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 $(a_1 a_2 \ldots a_n)^{-1} = a_n^{-1} a_{n-1}^{-1} \ldots a_1^{-1}$ for all $a_1, a_2, \ldots, a_n \in G$.

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

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

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

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

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

Proof. If $xy = yx$, then $y^{-1}xy = y^{-1}yx = 1x = x$. Multiplying by x^{-1} then gives $x^{-1}y^{-1}xy = 1$.

On the other hand, if $x^{-1}y^{-1}xy = 1$, then we may multiply on the left by x to get $y^{-1}xy = x$. Then multiplying on the left by y gives $xy = yx$ as desired. □

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. □

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

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

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 $|x| = n \leq |G|$ $\square$

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. 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. 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

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

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. □

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 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 $H - \{1\}$.

Proof. If $H = \{1\}$ then $H - \{1\}$ is the empty set which indeed generates the trivial subgroup H. So suppose $|H| > 1$ and pick a nonidentity element $h \in H$. Since $1 = hh^{-1} \in \langle H - \{1\} \rangle$ (Proposition 9), we see that $H \leq \langle H - \{1\} \rangle$. By minimality of $\langle H - \{1\} \rangle$, the reverse inclusion also holds so that $\langle H - \{1\} \rangle = H$. □

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.

Proof. If H is maximal, then we are done. If H is not maximal, then there is a subgroup K_1 of G such that $H < K_1 < G$. If K_1 is maximal, we are done. But if K_1 is not maximal, there is a subgroup K_2 with $H < K_1 < K_2 < G$. If K_2 is maximal, we are done, and if not, keep repeating the procedure. Since G is finite, this process must eventually come to an end, so that K_n is maximal for some positive integer n. Then K_n is a maximal subgroup containing H. □

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

Proof. Fix a positive integer $n > 1$ and let $H \leq D_{2n}$ consist of the rotations of D_{2n}. That is, $H = \langle r \rangle$. Now, this subgroup is proper since it does not contain s. If H is not maximal, then by the previous proof we know there is a maximal subset K containing H. Then K must contain a reflection sr^k for $k \in \{0, 1, \ldots, n-1\}$. Then since $sr^k \in K$ and $r^{n-k} \in K$, it follows by closure that

$$s = \left(sr^k\right)\left(r^{n-k}\right) \in K.$$

But $D_{2n} = \langle r, s \rangle$, so this shows that $K = D_{2n}$, which is a contradiction. Therefore H must be maximal. □

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.

Proof. Suppose H is a maximal subgroup of G. Then H is cyclic, and we may write $H = \left\langle x^k \right\rangle$ for some integer k, with $k > 1$. Let $d = (n, k)$. Since H is a proper subgroup, we know by Proposition 6 that $d > 1$. Choose a prime factor p of d. If $k = p = d$ then $k \mid n$ as required.

If, however, k is not prime, then consider the subgroup $K = \langle x^p \rangle$. Since p is a proper divisor of k, it follows that $H < K$. But H is maximal, so we must have $K = G$. Again by Proposition 6 , we must then have $(p, n) = 1$. However, p divides d which divides n, so $p \mid n$ and $(p, n) = p > 1$, a contradiction. Therefore $k = p$ and the left-to-right implication holds. Now, for the converse, suppose

$H = \langle x^p \rangle$ for p a prime dividing n. If H is not maximal then the first part of this exercise shows that there is a maximal subgroup K containing H. Then $K = \langle x^q \rangle$. So $x^p \in \langle x^q \rangle$, which implies $q \mid p$. But the only divisors of p are 1 and p. If $q = 1$ then $K = G$ and K cannot be a proper subgroup, and if $q = p$ then $H = K$ and H cannot be a proper subgroup of K. This contradiction shows that H is maximal. □

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. □

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.

Proof. Suppose H and K are normal subgroups of G. We already know that $H \cap K$ is a subgroup of G, so we need to show that it is normal. Choose any $g \in G$ and any $x \in H \cap K$. Since $x \in H$ and $H \trianglelefteq G$, we know $gxg^{-1} \in H$. Likewise, since $x \in K$ and $K \trianglelefteq G$, we have $gxg^{-1} \in K$. Therefore $gxg^{-1} \in H \cap K$. This shows that $g(H \cap K)g^{-1} \subseteq H \cap K$, and this is true for all $g \in G$. By Theorem 6 (5) (which we will prove in Exercise 3.1.25), this is enough to show that $H \cap K \trianglelefteq G$. □

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 $H \cap K = 1$. □

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).

Proof. Proof. Let G be a group and let I be a nonempty set of indices, not necessarily countable. Consider the collection of subgroups $\{N_\alpha \mid \alpha \in I\}$, where $N_\alpha \trianglelefteq G$ for each $\alpha \in I$. Let

$$N = \bigcap_{\alpha \in I} N_\alpha.$$

We know N is a subgroup of G. For any $g \in G$ and any $n \in N$, we must have $n \in N_\alpha$ for each α. And since $N_\alpha \trianglelefteq G$, we have $gng^{-1} \in N_\alpha$ for each α. Therefore $gng^{-1} \in N$, which shows that $gNg^{-1} \subseteq N$ for each $g \in G$. As before, this is enough to complete the proof. □

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

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

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

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

□

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. □

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 $\left\langle x^2 \right\rangle$ 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.

Proof. Let G be a finite abelian group. We use induction on $|G|$. Certainly the result holds for the trivial group. And if $|G| = p$ for some prime p, then the positive divisors of $|G|$ are 1 and p and the result is again trivial.

Now assume that the statement is true for all groups of order strictly smaller than $|G|$, and let n be a positive divisor of $|G|$ with $n > 1$. First, if n is prime then Cauchy's Theorem allows us to find an element $x \in G$ having order n. Then $\langle x \rangle$ is the desired subgroup. On the other hand, if n is not prime, then n has a prime divisor p, so that $n = kp$ for some integer k. Cauchy's Theorem allows us to find an element x having order p. Set $N = \langle x \rangle$. By Lagrange's Theorem,

$$|G/N| = \frac{|G|}{|N|} < |G|.$$

Now, by the inductive hypothesis, the group G/N must have a subgroup of order k. And by the Lattice Isomorphism Theorem, this subgroup has the form H/N for some subgroup H of G. Then $|H| = k|N| = kp = n$, so that H has order n. This completes the inductive step. □

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

Proof. Let G be a solvable group and let $H \leq G$. Since G is solvable, we may find a chain of subgroups

$$1 = G_0 \trianglelefteq G_1 \trianglelefteq G_2 \trianglelefteq \cdots \trianglelefteq G_n = G$$

so that each quotient G_{i+1}/G_i is abelian. For each i, define

$$H_i = G_i \cap H, \quad 0 \leq i \leq n.$$

Then $H_i \leq H_{i+1}$ for each i. Moreover, if $g \in H_{i+1}$ and $x \in H_i$, then in particular $g \in G_{i+1}$ and $x \in G_i$, so that

$$gxg^{-1} \in G_i$$

because $G_i \trianglelefteq G_{i+1}$. But g and x also belong to H, so

$$gxg^{-1} \in H_i,$$

which shows that $H_i \trianglelefteq H_{i+1}$ for each i. Next, note that

$$H_i = G_i \cap H = (G_i \cap G_{i+1}) \cap H = G_i \cap H_{i+1}.$$

By the Second Isomorphism Theorem, we then have

$$H_{i+1}/H_i = H_{i+1}/\left(H_{i+1} \cap G_i\right) \cong H_{i+1}G_i/G_i \leq G_{i+1}/G_i.$$

Since H_{i+1}/H_i is isomorphic to a subgroup of the abelian group G_{i+1}/G_i, it follows that H_{i+1}/H_i is also abelian. This completes the proof that H is solvable. □

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

Proof. Next, note that

$$H_i = G_i \cap H = (G_i \cap G_{i+1}) \cap H = G_i \cap H_{i+1}.$$

By the Second Isomorphism Theorem, we then have

$$H_{i+1}/H_i = H_{i+1}/\left(H_{i+1} \cap G_i\right) \cong H_{i+1}G_i/G_i \leq G_{i+1}/G_i.$$

Since H_{i+1}/H_i is isomorphic to a subgroup of the abelian group G_{i+1}/G_i, it follows that H_{i+1}/H_i is also abelian. This completes the proof that H is solvable. Next, let $N \trianglelefteq G$. For each i, define

$$N_i = G_iN, \quad 0 \leq i \leq n.$$

Now let $g \in N_{i+1}$, where $g = g_0n_0$ with $g_0 \in G_{i+1}$ and $n_0 \in N$. Also let $x \in N_i$, where $x = g_1n_1$ with $g_1 \in G_i$ and $n_1 \in N$. Then

$$gxg^{-1} = g_0n_0g_1n_1n_0^{-1}g_0^{-1}.$$

Now, since N is normal in $G, Ng = gN$, so $n_0g_1 = g_1n_2$ for some $n_2 \in N$. Then

$$gxg^{-1} = g_0g_1\left(n_2n_1n_0^{-1}\right)g_0^{-1} = g_0g_1n_3g_0^{-1}$$

for some $n_3 \in N$. Then $n_3g_0^{-1} = g_0^{-1}n_4$ for some $n_4 \in N$. And $g_0g_1g_0^{-1} \in G_i$ since $G_i \trianglelefteq G_{i+1}$, so

$$gxg^{-1} = g_0g_1g_0^{-1}n_4 \in N_i.$$

This shows that $N_i \trianglelefteq N_{i+1}$. So by the Lattice Isomorphism Theorem, we have $N_{i+1}/N \trianglelefteq N_i/N$. This shows that

$$1 = N_0/N \trianglelefteq N_1/N \trianglelefteq N_2/N \trianglelefteq \cdots \trianglelefteq N_n/N = G/N.$$

Moreover, the Third Isomorphism Theorem says that

$$(N_{i+1}/N)\,/\,(N_i/N) \cong N_{i+1}/N_i,$$

so the proof will be complete if we can show that N_{i+1}/N_i is abelian. Let $x, y \in N_{i+1}/N_i$. Then

$$x = (g_0 n_0)\,N_i \quad \text{and} \quad y = (g_1 n_1)\,N_i$$

for some $g_0, g_1 \in G_{i+1}$ and $n_0, n_1 \in N$. We have

$$\begin{aligned} xyx^{-1}y^{-1} &= (g_0 n_0)\,(g_1 n_1)\,(g_0 n_0)^{-1}\,(g_1 n_1)^{-1}\,N_i \\ &= g_0 n_0 g_1 n_1 n_0^{-1} g_0^{-1} n_1^{-1} g_1^{-1} N_i. \end{aligned}$$

Since $N \trianglelefteq G, gN = Ng$ for any $g \in G$, so we can find $n_2 \in N$ such that

$$xyx^{-1}y^{-1} = g_0 g_1 g_0^{-1} g^{-1} n_2 N_i.$$

Now $N_i = G_i N = N G_i$ since $N \trianglelefteq G$ (see Proposition 14 and its corollary). Therefore

$$n_2 N_i = n_2 N G_i = N G_i = G_i N$$

and we get

$$xyx^{-1}y^{-1} = g_0 g_1 g_0^{-1} g^{-1} G_i N = G_i N.$$

So $xyx^{-1}y^{-1} = 1N_i$ or $xy = yx$. This completes the proof that G/N is 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.

Proof. Suppose H is a nontrivial normal subgroup of the solvable group G. First, notice that H, being a subgroup of a solvable group, is itself solvable. By exercise $8, H$ has a chain of subgroups

$$1 \leq H_1 \leq \ldots \leq H$$

such that each H_i is a normal subgroup of H itself and H_{i+1}/H_i is abelian. But then the first group in the series

$$H_1/1 \cong H$$

is an abelian subgroup of H. □

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

$$g_1g_2 \cdot H = (g_1g_2)\, H\, (g_1g_2)^{-1} = g_1 \left(g_2Hg_2^{-1}\right) g_1^{-1} = g_1 \cdot (g_2 \cdot H)$$

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. Then H is normal in G. □

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 $a \in A$.

Proof. Let G be a transitive permutation group on the finite set $A, |A| > 1$. We want to find an element σ which doesn't stabilize anything, that is, we want a σ such that

$$\sigma \notin G_a$$

for all $a \in A$. Since the group is transitive, there is always a $g \in G$ such that $b = g \cdot a$. Let us see in what relationship the stabilizers of a and b are. We find

$$\begin{aligned} G_b &= \{h \in G \mid h \cdot b = b\} \\ &= \{h \in G \mid hg \cdot a = g \cdot a\} \\ &= \left\{h \in G \mid g^{-1}hg \cdot a = a\right\} \end{aligned}$$

Putting $h' = g^{-1}hg$, we have $h = gh'g^{-1}$ and

$$G_b = g\{h' \in H \mid h' \cdot a = a\}g^{-1}$$
$$= gG_ag^{-1}$$

By the above, the stabilizer subgroup of any element is conjugate to some other stabilizer subgroup. Now, the stabilizer cannot be all of G (else $\{a\}$ would be a orbit). Thus it is a proper subgroup of G. By the previous exercise, we have

$$\bigcup_{a \in A} G_a = \bigcup_{g \in G} gG_ag^{-1} \subset G$$

(the union of conjugates of a proper subgroup can never be all of G). This shows there is an element σ which is not in any stabilizer of any element of A. Then $\sigma(a) \neq a$ for all $a \in A$, as we wanted to show. □

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 of order pq. We need to prove that if p and q are distinct primes than G is cyclic. By Cauchy's theorem there are $a, b \in G$ with a of order p and b of order q. Since $(|a|, |b|) = 1$ and $ab = ba$ then $|ab| = |a| \cdot |b| = pq$. Therefore ab is an element of order pq, the order of G, which means G is cyclic. □

Exercise 4.4.6a Prove that characteristic subgroups are normal.

Proof. Let H be a characterestic subgroup of G. By definition $\alpha(H) \subset H$ for every $\alpha \in \mathrm{Aut}(G)$. So, H is in particular invariant under the inner automorphism. Let ϕ_g denote the conjugation automorphism by g. Then $\phi_g(H) \subset H \implies gHg^{-1} \subset H$. So, H is normal. □

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

Proof. We have to produce a group G and a subgroup H such that H is normal in G, but not characterestic. Consider the Klein's four group $G = \{e, a, b, ab\}$. This is an abelian group with each element having order 2. Consider $H = \{e, a\}$. H is normal in G. Define $\sigma : G \to G$ as $\sigma(a) = b, \sigma(b) = a, \sigma(ab) = ab$. Clearly σ does not fix H. So, H is not characterestic. □

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 group and H be the unique subgroup of order n. Now, let $\sigma \in \mathrm{Aut}(G)$. Now Clearly $|\sigma(G)| = n$, because σ is a one-one onto map. But then as H is the only subgroup of order n, and because of the fact that a automorphism maps subgroups to subgroups, we have $\sigma(H) = H$ for every $\sigma \in \mathrm{Aut}(G)$. Hence, H is a characterestic subgroup of 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.

Proof. We prove that H is invariant under every inner automorphism of G. Consider a inner automorphism ϕ_g of G. Now, $\phi_g|_K$ is a automorphism of K because K is normal in G. But H is a characterestic subgroup of K, so $\phi_g|_K(H) \subset H$, so in general $\phi_g(H) \subset H$. Hence H is characteretstic 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. 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.

Proof. Since $|G| = 56 = 2^3.7$, G has $2-$Sylow subgroup of order 8, as well as $7-$Sylow subgroup of order 7. Now, we count the number of such subgroups. Let n_7 be the number of $7-$Sylow subgroup and n_2 be the number of $2-$Sylow subgroup. Now $n_7 = 1 + 7k$ where $1 + 7k|8$. The choices for k are 0 or 1. If $k = 0$, there is only one $7-$Sylow subgroup and hence normal. So, assume now, that there are 8 $7-$Sylow subgroup(for $k = 1$). Now we look at $2-$ Sylow subgroups. $n_2 = 1 + 2k|7$. So choice for k are 0 and 3. If $k = 0$, there is only one $2-$Sylow subgroup and hence normal. So, assume now, that there are 7 $2-$Sylow subgroup (for $k = 3$). Now we claim that simultaneously, there cannot be 8 $7-$Sylow subgroup and 7 $2-$Sylow subgroup. So, either $7-$Sylow subgroup is normal being unique, or the $2-$Sylow subgroup is normal. Now, to prove the claim, we observe that there are 48 elements of order 7. Let H_1 and H_2 be two distinct $2-$Sylow subgroup. Now $|H_1| = 8$. So we already get $48 + 8 = 56$ distinct elements in the group. Now H_2 being distinct from H_1, has at least one element which is not in H_1. This adds one more element in the group, at the least. Now already we have number of elements in the group exceeding the number of element in G. This gives a contradiction and proves the claim. □

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

Proof. Since $|G| = 351 = 3^2.13$, G has $3-$Sylow subgroup of order 9, as well as $13-$Sylow subgroup of order 13. Now, we count the number of such subgroups. Let n_{13} be the number of $13-$Sylow subgroup and n_3 be the number of $3-$Sylow subgroup. Now $n_{13} = 1 + 13k$ where $1 + 13k|9$. The choices for k is 0. Hence, there is a unique $13-$Sylow subgroup and hence is normal.

□

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. Since $|G| = 351 = 3^2.13$, G has $3-$Sylow subgroup of order 9, as well as $13-$Sylow subgroup of order 13. Now, we count the number of such subgroups. Let n_{13} be the number of $13-$Sylow subgroup and n_3 be the number of $3-$Sylow subgroup. Now $n_{13} = 1 + 13k$ where $1 + 13k|9$. The choices for k is 0. Hence, there is a unique $13-$Sylow subgroup and hence is normal. □

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.

Proof. Let $|G| = pqr$. We also assume $p < q < r$. We prove that G has a normal Sylow subgroup of p, q or r. Now, Let n_p, n_q, n_r be the number of Sylow-p subgroup, Sylow-q subgroup, Sylow-r subgroup resp. So, we have $n_r = 1 + rk$ such that $1 + rk \mid pq$. So, in this case as r is greatest n_r can be 1 or pq. We assume $n_r = pq$. Now we have $n_q = 1 + qk$ such that $1 + qk \mid pr$. Now,as $p < q < r, n_q$ can be 1 or r, or pr. Assume that $n_q = r$. Now we turn to n_p. Again my similar method we can conclude n_p can be $1, q, r$, or qr. We assume that n_p is q. Now we count the number of elements of order p, q, r. Since $n_r = pq$, the number of elements of order r is $pq(r - 1)$. Since $n_q = r$, the number of elements of order q is $(q - 1)r$. And as $n_p = q$, the number of elements of order p is $(p - 1)q$. So, in total we get $pq(r - 1) + (q - 1)r + (p- 1)$ $q = pqr + qr - r - q = pqr + r(q - 1) - r$. But observe that as $q > 1, r(q - 1) - r >$ 0 . So the number of elements exceeds pqr. So, it proves that atleast n_p or n_q or n_r is 1, which ultimately proves the result, because a unique Sylow-p subgroup is always normal. □

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

Proof. Since $|G| = 105 = 3.5.7$, G has $3-$Sylow subgroup of order 3, as well as $5-$Sylow subgroup of order 5 and, $7-$Sylow subgroup of order 7. Now, we count the number of such subgroups. Let n_3 be the number of $3-$Sylow subgroup, n_5 be the number of $5-$Sylow subgroup, and n_7 be the number of $7-$Sylow subgroup. Now $n_7 = 1 + 7k$ where $1 + 7k|15$. The choices for k are 0 or 1. If $k = 0$, there is only one $7-$Sylow subgroup and hence normal. So, assume now, that there are 15 $7-$Sylow subgroup(for $k = 1$). Now we look at $5-$ Sylow subgroups. $n_5 = 1 + 5k|21$. So choice for k are 0 and 4. If $k = 0$, there is only one $5-$Sylow subgroup and hence normal. So, assume now, that there are 24 $5-$Sylow subgroup (for $k = 4$). Now we claim that simultaneously, there cannot be 15 $7-$Sylow subgroup and 24 $5-$Sylow subgroup. So, either $7-$Sylow subgroup is normal being unique, or the $5-$Sylow subgroup is normal. Now, to prove the claim, we observe that there are 90 elements of order 7. Also, see that there are $24 \times 4 = 96$ number of elements of order 5. So we get $90 + 94 = 184$ number of elements which exceeds the order of the group.

This gives a contradiction and proves the claim. So, now we have proved that there is either a normal $5-$Sylow subgroup or a normal $7-$Sylow subgroup. Now we prove that indeed both $5-$ Sylow subgroup and 7 -Sylow subgroup are normal. Assume that 7 -Sylow subgroup is normal. So, there is a unique 7 -Sylow subgroup, say H. Now assume that there are 245 -Sylow subgroups. So, we get again $24 \times 4=96$ elements of order 5 . From H we get 7 elements which gives us total of $96+7=103$ elements. Now consider the number of 3 -Sylow subgroups. $n_3=1+3k \mid 35$. Then the possibilities for k are 0 and 2 . But we can rule out $k=2$ because having 73 -Sylow subgroup, will mean we have 14 elements of order 3 . So we get $103+14=117$ elements in total which exceeds the order of the group. So we have now that there is a unique 3 -Sylow subgroup and hence normal. Call that subgroup K. Now take any one 5 -Sylow subgroup, call it L. Now observe LK is a subgroup of G with order 15 . We know that a group of order 15 is cyclic by an example in Page-143 of the book. So, there is an element of order 15. Actually we have $\phi(15)=8$ number of elements of order 15. But then again we already had 103 elements and then we actually get at least $103+8=111$ elements which exceeds the order of the group. So, there can't be 24 5-Sylow subgroups, and hence there is a unique 5-Sylow subgroup, and hence normal. □

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

Proof. Let G be a group of order $200=5^2 \cdot 8$. Note that 5 is a prime not dividing 8 . Let $P \in Syl_5(G)$. [We know P exists since $Syl_5(G) \neq \emptyset$ by Sylow's Theorem]

The number of Sylow 5-subgroups of G is of the form $1+k \cdot 5$, i.e., $n_5 \equiv 1(\bmod 5)$ and n_5 divides 8 . The only such number that divides 8 and equals $1(\bmod 5)$ is 1 so $n_5=1$. Hence P is the unique Sylow 5-subgroup. Since P is the unique Sylow 5-subgroup, this implies that P is normal in G. □

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

Proof. Since $|G|=132=2^2.3.11$, G has $2-$Sylow subgroup of order 4, as well as $11-$Sylow subgroup of order 11, and $3-$Sylow subgroup of order 3. Now, we count the number of such subgroups. Let n_{11} be the number of $11-$Sylow subgroup and n_3 be the number of $3-$Sylow subgroup. Now $n_{11}=1+11k$ where $1+11k|12$. The choices for k are 0 or 1. If $k=0$, there is only one $11-$Sylow subgroup and hence normal. So, assume now, that there are 12 $11-$Sylow subgroup(for $k=1$). Now we look at $3-$ Sylow subgroups. $n_3=1+3k|44$. So choice for k are 0, 1, and 7. If $k=0$, there is only one $3-$Sylow subgroup and hence normal. So, assume now, that there are 4 $2-$Sylow subgroup (for $k=3$). Now we claim that simultaneously, there cannot be 12 $11-$Sylow subgroup and 4 $3-$Sylow subgroups provided there is more than one $2-$Sylow subgroups. So, either $2-$Sylow subgroup is normal or if not, then, either $11-$Sylow subgroup is normal being unique, or the $3-$Sylow subgroup is normal(We don't consider the possibility of 22 3−Sylow subgroup because of obvious reason). Now, to prove the claim, we observe that there are 120 elements of order 11. Also there are 8 elements of order 3. So we already get $120+8+1 = 129$ distinct elements in the group. Let us count the number of 2−Sylow subgroups in G. $n_2 = 1 + 2k|33$. The possibilities for k are 0, 1, 5, 16. Now, assume there is more than one 2−Sylow subgroups. Let H_1 and H_2 be two distinct 2−Sylow subgroup. Now $|H_1| = 4$. So we already get $129 + 3 = 132$ distinct elements in the group. Now H_2 being distinct from H_1, has at least one element which is not in H_1. This adds one more element in the group, at the least. Now already we have number of elements in the group exceeding the number of element in G. This gives a contradiction and proves the claim. Hence G is not simple. □

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

Proof. Since $|G| = 1365 = 3.5.7.13$, G has 13−Sylow subgroup of order 13. Now, we count the number of such subgroups. Let n_{13} be the number of 13−Sylow subgroup. Now $n_{13} = 1 + 13k$ where $1 + 13k|3.5.7$. The choices for k is 0. Hence, there is a unique 13−Sylow subgroup and hence is normal. so G is not simple. □

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

Proof. Since $|G| = 2907 = 3^2.17.19$, G has 19−Sylow subgroup of order 19. Now, we count the number of such subgroups. Let n_{19} be the number of 19−Sylow subgroup. Now $n_{19} = 1 + 19k$ where $1 + 19k|3^2.17$. The choices for k is 0. Hence, there is a unique 19−Sylow subgroup and hence is normal. so G is not simple. □

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

Proof. Since $|G| = 132 = 2^2.3.11$, G has 2−Sylow subgroup of order 4, as well as 11−Sylow subgroup of order 11, and 3−Sylow subgroup of order 3. Now, we count the number of such subgroups. Let n_{11} be the number of 11−Sylow subgroup and n_3 be the number of 3−Sylow subgroup. Now $n_{11} = 1+11k$ where $1 + 11k|12$. The choices for k are 0 or 1. If $k = 0$, there is only one 11−Sylow subgroup and hence normal. So, assume now, that there are 12 11−Sylow subgroup(for $k = 1$). Now we look at 3− Sylow subgroups. $n_3 = 1 + 3k|44$. So choice for k are 0, 1, and 7. If $k = 0$, there is only one 3−Sylow subgroup and hence normal. So, assume now, that there are 4 2−Sylow subgroup (for $k = 3$). Now we claim that simultaneously, there cannot be 12 11−Sylow subgroup and 4 3−Sylow subgroups provided there is more than one 2−Sylow subgroups. So, either 2−Sylow subgroup is normal or if not, then, either 11−Sylow subgroup is normal being unique, or the 3−Sylow subgroup is normal(We don't consider the possibility of 22 3−Sylow subgroup because of obvious reason). Now, to prove the claim, we observe that there are 120 elements of order 11. Also there are 8 elements of order 3. So we already get $120+8+1 = 129$ distinct elements in the group. Let us count the number of $2-$Sylow subgroups in G. $n_2 = 1 + 2k|33$. The possibilities for k are 0, 1, 5, 16. Now, assume there is more than one $2-$Sylow subgroups. Let H_1 and H_2 be two distinct $2-$Sylow subgroup. Now $|H_1| = 4$. So we already get $129 + 3 = 132$ distinct elements in the group. Now H_2 being distinct from H_1, has at least one element which is not in H_1. This adds one more element in the group, at the least. Now already we have number of elements in the group exceeding the number of element in G. This gives a contradiction and proves the claim. Hence G is not simple. $\square$

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

Proof. Let G be a group of order $462 = 11 \cdot 42$. Note that 11 is a prime not dividing 42 . Let $P \in Syl_{11}(G)$. [We know P exists since $Syl_{11}(G) \neq \emptyset$]. Note that $|P| = 11^1 = 11$ by definition.

The number of Sylow 11-subgroups of G is of the form $1 + k \cdot 11$, i.e., $n_{11} \equiv 1 \pmod{11}$ and n_{11} divides 42 . The only such number that divides 42 and equals $1 \pmod{11}$ is 1 so $n_{11} = 1$. Hence P is the unique Sylow 11-subgroup.

Since P is the unique Sylow Il-subgroup, this implies that P is normal in G. $\square$

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.

Proof. Given that G is a group of order $1575 = 3^2.5^2.7$. Now, Let n_p be the number of Sylow-p subgroups. It is given that Sylow-3 subgroup is normal and hence is unique, so $n_3 = 1$. First we prove that both Sylow-5 subgroup and Sylow 7-subgroup are normal. Let P be the Sylow3 subgroup. Now, Consider G/P, which has order $5^2.7$. Now, the number of Sylow -5 subgroup of G/P is given by $1 + 5k$, where $1 + 5k \mid 7$. Clearly $k = 0$ is the only choice and hence there is a unique Sylow-5 subgroup of G/P, and hence normal. In the same way Sylow-7 subgroup of G/P is also unique and hence normal. Consider now the canonical map $\pi : G \to G/P$. The inverse image of Sylow-5 subgroup of G/P under π, call it H, is a normal subgroup of G, and $|H| = 3^2.5^2$. Similarly, the inverse image of Sylow-7 subgroup of G/P under π call it K is also normal in G and $|K| = 3^2.7$. Now, consider H. Observe first that the number of Sylow-5 subgroup in H is $1 + 5k$ such that $1 + 5k \mid 9$. Again $k = 0$ and hence H has a unique Sylow-5 subgroup, call it P_1. But, it is easy to see that P_1 is also a Sylow-5 subgroup of G, because $|P_1| = 25$. But now any other Sylow 5 subgroup of G is of the form gP_1g^{-1} for some $g \in G$. But observe that since $P_1 \subset H$ and H is normal in G, so $gP_1g^1 \subset H$, and gP_1g^{-1} is also Sylow-5 subgroup of H. But, then as Sylow-5 subgroup of H is unique we have $gP_1g^{-1} = P_1$. This shows that Sylow-5 subgroup of G is unique and hence normal in G.

Similarly, one can argue the same for K and deduce that Sylow-7 subgroup of G is unique and hence normal. So, the first part of the problem is done. $\square$

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 and P is a normal p-Sylow subgroup of $G.|G| = p^a.m$ where $p \nmid m$. Then $|P| = p^a$. Let H be a subgroup of G. Now if $|H| = k$ such that $p \nmid k$. Then $P \cap H = \{e\}$. There is nothing to prove in this case. Let $|H| = p^b.n$, where $b \leq a$, and $p \nmid n$. Now consider PH which is a subgroup of G, as P is normal. Now $|PH| = \frac{|P||H|}{|P \cap H|} = \frac{p^{a+b} \cdot n}{|P \cap H|}$. Now since $PH \leq G$, so $|PH| = p^a$.l, as $P \leq PH$. This forces $|P \cap H| = p^b$. So by order consideration we have $P \cap H$ is a sylow $-p$ subgroup of H. Now we know P is unique p - Sylow subgroup. Suppose H has a sylow-p subgroup distinct from $P \cap H$, call it H_1. Now H_1 is a p-subgroup of G. So, H_1 is contained in some Sylow-p subgroup of G, call it P_1. Clearly P_1 is distinct from P, which is a contradiction. So $P \cap H$ is the only p-Sylow subgroup of H, and hence normal in H $\square$

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

Proof. $H \trianglelefteq G$ is equivalent to $g^{-1}hg \in H, \forall g \in G, \forall h \in H$. We claim that holds if and only if $h^{-1}g^{-1}hg \in H, \forall g \in G, \forall h \in H$, i.e., $\left\{h^{-1}g^{-1}hg : h \in H, g \in G\right\} \subseteq H$. That holds by the following argument: If $g^{-1}hg \in H, \forall g \in G, \forall h \in H$, note that $h^{-1} \in H$, so multiplying them, we also obtain an element of H. On the other hand, if $h^{-1}g^{-1}hg \in H, \forall g \in G, \forall h \in H$, then

$$hh^{-1}g^{-1}hg = g^{-1}hg \in H, \forall g \in G, \forall h \in H.$$

Since $\left\{h^{-1}g^{-1}hg : h \in H, g \in G\right\} \subseteq H \Leftrightarrow \left\langle\left\{h^{-1}g^{-1}hg : h \in H, g \in G\right\}\right\rangle \leq H$, we've solved the exercise by definition of $[H, G]$. $\square$

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. $\square$

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 $x = -1$. $\square$

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. $\square$

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. $\square$

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 $\sum_{i+j=m+t} a_ib_j$, and on the other hand, it is 0 . Thus

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

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

$$a_tq(x)p(x) = 0$$

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

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. Let $M = \sum_{i=1}^n r_ig_i$ 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.

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

Thus $N \in Z(R[G])$. □

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. 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. 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

$$\alpha = \sum (x_iy_i + J) = \left(\sum x_iy_i\right) + J \in (I_1I_2)/J.$$

Now let $\alpha = (\sum x_iy_i) + J \in (I_1I_2)/J$. 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 $\mathbb{Z}/p^m\mathbb{Z}$. $\square$

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. $\square$

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 $\varphi(N)$: $dd' \equiv 1 \pmod{\varphi(N)}$.

Proof. Note that there is some $k \in \mathbb{Z}$ such that $M^{dd'} \equiv M^{k\varphi(N)+1} \equiv \left(M^{\varphi(N)}\right)^k \cdot M \bmod N$. By Euler's Theorem we have $M^{\varphi(N)} \equiv 1 \bmod N$, so that $M_1^{d'} \equiv M \bmod N$. $\square$

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 $n \geq N$.

Proof. Let $I \leq R$ be a nonzero ideal and let $I/\sim$ be the set of equivalence classes of elements of I with regards to the relation of being associates. We can equip $I/\sim$ with a partial order with $[x] \leq [y]$ if $y \mid x$. Condition (ii) implies all chains in $I/\sim$ have an upper bound, so By Zorn's lemma $I/\sim$ contains a maximal element, i.e. I contains a class of associated elements which are minimal with respect to divisibility.

Now let $a, b \in I$ be two elements such that $[a]$ and $[b]$ are minimal with respect to divisibility. By condition (i) a and b have a greatest common divisor d which can be expressed as $d = ax + by$ for some $x, y \in R$. In particular, $d \in I$. Since a and b are minimal with respect to divisibility, we have that $[a] = [b] = [d]$. Therefore I has at least one element a that is minimal with regard to divisibility and all such elements are associate, and we have $I = \langle a \rangle$ and so I is principal. We conclude R is a principal ideal domain. $\square$

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.

Proof. Let $n = \frac{a^2}{b^2} + \frac{c^2}{d^2}$, or, equivalently, $n(bd)^2 = a^2d^2 + c^2b^2$. From this, we see that $n(bd)^2$ can be written as a sum of two squared integers. Therefore, if $q \equiv 3(\text{mod}4)$ and q^i appears in the prime power factorization of n, i must be even. Let $j \in \mathbb{N} \cup \{0\}$ such that q^j divides bd. Then q^{i-2j} divides n. But since i is even, $i - 2j$ is even as well. Consequently, n can be written as a sum of two squared integers. $\square$

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.

Proof. Suppose $a = a_1 + a_2\sqrt{-n}, b = b_1 + b_2\sqrt{-n} \in R$ are such that $2 = ab$, then $N(a)N(b) = 4$. Without loss of generality we can assume $N(a) \leq N(b)$, so $N(a) = 1$ or $N(a) = 2$. Suppose $N(a) = 2$, then $a_1^2 + na_2^2 = 2$ and since $n > 3$ we have $a_2 = 0$, which implies $a_1^2 = 2$, a contradiction. So $N(a) = 1$ and a is a unit. Therefore 2 is irreducible in R.

Suppose now $\sqrt{-n} = ab$, then $N(a)N(b) = n$ and we can assume $N(a) < N(b)$ since n is square free. Suppose $N(a) > 1$, then $a_1^2 + na_2^2 > 1$ and $a_1^2 + na_2^2 \mid n$, so $a_2 = 0$, and therefore $a_1^2 \mid n$. Since n is squarefree, $a_1 = \pm 1$, a contradiction. Therefore $N(a) = 1$ and so a is a unit and $\sqrt{-n}$ is irreducible.

Suppose $1 + \sqrt{-n} = ab$, then $N(a)N(b) = n+1$ and we can assume $N(a) \leq N(b)$. Suppose $N(a) > 1$, then $a_1^2 + na_2^2 > 1$ and $a_1^2 + na_2^2 \mid n+1$. If $|a_2| \geq 2$, then since $n > 3$ we have a contradiction since $N(a)$ is too large. If $|a_2| = 1$, then $a_1^2 + n$ divides $1 + n$ and so $a_1 = \pm 1$, and in either case $N(a) = n + 1$ which contradicts $N(a) \leq N(b)$. If $a_2 = 0$ then $a_1^2 \left(b_1^2 + nb_2^2\right) = \left(a_1 b_1\right)^2 + n\left(a_1 b_2\right)^2 = n + 1$. If $|a_1 b_2| \geq 2$ we have a contradiction. If $|a_1 b_2| = 1$ then $a_1 = \pm 1$ which contradicts $N(a) > 1$. If $|a_1 b_2| = 0$, then $b_2 = 0$ and so $a_1 b_1 = \sqrt{-n}$, a contradiction. Therefore $N(a) = 1$ and so a is a unit and $1 + \sqrt{-n}$ is irreducible. □

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

Proof. Let $a + bi \in \mathbb{Z}[i]$. If $a \equiv b \bmod 2$, then $a + b$ and $b - a$ are even and $(1+i)\left(\frac{a+b}{2} + \frac{b-a}{2} i\right) = a + bi \in \langle 1+i \rangle$. If $a \not\equiv b \bmod 2$ then $a - 1 + bi \in \langle 1+i \rangle$. Therefore every element of $\mathbb{Z}[i]$ is in either $\langle 1+i \rangle$ or $1 + \langle 1+i \rangle$, so $\mathbb{Z}[i]/\langle 1+i \rangle$ is a finite ring of order 2 , which must be a field. □

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.

Proof. The division algorithm gives us that every element of $\mathbb{Z}[i]/\langle q \rangle$ is represented by an element $a + bi$ such that $0 \leq a, b < q$. Each such choice is distinct since if $a_1 + b_1 i + \langle q \rangle = a_2 + b_2 i + \langle q \rangle$, then $(a_1 - a_2) + (b_1 - b_2)\, i$ is divisible by q, so $a_1 \equiv a_2 \bmod q$ and $b_1 \equiv b_2 \bmod q$. So $\mathbb{Z}[i]/\langle q \rangle$ has order q^2.

Since $q \equiv 3 \bmod 4, q$ is irreducible, hence prime in $\mathbb{Z}[i]$. Therefore $\langle q \rangle$ is a prime ideal in $\mathbb{Z}[i]$, and so $\mathbb{Z}[i]/\langle q \rangle$ is an integral domain. So $\mathbb{Z}[i]/\langle q \rangle$ is a field. □

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

Proof. Suppose, to the contrary, that $(x, y) = p$ for some polynomial $p \in \mathbb{Q}[x, y]$. From $x, y \in (x, y) = (p)$ there are $s, t \in \mathbb{Q}[x, y]$ such that $x = sp$ and $y = tp$. Then:

$$\begin{aligned}
&0 = \deg_y(x) = \deg_y(s) + \deg_y(p) \text{ so} \\
&0 = \deg_y(p) \\
&0 = \deg_x(y) = \deg_x(s) + \deg_x(p) \text{ so} \\
&0 = \deg_x(p) \text{ so}
\end{aligned}$$

From : $\quad 0 = \deg_y(p) = \deg_x(p)$ we get $\deg(p) = 0$ and $p \in \mathbb{Q}$. But $p \in (p) = (x, y)$ so $p = ax + by$ for some $a, b \in \mathbb{Q}[x, y]$

$$\begin{aligned}
\deg(p) &= \deg(ax + by) \\
&= \min(\deg(a) + \deg(x), \deg(b) + \deg(y)) \\
&= \min(\deg(a) + 1, \deg(b) + 1) \geqslant 1
\end{aligned}$$

which contradicts $\deg(p) = 0$. So we conclude that (x, y) is not principal ideal in $\mathbb{Q}[x, y]$ □

Exercise 9.1.10 Prove that the ring $\mathbb{Z}[x_1, x_2, x_3, \ldots] / (x_1x_2, x_3x_4, x_5x_6, \ldots)$ contains infinitely many minimal prime ideals.

Proof. Let $R = \mathbb{Z}[x_1, x_2, \ldots, x_n]$ and consider the ideal $K = (x_{2k+1}x_{2k+2} \mid k \in \mathbb{Z}_+)$in R. Consider the family of subsets $X = \{\{x_{2k+1}, x_{2k+2}\} \mid k \in \mathbb{Z}_+\}$, and Y the set of choice function on X, ie the set of functions $\lambda : \mathbb{Z}_+ \to \cup_{\mathbb{Z}_+} \{x_{2k+1}, x_{2k+2}\}$ with $\lambda(a) \in \{x_{2a+1}, x_{2a+2}\}$ For each $\lambda \in Y$ we have the ideal $I_\lambda = (\lambda(0), \lambda(1), \ldots)$. All these ideals are distinct, ie for $\lambda \neq \lambda'$ we have $I_\lambda \neq I_{\lambda'}$. We also have that by construction $K \subset I_\lambda$ for all $\lambda \in Y$. By the Third Isomorphism Treorem

$$(R/K) / (I_\lambda/K) \cong R/I_\lambda$$

Note also that R/I_λ is isomorphic to the polynomial ring over R with indeterminates the x_i not in the image of λ, and since there is a countably infinite number of them we can conclude $R/I_\lambda \cong R$, an integral domain. Therefore I_λ/K is a prime ideal of R/K

We prove now that I_λ/K is a minimal prime ideal. Let $J/K \subseteq I_\lambda/K$ be a prime ideal. For each pair (x_{2k+1}, x_{2k+2}) we have that $x_{2k+1}x_{2k+2} \in K$ so $x_{2k+1}x_{2k+2} \bmod K \in J/K$ so J must contain one of the elements in $\{x_{2k+1}, x_{2k+2}\}$. But since $J/K \subseteq I_\lambda/K$ it must be $\lambda(k)$ for all $k \in \mathbb{Z}_+$. Therefore $J/K = I_\lambda/K$ □

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.

Proof. Let $f(x), g(x) \in \mathbb{Q}[x]$ be such that $f(x)g(x) \in \mathbb{Z}[x]$. By Gauss' Lemma there exists $r, s \in \mathbb{Q}$ such that $rf(x), sg(x) \in \mathbb{Z}[x]$, and $(rf(x))(sg(x)) = rsf(x)g(x) = f(x)g(x)$. From this last relation we can conclude that $s = r^{-1}$.

Therefore for any coefficient f_i of $f(x)$ and g_j of $g(x)$ we have that $rf_i, r^{-1}g_j \in \mathbb{Z}$ and by multiplicative closure and commutativity of $\mathbb{Z}$ we have that $rf_ir^{-1}g_j = f_ig_j \in \mathbb{Z}$ □

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

Proof.

$$x^4 - 4x^3 + 6$$

The polynomial is irreducible by Eisenstiens Criterion since the prime 2 doesnt divide the leading coefficient 2 divide coefficients of the low order term $-4, 0, 0$ but 6 is not divided by the square of 2. □

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

Proof.

$$x^6 + 30x^5 - 15x^3 + 6x - 120$$

The coefficients of the low order.: $30, -15, 0, 6, -120$ They are divisible by the prime 3 , but $3^2 = 9$ doesn 't divide -120. So this polynomial is irreducible over $\mathbb{Z}$. □

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

Proof.

$$p(x) = x^4 + 6x^3 + 4x^2 + 2x + 1$$

We calculate $p(x-1)$

$$\begin{aligned}
(x-1)^4 &= x^4 - 4x^3 + 6x^2 - 4x + 1 \\
6(x-1)^3 &= 6x^3 - 18x^2 + 18x - 6 \\
4(x-1)^2 &= 4x^2 - 8x + 4 \\
2(x-1) &= 2x - 2 \\
1 &= 1
\end{aligned}$$

$p(x-1) = (x-1)^4 + 6(x-1)^3 + 4(x-1)^2 + 2(x-1) + 1 = x^4 + 2x^3 - 8x^2 + 8x - 2$

$q(x) = x^4 + 2x^3 - 8x^2 + 8x - 2$

$q(x)$ is irreducible by Eisenstiens Criterion since the prime \$2\$ divides the lower coefficient but \$2^2\$ doesnt divide constant -2. Any factorization of $p(x)$ would provide a factor of $p(x)(x-1)$ Since:

$$\begin{aligned}
p(x) &= a(x)b(x) \\
q(x) &= p(x)(x-1) = a(x-1)b(x-1)
\end{aligned}$$

We get a contradiction with the irreducibility of $p(x-1)$, so $p(x)$ is irreducible in $Z[x]$ □

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

Proof. $\frac{(x+2)^p - 2^p}{x}$ $\quad$ p is on add pprime $Z[x]$

$$\frac{(x+2)^p - 2^p}{x} \qquad \text{as a polynomial we expand } (x+2)^p$$

2^p cancels with -2^p, every remaining term has x as a factor

$$\begin{aligned}
&x^{p-1} + 2\begin{pmatrix} p \\ 1 \end{pmatrix} x^{p-2} + 2^2 \begin{pmatrix} p \\ 2 \end{pmatrix} x^{p-3} + \ldots + 2^{p-1}\begin{pmatrix} p \\ p-1 \end{pmatrix} \\
&2^k \begin{pmatrix} p \\ k \end{pmatrix} x^{p-k-1} = 2^k \cdot p \cdot (p-1) \ldots (p-k-1), \quad 0 < k < p
\end{aligned}$$

Every lower order coef. has p as a factor but doesnt have \$p^2\$ as a fuction so the polynomial is irreducible by Eisensteins Criterion. □

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.

Proof. $Z[\sqrt{2}]$ is an Euclidean domain, and so a unique factorization domain. We have to prove $p(x) = x^2 - \sqrt{2}$ irreducible. Suppose to the contrary. if $p(x)$ is reducible then it must have root. Let $a + b\sqrt{2}$ be a root of $x^2 - \sqrt{2}$. Now we have

$$a^2 + 2b^2 + 2ab\sqrt{2} = \sqrt{2}$$

By comparing the coefficients we get $2ab = 1$ for some pair of integers a and b, a contradiction. So $p(x)$ is irredicible over $Z[\sqrt{2}]$. □

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

Proof.

$$p(x) = x^2 + y^2 - 1 \in Q[y][x] \cong Q[y, x]$$

We have that $y+1 \in Q[y]$ is prime and $Q[y]$ is an UFD, since $p(x) = x^2+y^2-1 = x^2 +\ (y + 1)(y - 1)$ by the Eisenstein criterion $x^2 + y^2 - 1$ is irreducibile in $Q[x, y]$. □

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

Proof. Since B is a basis of V, every element of V can be written uniquely as a finite linear combination of elements of B. Let X be the set of all such finite linear combinations. Then X has the same cardinality as V, since the map from X to V that takes each linear combination to the corresponding element of V is a bijection.

We will show that X has the same cardinality as B. Since B is countable and X is a union of countable sets, it suffices to show that each set X_n, consisting of all finite linear combinations of n elements of B, is countable.

Let $P_n(X)$ be the set of all subsets of X with cardinality n. Then we have $X_n \subseteq P_n(B)$. Since B is countable, we have $\text{card}(P_n(B)) \leq \text{card}(B^n) = \text{card}(B)$, where B^n is the Cartesian product of n copies of B.

Thus, we have $\text{card}(X_n) \leq \text{card}(P_n(B)) \leq \text{card}(B)$, so X_n is countable. It follows that X is countable, and hence has the same cardinality as B.

Therefore, we have shown that the cardinality of V is equal to the cardinality of B. Since F is countable, it follows that the cardinality of V is countable as well.

Now let Q be a countable field, and let R be a vector space over Q. Let n be a positive integer. Then any basis of R^n over Q has the same cardinality as R^n, which is countable. Since R is a direct sum of n copies of R^n, it follows that any basis of R over Q has the same cardinality as R. Hence, the cardinality of R is countable.

Finally, since R is a countable vector space and Q is a countable field, it follows that R and $Q^{\oplus \text{card}(R)}$ are isomorphic as additive abelian groups. Therefore, we have $R \cong_Q Q^{\oplus \text{card}(R)}$, and in particular $R \cong_Q R^n$ for any positive integer n. □