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

Greg Kikola

July 1, 2019

Contents

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, 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 m. 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 G. G is obviously nonempty. For any $a+ai$ and $b+bi$ in G, we have

$$(a + ai) - (b + bi) = (a - b) + (a - b)i \in G,$$

so by Proposition 1, $G \leq \mathbb{C}$. □

(b) the set of complex numbers of absolute value 1, i.e., the unit circle in the complex plane (under multiplication)

Proof. Let G denote the complex numbers of absolute value 1, and let $\overline{z}$ denote the conjugate of z. Then G is nonempty and for any $z, w \in G$, we have

$$|zw^{-1}| = |z||w^{-1}| = |z|\frac{|\overline{w}|}{|w|^2} = 1,$$

so $zw^{-1} \in G$. Therefore $G \leq \mathbb{C}^\times$. □

(c) for fixed $n \in \mathbb{Z}^+$ the set of rational numbers whose denominators divide n (under addition)

Proof. Let G denote the subset in question. G is clearly not empty. Let $a, b \in G$ be arbitrary. Then there is $x, y \in \mathbb{Z}$ and $k, \ell \in \mathbb{Z}^+$ so that $a = x/(kn)$ and $b = y/(\ell n)$. Then we have

$$a - b = \frac{x}{kn} - \frac{y}{\ell n} = \frac{\ell x - ky}{\ell kn} = \frac{z}{mn}$$

where $z \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$. Therefore $a - b \in G$ so that $G \leq \mathbb{Q}$. □

(d) for fixed $n \in \mathbb{Z}^+$ the set of rational numbers whose denominators are relatively prime to n (under addition)

Proof. Again, let G denote the subset, which is clearly nonempty. Take a/b and c/d in G, 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 $a/b - c/d \in G$. So $G \leq \mathbb{Q}$. □

(e) the set of nonzero real numbers whose square is a rational number (under multiplication)

Proof. Let G be the set in question, which is clearly nonempty. If $a, b \in G$, then $a^2, b^2 \in \mathbb{Q}$. Then

$$\left(\frac{a}{b}\right)^2 = \frac{a^2}{b^2} \in \mathbb{Q},$$

so $a/b \in G$. Hence $G \leq \mathbb{R}^\times$. □

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. □