Exercises from *Abstract Algebra* by David Dummit and Richard Foote

Exercise 1.1.2a Prove the the operation $\star$ on $\mathbb{Z}$ defined by $a \star b = a - b$ is not commutative.

Proof. Not commutative since

$$1 \star (-1) = 1 - (-1) = 2$$

$$(-1) \star 1 = -1 - 1 = -2.$$

$\square$

Exercise 1.1.3 Prove that the addition of residue classes $\mathbb{Z}/n\mathbb{Z}$ is associative.

Proof. We have

$$\begin{aligned}
(\bar{a} + \bar{b}) + \bar{c} &= \overline{a + b} + \bar{c} \\
&= \overline{(a + b) + c} \\
&= \overline{a + (b + c)} \\
&= \bar{a} + \overline{b + c} \\
&= \bar{a} + (\bar{b} + \bar{c})
\end{aligned}$$

since integer addition is associative. $\square$

Exercise 1.1.4 Prove that the multiplication of residue class $\mathbb{Z}/n\mathbb{Z}$ is associative.

Proof. We have

$$\begin{aligned}
(\bar{a} \cdot \bar{b}) \cdot \bar{c} &= \overline{a \cdot b} \cdot \bar{c} \\
&= \overline{(a \cdot b) \cdot c} \\
&= \overline{a \cdot (b \cdot c)} \\
&= \bar{a} \cdot \overline{b \cdot c} \\
&= \bar{a} \cdot (\bar{b} \cdot \bar{c})
\end{aligned}$$

since integer multiplication is associative. $\square$

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

Proof. Note that since $n > 1, \overline{1} \neq \overline{0}$. Now suppose $\mathbb{Z}/(n)$ contains a multiplicative identity element $\bar{e}$. Then in particular,

$$\bar{e} \cdot \overline{1} = \overline{1}$$

so that $\bar{e} = \overline{1}$. Note, however, that

$$\overline{0} \cdot \bar{k} = \overline{0}$$

for all k, so that $\overline{0}$ does not have a multiplicative inverse. Hence $\mathbb{Z}/(n)$ is not a group under multiplication. □

Exercise 1.1.15 Prove that $(a_1 a_2 \dots a_n)^{-1} = a_n^{-1} a_{n-1}^{-1} \dots a_1^{-1}$ for all $a_1, a_2, \dots, a_n \in G$.

Proof. For $n = 1$, note that for all $a_1 \in G$ we have $a_1^{-1} = a_1^{-1}$. Now for $n \geq 2$ we proceed by induction on n. For the base case, note that for all $a_1, a_2 \in G$ we have

$$(a_1 \cdot a_2)^{-1} = a_2^{-1} \cdot a_1^{-1}$$

since

$$a_1 \cdot a_2 \cdot a_2^{-1} a_1^{-1} = 1.$$

For the inductive step, suppose that for some $n \geq 2$, for all $a_i \in G$ we have

$$(a_1 \cdot \dots \cdot a_n)^{-1} = a_n^{-1} \cdot \dots \cdot a_1^{-1}.$$

Then given some $a_{n+1} \in G$, we have

$$\begin{aligned}(a_1 \cdot \dots \cdot a_n \cdot a_{n+1})^{-1} &= ((a_1 \cdot \dots \cdot a_n) \cdot a_{n+1})^{-1} \\ &= a_{n+1}^{-1} \cdot (a_1 \cdot \dots \cdot a_n)^{-1} \\ &= a_{n+1}^{-1} \cdot a_n^{-1} \cdot \dots \cdot a_1^{-1},\end{aligned}$$

using associativity and the base case where necessary. □

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. ($\Rightarrow$) Suppose $x^2 = 1$. Then we have $0 < |x| \leq 2$, i.e., $|x|$ is either 1 or 2 . ($\Leftarrow$) If $|x| = 1$, then we have $x = 1$ so that $x^2 = 1$. If $|x| = 2$ then $x^2 = 1$ by definition. So if $|x|$ is 1 or 2 , we have $x^2 = 1$. □

Exercise 1.1.17 Let x be an element of G. Prove that if $|x| = n$ for some positive integer n then $x^{-1} = x^{n-1}$.

Proof. We have $x \cdot x^{n-1} = x^n = 1$, so by the uniqueness of inverses $x^{-1} = x^{n-1}$. □

Exercise 1.1.18 Let x and y be elements of G. Prove that $xy = yx$ if and only if $y^{-1}xy = x$ if and only if $x^{-1}y^{-1}xy = 1$.

Exercise 1.1.20 For x an element in G show that x and x^{-1} have the same order.

Proof. Recall that the order of a group element is either a positive integer or infinity. Suppose $|x|$ is infinite and that $\left|x^{-1}\right| = n$ for some n. Then

$$x^n = x^{(-1)\cdot n\cdot(-1)} = \left(\left(x^{-1}\right)^n\right)^{-1} = 1^{-1} = 1,$$

a contradiction. So if $|x|$ is infinite, $\left|x^{-1}\right|$ must also be infinite. Likewise, if $\left|x^{-1}\right|$ is infinite, then $\left|\left(x^{-1}\right)^{-1}\right| = |x|$ is also infinite. Suppose now that $|x| = n$ and $\left|x^{-1}\right| = m$ are both finite. Then we have

$$\left(x^{-1}\right)^n = \left(x^n\right)^{-1} = 1^{-1} = 1,$$

so that $m \leq n$. Likewise, $n \leq m$. Hence $m = n$ and x and x^{-1} have the same order. $\square$

Exercise 1.1.22a If x and g are elements of the group G, prove that $|x| = \left|g^{-1}xg\right|$.

Proof. First we prove a technical lemma:

Lemma. For all $a, b \in G$ and $n \in \mathbb{Z}$, $\left(b^{-1}ab\right)^n = b^{-1}a^nb$. The statement is clear for $n = 0$. We prove the case $n > 0$ by induction; the base case $n = 1$ is clear. Now suppose $\left(b^{-1}ab\right)^n = b^{-1}a^nb$ for some $n \geq 1$; then

$$\left(b^{-1}ab\right)^{n+1} = \left(b^{-1}ab\right)\left(b^{-1}ab\right)^n = b^{-1}abb^{-1}a^nb = b^{-1}a^{n+1}b.$$

By induction the statement holds for all positive n. Now suppose $n < 0$; we have

$$\left(b^{-1}ab\right)^n = \left(\left(b^{-1}ab\right)^{-n}\right)^{-1} = \left(b^{-1}a^{-n}b\right)^{-1} = b^{-1}a^nb.$$

Hence, the statement holds for all integers n. Now to the main result. Suppose first that $|x|$ is infinity and that $\left|g^{-1}xg\right| = n$ for some positive integer n. Then we have

$$\left(g^{-1}xg\right)^n = g^{-1}x^ng = 1,$$

and multiplying on the left by g and on the right by g^{-1} gives us that $x^n = 1$, a contradiction. Thus if $|x|$ is infinity, so is $\left|g^{-1}xg\right|$. Similarly, if $\left|g^{-1}xg\right|$ is infinite and $|x| = n$, we have

$$\left(g^{-1}xg\right)^n = g^{-1}x^ng = g^{-1}g = 1,$$

a contradiction. Hence if $\left|g^{-1}xg\right|$ is infinite, so is $|x|$. Suppose now that $|x| = n$ and $\left|g^{-1}xg\right| = m$ for some positive integers n and m. We have

$$\left(g^{-1}xg\right)^n = g^{-1}x^n g = g^{-1}g = 1,$$

So that $m \leq n$, and

$$\left(g^{-1}xg\right)^m = g^{-1}x^m g = 1,$$

so that $x^m = 1$ and $n \leq m$. Thus $n = m$. □

Exercise 1.1.22b Deduce that $|ab| = |ba|$ for all $a, b \in G$.

Proof. Let a and b be arbitrary group elements. Letting $x = ab$ and $g = a$, we see that

$$|ab| = \left|a^{-1}aba\right| = |ba|.$$

□

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

Proof. Solution: Note that since $x^2 = 1$ for all $x \in G$, we have $x^{-1} = x$. Now let $a, b \in G$. We have

$$ab = (ab)^{-1} = b^{-1}a^{-1} = ba.$$

Thus G is abelian. □

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

Proof. ($\Rightarrow$) Suppose $a_1, a_2 \in A$ and $b_1, b_2 \in B$. Then

$$(a_1a_2, b_1b_2) = (a_1, b_1) \cdot (a_2, b_2) = (a_2, b_2) \cdot (a_1, b_1) = (a_2a_1, b_2b_1).$$

Since two pairs are equal precisely when their corresponding entries are equal, we have $a_1a_2 = a_2a_1$ and $b_1b_2 = b_2b_1$. Hence A and B are abelian. ($\Leftarrow$) Suppose $(a_1, b_1), (a_2, b_2) \in A \times B$. Then we have

$$(a_1, b_1) \cdot (a_2, b_2) = (a_1a_2, b_1b_2) = (a_2a_1, b_2b_1) = (a_2, b_2) \cdot (a_1, b_1).$$

Hence $A \times B$ is abelian. □

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. Solution: Suppose to the contrary that $x^a = x^b$ for some $0 \leq a < b \leq n - 1$. Then we have $x^{b-a} = 1$, with $1 \leq b - a < n$. However, recall that n is by definition the least integer k such that $x^k = 1$, so we have a contradiction. Thus all the x^i, $0 \leq i \leq n - 1$, are distinct. In particular, we have

$$\left\{x^i \mid 0 \leq i \leq n - 1\right\} \subseteq G,$$

so that $|x| = n \leq |G|$ □

Exercise 1.3.8 Prove that if $\Omega = \{1, 2, 3, \ldots\}$ then S_Ω is an infinite group

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

Proof. Solution: Recall from Exercise 1.6.2 that isomorphic groups necessarily have the same number of elements of order n for all finite n.

Now let $x \in \mathbb{R}^\times$. If $x = 1$ then $|x| = 1$, and if $x = -1$ then $|x| = 2$. If (with bars denoting absolute value) $|x| < 1$, then we have

$$1 > |x| > \left|x^2\right| > \cdots,$$

and in particular, $1 > |x^n|$ for all n. So x has infinite order in $\mathbb{R}^\times$. Similarly, if $|x| > 1$ (absolute value) then x has infinite order in $\mathbb{R}^\times$. So $\mathbb{R}^\times$has 1 element of order 1,1 element of order 2 , and all other elements have infinite order. In $\mathbb{C}^\times$, on the other hand, i has order 4 . Thus $\mathbb{R}^\times$and $\mathbb{C}^\times$are not isomorphic. $\square$

Exercise 1.6.11 Let A and B be groups. Prove that $A \times B \cong B \times A$.

Proof. Solution: We know from set theory that the mapping $\varphi : A \times B \to B \times A$ given by $\varphi((a, b)) = (b, a)$ is a bijection with inverse $\psi : B \times A \to A \times B$ given by $\psi((b, a)) = (a, b)$. Also φ is a homomorphism, as we show below. Let $a_1, a_2 \in A$ and $b_1, b_2 \in B$. Then

$$\begin{aligned}
\varphi\left((a_1, b_1) \cdot (a_2, b_2)\right) &= \varphi\left((a_1 a_2, b_1 b_2)\right) \\
&= (b_1 b_2, a_1 a_2) \\
&= (b_1, a_1) \cdot (b_2, a_2) \\
&= \varphi\left((a_1, b_1)\right) \cdot \varphi\left((a_2, b_2)\right)
\end{aligned}$$

Hence $A \times B \cong B \times A$. $\square$

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. $(\Rightarrow)$ Suppose G is abelian. Then

$$\varphi(ab) = (ab)^{-1} = b^{-1}a^{-1} = a^{-1}b^{-1} = \varphi(a)\varphi(b),$$

so that φ is a homomorphism. $(\Leftarrow)$ Suppose φ is a homomorphism, and let $a, b \in G$. Then

$$ab = \left(b^{-1}a^{-1}\right)^{-1} = \varphi\left(b^{-1}a^{-1}\right) = \varphi\left(b^{-1}\right)\varphi\left(a^{-1}\right) = \left(b^{-1}\right)^{-1}\left(a^{-1}\right)^{-1} = ba,$$

so that G is abelian. $\square$

Exercise 1.6.23 Let G be a finite group which possesses an automorphism σ 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.

Proof. Solution: We define a mapping $f : G \to G$ by $f(x) = x^{-1}\sigma(x)$. Claim: f is injective. Proof of claim: Suppose $f(x) = f(y)$. Then $y^{-1}\sigma(y) = x^{-1}\sigma(x)$, so that $xy^{-1} = \sigma(x)\sigma\left(y^{-1}\right)$, and $xy^{-1} = \sigma\left(xy^{-1}\right)$. Then we have $xy^{-1} = 1$, hence $x = y$. So f is injective.

Since G is finite and f is injective, f is also surjective. Then every $z \in G$ is of the form $x^{-1}\sigma(x)$ for some x. Now let $z \in G$ with $z = x^{-1}\sigma(x)$. We have

$$\sigma(z) = \sigma\left(x^{-1}\sigma(x)\right) = \sigma(x)^{-1}x = \left(x^{-1}\sigma(x)\right)^{-1} = z^{-1}.$$

Thus σ is in fact the inversion mapping, and we assumed that σ is a homomorphism. By a previous example, then, G is abelian. □

Exercise 1.7.5 Prove that the kernel of an action of the group G on a set A is the same as the kernel of the corresponding permutation representation $G \to S_A$.

Proof. Solution: Let G be a group acting on A. The kernel of the action is the set

$$K = \{g \in G \mid g \cdot a = a \text{ for all } a \in A\}.$$

The corresponding permutation representation is a group homomorphism $\varphi : G \to S_A$ given by $\varphi(g)(a) = g \cdot a$, and by definition

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

$K \subseteq \ker\varphi :$ Let $k \in K$. Then for all $a \in A$, we have

$$\varphi(k)(a) = k \cdot a = a,$$

so that

$$\varphi(k) = \mathrm{id}_A = 1.$$

Thus $g \in \ker\varphi$. $\ker\varphi \subseteq K :$ Let $k \in \ker\varphi$. Then for all $a \in A$, we have

$$k \cdot a = \varphi(k)(a) = \mathrm{id}_A(a) = a.$$

Thus $k \in K$. □

Exercise 1.7.6 Prove that a group G acts faithfully on a set A if and only if the kernel of the action is the set consisting only of the identity.

Proof. Solution: We know that a group action is faithful precisely when the corresponding permutation representation $\varphi : G \to S_A$ is injective. Moreover, a group homomorphism is injective precisely when its kernel is trivial. The kernel of a group action is equal to the kernel of the corresponding permutation representation. So G acts faithfully on A if and only if the kernel of the action is trivial. □

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

Proof. Solution: Under these conditions, there exists a nonidentity element $x \in H$ and an element $y \notin H$. Consider the product xy. If $xy \in H$, then since $x^{-1} \in H$ and H is a subgroup, $y \in H$, a contradiction. If $xy \notin H$, then we have $xy = y$. Thus $x = 1$, a contradiction. Thus no such subgroup exists. □

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. Solution: First, suppose there does not exist a nonzero element in H. Then $H = 0$. Now suppose there does exist a nonzero element $a \in H$; without loss of generality, say $a = p/q$ in lowest terms for some integers p and q - that is, $\gcd(p, q) = 1$. Now $q \cdot \frac{p}{q} = p \in H$, and since $q/p \in H$, we have $p \cdot \frac{q}{p} \in H$. There exist integers x, y such that $qx + py = 1$; note that $qx \in H$ and $py \in H$, so that $1 \in H$. Thus $n \in H$ for all $n \in \mathbb{Z}$. Moreover, if $n \neq 0, 1/n \in H$. Then $m/n \in H$ for all integers m, n with $n \neq 0$; hence $H = \mathbb{Q}$. □

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

Exercise 2.4.13 Prove that the multiplicative group of positive rational numbers is generated by the set $\left\{\frac{1}{p} \mid p \text{ is a prime}\right\}$.

Exercise 2.4.16a A subgroup M of a group G is called a maximal subgroup if $M \neq G$ and the only subgroups of G which contain M are M and G. Prove that if H is a proper subgroup of the finite group G then there is a maximal subgroup of G containing H.

Exercise 2.4.16b Show that the subgroup of all rotations in a dihedral group is a maximal subgroup.

Exercise 2.4.16c Show that if $G = \langle x \rangle$ is a cyclic group of order $n \geq 1$ then a subgroup H is maximal if and only $H = \langle x^p \rangle$ for some prime p dividing n.

Exercise 3.1.3a Let A be an abelian group and let B be a subgroup of A. Prove that A/B is abelian.

Proof. Lemma: Let G be a group. If $|G| = 2$, then $G \cong Z_2$. Proof: Since $G = \{ea\}$ has an identity element, say e, we know that $ee = e, ea = a$, and $ae = a$. If $a^2 = a$, we have $a = e$, a contradiction. Thus $a^2 = e$. We can easily see that $G \cong Z_2$.

If A is abelian, every subgroup of A is normal; in particular, B is normal, so A/B is a group. Now let $xB, yB \in A/B$. Then

$$(xB)(yB) = (xy)B = (yx)B = (yB)(xB).$$

Hence A/B is abelian. $\square$

Exercise 3.1.22a Prove that if H and K are normal subgroups of a group G then their intersection $H \cap K$ is also a normal subgroup of G.

Exercise 3.1.22b Prove that the intersection of an arbitrary nonempty collection of normal subgroups of a group is a normal subgroup (do not assume the collection is countable).

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. Solution: Let $|H| = p$ and $|K| = q$. We saw in a previous exercise that $H \cap K$ is a subgroup of both H and K; by Lagrange's Theorem, then, $|H \cap K|$ divides p and q. Since $\gcd(p, q) = 1$, then, $|H \cap K| = 1$. Thus $H \cap K = 1$. $\square$

Exercise 3.2.11 Let $H \leq K \leq G$. Prove that $|G : H| = |G : K| \cdot |K : H|$ (do not assume G is finite).

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 $a^p \equiv a (\bmod p)$ for all $a \in \mathbb{Z}$.

Proof. Solution: If p is prime, then $\varphi(p) = p - 1$ (where φ denotes the Euler totient). Thus

$$| \left((\mathbb{Z}/(p)\right)^\times | = p - 1.$$

So for all $a \in (\mathbb{Z}/(p))^\times$, we have $|a|$ divides $p - 1$. Hence

$$a = 1 \cdot a = a^{p-1} a = a^p \pmod{p}.$$

$\square$

Exercise 3.2.21a Prove that $\mathbb{Q}$ has no proper subgroups of finite index.

Proof. Solution: We begin with a lemma. Lemma: If D is a divisible abelian group, then no proper subgroup of D has finite index. Proof: We saw previously that no finite group is divisible and that every proper quotient D/A of a divisible group is divisible; thus no proper quotient of a divisible group is finite. Equivalently, $[D : A]$ is not finite. Because $\mathbb{Q}$ and $\mathbb{Q}/\mathbb{Z}$ are divisible, the conclusion follows. $\square$

Exercise 3.3.3 Prove that if H is a normal subgroup of G of prime index p then for all $K \leq G$ either $K \leq H$, or $G = HK$ and $|K : K \cap H| = p$.

Proof. Solution: Suppose $K \backslash N \neq \emptyset$; say $k \in K \backslash N$. Now $G/N \cong \mathbb{Z}/(p)$ is cyclic, and moreover is generated by any nonidentity- in particular by $\bar{k}$

Now $KN \leq G$ since N is normal. Let $g \in G$. We have $gN = k^a N$ for some integer a. In particular, $g = k^a n$ for some $n \in N$, hence $g \in KN$. We have $[K : K \cap N] = p$ by the Second Isomorphism Theorem. □

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 G is a finite group).

Proof. Solution: Let G be an abelian simple group. Suppose G is infinite. If $x \in G$ is a nonidentity element of finite order, then $\langle x \rangle < G$ is a nontrivial normal subgroup, hence G is not simple. If $x \in G$ is an element of infinite order, then $\langle x^2 \rangle$ is a nontrivial normal subgroup, so G is not simple.

Suppose G is finite; say $|G| = n$. If n is composite, say $n = pm$ for some prime p with $m \neq 1$, then by Cauchy's Theorem G contains an element x of order p and $\langle x \rangle$ is a nontrivial normal subgroup. Hence G is not simple. Thus if G is an abelian simple group, then $|G| = p$ is prime. We saw previously that the only such group up to isomorphism is $\mathbb{Z}/(p)$, so that $G \cong \mathbb{Z}/(p)$. Moreover, these groups are indeed simple. □

Exercise 3.4.4 Use Cauchy's Theorem and induction to show that a finite abelian group has a subgroup of order n for each positive divisor n of its order.

Exercise 3.4.5a Prove that subgroups of a solvable group are solvable.

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

Exercise 3.4.11 Prove that if H is a nontrivial normal subgroup of the solvable group G then there is a nontrivial subgroup A of H with $A \trianglelefteq G$ and A abelian.

Exercise 4.2.8 Prove that if H has finite index n then there is a normal subgroup K of G with $K \leq H$ and $|G : K| \leq n!$.

Proof. Solution: G acts on the cosets G/H by left multiplication. Let $\lambda : G \to S_{G/H}$ be the permutation representation induced by this action, and let K be the kernel of the representation. Now K is normal in G, and $K \leq \mathrm{stab}_G(H) = H$. By the First Isomorphism Theorem, we have an injective group homomorphism $\bar{\lambda} : G/K \to S_{G/H}$. Since $\left|S_{G/H}\right| = n!$, we have $[G : K] \leq n!$. □

Exercise 4.2.9a Prove that if p is a prime and G is a group of order p^α for some $\alpha \in \mathbb{Z}^+$, then every subgroup of index p is normal in G.

Proof. Solution: Let G be a group of order p^k and $H \leq G$ a subgroup with $[G : H] = p$. Now G acts on the conjugates gHg^{-1} by conjugation, since

$$g_1 g_2 \cdot H = (g_1 g_2)\, H\, (g_1 g_2)^{-1} = g_1 \left(g_2 H g_2^{-1}\right) g_1^{-1} = g_1 \cdot (g_2 \cdot H)$$

and $1 \cdot H = 1H1 = H$. Moreover, under this action we have $H \leq \operatorname{stab}(H)$. By Exercise 3.2.11, we have

$$[G : \operatorname{stab}(H)][\operatorname{stab}(H) : H] = [G : H] = p,$$

a prime. If $[G : \operatorname{stab}(H)] = p$, then $[\operatorname{stab}(H) : H] = 1$ and we have $H = \operatorname{stab}(H)$; moreover, H has exactly p conjugates in G. Let $\varphi : G \to S_p$ be the permutation representation induced by the action of G on the conjugates of H, and let K be the kernel of this representation. Now $K \leq \operatorname{stab}(H) = H$. By the first isomorphism theorem, the induced map $\bar{\varphi} : G/K \to S_p$ is injective, so that $|G/K|$ divides $p\,!$. Note, however, that $|G/K|$ is a power of p and that the only powers of p that divide $p\,!$ are 1 and p. So $[G : K]$ is 1 or p. If $[G : K] = 1$, then $G = K$ so that $gHg^{-1} = H$ for all $g \in G$; then $\operatorname{stab}(H) = G$ and we have $[G : \operatorname{stab}(H)] = 1$, a contradiction. Now suppose $[G : K] = p$. Again by Exercise 3.2.11 we have $[G : K] = [G : H][H : K]$, so that $[H : K] = 1$, hence $H = K$. Again, this implies that H is normal so that $gHg^{-1} = H$ for all $g \in G$, and we have $[G : \operatorname{stab}(H)] = 1$, a contradiction. Thus $[G : \operatorname{stab}(H)] \neq p$ If $[G : \operatorname{stab}(H)] = 1$, then $G = \operatorname{stab}(H)$. That is, $gHg^{-1} = H$ for all $g \in G$; thus $H \leq G$ is normal. □

Exercise 4.2.14 Let G be a finite group of composite order n with the property that G has a subgroup of order k for each positive integer k dividing n. Prove that G is not simple.

Proof. Solution: Let p be the smallest prime dividing n, and write $n = pm$. Now G has a subgroup H of order m, and H has index p. By Corollary 5 in the text, H is normal in G. □

Exercise 4.3.5 If the center of G is of index n, prove that every conjugacy class has at most n elements.

Exercise 4.3.26 Let G be a transitive permutation group on the finite set A with $|A| > 1$. Show that there is some $\sigma \in G$ such that $\sigma(a) \neq a$ for all $a \in A$.

Exercise 4.3.27 Let $g_1, g_2, \ldots, g_r$ be representatives of the conjugacy classes of the finite group G and assume these elements pairwise commute. Prove that G is abelian.

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.

Exercise 4.4.6a Prove that characteristic subgroups are normal.

Exercise 4.4.6b Prove that there exists a normal subgroup that is not characteristic.

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

Exercise 4.4.8a Let G be a group with subgroups H and K with $H \leq K$. Prove that if H is characteristic in K and K is normal in G then H is normal in G.

Exercise 4.5.1a Prove that if $P \in \mathrm{Syl}_p(G)$ and H is a subgroup of G containing P then $P \in \mathrm{Syl}_p(H)$.

Proof. Solution: If $P \leq H \leq G$ is a Sylow p-subgroup of G, then p does not divide $[G : P]$. Now $[G : P] = [G : H][H : P]$, so that p does not divide $[H : P]$; hence P is a Sylow p-subgroup of H. □

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

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

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

Exercise 4.5.16 Let $|G| = pqr$, where p, q and r are primes with $p < q < r$. Prove that G has a normal Sylow subgroup for either p, q or r.

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

Exercise 4.5.18 Prove that a group of order 200 has a normal Sylow 5-subgroup.

Exercise 4.5.19 Prove that if $|G| = 6545$ then G is not simple.

Exercise 4.5.20 Prove that if $|G| = 1365$ then G is not simple.

Exercise 4.5.21 Prove that if $|G| = 2907$ then G is not simple.

Exercise 4.5.22 Prove that if $|G| = 132$ then G is not simple.

Exercise 4.5.23 Prove that if $|G| = 462$ then G is not simple.

Exercise 4.5.28 Let G be a group of order 105. Prove that if a Sylow 3-subgroup of G is normal then G is abelian.

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.

Exercise 5.4.2 Prove that a subgroup H of G is normal if and only if $[G, H] \leq H$.

Exercise 7.1.2 Prove that if u is a unit in R then so is $-u$.

Proof. Solution: Since u is a unit, we have $uv = vu = 1$ for some $v \in R$. Thus, we have

$$(-v)(-u) = vu = 1$$

and

$$(-u)(-v) = uv = 1.$$

Thus $-u$ is a unit. □

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. Solution: If $x^2 = 1$, then $x^2 - 1 = 0$. Evidently, then,

$$(x-1)(x+1) = 0.$$

Since R is an integral domain, we must have $x - 1 = 0$ or $x + 1 = 0$; thus $x = 1$ or $x = -1$. □

Exercise 7.1.12 Prove that any subring of a field which contains the identity is an integral domain.

Proof. Solution: Let $R \subseteq F$ be a subring of a field. (We need not yet assume that $1 \in R$). Suppose $x, y \in R$ with $xy = 0$. Since $x, y \in F$ and the zero element in R is the same as that in F, either $x = 0$ or $y = 0$. Thus R has no zero divisors. If R also contains 1 , then R is an integral domain. □

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. Solution: Note first that for all $a \in R$,

$$-a = (-a)^2 = (-1)^2 a^2 = a^2 = a.$$

Now if $a, b \in R$, we have

$$a + b = (a + b)^2 = a^2 + ab + ba + b^2 = a + ab + ba + b.$$

Thus $ab + ba = 0$, and we have $ab = -ba$. But then $ab = ba$. Thus R is commutative. □

Exercise 7.2.2 Let $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ be an element of the polynomial ring $R[x]$. Prove that $p(x)$ is a zero divisor in $R[x]$ if and only if there is a nonzero $b \in R$ such that $bp(x) = 0$.

Proof. Solution: If $bp(x) = 0$ for some nonzero $b \in R$, then it is clear that $p(x)$ is a zero divisor. Now suppose $p(x)$ is a zero divisor; that is, for some $q(x) = \sum_{i=0}^{m} b_i x^i$, we have $p(x)q(x) = 0$. We may choose $q(x)$ to have minimal degree among the nonzero polynomials with this property. We will now show by induction that $a_i q(x) = 0$ for all $0 \leq i \leq n$. For the base case, note that

$$p(x)q(x) = \sum_{k=0}^{n+m} \left(\sum_{i+j=k} a_i b_j \right) x^k = 0.$$

The coefficient of x^{n+m} in this product is $a_n b_m$ on one hand, and 0 on the other. Thus $a_n b_m = 0$. Now $a_n q(x)p(x) = 0$, and the coefficient of x^m in q is $a_n b_m = 0$. Thus the degree of $a_n q(x)$ is strictly less than that of $q(x)$; since $q(x)$ has minimal degree among the nonzero polynomials which multiply $p(x)$ to 0 , in fact $a_n q(x) = 0$. More specifically, $a_n b_i = 0$ for all $0 \leq i \leq m$. For the inductive step, suppose that for some $0 \leq t < n$, we have $a_r q(x) = 0$ for all $t < r \leq n$. Now

$$p(x)q(x) = \sum_{k=0}^{n+m} \left(\sum_{i+j=k} a_i b_j \right) x^k = 0.$$

On one hand, the coefficient of x^{m+t} is $\sum_{i+j=m+t} a_i b_j$, and on the other hand, it is 0 . Thus

$$\sum_{i+j=m+t} a_i b_j = 0.$$

By the induction hypothesis, if $i \geq t$, then $a_i b_j = 0$. Thus all terms such that $i \geq t$ are zero. If $i < t$, then we must have $j > m$, a contradiction. Thus we have $a_t b_m = 0$. As in the base case,

$$a_t q(x)p(x) = 0$$

and $a_t q(x)$ has degree strictly less than that of $q(x)$, so that by minimality, $a_t q(x) = 0$. By induction, $a_i q(x) = 0$ for all $0 \leq i \leq n$. In particular, $a_i b_m = 0$. Thus $b_m p(x) = 0$. □

Exercise 7.2.12 Let $G = \{g_1, \ldots, g_n\}$ be a finite group. Prove that the element $N = g_1 + g_2 + \ldots + g_n$ is in the center of the group ring RG.

Proof. Solution: Let $M = \sum_{i=1}^n r_i g_i$ be an element of $R[G]$. Note that for each $g_i \in G$, the action of g_i on G by conjugation permutes the subscripts. Then we have the following.

$$\begin{aligned}
NM &= \left(\sum_{i=1}^n g_i\right)\left(\sum_{j=1}^n r_j g_j\right) \\
&= \sum_{j=1}^n \sum_{i=1}^n r_j g_i g_j \\
&= \sum_{j=1}^n \sum_{i=1}^n r_j g_j g_j^{-1} g_i g_j \\
&= \sum_{j=1}^n r_j g_j \left(\sum_{i=1}^n g_j^{-1} g_i g_j\right) \\
&= \sum_{j=1}^n r_j g_j \left(\sum_{i=1}^n g_i\right) \\
&= \left(\sum_{j=1}^n r_j g_j\right)\left(\sum_{i=1}^n g_i\right) \\
&= MN.
\end{aligned}$$

Thus $N \in Z(R[G])$. $\square$

Exercise 7.3.16 Let $\varphi : R \to S$ be a surjective homomorphism of rings. Prove that the image of the center of R is contained in the center of S.

Proof. Solution: Suppose $r \in \varphi[Z(R)]$. Then $r = \varphi(z)$ for some $z \in Z(R)$. Now let $x \in S$. Since φ is surjective, we have $x = \varphi y$ for some $y \in R$. Now

$$xr = \varphi(y)\varphi(z) = \varphi(yz) = \varphi(zy) = \varphi(z)\varphi(y) = rx.$$

Thus $r \in Z(S)$. $\square$

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. Solution: First we prove a lemma. Lemma: Let R be a ring, and let $I_1, I_2, J \subseteq R$ be ideals such that $J \subseteq I_1, I_2$. Then $(I_1/J)(I_2/J) = I_1I_2/J$. Proof: ($\subseteq$) Let

$$\alpha = \sum (x_i + J)(y_i + J) \in (I_1/J)(I_2/J).$$

Then

$$\alpha = \sum (x_i y_i + J) = \left(\sum x_i y_i\right) + J \in (I_1 I_2)/J.$$

Now let $\alpha = (\sum x_i y_i) + J \in (I_1 I_2)/J$. Then

$$\alpha = \sum (x_i + J)(y_i + J) \in (I_1/J)(I_2/J).$$

From this lemma and the lemma to Exercise 7.3.36, it follows by an easy induction that

$$(p\mathbb{Z}/p^m\mathbb{Z})^m = (p\mathbb{Z})^m/p^m\mathbb{Z} = p^m\mathbb{Z}/p^m\mathbb{Z} \cong 0.$$

Thus $p\mathbb{Z}/p^m\mathbb{Z}$ is nilpotent in $\mathbb{Z}/p^m\mathbb{Z}$. □

Exercise 7.4.27 Let R be a commutative ring with $1 \neq 0$. Prove that if a is a nilpotent element of R then $1 - ab$ is a unit for all $b \in R$.

Proof. $\mathfrak{N}(R)$ is an ideal of R. Thus for all $b \in R$, $-ab$ is nilpotent. Hence $1 - ab$ is a unit in R. □

Exercise 8.1.12 Let N be a positive integer. Let M be an integer relatively prime to N and let d be an integer relatively prime to $\varphi(N)$, where φ denotes Euler's φ-function. Prove that if $M_1 \equiv M^d \pmod N$ then $M \equiv M_1^{d'} \pmod N$ where d' is the inverse of d mod $\varphi(N)$: $dd' \equiv 1 \pmod{\varphi(N)}$.

Exercise 8.2.4 Let R be an integral domain. Prove that if the following two conditions hold then R is a Principal Ideal Domain: (i) any two nonzero elements a and b in R have a greatest common divisor which can be written in the form $ra + sb$ for some $r, s \in R$, and (ii) if $a_1, a_2, a_3, \ldots$ are nonzero elements of R such that $a_{i+1} \mid a_i$ for all i, then there is a positive integer N such that a_n is a unit times a_N for all $n \geq N$.

Exercise 8.3.4 Prove that if an integer is the sum of two rational squares, then it is the sum of two integer squares.

Exercise 8.3.5a Let $R = \mathbb{Z}[\sqrt{-n}]$ where n is a squarefree integer greater than 3. Prove that $2, \sqrt{-n}$ and $1 + \sqrt{-n}$ are irreducibles in R.

Exercise 8.3.6a Prove that the quotient ring $\mathbb{Z}[i]/(1+i)$ is a field of order 2.

Exercise 8.3.6b Let $q \in \mathbb{Z}$ be a prime with $q \equiv 3 \bmod 4$. Prove that the quotient ring $\mathbb{Z}[i]/(q)$ is a field with q^2 elements.

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

Exercise 9.1.10 Prove that the ring $\mathbb{Z}\left[x_1, x_2, x_3, \ldots\right] / \left(x_1 x_2, x_3 x_4, x_5 x_6, \ldots\right)$ contains infinitely many minimal prime ideals (cf. exercise.9.1.36 of Section 7.4).

Exercise 9.3.2 Prove that if $f(x)$ and $g(x)$ are polynomials with rational coefficients whose product $f(x)g(x)$ has integer coefficients, then the product of any coefficient of $g(x)$ with any coefficient of $f(x)$ is an integer.

Exercise 9.4.2a Prove that $x^4 - 4x^3 + 6$ is irreducible in $\mathbb{Z}[x]$.

Exercise 9.4.2b Prove that $x^6 + 30x^5 - 15x^3 + 6x - 120$ is irreducible in $\mathbb{Z}[x]$.

Exercise 9.4.2c Prove that $x^4 + 4x^3 + 6x^2 + 2x + 1$ is irreducible in $\mathbb{Z}[x]$.

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

Exercise 9.4.9 Prove that the polynomial $x^2 - \sqrt{2}$ is irreducible over $\mathbb{Z}[\sqrt{2}]$. You may assume that $\mathbb{Z}[\sqrt{2}]$ is a U.F.D.

Exercise 9.4.11 Prove that $x^2 + y^2 - 1$ is irreducible in $\mathbb{Q}[x, y]$.

Exercise 11.1.13 Prove that as vector spaces over $\mathbb{Q}, \mathbb{R}^n \cong \mathbb{R}$, for all $n \in \mathbb{Z}^+$.