Chapter 0 Preliminaries

0.1 Basics

In Exercises 1 to 4 let $\mathcal{A}$ be the set of 2×2 matrices with real number entries. Recall that matrix multiplication is defined by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} p & q \\ r & s \end{pmatrix} = \begin{pmatrix} ap+br & aq+bs \\ cp+dr & cq+ds \end{pmatrix}$$

Let

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

and let

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

Exercise 0.1. Determine which of the following elements of $\mathcal{A}$ lie in $\mathcal{B}$:

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

Proof. This problem is straightforward in that we can determine which of the matrices belong to $\mathcal{B}$ by checking the defining equation of $\mathcal{B}$: simply multiply each matrix first on the right and then on the left by M and check if the two products are equal. The first, third, and fifth matrices are in M.

■

Exercise 0.1.2. Prove that if $P, Q \in \mathcal{B}$, then $P + Q \in \mathcal{B}$ (where $+$ denotes the usual sum of two matrices).

Proof. This statement is that $\mathcal{B}$ is closed under matrix addition. This closure is a direct consequence of the distributivity of matrix multiplication over addition. Let $P, Q \in \mathcal{B}$. Then

$$M(P+Q) = MP + MQ = PM + QM = (P+Q)M$$

so that $P + Q \in \mathcal{B}$.

■

Exercise 0.1.3. Prove that if $P, Q \in \mathcal{B}$, then $P \cdot Q \in \mathcal{B}$ (where $\cdot$ denotes the usual product of two matrices).

Proof. Similar to the previous problem, but now the closure is under matrix multiplication, and is inherited from the associativity of matrix multiplication. Let $P, Q \in \mathcal{B}$. Then

$$M(PQ) = (MP)Q = (PM)Q = P(MQ) = P(QM) = (PQ)M$$

and so $PQ \in \mathcal{B}$.

■

Exercise 0.1.4. Find conditions on p, q, r, s which determine precisely when $\begin{pmatrix} p & q \\ r & s \end{pmatrix} \in \mathcal{B}$.

Proof. To find these conditions, we plug an arbitrary element of $\mathcal{A}$ into the defining equation of $\mathcal{B}$, $MA = AM$, and use this equality to find conditions on the arbitrary element.

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

and

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

Setting these equal to each other gives a system of four linear equations, which are readily solved to obtain $r = 0$ and $s = p$, thus there are two free variables to this solution, and the arbitrary element of $\mathcal{B}$ has the form

$$\begin{pmatrix} p & q \\ 0 & p \end{pmatrix} \quad \text{for} \quad p, q \in \mathbb{R}$$

■

Exercise 0.1.5. Determine whether the following functions f are well defined:

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

Proof.

- This function is not well defined, since $\frac{1}{2} = \frac{2}{4} \in \mathbb{Q}$, and yet

$$f\left(\frac{1}{2}\right) = 1 \neq 2 = f\left(\frac{2}{4}\right)$$

- This function is well defined, and we can see this by letting $\frac{a}{b}, \frac{c}{d}$ be two arbitrary rational numbers which are equal: $\frac{a}{b} = \frac{c}{d}$. Then

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

■

Exercise 0.1.6. Determine whether the function $f : \mathbb{R}^+ \to \mathbb{Z}$ 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.

Proof. This function is not well defined, and we can prove this in the same manner as the last problem – by providing two equal domain elements which map to different elements in the range. For instance, recall that

$$1 = 0.999\ldots = 1.000\ldots \in \mathbb{R}^+$$

However, note that

$$f(0.999\ldots) = 9 \neq 0 = f(1.000\ldots)$$

■

Exercise 0.1.7. Let $f : A \to B$ 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. It is straightforward to show that this relation is an equivalence relation. First, for any $a \in A$ we have $f(a) = f(a)$, and so $a \sim a$, i.e., $\sim$ is reflexive. It is symmetric since, for any $a, b \in A$, we have $f(a) = f(b) \iff f(b) = f(a)$, and so $a \sim b \iff b \sim a$. Lastly, if $a, b, c \in A$ with $a \sim b$ and $b \sim c$, then $f(a) = f(b) = f(c)$, and so $a \sim c$, i.e., $\sim$ is transitive. Hence, $\sim$ is an equivalence relation.

The equivalence class of $\sim$ over arbitrary $a \in A$ is

$$[a] = \{b \in A \mid f(b) = f(a)\}$$

Since f is surjective, any element z of B is $f(a)$ for some $a \in A$. The fiber of f over this arbitrary element of B is then

$$\begin{aligned} f^{-1}(b) = f^{-1}(\{f(a)\}) &= \{b \in A \mid f(b) \in \{f(a)\}\} \\ &= \{b \in A \mid f(b) = f(a)\} \\ &= [a] \end{aligned}$$

Hence, the fibers of the surjective map f are exactly the equivalence sets of the equivalence relation.

■

0.2 Properties of the Integers

Exercise 0.2.1. 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.

- $a = 20, b = 13$. The greatest common divisor can be computed through the Euclidean algorithm (repeated application of the division algorithm):

$$\begin{aligned} 20 &= 13 \cdot 1 + 7 \\ 13 &= 7 \cdot 1 + 6 \\ 7 &= 6 \cdot 1 + 1 \\ 6 &= 1 \cdot 6 \end{aligned}$$

and so $\gcd(20, 13) = 1$. Next, since $\operatorname{lcm}(20, 13) \cdot \gcd(20, 13) = 20 \cdot 13$, we have $\operatorname{lcm}(20, 13) = 20 \cdot 13/1 = 260$. Lastly, we write $\gcd(20, 13) = 1$ as a linear combination (in $\mathbb{Z}$) of 20 and 13 by "reversing" the above steps:

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

- $a = 69, b = 372$.

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

so $\gcd(69, 372) = 3$. Then $\operatorname{lcm}(69, 372) = 69 \cdot 372/3 = 8556$. Lastly,

$$\begin{aligned} 3 &= 15 - 12 \\ &= 15 - (27 - 15) \\ &= 2 \cdot 15 - 27 \\ &= 2(69 - 2 \cdot 27) - 27 \\ &= 2 \cdot 69 - 5 \cdot 27 \\ &= 2 \cdot 69 - 5(372 - 5 \cdot 69) \\ &= 27 \cdot 69 - 5 \cdot 372 \end{aligned}$$

- $a = 792, b = 275$.

$$\begin{aligned} 792 &= 275 \cdot 2 + 242 \\ 275 &= 242 \cdot 1 + 33 \\ 242 &= 33 \cdot 7 + 11 \\ 33 &= 11 \cdot 3 \end{aligned}$$

so $\gcd(792, 375) = 11$. Thus $\operatorname{lcm}(792, 375) = 792 \cdot 375/11 = 99000$. Lastly,

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

- $a = 11391, b = 5673$.

$$\begin{aligned} 11391 &= 5673 \cdot 2 + 45 \\ 5673 &= 45 \cdot 126 + 3 \\ 126 &= 3 \cdot 42 \end{aligned}$$

so $\gcd(11391, 5673) = 3$. Thus $\operatorname{lcm}(11391, 5673) = 11391 \cdot 5673/3 = 21540381$. Lastly,

$$\begin{aligned} 3 &= 5673 - 126 \cdot 45 \\ &= 5673 - 126 \cdot (11391 - 2 \cdot 5673) \\ &= -126 \cdot 11391 + 253 \cdot 5673 \end{aligned}$$

- $a = 1761, b = 1567$.

$$\begin{aligned} 1761 &= 1567 \cdot 1 + 194 \\ 1567 &= 194 \cdot 8 + 15 \\ 194 &= 15 \cdot 12 + 14 \\ 15 &= 14 \cdot 1 + 1 \\ 14 &= 1 \cdot 14 \end{aligned}$$

so $\gcd(1761, 1567) = 1$. Thus $\operatorname{lcm}(1761, 1567) = 1761 \cdot 1567/1 = 2759487$. Lastly,

$$\begin{aligned} 1 &= 15 - 14 \\ &= 15 - (194 - 12 \cdot 15) \\ &= 13 \cdot 15 - 194 \\ &= 13(1567 - 8 \cdot 194) - 194 \\ &= 13 \cdot 1567 - 105 \cdot 194 \\ &= 13 \cdot 1567 - 105(1761 - 1567) \\ &= 118 \cdot 1567 - 105 \cdot 1761 \end{aligned}$$

- $a = 507885, b = 60808$.

$$\begin{aligned} 507885 &= 60808 \cdot 8 + 21421 \\ 60808 &= 21421 \cdot 2 + 17966 \\ 21421 &= 17966 \cdot 1 + 3455 \\ 17966 &= 3455 \cdot 5 + 691 \\ 3455 &= 691 \cdot 5 \end{aligned}$$

so $\gcd(507885, 60808) = 691$. Thus $\operatorname{lcm}(507885, 60808) = 507885 \cdot 60808/691 = 44693880$. Lastly,

$$\begin{aligned}
691 &= 17966 - 5 \cdot 3455 \\
&= 17966 - 5\,(21421 - 17966) \\
&= 6 \cdot 17966 - 5 \cdot 21421 \\
&= 6\,(6080 - 2 \cdot 21421) - 5 \cdot 21421 \\
&= -17 \cdot 21421 + 6 \cdot 6080 \\
&= -17\,(507885 - 8 \cdot 60808) + 6 \cdot 60808 \\
&= -17 \cdot 507885 + 142 \cdot 60808
\end{aligned}$$

Exercise 0.2.2. 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. Let $k, a, b \in \mathbb{Z}$ where $k|a$ and $k|b$. That is, there are integers m, n such that $a = km$ and $b = kn$. Then for any $s, t \in \mathbb{Z}$, $as + bt = kms + knt = k\,(ms + nt)$ and $(ms + nt) \in \mathbb{Z}$ by closure of integer multiplication and addition. Hence we have $k|as + bt$ for any $s, t \in \mathbb{Z}$.

■

Exercise 0.2.3. 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. Let n be composite. Then there is some positive divisor of n which is not 1 or n, say p. Then $n = kp$ for some integer $k \in \mathbb{Z}$. Then certainly $n \mid kp$. We want to show that n does not divide either k or p. Assume by way of contradiction that $n \mid k$. Then there is some r such that $k = rn$. Then $n = kp = rpn$ and so $rp = 1$ but this cannot hold for the product of any two non-identity integers. Thus, n cannot divide k. The same contradiction follows if we assume n divides p. Hence, $n \mid kp$ but not n or p.

■

Exercise 0.2.4. 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

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

are also solutions to $ax + by = N$ (this is in fact the general solution).

Proof. This is easily verified by substitution and simplification via the properties of integer multiplication and addition:

$$\begin{aligned} ax + by &= a\left(x_0 + \frac{b}{d}t\right) + b\left(y_0 - \frac{a}{d}t\right) \\ &= ax_0 + by_0 + \frac{ab}{d}(t - t) \\ &= N + 0 \\ &= N \end{aligned}$$

■

Exercise 0.2.5. Determine the value $\phi(n)$ for each integer $n \leq 30$ where φ denotes the Euler φ-function.

Proof. This can be done by inspection by checking every integer from 1 to 30. We will omit this here.

■

Exercise 0.2.6. Prove the Well Ordering Property of $\mathbb{Z}$ by induction and prove the minimal element is unique.

Exercise 0.2.7. 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. This is the standard argument that $\sqrt{2}$ is not rational, in this case extended to arbitrary prime p.

Assume by way of contradiction that there are nonzero $a, b \in \mathbb{Z}$ with $a^2 = pb^2$. A key point is that we assume that a and b have no common factors; if they do, then we may just divide both sides of this equation by them until they are gone. Then $p|a^2$, since $b^2 \in \mathbb{Z}$. Since p is prime, we know that if $p|a^2$ then $p|a$ or $p|a$. Thus $p|a$, so $a = mp$ for some $m \in \mathbb{Z}$. Then $(mp)^2 = p^2m^2 = pb^2$, i.e., $pm^2 = b^2$, and so $p|b^2$, and thus $p|b$. We now have $p|a$ and $p|b$, but we ensured that a and b had no common factors, so this is a contradiction. Hence, $\sqrt{p}$ is not rational for prime p.

■

Exercise 0.2.8. Let p be a prime, $n \in \mathbb{Z}^+$. Find a formula for the largest power of p which divides $n! = n(n-1)(n-2)\ldots 2 \cdot 1$ (it involves the greatest integer function).

Exercise 0.2.9. Write a computer program to determine the greatest common divisor (a, b) of two integers a and b and two express (a, b) in the form $ax + by$ for some integers x and y.

Exercise 0.2.10. Prove for any given positive integer N there exist only finitely many integers n with $\phi(n) = N$ where ϕ denotes Euler's ϕ-function. Conclude in particular that $\phi(n)$ tends to infinity as n tends to infinity.

Exercise 0.2.11. Prove that if d divides n then $\phi(d)$ divides $\phi(n)$ where ϕ denotes Euler's ϕ-function.

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

Exercise 0.3.1. Write down explicitly all the elements in the residue classes of $\mathbb{Z}/18\mathbb{Z}$.

Proof. The residue classes of $\mathbb{Z}/18\mathbb{Z}$ are the equivalence classes of the integers under the operation of addition mod 18. That is, the classes are the sets of integers which differ by 18. For instance,

$$\overline{0} = \{0, \pm 18, \pm 36, \pm 54, \ldots\} \in \mathbb{Z}/18\mathbb{Z}$$

and

$$\overline{6} = \{\ldots, -30, -12, 6, 24, 42, \ldots\} \in \mathbb{Z}/18\mathbb{Z}$$

and so on for all elements $\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{16}, \overline{17}$.

■

Exercise 0.3.2. Prove that the distinct equivalence classes in $\mathbb{Z}/n\mathbb{Z}$ are precisely $\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}$ (use the Division Algorithm).

Proof. Let $[k] \in \mathbb{Z}$ arbitrary, and $n \in \mathbb{Z}^+$. Then we can use the division algorithm to find some $q, r \in \mathbb{Z}$ such that

$$k = qn + r \quad \text{where} \quad 0 \leq r < |b|$$

From this equation, we see that $k \equiv r \pmod{n}$, and so $[k] = [r] \in \mathbb{Z}/n\mathbb{Z}$ for this $r \in \{0, 1, 2, \ldots, n-1\}$. Hence, any arbitrary equivalence class of $\mathbb{Z}/n\mathbb{Z}$ is one of these classes. These classes are also distinct, because if $[a] = [b]$ for $a, b \in \{0, 1, 2, \ldots, n-1\}$ are any two of them, where without loss of generality $0 \leq a < b < n$, then $n \mid (b-a)$, i.e., there is some $m \in \mathbb{Z}$ with $mn = (b-a)$. But

$$0 \leq a < b < n \implies 0 < b - a < n$$

However, we then have

$$0 < mn < n$$

which is not possible for any $m \in \mathbb{Z}$, and we have a contradiction. Hence, the equivalence classes are distinct. Thus, $\mathbb{Z}/n\mathbb{Z}$ contains n unique elements (the equivalence classes).

■

Exercise 0.3.3. 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) [note that $10 \equiv 1 \pmod{9}$].

Proof. This can be proven by repeated application of the definition of the addition and multiplication of residue classes. We want to determine the remainder of a when divided by 9, i.e., the residue class $\overline{a}$ in $\mathbb{Z}/9\mathbb{Z}$. We have

$$\begin{aligned}\overline{a} &= \overline{a_n 10^n + a_{n-1}10^{n-1} + \cdots + a_1 10 + a_0} \\ &= \overline{a_n 10^n} + \overline{a_{n-1}10^{n-1}} + \cdots + \overline{a_1 10} + \overline{a_0} \\ &= \overline{a_n} \cdot \overline{10^n} + \overline{a_{n-1}} \cdot \overline{10^{n-1}} + \cdots + \overline{a_1} \cdot \overline{10} + \overline{a_0}\end{aligned}$$

Since $\overline{10} = \overline{1}$, we have $\overline{10^k} = \overline{1}$ for every $k \in \mathbb{Z}$. Hence,

$$\begin{aligned}\overline{a} &= \overline{a_n} + \overline{a_{n-1}} + \cdots + \overline{a_1} + \overline{a_0} \\ &= \overline{a_n + a_{n-1} + \cdots + a_1 + a_0}\end{aligned}$$

We conclude that

$$a \equiv a_n + a_{n-1} + \cdots + a_1 + a_0 \mod 9$$

■

Exercise 0.3.4. Compute the remainder when 37^{100} is divided by 29.

Proof. To compute the remainder, we are really seeking $37^{100} \mod 29$. We can use the fact that we can multiply congruences (congruence classes) to simplify this.

$$\begin{aligned}37^1 = 37 &\equiv 8 \mod 29 \\ 37^2 = 1369 &\equiv 6 \mod 29 \\ 37^4 = 1369^2 &\equiv 7 \mod 29 \\ 37^8 \equiv (7 \mod 29)^2 &\equiv 20 \mod 29 \\ 37^{16} &\equiv 23 \mod 29 \\ 37^{32} &\equiv 7 \mod 29 \\ 37^{64} &\equiv 20 \mod 29\end{aligned}$$

and so

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

so that the remainder is 23.

■

Exercise 0.3.5. Compute the last two digits of 9^{1500}.

Proof. The last two digits are extracted by computing $9^{1500} \mod 100$. We proceed

as in the examples and as in the previous problem.

$$\begin{aligned} 9^1 = 9 \equiv 9 \mod 100 \\ 9^2 = 81 \equiv 81 \mod 100 \\ 9^3 = 81^3 = 729 \equiv 29 \mod 100 \\ 9^5 \equiv 81 \cdot 29 \mod 100 \equiv 49 \mod 100 \\ 9^{10} = 9^5 \cdot 9^5 \equiv 49^2 \mod 100 \equiv 1 \mod 100 \end{aligned}$$

Hence, we can see that any exponent $k = 10n$, $n \in \mathbb{Z}$, i.e., a multiple of 10, will return $9^k = (9^10)^n \equiv 1^n \mod 100 \equiv 1 \mod 100$. Thus, we have in particular $9^{1500} \equiv 1 \mod 100$ and so the last two digits of 9^{1500} are 01.

■

Exercise 0.3.6. Prove that the squares of the elements in $\mathbb{Z}/4\mathbb{Z}$ are just $\overline{0}$ and $\overline{1}$.

Proof. Recall that $\mathbb{Z}/4\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$ and that multiplication of these residue classes is defined as $\overline{a} \cdot \overline{b} = \overline{ab}$ where the overline indicates the residue class modulo 4. Thus, we can readily compute the squares:

$$\overline{0} \cdot \overline{0} = \overline{0 \cdot 0} = \overline{0}$$

$$\overline{1} \cdot \overline{1} = \overline{1 \cdot 1} = \overline{1}$$

$$\overline{2} \cdot \overline{2} = \overline{2 \cdot 2} = \overline{0}$$

$$\overline{3} \cdot \overline{3} = \overline{3 \cdot 3} = \overline{1}$$

■

Exercise 0.3.7. 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. From the last problem, the square of any integer is either congruent modulo 4 to 0 or 1, and so the sum of two such squares is at most congruent to 2. Thus, there will be no remainder 3 when dividing a sum of two squares by 4.

■

Exercise 0.3.8. Prove that the equation $a^2 + b^2 = 3c^2$ has no solutions in nonzero integers a, b and c. [Consider the equation mod 4 as in the previous two exercises and show that a, b and c would all have to be divisible by 2. The each of a^2, b^2 and c^2 has a factor of 4 and by dividing through by 4 show that there would be a smaller set of solutions to the original equation. Iterate to reach a contradiction.]

Exercise 0.3.9. Prove that the square of any odd integer always leaves a remainder of 1 when divided by 8.

Proof. This can be proven by just looking at what any product of odd numbers would look like. Let $n = 2k + 1$ with $k \in \mathbb{Z}$ be an arbitrary odd integer. Its square is $n^2 = 4k(k+1) + 1$. Note that $k(k+1)$ is always even, since either k or $k+1$ is even and the product of an even and an odd number is even. Thus, $k(k+1) = 2m$ for some $m \in \mathbb{Z}$. Thus, we have $n^2 = 4 \cdot 2m + 1 = 8m + 1$ so that upon division by 8 we have a remainder of 1.

Alternately, we can look at the residue classes in $\mathbb{Z}/8\mathbb{Z}$ under multiplication. Note that since these classes partition $\mathbb{Z}$, every integer is in one of these classes. An odd integer is certainly an odd integer away from a multiple of 8, so any odd integer is in one of the residue classes $\overline{1}, \overline{3}, \overline{5}$, or $\overline{7}$. By squaring each of these elements, we have

$$\overline{1} \cdot \overline{1} = \overline{1}$$

$$\overline{3} \cdots \overline{3} = \overline{1}$$

$$\overline{5} \cdot \overline{5} = \overline{1}$$

$$\overline{7} \cdot \overline{7} = \overline{1}$$

Thus, the square of any odd integer is equivalent to 1 modulo 8, i.e., the remainder of division of a square of an odd integer by 8 is 1.

■

Exercise 0.3.10. Prove that the number of elements of $(\mathbb{Z}/n\mathbb{Z})^\times$ is $\phi(n)$ where ϕ denotes the Euler ϕ-function.

Proof. Recall that $(\mathbb{Z}/n\mathbb{Z})^\times$ is the subset of $\mathbb{Z}/n\mathbb{Z}$ of all elements with multiplicative inverses. Proposition 4 states that we have the alternate expression

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{\overline{a} \in \mathbb{Z}/n\mathbb{Z} \mid (a, n) = 1\}$$

That is, these elements are exactly those residue classes whose representative elements in $[0, \ldots, n-1]$ and n are relatively prime. Certainly, the number of these elements is $\varphi(n)$, the Euler ϕ-function applied to n.

Note that we use Proposition 4 without proof. We could be more thorough by proving that this expression of $(\mathbb{Z}/n\mathbb{Z})^\times$ is equivalent to the original definition. Let $\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^\times$ so that there is some $\overline{c} \in \mathbb{Z}/n\mathbb{Z}$ such that $\overline{a} \cdot \overline{c} = \overline{1}$. That is, $ac = kn + 1$ for some $k \in \mathbb{Z}$. Rearranging, we have $ac - kn = 1$. Assume by way of contradiction that there is some divisor m of both a and n. Then note that $m \mid ac - kn$, but then $m \mid 1$ and so $m = 1$. Hence, the only positive divisor of both a and n is 1, so $(a, n) = 1$.

Conversely, assume that $(a, n) = 1$. Then by the Euclidean algorithm, we can write 1 as a linear combination of a and n as $1 = ja + kn$ so that $ja = 1 - kn$ for some integers j, k. Then we have ja is representative of $\overline{1}$, so j and a are multiplicative inverses modulo n.

■

Exercise 0.3.11. Prove that if $\overline{a}, \overline{b} \in (\mathbb{Z}/n\mathbb{Z})^\times$, then $\overline{a} \cdot \overline{b} \in (\mathbb{Z}/n\mathbb{Z})^\times$.

Proof. If $\overline{a}, \overline{b} \in (\mathbb{Z}/n\mathbb{Z})^\times$, then a and b have multiplicative inverses modulo n, say c and d respectively. Then we have $\overline{a} \cdot \overline{c} = \overline{b} \cdot \overline{d} = \overline{1}$. We can write

$$\begin{aligned} 1 &= 1 \cdot 1 \\ &= (\overline{a} \cdot \overline{c}) \cdot \left(\overline{b} \cdot \overline{d}\right) \\ &= \left(\overline{a} \cdot \overline{b}\right) \cdot \left(\overline{c} \cdot \overline{d}\right) \end{aligned} \tag{1}$$

so we see that the multiplicative inverse of $\overline{a} \cdot \overline{b}$ modulo n is $\overline{c} \cdot \overline{d}$ and $\overline{a} \cdot \overline{b} \in (\mathbb{Z}/n\mathbb{Z})^\times$. Note that we assume the associativity of multiplication of residue classes, but it is pretty easy to convince oneself of these.

■

Exercise 0.3.12. 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. Assume that the hypotheses hold. If a and n are not relatively prime, then there is some $k = (a, n) > 1$. Then $k \mid n$ and so $b = \frac{n}{k} \in \mathbb{Z}$ and $1 \leq b < n$. Then notice that

$$ab = a\frac{n}{k} = n\frac{a}{k}$$

so that $n \mid ab$, i.e., $ab \equiv 0 \pmod{n}$.

Next, if $ac \equiv 1 \pmod{n}$, then $abc \equiv b \pmod{n}$, but since $ab \equiv 0 \pmod{n}$, we must have $abc \equiv 0 \pmod{n}$. Thus, we need $b \equiv 0 \pmod{n}$, but we know this is not true by our construction of b. Hence, no such c can exist.

■

Exercise 0.3.13. 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 relatively prime then there is an integer c such that $ac \equiv 1 \pmod{n}$ [use the fact that the g.c.d. of two integers is a $\mathbb{Z}$-linear combination of the integers].

Proof. As the hint suggests, we know that for a and n relatively prime we have $(a, n) = 1$ and we can expresses this as some linear combination $ac + nd = 1$ for $c, d \in \mathbb{Z}$. But then we can rearrange this as $ac = 1 - nd$, that is, we have $ac \equiv 1 \pmod{n}$.

■

Exercise 0.3.14. Conclude from the previous two exercises that $(\mathbb{Z}/n\mathbb{Z})^\times$ is the set of elements $\overline{a}$ of $\mathbb{Z}/n\mathbb{Z}$ with $(a, n) = 1$ and hence prove Proposition 4. Verify this directly in the case $n = 12$.

Proof. Proposition 4 claims that the set $(\mathbb{Z}/n\mathbb{Z})^\times$, which is defined as the set of all residue classes $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$ with multiplicative inverses, is the same as the subset of elements of $\mathbb{Z}/n\mathbb{Z}$ whose representative elements are relatively prime to n.

Exercise 13 proves that if a representative element and n are relatively prime, then that element's residue class has a multiplicative inverse; this shows one direction of the set equality. For the other direction, the contrapositive is proven in Exercise 12, where for a and n *not* relatively prime, we cannot have an inverse residue class for $\overline{a}$; that is, that we have a multiplicative inverse implies that a and n are relatively prime. We can thus conclude that the sets are one and the same.

For the case $n = 12$, we can construct a multiplication table (for residue class representative elements) and we should observe that the only elements with multiplicative inverses are those which are relatively prime to $n = 12$.

	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	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	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	1	8	3	10	5
8	0	8	4	0	8	4	0	8	4	0	8	4
9	0	9	6	3	0	9	6	3	0	9	6	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	1

(2)

By inspection of this table, the only elements which have a multiplicative inverse (elements whose rows/cols contain a 1) are 1, 5, 7, and 11. These are the exactly the positive integers less than $n = 12$ which are relatively prime to 12.

■

Exercise 0.3.15. 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 $\overline{a}$ in $\mathbb{Z}/n\mathbb{Z}$.

- $a = 13, n = 20$.
- $a = 69, n = 89$.
- $a = 1891, n = 3797$.
- $a = 6003722857, n = 77695236973$. [The Euclidean Algorithm requires only 3 steps for these integers.]

Proof. As suggested, the Euclidean Algorithm can be used to determine the gcd of the two integers, and we can sort of "work backward" to determine the inverses. Since this working backward allows us to compute the linear combination $ax+ny = (a,n)$, then we have $ax \equiv (a,n) \mod n$. Thus, if $(a,n) = 1$, i.e., they are relatively prime, then a and x are multiplicative inverses (as equivalence classes in $\mathbb{Z}/n\mathbb{Z}$).

- We follow Euclid's Algorithm:

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

so $(13, 20) = 1$. We can work backward from the identity element to construct the inverse of $\overline{a}$:

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

so that $\overline{13}^{-1} = \overline{-3}$ in $\mathbb{Z}/20\mathbb{Z}$. This can be verified directly: $\overline{13} \cdot \overline{-3} = \overline{-3 \cdot 13} = \overline{-39} = \overline{1}$.

- Next, we have

$$\begin{aligned} 89 &= 1 \cdot 69 + 20 \\ 69 &= 3 \cdot 20 + 9 \\ 20 &= 2 \cdot 9 + 2 \\ 9 &= 4 \cdot 2 + 1 \\ 2 &= 2 \cdot 1 \end{aligned}$$

so $(69, 89) = 1$. Then we have

$$\begin{aligned} 1 &= 9 - 4 \cdot 2 \\ &= 9 - 4\,(20 - 2 \cdot 9) \\ &= 9 \cdot 9 - 4 \cdot 20 \\ &= 9\,(69 - 3 \cdot 20) - 4 \cdot 20 \\ &= 9 \cdot 69 - 31 \cdot 20 \\ &= 9 \cdot 69 - 31\,(89 - 69) \\ &= 40 \cdot 69 - 31 \cdot 89 \end{aligned}$$

so that $\overline{69}^{-1} = \overline{40}$ in $\mathbb{Z}/89\mathbb{Z}$.

- Next, we have

$$\begin{aligned} 3797 &= 2 \cdot 1891 + 15 \\ 1891 &= 126 \cdot 15 + 1 \\ 15 &= 15 \cdot 1 \end{aligned}$$

so that $(1891, 3797) = 1$. Then we have

$$\begin{aligned} 1 &= 1891 - 126 \cdot 15 \\ &= 1891 - 126\,(3797 - 2 \cdot 1891) \\ &= 253 \cdot 1891 - 126 \cdot 3797 \end{aligned}$$

so that $\overline{1891}^{-1} = \overline{253}$ in $\mathbb{Z}/3797\mathbb{Z}$.

- Next, we have

$$\begin{aligned} 77695236973 &= 12 \cdot 6003722857 + 5650562689 \\ 6003722857 &= 1 \cdot 5650562698 + 353160168 \\ 5650562698 &= 16 \cdot 353160168 + 1 \\ 353160168 &= 353160168 \cdot 1 \end{aligned}$$

so that $(6003722857, 77695236973) = 1$. In reverse, we have

$$\begin{aligned} 1 &= 5650562698 - 16 \cdot 353160168 \\ &= 5650562698 - 16\,(6003722857 - 5650562698) \\ &= 17 \cdot 5650562698 - 16 \cdot 6003722857 \\ &= 17\,(77695236973 - 12 \cdot 6003722857) - 16 \cdot 6003722857 \\ &= -220 \cdot 6003722857 + 17 \cdot 77695236973 \end{aligned}$$

so that the multiplicative inverse of $\overline{a}$ in $\mathbb{Z}/n\mathbb{Z}$ is $\overline{-220}$.

■

Exercise 0.3.16. Write a computer program to add and multiply mod n, for any n given as input. The output of these operations should be the least residues of the sums and products of two integers. Also include the feature that if $(a, n) = 1$, an integer c between 1 and $n - 1$ such that $\overline{a} \cdot \overline{c} = \overline{1}$ may be printed on request. (Your program should not, of course, simply quote "mod" functions already built into many systems).

Chapter 1 Introduction to Groups

Sec. 1.1 Basic Axioms and Examples

Let G be a group.

Exercise 1.1.1. Determine which of the following binary operations are associative:

- the operation $\star$ on $\mathbb{Z}$ defined by $a \star b = a - b$
- the operation $\star$ on $\mathbb{R}$ defined by $a \star b = a + b + ab$
- the operation $\star$ on $\mathbb{Q}$ defined by $a \star b = \frac{a+b}{5}$
- the operation $\star$ on $\mathbb{Z} \times \mathbb{Z}$ defined by $(a, b) \star (c, d) = (ad + bc, bd)$
- the operation $\star$ on $\mathbb{Q} - \{0\}$ defined by $a \star b = \frac{a}{b}$.

Proof.
- Not associative. If $a, b, c \in \mathbb{Z}$, then $a \star (b \star c) = a \star (b - c) = a - b + c$ but $(a \star b) \star c = (a - b) \star c = a - b - c$.
- Associative. If $a, b, c \in \mathbb{Z}$, then we can show $a \star (b \star c) = (a \star b) \star c$.
- Not associative. If $a, b, c \in \mathbb{Z}$, then $a \star (b \star c) = \frac{a}{5} + \frac{b}{25} + \frac{c}{25}$, but $(a \star b) \star c = \frac{a}{25} + \frac{b}{25} + \frac{c}{5}$.
- Associative. I will skip the details, but this is shown easily in the usual way.
- Not associative. Let $a = 8, b = 4$, and $c = 2$; then $a \star (b \star c) = 8 \star (4 \star 2) = 8 \star 2 = 4$, but $(a \star b) \star c = (8 \star 4) \star 2 = 2 \star 2 = 1$.

■

Exercise 1.1.2. Decide which of the binary operations in the preceding exercise are commutative.

Proof. Commutativity of these functions is easier than associativity to ascertain. In these cases, we can check by inspection.

- Not commutative; in fact, $a \star b = -b \star a$, that is, it is anticommutative.
- Commutative.
- Commutative.
- Commutative.
- Not commutative.

■

∎

Exercise 1.1.3. Prove that addition of residue classes in $\mathbb{Z}/n\mathbb{Z}$ is associative (you may assume it is well defined).

Proof. Recall that addition of residue classes (elements of $\mathbb{Z}/n\mathbb{Z}$) is defined by

$$\overline{a} + \overline{b} = \overline{a+b}$$

for all $a, b \in \mathbb{Z}$. This is exactly the operation of addition $\bmod n$.

Let $a, b, c \in \mathbb{Z}$. Then

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

Note that this works because of the associativity of integer addition (under the overline).

∎

Exercise 1.1.4. Prove that multiplication of residue classes in $\mathbb{Z}/n\mathbb{Z}$ is associative (you may assume it is well defined).

Proof. This is very similar to the previous problem. Multiplication of residue classes $\overline{a}, \overline{b} \in \mathbb{Z}/n\mathbb{Z}$ is defined by

$$\overline{a} \cdot \overline{b} = \overline{ab}$$

Thus, for $a, b, c \in \mathbb{Z}/n\mathbb{Z}$, we have

$$\begin{aligned}\left(\overline{a} \cdot \overline{b}\right) \cdot \overline{c} &= \overline{ab} \cdot \overline{c} \\ &= \overline{(ab)\,c} \\ &= \overline{a\,(bc)} \\ &= \overline{a} \cdot \overline{bc} \\ &= \overline{a} \cdot \left(\overline{b} \cdot \overline{c}\right)\end{aligned}$$

This time, it works because of the associativity of integer multiplication.

∎

Exercise 1.1.5. Prove for all $n > 1$ that $\mathbb{Z}/n\mathbb{Z}$ is not a group under multiplication of residue classes.

What is the difference between this set under multiplication and this set under addition? When we make this into a multiplicative group, we must remove the (additive) zero element. Thus, we expect it to be problematic.

Proof. Consider $G = \mathbb{Z}/n\mathbb{Z}$ with $n > 1$. Then we know there are at least the equivalence classes $\overline{0}$ and $\overline{1}$. Note that $\overline{0}$ cannot be the multiplicative identity element, since $\overline{0} \cdot \overline{1} = \overline{0 \cdot 1} = \overline{0} \neq \overline{1}$. Assume $\overline{0}$ has some inverse element, say $\overline{a}$. Then $\overline{0} \cdot \overline{a} = \overline{0 \cdot a} = \overline{0}$, but $\overline{0}$ is not the identity element. Hence, $\overline{0}$ cannot have an inverse in G, and so G is not a group under multiplication of residue classes. ■

Exercise 1.1.6. Determine which of the following sets are groups under addition:

- the set of rational numbers (including $0 = 0/1$) in lowest terms whose denominators are odd
- the set of rational numbers (including $0 = 0/1$) in lowest terms whose denominators are even
- the set of rational numbers of absolute values < 1
- the set of rational numbers of absolute value ≥ 1 together with 0
- the set of rational numbers with denominators equal to 1 or 2
- the set of rational numbers with denominators equal to $1, 2$ or 3

Proof.

- This is a group. The (additive) identity $0 \in \mathbb{Q}$ is contained, and the inverse of any q in the set is clearly $-q$, in the set. Addition is associative since usual rational addition is associative. Lastly — and perhaps it should be firstly — we must ensure that the set is closed under the operation. Let $\frac{p_1}{q_1}, \frac{p_2}{q_2}$ be in the set. Then the sum is

$$\frac{p_1}{q_1} + \frac{p_2}{q_2} = \frac{p_1 q_2 + p_2 q_1}{q_1 q_2} = \frac{p}{q}$$

  where $\frac{p}{q}$ is the sum in lowest terms, i.e., with common factors eliminated. Then it remains to show that q is odd. Assume by way of contradiction that q is even. Then since q is a factorization of $q_1 q_2$, $q | q_1 q_2$. Since q even, $q = 2k$ for some $k \in \mathbb{Z}$; thus, $2k | q_1 q_2$, i.e., $2km = q_1 q_2$ for some $m \in \mathbb{Z}$, but then $q_1 q_2$ is even. However, the product of two odd integers is certainly odd, so this is a contradiction. Thus, q must be odd and so the set is closed under the operation of rational addition. This is a group.

- Clearly not a group, since $\frac{1}{2}$ is in this set but $\frac{1}{2} + \frac{1}{2} = \frac{1}{1}$ is not, so the group is not closed.

- Not a group, since it is not even closed under the group operation. For

instance $\frac{1}{2}+\frac{1}{2}=1>1$.

- Not a group, since it is not closed. Note that $\frac{2}{1},-\frac{3}{2}$ are in the set, but $\frac{2}{1}-\frac{3}{2}=\frac{1}{2}$ is not in the set.
- This is a group, but it takes some doing to show it. Consider two arbitrary elements in the set. We have four cases: $\frac{a}{1},\frac{b}{1}$; $\frac{a}{2},\frac{b}{1}$; $\frac{a}{1},\frac{b}{2}$; $\frac{a}{2},\frac{b}{2}$ where $a,b\in\mathbb{Z}$ and we assume these rational numbers are in reduced form. Then

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

which is certainly still in the set. The next case is

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

Now, if $a+2b$ is odd, then the denominator is 2; if $a+2b$ is even, then we can cancel the factor of 2 in the denominator and we get a denominator of 1 in the most reduced form, thus this sum is still in the set.

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

is certainly still in the set by the symmetry of the sum and the previous case. Last,

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

and this is again in the set, for the same reason as the past two cases.

- This is not a group, even though it is very similar to the previous case. This issue now is that, previously, adding two rationals only involved making the denominators equal to 1 or 2, and then reducing the sums could only change a 2 denominator to a 1. Now, we may have a denominator which is $1,2,3$, or 6, and we may not be able to reduce it any further. For instance, $-\frac{1}{2}$ and $\frac{4}{3}$ are in the set, but $-\frac{1}{2}+\frac{4}{3}=\frac{-3+8}{6}=\frac{5}{6}$ is not in the set, so it is not closed. ■

Exercise 1.1.7. Let $G=\{x\in\mathbb{R}\,|\,0\le x<1\}$ 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 I).

Proof. Let G and $\star$ be defined as in the problem statement. We want to first show that $\star$ is a well defined binary operation, that is, that G is closed under $\star$. Let $x,y\in G$. Then $x\star y=x+y-\lfloor x+y\rfloor$. Since $x,y<1$, we know that $x+y<2$ and so $\lfloor x+y\rfloor\in\{0,1\}$. We can look at this in three cases. If $0=x+y$, then $x\star y=0$ and so $x\star y\in G$. If $0<x+y<1$, then $\lfloor x+y\rfloor=0$ and so $x\star y=x+y<1$,

and so $x \star y \in G$. Lastly, if $1 \leq x + y < 2$, then $\lfloor x + y \rfloor = 1$ and $x \star y = x + y - 1$ so $0 \leq x \star y < 1$, and so $x \star y \in G$. Thus, in all cases G is closed under the binary operation of $\star$.

We must next show that the group axioms are satisfied. First, though, we can easily verify that G is abelian (commutative) since this is obvious by inspection of the operation of $\star$. Next, the identity axiom is satisfied: $0 \in G$ is the identity element, since for any $x \in G$, $x \star 0 = x + 0 + \lfloor x + 0 \rfloor = x + 0 = x$ and $x \star 0 = 0 \star x$ by commutativity. Inverses are also easily constructed. For $x \in G - \{0\}$, $-x = 1 - x$. This is easily seen:

$$x \star (1 - x) = x + (1 - x) - \lfloor x + 1 - x \rfloor = 1 - \lfloor 1 \rfloor = 0$$

and $(1 - x) \star x = 0$ by commutativity.

Associativity is the most complex part of this proof, and we again consider several cases. Let $x, y, z \in G$. First, consider $x + y < 1$ and $y + z < 1$. Then

$$\begin{aligned} x \star (y \star z) &= x \star (y + z - \lfloor y + z \rfloor) \\ &= x \star (y + z) \\ &= x + (y + z) - \lfloor x + (y + z) \rfloor \\ &= (x + y) + z - \lfloor (x + y) + z \rfloor \\ &= (x + y) \star z \\ &= (x + y - \lfloor x + y \rfloor) \star z \\ &= (x \star y) \star z \end{aligned}$$

Next, consider $1 \leq x + y$ and $1 \leq y + z$. Then

$$\begin{aligned} x \star (y \star z) &= x \star (y + z - \lfloor y + z \rfloor) \\ &= x \star (y + z - 1) \\ &= x + (y + z - 1) - \lfloor x + (y + z - 1) \rfloor \\ &= x + y + z - 1 - \lfloor x + y + z - 1 \rfloor \\ &= (x + y - 1) + z - \lfloor (x + y - 1) + z \rfloor \\ &= (x + y - \lfloor x + y \rfloor) \star z \\ &= (x \star y) \star z \end{aligned}$$

Next, consider $x+y<1$ and $1\leq y+z$. Then $\lfloor x+y\rfloor=0$ and we have

$$\begin{aligned}x\star(y\star z)&=x\star(y+z-\lfloor y+z\rfloor)\\&=x\star(y+z-1)\\&=x+(y+z-1)-\lfloor x+(y+z-1)\rfloor\\&=(x+y)+z-1+1-\lfloor(x+y)+z\rfloor\\&=(x+y)+z-\lfloor(x+y)+z\rfloor\\&=(x+y-\lfloor x+y\rfloor)+z-\lfloor(x+y-\lfloor x+y\rfloor)+z\rfloor\\&=(x+y-\lfloor x+y\rfloor)\star z\\&=(x\star y)\star z\end{aligned}$$

Lastly, consider the case $1\leq x+y$ and $y+z<1$. Then

$$\begin{aligned}x\star(y\star z)&=x\star(y+z-\lfloor y+z\rfloor)\\&=x+(y+z-\lfloor y+z\rfloor)-\lfloor x+y+z-\lfloor y+z\rfloor)\\&=(x+y-\lfloor x+y\rfloor)+z+1-\lfloor(x+y-\lfloor x+y\rfloor)+1+z\rfloor\\&=(x+y-\lfloor x+y\rfloor)+z-\lfloor(x+y-\lfloor x+y\rfloor)+1\rfloor\\&=(x+y-\lfloor x+y\rfloor)\star z\\&=(x\star y)\star z\end{aligned}$$

and so in all cases we have this operation associative. Finally, we can conclude that this is, indeed, a group.

■

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

- Prove that G is a group under multiplication (called the group of roots of unity in $\mathbb{C}$).
- Prove that G is not a group under addition.

Proof. • The identity of G is 1, which is easily shown: if $z\in G$, then $1z=z$ and $1^1=1$, so $1\in G$. Let $z\in G$. Then $z^n=1$ for some $n\in\mathbb{Z}^+$. The complex inverse, $\frac{\overline{z}}{z\overline{z}}$, where $\overline{z}$ is the complex conjugate of z, is the multiplicative inverse of z:

$$z\frac{\overline{z}}{z\overline{z}}=\frac{z\overline{z}}{z\overline{z}}=1$$

Further, we can show that this number is in G:

$$1=1^n=\left(z\frac{\overline{z}}{z\overline{z}}\right)^n=z^n\left(\frac{\overline{z}}{z\overline{z}}\right)^n=1\left(\frac{\overline{z}}{z\overline{z}}\right)^n=\left(\frac{\overline{z}}{z\overline{z}}\right)^n$$

hence this inverse is a root of unity, and so it is in G. Lastly, multiplication of elements of G is associative since multiplication of complex numbers is associative (G inherits this property from $\mathbb{C}$). Hence, G is a group under multiplication.

- We can show that this is not a group under addition by providing a counterexample. In this case, it is easy: note that $1 \in G$ since $1^1 = 1$, but $1 + 1 = 2 \notin G$ since $2^n \neq 1$.

■

Exercise 1.1.9. Let $G = \left\{a + b\sqrt{2} \in \mathbb{R} \,|\, a, b \in \mathbb{Q}\right\}$.

- Prove that G is a group under addition.
- Prove that the nonzero elements of G are a group under multiplication. ["Rationalize the denominators" to find multiplicative inverses.]

Proof.

- G is obviously closed under the binary operation of usual rational addition: if $a + b\sqrt{2}, c + d\sqrt{2} \in G$, then $\left(a + b\sqrt{2}\right) + \left(c + d\sqrt{2}\right) = (a + c) + (b + d)\sqrt{2} \in G$. The identity element of the group is $0 = 0 + 0\sqrt{2} \in G$, and an inverse for any $a + b\sqrt{2} \in G$ is $-a - b\sqrt{2} \in G$. Associativity is easily inherited from addition of the rational numbers. As an added bonus, this group is abelian (also inherited from addition on $\mathbb{Q}$).
- Next, consider the nonzero elements of G under multiplication. The identity element is $1 = 1 + 0\sqrt{2} \in G$. The inverse of $a + b\sqrt{2} \in G$ is $\frac{a - b\sqrt{2}}{a^2 - 2b^2} \in G$. Note that this is truly in G (since the numerator can never be zero with $a, b \in \mathbb{Q}$) and it is well-defined since $a^2 = 2b^2 \implies a = b\sqrt{2}$ but the only rational a, b satisfying this are $0, 0$, and we assumed this was not the case. Again, associativity follows from associativity of rational multiplication, and is easy to show.

■

Exercise 1.1.10. Prove that a finite group is abelian if and only if its group table is a symmetric matrix.

Proof. As defined in the text, the group table for group G with n elements is the $n \times n$ array M whose i, j entry, M_{ij}, is the group element (product) $g_i g_j$. Thus, if G abelian, then

$$M_{ij} = g_i g_j = g_j g_i = M_{ij}$$

and so M is symmetric. Conversely, if M symmetric, then let $g_i, g_j \in G$. Then

$$g_i g_j = M_{ij} = M_{ji} = g_j g_i$$

Since this holds for arbitrary i, j, G is abelian.

■

Exercise 1.1.11. Find the orders of each element of the additive group $\mathbb{Z}/12\mathbb{Z}$.

Proof. The group consists of the residue (equivalence) classes

$$\mathbb{Z}/12\mathbb{Z} = \left\{\overline{0}, \overline{1}, \ldots, \overline{10}, \overline{11}\right\}$$

The orders of the various elements are easily determined by iteratively adding the element to itself until the identity element, $\overline{0}$, is reached. For instance, $4^1 = 4$, $4^2 = 8$, $4^3 = 0$ and so $\left|\overline{4}\right| = 3$.

$$|0| = 0,\ |1| = |5| = |7| = |11| = 12,\ |2| = |10| = 6$$

$$|3| = |9| = 4,\ |4| = |8| = 3,\ |6| = 2$$

■

Exercise 1.1.12. Find the orders of the following elements of the multiplicative group $(\mathbb{Z}/12\mathbb{Z})^\times$: $\overline{1}, \overline{-1}, \overline{5}, \overline{7}, \overline{-7}, \overline{13}$.

Proof. Recall that $(\mathbb{Z}/12\mathbb{Z})^\times$ is the set of residue classes of elements of $\mathbb{Z}/12\mathbb{Z}$ which have multiplicative inverses. This problem is similar to the previous problem, but now the group operation is multiplication of residue classes. Fortunately, we know that this multiplication is defined as

$$\overline{a} \cdot \overline{b} = \overline{a \cdot b}$$

for $\overline{a}, \overline{b} \in (\mathbb{Z}/12\mathbb{Z})^\times$. Hence, for any $n \in Z$, we have

$$(\overline{a})^n = \overline{a^n}$$

and so the order of $\overline{a} \in (\mathbb{Z}/12\mathbb{Z})^\times$ is the smallest positive integer k such that

$$(\overline{a})^k = \overline{1} = \overline{a^k}$$

That is, from the last equation, k is the smallest positive integer such that a^k is equal to 1 up to multiplication mod 12. Thus, we can multiply out the integers in the residue classes, mod 12, and be sure that the orders of these elements are the same as the orders of the corresponding residue classes[a].

As an example, note that $1^1 = 1$, so $|1| = 1$. Similarly, $5^1 = 5$, $5^2 = 1$, so $|5| = 2$.

$$|1| = |13| = 1,\ |-1| = |5| = |7| = |-7| = 2$$

■

[a]This may seem like far too much detail to put into this point, but I am trying to emphasize the difference between the integers and these residue classes. In fact, I may be assuming too much at this point when I manipulate the exponents...

Exercise 1.1.13. Find the orders of the following elements of the additive group $\mathbb{Z}/36\mathbb{Z}$: $\overline{1}, \overline{2}, \overline{6}, \overline{9}, \overline{10}, \overline{12}, \overline{-1}, \overline{-10}, \overline{-18}$.

Proof. We can compute the orders of these elements by direct computation of the products until we hit the identity element, $\overline{0}$. Note that for $a \in \mathbb{Z}$ we have $\overline{-a} = \overline{36 - a}$. We find

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

■

Exercise 1.1.14. Find the orders of the following elements of the multiplicative group $(\mathbb{Z}/36\mathbb{Z})^\times$: $\overline{1}, \overline{-1}, \overline{5}, \overline{13}, \overline{-13}, \overline{17}$.

Proof. This is similar to the previous problem, but a different group is considered. The identity here is $\overline{1}$. We find

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

■

Exercise 1.1.15. 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. The proof proceeds by induction on n. For $n = 1$, the statement is trivial. For $n = 2$, it is easy to see: let $a_1, a_2 \in G$. Then

$$\left(a_2^{-1} a_1^{-1}\right)(a_1 a_2) = a_2^{-1}\left(a_1^{-1} a_1\right) a_2 = a_2^{-1} a_2 = e$$

hence $(a_1 a_2)^{-1} = a_2^{-1} a_1^{-1}$.

Assume that the statement is true for some positive integer n; that is, for any n elements $a_1, a_2, \dots, a_n \in G$, we have $(a_1 a_2 \dots a_n)^{-1} = a_n^{-1} a_{n-1}^{-1} \dots a_1^{-1}$. Now,

consider some $n+1$ arbitrary elements of G, $a_1, a_2, \ldots, a_n, a_{n+1}$. Then notice that

$$\begin{aligned}\left(a_{n+1}^{-1}a_n^{-1}\ldots a_2^{-1}a_1^{-1}\right)(a_1a_2\ldots a_na_{n+1}) &= a_{n+1}^{-1}\left(a_n^{-1}\ldots a_2^{-1}a_1^{-1}\right)(a_1a_2\ldots a_n)\,a_{n+1}\\ &= a_{n+1}^{-1}ea_{n+1}\\ &= e\end{aligned}$$

where the first equality holds from associativity of group operation. The second equality is by virtue of the induction hypothesis, and the third is by the definition of inverses (trivially, the base case of this induction proof). By the principle of mathematical induction, then, the statement holds.

■

Exercise 1.1.16. Let x be an element of G. Prove that $x^2 = 1$ if and only if $|x|$ is either 1 or 2.

Proof. Assume $x^2 = 1$. Then recall that the order of x, $|x|$, is the smallest positive integer k such that $x^k = 1$. Thus since $x^2 = 1$, $|x|$ is at most 2. The only other possibility is $|x| = 1$.

For the converse, assume that $|x| = 1$. That is, $x^1 = 1$. Then obviously $x^2 = x^1x^1 = 1 \cdot 1 = 1$. On the other hand, if $|x| = 2$, then by definition $x^2 = 1$.

■

Exercise 1.1.17. Let x be an element of G. Prove that if $|x| = n$ for some positive integer n then $x^{-1} = x^{n-1}$.

Proof. Let $x \in G$ with $|x| = n$ for some $n \in \mathbb{Z}^+$. Then by definition, $x^n = 1$. Then

$$x^{-1} = e \cdot x^{-1} = x^n x^{-1} = x^{n-1}$$

■

Exercise 1.1.18. Let x and y be elements of G. Prove that $xy = yx$ if and only if $y^{-1}xy = x$ if and only if $x^{-1}y^{-1}xy = 1$.

Proof. Let $x, y \in G$ and assume $xy = yx$. Then $x^{-1}, y^{-1} \in G$ by the group axioms, and so

$$y^{-1}xy = y^{-1}(xy) = y^{-1}(yx) = \left(y^{-1}y\right)x = 1 \cdot x = x$$

proving the middle statement. Next, starting from the middle statment,

$$x^{-1}y^{-1}xy = x^{-1}\left(y^{-1}xy\right) = x^{-1}x = 1$$

and so the last statement is proven. Lastly, we start with the last statement and prove the first, completing the chain of implications: assume $x^{-1}y^{-1}xy = 1$. Then recall that $x^{-1}y^{-1} = (yx)^{-1}$. Then

$$xy = 1 \cdot xy = (yx)\left(x^{-1}y^{-1}\right)xy = yx\left(x^{-1}y^{-1}xy\right) = yx \cdot 1 = yx$$

■

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

- Prove that $x^{a+b} = x^a x^b$ and $(x^a)^b = x^{ab}$.
- Prove that $(x^a)^{-1} = x^{-a}$.
- Establish part (a) for arbitrary integers a and b (positive, negative or zero).

Proof.

- We will be informal with these, as they are obvious:

$$x^{a+b} = \underbrace{x \cdot x \cdot \ldots \cdot x}_{a+b \text{ copies}} = \underbrace{x \cdot x \cdot \ldots \cdot x}_{a \text{ copies}} \cdot \underbrace{x \cdot x \cdot \ldots \cdot x}_{b \text{ copies}} = x^a \cdot x^b$$

  and similarly

$$(x^a)^b = \underbrace{x^a \cdot x^a \cdot \ldots \cdot x^a}_{b \text{ copies}} = x^{ab}$$

  by the first statement (and associativity of the group operation).

- For $a \in \mathbb{Z}$, we have

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

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

- We must consider all possibilities for combinations of signs of a and b.

■

Exercise 1.1.20. For x an element in G show that x and x^{-1} have the same order.

Proof. Let $x \in G$ and $|x| = n$. That is, n is the smallest positive integer such that $x^n = 1$. Then notice that

$$\left(x^{-1}\right)^n = \left(x^{-1}\right)^n \cdot 1 = \left(x^{-1}\right)^n \cdot x^n = 1$$

and so the order of x^{-1} is at most n. Assume by way of contradiction that the order of x^{-1} is some $k < n$. Then notice that we have

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

and so we have some integer $n - k < n$ such that $x^{n-k} = 1$; this contradicts the assumption that x has order n. Hence, the order of x^{-1} can be no less than n. Thus $|x^{-1}| = n$.

■

Exercise 1.1.21. 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 k.

Proof. Let $x \in G$ have order n, where n odd. Then $n = 2k - 1$ for some $k \in \mathbb{Z}^+$. By the definition of order of a group element, we have

$$x = x \cdot 1 = xx^{2k-1} = xx^{2k}x^{-1} = \left(x^2\right)^k \left(xx^{-1}\right) = \left(x^2\right)^k$$

■

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

First, we will prove a helpful lemma.

Lemma 1.2.22. Let $x, g \in G$. Then for any $n \in \mathbb{Z}^+$, we have $(g^{-1}xg)^n = g^{-1}x^ng$.

Proof. This is a basic induction proof. The base case, $n = 1$ is trivial. Assume that $(g^{-1}xg)^n = g^{-1}x^ng$ for some $n \in \mathbb{Z}^+$. Then notice that

$$\begin{aligned}\left(g^{-1}xg\right)^{n+1} &= \left(g^{-1}xg\right)^n \left(g^{-1}xg\right) \\ &= g^{-1}x^ngg^{-1}xg \\ &= g^{-1}x^{n+1}g\end{aligned}$$

and so the hypothesis is proven by the principle of mathematical induction.

■

We can now more easily prove the problem statement.

Proof. Let $x, g \in G$ and let $|x| = n$. Then n is the smallest positive integer such that $x^n = 1$. Notice that

$$\begin{aligned}\left(g^{-1}xg\right)^n &= g^{-1}x^ng \\ &= g^1 \cdot 1 \cdot g \\ &= 1\end{aligned}$$

and so $|g^{-1}xg| \leq n$. Next we show that this order can be no less than n. Assume there is some positive integer $k < n$ such that $\left(g^{-1}xg\right)^k = 1$. Then notice that

$$\begin{aligned}1 &= gg^{-1} \\ &= g \cdot 1 \cdot g^{-1} \\ &= g\left(g^{-1}xg\right)^k g^{-1} \\ &= g\left(g^{-1}x^kg\right) g^{-1} \\ &= \left(gg^{-1}\right) x^k \left(gg^{-1}\right) \\ &= x^k\end{aligned}$$

and so $|x| = k < n$, but we assumed x had order n, and so we have a contradiction.

Hence, $|g^{-1}xg| \geq n$. Taken together, the two parts of this proof lead to the conclusion that $|g^{-1}xg| = |x|$.

For the second statement of the problem, just let $x = ab$ and $g = a$ in the first statement: then

$$|ab| = \left|a^{-1}aba\right| = |ba|$$

■

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

Proof. By Problem 1.1.19, we know that we can manipulate integer exponents as $x^{ab} = (x^a)^b$. Then this becomes straightforward. If the order of x is n, finite, and n is factorable into the product of any two positive integers s and t, then by definition of order, n is the smallest positive integer such that

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

and so $|x^s| \leq t$. As in the previous problem, assume that there is some positive $k < t$ such that $|x^s| = k$. Then

$$\begin{aligned} 1 &= x^n \\ &= x^{st} \\ &= x^{s(t-k)+sk} \\ &= x^{s(t-k)} (x^s)^k \\ &= x^{s(t-k)} \cdot 1 \\ &= x^{s(t-k)} \end{aligned}$$

and so we have an positive integer exponent $s(t-k) < st = n$ such that x to this exponent is the identity element, and so the order of x is $s(t-k)$. But this is strictly less than $n = st$, which we assumed was the order of x, and we arrive at a contradiction. Hence, $|x^s| \geq t$.

Taken together, the two parts of this proof show that $|x^s| = t$.

■

Exercise 1.1.24. If a and b are commuting elements of G, prove that $(ab)^n = a^n b^n$ for all $n \in \mathbb{Z}$. [Do this by induction for positive n first.]

Proof. Let $a, b \in G$ where $ab = ba$. Then by definition, $(ab)^1 = ab$, and so the base case is proven. Assume $(ab)^n = a^n b^n$ for some positive integer n. Then

$$\begin{aligned} (ab)^{n+1} &= (ab)^n (ab) \\ &= a^n b^n ab \\ &= a^{n+1} b^{n+1} \end{aligned}$$

where we skipped some steps which used the commutativity of a and b^a.

Next, we extend to non-positive n. If $n = 0$, we have $(ab)^0 = 1 = a^0b^0$ by definition of zero exponents. Lastly, consider an integer exponent $n < 0$. Then $-n > 0$ and we can do

$$\begin{aligned}(ab)^n &= (ab)^{-n\cdot -1} \\ &= \left((ab)^{-n}\right)^{-1} \\ &= \left(a^{-n}b^{-n}\right)^{-1} \\ &= a^n b^n\end{aligned}$$

where again we omit some details leading to the last equality[b]. Thus, we have considered all cases for $n \in \mathbb{Z}$ and shown that $(ab)^n = a^n b^n$.

■

[a]Specifically, we assume that $b^n a = ab^n$ which itself should be proven in a separate induction proof.

[b]We should formally show the distribution of the outer exponent over the product inside, which only works here by virtue of the commutativity of a and b.

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

Proof. Assume that $x^2 = 1$ for all $x \in G$. That is, each x is its own inverse. Then notice that, for any $a, b \in G$, we have

$$\begin{aligned}ab &= 1 \cdot ab \cdot 1 \\ &= \left(b^2\right) ab \left(a^2\right) \\ &= bbabaa \\ &= b\,(ba)\,(ba)\,a \\ &= b\,(ba)^2\,a \\ &= b \cdot 1 \cdot a \\ &= ba\end{aligned}$$

and so arbitrary $a, b \in G$ commute. That is, G is an abelian group.

■

Exercise 1.1.26. Assume H is a nonempty subset of $(G, \star)$ 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[1] of G).

[1]This is expanded upon in the subsequent sections and chapters.

Proof. The group operation of G applied to H is a binary operation on H since H is closed under it, by definition. Since H is composed of elements of G and the same group operation as G, we know that associativity of the group operation is automatically guaranteed. Also, every element of H has an inverse in H since, by definition, H is closed under inversion. Lastly, let $x \in H$, and so $x^{-1} \in H$ by definition of H. Then $x \star x^{-1} = 1 \in H$ by closure under products; that is, the identity element is in H. We have shown the group axioms hold for H under the operation of G, and so H is a group in its own right.

■

Exercise 1.1.27. Prove that if x is an element of the group G then $\{x^n \mid n \in \mathbb{Z}\}$ is a subgroup (cf. the preceding exercise) of G (called the cyclic subgroup of G generated by x).

Proof. We can show that $H = \{x^n \mid n \in \mathbb{Z}\}$ is a subgroup of $(G, \star)$ by showing that it is closed under the binary operation and under inverses (this is the previous Problem's definition of subgroup).

Let x^n and x^m be elements of H. Then by properties of exponents (in the case of additive group, this corresponds to repeated addition),

$$x^n x^m = x^{n+m} \in H$$

and so H is closed under the group operation. Next, note that for $x^n \in H$, $x^n x^{-n} = 1$ and $x^{-n} \in H$, and so the inverse of any element of H is in H; H is closed under inverses. Thus, H is a subgroup of G.

■

Exercise 1.1.28. Let $(A, \star)$ and $(B, \diamond)$ be groups and let $A \times B$ be their direct product (as defined in Example 6). Verify all the group axioms for $A \times B$:

- prove that the associative law holds: for all $(a_1, b_i) \in A \times B, i = 1, 2, 3$

$$(a_1, b_1)\left[(a_2, b_2)(a_3, b_3)\right] = \left[(a_1, b_1)(a_2, b_2)\right](a_3, b_3),$$

- prove that $(1, 1)$ is the identity of $A \times B$, and
- prove that the inverse of (a, b) is (a^{-1}, b^{-1}).

Proof. The direct product of the two groups $(A, \star)$ and $(B, \diamond)$ is the Cartesian product $A \times B$ under the group operation defined as

$$(a_1, b_1)(a_2, b_2) = (a_1 \star a_2, b_1 \diamond b_2)$$

for any $(a_1, b_1), (a_2, b_2) \in A \times B$.

The identity element is the easiest to prove: let $(a, b) \in A \times B$. Then

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

where the 1 indicates the identity A or B, whenever appropriate. Thus, $(1,1)$ is the identity.

Next, let $(a,b) \in A \times B$. Then $a^{-1} \in A$ and $b^{-1} \in B$ by the group axioms on A, B. Hence, $(a^{-1}, b^{-1}) \in A \times B$ and we have

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

and so $A \times B$ has inverses under the direct product.

Lastly, we show associativity. This is the most tedious step. Let $(a_i, b_i) \in A \times B, i = 1,2,3$. Then

$$\begin{aligned}(a_1,b_1)\left[(a_2,b_2)(a_3,b_3)\right] &= (a_1,b_1)\left(a_2 \star a_3, b_2 \diamond b_3\right) \\ &= \left(a_1 \star (a_2 \star a_3), b_1 \diamond (b_2 \diamond b_3)\right) \\ &= \left((a_1 \star a_2) \star a_3, (b_1 \diamond b_2) \diamond b_3\right) \\ &= \left(a_1 \star a_2, b_1 \diamond b_2\right)(a_3,b_3) \\ &= \left[(a_1,b_1)(a_2,b_2)\right](a_3,b_3)\end{aligned}$$

and so $A \times B$ is associative under the direct product. Note that these last manipulations result from the associativities of the groups A and B.

■

Exercise 1.1.29. Prove that $A \times B$ is an abelian group if and only if both A and B are abelian.

Note that, contrary to the previous problem, we write the group operations of A and B both as usual multiplication to simplify the typesetting (i.e., no stars or diamonds). The particular operation being used will be obvious from context, e.g., products of elements of A will use the operation on group A.

Proof. First, assume that A and B are abelian. Then for $(a_1,b_1), (a_2,b_2) \in A \times B$ we have

$$\begin{aligned}(a_1,b_1)(a_2,b_2) &= (a_1a_2, b_1b_2) \\ &= (a_2a_1, b_2b_1) \\ &= (a_2,b_2)(a_1,b_1)\end{aligned}$$

and so $A \times B$ is abelian.

Conversely, assume that $A \times B$ is abelian. Then let $a_1, a_2 \in A$ and $b_1, b_2 \in B$ be arbitrary. Then by commutativity of $A \times B$, we have

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

where the middle equality holds from $A \times B$ being abelian. Then in particular we have $(a_1a_2, b_1b_2) = (a_2a_1, b_2b_1)$ and by equality in Cartesian product spaces we must have $a_1a_2 = a_2a_1$ and $b_1b_2 = b_2b_1$, i.e., these elements commute in their

respective groups A and B. Since a_1, a_2, b_1, b_2 were arbitrary, we conclude that A and B are both abelian groups.

By proving both directions, we conclude that A and B are abelian groups if and only if $A \times B$ is abelian.

■

Exercise 1.1.30. 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. Consider $(a, 1_B), (1_A, b) \in A \times B$. The Cartesian product of groups A and B has a group structure under the natural direct product operation, under which we have

$$(a, 1_B) \cdot (1_A, b) = (a \cdot 1_A, 1_B \cdot b) = (a, b)$$

and

$$(1_A, b) \cdot (a, 1_B) = (1_A \cdot a, b \cdot 1_B) = (a, b)$$

and so these elements commute.

Next, notice that we can decompose any $(a, b) \in A \times B$ into the product of two of these commuting elements: $(a, b) = (a, 1_B) \cdot (1_A, b)$. We can use induction to show that for any $n \in \mathbb{Z}^+$ we have $(a, b)^n = (a, 1_B)^n \cdot (1_A, b)^n$. In the case $n = 1$, this was already proved. Assume it holds for arbitrary $k \in \mathbb{Z}$: $(a, b)^k = (a, 1_B)^k \cdot (1_A, b)^k$. Then

$$\begin{aligned}
(a, b)^{k+1} &= (a, b) \cdot (a, b)^k \\
&= (a, 1_B) \cdot (1_A, b) \cdot (a, 1_B)^k \cdot (1_A, b)^k \\
&= (1_A, b) \cdot (a, 1_B) \cdot (a, 1_B)^k \cdot (1_A, b)^k \\
&= (1_A, b) \cdot (a, 1_B)^{k+1} \cdot (1_A, b)^k \\
&= (1_A, b) \cdot \left(a^{k+1}, 1_B\right) \cdot (1_A, b)^k \\
&= \left(a^{k+1}, 1_B\right) \cdot (1_A, b) \cdot (1_A, b)^k \\
&= (a, 1_B)^{k+1} \cdot (1_A, b)^{k+1}
\end{aligned}$$

where we used the fact that $(c, d)^k = \left(c^k, d^k\right)$ for any $(c, d) \in A \times B$ by nature of the direct product. Thus, the statement holds for arbitrary $k \in \mathbb{Z}$. Further, we can write $(a, b)^n = (a^n, b^n)$, which requires another easy (omitted) induction proof.

Next, let $r = \operatorname{lcm}(|a|, |b|)$. Then there exists $p, q \in \mathbb{Z}$ such that $pa = qb = r$. Then obviously

$$(a, b)^r = (a^r, b^r) = (1, 1)$$

and so the order of (a, b) is less than or equal to r. Let $s = |(a, b)|$, so that $s \leq r$. Then $(a, b)^s = (a^s, b^s) = 1$, so that $a^s = 1$ and $b^s = 1$. Thus, $|a|$ and $|b|$ both divide s, making s a common multiple of $|a|$ and $|b|$. But r was defined as the smallest

such multiple, so we know $r \leq s$. Taken together, we see that $r = s$, and so we conclude that $|(a,b)| = \operatorname{lcm}(|a|, |b|)$.

■

Exercise 1.1.31. Prove that any finite group G of even order contains an element of order 2. [Let $t(G)$ be the set $\{g \in G \mid g \neq g^{-1}\}$. Show that $t(G)$ has an even number of elements and every nonidentity element of $G - t(G)$ has order 2.]

Proof. Let G have finite even order. Then assume by way of contradiction that no element has order 2, i.e., for every element $g \in G$ we have $g \neq g^{-1}$. Then we can partition G into equivalence classes where each element of G is equivalent to its inverse. Then each class corresponding to non-identity $g \in G$ is of the form $[g] = \{g, g^{-1}\}$, a two-element subset. These are bona fide equivalence classes since group inverses are unique. For the identity element $1 \in G$, we have $[1] = \{1\}$, a singleton set. Then the total number of elements in G is twice the number of non-identity equivalence classes (since these are two-element subsets) plus 1 (for the identity class); thus, there is an odd number of elements in G, and this is a contradiction. Thus, there must be some element of order 2 in G.

■

The next proof is more in line with the hint suggested in the problem statement.

Proof. Let $t(G) = \{g \in G \mid g \neq g^{-1}\}$. By the symmetry of this construction, note that $g \in t(G) \implies g^{-1} \in G$, and that these are two unique elements of $t(G)$. Also, the pairs $\{g, g^{-1}\}$ partition $t(G)$ since inverses are unique in groups. Thus, elements of $t(G)$ come in pairs and so $|t(G)| = n$ is even. Then the elements of G which have order 2 are $G - t(G)$, and $|G - t(G)| = m$ is even since removing an even number of elements from a set of an even number of elements results in an even number remaining. Clearly $G - t(G) \neq \varnothing$ since 1 is included. Hence, there is a nonzero even number of elements. There thus must be some other $g \in G - t(G)$, i.e., a nonidentity $g \in G$ with $g^2 = 1$.

■

Exercise 1.1.32. If x is an element of finite order n in G, prove that the elements $1, x, x^2, \ldots, x^{n-1}$ are all distinct. Deduce that $|x| \leq |G|$.

Proof. Let $x \in G$ have finite order n. Assume by way of contradiction that we have $x^i = x^j$ for some pair $0 \leq i, j \leq n-1$, $i \neq j$. Then we can assume $i > j$ without loss of generality, and we have

$$1 = x^i \left(x^j\right)^{-1} = x^i x^{-j} = x^{i-j}$$

and we also have

$$0 = i - i < i - j < i < n$$

so that $0 < i - j < n$ and so $i - j = k$ for some $k \in [0, 1, 2, \ldots, n-1]$. But then

we have $x^k = 1$ for $0 \leq k < n$, but x has order n. This is a contradiction, and so all x^i are distinct for $i = 0, 1, 2, \ldots, n-1$. Thus, since $\{1, x^1, x^2, \ldots, x^{n-1}\} \subset G$ and these are all distinct, we have $n = |x| \leq G$.

■

Exercise 1.1.33. Let x be an element of finite order n in G.

- Prove that if n is odd then $x^i \neq x^{-i}$ for all $i = 1, 2, \ldots, n-1$.
- Prove that if $n = 2k$ and $1 \leq i < n$ then $x^i = x^{-i}$ if and only if $i = k$.

Proof. Let $x \in G$ have finite order n.

- Assume $n = 2k - 1$ where $k \in \mathbb{Z}$. Then n is the smallest integer such that $x^n = 1$, and $x^k = 1$ for any $k \in \mathbb{Z}$ implies that $n|k$. Thus if we assume by way of contradiction that $x^i = x^{-i}$ for some $i = 1, 2, \ldots, n-1$. Then notice in general that $x^i x^{n-i} = x^n = 1$, so that $(x^i)^{-1} = x^{-i} = x^{n-i}$. Then from our assumption, we have $x^i = x^{n-i}$. But then from the previous Exercise 1.1.32, these are distinct for $i \neq n - i$. The only way for these to be equal is for $i = n - i$, or $2i = n$. But since $n = 2k - 1$ odd, we have $2i = 2k - 1$, or $2(k - i) = 2i' = 1$ where $i' = k - i \in \mathbb{Z}$ and we know that 2 has no multiplicative inverse in $\mathbb{Z}$, so this is never satisfied. Hence, $x^i \neq x^{-1}$ for any $0 \leq i < n$.
- Assume $n = 2k$ (even) and $1 \leq i < n$. Then assume $x^i = x^{-i}$. As in the previous part of the Exercise, we have $(x^i)^{-1} = x^{-i} = x^{n-i}$, and so $x^i = x^{n-i}$. This is satisfied if $n = 2i$, and since $n = 2k$, this is satisfied for exactly $i = k$.

  Conversely, assume $i = k$. Then

  $$1 = x^n = x^{2k} = x^{k+k} = x^k x^k$$

  so that $\left(x^k\right)^{-1} = x^{-k} = x^k$ and we are done.

■

Exercise 1.1.34. If x is an element of infinite order in G, prove that the elements x^n, $n \in \mathbb{Z}$ are all distinct.

Proof. Assume x has infinite order, and assume by way of contradiction that some pair of elements are equal: $x^p = x^q$ for some $p, q \in \mathbb{Z}$, $p \neq q$. Then we have $x^p x^{-q} = x^{p-q} = 1$ and so x must have order $|x| \leq |p - q|$. Then the order of x is finite, which is a contradiction. Hence, all products of x must be unique.

■

Exercise 1.1.35. If x is an element of finite order n in G, use the Division Algorithm to show that any integral power of x equals one of the elements in the set $\{1, x, x^2, \ldots, x^{n-1}\}$ (so these are all the distinct elements of the cyclic subgroup (cf. Exercise 27 above) of G generated by x).

Note that this problem is conceptually similar to that of the modular addition group $\mathbb{Z}/n\mathbb{Z}$. In fact, this group is cyclic and is generated by $\overline{1}$.

Proof. Let $x \in G$ have finite order n, and let x^k be some arbitrary integral power of x. Then the division algorithm guarantees that we can express $k = qn + r$, $q, r \in \mathbb{Z}$, with $0 \leq r < n$. That is, $r \in \{0, 1, 2, \ldots, n-1\}$. Thus,

$$x^k = x^{qn+r} = x^{qn}x^r = (x^n)^q\, x^r = (1)^q\, x^r = x^r$$

so that $x^k = x^r$ for r some integer between 0 and $n-1$, inclusive. This is what we were trying to show.

Note that this demonstrates that the set of arbitrary products of x (of order n) is a subset of the set $\{x^0, x^1, x^2, \ldots, x^{n-1}\}$. Clearly, this set is itself a subset of the set of arbitrary products of x, and so, by double inclusion, the sets are equal. This shows that the cyclic group generated by element x of finite order n, $\langle x \rangle$ is exactly the set $\{x^0, x^1, \ldots, x^{n-1}\}$. Further, we can conclude that the order of this set is $|\langle x \rangle| = n$, since it contains at most n elements, and if any two elements are identical, say $x^p = x^q$, $0 \leq p, q < n$, then $x^{p-q} = 1$ and so x would have order $p - q < n$, a contradiction.

■

Exercise 1.1.36. 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 (so by Exercise 32, every element has order ≤ 3). Use the cancellation laws to show that there is a unique group table for G. Deduce that G is abelian.

Proof. Since the order of G is 4, there is some element of order 2, by Exercise 1.1.31. Arbitrarily let this be a, in which case $a^2 = 1$. Next, introduce element b and consider possibilities for ab. If $ab = 1$ then $b = a^{-1} = a$, which is not true since we assume the four elements are distinct. Similarly, $ab \neq b$ since this would imply $a = 1$ by right cancellation, thus we must have $ab = c$. This leaves $ac = b$ as the only option.

Next consider b. We must have $ab \neq a$ since then $b = 1$. If $ab = b$ then $a = 1$, so this doesn't work. If $ab = 1$, then $b = a^{-1} = a$, so this doesn't work. Thus, we must have $ab = c$. Next, if $b^2 = a$, then $1 = a^2 = b^4$ and so b has order 4 which we assumed doesn't happen; thus $b^2 \neq a$. Hence, $b^2 = 1$. Lastly $cb = a$ because this is the only remaining element left to appear in this row.

For the last row of the table, we work with c. Consider first ac. If $ac = a$ then $c = 1$, untrue. If $ac = c$ then $c = 1$, untrue. If $ac = 1$, then $c = a^{-1} = a$, untrue. So we must have $ac = b$. Next, consider bc. If $bc = b$, then $c = 1$, untrue. If $bc = c$, then $b = 1$, untrue. If $bc = 1$ then $c = b^{-1} = b$, untrue. Hence, $bc = a$. Lastly, we

must have $c^2 = 1$. Thus we have show a unique group table for G:

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

The symmetry of this group table indicates that the group is abelian: $g_j g_i = D_{ij} = D_{ji} = g_i g_j$ for all i, j.

■

Sec. 1.2 Dihedral Groups

In these exercises, D_{2n} has the usual presentation $D_{2n} = \langle r, s \,|\, r^n = s^2 = 1, rs = sr^{-1} \rangle$.

Exercise 1.2.1. Compute the order of each of the elements in the following groups:

- D_6
- D_8
- D_{10}.

Proof. • Note that $D_6 = D_{2 \cdot 3}$ and so the dihedral group of order 6 is the group of symmetries of a regular 3-gon, i.e., an equilateral triangle.

$$D_6 = \left\{ r^0, r^1, r^2, s, sr, sr^2 \right\}$$

where r is a rotation of $\frac{360}{3} = 120$ degrees and s is a reflection about the vertical line of symmetry. Then certainly $|s| = 2$, and this is seen from the usual presentation. Also, $|r^0| = |1| = 1$, $|r| = 3$, and $|r^2| = 3$. Now we have from the presentation

$$(sr)^2 = srsr = s\,(rs)\,r = ssr^{-1}r = s^2 = 1$$

and so $|sr| = 2$. Similarly,

$$\left(sr^2\right)^2 = srrsrr = srsr^{-1}rr = srsr = (sr)^2 = 1$$

and so $|sr^2| = 2$.

• D_8 is the group of symmetries of a regular 4-gon, i.e., a square.

$$D_8 = \left\{ r^0, r^1, r^2, r^3, s, sr, sr^2, sr^3 \right\}$$

So $|r^0| = 1$, $|r^1| = 4$, $|r^2| = 2$, $|r^3| = 4$. As always, $s^2 = 1$ so $|s| = 2$. Again we have $|sr| = |sr^2| = 2$ for the same reasons as in the case of D_6. Lastly,

$$\left(sr^3\right)^2 = sr^3sr^3 = sr^2sr^{-1}r^3 = srsr^{-2}r^3 = s^2r^{-3}r^3 = 1$$

and so $|sr^3| = 2$.

- D_{10} is the group of symmetries of a regular 5-gon, i.e., a pentagon.

$$D_{10} = \left\{r^0, r^1, r^2, r^3, r^4, s, sr, sr^2, sr^3, sr^4\right\}$$

From the previous two examples, we can see that $\left(sr^k\right)^2 = s^2r^{-k}r^k = 1$ for all $k = 0, 1, \ldots, n-1$. This can be easily proved using induction, but we will omit it here and just use the result. With this in hand, computing these orders is simple: $|r^0| = 1$, $|r^1| = |r^2| = |r^3| = |r^4| = 5$, $|s| = |sr| = |sr^2| = |sr^3| = |sr^4| = 2$.

■

Exercise 1.2.2. 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 $rx = xr^{-1}$.

This interesting statement says that if a dihedral group element involves a reflection, then performing this action followed by a rotation is the same as performing this action preceeded by the inverse rotation.

Proof. If $x \in D_{2n}$ is not a power of r, then it is of the form $x = sr^k$ for some $k = 0, 1, 2, \ldots, n-1$. Then

$$rx = rsr^k = (rs)\, r^k = sr^{-1}r^k = sr^{k-1} = sr^kr^{-1} = xr^{-1}$$

■

Exercise 1.2.3. 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. Let $x \in D_{2n}$ not be a power of r. Then $x = sr^k$ for some integer k. Then

$$x^2 = sr^ksr^k = s^2r^{-k}r^k = s^2 = 1$$

where we used the result of the previous problem to say $r^ks = sr^{-k}$ (formally we should probably have used induction on this step). Thus, $|x| = 2$.

To prove the last part of the statement, first let $x \in D_{2n}$ be some (integral) power of r, say $x = r^k$. Then

$$x = r^k = (1 \cdot r)^k = \left(s^2r\right)^k = (s\,(sr))^k$$

which is a product of s and sr. On the other hand, if x is not a power of r, say

$x = sr^k$, then

$$x = sr^k = s\left(s\left(sr\right)\right)^k$$

and so it is again a product of s and sr. Hence, any element in D_{2n} can be written as a product of s and sr, and so these are generators for D_{2n}, both of which have order 2 by the first part of the problem:

$$D_{2n} = \langle s, sr \rangle$$

■

Exercise 1.2.4. If $n = 2k$ is even and $n \geq 4$, show that $z = r^k$ is an element of order 2 which commutes with all elements of D_{2n}. Show also that z is the only nonidentity element of D_{2n} which commutes with all the elements of D_{2n}. [cf. Exercise 33 of Section 1.]

Proof. Let $n = 2k$ and $n \geq 4$. Consider element $z = r^k \in D_{2n}$. Then $z^2 = \left(r^k\right)^2 = r^{2k} = r^n = 1$, so $|z| = 2$. Also, given arbitrary r^i where $0 \leq i < n$, we have

$$\begin{aligned} r^i z &= r^i r^k \\ &= r^k r^i \\ &= z r^i \end{aligned}$$

and so elements without a factor of s commute with z. Next, consider arbitrary sr^i with $0 \leq i < n$. Then

$$\begin{aligned} sr^i z &= sr^i r^k \\ &= sr^k r^i \\ &= r^{-k} sr^i \\ &= r^{n-k} sr^i \\ &= r^{2k-k} sr^i \\ &= r^k sr^i \\ &= z sr^i \end{aligned}$$

and so z commutes with all elements of D_{2n}.

Assume now that there is some other element $x \in D_{2n}$ which commutes with all other elements. First, if $x = r^j$, $0 \leq j < n$, then

$$sx = sr^j \quad \text{and} \quad xs = r^j s = sr^{-j}$$

and these are equal if and only if $r^j = r^{-j}$. This means that $j = k$.

Next, if $x = sr^j$, $0 \leq j < n$, then

$$sx = s^2 r^j = r^j \quad \text{and} \quad xs = r^j s = sr^{-j}$$

so that these are equal if and only if $r^j = sr^{-j}$, i.e., $r^{2j} = s$. Intuitively this is never true since we cannot reach a reflection from any rotations. Hence, $x \neq sr^j$ for any j.

Thus, in both cases our element reduces to $r^k = r^{n/2}$ (n even).

■

Exercise 1.2.5. 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}. [cf. Exercise 33 of Section 1.]

Exercise 1.2.6. 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. Let $x, y \in G$ have order 2. Let $t = xy$. Then

$$tx = xyx = x\left(x^{-1}y^{-1}\right)^{-1} = x\left(xy\right)^{-1} = xt^{-1}$$

by the properties of the inverse of a product. Then if $|xy| = n < \infty$, x and t satisfy the same relations in G as s, r do in D_{2n}.

■

Exercise 1.2.7. Show that $\langle a, b \,|\, a^2 = b^2 = (ab)^n = 1\rangle$ gives a presentation for D_{2n} in terms of the two generators $a = s$ and $b = sr$ of order 2 computed in Exercise 3 above. [Show that the relations for r and s follow from the relations for a and b and, conversely, the relations for a and b follow from those for r and s.]

Exercise 1.2.8. Find the order of the cyclic subgroup of D_{2n} generated by r (cf. Exercise 27 of Section 1).

Proof. The cyclic subgroup of D_{2n} generated by r is the set of powers of r:

$$\langle r\rangle = \left\{r^j \,|\, j \in \mathbb{Z}\right\}$$

We want to show that this set has cardinality n. Since D_{2n} has the usual presentation, we know that $r^n = 1$, so r has order at most n; that is, $\langle r\rangle$ has at most n distinct elements:

$$\langle r\rangle = \left\{1, r, r^2, r^3, \ldots, r^{n-1}\right\}$$

and since we know these are distinct (?) we conclude that there are n distinct elements, i.e., that the subgroup generated by r has order n.

■

In each of Exercises 9 to 13 you can find the order of the group of rigid motions in $\mathbb{R}^3$ (also called the group of rotations) of the given Platonic solid by following the proof for the order of D_{2n}: find the number of positions to which an adjacent pair of vertices can be sent. Alternatively, you can find the number of places to which a given face may be sent and, once

a face is fixed, the number of positions to which a vertex on the face may be sent.

Stan's note: for these three-dimensional solids, we are looking at *rigid motions*, mimicking how we might manipulate a real solid object in 3-space. We do not consider any sort of "mirroring" as we do in the 2D case. I am not completely sure why: for instance, looking at one face of a tetrahedron, we can reverse the ordering of the vertices around this face by swapping any two of the vertices (this amounts to pulling the solid "inside out"). I think that these motions are just not even considered in the following problems, though they do seem to strictly be included in the set of symmetries of the object. Here, we are just looking at rigid motions, a subgroup of the symmetries.

Maybe it is because for a 2D object, such as a square, we can imagine flipping the object over, and this counts as a symmetry, but for a 3D object there is no real analogue to flipping it over (pulling it inside out is not something we can do in 3D for topological reasons).

Exercise 1.2.9. Let G be the group of rigid motions in $\mathbb{R}^3$ of a tetrahedron. Show that $|G| = 12$.

Proof. A tetrahedron is like a three-dimensional pyramid: four triangular faces, four vertices, each vertex having 3 adjacent vertices. If we consider the a particular vertex i connected to vertex j, a symmetry can move i to one of any $n = 4$ locations, and then j can move to any of the adjacent 3 vertices: there are $3 \cdot 4 = 12 = |G|$ rigid motions.

Alternately, any of the four faces can move to any of 4 locations, and any vertex on this face may move to any of 3 vertex locations, again giving $|G| = 12$.

■

Exercise 1.2.10. Let G be the group of rigid motions in $\mathbb{R}^3$ of a cube. Show that $|G| = 24$.

Proof. Any vertex on the cube can move to one of 8 locations, and any neighboring vertex has 3 possibilities of where to move, giving $8 \cdot 3 = 24 = |G|$ rigid motions.

Alternately, any face can move to one of 6 face locations, and each vertex on the face can move to one of 4 locations: $6 \cdot 4 = 24$.

■

Exercise 1.2.11. Let G be the group of rigid motions in $\mathbb{R}^3$ of a octahedron. Show that $|G| = 24$.

Proof. An octahedron is like two tetrahedrons sharing a face. Hence, they have 8 faces and each vertex has 4 neighbors, with a total of 6 vertices. Thus, any vertex can move to one of 6 locations, and there are 4 options for where to move any given neighboring vertex: $6 \cdot 4 = 24 = |G|$.

Alternately, any face can move to 8 places, and any of the 3 vertices on that face can move, obviously, to 3 places: $8 \cdot 3 = 24 = |G|$.

■

Exercise 1.2.12. Let G be the group of rigid motions in $\mathbb{R}^3$ of a dodecahedron. Show that $|G| = 60$.

Proof. A dodecahedron has 12 faces and 20 vertices, each vertex having 3 neighbors and each face having 5 vertices. Hence, each vertex can move to one of 20 locations, and any neighboring vertex can move to one of 3 locations: $20 \cdot 3 = 60 = |G|$.

Alternately, any of the 12 faces can move to 12 locations, and any of the 5 vertices on this face can move to one of 5 locations: $12 \cdot 5 = 60 = |G|$.

■

Exercise 1.2.13. Let G be the group of rigid motions in $\mathbb{R}^3$ of a icosahedron. Show that $|G| = 60$.

Proof. An icosahedron has 20 faces, 12 vertices, each face has 3 vertices, and each vertex has 5 neighbors. Hence, any vertex can go to one of 12 locations, and each of the 5 neighboring vertices can move to one of 5 locations: $12 \cdot 5 = 60 = |G|$.

Alternately, any face can move to one of 20 locations, and each of the 3 vertices on that face can move to one of 3 locations: $20 \cdot 3 = 60 = |G|$.

■

Exercise 1.2.14. Find a set of generators for $\mathbb{Z}$.

Proof. Recall that $\mathbb{Z}$ is a group under usual integer addition. Note that for any $z \in \mathbb{Z}$ we can write $z = z \cdot 1$ where the multiplicative notation is meant to indicate repeated addition. Thus, we see that $1 \in \mathbb{Z}$ is a generator. Hence,

$$\langle 1 \rangle = \mathbb{Z}$$

■

Exercise 1.2.15. Find a set of generators and relations for $\mathbb{Z}/n\mathbb{Z}$.

Proof. Recall that $\mathbb{Z}/n\mathbb{Z}$ is the group of residue classes of $\mathbb{Z}$ under addition mod n; that is, it is the set of equivalence classes of $\mathbb{Z}$ where $a, b \in \mathbb{Z}$ are equivalent if they are separated by some integer multiple of n.

We can see that $\mathbb{Z}/n\mathbb{Z}$ is cyclic and is generated by the residue class $\overline{1}$: for arbitrary element $\overline{k}$, where $k = 0, 1, 2, \ldots, n-1$ (these are the distinct elements), we have

$$\overline{k} = \overline{1 + 1 + \ldots + 1} = \overline{1} + \overline{1} + \ldots + \overline{1} = k \cdot \overline{1}$$

where we use the definition of addition of residue classes and write the sum of k copies of $\overline{1}$ as $k \cdot \overline{1}$.

As far as relations go, we need to specify the modular arithemetic part of the group. In particular, we need to constrain the sum of the generator $\overline{1}$ to "wrap around":

$$n\overline{1} = \overline{0}$$

and so this is our relation. In total, we can write

$$\mathbb{Z}/n\mathbb{Z} = \left\langle \overline{1} \,|\, n\overline{1} = \overline{0} \right\rangle$$

■

Exercise 1.2.16. Show that the group $\left\langle x_1, y_1 \,|\, x_1^2 = y_1^2 = (x_1 y_1)^2 = 1 \right\rangle$ is the dihedral group D_4 (where x_1 may be replaced by the letter r and y_1 by s). [Show that the last relation is the same as: $x_1 y_1 = y_1 x_1^{-1}$.]

Proof. Recall that D_4 has the presentation

$$D_4 = \left\langle r, s \,|\, r^2 = s^2 = 1, rs = sr^{-1} \right\rangle$$

Notice that

$$\begin{aligned} (rs)^2 &= rsrs \\ &= rssr^{-1} \\ &= rs^2 r^{-1} \\ &= r \cdot 1 \cdot r^{-1} \\ &= 1 \end{aligned}$$

so that $(rs)^2 = 1$. That is, the last relation in our presentation for D_4 is equivalent to saying that $(rs)^2 = 1$. Hence, there is an isomorphism between these two groups sending $r \mapsto x_1$ and $s \mapsto y_1$ and the presentations are unchanged. This group with x_1 and y_1 specified is just an alternative presentation of the same group, D_4.

■

Exercise 1.2.17. Let X_{2n} be the group whose presentation is displayed in (1.2).

- 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.
- Show that if $(3, n) = 1$, then x satisfies the additional relation: $x = 1$. In this case deduce that X_{2n} has order 2. [Use the facts that $x^n = 1$ and $x^3 = 1$.]

Proof. The group presentation in question is

$$X_{2n} = \left\langle x, y \,|\, x^n = y^2 = 1, xy = yx^2 \right\rangle$$

- Let $n = 3k$. The discussion of this presentation in the text shows that

$$x = xy^2 = yx^2 y = \ldots = y^2 x^4 = x^4$$

and so cancellation law in groups gives $x^3 = 1$ so that x has order at most 3.

■

Exercise 1.2.18. Let Y be the group whose presentation is displayed in (1.3).

- Show that $v^2 = v^{-1}$. [Use the relation: $v^3 = 1$.]
- Show that v commutes with u^3. [Show that $v^2u^3v = u^3$ by writing the left hand side as $(v^2u^2)(uv)$ and using the relations to reduce this to the right hand side. Then use part (a).]
- Show that v commutes with u. [Show that $u^9 = u$ and then use part (b).]
- Show that $uv = 1$ [Use part (c) and the last relation.]
- Show that $u = 1$, deduce that $v = 1$, and conclude that $Y = 1$. [Use part (d) and the equation $u^4v^3 = 1$.]

Sec. 1.3 Symmetric Groups

Exercise 1.3.1. 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: $\sigma, \tau, \sigma^2, \sigma\tau, \tau\sigma$, and $\tau^2\sigma$.

Proof. We can simply "walk through" the permutations to construct the cycle decompositions:

$$\sigma = (135)(24)$$
$$\tau = (15)(23)$$
$$\sigma^2 = (153)$$
$$\sigma\tau = (2534)$$
$$\tau\sigma = (1243)$$
$$\tau^2\sigma = (135)(24) = \sigma$$

■

Exercise 1.3.2. Let σ be the permutation

$$\begin{array}{ccccc} 1 \mapsto 13 & 2 \mapsto 2 & 3 \mapsto 15 & 4 \mapsto 14 & 5 \mapsto 10 \\ 6 \mapsto 6 & 7 \mapsto 12 & 8 \mapsto 3 & 9 \mapsto 4 & 10 \mapsto 1 \\ 11 \mapsto 7 & 12 \mapsto 9 & 13 \mapsto 5 & 14 \mapsto 11 & 15 \mapsto 8 \end{array}$$

and let τ be the permutation

$$\begin{array}{ccccc} 1 \mapsto 14 & 2 \mapsto 9 & 3 \mapsto 10 & 4 \mapsto 2 & 5 \mapsto 12 \\ 6 \mapsto 6 & 7 \mapsto 5 & 8 \mapsto 11 & 9 \mapsto 15 & 10 \mapsto 3 \\ 11 \mapsto 8 & 12 \mapsto 7 & 13 \mapsto 4 & 14 \mapsto 1 & 15 \mapsto 13 \end{array}$$

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

Proof. This is similar to the last problem, only much more tedious.

$$\sigma = (1\,13\,5\,10)\,(3\,15\,8)\,(4\,14\,11\,7\,12\,9)$$

$$\tau = (1\,14)\,(2\,9\,15\,13\,4)\,(3\,10)\,(5\,12\,7)\,(8\,11)$$

$$\sigma^2 = (1\,5)\,(3\,8\,15)\,(4\,11\,12)\,(7\,9\,14)\,(10\,13)$$

$$\sigma\tau = (1\,11\,3)\,(2\,4)\,(5\,9\,8\,7\,10\,15)\,(13\,14)$$

$$\tau\sigma = (1\,4)\,(2\,9)\,(3\,13\,12\,15\,11\,5)\,(8\,10\,14)$$

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

■

Exercise 1.3.3. For each of the permutations whose cycle decompositions were computed in the preceding two exercises compute its order.

Proof. Recall that we can compute the order of a permutation from a disjoint cycle decomposition as the least common multiple of the lengths of each cycle. Alternately, we can compute the order of a permutation (of a finite set) in a brute force manner by computing products of the permutation until we reach the identity permutation.

For the first exercise:

$$|\sigma| = \left|\tau^2\sigma\right| = 6,\ |\tau| = 2,\ \left|sigma^2\right| = 3,\ |\sigma\tau| = |\tau\sigma| = 4$$

For the second exercise:

$$|\sigma| = 12,\ |\tau| = 30,\ \left|\sigma^2\right| = |\sigma\tau| = |\tau\sigma| = 6,\ \left|\tau^2\sigma\right| = 13$$

■

Exercise 1.3.4. Compute the order of each of the elements in the following groups: (a) S_3, (b) S_4.

Proof. There are $3! = 6$ elements in S_3:

$$S_3 = \{(),\,(1\ 2),\,(1\ 3),\,(2\ 3),\,(1\ 2\ 3),\,(1\ 3\ 2)\}$$

since we have written each element as a single (trivially disjoint) cycle, the order

of each element is trivially just the length of the element. Hence,

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

For S_4, there are $4! = 24$ elements:

$$\begin{aligned} S_4 = \{&() ,\ (1\ 2) ,\ (1\ 3) ,\ (1\ 4) ,\ (2\ 3) ,\ (2\ 4) ,\ (3\ 4) ,\ (1\ 2)(3\ 4) ,\ (1\ 3)(2\ 4) ,\\ &(1\ 2\ 3) ,\ (1\ 3\ 2) ,\ (1\ 2\ 4) ,\ (1\ 4\ 2) ,\ (2\ 3\ 4) ,\ (2\ 4\ 3) ,\ (1\ 2\ 3\ 4) ,\ (2\ 1\ 3\ 4) ,\\ &(3\ 2\ 1\ 4) ,\ (4\ 2\ 3\ 1) ,\ (1\ 3\ 2\ 4) ,\ (1\ 2\ 4\ 3) ,\ (2\ 1\ 4\ 3) ,\ (3\ 4\ 1\ 2) ,\ (4\ 3\ 2\ 1)\} \end{aligned}$$

Without actually writing out the results, we can simply read off the order of each element as the length of each single cycle, or, when a permutation is a product of cycles, as the least common multiple of the lengths of the individual factor cycles; note that in this case, the only permutations in S_4 which are not single cycles are products of 2-cycles, and so these elements have order 2.

■

Exercise 1.3.5. Find the order of $(1\ 12\ 8\ 10\ 4)\,(2\ 13)\,(5\ 11\ 7)\,(6\ 9)$.

Proof. Since this permutation is a product of disjoint cycles, the order of the permutation is just the least common multiple of the lengths of the cycles. Hence, the order is $\operatorname{lcm}(5, 2, 3) = 30$.

■

Exercise 1.3.6. Write out the cycle decomposition of each element of order 4 in S_4.

Proof. Note that we did this in a previous Exercise, Problem 1.3.4.

■

Exercise 1.3.7. Write out the cycle decomposition of each element of order 2 in S_4.

Proof. Note that we did this in a previous Exercise, Problem 1.3.4.

■

Exercise 1.3.8. Prove that if $\Omega = \{1, 2, 3, \ldots\}$ then S_Ω is an infinite group.

Proof. Recall that a permutation on a set is a bijection from the set to itself. Thus, this problem asks us to show that there are infinitely many bijections from Ω to itself. We can easily construct these. For example, let σ_i, for $i \in \{1, 2, 3, \ldots\}$, be the permutation exchanging 1 with i: we may write $\sigma_i = (1\ i)$, even though not all elements of S_Ω can be expressed in this notation[a]. Then these are all distinct permutations of Ω, and there are countably many of them (thus infinitely many of them). Note that this is only a subset of S_Ω, but a set with an infinite subset is, itself, infinite. Hence, S_Ω is an infinite group.

■

[a]It is really only useful for permutations of finite sets.

Exercise 1.3.9. • 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?

- 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?
- 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?

Proof. Note: see problem 1.3.11 for a formal justification of the characterization we use here.

- As the previous Exercises, we can compute these group elements, σ^i, for $i = 1, 2, \ldots, 11$, write these products in their disjoint cycle decompositions, and see which are 12-cycles. By inspection, the 12-cycles are σ^i for $i \in \{1, 5, 7, 11\}$. Can we find a pattern? Note that $1, 5, 7, 11$ are relatively prime to 12.
- We can perform the same brute-force computation of the powers of τ and determine by inspection which are 8-cycles. Alternatively, we will take for granted that our results from above are correct in that 8-cycles will correspond to exponents which are relatively prime to 8: $i \in \{1, 3, 5, 7\}$.
- Again, the indices corresponding to 14-cycles are $i \in \{1, 3, 5, 9, 11, 13\}$.

■

Exercise 1.3.10. 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 residue mod m when $k + 1 > m$. Deduce that $|\sigma| = m$.

Proof. We can show this by induction on integer i. Let the m-cycle σ be given. Then certainly $\sigma^1(a_k) = a_{k+1}$, since we can read this right off of the expression for σ (this is the base case). Next, assume that for some positive integer i we have $\sigma^i(a_k) = a_{k+1}$. Then

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

where the sums in the denominator are performed modulo m. Then we have shown what we wanted to prove.

Next, we consider the order of σ. Consider an arbitrary a_i; without losing

generality we pick a_1. Then $\sigma^i(a_1) = a_{1+i}$ where the sum $1+i$ is performed modulo m. In order for σ^i to possibly be the identity, it must send a_1 to a_1, i.e., $1+i \equiv 1 \bmod m$. That is, $1+i-1 = i = km$ for some $k \in \mathbb{Z}$. Thus, the smallest such k is $k=1$, in which $i=m$, and so we have $\sigma^m(a_1) = a_1$. Hence, the order of σ is at least m. Also, note that σ^m sends every a_i to itself, and so σ^m is a product of σ which is the identity element. Hence, we have shown that $\sigma^m = 1$ and that $\sigma^k \neq 1$ for any $k < m$; in other words, $|\sigma| = m$.

■

Exercise 1.3.11. 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.

Note: see problem 1.3.9, where we invoked this theorem without proof.

Proof. Let $\sigma = (1\ 2\ \ldots\ m)$ and first assume that σ^i is also an m-cycle and that i and m are not relatively prime, i.e., there is some $k \in \mathbb{Z}$ which is a factor of both i and m.

■

Exercise 1.3.12.

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

Proof.

- Let τ be given as in the problem statement. Then note that every integer maps after k iterations to the integer next to it in the usual ordering and for a long cycle, we need to make several iterations through in order to make this swap. For example, $\tau(1) = 2$ so we need 1 and 2 to be quite far apart in the representation of σ. Since τ is comprised of 5 cycles, we will need $k = 10$. Note that

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

  does the trick, and $\tau = \sigma^5$.

- Assume that $\sigma^k = \tau$, that is, we have some permutation σ with τ as a positive power (≥ 5).

■

Exercise 1.3.15. 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. [Use Exercise 10 and Exercise 24 of Section 1.]

Proof. Let $\sigma = \tau_1 \cdots \tau_m$ be the (disjoint) cycle decomposition of the permutation $\sigma \in S_n$. Then the order of each cycle τ_i is simply its length; so $|\tau_i| = m$ where τ_i is an m-cycle. Then let $r = \text{lcm}\left(|\tau_1|, \ldots, |\tau_m|\right)$. Then certainly we have

$$\sigma^r = \tau_1^r \tau_2^r \cdots \tau_m^r = e$$

since the disjoint cycles commute, thus $|\sigma| \leq r$.

Next, assume that $|\sigma| = t < r$. Then

$$e = \sigma^t = \tau_1^t \tau_2^t \cdots \tau_m^t$$

since these cycles are disjoint. Then we must have $\tau_i^t = e$ for all i, again because the cycles are disjoint, and so the order of each τ_i must divide t. That is, t is a common multiple of the $|\tau_i|$. But r is the least such common multiple, and so $t = r$.

■

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

Proof. Such a permutation is of the form $\sigma = \left(i_1\ i_2\right)\left(i_3\ i_4\right)$ where none of the i_j are equal. Then we have n choices for i_1, $(n-1)$ choices for i_2, $(n-2)$ for i_3, and $(n-3)$ for i_4. Thus, without considering ordering, there are $n\left(n-1\right)\left(n-2\right)\left(n-3\right)$ possible products of disjoint 2-cycles. Note that the order of the 2-cycles does not matter, so this must be divided by a factor of 2. Similarly, the order of the pair (i_1, i_2) does not matter, and similarly for the other cycle. Thus, we divide by two further factors of 2 to obtain $n\left(n-1\right)\left(n-2\right)\left(n-3\right)/8$ possible distinct disjoint 2-cycles in S_n.

■

Exercise 1.3.18. Find all numbers n such that S_5 contains an element of order n. [Use Exercise 15.]

Proof. We are asked to determine which element orders are possible in S_5. We could directly enumerate all permutations in S_5 and check by inspection, but this would be time-consuming and inelegant. Instead, we can use the results of Exercise 15, which states that the order of an element in S_n is equal to the least common multiple of the lengths of the cycles in its (unique) disjoint cycle decomposition.

Certainly the orders $n = 1, 2, 3, 4, 5$ are possible, since we have these n-cycles in S_5. It may be possible to obtain cycles of larger order if the lcm of the disjoint cycle factors is larger than 5. Let us consider the possibilities. Any product of disjoint 2-cycles is again a 2-cycle, since $\text{lcm}\left(2, \ldots, 2\right) = 2$. We cannot have a product of two disjoint 3-cycles, since $|S_n| = 5$. Thus, the only other (nontrivial) possibility is the product of a 2-cycle and a 3-cycle, which would be a 6-cycle.

Thus, $n = 6$ is a possibility.

■

Exercise 1.3.19. Find all numbers n such that S_7 contains an element of order n. [Use Exercise 15.]

Proof. This problem proceeds exactly as the previous one, albeit a bit more complicated. We can obviously have $n = 1, 2, \ldots, 7$, since these n-cycles can easily be constructed. Since there are $|S_7| = 7$ elements to work with, we have more possibilities for combinations of disjoint cycles. As in the previous Exercise, the product of a 2-cycle and a 3-cycle is a 6-cycle, already accounted for. We can include a further 2-cycle, but this gives again a 6-cycle. The product of two disjoint 3-cycles is possible, and is clearly another 3-cycle. A disjoint 2-cycle and a 4-cycle may be composed, resulting in a 4-cycle. We may have a 3-cycle and a 4-cycle, which results in a 12-cycle. Lastly, we may have a 2-cycle and a 5-cycle, resulting in a 10-cycle. Thus, possible orders of elements are $n = 1, \ldots, 7, 10, 12$.

■

Sec. 1.4 Matrix Groups

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

Exercise 1.4.1. Prove that $|GL_2(\mathbb{F}_2)| = 6$.

Proof. Recall that

$$\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z} = \left\{\overline{0}, \overline{1}\right\}$$

under the group operation of addition (modulo 2). Then $GL_2(\mathbb{F}_2)$ is the set of all 2×2 matrices with entries in $\left\{\overline{0}, \overline{1}\right\}$, and nonzero determinant. Hence, there are at most $2^4 = 16$ elements in $GL_2(\mathbb{F}_2)$. However, not all of these are valid, since several have zero determinant. Consider an arbitrary element

$$\begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} \quad \text{where } a_i \in \left\{\overline{0}, \overline{1}\right\} \text{ for } i = 1, 2, 3, 4$$

and we have $a_1a_4 - a_2a_3 \neq 0$. When is this determinant zero? It is zero when all $a_i = \overline{1}$, or when one (or both) of $\{a_1, a_4\}$ is zero and one (or both) of $\{a_2, a_3\}$ is zero. Combinatorially, there are 3 cases for which a_1 or a_4 (inclusive or) is $\overline{0}$, and 3 for when a_2 or a_3 is $\overline{0}$. This gives a total of 9 cases of zero determinant, plus another 1 for the case when $a_1 = a_2 = a_3 = a_4 = \overline{1}$. Thus, 10 out of the 16 possible 2×2 arrays of elements in $\mathbb{F}_2$ have zero determinant, leaving $6 = |GL_2(\mathbb{F}_2)|$ valid matrices.

■

Exercise 1.4.2. Write out all the elements of $GL_2(\mathbb{F}_2)$ and compute the order of each element.

Proof. From the previous Exercise 1.4.1, we know that this group has 6 elements, so we can explicitly enumerate them. They are

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

where the matrix elements 0 and 1 are shorthand for the residue classes $\overline{0}$ and $\overline{1}$ respectively. We can directly compute the orders of these elements by brute-force multiplication. I will omit the exact answers to preserve clean typesetting. The multiplication is easy, but note that the actual combinations of matrix elements are performed in the group $\mathbb{F}_2$. For example,

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

and the sums and products performed in the right-hand expression are the *field operations* on $\mathbb{F}_2$.

■

Exercise 1.4.3. Show that $GL_2(\mathbb{F}_2)$ is non-abelian.

Proof. This amounts to finding two elements which do not commute. By inspection we find that

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

but

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

■

Exercise 1.4.4. Show that if n is not prime then $\mathbb{Z}/n\mathbb{Z}$ is not a field.

First we will look at some simple examples to get intuition. This is an exploratory prelude to the true proof, from which we seek to understand what it is that differentiates this particular case (n non-prime) from others (n prime). To this end, let us consider $\mathbb{F}_3 = \mathbb{Z}/3\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}\}$. Note that 3 is prime. The operation tables for this set under the usual operations are

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{0}$	$\overline{1}$

$\cdot$	$\overline{1}$	$\overline{2}$
$\overline{1}$	$\overline{1}$	$\overline{2}$
$\overline{2}$	$\overline{2}$	$\overline{1}$

These are standard Cayley tables for a (finite) group operation: every element appears in every row and column. Things make sense. Next, let's consider $\mathbb{F}_4 = \mathbb{Z}/4\mathbb{Z}$. Now $n = 4$ is not prime, and can be written $4 = 2 \cdot 2$. We predict that something about these factors will

cause problems. In particular, these are multiplicative factors, so we expect problems with the multiplication operation on $\mathbb{F}_4$. The tables are

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{0}$	$\overline{1}$	$\overline{2}$

$\cdot$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{2}$	$\overline{2}$	$\overline{0}$	$\overline{2}$
$\overline{3}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Now, the addition table looks nice, but the multiplication table is problematic. The row and the column corresponding to the factor $\overline{2}$ do not contain all of the elements of $\mathbb{F}_4^\times$; in fact, the intersection of this row and column is $\overline{0}$, the additive identity element of $\mathbb{F}_4$, which is not even supposed to appear in the multiplication table, since $\overline{0} \notin \mathbb{F}_4^\times$. In other words, $\mathbb{F}_4^\times$ is not even closed under the multiplication operation!

In more generality, notice that if we can factor n into the product of two positive integers, say $n = st$, then we can find some element in $\mathbb{F}_n^\times$ which has a product equal to the *additive* identity, which is outside of $\mathbb{F}_n^\times$. From the examples above, one option for this element is s. Then note that $s^t = \underbrace{s + s + \ldots + s}_{t \text{ times}} \bmod n = n \bmod n = 0$ and this is not in the multiplicative set $\mathbb{F}_n^\times$.

Now for the formal proof:

> *Proof.* Consider the set $\mathbb{F}_n = \mathbb{Z}/n\mathbb{Z}$ with n non-prime. Recall that $\mathbb{F}_n$ is a field if it is an abelian group under addition and $\mathbb{F}_n^\times = \mathbb{F}_n - \{0\}$ is an abelian group under multiplication. Since n composite, we can decompose $n = st$, $s, t \in \mathbb{Z}^+ - \{1\}$, into a product of factors. Then notice that $\overline{s}, \overline{t} \in \mathbb{F}_n^\times$ and we have
>
> $$\overline{s} \cdot \overline{t} = \overline{st} = \overline{n} = \overline{0} \notin \mathbb{F}_n^\times$$
>
> and so $\mathbb{F}_n^\times$ is not closed under multiplication, and so cannot be an abelian group. Hence, $\mathbb{F}$ cannot be a field under these operations.
>
> ■

Exercise 1.4.5. Show that $GL_n(F)$ is a finite group if and only if F has a finite number of elements.

> *Proof.* First, assume F has a finite number of elements, say $|F| = q$. Then Exercise 1.4.6 applies (we could just replicate the proof here) and so $|GL_n(F)| < q^{n^2} < \infty$, and so $GL_n(F)$ is a finite group.
>
> Conversely, assume that $GL_n(F)$ is a finite group but assume by way of contradiction that F is not finite. Then we can easily construct an infinite number of $n \times n$ matrices over F with nonzero determinant: let $f \in F - \{0\}$, then fI_n is an $n \times n$ matrix with $\det(fI_n) = f^n \neq 0$, and so $fI_n \in GL_n(F)$ for all $f \in F - \{0\}$. Since there are infinitely many such f, we have infinitely many such elements of $GL_n(F)$. This is a contradiction of our assumption that $GL_n(F)$ is finite. Hence,

we must have F finite.

■

Exercise 1.4.6. If $|F| = q$ if finite prove that $|GL_n(F)| < q^{n^2}$.

This hearkens back to Exercise 1.4.1 where we studied the particular example of $GL_2(\mathbb{F}_2)$ and used the same argument to bound the number of possible elements of this group. We formalize and generalize this argument here.

Proof. Let $|F| = q$. Then $GL_n(F)$ is the set of all $n \times n$ matrices containing elements from q, with nonzero determinant. Then each matrix has n^2 elements, and each can be one of q possibilities, giving q^{n^2} possible candidate arrays for $GL_n(F)$. However, notice that several of these arrays are not valid, since they will have determinant zero; for example, the array of all zero elements (of F) is one of these q^{n^2} arrays but has zero determinant and thus is not permitted in $GL_n(F)$. Hence we know that q^{n^2} is never attained, so the bound (with inequality) holds:

$$|GL_n(F)| < q^{n^2}$$

■

Exercise 1.4.7. Let p be a prime. Prove that the order of $GL_2(\mathbb{F}_p)$ is $p^4 - p^3 - p^2 + p$ (do not just quote the order formula in this section). [Subtract the number of 2×2 matrices which are *not* invertible from the total number of 2×2 matrices over $\mathbb{F}_p$. You may use the fact that a 2×2 matrix is not invertible if and only if one row is a multiple of the other.]

Proof. We can directly count the number of ways in which a matrix

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

with $a, b, c, d \in \mathbb{F}_p$ is *not* in $GL_2(\mathbb{F}_p)$. This occurs if $ad - bc = 0$. We can break this down into cases and consider each separately. First, assume $a \neq 0$. Then

$$ad - bc = 0 \implies d = a^{-1}bc$$

and so d is uniquely determined by our choices of a, b, c, and so there are $p^2(p-1)$ choices for X with $a \neq 0$ (the $(p-1)$ factor results from a nonzero).

On the other hand, if $a = 0$, then d can be any of the p elements in $\mathbb{F}_p$, and we must have $bc = 0$. If $b = 0$, then c can be any of the p elements in $\mathbb{F}_p$. Alternately, if $b \neq 0$, for which there are $(p-1)$ possibilities, then $bc = 0 \implies c = b^{-1}0$ and so c is also uniquely specified. Thus there are $p(p + (p-1))$ possibilities for choices of X with $a = 0$.

Taken together, these two cases give a total of

$$p^2(p-1) + p(p + (p-1)) = p^3 - p^2 + 2p^2 - p = p^3 + p^2 - p$$

choices of X which have zero determinant. Since there are total of p^4 possible 2×2 matrices with elements from $\mathbb{F}_p$, we have a total of

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

elements in $GL_2(\mathbb{F}_p)$.

■

Exercise 1.4.8. Show that $GL_n(F)$ is non-abelian for any $n \geq 2$ and any F.

Proof. The proof proceeds by induction on $n \geq 2$. Let F be an arbitrary field. For the case $n = 2$, let 1 be the multiplicative identity of F and 0 be the additive identity of F, guaranteed to exist in any field F by the field axioms. Then

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

and

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

For these two arrays to be equal, we would need $1^2 = 0$, but by definition of multiplicative identity we have $1^1 = 1$. Hence, $GL_2(F)$ is non-abelian.

Next, assume that $GL_n(F)$ is non-abelian. To show $GL_{n+1}(F)$ is non-abelian, we need to find two elements which do not commute. Let $A, B \in GL_n(F)$ such that $AB \neq BA$ (if no such existed, then $GL_n(F)$ would be abelian). Then notice that

$$\begin{pmatrix} A & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} B & 0 \\ 0 & 1 \end{pmatrix} \in GL_{n+1}(F)$$

where 1 is the multiplicative identity of F and 0 is a vector containing the additive identity of F. Upon multiplication via typical block-matrix algebra we have

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

and so we have two elements of $GL_{n+1}(F)$ which do not commute, so this group is non-abelian.

By the principle of mathematical induction, the hypothesis holds for any $n \geq 2$, and for any arbitrary field F.

■

Exercise 1.4.9. Prove that the binary operation of matrix multiplication of 2×2 matrices with real number entries is associative.

This is a masochistic Exercise, and is not particularly illuminating. It is just straightforward, brute-force computation of matrix products in the usual way. I will not clutter this up by fully solving this.

Proof. Let A, B, C be 2×2 matrices with real number entries (no condition is made on determinant because it does not affect associativity; if it is true in general, then it is true for those matrices with nonzero determinant). Then we write $A = \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix}$ and similarly for B and C. Then

$$\begin{aligned} A\left(BC\right) &= \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} \left[\begin{pmatrix} b_1 & b_2 \\ b_3 & b_4 \end{pmatrix} \begin{pmatrix} c_1 & c_2 \\ c_3 & c_4 \end{pmatrix} \right] \\ &= \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} \begin{pmatrix} b_1c_1 + b_2c_3 & b_1c_2 + b_2c_4 \\ b_3c_1 + b_4c_3 & b_3c_2 + b_4c_4 \end{pmatrix} \\ &= \begin{pmatrix} a_1b_1c_1 + a_1b_2c_3 + a_2b_3c_1 + a_2b_3c_1 + a_2b_4c_3 & \cdots \\ \cdots & \cdots \end{pmatrix} \end{aligned}$$

and similarly for the other product

$$\left(AB\right)C = \ldots$$

From these expressions, we can observe that the corresponding elements are equal, and so we conclude that matrix multiplication (in the case of 2×2 matrices over $\mathbb{R}$, at least) is associative.

■

Exercise 1.4.10. Let $G = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mid a, b, c \in \mathbb{R}, a \neq 0, c \neq 0 \right\}$.

- 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.
- Find the matrix inverse of $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$ and deduce that G is closed under inverses.
- Deduce that G is a subgroup of $GL_2\left(\mathbb{R}\right)$ (cf. Exercise 26, Section 1).
- Prove that the set of elements of G whose two diagonal entries are equal (i.e., $a = c$) is also a subgroup of $GL_2\left(\mathbb{R}\right)$.

Proof.

- The product of two arbitrary elements in G is

$$\begin{pmatrix} a_1 & a_2 \\ 0 & a_3 \end{pmatrix} \begin{pmatrix} b_1 & b_2 \\ 0 & b_3 \end{pmatrix} = \begin{pmatrix} a_1b_1 & a_1b_2 + a_2b_3 \\ 0 & a_3b_3 \end{pmatrix} \in G$$

and so G is closed under the usual matrix multiplication.

- Given arbitrary group element, $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$, note that

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

and

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

so that $\begin{pmatrix} \frac{1}{a} & -\frac{b}{ac} \\ 0 & \frac{1}{c} \end{pmatrix}$ is an inverse for $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$, which is well-defined since $a, c \neq 0$. Hence, G is closed under inverses.

- By Exercise 26 of Section 1, a subgroup is defined as a subset of a group which is closed under the same binary operation as the group, as well as closed under inversion of the operation. We have seen that G is closed under the matrix multiplication operation of $GL_2(\mathbb{R})$, and also that G contains its inverses; thus, G is a subgroup of $GL_2(\mathbb{R})$.

- Let $H = \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \mid a, b \in \mathbb{R}, a \neq 0 \right\}$. Then certainly

$$\begin{pmatrix} a & b \\ 0 & a \end{pmatrix}\begin{pmatrix} c & d \\ 0 & c \end{pmatrix} = \begin{pmatrix} ac & ad+bc \\ 0 & ac \end{pmatrix} \in H$$

and an inverse of $\begin{pmatrix} a & b \\ 0 & a \end{pmatrix}$ is easily $\begin{pmatrix} \frac{1}{a} & -\frac{b}{a^2} \\ 0 & \frac{1}{a} \end{pmatrix}$ from the above inverse computations, since H is a subset of G. Hence, H is also a subgroup of $GL_2(\mathbb{R})$.

■

The next exercise introduces the *Heisenberg group* over the field F and develops some of its basic properties. When $F = \mathbb{R}$ this group plays an important role in quantum mechanics and signal theory by giving a group theoretic interpretation (due to H. Weyl) of Heisenberg's Uncertainty Principle. Note also that the Heisenberg group may be defined more generally — for example, with entries in $\mathbb{Z}$.

Exercise 1.4.11. Let $H(F) = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \mid a, b, c \in F \right\}$ — called the *Heisenberg group* over F. Let $X = \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}$ and $Y = \begin{pmatrix} 1 & d & e \\ 0 & 1 & f \\ 0 & 0 & 1 \end{pmatrix}$ be elements of $H(F)$.

- Compute the matrix product 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).

- Find an explicit formula for the matrix inverse X^{-1} and deduce that $H(F)$ is closed under inverses.
- Prove the associative law for $H(F)$ and deduce that $H(F)$ is a group of order $|F|^3$. (Do not assume that matrix multiplication is associative.)
- Find the order of each element of the finite group $H(\mathbb{Z}/2\mathbb{Z})$.
- Prove that every nonidentity element of the group $H(\mathbb{R})$ has infinite order.

Proof.

- The product XY is computed as usual:

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

and so $H(F)$ is closed under products. However, note that

$$YX = \begin{pmatrix} 1 & d & e \\ 0 & 1 & f \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a+d & b+cd+e \\ 0 & 1 & c+f \\ 0 & 0 & 1 \end{pmatrix}$$

and the upper-right-most element of these matrices are the only which may not be equal. In particular, $XY \neq YX$ if and only if $af \neq cd$, and so any and $af - cd \neq 0$ gives two matrices X, Y which do not commute. Hence, $H(F)$ is not commutative.

- Note that $X^{-1} = \begin{pmatrix} 1 & -a & ac-b \\ 0 & 1 & -c \\ 0 & 0 & 1 \end{pmatrix}$ is a bona-fide inverse for X, and it is clearly in $H(F)$. Thus, $H(F)$ is closed under inversion.
- I am going to skip these computations, but as always it amounts to computing $A(BC)$ and $(AB)C$ and showing that these are equal for any triple $A, B, C \in H(F)$; it is rather straightforward, but tedious. Finally, we can conclude that $H(F)$ is a subgroup of $GL_3(F)$, and so is a group by itself. For each element of $H(F)$, we have 3 matrix elements which are unspecified elements of F, hence we have $|F|^3$ possible matrices. Since — unlike in the larger group $GL_3(F)$ — the constraint of nonzero determinant does not influence the choice of these 3 matrix elements, we conclude that $|H(F)| = |F|^3$.
- Consider the particular case where $F = \mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z} = \{\overline{0}, \overline{1}\}$. From the previous part of the problem, $|F| = 2$ and so $|H(F)| = 2^3 = 8$ elements:

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

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

I will not go through the computation of these orders, just to save space with the typesetting. It is done in the usual way: brute-force compute products of each of these until we hit the identity element I_3.

- Consider the group $H(\mathbb{R})$. Let X be some nonidentity element, i.e., in the expression for X above, this means that at least one of a, b, or c is nonzero. Then notice that

$$X^2 = \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2a & 2b+ac \\ 0 & 1 & 2c \\ 0 & 0 & 1 \end{pmatrix}$$

$$X^3 = \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2a & 2b+ac \\ 0 & 1 & 2c \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 3a & 3b+3ac \\ 0 & 1 & 3c \\ 0 & 0 & 1 \end{pmatrix}$$

$$X^4 = \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 3a & 3b+3ac \\ 0 & 1 & 3c \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 4a & 4b+6ac \\ 0 & 1 & 4c \\ 0 & 0 & 1 \end{pmatrix}$$

$$X^5 = \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 4a & 4b+6ac \\ 0 & 1 & 4c \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 5a & 5b+10ac \\ 0 & 1 & 5c \\ 0 & 0 & 1 \end{pmatrix}$$

and so on. We can see a pattern start to emerge:

$$X^n = \begin{pmatrix} 1 & na & nb + \frac{n(n-1)}{2}ac \\ 0 & 1 & nc \\ 0 & 0 & 1 \end{pmatrix}$$

and we can prove that this holds by induction. We know it holds for $n = 2$ (and also for $n = 3, 4, 5$). Assume it holds for arbitrary $k \in \mathbb{Z}^+$: $X^k =$

$\begin{pmatrix} 1 & ka & kb+\frac{k(k-1)}{2}ac \\ 0 & 1 & kc \\ 0 & 0 & 1 \end{pmatrix}$. Then

$$\begin{aligned} X^{k+1} &= X^k X \\ &= \begin{pmatrix} 1 & ka & kb+\frac{k(k-1)}{2}ac \\ 0 & 1 & kc \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & (k+1)\,a & (k+1)\,b+\frac{(k+1)k}{2}ac \\ 0 & 1 & (k+1)\,c \\ 0 & 0 & 1 \end{pmatrix} \end{aligned}$$

and so the expression is true for arbitrary $n \in \mathbb{Z}^+$.

Finally, we can use this pattern to conclude that every nonzero $X \in H(\mathbb{R})$ has infinite order. Assume by way of contradiction that $X = \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}$ has finite order k. Then $X^k = I_3$, or, using our expression,

$$\begin{pmatrix} 1 & ka & kb+\frac{k(k-1)}{2}ac \\ 0 & 1 & kc \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Since X is nonzero, this means that a, b, and c are not all simultaneously zero. If a nonzero, then $ka = 0$ is not satisfied by any $k \in \mathbb{Z}^+$, and so a must be zero. Similarly, c must be zero. But then we must have b nonzero for X to be nonzero. But the above equation insists $kb + \frac{k(k-1)}{2}ac = kb = 0$, which is only true if $b = 0$, a contradiction. Thus, no nonzero element of X may have finite order.

■

1.5 The Quaternion Group

Exercise 1.5.1. Compute the order of each of the elements in Q_8.

Proof. From the definition of the product operation on Q_8, the element 1 is the identity. Hence, $|1| = 1$. Also, $(-1)\cdot(-1) = 1 \implies |-1| = 2$. Also, $i \cdot i = -1$ and $-1^2 = 1$ implies $|i| = |j| = |k| = 4$. Finally, note that $-i = (-1)\cdot i$, and so

$$(-i)^2 = (-1)\cdot i\cdot(-1)\cdot i = (-1)\cdot(-i)\cdot i = (-1)^2\cdot i^2 = 1\cdot -1 = -1$$

and so $|-i| = |-j| = |-k| = 4$ as well.

Note that we were able to move around the negative signs and manipulate the products only by virtue of the extensive definition of the product on Q_8; without it, we would have no sensible way to know how these products would behave.

■

Exercise 1.5.2. Write out the group tables for S_3, D_8 and Q_8.

Proof. This is just straightforward computation of the various pairwise products of group elements.

S_3	()	(1 2)	(1 3)	(2 3)	(1 2 3)	(1 3 2)
()	()	(1 2)	(1 3)	(2 3)	(1 2 3)	(1 3 2)
(1 2)	(1 2)	()	(1 2 3)	(1 3 2)	(1 3)	(2 3)
(1 3)	(1 3)	(1 3 2)	()	(1 2 3)	(2 3)	(1 2)
(2 3)	(2 3)	(1 2 3)	(1 3 2)	()	(1 2)	(1 3)
(1 3 2)	(1 3 2)	(1 3)	(2 3)	(1 2)	()	(2 3)
(1 2 3)	(1 2 3)	(2 3)	(1 2)	(1 3)	(1 3 2)	()

Recall that for the dihedral groups, the presentation we have used specifies that $rs = sr^{-1}$, and in the case of D_8, $r^{-1} = r^3$. This can help us compute these products.

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

■

Exercise 1.5.3. Find a set of generators and relations for Q_8.

Proof. Recall that a set of generators for Q_8 is a subset $S \subset Q_8$ such that any arbitrary element of Q_8 can be written as a finite product of elements of S and their inverses. Any equations in Q_8 which the generators satisfy are called relations in G. A presentation of G is a set of generators S along with a collection of relations $R_1, R_2, \ldots, R_m$ such that any relation among the elements of S can be deduced

from these. Then we can write

$$Q_8 = \langle S \mid R_1, R_2, \ldots, R_m \rangle$$

Obvious generators for Q_8 are $S = \{-1, i, j, k\}$, since all of the elements can be written as products of these.

■

Sec. 1.6 Homomorphisms and Isomorphisms

Let G and H be groups.

Exercise 1.6.1. Let $\phi : G \to H$ be a homomorphism.

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

Proof. These are standard induction proofs. They inform us that — at least with regard to powers of an individual group element — homomorphisms preserve behaviors nicely. Let $\phi : G \to H$ be a homomorphism.

- Note that
$$\phi\left(x^2\right) = \phi(x \cdot x) = \phi(x) \cdot \phi(x) = \phi(x)^2$$
where we used the defining property of homomorphisms. This also holds trivially for $n = 1$.

  Next, assume $\phi(x^n) = \phi(x)^n$ for some $n \in \mathbb{Z}$. Then
$$\begin{aligned} \phi\left(x^{n+1}\right) &= \phi(x^n \cdot x) \\ &= \phi(x^n)\,\phi(x) \\ &= \phi(x)^n\,\phi(x) \\ &= \phi(x)^{n+1} \end{aligned}$$
and so by the principle of mathematical induction, the statement about homomorphisms applied to powers holds for $n \in \mathbb{Z}$.

- Next, let $n \in \mathbb{Z}^-$. Let $x \in G$, so that $x^{-1} \in G$ by the group axioms of G. Notice that
$$\begin{aligned} \phi(x)\,\phi\left(x^{-1}\right) &= \phi\left(xx^{-1}\right) \\ &= \phi(1) \end{aligned}$$
where 1 is the identity element of G. We can see that $\phi(1)$ is the group element of H (easy to show) and so the above shows that $\phi(x)^{-1} = \phi(x^{-1})$.

Next, notice that we can use the previous part of the proof to show that we have

$$\begin{aligned}\phi\left(x^{-(n+1)}\right) &= \phi\left(\left(x^{n+1}\right)^{-1}\right)\\ &= \phi\left(x^{n+1}\right)^{-1}\\ &= \left(\phi\left(x\right)^{n+1}\right)^{-1}\\ &= \phi\left(x\right)^{-(n+1)}\end{aligned}$$

and so the statement holds for arbitrary $-n$, $n \in \mathbb{Z}$.

■

Exercise 1.6.2. If $\phi : G \to H$ is an isomorphism, prove that $|\phi(x)| = |x|$ 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. Let $\phi : G \to H$ be an isomorphism. Let $x \in G$ have order n. Then n is the smallest integer such that $x^n = 1$. From the previous problem, we have

$$\phi\left(x\right)^n = \phi\left(x^n\right) = \phi\left(1\right)$$

which is the identity element in H. Thus, $\phi(x)$ has order at most n. Assume by way of contradiction that $\phi(x)$ has order $k < n$; that is, $\phi\left(x\right)^k = \phi\left(1\right)$. Then we know that

$$\phi\left(1\right) = \phi\left(x\right)^k = \phi\left(x^k\right)$$

but since ϕ is a bijection (since it is an isomorphism) we have $x^k = 1$. However, $k < n$ and we assume n is the smallest integer such that this is true. This is a contradiction, and so we conclude that $\phi(x)$ has order at least n. Thus, we can finally conclude that $|\phi(x)| = |x|$ for any $x \in G$ of finite order.

We must also consider the case in which x has infinite order. Assume by way of contradiction that $\phi(x)$ has finite order, say k. Then from the same logic above we have $\phi\left(1\right) = \phi\left(x\right)^k = \phi\left(x^k\right)$ and so $x^k = 1$ by bijectivity of ϕ. But then x has finite order k, a contradiction. Thus $\phi(x)$ also has infinite order.

These proofs have relied on the bijectivity of ϕ, a feature of an isomorphism which homomorphisms do not enjoy. A simple example is that in which the target group H is the trivial group $H = \{1\}$ and $\phi : G \to H$ sends every $g \in G$ to $1 \in H$: $\phi(g) = 1$. Then for $g_1, g_2 \in G$ we have

$$1 \cdot 1 = \phi\left(g_1\right)\phi\left(g_2\right) = \phi\left(g_1 g_2\right) = 1$$

and so ϕ is automatically a homomorphism, and every element of H (only the identity) has order 1. However, in general, the domain group G need not have

every element of order 1 (this is only true if G is also the trivial group). Hence, **the bijectivity guaranteed by isomorphisms is essential**.

■

Exercise 1.6.3. If $\phi : G \to H$ is an isomorphism, prove that G is abelian if and only if H is abelian. If $\phi : G \to H$ is a homomorphism, what additional conditions on ϕ (if any) are sufficient to ensure that if G is abelian, then so is H?

Proof. Let $\phi : G \to H$ be an isomorphism. Assume first that G is abelian. Let $h_1, h_2 \in H$. Then since ϕ is an isomorphism, and so is surjective, there are $g_1, g_2 \in G$ with $\phi(g_1) = h_1$ and $\phi(g_2) = h_2$. The

$$\begin{aligned} h_1 h_2 &= \phi(g_1)\,\phi(g_2) \\ &= \phi(g_1 g_2) \\ &= \phi(g_2 g_1) \\ &= \phi(g_2)\,\phi(g_1) \\ &= h_2 h_1 \end{aligned}$$

and so H is abelian.

Conversely, assume H is abelian. Let $g_1, g_2 \in G$. Then $\phi(g_1), \phi(g_2) \in H$. Then

$$\begin{aligned} g_1 g_2 &= \phi^{-1}(\phi(g_1))\,\phi^{-1}(\phi(g_2)) \\ &= \phi^{-1}(\phi(g_1)\,\phi(g_2)) \end{aligned}$$

where we used the fact that ϕ^{-1} is a homomorphism since ϕ is. Continuing,

$$\begin{aligned} g_1 g_2 &= \phi^{-1}(\phi(g_1)\,\phi(g_2)) \\ &= \phi^{-1}(\phi(g_2)\,\phi(g_1)) \\ &= \phi^{-1}(\phi(g_2))\,\phi^{-1}(\phi(g_1)) \\ &= g_2 g_1 \end{aligned}$$

and so G is abelian.

Note that our proofs required only the fact that ϕ, as a homomorphism, is surjective, so that we could find some $g \in G$ mapping to an arbitrary $h \in H$. Thus, the injectivity of an isomorphism is a bit superfluous.

■

Exercise 1.6.4. Prove that the multiplicative groups $\mathbb{R} - \{0\}$ and $\mathbb{C} - \{0\}$ are not isomorphic.

Proof. In light of some of the previous Exercises, we can try to find ways to rule out the possibility of an isomorphism. Let us look at the orders of the elements in these groups.

In $\mathbb{R} - \{0\}$, what are the possibilities of group element orders? Any num-

ber greater than 1 in magnitude, upon taking powers, will multiply toward $\pm\infty$. Numbers less than 1 in magnitude will multiply toward 0. These numbers thus all have infinite order. 1 has order 1 and -1 has order 2.

Next, consider $\mathbb{C} - \{0\}$. With the standard definitions of complex multiplication, we have much more exotic behaviors. The identity of this group is $1 = (1, 0)$, still with order 1. However, note that we have a number $(0, 1) = i \in \mathbb{C} - \{0\}$ which has order 4. Since order is preserved by isomorphisms, there must be some order-4 element in $\mathbb{R} - \{0\}$ but we know this to not be the case. Thus, these two groups cannot be isomorphic.

■

Exercise 1.6.5. Prove that the additive groups $\mathbb{R}$ and $\mathbb{Q}$ are not isomorphic.

We could generalize this proof to say that a countable and an uncountable group can never be isomorphic (or, in particular, bijective).

Proof. Assume that there is some isomorphism $\phi : \mathbb{R} \to \mathbb{Q}$. Then, in particular, ϕ is a bijection. Since $\mathbb{Q}$ is countable, there exists a bijection $\omega : \mathbb{Q} \to \mathbb{N}$. Then by properties of compositions of bijections, $\omega \circ \phi : \mathbb{R} \to \mathbb{N}$ is a bijection, and so $\mathbb{R}$ is countable. However, it is known that $\mathbb{R}$ is uncountable. Hence, $\mathbb{R}$ and $\mathbb{Q}$ cannot be isomorphic.

■

Exercise 1.6.6. Prove that the additive groups $\mathbb{Z}$ and $\mathbb{Q}$ are not isomorphic.

Proof. Since $\mathbb{Z}$ and $\mathbb{Q}$ are both countable, we cannot use the results of the previous Exercise. Thus, we must resort to invalidating the axioms of an isomorphism. Let us try to invalidate, in particular, the defining property of a homomorphism. A key feature of the rational numbers is that we can express the same number in multiple (infinitely many) ways. For instance, $2 = \frac{2}{1} = \frac{4}{2}$.

Assume that there is some isomorphism $\phi : \mathbb{Q} \to \mathbb{Z}$. Then let $x = \phi(1)$. But then

$$x = \phi\left(\frac{1}{2} + \frac{1}{2}\right) = 2\,\phi\left(\frac{1}{2}\right)$$

and

$$x = \phi\left(\frac{1}{3} + \frac{1}{3} + \frac{1}{3}\right) = 3\,\phi\left(\frac{1}{3}\right)$$

and in general

$$x = \phi\left(\frac{1}{n} + \ldots + \frac{1}{n}\right) = n\,\phi\left(\frac{1}{n}\right)$$

for any $n \in \mathbb{Z}^+$. Hence x has a factor of n for every $n \in \mathbb{Z}^+$. What does this mean about x?

Assume x is divisible by every positive integer, but $x \neq 0$.

■

Exercise 1.6.7. Prove that D_8 and Q_8 are not isomorphic.

Proof. We can look at the group operation tables constructed in Exercise 1.5.2 to get some intuition for why these groups might not be isomorphic. We can consider the orders of the elements in each of the groups, as in Exercise 1.6.4, and show that the orders give us problems. The multiplication tables can help us see the group elements which have order 2. Specifically, the non-identity entries along the main diagonal of the tables will be the identity if the element of that row (or column) has order 2.

In the table for D_8, we can read off 5 elements which have order 2. In Q_8, there is only 1 element with order 2. Since isomorphisms preserve order, an isomorphism from D_8 to Q_8 would have to send these 5 elements of order 2 to the single order-2 element in Q_8, but this would not be injective. Thus, no isomorphism can exist.

■

Exercise 1.6.8. Prove that if $n \neq m$, S_n and S_m are not isomorphic.

Proof. We know that S_n has order $n!$ and S_m has order $m!$, and so these groups have different orders for $n \neq m$. Since these orders are finite, we can have no isomorphism (a bijection) between the two groups.

■

Exercise 1.6.9. Prove that D_{24} and S_4 are not isomorphic.

Exercise 1.6.10. Fill in the details of the proof that the symmetric groups S_Δ and S_Ω are isomorphic if $|\Delta| = |\Omega|$ as follows: let $\theta : \Delta \to \Omega$ be a bijection. Define

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

and prove the following.

- 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.
- ϕ is a bijection from S_Δ onto S_Ω. [Find a 2-sided inverse for ϕ.]
- ϕ is a homomorphism, that is, $\phi(\sigma \circ \tau) = \phi(\sigma) \circ \phi(\tau)$.

Note the similarity to the *change of basis* or *similarity* transformations for matrices (we shall see the connections between these later in the text).

Proof. Let the $\theta : \Delta \to \Omega$ be a bijection on sets Δ, Ω, and define ϕ as a mapping between the groups of permutations of these sets (drawing a picture helps).

- Let $\sigma \in S_\Delta$. Then we need to show that $\phi(\sigma) = \theta \circ \sigma \circ \theta^{-1}$ is a permutation of Ω, i.e., it is a bijection from Ω to itself. First, let $a, b \in \Omega$ with $\phi(\sigma)(a) = \phi(\sigma)(b)$. Then note that since σ is a bijection (as a permutation) on Δ and θ is a bijection from Δ to Ω, both σ and θ are injective. Also, as a bijection,

θ^{-1} is injective. So

$$\phi(\sigma)(a) = \theta \circ \sigma \circ \theta^{-1}(a) = \theta\left(\sigma\left(\theta^{-1}(a)\right)\right)$$

and similarly

$$\phi(\sigma)(b) = \theta\left(\sigma\left(\theta^{-1}(b)\right)\right)$$

Since $\phi(\sigma)(a) = \phi(\sigma)(b)$, we have

$$\theta\left(\sigma\left(\theta^{-1}(a)\right)\right) = \theta\left(\sigma\left(\theta^{-1}(b)\right)\right)$$

and so by injectivity of θ we have

$$\sigma\left(\theta^{-1}(a)\right) = \sigma\left(\theta^{-1}(b)\right)$$

Then by injectivity of σ we have

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

and lastly by injectivity of θ^{-1} we have

$$a = b$$

and so $\phi(\sigma)$ is an injective map on Ω.

Next, let $y \in \Omega$. Then to show surjectivity we must demonstrate some $x \in \Omega$ such that $\phi(\sigma)(x) = \theta \circ \sigma \circ \theta^{-1}(x) = y$. Then since σ is a permutation, it has an inverse, σ^{-1}. Thus, note that $x = \theta \circ \sigma^{-1} \circ \theta(y) = \phi(\sigma^{-1})(y)$ does the trick:

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

and so ϕ is injective. Thus, $\phi(\sigma)$ is a permutation of Ω for any permutation σ of Δ; it is well defined.

- We want to show that $\phi : S_\Delta \to S_\Omega$ is a bijection. We could try to show directly that ϕ is injective and surjective, but an equivalent condition for bijectivity is the existence of a 2-sided inverse for ϕ; as per the problem hint, this is what we will seek. Since ϕ takes any permutation $\sigma \in S_\Delta$ and returns a permutation $\theta \circ \sigma \circ \theta^{-1} \in S_\Omega$, the inverse should take a permutation $\omega \in S_\Omega$ and return a permutation $\phi^{-1}(\omega) \in S_\Delta$. By inspection, let us try $\phi^{-1}(\omega) = \theta^{-1} \circ \omega \circ \theta$. Then

$$\phi \circ \phi^{-1}(\omega) = \theta \circ \left(\theta^{-1} \circ \omega \circ \theta\right) \circ \theta^{-1} = \omega$$

for arbitrary $\omega \in S_\Omega$ and we have

$$\phi^{-1} \circ \phi(\sigma) = \theta^{-1} \circ \left(\theta \circ \sigma \circ \theta^{-1}\right) \circ \theta = \sigma$$

for arbitrary $\sigma \in S_\Delta$. Thus our ϕ^{-1} is a 2-sided inverse for ϕ, and so ϕ is a bijection.

- The last thing to prove to conclude that our ϕ is an isomorphism on the symmetric groups is that ϕ is a homomorphism, i.e., it preserves the group's structures. Let $\sigma, \tau \in S_\Delta$. Then note that $\theta^{-1} \circ \theta = 1$ is the identity map on Δ, since θ bijective. Then

$$\begin{aligned}
\phi(\sigma \circ \tau) &= \theta \circ (\sigma \circ \tau) \circ \theta^{-1} \\
&= \theta \circ \sigma \circ 1 \circ \tau \circ \theta^{-1} \\
&= \theta \circ \sigma \circ \left(\theta^{-1} \circ \theta\right) \circ \tau \circ \theta^{-1} \\
&= \left(\theta \circ \sigma \circ \theta^{-1}\right) \circ \left(\theta \circ \tau \circ \theta^{-1}\right) \\
&= \phi(\sigma) \circ \phi(\tau)
\end{aligned}$$

and so ϕ is a homomorphism between the symmetric groups on Δ and Ω.

Thus, we have shown all the conditions required for ϕ to be an isomorphism between the symmetric groups on Δ and Ω. To summarize, given two bijective sets, we can construct an isomorphism between the symmetric groups on these sets: the symmetric groups correspond to shuffling the elements, and the isomorphism corresponds to a relabeling of the shuffles.

■

Exercise 1.6.11. Let A and B be groups. Prove that $A \times B \cong B \times A$.

Proof. To show these are isomorphic, we need to explicitly construct a bijection $\phi : A \times B \to B \times A$ and show that it is a homomorphism. An obvious candidate is ϕ defined as

$$\phi((a, b)) = (b, a)$$

for all $(a, b) \in A \times B$. If $\phi((a, b)) = \phi((c, d))$, that means that $(b, a) = (d, c)$, and so by definition of equality in Cartesian product spaces we have $a = c$ and $b = d$, i.e., $(a, b) = (c, d)$, so ϕ injective. Also, if $(b, a) \in B \times A$, then $(a, b) \in A \times B$ with $\phi((a, b)) = (b, a)$, so ϕ is surjective. Hence ϕ is a bijection.

Note that none of this has yet taken into account the group structures of A and B. This is required for discussion of homomorphisms, a group theoretic topic. Recall that $A \times B$ naturally inherits the groups structures of A and B under the direct product operation, represented here by $\cdot$. To show that ϕ is a

homomorphism, let $(a,b),(c,d) \in A \times B$. Then

$$\begin{aligned}\phi((a,b)) \cdot \phi((c,d)) &= (b,a) \cdot (d,c) \\ &= (bd, ac) \\ &= \phi((ac, bd)) \\ &= \phi((a,b) \cdot (c,d))\end{aligned}$$

and so ϕ is a homomorphism. Hence, we conclude that ϕ is an isomorphism, and so the groups $A \times B$ and $B \times A$ are isomorphic.

■

Exercise 1.6.12. 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. We need to construct an isomorphism $\phi : G \times C \to A \times H$. Breaking apart the domain and codomain, ϕ must map $(A \times B) \times C$ into $A \times (B \times C)$. It seems almost trivial[a] to postulate the function

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

as the function we need. Let $\phi((a_1,b_1),c_1) = \phi((a_2,b_2),c_2)$. Then $(a_1,(b_1,c_1)) = (a_2,(b_2,c_2))$ and so $a_1 = a_2$ and $(b_1,c_1) = (b_2,c_2)$. Then $b_1 = b_2$ and $c_1 = c_2$, and so ϕ is injective. Let $(a,(b,c)) \in A \times (B \times C)$ be arbitrary; then it is easy to see that $((a,b),c) \in (A \times B) \times C$ maps to it under ϕ, so ϕ surjective. Thus ϕ is a bijection. Lastly, let $((a_1,b_1),c_1),((a_2,b_2),c_2) \in (A \times B) \times C$, arbitrary, and note that

$$\begin{aligned}\phi((a_1,b_1),c_1) \cdot \phi((a_2,b_2),c_2) &= (a_1,(b_1,c_1)) \cdot (a_2,(b_2,c_2)) \\ &= (a_1a_2, (b_1,c_1) \cdot (b_2,c_2)) \\ &= (a_1a_2, (b_1b_2, c_1c_2)) \\ &= \phi((a_1a_2, b_1b_1), c_1c_2) \\ &= \phi((a_1,b_1) \cdot (a_2,b_2), c_1c_2) \\ &= \phi(((a_1,b_1),c_1) \cdot ((a_2,b_2),c_2))\end{aligned}$$

and so ϕ is a homomorphism. Thus, ϕ is an isomorphism between the two product groups.

■

[a] Note that these spaces are, indeed, distinct. The parenthesis do seem to matter when dealing with the Cartesian product.

Exercise 1.6.13. Let G and H be groups and let $\phi : G \to H$ be a homomorphism. Prove that the image of ϕ, $\phi(G)$, is a subgroup of H (cf. Exercise 26 of Section 1). Prove that if ϕ is injective then $G \cong \phi(G)$.

Proof. Let $a, b \in \phi(G) \subset H$. Then there are $g, h \in G$ such that $\phi(g) = a$ and $\phi(h) = b$, and so

$$\begin{aligned} ab &= \phi(g)\phi(h) \\ &= \phi(gh) \end{aligned}$$

and so $ab \in \phi(G)$ since $gh \in G$ by group axioms. Similarly, notice that if $a = \phi(g)$ for some $g \in G$, then $g^{-1} \in G$ and we have

$$\begin{aligned} a\phi\left(g^{-1}\right) &= \phi(g)\phi\left(g^{-1}\right) \\ &= \phi\left(gg^{-1}\right) \\ &= \phi(1) \\ &= 1_H \end{aligned}$$

so that $a^{-1} = \phi(g^{-1})$. Since $g^{-1} \in G$, $a^{-1} \in \phi(G)$. Thus, $\phi(G)$ is closed under the group operation and under inversion, so it is a subgroup of H, the codomain of ϕ.

Assume now that ϕ is injective. Then for every $a \in \phi(G)$, there exists by definition some $g \in G$ with $\phi(g) = a$; hence, ϕ is surjective as a map from G to $\phi(G)$. Then it is a bijective homomorphism, and so $G \cong \phi(G)$.

■

Exercise 1.6.14. Let G and H be groups and let $\phi : G \to H$ be a homomorphism. Define the *kernel* of ϕ to be $\{g \in G \mid \phi(g) = 1_H\}$ (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 (cf. Exercise 26 of Section 1) of G. Prove that ϕ is injective if and only if the kernel of ϕ is the identity subgroup of G.

Proof. Let $g, h \in \text{Kernel}(\phi)$ where this set is the kernel of ϕ as defined in the problem statement. Then

$$\begin{aligned} \phi(gh) &= \phi(g) \cdot \phi(h) \\ &= 1_H \cdot 1_H \\ &= 1_H \end{aligned}$$

by the defining property of ϕ as a homomorphism. Thus we have $gh \in \text{Kernel}(\phi)$, so it is closed under the group operation of G.

Next, $g^{-1} \in G$ by the group axioms of G. Then we have

$$\begin{aligned} \phi\left(g^{-1}\right) &= \phi(g)^{-1} \\ &= 1_H^{-1} \\ &= 1_H \end{aligned}$$

and so $g^{-1} \in \text{Kernel}(\phi)$. Thus, it is closed under inverses, and so finally is a subgroup of G.

For the second statement, assume first that the kernel of ϕ is the (trivial) identity subgroup of G, $\{1_G\}$. Then let $a, b \in G$ such that $\phi(a) = \phi(b)$. Then

$$\begin{aligned} 1_H &= \phi(a)\,\phi(a)^{-1} \\ &= \phi(b)\,\phi\left(a^{-1}\right) \\ &= \phi\left(ba^{-1}\right) \end{aligned}$$

where for the second equation we simultaneously used the identity $\phi(a) = \phi(b)$ (our assumption) and the fact that we can pull exponents inside of homomorphism operations. Thus, $ba^{-1} \in \text{Kernel}(\phi)$. Then $ba^{-1} = 1_G$ and so $b = a$. Thus ϕ is injective in this case.

Conversely, assume that ϕ is injective, and let $g \in \text{Kernel}(\phi)$. But then

$$\phi(g) = 1_H = \phi(1_G)$$

and so by injectivity of ϕ, $g = 1_G$. Thus the kernel is $\text{Kernel}(\phi) = \{1_G\}$, the identity subgroup.

■

Exercise 1.6.15. Define a map $\pi : \mathbb{R}^2 \to \mathbb{R}$ by $\pi((x, y)) = x$. Prove that π is a homomorphism and find the kernel of π (cf. Exercise 14).

Proof. This is the projection map of $\mathbb{R}^2$ onto the first component. Let $(x_1, y_1), (x_2, y_2) \in \mathbb{R}^2$ and note that the group operation on the domain and codomain is just usual addition of real 2-vectors and real numbers, respectively. Then

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

so that π is a homomorphism. The kernel of π are the plane points (x, y) which map under π to the additive identity element of $\mathbb{R}$, 0. This is clearly the y-axis:

$$\text{Kernel}(\pi) = \{(0, y) \mid y \in \mathbb{R}\}$$

■

Exercise 1.6.16. Let A and B be groups and let G be their direct product, $A \times B$. Prove that the maps $\pi_1 : G \to A$ and $\pi_2 : G \to B$ defined by $\pi_1((a, b)) = a$ and $\pi_2((a, b)) = b$ are homomorphisms and find their kernels (cf. Exercise 14).

Proof. This statement is something of a generalization of the previous Exercise 1.6.15, but now the addition group operations are replaced by the more general direct product operations. It is proved similarly. Let $(a,b),(c,d) \in G$. Then

$$\begin{aligned}\pi_1((a,b)\cdot(c,d)) &= \pi_1((ac,bd)) \\ &= ac \\ &= \pi_1((a,b))\,\pi_1((c,d))\end{aligned}$$

and so π_1 is a homomorphism. Nearly the same exact process shows that π_2 is also a homomorphism. The kernels of these are easy:

$$\text{Kernel}(\pi_1) = \{(0,b) \mid b \in B\}$$

and

$$\text{Kernel}(\pi_2) = \{(a,0) \mid a \in A\}$$

■

Exercise 1.6.17. Let G be any group. Prove that the map from G to itself defined by $g \mapsto g^{-1}$ is a homomorphism if and only if G is abelian.

Proof. Assume first that G is abelian and let $a, b \in G$. Then

$$\begin{aligned}(ab)^{-1} &= b^{-1}a^{-1} \\ &\quad a^{-1}b^{-1}\end{aligned}$$

and so the inversion operation is a homomorphism.

Conversely, assume that the inversion operation is a homomorphism, and let $a, b \in G$. Then

$$\begin{aligned}ab &= 1 \cdot ab \\ &= (ba)(ba)^1 ab \\ &= (ba)\,b^{-1}a^{-1}ab \\ &= (ba)(ab)^{-1}(ab) \\ &= ba\end{aligned}$$

and so G is abelian.

■

Exercise 1.6.18. 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. First assume that the map $g \mapsto g^2$ is a homomorphism. Then for $g, h \in G$

we have

$$\begin{aligned} gh &= 1 \cdot gh \cdot 1 \\ &= g^{-1}gghhh^{-1} \\ &= g^{-1}g^2h^2h^{-1} \\ &= g^{-1}\left(gh\right)^2 h^{-1} \\ &= g^{-1}\left(gh\right)\left(gh\right)h^{-1} \\ &= \left(g^{-1}g\right)hg\left(hh^{-1}\right) \\ &= hg \end{aligned}$$

and so G is abelian.

Conversely, assume G is abelian. Then

$$\begin{aligned} \left(gh\right)^2 &= ghgh \\ &= gghh \\ &= g^2h^2 \end{aligned}$$

and so the squaring operation is a homomorphism.

■

Exercise 1.6.19. Let $G = \{z \in \mathbb{C} \mid z^n = 1 \text{ for some } n \in \mathbb{Z}^+\}$. Prove that for any fixed integer $k > 1$ the map from G to itself defined by $z \mapsto z^k$ is a surjective homomorphism but is not an isomorphism.

Proof. Let $k > 1$ be a fixed integer and define $\phi_k : G \to G$ as $\phi_k\left(z\right) = z^k$ for any $z \in G$. Then letting $z_1, z_2 \in G$, we have

$$\begin{aligned} \phi_k\left(z_1 \cdot z_2\right) &= \left(z_1 \cdot z_2\right)^k \\ &= \left(z_1\right)^k \cdot \left(z_2\right)^k \\ &= \phi_k\left(z_1\right) \cdot \phi_k\left(z_2\right) \end{aligned}$$

by virtue of the multiplicative properties of complex numbers. Thus the homomorphism property is satisfied.

We should verify that G is closed under this operation, i.e., that ϕ_k is well defined. If $z \in G$, then there is some $n \in \mathbb{Z}^+$ such that $z^n = 1$. Then

$$\phi_k\left(z\right)^n = \left(z^k\right)^n = \left(z^n\right)^k = 1^n = 1$$

and so $\phi_k\left(z\right) \in G$. Thus, the ϕ_k is well defined as a map on G.

Lastly, we want to show that ϕ_k is surjective. Let $z \in G$, i.e., $z^n = 1$ for some $n \in \mathbb{Z}^+$. Then notice that

$$\phi_k\left(z^{\frac{1}{k}}\right) = \left(z^{\frac{1}{k}}\right)^k = z$$

and also we have $\left(z^{\frac{1}{k}}\right)^{nk} = z^n = 1$ and so $z^{\frac{1}{k}} \in G$. Thus ϕ_k is surjective. Note that the existence of complex roots allows us to be sure that $z^{\frac{1}{k}}$ exists.

This is not an injective function in general, however. For instance if $k = 4$ we have $\phi_4(i) = \phi_4(1) = 1$ but $i \neq 1$, certainly.

■

Exercise 1.6.20. 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 the *automorphisms* of G).

Proof. Let $\mathrm{Aut}(G) = \{\phi : G \to G \mid \phi \text{ is an isomorphism}\}$. We must simply show that the group axioms hold. First, we make sure that the group operation is well defined. Let $\phi, \theta \in \mathrm{Aut}(G)$. Then the composition $\phi \circ \theta$ is a bijection, surely, but we want to show that the homomorphism property holds. Let $g, h \in G$. Then

$$\begin{aligned}\phi \circ \theta(gh) &= \phi(\theta(gh)) \\ &= \phi(\theta(g)\,\theta(h)) \\ &= \phi(\theta(g)) \circ \phi(\theta(h))\end{aligned}$$

and so the composition is an automorphism, that is, $\mathrm{Aut}(G)$ is closed under composition, so this operation is well defined.

The identity element is the identity map on G, 1_G, obviously. For any $\phi \in \mathrm{Aut}(G)$, the inverse ϕ^{-1} is also an automorphism on G and so $\phi^{-1} \in \mathrm{Aut}(G)$. Thus, $\mathrm{Aut}(G)$ has inverses of any element.

Lastly, let $\phi, \theta, \eta \in \mathrm{Aut}(G)$ and $g \in G$. Then

$$\begin{aligned}(\phi \circ \theta) \circ \eta(g) &= (\phi \circ \theta)(\eta(g)) \\ &= \phi(\theta(\eta(g))) \\ &= \phi(\theta \circ \eta(g)) \\ &= \phi \circ (\theta \circ \eta)(g)\end{aligned}$$

and so $(\phi \circ \theta) \circ \eta = \phi \circ (\theta \circ \eta)$, i.e., $\mathrm{Aut}(G)$ is associative under function composition (this is trivially true by the usual associativity of function composition; I just decided to show it here).

Finally, $\mathrm{Aut}(G)$ satisfies all of the group axioms and so is a group under function composition.

■

Exercise 1.6.21. 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 $\mathbb{Q}$ (cf. Exercise 20).

Proof. Let $k \in \mathbb{Q} - \{0\}$ and define the map $\phi_k(q) = kq$ for all $q \in \mathbb{Q}$. This clearly is a map on $\mathbb{Q}$, and we must show that it is an isomorphism, i.e., is a bijection and a homomorphism.

Let $p, q \in \mathbb{Q}$ such that $\phi_k(p) = \phi_k(q)$. This means that $kp = kq$ and so $p = q$ since k, nonzero, has an inverse in $\mathbb{Q}$. Thus, ϕ_k is injective. Similarly, let $q \in \mathbb{Q}$. Then since $k \neq 0$, $k^{-1} \in \mathbb{Q}$ and we have $\phi_k(k^{-1}q) = q$, thus ϕ_k is surjective. Hence ϕ_k is a bijection.

Next, let $p, q \in \mathbb{Q}$. Then

$$\begin{aligned}\phi_k(p+q) &= k \cdot (p+q) \\ &= kp + kq \\ &= \phi_k(p) + \phi_k(q)\end{aligned}$$

since rational multiplication distributes over rational addition. Thus ϕ_k is a homomorphism, and we can conclude that it is an isomorphism and, in particular, an automorphism of $\mathbb{Q}$.

■

Exercise 1.6.22. 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. Define the map $\phi : A \to A$ on abelian group A as $\phi(a) = a^k$ for fixed $k \in \mathbb{Z}$. Then if $a, b \in A$ we have

$$\phi(ab) = (ab)^k = a^k b^k = \phi(a)\,\phi(b)$$

where we used the fact that exponents distribute over a product of group elements in an abelian group. Thus, this is a homomorphism on A.

Next consider the case $k = -1$: $\phi(a) = a^{-k}$ is the inversion operation. It is clearly injective since we know group inverses are unique, and it is surjective because every group element has an inverse (more correctly, every group element is the inverse of some other element). Thus this ϕ is a bijection, and so it is an isomorphism.

■

Exercise 1.6.23. Let G be a finite group which possesses an automorphism σ (cf. Exercise 20) 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). [Show that every element of G can be written in the form $x^{-1}\sigma(x)$ and apply σ to such an expression.]

Proof. Let the hypotheses hold and let $g, h \in G$. Then

■

Exercise 1.6.24. 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 $n = |xy|$. [See Exercise 6 in Section 2.]

Proof. We must construct a bijective homomorphism between G and D_{2n}. ■

Exercise 1.6.25. Let $n \in \mathbb{Z}^+$. Let r and s be the usual generators of D_{2n}, and let $\theta = 2\pi/n$.

- 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 ϕ radians.
- Prove that the map $\phi : D_{2n} \to GL_2(\mathbb{R})$ defined on generators by

$$\phi(r) = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \qquad \text{and} \qquad \phi(s) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

  extends to a homomorphism of D_{2n} into $GL_2(\mathbb{R})$.
- Prove that the homomorphism ϕ in part (b) is injective.

Proof. **Note:** this problem is confusing but also seems very important to understand. Refer to pages 38–39 in the text to see the general topic discussed.

- Let $v = (x, y)^T \in \mathbb{R}^2$ and define $A_\theta = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$. Then $|v| = \sqrt{x^2 + y^2}$ and the product $A_\theta v$ is

$$A_\theta v = \begin{pmatrix} x\cos\theta - y\sin\theta \\ x\sin\theta + y\cos\theta \end{pmatrix}$$

  with magnitude $|A_\theta v| = |v|$ (this is straightforward to show. Thus, any vector $v \in \mathbb{R}^2$ is mapped to some point at the same distance from the origin. The cosine of the angle between the vectors v and $A_\theta v$ is defined as

$$\frac{\langle v, A_\theta v\rangle}{|v|\,|A_\theta|} = \frac{x^2\cos\theta - xy\sin\theta + xy\sin\theta + y^2\cos\theta}{|v|^2} = \frac{x^2+y^2}{|v|^2}\cos\theta = \cos\theta$$

  and so the angle between v and $A_\theta v$ is θ. Hence, A_θ rotates vectors an angle of θ about the origin. To see what direction we rotate, consider the point $(1, 0)$ rotating through angle θ. Then $A_\theta(1, 0)^T = \begin{pmatrix} \cos\theta \\ \sin\theta \end{pmatrix}$ which is clearly in the first quadrant (if n large enough), thus the rotation is counterclockwise.
- Consider the map defined on the generators of D_{2n} as specified in the problem statement. To show that this extends to a homomorphism of D_{2n} into $GL_2(\mathbb{R})$, we can simply show that the images of the generators of D_{2n} satisfy the same relations as the generators of D_{2n}.

Clearly, $\phi(s)^2 = 1_{GL_2(\mathbb{R})}$, and $\phi(r)^n = 1_{GL_2(\mathbb{R})}$. Also,

$$\phi(r)\phi(s) = \begin{pmatrix} -\sin\theta & \cos\theta \\ \cos\theta & \sin\theta \end{pmatrix}$$

and $\phi(r)^{-1} = \begin{pmatrix} \cos(-\theta) & -\sin(-\theta) \\ \sin(-\theta) & \cos(-\theta) \end{pmatrix} = \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix}$, thus

$$\phi(s)\phi(r)^{-1} = \begin{pmatrix} -\sin\theta & \cos\theta \\ \cos\theta & \sin\theta \end{pmatrix}$$

and so we observe that $\phi(r)\phi(s) = \phi(s)\phi(r)^{-1}$, the analogue to the generator relations in D_{2n}. Since the same relations are satisfied, we know that ϕ extends to a homomorphism of D_{2n} into $GL_2(\mathbb{R})$.

My interpretation of this is that since $\phi(r)$ and $\phi(s)$ are elements of $GL_2(\mathbb{R})$ which satisfy the same relations as s, r do in D_{2n}, the "span" of $\{\phi(s), \phi(r)\}$ is a subgroup of $GL_2(\mathbb{R})$ which is identical to D_{2n} in the sense that the subset of $GL_2(\mathbb{R})$ generated by $\{\phi(r), \phi(s)\}$ is isomorphic to D_{2n}. That is, ϕ on G is isomorphic onto its image, its image being a subset of $GL_2(\mathbb{R})$. If $GL_2(\mathbb{R})$ was generated by $\{\phi(r), \phi(s)\}$, then ϕ would be an isomorphism between D_{2n} and $GL_2(\mathbb{R})$; as it stands, this is not the case, and we merely have sort of "embedded" D_{2n} into $GL_2(\mathbb{R})$ as a subgroup. This allows us to concretely represent our group elements r and s as matrices in $GL_2(\mathbb{R})$, as is familiar. In fact, it seems that an "embedding" in the mathematical sense requires the mapping to be injective, which is the third part of this problem! **Note:** it seems instructive to think of this as similar to the special case from linear algebra of linear maps between vector spaces, where we consider basis elements.

- Let ϕ be the homomorphism defined in the previous part. Then consider the subgroup $\langle \phi(r), \phi(s) \rangle < GL_2(\mathbb{R})$ generated by $\{\phi(r), \phi(s)\}$. ϕ is certainly surjective onto this set. Also, thanks to the properties of homomorphisms (and thus alternatively thanks to the generator relations which $\phi(r)$ and $\phi(s)$ satisfy), we know that the order of this set is the same as the order of the set D_{2n}: $|D_{2n}| = 2n = |\langle \phi(r), \phi(s) \rangle|$, and so ϕ is necessarily injective.

■

Exercise 1.6.26. Let i and j be the generators of Q_8 described in Section 5. Prove that the map ϕ from Q_8 to $GL_2(\mathbb{R})$ defined on generators by

$$\phi(i) = \begin{pmatrix} \sqrt{-1} & 0 \\ 0 & \sqrt{-1} \end{pmatrix} \qquad \text{and} \qquad \phi(j) = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

extends to a homomorphism. Prove that ϕ is injective.

Proof. **Note:** this problem is very similar to the previous one, but it is not specified how the map ϕ should act on the generator k of Q_8. Part of this extension will involve the appropriate definition of this mapping.

Let the map $\phi : Q_8 \to GL_2(\mathbb{C})$ be as written in the problem statement. As in the previous Exercise 1.6.25, we want to show that the image of the generators of Q_8 under ϕ satisfy the same generator relations in $GL_2(\mathbb{C})$, thus showing that ϕ extends to a homomorphism of Q_8 into $GL_2(\mathbb{C})$.

A common presentation for Q_8 (see Exercise 1.5.3) is

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

where -1 commutes with i, j, k. We want to show that the given $\phi(i)$ and $\phi(j)$ satisfy the same relations in $GL_2(\mathbb{C})$. Note that

$$\phi(i)^2 = \begin{pmatrix} \sqrt{-1} & 0 \\ 0 & \sqrt{-1} \end{pmatrix}^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = -I \in GL_2(\mathbb{C})$$

and similarly

$$\phi(j)^2 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = -I$$

As the (negative of the) identity element in $GL_2(\mathbb{C})$, $-I$ commutes with all other elements.

What about the third generator, k? Since $ij = k$ in Q_8, consider

$$\phi(i)\phi(j) = \begin{pmatrix} \sqrt{-1} & 0 \\ 0 & \sqrt{-1} \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & -\sqrt{-1} \\ \sqrt{-1} & 0 \end{pmatrix}$$

so let us define

$$\phi(k) = \begin{pmatrix} 0 & -\sqrt{-1} \\ \sqrt{-1} & 0 \end{pmatrix}$$

Last, notice that

$$\phi(k)^2 = \begin{pmatrix} 0 & -\sqrt{-1} \\ \sqrt{-1} & 0 \end{pmatrix}^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = -I$$

From this, we also have

$$\phi(i)\phi(j)\phi(k) = \phi(k)\phi(k) = -I$$

and so all of the generator relations are satisfied. Hence, ϕ extends to a homomorphism.

As in the previous problem, restricting the codomain of ϕ to the image of Q_8 under ϕ makes ϕ surjective, and we can show that the order of the group generated by $\{-I, \phi(i), \phi(j), \phi(k)\} \subset GL_2(\mathbb{R})$ is exactly that of Q_8, namely 8, and so ϕ is injective.

■

Sec. 1.7 Group Actions

Exercise 1.7.1. 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 (state clearly which axioms in the definition of a filed are used).

Proof. We must show that the map $\cdot : F^\times \times F \to F$ is a group action by showing that the two group action axioms hold. First, let $g_1, g_2 \in F^\times = F \setminus \{0\}$ and $a \in F$. Then

$$\begin{aligned} g_1 \cdot (g_2 \cdot a) &= g_1 \cdot (g_2 a) \\ &= g_1 (g_2 a) \\ &= (g_1 g_2) a \\ &= g_1 g_2 \cdot a \end{aligned} \tag{3}$$

where the second-to-last equality holds by the associativity of the multiplication operation on F. Thus, the first group action axiom holds.

Next, let 1 be the identity element of $F^\times$, $a \in F$ arbitrary. Then

$$1 \cdot a = 1a = a \tag{4}$$

where the second equality holds since 1 is the (multiplicative) identity element of the field F and $a \in F$. Hence, the second group action axiom holds, and so this is a group action of $F^\times$ on F.

■

Exercise 1.7.2. Show that the additive group $\mathbb{Z}$ acts on itself by $z \cdot a = z + a$ for all $z, a \in \mathbb{Z}$.

Proof. The group action of $G = \mathbb{Z}$ on $A = \mathbb{Z}$ is defined by $z \cdot a = z + a$ for all $z, a \in \mathbb{Z}$. This is certainly a map from $\mathbb{Z} \times \mathbb{Z}$ to $\mathbb{Z}$, and it will be a group action if the two group action axioms hold. Let $z_1, z_2, a \in \mathbb{Z}$, arbitrary. Then

$$\begin{aligned} z_1 \cdot (z_2 \cdot a) &= z_1 \cdot (z_2 + a) \\ &= z_1 + (z + 2 + a) \\ &= (z_1 + z_2) + a \\ &= (z_1 \cdot z_2) + a \\ &= (z_1 \cdot z_2) \cdot a \end{aligned}$$

and so the first axiom is satisfied. Next, let 0 be the identity element of $G = \mathbb{Z}$. Then

$$\begin{aligned} 0 \cdot a &= 0 + a \\ &= a \end{aligned}$$

and so the group identity fixes arbitrary $a \in A$. Hence, this is a group action. ■

Exercise 1.7.3. 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. We must show that the two axioms are satisfied. The map defined in the problem statement is certainly a map from $\mathbb{R} \times (\mathbb{R} \times \mathbb{R})$ to $\mathbb{R} \times \mathbb{R}$. It remains to consider the group action axioms. First, let $r_1, r_2 \in \mathbb{R}$ and let $(x, y) \in \mathbb{R} \times \mathbb{R}$. Then

$$\begin{aligned} r_1 \cdot (r_2 \cdot (x, y)) &= r_1 \cdot (x + ry, y) \\ &= ((x + r_2 y) + r_1 y, y) \\ &= (x + (r_1 + r_2)\, y, y) \\ &= (r_1 + r_2) \cdot (x, y) \end{aligned}$$

Note that the $+$ in the sum $r_1 + r_2$ indicates the group operation of $\mathbb{R}$, since this is the only defined way in which to combine these group elements. In the definition of group action, this $+$ would simply be written $\cdot$, but this is a bit confusing here. We are using shorthand $r_1 + r_2 = r_1 \cdot r_2$.

Next, let 0 be the identity element of $\mathbb{R}$. Then

$$0 \cdot (x, y) = (x + 0 \cdot y, y) = (x, y)$$

and so this is truly a group action of $\mathbb{R}$ on $\mathbb{R} \times \mathbb{R}$. ■

Exercise 1.7.4. 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 (cf. Exercise 26 of Section 1):

- the kernel of the action,
- $\{g \in G \mid ga = a\}$ — this subgroup is called the *stabilizer* of a in G.

Proof. Note that the difference between the two parts of this problem are that the kernel of the group action is the set of group elements which fix *all* set elements, and the *stabilizers* only fix a single, particular group element. The proofs are identical but for the fact that the kernel proofs consider arbitrary set elements but the stabilizer proofs consider one specific set element.

- Let us write the kernel of the action of G on A as

$$\text{Ker}\,(G, A) = \{g \in G \,|\, ga = a \,\text{for all}\, a \in A\}$$

Recall that a set is a subgroup of a group if it is closed under the operation of that group and if it is closed under inversion (i.e., contains inverses), as per the definition in Exercise 1.1.26. Let $g_1, g_2 \in \text{Ker}\,(G, A)$ and let $a \in A$ arbitrary. Then

$$(g_2 g_1)\,(a) = g_2\,(g_1\,(a)) = g_2\,(a) = a$$

where the first equality holds from the first axiom of group action. Thus, $g_2 g_1$ maps arbitrary a to itself, and so $g_2 g_1 \in \text{Ker}\,(G, A)$; that is, this kernel is closed under the group operation.

Next, let $g \in \text{Ker}\,(G, A)$. Then $g^{-1} \in G$ since G is a group, and for arbitrary $a \in A$ we have

$$g^{-1}\,(a) = g^{-1}\,(ga) = \left(g^{-1} g\right)(a) = 1\,(a) = a$$

where we used both group action axioms. Hence, $g^{-1} \in \text{Ker}\,(G, A)$ and so this kernel is closed under inversion. Thus, we conclude that $\text{Ker}\,(G, A)$ is a subgroup of G.

- Next consider a fixed $a \in A$ and the stabilizer of a in G, written for convenience as

$$G_a = \{g \in G \,|\, ga = a\}$$

That is, this is the set of group elements which fix this particular a. Note that it is nonempty since the identity element of g is in the set (thanks to the second group action axiom). We use the same criteria to show that this is a subgroup. Let $g_1, g_2 \in G_a$. Then, with almost no perceivable modifications to the previous part of the problem,

$$(g_2 g_1)\,(a) = g_2\,(g_1\,(a)) = g_2\,(a) = a$$

and we have, for $g \in G_a$,

$$g^{-1}\,(a) = g^{-1}\,(ga) = \left(g^{-1} g\right)(a) = 1\,(a) = a$$

and so G_a is closed under the group operation and under inversion. Thus, the stabilizer of any a in G is a subgroup of G.

■

Exercise 1.7.5. 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 $G \to S_A$ (cf. Exercise 14 in Section 6).

Proof. Let g be in the kernel of the action of G on A. That is, for every $a \in A$ we have $g \cdot a = a$. The permutation representation of g is the $\varphi(g) = \sigma_g$ such that $\sigma_g(a) = g \cdot a$. But then $\sigma_g(a) = g \cdot a = a$ for every $a \in A$. Hence, $\varphi(g) = \sigma_g$ is the identity permutation, and so g is in the kernel of the permutation representation $G \to S_A$ (which is the kernel of the homomorphism $\varphi : G \to S_A$).

Conversely, let g be in the kernel of the permutation representation. That is, $\varphi(g) = 1_{S_A}$, the identity permutation. Then

$$a = \varphi(g)(a) = g \cdot a$$

so that $g \cdot a = a$ for all $a \in A$. Thus, g is in the kernel of the group action of G on A.

In total, then, the kernel of a group action is exactly the kernel of the permutation representation.

■

Exercise 1.7.6. 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. Recall that a group action is faithful if distinct group elements induce distinct permutations of the set. Let G be a group acting on set A.

First, assume that the kernel of the action is the set consisting only of the identity:

$$\{g \in G \mid ga = a,\ \forall a \in A\} = \{1\}$$

Then assume by way of contradiction that there exist $g_1, g_2 \in G$ with $g_1 \neq g_2$ such that g_1 and g_2 induce the same permutation of A. That is, for all $a \in A$ we have

$$g_1 a = \sigma_{g_1}(a) = \sigma_{g_2}(a) = g_2 a$$

Then we have that $g_2^{-1} g_1(a) = a$, and this holds for all $a \in A$ since a arbitrary. Thus, $g_2^{-1} g_1$ is in the kernel of the group action. Since this kernel consists only of the identity, we have that $g_2^{-1} g_1 = 1$, but by the group axioms we have $g_1 = g_2$. This contradicts our assumption that these are distinct. Hence, we conclude that distinct group elements induce distinct permutation representations, i.e., the group action is faithful.

Conversely, assume that G acts faithfully on A. Then let $g \neq 1$ be in the kernel of the group action. That is, for any $a \in A$, we have $g \cdot a = a$. Then we also have $1 \cdot a = a$ for any $a \in A$, and so g and 1 give rise to the same permutation on A. By the faithfulness of the group action, then, $g = 1$. Hence, the identity element is the only element of the kernel of the group action.

■

Exercise 1.7.7. Prove that in Example 2 in this section the action is faithful.

Proof. Example 2 is a vector space V over a field F; the group $F^\times$ acts on the set V through the usual vector space axioms (scalar multiplication). Example 2 considers the special case $V = \mathbb{R}^n$ and $F = \mathbb{R}$. Then the action is

$$\alpha\left(r_1, r_2, \ldots, r_n\right) = \left(\alpha r_1, \alpha r_2, \ldots, \alpha r_n\right)$$

for $\alpha \in \mathbb{R}$ and $(r_1, r_2, \ldots, r_n) \in \mathbb{R}^n$ where αr_i is just the usual multiplication of real numbers.

We want to show that this action is faithful. The multiplicative identity of this group is $1 \in \mathbb{R}$, and by the previous Exercise 1.7.6 we know that $\mathbb{R}$ acts faithfully on $\mathbb{R}^n$ if and only if the kernel of this action is $\{1\}$. It is easy to see that this is the case: for arbitrary $(r_1, r_2, \ldots, r_n) \in \mathbb{R}^n$, we have

$$\alpha\left(r_1, r_2, \ldots, r_n\right) = \left(\alpha r_1, \alpha r_2, \ldots, \alpha r_n\right) = \left(r_1, r_2, \ldots, r_n\right)$$

if and only if $\alpha r_i = r_i$ for all i. That is, $\alpha = 1$. Hence, $\mathbb{R}$ acts faithfully.

Alternatively, we might have tried to prove the definition of faithful group action directly.

■

Exercise 1.7.8. 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 $\sigma \cdot \{a_1, \ldots, a_k\} = \{\sigma\left(a_1\right), \ldots, \sigma\left(a_k\right)\}$.

- Prove that this is a group action.
- Describe explicitly how the elements (1 2) and (1 2 3) act on the six 2-element subsets of $\{1, 2, 3, 4\}$.

Proof. Let the hypothesis hold.

- We want to show that the above defines a group action of S_A on B. First, let $\sigma_1, \sigma_2 \in S_A$, and $\{a_1, \ldots, a_k\} \in B$. Then

$$\begin{aligned}
\sigma_2 \cdot \left(\sigma_1 \cdot \{a_1, \ldots, a_k\}\right) &= \sigma_2 \cdot \{\sigma_1\left(a_1\right), \ldots \sigma_1\left(a_k\right)\} \\
&= \{\sigma_2\left(\sigma_1\left(a_1\right)\right), \ldots, \sigma_2\left(\sigma_1\left(a\right)\right)\} \\
&= \{\sigma_2 \circ \sigma_1\left(a\right), \ldots, \sigma_2 \circ \sigma_1\left(a\right)\} \\
&= \left(\sigma_2 \circ \sigma_1\right)\{a_1, \ldots, a_k\}
\end{aligned}$$

  and so the first group action axiom holds. Next, let $1 \in S_A$ be the identity permutation. Then $1\left(a\right) = a$ for all $a \in A$. Thus,

$$\begin{aligned}
1 \cdot \{a_1, \ldots, a_k\} &= \{1\left(a_1\right), \ldots, 1\left(a_k\right)\} \\
&= \{a_1, \ldots, a_k\}
\end{aligned}$$

and so the second group action axiom holds. Hence, this is a group action of S_A on B.

- In this particular case, $A = \{1, 2, 3, 4\}$ and

$$\begin{aligned} B &= \{\text{2-element subsets of } A\} \\ &= \{\{1,2\},\ \{1,3\},\ \{1,4\},\ \{2,3\},\ \{2,4\},\ \{3,4\}\} \end{aligned}$$

Applying the permutations (1 2) and (1 2 3) to these subsets gives

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

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

■

Exercise 1.7.9. 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 (note that, for example, the 2-tuples $(1, 2)$ and $(2, 1)$ are different even though the sets $\{1, 2\}$ and $\{2, 1\}$ are the same, so the sets being acted upon are different).

Proof. We rephrase the statement of the group action:

> 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 k-tuples of elements of A by $\sigma \cdot (a_1, \ldots, a_k) = (\sigma(a_1), \ldots, (a_k))$.

- We want to prove that this is a group action of S_A on B. The process is identical to the above proof but the braces are replaced with parentheses and order of the tuples is maintained throughout (the order was maintained in the previous case, regardless). We will omit this proof.
- To demonstrate the action of the permutations (1 2) and (1 2 3) on the 2-element subsets, note that there are now 12 instead of 6 2-element subsets,

since the order of the subsets matters now. For example (note the difference between the tuples and the permutations!):

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

and these are not equal as tuples. I will omit the rest of the computations because they are not particularly instructive beyond this note: the set being acted upon is important.

■

Exercise 1.7.10. With reference to the preceding two exercises determine:

- for which values of k the action of S_n on k-element subsets is faithful, and
- for which values of k the action of S_n on ordered k-tuples is faithful.

Proof. • The group action of S_A on B of k-element subsets of A is faithful if distinct elements of S_A induce distinct permutations of B (in this case, where the group is itself the permutation group, the induced permutation of a group element is just the group element itself). Let $\sigma, \omega \in S_A$ be distinct permutations of B. Then...

■

Exercise 1.7.11. Write out the cycle decomposition of the eight permutations in S_4 corresponding to the elements of 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).

Proof. In Section 2, the vertices of the square are labelled starting at 1 on the upper-right vertex and proceeding clockwise around the square. Then a permutation representation of this group action of D_8 on the vertices $\{1,2,3,4\}$ is a homomorphism $\phi : D_8 \to S_4$. We have

g	$\phi(g)$
1	1
r	$(1\ 2\ 3\ 4)$
r^2	$(1\ 3)\,(2\ 4)$
r^3	$(1\ 4\ 3\ 2)$
s	$(2\ 4)$
sr	$(1\ 4)\,(2\ 3)$
sr^2	$(1\ 3)$
sr^3	$(1\ 2)\,(3\ 4)$

and this defines the permutation representation of the action of D_8 on the vertices of the square.

■

Exercise 1.7.12. 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).

Exercise 1.7.13. Find the kernel of the left regular action.

Proof. Let G be a group. The left regular action (on itself) is the group action of G on itself, $G \times G \to G$, defined by

$$g \mapsto ga \quad \text{for all } a \in A$$

The kernel of this action is the set of group elements which act like the identity, i.e., the elements which fix all elements upon which the group acts:

$$\{g \in G \mid ga = a \quad \text{for all } a \in A\}$$

In this case, where $A = G$, the kernel is all $g \in G$ such that $gh = h$ for all $h \in G$. This coincides exactly with the definition of the group's (left) identity element. Hence, we can also conclude that a group's left regular action (on itself) is faithful ($gh = fh$ for all $h \in G$, then $f^{-1}gh = h$ and so $f^{-1}g$ is in the kernel, but the kernel is the set containing only the identity, and so $f = g$).

■

Exercise 1.7.14. 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. If G is a non-abelian group, then there are elements $g, h \in G$ such that $gh \neq hg$. Then let $a \in A = G$. Then

$$(gh) \cdot a = agh$$

but

$$g \cdot (h \cdot a) = g \cdot (ah) = ahg$$

For the first group action axiom to be satisfied, we need these to be equal, i.e., $agh = ahg$. But then by the left cancellation law for groups, $gh = hg$, and this contradicts our non-abelian assumption. Hence, the first group axiom is not satisfied, and this can not define a group action.

■

Exercise 1.7.15. 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 be a group and $A = G$. Define the operation $g \cdot a = ag^{-1}$ for all $g, a \in G$. Then this operation is certain a mapping of $G \times A$ into A, so it is well defined. Also, letting $g_1, g_2 \in G$ and $a \in A$, we have

$$\begin{aligned} g_1 g_2 \cdot (a) &= a \left(g_1 g_2\right)^{-1} \\ &= a g_2^{-1} g_1^{-1} \\ &= \left(g_1 \cdot a\right) g_1^{-1} \\ &= g_1 \cdot (g_2 \cdot a) \end{aligned}$$

and so the first axiom of group action is satisfied. Next, let $1 \in G$ be the group identity, with inverse $1^{-1} = 1$ (obvious). Then for any $a \in A$ we have

$$1 \cdot a = a1^{-1} = a1 = a$$

and so both group actions of (left) group action are satisfied, and so this operation defines a group action of G on itself.

■

Exercise 1.7.16. 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. Let $G = A$ be any group and define an operation of G on $A = G$ as $g \cdot a = gag^{-1}$ for all $g, a \in G$. This is clearly well defined as a map from $G \times A$ to A. Letting $g_1, g_2 \in G$ and $a \in A$, we have

$$\begin{aligned} g_1 g_2 \cdot a &= \left(g_1 g_2\right) a \left(g_1 g_2\right)^{-1} \\ &= g_1 g_2 a g_2^{-1} g_1^{-1} \\ &= g_1 \left(g_2 a g_2^{-1}\right) g_1^{-1} \\ &= g_1 \left(g_2 \cdot a\right) g_1^{-1} \\ &= g_1 \cdot (g_2 \cdot a) \end{aligned}$$

and so the first axiom of a group action is satisfied. Next, let $1 \in G$ be the group identity and $a \in A$ arbitrary. Then since $1^{-1} = 1$, we have

$$1 \cdot a = 1a1^{-1} = a1 = a$$

and so both group action axioms are satisfied: conjugation is a (left) group action of G on itself.

■

Exercise 1.7.17. 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 — cf. Exercise 20, Section 6). 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. Let $g \in G$, fixed, and define a map $\phi : G \to G$ as $\phi(x) = gxg^{-1}$; this is left conjugation by g. We show that this is an automorphism. First, let $x, y \in G$ such that $\phi(x) = \phi(y)$. Then we have

$$\begin{aligned} x &= \left(g^{-1}g\right) x \left(g^{-1}g\right) \\ &= g^{-1}\left(gxg^{-1}\right) g \\ &= g^{-1}\phi(x)\, g \\ &= g^{-1}\phi(y)\, g \\ &= g^{-1}\left(gyg^{-1}\right) g \\ &= \left(g^{-1}g\right) y \left(g^{-1}g\right) \\ &= y \end{aligned}$$

so ϕ is injective. Next, let $y \in G$. Then notice that $g^{-1}yg \in G$ by closure of the group operation of G, and that

$$\phi\left(g^{-1}yg\right) = g\left(g^{-1}yg\right)g^{-1} = y$$

so ϕ is surjective. Thus, ϕ is a bijection on G (so a permutation of G).

Lastly, let $x, y \in G$. Then

$$\begin{aligned} \phi(xy) &= gxyg^{-1} \\ &= gx\left(g^{-1}g\right)yg^{-1} \\ &= \left(gxg^{-1}\right)\left(gyg^{-1}\right) \\ &= \phi(x)\,\phi(y) \end{aligned}$$

and so ϕ is a homomorphism. Thus, ϕ is a bijective homomorphism from G to G, i.e., an automorphism on G.

Since we know that automorphisms (more particularly, isomorphisms[a]) preserve element orders, and so $|x| = |\phi(x)| = |gxg^{-1}|$ for all $x \in G$. If $A \subset G$, then we can restrict ϕ to A, $\phi|_A : G \to gAg^{-1}$, and this is still a bijection (and thus an isomorphism), and so the cardinalities of the domain and the codomain are equal. ■

[a] Homomorphisms do not do this, since the trivial homomorphism $\phi : G \to \{1\}$ sending all $g \in G$ to the identity group is a homomorphism but does not preserve element orders.

Exercise 1.7.18. Let H be a group acting on a set A. Prove that the relation $\sim$ on A defined by

$$a \sim b \qquad \text{if and only if} \qquad a = hb \quad \text{for some } h \in H$$

is an equivalence relation. (For each $x \in A$ the equivalence class 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.)

Note: the explanation in the problem statement above claims that the orbits partition the set, and we know that a partition is equivalent to the existence of an equivalence relation; we prove the existence of an equivalence relation in this problem, and so we also prove this statement.

Remember that the points in A are points of an arbitrary set, *not* group elements. This is an important distinction, since the orbits describe how set elements move under the influence of the group action, and the group action axioms describe how the group acts on the set (not the group axioms, but the *group action axioms*).

Proof. Let H be a group acting on set A and define the relation $\sim$ on A as $a \sim b$ if and only if $a = hb$ for some $h \in H$.

First, note that $a = 1_H a$, where $1_H \in H$ is the group identity element, by the second group action axiom. Thus, $a \sim a$, and so $\sim$ is reflexive. Then let $a, b, c \in A$ such that $a \sim b$ and $b \sim c$. Then there are some $g, h \in H$ such that $a = hb$ and $b = gc$. But then we have

$$a = hb = h\left(gc\right) = \left(hg\right)c$$

by the first group action axiom. Thus, since $hg \in H$ by group closure, $a \sim c$ and so $\sim$ is transitive. Lastly, assume $a \sim b$, i.e., there is some $h \in H$ with $a = hb$. But then $h^{-1} \in H$ by group closure under inversion, and so $b = 1b = h^{-1}hb = h^{-1}\left(hb\right) = h^{-1}a$ (where we used *both* of the group action axioms) and so $b \sim a$, and thus $\sim$ is symmetric. Thus, $\sim$ is an equivalence relation on the set A, defined with help from the group H acting on the set.

■

Exercise 1.7.19. Let H be a subgroup (cf. Exercise 26 of Section 1) 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

$$H \to \mathcal{O} \qquad \text{defined by} \qquad h \mapsto hx$$

is a bijection (hence all orbits have cardinality $|H|$). From this and the preceeding exercise deduce *Lagrange's Theorem*:

if G is a finite group and H is a subgroup of G then $|H|$ divides $|G|$

Proof. The map of interest, right multiplication of $h \in H$ by fixed $x \in G$, can be written as $\phi : H \to \mathcal{O}$, where $\phi\left(h\right) = hx$. Then if $y \in \mathcal{O}$, by definition of orbit $\mathcal{O}$ of x under the action of H, there is some element $h' \in H$ such that $h'x = y$. That is,

$$y = h'x = \phi\left(h'\right)$$

and so ϕ is surjective. Next, let $h, h' \in H$ such that $\phi\left(h\right) = \phi\left(h'\right)$. Then $hx = h'x$

and by right cancellation of x (being a group element of G), we have $h = h'$; ϕ is injective. Hence, ϕ is a bijection from H to this particular orbit $\mathcal{O}$ of x. By properties of bijections on finite sets, we know that $|H\| = |\mathcal{O}|$.

We know that the orbits $\mathcal{O}$ for arbitrary $x \in G$ partition G — i.e., they are disjoint — and each orbit has cardinality $|H|$. Thus the total cardinality of G is some multiple of $|H|$; in particular, it is $|G| = n\,|H|$ where n is the number of distinct orbits in G under the action of H. Hence, $|H|$ divides $|G|$.

■

Exercise 1.7.20. Show that the group of rigid motions of a tetrahedron is isomorphic to a subgroup (cf. Exercise 26 of Section 1) of S_4.

Proof. A tetrahedron has four vertices, $A = \{1, 2, 3, 4\}$. Let G denote the group of rigid motions of the tetrahedron. We know that each rigid motion induces a permutation on A (but not every permutation of A is valid as a rigid motion). Given rigid motion $g \in G$, there is an associated permutation representation $\sigma_g : A \to A$, bijective, such that $\sigma_g(i) = \sigma_g i$ is the usual permutation operation[a]. That is, $\sigma_g \in S_4$. This permutation representation of the action is $\phi : G \to S_A$ (assigns to every group element a permutation, such that this mapping $\phi(g) = \sigma_g$ is a homomorphism). This ϕ is certainly injective, since $\phi(h) = \phi(g)$ means $\sigma_g = \sigma_h$ and identical permutations correspond to identical group elements. So, $\phi : G \to S_4$ is an injective homomorphism; we can restrict the codomain to get an isomorphism (an injective *and surjective* homomorphism) $\phi : G \to \phi(G) \subset S_4$.

■

[a]This terminology and development follows that of pages 42–43.

Exercise 1.7.21. Show that the group of rigid motions of a cube is isomorphic to S_4. [This group acts on the set of four pairs of opposite vertices.]

Contrary to the previous problem, this group is actually isomorphic to the permutation group.

Proof. In light of the hint in the problem statement, let G be the group of rigid motions of a cube. Since this group acts on pairs of opposite vertices and these pairs are preserved, we can consider G acting on four points (instead of 8), and let $A = \{1, 2, 3, 4\}$. G acts on A by sending each pair of opposing vertices (represented as singular elements of A) to another pair of opposing vertices, i.e., G has an action on A and permutes A. We can construct the permutation representation of G, $\phi : G \to A$, by letting

$$\phi(g) : A \to A \quad \text{as} \quad \phi(g)(i) = \sigma_g i \quad \text{for } i \in A$$

where σ_g is a permutation.

The permutation representation ϕ is injective since if $\phi(g) = \phi(h)$, this means that $\sigma_g = \sigma_h$ and identical permutations are given rise to by identical group

elements: $g = h$. We know that the orders of G and S_4 are both 24, and so we have an injective homomorphism between sets of finite, equal cardinality, and so ϕ is surjective; hence, ϕ is an isomorphism.

■

Exercise 1.7.22. Show that the group of rigid motions of an octahedron is isomorphic to a subgroup (cf. Exercise 26 of Section 1) of S_4. [This group acts on the set of four pairs of opposite faces.] Deduce that the groups of rigid motions of a cube and an octahedron are isomorphic. (These groups are isomorphic because these solids are "dual" — see *Introduction to Geometry* by H. Coxeter, Wiley, 1961. We shall see later that the groups of rigid motions of the dodecahedron and icosahedron are isomorphic as well — these solids are also dual.)

Proof. Instead of labelling the vertices as in the previous two examples, we can label the pairs of opposing faces as $A = \{1, 2, 3, 4\}$. Then the same construction as in Exercise 1.7.21 applies, and we have the same conclusions: there is an isomorphism from the group of rigid motions of an octahedron to S_4. Since isomorphism is an equivalence relation (we never showed this), we can conclude that the group of rigid motions of an octahedron is isomorphic to the group of rigid motions of a cube.

■

Exercise 1.7.23. 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.

Proof. If we label opposite faces of the cube, we have three distinct labels: $A = \{1, 2, 3\}$ and our motions will be homomorphic to some subset of S_3. Recall that $|S_3| = 3! = 6$. We know that the group G of rigid motions of a cube has order $|G| = 24$. The action of G on A is faithful if distinct elements of G induce distinct permutations of A; that is, given $g, h \in G$, $g \neq h$ the permutations σ_g, σ_h are distinct: $\sigma_g \neq \sigma_h$. In other words, the assignment $\phi : G \to S_A$ (permutation representation) is injective. However, the domain of this injective map has larger cardinality than the codomain, and this does not work. Thus, ϕ cannot be injective, i.e., the action is not faithful.

The kernel of this action is the set of group elements which fixes all elements of A. To imagine this, consider one pair of opposite faces. If we rotate one of these faces 180° about its center, then the positions of all three pairs of opposite faces are fixed. For each pair of opposite faces, there is one (non-identity) rotation of 180°, and so these rotations and the identity element comprise the kernel of this group action.

■

Chapter 2 Subgroups

2.1 Definition and Examples

Let G be a group.

Exercise 1.2.1. In each of (a)—(e) prove that the specified subset is a subgroup of the given group:

- the set of complex numbers of the form $a + ai$, $a \in \mathbb{R}$ (under addition)
- the set of complex numbers of absolute value 1, i.e., the unit circle in the complex plane (under multiplication)
- for fixed $n \in \mathbb{Z}^+$ the set of rational numbers whose denominators divide n (under addition)
- for fixed $n \in \mathbb{Z}^+$ the set of rational numbers whose denominators are relatively prime to n (under addition)
- the set of nonzero real numbers whose square is a rational number (under multiplication).

Note: we can prove that these are subgroups directly (nonempty, closed under products and inverses), or we can use the subgroup criterion and show that they are subgroups since they are nonemepty and contain xy^{-1} for every x, y in the set.

Proof.

- Let $x = a + ia, y = b + iby$ be arbitrary elements of the set. Then $0 + i0$ is obviously the identity element of the set, and so it is nonempty, and note that $y^{-1} = -b - ib$, so that

$$xy^{-1} = a + ia + (-b - ib) = (a - b) + i\,(a - b)$$

which is certainly an element of the set. Thus, by the subgroup criterion we have this as a subgroup of the complex numbers under usual complex addition.

- Let $H = \{z \in \mathbb{C} \mid |z| = 1\}$. This set is obviously nonempty since $1 + i0 \in H$. Then let $x, y \in H$. We know from studying complex numbers that $|y|^2 = y^* y = 1$, and so $y^{-1} = y^*$ (the complex conjugate of y). We also have that $|y^{-1}|^2 = |y^*|^2 = (y^*)^*\, y^* = yy^* = 1$ so that $y^{-1} \in H$ for all $y \in H$. Let $x = a+ib$, $y = c+id \in H$ so that $|x| = \sqrt{a^2 + b^2} = 1$ and $|y| = \sqrt{a^2 + b^2} = 1$. Then

$$xy^{-1} = (a + ib)\,(c - id) = (ac + bd) + i\,(-ad + bc)$$

and

$$\left|xy^{-1}\right|^2 = (ac + bd)^2 + (bc - ad)^2 = \ldots = \left(a^2 + b^2\right)\left(c^2 + d^2\right) = 1 \cdot 1 = 1$$

so that $xy^{-1} \in H$. By the subgroup criterion, H is a subgroup of $\mathbb{C}$ under usual complex addition.

- Fix $n \in \mathbb{Z}^+$ and let $H = \left\{ \frac{p}{q} \in \mathbb{Q} \,|\, mq = n \text{ for some } m \in \mathbb{Z} \right\}$. This set is nonempty since $\frac{1}{n} \in H$. Then let $x = \frac{a}{b}, y = \frac{c}{d} \in H$. Thus b and d divide n. Then $y^{-1} = -\frac{c}{d}$, and

$$x + y^{-1} = \frac{a}{b} - \frac{c}{d} = \frac{ad - bc}{bd}$$

■

Exercise 2.1.2. In each of (a)—(c) prove that the specified subset is *not* a subgroup of the given group:

- the set of 2-cycles in S_n for $n \geq 3$
- the set of reflections in D_{2n} for $n \geq 3$
- for n a composite integer > 1 and G a group containing an element of order n, the set $\{x \in G \,|\, |x| = n\} \cup \{1\}$
- the set of (positive and negative) odd integers in $\mathbb{Z}$ together with 0
- the set of real numbers whose square is a rational number (under addition).

Proof.

- The identity permutation is not a 2-cycle, so the group could not be closed under multiplication with inverse elements. Hence, it is not even a group.
- The set is not closed. The composition of two distinct reflections results in a rotation, which is not in the set.
- This set is not closed, since if $|x| = n = pq$ for integers p, q (i.e., n composite), then

$$x^n = x^{pq} = (x^p)^q$$

Consider another y such that $|y| = n$. Then the product of x and y satisfies

$$(xy)^n$$

- This subset is not closed, since $1 + 1 = 2$ is not odd.
- Certainly not closed. Note that $\sqrt{2}$ and $\sqrt{3}$ are in this set but $\left(\sqrt{2} + \sqrt{3}\right)^2 = 2 + 3 + 2\sqrt{6} = 5 + 2\sqrt{6}$ is not rational.

■

Exercise 2.1.3. Show that the following subsets of the dihedral group D_8 are actually subgroups:

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

Proof. Since each H is a finite set, following the discussion on the top of page 48, we know that if H is automatically closed under inverses if it is closed under multiplication, and thus is a subgroup. Hence, we only need to check that each subset is closed under multiplication. Since these are small sets, we can check directly.

- Let's compute the multiplication table for H:

H	1	r^2	s	sr^2
1	1	r^2	s	sr^2
r^2	r^2	1	sr^2	s
s	s	sr^2	1	r^2
sr^2	sr^2	s	r^2	1

  Since every element in the table is an element of H, it is closed (in addition, we can see that each element has an inverse in H). Hence, H is a subgroup of D_{2n}.

- Let us proceed again for the next subset H:

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

  and so H is again a subgroup of D_{2n}.

■

Exercise 2.1.4. 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.

Proof. Let $G = \mathbb{Z}$ be the integers under usual addition and let $H = \mathbb{Z}^+ \subset G$. Then H is closed under integer addition, but does not contain inverses. Hence, it is not a subgroup. However, it is certainly an infinite subset.

■

Exercise 2.1.5. Prove that G cannot have a subgroup H with $|H| = n - 1$, where $n = |G| > 2$.

Proof. Assume that $n = |G| > 2$ and H is a subgroup of G with $|H| = n - 1$. Then there is some non-identity element of G, say g, such that $g \notin H$ (this is non-identity since the identity must be in H, as it is a subgroup). There is also some nonidentity element of H since $n = |G| > 2 \implies |H| = n - 1 > 1$; call this element h.

We can consider what happens to this product. Since $h \in H$, a subgroup, we have $h^{-1} \in H$. Then if $hg \in H$, we have $h^{-1}hg = g \in H$ by closure of H under multiplication; this is a contradiction. On the other hand, if $hg \notin H$, then $hg = g$ and by the cancellation law in G we have h the identity element, which is again a contradiction. Thus, we conclude that no such subgroup can exist.

■

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

Proof. Let g, h be in this subset. then $|g| = n$, $|h| = m$, both finite. Then $|h^{-1}| = m$, and we have

$$\left(gh^{-1}\right)^{mn} = g^{mn}h^{-mn} = (g^n)^m \left(\left(h^{-1}\right)^m\right)^n = 1 \cdot 1 = 1$$

where we used the fact that G was abelian to distribute the exponents over the product. Thus we have $|gh^{-1}| < mn < \infty$ and so gh^{-1} is in this subset for any g, h in the subset. Also, the set is clearly nonempty since 1 is contained in it. Hence, by the subgroup criterion, this is a subgroup of G.

■

Exercise 2.1.7. Fix some $n \in \mathbb{Z}$ with $n > 1$. Find the torsion subgroup (cf. the previous exercise) of $\mathbb{Z} \times (\mathbb{Z}/n\mathbb{Z})$. Show that the set of elements of infinite order together with identity is *not* a subgroup of this direct product.

Proof. Recall that the torsion subgroup of $\mathbb{Z}\times(\mathbb{Z}/n\mathbb{Z}) = \{(a, [b]) \mid a \in \mathbb{Z}, b \in \{0, 1, \ldots, n-1\}\}$ is the subset of elements of finite order. Assume $(a, [b])$ is in this torsion subgroup. Then this element has some finite order $k \in \mathbb{Z}^+$ so that

$$(a, [b])^k = (ka, [kb]) = (0, [0])$$

where the product kb is taken modulo n, and $(0, [0])$ is the identity element. Since the first component of this direct product is in $\mathbb{Z}$, this equality holds only if $ka = 0$ and so we must have $a = 0$. The second equation relates two residue classes, and so $[kb] = [0]$ if and only if $kb - 0 = pn$ for some $p \in \mathbb{Z}$. Intuitively, this equation must be satisfied for some p, eventually, since otherwise every product of $[b]$ would be distinct and $\mathbb{Z}/n\mathbb{Z}$ would be an infinite group, but we know that $\mathbb{Z}/n\mathbb{Z}$ is finite. Hence, this puts no restriction on the elements of the torsion subgroup. Thus, this

torsion subgroup is

$$\{(0,[b]) \mid b \in \{0,1,\ldots,n-1)\}$$

Note that the elements of infinite order include, in particular, the elements $(1,[0])$ and $(-1,[1])$. However, the product of these elements is

$$(1,[1]) \cdot (-1,[0]) = (1-1,[1]+[0]) = (0,[1])$$

which has finite order and is not the identity element. Thus, the elements of infinite order along with the identity element is not a subgroup of this direct product, since it is not closed.

■

Exercise 2.1.8. 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. Assume first that $H \subseteq K$. Then $H \cup K = K$, which is a subgroup of G by hypothesis. Similarly, if $K \subseteq H$, then $H \cup K = H$ which is also a subset of G.

Conversely, assume that $H \cup K$ is a subgroup of G. Assume that $H \not\subseteq K$; then there is some element $h \in H$ such that $h \notin K$. However, $h \in H \cup K$. So, for arbitrary $q \in K \subset H \cup K$, we have $hq \in H \cup K$ since this is a subgroup. We have two possibilities. If $hq \in H$, then since $h \in H$, $h^{-1} \in H$ and so $h^{-1}hq = q \in H$, so that arbitrary element $q \in K$ is in H, and $K \subseteq H$. On the other hand, if $hq \in K$, then since $q \in K$, $q^{-1} \in K$ and we have $hqq^{-1} = h \in K$, but this is a contradiction since we assumed $h \notin K$. Thus, we have shown that if $H \not\subseteq K$, then $K \subseteq H$.

Otherwise, if $H \subseteq K$, then we are done.

■

Exercise 2.1.9. 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. Certainly $SL_n(F) \subset GL_n(F)$, and it is nonempty since the identity matrix I_n has unit determinant. Since $\det(A) = 1 \neq 0$, there is a matrix inverse of A, A^{-1}, such that $\det(A^{-1}) = \det(A)^{-1} = 1$. Thus, $A^{-1} \in SL_n(F)$. Also, if A and B are in $SL_n(F)$, then the product has determinant $\det(AB) = \det(A) \cdot \det(B) = 1 \cdot 1 = 1$, so that the product is in $SL_n(F)$. Thus, $SL_n(F)$ is a subgroup of $GL_n(F)$ since it is a subset which is closed under inversion and the group operation (matrix multiplication).

■

Exercise 2.1.10.

- Prove that if H and K are subgroups of G then so is their intersection $H \cap K$.
- Prove that the intersection of an arbitrary nonempty collection of subgroups of G is again a subgroup of G (do not assume that collection is countable).

Proof.

- This intersection is nonempty since the subgroups H and K both contain the identity element of G. If $a, b \in H \cap K$, then $a, b \in H$ and $a, b \in K$. Then $ab^{-1} \in H$ since H is a subgroup and similarly $ab^{-1} \in K$. Thus, $ab^{-1} \in H \cap K$ and so $H \cap K$ is a subgroup of G since it satisfies the subgroup criterion.

- We cannot use induction since we cannot assume a countable intersection. Instead, let $H = \cap_{\alpha \in A} H_\alpha$ where A is some arbitrary indexing set and H_α is a subgroup of G for every $\alpha \in A$. Then the proof is a simple generalization of the above. H is nonempty since $1 \in H_\alpha$ for every $\alpha \in A$, so $1 \in H$. Thus, let $a, b \in H$. Then $ab^{-1} \in H_\alpha$ for every $\alpha \in A$ since each H_α is a subgroup. Hence, $ab^{-1} \in H$, and so by the subgroup criterion, H is a subgroup of G.

■

Exercise 1.2.11. Let A and B be groups. Prove that the following sets are subgroups of the direct product $A \times B$:

- $\{(a, 1) \mid a \in A\}$
- $\{(1, b) \mid b \in B\}$
- $\{(a, a) \mid a \in A\}$, where here we assume $B = A$ (called the *diagonal subgroup*).

Proof. First, note that the identity element of $A \times B$ is $(1, 1)$ where the 1 are understood as the identity elements of the groups A and B, respectively. Thus, these subgroups are not empty, since this element is easily in all of the sets.

- The inverse of $(a, 1)$ is $(a^{-1}, 1)$ which is certainly in the set. Hence, for two elements $(a, 1), (b, 1)$ in the set, we have

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

  which is certainly in the set since $ab^{-1} \in A$ as A is a group. Thus, this set is a subgroup of $A \times B$ by the subgroup criterion.

- An analogous proof proceeds as in the previous case. We will omit it here since it is very similar.

- The inverse of arbitrary element (a, a) in this set is (a^{-1}, a^{-1}), clearly also in the set. Then for (a, a) and (b, b) in the set, the product is

$$(a, a)(b, b) = (ab, ab)$$

  and $ab \in A$ since A is a group, and so this set is closed under multiplication. Hence, it is a subgroup (by definition of subgroup, *not* the subgroup criterion.

■

Exercise 2.1.12. Let A be an abelian group and fix some $n \in \mathbb{Z}$. Prove that the following sets are subgroups of A:

- $\{a^n \,|\, a \in A\}$
- $\{a \in A \,|\, a^n = 1\}$.

Proof. Let A be an abelian group, $n \in \mathbb{Z}$ fixed.

- Let $H = \{a^n \,|\, a \in A\}$. This is the set of the nth power of every element of A. It is nonempty since $1 \in H$. Note that for every $a \in A$, we have $a^{-1} \in A$ since A is a group. Then $a^n, a^{-n} \in H$ and these are inverses: $a^n a^{-n} = 1$. Since any $h \in H$ is $h = a^n$ for some $a \in A$, we have $h^{-1} = (a^{-1})^n \in H$. Then let $g, h \in H$. Then $g = a^n$ and $h = b^n$ for some $a, b \in A$. We have
$$gh^{-1} = a^n b^{-n} = \left(ab^{-1}\right)^n$$
by the abelian property of A. Then since $ab^{-1} \in A$, $gh^{-1} \in H$. Thus by the subgroup criterion we have H a subgroup of A.
- Let $H = \{a \in A \,|\, a^n = 1\}$. These are the nth roots of unity in A. The identity element of A, 1, is clearly in H since $1^n = 1$; thus H is nonempty. If $a \in H$, then $a^{-1} \in H$ since $(a^{-1})^n = (a^n)^{-1} = 1^{-1} = 1$. Then let $a, b \in H$. Then we have
$$\left(ab^{-1}\right) = a^n \left(b^{-1}\right)^n = 1 \cdot 1 = 1$$
Hence, H is a subgroup of A, by the subgroup criterion.

■

Exercise 1.2.13. 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. We can start with this condition and "build up" the entire set of rational numbers. Clearly $H = 0$ satisfies the property, so this case is trivial. Alternately, assume that $H \neq 0$. Then certainly $0 \in H$, and there is some non-identity element $x \in H$. Then since H is a group, the inverse $-x \in H$. Since x is rational, we can write it as $x = \frac{p}{q}$ for some integers p, q where $q \neq 0$. Then notice that the repeated sum $qx = q\frac{p}{q} = p \in H$ since H is a group and this is the group operation (addition). Then by the hypothesis, $1/p \in H$, and again repeated addition guarantees that $p\frac{1}{p} = 1 \in H$. Thus, we have $\mathbb{Z} \subseteq H$. Thus, for $k \in \mathbb{Z} \setminus \{0\} \subseteq H$, we have $\frac{1}{k} \in H$. Finally, for arbitrary $p, q \in \mathbb{Z} \subseteq H$ with $q \neq 0$, we have $p\frac{1}{q} = \frac{p}{q} \in H$ (this multiplication is just repeated rational addition). Thus, $H \subseteq \mathbb{Q}$.

Conversely, H is a subgroup of $\mathbb{Q}$ by hypothesis. We have shown double inclusion, and so $H = \mathbb{Q}$.

■

Exercise 1.2.14. Show that $\{x \in D_{2n} \mid x^2 = 1\}$ is not a subgroup of D_{2n} (here $n \geq 3$).

Proof. Let $H = \{x \in D_{2n} \mid x^2 = 1\}$. Since we are familiar with the structure of D_{2n}, without knowing the parity of n, we can only say that $s \in H$ since $s^2 = 1$. Hopefully we can show that closure is not satisfied. The element $sr \in D_{2n}$ has

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

so that $sr \in H$. But then $srs = s^2 r^{-1} = r^{-1}$ and $r^{-2} \neq 1$ since we know $n \geq 3$. Thus, H is not closed under multiplication, and so not a subgroup.

■

Exercise 1.2.15. Let $H_1 \leq H_2 \leq \cdots$ be an ascending chain of subgroups of G. Prove that $\cup_{i=1}^{\infty} H_i$ is a subgroup of G.

Proof. The union $\cup_{i=1}^{\infty} H_i$ is nonempty since $1 \in H_i$ for all i since each is a subgroup of G. Let $a, b \in \cup_{i=1}^{\infty} H_i$. Then $b \in H_i$ for some i. Since H_i is a subgroup, $b^{-1} \in H_i$ and so $b^{-1} \in \cup_{i=1}^{\infty} H_i$. Also, $a \in H_j$ for some j. Let $k = \max(i, j)$. Then $a, b^{-1} \in H_k$ thanks to the nested structure of the subgroups. Thus, $ab^{-1} \in H_k = \cup_{r=1}^{\infty} H_r$ so that this union is a subgroup by the subgroup criterion.

■

Exercise 1.2.16. 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. Denote this set as H and note that H is not empty since the identity matrix of $GL_n(F)$ is upper triangular.

Let $A, B \in H$ be upper triangular matrices. As usual, the ijth component of the product AB is computed as

$$(AB)_{ij} = \sum_{k=1}^{n} A_{ik} B_{kj}$$

Consider if $i > j$. Then we can expand this sum as

$$\begin{aligned} (AB)_{ij} &= \sum_{k=1}^{n} A_{ik} B_{kj} \\ &= \sum_{k=1}^{i-1} A_{ik} B_{kj} + \sum_{k=i}^{n} A_{ik} B_{kj} \end{aligned} \tag{5}$$

In the first term, we have $i > k$ and so $A_{ik} = 0$ for all $k = 1, \ldots, i-1$. In the second term, we have $k \geq i > j$, and so $B_{kj} = 0$. Thus, this sum is identically

zero for $i > j$. Hence, AB is upper triangular, and so H is closed under matrix multiplication.

Next, we must show that the inverse of an upper triangular matrix is also upper triangular. Let $A \in H$. Then $A \in GL_n(F)$ and so it has an inverse matrix $A^{-1} \in GL_n(F)$ so that $AA^{-1} = I$. That is, we have

$$\left(AA^{-1}\right)_{ij} = \sum_{k=1}^{n} A_{ik}A_{kj}^{-1} = \begin{cases} 1, & i = j \\ 0, & i \neq j \end{cases}$$

■

Exercise 1.2.17. 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. Let H be the subset in question. Certainly H is a subset of the subgroup of upper triangular matrices considered in the previous exercise, and so we know that the upper triangular structure of H is preserved by matrix multiplication and inversion. We need to show that the diagonals elements are all 1 for inverses and products.

Let $A \in H$. Then A^{-1} is upper triangular by the previous exercise. Then

$$1 = I_{ii} = \left(A^{-1}A\right)_{ii} = \sum_{k=1}^{n} A_{ik}^{-1}A_{ki}$$

Note that for the indices $k < i$, the components $A_{ik}^{-1} = 0$ since A^{-1} is upper triangular. SImilarly, $A_{ki} = 0$ for $k > i$. Hence, the only term of the sum which survives is the ii term:

$$A_{ii}^{-1}A_{ii} = 1$$

and so $A_{ii}^{-1} = 1/A_{ii} = 1$. That is, the diagonal terms of A^{-1} are all 1. Hence, $A^{-1} \in H$, so that H is closed under inversion.

Next, let $A, B \in H$. Then the product AB is upper diagonal by the previous exercise. The diagonal elements look like

$$(AB)_{ii} = \sum_{k=1}^{n} A_{ik}B_{ki} = A_{ii}B_{ii} = 1 \cdot 1 = 1$$

so that AB has all 1 on the diagonal. That is, $AB \in H$ and so H is closes under matrix multiplication. Finally, we can conclude that H is a subgroup of the group of upper triangular matrices, which is in turn a subgroup of $GL_n(F)$, hence $H \leq GL_n(F)$.

■

2.2 Centralizers and Normalizers, Stabilizers and Kernels

Exercise 2.2.1. Prove that $C_G(A) = \{g \in G \mid g^{-1}ag = a \text{ for all } a \in A\}$.

Proof. This is quite straightforward. Let $g \in C_G(A)$. Then $gag^{-1} = a$ for all $a \in A$. Then $g^{-1}ag = g^{-1}(gag^{-1})g = (g^{-1}g)a(g^{-1}g) = a$ for all $a \in A$. It is just as easy to proceed in the alternate direction.

■

Exercise 2.2.2. Prove that $C_G(Z(G)) = G$ and deduce that $N_G(Z(G)) = G$.

Proof. Recall that the center of G, $Z(G)$, is the subset of elements of G which commute with all elements of G. The centralizer of a subset A of G is $C_G(A)$, the set of elements of G which commute with all elements of A. It is quite obvious that $C_G(Z(G)) = G$.

To be complete, let $g \in C_G(Z(G))$. Then certainly $g \in G$ since this is a subset of G. Conversely, let $g \in G$. Then every element of $Z(G)$ commutes with g by definition of the center of a group. Then certainly $g \in C_G(Z(G))$ since g commutes with all elements of $Z(G)$. Thus, we have shown that $G = C_G(Z(G))$.

We know that the normalizer of $Z(G)$, $N_G(Z(G))$, is a supergroup of the centralizer $C_G(Z(G))$: $C_G(Z(G)) \leq N_G(Z(G))$. Hence, since $C_G(Z(G)) = G$, we have $G \subseteq N_G(Z(G))$. But we also know that $N_G(Z(G)) \subseteq G$, so that $N_G(Z(G)) = G$.

■

Exercise 2.2.3. 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. Let $A, B \subseteq G$ with $A \subseteq B$. Then if $g \in C_G(B)$, then g commutes with every element of B; since $A \subseteq B$, g commutes in particular with every element of A. Hence, $C_G(B) \subseteq C_G(A)$. Since both are subgroups, we have that $C_G(B) \leq C_G(A)$.

■

Exercise 2.2.4. 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 (Exercise 19 in Section 1.7) simplify your work?

Proof. Since the centralizers and centers are subgroups of these groups, and these are finite groups, we know from Lagrange's theorem that the orders of these subgroups divide the orders of the larger groups.

First, recall that S_3 is the group of permutations of $\{0, 1, 2\}$.

■

Exercise 2.2.5. In each of parts (a) to (c) show that for the specified group G and subgroup A of G, $C_G(A) = A$ and $N_G(A) = G$.

- $G = S_3$ and $A = \{1, (1\ 2\ 3), (1\ 3\ 2)\}$.

- $G = D_8$ and $A = \{1, s, r^2, sr^2\}$.
- $G = D_{10}$ and $A = \{1, r, r^2, r^3, r^4\}$.

Proof.

■

2.3 Cyclic Groups and Cyclic Subgroups

Exercise 2.3.1. Find all subgroups of $Z_{45} = \langle x \rangle$, giving a generator for each. Describe the containments between these subgroups.

Proof. Recall that Z_{45} is the cyclic subgroup of order 45, which is isomorphic to $\mathbb{Z}/45\mathbb{Z}$. The unique subgroups of Z_{45} are generated by x^r where $r \mid 45$. Otherwise, if r and 45 are relatively prime, then $\langle x^r \rangle = Z_{45}$. The interesting subgroups are thus

$$\begin{gathered}
\left\langle x^1 \right\rangle = \left\{1, x^1, x^2, x^2, \ldots, x^{43}, x^{44}\right\} \\
\left\langle x^3 \right\rangle = \left\{1, x^3, x^6, x^9, \ldots, x^{39}, x^{42}\right\} \\
\left\langle x^5 \right\rangle = \left\{1, x^5, x^{10}, x^{15}, \ldots, x^{35}, x^{40}\right\} \\
\left\langle x^9 \right\rangle = \left\{1, x^9, x^{18}, x^{27}, x^{36}\right\} \\
\left\langle x^{15} \right\rangle = \left\{1, x^{15}, x^{30}\right\} \\
\langle 1 \rangle = \{1\}
\end{gathered}$$

■

Exercise 2.3.2. 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 be an element of finite group G such that $|x| = |G|$. Certainly we have $\langle x \rangle \leq G$ since each product of x is an element of G by the group axioms of G. Write $n = |x| = |G| < \infty$ since G is a finite group. Next, let $g \in G$. But $\langle x \rangle = \{1, x^1, x^2, ldots, x^{n-1}\}$ consists of n distinct elements, and G does as well; further, G contains $\langle x \rangle$, so clearly we must have $g = x^r$ for some $0 \leq r < n$. Thus, $G \leq \langle x \rangle$. Hence, the two groups are equal.

Consider the additive group $\mathbb{Z}$. Then $\mathbb{Z}$ and the subgroup $\langle 2 \rangle$ are both of infinite order, but $\langle 2 \rangle < \mathbb{Z}$ since, for instance, $3 \in \mathbb{Z}$ but $3 \notin \langle 2 \rangle$.

■

Exercise 2.3.3. Find all generators for $\mathbb{Z}/48\mathbb{Z}$.

Proof. Recall that $\mathbb{Z}/48\mathbb{Z} \cong Z_{48}$. In Exercise 2.3.1, we found all proper subgroups of Z_{45} by finding the factors of 48. In contrast, we will here look for all integers k less than and relatively prime to 48, since x^k will then sweep over all elements in Z_{48}. We can decompose 48 into the prime factorization $48 = 2^4 \cdot 3$ so that any positive integers without these factors (or a product thereof) will work. This list is

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

and the generators are $\overline{x}$ for x in this list.

■

Exercise 2.3.4. Find all generators for $\mathbb{Z}/202\mathbb{Z}$.

Proof. As in the previous Exercise 2.3.3, we want to find all positive integers less than and relatively prime to 202. We can begin by finding the prime factorization of 202, which is $202 = 2 \cdot 101$. Thus, the positive integers which *don't* work are those with a factor of 2 (the even numbers), 101 itself, or 202. Hence, for $k < 202$ odd, excluding 101, we have $\overline{k}$ a generator of $\mathbb{Z}/202\mathbb{Z}$.

■

Exercise 2.3.5. Find the number of generators for $\mathbb{Z}/49000\mathbb{Z}$.

Proof. As in the previous two Exercises, generators of $\mathbb{Z}/49000\mathbb{Z}$ will be $\overline{x}$ for integers x less than and relatively prime to 49000. The number of such integers is given by the Euler φ-function, discussed in Section 0.2. Recall that this function has two useful properties: for p prime, $\alpha \geq 1$, and a, b relatively prime, we have

$$\varphi\left(p^\alpha\right) = p^\alpha - p^{\alpha-1}$$

and

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

We can use these to compute $\varphi(49000)$ by first noting that the prime factorization of 49000 is $49000 = 2^3 \cdot 5^3 \cdot 7^2$. Then

$$\begin{aligned} \varphi(49000) &= \varphi\left(2^3\right)\varphi\left(5^3\right)\varphi\left(7^2\right) \\ &= \left(2^3 - 2^2\right)\left(5^3 - 5^2\right)\left(7^2 - 7\right) \\ &= 4 \cdot 100 \cdot 42 \\ &= 16800 \end{aligned} \tag{6}$$

Hence there are 16800 generators for $\mathbb{Z}/49000\mathbb{Z}$.

■

Exercise 2.3.6. In $\mathbb{Z}/48\mathbb{Z}$ write out all elements of $\langle\overline{a}\rangle$ for every $\overline{a}$. Find all inclusions between subgroups in $\mathbb{Z}/48\mathbb{Z}$.

Proof.

■

Exercise 2.3.17. Find a presentation for Z_n with one generator.

Proof. Certainly x generates Z_n, and the "modulo" property of Z_n can be expressed as $x^n = 1$. For any power x^k of x, we can represent it as x^r for $0 \leq r < n$ by using the division algorithm: $x^k = x^{pn+r} = x^r$. Hence, a presentation of Z_n with one generator is $\langle x \,|\, x^n = 1 \rangle$.

■

Exercise 2.3.18. Show that if H is any group and h is an element of H with $h^n = 1$, then there is a unique homomorphism from $Z_n = \langle x \rangle$ to H such that $x \mapsto h$.

2.4 Subgroups Generated by Subsets of a Group

Exercise 2.4.1. Prove that if H is a subgroup of G then $\langle H \rangle = H$.

Proof. Certainly we have $H \subset \langle H \rangle$ and since H is a subgroup of G we have $H \leq \langle H \rangle$. Since $\langle H \rangle$ is the intersection of all subgroups of G containing H, H itself is such a subgroup and so $\langle H \rangle \leq H$. Thus, we have $\langle H \rangle = H$.

■

Exercise 2.4.2. Prove that if A is a subset of B then $\langle A \rangle \leq \langle B \rangle$. Give an example where $A \subseteq B$ with $A \neq B$ but $\langle A \rangle = \langle B \rangle$.

Proof. Let $A \subseteq B$. Then if $x \in \langle A \rangle$, then x is a product of elements of A. Since elements of A are also elements of B, x is a product of elements of B and so $x \in \langle B \rangle$. Hence, $\langle A \rangle \leq \langle B \rangle$.

A simple example is $A = \{2\}$ and $B = \{\ldots, -4, -2, 0, 2, 4, \ldots\}$. Then certainly $A \subset B$ but $\langle A \rangle = B = \langle B \rangle$.

■

Exercise 2.4.3. Prove that if H is an abelian subgroup of a group G then $\langle H, Z(G) \rangle$ is abelian. Give an explicit example of an abelian subgroup H of a group G such that $\langle H, C_G(H) \rangle$ is not abelian.

Proof. Let H be an abelian subgroup of G and consider $a, b \in \langle H, Z(G) \rangle$. Then we know that $a = a_1^{\epsilon_1} a_2^{\epsilon_2} \cdots a_n^{\epsilon_n}$ and $b = b_1^{\delta_1} b_2^{\delta_2} \cdots b_k^{\delta_m}$ where $a_i, b_j \in H \cup Z(G)$ for $i = 1, \ldots, n$ and $j = 1, \ldots, m$ and each $\epsilon_i, \delta_j \in \{-1, 1\}$. Then all of the a_i and b_j commute since the elements of H all commute with each other since H abelian

and the elements of $Z(G)$ commute with all elements in G. Hence

$$\begin{aligned} ab &= a_1^{\epsilon_1} a_2^{\epsilon_2} \cdots a_n^{\epsilon_n} b_1^{\delta_1} b_2^{\delta_2} \cdots b_k^{\delta_m} \\ &= b_1^{\delta_1} b_2^{\delta_2} \cdots b_k^{\delta_m} a_1^{\epsilon_1} a_2^{\epsilon_2} \cdots a_n^{\epsilon_n} \\ &= ba \end{aligned} \tag{7}$$

so that $\langle H, Z(G) \rangle$ is abelian.

■

Appendix I Cartesian Products and Zorn's Lemma

Cartesian Products

Exercise I.1.1. Let I and J be any two indexing sets and let A be an arbitrary set. For any function $\varphi : J \to I$ define

$$\varphi^* : \Pi_{i\in I} A \to \Pi_{j\in J} A \quad \text{by} \quad \varphi^*(f) = f \circ \varphi \quad \text{for all choice functions} \quad f \in \Pi_{i\in I} A.$$

- Let $I = \{1, 2\}$, let $J = \{1, 2, 3\}$ and let $\varphi : J \to I$ be defined by $\varphi(1) = 2$, $\varphi(2) = 2$ and $\varphi(3) = 1$. Describe explicitly how a 3-tuple in $A \times A \times A$ maps to an ordered pair in $A \times A$ under this φ^*.
- Let $I = J = \{1, 2, \ldots, n\}$ and assume φ is a permutation of I. Describe in terms of n-tuples in $A \times A \times \cdots \times A$ the function φ^*.

Partially Ordered Sets and Zorn's Lemma

Exercise I.2.1. Let A be the collection of all finite subsets of $\mathbb{R}$ ordered by inclusion. Discuss the existence (or nonexistence) of upper bounds, minimal and maximal elements (where minimal elements are defined analogously to maximal elements). Explain why this is not a well ordering.

> *Proof.* In this example, the set to be ordered is a set *of* sets. Not every such collection has an upper bound: for instance, the collection $\{\{i\} \mid i \in \mathbb{Z}\}$ of singleton sets are all members of A, but the collection has an infinite number of members and is not contained by a finite subset of $\mathbb{R}$ (i.e., a member of A).
>
> On the other hand, any finite collection of elements of A has a finite number of points, and can be covered by an element of A.
>
> There are no maximal (or minimal) elements of A since any candidate maximal element can be "increased" by taking the union of this candidate with an integer greater than the largest element in the candidate set (a similar argument holds for minimals).
>
> This is not a well ordering because it is not even a total ordering: the elements $\{1\}$ and $\{2\}$ of A are not comparable by inclusion.
>
> ■

Exercise I.2.2. Let A be the collection of all infinite subsets of $\mathbb{R}$ ordered by inclusion. Discuss the existence (or nonexistence) of upper bounds, minimal and maximal elements. Explain why this is not a well ordering.

> *Proof.* The set $A = \mathbb{R}$ itself is an infinite subset of $\mathbb{R}$ which is easily an upper bound for any collection of infinite subsets (alternately, given some collection of infinite subsets of $\mathbb{R}$, we can construct an upper bound by taking the union of this collection). $\mathbb{R}$ is also a maximal element of A.
>
> To show that there is no minimal element, let Z be some element of A, i.e., Z is an infinite subset of $\mathbb{R}$. Assume that Z is the minimal element of A, i.e., if

$X \leq Z$ for any $X \in A$, then $X = Z$. Then let z be some arbitrary element of Z and note that $Z \setminus \{z\} \leq Z$ is still an infinite subset of $\mathbb{R}$ but that $Z \setminus Z \neq Z$ and so Z is not a minimal element. Thus, we have a contradiction, and no such minimal element may exist.

As in the previous problem, this is not a well ordering since not every pair of infinite subsets of $\mathbb{R}$ may be compared by set inclusion; for instance, the set of even integers and the set of odd integers are disjoint and can not be compared. Hence, $\leq$ is not even a total ordering.

■

Exercise I.2.3. Show that the following partial orderings on the given sets are not well orderings:

- $\mathbb{R}$ under the usual relation $\leq$.
- $\mathbb{R}^+$ under the usual relation $\leq$.
- $\mathbb{R}^+ \cup \{0\}$ under the usual relation $\leq$.
- $\mathbb{Z}$ under the usual relation $\leq$.

Proof.

- Certainly, $\leq$ is a total ordering on $\mathbb{R}$. Note that $(1, 2)$ is a nonempty subset of $\mathbb{R}$ which has no smallest element. Thus $\leq$ is not a well ordering on $\mathbb{R}$.
- This case is very similar to the previous one, with the same conclusions.
- This case is very similar to the previous two.
- The relation $\leq$ is a total ordering on $\mathbb{Z}$. However, the even integers (including the negatives) are a nonempty subset with no smallest element, thus $\leq$ is not a well ordering.

■

Exercise I.2.4. Show that $\mathbb{Z}^+$ is well ordered under the usual relation $\leq$.

Proof. Since we can compare any two positive integers with $\leq$, it is clearly a total ordering on $\mathbb{Z}^+$. To show that this is well ordering, we take an aribtrary nonempty subset $A \subseteq \mathbb{Z}^+$ and demonstrate the existence of a minimum element.

Since A is nonempty, we can select some element $a \in A$. It would be nice if we could construct some iterative process by which to "walk down" from a in sequence: a, $a - 1$, $a - 2$, and so on until we hit the least element of A. However, we cannot be guaranteed that all of these elements are in A, and this adds some inelegant details.

Instead, consider the finite set $B = \{1, 2, 3, \ldots, a\}$. Certainly $A \cap B \neq \varnothing$ since $a \in A \cap B$. Since B is finite, this intersection is finite as well, and it has some least element, say c. Thus, $c \leq a$. Then let $b \in A$ be arbitrary. If $a \leq b$, then $c \leq b$ by transitivity of $\leq$. On the other hand, if $b \leq a$, then $b \in B$ and so $c \leq b$

since c is the smallest element. Thus, for any arbitrary element b of A, we have $c \leq b$, where $c \in A$. That is, c is a smallest element of A.

We have constructed a smallest element for any nonempty subset of $\mathbb{Z}^+$ under the total ordering $\leq$, hence this is a well ordering.

■