Group Theory Exercises 2

Jason Sass

July 20, 2023

Cyclic Groups

Order of a group element

Exercise 1. Compute the order of the elements below.
a. 5 in the group $(\mathbb{Z}_{12}, +)$.
b. $\sqrt{3}$ in the group $(\mathbb{R}, +)$.
c. $\sqrt{3}$ in the group $(\mathbb{R}^*, \cdot))$
d. $-i$ in the group $(\mathbb{C}^*, \cdot)$
e. 72 in the group $(\mathbb{Z}_{240}, +)$
f. 312 in the group $(\mathbb{Z}_{471}, +)$

Solution. a. Since $|\mathbb{Z}_{12}| = 12$, then the group $(\mathbb{Z}_{12}, +)$ is finite.
Every element of a finite group has finite order, so $5 \in \mathbb{Z}_{12}$ has finite order.
Let n be the order of 5.
Then n is the least positive integer such that $5n \equiv 0 \pmod{12}$, so n is the least positive integer such that 12 divides $5n$.
Therefore, $n = 12$, so $5 \in \mathbb{Z}_{12}$ has order 12 and $|5| = 12$.

b. There is no positive integer n such that $n\sqrt{3} = 0$, so $\sqrt{3} \in \mathbb{R}$ has infinite order.
We prove there is no $n \in \mathbb{Z}^+$ such that $n\sqrt{3} = 0$.
Let $n \in \mathbb{Z}^+$.
Then $n \in \mathbb{Z}$ and $n > 0$.
Since $n \in \mathbb{Z}$ and $\mathbb{Z} \subset \mathbb{R}$, then $n \in \mathbb{R}$.
Since $n > 0$, then $n \neq 0$.
Since $n \in \mathbb{R}$ and $n \neq 0$, then n is a nonzero real number.
Since $\sqrt{3} \in \mathbb{R}$ and $\sqrt{3} \neq 0$, then $\sqrt{3}$ is a nonzero real number.
The product of two nonzero real numbers is nonzero, so $n\sqrt{3}$ is a nonzero real number.
Hence, $n\sqrt{3} \neq 0$.
Thus, $n\sqrt{3} \neq 0$ for all $n \in \mathbb{Z}^+$, so there is no $\in \mathbb{Z}^+$ such that $n\sqrt{3} = 0$.
Therefore, $\sqrt{3} \in \mathbb{R}$ has infinite order and $|\sqrt{3}| = \infty$.

c. There is no $n \in \mathbb{Z}^+$ such that $n\sqrt{3} = 1$ so $\sqrt{3} \in \mathbb{R}^*$ has infinite order.
We prove there is no $n \in \mathbb{Z}^+$ such that $n\sqrt{3} = 1$.
Let $n \in \mathbb{Z}^+$.
The $n \geq 1$.
Since $3 > 1$, then $\sqrt{3} > \sqrt{1}$, so $\sqrt{3} > 1$.
Since $n \geq 1$ and $\sqrt{3} > 1$, then $n\sqrt{3} > 1$, so $n\sqrt{3} \neq 1$.
Hence, $n\sqrt{3} \neq 1$ for all $n \in \mathbb{Z}^+$, so there is no $n \in \mathbb{Z}^+$ such that $n\sqrt{3} = 1$.
Therefore, $\sqrt{3} \in \mathbb{R}^*$ has infinite order and $|\sqrt{3}| = \infty$.

d. Since $(-i)^1 = -i$ and $(-i)^2 = -1$ and $(-i)^3 = i$ and $(-i)^4 = 1$, then $-i$ has order 4, so $|-i| = 4$.

e. Since $|\mathbb{Z}_{240}| = 240$, then the group $(\mathbb{Z}_{240}, +)$ is finite.
Every element of a finite group has finite order, so $72 \in \mathbb{Z}_{240}$ has finite order.
Let n be the order of 72.
Then n is the least positive integer such that $72n \equiv 0 \pmod{240}$, so n is the least positive integer such that 240 divides $72n$.
Therefore, $n = 10$, so $72 \in \mathbb{Z}_{240}$ has order 10 and $|72| = 10$.

f. Since $|\mathbb{Z}_{471}| = 471$, then the group $(\mathbb{Z}_{471}, +)$ is finite.
Every element of a finite group has finite order, so $312 \in \mathbb{Z}_{471}$ has finite order.
Let n be the order of 312.
Then n is the least positive integer such that $312n \equiv 0 \pmod{471}$, so n is the least positive integer such that 471 divides $312n$.
Therefore, $n = 157$, so $312 \in \mathbb{Z}_{741}$ has order 157 and $|312| = 157$.

□

Exercise 2. Compute the order of the groups below.
a. $\mathbb{Z}_{18}$
b. D_4
c. S_4
d. S_5
e. $\mathbb{Z}_{18}^*$

Solution. a. The group $(\mathbb{Z}_{18}, +)$ is the group of integers modulo 18 under addition.
The order is $|\mathbb{Z}_{18}| = 18$ and $\mathbb{Z}_{18} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17\}$.

b. The group D_4 is TODO.

c. The group $(S_4, \circ)$ is the symmetric group of degree 4 under function composition.
The order of S_4 is $|S_4| = 4! = 24$, so there are 24 permutations on a set of 4 symbols.

d. The group $(S_5, \circ)$ is the symmetric group of degree 5 under function composition.

The order of S_5 is $|S_5| = 5! = 120$, so there are 120 permutations on a set of 5 symbols.

e. The group $(\mathbb{Z}_{18}^*, \cdot)$ is the group of units of the integers modulo 18 under multiplication.

The order of $\mathbb{Z}_{18}^*$ is $|\mathbb{Z}_{18}^*| = \phi(18) = 6$ and $\mathbb{Z}_{18}^* = \{1, 5, 7, 11, 13, 17\}$.

□

Exercise 3. The number 2 has infinite order in the group $(\mathbb{R}^*, \cdot)$.

Proof. We first prove $2^n > 1$ for all $n \in \mathbb{Z}^+$ by induction on n.

Define the predicate $p(n) : 2^n > 1$ over $\mathbb{Z}$.

We prove $p(n)$ is true for all $n \geq 1$ by induction on n.

Basis:

Since $2^1 = 2 > 1$, then $p(1)$ is true.

Induction:

Suppose $p(k)$ is true for any $k \in \mathbb{Z}^+$.

Then $2^k > 1$.

Since $2^{k+1} = 2^k \cdot 2 > 1 \cdot 2 = 2 > 1$, then $2^{k+1} > 1$, so $p(k+1)$ is true.

Therefore, $p(k)$ implies $p(k+1)$ for all $k \in \mathbb{Z}^+$.

Since $p(1)$ is true and $p(k)$ implies $p(k+1)$ for all $k \in \mathbb{Z}^+$, then by PMI, $p(n)$ is true for all $n \in \mathbb{Z}^+$.

Since $2^n > 1$ for all $n \in \mathbb{Z}^+$, then $2^n \neq 1$ for all $n \in \mathbb{Z}^+$, so there is no $n \in \mathbb{Z}^+$ such that $2^n = 1$.

Therefore, the order of 2 is infinite.

The cyclic subgroup generated by 2 is $\langle 2 \rangle = \{2^n : n \in \mathbb{Z}\} = \{..., \frac{1}{32}, \frac{1}{16}, \frac{1}{8}, \frac{1}{4}, \frac{1}{2}, 1, 2, 4, 8, 16, 32, ...\}$.

□

Exercise 4. Calculate the orders of each element in the 4^{th} roots of unity group $(U_4, \cdot)$.

Solution. Since $U_4 = \{1, i, -1, -i\}$, then $|U_4| = 4$, so U_4 is a finite group.

Since every element of a finite group has finite order, then every element of U_4 has finite order.

Since $1^1 = 1$, then the order of 1 is $|1| = 1$ and $\langle 1 \rangle = \{1\}$.

Since $i^1 = i$ and $i^2 = -1$ and $i^3 = -i$ and $i^4 = 1$, then the order of i is $|i| = 4$ and $\langle i \rangle = U_4$.

Since $(-1)^1 = -1$ and $(-1)^2 = 1$, then the order of -1 is $|-1| = 2$ and $\langle -1 \rangle = \{1, -1\}$.

Since $(-i)^1 = -i$ and $(-i)^2 = -1$ and $(-i)^3 = i$ and $(-i)^4 = i$, then the order of $-i$ is $|-i| = 4$ and $\langle -i \rangle = U_4$. □

Exercise 5. Calculate the order of the element $\sigma \in S_3$.

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

Solution. The symmetric group $(S_3, \circ)$ has order $|S_3| = 3! = 6$, so S_3 is a finite group.

Since every element of a finite group has finite order, then every element of S_3 has finite order.

Let k be the order of σ.

Then k is the least positive integer such that $\sigma^k = id$, where id is the identity permutation in $(S_3, \circ)$.

$$\sigma^2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

$$\sigma^3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$$

Therefore, $k = 3$, so the order of σ is $|\sigma| = 3$.

Hence, 3 is the order of the cyclic subgroup generated by σ.

The cyclic subgroup generated by σ is $\langle\sigma\rangle = \{id, \sigma, \sigma^2\}$. $\square$

Exercise 6. Calculate the order of the element 8 in the group $(\mathbb{Z}_{12}, +)$.

Solution. Since $(\mathbb{Z}_{12}, +)$ has order $|\mathbb{Z}_{12}| = 12$, then $\mathbb{Z}_{12}$ is a finite group.

Since every element of a finite group has finite order, then every element of $\mathbb{Z}_{12}$ has finite order.

The order of 8 is the least positive integer k such that $8k \equiv 0 \pmod{12}$.

We compute $8 * 1 = 8$ and $8 * 2 = 16 = 4$ and $8 * 3 = 24 = 0$.

Therefore, $k = 3$, so the order of 8 is $|8| = 3$.

Hence, 3 is the order of the cyclic subgroup generated by 8.

The cyclic subgroup generated by 8 is $\langle 8 \rangle = \{8k : k \in \mathbb{Z}\} = \{0, 4, 8\}$. $\square$

Exercise 7. Calculate the order of the element 5 in the group $(\mathbb{Z}_8^*, \cdot)$.

Solution. Since the group of units $(\mathbb{Z}_8^*, \cdot)$ has order $|\mathbb{Z}_8^*| = \phi(8) = 4$, then $\mathbb{Z}_8^*$ is a finite group.

Since every element of a finite group has finite order, then every element of $\mathbb{Z}_8^*$ has finite order.

The order of 5 is the least positive integer k such that $5^k \equiv 1 \pmod 8$.

We compute $5^1 = 5$ and $5^2 = 25 \equiv 1 \pmod 8$.

Therefore, $k = 2$, so the order of 5 is 2.

Alternatively, we analyze the Cayley multiplication table for the group of units $\mathbb{Z}_8^*$.

Since the order of $\mathbb{Z}_8^*$ is $\phi(8) = 4$, then there are 4 elements in the group of units $\mathbb{Z}_8^*$ and each element is relatively prime to the modulus 8. Hence, if $a \in \mathbb{Z}_8^*$, then $\gcd(a, 8) = 1$, so $a = 1$ or $a = 3$ or $a = 5$ or $a = 7$.

The Cayley table is below.

*	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

We observe that $|5| = 2$. Therefore, 2 is the order of the cyclic subgroup generated by 5.

The cyclic subgroup generated by 5 is $\{1, 5\}$. $\square$

Exercise 8. Calculate the order of the element $\sigma \in S_7$.

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 7 & 5 & 1 & 4 & 6 \end{pmatrix}$$

Solution. Since the symmetric group $(S_7, \circ)$ has order $|S_7| = 7! = 5040$, then S_7 is a finite group.

Since every element of a finite group has finite order, then every element of S_7 has finite order.

Let k be the order of σ.

Then k is the least positive integer such that $\sigma^k = id$, where id is the identity permutation in $(S_7, \circ)$.

$$\sigma^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 7 & 6 & 1 & 2 & 5 & 4 \end{pmatrix}$$

$$\sigma^3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 6 & 4 & 2 & 3 & 1 & 5 \end{pmatrix}$$

$$\sigma^4 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 6 & 4 & 5 & 3 & 7 & 2 & 1 \end{pmatrix}$$

$$\sigma^5 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 5 & 1 & 7 & 6 & 3 & 2 \end{pmatrix}$$

$$\sigma^6 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 1 & 2 & 6 & 4 & 7 & 3 \end{pmatrix}$$

$$\sigma^7 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 \end{pmatrix}$$

Therefore, $k = 7$, so the order of σ is 7.

Hence, 7 is the order of the cyclic subgroup generated by σ, so $|\sigma| = 7$.

The cyclic subgroup generated by σ is $\{id, \sigma, \sigma^2, \sigma^3, \sigma^4, \sigma^5, \sigma^6\}$. $\square$

Exercise 9. Calculate the order of the element $A \in GL_2(\mathbb{R})$.

$$A = \begin{bmatrix} 0 & -1 \\ 1 & 1 \end{bmatrix}$$

Solution. We first show that the matrix A is an element of $GL_2(\mathbb{R})$.
Since $\det A = 0(1) - (-1)1 = 1 \neq 0$, then A has an inverse, so A is invertible.
Therefore, A is an element of $GL_2(\mathbb{R})$.
The inverse matrix is

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

Observe that $AA^{-1} = A^{-1}A = I$, where I is the identity matrix.

Let k be the order of A.
Then k is the least positive integer such that $A^k = I$.
Observe that

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

$$A^3 = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$$

$$A^4 = \begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix}$$

$$A^5 = \begin{bmatrix} 1 & 1 \\ -1 & 0 \end{bmatrix}$$

$$A^6 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

Thus, $k = 6$, so the multiplicative order of A is 6 and $|A| = 6$.
Since the order of A is 6, then 6 is the order of the cyclic subgroup generated by A.
The cyclic subgroup generated by A is $\{I, A, A^2, A^3, A^4, A^5\}$. $\square$

Exercise 10. Calculate the order of the element $A \in GL_2(\mathbb{R})$.

$$A = \begin{bmatrix} -\frac{1}{2} & \frac{1}{2} \\ -\frac{3}{2} & -\frac{1}{2} \end{bmatrix}$$

Solution. We first show that the matrix A is an element of $GL_2(\mathbb{R})$.

Since $\det A = (\frac{-1}{2})(\frac{-1}{2}) - (\frac{1}{2})(\frac{-3}{2}) = 1 \neq 0$, then A has an inverse, so A is invertible.

Therefore, A is an element of $GL_2(\mathbb{R})$.

The inverse matrix is

$$A^{-1} = \begin{bmatrix} -\frac{1}{2} & -\frac{1}{2} \\ \frac{3}{2} & -\frac{1}{2} \end{bmatrix}$$

Observe that $AA^{-1} = A^{-1}A = I$, where I is the identity matrix.

Let k be the order of A.

Then k is the least positive integer such that $A^k = I$.

Observe that

$$A^2 = \begin{bmatrix} -\frac{1}{2} & -\frac{1}{2} \\ \frac{3}{2} & -\frac{1}{2} \end{bmatrix}$$

$$A^3 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

Thus, $k = 3$, so the multiplicative order of A is 3 and $|A| = 3$.

Since the order of A is 3, then 3 is the order of the cyclic subgroup generated by A.

The cyclic subgroup generated by A is $\{I, A, A^2\}$.

Note that $A^{-1} = A^2$. □

Cyclic subgroups

Exercise 11. The group $(3\mathbb{Z}, +)$ is a cyclic group.

Proof. For any $n \in \mathbb{Z}$, $(n\mathbb{Z}, +)$ is a subgroup of $(\mathbb{Z}, +)$, so $(3\mathbb{Z}, +)$ is a subgroup of $(\mathbb{Z}, +)$.

Hence, $(3\mathbb{Z}, +)$ is a group.

The cyclic subgroup generated by 3 is the set of all multiples of 3.

Therefore, $\langle 3 \rangle = \{3k : k \in \mathbb{Z}\} = 3\mathbb{Z}$.

Since $3 \in \mathbb{Z}$ and $3\mathbb{Z} = \langle 3 \rangle$, then $3\mathbb{Z}$ is a cyclic group with generator 3. □

Exercise 12. Let $H = \{2^k : k \in \mathbb{Z}\}$.
The group $(H, \cdot)$ is a cyclic group.

Proof. We previously proved that $(H, \cdot)$ is a subgroup of $(\mathbb{Q}^*, \cdot)$, so $(H, \cdot)$ is a group.

The cyclic subgroup generated by 2 is the set of all integer powers of 2.
Therefore, $\langle 2 \rangle = \{2^n : n \in \mathbb{Z}\} = H$.
Since $2 = 2^1$ and $1 \in \mathbb{Z}$, then $2 \in H$.
Since $2 \in H$ and $H = \langle 2 \rangle$, then H is a cyclic group generated by 2. $\square$

Exercise 13. Analyze the order of the group $(\mathbb{Z}, +)$.

Solution. Observe that $\mathbb{Z}$ is the abelian group of integers under addition.
Since $1 \cdot 0 = 0$, then the order of $0 \in \mathbb{Z}$ is $|0| = 1$ and the cyclic subgroup generated by 0 is $\langle 0 \rangle = \{0\}$.

We prove if $k \in \mathbb{Z}^*$, then $nk \neq 0$ for all $n \in \mathbb{Z}^+$.
Let $n \in \mathbb{Z}^+$.
Suppose $k \in \mathbb{Z}^*$.
Then $k \in \mathbb{Z}$ and $k \neq 0$, so either $k > 0$ or $k < 0$.
We consider these cases separately.
Case 1: Suppose $k > 0$.
Since $k \in \mathbb{Z}$ and $k > 0$, then k is a positive integer.
Since the product of positive integers is positive and n is a positive integer and k is a positive integer, then the product nk is a positive integer, so $nk > 0$.
Therefore, $nk \neq 0$.
Case 1: Suppose $k < 0$.
Since $k \in \mathbb{Z}$ and $k < 0$, then k is a negative integer.
Since the product of a positive integer and a negative integer is negative and n is a positive integer and k is a negative integer, then the product nk is negative, so $nk < 0$.
Therefore, $nk \neq 0$.
Hence, in all cases, $nk \neq 0$.

Thus, if $k \in \mathbb{Z}^*$, then $nk \neq 0$ for all $n \in \mathbb{Z}^+$, so if $k \in \mathbb{Z}^*$, then there is no $n \in \mathbb{Z}^+$ such that $nk = 0$.
Therefore, if $k \in \mathbb{Z}^*$, then k has infinite order.

Examples of cyclic subgroups generated by each non-zero integer are shown below.
$\langle 1 \rangle = \mathbb{Z}$ and 1 has infinite order
$\langle 2 \rangle = 2\mathbb{Z}$ and 2 has infinite order
$\langle 3 \rangle = 3\mathbb{Z}$ and 3 has infinite order
$\langle -1 \rangle = \mathbb{Z}$ and -1 has infinite order
$\langle -2 \rangle = 2\mathbb{Z}$ and -2 has infinite order
$\langle -3 \rangle = 3\mathbb{Z}$ and -3 has infinite order
Observe that $\mathbb{Z}$ is a cyclic group with generators 1 and -1.

The order of the inverse of an element is the same as the order of the element.
$|0| = |-0| = 1$
$|1| = |-1| = \infty$
$|2| = |-2| = \infty$
$|3| = |-3| = \infty$ $\square$

Exercise 14. Analyze the order of the cyclic group $(\mathbb{Z}_4, +)$.

Solution. Observe that $\mathbb{Z}_4$ is the group of integers modulo 4 under addition modulo 4.
The integers modulo 4 is $\{0, 1, 2, ..., 3\}$ and $|\mathbb{Z}_4| = 4$.

The Cayley table is below.

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

Every element of a group G generates a cyclic subgroup of G, so every element of $\mathbb{Z}_4$ generates a cyclic subgroup of $\mathbb{Z}_4$.
The cyclic subgroup generated by $a \in \mathbb{Z}_4$ is the same as the cyclic subgroup generated by a^{-1}, so we only need to consider the subgroups generated by $4/2 = 2$ elements and the identity 0.
The elements and additive inverses are:
$(0, 0), (1, 3), (2, 2), (3, 1)$
So, we consider the first 2 elements and the identity 0.

Since $\mathbb{Z}_4$ is a cyclic group of order 4, then $\mathbb{Z}_4$ is a finite cyclic group, so the number of generators is $\phi(4) = 2$ and the generators of $(\mathbb{Z}_4, +)$ are positive integers that are relatively prime to the modulus 4.
Therefore, the generators are positive integers a such that $\gcd(a, 4) = 1$.
The set of all generators of $\mathbb{Z}_4$ is $\{1, 3\}$.
Let $S = \{0, 1, 2\}$ and $T = \{1\}$.
Then $S - T = \{0, 2\}$ is the set of elements whose cyclic subgroups we need to consider and $|S - T| = 2$.

The cyclic subgroup generated by 0 is
$\langle 0 \rangle = \{0k : k \in \mathbb{Z}\} = \{0\}$.
The order of 0 is $|0| = 1$ since $1 \cdot 0 \equiv 0 \pmod 4$.

The cyclic subgroup generated by 2 is
$\langle 2 \rangle = \{2k : k \in \mathbb{Z}\} = \{0, 2\}$.
The order of 2 is $|2| = 2$ since $2 \cdot 2 \equiv 0 \pmod 4$.

The order of the inverse of an element is the same as the order of the element.
$|0| = |-0| = |0| = 1$
$|1| = |-1| = |3| = 4$
$|2| = |-2| = |2| = 2$
$|3| = |-3| = |1| = 4$

The subgroups of $(\mathbb{Z}_4, +)$ are:
$\mathbb{Z}_4 = \{0, 1, 2, 3\}$
$\{0, 2\}$
$\{0\}$

$\square$

Exercise 15. The group $(\mathbb{Z}_6, +)$ is a cyclic group.

Solution. The Cayley table is shown below.

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

Every element of a group G generates a cyclic subgroup of G, so every element of $\mathbb{Z}_6$ generates a cyclic subgroup of $\mathbb{Z}_6$.

The cyclic subgroup generated by $a \in \mathbb{Z}_6$ is the same as the cyclic subgroup generated by a^{-1}, so we only need to consider the subgroups generated by $6/2 = 3$ elements and the identity 0.

The elements and additive inverses are:
$(0, 0), (1, 5), (2, 4), (3, 3), (4, 2), (5, 1)$
So, we consider the first 6 elements and the identity 0.

Since $\mathbb{Z}_6$ is a cyclic group of order 6, then $\mathbb{Z}_6$ is a finite cyclic group, so the number of generators is $\phi(6) = 2$ and the generators of $(\mathbb{Z}_6, +)$ are positive integers that are relatively prime to the modulus 6.

Therefore, the generators are positive integers a such that $\gcd(a, 6) = 1$.
The set of all generators of $\mathbb{Z}_6$ is $\{1, 5\}$.
Let $S = \{0, 1, 2, 3\}$ and $T = \{1\}$.
Then $S - T = \{0, 2, 3\}$ is the set of elements whose cyclic subgroups we need to consider and $|S - T| = 3$.

The cyclic subgroup generated by 0 is
$\langle 0 \rangle = \{0k : k \in \mathbb{Z}\} = \{0\}$.
The order of 0 is $|0| = 1$ since $1 \cdot 0 \equiv 0 \pmod{6}$.

The cyclic subgroup generated by 2 is
$\langle 2\rangle = \{2k : k \in \mathbb{Z}\} = \{0, 2, 4\}$.
The order of 2 is $|2| = 3$ since $3 \cdot 2 \cdot 0 \equiv 0 \pmod 6$.

The cyclic subgroup generated by 3 is
$\langle 3\rangle = \{3k : k \in \mathbb{Z}\} = \{0, 3\}$.
The order of 3 is $|3| = 2$ since $2 \cdot 3 \cdot 0 \equiv 0 \pmod 6$.

The subgroups of $(\mathbb{Z}_6, +)$ are:
$\mathbb{Z}_6$
$\{0, 2, 4\}$
$\{0, 3\}$
$\{0\}$

$\square$

Exercise 16. The group $(\mathbb{Z}_{10}, +)$ is a cyclic group.

Solution. The Cayley table is shown below.

$+$	0	1	2	3	4	5	6	7	8	9
0	0	1	2	3	4	5	6	7	8	9
1	1	2	3	4	5	6	7	8	9	0
2	2	3	4	5	6	7	8	9	0	1
3	3	4	5	6	7	8	9	0	1	2
4	4	5	6	7	8	9	0	1	2	3
5	5	6	7	8	9	0	1	2	3	4
6	6	7	8	9	0	1	2	3	4	5
7	7	8	9	0	1	2	3	4	5	6
8	8	9	0	1	2	3	4	5	6	7
9	9	0	1	2	3	4	5	6	7	8

Every element of a group G generates a cyclic subgroup of G, so every element of $\mathbb{Z}_{10}$ generates a cyclic subgroup of $\mathbb{Z}_{10}$.

The cyclic subgroup generated by $a \in \mathbb{Z}_{10}$ is the same as the cyclic subgroup generated by a^{-1}, so we only need to consider the subgroups generated by $10/2 = 5$ elements and the identity 0.

The elements and additive inverses are:
$(0, 0), (1, 9), (2, 8), (3, 7), (4, 6), (5, 5), (6, 4), (7, 3), (8, 2), (9, 1)$
So, we consider the first 5 elements and the identity 0.

Since $\mathbb{Z}_{10}$ is a cyclic group of order 10, then $\mathbb{Z}_{10}$ is a finite cyclic group, so the number of generators is $\phi(10) = 4$ and the generators of $(\mathbb{Z}_{10}, +)$ are positive integers that are relatively prime to the modulus 10.

Therefore, the generators are positive integers a such that $\gcd(a, 10) = 1$.
The set of all generators of $\mathbb{Z}_{10}$ is $\{1, 3, 7, 9\}$.
Let $S = \{0, 1, 2, 3, ..., 5\}$ and $T = \{1, 3\}$.

Then $S - T = \{0, 2, 4, 5\}$ is the set of elements whose cyclic subgroups we need to consider and $|S - T| = 4$.

The cyclic subgroup generated by 0 is
$\langle 0 \rangle = \{0k : k \in \mathbb{Z}\} = \{0\}$.
The order of 0 is $|0| = 1$ since $1 \cdot 0 \equiv 0 \pmod{10}$.

The cyclic subgroup generated by 2 is
$\langle 2 \rangle = \{2k : k \in \mathbb{Z}\} = \{0, 2, 4, 6, 8\}$.
The order of 2 is $|2| = 5$ since $5 \cdot 2 \equiv 0 \pmod{10}$.

The cyclic subgroup generated by 4 is
$\langle 4 \rangle = \{4k : k \in \mathbb{Z}\} = \{0, 4, 8, 2, 6\}$.
The order of 4 is $|4| = 5$ since $5 \cdot 4 \equiv 0 \pmod{10}$.

The cyclic subgroup generated by 5 is
$\langle 5 \rangle = \{5k : k \in \mathbb{Z}\} = \{0, 5\}$.
The order of 5 is $|5| = 2$ since $2 \cdot 5 \equiv 0 \pmod{10}$.

The subgroups of $(\mathbb{Z}_{10}, +)$ are:
$\mathbb{Z}_{10}$
$\{0, 2, 4, 6, 8\}$
$\{0, 5\}$
$\{0\}$

$\square$

Exercise 17. The group $(\mathbb{Z}_{12}, +)$ is a cyclic group.

Solution. The Cayley table is shown below.

+	0	1	2	3	4	5	6	7	8	9	10	11
0	0	1	2	3	4	5	6	7	8	9	10	11
1	1	2	3	4	5	6	7	8	9	10	11	0
2	2	3	4	5	6	7	8	9	10	11	0	1
3	3	4	5	6	7	8	9	10	11	0	1	2
4	4	5	6	7	8	9	10	11	0	1	2	3
5	5	6	7	8	9	10	11	0	1	2	3	4
6	6	7	8	9	10	11	0	1	2	3	4	5
7	7	8	9	10	11	0	1	2	3	4	5	6
8	8	9	10	11	0	1	2	3	4	5	6	7
9	9	10	11	0	1	2	3	4	5	6	7	8
10	10	11	0	1	2	3	4	5	6	7	8	9
11	11	0	1	2	3	4	5	6	7	8	9	10

Every element of a group G generates a cyclic subgroup of G, so every element of $\mathbb{Z}_{12}$ generates a cyclic subgroup of $\mathbb{Z}_{12}$.

The cyclic subgroup generated by $a \in \mathbb{Z}_{12}$ is the same as the cyclic subgroup generated by a^{-1}, so we only need to consider the subgroups generated by $12/2 = 6$ elements and the identity 0.

The elements and additive inverses are:

$(0,0),(1,11),(2,10),(3,9),(4,8),(5,7),(6,6),(7,5),(8,4),(9,3),(10,2),(11,1)$

So, we consider the first 6 elements and the identity 0.

Since $\mathbb{Z}_{12}$ is a cyclic group of order 12, then $\mathbb{Z}_{12}$ is a finite cyclic group, so the number of generators is $\phi(12) = 4$ and the generators of $(\mathbb{Z}_{12}, +)$ are positive integers that are relatively prime to the modulus 12.

Therefore, the generators are positive integers a such that $\gcd(a, 12) = 1$.

The set of all generators of $\mathbb{Z}_{12}$ is $\{1, 5, 7, 11\}$.

Let $S = \{0, 1, 2, 3, ..., 6\}$ and $T = \{1, 5\}$.

Then $S - T = \{0, 2, 3, 4, 6\}$ is the set of elements whose cyclic subgroups we need to consider and $|S - T| = 5$.

The cyclic subgroup generated by 0 is

$\langle 0 \rangle = \{0k : k \in \mathbb{Z}\} = \{0\}$.

The order of 0 is $|0| = 1$ since $1 \cdot 0 \equiv 0 \pmod{12}$.

The cyclic subgroup generated by 2 is

$\langle 2 \rangle = \{2k : k \in \mathbb{Z}\} = \{0, 2, 4, 6, 8, 10\}$.

The order of 2 is $|2| = 6$ since $6 \cdot 2 \equiv 0 \pmod{12}$.

The cyclic subgroup generated by 3 is

$\langle 3 \rangle = \{3k : k \in \mathbb{Z}\} = \{0, 3, 6, 9\}$.

The order of 3 is $|3| = 4$ since $4 \cdot 3 \equiv 0 \pmod{12}$.

The cyclic subgroup generated by 4 is

$\langle 4 \rangle = \{4k : k \in \mathbb{Z}\} = \{0, 4, 8\}$.

The order of 4 is $|4| = 3$ since $3 \cdot 4 \equiv 0 \pmod{12}$.

The cyclic subgroup generated by 6 is

$\langle 6 \rangle = \{6k : k \in \mathbb{Z}\} = \{0, 6\}$.

The order of 6 is $|6| = 2$ since $2 \cdot 6 \equiv 0 \pmod{12}$.

The subgroups of $(\mathbb{Z}_{12}, +)$ are:

$\mathbb{Z}_{12} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$

$\{0, 2, 4, 6, 8, 10\}$

$\{0, 3, 6, 9\}$

$\{0, 4, 8\}$

$\{0, 6\}$

$\{0\}$

□

Exercise 18. The group $(\mathbb{Z}_{13}, +)$ is a cyclic group.

Solution. The Cayley table is shown below.

+	0	1	2	3	4	5	6	7	8	9	10	11	12
0	0	1	2	3	4	5	6	7	8	9	10	11	0
1	1	2	3	4	5	6	7	8	9	10	11	0	1
2	2	3	4	5	6	7	8	9	10	11	0	1	2
3	3	4	5	6	7	8	9	10	11	0	1	2	3
4	4	5	6	7	8	9	10	11	0	1	2	3	4
5	5	6	7	8	9	10	11	0	1	2	3	4	5
6	6	7	8	9	10	11	0	1	2	3	4	5	6
7	7	8	9	10	11	0	1	2	3	4	5	6	7
8	8	9	10	11	0	1	2	3	4	5	6	7	8
9	9	10	11	0	1	2	3	4	5	6	7	8	9
10	10	11	0	1	2	3	4	5	6	7	8	9	10
11	11	0	1	2	3	4	5	6	7	8	9	10	11
12	11	0	1	2	3	4	5	6	7	8	9	10	12

Every element of a group G generates a cyclic subgroup of G, so every element of $\mathbb{Z}_{13}$ generates a cyclic subgroup of $\mathbb{Z}_{13}$.

The cyclic subgroup generated by $a \in \mathbb{Z}_{13}$ is the same as the cyclic subgroup generated by a^{-1}, so we only need to consider the subgroups generated by $13/2 = 6$ elements and the identity 0.

The elements and additive inverses are:

$(0,0),(1,12),(2,11),(3,10),(4,9),(5,8),(6,7),(7,6),(8,5),(9,4),(10,3),(11,2),(12,1)$

So, we consider the first 6 elements and the identity 0.

Since $\mathbb{Z}_{13}$ is a cyclic group of order 13, then $\mathbb{Z}_{13}$ is a finite cyclic group, so the number of generators is $\phi(13) = 12$ and the generators of $(\mathbb{Z}_{13}, +)$ are positive integers that are relatively prime to the modulus 13.

Therefore, the generators are positive integers a such that $\gcd(a, 13) = 1$.

The set of all generators of $\mathbb{Z}_{13}$ is $\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$.

Let $S = \{0, 1, 2, 3, ..., 6\}$ and $T = \{1, 2, 3, 4, 5, 6\}$.

Then $S - T = \{0\}$ is the set of elements whose cyclic subgroups we need to consider and $|S - T| = 1$.

The cyclic subgroup generated by 0 is

$\langle 0 \rangle = \{0k : k \in \mathbb{Z}\} = \{0\}$.

The order of 0 is $|0| = 1$ since $1 \cdot 0 \equiv 0 \pmod{13}$.

The subgroups of $(\mathbb{Z}_{13}, +)$ are:
$\mathbb{Z}_{13}$
$\{0\}$
Observe that $\mathbb{Z}_{13}$ has no nontrivial proper subgroups. The only subgroups are $\mathbb{Z}_{13}$ itself and the trivial group. $\square$

Exercise 19. The group $(\mathbb{Z}_{16}, +)$ is a cyclic group.

Solution. The Cayley table is shown below.

+	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	0
2	2	3	4	5	6	7	8	9	10	11	12	13	14	15	0	1
3	3	4	5	6	7	8	9	10	11	12	13	14	15	0	1	2
4	4	5	6	7	8	9	10	11	12	13	14	15	0	1	2	3
5	5	6	7	8	9	10	11	12	13	14	15	0	1	2	3	4
6	6	7	8	9	10	11	12	13	14	15	0	1	2	3	4	5
7	7	8	9	10	11	12	13	14	15	0	1	2	3	4	5	6
8	8	9	10	11	12	13	14	15	0	1	2	3	4	5	6	7
9	9	10	11	12	13	14	15	0	1	2	3	4	5	6	7	8
10	10	11	12	13	14	15	0	1	2	3	4	5	6	7	8	9
11	11	12	13	14	15	0	1	2	3	4	5	6	7	8	9	10
12	12	13	14	15	0	1	2	3	4	5	6	7	8	9	10	11
13	13	14	15	0	1	2	3	4	5	6	7	8	9	10	11	12
14	14	15	0	1	2	3	4	5	6	7	8	9	10	11	12	13
15	15	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14

Every element of a group G generates a cyclic subgroup of G, so every element of $\mathbb{Z}_{16}$ generates a cyclic subgroup of $\mathbb{Z}_{16}$.

The cyclic subgroup generated by $a \in \mathbb{Z}_{16}$ is the same as the cyclic subgroup generated by a^{-1}, so we only need to consider the subgroups generated by $16/2 = 8$ elements and the identity 0.

The elements and additive inverses are:
$(0,0), (1,15), (2,14), (3,13), (4,12), (5,11), (6,10), (7,9), (8,8)$
$(9,7), (10,6), (11,5), (12,4), (13,3), (14,2), (15,1)$
So, we consider the first 8 elements and the identity 0.

Since $\mathbb{Z}_{16}$ is a cyclic group of order 16, then $\mathbb{Z}_{16}$ is a finite cyclic group, so the number of generators is $\phi(16) = 8$ and the generators of $(\mathbb{Z}_{16}, +)$ are positive integers that are relatively prime to the modulus 16.

Therefore, the generators are positive integers a such that $\gcd(a, 16) = 1$.

The set of all generators of $\mathbb{Z}_{16}$ is $\{1, 3, 5, 7, 9, 11, 13, 15\}$.

Let $S = \{0, 1, 2, 3, ..., 8\}$ and $T = \{1, 3, 5, 7\}$.

Then $S - T = \{0, 2, 4, 6, 8\}$ is the set of elements whose cyclic subgroups we need to consider and $|S - T| = 5$.

The cyclic subgroup generated by 0 is
$\langle 0 \rangle = \{0k : k \in \mathbb{Z}\} = \{0\}$.
The order of 0 is $|0| = 1$ since $1 \cdot 0 \equiv 0 \pmod{16}$.

The cyclic subgroup generated by 2 is
$\langle 2 \rangle = \{2k : k \in \mathbb{Z}\} = \{0, 2, 4, 6, 8, 10, 12, 14\}$.
The order of 2 is $|2| = 8$ since $8 \cdot 2 \equiv 0 \pmod{16}$.

The cyclic subgroup generated by 4 is
$\langle 4 \rangle = \{4k : k \in \mathbb{Z}\} = \{0, 4, 8, 12\}$.
The order of 4 is $|4| = 4$ since $4 \cdot 4 \equiv 0 \pmod{16}$.

The cyclic subgroup generated by 6 is
$\langle 6 \rangle = \{6k : k \in \mathbb{Z}\} = \{0, 6, 12, 2, 8, 14, 4, 10\}$.
The order of 6 is $|6| = 8$ since $8 \cdot 6 \equiv 0 \pmod{16}$.

The cyclic subgroup generated by 8 is
$\langle 8 \rangle = \{8k : k \in \mathbb{Z}\} = \{0, 8\}$.
The order of 8 is $|8| = 2$ since $2 \cdot 8 \equiv 0 \pmod{16}$.

The subgroups of $(\mathbb{Z}_{16}, +)$ are:
$\mathbb{Z}_{16}$
$\{0, 2, 4, 6, 8, 10, 12, 14\}$
$\{0, 4, 8, 12\}$
$\{0, 8\}$
$\{0\}$

□

Exercise 20. Analyze the group $(\mathbb{Z}_{18}, +)$.

Solution. Every element of a group G generates a cyclic subgroup of G, so every element of $\mathbb{Z}_{18}$ generates a cyclic subgroup of $\mathbb{Z}_{18}$.

The cyclic subgroup generated by $a \in \mathbb{Z}_{18}$ is the same as the cyclic subgroup generated by a^{-1}, so we only need to consider the subgroups generated by $18/2 = 9$ elements and the identity 0.

The elements and additive inverses are:
$(0, 0), (1, 17), (2, 16), (3, 15), (4, 14), (5, 13), (6, 12), (7, 11), (8, 10), (9, 9), (10, 8), (11, 7), (12, 6), (13, 5)$
$(14, 4), (15, 3), (16, 2), (17, 1)$
So, we consider the first 9 elements and the identity 0.

Since $\mathbb{Z}_{18}$ is a cyclic group of order 18, then $\mathbb{Z}_{18}$ is a finite cyclic group, so the number of generators is $\phi(18) = 6$ and the generators of $(\mathbb{Z}_{18}, +)$ are positive integers that are relatively prime to the modulus 18.

Therefore, the generators are positive integers a such that $\gcd(a, 18) = 1$.
The set of all generators of $\mathbb{Z}_{18}$ is $\{1, 5, 7, 11, 13, 17\}$.

Let $S = \{0, 1, 2, 3, ..., 9\}$ and $T = \{1, 5, 7\}$.

Then $S - T = \{0, 2, 3, 4, 6, 8, 9\}$ is the set of elements whose cyclic subgroups we need to consider and $|S - T| = 7$.

The cyclic subgroup generated by 0 is
$\langle 0 \rangle = \{0k : k \in \mathbb{Z}\} = \{0\}$.
The order of 0 is $|0| = 1$ since $1 \cdot 0 \equiv 0 \pmod{18}$.

The cyclic subgroup generated by 2 is
$\langle 2 \rangle = \{2k : k \in \mathbb{Z}\} = \{0, 2, 4, 6, 8, 10, 12, 14, 16\}$.
The order of 2 is $|2| = 9$ since $9 \cdot 2 \equiv 0 \pmod{18}$.

The cyclic subgroup generated by 3 is
$\langle 3 \rangle = \{3k : k \in \mathbb{Z}\} = \{0, 3, 6, 9, 12, 15\}$.
The order of 3 is $|3| = 16$ since $16 \cdot 3 \equiv 0 \pmod{18}$.

The cyclic subgroup generated by 4 is
$\langle 4 \rangle = \{4k : k \in \mathbb{Z}\} = \{0, 2, 4, 6, 8, 10, 12, 14, 16\}$.
The order of 4 is $|4| = 9$ since $9 \cdot 4 \equiv 0 \pmod{18}$.

The cyclic subgroup generated by 6 is
$\langle 6 \rangle = \{6k : k \in \mathbb{Z}\} = \{0, 6, 12\}$.
The order of 6 is $|6| = 3$ since $3 \cdot 6 \equiv 0 \pmod{18}$.

The cyclic subgroup generated by 8 is
$\langle 8 \rangle = \{8k : k \in \mathbb{Z}\} = \{0, 2, 4, 6, 8, 10, 12, 14, 16\}$.
The order of 8 is $|8| = 9$ since $9 \cdot 8 \equiv 0 \pmod{18}$.

The cyclic subgroup generated by 9 is
$\langle 9 \rangle = \{9k : k \in \mathbb{Z}\} = \{0, 9\}$.
The order of 9 is $|9| = 2$ since $2 \cdot 9 \equiv 0 \pmod{18}$.

The subgroups of $(\mathbb{Z}_{18}, +)$ are:
$\mathbb{Z}_{18}$
$\{0, 2, 4, 6, 8, 10, 12, 14, 16\}$
$\{0, 3, 6, 9, 12, 15\}$
$\{0, 6, 12\}$
$\{0, 9\}$
$\{0\}$

□

Exercise 21. Analyze the group $(\mathbb{Z}_{32}, +)$.

Solution. Every element of a group G generates a cyclic subgroup of G, so every element of $\mathbb{Z}_{32}$ generates a cyclic subgroup of $\mathbb{Z}_{32}$.

The cyclic subgroup generated by $a \in \mathbb{Z}_{32}$ is the same as the cyclic subgroup generated by a^{-1}, so we only need to consider the subgroups generated by $32/2 = 16$ elements and the identity 0.

The elements and additive inverses are:

$(0,0),(1,31),(2,30),(3,29),(4,28),(5,27),(6,26),(7,25),(8,24),(9,23),(10,22),(11,21),(12,20),(13,19)$

$(14,18),(15,17),(16,16),(17,15),(18,14),(19,13),(20,12)$

$(21,11),(22,10),(23,9),(24,8),(25,7),(26,6),(27,5),(28,4),(29,3),(30,2),(31,1)$

So, we consider the first 16 elements and the identity 0.

Since $\mathbb{Z}_{32}$ is a cyclic group of order 32, then $\mathbb{Z}_{32}$ is a finite cyclic group, so the number of generators is $\phi(32) = 16$ and the generators of $(\mathbb{Z}_{32}, +)$ are positive integers that are relatively prime to the modulus 32.

Therefore, the generators are positive integers a such that $\gcd(a, 32) = 1$.

The set of all generators of $\mathbb{Z}_{32}$ is $\{1,3,5,7,9,11,13,15,17,19,21,23,25,27,29,31\}$.

Let $S = \{0,1,2,3,...,16\}$ and $T = \{1,3,5,7,9,11,13,15\}$.

Then $S - T = \{0,2,4,6,8,10,12,14,16\}$ is the set of elements whose cyclic subgroups we need to consider and $|S - T| = 9$.

The cyclic subgroup generated by 0 is

$\langle 0 \rangle = \{0k : k \in \mathbb{Z}\} = \{0\}$.

The order of 0 is $|0| = 1$ since $1 \cdot 0 \equiv 0 \pmod{32}$.

The cyclic subgroup generated by 2 is

$\langle 2 \rangle = \{2k : k \in \mathbb{Z}\} = \{0,2,4,6,8,10,12,14,16,18,20,22,24,26,28,30\}$.

The order of 2 is $|2| = 16$ since $16 \cdot 2 \equiv 0 \pmod{32}$.

The cyclic subgroup generated by 4 is

$\langle 4 \rangle = \{4k : k \in \mathbb{Z}\} = \{0,4,8,12,16,20,24,28\}$.

The order of 4 is $|4| = 8$ since $8 \cdot 4 \equiv 0 \pmod{32}$.

The cyclic subgroup generated by 6 is

$\langle 6 \rangle = \{6k : k \in \mathbb{Z}\} = \{0,2,4,6,8,10,12,14,16,18,20,22,24,26,28,30\}$.

The order of 6 is $|6| = 16$ since $16 \cdot 6 \equiv 0 \pmod{32}$.

The cyclic subgroup generated by 8 is

$\langle 8 \rangle = \{8k : k \in \mathbb{Z}\} = \{0,8,16,24\}$.

The order of 8 is $|8| = 4$ since $4 \cdot 8 \equiv 0 \pmod{32}$.

The cyclic subgroup generated by 10 is

$\langle 10 \rangle = \{10k : k \in \mathbb{Z}\} = \{0,2,4,6,8,10,12,14,16,18,20,22,24,26,28,30\}$.

The order of 10 is $|10| = 16$ since $16 \cdot 10 \equiv 0 \pmod{32}$.

The cyclic subgroup generated by 12 is
$\langle 12\rangle = \{12k : k \in \mathbb{Z}\} = \{0, 4, 8, 12, 16, 20, 24, 28\}$.
The order of 12 is $|12| = 8$ since $8 \cdot 12 \equiv 0 \pmod{32}$.

The cyclic subgroup generated by 14 is
$\langle 14\rangle = \{14k : k \in \mathbb{Z}\} = \{0, 2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30\}$.
The order of 14 is $|14| = 16$ since $16 \cdot 14 \equiv 0 \pmod{32}$.

The cyclic subgroup generated by 16 is
$\langle 16\rangle = \{16k : k \in \mathbb{Z}\} = \{0, 16\}$.
The order of 16 is $|16| = 2$ since $2 \cdot 16 \equiv 0 \pmod{32}$.

The subgroups of $(\mathbb{Z}_{32}, +)$ are:
$\mathbb{Z}_{32}$
$\{0, 2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30\}$
$\{0, 4, 8, 12, 16, 20, 24, 28\}$
$\{0, 8, 16, 24\}$
$\{0, 16\}$
$\{0\}$

$\square$

Exercise 22. The group $(\mathbb{Z}_{48}, +)$ is a cyclic group.

Solution. Every element of a group G generates a cyclic subgroup of G, so every element of $\mathbb{Z}_{48}$ generates a cyclic subgroup of $\mathbb{Z}_{48}$.

The cyclic subgroup generated by $a \in \mathbb{Z}_{48}$ is the same as the cyclic subgroup generated by a^{-1}, so we only need to consider the subgroups generated by $48/2 = 24$ elements and the identity 0.

The elements and additive inverses are:
$(0, 0), (1, 47), (2, 46), (3, 45), (4, 44), (5, 43), (6, 42), (7, 41), (8, 40), (9, 39), (10, 38), (11, 37), (12, 36), (13, 35)$
$(14, 34), (15, 33), (16, 32), (17, 31), (18, 30), (19, 29), (20, 28), (21, 27), (22, 26), (23, 25), (24, 24)$
So, we consider the first 24 elements and the identity 0.

Since $\mathbb{Z}_{48}$ is a cyclic group of order 48, then $\mathbb{Z}_{48}$ is a finite cyclic group, so the number of generators is $\phi(48) = 16$ and the generators of $(\mathbb{Z}_{48}, +)$ are positive integers that are relatively prime to the modulus 48.

Therefore, the generators are positive integers a such that $\gcd(a, 48) = 1$.

The set of all generators of $\mathbb{Z}_{48}$ is $\{1, 5, 7, 11, 13, 17, 19, 23, 25, 29, 31, 35, 37, 41, 43, 47\}$.

Let $S = \{0, 1, 2, 3, ..., 24\}$ and $T = \{1, 5, 7, 11, 13, 17, 19, 23\}$.

Then $S - T = \{0, 2, 3, 4, 6, 8, 9, 10, 12, 14, 15, 16, 18, 20, 21, 22, 24\}$ is the set of elements whose cyclic subgroups we need to consider and $|S - T| = 17$.

The cyclic subgroup generated by 0 is
$\langle 0\rangle = \{0k : k \in \mathbb{Z}\} = \{0\}$.
The order of 0 is $|0| = 1$ since $1 \cdot 0 \equiv 0 \pmod{48}$.

The cyclic subgroup generated by 2 is
$\langle 2\rangle = \{2k : k \in \mathbb{Z}\} = \{0, 2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46\}$.
The order of 2 is $|2| = 24$ since $24 \cdot 2 \equiv 0 \pmod{48}$.

The cyclic subgroup generated by 3 is
$\langle 3\rangle = \{3k : k \in \mathbb{Z}\} = \{0, 3, 6, 9, 12, 15, 18, 21, 24, 27, 30, 33, 36, 39, 42, 45\}$.
The order of 3 is $|3| = 16$ since $16 \cdot 3 \equiv 0 \pmod{48}$.

The cyclic subgroup generated by 4 is
$\langle 4\rangle = \{4k : k \in \mathbb{Z}\} = \{0, 4, 8, 12, 16, 20, 24, 28, 32, 36, 40, 44\}$.
The order of 4 is $|4| = 12$ since $12 \cdot 4 \equiv 0 \pmod{48}$.

The cyclic subgroup generated by 6 is
$\langle 6\rangle = \{6k : k \in \mathbb{Z}\} = \{0, 6, 12, 18, 24, 30, 36, 42\}$.
The order of 6 is $|6| = 8$ since $8 \cdot 6 \equiv 0 \pmod{48}$.

The cyclic subgroup generated by 8 is
$\langle 8\rangle = \{8k : k \in \mathbb{Z}\} = \{0, 8, 16, 24, 32, 40\}$.
The order of 8 is $|8| = 6$ since $6 \cdot 8 \equiv 0 \pmod{48}$.

The cyclic subgroup generated by 9 is
$\langle 9\rangle = \{9k : k \in \mathbb{Z}\} = \{0, 3, 6, 9, 12, 15, 18, 21, 24, 27, 30, 33, 36, 39, 42, 45\}$.
The order of 9 is $|9| = 16$ since $16 \cdot 9 \equiv 0 \pmod{48}$.

The cyclic subgroup generated by 10 is
$\langle 10\rangle = \{10k : k \in \mathbb{Z}\} = \{0, 2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46\}$.
The order of 10 is $|10| = 24$ since $24 \cdot 10 \equiv 0 \pmod{48}$.

The cyclic subgroup generated by 12 is
$\langle 12\rangle = \{12k : k \in \mathbb{Z}\} = \{0, 12, 24, 36\}$.
The order of 12 is $|12| = 4$ since $4 \cdot 12 \equiv 0 \pmod{48}$.

The cyclic subgroup generated by 14 is
$\langle 14\rangle = \{14k : k \in \mathbb{Z}\} = \{0, 2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46\}$.
The order of 14 is $|14| = 24$ since $24 \cdot 14 \equiv 0 \pmod{48}$.

The cyclic subgroup generated by 15 is
$\langle 15\rangle = \{15k : k \in \mathbb{Z}\} = \{0, 3, 6, 9, 12, 15, 18, 21, 24, 27, 30, 33, 36, 39, 42, 45\}$.
The order of 15 is $|15| = 16$ since $16 \cdot 15 \equiv 0 \pmod{48}$.

The cyclic subgroup generated by 16 is
$\langle 16\rangle = \{16k : k \in \mathbb{Z}\} = \{0, 16, 32\}$.
The order of 16 is $|16| = 3$ since $3 \cdot 16 \equiv 0 \pmod{48}$.

The cyclic subgroup generated by 18 is
$\langle 18 \rangle = \{18k : k \in \mathbb{Z}\} = \{0, 6, 12, 18, 24, 30, 36, 42\}$.
The order of 18 is $|18| = 8$ since $8 \cdot 18 \equiv 0 \pmod{48}$.

The cyclic subgroup generated by 20 is
$\langle 20 \rangle = \{20k : k \in \mathbb{Z}\} = \{0, 4, 8, 12, 16, 20, 24, 28, 32, 36, 40, 44\}$.
The order of 20 is $|20| = 12$ since $12 \cdot 20 \equiv 0 \pmod{48}$.

The cyclic subgroup generated by 21 is
$\langle 21 \rangle = \{21k : k \in \mathbb{Z}\} = \{0, 3, 6, 9, 12, 15, 18, 21, 24, 27, 30, 33, 36, 39, 42, 45\}$.
The order of 21 is $|21| = 16$ since $16 \cdot 21 \equiv 0 \pmod{48}$.

The cyclic subgroup generated by 22 is
$\langle 22 \rangle = \{22k : k \in \mathbb{Z}\} = \{0, 2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46\}$.
The order of 22 is $|22| = 24$ since $24 \cdot 22 \equiv 0 \pmod{48}$.

The cyclic subgroup generated by 24 is
$\langle 24 \rangle = \{24k : k \in \mathbb{Z}\} = \{0, 24\}$.
The order of 24 is $|24| = 2$ since $2 \cdot 24 \equiv 0 \pmod{48}$.

The subgroups of $(\mathbb{Z}_{48}, +)$ are:
$\mathbb{Z}_{48}$
$\{0, 2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46\}$
$\{0, 3, 6, 9, 12, 15, 18, 21, 24, 27, 30, 33, 36, 39, 42, 45\}$
$\{0, 4, 8, 12, 16, 20, 24, 28, 32, 36, 40, 44\}$
$\{0, 6, 12, 18, 24, 30, 36, 42\}$
$\{0, 8, 16, 24, 32, 40\}$
$\{0, 12, 24, 36\}$
$\{0, 16, 32\}$
$\{0, 24\}$
$\{0\}$

□

Exercise 23. The group $(\mathbb{Z}_{60}, +)$ is a cyclic group.

Solution. Every element of a group G generates a cyclic subgroup of G, so every element of $\mathbb{Z}_{60}$ generates a cyclic subgroup of $\mathbb{Z}_{60}$.

The cyclic subgroup generated by $a \in \mathbb{Z}_{60}$ is the same as the cyclic subgroup generated by a^{-1}, so we only need to consider the subgroups generated by $60/2 = 30$ elements and the identity 0.

The elements and additive inverses are:
$(0, 0), (1, 59), (2, 58), (3, 57), (4, 56), (5, 55), (6, 54), (7, 53), (8, 52), (9, 51), (10, 50), (11, 49), (12, 48), (13, 47)$
$(14, 46), (15, 45), (16, 44), (17, 43), (18, 42), (19, 41), (20, 40), (21, 39), (22, 38), (23, 37), (24, 36), (25, 35)$
$(24, 34), (25, 33), (26, 32), (27, 31), (28, 30), (29, 31), (30, 30)$
So, we consider the first 30 elements and the identity 0.

Since $\mathbb{Z}_{60}$ is a cyclic group of order 60, then $\mathbb{Z}_{60}$ is a finite cyclic group, so the number of generators is $\phi(60) = 16$ and the generators of $(\mathbb{Z}_{60}, +)$ are positive integers that are relatively prime to the modulus 60.

Therefore, the generators are positive integers a such that $\gcd(a, 60) = 1$.

The set of all generators of $\mathbb{Z}_{60}$ is $\{1, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 49, 53, 59\}$.

Let $S = \{0, 1, 2, 3, ..., 30\}$ and $T = \{1, 7, 11, 13, 17, 19, 23, 29\}$.

Then $S-T = \{0, 2, 3, 4, 5, 6, 8, 9, 10, 12, 14, 15, 16, 18, 20, 21, 22, 24, 25, 26, 27, 28, 30\}$ is the set of elements whose cyclic subgroups we need to consider and $|S - T| = 23$.

The cyclic subgroup generated by 0 is
$\langle 0 \rangle = \{0k : k \in \mathbb{Z}\} = \{0\}$.
The order of 0 is $|0| = 1$ since $1 \cdot 0 \equiv 0 \pmod{60}$.

The cyclic subgroup generated by 2 is
$\langle 2 \rangle = \{2k : k \in \mathbb{Z}\} =$
$\{0, 2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58\}$.
The order of 2 is $|2| = 30$ since $30 \cdot 2 \equiv 0 \pmod{60}$.

The cyclic subgroup generated by 3 is
$\langle 3 \rangle = \{3k : k \in \mathbb{Z}\} = \{0, 3, 6, 9, 12, 15, 18, 21, 24, 27, 30, 33, 36, 39, 42, 45, 48, 51, 54, 57\}$.
The order of 3 is $|3| = 20$ since $20 \cdot 3 \equiv 0 \pmod{60}$.

The cyclic subgroup generated by 4 is
$\langle 4 \rangle = \{4k : k \in \mathbb{Z}\} = \{0, 4, 8, 12, 16, 20, 24, 28, 32, 36, 40, 44, 48, 52, 56\}$.
The order of 4 is $|4| = 15$ since $15 \cdot 4 \equiv 0 \pmod{60}$.

The cyclic subgroup generated by 5 is
$\langle 5 \rangle = \{5k : k \in \mathbb{Z}\} = \{0, 5, 10, 15, 20, 25, 30, 35, 40, 45, 50, 55\}$.
The order of 5 is $|5| = 12$ since $12 \cdot 5 \equiv 0 \pmod{60}$.

The cyclic subgroup generated by 6 is
$\langle 6 \rangle = \{6k : k \in \mathbb{Z}\} = \{0, 6, 12, 18, 24, 30, 36, 42, 48, 54\}$.
The order of 6 is $|6| = 10$ since $10 \cdot 6 \equiv 0 \pmod{60}$.

The cyclic subgroup generated by 8 is
$\langle 8 \rangle = \{8k : k \in \mathbb{Z}\} = \{0, 4, 8, 12, 16, 20, 24, 28, 32, 36, 40, 44, 48, 52, 56\}$.
The order of 8 is $|8| = 15$ since $15 \cdot 8 \equiv 0 \pmod{60}$.

The cyclic subgroup generated by 9 is
$\langle 9 \rangle = \{9k : k \in \mathbb{Z}\} = \{0, 3, 6, 9, 12, 15, 18, 21, 24, 27, 30, 33, 36, 39, 42, 45, 48, 51, 54, 57\}$.
The order of 9 is $|9| = 20$ since $20 \cdot 9 \equiv 0 \pmod{60}$.

The cyclic subgroup generated by 10 is
$\langle 10\rangle = \{10k : k \in \mathbb{Z}\} = \{0, 10, 20, 30, 40, 50\}$.
The order of 10 is $|10| = 6$ since $6 \cdot 10 \equiv 0 \pmod{60}$.

The cyclic subgroup generated by 12 is
$\langle 12\rangle = \{12k : k \in \mathbb{Z}\} = \{0, 12, 24, 36, 48\}$.
The order of 12 is $|12| = 5$ since $5 \cdot 12 \equiv 0 \pmod{60}$.

The cyclic subgroup generated by 14 is
$\langle 14\rangle = \{14k : k \in \mathbb{Z}\} =$
$\{0, 2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58\}$.
The order of 14 is $|14| = 30$ since $30 \cdot 14 \equiv 0 \pmod{60}$.

The cyclic subgroup generated by 15 is
$\langle 15\rangle = \{15k : k \in \mathbb{Z}\} = \{0, 15, 30, 45\}$.
The order of 15 is $|15| = 4$ since $4 \cdot 15 \equiv 0 \pmod{60}$.

The cyclic subgroup generated by 16 is
$\langle 16\rangle = \{16k : k \in \mathbb{Z}\} = \{0, 4, 8, 12, 16, 20, 24, 28, 32, 36, 40, 44, 48, 52, 56\}$.
The order of 16 is $|16| = 15$ since $15 \cdot 16 \equiv 0 \pmod{60}$.

The cyclic subgroup generated by 18 is
$\langle 18\rangle = \{18k : k \in \mathbb{Z}\} = \{0, 6, 12, 18, 24, 30, 36, 42, 48, 54\}$.
The order of 18 is $|18| = 10$ since $10 \cdot 18 \equiv 0 \pmod{60}$.

The cyclic subgroup generated by 20 is
$\langle 20\rangle = \{20k : k \in \mathbb{Z}\} = \{0, 20, 40\}$.
The order of 20 is $|20| = 3$ since $3 \cdot 20 \equiv 0 \pmod{60}$.

The cyclic subgroup generated by 21 is
$\langle 21\rangle = \{21k : k \in \mathbb{Z}\} = \{0, 3, 6, 9, 12, 15, 18, 21, 24, 27, 30, 33, 36, 39, 42, 45, 48, 51, 54, 57\}$.
The order of 21 is $|21| = 20$ since $20 \cdot 21 \equiv 0 \pmod{60}$.

The cyclic subgroup generated by 22 is
$\langle 22\rangle = \{22k : k \in \mathbb{Z}\} =$
$\{0, 2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58\}$.
The order of 22 is $|22| = 30$ since $30 \cdot 22 \equiv 0 \pmod{60}$.

The cyclic subgroup generated by 24 is
$\langle 24\rangle = \{24k : k \in \mathbb{Z}\} = \{0, 12, 24, 36, 48\}$.
The order of 24 is $|24| = 5$ since $5 \cdot 24 \equiv 0 \pmod{60}$.

The cyclic subgroup generated by 25 is
$\langle 25\rangle = \{25k : k \in \mathbb{Z}\} = \{0, 5, 10, 15, 20, 25, 30, 35, 40, 45, 50, 55\}$.
The order of 25 is $|25| = 12$ since $12 \cdot 25 \equiv 0 \pmod{60}$.

The cyclic subgroup generated by 26 is
$\langle 26\rangle = \{26k : k \in \mathbb{Z}\} =$
$\{0, 2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58\}$.
The order of 26 is $|26| = 30$ since $30 \cdot 26 \equiv 0 \pmod{60}$.

The cyclic subgroup generated by 27 is
$\langle 27\rangle = \{27k : k \in \mathbb{Z}\} =$
$\{0, 3, 6, 9, 12, 15, 18, 21, 24, 27, 30, 33, 36, 39, 42, 45, 48, 51, 54, 57\}$.
The order of 27 is $|27| = 20$ since $20 \cdot 27 \equiv 0 \pmod{60}$.

The cyclic subgroup generated by 28 is
$\langle 28\rangle = \{28k : k \in \mathbb{Z}\} =$
$\{0, 4, 8, 12, 16, 20, 24, 28, 32, 36, 40, 44, 48, 52, 56\}$.
The order of 28 is $|28| = 15$ since $15 \cdot 28 \equiv 0 \pmod{60}$.

The cyclic subgroup generated by 30 is
$\langle 30\rangle = \{30k : k \in \mathbb{Z}\} = \{0, 30\}$.
The order of 30 is $|30| = 2$ since $2 \cdot 30 \equiv 0 \pmod{60}$.

The subgroups of $(\mathbb{Z}_{60}, +)$ are:
$\mathbb{Z}_{60}$
$\{0, 2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58\}$
$\{0, 3, 6, 9, 12, 15, 18, 21, 24, 27, 30, 33, 36, 39, 42, 45, 48, 51, 54, 57\}$
$\{0, 4, 8, 12, 16, 20, 24, 28, 32, 36, 40, 44, 48, 52, 56\}$
$\{0, 5, 10, 15, 20, 25, 30, 35, 40, 45, 50, 55\}$
$\{0, 6, 12, 18, 24, 30, 36, 42, 48, 54\}$
$\{0, 10, 20, 30, 40, 50\}$
$\{0, 12, 24, 36, 48\}$
$\{0, 15, 30, 45\}$
$\{0, 20, 40\}$
$\{0, 30\}$
$\{0\}$

$\square$

Exercise 24. Analyze the generators of $(\mathbb{Z}_{60}, +)$.

Solution. The generators of $(\mathbb{Z}_{60}, +)$ are congruence classes $[k]$ such that $k \in \mathbb{Z}^+$ and $\gcd(k, 60) = 1$.

Hence, there are $\phi(60) = 16$ elements of $\mathbb{Z}_{60}$ that are relatively prime to the modulus 60.

Therefore, the set of generators of $\mathbb{Z}_{60}$ is $\{1, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 49, 53, 59\}$.

$\square$

Exercise 25. Which elements of $(\mathbb{Z}_n, +)$ are generators of the cyclic group $\mathbb{Z}_n$?

Solution. For $n \in \mathbb{Z}^+$ and $n > 1$, the additive group $\mathbb{Z}_n = \{[0], [1], ..., [n-1]\} = \langle [1] \rangle$ is cyclic and the congruence class $[1]$ is a generator of $\mathbb{Z}_n$.

For $\mathbb{Z}_1$ the generator is 0, so $\mathbb{Z}_1 = \langle 0 \rangle = \{0\}$ is a cyclic group.

For $\mathbb{Z}_2$ the generator is 1, so $\mathbb{Z}_2 = \langle 1 \rangle = \{0, 1\}$ is a cyclic group.

For $\mathbb{Z}_3$ the generators are $1, 2$ so $\mathbb{Z}_3 = \langle 1 \rangle = \langle 2 \rangle = \{0, 1, 2\}$ is a cyclic group.

For $\mathbb{Z}_4$ the generators are $1, 3$ so $\mathbb{Z}_4 = \langle 1 \rangle = \langle 3 \rangle = \{0, 1, 2, 3\}$ is a cyclic group.

For $\mathbb{Z}_5$ the generators are $1, 2, 3, 4$, so $\mathbb{Z}_5 = \langle 1 \rangle = \langle 2 \rangle = \langle 3 \rangle = \langle 4 \rangle = \{0, 1, 2, 3, 4\}$ is a cyclic group.

For $\mathbb{Z}_6$ the generators are $1, 5$ so $\mathbb{Z}_6 = \langle 1 \rangle = \langle 5 \rangle = \{0, 1, 2, 3, 4, 5\}$ is a cyclic group.

For $\mathbb{Z}_7$ the generators are $1, 2, 3, 4, 5, 6$, so $\mathbb{Z}_7 = \langle 1 \rangle = \langle 2 \rangle = \langle 3 \rangle = \langle 4 \rangle = \langle 5 \rangle = \langle 6 \rangle = \{0, 1, 2, 3, 4, 5\}$ is a cyclic group.

The pattern emerges that the generators of $(\mathbb{Z}_n, +)$ are any congruence classes $[a]$ such that $\gcd(a, n) = 1$. In other words, $[a]$ is a generator of $\mathbb{Z}_n$ whenever a is relatively prime to the modulus n. $\square$

Exercise 26. Analyze the group of units of $\mathbb{Z}_8$ under multiplication.

The group $(\mathbb{Z}_8^*, \cdot)$ is not cyclic.

Solution. Observe that $|\mathbb{Z}_8| = 8$.

The binary structure $(\mathbb{Z}_8^*, \cdot)$ is the group of units of integers modulo 8 under multiplication.

Thus, $|\mathbb{Z}_8^*| = \phi(8) = 4$ and $\mathbb{Z}_8^* = \{[a] : \gcd(a, 8) = 1\} = \{[1], [3], [5], [7]\}$.

We draw the Cayley table for $\mathbb{Z}_8^*$.

$\cdot$	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

By noting the symmetry along the main diagonal of the table, we see that the multiplication is commutative, so $\mathbb{Z}_8^*$ is an abelian group.

The identity is 1 and each element is its own inverse, so $x^2 = 1$ for all $x \in \mathbb{Z}_8^*$.

Every element of a group G generates a cyclic subgroup of G, so every element of $\mathbb{Z}_8^*$ generates a cyclic subgroup of $\mathbb{Z}_8^*$.

By looking at the table we can easily see the cyclic subgroups generated by each element.

$\langle 1 \rangle = \{1\}$ and $|1| = 1$ and $\{1\}$ is a subgroup of $\mathbb{Z}_8^*$.

$\langle 3 \rangle = \{1, 3\}$ and $|3| = 2$ and $\{1, 3\}$ is a subgroup of $\mathbb{Z}_8^*$.

$\langle 5 \rangle = \{1, 5\}$ and $|5| = 2$ and $\{1, 5\}$ is a subgroup of $\mathbb{Z}_8^*$.

$\langle 7 \rangle = \{1, 7\}$ and $|7| = 2$ and $\{1, 7\}$ is a subgroup of $\mathbb{Z}_8^*$.

The order of any element of $\mathbb{Z}_8^*$ is either 1 or 2, but not 4.

Hence, no element of $\mathbb{Z}_8^*$ is a generator of $\mathbb{Z}_8^*$, so $\mathbb{Z}_8^*$ cannot be cyclic.

Since none of the orders of the elements are 4, then $\mathbb{Z}_8^*$ is not cyclic.

However, $\mathbb{Z}_8^*$ is abelian and is finite.

The subgroups of $(\mathbb{Z}_8^*, \cdot)$ are:
$\mathbb{Z}_8^* = \{1, 3, 5, 7\}$
$\{1, 3\}$
$\{1, 5\}$
$\{1, 7\}$
$\{1\}$

$\square$

Exercise 27. $(\mathbb{Z}_8^*, \cdot)$ is not cyclic.

Proof. Observe that $|\mathbb{Z}_8^*| = 4$.
We first prove $[a]^2 = [1]$ for every $[a] \in \mathbb{Z}_8^*$.
Let $[a] \in \mathbb{Z}_8^*$.
Then $\gcd(a, 8) = 1$.
Hence, a is either 1 or 3 or 5 or 7, so a is odd.
Therefore, there exists an integer k such that $a = 2k + 1$.
Thus, $a-1 = 2k$ and $a+1 = 2k+2$, so $a^2-1 = (a-1)(a+1) = 2k(2k+2) = 4k(k+1)$.
The product of two consecutive integers is even.
Hence, $k(k+1)$ is even, so there exists an integer m such that $k(k+1) = 2m$.
Thus, $a^2 - 1 = 4k(k+1) = 4(2m) = 8m$, so $8|(a^2 - 1)$.
Therefore, $a^2 \equiv 1 \pmod 8$, so $[a^2] = [1]$.
Thus, $[1] = [a^2] = [aa] = [a][a] = [a]^2$, so $[a]^2 = [1]$.
Consequently, $[a]^2 = [1]$ for every $[a] \in \mathbb{Z}_8^*$.

Let $[x] \in \mathbb{Z}_8^*$.
Then either $[x] = [1]$ or $[x] \neq [1]$.
We consider these cases separately.
Case 1: Suppose $[x] = [1]$.
Since $[1]^1 = [1]$, then the order of $[1]$ is $1 \neq 4$.
Hence, $[1]$ is not a generator of $\mathbb{Z}_8^*$.
Case 2: Suppose $[x] \neq [1]$.
Since $[x]^1 = [x]$, then $[x]^1 \neq [1]$.
Since $[x]^2 = [1]$, then the order of $[x]$ is $2 \neq 4$.
Hence, $[x]$ is not a generator of $\mathbb{Z}_8^*$.
Therefore, in all cases $[x]$ is not a generator of $\mathbb{Z}_8^*$.
Since $[x]$ is arbitrary, then this implies every element of $\mathbb{Z}_8^*$ is not a generator of $\mathbb{Z}_8^*$.
Thus, there is no element of $\mathbb{Z}_8^*$ that is a generator of $\mathbb{Z}_8^*$, so $\mathbb{Z}_8^*$ is not cyclic. $\square$

Exercise 28. Analyze the group of units of $\mathbb{Z}_9$ under multiplication.
The group $(\mathbb{Z}_9^*, \cdot)$ is cyclic.

Solution. Observe that $|\mathbb{Z}_9| = 9$.
The binary structure $(\mathbb{Z}_9^*, *)$ is the group of units of integers modulo 9 under multiplication.

Thus, $|\mathbb{Z}_9^*| = \phi(9) = 6$ and $\mathbb{Z}_9^* = \{[a] : \gcd(a, 9) = 1\} = \{[1], [2], [4], [5], [7], [8]\}$.

We draw the Cayley table for $\mathbb{Z}_9^*$.

$\cdot$	1	2	4	5	7	8
1	1	2	4	5	7	8
2	2	4	8	1	5	7
4	4	8	7	2	1	5
5	5	1	2	7	8	4
7	7	5	1	8	4	2
8	8	7	5	4	2	1

By noting the symmetry along the main diagonal of the table, we see that the multiplication is commutative, so $\mathbb{Z}_9^*$ is an abelian group.

The identity is 1.

The inverses are:
$1^{-1} = 1$
$2^{-1} = 5$
$4^{-1} = 7$
$5^{-1} = 2$
$7^{-1} = 4$
$8^{-1} = 8$

Every element of a group G generates a cyclic subgroup of G, so every element of $\mathbb{Z}_9^*$ generates a cyclic subgroup of $\mathbb{Z}_9^*$.

By looking at the table we can easily see the cyclic subgroups generated by each element.

$\langle 1 \rangle = \{1\}$ and $|1| = 1$ and $\{1\}$ is a subgroup of $\mathbb{Z}_9^*$.
$\langle 2 \rangle = \{2, 4, 8, 7, 5, 1\}$ and $|2| = 6$ and $\{2, 4, 8, 7, 5, 1\}$ is a subgroup of $\mathbb{Z}_9^*$.
$\langle 4 \rangle = \{4, 7, 1\}$ and $|4| = 3$ and $\{4, 7, 1\}$ is a subgroup of $\mathbb{Z}_9^*$.
$\langle 5 \rangle = \{5, 7, 8, 4, 2, 1\}$ and $|5| = 6$ and $\{5, 7, 8, 4, 2, 1\}$ is a subgroup of $\mathbb{Z}_9^*$.
$\langle 7 \rangle = \{7, 4, 1\}$ and $|7| = 3$ and $\{7, 4, 1\}$ is a subgroup of $\mathbb{Z}_9^*$.
$\langle 8 \rangle = \{8, 1\}$ and $|8| = 2$ and $\{8, 1\}$ is a subgroup of $\mathbb{Z}_9^*$.

Since $|2| = 6 = |5| = |\mathbb{Z}_9^*|$, then 2 and 5 are generators of $\mathbb{Z}_9^*$, so $\mathbb{Z}_9^*$ is cyclic.

Also, $\mathbb{Z}_9^*$ is finite.

The subgroups of $(\mathbb{Z}_9^*, \cdot)$ are:
$\mathbb{Z}_9^* = \{1, 2, 4, 5, 7, 8\}$
$\{1, 4, 7\}$
$\{1, 8\}$
$\{1\}$

$\square$

Exercise 29. Analyze the order of the group $(\mathbb{Z}_{10}^*, \cdot)$.

Solution. Observe that $\mathbb{Z}_{10}^*$ is the group of units of $\mathbb{Z}_{10}$ under multiplication modulo 10.

The integers modulo 10 is $\{0, 1, 2, ..., 9\}$ and $|\mathbb{Z}_{10}| = 10$.

The group of units $\mathbb{Z}_{10}^*$ is $\{a \in \mathbb{Z} : \gcd(a, 10) = 1\} = \{1, 3, 7, 9\}$ and $|\mathbb{Z}_{10}^*| = \phi(10) = 4$, where ϕ is Euler's totient function.

The Cayley table is below.

$\cdot$	1	3	7	9
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

Every element of a group G generates a cyclic subgroup of G, so every element of $\mathbb{Z}_{10}^*$ generates a cyclic subgroup of $\mathbb{Z}_{10}^*$.

The cyclic subgroups generated by each element are shown below.

$\langle 1\rangle = \{1\}$ and $|1| = 1$

$\langle 3\rangle = \{1, 3, 7, 9\}$ and $|3| = 4$

$\langle 7\rangle = \{1, 3, 7, 9\}$ and $|7| = 4$

$\langle 9\rangle = \{1, 9\}$ and $|9| = 2$

Since $|3| = |7| = 4$, then 3 and 7 are generators of $\mathbb{Z}_{10}^*$, so $\mathbb{Z}_{10}^*$ is cyclic.

The order of the inverse of an element is the same as the order of the element.

$|1| = |1^{-1}| = |1| = 1$

$|3| = |3^{-1}| = |7| = 4$

$|7| = |7^{-1}| = |3| = 4$

$|9| = |9^{-1}| = |9| = 2$

The subgroups of $(\mathbb{Z}_{10}^*, \cdot)$ are:

$\mathbb{Z}_{10}^* = \{1, 3, 7, 9\}$

$\{1, 9\}$

$\{1\}$

□

Exercise 30. Analyze the order of the group $(\mathbb{Z}_{12}^*, \cdot)$.

Solution. Observe that $\mathbb{Z}_{12}^*$ is the group of units of $\mathbb{Z}_{12}$ under multiplication modulo 12.

The integers modulo 12 is $\{0, 1, 2, ..., 11\}$ and $|\mathbb{Z}_{12}| = 12$.

The group of units $\mathbb{Z}_{12}^*$ is $\{a \in \mathbb{Z} : \gcd(a, 12) = 1\} = \{1, 5, 7, 11\}$ and $|\mathbb{Z}_{12}^*| = \phi(12) = 4$, where ϕ is Euler's totient function.

The Cayley table is below.

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

Every element of a group G generates a cyclic subgroup of G, so every element of $\mathbb{Z}_{12}^*$ generates a cyclic subgroup of $\mathbb{Z}_{12}^*$.

The cyclic subgroups generated by each element are shown below.

$\langle 1 \rangle = \{1\}$ and $|1| = 1$

$\langle 5 \rangle = \{1, 5\}$ and $|5| = 2$

$\langle 7 \rangle = \{1, 7\}$ and $|7| = 2$

$\langle 11 \rangle = \{1, 11\}$ and $|11| = 2$

There is no element that generates the entire group, so $\mathbb{Z}_{12}^*$ is not cyclic.

The order of the inverse of an element is the same as the order of the element.

$|1| = |1^{-1}| = |1| = 1$

$|5| = |5^{-1}| = |5| = 2$

$|7| = |7^{-1}| = |7| = 2$

$|11| = |11^{-1}| = |11| = 2$

The subgroups of $(\mathbb{Z}_{12}^*, \cdot)$ are:

$\mathbb{Z}_{12}^* = \{1, 5, 7, 11\}$

$\{1, 5\}$

$\{1, 7\}$

$\{1, 11\}$

$\{1\}$

$\square$

Exercise 31. Analyze the order of the group $(\mathbb{Z}_{15}^*, \cdot)$.

Solution. Observe that $\mathbb{Z}_{15}^*$ is the group of units of $\mathbb{Z}_{15}$ under multiplication modulo 15.

The integers modulo 15 is $\{0, 1, 2, ..., 14\}$ and $|\mathbb{Z}_{15}| = 15$.

The group of units $\mathbb{Z}_{15}^*$ is $\{a \in \mathbb{Z} : \gcd(a, 15) = 1\} = \{1, 2, 4, 7, 8, 11, 13, 14\}$ and $|\mathbb{Z}_{15}^*| = \phi(15) = 8$, where ϕ is Euler's totient function.

The Cayley table is below.

$\cdot$	1	2	4	7	8	11	13	14
1	1	2	4	7	8	11	13	14
2	2	4	8	14	1	7	11	13
4	4	8	1	13	2	14	7	11
7	7	14	13	4	11	2	1	8
8	8	1	2	11	4	13	14	7
11	11	7	14	2	13	1	8	4
13	13	11	7	1	14	8	4	2
14	14	13	11	8	7	4	2	1

Every element of a group G generates a cyclic subgroup of G, so every element of $\mathbb{Z}_{15}^*$ generates a cyclic subgroup of $\mathbb{Z}_{15}^*$.

The cyclic subgroups generated by each element are shown below.

$\langle 1 \rangle = \{1\}$ and $|1| = 1$

$\langle 2\rangle = \{1, 2, 4, 8\}$ and $|2| = 4$
$\langle 4\rangle = \{1, 4\}$ and $|4| = 2$
$\langle 7\rangle = \{1, 7, 4, 13\}$ and $|7| = 4$
$\langle 8\rangle = \{1, 8, 4, 2\}$ and $|8| = 4$
$\langle 11\rangle = \{1, 11\}$ and $|11| = 2$
$\langle 13\rangle = \{1, 13, 4, 7\}$ and $|13| = 4$
$\langle 14\rangle = \{1, 14\}$ and $|14| = 2$
There is no element that generates the entire group, so $\mathbb{Z}_{15}^*$ is not cyclic.

The order of the inverse of an element is the same as the order of the element.
$|1| = |1^{-1}| = |1| = 1$
$|2| = |2^{-1}| = |8| = 4$
$|4| = |4^{-1}| = |4| = 2$
$|7| = |7^{-1}| = |13| = 4$
$|8| = |8^{-1}| = |2| = 4$
$|11| = |11^{-1}| = |11| = 2$
$|13| = |13^{-1}| = |7| = 4$
$|14| = |14^{-1}| = |14| = 2$

The subgroups of $(\mathbb{Z}_{15}^*, \cdot)$ are:
$\mathbb{Z}_{15}^* = \{1, 2, 4, 7, 8, 11, 13, 14\}$
$\{1, 2, 4, 8\}$
$\{1, 4, 7, 13\}$
$\{1, 4\}$
$\{1, 11\}$
$\{1, 14\}$
$\{1\}$

□

Exercise 32. Analyze the order of the group $(\mathbb{Z}_{18}^*, \cdot)$.

Solution. Observe that $\mathbb{Z}_{18}^*$ is the group of units of $\mathbb{Z}_{18}$ under multiplication modulo 18.

The integers modulo 18 is $\{0, 1, 2, ..., 17\}$ and $|\mathbb{Z}_{18}| = 18$.

The group of units $\mathbb{Z}_{18}^*$ is $\{a \in \mathbb{Z} : \gcd(a, 18) = 1\} = \{1, 5, 7, 11, 13, 17\}$ and $|\mathbb{Z}_{18}^*| = \phi(18) = 6$, where ϕ is Euler's totient function.

The Cayley table is below.

$\cdot$	1	5	7	11	13	17
1	1	5	7	11	13	17
5	5	7	17	1	11	13
7	7	17	13	5	1	11
11	11	1	5	13	17	7
13	13	11	1	17	7	5
17	17	13	11	7	5	1

Every element of a group G generates a cyclic subgroup of G, so every element of $\mathbb{Z}_{18}^*$ generates a cyclic subgroup of $\mathbb{Z}_{18}^*$.

The cyclic subgroups generated by each element are shown below.
$\langle 1 \rangle = \{1\}$ and $|1| = 1$
$\langle 5 \rangle = \{1, 5, 7, 11, 13, 17\}$ and $|5| = 6$
$\langle 7 \rangle = \{1, 7, 13\}$ and $|7| = 3$
$\langle 11 \rangle = \{1, 5, 7, 11, 13, 17\}$ and $|11| = 6$
$\langle 13 \rangle = \{1, 7, 13\}$ and $|13| = 3$
$\langle 17 \rangle = \{1, 17\}$ and $|17| = 2$
The set of generators is $\{5, 11\}$ so $\mathbb{Z}_{18}^*$ is cyclic.

The order of the inverse of an element is the same as the order of the element.
$|1| = |1^{-1}| = |1| = 1$
$|5| = |5^{-1}| = |11| = 6$
$|7| = |7^{-1}| = |13| = 3$
$|11| = |11^{-1}| = |5| = 6$
$|13| = |13^{-1}| = |7| = 3$
$|17| = |17^{-1}| = |17| = 2$

The subgroups of $(\mathbb{Z}_{18}^*, \cdot)$ are:
$\mathbb{Z}_{18}^* = \{1, 5, 7, 11, 13, 17\}$
$\{1, 7, 13\}$
$\{1, 17\}$
$\{1\}$

$\square$

Exercise 33. Analyze the order of the group $(\mathbb{Z}_{20}^*, \cdot)$.

Solution. Observe that $\mathbb{Z}_{20}^*$ is the group of units of $\mathbb{Z}_{20}$ under multiplication modulo 20.

The integers modulo 20 is $\{0, 1, 2, ..., 19\}$ and $|\mathbb{Z}_{20}| = 20$.

The group of units $\mathbb{Z}_{20}^*$ is $\{a \in \mathbb{Z} : \gcd(a, 20) = 1\} = \{1, 3, 7, 9, 11, 13, 17, 19\}$ and $|\mathbb{Z}_{20}^*| = \phi(20) = 8$, where ϕ is Euler's totient function.

The Cayley table is below.

$\cdot$	1	3	7	9	11	13	17	19
1	1	3	7	9	11	13	17	19
3	3	9	1	7	13	19	11	17
7	7	1	9	3	17	11	19	13
9	9	7	3	1	19	17	13	11
11	11	13	17	19	1	3	7	9
13	13	19	11	17	3	9	1	7
17	17	11	19	13	7	1	9	3
19	19	17	13	11	9	7	3	1

Every element of a group G generates a cyclic subgroup of G, so every element of $\mathbb{Z}_{20}^*$ generates a cyclic subgroup of $\mathbb{Z}_{20}^*$.

The cyclic subgroups generated by each element are shown below.

$\langle 1 \rangle = \{1\}$ and $|1| = 1$
$\langle 3 \rangle = \{1, 3, 9, 7\}$ and $|3| = 4$
$\langle 7 \rangle = \{1, 7, 9, 3\}$ and $|7| = 4$
$\langle 9 \rangle = \{1, 9\}$ and $|9| = 2$
$\langle 11 \rangle = \{1, 11\}$ and $|11| = 2$
$\langle 13 \rangle = \{1, 13, 9, 17\}$ and $|13| = 4$
$\langle 17 \rangle = \{1, 17, 9, 13\}$ and $|17| = 4$
$\langle 19 \rangle = \{1, 19\}$ and $|9| = 2$

There is no element that generates $\mathbb{Z}_{20}^*$, so $\mathbb{Z}_{20}^*$ is not cyclic.

The order of the inverse of an element is the same as the order of the element.

$|1| = |1^{-1}| = |1| = 1$
$|3| = |3^{-1}| = |7| = 4$
$|7| = |7^{-1}| = |3| = 4$
$|9| = |9^{-1}| = |9| = 2$
$|11| = |11^{-1}| = |11| = 2$
$|13| = |13^{-1}| = |17| = 4$
$|17| = |17^{-1}| = |13| = 4$
$|19| = |19^{-1}| = |19| = 2$

The subgroups are shown below.

$\mathbb{Z}_{20}^* = \{1, 3, 7, 9, 11, 13, 17, 19\}$
$\{1, 9, 13, 17\}$
$\{1, 3, 7, 9\}$
$\{1, 9\}$
$\{1, 11\}$
$\{1, 19\}$
$\{1\}$

$\square$

Exercise 34. Analyze the order of the group $(\mathbb{Z}_{24}^*, \cdot)$.

Solution. Observe that $\mathbb{Z}_{24}^*$ is the group of units of $\mathbb{Z}_{24}$ under multiplication modulo 24.

The integers modulo 24 is $\{0, 1, 2, ..., 23\}$ and $|\mathbb{Z}_{24}| = 24$.

The group of units $\mathbb{Z}_{24}^*$ is $\{a \in \mathbb{Z} : \gcd(a, 24) = 1\} = \{1, 5, 7, 11, 13, 17, 19, 23\}$ and $|\mathbb{Z}_{24}^*| = \phi(24) = 8$, where ϕ is Euler's totient function.

The Cayley table is below.

$\cdot$	1	5	7	11	13	17	19	23
1	1	5	7	11	13	17	19	23
5	5	1	11	7	17	13	23	19
7	7	11	1	5	19	23	13	17
11	11	7	5	1	23	19	17	13
13	13	17	19	23	1	5	7	11
17	17	13	23	19	5	1	11	7
19	19	23	13	17	7	11	1	5
23	23	19	17	13	11	7	5	1

Every element of a group G generates a cyclic subgroup of G, so every element of $\mathbb{Z}_{24}^*$ generates a cyclic subgroup of $\mathbb{Z}_{24}^*$.

The cyclic subgroups generated by each element are shown below.

$\langle 1\rangle = \{1\}$ and $|1| = 1$
$\langle 5\rangle = \{1, 5\}$ and $|3| = 2$
$\langle 7\rangle = \{1, 7\}$ and $|7| = 2$
$\langle 11\rangle = \{1, 11\}$ and $|9| = 2$
$\langle 13\rangle = \{1, 13\}$ and $|9| = 2$
$\langle 17\rangle = \{1, 17\}$ and $|9| = 2$
$\langle 19\rangle = \{1, 19\}$ and $|9| = 2$
$\langle 23\rangle = \{1, 23\}$ and $|9| = 2$

Observe that $x^2 = 1$ for all $x \in \mathbb{Z}_{24}^*$, so each element is its own inverse and the order of each non identity element is 2.

There is no element that generates $\mathbb{Z}_{24}^*$, so $\mathbb{Z}_{24}^*$ is not cyclic.

The order of the inverse of an element is the same as the order of the element.

$|1| = |1^{-1}| = |1| = 1$
$|5| = |5^{-1}| = |5| = 2$
$|7| = |7^{-1}| = |7| = 2$
$|11| = |11^{-1}| = |11| = 2$
$|13| = |13^{-1}| = |13| = 2$
$|17| = |17^{-1}| = |17| = 2$
$|19| = |19^{-1}| = |19| = 2$
$|23| = |23^{-1}| = |23| = 2$

The subgroups are shown below.

$\mathbb{Z}_{24}^* = \{1, 5, 7, 11, 13, 17, 19, 23\}$
$\{1, 5\}$
$\{1, 7\}$
$\{1, 11\}$
$\{1, 13\}$
$\{1, 17\}$
$\{1, 19\}$

$\{1, 23\}$
$\{1\}$

□

Exercise 35. Analyze the order of the group $(\mathbb{Z}_{30}^*, \cdot)$.

Solution. Observe that $\mathbb{Z}_{30}^*$ is the group of units of $\mathbb{Z}_{30}$ under multiplication modulo 30.

The integers modulo 30 is $\{0, 1, 2, ..., 29\}$ and $|\mathbb{Z}_{30}| = 30$.

The group of units $\mathbb{Z}_{30}^*$ is $\{a \in \mathbb{Z} : \gcd(a, 30) = 1\} = \{1, 7, 11, 13, 17, 19, 23, 29\}$ and $|\mathbb{Z}_{30}^*| = \phi(30) = 8$, where ϕ is Euler's totient function.

The Cayley table is below.

$\cdot$	1	7	11	13	17	19	23	29
1	1	7	11	13	17	19	23	29
7	7	19	17	1	29	13	11	23
11	11	17	1	23	7	29	13	19
13	13	1	23	19	11	7	29	17
17	17	29	7	11	19	23	1	13
19	19	13	29	7	23	1	17	11
23	23	11	13	29	1	17	19	7
29	29	23	19	17	13	11	7	1

Every element of a group G generates a cyclic subgroup of G, so every element of $\mathbb{Z}_{30}^*$ generates a cyclic subgroup of $\mathbb{Z}_{30}^*$.

The cyclic subgroups generated by each element are shown below.
$\langle 1 \rangle = \{1\}$ and $|1| = 1$
$\langle 7 \rangle = \{1, 7, 13, 19\}$ and $|7| = 4$
$\langle 11 \rangle = \{1, 11\}$ and $|11| = 2$
$\langle 13 \rangle = \{1, 7, 13, 19\}$ and $|13| = 4$
$\langle 17 \rangle = \{1, 17, 19, 23\}$ and $|17| = 4$
$\langle 19 \rangle = \{1, 19\}$ and $|19| = 2$
$\langle 23 \rangle = \{1, 17, 19, 23\}$ and $|23| = 4$
$\langle 29 \rangle = \{1, 29\}$ and $|29| = 2$

There is no element that generates $\mathbb{Z}_{30}^*$, so $\mathbb{Z}_{30}^*$ is not cyclic.

The order of the inverse of an element is the same as the order of the element.
$|1| = |1^{-1}| = |1| = 1$
$|7| = |7^{-1}| = |13| = 4$
$|11| = |11^{-1}| = |11| = 2$
$|13| = |13^{-1}| = |7| = 4$
$|17| = |17^{-1}| = |23| = 4$
$|19| = |19^{-1}| = |19| = 2$
$|23| = |23^{-1}| = |17| = 4$
$|29| = |29^{-1}| = |29| = 2$

The subgroups are shown below.
$\mathbb{Z}_{30}^* = \{1, 7, 11, 13, 17, 19, 23, 29\}$
$\{1, 7, 13, 19\}$
$\{1, 17, 19, 23\}$
$\{1, 11\}$
$\{1, 17\}$
$\{1, 19\}$
$\{1, 29\}$
$\{1\}$
□

Exercise 36. Analyze the subgroup of $(\mathbb{Z}, +)$ generated by $7 \in \mathbb{Z}$.

Solution. The cyclic subgroup generated by 7 is $\langle 7 \rangle = \{7k : k \in \mathbb{Z}\} = 7\mathbb{Z} = \{..., -21, -14, -7, 0, 7, 14, 21, 28, 35, ...\}$ the set of all multiples of 7 and the order of 7 is $|7| = \infty$. □

Exercise 37. Analyze the subgroup of $(\mathbb{Z}_{24}, +)$ generated by $15 \in \mathbb{Z}_{24}$.

Solution. The cyclic subgroup generated by 15 is $\langle 15 \rangle = \{15k : k \in \mathbb{Z}\} = \{0, 15, 6, 21, 12, 3, 18, 9\}$ and the order of 15 is $|15| = 8$. □

Exercise 38. Analyze the subgroup generated by 7 in the group $(\mathbb{R}^*, \cdot)$.

Solution. The cyclic subgroup generated by $7 \in \mathbb{R}^*$ is $\langle 7 \rangle = \{7^k : k \in \mathbb{Z}\}$.
There is no positive integer n such that $7^n = 1$, so 7 has infinite order.

To prove there is no $n \in \mathbb{Z}^+$ such that $7^n = 1$, we prove $7^n > 1$ for all $n \in \mathbb{Z}^+$.
Define predicate $p(n) : 7^n > 1$ over $\mathbb{Z}$.
We prove $p(n)$ is true for all $n \geq 1$ by induction on n.
Basis:
Since $7^1 = 7 > 1$, then $p(1)$ is true.
Induction:
Suppose $p(k)$ is true for any $k \in \mathbb{Z}^+$.
Then $7^k > 1$.
Since $7 > 1$, then $7^{k+1} = 7^k \cdot 7 > 1 \cdot 1 = 1$, so $7^{k+1} > 1$.
Hence, $p(k + 1)$ is true, so $p(k)$ implies $p(k + 1)$ for all $k \in \mathbb{Z}^+$.
Since $p(1)$ is true and $p(k)$ implies $p(k + 1)$ for all $k \in \mathbb{Z}^+$, then by PMI, $p(n)$ is true for all $n \in \mathbb{Z}^+$.
Thus, $7^n > 1$ for all $n \in \mathbb{Z}^+$, so $7^n \neq 1$ for all $n \in \mathbb{Z}^+$.
Therefore, there is no $n \in \mathbb{Z}^+$ such that $7^n = 1$, so 7 has infinite order.
Thus, $\langle 7 \rangle = \{..., 7^{-3}, 7^{-2}, 7^{-1}, 1, 7, 7^2, 7^3, ...\}$ is infinite and each power of 7 is distinct. □

Exercise 39. Analyze the subgroup generated by $2i$ in $(\mathbb{C}^*, \cdot)$.

Solution. Every element of a group generates a cyclic subgroup, so $2i \in \mathbb{C}^*$ generates a cyclic subgroup of $\mathbb{C}^*$.

The cyclic subgroup of $\mathbb{C}^*$ generated by $2i$ is
$\{(2i)^k : k \in \mathbb{Z}\} = \{..., 1, 2i, -4, -8i, 16, 32i, -64, ...$
of infinite order. The order of $2i$ is $|2i| = \infty$. □

Exercise 40. Analyze the subgroup generated by i in $(\mathbb{C}^*, \cdot)$.

Solution. Every element of a group generates a cyclic subgroup, so $i \in \mathbb{C}^*$ generates a cyclic subgroup of $\mathbb{C}^*$.

The cyclic subgroup of $\mathbb{C}^*$ generated by i is $\{1, i, -1, -i\}$ of order 4.
This finite group is a subgroup of the unit circle $\mathbb{T}$.
This is the 4^{th} roots of unity group U_4. □

Exercise 41. Analyze the 5^{th} roots of unity group and its generators.

Solution. The 5^{th} roots of unity is the set $U_5 = \{z \in \mathbb{C} : z^5 = 1\}$.
The group $(U_5, \cdot)$ is a cyclic group of order $|U_5| = 5$ with generator $g = e^{i2\pi/5}$.
Therefore, U_5 is the set
$\{1, e^{i\frac{2\pi}{5}}, e^{i\frac{4\pi}{5}}, e^{i\frac{6\pi}{5}}, e^{i\frac{8\pi}{5}}\} = \{g^0, g^1, g^2, g^3, g^4\}$.
This is a finite group of order 5 and is a subgroup of the circle group $\mathbb{T}$.

Since U_5 is a finite cyclic group of order 5 and $g = e^{i\frac{2\pi}{5}}$ is a generator of U_5, then the generators are elements g^k such that $\gcd(k, 5) = 1$.
Hence, $k \in \{1, 2, 3, 4\}$, so the other generators are:
$g^2 = (e^{i2\pi/5})^2 = e^{i4\pi/5}$
$g^3 = (e^{i2\pi/5})^3 = e^{i6\pi/5}$
$g^4 = (e^{i2\pi/5})^4 = e^{i8\pi/5}$.

The elements of U_5 written as powers of g^2 are:
$(g^2)^0 = 1$
$(g^2)^1 = e^{i4\pi/5}$
$(g^2)^2 = (e^{i4\pi/5})^2 = e^{i8\pi/5}$
$(g^2)^3 = (e^{i4\pi/5})^3 = e^{i12\pi/5} = e^{i2\pi/5}$
$(g^2)^4 = (e^{i4\pi/5})^4 = e^{i16\pi/5} = e^{i6\pi/5}$
Thus, $U_5 = \{(g^2)^0, (g^2)^1, (g^2)^2, (g^2)^3, (g^2)^4\}$.

The elements of U_5 written as powers of g^3 are:
$(g^3)^0 = 1$
$(g^3)^1 = e^{i6\pi/5}$
$(g^3)^2 = (e^{i6\pi/5})^2 = e^{i12\pi/5} = e^{i2\pi/5}$
$(g^3)^3 = (e^{i6\pi/5})^3 = e^{i18\pi/5} = e^{i8\pi/5}$
$(g^3)^4 = (e^{i6\pi/5})^4 = e^{i24\pi/5} = e^{i4\pi/5}$
Thus, $U_5 = \{(g^3)^0, (g^3)^1, (g^3)^2, (g^3)^3, (g^3)^4\}$.

The elements of U_5 written as powers of g^4 are:
$(g^4)^0 = 1$
$(g^4)^1 = e^{i8\pi/5}$
$(g^4)^2 = (e^{i8\pi/5})^2 = e^{i16\pi/5} = e^{i6\pi/5}$
$(g^4)^3 = (e^{i8\pi/5})^3 = e^{i24\pi/5} = e^{i4\pi/5}$
$(g^4)^4 = (e^{i8\pi/5})^4 = e^{i32\pi/5} = e^{i2\pi/5}$
Thus, $U_5 = \{(g^4)^0, (g^4)^1, (g^4)^2, (g^4)^3, (g^4)^4\}$. $\square$

Exercise 42. Analyze the subgroup generated by $\frac{1+i\sqrt{3}}{2}$ in $(\mathbb{C}^*, \cdot)$.

Solution. Every element of a group generates a cyclic subgroup, so $\frac{1+i\sqrt{3}}{2} \in \mathbb{C}^*$ generates a cyclic subgroup of $\mathbb{C}^*$.
The cyclic subgroup generated by $\frac{1+i\sqrt{3}}{2} = e^{i\frac{\pi}{3}}$ is
$\{1, e^{i\frac{\pi}{3}}, e^{i\frac{2\pi}{3}}, e^{i\pi}, e^{i\frac{4\pi}{3}}, e^{i\frac{5\pi}{3}}\} = \{g^0, g^1, g^2, g^3, g^4, g^5\}$.
This is a finite group of order 6 and is a subgroup of the circle group $\mathbb{T}$.
This is the 6^{th} roots of unity which is a cyclic group.

The generator for U_n is $g = e^{i\frac{2\pi}{n}}$.
Since $e^{i\pi/3} = g = e^{i\frac{2\pi}{n}}$, then $\frac{\pi}{3} = \frac{2\pi}{n}$.
Hence, $\pi n = 6\pi$, so $n = 6$.

Since U_6 is a finite cyclic group of order 6 and $g = e^{i\pi/3}$ is a generator of U_6, then the generators are elements g^k such that $\gcd(k, 6) = 1$.
Hence, $k \in \{1, 5\}$, so the other generator is $g^5 = (e^{i\pi/3})^5 = e^{i5\pi/3}$.
The elements of U_6 written as powers of g^5 are:
$(g^5)^0 = 1$
$(g^5)^1 = e^{i5\pi/3}$
$(g^5)^2 = (e^{i5\pi/3})^2 = e^{i10\pi/3} = e^{i4\pi/3}$
$(g^5)^3 = (e^{i5\pi/3})^3 = e^{i5\pi} = e^{i\pi} = -1$
$(g^5)^4 = (e^{i5\pi/3})^4 = e^{i20\pi/3} = e^{i2\pi/3}$
$(g^5)^5 = (e^{i5\pi/3})^5 = e^{i25\pi/3} = e^{i\pi/3}$
Thus, $U_6 = \{(g^5)^0, (g^5)^1, (g^5)^2, (g^5)^3, (g^5)^4, (g^5)^5\}$. $\square$

Exercise 43. Analyze the subgroup generated by $\frac{1+i}{\sqrt{2}}$ in $(\mathbb{C}^*, \cdot)$.

Solution. Every element of a group generates a cyclic subgroup, so $\frac{1+i}{\sqrt{2}} \in \mathbb{C}^*$ generates a cyclic subgroup of $\mathbb{C}^*$.
The cyclic subgroup of $\mathbb{C}^*$ generated by $\frac{1+i}{\sqrt{2}} = e^{i\frac{\pi}{4}}$ is
$\{1, e^{i\frac{\pi}{4}}, e^{i\frac{\pi}{2}}, e^{i\frac{3\pi}{4}}, e^{i\pi}, e^{i\frac{5\pi}{4}}, e^{i\frac{3\pi}{2}}, e^{i\frac{7\pi}{4}}\}$ a finite group of order 8.
This group is a subgroup of the unit circle $\mathbb{T}$.
This is the $8th$ roots of unity $(U_8, \cdot)$.
The generator for U_n is $g = e^{i\frac{2\pi}{n}}$.
Since $e^{i\pi/4} = g = e^{i\frac{2\pi}{n}}$, then $\frac{\pi}{4} = \frac{2\pi}{n}$.
Hence, $\pi n = 8\pi$, so $n = 8$.

Since U_8 is a finite cyclic group of order 8 and $g = e^{i\frac{\pi}{4}}$ is a generator of U_8, then the generators are elements g^k such that $\gcd(k, 8) = 1$.

Hence, $k \in \{1, 3, 5, 7\}$, so the other generators are:
$g^3 = (e^{i\pi/4})^3 = e^{i3\pi/4}$
$g^5 = (e^{i\pi/4})^5 = e^{i5\pi/4}$
$g^7 = (e^{i\pi/4})^7 = e^{i7\pi/4}$. $\square$

Exercise 44. Analyze the subgroup generated by the below matrix in $GL_2(\mathbb{R})$.

$$A = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$$

Solution. Since $\det A = 0 \cdot 0 - 1(-1) = 1$, then $\det A \neq 0$, so A^{-1} exists.

Hence, A is invertible, so $A \in GL_2(\mathbb{R})$.

Every element of a group G generates a cyclic subgroup of G.

Thus, A generates a cyclic subgroup of the general linear group $GL_2(\mathbb{R})$.

The cyclic subgroup generated by A is $\langle A \rangle = \{I, A, A^2, A^3\}$, where I is the identity matrix and

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

$$A^3 = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$$

The order of A is $|A| = |\langle A \rangle| = 4$, so A has finite order and $\langle A \rangle$ is a finite group.

The inverses are:
$I^{-1} = I$
$A^{-1} = A^3$
$(A^2)^{-1} = A^2$

Since $\langle A \rangle$ is a cyclic group of order 4, then $\langle A \rangle$ is a finite cyclic group.

Since A is a generator, the generators are elements A^k such that $\gcd(k, 4) = 1$.

Therefore, there are $\phi(4) = 2$ generators and $k \in \{1, 3\}$, so the set of generators is $\{A, A^3\}$. $\square$

Exercise 45. Analyze the subgroup generated by the below matrix in $GL_2(\mathbb{R})$.

$$A = \begin{bmatrix} 0 & \frac{1}{3} \\ 3 & 0 \end{bmatrix}$$

Solution. Since $\det A = 0 \cdot 0 - \frac{1}{3}(3) = -1$, then $\det A \neq 0$, so A^{-1} exists.

Hence, A is invertible, so $A \in GL_2(\mathbb{R})$.

Every element of a group G generates a cyclic subgroup of G.

Thus, A generates a cyclic subgroup of the general linear group $GL_2(\mathbb{R})$.

The cyclic subgroup generated by A is $\langle A \rangle = \{I, A\}$, where I is the identity matrix and

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

The order of A is $|A| = |\langle A \rangle| = 2$, so A has finite order and $\langle A \rangle$ is a finite group.

The inverses are:

$I^{-1} = I$

$A^{-1} = A$

Since $\langle A \rangle$ is a cyclic group of order 2, then $\langle A \rangle$ is a finite cyclic group.

Since A is a generator, the generators are elements A^k such that $\gcd(k, 2) = 1$.

Therefore, there is $\phi(2) = 1$ generator and $k \in \{1\}$, so the set of generators is $\{A\}$. $\square$

Exercise 46. Analyze the subgroup generated by the below matrix in $GL_2(\mathbb{R})$.

$$A = \begin{bmatrix} 1 & -1 \\ 1 & 0 \end{bmatrix}$$

Solution. Since $\det A = 1 \cdot 0 - (-1)(1) = 1$, then $\det A \neq 0$, so A^{-1} exists.

Hence, A is invertible, so $A \in GL_2(\mathbb{R})$.

Every element of a group G generates a cyclic subgroup of G.

Thus, A generates a cyclic subgroup of the general linear group $GL_2(\mathbb{R})$.

The cyclic subgroup generated by A is $\langle A \rangle = \{I, A, A^2, A^3, A^4, A^5\}$, where I is the identity matrix and

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

$$A^3 = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$$

$$A^4 = \begin{bmatrix} -1 & 1 \\ -1 & 0 \end{bmatrix}$$

$$A^5 = \begin{bmatrix} 0 & 1 \\ -1 & 1 \end{bmatrix}$$

The order of A is $|A| = |\langle A \rangle| = 6$, so A has finite order and $\langle A \rangle$ is a finite group.

The inverses are:
$I^{-1} = I$
$A^{-1} = A^5$
$(A^2)^{-1} = A^4$
$(A^3)^{-1} = A^3$
$(A^4)^{-1} = A^2$
$(A^5)^{-1} = A$

Since $\langle A \rangle$ is a cyclic group of order 6, then $\langle A \rangle$ is a finite cyclic group.

Since A is a generator, the generators are elements A^k such that $\gcd(k, 6) = 1$.

Therefore, there are $\phi(6) = 2$ generators and $k \in \{1, 5\}$, so the set of generators is $\{A, A^5\}$. $\square$

Exercise 47. Analyze the subgroup generated by the below matrix in $GL_2(\mathbb{R})$.

$$A = \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix}$$

Solution. Since $\det A = 1 \cdot 1 - (-1)(0) = 1$, then $\det A \neq 0$, so A^{-1} exists.

Hence, A is invertible, so $A \in GL_2(\mathbb{R})$.

Every element of a group G generates a cyclic subgroup of G.

Thus, A generates a cyclic subgroup of the general linear group $GL_2(\mathbb{R})$.

The cyclic subgroup generated by A is $\langle A \rangle = \{A^n : n \in \mathbb{Z}\} = \{B_n : n \in \mathbb{Z}\}$, where I is the identity matrix and

$$B_n = \begin{bmatrix} 1 & -n \\ 0 & 1 \end{bmatrix}$$

The order of A is $|A| = |\langle A \rangle| = \infty$, so A has infinite order and $\langle A \rangle$ is an infinite group and each power of A is distinct.

The inverses are:
$I^{-1} = I$
$A^{-1} = B_{-1}$
$(A^2)^{-1} = B_{-2}$
$(A^3)^{-1} = B_{-3}$
$(A^4)^{-1} = B_{-4}$
$(A^5)^{-1} = B_{-5}$ etc.

Since $\langle A \rangle$ is a cyclic group of order ∞, then $\langle A \rangle$ is an infinite cyclic group. $\square$

Exercise 48. Analyze the subgroup generated by the below matrix in $GL_2(\mathbb{R})$.

$$A = \begin{bmatrix} 1 & -1 \\ -1 & 0 \end{bmatrix}$$

Solution. Since $\det A = 1 \cdot 0 - (-1)(-1) = -1$, then $\det A \neq 0$, so A^{-1} exists.
Hence, A is invertible, so $A \in GL_2(\mathbb{R})$.
Every element of a group G generates a cyclic subgroup of G.
Thus, A generates a cyclic subgroup of the general linear group $GL_2(\mathbb{R})$.
The cyclic subgroup generated by A is $\langle A \rangle = \{A^n : n \in \mathbb{Z}\}$, where I is the identity matrix and $I = A^0$ and $F_1 = 1$ and $F_2 = 1$ and $F_n = F_{n-1} + F_{n-2}$ for $n > 1$.
If $n > 0$, then

$$A^n = \begin{bmatrix} F_{n+1} & -F_n \\ -F_n & F_{n+1} - F_n \end{bmatrix}$$

If $n < 0$ and n is even, then let $k = -n$ and

$$A^n = \begin{bmatrix} F_{k+1} - F_k & F_k \\ F_k & F_{k+1} \end{bmatrix}$$

If $n < 0$ and n is odd, then let $k = -n$ and

$$A^n = \begin{bmatrix} F_k - F_{k+1} & -F_k \\ -F_k & -F_{k+1} \end{bmatrix}$$

The order of A is $|A| = |\langle A \rangle| = \infty$, so A has infinite order and $\langle A \rangle$ is an infinite group and each power of A is distinct.
The inverses are:
$I^{-1} = I$
$A^{-1} = A^{-1}$
$(A^2)^{-1} = A^{-2}$
$(A^3)^{-1} = A^{-3}$
$(A^4)^{-1} = A^{-4}$
$(A^5)^{-1} = A^{-5}$ etc.

Since $\langle A\rangle$ is a cyclic group of order ∞, then $\langle A\rangle$ is an infinite cyclic group. $\square$

Exercise 49. Analyze the subgroup generated by the below matrix in $GL_2(\mathbb{R})$.

$$A = \begin{bmatrix} \frac{\sqrt{3}}{2} & \frac{1}{2} \\ -\frac{1}{2} & \frac{\sqrt{3}}{2} \end{bmatrix}$$

Solution. Since $\det A = \frac{\sqrt{3}}{2}\cdot\frac{\sqrt{3}}{2} - (\frac{1}{2})(-\frac{1}{2}) = 1$, then $\det A \neq 0$, so A^{-1} exists.
Hence, A is invertible, so $A \in GL_2(\mathbb{R})$.
Every element of a group G generates a cyclic subgroup of G.
Thus, A generates a cyclic subgroup of the general linear group $GL_2(\mathbb{R})$.
The cyclic subgroup generated by A is
$\langle A\rangle = \{I, A, A^2, A^3, A^4, A^5, A^6, A^7, A^8, A^9, A^{10}, A^{11}\}$,
where I is the identity matrix and

$$A^2 = \begin{bmatrix} \frac{1}{2} & \frac{\sqrt{3}}{2} \\ -\frac{\sqrt{3}}{2} & \frac{1}{2} \end{bmatrix}$$

$$A^3 = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$$

$$A^4 = \begin{bmatrix} -\frac{1}{2} & \frac{\sqrt{3}}{2} \\ -\frac{\sqrt{3}}{2} & -\frac{1}{2} \end{bmatrix}$$

$$A^5 = \begin{bmatrix} -\frac{\sqrt{3}}{2} & \frac{1}{2} \\ -\frac{1}{2} & -\frac{\sqrt{3}}{2} \end{bmatrix}$$

$$A^6 = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$$

$$A^7 = \begin{bmatrix} -\frac{\sqrt{3}}{2} & -\frac{1}{2} \\ \frac{1}{2} & -\frac{\sqrt{3}}{2} \end{bmatrix}$$

$$A^8 = \begin{bmatrix} -\frac{1}{2} & -\frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & -\frac{1}{2} \end{bmatrix}$$

$$A^9 = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$$

$$A^{10} = \begin{bmatrix} \frac{1}{2} & -\frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & \frac{1}{2} \end{bmatrix}$$

$$A^{11} = \begin{bmatrix} \frac{\sqrt{3}}{2} & -\frac{1}{2} \\ \frac{1}{2} & \frac{\sqrt{3}}{2} \end{bmatrix}$$

The order of A is $|A| = |\langle A \rangle| = 12$, so A has finite order and $\langle A \rangle$ is a finite group.

The inverses are:
$I^{-1} = I$
$A^{-1} = A^{11}$
$(A^2)^{-1} = A^{10}$
$(A^3)^{-1} = A^9$
$(A^4)^{-1} = A^8$
$(A^5)^{-1} = A^7$
$(A^6)^{-1} = A^6$
$(A^7)^{-1} = A^5$
$(A^8)^{-1} = A^4$
$(A^9)^{-1} = A^3$
$(A^{10})^{-1} = A^2$
$(A^{11})^{-1} = A$

Since $\langle A \rangle$ is a cyclic group of order 12, then $\langle A \rangle$ is a finite cyclic group.

Since A is a generator, the generators are elements A^k such that $\gcd(k, 12) = 1$.

Therefore, there are $\phi(12) = 4$ generators and $k \in \{1, 5, 7, 11\}$, so the set of generators is $\{A, A^5, A^7, A^{11}\}$. $\square$

Exercise 50. Compute the cyclic subgroups of the quaternion group Q_8.

Solution. Every element of a group G generates a cyclic subgroup of G, so every element of Q_8 generates a cyclic subgroup of Q_8.

The cyclic subgroup generated by $a \in Q_8$ is the same as the cyclic subgroup generated by a^{-1}.

The inverses are:
$1^{-1} = 1$
$(-1)^{-1} = -1$
$i^{-1} = -i$
$(-i)^{-1} = i$
$j^{-1} = -j$
$(-j)^{-1} = j$
$k^{-1} = -k$
$(-k)^{-1} = k$

The cyclic subgroups generated by each element are shown below.
$\langle 1 \rangle = \{1\}$ and $|1| = 1$
$\langle -1 \rangle = \{1, -1\}$ and $|1| = 2$
$\langle i \rangle = \{1, i, -1, -i\}$ and $|i| = 4$
$\langle -i \rangle = \{1, -i, -1, i\}$ and $|-i| = 4$
$\langle j \rangle = \{1, j, -1, -j\}$ and $|j| = 4$
$\langle -j \rangle = \{1, -j, -1, j\}$ and $|-j| = 4$
$\langle k \rangle = \{1, k, -1, -k\}$ and $|k| = 4$
$\langle -k \rangle = \{1, -k, -1, k\}$ and $|-k| = 4$
Since the order of each element of Q_8 is not $|Q_8| = 8$, then Q_8 is not cyclic.

The subgroups of Q_8 are:
$Q_8 = \{1, -1, i, -i, j, -j, k, -k\}$
$\{1\}$
$\{1, -1\}$
$\{1, i, -1, -i\}$
$\{1, j, -1, -j\}$
$\{1, k, -1, -k\}$

$\square$

Exercise 51. Compute the elements of finite order in the group $(\mathbb{Z}, +)$.

Solution. The only subgroups of $\mathbb{Z}$ are $(n\mathbb{Z}, +)$ for each $n \in \mathbb{Z}$.

Each nonzero $n \in \mathbb{Z}$ generates a cyclic subgroup of $\mathbb{Z}$ of infinite order and $\langle n \rangle = n\mathbb{Z}$ is the set of all multiples of nonzero integer n.

When $n = 0$, the cyclic subgroup generated by $0 \in \mathbb{Z}$ is $\{0\}$, a finite group.

Thus, 0 has finite order 1.

Therefore, the only element of $\mathbb{Z}$ of finite order is 0. $\square$

Exercise 52. Compute the elements of finite order in the group $(\mathbb{Q}^*, \cdot)$.

Solution. The cyclic subgroup generated by $1 \in \mathbb{Q}^*$ is $\langle 1 \rangle = \{1^k : k \in \mathbb{Z}\} = \{1\}$, so 1 has finite order $|1| = 1$.

The cyclic subgroup generated by $-1 \in \mathbb{Q}^*$ is $\langle -1 \rangle = \{(-1)^k : k \in \mathbb{Z}\} = \{1, -1\}$, so -1 has finite order $|-1| = 2$.

All other elements of $\mathbb{Q}^*$ generate a cyclic subgroup of infinite order, so all other elements of $\mathbb{Q}^*$ have infinite order. $\square$

Exercise 53. Compute the elements of finite order in the group $(\mathbb{R}^*, \cdot)$.

Solution. The cyclic subgroup generated by $1 \in \mathbb{R}^*$ is $\langle 1 \rangle = \{1^k : k \in \mathbb{Z}\} = \{1\}$, so 1 has finite order $|1| = 1$.

The cyclic subgroup generated by $-1 \in \mathbb{R}^*$ is $\langle -1 \rangle = \{(-1)^k : k \in \mathbb{Z}\} = \{1, -1\}$, so -1 has finite order $|-1| = 2$.

All other elements of $\mathbb{R}^*$ generate a cyclic subgroup of infinite order, so all other elements of $\mathbb{R}^*$ have infinite order. $\square$

Exercise 54. Find a cyclic group with exactly one generator.

Solution. The trivial group $\{e\}$ where e is the identity is a cyclic group and $\langle e \rangle = \{e^k : k \in \mathbb{Z}\} = \{e\}$.

Hence, e is the only generator of the trivial group, so the trivial group has exactly one generator.

The group $(\mathbb{Z}_2, +)$ is a finite cyclic group of order 2, so there is $\phi(2) = 1$ generator of $\mathbb{Z}_2$.

The only generator of $\mathbb{Z}_2$ is $[1] \in \mathbb{Z}_2$, since $\langle [1] \rangle = \{k[1] : k \in \mathbb{Z}\} = \{[k] : k \in \mathbb{Z}\} = \{[0], [1]\} = \mathbb{Z}_2$. $\square$

Exercise 55. Find a cyclic group with exactly two generators.

Solution. The cyclic group $(\mathbb{Z}, +)$ has exactly two generators.

The generators are in the set $\{1, -1\}$ and $\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$.

The cyclic group $(n\mathbb{Z}, +)$ has exactly two generators for $n \in \mathbb{Z}, n \neq 0$.

The generators are in the set $\{n, -n\}$ and $n\mathbb{Z} = \langle n \rangle = \langle -n \rangle$.

The cyclic group $(\mathbb{Z}_3, +)$ has $\phi(3) = 2$ generators.

The generators of $\mathbb{Z}_3$ are in the set $\{[1], [2]\}$.

The cyclic group $(\mathbb{Z}_4, +)$ has $\phi(4) = 2$ generators.

The generators of $\mathbb{Z}_4$ are in the set $\{[1], [3]\}$.

The cyclic group $(\mathbb{Z}_6, +)$ has $\phi(6) = 2$ generators.

The generators of $\mathbb{Z}_6$ are in the set $\{[1], [5]\}$. $\square$

Exercise 56. Find a cyclic group with exactly four generators.

Solution. The cyclic group $(\mathbb{Z}_5, +)$ has $\phi(5) = 4$ generators.

The generators of $\mathbb{Z}_5$ are in the set $\{[1], [2], [3], [4]\}$.

The cyclic group $(\mathbb{Z}_8, +)$ has $\phi(8) = 4$ generators.

The generators of $\mathbb{Z}_8$ are in the set $\{[1], [3], [5], [7]\}$.

The cyclic group $(\mathbb{Z}_{10}, +)$ has $\phi(10) = 4$ generators.

The generators of $\mathbb{Z}_{10}$ are in the set $\{[1], [3], [7], [9]\}$.

The cyclic group $(\mathbb{Z}_{12}, +)$ has $\phi(12) = 4$ generators.
The generators of $\mathbb{Z}_{12}$ are in the set $\{[1], [5], [7], [11]\}$. $\square$

Exercise 57. Determine which groups $(\mathbb{Z}_n^*, \cdot)$ are cyclic for $n \leq 20$.

Solution. $(\mathbb{Z}_1^*, \cdot)$ is cyclic with generator 0 and $\mathbb{Z}_1^* = \{0\}$.
$(\mathbb{Z}_2^*, \cdot)$ is cyclic with generator 1 and $\mathbb{Z}_2^* = \{1\}$.
$(\mathbb{Z}_3^*, \cdot)$ is cyclic with generator 2 and $\mathbb{Z}_3^* = \{1, 2\}$.
$(\mathbb{Z}_4^*, \cdot)$ is cyclic with generator 3 and $\mathbb{Z}_4^* = \{1, 3\}$.
$(\mathbb{Z}_5^*, \cdot)$ is cyclic with generators $2, 3$ and $\mathbb{Z}_5^* = \{1, 2, 3, 4\}$.
$(\mathbb{Z}_6^*, \cdot)$ is cyclic with generator 5 and $\mathbb{Z}_6^* = \{1, 5\}$.
$(\mathbb{Z}_7^*, \cdot)$ is cyclic with generators $3, 5$ and $\mathbb{Z}_7^* = \{1, 2, 3, 4, 5, 6\}$.
$(\mathbb{Z}_8^*, \cdot)$ is not cyclic and $\mathbb{Z}_8^* = \{1, 3, 5, 7\}$.
$(\mathbb{Z}_9^*, \cdot)$ is cyclic with generators $2, 5$ and $\mathbb{Z}_9^* = \{1, 2, 4, 5, 7, 8\}$.
$(\mathbb{Z}_{10}^*, \cdot)$ is cyclic with generators $3, 7$ and $\mathbb{Z}_{10}^* = \{1, 3, 7, 9\}$.
$(\mathbb{Z}_{11}^*, \cdot)$ is cyclic with generators $2, 6, 7, 8$ and $\mathbb{Z}_{11}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$.
$(\mathbb{Z}_{12}^*, \cdot)$ is not cyclic and $\mathbb{Z}_{12}^* = \{1, 5, 7, 11\}$.
$(\mathbb{Z}_{13}^*, \cdot)$ is cyclic with generators $2, 6, 7, 11$ and $\mathbb{Z}_{13}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$.
$(\mathbb{Z}_{14}^*, \cdot)$ is cyclic with generators $3, 5$ and $\mathbb{Z}_{14}^* = \{1, 3, 5, 9, 11, 13\}$.
$(\mathbb{Z}_{15}^*, \cdot)$ is not cyclic and $\mathbb{Z}_{15}^* = \{1, 2, 4, 7, 8, 11, 13, 14\}$.
$(\mathbb{Z}_{16}^*, \cdot)$ is not cyclic and $\mathbb{Z}_{16}^* = \{1, 3, 5, 7, 9, 11, 13, 15\}$.
$(\mathbb{Z}_{17}^*, \cdot)$ is cyclic with generators $3, 5, 6, 7, 10, 11, 12, 14$ and $\mathbb{Z}_1^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16\}$
$(\mathbb{Z}_{18}^*, \cdot)$ is cyclic with generators $5, 11$ and $\mathbb{Z}_{18}^* = \{1, 5, 7, 11, 13, 17\}$.
$(\mathbb{Z}_{19}^*, \cdot)$ is cyclic with generators $2, 3, 10, 13, 14, 15$ and
$\mathbb{Z}_{19}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18\}$.
$(\mathbb{Z}_{20}^*, \cdot)$ is not cyclic and $\mathbb{Z}_{20}^* = \{1, 3, 7, 9, 11, 13, 17, 19\}$.

We conjecture that if $n > 2$ and $(\mathbb{Z}_n^*, \cdot)$ is cyclic, then one of the generators is prime. $\square$

Proof. Let $n \in \mathbb{Z}$ and $n > 2$.
Suppose $(\mathbb{Z}_n^*, \cdot)$ is cyclic.
Then $\mathbb{Z}_n^*$ has a generator.
Either a generator of $\mathbb{Z}_n^*$ is prime or a generator of $\mathbb{Z}_n^*$ is not prime.
We consider these cases separately.
Case 1: Suppose a generator of $\mathbb{Z}_n^*$ is prime.
Then $\mathbb{Z}_n^*$ has a prime generator.
Case 2: Suppose a generator of $\mathbb{Z}_n^*$ is not prime.
Then there exists $g \in \mathbb{Z}_n^*$ such that $\mathbb{Z}_n^* = \langle g \rangle$ and g is not prime.
Thus, g is composite.
Let S be the set of all generators of $\mathbb{Z}_n^*$ that are composite.
Then $S = \{g \in \mathbb{Z}_n^* : \mathbb{Z}_n^* = \langle g \rangle \text{ and } g \text{ is composite}\}$.
Thus, $g \in S$, so $S \neq \emptyset$.
Since $g \in S$, then $g \in \mathbb{Z}_n^*$, so $1 \leq g < n$ and $g \in \mathbb{Z}$.
Hence, $g \in \mathbb{Z}^+$, so $S \subset \mathbb{Z}^+$.
Since $S \subset \mathbb{Z}^+$ and $S \neq \emptyset$, then by well ordering principle of $\mathbb{Z}^+$, S has a least element.

Let a be the least element of S.

Then $a \in S$ and $a \leq s$ for all $s \in S$.

Since $a \in S$, then $a \in \mathbb{Z}_n^*$ and $\mathbb{Z}_n^* = \langle a \rangle$ and a is composite.

Since $a \in \mathbb{Z}_n^*$ and $n > 2$, then $1 < a < n$ and $\gcd(a, n) = 1$.

Since $a > 1$ and a is not prime, then a is composite.

Since a is a generator of $\mathbb{Z}_n^*$ and $|\mathbb{Z}_n^*| = \phi(n)$, then $|a| = \phi(n)$.

Since $|\mathbb{Z}_n^*| = \phi(n)$, then $\mathbb{Z}_n^*$ is a finite group.

Since $\mathbb{Z}_n^*$ is a finite cyclic group of order $\phi(n)$ and a is a generator of $\mathbb{Z}_n^*$, then the generators of $\mathbb{Z}_n^*$ are elements $a^k \pmod n \in \mathbb{Z}_n^*$ such that $\gcd(k, \phi(n)) = 1$.

Can we prove there exists $k \in \mathbb{Z}$ such that $a^k \pmod n \in \mathbb{Z}_n^*$ is prime and $|a^k \pmod n| = \phi(n)$?

Find $k \in \mathbb{Z}^+$ such that $p \equiv a^k \pmod n$ and p is prime and $\gcd(p, \phi(n)) = 1$.

Let p be a prime factor of a and we want p to generate all of $\mathbb{Z}_n^*$.

Then p is prime and $p|a$, so $a = pb$ for some integer b.

Since $p|a$, then $p \leq a$.

Since $p \leq a$ and $a < n$, then $p < n$.

Since a is in $\mathbb{Z}_n^*$, then $1 < a < n$ and $\gcd(a, n) = 1$.

Since $\gcd(a, n) = 1$, then there exist integers x, y such that $xa + ny = 1$.

Thus, $1 = xg + ny = x(pb) + ny = p(xb) + ny$ is a linear combination of p and n.

Hence, $\gcd(p, n) = 1$.

Since $1 < p < n$ and $\gcd(p, n) = 1$, then $p \in \mathbb{Z}_n^*$.

Somehow show that there exists $k \in \mathbb{Z}$ such that $g^k \equiv p \pmod n$.

Then we must prove $\gcd(k, \phi(n)) = 1$.

Then we can say that $|p| = |g^k| = \frac{\phi(n)}{\gcd(k,\phi(n))}$.

Choose p to be the prime factor of a tthat also generates all of $\mathbb{Z}_n^*$.

How do we know such a p exists??

TODO

$\square$

Exercise 58. If every subgroup of a group G is cyclic, then G is a cyclic group.

Proof. Let G be a group.

Suppose every subgroup of G is cyclic.

Since G is a subgroup of G, then this implies G is cyclic.

Since G is a group and G is cyclic, then G is a cyclic group. $\square$

Exercise 59. Every group with a finite number of subgroups is finite.

Solution. Observations/conjecture

1. If G is of infinite order, then there is at least one subgroup of G that is of infinite order, namely G itself. It appears there are an infinite number of such subgroups of G. Some subgroups of an infinite group are infinite while other subgroups of an infinite group can be finite. For example, the n^{th} roots of unity is a finite subgroup of the infinite circle group $\mathbb{T}$.

2. If G is of finite order n, then there are a finite number of subgroups of G and each subgroup has a finite number of elements, so each subgroup is of finite

order. Furthermore, there are at most n such subgroups of G and the order of each subgroup seems to divide the order of G. $\square$

Proof. Let $e \in G$ be the identity of G.

Either G is the trivial group or G is not the trivial group.

We consider these cases separately.

Case 1: Suppose G is the trivial group.

Then $G = \{e\}$, so G is finite.

The only subgroup of G is $\{e\}$, so G has exactly one subgroup.

Hence, G has a finite number of subgroups.

Thus, G has a finite number of subgroups and G is finite.

Therefore, if G has a finite number of subgroups, then G is finite, as desired.

Case 2: Suppose G is not the trivial group.

Then $G \neq \{e\}$, so there exists $a \in G$ such that $a \neq e$.

Suppose G has a finite number of subgroups.

Let n be the number of subgroups of G.

Then there are exactly n subgroups of G.

Since $\{e\}$ is a subgroup of G, then $n \geq 1$.

Since every element of G generates a cyclic subgroup of G and $a \in G$, then a generates a cyclic subgroup of G.

Let H be the cyclic subgroup generated by a.

Then $H = \{a^k : k \in \mathbb{Z}\}$.

Since $a \neq e$, then $a \notin \{e\}$.

Since $a = a^1$, then $a \in H$.

Since $a \in H$ and $a \notin \{e\}$, then $H \neq \{e\}$, so H is a non-trivial subgroup of G.

Suppose a has infinite order.

Then $H = \{..., a^{-2}, a^{-1}, e, a, a^2, a^3, ...\}$ and each power of a is distinct.

We prove $\langle a^i \rangle \neq \langle a^j \rangle$ for all $i, j \in \mathbb{Z}^+$ with $i \neq j$.

Let $i, j \in \mathbb{Z}^+$ with $i \neq j$.

Without loss of generality, assume $i < j$.

Suppose $a^i = a^{jk}$ for some integer k.

Suppose $k = 0$.

Then $a^i = a^{jk} = a^{j0} = a^0 = e$, so $a^i = e$.

Thus, $a^i = e$ for some $i \in \mathbb{Z}^+$, so a has finite order.

But, this contradicts a has infinite order, so $k \neq 0$.

Since $1 \leq i < j$, then $0 < \frac{i}{j} < 1$, so $\frac{i}{j} \notin \mathbb{Z}$.

Since $\frac{i}{j} \notin \mathbb{Z}$ and $k \in \mathbb{Z}$, then $\frac{i}{j} \neq k$, so $i \neq jk$.

Since $i \in \mathbb{Z}$ and $jk \in \mathbb{Z}$ and $a^i = a^{jk}$ and $i \neq jk$, then a has finite order.

But, this contradicts a has infinite order, so there is no integer k such that $a^i = a^{jk}$.

Hence, $a^i \notin \langle a^j \rangle$.
Since $a^i \in \langle a^i \rangle$ and $a^i \notin \langle a^j \rangle$, then $\langle a^i \rangle \neq \langle a^j \rangle$.
Thus, $\langle a^i \rangle \neq \langle a^j \rangle$ for all $i, j \in \mathbb{Z}^+$ with $i \neq j$.
Hence, each cyclic subgroup $\langle a^i \rangle$ is a distinct subgroup of G for all integers $i \geq 1$.
Therefore, there are at least $n+1$ distinct cyclic subgroups of G, so there are at least $n+1$ distinct subgroups of G.
But, this contradicts that there are exactly n subgroups of G.
Therefore, a cannot have infinite order, so a must have finite order.
Hence, H is finite.

Since $a \in G$ is arbitrary, then this implies every non-trivial subgroup of G is finite.
Since G is a subgroup of G and G is not the trivial subgroup, then we conclude G is finite, as desired. □

Exercise 60. Let G be a finite group of order n.
Let $a \in G$.
Then $|a| \leq n$.

Proof. Every element of a finite group has finite order.
Since G is a finite group and $a \in G$, then a has finite order.
The order of a is the order of the cyclic subgroup of G generated by a.
Hence, $|a| = |\langle a \rangle|$ and $\langle a \rangle$ is a subgroup of G.
Since $\langle a \rangle$ is a subgroup of G, then $\langle a \rangle$ is a subset of G.
Since $\langle a \rangle$ is a subset of G and G is finite and $|G| = n$, then $|\langle a \rangle| \leq n$.
Therefore, $|a| \leq n$. □

Exercise 61. A group of order n does not necessarily contain an element of order n.

Solution. Let $n = 4$.
Let $G = \{e, a, b, c\}$ be the Klein 4 group with identity e.
Then G is a group of order n.
Let $x \in G$
Either $x = e$ or $x \neq e$.
We consider these cases separately.
Case 1: Suppose $x = e$.
The order of the identity e is 1, so $|x| = 1 \neq n$.
Case 2: Suppose $x \neq e$.
The Klein 4 group has the property $x^2 = e$ for all $x \in G$.
Hence, $|x| = 2$, so $|x| \neq n$.
Therefore, the order of every element of G is not n, so there is no element of G that has order n. □

Proposition 62. *Let $(G, *)$ be a group with identity $e \in G$.*
Let $n \in \mathbb{Z}$.
If $a \in G$ has infinite order, then $a^n = e$ iff $n = 0$.

Proof. Suppose $a \in G$ has infinite order.

We prove if $n = 0$, then $a^n = e$.
Suppose $n = 0$.
Then $a^n = a^0 = e$, so $a^n = e$. $\square$

Proof. Conversely, we prove if $a^n = e$, then $n = 0$.
Suppose $a^n = e$.
Since a has infinite order, then there is no positive integer n such that $a^n = e$.

Suppose there is a negative integer n such that $a^n = e$.
Then $e = e^{-1} = (a^n)^{-1} = a^{-n}$.
Since n is a negative integer, then $-n$ is a positive integer.
Thus, there exists a positive integer $-n$ such that $a^{-n} = e$, so a has finite order.
But, this contradicts the fact that a has infinite order.
Therefore, there is no negative integer n such that $a^n = e$.

Since $a^0 = e$, then 0 is a solution to the equation $a^n = e$.
Since there is no positive integer n such that $a^n = e$ and there is no negative integer n such that $a^n = e$, then 0 is the only solution to the equation $a^n = e$.
Therefore, $n = 0$. $\square$

Lemma 63. *The order of every element in a cyclic group of finite order divides the order of the group.*

Proof. Let $(G, *)$ be a cyclic group of finite order n.
Since G is a cyclic group, then there exists a generator $g \in G$ such that $G = \{g^k : k \in \mathbb{Z}\}$.
Since G has finite order n, then $n \in \mathbb{Z}^+$ and $|G| = n$.
The order of g is the order of the cyclic subgroup generated by g.
Thus, $|g| = |G| = n$.

Let $a \in G$.
Then $a = g^k$ for some integer k.
Since G is a group of finite order, then G is a finite group.
Since every element of a finite group has finite order, then we conclude a has finite order.
Let $|a|$ be the order of a.
Then $|a| = |g^k| = \frac{n}{\gcd(k,n)}$, so $|a| \cdot \gcd(k, n) = n$.
Since $\gcd(k, n)$ is an integer, then $|a|$ divides n, so the order of a divides the order of G.
Since a is arbitrary, then the order of every element of G divides the order of G.
Therefore, the order of every element of a finite cyclic group divides the order of the group. $\square$

Exercise 64. If p is prime, then $(\mathbb{Z}_p, +)$ has no nontrivial proper subgroups.

Proof. Let p be prime.

We prove by contradiction.

Suppose $\mathbb{Z}_p$ has a nontrivial proper subgroup.

Let G be a nontrivial proper subgroup of $\mathbb{Z}_p$.

Then G is not the trivial subgroup and G is a proper subgroup of $\mathbb{Z}_p$.

Since G is not the trivial subgroup, then $G \neq \{[0]\}$.

Since G is a proper subgroup of $\mathbb{Z}_p$, then $G \neq \mathbb{Z}_p$.

Since G is a subgroup of $\mathbb{Z}_p$, then $G \subset \mathbb{Z}_p$.

Since G is a subgroup of $\mathbb{Z}_p$ and G is not the trivial subgroup, then G must have a non-identity element.

Let $[a]$ be a non-identity element of G.

Then $[a] \in G$ and $[a] \neq [0]$.

Since $[a] \in G$ and $G \subset \mathbb{Z}_p$, then $[a] \in \mathbb{Z}_p$.

Since $|\mathbb{Z}_p| = p$, then $\mathbb{Z}_p$ is a finite group.

Every element of a finite group has finite order.

Since $\mathbb{Z}_p$ is a finite group and $[a] \in \mathbb{Z}_p$, then $[a]$ has finite order.

Let k be the order of $[a]$.

Then k is the least positive integer such that $ka \equiv 0 \pmod{p}$.

By the previous lemma 63, the order of an element in a cyclic group of finite order divides the order of the group.

Since $\mathbb{Z}_p$ is a cyclic group of finite order p and $[a] \in \mathbb{Z}_p$, then the order of $[a]$ divides p, so $k|p$.

Since $k \in \mathbb{Z}^+$ and $k|p$, then k is a positive divisor of p.

Since p is prime, the only positive divisors of p are 1 and p.

Hence, either $k = 1$ or $k = p$.

Suppose $k = 1$.

Then $1 \cdot a \equiv 0 \pmod{p}$, so $a \equiv 0 \pmod{p}$.

Thus, $[a] = [0]$.

But, this contradicts $[a] \neq [0]$, so $k \neq 1$.

Hence, $k = p$.

The order of $[a]$ is the order of the cyclic subgroup of $\mathbb{Z}_p$ generated by $[a]$.

Let $(H, +)$ be the cyclic subgroup of $(\mathbb{Z}_p, +)$ generated by $[a]$.

Then $|H| = k = p = |\mathbb{Z}_p|$, so $|H| = |\mathbb{Z}_p|$.

The cyclic subgroup generated by $[a]$ is the smallest subgroup of $\mathbb{Z}_p$ that contains $[a]$.

Thus, H is the smallest subgroup of $\mathbb{Z}_p$ that contains $[a]$.

Hence, if G is a subgroup of $\mathbb{Z}_p$ that contains $[a]$, then H is a subgroup of G.

Since G is a subgroup of $\mathbb{Z}_p$ and $[a] \in G$, then we conclude H is a subgroup of G.

Since H is a subgroup of G, then $H \subset G$.
Since G is a subgroup of $\mathbb{Z}_p$, then $G \subset \mathbb{Z}_p$.
Since $H \subset G$ and $G \subset \mathbb{Z}_p$, then $H \subset G \subset \mathbb{Z}_p$, so $H \subset \mathbb{Z}_p$.
Since $\mathbb{Z}_p$ is a finite set and $H \subset \mathbb{Z}_p$ and $|H| = |\mathbb{Z}_p|$, then $H = \mathbb{Z}_p$.
Since $H \subset G \subset \mathbb{Z}_p$ and $H = \mathbb{Z}_p$, then we are forced to conclude $G = \mathbb{Z}_p$.
But, this contradicts $G \neq \mathbb{Z}_p$.
Therefore, G cannot be a nontrivial proper subgroup of $\mathbb{Z}_p$, so there is no nontrivial proper subgroup of $\mathbb{Z}_p$. ☐

Exercise 65. A group with no proper nontrivial subgroups is cyclic.

Proof. Let G be a group that has no proper nontrivial subgroups.
Let $e \in G$ be the identity of G.
Since the trivial group $\{e\}$ does not have any proper nontrivial subgroups, then G cannot be the trivial group, so $G \neq \{e\}$.
Since G is a group and G is not the trivial group, then G must contain a non identity element.
Let g be a non identity element of G.
Then $g \neq e$, so $g \notin \{e\}$.

Every element of a group G generates a cyclic subgroup of G.
Since $g \in G$, then g generates a cyclic subgroup of G.
Let H be the cyclic subgroup of G generated by g.
Then $H = \{g^n : n \in \mathbb{Z}\}$.
Since $g \in H$ and $g \notin \{e\}$, then $H \neq \{e\}$.
Thus, H is a nontrivial subgroup of G.
Since G has no proper nontrivial subgroups and H is a nontrivial subgroup of G, then H must be a non proper subgroup of G.
Thus, H must be G itself, so $H = G$.
Since $g \in G$ and $G = H$, then G is cyclic. ☐

Lemma 66. *Let $k, n \in \mathbb{Z}$.*
If $\gcd(k, n) = 1$*, then* $\gcd(n - k, n) = 1$.

Proof. Suppose $\gcd(k, n) = 1$.
Then there exist integers a and b such that $ak + bn = 1$.
Observe that

$$\begin{aligned}
1 &= ak + bn \\
&= 0 + (ak + bn) \\
&= (-an + an) + (ak + bn) \\
&= -an + (an + ak) + bn \\
&= -an + (ak + an) + bn \\
&= (-an + ak) + (an + bn) \\
&= (-a)(n - k) + (an + bn) \\
&= (-a)(n - k) + (a + b)n.
\end{aligned}$$

Since $1 = (-a)(n-k) + (a+b)n$ is a linear combination of $n-k$ and n, then $\gcd(n-k, n) = 1$. $\square$

Exercise 67. Let $n \in \mathbb{Z}^+$.

If $n > 2$, then $(\mathbb{Z}_n, +)$ has an even number of generators.

Proof. Suppose $n > 2$.

Since $(\mathbb{Z}_n, +)$ is a cyclic group, then the generators of $\mathbb{Z}_n$ are congruence classes $[k]$ such that $k \in \mathbb{Z}^+$ and $1 \leq k \leq n$ and $\gcd(k, n) = 1$.

Thus, the number of generators is the number of positive integers k such that $1 \leq k \leq n$ and $\gcd(k, n) = 1$.

By lemma 66, if $\gcd(k, n) = 1$, then $\gcd(n-k, n) = 1$, so $(k, n-k)$ is a pair of integers relatively prime to n.

Suppose $k = n - k$.

Then $2k = n$, so $k = \frac{n}{2}$.

Since $n = 2k$, then $k|n$, so $\gcd(k, n) = k = \frac{n}{2}$.

Since $n > 2$, then $\frac{n}{2} > 1$, so $\gcd(k, n) > 1$.

Hence, $\gcd(k, n) \neq 1$.

Thus, $k = n - k$ implies $\gcd(k, n) \neq 1$.

Since $\gcd(k, n)$ must equal 1, then $k \neq n - k$.

Therefore, $(k, n-k)$ is a pair of distinct integers.

Let t represent the number of k values such that $\gcd(k, n) = 1$ and $1 \leq k \leq n$.

Then the total number of positive integers relatively prime to n is $t * 2 = 2t$.

Therefore, $\mathbb{Z}_n$ has an even number of generators.

Note that $2t = \phi(n)$. $\square$

Exercise 68. Let p and q be distinct primes.

Find the number of generators of $(\mathbb{Z}_{pq}, +)$.

Solution. Since $(\mathbb{Z}_n, +)$ is a finite cyclic group of order $|\mathbb{Z}_n| = n$, then the generators of $\mathbb{Z}_n$ are positive integers that are relatively prime to the modulus n.

Therefore, the number of generators of $\mathbb{Z}_n$ is $\phi(n)$.

If p and q are distinct primes, then the number of generators of $(\mathbb{Z}_{pq}, +)$ is $\phi(pq) = (p-1)(q-1)$.

TODO

We should prove this conjecture! $\square$

Exercise 69. Let p be prime and r be a positive integer.

Find the number of generators of $(\mathbb{Z}_{p^r}, +)$.

Solution. Since $(\mathbb{Z}_n, +)$ is a finite cyclic group of order $|\mathbb{Z}_n| = n$, then the generators of $\mathbb{Z}_n$ are positive integers that are relatively prime to the modulus n.

Therefore, the number of generators of $\mathbb{Z}_n$ is $\phi(n)$.

If p is prime and r is a positive integer, then the number of generators of $(\mathbb{Z}_{p^r}, +)$ is $\phi(p^r) = (p-1) \cdot p^{r-1}$.

TODO We should prove this conjecture! $\square$

Proposition 70. *Let p be prime.*

Let $(\mathbb{Z}_p^*, \cdot)$ be the multiplicative group of nonzero elements of $\mathbb{Z}_p$.

If G is a finite subgroup of $\mathbb{Z}_p^*$, then G is cyclic.

Proof. TODO DO TIHS PROOF. $\square$

Exercise 71. Let $H = \{[x] \in \mathbb{Z}_{21}^* : x \equiv 1 \pmod 3\}$ and $K = \{[x] \in \mathbb{Z}_{21}^* : x \equiv 1 \pmod 7\}$.

Then $H < \mathbb{Z}_{21}^*$ and $K < \mathbb{Z}_{21}^*$.

Solution. Observe that $\mathbb{Z}_{21}^* = \{[1],[2],[4],[5],[8],[10],[11],[13],[16],[17],[19],[20]\}$ and $(\mathbb{Z}_{21}^*, \cdot)$ is an abelian group of order $\phi(21) = 12$.

We compute H and K and find that $H = \{[1],[4],[10],[13],[16],[19]\}$ and $K = \{[1],[8]\}$.

Observe that H is a subgroup of $\mathbb{Z}_{21}^*$.

Both $[10]$ and $[19]$ are generators of H, so H is a cyclic group and $H =< [10] >=< [19] >$ and $H = \{[10]^k : k \in \mathbb{Z}\} = \{[19]^k : k \in \mathbb{Z}\}$.

Observe that K is a subgroup of $\mathbb{Z}_{21}^*$.

The element $[8]$ is a generator of K, so K is a cyclic group and $K =< [8] >$ and $K = \{[8]^k : k \in \mathbb{Z}\}$.

To prove H and K are subgroups of $\mathbb{Z}_{21}^*$, we use the finite subgroup test since H and K are finite sets. $\square$

Proof. Observe that $\mathbb{Z}_{21}^* = \{[1],[2],[4],[5],[8],[10],[11],[13],[16],[17],[19],[20]\}$ and $(\mathbb{Z}_{21}^*, \cdot)$ is an abelian group of order $\phi(21) = 12$.

Since $\mathbb{Z}_{21}^* = \{[1],[2],[4],[5],[8],[10],[11],[13],[16],[17],[19],[20]\}$ and $H = \{[1],[4],[10],[13],[16],[19]\}$, then H is a nonempty finite subset of the group $(\mathbb{Z}_{21}^*, \cdot)$.

Let $[a],[b] \in H$.

Then $[a],[b] \in \mathbb{Z}_{21}^*$ and $a \equiv 1 \pmod 3$ and $b \equiv 1 \pmod 3$.

Thus, $[a][b] = [ab]$ and $ab \equiv 1 \pmod 3$.

By closure of $\mathbb{Z}_{21}^*$, $[a][b] \in \mathbb{Z}_{21}^*$, so $[ab] \in \mathbb{Z}_{21}^*$.

Since $[ab] \in \mathbb{Z}_{21}^*$ and $ab \equiv 1 \pmod 3$, then $[ab] \in H$.

Therefore, $[a][b] \in H$, so H is closed under multiplication modulo 21.

Since H is a nonempty finite subset of the group $(\mathbb{Z}_{21}^*, \cdot)$ and H is closed under multiplication modulo 21, then by the finite subgroup test, $H < \mathbb{Z}_{21}^*$. $\square$

Proof. Since $\mathbb{Z}_{21}^* = \{[1],[2],[4],[5],[8],[10],[11],[13],[16],[17],[19],[20]\}$ and $K = \{[1],[8]\}$, then K is a nonempty finite subset of the group $(\mathbb{Z}_{21}^*, \cdot)$.

Let $[a], [b] \in K$.
Then $[a], [b] \in \mathbb{Z}_{21}^*$ and $a \equiv 1 \pmod 7$ and $b \equiv 1 \pmod 7$.
Thus, $[a][b] = [ab]$ and $ab \equiv 1 \pmod 7$.
By closure of $\mathbb{Z}_{21}^*$, $[a][b] \in \mathbb{Z}_{21}^*$, so $[ab] \in \mathbb{Z}_{21}^*$.
Since $[ab] \in \mathbb{Z}_{21}^*$ and $ab \equiv 1 \pmod 7$, then $[ab] \in K$.
Therefore, $[a][b] \in K$, so K is closed under multiplication modulo 21.

Since K is a nonempty finite subset of the group $(\mathbb{Z}_{21}^*, \cdot)$ and K is closed under multiplication modulo 21, then by the finite subgroup test, $K < \mathbb{Z}_{21}^*$. □

Exercise 72. Let p be a prime number of the form $p = 2^n + 1$ for $n \in \mathbb{N}$.
Then the order of $[2]$ in $\mathbb{Z}_p^*$ is $2n$ and n is a power of 2.

Proof. Every element of a finite group has finite order.
Hence, $[2] \in \mathbb{Z}_p^*$ has finite order.
Let k be the order of $[2]$.
Then k is the least positive integer such that $[2]^k = [1]_p$.
Since $p = 2^n + 1$, then $p - 1 = 2^n$, so $(p-1)^2 = 2^{2n}$.
Hence, $p^2 - 2p + 1 = 2^{2n}$, so $p^2 - 2p = 2^{2n} - 1$.
Thus, $p(p-2) = 2^{2n} - 1$, so p divides $2^{2n} - 1$.
Hence, $2^{2n} \equiv 1 \pmod p$, so $[2^{2n}] = [1]_p$.
Thus, $[2]^{2n} = [1]_p$.
Since $[2]^{2n} = [1]$ iff $k|2n$, then $k|2n$.
We must prove $k = 2n$.
We're stuck.
□

Exercise 73. Let G be a group.
Let $a \in G$ such that $a \neq e$.
Prove or disprove:
a. The element a has order 2 iff $a^2 = e$.
b. The element a has order 3 iff $a^3 = e$.
c. The element a has order 4 iff $a^4 = e$.

Proof. Let e be the identity of G.
Let k be the order of a.
Then k is the least positive integer such that $a^k = e$.
We consider the statement $|a| = 2$ iff $a^2 = e$.

Suppose $|a| = 2$.
Then 2 is the least positive integer such that $a^2 = e$.
Hence, $a^2 = e$.

Conversely, suppose $a^2 = e$.
Since the order of a is k, then $a^2 = e$ iff $k|2$.
Thus, $k|2$.
Hence, either $k = 1$ or $k = 2$.
Suppose $k = 1$.
Then $e = a^1 = a$, so $a = e$.
Thus, we have $a = e$ and $a \neq e$, a contradiction.
Therefore, $k \neq 1$, so $k = 2$.
Hence, $|a| = 2$.

We consider the statement $|a| = 3$ iff $a^3 = e$.
Suppose $|a| = 3$.
Then 3 is the least positive integer such that $a^3 = e$.
Hence, $a^3 = e$.
Conversely, suppose $a^3 = e$.
Since the order of a is k, then $a^3 = e$ iff $k|3$.
Thus, $k|3$.
Hence, either $k = 1$ or $k = 3$.
Suppose $k = 1$.
Then $e = a^1 = a$, so $a = e$.
Thus, we have $a = e$ and $a \neq e$, a contradiction.
Therefore, $k \neq 1$, so $k = 3$.
Hence, $|a| = 3$.

We consider the statement $|a| = 4$ iff $a^4 = e$.
Suppose $|a| = 4$.
Then 4 is the least positive integer such that $a^4 = e$.
Hence, $a^4 = e$.
Conversely, suppose $a^4 = e$.
We disprove that $a^4 = e$ implies $|a| = 4$.
Let $G = \mathbb{Z}_5^*$, the group of units of $\mathbb{Z}_5$.
Observe that $[4]_5 \in \mathbb{Z}_5^*$ and $[4]^2 = [1]$ and $[4]^4 = [1]$.
Thus, the order of $[4]_5$ is 2.
Therefore, $[4]^4 = [1]$ and $|[4]| \neq 4$. $\square$

Exercise 74. What is the order of $[72]$ in $(\mathbb{Z}_{240}, +)$?

Solution. Since $(\mathbb{Z}_{240}, +)$ is a group of order 240, then $(\mathbb{Z}_{240}, +)$ is a finite group.
Every element of a finite group has finite order.
Hence, $[72] \in \mathbb{Z}_{240}$ has finite order.

Let k be the order of $[72]$.
Then k is the least positive integer such that $k[72] = [0]$.
Observe that $[0] = k[72] = [72] + [72] + ... + [72] = [72k]$, so $[72k] = [0]$.
Hence, $72k \equiv 0 \pmod{240}$, so $240|72k - 0$.
Hence, $240|72k$.
Thus, $2^4 * 3 * 5|2^3 * 3^2 k$, so $2 * 3 * 5|3^2 k$.
Hence, $2 * 5|3k$, so $10|3k$.
Since $\gcd(10, 3) = 1$ and $10|3k$, then $10|k$.
Thus, k is a multiple of 10.
The least positive multiple of 10 is 10 itself, so $k = 10$.
Hence, the order of $[72]$ is 10, so $[72]$ generates a cyclic subgroup of $\mathbb{Z}_{240}$ of order 10. □

Exercise 75. Let $a^{12} = e$ in a group G.
What are the possible orders of a?

Solution. Let G be a group with identity $e \in G$.
Let $a \in G$ such that $a^{12} = e$.
Then a has finite order.
Let n be the order of a.
Then $a^k = e$ iff $n|k$ for all $k \in \mathbb{Z}$.
Thus, $a^{12} = e$ iff $n|12$.
Since $a^{12} = e$, then $n|12$, so n must be a positive divisor of 12.
The set of positive divisors of 12 is $\{1, 2, 3, 4, 6, 12\}$.
Thus, n must be one of the numbers in the set $\{1, 2, 3, 4, 6, 12\}$.
Therefore, the set of possible orders of a is $\{1, 2, 3, 4, 6, 12\}$. □

Exercise 76. Let $a^{24} = e$ in a group G.
What are the possible orders of a?

Solution. Let G be a group with identity $e \in G$.
Let $a \in G$ such that $a^{24} = e$.
Then a has finite order.
Let n be the order of a.
Then $a^k = e$ iff $n|k$ for all $k \in \mathbb{Z}$.
Thus, $a^{24} = e$ iff $n|24$.
Since $a^{24} = e$, then $n|24$, so n must be a positive divisor of 24.
The set of positive divisors of 24 is $\{1, 2, 3, 4, 6, 8, 12, 24\}$.
Thus, n must be one of the numbers in the set $\{1, 2, 3, 4, 6, 8, 12, 24\}$.
Therefore, the set of possible orders of a is $\{1, 2, 3, 4, 6, 8, 12, 24\}$. □

Exercise 77. Let G be a group with identity $e \in G$.
If $b \in G$ and $b \neq e$ and $b^p = e$ for some prime p, compute the order of b.

Solution. Suppose $b \in G$ and $b \neq e$ and $b^p = e$ for some prime p.
Since p is prime, then $p \in \mathbb{Z}^+$.
Since there exists $p \in \mathbb{Z}^+$ such that $b^p = e$, then b has finite order.
Let n be the order of b.

Then $b^p = e$ iff $n|p$.
Since $b^p = e$, then $n|p$, so n is a positive divisor of p.
Since p is prime, the only positive divisors of p are 1 and p, so either $n = 1$ or $n = p$.
Since $b \neq e$, then the order of b must be greater than 1, so $n > 1$.
Hence, $n \neq 1$, so $n = p$.
Therefore, the order of b is $|b| = p$. $\square$

Exercise 78. Let G be a group.
If $a \in G$ and $|a| = 12$, compute the order of the elements $a, a^2, a^3, ..., a^{11}$.

Solution. Suppose $a \in G$ and $|a| = 12$.
Then a has finite order 12, so the order of a^s is $\frac{12}{\gcd(s,12)}$ for all $s \in \mathbb{Z}$.
We compute the order of a^s for $s \in \{1, 2, 3, ..., 11\}$.

s	a^s	$\lvert a^s \rvert$
1	a^1	$\lvert a^1\rvert = 12$
2	a^2	$\lvert a^2\rvert = 6$
3	a^3	$\lvert a^3\rvert = 4$
4	a^4	$\lvert a^4\rvert = 3$
5	a^5	$\lvert a^5\rvert = 12$
6	a^6	$\lvert a^6\rvert = 2$
7	a^7	$\lvert a^7\rvert = 12$
8	a^8	$\lvert a^8\rvert = 3$
9	a^9	$\lvert a^9\rvert = 4$
10	a^{10}	$\lvert a^{10}\rvert = 6$
11	a^{11}	$\lvert a^{11}\rvert = 12$

Note that 12 is the order of the cyclic subgroup generated by a and $\langle a \rangle = \{e, a, a^2, a^3, a^4, a^5, a^6, a^7, a^8, a^9, a^{10}, a^{11}\}$. $\square$

Exercise 79. Let $G = \{a_1, a_2, ..., a_n\}$ be a finite abelian group of order n with identity $e \in G$.
Let $x = a_1 a_2 \cdots a_n$.
Then $x^2 = e$.

Proof. Let H be the set of all inverses of all elements in G.
Since G is a group, then every element of G has a unique inverse in G.
Since G is finite and $G = \{a_1, a_2, ..., a_n\}$, then this implies $a_i \in G$ has an inverse $(a_i)^{-1} \in H$ for each i with $1 \leq i \leq n$.
Thus, $H = \{(a_1)^{-1}, (a_2)^{-1}, ..., (a_n)^{-1}\}$ and $H \subset G$.

We prove $G \subset H$.
Let $g \in G$.
Let h be the inverse of g.
Then $h \in H$ and $h = g^{-1}$.
Either $h = g$ or $h \neq g$.
We consider these cases separately.
Case 1: Suppose $h = g$.

Since $g = h$ and $h \in H$, then $g \in H$.
Case 2: Suppose $h \neq g$.
Since $h \in H$ and $H \subset G$, then $h \in G$.
Hence, h has an inverse in H.
Thus, $h^{-1} \in H$.
Since $h^{-1} = (g^{-1})^{-1} = g$, then $g \in H$.
Therefore, in all cases, $g \in H$.
Thus, $g \in G$ implies $g \in H$, so $G \subset H$.

Since $G \subset H$ and $H \subset G$, then $G = H$.

Since $x = a_1 a_2 \cdot ... \cdot a_n$ is a product of all elements of G and $H = G$, then x is the product of all elements of H.

Since G is abelian, then the order of factors of x does not matter, so $x = (a_1)^{-1} \cdot (a_2)^{-1} \cdot ... \cdot (a_n)^{-1}$.

Observe that

$$\begin{aligned}
x^2 &= x \cdot x \\
&= (a_1 a_2 \cdot ... \cdot a_n)((a_1)^{-1} \cdot (a_2)^{-1} \cdot ... \cdot (a_n)^{-1}) \\
&= a_1 a_2 \cdot ... \cdot a_n \cdot (a_1)^{-1} \cdot (a_2)^{-1} \cdot ... \cdot (a_n)^{-1} \\
&= (a_1 \cdot (a_1)^{-1}) \cdot (a_2 \cdot (a_2)^{-1}) \cdot ... \cdot (a_n \cdot (a_n)^{-1}) \\
&= e \cdot e ... \cdot e \\
&= e^n \\
&= e.
\end{aligned}$$

Therefore, $x^2 = e$, as desired. $\square$

Lemma 80. *Let a and b be elements of a group G.*
Then $(aba^{-1})^n = ab^n a^{-1}$ for all $n \in \mathbb{Z}$.

Solution. Define predicate $p(n) : (aba^{-1})^n = ab^n a^{-1}$ over $\mathbb{Z}$.
To prove $p(n)$ is true for all integers, we must prove
1. $p(0)$ is true.
2. $p(n)$ is true for all $n \in \mathbb{Z}^+$.
3. $p(-n)$ is true for all $n \in \mathbb{Z}^+$.

Let $e \in G$ be the identity of G. $\square$

Proof. We prove $p(0)$.
Observe that

$$\begin{aligned}
(aba^{-1})^0 &= e \\
&= aa^{-1} \\
&= aea^{-1} \\
&= ab^0 a^{-1}.
\end{aligned}$$

Therefore, $(aba^{-1})^0 = ab^0 a^{-1}$, so $p(0)$ is true. $\square$

Proof. We prove $p(n)$ is true for all $n \in \mathbb{Z}^+$ by induction on n.

Basis:

Since $(aba^{-1})^1 = aba^{-1} = ab^1a^{-1}$, then $p(1)$ is true.

Induction:

Let $k \in \mathbb{Z}^+$ such that $p(k)$ is true.

Then $(aba^{-1})^k = ab^ka^{-1}$.

Observe that

$$\begin{aligned}
(aba^{-1})^{k+1} &= (aba^{-1})^k(aba^{-1}) \\
&= (ab^ka^{-1})(aba^{-1}) \\
&= (ab^k)(a^{-1}a)(ba^{-1}) \\
&= (ab^k)e(ba^{-1}) \\
&= (ab^k)(ba^{-1}) \\
&= a(b^kb)a^{-1} \\
&= ab^{k+1}a^{-1}.
\end{aligned}$$

Thus, $p(k+1)$ is true, so $p(k)$ implies $p(k+1)$ for all $k \in \mathbb{Z}^+$.

Since $p(1)$ is true and $p(k)$ implies $p(k+1)$ for all $k \in \mathbb{Z}^+$, then by induction, $p(n)$ is true for all $n \in \mathbb{Z}^+$. $\square$

Proof. To prove $p(-n)$ for all $n \in \mathbb{Z}^+$, let $q(n) = p(-n)$.

Then $q(n)$ is $(aba^{-1})^{-n} = ab^{-n}a^{-1}$.

We must prove $q(n)$ is true for all $n \in \mathbb{Z}^+$.

We prove $q(n)$ for all $n \in \mathbb{Z}^+$ by induction on n.

Basis:

Since $(aba^{-1})^{-1} = (a^{-1})^{-1}b^{-1}a^{-1} = ab^{-1}a^{-1}$, then $q(1)$ is true.

Induction:

Let $k \in \mathbb{Z}^+$ such that $q(k)$ is true.

Then $(aba^{-1})^{-k} = ab^{-k}a^{-1}$.

Observe that

$$\begin{aligned}
(aba^{-1})^{-(k+1)} &= (aba^{-1})^{-k}(aba^{-1})^{-1} \\
&= (ab^{-k}a^{-1})(aba^{-1})^{-1} \\
&= (ab^{-k}a^{-1})(ab^{-1}a^{-1}) \\
&= (ab^{-k})(a^{-1}a)(b^{-1}a^{-1}) \\
&= (ab^{-k})e(b^{-1}a^{-1}) \\
&= (ab^{-k})(b^{-1}a^{-1}) \\
&= a(b^{-k}b^{-1})a^{-1} \\
&= ab^{-k-1}a^{-1} \\
&= ab^{-(k+1)}a^{-1}.
\end{aligned}$$

Thus, $q(k+1)$ is true, so $q(k)$ implies $q(k+1)$ for all $k \in \mathbb{Z}^+$.

Since $q(1)$ is true and $q(k)$ implies $q(k+1)$ for all $k \in \mathbb{Z}^+$, then by induction, $q(n)$ is true for all $n \in \mathbb{Z}^+$. $\square$

Exercise 81. Let G be a group with identity $e \in G$.

Let $a, b \in G$.

Then $|bab^{-1}| = |a|$.

Proof. Suppose a has finite order n.

Then n is the least positive integer such that $a^n = e$ and $a^k = e$ iff $n|k$ for all $k \in \mathbb{Z}$.

We left multiply by b to obtain $ba^n = be = b$, so $ba^n = b$.

We right multiply by b^{-1} to obtain $ba^n b^{-1} = bb^{-1} = e$, so $ba^n b^{-1} = e$.

Since we proved previously that $(aba^{-1})^n = ab^n a^{-1}$ for all $n \in \mathbb{Z}$ in lemma 80, then we conclude $(bab^{-1})^n = ba^n b^{-1}$ for all $n \in \mathbb{Z}$.

Thus, $(bab^{-1})^n = ba^n b^{-1} = e$, so $(bab^{-1})^n = e$.

Let $x = bab^{-1}$.

Then $x^n = e$.

Since there exists a positive integer n such that $x^n = e$, then x has finite order.

Let m be the order of x.

Then $m \in \mathbb{Z}^+$ and $x^m = e$ and $x^k = e$ iff m divides k for all $k \in \mathbb{Z}$.

In particular, $x^n = e$ iff $m|n$.

Since $x^n = e$, then we conclude $m|n$.

Since $e = x^m = (bab^{-1})^m = ba^m b^{-1}$, then we right multiply by b to obtain $b = eb = (ba^m b^{-1})b = (ba^m)(b^{-1}b) = ba^m e = ba^m$, so $b = ba^m$.

Hence, $be = b = ba^m$, so by the left cancellation law we have $e = a^m$.

Since $a^k = e$ iff $n|k$ for all $k \in \mathbb{Z}$ and $m \in \mathbb{Z}$, then $a^m = e$ iff $n|m$.

Since $a^m = e$, then we conclude $n|m$.

Thus, $m|n$ and $n|m$, so $m = n$.

Therefore, $|bab^{-1}| = |x| = m = n = |a|$, so $|bab^{-1}| = |a|$. □

Exercise 82. Let $(G, *)$ be a group.

Let $a \in G$.

For every $g \in G$, $|a| = |g^{-1}ag|$.

Proof. Let e be the identity of G.

Let $g \in G$.

Since G is a group, then the inverse of g is in G, so $g^{-1} \in G$.

By closure of G under $*$, we have $g^{-1}ag \in G$.

Every element of a group generates a cyclic subgroup of that group.

Thus, a and $g^{-1}ag$ each generate a cyclic subgroup of G.

Let H be the cyclic subgroup of G generated by a.

Then $H = \{a^k : k \in \mathbb{Z}\}$.

Let H' be the cyclic subgroup of G generated by $g^{-1}ag$.

Then $H' = \{(g^{-1}ag)^m : m \in \mathbb{Z}\}$.

Since $(aba^{-1})^n = ab^n a^{-1}$ for all $n \in \mathbb{Z}$, then $(g^{-1}ag)^m = (g^{-1}a(g^{-1})^{-1})^m = g^{-1}a^m(g^{-1})^{-1} = g^{-1}a^m g$ for all $m \in \mathbb{Z}$.

Thus, $H' = \{g^{-1}a^m g : m \in \mathbb{Z}\}$.

The order of an element is the order of the cyclic subgroup generated by that element.

Hence, $|a| = |H|$ and $|g^{-1}ag| = |H'|$.

To prove $|a| = |g^{-1}ag|$, we must prove $|H| = |H'|$.

Either a has finite order or a has infinite order.

We consider these cases separately.

Case 1: Suppose a has finite order.

Let n be the order of a.

Then n is the least positive integer such that $a^n = e$ and $H = \{a, a^2, a^3, ..., a^n\} = \{a^k : 1 \leq k \leq n\}$.

Let $f : H \to H'$ be a relation defined by $f(a^k) = (g^{-1}ag)^k$ for all integers k.

Since $(aba^{-1})^n = ab^na^{-1}$ for all $n \in \mathbb{Z}$, then $(g^{-1}ag)^k = (g^{-1}a(g^{-1})^{-1})^k = g^{-1}a^k(g^{-1})^{-1} = g^{-1}a^kg$ for all $k \in \mathbb{Z}$.

Thus, $(g^{-1}ag)^k = g^{-1}a^kg$ for all $k \in \mathbb{Z}$, so $f(a^k) = (g^{-1}ag)^k = g^{-1}a^kg$ for all integers k.

We prove f is a function.

Let $a^k \in H$. Then k is an integer. Observe that $f(a^k) = g^{-1}a^kg$. Since k is an integer, then $g^{-1}a^kg \in H'$, so $f(a^k) \in H'$.

Let $a^k, a^m \in H$ such that $a^k = a^m$. Then $k, m \in \mathbb{Z}$ such that $1 \leq k, m \leq n$.

Since a has finite order n, then $a^k = a^m$ iff $k \equiv m \pmod n$. Thus, $k \equiv m \pmod n$, so $n|(k - m)$. Thus, $\frac{k-m}{n}$ is an integer.

Let $s = k - m$. Since $1 \leq k \leq n$ and $1 \leq m \leq n$, then the maximum value of $|s|$ is $n - 1$. Hence, $0 \leq |s| \leq n - 1$, so $0 \leq |s| < n$. Since $n > 0$, we divide by n to obtain $0 \leq \frac{|s|}{n} < 1$.

Since $\frac{k-m}{n} \in \mathbb{Z}$, then $\frac{s}{n} \in \mathbb{Z}$, so $\frac{|s|}{n} \in \mathbb{Z}$. The only integer between zero and 1 and less than 1 is zero. Hence, $\frac{|s|}{n} = 0$, so $|s| = 0$. Thus, $|k - m| = 0$, so $k - m = 0$. Therefore, $k = m$, so $(g^{-1}ag)^k = (g^{-1}ag)^m$. Thus, $f(a^k) = f(a^m)$. Consequently, $a^k = a^m$ implies $f(a^k) = f(a^m)$, so f is well defined. Thus, f is a function.

Observe that $a^n = e = a^0$. Since f is a function, then $a^n = a^0$ implies $f(a^n) = f(a^0)$. Hence, $f(a^n) = f(a^0)$, so $(g^{-1}ag)^n = (g^{-1}ag)^0 = e$. Thus, $(g^{-1}ag)^n = e$, so $g^{-1}ag$ has finite order.

Let n' be the order of $g^{-1}ag$. Then n' is the least positive integer such that $(g^{-1}ag)^{n'} = e$. Thus, $H' = \{g^{-1}ag, (g^{-1}ag)^2, (g^{-1}ag)^3, ..., (g^{-1}ag)^{n'}\} = \{(g^{-1}ag)^m : 1 \leq m \leq n'\}$.

We prove f is injective.

Let $f(a^k) = f(a^m)$ for $a^k, a^m \in H$. Then $(g^{-1}ag)^k = (g^{-1}ag)^m$ and $k, m \in \mathbb{Z}$. Since $(g^{-1}ag)^k, (g^{-1}ag)^m \in H'$, then $1 \leq k, m \leq n'$.

Since n' is the order of $g^{-1}ag$, then $(g^{-1}ag)^k = (g^{-1}ag)^m$ iff $k \equiv m \pmod{n'}$. Hence, $k \equiv m \pmod{n'}$. Since $1 \leq k, m \leq n'$ and $k \equiv m \pmod{n'}$, then $k = m$. Thus, $a^k = a^m$. Therefore, $f(a^k) = f(a^m)$ implies $a^k = a^m$, so f is injective.

We prove f is surjective. Let $(g^{-1}ag)^m \in H'$. Then m is an integer such that $1 \leq m \leq n'$. Observe that $f(a^m) = (g^{-1}ag)^m$. Hence, there exists an integer m such that $f(a^m) = (g^{-1}ag)^m$, so f is surjective.

Therefore, $f : H \to H'$ is a bijective function, so $|H| = |H'|$. Thus, the order of a is the order of $g^{-1}ag$.

Note: We could further prove that f is a homomorphism and therefore f is an isomorphism of H with H', so that H is isomorphic to H'.

Hence, $|H| = |H'|$.

Case 2: Suppose a has infinite order.

Then H is of infinite order and each integer power of a is distinct. Thus, if k and m are integers such that $k \neq m$, then $a^k \neq a^m$. Thus, if $a^k = a^m$, then $k = m$.

Since the order of a is infinite, then $(H, *)$ is isomorphic to $(\mathbb{Z}, +)$.

Prove $|H| = |H'|$.

Let $f : H \to H'$ be a relation defined by $f(a^k) = (g^{-1}ag)^k$ for all integers k.

Since $(aba^{-1})^n = ab^na^{-1}$ for all $n \in \mathbb{Z}$, then $(g^{-1}ag)^k = (g^{-1}a(g^{-1})^{-1})^k = g^{-1}a^k(g^{-1})^{-1} = g^{-1}a^kg$ for all $k \in \mathbb{Z}$.

Thus, $(g^{-1}ag)^k = g^{-1}a^kg$ for all $k \in \mathbb{Z}$, so $f(a^k) = (g^{-1}ag)^k = g^{-1}a^kg$ for all integers k.

We prove f is a function.

Let $a^k \in H$. Then k is an integer. Observe that $f(a^k) = g^{-1}a^kg$. Since k is an integer, then $g^{-1}a^kg \in H'$, so $f(a^k) \in H'$.

Let $a^k, a^m \in H$ such that $a^k = a^m$. Then $k, m \in \mathbb{Z}$ such that $1 \leq k, m \leq n$.

Since a has finite order n, then $a^k = a^m$ iff $k \equiv m \pmod{n}$. Thus, $k \equiv m \pmod{n}$, so $n|(k - m)$. Thus, $\frac{k-m}{n}$ is an integer.

Let $s = k - m$. Since $1 \leq k \leq n$ and $1 \leq m \leq n$, then the maximum value of $|s|$ is $n - 1$. Hence, $0 \leq |s| \leq n - 1$, so $0 \leq |s| < n$. Since $n > 0$, we divide by n to obtain $0 \leq \frac{|s|}{n} < 1$.

Since $\frac{k-m}{n} \in \mathbb{Z}$, then $\frac{s}{n} \in \mathbb{Z}$, so $\frac{|s|}{n} \in \mathbb{Z}$. The only integer between zero and 1 and less than 1 is zero. Hence, $\frac{|s|}{n} = 0$, so $|s| = 0$. Thus, $|k - m| = 0$, so $k - m = 0$. Therefore, $k = m$, so $(g^{-1}ag)^k = (g^{-1}ag)^m$. Thus, $f(a^k) = f(a^m)$. Consequently, $a^k = a^m$ implies $f(a^k) = f(a^m)$, so f is well defined. Thus, f is a function.

Observe that $a^n = e = a^0$. Since f is a function, then $a^n = a^0$ implies $f(a^n) = f(a^0)$. Hence, $f(a^n) = f(a^0)$, so $(g^{-1}ag)^n = (g^{-1}ag)^0 = e$. Thus, $(g^{-1}ag)^n = e$, so $g^{-1}ag$ has finite order.

Let n' be the order of $g^{-1}ag$. Then n' is the least positive integer such that $(g^{-1}ag)^{n'} = e$. Thus, $H' = \{g^{-1}ag, (g^{-1}ag)^2, (g^{-1}ag)^3, ..., (g^{-1}ag)^{n'}\} = \{(g^{-1}ag)^m : 1 \leq m \leq n'\}$.

We prove f is injective. Let $f(a^k) = f(a^m)$ for $a^k, a^m \in H$. Then $(g^{-1}ag)^k = (g^{-1}ag)^m$ and $k, m \in \mathbb{Z}$. Since $(g^{-1}ag)^k, (g^{-1}ag)^m \in H'$, then $1 \leq k, m \leq n'$.

Since n' is the order of $g^{-1}ag$, then $(g^{-1}ag)^k = (g^{-1}ag)^m$ iff $k \equiv m \pmod{n'}$. Hence, $k \equiv m \pmod{n'}$. Since $1 \leq k, m \leq n'$ and $k \equiv m \pmod{n'}$, then $k = m$. Thus, $a^k = a^m$. Therefore, $f(a^k) = f(a^m)$ implies $a^k = a^m$, so f is injective.

We prove f is surjective. Let $(g^{-1}ag)^m \in H'$. Then m is an integer such that $1 \leq m \leq n'$. Observe that $f(a^m) = (g^{-1}ag)^m$. Hence, there exists an integer m such that $f(a^m) = (g^{-1}ag)^m$, so f is surjective. $\square$

Exercise 83. Not every element of an infinite group has finite order.
Let

$$A = \begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix}$$

and

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

be elements of $GL_2(\mathbb{R})$.
Show that $|A| = 3$ and $|B| = 4$.
Show that AB has infinite order.

Solution. Let I be the identity 2×2 matrix.
Since

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

and

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

and $AA^{-1} = I = A^{-1}A$ and $BB^{-1} = I = B^{-1}B$, then $A, B \in GL_2(\mathbb{R})$.

We compute the integer powers of A.

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

$$A^3 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

Therefore, $|A| = 3$ and 3 is the order of the cyclic subgroup generated by A.
Thus, $\langle A \rangle = \{I, A, A^2\}$.

We compute the integer powers of B.

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

$$B^3 = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$$

$$B^4 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

Therefore, $|B| = 4$ and 4 is the order of the cyclic subgroup generated by B. Thus, $\langle B \rangle = \{I, B, B^2, B^3\}$.

We compute AB.

$$AB = \begin{bmatrix} 1 & 0 \\ -1 & 1 \end{bmatrix}$$

□

Proof. We prove for all $n \in \mathbb{Z}^+$,

$$(AB)^n = \begin{bmatrix} 1 & 0 \\ -n & 1 \end{bmatrix}.$$

Define the predicate $p(n)$ over $\mathbb{Z}$:

$$(AB)^n = \begin{bmatrix} 1 & 0 \\ -n & 1 \end{bmatrix}$$

We prove $p(n)$ is true for all $n \in \mathbb{Z}^+$ by induction on n.
Basis:
Since

$$(AB)^1 = \begin{bmatrix} 1 & 0 \\ -1 & 1 \end{bmatrix}$$

then $p(1)$ is true.

Induction:
Let $k \in \mathbb{Z}^+$ such that $p(k)$ is true.
Then

$$(AB)^k = \begin{bmatrix} 1 & 0 \\ -k & 1 \end{bmatrix}.$$

Observe that

$$(AB)^{k+1} = (AB)^k(AB) = \begin{bmatrix} 1 & 0 \\ -k & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ -1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ -k-1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ -(k+1) & 1 \end{bmatrix}$$

Therefore, $p(k+1)$ is true, so $p(k)$ implies $p(k+1)$ for all $k \in \mathbb{Z}^+$.

Since $p(1)$ is true and $p(k)$ implies $p(k+1)$ for all $k \in \mathbb{Z}^+$, then by PMI, $p(n)$ is true for all $n \in \mathbb{Z}^+$.
Therefore, for all $n \in \mathbb{Z}^+$,

$$(AB)^n = \begin{bmatrix} 1 & 0 \\ -n & 1 \end{bmatrix}.$$

Hence, for all $n \in \mathbb{Z}^+$,

$$(AB)^n \neq \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

Thus, there is no $n \in \mathbb{Z}^+$ such that

$$(AB)^n = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

Therefore, AB has infinite order. $\square$

Exercise 84. Let

$$A = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$$

and

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

be elements of $GL_2(\mathbb{R})$.

Show that A and B have finite orders, but AB has infinite order.

Solution. Let I be the identity 2×2 matrix.

Since

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

and

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

and $AA^{-1} = I = A^{-1}A$ and $BB^{-1} = I = B^{-1}B$, then $A, B \in GL_2(\mathbb{R})$.

We compute the integer powers of A.

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

$$A^3 = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$$

$$A^4 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

Therefore, $|A| = 4$ and 4 is the order of the cyclic subgroup generated by A.

Thus, $\langle A \rangle = \{I, A, A^2, A^3\}$.

We compute the integer powers of B.

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

$$B^3 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

Therefore, $|B| = 3$ and 3 is the order of the cyclic subgroup generated by B.

Thus, $\langle B \rangle = \{I, B, B^2\}$.

We compute AB.

$$AB = \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix}$$

$\square$

Proof. We prove for all $n \in \mathbb{Z}^+$,

$$(AB)^n = \begin{bmatrix} 1 & -n \\ 0 & 1 \end{bmatrix}$$

Define the predicate $p(n)$ over $\mathbb{Z}$:

$$(AB)^n = \begin{bmatrix} 1 & -n \\ 0 & 1 \end{bmatrix}$$

We prove $p(n)$ is true for all $n \in \mathbb{Z}^+$ by induction on n.
Basis:
Since

$$(AB)^1 = \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix}$$

then $p(1)$ is true.
Induction:
Let $k \in \mathbb{Z}^+$ such that $p(k)$ is true.
Then

$$(AB)^k = \begin{bmatrix} 1 & -k \\ 0 & 1 \end{bmatrix}.$$

Observe that

$$(AB)^{k+1} = (AB)^k(AB) = \begin{bmatrix} 1 & -k \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & -1-k \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & -(k+1) \\ 0 & 1 \end{bmatrix}$$

Therefore, $p(k+1)$ is true, so $p(k)$ implies $p(k+1)$ for all $k \in \mathbb{Z}^+$.

Since $p(1)$ is true and $p(k)$ implies $p(k+1)$ for all $k \in \mathbb{Z}^+$, then by PMI, $p(n)$ is true for all $n \in \mathbb{Z}^+$.

Therefore, for all $n \in \mathbb{Z}^+$,

$$(AB)^n = \begin{bmatrix} 1 & -n \\ 0 & 1 \end{bmatrix}.$$

Hence, for all $n \in \mathbb{Z}^+$,

$$(AB)^n \neq \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

Thus, there is no $n \in \mathbb{Z}^+$ such that

$$(AB)^n = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

Therefore, AB has infinite order. $\square$

Exercise 85. Compute i^{45}.

Solution. Since the 4^{th} roots of unity $(U_4, \cdot)$ is a group and $i \in U_4$ has finite order 4, then $i^s = i^t$ iff $s \equiv t \pmod 4$ for all $s, t \in \mathbb{Z}$.

Thus, $i^s = i^{45}$ iff $s \equiv 45 \pmod 4$.

Since $45 \pmod 4 = 1$, then $i^s = i^{45}$ iff $s \equiv 1 \pmod 4$.

Let $s = 1$.

Since $1 \equiv 1 \pmod 4$, then $s \equiv 1 \pmod 4$, so $i^s = i^{45}$.

Therefore, $i = i^1 = i^{45}$, so $i^{45} = i$. $\square$

Exercise 86. Compute $(-i)^{10}$.

Solution. Observe that

$$\begin{aligned}
(-i)^{10} &= i^{10} \\
&= i^{4*2+2} \\
&= i^{4*2} * i^2 \\
&= (i^4)^2 * i^2 \\
&= (1)^2 * (-1) \\
&= 1 * (-1) \\
&= -1.
\end{aligned}$$

Therefore, $(-i)^{10} = -1$. $\square$

Exercise 87. Every non-abelian group has order at least 6, so every group of order $2, 3, 4$, or 5 is abelian.

Proof. TODO ☐

Exercise 88. If every non-identity element of a group G has order 2, then G is abelian.

Proof. Let G be a group with identity $e \in G$.
Suppose every non-identity element of G has order 2.
Then $a^2 = e$ for all $a \in G$ with $a \neq e$.
Let $a \in G$ and $a \neq e$.
Then $e = a^2 = aa$, so $a^{-1} = a$.
Hence, a is its own inverse.
Therefore, each non-identity element of G is its own inverse.
Since the identity e is its own inverse, then each element of G is its own inverse.
Therefore, $a^{-1} = a$ for all $a \in G$.

Let $a, b \in G$.
Then $a^{-1} = a$ and $b^{-1} = b$ and $(ab)^{-1} = ab$.
Observe that

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

Therefore, $ab = ba$ for all $a, b \in G$, so G is abelian. ☐

Exercise 89. If a group has even order, then it contains an element of order 2.

Proof. TODO ☐

Exercise 90. Let G be a group of order 4 that contains no element of order 4.
a. No element of G has order 3.
b. Explain why every non-identity element of G has order 2.
c. Denote the elements of G by e, a, b, c and write out the Cayley table for G.

Proof. TODO ☐

Exercise 91. Let G be a group with identity $e \in G$.
Let $a, b \in G$ and $|a| = 5$ and $b \neq e$ and $aba^{-1} = b^2$.
Compute $|b|$.

Solution. Let n be the order of b.
Since $b \neq e$, then $n > 1$.

Suppose $n = 2$.
Then $b^2 = e$.
Thus $e = b^2 = aba^{-1}$, so $e = aba^{-1}$.
Thus, $ae = a = ea = aba^{-1}(a) = abe = ab$, so $ae = ab$.
By cancellation law, we obtain $e = b$, so $b = e$.
But, this contradicts that $b \neq e$.
Therefore, $b^2 \neq e$.
TODO □

Exercise 92. Let G be a group.

If $(ab)^i = a^i * b^i$ for three consecutive integers i and all $a, b \in G$, then G is abelian.

Proof. TODO □

Exercise 93. Let G be a nonempty finite set with an associative operation $\cdot$ such that for all $a, b, c, d \in G$, if $ab = ac$, then $b = c$ and if $bd = cd$, then $b = c$.

Then $(G, \cdot)$ is a group.

Show that this may be false if G is an infinite set.

Proof. TODO □

Exercise 94. Let G be a nonempty set with an associative operation $\cdot$ such that for all $a, b \in G$, the equations $ax = b$ and $ya = b$ have solutions.

Then $(G, \cdot)$ is a group.

Proof. TODO □

Exercise 95. Let G be an abelian group in which every element has finite order.

If $c \in G$ is an element of largest order in G (that is, $|a| \leq |c|$ for all $a \in G$), then the order of every element of G divides $|c|$.

Proof. TODO □

Exercise 96. The element $\sqrt{3}$ in the multiplicative group $(\mathbb{R}^*, *)$ has infinite order.

Proof. We prove $\sqrt{3}^n > 1$ for every positive integer n by induction.
Let $p(n)$ be the predicate $\sqrt{3}^n > 1$.
Let $n = 1$.
Then $\sqrt{3}^n = \sqrt{3}^1 = \sqrt{3} > 1$.
Hence, $p(1)$ is true.

Suppose m is an arbitrary positive integer such that $p(m)$ is true.
Then $\sqrt{3}^m > 1$.
Thus, $\sqrt{3}^m * \sqrt{3} > 1 * \sqrt{3}$, so $\sqrt{3}^{m+1} > \sqrt{3}$.
Since $\sqrt{3}^{m+1} > \sqrt{3}$ and $\sqrt{3} > 1$, then $\sqrt{3}^{m+1} > 1$.
Hence, $p(m+1)$ is true, so $p(m)$ implies $p(m+1)$.
Therefore, by induction, $\sqrt{3}^n > 1$ for all positive integers n.
Thus, $\sqrt{3} \neq 1$ for all positive integers n.
Hence, there does not exist a positive integer such that $\sqrt{3} = 1$.
Therefore, the order of $\sqrt{3}$ is infinite. $\square$

Exercise 97. Compute the order of $([15], [25]) \in \mathbb{Z}_{24} \times \mathbb{Z}_{30}$.
What is the largest possible order of an element in $\mathbb{Z}_{24} \times \mathbb{Z}_{30}$?
Is $\mathbb{Z}_{24} \times \mathbb{Z}_{30}$ cyclic?

Solution. Observe that

$$\begin{aligned} |([15],[25])| &= lcm(|[15]_{24}|, |[25]_{30}|) \\ &= lcm(\frac{24}{\gcd(15,24)}, \frac{30}{\gcd(25,30)}) \\ &= lcm(8,6) \\ &= 24. \end{aligned}$$

Thus, $([15], [25])$ generates a cyclic subgroup of $\mathbb{Z}_{24} \times \mathbb{Z}_{30}$ of order 24.

Suppose $\mathbb{Z}_{24} \times \mathbb{Z}_{30}$ is cyclic.
Then $\mathbb{Z}_{24} \times \mathbb{Z}_{30}$ is a cyclic group of order $|\mathbb{Z}_{24} \times \mathbb{Z}_{30}| = 24 * 30 = 720$.
Hence, $\mathbb{Z}_{24} \times \mathbb{Z}_{30}$ is isomorphic to $\mathbb{Z}_{720}$, so $\mathbb{Z}_{24} \times \mathbb{Z}_{30} \cong \mathbb{Z}_{720}$.
Since $\mathbb{Z}_{24} \times \mathbb{Z}_{30} \cong \mathbb{Z}_{720}$ iff $\gcd(24,30) = 1$ and $\gcd(24,30) = 6 \neq 1$, then $\mathbb{Z}_{24} \times \mathbb{Z}_{30} \ncong \mathbb{Z}_{720}$.
Hence, we have a contradiction, so $\mathbb{Z}_{24} \times \mathbb{Z}_{30}$ cannot be cyclic.
Therefore, there is no element of $\mathbb{Z}_{24} \times \mathbb{Z}_{30}$ of order 720.

Let $([a], [b]) \in \mathbb{Z}_{24} \times \mathbb{Z}_{30}$ have maximum order k.
Then $k = lcm(|[a]|, |[b]|)$.
Let $k_1 = |[a]|$ and $k_2 = |[b]|$.
Then $k = \frac{k_1 k_2}{\gcd(k_1,k_2)}$ and k has the maximum value.
The maximum value occurs when the product $k_1 k_2$ is maximized.
Hence, $k_1 = 24$ and $k_2 = 30$ and $\gcd(24, 30) = 6$.
Therefore, $k = \frac{24*30}{6} = 120$. $\square$

Exercise 98. A cyclic group with only one generator can have at most 2 elements.

Solution. The statement means:
Let $\langle G, * \rangle$ be a cyclic group.
If G has exactly one generator then G has at most 2 elements.
Let $P_1 : \langle G, * \rangle$ is a cyclic group.
Let $P_2 : G$ has exactly one generator.
Let $P_3 : |G| \leq 2$.
The statement to prove is: $P_1 \to (P_2 \to P_3)$.
We use direct proof.
Thus we assume P_1.
We must prove: $P_2 \to P_3$.
We can use direct proof by assuming P_2 and proving P_3 or use proof by contrapositive and prove $\neg P_3 \to \neg P_2$. □

Proof. Let $\langle G, * \rangle$ be a cyclic group.
Suppose G has exactly one generator.
Let $g \in G$ be the unique generator of G.
Since G is cyclic, by definition of cyclic group, $G = \langle g \rangle$.
Since G is a group, then the identity element exists.
Let $e \in G$ be the identity element.
Thus, $g \in G$ and $e \in G$.
Either $g = e$ or $g \neq e$.
We consider these cases separately.
There are two cases to consider.
Case 1: Suppose $g = e$.
Then $G = \langle g \rangle = \langle e \rangle$.
Thus G is the trivial group, so $|G| = 1$.
Case 2: Suppose $g \neq e$.
Since G is a group, by definition of group, $g^{-1} \in G$.
Either $g^{-1} = g$ or $g^{-1} \neq g$.
There are two cases to consider.
Case 2a: Suppose $g^{-1} = g$.
Then by definition of inverse element, $e = gg^{-1} = gg = g^2$.
Thus $g^3 = g^2 g = eg = g$.
Thus $g^4 = g^3 g = gg = e$.
Thus $g^5 = g^4 g = eg = g$.
Thus $g^6 = g^5 g = gg = e$, and so on.
Thus $g^{-2} = g^{-1} g^{-1} = gg = e$.
Thus $g^{-3} = g^{-2} g^{-1} = eg = g$.
Thus $g^{-4} = g^{-3} g^{-1} = gg = e$, and so on.
Hence, if n is even then $g^n = e$ and if n is odd then $g^n = g$.
Technically we should use induction to prove that $g^n = e$ if n is even and $g^n = g$ if n is odd.
Thus, $\langle g \rangle$ contains only two elements, g and e, so $|G| = |\langle g \rangle| = 2$.
Case 2b: Suppose $g^{-1} \neq g$.
Then $g^{-1} \neq e$ and $g^{-1} \neq g$.
Hence, g^{-1} is some other element in G.

Thus, e, g, and g^{-1} are distinct elements of G.
Hence G contains 3 elements, so $|G| > 2$.
Let $h \in G$ such that $h = g^{-1}$.
Then $gh = hg = e$ and $h \neq e$ and $h \neq g$.
Thus, $G = \{e, g, h\}$.

We must determine g^2.
If $g^2 = e$, then $gg = e$ so $g^{-1} = g$.
Thus, $g^{-1} = g$ and $g^{-1} \neq g$, a contradiction.
Hence $g^2 \neq e$.
If $g^2 = g$, then $gg = g$.
Since $eg = g = gg$, then by right cancellation law, $e = g$.
Thus, $g = e$ and $g \neq e$, a contradiction.
Hence, $g^2 \neq g$.
Thus, $g^2 \neq e$ and $g^2 \neq g$, so $g^2 = h$.

We must determine h^2.
If $h^2 = h$, then $hh = h$.
Since $eh = h$, then $hh = eh$.
Thus by right cancellation law, $h = e$.
Since $h = g^{-1}$, then $g^{-1} = e$.
Hence, $g^{-1} = e$ and $g^{-1} \neq e$, a contradiction.
Therefore, $h^2 \neq h$.
If $h^2 = e$, then $hh = e$.
Since h and g are inverses, then $hg = e$.
Thus, $hh = hg$.
By left cancellation law, $h = g$, so $g^{-1} = g$.
Hence, $g^{-1} = g$ and $g^{-1} \neq g$, a contradiction.
Therefore, $h^2 \neq e$.
Thus, $h^2 \neq h$ and $h^2 \neq e$, so $h^2 = g$.
Observe that $h^1 = h, h^2 = g, h^3 = h^2h = gh = e, h^4 = h^3h = eh = h, h^5 = hh = g, h^6 = gh = e, h^7 = eh = h, ...$ and so on.
Also, $h^0 = e$ and $h^{-1} = g, h^{-2} = gg = h, h^{-3} = hg = e, h^{-4} = hh = g, h^{-5} = gg = h, h^{-6} = hg = e, ...$ and so on.
Thus, $\langle h \rangle = \{h^n : n \in \mathbb{Z}\} = G$, so h is a generator of G.
Similarly, $\langle g \rangle = \{g^n : n \in \mathbb{Z}\} = G$, so g is a generator of G.
Hence, if $|G| > 2$, then G does not have a unique generator. □

Exercise 99. Let G be a cyclic group of finite order n generated by x.
If $y = x^k$ and $\gcd(k, n) = 1$, then y is a generator of G.

Proof. Since G is a cyclic group generated by $x \in G$, then $G = \langle x \rangle = \{x^k : k \in \mathbb{Z}\}$.
Let $y \in G$.
Then there exists an integer k such that $y = x^k$.
Suppose $\gcd(k, n) = 1$.

Every element of a finite group has finite order.
Since G is a finite group and $x \in G$, then x has finite order.
The order of x is the order of the cyclic subgroup of G generated by x.
Hence, $\langle x \rangle = \{e, x, x^2, x^3, ..., x^{n-1}\}$ and $|x| = |\langle x \rangle| = |G| = n$.
Since x has finite order n, then the order of y is

$$\begin{aligned} |y| &= |x^k| \\ &= \frac{|x|}{\gcd(k, |x|)} \\ &= \frac{n}{\gcd(k, n)} \\ &= \frac{n}{1} \\ &= n. \end{aligned}$$

Thus, $|y| = n$.
The order of y is the order of the cyclic subgroup of G generated by y.
Hence, $|\langle y \rangle| = |y| = n = |G|$, so $|\langle y \rangle| = |G|$.
Since $\langle y \rangle$ is a subgroup of G, then $\langle y \rangle$ is a subset of G.
Since G is a finite set and $\langle y \rangle$ is a subset of G and $|\langle y \rangle| = |G|$, then $\langle y \rangle = G$.
Since $y \in G$ and $G = \langle y \rangle$, then y is a generator of G. ∎

Exercise 100. Let $(G, *)$ be a group.
Let $g, h \in G$ such that $|g| = 15$ and $|h| = 16$.
Then the order of $\langle g \rangle \cap \langle h \rangle$ is 1.

Proof. Let A be the cyclic subgroup of G generated by $g \in G$.
Then $A = \langle g \rangle$ and $|A| = |\langle g \rangle| = |g| = 15$.
Let B be the cyclic subgroup of G generated by $h \in G$.
Then $B = \langle h \rangle$ and $|B| = |\langle h \rangle| = |h| = 16$.
The intersection of any two subgroups is a subgroup.
Since $A < G$ and $B < G$, then $A \cap B < G$.
Let $K = A \cap B$.
Then $K < G$. ∎

Proof. We prove $K < A$ and $K < B$.
Since $K = A \cap B$ and $A \cap B$ is a subset of A and of B, then $K \subset A$ and $K \subset B$.
Let $e \in G$ be the identity of G.
Since $K < G$, then $e \in K$, so $K \neq \emptyset$.
Since $|A| = 15$, then A is a finite group, so A is a finite set.
Every subset of a finite set is finite.
Since A is finite and $K \subset A$, then K is finite.
Since $K \subset A$ and $K \neq \emptyset$ and K is finite, then K is a nonempty finite subset of A.
Since $K \subset B$ and $K \neq \emptyset$ and K is finite, then K is a nonempty finite subset of B.

We prove K is closed under $*$.

Let $a, b \in K$.

Since $a \in K$, then $a \in A$ and $a \in B$, so $a = g^p$ for some integer p and $a = h^q$ for some integer q.

Since $b \in K$, then $b \in A$ and $b \in B$, so $b = g^r$ for some integer r and $b = h^s$ for some integer s

Thus, $ab = g^p * g^r$ and $ab = h^q * h^s$.

Since $ab = g^p * g^r = g^{p+r}$ and $p + r$ is an integer, then $ab \in A$.

Since $ab = h^q * h^s = h^{q+s}$ and $q + s$ is an integer, then $ab \in B$.

Hence, $ab \in A$ and $ab \in B$, so $ab \in A \cap B$.

Therefore, $ab \in K$, so K is closed under $*$.

Since K is closed under $*$ and $*$ is the binary operation of A, then K is closed under the binary operation of A.

Since K is closed under $*$ and $*$ is the binary operation of B, then K is closed under the binary operation of B.

Since K is a nonempty finite subset of A and K is closed under the binary operation of A, then by the finite subgroup test, $K < A$.

Since K is a nonempty finite subset of B and K is closed under the binary operation of B, then by the finite subgroup test, $K < B$. $\square$

Proof. Every subgroup of a cyclic group is cyclic.

Since $K < A$ and A is a cyclic group, then we conclude K is cyclic.

Hence, there exists a generator $k \in K$ such that $K = \langle k \rangle$.

Since $k \in K$ and $K = A \cap B$, then $k \in A$ and $k \in B$.

Since K is a finite set and K is a group, then K is a finite group.

Every element of a finite group has finite order.

Since K is a finite group and $k \in K$, then k has finite order.

Let n be the order of k.

Then $n \in \mathbb{Z}^+$.

By lemma 63, the order of every element of a finite cyclic group divides the order of the group.

Since A is a finite cyclic group, then the order of every element of A divides the order of A.

Since $k \in A$, then n divides $|A|$, so $n|15$.

Since the order of every element of a finite cyclic group divides the order of the group and B is a finite cyclic group, then the order of every element of B divides the order of B.

Since $k \in B$, then n divides $|B|$, so $n|16$.

Since $n|15$ and $n|16$, then n is a common divisor of 15 and 16.

Any common divisor of 15 and 16 divides $\gcd(15, 16)$.

Thus, n divides $\gcd(15, 16)$.

Since $\gcd(15, 16) = 1$, then n divides 1.

Since $n \in \mathbb{Z}^+$ and $n|1$, then $n = 1$.

Since $|\langle g \rangle \cap \langle h \rangle| = |A \cap B| = |K| = |\langle k \rangle| = |k| = n = 1$, then the order of $\langle g \rangle \cap \langle h \rangle$ is 1. $\square$

Lemma 101. *Let $(G, *)$ be a group with identity $e \in G$.*

Let $g, h \in G$ such that $|g| = m$ and $|h| = n$ and $\gcd(m, n) = 1$.

Then the order of $\langle g \rangle \cap \langle h \rangle$ is 1 *and $\langle g \rangle \cap \langle h \rangle = \{e\}$.*

Proof. Let A be the cyclic subgroup of G generated by $g \in G$.

Then $A = \langle g \rangle$ and $|A| = |\langle g \rangle| = |g| = m$.

Let B be the cyclic subgroup of G generated by $h \in G$.

Then $B = \langle h \rangle$ and $|B| = |\langle h \rangle| = |h| = n$.

The intersection of any two subgroups is a subgroup.

Since $A < G$ and $B < G$, then $A \cap B < G$.

Let $K = A \cap B$.

Then $K < G$. $\square$

Proof. We prove $K < A$ and $K < B$.

Since $K = A \cap B$ and $A \cap B$ is a subset of A and of B, then $K \subset A$ and $K \subset B$.

Since $K < G$, then $e \in K$, so $K \neq \emptyset$.

Since $|A| = m$, then A is a finite group, so A is a finite set.

Every subset of a finite set is finite.

Since A is finite and $K \subset A$, then K is finite.

Since $K \subset A$ and $K \neq \emptyset$ and K is finite, then K is a nonempty finite subset of A.

Since $K \subset B$ and $K \neq \emptyset$ and K is finite, then K is a nonempty finite subset of B.

We prove K is closed under $*$.

Let $a, b \in K$.

Since $a \in K$, then $a \in A$ and $a \in B$, so $a = g^p$ for some integer p and $a = h^q$ for some integer q.

Since $b \in K$, then $b \in A$ and $b \in B$, so $b = g^r$ for some integer r and $b = h^s$ for some integer s

Thus, $ab = g^p * g^r$ and $ab = h^q * h^s$.

Since $ab = g^p * g^r = g^{p+r}$ and $p + r$ is an integer, then $ab \in A$.

Since $ab = h^q * h^s = h^{q+s}$ and $q + s$ is an integer, then $ab \in B$.

Hence, $ab \in A$ and $ab \in B$, so $ab \in A \cap B$.

Therefore, $ab \in K$, so K is closed under $*$.

Since K is closed under $*$ and $*$ is the binary operation of A, then K is closed under the binary operation of A.

Since K is closed under $*$ and $*$ is the binary operation of B, then K is closed under the binary operation of B.

Since K is a nonempty finite subset of A and K is closed under the binary operation of A, then by the finite subgroup test, $K < A$.

Since K is a nonempty finite subset of B and K is closed under the binary operation of B, then by the finite subgroup test, $K < B$. $\square$

Proof. Every subgroup of a cyclic group is cyclic.

Since $K < A$ and A is a cyclic group, then we conclude K is cyclic.

Hence, there exists a generator $k \in K$ such that $K = \langle k \rangle$.

Since $k \in K$ and $K = A \cap B$, then $k \in A$ and $k \in B$.

Since K is a finite set and K is a group, then K is a finite group.

Every element of a finite group has finite order.

Since K is a finite group and $k \in K$, then k has finite order.

Let c be the order of k.

Then $c \in \mathbb{Z}^+$.

By lemma 63, the order of every element of a finite cyclic group divides the order of the group.

Since A is a finite cyclic group, then the order of every element of A divides the order of A.

Since $k \in A$, then c divides $|A|$, so $c|m$.

Since the order of every element of a finite cyclic group divides the order of the group and B is a finite cyclic group, then the order of every element of B divides the order of B.

Since $k \in B$, then c divides $|B|$, so $c|n$.

Since $c|m$ and $c|n$, then c is a common divisor of m and n.

Any common divisor of m and n divides $\gcd(m,n)$.

Thus, c divides $\gcd(m,n)$.

Since $\gcd(m,n) = 1$, then c divides 1.

Since $c \in \mathbb{Z}^+$ and $c|1$, then $c = 1$.

Since $|\langle g \rangle \cap \langle h \rangle| = |A \cap B| = |K| = |\langle k \rangle| = |k| = c = 1$, then the order of $\langle g \rangle \cap \langle h \rangle$ is 1.

The only group of order 1 is the trivial group.

Therefore, $\langle g \rangle \cap \langle h \rangle = \{e\}$. □

Exercise 102. Let a be an element of a group G with identity $e \in G$.

Let $m, n \in \mathbb{Z}$.

Find a generator for the subgroup $\langle a^m \rangle \cap \langle a^n \rangle$.

Solution. Let's try experimentation.

Let $A = \langle a^m \rangle$ be the cyclic subgroup generated by a^m.

Let $B = \langle a^n \rangle$ be the cyclic subgroup generated by a^n.

The intersection of any two subgroups is a subgroup.

Since A is a subgroup and B is a subgroup, the $A \cap B$ is a subgroup of G.

Let $K = A \cap B$.

We must find a generator for K.

If $m = 0$, then $A = \langle a^0 \rangle = \langle e \rangle = \{e\}$, so $K = A \cap B = \{e\} \cap B = \{e\}$.

Assume the order is finite and $m \leq n$.

If $m = 1 = n$, then $A = \langle a^1 \rangle = \langle a \rangle = B$, so $K = A \cap B = A \cap A = A = \langle a \rangle$.

If $m = 1$ and $n = 2$, then $A = \langle a^1 \rangle = \langle a \rangle$ and $B = \langle a^2 \rangle$.

Now, let's assume order of A is some fixed value, say 12, so $|a| = 12$.

TODO □

Theorem 103. *Order of* ab *is the least common multiple of the orders of* a *and* b*.*

Let G be a group and $a, b \in G$.

If $ab = ba$ and a has finite order m and b has finite order n, then ab has finite order $lcm(m,n)$.

Proof. Suppose $ab = ba$ and a has finite order m and b has finite order n.

Since a has finite order m, then m is the least positive integer such that $a^m = e$.

Since b has finite order n, then n is the least positive integer such that $b^n = e$.

Observe that

$$\begin{aligned}
(ab)^{mn} &= a^{mn} \cdot b^{mn} \\
&= a^{mn} \cdot b^{nm} \\
&= (a^m)^n \cdot (b^n)^m \\
&= e^n \cdot e^m \\
&= e \cdot e \\
&= e.
\end{aligned}$$

Since mn is a positive integer and $(ab)^{mn} = e$, then ab has finite order. □

Proof. Let t be the order of ab.

Then t is the least positive integer such that $(ab)^t = e$.

Since $ab = ba$, then $e = (ab)^t = a^t b^t$.

Since $e = a^t b^t$, then we conclude $a^t = e$ and $b^t = e$.

Since a has finite order m, then $a^t = e$ iff $m|t$.

Since $a^t = e$, then we conclude $m|t$.

Since b has finite order n, then $b^t = e$ iff $n|t$.

Since $b^t = e$, then we conclude $n|t$.

Since $m|t$ and $n|t$, then t is a multiple of m and n.

Since t is the least positive integer such that $(ab)^t = e$, then t must be the least common multiple of m and n.

Therefore, $t = lcm(m,n)$, so the order of ab is $lcm(m,n)$, as desired. □

Corollary 104. *Let G be a group $a, b \in G$*

If $ab = ba$ and a has finite order m and b has finite order n and $\gcd(m,n) = 1$, then ab has finite order mn.

Proof. Suppose $ab = ba$ and a has finite order m and b has finite order n and $\gcd(m,n) = 1$.

Since $ab = ba$ and a has finite order m and b has finite order n, then by the previous theorem 103, ab has finite order $lcm(m,n)$.

Observe that

$$\begin{aligned}
lcm(m,n) &= \frac{mn}{\gcd(m,n)} \\
&= \frac{mn}{1} \\
&= mn.
\end{aligned}$$

Since $lcm(m, n) = mn$, then ab has finite order mn. $\square$

Exercise 105. torsion subgroup of an abelian group

The set of all elements of finite order in an abelian group G is a subgroup of G.

This is the torsion subgroup of G.

Proof. Let $(G, *)$ be an abelian group with identity $e \in G$.

Let S be the set of all elements of G that have finite order.

Then $S = \{a \in G : a \text{ has finite order}\}$.

Thus, $S \subset G$.

We prove $S \neq \emptyset$.

Since $e^1 = e$, then the order of e is 1, so e has finite order.

Since $e \in G$ and e has finite order, then $e \in S$, so $S \neq \emptyset$.

Since $S \subset G$ and $S \neq \emptyset$, then S is a nonempty subset of G. $\square$

Proof. We prove S is closed under $*$ of G.

Let $a, b \in S$.

Since $a \in S$, then $a \in G$ and a has finite order.

Since $b \in S$, then $b \in G$ and b has finite order.

Since G is a group, then G is closed under $*$.

Since $a \in G$ and $b \in G$, then we conclude $ab \in G$.

We prove ab has finite order.

Since a has finite order, let m be the order of a.

Then a has finite order m.

Since b has finite order, let n be the order of b.

Then b has finite order n.

Since G is abelian and $ab \in G$, then $ab = ba$.

Since $ab = ba$ and a has finite order m and b has finite order n, then by the previous theorem 103, ab has finite order $lcm(m, n)$, so ab has finite order.

Since $ab \in G$ and ab has finite order, then $ab \in S$.

Therefore, $ab \in S$ for all $a, b \in S$. $\square$

Proof. We prove S is closed under inverses.

Let $s \in S$.

Then $s \in G$ and s has finite order.

Let t be the order of s.

Then t is the least positive integer such that $s^t = e$.

Since G is a group and $s \in G$, then $s^{-1} \in G$ and $ss^{-1} = s^{-1}s = e$.

Since the order of an element is the order of its inverse, then the order of s is the order of s^{-1}.

Hence, t is the order of s^{-1}, so t is the least positive integer such that $(s^{-1})^t = e$.

Therefore, s^{-1} has finite order.

Since $s^{-1} \in G$ and s^{-1} has finite order, then $s^{-1} \in S$.

Therefore, $s^{-1} \in S$ for all $s \in S$. $\square$

Proof. Since S is a nonempty subset of G and $ab \in S$ for all $a, b \in S$ and $s^{-1} \in S$ for all $s \in S$, then by the two-step subgroup test, S is a subgroup of G, so $S < G$. $\square$

Exercise 106. Let G be an abelian group that contains a pair of cyclic subgroups of order 2.

Then G must contain a subgroup of order 4.

Proof. Let C_1 and C_2 be a pair of cyclic subgroups of G of order 2.

Let $e \in G$ be the identity of G.

Since C_1 is a cyclic subgroup of G of order 2, then $C_1 = \langle a \rangle$ for some generator $a \in G$.

Thus, $C_1 = \{e, a\}$ and $a \neq e$.

The order of an element is the order of the cyclic subgroup generated by the element.

Thus, $|a| = |C_1| = 2$, so 2 is the least positive integer such that $a^2 = e$.

Since C_2 is a cyclic subgroup of G of order 2, then $C_2 = \langle b \rangle$ for some generator $b \in G$.

Thus, $C_2 = \{e, b\}$ and $b \neq e$ and $|b| = 2$.

The order of an element is the order of the cyclic subgroup generated by the element.

Thus, $|b| = |C_2| = 2$, so 2 is the least positive integer such that $b^2 = e$.

Since C_1 and C_2 are distinct cyclic subgroups of order 2, then $C_1 \neq C_2$.

Hence, $\{e, a\} \neq \{e, b\}$, so $a \neq b$.

Suppose $ab = a$.

Then $ab = a = ae$, so by cancellation we obtain $b = e$.

But, this contradicts $b \neq e$, so $ab \neq a$.

Suppose $ab = b$.

Then $ab = b = eb$, so by cancellation we obtain $a = e$.

But, this contradicts $a \neq e$, so $ab \neq b$.

Assume $ab \neq e$ and let $H = \{e, a, b, ab\}$.

Then $H \subset G$ and $|H| = 4$.

Observe that $a(ab) = (aa)b = a^2b = eb = b$.

Since G is abelian, then

$(ab)a = a(ab) = (aa)b = a^2b = eb = b$ and

$ba = ab$ and

$(ab)b = b(ab) = b(ba) = (bb)a = b^2a = ea = a$ and

$(ab)(ab) = (ab)(ba) = a(b^2)a = aea = aa = a^2 = e$.

We construct the Cayley table for H.

$*$	e	a	b	ab
e	e	a	b	ab
a	a	e	ab	b
b	b	ab	e	a
ab	ab	b	a	e

Since H is a nonempty finite subset of G and H is closed under $*$ of G, then by the finite subgroup test, H is a subgroup of G.

Therefore, H is a subgroup of order 4.

Observe that H is not cyclic and H is the Klein-4 group. $\square$

Exercise 107. Let G be an abelian group of order mn.

If $a \in G$ has order m and $b \in G$ has order n and $\gcd(m,n) = 1$, then G is cyclic.

Proof. Suppose $a \in G$ has order m and $b \in G$ has order n and $\gcd(m,n) = 1$.

Since G is abelian and $a \in G$ and $b \in G$, then $ab = ba$.

Since $ab = ba$ and a has finite order m and b has finite order n and $\gcd(m,n) = 1$, then by the previous corollary 104, ab has finite order mn.

Hence, $|ab| = mn$.

The order of ab is the order of the cyclic subgroup of G generated by ab.

Let $\langle ab \rangle$ be the cyclic subgroup of G generated by ab.

Then $|ab| = |\langle ab \rangle|$.

Since G has order mn, then $|G| = mn$.

Thus, $|G| = mn = |ab| = |\langle ab \rangle|$, so $|G| = |\langle ab \rangle|$.

Since $\langle ab \rangle$ is a subgroup of G, then $\langle ab \rangle$ is a subset of G.

Since $\langle ab \rangle$ is a subset of G and G is finite and $|\langle ab \rangle| = |G|$, then $\langle ab \rangle = G$.

Since $ab \in G$ and $G = \langle ab \rangle$, then G is cyclic, as desired. $\square$

Exercise 108. For all positive integers n, -1 is an n^{th} root of unity if and only if n is even.

Proof. Let $n \in \mathbb{Z}^+$.

Suppose n is even.

Then $n = 2k$ for some integer k.

The number $z \in \mathbb{C}$ is an n^{th} root of unity if $z^n = 1$.

Since $(-1)^n = (-1)^{2k} = [(-1)^2]^k = 1^k = 1$, then -1 is an n^{th} root of unity.

Conversely, suppose -1 is an n^{th} root of unity.

Then $(-1)^n = 1$.

Either n is even or n is odd.

Suppose n is odd.

Then $n = 2m + 1$ for some integer m.

Observe that

$$\begin{aligned} 1 &= (-1)^n \\ &= (-1)^{2m+1} \\ &= (-1)^{2m} \cdot (-1)^1 \\ &= [(-1)^2]^m \cdot (-1) \\ &= (1^m)(-1) \\ &= 1(-1) \\ &= -1. \end{aligned}$$

Hence, $1 = -1$, a contradiction.
Therefore, n cannot be odd, so n must be even. $\square$

Exercise 109. Let $m, n \in \mathbb{Z}^+$.
Let $d = \gcd(m, n)$.
Let $a \in \mathbb{C}^*$.
Then $a^m = a^n = 1$ iff $a^d = 1$.

Proof. Suppose $a^d = 1$.
Since $d = \gcd(m, n)$ then d is a positive integer and $d|m$ and $d|n$.
Hence, there exist integers k_1 and k_2 such that $m = dk_1$ and $n = dk_2$.
Observe that

$$\begin{aligned} a^m &= a^{dk_1} \\ &= (a^d)^{k_1} \\ &= 1^{k_1} \\ &= 1. \end{aligned}$$

and

$$\begin{aligned} a^n &= a^{dk_2} \\ &= (a^d)^{k_2} \\ &= 1^{k_2} \\ &= 1. \end{aligned}$$

Therefore, $a^m = 1 = a^n$, as desired.

Conversely, suppose $a^m = 1$ and $a^n = 1$.
Let $\langle a \rangle$ be the cyclic group subgroup of $(\mathbb{C}^*, \cdot)$ generated by a with identity 1.
Since $m \in \mathbb{Z}^+$ and $a^m = 1$, then a has finite order.
Let t be the order of a.
Then t is the least positive integer such that $a^t = 1$.
Since a has finite order t, then $a^k = 1$ iff $t|k$ for all integers k.

Since $a^m = 1$ and $m \in \mathbb{Z}$, then $t|m$.
Since $a^n = 1$ and $n \in \mathbb{Z}$, then $t|n$.
Since $t|m$ and $t|n$, then t is a common divisor of m and n.
Any common divisor of m and n divides $\gcd(m,n)$, so t divides $\gcd(m,n)$.
Hence, $t|d$.
Since $t|d$ and $d \in \mathbb{Z}$, then we conclude $a^d = 1$, as desired. $\square$

Exercise 110. Let $z \in \mathbb{C}^*$.
If $|z| \neq 1$, then z has infinite order.

Proof. Suppose $|z| \neq 1$.
We prove z has infinite order by contradiction.
Suppose z does not have infinite order.
Then z has finite order, so there exists a positive integer n such that $z^n = 1$.
Observe that

$$\begin{aligned} 0 &= 1 - 1 \\ &= |1| - 1 \\ &= |z^n| - 1 \\ &= |z|^n - 1. \end{aligned}$$

Hence, $|z|^n - 1 = 0$.
Since $|z| \in \mathbb{R}$ and $n \in \mathbb{Z}^+$ and $|z|^n - 1 = (|z| - 1)\sum_{k=0}^{n-1} |z|^k$ for all $n \in \mathbb{Z}^+$, then $|z|^n - 1 = (|z| - 1)\sum_{k=0}^{n-1} |z|^k$.
Thus, $0 = |z|^n - 1 = (|z| - 1)\sum_{k=0}^{n-1} |z|^k$, so $|z| - 1 = 0$.
Consequently, $|z| = 1$.
But, this contradicts the assumption $|z| \neq 1$.
Therefore, z has infinite order. $\square$

Exercise 111. Let $z \in \mathbb{T}$ such that $z = \cos\theta + i\sin\theta$ and $\theta \in \mathbb{Q}^*$.
Then z has infinite order.

Proof. We prove by contradiction.
Suppose z does not have infinite order.
Then z has finite order, so there exists a positive integer n such that $z^n = 1$.
Since $\theta \in \mathbb{Q}^*$, then there exist nonzero integers a and b such that $\theta = \frac{a}{b}$.
Since $a \neq 0$ and $b \neq 0$, then $\theta \neq 0$.
Observe that

$$\begin{aligned} e^{i0} &= 1 \\ &= z^n \\ &= (cis\theta)^n \\ &= (e^{i\theta})^n \\ &= e^{in\theta} \\ &= e^{in\frac{a}{b}}. \end{aligned}$$

Thus, $e^{i0} = e^{i\frac{na}{b}}$, so $0 = \frac{na}{b}$.
Since $b \neq 0$, the multiply both sides to obtain $0 = na$.
Since $a \neq 0$, then divide to obtain $0 = n$.
Since $n \in \mathbb{Z}^+$, then $n > 0$, so $n \neq 0$.
Hence, we have $n = 0$ and $n \neq 0$, a contradiction.
Therefore, z has infinite order. $\square$

Exercise 112. Let $(G, *)$ be an abelian group.
Let H be a finite cyclic subgroup of order p.
Let K be a finite cyclic subgroup of order q.
Then G contains a cyclic subgroup of order $lcm(p, q)$.
If $\gcd(p, q) = 1$, then G contains a cyclic subgroup of order pq.

Proof. Every element of G generates a cyclic subgroup of G.

Let H be the finite cyclic subgroup of G generated by $a \in G$. Then $H = \{a^k : k \in \mathbb{Z}\}$ and $|a| = p$. Let K be the finite cyclic subgroup of G generated by $b \in G$. Then $H = \{b^k : k \in \mathbb{Z}\}$ and $|b| = q$.

Let $g = ab$. Since G is closed under its binary operation, then $g \in G$. Let M be the cyclic subgroup of G generated by g. Then $M = \{(ab)^k : k \in \mathbb{Z}\}$ and $|M| = |ab|$.

We prove ab has finite order. Since $|a| = p$ and $|b| = q$, then p and q are the least positive integers such that $a^p = e$ and $b^q = e$. Since p and q are positive integers, then so is pq. Observe that

$$\begin{aligned} (ab)^{pq} &= a^{pq}b^{pq} \\ &= (a^p)^q b^{qp} \\ &= e^q (b^q)^p \\ &= ee^p \\ &= e^p \\ &= e. \end{aligned}$$

Hence, there exists a positive integer pq such that $(ab)^{pq} = e$.
Thus, ab has finite order.
Let k be the order of ab.
Then k is the least positive integer such that $(ab)^k = e$.
Let c be a multiple of q such that $c \equiv 1 \pmod p$.
This is NOT CORRECT because c may not exist, so the subsequent logic of this proof will not work.
Then $c = qm$ for some integer m.
Since a has finite order p and $c \equiv 1 \pmod p$, then $a^c = a^1$.

Thus,

$$\begin{aligned}
(ab)^c &= a^c b^c \\
&= a^c b^{qm} \\
&= a^c (b^q)^m \\
&= a^c (e)^m \\
&= a^c e \\
&= a^c \\
&= a^1 \\
&= a.
\end{aligned}$$

Therefore,

$$\begin{aligned}
p &= |a| \\
&= |(ab)^c| \\
&= \frac{|ab|}{\gcd(c, |ab|)} \\
&= \frac{k}{\gcd(c, k)}.
\end{aligned}$$

Hence, $p * \gcd(c, k) = k$.

Since $\gcd(c, k)$ is an integer, then $p|k$.

Let d be a multiple of p such that $d \equiv 1 \pmod{q}$.

Then $d = pn$ for some integer n and $b^d = b^1$ since $|b| = q$.

Thus,

$$\begin{aligned}
(ab)^d &= a^d b^d \\
&= a^{pn} b^d \\
&= (a^p)^n b^d \\
&= (e)^n b^d \\
&= e b^d \\
&= b^d \\
&= b^1 \\
&= b.
\end{aligned}$$

Therefore,

$$\begin{aligned}
q &= |b| \\
&= |(ab)^d| \\
&= \frac{|ab|}{\gcd(d, |ab|)} \\
&= \frac{k}{\gcd(d, k)}.
\end{aligned}$$

Hence, $q * \gcd(d, k) = k$.
Since $\gcd(d, k)$ is an integer, then $q|k$.
Thus, we have $p|k$ and $q|k$, so k is a multiple of p and q.
The least positive multiple of p and q is the least common multiple of p and q.
Hence, $k = lcm(p, q)$.
Suppose $\gcd(p, q) = 1$.
Then

$$\begin{aligned} k &= lcm(p, q) \\ &= \frac{pq}{\gcd(p, q)} \\ &= \frac{pq}{1} \\ &= pq. \end{aligned}$$

□

Exercise 113. If G is a finite group with an element g of order 5 and an element h of order 7, then $|G| \geq 35$.

Solution. The hypothesis is:
G is a finite group.
$g, h \in G$ such that $|g| = 5$ and $|h| = 7$.
We must prove $|G| \geq 35$. □

Proof. Since G is a finite group, then the order of G is some positive integer, say n.
We must prove $n \geq 35$.
Every element of a finite group has finite order.
Moreover, the order of an element of a finite group divides the order of the group.
Hence, $|g|$ divides n and $|h|$ divides n.
Thus, $5|n$ and $7|n$, so n is a multiple of 5 and 7.
Therefore, n is a multiple of 35.
The least positive multiple of 35 is the least common multiple of 35, namely 35.
Therefore, $n \geq 35$. □

Exercise 114. Let G be a group.
Let $a, b \in G$ such that $|b| = 2$ and $ba = a^2b$.
What is the order of a?

Solution. Let e be the identity of G.
Either $a = e$ or $a \neq e$.
We consider these cases separately.
Case 1: Suppose $a = e$.
Then $a^1 = e$, so $|a| = 1$.

Case 2: Suppose $a \neq e$.
Suppose $a^2 = e$.
Then $ba = a^2b = eb = b = be$.
By left cancellation, we have $a = e$.
Thus, we have $a = e$ and $a \neq e$, a contradiction.
Therefore, $a^2 \neq e$.
Since $|b| = 2$, then $b^2 = e$.
Since $ba = a^2b$, then $b = a^{-2}ba$.
Thus, $e = b^2 = (a^{-2}ba)(a^{-2}ba) = a^{-2}ba^{-1}ba = (a^{-2}ba^{-1})(ba)$.
Hence, $(ba)^{-1} = a^{-2}ba^{-1}$, so $a^{-1}b^{-1} = a^{-2}ba^{-1}$.
Therefore, $ab^{-1} = ba^{-1}$.
Observe that

$$\begin{aligned} a^3 &= a(a^2) \\ &= a(bab^{-1}) \\ &= (ab)(ab^{-1}) \\ &= (ab)(ba^{-1}) \\ &= a(bb)a^{-1} \\ &= aea^{-1} \\ &= aa^{-1} \\ &= e. \end{aligned}$$

Since $a \neq e$ and $a^2 \neq e$ and $a^3 = e$, then $|a| = 3$.
Therefore, either $|a| = 1$ or $|a| = 3$. ∎

Exercise 115. In $\mathbb{Z}_n$, if $\gcd(a, n) = d$, then $\langle [a] \rangle = \langle [d] \rangle$.

Proof. Let $n \in \mathbb{Z}^+$ and $a \in \mathbb{Z}$.
Suppose $\gcd(a, n) = d$.
Then $d \in \mathbb{Z}^+$ and $d|a$ and $d|n$.
Since $d|a$, then $a = dk$ for some integer k.
Thus, $[a]_n = [dk]_n = [kd]_n = [k][d] = k[d]$.
Hence, $[a] \in \langle [d] \rangle$.
Since $\langle [a] \rangle$ is the smallest subgroup that contains $[a]$, then any subgroup of $\mathbb{Z}_n$ that contains $[a]$ must contain $\langle [a] \rangle$. Thus, $\langle d \rangle$ must contain $\langle [a] \rangle$, so $\langle [a] \rangle \subset \langle [d] \rangle$.

We prove $[d] \in \langle [a] \rangle$.
Since d is the least positive linear combination of a and n, then there exist integers s and t such that $d = sa + nt$. Thus, $d - sa = nt$. Since $n > 0$, then $n|(d - sa)$, so $d \equiv sa \pmod{n}$. Hence, $[d] = [sa] = [s][a] = s[a]$, so $[d] \in \langle [a] \rangle$. Therefore, $\langle [a] \rangle$ must contain $\langle [d] \rangle$, so $\langle [d] \rangle \subset \langle [a] \rangle$.
Since $\langle [a] \rangle \subset \langle [d] \rangle$ and $\langle [d] \rangle \subset \langle [a] \rangle$, then $\langle [a] \rangle = \langle [d] \rangle$. ∎