

Chapter 3

Exercise 1.

- (a) $x = 7k + 3$ for some $k \in \mathbb{Z}$.
- (b) $x = 23k + 7$ for some $k \in \mathbb{Z}$.
- (c) $x = 26k + 18$ for some $k \in \mathbb{Z}$.
- (d) $x = 5k + 2$ for some $k \in \mathbb{Z}$.
- (e) $x = 6k + 5$ for some $k \in \mathbb{Z}$.
- (f) There are no $x \in \mathbb{Z}$ satisfying this equivalence.

Exercise 2.

- (a) Not a group, there is no identity element.
- (b) Is a group, identity is a , every element is its own inverse, table is associative and closed.
- (c) Is a group, identity is a , $a^{-1} = a$, $b^{-1} = d$, $c^{-1} = c$, $d^{-1} = b$, associative and commutative.
- (d) Not a group, identity is a but d has no inverse.

Exercise 3.

Symmetries of a rectangle:

- e : do nothing
- ρ : rotate 180°
- μ_1 : flip horizontally
- μ_2 : flip vertically

Cayley table for symmetries of a rectangle:

\circ	e	ρ	μ_1	μ_2
e	e	ρ	μ_1	μ_2
ρ	ρ	e	μ_2	μ_1
μ_1	μ_1	μ_2	e	ρ
μ_2	μ_2	μ_1	ρ	e

Cayley table for $(\mathbb{Z}_4, +)$:

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

These two groups are not the same. There is only 1 nontrivial proper subgroup of $(\mathbb{Z}_4, +)$, consisting of the elements 0 and 2, while there are 3 nontrivial proper subgroups of the symmetries of a rectangle, $H_1 = \{e, \rho\}$, $H_2 = \{e, \mu_1\}$, and $H_3 = \{e, \mu_3\}$.

Exercise 4.

Symmetries of a rhombus:

- e : do nothing
- ρ : rotate 180°
- μ_1 : flip about the long diagonal
- μ_2 : flip about the short diagonal

Cayley table for symmetries of a rhombus:

\circ	e	ρ	μ_1	μ_2
e	e	ρ	μ_1	μ_2
ρ	ρ	e	μ_2	μ_1
μ_1	μ_1	μ_2	e	ρ
μ_2	μ_2	μ_1	ρ	e

Comparing with the Cayley table for symmetries of a rectangle from above, we can see that the two groups are the same.

Exercise 5.

Symmetries of a square:

- e : do nothing
- ρ_1 : rotate clockwise 90°
- ρ_2 : rotate clockwise 180°
- ρ_3 : rotate clockwise 270°
- μ_1 : flip horizontally
- μ_2 : flip vertically
- δ_1 : flip along diagonal $y = x$
- δ_2 : flip along diagonal $y = -x$

Cayley table for symmetries of a square:

\circ	e	ρ_1	ρ_2	ρ_3	μ_1	δ_1	μ_2	δ_2
e	e	ρ_1	ρ_2	ρ_3	μ_1	δ_1	μ_2	δ_2
ρ_1	ρ_1	ρ_2	ρ_3	e	δ_1	μ_2	δ_2	μ_1
ρ_2	ρ_2	ρ_3	e	ρ_1	μ_2	δ_2	μ_1	δ_1
ρ_3	ρ_3	e	ρ_1	ρ_2	δ_2	μ_1	δ_1	μ_2
μ_1	μ_1	δ_2	μ_2	δ_1	e	ρ_3	ρ_2	ρ_1
δ_1	δ_1	μ_1	δ_2	μ_2	ρ_1	e	ρ_3	ρ_2
μ_2	μ_2	δ_1	μ_1	δ_2	ρ_2	ρ_1	e	ρ_3
δ_2	δ_2	μ_2	δ_1	μ_1	ρ_3	ρ_2	ρ_1	e

There are 24 ways to permute 4 objects. However, not each permutation is a valid symmetry of the square, e.g. (A, C, B, D).

Exercise 6.

Multiplication table for $U(12)$:

\cdot	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

Exercise 7.

Let $S = \mathbb{R} \setminus \{-1\}$ and define $*$ on S by $a * b = a + b + ab$.

Proof. $(S, *)$ is an abelian group.

(Closed) Addition and multiplication are closed under the reals. We will show that there are no elements $a, b \in S$ such that $a * b = -1$.

Suppose for the sake of contradiction that $a, b \in S$ with $a * b = -1$. Then $a * b = a + b + ab = -1$, and rearranging and factoring gives $(a + 1)(b + 1) = 0$. This implies that either a or b is -1 , which is a contradiction, since a and b are in S . Thus S is closed under $*$.

(Associative) Let $a, b, c \in S$. Then

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

(Identity) The identity element is 0. Let $a \in S$. Then $0 * a = 0 + a + 0 = a$, and $a * 0 = a + 0 + 0 = a$.

(Inverse) Let $a \in S$. Then the inverse a^{-1} is given by $a^{-1} = -\frac{a}{a+1}$. We can see this because $a * a^{-1} = a - \frac{a}{a+1} - \frac{a^2}{a+1} = 0$.

(Commutative) Let $a, b \in S$. Then $a * b = a + b + ab = b + a + ba = b * a$.

Since $(S, *)$ is closed, associative, has an identity and inverses, and is commutative, it is an abelian group. \square

Exercise 8.

Let $A = \begin{bmatrix} 1 & 2 \\ 2 & 3 \end{bmatrix}$ and $B = \begin{bmatrix} 2 & 1 \\ 3 & 1 \end{bmatrix}$. Then $AB = \begin{bmatrix} 8 & 3 \\ 13 & 5 \end{bmatrix}$ but $BA = \begin{bmatrix} 4 & 7 \\ 5 & 9 \end{bmatrix}$.

Exercise 9.

Proof. The product of two matrices in $SL_2(\mathbb{R})$ has determinant one. Let $A, B \in SL_2(\mathbb{R})$ with $A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$ and $B = \begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix}$. Then $AB = \begin{bmatrix} a_{11}b_{11} + a_{12}b_{21} & a_{11}b_{12} + a_{12}b_{22} \\ a_{21}b_{11} + a_{22}b_{21} & a_{21}b_{12} + a_{22}b_{22} \end{bmatrix}$.

Then

$$\begin{aligned}
 \det(AB) &= (a_{11}b_{11} + a_{12}b_{21})(a_{21}b_{12} + a_{22}b_{22}) - (a_{11}b_{12} + a_{12}b_{22})(a_{21}b_{11} + a_{22}b_{21}) \\
 &= (a_{11}a_{21}b_{11}b_{12} + a_{11}a_{22}b_{11}b_{22} + a_{12}a_{21}b_{12}b_{21} + a_{12}a_{22}b_{21}b_{22}) \\
 &\quad - (a_{11}a_{21}b_{11}b_{12} + a_{11}a_{22}b_{12}b_{21} + a_{12}a_{21}b_{11}b_{22} + a_{12}a_{22}b_{21}b_{22}) \\
 &= a_{11}a_{22}b_{11}b_{22} + a_{12}a_{21}b_{12}b_{21} - a_{11}a_{22}b_{12}b_{21} - a_{12}a_{21}b_{11}b_{22} \\
 &= (a_{11}a_{22} - a_{12}a_{21})(b_{11}b_{22} - b_{12}b_{21}) \\
 &= \det(A) \det(B) \\
 &= 1
 \end{aligned}$$

Since A and B were arbitrary, the product of two matrices in $SL_2(\mathbb{R})$ has determinant one. \square

Exercise 10.

Let H be the set of matrices of the form $\begin{bmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{bmatrix}$.

Proof. H is a group under matrix multiplication.

(Closed) Let $A, B \in H$ given by $A = \begin{bmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{bmatrix}$ and $B = \begin{bmatrix} 1 & x' & y' \\ 0 & 1 & z' \\ 0 & 0 & 1 \end{bmatrix}$.

Then $AB = \begin{bmatrix} 1 & x+x' & y+y'+xz' \\ 0 & 1 & z+z' \\ 0 & 0 & 1 \end{bmatrix} \in H$.

(Associative) Matrix multiplication is associative.

(Identity) The matrix $I = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \in H$ is the identity element. From matrix multiplication, we know that $AI = IA = A$ for any $A \in H$.

(Inverse) Let $A = \begin{bmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{bmatrix} \in H$. The inverse A^{-1} is given by the matrix $\begin{bmatrix} 1 & -x & xz - y \\ 0 & 1 & -z \\ 0 & 0 & 1 \end{bmatrix}$.

We can see that $AA^{-1} = \begin{bmatrix} 1 & x-x & y+xz-y-xz \\ 0 & 1 & z-z \\ 0 & 0 & 1 \end{bmatrix} = I$.

Since $(H, *)$ is closed, associative, has an identity and inverses, it is a group. \square

Exercise 11.

The proof that $\det(AB) = \det(A)\det(B)$ for $A, B \in GL_2(\mathbb{R})$ is nearly identical to the proof in exercise 9, except that $\det(A), \det(B) \neq 1$.

Proof. $GL_2(\mathbb{R})$ is closed.

Let $A, B \in GL_2(\mathbb{R})$. Since $\det(AB) = \det(A)\det(B)$, and $\det(A), \det(B) \neq 0$, then $\det(AB) \neq 0$, and $AB \in GL_2(\mathbb{R})$. \square

Exercise 12.

Let $\mathbb{Z}_2^n = \{(a_1, a_2, \dots, a_n) : a_i \in \mathbb{Z}_2\}$, and a binary operation on \mathbb{Z}_2^n by

$$(a_1, a_2, \dots, a_n) + (b_1, b_2, \dots, b_n) = (a_1 + b_1, a_2 + b_2, \dots, a_n + b_n)$$

Proof. $(\mathbb{Z}_2^n, +)$ is a group.

(Closed) Let $A, B \in \mathbb{Z}_2^n$. Then for each $i \in [n]$, $a_i + b_i \in \mathbb{Z}_2$, so $A + B \in \mathbb{Z}_2^n$.

(Associative) Let $A, B, C \in \mathbb{Z}_2^n$. Then

$$\begin{aligned} (A + B) + C &= (a_1 + b_1, a_2 + b_2, \dots, a_n + b_n) + C \\ &= (a_1 + b_1 + c_1, a_2 + b_2 + c_2, \dots, a_n + b_n + c_n) \\ &= A + (b_1 + c_1, b_2 + c_2, \dots, b_n + c_n) \\ &= A + (B + C) \end{aligned}$$

(Identity) The identity $\mathbf{0}$ is given by $(0, 0, \dots, 0)$. We can see that for $A \in \mathbb{Z}_2^n$, $A + \mathbf{0} = \mathbf{0} + A = A$.

(Inverse) Let $A \in \mathbb{Z}_2^n$. Then $A^{-1} = (-a_1, -a_2, \dots, -a_n)$. It is straightforward to compute that $A + A^{-1} = \mathbf{0}$.

Since $(\mathbb{Z}_2^n, +)$ is closed, associative, has an identity and inverses, it is a group. \square

Exercise 13.

Proof. $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$ is a group under multiplication.

The reals are closed under multiplication, and no two nonzero reals multiply to get zero. Multiplication over the reals is associative. 1 is the identity element, since $1 \cdot x = x \cdot 1 = 1$ for all $x \in \mathbb{R}^*$. The inverse of an element $x \in \mathbb{R}^*$ is given by $1/x$, since $x \cdot 1/x = 1$. \square

Exercise 14.

Given the groups \mathbb{R}^* and \mathbb{Z} , let $G = \mathbb{R}^* \times \mathbb{Z}$. Define a binary operation \circ on G by $(a, m) \circ (b, n) = (ab, m + n)$.

Proof. (G, \circ) is a group.

(Closed) Let $A, B \in G$ with $A = (a, m)$ and $B = (b, n)$. Then $A \circ B = (ab, m + n)$. Since \mathbb{R}^* is closed under multiplication and \mathbb{Z} is closed under addition, G is closed.

(Associative) Let $A, B, C \in G$ with $A = (a, m)$, $B = (b, n)$, and $C = (c, p)$. Then

$$\begin{aligned} (A \circ B) \circ C &= (ab, m + n) \circ C \\ &= (abc, m + n + p) \\ &= A \circ (bc, n + p) \\ &= A \circ (B \circ C) \end{aligned}$$

(Identity) The identity is given by $(1, 0)$. We can see that for $A = (a, m) \in G$, $(1, 0) \circ A = (1 * a, 0 + m) = (a, m) = (a * 1, m + 0) = A \circ (1, 0)$.

(Inverse) Let $A = (a, m) \in G$. The inverse A^{-1} is given by $(1/a, -m)$. We can see that $A \circ A^{-1} = (a * 1/a, m - m) = (1, 0)$, and $A^{-1} \circ A = (1/a * a, -m + m) = (1, 0)$. Since (G, \circ) is closed, associative, has an identity and inverses, it is a group. \square

Exercise 15.

This is false; the symmetries of a triangle are nonabelian.

Exercise 16.

Consider the group of the symmetries of a triangle, and elements ρ_1 and μ_1 . Then $(\rho_1\mu_1)^2 = \mu_3^2 = id$, but $\rho_1^2\mu_1^2 = \rho_2id = \rho_2$.

Exercise 17.

Three examples of groups with eight elements are: $(\mathbb{Z}_8, +)$, D_4 , and Q_8 . Firstly $(\mathbb{Z}_8, +)$ is abelian, while D_4 and Q_8 are not. To compare D_4 and Q_8 , we can look at the nontrivial proper subgroups. For Q_8 , we have $\{1, -1\}$, $\{1, I, -1, -I\}$, $\{1, J, -1, -J\}$, and $\{1, K, -1, -K\}$. For D_4 , we have $\{1, \rho_2\}$, $\{1, \mu_1\}$, $\{1, \delta_1\}$, $\{1, \mu_2\}$, $\{1, \delta_2\}$, $\{1, \rho_1, \rho_2, \rho_3\}$, $\{1, \rho_2, \mu_1, \mu_2\}$, and $\{1, \rho_2, \delta_1, \delta_2\}$. These subgroups are different, so the groups are different.

Exercise 18.

Proof. There are $n!$ permutations of a set containing n items.

Let $\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ a_1 & a_2 & \cdots & a_n \end{pmatrix}$. Then we have n ways to choose a_1 , $n - 1$ ways to choose a_2, \dots , 2 ways to choose a_{n-1} , and 1 way to choose a_n . Thus we have $(n)(n-1)\dots(2)(1) = n!$ ways to permute n items. \square

Exercise 19.

Let $n \in \mathbb{Z}^+$ and $a \in \mathbb{Z}_n$. By definition of modular congruence, $x \equiv y \pmod{n} \iff n \mid (x - y)$. Since $n \mid 0$, $n \mid (0 + a - a)$, so $0 + a \equiv a \pmod{n}$. Similarly, $n \mid (a + 0 - a)$, so $a + 0 \equiv a \pmod{n}$.

Exercise 20.

Similar to above, $n \mid 0$ so $n \mid (a \cdot 1 - a) \iff a \cdot 1 \equiv a \pmod{n}$.

Exercise 21.

Let $b = n - a$. Then $n \mid n \iff n \mid (a + n - a - 0) \iff n \mid (a + b - 0) \iff a + b \equiv 0 \pmod{n}$. A similar argument shows $b + a \equiv 0 \pmod{n}$.

Exercise 22.

Let $a, b, c \in \mathbb{Z}_n$. Then $(a + b) + c \equiv x \pmod{n} \iff n \mid (a + b) + c - x \iff n \mid a + (b + c) - x \iff a + (b + c) \equiv x \pmod{n}$. We also have $(ab)c \equiv x \pmod{n} \iff n \mid (ab)c - x \iff n \mid a(bc) - x \iff a(bc) \equiv x \pmod{n}$.

Exercise 23.

We have $n \mid 0 \iff n \mid (ab + ac - (ab + ac)) \iff n \mid (a(b + c) - (ab + ac)) \iff a(b + c) \equiv ab + ac \pmod{n}$.

Exercise 24. *Note:* This proof uses the identity in exercise 26.

Proof. $ab^n a^{-1} = (aba^{-1})^n$ for $n \in \mathbb{Z}$, where a and b are elements in a group G .
Let $a, b \in G$.

We will first show that the identity holds for $n \in \mathbb{Z}^+ \cup \{0\}$ by induction on $\mathbb{Z}^+ \cup \{0\}$.

(Base Case): $n = 0$. Then $ab^0 a^{-1} = aa^{-1} = e = (aba^{-1})^0$.

(Inductive Step): Assume $ab^n a^{-1} = (aba^{-1})^n$ for some $n \in \mathbb{Z}^+ \cup \{0\}$. We want to show that $ab^{n+1} a^{-1} = (aba^{-1})^{n+1}$.

We have $(aba^{-1})^{n+1} = (aba^{-1})^n (aba^{-1})$. Applying the inductive hypothesis, we have $(aba^{-1})^n (aba^{-1}) = ab^n a^{-1} aba^{-1} = ab^n ba^{-1} = ab^{n+1} a^{-1}$, as desired.

By the principle of mathematical induction, $ab^n a^{-1} = (aba^{-1})^n$ for all $n \in \mathbb{Z}^+ \cup \{0\}$.

Next, we will show that if $ab^n a^{-1} = (aba^{-1})^n$ for some $n \in \mathbb{Z}^+ \cup \{0\}$, then $ab^{-n} a^{-1} = (aba^{-1})^{-n}$. We have $(aba^{-1})^{-n} = ((aba^{-1})^{-1})^n = ((a^{-1})^{-1} b^{-1} a^{-1})^n = (ab^{-1} a^{-1})^n = ab^{-n} a^{-1}$, as desired.

Thus $ab^n a^{-1} = (aba^{-1})^n$ for $n \in \mathbb{Z}$. □

Exercise 25.

Proof. For any $n > 2$, there exists $k \in U(n)$ such that $k^2 = 1$ and $k \neq 1$.

Consider $k = n - 1$. Since $\gcd(n, n - 1) \mid (n - (n - 1)) \iff \gcd(n, n - 1) \mid 1$, we can conclude that $\gcd(n, n - 1) = 1$. Since k is relatively prime to n , $k \in U(n)$. Then $k^2 = n^2 - 2n + 1$, so $k^2 \equiv 1 \pmod{n}$. If $k = 1$, then $n \mid (n - 2)$, forcing $n = 2$, contradicting $n > 2$. Therefore $k \neq 1$. □

Exercise 26.

Proof. $(g_1 g_2 \dots g_{n-1} g_n)^{-1} = g_n^{-1} g_{n-1}^{-1} \dots g_2^{-1} g_1^{-1}$ for all $n \in \mathbb{Z}^+$.

We prove this by induction on \mathbb{Z}^+ .

(Base Case): $n = 1$. $g_1^{-1} = g_1^{-1}$.

(Inductive Step): Assume $(g_1 g_2 \dots g_{n-1} g_n)^{-1} = g_n^{-1} g_{n-1}^{-1} \dots g_2^{-1} g_1^{-1}$ for some $n \in \mathbb{Z}^+$. We want to show that $(g_1 g_2 \dots g_{n-1} g_n g_{n+1})^{-1} = g_{n+1}^{-1} g_n^{-1} g_{n-1}^{-1} \dots g_2^{-1} g_1^{-1}$. We have $g_{n+1}^{-1} g_n^{-1} g_{n-1}^{-1} \dots g_2^{-1} g_1^{-1} = g_{n+1}^{-1} (g_1 g_2 \dots g_{n-1} g_n)^{-1} = (g_1 g_2 \dots g_{n-1} g_n g_{n+1})^{-1}$, from the identity that $(ab)^{-1} = b^{-1} a^{-1}$. □

Exercise 27.

Proof. If G is a group and $a, b \in G$, $xa = b$ has unique solutions in G .

Suppose that $xa = b$. We must show that such an x exists. Multiplying both sides of $xa = b$ by a^{-1} , we have $x = xa a^{-1} = ba^{-1}$. To show uniqueness, suppose that x_1 and x_2 are both solutions of $xa = b$; then $x_1 a = b = x_2 a$. So $x_1 = x_1 a a^{-1} = x_2 a a^{-1} = x_2$. □

Exercise 28.

Note: I really don't want to do this proof because it's straightforward and boring, sorry :/

Exercise 29.

Proof. $ab = ac \implies b = c$ and $ba = ca \implies b = c$ for $a, b, c \in G$ in a group G .

Start with $ab = ac$. Multiply the left sides by a^{-1} , giving $a^{-1}ab = a^{-1}ac \implies b = c$. A similar argument follows for the other case. □

Exercise 30.

Proof. For a group G , if $a^2 = e$ for all $a \in G$, then G is abelian.

Assume $a^2 = e$ for all $a \in G$. Let $a, b \in G$. Since $(ab)^2 = e$, it follows that $(ab)(ab) = e$. Then $abab = e$. Multiplying by a on the left and b on the right, we get that $ba = ab$. Since a and b commute, then G is abelian. \square

Exercise 31.

Proof. If G is a finite group of even order, then there exists an $a \in G$ such that $a \neq e$ and $a^2 = e$. Assume for the sake of contradiction that no $a \in G$ satisfies $a \neq e$ and $a^2 = e$. Partition $G \setminus \{e\}$ into sets of a and its inverse. Since $a \neq a^{-1}$, these sets all have two elements. However, the number of elements in $G \setminus \{e\}$ is odd, so there is no way we were able to partition all elements into sets. Therefore there must exist an element $a \in G$ such that $a^2 = e$. \square

Exercise 32.

Proof. If G is a group, and $(ab)^2 = a^2b^2$ for all $a, b \in G$, then G is abelian.

Let $a, b \in G$. Since $(ab)^2 = abab = aabb$, we can multiply the left side by a^{-1} and the right side by b^{-1} to get that $ba = ab$, so G is abelian. \square

Exercise 33.

The subgroups of $\mathbb{Z}_3 \times \mathbb{Z}_3$ are $\{(0, 0)\}$, $\{(0, 0), (0, 1), (0, 2)\}$, $\{(0, 0), (1, 0), (2, 0)\}$, $\{(0, 0), (1, 1), (2, 2)\}$, $\{(0, 0), (1, 2), (2, 1)\}$, and $\mathbb{Z}_3 \times \mathbb{Z}_3$.

The subgroups of \mathbb{Z}_9 are $\{0\}$, $\{0, 3, 6\}$, and \mathbb{Z}_9 .

Exercise 34.

The subgroups of the symmetry group of an equilateral triangle are $\{id\}$, $\{id, \mu_1\}$, $\{id, \mu_2\}$, $\{id, \mu_3\}$, $\{id, \rho_1, \rho_2\}$, and the whole group.

Exercise 35.

Just like in exercise 17, we have $\{1\}$, $\{1, \rho_2\}$, $\{1, \mu_1\}$, $\{1, \delta_1\}$, $\{1, \mu_2\}$, $\{1, \delta_2\}$, $\{1, \rho_1, \rho_2, \rho_3\}$, $\{1, \rho_2, \mu_1, \mu_2\}$, $\{1, \rho_2, \delta_1, \delta_2\}$, and the whole group.

Exercise 36.

Proof. $H = \{2^k : k \in \mathbb{Z}\}$ is a subgroup of \mathbb{Q}^* .

We have $k = 0$ gives $2^0 = 1 \in H$. Let $a, b \in H$, with $a = 2^m$ and $b = 2^n$ for some $m, n \in \mathbb{Z}$. Then $ab^{-1} = 2^m 2^{-n} = 2^{m-n} \in H$. Thus H is a subgroup of \mathbb{Q}^* . \square

Exercise 37.

Let $n \geq 0$ and $n\mathbb{Z} = \{nk : k \in \mathbb{Z}\}$.

Proof. $n\mathbb{Z}$ is a subgroup of \mathbb{Z} , and these subgroups are the only subgroups.

We have $k = 0$ gives $n \cdot 0 = 0 \in n\mathbb{Z}$. Let $a, b \in n\mathbb{Z}$ with $a = nk$ and $b = nl$ for some $k, l \in \mathbb{Z}$. Then $a - b = nk - nl = n(k - l) \in n\mathbb{Z}$.

Let H be a subgroup of \mathbb{Z} . We will show that $H = n\mathbb{Z}$ for some $n \geq 0$. If $H = \{0\}$ then $H = 0\mathbb{Z}$. Otherwise, H contains some positive integer. Since H is a subset of \mathbb{Z} , by the well-ordering principle, H contains a smallest positive integer. Call this integer n .

We will show that $H = n\mathbb{Z}$.

(\supseteq) Since H is a subgroup of \mathbb{Z} , it is closed under addition. Since $n \in H$, $nk \in H$ for all $k \in \mathbb{Z}$.

(\subseteq) Let $m \in H$. Then we can use the division algorithm to write $m = qn + r$ with $0 \leq r < n$. Since H is closed under subtraction, $r = m - qn \in H$. Since n was the smallest positive integer of H , r must be 0. Therefore $m \in n\mathbb{Z}$.

Therefore, $H = n\mathbb{Z}$, and since H was an arbitrary subgroups of \mathbb{Z} , all subgroups are in the form $n\mathbb{Z}$. \square

Exercise 38.

Proof. $\mathbb{T} = \{z \in \mathbb{C}^* : |z| = 1\}$ is a subgroup of \mathbb{C}^* .

The identity $z = 1 + 0i \in \mathbb{T}$. Let $z, w \in \mathbb{T}$ with $z = a + bi$ and $w = c + di$. Then $zw^{-1} = \frac{(a+bi)(c-di)}{c^2+d^2} = (a+bi)(c-di) = (ac+bd) + (bc-ad)i$.

We can see that $|zw^{-1}| = \sqrt{(ac+bd)^2 + (bc-ad)^2} = \sqrt{(a^2+b^2)(c^2+d^2)} = 1$, so $zw^{-1} \in \mathbb{T}$. \square

Exercise 39.

Let G consist of the 2×2 matrices of the form $\begin{bmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{bmatrix}$, where $\theta \in \mathbb{R}$.

Proof. G is a subgroup of $SL_2(\mathbb{R})$.

We have $\theta = 0$ gives $I \in G$. Let $A, B \in G$ with A given by θ and B given by ϕ . Then

$$\begin{aligned} AB^{-1} &= \begin{bmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{bmatrix} \begin{bmatrix} \cos \phi & \sin \phi \\ -\sin \phi & \cos \phi \end{bmatrix} \\ &= \begin{bmatrix} \cos \theta \cos \phi + \sin \theta \sin \phi & \cos \theta \sin \phi - \sin \theta \cos \phi \\ \sin \theta \cos \phi - \cos \theta \sin \phi & \sin \theta \sin \phi + \cos \theta \cos \phi \end{bmatrix} \\ &= \begin{bmatrix} \cos(\theta - \phi) & -\sin(\theta - \phi) \\ \sin(\theta - \phi) & \cos(\theta - \phi) \end{bmatrix} \in G \end{aligned}$$

\square

Exercise 40.

Proof. $G = \{a + b\sqrt{2} : a, b \in \mathbb{Q} \text{ and } a, b \neq 0\}$ is a subgroup of \mathbb{R}^* under multiplication.

We have $a = 1, b = 0$ is the identity and is in G . Let $A, B \in G$ with $A = a + q\sqrt{2}$ and $B = b + r\sqrt{2}$.

Then $AB^{-1} = \frac{(a + q\sqrt{2})(b - r\sqrt{2})}{b^2 - 2r^2} = \frac{ab - 2rq}{b^2 - 2r^2} + \frac{bq - ar}{b^2 - 2r^2}\sqrt{2} \in G$. \square

Exercise 41. Let G be the group of 2×2 matrices under addition.

Proof. $H = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : a + d = 0 \right\}$ is a subgroup of G .

The matrix $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \in H$ is the identity element. If you have two matrices $A = \begin{bmatrix} a & x \\ y & -a \end{bmatrix}$ and

$B = \begin{bmatrix} b & z \\ w & -b \end{bmatrix}$, then $A - B = \begin{bmatrix} a - b & x - z \\ y - w & b - a \end{bmatrix}$ and we can see that $a - b + b - a = 0$ so $A - B \in H$. \square

Exercise 42.

Proof. $SL_2(\mathbb{Z})$ is a subgroup of $SL_2(\mathbb{R})$.

The matrix I is in $SL_2(\mathbb{Z})$ and serves as the identity. To show that for any $A, B \in SL_2(\mathbb{Z})$ that $AB^{-1} \in SL_2(\mathbb{Z})$, we can observe that the inverse of B is given by $B^{-1} = \frac{1}{\det B} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$, but since $\det B = 1$, B^{-1} only has integer coefficients. We can then convince ourselves that $AB^{-1} \in SL_2(\mathbb{Z})$. \square

Exercise 43.

Like in exercise 17, the subgroups of Q_8 are $\{1\}$, $\{1, -1\}$, $\{1, I, -1, -I\}$, $\{1, J, -1, -J\}$, $\{1, K, -1, -K\}$, and Q_8 .

Exercise 44.

Let H_1 and H_2 be subgroup of G .

Proof. $H_1 \cap H_2$ is a subgroup of G .

Since H_1 and H_2 are both subgroups of G , we know that the identity e is in both subgroups, so $e \in H_1 \cap H_2$.

Let $g, h \in H_1 \cap H_2$. We want to show that $gh^{-1} \in H_1$ and $gh^{-1} \in H_2$. Since $g, h \in H_1 \cap H_2$, then $g, h \in H_1$. Since H_1 is a group, $gh^{-1} \in H_1$ under closure. A similar argument follows for H_2 . \square

Exercise 45.

Claim: If H and K are subgroups of a group G , then $H \cup K$ is a subgroup of G .

Proof. This is false.

Consider the subgroups of the symmetries of a triangle. Two such subgroups are $\{id, \mu_1\}$ and $\{id, \mu_2\}$. We can see that the union $\{id, \mu_1, \mu_2\}$ is not a subgroup since $\mu_1\mu_2^{-1} = \rho_2 \notin \{id, \mu_1, \mu_2\}$. \square

Exercise 46.

Note: I'm lazy and I don't want to do the proof that it is false if G is not abelian. Consider S_3 .

Claim: If H and K are subgroups of a group G , then $HK = \{hk : h \in H \text{ and } k \in K\}$ is a subgroup of G .

Proof. If G is abelian, the claim is true.

Assume G is abelian. Consider arbitrary H and K that are subgroups of G . Since $e \in H$ and $e \in K$, then $ee = e \in HK$. Then consider $g = ab, h = cd \in HK$. We see that $gh^{-1} = abd^{-1}c^{-1}$. Since G is abelian, this is equal to $ac^{-1}bd^{-1} \in HK$, as desired. \square

Exercise 47.

Let G be a group and $Z(G) = \{x \in G : gx = xg \text{ for all } g \in G\}$.

Proof. $Z(G)$ is a subgroup of G .

We can see that $id \in Z(G)$ because $id \circ g = g \circ id = g$ for all $g \in G$. Suppose $a, b \in Z(G)$. Let $g \in G$. Then $ab^{-1}g = agb^{-1}$ because $b \in Z(G)$ and $agb^{-1} = gab^{-1}$ because $a \in Z(G)$. \square

Exercise 48.

Proof. Let $a, b \in G$. If $a^4b = ba$ and $a^3 = e$, then $ab = ba$.

We can see that $a^4b = ba \iff a^3ab = ba \iff eab = ba \iff ab = ba$. \square

Exercise 49.

$(\mathbb{Z}, +)$ is an infinite group and $n\mathbb{Z}$ are the only subgroups of \mathbb{Z} , and are infinite (besides $\{0\}$, which is trivial) by exercise 37.

Exercise 50.