Selected Solutions to Dummit and Foote's Abstract Algebra Third Edition

Greg Kikola

July 9, 2020

This document lives at:

https://www.gregkikola.com/projects/guides/

You can find the LaTeX source code on GitHub at:

https://github.com/gkikola/sol-dummit-foote

Contents

Preface

This is an unofficial solution guide to the book *Abstract Algebra*, Third Edition, by David S. Dummit and Richard M. Foote. It is intended for students who are studying algebra with Dummit and Foote's text. I encourage students who use this guide to first attempt each exercise for themselves before looking up the solution, as doing exercises is an essential part of learning mathematics.

In writing this guide, I have avoided using techniques or results before the point at which they are introduced in the text. My solutions should therefore be accessible to someone who is reading through Dummit and Foote for the first time.

Given the large number of exercises, errors are unavoidable in a work such as this. I have done my best to proofread each solution, but mistakes will make it through nonetheless. If you find one, please feel free to tell me about it in an email: gkikola@gmail.com. I appreciate any corrections or feedback.

Please know that this guide is currently unfinished. I am slowly working on adding the remaining chapters, but this will be done at my own pace. If you need a solution to an exercise that I have not included, try typing the problem statement into a web search engine such as Google; it is likely that someone else has already posted a solution.

I am deeply grateful to the authors, David S. Dummit and Richard M. Foote, for producing a wonderfully comprehensive and thoroughly well-written work. I also owe particular thanks to those readers who have taken the time to contact me in order to point out mistakes or to give general feedback.

Greg Kikola
www.gregkikola.com
gkikola@gmail.com

Chapter 0

Preliminaries

0.1 Basics

Let $\mathcal{A}$ be the set of 2×2 matrices over $\mathbb{R}$, let

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

and let

$$\mathcal{B} = \{X \in \mathcal{A} \mid MX = XM\}.$$

0.1.1 Exercise 1

Determine which of the following elements of $\mathcal{A}$ lie in $\mathcal{B}$:

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Solution. It is easy to verify that

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \quad \text{and} \quad \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

all commute with M: the first matrix is M itself, and the latter two are the zero matrix and the identity matrix, all of which will commute. So each of these matrices is in $\mathcal{B}$.

We can check the remaining matrices individually: Let

$$P = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}, \quad Q = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \quad \text{and} \quad R = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Direct computation shows that

$$MP = \begin{pmatrix} 2 & 2 \\ 1 & 1 \end{pmatrix} \neq \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix} = PM,$$

$$MQ = \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix} \neq \begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix} = QM,$$

and

$$MR = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \neq \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} = RM.$$

So $P, Q, R \notin \mathcal{B}$. □

0.1.2 Exercise 2

Prove that if $P, Q \in \mathcal{B}$, then $P + Q \in \mathcal{B}$.

Proof. Let

$$P = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \quad \text{and} \quad Q = \begin{pmatrix} e & f \\ g & h \end{pmatrix}$$

be matrices in the set $\mathcal{B}$, so that $MP = PM$ and $MQ = QM$. Then we have

$$\begin{aligned} M(P+Q) &= \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a+e & b+f \\ c+g & d+h \end{pmatrix} \\ &= \begin{pmatrix} a+e+c+g & b+f+d+h \\ c+g & d+h \end{pmatrix} \\ &= \begin{pmatrix} a+c & b+d \\ c & d \end{pmatrix} + \begin{pmatrix} e+g & f+h \\ g & h \end{pmatrix} \\ &= MP + MQ \\ &= PM + QM \\ &= \begin{pmatrix} a & a+b \\ c & c+d \end{pmatrix} + \begin{pmatrix} e & e+f \\ g & g+h \end{pmatrix} \\ &= \begin{pmatrix} a+e & a+b+e+f \\ c+g & c+d+g+h \end{pmatrix} \\ &= \begin{pmatrix} a+e & b+f \\ c+g & d+h \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \\ &= (P+Q)M. \end{aligned}$$

Therefore $P + Q \in \mathcal{B}$. □

0.1.3 Exercise 3

Prove that if $P, Q \in \mathcal{B}$, then $PQ \in \mathcal{B}$.

Proof. A similar argument to the one in Exercise 2 above will show that $PQ \in \mathcal{B}$ for any $P, Q \in \mathcal{B}$. □

0.1.4 Exercise 4

Find conditions on p, q, r, s which determine precisely when $\begin{pmatrix} p & q \\ r & s \end{pmatrix} \in \mathcal{B}$.

Solution. Let

$$P = \begin{pmatrix} p & q \\ r & s \end{pmatrix}.$$

Then

$$MP = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} p & q \\ r & s \end{pmatrix} = \begin{pmatrix} p+r & q+s \\ r & s \end{pmatrix}$$

while

$$PM = \begin{pmatrix} p & q \\ r & s \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} p & p+q \\ r & r+s \end{pmatrix}.$$

Therefore, $MP = PM$ if and only if $r = 0$ and $p = s$. Hence

$$\mathcal{B} = \left\{ \begin{pmatrix} p & p+q \\ 0 & p \end{pmatrix} \;\middle|\; p, q \in \mathbb{R} \right\}. \qquad \square$$

0.1.5 Exercise 5

Determine whether the following functions f are well defined:

(a) $f\colon \mathbb{Q} \to \mathbb{Z}$ defined by $f(a/b) = a$.

(b) $f\colon \mathbb{Q} \to \mathbb{Q}$ defined by $f(a/b) = a^2/b^2$.

Solution. (a) f is not well defined since, for example,

$$f(1/2) = 1, \quad f(2/4) = 2, \quad \text{but} \quad \frac{1}{2} = \frac{2}{4}.$$

(b) Suppose $a, b, c, d \in \mathbb{Z}$ with $b, d \neq 0$ are such that

$$\frac{a}{b} = \frac{c}{d}.$$

Then

$$f(a/b) = \frac{a^2}{b^2} = \left(\frac{a}{b}\right)^2 = \left(\frac{c}{d}\right)^2 = \frac{c^2}{d^2} = f(c/d).$$

Therefore f is well defined. $\square$

0.1.6 Exercise 6

Determine whether the function $f\colon \mathbb{R}^+ \to \mathbb{Z}$ defined by mapping a real number r to the first digit to the right of the decimal point in a decimal expansion of r is well defined.

Solution. f is not well defined since decimal expansions are not unique. For example, $1 = 1.0 = 0.999\ldots$ but $f(1.0) = 0$ and $f(0.999\ldots) = 9$. $\square$

0.1.7 Exercise 7

Let $f\colon A \to B$ be a surjective map of sets. Prove that the relation

$$a \sim b \text{ if and only if } f(a) = f(b)$$

is an equivalence relation whose equivalence classes are the fibers of f.

Proof. That $\sim$ is an equivalence relation on A follows directly from the fact that $=$ is an equivalence relation on the set B.

Now let $b \in B$ be arbitrary. Since f is surjective, there is an a in A such that $f(a) = b$. Then the equivalence class of a is the set

$$\{x \in A \mid x \sim a\}.$$

But by definition of $\sim$, this set is equal to

$$\{x \in A \mid f(x) = f(a) = b\}.$$

Therefore the equivalence class of a is precisely the fiber of f over b. $\square$

0.2 Properties of the Integers

0.2.1 Exercise 1

For each of the following pairs of integers a and b, determine their greatest common divisor, their least common multiple, and write their greatest common divisor in the form $ax + by$ for some integers x and y.

(a) $a = 20, b = 13$.

Solution. Applying the Division Algorithm repeatedly, we get

$$\begin{aligned} 20 &= 1(13) + 7 \\ 13 &= 1(7) + 6 \\ 7 &= 1(6) + 1 \\ 6 &= 6(1) + 0. \end{aligned}$$

The first nonzero remainder is 1, so $(20, 13) = 1$. That is, the two numbers are relatively prime.

The least common multiple, $[20, 13]$, is given by

$$\frac{20 \cdot 13}{(20, 13)} = 260.$$

To write 1 as a linear combination of 20 and 13, we work backwards and substitute:

$$\begin{aligned} 1 &= 7 - 1(6) \\ &= 7 - 1(13 - 1(7)) && \text{(Substituting } 6 = 13 - 7) \\ &= 2(7) - 1(13) \\ &= 2(20 - 1(13)) - 1(13) && \text{(Substituting } 7 = 20 - 13) \\ &= 2(20) - 3(13). \end{aligned}$$

□

(b) $a = 69, b = 372$.

Solution. As above, we have

$$\begin{aligned} 372 &= 5(69) + 27 \\ 69 &= 2(27) + 15 \\ 27 &= 1(15) + 12 \\ 15 &= 1(12) + 3 \\ 12 &= 4(3) + 0, \end{aligned}$$

so $(69, 372) = 3$, which gives $[69, 372] = 8556$. And again, as before, we

write

$$\begin{aligned}
3 &= 15 - 1(12) \\
&= 15 - 1(27 - 1(15)) && \text{(Substituting } 12 = 27 - 15\text{)} \\
&= 2(15) - 1(27) \\
&= 2(69 - 2(27)) - 1(27) && \text{(Substituting } 15 = 69 - 2(27)\text{)} \\
&= 2(69) - 5(27) \\
&= 2(69) - 5(372 - 5(69)) && \text{(Substituting } 27 = 372 - 5(69)\text{)} \\
&= 27(69) - 5(372). && \square
\end{aligned}$$

(c) $a = 792, b = 275$.

Solution.

$$\begin{aligned}
792 &= 2(275) + 242 \\
275 &= 1(242) + 33 \\
242 &= 7(33) + 11 \\
33 &= 3(11) + 0.
\end{aligned}$$

Hence $(792, 275) = 11$. Calculating the least common multiple gives $[792, 275] = 19\,800$. Then

$$\begin{aligned}
11 &= 242 - 7(33) \\
&= 242 - 7(275 - 242) \\
&= 8(242) - 7(275) \\
&= 8(792 - 2(275)) - 7(275) \\
&= 8(792) - 23(275). && \square
\end{aligned}$$

(d) $a = 11\,391, b = 5673$.

Solution. Using the methods above, we get

$$\begin{aligned}
(11\,391, 5673) &= 3, \\
[11\,391, 5673] &= 21\,540\,381
\end{aligned}$$

and

$$-126(11\,391) + 253(5673) = 3. \qquad \square$$

(e) $a = 1761, b = 1567$.

Solution.

$$\begin{aligned}
(1761, 1567) &= 1, \\
[1761, 1567] &= 2\,759\,487,
\end{aligned}$$

and

$$-105(1761) + 118(1567) = 1. \qquad \square$$

(f) $a = 507885, b = 60808$.

Solution.

$$(507885, 60808) = 691,$$
$$[507885, 60808] = 44\,693\,880,$$

and

$$-17(507885) + 142(60808) = 691. \qquad \square$$

0.2.2 Exercise 2

Prove that if the integer k divides the integers a and b then k divides $as + bt$ for every pair of integers s and t.

Proof. Suppose a and b are such that $k \mid a$ and $k \mid b$. By definition, this means that there exists integers m and n such that $a = mk$ and $b = nk$. Therefore, for any integers s and t,

$$\begin{aligned} as + bt &= (mk)s + (nk)t \\ &= (ms + nt)k. \end{aligned}$$

Since $ms + nt$ must be an integer (due to closure of integer addition and multiplication), this shows that $k \mid (as + bt)$. $\square$

0.2.3 Exercise 3

Prove that if n is composite then there are integers a and b such that n divides ab but n does not divide either a or b.

Proof. The Fundamental Theorem of Arithmetic guarantees that n is the product of two or more (possibly equal) prime factors. Let a be one of the prime factors, and let b be n/a. Note that b must be an integer since $a \mid n$. Note also that $a, b > 1$.

Now $n = ab$, so clearly $n \mid ab$. However, $n \nmid a$ since a is prime and n is composite.

Finally, suppose for contradiction that $n \mid b$. Then there is an integer $k > 1$ such that $b = kn$. Multiplying by a on both sides gives $ab = akn$ or $n = akn$. Dividing by n then gives $ak = 1$. But this is absurd because a and k are both integers greater than 1. This contradiction shows that $n \nmid b$, so the proof is complete. $\square$

0.2.4 Exercise 4

Let a, b, and N be fixed integers with a and b nonzero and let $d = (a, b)$ be the greatest common divisor of a and b. Suppose x_0 and y_0 are particular solutions to $ax + by = N$ (i.e., $ax_0 + by_0 = N$). Prove for any integer t that the integers

$$x = x_0 + \frac{b}{d}t \quad \text{and} \quad y = y_0 - \frac{a}{d}t \tag{1}$$

are also solutions to $ax + by = N$.

Proof. Substituting for x and y in $ax + by$ gives

$$\begin{aligned} a\left(x_0 + \frac{b}{d}t\right)x + b\left(y_0 - \frac{a}{d}t\right) &= (ax_0 + by_0) + \frac{ab}{d}t - \frac{ab}{d}t \\ &= ax_0 + by_0 \\ &= N. \end{aligned}$$

This holds regardless of the value of t, so (1) is always a valid solution. □

0.2.5 Exercise 5

Determine the value $\varphi(n)$ for each integer $n \leq 30$ where φ denotes the Euler φ-function.

Solution. For each n, the value of $\varphi(n)$ can be determined by first finding the prime factorization of n,

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}, \quad \text{where each } p_i \text{ is prime,}$$

and then by applying the formula given in the text:

$$\varphi(n) = p_1^{\alpha_1 - 1}(p_1 - 1)p_2^{\alpha_2 - 1}(p_2 - 1) \cdots p_k^{\alpha_k - 1}(p_k - 1).$$

For example, to find $\varphi(18)$, we factor $18 = 2 \cdot 3^2$. Applying the formula then gives

$$\begin{aligned} \varphi(18) &= 2^{1-1}(2-1) \cdot 3^{2-1}(3-1) \\ &= 1 \cdot 1 \cdot 3 \cdot 2 \\ &= 6. \end{aligned}$$

Applying this process to each $n \leq 30$ produces the following table:

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$\varphi(n)$	1	1	2	2	4	2	6	4	6	4	10	4	12	6	8

n	16	17	18	19	20	21	22	23	24	25	26	27	28
$\varphi(n)$	8	16	6	18	8	12	10	22	8	20	12	18	12

n	29	30
$\varphi(n)$	28	8

This process can be used to easily find $\varphi(n)$ for any n whose prime factorization is known. □

0.2.6 Exercise 6

Prove the Well Ordering Property of $\mathbb{Z}$ by induction and prove the minimal element is unique:

Theorem. *If A is any nonempty subset of $\mathbb{Z}^+$, there is some element $m \in A$ such that $m \leq a$, for all $a \in A$.*

Proof. Suppose for contradiction that A has no minimal element. We will prove by (strong) induction on n that for each $n \in \mathbb{Z}^+$, $n \notin A$. This will show that A is the empty set, which would contradict the requirement that A be nonempty.

Clearly $1 \notin A$, for otherwise 1 would be a least element (since $1 \leq a$ for all $a \in \mathbb{Z}^+$). Now suppose that $1, 2, \ldots, k \notin A$ for some positive integer k. Then $k+1$ cannot be a member of A since otherwise $k+1$ would be the minimal element. This completes the inductive step, which shows that A is the empty set, giving the needed contradiction to show that A has a minimal element.

Finally, to show that the minimal element is unique, suppose A has two minimal elements, a and b. Since a is minimal, $a \leq b$. But b is minimal, so $b \leq a$. So $a \leq b$ and $a \geq b$ and therefore $a = b$. □

0.2.7 Exercise 7

If p is a prime prove that there do not exist nonzero integers a and b such that $a^2 = pb^2$ (i.e., $\sqrt{p}$ is not a rational number).

Proof. Suppose for contradiction that a and b are nonzero integers with

$$a^2 = pb^2.$$

Without loss of generality we may also assume that a and b have no factors in common (if they do have factors in common, just divide the factors from both sides of the equation).

Now $p \mid a^2$. And since p is prime, we must also have $p \mid a$ (this uses the "important property" mentioned in item **(8)** on page 6 of the text). Then there is an integer m such that $a = pm$ and hence $(pm)^2 = pb^2$, or $p^2m^2 = pb^2$. This implies that $pm^2 = b^2$ so that $p \mid b^2$, which implies $p \mid b$. But a and b were chosen to have no factors in common, yet p is a common factor. This gives the needed contradiction. □

0.2.8 Exercise 8

Let p be a prime, $n \in \mathbb{Z}^+$. Find a formula for the largest power of p which divides $n! = n(n-1)(n-2)\cdots 2 \cdot 1$.

Solution. The only integers less than n that are divisible by p are the multiples of p, of which there are

$$\left\lfloor \frac{n}{p} \right\rfloor$$

of them, where $\lfloor x \rfloor$ denotes the floor of x (i.e., the greatest integer less than or equal to x).

However, multiples of p^2 each contribute a second factor of p. Multiples of p^3 contribute a third additional factor of p, and so on. Therefore the highest power of p that divides $n!$ is given by

$$\left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \cdots = \sum_{k=1}^{\lfloor \log_p n \rfloor} \left\lfloor \frac{n}{p^k} \right\rfloor.$$

□

0.2.10 Exercise 10

Prove for any given positive integer N there exist only finitely many integers n with $\varphi(n) = N$ where φ denotes Euler's φ-function. Conclude in particular that $\varphi(n)$ tends to infinity as n tends to infinity.

Solution. Fix a value of $N > 0$, and let A be the set of all solutions n to the equation $\varphi(n) = N$. We must show that A is a finite set.

First we will show that for any $n \in A$, there cannot be a prime factor of n larger than $N + 1$. For if there are prime factors larger than $N + 1$, then we may choose the smallest such prime p. Then if q is any prime factor of n with $q \geq p$, we may write $n = q^k r$, where r is some positive integer relatively prime to q. Therefore we have

$$\begin{aligned}\varphi(n) &= \varphi(q^k)\varphi(r) \\ &= q^{k-1}(q-1)\varphi(r) \\ &\geq q - 1 > N.\end{aligned}$$

But $\varphi(n) = N$, so this is a contradiction. This shows that all prime factors of n must be at most $N + 1$.

Now let $p_1, p_2, \ldots, p_m$ be all the prime factors less than or equal to $N + 1$ (note that this set of primes is finite). Then every $n \in A$ can be written in the form

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m},$$

where each $\alpha_i \geq 0$ and $\alpha_j > 0$ for at least one index j. Now observe that each α_i can be one of only finitely many possible values, since $\varphi(p_i^s) = p_i^s(p_i - 1) > N$ for sufficiently large values of s, and N is the product of each $\varphi(p_i^{\alpha_i})$. So the distinct values of n in A must be finite in number, because there are only finitely many possible primes in their prime factorizations and their exponents can take only finitely many possible values.

Finally, let M be any positive integer. Since there are only finitely many values of n such that $\varphi(n) \leq M$, we may choose the largest such n. Then $\varphi(m) > M$ for all $m > n$, which shows that $\varphi(n)$ tends to infinity as n tends to infinity. □

0.2.11 Exercise 11

Prove that if d divides n then $\varphi(d)$ divides $\varphi(n)$ where φ denotes Euler's φ-function.

Solution. First consider the case where $n = p^k$ for some prime number p. Then if $d \mid n$ we must have $d = p^\ell$ for some integer ℓ with $0 \leq \ell \leq k$. So

$$\varphi(n) = \varphi(p^k) = p^{k-1}(p-1) \quad \text{and} \quad \varphi(d) = \varphi(p^\ell) = p^{\ell-1}(p-1).$$

Now let $a = p^{k-\ell}$. Then $a\varphi(d) = \varphi(n)$, so $\varphi(d) \mid \varphi(n)$.

The more general case will follow from the fact that φ is a multiplicative function: Let n be a positive integer having prime factorization

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

and suppose d is an integer that divides n. Then d can be written as a product of these same prime factors $p_1, \ldots, p_k$, provided that we allow some of the exponents to be zero. That is, we may write

$$d = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k} \quad \text{with } 0 \leq \beta_i \leq \alpha_i \text{ for each } i.$$

Then

$$\varphi(n) = \varphi(p_1^{\alpha_1})\varphi(p_2^{\alpha_2}) \cdots \varphi(p_k^{\alpha_k}) \tag{2}$$

and

$$\varphi(d) = \varphi(p_1^{\beta_1})\varphi(p_2^{\beta_2}) \cdots \varphi(p_k^{\beta_k}). \tag{3}$$

Now each $p_i^{\beta_i}$ divides $p_i^{\alpha_i}$, so from the argument in the first paragraph, we know that $\varphi(p_i^{\beta_i}) \mid \varphi(p_i^{\alpha_i})$ for each i. Therefore we may find an integer a_i such that $\varphi(p_i^{\alpha_i}) = a_i \varphi(p_i^{\beta_i})$. Therefore, equations (2) and (3) imply that

$$\begin{aligned} \varphi(n) &= a_1 \varphi(p_1^{\beta_1}) \cdot a_2 \varphi(p_2^{\beta_2}) \cdots a_k \varphi(p_k^{\beta_k}) \\ &= (a_1 a_2 \cdots a_k)\varphi(d), \end{aligned}$$

so $\varphi(d) \mid \varphi(n)$. □

0.3 $\mathbb{Z}/n\mathbb{Z}$: The Integers Modulo n

0.3.1 Exercise 1

Write down explicitly all the elements in the residue classes of $\mathbb{Z}/18\mathbb{Z}$.

Solution. The residue classes are

$$\begin{aligned}
\bar{0} &= \{0, 18, -18, 36, -36, \ldots\},\\
\bar{1} &= \{1, 19, -17, 37, -35, \ldots\},\\
\bar{2} &= \{2, 20, -16, 38, -34, \ldots\},\\
\bar{3} &= \{3, 21, -15, 39, -33, \ldots\},\\
\bar{4} &= \{4, 22, -14, 40, -32, \ldots\},\\
\bar{5} &= \{5, 23, -13, 41, -31, \ldots\},\\
\bar{6} &= \{6, 24, -12, 42, -30, \ldots\},\\
\bar{7} &= \{7, 25, -11, 43, -29, \ldots\},\\
\bar{8} &= \{8, 26, -10, 44, -28, \ldots\},\\
\bar{9} &= \{9, 27, -9, 45, -27, \ldots\},\\
\overline{10} &= \{10, 28, -8, 46, -26, \ldots\},\\
\overline{11} &= \{11, 29, -7, 47, -25, \ldots\},\\
\overline{12} &= \{12, 30, -6, 48, -24, \ldots\},\\
\overline{13} &= \{13, 31, -5, 49, -23, \ldots\},\\
\overline{14} &= \{14, 32, -4, 50, -22, \ldots\},\\
\overline{15} &= \{15, 33, -3, 51, -21, \ldots\},\\
\overline{16} &= \{16, 34, -2, 52, -20, \ldots\},
\end{aligned}$$

and

$$\overline{17} = \{17, 35, -1, 53, -19, \ldots\}. \qquad \square$$

0.3.2 Exercise 2

Prove that the distinct equivalence classes in $\mathbb{Z}/n\mathbb{Z}$ are precisely $\bar{0}, \bar{1}, \bar{2}, \ldots, \overline{n-1}$ (use the Division Algorithm).

Proof. Consider the equivalence class $\bar{k}$. Using the Division Algorithm, we may find an integer q and an integer r such that

$$k = qn + r, \quad \text{with } 0 \leq r < n.$$

Now $k \equiv r \pmod{n}$ and r is an integer between 0 and $n-1$, so this shows that $\bar{k} = \bar{r}$. Thus the equivalence classes in $\mathbb{Z}/n\mathbb{Z}$ are a subset of $\{\bar{0}, \bar{1}, \ldots, \overline{n-1}\}$.

Finally, we note that the equivalence classes $\bar{0}, \ldots, \overline{n-1}$ are actually distinct from each other. For, if not, suppose $\bar{a} = \bar{b}$ where $0 \leq b \leq a \leq n-1$. Then $n \mid (a-b)$, and since $0 \leq a - b \leq n-1$, we must have $a - b = 0$ so that $a = b$. Therefore the distinct equivalence classes are precisely $\bar{0}, \ldots, \overline{n-1}$. $\square$

0.3.3 Exercise 3

Prove that if $a = a_n 10^n + a_{n-1}10^{n-1} + \cdots + a_1 10 + a_0$ is any positive integer then $a \equiv a_n + a_{n-1} + \cdots + a_1 + a_0 \pmod 9$ (note that this is the usual arithmetic rule that the remainder after division by 9 is the same as the sum of the decimal digits mod 9 – in particular an integer is divisible by 9 if and only if the sum of its digits is divisible by 9).

Solution. Let a be as stated. Since $10 \equiv 1 \pmod 9$ we may apply Theorem 3 to write

$$\begin{aligned} a &\equiv a_n 1^n + a_{n-1}1^{n-1} + \cdots + a_1 + a_0 \pmod 9 \\ &\equiv a_n + a_{n-1} + \cdots + a_1 + a_0 \pmod 9. \end{aligned}$$

□

0.3.4 Exercise 4

Compute the remainder when 37^{100} is divided by 29.

Solution. $37^2 = 1369 \equiv 6 \pmod{29}$. Successive squaring then yields

$$\begin{aligned} 37^4 &\equiv 6^2 = 36 \equiv 7 \pmod{29} \\ 37^8 &\equiv 7^2 = 49 \equiv 20 \pmod{29} \\ 37^{16} &\equiv 20^2 = 400 \equiv 23 \pmod{29} \\ 37^{32} &\equiv 23^2 = 529 \equiv 7 \pmod{29} \\ 37^{64} &\equiv 7^2 = 49 \equiv 20 \pmod{29}. \end{aligned}$$

So

$$37^{100} = 37^{64}37^{32}37^4 \equiv 20 \cdot 7 \cdot 7 \equiv 23 \pmod{29}.$$

Therefore 37^{100} has a remainder of 23 when divided by 29. □

0.3.5 Exercise 5

Compute the last two digits of 9^{1500}.

Solution. $9^{1500} = 3^{3000} = 27^{1000}$. Now $27^2 = 729 \equiv 29 \pmod{100}$, and successive squaring then gives

$$\begin{aligned} 27^4 &\equiv 29^2 = 841 \equiv 41 \pmod{100}, \\ 27^8 &\equiv 41^2 = 1681 \equiv 81 \pmod{100}, \\ 27^{16} &\equiv 81^2 = 6561 \equiv 61 \pmod{100}, \\ 27^{32} &\equiv 61^2 = 3721 \equiv 21 \pmod{100}, \\ 27^{64} &\equiv 21^2 = 441 \equiv 41 \pmod{100}. \end{aligned}$$

At this point the numbers start to repeat, so that $27^{128} \equiv 81 \pmod{100}$, $27^{256} \equiv 61 \pmod{100}$, and $27^{512} \equiv 21 \pmod{100}$. Therefore

$$\begin{aligned} 9^{1500} = 27^{1000} &= 27^{512}27^{256}27^{128}27^{64}27^{32}27^8 \\ &\equiv 21 \cdot 61 \cdot 81 \cdot 41 \cdot 21 \cdot 81 = (1281)(3321)(1701) \\ &\equiv 81 \cdot 21 \cdot 1 \equiv 1 \pmod{100}. \end{aligned}$$

Therefore, the last two digits of 9^{1500} are 01. □

0.3.6 Exercise 6

Prove that the squares of the elements in $\mathbb{Z}/4\mathbb{Z}$ are just $\bar{0}$ and $\bar{1}$.

Proof.

$$\begin{aligned} 0^2 = 0 &\equiv 0 \pmod 4, \\ 1^2 = 1 &\equiv 1 \pmod 4, \\ 2^2 = 4 &\equiv 0 \pmod 4, \\ 3^2 = 9 &\equiv 1 \pmod 4. \end{aligned}$$

□

0.3.7 Exercise 7

Prove for any integers a and b that $a^2 + b^2$ never leaves a remainder of 3 when divided by 4 (use the previous exercise).

Proof. a^2 and b^2 are each either congruent to 0 or to 1, modulo 4. Adding $a^2 + b^2$ then gives four cases:

$$\begin{aligned} 0 + 0 &\equiv 0 \pmod 4, \\ 0 + 1 &\equiv 1 \pmod 4, \\ 1 + 0 &\equiv 1 \pmod 4, \\ 1 + 1 &\equiv 2 \pmod 4. \end{aligned}$$

In every case, $a^2 + b^2$ never has a remainder of 3 when divided by 4. □

0.3.8 Exercise 8

Prove that the equation

$$a^2 + b^2 = 3c^2 \tag{4}$$

has no solutions in nonzero integers a, b, and c.

Proof. Consider the equation modulo 4. From the previous exercise, the left-hand side cannot be congruent to 3. However, the right-hand side is congruent to either 0 or 3, so therefore both sides must be congruent to 0. That is,

$$a^2 + b^2 \equiv c^2 \equiv 0 \pmod 4.$$

This immediately implies that c is even. Now, if a is even, then b must be even, since $b^2 = c^2 - a^2$ is even. On the other hand, if a is odd, then b must be odd for the same reason. But if a and b are both odd, then we may find integers m and n such that

$$\begin{aligned} a^2 + b^2 &= (2m + 1)^2 + (2n + 1)^2 \\ &= 4m^2 + 4m + 1 + 4n^2 + 4n + 1 \\ &\equiv 2 \pmod 4. \end{aligned}$$

This is impossible, so a, b, and c must all be even.

Now, if possible, suppose that a, b, and c are three positive integers which satisfy the equation (4). Since all three integers must be even, their squares each contain a factor of 4. Divide both sides by 4 to get a new equation,

$$\alpha^2 + \beta^2 = \gamma^2,$$

where $\alpha < a$, $\beta < b$, and $\gamma < c$.

But by the same argument as before, α, β, and γ must be even, so their squares are divisible by 4 and we can again find an even smaller set of solutions. This process could be repeated indefinitely, to get smaller and smaller positive integer solutions. Clearly this is not possible, so there are no solutions in the nonzero integers. □

0.3.9 Exercise 9

Prove that the square of any odd integer always leaves a remainder of 1 when divided by 8.

Proof. If a is an odd integer, then a can be written as $2k + 1$ for some integer k, and

$$a^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 4k(k + 1) + 1.$$

Now $k(k + 1)$ must be even, since it is the product of consecutive integers. Therefore $4k(k + 1)$ is divisible by 8. Therefore $a^2 \equiv 1 \pmod 8$. □

0.3.10 Exercise 10

Prove that the number of elements of $(\mathbb{Z}/n\mathbb{Z})^\times$ is $\varphi(n)$ where φ denotes the Euler φ-function.

Proof. We will show that the elements in $(\mathbb{Z}/n\mathbb{Z})^\times$ are precisely those residue classes whose representatives are relatively prime to n.

First suppose that $a \in (\mathbb{Z}/n\mathbb{Z})^\times$ and let b be the multiplicative inverse of a modulo n, so that $ab \equiv 1 \pmod n$. Then $n \mid (ab - 1)$ so we may find an integer m such that $mn = ab - 1$. Rearranging, we get $ab - mn = 1$. But this shows that the greatest common divisor of a and n is 1 (if not, we could factor the left-hand side to get a product of two integers, not both 1, that equals 1, which is impossible). Therefore any number in $(\mathbb{Z}/n\mathbb{Z})^\times$ must be relatively prime to n.

Now, for the other direction, suppose that a is any integer relatively prime to n. Then we can use the Euclidean algorithm to write the common divisor 1 as a linear combination of a and n, that is,

$$ax + ny = 1, \quad x, y \in \mathbb{Z}.$$

But then $ax \equiv 1 \pmod n$, so x is the multiplicative inverse of a modulo n, i.e., $a \in (\mathbb{Z}/n\mathbb{Z})^\times$.

Since there are exactly $\varphi(n)$ least residues which are coprime to n, the set $(\mathbb{Z}/n\mathbb{Z})^\times$ has exactly $\varphi(n)$ elements. □

0.3.11 Exercise 11

Prove that if $\bar{a}, \bar{b} \in (\mathbb{Z}/n\mathbb{Z})^\times$, then $\bar{a} \cdot \bar{b} \in (\mathbb{Z}/n\mathbb{Z})^\times$.

Proof. Let $\bar{a}$ and $\bar{b}$ be in $(\mathbb{Z}/n\mathbb{Z})^\times$ as stated. Then $\bar{a}$ has a multiplicative inverse $\bar{x}$ and $\bar{b}$ has an inverse $\bar{y}$. Then

$$(\bar{a}\bar{x})(\bar{b}\bar{y}) \equiv 1 \cdot 1 \equiv 1 \pmod{n}.$$

Rearranging the left-hand side, we see that $\bar{x}\bar{y}$ is the multiplicative inverse of $\bar{a}\bar{b}$, so that $\bar{a}\bar{b} \in (\mathbb{Z}/n\mathbb{Z})^\times$. □

0.3.12 Exercise 12

Let $n \in \mathbb{Z}$, $n > 1$, and let $a \in \mathbb{Z}$ with $1 \leq a \leq n$. Prove if a and n are not relatively prime, there exists an integer b with $1 \leq b < n$ such that $ab \equiv 0 \pmod{n}$ and deduce that there cannot be an integer c such that $ac \equiv 1 \pmod{n}$.

Proof. Let $d = (a, n)$ and let $b = n/d$. Then b is an integer with $1 \leq b < n$ (since $d > 1$). Similarly, a/d is also an integer. So we have

$$ab = a\left(\frac{n}{d}\right) = n\left(\frac{a}{d}\right) \equiv 0 \pmod{n}.$$

Now suppose c is such that $ac \equiv 1 \pmod{n}$. Then $abc \equiv b \pmod{n}$. But this is clearly impossible, since $abc \equiv 0 \pmod{n}$ and $b \not\equiv 0 \pmod{n}$. Therefore such a c cannot exist. □

0.3.13 Exercise 13

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

Proof. Since $(a, n) = 1$, we may find integers c and d such that $ac + nd = 1$. This implies that $ac \equiv 1 \pmod{n}$. □

0.3.14 Exercise 14

Conclude from the previous two exercises that $(\mathbb{Z}/n\mathbb{Z})^\times$ is the set of elements $\bar{a}$ of $\mathbb{Z}/n\mathbb{Z}$ with $(a, n) = 1$ and hence prove Proposition 4. Verify this directly in the case $n = 12$.

Solution. From the previous two exercises we know that a and n are relatively prime if and only if there is an integer c such that $ac \equiv 1 \pmod{n}$, i.e., if and only if a has a multiplicative inverse modulo n.

For $n = 12$, we have the following multiplication table:

	0	1	2	3	4	5	6	7	8	9	10	11
0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	$\boxed{1}$	2	3	4	5	6	7	8	9	10	11
2	0	2	4	6	8	10	0	2	4	6	8	10
3	0	3	6	9	0	3	6	9	0	3	6	9
4	0	4	8	0	4	8	0	4	8	0	4	8
5	0	5	10	3	8	$\boxed{1}$	6	11	4	9	2	7
6	0	6	0	6	0	6	0	6	0	6	0	6
7	0	7	2	9	4	11	6	$\boxed{1}$	8	3	10	5
8	0	8	4	0	8	4	0	8	4	0	8	4
9	0	9	6	3	0	6	9	3	0	6	9	3
10	0	10	8	6	4	2	0	10	8	6	4	2
11	0	11	10	9	8	7	6	5	4	3	2	$\boxed{1}$

The only values which have a multiplicative inverse are $1, 5, 7$, and 11, which are precisely those values which are coprime to 12. □

0.3.15 Exercise 15

For each of the following pairs of integers a and n, show that a is relatively prime to n and determine the multiplicative inverse of $\bar{a}$ in $\mathbb{Z}/n\mathbb{Z}$.

(a) $a = 13, n = 20$

Solution. Applying the Euclidean algorithm gives

$$\begin{aligned} 20 &= 1(13) + 7 \\ 13 &= 1(7) + 6 \\ 7 &= 1(6) + 1, \end{aligned}$$

so $(20, 13) = 1$. And we can write

$$\begin{aligned} 1 &= 7 - 6 \\ &= 7 - (13 - 7) \\ &= 2(7) - 13 \\ &= 2(20 - 13) - 13 \\ &= 2(20) - 3(13). \end{aligned}$$

So $\overline{(-3)} = \overline{17}$ is the multiplicative inverse of $\overline{13}$ in $\mathbb{Z}/20\mathbb{Z}$. □

(b) $a = 69, n = 89$

Solution. The same procedure will show that $(69, 89) = 1$ and that $\bar{a}$ has an inverse of $\overline{40}$. □

(c) $a = 1891, n = 3797$

Solution. $\bar{a}$ has an inverse of $\overline{253}$. □

(d) $a = 6\,003\,722\,857, n = 77\,695\,236\,973$

Solution. $\bar{a}$ has an inverse of $\overline{77\,695\,236\,753}$. □

Chapter 1

Introduction to Groups

1.1 Basic Axioms and Examples

1.1.1 Exercise 1

Determine which of the following binary operations are associative:

(a) the operation $\star$ on $\mathbb{Z}$ defined by $a \star b = a - b$

Solution. $(1 \star 2) \star 3 = -4$ while $1 \star (2 \star 3) = 2$, so $\star$ is not associative. □

(b) the operation $\star$ on $\mathbb{R}$ defined by $a \star b = a + b + ab$

Solution. $\star$ is associative: let a, b, c be real numbers. Then

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

□

(c) the operation $\star$ on $\mathbb{Q}$ defined by $a \star b = (a + b)/5$

Solution. $(5 \star 20) \star 15 = 4$ while $5 \star (20 \star 15) = 12/5$. Therefore $\star$ is not associative. □

(d) the operation $\star$ on $\mathbb{Z} \times \mathbb{Z}$ defined by $(a, b) \star (c, d) = (ad + bc, bd)$

Solution. $\star$ is associative: let $(a, b), (c, d), (e, f)$ be members of $\mathbb{Z} \times \mathbb{Z}$.

Then

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

(e) the operation $\star$ on $\mathbb{Q}-\{0\}$ defined by $a\star b=a/b$

Solution. $(125\star 25)\star 5=1$ while $125\star(25\star 5)=25$, so $\star$ is not associative. □

1.1.2 Exercise 2

Decide which of the binary operations in the preceding exercises are commutative.

(a) the operation $\star$ on $\mathbb{Z}$ defined by $a\star b=a-b$

Solution. $\star$ is not commutative since, for example, $1\star 2=-1$ while $2\star 1=1$. □

(b) the operation $\star$ on $\mathbb{R}$ defined by $a\star b=a+b+ab$

Solution. $\star$ is commutative since, for any $a,b\in\mathbb{R}$,

$$\begin{aligned}a\star b &= a+b+ab\\ &= b+a+ba\\ &= b\star a.\end{aligned}$$ □

(c) the operation $\star$ on $\mathbb{Q}$ defined by $a\star b=(a+b)/5$

Solution. $\star$ is commutative since $+$ is commutative in $\mathbb{Q}$. □

(d) the operation $\star$ on $\mathbb{Z}\times\mathbb{Z}$ defined by $(a,b)\star(c,d)=(ad+bc,bd)$

Solution. $\star$ is commutative: Let (a,b) and (c,d) be elements of $\mathbb{Z}\times\mathbb{Z}$. Then

$$\begin{aligned}(a,b)\star(c,d) &= (ad+bc,bd)\\ &= (cb+da,db)\\ &= (c,d)\star(a,b).\end{aligned}$$ □

(e) the operation $\star$ on $\mathbb{Q}-\{0\}$ defined by $a\star b=a/b$

Solution. $\star$ is not commutative since $1\star 2=1/2$ but $2\star 1=2$. □

1.1.3 Exercise 3

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

Proof. Let $\bar{a}, \bar{b}, \bar{c}$ be residue classes in $\mathbb{Z}/n\mathbb{Z}$. Then by Theorem 3 in Section 0.3 along with the associativity of $+$ in $\mathbb{Z}$, we may write

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

So addition of residue classes is associative. □

1.1.4 Exercise 4

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

Proof. As in the previous exercise, this follows from Theorem 3 in Section 0.3 together with the associativity of $\cdot$ in $\mathbb{Z}$. □

1.1.5 Exercise 5

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

Proof. Let $n > 1$. Then there is a residue class in $\mathbb{Z}/n\mathbb{Z}$ which does not contain 0. Call this nonzero residue class $\bar{a}$. Then $\bar{0}$ cannot be the identity element in $\mathbb{Z}/n\mathbb{Z}$ since $\bar{a} \cdot \bar{0} = \bar{0} \neq \bar{a}$. So suppose the identity element is $\bar{e}$. Then, $\bar{0}$ also has no inverse in $\mathbb{Z}/n\mathbb{Z}$, since $\bar{b} \cdot \bar{0} = \bar{0} \neq \bar{e}$ for any $\bar{b}$ in $\mathbb{Z}/n\mathbb{Z}$. Since the element $\bar{0}$ does not have an inverse, $\mathbb{Z}/n\mathbb{Z}$ is not a group under multiplication. □

1.1.6 Exercise 6

Determine which of the following sets are groups under addition:

(a) the set of rational numbers (including $0 = 0/1$) in lowest terms whose denominators are odd

Solution. Let the set be denoted A. Then A is a group having identity 0 and, for each $a \in A$, an inverse $-a$. To prove this, we need only show that A is closed under addition.

Suppose a and b are any elements in A. Then we can find integers p, q, r, s with

$$a = \frac{p}{q} \quad \text{and} \quad b = \frac{r}{s}$$

in lowest terms with q, s odd. Then we have

$$a + b = \frac{ps + rq}{qs} = \frac{u}{v},$$

where u and v are integers with u/v in lowest terms. Now, since u/v was obtained by eliminating common factors, we have $u \mid (ps + rq)$ and $v \mid qs$. But if $2 \mid v$, then necessarily $2 \mid qs$. But this cannot be, since qs is odd, being the product of odd integers. Hence A is closed under addition and is therefore a group. □

(b) the set of rational numbers in lowest terms whose denominators are even, together with 0

Solution. Let A denote the set. Then A is not a group since $3/2 \in A$ but

$$\frac{3}{2} + \frac{3}{2} = \frac{6}{2} = \frac{3}{1} \notin A.$$ □

(c) the set of rational numbers of absolute value < 1

Solution. Again, this set is not closed under addition since, for example,

$$\frac{3}{4} + \frac{3}{4} > 1.$$

Therefore it is not a group. □

(d) the set of rational numbers of absolute value ≥ 1 together with 0

Solution. This set is not closed under addition since, for example,

$$\frac{12}{5} - \frac{8}{5} = \frac{4}{5} \ngeq 1.$$

Therefore it is not a group. □

(e) the set of rational numbers with denominators equal to 1 or 2

Solution. Denote the set by A. Let a and b be arbitrary integers. Then $a, b, a/2, b/2 \in A$. There are several cases. First,

$$\frac{a}{1} + \frac{b}{1} = \frac{a+b}{1} \in A.$$

Now consider

$$\frac{a}{2} + \frac{b}{2} = \frac{a+b}{2}.$$

If this fraction is in lowest terms, then it is in A. If not, then there must be a common factor of 2 and the fraction can be written with a denominator of 1 and thus is in A.

Finally, consider

$$\frac{a}{1} + \frac{b}{2} = \frac{b}{2} + \frac{a}{1} = \frac{2a+b}{2}.$$

As before, this is either in lowest terms, or can be reduced to lowest terms by dividing the numerator and denominator by 2. In either case, this number is in A.

Since A is closed under addition, it is easily seen to be a group: the identity is $1 = 1/1$ and the inverse of $a/b \in A$ is $-a/b$. □

(f) the set of rational numbers with denominators equal to 1, 2, or 3

Solution. This set is not closed under addition, since

$$\frac{1}{2} + \frac{1}{3} = \frac{5}{6}.$$

Hence this is not a group. □

1.1.7 Exercise 7

Let $G = \{x \in \mathbb{R} \mid 0 \leq x < 1\}$ and for $x, y \in G$ let $x \star y$ be the fractional part of $x + y$ (i.e., $x \star y = x + y - [x + y]$ where $[a]$ is the greatest integer less than or equal to a). Prove that $\star$ is a well defined binary operation on G and that G is an abelian group under $\star$ (called the *real numbers mod* 1).

Proof. Let $x, y \in G$ be arbitrary. Then $0 \leq x + y < 2$. There are two cases: if $x + y < 1$ then $[x + y] = 0$ and $x \star y \in G$. On the other hand, if $1 \leq x + y < 2$ then $[x + y] = 1$ and $x \star y = x + y - 1 \in G$. Therefore $\star$ is a well defined binary operation on G.

Let $x, y, z \in G$. If $x + y < 1$ and $y + z < 1$, then

$$\begin{aligned}(x \star y) \star z &= (x + y - 0) \star z \\ &= x + y + z - [x + y + z] \\ &= x \star (y + z - 0) \\ &= x \star (y \star z).\end{aligned}$$

On the other hand, if $1 \leq x + y < 2$ and $1 \leq y + z < 2$, then

$$\begin{aligned}(x \star y) \star z &= (x + y - 1) \star z \\ &= x + y + z - 1 - [x + y + z - 1] \\ &= x \star (y + z - 1) \\ &= x \star (y \star z).\end{aligned}$$

Finally, if $1 \leq x + y < 2$ and $0 \leq y + z < 1$, then $[x + y] = 1$, $[y + z] = 0$, and $[x + y + z - 1] = [x + y + z] - 1$, so

$$\begin{aligned}(x \star y) \star z &= (x + y - 1) \star z \\ &= x + y + z - 1 - [x + y + z - 1] \\ &= x + y + z - 1 - [x + y + z] + 1 \\ &= x + y + z - [x + y + z] \\ &= x \star (y + z - 0) \\ &= x \star (y \star z).\end{aligned}$$

And the case where $x+y < 1$ and $y+z \geq 1$ is similar. Therefore, $\star$ is associative.

Since $0 \in G$, G has an identity ($x \star 0 = 0 \star x = x$ for each x in G). And every element has an inverse: the inverse of 0 is 0, and for nonzero $x \in G$, $1 - x \in G$ is an inverse since

$$x \star (1 - x) = x + (1 - x) - [x + (1 - x)] = 1 - 1 = 0.$$

Therefore G is a group under $\star$. □

1.1.8 Exercise 8

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

(a) Prove that G is a group under multiplication (called the group of *roots of unity* in $\mathbb{C}$).

Proof. Let $z, w \in G$ so that $z^n = 1$ and $w^m = 1$.

Note that $1 \in G$ since $1^1 = 1$, so G has an identity. And every element of G is nonzero, so for each $z \in G$ we may let $z^{-1} = 1/z$ so that every element in G has an inverse (since $(1/z)^n = 1/z^n = 1$ so $1/z \in G$).

By the commutativity of multiplication in $\mathbb{C}$, we have

$$(zw)^{nm} = z^{nm}w^{mn} = (z^n)^m(w^m)^n = 1^m 1^n = 1$$

for each $m, n \in \mathbb{Z}^+$. Therefore, G is closed under multiplication. And associativity follows from associativity of multiplication in $\mathbb{C}$.

Therefore G is a group. □

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

Proof. G is a not a group under addition since it is not closed: $1 \in G$ but $1 + 1 = 2 \notin G$ since there is no $n \in \mathbb{Z}^+$ with $2^n = 1$. □

1.1.9 Exercise 9

Let $G = \{a + b\sqrt{2} \in \mathbb{R} \mid a, b \in \mathbb{Q}\}$.

(a) Prove that G is a group under addition.

Proof. Associativity of $+$ in G follows from associativity of $+$ in $\mathbb{R}$. G has an identity $0 = 0 + 0\sqrt{2}$ and for every p in G we may take $q = -p$ as its additive inverse. So we need only show that G is closed under addition.

Let $p = a + b\sqrt{2}$ and $q = c + d\sqrt{2}$ with $a, b, c, d \in \mathbb{Q}$. Then

$$p + q = a + c + (b + d)\sqrt{2}, \quad \text{where } a + c \in \mathbb{Q} \text{ and } b + d \in \mathbb{Q},$$

so $p + q \in G$ and G is a group. □

(b) Prove that the nonzero elements of G are a group under multiplication.

Proof. Again, associativity follows from associativity in $\mathbb{R}$. This time the identity is $1 = 1 + 0\sqrt{2}$. And for any rational numbers a and b not both 0, $a + b\sqrt{2} \in G - \{0\}$ and

$$\begin{aligned}
\frac{1}{a + b\sqrt{2}} &= \frac{a - b\sqrt{2}}{(a + b\sqrt{2})(a - b\sqrt{2})} \\
&= \frac{a - b\sqrt{2}}{a^2 - 2b^2} \\
&= \frac{a}{a^2 - 2b^2} - \left(\frac{b}{a^2 - 2b^2}\right)\sqrt{2} \in G - \{0\},
\end{aligned}$$

so every element in $G - \{0\}$ has an inverse (note that the denominator $a^2 - 2b^2$ is nonzero since $a, b \in \mathbb{Q}$ and there is no rational square root of 2).

The set is also closed under multiplication since for any $a, b, c, d \in \mathbb{Q}$ with a, b not both 0 and c, d not both 0,

$$\left(a + b\sqrt{2}\right)\left(c + d\sqrt{2}\right) = ac + 2bd + (ad + bc)\sqrt{2} \in G - \{0\}.$$

This shows that $G - \{0\}$ is a group under multiplication. □

1.1.10 Exercise 10

Prove that a finite group is abelian if and only if its group table is a symmetric matrix.

Proof. List the elements of the group in a fixed order along the top row and first column of the group table. Then the group is abelian if and only if the i, jth entry in its group table is equal to the j, ith entry, which is true if and only if the table forms a symmetric matrix. □

1.1.11 Exercise 11

Find the orders of each element of the additive group $\mathbb{Z}/12\mathbb{Z}$.

Solution. $\bar{0}$ has order 1. $\bar{1}$ has order 12 since $1 \cdot \bar{1}$, $2 \cdot \bar{1}$, …, $11 \cdot \bar{1}$ are nonzero while $12 \cdot \bar{1} = \bar{0}$. Similarly, we find the following orders for the elements:

x	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$	$\bar{8}$	$\bar{9}$	$\overline{10}$	$\overline{11}$
$\lvert x\rvert$	1	12	6	4	3	12	2	12	3	4	6	12

□

1.1.12 Exercise 12

Find the orders of the following elements of the multiplicative group $(\mathbb{Z}/12\mathbb{Z})^\times$: $\bar{1}$, $\overline{-1}$, $\bar{5}$, $\bar{7}$, $\overline{-7}$, $\overline{13}$.

Solution. We get the following table:

x	$\bar{1}$	$\overline{-1}$	$\bar{5}$	$\bar{7}$	$\overline{-7}$	$\overline{13}$
$\lvert x\rvert$	1	2	2	2	2	1

□

1.1.13 Exercise 13

Find the orders of the following elements of the additive group $\mathbb{Z}/36\mathbb{Z}$: $\bar{1}$, $\bar{2}$, $\bar{6}$, $\bar{9}$, $\overline{10}$, $\overline{12}$, $\overline{-1}$, $\overline{-10}$, $\overline{-18}$.

Solution. We get the following table:

x	$\bar{1}$	$\bar{2}$	$\bar{6}$	$\bar{9}$	$\overline{10}$	$\overline{12}$	$\overline{-1}$	$\overline{-10}$	$\overline{-18}$
$\lvert x\rvert$	36	18	6	4	18	3	36	18	2

□

1.1.14 Exercise 14

Find the orders of the following elements of the multiplicative group $(\mathbb{Z}/36\mathbb{Z})^\times$: $\overline{1}, \overline{-1}, \overline{5}, \overline{13}, \overline{-13}, \overline{17}$.

Solution. We have the following table:

x	$\overline{1}$	$\overline{-1}$	$\overline{5}$	$\overline{13}$	$\overline{-13}$	$\overline{17}$
$\lvert x\rvert$	1	2	6	3	6	2

□

1.1.15 Exercise 15

Let G be a group. Prove that

$$(a_1 a_2 \dots a_n)^{-1} = a_n^{-1} a_{n-1}^{-1} \dots a_1^{-1}$$

for all $a_1, a_2, \dots, a_n \in G$.

Proof. We use induction on n. If $n = 1$, the result is obvious. Suppose it holds for $n = k$, where $k \geq 1$. Then for any $a_1, \dots, a_{k+1}$ in G, we have

$$\begin{aligned}(a_1 \dots a_k a_{k+1})(a_{k+1}^{-1} a_k^{-1} \dots a_1^{-1}) &= (a_1 \dots a_k)(a_{k+1} a_{k+1}^{-1})(a_k^{-1} \dots a_1^{-1}) \\ &= (a_1 \dots a_k)(a_k^{-1} \dots a_1^{-1}),\end{aligned}$$

and this is equal to 1 by the induction hypothesis. Therefore $(a_1 \dots a_{k+1})^{-1} = a_{k+1}^{-1} \dots a_1^{-1}$ and the statement holds for all positive integers n. □

1.1.16 Exercise 16

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

Proof. First, if $|x| = 1$ then $x = 1$ so $x^2 = 1^2 = 1$. If $|x| = 2$, then $x^2 = 1$ by definition.

For the other direction, suppose $x^2 = 1$. Then $|x| \leq 2$. But the order of an element must be at least 1, so $|x| = 1$ or $|x| = 2$. □

1.1.17 Exercise 17

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

Proof. Since $|x| = n$, we have $x^n = 1$. But $x^n = x^{n-1}x = xx^{n-1}$, so $x^{n-1}x = 1$ which shows that $x^{-1} = x^{n-1}$. □

1.1.18 Exercise 18

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

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

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

1.1.19 Exercise 19

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

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

Proof. $x^a x^b$ consists of a a factors of x, multiplied by b factors of x, for a total of $a+b$ factors of x. Therefore $x^{a+b} = x^a x^b$ by definition. Similarly, $(x^a)^b = x^{ab}$ by the same reasoning. □

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

Proof. Since $x^{-a} = (x^{-1})^a$, we need to show that $(x^a)^{-1} = (x^{-1})^a$. We use induction on a. For $a = 1$, the result is trivial. Suppose it holds for $a = k$, $k \geq 0$. Then

$$(x^{k+1})(x^{-1})^{k+1} = x^k(xx^{-1})(x^{-1})^k = x^k(x^{-1})^k,$$

which by the induction hypothesis must be 1. Therefore the result holds for all positive integers a. □

(c) Establish part (a) for arbitrary integers a and b (positive, negative, or zero).

Proof. For any integer a, $x^a x^0 = x^a = x^{a+0}$ and similarly $x^0 x^a = x^{0+a}$.

Now suppose $a > 0, b < 0$. If $a + b > 0$, then $x^{a+b}x^{-b} = x^{(a+b)+(-b)} = x^a$ by part (a). Multiplying both sides of this equation on the right by x^b gives $x^{a+b} = x^a x^b$ as desired. On the other hand, if $a + b < 0$, then $x^{-(a+b)}x^a = x^{-(a+b)+a} = x^{-b}$. Multiplying both sides of this equation on the right by x^{-a} gives $x^{-(a+b)} = x^{-b}x^{-a}$, so

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

The last equality follows from part (4) of Proposition 1 in the text. Since inverses are unique (by the same proposition) we have $x^{a+b} = x^a x^b$.

The case where $a < 0, b > 0$ is entirely similar to the argument above. Finally, if a and b are both negative, then

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

This completes the proof. □

1.1.20 Exercise 20

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

Proof. Suppose $|x| = n$ for finite n. Then $x^n = 1$ so

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

which shows x^{-1} has finite order and $|x^{-1}| \leq |x|$. On the other hand, if $|x^{-1}| = k$ then

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

so x has finite order and $|x| \leq |x^{-1}|$. This shows that $|x| = |x^{-1}|$ when either x or x^{-1} is of finite order. The only alternative is that x and x^{-1} are both of infinite order. □

1.1.21 Exercise 21

Let G be a finite group and let x be an element of G of order n. Prove that if n is odd, then $x = (x^2)^k$ for some integer $k \geq 1$.

Proof. If n is odd, then we may write $n = 2k - 1$ for some $k \in \mathbb{Z}^+$. Then we have

$$x^n = x^{2k-1} = 1.$$

Multiplying both sides by x then gives

$$x^{2k-1}x = x,$$

so

$$x = x^{2k-1+1} = x^{2k} = (x^2)^k.$$ □

1.1.22 Exercise 22

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

Proof. A simple induction argument will show that $(g^{-1}xg)^k = g^{-1}x^kg$ for any $k \in \mathbb{Z}^+$. So if $|x| = n$, then $x^n = 1$ and we have

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

which shows that $g^{-1}xg$ is of finite order and $|g^{-1}xg| \leq |x|$. However, if $|g^{-1}xg| = k$, then $(g^{-1}xg)^k = 1$ so

$$x^k = gg^{-1}x^kgg^{-1} = g(g^{-1}xg)^kg^{-1} = g1g^{-1} = 1,$$

which shows that x is of finite order and $|x| \leq |g^{-1}xg|$. Therefore $|x| = |g^{-1}xg|$.

This also shows that if x is of infinite order, then $g^{-1}xg$ is of infinite order and vice versa.

Finally, for any $a, b \in G$,

$$|ab| = |b(ab)b^{-1}| = |ba|.$$ □

1.1.23 Exercise 23

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

Proof. Let $|x| = n$ where $n = st$. Then

$$1 = x^n = x^{st} = (x^s)^t,$$

so $|x^s| \leq t$. Now suppose $|x^s| = r$. Then $(x^s)^r = x^{sr} = 1$. But $|x| = st$, so we have $sr \geq st$ or $r \geq t$, which gives $|x^s| \geq t$. Therefore $|x^s| = t$. □

1.1.24 Exercise 24

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

Lemma. *If a and b are commuting elements of a group G, then $a^n b = ba^n$ for all positive integers n.*

Proof. We use induction on n. The base case is trivial, so suppose $a^n b = ba^n$ for some positive integer n. Then

$$a^{n+1}b = aa^n b = aba^n = baa^n = ba^{n+1},$$

which completes the inductive step. Hence $a^n b = ba^n$ for all positive n. □

Proof of main result. First we will use induction on n to show that $(ab)^n = a^n b^n$ in the case where n is positive. For $n = 1$, the result is obvious. Suppose the result is true for $n = k$, for some positive integer k. Then

$$(ab)^{k+1} = (ab)(ab)^k = aba^k b^k = aa^k bb^k = a^{k+1}b^{k+1},$$

where the second-to-last equality makes use of the above lemma. This shows that the result holds for all positive integers n.

Next, in the case where $n = 0$, we get $(ab)^0 = 1 = a^0 b^0$.

Finally, using the result from Exercise 1.1.19, we have for any $n < 0$,

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

Therefore the result holds for all integers n. □

1.1.25 Exercise 25

Let G be a group. Prove that if $x^2 = 1$ for all $x \in G$ then G is abelian.

Proof. For any $x \in G$, we have $x = x^{-1}$. Let $a, b \in G$ be arbitrary. Then we have

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

Here we have made use of property (4) from Proposition 1. This shows that G is abelian. □

1.1.26 Exercise 26

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

Proof. (a) Associativity of $\star$ in H follows from associativity of $\star$ in G.

(b) Since H is nonempty, it must have an element a. Then by hypothesis $a^{-1} \in H$ and therefore $aa^{-1} = e \in H$, where e denotes the identity of G. Therefore H has an identity.

(c) For each $a \in H$, $a^{-1} \in H$ by hypothesis so every element of H has an inverse in H.

This shows that $(H, \star)$ is a group. □

1.1.27 Exercise 27

Prove that if x is an element of the group G then $\{x^n \mid n \in \mathbb{Z}\}$ is a subgroup of G (called the *cyclic subgroup* of G generated by x).

Proof. Let H be the subset stated above. We know H is nonempty since $x^0 = e$ is a member of H. If $a = x^m$ and $b = x^n$ are any two elements in H, then $ab = x^m x^n = x^{m+n}$ by Exercise 1.1.19. So $ab \in H$ which shows that H is closed under the binary operation of G. H is also closed under inverses, since $a^{-1} = (x^m)^{-1} = x^{-m} \in H$. Therefore, by the previous exercise, H is a subgroup of G. □

1.1.28 Exercise 28

Let $(A, \star)$ and $(B, \diamond)$ be groups and let $A \times B$ be their direct product. Verify all the group axioms for $A \times B$:

(a) prove that the associative law holds

(b) prove that $(1, 1)$ is the identity of $A \times B$, and

(c) prove that the inverse of (a, b) is (a^{-1}, b^{-1}).

Proof. (a) For all $(a_i, b_i) \in A \times B$ with $i = 1, 2, 3$ we have

$$\begin{aligned}(a_1, b_1)[(a_2, b_2)(a_3, b_3)] &= (a_1, b_1)(a_2 a_3, b_2 b_3) \\ &= \big(a_1(a_2 a_3), b_1(b_2 b_3)\big) \\ &= \big((a_1 a_2)a_3, (b_1 b_2)b_3\big) \\ &= (a_1 a_2, b_1 b_2)(a_3, b_3) \\ &= [(a_1, b_1)(a_2 b_2)](a_3, b_3).\end{aligned}$$

This shows associativity.

(b) For any $(a, b) \in A \times B$ we have

$$(a, b)(1, 1) = (a \star 1, b \diamond 1) = (a, b).$$

Therefore $(1, 1)$ is the identity of $A \times B$.

(c) For any $(a, b) \in A \times B$,

$$(a, b)(a^{-1}, b^{-1}) = (a \star a^{-1}, b \diamond b^{-1}) = (1, 1),$$

so $(a, b)^{-1} = (a^{-1}, b^{-1})$. □

1.1.29 Exercise 29

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

Proof. First, if A and B are abelian and if (a, b) and (c, d) are any members of $A \times B$, then

$$(a, b)(c, d) = (ac, bd) = (ca, db) = (c, d)(a, b),$$

so $A \times B$ is abelian.

For the other direction, suppose $A \times B$ is abelian. Let $a_1, a_2 \in A$ and $b_1, b_2 \in B$. Then since $A \times B$ is abelian, we have

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

Equating components shows that $a_1a_2 = a_2a_1$ and $b_1b_2 = b_2b_1$. Therefore A and B are both abelian. □

1.1.30 Exercise 30

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

Proof. If $a \in A$ and $b \in B$, then $(a, 1), (1, b) \in A \times B$ and

$$(a, 1)(1, b) = (a1, 1b) = (a, b) = (1a, b1) = (1, b)(a, 1).$$

Now, we will show by induction on n that $(a, b)^n = (a^n, b^n)$ for any positive integer n. The base case is obvious. Suppose $(a, b)^k = (a^k, b^k)$ for some $k > 0$. Then

$$(a, b)^{k+1} = (a, b)^k(a, b) = (a^k, b^k)(a, b) = (a^{k+1}, b^{k+1})$$

so the statement holds for all $n \in \mathbb{Z}^+$. This implies that $|(a, 1)| = |a|$ and $|(1, b)| = |b|$.

Let the least common multiple of $|a|$ and $|b|$ be ℓ and suppose $|(a, b)| = k$. Then $m|a| = n|b| = \ell$ for some integers m and n. Since $(a, 1)$ and $(1, b)$ commute, we have

$$\begin{aligned}(a, b)^\ell &= ((a, 1)(1, b))^\ell \\ &= (a, 1)^\ell(1, b)^\ell \\ &= (a, 1)^{m|a|}(1, b)^{n|b|} \\ &= (1, 1)(1, 1) \\ &= (1, 1).\end{aligned}$$

So $k \leq \ell$. Now since $(a, b)^k = (1, 1)$, we have $a^k = 1$ and $b^k = 1$. This implies $|a|$ divides k and $|b|$ divides k. So k is a common multiple of $|a|$ and $|b|$. Therefore $\ell \leq k$. This shows that $\ell = k$, which completes the proof. □

1.1.31 Exercise 31

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

Proof. Define $t(G)$ to be the set $\{g \in G \mid g \neq g^{-1}\}$. Then $t(G)$ must have an even number of elements because $g \in t(G)$ if and only if $g^{-1} \in t(G)$ and any such g, g^{-1} must be distinct. Since G also has an even number of elements, the set $G - t(G)$ has an even number of elements.

Now $G - t(G)$ is nonempty since the identity $e \notin t(G)$. Therefore there is a nonidentity element $a \in G - t(G)$. But since $a \notin t(G)$, we have $a = a^{-1}$ so that $a^2 = e$ but $a \neq e$. Thus a is an element of order 2, completing the proof. □

1.1.32 Exercise 32

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

Proof. Suppose the contrary, so that $x^s = x^t$ for $1 \leq s < t < n$. Then $x^t x^{-s} = x^{t-s} = 1$. But $1 \leq t - s < n$, so $|x| < n$, a contradiction. This shows that each of $1, x, \ldots, x^{n-1}$ are distinct so that $|G| \geq |x|$. □

1.1.33 Exercise 33

Let x be an element of finite order n in the group G.

(a) Prove that if n is odd then $x^i \neq x^{-i}$ for all $i = 1, 2, \ldots, n-1$.

Proof. Fix a positive integer $i < n$. Then $x^i x^{n-i} = 1$ so $x^{-i} = x^{n-i}$. By the previous exercise, if $i \neq n - i$, then $x^i \neq x^{n-i}$. Since inverses are unique, we have in this case that $x^i \neq x^{-i}$.

Now, if n is odd, then necessarily $i \neq n - i$, so $x^i \neq x^{-i}$. □

(b) Prove that if $n = 2k$ and $1 \leq i < n$ then $x^i = x^{-i}$ if and only if $i = k$.

Proof. For any $1 \leq i < n$ such that $i \neq k$, we have $i \neq n - i$ so $x^i \neq x^{-i}$ by the argument in the first part of the problem. And if $i = k$, then $x^i x^i = x^{2k} = x^n = 1$, so $x^i = x^{-i}$ in this case (and only this case). □

1.1.34 Exercise 34

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

Proof. Let x have infinite order and suppose $x^m = x^n$ with $n \leq m$. Then $x^{m-n} = 1$. If $m - n > 0$ then x has finite order, which is a contradiction. Therefore $m = n$. This shows that each x^m is distinct. □

1.1.35 Exercise 35

If x is an element of finite order n in a group G, use the Division Algorithm to show that *any* integral power of x equals one of the elements in the set $\{1, x, x^2, \ldots, x^{n-1}\}$.

Proof. Let x have order n and suppose k is any integer.

Since n must be greater than 0, we may use the Division Algorithm to find integers q and r such that $k = qn + r$, where $0 \leq r < n$. Then

$$x^k = x^{qn+r} = (x^n)^q x^r = 1x^r = x^r, \quad \text{where } 0 \leq r < n,$$

which completes the proof. □

1.1.36 Exercise 36

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

Proof. From the previous exercises, we know that each element in G besides 1 either has order equal to 2 or 3. By Exercise 1.1.31 there is an element in G with order 2. Without loss of generality, we may suppose that this element is a.

Then $a^2 = 1$. Now $ab \neq 1$ since that would imply $b = a^{-1} = a$. Next, $ab \neq a$ since otherwise the cancellation law would give $b = 1$. Similarly, $ab \neq b$ since otherwise $a = 1$. So we must have $ab = c$. Using the same reasoning, we must have $ba = c$ and $ac = ca = b$. Using this information, we have $b^2 = (ca)(ac) = c(a^2)c = c^2$.

Now, if $b^2 \neq 1$ then we must have $|b| = 3$ so that $b^3 = 1$. Then

$$a = ab^3 = (ab)b^2 = c^3.$$

But since $c^3 = a \neq 1$, we have $|c| = 2$ so $1 = c^2 = b^2$ and $|b| = 2$, a contradiction. This shows that $b^2 = c^2 = 1$. Finally,

$$bc = (ac)c = ac^2 = a,$$

and similarly $cb = a$.

Combining all of this information gives the following group table:

	1	a	b	c
1	1	a	b	c
a	a	1	c	b
b	b	c	1	a
c	c	b	a	1

And we can readily see that G is abelian. □

1.2 Dihedral Groups

In these exercises, D_{2n} has the usual presentation

$$D_{2n} = \langle r, s \mid r^n = s^2 = 1, rs = sr^{-1} \rangle.$$

1.2.1 Exercise 1

Compute the order of each of the elements in the following groups:

(a) D_6

Solution. The elements of D_6 are 1, r, r^2, s, sr, and sr^2. We have $|1| = 1$, $|r| = 3$, $|r^2| = 3$, and $|s| = 2$. Since $(sr)^2 = srsr = s^2r^{-1}r = 1$ and $(sr^2)^2 = sr^2sr^2 = s^2r^{-2}r^2 = 1$, we have $|sr| = |sr^2| = 2$. □

(b) D_8

Solution. Again we have $|1| = 1$, $|r| = 4$, $|r^2| = 2$, and $|r^3| = 4$. For k with $0 \leq k \leq 3$, we have $(sr^k)^2 = sr^ksr^k = s^2r^{-k}r^k = 1$ so $|sr^k| = 2$. □

(c) D_{10}

Solution. Since 5 is prime, we have for each k with $0 \leq k \leq 4$,

$$|r^k| = 5 \quad \text{and} \quad |sr^k| = 2.$$ □

1.2.2 Exercise 2

Use the generators and relations above to show that if x is any element of D_{2n} which is not a power of r, then $rx = xr^{-1}$.

Proof. Since any element of D_{2n} that is not a power of r has the form sr^k for some integer k, we have

$$rx = rsr^k = sr^{-1}r^k = sr^{-k} = sr^kr^{-1} = xr^{-1}.$$ □

1.2.3 Exercise 3

Use the generators and relations above to show that every element of D_{2n} which is not a power of r has order 2. Deduce that D_{2n} is generated by the two elements s and sr, both of which have order 2.

Proof. As in the previous exercise, such elements have the form sr^k. sr^k is distinct from the identity, and

$$(sr^k)^2 = sr^ksr^k = s^2r^{-k}r^k = 1,$$

so $|sr^k| = 2$.

Now, the elements of D_{2n} are $1, r, r^2, \ldots, r^n$, and $s, sr, \ldots, sr^n$. Each r^k can be written as $(s(sr))^k$, and each sr^k can be written as $s(s(sr))^k$, so D_{2n} is generated by $\{s, sr\}$, each element of which has order 2. □

1.2.4 Exercise 4

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

Proof. r has order n, so by Exercise 1.1.33, we know that $z = z^{-1}$, that is, $r^k = r^{-k}$. Let $x \in D_{2n}$ be arbitrary. Then x can be written either r^ℓ or sr^ℓ for some integer ℓ. In the first case,

$$zx = r^k r^\ell = r^{k+\ell} = r^\ell r^k = xz,$$

and in the second case,

$$zx = r^k sr^\ell = sr^{-k} r^\ell = sr^k r^\ell = sr^\ell r^k = xz.$$

This shows that z commutes with each element of D_{2n}.

Now suppose z' is any nonidentity element in D_{2n} which commutes with every element in D_{2n}. Then in particular z' commutes with s. So if $z' = r^t$ for some integer t, then $z's = sz'$, and

$$z's = r^t s = sr^{-t}.$$

Therefore $r^t = r^{-t}$. By Exercise 1.1.33, we must have $t = k$. On the other hand, if $z' = sr^t$, then

$$z's = sr^t s = s^2 r^{-t} = r^{-t}.$$

So $sr^t = r^{-t}$, but this is impossible, since a reflection cannot also be a rotation. Therefore $z' = z$ and z is the only nonidentity element which commutes with all elements in the group. □

1.2.5 Exercise 5

If n is odd and $n \geq 3$, show that the identity is the only element of D_{2n} which commutes with all elements of D_{2n}.

Proof. The proof is essentially the same as in the previous exercise, except the odd case from Exercise 1.1.33 is used instead of the even one. □

1.2.6 Exercise 6

Let x and y be elements of order 2 in any group G. Prove that if $t = xy$ then $tx = xt^{-1}$ (so that if $n = |xy| < \infty$ then x, t satisfy the same relations in G as s, r do in D_{2n}).

Proof. Note that $x = x^{-1}$ and $y = y^{-1}$. If $t = xy$ then

$$tx = xyx = xy^{-1}x^{-1} = x(xy)^{-1} = xt^{-1}.$$ □

1.2.7 Exercise 7

Show that $\langle a, b \mid a^2 = b^2 = (ab)^n = 1\rangle$ gives a presentation in D_{2n} in terms of the two generators $a = s$ and $b = sr$ of order 2 computed in Exercise 1.2.3 above.

Proof. Suppose $a^2 = b^2 = (ab)^n = 1$. Then $s^2 = a^2 = 1$ and $r^n = (s^2r)^n = (ab)^n = 1$. Since $b^2 = 1$, we have $srsr = 1$. Multiplying each side of this equation on the right by r^{-1} and then on the left by s gives $s^2(rs)1 = sr^{-1}$ or $rs = sr^{-1}$. This shows that the relations $s^2 = r^n = 1$ and $rs = sr^{-1}$ follow from the relations for a and b.

Now suppose $s^2 = r^n = 1$ and $rs = sr^{-1}$. Then $a^2 = s^2 = 1$, $b^2 = srsr = s^2r^{-1}r = 1$, and $(ab)^n = (s(sr))^n = (s^2r)^n = r^n = 1$. Therefore the relations for a and b follow from those for r and s, so that the above is a presentation for D_{2n} in terms of a and b. □

1.2.8 Exercise 8

Find the order of the cyclic subgroup of D_{2n} generated by r.

Solution. Let $G = \langle r\rangle$ be the cyclic subgroup of D_{2n} generated by r. Then each element of G can be written r^k for some integer k. If $k > 0$ then r^k is a clockwise rotation about the origin by $2k\pi/n$ radians. If $k < 0$, then r^k is a rotation counterclockwise by $-2k\pi/n$ radians. If $|k| \geq n$, then the rotation is equivalent to a rotation r^ℓ where $0 \leq \ell < n$. And $1, r, r^2, \ldots, r^{n-1}$ are distinct, so G is given by

$$G = \{1, r, r^2, \ldots, r^{n-1}\},$$

and we have $|G| = n$. □

1.2.9 Exercise 9

Let G be the group of rigid motions in $\mathbb{R}^3$ of a tetrahedron. Show that $|G| = 12$.

Proof. A tetrahedron has 4 vertices. Label them from 1 to 4. Then a rigid motion in G can send vertex 1 to 4 possible places. Once the new position of vertex 1 has been chosen, there are three adjacent vertices at which to place vertex 2. The positions of the remaining two vertices will then be completely determined by the positions of the first two. Therefore there are $4(3) = 12$ possible symmetries, so $|G| = 12$. □

1.2.10 Exercise 10

Let G be the group of rigid motions in $\mathbb{R}^3$ of a cube. Show that $|G| = 24$.

Proof. A cube has 8 vertices, and each vertex has 3 adjacent vertices. So there are 8 possibilities for the position of the first vertex, followed by 3 possibilities for the position of the second, resulting in $8(3) = 24$ symmetries. So $|G| = 24$. □

1.2.11 Exercise 11

Let G be the group of rigid motions in $\mathbb{R}^3$ of an octahedron. Show that $|G| = 24$.

Proof. An octahedron has 6 vertices and each vertex has 4 adjacent vertices. So, using the same reasoning as in the previous two exercises, we get $|G| = 6(4) = 24$. □

1.2.12 Exercise 12

Let G be the group of rigid motions in $\mathbb{R}^3$ of a dodecahedron. Show that $|G| = 60$.

Proof. We have 20 vertices, and each vertex has 3 neighboring vertices. So $|G| = 20(3) = 60$. □

1.2.13 Exercise 13

Let G be the group of rigid motions in $\mathbb{R}^3$ of an icosahedron. Show that $|G| = 60$.

Proof. We have 12 vertices, with each vertex adjacent to 5 vertices, giving $|G| = 12(5) = 60$. □

1.2.14 Exercise 14

Find a set of generators for $\mathbb{Z}$.

Solution. $\mathbb{Z}$ is generated by $\{1\}$ since each $n \in \mathbb{Z}$ can be written as $n1 = n$. □

1.2.15 Exercise 15

Find a set of generators and relations for $\mathbb{Z}/n\mathbb{Z}$.

Proof. Similar to the previous exercise, $\{\bar{1}\}$ can generate $\mathbb{Z}/n\mathbb{Z}$ since every element can be expressed as a repeated addition of $\bar{1}$. $\bar{1}$ satisfies the relation $n\bar{1} = \bar{0}$. □

1.2.16 Exercise 16

Show that the group $\langle x_1, y_1 \mid x_1^2 = y_1^2 = (x_1y_1)^2 = 1\rangle$ is the dihedral group D_4 (where x_1 may be replaced by the letter r and y_1 by s).

Proof. D_4 has the usual presentation $\langle r, s \mid r^2 = s^2 = 1, rs = sr^{-1}\rangle$. Since $r = r^{-1}$, that last relation become $rs = sr$. Let $x_1 = r$ and $y_1 = s$. Then $rs = sr$ implies $(x_1y_1)^2 = (rs)^2 = rsrs = r^2s^2 = 1$. On the other hand, if $(rs)^2 = 1$, then $rsrs = 1$ and, multiplying on the left by r and on the right by s, this becomes $sr = rs$. So the relations $rs = sr$ and $(x_1y_1)^2 = 1$ are equivalent. Therefore the above group is D^4. □

1.2.17 Exercise 17

Let X_{2n} be the group with presentation

$$X_{2n} = \langle x, y \mid x^n = y^2 = 1,\ xy = yx^2 \rangle.$$

(a) Show that if $n = 3k$ then X_{2n} has order 6, and it has the same generators and relations as D_6 when x is replaced by r and y by s.

Proof. Let $n = 3k$. Suppose $x^n = y^2 = 1$ and that $xy = yx^2$. Note that, as shown in the text,

$$x = xy^2 = yx^2y = yxyx^2 = y^2x^4 = x^4$$

and the cancellation law implies $x^3 = 1$. Letting $x = r$ and $y = s$, we then have $r^3 = s^2 = 1$ and

$$rs = xy = yx^2 = sr^2 = sr^{-1}.$$

Now suppose that $r^3 = s^2 = 1$ and $rs = sr^{-1}$. Then

$$x^n = x^{3k} = (r^3)^k = 1^k = 1,$$

$y^2 = s^2 = 1$, and

$$xy = rs = sr^{-1} = sr^2 = yx^2.$$

Since the generators and relations are the same, X_{2n} is D_6 and has order 6. □

(b) Show that if $(3, n) = 1$, then x satisfies the additional relation: $x = 1$. In this case deduce that X_{2n} has order 2.

Proof. Using the same argument as in the previous part, we must have $x^3 = 1$. If $(3, n) = 1$ then either $n = 3k + 1$ or $n = 3k + 2$ for some integer k. If $n = 3k + 1$ then

$$x = 1^k x = (x^3)^k x = x^{3k}x = x^{3k+1} = x^n = 1,$$

and if $n = 3k + 2$ then

$$x^{-1} = 1^{k+1}x^{-1} = (x^3)^{k+1}x^{-1} = x^{3k+3}x^{-1} = x^{3k+2} = x^n = 1.$$

But if $x^{-1} = 1$ then $x = 1$. In either case, the relation $x = 1$ holds so X_{2n} is the set $\{1, y\}$ with the relation $y^2 = 1$, so $|X_{2n}| = 2$. □

1.2.18 Exercise 18

Let Y be the group with presentation

$$Y = \langle u, v \mid u^4 = v^3 = 1,\ uv = v^2u^2 \rangle.$$

(a) Show that $v^2 = v^{-1}$.

Proof. $v(v^2) = v^3 = 1$ which implies $v^2 = v^{-1}$. □

(b) Show that v commutes with u^3.

Proof. Since

$$v^2u^3v = (v^2u^2)(uv) = (uv)(v^2u^2) = uv^3u^2 = u^3,$$

we have

$$vu^3 = v(v^2u^3v) = v^3u^3v = u^3v,$$

so v commutes with u^3. □

(c) Show that v commutes with u.

Proof. Since $u^4 = 1$, we have $u^9 = u^4u^4u = u$. And since v commutes with u^3 we have

$$uv = u^9v = u^6vu^3 = u^3vu^6 = vu^9 = vu.$$

Therefore v commutes with u. □

(d) Show that $uv = 1$.

Proof. Since u and v commute, we get

$$uv = (uv)(u^4v^3) = u^5v^4 = (v^2u^2)(u^3v^2) = (uv)(u^3v^2) = u^4v^3 = 1.$$ □

(e) Show that $u = 1$, deduce that $v = 1$, and conclude that $Y = 1$.

Proof. Since $u^4v^3 = 1$ we have

$$1 = u^4v^3 = u^3(uv)v^2 = u^3v^2 = u^2(uv)v = u^2v = u(uv) = u.$$

Then $v = uv = 1$ so that 1 is the only element of Y. Y is therefore the trivial group of order 1. □

1.3 Symmetric Groups

1.3.1 Exercise 1

Let σ be the permutation

$$1 \mapsto 3 \quad 2 \mapsto 4 \quad 3 \mapsto 5 \quad 4 \mapsto 2 \quad 5 \mapsto 1$$

and let τ be the permutation

$$1 \mapsto 5 \quad 2 \mapsto 3 \quad 3 \mapsto 2 \quad 4 \mapsto 4 \quad 5 \mapsto 1.$$

Find the cycle decompositions of each of the following permutations: σ, τ, σ^2, $\sigma\tau$, $\tau\sigma$, and $\tau^2\sigma$.

Solution. Applying the permutations from right to left, we get

$$\begin{aligned}\sigma &= (1\,3\,5)(2\,4)\\ \tau &= (1\,5)(2\,3)\\ \sigma^2 &= (1\,5\,3)\\ \sigma\tau &= (2\,5\,3\,4)\\ \tau\sigma &= (1\,2\,4\,3)\end{aligned}$$

and

$$\tau^2\sigma = (1\,3\,5)(2\,4). \qquad \square$$

1.3.2 Exercise 2

Let σ be the permutation

$1 \mapsto 13$	$2 \mapsto 2$	$3 \mapsto 15$	$4 \mapsto 14$	$5 \mapsto 10$
$6 \mapsto 6$	$7 \mapsto 12$	$8 \mapsto 3$	$9 \mapsto 4$	$10 \mapsto 1$
$11 \mapsto 7$	$12 \mapsto 9$	$13 \mapsto 5$	$14 \mapsto 11$	$15 \mapsto 8$

and let τ be the permutation

$1 \mapsto 14$	$2 \mapsto 9$	$3 \mapsto 10$	$4 \mapsto 2$	$5 \mapsto 12$
$6 \mapsto 6$	$7 \mapsto 5$	$8 \mapsto 11$	$9 \mapsto 15$	$10 \mapsto 3$
$11 \mapsto 8$	$12 \mapsto 7$	$13 \mapsto 4$	$14 \mapsto 1$	$15 \mapsto 13.$

Find the cycle decomposition of the following permutations: σ, τ, σ^2, $\sigma\tau$, $\tau\sigma$, and $\tau^2\sigma$.

Solution. We find

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

and

$$\tau^2\sigma = (1\ 2\ 15\ 8\ 3\ 4\ 14\ 11\ 12\ 13\ 7\ 5\ 10). \qquad \square$$

1.3.3 Exercise 3

For each of the permutations whose cycle decompositions were computed in the preceding two exercises compute its order.

Solution. For the first exercise, $\sigma = (1\,3\,5)(2\,4)$, $\sigma^2 = (1\,5\,3)$, $\sigma^3 = (2\,4)$, $\sigma^4 = (1\,3\,5)$, $\sigma^5 = (1\,5\,3)(2\,4)$ and $\sigma^6 = 1$. Therefore $|\sigma| = 6$. Similarly, $\tau = (1\,5)(2\,3)$ and $\tau^2 = 1$, so $|\tau| = 2$. σ^2 is a 3-cycle and so has order 3, and $\sigma\tau$ and $\tau\sigma$ are both 4-cycles and so have order 4. Lastly, $\tau^2\sigma = \sigma$ so $|\tau^2\sigma| = 6$.

For the second exercise, we could proceed in the same way. Or we could observe that, since a t-cycle has order t, the order of a product of disjoint cycles will be the least common multiple of the lengths of each cycle. This gives

$$\begin{aligned} |\sigma| &= [3,4,6] = 12, \\ |\tau| &= [2,3,5] = 30, \\ |\sigma^2| &= [2,3] = 6, \\ |\sigma\tau| &= [2,3,6] = 6, \\ |\tau\sigma| &= [2,3,6] = 6, \end{aligned}$$

and

$$|\tau^2\sigma| = 13.$$

□

1.3.4 Exercise 4

Compute the order of each of the elements in the following groups:

(a) S_3

Solution. All elements in S_3 can be written as a single t-cycle, with t being the order of the element:

Permutation	Order in S_3
1	1
$(1\,2)$	2
$(1\,3)$	2
$(2\,3)$	2
$(1\,2\,3)$	3
$(1\,3\,2)$	3

□

(b) S_4

Solution. The order of each element in S_4 is simply the least common multiple of the lengths of each cycle in its cycle decomposition:

Permutation	Order	Permutation	Order	Permutation	Order
1	1	(1 2 4)	3	(1 3)(2 4)	2
(1 2)	2	(1 3 4)	3	(1 4)(2 3)	2
(1 3)	2	(2 3 4)	3	(1 2 3 4)	4
(1 4)	2	(1 3 2)	3	(1 2 4 3)	4
(2 3)	2	(1 4 2)	3	(1 3 2 4)	4
(2 4)	2	(1 4 3)	3	(1 3 4 2)	4
(3 4)	2	(2 4 3)	3	(1 4 2 3)	4
(1 2 3)	3	(1 2)(3 4)	2	(1 4 3 2)	4

□

1.3.5 Exercise 5

Find the order of (1 12 8 10 4)(2 13)(5 11 7)(6 9).

Solution. Since the cycles are disjoint, the order of this element in S_{13} is the least common multiple of the cycle lengths: $[2, 3, 5] = 30$. □

1.3.6 Exercise 6

Write out the cycle decomposition of each element of order 4 in S_4.

Solution. See Exercise 1.3.4. □

1.3.7 Exercise 7

Write out the cycle decomposition of each element of order 2 in S_4.

Solution. See Exercise 1.3.4. □

1.3.8 Exercise 8

Prove that if $\Omega = \{1, 2, 3, \dots\}$ then S_Ω is an infinite group.

Proof. Let n be any positive integer and consider the permutation σ_n which sends $2n-1$ to $2n$ and sends $2n$ to $2n-1$, while fixing all other elements in Ω. Clearly $\sigma_n \in S_\Omega$.

Now, if i and j are distinct positive integers, then the numbers $2i-1$, $2i$, $2j-1$, $2j$ are distinct from one another, so that σ_i and σ_j have cycle decompositions that are disjoint. Thus $\sigma_1, \sigma_2, \dots, \sigma_n, \dots$ are distinct elements in S_Ω, and therefore S_Ω is infinite. □

1.3.9 Exercise 9

(a) Let σ be the 12-cycle (1 2 3 4 5 6 7 8 9 10 11 12). For which positive integers i is σ^i also a 12-cycle?

Solution. By applying σ twice we can determine that

$$\sigma^2 = (1\ 3\ 5\ 7\ 9\ 11)(2\ 4\ 6\ 8\ 10\ 12).$$

So σ^2 is not a 12-cycle. In this way we can also determine that σ^3 and σ^4 are also not 12-cycles. However,

$$\sigma^5 = (1\ 6\ 11\ 4\ 9\ 2\ 7\ 12\ 5\ 10\ 3\ 8)$$

so σ^5 is a 12-cycle.

Continuing in this way, we can see that σ^6 consists of a product of 2-cycles, σ^7 is a 12-cycle, σ^8 is a product of 3-cycles, σ^9 is a product of 4-cycles, σ^{10} is a product of 6-cycles, and σ^{11} is a 12-cycle. And higher powers will simply repeat the pattern.

Therefore, σ^i is a 12-cycle for $i = 1, 5, 7, 11$ as well as any integers which have a remainder of $1, 5, 7$, or 11 when divided by 12. We can also characterize these values as being precisely those values of i for which $(12, i) = 1$. □

(b) Let τ be the 8-cycle $(1\,2\,3\,4\,5\,6\,7\,8)$. For which positive integers i is τ^i also an 8-cycle?

Solution. As in the previous part, 8-cycles will be formed from any exponent i which is coprime to 8, that is, any i such that $(8, i) = 1$. This means that $i = 1, 3, 5, 7$ or any congruent values modulo 8. □

(c) Let ω be the 14-cycle $(1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ 10\ 11\ 12\ 13\ 14)$. For which positive integers i is ω^i also a 14-cycle.

Solution. Again, it is easy to verify that values of i for which $(14, i) = 1$ will produce 14-cycles. So $i = 1, 3, 5, 9, 11, 13$ or congruent values modulo 14. □

1.3.10 Exercise 10

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

Proof. Fix a positive integer m. We will use induction on i to show that $\sigma^i(a_k) = a_{k+i}$ for each positive integer i. Since σ cyclically permutes $a_1, \ldots, a_m$, we have $\sigma(a_k) = a_{k+1}$ for each k (taking $a_{m+1} = a_1$), so the base case is satisfied.

Now suppose $\sigma^i(a_k) = a_{k+i}$ for some positive integer i. Then

$$\begin{aligned}\sigma^{i+1}(a_k) &= \sigma(\sigma^i(a_k)) \\ &= \sigma(a_{k+i}) \\ &= a_{k+i+1},\end{aligned}$$

again replacing $k + i$ and $k + i + 1$ with their least positive residues mod m. This completes the inductive step, so $\sigma^i(a_k) = a_{k+i}$ for each integer $i > 0$.

Finally, if $1 \leq i < m$ then σ^i sends a_1 to $a_{1+i} \neq a_1$ so that σ^i is not the identity. But σ^m sends a_k to $a_{k+m} = a_k$ for each k. Therefore $\sigma^m = 1$, which shows that $|\sigma| = m$. □

1.3.11 Exercise 11

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

Proof. Fix a value for i. For the remainder of the proof, given a variable k, let k^* denote the least positive residue of k modulo m. That is, let k^* be the smallest positive integer such that $k^* \equiv k \pmod{m}$.

Now, if $(i, m) = 1$, then the residues i^*, $(2i)^*$, $\ldots$, $((m-1)i)^*$ must be distinct. To see this, note that i has a multiplicative inverse (by Proposition 4 of Section 0.3), so if s and t are integers with $si \equiv ti \pmod{m}$, it follows that $s \equiv t \pmod{m}$. Now, observe that $\sigma^i(m) = i^*$, $\sigma^i(i^*) = (2i)^*$, and in general, $\sigma^i((ki)^*) = ((k+1)i)^*$. So σ^i is the m-cycle

$$\sigma^i = (m\ i^*\ (2i)^*\ (3i)^*\ \ldots\ ((m-1)i)^*).$$

To prove the other direction, suppose σ^i is an m-cycle and let $d = (i, m)$. Then there are integers x and y such that $dx = i$ and $dy = m$. Then

$$(\sigma^i)^y = (\sigma^{dx})^y = (\sigma^{dy})^x = (\sigma^m)^x = 1^x = 1.$$

Therefore $|\sigma^i| \leq y$. But σ^i is an m-cycle, so its order is m. Therefore $y = m$ and $d = 1$. Hence i is relatively prime to m. □

1.3.12 Exercise 12

(a) If $\tau = (1\ 2)(3\ 4)(5\ 6)(7\ 8)(9\ 10)$ determine whether there is an n-cycle σ $(n \geq 10)$ with $\tau = \sigma^k$ for some integer k.

Solution. Consider the n-cycle

$$\sigma = (1\ 3\ 5\ 7\ 9\ 2\ 4\ 6\ 8\ 10).$$

Then $\sigma^5 = \tau$. □

(b) If $\tau = (1\ 2)(3\ 4\ 5)$ determine whether there is an n-cycle $(n \geq 5)$ with $\tau = \sigma^k$ for some integer k.

Solution. Suppose that it is possible, and let σ be an n-cycle such that $\sigma^k = \tau$.

If $n > 5$ then σ^k must fix $6, 7, \ldots$. But if σ is an n-cycle, then the only way σ^k can fix any of these values is if it fixes every value, that is, if $\sigma^k = 1 \neq \tau$. Therefore we can suppose that $n = 5$.

Now since σ^k is not an n-cycle, we know by the previous exercise that k is not relatively prime to n. But $n = 5$ is prime, so $5 \mid k$ and there is an integer ℓ such that $k = 5\ell$. Then $\sigma^k = (\sigma^5)^\ell = 1^\ell = 1 \neq \tau$. This is a contradiction, so our assumption that σ exists was invalid. □

1.3.13 Exercise 13

Show that an element has order 2 in S_n if and only if its cycle decomposition is a product of commuting 2-cycles.

Proof. Let n be a positive integer and suppose $\sigma \in S_n$ has order 2. Let i, j be distinct integers in $\{1, 2, \ldots, n\}$ such that $\sigma(i) = j$. Then since $\sigma^2 = 1$, we must have $\sigma(j) = i$. Thus $(i\ j)$ is a cycle in the cycle decomposition of σ. And this is true for any such integers, so that no cycle in the decomposition of σ has length more than 2. Thus we can write σ as a product of disjoint (and hence commuting) 2-cycles.

Now suppose that σ is a member of S_n such that its cycle decomposition is a product of commuting 2-cycles, so that

$$\sigma = (a_1\ b_1)(a_2\ b_2)(a_3\ b_3)\cdots(a_k\ b_k).$$

Since each cycle commutes, we have

$$\sigma^2 = (a_1\ b_1)^2(a_2\ b_2)^2\cdots(a_k\ b_k)^2 = 1^k = 1.$$

Since σ is not the identity, $|\sigma| = 2$. □

1.3.14 Exercise 14

Let p be a prime. Show that an element has order p in S_n if and only if its cycle decomposition is a product of commuting p-cycles. Show by an explicit example that this need not be the case if p is not prime.

Proof. This is a generalization of the previous exercise, and the proof will be similar. Fix a positive integer n.

Suppose that $\sigma \in S_n$ has order p. Write down the cycle decomposition of σ,

$$\sigma = \tau_1\tau_2\cdots\tau_k,$$

where each τ_i is a cycle and τ_i is disjoint from τ_j when $i \neq j$. Since these cycles are disjoint, they commute with each other and we can write

$$1 = \sigma^p = \tau_1^p\tau_2^p\cdots\tau_k^p.$$

Since the original cycles were disjoint, it follows that τ_i^p and τ_j^p are disjoint for $i \neq j$, and we must have $\tau_i^p = 1$ for each i. This implies that the length of the cycle τ_i divides p. But p is prime, so τ_i is either a p-cycle or the identity. Therefore σ is the product of commuting p-cycles.

To prove the other direction, suppose that $\sigma \in S_n$ can be written as a product of commuting p-cycles for p a prime, so that

$$\sigma = \tau_1\tau_2\cdots\tau_k$$

with each τ_i a p-cycle. Since the cycles commute, we have

$$\sigma^p = \tau_1^p\tau_2^p\cdots\tau_k^p = 1^k = 1.$$

So $|\sigma| \leq p$. On the other hand, since τ is a p-cycle, $\tau^t \neq 1$ for any positive integer t less than p. So σ^t cannot be the identity permutation. Therefore $|\sigma| = p$.

Lastly, suppose p is not prime. For example, take $p = 6$ and $n = 6$. Then $\sigma = (1\,2)(3\,4\,5)$ has order 6 but it cannot be written as a product of commuting 6-cycles. □

1.3.15 Exercise 15

Prove that the order of an element in S_n equals the least common multiple of the lengths of the cycles in its cycle decomposition.

Proof. Let $\sigma \in S_n$ have the cycle decomposition

$$\sigma = \tau_1\tau_2\tau_3\cdots\tau_k,$$

where each τ_i is a cycle and the cycles are pairwise disjoint (and therefore commute). Suppose $|\sigma| = n$. Then

$$1 = \sigma^n = \tau_1^n\tau_2^n\cdots\tau_k^n,$$

which implies that $\tau_i^n = 1$ for each i (the τ_i's are disjoint, so if any $\tau_i^n \neq 1$ then $\sigma^n \neq 1$). So if τ_i is a t-cycle, it follows that $t \mid n$. Therefore n is a common multiple of the lengths of each cycle in the cycle decomposition of σ.

On the other hand, if m is any common multiple of these lengths, then $\sigma^m = \tau_1^m\cdots\tau_k^m = 1$, so we must have $n \leq m$ which shows that n is the *least* common multiple of the cycle lengths. □

1.3.16 Exercise 16

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

$$\frac{n(n-1)(n-2)\cdots(n-m+1)}{m}. \tag{1.1}$$

Proof. We count the number of ways to form an m-cycle. There are n choices for the value in the first position, $n-1$ choices for the value in the second position, ..., and $(n-m+1)$ choices for the mth position. However, each cycle can be represented in m different ways, depending on the choice of starting value. So the actual number of distinct m-cycles is given by the expression (1.1). □

1.3.17 Exercise 17

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

Proof. Using the same reasoning as in the previous exercise, there are $n(n-1)/2$ ways to choose the first 2-cycle, and there are $(n-2)(n-3)/2$ ways to choose the second 2-cycle. However, the order of the two 2-cycles doesn't matter, so we divide the product by 2 to get $n(n-1)(n-2)(n-3)/8$ possibilities. □

1.3.18 Exercise 18

Find all numbers n such that S_5 contains an element of order n.

Solution. For each n with $1 \leq n \leq 5$, we can find an n-cycle in S_5. $n = 6$ is also possible, for example, with $(1\,2)(3\,4\,5)$. But a combination of longer cycles of different lengths is not possible since the underlying set $\{1, 2, 3, 4, 5\}$ only has five elements. Therefore the only possibilities for n are $1, 2, 3, 4, 5$, and 6. □

1.3.19 Exercise 19

Find all numbers n such that S_7 contains an element of order n.

Solution. Clearly $n = 1, 2, \ldots, 7$ are all valid. If $\sigma \in S_7$ contains a 2-cycle, then the only other cycles of different lengths that can be in the cycle decomposition of σ is a 3-cycle, a 4-cycle, or a 5-cycle. The $2, 3$ combination would have an order of 6, the $2, 4$ combination would have an order of 4, and the $2, 5$ combination would have an order of 10. We could also have a 3-cycle together with a 4-cycle, resulting in a permutation with order 12. So the only possible orders are $n = 1, 2, 3, 4, 5, 6, 7, 10$, and 12. □

1.3.20 Exercise 20

Find a set of generators and relations for S_3.

Solution. The set S_3 contains the six permutations 1, $(1\,2)$, $(1\,3)$, $(2\,3)$, $(1\,2\,3)$, and $(1\,3\,2)$. By taking powers of each element we can see that S_3 is not cyclic, so we need at least two generators. Let $\alpha = (1\,2)$ and $\beta = (1\,2\,3)$. Then $(1\,3) = \beta\alpha$, $(2\,3) = \alpha\beta$, and $(1\,3\,2) = \beta^2$. We have the relation $\alpha^2 = \beta^3 = 1$. But this is not enough information to deduce that $\alpha\beta$ has order 2, for example. So we may include $(\alpha\beta)^2 = 1$, which is enough to determine the orders of the remaining elements. So

$$S_3 = \langle \alpha, \beta \mid \alpha^2 = \beta^3 = (\alpha\beta)^2 = 1 \rangle.$$ □

1.4 Matrix Groups

Let F be a field and let $n \in \mathbb{Z}^+$.

1.4.1 Exercise 1

Prove that $|GL_2(\mathbb{F}_2)| = 6$.

Proof. Consider the matrix

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}, \quad a, b, c, d \in \mathbb{F}_2.$$

The determinant of this matrix is $ad - bc$. To be nonzero, either a and b are nonzero, or b and c are nonzero, but not both. So the members of $GL_2(\mathbb{F}_2)$ are

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \text{ and } \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}. \qquad \square$$

1.4.2 Exercise 2

Write out all the elements of $GL_2(\mathbb{F}_2)$ and compute the order of each element.

Solution. Direct computation produces the following orders:

A	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$	$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$	$\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$
$\lvert A \rvert$	1	2	2	2	3	3

$\square$

1.4.3 Exercise 3

Show that $GL_2(\mathbb{F}_2)$ is non-abelian.

Proof. We have

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

but

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Therefore $GL_2(\mathbb{F}_2)$ is non-abelian. $\square$

1.4.4 Exercise 4

Show that if n is not prime then $\mathbb{Z}/n\mathbb{Z}$ is not a field.

Proof. Let n be a composite number, so that $n = ab$ with $a, b > 1$. Then $(a, n) = a > 1$, so by Proposition 4 of Section 0.3, a does not have a multiplicative inverse. And a is nonzero, so $\mathbb{Z}/n\mathbb{Z}$ is not a field. $\square$

1.4.5 Exercise 5

Show that $GL_n(F)$ is a finite group if and only if F has a finite number of elements.

Proof. First, if F is finite, then $GL_n(F)$ must be finite since there are only finitely many $n \times n$ matrices with entries from F.

On the other hand, suppose F is not finite. Then for every $\alpha \in F$ with $\alpha \neq 0$, the matrix αI has nonzero determinant. Therefore $GL_n(F)$ is infinite. □

1.4.6 Exercise 6

If $|F| = q$ is finite, prove that $|GL_n(F)| < q^{n^2}$.

Proof. Since F has q elements, there are only q^{n^2} possible $n \times n$ matrices over F that can be formed. Since at least one of these matrices has zero determinant (take for example the zero matrix), it follows that $|GL_n(F)| < q^{n^2}$. □

1.4.7 Exercise 7

Let p be a prime. Prove that the order of $GL_2(\mathbb{F}_p)$ is $p^4 - p^3 - p^2 + p$.

Proof. Let A be a 2×2 matrix over $\mathbb{F}_p$ that is *not* in $GL_2(\mathbb{F}_p)$. Write

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

and note that $ad - bc = 0$. We have two cases: $a = 0$ or $a \neq 0$.

First, if $a = 0$ then d can take any of p possible values, while $bc = 0$. Again there are two cases: if $b = 0$ then there are p possible values that c can take. If $b \neq 0$ (this can happen in $p - 1$ ways), then $c = b^{-1}$. So there are p possibilities for d, multiplied by $p + (p - 1) = 2p - 1$ possibilities for b and c, which gives a total of $2p^2 - p$ choices for the case where $a = 0$.

Next, if $a \neq 0$, this can happen in $p - 1$ ways. Then $d = bca^{-1}$. Now b and c can take any value and then d is determined by the other variables, so there are $p^2(p - 1) = p^3 - p^2$ possibilities for this case.

Totaling the two cases, we find that there are

$$(p^3 - p^2) + (2p^2 - p) = p^3 + p^2 - p$$

possible matrices that A can be. Since there are p^4 total 2×2 matrices over $\mathbb{F}_p$, it follows that

$$|GL_2(\mathbb{F}_p)| = p^4 - p^3 - p^2 + p.$$ □

1.4.8 Exercise 8

Show that $GL_n(F)$ is non-abelian for any $n \geq 2$ and any F.

Proof. Note that every field has an additive identity 0 and a distinct multiplicative identity 1, so by restricting our proof to using only these two values from F, the result will hold for any F.

We will use induction on n. The base case $n = 2$ was proved in Exercise 1.4.3 (the proof works for any F as noted above). Now assume that $GL_{n-1}(F)$ is

non-abelian for some $n \geq 3$, and let A and B be non-commuting members of $GL_{n-1}(F)$. Then, using block matrices, we get

$$\begin{pmatrix} A & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} B & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} AB & 0 \\ 0 & 1 \end{pmatrix} \neq \begin{pmatrix} BA & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} B & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} A & 0 \\ 0 & 1 \end{pmatrix}.$$

Therefore $GL_n(F)$ is non-abelian, and this completes the proof. □

1.4.9 Exercise 9

Prove that the binary operation of matrix multiplication of 2×2 matrices with real number entries is associative.

Proof. Direct computation gives

$$\begin{aligned} \left[\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} e & f \\ g & h \end{pmatrix}\right] \begin{pmatrix} i & j \\ k & l \end{pmatrix} &= \begin{pmatrix} ae+bg & af+bh \\ ce+dg & cf+dh \end{pmatrix} \begin{pmatrix} i & j \\ k & l \end{pmatrix} \\ &= \begin{pmatrix} (ae+bg)i+(af+bh)k & (ae+bg)j+(af+bh)l \\ (ce+dg)i+(cf+dh)k & (ce+dg)j+(cf+dh)l \end{pmatrix}, \end{aligned}$$

while

$$\begin{aligned} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \left[\begin{pmatrix} e & f \\ g & h \end{pmatrix} \begin{pmatrix} i & j \\ k & l \end{pmatrix}\right] &= \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} ei+fk & ej+fl \\ gi+hk & gj+hl \end{pmatrix} \\ &= \begin{pmatrix} a(ei+fk)+b(gi+hk) & a(ej+fl)+b(gj+hl) \\ c(ei+fk)+d(gi+hk) & c(ej+fl)+d(gj+hl) \end{pmatrix}. \end{aligned}$$

Now, by comparing these two matrices using the associative and commutative properties of the real numbers, the result will follow. □

1.4.10 Exercise 10

Let

$$G = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \;\middle|\; a, b, c \in \mathbb{R}, a \neq 0, c \neq 0 \right\}.$$

(a) Compute the product of $\begin{pmatrix} a_1 & b_1 \\ 0 & c_1 \end{pmatrix}$ and $\begin{pmatrix} a_2 & b_2 \\ 0 & c_2 \end{pmatrix}$ to show that G is closed under matrix multiplication.

Solution. We have

$$\begin{pmatrix} a_1 & b_1 \\ 0 & c_1 \end{pmatrix} \begin{pmatrix} a_2 & b_2 \\ 0 & c_2 \end{pmatrix} = \begin{pmatrix} a_1a_2 & a_1b_2+b_1c_2 \\ 0 & c_1c_2 \end{pmatrix} \in G,$$

so G is closed under multiplication. □

(b) Find the matrix inverse of $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$ and deduce that G is closed under inverses.

Solution. Since $ac \neq 0$ the matrix is invertible and we get

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}^{-1} = \frac{1}{ac}\begin{pmatrix} c & -b \\ 0 & a \end{pmatrix} = \begin{pmatrix} \frac{1}{a} & -\frac{b}{ac} \\ 0 & \frac{1}{c} \end{pmatrix} \in G.$$

So, G is closed under inverses. □

(c) Deduce that G is a subgroup of $GL_2(\mathbb{R})$.

Solution. This follows from Exercise 1.1.26. □

(d) Prove that the set of elements of G whose two diagonal entries are equal (i.e., $a = c$) is also a subgroup of $GL_2(\mathbb{R})$.

Solution. Call this set H. We have

$$\begin{pmatrix} a_1 & b_1 \\ 0 & a_1 \end{pmatrix}\begin{pmatrix} a_2 & b_2 \\ 0 & a_2 \end{pmatrix} = \begin{pmatrix} a_1a_2 & a_1b_2 + b_1a_2 \\ 0 & a_1a_2 \end{pmatrix} \in H$$

and

$$\begin{pmatrix} a & b \\ 0 & a \end{pmatrix}^{-1} = \begin{pmatrix} \frac{1}{a} & -\frac{b}{a^2} \\ 0 & \frac{1}{a} \end{pmatrix} \in H.$$

H is closed under matrix multiplication and inversion, so H is a subgroup of $GL_2(\mathbb{R})$. □

1.4.11 Exercise 11

Let

$$H(F) = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \;\middle|\; a, b, c \in F \right\}.$$

Let

$$X = \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \quad \text{and} \quad Y = \begin{pmatrix} 1 & d & e \\ 0 & 1 & f \\ 0 & 0 & 1 \end{pmatrix}$$

be elements of $H(F)$.

(a) Compute the matrix XY and deduce that $H(F)$ is closed under matrix multiplication. Exhibit explicit matrices such that $XY \neq YX$ (so that $H(F)$ is always non-abelian).

Solution. We have

$$XY = \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & d & e \\ 0 & 1 & f \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a+d & af+b+e \\ 0 & 1 & c+f \\ 0 & 0 & 1 \end{pmatrix} \in H(F),$$

so $H(F)$ is closed under multiplication. Moreover,

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

while

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

so $H(F)$ is always non-abelian. □

(b) Find an explicit formula for the matrix inverse X^{-1} and deduce that $H(F)$ is closed under inverses.

Solution. Let

$$Z=\begin{pmatrix}1&-a&ca-b\\0&1&-c\\0&0&1\end{pmatrix}.$$

By performing the multiplication, it is easily seen that $XZ=ZX=I$, where I is the 3×3 identity matrix. It follows that $Z=X^{-1}$ and since $Z\in H(F)$, we see that $H(F)$ is closed under inverses. □

(c) Prove the associative law for $H(F)$ and deduce that $H(F)$ is a group of order $|F|^3$.

Solution. We have

$$\begin{aligned}&\left[\begin{pmatrix}1&a&b\\0&1&c\\0&0&1\end{pmatrix}\begin{pmatrix}1&d&e\\0&1&f\\0&0&1\end{pmatrix}\right]\begin{pmatrix}1&g&h\\0&1&i\\0&0&1\end{pmatrix}\\&\qquad=\begin{pmatrix}1&a+d&af+b+e\\0&1&c+f\\0&0&1\end{pmatrix}\begin{pmatrix}1&g&h\\0&1&i\\0&0&1\end{pmatrix}\\&\qquad=\begin{pmatrix}1&a+d+g&af+ai+b+di+e+h\\0&1&c+f+i\\0&0&1\end{pmatrix}\end{aligned}$$

and

$$\begin{aligned}&\begin{pmatrix}1&a&b\\0&1&c\\0&0&1\end{pmatrix}\left[\begin{pmatrix}1&d&e\\0&1&f\\0&0&1\end{pmatrix}\begin{pmatrix}1&g&h\\0&1&i\\0&0&1\end{pmatrix}\right]\\&\qquad=\begin{pmatrix}1&a&b\\0&1&c\\0&0&1\end{pmatrix}\begin{pmatrix}1&d+g&di+e+h\\0&1&f+i\\0&0&1\end{pmatrix}\\&\qquad=\begin{pmatrix}1&a+d+g&af+ai+b+di+e+h\\0&1&c+f+i\\0&0&1\end{pmatrix},\end{aligned}$$

so multiplication in $H(F)$ is associative. This shows that $H(F)$ is a subgroup of $GL_3(F)$.

Now, consider the matrix X above. If $|F|=n<\infty$ then each of a,b,c can take any of n values each. So $|H(F)|=n^3$. □

(d) Find the order of each element of the finite group $H(\mathbb{Z}/2\mathbb{Z})$.

Solution. Obviously $|I| = 1$. For the rest, we find

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}^2 = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}^2 = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}^2 = I,$$

so these have order 2,

$$\begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}^2 = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}^2 = I,$$

so these also have order 2, and

$$\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}^4 = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}^4 = I,$$

so these have order 4. $|H(\mathbb{Z}/2\mathbb{Z})| = 2^3 = 8$, so these are all the elements in the group. □

(e) Prove that every nonidentity element of the group $H(\mathbb{R})$ has infinite order.

Solution. We will show by induction on n that

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}^n = \begin{pmatrix} 1 & na & nb + n(n-1)ac/2 \\ 0 & 1 & nc \\ 0 & 0 & 1 \end{pmatrix}. \tag{1.2}$$

Since any nonidentity element has one of a, b, or c nonzero, this will be enough to show that the element has infinite order.

The base case $n = 1$ is evident. Suppose (1.2) holds for some $n \geq 1$. Then

$$\begin{aligned} \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}^{n+1} &= \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & na & nb + n(n-1)ac/2 \\ 0 & 1 & nc \\ 0 & 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & (n+1)a & (n+1)b + n(n+1)ac/2 \\ 0 & 1 & (n+1)c \\ 0 & 0 & 1 \end{pmatrix}, \end{aligned}$$

so (1.2) holds for all positive integers n and the result follows. □

1.5 The Quaternion Group

1.5.1 Exercise 1

Compute the order of each of the elements in Q_8.

Solution. 1 has order 1 and -1 has order 2. Since $i^2 = j^2 = k^2 = -1$, we see that i, j, k each have order 4. And since $(-i)^2 = (-j)^2 = (-k)^2 = -1$, we know that $-i$, $-j$, and $-k$ have order 4 also. □

1.5.2 Exercise 2

Write out the group tables for S_3, D_8 and Q_8.

Solution. S_3:

	1	$(1\,2)$	$(1\,3)$	$(2\,3)$	$(1\,2\,3)$	$(1\,3\,2)$
1	1	$(1\,2)$	$(1\,3)$	$(2\,3)$	$(1\,2\,3)$	$(1\,3\,2)$
$(1\,2)$	$(1\,2)$	1	$(1\,3\,2)$	$(1\,2\,3)$	$(2\,3)$	$(1\,3)$
$(1\,3)$	$(1\,3)$	$(1\,2\,3)$	1	$(1\,3\,2)$	$(1\,2)$	$(2\,3)$
$(2\,3)$	$(2\,3)$	$(1\,3\,2)$	$(1\,2\,3)$	1	$(1\,3)$	$(1\,2)$
$(1\,2\,3)$	$(1\,2\,3)$	$(1\,3)$	$(2\,3)$	$(1\,2)$	$(1\,3\,2)$	1
$(1\,3\,2)$	$(1\,3\,2)$	$(2\,3)$	$(1\,2)$	$(1\,3)$	1	$(1\,2\,3)$

D_8:

	1	r	r^2	r^3	s	sr	sr^2	sr^3
1	1	r	r^2	r^3	s	sr	sr^2	sr^3
r	r	r^2	r^3	1	sr^3	s	sr	sr^2
r^2	r^2	r^3	1	r	sr^2	sr^3	s	sr
r^3	r^3	1	r	r^2	sr	sr^2	sr^3	s
s	s	sr	sr^2	sr^3	1	r	r^2	r^3
sr	sr	sr^2	sr^3	s	r^3	1	r	r^2
sr^2	sr^2	sr^3	s	sr	r^2	r^3	1	r
sr^3	sr^3	s	sr	sr^2	r	r^2	r^3	1

Q_8:

	1	-1	i	$-i$	j	$-j$	k	$-k$
1	1	-1	i	$-i$	j	$-j$	k	$-k$
-1	-1	1	$-i$	i	$-j$	j	$-k$	k
i	i	$-i$	-1	1	k	$-k$	$-j$	j
$-i$	$-i$	i	1	-1	$-k$	k	j	$-j$
j	j	$-j$	$-k$	k	-1	1	i	$-i$
$-j$	$-j$	j	k	$-k$	1	-1	$-i$	i
k	k	$-k$	j	$-j$	$-i$	i	-1	1
$-k$	$-k$	k	$-j$	j	i	$-i$	1	-1

□

1.5.3 Exercise 3

Find a set of generators and relations for Q_8.

Solution. One presentation is

$$Q_8 = \langle -1, i, j, k \mid i^2 = j^2 = k^2 = ijk = -1 \rangle,$$

where -1 commutes with the other elements of Q_8. □

1.6 Homomorphisms and Isomorphisms

Let G and H be groups.

1.6.1 Exercise 1

Let $\varphi\colon G \to H$ be a homomorphism.

(a) Prove that $\varphi(x^n) = \varphi(x)^n$ for all $n \in \mathbb{Z}^+$.

Proof. We use induction on n. The case for $n = 1$ is clear. Suppose $\varphi(x^n) = \varphi(x)^n$ for some particular $n \in \mathbb{Z}^+$. Then

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

so the result holds for all $n \in \mathbb{Z}^+$. □

(b) Do part (a) for $n = -1$ and deduce that $\varphi(x^n) = \varphi(x)^n$ for all $n \in \mathbb{Z}$.

Solution. Let 1_G and 1_H denote the identities of G and H, respectively. Then

$$\varphi(1_G)\varphi(1_G) = \varphi(1_G) = \varphi(1_G)1_H,$$

and it follows from the cancellation law that $\varphi(1_G) = 1_H$. Since the identity is preserved, we will simply use 1 to denote the identity of both groups from this point forward.

Now, for any $x \in G$,

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

which shows that $\varphi(x^{-1}) = \varphi(x)^{-1}$. Then for $n \in \mathbb{Z}^+$,

$$\varphi(x^{-n}) = \varphi((x^n)^{-1}) = \varphi(x^n)^{-1} = \big(\varphi(x)^n\big)^{-1} = \varphi(x)^{-n}.$$

Therefore $\varphi(x^n) = \varphi(x)^n$ holds for all $n \in \mathbb{Z}$. □

1.6.2 Exercise 2

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

Proof. First suppose $|x| = n < \infty$. By the previous exercise, we have

$$\varphi(x)^n = \varphi(x^n) = \varphi(1) = 1.$$

So $|\varphi(x)| \leq n$. On the other hand, if $|\varphi(x)| = k$, then

$$\varphi(x^k) = \varphi(x)^k = 1.$$

But 1 is the only element in G which gets sent to 1 in H, since φ is a bijection. This shows that $x^k = 1$, so that $k \geq n$. Hence $|\varphi(x)| = n$.

Now suppose x has infinite order. If $|\varphi(x)| = n < \infty$, then $\varphi(x^n) = \varphi(x)^n = 1$, and since φ is a bijection we must have $x^n = 1$, a contradiction. Therefore $\varphi(x)$ must also have infinite order.

From the above we know that $|x| = |\varphi(x)|$ for each x, and since φ is a bijection this shows that G and H have the same number of elements of each order.

Finally, this result does not necessarily hold for homomorphisms. For example, let H be the trivial group $\{1\}$ and take the function $\theta\colon G \to H$ defined by $\theta(x) = 1$ for all $x \in G$. Then $\theta(x)\theta(y) = \theta(xy)$, so this is a homomorphism, but every element in H has order 1, which is not true of G (unless G is also trivial). □

1.6.3 Exercise 3

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

Solution. Since φ must be invertible (it is a bijection) and since φ^{-1} must be an isomorphism from H to G, the proof only needs to work in one direction. So let $x, y \in H$ be arbitrary, and let $a = \varphi^{-1}(x)$ and $b = \varphi^{-1}(y)$. If G is abelian, then

$$xy = \varphi(a)\varphi(b) = \varphi(ab) = \varphi(ba) = \varphi(b)\varphi(a) = yx,$$

so H is also abelian, and the proof is complete.

Note that the same result does not hold for homomorphisms. For instance, let $\varphi\colon \mathbb{Z}/2\mathbb{Z} \to D_6$ be given by $\varphi(\bar{0}) = 1$ and $\varphi(\bar{1}) = s$. Then φ is a homomorphism and $\mathbb{Z}/2\mathbb{Z}$ is abelian, but D_6 is not abelian.

However, if we add the constraint that φ is surjective, then the result does hold: Suppose G is abelian, let $x, y \in H$ be arbitrary, and pick $a \in \varphi^{-1}(x)$ and $b \in \varphi^{-1}(y)$ (that is, a and b are chosen from the fibers of φ over x and y). Then, as before,

$$xy = \varphi(a)\varphi(b) = \varphi(ab) = \varphi(ba) = \varphi(b)\varphi(a) = yx,$$

so H is abelian. □

1.6.4 Exercise 4

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

Proof. Every element in $\mathbb{R} - \{0\}$ has infinite order, aside from 1 and -1 which have orders 1 and 2, respectively. However, $\mathbb{C} - \{0\}$ has elements of order 4, namely i and $-i$. Therefore these groups are not isomorphic. □

1.6.5 Exercise 5

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

Proof. There is no bijection between $\mathbb{R}$ and $\mathbb{Q}$, since the former is uncountable and the latter is countable. Therefore the groups $(\mathbb{R}, +)$ and $(\mathbb{Q}, +)$ are not isomorphic. □

1.6.6 Exercise 6

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

Proof. Suppose the contrary, and let $\varphi\colon \mathbb{Q} \to \mathbb{Z}$ be an isomorphism. Let

$$a = \varphi(1).$$

Then

$$a = \varphi\left(\frac{1}{2} + \frac{1}{2}\right) = 2\varphi\left(\frac{1}{2}\right).$$

Therefore 2 divides a. For the same reason, we also have

$$a = 3\varphi\left(\frac{1}{3}\right).$$

So 3 divides a. Using the same argument we see that the integer a is actually divisible by every positive integer. The only way this is possible is if $a = 0$. But then, for any $n \in \mathbb{Z}$, we would have $\varphi(n) = n\varphi(1) = na = 0$. So φ is clearly not an injection, and this gives the necessary contradiction. Therefore the additive groups $\mathbb{Z}$ and $\mathbb{Q}$ are not isomorphic. □

1.6.7 Exercise 7

Prove that D_8 and Q_8 are not isomorphic.

Proof. We may simply look at the orders of the elements in each group. For example, D_8 has 4 elements with order 2 (namely, s, sr, sr^2, and sr^3), while Q_8 only has one element with order 2 (namely -1). Therefore $D_8 \ncong Q_8$. □

1.6.8 Exercise 8

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

Proof. Since S_n has order $n!$ and S_m has order $m!$, there is no bijection from S_n to S_m unless $n = m$. Therefore S_n and S_m are not isomorphic when $n \neq m$. □

1.6.9 Exercise 9

Prove that D_{24} and S_4 are not isomorphic.

Proof. D_{24} has elements of order 12, namely r, r^5, r^7, and r^{11}. However, S_4 has no elements of order 12, since every permutation in S_4 is either a 2-cycle or product of 2-cycles (which have order 2), a 3-cycle (which has order 3), or a 4-cycle (which has order 4). Since isomorphisms must preserve orders of elements, D_{24} and S_4 cannot be isomorphic. □

1.6.10 Exercise 10

Fill in the details of the proof that the symmetric group S_Δ and S_Ω are isomorphic if $|\Delta| = |\Omega|$ as follows: let $\theta\colon \Delta \to \Omega$ be a bijection. Define

$$\varphi\colon S_\Delta \to S_\Omega \quad \text{by} \quad \varphi(\sigma) = \theta \circ \sigma \circ \theta^{-1} \quad \text{for all } \sigma \in S_\Delta$$

and prove the following:

(a) φ is well defined, that is, if σ is a permutation of Δ then $\theta \circ \sigma \circ \theta^{-1}$ is a permutation of Ω.

Proof. For any permutation σ of Δ, it is clear that $\varphi(\sigma) = \theta \circ \sigma \circ \theta^{-1}$ is a function from Ω to itself. We want to show that it is a bijection.

Suppose $a, b \in \Omega$ are such that $\varphi(\sigma)(a) = \varphi(\sigma)(b)$. Since θ is an injection, this implies that $(\sigma \circ \theta^{-1})(a) = (\sigma \circ \theta^{-1})(b)$. But σ is also an injection, so $\theta^{-1}(a) = \theta^{-1}(b)$ and, similarly, we have $a = b$. This shows that $\varphi(\sigma)$ is an injection.

Now let $y \in \Omega$ be arbitrary. Then we may take

$$x = \varphi(\sigma^{-1})(y) = (\theta \circ \sigma^{-1} \circ \theta^{-1})(y)$$

so that $\varphi(\sigma)(x) = y$. This shows that $\varphi(\sigma)$ is a surjection. Hence $\varphi(\sigma)$ is a bijection from Ω to itself, that is, $\varphi(\sigma)$ is a permutation of Ω. □

(b) φ is a bijection from S_Δ to S_Ω.

Proof. Define $\psi\colon S_\Omega \to S_\Delta$ by

$$\psi(\tau) = \theta^{-1} \circ \tau \circ \theta \quad \text{for any } \tau \in S_\Omega.$$

By the same argument as in part (a), ψ is well-defined. Moreover, for any $\sigma \in S_\Delta$,

$$(\psi \circ \varphi)(\sigma) = \psi(\theta \circ \sigma \circ \theta^{-1}) = \theta^{-1} \circ \theta \circ \sigma \circ \theta^{-1} \circ \theta = \sigma,$$

and for any $\tau \in S_\Omega$,

$$(\varphi \circ \psi)(\tau) = \varphi(\theta^{-1} \circ \tau \circ \theta) = \theta \circ \theta^{-1} \circ \tau \circ \theta \circ \theta^{-1} = \tau.$$

Therefore ψ is a two-sided inverse of φ, so that φ is a bijection. □

(c) φ is a homomorphism, that is, $\varphi(\sigma \circ \tau) = \varphi(\sigma) \circ \varphi(\tau)$.

Proof. Let $\sigma, \tau \in S_\Delta$. Then

$$\varphi(\sigma) \circ \varphi(\tau) = \theta \circ \sigma \circ \theta^{-1} \circ \theta \circ \tau \circ \theta^{-1} = \theta \circ \sigma \circ \tau \circ \theta^{-1} = \varphi(\sigma \circ \tau).$$

Therefore φ is a homomorphism, and hence an isomorphism. □

1.6.11 Exercise 11

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

Proof. Define the function $\varphi\colon A \times B \to B \times A$ by

$$\varphi(a,b) = (b,a) \quad \text{for any } (a,b) \in A \times B.$$

This is a homomorphism, since

$$\varphi((a,b)(c,d)) = \varphi(ac,bd) = (bd,ac) = (b,a)(d,c) = \varphi(a,b)\varphi(c,d).$$

It is also a surjection, since for any $(b,a) \in B \times A$ we can take $(a,b) \in A \times B$ so that $\varphi(a,b) = (b,a)$. Finally, if $(a,b),(c,d) \in A \times B$ are such that $\varphi(a,b) = \varphi(c,d)$ then $(b,a) = (d,c)$. Then $b = d$ and $a = c$, so $(a,b) = (c,d)$ and φ is an injection. This shows that φ is a bijection and hence an isomorphism. □

1.6.12 Exercise 12

Let A, B, and C be groups and let $G = A \times B$ and $H = B \times C$. Prove that $G \times C \cong A \times H$.

Proof. Define $\varphi\colon G \times C \to A \times H$ as follows. For any $((a,b),c) \in G \times C$ by

$$\varphi((a,b),c) = (a,(b,c)).$$

It is very straightforward to verify that φ is a bijection and a homomorphism, and hence $G \times C \cong A \times H$. □

1.6.13 Exercise 13

Let G and H be groups and let $\varphi\colon G \to H$ be a homomorphism. Prove that the image of φ, $\varphi(G)$, is a subgroup of H. Prove that if φ is injective then $G \cong \varphi(G)$.

Proof. We know that $\varphi(G)$ is nonempty, since in particular $\varphi(1)$ is mapped to some element in H (we know from earlier exercises that the identity is preserved so $\varphi(1) = 1$, but we do not strictly need that information here). Let $a, b \in \varphi(G)$ be arbitrary. Then there exist $\alpha, \beta \in G$ such that $\varphi(\alpha) = a$, and $\varphi(\beta) = b$. Then

$$ab = \varphi(\alpha)\varphi(\beta) = \varphi(\alpha\beta),$$

so $ab \in \varphi(G)$ and $\varphi(G)$ is closed under the binary operation of H. Moreover, by Exercise 1.6.1,

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

so $\varphi(G)$ is closed under inverses. Hence $\varphi(G)$ is a subgroup of H.

Now, if we define $\varphi^*\colon G \to \varphi(G)$ by $\varphi^*(\gamma) = \varphi(\gamma)$ for each $\gamma \in G$, then φ^* is surjective by definition. If, in addition, φ is injective, then φ^* is a bijection and $G \cong \varphi(G)$. □

1.6.14 Exercise 14

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

Proof. From Exercise 1.6.1 we know that $\varphi(1_G) = 1_H$ so the kernel of φ is nonempty. Suppose $a, b \in \ker\varphi$. Then

$$\varphi(ab) = \varphi(a)\varphi(b) = 1_H 1_H = 1_H,$$

and $ab \in \ker\varphi$. Additionally, if $a \in \ker\varphi$ then

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

and $a^{-1} \in \ker\varphi$. Therefore $\ker\varphi$ is a subgroup of G. □

1.6.15 Exercise 15

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

Proof. For any $(x_1, y_1), (x_2, y_2) \in \mathbb{R}^2$, we have

$$\pi((x_1, y_1) + (x_2, y_2)) = \pi(x_1 + x_2, y_1 + y_2) = x_1 + x_2 = \pi(x_1, y_1) + \pi(x_2, y_2),$$

so π is a homomorphism. Also,

$$\ker\pi = \{(0, y) \in \mathbb{R}^2 \mid y \in \mathbb{R}\}.$$ □

1.6.16 Exercise 16

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

Proof. For any (a, b) and $(c, d) \in A \times B$, we have

$$\pi_1((a, b)(c, d)) = \pi_1(ac, bd) = ac = \pi_1(a, b)\pi_1(c, d)$$

and

$$\pi_2((a, b)(c, d)) = \pi_2(ac, bd) = bd = \pi_2(a, b)\pi_2(c, d),$$

so π_1 and π_2 are homomorphisms. Their kernels are

$$\ker\pi_1 = \{(1, b) \in A \times B \mid b \in B\}$$

and

$$\ker\pi_2 = \{(a, 1) \in A \times B \mid a \in A\}.$$ □

1.6.17 Exercise 17

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

Proof. Suppose G is abelian. Then for any $a, b \in G$,

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

so $g \mapsto g^{-1}$ is a homomorphism. Conversely, suppose $g \mapsto g^{-1}$ is a homomorphism and let $a, b \in G$ be arbitrary. Then $b^{-1}a^{-1} = (ba)^{-1}$ and we have

$$ab = (a^{-1})^{-1}(b^{-1})^{-1} = (b^{-1}a^{-1})^{-1} = [(ba)^{-1}]^{-1} = ba,$$

so G is abelian. □

1.6.18 Exercise 18

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

Proof. Suppose G is abelian. Then for any $a, b \in G$,

$$(ab)^2 = abab = a^2b^2,$$

and $g \mapsto g^2$ is a homomorphism. Now suppose $g \mapsto g^2$ is a homomorphism. Then for any $a, b \in G$,

$$a^2b^2 = (ab)^2 = abab,$$

and multiplying both sides of the equation $a^2b^2 = abab$ on the left by a and on the right by b gives $ab = ba$, so that G is abelian. □

1.6.20 Exercise 20

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

Proof. Let $\varphi, \psi \in \mathrm{Aut}(G)$. Then $\varphi \circ \psi$ is a bijection from G to itself. It is also a homomorphism, since for any $a, b \in G$,

$$(\varphi \circ \psi)(ab) = \varphi(\psi(a)\psi(b)) = (\varphi \circ \psi)(a)(\varphi \circ \psi)(b).$$

This shows that $\varphi \circ \psi \in \mathrm{Aut}(G)$ so $\mathrm{Aut}(G)$ is closed under composition. And function composition is always associative.

Clearly the identity map $1\colon G \to G$ is an isomorphism, so $\mathrm{Aut}(G)$ has an identity. And for any $\varphi \in \mathrm{Aut}(G)$, φ^{-1} must exist since φ is a bijection. Now, for any $a, b \in G$ let $a^* = \varphi^{-1}(a)$ and $b^* = \varphi^{-1}(b)$. Since φ is a homomorphism, we have

$$\varphi(a^*b^*) = \varphi(a^*)\varphi(b^*) = ab,$$

which implies that $a^*b^* = \varphi^{-1}(ab)$. Then

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

and we see that φ^{-1} is an isomorphism and hence $\varphi^{-1} \in \mathrm{Aut}(G)$. So elements in $\mathrm{Aut}(G)$ have inverses. Therefore $\mathrm{Aut}(G)$ is a group under function composition. □

1.6.21 Exercise 21

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

Proof. Fix a nonzero $k \in \mathbb{Q}$ and let $\varphi\colon \mathbb{Q} \to \mathbb{Q}$ be given by $\varphi(r) = kr$. Then for any $a, b \in \mathbb{Q}$,

$$\varphi(a+b) = k(a+b) = ka + kb = \varphi(a) + \varphi(b),$$

so φ is a homomorphism. To show that it is a bijection, note that it must be surjective since for any $a \in \mathbb{Q}$, we may take $b = a/k$ so that $\varphi(b) = a$. And φ must be injective since for any $a, b \in \mathbb{Q}$, $\varphi(a) = \varphi(b)$ implies $ka = kb$ which implies $a = b$ since k is nonzero. Therefore φ is a bijection and hence an automorphism of $\mathbb{Q}$. □

1.6.22 Exercise 22

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

Proof. Fix $k \in \mathbb{Z}$ and let $\varphi\colon A \to A$ be the mapping $a \mapsto a^k$. Then for any $a, b \in A$, we have

$$\varphi(ab) = (ab)^k = a^k b^k = \varphi(a)\varphi(b),$$

where the second equality follows from the fact that A is abelian. So φ is a homomorphism.

In the case where $k = -1$, φ must be a bijection since it is its own inverse function. Hence $a \mapsto a^{-1}$ is an automorphism of A. □

1.6.23 Exercise 23

Let G be a finite group which possesses an automorphism σ such that $\sigma(g) = g$ if and only if $g = 1$. If σ^2 is the identity map from $G \to G$, prove that G is abelian (such an automorphism σ is called *fixed point free* of order 2).

Proof. Consider the map $\varphi\colon G \to G$ given by $\varphi(x) = x^{-1}\sigma(x)$. For any $x, y \in G$, if $\varphi(x) = \varphi(y)$ then

$$x^{-1}\sigma(x) = y^{-1}\sigma(y)$$

or, rearranging,

$$\sigma(y) = yx^{-1}\sigma(x).$$

This gives

$$y = \sigma(\sigma(y)) = \sigma(yx^{-1}\sigma(x)) = \sigma(yx^{-1})x$$

and multiplying on the right by x^{-1} gives

$$yx^{-1} = \sigma(yx^{-1}). \tag{1.3}$$

Since σ is fixed point free, (1.3) then implies that $yx^{-1} = 1$ or $x = y$. Therefore φ is an injection, and hence a bijection since it maps the finite set G to itself. Therefore every $x \in G$ can be written in the form $x = y^{-1}\sigma(y)$ for some $y \in G$.

Now let $x \in G$ be arbitrary. Then, for some $y \in G$,

$$\sigma(x) = \sigma(y^{-1}\sigma(y)) = \sigma(y)^{-1}y.$$

However, since $(ab)^{-1} = b^{-1}a^{-1}$ for a, b in any group, we also have

$$\sigma(y)^{-1}y = \sigma(y)^{-1}(y^{-1})^{-1} = \big(y^{-1}\sigma(y)\big)^{-1} = x^{-1}.$$

Hence $\sigma(x) = x^{-1}$ for all $x \in G$.

Finally, let $a, b \in G$ be arbitrary. Then

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

But σ is an injection, so $ab = ba$. This shows that G is abelian. □

1.6.24 Exercise 24

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

Proof. Let $t = xy$. By Exercise 1.2.6, we have $tx = xt^{-1}$. Note also that x and t generate G, since y can be written as $y = xt$. So by repeated application of the relation $tx = xt^{-1}$, we may express any member of G uniquely in the form $x^i t^j$ for some integers i, j with $0 \leq i \leq 1$ and $0 \leq j < n$ (the representation is unique since t has order n, which implies that $t, t^2, \ldots, t^{n-1}$ are all distinct). Therefore $|G| = 2n$.

Now let $\varphi\colon D_{2n} \to G$ be given by

$$\varphi(s^i r^j) = x^i t^j, \quad \text{for } i, j \in \mathbb{Z} \text{ with } 0 \leq i \leq 1 \text{ and } 0 \leq j \leq n-1.$$

Since every element in D_{2n} can be written uniquely as $s^i r^j$ with the above restrictions on i and j, the function φ is well defined. And since x and t satisfy the same relations in G that s and r satisfy in D_{2n}, φ must be a homomorphism.

We will now show that φ is a bijection. For any $b \in G$, write $b = x^i t^j$ for $i \in \{0, 1\}$ and $j \in \{0, 1, \ldots, n-1\}$. Then if $a = s^i r^j$, we have $\varphi(a) = b$, which shows that φ is surjective. Since $|G| = |D_{2n}|$, this is enough to show that φ is a bijection.

The function φ is a bijective homomorphism, hence it is an isomorphism and $D_{2n} \cong G$. □

1.6.25 Exercise 25

Let $n \in \mathbb{Z}^+$, let r and s be the usual generators of D_{2n} and let $\theta = 2\pi/n$.

(a) Prove that the matrix $\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$ is the matrix of the linear transformation which rotates the x, y plane about the origin in a counterclockwise direction by θ radians.

Proof. For a vector (x, y) in $\mathbb{R}^2$ we have

$$\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x\cos\theta - y\sin\theta \\ x\sin\theta + y\cos\theta \end{pmatrix}.$$

The distance d of this point from the origin is

$$\begin{aligned} d &= \sqrt{(x\cos\theta - y\sin\theta)^2 + (x\sin\theta + y\cos\theta)^2} \\ &= \sqrt{x^2\cos^2\theta + y^2\sin^2\theta + x^2\sin^2\theta + y^2\cos^2\theta} \\ &= \sqrt{x^2+y^2}, \end{aligned}$$

which is the same distance as (x, y) is from the origin. Moreover, the angle α between these two vectors is given by

$$\begin{aligned} \cos\alpha &= \frac{x(x\cos\theta - y\sin\theta) + y(x\sin\theta + y\cos\theta)}{x^2+y^2} \\ &= \frac{x^2\cos\theta - xy\sin\theta + xy\sin\theta + y^2\cos\theta}{x^2+y^2} \\ &= \cos\theta = \cos\frac{2\pi}{n}. \end{aligned}$$

So we see that $\alpha = 2\pi/n$. This shows that the image of the point (x, y) under this transformation is the same point rotated about the origin by an angle of θ. □

(b) Prove that the map $\varphi\colon D_{2n} \to GL_2(\mathbb{R})$ defined on generators by

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

extends to a homomorphism of D_{2n} into $GL_2(\mathbb{R})$.

Proof. Since $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ is easily seen to be a reflection across the line $y = x$, it is evident that $\varphi(r)$ and $\varphi(s)$ satisfy the same relations as do r and s. Namely, if I is the 2×2 identity matrix, we have

$$\varphi(r)^n = \varphi(s)^2 = I \quad \text{and} \quad \varphi(r)\varphi(s) = \varphi(s)\varphi(r)^{-1}.$$

The latter relation comes from the fact that reflecting across the line $y = x$ and then rotating by θ is the same as first rotating by $2\pi - \theta$ and then reflecting across the line.

Since $\varphi(r)$ and $\varphi(s)$ satisfy the same relations as the corresponding generators of D_{2n}, we see that φ extends to a homomorphism. □

(c) Prove that the homomorphism φ in part (b) is injective.

Proof. Let H denote the subgroup of $GL_2(\mathbb{R})$ generated by $\varphi(r)$ and $\varphi(s)$. Then the function $\psi\colon D_{2n} \to H$ defined by restricting the codomain of φ is surjective. But it is not difficult to see that $|H| = 2n = |D_{2n}|$, so the map ψ and hence φ must also be injective. □

1.6.26 Exercise 26

Let i and j be the generators of Q_8 described in Section 5. Prove that the map φ from Q_8 to $GL_2(\mathbb{C})$ defined on generators by

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

extends to a homomorphism. Prove that φ is injective.

Proof. First, we have

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

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

so we may take $\varphi(-1) = -I$. And $-I$ commutes with all members of $GL_2(\mathbb{C})$.

Also,

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

So we may let

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

Note that $\varphi(k)^2 = -I$ as expected.

To summarize, we have

$$\varphi(i)^2 = \varphi(j)^2 = \varphi(k)^2 = \varphi(i)\varphi(j)\varphi(k) = \varphi(-1),$$

so $\varphi(i)$, $\varphi(j)$, $\varphi(k)$, and $\varphi(-1)$ satisfy all the same relations as given in our presentation for Q_8 in Exercise 1.5.3. Therefore φ extends to a homomorphism.

Lastly, consider the subgroup of $GL_2(\mathbb{C})$ generated by $\varphi(i)$, $\varphi(j)$, $\varphi(k)$, and $\varphi(-1)$. It is not difficult to see that this subgroup contains exactly eight elements (those named plus their inverses and the identity). So the function obtained from φ by restricting its codomain to this subgroup must be surjective. Since its domain and codomain share the same cardinality, it must also be injective. Hence φ is injective. □

1.7 Group Actions

1.7.1 Exercise 1

Let F be a field. Show that the multiplicative group of nonzero elements of F (denoted by $F^\times$) acts on the set F by $g \cdot a = ga$, where $g \in F^\times$, $a \in F$ and ga is the usual product in F of the two field elements.

Proof. Let $g_1, g_2 \in F^\times$. Then for any $a \in F$,

$$g_1 \cdot (g_2 \cdot a) = g_1 \cdot g_2 a = g_1(g_2 a) = (g_1 g_2)a = (g_1 g_2) \cdot a,$$

where the second-to-last equality follows from the associativity of multiplication in F. Also, for any $a \in F^\times$,

$$1 \cdot a = 1a = a,$$

since 1 is the identity of the group $F^\times$. And $1(0) = 0$ (which follows from distributivity), so we can say that $1 \cdot a = a$ for all $a \in F$. Therefore the mapping $(g, a) \mapsto ga$ of $F^\times \times F \to F$ is a group action. □

1.7.2 Exercise 2

Show that the additive group $\mathbb{Z}$ acts on itself by $z \cdot a = z + a$ for all $z, a \in \mathbb{Z}$.

Proof. For all $z_1, z_2, a \in \mathbb{Z}$, we have

$$z_1 \cdot (z_2 \cdot a) = z_1 + (z_2 + a) = (z_1 + z_2) + a = (z_1 + z_2) \cdot a$$

and

$$0 \cdot a = 0 + a = a.$$

Therefore $\mathbb{Z}$ acts on itself as stated. □

1.7.3 Exercise 3

Show that the additive group $\mathbb{R}$ acts on the x, y plane $\mathbb{R} \times \mathbb{R}$ by $r \cdot (x, y) = (x + ry, y)$.

Proof. For any $r_1, r_2 \in \mathbb{R}$ and any $(x, y) \in \mathbb{R}^2$, we have

$$\begin{aligned} r_1 \cdot (r_2 \cdot (x, y)) &= r_1 \cdot (x + r_2 y, y) \\ &= (x + r_2 y + r_1 y, y) \\ &= (x + (r_1 + r_2)y, y) \\ &= (r_1 + r_2) \cdot (x, y) \end{aligned}$$

and

$$0 \cdot (x, y) = (x + 0y, y) = (x, y).$$

Therefore $\mathbb{R}$ acts on $\mathbb{R}^2$ in the manner stated above. □

1.7.4 Exercise 4

Let G be a group acting on a set A and fix some $a \in A$. Show that the following sets are subgroups of G:

(a) the kernel of the action

Proof. Suppose g, h are in the kernel of the action. Then for any $b \in A$,

$$(gh) \cdot b = g \cdot (h \cdot b) = g \cdot b = b,$$

so gh is in the kernel, and the kernel is closed under the group operation. Moreover, if g is in the kernel then

$$b = 1 \cdot b = (g^{-1}g) \cdot b = g^{-1} \cdot (g \cdot b) = g^{-1} \cdot b,$$

so g^{-1} is in the kernel.

Therefore the kernel of the group action is a nonempty subset of G which is closed under the binary operation of G and which is closed under inverses, so the kernel is a subgroup of G. □

(b) $\{g \in G \mid ga = a\}$ (called the *stabilizer* of a in G)

Proof. The stabilizer of a is nonempty since 1 is a member. Now let g, h be any members of the stabilizer. Then

$$(gh) \cdot a = g \cdot (h \cdot a) = g \cdot a = a,$$

so the stabilizer is closed under the group operation. It is also closed under inverses, since

$$a = 1 \cdot a = (g^{-1}g) \cdot a = g^{-1} \cdot (g \cdot a) = g^{-1} \cdot a.$$

Therefore the stabilizer is a subgroup of G. □

1.7.5 Exercise 5

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

Proof. Let $\varphi\colon G \to S_A$ be the permutation representation of the group action on A, so that for $g \in G$ and $a \in A$, $\varphi(g)(a) = g \cdot a$.

If $g \in \ker \varphi$, then $\varphi(g) = 1$, where 1 is the identity permutation on A. Then $g.a = a$ for all $a \in A$, and g is in the kernel of the action. Conversely, if g is in the kernel of the action, then $g.a = a$ for all $a \in A$, so that $\varphi(g) = 1$ and $g \in \ker \varphi$. Therefore the kernel of the group action and the kernel of the corresponding permutation representation are the same. □

1.7.6 Exercise 6

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

Proof. First, suppose that G acts faithfully on A and let g be an element in the kernel of the action. Then $g \cdot a = a$ for all $a \in A$. However, $1 \cdot a = a$ for all $a \in A$, so the elements 1 and g induce the same permutation on A. Since G acts faithfully, this must mean that $g = 1$, so that the kernel of the action is the set $\{1\}$.

For the converse, suppose that the kernel of the action is the set $\{1\}$. Pick two elements g and h in G and suppose that g and h induce the same permutation on A. Then for any $a \in A$, $g \cdot a = h \cdot a$. But then

$$a = (g^{-1}g) \cdot a = g^{-1} \cdot (g \cdot a) = g^{-1} \cdot (h \cdot a) = (g^{-1}h) \cdot a.$$

Therefore $g^{-1}h$ is in the kernel of the action, so $g^{-1}h = 1$. This implies that $g = h$, so that distinct elements in G must induce distinct permutations on A. This shows that G acts faithfully on A. □

1.7.7 Exercise 7

Prove that in Example 2 in this section the action is faithful.

Proof. If V is a vector space over a field F, then the multiplicative group $F^\times$ acts on the set V via the mapping $a \cdot v = av$ for $a \in F^\times$ and $v \in V$. We want to show that this action is faithful.

Let $a, b \in F^\times$ be such that $a \cdot v = b \cdot v$ for all $v \in V$. Then

$$\begin{aligned} 0 &= a \cdot v + -(a \cdot v) \\ &= a \cdot v + -(b \cdot v) \\ &= av - bv \\ &= (a - b)v. \end{aligned}$$

Since $(a - b)v$ is 0 even when v is nonzero, this implies that $a - b = 0$ or $a = b$. Therefore distinct elements in $F^\times$ must induce distinct permutations on V and the action is faithful. □

1.7.8 Exercise 8

Let A be a nonempty set and let k be a positive integer with $k \leq |A|$. The symmetric group S_A acts on the set B consisting of all subsets of A of cardinality k by $\sigma \cdot \{a_1, \ldots, a_k\} = \{\sigma(a_1), \ldots, \sigma(a_k)\}$.

(a) Prove that this is a group action.

Proof. Suppose $\sigma_1, \sigma_2 \in S_A$. Then for any subset $\{a_1, \ldots, a_k\}$ of A,

$$\begin{aligned} \sigma_1 \cdot (\sigma_2 \cdot \{a_1, \ldots, a_k\}) &= \sigma_1 \cdot \{\sigma_2(a_1), \ldots, \sigma_2(a_k)\} \\ &= \{\sigma_1(\sigma_2(a_1)), \ldots, \sigma_1(\sigma_2(a_k))\} \\ &= (\sigma_1 \circ \sigma_2) \cdot \{a_1, \ldots, a_k\} \end{aligned}$$

and

$$1 \cdot \{a_1, \ldots, a_k\} = \{1(a_1), \ldots, 1(a_k)\} = \{a_1, \ldots, a_k\}.$$

Therefore the specified mapping is a group action. □

(b) Describe explicitly how the elements $(1\,2)$ and $(1\,2\,3)$ act on the six 2-element subsets of $\{1, 2, 3, 4\}$.

Solution. We have

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

and

$$\begin{aligned}
(1\,2\,3) \cdot \{1, 2\} &= \{2, 3\}, \\
(1\,2\,3) \cdot \{1, 3\} &= \{2, 1\}, \\
(1\,2\,3) \cdot \{1, 4\} &= \{2, 4\}, \\
(1\,2\,3) \cdot \{2, 3\} &= \{3, 1\}, \\
(1\,2\,3) \cdot \{2, 4\} &= \{3, 4\}, \\
(1\,2\,3) \cdot \{3, 4\} &= \{1, 4\}.
\end{aligned}$$

□

1.7.9 Exercise 9

Do both parts of the preceding exercise with "ordered k-tuples" in place of "k-element subsets," where the action on k-tuples is defined as above but with set braces replaced by parentheses.

Solution. The work is essentially the same, but with k-tuples replacing the k-element subsets, so we omit it. Note that in part (b) there are twice as many different 2-tuples as there are 2-element subsets, since the ordering of the elements is significant. □

1.7.10 Exercise 10

With reference to the preceding two exercises determine:

(a) for which values of k the action of S_n on k-element subsets is faithful

Solution. The action of S_A on k-element subsets of a set A is faithful for all integers k with $1 \leq k < |A|$, which we will now show. Suppose σ_1 and σ_2 are distinct permutations in S_A. Label the elements of A as $\{a_1, a_2, \ldots, a_n\}$, where $n = |A|$. Without loss of generality, we may suppose that $\sigma_1(a_1) \neq \sigma_2(a_1)$ (if not, relabel the elements of A so that this is true).

Now, take any k-element subset B of A which contains a_1 but which does not contain $(\sigma_1^{-1} \circ \sigma_2)(a_1)$ (this is possible since $1 \leq k < |A|$). Then $\sigma_1 \cdot B$ does not contain $\sigma_2(a_1)$, however $\sigma_2 \cdot B$ does. Therefore distinct permutations in S_A induce distinct permutations on the k-element subsets of A, so the action is faithful (again, assuming $1 \leq k < |A|$). □

(b) for which values of k the action of S_n on ordered k-tuples is faithful

Solution. The action of S_A on ordered k-tuples of elements of A is faithful for all integers k with $1 \leq k \leq |A|$. To see this, suppose that σ_1, σ_2 are distinct permutations in S_A. Suppose for example that $\sigma_1(a_1) \neq \sigma_2(a_1)$ and consider the k-tuple $B = (a_1, a_2, \ldots, a_k)$. Then the first coordinate in $\sigma_1 \cdot B$ is distinct from the first coordinate of $\sigma_2 \cdot B$. Therefore distinct permutations in S_A induce distinct permutations on the set of k-tuples, so the action is faithful. □

1.7.11 Exercise 11

Write out the cycle decomposition of the eight permutations in S_4 corresponding to the elements in D_8 given by the action of D_8 on the vertices of a square (where the vertices of the square are labelled as in Section 2).

Solution. Let $\varphi\colon D_8 \to S_4$ be the permutation representation associated to the action of D_8 on the vertices $\{1, 2, 3, 4\}$ of a square. Then

$$\begin{aligned}
\varphi(1) &= 1, \\
\varphi(r) &= (1\,2\,3\,4), \\
\varphi(r^2) &= (1\,3)(2\,4), \\
\varphi(r^3) &= (1\,4\,3\,2), \\
\varphi(s) &= (2\,4), \\
\varphi(sr) &= (1\,4)(2\,3), \\
\varphi(sr^2) &= (1\,3),
\end{aligned}$$

and

$$\varphi(sr^3) = (1\,2)(3\,4). \qquad \square$$

1.7.12 Exercise 12

Assume n is an even positive integer and show that D_{2n} acts on the set consisting of pairs of opposite vertices of a regular n-gon. Find the kernel of this action (label vertices as usual).

Solution. Fix an even positive integer n. The set of pairs of opposite vertices of a regular n-gon, labeled in the usual way, is the set $P = \{P_1, P_2, \ldots, P_{n/2}\}$ where

$$P_k = \left\{k, \frac{n}{2} + k\right\}.$$

D_{2n} acts on P by $x \cdot P_k = P_\ell$ where P_ℓ is the set of images of the vertices in P_k under the symmetry x. For example, in D_8, $sr \cdot \{2,6\} = \{7,3\}$ because sr maps vertex 2 to vertex 7 and vertex 6 to vertex 3.

Let $x, y \in D_{2n}$. It is clear by definition of the action that $x \cdot (y \cdot P_k) = (xy) \cdot P_k$ and that $1 \cdot P_k = P_k$. So this is a group action. The only symmetry in D_{2n} which fixes all vertices is the identity 1. However, since the order of vertices in each pair does not matter, any symmetry which only sends vertices to their opposites will also fix pairs of vertices. The only symmetry which does this is $r^{n/2}$. There is no symmetry which fixes only some vertices and which sends all others to their opposite vertices, so the kernel of the action is just the set $\{1, r^{n/2}\}$. □

1.7.13 Exercise 13

Find the kernel of the left regular action.

Solution. Let G be a group. The kernel of the left regular action is the set

$$\{g \in G \mid gh = h \text{ for all } h \in G\}.$$

By uniqueness of the identity, it is clear that this set is simply $\{1\}$. Therefore the left regular action is always faithful. □

1.7.14 Exercise 14

Let G be a group and let $A = G$. Show that if G is non-abelian then the maps defined by $g \cdot a = ag$ for all $g, a \in G$ do *not* satisfy the axioms of a (left) group action of G on itself.

Proof. Since G is non-abelian, there exist $g_1, g_2 \in G$ such that $g_1 g_2 \neq g_2 g_1$. Then $g_1 \cdot (g_2 \cdot a) = a g_2 g_1$ but $(g_1 g_2) \cdot a = a g_1 g_2$. If $a g_2 g_1 = a g_1 g_2$ then the cancellation law gives $g_2 g_1 = g_1 g_2$, a contradiction. Therefore this map does not define a left group action. □

1.7.15 Exercise 15

Let G be any group and let $A = G$. Show that the maps defined by $g \cdot a = ag^{-1}$ for all $g, a \in G$ *do* satisfy the axioms of a (left) group action of G on itself.

Proof. Let $g_1, g_2, a \in G$ be arbitrary. Then

$$g_1 \cdot (g_2 \cdot a) = g_1 \cdot (a g_2^{-1}) = a g_2^{-1} g_1^{-1} = a(g_1 g_2)^{-1} = (g_1 g_2) \cdot a$$

and

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

Therefore this map does define a group action. □

1.7.16 Exercise 16

Let G be any group and let $A = G$. Show that the maps defined by $g \cdot a = gag^{-1}$ for all $g, a \in G$ *do* satisfy the axioms of a (left) group action (this action of G on itself is called *conjugation*).

Proof. For any $g_1, g_2, a \in G$ we have

$$g_1 \cdot (g_2 \cdot a) = g_1 \cdot (g_2 a g_2^{-1}) = g_1 g_2 a g_2^{-1} g_1^{-1} = (g_1 g_2) a (g_1 g_2)^{-1} = (g_1 g_2) \cdot a$$

and

$$1 \cdot a = 1a1 = a,$$

so this mapping does define a group action. □

1.7.17 Exercise 17

Let G be a group and let G act on itself by left conjugation, so each $g \in G$ maps G to G by

$$x \mapsto gxg^{-1}.$$

For fixed $g \in G$, prove that conjugation by g is an isomorphism from G onto itself (i.e., is an automorphism of G). Deduce that x and gxg^{-1} have the same order for all x in G and that for any subset A of G, $|A| = |gAg^{-1}|$ (here $gAg^{-1} = \{gag^{-1} \mid a \in A\}$).

Proof. Fix a $g \in G$ and let $\varphi \colon G \to G$ denote the map $x \mapsto gxg^{-1}$. Then for any $x_1, x_2 \in G$ we have

$$\varphi(x_1 x_2) = g x_1 x_2 g^{-1} = (g x_1 g^{-1})(g x_2 g^{-1}) = \varphi(x_1)\varphi(x_2)$$

so φ is a homomorphism.

Next, suppose $\varphi(x_1) = \varphi(x_2)$. Then $gx_1g^{-1} = gx_2g^{-1}$ and multiplying both sides of this equation on the left by g^{-1} and on the right by g gives $x_1 = x_2$, so that φ is injective.

Now let $y \in G$ be arbitrary. Then $x = g^{-1}yg$ is such that $\varphi(x) = y$, so φ is surjective. Therefore φ is an automorphism.

Since isomorphisms preserve order, we see that each element x in G has the same order as its conjugate gxg^{-1}. Moreover, if $A \subseteq G$ then the restriction of φ to A, $\varphi|_A \colon A \to gAg^{-1}$, is still a bijection, so $|A| = |gAg^{-1}|$. □

1.7.18 Exercise 18

Let H be a group acting on a set A. Prove that the relation $\sim$ on A defined by

$$a \sim b \quad \text{if and only if} \quad a = hb \ \text{ for some } h \in H$$

is an equivalence relation. (For each $x \in A$ the equivalence classes of x under $\sim$ is called the *orbit* of x under the action of H. The orbits under the action of H partition the set A.)

Proof. Since $a = 1a$ we have $a \sim a$. And if $a = hb$ for $h \in H$ then

$$h^{-1}a = h^{-1}(hb) = (h^{-1}h)b = b,$$

so $a \sim b$ implies $b \sim a$.

Lastly, suppose $a \sim b$ and $b \sim c$ and let $h_1, h_2 \in H$ be such that $a = h_1 b$ and $b = h_2 c$. Then $a = h_1(h_2 c) = (h_1 h_2)c$ and $a \sim c$. Hence $\sim$ is an equivalence relation. □

1.7.19 Exercise 19

Let H be a subgroup of the finite group G and let H act on G (here $A = G$) by left multiplication. Let $x \in G$ and let $\mathcal{O}$ be the orbit of x under the action of H. Prove that the map

$$H \to \mathcal{O} \quad \text{defined by} \quad h \mapsto hx$$

is a bijection (hence all orbits have cardinality $|H|$). From this and the preceding exercises deduce *Lagrange's Theorem*:

if G is a finite group and H is a subgroup of G then $|H|$ divides $|G|$.

Proof. Let $\varphi\colon H \to \mathcal{O}$ denote the map $h \mapsto hx$. Suppose $\varphi(h) = \varphi(k)$ for $h, k \in H$. Then $hx = kx$ and right cancellation implies that $h = k$, so that φ is injective. And φ is surjective by definition ($y \in \mathcal{O}$ means that there is $h \in H$ such that $hx = y$). Therefore φ is a bijection and $|H| = |\mathcal{O}|$.

From the previous exercise, we know that the orbits under the action of H partition G. Each equivalence class $\mathcal{O}$ has cardinality $|H|$, so $|G| = n|H|$ where n is the number of orbits. Hence $|H|$ divides $|G|$. □

1.7.20 Exercise 20

Show that the group of rigid motions of a tetrahedron is isomorphic to a subgroup of S_4.

Proof. Call the group of rigid motions of the tetrahedron G. Number each vertex and let A denote the set $\{1, 2, 3, 4\}$. Then each rigid motion $\alpha \in G$ induces a permutation $\sigma_\alpha \in S_4$ of A. G acts on A via the map $\alpha i = \sigma_\alpha(i)$.

Since each distinct $\alpha \in G$ permutes the vertices in a different way, we get an injective homomorphism

$$\varphi\colon G \to S_4 \quad \text{given by} \quad \varphi(\alpha) = \sigma_\alpha.$$

Then $\varphi(G)$ is a subgroup of S_4, and by simply restricting the codomain of φ we have an isomorphism from G to this subgroup of S_4. □

1.7.21 Exercise 21

Show that the group of rigid motions of a cube is isomorphic to S_4.

Proof. Again let G denote the group of rigid motions and let $A = \{1, 2, 3, 4\}$, where each $i \in A$ corresponds to a pair of opposing vertices on a cube. Each $\alpha \in G$ sends each pair of opposing vertices to a new pair of opposing vertices. Therefore G acts on A.

Consider the homomorphism $\varphi\colon G \to S_4$ given by

$$\varphi(\alpha)(i) = \alpha i.$$

Then φ is injective since each distinct rigid motion $\alpha \in G$ gives rise to a different permutation of A. From Exercise 1.2.10 we know that $|G| = 24 = |S_4|$, so φ is in fact an isomorphism. □

1.7.22 Exercise 22

Show that the group of rigid motions of an octahedron is isomorphic to S_4. Deduce that the groups of rigid motions of a cube and an octahedron are isomorphic.

Proof. Number each pair of opposing faces of the octahedron $1, 2, 3, 4$. Let G be the group of rigid motions of the octahedron and let $A = \{1, 2, 3, 4\}$. Each $\alpha \in G$ sends each pair of opposing faces to a new pair of opposing faces, so G acts on A.

As in the previous exercise, we see that the homomorphism

$$\varphi\colon G \to S_4 \quad \text{given by} \quad \varphi(\alpha)(i) = \alpha i.$$

is injective. By Exercise 1.2.11 we have $|G| = 24 = |S_4|$, so φ is an isomorphism.

From this and the previous exercise, we see that the groups of rigid motions of the cube and the octahedron are isomorphic. □

1.7.23 Exercise 23

Explain why the action of the group of rigid motions of a cube on the set of three pairs of opposite faces is not faithful. Find the kernel of this action.

Solution. The group of rigid motions of a cube has order 24 but the permutations on the set of pairs of opposite faces has order $|S_3| = 6$. Therefore the action cannot be faithful.

Construct a line through the center of each pair of opposite faces. Then a 180° rotation about each of these lines will send each pair of opposite faces to itself. These are the only rotations that fix pairs of opposing faces, so the kernel of the action consists of these three 180° rotations along with the identity transformation. □

Chapter 2

Subgroups

2.1 Definition and Examples

Let G be a group.

2.1.1 Exercise 1

In each of (a)–(e) prove that the specified subset is a subgroup of the given group.

(a) the set of complex numbers of the form $a + ai$, $a \in \mathbb{R}$ (under addition)

Proof. Call the set H. H is obviously nonempty. For any $a+ai$ and $b+bi$ in H, we have

$$(a + ai) - (b + bi) = (a - b) + (a - b)i \in H,$$

so by Proposition 1, $H \leq \mathbb{C}$. □

(b) the set of complex numbers of absolute value 1, i.e., the unit circle in the complex plane (under multiplication)

Proof. Let H denote the complex numbers of absolute value 1, and let $\overline{z}$ denote the conjugate of z. Then H is nonempty and for any $z, w \in H$, we have

$$|zw^{-1}| = |z||w^{-1}| = |z|\frac{|\overline{w}|}{|w|^2} = 1,$$

so $zw^{-1} \in H$. Therefore $H \leq \mathbb{C}^\times$. □

(c) for fixed $n \in \mathbb{Z}^+$ the set of rational numbers whose denominators divide n (under addition)

Proof. Let H denote the subset in question. H is clearly not empty. Let $a/b \in H$ and $c/d \in H$ be in lowest terms, where $n = bx = dy$ for some $x, y \in \mathbb{Z}^+$. Then

$$\frac{a}{b} - \frac{c}{d} = \frac{ax}{n} - \frac{cy}{n} = \frac{ax - cy}{n}.$$

After writing this fraction in lowest terms, its denominator will be some factor of n, so $(a/b - c/d) \in H$ as required. Therefore $H \leq \mathbb{Q}$. □

(d) for fixed $n \in \mathbb{Z}^+$ the set of rational numbers whose denominators are relatively prime to n (under addition)

Proof. Again, let H denote the subset, which is clearly nonempty. Take a/b and c/d in H, so that $(b, n) = (d, n) = 1$. Then

$$\frac{a}{b} - \frac{c}{d} = \frac{ad - bc}{bd}.$$

Let $k = (bd, n)$. If $k > 1$, then there is a prime number m which divides k. Then $m \mid bd$ which implies $m \mid b$ or $m \mid d$, which is impossible since $m \mid n$. Therefore $k = 1$ and $a/b - c/d \in H$. So $H \leq \mathbb{Q}$. □

(e) the set of nonzero real numbers whose square is a rational number (under multiplication)

Proof. Let H be the set in question, which is clearly nonempty. If $a, b \in H$, then $a^2, b^2 \in \mathbb{Q}$. Then

$$\left(\frac{a}{b}\right)^2 = \frac{a^2}{b^2} \in \mathbb{Q},$$

so $a/b \in H$. Hence $H \leq \mathbb{R}^\times$. □

2.1.2 Exercise 2

In each of (a)–(e) prove that the specified subset is *not* a subgroup of the given group:

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

Proof. For any $n \geq 3$, the 2-cycles $(1\,2)$ and $(2\,3)$ are members of S_n, yet $(2\,3)(1\,2) = (1\,3\,2)$ which is not a 2-cycle. So this set is not a subgroup. □

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

Proof. Since s and sr are reflections, but $s(sr) = r$ is not, this set is not closed under the group operation so it is not a subgroup. □

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

Proof. Let $p \mid n$ for p a prime. Then $(x^{n/p})^p = x^n = 1$, so $|x^{n/p}| < n$ and the set is not closed under the group operation. □

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

Proof. Since $1+1 = 2$, this set is not closed under addition and is therefore not a subgroup. □

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

Proof. $\sqrt{2}$ and $\sqrt{3}$ are in this subset, but $\sqrt{2} + \sqrt{3}$ is not, so this cannot be a subgroup. □

2.1.3 Exercise 3

Show that the following subsets of the dihedral group D_8 are actually subgroups:

(a) $\{1, r^2, s, sr^2\}$

Proof. This is a finite group so it suffices to show that it is closed under the group operation of composition. We have

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

Therefore this subset is a subgroup. □

(b) $\{1, r^2, sr, sr^3\}$

Proof. Again, we can simply enumerate the possibilities. We find that

$$\begin{aligned} r^2(r^2) = sr(sr) = sr^3(sr^3) &= 1, \\ r^2(sr) = sr(r^2) &= sr^3, \\ r^2(sr^3) = sr^3(r^2) &= sr, \end{aligned}$$

and

$$sr(sr^3) = sr^3(sr) = r^2.$$

Therefore this is a subgroup. □

2.1.4 Exercise 4

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

Solution. Let $G = \mathbb{R}^\times$ with the operation of multiplication. Then if H is the nonzero integers, H is closed under multiplication but is not a subgroup since it is not closed under inverses (for example, 2 has no inverse in H). □

2.1.5 Exercise 5

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

Proof. If such a subgroup H does exist, then it must exclude exactly one element g from G. Since $|H| \geq 2$, we can take a nonidentity element $h \in H$.

Consider the element gh. If $gh \notin H$, then $gh = g$ and cancellation implies that h is the identity, which is a contradiction. On the other hand, if $gh \in H$, then $(gh)h^{-1} = g \in H$, a contradiction. So the subgroup H does not exist. □

2.1.6 Exercise 6

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

Solution. Let G be abelian and let H be the elements of G having finite order. H is nonempty since $1 \in H$. Suppose $a, b \in H$. Then $|a| = m$ and $|b| = n$ for some finite m and n. Since G is abelian we have

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

Therefore $ab^{-1} \in H$ and H is a subgroup of G.

Now, for a non-abelian counterexample, consider the group of invertible functions from $\mathbb{R} \to \mathbb{R}$ under function composition. Let $f\colon \mathbb{R} \to \mathbb{R}$ and $g\colon \mathbb{R} \to \mathbb{R}$ be given by

$$f(x) = -x \quad \text{and} \quad g(x) = 1 - x.$$

Then f and g have order 2 but $f \circ g$, given by $x \mapsto x - 1$, has infinite order. □

2.1.7 Exercise 7

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

Solution. Let $G = \mathbb{Z} \times (\mathbb{Z}/n\mathbb{Z})$ (with componentwise addition) and let H be the torsion subgroup. Since every nonzero integer has infinite order, members of H must have the form $(0, k)$ for $k \in \mathbb{Z}/n\mathbb{Z}$. But $\mathbb{Z}/n\mathbb{Z}$ is a finite group, so all of its members have finite order. Therefore $H = \{(0, k) \mid k \in \mathbb{Z}/n\mathbb{Z}\}$. And we know that this is a subgroup by the previous exercise.

Now let K be the set of elements of G having infinite order together with the identity. Then $(1, 1) \in K$ and $(-1, 0) \in K$, but $(1, 1) + (-1, 0) = (0, 1) \notin K$. Therefore K is not a subgroup of G. □

2.1.8 Exercise 8

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

Proof. Suppose $H \cup K$ is a subgroup of G. If $H \subseteq K$ then we are done. Suppose $H \not\subseteq K$ so that there is $h \in H$ such that $h \notin K$. Let k be any element in K. Since $h, k \in H \cup K$, we must have $hk \in H \cup K$. But if $hk \in K$, then $hk(k^{-1}) = h \in K$, which contradicts the choice of h. So $hk \in H$. And $h^{-1} \in H$, so $h^{-1}(hk) = k \in H$. Hence every element of K is in H so that $K \subseteq H$.

Conversely, suppose $H \subseteq K$. Then $H \cup K = K$ is a subgroup. Similarly, if $K \subseteq H$, then $H \cup K = H$ is a subgroup. This completes the proof. □

2.1.9 Exercise 9

Let $G = GL_n(F)$, where F is any field. Define

$$SL_n(F) = \{A \in GL_n(F) \mid \det(A) = 1\}$$

(called the *special linear group*). Prove that $SL_n(F) \leq GL_n(F)$.

Proof. First, note that $SL_n(F)$ is nonempty since the identity matrix I has determinant 1. Now let $A, B \in SL_n(F)$. We know from linear algebra that

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

so $AB^{-1} \in SL_n(F)$, which shows that $SL_n(F)$ is a subgroup. □

2.1.10 Exercise 10

(a) Prove that if H and K are subgroups of G then so is their intersection $H \cap K$.

Proof. Since $1 \in H$ and $1 \in K$, $1 \in H \cap K$ and the intersection is nonempty. For any $a, b \in H \cap K$, we must have $ab^{-1} \in H$ since $a, b \in H$ and H is a subgroup. Similarly we must have $ab^{-1} \in K$, so $ab^{-1} \in H \cap K$ and $H \cap K \leq G$. □

(b) Prove that the intersection of an arbitrary nonempty collection of subgroups of G is again a subgroup of G (do not assume the collection is countable).

Proof. Let H_α be a subgroup of G for all α belonging to some set of indices A. Let

$$H = \bigcap_{\alpha \in A} H_\alpha.$$

Then $1 \in H$ so H is nonempty. If $a, b \in H$, then for any α we have $a, b \in H_\alpha$, so $ab^{-1} \in H_\alpha$ and we see that $ab^{-1} \in H$ as well. Hence $H \leq G$. □

2.1.11 Exercise 11

Let A and B be groups. Prove that the following sets are subgroups of the direct product $A \times B$:

(a) $\{(a, 1) \mid a \in A\}$

Proof. Call the set H. Then $(1, 1) \in H$ so H is nonempty. For any $a_1, a_2 \in A$ we have $a_1 a_2^{-1} \in A$, so $(a_1, 1)(a_2, 1)^{-1} = (a_1 a_2^{-1}, 1) \in H$. Therefore $H \leq A \times B$. □

(b) $\{(1, b) \mid b \in B\}$

Proof. The proof is almost the same as in part (a): H is nonempty, and for any $b_1, b_2 \in B$ we have $(1, b_1)(1, b_2)^{-1} = (1, b_1 b_2^{-1}) \in H$, so $H \leq A \times B$. □

(c) $\{(a, a) \mid a \in A\}$, where here we assume $B = A$ (called the *diagonal subgroup*)

Proof. Again, call the subset H. $(1, 1) \in H$ so H is nonempty. For any $a_1, a_2 \in A$, we have $a_1 a_2^{-1} \in A$ so $(a_1, a_1)(a_2, a_2)^{-1} = (a_1 a_2^{-1}, a_1 a_2^{-1}) \in H$. Therefore H is a subgroup of A^2. □

2.1.12 Exercise 12

Let A be an abelian group and fix some $n \in \mathbb{Z}$. Prove that the following sets are subgroups of A:

(a) $\{a^n \mid a \in A\}$

Proof. Call the subset H. Then $1^n = 1 \in H$ so H is nonempty. If $a^n, b^n \in H$ then, since A is abelian,

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

Therefore $a^n (b^n)^{-1} \in H$ and $H \leq A$. □

(b) $\{a \in A \mid a^n = 1\}$

Proof. Again, call the set H. Then $1 \in H$ so H is nonempty. Suppose $a, b \in H$. Then $a^n = 1$ and $(b^{-1})^n = (b^n)^{-1} = 1^{-1} = 1$. Since A is abelian, we have $(ab^{-1})^n = a^n (b^{-1})^n = 1$ so $ab^{-1} \in H$. Therefore $H \leq A$. □

2.1.13 Exercise 13

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

Proof. Suppose H is a subgroup of $\mathbb{Q}$ with the given property. Certainly $0 \in H$. If $H = 0$ then there is nothing left to prove, so suppose $H \neq 0$. Then $x \in H$ for some nonzero $x \in \mathbb{Q}$. And we may take x to be positive, since if $x < 0$ then $-x > 0$ and $-x \in H$ since H is closed under additive inverses.

Write $x = a/b$ for positive integers a and b. Since H is closed under addition, we have

$$bx = \overbrace{\frac{a}{b} + \frac{a}{b} + \cdots + \frac{a}{b}}^{b \text{ terms}} = a \in H.$$

Also, a is nonzero, so by hypothesis $1/a \in H$. By the same reasoning as above, we have $a(1/a) = 1 \in H$. And since H is closed under addition and inverses, this shows that $\mathbb{Z} \subseteq H$.

Now, let $r \in \mathbb{Q}$ be arbitrary and write $r = p/q$ for integers p and q (with q nonzero). Since $q \in H$, we have $1/q \in H$ and so $p(1/q) = p/q \in H$. This shows that $\mathbb{Q} \subseteq H$. But $H \subseteq \mathbb{Q}$, so $H = \mathbb{Q}$ and the proof is complete. □

2.1.14 Exercise 14

Show that $\{x \in D_{2n} \mid x^2 = 1\}$ is not a subgroup of D_{2n} (here $n \geq 3$).

Proof. In D_{2n}, $s^2 = 1$ and $(sr)^2 = srsr = s^2r^{-1}r = 1$, so these elements are in the subset. However, their product $s(sr) = r$ has order $n > 2$. So this set is not closed under the group operation and thus is not a subgroup. □

2.1.15 Exercise 15

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

Proof. Let $H = \bigcup_{i=1}^{\infty} H_i$. Obviously $1 \in H$, so H is nonempty. Let $a, b \in H$. Then $a \in H_i$ for some i and $b \in H_j$ for some j. If $k = \max(i, j)$, then a and b both belong to H_k, so ab^{-1} belongs also to H_k. Therefore $ab^{-1} \in H$ as required. Hence $H \leq G$. □

2.1.16 Exercise 16

Let $n \in \mathbb{Z}^+$ and let F be a field. Prove that the set

$$\{(a_{ij}) \in GL_n(F) \mid a_{ij} = 0 \text{ for all } i > j\}$$

is a subgroup of $GL_n(F)$ (called the group of *upper triangular* matrices).

Proof. Fix an $n \in \mathbb{Z}^+$ and call the set of $n \times n$ upper triangular matrices H. H is nonempty, since the identity matrix is in H.

Let $A, B \in H$, where the ijth entry of A is a_{ij} and the corresponding entry of B is b_{ij}. If $AB = C$ with $C = (c_{ij})$ then

$$c_{ij} = \sum_{k=0}^{n} a_{ik} b_{kj},$$

and if $i > j$ then this sum must be 0 since $a_{ik} = 0$ for $k < i$ and $b_{kj} = 0$ for $k \geq i > j$. Therefore H is closed under multiplication.

Lastly, we need to show that H is closed under inverses. Consider the matrix A. Since $A \in GL_n(F)$ we know that A is invertible. And since the determinant of an upper triangular matrix is the product of the diagonal entries, we must have $a_{ii} \neq 0$ for each i.

Let $D = A^{-1}$, so that $DA = I$ for $D = (d_{ij})$. Suppose that D is not upper triangular, and let d_{ij} be nonzero for some $i > j$. Suppose also that d_{ij} is the first nonzero entry in row i. Then

$$\sum_{k=1}^{n} d_{ik} a_{kj} = 0$$

since $DA = I$. But $d_{ik} = 0$ for each $k < j$ since d_{ij} is the first nonzero entry in the row. And $a_{kj} = 0$ for each $k > j$ since A is upper triangular. Therefore the only term which survives is $d_{ij}a_{jj}$, which is nonzero. But then the sum is nonzero, which gives a contradiction. Therefore D is upper triangular and H is closed under inverses. This shows that $H \leq GL_n(F)$. □

2.1.17 Exercise 17

Let $n \in \mathbb{Z}^+$ and let F be a field. Prove that the set

$$\{(a_{ij}) \in GL_n(F) \mid a_{ij} = 0 \text{ for all } i > j, \text{ and } a_{ii} = 1 \text{ for all } i\}$$

is a subgroup of $GL_n(F)$.

Proof. Again, call the set H. We know H is nonempty since $I \in H$.

Let $A, B \in H$. By the previous exercise we know that the product AB must be upper triangular. So we need only check that the diagonal entries are each 1. For each i, we have

$$\sum_{k=1}^{n} a_{ik}b_{ki} = a_{ii}b_{ii} = 1,$$

since all nondiagonal terms are 0 (because $a_{ik} = 0$ for $k < i$ and $b_{ki} = 0$ for $k > i$). Therefore H is closed under products.

Now let $D = (d_{ij})$ be such that $DA = I$. Again, by the previous exercise we know that D must be an upper triangular matrix, so we need only ensure that the diagonal entries are each 1. For each i, we have

$$1 = \sum_{k=1}^{n} d_{ik}a_{ki} = d_{ii}a_{ii} = d_{ii},$$

since nondiagonal terms are 0. Therefore H is closed under inverses, and $H \leq GL_n(F)$. □

2.2 Centralizers and Normalizers, Stabilizers and Kernels

2.2.1 Exercise 1

Prove that

$$C_G(A) = \{g \in G \mid g^{-1}ag = a \text{ for all } a \in A\}.$$

Proof. By multiplying on the left by g and on the right by g^{-1}, we see that $g^{-1}ag = a$ if and only if $gag^{-1} = a$. Therefore the above set is a valid alternative way to define the centralizer of A. □

2.2.2 Exercise 2

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

Proof. Let $g \in G$ be arbitrary. If $a \in Z(G)$, then in particular, $ga = ag$ which shows that $gag^{-1} = a$. Therefore $g \in C_G(Z(G))$ for any $g \in G$, so $G \leq C_G(Z(G))$. But we know $C_G(Z(G)) \leq G$, so this establishes equality.

Since $C_G(A) \leq N_G(A)$ for any $A \subseteq G$, we must have $N_G(Z(G)) = G$. □

2.2.3 Exercise 3

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

Proof. Suppose A and B are as stated. Let $g \in C_G(B)$. Then $gbg^{-1} = b$ for any $b \in B$. But $A \subseteq B$, so $gag^{-1} = a$ for any $a \in A$ as well. Therefore $g \in C_G(A)$. This shows that $C_G(B) \subseteq C_G(A)$, and since both are subgroups of G, we have $C_G(B) \leq C_G(A)$. □

2.2.4 Exercise 4

For each of S_3, D_8, and Q_8 compute the centralizers of each element and find the center of each group. Does Lagrange's Theorem simplify your work?

Solution. The centralizer of 1 (for any group) is the entire group. The centralizers of the other elements can be computed directly. For example, $C_{S_3}((1\,2))$ must at minimum include 1 and $(1\,2)$ itself. We can test the other elements directly (note $(1\,2)^{-1} = (1\,2)$):

$$\begin{aligned}(1\,2)(1\,3)(1\,2) &= (2\,3),\\ (1\,2)(2\,3)(1\,2) &= (1\,3),\\ (1\,2)(1\,2\,3)(1\,2) &= (1\,3\,2),\\ (1\,2)(1\,3\,2)(1\,2) &= (1\,2\,3).\end{aligned}$$

So, $C_{S_3}((1\,2)) = \{1, (1\,2)\}$.

We can use Lagrange's Theorem to reduce some of the checking. For example, let $a = (1\,3)$. Then $C_{S_3}(a)$ must include the subgroup $\{1, (1\,3)\}$, so 2 divides $|C_{S_3}(a)|$. On the other hand, $|C_{S_3}(a)|$ divides $|S_3| = 6$. Therefore there are only two possibilities, either $|C_{S_3}(a)| = 2$ or 6. Since $(1\,3)$ does not commute

with $(1\,2)$, we know that the order must be 2. So $C_{S_3}(a) = \{1, (1\,3)\}$. Similarly, we find $C_{S_3}((2\,3)) = \{1, (2\,3)\}$.

Now let $a = (1\,2\,3)$. We have $a^{-1} = (1\,3\,2) = a^2$ so $C_{S_3}(a)$ must contain the cyclic subgroup $\{1, a, a^2\}$ and we see that 3 divides $|C_{S_3}(a)|$. So the order is either 3 or 6. But it must be 3, since $(1\,2\,3)$ does not commute with $(1\,2)$, for example. So $C_{S_3}(a) = \{1, a, a^2\}$. Similarly, $C_{S_3}((1\,3\,2))$ is this same set.

From the above results, we see that the center of S_3 is $Z(S_3) = \{1\}$, since no non-identity element commutes with every element of S_3.

Similarly, we may find the centralizers of D_8:

$$\begin{aligned} C_{D_8}(r) &= \{1, r, r^2, r^3\}, \\ C_{D_8}(r^2) &= D_8, \\ C_{D_8}(r^3) &= \{1, r, r^2, r^3\}, \\ C_{D_8}(s) &= \{1, r^2, s, sr^2\}, \\ C_{D_8}(sr) &= \{1, r^2, sr, sr^3\}, \\ C_{D_8}(sr^2) &= \{1, r^2, s, sr^2\}, \\ C_{D_8}(sr^3) &= \{1, r^2, sr, sr^3\}. \end{aligned}$$

And we see that $Z(D_8) = \{1, r^2\}$.

Finally, for Q_8, we have:

$$\begin{aligned} C_{Q_8}(-1) &= Q_8, \\ C_{Q_8}(i) &= \{1, -1, i, -i\}, \\ C_{Q_8}(-i) &= \{1, -1, i, -i\}, \\ C_{Q_8}(j) &= \{1, -1, j, -j\}, \\ C_{Q_8}(-j) &= \{1, -1, j, -j\}, \\ C_{Q_8}(k) &= \{1, -1, k, -k\}, \\ C_{Q_8}(-k) &= \{1, -1, k, -k\}. \end{aligned}$$

And $Z(Q_8) = \{1, -1\}$. □

2.2.5 Exercise 5

In each of parts (a) to (c) show that for the specified group G and subgroup A of G, $C_G(A) = A$ and $N_G(A) = G$.

(a) $G = S_3$ and $A = \{1, (1\,2\,3), (1\,3\,2)\}$.

Solution. A is a cyclic subgroup generated by $(1\,2\,3)$, so $A \leq C_G(A)$. By Lagrange's Theorem, 3 divides $|C_G(A)|$ which divides $|S_3| = 6$, so either $|C_G(A)| = 3$ or it is 6. But it can't be 6 since, for example, $(1\,2)$ does not commute with $(1\,2\,3)$. Therefore $|C_G(A)| = 3$ and we see that $C_G(A) = A$.

Since $C_G(A) \leq N_G(A)$, we again have either $|N_G(A)| = 3$ or 6. However,

$$(1\,2)A(1\,2) = \{1, (1\,3\,2), (1\,2\,3)\} = A,$$

so $|N_G(A)| > 3$. Therefore $N_G(A) = G$. □

(b) $G = D_8$ and $A = \{1, s, r^2, sr^2\}$.

Solution. The elements of A all commute with one another and in fact form a subgroup of D_8. By Lagrange, $|C_G(A)| = 4$ or 8. But r does not commute with s, for example, so $|C_G(A)| = 4$ and we have $C_G(A) = A$.

Since $C_G(A) \leq N_G(A)$, we must have either $N_G(A) = A$ or $N_G(A) = G$. Since

$$rAr^{-1} = \{1, sr^2, r^2, s\} = A,$$

we must have $N_G(A) = G$. □

(c) $G = D_{10}$ and $A = \{1, r, r^2, r^3, r^4\}$.

Solution. A is a cyclic subgroup. Again, by Lagrange, we must have $|C_G(A)| = 5$ or 10. But s and r do not commute, so it must be the former. Hence $C_G(A) = A$.

For the normalizer, we simply note that

$$sAs = \{1, r^4, r^3, r^2, r\} = A,$$

so $N_G(A) = G$. □

2.2.6 Exercise 6

Let H be a subgroup of the group G.

(a) Show that $H \leq N_G(H)$. Give an example to show that this is not necessarily true if H is not a subgroup.

Solution. Let $g \in H$. First, take $x \in gHg^{-1}$. Then $x = ghg^{-1}$ for some $h \in H$. Since H is a subgroup and thus closed under the group operation, we have $x \in H$. Conversely, if $x \in H$ then by definition $x \in gHg^{-1}$. Therefore $gHg^{-1} = H$ and we see that $g \in N_G(H)$. Since this is true for all $g \in H$, it follows that $H \leq N_G(H)$.

As a counterexample for the case where H is not a subgroup, consider $G = D_4$ and $H = \{1, r, s\}$. Then $sHs = \{1, r^3, s\} \neq H$, so $s \notin N_G(H)$ and $H \not\subseteq N_G(H)$. □

(b) Show that $H \leq C_G(H)$ if and only if H is abelian.

Proof. Suppose $H \leq C_G(H)$ and let $a, b \in H$. Then $a \in C_G(H)$ so in particular, $aba^{-1} = b$, or equivalently, $ab = ba$. Therefore H is abelian.

Conversely, suppose H is abelian. If $a \in H$, then $ah = ha$ for each $h \in H$. Equivalently, $aha^{-1} = h$, so that $a \in C_G(H)$. This shows that $H \leq C_G(H)$. □

2.2.7 Exercise 7

Let $n \in \mathbb{Z}$ with $n \geq 3$. Prove the following:

(a) $Z(D_{2n}) = 1$ if n is odd

Proof. Suppose $r^k \in Z(D_{2n})$ for $k \in \mathbb{Z}^+$. Since $sr^k = r^{-k}s$, we must have $r^k = r^{-k}$. Therefore $r^{2k} = 1$ and we see that $2 \mid n$, which is a contradiction.

s can't be in the center since it doesn't commute with r. Now suppose $sr^k \in Z(D_{2n})$, with $k \in \mathbb{Z}^+$. In order to commute with r, we must have $(sr^k)r = r(sr^k)$. This implies $sr^{k+1} = sr^{k-1}$, so $r^{k+1} = r^{k-1}$ and we see that $r^2 = 1$, which means $n \leq 2$, another contradiction.

Therefore the only element in $Z(D_{2n})$ is 1. □

(b) $Z(D_{2n}) = \{1, r^k\}$ if $n = 2k$

Proof. From the previous proof we know that the only possible candidates are 1 and r^k where $n = 2k$. And since $r^{2k} = 1$ we see that $r^k = r^{-k}$. Any element x in D_{2n} can be written as $x = s^i r^j$ for $i \in \{0, 1\}$ and $j \in \mathbb{Z}$, $j \geq 0$, so,

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

Hence $Z(D_{2n}) = \{1, r^k\}$. □

2.2.8 Exercise 8

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

Proof. Let $A = \{1, 2, \ldots, n\}$. We know that S_n acts on A by $\sigma \cdot j = \sigma(j)$. Then

$$G_i = \{\sigma \in G \mid \sigma \cdot i = i\}.$$

Now $1 \in G_i$ by definition of a group action, so G_i is nonempty. Suppose $\sigma, \tau \in G_i$. Again, by definition of an action,

$$\sigma\tau \cdot i = \sigma \cdot (\tau \cdot i) = \sigma \cdot i = i,$$

so G_i is closed under composition. And, since

$$i = (b^{-1}b) \cdot i = b^{-1} \cdot (b \cdot i) = b^{-1} \cdot i,$$

we see that G_i is closed under inverses. Therefore $G_i \leq G$.

Lastly, since every member of G_i fixes i, we have that $G_i \cong S_{n-1}$ so that $|G_i| = (n-1)!$. □

2.2.9 Exercise 9

For any subgroup H of G and any nonempty subset A of G define $N_H(A)$ to be the set $\{h \in H \mid hAh^{-1} = A\}$. Show that $N_H(A) = N_G(A) \cap H$ and deduce that $N_H(A)$ is a subgroup of H (note that A need not be a subset of H).

Proof. Certainly $N_H(A) \subseteq N_G(A)$, since every member h of $N_H(A)$ is a member of G for which $hAh^{-1} = A$. And $N_H(A) \subseteq H$, so $N_H(A) \subseteq N_G(A) \cap H$.

Now pick $h \in N_G(A) \cap H$. Since $h \in N_G(A)$, we have $hAh^{-1} = A$. And since $h \in H$, we see that $h \in N_H(A)$. This shows that $N_G(A) \cap H \subseteq N_H(A)$. Therefore $N_H(A) = N_G(A) \cap H$ and $N_H(A)$ must be a subgroup of G (and hence H) since it is the intersection of two subgroups of G (see Exercise 2.1.10). □

2.2.10 Exercise 10

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

Proof. Let $H = \{1, a\}$ and suppose $g \in N_G(H)$. Then $gHg^{-1} = H$. Since $g1g^{-1} = 1$, we must have $gag^{-1} = a$. Therefore $g \in C_G(H)$ and we see that $N_G(H) \leq C_G(H)$.

Now suppose $g \in C_G(H)$. Then $g1g^{-1} = 1$ and $gag^{-1} = a$, so $gHg^{-1} = H$ and $g \in N_G(H)$. Hence $C_G(H) \leq N_G(H)$ and in fact $C_G(H) = N_G(H)$.

Finally, if $N_G(H) = G$, then $C_G(H) = G$ so that $H \leq Z(G)$. □

2.2.11 Exercise 11

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

Proof. Fix a subset A of G. Let $g \in Z(G)$. Then $gag^{-1} = a$ for all $a \in A$, so this shows that $gAg^{-1} = A$. Therefore $Z(G) \leq N_G(A)$. □

2.2.12 Exercise 12

Let R be the set of all polynomials with integer coefficients in the independent variables x_1, x_2, x_3, x_4 i.e., the members of R are finite sums of elements of the form $ax_1^{r_1}x_2^{r_2}x_3^{r_3}x_4^{r_4}$, where a is any integer and $r_1, \ldots, r_4$ are nonnegative integers. For example,

$$12x_1^5x_2^7x_4 - 18x_2^3x_3 + 11x_1^6x_2x_3^3x_4^{23} \tag{2.1}$$

is a typical element of R. Each $\sigma \in S_4$ gives a permutation of $\{x_1, \ldots, x_4\}$ by defining $\sigma \cdot x_i = x_{\sigma(i)}$. This may be extended to a map from R to R by defining

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

for all $p(x_1, x_2, x_3, x_4) \in R$ (i.e., σ simply permutes the indices of the variables). For example, if $\sigma = (1\,2)(3\,4)$ and $p(x_1, \ldots, x_4)$ is the polynomial in (2.1) above, then

$$\begin{aligned}\sigma \cdot p(x_1, x_2, x_3, x_4) &= 12x_2^5x_1^7x_3 - 18x_1^3x_4 + 11x_2^6x_1x_4^3x_3^{23} \\ &= 12x_1^7x_2^5x_3 - 18x_1^3x_4 + 11x_1x_2^6x_3^{23}x_4^3.\end{aligned}$$

(a) Let $p = p(x_1, \ldots, x_4)$ be the polynomial in (2.1) above, let $\sigma = (1\,2\,3\,4)$ and let $\tau = (1\,2\,3)$. Compute $\sigma \cdot p$, $\tau \cdot (\sigma \cdot p)$, $(\tau \circ \sigma) \cdot p$, and $(\sigma \circ \tau) \cdot p$.

Solution. $\tau \circ \sigma = (1\,3\,4\,2)$ and $\sigma \circ \tau = (1\,3\,2\,4)$. So

$$\begin{aligned}\sigma \cdot p &= 12x_1x_2^5x_3^7 - 18x_3^3x_4 + 11x_1^{23}x_2^6x_3x_4^3,\\ \tau \cdot (\sigma \cdot p) &= 12x_1^7x_2x_3^5 - 18x_1^3x_4 + 11x_1x_2^{23}x_3^6x_4^3,\\ (\tau \circ \sigma) \cdot p &= 12x_1^7x_2x_3^5 - 18x_1^3x_4 + 11x_1x_2^{23}x_3^6x_4^3,\end{aligned}$$

and

$$(\sigma \circ \tau) \cdot p = 12x_1x_3^5x_4^7 - 18x_2x_4^3 + 11x_1^{23}x_2^3x_3^6x_4. \qquad \square$$

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

Proof. Clearly $1 \cdot p = p$ for any $p \in R$. For any $\sigma, \tau \in S_4$ we have

$$\begin{aligned}\sigma \cdot (\tau \cdot p(x_1, x_2, x_3, x_4)) &= \sigma \cdot p(x_{\tau(1)}, x_{\tau(2)}, x_{\tau(3)}, x_{\tau(4)})\\ &= p(x_{\sigma(\tau(1))}, x_{\sigma(\tau(2))}, x_{\sigma(\tau(3))}, x_{\sigma(\tau(4))})\\ &= (\sigma \circ \tau) \cdot p(x_1, x_2, x_3, x_4).\end{aligned}$$

Therefore the mapping is a group action. $\square$

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

Solution. The stabilizer of x_4 consists of all permutations which fix x_4: 1, $(1\,2)$, $(1\,3)$, $(2\,3)$, $(1\,2\,3)$, $(1\,3\,2)$. But these correspond precisely to the elements of S_3, so these permutations form a subgroup of S_4 which is isomorphic to S_3. $\square$

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

Solution. If σ is a member of the stabilizer $R_{x_1+x_2}$ then $\sigma \cdot (x_1 + x_2) = x_1 + x_2$. There are two ways this can happen: σ can fix 1 and 2, or σ can send 1 to 2 and vice versa. So the permutations in the stabilizer are 1, $(1\,2)$, $(3\,4)$, and $(1\,2)(3\,4)$. All of these elements commute with each other (since they consist of disjoint cycles), so $R_{x_1+x_2}$ is an abelian subgroup of order 4. $\square$

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

Solution. The permutations in S_4 which stabilize $x_1x_2 + x_3x_4$ are 1, $(1\,2)$, $(3\,4)$, $(1\,2)(3\,4)$, $(1\,3)(2\,4)$, $(1\,4)(2\,3)$, $(1\,3\,2\,4)$, and $(1\,4\,2\,3)$.

Let $\varphi\colon R_{x_1x_2+x_3x_4} \to D_8$ be the map for which

$$\varphi(1\,2) = s \quad \text{and} \quad \varphi(1\,3\,2\,4) = r.$$

Then φ extends to an isomorphism since $(1\,2)^2 = 1$, $(1\,3\,2\,4)^4 = 1$ and $(1\,2)(1\,3\,2\,4) = (1\,3\,2\,4)^{-1}(1\,2)$. $\square$

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

Solution. Checking each possibility in turn will show that the permutations in this stabilizer are exactly the same as those in the previous part of the problem. □

2.2.13 Exercise 13

Let n be a positive integer and let R be the set of all polynomials with integer coefficients in the independent variables $x_1, x_2, \ldots, x_n$, i.e., the members of R are finite sums of elements of the form $ax_1^{r_1}x_2^{r_2}\cdots x_n^{r_n}$, where a is any integer and $r_1, \ldots, r_n$ are nonnegative integers. For each $\sigma \in S_n$ define a map

$$\sigma\colon R \to R \quad \text{by} \quad \sigma \cdot p(x_1, x_2, \ldots, x_n) = p(x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(n)}).$$

Prove that this defines a (left) group action of S_n on R.

Proof. Clearly $1 \cdot p(x_1, \ldots, x_n) = p(x_1, \ldots, x_n)$. And for $\sigma, \tau \in S_n$ we have

$$\begin{aligned}\sigma \cdot (\tau \cdot p(x_1, x_2, \ldots, x_n)) &= \sigma \cdot p(x_{\tau(1)}, x_{\tau(2)}, \ldots, x_{\tau(n)}) \\ &= p(x_{\sigma(\tau(1))}, x_{\sigma(\tau(2))}, \ldots, x_{\sigma(\tau(n))}) \\ &= (\sigma \circ \tau) \cdot p(x_1, x_2, \ldots, x_n).\end{aligned}$$

Therefore this mapping does define a group action on R. □

2.2.14 Exercise 14

Let $H(F)$ be the Heisenberg group over the field F introduced in Exercise 1.4.11. Determine which matrices lie in the center of $H(F)$ and prove that $Z(H(F))$ is isomorphic to the additive group F.

Solution. Let

$$X = \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \quad \text{and} \quad Y = \begin{pmatrix} 1 & d & e \\ 0 & 1 & f \\ 0 & 0 & 1 \end{pmatrix}$$

be elements of $H(F)$. If $X \in Z(H(F))$ then $XY = YX$ for any $Y \in H(F)$. Computing XY and YX for the matrices above gives

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

and

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

So $af + b + e = b + cd + e$ or $af = cd$. Since Y can be arbitrary, the only way to guarantee this is for $a = c = 0$. If a and c are both nonzero, then any Y with $f = 0$ and $d = 1$ will not commute with X. Therefore,

$$Z(H(F)) = \left\{ \begin{pmatrix} 1 & 0 & a \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \in H(F) \;\middle|\; a \in F \right\}.$$

We can see that $Z(H(F)) \cong F$ since the map $\varphi\colon F \to Z(H(F))$ given by

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

is an isomorphism. □

2.3 Cyclic Groups and Cyclic Subgroups

2.3.1 Exercise 1

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

Solution. The subgroups are generated by x^d where d divides 45. And we have $\langle x^a \rangle \leq \langle x^b \rangle$ if $(b, 45) \mid (a, 45)$. This gives the following subgroup relationships:

$$\begin{aligned} Z_{45} = \langle x \rangle &> \langle x^3 \rangle, \langle x^5 \rangle, \langle x^9 \rangle, \langle x^{15} \rangle, 1, \\ \langle x^3 \rangle &> \langle x^9 \rangle, \langle x^{15} \rangle, 1, \\ \langle x^5 \rangle &> \langle x^{15} \rangle, 1, \\ \langle x^9 \rangle &> 1, \\ \langle x^{15} \rangle &> 1, \\ 1 = \langle x^0 \rangle. & \end{aligned}$$

□

2.3.2 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.

Proof. Let $x \in G$ where $|x| = |G| = n < \infty$. By Proposition 2, we know that $1, x, x^2, \ldots, x^{n-1}$ are all distinct elements in G. But G contains only n elements, so this must be the entirety of G. Therefore $G = \langle x \rangle$.

This is not always true if $|x| = |G| = \infty$. For example, in the additive group $\mathbb{Z}$, $|2| = |\mathbb{Z}| = \infty$ but clearly $\mathbb{Z}$ is not generated by 2. □

2.3.3 Exercise 3

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

Solution. The generators are those residue classes whose representatives are relatively prime to 48. Therefore the generators are $\overline{1}$, $\overline{5}$, $\overline{7}$, $\overline{11}$, $\overline{13}$, $\overline{17}$, $\overline{19}$, $\overline{23}$, $\overline{25}$, $\overline{29}$, $\overline{31}$, $\overline{35}$, $\overline{37}$, $\overline{41}$, $\overline{43}$, and $\overline{47}$. □

2.3.4 Exercise 4

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

Solution. $202 = 2 \cdot 101$, so the generators are all residue classes having odd representatives excluding $\overline{101}$. □

2.3.5 Exercise 5

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

Solution. If φ denotes the Euler φ-function, then the number of generators is given by

$$\begin{aligned}\varphi(49000) &= \varphi(2^3)\varphi(5^3)\varphi(7^2)\\ &= 2^2(2-1)5^2(5-1)7(7-1)\\ &= 4\cdot 100\cdot 42\\ &= 16800.\end{aligned}$$

□

2.3.6 Exercise 6

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

Solution. The elements of each subgroup are

$$\begin{aligned}\mathbb{Z}/48\mathbb{Z} = \langle \bar{1}\rangle &= \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \ldots, \overline{46}, \overline{47}\},\\ \langle \bar{2}\rangle &= \{\bar{0}, \bar{2}, \bar{4}, \bar{6}, \ldots, \overline{44}, \overline{46}\},\\ \langle \bar{3}\rangle &= \{\bar{0}, \bar{3}, \bar{6}, \bar{9}, \ldots, \overline{42}, \overline{45}\},\\ \langle \bar{4}\rangle &= \{\bar{0}, \bar{4}, \bar{8}, \overline{12}, \ldots, \overline{40}, \overline{44}\},\\ \langle \bar{6}\rangle &= \{\bar{0}, \bar{6}, \overline{12}, \overline{18}, \overline{24}, \overline{30}, \overline{36}, \overline{42}\},\\ \langle \bar{8}\rangle &= \{\bar{0}, \bar{8}, \overline{16}, \overline{24}, \overline{32}, \overline{40}\},\\ \langle \overline{12}\rangle &= \{\bar{0}, \overline{12}, \overline{24}, \overline{36}\},\\ \langle \overline{16}\rangle &= \{\bar{0}, \overline{16}, \overline{32}\},\\ \langle \overline{24}\rangle &= \{\bar{0}, \overline{24}\},\\ \langle \bar{0}\rangle &= \{\bar{0}\}.\end{aligned}$$

And we have the following inclusions:

$$\begin{aligned}\langle \bar{0}\rangle, \langle \bar{1}\rangle, \langle \bar{2}\rangle, \langle \bar{3}\rangle, \langle \bar{4}\rangle, \langle \bar{6}\rangle, \langle \bar{8}\rangle, \langle \overline{12}\rangle, \langle \overline{16}\rangle, \langle \overline{24}\rangle &\le \langle \bar{1}\rangle,\\ \langle \bar{0}\rangle, \langle \bar{2}\rangle, \langle \bar{4}\rangle, \langle \bar{6}\rangle, \langle \bar{8}\rangle, \langle \overline{12}\rangle, \langle \overline{16}\rangle, \langle \overline{24}\rangle &\le \langle \bar{2}\rangle,\\ \langle \bar{0}\rangle, \langle \bar{3}\rangle, \langle \bar{6}\rangle, \langle \overline{12}\rangle, \langle \overline{16}\rangle, \langle \overline{24}\rangle &\le \langle \bar{3}\rangle,\\ \langle \bar{0}\rangle, \langle \bar{4}\rangle, \langle \bar{8}\rangle, \langle \overline{12}\rangle, \langle \overline{16}\rangle, \langle \overline{24}\rangle &\le \langle \bar{4}\rangle,\\ \langle \bar{0}\rangle, \langle \bar{6}\rangle, \langle \overline{12}\rangle, \langle \overline{24}\rangle &\le \langle \bar{6}\rangle,\\ \langle \bar{0}\rangle, \langle \bar{8}\rangle, \langle \overline{16}\rangle, \langle \overline{24}\rangle &\le \langle \bar{8}\rangle,\\ \langle \bar{0}\rangle, \langle \overline{12}\rangle, \langle \overline{24}\rangle &\le \langle \overline{12}\rangle,\\ \langle \bar{0}\rangle, \langle \overline{16}\rangle &\le \langle \overline{16}\rangle,\\ \langle \bar{0}\rangle, \langle \overline{24}\rangle &\le \langle \overline{24}\rangle,\\ \langle \bar{0}\rangle &\le \langle \bar{0}\rangle.\end{aligned}$$

□

2.3.7 Exercise 7

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

Solution. The subgroups are $\langle x\rangle$, $\langle x^2\rangle$, $\langle x^3\rangle$, $\langle x^4\rangle$, $\langle x^6\rangle$, $\langle x^8\rangle$, $\langle x^{12}\rangle$, $\langle x^{16}\rangle$, $\langle x^{24}\rangle$, and 1. □

2.3.8 Exercise 8

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

Solution. Choose an a with $(a, 48) = d > 1$ and set $b = 48/d$. If φ_a is a homomorphism, then

$$\varphi_a(\bar{b}) = \varphi_a(b \cdot \bar{1}) = \varphi_a(\bar{1})^b = x^{ab} = (x^{48})^{a/d} = 1 = \varphi_a(\bar{0}).$$

Therefore, in this case, φ_a is not an injection and thus not an isomorphism.

This suggests that φ_a extends to an isomorphism if and only if $(a, 48) = 1$, which we will now prove. First we show that the function $\bar{b} \mapsto x^{ab}$ is well defined, i.e., that the value of the function is not affected by the choice of representative for $\bar{b}$. Suppose $\bar{b} = \bar{c}$. Then $48k = b - c$ for some integer k, and we have

$$\varphi_a(\bar{b}) = x^{ab} = x^{a(48k+c)} = (x^{48})^{ak} x^{ac} = 1^{ak} x^{ac} = x^{ac} = \varphi_a(\bar{c}).$$

Now, φ_a is certainly a homomorphism, since

$$\varphi_a(\bar{b} + \bar{c}) = x^{a(b+c)} = x^{ab} x^{ac} = \varphi_a(\bar{b}) \varphi_a(\bar{c}).$$

To show injectivity, suppose $\varphi_a(\bar{b}) = \varphi_a(\bar{c})$. Then $x^{ab} = x^{ac}$ or $x^{a(b-c)} = 1$. Hence $48 \mid a(b-c)$ and since $(a, 48) = 1$ we have $48 \mid (b-c)$. This shows that $\bar{b} = \bar{c}$.

Finally, since $|\mathbb{Z}/48\mathbb{Z}| = |Z_{48}| < \infty$, we know that injectivity of φ_a implies surjectivity, so that φ_a is an isomorphism. □

2.3.9 Exercise 9

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

Solution. Suppose $\bar{b} = \bar{c}$ for integers b and c. If ψ_a is well defined then $\psi_a(\bar{b}) = \psi_a(\bar{c})$, that is, $x^{ab} = x^{ac}$. Then $x^{a(b-c)} = 1$ so we must have $36 \mid a(b-c)$. But $48 \mid (b-c)$, so there is an integer k for which $48k = b - c$ and we have that $36 \mid 48ak$. If we choose $\bar{b}$ and $\bar{c}$ so that $k = 1$, then we must have $3 \mid a$ as a necessary condition for $36 \mid 48ak$. It is also sufficient that $3 \mid a$, since $36 \mid 144mk$.

Since

$$\psi_a(\bar{b} + \bar{c}) = x^{a(b+c)} = x^{ab} x^{ac} = \psi_a(\bar{b}) \psi_a(\bar{c}),$$

we see that ψ_a is a well defined homomorphism if and only if $3 \mid a$.

Lastly, suppose $\psi_a(\bar{b}) = x$. Since $a = 3k$ for some integer k, we have

$$x = \psi_a(\bar{b}) = x^{ab} = x^{3kb}.$$

Therefore $x^{3kb-1} = 1$ and we see that 36 divides $3kb - 1$. But this is impossible since if $36m = 3kb - 1$ then $1 = 3kb - 36m = 3(kb - 12m)$ and $3 \mid 1$, a contradiction. So the homomorphism ψ_a can never be surjective. □

2.3.10 Exercise 10

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

Solution. Since $|\bar{1}| = 54$, by Proposition 5 (2) we have

$$|\overline{30}| = |30 \cdot \bar{1}| = \frac{54}{(30, 54)} = \frac{54}{6} = 9.$$

Then

$$\langle\overline{30}\rangle = \{\bar{0}, \bar{6}, \overline{12}, \overline{18}, \overline{24}, \overline{30}, \overline{36}, \overline{42}, \overline{48}\}$$

where

$$\begin{aligned}
|\bar{0}| &= 1, \\
|\bar{6}| &= 9, \\
|\overline{12}| &= 9, \\
|\overline{18}| &= 3, \\
|\overline{24}| &= 9, \\
|\overline{30}| &= 9, \\
|\overline{36}| &= 3, \\
|\overline{42}| &= 9, \\
|\overline{48}| &= 9.
\end{aligned}$$

□

2.3.11 Exercise 11

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

Solution. The cyclic subgroups are

$$\begin{aligned}
\langle 1\rangle &= 1, \\
\langle r\rangle = \langle r^3\rangle &= \{1, r, r^2, r^3\}, \\
\langle r^2\rangle &= \{1, r^2\}, \\
\langle s\rangle &= \{1, s\}, \\
\langle sr\rangle &= \{1, sr\}, \\
\langle sr^2\rangle &= \{1, sr^2\}, \\
\langle sr^3\rangle &= \{1, sr^3\}.
\end{aligned}$$

A proper subgroup that is not cyclic is $\langle s, r^2\rangle = \{1, r^2, s, sr^2\}$. □

2.3.12 Exercise 12

Prove that the following groups are *not* cyclic:

(a) $Z_2 \times Z_2$

Proof. Let $Z_2 = \langle x \rangle$. Checking each element of $Z_2 \times Z_2$, we see that none generate the whole group:

$$\begin{aligned}\langle (1,1) \rangle &= \{(1,1)\},\\ \langle (1,x) \rangle &= \{(1,1),(1,x)\},\\ \langle (x,1) \rangle &= \{(1,1),(x,1)\},\end{aligned}$$

and

$$\langle (x,x) \rangle = \{(1,1),(x,x)\}.$$

Therefore $Z_2 \times Z_2$ is not cyclic. □

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

Proof. If $Z_2 \times \mathbb{Z}$ is cyclic, then it must have a generator of the form $(1,n)$ or (x,n) for some $n \in \mathbb{Z}$. But $(1,n)$ cannot be a generator since it only generates elements whose first component is 1.

So the generator must have the form (x,n). Now n can only be 1 or -1, since otherwise we could not get all the integers in the second component. But neither of these is a generator since, for example, $(1,1)$ is not in either cyclic subgroup. Therefore $Z_2 \times \mathbb{Z}$ is not cyclic. □

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

Proof. Any generator for $\mathbb{Z} \times \mathbb{Z}$ must have the form $(\pm 1, \pm 1)$ since there is no other way to generate all of the integers in each component. But every element in a subgroup generated by $(\pm 1, \pm 1)$ must have components which differ only in sign. For example, none of these elements will generate $(1,2)$. Therefore $\mathbb{Z} \times \mathbb{Z}$ is not cyclic. □

2.3.13 Exercise 13

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

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

Proof. Isomorphisms preserve order of elements, so $\mathbb{Z} \times Z_2$ cannot be isomorphic to $\mathbb{Z}$ since the element $(0,x)$ in $\mathbb{Z} \times Z_2$ has order 2 but no element in $\mathbb{Z}$ has order 2. □

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

Proof. Again, $\mathbb{Q}$ has no elements of order 2, but $|(0,x)| = 2$ in $\mathbb{Q} \times Z_2$. Hence the two groups are not isomorphic. □

2.3.14 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 $|\sigma| = 12$, the powers of σ consist of exactly 12 distinct elements. We can use the Division Algorithm to reduce arbitrary powers to their least residues. For example,

$$626 = 52(12) + 2,$$

so $\sigma^{626} = (\sigma^{12})^{52}\sigma^2 = \sigma^2$. Applying this process for each of the given values produces the following permutations:

$$\begin{aligned}
\sigma^{13} = \sigma^{1(12)+1} = \sigma &= (1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ 10\ 11\ 12)\\
\sigma^{65} = \sigma^{5(12)+5} = \sigma^5 &= (1\ 6\ 11\ 4\ 9\ 2\ 7\ 12\ 5\ 10\ 3\ 8)\\
\sigma^{626} = \sigma^{52(12)+2} = \sigma^2 &= (1\ 3\ 5\ 7\ 9\ 11)(2\ 4\ 6\ 8\ 10\ 12)\\
\sigma^{1195} = \sigma^{99(12)+7} = \sigma^7 &= (1\ 8\ 3\ 10\ 5\ 12\ 7\ 2\ 9\ 4\ 11\ 6)\\
\sigma^{-6} = \sigma^{-1(12)+6} = \sigma^6 &= (1\ 7)(2\ 8)(3\ 9)(4\ 10)(5\ 11)(6\ 12)\\
\sigma^{-81} = \sigma^{-7(12)+3} = \sigma^3 &= (1\ 4\ 7\ 10)(2\ 5\ 8\ 11)(3\ 6\ 9\ 12)\\
\sigma^{-570} = \sigma^{-48(12)+6} = \sigma^6 &= (1\ 7)(2\ 8)(3\ 9)(4\ 10)(5\ 11)(6\ 12)\\
\sigma^{-1211} = \sigma^{-101(12)+1} = \sigma &= (1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ 10\ 11\ 12).
\end{aligned}$$

□

2.3.15 Exercise 15

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

Proof. In Exercise 2.3.12 we showed that $\mathbb{Z} \times \mathbb{Z}$ is not cyclic. But $\mathbb{Z} \times \mathbb{Z}$ is a subgroup of $\mathbb{Q} \times \mathbb{Q}$, and a cyclic group cannot have a non-cyclic subgroup. Therefore $\mathbb{Q} \times \mathbb{Q}$ is not cyclic. □

2.3.16 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. Let ℓ be the least common multiple of m and n. Then there are integers a and b such that $am = \ell$ and $bn = \ell$. So if $|x| = m$ and $|y| = n$ for commuting elements x and y, then

$$(xy)^\ell = x^\ell y^\ell = (x^m)^a (y^n)^b = 1.$$

Therefore $|xy|$ must divide ℓ by Proposition 3, which completes the proof.

We note that this need not be true if x and y do not commute. For example, in the symmetric group S_3, $|(1\,2)| = |(2\,3)| = 2$ but $(1\,2)(2\,3) = (1\,2\,3)$ which has order 3. Clearly $3 \nmid 2$.

Finally, for an example where x and y commute but the order of xy does not equal the least common multiple of $|x|$ and $|y|$, consider the cyclic group Z_{10}. This group is abelian so all elements commute, and we have $|x^2| = 5$ and $|x^3| = 10$, but $|x^5| = 2 \neq 10$. □

2.3.17 Exercise 17

Find a presentation for Z_n with one generator.

Solution. We know that Z_n can be generated by a single element x which satisfies the one relation $x^n = 1$. Moreover, any group generated by a single element and satisfying only this relation must be isomorphic to Z_n, since all cyclic groups of the same order are isomorphic. So one possible presentation is

$$Z_n = \langle x \mid x^n = 1 \rangle. \qquad \square$$

2.3.18 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 $x \mapsto h$.

Proof. Define the function $\varphi\colon Z_n \to H$ by

$$\varphi(x^n) = h^n.$$

First we need to show that φ is well defined. Suppose $x^a = x^b$. Then $x^{a-b} = 1$ so $n \mid (a-b)$ (Proposition 3). So there is an integer c such that $cn = a - b$. We may then write $a = cn + b$ so that

$$\varphi(x^a) = h^a = h^{cn+b} = (h^n)^c h^b = h^b = \varphi(x^b)$$

as required.

To show that φ is a homomorphism, consider two arbitrary elements $y = x^k$ and $z = x^\ell$ in Z_n. By the exponent rules established in Exercise 1.1.19, we have

$$\varphi(yz) = \varphi(x^k x^\ell) = \varphi(x^{k+\ell}) = h^{k+\ell} = h^k h^\ell = \varphi(x^k)\varphi(x^\ell) = \varphi(y)\varphi(z),$$

so φ is indeed a homomorphism.

Lastly, to show uniqueness, suppose $\psi\colon Z_n \to H$ is any homomorphism such that $\psi(x) = h$. Then for any integer k, we wish to show that we must have

$$\psi(x^k) = h^k.$$

Note that we only need to consider $0 \leq k \leq n-1$ since any other power is equal to one of these. We now proceed by induction on k. $\psi(x) = h$ by assumption, so the base case is satisfied. Suppose $\psi(x^k) = h^k$ for some nonnegative integer k. Then by the definition of a homomorphism and by the inductive hypothesis,

$$\psi(x^{k+1}) = \psi(x^k x) = \psi(x^k)\psi(x) = h^k h = h^{k+1},$$

which establishes that $\varphi = \psi$ and thus completes the proof. $\square$

2.3.19 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 $1 \mapsto h$.

Proof. Let $\varphi\colon \mathbb{Z} \to H$ be given by

$$\varphi(n) = h^n.$$

Then φ is a function which maps 1 to h. It is also a homomorphism, since for any integers m and n,

$$\varphi(m+n) = h^{m+n} = h^m h^n = \varphi(m)\varphi(n).$$

Finally, this homomorphism is uniquely determined because any homomorphism $\psi\colon \mathbb{Z} \to H$ such that $\psi(1) = h$ must satisfy $\psi(n) = \psi(n1) = \psi(1)^n = h^n$. □

2.3.20 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 $m \leq n$.

Proof. If $x^{p^n} = 1$, then by Proposition 3 we have $|x|$ divides p^n. But the only integers that divide a prime power p^n are smaller prime powers p^m (including $p^0 = 1$). Therefore $|x| = p^m$ for some nonnegative integer m with $m \leq n$. □

2.3.23 Exercise 23

Show that $(\mathbb{Z}/2^n\mathbb{Z})^\times$ is not cyclic for any $n \geq 3$.

Proof. By Theorem 7 we know that if $(\mathbb{Z}/2^n\mathbb{Z})^\times$ is cyclic, then it must have at most one subgroup with order 2. Therefore the proof will be complete if we can show that $(\mathbb{Z}/2^n\mathbb{Z})^\times$ has more than one distinct subgroup of order 2. This is equivalent to showing that the group has more than one element with order 2.

For $n \geq 3$, we have

$$(2^n - 1)^2 \equiv (-1)^2 \equiv 1 \pmod{2^n}$$

and

$$\begin{aligned}(2^{n-1} - 1)^2 &= 2^{2n-2} - 2^n + 1 \\ &= 2^{n-2}2^n - 2^n + 1 \\ &\equiv 1 \pmod{2^n}.\end{aligned}$$

As long as $n \geq 3$, both of the elements $\overline{2^n - 1}$ and $\overline{2^{n-1} - 1}$ are distinct from $\bar{1}$ and hence have order 2. And the two elements are distinct, since $2^{n-1} \not\equiv 2^n \pmod{2^n}$. Hence $(\mathbb{Z}/2^n\mathbb{Z})^\times$ cannot be cyclic. □

2.3.24 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 $a \in \mathbb{Z}$.

Proof. If $g \in N_G(\langle x \rangle)$ then $g\langle x \rangle g^{-1} = \langle x \rangle$. Since $gxg^{-1} \in g\langle x \rangle g^{-1}$, we must have $gxg^{-1} \in \langle x \rangle$ or $gxg^{-1} = x^a$ for some integer a. □

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

Proof. Suppose $gxg^{-1} = x^a$ for an integer a.

First we will show that

$$gx^k g^{-1} = (gxg^{-1})^k \quad \text{for all } k \in \mathbb{Z}. \tag{2.2}$$

This obviously holds for $k = 0$, so suppose $k \neq 0$. Since $gx^{-1}g^{-1} = (gxg^{-1})^{-1}$, it is sufficient to show that (2.2) is true for positive integers k.

We proceed by induction on k. The base case is trivial. Suppose $gx^k g^{-1} = (gxg^{-1})^k$ for some positive integer k. Then

$$\begin{aligned} gx^{k+1}g^{-1} &= gx^k xg^{-1} = gx^k(g^{-1}g)xg^{-1} \\ &= (gx^k g^{-1})(gxg^{-1}) = (gxg^{-1})^{k+1}, \end{aligned}$$

so (2.2) holds for all integers k.

Now suppose $y \in g\langle x \rangle g^{-1}$. Then there is $k \in \mathbb{Z}$ such that $y = gx^k g^{-1}$. From the preceding paragraph, we then have $y = (gxg^{-1})^k = x^{ak}$. Therefore $y \in \langle x \rangle$ so that $g\langle x \rangle g^{-1} \leq \langle x \rangle$.

But we know that $|g\langle x \rangle g^{-1}| = |\langle x \rangle|$ by Exercise 1.7.17. Since x has finite order (G is finite), it follows that $g\langle x \rangle g^{-1} = \langle x \rangle$ and $g \in N_G(\langle x \rangle)$. □

2.3.25 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 to prove the same is true for any finite group of order n.

Proof. We will prove the general result directly. Fix an integer k relatively prime to n and let φ denote the map $x \mapsto x^k$ for the group G, where $|G| = n$. Since $(n, k) = 1$, we may find $a, b \in \mathbb{Z}$ such that

$$ak + bn = 1.$$

Now let $g \in G$ be arbitrary and consider the image of g^a under φ. We have

$$\varphi(g^a) = g^{ak} = g^{1-bn} = g(g^n)^{-b}.$$

We know by Langrange's Theorem that $|g|$ divides n (since $\langle g \rangle$ is a cyclic subgroup of order $|g|$), so $g^n = 1$. We then have

$$\varphi(g^a) = g,$$

which completes the proof that φ is surjective. □

2.3.26 Exercise 26

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

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

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

Proof. σ_a is a homomorphism since for any $x, y \in Z_n$,

$$\sigma_a(xy) = (xy)^a = x^a y^a = \sigma_a(x)\sigma_a(y),$$

where the second equality holds due to the fact that Z_n is abelian. Therefore σ_a is an automorphism if and only if it is bijective. But Z_n is finite, so σ_a is bijective if and only if it is surjective.

If a and n are relatively prime, then we know by the previous exercise that σ_a is surjective and hence an automorphism.

Conversely, suppose σ_a is a bijection, let $d = (n, a)$, and find integers b, c such that $n = bd$ and $a = cd$. If g is a generator for Z_n then

$$\sigma_a(g^b) = g^{ab} = g^{cdb} = g^{cn} = (g^n)^c = 1 = \sigma_a(1).$$

If g^b is distinct from 1, then the map σ_a is not injective and we have a contradiction. Therefore $g^b = 1$, and since $|g| = n$ it follows that $n = b$ so that $d = (n, a) = 1$. □

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

Proof. Let $Z_n = \langle g \rangle$.

First suppose that $\sigma_a = \sigma_b$. Then in particular

$$g^a = \sigma_a(g) = \sigma_b(g) = g^b$$

so that $g^{a-b} = 1$. Thus by Proposition 3, $n \mid (a - b)$. That is, $a \equiv b \pmod{n}$.

Conversely, if $a \equiv b \pmod{n}$ then $nc = a - b$ for some integer c and we have for any $g^k \in Z_n$,

$$\sigma_a(g^k) = g^{ak} = g^{(nc+b)k} = g^{bk}(g^n)^{ck} = g^{bk} = \sigma_b(g^k),$$

hence $\sigma_a = \sigma_b$ as required. □

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

Proof. Let $\varphi \in \mathrm{Aut}(Z_n)$ and suppose $\varphi(g) = g^k$, where g is a generator for Z_n. Then for any $g^i \in Z_n$, we have

$$\varphi(g^i) = \varphi(g)^i = (g^k)^i = g^{ik} = \sigma_k(g^i),$$

which shows that $\varphi = \sigma_k$. □

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

Proof. It is immediate from the definition of σ_a and σ_b that

$$(\sigma_a \circ \sigma_b)(g^i) = \sigma_a(g^{bi}) = g^{abi} = \sigma_{ab}(g^i)$$

for any $g^i \in Z_n$.

By part (a) above, we know that $\bar{a} \in (\mathbb{Z}/n\mathbb{Z})^\times$ if and only if $\sigma_a \in \mathrm{Aut}(Z_n)$. So we may define

$$\psi\colon (\mathbb{Z}/n\mathbb{Z})^\times \to \mathrm{Aut}(Z_n) \quad \text{by} \quad \psi(\bar{a}) = \sigma_a.$$

We know by part (b) that ψ is well defined. And ψ is a homomorphism since

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

Now, ψ is injective by part (b), and it is surjective by part (c). Therefore ψ is an isomorphism and $(\mathbb{Z}/n\mathbb{Z})^\times \cong \mathrm{Aut}(Z_n)$. It follows that $\mathrm{Aut}(Z_n)$ is an abelian group of order $\varphi(n)$ where φ is the Euler φ-function. □

2.4 Subgroups Generated by Subsets of a Group

2.4.1 Exercise 1

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

Proof. Let H be a subgroup of G. Certainly $H \leq \langle H \rangle$. Now suppose $h \in \langle H \rangle$. Then

$$h \in \bigcap_{\substack{H \subseteq K \\ K \leq G}} K.$$

But H itself is a subgroup of G containing itself as a subset, so by definition $h \in H$. This shows that $\langle H \rangle \leq H$ so that $\langle H \rangle = H$ as required. □

2.4.2 Exercise 2

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

Proof. Let $a \in \langle A \rangle$. Since $A \subseteq B$ we have $a \in B$ so that $a \in \langle B \rangle$. This shows that $\langle A \rangle \leq \langle B \rangle$.

For the requested example, simply consider Z_4 with $A = \{x\}$ and $B = \{x, x^3\}$. Certainly $A \subset B$ but $\langle A \rangle = \langle B \rangle$. □

2.4.3 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.

Proof. Let $H \leq G$ be an abelian subgroup and let $g, h \in \langle H, Z(G) \rangle$ be arbitrary. By Proposition 9, g and h can be written as a finite product

$$g = g_1^{\epsilon_1}, \ldots, g_m^{\epsilon_m} \quad \text{and} \quad h = h_1^{\delta_1}, \ldots, h_n^{\delta_n},$$

where each g_i and h_i (not necessarily distinct) is in $H \cup Z(G)$. Now, members of H commute with each other and with members of $Z(G)$, and members of $Z(G)$ commute with each other and with members of H. Therefore all of the elements in $H \cup Z(G)$ commute with one another, so we may write

$$gh = g_1^{\epsilon_1}, \ldots, g_m^{\epsilon_m} h_1^{\delta_1}, \ldots, h_n^{\delta_n} = h_1^{\delta_1}, \ldots, h_n^{\delta_n} g_1^{\epsilon_1}, \ldots, g_m^{\epsilon_m} = hg.$$

Since $g, h \in \langle H, Z(G) \rangle$ were arbitrary, this shows that $\langle H, Z(G) \rangle$ is abelian.

To show that $\langle H, C_G(H) \rangle$ is not necessarily abelian, consider the dihedral group D_8 with $H = \{1, r^2\}$. Since 1 and r^2 are in $Z(D_8)$, we have $C_G(H) = D_8$. Therefore $\langle H, C_G(H) \rangle = D_8$ is not abelian, even though H is abelian. □

2.4.4 Exercise 4

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

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

2.4.5 Exercise 5

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

Proof. There are three elements of order 2 in S_3, namely $(1\,2)$, $(1\,3)$, and $(2\,3)$. For $\langle (1\,2), (1\,3)\rangle$ we have

$$(2\,3) = (1\,3)(1\,2)(1\,3), \quad (1\,2\,3) = (1\,3)(1\,2), \quad \text{and} \quad (1\,3\,2) = (1\,2)(1\,3),$$

so $\langle (1\,2), (1\,3)\rangle = S_3$. By symmetry, we also have

$$\langle (1\,2), (2\,3)\rangle = \langle (1\,3), (2\,3)\rangle = S_3.$$

Therefore the desired result holds. □

2.4.6 Exercise 6

Prove that the subgroup of S_4 generated by $(1\,2)$ and $(1\,2)(3\,4)$ is a noncyclic group of order 4.

Proof. Let $a = (1\,2)$ and $b = (1\,2)(3\,4)$. Note that $a^2 = b^2 = 1$, and $ab = ba = (3\,4)$. We see that the set $A = \{1, a, b, (3\,4)\}$ is closed under composition and inverses and hence is a subgroup of order 4. Therefore $\langle a, b\rangle = A$ and we see that A is noncyclic since in particular it has two distinct elements with order 2. □

2.4.7 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.

Proof. Let $a = (1\,2)$, $b = (1\,3)(2\,4)$ and $c = (1\,3\,2\,4)$. It is easy to check that $ab = c$ so $c \in \langle a, b\rangle$.

Clearly $a^2 = c^4 = 1$. Since b is a product of disjoint 2-cycles, it follows that $b^{-1} = b$ so that

$$ca = aba = a(ab)^{-1} = ac^{-1}.$$

Since a and c satisfy all the same relations as do s and r in D_8, it follows that there is a homomorphism $\varphi\colon D_8 \to \langle a, b\rangle$ defined by

$$\varphi(s^i r^j) = a^i (ab)^j, \quad \text{where } i \in \{0, 1\} \text{ and } j \in \{0, 1, 2, 3\}.$$

Since c, c^2, and c^3 are all distinct, it follows that φ is injective. And φ is surjective since every finite product of powers of a and b can be reduced to the form $a^i(ab)^j$ in the same way that elements of D_8 can be expressed in the form $s^i r^j$. φ is bijective, so it is an isomorphism and we have $D_8 \cong \langle a, b\rangle$. □

2.4.8 Exercise 8

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

Proof. Let $A = \langle (1\,2\,3\,4), (1\,2\,4\,3)\rangle$. By inspection, we find that

$$(1\,4\,2) = (1\,2\,4\,3)(1\,2\,3\,4).$$

Therefore A contains an element of order 3 as well as elements of order 4. Thus 3 and 4 both divide $|A|$. But $|A|$ also divides 24, so the only possibilities for $|A|$ are 12 and 24.

To eliminate 12 as a possible order, note that

$$(1\,2) = (1\,2\,3\,4)(1\,2\,4\,3)^3(1\,2\,3\,4)$$

and

$$(1\,3\,2\,4) = (1\,3)(2\,4) = (1\,2\,3\,4)(1\,2\,4\,3)(1\,2\,3\,4)(1\,2\,4\,3)^2.$$

So by the previous exercise, we know that A contains a subgroup isomorphic to D_8. Therefore 8 divides $|A|$ so we must have $A = S_4$. □

2.4.9 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 $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$.

Proof. Let

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}.$$

Note that $A, B \in SL_2(\mathbb{F}_3)$. We are told that we may assume that the subgroup $SL_2(\mathbb{F}_3)$ has order 24, so we can show that $\langle A, B\rangle = SL_2(\mathbb{F}_3)$ if we can show that it has more than 12 elements (since the order of $\langle A, B\rangle$ must divide 24).

The matrices I, A, and B, make three elements, so we need to find ten more:

$$A^2 = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, \qquad B^2 = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix},$$

$$AB = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}, \qquad (AB)^2 = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix},$$

$$(AB)^3 = \begin{pmatrix} 1 & 2 \\ 2 & 2 \end{pmatrix}, \qquad BA = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix},$$

$$A^2B^2 = \begin{pmatrix} 2 & 2 \\ 2 & 1 \end{pmatrix}, \qquad ABA = \begin{pmatrix} 2 & 0 \\ 1 & 2 \end{pmatrix},$$

$$BAB = \begin{pmatrix} 2 & 1 \\ 0 & 2 \end{pmatrix}, \qquad A^2B = \begin{pmatrix} 0 & 2 \\ 1 & 1 \end{pmatrix}.$$

So $|\langle A, B\rangle| = 24$ and $\langle A, B\rangle = SL_2(\mathbb{F}_3)$. □

2.4.10 Exercise 10

Prove that the 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.

Proof. Let

$$A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad , B = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad \text{and} \quad C = AB = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}.$$

Now note that $A^2 = B^2 = C^2 = ABC = -I$ and that $-I$ commutes with A, B, and C. Therefore there is a surjective homomorphism $\varphi\colon Q_8 \to \langle A, B\rangle$ given by

$$\varphi(i) = A \quad \text{and} \quad \varphi(j) = B.$$

This shows that $|\langle A, B\rangle| \leq 8$. But $I, -I, A, B, C$ are five distinct elements of $\langle A, B\rangle$, so $|\langle A, B\rangle| = 8$ and φ is an isomorphism. □

2.4.11 Exercise 11

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

Proof. In the previous exercise we saw that $SL_2(\mathbb{F}_3)$ has a subgroup isomorphic to Q_8. Q_8 has six elements of order 4 (Exercise 1.5.1) while S_4 also has six elements of order 4 (Exercise 1.3.4). But earlier we showed that S_4 was generated by two of these elements (Exercise 2.4.8). Therefore S_4 cannot contain a subgroup isomorphic to Q_8, and this is enough to show that $SL_2(\mathbb{F}_3)$ is not isomorphic to S_4. □

2.4.12 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.

Proof. Let T denote the upper triangular matrices of $GL_3(\mathbb{F}_2)$. There are 6 entries in a 3×3 matrix that are on or above the diagonal. However, none of the diagonal entries can be zero since such matrices would have a determinant of zero. Therefore T has only $2^3 = 8$ elements.

Now, let

$$A = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

By direct computation we can see that $A^4 = B^2 = I$ and that $AB = BA^{-1}$. Thus the mapping $\varphi\colon D_8 \to T$ for which $\varphi(r) = A$ and $\varphi(s) = B$ extends to a homomorphism. Since A generates a cyclic subgroup of T with order 4 and B is not in this subgroup, it follows that $\langle A, B\rangle = T$ which shows that φ is actually surjective. Since $|T| = |D_8|$ it must be injective as well. Hence $T \cong D_8$. □

2.4.13 Exercise 13

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

$$\left\{ \frac{1}{p} \;\middle|\; p \text{ is a prime} \right\}.$$

Proof. Call the set A and let $r = s/t$ be a positive rational number, where s and t are relatively prime integers. s and t can each be factored into a finite (possibly empty) product of powers of distinct prime factors. But every prime p is a member of $\langle A \rangle$, since $1/p \in A$ and $\langle A \rangle$ is closed under inverses. Therefore r is a finite product of members of $\langle A \rangle$, so $r \in \langle A \rangle$ by Proposition 9. This shows that $\langle A \rangle$ is the multiplicative group $\mathbb{Q}^+$. □

2.4.14 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.

Proof. If G is a finite group, then simply note that $G = \langle G \rangle$. □

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

Proof. $\mathbb{Z}$ is finitely generated since it is cyclic: it is generated by $\{1\}$. □

(c) Prove that every finitely generated subgroup of the additive group $\mathbb{Q}$ is cyclic.

Proof. Let H be a finitely generated subgroup of $\mathbb{Q}$, so that $H = \langle A \rangle$ for some finite set

$$A = \left\{ \frac{a_1}{b_1}, \frac{a_2}{b_2}, \ldots, \frac{a_n}{b_n} \right\},$$

where each $b_i \neq 0$ and $(a_i, b_i) = 1$ for each i. Set $K = b_1 b_2 \cdots b_n$. We will show that H is a subgroup of the cyclic subgroup generated by $1/K$.

Now, every element h of H can be written

$$h = c_1 \frac{a_{i_1}}{b_{i_1}} + c_2 \frac{a_{i_2}}{b_{i_2}} + \cdots + c_k \frac{a_{i_k}}{b_{i_k}}, \quad c_j \in \mathbb{Z}.$$

By multiplying the numerator and denominator of each fraction by the necessary quantity, we can make each fraction have K in its denominator. Then the fractions can be added together to get a single fraction of the form

$$h = \frac{J}{K} = J\left(\frac{1}{K}\right), \quad J \in \mathbb{Z}.$$

This shows that $h \in \langle 1/K \rangle$, so H is a subgroup of a cyclic group and is hence cyclic. □

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

Proof. Suppose $\mathbb{Q}$ is finitely generated. Then it must be cyclic by the previous part of the exercise. Therefore $\mathbb{Q} = \langle p/q \rangle$ for some relatively prime integers p and q with q nonzero. Let r be any prime number that is not a factor of q. Since p/q is a generator for $\mathbb{Q}$ we must have

$$k\frac{p}{q} = \frac{1}{r} \quad \text{for some } k \in \mathbb{Z}.$$

But then $q = pkr$, so that r is a factor of q. This contradiction shows that $\mathbb{Q}$ cannot be finitely generated. □

2.4.15 Exercise 15

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

Solution. By the previous exercise, we know that such a subgroup cannot be finitely generated. Consider the set A given by

$$A = \left\{ \frac{1}{2^k} \;\middle|\; k = 0, 1, 2, \dots \right\}.$$

Let $H = \langle A \rangle$. Then H is a proper subgroup of $\mathbb{Q}$ since, for example, $1/3$ is not a member. If H is cyclic, let it be generated by p/q where $p, q \in \mathbb{Z}$. Now q must be a power of 2, say $q = 2^n$. Then $1/2^{n+1}$ is not an integer multiple of p/q, but it is in H. This shows that H is not cyclic. □

2.4.16 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.

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

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

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

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

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

(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.

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

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

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

2.4.17 Exercise 17

This is an exercise involving Zorn's Lemma to prove that every nontrivial finitely generated group possesses 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.

Proof. We assume that $\mathcal{C}$ is nonempty. Set

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

Since a subgroup cannot be empty, H is nonempty. Suppose a and b are any members of H. Then $a \in K_1$ and $b \in K_2$ for some $K_1, K_2 \in \mathcal{C}$. Since $\mathcal{C}$ is a chain, we must have either $K_1 \leq K_2$ or $K_2 \leq K_1$ (or both). Without loss of generality, we may assume $K_1 \leq K_2$. Then a and b both belong to K_2. K_2 is a subgroup, so ab^{-1} also belongs to K_2 and hence to H. This shows that H is a subgroup of G. □

(b) Prove that H is a *proper* subgroup.

Proof. Assume the contrary, so that in particular H contains each generator $g_1, \ldots, g_n$ of G. Then there are subgroups $K_1, K_2, \ldots, K_n$ (not

necessarily distinct) such that $g_i \in K_i$ for each i with $1 \leq i \leq n$. Since $\mathcal{C}$ is a chain, we can order the K_i so that

$$K_1 \leq K_2 \leq K_3 \leq \cdots \leq K_n.$$

Then every generator of G belongs to the subgroup K_n. This shows that *every* element of G must belong to K_n, so that K_n is not proper. But every member of $\mathcal{C}$ is a proper subgroup, so this gives a contradiction. □

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

Proof. Since G is nontrivial, the set $\mathcal{S}$ is nonempty because the trivial subgroup is a proper subgroup. The set H constructed above is also a proper subgroup and so belongs to $\mathcal{S}$. And each K_i in $\mathcal{C}$ is a subgroup of H, so H is an upper bound for $\mathcal{C}$. Since $\mathcal{C}$ was chosen arbitrarily, we have shown that every chain in the nonempty partially ordered set $\mathcal{S}$ has an upper bound. By Zorn's Lemma, $\mathcal{S}$ must have a maximal element. □

2.4.19 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 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 of A).

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

Proof. Let $r \in \mathbb{Q}$ and $k \in \mathbb{Z}$ be arbitrary, with k nonzero. Then $x = r/k$ is such that $kx = r$. Hence $\mathbb{Q}$ is divisible. □

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

Proof. Let G be any nontrivial finite abelian group, and suppose $|G| = n$. Since G is nontrivial, we may choose a nonidentity element $x \in G$. Then there is no element $y \in G$ such that $y^n = x$, for the simple reason that we must have $y^n = 1$ (since $|y|$ has to divide n). Therefore G is not divisible. □

2.4.20 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.

Proof. Suppose $A \times B$ is divisible. Let $a \in A$ and $b \in B$ be arbitrary, and let k be any nonzero integer. Then there is $(c, d) \in A \times B$ such that $(c, d)^k = (a, b)$. But $(c, d)^k = (c^k, d^k)$, so $c^k = a$ and $d^k = b$, which shows that A and B are both divisible.

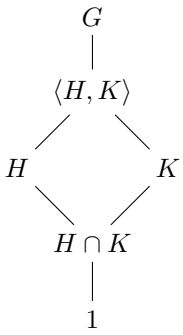
Conversely, let A and B be divisible, let $(a, b) \in A \times B$ be arbitrary, and let k be any nonzero integer. Since A is divisible, there is $c \in A$ with $c^k = a$, and since B is divisible there is $d \in B$ with $d^k = b$. Then $(c, d)^k = (a, b)$, which shows that $A \times B$ is divisible. □

2.5 The Lattice of Subgroups of a Group

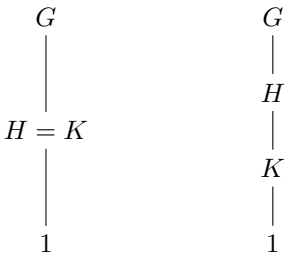
2.5.1 Exercise 1

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

Solution. In general, when H and K are distinct, with a nontrivial intersection and a join that is a proper subgroup, the sublattice might look something like the following:



In other cases, we may have $H = K$, or $H \geq K$:



There are several other possibilities, for example one of H or K could be trivial, or we could have $\langle H, K\rangle = G$, and various other options. The drawings are distinguished by the relationships between the various subgroups. □

2.5.2 Exercise 2

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

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

Solution. From the lattice given in the text, we see that the subgroups contained in $\langle sr^2, r^4\rangle$ are $\langle sr^2, r^4\rangle$, $\langle sr^6\rangle$, $\langle sr^2\rangle$, $\langle r^4\rangle$, and 1. □

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

Solution. $\langle sr^7, r^4\rangle = \langle sr^3, r^4\rangle$, so the subgroups contained in this subgroup are $\langle sr^3, r^4\rangle$, $\langle r^4\rangle$, $\langle sr^3\rangle$, $\langle sr^7\rangle$, and 1. □

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

Solution. The subgroups containing $\langle r^4\rangle$ are $\langle r^4\rangle$, $\langle sr^2, r^4\rangle$, $\langle s, r^4\rangle$, $\langle r^2\rangle$, $\langle sr^3, r^4\rangle$, $\langle sr^5, r^4\rangle$, $\langle s, r^2\rangle$, $\langle r\rangle$, $\langle sr, r^2\rangle$, and D_{16} itself. □

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

Solution. The subgroups containing $\langle s\rangle$ are $\langle s\rangle$, $\langle s, r^4\rangle$, $\langle s, r^2\rangle$, and D_{16}. □

2.5.3 Exercise 3

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

Proof. The subgroup $\langle s, r^2\rangle$ consists of the elements $\{1, s, r^2, sr^2\}$, and $V_4 = \{1, a, b, c\}$. Note that both groups are abelian and of order 4.

Define the mapping $\varphi\colon \langle s, r^2\rangle \to V_4$ by

$$\varphi(1) = 1, \quad \varphi(s) = a, \quad \varphi(r^2) = b, \quad \text{and} \quad \varphi(sr^2) = c.$$

We now directly verify that φ is a homomorphism:

$$\begin{aligned}
\varphi(s^2) &= \varphi(1) = 1 = a^2 = \varphi(s)^2,\\
\varphi(sr^2) &= c = ab = \varphi(s)\varphi(r^2),\\
\varphi(ssr^2) &= \varphi(r^2) = b = ac = \varphi(s)\varphi(sr^2),\\
\varphi(r^4) &= \varphi(1) = 1 = b^2 = \varphi(r^2)^2,\\
\varphi(r^2sr^2) &= \varphi(s) = a = bc = \varphi(r^2)\varphi(sr^2),\\
\varphi((sr^2)^2) &= \varphi(1) = 1 = c^2 = \varphi(sr^2)^2.
\end{aligned}$$

Since both groups are abelian, this is enough to show that φ is a homomorphism. But φ is clearly also a bijection, so φ is an isomorphism and $\langle s, r^2\rangle \cong V_4$. □

2.5.4 Exercise 4

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

Solution. First, we know that $D_8 = \langle s, r\rangle$. Now, looking at the cyclic subgroups in the lattice, we see that the only subgroup containing both $\langle s\rangle$ and $\langle rs\rangle$ is D_8 itself. Hence $\langle s, rs\rangle = D_8$. Similarly, the only subgroup containing $\langle s\rangle$ and $\langle r^3s\rangle$ is D_8, so $\langle s, r^3s\rangle = D_8$. Continuing in this way, we can find all the pairs that generate D_8 (noting that $\langle r\rangle = \langle r^3\rangle$):

$$\begin{aligned}
&\langle s, r\rangle, \langle s, r^3\rangle, \langle s, rs\rangle, \langle s, r^3s\rangle, \langle r^2s, r\rangle, \langle r^2s, r^3\rangle,\\
&\qquad\qquad \langle r^2s, rs\rangle, \langle r^2s, r^3s\rangle, \langle r, rs\rangle, \langle r^3, rs\rangle, \langle r^3, r^3s\rangle, \langle r, r^3s\rangle.
\end{aligned}$$

No other pairing can generate all of D_8. □

2.5.5 Exercise 5

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

Solution. Note that $\langle r \rangle = \langle r^3 \rangle = \langle r^5 \rangle = \langle r^7 \rangle$. We now proceed as in the previous problem, pairing $\langle s \rangle$ with other cyclic subgroups such that all of D_{16} is the smallest group containing both subgroups. We find the following generating pairs:

$$\langle s, r \rangle, \langle s, r^3 \rangle, \langle s, r^5 \rangle, \langle s, r^7 \rangle, \langle s, sr^3 \rangle, \langle s, sr^7 \rangle, \langle s, sr^5 \rangle, \langle s, sr \rangle. \qquad \square$$

2.5.6 Exercise 6

Use the given lattices to help find the centralizers of every element in the following groups:

(a) D_8

Solution. Since s commutes with r^2, we see from the lattice that $C_{D_8}(s) = \langle s, r^2 \rangle$ (this centralizer cannot be all of D_8 since s does not commute with r). r^2 commutes with everything (it is in the center of D_8), so $C_{D_8}(r^2) = D_8$. By similar reasoning, we find the following centralizers:

$$\begin{aligned} C_{D_8}(1) &= D_8, \\ C_{D_8}(r) &= \langle r \rangle, \\ C_{D_8}(r^2) &= D_8, \\ C_{D_8}(r^3) &= \langle r \rangle, \\ C_{D_8}(s) &= \langle s, r^2 \rangle, \\ C_{D_8}(rs) &= \langle rs, r^2 \rangle, \\ C_{D_8}(r^2 s) &= \langle s, r^2 \rangle, \\ C_{D_8}(r^3 s) &= \langle rs, r^2 \rangle. \end{aligned}$$ $\square$

(b) Q_8

Solution. We know that -1 commutes with every element, but i, j, and k do not commute with each other. Therefore

$$\begin{aligned} C_{Q_8}(1) &= Q_8, \\ C_{Q_8}(-1) &= Q_8, \\ C_{Q_8}(i) = C_{Q_8}(-i) &= \langle i \rangle, \\ C_{Q_8}(j) = C_{Q_8}(-j) &= \langle j \rangle, \\ C_{Q_8}(k) = C_{Q_8}(-k) &= \langle k \rangle. \end{aligned}$$ $\square$

(c) S_3

Solution. From the lattice we see that every nontrivial subgroup is maximal, so the centralizer of each cycle is either the subgroup generated by

that cycle, or else all of S_3. But none of $(1\,2)$, $(1\,3)$, $(2\,3)$, and $(1\,2\,3)$ commute with each other, so none of the centralizers can be all of S_3, aside from $C_{S_3}(1)$. This gives

$$\begin{aligned} C_{S_3}(1) &= S_3, \\ C_{S_3}(1\,2) &= \langle (1\,2) \rangle, \\ C_{S_3}(1\,3) &= \langle (1\,3) \rangle, \\ C_{S_3}(2\,3) &= \langle (2\,3) \rangle, \\ C_{S_3}(1\,2\,3) = C_{S_3}(1\,3\,2) &= \langle (1\,2\,3) \rangle. \end{aligned}$$ □

(d) D_{16}

Solution. We use similar reasoning as we did for D_8.

$$\begin{aligned} C_{D_{16}}(1) &= D_{16}, \\ C_{D_{16}}(r) = C_{D_{16}}(r^2) = C_{D_{16}}(r^3) &= \langle r \rangle, \\ C_{D_{16}}(r^5) = C_{D_{16}}(r^6) = C_{D_{16}}(r^7) &= \langle r \rangle, \\ C_{D_{16}}(r^4) &= D_{16}, \\ C_{D_{16}}(s) = C_{D_{16}}(sr^4) &= \langle s, r^4 \rangle, \\ C_{D_{16}}(sr) = C_{D_{16}}(sr^5) &= \langle sr^5, r^4 \rangle, \\ C_{D_{16}}(sr^2) = C_{D_{16}}(sr^6) &= \langle sr^2, r^4 \rangle, \\ C_{D_{16}}(sr^3) = C_{D_{16}}(sr^7) &= \langle sr^3, r^4 \rangle. \end{aligned}$$ □

2.5.7 Exercise 7

Find the center of D_{16}.

Solution. We already found in Exercise 2.2.7 that $Z(D_{2n}) = 1$ if n is odd and $Z(D_{2n}) = \{1, r^k\}$ if $n = 2k$. Therefore $Z(D_{16}) = \{1, r^4\}$. Alternatively, we could use the results from the previous problem, where we saw that 1 and r^4 were the only elements with centralizers equal to all of D_{16}. □

2.5.8 Exercise 8

In each of the following groups find the normalizer of each subgroup:

(a) S_3

Solution. S_3 has six subgroups. From the lattice, we see that each nontrivial proper subgroup H of S_3 is maximal, so we either have $N_{S_3}(H) = H$ or $N_{S_3}(H) = S_3$.

For $H = \langle (1\,2) \rangle$, since

$$(1\,3)(1\,2)(1\,3) = (2\,3) \notin \langle (1\,2) \rangle,$$

we see that $(1\,3)H(1\,3)^{-1} \neq H$, so $N_{S_3}(H) = H$. The same is true for the other subgroups generated by 2-cycles. So,

$$N_{S_3}(\langle (1\,2) \rangle) = \langle (1\,2) \rangle, \quad N_{S_3}(\langle (1\,3) \rangle) = \langle (1\,3) \rangle, \quad \text{and} \quad N_{S_3}(\langle (2\,3) \rangle) = \langle (2\,3) \rangle.$$

For $H = \langle (1\,2\,3) \rangle = \{1, (1\,2\,3), (1\,3\,2)\}$, we have

$$(1\,2)(1\,2\,3)(1\,2) = (1\,3\,2) \in H,$$
$$(1\,2)(1\,3\,2)(1\,2) = (1\,2\,3) \in H,$$

so $(1\,2)$ is in the normalizer of H. Therefore

$$N_{S_3}(\langle 1\,2\,3 \rangle) = N_{S_3}(1) = N_{S_3}(S_3) = S_3. \qquad \square$$

(b) Q_8

Solution. Since 1 and -1 are in the center of Q_8, we have

$$N_{Q_8}(1) = N_{Q_8}(-1) = N_{Q_8}(Q_8) = Q_8.$$

The other subgroups are maximal, so each normalizer is either the subgroup itself or else all of Q_8. Since

$$j(i)j^{-1} = (-k)(-j) = kj = -i \in \langle i \rangle,$$

and

$$j(-i)j^{-1} = k(-j) = -kj = i \in \langle i \rangle,$$

we see that $j \in N_{Q_8}(\langle i \rangle)$. Therefore $N_{Q_8}(\langle i \rangle) = Q_8$. By an entirely similar argument, we see that the same is true for $\langle j \rangle$ and $\langle k \rangle$. So

$$N_{Q_8}(\langle i \rangle) = N_{Q_8}(\langle j \rangle) = N_{Q_8}(\langle k \rangle) = Q_8. \qquad \square$$

2.5.9 Exercise 9

Draw the lattices of subgroups of the following groups:

(a) $\mathbb{Z}/16\mathbb{Z}$

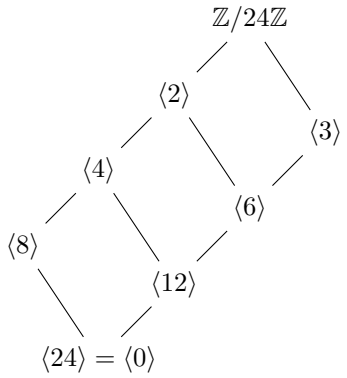
Solution.

$$\begin{array}{c} \mathbb{Z}/16\mathbb{Z} \\ | \\ \langle 2 \rangle \\ | \\ \langle 4 \rangle \\ | \\ \langle 8 \rangle \\ | \\ \langle 16 \rangle = \langle 0 \rangle \end{array}$$

$\square$

(b) $\mathbb{Z}/24\mathbb{Z}$

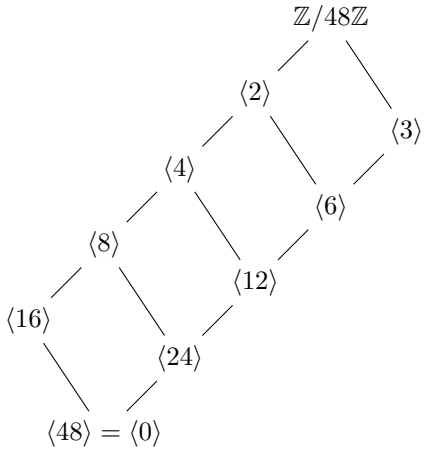
Solution.



□

(c) $\mathbb{Z}/48\mathbb{Z}$

Solution.



□

2.5.10 Exercise 10

Classify groups of order 4 by proving that if $|G| = 4$ then $G \cong Z_4$ or $G \cong V_4$.

Proof. Let $G = \{1, a, b, c\}$. If G is cyclic, then certainly $G \cong Z_4$ since all cyclic groups of the same order are isomorphic. So assume that G is not cyclic, so that no element has order 4. Since the order of each element must divide the order of the group, it follows that a, b, c each have order 2.

Now consider the product ab. If $ab = 1$, then multiplying by a on the left gives $b = a$, so a and b are not distinct, which is a contradiction. If $ab = a$, then multiplying by a gives $b = 1$, another contradiction. For the same reason we cannot have $ab = b$. So the only possibility is $ab = c$.

Using exactly the same argument, we can see that $ba = c$, $ac = ca = b$, and $bc = cb = a$. Since G has the same multiplication table as V_4, it follows that $G \cong V_4$. Indeed, any identity-preserving bijection between them is an isomorphism. □

2.5.11 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: $\langle \tau, \sigma^2 \rangle \cong D_8$, $\langle \sigma \rangle \cong Z_8$ and $\langle \sigma^2, \sigma\tau \rangle \cong Q_8$ and every proper subgroup is contained in one of these three subgroups. Fill in the missing subgroups in the provided lattice of all subgroups of the quasidihedral group, exhibiting each subgroup with at most two generators.

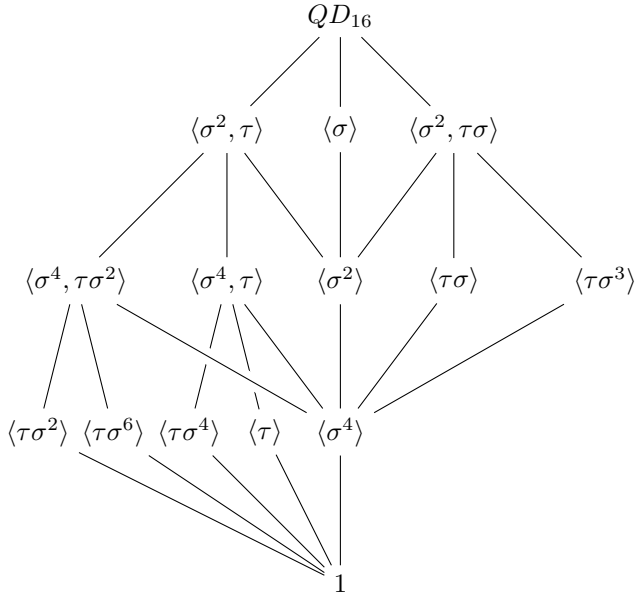
Solution. Certainly $\langle \sigma^2 \rangle$ is between $\langle \sigma \rangle$ and $\langle \sigma^4 \rangle$. By taking powers of the other elements, we see that the other missing cyclic subgroups are

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

and

$$\langle \tau\sigma^6 \rangle = \{1, \tau\sigma^6\}.$$

$\langle \sigma^4, \tau \rangle$ must contain $\langle \tau\sigma^4 \rangle$, and we see that $\langle \tau\sigma^6 \rangle$ must be the sibling of $\langle \tau\sigma^2 \rangle$, whose containing subgroup would then be $\langle \sigma^4, \tau\sigma^2 \rangle$. The remaining cyclic subgroups are contained in $\langle \sigma^2, \tau\sigma \rangle$. This gives the following lattice.



□

2.5.12 Exercise 12

The group

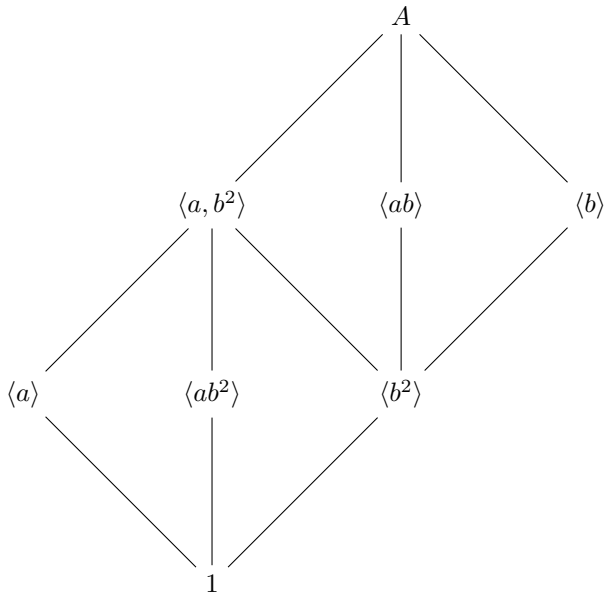
$$A = Z_2 \times Z_4 = \langle a, b \mid a^2 = b^4 = 1,\ ab = ba \rangle$$

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. Writing out the elements of A (in terms of a and b) gives

$$A = \{1, a, b, b^2, b^3, ab, ab^2, ab^3\}.$$

There are three elements with order 2, namely a, b^2, and ab^2. Since $\langle a, b^2 \rangle \cong V_4$, we see that $\langle a \rangle$, $\langle b^2 \rangle$, and $\langle ab^2 \rangle$ must be directly contained in $\langle a, b^2 \rangle$. From this and the other given information, we form the following lattice.



□

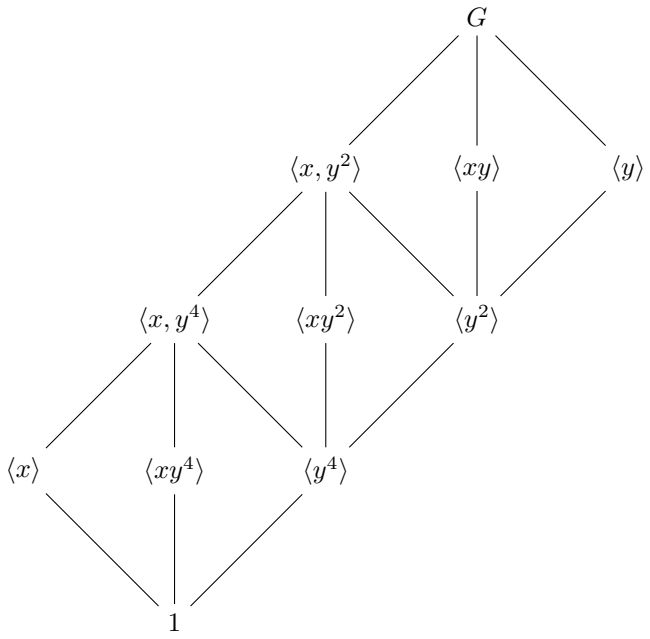
2.5.13 Exercise 13

The group

$$G = Z_2 \times Z_8 = \langle x, y \mid x^2 = y^8 = 1,\ xy = yx \rangle$$

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.

Solution. Since $\langle x, y^2 \rangle \cong Z_2 \times Z_4$, we see that the lattice of G contains the lattice from the previous exercise within its structure, with a replaced by x and b replaced by y^2. Adding in the maximal subgroups $\langle y \rangle$ and $\langle xy \rangle$ produces the following lattice.



□

2.5.14 Exercise 14

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

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

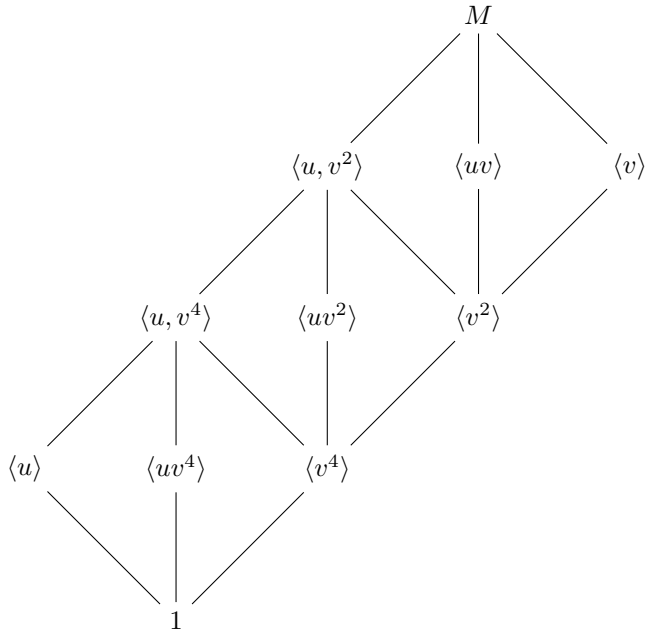
(sometimes called the *modular* group of order 16). It has three subgroups of order 8: $\langle u, v^2 \rangle$, $\langle v \rangle$ and $\langle uv \rangle$ and every proper subgroup is contained in one of these three. Prove that $\langle u, v^2 \rangle \cong Z_2 \times Z_4$, $\langle v \rangle \cong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

Solution. We will use the presentation for $Z_2 \times Z_4$ given in Exercise 2.5.12. Since $u^2 = (v^2)^4 = 1$ and $u(v^2) = (v^2)u$, it follows that the mapping $\varphi\colon Z_2 \times Z_4 \to \langle u, v^2 \rangle$ defined by

$$\varphi(a) = u \quad \text{and} \quad \varphi(b) = v^2$$

extends to a homomorphism. φ is surjective by construction and hence bijective since we know that both groups $Z_2 \times Z_4$ and $\langle u, v^2 \rangle$ have order 8. Therefore $\langle u, v^2 \rangle \cong Z_2 \times Z_4$.

Since we know $|\langle v \rangle| = |\langle uv \rangle| = 8$, we automatically know that both subgroups are isomorphic to Z_8, since all cyclic groups of the same order are isomorphic. We see that the subgroups of M share the same relationships as the subgroups of $Z_2 \times Z_8$, so they have the same lattice, with x replaced by u and y replaced by v:



Finally, we note that, despite having the same lattice, M is not isomorphic to $Z_2 \times Z_8$ since the latter is abelian and M is not ($uv \neq vu$). □

2.5.15 Exercise 15

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

Solution. Since $|r| = 8$, we see that $\langle r \rangle \cong Z_8$.

Next, consider the subgroup $H = \langle s, r^2 \rangle$ and observe that

$$(r^2)^4 = s^2 = 1 \quad \text{and} \quad (r^2)s = sr^6 = s(r^2)^{-1}.$$

Since s and r^2 in D_{16} satisfy the same relations as s and r do in D_8, the map $\varphi\colon D_8 \to H$ given by

$$\varphi(r) = r^2 \quad \text{and} \quad \varphi(s) = s$$

extends to a surjective homomorphism. And it is easy to see that H consists of only eight elements, namely elements of the form $s^i r^{2j}$ where $i \in \{0, 1\}$ and $j \in \{0, 1, 2, 3\}$. Therefore φ must be a bijection, and we have $\langle s, r^2 \rangle \cong D_8$.

Now consider the subgroup $K = \langle sr, r^2 \rangle$. We have

$$(r^2)^4 = (sr)^2 = 1 \quad \text{and} \quad (r^2)(sr) = sr^7 = (sr)(r^2)^{-1}.$$

So the map $\psi\colon D_8 \to K$ given by

$$\varphi(r) = r^2 \quad \text{and} \quad \varphi(s) = sr$$

extends to a surjective homomorphism, which must be injective as well since K has 8 elements. Therefore $\langle sr, r^2 \rangle \cong D_8$. □

2.5.16 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 $\langle \tau, \sigma^2 \rangle$.

Proof. Every element of order 2 generates a cyclic subgroup having order 2. From the lattice of QD_{16} (Exercise 2.5.11) we see that every cyclic subgroup of QD_{16} is contained in $\langle \sigma^2, \tau \rangle$ except for $\langle \tau\sigma \rangle$ and $\langle \tau\sigma^3 \rangle$. But neither $\tau\sigma$ nor $\tau\sigma^3$ has order 2 (they both have order 4), so we see that every element of order 2 is indeed contained in $\langle \sigma^2, \tau \rangle$. □

2.5.17 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.

Proof. We know from Exercise 2.5.10 that every group of order 4 is isomorphic to either Z_4 or V_4. From the lattice we constructed in Exercise 2.5.14, we see that $\langle u, v^4 \rangle$ contains only the four elements 1, u, v^4, and uv^4. Since each of these (aside from 1) has order 2, we know that $\langle u, v^4 \rangle$ is not cyclic and so cannot be isomorphic to Z_4. Therefore $\langle u, v^4 \rangle \cong V_4$. □

2.5.18 Exercise 18

Use the lattice to help find the centralizer of every element of QD_{16}.

Solution. Since $\sigma^4\tau = \tau\sigma^{12} = \tau\sigma^4$, we see that σ^4 commutes with τ and hence belongs to the center of the group (since it commutes with each generator).

From the lattice, we see that the centralizer of τ is either equal to $\langle \sigma^4, \tau \rangle$, or to $\langle \sigma^2, \tau \rangle$, or to all of QD_{16}. But we can rule out the latter two cases, since τ does not commute with σ^2:

$$\sigma^2\tau = \tau\sigma^6.$$

A similar case can be made for the centralizer of $\tau\sigma^4$.

For $\tau\sigma^2$ and $\tau\sigma^6$ we see that both commute with σ^4 and $\tau\sigma^2$, but neither commutes with σ^2, so their centralizer must be $\langle \sigma^4, \tau\sigma^2 \rangle$.

$\tau\sigma$ and $\tau\sigma^3$ do not commute with σ^2, so their respective centralizers are just the cyclic subgroups that they generate.

Lastly, the powers of σ all commute with each other. Putting all this information together, we get

$$\begin{aligned}
C_{QD_{16}}(1) = C_{QD_{16}}(\sigma^4) &= QD_{16}, \\
C_{QD_{16}}(\sigma) = C_{QD_{16}}(\sigma^2) = C_{QD_{16}}(\sigma^3) &= \langle \sigma \rangle, \\
C_{QD_{16}}(\sigma^5) = C_{QD_{16}}(\sigma^6) = C_{QD_{16}}(\sigma^7) &= \langle \sigma \rangle, \\
C_{QD_{16}}(\tau) = C_{QD_{16}}(\tau\sigma^4) &= \langle \sigma^4, \tau \rangle, \\
C_{QD_{16}}(\tau\sigma^2) = C_{QD_{16}}(\tau\sigma^6) &= \langle \sigma^4, \tau\sigma^2 \rangle, \\
C_{QD_{16}}(\tau\sigma) = C_{QD_{16}}(\tau\sigma^5) &= \langle \tau\sigma \rangle, \\
C_{QD_{16}}(\tau\sigma^3) = C_{QD_{16}}(\tau\sigma^7) &= \langle \tau\sigma^3 \rangle.
\end{aligned}$$

□

2.5.19 Exercise 19

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

Solution. Let $H = \langle s, r^4\rangle$. From the lattice, we see that the normalizer of H must be either H itself, or $\langle s, r^2\rangle$, or D_{16}. Since

$$r^2(r^4)(r^2)^{-1} = r^2r^4r^6 = r^4 \in H,$$
$$r^2s(r^2)^{-1} = r^2sr^6 = sr^4 \in H,$$

and

$$r^2(sr^4)(r^2)^{-1} = r^2sr^2 = s \in H,$$

we see that $r^2H(r^2)^{-1} = H$ so $\langle s, r^2\rangle \leq N_{D_{16}}(H)$. However, since

$$rsr^7 = sr^7r^7 = sr^6 \notin H,$$

we see that $rHr^{-1} \neq H$ so the normalizer of H cannot be all of D_{16}. Therefore $N_{D_{16}}(H) = \langle s, r^2\rangle$. □

2.5.20 Exercise 20

Use the lattice of subgroups of QD_{16} to help find the normalizers

(a) $N_{QD_{16}}(\langle\tau\sigma\rangle)$

Solution. Let $H = \langle\tau\sigma\rangle$. From the lattice (Exercise 2.5.11) we see that there are only three possibilities for the normalizer of H: it is either H itself, or $\langle\sigma^2, \tau\sigma\rangle$ or else all of QD_{16}. Since $H = \{1, \tau\sigma, \sigma^4, \tau\sigma^5\}$, we can compute the elements of $\sigma^2H(\sigma^2)^{-1}$ as follows:

$$\sigma^2(\tau\sigma)\sigma^6 = \tau\sigma^6\sigma^7 = \tau\sigma^5,$$
$$\sigma^2\sigma^4\sigma^6 = \sigma^4,$$
$$\sigma^2(\tau\sigma^5)\sigma^6 = \sigma^2\tau\sigma^3 = \tau\sigma.$$

So $\sigma^2H(\sigma^2)^{-1} = H$ and therefore σ^2 is in the normalizer of H. But σ is not in the normalizer, since

$$\sigma(\tau\sigma)\sigma^7 = \sigma\tau = \tau\sigma^3 \notin H.$$

Thus the only possibility is $N_{QD_{16}}(H) = \langle\sigma^2, \tau\sigma\rangle$. □

(b) $N_{QD_{16}}(\langle\tau, \sigma^4\rangle)$

Solution. Let $K = \langle\tau, \sigma^4\rangle$. Again there are three possibilities. $K = \{1, \tau, \sigma^4, \tau\sigma^4\}$, so as before, we compute the elements of $\sigma^2K(\sigma^2)^{-1}$:

$$\sigma^2\tau\sigma^6 = \tau\sigma^{12} = \tau\sigma^4,$$
$$\sigma^2\sigma^4\sigma^6 = \sigma^4,$$
$$\sigma^2(\tau\sigma^4)\sigma^6 = \sigma^2\tau\sigma^2 = \tau.$$

So $\sigma^2 K(\sigma^2)^{-1} = K$ and we must have $\langle \tau, \sigma^2 \rangle \leq N_{QD_{16}}(K)$. And since

$$\sigma\tau\sigma^7 = \tau\sigma^2 \notin K,$$

we see that the normalizer cannot be all of QD_{16}. Therefore $N_{QD_{16}}(K) = \langle \tau, \sigma^2 \rangle$. □

Chapter 3

Quotient Groups and Homomorphisms

3.1 Definitions and Examples

Let G and H be groups.

3.1.1 Exercise 1

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

Proof. Note that $\varphi(1) = 1 \in E$ so $\varphi^{-1}(E)$ is nonempty. Suppose $a, b \in \varphi^{-1}(E)$, so that $\varphi(a) = x$ and $\varphi(b) = y$ for some $x, y \in E$. Then, since φ is a homomorphism, we have

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

which shows that $ab^{-1} \in \varphi^{-1}(E)$. By the subgroup criterion, this shows that $\varphi^{-1}(E) \leq G$.

Now suppose that E is a normal subgroup of H. Let $g \in G$ and $n \in \varphi^{-1}(E)$. Then $\varphi(g) = h$ for some $h \in H$ and $\varphi(n) = x$ for some $x \in E$. We have

$$\begin{aligned}\varphi(gng^{-1}) &= \varphi(g)\varphi(n)\varphi(g)^{-1} \\ &= hxh^{-1}.\end{aligned}$$

But $hxh^{-1} \in E$ since $E \trianglelefteq H$, so $gng^{-1} \in \varphi^{-1}(E)$. The choice of g and n were arbitrary, so this shows that $\varphi^{-1}(E) \trianglelefteq G$.

Lastly, if we let E be the trivial subgroup of H, then the above shows that $\ker\varphi = \varphi^{-1}(E) \trianglelefteq G$ since the trivial subgroup is always normal. □

3.1.2 Exercise 2

Let $\varphi\colon G \to H$ 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 $uv = w$.

Proof. Let $v = u^{-1}w$. We want to show that $v \in Y$, or $\varphi(v) = b$. Since φ is a homomorphism and since $Z = \varphi^{-1}(ab)$, we have

$$\begin{aligned}\varphi(v) &= \varphi(u^{-1}w)\\ &= \varphi(u)^{-1}\varphi(w)\\ &= a^{-1}(ab)\\ &= (a^{-1}a)b\\ &= b.\end{aligned}$$

So $v \in Y$ as required. □

3.1.3 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. Let $a_1B, a_2B \in A/B$, where $a_1, a_2 \in A$. Since A is abelian, we have

$$a_1Ba_2B = (a_1a_2)B = (a_2a_1)B = a_2Ba_1B.$$

Therefore A/B is abelian.

For the second part of the problem, let G be the non-abelian dihedral group D_8 and let N the proper normal subgroup $\langle r^2\rangle$. In the text it was shown that $G/N \cong V_4$, the Klein four-group, which is abelian. Therefore G/N is abelian even though G is not. □

3.1.4 Exercise 4

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

Proof. First, if $\alpha = 0$, then $(gN)^0 = 1N = g^0N$, so the statement is true in this case. We also know by Proposition 5 that $(gN)^{-1} = g^{-1}N$. So it will suffice to prove the statement only for positive α, which we will do by induction on α.

The case where $\alpha = 1$ is trivial. For the inductive step, suppose that the statement $(gN)^k = g^kN$ holds for some particular $k \geq 1$. Then

$$\begin{aligned}(gN)^{k+1} &= (gN)^k gN\\ &= g^kNgN\\ &= (g^kg)N\\ &= g^{k+1}N.\end{aligned}$$

By induction, we conclude that $(gN)^\alpha = g^\alpha N$ for all $\alpha \geq 1$, so the proof is complete. □

3.1.5 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. Fix an element gN in G/N. First, if possible, let n be the smallest positive integer such that $g^n \in N$. Then $g^n N = 1N$. So, by the previous exercise, we know that $(gN)^n = 1N$. This shows that $|gN| \leq n$. On the other hand, if m is any positive integer with $(gN)^m = 1N$ then, using the previous exercise again, $g^m N = 1N$ so that $g^m \in N$. Since n is the smallest positive integer with $g^n \in N$, this shows that $|gN| \geq n$, which completes the proof for the case of finite order.

Next, suppose that there is no such n. Then for each positive integer k, $g^k \notin N$. If gN were to have finite order, say $(gN)^m = 1N$, then the previous exercise would show that $g^m \in N$, giving a contradiction. This shows that gN has infinite order, which completes the proof.

Lastly, for the example, consider $G = Z_4$, the cyclic group of order 4. Let x be a generator for G and take $N = \langle x^2 \rangle = \{1, x^2\}$. Now the element x^2 has order 2 in G, but $x^2 N = 1N$ has order 1 in G/N. □

3.1.6 Exercise 6

Define $\varphi\colon \mathbb{R}^\times \to \{\pm 1\}$ 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. The fiber above 1 is the positive reals, and the fiber above -1 is the negative reals.

Let $x, y \in \mathbb{R}^\times$ be arbitrary. Then

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

so φ is a homomorphism. □

3.1.7 Exercise 7

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

Solution. For any $(x_1, y_1), (x_2, y_2) \in \mathbb{R}^2$, we have

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

so π is a homomorphism. And for any $x \in \mathbb{R}$, we have $\pi((x, 0)) = x + 0 = x$, so π is also surjective.

$\ker \pi$ is simply the diagonal line whose equation is $x + y = 0$. And for $a \in \mathbb{R}$, the fiber over a is the line with equation $x + y = a$, which is just a translate of the kernel. □

3.1.8 Exercise 8

Let $\varphi\colon \mathbb{R}^\times \to \mathbb{R}^\times$ 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. For any $x, y \in \mathbb{R}^\times$ we have

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

and φ is a homomorphism. Its image is $\mathbb{R}^+$, the positive reals.

The kernel of φ is the set $\{-1, 1\}$, since $\varphi(\pm 1) = 1$ and no other real number has an absolute value of 1. Likewise, the fiber over the real number a is $\{-a, a\}$. □

3.1.9 Exercise 9

Define $\varphi\colon \mathbb{C}^\times \to \mathbb{R}^\times$ 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. Let $a + bi$ and $c + di$ be any members of $\mathbb{C}^\times$. Then

$$\begin{aligned}
\varphi((a + bi)(c + di)) &= \varphi((ac - bd) + (ad + bc)i) \\
&= (ac - bd)^2 + (ad + bc)^2 \\
&= a^2c^2 - 2abcd + b^2d^2 + a^2d^2 + 2abcd + b^2c^2 \\
&= a^2(c^2 + d^2) + b^2(c^2 + d^2) \\
&= (a^2 + b^2)(c^2 + d^2) \\
&= \varphi(a + bi)\varphi(c + di),
\end{aligned}$$

and φ is a homomorphism. Let $a + bi \in \mathbb{C}^\times$. Since a and b cannot both be zero, $a^2 + b^2 > 0$. So $\operatorname{im}\varphi \subseteq \mathbb{R}^+$. But for any $a \in \mathbb{R}^+$, we have $\varphi(\sqrt{a} + 0i) = a$ and we see that $\operatorname{im}\varphi = \mathbb{R}^+$.

The kernel of φ is the set

$$\ker\varphi = \{a + bi \in \mathbb{C}^\times \mid a^2 + b^2 = 1\}.$$

This is a circle of radius 1 centered at the origin in the complex plane. For $a \in \mathbb{R}^+$, the fiber over a is the circle of radius $\sqrt{a}$. □

3.1.10 Exercise 10

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

Solution. To show that φ is well defined we need to show that any choice of representative for a particular congruence class in $\mathbb{Z}/8\mathbb{Z}$ will produce the same

congruence class in $\mathbb{Z}/4\mathbb{Z}$ under φ. Suppose then that $\bar{a} = \bar{b}$, where $\bar{a}, \bar{b} \in \mathbb{Z}/8\mathbb{Z}$. Then for some integer k, $a = b + 8k$ and we have

$$\begin{aligned}\varphi(\bar{a}) &= \varphi(\overline{b+8k}) \\ &= \overline{b+8k} \\ &= \overline{b+4(2k)} \\ &= \bar{b} \\ &= \varphi(\bar{b})\end{aligned}$$

and φ is well defined. It is also a homomorphism since

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

And it is clearly surjective.

The fibers of φ are

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

and $\ker\varphi = \varphi^{-1}(\bar{0}) = \{\bar{0}, \bar{4}\}$. □

3.1.11 Exercise 11

Let F be a field and let

$$G = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \;\middle|\; a, b, c \in F, \;\; ac \neq 0 \right\} \leq GL_2(F).$$

(a) Prove that the map

$$\varphi\colon \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mapsto a$$

is a surjective homomorphism from G onto $F^\times$. Describe the fibers and kernel of φ.

Solution. First, for any $a \in F^\times$, we have

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

so φ is surjective. And for any $a, b, c, d, e, f \in F$ with $ac \neq 0$ and $df \neq 0$, we have

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

so φ is a homomorphism.

For each $a \in F^\times$, the fiber over a is given by

$$\varphi^{-1}(a) = \left\{ \begin{pmatrix} a & x \\ 0 & y \end{pmatrix} \;\middle|\; x, y \in F,\ \ y \neq 0 \right\},$$

with the kernel being the fiber above 1. □

(b) Prove that the map

$$\psi\colon \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mapsto (a, c)$$

is a surjective homomorphism from G onto $F^\times \times F^\times$. Describe the fibers and kernel of ψ.

Solution. The proof is entirely similar to the proof for φ in the previous part of the problem and is omitted here. The fiber over (a, c) is

$$\psi^{-1}((a, c)) = \left\{ \begin{pmatrix} a & x \\ 0 & c \end{pmatrix} \;\middle|\; x \in F \right\},$$

with $\ker \psi = \psi^{-1}((1, 1))$. □

(c) Let

$$H = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \;\middle|\; b \in F \right\}.$$

Prove that H is isomorphic to the additive group F.

Proof. Define $\rho\colon H \to F$ by

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

Then ρ is a bijection since it has the obvious two-sided inverse $\rho^{-1}\colon F \to H$ given by

$$\rho^{-1}(b) = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix},$$

and it is a homomorphism since

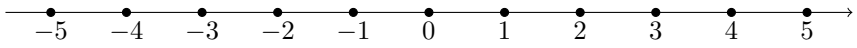
$$\begin{aligned} \rho\left(\begin{pmatrix} 1 & b_1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & b_2 \\ 0 & 1 \end{pmatrix} \right) &= \rho\left(\begin{pmatrix} 1 & b_1 + b_2 \\ 0 & 1 \end{pmatrix} \right) \\ &= b_1 + b_2 \\ &= \rho\left(\begin{pmatrix} 1 & b_1 \\ 0 & 1 \end{pmatrix} \right) + \rho\left(\begin{pmatrix} 1 & b_2 \\ 0 & 1 \end{pmatrix} \right). \end{aligned}$$

Therefore ρ is an isomorphism and $H \cong F$. □

3.1.12 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 $\varphi\colon G \to H$ be the homomorphism $\varphi\colon r \mapsto e^{2\pi i r}$. 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. The kernel of φ is simply $\mathbb{Z}$, since $e^{2\pi i r} = 1$ if and only if r is an integer:



The specified fibers are

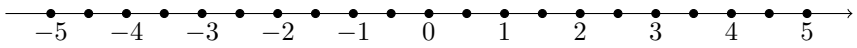
$$\begin{aligned}
\varphi^{-1}(-1) &= \frac{1}{2} + \mathbb{Z} = \left\{ k + \frac{1}{2} \;\middle|\; k \in \mathbb{Z} \right\}, \\
\varphi^{-1}(i) &= \frac{1}{4} + \mathbb{Z} = \left\{ k + \frac{1}{4} \;\middle|\; k \in \mathbb{Z} \right\}, \\
\varphi^{-1}(e^{4\pi i/3}) &= \frac{2}{3} + \mathbb{Z} = \left\{ k + \frac{2}{3} \;\middle|\; k \in \mathbb{Z} \right\}.
\end{aligned}$$

□

3.1.13 Exercise 13

Repeat the preceding exercise with the map φ replaced by the map $\varphi\colon r \mapsto e^{4\pi i r}$.

Solution. In this case the kernel is $\frac{1}{2}\mathbb{Z}$:



The fibers are

$$\begin{aligned}
\varphi^{-1}(-1) &= \frac{1}{4} + \frac{1}{2}\mathbb{Z} = \left\{ \frac{2k+1}{4} \;\middle|\; k \in \mathbb{Z} \right\}, \\
\varphi^{-1}(i) &= \frac{1}{8} + \frac{1}{2}\mathbb{Z} = \left\{ \frac{4k+1}{8} \;\middle|\; k \in \mathbb{Z} \right\}, \\
\varphi^{-1}(e^{4\pi i/3}) &= \frac{1}{3} + \frac{1}{2}\mathbb{Z} = \left\{ \frac{3k+2}{6} \;\middle|\; k \in \mathbb{Z} \right\}.
\end{aligned}$$

□

3.1.14 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 $0 \le q < 1$.

Proof. Let $t \in \mathbb{Q}$ be arbitrary. Write $t = m/n$ in lowest terms. We may use the division algorithm to find unique integers q and r with $0 \le r < n$ such that $m = nq + r$. Then $t = q + r/n$, where $0 \le r/n < 1$. Then we have

$$t + \mathbb{Z} = \{t + k \mid k \in \mathbb{Z}\} = \left\{ \frac{r}{n} + (k+q) \;\middle|\; k \in \mathbb{Z} \right\} = \frac{r}{n} + \mathbb{Z}.$$

From the uniqueness of q and r, it follows that r/n is the only representative of $t + \mathbb{Z}$ that is in the range $[0, 1)$. □

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

Proof. Again, let $t \in \mathbb{Q}$ be arbitrary, with $t = m/n$ for integers m and n, with $n > 0$. Then

$$n(t + \mathbb{Z}) = nt + \mathbb{Z} = m + \mathbb{Z} = 0 + \mathbb{Z},$$

so $t + \mathbb{Z}$ has finite order (note that the first equality follows from Exercise 3.1.4).

Given any positive integer k, the coset $1/k + \mathbb{Z}$ has order k. Since k can be made arbitrarily large, we see that $\mathbb{Q}/\mathbb{Z}$ contains elements of arbitrarily large order. □

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

Proof. We need to show that the only elements in $\mathbb{R}/\mathbb{Z}$ having finite order belong to $\mathbb{Q}/\mathbb{Z}$. So suppose r is an irrational representative of a coset having finite order n. Then

$$nr + \mathbb{Z} = n(r + \mathbb{Z}) = 0 + \mathbb{Z}.$$

This implies that $nr \in \mathbb{Z}$, say $m = nr$. Then $r = m/n$ and $r \in \mathbb{Q}$, contradicting our choice of r. Therefore r cannot have finite order. So $\mathbb{Q}/\mathbb{Z}$ is indeed the torsion subgroup of $\mathbb{R}/\mathbb{Z}$. □

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

Proof. Let S^1 be the unit circle in the complex plane and let G be the multiplicative group of the roots of unity. From Exercise 3.1.12 we know that $\mathbb{R}/\mathbb{Z} \cong S^1$, as we can exhibit the explicit isomorphism φ by

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

Now consider the torsion subgroup of S^1. By definition, $z \in S^1$ has finite order, say n, if and only if $z^n = 1$, i.e. if and only if $z \in G$. So we see that G is actually the torsion subgroup of S^1.

Since $\mathbb{R}/\mathbb{Z}$ is isomorphic to S^1, it follows that their torsion subgroups are also isomorphic. Hence $\mathbb{Q}/\mathbb{Z} \cong G$. □

3.1.15 Exercise 15

Prove that a quotient of a divisible abelian group by any proper subgroup is also divisible. Deduce that $\mathbb{Q}/\mathbb{Z}$ is divisible.

Proof. Let G be a divisible abelian group and let $H < G$ be a proper subgroup. Let $g \in G$ be arbitrary and let $k \neq 0$ be an integer. Since G is divisible, there is an element $x \in G$ such that $x^k = g$. Then, by Exercise 3.1.4, we know that

$$(xH)^k = x^k H = gH,$$

which shows that G/H is also divisible.

We have shown in Exercise 2.4.19 that $\mathbb{Q}$ is divisible. Since $\mathbb{Z}$ is a proper subgroup, we must have that $\mathbb{Q}/\mathbb{Z}$ is divisible as well. □

3.1.16 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 $\overline{G} = \langle \bar{x}, \bar{y}\rangle$. Prove more generally that if $G = \langle S\rangle$ for any subset S of G, then $\overline{G} = \langle \overline{S}\rangle$.

Proof. We will prove the general case, since the arguments are similar. Suppose $G = \langle S\rangle$. If S is empty then G and N are trivial and we vacuously have $\overline{G} = \langle \overline{S}\rangle$. So let S be nonempty. Then for any $g \in G$, we may write

$$g = s_1 s_2 \cdots s_k, \quad \text{where } s_i \in S \text{ for } 1 \leq i \leq k.$$

Let $\overline{S}$ be cosets of the form sN, where $s \in S$. Then gN may be written as

$$\begin{aligned} gN &= (s_1 s_2 \cdots s_k)N \\ &= (s_1 N)(s_2 N)\cdots(s_k N). \end{aligned}$$

This shows that every coset in $\overline{G}$ can be written as a product of cosets in $\overline{S}$. Therefore $\overline{G} = \langle \overline{S}\rangle$. □

3.1.17 Exercise 17

Let G be the dihedral group of order 16:

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

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.

Solution. $\langle r^4\rangle = \{1, r^4\}$. So for each $g \in G$, we can write $g\langle r^4\rangle = \{g, gr^4\}$, and we see that the cosets in $\overline{G}$ partition G into sets of two elements. $|G| = 16$, so there must be 8 distinct cosets in $\overline{G}$. □

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

Solution. The elements of $\overline{G}$ are

$$\begin{aligned} \bar{1} &= \{1, r^4\}, & \bar{s} &= \{s, sr^4\}, \\ \bar{r} &= \{r, r^5\}, & \bar{s}\bar{r} &= \{sr, sr^5\}, \\ \bar{r}^2 &= \{r^2, r^6\}, & \bar{s}\bar{r}^2 &= \{sr^2, sr^6\}, \\ \bar{r}^3 &= \{r^3, r^7\}, & \bar{s}\bar{r}^3 &= \{sr^3, sr^7\}. \end{aligned}$$

□

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

Solution. The orders are

$$\begin{aligned} |\bar{1}| &= 1, & |\bar{s}| &= 2, \\ |\bar{r}| &= 4, & |\overline{sr}| &= 2, \\ |\overline{r^2}| &= 2, & |\overline{sr^2}| &= 2, \\ |\overline{r^3}| &= 4, & |\overline{sr^3}| &= 2. \end{aligned}$$ □

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

Solution. Since $rs = sr^{-1} = sr^7$, and since $\overline{sr^7} = \overline{sr^3}$, we have $\overline{rs} = \overline{sr^3}$. Likewise,

$$\overline{sr^{-2}s} = \overline{s^2r^2} = \overline{r^2}$$

and

$$\overline{s^{-1}r^{-1}sr} = \overline{s^{-1}sr^2} = \overline{r^2}.$$ □

(e) Prove that $\overline{H} = \langle \bar{s}, \bar{r}^2 \rangle$ 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 G.

Solution. By definition, $\overline{H}$ is a subgroup of $\overline{G}$ since it is generated by members of $\overline{G}$. To show that $\overline{H} \trianglelefteq \overline{G}$, we need only check that the conjugates of the generators of $\overline{H}$ lie in $\overline{H}$.

Take any element $\bar{g} \in \overline{G}$. If $\bar{g} = \overline{r^k}$ for some integer k with $0 \leq k \leq 3$, then

$$\overline{gsg^{-1}} = \overline{r^k s r^{-k}} = \overline{sr^{-2k}} = \overline{s(r^2)^{-k}} \in \overline{H}$$

and

$$\overline{gr^2g^{-1}} = \overline{r^k r^2 r^{-k}} = \overline{r^2} \in \overline{H}.$$

The other possibility is that $\bar{g} = \overline{sr^k}$. Then

$$\overline{gsg^{-1}} = \overline{sr^k s(sr^k)^{-1}} = \overline{sr^k s s r^k} = \overline{sr^{2k}} = \overline{s(r^2)^k} \in \overline{H}$$

and

$$\overline{gr^2g^{-1}} = \overline{sr^k r^2 (sr^k)^{-1}} = \overline{sr^{k+2}sr^k} = \overline{r^{-2}} = \overline{(r^2)^{-1}} \in \overline{H}.$$

This shows that $\overline{H}$ is normal in $\overline{G}$.

Note that $\overline{H} = \{1, \overline{r^2}, \bar{s}, \overline{sr^2}\}$ has exactly four elements. It has already been shown that every group having four elements is isomorphic to either the Klein 4-group V_4 or to the cyclic group Z_4 (see Exercise 2.5.10). Z_4 has only one element of order 2, but it is easy to check that every nonidentity element in $\overline{H}$ has order 2, so $\overline{H} \cong V_4$.

Lastly, the complete preimage of $\overline{H}$ is $\pi^{-1}(\overline{H})$, where $\pi\colon G \to \overline{G}$ is the natural projection of G onto $\overline{G}$. From the cosets found earlier, we find that

$$\pi^{-1}(\overline{H}) = \{1, r^2, r^4, r^6, s, sr^2, sr^4, sr^6\}.$$

Call this preimage A. If we notice that

$$(r^2)^4 = s^2 = 1 \quad \text{and} \quad r^2 s = sr^{-2} = s(r^2)^{-1},$$

we see that this subgroup A behaves like D_8, and indeed, the mapping $\varphi\colon A \to D_8$ determined by $\varphi(r^2) = r$ and $\varphi(s) = s$ extends to a bijective homomorphism. Therefore $A \cong D_8$. □

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

Solution. From Exercise 3.1.16, we know that $\overline{G} = \langle \bar{r}, \bar{s} \rangle$. Since $\overline{r^2}$ commutes with both of these generators, $\overline{r^2} \in Z(\overline{G})$. However, the elements $\bar{r}$ and $\overline{r^3}$ do not commute with $\bar{s}$, and the elements $\overline{sr}$, $\overline{sr^2}$, and $\overline{sr^3}$ do not commute with $\bar{r}$. So

$$Z(\overline{G}) = \{\bar{1}, \overline{r^2}\}.$$

The elements of $\overline{G}/Z(\overline{G})$ are

$$\begin{aligned} \overline{\bar{1}} &= \{\bar{1}, \overline{r^2}\}, & \overline{\bar{s}} &= \{\bar{s}, \overline{sr^2}\}, \\ \overline{\bar{r}} &= \{\bar{r}, \overline{r^3}\}, & \overline{\overline{sr}} &= \{\overline{sr}, \overline{sr^3}\}. \end{aligned}$$

Notice that each nonidentity element has order 2. Therefore $\overline{G}/Z(\overline{G})$ is isomorphic to the Klein 4-group, V_4. □

3.1.18 Exercise 18

Let G be the quasidihedral group of order 16:

$$G = \langle \sigma, \tau \mid \sigma^8 = \tau^2 = 1, \sigma\tau = \tau\sigma^3 \rangle$$

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

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

Solution. Since $\langle \sigma^4 \rangle = \{1, \sigma^4\}$, its cosets partition G into pairs of elements, so that there must be 8 distinct cosets. □

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

Solution. The elements of $\overline{G}$ are as follows.

$$\begin{aligned} \bar{1} &= \{1, \sigma^4\}, & \bar{\tau} &= \{\tau, \tau\sigma^4\}, \\ \bar{\sigma} &= \{\sigma, \sigma^5\}, & \overline{\tau\sigma} &= \{\tau\sigma, \tau\sigma^5\}, \\ \overline{\sigma^2} &= \{\sigma^2, \sigma^6\}, & \overline{\tau\sigma^2} &= \{\tau\sigma^2, \tau\sigma^6\}, \\ \overline{\sigma^3} &= \{\sigma^3, \sigma^7\}, & \overline{\tau\sigma^3} &= \{\tau\sigma^3, \tau\sigma^7\}. \end{aligned}$$

□

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

Solution. Computing the orders of the elements, we find

$$\begin{aligned} |\bar{1}| &= 1, & |\bar{\tau}| &= 2, \\ |\bar{\sigma}| &= 4, & |\overline{\tau\sigma}| &= 2, \\ |\overline{\sigma^2}| &= 2, & |\overline{\tau\sigma^2}| &= 2, \\ |\overline{\sigma^3}| &= 4, & |\overline{\tau\sigma^3}| &= 2. \end{aligned}$$ □

(d) Write each of the following elements of $\overline{G}$ in the form $\bar{\tau}^a\bar{\sigma}^b$, for some integers a and b as in (b): $\overline{\sigma\tau}$, $\overline{\tau\sigma^{-2}\tau}$, $\overline{\tau^{-1}\sigma^{-1}\tau\sigma}$.

Solution. We have

$$\begin{aligned} \overline{\sigma\tau} &= \overline{\tau\sigma^3}, \\ \overline{\tau\sigma^{-2}\tau} &= \overline{\sigma^2}, \end{aligned}$$

and

$$\overline{\tau^{-1}\sigma^{-1}\tau\sigma} = \overline{\sigma^6} = \overline{\sigma^2}.$$ □

(e) Prove that $\overline{G} \cong D_8$.

Proof. In $\overline{G}$, we know $|\bar{\tau}| = 2$ and $|\bar{\sigma}| = 4$, and we also know that

$$\overline{\sigma\tau} = \overline{\tau\sigma^3} = \overline{\tau\sigma^7} = \overline{\tau\sigma^{-1}}.$$

So $\overline{G}$ satisfies the same relations as those given in the presentation of D_8 and has the same number of elements as D_8. Therefore $\overline{G} \cong D_8$. □

3.1.19 Exercise 19

Let G be the modular group of order 16:

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

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

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

Solution. As in the previous two exercises, the cosets of $\langle v^4 \rangle = \{1, v^4\}$ partition $\overline{G}$ into pairs of elements, so that $\overline{G} = 8$. □

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

Solution. The elements are

$$\begin{aligned} \bar{1} &= \{1, v^4\}, & \bar{u} &= \{u, uv^4\}, \\ \bar{v} &= \{v, v^5\}, & \bar{u}\bar{v} &= \{uv, uv^5\}, \\ \bar{v}^2 &= \{v^2, v^6\}, & \bar{u}\bar{v}^2 &= \{uv^2, uv^6\}, \\ \bar{v}^3 &= \{v^3, v^7\}, & \bar{u}\bar{v}^3 &= \{uv^3, uv^7\}. \end{aligned}$$ □

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

Solution. The orders of the elements are

$$\begin{aligned} |\bar{1}| &= 1, & |\bar{u}| &= 2, \\ |\bar{v}| &= 4, & |\overline{uv}| &= 4, \\ |\overline{v^2}| &= 2, & |\overline{uv^2}| &= 2, \\ |\overline{v^3}| &= 4, & |\overline{uv^3}| &= 4. \end{aligned}$$ □

(d) Write each of the following elements of $\overline{G}$ in the form $\bar{u}^a\bar{v}^b$, for some integers a and b as in (b): $\overline{vu}$, $\overline{uv^{-2}u}$, $\overline{u^{-1}v^{-1}uv}$.

Solution. We have $\overline{vu} = \overline{uv^5} = \overline{uv}$,

$$\overline{uv^{-2}u} = \overline{uv^6u} = \overline{vuvu} = \overline{vuuv^5} = \overline{v^6} = \overline{v^2},$$

and

$$\overline{u^{-1}v^{-1}uv} = \overline{uv^7uv} = \overline{uv^5(v^2uv)} = \overline{vuuv^{10}v} = \overline{v^{12}} = \bar{1}.$$ □

(e) Prove that $\overline{G}$ is abelian and is isomorphic to $Z_2 \times Z_4$.

Proof. First, note that since $\overline{uv} = \overline{uv^5} = \overline{vu}$, the generators of $\overline{G}$ commute. Therefore $\overline{G}$ is abelian.

Let x be a generator for Z_2 and y a generator for Z_4. Define the map $\varphi\colon \overline{G} \to Z_2 \times Z_4$ by

$$\varphi(\bar{u}^a\bar{v}^b) = (x^a, y^b), \quad a, b \in \mathbb{Z}.$$

It is not hard to see that φ is well defined, since in both groups the exponents a and b can be reduced modulo 2 or 4, respectively, in the same way.

Now, let $\bar{g} = \bar{u}^a\bar{v}^b$ and $\bar{h} = \bar{u}^c\bar{v}^d$ be two elements of $\overline{G}$. Then

$$\begin{aligned} \varphi(\bar{g}\bar{h}) &= \varphi(\overline{u^av^bu^cv^d}) \\ &= \varphi(\overline{u^{a+c}v^{b+d}}) \\ &= (x^{a+c}, y^{b+d}) \\ &= (x^a, y^b)(x^c, y^d) \\ &= \varphi(\bar{g})\varphi(\bar{h}), \end{aligned}$$

and we see that φ is a homomorphism.

φ is also surjective since each element of $Z^2 \times Z^4$ can be obtained with the appropriate exponents on $\bar{u}$ and $\bar{v}$. Being a surjective map between two sets of the same size, φ must be a bijection, and thus an isomorphism. Hence $\overline{G} \cong Z_2 \times Z_4$. □

3.1.20 Exercise 20

Let $G = \mathbb{Z}/24\mathbb{Z}$ and let $\widetilde{G} = G/\langle\overline{12}\rangle$, where for each integer a we simplify notation by writing $\widetilde{\overline{a}}$ as $\tilde{a}$.

(a) Show that $\widetilde{G} = \{\tilde{0}, \tilde{1}, \ldots, \widetilde{11}\}$.

Proof. Since $\langle\overline{12}\rangle = \{\bar{0}, \overline{12}\}$, each coset will consist of the pair

$$\{\bar{n}, \overline{12+n}\} = \tilde{n} \quad \text{for } 0 \leq n \leq 11,$$

and each of these is distinct. □

(b) Find the order of each element of $\widetilde{G}$.

Solution. The orders are

$$\begin{aligned} |\tilde{0}| &= 1, & |\tilde{6}| &= 2, \\ |\tilde{1}| &= 12, & |\tilde{7}| &= 12, \\ |\tilde{2}| &= 6, & |\tilde{8}| &= 3, \\ |\tilde{3}| &= 4, & |\tilde{9}| &= 4, \\ |\tilde{4}| &= 3, & |\widetilde{10}| &= 6, \\ |\tilde{5}| &= 12, & |\widetilde{11}| &= 12. \end{aligned}$$

□

(c) Prove that $\widetilde{G} \cong \mathbb{Z}/12\mathbb{Z}$.

Proof. Define the function $\varphi\colon \widetilde{G} \to \mathbb{Z}/12\mathbb{Z}$ by

$$\varphi(\tilde{n}) = \bar{n}.$$

This is clearly a bijection, and it is a homomorphism since

$$\varphi(\widetilde{m} + \tilde{n}) = \overline{m+n} = \overline{m} + \bar{n} = \varphi(\widetilde{m}) + \varphi(\tilde{n})$$

for any $\widetilde{m}, \tilde{n} \in \widetilde{G}$. Therefore $\widetilde{G} \cong \mathbb{Z}/12\mathbb{Z}$. □

3.1.21 Exercise 21

Let $G = Z_4 \times Z_4$ be given in terms of the following generators and relations:

$$G = \langle x, y \mid x^4 = y^4 = 1, xy = yx\rangle.$$

Let $\overline{G} = G/\langle x^2y^2\rangle$ (note that every subgroup of the abelian group G is normal).

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

Proof. Since x and y commute, $(x^2y^2)^2 = 1$ and so $\langle x^2y^2\rangle = \{1, x^2y^2\}$. The cosets of $\langle x^2y^2\rangle$ in G are as follows:

$$\begin{aligned} \bar{1} &= \{1, x^2y^2\}, & \bar{y} &= \{y, x^2y^3\}, \\ \bar{x} &= \{x, x^3y^2\}, & \overline{xy} &= \{xy, x^3y^3\}, \\ \overline{x^2} &= \{x^2, y^2\}, & \overline{x^2y} &= \{x^2y, y^3\}, \\ \overline{x^3} &= \{x^3, xy^2\}, & \overline{x^3y} &= \{x^3y, xy^3\}. \end{aligned}$$

Each of these is distinct, and all elements in G are accounted for. Therefore $|\overline{G}| = 8$. □

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

Solution. As given above, the elements are $\bar{1}$, $\bar{x}$, $\overline{x^2}$, $\overline{x^3}$, $\bar{y}$, $\overline{xy}$, $\overline{x^2y}$, and $\overline{x^3y}$. □

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

Solution. The orders are

$$\begin{aligned} |\bar{1}| &= 1, & |\bar{y}| &= 4, \\ |\bar{x}| &= 4, & |\overline{xy}| &= 2, \\ |\overline{x^2}| &= 2, & |\overline{x^2y}| &= 4, \\ |\overline{x^3}| &= 4, & |\overline{x^3y}| &= 2. \end{aligned}$$ □

(d) Prove that $\overline{G} \cong Z_4 \times Z_2$.

Proof. Let a be a generator for Z_4 and b a generator for Z_2. Also, in $\overline{G}$, let $\bar{u} = \bar{x}$ and $\bar{v} = \overline{xy}$, and note that every element in $\overline{G}$ can be written in the form $\bar{u}^m\bar{v}^n$ for integers m and n. Define a function $\varphi\colon \overline{G} \to Z_4 \times Z_2$ by

$$\varphi(\overline{u^m v^n}) = (a^m, b^n).$$

First we show that φ is well defined. Suppose $\overline{u^m v^n} = \overline{u^p v^q}$. Then $\overline{x^{m+n}y^n} = \overline{x^{p+q}y^q}$ and we must have $n \equiv q \pmod 4$ and $m + n \equiv p + q \pmod 4$, which together imply that $m \equiv p \pmod 4$ and $n \equiv q \pmod 2$. This means that in $Z_4 \times Z_2$, the elements (a^m, b^n) and (a^p, b^q) are actually the same, so φ is a well defined function.

Next, φ is easily seen to be surjective. And since both groups have the same order, it is also a bijection.

Finally, φ is a homomorphism since

$$\begin{aligned} \varphi((a^m, b^n)(a^p, b^q)) &= \varphi((a^{m+p}, b^{n+q})) \\ &= \overline{x^{m+p}y^{n+q}} \\ &= \overline{x^m y^n} \cdot \overline{x^p y^q} \\ &= \varphi((a^m, b^n))\varphi((a^p, b^q)). \end{aligned}$$

Therefore $\overline{G} \cong Z_4 \times Z_2$. □

3.1.22 Exercise 22

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

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

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

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

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

We know N is a subgroup of G by Exercise 2.1.10.

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

3.1.23 Exercise 23

Prove that the join of any nonempty collection of normal subgroups of a group is a normal subgroup.

Proof. Let G be a group and I a nonempty set of indices, and let $\{N_\alpha \mid \alpha \in I\}$ be a collection of subgroups of G, with $N_\alpha \trianglelefteq G$ for each $\alpha \in I$. Let N be the join of all the subgroups in the collection:

$$N = \langle N_\alpha \mid \alpha \in I \rangle.$$

Fix an element $g \in G$ and $n \in N$. Since n belongs to the join of $\{N_\alpha\}$, we can write n as the product of finitely many elements, each belonging to one of the sets in the collection:

$$n = x_1 x_2 \cdots x_k, \quad \text{where for each } i,\ x_i \in N_{\alpha_i} \text{ for some } \alpha_i \in I.$$

Since $N_{\alpha_i} \trianglelefteq G$ for each i, we have $gx_ig^{-1} \in N_{\alpha_i} \subseteq N$. Now notice that we can write

$$\begin{aligned} gng^{-1} &= gx_1x_2x_3 \cdots x_{k-1}x_kg^{-1} \\ &= gx_1(g^{-1}g)x_2(g^{-1}g)x_3 \cdots x_{k-1}(g^{-1}g)x_kg^{-1} \\ &= (gx_1g^{-1})(gx_2g^{-1}) \cdots (gx_kg^{-1}). \end{aligned}$$

Therefore gng^{-1} can be written as a product of elements in N, and so must be in N by closure. Since g and n were chosen arbitrarily, this shows that $gNg^{-1} \subseteq N$ for each $g \in G$ so that $N \trianglelefteq G$. □

3.1.24 Exercise 24

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

Proof. We know that the intersection of two subgroups is a subgroup, so $N \cap H$ is a subgroup of H. Let $h \in H$ and $x \in N \cap H$. Then since $x \in N$ and $N \trianglelefteq G$, $hxh^{-1} \in N$. But $x \in H$ so $hxh^{-1} \in H$. Therefore $hxh^{-1} \in N \cap H$. Since this is true for any $h \in H$ and $x \in N \cap H$, we have $N \cap H \trianglelefteq H$. □

3.1.25 Exercise 25

(a) Prove that a subgroup N of G is normal if and only if $gNg^{-1} \subseteq N$ for *all* $g \in G$.

Proof. The left-to-right implication is immediate from the definition. For the other direction, suppose that N is a subgroup of a group G, with

$$gNg^{-1} \subseteq N \quad \text{for each } g \in G. \tag{3.1}$$

Fix an element $g_0 \in G$ and let $x \in N$. Consider the element $y = g_0^{-1}xg_0$. Then $y \in N$ by (3.1) (simply take $g = g_0^{-1}$). Therefore

$$g_0 y g_0^{-1} = g_0(g_0^{-1}xg_0)g_0^{-1} = x.$$

This shows that $x \in g_0 N g_0^{-1}$. Since $g_0 \in G$ was arbitrary, $x \in gNg^{-1}$ for each g so that $N \subseteq gNg^{-1}$. Together with (3.1), we have $gNg^{-1} = N$ so that $N \trianglelefteq G$. □

(b) Let $G = GL_2(\mathbb{Q})$, let N be the subgroup of upper triangular matrices with integer entries and 1's on the diagonal, and let g be the diagonal matrix with entries $2, 1$. Show that $gNg^{-1} \subseteq N$ but g does *not* normalize N.

Proof. We have

$$N = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \,\middle|\, b \in \mathbb{Z} \right\} \quad \text{and} \quad g = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}.$$

For any $b \in \mathbb{Z}$,

$$g \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} g^{-1} = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \frac{1}{2} & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2b \\ 0 & 1 \end{pmatrix} \in N,$$

and we see that $gNg^{-1} \subseteq N$.

But notice that elements in gNg^{-1} must have an even integer in the upper-right entry. This will always be the case, regardless of which $n \in N$ we use. Now consider the element

$$x = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in N.$$

Then there is no matrix n in N with the property that $gng^{-1} = x$, because as we have observed, the upper-right entry of gng^{-1} is always even. Consequently, g does not normalize N. □

3.1.26 Exercise 26

Let $a, b \in G$.

(a) Prove that the conjugate of the product of a and b is the product of the conjugate of a and the conjugate of b. Prove that the order of a and the order of any conjugate of a are the same.

Proof. For any $g \in G$, we have

$$g(ab)g^{-1} = ga(g^{-1}g)bg^{-1} = (gag^{-1})(gbg^{-1}),$$

so the conjugate of a product is the product of the conjugates. Note that a simple induction argument will allow us to extend this result to products of any finite number of elements of G.

Next, suppose $|a| = n < \infty$. From the above result, we have

$$(gag^{-1})^n = ga^n g^{-1} = gg^{-1} = 1,$$

so $|gag^{-1}| \leq n$. On the other hand, if $(gag^{-1})^k = 1$, then $ga^k g^{-1} = 1$, and multiplying on the left by g^{-1} and on the right by g gives $a^k = g^{-1}g = 1$, so that $|gag^{-1}| \geq n$. Therefore

$$|gag^{-1}| = n = |a|, \quad \text{for all } g \in G.$$

Lastly, if $|a| = \infty$, then there is no positive integer n such that $a^n = 1$. But if $(gag^{-1})^n = 1$ for some positive n, then the same argument as before shows that $a^n = 1$, which is a contradiction. Therefore $|gag^{-1}| = \infty$ in this case. □

(b) Prove that the conjugate of a^{-1} is the inverse of the conjugate of a.

Proof. For any $g \in G$,

$$(ga^{-1}g^{-1})(gag^{-1}) = ga^{-1}(g^{-1}g)ag^{-1} = ga^{-1}ag^{-1} = gg^{-1} = 1,$$

so $ga^{-1}g^{-1} = (gag^{-1})^{-1}$. □

(c) Let $N = \langle S \rangle$ for some subset S of G. Prove that $N \trianglelefteq G$ if $gSg^{-1} \subseteq N$ for all $g \in G$.

Proof. First note that if S is the empty set, then N is the trivial subgroup and is therefore normal in G. So assume that S is nonempty.

Now suppose $gSg^{-1} \subseteq N$ for all $g \in G$, and pick any $x \in N$. Since $N = \langle S \rangle$, we may write

$$x = s_1 s_2 \cdots s_k, \quad \text{where } s_i \in S \text{ for each } i = 1, 2, \ldots, k.$$

Since we have already proven above that the conjugate of a product is the product of the conjugates, we have for all $g \in G$ that

$$gxg^{-1} = (gs_1g^{-1})(gs_2g^{-1}) \cdots (gs_kg^{-1}) \in N.$$

Therefore $gNg^{-1} \subseteq N$ for all $g \in G$ and we can conclude that $N \trianglelefteq G$. □

(d) Deduce that if N is the cyclic group $\langle x \rangle$, then N is normal in G if and only if for each $g \in G$, $gxg^{-1} = x^k$ for some $k \in \mathbb{Z}$.

Proof. Since $a \in N$ if and only if $a = x^k$ for some integer k, the left-to-right implication is immediate from the definition of a normal subgroup, and the other direction is just a special case of the previous result, with $S = \{x\}$. □

(e) Let n be a positive integer. Prove that the subgroup N of G generated by all the elements of G of order n is a normal subgroup of G.

Proof. Let $S = \{g \in G \mid |g| = n\}$ and let $N = \langle S \rangle$. If S is empty then N is the trivial subgroup and is normal in G, so assume S is nonempty. Then for any $s \in S$ and $g \in G$, we have

$$|gsg^{-1}| = |s| = n,$$

so $gsg^{-1} \in S \subseteq N$. Then $gSg^{-1} \subseteq N$ for each $g \in G$, and we can apply our earlier result to conclude that $N \trianglelefteq G$. □

3.1.27 Exercise 27

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

Proof. Fix an element $g \in G$. If $gNg^{-1} = N$ then certainly $gNg^{-1} \subseteq N$.

Conversely, suppose that $gNg^{-1} \subseteq N$. Define the function $\varphi\colon N \to gNg^{-1}$ by

$$\varphi(x) = gxg^{-1}.$$

We will show that φ is a bijection. First, if $gag^{-1} = gbg^{-1}$ for $a, b \in N$, then cancellation shows that $a = b$. Therefore φ is injective. And if $y \in gNg^{-1}$, then by definition there is some $x \in N$ with $y = gxg^{-1} = \varphi(x)$, so φ is surjective. We conclude that φ is a bijection, and therefore $|gNg^{-1}| = |N|$. But $gNg^{-1} \subseteq N$ and N is finite, so we must have equality:

$$gNg^{-1} = N.$$

Finally, we know by definition that $N_G(N) = \{g \in G \mid gNg^{-1} = N\}$. As was just proved, $gNg^{-1} = N$ if and only if $gNg^{-1} \subseteq N$ (since N is finite), so the normalizer can also be written as

$$N_G(N) = \{g \in G \mid gNg^{-1} \subseteq N\}.$$ □

3.1.28 Exercise 28

Let N be a *finite* subgroup of a group G and assume $N = \langle S \rangle$ for some subset S of G. Prove that an element $g \in G$ normalizes N if and only if $gSg^{-1} \subseteq N$.

Proof. Fix an element $g \in G$. First, if $gNg^{-1} = N$ then it must be true that $gSg^{-1} \subseteq N$, since gSg^{-1} is a subset of gNg^{-1}.

Conversely, suppose $gSg^{-1} \subseteq N$. If S is empty then N is trivial and must be normal, so suppose S is nonempty. Choose any $x \in N$. Since S generates N, we have

$$x = s_1 s_2 \cdots s_k, \quad \text{where } s_i \in S \text{ for each } i = 1, 2, \ldots, k.$$

As the conjugate of a product is the product of the conjugates, we know that $gxg^{-1} = gs_1g^{-1}\cdots gs_kg^{-1}$. Since $gs_ig^{-1} \in gSg^{-1} \subseteq N$, we have $gxg^{-1} \in N$. And our choice of $x \in N$ was arbitrary, so $gNg^{-1} \subseteq N$. Since N is finite, we may use the result from Exercise 3.1.27, to conclude that g normalizes N. □

3.1.29 Exercise 29

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

Proof. If N is normal in G then $gNg^{-1} = N$ for all $g \in G$, so clearly $tSt^{-1} \subseteq N$ for any $t \in T$.

For the other direction, suppose that $tSt^{-1} \subseteq N$ for all $t \in T$. If S or T is the empty set, then the result is obvious, so suppose S and T are nonempty. Choose any $g \in G$. We can write

$$g = t_1t_2\cdots t_k \quad \text{with } t_i \in T \text{ for each } i = 1, 2, \ldots, k.$$

We will use induction on k to prove that $gSg^{-1} \subseteq N$. If $k = 1$, then $gSg^{-1} = t_1St_1^{-1} \subseteq N$, so the base case is satisfied. Now assume that $gSg^{-1} \subseteq N$ whenever g can be written as the product of k elements from t, and consider

$$g = t_1t_2\cdots t_kt_{k+1}, \quad t_i \in T \text{ for each } i.$$

Set $h = t_1t_2\cdots t_k$, so that $g = ht_{k+1}$. By the induction assumption, $hSh^{-1} \subseteq N$. So for any $s \in S$, we have

$$gsg^{-1} = ht_{k+1}s(ht_{k+1})^{-1} = ht_{k+1}st_{k+1}^{-1}h^{-1} = hxh^{-1},$$

where $x = t_{k+1}st_{k+1}^{-1} \in N$. So x can be written as

$$x = s_1s_2\cdots s_\ell, \quad s_i \in S \text{ for } i = 1, 2, \ldots, \ell$$

and

$$hxh^{-1} = (hs_1h^{-1})(hs_2h^{-1})\cdots(hs_\ell h^{-1}) \in N.$$

So $gsg^{-1} \in N$, which gives $gSg^{-1} \subseteq N$. By induction, this statement is true for any $g \in G$. And since N is finite, our result from Exercise 3.1.28 finishes the proof. □

3.1.30 Exercise 30

Let $N \leq G$ and let $g \in G$. Prove that $gN = Ng$ if and only if $g \in N_G(N)$.

Proof. Suppose $gN = Ng$. Then for any $x \in N$, there is a $y \in N$ such that $gx = yg$. Multiplying on the right by g^{-1} gives $gxg^{-1} = y \in N$. This is true for any $x \in N$, so $gNg^{-1} \subseteq N$. On the other hand, if $x \in N$, then there is a $y \in N$ such that $xg = gy$, and multiplying on the right by g^{-1} gives $x = gyg^{-1} \in gNg^{-1}$. So $N \subseteq gNg^{-1}$ and we conclude that the two sets are equal. Therefore $g \in N_G(N)$.

Conversely, suppose g normalizes N. Let $x \in N$ be arbitrary. Then we have $x \in gNg^{-1}$ so that $x = gyg^{-1}$ for some $y \in N$. Multiplying on the right by g gives $xg = gy$. Therefore $xg \in gN$ for all $x \in N$, so $Ng \subseteq gN$. By a symmetric argument, we also have $gN \subseteq Ng$. Therefore the two sets are equal: $gN = Ng$. □

3.1.31 Exercise 31

Prove that if $H \leq G$ and N is a normal subgroup of H then $H \leq N_G(N)$. Deduce that $N_G(N)$ is the largest subgroup of G in which N is normal (i.e., is the join of all subgroups H for which $N \trianglelefteq H$).

Proof. We already know that $N_G(N)$ is a subgroup, so we only need to establish that $H \subseteq N_G(N)$. But this is easy: Let $h \in H$. Since $N \trianglelefteq H$ we have $hNh^{-1} = N$. Therefore $h \in N_G(N)$. This shows that $H \leq N_G(N)$.

Clearly $N \trianglelefteq N_G(N)$, and we have shown that every subgroup of G in which N is normal must be a subgroup of $N_G(N)$. This implies that $N_G(N)$ is the largest subgroup of G in which N is normal. □

3.1.32 Exercise 32

Prove that every subgroup of Q_8 is normal. For each subgroup find the isomorphism type of its corresponding quotient.

Solution. The subgroups of Q_8 are 1, $\langle -1\rangle$, $\langle i\rangle$, $\langle j\rangle$, $\langle k\rangle$, and Q_8. From the lattice for Q_8, we know that $\langle i\rangle$, $\langle j\rangle$, and $\langle k\rangle$ are maximal subgroups, so their normalizers are either themselves or Q_8. But it is easy to check that, for example, $j\langle i\rangle(-j) = \langle i\rangle$, so $N_{Q_8}(\langle i\rangle) = Q_8$. By a similar argument, we conclude that

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

so each of these subgroups is normal. And $\langle -1\rangle$ is certainly normal since it is in the center of Q_8. Therefore every subgroup of Q_8 is normal.

Now $Q_8/\langle -1\rangle = \{\bar{1}, \bar{i}, \bar{j}, \bar{k}\}$ has order 4. And since $\bar{i}\cdot\bar{i} = \overline{-1} = \bar{1}$, we see that $\bar{i}$ has order 2. Similarly $\bar{j}$ and $\bar{k}$ have order 2. From the classification of groups of order 4, we know that $Q_8/\langle -1\rangle \cong V_4$, where V_4 is the Klein four-group.

Similarly, $Q_8/\langle i\rangle = \{\bar{1}, \bar{j}\}$ has order 2, so it must be isomorphic to Z_2. By symmetry, $Q_8/\langle j\rangle \cong Q_8/\langle k\rangle \cong Z_2$ as well. □

3.1.33 Exercise 33

Find all normal subgroups of D_8 and for each of these find the isomorphism type of its corresponding quotient.

Solution. Certainly the trivial subgroup $\langle 1\rangle$ is normal in D_8, as is D_8 itself. $D_8/\langle 1\rangle \cong D_8$ and $D_8/D_8 \cong \langle 1\rangle$.

Now consider the subgroups of order 2, aside from $\langle r^2\rangle$. For these we have

$$\begin{aligned} rsr^{-1} &= rsr^3 = sr^2 \notin \langle s\rangle, \\ r(sr)r^{-1} &= rs = sr^3 \notin \langle sr\rangle, \\ r(sr^2)r^{-1} &= rsr = s \notin \langle sr^2\rangle, \\ r(sr^3)r^{-1} &= rsr^2 = sr \notin \langle sr^3\rangle, \end{aligned}$$

so none of $\langle s\rangle$, $\langle sr\rangle$, $\langle sr^2\rangle$, and $\langle sr^3\rangle$ are normal in D_8.

Next, since $\langle r^2 \rangle = Z(D_8)$, we know that $\langle r^2 \rangle \trianglelefteq D_8$. The cosets in $D_8/\langle r^2 \rangle$ are

$$\begin{aligned} \bar{1} &= \{1, r^2\}, \\ \bar{r} &= \{r, r^3\}, \\ \bar{s} &= \{s, sr^2\}, \\ \overline{sr} &= \{sr, sr^3\}. \end{aligned}$$

Since $|\bar{r}| = |\bar{s}| = |\overline{sr}| = 2$, we see that $D_8/\langle r^2 \rangle \cong V_4$.

From the lattice for D_8, we know that the remaining subgroups are maximal. So their normalizers are either the subgroups themselves or all of D_8. Since

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

and

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

we see that $N_{D_8}(\langle r \rangle) = N_{D_8}(\langle s, r^2 \rangle) = N_{D_8}(\langle sr, r^2 \rangle) = D_8$. Therefore $\langle r \rangle$, $\langle s, r^2 \rangle$, and $\langle sr, r^2 \rangle$ are normal in D_8. The cosets of $\langle r \rangle$ are

$$\bar{1} = \{1, r, r^2, r^3\} \quad \text{and} \quad \bar{s} = \{s, sr, sr^2, sr^3\},$$

the cosets of $\langle s, r^2 \rangle$ are

$$\bar{1} = \{1, s, r^2, sr^2\} \quad \text{and} \quad \bar{r} = \{r, r^3, sr^3, sr\},$$

and the cosets of $\langle sr, r^2 \rangle$ are

$$\bar{1} = \{1, sr, r^2, sr^3\} \quad \text{and} \quad \bar{r} = \{r, s, r^3, sr^2\}.$$

Since there are only two distinct cosets in each case, we have

$$D_8/\langle r \rangle \cong D_8/\langle s, r^2 \rangle \cong D_8/\langle sr, r^2 \rangle \cong Z_2. \qquad \square$$

3.1.34 Exercise 34

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

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

Proof. First, since r^k commutes with r, we know that $r \in N_{D_{2n}}(\langle r^k \rangle)$. Also,

$$sr^k s^{-1} = sr^k s = s^2 r^{-k} = (r^k)^{-1} \in \langle r^k \rangle.$$

Therefore $s \in N_{D_{2n}}(\langle r^k \rangle)$. Since both s and r (the generators of D_{2n}) normalize $\langle r^k \rangle$, we must have $N_{D_{2n}}(\langle r^k \rangle) = D_{2n}$. Therefore $\langle r^k \rangle \trianglelefteq D_{2n}$. $\square$

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

Proof. Since $\langle r^k \rangle = \{1, r^k, r^{2k}, \ldots, r^{n-k}\}$, we see that the order of $\langle r^k \rangle$ is n/k. Therefore, each coset will consist of n/k elements, so the cosets will partition D_{2n} into $2n/(n/k) = 2k$ distinct sets.

Consider the two cosets

$$\bar{r} = \{r, r^{k+1}, r^{2k+1}, \ldots, r^{n-k+1}\}$$

and

$$\bar{s} = \{s, sr^k, sr^{2k}, \ldots, sr^{n-k}\}.$$

These are clearly distinct. Observe that

$$(\bar{r})^k = \overline{r^k} = \bar{1} \quad \text{and} \quad (\bar{s})^2 = \overline{s^2} = \bar{1},$$

so $|\bar{s}| = 2$ and $|\bar{r}| \leq k$. But if $0 < i < k$, then $\overline{r^i} \neq \bar{1}$, so $|\bar{r}| = k$. Moreover,

$$(\bar{r})(\bar{s}) = \overline{rs} = \overline{sr^{-1}} = (\bar{s})(\bar{r})^{-1}.$$

Since we have shown that $D_{2n}/\langle r^k \rangle$ has the same number of elements as D_{2k}, and since $\bar{r}$ and $\bar{s}$ satisfy the same relations as r and s do in the group presentation for D_{2k}, it follows that $D_{2n}/\langle r^k \rangle \cong D_{2k}$. □

3.1.35 Exercise 35

Prove that $SL_n(F) \trianglelefteq GL_n(F)$ and describe the isomorphism type of the quotient group.

Solution. We have shown in Exercise 2.1.9 that $SL_n(F) \leq GL_n(F)$, so we only need to show that it is normal.

Take any matrix $A \in GL_n(F)$ and $B \in SL_n(F)$. Then

$$\det(ABA^{-1}) = \det(A)\det(B)\det(A)^{-1} = \det(A) \cdot 1 \cdot \det(A)^{-1} = 1.$$

This shows that $ABA^{-1} \in SL_n(F)$, and we conclude that $SL_n(F) \trianglelefteq GL_n(F)$.

Now let $G = GL_n(F)/SL_n(F)$ and consider the map $\varphi\colon G \to F^\times$ defined by

$$\varphi(\overline{A}) = \det(A),$$

where $\overline{A}$ is the coset whose representative is A.

First we must show that this mapping is well defined. Suppose the matrices $A, B \in GL_n(F)$ are such that $\overline{A} = \overline{B}$. Each element in the coset $\overline{A}$ is of the form AS, for some $S \in SL_n(F)$. Then $\det(AS) = \det(A)\det(S) = \det(A)$. But $\overline{A} = \overline{B}$ so we also have $AS = BS_0$ for some $S_0 \in SL_n(F)$. Then

$$\det(A) = \det(BS_0) = \det(B)\det(S_0) = \det(B).$$

So φ is a well defined function from G to $F^\times$.

Next we show that φ is injective. Suppose $\det(A) = \det(B)$ for the matrices $A, B \in GL_n(F)$. We need to show that $\overline{A} = \overline{B}$. Take any $X \in \overline{A}$, so that $X = AS$ for some $S \in SL_n(F)$. Then the matrix $T = B^{-1}AS$ belongs to $SL_n(F)$ since

$$\det(T) = \det(B^{-1}AS) = \det(B)^{-1}\det(A)\det(S) = \det(A)^{-1}\det(A) = 1.$$

Now $X = (BB^{-1})(AS) = BT \in \overline{B}$, so that $\overline{A} \subseteq \overline{B}$. By symmetry, the reverse inclusion holds and we see that $\overline{A} = \overline{B}$ so that φ is injective.

For surjectivity, let $f \in F^\times$ be arbitrary. Let A be the diagonal matrix with upper-left entry f and all other diagonal entries 1. Then $\det(A) = f$ so that $\varphi(\overline{A}) = f$ and φ is surjective.

Lastly, we show that φ is a homomorphism. For any $\overline{A}, \overline{B} \in G$, we have

$$\varphi(\overline{AB}) = \det(AB) = \det(A)\det(B) = \varphi(\overline{A})\varphi(\overline{B}).$$

We have now established that φ is a bijective homomorphism from G to $F^\times$. Therefore $G \cong F^\times$. □

3.1.36 Exercise 36

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

Proof. Let G be a group such that $G/Z(G)$ is cyclic. Then $G/Z(G) = \langle xZ(G)\rangle$ for some $x \in G$. In particular, any coset $yZ(G)$ can be written in the form

$$yZ(G) = (xZ(G))^k = x^k Z(G), \quad k \in \mathbb{Z}. \tag{3.2}$$

Now let $a, b \in G$. Since every element of G belongs to some coset of $Z(G)$, (3.2) allows us to write

$$a = x^i z_1 \quad \text{and} \quad b = x^j z_2,$$

for some $i, j \in \mathbb{Z}$ and $z_1, z_2 \in Z(G)$. Since z_1 and z_2 commute with x, and since x commutes with itself, we have

$$ab = x^i z_1 x^j z_2 = x^j z_2 x^i z_1 = ba.$$

This shows that G is abelian. □

3.1.37 Exercise 37

Let A and B be groups. Show that $\{(a, 1) \mid a \in A\}$ is a normal subgroup of $A \times B$ and the quotient of $A \times B$ by this subgroup is isomorphic to B.

Proof. Let $G = A \times B$ and $H = \{(a, 1) \mid a \in A\}$. Then for any $(a, 1) \in H$ and $(x, y) \in G$, we have

$$\begin{aligned}(x, y)(a, 1)(x, y)^{-1} &= (x, y)(a, 1)(x^{-1}, y^{-1}) \\ &= (xax^{-1}, yy^{-1}) \\ &= (xax^{-1}, 1) \in H.\end{aligned}$$

This shows that $H \trianglelefteq G$.

Define the mapping $\varphi\colon G/H \to B$ by

$$\varphi((a, b)H) = b.$$

Suppose (a_1, b_1) and (a_2, b_2) are representatives of the same coset of H. Then

$$(a_1, b_1)^{-1}(a_2, b_2) = (a_1^{-1}a_2, b_1^{-1}b_2) \in H.$$

So $b_1^{-1}b_2 = 1$, which implies that $b_1 = b_2$, so φ is well defined.

Next we show that φ is a bijection. Let $(a_1, b)H$ and $(a_2, b)H$ be cosets in G/H, so that both cosets have the same image under φ. Then

$$(a_1, b)^{-1}(a_2, b) = (a_1^{-1}a_2, b^{-1}b) = (a_1^{-1}a_2, 1) \in H.$$

This shows that $(a_1, b)H = (a_2, b)H$ so that φ is injective. And for any $b \in B$, $\varphi((1, b)H) = b$, so φ is surjective also.

Finally, let $(a_1, b_1)H$ and $(a_2, b_2)H$ be cosets of H. Then

$$\begin{aligned}\varphi((a_1, b_1)H(a_2, b_2)H) &= \varphi((a_1a_2, b_1b_2)H) \\ &= b_1b_2 \\ &= \varphi((a_1, b_1)H)\varphi((a_2, b_2)H),\end{aligned}$$

and φ is a bijective homomorphism. Therefore $G/H \cong B$. □

3.1.38 Exercise 38

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

Proof. Since A is abelian, $A \times A$ is abelian. Every subgroup of an abelian group is normal, so $D \trianglelefteq A \times A$.

Two cosets $(a_1, b_1)D$ and $(a_2, b_2)D$ are equal if and only if

$$(a_1, b_1)^{-1}(a_2, b_2) \in D,$$

that is if and only if $a_1^{-1}a_2 = b_1^{-1}b_2$ or $a_1b_1^{-1} = a_2b_2^{-1}$. Therefore the mapping $\varphi\colon (A \times A)/D \to A$ given by

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

is a well defined injection. It is also a surjection, since for any element $a \in A$, $\varphi((a, 1)D) = a$. And φ is a homomorphism since

$$\begin{aligned}\varphi((a_1, b_1)D(a_2, b_2)D) &= \varphi((a_1a_2, b_1b_2)D) \\ &= a_1a_2(b_1b_2)^{-1} \\ &= (a_1b_1^{-1})(a_2b_2^{-1}) \\ &= \varphi((a_1, b_1)D)\varphi((a_2, b_2)D),\end{aligned}$$

where the second-to-last equality follows from the fact that A is abelian. We have shown that φ is an isomorphism of groups, so $(A \times A)/D \cong A$. □

3.1.39 Exercise 39

Suppose A is the non-abelian group S_3 and D is the diagonal subgroup

$$\{(a, a) \mid a \in A\}$$

of $A \times A$. Prove that D is not normal in $A \times A$.

Proof. Let $a = (1\,3)$ and $b = (1\,2\,3)$ be members of $A = S_3$. Then $a^{-1} = a$ and $b^{-1} = (3\,2\,1)$. Let

$$x = (a, b) \in A \times A \quad \text{and} \quad y = (a, a) \in D.$$

Then

$$xyx^{-1} = (a^3, bab^{-1}) = (a, bab^{-1}).$$

If $D \trianglelefteq A \times A$, then we must have $xyx^{-1} \in D$, so that $a = bab^{-1}$. But

$$bab^{-1} = (1\,2\,3)(1\,3)(3\,2\,1) = (2\,3) \neq (1\,3) = a.$$

We conclude that D is not a normal subgroup of $A \times A$. □

3.1.40 Exercise 40

Let G be a group, let N be a normal subgroup of G and let $\overline{G} = G/N$. Prove that $\bar{x}$ and $\bar{y}$ commute in $\overline{G}$ if and only if $x^{-1}y^{-1}xy \in N$. (The element $x^{-1}y^{-1}xy$ is called the *commutator* of x and y and is denoted $[x, y]$.)

Proof. First suppose that $\overline{xy} = \overline{yx}$. Then $xyN = yxN$ so that $xyz_1 = yxz_2$ for some $z_1, z_2 \in N$, which implies that

$$x^{-1}y^{-1}xy = z_2 z_1^{-1} \in N.$$

Conversely, assume that $x^{-1}y^{-1}xy \in N$, so that $x^{-1}y^{-1}xy = z$ for some $z \in N$. Then

$$xy = yxz.$$

Now $a \in xyN$ if and only if $a = xyz_0$ for some $z_0 \in N$, if and only if $a = yxzz_0$, if and only if $a \in yxN$. Therefore $\overline{xy} = \overline{yx}$. □

3.1.41 Exercise 41

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

Proof. For any $g \in G$ and $x^{-1}y^{-1}xy \in N$ we have

$$\begin{aligned} g(x^{-1}y^{-1}xy)g^{-1} &= gx^{-1}(g^{-1}g)y^{-1}(g^{-1}g)x(g^{-1}g)yg^{-1} \\ &= (gxg^{-1})^{-1}(gyg^{-1})^{-1}(gxg^{-1})(gyg^{-1}) \in N. \end{aligned}$$

Since the conjugates of the generators of N are themselves in N, this shows that $gNg^{-1} \subseteq N$ for all $g \in G$. That is, $N \trianglelefteq G$.

We know that G/N is abelian by Exercise 3.1.40, since $[x, y] \in N$ for any $\bar{x}, \bar{y} \in G/N$. □

3.1.42 Exercise 42

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

Proof. Fix $x \in H$ and $y \in K$. Since $H \trianglelefteq G$, we know that $y^{-1}xy \in H$. So $x^{-1}y^{-1}xy \in H$ also. And since $K \trianglelefteq G$, we have $x^{-1}y^{-1}x \in K$ so that $x^{-1}y^{-1}xy \in K$ also. Therefore $x^{-1}y^{-1}xy \in H \cap K$. But $H \cap K = 1$. This shows that

$$x^{-1}y^{-1}xy = 1, \quad \text{or} \quad xy = yx.$$

Since this is true for any $x \in H$ and $y \in K$, the proof is complete. □

3.1.43 Exercise 43

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

Proof. Let $\mathcal{P}$ be as stated. For any $x \in G$, let $\bar{x}$ denote the element of $\mathcal{P}$ which contains x.

First we show that $\bar{1} \leq G$. $1 \in \bar{1}$ so the set is nonempty. Take any $x, y \in \bar{1}$, so that $\bar{x} = \bar{y} = \bar{1}$. By definition of the operation on $\mathcal{P}$, we have

$$\overline{xy} = \bar{x} \cdot \bar{y} = \bar{1} \cdot \bar{1} = \overline{1 \cdot 1} = \bar{1},$$

so $xy \in \bar{1}$. Moreover,

$$\overline{x^{-1}} = \bar{1} \cdot \overline{x^{-1}} = \bar{x} \cdot \overline{x^{-1}} = \overline{xx^{-1}} = \bar{1},$$

and $x^{-1} \in \bar{1}$. This shows that $\bar{1}$ is a subgroup of G.

Next, take any $g \in G$ and $x \in \bar{1}$. Then

$$\overline{gxg^{-1}} = \bar{g} \cdot \bar{x} \cdot \overline{g^{-1}} = \bar{g} \cdot \bar{1} \cdot \overline{g^{-1}} = \overline{gg^{-1}} = \bar{1}.$$

Therefore $gxg^{-1} \in \bar{1}$ and $\bar{1} \trianglelefteq G$.

Finally, we show that the coset $g\bar{1}$ is a member of $\mathcal{P}$. In particular, we show that $g\bar{1} = \bar{g}$. If $x \in g\bar{1}$, then $x = gy$ for some $y \in \bar{1}$. Then

$$\bar{x} = \overline{gy} = \bar{g} \cdot \bar{y} = \bar{g} \cdot \bar{1} = \bar{g},$$

so $x \in \bar{g}$ and $g\bar{1} \subseteq \bar{g}$.

Conversely, if $x \in \bar{g}$, then $\bar{x} = \bar{g}$. Multiplying on the left by $\bar{g}^{-1}$ gives $\overline{g^{-1}x} = \overline{g^{-1}g} = \bar{1}$. Therefore $g^{-1}x \in \bar{1}$. So

$$x = gg^{-1}x = g(g^{-1}x) \in g\bar{1},$$

and we see that $g\bar{1} \supseteq \bar{g}$. This shows that $g\bar{1} = \bar{g}$ as required. □

3.2 More on Cosets and Lagrange's Theorem

Let G be a group.

3.2.1 Exercise 1

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

Solution. The permissible orders are 1, 2, 5, 15, and 60. The other orders do not divide 120 and so by Lagrange's Theorem are not possible.

The subgroup of order 1 would have index 120, the subgroup of order 2 would have index 60, the subgroup of order 5 would have index 24, the subgroup with order 15 would have index 8, and the subgroup of order 60 would have index 2. □

3.2.2 Exercise 2

Prove that the lattice of subgroups of S_3 in Section 2.5 is correct (i.e., prove that it contains all subgroups of S_3 and that their pairwise joins and intersections are correctly drawn).

Proof. The subgroups contained in the lattice are 1, $\langle(1\,2)\rangle$, $\langle(1\,3)\rangle$, $\langle(2\,3)\rangle$, $\langle(1\,2\,3)\rangle$, and S_3 itself. Since $|S_3| = 6$, any nontrivial subgroups must have order 2 or 3. Since $\langle(1\,2\,3)\rangle = \langle(1\,3\,2)\rangle$, all cyclic subgroups are accounted for.

Now suppose S_3 has a non-cyclic proper subgroup H. Say H is generated by σ and τ. Then $|H| = 3$ and $H = \{1, \sigma, \tau\}$. But $|\sigma|$ must divide $|H|$, so $|\sigma| = 3$. Then σ and σ^2 are distinct, and we must have $\tau = \sigma^2$. Hence H is cyclic, which gives a contradiction. This shows that all proper subgroups of S_3 are cyclic. Therefore all subgroups are present in the lattice.

Note that the subgroups of order 2 cannot themselves be subgroups of $\langle(1\,2\,3)\rangle$, since $2 \nmid 3$. Therefore every nontrivial subgroup is maximal, and the lattice is correct. □

3.2.3 Exercise 3

Prove that the lattice of subgroups of Q_8 in Section 2.5 is correct.

Proof. By Lagrange's Theorem the possible subgroups of Q_8 have orders 1, 2, 4, and 8. So every nontrivial subgroup has order 2 or 4. The only element of Q_8 having order 2 is -1, so $\langle -1\rangle$ is the only possible subgroup with that order. Every other nonidentity element has order 4. The only subgroups of order 4 are $\langle i\rangle$, $\langle j\rangle$, and $\langle k\rangle$, since all elements of Q_8 belong to one of these subgroups.

$\langle -1\rangle$ is contained in each of $\langle i\rangle$, $\langle j\rangle$, and $\langle k\rangle$, and the latter three are maximal by Lagrange. Therefore the lattice is correct. □

3.2.4 Exercise 4

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

Proof. Let G be as stated. If G is abelian, there is nothing left to prove, so suppose G is not abelian. Then $Z(G)$ is proper. By Lagrange, there are only three possibilities for the order of $Z(G)$: the order is either 1, p, or q.

Now assume that $Z(G)$ is not trivial. Then without loss of generality we may suppose that $|Z(G)| = p$. Since the center of a group is always normal, we may consider the quotient group $G/Z(G)$. Again by Lagrange, we have

$$|G/Z(G)| = \frac{|G|}{|Z(G)|} = \frac{pq}{p} = q.$$

Now, q is prime, so we may apply Corollary 10 to conclude that $G/Z(G)$ is cyclic. Then by Exercise 3.1.36, it follows that G is abelian, which is a contradiction. Therefore $Z(G)$ is the trivial subgroup, and the proof is complete. □

3.2.5 Exercise 5

Let H be a subgroup of G and fix some element $g \in G$.

(a) Prove that gHg^{-1} is a subgroup of G of the same order as H.

Proof. $1 \in gHg^{-1}$, so gHg^{-1} is nonempty. Let $x, y \in gHg^{-1}$. Then $x = gh_1g^{-1}$ and $y = gh_2g^{-1}$ for some $h_1, h_2 \in H$. We have

$$\begin{aligned} xy^{-1} &= (gh_1g^{-1})(gh_2g^{-1})^{-1} \\ &= (gh_1g^{-1})(gh_2^{-1}g^{-1}) \\ &= gh_1(g^{-1}g)h_2^{-1}g^{-1} \\ &= gh_1h_2^{-1}g^{-1} \in gHg^{-1}. \end{aligned}$$

By the subgroup criterion, $gHg^{-1} \leq G$.

Now define the map $\varphi\colon H \to gHg^{-1}$ by $\varphi(h) = ghg^{-1}$. Then φ is clearly surjective. It is also injective, since $gh_1g^{-1} = gh_2g^{-1}$ implies that $h_1 = h_2$ by the left and right cancellation laws. This shows that $|H| = |gHg^{-1}|$ (in fact they are isomorphic). □

(b) Deduce that if $n \in \mathbb{Z}^+$ and H is the unique subgroup of G of order n then $H \trianglelefteq G$.

Proof. For any $g \in G$, we know from the above that $gHg^{-1} \leq G$ and that $|gHg^{-1}| = |H| = n$. Since H is the only subgroup of G with order n, it follows that $H = gHg^{-1}$. Since this is true for every $g \in G$, $H \trianglelefteq G$ by definition. □

3.2.6 Exercise 6

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

Proof. Suppose $Hg = aH$ for some $a \in G$. Since $g \in Hg$, we have $g \in aH$. Since the (right) cosets of H form a partition of G (Proposition 4), this implies that $aH = gH$. Therefore $Hg = gH$ and $g \in N_G(H)$. □

3.2.7 Exercise 7

Let $H \leq G$ and define a relation $\sim$ on G by

$$a \sim b \quad \text{if and only if} \quad b^{-1}a \in H.$$

Prove that $\sim$ is an equivalence relation and describe the equivalence class of each $a \in G$. Use this to prove Proposition 4.

Proof. For any $a \in G$, we certainly have $a^{-1}a = 1 \in H$, so $a \sim a$ and $\sim$ is reflexive. If $a \sim b$ for $a, b \in G$ then, since H must be closed under inverses, we have $a^{-1}b = (b^{-1}a)^{-1} \in H$ so that $b \sim a$, and $\sim$ is symmetric. Lastly, if $a \sim b$ and $b \sim c$ for $a, b, c \in G$, then

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

so $a \sim c$ and we see that $\sim$ is transitive. This shows that $\sim$ is an equivalence relation.

Note that the equivalence classes of $\sim$ form a partition of G (see Proposition 2 of Section 0.1). It is not difficult to see that $a \sim b$ if and only if a and b belong to the same left coset of H. Therefore the left cosets of H form a partition of G, providing an alternative proof for Proposition 4. □

3.2.8 Exercise 8

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

Proof. Let H and K be as stated, and let $n = |H \cap K|$. We know that the intersection of two subgroups is a subgroup, so $H \cap K \leq H$. By Lagrange's Theorem, n must divide $|H|$. But $H \cap K \leq K$ also, so n must divide $|K|$. And since $|H|$ and $|K|$ have no common divisor other than 1, we must have $n = 1$. Therefore $H \cap K$ is the trivial subgroup. □

3.2.9 Exercise 9

Let G be a finite group and let p be a prime dividing $|G|$. Let $\mathcal{S}$ denote the set of p-tuples of elements of G the product of whose coordinates is 1:

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

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

Proof. Let $\mathcal{T}$ be the set of all $(p-1)$-tuples of elements of G. Then $\mathcal{T}$ has $|G|^{p-1}$ elements. We show that $\mathcal{S}$ and $\mathcal{T}$ share the same cardinality.

Define $\varphi\colon \mathcal{T} \to \mathcal{S}$ by

$$\varphi(x_1, x_2, \ldots, x_{p-1}) = (x_1, x_2, \ldots, x_{p-1}, (x_1 x_2 \cdots x_{p-1})^{-1}).$$

Given two elements $\alpha, \beta \in \mathcal{S}$, if $\alpha = \beta$ then clearly their first $p-1$ coordinates must be equal, so $\mathcal{T}$ is injective. Now suppose $\alpha \in \mathcal{S}$. Then the image of the first $p-1$ coordinates of α under $\mathcal{T}$ must be α, since the last coordinate is completely determined by the others (group inverses are unique). Therefore φ is a bijection, so $|\mathcal{S}| = |\mathcal{T}| = |G|^{p-1}$. □

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

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

Proof. Let $\alpha = (x_1, x_2, \ldots, x_p) \in \mathcal{S}$. Then $x_1 x_2 \cdots x_p = 1$. Multiplying on the left by x_p and then on the right by x_p^{-1} gives

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

Therefore $(x_p, x_1, x_2, \ldots, x_{p-1}) \in \mathcal{S}$. We may repeat this process $p-1$ times to see that all cyclic permutations of α are in $\mathcal{S}$. □

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

Proof. Let $\alpha, \beta, \gamma \in \mathcal{S}$ be arbitrary. α is a cyclic permutation of itself (namely the identity permutation), so $\alpha \sim \alpha$ and $\sim$ is reflexive.

If $\alpha \sim \beta$ then β is a cyclic permutation of α, so by taking the inverse of this permutation we see that α is a cyclic permutation of β. Therefore $\beta \sim \alpha$, and $\sim$ is symmetric.

Lastly, if $\alpha \sim \beta$ and $\beta \sim \gamma$ then γ is a cyclic permutation of β and β is a cyclic permutation of α, and by taking the composition of these two permutations we see that γ is a cyclic permutation of α, so that $\alpha \sim \gamma$. Thus $\sim$ is transitive and the proof is complete. □

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

Proof. Take any $\alpha \in \mathcal{S}$ and let $[\alpha]$ denote the equivalence class containing α.

First, if α is the only element in $[\alpha]$, then all cyclic permutations of α must be the same. This is not possible unless all coordinates of α are the same. So α has the form $(x, x, \ldots, x)$, where $x^p = 1$.

Conversely, if α has the form $(x, x, \ldots, x)$ with all coordinates the same, then every cyclic permutation of α will leave α unchanged. Therefore $[\alpha]$ contains only the one element. □

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

Proof. Again, let $\alpha \in \mathcal{S}$ with $[\alpha]$ denoting the corresponding equivalence class, and let

$$\alpha = (x_1, x_2, \ldots, x_p),$$

with the x_i's not necessarily distinct. Suppose $[\alpha]$ contains exactly n members. Then $1 \leq n \leq p$. For all $k \in \mathbb{Z}$, we must have

$$x_i = x_j \quad \text{whenever} \quad i + kn \equiv j \pmod{p}, \tag{3.3}$$

since α can only be cycled n times before arriving back at itself.

Now there are two cases, either $n = p$ or $1 \leq n < p$. In the first case there is nothing left to prove, so assume $1 \leq n < p$. Then $(n, p) = 1$ since p is prime. So by Exercise 0.3.14, we know that n has a multiplicative inverse, n^{-1}, modulo p. Then, taking $k = n^{-1}$, (3.3) tells us that $x_i = x_j$ whenever $i + 1 \equiv j \pmod{p}$. Therefore $x_{i+1} = x_i$ for all i with $1 \leq i < p$, and $x_1 = x_p$. But then every coordinate of α is the same, so $[\alpha]$ has only one member. Hence $n = 1$ in this case.

We have shown that if $[\alpha]$ has exactly n elements, then $n = 1$ or $n = p$. Since the equivalence classes partition $\mathcal{S}$, we see that

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

where k is the number of classes of size 1 and d is the number of classes of size p. □

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

Proof. Since p divides $|G|$, it certainly divides $|G|^{p-1}$. So $p \mid (k + pd)$. But this implies that $p \mid k$. Therefore $k > 1$, so there must be more than one equivalence class of $\sim$ having only one element. One of these must be of the form $(x, x, \ldots, x)$ where x is not the identity of G. Therefore this x is such that $x^p = 1$, so $|x|$ divides p. We know x is not the identity, so $|x| = p$. □

3.2.10 Exercise 10

Suppose H and K are subgroups of finite index in the (possibly infinite) group G with $|G : H| = m$ and $|G : K| = n$. Prove that

$$\text{l.c.m.}(m, n) \leq |G : H \cap K| \leq mn.$$

Deduce that if m and n are relatively prime then $|G : H \cap K| = |G : H| \cdot |G : K|$.

Proof. For any $g \in G$, consider the cosets gH, gK, and $g(H \cap K)$. First, if $x \in g(H \cap K)$, then $x \in gH$ and $x \in gK$ so $g(H \cap K) \subseteq (gH \cap gK)$. On the other hand, if $x \in gH$ and $x \in gK$, then $g^{-1}x \in H \cap K$, so $x \in g(H \cap K)$ and we have $(gH \cap gK) \subseteq g(H \cap K)$. Therefore

$$gH \cap gK = g(H \cap K) \quad \text{for all } g \in G.$$

Now each coset of $H \cap K$ is the intersection of one coset of H and one coset of K. There are exactly mn such intersections, so $|G : H \cap K|$ is finite and is at most mn.

As we will show in Exercise 3.2.11 below, we must have

$$|G : H \cap K| = |G : H||H : H \cap K|.$$

So $|G : H|$ divides $|G : H \cap K|$. That is, if $|G : H \cap K| = s$, then $m \mid s$. By the same argument, we know that $n \mid s$ also. Therefore $s \geq [m, n]$, where $[m, n]$ denotes the least common multiple of m and n. This completes the proof of the inequality.

Finally, if $(m, n) = 1$, then $[m, n] = mn$, and we see that $|G : H \cap K|$ must equal mn. □

3.2.11 Exercise 11

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

Proof. Since cosets of H are contained within cosets of K, if H has infinite index in K or if K has infinite index in G then H has infinite index in G also. So we will assume that $|K : H|$ and $|G : K|$ are finite.

Let $m, n \in \mathbb{Z}^+$ where

$$m = |G : K| \quad \text{and} \quad n = |K : H|.$$

Let $g_1, g_2, \ldots, g_m$ be representatives of the distinct cosets of K in G, and let $k_1, k_2, \ldots, k_n$ be representatives of the distinct cosets of H in K. Take any element $a \in G$. Since the cosets of K partition G, a belongs to exactly one coset g_iK, so $a = g_ib$ for some $b \in K$. And since the cosets of H partition K, b belongs to exactly one coset k_jH, so $b = k_jc$ for some $c \in H$. Then $a = g_ik_jc$, where i and j are uniquely determined.

Note that, within each coset g_iK, we cannot have $g_ik_{j_1}H = g_ik_{j_2}H$ with $j_1 \neq j_2$. For, if this is possible, then let x belong to this common coset. Then $x = g_ik_{j_1}h_1$ and $x = g_ik_{j_2}h_2$ for some $h_1, h_2 \in H$. Multiplying on the left by g_i^{-1} then gives $k_{j_1}h_1 = k_{j_2}h_2$, and we see that k_{j_1} and k_{j_2} are representatives of the same coset of H in K, which is a contradiction.

Therefore the cosets of H partition G into mn disjoint subsets, so

$$|G : H| = mn = |G : K| \cdot |K : H|.$$ □

3.2.12 Exercise 12

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

Proof. Let φ be a mapping between the set of left cosets of H in G to the set of right cosets, given by

$$\varphi(xH) = Hx^{-1}.$$

First we show that φ is well defined. Suppose x and y are representatives of the same left coset gH. Then $x = gh_1$ and $y = gh_2$ for some $h_1, h_2 \in H$. So $x^{-1} = h_1^{-1}g^{-1} \in Hg^{-1}$ and $y^{-1} = h_2^{-1}g^{-1} \in Hg^{-1}$, and we see that φ sends both xH and yH to the same right coset Hg^{-1} and is therefore well defined.

To show that φ is a bijection, we simply exhibit a two-sided inverse function. Let ψ map the set of right cosets of H in G onto the set of left cosets via the map $Hx \mapsto x^{-1}H$. By the same argument as before, ψ is well defined. $\psi \circ \varphi$ and $\varphi \circ \psi$ are obviously the identity, so $\psi = \varphi^{-1}$ and φ is a bijection. It follows that the number of left cosets of H in G is equal to the number of right cosets. □

3.2.13 Exercise 13

Fix any labelling of the vertices of a square and use this to identify D_8 as a subgroup of S_4. Prove that the elements of D_8 and $\langle(1\,2\,3)\rangle$ do not commute in S_4.

Proof. Let the vertices of a square be labelled $1, 2, 3, 4$ in a clockwise fashion. Then every element in D_8 induces a distinct permutation of these vertices. It is easy to see that these permutations form a subgroup of S_4. r is identified with $(1\,2\,3\,4)$ and s is identified with $(2\,4)$.

We have

$$(1\,2\,3\,4)(1\,2\,3) = (1\,3\,2\,4) \neq (1\,3\,4\,2) = (1\,2\,3)(1\,2\,3\,4)$$

and

$$(2\,4)(1\,2\,3) = (1\,4\,2\,3) \neq (1\,2\,4\,3) = (1\,2\,3)(2\,4).$$

Since the generators of D_8 and the generator of $\langle(1\,2\,3)\rangle$ do not commute, we see that the elements in the two subgroups do not in general commute with one another. □

3.2.14 Exercise 14

Prove that S_4 does not have a normal subgroup of order 8 or a normal subgroup of order 3.

Proof. Suppose S_4 has a normal subgroup H of order 8. Now, consider that the elements $(1\,2\,3\,4)$ and $(1\,2\,4\,3)$ cannot both be in H since they generate all of S_4, as we showed in Exercise 2.4.8. But

$$(1\,2\,3\,4) = (1\,4)(3\,2)(1\,3) \quad \text{and} \quad (1\,2\,4\,3) = (3\,4)(3\,2)(1\,3),$$

so H cannot contain all of the 2-cycles $(1\,4)$, $(3\,2)$, $(3\,4)$, and $(1\,3)$. We see then that S_4 contains an element σ of order 2 which does not belong to H. Therefore $H \cap \langle\sigma\rangle = 1$ and we have by Corollary 15 that $H\langle\sigma\rangle \leq S_4$. And by Proposition 13 we see that

$$|H\langle\sigma\rangle| = \frac{|H||\langle\sigma\rangle|}{|H \cap \langle\sigma\rangle|} = 8 \cdot 2 = 16.$$

Now S_4, a group of order 24, has a subgroup of order 16, which contradicts Lagrange's Theorem. Therefore H does not exist: there is no normal subgroup of order 8 in S_4.

Next, suppose that S_4 has a normal subgroup K of order 3. We know by Corollary 10 that any subgroup of order 3 is cyclic. Now, S_4 has more than one subgroup of order 3, for example

$$\langle (1\,2\,3) \rangle = \{1, (1\,2\,3), (1\,3\,2)\} \quad \text{and} \quad \langle (2\,3\,4) \rangle = \{1, (2\,3\,4), (2\,4\,3)\}.$$

So K has a trivial intersection with some subgroup $\langle \tau \rangle$ of order 3. Then since K is normal we know $K\langle \tau \rangle \leq S_4$ having order $3 \cdot 3 = 9$, but this is impossible. Therefore S_4 has no normal subgroup of order 3. □

3.2.15 Exercise 15

Let $G = S_n$ and for fixed $i \in \{1, 2, \ldots, n\}$ let G_i be the stabilizer of i. Prove that $G_i \cong S_{n-1}$.

Proof. Let G act on $\{1, 2, \ldots, n\}$ and fix some i from this latter set. Now suppose $\sigma \in G_i$. We can always write σ as a product of disjoint cycles using the Cycle Decomposition Algorithm presented in Section 1.3. Each of the cycles in the cycle decomposition of sigma must not contain i, since i needs to be stabilized. Therefore G_i consists of all permutations of the set $\{1, 2, \ldots, n\} - \{i\}$, that is it is the permutations of a set with $n - 1$ elements. And it has been shown that, for finite sets A and B, $S_A \cong S_B$ when $|A| = |B|$. Therefore $G_i \cong S_{n-1}$. □

3.2.16 Exercise 16

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

Proof. Let p be a prime. Then

$$(\mathbb{Z}/p\mathbb{Z})^\times = \{\bar{1}, \bar{2}, \bar{3}, \ldots, \overline{p-1}\}.$$

Now either a is a multiple of p or not. If not, then $\bar{a} \in (\mathbb{Z}/p\mathbb{Z})^\times$ and by Lagrange's Theorem and Corollary 9, we know that $|\bar{a}|$ must divide $p-1$. Therefore $\bar{a}^{p-1} = \bar{1}$, so

$$a^{p-1} \equiv 1 \pmod{p},$$

and multiplying both sides by a gives the desired result.

The other possibility is that a and p are not relatively prime. In this case, we have

$$a^p \equiv 0 \equiv a \pmod{p},$$

and the result still holds. □

3.2.17 Exercise 17

Let p be a prime and let n be a positive integer. Find the order of $\bar{p}$ in

$$(\mathbb{Z}/(p^n - 1)\mathbb{Z})^\times$$

and deduce that $n \mid \varphi(p^n - 1)$ (here φ is Euler's function).

Solution. Note that $p^n \equiv 1 \pmod{p^n - 1}$ so $|\bar{p}| \leq n$. On the other hand, if $p^k \equiv 1 \pmod{p^n - 1}$, then $(p^n - 1) \mid (p^k - 1)$ and we see that $k \geq n$. Therefore $|\bar{p}| = n$.

Since $(\mathbb{Z}/(p^n - 1)\mathbb{Z})^\times$ has order $\varphi(p^n - 1)$, we know by Corollary 9 that $n \mid \varphi(p^n - 1)$. □

3.2.18 Exercise 18

Let G be a finite group, let H be a subgroup of G and let $N \trianglelefteq G$. Prove that if $|H|$ and $|G : N|$ are relatively prime then $H \leq N$.

Proof. By Proposition 13 we know that

$$|HN| = \frac{|H||N|}{|H \cap N|}.$$

Now $H \cap N \leq H$, so $|H \cap N|$ divides $|H|$ and we can write

$$|HN| = k|N|,$$

where $k = |H|/|H \cap N|$. But $HN \leq G$ since N is normal in G (Corollary 15), so $k|N|$ divides $|G|$. That is, there is an integer ℓ such that

$$k\ell|N| = |G|, \quad \text{or} \quad k\ell = \frac{|G|}{|N|} = |G : N|.$$

We see that k divides $|G : N|$. But k also divides $|H|$. Since k is a common divisor of two relatively prime numbers, it follows that $k = 1$. Therefore

$$|H| = |H \cap N|$$

and we must have $H = H \cap N$ so that $H \leq N$. □

3.2.19 Exercise 19

Prove that if N is a normal subgroup of the finite group G and $(|N|, |G : N|) = 1$ then N is the unique subgroup of G of order $|N|$.

Proof. Suppose H is a subgroup that also has order $|N|$. Then $|H|$ and $|G : N|$ are relatively prime, so we may apply the result from the previous exercise to conclude that $H \leq N$. And since they have the same order, $H = N$. Therefore N is the only subgroup with order $|N|$. □

3.2.20 Exercise 20

If A is an abelian group with $A \trianglelefteq G$ and B is any subgroup of G prove that $A \cap B \trianglelefteq AB$.

Proof. We know that AB is a subgroup of G by Corollary 15. We want to show that $A \cap B \trianglelefteq AB$. Take any member $ab \in AB$, where $a \in A$ and $b \in B$, and let $c \in A \cap B$. Then

$$(ab)c(ab)^{-1} = abcb^{-1}a^{-1}.$$

Now, since $A \trianglelefteq G$, it follows that $bcb^{-1} \in A$, and since a^{-1} must commute with other members of A, we have

$$(ab)c(ab)^{-1} = a(bcb^{-1})a^{-1} = aa^{-1}(bcb^{-1}) = bcb^{-1}.$$

We know already that $bcb^{-1} \in A$. But bcb^{-1} is also a product of elements from B, so $bcb^{-1} \in A \cap B$. What we have shown is that for all $ab \in AB$,

$$(ab)(A \cap B)(ab)^{-1} \subseteq A \cap B.$$

This proves that $A \cap B \trianglelefteq AB$. □

3.2.21 Exercise 21

Prove that $\mathbb{Q}$ has no proper subgroups of finite index. Deduce that $\mathbb{Q}/\mathbb{Z}$ has no proper subgroups of finite index.

Proof. Suppose $\mathbb{Q}$ does have a proper subgroup of finite index, call it H. Since $\mathbb{Q}$ is abelian, $H \trianglelefteq \mathbb{Q}$. In Exercise 3.1.15 of the previous section, we showed that the quotient of a divisible abelian group by a proper subgroup must also be divisible. And we know $\mathbb{Q}$ is divisible by Exercise 2.4.19, so $\mathbb{Q}/H$ is divisible. But then $\mathbb{Q}/H$ is a finite abelian group that is divisible, and we showed that this was impossible in that same exercise. Therefore H cannot be a proper subgroup of finite index.

We know that $\mathbb{Q}/\mathbb{Z}$ cannot have proper subgroups of finite index for exactly the same reason. □

3.2.22 Exercise 22

Use Lagrange's Theorem in the multiplicative group $(\mathbb{Z}/n\mathbb{Z})^\times$ to prove *Euler's Theorem*: $a^{\varphi(n)} \equiv 1 \pmod{n}$ for every integer a relatively prime to n, where φ denotes Euler's φ-function.

Proof. We know that $(\mathbb{Z}/n\mathbb{Z})^\times$ has order equal to $\varphi(n)$. If a is relatively prime to n, then $\bar{a} \in (\mathbb{Z}/n\mathbb{Z})^\times$ so $|\bar{a}|$ must divide $\varphi(n)$. Therefore $a^{\varphi(n)} \equiv 1 \pmod{n}$. □

3.2.23 Exercise 23

Determine the last two digits of $3^{3^{100}}$.

Solution. Since $100 = 2^2 \cdot 5^2$, we compute

$$\varphi(100) = \varphi(2^2)\varphi(5^2) = (2^2 - 2)(5^2 - 5) = 40.$$

Also, $\varphi(40) = \varphi(2^3)\varphi(5) = 16$.

Now $(3, 16) = 1$, so by Euler's Theorem we know that

$$3^{\varphi(40)} = 3^{16} \equiv 1 \pmod{40}.$$

Therefore

$$\begin{aligned} 3^{100} &= 3^{6\cdot 16+4} \\ &= (3^{16})^6 \cdot 3^4 \\ &\equiv 1^6 \cdot 3^4 \pmod{40} \\ &\equiv 81 \pmod{40} \\ &\equiv 1 \pmod{40}. \end{aligned}$$

This shows that $3^{100} = 1 + 40k$ for some $k \in \mathbb{Z}$.

Since $(3, 100) = 1$, we again have by Euler's Theorem that

$$3^{\varphi(100)} = 3^{40} \equiv 1 \pmod{100}.$$

Therefore

$$\begin{aligned} 3^{3^{100}} &= 3^{1+40k} \\ &= 3 \cdot (3^{40})^k \\ &\equiv 3 \cdot 1^k \pmod{100} \\ &\equiv 3 \pmod{100}. \end{aligned}$$

So the last two digits of $3^{3^{100}}$ in decimal notation are 03. □

3.3 The Isomorphism Theorems

Let G be a group.

3.3.1 Exercise 1

Let F be a finite field of order q and let $n \in \mathbb{Z}^+$. Prove that

$$|GL_n(F) : SL_n(F)| = q - 1.$$

Proof. In Exercise 3.1.35 we saw that $GL_n(F)/SL_n(F) \cong F^\times$. Therefore

$$|GL_n(F) : SL_n(F)| = |GL_n(F)/SL_n(F)| = |F^\times| = q - 1,$$

since $F^\times$ consists of all members of F excluding the 0 element. □

3.3.2 Exercise 2

Prove all parts of the Lattice Isomorphism Theorem.

Proof. First we show that there is a bijection from the set $\mathcal{A}$ of subgroups A of G containing N onto the set $\overline{\mathcal{A}}$ of subgroups $\overline{A} = A/N$ of G/N. Let $\pi\colon G \to G/N$ be the natural projection of G onto G/N. Then define the map $\Phi\colon \mathcal{A} \to \overline{\mathcal{A}}$ by

$$\Phi(A) = \pi(A) = \{aN \mid a \in A\}.$$

That $\Phi(A) \leq G/N$ for any $A \leq G$ is easy to check: $\Phi(A)$ is nonempty since it includes $1N$, and if $a, b \in A$, then

$$(aN)(bN)^{-1} = (ab^{-1})N \in \Phi(A).$$

To show Φ is injective, suppose $\Phi(A) = \Phi(B)$. Let $a \in A$. Then $\pi(a) = \pi(b)$ for some $b \in B$, so $b^{-1}a \in N$ and $a \in bN$. Since $N \leq B$, this shows that $a \in B$ so that $A \subseteq B$. A similar argument will show that $A \supseteq B$ and so $A = B$.

To see that Φ is surjective, let $\overline{A} = A/N$ be a subgroup of G/N. We saw in Exercise 3.1.1 that the complete preimage of a subgroup in G/N is a subgroup of G, so there is $A \in \mathcal{A}$ such that $\Phi(A) = \overline{A}$.

We have shown that Φ is a bijection. Now suppose $A, B \leq G$ with $N \leq A$ and $N \leq B$.

(a) $A \leq B$ if and only if $\overline{A} \leq \overline{B}$.

If $A \leq B$, then every coset of N in A is clearly also a coset of N in B, so that $\overline{A} \leq \overline{B}$. On the other hand, if $\overline{A} \leq \overline{B}$ then for any $a \in A$, we have $aN \in \overline{B}$ so that $b^{-1}a \in N$ for some $b \in B$, which implies $a \in bN \subseteq B$, so $A \leq B$.

(b) If $A \leq B$, then $|B : A| = |\overline{B} : \overline{A}|$.

Every coset bA of A in B corresponds to a coset $\overline{bA}$ of $\overline{A}$ in $\overline{B}$. And every coset $\overline{bA}$ of $\overline{A}$ corresponds to a coset bA of A. It is then easy to check that $bA \mapsto \overline{bA}$ is a bijection from the cosets of A in B onto the cosets of $\overline{A}$ in $\overline{B}$. Therefore

$$|B : A| = |\overline{B} : \overline{A}|.$$

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

$xN \in \overline{\langle A, B\rangle}$ if and only if $x \in \langle A, B\rangle$, if and only if

$$x = x_1 x_2 \cdots x_n, \quad \text{where } x_i \in A \cup B \text{ for each } i.$$

But this is true if and only if

$$xN = (x_1 N)(x_2 N)\cdots(x_n N), \quad x_i N \in \overline{A} \cup \overline{B} \text{ for each } i,$$

if and only if $xN \in \langle \overline{A}, \overline{B}\rangle$. Therefore $\overline{\langle A, B\rangle} = \langle \overline{A}, \overline{B}\rangle$.

(d) $\overline{A \cap B} = \overline{A} \cap \overline{B}$.

$xN \in \overline{A \cap B}$ if and only if $x \in A \cap B$ if and only if $x \in A$ and $x \in B$, and this is true if and only if $xN \in \overline{A}$ and $xN \in \overline{B}$, that is, $xN \in \overline{A} \cap \overline{B}$.

(e) $A \trianglelefteq G$ if and only if $\overline{A} \trianglelefteq \overline{G}$.

Suppose $A \trianglelefteq G$. Then if $g \in G$ and $a \in A$, we have $gag^{-1} \in A$, and

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

Therefore $\overline{A} \trianglelefteq \overline{G}$.

Conversely, suppose $\overline{A} \trianglelefteq \overline{G}$. Then if $\bar{g} \in \overline{G}$ and $\bar{a} \in \overline{A}$, we have

$$\bar{g}\bar{a}\bar{g}^{-1} = (gag^{-1})N \in \overline{A},$$

so $gag^{-1} \in A$. Hence $A \trianglelefteq G$. □

3.3.3 Exercise 3

Prove that if H is a normal subgroup of G of prime index p then for all $K \leq G$ either

(a) $K \leq H$ or

(b) $G = HK$ and $|K : K \cap H| = p$.

Proof. Let H have prime index p as stated. Since $K \leq N_G(H) = G$, we may apply the Second Isomorphism Theorem to see that $KH \leq G$ and $H \trianglelefteq KH$. And $KH = HK$ by Proposition 14. Now consider the index of HK in G.

We know by Exercise 3.2.11 that

$$|G : H| = |G : HK| \cdot |HK : H|.$$

But $|G : H|$ is prime, so there are only two possibilities for $|G : HK|$: Either HK has index 1, in which case $HK = G$, or $|G : HK| = p$. In the latter case, $|HK : H| = 1$ so $H = HK$ which implies that $K \leq H$.

So either $K \leq H$ or $G = HK$. And if $G = HK$, then the Second Isomorphism Theorem tells us that $K/(H \cap K) \cong HK/H$, so

$$|K : H \cap K| = |HK : H| = |G : H| = p.$$ □

3.3.4 Exercise 4

Let C be a normal subgroup of the group A and let D be a normal subgroup of the group B. Prove that

$$(C \times D) \trianglelefteq (A \times B) \quad \text{and} \quad (A \times B)/(C \times D) \cong (A/C) \times (B/D).$$

Proof. Define the map $\varphi\colon A \times B \to (A/C) \times (B/D)$ by

$$\varphi((a, b)) = (aC, bD).$$

This is a homomorphism since

$$\begin{aligned} \varphi((a_1, b_1)(a_2, b_2)) &= \varphi((a_1a_2, b_1b_2)) \\ &= (a_1a_2C, b_1b_2D) \\ &= (a_1C, b_1D)(a_2C, b_2D) \\ &= \varphi((a_1, b_1))\varphi((a_2, b_2)). \end{aligned}$$

Moreover, we can show that $\ker\varphi = C \times D$. For, if $\varphi((a, b)) = (1C, 1D)$, then $a \in C$ and $b \in D$ so that $(a, b) \in C \times D$ and $\ker\varphi \leq C \times D$. On the other hand, if $(c, d) \in C \times D$ then $\varphi((c, d)) = (cC, dD) = (1C, 1D)$ so $\ker\varphi \geq C \times D$. Therefore $\ker\varphi = C \times D$.

We now have, by the First Isomorphism Theorem, that $C \times D \trianglelefteq A \times B$ and $(A \times B)/(C \times D) \cong \varphi(A \times B) = (A/C) \times (B/D)$. □

3.3.5 Exercise 5

Let $QD_{16} = \langle \sigma, \tau \rangle$ be the quasidihedral group described in Exercise 2.5.11. Prove that $\langle \sigma^4 \rangle$ is normal in QD_{16} and use the Lattice Isomorphism Theorem to draw the lattice of subgroups of $QD_{16}/\langle \sigma^4 \rangle$. Which group of order 8 has the same lattice as this quotient? Use generators and relations for $QD_{16}/\langle \sigma^4 \rangle$ to decide the isomorphism type of this group.

Solution. Note that

$$\sigma^4\tau = \tau\sigma^{12} = \tau\sigma^4,$$

so σ^4 commutes with every element of QD_{16}. This is enough to show that $\langle \sigma^4 \rangle \trianglelefteq QD_{16}$.

Using the Lattice Isomorphism Theorem, we draw the lattice for $QD_{16}/\langle \sigma^4 \rangle$ below. We can see that the dihedral group D_8 has the same lattice structure as $QD_{16}/\langle \sigma^4 \rangle$.

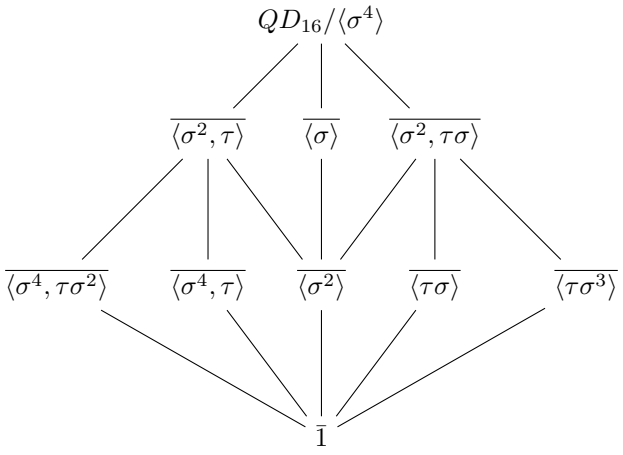
Since

$$\bar{\sigma}^4 = \overline{\sigma^4} = \bar{1}, \qquad \bar{\tau}^2 = \overline{\tau^2} = \bar{1},$$

and

$$\bar{\tau}\bar{\sigma} = \overline{\tau\sigma} = \overline{\sigma^3\tau} = \bar{\sigma}^{-1}\bar{\tau},$$

we see that the generators $\bar{\sigma}$ and $\bar{\tau}$ satisfy the same relations as r and s do in D_8. Therefore $QD_{16}/\langle \sigma^4 \rangle \cong D_8$.



□

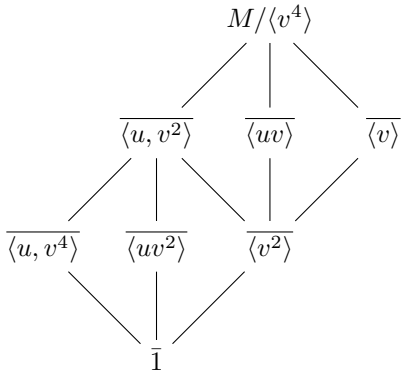
3.3.6 Exercise 6

Let $M = \langle v, u\rangle$ be the modular group of order 16 described in Exercise 2.5.14. Prove that $\langle v^4\rangle$ is normal in M and use the Lattice Isomorphism Theorem to draw the lattice of subgroups of $M/\langle v^4\rangle$. Which group of order 8 has the same lattice as this quotient? Use generators and relations for $M/\langle v^4\rangle$ to decide the isomorphism type of this group.

Solution. Since

$$uv^4 = uv^{20} = v^4u,$$

we see that v^4 commutes with every element of M so that $\langle v^4\rangle \trianglelefteq M$. We get the following lattice.



Notice that the lattice looks similar to the one we constructed for $Z_2 \times Z_4$ in Exercise 2.5.12. We have

$$\bar{u}^2 = \overline{u^2} = \bar{1}, \qquad \bar{v}^4 = \overline{v^4} = \bar{1},$$

and

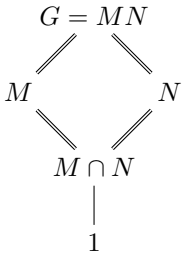
$$\bar{u}\bar{v} = \overline{uv} = \overline{uv^{25}} = \overline{v^5u} = \bar{v}\bar{u}.$$

Since the generators $\bar{u}$ and $\bar{v}$ satisfy the same relations as do a and b in the presentation for $Z_2 \times Z_4$ (given in Exercise 2.5.12), we conclude that $M/\langle v^4 \rangle$ is isomorphic to $Z_2 \times Z_4$. □

3.3.7 Exercise 7

Let M and N be normal subgroups of G such that $G = MN$. Prove that $G/(M \cap N) \cong (G/M) \times (G/N)$.

Solution. We draw the lattice for G, with the double-lines representing the quotient group $G/(M \cap N)$.



Define $\varphi\colon G \to (G/M) \times (G/N)$ by

$$\varphi(g) = (gM, gN).$$

This is a homomorphism since

$$\varphi(ab) = (abM, abN) = (aM, aN)(bM, bN) = \varphi(a)\varphi(b).$$

We also have $\ker \varphi = M \cap N$.

Next, we will show that φ is a surjection. Let $(aM, bN) \in (G/M) \times (G/N)$. Since $G = MN$, we can write $a = m_1 n_1$ and $b = m_2 n_2$ for some $m_1, m_2 \in M$ and $n_1, n_2 \in N$. Then

$$aM = Ma = Mm_1 n_1 = Mn_1 = n_1 M \quad \text{and} \quad bN = m_2 n_2 N = m_2 N.$$

Now

$$\varphi(m_2 n_1) = (Mm_2 n_1, m_2 n_1 N) = (n_1 M, m_2 N) = (aM, bN).$$

So, by the First Isomorphism Theorem, we have

$$G/(M \cap N) \cong (G/M) \times (G/N)$$

as required. □

3.3.9 Exercise 9

Let p be a prime and let G be a group of order $p^a m$, where p does not divide m. Assume P is a subgroup of G of order p^a and N is a normal subgroup of G of order $p^b n$, where p does not divide n. Prove that $|P \cap N| = p^b$ and $|PN/N| = p^{a-b}$. (The subgroup P of G is called a *Sylow p-subgroup* of G. This exercise shows that the intersection of any Sylow p-subgroup of G with a normal subgroup N is a Sylow p-subgroup of N.)

Proof. We know by Lagrange's Theorem that $|PN|$ divides $|G|$, so that

$$|PN| = p^k t \quad \text{where } 0 \leq k \leq a \text{ and } t \mid m.$$

Since $P \leq PN$, we also know that $p^a \mid p^k t$, so that $k = a$. And since $N \leq PN$, we know that $n \mid t$. Therefore

$$|PN/N| = \frac{|PN|}{|N|} = \frac{p^a t}{p^b n} = p^{a-b} s, \quad \text{for some } s \in \mathbb{Z} \text{ with } t = ns.$$

Since N is normal, we may apply the Second Isomorphism Theorem to determine that $PN/N \cong P/P \cap N$. Then

$$|P/P \cap N| = |PN/N| = p^{a-b} s.$$

But $|P|$ must divide $|P/P \cap N|$, so

$$|P/P \cap N| = p^{a-b}.$$

By Lagrange, this implies that

$$|P \cap N| = |P|/p^{a-b} = p^b.$$

So $|PN/N| = p^{a-b}$ and $|P \cap N| = p^b$. □

3.3.10 Exercise 10

Generalize the preceding exercise as follows. A subgroup H of a finite group G is called a *Hall subgroup* of G if its index in G is relatively prime to its order: $(|G : H|, |H|) = 1$. Prove that if H is a Hall subgroup of G and $N \trianglelefteq G$, then $H \cap N$ is a Hall subgroup of N and HN/N is a Hall subgroup of G/N.

Proof. Since $|H|$ divides $|G|$, we can write $|G| = k|H|$ for some integer k, with $(k, |H|) = 1$.

By the formula from Proposition 13, we have

$$|HN| = \frac{|H||N|}{|H \cap N|} = |H| \cdot \frac{|N|}{|H \cap N|}.$$

Since $|HN|$ must divide $|G|$, we have

$$\frac{|N|}{|H \cap N|} \quad \text{divides} \quad k.$$

This tells us that $(|N : H \cap N|, |H|) = 1$. And since $|H \cap N|$ divides $|H|$, we also have

$$(|N : H \cap N|, |H \cap N|) = 1,$$

so that $H \cap N$ is a Hall subgroup of N.

Next, observe that

$$\begin{aligned} |G/N : HN/N| &= \frac{|G|/|N|}{|HN|/|N|} = \frac{|G|}{|HN|} \\ &= \frac{|G|/|H|}{|HN|/|H|} = \frac{|G : H|}{|HN : H|}. \end{aligned}$$

This implies that $|G/N : HN/N|$ divides $|G : H|$. Also,

$$|HN/N| = \frac{|H||N|}{|N||H \cap N|} = \frac{|H|}{|H \cap N|},$$

which shows that $|HN/N|$ divides $|H|$. But $|G : H|$ and $|H|$ are relatively prime, so

$$(|G/N : HN/N|, |HN/N|) = 1.$$

Therefore HN/N is also a Hall subgroup of G/N. □

3.4 Composition Series and the Hölder Program

3.4.1 Exercise 1

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

Proof. Let G be an abelian simple group. Then $|G| > 1$ and we may take some nonidentity element x of G. Now, either $\langle x \rangle \neq G$ or $\langle x \rangle = G$.

In the first case, $\langle x \rangle$ is a nontrivial proper subgroup of G. But G is abelian, so $\langle x \rangle$ must be a normal proper subgroup, which contradicts the fact that G is simple. Hence $\langle x \rangle = G$.

Then G is cyclic. If G has infinite order, then by Theorem 7 of Chapter 2, $\langle x^2 \rangle$ is a nontrivial proper subgroup, again a contradiction. Therefore G has finite order. But then, again by Theorem 7 of Chapter 2, $\langle x^n \rangle$ is a proper subgroup for any proper divisor n of $|G|$. Therefore $|G|$ is prime, and by Theorem 4 of Chapter 2, $G \cong Z_p$. □

3.4.2 Exercise 2

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

Solution. For Q_8, the composition series are

$$1 \trianglelefteq \langle -1 \rangle \trianglelefteq \langle i \rangle \trianglelefteq Q_8,$$
$$1 \trianglelefteq \langle -1 \rangle \trianglelefteq \langle j \rangle \trianglelefteq Q_8,$$

and

$$1 \trianglelefteq \langle -1 \rangle \trianglelefteq \langle k \rangle \trianglelefteq Q_8.$$

Note that each subgroup has index 2 in its containing subgroup, and so must be normal. Each of the composition factors is isomorphic to Z_2.

For D_8, we get the following composition series:

$$1 \trianglelefteq \langle s \rangle \trianglelefteq \langle s, r^2 \rangle \trianglelefteq D_8,$$
$$1 \trianglelefteq \langle r^2 s \rangle \trianglelefteq \langle s, r^2 \rangle \trianglelefteq D_8,$$
$$1 \trianglelefteq \langle r^2 \rangle \trianglelefteq \langle s, r^2 \rangle \trianglelefteq D_8,$$
$$1 \trianglelefteq \langle r^2 \rangle \trianglelefteq \langle r \rangle \trianglelefteq D_8,$$
$$1 \trianglelefteq \langle r^2 \rangle \trianglelefteq \langle rs, r^2 \rangle \trianglelefteq D_8,$$
$$1 \trianglelefteq \langle rs \rangle \trianglelefteq \langle rs, r^2 \rangle \trianglelefteq D_8,$$
$$1 \trianglelefteq \langle r^3 s \rangle \trianglelefteq \langle rs, r^2 \rangle \trianglelefteq D_8.$$

Again, each subgroup is normal within its containing subgroup since they each have index 2. Each composition factor is isomorphic to Z_2. □

3.4.3 Exercise 3

Find a composition series for the quasidihedral group of order 16. Deduce that QD_{16} is solvable.

Solution. Since any subgroup of index 2 is normal, we see from the lattice (Exercise 2.5.11) that

$$1 \trianglelefteq \langle \sigma^4 \rangle \trianglelefteq \langle \sigma^2 \rangle \trianglelefteq \langle \sigma \rangle \trianglelefteq QD_{16}$$

is a composition series. Since each composition factor has order 2 and is thus isomorphic to the abelian group Z_2, we see that QD_{16} is solvable. □

3.4.4 Exercise 4

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

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

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

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

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

3.4.5 Exercise 5

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

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

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

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

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

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

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

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

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

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

Next, note that

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

By the Second Isomorphism Theorem, we then have

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

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

Next, let $N \trianglelefteq G$. For each i, define

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

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

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

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

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

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

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

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

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

Moreover, the Third Isomorphism Theorem says that

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

so the proof will be complete if we can show that N_{i+1}/N_i is abelian.

Let $x, y \in N_{i+1}/N_i$. Then

$$x = (g_0n_0)N_i \quad \text{and} \quad y = (g_1n_1)N_i$$

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

$$\begin{aligned} xyx^{-1}y^{-1} &= (g_0n_0)(g_1n_1)(g_0n_0)^{-1}(g_1n_1)^{-1}N_i \\ &= g_0n_0g_1n_1n_0^{-1}g_0^{-1}n_1^{-1}g_1^{-1}N_i. \end{aligned}$$

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

$$xyx^{-1}y^{-1} = g_0g_1g_0^{-1}g^{-1}n_2N_i.$$

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

$$n_2N_i = n_2NG_i = NG_i = G_iN$$

and we get

$$xyx^{-1}y^{-1} = g_0g_1g_0^{-1}g^{-1}G_iN = G_iN.$$

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

3.4.6 Exercise 6

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

Proof. Let G be a finite group with $G \neq 1$. We want to show that G has a composition series. We will use induction on $|G|$.

First, if $|G| = 2$, then $G \cong Z_2$ and G has the composition series $1 \trianglelefteq G$.

Now suppose $|G| > 2$, and assume that all nontrivial groups with order strictly less than G have a composition series.

If G is simple, then it has the composition series $1 \trianglelefteq G$ and we are done. So assume G is not simple. Let N be a normal subgroup of G, with $N \neq 1$ and $N \neq G$, and choose N so that no other proper normal subgroup has larger order.

Since N is a proper subgroup, it has by the induction hypothesis a composition series

$$1 = G_0 \trianglelefteq G_1 \trianglelefteq G_2 \trianglelefteq \cdots \trianglelefteq G_r = N.$$

Consider the quotient group G/N. If G/N is not simple, then it has a nontrivial proper normal subgroup $\overline{M}$. By the Lattice Isomorphism Theorem, there is a subgroup $M \trianglelefteq G$ with $N < M$, contradicting the fact that N is maximal. So G/N is simple and G has the composition series

$$1 = G_0 \trianglelefteq G_1 \trianglelefteq G_2 \trianglelefteq \cdots \trianglelefteq G_r = N \trianglelefteq G.$$

By induction, the proof is complete. □

3.4.7 Exercise 7

If G is a finite group and $H \trianglelefteq G$, prove that there is a composition series of G, one of whose terms is H.

Proof. Note that if $H = G$ then any composition series for G must contain H as its final term, so it will suffice to prove the statement for proper subgroups $H \triangleleft G$.

If $|G| = 1$, then the result is clear. So suppose $|G| > 1$ and assume that the statement is true for all groups with order strictly smaller than G. Fix a proper normal subgroup $H \triangleleft G$.

Now let N be a maximal proper normal subgroup of G containing H. Then G/N is simple (by the same argument we used in the previous exercise) and $|N| < |G|$. Apply the induction hypothesis to N in order to find a composition series

$$1 = G_0 \trianglelefteq G_1 \trianglelefteq G_2 \trianglelefteq \cdots \trianglelefteq G_r = N \trianglelefteq G,$$

where $H = G_i$ for some i with $0 \leq i \leq r$. Then this is a composition series for G, one of whose terms is H. By induction, the result holds for all finite groups. □

3.4.9 Exercise 9

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

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

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

Proof. First note that $r > 1$ since the existence of M_1 shows that G is not simple.

Let $H = M_1 \cap N_{r-1}$. By Exercise 3.1.24 we know that $H \trianglelefteq M_1$. But $M_1 \cong M_1/1$ is a simple group, so we must have $H = 1$ or $H = M_1$.

If $H = M_1$ then $N_{r-1} \trianglelefteq M_1$. Since M_1 is simple, $N_{r-1} = M_1$ and we must have $r = 2$. In this case, both composition series are exactly the same. So we will suppose that $H = 1$.

Since M_1 and N_{r-1} are normal subgroups of G, their product M_1N_{r-1} is also normal since for $m \in M_1$, $n \in N_{r-1}$, and $g \in G$ we have

$$gmng^{-1} = gm(g^{-1}g)ng^{-1} = (gmg^{-1})(gng^{-1}) \in M_1N_{r-1}.$$

Now if $M_1N_{r-1} \neq G$ then $M_1 \triangleleft M_1N_{r-1} \triangleleft G$. By the Lattice Isomorphism Theorem we can see that $1 = M_1/M_1 \triangleleft M_1N_{r-1}/M_1 \triangleleft G/M_1$. But G/M_1 is simple, so this is impossible. Therefore $M_1N_{r-1} = G$.

By the Second Isomorphism Theorem, we have

$$G/M_1 = M_1N_{r-1}/M_1 \cong N_{r-1}/(M_1 \cap N_{r-1}) = N_{r-1}/H = N_{r-1}/1 \cong N_{r-1}.$$

Since $N_{r-1} \cong G/M_1$, we have that N_{r-1} is simple and $r = 2$.

Moreover, the composition factors in both series are isomorphic, but in the reverse order:

$$G/N_{r-1} \cong (G/1)/(G/M_1) \cong M_1/1 \quad \text{and} \quad N_{r-1}/1 \cong N_{r-1} \cong G/M_1.$$

This completes the proof. □

3.4.10 Exercise 10

Prove part (2) of the Jordan–Hölder Theorem by induction on $\min\{r, s\}$.

Proof. Suppose G has the two composition series

$$1 = N_0 \trianglelefteq N_1 \trianglelefteq N_2 \trianglelefteq \cdots \trianglelefteq N_r = G \tag{3.4}$$

and

$$1 = M_0 \trianglelefteq M_1 \trianglelefteq M_2 \trianglelefteq \cdots \trianglelefteq M_s = G. \tag{3.5}$$

We want to show that $r = s$ and that the composition factors (possibly taken in a different order) are the same up to isomorphism.

As instructed, we will use induction on $\min\{r, s\}$. In Exercise 3.4.9, we have already taken care of the cases where $\min\{r, s\} \leq 2$. Now suppose the statement is true whenever $\min\{r, s\} \leq k$ for some $k \geq 2$.

Let $H = N_{r-1} \cap M_{s-1}$. Note that N_{r-1} cannot be a proper subgroup of M_{s-1} since it would then be a normal subgroup and, after taking quotients, we would have

$$1 \triangleleft M_{s-1}/N_{r-1} \triangleleft G/N_{r-1},$$

contradicting the fact that G/N_{r-1} is simple. For the same reason, M_{s-1} cannot be a proper subgroup of N_{r-1}.

Now consider the case where $M_{s-1} = N_{r-1}$. Then we can apply the induction hypothesis to M_{s-1} to show that $r = s$ and that all composition factors in the two series

$$1 = N_0 \trianglelefteq \cdots \trianglelefteq N_{r-1} \quad \text{and} \quad 1 = M_0 \trianglelefteq \cdots \trianglelefteq M_{s-1}$$

are the same up to isomorphism and reordering. Since $G/M_{s-1} = G/N_{r-1}$, this would complete the inductive step of the proof.

So we will assume that M_{s-1} and N_{r-1} are distinct and that neither is contained in the other. This implies that both subgroups are proper normal subgroups of $M_{s-1}N_{r-1}$. If $M_{s-1}N_{r-1} \neq G$, then we can apply the Lattice Isomorphism Theorem to determine that

$$1 \triangleleft M_{s-1}N_{r-1}/M_{s-1} \triangleleft G/M_{s-1},$$

which contradicts the fact that G/M_{s-1} is simple. Therefore $G = M_{s-1}N_{r-1}$.

Now we may apply the Second Isomorphism Theorem to get

$$G/M_{s-1} = M_{s-1}N_{r-1}/M_{s-1} \cong N_{r-1}/H \tag{3.6}$$

and

$$G/N_{r-1} = M_{s-1}N_{r-1}/N_{r-1} \cong M_{s-1}/H, \tag{3.7}$$

showing that both N_{r-1}/H and M_{s-1}/H are simple.

Now let H have the composition series

$$1 = H_0 \trianglelefteq H_1 \trianglelefteq H_2 \trianglelefteq \cdots \trianglelefteq H_t = H. \tag{3.8}$$

Then

$$1 = H_0 \trianglelefteq H_1 \trianglelefteq \cdots \trianglelefteq H_t = H \trianglelefteq N_{r-1}$$

is a composition series for N_{r-1}. By the induction hypothesis, $t = r-2$ and the composition factors for this series are the same as in the series

$$1 = N_0 \trianglelefteq N_1 \trianglelefteq \cdots \trianglelefteq N_{r-1}$$

in some order.

Similarly,

$$1 = H_0 \trianglelefteq H_1 \trianglelefteq \cdots \trianglelefteq H_t = H \trianglelefteq M_{s-1}$$

is a composition series for M_{s-1}, and by hypothesis, $t = s-2$, and the composition factors are the same as those in the series

$$1 = M_0 \trianglelefteq M_1 \trianglelefteq \cdots \trianglelefteq M_{s-1}$$

in some order. This shows that $s = t+2 = r$.

Moreover, the composition factors in (3.4) and (3.5) are isomorphic in some order: $r-2$ of the factors are isomorphic to the factors in (3.8), and the remaining two factors in each series are also isomorphic but in the reverse order, as shown in (3.6) and (3.7).

By induction, we can conclude that part (2) of the Jordan–Hölder Theorem holds in all cases. □

3.4.12 Exercise 12

Prove (without using the Feit–Thompson Theorem) that the following are equivalent:

(a) every group of odd order is solvable

(b) the only simple groups of odd order are those of prime order.

Proof. First, suppose that every group of odd order is solvable. Let G be a simple group of odd order. Then G is solvable, so G has a chain of subgroups

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

where G_{i+1}/G_i is abelian. But G is simple, so $s = 1$ and G itself is abelian. Since an abelian group of finite order n has a normal subgroup of order d for every d dividing n, it follows that G, which is simple, must have prime order. This completes the proof of the left-to-right implication.

Next, assume that the only simple groups of odd order are those of prime order. Let G be a group of odd order. Now let

$$1 = N_0 \trianglelefteq N_1 \trianglelefteq N_2 \trianglelefteq \cdots \trianglelefteq N_r = G$$

be a composition series for G. Fix an i with $0 \leq i \leq r-1$, and consider the quotient group N_{i+1}/N_i. By Lagrange's Theorem, this quotient group must have odd order (if G has a subgroup of even order then G itself would have even order). But then N_{i+1}/N_i is a simple group of odd order, so by hypothesis it has prime order. But any group of prime order is abelian (Corollary 10), so all the composition factors of G are abelian. Thus G is solvable, completing the proof. □

Appendix A

Cartesian Products and Zorn's Lemma

A.1 Cartesian Products

A.1.1 Exercise 1

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

$$\varphi^*\colon \prod_{i\in I} A \to \prod_{j\in J} A \quad \text{by} \quad \varphi^*(f) = f \circ \varphi \quad \text{for all choice functions } f \in \prod_{i\in I} A.$$

(a) Let $I = \{1, 2\}$, let $J = \{1, 2, 3\}$ and let $\varphi\colon J \to I$ 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^*.

Solution. Suppose f corresponds to the ordered pair (a, b) in A^2. Since φ sends indices 1 and 2 in J to index 2 in I and index 3 in J to index 1 in I, we see that $\varphi^*(f)$ corresponds to the 3-tuple (b, b, a) in A^3. □

(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. φ^* sends the n-tuple $(a_1, a_2, \ldots, a_n)$ in A^n to the n-tuple

$$(a_{\varphi(1)}, a_{\varphi(2)}, \ldots, a_{\varphi(n)})$$

in A^n. □

A.2 Partially Ordered Sets and Zorn's Lemma

A.2.1 Exercise 1

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

Solution. Subsets of A may or may not have upper bounds. For example, take the set of all singleton sets containing integers,

$$X = \{\{1\}, \{2\}, \{3\}, \dots\}.$$

X is a subset of A but it does not have an upper bound since $\mathbb{Z}^+ \notin A$. Any finite subset of A, however, will have an upper bound, namely the union of the sets in the subset. So for example $\{\emptyset, \{1,2\}, \{1,3,5\}\} \subset A$ has the upper bound $\{1,2,3,5\} \in A$.

A does not have any maximal elements, since given any Y in A, we can simply append to the set Y any real number not already in Y, in order to obtain a new finite subset of $\mathbb{R}$ containing Y. A does have a minimal element, however, namely the empty set.

Set inclusion ($\subseteq$) is not a well ordering on A since it is not a total ordering. That is, there exist elements X and Y of A such that $X \not\subseteq Y$ and $Y \not\subseteq X$ (for an example, take $X = \{0\}$ and $Y = \{1\}$). □

A.2.2 Exercise 2

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

Solution. In this case, every subset of A has an upper bound since the union of the sets in the subset is a member of A. A has one maximal element, $\mathbb{R}$ itself, but no minimal elements since, given any set $X \in A$, we may pick some element x in X, so that $X - \{x\}$ is an infinite subset of $\mathbb{R}$ which is contained in X.

This ordering is not a well ordering for the same reason as in the previous exercise: set inclusion $\subseteq$ is not a total ordering on A. For example, take X to be the set of even integers and take Y to be the set of odd integers. Then $X \not\subseteq Y$ and $Y \not\subseteq X$. □

A.2.3 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 $\leq$.

Proof. In each case, $\leq$ is a total ordering. However, it is not a well ordering since in each case there exist nonempty subsets which have no smallest element.

For $\mathbb{R}$, $\mathbb{R}^+$, and $\mathbb{R}^+ \cup \{0\}$ the interval $(0, 1)$ is a subset of each but has no smallest member. For $\mathbb{Z}$, the entire set $\mathbb{Z}$ itself is a subset with no smallest member. □

A.2.4 Exercise 4

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

Proof. Given any two positive integers m and n, we must have either $m \leq n$, $n \leq m$, or both (if $m = n$). Therefore $\leq$ is a total ordering.

Let A be an arbitrary nonempty subset of $\mathbb{Z}^+$. Pick an integer $a \in A$. Then the set $\{1, 2, \ldots, a\} \cap A$ is nonempty and finite. Being finite, it must have a smallest member b. If $c \in A$ is such that $c \leq b$, then certainly $c \leq a$ (by transitivity), so $c \in \{1, 2, \ldots, a\} \cap A$. Since b is the smallest member of this set, we must have $c = b$.

We have shown that $\leq$ is a total ordering such that any nonempty subset of $\mathbb{Z}^+$ has a smallest member. Therefore $\mathbb{Z}^+$ is well ordered under the relation $\leq$. □