} \neq f_{p',q'}$ then at least one of p, p' and q, q' must be distinct. Without loss of generality, say p, p' is distinct. Then $f_{p,q}(z)(u, v) = (\tau_p(z)u, \tau_q(z)v)$, while $f_{p',q'}(z)(u, v) = (\tau_{p'}(z)u, \tau_{q'}(z)v)$. Indeed since $p \neq p'$, it must be the case that $\tau_p(z)u \neq \tau_{p'}(z)u$, in particular, since $\overline{z} \neq z$ for any non-real complex number. Thus ι is not a $\mathbb{C}$-algebra homomorphism from $\mathbb{C}\times\mathbb{C}$ with $f_{p,q}$ to $\mathbb{C}\times\mathbb{C}$ with $f_{p',q'}$, but is a $\mathbb{R}$-algebra homomorphism.

(c) If $p = q = 1$ then the desired ring isomorphism is clear, namely we may just take the identity map on $\mathbb{C} \times \mathbb{C}$ and obtain an isomorphism of $\mathbb{C}$-algebras via

$$\iota(f_{1,1}(z)(u, v)) = f_{1,1}(z) \cdot \iota(u, v)$$

Now consider the case where $p = q = 2$. Note that the map $\varphi : \mathbb{C} \times \mathbb{C} \to \mathbb{C} \times \mathbb{C}$ defined by $\varphi(u, v) = (\overline{u}, \overline{v})$ is clearly a ring isomorphism; φ is complex conjugation on two copies of $\mathbb{C}$. Now observe that

$$\varphi(f_{2,2}(z)(u, v)) = \varphi(\overline{z}u, \overline{z}v) = (z\overline{u}, z\overline{v}) = f_{1,1}(z)(\overline{u}, \overline{v}) = f_{1,1}(z)\varphi(u, v)$$

so that indeed we have $\varphi(z \cdot (u, v)) = z \cdot \varphi(u, v)$ for all $z \in \mathbb{C}$ and $(u, v) \in \mathbb{C} \times \mathbb{C}$.

Consider the case where $p = 2$ and $q = 1$. Then based on our above results we know that $z \cdot (u, v) = f_{2,1}(z)(u, v) \mapsto (zu, \overline{z}v)$ as we showed in part (a). The ring homomorphism $\psi_1 : \mathbb{C} \times \mathbb{C} \to \mathbb{C} \times \mathbb{C}$ defined by $\psi_1(u, v) = (\overline{u}, v)$ is actually seen to be an isomorphism of rings. Furthermore, we can see that

$$\psi_1(f_{2,1}(z)(u, v)) = \psi_1(\overline{z}u, zv) = (z\overline{u}, zv) = f_{1,1}(z)(\overline{u}, v) = f_{1,1}(z)\psi_1(u, v)$$

and so ψ_1 is the desired ring isomorphism that induces an isomorphism of $\mathbb{C}$-algebras induced by $f_{2,1}$ to that induced by $f_{1,1}$. The case where $p = 1$ and $q = 2$ is nearly identical, whereby we may take $\psi_2 : \mathbb{C} \times \mathbb{C} \to \mathbb{C} \times \mathbb{C}$ defined by $\psi_2(u, v) = (u, \overline{v})$ for all $(u, v) \in \mathbb{C} \times \mathbb{C}$. Then

$$\psi_2(f_{1,2}(z)(u, v)) = \psi_2(zu, \overline{z}v) = (zu, z\overline{v}) = f_{1,1}(z)(u, \overline{v}) = f_{1,1}(z)\psi_2(u, v)$$

which again satisfies the definition of an isomorphism of $\mathbb{C}$-algebras. Since these four cases exhaust all possibilities for p, q, we have shown that each map $f_{p,q}$ there exists a ring isomorphism of $\mathbb{C} \times \mathbb{C}$ that induces an isomorphism of $\mathbb{C}$-algebras from $\mathbb{C} \times \mathbb{C}$.

■

10.2 Quotient Modules and Module Homomorphisms

Exercise 10.2.1

Exercise 10.2.2

Exercise 10.2.3 Give an explicit example of a map from one R-module to another which is a group homomorphism but not an R-module homomorphism.

Proof. Consider $\mathbb{Q}^\times = \mathbb{Q} \setminus \{0\}$ as a $\mathbb{Z}$-module. Consider the map $\varphi : \mathbb{Q}^\times \to \mathbb{Q}^\times$ defined by $a \mapsto a^2$. Clearly we have $1 \mapsto 1$ so the identity is preserved, and for $a, b \in \mathbb{Q}^\times$ we have $\varphi(ab) = (ab)^2 = a^2b^2 = \varphi(a)\varphi(b)$. However,

$$\varphi(-1 \cdot a) = \varphi(-a) = (-a)^2 = a^2 \neq -1 \cdot \varphi(a) = -a^2$$

and thus φ is not a $\mathbb{Z}$-module homomorphism, since it is not $\mathbb{Z}$-linear. ■

Exercise 10.2.4 Let A be any $\mathbb{Z}$-module, let a be any element of A and let n be a positive integer. Prove that the map $\varphi_a : \mathbb{Z}/n\mathbb{Z} \to A$ given by $\varphi_a(\overline{k}) = ka$ is a well-defined $\mathbb{Z}$-module homomorphism if and only if $na = 0$. Prove that $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, A) \cong A_n$, where $A_n = \{a \in A \mid na = 0\}$ (so A_n is the annihilator in A of the ideal (n) of $\mathbb{Z}$–cf. Exercise 10, Section 1).

Proof. Let A be a $\mathbb{Z}$-module and $a \in A$. Take $n \in \mathbb{Z}^+$. Suppose $\varphi_a : \mathbb{Z}/n\mathbb{Z} \to A$ given by $\varphi_a(\overline{k}) = ka$ is a well-defined $\mathbb{Z}$-module homomorphism. By definition of well-definition of φ_a, this means that if $\overline{k} = \overline{k'}$ in $\mathbb{Z}/n\mathbb{Z}$ then $ka = k'a$ in A. In particular, in $\mathbb{Z}/n\mathbb{Z}$ we have $\overline{n} = \overline{0}$, and thus $na = 0a$, and so clearly $na = 0$ in A.

Conversely, suppose that $na = 0$. We prove that $\varphi_a : \mathbb{Z}/n\mathbb{Z} \to A$ is well-defined as a function, and that φ_a is a $\mathbb{Z}$-module homomorphism. If $\overline{m} = \overline{m'}$ then m and m' are congruent modulo n, and hence

$$m - m' = kn$$

for some $k \in \mathbb{Z}$. Multiplication of the above equation by a on the right yields

$$(m - m')a = ma - m'a = kna = k(na) = k0 = 0$$

and hence $ma = m'a$, so that $\varphi_a(m) = \varphi_a(m')$ and φ_a is thus well-defined. Note that $\varphi_a(\overline{0}) = 0a = 0$ in A. Furthermore, for $\overline{m}$ and $\overline{m'}$ in $\mathbb{Z}/n\mathbb{Z}$ and any $r \in \mathbb{Z}$ we have

$$\varphi_a(\overline{m} + \overline{m'}) = \varphi_a(\overline{m + m'}) = (m + m')a = ma + m'a = \varphi_a(m) + \varphi_a(m')$$

$$\varphi_a(r \cdot \overline{m}) = \varphi_a(\overline{rm}) = (rm)a = r(ma) = r\varphi_a(m)$$

The above shows that φ_a is a $\mathbb{Z}$-module homomorphism, proving the converse statement.

Now we show that $\text{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, A) \cong A_n$ as $\mathbb{Z}$-modules. This makes sense since $A_n = \text{Ann}_A(n\mathbb{Z})$, i.e., A_n is the annihilator of $(n) = n\mathbb{Z}$ in A.We shall do this by constructing a map

$$\Psi : A_n \longrightarrow \text{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, A)$$

$$\Psi(a) = \varphi_a$$

where $A_n = \{a \in A \mid na = 0\}$, as defined in the problem description. It is clear to see that each $a \in A_n$ gives rise to an $\mathbb{Z}$-module homomorphism $\varphi_a : \mathbb{Z}/n\mathbb{Z} \longrightarrow A$ as we saw via the if and only if statement proved above. Take $a, b \in A_n$. Note that

$$\varphi_{a+b}(\overline{k}) = k(a + b) = ka + kb = \varphi_a(\overline{k}) + \varphi_b(\overline{k})$$

$$\varphi_{ra}(\overline{k}) = k(ra) = (kr)a = (rk)a = r(ka) = r\varphi_a(\overline{k})$$

for all $\overline{k} \in \mathbb{Z}/n\mathbb{Z}$ and any $r \in \mathbb{Z}$. In this way, it is obvious that

$$\Psi(a + b) = \varphi_{a+b} = \varphi_a + \varphi_b = \Psi(a) + \Psi(b)$$

$$\Psi(ra) = \varphi_{ra} = r\varphi_a = r\Psi(a)$$

and so Ψ is indeed a $\mathbb{Z}$-module homomorphism. We now show Ψ is injective. Suppose $\varphi_a = \varphi_b$ for $a, b \in A_n$. Then, in particular, φ_a and φ_b agree on their image of $\overline{1}$ in $\mathbb{Z}/n\mathbb{Z}$, i.e., $\varphi_a(\overline{1}) = \varphi_b(\overline{1})$. It is then clear that

$$a = 1a = \varphi_a(\overline{1}) = \varphi_b(\overline{1}) = 1b = b$$

holds; hence the map Ψ is injective. Finally, we show surjectivity. Assume $\psi : \mathbb{Z}/n\mathbb{Z} \longrightarrow A$ is a $\mathbb{Z}$-module homomorphism. Then $\psi(\overline{1}) = a$ for some $a \in A$. In particular, for any $\overline{k} \in \mathbb{Z}/n\mathbb{Z}$, we require

$$\psi(\overline{k}) = \psi(k \cdot \overline{1}) = k\psi(\overline{1}) = ka$$

which follows since $k \in \mathbb{Z}$ may be pulled out of ψ (by assumption that ψ is a $\mathbb{Z}$-module homomorphism. In particular, $\psi = \varphi_a$ in the obvious way, and hence Ψ is surjective; hence Ψ is an isomorphism, and so $\text{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, A) \cong A_n$, as desired. ■

Exercise 10.2.5 Exhibit all $\mathbb{Z}$-module homomorphisms from $\mathbb{Z}/30\mathbb{Z}$ to $\mathbb{Z}/21\mathbb{Z}$.

Proof. Note that both $\mathbb{Z}/30\mathbb{Z}$ and $\mathbb{Z}/21\mathbb{Z}$ are $\mathbb{Z}$-modules. We know from Exercise 10.2.4 above that

$$\text{Hom}_{\mathbb{Z}}(\mathbb{Z}/30\mathbb{Z}, \mathbb{Z}/21\mathbb{Z}) \cong A_{30} = \text{Ann}_{\mathbb{Z}/21\mathbb{Z}}(30\mathbb{Z})$$

Where the $\mathbb{Z}$-module on the right is the set of $\overline{k} \in \mathbb{Z}/21\mathbb{Z}$ for which $\overline{30k} = \overline{0}$ in $\mathbb{Z}/21\mathbb{Z}$ (refer to Exercise 10.2.4). This is equivalent to $30k = 21n$ for some $n \in \mathbb{Z}$; i.e., $30k$ is a multiple of 21. In particular, from the same exercise, the $\mathbb{Z}$-module homomorphisms from $\mathbb{Z}/30\mathbb{Z}$ to $\mathbb{Z}/21\mathbb{Z}$ are all of the form φ_a, (taking $\overline{k} \mapsto ka$) where $a \in A_{30}$ satisifes $\overline{30a} = \overline{0}$ in $\mathbb{Z}/21\mathbb{Z}$.

Note $30 = 2 \cdot 3 \cdot 5$ and $21 = 3 \cdot 7$ as factorizations into primes. In particular, if $7 \mid k$, i.e., k has 7 as a prime factor, then we may write $k = 7k'$ for some $k' \in \mathbb{Z}$, and then

$$30k = 2 \cdot 3 \cdot 5 \cdot 7 \cdot k' = 21 \cdot 2 \cdot 5 \cdot k' = 21(10k')$$

so that $30k$ is a multiple of 21, and hence by our above discussion defines a map $\varphi_k : \mathbb{Z}/30\mathbb{Z} \to \mathbb{Z}/21\mathbb{Z}$ which is a well-defined $\mathbb{Z}$-module homomorphism. Conversely, a map $\varphi_k : \mathbb{Z}/30\mathbb{Z} \to \mathbb{Z}/21\mathbb{Z}$ defines such a homomorphism only if $30k = 21n$ for some n, and so clearly $7 \mid k$. In particular, since $7 \mid 0$, $7 \mid 7$, and $7 \mid 14$, so that $0, 7, 14$ are the only integers $0 < x < 21$ which 7 divides. Thus the zero homomorphism φ_0, along with φ_7, and φ_{14} are the only $\mathbb{Z}$-module homomorphisms from $\mathbb{Z}/30\mathbb{Z} \to \mathbb{Z}/21\mathbb{Z}$. ■

Exercise 10.2.6

Exercise 10.2.7 Let z be a fixed element of the center of R. Prove that the map $m \mapsto zm$ is an R-module homomorphism from M to itself. Show that for a commutative ring R the map from R to $\mathrm{End}_R(M)$ given by $r \mapsto rI$ is a ring homomorphism (where I is the identity endomorphism).

Proof. Fix $z \in Z(R)$. Consder the map $f_z : M \to M$ defined by $f_z(m) = zm$ for all $m \in M$. We have $f_z(0) = z0 = 0$ and so the additive identity of M is preserved. If $m, n \in M$ then

$$f_z(m + n) = z(m + n) = zm + zn = f_z(m) + f_z(n)$$

and so f_z is a group homomorphism from M to itself. Now let $r \in R$ be arbitrary and take $m \in M$. Then we have

$$f_z(rm) = z(rm) = (zr)m = (rz)m = r(zm) = rf_z(m)$$

since $rz = zr$ as $z \in Z(R)$. Therefore f_z is an R-module homomorphism.

Now let R be a commutative ring. Consider the map $\psi : R \to \mathrm{End}_R(M)$ defined by $\psi(r) = rI$, where I is the identity R-endomorphism of M. Note that $\psi(0) = 0I = 0$, the zero endomorphism, and further that $\psi(1) = 1I = I$, the identity endomorphism. Thus the additive and multiplicative identities are preserved under ψ. Now let $r, s \in R$ be arbitary. Then

$$\psi(r + s) = (r + s)I = rI + sI = \psi(r) + \psi(s)$$

$$\psi(rs) = (rs)I = rsI = rIsI = \psi(r)\psi(s)$$

since multiplication by rs may be viewed as multiplication by s followed by multiplication by r in the natural way. In particular, ψ is a homomorphism of rings. ■

Exercise 10.2.8 Let $\varphi : M \to N$ be an R-module homomorphism. Prove that $\varphi(\mathrm{Tor}(M)) \subseteq \mathrm{Tor}(N)$. [cf. Exercise 8 in Section 1]

Proof. Suppose $n \in \varphi(\mathrm{Tor}(M))$. Then $n = \varphi(m)$ for some $m \in \mathrm{Tor}(M)$. By construction there exists $r \in R$ such that $rm = 0$. Since $\varphi(rm) = r\varphi(m)$ by properties of R-module homomorphisms, we know that

$$rn = r\varphi(m) = \varphi(rm) = \varphi(0) = 0$$

to which $rn = 0$ and thus $n \in \mathrm{Tor}(N)$ by definition. Hence we have shown the inclusion $\varphi(\mathrm{Tor}(M)) \subseteq \mathrm{Tor}(N)$, as desired. ■

Exercise 10.2.9 Let R be a commutative ring. Prove that $\mathrm{Hom}_R(R, M)$ and M are isomorphic as left R-modules.

Proof. Let R be a commutative ring and let M be an R-module. Construct a map

$$\psi : \mathrm{Hom}_R(R, M) \to M$$

defined by $\psi(f) = f(1)$ for all $f \in \mathrm{Hom}_R(R, M)$. In other words, we take each R-module homomorphism from $R \to M$ and take its value at 1, the identity of R. Let f and g be R-module homomorphisms from $R \to M$. We can easily find that

$$\psi(f + g) = (f + g)(1) = f(1) + g(1) = \psi(f) + \psi(g)$$

and for arbitrary $r \in R$ we have

$$\psi(rf) = (rf)(1) = rf(1) = r\psi(f)$$

Hence ψ is an R-module homomorphism. Now we prove that ψ is bijective.

Suppose $f \in \ker\psi$. Then $f(1) = 0$. Let $r \in R$ be arbitrary. Then $rf(1) = f(r1) = f(r) = 0$ and so f is the zero map on R. Conversely, the zero R-module homomorphism in $\mathrm{Hom}_R(R, M)$ clearly lies in $\ker\psi$, so that $\ker\psi$ contains only the zero map from $R \to M$, and is thus trivial; hence ψ is injective.

Now suppose $m \in M$. Construct $h : R \to M$ defined by $h(r) = rm$ for all $r \in R$. Take $r, s \in R$ and note that

$$h(r + s) = (r + s)m = rm + sm = h(r) + h(s)$$

and also that for an arbitrary $r' \in R$ we have

$$h(r'r) = (r'r)m = r'(rm) = r'h(r)$$

In other words, we have proved that h is an R-module homomorphism from $R \to M$. For this h, we have $h(1) = 1m = m$. Thus for any $m \in M$ we can find an R-module homomorphism $h \in \text{Hom}_R(R, M)$ for which $\psi(h) = m$. Therefore ψ is surjective.

In particular, we have shown that $\text{Hom}_R(R, M) \cong M$ as left R-modules, which was the desired statement. ■

Exercise 10.2.10

Exercise 10.2.11

Exercise 10.2.12

Exercise 10.2.13

Exercise 10.2.14

10.3 Generation of Modules, Direct Sums, and Free Modules

Exercise 10.3.1 Prove that if A and B are sets of the same cardinality, then the free modules $F(A)$ and $F(B)$ are isomorphic.

Proof. Let A and B be sets with equal cardinality. By definition of cardinality, there exists a bijection from A to B, call it f. Now consider the free R-modules $\mathcal{F}(A)$ and $\mathcal{F}(B)$ on A and B, respectively. We also have the natural inclusions $\iota_A : A \longrightarrow \mathcal{F}(A)$ and $\iota_B : B \longrightarrow \mathcal{F}(B)$. Note that $\iota_B \circ f$ is a set-map from A to the R-module $\mathcal{F}(B)$, and thus by Theorem 6 there exists a unique R-module homomorphism $\Phi : \mathcal{F}(A) \longrightarrow \mathcal{F}(B)$ such that $\Phi \circ \iota_A = \iota_B \circ f$.

Similarly, note that $\iota_A \circ f^{-1}$ is a set-map from B to the R-module $\mathcal{F}(A)$. Thus, once more, by Theorem 6, there exists a unique R-module homomorphism $\Phi' : \mathcal{F}(B) \longrightarrow \mathcal{F}(A)$ such that $\Phi' \circ \iota_B = \iota_A \circ f^{-1}$.

Now note that

$$\Phi' \circ \Phi \circ \iota_A = \Phi' \circ \iota_B \circ f = \iota_A \circ f^{-1} \circ f = \iota_A$$

And so we have that $\Phi' \circ \Phi = \mathrm{id}_{\mathcal{F}(A)}$. In an analagous manner, we have $\Phi \circ \Phi' = \mathrm{id}_{\mathcal{F}(B)}$, so that, in fact, we have $\Phi^{-1} = \Phi'$. In particular, we have found a bijective R-module homomorphism from $\mathcal{F}(A)$ to $\mathcal{F}(B)$, proving that $\mathcal{F}(A) \cong \mathcal{F}(B)$ as R-modules. ■

Exercise 10.3.2

Exercise 10.3.3

Exercise 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., $M = \mathrm{Tor(M)}$ in the notation of Exercise 8 of Section 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.

Proof. Let A be a finite abelian group, say with order n. We know that A is automatically a $\mathbb{Z}$-module. If we take $a \in A$, then by properties of A as an abelian group, we know multiplying a by the order of A which is n yields the identity. In particular, we have $na = 0$ by properties of A, and clealy $n \neq 0$. This shows that A is a torsion $\mathbb{Z}$-module.

Now consider the infinite abelian group $\prod_{n \in \mathbb{N}} \mathbb{Z}/p\mathbb{Z} = (\mathbb{Z}/p\mathbb{Z})^\infty$, where p is a prime. Note that for any element x in this group, $x = (a_1, a_2, \ldots)$, where each $a_i \in \mathbb{Z}/p\mathbb{Z}$. It is clear to see that $p \in \mathbb{Z}$ works towards $px = (pa_1, pa_2, \ldots) =$

$(0, 0, \ldots) = 0$. Therefore we have shown an example of an infinite abelian group that is a torsion $\mathbb{Z}$-module. ■

Exercise 10.3.5

Exercise 10.3.6

Exercise 10.3.7

Exercise 10.3.8

Exercise 10.3.9 An R-module M is called irreducible if $M \neq 0$ and if 0 and M are the only submodules of M. Show that M is irreducible if and only if $M \neq 0$ and M is a cyclic module with any nonzero element as generator. Determine all the irreducible $\mathbb{Z}$-modules.

Proof. Let M be an R-module. Suppose M is irreducible. By definition, $M \neq 0$ and the only submodules of M are 0 and M itself. Since $M \neq 0$, there exists some nonzero element $m \in M$. However then Rm is a submodule of M generated by m. It follows that either $Rm = 0$ or $Rm = M$. If $Rm = 0$ then since R is a unital ring this implies $1m = m = 0$, a contradiction for we took $m \neq 0$. Thus $Rm = M$, meaning M is a cyclic module, with any $m \in M$ such that $m \neq 0$ as a generator. The above suffices to prove the statement in both directions.

In order to determine all irreducible $\mathbb{Z}$-modules, we must recall that a $\mathbb{Z}$-module is simply an abelian group, and $\mathbb{Z}$-submodules are subgroups of these abelian groups. Thus, if A is an irreducible $\mathbb{Z}$-module, the only $\mathbb{Z}$-submodules of A are 0 and A itself, to which the only subgroups of A are the trivial subgroup and A itself. In particular, A is a simple group since the only subgroups of A, which are automatically normal since A is abelian, are 0 and A itself. Therefore we may conclude that the irreducible $\mathbb{Z}$-modules are exactly the abelian simple groups. ■

Exercise 10.3.10 Assume R is commutative. Show that an R-module M is irreducible if and only if M is isomorphic (as an R-module) to R/I where I is a maximal ideal of R.

Proof. Let M be an R-module, where R is a unital commutative ring. Suppose M is irreducible. By [[DF-10.3-9]], Exercise 10.3.9, that M is a cyclic module, generated by any nonzero $m \in M$. In other words, $M = Rm$. Fix such an $m \in M$. In this way we have a natural map $\varphi : R \to M$ taking $r \mapsto rm$.

Let I be a maximal ideal of R. Now consider the field R/I as an R-module. Consider the map $\varphi : R/I \longrightarrow M$ defined by $\varphi(r+I) = rm$ for all $r + I \in R/I$. We prove that φ is a homomorphism of R-modules. To do this, let $r + I, s + I \in R/I$. Then

$$\varphi((r+I)+(s+I)) = \varphi(r+s+I) = (r+s)m = rm+sm = \varphi(r+I)+\varphi(s+I)$$

where $(r+s)m = rm+sm$ since M is an R-module. Now let $r' \in R$ be arbitrary. Then

$$\varphi(r'(r+I)) = (r'r)m = r'(rm) = r'\varphi(r+I))$$

where once more $(r'r)m = r'(rm)$ follows by module axioms. Thus the map φ above is an R-module homomorphism. In particular, if we let $n \in M$ be arbitrary, then since $M = Rm$, there exists some $s \in R$ for which $n = sm$. In other words, we have that $\varphi(s+I) = sm = n$. Thus φ is surjective. Since $\ker\varphi$ is an R-submodule of R/I by the first module isomorphism theorem, we know that $\ker\varphi$ is an ideal of R/I. However, since R/I is a field by the assumption that I is maximal, it follows that the only ideals of R/I are 0 and R/I itself. Thus either $\ker\varphi = 0$ or $\ker\varphi = R/I$. But if $\ker\varphi = R/I$ then $M \cong (R/I)/\ker\varphi = 0$. This is a contradiction, for we took $M \neq 0$. It therefore follows that $\ker\varphi = 0$, and so φ is injective. In conclusion, the map φ is an isomorphism of R-modules, and we have hence shown that M is isomorphic to R/I, for some maximal ideal I of R.

Conversely, assume that $M \cong R/I$ as R-modules, where I is some maximal ideal of R. Indeed, the fact that I is maximal implies R/I is a field, and so the only ideals of R/I are 0 and R/I itself. Since the R-submodules of R/I as an R-module are precisely the ideals of R/I, this implies that R/I has 0 and R/I itself as submodules. In other words, we have that R/I is an irreducible module; hence M is an irreducible R-module. ■

Exercise 10.3.11 Show that if M_1 and M_2 are irreducible R-modules, then any nonzero R-module homomorphism from M_1 to M_2 is an isomorphism. Deduce that if M is irreducible then $\mathrm{End}_R(M)$ is a division ring (this result is called Schur's Lemma).

Proof. Let M_1 and M_2 be irreducible R-modules. Suppose ψ is some R-module homomorphism from M_1 to M_2 that is not the zero homomorphism. We show that ψ is an isomorphism.

From the first module isomorphism theorem, we know that $M_1/\ker\psi \cong \psi(M_1)$. Indeed we then have that $\ker\psi$ is an R-submodule of M_1 and $\psi(M_1)$ is an R-submodule of M_2.

The results of [[DF-10.3-9]], Exercise 10.3.9, assure us that, since M_1 and M_2 are irreducible, the only R-submodules of M_1 and M_2 are 0 and M_1, as well as 0 and M_2, respectively.

Thus either $\ker\psi = 0$ or $\ker\psi = M_1$ and either $\psi(M_1) = 0$ or $\psi(M_1) = M_2$. If $\ker\psi = M_1$ then $M_1/\ker\psi = M_1/M_1 = 0 \cong \psi(M_1)$, implying that ψ is the zero homomorphism, a contradiction. The same is true if $\psi(M_1) = 0$. Therefore it must be the case that $\ker\psi = 0$ and $\psi(M_1) = M_2$. Equivalently, ψ is both injective and surjective, and so an isomorphism of R-modules; so $M_1 \cong M_2$.

For our deduction, take $M = M_1 = M_2$. If M is irreducible, then any R-module homomorphism from M to itself is an isomorphism. This means if $\varphi \in \operatorname{End}_R(M)$ then there exists some $\varphi^{-1} \in \operatorname{End}_R(M)$, since isomorphisms require inverses. This fact, that every nonzero element of $\operatorname{End}_R(M)$ has an inverse, permits us to write that the unital ring $\operatorname{End}_R(M)$ is a division ring.

■

Exercise 10.3.12

Exercise 10.3.13

Exercise 10.3.14

Exercise 10.3.15

Exercise 10.3.16 For any ideal I of R let IM be the submodule defined in Exercise 5 of Section 1. Let $A_1, \ldots, A_k$ be any ideals in the ring R. Prove that the map

$$M \longrightarrow M/A_1M \times M/A_2M \times \cdots \times M/A_kM \text{ defined by } m \mapsto (m + A_1M, \ldots, m + A_kM)$$

is an R-module homomorphism with kernel $A_1M \cap A_2M \cap \cdots \cap A_kM$.

Proof. Let $A_1, \ldots, A_k$ be ideals of the ring R. Recall that in [[DF-10.1-5]], Exercise 10.1.5, we showed that A_iM is an R-submodule of M for each $1 \leq i \leq k$. In particular, the direct product $\prod_{i=1}^k M/A_iM$ is a quotient R-module by Proposition 3. Consider the map $\varphi : M \longrightarrow \prod_{i=1}^k M/A_iM$ defined by $\varphi(m) = (m + A_1M, \ldots, A_kM)$ for all $m \in M$. Let $n, m \in M$ be arbitrary. Note

$$\begin{aligned}
\varphi(m+n) &= (m + n + A_1M, \ldots, m + n + A_kM) \\
&= ((m + A_1M) + (n + A_1M), \ldots, (m + A_kM) + (n + A_kM)) \\
&= (m + A_1M, \ldots, m + A_kM) + (n + A_1M, \ldots, n + A_kM) \\
&= \varphi(m) + \varphi(n)
\end{aligned}$$

and so the additive structure of the R-modules is preserved. Now let $r \in R$; we find

$$\varphi(rm) = (rm + A_1M, \ldots, rm + A_kM)$$

$$= (r(m + A_1M), \dots, r(m + A_kM))$$
$$= r(m + A_1M, \dots, m + A_kM)$$
$$= r\varphi(m)$$

and thus the axioms for an R-module homomorphism are satisfied for the map φ. To conclude the problem, we determine $\ker\varphi$ directly. Take $m \in \ker\varphi$. Then

$$\varphi(m) = (m + A_1M, \dots, m + A_kM) = (0 + A_1M, \dots, 0 + A_kM)$$

which, in turn, implies that $m \in A_iM$ for every $i \in \{1, \dots, k\}$. In other words, we have shown $m \in \bigcap_{i=1}^k A_iM$, to which $\ker\varphi \subseteq \bigcap_{i=1}^k A_iM$. The reverse inclusion is trivially clear; hence $\ker\varphi = A_1M \cap A_2M \cap \cdots \cap A_kM$, as desired. ■

Exercise 10.3.17

Exercise 10.3.18

Exercise 10.3.19

Exercise 10.3.20

Exercise 10.3.21

Exercise 10.3.22

Exercise 10.3.23

Exercise 10.3.24

Exercise 10.3.25

Exercise 10.3.26

Exercise 10.3.27

10.4 Tensor Product of Modules

Exercise 10.4.1 Let $f : R \to S$ be a ring homomorphism from the ring R to the ring S with $f(1_R) = 1_S$. Verify the details that $sr = sf(r)$ defines a right R-action on S under which S is an (S, R)-bimodule.

Proof. Consider the action $S \times R \to S$ defined by $(s, r) \mapsto sf(r)$ for all $(s, r) \in S \times R$. Let $s, s_1, s_2 \in S$ and $r, r_1, r_2 \in R$ be arbitrary. We verify that S under this right R-action is a right R-module. Note

$$(s, r_1 + r_2) \mapsto sf(r_1 + r_2) = s(f(r_1) + f(r_2)) = sf(r_1) + sf(r_2)$$

$$(s, r_1r_2) \mapsto sf(r_1r_2) = sf(r_1)f(r_2) = (sf(r_1))f(r_2)$$

$$(s_1 + s_2, r) \mapsto (s_1 + s_2)f(r) = s_1f(r) + s_2f(r)$$

While clearly $(s, 1_R) = sf(1_R) = s1_S = s$ for all $s \in S$. In particular, this right R-action gives S the structure of a right R-module. Since S is naturally a left S-module over itself, these two facts allow us to conclude that S is an (S, R)-bimodule. ■

Exercise 10.4.2 Show that the element "$2\otimes 1$" is 0 in $\mathbb{Z}\otimes_{\mathbb{Z}}\mathbb{Z}/2\mathbb{Z}$ but is nonzero in $2\mathbb{Z}\otimes_{\mathbb{Z}}\mathbb{Z}/2\mathbb{Z}$.

Proof. To verify that $2 \otimes 1$ is 0 in $\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z}$ we can see that

$$2 \otimes [1]_2 = (1 \cdot 2) \otimes [1]_2 = 1 \otimes (2 \cdot [1]_2) = 1 \otimes [2]_2 = 1 \otimes 0 = 0$$

which follows since $2 \cdot [1]_2 = [2]_2 = [0]_2$ in the ring $\mathbb{Z}/2\mathbb{Z}$, and the ring element 2 of $\mathbb{Z}$ commutes under the tensor. However, in the tensor product $2\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z}$ the same trick does not work since $1 \notin 2\mathbb{Z}$, and hence we cannot pull out the 2 from $2 \otimes [1]_2$ as we did above. ■

Exercise 10.4.3 Show that $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C}$ and $\mathbb{C} \otimes_{\mathbb{C}} \mathbb{C}$ are both left $\mathbb{R}$-modules but are not isomorphic as $\mathbb{R}$-modules.

Proof. Since $\mathbb{C}$ is, in particular, a free module of rank 1 over $\mathbb{C}$, we know from Corollary 18 that $\mathbb{C} \otimes_{\mathbb{C}} \mathbb{C} \cong \mathbb{C}$ as a left $\mathbb{C}$-module, and so in particular a left $\mathbb{R}$-module.

Now we consider $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C}$. Note that $\mathbb{C} = \mathbb{R} \oplus \mathbb{R}i$. From Theorem 17, the commutativity of $\mathbb{R}$ provides us with an isomorphism of $\mathbb{R}$-modules as follows:

$$\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C} = \mathbb{C} \otimes_{\mathbb{R}} (\mathbb{R} \oplus \mathbb{R}i) \cong (\mathbb{C} \otimes_{\mathbb{R}} \mathbb{R}) \oplus (\mathbb{C} \otimes_{\mathbb{R}} \mathbb{R}i)$$

Extending scalars (Corollary 18) gives us that $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{R} \cong \mathbb{C}$ as a left $\mathbb{C}$-module, and hence a left $\mathbb{R}$-module. Since $\mathbb{R} \cong \mathbb{R}i$ in the natural way, we have that $\mathbb{C}\otimes_{\mathbb{R}}\mathbb{C} \cong \mathbb{C}\oplus\mathbb{C}$. In particular, $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C} \ncong \mathbb{C} \otimes_{\mathbb{C}} \mathbb{C}$ as $\mathbb{R}$-modules. ■

Exercise 10.4.4

Exercise 10.4.5

Exercise 10.4.6 If R is any integral domain with quotient field Q, prove that $(Q/R) \otimes_R (Q/R) = 0$.

Proof. Let R be an integral domain and Q be its field of fractions. Any element of $(Q/R) \otimes_R (Q/R)$ can be written as

$$(\frac{a}{b} \bmod R) \otimes (\frac{c}{d} \bmod R)$$

for some $a, b, c, d \in R$ with $b, d \neq 0$. We may observe that

$$\begin{aligned}(\frac{a}{b} \bmod R) \otimes (\frac{c}{d} \bmod R) &= (d\frac{a}{bd} \bmod R) \otimes (\frac{c}{d} \bmod R) \\ &= (\frac{a}{bd} \bmod R) \otimes (d\frac{c}{d} \bmod R) \\ &= (\frac{a}{bd} \bmod R) \otimes (c \bmod R) \\ &= (\frac{a}{b} \bmod R) \otimes 0 \\ &= 0\end{aligned}$$

which follows since $c \in R$ by assumption. Therefore every simple tensor in $(Q/R) \otimes_R (Q/R)$ is equal to 0, and so $(Q/R) \otimes_R (Q/R)$ itself is equal to 0. ■

Exercise 10.4.7 If R is any integral domain with quotient field Q and N is a left R-module, prove that every element of the tensor product $Q \otimes_R N$ can be written as a simple tensor of the form $(1/d) \otimes n$ for some nonzero $d \in R$ and some $n \in N$.

Proof. Let R be an integral domain with field of fractions Q. Let N be a left R-module. Consider the tensor product $Q \otimes_R N$. Every simple tensor in $Q \otimes_R N$ may be written as

$$\frac{a}{b} \otimes n$$

for some $a, b \in R$ with $b \neq 0$ and $n \in N$. In particular, we can see

$$\frac{a}{b} \otimes n = a(\frac{1}{b}) \otimes n = \frac{1}{b} \otimes an$$

and $an \in N$ since N was assumed a left R-module, and so $an = m$ for some $m \in N$. In particular, every simple tensor in $Q \otimes_R N$ may be written as $1/b \otimes m$ for some $b \in R \setminus \{0\}$ and $m \in N$. ■

Exercise 10.4.8

Exercise 10.4.9

Exercise 10.4.10

Exercise 10.4.11

Exercise 10.4.12

Exercise 10.4.13

Exercise 10.4.14

Exercise 10.4.15

Exercise 10.4.16

Exercise 10.4.17 Let $I = (2, x)$ be the ideal generated by 2 and x in the ring $R = \mathbb{Z}[x]$. The ring $\mathbb{Z}/2\mathbb{Z} = R/I$ is naturally an R-module annihilated by both 2 and x.
(a) Show that the map $\varphi : I \times I \to \mathbb{Z}/2\mathbb{Z}$ defined by

$$\varphi(a_0 + a_1x + \cdots + a_nx^n, b_0 + b_1x + \cdots + b_mx^m) = \frac{a_0}{2}b_1 \pmod 2$$

is R-bilinear.
(b) Show that there is an R-module homomorphism from $I \otimes_R I \to \mathbb{Z}/2\mathbb{Z}$ mapping $p(x) \otimes q(x)$ to $\frac{p(0)}{2}q'(0)$ where q' denotes the usual polynomial derivative of q.
(c) Show that $2 \otimes x \neq x \otimes 2$ in $I \otimes_R I$.

Proof. (a) We manually check that the map $\varphi : I \times I \to \mathbb{Z}/2\mathbb{Z}$ in the problem description is $R = \mathbb{Z}[x]$-bilinear. We can see

$$\varphi(\sum_{i=0}^{n} a_ix^i + \sum_{i=0}^{n'} a'_ix^i, \sum_{i=1}^{m} b_ix^i) = \frac{a_0 + a'_0}{2}b_1 \pmod 2$$

$$= \frac{a_0}{2}b_1 + \frac{a'_0}{2}b_1 \pmod 2$$

$$= \varphi(\sum_{i=0}^{n} a_ix^i, \sum_{i=0}^{m} b_ix^i) + \varphi(\sum_{i=0}^{n'} a'_ix^i, \sum_{i=0}^{m} b_ix^i)$$

And for the next check we have

$$\varphi(\sum_{i=0}^{n} a_i x^i, \sum_{i=0}^{m} b_i x^i + \sum_{i=0}^{m'} b'_i x^i) = \frac{a_0}{2}(b_1 + b'_1) \pmod 2$$

$$= \frac{a_0}{2}b_1 + \frac{a_0}{2}b'_1 \pmod 2$$

$$= \varphi(\sum_{i=0}^{n} a_i x^i, \sum_{i=0}^{m} b_i x^i) + \varphi(\sum_{i=0}^{n} a_i x^i, \sum_{i=0}^{m'} b'_i x^i)$$

Finally, let $r \in R = \mathbb{Z}[x]$, so that $r = a + bx$ for $a, b \in \mathbb{Z}$. Note that

$$\varphi(\sum_{i=0}^{n} a_i x^i r, \sum_{i=0}^{m} b_i x^i) = \varphi(\sum_{i=0}^{n} (a_i r) x^i, \sum_{i=0}^{m} b_i x^i)$$

$$= \varphi(\sum_{i=0}^{n} (a_i(a + bx)) x^i, \sum_{i=0}^{m} b_i x^i)$$

$$= \varphi(\sum_{i=0}^{n} a_i a x^i + a_i b x^{i+1}, \sum_{i=0}^{m} b_i x^i)$$

$$= \varphi(\sum_{i=0}^{n} (a_i a) x^i + \sum_{i=0}^{n} (a_i b) x^{i+1}, \sum_{i=0}^{m} b_i x^i)$$

$$= \frac{a_0 a + a_0 b x}{2} b_1 \pmod 2$$

$$= \frac{a_0(a + bx)}{2} b_1 \pmod 2$$

$$= \frac{a_0}{2}(a + bx) b_1 \pmod 2$$

$$= \frac{a_0}{2}(r b_1) \pmod 2$$

$$= \varphi(\sum_{i=0}^{n} a_i x^i, \sum_{i=0}^{m} (r b_i) x^i)$$

and so indeed the mapping φ is R-bilinear, which was the desired statement.

(b) In part (a) we proved that the map $\varphi : I \times I \longrightarrow \mathbb{Z}/2\mathbb{Z}$ is $\mathbb{Z}[x] = R$-bilinear. Give I the standard R-module structure and consider $I \otimes_R I$. Corollary 12 asserts that there is a corresponding R-module homomorphism $\Phi : I \otimes_R I \longrightarrow \mathbb{Z}/2\mathbb{Z}$ such that $\Phi \circ \iota = \varphi$, where $\iota : I \times I \longrightarrow I \otimes_R I$ is given by $\iota(m, n) = m \otimes n$. In particular, $\iota(p(x), q(x)) = p(x) \otimes q(x)$ for $p(x), q(x) \in I$, and hence we require

$$\Phi(p(x) \otimes q(x)) = \varphi(p(x), q(x)) = \frac{p(0)}{2} q'(0) \pmod 2$$

which gives us the desired R-module homomorphism.

(c) Now we show that $2 \otimes x \neq x \otimes 2$ in $I \otimes_R I$. To see this, we employ the map Φ found in part (b). In particular, we have

$$\Phi(2 \otimes x) = \frac{2}{2}(1) \pmod 2 = 1 \pmod 2$$

$$\Phi(x \otimes 2) = \frac{0}{2}(0) \pmod 2 = 0 \pmod 2$$

and since one of the results of Corollary 12 is that the map Φ is well-defined, if $2 \otimes x = x \otimes 2$ held true then their images under Φ would have to agree. Clearly this is not the case, so we must have $2 \otimes x \neq x \otimes 2$, as desired.

■

Exercise 10.4.18

Exercise 10.4.19

Exercise 10.4.20

Exercise 10.4.21

Exercise 10.4.22

Exercise 10.4.23

Exercise 10.4.24

Exercise 10.4.25

Exercise 10.4.26

Exercise 10.4.27

10.5 Exact Sequences–Projective, Injective, and Flat Modules

Exercise 10.5.1 Suppose that

$$\begin{array}{ccccc} A & \xrightarrow{\psi} & B & \xrightarrow{\varphi} & C \\ \alpha\downarrow & & \beta\downarrow & & \gamma\downarrow \\ A' & \xrightarrow{\psi'} & B' & \xrightarrow{\varphi'} & C' \end{array}$$

is a commutative diagram of groups and that the rows are exact. Prove that
(a) if φ and α are surjective, and β is injective then γ is injective. [If $c \in \ker\gamma$, show there is a $b \in B$ with $\varphi(b) = c$. Show that $\varphi'(\beta(b)) = 0$ and deduce that $\beta(b) = \psi'(a')$ for some $a' \in A'$. Show there is an $a \in A$ with $\alpha(a) = a'$ and that $\beta(\psi(a)) = \beta(b)$. Conclude that $b = \psi(a)$ and hence $c = \varphi(b) = 0$.]
(b) if ψ', α, and γ are injective, then β is injective.
(c) if φ, α, and γ are surjective, then β is surjective.
(d) if β is injective, α and φ are surjective, then γ is injective. (e) if β is surjective, γ and ψ' are injective, then α is surjective.

Proof. (a) Suppose φ and α are surjective, and that β is injective. Assume $c \in \ker\gamma$. Since $\varphi : B \to C$ is surjective, there exists $b \in B$ for which $\varphi(b) = c$. Since the diagram was assumed to commute, we require that $\varphi'(\beta(b)) = 0$. Thus $\beta(b) \in \ker\varphi'$, and since the bottom row in the diagram is exact, this is equivalent to $\beta(b) \in \operatorname{im}\psi'$. Since $\psi' : A' \to B'$, we know there exists some $a' \in A'$ for which $\psi'(a') = \beta(b)$. Now, since we assumed $\alpha : A \to A'$ was surjective, there exists some $a \in A$ for which $\alpha(a) = a'$. The commutativity of the diagram once more asserts that $\beta(\psi(a)) = \beta(b)$. Injectivity of β provides $\psi(a) = b$. However, above we saw that $\varphi(b) = c$, and so now we may note that $\varphi(\psi(a)) = c$. But the top row is exact, and so $\operatorname{im}\psi = \ker\varphi$. Since $\psi(a) \in \operatorname{im}\psi$, this means $\psi(a) \in \ker\varphi$, so that $\varphi(\psi(a)) = 0$, and hence $c = 0$. Therefore, $\ker\gamma = \{0\}$, and hence γ is injective.

(b) Suppose ψ', α, and γ are injective. Assume $b \in \ker\beta$. We know that $\varphi(b) = c$ for some $c \in C$, and further that $\gamma(c) = 0$ since the diagram commutes, and $\beta(b) = 0$ implies $\varphi'(\beta(b)) = 0$. This means that $c \in \ker\gamma$, and since γ is injective we have $c = 0$. Now $\varphi(b) = 0$, so that $b \in \ker\varphi$, and since the top row is exact, $b \in \operatorname{im}\psi$. Thus there exists $a \in A$ for which $\psi(a) = b$. Since $\beta(b) = 0$, the commutativity of the diagram forces $\psi'(\alpha(a)) = 0$. Since ψ' is injective, this means $\alpha(a) = 0$, and since α is injective, this means $a = 0$. But then $\psi(0) = b$, and so $b = 0$. Thus $\ker\beta = \{0\}$ and so β is injective.

(c) Suppose φ, α, γ are surjective. Let $b' \in B'$. We know that $\varphi'(b') = c'$ for some $c' \in C'$, and furthermore that there exists some $c \in C$ for which $\gamma(c) = c'$ by surjectivity of γ. Since φ is surjective, there exists $b \in B$ for which $\varphi(b) = c$.

Now, by commutativity of the diagram, we require $\varphi'(\beta(b)) = c'$ as well, and so $\varphi'(\beta(b)) = \varphi'(b')$. Now

$$\varphi'(\beta(b))\varphi'(b')^{-1} = 0 \iff \varphi'(\beta(b)(b')^{-1}) = 0$$

and so $\beta(b)(b')^{-1} \in \ker\varphi'$. Since the bottom row is exact, this means that $\beta(b)(b')^{-1} \in \operatorname{im}\psi'$ and so there exists $a' \in A$ such that $\psi'(a') = \beta(b)(b')^{-1}$. Since α is surjective, there exists $a \in A$ such that $\alpha(a) = a'$. By commutativity of the diagram, we know that $\beta(\psi(a)) = \beta(b)(b')^{-1}$. Now

$$b' = \beta(\psi(a))^{-1}\beta(b) = \beta(\psi(a)^{-1}b)$$

and since $\psi(a)^{-1}b \in B$, we have found such an element of B which equals b' under β. In particular, this shows that β is surjective, as desired.

(d) Suppose β is injective, α and φ are surjective. Assume $c \in \ker\gamma$. Since φ is surjective, there exists $b \in B$ such that $\varphi(b) = c$. Since the diagram commutes, we know $\varphi'(\beta(b)) = 0$ is required. This means that $\beta(b) \in \ker\varphi'$, and since the bottom row is exact, we have that $\beta(b) \in \operatorname{im}\psi'$ as well. Thus, there exists some $a' \in A'$ for which $\psi'(a') = \beta(b)$. Since $\alpha : A \to A'$ is surjective by assumption, there also exists some $a \in A$ such that $\alpha(a) = a'$.

To summarize: we have $\psi'(\alpha(a)) = \beta(b)$. Furthermore, since the diagram commutes, we require $\beta(\psi(a)) = \beta(b)$. Since β is injective, this implies $\psi(a) = b$. However, it is obvious that $\psi(a) \in \operatorname{im}\psi$, and since the top row is exact, we have $\operatorname{im}\psi = \ker\varphi$, so that $\psi(a) \in \ker\varphi$. Now $\varphi(\psi(a)) = 0$ and so $\varphi(b) = 0$. But we assumed that $\varphi(b) = c$, and so it follows that $c = 0$. Hence $\ker\gamma = \{0\}$, and thus γ is injective.

(e) Suppose β is surjective, γ and ψ' are injective. Let $a' \in A'$ be arbitrary. Obviously $\psi'(a') \in \operatorname{im}\psi'$, and since the bottom row is exact this means $\psi'(a') \in \ker\varphi'$. Hence $\varphi'(\psi'(a')) = 0$.

Now, since β is surjective, there exists some $b \in B$ for which $\beta(b) = \psi'(a')$. From the commutativity of the diagram, we require $\gamma(\varphi(b)) = 0$ to hold as well (since above $\varphi'(\psi'(a')) = 0$ holds). However, since γ is injective by assumpton, this means $\varphi(b) = 0$. In particular, we have $b \in \ker\varphi$. The exactness of the top row implies that $b \in \operatorname{im}\psi$. Hence there exists $a \in A$ for which $\psi(a) = b$.

In particular, $\beta(\psi(a)) = \psi'(a')$ must hold since $\beta(b) = \psi'(a')$, as we saw above. By commutativity of the diagram, we require $\psi'(\alpha(a)) = \psi'(a')$ to hold as well. But injectivity of ψ' assures us that $\alpha(a) = a'$. Thus we have found some $a \in A$ which equals a' under α, and since a' was arbitrary this means α is surjective. ■

Exercise 10.5.2 Suppose that

$$\begin{tikzcd} A \arrow[r] \arrow[d, "\alpha"'] & B \arrow[r] \arrow[d, "\beta"'] & C \arrow[r] \arrow[d, "\gamma"'] & D \arrow[d, "\delta"'] \\ A' \arrow[r] & B' \arrow[r] & C' \arrow[r] & D' \end{tikzcd}$$

is a commutative diagram of groups, and that the rows are exact. Prove that
(a) if α is surjective, and β, δ are injective, then γ is injective.
(b) if δ is injective, and α, γ are surjective, then β is surjective.

Proof. (a) Suppose α is surjective and β, δ are injective. We will write

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[d, "\alpha"'] & B \arrow[r, "g"] \arrow[d, "\beta"'] & C \arrow[r, "h"] \arrow[d, "\gamma"'] & D \arrow[d, "\delta"'] \\ A' \arrow[r, "f'"] & B' \arrow[r, "g'"] & C' \arrow[r, "h'"] & D' \end{tikzcd}$$

for convenience. Assume $c \in \ker \gamma$. Then $\gamma(c) = 0$, and in particular we know that $h'(\gamma(c)) = 0$ also holds. By commutativity of the diagram we know $\delta(h(c)) = 0$ as well. Since δ is injective, $h(c) = 0$. Thus $c \in \ker h$ and so $c \in \operatorname{im} g$ by exactness of the top row. In particular, there exists $b \in B$ such that $g(b) = c$.

Once again, commutativity of the diagram asserts that $g'(\beta(b)) = \gamma(g(b))$ and so $g'(\beta(b)) = 0$. In particular, $\beta(b) \in \ker g'$ and so $\beta(b) \in \operatorname{im} f'$ by exactness of the bottom row. Thus there exists $a' \in A'$ for which $f'(a') = \beta(b)$. Since α is surjective, there exists $a \in A$ for which $\alpha(a) = a'$.

In particular, we kow that $f'(\alpha(a)) = \beta(f(a))$ by commutativity of the diagram. This means $\beta(b) = \beta(f(a))$. Since β was assumed injective, we have $b = f(a)$. With this in mind clearly we have $b = f(a) \in \operatorname{im} f$, and since the top row is exact, we have $b = f(a) \in \ker g$. Hence $g(b) = 0$. However, above we saw that $g(b) = c$, and so we require $c = 0$. Therefore $\ker \gamma = \{0\}$, and so γ is injective, as desired.

(b) Suppose δ is injective, and α, γ are surjective. We aim to show that β is surjective. Refer to the diagram given in part (a). Let $b' \in B'$ be arbitrary. Then $g'(b') \in \operatorname{im} g'$ and by exactness of the bottom row we have $g'(b') \in \ker h'$. Thus $h'(g'(b')) = 0$.

Now, since $g'(b') \in C'$, the surjectivity of γ implies that there exists $c \in C$ for which $\gamma(c) = g'(b')$. Since the diagram commutes, we require that $\delta(h(c)) = h'(g'(b')) = 0$. But since δ is injective by assumption, this means $h(c) = 0$. Thus $c \in \ker h$ and by exactness of the top row we have $c \in \operatorname{im} g$. Now there exists some $b \in B$ for which $g(b) = c$.

Then commutativity of the diagram means $g'(\beta(b)) = \gamma(g(b))$ and so $g'(\beta(b)) = g'(b')$. In particular, we have

$$g'(\beta(b))g'(b')^{-1} = 0 \iff g'(\beta(b)(b')^{-1}) = 0$$

since $g' : B' \to C'$ is a group homomorphism. The above indicates that $\beta(b)(b')^{-1} \in \ker g'$, and so $\beta(b)(b')^{-1} \in \text{im } f'$ by exactness. Thus there exists $a' \in A'$ for which $f'(a') = \beta(b)(b')^{-1}$. Since α is surjective by assumption, there exists $a \in A$ for which $\alpha(a) = a'$ as well. Commutativity of the diagram forces $\beta(f(a)) = f'(\alpha(a))$, which is equivalent to $\beta(f(a)) = \beta(b)(b')^{-1}$. We have

$$\beta(f(a)) = \beta(b)(b')^{-1} \iff b' = \beta(f(a))^{-1}\beta(b) = \beta(f(a)^{-1}b)$$

since $\beta : B \to B'$ is a group homomorphism. However note that we have found an element $f(a)^{-1}b \in B$ which equals b' under β. Since $b' \in B'$ was arbitrary, this proves that β is surjective, as desired. ■

Exercise 10.5.3 Let P_1 and P_2 be R-modules. Prove that $P_1 \oplus P_2$ is a projective R-module if and only if both P_1 and P_2 are projective.

Proof. Suppose $P_1 \oplus P_2$ is a projective R-module. Then $P_1 \oplus P_2$ is the direct summand of a free R-module, i.e., $F = P_1 \oplus P_2 \oplus K$ for some R-submodule K of F. In particular, both P_1 and P_2 are direct summands of a free R-module, namely F, since they are in particular direct summands of $P_1 \oplus P_2$.

We prove the converse. Suppose P_1 and P_2 are projective R-modules. Then there exists free R-modules F and F' for which $F = P_1 \oplus K$ and $F' = P_2 \oplus K'$. In Exercise 10.3.23 we showed that the direct sum of free R-modules is once again free, and so $F \oplus F'$ is free. Note

$$F \oplus F' = P_1 \oplus K \oplus P_2 \oplus K' = (P_1 \oplus P_2) \oplus (K \oplus K')$$

and so clearly $P_1 \oplus P_2$ is a direct summand of the free R-module $F \oplus F'$, and so is itself projective by Proposition 30(4). ■

Exercise 10.5.4 Let Q_1 and Q_2 be R-modules. Prove that $Q_1 \oplus Q_2$ is an injective R-module if and only if both Q_1 and Q_2 are injective.

Proof. Suppose Q_1 and Q_2 are injective. Let L and M be R-modules and suppose $0 \to L \xrightarrow{\psi} M$ is exact. Suppose $f \in \text{Hom}_R(L, Q_1 \oplus Q_2)$. We have natural projection R-module homomorphisms given by $\pi_1 : Q_1 \oplus Q_2 \to Q_1$ and $\pi_2 : Q_1 \oplus Q_2 \to Q_2$. In particular, $\pi_1 \circ f \in \text{Hom}_R(L, Q_1)$ and $\pi_2 \circ f \in \text{Hom}_R(L, Q_2)$ since the composition of R-module homomorphisms is an R-module homomorphism. Now, since Q_1 and Q_2 are injective, Proposition 34(2) asserts that there exists a lift

$F_1 \in \mathrm{Hom}_R(M, Q_1)$ and $F_2 \in \mathrm{Hom}_R(M, Q_2)$ such that

$$\begin{tikzcd} 0 \arrow[r] & L \arrow[r, "\psi"] \arrow[d, "f"'] & M \arrow[ddl, "F_1"] \\ & Q_1 \oplus Q_2 \arrow[d, "\pi_1"'] & \\ & Q_1 & \end{tikzcd}$$

commutes; i.e., we have $F_1 \circ \psi = \pi_1 \circ f$, and likewise we have $F_2 \circ \psi = \pi_2 \circ f$. Now construct a map $\tilde{F} : M \to Q_1 \oplus Q_2$ defined by $\tilde{F}(m) = (F_1(m), F_2(m))$ for all $m \in M$. It is obvious to see that $\tilde{F}$ is an R-module homomorphism as a consequence of F_1 and F_2 being R-module homomorphisms.

What remains is to check that $\tilde{F} \circ \psi = f$. So take $l \in L$. Assume $f(l) = (q_1, q_2)$ for $q_1 \in Q_1$ and $q_2 \in Q_2$. Then $\pi_1(f(l)) = q_1$ and $\pi_2(f(l)) = q_2$. As above, we have $F_1(\psi(l)) = q_1$ and $F_2(\psi(l)) = q_2$. Now we have

$$\tilde{F}(\psi(l)) = (F_1(\psi(l)), F_2(\psi(l))) = (q_1, q_2) = f(l)$$

and so the diagram commutes. In partocular, the diagram

$$\begin{tikzcd} 0 \arrow[r] & L \arrow[r, "\psi"] \arrow[d, "f"'] & M \arrow[dl, "\tilde{F}"] \\ & Q_1 \oplus Q_2 & \end{tikzcd}$$

commutes, and so by Proposition 34(2) we have that $Q_1 \oplus Q_2$ is an injective R-module.

Conversely, suppose $Q_1 \oplus Q_2$ is injective. Let L and M be R-modules and suppose $0 \to L \xrightarrow{\psi} M$ is exact. Suppose $f_1 \in \mathrm{Hom}_R(L, Q_1)$ and $f_2 \in \mathrm{Hom}_R(L, Q_2)$. We then have an obvious R-module homomorphism given by $f : L \to Q_1 \oplus Q_2$ defined by $f(l) = (f_1(l), f_2(l))$ for all $l \in L$. By assumption that $Q_1 \oplus Q_2$ is injective, there exists a lift $F : M \to Q_1 \oplus Q_2$ such that $F \circ \psi = f$. We have a diagram

$$\begin{tikzcd} & Q_1 \arrow[rrr, bend left, "\iota_1"] & & & \\ 0 \arrow[r] & L \arrow[u, "f_1"] \arrow[d, "f_2"', dash] \arrow[r, "\psi"] \arrow[rr, bend right, "f"'] & M \arrow[r, "F"] & Q_1 \oplus Q_2 & \\ & Q_2 \arrow[urr, bend right, "\iota_2"'] & & & \end{tikzcd}$$

Then it is clear that $\pi_1 \circ F : M \to Q_1$ and $\pi_2 \circ F : M \to Q_2$ are both R-module homomorphisms. Furthermore, $(\pi_1 \circ F) \circ \psi = f_1$ and $(\pi_2 \circ F) \circ \psi = f_2$ since if $l \in L$ and $f_1(l) = q_1$ and $f_2(l) = q_2$, then

$$\pi_1(F(\psi(l))) = \pi_1(f(l)) = \pi_1(f_1(l), f_2(l)) = q_1$$

$$\pi_2(F(\psi(l))) = \pi_2(f(l)) = \pi_2(f_1(l), f_2(l)) = q_2$$

and therefore there exists lifts $\pi_1 \circ F \in \mathrm{Hom}_R(M, Q_1)$ and $\pi_2 \circ F \in \mathrm{Hom}_R(M, Q_2)$, which makes Q_1 and Q_2 injective by Proposition 34(2). ■

Exercise 10.5.5. Let A_1 and A_2 be R-modules. Prove that $A_1 \oplus A_2$ is a flat R-module if and only if each A_i is flat. More generally, prove that an arbitrary direct sum $\sum A_i$ of R-modules is flat if and only if each A_i is flat. [Use the fact that tensor product commutes with arbitrary direct sums.]

Proof. Suppose $\bigoplus_i A_i$ is a flat R-module, and let $0 \to L \to M \to N \to 0$ be an arbitrary short exact sequence of R-modules. We then have a commutative diagram:

$$\begin{tikzcd}
0 \arrow[r] & (\bigoplus_i A_i) \otimes_R L \arrow[r, hook] \arrow[d, "\cong"] & (\bigoplus_i A_i) \otimes_R M \arrow[r, two heads] \arrow[d, "\cong"] & (\bigoplus_i A_i) \otimes_R N \arrow[r] \arrow[d, "\cong"] & 0 \\
0 \arrow[r] & \bigoplus_i (A_i \otimes_R L) \arrow[r, hook] \arrow[d, two heads] & \bigoplus_i (A_i \otimes_R M) \arrow[r, two heads] \arrow[d, two heads] & \bigoplus_i (A_i \otimes_R N) \arrow[r] \arrow[d, two heads] & 0 \\
0 \arrow[r] & A_i \otimes_R L \arrow[r, hook] & A_i \otimes_R M \arrow[r, two heads] & A_i \otimes_R N \arrow[r] & 0
\end{tikzcd}$$

Where the first row is a short exact sequence since $\bigoplus_i A_i$ is flat, and the isomorphisms going down into the second row are those induced via the fact that tensor products commute with direct sums, Exercise 10.4.14, or also Theorem 17 in Section 10.4. Now, from the second row to the last row, we have projections onto the components of the direct sums, which preserve the short exact sequence. In particular, for each i, we have a short exact sequence $0 \to A_i \otimes_R L \to A_i \otimes_R M \to A_i \otimes_R N \to 0$, hence that each A_i is a flat R-module since the initial exact sequence was arbitrary.

To see the converse, if we have A_i flat R-modules for all i in some arbitrary index set, then for an arbitrary short exact sequence $0 \to L \to M \to N \to 0$, we have short exact sequences $0 \to A_i \otimes_R L \to A_i \otimes_R M \to A_i \otimes_R N \to 0$ for each i, and so taking the direct sum of each, combined with the commutativity of tensor products with direct sums, we get our result. ■

Exercise 10.5.6. Prove that the following are equivalent for a ring R:
(i) Every R-module is projective.
(ii) Every R-module is injective.

Proof. Let R be a ring. Suppose every R-module is projective. Let Q be an arbitrary R-module. We show Q is injective. To do this, we show that Q satisfies Proposition 34(3). So suppose $0 \to Q \to M \to N \to 0$ is a short exact sequence of R-modules.

Since N is an R-module, by assumption we have that N is projective. In particular, every short exact sequence $0 \to L \to M \to N \to 0$ splits. In our case, take $L = Q$. Hence $0 \to Q \to M \to N \to 0$ splits, and so Q is injective.

Conversely, suppsoe every R-module is injective. Let P be an arbitrary R-module. We show that P is projective by showing that P satisfies Proposition 30(3). So suppose $0 \to L \to M \to P \to 0$ is a short exact sequence of R-modules. By assumption L is an injective R-module, and hence every short exact sequence $0 \to L \to M \to N \to 0$ splits. Take $N = P$. Then $0 \to L \to M \to P \to 0$ splits and so P is projective. ∎

Exercise 10.5.7. Let A be a nonzero finite abelian group.
(a) Prove that A is not a projective $\mathbb{Z}$-module.
(b) Prove that A is not an injective $\mathbb{Z}$-module.

Proof. (a) Assume, for contradiction, that A is a projective $\mathbb{Z}$-module. Then by Proposition 30(4), we know A is a direct summand of a free $\mathbb{Z}$-module, say $A \oplus B \cong \mathbb{Z}^n$ for some abelian group B and $n \in \mathbb{Z}^+$. However, no elements in the group $\mathbb{Z}^n$ have finite order, while every element of the subgroup A of $A \oplus B$ has finite order. Hence $A = 0$ is forced, contradicting our assumption that $A \neq 0$, and hence also that A is projective.

(b) Assume, for contradiction, that A is an injective $\mathbb{Z}$-module. Since $\mathbb{Z}$ is a P.I.D., we may apply Proposition 36(2) to write that A is divisible, and hence that $nA = A$ for any $n \in \mathbb{Z} \setminus \{0\}$. Since A is finite, however, we have $|A| = m$ for some integer m, and clearly $mA = 0$ since $ma = 0$ for all $a \in A$. Thus $A = 0$, a contradiction, to which A is not injective. ∎

Exercise 10.5.8.

Exercise 10.5.9. Assume R is commutative with 1.
(a) Prove that the tensor product of two free R-modules is free. [Use the fact that tensor products commute with direct sums.]
(b) Use (a) to prove that the tensor product of two projective R-modules is projective.

Proof. (a) Let M and N be two free R-modules. If $M \cong R^m$ and $N \cong R^n$ where $m, n < \infty$ then Corollary 19 in Section 10.4 gives that $M \otimes_R N \cong R^{nm}$, hence that the tensor product of M and N is free.

Without loss of generality, suppose that N is a free R-module of infinite rank.

Then from Exercise 10.4.14 we know that

$$M \otimes_R N \cong M \otimes_R (\bigoplus_{i=1}^{\infty} R) \cong \bigoplus_{i=1}^{\infty}(M \otimes_R R) \cong \bigoplus_{i=1}^{\infty} M$$

Now, since M is a free R-module, and the direct sum of free R-modules is free by Exercise 10.3.23, we know that $M \otimes_R N$ above is free as an R-module as well. Note also that the above deals with the case where M is of infinite rank as well; hence we conclude that the tensor product of free R-modules is free.

(b) Let P_1 and P_2 be projective R-modules. Then from Proposition 30(4) both P_1 and P_2 are direct summands of some free modules. Let $P_1 \oplus N_1 \cong F_1$ and $P_2 \oplus N_2 \cong F_2$, where F_1 and F_2 are free R-modules. We have

$$\begin{aligned} F_1 \otimes_R F_2 &\cong (P_1 \oplus N_1) \otimes_R (P_2 \oplus N_2) \\ &\cong (P_1 \otimes_R (P_2 \oplus N_2)) \oplus (N_1 \otimes_R (P_2 \oplus N_2)) \\ &\cong (P_1 \otimes_R P_2) \oplus (P_1 \otimes_R N_2) \oplus (N_1 \otimes_R P_2) \oplus (N_1 \otimes_R N_2) \end{aligned}$$

Where the first isomorphism is clear, and the second and third isomorphisms follow from Theorem 17 in Section 10.4, tensor products of direct sums.

Since $F_1 \otimes_R F_2$ is free by part (a) above, we have proved that $P_1 \otimes_R P_2$ is a direct summand of a free module, and hence by the same proposition that $P_1 \otimes_R P_2$ is projective as an R-module. ∎

Exercise 10.5.10. Let R and S be rings with 1 and let M and N be left R-modules. Assume also that M is an (R, S)-bimodule.
(a) For $s \in S$ and for $\varphi \in \mathrm{Hom}_R(M, N)$ define $(s\varphi) : M \to N$ by $(s\varphi)(m) = \varphi(ms)$. Prove that $s\varphi$ is a homomorphism of left R-modules, and that this action of S on $\mathrm{Hom}_R(M, N)$ makes it into a *left* S-module.
(b) Let $S = R$ and $M = R$ (considered as an (R, R)-bimodule by left and right ring multiplication on itself). For each $n \in N$ define $\varphi_n : R \to N$ by $\varphi_n(r) = rn$, i.e., φ_n is the unique R-module homomorphism mapping 1_R to n. Show that $\varphi_n \in \mathrm{Hom}_R(R, N)$. Use part (a) to show that the map $n \mapsto \varphi_n$ is an isomorphism of left R-modules: $N \cong \mathrm{Hom}_R(R, N)$.
(c) Deduce that if N is a free (respectively, projective, injective, flat) left R-module, then $\mathrm{Hom}_R(R, N)$ is also a free (respectively, projective, injective, flat) left R-module.

Proof. (a) Take $s \in S$ and $\varphi \in \mathrm{Hom}_R(M, N)$. We prove that $s\varphi$ is a left R-module homomorphism. Observe that for $m, n \in M$ and all $r \in R$ we have

$$(s\varphi)(m + n) = \varphi((m + n)s) = \varphi(ms + ns) = \varphi(ms) + \varphi(ns) = (s\varphi)(m) + (s\varphi)(n)$$

$$(s\varphi)(rm) = \varphi((rm)s) = \varphi(r(ms)) = r\varphi(ms) = r(s\varphi)(m)$$

where we have used the assumption that φ is an R-module homomorphism from M to N. Now we show that

$$S \times \mathrm{Hom}_R(M, N) \to \mathrm{Hom}_R(M, N)$$

$$(s, \varphi) \longmapsto (s\varphi)$$

is a left action of S on $\mathrm{Hom}_R(M, N)$. For $r, s \in S$ and any $m \in M$ we have

$$((r+s)\varphi)(m) = \varphi(m(r+s)) = \varphi(mr + ms) = \varphi(mr) + \varphi(ms) = (r\varphi)(m) + (s\varphi)(m)$$

$$((rs)\varphi)(m) = \varphi(m(rs)) = \varphi((mr)s) = (s\varphi)(mr) = r(s\varphi)(m)$$

$$(r)(\varphi + \psi)(m) = (\varphi + \psi)(mr) = \varphi(mr) + \psi(mr) = (r\varphi)(m) + (r\psi)(m)$$

where the final equality in the second line above comes from the assumptino that $(s\varphi)$ is a left R-module homomorphism, which we showed above. In particular, the above verifications make $\mathrm{Hom}_R(M, N)$ into a left S-module, as desired.

(b) Fix $n \in N$. First we show that $\varphi_n : R \to N$ defined by $r \mapsto rn$ for all $r \in R$ is am R-module homomorphism from R to N. For $r, r', s \in R$ we have

$$\varphi_n(r+s) = (r+s)n = rn + sn = \varphi_n(r) + \varphi_n(s)$$

$$\varphi_n(rr') = (rr')n = r(r'n) = r\varphi_n(r')$$

which gives us the result. Now we construct a map $\Psi : N \to \mathrm{Hom}_R(R, N)$ defined by $\Psi(n) = \varphi_n$ for all $n \in N$. Let $n, m \in N$ and $s, r \in R$ be arbitrary. Observe

$$\Psi(n+m)(r) = \varphi_{n+m}(r) = r(m+n) = rn + rm = \varphi_n(r) + \varphi_m(r) = (\Psi(n) + \Psi(m))(r)$$

$$\Psi(rn) = \varphi_{rn}(s) = s(rn) = (sr)n = \varphi_n(sr) = (r\varphi_n)(s) = (r\Psi(n))(s)$$

and hence Ψ is an R-module homomorphism. We show Ψ is bijective. Let $\varphi \in \mathrm{Hom}_R(R, N)$ be arbitrary. We know that φ is determined by where it sends 1_R, and so take $n = \varphi(1_R)$. Now we have $\varphi(r) = \varphi(r1_R) = \varphi(r)\varphi(1_R) = \varphi(r)n$ for all $r \in R$, so just take φ_n; hence Ψ is surjective. For injectivity, assume $\Psi(n) = \Psi(n')$. Then $\varphi_n(r) = \varphi_{n'}(r)$ for all $r \in R$, in particular for $r = 1_R$, and hence $\varphi_n(1_R) = \varphi_{n'}(1_R)$ means that $1_R n = 1_R n'$ and so $n = n'$, Hence Ψ is injective as well; thus a bijection and so an isomorphism of left R-modules $N \cong \mathrm{Hom}_R(R, N)$.

(c) It is automatic that if N is either projective, injective, flat, free, then $\mathrm{Hom}_R(R, N)$ satisfies the same properties via the isomorphism. ■

Exercise 10.5.11. Let R and S be rings with 1 and let M and N be left R-modules. Assume also that N is an (R, S)-bimodule.

(a) For $s \in S$ and for $\varphi \in \mathrm{Hom}_R(M, N)$ define $(\varphi s) : M \to N$ by $(\varphi s)(m) = \varphi(m)s$. Prove

that φs is a homomorphism of left R-modules, and that this action of S on $\text{Hom}_R(M, N)$ makes it into a *right* S-module. Deduce that $\text{Hom}_R(M, R)$ is a right R-module, for any R-module M–called the *dual module* to M.
(b) Let $N = R$ considered as an (R, R)-bimodule as usual. Under the action defined in part (a) show that the map $r \mapsto \varphi_r$ is an isomorphism of right R-modules: $\text{Hom}_R(R, R) \cong R$, where φ_r is the homomorphism that maps 1_R to r. Deduce that if M is a finitely generated free left R-module, then $\text{Hom}_R(M, R)$ is a free right R-module of the same rank. (cf. also Exercise 13.)
(c) Show that if M is a finitely generated projective R-module then its dual module $\text{Hom}_R(M, R)$ is also projective.

Proof. (a) For any $s \in S$ and $\varphi \in \text{Hom}_R(M, N)$, the map $(\varphi s) : M \to N$ sending m to $\varphi(m)s$ is well-defined since N is, in particular, a right S-module, and hence $\varphi(m)s \in N$. Let $\varphi, \psi \in \text{Hom}_R(M, N)$ and $s, s' \in S$ be arbitrary. Then we can see that

$$((\varphi + \psi)s)(m) = (\varphi + \psi)(m)s = (\varphi(m) + \psi(m))s = \varphi(m)s + \psi(m)s = (\varphi s)(m) + (\psi s)(m)$$

$$(\varphi(ss'))(m) = \varphi(m)ss' = (\varphi(m)s)s' = (\varphi s)(m)s' = ((\varphi s)s')(m)$$

$$(\varphi(s + s'))(m) = \varphi(m)(s + s') = \varphi(m)s + \varphi(m)s' = (\varphi s)(m) + (\varphi s')(m)$$

and hence $\text{Hom}_R(M, N)$ is a right S-module. Moreover, taking $S = R$ and $N = R$ gives us that $\text{Hom}_R(M, R)$ is a right R-module, in fact for any R-module M.

(b) Consider R as an (R, R)-bimodule over itself. Consider the map

$$R \longrightarrow \text{Hom}_R(R, R)$$

$$r \mapsto \varphi_r$$

where $\varphi_r : R \to R$ is defined by $\varphi_r(1_R) = r$, which suffices to define the map on all of R. To see that the above mapping is injective, note that if $\varphi_r = \varphi_{r'}$ then $r = r'$ is forced, since the maps agree on their value for 1_R. For surjectivity, simply note that any R-module homomorphism from R to R is completely determined by its value on 1_R, and hence if $\psi : R \to R$ is such a homomorphism, then $\psi(1_R) \in R$. Hence the mapping is an isomorphism, and so $R \cong \text{Hom}_R(R, R)$.

Now assume M is a finitely generated free left R-module. Then $M \cong R^n$ for some $n \in \mathbb{Z}^+$. In particular, we have that

$$\text{Hom}_R(M, R) \cong \text{Hom}_R(R^n, R) \cong \bigoplus_{i=1}^{n} \text{Hom}_R(R, R) \cong \bigoplus_{i=1}^{n} R = R^n$$

where the second isomorphism of R-modules comes from Proposition 29(2). The above shows that $\text{Hom}_R(M, R)$ is a free right R-module with rank equal to that of

M.

(c) Now suppose that M is a finitely generated projective left R-module. Corollary 31 asserts that M is a direct summand of a free R-module, i.e., we have $M \oplus L \cong R^n$ for some R-module L and $n \in \mathbb{Z}^+$. Note that

$$\mathrm{Hom}_R(M,R) \oplus \mathrm{Hom}_R(L,R) \cong \mathrm{Hom}_R(M \oplus L, R) \cong \mathrm{Hom}_R(R^n, R) \cong R^n$$

The second isomorphism above follows via Proposition 29(2) and the third from our work in part (b) above. In particular, the dual module $\mathrm{Hom}_R(M,R)$ is a direct summand of a free R-module, and hence is projective by Corollary 31 once more. ■

Exercise 10.5.12.

Exercise 10.5.13.
(a) Show that the dual of the free $\mathbb{Z}$-module with countable basis is not free. [Use the preceding exercise and Exercise 24, Section 3.] (See also Exercise 5 in Section 11.3.)
(b) Show that the dual of the free $\mathbb{Z}$-module with countable basis is also not projective. [You may use the fact that any submodule of a free $\mathbb{Z}$-module is free.]

Proof. (a) Let $\mathbb{Z}^{\mathbb{N}}$ denote the free $\mathbb{Z}$-module with countable basis. Then dual $\mathbb{Z}$-module to $\mathbb{Z}^{\mathbb{N}}$ is $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}^{\mathbb{N}}, \mathbb{Z})$. Since we have the isomorphism $\mathbb{Z}^{\mathbb{N}} \cong \bigoplus_{n\in\mathbb{N}} \mathbb{Z}$, we know from Exercise 10.5.12(a) that

$$\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}^{\mathbb{N}}, \mathbb{Z}) \cong \mathrm{Hom}_{\mathbb{Z}}\left(\bigoplus_{n\in\mathbb{N}} \mathbb{Z}, \mathbb{Z}\right) \cong \prod_{n\in\mathbb{N}} \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z},\mathbb{Z}) \cong \prod_{n\in\mathbb{N}} \mathbb{Z}$$

where the final isomorphism of $\mathbb{Z}$-modules above follows from Exercise 10.2.9, since $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z},\mathbb{Z}) \cong \mathbb{Z}$ holds. In particular, we have shown that

$$\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}^{\mathbb{N}}, \mathbb{Z}) \cong M$$

where M is the $\mathbb{Z}$-module of Exercise 10.3.24; in that exercise, we showed that M is not a free $\mathbb{Z}$-module, and hence we may conclude that the dual of the free $\mathbb{Z}$-module with countable basis is not free.

(b) Now we claim that the dual of the free $\mathbb{Z}$-module with countable basis, $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}^{\mathbb{N}}, \mathbb{Z})$, is not projective. To see why, assume the contrary, that is, that $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}^{\mathbb{N}}, \mathbb{Z})$ is projective as a $\mathbb{Z}$-module. From Proposition 30(4), we know $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}^{\mathbb{N}}, \mathbb{Z})$ is a direct summand of a free $\mathbb{Z}$-module. Note, however, that any submodule of a free $\mathbb{Z}$-module si free, and hence $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}^{\mathbb{N}}, \mathbb{Z})$ must be free, a contradiction, for in part (a) above we showed this is impossible. Therefore $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}^{\mathbb{N}}, \mathbb{Z})$ is not projective, as desired. ■

Exercise 10.5.14.

Exercise 10.5.15. Let M be a left $\mathbb{Z}$-module and let R be a ring with 1.
(a) Show that $\mathrm{Hom}_{\mathbb{Z}}(R, M)$ is a left R-module under the action $(r\varphi)(r') = \varphi(r'r)$ (see Exercise 10).
(b) Suppose $0 \to A \xrightarrow{\psi} B$ is an exact sequence of R-modules. Prove that if every $\mathbb{Z}$-module homomorphism f from A to M lifts to a $\mathbb{Z}$-module homomorphism F from B to M with $f = F \circ \psi$, then every R-module homomorphism f' from A to $\mathrm{Hom}_{\mathbb{Z}}(R, M)$ lifts to an R-module homomorphism F' from B to $\mathrm{Hom}_{\mathbb{Z}}(R, M)$ with $f' = F' \circ \psi$. [Given f', show that $f(a) = f'(a)(1_R)$ defines a $\mathbb{Z}$-module homomorphism of A to M. If F is the associated lift of f to B, show that $F'(b)(r) = F(rb)$ defines an R-module homomorphism from B to $\mathrm{Hom}_{\mathbb{Z}}(R, M)$ that lifts f'.]
(c) Prove that if Q is an injective $\mathbb{Z}$-module then $\mathrm{Hom}_{\mathbb{Z}}(R, Q)$ is an injective R-module.

Proof. (a) Recall that the ring R has the structure of an abelian group, and hence may be considered a $\mathbb{Z}$-module over itself. In fact, the fact that R is abelian gives R a $(\mathbb{Z}, \mathbb{Z})$-bimodule structure. Since M is a left $\mathbb{Z}$-module, we may appeal to Exercise 10.5.10(a) to write that $\mathrm{Hom}_{\mathbb{Z}}(R, M)$ has the structure of a left R-module (we are taking $S = \mathbb{Z}$ in the notation of that exercise).

(b) Now suppose every injective Z-module homomorphisms $\psi : A \to B$ with $\mathbb{Z}$-module homomorphism $f : A \to M$ has an associated lift $F : B \to M$ with $f = F \circ \psi$. Suppose now that we have some $f' : A \to \mathrm{Hom}_{\mathbb{Z}}(R, M)$ an R-module homomorphism.

Consider the map $f : A \to M$ defined by $f(a) = f'(a)(1_R)$ for all $a \in A$. To show that f is a $\mathbb{Z}$-module homomorphism, in particular an abelian group homomorphism, we need only remark that

$$f(a + b) = f'(a + b)(1_R) = f'(a)(1_R) + f'(b)(1_R) = f(a) + f(b)$$

which follows since f' was assumed an R-module homomorphism. By assumption, there exists a lift $F : B \to M$ such that $f = F \circ \psi$.

Consider the map $F' : B \to \mathrm{Hom}_{\mathbb{Z}}(R, M)$ defined by $F'(b)(r) = F(rb)$ for all $r \in R$ and $b \in B$. We show that F' is an R-module homomorphism that lifts f'. We note

$$F'(b + d)(r) = F(r(b + d)) = F(rb + rd) = F(rb) + F(rd) = F'(b)(r) + F'(d)(r)$$

$$F'(sb)(r) = F(r(sb)) = sF(rb) = sF'(b)(r)$$

where we have used the fact that F is an R-module homomorphism twice in the above. Now to prove that F' lifts f', we show $f' = F' \circ \psi$. So for $a \in A$ and $r \in R$, we have

$$\begin{aligned}(F' \circ \psi)(a)(r) &= F'(\psi(a))(r) \\ &= F(r\psi(a)) \\ &= F(\psi(ra)) \\ &= f(ra) \\ &= f'(ra)(1_R) \\ &= f'(a)(r)\end{aligned}$$

and hence F' is indeed a lift for f', which proves the desired statement.

(c) Now suppose Q is an injective $\mathbb{Z}$-module. Then Given $0 \longrightarrow A \xrightarrow{\psi} B$ an exact sequence of R-modules, in particular $\mathbb{Z}$-modules since modules have an underlying abelian group structure, and a $\mathbb{Z}$-module homomorphism $f : A \longrightarrow Q$, we know that there exists a lift $F : B \longrightarrow Q$ such that $f = F \circ \psi$, which is a consequence of Q being injective, Proposition 34(2).

Now suppose $f : A \longrightarrow \mathrm{Hom}_{\mathbb{Z}}(R, Q)$ is an R-module homomorphism. Since, as the previous paragraph explains, we have satisfied the hypothesis of part (b), we may write that there exists a lift $F : B \longrightarrow \mathrm{Hom}_{\mathbb{Z}}(R, Q)$ such that $f = F \circ \psi$. One notes that, since the exact sequence of R-modules $0 \longrightarrow A \xrightarrow{\psi} B$ was arbitrary, and we can always find a lift, Proposition 34(2) is satisfied, and so $\mathrm{Hom}_{\mathbb{Z}}(R, Q)$ is an injective R-module, as desired. ∎

Exercise 10.5.16. This exercise proves Theorem 38 that every left R-module M is contained in an injective left R-module.
(a) Show that M is contained in an injective $\mathbb{Z}$-module Q. [M is a $\mathbb{Z}$-module—use Corollary 37.]
(b) Show that $\mathrm{Hom}_R(R, M) \subseteq \mathrm{Hom}_{\mathbb{Z}}(R, M) \subseteq \mathrm{Hom}_{\mathbb{Z}}(R, Q)$.
(c) Use the R-module isomorphism $M \cong \mathrm{Hom}_R(R, M)$ (Exercise 10) and the previous exercise to conclude that M is contained in an injective R-module.

Proof. (a) Suppose M is a left R-module. In particular, M is an additive abelian group, and so we may consider M as a $\mathbb{Z}$-module in the usual way. Corollary 37 then asserts that M is contained as a submodule in an injective $\mathbb{Z}$-module, say Q.

(b) Any R-module homomorphism $f \in \mathrm{Hom}_R(R, M)$ is, in particular, an abelian group homomorphism, and hence $f \in \mathrm{Hom}_{\mathbb{Z}}(R, M)$, to which $\mathrm{Hom}_R(R, M) \subseteq \mathrm{Hom}_{\mathbb{Z}}(R, M)$. Since M is a $\mathbb{Z}$-submodule of Q by part (a), we have the inclusion $\mathbb{Z}$-module homomorphism $\iota : M \longrightarrow Q$, which we may compose with f to obtain $\iota \circ f : R \longrightarrow Q$ a $\mathbb{Z}$-module homomorphism. The maps $\iota \circ f$ and f may be identified by viewing M as a submodule of Q, and in particular this gives $f \in \mathrm{Hom}_{\mathbb{Z}}(R, Q)$.

Thus we have proved

$$\mathrm{Hom}_R(R, M) \subseteq \mathrm{Hom}_{\mathbb{Z}}(R, M) \subseteq \mathrm{Hom}_{\mathbb{Z}}(R, Q)$$

which was the desired statement.

(c) From Exercise 10.5.10 we have that $\mathrm{Hom}_R(R, M) \cong M$, since M is a left R-module. In particular, M has an isomorphic copy inside of $\mathrm{Hom}_{\mathbb{Z}}(R, Q)$ by part (b). However, from Exercise 10.5.15, we know that $\mathrm{Hom}_{\mathbb{Z}}(R, Q)$ is an injective R-module since Q is an injective $\mathbb{Z}$-module. In particular, we have that M is contained in an injective R-module, proving the claim of Theorem 38. ∎

Exercise 10.5.17. This exercise completes the proof of Proposition 34. Suppose that Q is an R-module with the property that every short exact sequence $0 \to Q \to M_1 \to N \to 0$ splits and suppose that the sequence $0 \to L \xrightarrow{\psi} M$ is exact. Prove that every R-module homomorphism f from L to Q can be lifted to an R-module homomorphism F from M to Q with $f = F \circ \psi$. [By the previous exercise, Q is contained in an injective R-module. Use the splitting property together with Exercise 4 (noting that Exercise 4 can be proved using (2) in Proposition 34 as the definition of an injective module.]

Proof. Let Q be an R-module and suppose that every short exact sequence $0 \to Q \to M_1 \to N \to 0$ of R-modules splits. Suppose $\psi : L \to M$ is an injective R-module homomorphism. Take $f : L \to Q$ an R-module homomorphism. By Exercise 10.5.16 we know that Q is contained in an injective R-module, say I. Thus we have a short exact sequence

$$0 \to Q \xrightarrow{\text{incl}} I \xrightarrow{\pi} I/Q \to 0$$

given by the inclusion and natural projection R-module homomorphisms. By assumption, this short exact sequence splits, i.e., up to isomorphism we have $I \cong Q \oplus I/Q$. Since I is injective, Exercise 10.5.4 asserts that both Q and I/Q are injective (in the sense of (2) in Proposition 34). By Theorem 33, which essentially proves the equivalence of (1) and (2) in Proposition 34, this is equivalent to there existing a lift $F : M \to Q$ such that $F \circ \psi = f$, proving the claim.

In particular, the above work shows that (3) implies (2), which suffices to finish the proof given in the textbook regarding Proposition 34. ∎

Exercise 10.5.18. Prove that the injective hull of the $\mathbb{Z}$-module $\mathbb{Z}$ is $\mathbb{Q}$. [Let H be the injective hull of $\mathbb{Z}$ and argue that $\mathbb{Q}$ contains an isomorphic copy of H. Use the divisibility of H to show $1/n \in H$ for all nonzero integers n, and deduce that $H = \mathbb{Q}$.]

Proof. Consider $\mathbb{Z}$ as a $\mathbb{Z}$-module over itself. Let H be the injective hull of $\mathbb{Z}$; i.e., H is the minimal injective $\mathbb{Z}$-module containing $\mathbb{Z}$.

First, recall that $\mathbb{Q}$ considered as a $\mathbb{Z}$-module is injective. To see this, note that $\mathbb{Z}$ is a PID, and $r\mathbb{Q} = \mathbb{Q}$ for all $r \in \mathbb{Z} \setminus \{0\}$. In other words, $\mathbb{Q}$ is divisible. Since $\mathbb{Q}$ contains $\mathbb{Z}$, and $\mathbb{Q}$ is injective, we know that there is an injection $\iota : H \hookrightarrow \mathbb{Q}$ which restricts to the identity map on $\mathbb{Z}$. In particular, $H \cong \iota(H) \subseteq \mathbb{Q}$. Now identify H with the isomorphic copy $\iota(H)$ inside $\mathbb{Q}$.

Since H is an injective $\mathbb{Z}$-module, we know $nH = H$ for all $n \in \mathbb{Z} \setminus \{0\}$ by the same reasoning (H is divisible). In particular, we have $H = \frac{1}{n}H$. Since $1 \in H$ this means $\frac{1}{n} \in H$. However now if $\frac{a}{b} \in \mathbb{Q}$ then $\frac{1}{b} \in H$ and $a \in H$ and so $\frac{a}{b} \in H$. Thus $\mathbb{Q} \subseteq H$. Since above we showed the reverse inclusion, we necessarily have that $H = \mathbb{Q}$. ∎

Exercise 10.5.19. If F is a field, prove that the injective hull of F is F.

Proof. Let F be a field and consider F as an F-module over itself. Now let H be the injective hull of F. Recall that H is the minimal injective F-module containing F, so $F \subseteq H$. Note that F is trivially a PID, since the only ideals of F are $0 = (0)$ and $F = (1)$. If we take any $r \in F \setminus \{0\}$ then $rF = F$ by closure. Proposition 36(2) asserts that this is equivalent to F being an injective F-module. Since H was assumed the minimal injective F-module containing F, we have $F \subseteq H \subseteq F$, and therefore $H = F$. ∎

Exercise 10.5.20. Prove that the polynomial ring $R[x]$ in the indeterminate x over the commutative ring R is a flat R-module.

Proof. Let R be a commutative ring and consider $R[x]$ as an R-module. Consider the subset $A = \{1, x, x^2, \ldots\}$ of $R[x]$. An arbitrary element of $p(x) \in R[x]$ looks like

$$p(x) = \sum_{i=0}^{n} r_i x^i$$

for some $r_1, \ldots, r_n \in R$ and $n \in \mathbb{Z}^+$. In particular, we may note that

$$p(x) = r_0 + r_1 x + \cdots + r_n x^n$$

is the unique description of $p(x)$ in terms of elements of the subset A; i.e., we have that A is a basis for $R[x]$. In particular, it is clear that $R[x]$ is free on A, and so is itself a free R-module. In Corollary 42, we saw that free modules are flat, which proves the desired statement: $R[x]$ is a flat R-module. ∎

Exercise 10.5.21. Let R and S be rings with 1 and suppose M is a right R-module, and N is an (R, S)-bimodule. If M is flat over R and N is flat as an S-module prove that $M \otimes_R N$ is flat as a right S-module.

Proof. Let M be a right R-module and N an (R, S)-bimodule. Suppose M is a flat R-module and N is a flat S-module. To prove the desired statement, that $M \otimes_R N$ is flat as an S-module, we use the associativity of the tensor product and the fact that both M and N are flat as R-modules and S-modules, respectively, to iterate Proposition 40(2).

Let L and L' be arbitrary left S-modules, and suppose that $\psi : L \to L'$ is an injective S-module homomorphism. First, consider the following map of abelian groups:

$$N \otimes_S L \xrightarrow{1\otimes\psi} N \otimes_S L'$$

Since N was assumed flat as an S-module, with L and L' left S-modules, with ψ an injection of S-modules, Proposition 40(2) gives us that $1 \otimes \psi$ is an injection.

Now consider the map of abelian groups given by:

$$M \otimes_R (N \otimes_S L) \xrightarrow{1\otimes(1\otimes\psi)} M \otimes_R (N \otimes_S L')$$

Since M was assumed flat as an R-module, and both $N \otimes_S L$ and $N \otimes_S L'$ are left R-modules in the natural way (explicitly, N was assumed an (R, S)-bimodule, so we may simply define an action of R on the left by $r(n_i \otimes l_i) = rn_i \otimes l_i$ for all elements of the group $N \otimes_S L$ and $N \otimes_S L'$ both) and we also have that the map $1 \otimes \psi$ is an injection of R-modules from above, we can refer to Proposition 40(2) to once more state that $1 \otimes (1 \otimes \psi)$ is injective.

Now recall that we have an isomorphism of abelian groups

$$(M \otimes_R N) \otimes_S L \cong M \otimes_R (N \otimes_S L)$$

which follows by the associativity of the tensor product, Theorem 14 in Section 10.4. We also have the corresponding isomorphism of abelian groups

$$(M \otimes_R N) \otimes_S L' \cong M \otimes_R (N \otimes_S L')$$

from the same theorem.

In particular, by the above isomorphism of abelian groups, as well as the injection $1 \otimes (1 \otimes \psi)$, we have that the mapping

$$(M \otimes_R N) \otimes_S L \xrightarrow{(1\otimes1)\otimes\psi=1\otimes\psi} (M \otimes_R N) \otimes_S L'$$

is injective. Since the left S-modules L and L' were arbitary, as well as the injection $\psi : L \to L'$, the above suffices to prove that $M \otimes_R N$ is a flat S-module by Proposition 40(2). ∎

Exercise 10.5.22. Suppose that R is a commutative ring and that M and N are flat R-modules. Prove that $M \otimes_R N$ is a flat R-module. [Use the previous exercise.]

Proof. Let R be a commutative ring, with M and N both R-modules. Suppose M and N are flat R-modules. In particular, M and N are both left and right R-modules, and in fact both may considered (R, R)-bimodules. Since both are flat, we may refer to Exercise 10.5.23 above to write that $M \otimes_R N$ is flat as a right R-module, and since R is commutative, also as a left R-module. Hence $M \otimes_R N$ is flat. ■

Exercise 10.5.23. Prove that the (right) module $M \otimes_R S$ obtained by changing the base from the ring R to the ring S (by some homomorphism $f : R \to S$ with $f(1_R) = 1_S$, cf. Example 6 following Corollary 12 in Section 4) of the flat (right) R-module M is a flat S-module.

Proof. Let R and S be rings with 1 and let $f : R \to S$ be a ring homomorphism with $f(1_R) = 1_S$. Then S becomes an R-module via base change. Let M be a right R-module and suppose that M is flat as an R-module.

Let $0 \to A \to B \to C \to 0$ be a short exact sequence of S-modules. We apply the functor $(M \otimes_R S) \otimes_S -$ to the sequence to obtain a (not necessarily exact) sequence

$$0 \to (M \otimes_R S) \otimes_S A \to (M \otimes_R S) \otimes_S B \to (M \otimes_R S) \otimes_S C \to 0$$

which is not exact on the left since the functor is right exact. From Theorem 14 in Section 10.4, the associativity of the tensor product, whose hypothesis is satisfied since M is a right R-module and all of A, B, and C are in particular (R, S)-bimodules, we have

$$(M \otimes_R S) \otimes_S A \cong M \otimes_R (S \otimes_S A) \cong M \otimes_R A$$

where the last isomorphism follows since extending scalars from S to S does not change the S-module A, i.e., $S \otimes_S A \cong A$, cf. Example 1 following Corollary 9 in Section 10.4. The above likewise holds for B and C, and so our sequence above becomes

$$0 \to M \otimes_R A \to M \otimes_R B \to M \otimes_R C \to 0$$

But, by assumption, M is a flat R-module and hence the above sequence is actually exact, and so too must our original sequence be. In particular, since the short exact sequence $0 \to A \to B \to C \to 0$ was arbitrary, this shows that $M \otimes_R S$ is exact as an S-module, which was the desired statement. ■

Exercise 10.5.24.

Exercise 10.5.25. (*A Flatness Criterion*) Parts (a)-(c) of this exercise prove that A is a flat R-module if and only if for every finitely generated ideal I of R, the map from

$A \otimes_R I \to A \otimes_R R \cong A$ induced by the inclusion $I \subseteq R$ is again injective (or, equivalently, $A \otimes_R I \cong AI \subseteq A$).
(a) Prove that if A is flat then $A \otimes_R I \to A \otimes_R R$ is injective.
(b) If $A \otimes_R I \to A \otimes_R R$ is injective for every finitely generated ideal I, prove that $A \otimes_R I \to A \otimes_R R$ is injective for every ideal I. Show that if K is any submodule of a finitely generated free module F then $A \otimes_R K \to A \otimes_R F$ is injective. Show that the same is true for any free module F. [Cf. the proof of Corollary 42.]
(c) Under the assumption in (b), suppose L and M are R-modules and $L \xrightarrow{\psi} M$ is injective. Prove that $A \otimes_R L \xrightarrow{1\otimes\psi} A \otimes_R M$ is injective and conclude that A is flat. [Write M as a quotient of a free module F, giving a short exact sequence

$$0 \to K \to F \xrightarrow{f} M \to 0$$

Show that if $J = f^{-1}(\psi(L))$ and $\iota : J \to F$ is the natural injection, then the diagram

$$\begin{tikzcd} 0 \arrow[r] & K \arrow[r] \arrow[d, "\mathrm{id}"] & J \arrow[r] \arrow[d, "\iota"] & L \arrow[r] \arrow[d, "\psi"] & 0 \\ 0 \arrow[r] & K \arrow[r] & F \arrow[r] & M \arrow[r] & 0 \end{tikzcd}$$

is commutative with exact rows. Show that the induced diagram

$$\begin{tikzcd} A \otimes_R K \arrow[r] \arrow[d, "\mathrm{id}"] & A \otimes_R J \arrow[r] \arrow[d, "1\otimes\iota"] & A \otimes_R L \arrow[r] \arrow[d, "1\otimes\psi"] & 0 \\ A \otimes_R K \arrow[r] & A \otimes_R F \arrow[r] & A \otimes_R M \arrow[r] & 0 \end{tikzcd}$$

is commutative with exact rows. Use (b) to show that $1 \otimes \iota$ is injective, then use Exercise 1 to conclude that $1 \otimes \psi$ is injective.]
(d) (*A Flatness Criterion for Quotients*) Suppose $A = F/K$ where F is flat (e.g., if F is free) and K is an R-submodule of F. Prove that A is flat if and only if $FI \cap K = KI$ for every finitely generated ideal I of R. [Use (a) to prove $F \otimes_R I \cong FI$ and observe the image of $K \otimes_R I$ is KI; tensor the exact sequence $0 \to K \to F \to A \to 0$ with I to prove that $A \otimes_R I \cong FI/KI$, and apply the flatness criterion.]

Proof. (a) If A is a flat R-module, and I is any ideal of R, then we have an exact sequence $0 \to I \to R$ given by inclusion, and since A is flat, we get $0 \to A \otimes_R I \to A \otimes_R R$ an exact sequence, hence an injective map $A \otimes_R I \to A \otimes_R R$.

(b) Suppose that $A \otimes_R I \to A \otimes_R R$ is injective for all finitely generated ideals I of R. Let J be an arbitrary (not necessarily finitely generated) ideal of R. Assume, for contradiction, that $A \otimes_R J \to A \otimes_R R$ is not injective. Then we have some non-zero element $\sum_i a_i \otimes \beta_i$ of $A \otimes_R J$ which gets sent to 0 in $A \otimes_R R$. Since the map from $I \to R$ is just that induced by inclusion, we have that

$$\sum_i a_i \otimes \beta_i = 0$$

in the tensor product $A \otimes_R R$. But then $\sum_i a_i \otimes \beta_i$ can be written as a (finite) sum of generators for 0 in the free group $A \times R$ (recall that the tensor product is a quotient group of $A \times R$ by a finite number of equations). Thus the second coordinates of all of the $\sum_i a_i \otimes \beta_i$ are contained in a finitely generated ideal I of R; hence

$$A \otimes_R I \to A \otimes_R R$$

$$\sum_i a_i \otimes \beta_i \mapsto 0$$

but since I is finitely generated, by assumption the map above is injective, hence the element $\sum_i a_i \otimes \beta_i = 0$ in $A \otimes_R I$, and hence $A \otimes_R J$ since $I \subseteq J$. Thus the original map $A \otimes_R J \to A \otimes_R R$ is injective.

(c)

(d) ∎

Exercise 10.5.26. Suppose R is a P.I.D. This exercise proves that A is a flat R-module if and only if A is a torsion free R-module (i.e., if $a \in A$ is nonzero and $r \in R$, then $ra = 0$ implies $r = 0$).
(a) Suppose that A is flat and for fixed $r \in R$ consider the map $\psi_r : R \to R$ defined by multiplication by r: $\psi_r(x) = rx$. If r is nonzero show that ψ_r is an injection. Conclude from the flatness of A that the map from A to A defined by mapping a to ra is injective and that A is torsion free.
(b) Suppose that A is torsion free. If I is a nonzero ideal of R, then $I = rR$ for some nonzero $r \in R$. Show that the map ψ_r in (a) induces an isomorphism $R \cong I$ of R-modules and that the composite $R \xrightarrow{\psi} I \xrightarrow{\iota} R$ of ψ_r with the inclusion $\iota : I \subseteq R$ is multiplication by r. Prove that the composite $A \otimes_R R \xrightarrow{1\otimes\psi} A \otimes_R I \xrightarrow{1\otimes\iota} A \otimes_R R$ corresponds to the map $a \mapsto ra$ under the identification $A \otimes_R R = A$ and that this composite is injective since A is torsion free. Show that $1 \otimes \psi_r$ is an isomorphism and deduce that $1 \otimes \iota$ is injective. Use the previous exercise to conclude that A is flat.

Proof. (a)

(b) Take A to be torsion-free. Since R is a P.I.D., for any ideal $I \neq (0)$ of R we have that $I = (r)$ for some $r \in R \setminus \{0\}$. Notice that the map $\psi_r : R \to I$ defined by $x \mapsto rx$ is an R-module homomorphism, as can easily be verified. Moreover, if $y \in I$ is arbitrary, then $y = rx$ for some $x \in R$, and hence $\psi_r(x) = y$, so that ψ_a

is surjective. Injectivity is also clear, for if $rx = ry$ then $rx - ry = r(x - y) = 0$, and since R is an integral domain and $r \neq 0$, we require that $x - y = 0$ to which $x = y$. Thus the map ψ_r is an isomorphism of R-modules, $R \cong I$. As such, we have a sequence of R-module homomorphisms

$$R \xrightarrow{\psi_r} I \xrightarrow{\iota} R.$$

Tensoring the above sequence of R-module homomorphisms with the R-module A yields an induced sequence

$$A \otimes_R R \xrightarrow{1 \otimes \psi_r} A \otimes_R I \xrightarrow{1 \otimes \iota} A \otimes_R R$$

Recall now that the R-module isomorphism $A \cong A \otimes_R R$ always holds, for instance via $\varphi : A \otimes_R R \to A$ defined by $a \otimes r \mapsto ra$. The inverse is $\varphi^{-1} : A \to A \otimes_R R$ defined by $a \mapsto a \otimes 1$. In view of this, we have a sequence

$$A \xrightarrow{\varphi^{-1}} A \otimes_R R \xrightarrow{1 \otimes \psi_r} A \otimes_R I \xrightarrow{1 \otimes \iota} A \otimes_R R \xrightarrow{\varphi} A$$

$$a \longmapsto a \otimes 1 \longmapsto a \otimes r \longmapsto a \otimes r \longmapsto ra.$$

We claim that the composite sequence above, which we denote by Φ, is injective. To see this, if $ra = 0$ then since A is torsion-free, and $r \neq 0$ by assumption, we require that $a = 0$. Hence Φ is injective as an R-module homomorphism.

■

Exercise 10.5.27. Let M, A and B be R-modules.
(a) Suppose $f : A \to M$ and $g : B \to M$ are R-module homomorphisms. Prove that $X = \{(a, b) \mid a \in A, b \in B \text{ with } f(a) = g(b)\}$ is an R-submodule of the direct sum $A \oplus B$ (called the *pullback* or *fiber product* of f and g) and that there is a commutative diagram

$$\begin{array}{ccc} X & \xrightarrow{\pi_2} & B \\ {\scriptstyle \pi_1}\downarrow & & \downarrow{\scriptstyle g} \\ A & \xrightarrow{f} & M \end{array}$$

where π_1 and π_2 are the natural projections onto the first and second components.
(b) Suppose $f' : M \to A$ and $g' : M \to B$ are R-module homomorphisms. Prove that the quotient Y of $A \oplus B$ by $\{(f'(m), -g'(m)) \mid m \in M\}$ is an R-module (called the *pushout* or *fiber sum* of f' and g') and that there is a commutative diagram

$$\begin{array}{ccc} M & \xrightarrow{g'} & B \\ {\scriptstyle f'}\downarrow & & \downarrow{\scriptstyle \pi_2'} \\ A & \xrightarrow{\pi_1'} & Y \end{array}$$

where π_1' and π_2' are the natural maps to the quotient induced by the maps into the first and second components.

Proof. (a) Let $f : A \to M$ and $g : B \to M$ be R-module homomorphisms. We consider the subgroup of the abelian group $A \oplus B$ as

$$X = \langle (a, b) \mid a \in A, b \in B \text{ with } f(a) = g(b) \rangle$$

Note that X is a subgroup immediately since it is generated by specific elements from $A \oplus B$. To show that X is an R-submodule of $A \oplus B$, note that if $(a, b) \in X$ and $r \in R$ then

$$f(ra) = rf(a) = rg(b) = g(rb)$$

since both f and g are R-module homomorphisms. Thus $(ra, rb) \in X$. What remains is to show that the commutative diagram in the problem description commutes. Let $(a, b) \in X$. Then

$$f(\pi_1((a, b))) = f(a) = g(b) = g(\pi_2((a, b)))$$

and so indeed $f \circ \pi_1 = g \circ \pi_2$; i.e., the diagram commutes.

(b) Let $f' : M \to A$ and $g' : M \to B$ be R-module homomorphisms. Consider the subgroup of $A \oplus B$ given by

$$H = \langle (f'(m), -g'(m)) \mid m \in M \rangle$$

Note that for arbitrary $r \in R$ and $(a, b) \in H$, we have that $a = f'(m)$ and $b = -g'(m)$ for some $m \in M$, and that

$$r(a, b) = (ra, rb) = (rf'(m), -rg'(m)) = (f'(rm), -g'(rm)) \in H$$

which follows since $rm \in M$ by closure and the assumption that f' and g' were R-module homomorphisms. In particular, H is an R-submodule of $A \oplus B$. Now define a quotient R-module Y given by

$$Y = (A \oplus B)/H$$

Let $m \in M$ be arbitrary. Then, keeping in mind that $(0, 0)H = (f'(m), -g'(m))H$ in the quotient Y (essentially adding or subtracting this quantity stays inside H, and so is the identity in the quotient group Y), we may observe:

$$\begin{aligned}
\pi_1'(f'(m)) &= (f'(m), 0)H \\
&= (f'(m), 0)H - (f'(m), -g'(m))H \\
&= (f'(m) - f'(m), 0 - (-g'(m))H \\
&= (0, g'(m))H \\
&= \pi_2'(g'(m))
\end{aligned}$$

and so in particular, $\pi_1' \circ f' = \pi_2' \circ g'$, so that the diagram commutes. ∎

Exercise 10.5.28. (a) (*Schanuel's Lemma*) If $0 \to K \to P \xrightarrow{\varphi} M \to 0$ and $0 \to K' \to P' \xrightarrow{\varphi'} M \to 0$ are exact sequences of R-modules where P and P' are projective, prove $P \oplus K' \cong P' \oplus K$ as R-modules. [Show that there is an exact sequence $0 \to \ker \pi \to X \xrightarrow{\pi} P \to 0$ with $\ker \pi \cong K'$, where X is the fiber product of φ and φ' as in the previous exercise. Deduce that $X \cong P \oplus K'$. Show similarly that $X \cong P' \oplus K$.]
(b) If $0 \to M \to Q \xrightarrow{\psi} L \to 0$ and $0 \to M \to Q' \xrightarrow{\psi'} L' \to 0$ are exact sequences of R-modules where Q and Q' are injective, prove $Q \oplus L' \cong Q' \oplus L$ as R-modules.

Proof. (a) Suppose $0 \to K \to P \xrightarrow{\varphi} M \to 0$ and $0 \to K' \to P' \xrightarrow{\varphi'} M \to 0$ are exact sequences of R-modules, and that P and P' are projective R-modules. Immediately, we have R-module homomorphisms $\varphi : P \to M$ and $\varphi' : P' \to M$, and so we have the pullback X an R-submodule of $P \oplus P'$, with a commutative diagram

$$\begin{tikzcd} X \arrow[r, "\pi"] \arrow[d, "\pi'"'] & P \arrow[d, "\varphi"'] \\ P' \arrow[r, "\varphi'"] & M \end{tikzcd}$$

where π and π' are natural projection maps. So that $\varphi \circ \pi = \varphi' \circ \pi'$. Now, note that $\ker \pi$ and $\ker \pi'$ both have natural embeddings ι and ι' into X, i.e., so we have

$$\begin{tikzcd} 0 \arrow[r] \arrow[d] & \ker \pi \arrow[d, "\iota'"] & & \\ \ker \pi' \arrow[r, "\iota'"] & X \arrow[r, "\pi"] \arrow[d, "\pi'"] & P \arrow[r] \arrow[d, "\varphi"] & 0 \\ & P' \arrow[r, "\varphi'"] \arrow[d] & M & \\ & 0 & & \end{tikzcd}$$

And since π and π' are surjective, we have exact sequences from the diagram above given by $0 \to \ker \pi \xrightarrow{\iota} X \xrightarrow{\pi} P \to 0$ and $0 \to \ker \pi' \xrightarrow{\iota'} X \xrightarrow{\pi'} P' \to 0$.

Note that $\ker \pi = \{x \in X \mid \pi(x) = 0\}$, and since

$$X = \{(p, p') \mid p \in P, p' \in P' \text{ with } \varphi(p) = \varphi'(p')\}$$

if $x \in \ker \pi$ then $\pi(x) = 0$ and so $\varphi(x) = 0$ and hence $\varphi'(x) = 0$ by construction of X, so that $x \in \ker \varphi'$. The converse is clear, and the case for $\ker \pi'$ is similar.

In particular, we have $\ker \pi = \ker \varphi'$. Similarly, we can find that $\ker \pi' = \ker \varphi$. But by the assumption that $0 \to K \to P \xrightarrow{\varphi} M \to 0$ and $0 \to K' \to P' \xrightarrow{\varphi'} M \to 0$ are short exact sequences, we know that there is an isomorphic copy of K embedded in P and similarly for K' in P'. In particular, both of these isomorphic copies are equal to the kernel of φ and φ', respectively, by exactness. Thus $K \cong \ker\varphi = \ker\pi'$ and $K' \cong \ker\varphi' = \ker\pi$.

Since P and P' are projective, we know that these short exact sequences are split, refer to Proposition 30(3), so that $X = \ker\pi \oplus C$ and $X = \ker\pi' \oplus C'$, where $\pi(C) \cong P$ and $\pi(C') \cong P'$. But above we saw that $\ker\pi' \cong K$ and $\ker\pi \cong K'$. Thus we have

$$X \cong \ker\pi' \oplus C' \cong K \oplus P'$$

$$X \cong \ker\pi \oplus C \cong K' \oplus P$$

and hence $P \oplus K' \cong P' \oplus K'$ as R-modules, which was the desired statement.

(b) Suppose $0 \to M \xrightarrow{f} Q \xrightarrow{\psi} L \to 0$ and $0 \to M \xrightarrow{f'} Q' \xrightarrow{\psi} L' \to 0$ are exact sequences of R-modules, and further that Q, Q' are injective. Immediately we have two R-module homomorphisms, each of which are injective, given by $f : M \to Q$ and $f' : M \to Q'$. Let Y denote the pushout of f and f'. We have maps $\pi : Q \to Y$ and $\pi' : Q' \to Y$ given by $q \mapsto \overline{(q,0)}$ and $q' \mapsto \overline{(0,q')}$, respectively. Note that

$$\ker\pi = \{q \in Q \mid (q,0) = (f(m), -f'(m) \text{ for some } m \in M\}$$

so if $q \in \ker\pi$ then say $m \in M$ gives $(q,0) = (f(m), -f'(m))$. Then $-f'(m) = 0$ implies $f'(m) = 0$ and hence $m \in \ker f'$. But since $0 \to M \xrightarrow{f'} Q' \xrightarrow{\psi} L' \to 0$ is exact, we know that $\ker f = \{0\}$ so that $m = 0$. However now $f(0) = 0$ is required, so that $(q,0) = (0,0)$ and $q = 0$. Thus $\ker\pi = \{0\}$, and hence π is injective. A completely analagous process holds for π', and so we have as well that π' is injective.

Now consider the sequences $0 \to Q \xrightarrow{\pi} Y \xrightarrow{F} L' \to 0$ and $0 \to Q' \xrightarrow{\pi'} Y \xrightarrow{F'} L \to 0$, where $F : Y \to L'$ takes $\overline{(q,q')} \mapsto \psi'(q')$ and $F' : Y \to L$ takes $\overline{(q,q')} \mapsto \psi(q)$. Both F and F' are surjective R-module homomorphisms since both ψ and ψ' are assumed to be surjective. Furthermore, it is obvious that $\operatorname{im}\pi = \ker F$ and $\operatorname{im}\pi' = \ker F'$. To see this, note $\overline{(q,q')} \in \operatorname{im}\pi$ implies there exists some $p \in Q$ for which $\pi(p) = \overline{(q,q')}$, so that $\overline{(p,0)} = \overline{(q,q')}$ implies $\psi'(0) = \psi'(q')$ and thus $\psi'(q') = 0$, to which $\overline{(q,q')} \in \ker F$. Conversely, if $\overline{(q,q')} \in \ker F$ then $\psi'(q') = 0$ and so $q' \in \ker\psi'$, which implies $q' \in \operatorname{im} f'$ by exactness of our initial sequence, and so $q' = f'(m)$ for some $m \in M$. But now

$$\overline{(q,q')} = \overline{(q,q')} + \overline{(0,0)} = \overline{(q,f'(m))} + \overline{(f(m),-f'(m))} = \overline{(q+f(m),0)}$$

and so taking $q + f(m) \in Q$ gives us $\pi(q + f(m)) = \overline{(q,q')}$. We have shown both directions of the inclusion; hence $\operatorname{im}\pi = \ker F$. In a similar fashion, one can show that $\operatorname{im}\pi' = \ker F'$.

In particular, we have shown that $0 \to Q \xrightarrow{\pi} Y \to L' \to 0$ and $0 \to Q' \xrightarrow{\pi'} Y \to L' \to 0$ are short exact sequences. Since Q and Q' are injective, Proposition 34(2) gives us that both sequences split. Thus, up to isomorphism, we have $Y \cong Q \oplus L'$ and $Y \cong Q' \oplus L$. Therefore, we may conclude $Q_1 \oplus L' \cong Q_2 \oplus L$, as desired. ■

❊ Vector Spaces

11.1 Definitions and Basic Theory

11.2 The Matrix of a Linear Transformation

11.3 Dual Vector Spaces

11.4 Determinants

11.5 Tensor Algebras, Symmetric and Exterior Algebras

※ Modules over Principal Ideal Domains

12.1 The Basic Theory

Exercise 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 $M/\text{Tor}(M)$.

Proof. (a) Recall that the rank of a module M over an integral domain R is the maximum number of R-linearly independent elements of M. If $x \neq 0$ is a torsion element of M, so that there exists some non-zero $r \in R$ for which $rx = 0$, so then x and 0 are R-linearly dependent; in particular, the maximum number of R-linearly independent torsion elements of M is 0; hence the rank of $\text{Tor}(M)$ is 0, and likewise any torsion R-module has rank 0 for the same reason.

(b) In part (a) above we showed that $\text{Tor}(M)$ has rank 0. If the rank of M and the rank of $M/\text{Tor}(M)$ are both finite, say of n and m, respectively, then Exercise 12.1.4 asserts that

$$n = \text{rank}(M) = \text{rank}(\text{Tor}(M)) + \text{rank}(M/\text{Tor}(M)) = 0 + m = m$$

hence $n = m$ holds.

So we reduce to analyzing the case where at least one of the ranks of M or $M/\text{Tor}(M)$ is infinite. To this end: let $\overline{x}_1, \ldots, \overline{x}_n$ be R-linearly independent elements of $M/\text{Tor}(M)$. Then, if there existed $r_1, \ldots, r_n \in R$, not all zero, such that

$$\sum_{i=1}^{n+1} r_i x_i = 0,$$

i.e., if the $x_1, \ldots, x_n$ were R-linearly dependent in M, then we would require that:

$$\sum_{i=1}^{n+1} \overline{r_i x_i} = \overline{0} \implies \sum_{i=1}^{n+1} r_i \overline{x}_i = \overline{0}$$

which is a contradiction, for the $\overline{x}_i$ were assumed R-linearly independent; hence the $x_1, \ldots, x_n$ must be R-linearly independent in M; thus the rank of M is bounded by the rank of $M/\text{Tor}(M)$; hence if M has infinite rank then $M/\text{Tor}(M)$ must also have infinite rank.

Now assume that M has infinite rank; so there exists elements $x_1, x_2, \ldots$ of M that are R-linearly independent. We claim that $\overline{x}_1, \overline{x}_2, \ldots$ are R-linearly independent in $M/\text{Tor}(M)$. If this is not the case, then there exists $r_1, r_2, \ldots \in R$, not all zero, for which

$$\sum_{n=1}^{\infty} r_i\overline{x}_i = \overline{0} \iff \sum_{i=1}^{\infty} \overline{r_i x_i} = \overline{0},$$

hence $\sum_{i=1}^{\infty} r_i x_i \in \operatorname{Tor}(M)$ holds, to which there exists some non-zero $s \in R$ for which

$$s\left(\sum_{i=1}^{\infty} r_i x_i\right) = \sum_{i=1}^{\infty}(sr_i)x_i = 0$$

But $sr_i \neq 0$ for at least one i, since R is an integral domain and $s \neq 0$, and not all of the r_i are zero by assumption. Thus we have found an R-linear dependence relation amongst the $x_1, x_2, \ldots$, which is a contradiction; hence the $\overline{x}_1, \overline{x}_2, \ldots$ are R-linearly independent in $M/\operatorname{Tor}(M)$; hence $M/\operatorname{Tor}(M)$ has infinite rank as well. ■

Exercise 12.1.2. Let M be a module over the integral domain R.
(a) Suppose that M has rank n and that $x_1, x_2, \ldots, x_n$ 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 non-zero 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 basus for N for some non-zero elements $r_1, \ldots, r_{n+1}$ of R. Use the argument as in the proof of Proposition 3 to see that the r_iy_i, and hence also the y_i, are linearly dependent.]

Proof. (a) Let e_i denote the element of R^n with 1 in the ith component and zeroes elsewhere; it is clear that the set of all e_i generate R^n as an R-module. With $N = Rx_1 + \cdots + Rx_n$, we can construct a mapping $\psi : R^n \to N$ defined by $\psi(e_i) = x_i$ for all $1 \leq i \leq n$. The fact that ψ is an R-module homomorphism is immediate; we also have surjectivity, since for any $y \in N$ we have $y = \sum_{i=1}^{n} r_i x_i$ for some $r_i \in R$, $1 \leq i \leq n$, and hence $\psi(r_1, \ldots, r_n) = y$. Injectivity is also clear, for if $(r_1, \ldots, r_n)$ is an element of R^n which is sent to 0 by ψ, then we require $\sum_{i=1}^{n} r_i x_i = 0$ in N, and by the linear independence of the x_i, this forces $r_i = 0$ for all i; hence $N \cong R^n$ as R-modules.

Now we show that M/N is torsion. Since M has rank n, the maximum number of linearly independent elements of M is n; hence the set $\{y, x_1, \ldots, x_n\}$ must be R-linearly dependent, so that there exists $r_1, \ldots, r_{n+1} \in R$, not all zero, such that

$$r_1x_1 + \cdots + r_nx_n + r_{n+1}y = 0$$

and hence with

$$r_{n+1}y = -(r_1x_1 + \cdots + r_nx_n)$$

This of course means $r_{n+1}y \in N$, hence that $\overline{r_{n+1}y} = \overline{0}$ in M/N, to which $\overline{y} \in \mathrm{Tor}(M/N)$. Therefore, M/N is a torsion R-module.

(b) Conversely, suppose that M contains a submodule $N \cong R^n$ such that M/N is a torsion R-module. Let $y_1, \ldots, y_{n+1}$ be any $n+1$ elements of R. Since M/N is torsion, for each equivalence class $\overline{y_i}$ in M/N there exists some $r_i \in R$ such that $\overline{r_i y_i} = \overline{0}$, which means $r_i y_i \in N$. Thus we have a set

$$\{r_1y_1, \ldots, r_{n+1}y_{n+1}\}$$

of elements of N, and since N is free of rank n, Proposition 3 asserts that there exists $s_1, \ldots, s_{n+1} \in R$, not all zero, such that

$$s_1(r_1y_1) + \cdots + s_{n+1}(r_{n+1}y_{n+1}) = 0$$

Letting $t_i = s_1r_1$, we see that

$$t_1y_1 + \cdots + t_{n+1}y_{n+1} = 0$$

and hence the set $\{y_1, \ldots, y_{n+1}\}$ is R-linearly dependent in M, so too must be any set of $n+1$ elements of M, since we chose the y_i arbitrarily. Thus the maximam number of R-linearly independent elements of M is n, since, for instance, the submodule N of M has this property. By definition, then, M is of rank n. ■

Exercise 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 $m+n$.

Proof. From Exercise 12.1.2 above, we know that A has a submodule R^m such that A/R^m is a torsion R-module. Likewise, B has a submodule R^n which is free of rank n such that B/R^n is torsion as an R-module. It is clear to see that $R^m \oplus R^n$ is then a submodule of $A \oplus B$; we also have that $R^m \oplus R^n \cong R^{m+n}$ by Exercise 10.3.23. Now, from Exercise 10.2.11, we know

$$(A \oplus B)/R^{m+n} \cong (A \oplus B)/(R^m \oplus R^n) \cong (A/R^m) \oplus (B/R^n)$$

and since the direct sum of torsion R-modules are torsion once more, we have that $A \oplus B$ is an R-module with a submodule which is free of rank $m+n$ such that the quotient of $A \oplus B$ with this submodule is torsion. Thus by Proposition 3, $A \oplus B$ has rank $m+n$. ■

Exercise 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 $x_1, x_2, \ldots, x_s$ be elements of M whose images in M/N are a maximal set of linearly independent elements and let $x_{s+1}, x_{s+2}, \ldots, x_{s+r}$ be a maximal set of independent elements in N. Prove that $x_1, x_2, \ldots, x_{s+r}$ are linearly independent in M and that for any element $y \in M$ there is a non-zero element $r \in R$ such that ry is a linear combination of these elements. Then use Exercise 2.]

Proof. Let $x_1, \ldots, x_s$ be lifts of a maximal R-linearly independent set of elements of M/N. Let $x_{s+1}, \ldots, x_{s+r}$ be a maximal set of R-linearly independent elements in N. We claim now that $x_1, \ldots, x_{s+r}$ form a set of R-linearly independent elements in M. Assume this is not true; that is, there exists $t_1, \ldots, t_{s+r} \in R$, not all zero, such that

$$\sum_{i=1}^{s+r} t_i x_i = 0$$

On passing to the quotient module M/N, each of the x_i with $s+1 \leq i \leq s+r$ become 0 since these elements lie in N by assumption, hence

$$\sum_{i=1}^{s} \overline{t_i x_i} = \overline{0}$$

holds. But we know that the x_i for $1 \leq i \leq s$ are lifts of a maximal R-linearly independent subset of M/N, that is, we have $\overline{x_i}$ for $1 \leq i \leq s$ are R-linearly independent in M/N; hence $t_i = 0$ for all $1 \leq i \leq s$. Thus, our original equation becomes

$$\sum_{i=1}^{s+r} t_i x_i = \sum_{i=s+1}^{s+r} t_i x_i = 0$$

in M. But note that since each of the x_i for $s+1 \leq i \leq s+r$ lie in N, the whole equation above lies in N since N is closed under the ring action of R, since it is a submodule of M. In particular, the assumption that x_i for $s+1 \leq i \leq s+r$ form a maximal R-linearly independent set in N implies $t_i = 0$ for all $s+1 \leq i \leq s+r$. In particular, all of the $t_i = 0$ for $1 \leq i \leq s+r$, which is a contradiction, for we assumed at least one of the t_i were non-zero. Hence the original set $x_1, \ldots, x_{s+r}$ of elements of M is indeed R-linearly independent.

We now show that, for any non-zero element $y \in M$, there exists $t \in R \setminus \{0\}$ such that ry may be written as a linear combination of the $x_1, \ldots, x_{s+r}$. Note that for any such $y \in M \setminus \{0\}$ we have $\overline{y} \in M/N$, hence the set $\overline{y}, \overline{x_1}, \ldots, \overline{x_s}$ is R-linearly dependent (since we assumed the set $x_1, \ldots, x_s$ was a lift of a maximal R-linearly independent set in M/N), and hence there exists $t_i \in R$, not all zero, such that

$$\overline{t_1 x_1} + \cdots + \overline{t_s x_s} + \overline{t_{s+1} y} = \overline{0}$$

Letting $\overline{\alpha} = \overline{t_1 x_1} + \cdots + \overline{t_s x_s} + \overline{t_{s+1} y}$, we have that $\alpha \in N$ holds. Now we know that $\alpha, x_{s+1}, \ldots, x_{s+r}$ is an R-linearly dependent set of elements of N (since, by assumption, $x_{s+1}, \dots, x_{s+r}$ was a maximal R-linearly independent set in N); hence there exists $u_i \in R$, not all zero, such that

$$u_{s+1}x_{s+1} + \cdots + u_{s+r}x_{s+r} + u_{s+r+1}\alpha = 0$$

in N, and hence also in M. Upon rewriting what we have so far,

$$0 = \left(\sum_{i=s+1}^{s+r} u_i x_i\right) + u_{s+r+1}\alpha = \left(\sum_{i=s+1}^{s+r} u_i x_i\right) + u_{s+r+1}\left(t_{s+1}y + \sum_{i=1}^{s} t_i x_i\right)$$

Rearranging the above equation, we can isolate the term involving y, getting

$$u_{s+r+1}t_{s+1}y = -\left(\sum_{i=s+1}^{s+r} u_i x_i\right) - u_{s+r+1}\left(\sum_{i=1}^{s} t_i x_i\right)$$

In particular, $\beta := u_{s+r+1}t_{s+1}$ is a non-zero element of R such that βy may be written as a linear combination of $x_1, \dots, x_{s+r}$.

Now consider the submodule $L = Rx_1 + \cdots + Rx_{s+r}$ of M. Clearly $L \cong R^{s+r}$ as R-modules, so that L is a free R-module of rank $s + r$. Moreover, the quotient M/L is a torsion R-module, since for any non-zero $y \in M$, as above, there exists some non-zero $\beta \in R$ for which $\beta y \in L$. By Exercise 12.1.2, this occurs if and only if M has rank $s + r$. Therefore, we have $n = s + r$, as desired. ∎

Exercise 12.1.5.

Exercise 12.1.6.

Exercise 12.1.7.

Exercise 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 $\mathrm{Ann}_R(B) \subseteq (p)$.

Proof. Suppose $pb = 0$ for some non-zero $b \in B$. Since $\mathrm{Ann}_R(B)$ is an ideal of R, and R is a P.I.D., we know $\mathrm{Ann}_R(B) = (r)$ for some $r \in R$. Consider the ideal $(d) = (r) + (p)$; we know that d is the greatest common divisor of r and p. Since p is a prime element of R, either $d = 1$ or $d = p$. In the former case, there exists $s, t \in R$ such that

$$sr + tp = 1$$

As such, we have

$$b = 1b = (sr + tp)b = (sr)b + (tp)b = s(rb) + t(pb) = s0 + t0 = 0 + 0 = 0$$

and hence $b = 0$, a contradiction, for we took $b \in B \setminus \{0\}$. Thus the latter case holds; that is, $d = p$, so that p divides (r), and hence $\mathrm{Ann}_R(B) = (r) \subseteq (p)$. ∎

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

Proof. TBD. ■

Exercise 12.1.10.

Exercise 12.1.11.

Exercise 12.1.12.

Exercise 12.1.13.

Exercise 12.1.14.

Exercise 12.1.15.

Exercise 12.1.16.

Exercise 12.1.17.

Exercise 12.1.18.

Exercise 12.1.19.

Exercise 12.1.20.

Exercise 12.1.21. Prove that a finitely generated module over a P.I.D. is projective if and only if it is free.

Proof. Let R be a principal ideal domain and take M to be a finitely generated R-module. If M is free, then clearly M is projective, for instance by Corollary 31 in Section 10.5. We now prove the converse. Suppose M is projective as an R-module.

We may let $M \cong R^r \oplus R/(a_1) \oplus \cdots \oplus R/(a_m)$ for some integer $r \geq 0$ and $a_i \in R \backslash \{0\}$. From Exercise 10.5.3 we know that the fact that M is projective means R^r and each of $R/(a_i)$ are projective.

We show that $R/(a_i)$ is not projective for all $i \in \{1, \ldots, n\}$. We have the obvious short exact sequence of R-modules

$$0 \longrightarrow R \xrightarrow{a_i} R \xrightarrow{\pi} R/(a_i) \longrightarrow 0$$

where the first map is multiplication by a_i and the second is the natural projection homomorphism.

Observe that if $\varphi : R/(a_i) \longrightarrow R$ is an R-module homomorphism, then Exercise 10.2.8 states that $\varphi(\mathrm{Tor}(R/(a_i))) \subseteq \mathrm{Tor}(R)$. Since R is an integral domain (as are all principal ideal domains), we know $\mathrm{Tor}(R) = 0$. Since $\mathrm{Tor}(R/(a_i)) = R/(a_i)$, which can be seen since $a_i x = 0$ for all $x \in R/(a_i)$, we thus have

$$\varphi(\mathrm{Tor}(R/(a_i))) = \varphi(R/(a_i)) \subseteq 0 = \mathrm{Tor}(R)$$

and hence $\varphi(R/(a_i)) = 0$ is required, meaning that φ is the zero R-module homomorphism. This proves that $\mathrm{Hom}_R(R/(a_i), R) = 0$.

Using the above, we apply the functor $\mathrm{Hom}_R(R/(a_i), -)$ to the above sequence to obtain

$$0 \longrightarrow 0 \xrightarrow{a_i'} 0 \xrightarrow{\pi'} \mathrm{Hom}_R(R/(a_i), R/(a_i)) \longrightarrow 0$$

Now, since $\mathrm{Hom}_R(R/(a_i), R/(a_i))$ contains both the zero homomorphism and the identity homomorphism, this R-module is non-trivial, and hence the above sequence is not a short exact sequence. This contradicts $R/(a_i)$ being projective by Proposition 30(1) in Section 10.5.

Therefore, we require $R/(a_i) = 0$ for all $i \in \{1, \ldots, n\}$. In particular, this means that $M \cong R^r$ holds, so that M is a free R-module. ■

Exercise 12.1.22. Let R be a P.I.D. that is not a field. Prove that no finitely generated R-module is injective. [Use Exercise 4, Section 10.5 to consider torsion and free modules separately.]

Proof. Let M be a finitely generated R-module. Assume, for contradiction, that M is injective. We may write $M \cong R^r \oplus R/(a_1) \oplus \cdots \oplus R/(a_m)$ for some integer $r \geq 0$ and $a_i \in R \setminus \{0\}$ which are not units. From Exercise 10.5.4 we know that M is injective if and only if R^r and each of $R/(a_i)$ are injective R-modules.

From Proposition 36(2), Baer's criterion, which applies since R is a principal ideal domain, we know that $R/(a_i)$ is injective if and only if $sR/(a_i) = R/(a_i)$ for all $s \in R \setminus \{0\}$. Note, however, that $a_i \in R \setminus \{0\}$ and clearly $a_i R/(a_i) = 0$. This forces $R/(a_i) = 0$, and hence forces $M \cong R^r$.

Since, by assumption, R is not a field, we know there exists some $y \in R \setminus \{0\}$ which is not a unit, i.e., is not invertible, so that there exists no element $x \in R$ for which $xy = 1$ or $yx = 1$.

Baer's criterion again asserts that since M is injective, we have $sM = M$ for all $s \in R \setminus \{0\}$. In particular, since $y \neq 0$, $M/yM = 0$ is required. We may note that from Exercise 10.2.12, we have

$$R^r/yR^r \cong R/yR \times \cdots \times R/yR$$

and since $M/yM \cong R^r/yR^r$ this necessitates $R/yR = 0$. In particular, $yR = R$. Note that $1 \in R$, and so there exists some $x \in R$ such that $yx = 1$, which is a contradiction, for we took y to not be a unit. Therefore we may conclude that M is not injective. ■

12.2 The Rational Canonical Form

12.3 The Jordan Canonical Form

❊ Field Theory

13.1 Basic Theory of Field Extensions

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

Proof. Note that $\deg(p(x)) = 3$. Over the field $\mathbb{Q}$, this implies that $p(x)$ is irreducible if and only if it has no rational roots. To show that $p(x)$ has no rational roots, we employ Proposition 11 of Chapter 9.4, the rational root test. Assume r/s is a root of $p(x)$. Then $r \mid 6$ and $s \mid 1$. Since $s \mid 1$ we know that $s = \pm 1$. In this manner, it must be the case that $r/s = \pm r \in \mathbb{Z}$. Thus our root must be an integer. By Eisenstein's criterion for $\mathbb{Z}[x]$, since $p = 3$ divides 6 and 9, but $p^2 = 9$ does not divide 6, we may conclude that $p(x)$ is irreducible in $\mathbb{Q}[x]$.

Now let θ be a root of $p(x)$. Then $p(\theta) = \theta^3 + 9\theta + 6 = 0$. From this, we have

$$\theta^3 + 9\theta + 6 = 0 \iff \theta(\theta^2 + 9) = -6 \iff \theta = -6(\theta^2 + 9)^{-1}$$

Adding the quantity 1 to both sides of the above equation yields

$$\theta + 1 = -6(\theta^2 + 9)^{-1} + 1 \iff (\theta + 1)^{-1} = (-6(\theta^2 + 9) + 1)^{-1}$$

which is the desired quantity. ■

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

Proof. The polynomial $x^3 - 2x - 2$ is irreducible over $\mathbb{Q}$ by Eisenstein's criterion at $p = 2$. Let θ be a root. Then $\theta^3 - 2\theta - 2 = 0$, and so $\theta^3 = 2\theta + 2$. We can find that:

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

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

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

Now we aim to compute $\frac{1+\theta}{1+\theta+\theta^2}$. To do this, we compute $(1+\theta+\theta^2)^{-1}$. We attempt to solve the equation:

$$(1 + \theta + \theta^2)(x + y\theta + z\theta^2) = 1$$

where $x, y, z \in \mathbb{Q}$. Multiplying out the above and simplifying, we obtain the equation:

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

and so we require $x + 2y + 2z = 1$, $x + 3y + 4z = 0$, and $x + y + 3z = 0$ as well. Three equations with three unknowns, we eventually find that

$$x = -\frac{2}{3},\ y = \frac{1}{3},\ z = -\frac{2}{3}$$

and so $(1 + \theta + \theta^2)^{-1} = -\frac{2}{3} + \frac{1}{3}\theta - \frac{2}{3}\theta^2$. Now we can find:

$$\frac{1+\theta}{1+\theta+\theta^2} = (-\frac{2}{3} + \frac{1}{3}\theta - \frac{2}{3}\theta^2)(1+\theta) = \frac{1}{3} - \frac{2}{3}\theta - \frac{1}{3}\theta^2$$

which was the desired calculation. ■

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

Proof. Let $p(x) = x^3 + x + 1$. Note $p(0) = 1$ and $p(1) = 1 + 1 + 1 = 1$. Thus $p(x)$ has no roots in $\mathbb{F}_2$, and since $\deg(p(x)) = 3$, this suffices to show that $p(x)$ is irreducible over $\mathbb{F}_2$. Now take θ a root of $p(x)$. We know

$$\mathbb{F}_2[x]/(p(x)) \cong \mathbb{F}_2(\theta) = \{a_0 + a_1\theta + a_2\theta^2 \mid a_0, a_1, a_2 \in \mathbb{F}_2\}$$

Now since $\theta^3 + \theta + 1 = 0$, we can subtract 1 from both sides and rewrite as

$$\theta(\theta^2 + 1) = -1 \iff \theta^2 + 1 = -\theta^{-1} \iff \theta^2 = -\theta^{-1} - 1$$

Therefore $\theta^2 = \theta^{-1} + 1$ since the underlying field is $\mathbb{F}_2$. By virtue of the construction of $\mathbb{F}_2(\theta)$ above, any higher power of θ may be written as some linear combination of 1, θ, and $\theta^{-1} + 1$. ■

Exercise 13.1.4 Prove directly that the map $a + b\sqrt{2} \mapsto a - b\sqrt{2}$ is an isomorphism of $\mathbb{Q}(\sqrt{2})$ with itself.

Proof. From prior derivations we know that $\mathbb{Q}[x]/(x^2 - 2) \cong \mathbb{Q}(\sqrt{2})$. In particular, $\mathbb{Q}(\sqrt{2})$ is a field. Consider the map $\tau : \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{2})$ defined by $\tau(a + b\sqrt{2}) = a - b\sqrt{2}$. We may observe that

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

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

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

so that the additive sttructure is preserved. Furthermore, we have

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

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

$$\begin{aligned}
&= ac + 2bd - (ad + bc)\sqrt{2} \\
&= ac + 2bd - ad\sqrt{2} - bc\sqrt{2} \\
&= a(c - d\sqrt{2}) + b\sqrt{2}(d\sqrt{2} - c) \\
&= a(c - d\sqrt{2}) - b\sqrt{2}(c - d\sqrt{2}) \\
&= (a - b\sqrt{2})(c - d\sqrt{2}) = \tau(a + b\sqrt{2})\tau(c + d\sqrt{2})
\end{aligned}$$

and so the multiplicative structure is preserved by τ also. Now, note that $\tau(1) = 1$. In particular, τ is not the zero map and so this homomorphism of fields is automatically injective. For surjectivity, if $a + b\sqrt{2} \in \mathbb{Q}(\sqrt{2})$, then we can easily find $\tau(a - b\sqrt{2}) = a + b\sqrt{2}$. Therefore τ is a bijective homomorphism of fields, and so is an isomorphism of $\mathbb{Q}(\sqrt{2})$ with itself ∎

Exercise 13.1.5 Suppose α is a rational root of a monic polynomil in $\mathbb{Z}[x]$. Prove that α is an integer.

Proof. Suppose α is a rational root of some monic polynomial in $\mathbb{Z}[z]$. We may write $\alpha = r/s$ for some integers r, s with $s \neq 0$. By the rational root test, we know $r \mid a_0$ and $s \mid 1$, which forces $s = \pm 1$. Now it is clear that $r/s = r/\pm 1 = \pm r$, and since $r \in \mathbb{Z}$ this shows that $\alpha \in \mathbb{Z}$ as well. ∎

Exercise 13.1.6 Show that if α is a root of $a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ then $a_n\alpha$ is a root of the monic polynomial $x^n + a_{n-1}x^{n-1} + a_n a_{n-2}x^{n-2} + \cdots + a_n^{n-2}a_1 x + a_n^{n-1}a_0$.

Proof. Let α be such a root of the polynomial in the problem description. Then we know

$$a_n\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0$$

Using this fact, we can evaluate the desired monic polynomial at the value $a_n\alpha$ as follows:

$$\begin{aligned}
&(a_n\alpha)^n + a_{n-1}(a_n\alpha)^{n-1} + a_n a_{n-2}(a_n\alpha)^{n-2} + \cdots + a_n^{n-2}a_1(a_n\alpha) + a_n^{n-1}a_0 \\
&= a_n^n\alpha^n + a_{n-1}a_n^{n-1}\alpha^{n-1} + a_n a_{n-2}a_n^{n-2}\alpha^{n-2} + \cdots + a_n^{n-2}a_1 a_n\alpha + a_n^{n-1}a_0 \\
&= a_n^{n-1}(a_n\alpha^n + a_{n-1}\alpha^{n-1} + a_{n-2}\alpha^{n-2} + \cdots + a_1\alpha + a_0) \\
&= a_n^{n-1}(0) = 0
\end{aligned}$$

and so we have found that $a_n\alpha$ is a root of the polynomial given in the problem description, as desired. ∎

Exercise 13.1.7 Prove that $x^3 - nx + 2$ is irreducible for $n \neq -1, 3, 5$.

Proof. There is no ambient polynomial ring specified in the problem, so I guess we will just assume this is in $\mathbb{Z}[x]$. So suppose $f(x) = x^3 - nx + 2$ is reducible over $\mathbb{Z}$. Since $\deg(f(x)) = 3$, this implies $f(x)$ has at least one linear factor, and so has at least one root in $\mathbb{Z}$. Take α to be this root. Then we may rewrite

$$x^3 - nx + 2 = (x - \alpha)(ax^2 + bx + c)$$

for some $a, b, c \in \mathbb{Z}$. Multiplying out the right hand side of the above equation, we find

$$\begin{aligned} x^3 - nx + 2 &= ax^3 + bx^2 + cx - \alpha ax^2 - \alpha bx - \alpha c \\ &= ax^3 + (b - \alpha a)x^2 + (c - \alpha b)x - \alpha c \end{aligned}$$

By virtue of the equality above, we now know $a = 1$, $b - \alpha a = 0$, $c - \alpha b = -n$, and $-\alpha c = 2$. Since $a = 1$, it is clear that $b - \alpha = 0$, to which $\alpha = b$. In conjunction with the fact that $c - \alpha b = -n$, we have $c - \alpha^2 = -n$. Now we determine α explicitly. Since $-\alpha c = 2$, we know $\alpha = -2/c$, which follows since we assumed $\alpha \in \mathbb{Z}$, and this assumption forces c to divide -2. But now it must be the case that $c = \pm 1, \pm 2$.

We pursue each case seperately using a value of c to determine the value of α, and then using the equation $c - \alpha^2 = -n$. Firstly, if $c = 1$, then $\alpha = -2$ and so we have $1 - (-2)^2 = -3$ to which $n = 3$. Second, if $c = -1$, then $\alpha = 2$, and so $-1 - 2^2 = -5$ to which $n = 5$. Third, if $c = 2$, then $\alpha = -1$, and so $2 - (-1)^2 = 1$ to which $n = -1$. For the fourth and final case, if $c = -2$, then $\alpha = 1$, and so $-2 - 1^2 = -3$ again implies $n = 3$.

Therefore the polynomial $x^3 - nx + 2$ is reducible if and only if n takes one of the values -1, 3, or 5 as determined above. This is equivalent to the desired statement, namely that $x^3 - nx + 2$ is irreducible for $n \neq -1, 3, 5$. ■

Exercise 13.1.8

13.2 Algebraic Extensions

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

Proof. Take p a prime and let $\mathbb{F}$ be a finite field with $\text{char}(\mathbb{F}) = p$. Let F denote the prime subfield of $\mathbb{F}$. We know that $\mathbb{F}/F$ is a finite extension of F since $\mathbb{F}$ is itself finite. As such, $[\mathbb{F} : F]$ is finite, so take $[\mathbb{F} : F] = n$ for some $n \in \mathbb{Z}^+$.

Since $[\mathbb{F} : F] = n$ implies $\mathbb{F}$ is an F-vector space of dimension n, a basis for this vector space is of cardinality n. Each $\alpha \in \mathbb{F}$ can be represented as some linear combination of these n basis elements. In other words, if we fix a basis as $\{v_1, \dots, v_n\}$, then

$$\mathbb{F} = \{\sum_{j=1}^{n} a_j v_j \mid a_j \in F,\ 1 \leq j \leq n\}$$

Since each $a_j \in F$, and $|F| = p$, we know that there are p options for each scalar a_j. Thus there are $p \cdots p = p^n$ options for elements of $\mathbb{F}$. This is equivalent to $|\mathbb{F}| = p^n$, the desired statement. ■

Exercise 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 $f(x) = g(x)h(x)$ 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.

Proof. First we consider $F = \mathbb{F}_2$ and $g(x)$. Since $\deg(g(x)) = 2$, to show that $g(x)$ is irreducible over $\mathbb{F}_2$ we need only show that it has no roots in this field. Since $g(0) = 0 + 0 - 1 = -1$ and $g(1) = 1 + 1 - 1 = 1$, indeed there are no roots. Now let α be a root of $g(x)$. Then

$$\mathbb{F}_2(\alpha) \cong \mathbb{F}_2[x]/(g(x)) = \mathbb{F}_2[x]/(x^2 + x - 1)$$

where $\mathbb{F}_2(\alpha) = \{a_0 + a_1\alpha \mid a_0, a_1 \in \mathbb{F}_2\}$, which shows $|\mathbb{F}_2(\alpha)| = 4$. Thus the field $\mathbb{F}_2(\alpha)$ is our desired field of 4 elements. To construct a field with 8 elements, we now consider the polynomial $h(x)$. Once again, we check for roots in $\mathbb{F}_2$. We find $h(0) = 0 - 0 + 1 = 1$ and $h(1) = 1 - 1 + 1 = 1$, to which $h(x)$ is irreducible over $\mathbb{F}_2$. Taking β to be a root of $h(x)$, we find

$$\mathbb{F}_2(\beta) \cong \mathbb{F}_2[x]/(h(x)) = \mathbb{F}_2[x]/(x^3 - x + 1)$$

where $\mathbb{F}_2(\beta) = \{b_0 + b_1\beta + b_2\beta^2 \mid b_j \in \mathbb{F}_2\}$. This shows $|\mathbb{F}_2(\beta)| = 8$, since there are 2 options for each b_j for $j = 0, 1, 2$. Thus $\mathbb{F}_2(\beta)$ is our desired field of 8 elements.

Now we consider $F = \mathbb{F}_3$. To construct a field of 9 elements, we consider $g(x)$. Since $\deg(g(x)) = 2$, $g(x)$ is irreducible over $\mathbb{F}_3$ only if $g(x)$ has no roots in $\mathbb{F}_3$. So since $g(0) = 0 + 0 - 1 = -1$, $g(1) = 1 + 1 - 1 = 1$, and $g(2) = 4 + 2 - 1 = 2$, we know $g(x)$ is irreducible. Let α be a root. Then

$$\mathbb{F}_3(\alpha) \cong \mathbb{F}_3[x]/(g(x)) = \mathbb{F}_3[x]/(x^2 + x - 1)$$

where $\mathbb{F}_3(\alpha) = \{a_0 + a_1\alpha \mid a_0, a_1 \in \mathbb{F}_3\}$. This shows $|\mathbb{F}_3(\alpha)| = 9$ since there are 3 options for each scalar a_0 and a_1. Thus $\mathbb{F}_3(\alpha)$ is our desired field of 9 elements. To construct a field of 27 elements, we now consider $h(x)$. Since $h(0) = 0 - 0 + 1 = 1$, $h(1) = 1 - 1 + 1 = 1$, and $h(2) = 8 - 2 + 1 = 1$, it follows that $h(x)$ is irreducible over $\mathbb{F}_3$. Let β be a root. Then

$$\mathbb{F}_3(\beta) \cong \mathbb{F}_3[x]/(h(x)) = \mathbb{F}_3[x]/(x^3 - x + 1)$$

and so $\mathbb{F}_3(\beta) = \{b_0 + b_1\beta + b_2\beta^2 \mid b_j \in \mathbb{F}_3\}$. This shows $|\mathbb{F}_3(\beta)| = 27$, showing that $\mathbb{F}_3(\beta)$ is our desired field of 27 elements.

Now we construct multiplication tables for the fields with 4 and 9 elements. First, we consider $\mathbb{F}_2(\alpha)$ from above. We find

	1	α	$\alpha+1$
1	1	α	$\alpha+1$
α	α	$\alpha+1$	1
$\alpha+1$	$\alpha+1$	1	α

It is clear that $\langle\alpha\rangle = \{1, \alpha, \alpha+1\}$ is the cyclic group formed by the nonzero elements of $\mathbb{F}_2(\alpha)$, following since $\alpha^2 = \alpha + 1$ and $\alpha^3 = 1$. Next we construct the table for $\mathbb{F}_3(\alpha)$. We find

x	1	2	α	$\alpha+1$	$\alpha+2$	2α	$2\alpha+1$	$2\alpha+2$
1	1	2	α	$\alpha+1$	$\alpha+2$	2α	$2\alpha+1$	$2\alpha+2$
2	2	1	2α	$2\alpha+2$	$2\alpha+1$	α	$\alpha+2$	$\alpha+1$
α	α	2α	$2\alpha+1$	1	$\alpha+1$	$\alpha+2$	$2\alpha+2$	2
$\alpha+1$	$\alpha+1$	$2\alpha+2$	1	$\alpha+2$	2α	2	α	$2\alpha+1$
$\alpha+2$	$\alpha+2$	$2\alpha+1$	$\alpha+1$	2α	2	$2\alpha+2$	1	α
2α	2α	α	$\alpha+2$	2	$2\alpha+2$	α	$\alpha+1$	1
$2\alpha+1$	$2\alpha+1$	$\alpha+2$	$2\alpha+2$	α	1	$\alpha+1$	2	2α
$2\alpha+2$	$2\alpha+2$	$\alpha+1$	2	$2\alpha+1$	α	1	2α	$\alpha+2$

It is again clear that $\langle\alpha\rangle$ is the cyclic subgroup generated by these nonzero elements. ■

Exercise 13.2.3 Determine the minimal polynomial over $\mathbb{Q}$ for the element $1 + i$.

Proof. We aim to find the unique monic irreducible polynomial over $\mathbb{Q}$ with $1+i$ as a root. Experimenting with powers of this element, we find $(1+i)^2 = 1+2i-1 = 2i$.

Now we can use this fact to see that

$$(1+i)^2 - 2(1+i) + 2 = 0$$

So our guess is the polynomial $x^2 - 2x + 2$ which is indeed an element of $\mathbb{Q}[x]$. The question becomes whether this polynomial is irreducible over $\mathbb{Q}$. The quadratic equation tells us that

$$x = \frac{2 \pm \sqrt{4-8}}{2} = \frac{2 \pm \sqrt{-4}}{2} = \frac{2 \pm 2i}{2} = 1 \pm i$$

are the only two roots of this equation. Since $\mathbb{Q}$ is a field and $x^2 - 2x + 2$ has degree 2, we know $x^2 - 2x + 2$ is reducible if and only if it has roots in $\mathbb{Q}$. However the fact that the only two roots are $1+i$ and $1-i$ permit us to conclude that $x^2 - 2x + 2$ is irreducible over $\mathbb{Q}$ since $1 \pm i \notin Q$. Therefore we may conclude that $x^2 - 2x + 2$ is the minimal polynomial of $1+i$ over $\mathbb{Q}$. ∎

Exercise 13.2.4

Exercise 13.2.5

Exercise 13.2.6

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

Proof. The inclusion $\mathbb{Q}(\sqrt{2}+\sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3})$ is obvious. To prove the reverse inclusion, we show that $\sqrt{2}$ and $\sqrt{3}$ can be expressed as linear combinations of $\sqrt{2}+\sqrt{3}$. Since $\mathbb{Q}(\sqrt{2}+\sqrt{3})$ is a field, we know that the element $\sqrt{2}+\sqrt{3}$ has a multiplicative inverse. Namely, this must be the element $(\sqrt{2}+\sqrt{3})^{-1}$. Note

$$(\sqrt{2}+\sqrt{3})^{-1} = \frac{1}{\sqrt{2}+\sqrt{3}} = \frac{1}{\sqrt{2}+\sqrt{3}} \cdot \frac{\sqrt{2}-\sqrt{3}}{\sqrt{2}-\sqrt{3}} = \frac{\sqrt{2}-\sqrt{3}}{2-3} = \sqrt{3}-\sqrt{2}$$

Therefore $\sqrt{3}-\sqrt{2} \in \mathbb{Q}(\sqrt{2}+\sqrt{3})$ by closure under inverses for nonzero elements. But now it is clear that

$$(\sqrt{2}+\sqrt{3}) + (\sqrt{2}+\sqrt{3})^{-1} = \sqrt{2}+\sqrt{3}+\sqrt{3}-\sqrt{2} = 2\sqrt{3}$$

is also an element of $\mathbb{Q}(\sqrt{2}+\sqrt{3})$ by closure under addition. But since $1/2$ is an element of $\mathbb{Q}(\sqrt{2}+\sqrt{3})$, we obtain $1/2 \cdot 2\sqrt{3} = \sqrt{3} \in \mathbb{Q}(\sqrt{2}+\sqrt{3})$ by closure under multiplication. Since $\sqrt{2}+\sqrt{3}-\sqrt{3} = \sqrt{2} \in \mathbb{Q}(\sqrt{2}+\sqrt{3})$, we have found that both $\sqrt{2}, \sqrt{3} \in \mathbb{Q}(\sqrt{2}+\sqrt{3})$. Since the field $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ is generated over $\mathbb{Q}$ by $\sqrt{2}$ and

$\sqrt{3}$, we have shown $\mathbb{Q}(\sqrt{2}, \sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2} + \sqrt{3})$. This fact combined with the reverse inclusion permits us to write $\mathbb{Q}(\sqrt{2} + \sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, as desired.

To see that $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$, apply the results of Exercise 13.2.8, [[DF-13.2-8]], and note that 2 and 3 are squarefree in $\mathbb{Q}$, and so is $2 \cdot 3 = 6$.

An irreducible polynomial that $\sqrt{2} + \sqrt{3}$ satisfies is the polynomial $x^4 - 10x^2 + 1$. This can be seen for

$$(\sqrt{2} + \sqrt{3})^2 = 5 + 2\sqrt{6} \iff (\sqrt{2} + \sqrt{3})^2 - 5 = 2\sqrt{6}$$

Squaring both sides of the above once more yields the equation

$$((\sqrt{2} + \sqrt{3})^2 - 5)^2 = 4 \cdot 6 = 24$$

Expanding the left hand side of the above shows

$$(\sqrt{2} + \sqrt{3})^4 - 10(\sqrt{2} + \sqrt{3})^2 + 25 = 24$$

Subtracting 24 from both sides of the above finally grants us

$$(\sqrt{2} + \sqrt{3})^4 - 10(\sqrt{2} + \sqrt{3})^2 + 1 = 0$$

And so $\sqrt{2} + \sqrt{3}$ indeed satisfies the polynomial $x^4 - 10x^2 + 1$. Since above we showed $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$, and $\mathbb{Q}(\sqrt{2} + \sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, it follows that the minimal polynomial of $\sqrt{2} + \sqrt{3}$ over $\mathbb{Q}$ must have degree 4. Since $x^4 - 10x^2 + 1$ has $\sqrt{2} + \sqrt{3}$ as a root, and the minimal polynomial divides any other polynomial with $\sqrt{2} + \sqrt{3}$ as a root, we have equality in terms of polynomials. In particular, $x^4 - 10x^2 + 1$ is the minimal polynomial of $\sqrt{2} + \sqrt{3}$ over $\mathbb{Q}$, and so is necessarily irreducible. ∎

Exercise 13.2.8 Let F be a field of characteristic $\neq 2$. Let D_1 and D_2 be elements of F, neither of which is a square in F. Prove that $F(\sqrt{D_1}, \sqrt{D_2})$ is of degree 4 over F if $D_1 D_2$ is not a square in F and is of degree 2 over F otherwise. When $F(\sqrt{D_1}, \sqrt{D_2})$ is of degree 4 over F the field is called a biquadratic extension of F.

Proof. Let F be a field for which $\mathrm{char}(F) \neq 2$. Take $D_1, D_2 \in F$ such that neither D_1 nor D_2 is a square in F, meaning there exists no elements of F whose square is either D_1 or D_2. From these assumptions, we know that the polynomials $x^2 - D_1$ and $x^2 - D_2$ have no solutions in F. Since these polynomials are of degree 2 and have no roots in the field F, we know that each is irreducible over F. Letting $\sqrt{D_1}$ and $\sqrt{D_2}$ denote roots of $x^2 - D_1$ and $x^2 - D_2$, respectively, we can see that $x^2 - D_1$ is the minimal polynomial of $\sqrt{D_1}$ over F, and likewise for $x^2 - D_2$ and $\sqrt{D_2}$ over F. Thus $[F(\sqrt{D_1}) : F] = 2$ and $[F(\sqrt{D_2} : F] = 2$.

Towards the problem, suppose $D_1 D_2$ is not a square in F. Since $F(\sqrt{D_1}, \sqrt{D_2})$ is a finite extension of $F(\sqrt{D_2})$, we know that this extension is algebraic. Let $f(x)$

denote the minimal polynomial of $\sqrt{D_1}$ over $F(\sqrt{D_2})$. By Corollary 10, the minimal polynomial of $\sqrt{D_1}$ over $F(\sqrt{D_2})$ divides the minimal polynomial of $\sqrt{D_1}$ over F. Specifically, $f(x) \mid (x^2 - D_1)$, so that $\deg(f(x)) \leq 2$. We prove that $\deg(f(x)) = 2$. If this were not the case, then $f(x) = x - \sqrt{D_1}$ would hold, which would imply $\sqrt{D_1} \in F(\sqrt{D_2})$ since $f(x) \in F(\sqrt{D_2})[x]$. But then we could write $\sqrt{D_1} = a + b\sqrt{D_2}$ for some $a, b \in F$ by construction of $F(\sqrt{D_2})$. This would imply

$$\sqrt{D_1} - b\sqrt{D_2} = a \iff D_1 - 2b\sqrt{D_1}\sqrt{D_2} + b^2 D_2 = a^2$$

Rearranging the above equation, we obtain

$$\sqrt{D_1}\sqrt{D_2} = \sqrt{D_1 D_2} = \frac{-1}{2b}(a^2 - D_1 - b^2 D_2)$$

Since the right hand side of the above equation lies in F, it then follows that $\sqrt{D_1 D_2} \in F$ also, which is a contradiction to our assumption that $D_1 D_2$ was not a square in F. Thus $\deg(f(x)) = 2$, so $[F(\sqrt{D_1}, \sqrt{D_2}) : F(\sqrt{D_2})] = 2$ follows. This then implies

$$[F(\sqrt{D_1}, \sqrt{D_2}) : F] = [F(\sqrt{D_1}, \sqrt{D_2}) : F(\sqrt{D_2})] \cdot [F(\sqrt{D_2}) : F] = 4$$

and therefore we may conclude $F(\sqrt{D_1}, \sqrt{D_2})$ is of degree 4 over F.

If, on the other hand, we assume that $D_1 D_2$ is a square in F, then our above derivation does not fail, and in fact gives us an expression for $\sqrt{D_1}$ in terms of a linear combination of 1 and $\sqrt{D_2}$. This would then imply that $f(x) = x - \sqrt{D_1}$ would be a valid element of $F(\sqrt{D_2})[x]$, and so then the minimal polynomial of $\sqrt{D_1}$ over $F(\sqrt{D_2})$. This would imply $[F(\sqrt{D_1}, \sqrt{D_2}) : F(\sqrt{D_2})] = 1$, which would necessitate $[F(\sqrt{D_1}, \sqrt{D_2}) : F] = 2$. ■

Exercise 13.2.9 Let F be a field of characteristic $\neq 2$. Let a, b be elements of the field F with b not a square in F. Prove that a necessary and sufficient condition for $\sqrt{a + \sqrt{b}} = \sqrt{m} + \sqrt{n}$ for some m and n in F is that $a^2 - b$ is a square in F. Use this to determine when the field $\mathbb{Q}(\sqrt{a + \sqrt{b}})(a, b \in \mathbb{Q})$ is biquadratic over $\mathbb{Q}$.

Proof. Let F be a field such that $\text{char}(F) \neq 2$ and $a, b \in F$ such that b is not a square. Suppose $\sqrt{a + \sqrt{b}} = \sqrt{m} + \sqrt{n}$ for $m, n \in F$. Upon squaring both sides of this equation, we find this statement is equivalent to

$$a + \sqrt{b} = m + 2\sqrt{mn} + n = n + m + \sqrt{4nm}$$

Now let $a = n + m$ and $b = 4nm$. Then it follows that

$$a^2 - b = (n + m)^2 - 4nm = n^2 - 2nm + m^2 = (n - m)^2$$

and since $n, m \in F$ by assumption, we know that $n - m \in F$ by closure. Thus $a^2 - b$ is a square in F; specifically it is the square of $n - m$. For the reverse implication we need only express the square of $a^2 - b$ as the difference of n and m in F such that $a = n + m$ and $b = 4nm$.

Now we use the above condition to determine when $\mathbb{Q}(\sqrt{a+\sqrt{b}})$ is biquadratic over $\mathbb{Q}$. Towards this goal, suppose $\sqrt{a+\sqrt{b}} = \sqrt{m} + \sqrt{n}$. Then we know that $\mathbb{Q}(\sqrt{a+\sqrt{b}}) = \mathbb{Q}(\sqrt{m}+\sqrt{n})$. In general $\mathbb{Q}(\sqrt{m}+\sqrt{n}) \subseteq \mathbb{Q}(\sqrt{m},\sqrt{n})$. We prove the reverse inclusion in this case. We can find that

$$(\sqrt{m}+\sqrt{n})^{-1} = \frac{1}{\sqrt{m}+\sqrt{n}} = \frac{\sqrt{m}-\sqrt{n}}{m-n}$$

is an element of $\mathbb{Q}(\sqrt{m}+\sqrt{n})$ by closure under multiplicative inverses. Since $m, n \in \mathbb{Q}$ was assumed, it is clear that $m - n \in \mathbb{Q}$, which implies that

$$(m-n)(\sqrt{m}+\sqrt{n})^{-1} = (m-n)\cdot\frac{\sqrt{m}-\sqrt{n}}{m-n} = \sqrt{m}-\sqrt{n}$$

is also an element of $\mathbb{Q}(\sqrt{m}+\sqrt{n})$. But then $\sqrt{m}+\sqrt{n}+\sqrt{m}-\sqrt{n} = 2\sqrt{m}$ is in this field by closure, which means $\sqrt{m} \in \mathbb{Q}(\sqrt{m}+\sqrt{n})$. Similarly we can find that $\sqrt{n} \in \mathbb{Q}(\sqrt{m}+\sqrt{n})$, giving us $\mathbb{Q}(\sqrt{m}+\sqrt{n}) = \mathbb{Q}(\sqrt{m},\sqrt{n})$. Therefore $\mathbb{Q}(\sqrt{a+\sqrt{b}}) = \mathbb{Q}(\sqrt{m},\sqrt{n})$.

Recall the results of Exercise 13.2.8, [[DF-13.2-8]]. Given our above derivation, if we can show that n and m are not squares in $\mathbb{Q}$, and that nm is not a square in $\mathbb{Q}$, then we will have showed that $\mathbb{Q}(\sqrt{m},\sqrt{n})$ is biquadratic over $\mathbb{Q}$. ■

Exercise 13.2.10 Determine the degree of the extension $\mathbb{Q}(\sqrt{3+2\sqrt{2}})$ over $\mathbb{Q}$.

Proof. To determine the degree of $\mathbb{Q}(\sqrt{3+2\sqrt{2}})/\mathbb{Q}$ we will use the results of Exercise 13.2.9, [[DF-13.2-9]]. We may rewrite $\sqrt{3+2\sqrt{2}} = \sqrt{3+\sqrt{8}}$. Now let $a = 3$ and $b = 8$. Since $a^2 - b = 9 - 8 = 1$ is a square in $\mathbb{Q}$, we know that $\sqrt{3+2\sqrt{2}} = \sqrt{m}+\sqrt{n}$ for some $m, n \in \mathbb{Q}$ by Exercise 13.2.9. In particular, $3 = m + n$ and $8 = 4nm$ implies $nm = 2$ to which $n(3-n) = 2$. Expanding out we find that $n^2 - 3n + 2 = 0$. Solving for n using the quadratic formula, we find

$$n = \frac{3 \pm \sqrt{9-8}}{2} = \frac{3 \pm 1}{2}$$

so that either $n = 1$ or $n = 2$. If $n = 1$ then $m = 2$, and if $n = 2$ then $m = 1$. Without loss of generality take $n = 2$ and $m = 1$. We may write

$$\sqrt{3+2\sqrt{2}} = \sqrt{m}+\sqrt{n} = \sqrt{1}+\sqrt{2} = 1+\sqrt{2}$$

Therefore $\mathbb{Q}(\sqrt{3+2\sqrt{2}}) = \mathbb{Q}(1+\sqrt{2}) = \mathbb{Q}(\sqrt{2})$. We have seen before, and it is easily verified, that $\mathbb{Q}(\sqrt{2})$ is an extension of degree 2 over $\mathbb{Q}$. Therefore we may conclude that $\mathbb{Q}(\sqrt{3+2\sqrt{2}})/\mathbb{Q}$ is a degree 2 extension. ■

Exercise 13.2.11

Exercise 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.

Proof. Let K/F be an extension of fields for which $[K : F] = p$, for p a prime. Suppose E is a subfield of K containing F. Then we have a tower of fields $F \subseteq E \subseteq K$. By the multiplicativity of degrees in towers, we may write

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

From the above we know both $[K : E]$ and $[E : F]$ must divide $[K : F] = p$. Since p is prime, however, it follows that each $[K : E]$ and $[E : F]$ are either 1 or p.

If $[K : E] = p$ then it must be that $[E : F] = 1$. But this implies E is a one-dimensional F-vector space, and since F is automatically an F-subspace of E with the same dimesnion as E, this implies $E = F$.

Otherwise we have $[K : E] = 1$, which implies $[E : F] = p$. In this case, the dimension of K as an F-vector space is equal to the dimension of E as an F-subspace of K, and so $K = E$.

Therefore if E is an intermediary subfield of K/F where $[K : F] = p$, the above shows that either $E = K$ or $E = F$, as so desired. ■

Exercise 13.2.13 Suppose $F = \mathbb{Q}(\alpha_1, \alpha_2, \ldots, \alpha_n)$ where $\alpha_i^2 \in \mathbb{Q}$ for $i = 1, 2, \ldots, n$. Prove that $\sqrt[3]{2} \notin F$.

Proof. Assume, for contradiction, that $\sqrt[3]{2} \in \mathbb{Q}(\alpha_1, \ldots, \alpha_n)$, where we have $\alpha_i^2 \in \mathbb{Q}$ for all $1 \leq i \leq n$. Consider the extension $\mathbb{Q}(\alpha_1, \ldots, \alpha_n)$ over $\mathbb{Q}(\alpha_1, \ldots, \alpha_{n-1})$, which we may rewrite more clearly as

$$\mathbb{Q}(\alpha_1, \ldots, \alpha_{n-1})(\alpha_n)/\mathbb{Q}(\alpha_1, \ldots, \alpha_{n-1})$$

In particular, the above makes it clear that α_n generates the extension. Note that the minimal polynomial for α_n over $\mathbb{Q}(\alpha_1, \ldots, \alpha_{n-1})$ is either $x^2 - \alpha_n^2$ or $x - \alpha_n$, where the first case may hold since $\alpha_n^2 \in \mathbb{Q}$ by assumption. Thus either the degree of the extension is 2 or 1. The above holds without loss of generality as we travel down the α_i over $1, \ldots, n$. Hence

$$[\mathbb{Q}(\alpha_1, \ldots, \alpha_n) : \mathbb{Q}] = 2^k$$

for some $k \in \mathbb{Z}^+$, possibly with $k = 1$ if all of the α_i lie in $\mathbb{Q}$. We assumed that $\sqrt[3]{2} \in \mathbb{Q}(\alpha_1, \ldots, \alpha_n)$, and since $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$, we require $3 \mid 2^k$, which is clearly a contradiction no matter our k. Therefore $\sqrt[3]{2} \notin \mathbb{Q}(\alpha_1, \ldots, \alpha_n)$, as desired. ■

Exercise 13.2.14 Prove that if $[F(\alpha) : F]$ is odd then $F(\alpha) = F(\alpha^2)$.

Proof. Let F be a field. Suppose $[F(\alpha) : F]$ is odd. It is clear that $F(\alpha^2) \subseteq F(\alpha)$. In particular, we have a tower of field extensions given by $F \subseteq F(\alpha^2) \subseteq F(\alpha)$. By the multiplicativity of degrees in towers, we know that both $[F(\alpha) : F(\alpha^2)]$ and $[F(\alpha^2) : F]$ divide $[F(\alpha) : F]$.

Note that $x^2 - \alpha^2$ is a polynomial in $F(\alpha^2)[x]$ that has α as a root. Thus we know that the minimal polynomial of α over $F(\alpha^2)$, call it $m_{\alpha,F(\alpha^2)}(x)$, divides $x^2 - \alpha^2$. In particular, this implies that $\deg(m_{\alpha,F(\alpha^2)}(x)) \leq 2$.

If we assume $\deg(m_{\alpha,F(\alpha^2)}(x)) = 2$ then $[F(\alpha) : F(\alpha^2)] = 2$ would naturally follow. However, since $[F(\alpha) : F(\alpha^2)]$ divides $[F(\alpha) : F]$ as per the above, this is a contradiction, as 2 cannot divide an odd number. Thus the only possibility is that $\deg(m_{\alpha,F(\alpha^2)}(x)) = 1$, implying $m_{\alpha,F(\alpha^2)}(x) = x - \alpha$. But this means $\alpha \in F(\alpha^2)$. Therefore $F(\alpha) \subseteq F(\alpha^2)$. Combined with the reverse inclusion above, this proves $F(\alpha) = F(\alpha^2)$. ■

Exercise 13.2.15

Exercise 13.2.16

Exercise 13.2.17

Exercise 13.2.18

Exercise 13.2.19

Exercise 13.2.20

Exercise 13.2.22

13.3 Classical Straightedge and Compass Constructions

so boring

13.4 Splitting Fields and Algebraic Closures

Exercise 13.4.1 Determine the splitting field and its degree over $\mathbb{Q}$ for $x^4 - 2$.

Proof. Consider the polynomial $x^4 - 2$ over $\mathbb{Q}$. To find the splitting field, we factor this polynomial completely and determine its roots. We can find

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

as a factorization of $x^4 - 2$ into linear factors. The roots are $\pm\sqrt[4]{2}$ and $\pm i\sqrt[4]{2}$. Clearly any splitting field for $x^4 - 2$ over $\mathbb{Q}$ must contain all of these roots, and so the extension $\mathbb{Q}(\sqrt[4]{2}, i\sqrt[4]{2})$ over $\mathbb{Q}$ is the natural choice. In fact, this is the smallest extension of $\mathbb{Q}$ containing all of the roots of $x^4 - 2$ since it is generated by $\sqrt[4]{2}$ and $i\sqrt[4]{2}$ over $\mathbb{Q}$.

To determine the degree of the extension, note that we have a tower of fields given by $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[4]{2}) \subseteq \mathbb{Q}(\sqrt[4]{2}, i\sqrt[4]{2})$. The polynomial $x^4 - 2$ is irreducible over $\mathbb{Q}$ by Eisenstein's criterion for $p = 2$. Since $\sqrt[4]{2}$ is a root, it follows that $x^4 - 2$ is the minimal polynomial for $\sqrt[4]{2}$ over $\mathbb{Q}$. Thus $[\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = 4$.

Now we determine $[\mathbb{Q}(\sqrt[4]{2}, i\sqrt[4]{2}) : \mathbb{Q}(\sqrt[4]{2})]$. Note $x^2 + \sqrt{2}$ is a polynomial in $\mathbb{Q}(\sqrt[4]{2})[x]$ that has $i\sqrt[4]{2}$ as a root, since $(\sqrt[4]{2})^2 = \sqrt{2} \in \mathbb{Q}(\sqrt[4]{2})$. Since the minimal polynomial of $i\sqrt[4]{2}$ over $\mathbb{Q}(\sqrt[4]{2})$ divides any polynomial in $\mathbb{Q}(\sqrt[4]{2})[x]$ with $i\sqrt[4]{2}$ as a root, we know that it divides $x^2 + \sqrt{2}$. Therefore its degree is less than or equal to 2.

Assume, for contradiction, that its degree is 1. Then, letting $f(x)$ denote the minimal polynomial of $i\sqrt[4]{2}$ over $\mathbb{Q}(\sqrt[4]{2})$, it must be the case that $f(x) = x - i\sqrt[4]{2}$. However this implies $i\sqrt[4]{2} \in \mathbb{Q}(\sqrt[4]{2})$. Since $\sqrt[4]{2} \in \mathbb{Q}(\sqrt[4]{2})$ has an inverse in this field, closure under multiplication implies $i\sqrt[4]{2} \cdot (\sqrt[4]{2})^{-1} = i \in \mathbb{Q}(\sqrt[4]{2})$. This is a contradiction, for if this were the case tthen $i = a_0 + a_1\sqrt[4]{2} + a_2\sqrt[4]{4} + a_3\sqrt[4]{8}$ for some $a_j \in \mathbb{Q}$ for $j = 0, 1, 2, 3$. Since the i is purely imaginary, it is not representable as a linear combination of purely real numbers.

Therefore it must be the case that the degree of the minimal polynomial of $i\sqrt[4]{2}$ over $\mathbb{Q}(\sqrt[4]{2})$ is 2, to which we may write $[\mathbb{Q}(\sqrt[4]{2}, i\sqrt[4]{2}) : \mathbb{Q}(\sqrt[4]{2})] = 2$. By the multiplicativity of degrees in towers, we have the equation

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

which is the desired degree of the splitting field of $x^4 - 2$ over $\mathbb{Q}$. ∎

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

Proof. First we will give a factorization of $x^4 + 2$ into linear factors. Recall that $\sqrt{i} = (1 + i)/\sqrt{2} = \zeta_8$. In particular, $\zeta_8^4 = (\sqrt{i})^4 = i^2 = -1$. We can also find that

$(\zeta_8^3)^4 = \zeta_8^{12} = (\zeta_8^4)^3 = (-1)^3 = -1$. A similar process shows that ζ_8^5, ζ_8^7 are also equal to -1 when raised to the fourth power. This allows us to see that

$$x^4 + 2 = (x - \zeta_8\sqrt[4]{2})(x - \zeta_8^3\sqrt[4]{2})(x - \zeta_8^5\sqrt[4]{2})(x - \zeta_8^7\sqrt[4]{2})$$

In particular, the roots of $x^4 + 2$ are $\zeta_8\sqrt[4]{2}$, $\zeta_8^3\sqrt[4]{2}$, $\zeta_8^5\sqrt[4]{2}$, and $\zeta_8^7\sqrt[4]{2}$. Therefore the splitting field must contain these roots. Note that

$$\zeta_8^7\sqrt[4]{2} = (\zeta_8)^7\sqrt[4]{2} = (\sqrt{i})^7\sqrt[4]{2} = -i\zeta_8\sqrt[4]{2} = \frac{\sqrt[4]{2}}{\sqrt{2}} - \frac{\sqrt[4]{2}}{\sqrt{2}}i$$

Adding the element above to $\zeta_8\sqrt[4]{2}$ we find that

$$\zeta_8\sqrt[4]{2} + \zeta_8^7\sqrt[4]{2} = \frac{\sqrt[4]{2}}{\sqrt{2}} + \frac{\sqrt[4]{2}}{\sqrt{2}}i + \frac{\sqrt[4]{2}}{\sqrt{2}} - \frac{\sqrt[4]{2}}{\sqrt{2}}i = 2\frac{\sqrt[4]{2}}{\sqrt{2}} = 2 \cdot \frac{1}{\sqrt[4]{2}}$$

Therefore the splitting field of $x^4 + 2$ must contain $\sqrt[4]{2}$ and ζ_8, and conversely any field extension containing $\sqrt[4]{2}$ and ζ_8 must contain the four roots above. In particular, the spliting field for the polynomial $x^4 + 2$ over $\mathbb{Q}$ is $\mathbb{Q}(\zeta_8, \sqrt[4]{2})$.

Note that we have a tower of extensions via $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[4]{2}) \subseteq \mathbb{Q}(\zeta_8, \sqrt[4]{2})$. Since $x^4 - 2$ is an irreducible polynomial, namely by Eisenstein's at $p = 2$, and $\sqrt[4]{2}$ is a root, we have $[\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = 4$.

To determine $[\mathbb{Q}(\zeta_8, \sqrt[4]{2}) : \mathbb{Q}(\sqrt[4]{2})]$, we first recall that $\mathbb{Q}(\zeta_8) = \mathbb{Q}(\sqrt{2}, i)$. Then we see $\mathbb{Q}(\zeta_8, \sqrt[4]{2}) = \mathbb{Q}(\sqrt[4]{2}, i)$. Note that $x^2 + 1$ is the minimal polynomial for i over $\mathbb{Q}$. The minimal polynomial for i over $\mathbb{Q}(\sqrt[4]{2})$ divides $x^2 + 1$ and so is either of degree 1 or 2. However if it were of degree one then $i \in \mathbb{Q}(\sqrt[4]{2})$, which is a contradiction for every element of $\mathbb{Q}(\sqrt[4]{2})$ is purely real. Therefore $[\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}(\sqrt[4]{2})] = 2$, and so

$$[\mathbb{Q}(\zeta_8, \sqrt[4]{2}) : \mathbb{Q}] = [\mathbb{Q}(\zeta_8, \sqrt[4]{2}) : \mathbb{Q}(\sqrt[4]{2})] \cdot [\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = 2 \cdot 4 = 8$$

Thus we may conclude that the splitting field for $x^4 + 2$ over $\mathbb{Q}$ is a degree 8 extension of $\mathbb{Q}$, as desired. ■

Exercise 13.4.3 Determine the splitting field and its degree over $\mathbb{Q}$ for $x^4 + x^2 + 1$.

Proof. First we determine a complete factorization of $x^4 + x^2 + 1$ over $\mathbb{Q}$. We can find

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

is such a factorization into a product of irreducible quadratic factors. We can see that these factors are irreducible by examining their roots. Using the quadratic equation, we find that

$$x = \frac{-1 \pm \sqrt{1-4}}{2} = -\frac{1}{2} \pm \frac{\sqrt{3}}{2}i$$

are the roots of the first quadratic factor. For the second, we use the formula again to find

$$x = \frac{1 \pm \sqrt{1-4}}{2} = \frac{1}{2} \pm \frac{\sqrt{3}}{2} i$$

as the two roots of the second quadratic factor. It is also worth noting that these four roots are equal to $\pm\zeta_3$ and $\pm\zeta_6$, respectively. It can be easily verified that adjoining any one of the four roots above to $\mathbb{Q}$ is equivalent to adjoining all four roots to $\mathbb{Q}$. Thus it is clear that the smallest extension of $\mathbb{Q}$ which contains all roots of $x^4 + x^2 + 1$ is $\mathbb{Q}(\zeta_3)$ (or $\mathbb{Q}(\zeta_6)$, they are equivalent).

To determine the degree of $\mathbb{Q}(\zeta_3)$ over $\mathbb{Q}$, we need only recall the 3rd cyclotomic polynomial $\Phi_3(x) = x^2 + x + 1$, which has ζ_3 as a root, and $\Phi_3(x)$ is irreducible over $\mathbb{Q}$. It follows that $[\mathbb{Q}(\zeta_3) : \mathbb{Q}] = 2$ is the desired degree. This could also have been seen using the formula $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$, where $\varphi(x)$ is Euler's totient function, as discussed in the text of this chapter section. ■

Exercise 13.4.4 Determine the splitting field and its degree over $\mathbb{Q}$ for $x^6 - 4$.

Proof. First we will determine a complete factorization of $x^6 - 4$ into linear factors. We have

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

Note that both of the cubic factors above are irreducible over $\mathbb{Q}$, say by Eisenstein's criterion applied for $p = 3$. Now we expand the two cubics above as follows:

$$x^6 - 4 = (x + \sqrt[3]{2})(x + \sqrt[3]{2}\zeta_3)(x + \sqrt[3]{2}\zeta_3^2)(x - \sqrt[3]{2})(x - \sqrt[3]{2}\zeta_3)(x - \sqrt[3]{2}\zeta_3^2)$$

Therefore the six roots of the polynomial are $\pm\sqrt[3]{2}$, $\pm\sqrt[3]{2}\zeta_3$, and $\pm\sqrt[3]{2}\zeta_3^2$. The splitting field for $x^6 - 4$ is the field obtained by adjoining the six roots above to $\mathbb{Q}$. In fact, we can see $\mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}\zeta_3, \sqrt[3]{2}\zeta_3^2) = \mathbb{Q}(\sqrt[3]{2}, \zeta_3)$ which follows by closure. Since $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)$ is generated by $\sqrt[3]{2}$ and ζ_3 over $\mathbb{Q}$, it is the smallest extension field containing all of the roots above. Therefore $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)$ is the splitting field for $x^6 - 4$ over $\mathbb{Q}$.

We have towers of fields $\mathbb{Q} \subseteq \mathbb{Q}(\zeta_3) \subseteq \mathbb{Q}(\sqrt[3]{2}, \zeta_3)$ and $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{Q}(\sqrt[3]{2}, \zeta_3)$. We know that $[\mathbb{Q}(\zeta_3) : \mathbb{Q}] = 3 - 1 = 2$ by the discussion in this section. Also, we may write that $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ since $x^3 - 2$ is irreducible by Eisenstein's criterion at $p = 2$ and $\sqrt[3]{2}$ is a root. Since $\gcd(2, 3) = 1$, we may appeal to Corollary 22 to write that $[\mathbb{Q}(\sqrt[3]{2}, \zeta_3) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] \cdot [\mathbb{Q}(\zeta_3) : \mathbb{Q}] = 3 \cdot 2 = 6$. Thus the degree of ths splitting field $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)/\mathbb{Q}$ is 6. ■

Exercise 13.4.5 Let K be a finite extension of F. Prove that K is a splitting field over F if and only if every irreducible polynomial in $F[x]$ which has a root in K splits completely in $K[x]$. [Use Theorems 8 and 27.]

Proof. Let K/F be a finite extension of fields. Suppose K is a splitting field for a family of polynomials $\{f_i\}_{i\in I}$ in $F[x]$. Let F^a denote the algebraic closure of F. If α_i is a root of f_i contained in K, then any embedding $\sigma : K \to F^a$ takes α_i to another root $\sigma(\alpha_i)$ of f_i. Since K is the extension of F generated by the roots of these polynomials by assumption, it follows that every such embedding σ is an automorphism of K which fixes F.

Conversely, assume that any embedding of K into F^a induces an automorphism of K. Let $\alpha \in K$ and let $m_\alpha(x)$ be the minimal polynomial for α over F. Let β be another root of $m_\alpha(x)$, contained in F^a but not necessarily in K. By Theorem 8, there exists an isomorphism $F(\alpha)$ to $F(\beta)$ which restricts to the identity on F, and maps $\alpha \mapsto \beta$. We may extend this map to an embedding of K into F^a, and so by the above paragraph, we have an automorphism of K. But this means that $\beta \in K$. In particular, every root of an irreducible polynomial in $F[x]$ which is contained in K splits complextely in K, and so K is the splitting field for any such polynomial.

We have shown that if every embedding of K into F^a induces an automorphism of K, then K is a splitting field and each irreducible polynomial with a root in K splits completely in K. Since in the first paragraph we showed that K being a splitting field for F implies each such embedding gives an automorphism, we need only prove that if every irreducible polynomial with a root in K splits completely in K, then each embedding of K into F^a is an automorphism.

To this end, let σ be an embedding of K in F^a which fixes F. Let $\alpha \in K$ with minimal polynomial $m(x)$ over F. We know that σ takes roots of $m(x)$ to roots of $m(x)$, and by assumption, such roots are contained in K. Thus σ maps K to itself. ∎

Exercise 13.4.6 Let K_1 and K_2 be finite extensions of F contained in the field K, and assume both are splitting fields over F.
(a) Prove that their composite K_1K_2 is a splitting field over F.
(b) Prove that $K_1 \cap K_2$ is a splitting field over F. [Use the preceding exercise]

Proof. (a) Since both K_1 and K_2 are splitting fields over F, both are finite extensions of F generated by roots of polynomials. In particular, their compositum K_1K_2 is a finite extension of F generated by the roots of polynomials in F; hence is a splitting field over F.

(b) If $f(x) \in F[x]$ is an irreducible polynomial with a root α in $K_1 \cap K_2$, then $\alpha \in K_1$ and $\alpha \in K_2$, and by Exercise 13.4.5, the fact that both K_1 and K_2 are splitting fields imoly $f(x)$ splits completely in $K_1[x]$ and $K_2[x]$, and hence in $K_1 \cap K_2[x]$. Now by the same exercise, $K_1 \cap K_2$ is a splitting field over F. ∎

13.5 Seperable and Inseperable Extensions

Exercise 13.5.1

Exercise 13.5.2 Find all irreducible polynomials of degrees 1, 2, and 4 over $\mathbb{F}_2$ and prove that their product is $x^{16} - x$.

Proof. Consider the field $\mathbb{F}_2$. The irreducible polynomials of degree 1 over $\mathbb{F}_2$ are simply x and $x - 1$, the linear polynomials, since $\mathbb{F}_2 = \{0, 1\}$. There are $4 = 1 \cdot 2 \cdot 2$ possible quadratic polynomials over $\mathbb{F}_2$. These polynomials are $x^2 + x + 1$, $x^2 + x$, $x^2 + 1$, and x^2. The polynomial $x^2 + x + 1$ is the only quadratic with no roots in $\mathbb{F}_2$; note $x^2 + x$ has 0 and 1 as a root, $x^2 + 1$ has 1 as a root, and x^2 has 0 as a root. Thus, since degree 2 polynomials are reducible over fields only when they have roots in the field, we know $x^2 + x + 1$ is the only irreducible quadratic over $\mathbb{F}_2$.

There are $16 = 1 \cdot 2 \cdot 2 \cdot 2 \cdot 2$ possible quartic polynomials over $\mathbb{F}_2$. In order to determine which are irreducible without manually checking, we resort to alternate means. We can immediately remove those quartics with x as a factor, as these are trivially reducible; now we must have a constant term, of which our only option is 1, in our irreducible quartic. This narrows our search down to $8 = 1 \cdot 2 \cdot 2 \cdot 2 \cdot 1$ quartics. These 8 polynomials are as follows:

$$x^4 + 1;\ x^4 + x + 1;\ x^4 + x^2 + x + 1;\ x^4 + x^3 + x^2 + x + 1;$$

$$x^4 + x^2 + 1;\ x^4 + x^3 + 1;\ x^4 + x^3 + x^2 + 1;\ x^4 + x^3 + x + 1.$$

Only 4 of the 8 quartics above do not have roots in $\mathbb{F}_2$; i.e., 4 of them have $x = 1$ as a root, and so have $x - 1 (= x + 1)$ as a linear factor, so are reducible. Removing these polynomials, we are left with

$$x^4 + x + 1;\ x^4 + x^3 + 1;\ x^4 + x^2 + 1;\ x^4 + x^3 + x^2 + x + 1.$$

Since each of the polynomials above do not have a linear factor, in order to be reducible they must be equal to the product of two irreducible quadratic factors. However in our work above we showed there is only one irreducible quadratic factor over $\mathbb{F}_2$, namely $x^2 + x + 1$. We can find

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

and so we may remove $x^4 + x^2 + 1$ from our above list of 4 polynomials since it is reducible. Therefore we are left with three quartic polynomials that are not equal to a product of two irreducible quadratic factors, and do not have linear factors, and thus are irreducible over $\mathbb{F}_2$: the polynomials $x^4 + x + 1$, $x^4 + x^3 + 1$, and $x^4 + x^3 + x^2 + x + 1$.

Now we have found all irreducible polynomials of degrees 1, 2, and 4 over $\mathbb{F}_2$. What remains is to prove that their product is equal to $x^{16} - x$. Since $x^{16} - x (= x^{16} + x)$, we can find that

$$x^{16} + x = (x^{12} + x^9 + x^6 + x^3 + 1)(x^4 + x)$$
$$= (x^8 + x^7 + x^5 + x^4 + x^3 + x + 1)(x^4 + x^3 + x^2 + x + 1)(x^4 + x)$$
$$= (x^4 + x + 1)(x^4 + x^3 + 1)(x^4 + x^3 + x^2 + x + 1)(x^2 + x + 1)(x + 1)x$$

and so indeed the product of all of the irreducibles above is equal to $x^{16} - x$, as desired. ■

Exercise 13.5.3 Prove that d divides n if and only if $x^d - 1$ divides $x^n - 1$.

Proof. Assume $d \mid n$. Then this implies $n = dk$ for some $k \in \mathbb{Z}^+$. In this way we know

$$x^n - 1 = x^{dk} - 1 = (x^d)^k - 1^k = (x^d - 1)((x^d)^k + (x^d)^{k-1} + \cdots + x^d + 1)$$

so that $(x^d - 1) \mid (x^n - 1)$. We could have equivalently proved this direction by recalling the formula $\gcd(x^n - 1, x^m - 1) = x^{\gcd(n,m)} - 1$. Here, since $d \mid n$ by assumption, it is clear that $\gcd(d, n) = d$ itself, and so $x^d - 1$ is the greatest common divisor of $x^n - 1$ and $x^d - 1$, proving that $x^d - 1$ indeed divides $x^n - 1$.

Conversely, assume $x^d - 1$ divides $x^n - 1$. It is clear that $d \leq n$. By the division algorithm, we may then write that

$$x^n - 1 = (x^d - 1)q(x)$$

for some $q(x) \in \mathbb{Z}[x]$. Now, taking the derivative of both sides of the above equation, we have the following

$$D_x(x^n - 1) = D_x((x^d - 1)q(x)) = D_x(x^d - 1)q(x) + (x^d - 1)D_x(q(x))$$

Computing the above derivatives explicitly, we may find

$$nx^{n-1} = (dx^{d-1})q(x) + (x^d - 1)q'(x)$$

Now substituting $x = 1$, we see that $(x^d - 1)q'(x) = (1 - 1)q'(1) = 0$, and so we are left with

$$n = dq(1)$$

But note that $q(x)$ was a polynomial in $\mathbb{Z}[x]$, and so it follows that $q(1) \in \mathbb{Z}$ as well. Indeed, this implies that $d \mid n$, as so desired. ■

Exercise 13.5.4 Let $a > 1$ be an integer. Prove for any positive integers n, d that d divides n if and only if $a^d - 1$ divides $a^n - 1$ (cf. the previous exercise). Conclude in particular that $\mathbb{F}_{p^d} \subseteq \mathbb{F}_{p^n}$ if and only if d divides n.

Proof. Take $a \in \mathbb{Z}^+$ such that $a \neq 1$, and let $n, d \in \mathbb{Z}^+$. Assume $d \mid n$. By Exercise 13.5.3, [[DF-13.5-3]], this implies $x^d - 1$ divides $x^n - 1$. In particular, setting $x = a$ grants us that $a^d - 1$ divides $a^n - 1$. The converse follows similarly from the previous exercise.

Now assume $\mathbb{F}_{p^d} \subseteq \mathbb{F}_{p^n}$. Then note $\mathbb{F}_{p^d}^\times \subseteq \mathbb{F}_{p^n}^\times$ follows. It is clear that, when considered as a multiplicative abelian group, $\mathbb{F}_{p^d}^\times$ is a subgroup of $\mathbb{F}_{p^n}^\times$. In particular, by Lagrange's Theorem we know that $p^d - 1$ divides $p^n - 1$. However since $p \in \mathbb{Z}^+$ and $p \neq 1$, our result above permits us to write that $d \mid n$. The converse follows similarly, in that assuming $d \mid n$ means $(p^d - 1) \mid (p^n - 1)$, and since finite fields of order p^n exist, namely $\mathbb{F}_{p^n}$, and p^d divides p^n, Sylow's Theorem guarantees the existence of the subgroup $\mathbb{F}_{p^d}$ of $\mathbb{F}_{p^n}$, so that indeed $\mathbb{F}_{p^d} \subseteq \mathbb{F}_{p^n}$. ■

Exercise 13.5.5 For any prime p and any nonzero $a \in \mathbb{F}_p$ prove that $x^p - x + a$ is irreducible and seperable over $\mathbb{F}_p$. [For the irreducibility: One approach – prove first that if α is a root then $\alpha + 1$ is also a root. Another approach: – suppose it's reducible and compute derivatives.]

Proof. Let p be a prime and $a \in \mathbb{F}_p \setminus \{0\}$. Consider the polynomial $x^p - x + a \in \mathbb{F}_p[x]$. Suppose β is a root of this polynomial. Then we have:

$$\beta^p - \beta + a = 0$$

Now observe the following fact:

$$(\beta + 1)^p - (\beta + 1) + a = \beta^p + 1 - \beta - 1 + a = \beta^p - \beta + a$$

The equation above equals 0 by the assumption that β is a root of this polynomial. In partocular, we have shown that $\beta + 1$ is another root. Further, we can see that for any $n \in \mathbb{F}_p$, we have:

$$(\beta + n)^p - (\beta + n) + a = \beta^p + n - \beta - n + a = \beta^p - \beta + a = 0$$

Which follows since $n^p = (1 + \cdots + 1)^p = 1 + \cdots + 1 = n$ for each such n. In particular, we have $\beta, \beta + 1, \ldots, \beta + p - 1$ as roots of $x^p - x + a$. TO FINISH XXX ■

Exercise 13.5.6 Prove that $x^{p^n - 1} - 1 = \prod_{\alpha \in \mathbb{F}_{p^n}^\times}(x - \alpha)$. Conclude that $\prod_{\alpha \in \mathbb{F}_{p^n}^\times} \alpha = (-1)^{p^n}$ so the product of the nonzero elements of a finite field is $+1$ if $p = 2$ and -1 if p is odd. For p odd and $n = 1$ derive Wilson's Theorem: $(p - 1)! \equiv -1 \pmod{p}$.

Proof. Let F be some finite field of characteristic p, where p is a prime. We may write that $|F| = p^n$ for some $n \in \mathbb{Z}^+$, so that $F = \mathbb{F}_{p^n}$. Since $|\mathbb{F}_{p^n}^\times| = p^n - 1$, recall that $\alpha^{p^{n-1}} = 1$ for every $\alpha \neq 0$ in $\mathbb{F}_{p^n}$. In particular, the polynomial $x^{p^n - 1} - 1$ over $\mathbb{F}_{p^n}$ has each $\alpha \in \mathbb{F}_{p^n}^\times$ for a root. Therefore $x - \alpha$ divides $x^{p^n - 1} - 1$ for all $\alpha \in \mathbb{F}_{p^n}^\times$.

Since the product of the linear factors, $\prod_{\alpha\in\mathbb{F}_{p^n}^\times}(x-\alpha)$ has degree p^n-1 and divides $x^{p^n-1}-1$, it follows that

$$x^{p^n-1}-1=\prod_{\alpha\in\mathbb{F}_{p^n}^\times}(x-\alpha)$$

Now, after rearranging the above equation, we may find that

$$x^{p^n-1}-1=(-1)^{p^n-1}\prod_{\alpha\in\mathbb{F}_{p^n}^\times}(\alpha-x)$$

Substituting the value $x=0$ into the above equation yields the following

$$-1=(-1)^{p^n-1}\prod_{\alpha\in\mathbb{F}_{p^n}^\times}\alpha$$

Finally, we may multiply both sides of the above equation by $(-1)^{p^n-1}$ and find

$$(-1)^{p^n}=(-1)^{2(p^n-1)}\prod_{\alpha\in\mathbb{F}_{p^n}^\times}\alpha=(1^{p^n-1})\prod_{\alpha\in\mathbb{F}_{p^n}^\times}\alpha=\prod_{\alpha\in\mathbb{F}_{p^n}^\times}\alpha$$

which is the desired statement. If $p=2$ then $(-1)^{2^n}=1^n=1$ is equal to the product of the nonzero elements of $\mathbb{F}_{2^n}$. If p is odd, then $(-1)^{p^n}=-1$, and so the product of all nonzero elements of $\mathbb{F}_{p^n}$ is -1.

Now we will derive Wilson's Theorem. Set $n=1$ and let p be an odd prime. Then $\mathbb{F}_{p^n}=\mathbb{F}_p$. Note $\mathbb{F}_p=\{0,1,\dots,p-1\}$. Observe that since p is odd, $(-1)^p=-1$, and so from the above identity, we can find

$$-1=\prod_{\alpha\in\mathbb{F}_p^\times}\alpha=(p-1)\cdot(p-2)\cdots 1=(p-1)!$$

In particular, since the above computation takes place over $\mathbb{F}_p$, the above equation indeed shows that $(p-1)!\equiv -1 \pmod{p}$, as desired. ■

Exercise 13.5.7 Suppose K is a field of characteristic p which is not a perfect field: $K\neq K^p$. Prove there exist irreducible inseperable polynomials over K. Conclude that there exist inseperable finite extensions of K.

Proof. Let K be a field that is not perfect such that $\mathrm{char}(K)=p$. Every irreducible polynomial over a finite field is seperable, so K must be infinite. In particular, $K/\mathbb{F}_p$ is an infinite extension. Thus $K=\mathbb{F}_p(t_1,t_2,\dots)$. Consider the polynomial $p(x)=x^p-t_1$ over K. It is clear that $p(x)$ is irreducible over K by Eisenstein's criterion applied at the prime ideal (t_1) of K. Furthermore we have $D_x(p(x))=px^{p-1}=0$ so that $p(x)$ is inseperable by Proposition 33. In particular we have $p(x)=x^p-t_1=(x-\sqrt[p]{t_1})^p$. Therefore taking $K(\sqrt{t_1})$ gives us a finite extension of K that is inseperable, namely since the element $\sqrt{t_1}$ is nit the root of a seperable polynomial over K. ■

Exercise 13.5.8 Prove that $f(x)^p = f(x^p)$ for any polynomial $f(x) \in \mathbb{F}_p[x]$.

Proof. Let $\mathbb{F}_p$ be the finite field of p elements. Take $f(x) \in \mathbb{F}_p[x]$ an arbitrary polynomial, say with $f(x) = \sum_{j=0}^{n} a_j x^j$ where $a_j \in \mathbb{F}_p$ for each $1 \leq j \leq n$. Now, by Proposition 35, the Frobenius endomorphism of $\mathbb{F}_p$ permits us to write that

$$f(x)^p = (\sum_{j=0}^{n} a_j x^j)^p = \sum_{j=0}^{p} (a_j x^j)^p$$

By the commutativity of multiplication in the field $\mathbb{F}_p$ and the fact that $\alpha^p = \alpha$ for all $\alpha \in \mathbb{F}_p$ since $\text{char}(\mathbb{F}_p) = p$, we may rewrite the above equation as

$$f(x)^p = \sum_{j=0}^{n} (a_j x^j)^p = \sum_{j=0}^{n} a_j^p (x^j)^p = \sum_{j=0}^{n} a_j (x^p)^j = f(x^p)$$

which is precisely the desired statemnet for polynomials in $\mathbb{F}_p[x]$. ∎

Exercise 13.5.9

Exercise 13.5.10 Let $f(x_1, x_2, \ldots, x_n) \in \mathbb{Z}[x_1, x_2, \ldots, x_n]$ be a polynomial in the variables $x_1, x_2, \ldots, x_n$ with integer coefficients. For any prime p prove that the polynomial

$$f(x_1, x_2, \ldots, x_n)^p - f(x_1^p, x_2^p, \ldots, x_n^p) \in \mathbb{Z}[x_1, x_2, \ldots, x_n]$$

has all its coefficients divisible by p.

Proof. Let $f(x_1, \ldots, x_n) \in \mathbb{Z}[x_1, \ldots, x_n]$ be arbitrary, and let p be some prime. The desired statement, specifically that

$$f(x_1, \ldots, x_n)^p - f(x_1^p, \ldots, x_n^p) \in \mathbb{Z}[x_1, \ldots, x_n]$$

has all its coefficients divisible by p, is equivalent to saying that

$$f(x_1, x_2, \ldots, x_n)^p - f(x_1^p, x_2^p, \ldots, x_n^p) = 0$$

when considered over $\mathbb{F}_p$. This follows since if the coefficients of the desired polynomial are all divisible by p, then they are identically 0 in $\mathbb{F}_p$, so that the above polynomial is equal to the zero polynomial in $\mathbb{F}_p[x]$. By Proposition 33, the Frobenius endomorphism in $\mathbb{F}_p$, we may proceed as in Exercise 13.5.8, [[DF-13.5-8]], to write that

$$f(x_1, \ldots, x_n)^p = (\sum_{i=0}^{n} a_i x_1^{d_{1_i}} \cdots x_n^{d_{n_i}})^p = \sum_{i=0}^{n} a_i^p (x_1^{d_{1_i}})^p \cdots (x_n^{d_{n_i}})^p$$

Next, since $a_i^p = a_i$ for all $a_i \in \mathbb{F}_p$, and the commutativity of multiplication, we find

$$f(x_1, \ldots, x_n)^p = \sum_{i=0}^{n} a_i^p (x_1^{d_{1_i}})^p \cdots (x_n^{d_{n_i}})^p$$

$$= \sum_{i=0}^{n} a_i (x_1^p)^{d_{1_i}} \cdots (x_n^p)^{d_{n_i}} = f(x_1^p, \ldots, x_n^p)$$

Therefore, given this result above we may conclude that indeed

$$f(x_1, x_2, \ldots, x_n)^p = f(x_1^p, x_2^p, \ldots, x_n^p)$$

holds, so that the difference of the two polynomials above is equal to the zero polynomial when considered in $\mathbb{F}_p[x]$. This implies that each of the coefficients of the polynomial $f(x_1, x_2, \ldots, x_n)^p - f(x_1^p, x_2^p, \ldots, x_n^p)$ are divisible by p, as desired. ■

Exercise 13.5.11 Suppose $K[x]$ is a polynomial ring over the field K and F is a subfield of K. If F is a perfect field and $f(x) \in F[x]$ has no repeated irreducible factors in $F[x]$, prove that $f(x)$ has no repeated irreducible factors in $K[x]$.

Proof. Let K/F be an extension of fields. Suppose F is a perfect field and $f(x) \in F[x]$ has no repeated irreducible factors in $F[x]$. Assume, for contradiction, that $f(x)$ has some repeated irreducible factor in $K[x]$, say $\pi(x)$. Then, letting α denote a root of $\pi(x)$, we know that over a splitting field for $f(x)$, α is a multiple root of multiplicity ≥ 1. Since every polynomial over a perfect field is seperable, in this case $f(x)$ over F, we know that $f(x)$ has no repeated roots. But since α is such a repeated root of $f(x)$, this is a contradiction. Therefore $f(x)$ has no repeated irreducible factors in $K[x]$. ■

13.6 Cyclotomic Polynomials and Extensions

Exercise 13.6.1

Exercise 13.6.2

Exercise 13.6.3

Exercise 13.6.4

Exercise 13.6.5

Exercise 13.6.6

Exercise 13.6.7

Exercise 13.6.8

Exercise 13.6.9

Exercise 13.6.10

Exercise 13.6.11 Let φ denote the Frobenius map $x \mapsto x^p$ on the finite field $\mathbb{F}_{p^n}$. Prove that φ gives an isomorphism of $\mathbb{F}_{p^n}$ to itself (such an isomorphism is called an automorphism). Prove that φ^n is the identity map and that no lower power of φ is the identity.

Proof. Consider the finite field $\mathbb{F}_{p^n}$. Construct $\varphi : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ defined by $\varphi(\alpha) = \alpha^p$ for all $\alpha \in \mathbb{F}_{p^n}$. Let $a, b \in \mathbb{F}_{p^n}$. Since $\mathbb{F}_{p^n}$ is a field of characteristic p, Proposition 35, the Frobenius endomorphism, allows us to conclude that

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

in addition to

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

so that the multiplicative and additive structure of $\mathbb{F}_{p^n}$ is preserved by φ. Since $\varphi(1) = 1^p = 1$, we know that φ is not the zero map, and so this ring homomorphism of fields is automatically injective by Proposition 2. Since $|\mathbb{F}_{p^n}| = p^n < \infty$, and φ maps $\mathbb{F}_{p^n}$ to itself, injectivity forces surjectivity as well. Therefore φ is an isomorphism of fields, and since $\varphi : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$, we know φ is an automorphism of $\mathbb{F}_{p^n}$, so that $\varphi \in \text{Aut}(\mathbb{F}_{p^n})$.

Since $\mathbb{F}_{p^n}^\times$ is a multiplicative abelian group of order $p^n - 1$, we know that $\alpha^{p^n-1} = 1$ for all $\alpha \in \mathbb{F}_{p^n}^\times$. In particular, $\alpha^{p^n} = \alpha$ holds in general for elements of $\mathbb{F}_{p^n}$. Note that $\varphi^n(\alpha) = (\alpha^p)^n = \alpha^{p^n} = \alpha$ for all $\alpha \in \mathbb{F}_{p^n}$. Therefore, in the group of automorphisms of $\mathbb{F}_{p^n}$, the order of φ is less than or equal to n, equivalently $|\varphi| \leq n$. If we assumed $|\varphi| = k < n$, then $\varphi^k(\alpha) = \alpha^{p^k} = \alpha$ implies $\alpha^{p^k-1} = 1$ in the group $\mathbb{F}_{p^n}^\times$. But then $x^{p^k-1} - 1$ would have all elements $\alpha \in \mathbb{F}_{p^n}^\times$ as roots, so would have $p^n - 1$ roots, which is a contradiction for the polynomial $x^{p^k-1} - 1$ can have at most $p^k - 1$ roots, and $k < n$. Thus $|\varphi| = n$ must hold, as desired. ∎

Exercise 13.6.12

Exercise 13.6.13 (Wedderburn's Theorem on Finite Division Rings) This exercise outlines a proof (following Witt) of Wedderburn's Theorem that a finite division ring D is a field (i.e., is commutative).

(a) Let Z denote the center of D (i.e., the elements of D which commute with every element of D). Prove that Z is a field containing $\mathbb{F}_p$ for some prime p. If $Z = \mathbb{F}_q$ prove that D has order q^n for some integer n.

(b) The nonzero elements $D^\times$ of D form a multiplicative group. For any $x \in D^\times$ show that the elements of D which commute with x form a division ring which contains Z. Show that this division ring is of order q^m for some integer m and that $m < n$ if x is not an element of Z.

(c) Show that the class equation (Theorem 4.7) for the group $D^\times$ is

$$q^n - 1 = (q-1) + \sum_{i=1}^{r} \frac{q^n - 1}{|C_{D^\times}(x_i)|}$$

where $x_1, x_2, \ldots, x_r$ are representatives of the distinct conjugacy classes in $D^\times$ not contained in the center of $D^\times$. Conclude from (b) that for each i, $|C_{D^\times}(x_i)| = q^{m_i} - 1$ for some $m_i < n$.

(d) Prove that since $\frac{q^n-1}{q^{m_i}-1}$ is an integer (namely, the index $|D^\times : C_{D^\times}(x_i)|$) then m_i divides n (cf. Exercise 4 of Section 5). Conclude that $\Phi_n(x)$ divides $(x^n - 1)/(x^{m_i} - 1)$ and hence that the integer $\Phi_n(q)$ divides $(q^n - 1)/(q^{m_i} - 1)$ for $i = 1, 2, \ldots, r$.

(e) Prove that (c) and (d) imply that $\Phi_n(q) = \prod_{\zeta \text{ primitive}}(q - \zeta)$ divides $q - 1$. Prove that $|q - \zeta| > q-$ (complex absolute value) for any root of unity $\zeta \neq 1$. Conclude that $n = 1$, i.e., that $D = Z$ is a field.

Proof. (a) Recall that a divison ring is a unital ring where every nonzero element has a multiplicative inverse. Let D be a finite divison ring, and let Z denote the center of D. Since D is a division ring, D is an additive abelian group. Let $a, b \in Z$.

Since $b^{-1} \in D$, we know $bb^{-1} = b^{-1}b = 1$. Then, letting $c \in D$ be arbitrary, we can observe that

$$(ab^{-1})c = ab^{-1}c \cdot 1 = ab^{-1}cbb^{-1} = ab^{-1}bcb^{-1} = acb^{-1} = acb^{-1} = c(ab^{-1})$$

which follows since a and b commute with all elements of D by containment in Z. Thus $ab^{-1} \in Z$, to which the subgroup criterion guarantees $Z \leq D$, so Z is in particular an additive abelian group itself. The associativity and distributivity endowed to D carry over to Z. Furthermore, note that $1a = a1 = a$ for all $a \in D$, so that $1 \in Z$. Thus Z is a unital ring itself. To show that Z is a field, it suffices to prove that multiplication in Z is commutative and every element has a multiplicative inverse. So let $a \in Z$. Then we know $a^{-1} \in D$. In particular, if $b \in D$, then

$$(a^{-1})b = a^{-1}b \cdot 1 = a^{-1}baa^{-1} = a^{-1}aba^{-1} = 1 \cdot ba^{-1} = b(a^{-1})$$

and therefore $a^{-1} \in Z$ holds as well; hence Z is closed under multiplicative inverses. Next, let $a, b \in Z$. Then since a and b commute with all elements of D by construction, and $a, b \in Z \subseteq D$, we know $ab = ba$; hence multiplication in Z is commutative.

Now we show that the prime subfield of Z is $\mathbb{F}_p$ for some prime p. This fact is clear to see for if this were not the case, then $\mathbb{Q}$ would be the prime subfield of Z, necessarily implying $\mathbb{Q} \subseteq Z$. But $Z \subseteq D$ and $|D| < \infty$ by assumption. Since $\mathbb{Q}$ is infinite, we have our contradiction. Thus $\mathbb{F}_p \subseteq Z$.

Assume $Z = \mathbb{F}_q$. Since Z is a ring contained in D, it is a subring of D. In particular, the multiplicative identity of Z is the same as that of D, and so D has a natural Z-module structure. Since Z is a field, this makes D into an $\mathbb{F}_q$-vector space. Since D is finite, it has a finite basis, say of cardinality n. In this case $|D| = q^n$ must follow, since there are q choices for each coefficient of each of the n basis vectors.

(b) Take any $x \in D^\times = D \setminus \{0\}$. The set $D^\times$ is a multiplicative abelian group. Let D_x denote the set of elements of D that commute with x. We prove D_x is a divison ring. Note $D_x \subseteq D$. To show that D_x is a subring of D, it suffices to show that D_x is non-empty, closed under subtraction, and closed under multiplication. Note that $1 \in D$ commutes with all elements of D automatically, and so $1 \in D_x$, to which $D_x \neq \varnothing$. Also $0 \in D_x$ since $0x = x0 = 0$. Now let $a, b \in D_x$. Then

$$(a - b)x = ax - bx = xa - xb = x(a - b)$$

$$(ab)x = a(bx) = a(xb) = (ax)b = (xa)b = x(ab)$$

and so indeed D_x is closed under both operations, making D_x a subring of D; in particular, D_x is a unital ring with $1 \neq 0$. Now let $a \in D_x$ such that $a \neq 0$. Tnen

$$a^{-1}x = a^{-1}x \cdot 1 = a^{-1}xaa^{-1} = a^{-1}axa^{-1} = 1 \cdot xa^{-1} = xa^{-1}$$

and hence $a^{-1} \in D_x$ follows. Therefore D_x is a division ring. Furthermore, if $b \in Z$, then b commutes with all elements of D by construction of Z, and so in particular b commutes with x. This proves $x \in D_x$, and so $Z \subseteq D_x$ holds generally.

Since D_x is a subring of D, the additive group D_x is a subgroup of the additive group D. In part (a) we showed that $|D| = q^n$ for some $n \in \mathbb{Z}^+$. By Lagrange's Theorem, the order of D_x must divide q^n, forcing $|D_x| = q^m$ for some integer m dividing n.

If we add the restriction that there is some $x \in D$ such that $x \notin Z$, then there exists some element of D for which x does not commute. This implies the strict inequality $|D_x| < |D|$, and so it must be the case that $m < n$.

(c) Consider the group $D^\times = D \setminus \{0\}$. In part (b) we showed $|D| = q^n$ for some n. It then follows that $|D^\times| = q^n - 1$. Let $x_1, \ldots, x_r$ denote the representatives of the distinct conjugacy classes of $D^\times$ not contained in $Z(D^\times)$, the center of $D^\times$. Then Theorem 4.7, the class equation, permits us to write that

$$|D^\times| = |Z(D^\times)| + \sum_{i=1}^{r} |D^\times : C_{D^\times}(x_i)|$$

The center of the group $D^\times$ is the set $Z(D^\times) = Z \setminus \{0\}$, where Z is the center of the ring D as before. In part (a) we saw $|Z| = q$, which given the above implies that $|Z(D^\times)| = q - 1$. In part (b), we showed that the cardinality of the set of elements of D that commuted with a particular element of $D^\times$ was q^m for some integer m dividing n. These sets, which we denoted D_x, satisfy $D_x \setminus \{0\} = C_{D^\times}(x)$ for the specific $x \in D^\times$, they are equal to the centralizers of x in $D^\times$, implying $|C_{D^\times}(x)| = q^m - 1$. In particular, for each $i = 1, \ldots, r$ we have $|C_{D^\times}(x_i)| = q^{m_i} - 1$ for some $m_i < n$ since each $x_i \notin Z(D^\times)$ by assumption. Therefore

$$q^n - 1 = (q-1) + \sum_{i=1}^{r} \frac{q^n - 1}{|C_{D^\times}(x_i)|} = (q-1) + \sum_{i=1}^{r} \frac{q^n - 1}{q^{m_i} - 1}$$

is what our class equation becomes upon substituting the values derived above.

(d) We know that the index of a subgroup is always a positive integer. In particular, this means that the quantity $(q^n - 1)/(q^{m_i} - 1)$ seen above in the class equation is an integer, for it is the index of $C_{D^\times}(x_i)$ in $D^\times$ for each representative $x_1, \ldots, x_r$. This implies that $(q^{m_i} - 1) \mid (q^n - 1)$. In Exercise 13.5.4, [[DF-13.5-4]], we showed that $q^{m_i} - 1$ divides $q^n - 1$ if and only if m_i divides n. Therefore $m_i \mid n$ for each $i = 1, \ldots, r$. This gives us the relation $\mu_{m_i} \subseteq \mu_n$, a relation between the group of roots of unity.

Recall that the roots of $x^n - 1$ and x^{m_i} are exactly the nth and m_ith roots of unity, respectively. In particular, we have

$$x^n - 1 = \prod_{\zeta \in \mu_n} (x - \zeta) \quad \text{and} \quad x^{m_i} - 1 = \prod_{\zeta \in \mu_{m_i} \subseteq \mu_n} (x - \zeta)$$

However then, taking the quotient of the two polynomials above, this implies

$$\frac{x^n - 1}{x^{m_i} - 1} = \prod_{\zeta \in \mu_n \setminus \mu_{m_i}} (x - \zeta)$$

so that this quotient is equal to the product of the linear factors $x - \zeta$, where ζ is an nth root of unity that is not an m_ith root of unity. Consider the nth cyclotomic polynomial $\Phi_n(x)$. Recall the definition

$$\Phi_n(x) = \prod_{\zeta \text{ primitive } \in \mu_n} (x - \zeta)$$

i.e., $\Phi_n(x)$ is the polynomial whose roots are the primitive nth roots of unity. Thus, in order to show that $\Phi_n(x)$ divides $(x^n - 1)/(x^{m_i} - 1)$, we need only prove that no primitive nth roots of unity are contained in μ_{m_i}, the m_ith roots of unity. But this is clear for if some $\zeta \in \mu_{m_i}$ was a primitive nth root of unity then it would generate μ_n, so that $\mu_n \subseteq \mu_{m_i}$, implying that $\mu_n = \mu_{m_i}$. This would imply $n = m_i$, which is a contradiction for $m_i < n$. Thus $\Phi_n(x)$ divides $(x^n - 1)/(x^{m_i} - 1)$.

The above implies that for $x = q$, we obtain $\Phi_n(q)$ divides $(q^n - 1)/(q^{m_i} - 1)$ for each $i = 1, \ldots, r$, as desired.

(e) From part (c), we can manipulate the class equation as follows

$$q^n - 1 - \sum_{i=1}^{r} \frac{q^n - 1}{q^{m_i} - 1} = q - 1$$

In part (d) we showed that $\Phi_n(q)$ divides $(q^n - 1)/(q^{m_i} - 1)$ for each $i = 1, \ldots, r$. In particular, $\Phi_n(q)$ must divide the sum $\sum_{i=1}^{r} (q^n - 1)/(q^{m_i} - 1)$. Since $\Phi_n(q)$ trivially divides $q^n - 1$, this implies that the entire left hand side of the above equation is divisible by $\Phi_n(q)$. But this means that $\Phi_n(q)$ divides $q - 1$, the right hand side of the above equatuon. Recall the definition

$$\Phi_n(q) = \prod_{\zeta \text{ primitive } \in \mu_n} (q - \zeta)$$

and so indeed the above quantity divides $q - 1$. Recall that the modulus of a complex number is its distance from the origin. Now note that, since 1 and q are positive real numbers, we have the relation

$$q - 1 = |q| - |1| \leq |q - \zeta|$$

and furthermore if $\zeta \neq 1$, then $q - 1 < |q - \zeta|$ holds. Since this inequality holds for all primitive nth roots of unity $\zeta \in \mu_n$, we know that

$$q - 1 < \prod_{\zeta \text{ primitive } \in \mu_n} |q - \zeta| = |\prod_{\zeta \text{ primitive } \in \mu_n} (q - \zeta)| = |\Phi_n(q)|$$

But since $\Phi_n(q)$ is a real number, we know $|\Phi_n(q)| = \Phi_n(q)$, and so we are left with $q - 1 < \Phi_n(q)$. However since $\Phi_n(q)$ divides $q - 1$, this implies $\Phi_n(q) = q - 1$. In general $\Phi_1(x) = x - 1$. Since $\Phi_1(q) = q - 1$, this means that $n = 1$.

Since $n = 1$, this implies that $|D| = q^n = q$. Since $|Z| = q$ was assumed, and $Z \subseteq D$, this suffices to show that $Z = D$. In other words, D is a field itself. ■

Exercise 13.6.14

Exercise 13.6.15

Exercise 13.6.16

Exercise 13.6.17

※ Galois Theory

14.1 Basic Definitions

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

Proof. (a) Let $K = F(\alpha_1, \ldots, \alpha_n)$. Note that any $\beta \in K$ may be written in the form $\beta = a_1\alpha_1 + \cdots + a_n\alpha_n$ for some $a_1, \ldots, a_n \in F$. Now if $\sigma \in \mathrm{Aut}(K/F)$, then $\sigma(\beta) = a_1\sigma(\alpha_1) + \cdots + a_n\sigma(\alpha_n)$, so that the automorphism σ is completely determined by its value on each of the α_i, i.e., by $\sigma(\alpha_1), \ldots, \sigma(\alpha_n)$. In particular, if σ is an automorphism which fixes K, then $\sigma(\beta) = \beta$ for all $\beta \in K$, and so as we saw before each of $\sigma(\alpha_i) = \alpha_i$ for all $i \in \{1, \ldots, n\}$, so that the generators for K are fixed as well.

(b) Let G be such a subgroup of $\mathrm{Gal}(K/F)$ such that $G = \langle \sigma_1, \ldots, \sigma_n \rangle$. Suppose that the subfield E/F is fixed by G. This means $\sigma(\beta) = \beta$ for all $\beta \in E$ and $\sigma \in G$. Since each $\sigma \in G$ may be written in terms of the generators σ_i, it follows trivially that the σ_i must also fix E. Conversely, if E/F is fixed by the generators $\sigma_1, \ldots, \sigma_n$, then it is trivially fixed by the subgroup G. ■

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

Proof. Let $a + bi$ and $c + di$ be arbitrary elements of $\mathbb{C}$. We can easily find that

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

$$= (a + c) - (b + d)i$$

$$= a - bi + c - di$$

$$= \tau(a + bi) + \tau(c + di)$$

and so addition is preserved. For multiplication, we find that

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

$$= (ac - bd) - (ad + bc)i$$

$$= ac - bd - adi - bci$$

$$= ac - adi - bci + bdi^2$$
$$= (a - bi)(c - di)$$
$$= \tau(a + bi)\tau(c + di)$$

and so indeed τ is a homomorphism of the ring $\mathbb{C}$ to itself. For injectivity, simply note that $a + bi \in \ker \tau$ if and only if $a - bi = 0$, so that $a = bi$ and hence $a = b = 0$. For surjectivity, if $a + bi \in \mathbb{C}$ then $\tau(a - bi) = a + bi$ in the natural way. Hence τ is an isomorphism of $\mathbb{C}$ with itself, and hence an automorphism. ■

Exercise 14.1.3 Determine the fixed field of complex conjugation on $\mathbb{C}$.

Proof. Note that an element $a + bi \in \mathbb{C}$ is fixed under complex conjugation if and only if $a + bi = a - bi$, which is equivalent to $b = -b$, so that $b = 0$ is forced. In particular, the fixed field of $\mathbb{C}$ under complex conjugation is contained in $\mathbb{R}$. Conversely, it is easy to see that any real number is fixed under complex conjugation, so that in fact the fixed field of complex conjugation is $\mathbb{R}$ itself. ■

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

Proof. Assume, for contradiction, that they were isomorphic, so that there exists some isomorphism $\sigma : \mathbb{Q}(\sqrt{2}) \longrightarrow \mathbb{Q}(\sqrt{3})$ between them. We know that $(\sqrt{2})^2 = 2$ in $\mathbb{Q}(\sqrt{2})$. Since $\sigma(0) = 0$ and $\sigma(1) = 1$, i.e., the additive and multplicative identities are preserved by the automorphism, we require that

$$\sigma(2) = \sigma(1 + 1) = \sigma(1) + \sigma(1) = 1 + 1 = 2$$

hold. Similarly, we require that the relation

$$\sigma(\sqrt{2})^2 = 2$$

hold in $\mathbb{Q}(\sqrt{3})$. Since $\sigma(\sqrt{2}) \in \mathbb{Q}(\sqrt{3})$, we may let $\sigma(\sqrt{2}) = a + b\sqrt{3}$ for some $a, b \in \mathbb{Q}$. Then

$$(a + b\sqrt{3})^2 = a^2 + 2ab\sqrt{3} + 3b^2 = 2$$

must hold true. Thus we require $2ab = 0$ and $a^2 + 3b^2 = 2$. We are forced to take $b = 0$, for if not then $a^2 + 3 > 2$. Since $b = 0$, we now require $a^2 = 2$. However, since we assumed $a \in \mathbb{Q}$, this is a contradiction, for $a = \pm\sqrt{2} \notin \mathbb{Q}$. Therefore no such isomoprhism σ can exist, and $\mathbb{Q}(\sqrt{2}) \ncong \mathbb{Q}(\sqrt{3})$. ■

Exercise 14.1.5 Determine the automorphisms of the extension $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})$ explicitly.

Proof. An automorphism σ of the extension $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})$ must fix $\mathbb{Q}$ and $\sqrt{2}$, while sending the generator $\sqrt[4]{2}$ elsewhere, but maintaing the relation $(\sqrt[4]{2})^2 = \sqrt{2}$. It is clear that the only options for sending $\sqrt[4]{2}$ elsewhere become $\sqrt[4]{2} \mapsto \sqrt[4]{2}$, the identity, or $\sqrt[4]{2} \mapsto -\sqrt[4]{2}$, which maintains the relation $(-\sqrt[4]{2})^2 = \sqrt{2}$ from the generator. We cannot send $\sqrt[4]{2}$ elsewhere, say to $\sqrt[4]{8}$, since if this were the case, then since we have the relation $(\sqrt[4]{8})^2 = 2\sqrt{2}$,. we would require that $\sigma(\sqrt[4]{8})^2 = \sigma(2\sqrt{2})$ under the automorphism. Since $\sqrt{2}$ is fixed by σ, this means that

$$2\sqrt{2} = \sigma(\sqrt[4]{8})^2 = (\sqrt[4]{2})^2 = \sqrt{2}$$

which is clearly a contradiction. In a similar way, we cannot send $\sqrt[4]{2} \mapsto -\sqrt[4]{8}$. Thus the automorphisms of the extension $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})$ are the identity automorphism and that sending $\sqrt[4]{2} \mapsto -\sqrt[4]{2}$. ∎

Exercise 14.1.6

Exercise 14.1.7 This exercise determines $\mathrm{Aut}(\mathbb{R}/\mathbb{Q})$.
(a) Prove that any $\sigma \in \mathrm{Aut}(\mathbb{R}/\mathbb{Q})$ takes squares to squares and takes positive reals to positive reals. Conclude that $a < b$ implies $\sigma a < \sigma b$ for every $a, b \in \mathbb{R}$.
(b) Prove that $-\frac{1}{m} < a - b < \frac{1}{m}$ implies $-\frac{1}{m} < \sigma a - \sigma b < \frac{1}{m}$ for every positive integer m. Conclude that σ is a continuous map on $\mathbb{R}$.
(c) Prove that any continuous map on $\mathbb{R}$ which is the identity on $\mathbb{Q}$ is the identity map, hence $\mathrm{Aut}(\mathbb{R}/\mathbb{Q}) = 1$.

Proof. (a) Suppose we have a square $x \in \mathbb{R}$, say with $x = y^2$ for some $y \in \mathbb{R}$. Then we have that $\sigma(x) = \sigma(y^2) = \sigma(y)^2$ by properties of the automorphism σ, so that $\sigma(x)$ is also a square in $\mathbb{R}$. Thus squares are sent to squares under σ.

It is clear that $\sigma(0) = 0$. Now suppose x is a positive real number. Then $x = (\sqrt{x})^2$ is a squrae, and so by the above $\sigma(x)$ is also a square. Thus there exists $y \in \mathbb{R}$ such that $\sigma(x) = y^2$, which implies that $\sqrt{\sigma(x)} = y$, hence that $\sigma(x) > 0$, so that $\sigma(x)$ is also a positive real number.

Note that $a < b$ is equivalent to $0 < b - a$, so that $b - a$ is a positive real number, which by the above lets us write that $0 < \sigma(b) - \sigma(a)$, so that $\sigma(a) < \sigma(b)$ holds.

(b) Now let $m \in \mathbb{Z}^+$ be arbitrary and suppose that

$$-\frac{1}{m} < a - b < \frac{1}{m}$$

holds true. Since $\sigma \in \mathrm{Aut}(\mathbb{R}/\mathbb{Q})$, we know that $\sigma(1/m) = 1/m$, since $1/m \in \mathbb{Q}$, and hence by part (a) above our assumption yields

$$-\frac{1}{m} < \sigma(a) - \sigma(b) < \frac{1}{m}$$

Equivalently, for any $\epsilon > 0$, the assumption that $|a-b| < \delta$ implies $|\sigma(a)-\sigma(b)| < \epsilon$, where here we have set $\delta = \epsilon$; i.e., the map σ is a continuous map in the sense of the ϵ-δ definition of continuity.

(c) Suppose f is a continuous function on $\mathbb{R}$ which is the identity on $\mathbb{Q}$. Recall that any real number is the limit of a sequence of rational numbers, and that continuous functions preserve limits. In particular, if $(a_n) \to x$ then $(\sigma(a_n)) = (a_n) \to \sigma(x) = x$. Thus $\sigma(x) = x$ for all real numbers x. Since in part (b) we showed that any $\sigma \in \mathrm{Aut}(\mathbb{R}/\mathbb{Q})$ is a continuous function on $\mathbb{R}$ which fixes $\mathbb{Q}$, it thus follows that $\sigma = \mathrm{id}$, the identity. Hence $\mathrm{Aut}(\mathbb{R}/\mathbb{Q}) = 1$, as desired. ■

Exercise 14.1.8

Exercise 14.1.9

Exercise 14.1.10 Let K be an extension of the field F. Let $\varphi : K \to K'$ be an isomorphism of K with a field K' which maps F to the subfield F' of K'. Prove that the map $\sigma \mapsto \varphi\sigma\varphi^{-1}$ defines a group isomorphism $\mathrm{Aut}(K/F) \xrightarrow{\sim} \mathrm{Aut}(K'/F')$.

Proof. Let K/F and K'/F' be field extensions, and suppose $\varphi : K \to K'$ is an isomorphism such that $\varphi(F) = F'$. It is clear that the mapping

$$\mathrm{Aut}(K/F) \to \mathrm{Aut}(K'/F')$$

$$\sigma \mapsto \varphi\sigma\varphi^{-1}$$

is a group homomorphism. To see this, note that if $\sigma, \tau \in \mathrm{Aut}(K/F)$ then

$$\varphi\sigma\tau\varphi^{-1} = \varphi\sigma\mathrm{id}\tau\varphi^{-1} = \varphi\sigma(\varphi^{-1}\varphi)\tau\varphi^{-1} = (\varphi\sigma\varphi^{-1})(\varphi\tau\varphi^{-1})$$

which is valid given that φ was assumed an isomorphism, and so has an inverse, and thus $\varphi\varphi^{-1} = \mathrm{id}$ holds true. We can also see that $\varphi\sigma\varphi^{-1}$ is an automorphism of K' which fixes F', as we have

$$\varphi\sigma\varphi^{-1}(F') = \varphi(\sigma(\varphi^{-1}(F'))) = \varphi(\sigma(F)) = \varphi(F) = F'$$

which follows since $\varphi(F) = F'$ was assumed, and by definition σ is an automorphism of K which fixes F, so that $\sigma(F) = F$.

Given what we have discussed above, to show that this mapping is an isomorphism of groups, we need to show that it is injective and surjective. For injectivity, note that if $\varphi\sigma\varphi^{-1} = \mathrm{id}_{K'}$ then we may apply φ to the right and obtain $\varphi\sigma = \varphi$, and now applying φ^{-1} on the left yields $\sigma = \varphi^{-1}\varphi = \mathrm{id}_K$. For surjectivity, if $\tau \in \mathrm{Aut}(K'/F')$ then clearly

$$\varphi^{-1}\tau\varphi \mapsto \varphi(\varphi^{-1}\tau\varphi)\varphi^{-1} = \mathrm{id}\tau\mathrm{id} = \tau$$

and indeed $\varphi^{-1}\tau\varphi \in \mathrm{Aut}(K/F)$ is a valid element. In particular, the mapping described above is a bijection, and hence an isomorphism of groups, as desired. ■

14.2 The Fundamental Theorem of Galois Theory

14.3 Finite Fields

14.4 Composite Extensions and Simple Extensions

14.5 Cyclotomic Extensions and Abelian Extensions over $\mathbb{Q}$

14.6 Galois Groups of Polynomials

14.7 Solvable and Radical Extensions: Insolvability of the Quintic

14.8 Computation of Galois Groups over $\mathbb{Q}$

14.9 Transcendental Extensions, Inseperable Extensions, and Infinite Galois Groups

❈ Commutative Rings and Algebraic Geometry

15.1 Noetherian Rings and Affine Algebraic Sets

Exercise 15.1.1 Prove the converse to Hilbert's Basis Theorem: if the polynomial ring $R[x]$ is Noetherian, then R is Noetherian.

Proof. Suppose $R[x]$ is Noetherian. Consider the map $\varphi : R[x] \to R$ defined by $\varphi(r) = r$ for all $r \in R$ and $\varphi(x) = 0$. For $f, g \in R[x]$ we may observe that

$$\varphi(f(x) + g(x)) = \varphi((f + g)(x)) = (f + g)(0) = f(0) + g(0) = \varphi(f(x)) + \varphi(g(x))$$

$$\varphi(f(x)g(x)) = \varphi((fg)(x)) = (fg)(0) = f(0)g(0) = \varphi(f(x))\varphi(g(x))$$

whence φ is ring homomorphism. Note that if $r \in R$ then $f(x) = r \in R[x]$ maps to r trivially under φ, so that φ is surjective, i.e., $\varphi(R[x]) = R$. Since the homomorphic image of a Noetherian ring is Noetherian, we have that R is Noetherian, as desired. ■

Exercise 15.1.2

Exercise 15.1.3

Exercise 15.1.4

Exercise 15.1.5 (*Fitting's Lemma*) Suppose M is a Noetherian R-module and $\varphi : M \to M$ is an R-module endomorphism of M. Prove that $\ker(\varphi^n) \cap \operatorname{im}(\varphi^n) = 0$ for n sufficiently large. Show that if φ is surjective, then φ is an isomorphism. [Observe that $\ker(\varphi) \subseteq \ker(\varphi^2) \subseteq \ldots$.]

Proof. Let M be a Noetherian R-module and take an endomorphism $\varphi : M \to M$. Since $x \in \ker(\varphi)$ means $\varphi(x) = 0$, we clearly have $\varphi^2(x) = 0$, and hence $x \in \ker(\varphi^2)$. Continuing, we find that $\ker(\varphi) \subseteq \ker(\varphi^2) \subseteq \cdots$ is an ascending chain of R-submodules of M, which must stabilize since M is Noetherian, say $\ker(\varphi^{N'}) = \ker(\varphi^n)$ for all $n \geq N'$. Similarly, we can find that $\operatorname{im}(\varphi) \subseteq \operatorname{im}(\varphi^2) \subseteq \cdots$ is an ascending chain of R-submodules of M, and hence we have that $\operatorname{im}(\varphi^{N''}) = \operatorname{im}(\varphi^m)$ for all $n \geq N''$.

Now set $N = \max\{N', N''\}$. Suppose $x \in \ker(\varphi^N) \cap \operatorname{im}(\varphi^N)$. Then $\varphi^N(x) = 0$ and there exists $y \in M$ for which $\varphi^N(y) = x$. We may observe that

$$\varphi^{2N}(y) = \varphi^N(\varphi^N(y)) = \varphi^N(x) = 0$$

and since $2N > N > N'$ we also know $\ker(\varphi^{2N}) = \ker(\varphi^N)$. Thus $y \in \ker(\varphi^N)$ must hold, which means $\varphi^N(y) = 0$. However we already stated that $\varphi^N(y) = x$ and so we require $x = 0$. Hence we conclude that $\ker(\varphi^N) \cap \operatorname{im}(\varphi^N = 0$.

Now if we assume that $\varphi : M \to M$ is surjective, then $\text{im}(\varphi) = M$, and in particular we have $\text{im}(\varphi^n) = M$ for all $n \geq 1$. From our above work, there exists sufficiently large $N \in \mathbb{N}$ for which we have

$$\ker(\varphi^N) \cap \text{im}(\varphi^N) = \ker(\varphi^N) \cap M = 0$$

and hence $\ker(\varphi^N) = 0$ is required since $\ker(\varphi^N)$ is a submodule of M, and thus contained in M. However note that $\ker(\varphi) \subseteq \ker(\varphi^N)$ was assumed, and hence $\ker(\varphi) = 0$ is also required; hence φ is injective, and thus an isomorphism. ■

Exercise 15.1.6 Suppose that $0 \to M' \to M \to M'' \to 0$ is an exact sequence of R-modules. Prove that M is a Noetherian R-module if and only if M' and M'' are Noetherian R-modules.

Proof. Take some such short exact sequence

$$0 \longrightarrow M' \xrightarrow{\phi} M \xrightarrow{\psi} M'' \longrightarrow 0$$

Suppose first that M is a Noetherian R-module. If $M_1' \subseteq M_2' \subseteq \cdots$ is an ascending chain of R-submodules of M' then $\phi(M_1') \subseteq \phi(M_2') \subseteq \cdots$ is an ascending chain of R-submodules of M. By the A.C.C. on submodules of M, this chain terminates, so that $\phi(M_n') = \phi(M_N')$ for all $n \geq N$ for some fixed $N \in \mathbb{Z}^+$. By the exactness of the sequence, we know ϕ is an injective R-module homomorphism, and hence that $M_n' = M_N'$ for all $n \geq N$. Thus the original chain of R-submodules of M' terminates, hence M' is Noetherian as an R-module.

Likewise, if we take an ascending chain of R-submodules of M'', say $M_1'' \subseteq M_2'' \subseteq \cdots$, then since the sequence above is exact we have ψ is a surjection, and hence that $M/M' \cong M''$ as R-modules, to which the R-submodules of M'' correspond bijectively with the R-submodules of M containing M'. Thus for each i we have $M_i'' = M_i/M'$ for some R-submodule M_i of M, and so we have an ascending chain of R-submodules of M, $M_1 \subseteq M_2 \subseteq \cdots$, which must terminate since M is a Noetherian R-module. Thus $M_n = M_N$ for all $n \geq N$ for some fixed $N \in \mathbb{Z}^+$, and thus

$$M_n'' = M_n/M' = M_N/M' = M_N''$$

holds for all $n \geq N$ as well; thus the original chain of R-submodules of M'' terminates, and hence M'' is also a Noetherian R-module.

Now we prove the converse. That is, suppose M' and M'' are both Noetherian R-modules. To prove that M is a Noetherian R-module, it suffices to show that every R-submodule of M is finitely generated (see Theorem 1 in Section 12.1). So let N be an R-submodule of M. We have an R-module homomorphism

$$\psi|_N : N \to M''$$

So we have that $\ker(\psi|_N)$ is an R-submodule of M' and $\operatorname{im}(\psi|_N)$ is an R-submodule of M'', and both are finitely generated since they are submodules of Noetherian modules. Since we have $N/\ker(\psi|_N) \cong \operatorname{im}(\psi|_N)$, we refer to Exercise 10.3.7 to write that N is finitely generated. Since N was an arbitrary submodule of M, this proves M is a Noetherian R-module, and completes the proof. ∎

Exercise 15.1.7 Prove that submodules, quotient modules, and finite direct sums of Noetherian R-modules are again Noetherian R-modules.

Proof. Let M be a Noetherian submodule. If N is any R-submodule of M, then we have a short exact sequence

$$0 \to N \to M \to M/N \to 0$$

given by the inclusion and natural projection R-module homomorphisms. Since M is Noetherian, Exercise 15.1.6 shows that N and M/N are Noetherian R-modules. Thus any submodule of a Noetherian module is Noetherian, and likewise any quotient module, for such a quotient module is of the form M/N for some submodule N of M.

We now consider finite direct sums. We use induction to prove the desired result. The case for $n = 1$ is trivial, so suppose that the result holds in the $(n-1)$th case. If $M_1, \ldots, M_n$ are Noetherian R-modules, then we have a short exact sequence

$$0 \to \bigoplus_{i=1}^{n-1} M_i \to \bigoplus_{i=1}^{n} M_i \to M_n \to 0$$

given by inclusion and then projection. Since M_n (by assumption) is a Noetherian R-module, and likewise since $\bigoplus_{i=1}^{n-1} M_i$ is a Noetherian R-module (by inductive hypothesis), Exercise 15.1.6 shows that $\bigoplus_{i=1}^{n} M_i$ is a Noetherian R-module. ∎

Exercise 15.1.8. If R is a Noetherian ring, prove that M is a Noetherian R-module if and only if M is a finitely generated R-module. (Thus any submodule of a finitely generated module over a Noetherian ring is also finitely generated.)

Proof. Let R be a Noetherian ring, and M an R-module. If we suppose that M is a Noetherian R-module, then by Theorem 1 in Section 12.1 we know any R-submodule of M is finitely generated; since $M \subseteq M$ trivially, this applies to M, giving one direction.

Conversely, suppose that M is a finitely generated R-module, say with $M = (m_1, \ldots, m_n)$. We have the obvious isomorphism of R-modules:

$$M \cong \bigoplus_{i=1}^{n} Rm_i$$

We aim to show that Rm_i is a Noetherian R-module for each i. To do this, note that via the surjective (obvious) R-module homomorphism

$$\phi : R \to Rm_i$$

$$r \mapsto rm_i$$

we have kernel equal to the annihilator of Rm_i in R, and so an isomorphism:

$$R/\mathrm{Ann}_R(Rm_i) \cong Rm_i$$

Any ascending chain of submodules of $R/\mathrm{Ann}_R(Rm_i)$ corresponds to an ascending chain of ideals of R (which are the same as submodules of R when considering R as an R-module over itself) which contain $\mathrm{Ann}_R(Rm_i)$. Such a chain of ideals must terminate since R is a Noetherian, and so the chain of submodules terminates in $R/\mathrm{Ann}_R(Rm_i)$, hence $R/\mathrm{Ann}_R(Rm_i)$ is a Noetherian module, whence Rm_i is a Noetherian R-module.

Now since M is the finite direct sum of Noetherian R-modules, we conclude by Exercise 15.1.7 that M is a Noetherian R-module. ∎

Exercise 15.1.9. For k a field show that any subring of the polynomial ring $k[x]$ containing k is Noetherian. Given an example to show such subrings need not be U.F.D.s. [If $k \subset R \subseteq k[x]$ and $y \in R \setminus k$ show that $k[x]$ is a finitely generated $k[y]$-module; then use the previous two exercises. For the second, consider $k[x^2, x^3]$.]

Proof. TBD. ∎

Exercise 15.1.10.

Exercise 15.1.11. Suppose R is a commutative ring in which all prime ideals are finitely generated. This exercise proves that R is Noetherian.
(a) Prove that if the collection of ideals of R that are not finitely generated is nonempty, then it contains a maximal element I, and that R/I is a Noetherian ring.
(b) Prove that there are finitely generated ideals J_1 and J_2 containing I with $J_1J_2 \subseteq I$ and that J_1J_2 is finitely generated. [Observe that I is not a prime ideal.]
(c) Prove that I/J_1J_2 is a finitely generated R/I-submodule of J_1/J_1J_2. [Use Exercise 8.]
(d) Show that (c) implies the contradiction that I would be finitely generated over R and deduce that R is Noetherian.

Proof. (a) Let Σ denote the set of all ideals of R that are not finitely generated. Order Σ by inclusion. Suppose $\Sigma \neq \varnothing$. Let $\{I_\alpha\}_\alpha$ be a chain of elements of Σ. We know that $\sum_\alpha I_\alpha$ is an ideal of R and moreover that $\sum_\alpha I_\alpha$ is not finitely generated. Since $\sum_\alpha I_\alpha$ contains all I_α in the chain and lies in the chain, it is an upper bound, hence by Zorn's lemma the set Σ has a maximal element, call it I.

We claim that R/I is a Noetherian ring. Recall that any ideal of the quotient ring R/I is of the form J/I for an ideal J of R containing I. To show that R/I is Noetherian, we show that any ideal is finitely generated. So assume, for contradiction, that we have some non-finitely generated ideal J/I of R/I. We know then that J is a non-finitely generated ideal of R, for if not then the images of the generators for J in the quotient J/I would generate J/I, a contradiction. But since J is not finitely generated we have $J \in \Sigma$, and since $I \subseteq J$, we have a contradiction to the maximality of I in Σ. Hence it follows that J/I is finitely generated, hence that R/I is a Noetherian ring.

(b) In the exercise we are assuming that all prime ideals of R are finitely generated, and so we know that I is not a prime ideal of R. Thus, by definition, there must exist $x, y \in R$ such that $xy \in I$ with neither x nor y lies in I. Let $J_1 = I + (x)$ and $J_2 = I + (y)$.

Since $I \subseteq J_1$ and $I \subseteq J_2$, we know that J_1 and J_2 are finitely generated ideals of R, for if this were not the case then both would belong to Σ, which would contradict the maximality of I in Σ.

We also have the following containment:

$$J_1J_2 = (I + (x))(I + (y)) = I^2 + (y)I + (x)I + (xy) \subseteq I$$

since we are assuming $xy \in I$ holds.

Lastly, observe also that J_1J_2 is finitely generated, for we know that both J_1 and J_2 are finitely generated, so taking all possible products of generators for J_1 and J_2 would give a (finite) set of generators for J_1J_2.

(c) Since $J_1J_2 \subseteq I$ by part (b), we can refer to the third isomorphism theorem for rings to write

$$R/I \cong \frac{R/J_1J_2}{I/J_1J_2}$$

Since J_1/J_1J_2 is an ideal of R/J_1J_2, we can consider it is an R/J_1J_2-module, and hence also as an $(R/J_1J_2)/(I/J_1J_2)$-module, hence as an R/I-module by the isomorphism we found above. Moreover, J_1/J_1J_2 is finitely generated over R/I since both J_1 and J_1J_2 are finitely generated over R. But R/I is a Noetherian ring by part (a), and since Exercise 15.1.8 proves that submodules of finitely generated modules over Noetherian rings are finitely generated, we have that I/J_1J_2 is a finitely generated

R/I-submodule of J_1/J_1J_2.

(d) We show how part (c) gives a contradiction to I being non-finitely generated over R.

From part (c) we know that I/J_1J_2 is finitely generated as an R/I-module, hence also as an R-module (we have $\pi : R \to R/I$ which can be used to extend the action of R/I on I/J_1J_2). In part (b) we showed that J_1J_2 is finitely generated as an R-module, and so by Exercise 10.3.7 we know that I is finitely generated as an R-module. But I is an ideal of R, and so must too be finitely generated as an ideal of R, which is a contradiction.

Thus the set Σ from part (a) cannot be non-empty, and since Σ is the set of all non-finitely generated ideals of R, it follows that all ideals of R are finitely generated, which is what we aimed to prove. ■

Exercise 15.1.12.

Exercise 15.1.13. Verify properties (1) to (10) of the maps $\mathcal{Z}$ and $\mathcal{I}$.

Proof. (1) If $S \subseteq T \subseteq k[x_1, \ldots, x_n]$ then if $p \in \mathcal{Z}(T)$ we know that $f(p) = 0$ for all $f \in T$, and hence all $f \in S \subseteq T$, and hence $p \in \mathcal{Z}(S)$, giving $\mathcal{Z}(T) \subseteq \mathcal{Z}(S)$.

(2) Suppose $S \subseteq k[x_1, \ldots, x_n]$. Let $I = (S)$ be the ideal generated by S. If we take $p \in \mathcal{Z}(S)$ then $f(p) = 0$ for all $f \in S$, and hence any linear combination of elements of S, which means p is a zero for every element of I; hence $\mathcal{Z}(S) \subseteq \mathcal{Z}(I)$. The reverse inclusion is obvious, for clearly $S \subseteq I$ and from (1) we have $\mathcal{Z}(I) \subseteq \mathcal{Z}(S)$.

(3) If $p \in \mathcal{Z}(S) \cap \mathcal{Z}(T)$ then $f(p) = 0$ for all $f \in S$ and $f \in T$, and hence any $f \in S \cup T$ satisfies $f(p) = 0$ since f lies in either one or both of S and T, giving $p \in \mathcal{Z}(S \cup T)$. For the reverse containment, note that if $p \in \mathcal{Z}(S \cup T)$ then p is a zero for any $f \in S$ or $f \in T$ or $f \in S \cap T$, and hence $p \in \mathcal{Z}(S) \cap \mathcal{Z}(T)$, to which $\mathcal{Z}(S \cup T) = \mathcal{Z}(S) \cap \mathcal{Z}(T)$. A simple induction proves this for the general case of an arbitrary collection of subsets, using the above as a base case.

(4) Let I and J be ideals in $k[x_1, \ldots, x_n]$. Suppose $p \in \mathcal{Z}(I) \cup \mathcal{Z}(J)$. If $f \in IJ$ then $f = gh$ for some $g \in I$ and $h \in J$, and hence $f(p) = g(p)h(p) = 0$ since p must either vanish on every element of I (and hence on g) or every element of J (hence on h), or every element in $I \cap J$. Thus $p \in \mathcal{Z}(IJ)$ holds, giving $\mathcal{Z}(I) \cup \mathcal{Z}(J) \subseteq \mathcal{Z}(IJ)$.

Conversely, assume $p \in \mathcal{Z}(IJ)$. Since every $f \in IJ$ may be written $f = gh$ for $g \in I$ and $h \in J$, since we have $f(p) = 0$ it follows that either $g(p) = 0$ or $h(p) = 0$ or

$g(p) = h(p) = 0$ simultaneously. In particular, $p \in \mathcal{Z}(I) \cup \mathcal{Z}(J)$, giving the reverse containment.

(5) The zero polynomial takes every $p \in \mathbb{A}^n$ to 0, and hence $\mathcal{Z}(0) = \mathbb{A}^n$. The constant polynomial 1 takes every element of $\mathbb{A}^n$ to 1, and hence has no zeros, and hence $\mathcal{Z}(1) = \varnothing$.

(6) If $A \subseteq B \subseteq \mathbb{A}^n$ and we take some $f \in \mathcal{I}(B)$, then $f(p) = 0$ for all $p \in B$ and hence all $p \in A \subseteq B$, to which $f \in \mathcal{I}(A)$, giving $\mathcal{I}(B) \subseteq \mathcal{I}(A)$.

(7) Suppose $f \in \mathcal{I}(A \cup B)$. Then $f(p) = 0$ for all $p \in A$ and $f(q) = 0$ for all $q \in B$ since we have $A, B \subseteq A \cup B$; hence $f \in \mathcal{I}(A)$ and $f \in \mathcal{I}(B)$ to which $f \in \mathcal{I}(A) \cap \mathcal{I}(B)$. If, conversely, we assume that $f \in \mathcal{I}(A) \cap \mathcal{I}(B)$ then if $p \in A \cup B$ either $p \in A$ or $p \in B$ or $p \in A \cap B$, and in any case we have $f(p) = 0$, to which $f \in \mathcal{I}(A \cup B)$.

(8) Note that $1 \in \mathcal{I}(\varnothing)$ vacuously holds, and hence $(1) = k[x_1, \ldots, x_n] = \mathcal{I}(\varnothing)$. Now suppose k is infinite. Each element of $k[x_1, \ldots, x_n]$ has only finitely many zeroes except 0. Hence $\mathcal{I}(\mathbb{A}^n) = 0$.

(9) Suppose $A \subseteq \mathbb{A}^n$. If $p \in A$ then for any $f \in \mathcal{Z}(A)$ we have $f(p) = 0$, and hence $p \in \mathcal{Z}(\mathcal{I}(A))$, giving $A \subseteq \mathcal{Z}(\mathcal{I}(A))$. If I is an ideal of $k[x_1, \ldots, x_n]$ then for any $f \in I$ we know that $f(p) = 0$ for all $p \in \mathcal{Z}(I)$ by construction, and hence $f \in \mathcal{I}(\mathcal{Z}(I))$, giving $I \subseteq \mathcal{I}(\mathcal{Z}(I))$.

(10) Consider $\mathcal{Z}(I) \subseteq \mathbb{A}^n$. From (9) above we have $\mathcal{Z}(I) \subseteq \mathcal{Z}(\mathcal{I}(\mathcal{Z}(I)))$. Take any $p \in \mathcal{Z}(\mathcal{I}(\mathcal{Z}(I)))$. Then $f(p) = 0$ for all $f \in \mathcal{I}(\mathcal{Z}(I))$, and hence $p \in \mathcal{Z}(I)$ by construction, giving the reverse inclusion: $\mathcal{Z}(I) = \mathcal{Z}(\mathcal{I}(\mathcal{Z}(I)))$. The other set equality is shown in a similar manner, just a stringing together of definitions. ■

Exercise 15.1.14 Show that the affine algebraic sets in $\mathbb{A}^1$ over any field k are $\varnothing$, k, and finite subsets of k.

Proof. We note that $\varnothing = \mathcal{Z}(1)$, where 1 is the constant polynomial with coefficient 1 in $k[\mathbb{A}^1] = k[x]$. Also we have $\mathbb{A}^1 = \mathcal{Z}(0)$, where 0 is the zero polynomial, with all points as roots. In particular, both $\varnothing$ and $\mathbb{A}^1$ are affine algebraic sets.

Now, if $V \subseteq \mathbb{A}^1$ is an affine algebraic set, then there is a subset $S \subseteq k$ for which $V = \mathcal{Z}(S)$. Note that the coordinate ring $k[x]$ is a PID, and hence the ideal generated by S is $(S) = (f)$ for some $f \in k[x]$. In particular, $V = \mathcal{Z}(f)$ is the set of zeros of the polynomial f, whence finite and less than or equal to the degree of

f. ■

Exercise 15.1.15 If $k = \mathbb{F}_2$ and $V = \{(0,0),(1,1)\} \subset \mathbb{A}^2$, show that $\mathcal{I}(V)$ is the product ideal $\mathfrak{m}_1\mathfrak{m}_2$ where $\mathfrak{m}_1 = (x, y)$ and $\mathfrak{m}_2 = (x-1, y-1)$.

Proof. Note that $\mathbb{F}_2[x,y]/(x,y) \cong \mathbb{F}_2$ via the obvious evaluation ring homomorphism; since $\mathbb{F}_2$ is a field, we have $\mathfrak{m}_1 = (x,y)$ a maximal ideal of $\mathbb{F}_2[x,y]$. Also, $\mathbb{F}_2[x,y]/(x-1,y-1) \cong \mathbb{F}_2$ follows similarly, so that $\mathfrak{m}_2 = (x-1,y-1)$ is maximal.

We have the obvious containments $\mathfrak{m}_1 \subseteq \mathcal{I}((0,0))$ and $\mathfrak{m}_2 \subseteq \mathcal{I}((1,1))$. Furthermore, since both $\mathfrak{m}_1$ and $\mathfrak{m}_2$ are maximal, and $\mathcal{I}((0,0)), \mathcal{I}((1,1)) \neq \mathbb{F}_2[x,y]$, we have that $\mathcal{I}((0,0)) = \mathfrak{m}_1$ and $\mathcal{I}((1,1)) = \mathfrak{m}_2$.

With this information in mind, observe that

$$\mathcal{I}(V) = \mathcal{I}(\{(0,0)\} \cup \{(1,1)\}\} = \mathcal{I}((0,0)) \cap \mathcal{I}((1,1)) = \mathfrak{m}_1 \cap \mathfrak{m}_2$$

Now, since $\mathfrak{m}_1 + \mathfrak{m}_2 = \mathbb{F}_2[x,y]$, i.e., $\mathfrak{m}_1$ and $\mathfrak{m}_2$ are comaximal, Exercise 7.3.34(d) asserts that $\mathfrak{m}_1 \cap \mathfrak{m}_2 = \mathfrak{m}_1\mathfrak{m}_2$. Therefore $\mathcal{I}(V) = \mathfrak{m}_1\mathfrak{m}_2$, as desired. ■

Exercise 15.1.16 Suppose that V is a finite algebraic set in $\mathbb{A}^n$. If V has m points, prove that $k[V]$ is isomorphic as a k-algebra to k^m. [Use the Chinese Remainder Theorem.]

Proof. Let $V = \{a_1, \ldots, a_m\}$ be an algebraic set in $\mathbb{A}^n$. We can see immediately that

$$\mathcal{I}(V) = \mathcal{I}(\bigcup_{i=1}^{m} a_i) = \bigcap_{i=1}^{m} \mathcal{I}(a_i)$$

for instance from Exercise 15.1.13. We make a quick remark. For each $i \in \{1, \ldots, m\}$ we have a surjective ring homomorphism

$$\varphi_i : k[x_1, \ldots, x_n] \longrightarrow k$$

$$f \longmapsto f(a_i)$$

with $\ker(\varphi_i) = \mathcal{I}(a_i)$. As such we have $k[x_1, \ldots, x_n]/\mathcal{I}(a_i) \cong k$, and since k is a field this is equivalent to $\mathcal{I}(a_i)$ being a maximal ideal of $k[x_1, \ldots, x_n]$.

We also trivially have that $\mathcal{I}(a_i) + \mathcal{I}(a_j) = k[x_1, \ldots, x_n]$ for all $i \neq j$, i.e., each of the ideals are comaximal, a fact which follows easily.

Now we have maximal ideals $\mathcal{I}(a_1), \ldots, \mathcal{I}(a_m)$ of $k[x_1, \ldots, x_n]$ with $\mathcal{I}(a_i)$ and $\mathcal{I}(a_j)$ comaximal for all $i \neq j$, and so by the Chinese Remainder Theorem, Theorem 7.17, we have

$$\frac{k[x_1, \ldots, x_n]}{\bigcap_{i=1}^{m} \mathcal{I}(a_i)} \cong \prod_{i=1}^{m} \frac{k[x_1, \ldots, x_n]}{\mathcal{I}(a_i)} \cong \prod_{i=1}^{m} k \cong k^m$$

where the second isomorphism follows by pplying the evaluation at a_i ring homomorphism to each of the components in the direct product. Now, from our initial work, we have $\mathcal{I}(V) = \bigcap_{i=1}^m \mathcal{I}(a_i)$ and hence

$$k[V] = \frac{k[x_1, \ldots, x_n]}{\mathcal{I}(V)} \cong k^m$$

which was exactly the desired statement. ∎

Exercise 15.1.17 If k is a finite field show that every subset of $\mathbb{A}^n$ is an affine algebraic set.

Proof. We have $\mathcal{Z}(0) = \mathbb{A}_k^n$ and $\mathcal{Z}(1) = \varnothing$ and so $\varnothing$ and $\mathbb{A}_k^n$ are affine algebraic sets. Now take any subset $X \subseteq \mathbb{A}_k^n$. Since k is finite, we know that $|\mathbb{A}_k^n| = |k|^n$ is finite, and hence X is finite as well; hence we may write $X = \bigcup_{a \in X}\{a\}$. Note that for each $a \in X$ we have $a = (a_1, \ldots, a_n)$ and so $\mathcal{Z}(x_1 - a_1, \ldots, x_n - a_n) = \{a\}$ holds. In particular, each $\{a\}$ is an affine algebraic set, and since X is the union of finitely many such affine algebraic sets, it too must be affine algebraic. ∎

Exercise 15.1.18

Exercise 15.1.19

Exercise 15.1.20 If f and g are irreducible polynomials in $k[x, y]$ that are not associates (do not divide each other), show that $\mathcal{Z}((f, g))$ is either $\varnothing$ or a finite set in $\mathbb{A}^2$. [If $(f, g) \neq (1)$, show (f, g) contains a nonzero polynomial in $k[x]$ (and similarly a nonzero polynomial in $k[y]$) by letting $R = k[x]$, $F = k(x)$, and applying Gauss's Lemma to show f and g are relatively prime in $F[y]$.]

Proof. This is not stated in the problem, but here I assume that k is an algebraically closed field. Let $f, g \in k[x, y]$ be irreducible polynomials with $f \nmid g$ and $g \nmid f$. Considering $k[x, y] = k[y][x]$ as a subring of $k(y)[x]$, we prove that f (and so also g) is irreducible in $k(y)[x]$. So suppose this is not the case; that is, there exists $h_1, h_2 \in k[y]$ and $f_1, f_2 \in k[x, y]$ such that

$$f(x, y) = \frac{f_1(x, y)}{h_1(y)} \cdot \frac{f_2(x, y)}{h_2(y)}$$

Multiplying across by $h_1(y)h_2(y)$ yields

$$h_1(y)h_2(y)f(x, y) = f_1(x, y)f_2(x, y)$$

and now evaluating the above equation at $y = 1$ gives:

$$h_1(1)h_2(1)f(x, 1) = f_1(x, 1)f_2(x, 1) \iff f(x, 1) = \frac{1}{h_1(1)h_2(1)} \cdot f_1(x, 1)f_2(x, 1)$$

In particular, since $f(x,y)$ was assumed irreducible in $k[x,y] = k[y][x]$, it must also be irreducible in $k[x]$, and hence the above is a contradiction, as we have written f as the product of distinct polynomials in $k[x]$. In particular both f and g remain irreducible in the larger ring $k(y)[x]$. Now we show that f and g are relatively prime in this larger ring. So once again, assume not; that is, assume there exists $h_1 \in k[x,y]$ and $h_2 \in k[y]$ such that

$$f(x,y) = \frac{h_1(x,y)}{h_2(y)} g(x,y)$$

Once more, we multiply both sides of the above by h_2 and then evaluate at $y = 1$ to obtain:

$$h_2(1)f(x,1) = h_1(x,1)g(x,1) \iff f(x,1) = \frac{1}{h_2(1)} h_1(x,1)g(x,1)$$

And indeed, once more, the above is a decomposition of f into distinct polynomials in $k[x]$, which is a contradiction for we assumed f to be irreducible in $k[x,y]$, hence in $k[x]$. Thus f and g are relatively prime in $k(y)[x]$. Thus there exists polynomials $h_1, h_1' \in k[x,y]$ and $h_2, h_2' \in k[y]$ such that:

$$\frac{h_1(x,y)}{h_2(y)} f(x,y) + \frac{h_1'(x,y)}{h_2'(y)} g(x,y) = 1$$

Now clearing denominators by multiplying both sides of the above equation by $h_2 h_2'$ yields

$$h_2'(y)h_1(x,y)f(x,y) + h_2(y)h_1'(x,y)g(x,y) = h_2(y)h_2'(y)$$

Now if $(a,b) \in \mathcal{Z}((f,g))$ is a common zero of both f and g, then the left hand side of the above equation becomes 0, and hence we require that:

$$h_2(b)h_2'(b) = 0$$

Thus b must be a zero of either h_2 or h_2' in $k[y]$, and hence there are only finitely many possible choices for b. However, note that if (a,b) is a solution to $f(x,y)$ then a must be a zero of $f(x,b)$; note that $f(x,b) \neq 0$ for then $y - b$ would divide f in $k(y)[x]$, a contradiction to the irreducibility of f. Thus there are only finitely many such a since there are only finitely many zeros of $f(x,b)$ in $k[x]$. In particular, there are only finitely many such solutions (a,b) which f and g can share; hence $\mathcal{Z}((f,g)) = \mathcal{Z}(f) \cap \mathcal{Z}(g)$ is a finite subset of $\mathbb{A}^2$, or is empty of f and g share no common zeroes. ■

Exercise 15.1.21

Exercise 15.1.22

Exercise 15.1.23

Exercise 15.1.24

Exercise 15.1.25

Exercise 15.1.26

Exercise 15.1.27 Suppose $\varphi : V \longrightarrow W$ is a morphism of affine algebraic sets. If W' is an affine algebraic subset of W prove that the preimage $V' = \varphi^{-1}(W')$ of W' in V is an affine algebraic subset of V. If $W' = \mathcal{Z}(I)$ show that $V' = \mathcal{Z}(\widetilde{\varphi}(I))$ for the corresponding morphism $\widetilde{\varphi} : k[W] \longrightarrow k[V]$.

Proof. Let $\varphi : \mathbb{A}^m \longrightarrow \mathbb{A}^n$ be a morphism of affine algebraic sets. We show that the preimage of an affine algebraic set is an affine algebraic set. So take $W = \mathcal{Z}(I) \subset \mathbb{A}^m$ for some ideal I of $k[x_1, \ldots, x_n]$.

We have an associated homomorphism of k-algebras given by $\widetilde{\varphi} : k[\mathbb{A}^n] \longrightarrow k[\mathbb{A}^m]$ defined by $\widetilde{\varphi}(f) = f \circ \varphi$. We claim that $\varphi^{-1}(W) = \mathcal{Z}(\widetilde{\varphi}(I))$.

Note first that if $(a_1, \ldots, a_m) \in \varphi^{-1}(W) = \varphi^{-1}(\mathcal{Z}(I))$, then $\varphi((a_1, \ldots, a_m)) \in \mathcal{Z}(I)$, and if we let $\varphi(a_1, \ldots, a_m) = (\varphi_1(a_1, \ldots, a_m), \ldots, \varphi_n(a_1, \ldots, a_m))$, we have that

$$(g \circ \varphi)(a_1, \ldots, a_m)) = g((\varphi_1(a_1, \ldots, a_m), \ldots, \varphi_n(a_1, \ldots, a_m))) = 0$$

for all $g \in I$. In particular, $(a_1, \ldots, a_m) \in \mathcal{Z}(\widetilde{\varphi}(I))$ holds, since $g \circ \varphi = \widetilde{\varphi}(g)$; hence we have shown $\varphi^{-1}(W) \subseteq \mathcal{Z}(\widetilde{\varphi}(I))$.

For the reverse containment, assume $(a_1, \ldots, a_m) \in \mathcal{Z}(\widetilde{\varphi}(I))$. Now, for any $f \in I$, we have $\widetilde{\varphi}(f) = f \circ \varphi \in \widetilde{\varphi}(I)$, and hence $(f \circ \varphi)(a_1, \ldots, a_m) = 0$, which means that $\varphi(a_1, \ldots, a_m)$ is a zero of f, and since $f \in I$ was arbitrary, $\varphi(a_1, \ldots, a_m)$ is a zero of all elements of I, and hence $\varphi(a_1, \ldots, a_m) \in \mathcal{Z}(I) = W$. Thus $(a_1, \ldots, a_m) \in \varphi^{-1}(W)$ holds true; this proves $\mathcal{Z}(\widetilde{\varphi}(I)) \subseteq \varphi^{-1}(W)$; hence equality.

In particular, we have shown that $\varphi^{-1}(W) = \mathcal{Z}(\widetilde{\varphi}(I))$, and since $\widetilde{\varphi}(I)$ is an ideal of $k[x_1, \ldots, x_m] = k[\mathbb{A}^m]$, this proves that $\varphi^{-1}(W)$ is an affine algebraic set in $\mathbb{A}^m$, as desired. ■

Exercise 15.1.28

Exercise 15.1.29 If $R = \mathbb{Z}$ and $M = \mathbb{Z}/n\mathbb{Z}$, show that $\text{Ass}_R(M)$ consists of the prime ideals (p) for the prime divisors of n.

Proof. Every prime ideal of $\mathbb{Z}$ is in the form $p\mathbb{Z}$ for some prime p. Suppose then that we have $p\mathbb{Z} \in \text{Ass}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z})$ for such a prime. Then there exists $\overline{m} \in \mathbb{Z}/n\mathbb{Z}$ such that $\text{Ann}(\overline{m}) = p\mathbb{Z}$. This is equivalent to $\mathbb{Z}/n\mathbb{Z}$ containing $\mathbb{Z}$-submodule isomorphic to $\mathbb{Z}/p\mathbb{Z}$, and so by Lagrange's Theorem (which holds since $\mathbb{Z}$-modules are abelian groups) we have $p \mid n$.

Conversely, if $p \mid n$ then there is a unique subgroup (m) of $\mathbb{Z}/n\mathbb{Z}$ which is isomorphic to $\mathbb{Z}/p\mathbb{Z}$. The subgroup (m) is a $\mathbb{Z}$-submodule of $\mathbb{Z}/n\mathbb{Z}$, and hence $\mathrm{Ann}(\overline{m}) = p\mathbb{Z}$ which gives $p\mathbb{Z} \in \mathrm{Ass}_R(\mathbb{Z}/n\mathbb{Z})$. ∎

Exercise 15.1.30 If M is the union of some collection of submodules M_i, prove that $\mathrm{Ass}_R(M)$ is the union of the collection $\mathrm{Ass}_R(M_i)$.

Proof. Let $M = \bigcup_{i \in \mathcal{I}} M_i$ where $\mathcal{I}$ is an index set and each M_i is an R-submodule of M. We aim to show that

$$\mathrm{Ass}_R(M) = \bigcup_{i \in \mathcal{I}} \mathrm{Ass}_R(M_i)$$

If $M = 0$ then the result trivially holds, so assume $M \neq 0$. Now suppose $P \in \mathrm{Ass}_R(M)$. Then there exists some $m \in M \setminus \{0\}$ for which $\mathrm{Ann}(m) = P$. Since $M = \bigcup_{i \in \mathcal{I}} M_i$, it follows that $m \in M_i$ for at least one $i \in \mathcal{I}$, and hence that $P \in \mathrm{Ass}_R(M_i) \subseteq \bigcup_{i \in \mathcal{I}} \mathrm{Ass}_R(M_i)$. This proves one containment.

For the reverse, suppose $P \in \bigcup_{i \in \mathcal{I}} \mathrm{Ass}_R(M_i)$. Then, in particular, there is at least one $i \in \mathcal{I}$ for which $P \in \mathrm{Ass}_R(M_i)$, and hence there exists some $m \in M_i$ such that $P = \mathrm{Ann}(m)$. Since $m \in M_i \subseteq M$ trivially holds, we have $P \in \mathrm{Ass}_R(M)$, giving our desired containment and proving the claim. ∎

Exercise 15.1.31 Suppose that $\mathrm{Ann}(m) = P$, i.e., that $Rm \cong R/P$. Prove that if $0 \neq m' \in Rm$ then $\mathrm{Ann}(m') = P$. Deduce that $\mathrm{Ass}_R(R/P) = \{P\}$. [Observe that R/P is an integral domain.]

Proof. Let M be an R-module and take $m \in M$. Suppose $\mathrm{Ann}(m) = P$ where P is a prime ideal of R. This is equivalent to $Rm \cong R/P$, and since P is prime, we must have that Rm is an integral domain (since it is isomorphic to an integral domain).

Now choose $m' \in Rm \setminus \{0\}$. Then $m' = sm$ for some $s \in R \setminus \{0\}$. We show that Rm and Rm' are isomorphic as rings. Consider the map $\varphi : Rm \longrightarrow Rm'$ defined by $\varphi(rm) = rm'$ for all $r \in R$. We verify preservation of the additive and multiplicative structure: for all $r, t \in R$ we have

$$\varphi(rm + tm) = \varphi((r+t)m) = (r+t)m' = rm' + tm' = \varphi(rm) + \varphi(tm)$$

$$\varphi((rm)(tm)) = \varphi((rt)m) = (rt)m' = (rm')(tm') = \varphi(rm)\varphi(tm)$$

and hence φ is indeed a ring homomorphism. Given $x \in Rm'$ we have $x = rm'$ for some $r \in R$, and hence $\varphi(rm) = x$, whence φ is surjective. Now assume $x \in \ker\varphi$. Then $x = rm$ for some $r \in R$ and $\varphi(x) = \varphi(rm) = rm' = 0$. Now, recalling that $m' = sm$ we see

$$rm' = r(sm) = (rs)m = (rm)(sm) = 0$$

Since Rm is an integral domain, either $rm = 0$ or $sm = 0$. If $rm = 0$ then $x = rm = 0$ and so $\ker \varphi = 0$. Otherwise, $m' = sm = 0$, a contradiction since we assumed $m' \neq 0$. Thus we conclude φ is injective; hence bijective and so $Rm \cong Rm'$. Since $Rm \cong R/P$ we naturally have that $Rm' \cong R/P$, equivalently that $\text{Ann}(m') = P$, proving the claim.

Note that $1+P \neq 0+P$ in the quotient ring R/P, since if $1 \in P$ then $P = R$, a contradiction to P being a prime ideal. With this in mind, we claim that $\text{Ann}(1+P) = P$.

If $r \in \text{Ann}(1+P)$ then $r(1+P) = r+P = 0+P$ is required, and hence $r \in P$. Since r was arbitrary we have $\text{Ann}(1+P) \subseteq P$. Conversely, if $p \in P$ then $p(1+P) = p+P = 0+P$ and hence $p \in \text{Ann}(1+P)$, so $P \subseteq \text{Ann}(1+P)$. This proves the claim.

We can easily see that $R(1+P) = R/P$. Thus for any $r+P \in R/P$ such that $r+P \neq 0+P$, we have $\text{Ann}(r+P) = P$ by our work above. In particular, this shows that the only prime associated to P is P itself, i.e., $\text{Ass}_R(R/P) = \{P\}$. ■

Exercise 15.1.32

Exercise 15.1.33 Suppose R is a Noetherian ring and $M \neq 0$ is an R-module. Prove that $\text{Ass}_R(M) \neq \varnothing$. [Use Exercise 32.]

Proof. Let C be the set of all ideals I of R for which $I = \text{Ann}(m)$ for some $m \in M$. Since $M \neq 0$, there exists at least one $m \neq 0$ in M, and $\text{Ann}(m)$ is an ideal of R by Exercise 10.1.9. Hence $C \neq \varnothing$. Any non-empty set of ideals in the Noetherian ring R has a maximal element under set inclusion by Theorem 2. Let P be this maximal element under inclusion, where $P = \text{Ann}(n)$ for an element $n \in M$. From Exercise 15.1.32, we may write that P is a prime ideal of R and hence that $P \in \text{Ass}_R(M)$, to which $\text{Ass}_R(M) \neq \varnothing$. ■

Exercise 15.1.34

Exercise 15.1.35

Exercise 15.1.36

Exercise 15.1.37

Exercise 15.1.38

Exercise 15.1.39

Exercise 15.1.40

Exercise 15.1.41

Exercise 15.1.42

Exercise 15.1.43

Exercise 15.1.44

Exercise 15.1.45

Exercise 15.1.46

Exercise 15.1.47

Exercise 15.1.48

15.2 Radicals and Affine Varieties

Exercise 15.2.1

Exercise 15.2.2 Let I and J be ideals in the ring R. Prove the following statements:
(a) If $I^k \subseteq J$ for some $k \geq 1$ then $\text{rad}(I) \subseteq \text{rad}(J)$.
(b) If $I^k \subseteq J \subseteq I$ for some $k \geq 1$ then $\text{rad}(I) = \text{rad}(J)$.
(c) $\text{rad}(IJ) = \text{rad}(I \cap J) = \text{rad}(I) \cap \text{rad}(J)$.
(d) $\text{rad}(\text{rad}(I)) = \text{rad}(I)$.
(e) $\text{rad}(I) + \text{rad}(J) \subseteq \text{rad}(I + J)$ and $\text{rad}(I + J) = \text{rad}(\text{rad}(I) + \text{rad}(J))$.

Proof. (a) If $I^k \subseteq J$ for some $k \geq 1$ then if $x \in \text{rad}(I)$ we have $x^m \in I$ for some $m \geq 1$, and so $(x^m)^k = x^{mk} \in J$ must hold, to which $x \in \text{rad}(J)$; hence $\text{rad}(I) \subseteq \text{rad}(J)$.

(b) If we go further and assume $I^k \subseteq J \subseteq I$ for some $k \geq 1$, then if $x \in \text{rad}(J)$ we have that $x^m \in J$ for some $m \geq 1$, and hence $x^m \in I$ since $J \subseteq I$; thus $\text{rad}(J) \subseteq \text{rad}(I)$. Combined with part (a) above, this gives us the desired equality.

(c) First, note that if $x \in \text{rad}(IJ)$ then $x^k \in IJ$ for some $k \geq 1$, and since, in general, we have that $IJ \subseteq I \cap J$, this means that $x^k \in I \cap J$ and hence that $x \in \text{rad}(I \cap J)$, giving us that $\text{rad}(IJ) \subseteq \text{rad}(I \cap J)$. Secondly, if we assume $x \in \text{rad}(I \cap J)$ then $x^k \in I \cap J$ for some $k \geq 1$, and in particular $x^k \in I$ and $x^k \in J$, and so $x \in \text{rad}(I)$ and $x \in \text{rad}(J)$, whence $x \in \text{rad}(I) \cap \text{rad}(J)$; hence $\text{rad}(I \cap J) \subseteq \text{rad}(I) \cap \text{rad}(J)$ holds true. Lastly, if we assume that $x \in \text{rad}(I) \cap \text{rad}(J)$ then $x^k \in I$ and $x^m \in J$ for some $k, m \geq 1$. We can easily see that $x^{k+m} = x^k x^m \in IJ$, whence $x \in \text{rad}(IJ)$, and hence $\text{rad}(I) \cap \text{rad}(J) \subseteq \text{rad}(IJ)$. Tracing through the inclusions we have shown proves that the desired equality holds.

(d) If $x \in \text{rad}(\text{rad}(I))$ then $x^k \in \text{rad}(I)$ for some $k \geq 1$, and hence $(x^k)^m \in I$ for some $m \geq 1$ by definition of the radical of an ideal; in particular, $x^{km} \in I$ and so $x \in \text{rad}(I)$; thus $\text{rad}(\text{rad}(I)) \subseteq \text{rad}(I)$. Now, since in general an ideal is contained in its radical, we trivially have that $\text{rad}(I) \subseteq \text{rad}(\text{rad}(I))$, whence the equality.

(e) If $x \in \text{rad}(I) + \text{rad}(J)$ then $x = y + z$ for soem $y \in \text{rad}(I)$ and $z \in \text{rad}(J)$.

By definition of the radical, there exists $k, m \geq 1$ for which $y^k \in I$ and $z^m \in J$. Since R is a commutative ring with 1, the binomial theorem holds, see Exercise 7.3.25, and so setting $n = m + k$ gives:

$$x^n = (y+z)^n = \sum_{i=0}^{n} \binom{n}{i} y^i z^{n-i} \in I + J$$

Hence $x \in \text{rad}(I+J)$, whence $\text{rad}(I) + \text{rad}(J) \subseteq \text{rad}(I+J)$ holds true.

Now, we claim that $I + J \subseteq \text{rad}(I) + \text{rad}(J)$. This can be seen for if $x \in I + J$ then $x = y + z$ for $y \in I$ and $z \in J$, and clearly then $y \in \text{rad}(I)$ and $z \in \text{rad}(J)$ since in general an ideal is contained in its radical; in particular, $x \in \text{rad}(I) + \text{rad}(J)$, proving the claim. Now from part (a) we have that $\text{rad}(I+J) \subseteq \text{rad}(\text{rad}(I)+\text{rad}(J))$.

This inclusion, combined with that of the previous paragraph, gives us the desired equality of sets. ■

Exercise 15.2.3 Prove that the intersection of two radical ideals is again a radical ideal.

Proof. Suppose I and J are radical ideals of R. Then $I = \text{rad}(I)$ and $J = \text{rad}(J)$ by definition. From Exercise 15.2.2 parts (c) and (d), we may write that

$$\text{rad}(I \cap J) = \text{rad}(I) \cap \text{rad}(J) = I \cap J$$

whence $I \cap J$ is a radical ideal as well. ■

Exercise 15.2.4

Exercise 15.2.5

Exercise 15.2.6 Give an example to show that over a field k that is not algebraically closed the containment $I \subseteq \mathcal{I}(\mathcal{Z}(I))$ can be proper even when I is a radical ideal.

Proof. Take $k = \mathbb{R}$, which is not algebraically closed. Take $I = (x^2+1)$. Note that $x^2 + 1$ is irreducible in $\mathbb{R}[x]$, and hence I is a prime ideal, and hence a radical ideal. Note, however, that $x^2 + 1$ has no zeroes in $\mathbb{R}$, and therefore:

$$\mathcal{I}(\mathcal{Z}(I)) = \mathcal{I}(\varnothing) = \mathbb{R}[x]$$

holds true. Clearly the containment is proper, $I \subset \mathbb{R}[x]$, despite I being a radical ideal. ■

Exercise 15.2.7

Exercise 15.2.8 Suppose the prime ideal P contains the ideal I. Prove that P contains the radical of I.

Proof. If we let I be an ideal and P a prime ideal containing I, we may take some $x \in \text{rad}(I)$ and note that $x^k \in I$ for some $k \geq 1$, and hence $x^k \in P$, and hence either $x \in P$ or $x^{k-1} \in P$. But if $x^{k-1} \in P$ then either $x \in P$ or $x^{k-2} \in P$; continuing in this fashion we eventually obtain that $x \in P$, and so we require that $\text{rad}(I) \subseteq P$. ■

Exercise 15.2.9

Exercise 15.2.10 Prove that for k a finite field the Zariski topology is the same as the discrete topology: every subset is closed (and open).

Proof. Let k be a finite field, and let $A \subseteq \mathbb{A}_k^n$. It is clear that A is finite since k is finite, and so we may write $A = \bigcup_{a \in A} \{a\}$. For each $a \in A$, we have $a = (a_1, \ldots, a_n)$ and hence $\{a\} = \mathcal{Z}(x_1 - a_1, \ldots, x_n - a_n)$ is an algebraic set. Since A is the finite union of algebraic sets, it too must be algebraic. Therefore every subset of $\mathbb{A}_k^n$ is algebraic, and so closed in the Zariski topology on $\mathbb{A}_k^n$. Thus the Zariski topology and the discrete topology on $\mathbb{A}_k^n$ coincide. ■

Exercise 15.2.11 Let V be a variety in $\mathbb{A}^n$ and let U_1 and U_2 be two subsets of $\mathbb{A}^n$ that are open in the Zariski topology. Prove that if $V \cap U_1 \neq \varnothing$ and $V \cap U_2 \neq \varnothing$, then $V \cap U_1 \cap U_2 \neq \varnothing$. Conclude that *any* nonempty open subset of a variety is *everywhere dense* in the Zariski topology (i.e., its closure is all of V).

Proof. We prove this via the contrapositive; so suppose $V \cap U_1 \cap U_2 = \varnothing$, where V is a variety in $\mathbb{A}^n$ and U_1, U_2 open subsets. We may write $U_1 = \mathbb{A}_k^n \setminus \mathcal{Z}(J_1)$ and $U_2 = \mathbb{A}_k^n \setminus \mathcal{Z}(J_2)$ for some ideals J_1 and J_2 of $k[x_1, \ldots, x_n]$. Similarly, we may write $V = \mathcal{Z}(I)$ for some ideal I. Now our assumption translates to:

$$\mathcal{Z}(I) \cap (\mathbb{A}_k^n \setminus \mathcal{Z}(J_1)) \cap (\mathbb{A}_k^n \setminus \mathcal{Z}(J_2)) = \mathcal{Z}(I) \cap (\mathbb{A}_k^n \setminus (\mathcal{Z}(J_1) \cup \mathcal{Z}(J_2))) = \varnothing$$

which means that $V = \mathcal{Z}(I) \subseteq \mathcal{Z}(J_1) \cup \mathcal{Z}(J_2)$. However, if we set $V_1 = V \cap \mathcal{Z}(J_1)$ and $V_2 = V \cap \mathcal{Z}(J_2)$ then $V = V_1 \cup V_2$ holds, where V_1 and V_2 are algebraic sets in V. This is a contradiction, for we assumed that V was a variety, and hence one or both of the V_1 or V_2 is not proper, that is, we may take either $V = V_1$ or $V = V_2$. In particular, this means that either $\mathcal{Z}(I) \subseteq \mathcal{Z}(J_1)$ or $\mathcal{Z}(I) \subseteq \mathcal{Z}(J_2)$ or $\mathcal{Z}(I) \subseteq \mathcal{Z}(J_1) \cap \mathcal{Z}(J_2)$.

In the first case, we have that $\mathcal{Z}(I) \cap (\mathbb{A}_k^n \setminus \mathcal{Z}(J_1)) = \varnothing$, and hence that $V \cap U_1 = \varnothing$. In the second case, a similar process yields $V \cap U_2 = \varnothing$. In the third case, both $V \cap U_1 = \varnothing$ and $V \cap U_2 = \varnothing$ holds true. In any of the above three cases, either one or both of $V \cap U_1 = \varnothing$ or $V \cap U_2 = \varnothing$ holds; note that this is the logical negation of both $V \cap U_1 \neq \varnothing$ and $V \cap U_2 \neq \varnothing$.

Thus we have proved that if $V \cap U_1 \cap U_2 = \varnothing$ then one of $V \cap U_1$ or $V \cap U_2$ or both is empty. The contrapositive of this is the desired statement.

Now suppose U is an open subset of a variety V. Clearly we have that $V \cap U \neq \varnothing$. Let $\overline{U}$ denote the Zariski closure of U in $\mathbb{A}_k^n$, and set $U' = \mathbb{A}^n \setminus \overline{U}$. Since V is, in particular, an algebraic set containing U, we have that $V \cap \overline{U} \neq \varnothing$. Now, if $V \neq \overline{U}$, then $V \cap U' \neq \varnothing$, where U' is an open set. By what we have shown above, we conclude that $V \cap U \cap U' \neq \varnothing$, which is a contradiction, for $U \cap U' = \varnothing$. Hence, we require $V = \overline{U}$, so that the Zariski closure of U in V is V itself. ■

Exercise 15.2.12 Use the fact that nonempty open sets of an affine variety are everywhere dense to prove that an affine variety is connected in the Zariski topology. (A topological space is *connected* if it is not the union of two disjoint, proper, open subsets.)

Proof. Let V be an affine variety. Suppose V is disconnected; that is, $V = U_1 \cup U_2$ where U_1 and U_2 are proper open subsets of V such that $U_1 \cap U_2 = \varnothing$. Then $U_1 \subseteq V \setminus U_2$ and likewise $U_2 \subseteq V \setminus U_1$. Both $V \setminus U_2$ and $V \setminus U_1$ are closed sets in V containing U_1 and U_2, respectively. In particular, the closure of U_1 in V must contain $V \setminus U_2$, and likewise the closure of U_2 in V must contain $V \setminus U_1$; but recall from Exercise 15.2.11 that the open sets U_1 and U_2 are everywhere dense in V, and thus their closures in V are equal to V itself. Hence we obtain that $V \subseteq V \setminus U_1$ and $V \subseteq V \setminus U_2$, and hence $V = V \setminus U_1$ and $V = V \setminus U_2$, to which $U_1 = U_2 = \varnothing$ holds. Since $V \neq \varnothing$, and we assumed $V = U_1 \cup U_2$, this is a contradiction; hence V is connected in the Zariski topology. ■

Exercise 15.2.13

Exercise 15.2.14 Prove that if k is an infinite field, then the varieties in $\mathbb{A}^1$ are the empty set, the whole space, and the one point subsets. What are the varieties in $\mathbb{A}^1$ in the case of a finite field k?

Proof. Let k be an infinite field and consider $\mathbb{A}_k^1$. We have already seen that the algebraic sets in $\mathbb{A}_k^1$ are the finite subsets, in addition to $\mathbb{A}_k^1$ and $\varnothing$. Since k is infinite, so too must be $\mathbb{A}_k^1$; hence $\mathbb{A}_k^1$ cannot be written as a union of proper algebraic sets, since each such proper algebraic set is finite. Thus $\mathbb{A}_k^1$ is irreducible, and hence a variety. Similarly, the algebraic set $\varnothing$ cannot be written as the union of proper algebraic sets in $\varnothing$, since the only such set is $\varnothing$ itself; hence $\varnothing$ is irreducible, hence a variety. Lastly, any finite subset $A \subseteq \mathbb{A}_k^1$ containing more than two points can be written as $\bigcup_{a \in A} \{a\} = A$. Since each $\{a\}$ for $a \in A$ is an irreducible algebraic set, which follows since $\{a\} = \mathcal{Z}(x - a)$, it follows that A is not irreducible. Hence only the one point subsets of $\mathbb{A}_k^1$ are varieties.

Now assume k is finite. Then every subset of $\mathbb{A}_k^1$ is an algebraic set. The only varieties of $\mathbb{A}_k^1$ are $\varnothing$ and the one point subsets, however. This follows for the same reasons as above, but we shall have to alter our argument and provet that $\mathbb{A}_k^1$ is reducible. Indeed, for any $a \in \mathbb{A}_k^1$, we can write $\mathbb{A}_k^1 = (\mathbb{A}_k^1 \setminus \{a\}) \cup \{a\}$, and since $\{a\}$ and $\mathbb{A}_k^1 \setminus \{a\}$ are finite sets, they are algebraic sets, and moreover proper, to which $\mathbb{A}_k^1$ is not irreducible; hence not a variety. ■

Exercise 15.2.15

Exercise 15.2.16

Exercise 15.2.17

Exercise 15.2.18

Exercise 15.2.19

Exercise 15.2.20

Exercise 15.2.21

Exercise 15.2.22

Exercise 15.2.23

Exercise 15.2.24

Exercise 15.2.25

Exercise 15.2.26

Exercise 15.2.27

Exercise 15.2.28

Exercise 15.2.29 Suppose that A and B are ideals with $AB \subseteq Q$ for a primary ideal Q. Prove that if $A \not\subseteq Q$ then $B \subset \operatorname{rad}(Q)$.

Proof. Take any $b \in B$. Since $A \not\subseteq Q$ there exists some $a \in A$ such that $a \notin Q$. Since $AB \subseteq Q$ we know that $ab \in Q$ is required, and since $a \notin Q$ this means that $b \in \operatorname{rad}(Q)$ since Q is a primary ideal. Since b was an arbitrary element of B, this proves that $B \subseteq \operatorname{rad}(Q)$. ■

Exercise 15.2.30 Let Q be a P-primary ideal and suppose A is an ideal not contained in Q. Define $A' = \{r \in R \mid rA \subseteq Q\}$ to be elements of R that when multiplied by elements of A give elements of Q. Prove that A' is a P-primary ideal.

Proof. We first check that A' is an ideal of R. If $x \in A'$ and $r \in R$ then $(rx)a = r(xa) \in Q$ since $xa \in Q$ by assumption, and since Q is an ideal, $rQ \subseteq Q$ holds; hence $rx \in A'$. If $x, y \in A'$ then $(x + y)a = xa + ya \in Q$ since $xa \in Q$ and $ya \in Q$ by assumption, and the ideal A' is closed under addition.

We show that $\operatorname{rad}(A') = P$. To begin, we claim that $A'A \subseteq Q$. To see this, note that if $x \in A'$ and $a \in A$ then $xA \subseteq Q$ and hence $xa \in Q$ holds, proving the claim. Since $A \not\subseteq Q$ by assumption, we refer to Exercise 15.2.29 to write that $A' \subseteq \operatorname{rad}(Q) = P$; hence $\operatorname{rad}(A') \subseteq P$ by Exercise 15.2.2(a). For the reverse inclusion, if $x \in P$ then $x^k \in Q$ for some $k \geq 1$, and hence $x^kA \subseteq Q$ holds by closure under multiplication by ring elements of the ideal Q, to which $x^k \in A'$ and hence $x \in \text{rad}(A')$, giving $P \subseteq \text{rad}(A')$ and thus proving the equality of sets $\text{rad}(A') = P$.

In order to show that A' is a P-primary ideal of R, what remains is to prove that A' is a primary ideal, which we do so now.

We make a preliminary note that $Q \subseteq A'$. This holds since if $z \in Q$ then $zr \in Q$ for all $r \in R$ by closure under multiplication by ring elements in the ideal Q; in particular, we have $za \in Q$ for all $a \in A \subseteq R$, and hence $zA \subseteq Q$ holds true. This means that $z \in A'$, proving $Q \subseteq A'$.

We now move to show that A' is a primary ideal of R. Suppose $xy \in A'$ with $x \notin A'$. Since $x \notin A'$ we know that $xA \nsubseteq Q$; in particular, there exists some element $a \in A$ for which $xa \notin Q$. Since Q is primary and $xya = (xa)y \in Q$ with $xa \notin Q$, this forces $y \in \text{rad}(Q) = P$. As we saw above, $P = \text{rad}(A')$, and so this gives us that A' is a primary ideal. ∎

Exercise 15.2.31. Prove that if Q_1 and Q_2 are are primary ideals belonging to the same prime ideal P, then $Q_1 \cap Q_2$ is a primary ideal belonging to P. Conclude that a finite intersection of P-primary ideals is again P-primary.

Proof. Let Q_1 and Q_2 be P-primary ideals. This means that the radical of both of these ideals is precisely equal to P. Now, from Exercise 15.2.2(c) we know that

$$\text{rad}(Q_1 \cap Q_2) = \text{rad}(Q_1) \cap \text{rad}(Q_2) = P \cap P = P$$

and hence the radical of $Q_1 \cap Q_2$ is P. To prove the desired claim then, it suffices to show that $Q_1 \cap Q_2$ is a primary ideal.

So suppose $xy \in Q_1 \cap Q_2$ with $x \notin Q_1 \cap Q_2$. We want to show that $y \in \text{rad}(Q_1 \cap Q_2) = P$. Since $x \notin Q_1 \cap Q_2$, we know that x must not be contained in at least one, possibly both of, Q_1 or Q_2; there are three cases.

For the first, if $x \notin Q_1$. Since Q_1 is a P-primary ideal, and $xy \in Q_1$ holds, we know $y \in \text{rad}(Q_1) = P$. The second case and third cases are dealt with analogously, again by referring to the definition of each Q_1, Q_2 being P-primary ideals. In any case, we must have $y \in P$, which proves that $Q_1 \cap Q_2$ is P-primary.

Using a simple induction argument we can find that any finite intersection of P-primary ideals is again P-primary. ∎

Exercise 15.2.32. Prove that if Q_1 and Q_2 are primary ideals belonging to the same *maximal* ideal M, then $Q_1 + Q_2$ and $Q_1 Q_2$ are primary ideals belonging to M. Conclude that finite sums and finite products of M-primary ideals are again M-primary.

Proof. TBD. ∎

Exercise 15.2.33. Let $I = (x^2, xy, xz, yz)$ in $k[x, y, z]$. Prove that a primary decomposition of I is $I = (x, y) \cap (x, z) \cap (x, y, z)^2$, determine the isolated and embedded primes of I, and find $\operatorname{rad}(I)$.

Proof. Let $\mathfrak{p}_1 = (x, y)$, $\mathfrak{p}_2 = (x, z)$, and $\mathfrak{m} = (x, y, z)$. We note that since $k[x, y, z]/\mathfrak{p}_1 \cong k[z]$ is an integral domain, we have that $\mathfrak{p}_1$ is a prime ideal of $k[x, y, z]$, hence a $\mathfrak{p}_1$-primary ideal. Similarly, $\mathfrak{p}_2$ is a $\mathfrak{p}_2$-primary ideal. Note also that $\mathfrak{m}$ is a maximal ideal of $k[x, y, z]$ since $k[x, y, z]/\mathfrak{m} \cong k$ is a field; we have that $\mathfrak{m}^2 \subseteq \mathfrak{m}^2 \subseteq \mathfrak{m}$ and so by Proposition 19(5) we have that $\mathfrak{m}^2 = (x, y, z)^2$ is an $\mathfrak{m}$-primary ideal.

We see that $I = (x^2, xy, xz, yz) = \mathfrak{p}_1\mathfrak{p}_2$ holds. We would now like to prove that:

$$I = \mathfrak{p}_1 \cap \mathfrak{p}_2 \cap \mathfrak{m}^2$$

is a minimal primary decomposition of I. We can check directly that

$$\mathfrak{p}_1 \cap \mathfrak{p}_2 = (x, y) \cap (x, z) = (x, yz)$$

$$\mathfrak{p}_1 \cap \mathfrak{m}^2 = (x, y) \cap (x^2, y^2, z^2, xy, xz, yz) = (x^2, y^2, xy, xz, yz)$$

$$\mathfrak{p}_2 \cap \mathfrak{m}^2 = (x, z) \cap (x^2, y^2, z^2, xy, xz, yz) = (x^2, z^2, xy, xz, yz)$$

Indeed, we see that each of $\mathfrak{p}_1 \cap \mathfrak{m}^2 \not\subseteq \mathfrak{p}_2$ and $\mathfrak{p}_2 \cap \mathfrak{m}^2 \not\subseteq \mathfrak{p}_1$ and $\mathfrak{p}_1 \cap \mathfrak{p}_2 \not\subseteq \mathfrak{m}^2$ holds, so no primary ideal contains the intersection of the remaining primary ideals. The associated primes, moreover, are all distinct, for clearly we have $\mathfrak{p}_1 \neq \mathfrak{p}_2$ and $\mathfrak{p}_1 \neq \mathfrak{m}$ and $\mathfrak{p}_2 \neq \mathfrak{m}$. We have:

$$\mathfrak{p}_1 \cap \mathfrak{p}_2 \cap \mathfrak{m}^2 = \mathfrak{p}_1 \cap (\mathfrak{p}_2 \cap \mathfrak{m}^2) = (x, y) \cap (x^2, z^2, xy, xz, yz) = (x^2, xy, xz, yx) = I$$

Thus the primary decomposition for I above is, in fact, minimal.

We now find $\operatorname{rad}(I)$. We know from Exercise 15.2.2(c) that

$$\begin{aligned}
\operatorname{rad}(I) &= \operatorname{rad}(\mathfrak{p}_1 \cap \mathfrak{p}_2 \cap \mathfrak{m}^2) \\
&= \operatorname{rad}(\mathfrak{p}_1) \cap \operatorname{rad}(\mathfrak{p}_2) \cap \operatorname{rad}(\mathfrak{m}^2) \\
&= \mathfrak{p}_1 \cap \mathfrak{p}_2 \cap \mathfrak{m} \\
&= \mathfrak{p}_1 \cap \mathfrak{p}_2
\end{aligned}$$

Where the last line follows from the preivious since $\mathfrak{p}_1 \subseteq \mathfrak{m}$ and $\mathfrak{p}_2 \subseteq \mathfrak{m}$ holds, to which the intersection $\mathfrak{p}_1 \cap \mathfrak{p}_2 \subseteq \mathfrak{m}$ as well; in addition, we can see that $\mathfrak{p}_1 \not\subseteq \mathfrak{p}_2$ since for instance $y \notin \mathfrak{p}_2$, and that $\mathfrak{p}_2 \not\subseteq \mathfrak{p}_1$, since for instance $z \notin \mathfrak{p}_1$. In particular, $\operatorname{rad}(I) = (x, yz)$. The previous two sentences also proves that $\mathfrak{p}_1$ and $\mathfrak{p}_2$ are the isolated primes associated to I and that $\mathfrak{m}$ is an embedded prime associated to I. ∎

Exercise 15.2.34 Suppose $\varphi : R \to S$ is a surjective ring homomorphism. Prove that an ideal Q in R containing the kernel of φ is primary if and only if $\varphi(Q)$ is primary in S, and when this is the case the prime associated to $\varphi(Q)$ is the image of $\varphi(P)$ of the prime P associated to Q.

Proof. Suppose $\varphi : R \to S$ is a surjective ring homomorphism and that Q is an ideal of R such that $\ker\varphi \subseteq Q$. Suppose Q is primary. Take any $a, b \in S$ and suppose $ab \in \varphi(Q)$ with $a \notin \varphi(Q)$. Since φ is surjective, there exists $r, t \in R$ such that $\varphi(r) = a$ and $\varphi(t) = b$. In particular, we have that $\varphi(rt) = \varphi(r)\varphi(t) = ab \in \varphi(Q)$ since φ is a ring homomorphism, and hence $rt \in Q$. Since $a \notin \varphi(Q)$, we know that $\varphi(r) = a \notin \varphi(Q)$, and hence $r \notin Q$. Since Q is primary, and $rt \in Q$, this means that $t^k \in Q$ for some int $k \geq 1$; hence $\varphi(t)^k = \varphi(t^k) \in Q$ holds. By definition, $\varphi(Q)$ is a primary ideal in S.

Now in this case, we would like to show that $\varphi(\text{rad}(Q)) = \text{rad}(\varphi(Q))$. If we have $x \in \varphi(\text{rad}(Q))$ then there exists $r \in \text{rad}(Q)$ for which $\varphi(r) = x$. Since $r \in \text{rad}(Q)$ we know that $r^k \in Q$ for some integer $k \geq 1$; hence $x^k = \varphi(r)^k = \varphi(r^k) \in \varphi(Q)$, which implies that $x \in \text{rad}(\varphi(Q))$, proving $\varphi(\text{rad}(Q)) \subseteq \text{rad}(\varphi(Q))$. For the reverse containment, if $x \in \text{rad}(\varphi(Q))$ then there exists an integer $m \geq 1$ such that $x^m \in \varphi(Q)$; since φ is surjective, there is some $r \in R$ for which $\varphi(r) = x$. Now we can see that $\varphi(r^m) = \varphi(r)^m = x^m \in \varphi(Q)$ implies $r^m \in Q$, and hence that $r \in \text{rad}(Q)$. Thus $x \in \varphi(\text{rad}(Q))$, and so we have shown the equality $\varphi(\text{rad}(Q)) = \text{rad}(\varphi(Q))$. In other words, the prime associated to the primary ideal $\varphi(Q)$ in S is the image $\varphi(P)$ of the prime associated to Q in R, $P = \text{rad}(Q)$. ∎

Exercise 15.2.35

Exercise 15.2.36 Let $I = (xy, x-yz)$ in $k[x, y, z]$. Prove that $(x, z) \cap (y^2, x-yz)$ is a minimal primary decomposition of I. [Consider the ring homomorphism $\varphi : k[x, y, z] \to k[y, z]$ given by mapping x to yz, y to y, and z to z and use the previous exercise.]

Proof. Let $I = (xy, x-yz) \subseteq k[x, y, z]$ and consider the k-algebra homomorphism $\varphi : k[x, y, z] \to k[y, z]$ defined on generators by mapping $x \mapsto yz$, $y \mapsto y$, and $z \mapsto z$. Clearly the mapping φ is a surjective ring homomorphism.

We would like to apply the results of Exercise 15.2.34(b), and so we would like to find a minimal primary decomposition of the ideal:

$$\varphi(I) = \varphi(xy, x-yz) = (y^2 z, yz - yz) = (y^2 z)$$

in $k[y, z]$. It is clear to see that $(y^2 z) = (yz, z) \cap (y^2)$ holds. We prove that this is, in fact, a minimal primary decomposition of $\varphi(I) = (y^2 z)$ in $k[y, z]$.

First, we can see that (yz, z) is a prime ideal of $k[y, z]$ since $k[y, z]/(yz, z) \cong k[y]/(y0) = k[y]$ is an integral domain; hence (yz, z) is primary. To see why (y^2) is a primary ideal of $k[y, z]$, note that if we suppose $ab \in (y^2)$ with $a \notin (y^2)$ then two cases arise: either $a \in (y)$ or $a \notin (y)$. In the first case, since $ab \in (y^2)$ we know that y^2 divides ab, and so we require that y divide b, hence that $b \in (y) = \text{rad}(y^2)$. In the second case, we require that y^2 divide b, and hence that $b \in (y^2) \subseteq \text{rad}(y^2)$. In either case, we have that $b \in \text{rad}(y^2)$; hence (y^2) is a primary ideal.

We find the radicals of the primary ideals (yz, z) and (y^2). We already saw that the radical of (yz, z) is simply (yz, z) (since this ideal is prime). For (y^2), we can use Exercise 15.2.2 to see that:

$$\begin{aligned}
\text{rad}(yz, z) &= \text{rad}((yz) + (z)) \\
&= \text{rad}(yz) \cap \text{rad}(z) \\
&= \text{rad}(y) \cap \text{rad}(z) \cap \text{rad}(z) \\
&= (y) \cap (z) \cap (z) \\
&= (y) \cap (z) \\
&= (yz)
\end{aligned}$$

holds.

We now prove that the primary decomposition $(y^2 z) = (yz, z) \cap (y^2)$ is minimal. Clearly we have that $(y^2) \not\subseteq (yz, z)$, for instance since $y^2 \notin (yz, z)$. Similarly, we see that $(yz, z) \not\subseteq (y^2)$ since $z \notin (y^2)$. The radical ideals of (yz, z) and (y^2) are (yz) and (y), respectively, and clearly these ideals are not equal; hence we conclude that the decomposition is minimal.

Using the above, we may refer to Exercise 15.2.35(b), whose results allow us to write that

$$I = \varphi^{-1}(\varphi(I)) = \varphi^{-1}(y^2 z) = \varphi^{-1}(yz, z) \cap \varphi^{-1}(y^2)$$

is a minimal primary decomposition of I in $k[x, y, z]$. We can find directly that

$$\varphi^{-1}(yz, z) = (x, z)$$

$$\varphi^{-1}(y^2) = (y^2, x - yz)$$

Therefore $I = (x, z) \cap (y^2, x - yz)$ is a minimal primary decomposition of I in $k[x, y, z]$, as desired. ■ ■

Exercise 15.2.37 Prove that a prime ideal P contains the ideal I if and only if P contains one of the associated primes of a minimal primary decomposition of I. [Use Exercise 3 and Exercise 11 in Section 7.4.]

Proof. Let P be a prime ideal and I an ideal. For the first direction, suppose $I \subseteq P$. Let $\bigcap_{i=1}^m Q_i$ be a minimal primary decomposition for I. From Exercise 7.4.11 we know that if $JK \subseteq P$ then either $J \subseteq P$ or $K \subseteq P$ for ideals J and K. Thus, since, in general, we have $JK \subseteq J \cap K$ for ideals, we may write that

$$\prod_{i=1}^{m} Q_i \subseteq \bigcap_{i=1}^{m} Q_i = I \subseteq P$$

and hence that $Q_k \subseteq P$ for some $k \in \{1, \dots, m\}$. Since Q_k is a primary ideal, we know from Proposition 19 that $\text{rad}(Q_k)$ is the unique smallest prime ideal containing Q_k; in particular, we require that $Q_k \subseteq \text{rad}(Q_k) \subseteq P$. Thus P contains the associated prime $\text{rad}(Q_k)$. Conversely, assume that P contains some associated prime $\text{rad}(Q_k)$ of a minimal primary decomposition of I. Then we have:

$$I = \bigcap_{i=1}^{m} Q_i \subseteq Q_k \subseteq \text{rad}(Q_k) \subseteq P$$

so that $I \subseteq P$, whicb is the desired statement. ∎

Exercise 15.2.38 Show that every associated prime ideal for a radical ideal is isolated. [Suppose that $P_2 = \text{rad}(Q_2) \subseteq P_1 = \text{rad}(Q_1)$ in the decomposition of Theorem 21 for the radical ideal I. Show that if $a \in Q_2 \cap \cdots \cap Q_m \subseteq P_2$ then $a^n \in I$ for some $n \geq 1$, conclude that $a \in Q_1$ and derive a contradiction to the minimality of the primary decomposition.]

Proof. Let I be a radical ideal of the Noetherian ring R and suppose $I = \bigcap_{i=1}^{m} Q_i$ is a minimal primary decomposition for I with $\text{rad}(Q_i) = P_i$ for each i. Since $I = \text{rad}(I)$, we know that

$$I = \text{rad}(I) = \text{rad}\left(\bigcap_{i=1}^{m} Q_i\right) = \bigcap_{i=1}^{m} \text{rad}(Q_i) = \bigcap_{i=1}^{m} P_i$$

from Exercise 15.2.2(c). Assume, for contradiction, that I has an associated prime which is embedded. That is, without loss of generality, suppose we have $P_2 = \text{rad}(Q_2) \subseteq \text{rad}(Q_1) = P_1$. We intend to contradict the minimality of the decomposition. To this end, observe that if $x \in \bigcap_{j\neq 1}^{m} Q_j$, then

$$x \in \bigcap_{j\neq 1}^{m} Q_j \subseteq \bigcap_{j\neq 1}^{m} P_{j|} \subseteq P_2 \subseteq P_1$$

Thus $x \in P_i$ for all $i \in \{1, \dots, m\}$ and hence $x \in I$ holds. Thus $x \in Q_i$ for each $i \in \{1, \dots, n\}$ and so in particular $x \in Q_1$. Note, however, that since x was arbitrary this implies

$$\bigcap_{j\neq 1}^{m} Q_j \subseteq Q_1$$

which is a contradiction to the assumption that the primary decomposition for I was minimal; hence no embedded primes exist for I; each associated prime is isolated. ∎

Exercise 15.2.39

Exercise 15.2.40

Exercise 15.2.41

Exercise 15.2.42

Exercise 15.2.43

Exercise 15.2.44

Exercise 15.2.45

Exercise 15.2.46

Exercise 15.2.47

Exercise 15.2.48

Exercise 15.2.49

Exercise 15.2.50

Exercise 15.2.51

Exercise 15.2.52

Exercise 15.2.53

Exercise 15.2.54

15.3 Integral Extensions and Hilbert's Nullstellensatz

Exercise 15.3.1.

Exercise 15.3.2.

Exercise 15.3.3.

Exercise 15.3.4.

Exercise 15.3.5.

Exercise 15.3.6.

Exercise 15.3.7. Let $\mathcal{O}_K$ be the ring of integers in a number field K.
(a) Suppose that every nonzero ideal I of $\mathcal{O}_K$ can be written as the product of powers of prime ideals. Prove that an ideal Q of $\mathcal{O}_K$ is P-primary if and only if $Q = P^m$ for some $m \geq 1$. [Show first that since nonzero primes in $\mathcal{O}_K$ are maximal that $P_1^{m_1} \subseteq P_2^{m_2}$ for distinct nonzero primes P_1, P_2 implies $P_1 = P_2$.]
(b) Suppose that an ideal Q of $\mathcal{O}_K$ is P-primary if and only if $Q = P^m$ for some $m \geq 1$. Assuming all of Theorem 21, prove that every nonzero ideal I of $\mathcal{O}_K$ can be written uniquely as the product of powers of prime ideals. [Prove that $P_1^{m_1}$ and $P_2^{m_2}$ are comaximal ideals if P_1 and P_2 are distinct nonzero prime ideals and use the Chinese Remainder Theorem.]

Proof. (a) Under the assumption in the problem description, suppose Q is a P-primary ideal, where P is a non-zero prime ideal of $\mathcal{O}_K$. Then, under the assumption, we may write

$$Q = \prod_{i=1}^{n} P_i^{\alpha_i},$$

where $P_1, \ldots, P_n$ are distinct non-zero prime ideals of $\mathcal{O}_K$ and the $\alpha_1, \ldots, \alpha_n \geq 1$ are integers. From Exercise 15.2.2(c), we know that

$$P = \operatorname{rad}(Q) = \operatorname{rad}\left(\prod_{i=1}^{n} P_i^{\alpha_i}\right) = \bigcap_{i=1}^{n} \operatorname{rad}(P_i^{\alpha_i}) = \bigcap_{i=1}^{n}\left(\bigcap_{j=1}^{\alpha_i} \operatorname{rad}(P_i)\right) = \bigcap_{i=1}^{n}\left(\bigcap_{j=1}^{\alpha_i} P_i\right) = \bigcap_{i=1}^{m} P_i.$$

Now, from (2) of Theorem 26 in the text, we know that non-zero prime ideals of $\mathcal{O}_K$ are maximal, and so since $P \subseteq P_j$ by the above, and $P, P_j \neq 0$ with both prime, we require that $P = P_j$ for all $j \in \{1, \ldots, n\}$. Thus

$$Q = \prod_{i=1}^{m} P_i^{\alpha_i} = \prod_{i=1}^{m} P^{\alpha_i} = P^m,$$

where $m = \alpha_1 + \cdots + \alpha_n$. Indeed, $m \geq 1$ since by assumption each $\alpha_i \geq 1$; hence one direction is proven. Conversely, if $Q = P^m$ for some $m \geq 1$, then by the same exercise we have $\operatorname{rad}(Q) = \bigcap_{i=1}^{m} \operatorname{rad}(P) = \bigcap_{i=1}^{m} P = P$, and so Q is P-primary.

(b) Now, under the hypothesis of part (a) above, and assuming the results of Theorem 21, let I be a non-zero ideal of $\mathcal{O}_K$. The Primary Decomposition Theorem asserts that there exists a minimal primary decomposition

$$I = \bigcap_{i=1}^{n} Q_i$$

for I (which follows since $\mathcal{O}_K$ is a Noetherian ring by Theorem 29(1)). Each Q_i is P_i-primary for distinct non-zero prime ideals $P_1, \ldots, P_n$ of $\mathcal{O}_K$. By part (a), this implies that $Q_i = P_i^{\alpha_i}$ for some $\alpha_i \geq 1$ for each $i \in \{1, \ldots, n\}$. Hence

$$I = \bigcap_{i=1}^{n} Q_i = \bigcap_{i=1}^{n} P_i^{\alpha_i}.$$

Now, since P_i and P_j for $i \neq j$ are distinct, we claim that $P_i^{\alpha_i}$ and $P_j^{\alpha_j}$ are comaximal. To see why this is the case, let $\beta = \max\{\alpha_i, \alpha_j\}$. Then we claim that

$$(P_i + P_j)^{2\beta} \subseteq P_i^{\alpha_i} + P_j^{\alpha_j}$$

holds. This is because any element of the ideal on the left is a sum of elements of the form

$$(x_1 + y_1)(x_2 + y_2) \cdots (x_{2\beta} + y_{2\beta}),$$

with $x_k \in P_i$ and $y_k \in P_j$ for each $k \in \{1, \ldots, 2\beta\}$. But note that expanding (i.e., multiplying out) each expression above yields an expression with at least β of the x_k or at least β of the y_k. Since β is the larger of α_i and α_j, this proves our claim.

Now, since all non-zero prime ideals in $\mathcal{O}_K$ are maximal, and P_i and P_j are distinct prime ideals, we know that $P_i + P_j = (1)$, and hence by our claim above that

$$(1) = (1)^{2\beta} = (P_i + P_j)^{2\beta} \subseteq P_i^{\alpha_i} + P_j^{\alpha_j},$$

whence $P_i^{\alpha_i} + P_j^{\alpha_j} = (1)$ and so these ideals are comaximal. Now the Chinese Remainder Theorem gives

$$I = \bigcap_{i=1}^{n} P_i^{\alpha_i} = \prod_{i=1}^{n} P_i^{\alpha_i},$$

and so we have written I as a product of powers of prime ideals in $\mathcal{O}_K$. The uniqueness of this factorization is immediate from the uniqueness of the minimal primary decomposition via the Primary Decomposition Theorem applied above.

■

Exercise 15.3.8.

Exercise 15.3.9.

Exercise 15.3.10.

Exercise 15.3.11.

Exercise 15.3.12.

Exercise 15.3.13.

Exercise 15.3.14.

Exercise 15.3.15.

Exercise 15.3.16.

Exercise 15.3.17.

Exercise 15.3.18.

Exercise 15.3.19.

Exercise 15.3.20.

Exercise 15.3.21.

Exercise 15.3.22.

Exercise 15.3.23.

Exercise 15.3.24.

Exercise 15.3.25.

Exercise 15.3.26.

Exercise 15.3.27.

Exercise 15.3.28.

15.4 Localization

Exercise 15.4.1.

Exercise 15.4.2.

Exercise 15.4.3.

Exercise 15.4.4.

Exercise 15.4.5.

Exercise 15.4.6.

Exercise 15.4.7.

Exercise 15.4.8.

Exercise 15.4.9.

Exercise 15.4.10.

Exercise 15.4.11.

Exercise 15.4.12.

Exercise 15.4.13.

Exercise 15.4.14. Suppose $\varphi : M \to N$ is an R-module homomorphism. Prove that φ is injective (respectively, surjective) if and only if the induced R_P-module homomorphism $\varphi : M_P \to N_P$ is injective (respectively, surjective) for every prime ideal P of R (or just for every maximal ideal of R).

Proof. If $\varphi : M \to N$ is an injective R-module homomorphism then we have an exact sequence $0 \to M \to N$; since localization is exact.

$$0 \to M \xrightarrow{\varphi} N$$

If, on the other hand, $\varphi : M \to N$ is surjective, then we have a short exact sequence

$$0 \to \ker \varphi \to M \xrightarrow{\varphi} N \to 0$$

which, once again, upon localizing, gives us an induced short exact sequence

$$0 \to (\ker \varphi)_P \to M_P \xrightarrow{\varphi_P} N_P \to 0$$

Since $(\ker \varphi)_P = \ker(\varphi_P)$, this shows that $\varphi_P : M_P \to N_P$ is surjective.

Conversely, if $\varphi_P : M_P \to N_P$ is injective for all prime ideals P, where φ_P is that induced by $\varphi : M \to N$, then we have an exact sequence

$$0 \to \ker \varphi \to M \to N$$

Since localization is exact,

∎

Exercise 15.4.15.

Exercise 15.4.16.

Exercise 15.4.17. Prove that the R-module A is a flat R-module if and only if A_P is a flat R_P-module for every prime ideal P of R (or just for every maximal ideal of R). [Use Proposition 41, Exercises 14 and 16, and the exactness properties of localization.]

Proof. Suppose A is a flat R-module. Extending scalars via the canonical ring homomorphism $R \longrightarrow R_P$ for any prime ideal P of R, we have that

$$A_P \cong A \otimes_R R_P$$

by Proposition 41. From Exercise 10.5.23, we have that A_P is a flat R_P-module since A is a flat R-module. Thus A_P is a flat R_P-module for all prime ideals P of R.

Clearly if A_P is a flat R_P-module for all prime ideals of R, then $A_\mathfrak{m}$ is a flat $R_\mathfrak{m}$-module for all maximal ideals $\mathfrak{m}$ of R.

Suppose now that $A_\mathfrak{m}$ is a flat $R_\mathfrak{m}$-module for all maximal ideals $\mathfrak{m}$ of R. If we take some short exact sequence of R-modules, say

$$0 \longrightarrow L \longrightarrow M \longrightarrow N \longrightarrow 0$$

then we can localize at each maximal ideal $\mathfrak{m}$ to get a short exact sequence of $R_\mathfrak{m}$-modules

$$0 \longrightarrow L_\mathfrak{m} \longrightarrow M_\mathfrak{m} \longrightarrow N_\mathfrak{m} \longrightarrow 0$$

Since $A_\mathfrak{m}$ is a flat $R_\mathfrak{m}$-module, we can tensor the above short exact sequence to get another short exact sequence

$$\begin{tikzcd}
0 \arrow[r] & A_\mathfrak{m} \otimes_{R_\mathfrak{m}} L_\mathfrak{m} \arrow[r] \arrow[d, "\cong"] & A_\mathfrak{m} \otimes_{R_\mathfrak{m}} M_\mathfrak{m} \arrow[r] \arrow[d, "\cong"] & A_\mathfrak{m} \otimes_{R_\mathfrak{m}} N_\mathfrak{m} \arrow[r] \arrow[d, "\cong"] & 0 \\
0 \arrow[r] & (A \otimes_R L)_\mathfrak{m} \arrow[r] & (A \otimes_R M)_\mathfrak{m} \arrow[r] & (A \otimes_R N)_\mathfrak{m} \arrow[r] & 0
\end{tikzcd}$$

where the isomorphisms going down follow since localization commutes with tensor products, Exercise 15.4.16. The short exact sequence in the bottom row of the above diagram implies that

$$(A \otimes_R L)_\mathfrak{m} \longrightarrow (A \otimes_R M)_\mathfrak{m}$$

is an injection of $R_\mathfrak{m}$-modules for all maximal ideals $\mathfrak{m}$ of R, which by Exercise 15.4.14 implies that

$$A \otimes_R L \longrightarrow A \otimes_R M$$

is an injection of R-modules. In a completely analogous manner, the fact that

$$(A \otimes_R M)_{\mathfrak{m}} \longrightarrow (A \otimes_R N)_{\mathfrak{m}}$$

is surjective for all maximal ideals implies that

$$A \otimes_R M \longrightarrow A \otimes_R N$$

is surjective. Combining these two facts, we have that

$$0 \longrightarrow A \otimes_R L \longrightarrow A \otimes_R M \longrightarrow A \otimes_R N \longrightarrow 0$$

is a short exact sequence of R-modules; in other words, A is a flat R-module, proving the desired statement. ■

Exercise 15.4.18.

Exercise 15.4.19.

Exercise 15.4.20.

Exercise 15.4.21.

Exercise 15.4.22.

Exercise 15.4.23.

Exercise 15.4.24.

Exercise 15.4.25.

Exercise 15.4.26.

Exercise 15.4.27.

Exercise 15.4.28.

Exercise 15.4.29.

Exercise 15.4.30.

Exercise 15.4.31.

Exercise 15.4.32.

Exercise 15.4.33.

Exercise 15.4.34.

Exercise 15.4.35.

Exercise 15.4.36.

Exercise 15.4.37.

Exercise 15.4.38.

Exercise 15.4.39.

Exercise 15.4.40.

15.5 The Prime Spectrum of a Ring

Exercise 15.5.1.

Exercise 15.5.2.

Exercise 15.5.3.

Exercise 15.5.4.

Exercise 15.5.5.

Exercise 15.5.6.

Exercise 15.5.7.

Exercise 15.5.8.

Exercise 15.5.9.

Exercise 15.5.10.

Exercise 15.5.11.

Exercise 15.5.12.

Exercise 15.5.13.

Exercise 15.5.14.

Exercise 15.5.15.

Exercise 15.5.16.

Exercise 15.5.17.

Exercise 15.5.18.

Exercise 15.5.19.

Exercise 15.5.20.

Exercise 15.5.21.

Exercise 15.5.22.

Exercise 15.5.23.

Exercise 15.5.24.

Exercise 15.5.25.

Exercise 15.5.26.

Exercise 15.5.27.

Exercise 15.5.28.

Exercise 15.5.29.

Exercise 15.5.30.

Exercise 15.5.31.

❈ Artinian Rings, Discrete Valuation Rings, and Dedekind Domains

16.1 Artinian Rings

Exercise 16.1.1. Suppose R is an Artinian ring and I is an ideal in R. Prove that R/I is also Artinian.

Proof. Suppose R is an Artinian ring with I an ideal of R. Let $I_1 \supseteq I_2 \supseteq I_3 \supseteq \cdots$ be a descending chain of ideals of the quotient ring R/I. By the lattice isomorphism theorem for rings, each $I_i = N_i/I$ for some ideal N_i of R containing I. In particular, we have that $N_1 \supseteq N_2 \supseteq N_3 \supseteq \cdots$ is a descending chain of ideals of R, and so must terminate since R is Artinian. But this means that there exists $k \in \mathbb{Z}^+$ for which $N_k = N_m$ for all $m \geq k$. As such, we have $N_k/I = N_m/I$ for all $m \geq k$, and thus $I_k = I_m$. Thus any descending chain of ideals of R/I must also terminate, and so R/I is Artinian, as desired. ∎

Exercise 16.1.2. Show that any finite commutative ring with 1 is Artinian.

Proof. Let R be a finite commutative ring with 1. Let $I_1 \supseteq I_2 \supseteq I_3 \supseteq \cdots$ be a descending chain of ideals of R. Since $I_i \subseteq R$ for all i, we know $|I_i| \leq |R| < \infty$. Similarly, since $I_i \subseteq I_{i+1}$ for all i, we have $|I_{i+1}| \leq |I_i| \leq |R|$. Since $|I_i| > 0$ always, either this chain stabilizes or reaches the zero ideal, in which case we also have stabilization. Either way, R is Artinian. ∎

Exercise 16.1.3. Prove that an integral domain of Krull dimension 0 is a field.

Proof. Let R be an integral domain and suppose $\dim(R) = 0$. Since R is an integral domain, the zero ideal 0 is a prime ideal of R. If P was some non-trivial proper prime ideal of R, then $0 \subseteq P \subseteq R$ is a chain of prime ideals which exceeds length 0, ando so the only proper prime ideal of R is the zero ideal. Now if I was some other ideal of R, then $I \subseteq M$ for some maximal ideal of R, which is also a prime ideal, and this $M = 0$, forcing $I = 0$. In particular, the only ideals of R are 0 and R itself, to which R is a field. ∎

Exercise 16.1.4. Prove that an Artinian integral domain is a field.

Proof. Let R be an integral domain which is also Artinian. From Corollary 16.1.4, R is Noetherian and has Krull dimension 0. Thus R is a field by the previous exercise. ∎

Exercise 16.1.5, Suppose I is a nilpotent ideal in R and $M = IM$ for some R-module M. Prove that $M = 0$.

Proof. Since I is a nilpotent ideal in R, $I^k = 0$ for some $k \in \mathbb{Z}^+$, forcing $a^k = 0$ for all $a \in I$, and hence $I \subseteq \text{nil}(0)$. Theorem 16.1.3(3) asserts that $\text{nil}(0) = \text{Jac}(R)$, and so we have $I \subseteq \text{Jac}(R)$. Since $IM \subseteq \text{Jac}(R)M$, and $IM = M$ by assumption, we necessarily have $M \subseteq \text{Jac}(R)M$. The reverse inclusion is trivial, so we require $\text{Jac}(R)M = M$. Nakayama's lemma forces $M = 0$, as desired. ∎

Exercise 16.1.6.

Exercise 16.1.7.

Exercise 16.1.8.

Exercise 16.1.9.

Exercise 16.1.10.

Exercise 16.1.11.

Exercise 16.1.12.

Exercise 16.1.13.

Exercise 16.1.14.

16.2 Discrete Valuation Rings

Exercise 16.2.1. Suppose R is a Discrete Valuation Ring with respect to the valuation v on the fraction field K of R. If $x, y \in K$ with $v(x) < v(y)$ prove that $v(x+y) = \min(v(x), v(y))$. [Note that x+y=x(1+y/x).]

Proof. Suppose $x, y \in K$ with $v(x) < v(y)$. Clearly $\min\{v(x), v(y)\} = v(x)$. Since v is a valuation on K we know that

$$v(x+y) = v\left(x(1+\frac{y}{x})\right) = v(x) + v\left(1+\frac{y}{x}\right)$$

Now we analyze the sum above further. Note that

$$v\left(1+\frac{y}{x}\right) \geq \min\{v(1), v\left(\frac{y}{x}\right)\}$$

by properties of the DVR. Since $x^{-1} \in K$, and $v(1) = v(xx^{-1}) = v(x) + v(x^{-1}) = 0$, we have that $v(x) = -v(x^{-1})$, and hence we may make the substitution:

$$v(y/x) = v(y \cdot x^{-1}) = v(y) + v(x^{-1}) = v(y) - v(x)$$

And since $v(x) < v(y)$ by assumption, it follows that $v(y/x) > 0$. In particular, since $v(1) = 0$, this means that $\min\{v(1), v(y/x)\} = 0$, and hence that $v(1+y/x) = 0$. Thus we have

$$v(x+y) = v(x) = \min\{v(x), v(y)\}$$

which was the desired result. ∎

Exercise 16.2.2.

Exercise 16.2.3.

Exercise 16.2.4.

Exercise 16.2.5.

Exercise 16.2.6. Let R be an integral domain with fraction field K. Prove that every finitely generated R-submodule of K is a fractional ideal of R. If R is Noetherian, prove that A is a fractional ideal of R if and only if A is a finitely generated R-submodule of K.

Proof. Suppose A is a finitely generated R-submodule of K, say by $a_1, \ldots, a_n$. Note that since $a_i \in K$ we have that Ra_i is a principal fractional ideal of R for each $i \in \{1, \ldots, n\}$. Then since

$$A = \prod_{i=1}^{n} Ra_i$$

and the product of principal fractonal ideals is a fractional ideal, see for instance the discussion above Proposition 9 in the text, we have that A is a fractional ideal of R, as desired.

Going further, suppose that R is a Noetherian ring, Now suppose A is a fractional ideal, so that we know $A = d^{-1}I$ for some $d \in R \setminus \{0\}$ and ideal I of R. In a Noetherian ring, all ideals are finitely generated, and hence I is finitely generated, and so clearly A must also be. The converse holds from the above, as Noetherian rings are integral domains, giving the if and only if statement. ∎

Exercise 16.2.7. If R is an integral domain and A is a fractional ideal of R, prove that if A is projective then A is finitely generated. Conclude that every integral domain that is not Noetherian contains an ideal that is not projective.

Proof. Let A be a fractional ideal of R and suppose A is projective as an R-module. Proposition 10 gives that A is invertible, and Propositiion 9(3) gives that A is finitely generated, proving the statement.

Now if D is an integral domain which is not Noetherian, then there exists some ideal I of D which is not finitely generated. Recall that ideals are fractional ideals, and so we have that I is a non-finitely generated fractional ideal, which by the contrapositive of the above means that I is not projective as an R-module. Hence D must contain an ideal that is not projective. ∎

Exercise 16.2.8.

Exercise 16.2.9.

16.3 Dedekind Domains

Exercise 16.3.1.

Exercise 16.3.2.

Exercise 16.3.3.

Exercise 16.3.4.

Exercise 16.3.5.

Exercise 16.3.6.

Exercise 16.3.7.

Exercise 16.3.8.

Exercise 16.3.9.

Exercise 16.3.10.

Exercise 16.3.11.

Exercise 16.3.12. If I and J are nonzero fractional ideals for the Dedekind Domain R prove there are elements $\alpha, \beta \in K$ such that αI and βJ are nonzero integral ideals in R that are relatively prime.

Proof. Choosing some non-zero $x_2 \in J^{-1}$, we have that $x_2 J$ is an integral ideal of R. Since R is Dedekind, we let $P_1, \dots, P_s$ denote the distinct prime ideals dividing $x_2 J$. Now, for each i, $1 \leq i \leq s$, we have the containment

$$I_1^{-1} P_1 \cdots P_s \subsetneq I_1^{-1} P_1 \cdots P_{i-1} P_{i+1} \cdots P_s$$

so we may choose some $y_i \in (I_1^{-1} P_1 \cdots P_{i-1} P_{i+1} \cdots P_s) \setminus (I_1^{-1} P_1 \cdots P_s)$. Now set

$$x_1 := y_1 + \cdots + y_s$$

Then clearly we have the containment

$$x_1 \in I_1^{-1} \left(\sum_{i=1}^{s} P_1 \cdots P_{i-1} P_{i+1} \cdots P_s \right) \subseteq I_1^{-1},$$

hence $x_1 \in I_1^{-1}$ holds. We next prove that, for each i, $1 \leq i \leq s$, the prime ideal P_i does not divide the integral ideal $I_1 x_1$ of R. Since, in a Dedekind Domain, to contain is to divide, it suffices to show that $I_1 x_1$ is not contained in P_i. We have

$$x_1 I_1 = I_1(y_1 + \cdots + y_s) = \{\sum_{i=1}^{s} \alpha y_i \mid \alpha \in I_1\}$$

For each i, $1 \leq i \leq s$, note that for all $\alpha \in I_1$, and for all $j \neq i$, $1 \leq j \leq s$, we have that $\alpha y_j \in P_i$ by closure, as $y_j \in P_i$ since

$$y_j \in I_1^{-1} P_1 \cdots P_{j-1} P_{j+1} \cdots P_s \subseteq P_i$$

following since we took $j \neq i$. In particular, then, $I_1 y_i \not\subseteq P_i$, and hence $I_1 x_1 \not\subseteq P_i$ also holds. Since $I_1 x_1 \not\subseteq P_i$ for all $P_1, \ldots, P_s$ in the prime factorization of $I_2 x_2$, this means that $I_1 x_1$ and $I_2 x_2$ are relatively prime, as desired. ■

Exercise 16.3.13.

Exercise 16.3.14.

Exercise 16.3.15. If P is a nonzero prime ideal in the Dedekind Domain R prove that R/P^n is not a projective R-module for any $n \geq 1$. [Consider the exact sequence $0 \to P^n/P^{n+'1} \to R/P^{n+1} \to R/P^n \to 0$.] Conclude that if $M \neq 0$ is a finitely generated torsion R-module then M is not projective. [cf. Exercise 3, Section 10.5.]

Proof. If we assume, for contradiction, that R/P^n is projective as an R-module, then we have that $R_P/P^n R_P$ is a projective R_P-module, since the localization of a projective R-module is a projective module over the localized ring.

Moreover, since the localization of a Dedekind Domain at a prime ideal is, in particular, a P.I.D., via Theorem 15(2), we have that $R_P/P^n R_P$ is a finitely generated projective R_P-module; hence $R_P/P^n R_P$ is free by Exercise 12.1.21. This is clearly a contradiction, for freeness implies torsion-freeness for integral domains, and we obviously have $\operatorname{Tor}(R_P/P^n R_P) = P^n R_P \neq 0$ since by assumption $P \neq 0$. Therefore R/P^n is not a projective R-module for any $n \geq 1$.

For the second statement of the exercise, take some non-zero finitely generated torsion R-module M. Then by Theorem 22 we have

$$M = \operatorname{Tor}(M) \cong \bigoplus_{i=1}^{s} \left(R/P_i^{e_i}\right)$$

for some not necessarily distinct prime ideals $P_1, \ldots, P_s$ and some integers $e_1, \ldots, e_s \geq 1$. As we saw in the above paragraph, $R/P_i^{e_i}$ is not a projective R-module; hence M is not a projective R-module by Exercise 10.5.3. ■

Exercise 16.3.16.

Exercise 16.3.17.

Exercise 16.3.18.

Exercise 16.3.19.

Exercise 16.3.20.

Exercise 16.3.21.

Exercise 16.3.22.

Exercise 16.3.23.

Exercise 16.3.24.

Exercise 16.3.25.

※ Introduction to Homological Algebra and Group Cohomology

17.1 Introduction to Homological Algebra–Ext and Tor

Exercise 17.1.1. Give the details of the proof of Proposition 1.

Proof. Suppose $\alpha : \mathcal{A} \to \mathcal{B}$ is a homomorphism of cochain complexes. Let $\mathcal{A} = \{A^n\}_{n=1}^{\infty}$ and $\mathcal{B} = \{B^n\}_{n=1}^{\infty}$, with $\alpha = \{\alpha_n\}_{n=1}^{\infty}$ the collection of homomorphisms. We contend that the map of cohomology groups

$$\Psi : H^n(\mathcal{A}) \to H^n(\mathcal{B})$$

$$\Psi(x + \operatorname{im}(d_n)) = \alpha_n(x) + \operatorname{im}(e_n)$$

is a group homomorphism for all $n \in \mathbb{N}$, where $d_n : A^{n-1} \to A^n$ and $e_n : B^{n-1} \to B^n$ are the homomorphisms in the cochain complexes $\mathcal{A}$ and $\mathcal{B}$, respectively.

First we show that Ψ is well-defined. Suppose $x + \operatorname{im}(d_n) = y + \operatorname{im}(d_n)$. Then we know that $(x - y) + \operatorname{im}(d_n) = \operatorname{im}(d_n)$, and hence that $x - y \in \operatorname{im}(d_n)$. Thus there exists some $z \in A^n$ for which $d_n(z) = x - y$. By the commutativity of the diagram given by the homomorphism of cochain complexes, we require $e_n(\alpha_{n-1}(z)) = \alpha_n(x - y)$. In particular, the image of $\alpha_{n-1}(z)$ under e_n is $\alpha_n(x - y)$, and hence $\alpha_n(x - y) \in \operatorname{im}(e_n)$. This implies

$$\alpha_n(x - y) + \operatorname{im}(e_n) = \operatorname{im}(e_n) \iff \alpha_n(x) - \alpha_n(y) + \operatorname{im}(e_n) = \operatorname{im}(e_n)$$

which follows since α_n is a group homomorphism from $A^n \to B^n$. Now the above proves that $\alpha_n(x) + \operatorname{im}(e_n) = \alpha_n(y) + \operatorname{im}(e_n)$, hence showing that Ψ is well-defined. The check that Ψ is a group homomorphism is trivial, as we have

$$\begin{aligned}\Psi((x + y) + \operatorname{im}(d_n)) &= \alpha_n(x + y) + \operatorname{im}(e_n)\\ &= \alpha_n(x) + \alpha_n(y) + \operatorname{im}(e_n)\\ &= (\alpha_n(x) + \operatorname{im}(e_n)) + (\alpha_n(y) + \operatorname{im}(e_n))\\ &= \Psi(x + \operatorname{im}(d_n)) + \Psi(y + \operatorname{im}(d_n))\end{aligned}$$

and so Proposition 1 is proved; i.e., a homomorphism of cochain complexes induces a homomorphism of the cohomology groups associated to those complexes. ∎

Exercise 17.1.2. This exercise defines the connecting map δ_n in the Long Exact Sequence of Theorem 2 and proves it is a homomorphism. In the notation of Theorem 2 let $0 \to \mathcal{A} \xrightarrow{\alpha} \mathcal{B} \xrightarrow{\beta} \mathcal{C} \to 0$ be a short exact sequence of cochain complexes, where for simplicity the cochain maps for $\mathcal{A}$, $\mathcal{B}$, and $\mathcal{C}$ are all denoted by the same d.
(a) If $c \in C^n$ represents the class $x \in H^n(\mathcal{C})$ show that there is some $b \in B^n$ with

$\beta_n(b) = c$.
(b) Show that $d_{n+1}(b) \in \ker\beta_{n+1}$ and conclude that there is a unique $a \in A^{n+1}$ such that $\alpha_{n+1}(a) = d_{n+1}(b)$. [Use $c \in \ker d_{n+1}$ and the commutativity of the diagram.]
(c) Show that $d_{n+2}(a) = 0$ and conclude that a defines a class $\overline{a}$ in the quotient group $H^{n+1}(\mathcal{A})$. [Use the fact that α_{n+2} is injective.]
(d) Prove that $\overline{a}$ is independent of the choice of b, i.e., if b' is another choice and a' is its unique preimage in A^{n+1} then $\overline{a} = \overline{a'}$, and that $\overline{a}$ is also independent of the choice of c representing the class x.
(e) Define $\delta_n(x) = \overline{a}$ and prove that δ_n is a group homomorphism from $H^n(C)$ to $H^{n+1}(\mathcal{A})$. [Use the fact that $\delta_n(x)$ is independent of the choices of c and b to compute $\delta_n(x_1 + x_2)$.]

Proof. (a) Suppose $c \in C^n$ represents $\overline{x} \in H^n(C)$. In particular, we know that $H^n(C) = \ker(f_{n+1})/\mathrm{im}(f_n)$, so that $c \in \ker(f_{n+1})$ necessarily holds. This will be used for part (b). For part (a), note that the assumption that $0 \to \mathcal{A} \xrightarrow{\alpha} \mathcal{B} \xrightarrow{\beta} C \to 0$ is a short exact sequences of cochain complexes gives that $0 \to A^n \xrightarrow{\alpha_n} B^n \xrightarrow{\beta_n} C^n \to 0$ is a short exact sequence of groups for all $n \in \mathbb{N}$. In particular, we have that β_n is surjective, so that there exists some $b \in B^n$ for which $\beta_n(b) = c$.

(b) Recall that $c \in C^n$ representing $\overline{x} \in H^n(C)$ gives $c \in \ker(f_{n+1})$, and by commutativity of the diagram we require that $\beta_{n+1}(e_{n+1}(b)) = f_{n+1}(\beta_n(b))$, so in other words $\beta_{n+1}(e_{n+1}(b)) = f_{n+1}(c) = 0$, hence $e_{n+1}(b) \in \ker\beta_{n+1}$. Since $0 \to A^{n+1} \xrightarrow{\alpha_{n+1}} B^{n+1} \xrightarrow{\beta_{n+1}} C^{n+1} \to 0$ is a short exact sequence, we know that $\mathrm{im}\ \alpha_{n+1} = \ker\beta_{n+1}$, and so $e_{n+1}(b) \in \mathrm{im}\ \alpha_{n+1}$, which implies there exists $a \in A^{n+1}$ such that $\alpha_{n+1}(a) = e_{n+1}(b)$ in B^{n+1}.

(c) Since $\{B^n\}$ is a cochain complex, we know that $\mathrm{im}(e_n) \subseteq \ker(e_{n+1})$ for all n. In particular, since $e_{n+1}(b) \in \mathrm{im}(e_{n+1})$ is clear, we have $e_{n+1}(b) \in \ker(e_{n+2})$, so that $e_{n+2}(e_{n+1}(b)) = 0$. By commutativity of the diagram, and the fact that $\alpha_{n+1}(a) = e_{n+1}(b)$, we know that $\alpha_{n+2}(d_{n+2}(a)) = 0$ is required. However, since $0 \to A^{n+2} \xrightarrow{\alpha_{n+2}} B^{n+2} \xrightarrow{\beta_{n+2}} C^{n+2} \to 0$ is a short exact sequence, we know α_{n+2} is injective, and hence $d_{n+2}(a) = 0$ must hold. Hence $a \in \ker(d_{n+2})$ and so a represents some class, call it $\overline{a} \in H^{n+1}(\mathcal{A}) = \ker(d_{n+2})/\mathrm{im}(d_{n+1})$.

(d) Now we show that $\overline{a}$ in $H^{n+1}(\mathcal{A})$ is independent of the choice of $b \in B^n$. Suppose b' was another choice in B^n for which $\beta_n(b') = c$. Then $\beta_n(b)-\beta_n(b') = c-c = 0$ and since β_n is an R-module homomorphism this gives $\beta_n(b - b') = 0$. Thus $b - b' \in \ker\beta_n$ and by exactness this means $b - b' \in \mathrm{im}\ \alpha_n$, so that there exists some $a'' \in A^n$ for which $\alpha_n(a'') = b - b'$.

However now by commutativity of the diagram, we require that

$$\begin{aligned}\alpha_{n+1}(d_{n+1}(a'')) &= d_{n+1}(b-b') \\ &= d_{n+1}(b) - d_{n+1}(b') \\ &= \alpha_{n+1}(a) - \alpha_{n+1}(a') \\ &= \alpha_{n+1}(a-a')\end{aligned}$$

and since α_{n+1} is injective, this means $d_{n+1}(a'') = a - a'$. In other words, $a - a' \in \operatorname{im} d_{n+1}$, and so we have equality of classes $\overline{a} = \overline{a'}$ in $H^{n+1}(\mathcal{A})$. Using an analagous process we find that $\overline{a}$ is independent of choice of representative c for $x \in H^n(C)$.

(e) Define $\delta_n : H^n(C) \to H^{n+1}(\mathcal{A})$ by $\delta_n(x) = \overline{a}$ for each class $x \in H^n(C)$. We prove that δ_n is a group homomorphism. First we show δ_n is well defined. Assume $x = x'$ in $H^n(C)$. In part (d) above we showed that $\overline{a}$ is independent of choice of representative, and since x, x' both lie in the same class, they must agree on $\overline{a}$, giving well definition. Part (d) above trivially gives that $\delta_n(x+x') = \delta_n(x) + \delta_n(x')$ since if x and x' correspond to $\overline{a}$ and $\overline{a'}$, respectively, then $x + x'$ must correspond to $\overline{a+a'}$ in $H^{n+1}(\mathcal{A})$. ■

Exercise 17.1.3. Suppose

$$\begin{tikzcd} & A \arrow[r, "\alpha"] \arrow[d, "f"'] & B \arrow[r, "\beta"] \arrow[d, "g"'] & C \arrow[r] \arrow[d, "h"'] & 0 \\ 0 \arrow[r] & A' \arrow[r, "\alpha'"] & B' \arrow[r, "\beta'"] & C' & \end{tikzcd}$$

is a commutative diagram of R-modules with exact rows.
(a) If $c \in \ker h$ and $\beta(b) = c$ prove that $g(b) \in \ker \beta'$ and conclude that $g(b) = \alpha'(a')$ for some $a' \in A'$. [Use the commutativity of the diagram.]
(b) Show that $\delta(c) = a'$ (mod image f) is a well defined R-module homomorphism from $\ker h$ to the quotient $A'/\text{image } f$.
(c) (*The Snake Lemma*) Prove there is an exact sequence

$$\ker f \to \ker g \to \ker h \xrightarrow{\delta} \operatorname{coker} f \to \operatorname{coker} f \to \operatorname{coker} h$$

where $\operatorname{coker} f$ (the cokernel of f) is $A'/(\text{image } f)$ and similarly for $\operatorname{coker} g$ and $\operatorname{coker} h$.
(d) Show that if α is injective and β' is surjective (i.e., the two rows in the commutative diagram above can be extended to short exact sequences) then the exact sequence in (c) can be extended to the exact sequence

$$0 \to \ker f \to \ker g \to \ker h \xrightarrow{\delta} \operatorname{coker} f \to \operatorname{coker} f \to \operatorname{coker} h \to 0$$

Proof. (a) Since the top row is exact, we know that β is surjective, so taking $c \in \ker h \subseteq C$ gives the existence of a $b \in B$ for which $\beta(b) = c$. Since the diagram commutes, we know that $h(\beta(b)) = \beta'(g(b))$. Since $h(c) = 0$, we know

$h(c) = h(\beta(b)) = 0$, and hence that $\beta'(g(b)) = 0$ which provides $g(b) \in \ker \beta'$. Since the bottom row is exact, $\operatorname{im} \alpha' = \ker \beta'$ and hence $g(b) \in \operatorname{im} \alpha'$ and so there exists $a' \in A'$ for which $\alpha'(a') = g(b)$.

(b) Define a map $\delta : \ker h \to A'/\operatorname{im} f$ by $\delta(c) = a' \pmod{\operatorname{im} f}$ for all $c \in C$, where a' is the element of A' obtained via the procedure in part (a) for a particular choice of $c \in C$. To show that δ is well defined, suppose $c_1 = c_2$ in $\ker h$. Then, as from part (a), there is some $b \in B$ for whih $\beta(b) = c_1 = c_2$ and hence $\alpha'(a') = g(b)$ must also be the same $a' \in A'$, proving our claim, since $a' = a'$ trivially.

Now we show that δ is an R-module homomorphism. Let $c_1, c_2 \in \ker h$ and $r \in R$. Then there exists $b_1, b_2 \in B$ for which $\beta(b_1) = c_1$ and $\beta(b_2) = c_2$, and hence there exists $a_1', a_2' \in A'$ for which $\alpha'(a_1') = g(b_1)$ and $\alpha'(a_2') = g(b_2)$. In particular, we have

$$\delta(c_1) = a_1' \pmod{\operatorname{im} f}$$
$$\delta(c_2) = a_2' \pmod{\operatorname{im} f}$$

adding these two classes together, we obtain

$$\delta(c_1) + \delta(c_2) = a_1' + a_2' \pmod{\operatorname{im} f}$$

We also obtain that $\alpha'(a_1') + \alpha'(a_2') = g(b_1) + g(b_2)$, and since both α' and g are R-module homomorphisms, we have the equality $\alpha'(a_1' + a_2') = g(b_1 + b_2)$. We shall use this fact later in the proof.

We would now like to show that $\delta(c_1 + c_2) = \delta(c_1) + \delta(c_2)$.

For the element $c_1 + c_2 \in \ker h$, part (a) gives us the existence of some $b \in B$ for which $\beta(b) = c_1 + c_2$. By our above work, we may write that

$$c_1 + c_2 = \beta(b_1) + \beta(b_2) = \beta(b_1 + b_2)$$

since β is an R-module homomorphism. Hence $\beta(b) = \beta(b_1 + b_2)$ must hold. In particular, this means that

$$\beta(b) - \beta(b_1 + b_2) = 0 \iff \beta(b - b_1 - b_2) = 0$$

since β is an R-module homomorpism. Hence $b - b_1 - b_2 \in \ker \beta$. Since the top row is exact, we have $\operatorname{im} \alpha = \ker \beta$ and hence $b - b_1 - b_2 \in \operatorname{im} \alpha$, and so there exists $a \in A$ for which $f(a) = b - b_1 - b_2$. Since the diagram commutes, we must then have

$$\alpha'(f(a)) = g(b - b_1 - b_2) = g(b) - (g(b_1) + g(b_2))$$

where the last equality follows since g is an R-module homomorphism. Now, since above we saw that $g(b) = \alpha'(a')$ and $g(b_1) + g(b_2) = \alpha'(a_1') + \alpha'(a_2')$, the above equation means that

$$\alpha'(f(a)) = \alpha'(a') - (\alpha'(a_1') + \alpha'(a_2')) = \alpha'(a' - a_1' - a_2')$$

Where once again the last equality follows since α' is an R-module homomorphism. Since, in particular, α' is injective by the exactness of the bottom row, this means that

$$\begin{aligned} f(a) = a' - a_1' - a_2' &\iff a' - a_1' - a_2' \in \operatorname{im} f \\ &\iff a' \equiv a_1' + a_2' \pmod{\operatorname{im} f} \\ &\iff \delta(b) = \delta(c_1) + \delta(c_2) \end{aligned}$$

which is exactly what we aimed to show. We also have to show that $\delta(rc) = r\delta(c)$ for all $r \in R$ and $c \in \ker h$.

Once again, for $c \in \ker h$, let $\delta(c) = a' \pmod{\operatorname{im} f}$ for some $a' \in A'$. Now, for $r \in R$, we have $r\delta(c) = ra' \pmod{\operatorname{im} f}$. For $rc \in \ker h$, there exists $x \in B$ for which $\beta(x) = rc$, and hence also some $y \in A'$ for which $\alpha'(y) = g(x)$ from part (a).

Since β is an R-module homomorphism, we know $r\beta(b) = \beta(rb)$ and hence that $\beta(rb) = rc$. Thus $\beta(rb) = \beta(x)$ must hold. Subtracting yields $\beta(rb) - \beta(x) = 0$ and hence $\beta(rb - x) = 0$. This implies $rb - x \in \ker \beta$ and hence $rb - x \in \operatorname{im} \alpha$ by exactness. Thus there exists $a \in A$ for which $f(a) = rb - x$. By commutativity, we have

$$\alpha'(f(a)) = g(rb - x) = g(rb) - g(x) = rg(b) - g(x)$$

Since $g(b) = \alpha'(a')$ and $g(x) = \alpha'(y)$ as above, the above equation becomes

$$\alpha'(f(a)) = r\alpha'(a') - \alpha'(y) = \alpha'(ra' - y)$$

since α' is an R-module homomorphism. Since α' is injective, this means that $f(a) = ra' - y$ and hence that $ra' - y \in \operatorname{im} f$ and so

$$ra' = y \pmod{\operatorname{im} f}$$

Since $\delta(c) = a'$ and $\delta(rc) = y$, this means that $\delta(rc) = r\delta(c)$, which was the desired statement. Therefore, we may conclude that δ is an R-module homomorphism.

(c) We want to show that the sequence

$$\ker f \to \ker g \to \ker h \xrightarrow{\delta} \operatorname{coker} f \to \operatorname{coker} f \to \operatorname{coker} h$$

is exact. We may rewrite our current diagram as follows

$$\begin{tikzcd}
 & \ker f \arrow[r] \arrow[d, hook] & \ker g \arrow[r] \arrow[d, hook] & \ker h \arrow[d, hook] & \\
 & A \arrow[r, "\alpha"] \arrow[d, "f"] & B \arrow[r, "\beta"] \arrow[d, "g"] & C \arrow[r] \arrow[d, "h"] & 0 \\
0 \arrow[r] & A' \arrow[r, "\alpha'"] \arrow[d, two heads] & B' \arrow[r, "\beta'"] \arrow[d, two heads] & C' \arrow[d, two heads] & \\
 & \operatorname{coker} f \arrow[r] & \operatorname{coker} g \arrow[r] & \operatorname{coker} h &
\end{tikzcd}$$

Where $\widehat{\alpha} : \ker f \to \ker g$ takes $\widehat{\alpha}(a) = \alpha(a)$, $\widehat{\beta} : \ker g \to \ker h$ takes $\widehat{\beta}(b) = \beta(b)$, $\widehat{\alpha'}$: coker $f \to$ coker g takes $\widehat{\alpha'}(a' \pmod{\text{im } f)}) = \alpha'(a') \pmod{\text{im } g}$ and finally $\widehat{\beta'}$: coker $g \to$ coker h takes $\widehat{\beta'}(b' \pmod{\text{im } g)}) = \beta'(b') \pmod{\text{im } h}$.

We must show that these maps above are actual R-module homomorphisms. Starting with $\widehat{\alpha}$, we find that if $a \in \ker f$ then $f(a) = 0$. Hence $\alpha'(f(a)) = \alpha'(0) = 0$. Since the diagram commutes, this means that $g(\alpha(a)) = 0$ as well, and hence $\alpha(a) \in \ker g$. Thus we have our map. A similar process shows that $\widehat{\beta}$ works as well, and the others are trivial to see.

We check that the sequence initially shown is exact at $\ker g$, $\ker h$, coker f, and coker g.

The exactness at $\ker g$ follows since for $a \in \ker f$ we have $a \in \text{im } \alpha$ if and only if $\alpha \in \ker \beta$ by the assumed exactness of the top row.

The exactness at $\ker h$ follows since if $c \in \ker h$, then there exists $b \in \ker g$ for which $\beta(b) = c$ if and only if $g(b) = 0$ so that $\alpha'(a') = 0$ where $\delta(c) = a'$ (mod im f). By the injectivity of α' this means $a' = 0$ and hence $\delta(c) \in \text{im } f$.

The exactness at coker f follows since if $c \in \ker h$ maps to $a' \pmod{\text{im } f}$ in coker f, i.e., there exists $b \in B$ for which $\beta(b) = c$, then we know that $g(b) = \alpha'(a')$ by part (a) and hence $\alpha'(a') \in \text{im } g$ and so $\alpha'(a') = 0 \pmod{\text{im } g}$.

Finally, exactness at coker g follows since if $a' \pmod{\text{im } f}$ mapsto to $b' \pmod{\text{im } g}$ then $\alpha'(a') = b'$ and since the bottom row is exact this means $b' \in \ker \beta'$, to which $\beta'(b') = 0 \pmod{\text{im } h}$.

(d) Suppose α is injective and β' is surjective. We need only prove exactness of the sequence in part (c) at $\ker f$ and coker h. This is equivalent to show that $\widehat{\alpha}$ is injective and that $\widehat{\beta'}$ is surjective. Assume $a \in \ker f$ satisfies $\widehat{\alpha}(a) = 0$. Then $\alpha(a) = 0$ and since α is injective this means tht $a = 0$; hence $\widehat{\alpha}$ is injective.

Now assume $c' \pmod{\text{im } h} \in$ coker h. Then, in particular, $c' \in C$ and hence by the surjectivity of β' there exists $b' \in B'$ for which $\beta'(b') = c'$. Hence the equivalence class $b' \pmod{\text{im } g}$ maps to $c' \pmod{\text{im } h}$ under $\widehat{\beta'}$, which means that $\widehat{\beta'}$ is surjective.

Therefore the sequence from part (c) when extended,

$$0 \to \ker f \xrightarrow{\widehat{\alpha}} \ker g \xrightarrow{\widehat{\beta}} \ker h \xrightarrow{\delta} \text{coker } f \xrightarrow{\widehat{\alpha'}} \text{coker } f \xrightarrow{\widehat{\beta'}} \text{coker } h \to 0$$

is exact, as desired. ■

Exercise 17.1.4. Let $\mathcal{A} = \{A^n\}$ and $\mathcal{B} = \{B^n\}$ be cochain complexes, where the maps $A^n \to A^{n+1}$ and $B^n \to B^{n+1}$ in both complexes are denoted by d_{n+1} for all n. Cochain complex homomorphisms α and β from $\mathcal{A}$ to $\mathcal{B}$ are said to be *homotopic* if for all n there are module homomorphisms $s_n : A^{n+1} \longrightarrow B^n$ such that the maps $\alpha_n - \beta_n$ from A^n to B^n satisfy

$$\alpha_n - \beta_n = d_n s_{n-1} + s_n d_{n+1}$$

The collection of maps $\{s_n\}$ is called a *cochain homotopy* from α to β. One may similarly define chain homotopies between chain complexes.
(a) Prove that homotopic maps of cochain complexes induce the same maps on cohomology, i.e., if α and β are homotopic homomorphisms of cochain complexes then the induced group homomorphisms from $H^n(\mathcal{A})$ to $H^n(\mathcal{B})$ are equal for every $n \geq 0$. (Thus "homotopy" gives a sufficient condition for two maps of complexes to induce the same maps on cohomology or homology; this condition is not in general necessary.) [Use the definition of homotopy to show $(\alpha_n - \beta_n)(z) \in \text{im } d_n$ for every $z \in \ker d_{n+1}$.]
(b) Prove that the relation $\alpha \sim \beta$ if α and β are homotopic is an equivalence relation on any set of cochain complex homomorphisms.

Proof. (a) Suppose α and β are cochain homomorphisms from $\mathcal{A}$ to $\mathcal{B}$ which are homotopic. That is, there exists a cochain homotopy $\{s_n\}$ from α to β. For any $z \in \ker d_{n+1}$, observe that

$$\begin{aligned}(\alpha_n - \beta_n)(z) &= (d_n s_{n-1} + s_n d_{n+1})(z)\\ &= (d_n s_{n-1})(z) + (s_n d_{n+1})(z)\\ &= d_n(s_{n-1}(z)) + s_n(d_{n+1}(z))\\ &= d_n(s_{n-1}(z)) + s_n(0)\\ &= d_n(s_{n-1}(z))\end{aligned}$$

which means that $(\alpha_n - \beta_n)(z) \in \text{im } d_n$. As such, we have the relations in cohomology given by

$$\alpha_n(z) - \beta_n(z) \equiv 0 \pmod{\text{im } d_n} \iff \alpha_n(z) \equiv \beta_n(z) \pmod{\text{im } d_n}$$

for all $z \in \ker d_{n+1}$. Recall from Exercise 17.1.1 that the induced group homomorphism of α and β on cohomology is given by

$$\Psi_\alpha : H^n(\mathcal{A}) \longrightarrow H^n(\mathcal{B})$$

$$x + \text{im } d_n \longmapsto \alpha_n(x) + \text{im } d_n$$

and likewise for Ψ_β. Since above we showed that $\alpha_n(z)$ and $\beta_n(z)$ are equivalent modulo the image of d_n for all $z \in \ker d_{n+1}$, this, in particular, shows that $\Psi_\alpha = \Psi_\beta$, i.e., that the induced group homomorphisms on cohomology agree on all values.

(b) Define a relation on the set of all cochain homomorphisms from cochain complexes $\mathcal{A}$ to $\mathcal{B}$ by $\alpha \sim \beta$ if and only if α is homotopic to β. Clearly $\alpha \sim \alpha$

by taking $s_n = 0$ the zero map for all n, so that the relation $\sim$ is reflexive. Now suppose $\alpha \sim \beta$. Then there exists a cochain homotpy $\{s_n\}$ for which

$$\alpha_n - \beta_n = d_n s_{n-1} + s_n d_{n+1} \iff \beta_n - \alpha_n = -d_n s_{n-1} - s_n d_{n+1}$$

and so taking $\{-s_n\}$ gives the cochain homotopy, hence $\beta \sim \alpha$, so that the relation is symmetric. What remains is transitivity. Suppose $\alpha \sim \beta$ and $\beta \sim \gamma$. Then there exists cochain homotopies $\{s_n\}$ and $\{t_n\}$ for which

$$\alpha_n - \beta_n = d_n s_{n-1} + s_n d_{n+1}$$

$$\beta_n - \gamma_n = d_n t_{n-1} + t_n d_{n+1}$$

Note that adding both equations above together yields

$$\begin{aligned} \alpha_n - \gamma_n &= d_n s_{n-1} + s_n d_{n+1} - d_n t_{n-1} - t_n d_{n+1} \\ &= d_n(s_{n-1} - t_{n-1}) + (s_n - t_n)d_{n+1} \end{aligned}$$

Hence taking the cochain homotopy $\{s_n - t_n\}$ gives us that $\alpha \sim \gamma$. Therefore the relation "is homotopic to" is an equivalence relation on the set of all cochain homomorphisms of complexes. ■

Exercise 17.1.5. Establish the first step in the Simultaneous Resolution result of Proposition 7 as follows: assume the first two nonzero rows in diagram (11) are given, except for the map from $P_0 \oplus \overline{P_0}$ to M (where the maps along the row of projective modules are the obvious injection and projection for this split exact sequence). Let $\mu : \overline{P_0} \longrightarrow M$ be a lifting to $\overline{P_0}$ of the map $\overline{P_0} \longrightarrow N$ (which exists because $\overline{P_0}$ is projective). Let λ be the composition $P_0 \longrightarrow L \longrightarrow M$ in the diagram. Define

$$\pi : P_0 \oplus \overline{P_0} \longrightarrow M \quad \text{by} \quad \pi(x, y) = \lambda(x) + \mu(y)$$

Show that with this definition the first two nonzero rows of (11) form a commutative diagram.

Proof. We have the obvious injection and projection maps $\varphi_n : P_n \longrightarrow P_n \oplus \overline{P_n}$ and $\psi_n : P_n \oplus \overline{P_n} \longrightarrow \overline{P_n}$, respectively. Since $M \longrightarrow N$ is surjective, by the assumption of exactness of the original sequence $0 \longrightarrow L \longrightarrow M \longrightarrow N \longrightarrow 0$ being short exact, and we have a map $\overline{P_0} \longrightarrow M$, the fact that $\overline{P_0}$ is projective as an R-module means there exists such a lfit $\mu : \overline{P_0} \longrightarrow M$ making the diagram commute.

Similarly, define λ as in the problem description. We now show that the diagram

$$\begin{tikzcd}
 & \vdots \arrow[d] & \vdots \arrow[d] & \vdots \arrow[d] & \\
0 \arrow[r] & P_0 \arrow[r, hook, "\iota_1"] \arrow[d, "\epsilon_0"'] & P_0 \oplus \overline{P_0} \arrow[r, two heads, "\pi_2"] \arrow[d, "\pi"] & \overline{P_0} \arrow[r] \arrow[d, "\overline{\epsilon_0}"] & 0 \\
0 \arrow[r] & L \arrow[r, hook, "\psi"'] \arrow[d] & M \arrow[r, two heads, "\varphi"'] \arrow[d] & N \arrow[r] \arrow[d] & 0 \\
 & 0 & 0 & 0 &
\end{tikzcd}$$

commutes. If $p \in P_0$ then we have

$$(\overline{\epsilon_0} \circ \pi_2 \circ \iota_1)(p) = (\overline{\epsilon_0} \circ \pi_2)(p, 0) = \overline{\epsilon_0}(0) = 0$$

$$(\varphi \circ \pi \circ \iota_1)(p) = (\varphi \circ \pi)(p, 0) = \varphi(\lambda(p) + \mu(0)) = \varphi(\psi(\epsilon_0(p))) = 0$$

where the last equality follows since $\operatorname{im}(\psi) = \ker(\varphi)$ by exactness of the first row. What remains is

$$(\varphi \circ \psi \circ \epsilon_0)(p) = \varphi(\psi(\epsilon_0(p)) = 0$$

for the same reason just mentioned. In particular, under this definition of $\pi : P_0 \oplus \overline{P_0} \to M$, we have that the first two non-zero rows of the diagram commute. ■

Exercise 17.1.6. Let $0 \to \mathcal{A} \xrightarrow{\alpha} \mathcal{B} \xrightarrow{\beta} \mathcal{C} \to 0$ be a short exact sequence of cochain complexes. Prove that if any two of $\mathcal{A}$, $\mathcal{B}$, or $\mathcal{C}$ are exact, then so is the third. [Use Theorem 2.]

Proof. Given a short exact sequence $0 \to \mathcal{A} \xrightarrow{\alpha} \mathcal{B} \xrightarrow{\beta} \mathcal{C} \to 0$ of cochain complexes we have the long exact sequence in cohomology

$$0 \to H^0(\mathcal{A}) \to H^0(\mathcal{B}) \to H^0(\mathcal{C}) \xrightarrow{\delta_0} H^1(\mathcal{A}) \to H^1(\mathcal{B}) \to H^1(\mathcal{C}) \xrightarrow{\delta_1} H^2(\mathcal{A}) \to \cdots$$

Suppose $\mathcal{A}$ and $\mathcal{B}$ are exact. Then $H^n(\mathcal{A}) = \ker d_{n+1}/\operatorname{im} d_n = 0$ for all $n \geq 0$, and likewise for $H^n(\mathcal{B}) = 0$. In this case, the long exact sequence in cohomology above gives

$$0 \to 0 \to 0 \to H^0(\mathcal{C}) \to 0 \to 0 \to H^1(\mathcal{C}) \to 0 \to 0 \to \cdots$$

Clearly then $0 \to H^n(\mathcal{C}) \to 0$ is exact for all $n \geq 0$, and we have $\operatorname{im} 0 = \{0\}$ and $\ker 0 = H^n(\mathcal{C})$ and so exactness gives $H^n(\mathcal{C}) = 0$. Hence the cochain complex $\mathcal{C}$ is exact as well.

Now, if $\mathcal{A}$ and $\mathcal{C}$ are exact, we have $H^n(\mathcal{A}) = 0$ and $H^n(\mathcal{B}) = 0$ for all $n \geq 0$, and so the long exact sequence yields

$$0 \to 0 \to H^0(\mathcal{B}) \to 0 \to 0 \to 0 \to H^1(\mathcal{B}) \to 0 \to 0 \to \cdots$$

and hence once again the exactness of the above sequence yields $H^n(\mathcal{B}) = 0$ for all $n \geq 0$. Hence $\mathcal{B}$ is an exact cochain complex.

The case where $\mathcal{B}$ and $\mathcal{C}$ are exact follows completely analogously as the above, and hence we have proved the desired statement. ∎

Exercise 17.1.7. Prove that a finitely generated abelian group A is free if and only if $\operatorname{Ext}^1_{\mathbb{Z}}(A, \mathbb{Z}) = 0$.

Proof. Let A be a finitely generated abelian group. Then via Theorem 3 in Section 5.2 we have

$$A \cong \mathbb{Z}^m \times \mathbb{Z}/p_1\mathbb{Z} \times \cdots \times \mathbb{Z}/p_n\mathbb{Z}$$

for appropriately chosen integers $m, p_1, \ldots, p_n$. Now suppose that A is free. Then $p_1, \ldots, p_n = 1$ and we have $A \cong \mathbb{Z}^m$. Free implies projective, and hence A is a projective $\mathbb{Z}$-module to which $\operatorname{Ext}^1_{\mathbb{Z}}(A, \mathbb{Z}) = 0$ by Proposition 11.

Conversely, suppose that $\operatorname{Ext}^1_{\mathbb{Z}}(A, \mathbb{Z}) = 0$. Then, from Exercise 17.1.10, we have that

$$\begin{aligned}\operatorname{Ext}^1_{\mathbb{Z}}(A, \mathbb{Z}) &\cong \operatorname{Ext}^1_{\mathbb{Z}}(\mathbb{Z}^m \oplus \mathbb{Z}/p_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p_n\mathbb{Z}, \mathbb{Z}) \\ &\cong \operatorname{Ext}^1_{\mathbb{Z}}(\mathbb{Z}^m, \mathbb{Z}) \oplus \operatorname{Ext}^1_{\mathbb{Z}}(\mathbb{Z}/p_1\mathbb{Z}, \mathbb{Z}) \oplus \cdots \oplus \operatorname{Ext}^1_{\mathbb{Z}}(\mathbb{Z}/p_n\mathbb{Z}, \mathbb{Z})\end{aligned}$$

We know that $\operatorname{Ext}^1_{\mathbb{Z}}(\mathbb{Z}^m, \mathbb{Z}) = 0$ since $\mathbb{Z}^m$ is clearly a free (hence projective) $\mathbb{Z}$-module. Our assumption that $\operatorname{Ext}^1_{\mathbb{Z}}(A, \mathbb{Z}) = 0$ now forces $\operatorname{Ext}^1_{\mathbb{Z}}(\mathbb{Z}/p_i\mathbb{Z}, \mathbb{Z}) = 0$ for all $i \in \{1, \ldots, n\}$. Example 1 below Proposition 3 in the section tells us that $\operatorname{Ext}^1_{\mathbb{Z}}(\mathbb{Z}/p_i\mathbb{Z}, \mathbb{Z}) \cong \mathbb{Z}/p_i\mathbb{Z}$ for all such i, and hence $\mathbb{Z}/p_i\mathbb{Z} = 0$ holds for all i. Thus $p_i = 1$ for all i, and hence $A \cong \mathbb{Z}^m$ holds, to which A is free. ∎

Exercise 17.1.8.

Exercise 17.1.9.

Exercise 17.1.10.

Exercise 17.1.11.

Exercise 17.1.12. Prove Proposition 13: $\operatorname{Tor}^R_0(D, A) \cong D \otimes_R A$. [Follow the proof of Proposition 3.]

Proof. Let D be a right R-module and let A be a left R-module. Take a projective resolution

$$\cdots \xrightarrow{d_2} P_1 \xrightarrow{d_1} P_0 \xrightarrow{\epsilon} A \longrightarrow 0$$

for A. Such a resolution is an exact sequence, and so in particular, we have an exact sequence of R-modules given by

$$P_1 \xrightarrow{d_1} P_0 \xrightarrow{\epsilon} A \longrightarrow 0$$

Applying the covariant right exact functor $D \otimes_R -$ gives an exact sequence

$$D \otimes_R P_1 \xrightarrow{1 \otimes d_1} D \otimes_R P_0 \xrightarrow{1 \otimes \epsilon} D \otimes_R A \longrightarrow 0$$

As such, we have that $\mathrm{im}(1 \otimes d_1) = \ker(1 \otimes \epsilon)$ and $\mathrm{im}(1 \otimes \epsilon) = D \otimes_R A$. Hence, by definition of the 0th homology group derived from $D \otimes_R -$ we have

$$\mathrm{Tor}_0^R(D, A) = \frac{D \otimes_R P_0}{\mathrm{im}(1 \otimes d_1)} = \frac{D \otimes_R P_0}{\ker(1 \otimes \epsilon)} \cong \mathrm{im}(1 \otimes \epsilon) = D \otimes_R A$$

where the isomorphism above comes from the first isomorphism theorem for R-modules. Hence Proposition 12 is proved. ■

Exercise 17.1.13. Prove Proposition 16 characterizing flat modules.

Proof. Let D be a right R-module. First we shall prove (1) $\Longrightarrow$ (3). Suppose D is flat. Then we know that the functor $D \otimes_R -$ is exact. Let B be a left R-module and let

$$\cdots \xrightarrow{d_2} P_1 \xrightarrow{d_1} P_0 \xrightarrow{\epsilon} B \longrightarrow 0$$

be a projective resolution of B. In particular, the above sequence is exact, and so applying the functor $D \otimes_R -$ gives

$$\cdots \xrightarrow{1 \otimes d_2} D \otimes_R P_1 \xrightarrow{1 \otimes d_1} D \otimes_R P_0 \xrightarrow{1 \otimes \epsilon} D \otimes_R B \longrightarrow 0$$

an exact sequence. The exactness of the above sequence implies that $\mathrm{im}(1 \otimes d_n) = \ker(1 \otimes d_n)$ for all $n \geq 1$, and hence that

$$\mathrm{Tor}_n^R(D, B) = \frac{\ker(1 \otimes d_n)}{\mathrm{im}(1 \otimes d_{n+1})} = 0$$

for all $n \geq 1$. Since B was arbitrary, we have proved (1) $\Longrightarrow$ (3).

The proof that (3) $\Longrightarrow$ (2) is immediate.

Now we prove that (2) $\Longrightarrow$ (1) which will finish the proof. Suppose $\mathrm{Tor}_1^R(D, B) = 0$ for all left R-modules B. Let $0 \to L \to M \to N \to 0$ be an exact sequence of left R-modules. From Theorem 15 we have a long exact sequence of abelian groups

$$\cdots \longrightarrow \mathrm{Tor}_2^R(D, N) \xrightarrow{\delta_1} \mathrm{Tor}_1^R(D, L) \longrightarrow \mathrm{Tor}_1^R(D, M) \longrightarrow \mathrm{Tor}_1^R(D, N)$$

$$\xrightarrow{\delta_0} D \otimes_R L \longrightarrow D \otimes_R M \longrightarrow D \otimes_R N \longrightarrow 0$$

Now by assumption $\operatorname{Tor}_1^R(D, N) = 0$ since N is a left R-module, and hence we have an exact sequence of abelian groups

$$0 \xrightarrow{\delta_0} D \otimes_R L \to D \otimes_R M \to D \otimes_R N \to 0$$

Since the exact sequence $0 \to L \to M \to N \to 0$ was arbitrary, this suffices to prove that $D \otimes_R -$ is exact, and hence that D is flat as an R-module. ∎

Exercise 17.1.14. Suppose $0 \to A \to B \to C \to 0$ is a short exact sequence of R-modules. Prove that if C is a flat R-module, then A is flat if and only if B is flat. [Use the Tor long exact sequence.] Give an example to show that if A and B are flat then C need not be flat.

Proof. Let $0 \to A \to B \to C \to 0$ be a short exact sequence of right R-modules and suppose C is flat. Then for some left R-module D there is a long exact sequence in homology given by

$$\cdots \to \operatorname{Tor}_2^R(C, D) \xrightarrow{\delta_1} \operatorname{Tor}_1^R(A, D) \to \operatorname{Tor}_1^R(B, D) \to \operatorname{Tor}_1^R(C, D)$$

$$\xrightarrow{\delta_0} A \otimes_R D \to B \otimes_R D \to C \otimes_R D \to 0$$

which is an exact sequence of abelian groups. For more info on where this comes from (it is not Theorem 15) look at the discussion below Proposition 16. This is the long exact sequence in homology coming from the right exact functor $- \otimes_R D$.

Since D is a left R-module, the flatness of C means that $\operatorname{Tor}_n^R(C, D) = 0$ for all $n \geq 1$. In particular, the long exact sequence above becomes

$$\cdots \to 0 \xrightarrow{\delta_1} \operatorname{Tor}_1^R(A, D) \to \operatorname{Tor}_1^R(B, D) \to 0$$

$$\xrightarrow{\delta_)} 0 \to A \otimes_R D \to B \otimes_R D \to C \otimes_R D \to 0$$

Now we proceed with the main statement ot be proved. Suppose A is flat. Then Proposition 16 gives that $\operatorname{Tor}_n^R(A, D) = 0$ for all $n \geq 1$. In particular, the long exact sequence above becomes

$$\cdots \to 0 \xrightarrow{\delta_1} 0 \to \operatorname{Tor}_1^R(B, D) \to 0 \xrightarrow{\delta_0} 0 \to A \otimes_R D \to B \otimes_R D \to C \otimes_R D \to 0$$

And hence $\operatorname{Tor}_1^R(B, D) = 0$ since the sequence is exact at $\operatorname{Tor}_1^R(B, D)$. Since D was arbitrary, Proposition 16 once again permits us to write that B is flat.

A completely symmetric argument to the above works to show that if B is assumed flat then A must also be flat. Simply take the original long exact sequence and then $\operatorname{Tor}_n^R(B, D) = 0$ for all $n \geq 1$, which forces $\operatorname{Tor}_1^R(A, D) = 0$. Hence A is flat if and only if B is flat, as desired.

Now we give the requested example. Consider the short exact sequence

$$0 \to \mathbb{Z} \xrightarrow{2} \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \to 0$$

of $\mathbb{Z}$-modules. Clearly $\mathbb{Z}$ is flat, since it is projective, as a $\mathbb{Z}$-module. However, $\mathbb{Z}/2\mathbb{Z}$ is not flat as a $\mathbb{Z}$-module. To see this, note that $\mathbb{Z} \hookrightarrow \mathbb{Q}$ is an injection of $\mathbb{Z}$-modules, yet

$$\mathbb{Z}/2\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Q} = 0$$

is clearly not an injection. ■

Exercise 17.1.15.
(a) If I is an ideal in R and M is an R-module, prove that $\mathrm{Tor}_1^R(M, R/I)$ is isomorphic to the kernel of the map $M \otimes_R I \to M$ that maps $m \otimes i$ to mi for $i \in I$ and $m \in M$. [Use the Tor long exact sequence associated to $0 \to I \to R \to R/I \to 0$ noting that R is flat.]
(b) (*A Flatness Criterion using Tor*) Prove that the R-module M is flat if and only if $\mathrm{Tor}_1^R(M, R/I) = 0$ for every finitely generated ideal I or R. [Use Exercise 25 in Section 10.5.]

Proof. (a) Let M be an R-module with $I \trianglelefteq R$ an ideal. We have a short exact sequence of R-modules

$$0 \to I \to R \to R/I \to 0$$

From Theorem 15 we obtain a long exact sequence of abelian groups from the above via

$$\cdots \to \mathrm{Tor}_2^R(M, R/I) \xrightarrow{\delta_1} \mathrm{Tor}_1^R(M, I) \to \mathrm{Tor}_1^R(M, R) \to \mathrm{Tor}_1^R(M, R/I)$$

$$\xrightarrow{\delta_0} M \otimes_R I \to M \otimes_R R \to M \otimes_R R/I \to 0$$

Note that $M \otimes_R R \cong M$ via the isomoprhism $m \otimes r \mapsto rm$. In particular, since R is flat as an R-module, for instance since it is clearly free, we have $\mathrm{Tor}_1^R(M, R) = 0$, see the discussion below Proposition 16. Thus we have an exact sequence

$$0 \to \mathrm{Tor}_1^R(M, R/I) \xrightarrow{\delta_0} M \otimes_R I \to M$$

which suffices to prove the claim.

(b) Let M be an R-module. Suppose M is flat. Any finitely generated ideal I of R has R/I an R-module. In particular, the flatness of M with Proposition 16 gives that $\mathrm{Tor}_1^R(M, R/I) = 0$, proving one direction.

For the other, suppose $\mathrm{Tor}_1^R(M, R/I) = 0$ for all finitely generated ideals $I \trianglelefteq R$. In Exercise 10.5.25 we proved that M is flat if and only if for every finitely generated ideal I of R the map from $M \otimes_R I \to M \otimes_R R \cong M$ induced by the inclusion $I \subseteq R$

is injective. Note that the map $M \otimes_R I \to M$ is exactly $m \otimes i \mapsto mi$ for all $i \in I$ and $m \in M$. In particular, part (a) above shows that $\operatorname{Tor}_1^R(M, R/I)$ is the kernel of this map, and since $\operatorname{Tor}_1^R(M, R/I) = 0$, we have a trivial kernel, and hence the map $M \otimes_R I \to M$ is injective. Thus M is flat. ■

Exercise 17.1.16. Suppose R is a P.I.D. and A and B are R-modules. If $t(B)$ denotes the torsion submodule of B show that $\operatorname{Tor}_1^R(A, t(B)) \cong \operatorname{Tor}_1^R(A, B)$ and deduce that $\operatorname{Tor}_1^R(A, B)$ is isomorphic to $\operatorname{Tor}_1^R(t(A), t(B))$. [Use Exercise 26 in Section 10.5 to show that $B/t(B)$ is flat over R, then use the Tor long exact sequence with $D = A$ applied to the short exact sequence $0 \to t(B) \to B \to B/t(B) \to 0$ and the remarks following Proposition 16.]

Proof. Let R be a PID with A and B two R-modules. We know that $B/t(B)$ and $A/t(A)$ are clearly torsion-free R-modules, and hence by Exercise 10.5.26 both are flat over R. Consider the short exact sequence

$$0 \to t(B) \to B \to B/t(B) \to 0$$

and apply the right exact functor $A \otimes_R -$ and take the Tor long exact sequence of Theorem 15 to obtain

$$\cdots \to \operatorname{Tor}_2^R(A, B/t(B)) \xrightarrow{\delta_1} \operatorname{Tor}_1^R(A, t(B)) \to \operatorname{Tor}_1^R(A, B) \to \operatorname{Tor}_1^R(A, B/t(B))$$

$$\xrightarrow{\delta_0} A \otimes_R t(B) \to A \otimes_R B \to A \otimes_R B/t(B) \to 0$$

Now, since $B/t(B)$ is flat, we have $\operatorname{Tor}_1^R(A, B/t(B)) = 0$, see for instance the remarks below Proposition 16. In particular, the long exact sequence above becomes

$$\cdots \to 0 \xrightarrow{\delta_1} \operatorname{Tor}_1^R(A, t(B)) \to \operatorname{Tor}_1^R(A, B) \to 0$$

$$\xrightarrow{\delta_0} A \otimes_R t(B) \to A \otimes_R B \to A \otimes_R B/t(B) \to 0$$

Hence we have an exact sequence $0 \to \operatorname{Tor}_1^R(A, t(B)) \to \operatorname{Tor}_1^R(A, B) \to 0$ which necessarily means that $\operatorname{Tor}_1^R(A, B) \cong \operatorname{Tor}_1^R(A, t(B))$. Note that we could just as well have taken the short exact sequence $0 \to t(A) \to A \to A/t(A) \to 0$ and tensored over the R-module $t(B)$ to get a long exact sequence

$$\cdots \to \operatorname{Tor}_2^R(A/t(A), t(B)) \xrightarrow{\delta_1} \operatorname{Tor}_1^R(t(A), t(B)) \to \operatorname{Tor}_1^R(A, t(B)) \to$$

$$\operatorname{Tor}_1^R(A/t(A), t(B)) \xrightarrow{\delta_0} t(A) \otimes_R t(B) \to A \otimes_R t(B) \to A/t(A) \otimes_R t(B) \to 0$$

and since $A/t(A)$ is flat we have $\operatorname{Tor}_1^R(A/t(A), t(B)) = 0$ via Proposition 16, to which we get an exact sequence $0 \to \operatorname{Tor}_1^R(t(A), t(B)) \to \operatorname{Tor}_1^R(A, t(B)) \to 0$ which is simply an isomorphism $\operatorname{Tor}_1^R(t(A), t(B)) \cong \operatorname{Tor}_1^R(A, t(B))$. Combined with our initial result, we have

$$\operatorname{Tor}_1^R(A, B) \cong \operatorname{Tor}_1^R(A, t(B)) \cong \operatorname{Tor}_1^R(t(A), t(B))$$

which was exactly the desired statement, finishing the proof. ■

Exercise 17.1.17. Let $A = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} \oplus \cdots$. Prove that $\mathrm{Ext}^1(A, B) \cong (B/2B) \times (B/3B) \times (B/4B) \times \cdots$ for any abelian group B. [Use Exercise 10.] Prove that $\mathrm{Ext}^1(A, B) = 0$ if and only if B is divisible.

Proof. Let A be as in the problem description, and let B be any abelian group. Then we have

$$\mathrm{Ext}^1_{\mathbb{Z}}(A, B) = \mathrm{Ext}^1_{\mathbb{Z}}(\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \oplus \cdots, B) \cong \prod_{n \in \mathbb{Z}^+} \mathrm{Ext}^1_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, B) \cong \prod_{n \in \mathbb{Z}^+} (B/nB)$$

where the first isomorphism above follows from Exercise 17.1.10 and the second comes from Example 1 following Proposition 3 in the section.

Now if we suppose that $\mathrm{Ext}^1_{\mathbb{Z}}(A, B) = 0$, we require $\prod_{n \in \mathbb{Z}^+} (B/nB) = 0$, and hence $B/nB = 0$ for all integers $n \geq 2$. Moreover, if $n = 1$ then $B/B = 0$ always. In particular, $nB = B$ for all $n \in \mathbb{Z} \setminus \{0\}$, as can easily be seen. This is the definition of B being a divisible group.

The converse is easy to see: if B is divisible, then $nB = B$ for all non-zero integers n, and hence $B/nB = 0$ for all $n \geq 1$, and so $\mathrm{Ext}^1_{\mathbb{Z}}(A, B) = 0$ from our above work. ∎

Exercise 17.1.18.

Exercise 17.1.19.

Exercise 17.1.20.

Exercise 17.1.21. Let $R = k[x, y]$ where k is a field, and let I be the ideal (x, y) in R.
(a) Let $\alpha : R \to R^2$ be the map $\alpha(r) = (yr, -xr)$ and let $\beta : R^2 \to R$ be the map $\beta((r_1, r_2)) = r_1 x + r_2 y$. Show that

$$0 \to R \xrightarrow{\alpha} R^2 \xrightarrow{\beta} R \to k \to 0$$

where the map $R \to R/I = k$ is the canonical projection, gives a free resolution of k as an R-module.
(b) Use the resolution in (a) to show that $\mathrm{Tor}_2^R(k, k) \cong k$.
(c) Prove that $\mathrm{Tor}_1^R(k, I) \cong k$. [Use the long exact sequence corresponding to the short exact sequence $0 \to I \to R \to R/I \to 0$ and (b).]
(d) Conclude from (c) that the torsion free R-module I is not flat (compare to Exercise 26 in Section 10.5).

Proof. TBD ∎

Exercise 17.1.22. (*Flat Base Change for Tor*) Suppose R and S are commutative rings and $f : R \to S$ is a ring homomorphism making S into an R-module as in Example 6 following Corollary 12 in Section 10.4. Prove that if S is flat as an R-module, then $\text{Tor}_n^R(A, B) \cong \text{Tor}_n^S(S \otimes_R A, B)$ for all R-modules A and all S-modules B. [Show that since S is flat, tensoring an R-module projective resolution for A with S gives an S-module projective resolution of $S \otimes_R A$.]

Proof. Let A and B be R-modules, with B also having the structure of an S-module. We know that any R-module A has a free resolution (for instance given by splicing, see the discussion under the definition of a projective resolution in the text), say with

$$\cdots \xrightarrow{d_2} P_1 \xrightarrow{d_1} P_0 \xrightarrow{\epsilon} A \to 0$$

Since each P_n is a free R-module, we have that $P_n \cong R^{k_n}$ for some $k_n \in \mathbb{Z}^+$. In particular, our resolution above becomes

$$\cdots \xrightarrow{d_2} R^{k_1} \xrightarrow{d_1} R^{k_0} \xrightarrow{\epsilon} A \to 0$$

Now suppose that S is flat as an R-module (considered via the ring homomorphism $f : R \to S$ mentioned in the problem description). In this case we know that $S \otimes_R -$ is a covariant exact functor, and hence that the complex

$$\cdots \xrightarrow{d_2} S \otimes_R R^{k_1} \xrightarrow{d_1} S \otimes_R R^{k_0} \xrightarrow{\epsilon} S \otimes_R A \to 0$$

is exact. Now we can extend scalars for the free modules above, referring to Corollary 18 in Section 10.4, to get that $S \otimes_R R^{k_n} \cong S^{k_n}$ for all $n \in \mathbb{Z}^+$. In particular, it is clear that $S \otimes_R P_n$ is a projective S-module for all $n \in \mathbb{Z}^+$. Thus our complex,

$$\cdots \xrightarrow{d_2} S \otimes_R P_1 \xrightarrow{d_1} S \otimes_R P_0 \xrightarrow{\epsilon} S \otimes_R A \to 0$$

which is exact, above becomes an S-module projective resolution of the S-module $S \otimes_R A$.

Now, from the associativity of the tensor product, referring to Theorem 14 in Section 10.4, whose hypothesis is satisfied since B is in particular a right S-module and S is a (S, R)-bimodule trivially (both R and S are commutative), we have

$$B \otimes_S (S \otimes_R P_n) \cong (B \otimes_S S) \otimes_R P_n \cong B \otimes_R P_n$$

where the last isomorphism follows since $B \otimes_S S \cong B$ since B is an S-module. The above gives us that

$$\text{Tor}_n^S(B, S \otimes_R A) \cong \text{Tor}_n^R(B, A)$$

and since both R and S are commutative, we may swap terms in the Tor groups above (refer to the discussion below Proposition 16 in Section 17.1) and we obtain

$$\text{Tor}_n^R(A, B) \cong \text{Tor}_n^S(S \otimes_R A, B)$$

Since the R-module A and the S-module B were arbitrary, the above gives us our desired result. ∎

Exercise 17.1.23.

Exercise 17.1.24.

Exercise 17.1.25.

Exercise 17.1.26.
(a) Prove that every finitely generated module over a Noetherian ring R is finitely presented. [Use Exercise 8 in Section 15.1.]
(b) Prove that an R-module M is finitely presented and projective if and only if M is a direct summand of R^n for some integer $n \geq 1$.

Proof. TBD ∎

Exercise 17.1.27. Suppose that M is a finitely presented R-module and that $0 \to A \xrightarrow{\alpha} B \xrightarrow{\beta} M \to 0$ is an exact sequence of R-modules. This exercise proves that if B is a finitely generated R-module then A is also a finitely generated R-module.
(a) Suppose $R^s \xrightarrow{\psi} R^t \xrightarrow{\varphi} M \to 0$ and $e_1, \ldots, e_t$ is an R-module basis for R^t. Show that there exist $b_1, \ldots, b_t \in B$ so that $\beta(b_i) = \varphi(e_i)$ for $i = 1, \ldots, t$.
(b) If f is the R-module homomorphism from R^t to B defined by $f(e_i) = b_i$ for $i = 1, \ldots, t$, show that $f(\psi(R^s)) \subseteq \ker \beta$. [Use $\varphi \circ \psi = 0$.] Conclude that there is a commutative diagram

$$\begin{tikzcd}
 & R^s \arrow[r, "\psi"] \arrow[d, "g"'] & R^t \arrow[r, "\varphi"] \arrow[d, "f"'] & M \arrow[r] \arrow[d, equal] & 0 \\
0 \arrow[r] & A \arrow[r, "\alpha"] & B \arrow[r, "\beta"] & M \arrow[r] & 0
\end{tikzcd}$$

of R-modules with exact rows.
(c) Prove that $A/\text{image } g \cong B/\text{image } f$ and use this to prove that A is finitely generated. [For the isomorphism, use the Snake Lemma in Exercise 3. Then show that image g and $A/\text{image } g$ are both finitely generated and apply Exercise 7 of Section 10.3.]
(d) If I is an ideal of R conclude that R/I is a finitely presented R-module if and only if I is a finitely generated ideal.

Proof. (a) Given the R-basis $\{e_i\}$ for R^t, and since $\beta : B \to M$ is surjective, we know that for each $\varphi(e_i) \in M$ there exists some $b_i \in B$ for which $\beta(b_i) = \varphi(e_i)$ for all $i \in \{1, \ldots, t\}$.

(b) Now consider $f : R^t \to B$ defined by $f(e_i) = b_i$ for each $i \in \{1, \dots, t\}$. The fact that f is an R-module homomorphism is easily verified, as a consequence of the fact that β and φ are both such maps.

Take $x \in R^s$ and consider the element $\psi(x) \in R^t$. Note that since $e_1, \dots, e_t$ is an R-basis for R^t, we have that $\psi(x) = \sum_{i=1}^t r_i e_i$ for some $r_i \in R$. Now

$$f(\psi(x)) = f\left(\sum_{i=1}^t r_i e_i\right) = \sum_{i=1}^t r_i f(e_i) = \sum_{i=1}^t r_i b_i$$

which follows since f is an R-module homomorphism. However, note that $\varphi \circ \psi = 0$ since $R^s \xrightarrow{\psi} R^t \xrightarrow{\varphi} M \to 0$ is exact, and hence

$$\beta(f(\psi(x))) = \beta\left(\sum_{i=1}^t r_i b_i\right) = \sum_{i=1}^t r_i \beta(b_i) = \sum_{i=1}^t r_i \varphi(e_i) = \varphi\left(\sum_{i=1}^t r_i e_i\right) = \varphi(\psi(x)) = 0$$

and hence $f(\psi(x)) \in \ker \beta$. Since $x \in R^s$ was arbitrary, we conclude $f(\psi(R^s)) \subseteq \ker \beta$.

Now using this fact, we may remark that since $0 \to A \xrightarrow{\alpha} B \xrightarrow{\beta} M \to 0$ is exact, and $\operatorname{im}(\alpha) = \ker(\beta)$, we have that

$$R^s \xrightarrow{\psi} R^s \xrightarrow{f|_{\psi(R^s)}} \operatorname{im}(\alpha) \cong A/\ker(\alpha) \cong A$$

via the first isomorphism theorem, and since $\ker(\alpha) = 0$ since α is injective. In particular, we have a map from R^s to A which we shall denote g. Hence we have a diagram

$$\begin{tikzcd}
& & & R^s \arrow[d, "\psi"] \arrow[ddll, "g"'] & \\
& & & R^t \arrow[d, "\varphi"] \arrow[dl, "f"'] & \\
0 \arrow[r] & A \arrow[r, "\alpha"] & B \arrow[r, "\beta"] & M \arrow[r] & 0
\end{tikzcd}$$

which commutes. Rewriting the above yields the diagram in the problem description, that of

$$\begin{tikzcd}
& R^s \arrow[r, "\psi"] \arrow[d, "g"'] & R^t \arrow[r, "\varphi"] \arrow[d, "f"'] & M \arrow[r] \arrow[d, equal] & 0 \\
0 \arrow[r] & A \arrow[r, "\alpha"] & B \arrow[r, "\beta"] & M \arrow[r] & 0
\end{tikzcd}$$

which was the desired result.

(c) Now, from Exercise 17.1.3, the Snake Lemma, we have an exact sequence

$$\ker(f) \to \ker(g) \to \ker(\mathrm{id}_M) \xrightarrow{\delta} \operatorname{coker}(f) \to \operatorname{coker}(g) \to \operatorname{coker}(\mathrm{id}_M)$$

which, since $\ker(\mathrm{id}_M) = 0$ and $\mathrm{coker}(\mathrm{id}_M) = 0$, in particular gives an exact sequence

$$0 \to \mathrm{coker}(f) \cong B/\mathrm{im}(f) \to \mathrm{coker}(g) \cong A/\mathrm{im}(g) \to 0$$

which necessarily means that $B/\mathrm{im}(f) \cong A/\mathrm{im}(g)$.

Recall that we assumed B was finitely generated as an R-module. In particular, this automatically gives that $B/\mathrm{im}(f)$ is finitely generated, for if $b_1', \ldots, b_k'$ is a set of generators for B then $b_1' + \mathrm{im}(f), \ldots, b_k' + \mathrm{im}(f)$ is a set of generators for $B/\mathrm{im}(f)$. Hence $A/\mathrm{im}(g)$ is finitely generated. Also, note that $\mathrm{im}(g) \cong R^s/\ker(g)$ where R^s (and so $\ker(g)$) are both finitely generated. In particular, both $\mathrm{im}(g)$ and $A/\mathrm{im}(g)$ are finitely generated R-modules, and so by Exercise 10.3.7 we have that A is finitely generated.

(d) If R/I is a finitely presented R-module then since $0 \to I \to R \to R/I \to 0$ is a short exact sequence via the usual maps and R is trivially finitely generated as an R-module (for instance via $R = 1R$), parts (a-c) above give that I is finitely generated as an R-module, hence a finitely generated ideal of R.

For the converse, assume that I is finitely generated as an ideal of R, say by $a_1, \ldots, a_n$. In particular, we have that the kernel of the natural projection $R \to R/I$ can be generated by n elements of R, and hence that $R^n \to R \to R/I \to 0$ is exact. ■

Exercise 17.1.28.

Exercise 17.1.29.

Exercise 17.1.30

Exercise 17.1.31.

Exercise 17.1.32.

Exercise 17.1.33.

Exercise 17.1.34.

Exercise 17.1.35.

17.2 The Cohomology of Groups

Exercise 17.2.1

Exercise 17.2.2

Exercise 17.2.3

Exercise 17.2.4

Exercise 17.2.5

Exercise 17.2.6

Exercise 17.2.7

Exercise 17.2.8

Exercise 17.2.9

Exercise 17.2.10

Exercise 17.2.11

Exercise 17.2.12

Exercise 17.2.13

Exercise 17.2.14

Exercise 17.2.15

Exercise 17.2.16

Exercise 17.2.17

Exercise 17.2.18

Exercise 17.2.19

Exercise 17.2.20

Exercise 17.2.21

Exercise 17.2.22

Exercise 17.2.23

Exercise 17.2.24

Exercise 17.2.25

17.3 Crossed Homomorphisms and $H^1(G, A)$

Exercise 17.3.1

Exercise 17.3.2

Exercise 17.3.3

Exercise 17.3.4

Exercise 17.3.5

Exercise 17.3.6

Exercise 17.3.7

Exercise 17.3.8

Exercise 17.3.9

Exercise 17.3.10

Exercise 17.3.11

Exercise 17.3.12

Exercise 17.3.13 The Galois group of the extension $\mathbb{C}/\mathbb{R}$ is the cyclic group $G = \langle \tau \rangle$ of order 2 generated by complex conjugation τ. Prove that $H^2(G, \mathbb{C}^\times) \cong \mathbb{R}^\times/\mathbb{R}^+ \cong \mathbb{Z}/2\mathbb{Z}$ where $\mathbb{R}^+$ denotes the positive real numbers.

Proof. From the cohomology of finite cyclic groups, we know that

$$H^2(G, \mathbb{C}^\times) = (\mathbb{C}^\times)^G / N\mathbb{C}^\times$$

where $N = 1 + \tau$ is the norm map. Note that $(\mathbb{C}^\times)^G = \mathbb{R}^\times$ since the extension is Galois with group G. For the image of $\mathbb{C}^\times$ under the norm map, we have the following:

$$N(a + bi) = (1 + \tau)(a + bi) = (a + bi)(a - bi) = a^2 + b^2$$

where the multiplication is carried out since the operation in $\mathbb{C}^\times$ is of course multiplication. Clearly $N\mathbb{C}^\times \subseteq \mathbb{R}^+$ since at least one of a or b is non-zero. The reverse containment is obvious, and hence $N\mathbb{C}^\times = \mathbb{R}^+$.

For any $r \in \mathbb{R}^\times$ we know that $r^2 \in \mathbb{R}^+$ since the square of a non-zero real number is positive. In particular, the group $\mathbb{R}^\times/\mathbb{R}^+$ has 2 elements, one being the set of positive non-zero real numbers and the other being the negative non-zero real numbers, and is thus isomorphic to $\mathbb{Z}/2\mathbb{Z}$. Concluding, we have that $H^2(G, \mathbb{C}^\times) \cong \mathbb{Z}/2\mathbb{Z}$, as desired. ∎

Exercise 17.3.14

Exercise 17.3.15

17.4 Group Extensions, Factor Sets, and $H^2(G, A)$

Exercise 17.4.1

Exercise 17.4.2 Let $A = \mathbb{Z}/4\mathbb{Z}$ and let G be the cyclic group of order 2 acting trivially on A.
(a) Prove that $|C^2(G, A)| = 2^8$.
(b) Use the coboundary condition to show that $|B^2(G, A)| = 2^3$.
(c) Show that $|H^2(G, A)| = 2$ by exhibiting two inequivalent extensions of G by A and their corresponding cocycles.

Proof. (a) It is clear that the number of possible maps $f : G \times G \to A$ is equal to $|A|^{|G\times G|} = |4|^4 = 2^4 2^4 = 2^8$.

(b) Recall that $f : G \times G \to A$ is a 2-coboundary if it is a 2-cocycle with the additional requirement that there exists $f_1 : G \to A$ such that

$$f(g, h) = g \cdot f_1(h) - f_1(gh) + f_1(g)$$

In our case, G acts trivially on A, so $g \cdot f_1(h) = f_1(h)$. Since $G = \langle g \rangle$ we have possible values for any 2-coboundary given by:

$$f(1, 1) = f_1(1) - f_1(1) + f_1(1) = f_1(1)$$

$$f(g, 1) = f_1(1) - f_1(g) + f_1(g) = f_1(1)$$

$$f(1, g) = f_1(g) - f_1(g) + f_1(1) = f_1(1)$$

$$f(g, g) = f_1(g) - f_1(1) + f_1(g) = 2f_1(g) - f_1(1)$$

Clearly we have four options for $f_1(1)$ corresponding to the four elements of A. To determine $f(g, g)$, it then suffices to choose a value for $f_1(g)$. Note that choosing $f_1(g) = 1$ or $f_1(g) = 3$ gives $f(g, g) = 2 - f_1(1)$ and $f(g, g) = 6 - f_1(1)$. respectively, which are the same since $6 \equiv 2 \pmod 4$. Also choosing $f_1(g) = 0$ or $f_1(g) = 2$ gives $f(g, g) = 0 - f_1(1) = f_1(1)$ and $f(g, g) = 4 - f_1(1) = f_1(1)$, respectively, since $0 \equiv 4 \pmod 4$. In particular, we have two options for the value of $f_1(1)$. Combining all this together, we have $4 \cdot 2 = 8$ options for 2-coboundaries. Hence $|B^2(G, A)| = 2^3$.

(c) We prove that $|Z^2(G, A)| \leq 2^4$. Any 2-cocycle $f : G \times G \to A$ must satisfy

$$f(g, h) + f(gh, k) = g \cdot f(h, k) + f(g, hk)$$

for all $g, h, k \in G$. Since G acts trivially on A in our case, we have $g \cdot f(h, k) = f(h, k)$. There are four possible values for each 2-cocycle, $f(1, 1)$, $f(1, g)$, $f(g, 1)$, and $f(g, g)$. We can see that

$$f(1, 1) + f(1, g) = f(1, g) + f(1, g)$$

gives $f(1,1) = f(1,g)$, while

$$f(g,g) + f(1,g) = f(g,g) + f(g,1)$$

gives $f(1,g) = f(g,1)$. Hence there are four options for $f(1,1) = f(1,g) = f(g,1)$ corresponding to the four elements of A, and four options for $f(g,g)$. In particular, this means that $|Z^2(G,A)| \leq 4 \cdot 4 = 2^4$.

(d) From parts (b) and (c) above we have that $|H^2(G,A)| \leq 2$. To prove that $|H^2(G,A)| = 2$, we exhibit two inequivalent extensions of G by A. Let $Z_4 \times Z_2 = \langle x \rangle \times \langle y \rangle$ and consider the sequence

$$1 \longrightarrow A \xrightarrow{\iota} Z_4 \times Z_2 \xrightarrow{\pi} Z_2 \longrightarrow 1$$

where $\iota(1) = (x,1)$ and $\pi(x,1) = 1$ and $\pi(1,y) = g$. Then $\ker(\pi) = \{(x^i,1) \mid i = 0,1,2,3\}$ is clear; in fact we clearly have that $\operatorname{im}(\iota) = \ker(\pi)$, so that the sequence is a short exact sequence; hence $Z_4 \times Z_2$ is an extension of G by A.

Now we determine the 2-cocycle corresponding to this extension. Any section $\mu : Z_2 \longrightarrow Z_4 \times Z_2$ must satisfy $(\pi \circ \mu)(g) = g$ for all $g \in G$, and hence $\pi(\mu(g)) = g$ and $\pi(\mu(1)) = 1$. There are four options for $\mu(1)$, which are $(x,1)$, $(x^2,1)$, $(x^3,1)$, and $(1,1)$. There is only one option for $\mu(g)$, which is $(1,y)$. However, if we assume μ to be a normalized section, then $\mu(1) = (1,1)$ is required. We have:

$$\mu(1)\mu(1) = f(1,1)\mu(1)$$
$$\mu(g)\mu(1) = f(g,1)\mu(g)$$
$$\mu(1)\mu(g) = f(1,g)\mu(g)$$
$$\mu(g)\mu(g) = f(g,g)\mu(1)$$

and using the fact that $\mu(g) = (1,y)$, our equations above, and the fact that $Z_4 \times Z_2$ is abelian, we may find that

$$\mu(1) = f(1,1) = f(g,1) = f(1,g) = (1,1)$$

and $f(g,g)(1,1) = (1,1)$ so that $f(g,g) = (1,1)$. Hence the 2-cocycle f corresponding to μ is identically 0, meaning that this extension corresponds to the trivial cohomology class in $H^2(G,A)$.

For another extension, consider the sequence

$$1 \longrightarrow A \xrightarrow{\iota'} D_8 \xrightarrow{\pi'} G \longrightarrow 1$$

where $\iota'(1) = r$ and $\pi'(s) = g$ and $\pi'(r) = 1$. We clearly have $\ker(\pi') = \operatorname{im}(\iota')$, and hence this is a short exact sequence and thus D_8 is an extension of G by A.

To determine the normalized 2-cocycle associated to this extension, we choose a normalized section $\mu : G \longrightarrow D_8$ which must satisfy $\pi(\mu(1)) = 1$ and $\pi(\mu(g)) = g$, and hence either $\mu(1)$ is equal to 1, r, r^2, or r^3, while $\mu(g)$ is equal to one of s, sr, sr^2, or sr^3. If μ is normalized, then we require $\mu(1) = 1$. Now following a similar procedure as to the above, we find

$$\mu(1) = f(1,1) = f(g,1) = f(1,g) = 1$$

and $f(g,g) = \mu(g)\mu(g)$, so that $f(g,g) = 1$ or $f(g,g) = r^2$. If $f(g,g) = 1$ then the normalized factor set f would be identically 0, and so correspond to the trivial cohomology class. However, setting $f(g,g) = r^2$, so that $\mu(g) = sr$ is chosen, gives us a non-trivial normalized factor set.

Since no isomorphism from $Z_4 \times Z_2$ to D_8 is possible, as $Z_4 \times Z_2$ is abelian while D_8 is non-abelian, it follows that these two extensions of G by A are non-equivalent, and hence correspond to distinct cohomology classes in $H^2(G,A)$. Thus $|H^2(G,A)| \geq 2$, and combined with our above work we get $|H^2(G,A)| = 2$, as desired. ■

Exercise 17.4.3

Exercise 17.4.4

Exercise 17.4.5

Exercise 17.4.6

Exercise 17.4.7

Exercise 17.4.8

Exercise 17.4.9

Exercise 17.4.10 Suppose $\mathbb{F}_q$ is a finite field with $G = \mathrm{Gal}(\mathbb{F}_{q^d}/\mathbb{F}_q) = \langle \sigma_q \rangle$ where σ_q is the Frobenius automorphism, and let N be the usual norm element for the cyclic group G.
(a) Use Hilbert's Theorem 90 to prove that $|{}_N(\mathbb{F}_{q^d}^\times)| = (q^d - 1)/(q-1)$, and deduce that the norm map from $\mathbb{F}_{q^d}$ to $\mathbb{F}_q$ is surjective.
(b) Prove that $H^n(G, \mathbb{F}_{q^d}^\times) = 0$ for all $n \geq 1$.

Proof. (a) From the cohomology of finite cyclic groups, we know that

$$H^1(G, \mathbb{F}_{q^d}^\times) = {}_N(\mathbb{F}_{q^d}^\times)/(\sigma_q - 1)\mathbb{F}_{q^d}^\times$$

Hilbert's Theorem 90 asserts that $H^1(G, \mathbb{F}_{q^d}^\times) = 0$, which follows since $\mathbb{F}_{q^d}/\mathbb{F}_q$ is a finite Galois extension with cyclic Galois group G. In particular, we have ${}_N(\mathbb{F}_{q^d}^\times) = (\sigma_q - 1)\mathbb{F}_{q^d}^\times$. From the first isomorphism theorem we have the following:

$$(\sigma_q - 1)\mathbb{F}_{q^d}^\times \cong \mathbb{F}_{q^d}^\times/\ker(\sigma_q - 1)$$

Moreover, since $\ker(\sigma_q - 1) = \mathbb{F}_q^\times$ we require

$$|(\sigma_q - 1)\mathbb{F}_{q^d}^\times| = \frac{|\mathbb{F}_{q^d}^\times|}{|\mathbb{F}_q^\times|} = \frac{q^d - 1}{q - 1}$$

Thus $|_N(\mathbb{F}_{q^d}^\times)| = (q^d - 1)/(q - 1)$. Now, we consider the norm map $N : \mathbb{F}_{q^d}^\times \to \mathbb{F}_q^\times$, and observe that $\ker(N) =_N (\mathbb{F}_{q^d}^\times)$; hence the first isomorphism theorem may be employed once more to yield $\mathbb{F}_{q^d}^\times/\ker(N) \cong N(\mathbb{F}_{q^d}^\times)$. In particular, we require that

$$|N(\mathbb{F}_{q^d}^\times)| = \frac{q^d - 1}{(q^d - 1)/(q - 1)} = q - 1$$

However since $N(\mathbb{F}_{q^d}^\times) \subseteq \mathbb{F}_q$ by construction, the above forces $\mathbb{F}_q = N(\mathbb{F}_{q^d}^\times)$, and hence we know that the norm map is surjective.

(b) From the cohomology of finite cyclic groups, we have the following:

$$H^n(G, \mathbb{F}_{q^d}^\times) = \left\{ \begin{array}{ll} (\mathbb{F}_{q^d}^\times)^G / N(\mathbb{F}_{q^d}^\times), & \text{if } n \text{ is even, } n \geq 2 \\ \\ {}_N(\mathbb{F}_{q^d}^\times)/(\sigma_q - 1)\mathbb{F}_{q^d}^\times, & \text{if } n \text{ is odd, } n \geq 1 \end{array} \right\}$$

Hilbert's Theorem 90, as in part (a), gives us that $H^n(G, \mathbb{F}_{q^d}^\times) = 0$ for all odd $n \geq 1$. From part (a) as well, the surjectivity of the norm map, combined with the fact that $(\mathbb{F}_{q^d}^\times)^G = \mathbb{F}_q^\times$, which holds since G is the Galois group of $\mathbb{F}_{q^d}/\mathbb{F}_q$, yields that $H^n(G, \mathbb{F}_{q^d}^\times) = 0$ for all even $n \geq 2$. In particular, we have shown that $H^n(G, \mathbb{F}_{q^d}^\times) = 0$ for all $n \geq 1$, as desired. ■

※ Representation Theory and Character Theory

18.1 Linear Actions and Modules over Group Rings

Exercise 18.1.1 Prove that if $\varphi : G \to \mathrm{GL}(V)$ is any representation, then φ gives a faithful representation of $G/\ker\varphi$.

Proof. Let $\varphi : G \to \mathrm{GL}(V)$ be a representation of G. The first isomorphism theorem gives $G/\ker\varphi \cong \varphi(G) \subseteq \mathrm{GL}(V)$, and hence we may extend this isomorphism to a group homomorphism $\psi : G/\ker\varphi \to \mathrm{GL}(V)$ defined by $\psi(\overline{g}) = \varphi(g)$ for all $\overline{g} \in G/\ker\varphi$. To see this this representation is faithful, note that $\overline{g} \in \ker\psi$ if and only if $\psi(\overline{g}) = \mathrm{id}_V$, and so $\varphi(g) = \mathrm{id}_V$ and hence $g \in \ker\varphi$. ∎

Exercise 18.1.2 Let $\varphi : G \to \mathrm{GL}_n(F)$ be a matrix representation. Prove that the map $g \mapsto \det(\varphi(g))$ is a degree 1 representation.

Proof. Since $\varphi : G \to \mathrm{GL}_n(F)$ is a matrix representation, we know that for each $g \in G$ we have an $n\times n$ matrix $\varphi(g)$ with coefficients in F. Recall that the $\det : \mathrm{GL}_n(F) \to F$ is the determinant map, which is in particular a group homomorphism of $\mathrm{GL}_n(F)$ to F considered as an additive abelian group. Noting that $\mathrm{GL}_1(F) = F$, we may compose the matrix representation φ with det to obtain a new map ψ which is defined by

$$\psi = \det\circ\varphi : G \to \mathrm{GL}_1(F)$$

$$\psi(g) = \det(\varphi(g))$$

and the map ψ is once more a group homomorphism since both det and φ are as well. Since F is a 1-dimensional vector space over itself, we have shown that ψ is a degree 1 F-representation of G on F. ∎

Exercise 18.1.3 Prove that the degree 1 representations of G are in bijective correspondence with the degree 1 representations of the abelian group G/G' (where G' is the commutator subgroup of G).

Proof. Since $F = \mathrm{GL}_1(F)$, we aim to show that group homomorphisms $G \to F$ are in bijective correspondence with group homomorphisms $G/G' \to F$, where G' is the commutator subgroup of G.

Consider the field F as an additive abelian group. Given a group homomorphism $\varphi : G \to F$, the fact that F is an abelian group allows us to refer to Proposition 7 in Section 5.4 to write that φ factors through G', i.e., that the diagram

$$\begin{tikzcd} G \arrow[r, "\pi"] \arrow[dr, "\varphi"'] & G/G' \arrow[d, "\widetilde{\varphi}"] \\ & F \end{tikzcd}$$

commutes, where π is the natural projection homomorphism and $\widetilde{\varphi} : G/G' \to F$ is the group homomorphism defined by $\widetilde{\varphi}(g + G') = \varphi(g)$ for all $g + G' \in G/G'$. Note that $\widetilde{\varphi}$ is a degree 1 representation of G/G', giving us one direction of the correspondence.

The reverse direction of the correspondence is trivial, for if we assume that $\varphi : G/G' \to F$ is a group homomorphism then we may post-compose φ with the natural projection map $\pi : G \to G/G'$, obtaining a group homomorphism $\varphi \circ \pi : G \to F$, a degree 1 representation of G. ■

Exercise 18.1.4 Let V be a (possibly infinite dimensional) FG-module (G is a finite group). Prove that for each $v \in V$ there is an FG-submodule containing v of dimension $\leq |G|$.

Proof. Let V be an $F[G]$-module and take any $v \in V$. Let $\varphi : G \to \mathrm{GL}(V)$ be the representation afforded by V.

We aim to find a G-stable subspace of V containing v of dimension $\leq |G|$.

Since G is a finite group, we may let $G = \{g_1, \dots, g_n\}$, where g_1 is the identity element of G. Now take any $v \in V$. Then $\varphi(g_1)(v), \dots \varphi(g_n)(v)$ are each elements of V, and so we may consider the subspace

$$W = \mathrm{span}(\varphi(g_1)(v), \dots, \varphi(g_n)(v))$$

Since $\varphi(g_1)(v) = v$, as g_1 is the identity element of G, we have that $v \in W$. Moreover, note that for any $g \in G$ we have

$$\varphi(g)\left(\sum_{i=1}^{n} \alpha_i \varphi(g_i)(v)\right) = \sum_{i=1}^{n} \alpha_i \varphi(g g_i)(v) \in W$$

which follows since for each $i \in \{1, \dots, n\}$ there is a $j \in \{1, \dots, n\}$ for which $g g_i = g_j$. In other words, the action of g on the element of W simply rearranges $\varphi(g_i)(v)$, and hence stays within W. This means that W is a G-stable subspace of V, and hence an $F[G]$-submodule of V which contains v. Clearly $\dim_F(W) \leq |G|$ since W is the span of precisely $|G|$ elements. ■

Exercise 18.1.5

Exercise 18.1.6 Write out the matrcies $\varphi(g)$ for every $g \in G$ for each of the following representations that were described in the second set of examples:

(a) the representation of S_3 described in Example 3 (let $n = 3$ in that example).
(b) the representation of D_8 described in Example 6 (i.e., let $n = 4$ in that example and write out the values of all the sines and cosines, for all group elements)
(c) the representation of Q_8 described in Example 7
(d) the representation of Q_8 described in Example 8.

Proof. (a)

$$\varphi((1)) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad \varphi((1\ 2)) = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

$$\varphi((1\ 3)) = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}, \quad \varphi((2\ 3)) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$$

$$\varphi((1\ 2\ 3)) = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \quad \varphi((1\ 3\ 2)) = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$$

(b) Since $n = 4$, we use the matrix R in Example 6 to compute:

$$\varphi(r) = \begin{pmatrix} \cos \pi/2 & -\sin \pi/2 \\ \sin \pi/2 & \cos \pi/2 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

Now we may determine every other $\varphi(g)$ for all $g \in D_8$. We have

$$\varphi(1) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \varphi(r) = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

$$\varphi(r^2) = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \quad \varphi(r^3) = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

$$\varphi(s) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \varphi(sr) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

$$\varphi(sr^2) = \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}, \quad \varphi(sr^3) = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$$

(c) The elements of Q_8 in the presentation given in Example 7 may be written as $1, i, i^2, i^3, j, ij, i^2j$, and i^3j. As such, we may find:

$$\varphi(1) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \varphi(i) = \begin{pmatrix} \sqrt{-1} & 0 \\ 0 & -\sqrt{-1} \end{pmatrix}$$

$$\varphi(j) = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad \varphi(ij) = \begin{pmatrix} 0 & -\sqrt{-1} \\ -\sqrt{-1} & 0 \end{pmatrix}$$

$$\varphi(i^2) = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \varphi(i^3) = \begin{pmatrix} -\sqrt{-1} & 0 \\ 0 & \sqrt{-1} \end{pmatrix}$$

$$\varphi(i^2 j) = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad \varphi(i^3 j) = \begin{pmatrix} 0 & \sqrt{-1} \\ \sqrt{-1} & 0 \end{pmatrix}$$

(d)

$$\varphi(1) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad \varphi(i) = \begin{pmatrix} 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

$$\varphi(j) = \begin{pmatrix} 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{pmatrix}, \quad \varphi(ij) = \begin{pmatrix} 0 & 0 & 0 & -1 \\ 0 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

$$\varphi(i^2) = \begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}, \quad \varphi(i^3) = \begin{pmatrix} 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 \end{pmatrix}$$

$$\varphi(i^2 j) = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \\ -1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}, \quad \varphi(i^3 j) = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & -1 & 0 & 0 \\ -1 & 0 & 0 & 0 \end{pmatrix}$$

■

Exercise 18.1.7 Let V be the 4-dimensional permutation module for S_4 described in Example 3 of the second set of examples. Let $\pi : D_8 \longrightarrow S_4$ be the permutation representation for D_8 obtained from the action of D_8 by left multiplication on the set of left cosets of its subgroup $\langle s \rangle$. Make V into an FD_8-module via π as described in Example 4 and write out the 4×4 matrices for r and s given by this representation with respect to the basis $e_1, \dots, e_4$.

Proof. We let D_8 act on $D_8/\langle s \rangle$ by left multiplication, i.e., $g \cdot h\langle s \rangle = gh\langle s \rangle$ for all $g, h \in D_8$. Fixing a labelling of the elements of $D_8/\langle s \rangle = \{\langle s \rangle, r\langle s \rangle, r^2\langle s \rangle, r^3\langle s \rangle\}$ by $\{1, 2, 3, 4\}$ in the usual sense, we obtain the permutation representation $\pi : D_8 \longrightarrow S_4$ given by

$$\pi(r) = (1\ 2\ 3\ 4) \quad \text{and} \quad \pi(s) = (2\ 4)$$

for instance since $r \cdot r^i\langle s\rangle = r^{i+1}\langle s\rangle$ and $s \cdot r^i\langle s\rangle = sr^i\langle s\rangle = r^{-i}s\langle s\rangle = r^{-i}\langle s\rangle$. Checking the values for each $i \in \{1, \ldots, 4\}$ gives us the above values for the permutation representation.

Now if V is the 4-dimensional permutation module for S_4 as mentioned, we have a representation $\varphi : S_4 \to \mathrm{GL}_4(F)$, and so may compose φ with π above to obtain a 4-dimensional representation of D_8, sufficing to make V into an $F[D_8]$-module. Specifically,

$$(\varphi \circ \pi)(r)(e_i) = e_{\pi(r)(i)} = e_{(1\,2\,3\,4)(i)}$$

$$(\varphi \circ \pi)(s)(e_i) = e_{\pi(s)(i)} = e_{(2\,4)(i)}$$

Computing some values for different i, we obtain matrices given by

$$(\varphi \circ \pi)(r) = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

$$(\varphi \circ \pi)(s) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

which was the desired computation. ∎

Exercise 18.1.8 Let V be the FS_n-module described in Example 3 and 10 in the second set of examples.
(a) Prove that if v is an element of V such that $\sigma \cdot v = v$ for all $\sigma \in S_n$ then v is an F-multiple of $e_1 + e_2 + \cdots + e_n$.
(b) Prove that if $n \geq 3$, then V has a unique 1-dimensional submodule, namely the submodule N consisting of all F-multiples of $e_1 + e_2 + \cdots + e_n$.

Proof. (a) Suppose $v \in V$ is such that $\sigma \cdot v = v$ for all $\sigma \in S_n$. Since $e_1, \ldots, e_n$ is an F-basis for V we may write $v = a_1e_1 + \cdots + a_ne_n$ for some $a_i \in F$, $1 \leq i \leq n$. Then our assumption states that

$$\sigma \cdot v = \sigma \cdot (a_1e_1 + \cdots + a_ne_n) = a_1e_{\sigma(1)} + \cdots a_ne_{\sigma(n)}$$

must be equal to $a_1e_1 + \cdots + a_ne_n$ for all $\sigma \in S_n$. In particular, we know that the permutation $\tau = (1\ \cdots\ n)$ is an element of S_n, and hence we have the equation:

$$a_1e_2 + a_2e_3 + \cdots + a_{n-1}e_n + a_ne_1 = a_1e_1 + a_2e_2 + \cdots + a_{n-1}e_{n-1} + a_ne_n$$

Subtracting the terms from the right hand side, and collecting scalars for each basis element, we obtain the following:

$$(a_1 - a_2)e_2 + (a_2 - a_3)e_3 + \cdots + (a_{n-1} - a_n)e_n + (a_n - a_1)e_1 = 0$$

In particular, since $e_1, \ldots, e_n$ is an F-basis for V, linear independence implies that each of the scalars above are equal to 0, so that $a_1 - a_2 = 0$ and $a_2 - a_3 = 0$ and so on until $a_n - a_1 = 0$. Thus we require $a_1 = a_2$, and $a_2 = a_3$, and so on until $a_n = a_1$. Clearly we can see that this implies $a_1 = a_2 = \cdots = a_n$, and hence our original element v must satisfy

$$v = a_1e_1 + \cdots + a_ne_n = \alpha e_1 + \cdots + \alpha e_n$$

where α is the common value of the a_i for $1 \le i \le n$. This means that v is a scalar multiple of $e_1 + \cdots + e_n$, which was the desired result.

(b) Now take $n \ge 3$. Let N be the submodule of V consisting of all F-multiples of $e_1 + \cdots + e_n$. Clearly N is 1-dimensional, for instance since it is spanned by one element of V. Now suppose M is some other 1-dimensional submodule of V. Then there exists some $x \in V$ for which $M = \text{span}(x)$. We may let $x = a_1e_1 + \cdots + a_ne_n$ for some $a_i \in F$, $1 \le i \le n$. Since M is a submodule, we know that it is an S_n-stable subspace of V, which in particular means that $\sigma \cdot x \in M$ for all $\sigma \in S_n$.

However note that elements of M are F-multiples of x, as $M = \text{span}(x)$. Since $\tau = (1\ n)$ is an element of S_n, we may thus write that $\tau \cdot x = \beta x$ for some $\beta \in F$. Since we have

$$\tau \cdot x = \tau \cdot (a_1e_1 + \cdots + a_ne_n) = a_1e_{\tau(1)} + \cdots + a_ne_{\tau(n)} = a_1e_n + a_2e_2 + \cdots + a_ne_1$$

we require that the following equation:

$$a_1e_n + a_2e_e + \cdots + a_{n-1}e_{n-1} + a_ne_1 = \beta a_1e_1 + \beta a_2e_2 + \cdots + \beta a_ne_n$$

holds true. Subtracting terms from the right hand side and collecting scalars via basis elements gives us the equation

$$(a_1 - \beta a_n)e_n + (a_2 - \beta a_2)e_2 + \cdots + (a_{n-1} - \beta a_{n-1})e_{n-1} + (a_n - \beta a_1)e_1 = 0$$

and since $e_1, \ldots, e_n$ is an F-basis for V, linear independence means that each of the scalars above is equal to 0, hence that $a_1 - \beta a_n = 0$ and $a_2 - \beta a_2 = 0$ and so on until $a_n - \beta a_1 = 0$. Thus we must have $a_i = \beta a_i$ for all $i \in \{2, \ldots, n-1\}$ and $a_1 = \beta a_n$ and $a_n = \beta a_1$.

Since $a_1 = \beta a_n$ and $a_n = \beta a_1$, we know that $a_1/a_n = \beta = a_n/a_1$ must hold true, where we may divide since $a_1, a_n \in F$ which is a field. Hence $a_1^2 = a_n^2$ holds true, and subtracting and factoring yields $a_1^2 - a_n^2 = (a_1 + a_n)(a_1 - a_n) = 0$. Since F is a field, in particular an integral domain, one of $a_1 + a_n$ or $a_1 - a_n$ must equal 0.

If $a_1 - a_n = 0$ then $a_1 = a_n$ and we have $\beta = 1$. Alternatively, if $a_1 + a_n = 0$ then $a_1 = -a_n$ and so $x = -a_n e_1 + a_n e_n$ must hold.

Now since $\tau \cdot x = -a_n e_1 + a_n e_n$ must be equal to $\beta x = -\beta a_n e_1 + \beta a_n e_n$ it follows that

$$\tau \cdot x - \beta x = (-a_n + \beta a_n)e_1 + (a_n - \beta a_n)e_n = 0$$

and since e_1 and e_2 are linearly independent, as elements of a basis for V over F, we require that $-a_n + \beta a_n = 0$ and $a_n - \beta a_n = 0$, which means $a_n = \beta a_n$. If $a_n = 0$ then we have that $x = 0$, which is a contradiction for then $\dim_F(M) = 0$ and we assumed that $M = \operatorname{span}(x)$ had dimension 1. Thus $a_n \neq 0$ which implies that $\beta = 1$ must hold.

In particular, we have shown that $\tau \cdot x = \beta x = x$ must hold. Note, however, that the transposition τ was not special to the above work, i.e., the above result holds without loss of generality for any transposition $\sigma \in S_n$.

Recall that every element of S_n may be written as a product of transpositions. Thus if $\sigma \in S_n$ is arbitrary then $\sigma = \tau_1 \circ \cdots \circ \tau_k$ for transpositions $\tau_i \in S_n$, $1 \leq i \leq k$. In particular, our above work shows that

$$\sigma \cdot x = (\tau_1 \circ \cdots \circ \tau_k) \cdot x = (\tau_1 \circ \cdots \circ \tau_{k-1}) \cdot (\tau_k \cdot x) = (\tau_1 \circ \cdots \circ \tau_{k-1}) \cdot x$$

and so on until eventually we find $\sigma \cdot x = x$. Thus, by part (a) above, since $\sigma \cdot x = x$ for all $\sigma \in S_n$, we have that x is a multiple of $e_1 + \cdots + e_n$, and hence that

$$W = \operatorname{span}(x) = \operatorname{span}(e_1 + \cdots + e_n) = N$$

proving the uniqueness of the 1-dimensional submodule N of V, as desired. ■

Exercise 18.1.9 Prove that the 4-dimensional representation of Q_8 on $\mathbb{H}$ described in Example 8 in the second set of examples is irreducible. [Show that any Q_8-stable subspace is a left ideal.]

Proof. Let $\varphi : Q_8 \to GL_4(\mathbb{R})$ be the 4-dimensional representation of Q_8 on $\mathbb{H}$ induced by left multiplication by elements of Q_8 on $\mathbb{H}$. Suppose V is a non-zero proper $\mathbb{R}[Q_8]$-submodule of $\mathbb{H}$. That is, we have $V \neq 0$ and $V \neq \mathbb{H}$. In particular, V is a Q_8-stable subspace of $\mathbb{H}$.

Let $\alpha = x + yi + zj + wk$ be an arbitrary element of $\mathbb{H}$, where $x, y, z, w \in \mathbb{R}$. Since $V \neq 0$, there exists some $v \in V$ such that $v \neq 0$. Observe that:

$$\begin{aligned}
\alpha v &= (x + yi + zj + wk)v \\
&= xv + (yi)v + (zj)v + (wk)v \\
&= xv + i(yv) + j(zv) + k(wv)
\end{aligned}$$

Since V contains v, we know all $\mathbb{R}$-multiples of v are contained in V. As such, we have that $yv, zv, wv \in V$. Note now that since V is Q_8-stable, we require $g \cdot w = gw \in V$ for all $g \in Q_8$ and all $w \in V$. In particular, since $i, j, k \in Q_8$ and $yv, zv, wv \in V$, this means that each of $i(yv)$, $j(zv)$, and $k(wv)$ are elements of V. Since subspaces are closed under addition, we know that the sum $xv + i(yv) + j(zv) + k(wv)$ also lies in V. In particular this means that $\alpha v \in V$ must hold, and since $\alpha \in \mathbb{H}$ was arbitrary, we have shown that V is a left ideal of $\mathbb{H}$ considered as a ring. But then since $v \in V \subseteq \mathbb{H}$, we know that $v^{-1} \in \mathbb{H}$, since $\mathbb{H}$ is a division ring, and hence by closure under left multiplication we have $v^{-1}v = 1 \in V$, which forces $V = \mathbb{H}$, contradictory to our assumption. Hence the representation φ above is irreducible, as the only $\mathbb{R}[Q_8]$-submodules of $\mathbb{H}$ are 0 and $\mathbb{H}$. ∎

Exercise 18.1.10

Exercise 18.1.11

Exercise 18.1.12

Exercise 18.1.13 Let R be a ring and let M and N be simple (i.e., irreducible) R-modules.
(a) Prove that every nonzero R-module homomorphism from M to N is an isomorphism. [Consider its kernel and image]
(b) Prove Schur's Lemma: if M is a simple R-module then $\mathrm{Hom}_R(M, M)$ is a division ring (recall that $\mathrm{Hom}_R(M, M)$ is the ring of all R-module homomorphisms from M to M, where multiplication in this ring is function composition).

Proof. (a) Suppose $\varphi : M \to M$ is a non-zero R-module homomorphism. Since M is simple, the only R-submodules of M are $\{0\}$ and M. Since $\ker\varphi$ is an R-submodule of M, and $\varphi \neq 0$, we have $\ker\varphi = \{0\}$; hence φ is injective. Also, $\varphi(M)$ is an R-submodule of N, and since $\varphi \neq 0$ we have $\varphi(M) = N$; hence φ is surjective.

(b) Suppose M is a simple R-module. Take a non-zero $\varphi \in \mathrm{Hom}_R(M, M)$. From part (a) we know that φ is an isomorphism; hence $\varphi^{-1} \in \mathrm{Hom}_R(M, M)$. Thus every non-zero element of the ring $\mathrm{Hom}_R(M, M)$ has an inverse, and so $\mathrm{Hom}_R(M, M)$ is a division ring. ∎

Exercise 18.1.14 Let $\varphi : G \to \mathrm{GL}(V)$ be a representation of G. The *centralizer* of φ is defined to be the set of all linear transformations, A, from V to itself such that $A\varphi(g) = \varphi(g)A$ for all $g \in G$ (i.e., the linear transformations of V which commute with all $\varphi(g)$'s).
(a) Prove that a linear transformation A from V to V is in the centralizer of φ if and only

if it is an FG-module homomorphism from V to itself (so the centralizer of φ is the same as the *ring* $\mathrm{Hom}_{FG}(V, V)$).
(b) Show that if z is in the center of G then $\varphi(z)$ is in the centralizer of φ.
(c) Assume φ is an irreducible representation (so V is a simple FG-module). Prove that if H is any finite *abelian* subgroup of $\mathrm{GL}(V)$ such that $A\varphi(g) = \varphi(g)A$ for all $A \in H$ then H is cyclic (in other words, any finite abelian subgroup of the multiplicative group of units in the ring $\mathrm{Hom}_{FG}(V, V)$ is cyclic). [By the preceding exercise, $\mathrm{Hom}_{FG}(V, V)$ is a division ring, so this reducies to proving that a finite abelian subgroup of the multiplicative group of nonzero elements in a division ring is cyclic. Show that the division subring generated by an abelian subgroup of any division ring is a field and use Proposition 18, Section 9.5.]
(d) Show that if φ is a faithful irreducible representation then the center of G is cyclic.
(e) Deduce from (d) that if G is abelian and φ is any irreducible representation then $G/\ker\varphi$ is cyclic.

Proof. (a) Suppose the linear transformation $A : V \to V$ is in the centralizer of φ. We must show that A preserves the $F[G]$-module structure of V. To this end, observe that:

$$\begin{aligned}
A\left(\sum_{g\in G} \alpha_g [g] \cdot v\right) &= A\left(\sum_{g\in G} \alpha_g \varphi(g)(v)\right) \\
&= \sum_{g\in G} \alpha_g A(\varphi(g)(v)) \\
&= \sum_{g\in G} \alpha_g (A \circ \varphi(g))(v) \\
&= \sum_{g\in G} \alpha_g (\varphi(g) \circ A)(v) \\
&= \sum_{g\in G} \alpha_g \varphi(g)(A(v)) \\
&= \sum_{g\in G} \alpha_g [g] \cdot A(v)
\end{aligned}$$

where the second equality follows from the first since A is F-linear, and the fourth equality follows from the third by the fact that A lies in the centralizer of φ. The other verifications that A is an $F[G]$-module homomorphism follow immediately via A being a linear transformation from V to V.

Conversely, if A is an $F[G]$-module homomorphism from V to V then recalling that $\varphi(g)(v) = g \cdot v$ for any $v \in V$ and $g \in G$, we may note that

$$\begin{aligned}(A \circ \varphi(g))(v) &= A(\varphi(g)(v)) \\ &= A(g \cdot v) \\ &= g \cdot A(v) \\ &= \varphi(g)(A(v)) \\ &= (\varphi(g) \circ A)(v)\end{aligned}$$

must hold, where the third equality follows from the second since A is an $F[G]$-module homomorphism. The above proves that A lies in the centralizer of φ, and obviously A is a linear tranformation from $V \to V$ (since it is already $F[G]$-linear, and hence F-linear).

(b) Suppose $z \in Z(G)$, the center of G. Then, in particular, $zg = gz$ for all $g \in G$, and hence

$$\begin{aligned}(\varphi(g) \circ \varphi(z))(v) &= \varphi(g)(\varphi(z)(v)) \\ &= g \cdot (z \cdot v) \\ &= (gz) \cdot v \\ &= (zg) \cdot v \\ &= z \cdot (g \cdot v) \\ &= \varphi(z)(\varphi(g)(v)) \\ &= (\varphi(z) \circ \varphi(g))(v)\end{aligned}$$

where lines two through five follow since $G \times V \to V$ defined by $(g, v) \mapsto \varphi(g)(v)$ is a group action, and so the axioms for a group action hold. Hence $\varphi(z)$ is in the centralizer of φ, as desired.

(c) Assume φ is an irreducible representation of G on V over F.

Then, in particular, V is a simple $F[G]$-module, and hence by Exercise 18.1.13(b), Schur's Lemma, we know that $\mathrm{Hom}_{F[G]}(V, V)$ is a division ring,

Take H to be a finite abelian subgroup of $\mathrm{GL}(V)$ such that $A\varphi(g) = \varphi(g)A$ for all $A \in H$ and all $g \in G$. In particular, we know that A is in the centralizer of φ for all $A \in H$, and hence all $A \in H$ lie inside $\mathrm{Hom}_{F[G]}(V, V)$ since this ring coincides with the centralizer of φ.

Consider the subring of $\mathrm{Hom}_{F[G]}(V, V)$ generated by H, call it S. Note that S is, in particular, a division ring itself, and moreover since H is abelian, so we must have that all multiplication in S is commutative. Hence S is a field, and since H is a finite subgroup of S, Proposition 18 in Section 9.5 asserts that H is cyclic.

(d) Suppose φ is a faithful irreducible representation of G on V over F. Since

G is a finite, we know that the center of G, $Z(G)$, is finite as well. Moreover, part (b) above states that for any $z \in Z(G)$ we have that $\varphi(z)$ lies in the centralizer of φ. Thus the set

$$H = \{\varphi(z) \mid z \in Z(G)\}$$

lies in the centralizer of φ, which coincides with the ring $\text{Hom}_{F[G]}(V, V)$, and it is clear immediately that H is a finite (since $Z(G)$ is finite) abelian subgroup of $\text{Hom}_{F[G]}(V, V)$ since any other linear transformation in the centralizer must commute with any element of H by design.

Thus by part (c) above, we know that H must be cyclic, say with generator $\varphi(w)$ for some $w \in Z(G)$. Now we can see that $\varphi(z) = \varphi(w)^k$ for some $k \in \mathbb{Z}^+$, and hence $\varphi(z) = \varphi(w^k)$, and since φ is injective (since φ is faithful) this implies that $z = w^k$. However this means that any element of $Z(G)$ is a power of w, and hence $Z(G) = \langle w \rangle$ is a cyclic group, as desired.

(e) Now suppose G is abelian and $\varphi : G \to \text{GL}(V)$ is an irreducible representation of G. on V over F. Then $\varphi : G/\ker\varphi \to \text{GL}(V)$ is a faithful representation of $G/\ker\varphi$. Moreover, φ is an irreducible representation of $G/\ker\varphi$ as well since if this were not the case then V would have some non-trivial $F[G/\ker\varphi]$-submodule, say W, which would also necessarily be a non-trivial $F[G]$-submodule (note that $g \cdot v = \varphi(g)(v) = 0$ for all $g \in \ker\varphi$).

Thus φ is an irreducible faithful representation of $G/\ker\varphi$. In fact, since G is abelian, we know that $G = Z(G)$, and also that $G/\ker\varphi$ is abelian as well, hence $Z(G/\ker\varphi) = G/\ker\varphi$. Hence by part (d) above we know that $G/\ker\varphi$ is cyclic. ■

Exercise 18.1.15 Exhibit all 1-dimensional complex representations of a finite cyclic group; make sure to decide which are inequivalent.

Proof. Let G be a finite cyclic group, so that $G = \langle g \rangle \cong Z_n$ for some $n \in \mathbb{Z}^+$. Recall that the 1-dimensional complex representations of G are precisely those group homomorphisms $\varphi : G \to \text{GL}_1(\mathbb{C}) \cong \mathbb{C}^\times$. If φ is such a group homomorphism, then since $g^n = 1$ we require that $\varphi(g)^n = 1$. In other words, $\varphi(g)$ is an nth root of unity in $\mathbb{C}^\times$. Recall that there are n such roots of unity, and hence we have n different representations of G on $\mathbb{C}$.

We shall fix a labelling $\zeta_1, \ldots, \zeta_n$ to denote the n different nth roots of unity, and denote by φ_i the representation taking g to ζ_i.

To determine which of these representations are equivalent, or inequivalent, we recall that two representations φ and ψ are equivalent if and only if there exists $\beta \in \text{GL}_1(\mathbb{C}) \cong \mathbb{C}^\times$ such that $\beta\varphi(g)\beta^{-1} = \psi(g)$.

In our present case, note that if $i \neq j$ then for any $\beta \in \mathbb{C}^\times$ we have $\beta\varphi_i(g)\beta^{-1} = \beta\beta^{-1}\varphi_i(g) \neq \varphi_j(g)$ by commutativity of multiplication in $\mathbb{C}^\times$. Thus any two of the n representations φ_i above are inequivalent. ■

Exercise 18.1.16 Exhibit all 1-dimensional complex representations of a finite abelian group. Deduce that the number of inequivalent degree 1 complex representations of a finite abelian group equals the order of the group. [First decompose the abelian group into a direct product of cyclic groups, then use the preceding exercise.]

Proof. Suppose A is a finite abelian group. Decomposing A into a direct product of cyclic groups, we may write $A \cong C_1 \times \cdots \times C_n$ where $|C_i| = |\langle g_i \rangle| = d_i$ for integers $d_i \in \mathbb{Z}^+$, $1 \leq i \leq n$. The 1-dimensional complex representations of A are group homomorphisms $\varphi : A \to \mathrm{GL}_1(\mathbb{C}) \cong \mathbb{C}^\times$, and so to determine such homomorphisms we need to send generators for each of the cyclic groups making up the direct product to some elements of $\mathbb{C}^\times$.

As in Exercise 18.1.15 above, we may map each the generators g_i of C_i to the primitive d_ith roots of unity in $\mathbb{C}^\times$, of which there are d_i. This gives d_i possible homomorphisms from each C_i to $\mathbb{C}^\times$, and hence $d_1 \cdots d_n$ possible homomorphisms from A to $\mathbb{C}^\times$. Moreover, each of these representations are inequivalent for the same reasons discussed in Exercise 18.1.15. Thus there are a total of $|A| = |C_1| \cdots |C_n|$ inequivalent $\mathbb{C}$-representations of A. ■

Exercise 18.1.17

Exercise 18.1.18

Exercise 18.1.19

Exercise 18.1.20

Exercise 18.1.21

Exercise 18.1.22

Exercise 18.1.23

Exercise 18.1.24

18.2 Wedderburn's Theorem and Some Consequences

Exercise 18.2.1

Exercise 18.2.2

Exercise 18.2.3

Exercise 18.2.4

Exercise 18.2.5

Exercise 18.2.6

Exercise 18.2.7

Exercise 18.2.8

Exercise 18.2.9

Exercise 18.2.10

Exercise 18.2.11

Exercise 18.2.12

Exercise 18.2.13

Exercise 18.2.14

Exercise 18.2.15

Exercise 18.2.16

Exercise 18.2.17

Exercise 18.2.18

18.3 Character Theory and the Orthogonality Relations

Exercise 18.3.1

Exercise 18.3.2

Exercise 18.3.3

Exercise 18.3.4

Exercise 18.3.5

Exercise 18.3.6

Exercise 18.3.7

Exercise 18.3.8

Exercise 18.3.9

Exercise 18.3.10

Exercise 18.3.11

Exercise 18.3.12

Exercise 18.3.13

Exercise 18.3.14

Exercise 18.3.15

Exercise 18.3.16

Exercise 18.3.17

Exercise 18.3.18

Exercise 18.3.19

Exercise 18.3.20

Exercise 18.3.21

Exercise 18.3.22

Exercise 18.3.23

Exercise 18.3.24

Exercise 18.3.25

Exercise 18.3.26

Exercise 18.3.27

Exercise 18.3.28

❈ Examples and Applications of Character Theory

19.1 Characters of Groups of Small Order

Exercise 19.1.1

Exercise 19.1.2

Exercise 19.1.3

Exercise 19.1.4

Exercise 19.1.5

Exercise 19.1.6

Exercise 19.1.7

Exercise 19.1.8

Exercise 19.1.9

Exercise 19.1.10

Exercise 19.1.11

Exercise 19.1.12

Exercise 19.1.13

Exercise 19.1.14

Exercise 19.1.15

Exercise 19.1.16

Exercise 19.1.17

19.2 Theorems of Burnside and Hall

Exercise 19.2.1

Exercise 19.2.2

Exercise 19.2.3

Exercise 19.2.4

Exercise 19.2.5

19.3 Introduction to the Theory of Induced Characters

Exercise 19.3.1

Exercise 19.3.2

Exercise 19.3.3

Exercise 19.3.4

Exercise 19.3.5

Exercise 19.3.6

Exercise 19.3.7

Exercise 19.3.8

Exercise 19.3.9

Exercise 19.3.10

Exercise 19.3.11

Exercise 19.3.12

Exercise 19.3.13

Exercise 19.3.14

Exercise 19.3.15

❋ Appendix I

20.1 Cartesian Products

20.2 Partially Ordered Sets and Zorn's Lemma

❋ Appendix II

21.1 Categories and Functors

21.2 Natural Transformations and Universals