# Homework for Introduction to Abstract Algebra I

Nicholas Camacho
Department of Mathematics
University of Iowa
Fall 2016

Most exercises are from
*Abstract Algebra* (3rd Edition) by Dummit & Foote.
For example, "4.2.8" means exercise 8
from section 4.2 in Dummit & Foote.
Beware: Some solutions may be incorrect!

0.3.13 Let $n \in \mathbb{Z}$, $n > 1$, and let $a \in \mathbb{Z}$ with $1 \leq a \leq n$. Prove that if $a$ and $n$ are relatively prime, then there is an integer $c$ such that $ac \equiv \pmod{n}$.

*Proof.* Let $n \in \mathbb{Z}$, $n > 1$, and let $a \in \mathbb{Z}$ with $1 \leq a \leq n$. Assume $a$ and $n$ are relatively prime. In other words, there exists integers $b$ and $c$ so that $nb + ac = 1$. Then, $1 - ac = nb$ and so $n$ divides $(1 - ac)$. Thus, $ac \equiv 1 \pmod{n}$. ■

1.1.8 Let $G = \{z \in \mathbb{C} | z^n = 1 \text{ for some } n \in \mathbb{Z}^+\}$.

(a) Prove that $G$ is a group under multiplication.

*Proof.* First, notice that $1 \in G$ as $1^1 = 1$. Since 1 is the identity element of $\mathbb{C}$ and $G \subset \mathbb{C}$, then 1 is the identity element of $G$. Similarly, since $\mathbb{C}$ is associative, and $G \subset \mathbb{C}$, then $G$ is also associative.

To show closure, first assume $x, y \in G$. Then, there exists $n, m \in G$ so that $x^n = 1$ and $y^m = 1$. Notice that $x^{nm} = (x^n)^m = 1^m = 1$ and similarly $y^{nm} = y^{mn} = (y^m)^n = 1^n = 1$. Since $x, y \in \mathbb{C}$ and $\mathbb{C}$ is an abelian group we can compute

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

Thus, $xy \in G$ and hence $G$ is closed under multiplication.

Next, by properties of complex numbers, we know that $xx^{-1} = 1$, i.e., $x^{-1}$ is the inverse of $x$. To see that $x^{-1} \in G$, simply observe that $(x^{-1})^n = x^{-n} = (x^n)^{-1} = 1^{-1} = 1$. Thus, $G$ contains inverses. ■

(b) Prove that $G$ is not a group under addition.

*Proof.* $G$ is not a group under addition because there is no identity element. To show this, we assume that $G$ is a group with identity element $e$. Let $x \in G$ and notice that by a group axiom, $e + x = x$. Applying the inverse of $x$ to both sides on the right gives $e = 0$. But, $0^n = 0$ for all $n \in \mathbb{Z}^+$ so $e \notin G$. $\Rightarrow\Leftarrow$ ■

1.1.19 Let $x \in G$ and let $a, b \in \mathbb{Z}^+$

(a) Prove that $x^{a+b} = x^a x^b$ and $(x^a)^b = x^{ab}$

*Proof.* $x^{a+b} = \underbrace{x \cdot x \cdots x}_{a+b \text{ times}} = \underbrace{(x \cdot x \cdots x)}_{a \text{ times}} \cdot \underbrace{(x \cdot x \cdots x)}_{b \text{ times}} = x^a x^b$

$(x^a)^b = \underbrace{x^a \cdot x^a \cdots x^a}_{b \text{ times}} = \underbrace{\underbrace{(x \cdot x \cdots x)}_{a \text{ times}} \cdot \underbrace{(x \cdot x \cdots x)}_{a \text{ times}} \cdots \underbrace{(x \cdot x \cdots x)}_{a \text{ times}}}_{b \text{ times}} = x^{ab}$ ■

(b) Prove that $(x^a)^{-1} = x^{-a}$.

*Proof.* Since $x \in G$, then $x^a \in G$ by closure in groups. Thus, $(x^a)^{-1} \in G$ and

$$x^a \cdot (x^a)^{-1} = 1 \tag{1}$$

Then, multiplying both sides of (1) by $x^{-1}$ exactly $a$-times on the left,

$$\underbrace{(x^{-1} \cdot x^{-1} \cdots x^{-1})}_{a \text{ times}}(x^a \cdot (x^a)^{-1}) = \underbrace{(x^{-1} \cdot x^{-1} \cdots x^{-1})}_{a \text{ times}} \cdot 1.$$

Then, after we re-associate and write $x^a$ as $x \cdot x \cdots x$ (exactly $a$ times), we have

$$(\underbrace{x^{-1} \cdot x^{-1} \cdots x^{-1}}_{a \text{ times}} \cdot \underbrace{x \cdot x \cdots x}_{a \text{ times}})(x^a)^{-1} = \underbrace{(x^{-1} \cdot x^{-1} \cdots x^{-1})}_{a \text{ times}}.$$

Thus,

$$(x^a)^{-1} = x^{-a}.$$

■

(c) Establish part (a) for arbitrary integers $a$ and $b$.

*Proof.*

*Case* 1 — $a, b \in \mathbb{Z}^+$ completed in part (a).
*Case* 2 — $a, b \in \mathbb{Z}^-$

(i) $x^{a+b} = (x^{-a-b})^{-1} = (x^{-b-a})^{-1} \overbrace{=}^{\text{by Case 1}} (x^{-b}x^{-a})^{-1} = (x^{-a})^{-1}(x^{-b})^{-1} = x^a x^b$

(ii) $(x^a)^b = ((x^a)^{-b})^{-1} = (\underbrace{x^a \cdot x^a \cdots x^a}_{-b \text{ times}})^{-1}$

$$= \left( \underbrace{\underbrace{(x \cdot x \cdots x)}_{a \text{ times}} \cdot \underbrace{(x \cdot x \cdots x)}_{a \text{ times}} \cdots \underbrace{(x \cdot x \cdot \cdots x)}_{a \text{ times}}}_{-b \text{ times}} \right)^{-1} = (x^{-ab})^{-1} = x^{ab}$$

*Case* 3 — $a \in \mathbb{Z}^+, b \in \mathbb{Z}^-$.

(i) • If $|b| < a$, then $a + b > 0$. First, notice that

$$(x^{a+b})(x^{-b}x^{-a}) = x^{a+b-b}x^{-a} = x^a x^{-a} = 1$$

Thus, $(x^{a+b})^{-1} = (x^{-b}x^{-a}) = (x^a x^b)^{-1}$. Then, since inverses are unique, $x^{a+b} = x^a x^b$

• If $|b| > a$, then $a + b < 0$ which implies $-b - a > 0$. Using the previous subcase,

$$x^{a+b} = (x^{-b-a})^{-1} = (x^{(-b)+(-a)})^{-1} = (x^{-b}x^{-a})^{-1} = (x^{-a})^{-1}(x^{-b})^{-1} = x^a x^b$$

- If $|b| = a$, then $a + b = 0$. Notice that this implies $x^a = x^{-b}$. Then,

$$x^{a+b} = x^0 = 1 = x^a x^{-a} = x^a x^b$$

---

(ii)

$$(x^a)^b = ((x^a)^{-b})^{-1} \overbrace{=}^{\text{by Case 1}} (x^{-ab})^{-1} = x^{ab}$$

*Case* 4 — $a = 0, b \in \mathbb{Z}$.

(i) $x^{a+b} = x^{0+b} = x^b = 1 \cdot x^b = x^0 x^b = x^a x^b$

(ii) $(x^a)^b = (x^0)^b = 1^b = 1 = x^0 = x^{0 \cdot b} = x^{ab}$

■

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

*Proof.* Let $x^2 = 1$ for all $x$ in a group $G$. Let $x, y \in G$. By closure in groups, $(xy) \in G$ and so $(xy)(xy) = 1$. Then,

$$\begin{aligned}
(xy)(xy) &= 1 \\
(yx)(xy)(xy) &= (yx)1 \\
y(xx)yxy &= yx \\
y(1)yxy &= yx \\
(yy)xy &= yx \\
xy &= yx
\end{aligned}$$

and so $G$ is abelian. ■

1.2.4 If $n = 2k$ is even and $n \geq 4$, show that $z = r^k$ is an element of order 2 which commutes with all elements of $D_{2n}$. Show that $z$ is the only nonidentity element in $D_{2n}$ which commutes with all elements in $D_{2n}$.

*Proof.* Let $n = 2k$ be even with $n \geq 4$. Consider the element $z = r^k \in D_{2n}$. Clearly, $z^2 = r^{2k} = r^n = 1$ and so the order of $z$ is 2. Now, we prove that $z$ commutes with all elements of $D_{2n}$. First, we note that $z$ commutes trivially with the identity. Next, we see that $z$ commutes with all rotations because, for an arbitrary rotation $r^m$ with $1 \leq m \leq n-1$, we have

$$r^k r^m = r^{k+m} = r^{m+k} = r^m r^k$$

Finally, we claim that

$$r^k s = s r^{-k} \tag{$*$}$$

Using the relation $rs = sr^{-1}$, we prove $(*)$ by showing that

$$r^k s = \underbrace{rr\cdots r}_{k-1 \text{ times}}(rs) = \underbrace{rr\cdots r}_{k-1 \text{ times}}(sr^{-1}) = \underbrace{rr\cdots r}_{k-2 \text{ times}}(rs)r^{-1} = \underbrace{rr\cdots r}_{k-2 \text{ times}}(sr^{-1})r^{-1} = \cdots = sr^{-k}.$$

Now, notice that since $r^n = 1$ then $r^{2k} = 1$, which implies $r^k = r^{-k}$. Then, by $(*)$,

$$r^k s = sr^{-k} \implies r^k s = sr^k,$$

and so $r^k$ commutes with the reflection $s$.
Now, to show that $z$ is the only nonidentity element which commutes with all elements in $D_{2n}$, first let $r^t$ be an any rotation, $t \neq k$. Now, we want to show that $r^t \neq r^{-t}$. So, assume that in fact $r^t = r^{-t}$. This would imply $r^{2t} = 1 = r^n$. In other words, $2t = n$, and thus $t = k$, a contradiction. By $(*)$ we know that $r^t s = sr^{-t}$. Since $r^t \neq r^{-t}$, then $r^t s \neq sr^t$. So, $r^t$ does not commute with all elements in $D_{2n}$. We've also show that, the only other nonidentity element in $D_{2n}$, $s$, does not commute with all elements in $D_{2n}$. ■

1.3.2

$$\begin{aligned}
\sigma &= (1\ 13\ 5\ 10)(3\ 15\ 8)(4\ 14\ 11\ 7\ 12\ 9) \\
\tau &= (1\ 14)(2\ 9\ 15\ 13\ 4)(3\ 10)(5\ 12\ 7)(8\ 11) \\
\sigma^2 &= (1\ 5)(3\ 8\ 15)(4\ 11\ 12)(7\ 9\ 14)(10\ 13) \\
\sigma\tau &= (1\ 11\ 3)(2\ 4)(5\ 9\ 8\ 7\ 10\ 15)(13\ 14) \\
\tau\sigma &= (1\ 4)(2\ 9)(3\ 13\ 12\ 15\ 11\ 5)(8\ 10\ 14) \\
\tau^2\sigma &= (1\ 2\ 15\ 8\ 3\ 4\ 14\ 11\ 12\ 13\ 7\ 5\ 10)
\end{aligned}$$

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

*Proof.* Let $x, g \in G$ and $|g^{-1}xg| = n < \infty$. Then,

$$\begin{aligned} (g^{-1}xg)^n &= 1 && (*) \\ \underbrace{(g^{-1}xg)(g^{-1}xg)\cdots(g^{-1}xg)}_{n \text{ factors}} &= 1 \\ g^{-1}x(gg^{-1})x(gg^{-1})x\cdots x(gg^{-1})xg &= 1 \\ g^{-1}x(1)x(1)x(1)x\cdots x(1)x(1)xg &= 1 \\ g^{-1}\underbrace{(xx\cdots x)}_{n \text{ factors}}g &= 1 \\ g^{-1}x^n g &= 1 && (**) \\ (g)g^{-1}x^n g(g^{-1}) &= (g)1(g^{-1}) \\ x^n &= gg^{-1} \\ x^n &= 1 \end{aligned}$$

Hence, $|g^{-1}xg| = n$ implies $|x| = n$. Following the equations in the opposite direction shows $|x| = n \iff |g^{-1}xg| = n$, i.e., $|x| = |g^{-1}xg|$.
Notice that $(*) \implies (**)$, which then implies

$$(g^{-1}xg)^n = g^{-1}x^n g$$

Now, by way of contradiction, suppose $|g^{-1}xg|$ is infinity, but $|x| = n < \infty$. Then,

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

a contradiction. Similarly, suppose $|x|$ is infinite, but $|g^{-1}xg| = n < \infty$. Then,

$$1 = (g^{-1}xg)^n = g^{-1}x^n g.$$

Then,

$$1 = g^{-1}x^n g \implies gg^{-1} = x^n \implies 1 = x^n,$$

a contradiction. Thus, $|x|$ is infinite if and only if $|g^{-1}xg|$ is infinite.

Now, let $a, b \in G$, $x = ab$, and $g = a$. Then,

$$|ab| = |x| = |g^{-1}xg| = |(a^{-1})(ab)(a)| = |(a^{-1}a)ba| = |ba|$$

■

1.1.23 Suppose $x \in G$ and $|x| = n < \infty$. If $n = st$ for some positive integers $s$ and $t$, prove that $|x^s| = t$.

*Proof.* Notice that $1 = x^n = x^{st} = (x^s)^t$. Hence, $|x^s| \leq t$. Assume that $|x^s| = q < t$. This implies $sq < st = n$, and so $1 = (x^s)^q = x^{sq}$, i.e., $|x| = sq < st = n$, a contradiction. Thus, $|x^s| = t$. ■

1.3.10 Prove that if $\sigma$ is the $m$-cycle $(a_1\ a_2 \ldots a_m)$, then for all $i \in \{1, 2, , \ldots, m\}, \sigma^i(a_k) = a_{k+i}$, where $k+i$ is replaced by its least residue mod $m$ when $k+i > m$. Deduce that $|\sigma| = m$.

*Proof.* Let $a_k \in \sigma$. We proceed by induction on $i$. For the base case, let $i = 1$. By definition of the function $\sigma$, we see that $\sigma^1(a_k) = (a_1\ a_2 \ldots a_m)(a_k) = a_{k+1 \pmod m}$. For the inductive step, assume that $\sigma^n(a_k) = a_{k+n}$ for $1 \leq n \leq i$. Then,

$$\sigma^{i+1}(a_k) = (\sigma^1 \circ \sigma^i)(a_k) = (\sigma^1)(a_{k+i}) = a_{k+i+1}$$

and so the conclusion holds. Now, we claim $|\sigma| = m$. That is, $\sigma^m(a_k) = a_k$ for $1 \leq k \leq m$. By way of contradiction, assume otherwise. That is, $\sigma^m(a_k) \neq a_k$. So,

$$a_{k+m} = \sigma^m(a_k) \neq a_k$$

This implies $k + m \neq k$, which implies $m \neq 0$ mod $m$, a contradiction. Thus, $|\sigma| = m$. ■

1.3.11 Let $\sigma$ be the $m$-cycle $(1, 2, \ldots, m)$. Show that $\sigma^i$ is also an $m$-cycle if and only if $i$ is relatively prime to $m$.

*Proof.* First note that since $\sigma$ is an $m$-cycle, then $o(\sigma) = m$ by the previous exercise. Again by the previous exercise, $\sigma^i$ is an $m$-cycle if and only if $o(\sigma^i) = m$. By Proposition 5,

$$m = o(\sigma^i) = \frac{o(\sigma)}{gcd(m,i)} = \frac{m}{gcd(m,i)},$$

and clearly $m = m/gcd(m,i)$ if and only if $gcd(m,i) = 1$, i.e., $m$ and $i$ are relatively prime. ■

1.3.16 Show that if $n \geq m$, then the number of $m$-cycles in $S_n$ is given by

$$\frac{n(n-1)(n-2)\cdots(n-m+1)}{m}$$

*Proof.* If we want to construct an $m$-cycle in $S_n$, $n \geq m$ then we have $n$ choices for the first element in the cycle, $(n-1)$ choices for the second element in the cycle, $(n-2)$ choices for the third element in the cycle, etc. In general, there are $n-i$ choices for the $i+1$ element in the cycle. Since we want exactly $m$ elements in our cycle, there are $(n-(m-1)) = n-m+1$ choices for the last element in our cycle. So, there are

$$n(n-1)(n-2)\cdots(n-m+1)$$

ways to construct an $m$-cycle. However, since each cycle can be represented in $m$ different ways, we have over-counted by a factor of $m$, and so we divide by $m$ to obtain

$$\frac{n(n-1)(n-2)\cdots(n-m+1)}{m}$$

$m$-cycles in $S_n$. ■

1.3.17 Show that if $n \geq 4$, then the number of permutations in $S_n$ which are the product of two disjoint 2-cycles is $n(n-1)(n-2)(n-3)/8$.

*Proof.* Any permutation in $S_n$ that can be written as the product of two disjoint 2-cycles will look like $(qr)(st)$. In this representation, there are $n$ choices for $q$, $(n-1)$ choices for $r$, $(n-2)$ choices for $s$, and finally $(n-3)$ choices for $t$. So, we have $n(n-1)(n-2)(n-3)$ permutations in $S_n$ that can be written this way. However, since there are 2 ways to write the permutation $(qr)$, 2 ways to write the permutation $(st)$, and 2 ways to write the product $(qr)(st)$, we must divide by a factor of $2 \cdot 2 \cdot 2 = 8$. Thus, there are $n(n-1)(n-2)(n-3)/8$ number of permutations in $S_n$ which are the product of two disjoint 2-cycles.

■

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 $\varphi : G \to G$ defined by $g \to g^{-1}$ is a homomorphism. Let $a, b \in G$. Then

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

and thus $G$ is abelian.
($\Leftarrow$) Suppose $G$ is abelian. Let $a, b \in G$ and let the map $\varphi : G \to G$ be defined by $g \mapsto g^{-1}$. Then

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

and thus $\varphi$ is a homomorphism. ■

1.6.20 Prove that $\text{Aut}(G)$ is a group under function composition.

*Proof.* We show that $\text{Aut}(G)$ is a subgroup of $S_G$ and thus a group. Since $S_G$ is the set of all bijections from $G$ to itself, then certainly all of the homomorphic bijections from $G$ to itself are in $S_G$, and thus, $\text{Aut}(G) \subseteq S_G$. Notice that $\text{Aut}(G) \neq \emptyset$ since the identity map $\varphi : G \to G$ defined by $g \mapsto g$ is in $\text{Aut}(G)$. Now, let $\varphi, \psi \in \text{Aut}(G)$. Then, $\varphi \circ \psi^{-1} : G \to G$ is in $\text{Aut}(G)$ since isomorphic functions are closed under function composition. Therefore, $\text{Aut}(G)$ is a subgroup of $S_G$ by the Subgroup Test. ■

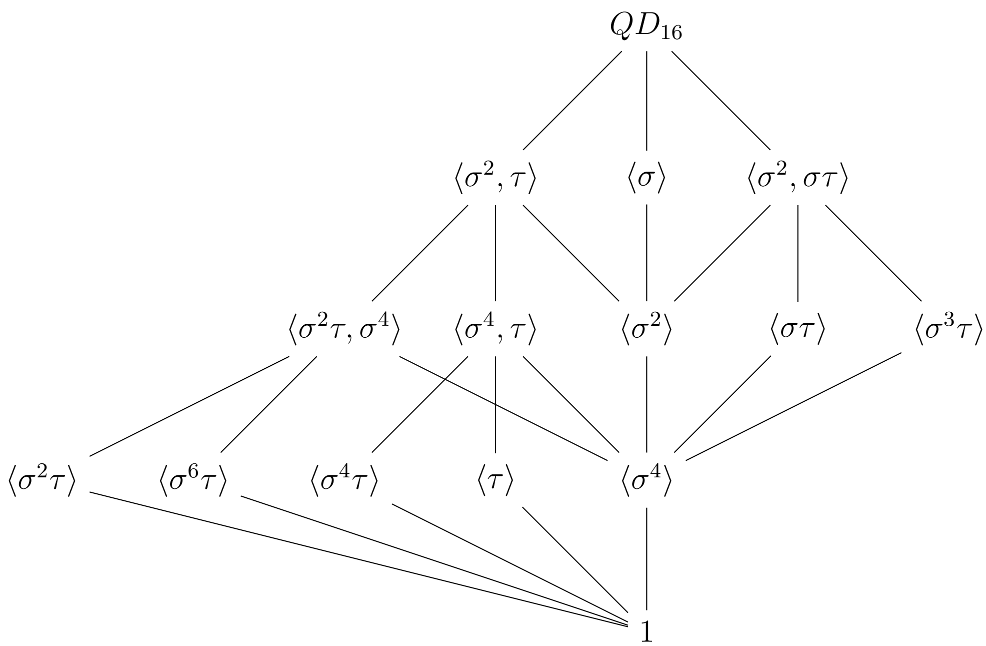
2.1.15 Let $H_1 \leq H_2 \leq \ldots$ be an ascending chain of subgroups of $G$. Prove that $\cup_{i=1}^{\infty} H_i$ is a subgroup of $G$.

*Proof.* Since $1_G \in H_i$ for all $i$, then $1_G \in \cup_{i=1}^{\infty} H_i$ and so $\cup_{i=1}^{\infty} H_i \neq \emptyset$. Let $a, b \in \cup_{i=1}^{\infty} H_i$. So, there exists $j$ and $k$ so that $a \in H_j$ and $b \in H_k$. Let $m = \max\{j, k\}$. So, $a, b \in H_m$ and thus $ab^{-1} \in H_m$ by closure in groups and so $ab^{-1} \in \cup_{i=1}^{\infty} H_i$. Thus, $\cup_{i=1}^{\infty} H_i$ is a subgroup of $G$ by the Subgroup Test. ■

2.5.11 Subgroup lattice of

$$QD_{16} = \langle \sigma, \tau | \sigma^8 = \tau^2 = 1, \sigma\tau = \tau\sigma^3 \rangle$$

**Solution:**




3.1.1 Let $\varphi : G \to H$ be a homomorphism and let $E$ be a subgroup of $H$. Prove that $\varphi^{-1}(E) \leq G$ (i.e., the preimage or pullback of a subgroup under a homomorphism is a subgroup). If $E \trianglelefteq H$ prove that $\varphi^{-1}(E) \trianglelefteq G$. Deduce that $\ker \varphi \trianglelefteq G$.

*Proof.* Let $\varphi : G \to H$ be a homomorphism and let $E \leq H$. We first show that $\varphi^{-1}(E) \leq G$. First note that $\varphi^{-1}(E) = \{g \in G | \varphi(g) \in E\}$. Since $E \leq H$, $1_H \in E$ and so $\varphi^{-1}(1_H) = 1_G$ is in $\varphi^{-1}(E)$. Thus, $\varphi^{-1}(E) \neq \emptyset$. Now, let $a, b \in \varphi^{-1}(E)$. Then

$$\varphi(ab^{-1}) = \varphi(a)\varphi(b^{-1}) = \varphi(a)\varphi(b)^{-1} \in E \;\text{ by closure in } E.$$

Thus, $ab^{-1} \in \varphi^{-1}(E)$ and so $\varphi^{-1}(E) \leq G$ by the Subgroup Test.

---

Now suppose $E \trianglelefteq H$. Let $g \in G$ and let $a \in \varphi^{-1}(E)$. Then,

$$\varphi(gag^{-1}) = \varphi(g)\phi(a)\varphi(g)^{-1} \in E \;\text{ since } E \trianglelefteq H,$$

and thus $gag^{-1} \in \varphi^{-1}(E)$.

---

Since $\{1_H\} \trianglelefteq H$ — $(h1_Hh^{-1} = 1_H \in \{1_h\} \forall h \in H)$ — then $\ker \varphi = \varphi^{-1}(1_h) \trianglelefteq G$ by the previous proof. ∎

3.1.29 Let $N$ be a *finite* subgroup of $G$ and suppose $G = \langle T \rangle$ and $N = \langle S \rangle$ for some subsets $S$ and $T$ of $G$. Prove that $N$ is normal in $G$ if and only if $tSt^{-1} \subseteq N$ for all $t \in T$.

*Proof.* ($\Rightarrow$)

$$N \trianglelefteq G \implies t\langle S \rangle t^{-1} \subseteq N \ \forall t \in T \implies tSt^{-1} \subseteq N \ \forall t \in T$$

($\Leftarrow$) Suppose $tSt^{-1} \subseteq N$. This implies that $\langle tSt^{-1} \rangle \subseteq N$ by closure in $N$. Note that since the conjugate of a product is the product of conjugates, then for all $t \in T$, we have $t\langle S \rangle t^{-1} = \langle tSt^{-1} \rangle$.

$$tNt^{-1} = t\langle S \rangle t^{-1} = \langle tSt^{-1} \rangle \subseteq N$$

Since $N$ is finite, $|tNt^{-1}| = |N|$, and thus, $tNt^{-1} = N$ for all $t \in T$. This implies $T \subseteq N_G(N)$, and so $G = \langle T \rangle \subseteq N_G(N)$, and then $G = N_G(N)$ which means $N \trianglelefteq G$. ■

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

*Proof.* Let $H = \{g \in G \mid |g| < \infty\}$. Notice that $1_G \in H$ since $(1_G)^1 = 1_G$. Let $x, y \in H$. Then $x^n = 1$ and $y^m = 1$ for some $n, m \in \mathbb{Z}^+$. Notice that $x^{nm} = (x^n)^m = 1^m = 1$ and $(y^{-1})^{nm} = (y^m)^{-n} = 1^{-n} = 1$. Then, since $G$ is abelian,

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

and so $xy \in\in H$. Thus $H$ is a subgroup of $G$ by the subgroup test.

---

Consider the nonabelian group $SL_2(\mathbb{Z})$. Notice that

$$\left|\begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}\right| = 6 \quad \text{and} \quad \left|\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\right| = 4$$

but

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

which has infinite order since

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^k = \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}$$

for all $k \in \mathbb{Z}^+$.

■

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

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

(a) Prove that $\sigma_a$ is an automorphism of $Z_n$ if and only if $a$ and $n$ are relatively prime.

*Proof.* ($\Rightarrow$) Suppose $\sigma_a$ is an automorphism of $Z_n$ and let $x^k \in Z_n$ for $1 \leq k \leq n$. By surjectivity of $\sigma_a$, there exists $x^\ell \in Z_n$ so that $\phi_a(x^\ell) = x^k$. Notice that

$$(x^a)^\ell = (x^\ell)^a = \phi_a(x^\ell) = x^k$$

Since this is true for each $k \in \{1, \dots, n-1\}$, we have that $\langle x^a \rangle = Z_n$. This means that $(a, n) = 1$ by Proposition 6 (2).
($\Leftarrow$) Conversely, suppose $(a, n) = 1$ and let $x, y \in Z_n$. Then, as $Z_n$ is abelian,

$$\phi_a(xy) = (xy)^a = x^a y^a = \phi_a(x)\phi_b(x)$$

and so $\phi_a$ is a homomorphism. We now show that $\phi_a$ is bijective. Note that since $(a, n) = 1$, there exists integers $w, z$ so that $aw = 1 - zn$. Let $x^k \in Z_n$. Then,

$$\phi_a(x^{wk}) = (x^{wk})^a = (x^{aw})^k = (x^{(1-zn)})^k = (x^1(x^n)^{-z})^k = x^k$$

and thus $\phi_a$ is surjective. Since we have a surjective map between two groups of the same cardinality, the map must also be injective. Thus, $\phi_a$ is a automorphism of $Z_n$. ■

(b) Prove that $\sigma_a = \sigma_b$ if and only if $a \equiv b \pmod{n}$.

*Proof.*

$$\begin{aligned} \sigma_a = \sigma_b &\iff x^a = \sigma_a(x) = \sigma_b(x) = x^b \\ &\iff x^{a-b} = 1 \\ &\iff (a-b)|n \\ &\iff a \equiv b \pmod{n} \end{aligned}$$

■

(c) Prove that *every* automorphism of $Z_n$ is equal to $\sigma_a$ for some integer $a$.

*Proof.* Let $\phi$ be an automorphism of $Z_n$. Then, since $x$ generates $Z_n$, we have $\phi(x) = x^k$ for some $0 \leq k \leq n-1$. So, for any $x^\ell \in Z_n$

$$\phi(x^\ell) = \phi(x)^\ell = x^{k\ell} = x^{\ell k} = \sigma_k(x^\ell)$$

■

(d) Prove that $\sigma_a \circ \sigma_b = \sigma_{ab}$. Deduce that the map $\overline{a} \to \sigma_a$ is an isomorphism of $(\mathbb{Z}/n\mathbb{Z})^\times$ onto the automorphism group of $Z_n$ (so $\mathrm{Aut}(Z_n)$ is an abelian group of order $\varphi(n)$).

*Proof.* Let $x^\ell \in Z_n$ for $0 \leq k \leq n-1$. Then,

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

Thus, we see that the map

$$\varphi : (\mathbb{Z}/n\mathbb{Z})^\times \to \mathrm{Aut}(Z_n)$$

defined by $\overline{a} \to \sigma_a$ is a homomorphism by what was just shown, an injection by part (*b*), and a surjection by part (*c*). ■

3.1.14 Consider the additive quotient group $\mathbb{Q}/\mathbb{Z}$.

(a) Show that every coset of $\mathbb{Z}$ in $\mathbb{Q}$ contains exactly one representative $q \in \mathbb{Q}$ in the range $0 \leq q < 1$.

*Proof.* We first show the existence of such a $q$. We define the rationals to be $\mathbb{Q} = \{a/b \mid a \in \mathbb{Z}, b \in \mathbb{Z}^+\}$. Given any rational, $a/b$, then by the Division Algorithm, there exists $m, r \in \mathbb{Z}, 0 \leq r < b$ so that $a = mb + r$. So,

$$\frac{a}{b} = m + \frac{r}{b}$$

and thus $a/b + \mathbb{Z} = r/b + \mathbb{Z}$, since $a/b$ and $r/b$ differ by an integer. Since $r < b$, then $0 \leq r/b < 1$ and so our representative is $q = r/b$. That was fun; now onto uniqueness. Suppose that $k + \mathbb{Z} = q + \mathbb{Z}$ for $0 \leq k, q < 1$. Then

$$k + \mathbb{Z} = q + \mathbb{Z} \implies (k - q) + \mathbb{Z} = \mathbb{Z} \implies (k - q) \in \mathbb{Z}$$

Since $0 \leq k, q < 1$ and $(k - q) \in \mathbb{Z}$, it must be the case that $k - q = 0$, i.e., $k = q$. So, $q$ is unique! ■

(b) Show that every element of $\mathbb{Q}/\mathbb{Z}$ has finite order but that there are elements of arbitrarily large order.

*Proof.* Given a coset $a/b + \mathbb{Z}$ in $\mathbb{Q}/\mathbb{Z}$, the order of this coset is at most $b$ since

$$\left(\frac{a}{b} + \mathbb{Z}\right) b = a + b\mathbb{Z} = a + \mathbb{Z} = \mathbb{Z}$$

Consider the coset $1/n + \mathbb{Z}$. Since $1/n$ is in lowest terms, the order of this coset is $n$, which can be made arbitrarily large. ■

(c) Show that $\mathbb{Q}/\mathbb{Z}$ is the torsion subgroup of $\mathbb{R}/\mathbb{Z}$.

*Proof.* Let $H$ be the torsion subgroup of $\mathbb{R}/\mathbb{Z}$. By part $(b)$, we know that $\mathbb{Q}/\mathbb{Z} \subseteq H$. To see that $\mathbb{Q}/\mathbb{Z} = H$, we prove that all cosets in $\mathbb{Q}^c/\mathbb{Z}$ are not in $H$. To get a contradiction, assume there was a $i + \mathbb{Z} \in \mathbb{Q}^c/\mathbb{Z}$ so that $|i + \mathbb{Z}| = n < \infty$ for some $n \in \mathbb{Z}^+$. This implies,

$$(i + \mathbb{Z})n = in + n\mathbb{Z} = in + \mathbb{Z} \implies in \in \mathbb{Z}$$

So, $in = z$ for some integer $z$. This implies $i = z/n$, i.e., $i$ is rational, a contradiction. Thus, no such coset exists. Therefore, $\mathbb{Q}/\mathbb{Z} = H$. ■

(d) Prove that $\mathbb{Q}/\mathbb{Z}$ is isomorphic to the multiplicative group of root of unity in $\mathbb{C}^\times$.

*Proof.* We claim that $\varphi : \mathbb{Q}/\mathbb{Z} \to Z(\mathbb{C}^\times)$ defined by $(q + \mathbb{Z}) \mapsto e^{2\pi i q}$ is an isomorphism. Let $q + \mathbb{Z}, k + \mathbb{Z} \in \mathbb{Q}/\mathbb{Z}$. Then,

$$\varphi((q + \mathbb{Z}) + (k + \mathbb{Z})) = \varphi((q + k) + \mathbb{Z}) = e^{2\pi i(q+k)} = e^{2\pi i q}e^{2\pi i k} = \varphi(q + \mathbb{Z})\varphi(k + \mathbb{Z})$$

and so $\varphi$ preserves operation. Note that if $e^{2\pi i n} = 1$, then $n \in \mathbb{Z}$ because

$$1 = e^{2\pi i n} = \cos(2\pi n) + i \sin(2\pi n) \implies \sin(2\pi n) = 0 \quad \text{and} \quad \cos(2\pi n) = 1$$

which occurs only when $n \in \mathbb{Z}$. Now, assume $\varphi(q + \mathbb{Z}) = \varphi(k + \mathbb{Z})$. Then

$$e^{2\pi i q} = e^{2\pi i k} \implies e^{2\pi i(q-k)} = 1$$

which only occurs when $q - k \in \mathbb{Z}$, which means $(q - k) + \mathbb{Z} = \mathbb{Z}$ and so $q + \mathbb{Z} = k + \mathbb{Z}$. Thus, $\varphi$ is injective. Let $e^{2\pi i q} \in Z(\mathbb{C}^\times)$. Then, there exists $n \in \mathbb{Z}^+$ so that

$$1 = (e^{2\pi i q})^n = e^{2\pi i q n}$$

which means $qn = z \in \mathbb{Z}$ and thus, $\mathbb{Q} \ni q = z/n$. Thus, $\varphi(q) = e^{2\pi i q}$. Therefore, $\varphi$ is an isomorphism. ■

3.1.34 Let $D_{2n} = \langle r, s | r^n = s^2 = 1, rs = sr^{-1}\rangle$ be the usual presentation of the dihedral group of order $2n$ and let $k$ be a positive integer dividing $n$.

(a) Prove that $\langle r^k \rangle$ is a normal subgroup of $D_{2n}$

*Proof.* Given $r^\ell \in \langle r^k \rangle$, and $r^q \in D_{2n}$, notice that

$$r^q r^\ell r^{-q} = r^\ell \in \langle r^k \rangle$$

and

$$sr^\ell s^{-1} = (r^\ell)^{-1} = r^{n-\ell} \in \langle r^k \rangle$$

and thus $g\langle r^k \rangle g^{-1} \subseteq \langle r^k \rangle$ for all $g \in D_{2n}$ and so $\langle r^k \rangle \trianglelefteq D_{2n}$. ■

(b) Prove that $D_{2n}/\langle r^k \rangle \cong D_{2k}$.

*Proof.* Note that $D_{2k} = \langle \rho, \sigma \mid \rho^k = 1 = \sigma^2, \rho\sigma = \sigma\rho^{-1}\rangle$.
We first show that the quotient group $D_{2n}/\langle r^k \rangle$ is generated by two elements which satisfy the same relations as the two generators of $D_{2k}$. We claim that these are $r\langle r^k \rangle$ and $s\langle r^k \rangle$. First notice that the smallest $i \in \mathbb{Z}^+$ so that $(r\langle r^k \rangle)^i = \langle r^k \rangle$ is also the smallest $i \in \mathbb{Z}^+$ so that $r^i \in \langle r^k \rangle$. Since $\langle r^k \rangle = \{1, r^k, r^{2k}, \dots r^{mk-1}\}$, (assuming $n = mk, k \in \mathbb{Z}^+$), then it is clear that $i = k$. Thus, $|r\langle r^k \rangle| = k$. Likewise, $(s\langle r^k \rangle)^\ell = \langle r^k \rangle$ when $s^\ell \in \langle r^k \rangle$. The smallest $\ell \in \mathbb{Z}^+$ with such a property is clearly $\ell = 2$. So, $|s\langle r^k \rangle| = 2$. Now, notice that

$$(r\langle r^k \rangle)(s\langle r^k \rangle) = (rs)\langle r^k \rangle = (sr^{-1})\langle r^k \rangle = s\langle r^k \rangle r^{-1}\langle r^k \rangle$$

Thus, the generators $r\langle r^k \rangle$ and $s\langle r^k \rangle$ satisfy the same relations as $\rho$ and $\sigma$, respectively. Therefore, we define a map $\psi : D_{2n}/\langle r^k \rangle \to D_{2k}$ by

$$r\langle r^k \rangle \mapsto \rho \quad \text{and} \quad s\langle r^k \rangle \mapsto \sigma$$

Let $s^\ell\langle r^k \rangle, r^i\langle r^k \rangle \in D_{2n}/\langle r^k \rangle$. Then,

$$\psi(s^\ell\langle r^k \rangle r^i\langle r^k \rangle) = \psi(s^\ell r^i\langle r^k \rangle) = \sigma^\ell\rho^i = \psi(s^\ell\langle r^k \rangle)\psi(r^i\langle r^k \rangle)$$

and so $\phi$ preserves operation. If $\sigma^{\ell_1}\rho^{i_1} = \sigma^{\ell_2}\rho^{i_2}$, then $s^{\ell_1}r^{i_1} = s^{\ell_2}r^{i_2}$, and so $\sigma^{\ell_1-\ell_2}\rho^{i_1-i_2} = 1$, which means $\ell_1 - \ell_2 = 0$ and $i_1 - i_2 = 0$, i.e., $\ell_1 = \ell_2$ and $i_1 = i_2$. Thus, $\psi$ is injective. Suppose $\sigma^\ell\rho^i \in D_{2k}$. Then,

$$\psi(s^\ell r^i) = \sigma^\ell\rho^i$$

and so clearly $\psi$ is surjective. Thus, $\psi$ is an isomorphism. ■

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

*Proof.* Let $G$ be a group and suppose $G/Z(G)$ is cyclic. Let $\langle xZ(G)\rangle = G/Z(G)$ and $g \in G$. Then, $g \in x^a Z(G)$ for some coset $x^a Z(G) \in G/Z(G)$ for $a \in \mathbb{Z}$. So, $g = x^a z_i$ for some $z_i \in Z(G)$. Now, let $g_1, g_2 \in G$ and let

$$g_1 = x^a z_i \text{ and } g_2 = x^b z_j$$

for some $a, b \in \mathbb{Z}$ and $z_i, z_j \in Z(G)$. Then

$$\begin{aligned} g_1 g_2 &= (x^a z_i)(x^b z_j) \\ &= z_i(x^a x^b) z_j \\ &= z_i(x^{a+b}) z_j \\ &= z_i(x^{b+a}) z_j \\ &= z_i x^b x^a z_j \\ &= x^b z_i x^a z_j \\ &= x^b z_i z_j x^a \\ &= x^b z_j z_i x^a \\ &= (x^b z_j)(x^a z_i) = g_2 g_1 \end{aligned}$$

and thus $G$ is abelian. ∎

3.1.38 Let $A$ be an abelian group and let $D$ be the (diagonal) subgroup $\{(a,a) | a \in A\}$ of $A \times A$. Prove that $D$ is a normal subgroup of $A \times A$ and $(A \times A)/D \cong A$.

*Proof.* Let $(a_1, a_2) \in A \times A$ and $(d, d) \in D$. Then,

$$\begin{aligned} (a_1, a_2)(d, d)(a_1, a_2)^{-1} &= (a_1 d, a_2 d)(a_1^{-1}, a_2^{-1}) \\ &= (a_1 d a_1^{-1}, a_2 d a_2^{-1}) \\ &= (a_1 a_1^{-1} d, a_2 a_2^{-1} d) && \text{(since } A \text{ is abelian)} \\ &= (d, d) \in D \end{aligned}$$

and so $D \trianglelefteq (A \times A)$. Now, define a map $\varphi : A \to (A \times A)/D$ by $a \mapsto (a, 1_A)D$. Let $a, a' \in A$. Then,

$$\varphi(aa') = (aa', 1_A)D = (a, 1_A)D(a', 1_A)D = \varphi(a)\varphi(a')$$

and so $\varphi$ is a group homomorphism. Now, suppose $\varphi(a) = \varphi(a')$. Then

$$\begin{aligned} (a, 1_A)D = (a', 1_A)D &\implies (a'^{-1}, 1_A)(a, 1_A) \in D \\ &\implies (a'^{-1} a, 1_A) \in D \\ &\implies a'^{-1} a = 1_A \\ &\implies a = a' \end{aligned}$$

and so $\varphi$ is injective. Now, suppose $(a,a')D \in (A \times A)/D$. Notice that since $(a'^{-1}, a'^{-1}) \in D$ then,

$$(a,a')D = (a,a')(a'^{-1}, a'^{-1})D = (aa'^{-1}, 1)D$$

So,

$$\varphi(aa'^{-1}) = (aa'^{-1}, 1)D = (a,a')D$$

and thus, $\varphi$ is surjective. ∎

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

*Proof.* Claim: If $G$ is a group and $H = \langle S\rangle$ for some subset $S$ of $G$, then $H$ is a normal subgroup of $G$ if and only if for all $g \in G$ and all $s \in S$ we have that $gsg^{-1} \in H$.
Proof of Claim: ($\Rightarrow$) Let $G$ and $H$ be defined as above and suppose $H \trianglelefteq G$. Since $S \subseteq G$, then for any $s \in S$ we have $gsg^{-1} \in H$.
($\Leftarrow$) Now, suppose $gsg^{-1} \in H$ for all $g \in G$ and $s \in S$. Let $S^{-1}$ be the set of all inverses for elements in $S$. Then, for $s_1, s_2, s_3, \dots \in S \cup S^{-1}$ and $g \in G$,

$$H \ni (gs_1^a g^{-1})(gs_2^b g^{-1})(gs_3^c g^{-1}) \cdots = g(s_1^a s_2^b s_3^c \dots)g^{-1} = ghg^{-1}$$

For some $h = (s_1^a s_2^b s_3 c \dots) \in H$. Thus, $gHg^{-1} \subseteq H$ for all $g \in G$ and so $H \trianglelefteq G$.

Let $G$ be a group and $N = \langle x^{-1}y^{-1}xy | x, y \in G\rangle$. By the claim, $N \trianglelefteq G$. Now, consider $G/N$. Let $a, b \in G$. Then,

$$\begin{aligned} a^{-1}b^{-1}ab \in N &\iff (ba)^{-1}ab \in N \\ &\iff abN = baN \\ &\iff aNbN = bNaN \end{aligned}$$

and thus, $G/N$ is abelian. ∎

3.2.12 Let $H \leq G$. Prove that the map $x \mapsto x^{-1}$ sends each left coset of $H$ in $G$ onto a right coset of $H$ and gives a bijection between the set of left cosets and the set of right cosets of $H$ in $G$ (hence the number of left cosets of $H$ in $G$ equals the number of right cosets).

*Proof.* Define $\varphi : G \to G$ by $x \mapsto x^{-1}$. Then, given an element $gh \in gH$, we have

$$\varphi(gh) = (gh)^{-1} = h^{-1}g^{-1} \in Hg^{-1}$$

So, $\varphi$ maps elements in the left coset $gH$ precisely to elements in the right coset $Hg^{-1}$. We claim that $\varphi$ gives a bijection between left and right cosets. To see this, let $gh_1, gh_2 \in gH$ and suppose $\varphi(gh_1) = \varphi(gh_2)$. Then,

$$\varphi(gh_1) = \varphi(gh_2) \implies h_1^{-1}g^{-1} = h_2^{-1}g^{-1} \implies h_1^{-1} = h_2^{-1} \implies h_1 = h_2$$

and so $\varphi$ is injective. Now, suppose $h_1 g \in Hg$. Then, observe that

$$\varphi(g^{-1}h_1) = h_1^{-1}(g^{-1})^{-1} = h_1^{-1}g$$

and so each element in $Hg$ can be attained through the map $\varphi$, and so it is surjective. $\blacksquare$

3.3.4 Let $C$ be a normal subgroup of the group $A$ and let $D$ be a normal subgroup of the group $B$. Prove that $(C \times D) \trianglelefteq (A \times B)$ and $(A \times B)/(C \times D) \cong (A/C) \times (B/D)$.

*Proof.* We first show that $(C \times D) \leq (A \times B)$. First, notice that since $C$ and $D$ are subgroups of $A$ and $B$, respectively, then $1_A \in C$ and $1_B \in D$ and so$(1_A, 1_B) \in (C \times D)$. Now, let $(c', d'), (c, d) \in (C \times D)$. Then,

$$(c', d')(c, d)^{-1} = (c', d')(c^{-1}, d^{-1}) = (c'c^{-1}, d'd^{-1}) \in C \times D$$

because $c'c^{-1} \in C$ and $d'd^{-1} \in D$ by closure in $C$ and $D$. So, $(C \times D) \leq (A \times B)$. We now show that $(C \times D) \trianglelefteq (A \times B)$. Let $(c, d) \in (C \times D)$ and $(a, b) \in (A \times B)$. Then,

$$(c, d)(a, b)(c, d)^{-1} = (c, d)(a, b)(c^{-1}, d^{-1}) = (cac^{-1}, dbd^{-1}) \in (C \times D)$$

because $cac^{-1} \in C$ and $dbd^{-1} \in D$ since $C$ and $D$ are normal in $A$ and $B$, respectively. Thus, $(C \times D) \trianglelefteq (A \times B)$.
Now, consider the map $\varphi : (A \times B) \to (A/C) \times (B/D)$ defined by $(a, b) \mapsto (aC, bD)$. Suppose $(aC, bD) \in (A/C) \times (B/D)$. Then clearly $\varphi$ is surjective since $\varphi((a, b)) = (aC, bD)$. Now, we consider $\ker \varphi$:

$$\begin{aligned} \ker \varphi &= \{(a, b) \in A \times B \mid \varphi((a, b)) = (C, D)\} \\ &= \{(a, b) \in A \times B \mid a \in C \text{ and } b \in D\} = (C \times D) \end{aligned}$$

We conclude by the First Isomorphism Theorem $(A \times B)/(C \times D) \cong (A/C) \times (B/D)$. $\blacksquare$

3.2.9 This exercise outlines a proof for Cauchy's Theorem. Let $G$ be a finite group and let $p$ be a prime dividing $|G|$. Let $\mathcal{S}$ denote the set of $p$-tuples of elements of $G$ the product of whose coordinates is 1:

$$\mathcal{S} = \{(x_1, x_2, \ldots, x_p) \mid x_i \in G \text{ and } x_1 x_2 \cdots x_p = 1\}$$

(a) Show that $\mathcal{S}$ has $|G|^{p-1}$ elements, hence has order divisible by $p$.

*Proof.* For the $p$-tuple $(x_1, x_2, \ldots, x_p)$ to be in $\mathcal{S}$, we must have

$$(x_1 x_2 \cdots x_{p-1}) = x_p^{-1}$$

In other words, we have precisely $|G|$ choices for the first $p-1$ elements of the $p$-tuple, and 1 choice for the $x_p$ term. So, there are $|G|^{p-1}$ elements in $\mathcal{S}$. ∎

Define the relation $\sim$ on $\mathcal{S}$ by letting $\alpha \sim \beta$ if $\beta$ is a cyclic permutation of $\alpha$.

(b) Show that a cyclic permutation of an element of $\mathcal{S}$ is again an element of $\mathcal{S}$.

*Proof.* Let $(x_1, x_2, \ldots, x_p) \in \mathcal{S}$. Consider the cycle permutation of this element $(x_k, \ldots, x_p, x_1, \ldots, x_{k-}$
Notice that

$$\begin{aligned}(x_1 x_2 \ldots x_p) = (x_1 \cdots x_{k-1} x_k \cdots x_p) &= 1 \\ (x_1 \cdots x_{k-1})(x_k \cdots x_p) &= 1 \\ (x_1 \cdots x_{k-1}) &= (x_k \cdots x_p)^{-1} \\ (x_k \cdots x_p)(x_1 \cdots x_{k-1}) &= 1\end{aligned}$$

So,

$$(x_k \cdots x_p x_1 \cdots x_{k-1}) = (x_k \cdots x_p)(x_1 \cdots x_{k-1}) = 1$$

∎

(c) Prove that $\sim$ is an equivalence relation on $\mathcal{S}$.

*Proof.* Let $\alpha, \beta, \gamma$ be cycle permutations of elements of $S$.
*Reflexivity:* Given a cycle permutation $\alpha$, the identity cyclic permutation is a permutation of $\alpha$, i.e., $\alpha \sim \alpha$
*Symmetry:* Let $\alpha \sim \beta$ and suppose $\beta$ is a $k$-th cyclic permutation of $\alpha$, where $0 \leq k \leq p-1$. Then, $\alpha$ is the $(p-k)$-th cyclic permutation of $\beta$. Hence, $\alpha \sim \beta \implies \beta \sim \alpha$
*Transitivity:* Let $\alpha \sim \beta$ and $\beta \sim \gamma$ and suppose that $\beta$ is a $k$-th cyclic permutation of $\alpha$, and $\gamma$ is an $\ell$-th cyclic permutation of $\beta$. Then, $\gamma$ is a $(k+\ell)$-th cyclic permutation of $\alpha$, i.e., $\alpha \sim \beta$ and $\beta \sim \gamma \implies \alpha \sim \gamma$. ∎

(d) Prove that an equivalence class contains a single element if and only if it is of the form $(x, x, \ldots, x)$ with $x^p = 1$.

*Proof.* Suppose that we have an equivalence class of $\mathcal{S}$ with a single element of $\mathcal{S}$, and let $\alpha$ be the cycle associated with this element. Then each $i$-th cyclic permutation of $\alpha$ for all $0 \leq i \leq p-1$ is precisely $\alpha$. This occurs only when $x_1 = x_2 = \cdots = x_p$. So, the element of $\mathcal{S}$ associated with $\alpha$ is of the form $(x, x, \ldots, x)$ with $x^p = 1$. On the other hand, suppose an element of $\mathcal{S}$ is of the form $(x, x \ldots, x)$ with $x^p = 1$. Then, the permutation associated with this element, $\alpha$, has the property that every $i$-th cyclic permutation of $\alpha$ for $0 \leq i \leq p-1$ is precisely $\alpha$, i.e., the equivalence class associated with $\alpha$ contains a single element. ∎

(e) Prove that every equivalence class has order 1 or $p$ (this uses the fact that $p$ is a *prime*). Deduce that $|G|^{p-1} = k + pd$ where $k$ is the number of classes of size 1 and $d$ is the number of classes of size $p$.

*Proof.* Suppose the equivalence class of $(x_1, ..., x_p)$ contains more than 1 element. Then there exist $i < j$ such that $x_i \neq x_j$. We want to show that for all $1 \leq b < c \leq p$,

$$(x_b, ..., x_p, x_1, ..., x_{b-1}) \neq (x_c, ..., x_p, x_1, ..., x_{c-1})$$

Rearranging, this means that for all $2 \leq a \leq p$, we want to show

$$(x_a, ..., x_p, x_1, ..., x_{a-1}) \neq (x_1, ..., x_p) \tag{1}$$

Now, suppose we had equality in (1). Then, let $\sigma = (1, 2, \ldots, p)$ and $\rho = \sigma^a$. Notice that

$$(x_{\rho(1)}, x_{\rho(2)}, \ldots, x_{\rho(p)}) = (x_a, ..., x_p, x_1, ..., x_{a-1})$$

Equality in (1) implies that $x_i = x_{\rho(i)}$ for $1 \leq i \leq p$. Without loss of generality, let $i = 1$. So, by our assumption that each equivalence class has more than one element, $x_1 \neq x_j$ for $1 < j \leq p$. From Exercise 11 of section 1.3, we know that since $(a, p) = 1$, then $\rho$ is a $p$-cycle. Since $\rho$ is a $p$-cycle, then there exists $k \in \mathbb{Z}^+$ so that $\rho^k(1) = j$. So,

$$x_1 = x_{\rho^k(1)} = x_j$$

a contradiction. So the statement in (1) holds. Therefore, every equivalence class has order $p$, or order which divides $p$. Since $p$ is prime, the equivalence classes have order $p$ or 1. So, if $\mathcal{S}$ has $k$ classes of size 1, and $d$ classes of size $p$, then

$$|\mathcal{S}| = |G|^{p-1} = k + dp$$

■

(f) Since $\{(1, 1, \ldots, 1)\}$ is an equivalence class of size 1, conclude from (*e*) that there must be a nonidentity element $x$ in $G$ with $x^p = 1$, i.e., $G$ contains an element of order $p$. [Show $p \mid k$ and so $k > 1$].

*Proof.* Since $|G|^{p-1} = k + dp$, then $k = |G|^{p-1} - dp$. Since $p$ divides $|G|^{p-1}$ and $dp$, then $k$ is divisible by $p$ and so $k > 1$. Thus, there must be a nonidentity element in $G$ so that $x^p = 1$. ■

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.* Since the (left) cosets of $K$ in $G$ partition $G$, then

$$G = \bigsqcup_{\ell \in I_1} g_\ell H \tag{2}$$

where $I_1$ is an indexing set so that each $g_\ell$ is a representative from each coset of $H$ in $G$. In other words, $|I_1| = [G : H]$. Similarly, we have

$$K = \bigsqcup_{j \in I_2} k_j H \quad \text{and} \quad G = \bigsqcup_{i \in I_3} x_i K$$

so that $|I_2| = [K : H]$ and $|I_3| = [G : K]$. Since the (left) cosets of $H$ partition $G$ and the (left) cosets of $K$ partition $H$, then $G$ can be written as

$$G = \bigsqcup_{i \in I_3} \bigsqcup_{j \in I_2} x_i k_j K$$

Written this way, we have $G$ partitioned into $|I_2| \cdot |I_3|$ pieces. We can also write $G$ as in (2), so that

$$\bigsqcup_{\ell \in I_1} g_\ell H = \bigsqcup_{i \in I_3} \bigsqcup_{j \in I_2} x_i k_j K \tag{2}$$

and so $[G : H] = [G : K] \cdot [K : H]$ as desired. ■

3.3.2 Prove all parts of the Lattice Isomorphism Theorem.
Let $G$ be a group, let $N \trianglelefteq G$. Define

$$\mathcal{G} = \{H \mid N \leq H \leq G\} \quad \text{and} \quad \overline{\mathcal{G}} = \{\overline{H} \mid \overline{H} \leq G/N\}$$

Then the map

$$f : \mathcal{G} \to \overline{\mathcal{G}}$$

defined by $H \mapsto H/N$ is a bijection. Moreover, define $\overline{G} := G/N$. If $A, B \in \mathcal{G}$ define $\overline{A} = A/N, \overline{B} = B/N$.

(1) $A \leq B \iff \overline{A} \leq \overline{B}$

*Proof.* ($\Rightarrow$) Since $\overline{A}, \overline{B} \in \overline{\mathcal{G}}$, then they are both groups. We want to show that $\overline{A} \leq \overline{B}$. Let $aN \in \overline{A}$ for $a \in A$. By our assumption $a \in B$, and so $aN = bN \in \overline{B}$ for some $b \in B$. Thus, $aN \in \overline{B}$. ($\Leftarrow$) Since $A, B \in \mathcal{G}$, then $A$ and $B$ are groups. We want to show that $A \leq B$. Let $a \in A$ and consider $aN \in \overline{A}$. By our assumption, $aN \in \overline{B}$ and so $aN = bN$ for some $b \in B$. Then,

$$ab^{-1}N = N \implies ab^{-1} \in N \implies ab^{-1} = n, n \in N \implies a = nb$$

and so $a \in B$ since $n, b \in B$. ■

(2) If $A \leq B$ then $[B : A] = [\overline{B} : \overline{A}]$

*Proof.* Since $A \leq B$, then $\overline{A} \leq \overline{B}$ by (1). So, we consider $B/A$ and $\overline{B}/\overline{A}$ and define a map

$$\varphi : B/A \to \overline{B}/\overline{A} \quad \text{by} \quad bA \mapsto \overline{b}\ \overline{A}$$

where $\overline{b}$ denotes $bN$.

*$\varphi$ is well-defined:* Suppose $b_1A = b_2A$. This implies $b_1 = b_2a$ for some $a \in A$. So,

$$\varphi(b_1A) = \overline{b_1}\ \overline{A} = \overline{b_2a}\ \overline{A} = \overline{b_2}\ \overline{a}\ \overline{A} = \overline{b_2}\ \overline{A} = \varphi(b_2A)$$

*$\varphi$ is injective:* Suppose $\varphi(b_1A) = \varphi(b_2A)$. Then, $\overline{b_1}\ \overline{A} = \overline{b_2}\ \overline{A}$ which implies $\overline{b_2^{-1}}\ \overline{b_1} \in \overline{A}$, and so we have $\overline{b_1^{-1}b_2} = \overline{a}$ for some $a \in A$. Unraveling the notation, we have $(b_2^{-1}b_1)N = aN$, which means $(a^{-1}b_2^{-1}b_1)N = N$ and so $(a^{-1}b_2^{-1}b_1) \in N$. Now, this implies $b_1^{-1}b_1 \in aN$. Since $aN \subset A$, then $b_2^{-1}b_1 \in A$ and so $b_1A = b_2A$.

*$\varphi$ is surjective:* Let $\overline{b}\ \overline{A} \in \overline{B}/\overline{A}$. Then, $\varphi(bA) = \overline{b}\ \overline{A}$ and so $\varphi$ is surjective.

So, $\varphi$ is a bijection and we conclude $[B : A] = [\overline{B} : \overline{A}]$. ■

(3) $\overline{\langle A, B\rangle} = \langle \overline{A}, \overline{B}\rangle$

*Proof.* Let $x \in \overline{\langle A, B\rangle}$. Then, $x = yN$ for some $y \in \langle A, B\rangle$. Then, $y = c_1c_2c_3\dots$ where $c_i \in A$ or $c_i \in B$ for all $i$. So,

$$x = yN = (c_1c_2c_3\dots)N = c_1Nc_2Nc_3N\dots$$

Since each $(c_iN) \in \overline{A}$ or $\overline{B}$ for all $i$, then $x \in \langle \overline{A}, \overline{B}\rangle$.
Conversely, suppose $x \in \langle \overline{A}, \overline{B}\rangle$. Then,

$$x = (d_1N)(d_2N)(d_3N)...$$

for some $(d_iN) \in \overline{A}$ or $(d_iN) \in \overline{B}$ for all $i$, which means $d_i \in A$ or $d_i \in B$ for all $i$. This means $(d_1d_2d_3...) = z$ for some $z \in \langle A, B\rangle$. So,

$$x = (d_1N)(d_2N)(d_3N)... = zN$$

and thus $x \in \overline{\langle A, B\rangle}$. ■

(4) $\overline{A \cap B} = \overline{A} \cap \overline{B}$

*Proof.* Let $x \in \overline{A \cap B}$. Then, $x = yN$ for some $y \in A \cap B$. Since $y \in A \cap B$, then $y \in A$ and $y \in B$, and so $yN \in \overline{A}$ and $yN \in \overline{B}$. Thus, $x \in \overline{A} \cap \overline{B}$.
Conversely, suppose $x \in \overline{A} \cap \overline{B}$. So, $x \in \overline{A}$ and $x \in \overline{B}$, which means $x = aN \in \overline{A}$ and $x = bN \in \overline{B}$ for some $a \in A$ and $b \in B$. So, $aN = bN$, which means $b^{-1}a \in N$, and so $a \in bN$. Since $bN \subseteq B$, then $a \in B$. Thus, $a \in A \cap B$, and so $x = aN \in \overline{A \cap B}$. ■

(5) $A \trianglelefteq G \iff \overline{A} \trianglelefteq \overline{G}$

*Proof.* $(\Rightarrow)$ Let $a \in A$ and $g \in G$. Since $A \trianglelefteq G$, then $a' = gag^{-1} \in A$. Let $aN \in \overline{A}$ and $gN \in \overline{G}$. Then,

$$(gN)(aN)(g^{-1}N) = (gag^{-1})N = a'N \in \overline{A}.$$

and so $\overline{A} \trianglelefteq \overline{G}$.
$(\Leftarrow)$ Let $a \in A$ and $g \in G$. Since $\overline{A} \trianglelefteq \overline{G}$, then $(gN)(aN)(g^{-1}N) = (gag^{-1})N \in \overline{A}$. Suppose $(gag^{-1})N = xN$ for some $x \in A$. This means that $x^{-1}gag^{-1} \in N$. So, $gag^{-1} \in xN$. Since $xN \subseteq A$, then $gag^{-1} \in A$ and thus $A \trianglelefteq G$. ■

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.* We claim that if $G$ is an abelian simple group, then $|G| = p$ for some prime $p$. Then, every non-identity element of $G$ must have order $p$, which means every non-identity element of $G$ generates $G$. Then $G \cong Z_p$ since every cyclic group of order $p$ is isomorphic to $Z_p$.
To prove the claim, first suppose $G$ is an infinite group and let $x \in G$ be a non-identity element. Remember that every subgroup of an abelian group is normal. If $|x|$ is finite, then $\langle x \rangle \lneq G$ and since $G$ is abelian $\langle x \rangle \trianglelefteq G$, which means $G$ is not simple. If $|x|$ is infinite, then $\langle x^2 \rangle \lneq G$, and $\langle x^2 \rangle \trianglelefteq G$, which means $G$ is not simple. So, $G$ cannot be infinite. Now, suppose $|G| = c$ for some composite number $c$. Let $p$ be a prime so that $p|c$. Then, there exists $x \in G$ with $|x| = p$ by Cauchy's Theorem. Then, $\langle x \rangle \lneq G$ and $\langle x \rangle \trianglelefteq G$, which means $G$ is not simple, a contradiction. Thus, $G$ must be of prime order. ■

3.4.6 Prove part (1) of the Jordan–Hölder Theorem by induction on $|G|$.

**Theorem** (Jordan–Hölder)**.** *Let $G$ be a finite group with $G \neq 1$. Then*
*(1) $G$ has a composition series.*

*Proof.* For the base case, we consider the case when $|G| = 2$. So, $G$ is simple and so the composition series is $1 \trianglelefteq G$ and $G/1$ is trivially simple. Now, suppose that whenever $G$ has order less than or equal to $n$, $G$ has a composition series. Let $|G| = n + 1$. If $G$ is simple, then we are done (because its composition series is trivial). If $G$ is not simple, then $G$ has a nontrivial normal subgroup $N$. Notice that $|N| < n$ which means $|G/N| < n$. By our inductive hypothesis, $N$ and $G/N$ have a composition series:

$$1 = H_1 \trianglelefteq H_2 \trianglelefteq \ldots \trianglelefteq H_k = N$$

and

$$1 = S_1/N \trianglelefteq S_2/N \trianglelefteq \ldots \trianglelefteq S_\ell/N = G/N$$

Notice that

$$N/H_k = 1 = S_1/N \implies H_k = S_1.$$

Also notice that since $S_i/N \trianglelefteq S_{i+1}/N$, then $S_i \trianglelefteq S_{i+1}$. So, we construct the following composition series for $G$:

$$1 = H_1 \trianglelefteq H_2 \trianglelefteq \ldots \trianglelefteq H_k = N = S_1 \trianglelefteq S_2 \trianglelefteq \ldots \trianglelefteq S_\ell = G.$$

Thus, every finite group has a composition series. ■

3.5.3 Prove that $S_n$ is generated by $\{(i\ i+1) \mid 1 \leq i \leq n-1\}$. (Consider conjugates, viz. $(23)(12)(23)^{-1}$.)

*Proof.* Let $n \in \mathbb{Z}^+$ and $\sigma \in S_n$. We know that $\sigma$ can be written as the product of transpositions. Given any transposition which is in the product of the transposition decomposition of $\sigma$, say $(a\ b)$, notice that

$$(a\ b) = (b-1\ b)(b\ b+1)\ldots(a+1\ a+2)(a\ a+1)(a+1\ a+2)\ldots(b\ b+1)(b-1\ b)$$

This implies that $\sigma$ can be expressed as the product of elements in the set

$$\{(i\ i+1) \mid 1 \leq i \leq n-1\},$$

and so $S_n$ is generated by this set. ■

3.5.4 Show that $S_n = \langle (12), (12\dots n)\rangle$ for all $n \geq 2$.

*Proof.* Let $n \geq 2$. Since $S_n = \langle \{(i\ i+1) \mid 1 \leq i \leq n-1\}\rangle$ by the previous exercise, we show

$$\langle (12), (12\dots n)\rangle = \langle \{(i\ i+1) \mid 1 \leq i \leq n-1\}\rangle.$$

First notice that $(1,2), (123\dots n) \in S_n$. Thus, $\langle (12)(12\dots n)\rangle \leq S_n$. Now, let

$$\sigma = (123\dots n) \ \text{ and } \ \tau = (12).$$

Let $i \in \{2,3,4,\dots n-1\}$. We claim

$$(i\ i+1) = \sigma^{i-1}\tau\sigma^{1-i}.$$

When we prove this claim, we have $S_n \leq \langle (12)(12\dots n)\rangle$ and so conclude that

$$S_n = \langle (12)(12\dots n)\rangle.$$

To prove the claim, we need to show that $\sigma^{i-1}\tau\sigma^{1-i}$ obeys the same mapping as $(i\ i+1)$. Namely, the mapping that sends $i$ to $i+1$, and $i+1$ to $i$, and fixes all other points in $\{1,2,\dots,n\}$.

Let $j \in \{1,2,\dots,n\}$. We know from a previous assignment that for any $m$-cycle $\rho = (12\dots m)$, we have $\rho^a(j) = j+a$. So, notice

$$\begin{aligned}(\sigma^{i-1}\tau\sigma^{1-i})(j) &= (\sigma^{i-1}\tau)(\sigma^{1-i}(j))\\ &= (\sigma^{i-1}\tau)(j+1-i \mod n)\\ &= (\sigma^{i-1})\tau(j+1-i \mod n)\end{aligned}$$

At this point, we claim that the number $j+1-i \pmod n$ does not equal 1 nor 2, and so $\tau$ fixes it. If $j+1-i = 1 \pmod n$ then $j-i=n$. But, the restriction of values on $i$ and $j$ tell us that $|i-j|<n$. If $j+1-i = 2 \mod n$ then $j-(i+1) = n$. But again, the restriction of values for $i$ and $j$ tell us that $|j-(i+1)|<n$. So,

$$\begin{aligned}(\sigma^{i-1})\tau(j+1-i \mod n) &= \sigma^{i-1}(j+1-i \mod n)\\ &= j+1-i+(i-1) \mod n\\ &= j \mod n\\ &= j\end{aligned}$$

Now, observe that

$$\begin{aligned}(\sigma^{i-1}\tau\sigma^{1-i})(i) &= (\sigma^{i-1}\tau)(\sigma^{1-i}(i))\\ &= (\sigma^{i-1}\tau)(1)\\ &= (\sigma^{i-1})(\tau)(1)\\ &= (\sigma^{i-1})(2)\\ &= i+1\end{aligned}$$

and also that

$$\begin{aligned}(\sigma^{i-1}\tau\sigma^{1-i})(i+1) &= (\sigma^{i-1}\tau)(\sigma^{1-i}(i+1)) \\ &= (\sigma^{i-1}\tau)(2) \\ &= (\sigma^{i-1})(\tau)(2) \\ &= (\sigma^{i-1})(1) \\ &= i\end{aligned}$$

■

4.1.1 Let $G$ act on the set $A$. Prove that if $a, b \in A$ and $b = g \cdot a$ for some $g \in G$, then $G_b = gG_ag^{-1}$ ($G_a$ is the stabilizer of $a$). Deduce that if $G$ acts transitively on $A$ then the kernel of the action is $\bigcap_{g\in G} gG_ag^{-1}$.

*Proof.* Let $a, b \in A$ so that $g \cdot a = b$ for some $g \in G$. We show $G_b = gG_ag^{-1}$.

$$\begin{aligned} h \in G_b &\iff h \cdot b = b \\ &\iff (h \cdot b) = g \cdot a \\ &\iff g^{-1}(h \cdot b) = a \\ &\iff (g^{-1}h) \cdot b = a \\ &\iff g^{-1}h(g \cdot a) = a \\ &\iff (g^{-1}hg) \cdot a = a \\ &\iff (g^{-1}hg) \in G_a \\ &\iff h \in gG_ag^{-1}\end{aligned}$$

The kernel of this group action is $\bigcap_{x\in A} G_x$. If $G$ acts on $A$ transitively, then $G_b = gG_ag^{-1}$ for all $a, b \in A$. So,

$$\bigcap_{g\in G} gG_ag^{-1}$$

■

3.4.9 Prove the following special case of part (2) of the Jordan-Hölder Theorem: assume the finite group $G$ has two composition series

$$1 = N_0 \trianglelefteq N_1 \trianglelefteq \ldots \trianglelefteq N_r = G \quad \text{and} \quad 1 = M_0 \trianglelefteq M_1 \trianglelefteq M_2 = G.$$

Show that $r = 2$ and that the list of composition factors is the same.

*Proof.* We first state and prove the following lemma:

**Lemma.** *If $A$ and $B$ are normal subgroups of $G$, then $AB \trianglelefteq G$.*

*Proof.* Let $A, B$ and $G$ be defined as above. Then, for all $g \in G$,

$$gAg^{-1} = A \quad \text{and} \quad gBg^{-1} = B$$

So,

$$gABg^{-1} = gABg^{-1} = gAg^{-1}gBg^{-1} = AB$$

and so $AB \trianglelefteq G$.

Now, we show that $r \geq 2$. If $r = 0$, then $G$ is the trivial group, which cant have a compositions series. If $r = 1$, then $G$ does not have any nontrivial normal subgroups, but $M_1$ is nontrivial and is normal in $G$. Thus, $r \geq 2$.

Since $M_1$ and $N_{r-1}$ are normal in $G$, then by the Lemma, $M_1N_{r-1} \trianglelefteq G$. Also, notice that $M_1 \cap N_{r-1} \trianglelefteq G$. By the Second Isomorphism Theorem.

$$\begin{tikzcd}[arrows=dash]
 & G \arrow[d] & \\
 & M_1N_{r-1} \arrow[dl] \arrow[dr] & \\
M_1 \arrow[dr] & & N_{r-1} \arrow[dl] \\
 & M_1 \cap N_{r-1} \arrow[d] & \\
 & 1 &
\end{tikzcd}$$

By the composition series, we know that $M_1/1 = M_1$ is simple. Also, since $M_1 \cap N_{r-1} \trianglelefteq G$, then $M_1 \cap N_{r-1} \trianglelefteq M_1$. Thus, either

$$(1)\ M_1 \cap N_{r-1} = M_1 \quad \text{or} \quad (2)\ M_1 \cap N_{r-1} = 1.$$

(1) $M_1 \cap N_{r-1} = M_1$
This implies that $M_1 \leq N_{r-1}$. By the Fourth Isomorphism Theorem, we have

$$N_{r-1}/M_1 \trianglelefteq G/M_1$$

Since $G/M_1$ is simple, then either

$$(a)\ N_{r-1}/M_1 = G/M_1 \ \text{ or } \ (b)\ N_{r-1}/M_1 = M_1$$

(a) $N_{r-1}/M_1 = G/M_1$
This implies $N_{r-1} = G$. But from the composition series, $N_{r-1} \lneq G$, thus, $N_{r-1} \neq G$.

(b) $N_{r-1}/M_1 = M_1$
This implies $N_{r-1} = M_1$. because $M_1$ is simple, we have $N_{r-1} = 1$, which implies $r = 2$.

(2) $M_1 \cap N_{r-1} = 1$
This implies that $M_1 \leq N_{r-1}M_1$. We know that $N_{r-1}M_1 \trianglelefteq G$, and since $M_1 \trianglelefteq G$, then $M_1$ is a strict normal subgroup of $N_{r-1}M_1$. By the composition series, we have

$$N_{r-1}M_1 = G$$

and from the Fourth Isomorphism Theorem,

$$N_{r-1}M_1/M_1 \cong G/M_1$$

Since $G/M_1$ is simple, then either

$$(a)\ N_{r-1}M_1/M_1 = 1 \ \text{ or } \ (b)\ N_{r-1}M_1/M_1 = G/M - 1$$

(a) $N_{r-1}M_1/M_1 = 1$
This implies $N_{r-1} = M_1$, but since $M_1$ is simple, then $N_{r-1} = 1$ or $N_{r-1} = M_1$. If $N_{r-1} = 1$, then $G$ is simple, but that contradicts the fact that $M_1$ is a strict normal subgroup of $G$. So, $N_{r-1} = M_1$ implies $N_{r-2} = 1$, which implies $r = 2$.

(b) $N_{r-1}M_1/M_1 = G/M - 1$
This implies $G = N_{r-1}M_1$, which means $G/M_1 \cong N_{r-1}$. So, $N_{r-1} = 1$, which means $r = 2$.

By part 2(a), $N_{r-1} = M_1$, and since $r = 2$, then $N_1 = M_1$, which means the composition series is the same. ☕

4.1.7 Let $G$ be a transitive permutation group on the finite set $A$. A *block* is a nonempty subset $B$ of $A$ such that for all $\sigma \in G$ either $\sigma(B) = B$ or $\sigma(B) \cap B = \emptyset$ (here $\sigma(B) = \{\sigma(b) \mid b \in B\}$).

(a) Prove that if $B$ is a block containing the element $a$ of $A$, then the set $G_B$ defined by $G_B = \{\sigma \in G \mid \sigma(B) = B\}$ is a subgroup of $G$ containing $G_a$.

*Proof.* Let $a \in A$ and $\sigma \in G_a$. Suppose $a \in B$. Then

$$\sigma(a) = a \in B \implies \sigma(B) = B \implies \sigma \in G_B \implies G_a \subseteq G_B$$

Notice that $G_B \neq \emptyset$ since $\sigma_{id}(B) = B$ and so $\sigma_{id} \in G_B$. Let $\sigma, \tau \in G_B$. Then

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

and so, $\sigma \circ \tau^{-1} \in G_B$, thus $G_B \leq G$.

(b) Show that if $B$ is a block and $\sigma_1(B), \sigma_2(B), \ldots, \sigma_n(B)$ are all the distinct images of $B$ under the elements of $G$, then these form a partition of $A$.

*Proof.* We show that for $\ell, k \in \{1, 2, \ldots n\}$, either $\sigma_\ell(B) \cap \sigma_k(B) = \emptyset$ or $\sigma_\ell(B) = \sigma_k(B)$. Suppose $\sigma_\ell(B) \cap \sigma_k(B) \neq \emptyset$ and let $x \in \sigma_\ell(B) \cap \sigma_k(B)$. Then, there exists $b_1, b_2 \in B$ so that $\sigma_\ell(b_1) = x = \sigma_k(b_2)$. Then,

$$\begin{aligned} \sigma_\ell(b_1) = \sigma_k(b_2) &\implies b_1 = \sigma_\ell^{-1}\sigma_k(b_1) \\ &\implies \sigma_\ell^{-1} \circ \sigma_k \in B \\ &\implies (\sigma_\ell^{-1} \circ \sigma_k)(B) = B \\ &\implies \sigma_k(B) = \sigma_\ell(B) \end{aligned}$$

Thus, $\sigma_\ell$ and $\sigma_k$ are either the same or disjoint. Now, it is clear that

$$\bigcup_{i=1}^{n} \sigma_i(B) \subset A.$$

Let $a \in A$ and $b \in B$. Then, since $G$ acts transitively on $A$, there exists $\sigma_k \in G$ so that $\sigma(b) = a$. So, $a \in \bigcup_{i=1}^{n} \sigma_i(B)$ and therefore,

$$\bigcup_{i=1}^{n} \sigma_i(B) = A.$$

4.1.9 ***(Worked with Meghan Malachi and Anup Poudel)***
Assume $G$ acts transitively on the finite set $A$ and let $H$ be a normal subgroups of $G$. Let $\mathcal{O}_1, \mathcal{O}_2, \ldots, \mathcal{O}_r$ be distinct orbits of $H$ on $A$.

(a) i. Prove that $G$ permutes the sets $\mathcal{O}_1, \mathcal{O}_2, \ldots, \mathcal{O}_r$ in the sense that for each $g \in G$ and each $i \in \{1, \ldots, r\}$ there is a $j$ such that $g\mathcal{O}_i = O_j$, where $g\mathcal{O} = \{g \cdot a \mid a \in \mathcal{O}\}$ (i.e., $\mathcal{O}_1, \ldots, \mathcal{O}_r$ are blocks).

*Proof.* Recall that $H \trianglelefteq G$. If $g \in G$ and $a \in A$, then we can call $H \cdot a$ an orbit of $H$ on $A$. So,

$$\begin{aligned} g \cdot a_1 &= a_2 \text{ for some } a_2 \in A \\ g \cdot (H \cdot a_1) &= gH \cdot a_1 \\ &= Hg \cdot a_1 \\ &= H(g \cdot a_1) = H \cdot a_2 \end{aligned}$$

And so, we have $g\cdot(H\cdot a_1) = H\cdot a_2$. Which means $G$ permutes $\mathcal{O}_1, \mathcal{O}_2, \ldots, \mathcal{O}_r$.

ii. Prove $G$ is transitive on $\{\mathcal{O}_1, \ldots, \mathcal{O}_r\}$.

*Proof.* We want to show that for all $H\cdot a, H\cdot a_2 \in \{\mathcal{O}_1, \mathcal{O}_2, \ldots, \mathcal{O}_r\}$, there exists a $g \in G$ so that

$$g \cdot (H \cdot a_1) = H \cdot a_2$$

Let $a_1, a_2 \in A$, then since $G$ acts transitively on $A$, there exists $g \in G$ such that $g \cdot a_1 = a_2$. So,

$$\begin{aligned} H(g \cdot a_1) &= H \cdot a_2 \\ gH \cdot a_1 &= H \cdot a_2 \\ gH \cdot a_1 &= H \cdot a_2 \\ g(H \cdot a_1) &= H \cdot a_2 \end{aligned}$$

And so, there exists a $g$ so that

$$g \cdot (H \cdot a_1) = H \cdot a_2$$

iii. Deduce that all orbits of $H$ on $A$ have the same cardinality.

*Proof.* Let $a_1, a_2 \in A$ and $g \cdot a_1 = a_2$ for all $g \in G$. Since $H \trianglelefteq G$, then $gH = Hg$ for all $g \in G$, which means $gHg^{-1} = h_0$ for some $h, h_0 \in H$ and for all $g \in G$. This means that $gh = h_0 g$. We define a bijection between the orbits: Define the map

$$\varphi : H \cdot a_1 \to H \cdot a_2$$

by $h \cdot a_1 \mapsto h_0 \cdot a_2$. Because $G$ acts transitively on $A$, then for all $a_1, a_2 \in A$ there exists a $g \in G$ such that $g \cdot a_1 = a_2$. This implies $g(H \cdot a_1) = a_2$ and so $G$ acts transitively on each $\mathcal{O}_i$. Now, because $g \cdot (ha) = g \cdot (h_0 a_1)$, then $ha_1 = h_0 a_2$. So, each $\mathcal{O}_i$ has the same cardinality.

(b) Prove that if $a \in \mathcal{O}_1$ then $|\mathcal{O}_1| = [H : H \cap G_a]$ and prove that $r = [G : HG_a]$.

*Proof.* We know that $|G \cdot a| = [G : G_a]$, so $H \cdot a| = [H : H_a]$. Therefore, $H_a = H \cap G_a$ since $H \leq G$ ( and so $H \subset G$). Then,

$$|H \cdot a| = [H : H_a] = [H : H \cap G_a]$$

Since $G$ acts transitively, the number of distinct orbits of $H$ on $A$ is

$$r = |\{H \cdot a \mid a \in A\}| = [G : G_{H\cdot a}]$$

We want to show $[G : G_{H\cdot a}] = [G : HG_a]$, i.e., $G_{H\cdot a} = HG_a$.
If $g \in G_{H\cdot a}$, then $Hg \cdot a = (gH) \cdot a = g \cdot (H \cdot a) = H$. So, $g \cdot a = h \cdot a$ for $h \in H$. Then, $h^{-1}(g \cdot a) = a \implies (h^{-1}g) \cdot a = a$. So, $h^{-1}g \in G_a$, which means $g \in hG_a$

and so $g \in HG_a$.
If $g \in HG_a$, then $g = h_1 x$ for $h_1 \in H$ and $x \in G_a$. Then,

$$g \cdot (H \cdot a) = (gH) \cdot a = hxH \cdot a = hHx \cdot a = Hhx \cdot a = H \cdot a$$

which means $g \in G_{H \cdot a}$. ☕

4.1.10 ***(Worked with Meghan Malachi and Anup Poudel)***
Let $H$ and $K$ be subgroups of the group $G$. For each $x \in G$ define the $HK$ *double coset* of $x$ in $G$ to be the set

$$HxK = \{hxk \mid h \in H, k \in K\}$$

(a) Prove that $HxK$ is the union of the left cosets $x_1K, \dots, x_nK$ where $\{x_1K, \dots, x_nK\}$ is the orbit containing $xK$of $H$ acting by left multiplication on the set of left cosets of $K$.

*Proof.* Let $hxk \in HxK$ for $x \in G$. Notice $hxK = h(xK) \in HxK$ and $hxk \in (hx)K$. So,

$$hxk \in \bigcup_{x_iK \in H \cdot xK} x_iK.$$

Now, let $y \in \bigcup_{x_iK \in H \cdot xK} x_iK$. Then, $y \in x_iK$ for some $x_iK \in H \cdot xK$. This implies $x_iK = h \cdot xK = hxK$ for some $h \in H$, so $y \in hxK$. Then, $y = hxk_0$ for $k_0 \in K$. Thus, $y \in HxK$. So,

$$HxK = \bigcup_{x_iK \in H \cdot xK} x_iK$$

☕

(b) Prove that $HxK$ is a union of right cosets of $H$.

*Proof.* We want to show

$$HxK = \bigcup_{Hb \in H \cdot xK} Hb.$$

Let $hxk \in HxK$. Notice that $Hxk = Hx \cdot k$ and $Hx \cdot k \in Hx \cdot K$. This implies $hxk \in HxK$, and so

$$hxk \in \bigcup_{Hb \in H \cdot xK} Hb$$

Let $g \in \bigcup_{Hb \in H \cdot xK} Hb$. Then $g \in Hb$ for some $Hb \in Hx \cdot K$ and $Hb = Hx \cdot k$ for some $k \in K$. Then, $Hb = Hxk$, which means $Hb \in HxK$. Thus, $g \in HxK$. ☕

(c) Show that $HxK$ and $HyK$ are either the same set or are disjoint for all $x, y \in G$. Show that the set of $HK$ double cosets partitions $G$.

*Proof.* We claim that $G = \bigcup HxK$. If $x \in G$ then $x = 1x1 \in HxK$. If $x \in HxK$ then clearly $x \in G$. Now, we want to show $HxK \cap HyK \neq \emptyset$ implies $HxK = HyK$. Suppose $h_1xk_1 = h_2yk_2$ where $h_1xk_1 \in HxK$ and $h_2yk_2 \in HyK$. Then,

$$xk_1 = h_1^{-1}h_2yk_2 \implies x = h_1^{-1}h_2yk_2k_1^{-1} \implies x \in HyK \implies HxK \subseteq HyK$$

Similarly,

$$h_2y = h_1xk_1k_2^{-1} \implies y = h_2^{-1}h_1xk_1k_2^{-1} \implies y \in HxK \implies HyK \subseteq HxK$$

Thus, $HxK = HyK$.

(d) Prove that $|HxK| = |K| \cdot [H : H \cap xKx^{-1}]$.

*Proof.* We know that

$$HxK = \bigsqcup_{yK \in H \cdot xK} yK.$$

Since each $yK$ is disjoint, $|yK| = |K|$. So,

$$|HxK| = |K| \cdot |H \cdot xK| = |K| \cdot [H : H_{xK}]$$

So, we claim $H_{xK} = H \cap xKx^{-1}$, and the conclusion follows. To prove the claim, observe that

$$\begin{aligned} h \in H_{xK} &\iff h \cdot (xk) = xk \\ &\iff hxk = xk \\ &\iff x^{-1}hxk = k \\ &\iff x^{-1}hx \in K \\ &\iff h \in xKx^{-1} \\ &\iff h \in H \cap xKx^{-1} \end{aligned}$$

(e) Prove that $|HxK| = |H| \cdot [K : K \cap x^{-1}Hx]$.

*Proof.* We know that

$$HxK = \bigsqcup_{Hy \in H \cdot xk} Hy.$$

Since each $Hy$ is disjoint, $|Hy| = |K|$. So,

$$|HxK| = |H| \cdot |Hx \cdot K| = |H| \cdot [K : K_{Hx}]$$

As before, we claim $K_{Hx} = K \cap x^{-1}Hx$. Then,

$$k \in K_{Hx} \implies Hx \cdot k = Hxk = Hx$$

We Have that $xKx^{-1}\imath H$. So,

$$k \in x^{-1}Hx \implies k \in K \text{ and } k \in x^{-1}Hx$$

Now, if $k \in K \cap x^{-1}Hx$, then $xkx^{-1} = h$ for $h \in H$, and so

$$xhx^{-1} \in H \implies Hx \cdot k = HxK = Hx \implies k \in K_{Hx}$$

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.* Let $\mathcal{C} = \{gH \mid g \in G\}$ be the set of left cosets of $H$ in $G$. We let $G$ act on $C$ by left multiplication. Let $\pi_H$ be the associated permutation representation afforded by this action, i.e.,

$$\pi_H : G \to S_{\mathcal{C}}.$$

Then, by Theorem 3 (Chapter 4, Dummit and Foote), we know $K = \ker \pi_H \trianglelefteq G$ and $K \leq H$. Now, since $[G : H] = n$, then $S_{\mathcal{C}} \cong S_n$. Since $|S_n| = n!$, then $|S_{\mathcal{C}}| = n!$ as well. So, $|\pi_H(G)| \leq n!$. By the First Isomorphism Theorem, $G/K \cong \pi_H(G)$. Thus,

$$n! \geq |\pi_H(G)| = |G/K| = [G : K]$$

☕

3.2.9 (Cauchy's Theorem Revisited)
Look again at 3.2.9. Let $S = \{(x_1, \dots, x_p) \mid x_i \in G \text{ and } x_1 \cdots x_p = 1\}$. Let $\sigma$ be the $p$-cycle $(1, 2, \dots, p)$ in $S_p$, and let $H = \langle \sigma \rangle$. For all $\tau \in H$ and all $(x_i, \dots, x_p) \in S$, define

$$\tau.(x_1, \dots, x_p) = (x_{\tau(1)}, \dots, x_{\tau(p)})$$

(i) Show that this defines a left action of $H$ on $S$.

*Proof.* Let $(x_1, \dots, x_p) \in S$ and $\sigma_{id}$ be the identity permutation of $H$. Then,

$$\sigma_{id}.(x_1, \dots, x_p) = (x_{\sigma_{id}(1)}, \dots, x_{\sigma_{id}(p)}) = (x_1, \dots, x_p).$$

Now, let $\sigma_\ell, \sigma^k \in H, 1 \leq \ell, k \leq p$ and $(x_1, \dots, x_p) \in S$. By a previous exercise, we know that for any $j \in \{1, 2 \dots, n\}$ and any power of a $p$-cycle, $\sigma^\ell$, we have $\sigma^\ell(j) = j + \ell$. So,

$$\begin{aligned}
\sigma^\ell.(\sigma^k.(x_1, \dots, x_p) &= \sigma^\ell.(x_{\sigma^k(1)}, \dots, x_{\sigma^k(p)}) \\
&= \sigma^\ell.(x_{1+k}, \dots, x_{p+k}) \\
&= (x_{\sigma^\ell(1+k)}, \dots, x_{\sigma^\ell(p+k)}) \\
&= (x_{1+k+\ell}, \dots, x_{p+k+\ell}) \\
&= (x_{\sigma^{k+\ell}(1)}, \dots, x_{\sigma^{k+\ell}(p)}) \\
&= \sigma^{k+\ell}.(x_1, \dots, x_p) \\
&= (\sigma^k \sigma^\ell).(x_1, \dots, x_p)
\end{aligned}$$

Thus, the given mapping defines a left action of $H$ on $S$. ☕

(ii) Show that the $H$-orbits of this action are precisely the equivalence classes of the equivalence relation defined exercise 3.2.9.

*Proof.* Let $\alpha = (x_1, \dots, x_p) \in S$. Then,

$$\begin{aligned}
\mathcal{O}_\alpha &= \{\tau.\alpha \mid \tau \in H\} \\
&= \{\beta \mid \beta = \tau.\alpha, \tau \in H\} \\
&= \{\beta = (x_{\tau(1)}, \dots, x_{\tau(p)}) \mid \tau \in H\} \\
&= \{\beta = (x_{\tau(1)}, \dots, x_{\tau(p)}) \mid \tau \text{ is a power of the } p\text{-cycle } \sigma\} \\
&= \{\beta \text{ is cyclic permutation of } \alpha\}
\end{aligned}$$

And so $\mathcal{O}_\alpha$ is the set of elements which are cyclic permutations of $\alpha$, i.e., $\mathcal{O}_\alpha$ is an equivalence class of the relation defined in 3.2.9. ☕

(iii) Use the orbit lemma to prove that every $H$-orbit has order 1 or $p$ (thus giving a shorter proof of part (e) of 3.2.9).

*Proof.* Let $\alpha \in S$ and note that

$$[H : H_\alpha] = \frac{|H|}{H_a} = \frac{p}{|H_a|}.$$

Since $p$ is prime, $|H_a| = 1$ or $|H_a| = p$. Thus,

$$[H : H_\alpha] = \frac{p}{1} = p \text{ or } [H : H_\alpha] = \frac{p}{p} = 1.$$

By the Orbit Lemma, $|\mathcal{O}_\alpha| = [H : H_\alpha]$, which means $|\mathcal{O}_\alpha| = 1$ or $|\mathcal{O}_\alpha| = p$. ☕

4.3.29 Let $p$ be a prime and let $G$ be a group of order $p^\alpha$. Prove that $G$ has a subgroup of order $p^\beta$ for every $\beta$ with $0 \leq \beta \leq \alpha$.

*Proof.* We proceed by induction on $\alpha$. For the base case, suppose $\alpha = 1$. Then $|G| = p$ and $G$ has subgroups $\{1_G\}$ and $G$. Clearly, $|\{1_G\}| = p^0$ and $|G| = p^1$, and so $G$ has a subgroup of order $p^\beta$ for each $0 \leq \beta \leq \alpha = 1$. For the inductive hypothesis, suppose that for each $1 \leq \alpha \leq n-1$, the group $G$ of order $p^\alpha$ has a subgroup of order $p^\beta$ for each $0 \leq \beta \leq \alpha$.
Let $G$ be a group of order $p^n$. By Cauchy's Theorem, there exists $g \in G$ with $|g| = p$. Let $N = \langle p \rangle$. So, $|G/N| = p^{n-1}$, and by the induction hypothesis, $G/N$ has subgroups of order $p^\gamma$ for each $0 \leq \gamma \leq n-1$. By the 4th Isomorphism Theorem, the subgroups of $G/N$ are of the form $H/N$ where $H \leq G$. So for each $0 \leq \gamma \leq n-1$, there is a subgroup $H \leq G$ so that

$$|H/N| = \frac{|H|}{|N|} = \frac{|H|}{p} = p^\gamma \implies |H| = p^{\gamma+1}$$

So, $G$ has subgroups of order $p^{\gamma+1}$ for each $\gamma \in \{0, 1, \ldots, n-1\}$, i.e., $G$ has subgroups of order $p^\beta$ for each $\beta \in \{1, \ldots, n\}$,. Note that clearly the trivial subgroup of $G$ is of order $p^0$ so $G$ contains a subgroup of order $p^\beta$ for each $0 \leq \beta \leq n$.

☕

4.3.31 Using the usual generators and relations for the dihedral group $D_{2n}$, show that for $n = 2k$ an even integer, the conjugacy classes in $D_{2n}$ are the following:

$$\{1\}, \{r^k\}, \{r^{\pm 1}\}, \{r^{\pm 2}\}, \ldots, \{r^{\pm(k-1)}\}, \{sr^{2b} \mid b = 1, \ldots, k\} \text{ and } \{sr^{2b-1} \mid b = 1, \ldots, k\}$$

Give the class equation for $D_{2n}$.

*Proof.* We know from a previous exercise that $Z(D_{2n}) = \{1, r^k\}$. Thus, $\{1\}$ and $\{r^k\}$ are conjugacy classes of $D_{2n}$. Let $1 \leq i, \ell \leq k-1$ and $j \in \{1, 2\}$. Then, any non-identity element of $D_{2n}$ can be written as $s^j r^i$. Now, we find the conjugacy class of $r^\ell$:

$$\begin{aligned}(s^j r^i)(r^\ell)(s^j r^i)^{-1} &= (s^j r^i)(r^\ell)(r^{-i} s^{-j}) \\ &= s^j r^{i+\ell-i} s^j && \text{(Note that } s^j = s^{-j}) \\ &= s^j r^\ell s^j.\end{aligned}$$

Recall that $sr^\ell s = r^{-\ell}$. When $j = 1$, we have

$$s^j r^\ell s^j = sr^\ell s = r^{-\ell},$$

and when $j = 2$,

$$s^j r^\ell s^j = 1r^\ell 1 = r^\ell.$$

Thus, $\{r^{\pm\ell}\}$ are conjugacy classes for each $\ell \in \{1, 2, \dots, k-1\}$. We now find the conjugacy class of $s$:

$$(s^j r^i)(s)(s^j r^i)^{-1} = (s^j r^i)(s)(r^{-i} s^j).$$

Recall that $r^{-i}s = sr^i$. When $j = 1$

$$(s^j r^i)(s)(r^{-i} s^j) = sr^i sr^{-i} s = sr^i s(sr^i) = sr^i s^2 r^i = sr^{2i},$$

and when $j = 2$,

$$(s^j r^i)(s)(r^{-i} s^j) = r^i sr^{-i} = (sr^{-i})r^{-i} = sr^{-2i} = sr^{-2(n-i)}.$$

Thus, the conjugacy class of $s$ is $\{sr^{2i} \mid 1 \leq i \leq k\}$. Finally, we find the conjugacy class of $sr$:

$$(s^j r^i)(sr)(s^j r^i)^{-1} = (s^j r^i)(sr)(r^{-i} s^j)$$

Then, when $j = 1$,

$$\begin{aligned}
(s^j r^i)(sr)(r^{-i} s^j) &= (sr^i)(sr)(r^{-i} s) \\
&= sr^i (r^{-1} s) r^{-i} s \\
&= sr^{i-1}(sr^{-i}) s \\
&= sr^{i-1}(r^i s) s \\
&= sr^{2i-1}.
\end{aligned}$$

and when $j = 2$, we have

$$\begin{aligned}
(s^j r^i)(sr)(r^{-i} s^j) &= r^i (sr) r^{-i} \\
&= r^i (r^{-1} s) r^{-i} \\
&= (r^{i-1} s) r^{-i} \\
&= (sr^{-i+1}) r^{-i} \\
&= sr^{-2i+1} \\
&= sr^{-2(n-i)+1}.
\end{aligned}$$

So, the conjugacy class of $sr$ is $\{sr^{2i-1} \mid 1 \leq i \leq k-1\}$. So, the class equation of $D_{2n}$ is as follows:

$$|D_{2n}| = 1 + 1 + \underbrace{2 + 2 + \cdots + 2}_{(k-1)-\text{ summands}} + k + k$$

☕

4.4.8 Let $G$ be a group with subgroups $H$ and $K$ with $H \leq K$.

(a) Prove that if $H$ is characteristic in $K$ and $K$ is normal in $G$, then $H$ is normal in $G$.

*Proof.* Let $\sigma_g \in \text{Aut}(G)$ be conjugation by $g$ for each $g \in G$. Since $K$ is normal in $G$, then for each $\sigma_g \in \text{Aut}(G)$, we have

$$\sigma_g(K) = gKg^{-1} = K.$$

Therefore, $\sigma_g \in \text{Aut}(K)$ for each $g \in G$. Since $H$ is characteristic in $K$, then for each $\sigma_g \in \text{Aut}(K)$, we have

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

Thus, $H$ is normal in $G$. ☕

(b) Prove that if $H$ is characteristic in $K$ and $K$ is characteristic in $G$ then $H$ is characteristic in $G$. Use this to prove that the Klein 4-group $V_4$ is characteristic in $S_4$.

*Proof.* Let $\sigma \in \text{Aut}(G)$. Then, as $K$ is characteristic in $G$,

$$\sigma(K) = K.$$

Thus, $\sigma \in \text{Aut}(K)$. Since $H$ is characteristic in $K$, then

$$\sigma(H) = H$$

and so $H$ is characteristic in $G$.

---

To show $V_4$ is characteristic in $S_4$, we first prove the following: If $H$ is a unique subgroup of a given order in a group $G$, then $H$ is characteristic in $G$.
To see this, let $\sigma \in \text{Aut}(G)$. Then, since $\sigma$ is bijective, then the order of the image of $H$ under $\sigma$, $\sigma(H)$, is the order of $|H|$. Since $\sigma$ is a homomorphism, $\sigma(H)$ is a subgroup of $G$. Since $H$ is the only subgroup of order $|H|$, then $\sigma(H) = H$, and thus $H$ is characteristic in $G$.
Now, since $V_4$ is the unique subgroup of $A_4$ of order 4, then $V_4$ is characteristic in $A_4$. Also, since $A_4$ is the unique subgroup of order 12 in $S_4$, then $A_4$ is characteristic in $S_4$. So, by the result above, we know $V_4$ is characteristic in $S_4$. ☕

(c) Give an example to show that if $H$ is normal in $K$ and $K$ is characteristic in $G$ then $H$ need not be normal in $G$.
**Solution:**
We know that since $V_4 = \{(), (12)(34), (13)(24), (14)(23)\}$ is abelian, then the subgroup $H = \{(), (14)(23)\}$ of $V_4$ is normal. So, we know that

$$H \trianglelefteq V_4 \text{ char } A_4.$$

But

$$(123)(14)(23)(132) = (13)(24) \notin H,$$

and so $H \ntrianglelefteq A_4$.

4.3.17 Let $A$ be a nonempty set and let $X$ be any subset of $S_A$. Let

$$F(X) = \{a \in A \mid \sigma(A) = a \text{ for all } \sigma \in X\} \quad \text{— the } \textit{fixed set} \text{ of } X.$$

Let $M(X) = A - F(X)$ be the elements which are *moved* by some element of $X$. Let $D = \{\sigma \in S_A \mid \ |M(\sigma)| < \infty\}$. Prove that $D$ is a normal subgroup of $S_A$.

*Proof.* We first show that $D$ is a subgroup of $S_A$. Notice that $\sigma_{id} \in D$ since

$$|M(\sigma_{id})| = |A - F(\sigma_{id})| = |A - A| = |\emptyset| = 0 < \infty.$$

Let $\sigma, \tau \in D$. Notice that $M(\tau) = M(\tau^{-1})$. We show that $\sigma \circ \tau^{-1} \in D$. Suppose $|M(\sigma)| = s < \infty$ and $|M(\tau^{-1})| = |M(\tau)| = t < \infty$. Notice that

$$M(\sigma \circ \tau) \subseteq M(\sigma) \cup M(\tau)$$

and so

$$|M(\sigma \circ \tau)| \leq |M(\sigma)| + |M(\tau)| = s + t < \infty.$$

We now show $D \trianglelefteq S_A$. Let $\sigma \in S_A$, and $\tau \in D$. We claim that $\sigma\tau\sigma^{-1} \in D$, i.e., $|M(\sigma\tau\sigma^{-1})| < \infty$. If $|A| < \infty$, then we are done. Suppose $|A| = \infty$. We proceed by contradiction. Suppose $|M(\sigma\tau\sigma^{-1})| = \infty$. Then, there exists an infinite subset $B \subseteq A$ so that for all $b \in B$ we have

$$(\sigma\tau\sigma^{-1})(b) \neq b.$$

This implies that for all $b \in B$,

$$\tau(\sigma^{-1}(b)) \neq \sigma^{-1}(b).$$

In other words $|M(\tau)| = \infty$, a contradiction, as $\tau \in D$. Thus, $|M(\sigma\tau\sigma)| < \infty$, and so $D \trianglelefteq S_A$. ☕

4.3.19 Assume $H \trianglelefteq G$, and $\mathcal{K}$ is a conjugacy class of $G$ contained in $H$ and $x \in \mathcal{K}$. Prove that $\mathcal{K}$ is a union of $k$ conjugacy classes of equal size in $H$, where $k = [G : HC_G(x)]$. Deduce that a conjugacy class in $S_n$ which consists of even permutations is either a single conjugacy class under the action of $A_n$ or is a union of two classes of the same size in $A_n$. [Let $A = C_G(x)$ and $B = H$ so $A \cap B = C_H(x)$. Draw the lattice diagram associated to the Second Isomorphism Theorem and interpret the appropriate indices. See also Exercise 9, Section 1.]

*Proof.* Let $H$ act on $\mathcal{K}$ by conjugation. Then, $\mathcal{K}$ is the union of $H$-orbits;

$$\mathcal{K} = \bigcup_{x \in \mathcal{K}} H.x$$

We claim that the $H$-orbit has of equal size. Let $H.a$ and $H.b$ be distinct $H$-orbits (conjugacy classes of $\mathcal{K}$ in $H$). Then, as $a$ and $b$ are in the same conjugacy class $\mathcal{K}$, there exists a $g \in G$ so that $gag^{-1} = b$. We claim $|H.a| = |H.b|$. Notice

$$\begin{aligned}
g(H.a)g^{-1} &= \{g(hah^{-1})g^{-1} \mid h \in H\} \\
&= \{(gh)a(gh)^{-1} \mid h \in H\} \\
&= \{xax^{-1} \mid x \in gH\} \\
&= \{yay^{-1} \mid y \in Hg\} && (gH = Hg \text{ since } H \trianglelefteq G) \\
&= \{(hg)a(hg)^{-1} \mid h \in H\} \\
&= \{h(gag^{-1})h^{-1} \mid h \in H\} \\
&= \{hbh^{-1} \mid h \in H\} \\
&= H.b
\end{aligned}$$

Thus, $H.a$ and $H.b$ are conjugate and so $|H.a| = |H.b|$. Suppose $x \in \mathcal{K}$. Since all conjugacy classes in $\mathcal{K}$ have equal size,

$$|\mathcal{K}| = k \cdot |H.x| \text{ for some } k \in \mathbb{Z}^+.$$

We claim that $k = [G : HC_G(x)]$. Since $K = G.x$ is a conjugacy class of $G$, then $G_x = C_G(x)$. Likewise, as $H.x$ is a conjugacy call of $H$, then $H_x = C_H(x)$. Then by the Orbit-Stabilizer Theorem,

$$|G.x| = [G : G_x] = [G : C_G(x)] \text{ and } |H.x| = [H : H_x] = [H : C_H(x)].$$

So,

$$|\mathcal{K}| = k \cdot |H.x| \implies \frac{|\mathcal{K}|}{|H.x|} = \frac{|G.x|}{|H.x|} = \frac{[G : C_G(x)]}{[H : C_H(x)]}.$$

Since $H \trianglelefteq G$ and $C_G(x) \leq G$, then $HC_G(x) \leq G$ by Corollary 15 of Section 3.2 (D&F). So,

$$C_G(x) \leq HC_G(x) \leq G.$$

By Exercise 11 of Section 3.2, we have

$$[G : C_G(x)] = [G : HC_G(x)] \cdot [HC_G(x) : C_G(x)].$$

So,

$$\frac{[G : C_G(x)]}{[H : C_H(x)]} = \frac{[G : HC_G(x)] \cdot [HC_G(x) : C_G(x)]}{[H : C_H(x)]}.$$

Note that $H \cap C_G(x) = C_H(x)$. Since $H \trianglelefteq G$ and $C_G(x) \leq G$, then by the Second Isomorphism Theorem,

$$HC_G(x)/H \cong C_G(x)/H \cap C_G(x) = C_G(x)/C_H(x).$$

This means

$$[HC_G(x) : H] = [C_G(x) : C_H(x)], \quad \text{which implies } \frac{|HC_G(x)|}{|H|} = \frac{|C_G(x)|}{C_H(x)}.$$

Rearranging, we get

$$\frac{|HC_G(x)|}{|C_G(x)|} = \frac{|H|}{C_H(x)} \text{ which implies } [HC_G(x) : C_G(x)] = [H : C_H(x)].$$

So,

$$\frac{[G : HC_G(x)] \cdot [HC_G(x) : C_G(x)]}{[H : C_H(x)]} = \frac{[G : HC_G(x)][H : C_H(x)]}{[H : C_H(x)]}$$

$$= [G : HC_G(x)].$$

Therefore, $k = [G : HC_G(x)]$.

Now, consider the normal subgroup $A_n$ of $S_n$. Suppose $K$ is a conjugacy class of $S_n$ and $K \subseteq A_n$. If $\sigma \in K$, then by what was just proved, $K$ is a union of distinct conjugacy classes of $A_n$ of equal size. In particular, $K$ is made up of $k = [S_n : A_n C_{S_n}(\sigma)]$ conjugacy classes of $A_n$ of equal size. Now, since

$$A_n \leq A_n C_{S_n}(\sigma) \leq S_n$$

and $A_n$ is a maximal subgroup of $S_n$, then either $A_n C_{S_n}(\sigma) = A_n$ or $A_n C_{S_n}(\sigma) = S_n$. In the former case, $K$ is a single conjugacy class under the action of $A_n$. In the latter case, $K$ is the union of two conjugacy classes of the same size in $A_n$. ☕

4.3.23 Recall that a proper subgroup $M$ of $G$ is called *maximal* if whenever $M \leq H \leq G$, either $H = M$ or $H = G$. Prove that if $M$ is a maximal subgroup of $G$ then either $N_G(M) = M$ or $N_G(M) = G$. Deduce that if $M$ is a maximal subgroup of $G$ that is not normal in $G$ then the number of nonidentity elements of $G$ that are contained in conjugates of $M$ is at most $(|M| - 1)[G : M]$.

*Proof.* *From Online Solution Manual*
Since $M$ is a subgroup, we have $M \leq N_G(M) \leq G$. Then, $N_G(M) = M$ or $N_G(M) = G$. If $M$ is not normal, then $N_G(M) = M$.
By the Orbit-Stabilizer Theorem, the number of conjugates of $M$ is $|G.M| = [G : N_G(M)] = [G : M]$. Now all conjugates of $M$ have the same cardinality as $M$, ans we will have the largest number of nonidentity elements in the conjugates of $M$ precisely when these conjugates intersect trivially. In this case, the number of nonidentity elements in the conjugates of $M$ is at most $(|M| - 1) \cdot [G : M]$. ☕

4.3.24 Assume $H$ is a proper subgroup of the finite group $G$. Prove $G \neq \cup_{g \in G}$, i.e., $G$ is not the union of the conjugates of any proper subgroup.

*Proof.* *From Online Solution Manual*
There exists a maximal subgroup $M$ containing $H$. If $M$ is normal in $G$, then

$$\bigcup_{g \in G} gHg^{-1} \subseteq \bigcup_{g \in G} gMg^{-1} = M \neq G.$$

If $M$ is not normal, we still have

$$\bigcup_{g \in G} gHg^{-1} \subseteq \bigcup_{g \in G} gMg^{-1}.$$

By Exercise 23 above, we know that

$$\bigcup_{g \in G} gMg^{-1}$$

contains at most $(|M| - 1) \cdot [G : M]$ nonidentity elements. Thus,

$$\left| \bigcup_{g \in G} gHg^{-1} \right| \leq |G| - [G : M] + 1 < |G|$$

because $[G : M] \geq 2$. Since $G$ is finite,

$$G \neq \bigcup_{g \in G} gHg^{-1}.$$

Thus, $G$ is not the union of all conjugates of any proper subgroup. ☕

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 $a \in A$ (such an element is called *fixed point free*).

*Proof.* *From Online Solution Manual*
By way of contradiction, suppose that for all $\sigma \in G$, there exists $a \in A$ such that $\sigma(a) = a$. Then

$$\bigcup_{a \in A} G_a.$$

Now because this action is transitive, if we fix $b \in A$, then as $\sigma$ ranges over $G$, $\sigma \cdot b$ is arbitrary in $A$. So in fact,

$$G = \bigcup_{\sigma \in G} G_{\sigma(b)} = \bigcup_{\sigma \in G} \sigma G_b \sigma^{-1}.$$

Now, because the action is transitive, and $|A| > 1$, we know that $G_b$ is a proper subgroup. Thus, $G \leq S_a$ is finite. By Exercise 24 above, we have a contradiction. Thus, there exists an element $\sigma \in G$ that is fixed point free.

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.

*Proof.* *From Online Solution Manual*
Let $G$ act on itself by conjugation. Not that

$$g_1, g_2, \ldots, g_r \in G_{g_k}$$

for all $k \in \{1, \ldots, r\}$. Let $x \in G$. Then,

$$x = a g_i a^{-1}$$

for some $a \in G$ and $g_i$. Thus, $x \in a G_{g_k} a^{-1}$ for each $k$ since $g_i$ stabilizes each $g_k$. Moreover,

$$x \in \bigcup_{a \in G} a G_{g_k} a^{-1}$$

for all $k$. So,

$$G = \bigcup_{a \in G} a G_{g_k} a^{-1}$$

for each $k$. Since $G$ is finite, then by Exercise 24, $G_{g_k}$ must not be a proper subgroup, i.e., $G_{g_k} = G$ for each $g_k$.

Now, let $a, b \in G$ where $a = x g_a x^{-1}$ and $b = y g_b y^{-1}$. Then,

$$\begin{aligned} ab &= (x g_a x^{-1})(y g_b y^{-1}) \\ &= x x^{-1} g_a g_b y y^{-1} \\ &= g_b g_a \\ &= y y^{-1} g_b g_a x x^{-1} \\ &= y g_b y^{-1} x g_a x^{-1} \\ &= ba \end{aligned}$$

Therefore, $G$ is abelian.

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 subgroup for either $p, q$, or $r$.

*Proof.* Suppose no Sylow subgroup for either $p, q$, or $r$ is normal. Then, since $n_r | pq$ then $n_r \in \{p, q, pq\}$. But since $p < q < r$, then neither $p$ nor $q$ can be congruent to $1 \mod r$. So, $n_r = pq$. Since each Sylow $r$-subgroup of $G$ has exactly $r - 1$ non-identity elements, we have

$$pq(r-1) = pqr - pq \tag{1}$$

total non-identity elements of $G$ from the Sylow $r$-subgroups.
Since $n_q | pr$ then $n_1 \in \{p, r, pr\}$. But since $p < q$, then $p$ cannot be congruent to $1 \mod q$. Thus, $n_q = r$ or $n_q = pr$. In either case,

$$n_q(q-1) > p(q-1) = pq - p, \tag{2}$$

i.e., there are more than $pq - p$ non-identity elements from the Sylow $q$- subgroups. Since $n_p | qr$, then $n_p \in \{q, r, qr\}$. By (1) and (2), $G$ has less than

$$pqr - ((pqr - pq) + (pq - p) + 1) = p - 1$$

elements left to make up the number of nonidentity elements in the Sylow $p$-subgroups, which is impossible since there are at least $q(p-1)$ nonidentity elements from the Sylow $p$-subgroups. Thus, we have a contradiction. ☕

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

*Proof.* Notice that $132 = 2^2 \cdot 3 \cdot 11$. Since $n_2 | (3 \cdot 11)$ and $n_2 \equiv 1 \mod 2$, then $n_2 \in \{1, 3, 11\}$. Similarly, since $n_3 | (2^2 \cdot 11)$ and $n_3 \equiv 1 \mod 3$ then $n_3 \in \{1, 4\}$. And finally, since $n_{11} | (2^2 \cdot 3)$ and $n_{11} \equiv 1 \mod 11$ then $n_{11} \in \{1, 12\}$. Suppose for contradiction that $G$ is simple. Then, $n_3 = 4$, which means $G$ contains exactly $4(3-1) = 8$ elements of order 3. Similarly, $n_{11} = 12$ which means $G$ contains exactly $12(11-1) = 120$ elements of order 11 in $G$. Then there are $132 - 8 - 120 = 4$ elements of order $G$ which are not of order 3 nor 11. So, there is space for exactly 1 Sylow 2-subgroup of order 4, i.e., $n_2 = 1$ and so $G$ contains a normal subgroup of order 4, a contradiction. Thus $G$ is not simple.

☕

5.1.2 Let $G_1, G_2, \ldots, G_n$ be groups and let $G = G_1 \times \cdots \times G_n$. Let $I$ be a proper, nonempty subset of $\{1, \ldots, n\}$ and let $J = \{1, \ldots, n\} - I$. Define $G_I$ to be the set of elements of $G$ that have the identity of $G_j$ in position $j$ for all $j \in J$.

(a) Prove that $G_I$ is isomorphic to the direct product of the groups $G_i$, $i \in J$,

*Proof.* We first show that $G_I \leq G$. Since $(1, 1, \ldots, 1, 1, 1) \in G_I$, then $G_I \neq \emptyset$. Let $x, y \in G_I$. For each $i \in I$, the coordinates $x_i$ and $y_i^{-1}$ of $x$ and $y^{-1}$ respectively are in $G_i$ and so $x_i y_i^{-1} \in G_i$. For each $j \in J$, we have $x_j = 1_{G_j}$ and $y_j^{-1} = 1_{G_j}$ as the $j$-th coordinate of $x$ and $y$, respectively, and so $x_j y_j^{-1} = 1_{G_j} \in G_j$. Since the $k$-th coordinate of the product of $xy^{-1}$ is in $G_k$ for all $1 \leq k \leq n$, then $xy^{-1} \in G_I$. So, $G_I \leq G$.

Let $I = \{i_1, i_2, \dots, i_k\}$. We define a map

$$\varphi : G_I \to G_{i_1} \times G_{i_2} \times \cdots \times G_{i_k}$$

where the $n$-tuple $x$ is mapped to the $k$-tuple $y$ in the following way: The $r$-th coordinate of $y$ takes the value corresponding to the coordinate $x_{i_r}$ of $x$, where $i_r \in I$.
Given $y \in G_{i_1} \times \cdots \times G_{i_k}$, we can choose $x \in G_I$ so that for all $i_r \in I$, the $i_r$-th coordinate of $x$ corresponds to the $r$-th coordinate of $y$. Thus, $\varphi$ is surjective. Also, if two elements $x, y \in G_I$ are not equal, then it must be the case that for at least one index $i_r \in I$, the coordinates $x_{i_r}$ and $y_{i_r}$ of $x$ and $y$, respectively, are not equal. Thus, by definition of $\varphi$, we will have $\varphi(x) \neq \varphi(y)$ and so $\varphi$ is injective. Finally, for any $x, y \in G_I$, consider the coordinates $x_{i_r}$ and $y_{i_r}$ of $x$ and $y$, respectively, $i_r \in I$. Then, the product $xy$ will have $x_{i_r}y_{i_r}$ as it's $i_r$-th coordinate. So, $\varphi(xy)$ will have $x_{i_r}y_{i_r}$ as it's $r$-th coordinate. Then, $\varphi(x)$ and $\varphi(y)$ will have their $r$-th coordinates the values $x_{i_r}$ and $y_{i_r}$, respectively. So, $\varphi(x)\varphi(y)$ will have as it's $r$-th coordinate the value $x_{i_r}y_{i_r}$. Thus, $\varphi(xy) = \varphi(x)\varphi(y)$. So, $\varphi$ is an isomorphism. ☕

(b) Prove that $G_I$ is a normal subgroup of $G$ and $G/G_I \cong G_J$.

*Proof.* Let $J = \{j_1, \dots, j_\ell\}$. Define a map

$$\psi : G \to G_J$$

where the $n$ tuple $x$ is sent to the $\ell$-tuple $y$ in the following way: The $t$-th coordinate of $y$ takes on the values corresponding to the $j_t$-th coordinate of $x$.
Given any $y \in G_j$, we can let $x \in G$ be the $n$-tuple which has $x_{j_t}$ as the $j_t$-th coordinate where $x_{j_t}$ equals the $t$-th coordinate of $y$ for all $j_t \in J$. Then $\psi(x) = y$ and so $\psi$ is surjective. By a very similar argument as in part (a), we see that $\psi$ is a group homomorphism. Now,

$$\begin{aligned}
\ker(\psi) &= \{x \in G \mid \psi(x) = (1,1,1\dots,1) = \text{ the } \ell\text{-tuple consisting of all identity elements.}\} \\
&= \{x \in G \mid x = (1,1,\dots,1) = \text{ the } n\text{-tuple consisting of all identity elements.}\} \\
&= \{x \in G \mid x \text{ has the identity in the } j\text{-th coordinate for all } j \in J.\} \\
&= G_I
\end{aligned}$$

By the First Isomorphism Theorem, $G_I \trianglelefteq G$ and $G/G_I \cong G_J$. ☕

(c) Prove that $G \cong G_I \times G_J$.

*Proof.* Since $G_I \trianglelefteq G$, and $G_J \leq G$, then $G_IG_J \leq G$. Since $G_I \cap G_J = 1$, then

$$|G_IG_J| = \frac{|G_I||G_J|}{|G_I \cap G_J|} = \frac{|G_I||G_J|}{1} = |G|.$$

So, $G = G_IG_J$. By a similar map as in $(b)$, we get that $G_J \trianglelefteq G$ and so by Theorem 9, (pg. 171, D&F), we have $G \cong G_I \times G_K$. ☕

5.4.11 Prove that if $G = HK$ where $H$ and $K$ are characteristic subgroups of $G$ with $H \cap K = 1$, then $\mathrm{Aut}(G) \cong \mathrm{Aut}(H) \times \mathrm{Aut}(K)$. Deduce that if $G$ is an abelian group of finite order then $\mathrm{Aut}(G)$ is isomorphic to the direct product of the automorphism groups of its Sylow subgroups.

*Proof.* Define the map

$$f : \mathrm{Aut}(G) \to \mathrm{Aut}(H) \times \mathrm{Aut}(K) \text{ by } \sigma \mapsto (\sigma|_H, \sigma|_K).$$

<u>$f$ is a homomorphism:</u> Let $\sigma, \tau \in \mathrm{Aut}(G)$. Since $H$ is characteristic in $G$, $\sigma|_H(H) = H$ and similarly, $\tau|_H(H) = H$. So, $(\sigma \circ \tau)|_H = \sigma|_H \circ \tau|_H$. Similarly for $K$. Then,

$$\begin{aligned} f(\sigma \circ \tau) &= ((\sigma \circ \tau)|_H, (\sigma \circ \tau)|_K) \\ &= (\sigma|_H \circ \tau|_H, \sigma|_K \circ \tau|_K) \\ &= (\sigma|_H, \sigma|_K)(\tau|_H, \tau|_K) \\ &= f(\sigma) \circ f(\tau). \end{aligned}$$

<u>$f$ is surjective:</u> Let $(\alpha, \beta) \in \mathrm{Aut}(H) \times \mathrm{Aut}(K)$. We need to find $\sigma \in \mathrm{Aut}(G)$ so that $f(\sigma) = (\alpha, \beta)$. First, define

$$\tilde{\sigma} : H \times K \to H \times K, \quad \text{where } \tilde{\sigma}(h, k) = (\alpha(h), \beta(k)).$$

We claim $\tilde{\sigma} \in \mathrm{Aut}(H \times K)$.

- $\tilde{\sigma}$ is a group homomorphism:
  Let $h, h' \in H, k, k' \in K$. Then

$$\begin{aligned} \tilde{\sigma}((h,k)(h',k')) &= \tilde{\sigma}((hh', kk')) \\ &= (\alpha(hh'), \beta(kk')) \\ &= (\alpha(h)\alpha(h'), \beta(k)\beta(k')) \\ &= (\alpha(h), \beta(k))(\alpha(h'), \beta(k')) \\ &= \tilde{\sigma}((h,k))\tilde{\sigma}((h',k')) \end{aligned}$$

- $\tilde{\sigma}$ is surjective:
  Since $\alpha, \beta$ are surjective, then given $h' \in H, k' \in K$, there exists $h \in H, k \in K$ so that $\alpha(h) = h'$ and $\beta(k) = k'$. Thus, $\tilde{\sigma}((h,k)) = (\alpha(h), \beta(k)) = (h', k')$.
- $\tilde{\sigma}$ is injective:
  If $\tilde{\sigma}((h,k)) = \tilde{\sigma}((h'k'))$, then $(\alpha(h), \beta(k)) = (\alpha(h'), \beta(k'))$, which means $\alpha(h) = \alpha(h')$ and $\beta(k) = \beta(k')$. Since both $\alpha$ and $\beta$ are injective, $h = h'$ and $k = k'$ which means $(h,k) = (h',k')$.

Since $H$ and $K$ are characteristic in $G$, they are normal subgroups of $G$. Since $H \cap K = 1$ and $G = HK$, then by Theorem 9, (p 171, D& F), $G \cong H \times K$. Now, let

$$j : G \to H \times K \text{ where } hk \mapsto (h,k)$$

be the canonical isomorphism between $G$ and $H \times K$. Since $H \cap K = 1$ and $HK = G$, then each element $g \in G$ can be expressed as a *unique* product $hk$ for $h \in H, k \in K$. Therefore, $j^{-1}$ is well-defined. Then,

$$j^{-1} \circ \tilde{\sigma} \circ j : G \to H \times K \to H \times K \to G.$$

Claim: $\sigma = j^{-1} \circ \tilde{\sigma} \circ j$ gives $f(\sigma) = (\alpha, \beta)$ as desired. We show that $\sigma|_H = \alpha$. Let $h \in H$. Then,

$$\begin{aligned}\sigma(h) &= (j^{-1} \circ \tilde{\sigma} \circ j)(h) \\ &= (j^{-1} \circ \tilde{\sigma}) j(h) \\ &= j^{-1}(\tilde{\sigma}(h, 1_G)) \\ &= j^{-1}((\alpha(h), \beta(1_G))) \\ &= j^{-1}((\alpha(h), 1_G)) \\ &= \alpha(h) \cdot 1_G \\ &= \alpha(h).\end{aligned}$$

Similarly, we get $\sigma|_K = \beta$. Thus, $f(\sigma) = (\sigma|_H, \beta|_K) = (\alpha, \beta)$ and $f$ is surjective.
$f$ is injective: Let $\sigma, \tau \in \mathrm{Aut}(G)$ and suppose $f(\sigma) = f(\tau)$. Then $(\sigma|_H, \sigma|_K) = (\tau|_H, \tau|_K)$ and so $\sigma|_H = \tau|_H$ and $\sigma|_K = \tau|_K$. Let $g \in G$. We need to show that $\sigma(g) = \tau(g)$. Since $G = HK$, $g = hk$ for some $h \in H, k \in K$. So,

$$\sigma(g) = \sigma(hk) = \sigma(h)\sigma(k) = \tau(h)\tau(k) = \tau(hk) = \tau(g).$$

---

Let $G$ be abelian and $|G| = n < \infty$ and let the unique factorization of $n$ into distinct prime powers be

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$$

Since $G$ is abelian, then all of its subgroups are normal subgroups. In particular, every Sylow $p_j$-subgroup is normal for all $1 \leq j \leq k$. Let $Q_j \in \mathrm{Syl}_{p_j}(G)$ for all $1 \leq j \leq k$. Since each $Q_j$ is normal in $G$, each $Q_j$ is the unique Sylow $p_j$-subgroup of order $p_j^{\alpha_j}$. Since each $Q_j$ is normal in $G$, then

$$Q_1 Q_2 \dots Q_k \leq G.$$

For each fixed $i \in \{1, \dots, k\}$ and $j \in \{1, \dots, k\}$ if $i \neq j$ then $Q_i \cap Q_j = 1$ and so $|Q_1 Q_2 \dots Q_k| = |G|$. Thus, $Q_1 Q_2 \dots Q_k = G$. Therefore, by what was just proved,

$$\mathrm{Aut}(G) \cong \mathrm{Aut}(Q_1) \times \mathrm{Aut}(Q_2) \times \cdots \times \mathrm{Aut}(Q_k).$$

☕

4.5.32 Let $P$ be a Sylow $p$-subgroup of $H$ and let $H$ be a subgroup of $K$. If $P \trianglelefteq H$ and $H \trianglelefteq K$ prove that $P$ is normal in $K$. Deduce that if $P \in Syl_p(G)$ and $H = N_G(P)$ then $N_G(H) = H$.

*Proof.* Since $P \trianglelefteq H$ and $P$ is a Sylow $p$-subgroup of $H$, then $P$ is characteristic in $H$. Since $H \trianglelefteq K$ then $conj(k)(H) = kHk^{-1} = H$ for all $k \in K$. So $conj(k) \in \mathrm{Aut}(H)$ for all $k \in K$. Since $P$ is characteristic in $H$, then

$$P = conj(k)(P) = kPk^{-1} \quad \forall k \in K.$$

Therefore, $P \trianglelefteq K$.

---

Since $H = N_G(P)$ then $P \trianglelefteq H$. Let $K = N_G(H)$. Since $H \trianglelefteq N_G(H) = K$ then by what was just proved, $P \trianglelefteq K = N_G(H)$, which implies $N_G(H) = N_G(P) = H$. ☕

4.5.34 Let $P \in Syl_p(G)$ and assume $N \trianglelefteq G$. Use the conjugacy part of Sylow's Theorem to prove that $P \cap N$ is a Sylow $p$-subgroup of $N$. Deduce that $PN/N$ is a Sylow $p$-subgroup of $G/N$.

*Proof.* Let $Q \in Syl_p(N)$. Then there exists $g \in G$ so that $Q \leq gPg^{-1}$. Since $Q \leq N$ and $Q \leq gPg^{-1}$ then $Q \leq gPg^{-1} \cap N$. Then,

$$\begin{aligned} Q &\leq gPg^{-1} \cap N \\ Q &\leq gPg^{-1} \cap gNg^{-1} && \text{(Since } N \trianglelefteq G\text{)} \\ Q &\leq g(P \cap N)g^{-1} \\ g^{-1}Qg &\leq P \cap N \end{aligned}$$

Since $g^{-1}Qg \in Syl_p(N)$ then $g^{-1}Qg$ is of maximal prime power order in $N$. Since $P \cap N$ is a subgroup of $N$ with prime order, it must be that $P \cap N = g^{-1}Qg$, i.e., $P \cap N \in Syl_p(N)$.

Observe that

$$|G/N| = \frac{|G|}{|N|} = p^{\alpha-\beta} \cdot (m\tilde{n}).$$

By the Second Isomorphism Theorem, $PN/N \cong P/P \cap N$. So,

$$|PN/N| = |P/P \cap N| = \frac{|P|}{|P \cap N|} = \frac{p^\alpha}{p^\beta} = p^{\alpha-\beta}.$$

Therefore, $PN/N \in Syl_p(G/N)$. ☕

4.5.36 Prove that if $N \trianglelefteq G$ then $n_p(G/N) \leq n_p(G)$.

*Proof.* Let $|G| = p^\alpha \cdot m$ and $|N| = p^\beta \cdot \tilde{n}$ where $m$ and $\tilde{n}$ do not divide $p^\alpha$ and $p^\beta$, respectively. Note that from the previous exercise, $PN/N \in Syl_p(G/N)$ for any $P \in Syl_p(G)$. Define a map

$$\varphi : Syl_p(G) \to Syl_p(G/N) \text{ by } P \mapsto PN/N.$$

We show that $\varphi$ is surjective so that $|Syl_p(G)| \leq |Syl_p(G/N)|$, i.e., $n_p(G/N) \leq n_p(G)$. Let $\overline{Q} \in Syl_p(G/N)$. By the 4th Isomorphism Theorem, there exists a subgroup $Q \leq G$ so that $N \leq Q$ and $Q/N = \overline{Q}$. Notice

$$p^{\alpha-\beta} = |\overline{Q}| = \big|Q/N\big| = \frac{|Q|}{|N|} \implies |Q| = p^{\alpha} \cdot \tilde{n}.$$

Let $R \in Syl_p(Q)$. Then $|R| = p^{\alpha}$ and so $R \in Syl_p(G)$. Again by the previous exercise, $RN/N \in Syl_p(G/N)$. Notice that $R \leq Q$ and $N \trianglelefteq Q$ so that $RN \leq Q$. Then $RN/N \leq Q/N$ but

$$|RN/N| = p^{\alpha-\beta} = |Q/N|.$$

Therefore,

$$\varphi(R) = RN/N = Q/N = \overline{Q}.$$

☕

5.1.4 Let $A$ and $B$ be finite groups a $p$ be prime. Prove that any Sylow $p$-subgroup of $A \times B$ is of the form $P \times Q$, where $P \in Syl_p(A)$ and $Q \in Syl_p(B)$. Prove that $n_p(A \times B) = n_p(A)n_p(B)$. Generalize both of these results to a direct product of any finite number of finite groups (so that the numbers of Sylow $p$-subgroups of a direct product is the product of the numbers of Sylow $p$-subgroups of the factors).

*Proof.* First notice that

$$\begin{aligned} N_{A\times B}(P \times Q) &= \{(a,b) \in A \times B \mid (a,b)(p,q)(a^{-1},b^{-1}) \in P \times Q \ \ \forall\ (p,q) \in P \times Q\} \\ &= \{(a,b) \in A \times B \mid (apa^{-1}, bqb^{-1}) \in P \times Q \ \ \forall\ p \in P, \ \ \forall\ q \times Q\} \\ &= \{a \in A, b \in B \mid apa^{-1} \in P, bqb^{-1} \in Q \ \ \forall\ p \in P, \ \ \forall\ q \in Q\} \\ &= \{a \in A \mid apa^{-1} \in P \ \ \forall\ p \in P\} \times \{b \in B \mid bqb^{-1} \in Q \ \ \forall\ q \in Q\} \\ &= N_A(P) \times N_B(Q) \end{aligned}$$

Which gives

$$n_p(A)n_p(B) = \frac{|A| \cdot |B|}{|N_A(P)| \cdot |N_B(Q)|} = \frac{|A| \cdot |B|}{|N_A(P) \times N_B(Q)|} = \frac{|A \times B|}{|N_{A\times B}(P \times Q)|} = n_p(A \times B).$$

Let $|A| = p^{\alpha} \cdot m$ and $|B| = p^{\beta} \cdot \tilde{n}$. Let $P \in Syl_p(A)$ and $Q \in Syl_p(B)$. Then, $P \times Q \leq A \times B$ and $|P \times Q| = |P| \cdot |Q| = p^{\alpha+\beta}$ which implies $P \times Q \in Syl_p(A \times B)$.
(Couldn't figure out the opposite direction for this proof. What is left is from the online solution manual).
Now, let $R \in Syl_p(A \times B)$. Define $X = \{x \in A \mid (x,y) \in R \text{ for some } y \in B\}$ and $Y = \{y \in B \mid (x,y) \in R \text{ for some } x \in A\}$. Then $X \leq A$ because

$$\begin{aligned} x_1, x_2 \in X &\implies (x_1,y_1),(x_2,y_2) \in R \text{ for some } y_1, y_2 \in B \\ &\implies (x_1x_2^{-1}, y_1, y_2^{-1}) \in R \\ &\implies x_1, x_2^{-1} \in X \\ &\implies X \leq A. \end{aligned}$$

Similarly, we get $Y \leq B$. Note that if $(x, y) \in R$ then $|(x, y)| = p^k$ for some $k$. We also know $|(x, y)| = \text{lcm}(|x|, |y|)$ so that $x$ and $y$ have $p$-power order. So, $X$ and $Y$ are $p$-subgroups, as otherwise some nonidentity element does not have $p$-power order. By Sylow's Theorem, there exist Sylow $p$-subgroups $P$ and $Q$ of $A$ and $B$, respectively so that $X$ is contained in $P$ and $Y$ is contained in $Q$, i.e., $X \leq P$ and $Y \leq Q$. Then, $R \leq X \times Y \leq P \times Q$. But since $|R| = p^{\alpha+\beta} = |P \times Q|$ implies $R = P \times Q$.
Thus any Sylow $p$-subgroup of $A \times B$ has the form $P \times Q$ for some $P \in Syl_p(A)$ and $Q \in Syl_p(B)$.

---

By induction we can show that the numbers of Sylow $p$-subgroups of a direct product is the product of the numbers of Sylow $p$-subgroups of the factors. The base case is done above. Suppose for some $k \geq 2$, for an arbitrary direct product of groups $G = \prod_{i=1}^k G_i$, every Sylow $p$-subgroup of $G$ is a product of Sylow $p$-subgroups of the $G_i$'s, and vice versa. Let $G = \prod_{i=1}^{k+1}$ be arbitrary. Then every Sylow $p$-subgroup of $G$ is of the form $P \times P_{k+1}$ where $P \leq \prod_{i=1}^k G_i$ and $P_{k+1} \leq G_{k+1}$ are Sylow $p$-subgroups, and vice versa. By the induction hypothesis, $P = \prod_{i=1}^k P_i$ for Sylow $p$-subgroups $P_1 \leq G_i$. Thus every Sylow $p$-subgroup of $G$ has the form $\prod_{i=1}^k P_i$ for some Sylow $p$-subgroups $P_i \leq G_i$ and vice versa. Also,

$$n_p\left(\prod_{i=1}^k G_i\right) = \prod_{i=1}^k n_p(G_i)$$

☕

5.4.15 If $A$ and $B$ are normal subgroups of $G$ such that $G/A$ and $G/B$ are both abelian, prove that $G/(A \cap B)$ is abelian.

*Proof.* Since $G/A$ and $G/B$ are abelian then by Proposition 7, part (4), (D& F,§5.4) , $G' \leq A$ and $G' \leq B$. Then $G' \leq A \cap B$. Then by the same proposition, we have $A \cap B \trianglelefteq G$ and $G/(A \cap B)$ is abelian. ☕

5.5.1 Let $H$ and $K$ be groups, let $\varphi$ be a homomorphism from $K$ into $\mathrm{Aut}(H)$ and, as usual, identify $H$ and $K$ as subgroups of $G = H \rtimes_{\varphi} K$. Prove that $C_K(H) = \ker \varphi$.

*Proof.*

$$\begin{aligned}
\ker \varphi &= \{k \in K \mid \varphi(k) = 1_{\mathrm{Aut}(H)}\} \\
&= \{k \in K \mid \varphi(k)(h) = h \ \ \forall h \in H\} \\
&= \{k \in K \mid k \cdot h = h \ \ \forall h \in H\} \\
&= \{k \in K \mid khk^{-1} = h \ \ \forall h \in H\} \\
&= \{k \in K \mid k \in C_G(H)\} \\
&= K \cap C_G(H) \\
&= C_K(H)
\end{aligned}$$

---

*Alternate proof:*
Let $(1, k) \in C_K(H)$. Then for all $(h, 1) \in H$,

$$\begin{aligned}
(h, 1) &= ((1, k)(h, 1)(1, k^{-1})) \\
&= (1k \cdot h, k)(1, k^{-1}) \\
&= (\varphi(k)(h), k)(1, k^{-1}) \\
&= ((\varphi(k)(h))k \cdot 1, kk^{-1}) \\
&= (\varphi(k)(h)\varphi(k)(1), 1) \\
&= (\varphi(k)(h1), 1) \\
&= (\varphi(k)(h), 1).
\end{aligned}$$

Thus, $h = \varphi(k)(h)$, which means $\varphi(k) = 1_{Aut(H)}$. Identifying $k$ as $(1, k)$, we have $(1, k) \in \ker \varphi$.

☕

5.5.2 Let $H$ and $K$ be groups, let $\varphi$ be a homomorphism from $K$ into $\mathrm{Aut}(H)$ and, as usual, identify $H$ and $K$ as subgroups of $G = H \rtimes_{\varphi} K$. Prove that $C_H(K) = N_H(K)$.

*Proof.* Since the centralizer of $K$ is always contained in the normalizer of $K$, it suffices to show that $N_H(K) \leq C_H(K)$. Let $(h, 1) \in N_H(K)$. Then for all $(1, k) \in K$, we have

$$\begin{aligned}
K \ni (h, 1)(1, k)(h^{-1}, 1) &= (h1 \cdot 1, 1k)(h^{-1}, 1) \\
&= (h, k)(h^{-1}, 1) \\
&= (hk \cdot h^{-1}, k1) \\
&= (h\varphi(k)(h^{-1}), k).
\end{aligned}$$

But $(h\varphi(k)(h^{-1}), k) \in K \implies (h\varphi(k)(h^{-1}), k) = (1, k)$, or in other words,

$$(h, 1)(1, k)(h^{-1}, 1) = (h\varphi(k)(h^{-1}), k) = (1, k)$$

so that $(h, 1) \in C_H(K)$. ☕

6.1.17 Prove that $G^{(i)}$ is a characteristic subgroup of $G$ for all $i$.

*Proof.* We proceed by induction on $i$. For $i = 0$, we have $G^0 = G$, so trivially, $G$ is characteristic in $G$. Now, let $i \geq 1$ and suppose $G^{(i)}$ is characteristic in $G$. Let $\sigma \in \text{Aut}(G)$. Notice that if $[x, y] \in G^{(i)}$, then

$$\sigma([x, y]) = \sigma(x^{-1}y^{-1}xy) = \sigma(x)^{-1}\sigma(y)^{-1}\sigma(x)\sigma(y) = [\sigma(x), \sigma(y)]$$

and so $\sigma([x, y]) \in G^{(i)}$, which means for any commutator $[x, y] \in G^{(i)}$, we have $\sigma([x, y])$ is again a commutator of $G^{(i)}$. So, $\sigma([G^{(i)}, G^{(i)}]) = [\sigma(G^{(i)}), \sigma(G^{(i)})]$. Therefore,

$$\sigma(G^{(i+1)}) = \sigma([G^{(i)}, G^{(i)}]) = [\sigma(G^{(i)}), \sigma(G^{(i)})] = [G^{(i)}, G^{(i)}] = G^{(i+1)}$$

which completes the induction. ☕

1. The following exercise classifies all groups of order 231 up to isomorphism: Let $G$ be a group of order 231.

   (a) Prove that there is a unique $P \in Syl_7(G)$ and a unique $H \in Syl_{11}(G)$ and that $H$ lies in the center $Z(G)$.

   *Proof.* Let $|G| = 231$. notice that $231 = 3 \cdot 7 \cdot 11$. So by Sylow's Theorem, we get the following:

$$n_7 \equiv 1 \mod 7 \text{ and } n_7 \big| 3 \cdot 11 \implies n_7 = 1,$$
$$n_{11} \equiv 1 \mod 11 \text{ and } n_{11} \big| 3 \cdot 7 \implies n_{11} = 1.$$

   Let $H \in Syl_{11}(G)$. Since $|H| = 11$, then $H \cong \mathbb{Z}/11$. By Proposition 16 (D& F,§4.4 ) we have $\text{Aut}(\mathbb{Z}/11) \cong (\mathbb{Z}/11\mathbb{Z})^\times$. Thus, $\text{Aut}(H) \cong (\mathbb{Z}/11\mathbb{Z})^\times \cong \mathbb{Z}/10$. Since $H$ is the unique Sylow 11-subgroup, $H \trianglelefteq G$, i.e., $N_G(H) = G$. Recall that $N_G(H)/C_G(H)$ is isomorphic to a subgroup of $\text{Aut}(H)$. Thereore,

$$G/C_G(H) = N_G(H)/C_G(H) \cong J \leq \text{Aut}(H) \cong \mathbb{Z}/10$$

   for some subgroup $J \leq \text{Aut}(H)$. Since $H$ is cyclic of prime order, it is abelian, which means $H \leq C_G(H)$, and so

$$H \leq C_G(H) \leq G.$$

   Since $[G : H] = [G : C_G(H)] \cdot [C_G(H) : H]$, then $[G : C_G(H)]$ divides $[G : H] = |G|/|H| = 21$. Since $G/C_G(H) \cong J$ then $|J|$ divides 21. And since $J \leq \mathbb{Z}/10$, then $|J|$ divides 10. But since $\gcd(10, 21) = 1$, then $J$ is trivial. So, $[G : C_G(H)] = 1$, which implies $C_G(H) = G$ and so $H \leq Z(G)$. ☕

   (b) Prove that there exist elements $x, y \in G$ such that $o(x) = 3$ and $o(y) = 7$. Let $K = \langle x, y\rangle$. Prove that $G = HK$ and that $K$ is a normal subgroup of $G$ which has trivial intersection with $H$. Deduce that $G$ is isomorphic to $H \times K$.

   *Proof.* Since 3 and 7 are primes dividing $|G|$, then there exists $x, y \in G$ where $|x| = 3$ and $|y| = 7$ by Cauchy's Theorem. Let $K = \langle x, y\rangle$. Since $H \trianglelefteq G$ and $K \leq G$, then $HK \leq G$. Notice that $|\langle x, y\rangle| = |\langle x\rangle \times \langle y\rangle|$ since the map $(x^i, y^j) \mapsto x^i y^j$ is an isomorphism. So, $|K| = |\langle x, y\rangle| = |\langle x\rangle \times \langle y\rangle| = 3 \cdot 7$.
   Since every non-identity element of $H$ and $K$ have order 11 and 3, respectively, then $H \cap K = \{1\}$. Then by Theorem 9, (D& F, §5.4) we have $G \cong H \times K$. ☕

   (c) Show that there are precisely two isomorphism types of groups of order 231 (use our criterion for semidirect products to describe the two possible isomorphism types of $K$). Let $H = \langle z\rangle$. Give a presentation with generators and relations of the two isomorphism types of $G$.

   *Proof.* Since $H$ is cyclic, of prime order, and has one generator, it cannot be broken down into a direct product or semidirect product. However, we can write $K$ as a semidirect product. Since $\langle x, y\rangle \cong \langle x\rangle \times \langle y\rangle$, $\langle y\rangle \trianglelefteq K$ and $\langle x\rangle \cap \langle y\rangle = \{1\}$, then

$$K = \langle x, y\rangle \cong \langle y\rangle \rtimes_\varphi \langle x\rangle$$

where $\varphi : \langle x \rangle \to \mathrm{Aut}(\langle y \rangle)$. By the First Isomorphism Theorem, $\varphi(\langle x \rangle) \cong \langle x \rangle / \ker \varphi$. Since $\langle x \rangle \cong \mathbb{Z}/3$ and $\ker \varphi \trianglelefteq \langle x \rangle$, then $|\ker \varphi|$ is either 3 or 1. If it is 3, then $|\varphi(\langle x \rangle)| = 1$ which means $\varphi$ is the trivial map. Thus,

$$\langle y \rangle \underset{\varphi}{\rtimes} \langle x \rangle \cong \langle y \rangle \times \langle x \rangle$$

and so $K \cong \langle y \rangle \times \langle x \rangle$. Now, if $|\ker \varphi| = 1$ then $|\varphi(\langle x \rangle)| = 3$. Since $\langle y \rangle \cong \mathbb{Z}/7$, then $\mathrm{Aut}(\langle y \rangle) \cong (\mathbb{Z}/7\mathbb{Z})^\times \cong \mathbb{Z}/6$. Thus $\mathrm{Aut}(\langle y \rangle)$ has order 6 and is cyclic. Let $\sigma \in Aut(\langle y \rangle)$ be given by the map $y \mapsto y^2$. Since $|\varphi(\langle x \rangle)| = 3$, then $\varphi(\langle x \rangle) = \{id, \sigma, \sigma^2\}$. So, $\varphi$ can be defined in one of the following ways:

$$\varphi_1 : \langle x \rangle \to \mathrm{Aut}(\langle y \rangle) \;\text{ by }\; x \mapsto \sigma$$

or

$$\varphi_2 : \langle x \rangle \to \mathrm{Aut}(\langle y \rangle) \;\text{ by }\; x \mapsto \sigma^2.$$

We claim that in fact $\langle y \rangle \underset{\varphi_1}{\rtimes} \langle x \rangle \cong \langle y \rangle \underset{\varphi_2}{\rtimes} \langle x \rangle$. In order to show this, we show that the following defined an isomorphism between these two semidirect products:

$$\Phi : \langle y \rangle \underset{\varphi_1}{\rtimes} \langle x \rangle \to \langle y \rangle \underset{\varphi_2}{\rtimes} \langle x \rangle \;\text{ by }\; (y^a, x^b) \mapsto (y^a, x^{2b}).$$

$\Phi$ *is a homomorphism:*

$$\begin{aligned}
\Phi((y^{a_1}, x^{b_1})(y^{a_2}, x^{b_2})) &= \Phi(y^{a_1}\varphi_2(x^{b_1})(y^{a_2}), x^{b_1+b_2})) \\
&= \Phi(y^{a_1}\sigma^2(x^{b_1})(y^{a_2}), x^{b_1+b_2})) \\
&= \Phi(y^{a_1}\sigma(x^{2b_1})(y^{a_2}), x^{b_1+b_2})) \\
&= (y^{a_1}\sigma(x^{2b_1})(y^{a_2}), x^{2(b_1+b_2)}) \\
&= (y^{a_1}, x^{2b_1})(y^{a_2}, x^{2b_2}) \\
&= \Phi((y^{a_1}, x^{b_1}))\ \Phi((y^{a_2}, x^{b_2}))
\end{aligned}$$

$\Phi$ *is injective:*
If $\Phi((c,d)) = \Phi((c',d'))$ then $(c, 2d) = (c', 2d')$. Then $c = c' \mod 7$. Likewise, $2d = 2d' \mod 3 \implies 2(d-d') = 0 \mod 3 \implies d = d' \mod 3$. So, $(c,d) = (c',d')$.

$\Phi$ *is surjective:*
Given $(c,d) \in \langle y \rangle \underset{\varphi_2}{\rtimes} \langle x \rangle$, then $\Phi((c, 2d)) = (c, 4d) = (c, d)$ (since $4d = 1 \mod 3$).

Therefore, the semidirect products induced by $\varphi_1$ and $\varphi_2$ are precisely the same. In sum, we have the following two possibilities for $K$:

$$K \cong \langle y \rangle \times \langle x \rangle \cong \mathbb{Z}/7 \times \mathbb{Z}/3$$

or

$$K \cong \langle y \rangle \underset{\varphi_1}{\rtimes} \langle x \rangle \cong \mathbb{Z}/7 \underset{\varphi_1}{\rtimes} \mathbb{Z}/3.$$

Therefore, we get

$$G = H \times K \cong \mathbb{Z}/11 \times \mathbb{Z}/7 \times \mathbb{Z}/3 \tag{1}$$

or

$$G = H \times K \cong \mathbb{Z}/11 \times \mathbb{Z}/7 \rtimes_{\varphi_1} \mathbb{Z}/3. \tag{2}$$

Then, a presentation for $G$ in (1) is:

$$\langle a, b, c \mid a^{11} = b^7 = c^3 = 1, ab = ba, bc = cb, ac = ca \rangle.$$

To determine the presentation for $G$ in (2), we identify $y, x$ with $r, s$, respectively, and consider what relations the multiplication in the semidirect product $\langle y \rangle \rtimes_{\varphi_1} \langle x \rangle$ induce on $r, s$ through the map $(y^a, x^b) \mapsto r^a s^b$. We find that a presentation for $G$ in (2) is

$$\langle r, s \mid r^7 = s^3 = 1, r^2 s = sr \rangle.$$

2. The following exercise uses Sylow's Theorems to prove that all groups of order $9 \cdot 49 \cdot 13$ are solvable. Let $G$ be a group of this order. Prove that $G$ has a unique Sylow 13-subgroup $G_1$. Then prove that $G/G_1$ has a unique Sylow 7-subgroup $Y_2$. Let $G_2$ be the complete preimage of $Y_2$ in $G$. Show that

$$1 = G_0 \leq G_1 \leq G_2 \leq G$$

is a chain of subgroups of $G$ such that $G_1$ is normal in $G_2$ and $G_2$ is normal in $G$ and such that the successive quotients are abelian. Conclude that $G$ is solvable.

*Proof.* Let $|G| = 9 \cdot 49 \cdot 13$. Then by Sylow's Theorem we find that:

$$n_{13} \equiv 1 \mod 13 \text{ and } n_{13} \big| 9 \cdot 49 = 441.$$

So we consider divisors of 441: 1,3,7,9,21,49,63,147,441, and positive integers which are congruent to 1 mod 13: 1,14,27,40,53,66,79,92,105,118,131,144,157,..., 429,442. So we see that $n_{13}(G) = 1$. Now, let $G_1 \in Syl_{13}(G)$. Then $|G_1| = 13$, $G_1 \trianglelefteq G$, and $|G/G_1| = 9 \cdot 7^2$. Again by the Sylow Theorems

$$n_7(G/G_1) \equiv 1 \mod 7 \text{ and } n_7 \big| 9 \implies n_7(G/G_1) = 1.$$

Let $Y_2 \in Syl7(G/G_1)$. By the 4th Isomorphism Theorem, there exists a subgroup $G_2 \leq G$ so that $G_1 \trianglelefteq G_2$ and $G_2/G_1 \cong Y_2$. Since $|Y^2| = 7^2$, then

$$|G_2/G_1| = \frac{|G_2|}{|G_1|} = \frac{|G_2|}{13} \implies |G_2| = 13 \cdot 7^2.$$

Now notice:

- $G_1$ is of prime order and thus, cyclic, so $G_1/\{1\}$ is abelian.
- $G_2/G_1$ is abelian since $|G_2/G_1| = 7^2$, and all groups of order a square of a prime are abelian.
- $G/G_2$ is abelian since $|G/G_2| = 3^2$, and all groups of order a square of a prime are abelian.

and

- $G_1 \trianglelefteq G_2$ since $G_1 \trianglelefteq G$
- $G_2 \trianglelefteq G$ since $Y_2$ is the unique Sylow 7-subgroup of $(G/G_1)$ and thus $Y_2 \trianglelefteq (G/G_1)$ and by the 4th Isomorphism Theorem,
$$G_2/G_1 \cong Y_2 \trianglelefteq G/G_1 \iff G_2 \trianglelefteq G.$$

So,
$$1 = G_0 \trianglelefteq G_1 \trianglelefteq G_2 \trianglelefteq G$$
is a finite chain of subgroups so that $G_0 \trianglelefteq G_1, G_1 \trianglelefteq G_2$, and $G_2 \trianglelefteq G$ and successive quotient are abelian. So, $G$ is solvable. ☕

5.4.17 If $K$ is a normal subgroup of $G$ and $K$ is cyclic, prove that $G' \leq C_G(K)$.

*Proof.* First note that the automorphism groups an infinite cyclic group is abelian. To see this, let $\alpha \in \text{Aut}(\mathbb{Z})$. Then $\alpha(1) = n$ for some $n \in \mathbb{Z}$. Then for some $m \in \mathbb{Z}$, we have $\alpha(m) = 1$. So,
$$1 = \alpha(m) = \alpha(m \cdot 1) = m \cdot \alpha(1) = mn.$$
So $n$ must be 1 or $-1$, i.e., there are only 2 automorphisms in $\text{Aut}(\mathbb{Z})$ and thus $\text{Aut}(\mathbb{Z})$ is abelian.
Since $K$ is cyclic, $\text{Aut}(K)$ is abelian. Since $K \trianglelefteq G$, then $G = N_G(K)$. Then
$$G/C_G(K) = N_G(K)/C_G(K) \cong H \leq \text{Aut}(K)$$
for some subgroup $H \leq \text{Aut}(K)$. Since $\text{Aut}(K)$ is abelian, $H$ is abelian, which means $G/C_G(K)$ is abelian. Then by Proposition 7, Part (4) (D& F, §5.4, $G' \leq C_G(K)$. ☕

5.4.18 Let $K_1, K_2, \dots, K_n$ be non-abelian simple groups and let $G = K_1 \times K_2 \times \cdots \times K_n$. Prove that every normal subgroup of $G$ is of the for $G_I$ for some subset $I$ of $\{1, 2 \dots, n\}$ (where $G_I$) is defined in Exercise 2 of section 1.

*Proof.* Let $i \in \{1, 2, \dots, n\}$ and $a_i \in K_i$ where $a_i \neq 1_{K_i}$. Suppose $N \trianglelefteq G$ and let $x \in N$ with $x = (a_1, \dots, a_i, \dots, a_n)$. Since $K_i$ is non-abelian then there exists $g_i \in K_i$ such that $g_i a_i \neq a_i g_i$. Let $\tilde{g}_i = (1, \dots, 1, g_i, 1 \dots, 1)$ where $g_i$ appears in the $i$th coordinate. Since $x \in N \trianglelefteq G$ and $\tilde{g}_i \in G$,
$$\tilde{g}_i x^{-1} \tilde{g}_i \in N$$
and so $[\tilde{g}_i, x] \in N$ where
$$1_g \neq [\tilde{g}_i, x] = (1, \dots, 1, [g_i, a_i], 1 \dots, 1) \in N.$$
Define $A_i = \{h_i \in K_i \mid (1, \dots, 1, h_i, 1, \dots 1) \in N\}$. Then $A_i \leq K_i$. Moreover, $A_i \neq \{1_{K_i}\}$ because by the previous argument $[g_i, a_i] \neq 1_{K_i}$ and $[g_i, a_i] \in A_i$. We claim that $A_i = K_i$. Since $K_i$ is simple, it suffices to show that $A_i \trianglelefteq K_i$. let $h_i \in K_i$ and $g_i \in K_i$. Then
$$g_i h_i g_i^{-1} \in A_i \iff (1, \dots, 1, g_i h_i g_i^{-1}, 1, \dots, 1) \in N \iff \tilde{g}_i \tilde{h}_i \tilde{g}_i^{-1} \in N.$$
The latter is true since $\tilde{h}_i \in N$ and $N \trianglelefteq G$. Let $I \subseteq \{1, 2, \dots, n\}$ where $i \in I$ if and only if $A_i = K_i$. Then if $j \in \{1, \dots n\}$ and there exists $x = (a_1, \dots, a_j, \dots, a_n) \in N$ with $a_j \neq 1_{K_j}$. By the previous argument, $K_j = A_j \subseteq N$. Therefore $N = G_I$. ☕

7.1.7 The *center* of a ring $R$ is $\{z \in R \mid zr = rz \text{ for all } r \in R\}$. Prove that the center of a ring is a subring that contains the identity. Prove that the center of a division ring is a field.

*Proof.* Since $1_R r = r 1_R$ for all $r \in R$ then $1_R$ is in the center of $R$. Let $x, y$ be in center of $R$ and $r \in R$. Then

$$(x-y)r = xr - yr = rx - ry = r(x-y) \implies x - y \text{ is in the center of } R,$$

and

$$(xy)r = x(yr) = x(ry) = (xr)y = (rx)y = r(xy) \implies xy \text{ is in the center of } R.$$

Thus the center of $R$ is a subring of $R$. Now suppose $R$ is a division ring. If $x$ and $y$ are in the center of $R$, then certainly $xy = yx$ so that the center of $R$ is commutative. Since $R$ is a division ring, there exists $z \in R$ so that $xz = zx = 1$ for $x \neq 0_R$ in the center of $R$. Let $r \in R$. Then,

$$zr = z(r \cdot 1_R) = zr(xz) = z(xr)z = (zx)rz = (1_R)rz = rz,$$

so $z$ is in the center of $R$ and thus all elements of the center of $R$ not equal to 0 have multiplicative inverses. Thus the center of $R$ is a field. ☕

7.1.17 Let $R$ and $S$ be rings. Prove that the direct product $R \times S$ is a ring under componentwise addition and multiplication. Prove that $R \times S$ is commutative if and only if both $R$ and $S$ are commutative. Prove that $R \times S$ has an identity if and only if both $R$ and $S$ have identities.

*Proof.* We know that $(R \times S, +)$ is an abelian group since both $R$ and $S$ are abelian groups. Let $r_2, r_2, r_2 \in R$ and $s_1, s_2, s_3 \in S$. Observe that

$$\begin{aligned}(r_1, s_1)((r_2, s_2)(r_3, s_3)) &= (r_1, s_1)(r_2 r_3, s_2 s_3)\\ &= (r_1 r_2 r_3, s_1 s_2 s_3)\\ &= (r_1 r_2, s_1 s_2)(r_2, s_3)\\ &= ((r_1, s_1)(r_2, s_2))(r_3, s_3)\end{aligned}$$

so that $\cdot$ is associative. Also,

$$\begin{aligned}(r_, s_1)((r_2, s_2) + (r_3, s_3)) &= (r_1, s_1)(r_2 + r_3, s_2 + s_3)\\ &= (r_1(r_2 + r_3), s_1(s_2 + s_3))\\ &= (r_1 r_2 + r_1 r_3, s_1 s_2 + s_1 s_3)\\ &= (r_1 r_2, s_1 s_2) + (r_1 r_3, s_1 s_3)\\ &= (r_1, s_1)(r_2, s_2) + (r_1, s_1)(r_3, s_3)\end{aligned}$$

so that the left distributive law holds in $R \times S$. Similarly for the right distributive law. Therefore, $R \times S$ is a ring. Now,

$$\begin{aligned}R, S \text{ commutative rings} &\iff r_1 r_2 = r_2 r_1, s_1 s_2 = s_2 s_1\\ &\iff (r_1 r_2, s_1 s_2) = (r_2 r_1, s_2 s_1)\\ &\iff (r_1, s_1)(r_2, s_2) = (r_2, s_2)(r_1, s_1)\\ &\iff R \times S \text{ is a commutative ring.}\end{aligned}$$

Let $r \in R, s \in S$. Then

$$\begin{aligned} R, S \text{ contain a } 1 &\iff r1_R = 1_R r = r, s1_S = 1_S s = s \\ &\iff (r1_R, s1_S) = (1_R r, 1_S s) = (r, s) \\ &\iff (r, s)(1_R, 1_S) = (1_R, 1_S)(r, s) = (rs) \\ &\iff R \times S \text{ contains a } 1. \end{aligned}$$

☕

7.3.19 Prove that if $I_1 \subseteq I_2 \subseteq \dots$ are ideals of $R$ then $\bigcup_{n=1}^{\infty} I_n$ is an ideal of $R$.

*Proof.* Since each $I_n$ is a subgroup of $(R, +)$, then $\bigcup_{n=1}^{\infty} I_n$ is nonempty. Let $x, y \in \bigcup_{n=1}^{\infty} I_n$. Then $x \in I_{n_x}, y \in I_{n_y}$ for some $I_{n_x}, I_{n_y} \in \bigcup_{n=1}^{\infty} I_n$. Without loss of generality, assume $n_x \leq n_y$ so that $I_{n_x} \subseteq I_{n_y}$. Then, $x, y \in I_{n_y}$ and so $x - y \in I_{n_y}$. Thus, $x - y \in \bigcup_{n=1}^{\infty} I_n$ so that $\bigcup_{n=1}^{\infty} I_n \leq (R, +)$. Let $r \in R$ and $a \in \bigcup_{n=1}^{\infty} I_n$. Then there exists $n \in \mathbb{N}$ so that $a \in I_n$. Since $I_n$ is an ideal of $R$, then $ar, ra \in I_n$. So $ar, ra \in \bigcup_{n=1}^{\infty} I_n$. ☕

7.3.24 Let $\varphi : R \to S$ be a ring homomorphism.

(a) Prove that if $J$ is an ideal of $S$ then $\varphi^{-1}(J)$ is an ideal of $R$. Apple this to the special case when $R$ is a subring of $S$ and $\varphi$ is the inclusion homomorphism to deduce that if $J$ is an ideal of $S$ then $J \cap R$ is an ideal of $R$.

*Proof.* Let $J$ be an ideal of $S$, $x \in \varphi^{-1}(J)$ and $r \in R$. Then

$$\varphi(xr) = \varphi(x)\varphi(r) \in J$$

because $\varphi(x) \in J, \varphi(r) \in S$ and $J$ is an ideal of $S$. Thus, $xr \in \varphi^{-1}(J)$. Similarly, we get $rx \in \varphi^{-1}(J)$. Thus $\varphi^{-1}(J)$ is an ideal of $R$.

---

Now suppose $R$ is a subring of $S$, $J$ is an ideal of $S$ and $\varphi$ is the inclusion ring homomorphism. Then $\varphi^{-1}(J) = J \cap R$, which is an ideal of $R$ by what was proved above. ☕

(b) Prove that if $\varphi$ is surjective and $I$ is an ideal of $R$ then $\varphi(I)$ is an ideal of $S$. Give and example where this fails if $\varphi$ is not surjective.

*Proof.* Let $y \in \varphi(I)$ and $s \in S$. Since $y \in \varphi(I)$ there exists $x \in I$ so that $\varphi(x) = y$. Since $\varphi$ is surjective, there exists $r \in R$ so that $\varphi(r) = s$. Since $I$ is an ideal of $R$, then $xr, rx \in I$ so that

$$\varphi(xr) = \varphi(x)\varphi(r) = ys \in \varphi(I)$$

and similarly we get $\varphi(rx) \in \varphi(I)$. Therefore, $\varphi(I)$ is an ideal of $S$.

---

Consider the ring homomorphism $\varphi : R \to R[x]$ where $\varphi$ is the inclusion map. This map is not surjective and the ideal $R$ of $R$ has image $\varphi(R) = R$, which is not an ideal of $R[x]$ since $xr \notin R[x]$. ☕

7.1.14 Let $x$ be a nilpotent element of the commutative ring $R$. Let $m \in \mathbb{Z}^+$ be the smallest so that $x^m = 0$.

(a) Prove that $x$ is either zero or a zero divisor.

*Proof.* If $m = 1$, then $0 = x^m = x$. If $m > 1$ then $0 = x^m = x^{m-1} \cdot x$ so that $x$ is a zero divisor.

(b) Prove that $rx$ is nilpotent for all $r \in R$.

*Proof.* Let $r \in R$. Then $(rx)^m = r^m x^m$ since $R$ is commutative and so $(rx)^m = r^m \cdot 0 = 0$.

(c) Prove that $1 + x$ is a unit in $R$.

*Proof.* Notice that

$$(1-(-x))(1-(-x)-(-x)^2-\cdots-(-x)^{m-1}) = 1-(-x)^m = 1-(-1)x^m = 1-0 = 1.$$

(d) Deduce that the sum of a nilpotent element and a unit is a unit.

*Proof.* Let $s$ be a unit in $R$ with $st = ts = 1$. Then $tx$ is nilpotent so that $(1 + tx)$ is a unit. Since the product of units is a unit, then $s(1+tx) = s+stx = s+x$ is a unit.

7.2.6 Let $S$ be a ring with identity $1 \neq 0$. Let $n \in \mathbb{Z}^+$ and let $A$ be an $n \times n$ matrix with entries from $S$ whose $i, j$ entry is $a_{ij}$/ Let $E_{ij}$ be the element of $M_n(S)$ whose $i, j$ entry is 1 and whose other entries are all 0.

(a) Prove that $E_{ij}A$ is the matrix whose $i^{th}$ row equals the $j^{th}$ row of $A$ and all other rows are zero.

*Proof.* Let $E_{ij} = (e_{ij})$, $A = (a_{ij})$, and $(b_{pq}) = E_{ij}A$. Then $(b_{pq}) = \sum_{k=1}^{n} e_{pk}a_{kq}$. The $i^{th}$ row of $(b_{pq})$ consists of elements of the form $e_{ik}a_{kq}$ for each $1 \leq k \leq n$. If $k \neq j$, then $e_{ik} = 0$ so that $b_{pq} = e_{ik}a_{kq} = 0$. When $p \neq i$ the $p^{th}$ row of $(b_{pq})$ contains all zeros. When $k = j$, then $b_{pq} = e_{ik}a_{kq} = e_{ij}a_{jq} = 1 \cdot a_{jq} = a_{jq}$. The collection of all $a_{jq}$ for each $1 \leq q \leq n$ is precisely the $j^{th}$ row of $A$.

(b) Prove that $AE_{ij}$ is the matrix whose $j^{th}$ column equals the $i^{th}$ column of $A$ and all other columns are zero.

*Proof.* Let $E_{ij} = (e_{ij})$, $A = (a_{ij})$, and $(c_{pq}) = AE_{ij}$. Then $(c_{pq}) = \sum_{k=1}^{n} a_{pk}e_{kq}$. The $j^{th}$ column of $(c_{pq})$ consists of elements of the form $a_{pk}e_{kj}$ for each $1 \leq k \leq n$. If $k \neq i$, then $e_{kj} = 0$ so that $c_{pq} = 0$. When $q \neq j$ the $q^{th}$ column of $(c_{pq})$ contains all zeroes. When $k = i$, then $c_{pq} = a_{pi}e_{ij} = a_{pi}$. The collection of all $a_{pi}$ for each $1 \leq p \leq n$ is precisely the $i^{th}$ column of $A$.

(c) Deduce that $E_{pq}AE_{rs}$ is the matrix whose $p, s$ entry is $a_{qr}$ and all other entries are zero.

*Proof.* By parts (a), the $p^{th}$ row of $E_{pq}A$ is the $q^{th}$ row of $A$, and all other entries 0. Then by part (b), $E_{pq}AE_{rs}$ is the matrix whose $s^{th}$ column is the $r^{th}$ column of $E_{pq}A$, which is all zeroes except for the $p^{th}$ row, whose entry is the $q, r$ entry of $A$, and all other entries are zero. Thus the $p, s$ entry of $E_{pq}AE_{rs}$ is $a_{qr}$. ☕

7.2.7 Prove that the center of the ring $M_n(R)$ is the set of scalar matrices. [Use the preceding exercise.]

*Proof.* We need to show $Z(M_n(R)) = \{rI \mid r \in R\}$.
" $\subseteq$ " Suppose $A = (a_{ij}) \in Z(M_N(R))$. By the previous exercise, the $p, t$ entry of $E_{pq}AE_{rs}$ is $a_{qr}$. If $q \neq r$, then $a_{qr} = 0$. Thus, $A$ must be a diagonal matrix. If $q = r$, then the $p, s$ entry of $E_{ps}A$ is $a_{qq}$. But notice that the $p^{th}$ row of $E_{pr}A$ is the $s^{th}$ row of $B$ so that the $p, s$ entry of $E_{ps}A$ is $a_{ss}$. Thus, $a_{qq} = a_{ss}$ for all $q$ and $s$. Hence $A = aI$ for some $a \in R$. So, $Z(M_n(R)) \subseteq \{rI \mid r \in R\}$.
" $\supseteq$ " Let $B \in M_n(R)$, and $A = aI \in \{rI \mid r \in R\}$. Notice that since $R$ is commutative $aB = Ba$ and $aI = Ia$. Then

$$AB = (aI)B = a(IB) = aB = Ba = (BI)a = B(Ia) = BaI = BA.$$

☕

7.3.21 Prove that every (two-sided) ideal of $M_n(R)$ is equal to $M_n(J)$ for some (two-sided) ideal $J$ of $R$. [Use Exercise 6(c)] of section 2 to show first that the set of entries of matrices in an ideal of $M_n(R)$ form an ideal in $R$.]

*Proof.* Let $I$ be an ideal of $M_n(R)$ and define $J = \{a_{ij} \mid (a_{ij}) \in I\}$ be the set containing entries of matrices of $I$. We first show that $J$ is an ideal of $R$ and then show $I = M_n(J)$.

*$J$ is an ideal of $R$:*
Since $I$ is an ideal, then $(0_{ij}) \in I$ so that $0 \in J$. Let $(a_{ij}), (b_{ij}) \in I$ and $E_{pq}, E_{rs} \in M_n(R)$ be defined as in exercise 6 of section 7.2. Since $I$ is an ideal, $E_{pq}(a_{ij})E_{rs}$ and $E_{pq}(a_{ij})E_{rs}$ are in $I$. Notice that by exercise 6, section 7.2, the $p, s$ entry of $E_{pq}(a_{ij})E_{rs}$ is $a_{qr}$. Likewise, the $p, s$ entry of $E_{pq}(b_{ij})E_{rs}$ is $b_{qr}$. Then,

$$E_{pq}(a_{ij})E_{rs} - E_{pq}(b_{ij})E_{rs} \tag{1}$$

and the $p, s$ entry of (1) is $a_{qr} - b_{qr}$ so that $J$ is closed under subtraction. Thus $(J, +) \leq (R, +)$. Now, let $d \in R$, $a_{qr} \in J$. Then, $d\mathcal{I}(a_{ij}) = d(a_{ij}) \in I$ with $q, r$ entry $da_{qr}$ so that $da_{qr} \in J$, and similarly, $a_{qr}d \in J$. Thus $J$ is an ideal of $R$.

*$I = M_n(J)$:*
" $\subseteq$ " Given any matrix in $I$, its entries are elements of $J$ so that $I \subseteq M_n(J)$.
" $\supseteq$ " Let $(a_{ij}) \in M_n(J)$. Then each entry of $(a_{ij})$ is an element of $J$. Since $J$ consists of elements which come from entries of matrices in $I$, we can find matrices $(b_{ij})$ in $I$ with at least one element matching each entry in $(a_{ij})$, then multiply by $E_{pq}$ and $E_{rs}$ on the left and right of the $(b_{ij}$'s as needed to write $(a_{ij})$ as the sum of matrices of the form $E_{pq}(b_{ij})E_{rs}$. Then, each of these lie in $I$, so that their sum also does. Hence, $(a_{ij}) \in I$. ☕

7.3.34 Let $I$ and $J$ be ideals of $R$.

(a) Prove that $I+J$ is the smallest ideal of $R$ containing both $I$ and $J$.

*Proof.* We first show that $I+J$ is an ideal of $R$. Since $0_R \in I, J$ then $0_R = 0_R + 0_R \in I+J$, so $I+J \neq \emptyset$. Let $x_1, x_2 \in I$ and $y_1, y_2 \in J$. Then $x_1+y_1, x_2+y_2 \in I+J$ and

$$(x_1+y_1)-(x_2+y_2) = x_1+y_1-x_1-y_2 = (x_1-x_2)+(y_1-y_2) \in I+J$$

since $x_1 - x_2 \in I$ and $y_1 - y_2 \in J$. So $(I+J,+) \leq (R,+)$. Let $r \in R$. Then

$$r(x_1+y_1) = rx_1 + ry_1 \in I+J \quad \text{and} \quad (x_1+y_1)r = x_1r + y_1r \in I+J$$

since $rx_1, x_1r \in I$ and $ry_1, y_1r \in J$. Hence $I+J$ is an ideal of $R$.

To see that $I+K$ contains $I$ and $K$, notice that since $0_R \in J$, then $I = I + 0_R \subseteq I+J$. Similarly, $0_R \in I$ and so $J = 0_R + J \subseteq I+J$.

Now suppose $K$ is an ideal of $R$ containing both $I$ and $J$. Let $x_1 \in I$ and $y_1 \in J$ and $x_1+y_1 \in I+J$. Since $K$ contains $I$ and $J$, then $x_1, y_1 \in K$. So $x_1+y_1 \in K$ since $K$ is closed under addition. Thus, $I+J \subseteq K$, so that $I+J$ is the smallest ideal of $R$ containing both $I$ and $J$. ☕

(b) Prove that $IJ$ is an ideal contained in $I \cap J$.

*Proof.* Recall that

$$IJ = \left\{ \sum_{k=1}^{n} a_k b_k \mid n \in \mathbb{Z}^+, a_k \in I, b_k \in J, \forall\ 1 \leq k \leq n \right\}.$$

We first show that $IJ$ is an ideal of $R$. Since $0_R \in I$ and $0_R \in J$ then $0_R \cdot 0_R = 0_R \in IJ$. Let $\alpha, \beta \in IJ$, where $\alpha = \sum_{k=1}^{n} a_k b_k$ and $\beta = \sum_{k=1}^{m} c_k d_k$. Note that since $c_k \in I$ , and $I$ is a subgroup, then $-c_k \in I$ for all $1 \leq k \leq m$. So

$$\begin{aligned} \alpha - \beta &= \sum_{k=1}^{n} a_k b_k + \sum_{k=1}^{m} (-c_k) d_k \\ &= a_1 b_1 + \cdots + a_n b_n + (-c_1) d_1 + \cdots + (-c_m) d_m \in IJ \end{aligned}$$

because $\alpha - \beta$ is a finite sum of products of the form $ij$ where $i \in I$, $j \in J$. So $(IJ,+) \leq (R,+)$. Let $r \in R$. Note that since $I$ is an ideal, then $r(a_k) \in I$ for all $1 \leq k \leq n$ and since $J$ is an ideal, then $b_k r \in J$ for all $1 \leq k \leq n$. So

$$r\alpha = \sum_{k=1}^{n} (ra_k) b_k \in IJ \quad \text{and} \quad \alpha r = \sum_{k=1}^{n} a_k (b_k r) \in IJ.$$

Thus, $IJ$ is an ideal of $R$.

Let $\alpha \in IJ$ be defined as before and notice that since $I$ and $J$ are ideals, then $a_k b_k \in I$ and $a_k b_k \in J$ for all $1 \leq k \leq n$. Thus, $\alpha \in I \cap J$. Hence $IJ \subseteq I \cap J$. ☕

7.4.13 (a) Prove that if $P$ is a prime ideal of $S$ then either $\varphi^{-1}(P) = R$ or $\varphi^{-1}(P)$ is a prime ideal of $R$. Apply this to the special case when $R$ is a subring of $S$ and $\varphi$ is the inclusion homomorphism to deduce that if $P$ is a prime ideal of $S$ then $P \cap R$ is either $R$ or a prime ideal of $R$.

*Proof.* We know from a previous exercise that since $P$ is an ideal of $S$, then $\varphi^{-1}(P)$ is an ideal of $R$. If $\varphi^{-1}(P) = R$ then $\varphi^{-1}(P)$ is not a prime ideal (since prime ideals must be proper). If $\varphi^{-1}(P) \neq R$, then let $r_1 r_2 \in \varphi^{-1}(P)$. Then $\varphi(r_1)\varphi(r_2) = \varphi(r_1 r_2) \in P$. Since $P$ is a prime ideal then either $\varphi(r_1)$ or $\varphi(r_2) \in P$. Hence $r_1 \in \varphi^{-1}(P)$ or $r_2 \in \varphi^{-1}(P)$. Therefore, $\varphi^{-1}(P)$ is a prime ideal of $R$.

Suppose $R$ is a subring of $S$ and let $\varphi(r) = r$ for all $r \in R$. Then $\varphi^{-1}(P) = P \cap R$. By what was just shown, either $P \cap R = R$ (which means $P \subseteq R$) or $P \cap R$ is a prime ideal of $R$. ☕

(b) Prove that if $M$ is a maximal ideal of $S$ and $\varphi$ is surjective then $\varphi^{-1}(M)$ is a maximal ideal of $R$. Give and example to show that this need not be the case if $\varphi$ is not surjective.

*Proof.* We know from a previous exercise that since $M$ is an ideal of $S$, then $\varphi^{-1}(M)$ is an ideal of $R$. Notice that $\varphi^{-1}(M) \neq R$. Otherwise, since $\varphi$ is surjective, then $\varphi(R) = S$ and if $\varphi^{-1}(M) = R$, then $S = \varphi(R) = M$, which contradicts the fact that $M \neq S$ (since $M$, being a maximal ideal of $S$, must be a proper ideal of $S$).

Let $M' = \varphi^{-1}(M)$ and consider the quotient $R/M'$. We claim $R/M'$ is a field so that $M'$ is maximal in $R$. Let $\pi : S \to S/M$ be the natural projection homomorphism. Then define

$$\psi = \pi \circ \varphi : R \to S/M.$$

Since both $\varphi$ and $\pi$ are surjective ring homomorphisms, then $\psi$ is a surjective ring homomorphism, i.e., $\psi(R) = S/M$. Then

$$\begin{aligned}
\ker \psi &= \{r \in R \mid \psi(r) = 0_{S/M}\} \\
&= \{r \in R \mid \psi(r) = M\} \\
&= \{r \in R \mid \pi(\varphi(r)) = M\} \\
&= \{r \in R \mid \varphi(r) \in M\} \\
&= \{r \in R \mid r \in \varphi^{-1}(M)\} \\
&= \{r \in R \mid r \in M'\}.
\end{aligned}$$

By the First Isomorphism Theorem,

$$R/M' = R/\ker\psi \cong \psi(R) = S/M.$$

Therefore, $R/M'$ and $S/M$ are isomorphic as rings. Since $M$ is a maximal ideal of $S$, then $S/M$ is a field. We want that $R/M'$ and $S/M$ are isomorphic as fields. Then $R/M'$ is a field, and $M'$ is maximal in $R$. In order to check this, we need that $\psi(1_R) = 1_{S/M} = 1_S + M$. Since $\pi(1_S) = 1_S + M$, we only need to show that $\varphi(1_R) = 1_S$. To that end, notice that since $\varphi$ is surjective, there exists $r \in R$ so that $\varphi(r) = 1_S$. Then

$$1_S = \varphi(r) = \varphi(r \cdot 1_R) = \varphi(r)\varphi(1_R) = 1_S\varphi(1_R) = \varphi(1_R)$$

Let $\varphi : \mathbb{Z} \to \mathbb{Q}$ be the inclusion ring homomorphism. Then $\{0_{\mathbb{Q}}\}$ is maximal in $\mathbb{Q}$. Then $\varphi^{-1}(\{0_{\mathbb{Q}}\}) = 0_{\mathbb{Z}}$, but $\{0_{\mathbb{Z}}\}$ is not a maximal in $\mathbb{Z}$. ☕

7.4.36 Assume $R$ is commutative. Prove that the set of prime ideals in $R$ has a minimal element with respect to inclusion (possibly the zero ideal). [Use Zorn's Lemma.]

*Proof.* Let $\mathcal{S} = \{P \mid P \text{ is a prime ideal of } R\}$. Since $R$ is a ring with $1 \neq 0$, then $R$ contains a proper ideal. Since every proper ideal in a ring with $1 \neq 0$ is contained in a maximal ideal, then $R$ has a maximal ideal. Since maximal ideals are prime ideals, then $\mathcal{S}$ is nonempty. We use as partial order on $\mathcal{S}$ inverse inclusion "$\supseteq$". Let $\mathcal{B}$ be a chain in $\mathcal{S}$. Define

$$U = \bigcap_{J \in \mathcal{B}} J.$$

We claim that $U$ is an upper bound of $\mathcal{B}$. Since $J \supseteq U$ for all $J \in \mathcal{B}$, then if we can show $U \in \mathcal{S}$, then $U$ is an upper bound for $\mathcal{B}$. Then, applying Zorn's Lemma, we conclude that $\mathcal{S}$ has maximal element with respect to reverse inclusion, i.e., $\mathcal{S}$ has a minimal element with respect to inclusion.

<u>$(U, +) \leq (R, +)$</u>: Since $0_R \in J$ for all $J \in \mathcal{B}$, then $0_R \in U$ and so $U \neq \emptyset$. Let $a, b \in U$. Then $a, b, a - b \in J$ for all $J \in \mathcal{B}$ and so $a - b \in U$.

<u>$U$ is an ideal of $R$</u>: Let $r \in R, a \in U$. Then $a, ar, ra \in J$ for all $J \in \mathcal{B}$ and so $ar, ra \in U$.

<u>$U$ is a prime ideal of $R$</u>: Let $ab \in U$. Then $ab \in J$ for all $J \in \mathcal{B}$. By way of contradiction, suppose without loss of generality that $a \notin U$. So, there exists $J_x \in \mathcal{B}$ such that $a \notin J'$. Since $ab \in J'$ and $J'$ is a prime ideal, then $b \in J'$. Then $a \notin K$ for all $K \in \mathcal{B}$ contained in $J'$. For all such $K$, $b \in K$ since each $K$ is a prime ideal. We claim that

$$\bigcap_{K \subseteq J', K \in \mathcal{B}} K = \bigcap_{J \in \mathcal{B}} J = U.$$

Then $b \in U$, and $U$ is a prime ideal of $R$. Since the LHS is an intersection of a subset of ideals in $\mathcal{B}$, then the LHS is contained in the RHS. Conversely, given any point $r \in U$, it is necessarily in all ideals of $\mathcal{B}$. In particular, $r \in K$ for all $K \subseteq J', K \in \mathcal{B}$. Therefore, the equality above holds. ☕

7.4.37 A commutative ring $R$ is called a *local ring* if it has a unique maximal ideal. Prove that if $R$ is a local ring with maximal ideal $M$ then every element of $R - M$ is a unit. Prove conversely that if $R$ is a commutative ring with 1 in which the set of nonunits forms an ideal $M$, then $R$ is a local ring with unique maximal ideal $M$.

*Proof.* Let $R$ is a local ring with unique maximal ideal $M$. Let $u \in R - M$ and consider the principal ideal $(u)$. Notice that $(u) = R$. Otherwise, $(u)$ is a proper ideal of $R$, and thus contained in $M$. Then $u \in M$, which is a contradiction. So, $1 \in (u)$, which means there exists $v \in R$ for which $uv = vu = 1_R$. Hence, $u$ is a unit.

---

Let $R$ be a commutative ring with 1 in which the set of nonunits forms an ideal $M$. Suppose $I$ is an ideal of $R$ containing $M$. If $I$ contains a unit, then $I = R$. If $I$ contains no units, then $I \subseteq M$, and since $M \subseteq I$, then $I = M$. Therefore, $M$ is a maximal ideal.

To show uniqueness of $M$, suppose $N$ is another maximal ideal of $R$. Since $N$ is a proper ideal of $R$, it contains no units and so $N \subseteq M$. If $N \neq M$, then $N$ is not maximal, since it is contained in a proper ideal of $R$. Therefore $N = M$. ☕

Let $R$ be a ring with identity $1 \neq 0$

7.6.1 An element $e$ is called an *idempotent* if $e^2 = e$. Assume $e$ is an idempotent in $R$ and $er = re$ for all $r \in R$. Prove that $Re$ and $R(1-e)$ are two-sided ideals of $R$ and that $R \cong Re \times R(1-e)$. Show that $e$ and $1-e$ are identities for the subrings $Re$ and $R(1-e)$ respectively.

*Proof. Re is a two-sided ideal:*

$$\begin{aligned} 0e = 0 \in Re &\implies Re \neq \emptyset \\ \text{If } re, se \in Re, \text{ then } re - se = (r-s)e \in Re &\implies Re \leq R \\ \text{If } t \in R, \text{ then } tre, ret = rte \in Re &\implies Re \text{ is a two-sided ideal of } R. \end{aligned}$$

*$R(1-e)$ is a two-sided ideal:*

$$\begin{aligned} 0(1-e) = 0 &\in R(1-e) \\ \implies R(1-e) &\neq \emptyset \end{aligned}$$

$$\begin{aligned} \text{If } r(1-e), s(1-e) &\in R(1-e), \\ \text{then } r(1-e) - s(1-e) = (r-s)(1-e) &\in R(1-e) \\ \implies R(1-e) &\leq R \end{aligned}$$

$$\begin{aligned} \text{If } t \in R, \text{ then } tr(1-e) &\in R(1-e) \text{ and} \\ r(1-e)t = r(t-et) = r(t-te) = rt(1-e) &\in R(1-e) \\ \implies R(1-e) &\text{ is a two-sided ideal of } R. \end{aligned}$$

We show that $R \cong Re \times R(1-e)$ as groups, then show that they are isomorphic as rings as well. To that end, observe that $Re \cap R(1-e) = 0$ because

$$\begin{aligned} x \in Re \cap R(1-e) &\implies re = s(1-e) \text{ for some } r, s \in R \\ &\implies re = s - se \\ &\implies re^2 = se - se^2 \\ &\implies re = se - se = 0 \\ &\implies x = 0. \end{aligned}$$

Also observe that for any $r \in R$, we have $r = re + r - re = re + r(1-e)$. Therefore, $R \subseteq Re + R(1-e)$. By the previous two observations, we apply the recognition theorem for direct products of groups (Theorem 9, §5.4, D& F) to conclude that the map

$$\varphi : Re \times R(1-e) \to R \text{ by } \varphi(a,b) = a + b$$

is in isomorphism between groups. We claim that $\varphi$ is in fact a ring isomorphism as well. To that end, let $(r_1e, s_1(1-e))(r_2e, s_2(1-e)) \in Re \times R(1-e)$. Notice that

$(1-e)^2 = 1 - 2e + e = 1 - e$ so that $1-e$ is idempotent.

$$\begin{aligned}\varphi\big((r_1e, s_1(1-e))(r_1e, s_1(1-e))\big) &= \varphi((r_1r_2e, s_1s_2(1-e))) \\ &= r_1r_2e + s_1s_2(1-e) = r_1r_2e^2 + s_1s_2(1-e)^2 \\ &= r_1er_2e + r_1s_2(e-e^2) + r_2s_1(e-e^2) + s_1(1-e)s_2(1-e) \\ &= (r_1e + s_1(1-e))(r_2e + s_2(1-e)) \\ &= \varphi((r_1e, s_1(1-e))) \cdot \varphi((r_1e, s_1(1-e)).\end{aligned}$$

So $R \cong Re \times R(1-e)$ as rings.

*$e$ and $1-e$ are the identities of $Re$ and $R(1-e)$, respectively:*

$$\begin{aligned}\text{If } re \in Re, \text{ then } ere = re^2 = re \text{ and } re^2 = re \\ \implies e \text{ is an identity in } Re.\end{aligned}$$

$$\begin{aligned}\text{If } r(1-e) \in R(1-e), \\ \text{then } [r(1-e)](1-e) = r(1-e)^2 = r(1-e) \\ \text{and } (1-e)r(1-e) = (r-er)(1-e) = r(1-e)^2 = r(1-e) \\ \implies 1-e \text{ is an identity in } R(1-e).\end{aligned}$$

☕

7.6.3 Let $R$ and $S$ be rings with identities. Prove that every ideal of $R \times S$ is of the form $I \times J$ where $I$ is an ideal of $R$ and $J$ is an ideal of $S$.

*Proof.* Let $K$ be an ideal of $R \times S$ and define

$$\begin{aligned}I &= \{a \in R \mid (a,b) \in K \text{ for some } b \in S\} \\ J &= \{b \in R \mid (a,b) \in K \text{ for some } a \in S\}.\end{aligned}$$

We show that $I \times J = K$ and that $I$ and $J$ are ideals of $R$ and $S$ respectively. To that end, we certainly have $K \subseteq I \times K$ by definition of $I$ and $J$. Then, let $a \in I$ and $b \in J$ and $(a,b) \in I \times J$. Therefore, there exists $b' \in S$ and $a' \in R$ so that $(a,b'), (a',b) \in K$. Since $R$ and $S$ have multiplicative identities, $(1_R, 0), (0, 1_S) \in K$. Notice that since $K$ is closed under multiplication and addition,

$$(a,b) = (1_R, 0)(a,b') + (0,1_S)(a',b) \in K.$$

So, $K = I \times J$. To see that $I$ and $J$ are ideals, first notice that by definition of $I$, we have $(I,+) \leq (R,+)$. Let $a_1 \in I$. So there exists $b_1 \in S$ so that $(a_1,b_1) \in K$. Let $r \in R$. Then $(r, 1_S) \in K$. Then since $K$ is closed under multiplication,

$$\begin{aligned}(r,1_S)(a_1,b_1) &= (ra_1, b_1) \in K \\ (a_1,b_1)(r,1_S) &= (a_1r, b_1) \in K\end{aligned}$$

so $ra_1, a_1r \in I$ so that $I$ is an ideal of $R$. Similarly, we get that $J$ is an ideal of $S$.

Now, Let $I$ and $J$ be ideals of $R$ and $S$ respectively. We know that the direct product $I \times J$ is a subgroup of $R \times S$. Let $(a, b) \in I \times J$ and $(r, s) \in R \times S$. Then

$$(a, b)(r, s) = (ar, bs) \in I \times J$$
$$(r, s)(a, b) = (ra, sb) \in I \times J$$

because $I$ and $J$ are ideals themselves. Therefore, $I \times J$ is an ideal of $R \times S$. ☕

7.6.5 Let $n_1, n_2, \ldots, n_k$ be integers which are relatively prime in pairs: $(n_i, n_j) = 1$ for all $i \neq j$.

(a) Show the Chinese Reminder Theorem implies that for any $a_1, \ldots, a_k \in \mathbb{Z}$ there is a solution $x \in \mathbb{Z}$ to the simultaneous congruences

$$x \equiv a_1 \bmod n_1, \quad x \equiv a_2 \bmod n_2, \ \ldots \ , x \equiv a_k \bmod n_k$$

and the solution $x$ is unique mod $n = n_1 n_2 \ldots n_k$.

*Proof.* First, notice that since $\gcd(n_i, n_j) = 1$ for all $i \neq j$. For any fixed $i \neq j$, there exists integers $x, y$ so that $1 = n_i x + n_j y$. Thus, any element of $\mathbb{Z}$ can be written as a multiple of a linear combination of $n_i$ and $n_j$. Therefore, the ideals $(n_i)$ and $(n_j)$ are comaximal in $\mathbb{Z}$. Consider the map

$$\varphi : \mathbb{Z} \to \mathbb{Z}/(n_1) \times \mathbb{Z}/(n_2) \times \cdots \times \mathbb{Z}/(n_k) \quad \text{by} \quad z \mapsto (z + (n_1), z + (n_2), \ldots, z + (n_k)).$$

By the Chinese Remainder Theorem, this map is surjective and

$$\ker(\varphi) = (n_1)(n_2) \ldots (n_k).$$

Then by the First Isomorphism Theorem,

$$\mathbb{Z}/(n_1)(n_2) \ldots (n_k) \cong \mathbb{Z}/(n_1) \times \mathbb{Z}/(n_2) \times \cdots \times \mathbb{Z}/(n_k). \tag{1}$$

Consider the element $\overline{(a_i)} = (a_1 + (n_1), a_2 + (n_2), \ldots, a_k + (n_k))$. Since $\varphi$ is surjective, there exists $x \in \mathbb{Z}$ so that $\varphi(x) = \overline{(a_i)}$. By (1),

$$x + (n_1)(n_2) \ldots (n_k) = (x + (n_1), x + (n_2), \ldots, x + (n_k)).$$

So,

$$\begin{aligned}
(a_1 + (n_1), a_2 + (n_2), \ldots, a_k + (n_k)) &= \overline{(a_i)} \\
&= \varphi(x) \\
&= x + (n_1)(n_2) \ldots (n_k) \\
&= (x + (n_1), x + (n_2), \ldots, x + (n_k)),
\end{aligned}$$

which implies

$$x \equiv a_1 \bmod n_1, \quad x \equiv a_2 \bmod n_2, \ \ldots \ , x \equiv a_k \bmod n_k.$$

The isomorphism in (1) is in particular injective. Therefore, $x$ is unique mod $n = n_1 n_2 \ldots n_k$. ☕

(b) Let $n_i' = n/n_i$ be the quotient of $n$ by $n_i$, which is relatively prime to $n_i$ by assumption. Let $t_i$ be the inverse of $n_i'$ mod $n_i$. Prove that the solution $x$ in (a) is given by

$$x = a_1t_1n_1' + a_2t_2n_2' + \cdots + a_kt_kn_k' \text{ mod } n.$$

Note that the elements $t_i$ can be quickly found by the Euclidean Algorithm as described in Section 2 of the Preliminaries chapter (writing $an_i + bn_i' = (n_i, n_i') = 1$ gives $t_i = b$) and that these then quickly give the solutions to the system of congruences above for any choice of $a_1, a_2, \ldots, a_k$.

*Proof.* We need to show that the definition of $x$ given above is in fact a solution, i.e., that

$$\varphi(x) = \varphi\left(\sum_{i=1}^{k} a_it_in_i' \mod n\right) = \overline{(a_i)}.$$

Notice that by definition, $n_j$ divides $n_i' = n/n_i$ for all $i \neq j$. So the $j$th coordinate of $\varphi(x)$ is

$$a_1t_1n_1' + a_2t_2n_2' + \cdots + a_kt_kn_k' \text{ mod } n + (n_j) = a_j$$

since $t_j$ is the inverse of $n_j'$ mod $n_j$. So $\varphi(x) = \overline{(a_i)}$. ☕

8.1.4 Let $R$ be a Euclidean Domain.

(a) Prove that if $(a, b) = 1$ and $a$ divides $dc$ then $a$ divides $c$. More generally, show that if $a$ divides $bc$ with nonzero $a, b$, then $\dfrac{a}{\gcd(a,b)}$ divides $c$.

*Proof.* Since $(a, b) = 1$ then there exists $x, y \in R$ so that $ax + by = 1$. Since $a$ divides $bc$, there exist $z \in R$ so that $az = bc$. Then

$$\begin{aligned} ax + by &= 1 \\ acx + (bc)y &= c \\ a(cx + yz) &= c \implies a|c. \end{aligned}$$

More generally, if $\gcd(a, b) = d$ and since $a$ divides $bc$, then there exists $x, y, z \in R$ so that $ax + by = d$ and $az = bc$. Moreover, since $d$ divides $a$ there exists $m \in R$ with $dm = a$. Therefore,

$$\begin{aligned} ax + by &= d \\ acx + (bc)y &= dc \\ a(cx + yz) &= dc \\ am(cx + yz) &= (dm)c \\ am(cx + yz) &= ac \\ m(cx + yz) &= c && \text{(Cancellation in } R \text{ since } a \neq 0.) \\ \implies m &= a/d \text{ divides } c. \end{aligned}$$

(b) Consider the Diophantine Equation $ax + by = N$ where $a, b$ and $N$ are integers and $a, b$ are nonzero. Suppose $x_0, y_0$ is a solution: $ax_0 + by_0 = N$. Prove that the full set of solutions to this equation is given by

$$x = x_0 + m\frac{b}{\gcd(a,b)}, \quad y = y_0 - m\frac{a}{\gcd(a,b)}$$

as $m$ ranges over the integers. [If $x, y$ is a solution to $ax + by = N$, show that $a(x - x_0) = b(y_0 - y)$ and use (a).]

*Proof.* Suppose $x, y$ is a solution to $ax + by = N$. Since $x_0, y_0$ is also a solution, then

$$\begin{aligned} ax + by &= ax_0 + by_0 \\ ax - ax_0 &= by_0 - by \\ a(x - x_0) &= b(y_0 - y). \end{aligned}$$

Letting $c = (y_0 - y)$ in part (a), we have $\dfrac{a}{\gcd(a,b)}$ divides $y_0 - y$. Hence, there exists $m \in \mathbb{Z}$ with

$$m\frac{a}{\gcd(a,b)} = y_0 - y \implies y = y_0 - m\frac{a}{\gcd(a,b)}.$$

Then

$$\begin{aligned} ax + by_0 - m\frac{ab}{\gcd(a,b)} &= ax_0 + by_0 \\ ax - m\frac{ab}{\gcd(a,b)} &= ax_0 \\ a\left(x - m\frac{b}{\gcd(a,b)}\right) &= ax_0 \\ x &= x_0 + m\frac{b}{\gcd(a,b)}. \end{aligned}$$

☕

8.1.11 Let $R$ be a commutative ring with 1 and let $a$ and $b$ be nonzero elements of $R$. A *least common multiple* of $a$ and $b$ is an element $e$ of $R$ such that

(i) $a|e$ and $b|e$, and

(ii) if $a|e'$ and $b|e'$ then $e|e'$.

(a) Prove that a least common multiple of $a$ and $b$ (if such exists) is a generator for the unique largest principal ideal contained in $(a) \cap (b)$.

*Proof.* Suppose $e$ is the least common multiple of $a$ and $b$. Then $a$ and $b$ both divide $e$ so that $(e) \subseteq (a) \cap (b)$. Suppose $e' \in R$ and $(e')$ is an ideal for which $(e) \subseteq (e') \subseteq (a) \cap (b)$. Thus $a$ and $b$ each divide $e'$. Since $e$ is the least common multiple of $a$ and $b$, then $e$ divides $e'$, which means $(e') \subseteq (e)$, i.e., $(e) = (e')$ so that $e$ is a generator for the unique largest principal ideal contained in $(a) \cap (b)$. ☕

(b) Deduce that any two nonzero elements in a Euclidean Domain have a least common multiple which is unique up to multiplication by a unit.

*Proof.* Suppose $e$ and $e'$ are two least common multiples of $a$ and $b$. Then $e$ divides $e'$ and $e'$ divides $e$. Then there exists $x, y \in R$ with $ex = e'$ and $e'y = e$. So, $(e'y)x = e \implies yx = 1 \implies x, y$ are units. Therefore, least common multiples of $a$ and $b$ are associate. ☕

(c) Prove that in a Euclidean Domain the least common multiple of $a$ and $b$ is $\dfrac{ab}{\gcd(a,b)}$.

*Proof.* Let $d = \gcd(a,b)$ and $e = \text{lcm}(a,b)$. Notice

$$\frac{ab}{d} = a \cdot \frac{b}{d} \quad \text{and} \quad \frac{ab}{d} = b \cdot \frac{a}{d}$$

so that $a$ and $b$ both divide $\frac{ab}{d}$. So, $e$ divides $\frac{ab}{d}(*)$. Since $a$ divides $e$, then there exists $x \in R$ so that $ax = e$. Then $abx = be$ so that $\frac{ab}{e} \cdot x = b$ and thus $\frac{ab}{e}$ divides $b$. Similarly, $\frac{ab}{e}$ divides $a$. Thus, $\frac{ab}{e}$ divides $d$. Then there exists $z \in R$ so that $\frac{ab}{e} \cdot z = d$. Then $\frac{ab}{d} \cdot z = e$ so that $\frac{ab}{d}$ divides $e$ $(**)$. So by $(*)$ and $(**)$, we have that $e = \frac{ab}{d}$. ☕

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

*Proof.* Note that

$$(x, y) = \{x \cdot g(x, y) + y \cdot h(x, y) \mid g(x, y), h(x, y) \in \mathbb{Q}[x, y]\}.$$

By way of contradiction, suppose $(f(x, y)) = (x, y)$ for some nonzero polynomial $f(x, y) \in \mathbb{Q}[x, y]$. Since $f(x, y) \in (x, y)$, then $f$ has no constant term. If $f$ has any term with the variable $x$, then the polynomial $y \notin (f(x, y))$. Thus, $f$ has no term with the variable $x$. Similarly, if $f$ has any term with the variable $y$, then $x \notin (f(x, y))$. Hence, $f$ has no term with $x$ and no term with $y$, i.e., $f$ is a constant polynomial. But then $f \notin (x, y)$, a contradiction. Thus,$(x, y)$ is not a principle ideal in $\mathbb{Q}[x, y]$. ☕

9.1.7 Let $R$ be a commutative ring with 1. Prove that a polynomial ring in more than one variable over $R$ is not a Principal Ideal Domain.

*Proof.* Let $R$ be a commutative ring with 1 and $n \in \mathbb{Z}^+, n > 1$. Suppose for contradiction that $R[x_1, x_2, \ldots, x_n]$ is a Principal Ideal Domain. Since

$$R[x_1, x_2, \ldots, x_{n-1}][x_n] = R[x_1, x_2, \ldots, x_n]$$

then by Corollary 8, (D&F §8.2), $R[x_1, x_2, \ldots, x_{n-1}]$ is a field, which is a contradiction, since no polynomial ring is a field. ☕

8.2.4 Let $R$ be an integral domain. Prove that if the following two conditions hold then $R$ is a Principle 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 $a_{i+1} \big| a_i$ for all $i$, then there is a positive integer $N$ such that $a_n$ is a unit time $a_N$ for all $n \geq N$.

*Proof.* Let $I$ be a nonzero ideal of $R$ and $S = \{(x) \mid x \in I\}$ be a set ordered by inclusion. Since $0_R \in I$ then the ideal $\{0_r\} \in S$, i.e. $S \neq \emptyset$. Let $\mathcal{C}$ be a chain in $S$. We claim that $\mathcal{C}$ has a maximal element, and thus has an upper bound in $S$.[1] Suppose there exists no maximal element in $\mathcal{C}$. Let $(a_1)$ be an ideal in $\mathcal{C}$. Since $(a_1)$ is not maximal, there exists $(a_2) \in \mathcal{C}$ for which $(a_1) \subsetneq (a_2)$. Similarly, there exists $(a_3) \in \mathcal{C}$ for which $(a_1) \subsetneq (a_2) \subsetneq (a_3)$. Given a chain of ideals in the chain $\mathcal{C}$,

$$(a_1) \subsetneq (a_2) \subsetneq (a_3) \subsetneq \cdots \subsetneq (a_n),$$

since $(a_n)$ is not maximal, there exists $(a_{n+1}) \in \mathcal{C}$ with $(a_n) \subsetneq (a_{n+1})$. Since $\mathcal{C}$ has no maximal element, this chain will continue indefinitely. So, $a_{i+1}|a_i$ for all $i$, and there does not exists an integer $N$ after which $(a_n) = (a_N)$ for all $n \geq N$, which is a contradiction of (ii). Now, we claim that $I$ is in fact a maximal element of $S$. Let $(a)$ be a maximal element of $S$. Then $a \in I$ so that $(a) \subseteq I$. Let $b \in I$. By (i), $\gcd(a, b) = d$ exists and $d = ra + sb$ for some $r, s \in R$. Since $a, b \in I$, then $ra, sb \in I$ and $d = ra + sb \in I$. Since $d|a$ and $d|b$, then $(a) \subseteq (d)$ and $(b) \subseteq (d)$. Since $(a)$ is maximal, then we must have $(a) = (d)$, which means $(b) \subseteq (d) = (a)$ and hence $b \in (a)$. Therefore $I = (a)$, which means $R$ is a Principal Ideal Domain. ☕

8.2.6 Let $R$ be an integral domain and suppose that every *prime* ideal in $R$ is principal. This exercise proves that every ideal of $R$ is principal, i.e., $R$ is a P.I.D.

(a) Assume that the set of ideals of $R$ that are not principal is nonempty and prove that this set has a maximal element under inclusion (which, by hypothesis, is not prime). [Use Zorn's Lemma.]

*Proof.* Let $S = \{I \mid I \subseteq R \text{ is a nonprincipal ideal}\}$ be a set ordered by inclusion. Suppose $S$ is nonempty and let $\mathcal{C}$ be a chain in $S$. Define $J = \bigcup_{C \in \mathcal{C}} C$. Then $J$ is an upper bound for $\mathcal{C}$. It remains to show that $J$ is an element of $S$. Once this is verified, then $S$ contains a maximal element by Zorn's Lemma. Since the union of totally ordered ideals is an ideal, then $J$ is an ideal. Suppose for contradiction that $J$ was principal with $(j) = J$ for some $j \in R$. Since $j \in J$, then $j \in C_j$ for some $C_j \in \mathcal{C}$. So $(j) \subseteq C_j$ and $C_j \subseteq J = (j)$, which means $C_j = (j)$, i.e., $C_j$ is principal, a contradiction. Thus $J \in S$. ☕

[1] Since every element in $\mathcal{C}$ can be compared, a maximal element in $\mathcal{C}$ is an upper bound in $\mathcal{C}$, and in particular an upper bound in $S$.

(b) Let $I$ be an ideal which is maximal with respect to being nonprincipal, and let $a, b \in R$ with $ab \in I$ but $a \notin I$ and $b \notin I$. Let $I_a = (I, a)$ be the ideal generated by $I$ and $a$, let $I_b = (I, b)$ be the ideal generated by $I$ and $b$, and define $J = \{r \in R \mid rI_a \subseteq I\}$. Prove that $I_a = (\alpha)$ and $J = (\beta)$ are principal ideals in $R$ with $I \subsetneq I_b \subseteq J$ and $I_a J = (\alpha\beta) \subseteq I$.

*Proof.*

- $I_a$ is principal.
  If $i \in I$ then $i \in I_a$ and so $I \subseteq I_a$. Since $a \in I_a$ but $a \notin I$, then $I \subsetneq I_a$, which implies $I_a$ is a principal ideal since $I$ is maximal in $R$ with respect to being nonprincipal.
- $J$ is principal.
  Note that $J$ is an ideal. Let $i \in I$. Then $iI_a = I$ which means $i \in J$. Hence $I \subseteq J$. Notice that since $bI = I$ and $ba \in I$, then sums of elements in $bI$ with $ab$ lie in $I$. Hence, $bI_a = I$. So, $b \in J$. Since $b \notin I$, then $I \subsetneq J$, which means $J$ is principal.
- $I \subsetneq I_b \subseteq J$ and $I_a J = (\alpha\beta) \subseteq I$
  Since $b \notin I$ and $b \in I_b$, then $I \subsetneq I_b$. Moreover, since $I \subseteq J$ and $b \in J$, then $I_b \subseteq J$ so that
  $$I \subsetneq I_b \subseteq J.$$
  Letting $I_a = (\alpha)$ and $J = (\beta)$ for $\alpha, \beta \in R$, we have $(\alpha)(\beta) = (\alpha\beta)$, which gives
  $$I_a J = (\alpha\beta) \subseteq I.$$

☕

(c) If $x \in I$ show that $x = s\alpha$ for some $s \in J$. Deduce that $I = I_a J$ is principal, a contradiction, and conclude that $R$ is a P.I.D.

*Proof.* Let $x \in I$. Since $I \subsetneq I_a = (\alpha)$, then $x = s\alpha$ for some $s \in R$. Since

$$sI_a = s(\alpha) = (s\alpha) = (x) \subseteq I,$$

then $s \in J$.So $x \in I_a J$, which means $I \subseteq I_a J$. Therefore, $I = I_a J$ so that $I$ is a principal ideal, which is a contradiction. Therefore, the set $S$ in part (a) is empty, which means $R$ is a P.I.D. ☕

8.3.5 Let $R = \mathbb{Z}[\sqrt{-n}]$ where $n$ is a squarefree integer greater than 3.

(a) Prove that 2, $\sqrt{-n}$, and $1 + \sqrt{-n}$ are irreducibles in $R$.

*Proof.* We use the standard norm of the complex numbers, $N(a + b\sqrt{-n}) = a^2 + b^2 n$, restricted to $R$. So, $N(\alpha)N(\beta) = N(\alpha\beta)$. We claim $N(x) = 1 \iff x$ is a unit. First suppose $x$ is a unit. Then there exists $y \in R$ with $xy = 1$. Then $N(x)N(y) = N(xy) = N(1) = 1$ which implies $N(x)$ and $N(y)$ are both 1. Conversely, suppose $x = a + b\sqrt{-n}$ and $N(x) = 1$. Then $1 = N(x) = a^2 + b^2 n$, and since $n > 3$, we must have $b = 0$ and $1 = a^2$, which means $x = \pm 1$ and thus $x$ is a unit.

- <u>2 is irreducible.</u>
  Suppose $2 = \alpha\beta$. Then $4 = N(2) = N(\alpha)N(\beta)$. If $N(\alpha) = 1$ then $\alpha$ is a unit, and 2 is irreducible. If $N(\alpha) = 4$ then $N(\beta) = 1$ which means $\beta$ is a unit so that 2 is irreducible. Suppose $\alpha = a + b\sqrt{-n}$ and $N(\alpha) = 2$. So $2 = N(\alpha) = a^2 + b^2 n$, which implies $b = 0$ since $n > 3$. Thus, $2 = a^2$, which means $a \notin \mathbb{Z}$, a contradiction. Thus, $N(\alpha) \neq 2$.
- <u>$\sqrt{-n}$ is irreducible.</u>
  Suppose $\sqrt{-n} = \alpha\beta$. Then $N(\alpha)N(\beta) = N(\sqrt{-n}) = n$. Since $n$ is squarefree, $N(\alpha) \neq N(\beta)$. Without loss of generality, suppose $N(\alpha) < N(\beta)$. Let $\alpha = a + b\sqrt{-n}$. Since $n = N(\alpha)N(\beta)$ then

  $$N(\alpha) < \sqrt{n} < N(\beta) \qquad (*)$$

  If this inequality did not hold, then either

  $$N(\alpha) < N(\beta) < \sqrt{n} \quad \text{or} \quad \sqrt{n} < N(\alpha) < N(\beta).$$

  In the former case,

  $$N(\alpha) < \sqrt{n} \ \text{ and } \ N(\beta) < \sqrt{n} \implies N(\alpha)N(\beta) < n,$$

  which is a contradiction. In the latter case,

  $$\sqrt{n} < N(\alpha) \ \text{ and } \ \sqrt{n} < N(\beta) \implies n < N(\alpha)N(\beta),$$

  which again is a contradiction. So, the inequality in $(*)$ holds. Therefore,

  $$a^2 + b^2 n = N(\alpha) < \sqrt{n}.$$

  Since $n > 3$, then $\sqrt{n} < n$. Hence, $b^2 = 0$. Thus $N(\alpha) = a^2$ and so

  $$n = N(\alpha)N(\beta) = a^2 N(\beta).$$

  Since $n$ is squarefree, then $a^2 = 1$, i.e., $N(\alpha) = 1$, which means $\alpha$ is a unit. Therefore, $\sqrt{-n}$ is irreducible.

- $1+\sqrt{-n}$ is irreducible.

  Suppose $1+\sqrt{-n} = \alpha\beta$ and $\alpha = a + b\sqrt{-n}$ and $\beta = c + d\sqrt{-n}$. Then

$$\begin{aligned} 1+n = N(1+\sqrt{-n}) &= N(\alpha)N(\beta) \\ &= (a^2+b^2n)(c^2+d^2n) \\ &= a^2c^2 + (a^2d^2+b^2c^2)n + (b^2d^2)n^2, \end{aligned}$$

  which gives the following equalities: $a^2c^2 = 1$, $a^2d^2 + b^2c^2 = 1$, and $b^2d^2 = 0$. The first equality gives $a, c = \pm 1$ which means $d^2 + b^2 = 1$ and so

$$d^2 = 1 - b^2, \quad b^2(1-b^2) = 0 \implies b = 0 \text{ or } b = \pm 1.$$

  Then, $\alpha = 1 + b\sqrt{-n}$ and so $N(\alpha) = 1^2 + b^2 n \leq 1 + n$. Therefore,

$$1 + n = N(\alpha)N(\beta) \leq (1+n)N(\beta) \implies N(\beta) = 1 \implies \beta \text{ is a unit}$$

  and hence $1+\sqrt{-n}$ is irreducible.

(b) Prove that $R$ is not a U.F.D. Conclude that the quadratic integer ring $\mathcal{O}$ is not a U.F.D. for $D \equiv 2, 3 \mod 4, D < -3$ (so also not Euclidean and not a P.I.D.) [Show that either $\sqrt{-n}$ or $1+\sqrt{-n}$ is not prime.]

*Proof.* We claim $n \in \mathbb{Z}[\sqrt{-n}]$ has two distinct factorizations into irreducibles so that $\mathbb{Z}[\sqrt{n}]$ is not a U.F.D. If $n$ is even then $n = 2k$ for some $k \in \mathbb{Z}$ odd and also $n = (-1)(\sqrt{-n})^2$, and these factorizations are distinct. Now suppose $n$ is odd. Then $n+1$ is even, and $n+1 = (1+\sqrt{-n})(1-\sqrt{-n})$, but also $n + 1 = 2m$ for some $m \in \mathbb{Z}$, which gives two distinct factorizations of $n+1$. Hence $\mathbb{Z}[\sqrt{-n}]$ is not a U.F.D. By definition of the quadratic integer ring,

$$\mathcal{O} := \mathcal{O}_{\mathbb{Q}(\sqrt{D})} = \mathbb{Z}[\omega] = \{a + b\omega \mid a, b \in \mathbb{Z}\},$$

where

$$\omega = \begin{cases} \sqrt{D} & \text{if } D \equiv 2, 3 \mod 4 \\ \frac{1+\sqrt{D}}{2} & \text{if } D \equiv 1 \mod 4. \end{cases}$$

Since $n > 3$, then setting $D = -n$ means $D < -3$. Suppose $D \equiv 2, 3 \mod 4$. Then

$$\mathcal{O} = \mathbb{Z}[\sqrt{D}] = \mathbb{Z}[\sqrt{-n}]$$

which is not a U.F.D. by the above proof.

Let $F$ be a field and $x$ be an indeterminate over $F$.

9.2.1 Let $f(x) \in F[x]$ be a polynomial of degree $n \geq 1$ and let bars denote passage to the quotient $F[x]/(f(x))$. Prove that for each $\overline{g(x)}$ there is a unique polynomial $g_0(x)$ of degree $\leq n-1$ such that $\overline{g(x)} = \overline{g_0(x)}$.

*Proof.* Notice that $\overline{g(x)} = \overline{g_0(x)}$ if and only if $g(x) - g_0(x) \in (f(x))$ if and only if $f(x)$ divides $g(x) - g_0(x)$. Since $F$ is a field, $F[x]$ is a Euclidean Domain where the division algorithm in $F[x]$ yields *unique* $q(x), r(x) \in F[x]$ such that

$$g(x) = q(x)f(x) + r(x) \qquad \text{with} \quad r(x) = 0 \quad \text{or} \quad \deg r(x) < \deg f(x).$$

Define $g_0(x) := r(x)$ so that $g(x) - g_0(x) = q(x)f(x)$ and thus $\overline{g(x)} = \overline{g_0(x)}$ where $\deg g_0(x) < \deg f(x) = n$. ☕

9.2.5 Exhibit *all* the ideals in the ring $F[x]/(p(x))$ where $p(x)$ is a polynomial in $F[x]$.

*Proof.* Since $F$ is a field, then $F[x]$ is a Euclidean Domain. In particular, $F[x]$ is a UFD. Thus if $p(x)$ is an irreducible polynomial, then $p(x)$ is prime polynomial so that $(p(x))$ is a prime ideal. Since $F[x]$ is a Euclidean Domain, then in particular $F[x]$ is a PID so that $(p(x))$ is a maximal ideal since prime ideals in a PID are also maximal ideals. Therefore, $F[x]/(p(x))$ is a field which means its only ideals are $(0_F + p(x))$ and $F[x]/(p(x))$.

Now suppose $p(x)$ is reducible. By the 4th Isomorphism Theorem for rings, there is a bijection between the ideals of $F[x]$ which contain $p(x)$ and the ideals of $F[x]/(p(x))$. Since $F[x]$ is a PID, then all of the ideals which contain $p(x)$ are principal. Moreover, if $p(x) \in (f(x))$ for some $f(x) \in F[x]$, then $f(x)$ divides $p(x)$. So, the ideals of $F[x]/p(x)$ are precisely those of the form $(f(x))/(p(x))$ where $f(x) \in F[x]$ divides $p(x)$ (and of course the zero ideal). ☕

9.4.17 Prove the following version of Eisenstein's Criterion: Let $P$ be a prime ideal in the UFD $R$ and let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ be a polynomial in $R[x]$ with $n \geq 1$. Suppose $a_n \notin P, a_{n-1}, \ldots, a_0 \in P$ and $a_0 \notin P^2$. Prove that $f(x)$ is irreducible in $F[x]$, where $F$ is the quotient field of $R$.

*Proof.* Suppose $f(x)$ is reducible in $F[x]$. Then there exists polynomials

$$c(x) = c_k x^k + \cdots + c_1 x + c_0 \quad \text{and} \quad d(x) = d_\ell x^\ell + \ldots d_1 x + d_0$$

in $F[x]$ with $c_k \neq 0 \neq d_k$ and $1 \leq k, \ell < n$ such that $f(x) = c(x)d(x)$. Now, we compare the coefficients of $p(x) = c(x)d(x)$. Since $a_0 = c_0 d_0$ and $a_0 \in P$, then either $c_0$ or $d_0$ is in $P$. Without loss of generality, suppose $c_0 \in P$. Since $a_0 \notin P^2$, then $d_0 \notin P$. Then

$$a_1 = c_1 d_0 + c_0 d_1.$$

Since $c_0 \in P$ then $c_0 d_1 \in P$. Since $a_1 \in P$, then $c_1 d_0 \in P$. But since $d_0 \notin P$, then $c_1 \in P$ since $P$ is a prime ideal. For $1 \leq i \leq k < n$, we have

$$a_i = c_i d_0 + c_{i-1} d_1 + \cdots + c_0 d_\ell.$$

By induction, $c_{i-1}d_1 + \cdots + c_0 d_\ell \in P$. Since $a_i \in P$, then $c_i d_0 \in P$. But again since $d_0 \notin P$, then $c_i \in P$ since $P$ is a prime ideal. Hence $c_i \in P$ for all $1 \leq i \leq k$. In particular, $c_k \in P$, which implies that $c_k d_\ell \in P$. But $c_k d_\ell = a_n \notin P$, a contradiction. ☕

9.3.4 Let $R = \mathbb{Z} + x\mathbb{Q}[x] \subset \mathbb{Q}[x]$ be the set of polynomials in $x$ with rational coefficients whose constant term is an integer.

(a) Prove that $R$ is an integral domain and its units are $\pm 1$.

*Proof.* Let $f(x), g(x) \in R$ with leading coefficients $a$ and $b$, respectively. Then $f(x)g(x) = 0$ if and only if $ab = 0$ if and only if $a = 0$ or $b = 0$ (since $\mathbb{Q}$) is an integral domain) if and only if $f(x) = 0$ or $g(x) = 0$. Therefore, $R$ is an integral domain.

Moreover, since $R \subset \mathbb{Q}[x]$, then $R^\times \subseteq (\mathbb{Q}[x])^\times = \mathbb{Q}^\times$. However, since the constant polynomials in $R$ are isomorphic to $\mathbb{Z}$, then $R^\times = \mathbb{Z}^\times = \{\pm 1\}$. ☕

(b) Show that the irreducibles in $R$ are $\pm p$ where $p$ is a prime in $\mathbb{Z}$ and the polynomials $f(x)$ that are irreducible in $\mathbb{Q}[x]$ and have constant term $\pm 1$. Prove that these irreducibles are prime in $R$.

*Proof.* If $f(x) = a \in R$ is a constant polynomial, then $a \in \mathbb{Z}$ which means $f(x)$ is irreducible if and only if $a$ is irreducible in $\mathbb{Z}$ if and only if $a$ is prime in $\mathbb{Z}$ (since $\mathbb{Z}$ is a UFD).

Now suppose $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in R$ with $n \geq 1$ and $a_0 \neq 0$. Then we can factor $f(x)$ into the product

$$f(x) = (a_0)\left(\frac{a_n}{a_0}x^n + \frac{a_{n-1}}{a_0}x^{n-1} + \cdots + \frac{a_1}{a_0}x + 1\right).$$

If $a_0 \neq \pm 1$, then $f(x)$ is reducible, since the above factorization exhibits $f(x)$ as the product of two nonunits in $R$. Since $n \geq 1$, then the second factor of $f(x)$ written above is not a unit in $R$. So $f(x)$ is irreducible precisely when $a_0 = \pm 1$ and $f(x)$ is irreducible in $\mathbb{Q}[x]$.

Suppose $f(x)$ is irreducible in $R$. If $f$ is a constant polynomial, then as we stated above, $f(x) = p$ for some prime in $\mathbb{Z}$. Since $\mathbb{Z} \subset R$, then $f(x) = p$ is prime in $R$.

Now suppose $f(x) \in R$ is irreducible and not a constant polynomial, and suppose $f(x) = a(x)b(x)$ for $a(x), b(x) \in R$. Since $\mathbb{Q}$ is a field then $\mathbb{Q}[x]$ is a Euclidean Domain, and in particular $\mathbb{Q}[x]$ is a UFD, so that every irreducible polynomial in $\mathbb{Q}[x]$ is prime in $\mathbb{Q}[x]$. Therefore, since $f(x) \in \mathbb{Q}[x]$ then either $f(x)|a(x)$ or $f(x)|b(x)$. Without loss of generality, suppose $f(x)|a(x)$. So $a(x) = f(x)q(x)$ for some $q(x) \in \mathbb{Q}[x]$. Let $a_0, q_0, f_0$ be the constant terms in $a(x), q(x)$, and $f(x)$, respectively. Since $a(x) \in R$, then $a_0 \in \mathbb{Z}$. Since $f_0 = \pm 1$, then $a_0 = \pm q_0$, i.e., $q_0 \in \mathbb{Z}$. Therefore, $q(x) \in R$ and so $f(x)$ is prime in $R$. ☕

(c) Show that $x$ cannot be written as the product of irreducibles in $R$ (in particular, $x$ is not irreducible) and conclude that $R$ is not a UFD.

*Proof.* Suppose $x = f_1(x)f_2(x)\cdots f_k(x)$ where $f_i(x) \in R$ is irreducible for all $1 \leq i \leq k$. Then

$$1 = \deg(x) = \deg(f_1(x)\cdots f_k(x)) = \deg(f_1(x)) + \cdots + \deg(f_k(x)),$$

which means all but one of the factors of $x$ are constant polynomials. Without loss of generality, suppose $f_1(x)$ is the one nonconstant polynomial in the factorization of $x$. Then $f_1(x) = a_1 x + b$ for some $a_1 \in \mathbb{Q}$, and $b \in \mathbb{Z}$. Since $f_1(x)$ is irreducible in $R$, then and $b = \pm 1$ by part (b). Let $f_i(x) = a_i$ where $a_i \in \mathbb{Z}$ are irreducible for all $2 \leq i \leq k$. Notice that

$$x = (a_1 x \pm 1)a_2 a_3 \cdots a_k = (a_1 a_2 \cdots a_k)x \pm a_2 a_3 \cdots a_k.$$

But since $a_2, a_3, \cdots, a_k$ are irreducible, then their product is nonzero, which means $x$ has a nonzero constant term, a contradiction. Therefore, $R$ is not a UFD, since $x \in R$ cannot be factored into a finite product of irreducibles. ☕

(d) Show that $x$ is not a prime in $R$ and describe the quotient ring $R/(x)$.

*Proof.* Notice that $x$ is not prime in $R$ since it is not irreducible in $R$. Therefore $R/(x)$ is not an integral domain since $(x)$ is not prime. Moreover $R/(x)$ has identity element $f(x) + (x)$ where $f(x)$ is a polynomial with no constant term and an integer coefficient on its $x$ term. **I couldn't figure out how the rest of the cosets looked, so the following is from the online solution manual**: $R/(x) = \{a + bx + (x) \mid a \in \mathbb{Z}, b \in \mathbb{Q}, b \in [0, 1)\}$. ☕

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

*Proof.* Let $p(x) = (x-1)(x-2)\dots(x-n)-1$ and suppose $p(x) = f(x)g(x)$ for some polynomials $f(x), g(x) \in \mathbb{Z}[x]$. Notice that since $p(x)$ has degree $n$, both $f(x)$ and $g(x)$ have degree less than $n$. Without loss of generality suppose $\deg f(x) \leq \deg g(x)$. Notice that for all $1 \leq k \leq n$, we have $f(k)g(k) = -1$. So, $f(k)$ and $g(k)$ are equal to $\pm 1$ for all $1 \leq k \leq n$.

Now, consider the polynomial $p(x) + (f(x))^2$. . Since $\deg f(x) \leq \deg g(x)$, then $\deg f(x) \leq n/2$. Thus $\deg(f(x))^2 \leq n$ and so $\deg(p(x) + (f(x))^2) = n$. Notice that the roots of this polynomial are $k \in \{1, \cdots, n\}$. Then

$$p(x) + (f(x))^2 = (x-1)(x-2)\cdots(x-n) = p(x) + 1,$$

i.e., $(f(x))^2 = 1$ and so $f(x) = \pm 1$. Behold! This means $f(x)$ is a unit in $\mathbb{Z}[x]$ so that $p(x)$ is irreducible.

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

*Proof.* Since $\mathbb{Q}[x, y] = \mathbb{Q}[x][y]$, we consider $y^2 + x^2 - 1$ as a polynomial in the variable $y$ with coefficients in $\mathbb{Q}[x]$. Thus $y^2 + x^2 - 1$ is a monic polynomial with constant term $x^2 - 1$. We claim that $x + 1$ is a prime element in $\mathbb{Q}[x, y]$. Once this is verified, then the ideal $P = (x + 1)$ is a prime ideal containing the constant term $(x-1)^2$ — indeed, $(x-1)^2 = (x+1)(x-1)$ — but the ideal $P^2 = ((x+1)^2)$ does not contain the constant term $(x-1)^2$. Then by Eisenstein's Criterion, $y^2 + x^2 - 1$ is irreducible.

Since $\mathbb{Q}$ is a UFD, then $\mathbb{Q}[x][y]$ is also a UFD, and hence it suffices to show that $x+1$ is irreducible in $\mathbb{Q}[x][y]$. To that end, suppose $x + 1 = f(x, y)g(x, y)$ for some $f(x, y), g(x, y) \in \mathbb{Q}[x][y]$. Then

$$0 = \deg(x + 1) = \deg(f(x, y)) + \deg(g(x, y))$$

which means $\deg(g(x, y)) = \deg(f(x, y)) = 0$, i.e., $f(x, y), g(x, y)$ are constant polynomials. Then $f(x, y), g(x, y)$ are both units since $\mathbb{Q}$ is a field. Hence, $x + 1$ is irreducible.