Solutions to Abstract Algebra (Third Edition) - David S. Dummit & Richard M. Foote

Samy Lahlou

December 3, 2024

Preface

The goal of this document is to share my personal solutions to the exercises in the third edition of Abstract Algebra by David S. Dummit and Richard M. Foote during my reading.
As a disclaimer, the solutions are not unique and there will probably be better or more optimized solutions than mine. Feel free to correct me or ask me anything about the content of this document at the following address : samy.lahloukamal@mcgill.ca

Contents

Preliminaries

0.1 Basics

0.2 Properties of the Integers

0.3 The Integers Modulo n

Part I

GROUP THEORY

Chapter 1

Introduction to Groups

1.1 Basic Axioms and Examples

Chapter 2

Subgroups

2.1 Definition and Examples

2.2 Centralizers and Normalizers, Stabilizers and Kernels

[Pas encore numérisé.]

2.3 Cyclic Groups and Cyclic Subgroups

Exercise 1
Find all subgroups of $Z_{45} = \langle x \rangle$, giving a generator for each. Describe the containments between these subgroups.

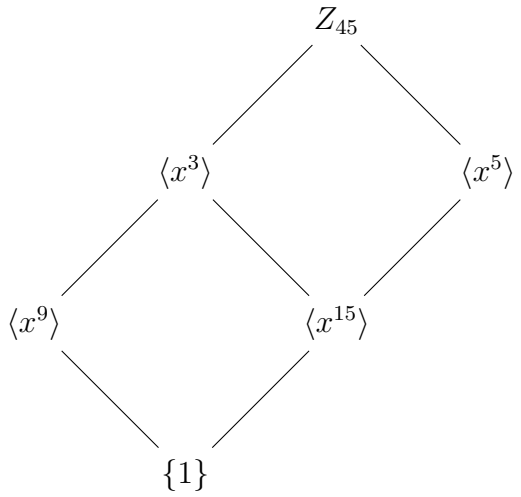
Solution
First, recall that the positive divisors of 45 are the following:

$$1, 3, 5, 9, 15, 45$$

By Theorem 7, the subgroups of Z_{45} are exactly $\langle x^d \rangle$ where d is a divisor. Hence, the subgroups are :

- $\langle x^1 \rangle = Z_{45}$
- $\langle x^3 \rangle = \{1, x^3, x^6, x^9, x^{12}, x^{15}, x^{18}, x^{21}, x^{24}, x^{27}, x^{30}, x^{33}, x^{36}, x^{39}, x^{42}\}$
- $\langle x^5 \rangle = \{1, x^5, x^{10}, x^{15}, x^{20}, x^{25}, x^{30}, x^{35}, x^{40}\}$
- $\langle x^9 \rangle = \{1, x^9, x^{18}, x^{27}, x^{36}\}$
- $\langle x^{15} \rangle = \{1, x^{15}, x^{30}\}$
- $\langle x^{45} \rangle = \{1\}$

We can represent the inclusions between the subgroups with the following diagram:



Exercise 2
If x is an element of the finite group G and $|x| = |G|$, prove that $G = \langle x \rangle$. Give an explicit example to show that this result need not be true if G is an infinite group.

Solution
As proved in exercise 27 of section 1.1, $\langle x \rangle$ is a subgroup of G. Moreover, by Proposition, we must have

$$|\langle x \rangle| = |x| = G$$

Hence, $\langle x \rangle$ is a subgroup of G with the same finite cardinality, so $G = \langle x \rangle$.
This conclusion may not be true if G is infinite. Take for example the groupe $G = \mathbb{Z}$

under addition $2 \in G$. The subgroup generated by 2 is the set of even integers which has the same cardinality as G but obviously $\langle 2 \rangle \neq G$.

Exercise 3
Find all generators of $\mathbb{Z}/48\mathbb{Z}$.

Solution
Using Proposition 6, we know that the generators of $\mathbb{Z}/48\mathbb{Z}$ are exactly the elements $\overline{n}$ such that $(48, n) = 1$ where n is between 1 and 47. By looking at the prime factors of 48 (which are 2 and 3), we find that the generators are exactly

$$\overline{1},\ \overline{5},\ \overline{7},\ \overline{11},\ \overline{13},\ \overline{17},\ \overline{19},\ \overline{23},\ \overline{25},\ \overline{29},\ \overline{31},\ \overline{35},\ \overline{37},\ \overline{41},\ \overline{43},\ \overline{47}$$

Exercise 4
Find all generators for $\mathbb{Z}/202\mathbb{Z}$.

Solution
Using Proposition 6, we know that the generators of $\mathbb{Z}/202\mathbb{Z}$ are exactly the elements $\overline{n}$ such that $(202, n) = 1$ where n is between 1 and 202. By looking at the prime factors of 202 (which are 2 and 101), we can see that the integers n between 2 and 101 that are prime with 202 are odd integers that don't contain 101 as a prime factor. Hence, the generators are simply $\overline{n}$ where n is odd and different than $\overline{101}$.

Exercise 5
Find the number of generators for $\mathbb{Z}/49000\mathbb{Z}$.

Solution
By Proposition 6, we know that $\mathbb{Z}/49000\mathbb{Z}$ has $\varphi(49000)$ generators:

$$\begin{aligned}\varphi(49000) &= \varphi(2^3 \cdot 5^3 \cdot 7^2) \\ &= 2^2(2-1)5^2(5-1)7^1(7-1) \\ &= 16800\end{aligned}$$

Exercise 6
In $\mathbb{Z}/48\mathbb{Z}$, write out all elements of $\langle \overline{a} \rangle$ for every $\overline{a}$. Find all inclusions between subgroups in $\mathbb{Z}/48\mathbb{Z}$.

Solution
First, let's determine all subgroups of $\mathbb{Z}/48\mathbb{Z}$. By Theorem 7, the subgroups are exactly

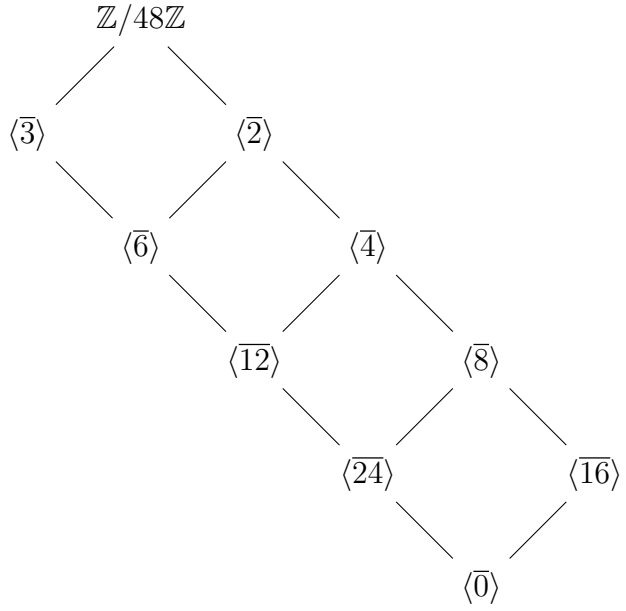
- $\langle \overline{1} \rangle = \mathbb{Z}/48\mathbb{Z}$
- $\langle \overline{2} \rangle = \{\overline{0}, \overline{2}, \overline{4}, \overline{6}, \overline{8}, \overline{10}, \overline{12}, \overline{14}, \overline{16}, \overline{18}, \overline{20}, \overline{22}, \overline{24}, \overline{26}, \overline{28}, \overline{30}, \overline{32}, \overline{34}, \overline{36}, \overline{38}, \overline{40}, \overline{42}, \overline{44}, \overline{46}\}$
- $\langle \overline{3} \rangle = \{\overline{0}, \overline{3}, \overline{6}, \overline{9}, \overline{12}, \overline{15}, \overline{18}, \overline{21}, \overline{24}, \overline{27}, \overline{30}, \overline{33}, \overline{36}, \overline{39}, \overline{42}, \overline{45}\}$
- $\langle \overline{4} \rangle = \{\overline{0}, \overline{4}, \overline{8}, \overline{12}, \overline{16}, \overline{20}, \overline{24}, \overline{28}, \overline{32}, \overline{36}, \overline{40}, \overline{44}\}$
- $\langle \overline{6} \rangle = \{\overline{0}, \overline{6}, \overline{12}, \overline{18}, \overline{24}, \overline{30}, \overline{36}, \overline{42}\}$

- $\langle\overline{8}\rangle = \{\overline{0}, \overline{8}, \overline{16}, \overline{24}, \overline{32}, \overline{40}\}$
- $\langle\overline{12}\rangle = \{\overline{0}, \overline{12}, \overline{24}, \overline{36}\}$
- $\langle\overline{16}\rangle = \{\overline{0}, \overline{16}, \overline{32}\}$
- $\langle\overline{24}\rangle = \{\overline{0}, \overline{24}\}$
- $\langle\overline{48}\rangle = \{\overline{0}\}$

Now, using Theorem 7, we can classify all $\langle\overline{a}\rangle$ since $\langle\overline{a}\rangle = \langle\overline{(48, a)}\rangle$:

- $\langle\overline{1}\rangle = \langle\overline{5}\rangle = \langle\overline{7}\rangle = \langle\overline{11}\rangle = \langle\overline{13}\rangle = \langle\overline{17}\rangle = \langle\overline{19}\rangle = \langle\overline{23}\rangle = \langle\overline{25}\rangle = \langle\overline{29}\rangle = \langle\overline{31}\rangle = \langle\overline{35}\rangle = \langle\overline{37}\rangle = \langle\overline{41}\rangle = \langle\overline{43}\rangle = \langle\overline{47}\rangle = \mathbb{Z}/48\mathbb{Z}$
- $\langle\overline{2}\rangle = \langle\overline{10}\rangle = \langle\overline{14}\rangle = \langle\overline{22}\rangle = \langle\overline{26}\rangle = \langle\overline{34}\rangle = \langle\overline{38}\rangle = \langle\overline{46}\rangle = \{\overline{0}, \overline{2}, \overline{4}, \overline{6}, \overline{8}, \overline{10}, \overline{12}, \overline{14}, \overline{16}, \overline{18}, \overline{20}, \overline{22}, \overline{24}, \overline{26}, \overline{28}, \overline{30}, \overline{32}, \overline{34}, \overline{36}, \overline{38}, \overline{40}, \overline{42}, \overline{44}, \overline{46}\}$
- $\langle\overline{3}\rangle = \langle\overline{9}\rangle = \langle\overline{15}\rangle = \langle\overline{18}\rangle = \langle\overline{21}\rangle = \langle\overline{27}\rangle = \langle\overline{33}\rangle = \langle\overline{39}\rangle = \langle\overline{45}\rangle = \{\overline{0}, \overline{3}, \overline{6}, \overline{9}, \overline{12}, \overline{15}, \overline{18}, \overline{21}, \overline{24}, \overline{27}, \overline{30}, \overline{33}, \overline{36}, \overline{39}, \overline{42}, \overline{45}\}$
- $\langle\overline{4}\rangle = \langle\overline{20}\rangle = \langle\overline{28}\rangle = \langle\overline{44}\rangle = \{\overline{0}, \overline{4}, \overline{8}, \overline{12}, \overline{16}, \overline{20}, \overline{24}, \overline{28}, \overline{32}, \overline{36}, \overline{40}, \overline{44}\}$
- $\langle\overline{6}\rangle = \langle\overline{30}\rangle = \langle\overline{42}\rangle = \{\overline{0}, \overline{6}, \overline{12}, \overline{18}, \overline{24}, \overline{30}, \overline{36}, \overline{42}\}$
- $\langle\overline{8}\rangle = \langle\overline{48}\rangle = \{\overline{0}, \overline{8}, \overline{16}, \overline{24}, \overline{32}, \overline{40}\}$
- $\langle\overline{12}\rangle = \langle\overline{36}\rangle = \{\overline{0}, \overline{12}, \overline{24}, \overline{36}\}$
- $\langle\overline{16}\rangle = \langle\overline{32}\rangle = \{\overline{0}, \overline{16}, \overline{32}\}$
- $\langle\overline{24}\rangle = \{\overline{0}, \overline{24}\}$
- $\langle\overline{0}\rangle = \{\overline{0}\}$

The inclusions between the subgroups can be represented with the following diagram:



Exercise 7
Let $Z_{48} = \langle x \rangle$ and use the isomorphism $\mathbb{Z}/48\mathbb{Z} \cong Z_{48}$ given by $\overline{1} \mapsto x$ to list all subgroups of Z_{48} as computed in the previous exercise.

Solution
By the properties of isomorphisms and cyclic groups, using the previous exercise, the subgroups of Z_{48} are exactly:

$$\langle x \rangle,\ \langle x^2 \rangle,\ \langle x^3 \rangle,\ \langle x^4 \rangle,\ \langle x^6 \rangle,\ \langle x^8 \rangle,\ \langle x^{12} \rangle,\ \langle x^{16} \rangle,\ \langle x^{24} \rangle,\ \langle 1 \rangle$$

Exercise 8
Let $Z_{48} = \langle x \rangle$. For which integers a does the map φ_a defined by $\varphi_a : \overline{1} \mapsto x^a$ extends to an *isomorphism* from $\mathbb{Z}/48\mathbb{Z}$ onto Z_{48}.

Solution
Let's prove that φ_a is an isomorphism iff $(a, 48) = 1$.

Proof. ($\implies$) Suppose $(a, 48) \neq 1$, then x^a is not a generator of Z_{48} by Proposition 6, so $\langle x^a \rangle \subsetneq Z_{48}$. Since $\operatorname{im} \varphi_a = \langle x^a \rangle$, then $\operatorname{im} \varphi_a \neq Z_{48}$. Therefore, φ_a is not an isomorphism since it is not surjective.
($\impliedby$) Suppose $(a, 48) = 1$, then $Z_{48} = \langle x^a \rangle$ by Proposition 66. Therefore, by Theorem 4, the map $\varphi_a : \langle \overline{1} \rangle \to \langle x^a \rangle$ mapping $\overline{1}$ to x^a must extend to an isomorphism. ■

Exercise 9
Let $Z_{36} = \langle x \rangle$. For which integers a does the map ψ_a defined by $\psi_a : \overline{1} \mapsto x^a$ extend to a *well defined homomorphism* from $\mathbb{Z}/48\mathbb{Z}$ into Z_{36}. Can ψ_a ever be a surjective homomorphism?

Solution
First, let's show that ψ_a is a well defined homomorphism iff $3 \mid a$.

Proof. ($\implies$) Suppose that ψ_a is a well defined homomorphism, then

$$\psi_a(\overline{48}) = \psi_a(\overline{0}) = 1$$

But we also have

$$\psi_a(\overline{48}) = \psi_a(48 \cdot \overline{1}) = \big(\psi_a(\overline{1})\big)^{48} = x^{48a}$$

Hence,

$$\begin{aligned} x^{48a} = 1 &= 36 \mid 48a \\ &= 3 \mid 4a \\ &= 3 \mid a \end{aligned}$$

($\impliedby$) Suppose that $3 \mid a$, let's first prove that ψ_a is well defined. Let $\overline{n}, \overline{m} \in$

$\mathbb{Z}/48\mathbb{Z}$ such that $\overline{n} = \overline{m}$, then

$$\begin{aligned}
\overline{n} = \overline{m} &\implies 48 \mid n - m \\
&\implies 3 \cdot 48 \mid a(n-m) \\
&\implies 36 \mid 4 \cdot 36 = 3 \cdot 48 \mid a(n-m) \\
&\implies 36 \mid a(n-m) \\
&\implies x^{a(n-m)} = 1 \\
&\implies x^{an} = x^{am} \\
&\implies \psi_a(\overline{n}) = \psi_a(\overline{m})
\end{aligned}$$

It directly follows that ψ_a is homomorphism since for any $\overline{n}, \overline{m} \in \mathbb{Z}/48\mathbb{Z}$, we get

$$\begin{aligned}
\psi_a(\overline{n} + \overline{m}) &= \psi_a(\overline{n+m}) \\
&= x^{a(n+m)} \\
&= x^{an} x^{am} \\
&= \psi_a(\overline{n})\psi_a(\overline{m})
\end{aligned}$$

■

Let's now prove that ψ_a can never be surjective.

Proof. Suppose that there is an integer a such that ψ_a is surjective, then there is an integer y such that $\psi_a(\overline{y}) = x$, however:

$$\begin{aligned}
\psi_a(\overline{y}) = x &\implies x^{ay} = x \\
&\implies x^{ay-1} = 1 \\
&\implies 36 \mid ay - 1 \\
&\implies 3 \mid ay - 1
\end{aligned}$$

which is impossible because by our previous criterion, $3 \mid a$ which implies $3 \mid ay$. But if 3 divides both ay and $ay - 1$, then 3 must also divide 1, a contradiction. Therefore, ψ_a cannot be surjective.

■

Exercise 10
What is the order of $\overline{30}$ in $\mathbb{Z}/54\mathbb{Z}$? Write out all of the elements and their orders in $\langle\overline{30}\rangle$.

Solution
By Proposition 5

$$|\overline{30}| = \frac{54}{(30, 54)} = \frac{54}{6} = 9$$

The elements in $\langle\overline{30}\rangle$ and their respective order are

- $\overline{0}$ has order 1.
- $\overline{30}$ has order 9.
- $\overline{6}$ has order 9.

- $\overline{36}$ has order 3.
- $\overline{12}$ has order 9.
- $\overline{42}$ has order 9.
- $\overline{18}$ has order 3.
- $\overline{48}$ has order 9.
- $\overline{24}$ has order 9.

We can find the order of each $\overline{30n}$ by thinking of $\langle\overline{30}\rangle$ as $\mathbb{Z}/9\mathbb{Z}$ which gives us the formula

$$|\overline{30n}| = 9/(9, n)$$

Exercise 11
Find all cyclic subgroups of D_8. Find a proper subgroup of D_8 which is not cyclic.

Solution
First, since every cyclic subgroup of D_8 must be of the form $\langle x\rangle$ for a $x \in D_8$ and vice versa, then the cyclic subgroups of D_8 are the following:

- $\langle 1\rangle = \{1\}$
- $\langle r\rangle = \{1, r, r^2, r^3\}$
- $\langle r^2\rangle = \{1, r^2\}$
- $\langle r^3\rangle = \{1, r^3, r^2, r\}$
- $\langle s\rangle = \{1, s\}$
- $\langle sr\rangle = \{1, sr\}$
- $\langle sr^2\rangle = \{1, sr^2\}$
- $\langle sr^3\rangle = \{1, sr^3\}$

However, not every subgroup of D_8 is cyclic. As an example, $\{1, r^2, sr, sr^3\}$ is a subgroup but every element has order 2 so it cannot be cyclic.

Exercise 12
Prove that the following groups are *not* cyclic:

(a) $Z_2 \times Z_2$

(b) $Z_2 \times \mathbb{Z}$

(c) $\mathbb{Z} \times \mathbb{Z}$

Solution
Here, we denote by x the generator of Z_2 : $Z_2 = \langle x\rangle$.

(a) $Z_2 \times Z_2$ cannot be cyclic because it has order 4 and all of its elements have order 2, so $\langle x \rangle \neq Z_2 \times Z_2$ for all $x \in Z_2 \times Z_2$.

(b) Suppose that $Z_2 \times \mathbb{Z}$ is cyclic, then there is a double (a, b) with $a \in Z_2$ and $b \in \mathbb{Z}$ such that

$$\langle (a, b) \rangle = Z_2 \times \mathbb{Z}$$

Since every element in $Z_2 \times \mathbb{Z}$ is a power of (a, b), then there is an integer n such that

$$\begin{aligned} (a, b)^n = (xa^{-1}, b) &\implies (a^n, bn) = (xa^{-1}, b) \\ &\implies a^n = xa^{-1} \text{ and } bn = b \\ &\implies a^n = xa^{-1} \text{ and } n = 1 \\ &\implies a = xa^{-1} \\ &\implies x = a^2 = 1 \end{aligned}$$

A contradiction since $Z_2 = \{1, x\}$ and $x \neq 1$. Therefore, $Z_2 \times \mathbb{Z}$ cannot be cyclic.

(c) Suppose that $\mathbb{Z} \times \mathbb{Z}$ is cyclic, then there is a double (a, b) with $a, b \in \mathbb{Z}$ such that

$$\langle (a, b) \rangle = \mathbb{Z} \times \mathbb{Z}$$

Since every element in $\mathbb{Z} \times \mathbb{Z}$ is a multiple of (a, b), then there is an integer n such that

$$\begin{aligned} n \cdot (a, b) = (a + 1, b) &\implies (na, nb) = (a + 1, b) \\ &\implies na = a + 1 \text{ and } bn = b \\ &\implies na = a + 1 \text{ and } n = 1 \\ &\implies a = a + 1 \\ &\implies 1 = 0 \end{aligned}$$

which is a contradiction. Therefore, $\mathbb{Z} \times \mathbb{Z}$ cannot be cyclic.

Exercise 13
Prove that the following pairs of groups are *not* isomorphic:

(a) $\mathbb{Z} \times Z_2$ and $\mathbb{Z}$

(b) $\mathbb{Q} \times Z_2$ and $\mathbb{Q}$

Solution
First, let's show that isomorphisms preserve cyclicity:

Proof. Let A and B be isomorphic groups such that A is cyclic. Let $\varphi : A \to B$ be an isomorphism and a a generator of A. Define $b := \varphi(a) \in B$ and let's show that B is generated by b.
Let $y \in B$, then there is an $x \in A$ such that $\varphi(x) = y$. But $x \in \langle a \rangle$ so there is an integer n such that $x = a^n$. Thus,

$$y = \varphi(x) = \varphi(a^n) = (\varphi(a))^n = b^n$$

Hence, $y \in \langle b \rangle$ which proves that B is generated by b. Therefore, B is cyclic as well. ■

Now that we proved this statement, let's prove part (a) and (b). Moreover, as for the previous exercise, denote by x the generator of Z_2.

(a) Suppose that $\mathbb{Z} \times Z_2$ and $\mathbb{Z}$ are isomorphic, since $\mathbb{Z}$ is cyclic, then by our lemma, $\mathbb{Z} \times Z_2$ must be cyclic as well. Moreover, by exercise 11 of Section 1.6, $\mathbb{Z} \times Z_2$ and $Z_2 \times \mathbb{Z}$ are isomorphic so our lemma implies that $Z_2 \times \mathbb{Z}$ is cyclic. This contradicts part (b) of the previous question. Therefore, $\mathbb{Z} \times Z_2$ and $\mathbb{Z}$ cannot be isomorphic.

(b) Suppose there is an isomorphism $\varphi : \mathbb{Q} \times Z_2 \to \mathbb{Q}$, then since φ maps the identity in $\mathbb{Q} \times Z_2$ to the identity in $\mathbb{Q}$, we get

$$\varphi(0, 1) = 0$$

Hence,

$$\begin{aligned} & \varphi(0, x) + \varphi(0, x) = \varphi(0 + 0, x^2) \\ \implies \quad & 2\varphi(0, x) = \varphi(0, 1) = 0 \\ \implies \quad & \varphi(0, x) = 0 \end{aligned}$$

which contradicts the fact that φ is injective.
Therefore, $\mathbb{Q} \times Z_2$ and $\mathbb{Q}$ are not isomorphic.

Exercise 14
Let $\sigma = (1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ 10\ 11\ 12)$. For each of the following integers a, compute σ^a: $a = 13,\ 65,\ 626,\ 1195, -6, -81, -570$ and -1211.

Solution
Since σ is a 12-cycle, then $\sigma^a = \sigma^r$ where is the residue of a modulo 12. Therefore,

- $\sigma^{13} = \sigma^1 = (1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ 10\ 11\ 12)$
- $\sigma^{65} = \sigma^5 = (1\ 6\ 11\ 4\ 9\ 2\ 7\ 12\ 5\ 10\ 3\ 8)$
- $\sigma^{626} = \sigma^2 = (1\ 3\ 5\ 7\ 9\ 11)(2\ 4\ 6\ 8\ 10\ 12)$
- $\sigma^{1195} = \sigma^7 = (1\ 8\ 3\ 10\ 5\ 12\ 7\ 2\ 9\ 4\ 11\ 6)$
- $\sigma^{-6} = \sigma^6 = (1\ 7)(2\ 8)(3\ 9)(4\ 10)(5\ 11)(6\ 12)$
- $\sigma^{-81} = \sigma^3 = (1\ 4\ 7\ 10)(2\ 5\ 8\ 11)(3\ 6\ 9\ 12)$
- $\sigma^{-570} = \sigma^6 = (1\ 7)(2\ 8)(3\ 9)(4\ 10)(5\ 11)(6\ 12)$
- $\sigma^{-1211} = \sigma^1 = (1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ 10\ 11\ 12)$

Exercise 15
Prove that $\mathbb{Q} \times \mathbb{Q}$ is not cyclic.

Solution
First, by contradiction, suppose that $\mathbb{Q} \times \mathbb{Q}$ is cyclic, then there exist a pair (a, b) in $\mathbb{Q} \times \mathbb{Q}$ such that $\langle (a, b) \rangle = \mathbb{Q} \times \mathbb{Q}$. obviously, a must be nonzero because if

$a = 0$, it would be impossible to generate any element of $\mathbb{Q} \times \mathbb{Q}$ with a nonzero first coordinate. For the same reason, b must be nonzero as well.
Hence, there must be an integer n such that $n \cdot (a, b) = (2a, 3b)$ which would imply

$$\begin{aligned} n \cdot (a, b) = (2a, 3b) &\implies (na, nb) = (2a, 3b) \\ &\implies na = 2a \text{ and } nb = 3b \\ &\implies n = 2 \text{ and } n = 3 \end{aligned}$$

a contradiction. Therefore, $\mathbb{Q} \times \mathbb{Q}$ is not cyclic.

Exercise 16
Assume $|x| = n$ and $|y| = m$. Suppose that x and y commute:$xy = yx$. Prove that $|xy|$ divides the least common multiple of m and n. Need this be true if x and y do *not* commute? Give an example of commuting elements x,y such that the order of xy is not equal to the least common multiple of $|x|$ and $|y|$.

Solution
First, let's prove the claim made at the beginning of the exercise.

Proof. Assume $|x| = n$ and $|y| = m$ and suppose that x and y commute. Then, by Exercise 24 of Section 1.1:

$$(xy)^{\text{lcm}(n,m)} = x^{\text{lcm}(n,m)} y^{\text{lcm}(n,m)} = 1$$

Thus, by Proposition 3, $|xy| \mid \text{lcm}(n, m)$.

■

In Exercise 6 of Section 2.1, we proved that for a non-abelian group, the set of elements of finite order may not be a subgroup because there exist two elements f and g of order 2 in $S_{\mathbb{Z}}$ such that $|f \circ g| = \infty$. Hence, this same example works as a counterexample in our situation.
As an example of commuting x and y such that $|xy| \neq \text{lcm}(|x|, |y|)$, we can take $x = y = r^2 \in D_8$ since $\text{lcm}(|x|, |y|) = \text{lcm}(2, 2) = 2$ but $|xy| = |r^4| = |1| = 1$.

Exercise 17
Find a presentation for Z_n with one generator.

Solution
Since $Z_n = \langle x \rangle$ and every property of Z_n can be deduced from the fact that $x^n = 1$, then

$$Z_n = \langle x \mid x^n = 1 \rangle$$

Exercise 18
Show that if H is any group and h is an element of H with $h^n = 1$, then there is a unique homomorphism from $Z_n = \langle x \rangle$ to H such that $x \mapsto h$.

Solution
Since h has order n, then $\langle h \rangle$ is a cyclic group of order h which implies that there is a isomorphism $\varphi : Z_n \to \langle h \rangle$ such that $x^k \mapsto h^k$ for all integers k. In particular, for $k = 1$, $\varphi(x) = h$. If we change the codomain to H, then φ becomes a homomorphism.

Let $\psi : Z_n \to H$ be a homomorphism satisfying $x \mapsto h$, then by Exercise 1 of Section 1.6, $x^k \mapsto h^k$ for all integers k. Hence, $\varphi = \psi$ so such homomorphism is unique.

Exercise 19
Show that if H is any group and h is an element of H, then there is a unique homomorphism from $\mathbb{Z}$ to H such that $1 \mapsto h$.

Solution
First, define the map $\varphi : \mathbb{Z} \to H$ by $k \mapsto h^k$. Obviously, by properties of exponents and by definition, φ is a homomorphism from $\mathbb{Z}$ to H such that $1 \mapsto h$.
To show the uniqueness of such homomorphism, let $\psi : \mathbb{Z} \to H$ be a homomorphism mapping 1 to h, then by Exercise 1 of Section 1.6, $\psi(k) = h^k = \varphi(k)$ for all integers k. Hence, $\varphi = \psi$. Therefore, such homomorphism is unique.

Exercise 20
Let p be a prime and let n be a positive integer. Show that if x is an element of the group G such that $x^{p^n} = 1$ then $|x| = p^m$ for some $m \leq n$.

Solution
If $x^{p^n} = 1$, then $|x|$ must divide p^n by Proposition 3. However, the only divisors of p^n are p^m where $m \leq n$ so $|x|$ must be equal to p^m for a $m \leq n$.

Exercise 21
Let p be an odd prime and let n be a positive integer. Use the Binomial Theorem to show that $(1+p)^{p^{n-1}} \equiv 1 \pmod{p^n}$ but $(1+p)^{p^{n-2}} \not\equiv 1 \pmod{p^n}$. Deduce that $1+p$ is an element of order p^{n-1} in the multiplicative group $(\mathbb{Z}/p^n\mathbb{Z})^\times$.

Solution
The goal of this exercise is to show that $1+p$ is an element of order p^{n-1} is the multiplicative group $(\mathbb{Z}/p^n\mathbb{Z})^\times$. To prove it, we will prove separatly the cases where $n = 1$ and $n \geq 2$. When $n = 1$, then $1 + p \equiv 1 \pmod{p}$ is simply the identity which means it has order $1 = p^{n-1}$.
Consider now the case where $n \geq 2$. Let k be a positive integer and consider $m_k \in \mathbb{N}$ the number of times p divdes $k!$ and notice that $k! = p^{m_k}t$ where t is relatively prime with p. With a little bit of number theory and by counting the number of times the successive powers of p divide $k!$, we can prove that

$$m_k = \sum_{i=1}^{\infty} \left\lfloor \frac{k}{p^i} \right\rfloor$$

Let's prove that $k - m_k \geq 1$ when $k \geq 1$ and $k - m_k \geq 2$ when $k \geq 2$. To do so, notice that for $k \geq 4$, we get

$$\begin{aligned} 4 \leq k &\implies k \leq 2k - 4 \\ &\implies \frac{k}{2} \leq k - 2 \end{aligned}$$

which implies

$$\begin{aligned} m_k &= \sum_{i=1}^{\infty} \left\lfloor \frac{k}{p^i} \right\rfloor \\ &\leq \sum_{i=1}^{\infty} \frac{k}{p^i} \\ &= \frac{k}{p} \sum_{i=0}^{\infty} \frac{1}{p^i} \\ &= \frac{k}{p} \frac{1}{1-\frac{1}{p}} \\ &= \frac{k}{p-1} \\ &\leq \frac{k}{2} \\ &\leq k-2 \end{aligned}$$

By rearranging the terms, we get

$$k - m_k \geq 2$$

For $k = 2$, notice that m_k is always 0 since p is odd, thus : $k - m_k = 2 - 0 \geq 2$ Similarly, when $k = 3$, $m_k = 1$ only if $p = 3$ and 0 otherwise. Thus, $m_k \leq 1$ which implies $k - m_k \geq 3 - 1 = 2$. Therefore, the inequality holds for all $k \geq 2$.
From this, $k - m_k \geq 1$ obviously holds for all $k \geq 2$. When $k = 1$, then m_k is always 0 so $k - m_k = 1 - 0 \geq 1$. Therefore, for all $k \geq 1$:

$$k - m_k \geq 1$$

Using these inequalities, we get that for $k \geq 2$

$$\begin{aligned} k - m_k \geq 2 &\implies n - 2 - m_k + k \geq n \\ &\implies p^n \mid p^{n-2-m_k+k} \\ &\implies p^{n-2-m_k+k} \equiv 0 \pmod{p^n} \end{aligned}$$

and similarly for $k \geq 1$:

$$p^{n-1-m_k+k} \equiv 0 \pmod{p^n}$$

Consider the binomial coefficients $\binom{p^{n-1}}{k}$ and $\binom{p^{n-2}}{k}$ and rewrite them as

$$\begin{aligned} \binom{p^{n-1}}{k} &= \frac{(p^{n-1})!}{(p^{n-1}-k)! \cdot k!} \\ &= \frac{p^{n-1}(p^{n-1}-1)\dots(p^{n-1}-k+1)}{p^{m_k} t} \end{aligned}$$

and

$$\begin{aligned} \binom{p^{n-2}}{k} &= \frac{(p^{n-2})!}{(p^{n-2}-k)! \cdot k!} \\ &= \frac{p^{n-2}(p^{n-2}-1)\dots(p^{n-2}-k+1)}{p^{m_k} t} \end{aligned}$$

Since both are integers, then using the fact that t is relatively prime with p and Gauss' Lemma, we get

$$\begin{aligned} t \mid p^{m_k} t &\implies t \mid p^{n-1}(p^{n-1}-1)\dots(p^{n-1}-k+1) \\ &\implies t \mid (p^{n-1}-1)\dots(p^{n-1}-k+1) \\ &\implies \frac{(p^{n-2}-1)\dots(p^{n-2}-k+1)}{t} \in \mathbb{Z} \\ &\implies \binom{p^{n-1}}{k} = p^{n-1-m_k} c_k, \qquad c_k \in \mathbb{Z} \end{aligned}$$

and similarly:

$$\binom{p^{n-2}}{k} = p^{n-2-m_k} d_k, \qquad d_k \in \mathbb{Z}$$

Therefore, using the congruences we developed before, for $k \geq 1$:

$$\binom{p^{n-1}}{k} p^k \equiv p^{n-1-m_k+k} c_k \equiv 0 \pmod{p^n}$$

and for $k \geq 2$:

$$\binom{p^{n-2}}{k} p^k \equiv p^{n-2-m_k+k} d_k \equiv 0 \pmod{p^n}$$

Therefore, using the Binomial Theorem:

$$\begin{aligned} (1+p)^{p^{n-1}} &\equiv \sum_{k=0}^{p^{n-1}} \binom{p^{n-1}}{k} p^k \\ &\equiv \binom{p^{n-1}}{0} p^0 + \sum_{k=1}^{p^{n-1}} \binom{p^{n-1}}{k} p^k \\ &\equiv 1 + \sum_{k=1}^{n-1} 0 \\ &\equiv 1 \pmod{p^n} \end{aligned}$$

and

$$\begin{aligned} (1+p)^{p^{n-2}} &\equiv \sum_{k=0}^{p^{n-2}} \binom{p^{n-2}}{k} p^k \\ &\equiv \binom{p^{n-2}}{0} p^0 + \binom{p^{n-2}}{1} p^1 + \sum_{k=2}^{p^{n-2}} \binom{p^{n-2}}{k} p^k \\ &\equiv 1 + p^{n-1} + \sum_{k=2}^{p^{n-2}} 0 \\ &\equiv 1 + p^{n-1} \\ &\not\equiv 1 \pmod{p^n} \end{aligned}$$

Using Exercise 20, this implies that $|1+p| = p^m$ where $m \leq n-1$. However, if $m \leq n-2$, then it easily follows that $(1+p)^{p^{n-2}} \equiv 1$, a contradiction. Therefore,

$1+p$ has order $n-1$ in the multiplicative group $(\mathbb{Z}/p^n\mathbb{Z})^\times$.

Exercise 22
Let n be an integer ≥ 3. Use the Binomial Theorem to show that $(1+2^2)^{2^{n-2}} \equiv 1 \pmod{2^n}$ but $(1+2^2)^{2^{n-3}} \not\equiv 1 \pmod{2^n}$. Deduce that 5 is an element of order 2^{n-2} in the multiplicative group $(\mathbb{Z}/2^n\mathbb{Z})^\times$.

Solution
In a similar way as for the previous exercise , the goal here is to prove that 5 has order 2^{n-2}. The solution to this exercise will be similar to the previous one. First, let k be a positive integer and define m_k as the power of 2 in the prime decomposition of $k!$. From this, we get that

$$k! = 2^{m_k}t, \qquad (p,t) = 1$$

Let's prove show that

$$2k - 2 - m_k \geq 0 \tag{1}$$

and also

$$2k - 3 - m_k \geq 0 \tag{2}$$

if $k \geq 2$. To do so, first notice that for $k \geq 3$, it's easy to see that $k \leq 2k-3$. Moreover, since we can express m_k as an inifinite series in the following way, then

$$\begin{aligned} m_k &= \sum_{i=1}^{\infty} \left\lfloor \frac{k}{2^i} \right\rfloor \\ &\leq \sum_{i=1}^{\infty} \frac{k}{2^i} \\ &= k \sum_{i=1}^{\infty} \frac{1}{2^i} \\ &= k \\ &\leq 2k-3 \end{aligned}$$

Thus, by rearring the terms, we get inequality (2) for $k \geq 3$. If $k = 2$, then $m_k = 1$ which implies

$$2k - 3 - m_k = 4 - 3 - 1 \geq 0$$

Therefore, inequality (2) holds for all $k \geq 2$ as we wanted. It directly follows that inequality (1) holds for $k \geq 2$ as well. When $k = 1$, $m_k = 0$ so

$$2k - 2 - m_k = 2 - 1 - 0 \geq 0$$

Therefore, inequality (1) holds for all positive integers k.
From this, it is easy to see that for each inequality, adding n on both sides implies the following congruences:

$$2^{n-2-m_k+2k} \equiv 0 \pmod{2^n} \tag{3}$$

and when $k \geq 2$:

$$2^{n-3-m_k+2k} \equiv 0 \pmod{2^n} \tag{4}$$

Consider now the binomial coefficients $\binom{2^{n-2}}{k}$ and $\binom{2^{n-3}}{k}$. As in the previous exercise, using Gauss' Lemma and by the fact that these coefficients are integers, for $k \leq 2^{n-2}$ we have:

$$\begin{aligned}
\binom{2^{n-2}}{k} = \frac{2^{n-2}(2^{n-2}-1)\dots(2^{n-2}-k+1)}{k!} &\implies k! \mid 2^{n-2}(2^{n-2}-1)\dots(2^{n-2}-k+1) \\
&\implies t \mid 2^{n-2-m_k}(2^{n-2}-1)\dots(2^{n-2}-k+1) \\
&\implies t \mid (2^{n-2}-1)\dots(2^{n-2}-k+1) \\
&\implies \frac{(2^{n-2}-1)\dots(2^{n-2}-k+1)}{t} \in \mathbb{Z} \\
&\implies \binom{2^{n-2}}{k} = 2^{n-2-m_k}c_k, \quad c_k \in \mathbb{Z} \\
&\implies \binom{2^{n-2}}{k}2^{2k} = 2^{n-2-m_k+2k}c_k \\
&\implies \binom{2^{n-2}}{k}2^{2k} \equiv 0 \pmod{2^n}
\end{aligned}$$

Similarly, for $k \in [\![2, 2^{n-3}]\!]$, with the exact same methods, we can show that

$$\binom{2^{n-3}}{k}2^{2k} \equiv 0 \pmod{2^n}$$

Therefore, using the Binomial Theorem:

$$\begin{aligned}
(1+2^2)^{2^{n-2}} &\equiv \sum_{k=0}^{2^{n-2}} \binom{2^{n-2}}{k}2^{2k} \\
&\equiv \binom{2^{n-2}}{0}2^0 + \sum_{k=1}^{2^{n-2}} \binom{2^{n-2}}{k}2^{2k} \\
&\equiv 1 + \sum_{k=1}^{2^{n-2}} 0 \\
&\equiv 1 \pmod{2^n}
\end{aligned}$$

and

$$\begin{aligned}
(1+2^2)^{2^{n-3}} &\equiv \sum_{k=0}^{2^{n-3}} \binom{2^{n-3}}{k}2^{2k} \\
&\equiv \binom{2^{n-3}}{0}2^0 + \binom{2^{n-3}}{1}2^2 + \sum_{k=2}^{2^{n-3}} \binom{2^{n-3}}{k}2^{2k} \\
&\equiv 1 + 2^{n-1} + \sum_{k=1}^{2^{n-3}} 0 \\
&\equiv 1 + 2^{n-1} \\
&\not\equiv 1 \pmod{2^n}
\end{aligned}$$

As in the previous exercise, by Exercise 20, this implies that 5 has order 2^m for some $m \leq n-2$ but we also know that m cannot be less than $n-3$. Therefore, 5 is an

element of order 2^{n-2} in $(\mathbb{Z}/2^n\mathbb{Z})^\times$.

Exercise 23
Show that $(\mathbb{Z}/2^n\mathbb{Z})^\times$ is not cyclic for any $n \geq 3$. [Find two distinct subgroups of order 2.]

Solution
Let $n \geq 3$, then by the previous exercise, 5 has order 2^{n-2}. Therefore, $5^{2^{n-3}}$ must have order 2. Moreover, we also showed that $5^{2^{n-3}} \equiv 1 + 2^{n-1} \pmod{2^n}$ so $1 + 2^{n-1}$ has order 2 in $(\mathbb{Z}/2^n\mathbb{Z})^\times$. Let's prove that $1 + 2^{n-1} \not\equiv -1$. By contradiction:

$$\begin{aligned} 1 + 2^{n-1} \equiv -1 &\implies 2^{n-1} \equiv -2 \pmod{2^n} \\ &\implies 2^n \equiv -4 \\ &\implies 4 \equiv 0 \\ &\implies 2^n \mid 2^2 \\ &\implies n \leq 2 \end{aligned}$$

A contradiction since $n \geq 3$. Thus, $1 + 2^{n-1}$ and -1 are distinct elements of order 2, it follows that $\langle 1 + 2^{n-1} \rangle$ and $\langle -1 \rangle$ are distinct subgroups of order 2. Suppose by contradiction that $(\mathbb{Z}/2^n\mathbb{Z})^\times$ is cyclic, then it has a unique subgroup of order 2 (by Theorem 7.(3)). Therefore, it is not cylic.

Exercise 24
Let G be a finite group and let $x \in G$.

(a) Prove that if $g \in N_G(\langle x \rangle)$ then $gxg^{-1} = x^a$ for some $a \in \mathbb{Z}$.

(b) Prove conversely that if $gxg^{-1} = x^a$ for some $a \in \mathbb{Z}$ then $g \in N_G(\langle x \rangle)$. [Show first that $gx^kg^{-1} = (gxg^{-1})^k = x^{ak}$ for any integer k, so that $g\langle x \rangle g^{-1} \leq \langle x \rangle$. If x has order n, show the elements gx^ig^{-1}, $i = 0, 1, \ldots, n-1$ are distinct, so that $|g\langle x \rangle g^{-1}| = |x| = n$ and conclude that $g\langle x \rangle g^{-1} = x$.]

Note that this cuts down some of the work in computing normalizers of cyclic subgroups since one does not have to check $ghg^{-1} \in \langle x \rangle$ for every $h \in \langle x \rangle$.

Solution

(a) If $g \in N_G(\langle x \rangle)$, then by definition, $g\langle x \rangle g^{-1} = \langle x \rangle$. Since $gxg^{-1} \in g\langle x \rangle g^{-1}$, the equality between the sets tells us that $gxg^{-1} \in \langle x \rangle$. Therefore, $gxg^{-1} = x^a$ for some $a \in \mathbb{Z}$.

(b) Suppose now that $gxg^{-1} = x^a$ for some $a \in \mathbb{Z}$. Let's prove by induction on $k \geq 0$ that

$$gx^kg^{-1} = x^{ak}$$

holds. When $k = 0$, we get

$$gx^0g^{-1} = gg^{-1} = 1 = x^0 = x^{a0}$$

Suppose now that $gx^jg^{-1} = x^{aj}$ for some $j \geq 0$, then

$$\begin{aligned} gx^jg^{-1} = x^{aj} &\implies (gx^jg^{-1})(gxg^{-1}) = (x^{aj})(x^a) \\ &\implies gx^jxg^{-1} = x^{aj}x^a \\ &\implies gx^{j+1}g^{-1} = x^{aj+a} \\ &\implies gx^{j+1}g^{-1} = x^{a(j+1)} \end{aligned}$$

Thus, by induction, it holds for all $k \geq 0$.
Let $k < 0$, then $-k \geq 0$ which implies

$$\begin{aligned} gx^{-k}g^{-1} = x^{-ak} &\implies (gx^{-k}g^{-1})^{-1} = (x^{-ak})^{-1} \\ &\implies (g^{-1})^{-1}(x^{-k})^{-1}(g)^{-1} = x^{-(-ak)} \\ &\implies gx^kg^{-1} = x^{ak} \end{aligned}$$

Therefore, it holds for all integers k. It directly follows that $g\langle x\rangle g^{-1} \leq \langle x\rangle$ since the conjugate of any element in $\langle x\rangle$ is in $\langle x\rangle$ as well.
By finiteness of G, $\langle x\rangle$ must be finite as well. Let n be the order of $\langle x\rangle$, then for $i, j \in [\![0, n-1]\!]$, $x^i = x^j$ if and only if $i = j$. Let $i, j \in [\![0, n-1]\!]$, then

$$\begin{aligned} gx^ig^{-1} = gx^jg^{-1} &\implies g^{-1}(gx^ig^{-1})g = g^{-1}(gx^jg^{-1})g \\ &\implies x^i = x^j \\ &\implies i = j \end{aligned}$$

Thus, $g\langle x\rangle g^{-1}$ has at least n distinct elements. But $g\langle x\rangle g^{-1} \leq \langle x\rangle$ so $g\langle x\rangle g^{-1}$ has at most n distinct elements. Hence, $g\langle x\rangle g^{-1}$ is equal to $\langle x\rangle$ since it is a subgroup of the same cardinality of n. Therefore, $g \in N_G(\langle x\rangle)$.

Exercise 25
Let G be a cyclic group of order n and let k be an integer relatively prime to n. Prove that the map $x \mapsto x^k$ is surjective. Use Lagrange's Theorem (Exercise 19, Section 1.7) to prove the same is true for any finite group of order n. (For such k each element has a k^{th} root in G. It follows from Cauchy's Theorem in Section 3.2 that if k is not relatively prime to the order of G then the map $x \mapsto x^k$ is not surjective.)

Solution
First, suppose that G is cyclic and let g be a generator. By Porposition 6, $G = \langle g^k\rangle$ since $(k, n) = 1$. Hence, for all $y \in G$, there is an integer a such that $y = (g^k)^a = (g^a)^k$. If we let $x = g^a$, then y is the image of x under the map $x \mapsto x^k$. Therefore, the map is surjective.
Let's now prove it for the general case when G may not be cyclic. Let $y \in G$ and let's show that there is a $x \in G$ such that $y = x^k$. Obviously, y is in the cyclic subgroup $\langle y\rangle$ which has an order m that divides n (by Lagrange's Theorem). Hence, we must have $(k, m) = 1$ as well. Applying what we proved above for the cyclic group $\langle y\rangle$ tells us that the map $x \mapsto x^k$ with domain $\langle y\rangle$ is onto $\langle y\rangle$. Therefore, there is a $x \in \langle y\rangle \subseteq G$ such that $y = x^k$ which proves that the map is surjective.

Exercise 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 σ_a is an automorphism of Z_n if and only if a and n are relatively prime (automorphisms were introduced in Exercise 20, Section 1.6).

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

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

(d) Prove that $\sigma_a \circ \sigma_b = \sigma_{ab}$. Deduce that the map $\overline{a} \mapsto \sigma_a$ 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 $\varphi(n)$).

Solution
In this exercise, denote by z a generator of Z_n.

(a) Suppose that a and n are relatively prime, then by Proposition 6, $Z_n = \langle z^a \rangle$. From this, since σ_a is simply the map $z^b \mapsto (z^a)^b$, then by Theorem 4, it is an isomorphism from $\langle z \rangle$ to $\langle z^a \rangle$. Therefore, σ_a is an automorphism of Z_n.
Suppose now that a and n have a common divisor $d > 1$, then $n = kd$ and $a = k'd$ for some integers $1 < k < n$ and $1 < k' < a$. From this, define $x = z^k$ and notice that $x \neq 1$ by properties of k. However, we have

$$\sigma_a(x) = (z^k)^a = z^{kk'd} = (z^n)^{k'} = 1$$

Hence, $\sigma_a(x) = \sigma_a(1)$ so it is not injective. Therefore, σ_a cannot be an automorphism of Z_n.

(b) Suppose that $\sigma_a = \sigma_b$. Since $|z| = n$, then

$$\begin{aligned} \sigma_a(z) = \sigma_b(z) &\implies z^a = z^b \\ &\implies z^{a-b} = 1 \\ &\implies n \mid a - b \\ &\implies a \equiv b \pmod{n} \end{aligned}$$

Suppose now that $a \equiv b \pmod{n}$ and let $x \in G$. Since G has order n, then $|x| \mid n$. Moreover, $n \mid a - b$ which implies that $|x| \mid a - b$. Therefore,

$$\begin{aligned} x^{a-b} = 1 &\implies x^a = x^b \\ &\implies \sigma_a(x) = \sigma_b(x) \end{aligned}$$

Since it holds for all x in G, then the functions are equal.

(c) Let φ be an automorphism of Z_n and let a be an integer that satisfies

$$\varphi(z) = z^a$$

To prove that $\varphi = \sigma_a$, let $x \in G$ and $b \in \mathbb{Z}$ such that $x = z^b$, then

$$\begin{aligned}\varphi(x) &= \varphi(z^b)\\ &= (\varphi(z))^b\\ &= (z^a)^b\\ &= (z^b)^a\\ &= \sigma_a(x)\end{aligned}$$

Therefore, $\varphi = \sigma_a$ so any automorphism can be written in this form.

(d) Let a and b be integers and $x \in G$:

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

Thus, $\sigma_a \circ \sigma_b = \sigma_{ab}$.
Define now the function $\sigma : (\mathbb{Z}/n\mathbb{Z})^\times \to \mathrm{Aut}(Z_n)$ defined by

$$\sigma(\overline{a}) = \sigma_a$$

Notice that the fact that σ is well-defined and injective is exactly what we proved in part (b) of this exercise. The fact that σ is a group homomorphism is exactly what we proved at the beginning of part (d). The fact that σ is surjective and onto $\mathrm{Aut}(Z_n)$ is exactly what we proved in part (a) and (c). Therefore, σ is an isomorphism of $(\mathbb{Z}/n\mathbb{Z})^\times$ to $\mathrm{Aut}(Z_n)$.

2.4 Subgroups Generated by a Subset of a Group

Exercise 1
Prove that if H is a subgroup of G then $H = \langle H \rangle$.

Solution
First, since H is a subgroup of G that contains H, then $\langle H \rangle \subseteq H$. Moreover, since $\langle H \rangle$ is the intersections of all the subgroups of G that contains H, then $H \subseteq \langle H \rangle$. Therefore, $H = \langle H \rangle$.

Exercise 2
Prove that if A is a subset of B then $\langle A \rangle \subseteq \langle B \rangle$. Give an example where $A \subseteq B$ with $A \neq B$ but $\langle A \rangle \neq \langle B \rangle$.

Solution
Since $B \subseteq \langle B \rangle$, then $A \subseteq \langle B \rangle$. Hence, $\langle B \rangle$ is a subgroup of G that contains A. Therefore, $\langle A \rangle \subseteq \langle B \rangle$.
As an example, take $A = G \setminus \{1\}$ and $B = G$. Obviously, A is a proper subset of B. However, the only subgroup of G that contains A is G itself. Therefore,

$$\langle A \rangle = G = \langle B \rangle$$

Exercise 3
Prove that if H is an abelian subgroup of a group G then $\langle H, Z(G) \rangle$ is abelian. Give an explicit example of an abelian subgroup H of a group G such that $\langle H, C_G(H) \rangle$ is not abelian.

Solution
First, to show that $\langle H, Z(G) \rangle$ is abelian, let's use the fact that $\langle H, Z(G) \rangle = \overline{H \cup Z(G)}$. Let $a, b \in \langle H, Z(G) \rangle$, then $a = a_1^{e_1} \dots a_n^{e_n}$ and $b = b_1^{f_1} \dots b_m^{f_m}$ for some $a_i, b_j \in H \cup Z(G)$, $e_i, f_j \in \mathbb{Z}$ and $n, m \in \mathbb{N}$. But notice here that every element commute with every other element, hence we can rearrange the terms in any way we like without changing the value of the expression:

$$\begin{aligned} ab &= a_1^{e_1} \dots a_n^{e_n} b_1^{f_1} \dots b_m^{f_m} \\ &= b_1^{f_1} \dots b_m^{f_m} a_1^{e_1} \dots a_n^{e_n} \\ &= ba \end{aligned}$$

Therefore, $\langle H, Z(G) \rangle$ is abelian.
As an example of a group G, and an abelian subgroup H such that $\langle H, C_G(H) \rangle$ is not abelian, let $G = S_5$ and $H = \{1, (1\ 2)\}$. Obviously, H is abelian and $H \subseteq C_{S_5}(H)$, thus:

$$\langle H, C_{S_5}(H) \rangle = \langle H \cup C_{S_5}(H) \rangle = \langle C_{S_5}(H) \rangle = C_{S_5}(H)$$

Notice that both (3 4) and (4 5) are in $C_{S_5}(H)$ but

$$(3\ 4)(4\ 5) = (3\ 4\ 5)$$

$$(4\ 5)(3\ 4) = (3\ 5\ 4)$$

Therefore, $C_{S_5}(H) = \langle H, C_{S_5}(H)\rangle$ is not abelian.

Exercise 4
Prove that if H is a subgroup of G then H is generated by the set $H - \{1\}$.

Solution
Let's show that H is the smallest subgroup of G that contains $H - \{1\}$. Obviously, H is a subgroup of G that contains $H - \{1\}$. To prove that it is the smallest, let S be a subgroup of G that contains $H - \{1\}$, since it is a subgroup, then $1 \in S$. Thus, $H = (H - \{1\}) \cup \{1\} \subseteq S$. Hence, H is the smallest subgroup of G that contains $H - \{1\}$. By uniqueness, it implies that $H = \langle H - \{1\}\rangle$. Therefore, H is generated by $H - \{1\}$.

Exercise 5
Prove that the subgroup generated by any two distinct elements of order 2 in S_3 is all of S_3.

Solution
A set of two elements in S_3 of order 2 must be of the form $\{(a\ b), (b\ c)\}$ where a, b, c are distinct integers between 1 and 3 since the elements of order 2 are exactly

$$(1\ 2) \quad (1\ 3) \quad (2\ 3)$$

We know that $\langle (a\ b), (b\ c)\rangle \leq S_3$ so its order must divide 6 by Lagrange's Theorem. We also know that $\langle (a\ b), (b\ c)\rangle$ contains 1, $(a\ b)$, $(b\ c)$ and $(a\ b\ c)$ since

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

and $\langle (a\ b), (b\ c)\rangle$ is closed under multiplication. Thus, its order is greater than 4. Since the order of $\langle (a\ b), (b\ c)\rangle$ also divides 6, then it must be 6. Therefore, $\langle (a\ b), (b\ c)\rangle$ is a subgroup of order 6 of S_3 so $\langle (a\ b), (b\ c)\rangle$ must be all of S_3.

Exercise 6
Prove that the subgroup of S_4 generated by (1 2) and (1 2)(3 4) is a noncylic group of order 4.

Solution
Let $S = \{(1\ 2), (1\ 2)(3\ 4)\}$ and $H = \{1, (1\ 2), (3\ 4), (1\ 2)(3\ 4)\}$ and let's show that $H = \langle S\rangle$. Obviously, H is a subgroup of S_4 that contains S so $\langle S\rangle \subseteq H$. Moreover, for any subgroup A of G that contains S, A must contain the identity, S and the product of (1 2) and (1 2)(3 4) which is simply (3 4). Hence, $H \subseteq A$ which implies that $H \subseteq \langle S\rangle$. Therefore, $\langle S\rangle$ is a subgroup of order which is noncyclic since no element has order 4 (every element has order 1 or 2).

Exercise 7
Prove that the subgroup of S_4 generated by (1 2) and (1 3)(2 4) is isomorphic to the dihedral group of order 8.

Solution
First, recall that D_8 has the following presentation:

$$D_8 = \langle a, b \mid a^2 = b^2 = (ab)^n = 1 \rangle$$

Notice that

$$\begin{aligned}
&(1\ 2)^2 = 1 \\
&((1\ 3)(2\ 4))^2 = (1\ 3)^2(2\ 4)^2 = 1 \\
&((1\ 2)(1\ 3)(2\ 4))^4 = (1\ 3\ 2\ 4)^4 = 1
\end{aligned}$$

Hence, $(1\ 2)$ and $(1\ 3)(2\ 4)$ satisfy the same relations as a and b. Thus, there is a surjective homomorphism from $\langle (1\ 2), (1\ 3)(2\ 4) \rangle$ to D_8 that maps $(1\ 2)$ to a and $(1\ 3)(2\ 4)$ to b. By surjectivity, we know that the order of $\langle (1\ 2), (1\ 3)(2\ 4) \rangle$ is greater than 8. Moreover, using the homomorphism, we can easily find the subgroup $\{1, (1\ 3\ 2\ 4), (1\ 2)(3\ 4), (1\ 4\ 2\ 3), (1\ 2), (1\ 3)(2\ 4), (3\ 4), (1\ 4)(2\ 3)\}$ of S_4 of order 8 that contains our two generators. Thus, the order of $\langle (1\ 2), (1\ 3)(2\ 4) \rangle$ is less than 8. Therefore, $\langle (1\ 2), (1\ 3)(2\ 4) \rangle$ has order 8 which implies that the surjective homomorphism between $\langle (1\ 2), (1\ 3)(2\ 4) \rangle$ onto D_8 is actually an isomorphism.

Exercise 8
Prove that $S_4 = \langle (1\ 2\ 3\ 4), (1\ 2\ 4\ 3) \rangle$.

Solution
I don't know yet if there is an easier method but it is sufficient to prove that at least 13 elements of S_4 can be written as a product of $(1\ 2\ 3\ 4), (1\ 2\ 4\ 3)$. To make the notation easier, let $a = (1\ 2\ 3\ 4)$ and $b = (1\ 2\ 4\ 3)$. By Lagrange's Theorem, this would mean that $\langle (1\ 2\ 3\ 4), (1\ 2\ 4\ 3) \rangle$ has order that divides 24 while having an order biggr than 13.

- $1 = aa^{-1}$
- $(1\ 4)(2\ 3) = b^2$
- $(1\ 2\ 4) = baba$
- $(1\ 2\ 3\ 4) = a$
- $(1\ 3\ 4\ 2) = b^3$
- $(1\ 3)(2\ 4) = a^2$
- $(1\ 3\ 2) = ab$
- $(2\ 4) = ab^2$
- $(1\ 4\ 3\ 2) = a^3$
- $(1\ 2\ 3) = abab$
- $(1\ 2\ 4\ 3) = b$
- $(1\ 4\ 2) = ba$
- $(1\ 3) = a^3b^2$

Therefore, $\langle (1\ 2\ 3\ 4), (1\ 2\ 4\ 3) \rangle = S_4$.

Exercise 9
Prove that $SL_2(\mathbb{F}_3)$ is the subgroup of $GL_2(\mathbb{F}_3)$ generated by $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, and $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$.
[Recall from Exercise 9 of Section 1 that $SL_2(\mathbb{F}_3)$ is the subgroup of matrices of determinant 1. You may assume this subgroup has order 24 - this will be an exercise in Section 3.2.]

Solution
As for the previous exercise, let's show that at least 13 elements of $SL_2(\mathbb{F}_3)$ can be

written as a product of $\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}$, and $\begin{pmatrix}1 & 0\\ 1 & 1\end{pmatrix}$. To make it easier, let

$$A = \begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix} \qquad B = \begin{pmatrix}1 & 0\\ 1 & 1\end{pmatrix}$$

Then we get

- $I_3 = AA^{-1}$
- $\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix} = A$
- $\begin{pmatrix}1 & 2\\ 0 & 1\end{pmatrix} = A^2$
- $\begin{pmatrix}1 & 0\\ 1 & 1\end{pmatrix} = B$
- $\begin{pmatrix}1 & 0\\ 2 & 1\end{pmatrix} = B^2$
- $\begin{pmatrix}1 & 1\\ 1 & 2\end{pmatrix} = BA$
- $\begin{pmatrix}1 & 2\\ 1 & 0\end{pmatrix} = BA^2$
- $\begin{pmatrix}1 & 1\\ 2 & 0\end{pmatrix} = B^2A$
- $\begin{pmatrix}1 & 2\\ 2 & 2\end{pmatrix} = B^2A^2$
- $\begin{pmatrix}2 & 1\\ 1 & 1\end{pmatrix} = AB$
- $\begin{pmatrix}0 & 2\\ 1 & 1\end{pmatrix} = A^2B$
- $\begin{pmatrix}0 & 1\\ 2 & 1\end{pmatrix} = AB^2$
- $\begin{pmatrix}2 & 2\\ 2 & 1\end{pmatrix} = A^2B^2$

Therefore, $\left\langle \begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}, \begin{pmatrix}1 & 0\\ 1 & 1\end{pmatrix} \right\rangle = SL_2(\mathbb{F}_3)$.

Exercise 10
Prove that subgroup of $SL_2(\mathbb{F}_3)$ generated by $\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}$ and $\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}$ is isomorphic to the quaternion group of order 8. [Use a presentation of Q_8.]

Solution
Recall that Q_8 has the following presentation:

$$Q_8 = \langle i, j \mid i^4 = 1,\ i^2 = j^2\ ij = ji^{-1} \rangle$$

To make things easier, define

$$A = \begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix} \qquad B = \begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}$$

Notice that

$$A^2 = \begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix}$$

and

$$B^2 = \begin{pmatrix}2 & 0\\ 0 & 2\end{pmatrix} = \begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix}$$

Thus, $A^2 = B^2$, and obviously: $A^4 = I_3$. Moreover,

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

which implies

$$AB = BA^{-1}$$

Therefore, A and B satisfy the same relations as i and j in the group presentation of Q_8 so the function mapping A to i and B to j has a unique extension into a surjective homomorphism. Moreover, we can easily from this correspondence find a subgroup of $SL_2(\mathbb{F}_3)$ or order 8 that contains $\langle A, B\rangle$ so $\langle A, B\rangle$ has order 8 which means that the surjective homomorphism must be an isomorphism. Therefore, $\langle A, B\rangle$ is isomorphic to Q_8.

Exercise 11
Show that $SL_2(\mathbb{F}_3)$ and S_4 are two nonisomorphic groups of order 24.

Solution
By contradiction, suppose that they are indeed isomorphic, then by the previous exercise, it must be that S_4 has a subgroup isomorphic to Q_8. Thus, S_4 has elements σ and τ of order 2 that satisfiy

$$\sigma^2 = \tau^2 \qquad \sigma\tau\sigma = \tau$$

The only elements of order 4 in S_4 are 4-cycles. Hence, the first condition on σ and τ implies that

$$\sigma = (1\ a\ b\ c) \qquad \tau = (1\ c\ b\ a)$$

for some distinct $a, b, c \in \{2, 3, 4\}$. The second condition tells us that

$$\begin{aligned}\tau &= \sigma\tau\sigma \\ &= (1\ a\ b\ c)(1\ c\ b\ a)(1\ a\ b\ c) \\ &= (1\ a\ b\ c) \\ &= \sigma\end{aligned}$$

A contradiction since that σ and τ are distinct. Therefore, $SL_2(\mathbb{F}_3)$ and S_4 are two nonisomorphic groups of order 24.

Exercise 12
Prove that the subgroup of upper triangular matrices in $GL_3(\mathbb{F}_2)$ is isomorphic to the dihedral group of order 8 (cf. Exercise 16, Section 1) [First find the order of this subgroup.]

Solution
First, to determine the number of upper triangular matrices in $GL_3(\mathbb{F}_2)$, recall that each such matrice has the following form:

$$\begin{pmatrix} * & * & * \\ 0 & * & * \\ 0 & 0 & * \end{pmatrix}$$

However, if the element of coordinate 1,1 is 0, then the matrix cannot be invertible since one of its column vectors are not linearly independant which is impossible since we are considering elements of $GL_3(\mathbb{F}_2)$. Thus, the first entry of the first line is 1. Similarly, the last entry of the last line is 1 as well. Thus, every such matrix has the following form:

$$\begin{pmatrix} 1 & * & * \\ 0 & * & * \\ 0 & 0 & 1 \end{pmatrix}$$

If the entry 2,2 in the middle of the matrix is 0, then the entry above it cannot be 0 since it would give a zero vector as a column vector of the matrix. But it cannot be one since the first two column vectors of the matrix would be equal (which would make the matrix non invertible). Therefore, the entry in the middle must be 1:

$$\begin{pmatrix} 1 & * & * \\ 0 & 1 & * \\ 0 & 0 & 1 \end{pmatrix}$$

Now, for such matrices, it is easy to see that whatever way we choose to fill in the *, it will be an upper triangular matrix in $GL_3(\mathbb{F}_2)$. Therefore, there are 8 upper triangular matrices in $GL_3(\mathbb{F}_2)$. To make the notation easier, let's denote each matrix as a vector in $\mathbb{F}_2^3$ in the following way:

$$(a, b, c) \sim \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}$$

Hence, the multiplication is defined as follows:

$$(a, b, c) \cdot (e, f, g) = (a + e, f + ag + b, c + g)$$

To show that our group is isomorphic to D_8, let's find two matrices that act as r and s in our group. Let $S = (1, 0, 0)$ and $R = (1, 1, 1)$ be two matrices. Notice that

$$S^2 = (1, 0, 0) \cdot (1, 0, 0) = (2, 0, 0) = (0, 0, 0) = I_3$$

and

$$\begin{aligned} R^2 &= (1, 1, 1) \cdot (1, 1, 1) = (2, 3, 2) = (0, 1, 0) \\ R^3 &= (1, 1, 1) \cdot (0, 1, 0) = (1, 2, 1) = (1, 0, 1) \\ R^4 &= (1, 1, 1) \cdot (1, 0, 1) = (2, 2, 2) = (0, 0, 0) = I_3 \end{aligned}$$

and finaly:

$$\begin{aligned} RSR &= (1, 1, 1) \cdot (1, 0, 0) \cdot (1, 1, 1) \\ &= (1, 1, 1) \cdot (0, 0, 1) \\ &= (1, 0, 0) \\ &= S \end{aligned}$$

which implies that $SR = R^{-1}S$. Therefore, the function that maps R to $r \in D_8$ and S to $s \in D_8$ can be extended to a homomorphism. Notice that we already showed that R and S generate 5 of the 8 matrices we are considering in this exercise. By Lagrange's Theorem, this implies that R and S are generators of the group of upper traingular matrices in $GL_3(\mathbb{F}_2)$. Hence, the homomorphism is surjective. Since both groups have order 8, then it must be an isomorphism. Therefore, the group of upper traingular matrices in $GL_3(\mathbb{F}_2)$ is isomorphic to D_8.

Exercise 13
Prove that the multiplicative group of positive rational numbers is generated by the

set $\{\frac{1}{p} \mid p \text{ is a prime}\}$.

Solution
To make the notation easier, let $P = \{\frac{1}{p} \mid p \text{ is a prime}\}$. By proposition 9, we know that $\langle P \rangle = \overline{P}$ so it is sufficient to prove that $\mathbb{Q}_{>0} = \overline{P}$. Obviously, $\overline{P} \subseteq \mathbb{Q}_{>0}$. Let $q \in \mathbb{Q}_{>0}$, then $q = a/b$ where a and b are positive integers. There are four possible cases, if both a and b are equal to 1, then $q \in \overline{P}$ follows from the fact that $\overline{P}$ is a subgroup. If $a = 1$ and b is an integer bigger than 2, then b can be written as a product of prime numbers:

$$b = p_1^{a_1} \dots p_n^{a_n}$$

Thus,

$$q = \frac{1}{b} = \frac{1}{p_1^{a_1} \dots p_n^{a_n}} = \left(\frac{1}{p_1}\right)^{a_1} \dots \left(\frac{1}{p_n}\right)^{a_n} \in \overline{P}$$

If $b = 1$ and a is an integer bigger than 2, then we just proved that $1/q = 1/a$ must be in $\overline{P}$. Since $\overline{P}$ is a subgroup, then it follows that $q \in \overline{P}$.
If both a and b are integers bigger than 2, then we just showed that both a and $1/b$ are in $\overline{P}$. Again, since $\overline{P}$ is a subgroup, then it follows that $q = a\frac{1}{b} \in \overline{P}$.
In every possible case, we showed that $q \in \overline{P}$ so it follows that $\mathbb{Q}_{>0} \subseteq \overline{P}$. Therefore, $\mathbb{Q}_{>0} = \overline{P} = \langle \{\frac{1}{p} \mid p \text{ is a prime}\} \rangle$.

Exercise 14
A group H is called *finitely generated* if there is a finite set A such that $H = \langle A \rangle$.

(a) Prove that every finite group is finitely generated.

(b) Prove that $\mathbb{Z}$ is finitely generated.

(c) Prove that every finitely generated subgroup of the additive group $\mathbb{Q}$ is cyclic. [If H is a finitely generated subgroup of $\mathbb{Q}$, show that $H \leq \langle \frac{1}{k} \rangle$, where k is the product of all denominators which appear in a set of generators of H.]

(d) Prove that $\mathbb{Q}$ is not finitely generated.

Solution

(a) If G is a group, then obviously, $G = \langle G \rangle$. So if G is finite, it can be written as $\langle H \rangle$ where H is a finite set ($H = G$).

(b) Since $\mathbb{Z} = \langle 1 \rangle$, then it directly follows that it is finitely generated.

(c) Let H be a finitely generated subgroup of $\mathbb{Q}$, then there exist rationals a_i/b_i such that

$$H = \left\langle \frac{a_1}{b_1}, \dots, \frac{a_n}{b_n} \right\rangle$$

Define $k = \prod_{i=1}^{n} b_i$ and let's show that the generators of H are all contained in $\langle \frac{1}{k} \rangle$. Let $j \in [\![1, n]\!]$ and notice that

$$\frac{a_j}{b_j} = \frac{a_j \prod_{\substack{i=1 \\ i \neq j}}^{n} b_i}{b_j \prod_{\substack{i=1 \\ i \neq j}}^{n} b_i} = \frac{a_j \prod_{\substack{i=1 \\ i \neq j}}^{n} b_i}{k} = a_j \prod_{\substack{i=1 \\ i \neq j}}^{n} b_i \cdot \frac{1}{k} \in \left\langle \frac{1}{k} \right\rangle$$

Thus, we showed that $\{\frac{a_1}{b_1}, \ldots, \frac{a_n}{b_n}\} \subseteq \left\langle \frac{1}{k} \right\rangle$. Hence, by Exercise 2:

$$H = \left\langle \frac{a_1}{b_1}, \ldots, \frac{a_n}{b_n} \right\rangle \leq \left\langle \left\langle \frac{1}{k} \right\rangle \right\rangle = \left\langle \frac{1}{k} \right\rangle$$

Therefore, H must be cyclic since it is a subgroup of the cyclic group $\left\langle \frac{1}{k} \right\rangle$.

(d) By contradiction, if $\mathbb{Q}$ is finitely generated, then by our previous proof, it would mean that $\mathbb{Q}$ is cyclic, i.e., there is a rational a/b such that $\mathbb{Q} = \langle \frac{a}{b} \rangle$. But this is impossible since it implies that any element of $\mathbb{Q}$ can be written as a multiple of a/b and some rationals ($\frac{1}{b+1}$ for example) cannot be written as an/b. Therefore, $\mathbb{Q}$ is not finitely generated.

Exercise 15
Exhibit a proper subgroup of $\mathbb{Q}$ which is not cyclic.

Solution
Consider the set $H = \{\frac{1}{p} \mid p \text{ prime and } p \leq 3\}$ and the subgroup that it generates. Let's first prove that $\langle H \rangle$ is not cyclic. By contradiction, suppose that $\langle H \rangle$ is cyclic, then there are positive integers a and b such that $\langle H \rangle = \langle \frac{a}{b} \rangle$. Since there are infinitely many odd primes, then there is an odd prime p such that $b \leq p$. By definition of H and by our assumption, we have

$$\begin{aligned}
\frac{1}{p} \in H &\implies \frac{1}{p} \in \langle H \rangle \\
&\implies \frac{1}{p} \in \left\langle \frac{a}{b} \right\rangle \\
&\implies \frac{1}{p} = n\frac{a}{b}, \qquad \text{for some } n \in \mathbb{Z} \\
&\implies b = nap \\
&\implies p \mid b
\end{aligned}$$

which is a contradiction since both integers are positive and $b \leq p$. Therefore, $\langle H \rangle$ cannot be cyclic.
Let's now prove that $\langle H \rangle$ is a proper subgroup of $\mathbb{Q}$. Suppose by contradiction that $1/2 \in \langle H \rangle$, then there exist some integers a_i's and odd primes p_i's such that

$$\frac{1}{2} = \sum_{i=1}^{n} \frac{a_i}{p_i}$$

By rearranging the terms, we get

$$2 \cdot c = \prod_{i=1}^{n} p_i$$

where $c := \sum_{i=1}^{n} (\frac{a_i}{p_i} \prod_{j=1}^{n} p_j) \in \mathbb{Z}$. Thus, 2 divides the product of the p_i's which implies that there is a $j \in [\![1, n]\!]$ such that $2 \mid p_j$. A contradiction with the fact that the p_i's are odd primes. Therefore, $1/2 \notin \langle H \rangle$ which proves that $\langle H \rangle$ is noncyclic

proper subgroup of $\mathbb{Q}$.

Exercise 16
A subgroup M of a group G is called a *maximal subgroup* if $M \neq G$ and the only subgroups of G which contain M are M and G.

(a) Prove that if H is a proper subgroup of the finite group G then there is a maximal subgroup of G containing H.

(b) Show that the subgroup of all rotations in a dihedral group is a maximal subgroup.

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

Solution

(a) Let H be a proper subgroup of the finite group G of order $n \in \mathbb{Z}^+$. Suppose by contradiction that there is no maximal subgroup of G containing H, then we can define the increasing sequence $\{H_k\}_k$ of subgroups of G recursively where each H_k is a proper subset of H_{k+1}.
Define H_1 as H and for $k \in \mathbb{Z}^+$, since H_k is a subgroup of G that contains H, then it cannot be contained in a maximal subgroup of G, otherwise, H would be contained in a maximal subgroup of G. Hence, there must be a subgroup H_{k+1} of G that contains H_k which is different from H_k and G. Thus, $H_k < H_{k+1}$ for all $k \in \mathbb{Z}^+$.
Notice that the sequence of sets is strictly increasing so the sequence of their respective order $\{|H_k|\}_k$ must blow up to infinity. Therefore, there exist a subgroup H_k of G of order strictly greater than G. A contradiction which implies that H must be contained in a maximal subgroup of G.

(b) Let $M = \langle r \rangle$ and let's show that it is maximal. First, obviously $M \neq G$ since $s \notin M$. Now, let H be a subgroup of G that contains M, then there are two cases. If H contains no elements of the form sr^i where $i \in Z$, then it follows that $H = M$. If there is an integer i such that $sr^i \in H \geq M$, then it must also contain r^{n-i} which implies

$$s = (sr^i)(r^{n-i}) \in H$$

Thus, $\{r, s\} \subseteq H$ which implies (by Exercise 1 and 2):

$$D_{2n} = \langle r, s \rangle \subseteq \langle H \rangle = H$$

Hence, $H = D_{2n}$. Since any subgroup of G that contains M is either M or D_{2n}, then M is maximal by definition.

(c) Let $G = \langle x \rangle$ be a cyclic group of order $n \geq 1$ and H a subgroup of G. Suppose first that H is maximal, since G is cyclic, then it follows that $H = \langle x^m \rangle$ for m divides n. By contradiction, if m is composite, then there exist integers $1 < a, b < m$ such that $m = ab$. Consider the subgroup $\langle x^a \rangle$ and notice that $\langle x^m \rangle \leq \langle x^a \rangle$ which implies by our assumption on the maximality of H that

$\langle x^a \rangle = H$ or $\langle x^a \rangle = G$. If $\langle x^a \rangle = H = \langle x^m \rangle$, then it means that $x^a \in \langle x^m \rangle$ so $x^a = x^{km}$ for some integer. Thus,

$$\begin{aligned} x^a = x^{km} &\implies x^{km-a} = 1 \\ &\implies n \mid km - a \\ &\implies m \mid km - a \\ &\implies m \mid a \end{aligned}$$

a contradiction so $\langle x^a \rangle \neq H$. Hence, we must have $\langle x^a \rangle = G = \langle x \rangle$. But this means that $x \in \langle x^a \rangle$ and for some integer k:

$$\begin{aligned} x = x^{ak} &\implies x^{ak-1} = 1 \\ &\implies n \mid ak - 1 \\ &\implies a \mid ak - 1 \\ &\implies a \mid 1 \end{aligned}$$

again, a contradiction since a is a positive integer strictly greater than 1. Hence, $\langle x^a \rangle$ is neither equal to H or G. Thus, it contradicts the fact that H is maximal so our assumption that m is composite must be false. Therefore, $H = \langle x^m \rangle$ where m is a prime dividing n.
Suppose now that $H = \langle x^p \rangle$ where p is a prime dividing n and let's show that H is maximal. Let $\langle x^d \rangle$ be a subgroup of G that contains H, then d divides n which means that $d = rn$ for some integer r. Moreoever,

$$\begin{aligned} \langle x^p \rangle \leq \langle x^d \rangle &\implies x^p \in \langle x^d \rangle \\ &\implies x^p = x^{kd}, \qquad k \in \mathbb{Z} \\ &\implies x^{kd-p} = 1 \\ &\implies n \mid kd - p \\ &\implies kd - p = tn, \qquad t \in \mathbb{Z} \\ &\implies kd - p = trd \\ &\implies p = (k - tr)d \\ &\implies d \mid p \\ &\implies d = 1 \text{ or } d = p \end{aligned}$$

If $d = 1$, then $\langle x^d \rangle = G$, if $d = p$, $\langle x^d \rangle = H$. Therefore, by definition, H is maximal.

Exercise 17
This is an exercise involving Zorn's Lemma (see Appendix I) to prove that every nontrivial finitely generated group posseses maximal subgroups. Let G be a finitely generated group, say $G = \langle g_1, g_2, \ldots, g_n \rangle$, and let $\mathcal{S}$ be the set of all proper subgroups of G. Then $\mathcal{S}$ is partially ordered by inclusion. Let $\mathcal{C}$ be a chain in $\mathcal{S}$.

(a) Prove that the union, H, of all the subgroups in $\mathcal{C}$ is a subgroup of G.

(b) Prove that H is a *proper* subgroup. [if not, each g_i must line in H and so must lie in some element of the chain $\mathcal{C}$. Use the definition of a chain to arrive at a contradiction.]

(c) Use Zorn's Lemma to show that $\mathcal{S}$ has a maximal element (which is, by definition, a maximal subgroup).

Solution

(a) Obviously, $H =$ is a subset of G. To show that it is actually a subgroup, let $x, y \in H$ and let's show that $xy^{-1} \in H$. By definition of H, there exist sets C_1 and C_2 in $\mathcal{C}$ such that $x \in C_1$ and $y \in C_2$. Since $\mathcal{C}$ is a chain, we must have $C_1 \subseteq C_2$ or $C_2 \subseteq C_1$, in both cases, $C_1 \cup C_2$ is a subgroup of G contained in $\mathcal{C}$. Hence, $x, y \in C_1 \cup C_2$ which implies that $xy^{-1} \in C_1 \cup C_2 \subseteq H$. To finish the argument, notice that H is nonempty since it is a union of nonempty sets. Therefore, H is a subgroup of G.

(b) Suppose by contradiction that $H = G$, then there exist sets $C_1, \ldots, C_n \in \mathcal{C}$ such that $g_i \in C_i$ for all $i \in [\![1, n]\!]$. Since the inclusion is a total ordering on $\mathcal{C}$, then $\cup_{i=1}^n C_i$ is equal to C_j for some $j \in [\![1, n]\!]$. Thus, $\cup_{i=1}^n C_i$ is an element of $\mathcal{S}$ so it is a proper subgroup of G that contains all of the generators of G. However, notice that this implies (by Exercise 1 and 2):

$$\begin{aligned} \{g_1, \ldots, g_n\} \subseteq \bigcup_{i=1}^n C_i &\implies \langle g_1, \ldots, g_n \rangle \subseteq \left\langle \bigcup_{i=1}^n C_i \right\rangle \\ &\implies G \subseteq \bigcup_{i=1}^n C_i \\ &\implies \bigcup_{i=1}^n C_i = G \end{aligned}$$

which is a contradiction. Therefore, H is a proper subgroup of G.

(c) First, notice that H is an upperbound for $\mathcal{C}$ since each $C \in \mathcal{C}$ satisfies $C \subseteq H$. Therefore, we showed in the previous parts of this exercise that each chain in $\mathcal{S}$ has an upperbound. Thus, by Zorn's Lemma, it directly follows that there is an element $M \in \mathcal{S}$ such that if $M \subseteq M'$ where M' is a proper subgroup of G, then $M' = G$. Equivalently, if M' is any subgroup of G that satisfies $M \subseteq M'$, then we either have $M' = G$ or $M' = M$. Therefore, by definition, G has a maximal element.

Exercise 18

Let p be a prime and let $Z = \{z \in \mathbb{C} | z^{p^n} = 1 \text{ for some } n \in \mathbb{Z}^+\}$ (so Z is the multiplicative group of all p-power roots of unity in $\mathbb{C}$). For each $k \in \mathbb{Z}^+$ let $H_k = z \in \mathbb{C} | z^{p^k} = 1$ (the group of p^k-th roots of unity). Prove the following:

(a) $H_k \leq H_m$ if and only if $k \leq m$

(b) H_k is cyclic for all k (assume that for any $n \in \mathbb{Z}^+$, $\{e^{2\pi i t/n} | t = 0, 1, \ldots, n-1\}$ is the set of all n^{th} roots of 1 in $\mathbb{C}$)

(c) every proper subgroup of Z equals H_k for some $k \in \mathbb{Z}^+$ (in particular, every proper subgroup of Z is finite and cyclic)

(d) Z is not finitely generated.

Solution

(a) Let k and m be positive integers. Suppose that $H_k \leq H_m$ and let z be a complex number of order p^k ($z = e^{\frac{2}{\pi}i/p^k}$ for example), then we obviously have $z \in H_k$. By our assumption, we also have $z \in H_m$ which implies that $z^{p^m} = 1$:

$$\begin{aligned} z^{p^m} = 1 &\implies |z| \mid p^m \\ &\implies p^k \mid p^m \\ &\implies k \leq m \end{aligned}$$

To prove the reverse inclusion, suppose now that $k \leq m$ and let z be an arbitrary element of H_k, then notice that

$$\begin{aligned} z \in H_k &\implies z^{p^k} = 1 \\ &\implies (z^{p^k})^{p^{m-k}} = 1^{p^{m-k}} \\ &\implies z^{p^k p^{m-k}} = 1 \\ &\implies z^{p^m} = 1 \\ &\implies z \in H_m \end{aligned}$$

Therefore, $H_k \leq H_m$.

(b) Let $k \in \mathbb{Z}^+$, since $H_k = \{e^{2\pi it/p^k} | t = 0, 1, \ldots, p^k - 1\}$, then it obviously implies by the 2π-periodicity of $e^{i\theta}$ that

$$\begin{aligned} H_k &= \{e^{2\pi it/p^k} \mid t = 0, 1, \ldots, p^k - 1\} \\ &= \{e^{2\pi it/p^k} \mid t \in \mathbb{Z}\} \\ &= \{(e^{2\pi i/p^k})^t \mid t \in \mathbb{Z}\} \\ &= \langle e^{2\pi i/p^k} \rangle \end{aligned}$$

Therefore, H_k is cyclic.

(c) Let H be a proper subgroup of Z. For each $h \in H$, consider the set S_h defined by

$$S_h = \{n \in \mathbb{Z}^+ \mid h \in H_n\}$$

Since, $Z = \cup_{n=1}^{\infty} H_n$, then $S_h \neq \varnothing$. Thus, by the well ordering of $\mathbb{Z}^+$, S_h has a minimum m_h. Hence, there is a $t \in [\![0, p^{m_h} - 1]\!]$ such that $h = e^{2\pi it/p^{m_h}}$. Moreover, since m_h is the minimum of S_h, we must have $(t, p) = 1 = (t, p^{m_h})$. Therefore, since $e^{2\pi i/p^{m_h}}$ has order p^{m_h}, then by the theorems from the previous section:

$$\begin{aligned} \langle h \rangle &= \left\langle (e^{2\pi i/p^{m_h}})^t \right\rangle \\ &= \langle e^{2\pi i/p^{m_h}} \rangle \\ &= H_{m_h} \end{aligned}$$

From this, it is easy to see that

$$H = \bigcup_{h \in H} \langle h \rangle = \bigcup_{h \in H} H_{m_h}$$

Consider now the set $M = \{m_h \mid h \in H\}$, if M is unbounded above, then $H_n \leq H$ for all $n \in \mathbb{Z}^+$ which implies that $H = Z$. A contradiction since H is a proper subgroup of Z. Hence, since M is a set of integers, then it has a maximum k. Thus, there is a $h \in H$ such that $\langle h \rangle = H_k$ which implies $H_k \leq H$. Moreover, for any $h \in H$,

$$\begin{aligned} H_{m_h} \leq H_k &\implies \bigcup_{n=1}^{\infty} H_{m_h} \leq H_k \\ &\implies H \leq H_k \end{aligned}$$

Therefore, $H = H_k$ for some $k \in \mathbb{Z}^+$.

(d) Let H be an arbitrary proper subgroup of Z, then by part (c), we know that $H = H_k$ for some k. Hence, there is a proper subgroup of Z, for example H_{k+1}, that contains H_k and that is distinct from H and Z. Thus, H cannot be a maximal subgroup of Z. Therefore, Z cannot be finitely generated since it has no maximal subgroup (by Exercise 17).

Exercise 19
A nontrivial abelian group A (written multiplicatively) is called *divisible* if for each element $a \in A$ and each nonzero integer k there is a an element $x \in A$ such that $x^k = a$, i.e., each element has a k^{th} root in A (in additive notation, each element is the k^{th} multiple of some element in A).

(a) Prove that the additive group of rational numbers, $\mathbb{Q}$, is divisible.

(b) Prove that no finite abelian group is divisible.

Solution

(a) To prove that the additive group $\mathbb{Q}$ is divisible, we need to prove that any rational is the k^{th} multiple of some rational for any integer k. To do so, let a/b be an arbitrary rational and k an arbitrary nonzero integer, define x to be equal to a/kb. Then, obviously, $kx = a/b$. Therefore, $\mathbb{Q}$ is divisible.

(b) Let A be a finite nontrivial abelian group of order $n \in \mathbb{Z}^+$, let $a \in A$ be an element different than 1. Notice that for all $x \in A$,

$$x^n = 1 \neq a$$

so a has no n^{th} root. Therefore, A is not divisible.

Exercise 20
Prove that if A and B are nontrivial abelian groups, then $A \times B$ is divisible if and only if both A and B are divisible groups.

Solution
Suppose first that $A \times B$ is divisible, to show that both A and B are divisible, let $a \in A$, $b \in B$ and $k \in \mathbb{Z} - \{0\}$, by divisibility of $A \times B$, there is a tuple $(x, y) \in A \times B$ such that $(x, y)^k = (a, b)$. Thus, there is a $x \in A$ such that $x^k = a$ and a $y \in B$ such that $y^k = b$. Therefore, both A and B are divisible.
Suppose now that both A and B are divisible. Let $(a, b) \in A \times B$ and $k \in \mathbb{Z} - \{0\}$, then by divisibility of A and B, there is a $x \in A$ such that $x^k = a$ and a $y \in B$ such that $y^k = b$. Thus, $(x, y)^k = (a, b)$. Therefore, $A \times B$ is divisible.

2.5 The Lattice of Subgroups of a Group

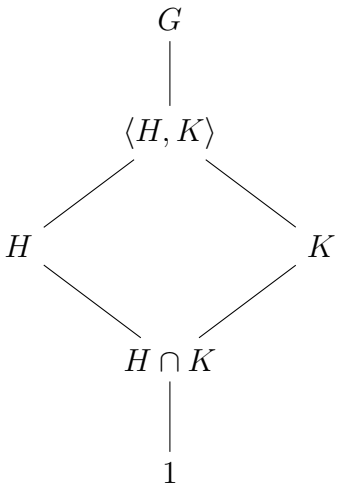
Exercise 1
Let H and K be subgroups of G. Exhibit all possible sublattices which shows only G, 1, H, K and their joins and intersections. What distinguishes the different drawings ?

Solution
To find these lattices, consider the three following cases :

1. If $K \leq H$, then it obviously follows that $H \cap K = K$ and $\langle H, K \rangle = H$. Therefore, the lattice can be drawn as follows:

2. If $H \leq K$, then it obviously follows that $H \cap K = H$ and $\langle H, K \rangle = K$. Therefore, the lattice can be drawn as follows:

3. If H and K are not comparable, all of H, K, $H \cap K$ and $\langle H, K \rangle$ are distinct. Hence:



Therefore, the only thing that distinguishes the different drawings, beside the name of the nodes, is the fact that one is a straight line and the other splits in the middle.

Exercise 2
In each of (a) to (d) list all subgroups of D_{16} that satisfy the given conition.

(a) Subgroups that are contained in $\langle sr^2, r^4\rangle$

(b) Subgroups that are contained in $\langle sr^7, r^4\rangle$

(c) Subgroups that contain $\langle r^4\rangle$

(d) Subgroups that contain $\langle s\rangle$.

Solution

(a) The subgroups of D_{16} that are contained in $\langle sr^2, r^4\rangle$ are

$$1, \quad \langle sr^6\rangle, \quad \langle sr^2\rangle, \quad \langle r^4\rangle, \quad \langle sr^2, r^4\rangle$$

(b) First, notice that $\langle sr^7, r^4\rangle$ is equal to $\langle sr^3, r^4\rangle$. Hence, the subgroups of D_{16} that are contained in $\langle sr^7, r^4\rangle$ are

$$1, \quad \langle sr^3\rangle, \quad \langle sr^7\rangle, \quad \langle r^4\rangle, \quad \langle sr^7, r^4\rangle$$

(c) The subgroups of D_{16} that contain $\langle r^4\rangle$ are

$$\langle r^4\rangle, \quad \langle sr^2, r^4\rangle, \quad \langle s, r^4\rangle, \quad \langle r^2\rangle, \quad \langle sr^3, r^4\rangle$$
$$\langle sr^5, r^4\rangle, \quad \langle s, r^2\rangle, \quad \langle r\rangle, \quad \langle sr, r^2\rangle, \quad D_{16}$$

(d) The subgroups of D_{16} that contain $\langle s\rangle$ are

$$\langle s\rangle, \quad \langle s, r^4\rangle, \quad \langle s, r^2\rangle, \quad D_{16}$$

Exercise 3
Show that the subgroup $\langle s, r^2\rangle$ of D_8 is isomorphic to V_4.

Solution
First, recall that $V_4 = \{1, a, b, c\}$ with the following multiplication table:

$\cdot$	1	a	b	c
1	1	a	b	c
a	a	1	c	b
b	b	c	1	a
c	c	b	a	1

Notice that $\{1, s, r^2, sr^2\}$ is a group subgroup of D_8 that contains s, r^2 and all of the possible combinations of these elements. Hence,

$$\langle s, r^2\rangle = \{1, s, r^2, sr^2\}$$

From this, we get the following multiplication table for $\langle s, r^2\rangle$:

$\cdot$	1	s	r^2	sr^2
1	1	s	r^2	sr^2
s	s	1	sr^2	r^2
r^2	r^2	sr^2	1	s
sr^2	sr^2	r^2	s	1

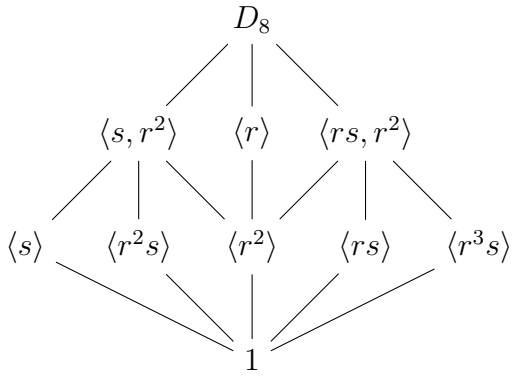
which directly implies that the function $\varphi : \langle s, r^2 \rangle \to V_4$ defined by

$$1 \mapsto 1, \quad a \mapsto s, \quad b \mapsto r^2, \quad c \mapsto sr^2$$

is an isomorphism. Therefore, $\langle s, r^2 \rangle \cong V_4$.

Exercise 4
Use the given lattice to find all pairs of elements that generate D_8 (there are 12 pairs).

Solution
Recall that the lattice of subgroups of D_8 looks like this:



Finding pairs (a, b) such that $\langle a, b \rangle = D_8$ is equivalent to finding elements a and b such that the least common upperbound of their corresponding sets $\langle a \rangle$ and $\langle b \rangle$ on the lattice is D_8. Hence, if we recall that $\langle r^3 \rangle = \langle r \rangle$, then we get the following pairs:

$$(s, r), \quad (s, rs), \quad (s, r^3 s), \quad (r^2 s, r), \quad (r^2 s, rs), \quad (r^2 s, r^3 s)$$

$$(s, r^3), \quad (r, rs), \quad (r, r^3 s), \quad (r^2 s, r^3), \quad (r^3, rs), \quad (r^3, r^3 s)$$

Exercise 5
Use the given lattice to find all elements $x \in D_{16}$ such that $D_{14} = \langle x, s \rangle$ (there are 8 such elements).

Solution
The idea is exactly the same as for the previous exercise. Hence, our possible values for x are:

$$r, \quad r^3, \quad r^5, \quad r^7, \quad sr, \quad sr^3, \quad sr^5, \quad sr^7$$

Exercise 6
Use the given lattices to help find the centralizers of every element in the following

groups:
(a) D_8 **(b)** Q_8 **(c)** S_3 **(d)** D_{16}

Solution

(a)
- $C_{D_8}(1) = D_8$
- $C_{D_8}(r) = \langle r \rangle$
- $C_{D_8}(r^2) = D_8$
- $C_{D_8}(r^3) = \langle r \rangle$
- $C_{D_8}(s) = \langle s, r^2 \rangle$
- $C_{D_8}(rs) = \langle rs, r^2 \rangle$
- $C_{D_8}(r^2s) = \langle s, r^2 \rangle$
- $C_{D_8}(r^3s) = \langle rs, r^2 \rangle$

(b)
- $C_{Q_8}(1) = Q_8$
- $C_{Q_8}(-1) = Q_8$
- $C_{Q_8}(i) = \langle i \rangle$
- $C_{Q_8}(-i) = \langle i \rangle$
- $C_{Q_8}(j) = \langle j \rangle$
- $C_{Q_8}(-j) = \langle j \rangle$
- $C_{Q_8}(k) = \langle k \rangle$
- $C_{Q_8}(-k) = \langle k \rangle$

(c)
- $C_{S_3}(1) = S_3$
- $C_{S_3}((1\ 2)) = \langle (1\ 2) \rangle$
- $C_{S_3}((1\ 3)) = \langle (1\ 3) \rangle$
- $C_{S_3}((2\ 3)) = \langle (2\ 3) \rangle$
- $C_{S_3}((1\ 2\ 3)) = \langle (1\ 2\ 3) \rangle$
- $C_{S_3}((1\ 3\ 2)) = \langle (1\ 3\ 2) \rangle$

(d)
- $C_{D_{16}}(1) = D_{16}$
- $C_{D_{16}}(r) = \langle r \rangle$
- $C_{D_{16}}(r^2) = \langle r \rangle$
- $C_{D_{16}}(r^3) = \langle r \rangle$
- $C_{D_{16}}(r^4) = D_{16}$
- $C_{D_{16}}(r^5) = \langle r \rangle$
- $C_{D_{16}}(r^6) = \langle r \rangle$
- $C_{D_{16}}(r^7) = \langle r \rangle$
- $C_{D_{16}}(s) = \langle s, r^4 \rangle$
- $C_{D_{16}}(sr) = \langle sr^5, r^4 \rangle$
- $C_{D_{16}}(sr^2) = \langle sr^2, r^4 \rangle$
- $C_{D_{16}}(sr^3) = \langle sr^3, r^4 \rangle$
- $C_{D_{16}}(sr^4) = \langle s, r^4 \rangle$
- $C_{D_{16}}(sr^5) = \langle sr^5, r^4 \rangle$
- $C_{D_{16}}(sr^6) = \langle sr^2, r^4 \rangle$
- $C_{D_{16}}(sr^7) = \langle sr^3, r^4 \rangle$

Exercise 7
Find the center of D_{16}.

Solution
To find the center of D_{16}, we can take the intersection of all the subgroups we found in part (d) of the previous question, that is:

$$D_{16} \cap \langle r \rangle \cap \langle s, r^4 \rangle \cap \langle sr^2, r^4 \rangle \cap \langle sr^3, r^4 \rangle \cap \langle sr^5, r^4 \rangle$$

Obviously, 1 and r^4 are in this intersection. However, since $sr^i \notin \langle r \rangle$ for $i \in [\![0, n-1]\!]$, then other elements in the intersection must be powers of r. However, the only power of r in $\langle s, r^4 \rangle$ is r^4. Therefore,

$$Z(D_{16}) = \{1, r^4\}$$

Exercise 8
In each of the following groups find the normalizer of each subgroup:
(a) S_3 **(b)** Q_8

Solution

(a)

- $N_{S_3}(1) = S_3$
- $N_{S_3}(\langle(1\ 2)\rangle) = \langle(1\ 2)\rangle$
- $N_{S_3}(\langle(1\ 3)\rangle) = \langle(1\ 3)\rangle$
- $N_{S_3}(\langle(2\ 3)\rangle) = \langle(2\ 3)\rangle$
- $N_{S_3}(\langle(1\ 2\ 3)\rangle) = S_3$
- $N_{S_3}(S_3) = S_3$

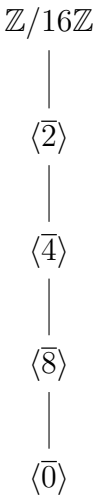
(b)

- $N_{Q_8}(1) = Q_8$
- $N_{Q_8}(\langle -1\rangle) = Q_8$
- $N_{Q_8}(\langle i\rangle) = Q_8$
- $N_{Q_8}(\langle j\rangle) = Q_8$
- $N_{Q_8}(\langle k\rangle) = Q_8$
- $N_{Q_8}(Q_8) = Q_8$

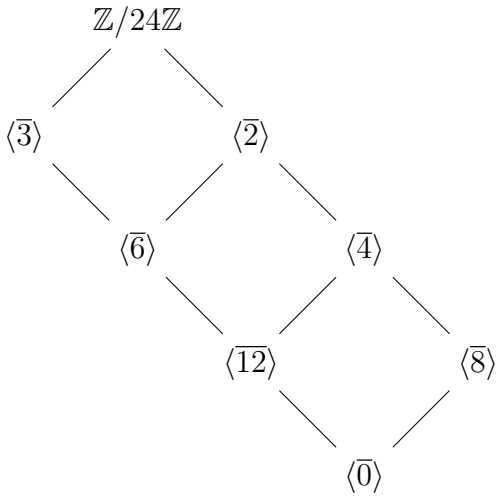
Exercise 9
Draw the lattices of subrgoups of the following groups:
(a) $\mathbb{Z}/16\mathbb{Z}$ **(b)** $\mathbb{Z}/24\mathbb{Z}$ **(c)** $\mathbb{Z}/48\mathbb{Z}$. [See Exercise 6 in Section 3.]

Solution

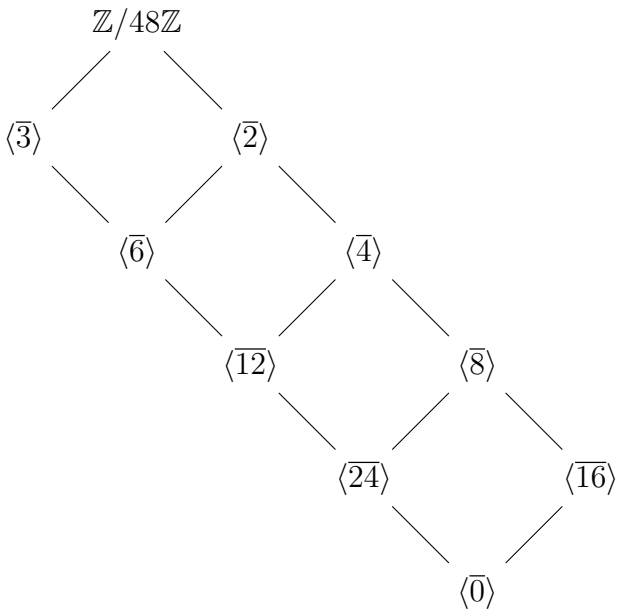
(a) Lattice of subgroups of $\mathbb{Z}/16\mathbb{Z}$:



(b) Lattice of subgroups of $\mathbb{Z}/24\mathbb{Z}$:



(c) We already drew the lattice of subgroups of $\mathbb{Z}/48\mathbb{Z}$ in Exercise 6 of section 3:



Exercise 10
Classify groups of order 4 by proving that if $|G| = 4$ then $G \cong Z_4$ or $G \cong V_4$. [See Exercise 36, Section 1.1.]

Solution
Let's prove it by cases. If G contains an element of order 4, then it directly follows that G is a cyclic group of order 4 which implies that $G \cong Z_4$.
Otherwise, if G has no elements of order 4, then we already proved in Exercise 36 of Section 1.1 that it automoaticaly implies that G has the following multiplication table: which is exactly the same multiplication as V_4 so both are isomorphic. There-

$\cdot$	1	a	b	c
1	1	a	b	c
a	a	1	c	b
b	b	c	1	a
c	c	b	a	1

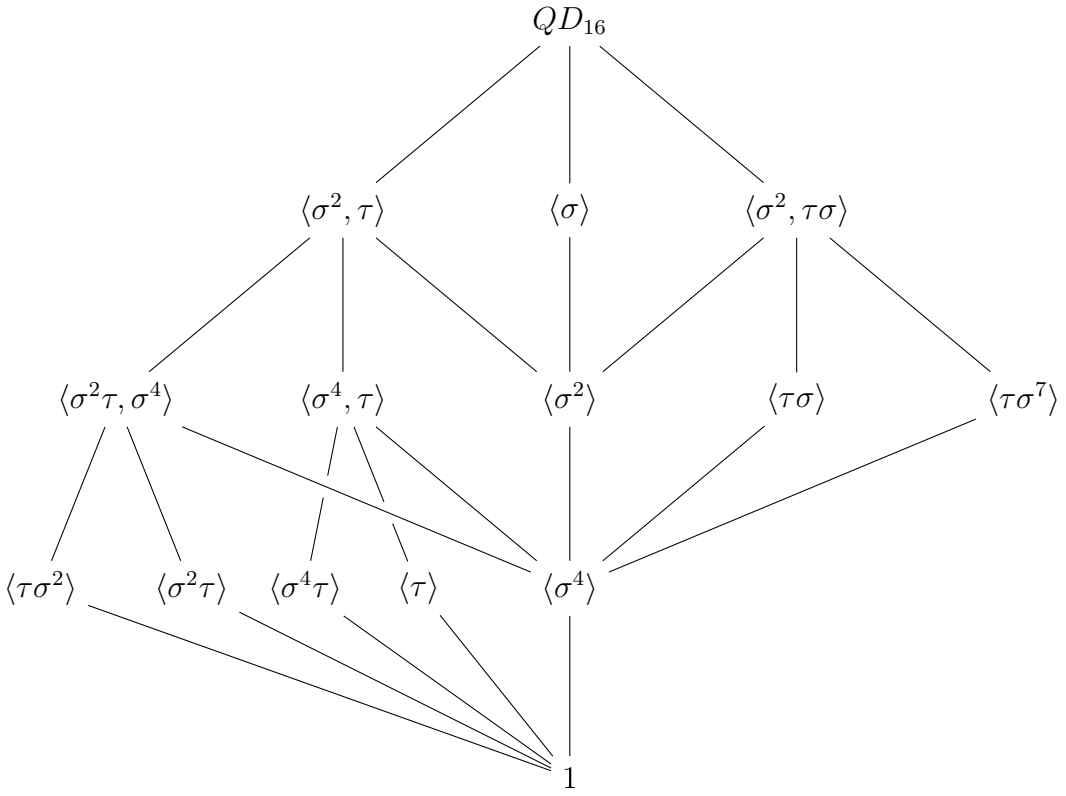
fore, we either have $G \cong Z_4$ or $G \cong V_4$.

Exercise 11
Consider the group of order 16 with the following presentation:

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

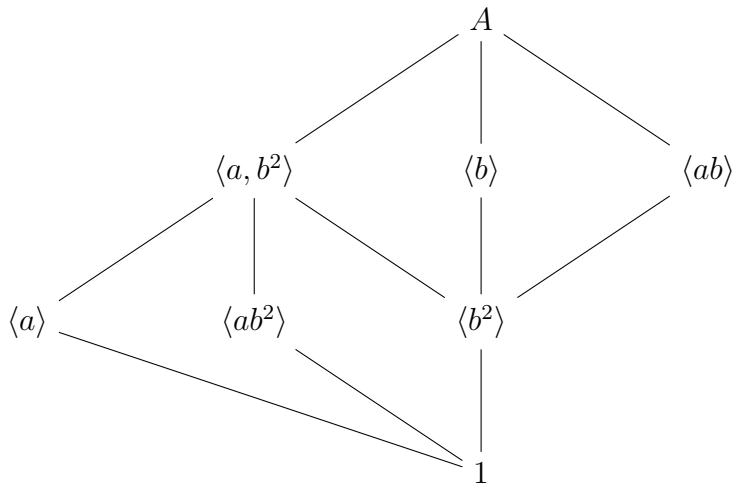
(called the *quasidihedral* or *semidihedral* group of order 16). This group has three subgroups of order 8: $\langle\tau, \sigma^2\rangle \cong D_8$, $\langle\tau\rangle \cong Z_8$ and $\langle\sigma^2, \sigma\tau\rangle \cong Q_8$ and every proper subgroup is contained in one of these subgroups. Fill in the missing subgroups in the lattice of all subgroups of the quasidihedral group on the following page, exhibiting each subgroup with at most two generators. (This is another example of a nonplanar lattice.)

Solution
Using the isomorphisms $\langle \tau, \sigma^2 \rangle \cong D_8$, $\langle \tau \rangle \cong Z_8$ and $\langle \sigma^2, \sigma\tau \rangle \cong Q_8$, we can make our life easier by considering σ^2 and τ as r and s respectively in D_8. Moreover, in the same way, we can consider σ^4, σ^2, $\tau\sigma$ and $\tau\sigma^7$ as -1, i, j and k respectively. Therefore, we get the following lattice of subgroups for QD_{16}:



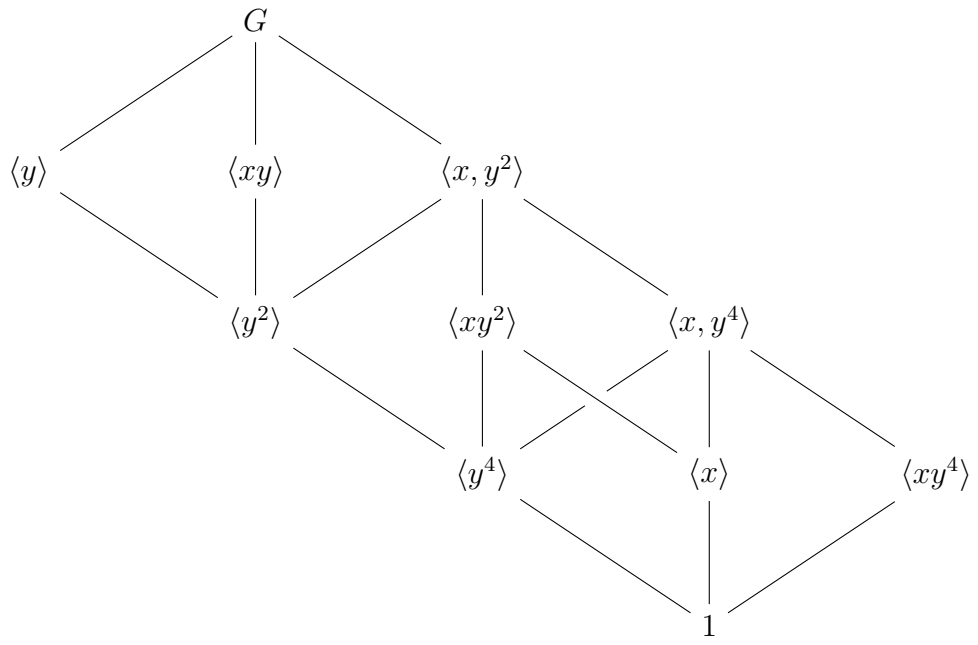
Exercise 12
The group $A = Z_2 \times Z_4 = \langle\ a, b\ |a^2 = b^4 = 1,\ ab = ba\ \rangle$ has order 8 and has three subgroups of order 4: $\langle a, b^2 \rangle \cong V_4$, $\langle b \rangle \cong Z_4$ and $\langle ab \rangle \cong Z_4$ and every proper subgroup is contained in one of these three. Draw the lattice of all subgroups of A, giving each subgroup in terms of at most two generators.

Solution As in the previous exercise, we will mostly rely on the fact that all the subgroups of order 4 are $\langle a, b^2 \rangle \cong V_4$, $\langle b \rangle \cong Z_4$ and $\langle ab \rangle \cong Z_4$. Hence, we get:



Exercise 13
The group $G = Z_2 \times Z_8 = \langle\ x, y\ | x^2 = y^8 = 1,\ xy = yx\ \rangle$ has order 16 and has three subgroups of order 8: $\langle x, y^2\rangle \cong Z_2 \times Z_4$, $\langle y\rangle \cong Z_8$ and $\langle xy\rangle \cong Z_8$ and every proper subgroup is contained in one of these three. Draw the lattice of all subgroups of G, giving each subgroup in terms of at most two generators (cf. Exercise 12).

Solution As in the previous exercise, we will mostly rely on the fact that all the subgroups of order 8 are $\langle x, y^2\rangle \cong Z_2 \times Z_4$, $\langle y\rangle \cong Z_8$ and $\langle xy\rangle \cong Z_8$. Moreover, since we already drew the lattice of subgroups of the group $Z_2 \times Z_4$ in the previous question, then we get:



Exercise 14
Let M be the group of order 16 with the following presentation:

$$\langle\ u, v\ |\ u^2 = v^8 = 1,\ vu = uv^5\ \rangle$$

(sometimes called the *modular* group of order 16). It has three subgroups of order 8: $\langle u, v^2\rangle$, $\langle v\rangle$ and $\langle uv\rangle$ and every proper subgroup is contained in oneof these three. Prove that $\langle u, v^2\rangle \cong Z_2 \times Z_4$, $\langle v\rangle \cong Z_8$ and $\langle uv\rangle \cong Z_8$. Show that the lattice of subgroups of M is the same as the lattice of subgroups of $Z_2 \times Z_8$ (cf. Exercise 13) but that these two groups are not isomorphic.

Solution
First, let's prove the three isomorphisms. Obviously, $\langle v\rangle \cong Z_8$ since v is an element of order 8. Similarly, to show that $\langle uv\rangle \cong Z_8$, we simply need to show that uv has order 8. To do so, notice that

$$(uv)^2 = uvuv = uuv^5v = v^6$$

Thus,

$$(uv)^8 = (v^6)^4 = v^{24} = 1$$

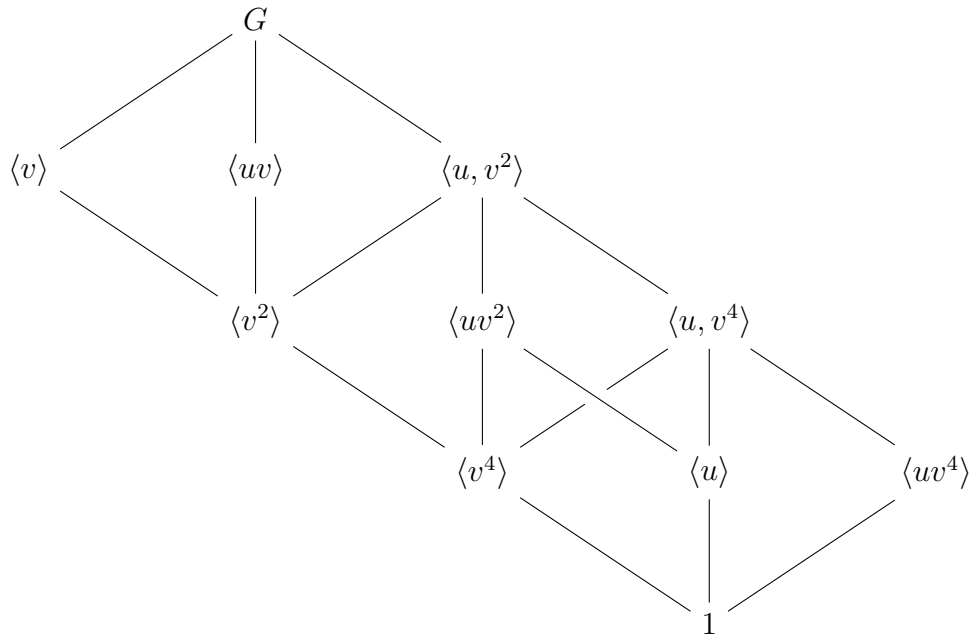
Hence, uv must have order 1, 2, 4 or 8. But notice that

$$(uv)^4 = (v^6)^2 = v^12 = v^4 \neq 1$$

Therefore, uv has order 8 which shows that $\langle uv \rangle \cong Z_8$. Finally, since

$$uv^2 = (uv^2)v^8 = (uv^5)v^5 = v(uv^5) = v^2u$$

then elements in $\langle u, v^2 \rangle$ have the form $u^n(v^2)^m$. Thus, obviously, $\langle u, v^2 \rangle \cong Z_2 \times Z_4$. From this, we get that



which obviously shows that M has the same lattice of subgroups of $Z_2 \times Z_8$.
Now, let's show that $M \ncong Z_2 \times Z_8$. By contradiction, if $M \cong Z_2 \times Z_8$, then M must be abelian so we have

$$uv = vu = uv^5$$

which implies that

$$v^4 = 1$$

But this is a contradiction since v has order 8. Therefore, $M \ncong Z_2 \times Z_8$ even if they have the same lattice of subgroups.

Exercise 15
Describe the isomorphism type of each of the three subgroups of D_{16} of order 8.

Solution The three subgroups of order 8 of D_{16} are $\langle s, r^2 \rangle$, $\langle r \rangle$ and $\langle sr, r^2 \rangle$. Obviously, $\langle r \rangle \cong Z_8$ since it is cyclic and has order 8. By looking at the lattice of subgroups of D_{16} and D_8, we can guess that both $\langle s, r^2 \rangle$ and $\langle sr, r^2 \rangle$ are isomorphic to D_8. To prove it, notice that the function that associates s in D_{16} to s in D_8 and r^2 in D_{16} to r in D_8 extends to an isomorphism since s has order 2, r^2 has order 4 and

$$(r^2)s = r(rs) = (rs)r^{-1} = s(r^2)^{-1}$$

The same holds if we replace s with sr. Therefore, we get that $\langle s, r^2 \rangle \cong \langle sr, r^2 \rangle \cong D_8$.

Exercise 16
Use the lattice of subgroups of the quasidihedral group of order 16 to show that every element of order 2 is contained in the proper subgroup $\langle \tau, \sigma^2 \rangle$ (cf. Exercise 11).

Solution
Proving this is equivalent to showing that every subgroup of QD_{16} of order 2 is a subgroup of $\langle \tau, \sigma^2 \rangle$. The subgroups of order 2 are precisely $\langle \tau \rangle$, $\langle \sigma^4 \rangle$, $\langle \sigma^4 \tau \rangle$, $\langle \sigma^2 \tau \rangle$ and $\langle \tau \sigma^2 \rangle$. But notice that all of them are *below* $\langle \tau, \sigma^2 \rangle$ in the lattice. Thus, $\langle \tau, \sigma^2 \rangle$ contains every element of order 2.

Exercise 17
Use the lattice of subgroups of the modular group M of order 16 to show that the set $\{x \in M \mid x^2 = 1\}$ is a subgroup of M isomorphic to the Klein 4-group (cf. Exercise 14).

Solution
The elements x in M that satisfy $x^2 = 1$ are precisely 1, v^4, u and uv^4. But notice that $\langle u, v^4 \rangle$ contains exactly these four elements. Hence, it is a subgroup of M of order 4 that is not cyclic, thus, it must isomorphic the Klein 4-group.

Exercise 18
Use the lattice to help find the centralizers of every element of QD_{16} (cf. Exercise 11).

Solution

- $C_{QD_{16}}(1) = QD_{16}$
- $C_{QD_{16}}(\sigma) = \langle \sigma \rangle$
- $C_{QD_{16}}(\sigma^2) = \langle \sigma \rangle$
- $C_{QD_{16}}(\sigma^3) = \langle \sigma \rangle$
- $C_{QD_{16}}(\sigma^4) = QD_{16}$
- $C_{QD_{16}}(\sigma^5) = \langle \sigma \rangle$
- $C_{QD_{16}}(\sigma^6) = \langle \sigma \rangle$
- $C_{QD_{16}}(\sigma^7) = \langle \sigma \rangle$
- $C_{QD_{16}}(\tau) = \langle \sigma^4, \tau \rangle$
- $C_{QD_{16}}(\tau\sigma) = \langle \tau\sigma \rangle$
- $C_{QD_{16}}(\tau\sigma^2) = \langle \sigma^2\tau, \sigma^4 \rangle$
- $C_{QD_{16}}(\tau\sigma^3) = \langle \tau\sigma^7 \rangle$
- $C_{QD_{16}}(\tau\sigma^4) = \langle \sigma^4, \tau \rangle$
- $C_{QD_{16}}(\tau\sigma^5) = \langle \tau\sigma \rangle$
- $C_{QD_{16}}(\tau\sigma^6) = \langle \sigma^2\tau, \sigma^4 \rangle$
- $C_{QD_{16}}(\tau\sigma^7) = \langle \tau\sigma^7 \rangle$

Exercise 19
Use the lattice to help find $N_{D_{16}}(\langle s, r^4 \rangle)$.

Solution

To find the normalizer of $\langle s, r^4 \rangle$, first notice that

$$\begin{aligned} s\langle s, r^4 \rangle s^{-1} &= \{s1s,\ sss,\ sr^4s,\ ssr^4s\} \\ &= \{1,\ s,\ r^4,\ sr^4\} \\ &= \langle s, r^4 \rangle \end{aligned}$$

and

$$\begin{aligned} r^2\langle s, r^4 \rangle r^{-2} &= \{r^21r^{-2},\ r^2sr^{-2},\ r^2r^4r^{-2},\ r^2sr^4r^{-2}\} \\ &= \{1,\ sr^4,\ r^4,\ s\} \\ &= \langle s, r^4 \rangle \end{aligned}$$

which implies that both s and r^2 are in $N_{D_{16}}(\langle s, r^4 \rangle)$. Thus, $\langle s, r^2 \rangle \leq N_{D_{16}}(\langle s, r^4 \rangle)$ which implies by the given lattice that $N_{D_{16}}(\langle s, r^4 \rangle)$ is either $\langle s, r^2 \rangle$ or D_{16}. However, notice that

$$\begin{aligned} r\langle s, r^4 \rangle r^{-1} &= \{r1r^{-1},\ rsr^{-1},\ rr^4r^{-1},\ rsr^4r^{-1}\} \\ &= \{1,\ sr^6,\ r^4,\ sr^2\} \\ &\neq \langle s, r^4 \rangle \end{aligned}$$

so $N_{D_{16}}(\langle s, r^4 \rangle) \neq D_{16}$. Therefore, it follows that $N_{D_{16}}(\langle s, r^4 \rangle) = \langle s, r^2 \rangle$.

Exercise 20
Use the lattice of subgroups of QD_{16} (cf. Exercise 11) to help find the normalizers
(a) $N_{QD_{16}}(\langle \tau\sigma \rangle)$ **(b)** $N_{QD_{16}}(\langle \tau, \sigma^4 \rangle)$

Solution

(a) To find the normalizer of $\langle \tau\sigma \rangle$, first notice that $\tau\sigma$ is obviously in it and that

$$\begin{aligned} \sigma^2\langle \tau\sigma \rangle\sigma^{-2} &= \{\sigma^21\sigma^{-2},\ \sigma^2\tau\sigma\sigma^{-2},\ \sigma^2\sigma^4\sigma^{-2},\ \sigma^2\tau\sigma^5\sigma^{-2}\} \\ &= \{1,\ \tau\sigma^5,\ \sigma^4,\ \tau\sigma\} \\ &= \langle \tau\sigma \rangle \end{aligned}$$

which implies that both σ^2 and $\tau\sigma$ are in $N_{QD_{16}}(\langle \tau\sigma \rangle)$. Thus, $\langle \sigma^2, \tau\sigma \rangle \leq N_{QD_{16}}(\langle \tau\sigma \rangle)$ which implies by the given lattice that $N_{QD_{16}}(\langle \tau\sigma \rangle)$ is either $\langle \sigma^2, \tau\sigma \rangle$ or QD_{16}. However, notice that

$$\begin{aligned} \sigma\langle \tau\sigma \rangle\sigma^{-1} &= \{\sigma1\sigma^{-1},\ \sigma\tau\sigma\sigma^{-1},\ \sigma\sigma^4\sigma^{-1},\ \sigma\tau\sigma^5\sigma^{-1}\} \\ &= \{1,\ \tau\sigma^3,\ \sigma^4,\ \tau\sigma^7\} \\ &\neq \langle \tau\sigma \rangle \end{aligned}$$

so $N_{QD_{16}}(\langle \tau\sigma \rangle) \neq QD_{16}$. Therefore, it follows that $N_{QD_{16}}(\langle \tau\sigma \rangle) = \langle \sigma^2, \tau\sigma \rangle$.

(b) To find the normalizer of $\langle \tau, \sigma^4 \rangle$, first notice that

$$\begin{aligned} \sigma^2\langle \tau, \sigma^4 \rangle\sigma^{-2} &= \{\sigma^21\sigma^{-2},\ \sigma^2\tau\sigma^{-2},\ \sigma^2\sigma^4\sigma^{-2},\ \sigma^2\tau\sigma^4\sigma^{-2}\} \\ &= \{1,\ \tau\sigma^4,\ \sigma^4,\ \tau\sigma^4\} \\ &= \langle \tau, \sigma^4 \rangle \end{aligned}$$

and

$$\begin{aligned}\tau\langle\tau,\sigma^4\rangle\tau^{-1} &= \{\tau 1\tau^{-1},\ \tau\tau\tau^{-1},\ \tau\sigma^4\tau^{-1},\ \tau\tau\sigma^4\tau^{-1}\}\\ &= \{1,\ \tau,\ \sigma^4,\ \tau\sigma^4\}\\ &= \langle\tau,\sigma^4\rangle\end{aligned}$$

which implies that both σ^2 and τ are in $N_{QD_{16}}(\langle\tau,\sigma^4\rangle)$. Thus, $\langle\sigma^2,\tau\rangle \leq N_{QD_{16}}(\langle\tau,\sigma^4\rangle)$ which implies by the given lattice that $N_{QD_{16}}(\langle\tau\sigma\rangle)$ is either $\langle\sigma^2,\tau\rangle$ or QD_{16}. However, notice that

$$\begin{aligned}\sigma\langle\tau,\sigma^4\rangle\sigma^{-1} &= \{\sigma 1\sigma^{-1},\ \sigma\tau\sigma^{-1},\ \sigma\sigma^4\sigma^{-1},\ \sigma\tau\sigma^4\sigma^{-1}\}\\ &= \{1,\ \tau\sigma^2,\ \sigma^4,\ \tau\sigma^6\}\\ &\neq \langle\tau,\sigma^4\rangle\end{aligned}$$

so $N_{QD_{16}}(\langle\tau,\sigma^4\rangle) \neq QD_{16}$. Therefore, it follows that $N_{QD_{16}}(\langle\tau,\sigma^4\rangle) = \langle\sigma^2,\tau\rangle$.

Chapter 3

Quotient Groups and Homomorphisms

3.1 Definitions and Examples

Exercise 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 $\ker \varphi \trianglelefteq G$.

Solution
Let E be a subgroup, to show that $\varphi^{-1}(E) \leq G$, we can use the subgroup criterion which says that if it is closed under $(x, y) \mapsto xy^{-1}$ then it is a subgroup. Let x and y be arbitrary elements of $\varphi^{-1}(E)$, then both $\varphi(x)$ and $\varphi(y)$ are in E. Thus, since E is a subgroup of H, we have:

$$\begin{aligned} \varphi(x)\varphi(y)^{-1} \in E &\implies \varphi(xy^{-1}) \in E \\ &\implies xy^{-1} \in \varphi^{-1}(E) \end{aligned}$$

which lets us conclude that it is a subgroup.
Suppose now that $E \trianglelefteq H$, then by the previous proof, we know that $\varphi^{-1}(E) \leq G$. Moreover, by Theorem 6, we have that for all $h \in H$,

$$hEh^{-1} \subseteq E$$

Let g be an arbitrary element in G, then for all $y \in g\varphi^{-1}(E)g^{-1}$, there is a $x \in \varphi^{-1}(E)$ such that $y = gxg^{-1}$. Thus,

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

so $y \in \varphi^{-1}(E)$. Since it holds for all y, then $g\varphi^{-1}(E)g^{-1} \subseteq \varphi^{-1}(E)$. Therefore, since it holds for all $g \in G$, we get by Theorem 6: $\varphi^{-1}(E) \trianglelefteq G$.
Trivialy, since $\{1\}$ is normal in H, then $\ker \varphi = \varphi^{-1}(\{1\})$ is normal in G.

Exercise 2
Let $\varphi : G \to H$ be a homomorphism of groups with kernel K and let $a, b \in \varphi(G)$. Let $X \in G/K$ be the fiber above a and let Y be the fiber above b, i.e., $X = \varphi^{-1}(a)$, $Y = \varphi^{-1}(b)$. Fix an element u of X (so $\varphi(u) = a$). Prove that if $XY = Z$ in the

quotient group G/K and w is any member of Z, then there is some $v \in Y$ such that $uv = w$. [Show $u^{-1}w \in Y$.]

Solution By the definition of the products of fibers, the set XY is the fiber above ab. Hence:

$$\begin{aligned} w \in XY &\implies \varphi(w) = ab \\ &\implies \varphi(w) = \varphi(u)b \\ &\implies \varphi(u^{-1}w) = b \\ &\implies u^{-1}w \in Y \\ &\implies v = u^{-1}w, \qquad \text{for some } v \in Y \\ &\implies uv = w, \qquad \text{for some } v \in Y \end{aligned}$$

which is the desired equality.

Exercise 3
Let A be an abelian group and let B be a subgroup of A. Prove that A/B is abelian. Give an example of a non-abelian group G containing a proper normal subgroup N such that G/N is abelian.

Solution
First, notice that B must be normal since for all $a \in A$:

$$aB = \{ab \mid b \in B\} = \{ba \mid b \in B\} = Ba$$

Hence, A/B is a group. Moreover, for all $uB, vB \in A/B$:

$$(uB)(vB) = (uv)B = (vu)B = (vB)(uB)$$

Therefore, A/B is an abelian group.
As an example of abelian group G/N where G is non-abelian and N is a proper subgroup, take $G = D_8$ and $N = \langle r^2 \rangle$ and notice that N must be normal since $N = Z(D_8)$. Moreover, G/N contains the elements

$$\{1, r^2\},\ \{r, r^3\},\ \{s, sr^2\},\ \{sr, sr^3\}$$

hence it is a group of order 4. Therefore, by the classification of groups of order 4, G/N must be abelian.

Exercise 4
Prove that in the quotient group G/N, $(gN)^\alpha = g^\alpha N$ for all $\alpha \in \mathbb{Z}$.

Solution
First, recall that $\varphi : G \to G/N$ defined by $g \mapsto gN$ is a homomorphism. Hence, for all $\alpha \in \mathbb{Z}$, we have:

$$\varphi(g^\alpha) = \varphi(g)^\alpha$$

which is equivalent to

$$(gN)^\alpha = g^\alpha N$$

by the definition of φ.

Exercise 5
Use the preceding exercise to prove that the order of the element gN in G/N is n, where n is the smallest positive integer such that $g^n \in N$ (and gN has infinite order if no such positive integer exists). Give an example to show that the order of gN in G/N may be strictly smaller than the order of g in G.

Solution
By the definition and by the preceding exercise, $|gN|$ is the smallest natural number n such that $g^nN = (gN)^n = 1_{G/N} = N$. Let's prove that $g^nN = N$ iff $g^n \in N$. Obviously, if $g^nN = N$, then $g^n \in g^nN$ implies that $g^n \in N$. Moreover, if $g^n \in N$, then by Proposition 4, it must be that $g^nN = N$ since $1^{-1}g^n \in N$. Therefore, $|gN|$ is the smallest natural number n such that $g^n \in N$.
To give an example of a group G and a normal subgroup N such that an element of G has an order strictly greater than its associated element in G/N, consider $G = \mathbb{Z}$, $N = 3\mathbb{Z}$ and the element $2 \in G$. Obviously, 2 has infinite order in G but $2 + N = \overline{2}$ has order 3 in $G/N = \mathbb{Z}/3\mathbb{Z}$.

Exercise 6
Define $\varphi : \mathbb{R}^\times \to \{\pm 1\}$ by letting $\varphi(x)$ be x divided by the absolute value of x. Describe the fibers of φ and prove that φ is a homomorphism.

Solution
Notice that the fibers of φ are $\varphi^{-1}(1)$ and $\varphi^{-1}(-1)$. For the first one, we have

$$\begin{aligned} x \in \varphi^{-1}(1) &\iff \varphi(x) = 1 \\ &\iff \frac{x}{|x|} = 1 \\ &\iff x = |x| \\ &\iff x \geq 0 \end{aligned}$$

Similarly, $x \in \varphi^{-1}(-1)$ if and only if $x \leq 0$. Therefore, the fibers of φ are exactly the set of positive reals and the set of negative reals.
To show that φ is a homomorphism, let x and y be arbitrary elements of $\mathbb{R}^\times$ and notice that

$$\begin{aligned} \varphi(xy) &= \frac{xy}{|xy|} \\ &= \frac{x}{|x|} \cdot \frac{y}{|y|} \\ &= \varphi(x)\varphi(y) \end{aligned}$$

Therefore, φ is a homomorphism.

Exercise 7
Define $\pi : \mathbb{R}^2 \to \mathbb{R}$ by $\pi((x, y)) = x + y$. Prove that π is a surjective homomorphism and describe the kernel and the fibers of π geometrically.

Solution
Obviously, π is surjective since for all $y \in \mathbb{R}$, we have $\pi((x,0)) = x + 0 = x$. Moreover, it is a homomorphism since for all $(x_1, y_1), (x_2, y_2) \in \mathbb{R}^2$, we have

$$\begin{aligned}\pi((x_1, y_1) + (x_2, y_2)) &= \pi((x_1 + x_2, y_1 + y_2)) \\ &= (x_1 + x_2) + (y_1 + y_2) \\ &= (x_1 + y_1) + (x_2 + y_2) \\ &= \pi((x_1, y_1)) + \pi((x_2, y_2))\end{aligned}$$

Geometrically, since $\ker \pi$ is the set

$$\{(x, y) \in \mathbb{R}^2 \mid x + y = 0\}$$

which corresponds to the graph of the function $x \mapsto -x$. More generally, the fiber of a corresponds to the graph of the function $x \mapsto a - x$ since

$$\begin{aligned}\pi^{-1}(a) &= \{(x, y) \in \mathbb{R}^2 \mid x + y = a\} \\ &= \{(x, y) \in \mathbb{R}^2 \mid y = a - x\}\end{aligned}$$

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

Exercise 8
Let $\varphi : \mathbb{R}^\times \to \mathbb{R}^\times$ be the map sending x to the absolute value of x. Prove that φ is a homomorphism and find the image of φ. Describe the kernel and the fibers of φ.

Solution
First, to show that φ is a homomorphism, let $x, y \in \mathbb{R}^\times$ and notice that

$$\varphi(xy) = |xy| = |x| \cdot |y| = \varphi(x)\varphi(y)$$

To find the image, notice that $\varphi(x) \in \mathbb{R}^\times_{\geq 0}$ for all $x \in \mathbb{R}^\times$. Moreover, for all $x \in \mathbb{R}^\times_{\geq 0}$, we have $x = \varphi(x) \in \operatorname{im} \varphi$. Therefore, $\operatorname{im} \varphi = \mathbb{R}^\times_{\geq 0}$.
The elements x in kernel satisfy the equation $|x| = 1$, so the elements in the kernel are exactly 1 and -1. Similarly, for all $a \in \operatorname{im} \varphi$, the elements in the fiber of a are exactly a and $-a$.

Exercise 9
Define $\varphi : \mathbb{C}^\times \to \mathbb{R}^\times$ by $\varphi(a + bi) = a^2 + b^2$. Prove that φ is a homomorphism and find the image of φ. Describe the kernel and the fibers of φ geometrically (as subsets of the plane).

Solution
To prove that φ is a homomorphism, let $x, y \in \mathbb{C}^\times$, then there exist $x_1, x_2, y_1, y_2 \in \mathbb{R}$

such that $x = x_1 + x_2 i$ and $y = y_1 + y_2 i$. Hence, we get

$$\begin{aligned}
\varphi(xy) &= \varphi((x_1 + x_2 i)(y_1 + y_2 i)) \\
&= \varphi((x_1 y_1 - x_2 y_2) + (x_1 y_2 + x_2 y_1) i) \\
&= (x_1 y_1 - x_2 y_2)^2 + (x_1 y_2 + x_2 y_1)^2 \\
&= x_1^2 y_1^2 - 2 x_1 x_2 y_1 y_2 + x_2^2 y_2^2 + x_1^2 y_2^2 + 2 x_1 x_2 y_1 y_2 + x_2^2 y_1^2 \\
&= x_1^2 y_1^2 + x_2^2 y_2^2 + x_1^2 y_2^2 + x_2^2 y_1^2 \\
&= (x_1^2 + x_2^2)(y_1^2 + y_2^2) \\
&= \varphi(x_1 + x_2 i)\varphi(y_1 + y_2 i) \\
&= \varphi(x)\varphi(y)
\end{aligned}$$

Notice that φ is surjective since for any $x \in \mathbb{R}^\times$, we can attain x as an output of φ with

$$\varphi(\sqrt{x} + 0i) = \sqrt{x}^2 + 0^2 = x$$

Therefore, $\operatorname{im} \varphi = \mathbb{R}^\times$.
Concerning fibers of φ, for any $a \in \mathbb{R}^\times$, we have

$$\begin{aligned}
\varphi^{-1}(a) &= \{x + yi \in \mathbb{C}^\times \mid \varphi(x + yi) = a\} \\
&= \{x + yi \in \mathbb{C}^\times \mid x^2 + y^2 = a\} \\
&= \{(x, y) \in \mathbb{R} \mid x^2 + y^2 = a\}
\end{aligned}$$

which corresponds to the circle of radius $\sqrt{a}$ on the plane. Thus, the kernel corresponds to the unit circle on the plane.

Exercise 10
Let $\varphi : \mathbb{Z}/8\mathbb{Z} \to \mathbb{Z}/4\mathbb{Z}$ by $\varphi(\overline{a}) = \overline{a}$. Show that this is a well-defined, surjective homomorphism and describe the fibers and kernel explicitly (showing that φ is well defined involves the fact that $\overline{a}$ has a different meaning in the domain and range of φ).

Solution
First, to make it unambiguous, let's denote by $[a]_8$ the elements in $\mathbb{Z}/8\mathbb{Z}$ and by $[a]_4$ the elements in $\mathbb{Z}/4\mathbb{Z}$ instead of $\overline{a}$ for both. Hence, with this notation, we get that φ is defined by the mapping

$$[a]_8 \mapsto [a]_4$$

To show that it is well-defined, let $[x]_8, [y]_8 \in \mathbb{Z}/8\mathbb{Z}$ such that $[x]_8 = [y]_8$, then

$$\begin{aligned}
[x]_8 = [y]_8 &\implies 8 \mid x - y \\
&\implies 4 \mid x - y \\
&\implies [x]_4 = [y]_4 \\
&\implies \varphi(x) = \varphi(y)
\end{aligned}$$

Hence, φ is well-defined. It directly follows that φ is surjective since for all $y = [a]_4 \in \mathbb{Z}/4\mathbb{Z}$, if we let $x = [a]_8$, then we get

$$\varphi(x) = \varphi([a]_8) = [a]_4 = y$$

To show that it is a homomorphism, simply notice that for all $[a]_8, [b]_8 \in \mathbb{Z}/8\mathbb{Z}$, we have

$$\begin{aligned}\varphi([a]_8 + [b]_8) &= \varphi([a+b]_8) \\ &= [a+b]_4 \\ &= [a]_4 + [b]_4 \\ &= \varphi([a]_8) + \varphi([b]_8)\end{aligned}$$

Therefore, φ is a well-defined, surjective homomorphism.
Explicitly, the fibers of φ are

$$\begin{aligned}\varphi^{-1}([0]_4) &= \{[0]_8,\ [4]_8\} \\ \varphi^{-1}([1]_4) &= \{[1]_8,\ [5]_8\} \\ \varphi^{-1}([2]_4) &= \{[2]_8,\ [6]_8\} \\ \varphi^{-1}([3]_4) &= \{[3]_8,\ [7]_8\}\end{aligned}$$

Exercise 11
Let F be a field and let $G = \{\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mid a, b, c \in F,\ a, c \neq 0\} \leq GL_2(F)$.

(a) Prove that the map $\varphi : \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mapsto a$ is a surjective homomorphism from G onto $F^\times$ (recall that $F^\times$ is the multiplicative group of nonzero elements in F). Describe the fibers and kernel of φ.

(b) Prove that the map $\psi : \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mapsto (a, c)$ is a surjective homomorphism from G onto $F^\times \times F^\times$. Describe the fibers and kernel of ψ.

(c) Let $H = \{\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \mid b \in F\}$. Prove that H is isomorphic to the additive group F.

Solution

(a) First, let's show that it is a homomorphism. For all $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}, \begin{pmatrix} d & e \\ 0 & f \end{pmatrix} \in G$, we have

$$\begin{aligned}\varphi\left(\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}\begin{pmatrix} d & e \\ 0 & f \end{pmatrix}\right) &= \varphi\left(\begin{pmatrix} ad & ae+bf \\ 0 & cf \end{pmatrix}\right) \\ &= ad \\ &= \varphi\left(\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}\right)\varphi\left(\begin{pmatrix} d & e \\ 0 & f \end{pmatrix}\right)\end{aligned}$$

Hence, it is a homomorphism. To show that it is surjective, let $a \in F^\times$ be an arbitrary element and define $X = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} = aI_3$, then obviously, $X \in G$ since it is invertible (its inverse is $a^{-1}I_3$). Moreover,

$$\varphi(X) = \varphi\left(\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}\right) = a$$

Thus, it is surjective since for all $a \in F^\times$, there is an $X \in G$ satisfying $\varphi(X) = a$.
For a given $a \in F^\times$, the fiber of a is the set

$$\{\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mid b \in F \text{ and } c \in F^\times\}$$

Hence, the kernel is exactly the set of matrices of the form

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

where b and c are any elements of F with $c \neq 0$.

(b) First, let's show that it is a homomorphism. Let $X = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$ and $Y = \begin{pmatrix} d & e \\ 0 & f \end{pmatrix}$ be elements of G, then we have

$$\begin{aligned}
\psi(XY) &= \psi\left(\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}\begin{pmatrix} d & e \\ 0 & f \end{pmatrix}\right) \\
&= \psi\left(\begin{pmatrix} ad & ae+bf \\ 0 & cf \end{pmatrix}\right) \\
&= (ad, cf) \\
&= (a,c)(d,f) \\
&= \psi\left(\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}\right)\psi\left(\begin{pmatrix} d & e \\ 0 & f \end{pmatrix}\right) \\
&= \psi(X)\psi(Y)
\end{aligned}$$

Hence, it is a homomorphism. To show that it is surjective, let $(a,c) \in F^\times \times F^\times$ be an arbitrary element and define $X = \begin{pmatrix} a & 0 \\ 0 & c \end{pmatrix}$, then obviously, $X \in G$ since it is invertible (its determinant is $ac \neq 0$). Moreover,

$$\psi(X) = \psi\left(\begin{pmatrix} a & 0 \\ 0 & c \end{pmatrix}\right) = (a,c)$$

Thus, it is surjective since for all $(a,c) \in F^\times$, there is an $X \in G$ satisfying $\varphi(X) = (a,c)$.
For a given $(a,c) \in F^\times$, the fiber of (a,c) is the set

$$\{\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mid b \in F\}$$

Hence, the kernel is exactly the set of matrices of the form

$$\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$$

where b is any elements of F.

(c) First, define the function $\varphi : H \to F$ by $\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \mapsto b$. Let's prove first that it is a homomorphism. Let $X = \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$ and $Y = \begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix}$ be elements of H, then we have

$$\begin{aligned} \varphi(XY) &= \varphi\left(\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix}\right) \\ &= \varphi\left(\begin{pmatrix} 1 & x+y \\ 0 & 1 \end{pmatrix}\right) \\ &= x + y \\ &= \varphi\left(\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}\right) + \varphi\left(\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}\right) \\ &= \varphi(X) + \varphi(Y) \end{aligned}$$

Obviously, it is surjective since for all $b \in F$, we have

$$\varphi\left(\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}\right) = b$$

Moreover, it is also injective since for all $X = \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$ and $Y = \begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix}$ in H, we have

$$\begin{aligned} \varphi(X) = \varphi(Y) &\implies \varphi\left(\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}\right) = \varphi\left(\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}\right) \\ &\implies x = y \\ &\implies \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \\ &\implies X = Y \end{aligned}$$

Therefore, $H \cong F$ since φ is a bijective homomorphism.

Exercise 12
Let G be the additive group of real numbers, let H be the multiplicative group of complex numbers of absolute value 1 (the unit circle S^1 in the complex plane) and let $\varphi : G \to H$ be the homomorphism $\varphi : r \mapsto e^{2\pi i r}$. Draw the points on a real line which lie in the kernel of φ. Describe similarly the elements in the fibers of φ above the points -1, i and $e^{4\pi i/3}$ of H.

Solution
First, let's determine the elements in the kernel of φ. For all $x \in G$, we have

$$\begin{aligned} x \in \ker\varphi &\iff \varphi(x) = 1 \\ &\iff e^{2\pi x i} = 1 \\ &\iff 2\pi x \in 2\pi\mathbb{Z} \\ &\iff x \in \mathbb{Z} \end{aligned}$$

Hence, on the real line, the kernel of φ corresponds to the integer points.
Using Proposition 2, we only to find one element x in $\varphi^{-1}(a)$ to determine that $\varphi^{-1}(a)$ is the set $x + \mathbb{Z}$. For $a = -1$, we know that

$$\varphi(1/2) = e^{2\pi i/2} = e^{i\pi} = -1$$

so it follows that $\varphi^{-1}(-1) = 1/2 + \mathbb{Z}$. Similarly, since

$$\varphi(1/4) = e^{2\pi i/4} = e^{i\pi/2} = i$$

we have that $\varphi^{-1}(i) = 1/4 + \mathbb{Z}$. Finally, since

$$\varphi(2/3) = e^{2(2\pi i)/3} = e^{4\pi i/3}$$

we have that $\varphi^{-1}(i) = 2/3 + \mathbb{Z}$.

Exercise 13
Repeat the preceding exercise with the map φ replaced by the map $\varphi : r \mapsto e^{4\pi ir}$.

Solution
First, let's determine the elements in the kernel of φ. For all $x \in G$, we have

$$\begin{aligned} x \in \ker\varphi &\iff \varphi(x) = 1 \\ &\iff e^{4\pi xi} = 1 \\ &\iff 4\pi x \in 2\pi\mathbb{Z} \\ &\iff x \in \frac{1}{2}\mathbb{Z} \end{aligned}$$

Hence, on the real line, the kernel of φ corresponds to the integers points scaled by down by a factor of $1/2$.
Using Proposition 2, and a similar reasoning as in the previous exercise, since we know that

$$\varphi(1/4) = e^{4\pi i/4} = e^{i\pi} = -1$$

then it follows that $\varphi^{-1}(-1) = \frac{1}{4} + \frac{1}{2}\mathbb{Z}$. Similarly, since

$$\varphi(1/8) = e^{4\pi i/8} = e^{i\pi/2} = i$$

we have that $\varphi^{-1}(i) = \frac{1}{8} + \frac{1}{2}\mathbb{Z}$. Finally, since

$$\varphi(1/3) = e^{4\pi i/3}$$

we have that $\varphi^{-1}(i) = \frac{1}{3} + \frac{1}{2}\mathbb{Z}$.

Exercise 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 $0 \leq q < 1$.

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

(c) Show that $\mathbb{Q}/\mathbb{Z}$ is the torsion subgroup of $\mathbb{R}/\mathbb{Z}$ (cf. Exercise 6, Section 2.1).

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

Solution

(a) Let $\frac{a}{b}+\mathbb{Z} \in \mathbb{Q}/\mathbb{Z}$, by the Division Algorithm, there exist integers q and r such that $a = qb + r$ with $0 \leq r \leq b-1$. Hence:

$$\begin{aligned}\frac{a}{b}+\mathbb{Z} &= \frac{qb+r}{b}+\mathbb{Z}\\ &= \left(\frac{r}{b}+q\right)+\mathbb{Z}\\ &= \left(\frac{r}{b}+\mathbb{Z}\right)+(q+\mathbb{Z})\\ &= \left(\frac{r}{b}+\mathbb{Z}\right)+(0+\mathbb{Z})\\ &= \left(\frac{r}{b}\right)+\mathbb{Z}\end{aligned}$$

Thus, r/b is a representative of $\frac{a}{b}+\mathbb{Z}$ and since $0 \leq r \leq b-1$, then we must have that $0 \leq r/b < 1$.

(b) Let $\frac{\overline{a}}{b} \in \mathbb{Q}/\mathbb{Z}$, then it is easy to see that it has finite order since

$$b\left(\frac{\overline{a}}{b}\right) = \overline{\left(b\frac{a}{b}\right)} = \overline{a} = \overline{0}$$

which implies that $\left|\frac{\overline{a}}{b}\right| \leq b < \infty$ Moreover, for any $n \in \mathbb{N}$, we can easily find an element of order bigger than n, namely : $1/n$. It follows from the fact that if we denote $m = \left|\frac{\overline{1}}{n}\right|$, then we have

$$\begin{aligned}m\left(\frac{\overline{1}}{n}\right) = \overline{0} &\implies \overline{\left(\frac{m}{n}\right)} = \overline{0}\\ &\implies \frac{m}{n} \in \mathbb{Z}\\ &\implies n \mid m\\ &\implies n \leq m\end{aligned}$$

The last implication follows from the fact that both m and n are positive. Moreover, notice that we could have proved that $n = m$ but it is not necessary to prove what is asked. Hence, we can find elements of arbitrarily large order.

(c) Let T be the torsion group of $\mathbb{R}/\mathbb{Z}$, then from the previous part, we have that

$$\mathbb{Q}/\mathbb{Z} \leq T$$

To show the reverse inclusion, let $t \in T$, then $t = \overline{r}$ where $r \in \mathbb{R}$. Moreover, by definition of T, there is a $n \in \mathbb{N}$ such that $nt = \overline{nr} = \overline{0}$. But this implies

that

$$\begin{aligned} \overline{nr} = \overline{0} &\implies nr \in \mathbb{Z} \\ &\implies nr = k, \quad \text{for some } k \in \mathbb{Z} \\ &\implies r = \frac{n}{k} \\ &\implies r \in \mathbb{Q} \\ &\implies t \in \mathbb{Q}/\mathbb{Z} \end{aligned}$$

Therefore, $\mathbb{Q}/\mathbb{Z}$ is the torsion group of $\mathbb{R}/\mathbb{Z}$.

(d) First, recall that

$$U = \{e^{2\pi ik/n} \mid n \in \mathbb{N} \text{ and } 0 \leq k \leq n-1\}$$

where U denotes the multiplicative group of roots of unity in $\mathbb{C}^\times$. Define the map $\varphi : \mathbb{Q}/\mathbb{Z} \to U$ by $\frac{\overline{k}}{n} \mapsto e^{2\pi ik/n}$ where $\frac{k}{n}$ is the unique representative of the $\frac{\overline{k}}{n}$ in the range $[0, 1)$. By uniqueness of this representative (proved in part a), the map is well-defined. From this, we can prove that for all $\frac{\overline{a}}{n} \in \mathbb{Q}/\mathbb{Z}$ (where a/b is not necessarily between 0 and 1), we have

$$\varphi\left(\frac{\overline{a}}{b}\right) = e^{2\pi ia/b}$$

To prove this, notice that by the Division Algorithm, we have that $a = qb + r$ which implies that $\frac{\overline{a}}{b} = \frac{\overline{r}}{b}$. Moreover, since $0 \leq \frac{r}{b} < 1$, then $\frac{r}{b}$ is the unique representative of $\frac{\overline{a}}{b}$ between 0 and 1. Thus, we get:

$$\begin{aligned} \varphi\left(\frac{\overline{a}}{b}\right) &= \varphi\left(\frac{\overline{r}}{b}\right) \\ &= e^{i\frac{2\pi r}{b}} \\ &= e^{i\frac{2\pi r}{b} + 2\pi iq} \\ &= e^{2\pi i\left(\frac{r}{b} + q\right)} \\ &= e^{2\pi i\frac{qb+r}{b}} \\ &= e^{i\frac{2\pi a}{b}} \end{aligned}$$

This will make some computations easier.
Let's now show that it is a homomorphism. To do so, let $\frac{\overline{a}}{b}, \frac{\overline{c}}{d} \in \mathbb{Q}/\mathbb{Z}$ and notice that

$$\begin{aligned} \varphi\left(\frac{\overline{a}}{b} + \frac{\overline{c}}{d}\right) &= \varphi\left(\overline{\frac{a}{b} + \frac{c}{d}}\right) \\ &= \varphi\left(\overline{\frac{ad+bc}{bd}}\right) \\ &= e^{2\pi i\frac{ad+bc}{bd}} \\ &= e^{2\pi i\left(\frac{a}{b} + \frac{c}{d}\right)} \\ &= e^{i\frac{2\pi a}{b}} e^{i\frac{2\pi c}{d}} \\ &= \varphi\left(\frac{\overline{a}}{b}\right)\varphi\left(\frac{\overline{c}}{d}\right) \end{aligned}$$

Therefore, φ is a homomorphism.
Let's now prove that it is a bijection. Obviously, the map is surjective since for any $e^{2\pi ik/n} \in U$, we have the element $\overline{\frac{k}{n}} \in \mathbb{Q}/\mathbb{Z}$ that maps to $e^{2\pi ik/n}$ by φ. To prove the injectivity, since it is a homomorphism, we can simply prove that the kernel is trivial. Hence, let $\overline{\frac{a}{b}} \in \ker\varphi$, then

$$\begin{aligned}
\varphi\left(\overline{\frac{a}{b}}\right) = 1 &\implies e^{i\frac{2\pi a}{b}} = 1 \\
&\implies 2\pi i\frac{a}{b} = 2\pi ik, \qquad \text{for some } k \in \mathbb{Z} \\
&\implies \frac{a}{b} = k \in \mathbb{Z} \\
&\implies \overline{\frac{a}{b}} = \overline{0}
\end{aligned}$$

which proves injectivity. Therefore, since φ is a bijective homomorphism, we get that $\mathbb{Q}/\mathbb{Z} \cong U$.

Exercise 15
Prove that the quotient of a divisible abelian group by any proper subgroup is also divisible. Deduce that $\mathbb{Q}/\mathbb{Z}$ is divisible (cf. Exercise 19, Section 2.4).

Solution
To prove it, let A be a divisible abelian group and B a proper subgroup of A, then by definition, for all $a \in A$ and $k \in \mathbb{Z} \setminus \{0\}$, there is an $x \in A$ such that $x^k = a$. Now, let $aB \in A/B$ and $k \in \mathbb{Z} \setminus \{0\}$, then there is an $x \in A$ such that $x^k = a$. With cosets, this means that $(xB)^k = (x^k)B = aB$. Moreover, B is a proper subgroup of A so A/B is nontrivial. Therefore, A/B is divisible.
From this, it is easy to see that $\mathbb{Q}/\mathbb{Z}$ is divisible using the fact that $\mathbb{Q}$ is divisible and the fact that $\mathbb{Z}$ is a proper subgroup of $\mathbb{Q}$.

Exercise 16
Let G be a group, let N be a normal subgroup of G and let $\overline{G} = G/N$. Prove that if $G = \langle x, y\rangle$, then $\overline{G} = \langle \overline{x}, \overline{y}\rangle$. Prove more generally that if $G = \langle S\rangle$ for any subset S of G, then $\overline{G} = \langle \overline{S}\rangle$.

Solution
For the first claim, suppose that $G = \langle x, y\rangle$, then this means that any element of G can be written using only x, x^{-1}, y and y^{-1}. Let $\overline{g} \in \overline{G}$, since g can be written as $x^{a_1}y^{b_1}...x^{a_n}y^{b_n}$ for some $n \in \mathbb{N}$ and integers $a_i, b_i \in \mathbb{Z}$, then it follows that

$$\overline{g} = \overline{x^{a_1}y^{b_1}...x^{a_n}y^{b_n}} = \overline{(x^{a_1})} \cdot \overline{(y^{b_1})} \cdot ... \cdot \overline{(x^{a_n})} \cdot \overline{(y^{a_n})} = (\overline{x})^{a_1}(\overline{y})^{b_1}...(\overline{x})^{a_n}(\overline{y})^{b_n}$$

Hence, $\overline{g}$ can be written as a combination of $\overline{x}$ and $\overline{y}$. Thus, $\overline{G} \leq \langle \overline{x}, \overline{y}\rangle$. Therefore, $\overline{G} = \langle \overline{x}, \overline{y}\rangle$. If we replace $\{x, y\}$ be any subset S of G, the proof is precisely the same up to some variable names.

Exercise 17
Let G be the dihedral group of order 16 (whose lattice appears in Section 2.5):

$$G = \langle r, s \mid r^8 = s^2 = 1,\ rs = sr^{-1}\rangle$$

and let $\overline{G} = G/\langle r^4 \rangle$ be the quotient of G by the subgroup generated by r^4 (this subgroup is the center of G, hence is normal).

(a) Show that the order of $\overline{G}$ is 8.

(b) Exhibit each element of $\overline{G}$ in the form $\overline{s}^a\overline{r}^b$, for some integers a and b.

(c) Find the order of each of the elements of $\overline{G}$ exhibited in (b).

(d) Write each of the following elements of $\overline{G}$ in the form $\overline{s}^a\overline{r}^b$, for some integers a and b as in (b): $\overline{rs}$, $\overline{sr^{-2}s}$, $\overline{s^{-1}r^{-1}sr}$

(e) Prove that $\overline{H} = \langle \overline{s}, \overline{r}^2 \rangle$ is a normal subgroup of $\overline{G}$ and $\overline{H}$ is isomorphic to the Klein 4-group. Describe the isomorphism type of the complete preimage of $\overline{H}$ in $\overline{G}$.

(f) Find the center of $\overline{G}$ and describe the isomorphism type of $\overline{G}/Z(\overline{G})$.

Solution

(a) Each element of $\overline{G}$ is a coset of $\{1, r^4\}$, hence a set of order 2. Moreover, the cosets form a partition of G so there can only be 8 of them ($16/2 = 8$).

(b) The elements of $\overline{G}$ are the following:

- $\{1,\ r^4\} = \overline{1} = \overline{s}^0 \cdot \overline{r}^0$
- $\{r,\ r^5\} = \overline{r} = \overline{s}^0 \cdot \overline{r}^1$
- $\{r^2,\ r^6\} = \overline{r}^2 = \overline{s}^0 \cdot \overline{r}^2$
- $\{r^3,\ r^7\} = \overline{r}^3 = \overline{s}^0 \cdot \overline{r}^3$
- $\{s,\ sr^4\} = \overline{s} = \overline{s}^1 \cdot \overline{r}^0$
- $\{sr,\ sr^5\} = \overline{s} \cdot \overline{r} = \overline{s}^1 \cdot \overline{r}^1$
- $\{sr^2,\ sr^5\} = \overline{s} \cdot \overline{r}^2 = \overline{s}^1 \cdot \overline{r}^2$
- $\{sr^3,\ sr^5\} = \overline{s} \cdot \overline{r}^3 = \overline{s}^1 \cdot \overline{r}^3$

(c) Orders of elements in $\overline{G}$:

- $|\overline{1}| = 1$
- $|\overline{r}| = 4$
- $|\overline{r}^2| = 2$
- $|\overline{r}^3| = 4$
- $|\overline{s}| = 2$
- $|\overline{s} \cdot \overline{r}| = 2$
- $|\overline{s} \cdot \overline{r}^2| = 2$
- $|\overline{s} \cdot \overline{r}^3| = 2$

(d)

- $\overline{rs} = \overline{sr^{-1}} = \overline{sr^7} = \overline{sr^3} = \overline{s}^1 \cdot \overline{r}^3$
- $\overline{sr^{-2}s} = \overline{r^2} = \overline{s}^0 \cdot \overline{r}^2$
- $\overline{s^{-1}r^{-1}sr} = \overline{r^2} = \overline{s}^0 \cdot \overline{r}^2$

(e) To do so, first notice that $\overline{G} \cong D_8$ since $\overline{G} = \langle \overline{s}, \overline{r} \rangle$, it has order 8 and $\overline{s}$ and $\overline{r}$ satisfy the same relations as s and r in D_8. Hence, $\langle \overline{s}, \overline{r}^2 \rangle \cong \langle s, r^2 \rangle$, we also showed in the previous chapter that the normalizer of $\langle s, r^2 \rangle$ is D_8. Thus, the normalizer of $\langle \overline{s}, \overline{r}^2 \rangle$ is G which implies that it is normal. Finaly, since $\langle s, r^2 \rangle \cong V_4$, then $\langle \overline{s}, \overline{r} \rangle \cong V_4$.

(f) Using the fact that $\overline{G} \cong D_8$ and the fact that $Z(D_8) = \langle r^2 \rangle$, then we get $Z(\overline{G}) = \langle \overline{r}^2 \rangle$. Moreover, in the same way we showed that $D_{16}/\langle r^4 \rangle \cong D_8$, we have that $D_8/\langle r^2 \rangle \cong D_4$. Therefore,

$$\overline{G}/Z(\overline{G}) \cong D_8/\langle r^2 \rangle \cong D_4 \cong \mathbb{Z}/4\mathbb{Z}$$

3.2 More on Cosets and Lagrange's Theorem

Heyy...

Part II

RING THEORY

Chapter 4

Introduction to Rings

Appendix I

Cartesian Products and Zorn's Lemma

I.1 Cartesian Products

Exercise 1
Let I and J be any two indexing sets and let A be an arbitrary set. For any function $\varphi : J \to I$ define

$$\varphi^* : \prod_{i\in I} A \to \prod_{i\in I} A \qquad \text{by} \qquad \varphi^*(f) = f \circ \varphi \ \text{ for all choice functions } f \in \prod_{i\in I} A$$

(a) Let $I = \{1, 2\}$, let $J = \{1, 2, 3\}$ and let $\varphi : J \to I$ be defined by $\varphi(1) = 2$, $\varphi(2) = 2$ and $\varphi(3) = 1$. Describe explicitly how an ordered pair in $A \times A$ maps to a 3-tuple in $A \times A \times A$ under this φ^*.

(b) Let $I = J = \{1, 2, \ldots, n\}$ and assume φ is a permutation of I. Describe in terms of n-tuples in $A \times A \times \cdots \times A$ the function φ^*.

Solution

(a) Let f be an arbitrary element of A^I, then there exist elements a_1 and a_2 in A such that

$$f(1) = a_1 \qquad f(2) = a_2$$

or simply

$$f \sim (a_1, a_2)$$

By definition, notice that

- $\varphi^*(f)(1) = (f \circ \varphi)(1) = f(\varphi(1)) = f(2) = a_2$
- $\varphi^*(f)(2) = (f \circ \varphi)(2) = f(\varphi(2)) = f(2) = a_2$
- $\varphi^*(f)(3) = (f \circ \varphi)(3) = f(\varphi(3)) = f(1) = a_1$

Hence, as a 3-tuple, we can represent $\varphi^*(f)$ as (a_2, a_2, a_1).

(b) Let f be an arbitrary element in A^n, then there exist elements $a_1, \ldots, a_n$ in A such that $f(i) = a_i$ for all $i \in I$. For each $i \in I$, we have

$$\varphi^*(f)(i) = (f \circ \varphi)(i) = f(\varphi(i)) = a_{\varphi(i)}$$

Hence, we can represent $\varphi^*(f)$ as $(a_{\varphi(1)}, \ldots, a_{\varphi(n)})$ which is simply the φ-permutation of the n-tuple $(a_1, \ldots, a_n)$ that represents f.

I.2 Partially Ordered Sets and Zorn's Lemma

Exercise 1
Let A be the collection of all finite subsets of $\mathbb{R}$ ordered by inclusion. Discuss the existence (or nonexistence) of upperbounds, minimal and maximal elements (where minimal elements are defined analogously to maximal elements). Explain why this is not a well ordering.

Solution
If B is a subset of A, then B has an upperbound if and only if $\bigcup B$ is a finite subset of $\mathbb{R}$ since any upperbound of B must contain $\bigcup B$.
Concerning maximal elements, if m is in A, then m is finite so there must be a real number r such that $r \notin m$. Thus, $m' = m \cup \{r\}$ satisfies $m \subsetneq m'$ which directly implies that m is not maximal. Therefore, since m is arbitrary, A has no maximal element.
Concerning minimal elements, simply notice that $\varnothing$ is a finite subset of $\mathbb{R}$ that satisfies the fact that any $m \subseteq \varnothing$ must be the empty set itself. Therefore, A has a minimal element.
Lastly, A is not well ordered under inclusion since singletons in A are not comparable.

Exercise 2
Let A be the collection of all infinite subsets of $\mathbb{R}$ ordered by inclusion. Discuss the existence (or nonexistence) of upperbounds, minimal and maximal elements. Explain why this is not a well ordering.

Solution
Concerning upperbounds, notice that any $B \subseteq A$ is bounded above by $\mathbb{R}$ itself since it is an infinite subset of $\mathbb{R}$ that contains all of its subsets.
Concerning minimal elements, let $m \in A$, then m is an infinite subset of $\mathbb{R}$. Thus, there is a real number r such that $r \in m$. Consider the set $m' = m - \{r\}$ and notice that m' is an infinite subset of $\mathbb{R}$ as well that satisfies $m' \subsetneq m$ which directly implies that m is not minimal. Since it holds for all m in A, then A has no minimal element.
Concerning maximal elements notice that $\mathbb{R}$ is an element of A and if $m \in A$ satisfies $\mathbb{R} \subseteq m$, then it directly follows that $m = \mathbb{R}$. Thus, $\mathbb{R}$ is a maximal element in A.
Lastly, A is not well ordered under inclusion since both $[0, 1]$ and $[2, 3]$ are in A but are not comparable.

Exercise 3
Show that the following partial orderings on the given sets are not well orderings:

(a) $\mathbb{R}$ under the usual relation $\leq$.

(b) $\mathbb{R}^+$ under the usual relation $\leq$.

(c) $\mathbb{R}^+ \cup \{0\}$ under the usual relation $\leq$.

(d) $\mathbb{Z}$ under the usual relation $\leq$.

Solution

(a) It is not a well ordering because the set $\mathbb{R}$ has no minimum.

(b) It is not a well ordering because $(0, 1)$ has no minimum.

(c) It is not a well ordering because $(0, 1)$ has no minimum.

(d) It is not a well ordering because $\mathbb{Z}$ has no minimum.

Exercise 4
Show that $\mathbb{Z}^+$ is well ordered under the usual relation $\leq$.

Solution
This was proved by induction in Exercise 6 of Section 0.2.