Group Theory Examples

Jason Sass

July 16, 2023

Binary Operations

Example 1. $(2^S, \cup)$ **is an associative binary structure**
Let S be a set.
Let 2^S be the powerset of S.
Then set union $\cup$ is a binary operation on 2^S.

Proof. Let $X, Y \in 2^S$.
Then $X \subset S$ and $Y \subset S$.
By definition of set union, $X \cup Y$ is a set uniquely determined by X and Y.

Let $a \in X \cup Y$.
Then either $a \in X$ or $a \in Y$.
We consider these cases separately.
Case 1: Suppose $a \in X$.
Since $X \subset S$, then $a \in S$.
Case 2: Suppose $a \in Y$.
Since $Y \subset S$, then $a \in S$.
Hence, in either case $a \in S$.
Thus, $a \in X \cup Y$ implies $a \in S$, so $X \cup Y \subset S$.
Therefore, $X \cup Y \in 2^S$.
Since $X \cup Y \in 2^S$ and $X \cup Y$ is unique, then set union is a binary operation on 2^S.
Hence, $(2^S, \cup)$ is a binary structure.
Since set union is associative, then $(2^S, \cup)$ is an associative binary structure. □

Example 2. $(2^S, \cap)$ **is an associative binary structure**
Let S be a set.
Let 2^S be the powerset of S.
Then set intersection $\cap$ is a binary operation on 2^S.

Proof. Let $X, Y \in 2^S$.
Since $X \in 2^S$, then $X \subset S$.
Since $Y \in 2^S$, then $Y \subset S$.

By definition of set intersection, $X \cap Y$ is a set uniquely determined by X and Y.

In general, $A \cap B \subset A$ for any sets A, B.

In particular, $X \cap Y \subset X$.

Since $X \cap Y \subset X$ and $X \subset S$, then by transitivity of the subset relation, $X \cap Y \subset S$.

Therefore, $X \cap Y \in 2^S$.

Since $X \cap Y \in 2^S$ and $X \cap Y$ is unique, then set intersection is a binary operation on 2^S.

Hence, $(2^S, \cap)$ is a binary structure.

Since set intersection is associative, then $(2^S, \cap)$ is an associative binary structure. □

Example 3. Let S be a nonempty set.

Let $\mathscr{P}$ be the power set of S.

A. $(\mathscr{P}, \cup)$

Set union is a binary operation on $\mathscr{P}$, so $(\mathscr{P}, \cup)$ is a binary structure and $\cup$ is associative and commutative and identity is $\emptyset$ and the zero is S and each subset of S is idempotent with respect to set union.

The empty set is its inverse under $\cup$ since $\emptyset \cup \emptyset = \emptyset$. Every nonempty subset of S is not invertible.

B. $(\mathscr{P}, \cap)$.

Set intersection is a binary operation on $\mathscr{P}$, so $(\mathscr{P}, \cap)$ is a binary structure and $\cap$ is associative and commutative and identity is S and the zero is $\emptyset$ and each subset of S is idempotent with respect to set intersection.

The set S is its inverse under $\cap$ since $S \cap S = S$. Every nonempty subset of S is not invertible.

Example 4. $(T, \circ)$ **is a binary structure**

Let S be a set.

Let $T = \{X : X \subset S \times S\}$.

Then composition of relations $\circ$ is a binary operation on T.

Proof. Let $A, B \in T$.

Then $A \subset S \times S$ and $B \subset S \times S$, so A and B are relations on set S.

By definition of composition of relations, we have $B \circ A = \{(a, c) \in S \times S : \exists b \in S.aAb \wedge bBc\}$, so $B \circ A \subset S \times S$.

Therefore, $B \circ A \in T$, so T is closed under $\circ$.

By definition of composition of relations, $B \circ A$ is uniquely determined, so $B \circ A$ is unique.

Since A and B are arbitrary, then $B \circ A \in T$ is unique for all $A, B \in T$.

Therefore, $\circ$ is a binary operation on T. □

Example 5. $(S^S, \circ)$ **is an associative binary structure**

Let S be a set.

Let $S^S = \{f : S \to S | f \text{ is a function}\}$.

Then $(S^S, \circ)$ is an associative binary structure.

Proof. Let $f, g \in S^S$.

Then $f : S \to S$ and $g : S \to S$ are functions.

By definition of function composition, $f \circ g : S \to S$ is the unique function defined by $(f \circ g)(x) = f(g(x))$ for all $x \in S$.

Hence, $f \circ g \in S^S$ and $f \circ g$ is unique.

Therefore, function composition is a binary operation on S^S, so $(S^S, \circ)$ is a binary structure.

Since function composition is associative, then $\circ$ is associative, so $(S^S, \circ)$ is an associative binary structure. $\square$

Example 6. Let S be a nonempty set.

Let $S^S = \{f : S \to S | f \text{ is a function}\}$.

Then function composition $\circ$ is a binary operation on S^S, so $(S^S, \circ)$ is a binary structure and $\circ$ is associative, but not commutative.

The identity is the identity function $I : S \to S$ defined by $I(x) = x$ for all $x \in S$.

Each bijective function is invertible.

The identity function is idempotent with respect to function composition.

Example 7. Let $F = \{f : \mathbb{R} \to \mathbb{R} | f \text{ is a function}\}$.

Let $f, g \in F$.

Define $f + g$ by $(f + g)(x) = f(x) + g(x)$ for all $x \in \mathbb{R}$.

Define $f - g$ by $(f - g)(x) = f(x) - g(x)$ for all $x \in \mathbb{R}$.

Define $f \cdot g$ by $(f \cdot g)(x) = f(x)g(x)$ for all $x \in \mathbb{R}$.

Define $f \circ g$ by $(f \circ g)(x) = f(g(x))$ for all $x \in \mathbb{R}$.

Then $(F, +)$ is a binary structure and $+$ is associative and commutative.

The additive identity is the zero function $Z : \mathbb{R} \to \mathbb{R}$ defined by $Z(x) = 0$ for all $x \in \mathbb{R}$.

If $f : \mathbb{R} \to \mathbb{R}$ is a function, then its inverse is the function $g : \mathbb{R} \to \mathbb{R}$ defined by $g(x) = -f(x)$ for all $x \in \mathbb{R}$.

Then $(F, -)$ is a binary structure and $-$ is not associative and not commutative.

Then $(F, \cdot)$ is binary structure and $\cdot$ is associative and commutative.

The multiplicative identity is the constant function $I : \mathbb{R} \to \mathbb{R}$ defined by $I(x) = 1$ for all $x \in \mathbb{R}$.

If $f : \mathbb{R} \to \mathbb{R}$ is a function, then its inverse is the function $g : \mathbb{R} \to \mathbb{R}$ defined by $g(x) = \frac{1}{f(x)}$ where $f(x) \neq 0$.

The zero is the function $Z : \mathbb{R} \to \mathbb{R}$ defined by $Z(x) = 0$ for all $x \in \mathbb{R}$.

Then $(F, \circ)$ is a binary structure and $\circ$ is associative, but not commutative.

The identity is the identity function $I : R \to R$ defined by $I(x) = x$ for all $x \in \mathbb{R}$.

Each bijective function is invertible.

The identity function is idempotent with respect to function composition.

Additive Number Groups

Example 8. The set of all integers under addition is an abelian group.

$(\mathbb{Z}, +)$ is an abelian group.

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

Since $\mathbb{Z}$ is closed under addition, then $a + b$ is a unique integer, so addition is a binary operation on $\mathbb{Z}$.

Since $(a + b) + c = a + (b + c)$ for all $a, b, c \in \mathbb{Z}$, then addition of integers is associative.

Since $a + b = b + a$ for all $a, b \in \mathbb{Z}$, then addition of integers is commutative.

Since $0 \in \mathbb{Z}$ and $0 + a = a + 0 = a$ for all $a \in \mathbb{Z}$, then $0 \in \mathbb{Z}$ is an additive identity.

For each $a \in \mathbb{Z}$, there is $-a \in \mathbb{Z}$ such that $a + (-a) = -a + a = 0$, so for each integer a there is an additive inverse $-a \in \mathbb{Z}$.

Since addition is a binary operation on $\mathbb{Z}$ and addition of integers is associative and $0 \in \mathbb{Z}$ is an additive identity and for each integer a there is an additive inverse $-a \in \mathbb{Z}$, then $(\mathbb{Z}, +)$ is a group.

Since $(\mathbb{Z}, +)$ is a group and addition of integers is commutative, then $(\mathbb{Z}, +)$ is an abelian group. $\square$

Example 9. The set of all multiples of an integer n under addition is an abelian group.

Let $n \in \mathbb{Z}$.

Then $(n\mathbb{Z}, +)$ is an abelian group.

Proof. We prove addition is a binary operation on $n\mathbb{Z}$.

Let $na, nb \in n\mathbb{Z}$.

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

Since $\mathbb{Z}$ is closed under addition and $a, b \in \mathbb{Z}$, then $a+b \in \mathbb{Z}$, so $n(a+b) \in n\mathbb{Z}$.

Hence, $na + nb \in n\mathbb{Z}$, so $n\mathbb{Z}$ is closed under addition.

Therefore, addition is a binary operation on $n\mathbb{Z}$.

We prove addition over $n\mathbb{Z}$ is associative.

Let $na, nb, nc \in n\mathbb{Z}$.

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

Since $\mathbb{Z}$ is closed under multiplication and $n \in \mathbb{Z}$ and $a, b, c \in \mathbb{Z}$, then $na, nb, nc \in \mathbb{Z}$.

Since addition of integers is associative, then $(na+nb)+nc = na+(nb+nc)$.
Therefore, addition over $n\mathbb{Z}$ is associative.

We prove addition over $n\mathbb{Z}$ is commutative.
Let $na, nb \in n\mathbb{Z}$.
Then $a, b \in \mathbb{Z}$.
Since $\mathbb{Z}$ is closed under multiplication and $n \in \mathbb{Z}$ and $a, b \in \mathbb{Z}$, then $na, nb \in \mathbb{Z}$.
Since addition of integers is commutative, then $na + nb = nb + na$.
Therefore, addition over $n\mathbb{Z}$ is commutative.

We prove $0 \in n\mathbb{Z}$ is an additive identity.
Since $0 \in \mathbb{Z}$ and $0 = n \cdot 0$, then $0 \in n\mathbb{Z}$.
Let $na \in n\mathbb{Z}$.
Since $n\mathbb{Z} \subset \mathbb{Z}$, then $na \in \mathbb{Z}$.
Since $0 \in \mathbb{Z}$ is additive identity, then $na + 0 = na = 0 + na$, so $na + 0 = na = 0 + na$ for all $na \in n\mathbb{Z}$.
Since $0 \in n\mathbb{Z}$ and $na + 0 = na = 0 + na$ for all $na \in n\mathbb{Z}$, then $0 \in n\mathbb{Z}$ is an additive identity.

We prove for every $nk \in n\mathbb{Z}$ there is an additive inverse $-nk \in n\mathbb{Z}$.
Let $nk \in n\mathbb{Z}$.
Then $k \in \mathbb{Z}$, so $-k \in \mathbb{Z}$.
Since $-nk = n(-k)$ and $-k \in \mathbb{Z}$, then $-nk \in n\mathbb{Z}$.
Observe that

$$\begin{aligned}
nk + (-nk) &= nk - nk \\
&= 0 \\
&= 0k \\
&= (-n + n)k \\
&= -nk + nk.
\end{aligned}$$

Thus, $nk + (-nk) = 0 = -nk + nk$.
Since $-nk \in n\mathbb{Z}$ and $nk + (-nk) = 0 = -nk + nk$, then $-nk \in n\mathbb{Z}$ is an additive inverse of nk.
Therefore, for every $nk \in n\mathbb{Z}$ there is an additive inverse $-nk \in n\mathbb{Z}$.

Since addition is a binary operation on $n\mathbb{Z}$ and addition over $n\mathbb{Z}$ is associative and $0 \in n\mathbb{Z}$ is an additive identity and for every $nk \in n\mathbb{Z}$ there is an additive inverse $-nk \in n\mathbb{Z}$, then $(n\mathbb{Z}, +)$ is a group.

Since $(n\mathbb{Z}, +)$ is a group and addition over $n\mathbb{Z}$ is commutative, then $(n\mathbb{Z}, +)$ is an abelian group. $\square$

Example 10. Integers modulo n under addition is an abelian group.

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

Then $(\mathbb{Z}_n, +)$ is an abelian group.

Proof. Let n be a positive integer.

Let $\mathbb{Z}_n$ be the set of all congruence classes modulo n.

Then $\mathbb{Z}_n = \{[a] : a \in \mathbb{Z}\}$ and addition modulo n is a binary operation on $\mathbb{Z}_n$.

Since $([a] + [b]) + [c] = [a] + ([b] + [c])$ for all $[a], [b], [c] \in \mathbb{Z}_n$, then addition modulo n is associative.

Since $[a] + [b] = [b] + [a]$ for all $[a], [b] \in \mathbb{Z}_n$, then addition modulo n is commutative.

Since $[0] \in \mathbb{Z}_n$ and $[0] + [a] = [a] + [0] = [a]$ for all $[a] \in \mathbb{Z}_n$, then $[0] \in \mathbb{Z}_n$ is an additive identity.

We prove for every $[a] \in \mathbb{Z}_n$ there is an additive inverse $[n - a] \in \mathbb{Z}_n$.

Let $[a] \in \mathbb{Z}_n$.

Then $a \in \mathbb{Z}$.

Since $a \in \mathbb{Z}$ and $n \in \mathbb{Z}$ and $\mathbb{Z}$ is closed under subtraction, then $n - a \in \mathbb{Z}$, so $[n - a] \in \mathbb{Z}_n$.

Observe that

$$\begin{aligned}
[a] + [n - a] &= [a + (n - a)] \\
&= [n] \\
&= [0] \\
&= [n] \\
&= [(n - a) + a] \\
&= [n - a] + [a].
\end{aligned}$$

Thus, $[a] + [n - a] = [0] = [n - a] + [a]$.

Since $[n - a] \in \mathbb{Z}_n$ and $[a] + [n - a] = [0] = [n - a] + [a]$, then $[n - a]$ is an additive inverse of $[a]$.

Therefore, for every $[a] \in \mathbb{Z}_n$ there exists an additive inverse $[n - a] \in \mathbb{Z}_n$.

Since addition modulo n is a binary operation on $\mathbb{Z}_n$ and addition modulo n is associative and $[0] \in \mathbb{Z}_n$ is an additive identity and for every $[a] \in \mathbb{Z}_n$ there is an additive inverse $[n - a] \in \mathbb{Z}_n$, then $(\mathbb{Z}_n, +)$ is a group.

Since $(\mathbb{Z}_n, +)$ is a group and addition modulo n is commutative, then $(\mathbb{Z}_n, +)$ is an abelian group. $\square$

Example 11. The set of all rational numbers under addition is an abelian group.

$(\mathbb{Q}, +)$ is an abelian group.

Proof. Addition is a binary operation on $\mathbb{Q}$ and addition over $\mathbb{Q}$ is associative and commutative.

We prove $0 \in \mathbb{Q}$ is an additive identity.

Since 0 and 1 are integers and $1 \neq 0$, then $0 = \frac{0}{1} \in \mathbb{Q}$.

Observe that $\frac{a}{b} + 0 = 0 + \frac{a}{b} = \frac{a}{b}$ for all $\frac{a}{b} \in \mathbb{Q}$.

Since $0 \in \mathbb{Q}$ and $\frac{a}{b} + 0 = 0 + \frac{a}{b} = \frac{a}{b}$ for all $\frac{a}{b} \in \mathbb{Q}$, then $0 \in \mathbb{Q}$ is an additive identity.

We prove for every $\frac{a}{b} \in \mathbb{Q}$ there is an additive inverse $\frac{-a}{b} \in \mathbb{Q}$.

Let $\frac{a}{b} \in \mathbb{Q}$.

Then $a, b \in \mathbb{Z}$ and $b \neq 0$.

Since $a \in \mathbb{Z}$, then $-a \in \mathbb{Z}$.

Since $-a$ and b are integers and $b \neq 0$, then $\frac{-a}{b} \in \mathbb{Q}$.

Observe that $\frac{a}{b} + \frac{-a}{b} = \frac{-a}{b} + \frac{a}{b} = 0$.

Since $\frac{-a}{b} \in \mathbb{Q}$ and $\frac{a}{b} + \frac{-a}{b} = \frac{-a}{b} + \frac{a}{b} = 0$, then $\frac{-a}{b}$ is an additive inverse of $\frac{a}{b}$.

Therefore, for every $\frac{a}{b} \in \mathbb{Q}$ there is an additive inverse $\frac{-a}{b} \in \mathbb{Q}$.

Since addition is a binary operation on $\mathbb{Q}$ and addition over $\mathbb{Q}$ is associative and $0 \in \mathbb{Q}$ is an additive identity and for every $\frac{a}{b} \in \mathbb{Q}$ there is an additive inverse $\frac{-a}{b} \in \mathbb{Q}$, then $(\mathbb{Q}, +)$ is a group.

Since $(\mathbb{Q}, +)$ is a group and addition over $\mathbb{Q}$ is commutative, then $(\mathbb{Q}, +)$ is an abelian group. $\square$

Example 12. The set of all real numbers under addition is an abelian group.

$(\mathbb{R}, +)$ is an abelian group.

Proof. Let $a, b \in \mathbb{R}$.

Then $a + b$ is a unique real number.

Therefore, $\mathbb{R}$ is closed under addition, so addition is a binary operation on $\mathbb{R}$.

Addition of real numbers is associative and commutative.

Since $0 \in \mathbb{R}$ and $a + 0 = 0 + a = a$ for all $a \in \mathbb{R}$, then $0 \in \mathbb{R}$ is an additive identity.

For each $a \in \mathbb{R}$, there exists $-a \in \mathbb{R}$ such that $a + (-a) = -a + a = 0$, so for every real number a there is an additive inverse $-a \in \mathbb{R}$.

Since addition is a binary operation on $\mathbb{R}$ and addition of real numbers is associative and $0 \in \mathbb{R}$ is an additive identity and for every real number a there is an additive inverse $-a \in \mathbb{R}$, then $(\mathbb{R}, +)$ is a group.

Since $(\mathbb{R}, +)$ is a group and addition of real numbers is commutative, then $(\mathbb{R}, +)$ is an abelian group. $\square$

Example 13. The set of all complex numbers under addition is an abelian group.

$(\mathbb{C}, +)$ is an abelian group.

Proof. Addition is a binary operation on $\mathbb{C}$ and addition over $\mathbb{C}$ is associative and commutative.

Since $0 = 0 + 0i \in \mathbb{C}$ and $z + 0 = 0 + z = z$ for all $z \in \mathbb{C}$, then $0 \in \mathbb{C}$ is an additive identity.

We prove for every $z \in \mathbb{C}$ there is an additive inverse $-z \in \mathbb{C}$.

Let $z \in \mathbb{C}$.

Then $z = x + yi$ for some $x, y \in \mathbb{R}$.

Since $x \in \mathbb{R}$, then $-x \in \mathbb{R}$.

Since $y \in \mathbb{R}$, then $-y \in \mathbb{R}$.

Let $-z = -x - yi$.

Since $-x \in \mathbb{R}$ and $-y \in \mathbb{R}$, then $-z \in \mathbb{C}$.

Observe that

$$\begin{aligned} z + (-z) &= -z + z \\ &= (-x - yi) + (x + yi) \\ &= (-x + x) + (-y + y)i \\ &= 0 + 0i \\ &= 0. \end{aligned}$$

Therefore, $z + (-z) = (-z) + z = 0$.

Since $-z \in \mathbb{C}$ and $z + (-z) = (-z) + z = 0$, then $-z$ is an additive inverse of z.

Therefore, for every $z \in \mathbb{C}$ there is an additive inverse $-z \in \mathbb{C}$.

Since addition is a binary operation on $\mathbb{C}$ and addition of complex numbers is associative and $0 = 0 + 0i \in \mathbb{C}$ is an additive identity and for every $z \in \mathbb{C}$ there is an additive inverse $-z \in \mathbb{C}$, then $(\mathbb{C}, +)$ is a group.

Since $(\mathbb{C}, +)$ is a group and addition of complex numbers is commutative, then $(\mathbb{C}, +)$ is an abelian group. $\square$

Multiplicative Number Groups

Example 14. The set of all nonzero rational numbers under multiplication is an abelian group.

$(\mathbb{Q}^*, \cdot)$ is an abelian group.

Proof. We prove multiplication is a binary operation on $\mathbb{Q}^*$.
Let $\frac{a}{b}, \frac{c}{d} \in \mathbb{Q}^*$.
Since $\frac{a}{b} \in \mathbb{Q}^*$, then $\frac{a}{b} \in \mathbb{Q}$ and $\frac{a}{b} \neq 0$.
Since $\frac{c}{d} \in \mathbb{Q}^*$, then $\frac{c}{d} \in \mathbb{Q}$ and $\frac{c}{d} \neq 0$.
Since $\frac{a}{b} \in \mathbb{Q}$, then $a, b \in \mathbb{Z}$ and $b \neq 0$.
Since $\frac{c}{d} \in \mathbb{Q}$, then $c, d \in \mathbb{Z}$ and $d \neq 0$.
Since multiplication is a binary operation on $\mathbb{Q}$, then $\mathbb{Q}$ is closed under multiplication.
Since $\frac{a}{b} \in \mathbb{Q}$ and $\frac{c}{d} \in \mathbb{Q}$, then this implies $\frac{a}{b} \cdot \frac{c}{d} \in \mathbb{Q}$, so $\frac{ac}{bd} \in \mathbb{Q}$.
Since $\frac{a}{b} \neq 0$ and $b \neq 0$, then $a \neq 0$.
Since $\frac{c}{d} \neq 0$ and $d \neq 0$, then $c \neq 0$.
Since $a, c \in \mathbb{Z}$ and $a \neq 0$ and $c \neq 0$, then $ac \neq 0$.
Since $\frac{ac}{bd} \in \mathbb{Q}$ and $ac \neq 0$, then $\frac{ac}{bd} \neq 0$.
Since $\frac{ac}{bd} \in \mathbb{Q}$ and $\frac{ac}{bd} \neq 0$, then $\frac{ac}{bd} \in \mathbb{Q}^*$, so $\mathbb{Q}^*$ is closed under multiplication.
Therefore, multiplication is a binary operation on $\mathbb{Q}^*$.

Since multiplication over $\mathbb{Q}$ is associative and $\mathbb{Q}^* \subset \mathbb{Q}$, then multiplication over $\mathbb{Q}^*$ is associative.

Since multiplication over $\mathbb{Q}$ is commutative and $\mathbb{Q}^* \subset \mathbb{Q}$, then multiplication over $\mathbb{Q}^*$ is commutative.

We prove $1 \in \mathbb{Q}^*$ is a multiplicative identity.
Since $1 \in \mathbb{Z}$ and $1 = \frac{1}{1}$ and $1 \neq 0$, then $1 \in \mathbb{Q}^*$.
Let $\frac{a}{b} \in \mathbb{Q}^*$.
Since $\mathbb{Q}^* \subset \mathbb{Q}$, then $\frac{a}{b} \in \mathbb{Q}$.
Thus, $\frac{a}{b} \cdot 1 = 1 \cdot \frac{a}{b} = \frac{a}{b}$.
Since $1 \in \mathbb{Q}^*$ and $\frac{a}{b} \cdot 1 = 1 \cdot \frac{a}{b} = \frac{a}{b}$, then $1 \in \mathbb{Q}^*$ is a multiplicative identity.

We prove for every $\frac{a}{b} \in \mathbb{Q}^*$, there is a multiplicative inverse $\frac{b}{a} \in \mathbb{Q}^*$.
Let $\frac{a}{b} \in \mathbb{Q}^*$.
Then $\frac{a}{b} \in \mathbb{Q}$ and $\frac{a}{b} \neq 0$.
Since $\frac{a}{b} \in \mathbb{Q}$, then $a, b \in \mathbb{Z}$ and $b \neq 0$.
Since $\frac{a}{b} \neq 0$ and $b \neq 0$, then $a \neq 0$, so $\frac{b}{a} \neq 0$.
Since $a, b \in \mathbb{Z}$ and $a \neq 0$ and $b \neq 0$, then $ab \neq 0$.
Since $b, a \in \mathbb{Z}$ and $a \neq 0$, then $\frac{b}{a} \in \mathbb{Q}$.
Since $\frac{b}{a} \in \mathbb{Q}$ and $\frac{b}{a} \neq 0$, then $\frac{b}{a} \in \mathbb{Q}^*$.

Observe that

$$\begin{aligned}
\frac{a}{b} \cdot \frac{b}{a} &= \frac{ab}{ba} \\
&= \frac{ab}{ab} \\
&= 1 \\
&= \frac{ab}{ab} \\
&= \frac{ba}{ab} \\
&= \frac{b}{a} \cdot \frac{a}{b}.
\end{aligned}$$

Thus, $\frac{a}{b} \cdot \frac{b}{a} = 1 = \frac{b}{a} \cdot \frac{a}{b}$.

Since there exists $\frac{b}{a} \in \mathbb{Q}^*$ such that $\frac{a}{b} \cdot \frac{b}{a} = 1 = \frac{b}{a} \cdot \frac{a}{b}$, then $\frac{b}{a} \in \mathbb{Q}^*$ is a multiplicative inverse of $\frac{a}{b}$.

Therefore, for every $\frac{a}{b} \in \mathbb{Q}^*$, there is a multiplicative inverse $\frac{b}{a} \in \mathbb{Q}^*$.

Since multiplication is a binary operation on $\mathbb{Q}^*$ and multiplication over $\mathbb{Q}^*$ is associative and $1 \in \mathbb{Q}^*$ is a multiplicative identity and for every $\frac{a}{b} \in \mathbb{Q}^*$, there is a multiplicative inverse $\frac{b}{a} \in \mathbb{Q}^*$, then $(\mathbb{Q}^*, \cdot)$ is a group.

Since $(\mathbb{Q}^*, \cdot)$ is a group and multiplication over $\mathbb{Q}^*$ is commutative, then $(\mathbb{Q}^*, \cdot)$ is an abelian group. □

Example 15. The set of all nonzero real numbers under multiplication is an abelian group.

$(\mathbb{R}^*, \cdot)$ is an abelian group.

Proof. We prove multiplication is a binary operation on $\mathbb{R}^*$.

Let $a, b \in \mathbb{R}^*$.

Then $a, b \in \mathbb{R}$ and $a \neq 0$ and $b \neq 0$.

Since $\mathbb{R}$ is closed under multiplication and $a, b \in \mathbb{R}$, then $ab \in \mathbb{R}$.

Since the product of two nonzero real numbers is nonzero and $a \neq 0$ and $b \neq 0$, then $ab \neq 0$.

Since $ab \in \mathbb{R}$ and $ab \neq 0$, then $ab \in \mathbb{R}^*$, so $\mathbb{R}^*$ is closed under multiplication.

Since ab is unique, then this implies multiplication is a binary operation on $\mathbb{R}^*$.

Since multiplication of real numbers is associative and $\mathbb{R}^* \subset \mathbb{R}$, then multiplication over $\mathbb{R}^*$ is associative.

Since multiplication of real numbers is commutative and $\mathbb{R}^* \subset \mathbb{R}$, then multiplication over $\mathbb{R}^*$ is commutative.

We prove $1 \in \mathbb{R}^*$ is a multiplicative identity.

Since $1 \in \mathbb{R}$ and $1 \neq 0$, then $1 \in \mathbb{R}^*$.

Since the number 1 is a multiplicative identity of $\mathbb{R}$, then $1x = x1 = x$ for all $x \in \mathbb{R}$.

Let $r \in \mathbb{R}^*$.

Since $\mathbb{R}^* \subset \mathbb{R}$, then $r \in \mathbb{R}$, so $1r = r1 = r$.

Hence, $1r = r1 = r$ for all $r \in \mathbb{R}^*$.

Since $1 \in \mathbb{R}^*$ and $1r = r1 = r$ for all $r \in \mathbb{R}^*$, then $1 \in \mathbb{R}^*$ is a multiplicative identity of $\mathbb{R}^*$.

We prove for every $a \in \mathbb{R}^*$ there is a multiplicative inverse $\frac{1}{a} \in \mathbb{R}^*$.

Let $a \in \mathbb{R}^*$.

Then $a \in \mathbb{R}$ and $a \neq 0$.

Thus, $\frac{1}{a} \in \mathbb{R}$ and $\frac{1}{a} \neq 0$, so $\frac{1}{a} \in \mathbb{R}^*$.

Since $a \cdot \frac{1}{a} = \frac{1}{a} \cdot a = 1$, then $\frac{1}{a} \in \mathbb{R}^*$ is a multiplicative inverse of a.

Therefore, for every $a \in \mathbb{R}^*$ there is a multiplicative inverse $\frac{1}{a} \in \mathbb{R}^*$.

Since multiplication is a binary operation on $\mathbb{R}^*$ and multiplication over $\mathbb{R}^*$ is associative and $1 \in \mathbb{R}^*$ is a multiplicative identity and for every $a \in \mathbb{R}^*$ there is a multiplicative inverse $\frac{1}{a} \in \mathbb{R}^*$, then $(\mathbb{R}^*, \cdot)$ is a group.

Since $(\mathbb{R}^*, \cdot)$ is a group and multiplication over $\mathbb{R}^*$ is commutative, then $(\mathbb{R}^*, \cdot)$ is an abelian group. ☐

Example 16. The set of all nonzero complex numbers under multiplication is an abelian group.

$(\mathbb{C}^*, \cdot)$ is an abelian group.

Proof. We prove multiplication is a binary operation on $\mathbb{C}^*$.

Let $z, w \in \mathbb{C}^*$.

Then $z \in \mathbb{C}$ and $z \neq 0$ and $w \in \mathbb{C}$ and $w \neq 0$.

Since $z \in \mathbb{C}$, then $z = a + bi$ for some $a, b \in \mathbb{R}$.

Since $w \in \mathbb{C}$, then $w = c + di$ for some $c, d \in \mathbb{R}$.

Since multiplication is a binary operation on $\mathbb{C}$, then $\mathbb{C}$ is closed under multiplication.

Since $z \in \mathbb{C}$ and $w \in \mathbb{C}$, then this implies $zw \in \mathbb{C}$.

Observe that $zw = (a+bi)(c+di) = (ac-bd)+(ad+bc)i$ is zero iff $ac-bd = 0$ and $ad + bc = 0$.

We prove $ac - bd = 0$ and $ad + bc = 0$ if and only if either $a = b = 0$ or $c = d = 0$.

Suppose either $a = b = 0$ or $c = d = 0$.

If $a = b = 0$, then $ac - bd = 0c - 0d = 0 - 0 = 0$ and $ad + bc = 0d + 0c = 0 + 0 = 0$.

If $c = d = 0$, then $ac - bd = a0 - b0 = 0 - 0 = 0$ and $ad + bc = a0 + b0 = 0 + 0 = 0$.

Conversely, we prove if $ac - bd = 0$ and $ad + bc = 0$, then either $a = b = 0$ or $c = d = 0$.

Suppose $ac - bd = 0$ and $ad + bc = 0$ and either $a \neq 0$ or $b \neq 0$.

We must prove $c = d = 0$.

Since $a \neq 0$ or $b \neq 0$, we consider these cases separately.

We consider these cases separately.

Case 1: Suppose $a \neq 0$.

Since $ac - bd = 0$, then $ac = bd$.

Since $0 = ad + bc$, we multiply by d to obtain

$$\begin{aligned} 0 &= d0 \\ &= d(ad + bc) \\ &= dad + dbc \\ &= dad + (bd)c \\ &= dad + (ac)c \\ &= a(d^2 + c^2). \end{aligned}$$

Thus, $a(d^2 + c^2) = 0$, so either $a = 0$ or $d^2 + c^2 = 0$.

Since $a \neq 0$, then $d^2 + c^2 = 0$, so $c^2 = -d^2$.

If $c \neq 0$, then $c^2 > 0$, so $-d^2 > 0$.

Thus, $d^2 < 0$, a contradiction, since the square of a real number is nonnegative.

Hence, $c = 0$, so $0 = d^2 + c^2 = d^2 + 0^2 = d^2 + 0 = d^2$.

Therefore, $d^2 = 0$, so $d = 0$.

Consequently, $c = 0 = d$, as desired.

Case 2: Suppose $b \neq 0$.

Since $ac - bd = 0$, then $ac = bd$.

Since $0 = ad + bc$, we multiply by c to obtain

$$\begin{aligned} 0 &= c0 \\ &= c(ad + bc) \\ &= cad + cbc \\ &= (ac)d + cbc \\ &= (bd)d + cbc \\ &= b(d^2 + c^2). \end{aligned}$$

Thus, $b(d^2 + c^2) = 0$, so either $b = 0$ or $d^2 + c^2 = 0$.

Since $b \neq 0$, then $d^2 + c^2 = 0$, so $c^2 = -d^2$.

If $c \neq 0$, then $c^2 > 0$, so $-d^2 > 0$.

Thus, $d^2 < 0$, a contradiction, since the square of a real number is nonnegative.

Hence, $c = 0$, so $0 = d^2 + c^2 = d^2 + 0^2 = d^2 + 0 = d^2$.

Therefore, $d^2 = 0$, so $d = 0$.

Consequently, $c = 0 = d$, as desired.

Therefore, we proved $ac-bd = 0$ and $ad+bc = 0$ if and only if either $a = b = 0$ or $c = d = 0$.

Hence, zw is zero if and only if either $a = b = 0$ or $c = d = 0$, so $zw = 0$ if and only if either $a = b = 0$ or $c = d = 0$.

Thus, $zw \neq 0$ if and only if both $a \neq 0$ or $b \neq 0$ and $c \neq 0$ or $d \neq 0$.

Since $z = 0$ if and only if $a = b = 0$, then $z \neq 0$ if and only if either $a \neq 0$ or $b \neq 0$.

Since $z \neq 0$, then we conclude either $a \neq 0$ or $b \neq 0$.

Since $w = 0$ if and only if $c = d = 0$, then $w \neq 0$ if and only if either $c \neq 0$ or $d \neq 0$.

Since $w \neq 0$, then we conclude either $c \neq 0$ or $d \neq 0$.

Thus, both $a \neq 0$ or $b \neq 0$ and $c \neq 0$ or $d \neq 0$, so we conclude $zw \neq 0$.

Since $zw \in \mathbb{C}$ and $zw \neq 0$, then $zw \in \mathbb{C}^*$, so $\mathbb{C}^*$ is closed under multiplication.

Since zw is unique, then we conclude multiplication is a binary operation on $\mathbb{C}^*$. □

Proof. Since multiplication of complex numbers is associative and $\mathbb{C}^* \subset \mathbb{C}$, then multiplication over $\mathbb{C}^*$ is associative.

Since multiplication of complex numbers is commutative and $\mathbb{C}^* \subset \mathbb{C}$, then multiplication over $\mathbb{C}^*$ is commutative. □

Proof. We prove $1 \in \mathbb{C}^*$ is a multiplicative identity.

Since $1 = 1 + 0i$, then $1 \in \mathbb{C}$.

Since $1 \neq 0$, then $1 \in \mathbb{C}^*$.

Let $z \in \mathbb{C}^*$.

Since $\mathbb{C}^* \subset \mathbb{C}$, then $z \in \mathbb{C}$.

Thus, $1 \cdot z = z \cdot 1 = z$, so $1 \cdot z = z \cdot 1 = z$ for all $z \in \mathbb{C}^*$.

Since $1 \in \mathbb{C}^*$ and $1 \cdot z = z \cdot 1 = z$ for all $z \in \mathbb{C}^*$, then $1 \in \mathbb{C}^*$ is a multiplicative identity. □

Proof. We prove every nonzero complex number has a multiplicative inverse.

Let $z \in \mathbb{C}^*$.

Then $z \in \mathbb{C}$ and $z \neq 0$, so there exists $\frac{1}{z} \in \mathbb{C}^*$ such that $\frac{1}{z} = \frac{\bar{z}}{|z|^2}$ and $z \cdot \frac{1}{z} = \frac{1}{z} \cdot z = 1$.

Hence, $\frac{1}{z} \in \mathbb{C}^*$ is a multiplicative inverse of z.

Therefore, every nonzero complex number has a multiplicative inverse. □

Proof. Since multiplication is a binary operation on $\mathbb{C}^*$ and multiplication over $\mathbb{C}^*$ is associative and $1 \in \mathbb{C}^*$ is a multiplicative identity and every nonzero complex number has a multiplicative inverse in $\mathbb{C}^*$, then $(\mathbb{C}^*, \cdot)$ is a group.

Since multiplication over $\mathbb{C}^*$ is commutative, then $(\mathbb{C}^*, \cdot)$ is an abelian group. □

Example 17. The set of all positive rational numbers under multiplication is an abelian group.

$(\mathbb{Q}^+, \cdot)$ is an abelian group.

Proof. We prove multiplication is a binary operation on $\mathbb{Q}^+$.

Let $\frac{a}{b}, \frac{c}{d} \in \mathbb{Q}^+$.

Since $\frac{a}{b} \in \mathbb{Q}^+$, then $\frac{a}{b} \in \mathbb{Q}$ and $\frac{a}{b} > 0$.

Since $\frac{c}{d} \in \mathbb{Q}^+$, then $\frac{c}{d} \in \mathbb{Q}$ and $\frac{c}{d} > 0$.

Since $\frac{a}{b} \in \mathbb{Q}$, then $a, b \in \mathbb{Z}$ and $b \neq 0$.

Since $\frac{c}{d} \in \mathbb{Q}$, then $c, d \in \mathbb{Z}$ and $d \neq 0$.

Since $\mathbb{Q}$ is closed under multiplication and $\frac{a}{b} \in \mathbb{Q}$ and $\frac{c}{d} \in \mathbb{Q}$, then $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd} \in \mathbb{Q}$.

Since $b \neq 0$, then either $b > 0$ or $b < 0$.

Since $d \neq 0$, then either $d > 0$ or $d < 0$.

Thus, either $b > 0$ and $d > 0$, or $b > 0$ and $d < 0$, or $b < 0$ and $d > 0$, or $b < 0$ and $d < 0$.

We consider these cases separately.

Case 1: Suppose $b > 0$ and $d > 0$.

Then $bd > 0$.

Since $\frac{a}{b} > 0$ and $b > 0$, then $a > 0$.

Since $\frac{c}{d} > 0$ and $d > 0$, then $c > 0$.

Since $a > 0$ and $c > 0$, then $ac > 0$.

Since $ac > 0$ and $bd > 0$, then $\frac{ac}{bd} > 0$.

Case 2: Suppose $b > 0$ and $d < 0$.

Then $bd < 0$.

Since $\frac{a}{b} > 0$ and $b > 0$, then $a > 0$.

Since $\frac{c}{d} > 0$ and $d < 0$, then $c < 0$.

Since $a > 0$ and $c < 0$, then $ac < 0$.

Since $ac < 0$ and $bd < 0$, then $\frac{ac}{bd} > 0$.

Case 3: Suppose $b < 0$ and $d > 0$.

Then $bd < 0$.

Since $\frac{a}{b} > 0$ and $b < 0$, then $a < 0$.

Since $\frac{c}{d} > 0$ and $d > 0$, then $c > 0$.

Since $a < 0$ and $c > 0$, then $ac < 0$.

Since $ac < 0$ and $bd < 0$, then $\frac{ac}{bd} > 0$.

Case 4: Suppose $b < 0$ and $d < 0$.

Then $bd > 0$.

Since $\frac{a}{b} > 0$ and $b < 0$, then $a < 0$.

Since $\frac{c}{d} > 0$ and $d < 0$, then $c < 0$.

Since $a < 0$ and $c < 0$, then $ac > 0$.

Since $ac > 0$ and $bd > 0$, then $\frac{ac}{bd} > 0$.

Thus, in all cases, $\frac{ac}{bd} > 0$.

Since $\frac{ac}{bd} \in \mathbb{Q}$ and $\frac{ac}{bd} > 0$, then $\frac{ac}{bd} \in \mathbb{Q}^+$, so $\mathbb{Q}^+$ is closed under multiplication.

Therefore, multiplication is a binary operation on $\mathbb{Q}^+$. $\square$

Proof. Since multiplication of rational numbers is associative and $\mathbb{Q}^+ \subset \mathbb{Q}$, then multiplication over $\mathbb{Q}^+$ is associative.

Since multiplication of rational numbers is commutative and $\mathbb{Q}^+ \subset \mathbb{Q}$, then multiplication over $\mathbb{Q}^+$ is commutative. $\square$

Proof. We prove $1 \in \mathbb{Q}^+$ is a multiplicative identity.

Since $1 = \frac{1}{1} \in \mathbb{Q}$ and $1 > 0$, then $1 \in \mathbb{Q}^+$.

Since the number 1 is a multiplicative identity of $\mathbb{Q}$, then $1q = q1 = q$ for all $q \in \mathbb{Q}$.

Let $q \in \mathbb{Q}^+$.

Since $\mathbb{Q}^+ \subset \mathbb{Q}$, then $q \in \mathbb{Q}$, so $1q = q1 = q$.

Hence, $1q = q1 = q$ for all $q \in \mathbb{Q}^+$.

Since $1 \in \mathbb{Q}^+$ and $1q = q1 = q$ for all $q \in \mathbb{Q}^+$, then $1 \in \mathbb{Q}^+$ is a multiplicative identity. $\square$

Proof. We prove for every $\frac{a}{b} \in \mathbb{Q}^+$ there is a multiplicative inverse $\frac{b}{a} \in \mathbb{Q}^+$.

Let $\frac{a}{b} \in \mathbb{Q}^+$.

Then $\frac{a}{b} \in \mathbb{Q}$ and $\frac{a}{b} > 0$.

Since $\frac{a}{b} \in \mathbb{Q}$, then $a, b \in \mathbb{Z}$ and $b \neq 0$.

Since $\frac{a}{b} > 0$, then $\frac{b}{a} > 0$.

Since $b \neq 0$, then either $b > 0$ or $b < 0$.

We consider these cases separately.

Case 1: Suppose $b > 0$.

Since $\frac{a}{b} > 0$ and $b > 0$, then $a > 0$, so $a \neq 0$.

Case 2: Suppose $b < 0$.

Since $\frac{a}{b} > 0$ and $b < 0$, then $a < 0$, so $a \neq 0$.

Therefore, in all cases, $a \neq 0$.

Since $a, b \in \mathbb{Z}$ and $a \neq 0$ and $b \neq 0$, then $ab \neq 0$.

Since $b, a \in \mathbb{Z}$ and $a \neq 0$, then $\frac{b}{a} \in \mathbb{Q}$.

Since $\frac{b}{a} \in \mathbb{Q}$ and $\frac{b}{a} > 0$, then $\frac{b}{a} \in \mathbb{Q}^+$.

Observe that

$$\begin{aligned}
\frac{a}{b} \cdot \frac{b}{a} &= \frac{ab}{ba} \\
&= \frac{ab}{ab} \\
&= 1 \\
&= \frac{ab}{ab} \\
&= \frac{ba}{ab} \\
&= \frac{b}{a} \cdot \frac{a}{b}.
\end{aligned}$$

Thus, $\frac{a}{b} \cdot \frac{b}{a} = 1 = \frac{b}{a} \cdot \frac{a}{b}$.

Since there exists $\frac{b}{a} \in \mathbb{Q}^+$ such that $\frac{a}{b} \cdot \frac{b}{a} = 1 = \frac{b}{a} \cdot \frac{a}{b}$, then $\frac{b}{a} \in \mathbb{Q}^+$ is a multiplicative inverse of $\frac{a}{b}$.

Therefore, for every $\frac{a}{b} \in \mathbb{Q}^+$ there is a multiplicative inverse $\frac{b}{a} \in \mathbb{Q}^+$. $\square$

Proof. Since multiplication is a binary operation on $\mathbb{Q}^+$ and multiplication over $\mathbb{Q}^+$ is associative and $1 \in \mathbb{Q}^+$ is a multiplicative identity and for every $\frac{a}{b} \in \mathbb{Q}^+$ there is a multiplicative inverse $\frac{b}{a} \in \mathbb{Q}^+$, then $(\mathbb{Q}^+, \cdot)$ is a group.

Since $(\mathbb{Q}^+, \cdot)$ is a group and multiplication over $\mathbb{Q}^+$ is commutative, then $(\mathbb{Q}^+, \cdot)$ is an abelian group. $\square$

Example 18. The set of all positive real numbers under multiplication is an abelian group.

$(\mathbb{R}^+, \cdot)$ is an abelian group.

Proof. We prove multiplication is a binary operation on $\mathbb{R}^+$.

Let $a, b \in \mathbb{R}^+$.

Then $a, b \in \mathbb{R}$ and $a > 0$ and $b > 0$.

Since $\mathbb{R}$ is closed under multiplication and $a, b \in \mathbb{R}$, then $ab \in \mathbb{R}$.

Since the product of two positive real numbers is positive and $a > 0$ and $b > 0$, then $ab > 0$.

Since $ab \in \mathbb{R}$ and $ab > 0$, then $ab \in \mathbb{R}^+$, so $\mathbb{R}^+$ is closed under multiplication.

Since ab is unique, then this implies multiplication is a binary operation on $\mathbb{R}^+$.

Since multiplication of real numbers is associative and $\mathbb{R}^+ \subset \mathbb{R}$, then multiplication over $\mathbb{R}^+$ is associative.

Since multiplication of real numbers is commutative and $\mathbb{R}^+ \subset \mathbb{R}$, then multiplication over $\mathbb{R}^+$ is commutative.

We prove $1 \in \mathbb{R}^+$ is a multiplicative identity.

Since $1 \in \mathbb{R}$ and $1 > 0$, then $1 \in \mathbb{R}^+$.

Since the number 1 is a multiplicative identity of $\mathbb{R}$, then $1x = x1 = x$ for all $x \in \mathbb{R}$.

Let $r \in \mathbb{R}^+$.

Since $\mathbb{R}^+ \subset \mathbb{R}$, then $r \in \mathbb{R}$, so $1r = r1 = r$.

Hence, $1r = r1 = r$ for all $r \in \mathbb{R}^+$.

Since $1 \in \mathbb{R}^+$ and $1r = r1 = r$ for all $r \in \mathbb{R}^+$, then $1 \in \mathbb{R}^+$ is a multiplicative identity of $\mathbb{R}^+$.

We prove for every $a \in \mathbb{R}^+$ there is a multiplicative inverse $\frac{1}{a} \in \mathbb{R}^+$.

Let $a \in \mathbb{R}^+$.

Then $a \in \mathbb{R}$ and $a > 0$.

Thus, $\frac{1}{a} \in \mathbb{R}$ and $\frac{1}{a} > 0$, so $\frac{1}{a} \in \mathbb{R}^+$.

Since $a \cdot \frac{1}{a} = \frac{1}{a} \cdot a = 1$, then $\frac{1}{a} \in \mathbb{R}^+$ is a multiplicative inverse of a.

Therefore, for every $a \in \mathbb{R}^+$ there is a multiplicative inverse $\frac{1}{a} \in \mathbb{R}^+$.

Since multiplication is a binary operation on $\mathbb{R}^+$ and multiplication over $\mathbb{R}^+$ is associative and $1 \in \mathbb{R}^+$ is a multiplicative identity and for every $a \in \mathbb{R}^+$ there is a multiplicative inverse $\frac{1}{a} \in \mathbb{R}^+$, then $(\mathbb{R}^+, \cdot)$ is a group.

Since $(\mathbb{R}^+, \cdot)$ is a group and multiplication over $\mathbb{R}^+$ is commutative, then $(\mathbb{R}^+, \cdot)$ is an abelian group. $\square$

Subgroup Relationships of number groups

Example 19. $(\mathbb{Z}, +)$ is a subgroup of $(\mathbb{Q}, +)$.

Proof. We prove $\mathbb{Z} \subset \mathbb{Q}$.
Let $n \in \mathbb{Z}$.
Then $n = \frac{n}{1}$.
Since $n \in \mathbb{Z}$ and $1 \in \mathbb{Z}$ and $1 \neq 0$, then $n \in \mathbb{Q}$, so $\mathbb{Z} \subset \mathbb{Q}$.

Since $0 \in \mathbb{Z}$, then $\mathbb{Z} \neq \emptyset$.

We prove $a + b \in \mathbb{Z}$ for all $a, b \in \mathbb{Z}$.
Since $\mathbb{Z}$ is closed under addition, then $a + b \in \mathbb{Z}$ for all $a, b \in \mathbb{Z}$.

We prove $-a \in \mathbb{Z}$ for all $a \in \mathbb{Z}$.
Every integer has an inverse, so if $a \in \mathbb{Z}$, then $-a \in \mathbb{Z}$.
Therefore, $-a \in \mathbb{Z}$ for all $a \in \mathbb{Z}$.

Since $\mathbb{Z} \neq \emptyset$ and $\mathbb{Z} \subset \mathbb{Q}$ and $(\mathbb{Q}, +)$ is a group, then $\mathbb{Z}$ is a nonempty subset of the additive group $\mathbb{Q}$.
Since $a+b \in \mathbb{Z}$ for all $a, b \in \mathbb{Z}$ and $-a \in \mathbb{Z}$ for all $a \in \mathbb{Z}$, then by the two-step subgroup test, $\mathbb{Z}$ is a subgroup of $\mathbb{Q}$, so $(\mathbb{Z}, +) < (\mathbb{Q}, +)$. $\square$

Example 20. $(\mathbb{R}^+, \cdot)$ is a subgroup of $(\mathbb{R}^*, \cdot)$.

Proof. We prove $\mathbb{R}^+ \subset \mathbb{R}^*$.
Let $r \in \mathbb{R}^+$.
Then $r \in \mathbb{R}$ and $r > 0$.
Since $r > 0$, then $r \neq 0$.
Since $r \in \mathbb{R}$ and $r \neq 0$, then $r \in \mathbb{R}^*$.
Therefore, $\mathbb{R}^+ \subset \mathbb{R}^*$.

Since $1 \in \mathbb{R}$ and $1 > 0$, then $1 \in \mathbb{R}^+$, so $\mathbb{R}^+ \neq \emptyset$.

We prove $ab \in \mathbb{R}^+$ for all $a, b \in \mathbb{R}^+$.
Let $a, b \in \mathbb{R}^+$.
Then a and b are positive real numbers.
The product of positive real numbers is a positive real number, so ab is a positive real number.
Therefore, $ab \in \mathbb{R}^+$, so $ab \in \mathbb{R}^+$ for all $a, b \in \mathbb{R}^+$.

We prove $a^{-1} \in \mathbb{R}^+$ for all $a \in \mathbb{R}^+$.
Let $a \in \mathbb{R}^+$.
Then $a \in \mathbb{R}$ and $a > 0$.
Since $a \in \mathbb{R}^+$ and $\mathbb{R}^+ \subset \mathbb{R}^*$, then $a \in \mathbb{R}^*$.
Since $(\mathbb{R}^*, \cdot)$ is a group, the inverse of a is $a^{-1} = \frac{1}{a} \in \mathbb{R}^*$.
Since $a \in \mathbb{R}$ and $a > 0$, then $\frac{1}{a} \in \mathbb{R}$ and $\frac{1}{a} > 0$, so $\frac{1}{a} \in \mathbb{R}^+$.
Therefore, $a^{-1} \in \mathbb{R}^+$, so $a^{-1} \in \mathbb{R}^+$ for all $a \in \mathbb{R}^+$.

Since $\mathbb{R}^+ \neq \emptyset$ and $\mathbb{R}^+ \subset \mathbb{R}^*$ and $(\mathbb{R}^*, \cdot)$ is a group, then $\mathbb{R}^+$ is a nonempty subset of the group $\mathbb{R}^*$.

Since $ab \in \mathbb{R}^+$ for all $a, b \in \mathbb{R}^+$ and $a^{-1} \in \mathbb{R}^+$ for all $a \in \mathbb{R}^+$, then by the two-step subgroup test, $\mathbb{R}^+$ is a subgroup of $\mathbb{R}^*$, so $(\mathbb{R}^+, \cdot) < (\mathbb{R}^*, \cdot)$. $\square$

Example 21. Gaussian integers $(\mathbb{Z}[i], +)$
Let $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$.
Then $(\mathbb{Z}[i], +)$ is an abelian group under complex addition.

Proof. We prove $(\mathbb{Z}[i], +)$ is a subgroup of $(\mathbb{C}, +)$ using the two-step subgroup test.

We prove $\mathbb{Z}[i] \subset \mathbb{C}$.
Let $n \in \mathbb{Z}[i]$.
Then $n = a + bi$ for some $a, b \in \mathbb{Z}$.
Since $a \in \mathbb{Z}$ and $\mathbb{Z} \subset \mathbb{R}$, then $a \in \mathbb{R}$.
Since $b \in \mathbb{Z}$ and $\mathbb{Z} \subset \mathbb{R}$, then $b \in \mathbb{R}$.
Since $a \in \mathbb{R}$ and $b \in \mathbb{R}$, then $n \in \mathbb{C}$, so $\mathbb{Z}[i] \subset \mathbb{C}$.

Since $0 \in \mathbb{Z}$, then $0 + 0i \in \mathbb{Z}[i]$, so $\mathbb{Z}[i]$ is not empty.
Since $\mathbb{Z}[i] \subset \mathbb{C}$ and $\mathbb{Z}[i]$ is not empty, then $\mathbb{Z}[i]$ is a nonempty subset of $\mathbb{C}$.

We prove $\mathbb{Z}[i]$ is closed under addition.
Let $z, w \in \mathbb{Z}[i]$.
Then $z = a + bi$ and $w = c + di$ for some integers a, b, c, d.
Thus, $z + w = (a + bi) + (c + di) = (a + c) + (b + d)i$.
Since $a + c \in \mathbb{Z}$ and $b + d \in \mathbb{Z}$, then $z + w \in \mathbb{Z}[i]$.
Therefore, $\mathbb{Z}[i]$ is closed under addition.

We prove $\mathbb{Z}[i]$ is closed under inverses.
Let $z \in \mathbb{Z}[i]$.
Then $z = a + bi$ for some $a, b \in \mathbb{Z}$.
Thus, $-z = -a - bi$ and $z + (-z) = -z + z = 0$.
Since $a \in \mathbb{Z}$, then $-a \in \mathbb{Z}$.
Since $b \in \mathbb{Z}$, then $-b \in \mathbb{Z}$.
Since $-a, -b \in \mathbb{Z}$, then $-z \in \mathbb{Z}[i]$.
Therefore, $\mathbb{Z}[i]$ is closed under inverses.

Since $\mathbb{Z}[i]$ is a nonempty subset of $\mathbb{C}$ and $\mathbb{Z}[i]$ is closed under addition and inverses, then by the two-step subgroup test, $\mathbb{Z}[i]$ is a subgroup of $\mathbb{C}$, so $(\mathbb{Z}[i], +) < (\mathbb{C}, +)$.

Therefore, $(\mathbb{Z}[i], +)$ is a group.

Since $(\mathbb{C}, +)$ is an abelian group, then addition over $\mathbb{C}$ is commutative.

Since addition over $\mathbb{C}$ is commutative and $\mathbb{Z}[i] \subset \mathbb{C}$, then addition over $\mathbb{Z}[i]$ is commutative.

Since $\mathbb{Z}[i]$ is a group and addition over $\mathbb{Z}[i]$ is commutative, then $\mathbb{Z}[i]$ is an abelian group. □

Example 22. $(U_4, \cdot)$ is a subgroup of $(\mathbb{C}^*, \cdot)$.

Proof. We prove $U_4 \subset \mathbb{C}^*$.

Let $z \in U_4$.

Then $z \in \mathbb{C}$ and $z^4 = 1$.

Since $0^4 = 0 \neq 1$, then $z \neq 0$.

Since $z \in \mathbb{C}$ and $z \neq 0$, then $z \in \mathbb{C}^*$.

Therefore, $U_4 \subset \mathbb{C}*$.

Since $1 = 1 + 0i \in \mathbb{C}$ and $1^4 = 1$, then $1 \in U_4$, so $U_4 \neq \emptyset$.

We prove $z_1 z_2 \in U_4$ for all $z_1, z_2 \in U_4$.

Let $z_1, z_2 \in U_4$.

Since $z_1 \in U_4$, then $z_1 \in \mathbb{C}$ and $(z_1)^4 = 1$.

Since $z_2 \in U_4$, then $z_2 \in \mathbb{C}$ and $(z_2)^4 = 1$.

Since $\mathbb{C}$ is closed under multiplication and $z_1 \in \mathbb{C}$ and $z_2 \in \mathbb{C}$, then $z_1 z_2 \in \mathbb{C}$.

Observe that

$$\begin{aligned} (z_1 \cdot z_2)^4 &= (z_1)^4 \cdot (z_2)^4 \\ &= 1 \cdot 1 \\ &= 1. \end{aligned}$$

Since $z_1 z_2 \in \mathbb{C}$ and $(z_1 z_2)^4 = 1$, then $z_1 z_2 \in U_4$.

Therefore, $z_1 z_2 \in U_4$ for all $z_1, z_2 \in U_4$.

We prove $z^{-1} \in U_4$ for all $z \in U_4$.

Let $z \in U_4$.

Then $z \in \mathbb{C}$ and $z^4 = 1$.

Since $z \in U_4$ and $U_4 \subset \mathbb{C}^*$, then $z \in \mathbb{C}^*$.

Since $(\mathbb{C}^*, \cdot)$ is a group, the inverse of z is $z^{-1} \in \mathbb{C}*$.

Thus, $z^{-1} \in \mathbb{C}$ and $z^{-1} \neq 0$.

Observe that

$$\begin{aligned}(z^{-1})^4 &= z^{-4}\\ &= \frac{1}{z^4}\\ &= \frac{1}{1}\\ &= 1.\end{aligned}$$

Since $z^{-1} \in \mathbb{C}$ and $(z^{-1})^4 = 1$, then $z^{-1} \in U_4$.
Therefore, $z^{-1} \in U_4$ for all $z \in U_4$.

Since $U_4 \neq \emptyset$ and $U_4 \subset \mathbb{C}^*$ and $(\mathbb{C}^*, \cdot)$ is a group, then U_4 is a nonempty subset of the group $\mathbb{C}^*$.

Since $z_1 z_2 \in U_4$ for all $z_1, z_2 \in U_4$ and $z^{-1} \in U_4$ for all $z \in U_4$, then by the two-step subgroup test, U_4 is a subgroup of $\mathbb{C}^*$, so $(U_4, \cdot) < (\mathbb{C}^*, \cdot)$. $\square$

Group of Units of Integers modulo n

Lemma 23. *Let $a, b \in \mathbb{Z}$ and $n \in \mathbb{Z}^+$.*
If $\gcd(a,n) = \gcd(b,n) = 1$*, then* $\gcd(ab, n) = 1$.

Proof. Suppose $\gcd(a,n) = \gcd(b,n) = 1$.
Then there exist integers x, y, s, and t such that $xa + yn = 1$ and $sb + tn = 1$.
Observe that

$$\begin{aligned}1 &= 1 \cdot 1\\ &= (xa + yn)(sb + tn)\\ &= xasb + xatn + ynsb + yntn\\ &= (xs)ab + n(xat + ysb + ytn)\\ &= (xs)ab + (xat + ysb + ytn)n.\end{aligned}$$

Since $(xs)ab + (xat + ysb + ytn)n = 1$ is a linear combination of ab and n, then $\gcd(ab, n) = 1$. $\square$

Proposition 24. *Group of units of $\mathbb{Z}_n$ under multiplication is abelian.*
Let $n \in \mathbb{Z}^+$.
Let $\mathbb{Z}_n^*$ be the set of all congruence classes of $\mathbb{Z}_n$ that have multiplicative inverses.
Then $(\mathbb{Z}_n^*, \cdot)$ is an abelian group under multiplication modulo n.

Proof. We prove multiplication modulo n is a binary operation on $\mathbb{Z}_n^*$.
Since $\mathbb{Z}_n^* = \{[a] \in \mathbb{Z}_n : \gcd(a,n) = 1\}$, then $\mathbb{Z}_n^* \subset \mathbb{Z}_n$.
Let $[x], [y] \in \mathbb{Z}_n^*$.
Since $[x] \in \mathbb{Z}_n^*$, then $[x] \in \mathbb{Z}_n$ and $\gcd(x,n) = 1$.
Since $[y] \in \mathbb{Z}_n^*$, then $[y] \in \mathbb{Z}_n$ and $\gcd(y,n) = 1$.

Since multiplication modulo n is a binary operation on $\mathbb{Z}_n$, then $[x][y] = [xy] \in \mathbb{Z}_n$ and $[xy]$ is unique.

By the previous lemma, if $\gcd(x,n) = \gcd(y,n) = 1$, then $\gcd(xy,n) = 1$.

Since $\gcd(x,n) = 1 = \gcd(y,n)$, then we conclude $\gcd(xy,n) = 1$.

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

Since $[xy] \in \mathbb{Z}_n^*$ and is unique, then multiplication modulo n is a binary operation on $\mathbb{Z}_n^*$.

Since multiplication modulo n over $\mathbb{Z}_n$ is associative and $\mathbb{Z}_n^* \subset \mathbb{Z}_n$, then multiplication modulo n over $\mathbb{Z}_n^*$ is associative.

Since multiplication modulo n over $\mathbb{Z}_n$ is commutative and $\mathbb{Z}_n^* \subset \mathbb{Z}_n$, then multiplication modulo n over $\mathbb{Z}_n^*$ is commutative.

We prove $[1] \in \mathbb{Z}_n^*$ is a multiplicative identity.

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

Since $[1]$ is a multiplicative identity in $\mathbb{Z}_n$, then $[1][a] = [a][1] = [a]$ for every $[a] \in \mathbb{Z}_n$.

Let $[x] \in \mathbb{Z}_n^*$.

Since $\mathbb{Z}_n^* \subset \mathbb{Z}_n$, then $[x] \in \mathbb{Z}_n$, so $[1][x] = [x][1] = [x]$.

Hence, $[1][x] = [x][1] = [x]$ for all $x \in \mathbb{Z}_n^*$.

Since $[1] \in \mathbb{Z}_n^*$ and $[1][x] = [x][1] = [x]$ for all $x \in \mathbb{Z}_n^*$, then $[1] \in \mathbb{Z}_n^*$ is a multiplicative identity.

We prove for every $[x] \in \mathbb{Z}_n^*$ there is a multiplicative inverse $[y] \in \mathbb{Z}_n^*$.

Let $[x] \in \mathbb{Z}_n^*$.

Then $[x] \in \mathbb{Z}_n$ and $[x]$ is a unit, so $[x]$ has a multiplicative inverse in $\mathbb{Z}_n$.

Thus, there exists $[y] \in \mathbb{Z}_n$ such that $[x][y] = [y][x] = [1]$.

Hence, there exists $[x] \in \mathbb{Z}_n$ such that $[y][x] = [x][y] = [1]$, so $[x]$ is an inverse of $[y]$.

Consequently, $[y]$ is a unit.

Since $[y] \in \mathbb{Z}_n$ and $[y]$ is a unit, then $[y] \in \mathbb{Z}_n^*$.

Thus, there exists $[y] \in \mathbb{Z}_n^*$. such that $[x][y] = [y][x] = [1]$.

Therefore, for every $[x] \in \mathbb{Z}_n^*$ there is a multiplicative inverse $[y] \in \mathbb{Z}_n^*$ such that $[x][y] = [y][x] = [1]$.

Since multiplication modulo n is a binary operation on $\mathbb{Z}_n^*$ and multiplication modulo n over $\mathbb{Z}_n^*$ is associative and $[1] \in \mathbb{Z}_n^*$ is a multiplicative identity and for every $[x] \in \mathbb{Z}_n^*$ there is a multiplicative inverse $[y] \in \mathbb{Z}_n^*$ such that $[x][y] = [y][x] = [1]$, then $(\mathbb{Z}_n^*, \cdot)$ is a group.

Since $(\mathbb{Z}_n^*, \cdot)$ is a group and multiplication modulo n over $\mathbb{Z}_n^*$ is commutative, then $(\mathbb{Z}_n^*, \cdot)$ is an abelian group. $\square$

Proposition 25. *Let $n \in \mathbb{Z}^+$.*
Let $\mathbb{Z}_n^*$ be the group of units of $\mathbb{Z}_n$.
Then $|\mathbb{Z}_n^*| = \phi(n)$.

Proof. Let n be a positive integer.
Observe that $\mathbb{Z}_n = \{[a] : a \in \mathbb{Z}\} = \{[0], [1], ..., [n-1]\} = \{[1], [2], ..., [n-1], [n]\}$ and $\mathbb{Z}_n^* = \{[a] \in \mathbb{Z}_n : \gcd(a, n) = 1\}$.
Let $[a] \in \mathbb{Z}_n^*$.
Then $[a] \in \mathbb{Z}_n$ and $\gcd(a, n) = 1$.
Since $[a] \in \mathbb{Z}_n$, then $a \in \mathbb{Z}^+$ and $1 \leq a \leq n$.
Thus, $\mathbb{Z}_n^*$ consists of all congruence classes $[a]$ such that a is a positive integer less than or equal to n and relatively prime to n.
Therefore, $|\mathbb{Z}_n^*| = \phi(n)$. □

Complex Number Groups

Example 26. The circle group is a subgroup of $(\mathbb{C}^*, \cdot)$
Let $\mathbb{T} = \{z \in \mathbb{C} : |z| = 1\}$.
Then $(\mathbb{T}, \cdot)$ is a subgroup of $(\mathbb{C}^*, \cdot)$.

Proof. We prove using the two-step subgroup test.

We prove $\mathbb{T} \subset \mathbb{C}^*$.
Let $t \in \mathbb{T}$.
Then $t \in \mathbb{C}$ and $|t| = 1$.
Since $|t| = 1$, then $|t| \neq 0$.
Since $t \in \mathbb{C}$ and $|t| \neq 0$, then $t \neq 0$.
Since $t \in \mathbb{C}$ and $t \neq 0$, then $t \in \mathbb{C}^*$.
Therefore, $\mathbb{T} \subset \mathbb{C}^*$.

We prove $\mathbb{T}$ is not empty.
Since $1 + 0i \in \mathbb{C}$ and $|1 + 0i| = \sqrt{1^2 + 0^2} = 1$, then $1 + 0i \in \mathbb{T}$, so $\mathbb{T} \neq \emptyset$.
Therefore, $\mathbb{T}$ is not empty.

Since $\mathbb{T} \subset \mathbb{C}^*$ and $\mathbb{T}$ is not empty, then $\mathbb{T}$ is a nonempty subset of $\mathbb{C}^*$. □

Proof. We prove $\mathbb{T}$ is closed under complex multiplication.
Let $z_1, z_2 \in \mathbb{T}$.
Then $z_1 \in \mathbb{C}$ and $|z_1| = 1$ and $z_2 \in \mathbb{C}$ and $|z_2| = 1$.
Hence, there exist $\theta_1, \theta_2 \in \mathbb{R}$ such that $z_1 = |z_1|(\cos\theta_1 + i\sin\theta_1)$ and $z_2 = |z_2|(\cos\theta_2 + i\sin\theta_2)$.
Since $\mathbb{C}$ is closed under multiplication and $z_1 \in \mathbb{C}$ and $z_2 \in \mathbb{C}$, then $z_1 \cdot z_2 \in \mathbb{C}$.

Observe that

$$\begin{aligned} z_1 &= |z_1| \cdot (\cos\theta_1 + i\sin\theta_1) \\ &= 1 \cdot (\cos\theta_1 + i\sin\theta_1) \\ &= \cos\theta_1 + i\sin\theta_1 \\ &= e^{i\theta_1}. \end{aligned}$$

and

$$\begin{aligned} z_2 &= |z_2| \cdot (\cos\theta_2 + i\sin\theta_2) \\ &= 1 \cdot (\cos\theta_2 + i\sin\theta_2) \\ &= \cos\theta_2 + i\sin\theta_2 \\ &= e^{i\theta_2}. \end{aligned}$$

and

$$\begin{aligned} z_1 \cdot z_2 &= e^{i\theta_1} \cdot e^{i\theta_2} \\ &= e^{i\theta_1 + i\theta_2} \\ &= e^{i(\theta_1+\theta_2)}. \end{aligned}$$

Since $\theta_1, \theta_2 \in \mathbb{R}$, then $\theta_1 + \theta_2 \in \mathbb{R}$, so $|e^{i(\theta_1+\theta_2)}| = 1$.
Since $z_1 \cdot z_2 = e^{i(\theta_1+\theta_2)}$, then this implies $|z_1 \cdot z_2| = 1$.
Since $z_1 \cdot z_2 \in \mathbb{C}$ and $|z_1 \cdot z_2| = 1$, then $z_1 \cdot z_2 \in \mathbb{T}$.
Therefore, $\mathbb{T}$ is closed under complex multiplication. $\square$

Proof. We prove $\mathbb{T}$ is closed under inverses.
Let $z \in \mathbb{T}$.
Then $z \in \mathbb{C}$ and $|z| = 1$.
Since $z \in \mathbb{T}$ and $\mathbb{T} \subset \mathbb{C}^*$, then $z \in \mathbb{C}^*$.
Hence there exists $\frac{1}{z} \in \mathbb{C}^*$ such that $z \cdot \frac{1}{z} = \frac{1}{z} \cdot z = 1$.
Since $\frac{1}{z} \in \mathbb{C}^*$ and $\mathbb{C}^* \subset \mathbb{C}$, then $\frac{1}{z} \in \mathbb{C}$.
Observe that

$$\begin{aligned} 1 &= |1| \\ &= |z \cdot \frac{1}{z}| \\ &= |z| \cdot |\frac{1}{z}| \\ &= 1 \cdot |\frac{1}{z}| \\ &= |\frac{1}{z}|. \end{aligned}$$

Thus, $|\frac{1}{z}| = 1$.
Since $\frac{1}{z} \in \mathbb{C}$ and $|\frac{1}{z}| = 1$, then $\frac{1}{z} \in \mathbb{T}$.
Therefore, the multiplicative inverse $\frac{1}{z}$ is an element of $\mathbb{T}$ for every $z \in \mathbb{T}$, so $\mathbb{T}$ is closed under inverses.

Since $\mathbb{T}$ is a nonempty subset of $\mathbb{C}^*$ and $\mathbb{T}$ is closed under complex multiplication and $\mathbb{T}$ is closed under inverses, then by the two-step subgroup test, $(\mathbb{T}, \cdot)$ is a subgroup of $(\mathbb{C}^*, \cdot)$, so $(\mathbb{T}, \cdot)$ is a group.

Since $\mathbb{C}^*$ is an abelian group, then complex multiplication over $\mathbb{C}^*$ is commutative.

Since complex multiplication over $\mathbb{C}^*$ is commutative and $\mathbb{T} \subset \mathbb{C}^*$, then complex multiplication over $\mathbb{T}$ is commutative.

Since $(\mathbb{T}, \cdot)$ is a group and complex multiplication over $\mathbb{T}$ is commutative, then $(\mathbb{T}, \cdot)$ is an abelian group. □

Example 27. n^{th} **Roots of Unity is a subgroup of the circle group under complex multiplication**

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

Then n^{th} roots of unity $(U_n, \cdot)$ is a subgroup of the circle group $(\mathbb{T}, \cdot)$.

Proof. We prove using the two-step subgroup test.

We prove $U_n \subset \mathbb{T}$.

Let $z \in U_n$.

Then $z \in \mathbb{C}$ and $z^n = 1$.

Since $z \in \mathbb{C}$, then $z = |z| \cdot (\cos\theta + i\sin\theta)$ for some $\theta \in \mathbb{R}$.

Since $|z|^n = |z^n| = |1| = 1$, then $|z|^n = 1$, so $|z|^n - 1 = 0$.

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 $|z| - 1 = 0$.

Hence, $|z| = 1$.

Since $z \in \mathbb{C}$ and $|z| = 1$, then $z \in \mathbb{T}$.

Therefore, $U_n \subset \mathbb{T}$.

We prove U_n is not empty.

Since $1 \in \mathbb{C}$ and $1^n = 1$, then $1 \in U_n$, so $U_n \neq \emptyset$.

Therefore, U_n is not empty.

Since $U_n \subset \mathbb{T}$ and U_n is not empty, then U_n is a nonempty subset of $\mathbb{T}$. □

Proof. We prove U_n is closed under complex multiplication.

Let $z_1, z_2 \in U_n$.

Then $z_1 \in \mathbb{C}$ and $(z_1)^n = 1$ and $z_2 \in \mathbb{C}$ and $(z_2)^n = 1$.

Since $\mathbb{C}$ is closed under multiplication and $z_1 \in \mathbb{C}$ and $z_2 \in \mathbb{C}$, then $z_1 \cdot z_2 \in \mathbb{C}$.

Since $z_1, z_2 \in U_n$ and $U_n \subset \mathbb{T}$, then $z_1, z_2 \in \mathbb{T}$.

Since $(\mathbb{T}, \cdot)$ is an abelian group, then $(ab)^n = a^n b^n$ for every integer n and every $a, b \in \mathbb{T}$.

Observe that

$$\begin{aligned}(z_1 z_2)^n &= (z_1)^n \cdot (z_2)^n \\ &= 1 \cdot 1 \\ &= 1.\end{aligned}$$

Thus, $(z_1 z_2)^n = 1$.
Since $z_1 \cdot z_2 \in \mathbb{C}$ and $(z_1 z_2)^n = 1$, then $z_1 z_2 \in U_n$.
Therefore, U_n is closed under complex multiplication. $\square$

Proof. We prove U_n is closed under inverses.
Let $z \in U_n$.
Then $z \in \mathbb{C}$ and $z^n = 1$.
Since $z \in U_n$ and $U_n \subset \mathbb{T}$ and $\mathbb{T} \subset \mathbb{C}^*$, then $z \in \mathbb{C}^*$.
Hence there exists $\frac{1}{z} \in \mathbb{C}^*$ such that $z \cdot \frac{1}{z} = \frac{1}{z} \cdot z = 1$.
Since $\frac{1}{z} \in \mathbb{C}^*$ and $\mathbb{C}^* \subset \mathbb{C}$, then $\frac{1}{z} \in \mathbb{C}$.
Observe that

$$\begin{aligned}(\frac{1}{z})^n &= \frac{1}{z^n} \\ &= \frac{1}{1} \\ &= 1.\end{aligned}$$

Thus, $(\frac{1}{z})^n = 1$.
Since $\frac{1}{z} \in \mathbb{C}$ and $(\frac{1}{z})^n = 1$, then $\frac{1}{z} \in U_n$.
Therefore, the multiplicative inverse $\frac{1}{z}$ is an element of U_n for every $z \in U_n$, so U_n is closed under inverses.

Since U_n is a nonempty subset of $\mathbb{T}$ and U_n is closed under complex multiplication and U_n is closed under inverses, then by the two-step subgroup test, $(U_n, \cdot)$ is a subgroup of $(\mathbb{T}, \cdot)$, so $(U_n, \cdot)$ is a group.

Since complex multiplication over $\mathbb{C}$ is commutative and $U_n \subset \mathbb{C}$, then complex multiplication over U_n is commutative.

Since $(U_n, \cdot)$ is a group and complex multiplication over U_n is commutative, then $(U_n, \cdot)$ is an abelian group. $\square$

Example 28. Quaternion Group of Order 8 $(Q_8, \cdot)$
Let $i^2 = -1$ and define

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

$$i = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}$$

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

$$k = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}$$

Then $i^2 = j^2 = k^2 = -1$ and
$ij = k$ and $jk = i$ and $ki = j$ and
$ik = -j$ and $kj = -i$ and $ji = -k$.
Let $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$.
Then $(Q_8, \cdot)$ is a non-abelian group where $\cdot$ is matrix multiplication over $\mathbb{C}$.
$|Q_8| = 8$

·	1	-1	i	-i	j	-j	k	-k
1	1	-1	i	-i	j	-j	k	-k
-1	-1	1	-i	i	-j	j	-k	k
i	i	-i	-1	1	k	-k	-j	j
-i	-i	i	1	-1	-k	k	j	-j
j	j	-j	-k	k	-1	1	i	-i
-j	-j	j	k	-k	1	-1	-i	i
k	k	-k	j	-j	-i	i	-1	1
-k	-k	k	-j	j	i	-i	1	-1

Proof. We prove $(Q_8, \cdot)$ is a non-abelian group.

The Cayley multiplication table for Q_8 shows that the product of any two elements of Q_8 is a unique element of Q_8, so matrix multiplication is a binary operation on Q_8.

Matrix multiplication is associative in general, so matrix multiplication over $\mathbb{C}$ is associative.
Since Q_8 consists of 2×2 matrices over $\mathbb{C}$, then matrix multiplication over Q_8 is associative.

The Cayley multiplication table for Q_8 shows that $1 \cdot m = m = m \cdot 1$ for all $m \in Q_8$, so $1 \in Q_8$ is identity for $\cdot$.

The Cayley multiplication table for $(Q_8, \cdot)$ shows the following.
Since $1 \cdot 1 = 1$, then 1 is an inverse of 1.
Since $-1 \cdot -1 = 1$, then -1 is an inverse of itself.
Since $i \cdot -i = 1 = -i \cdot i$, then i and $-i$ are inverses of each other.
Since $j \cdot -j = 1 = -j \cdot j$, then j and $-j$ are inverses of each other.
Since $k \cdot -k = 1 = -k \cdot k$, then k and $-k$ are inverses of each other.
Therefore, for every $m \in Q_8$ there is a multiplicative inverse $m^{-1} \in Q_8$.

Since matrix multiplication is a binary operation on Q_8 and matrix multiplication over Q_8 is associative and $1 \in Q_8$ is a multiplicative identity for $\cdot$ and for every $m \in Q_8$ there is a multiplicative inverse $m^{-1} \in Q_8$, then $(Q_8, \cdot)$ is a group.

Since $i \cdot j = k \neq -k = j \cdot i$, then matrix multiplication over Q_8 is not commutative.

Since $(Q_8, \cdot)$ is a group and matrix multiplication over Q_8 is not commutative, then $(Q_8, \cdot)$ is a non-abelian group. $\square$

Subgroups

Example 29. For all $n \in \mathbb{Z}$, $(n\mathbb{Z}, +) < (\mathbb{Z}, +)$.

Proof. Let $n \in \mathbb{Z}$.

We prove $n\mathbb{Z} \subset \mathbb{Z}$.
Observe that $n\mathbb{Z} = \{nk : k \in \mathbb{Z}\}$.
Let $x \in n\mathbb{Z}$.
Then there exists an integer k such that $x = nk$.
By closure of $\mathbb{Z}$ under multiplication, $nk \in \mathbb{Z}$, so $x \in \mathbb{Z}$.
Therefore, $x \in n\mathbb{Z}$ implies $x \in \mathbb{Z}$, so $n\mathbb{Z} \subset \mathbb{Z}$.

We prove $n\mathbb{Z}$ is closed under addition.
Let $a, b \in n\mathbb{Z}$.
Since $a \in n\mathbb{Z}$, then $a = ns$ for some integer s.
Since $b \in n\mathbb{Z}$, then $b = nt$ for some integer t.
Thus, $a + b = ns + nt = n(s + t)$.
Since $s + t$ is an integer, then $n(s + t) \in n\mathbb{Z}$, so $a + b \in n\mathbb{Z}$.
Therefore, $n\mathbb{Z}$ is closed under addition.

We prove the additive identity $0 \in \mathbb{Z}$ is in $n\mathbb{Z}$.
Since $0 = n \cdot 0$ and $0 \in \mathbb{Z}$ is the additive identity of $\mathbb{Z}$, then $0 \in n\mathbb{Z}$.
Therefore, the additive identity $0 \in \mathbb{Z}$ is in $n\mathbb{Z}$.

We prove $n\mathbb{Z}$ is closed under inverses.
Let $nk \in n\mathbb{Z}$.
Then $k \in \mathbb{Z}$.
Since $nk+(-nk) = [n+(-n)]k = 0k = 0 = k0 = k(-n+n) = k(-n)+kn = (-n)k+nk = (-nk)+nk$, then $nk+(-nk) = 0 = (-nk)+nk$, so $-nk$ is additive inverse of nk.

Since $-nk = n(-k)$ and $-k \in \mathbb{Z}$, then $-nk \in n\mathbb{Z}$.

Therefore, for every $nk \in n\mathbb{Z}$, there is an additive inverse $-nk$ in $n\mathbb{Z}$, so $n\mathbb{Z}$ is closed under inverses.

Since $n\mathbb{Z} \subset \mathbb{Z}$ and $n\mathbb{Z}$ is closed under addition and the additive identity $0 \in \mathbb{Z}$ is in $n\mathbb{Z}$ and $n\mathbb{Z}$ is closed under inverses, then by the first subgroup test, $n\mathbb{Z}$ is a subgroup of $\mathbb{Z}$. $\square$

Example 30. $(\mathbb{Z}, +) < (\mathbb{Q}, +)$.

Proof. Let $n \in \mathbb{Z}$. Then $n = \frac{n}{1}$. Since $1, n \in \mathbb{Z}$ and $1 \neq 0$, then $n \in \mathbb{Q}$. Hence, $n \in \mathbb{Z}$ implies $n \in \mathbb{Q}$, so $\mathbb{Z} \subset \mathbb{Q}$.

Since $\mathbb{Z}$ is an additive group, then $\mathbb{Z}$ is closed under addition .

The additive identity of $\mathbb{Q}$ is zero. Since 0 is an integer, then the additive identity of $\mathbb{Q}$ is in $\mathbb{Z}$.

Let $n \in \mathbb{Z}$. Since $\mathbb{Z} \subset \mathbb{Q}$, then $n \in \mathbb{Q}$. The additive inverse of n in $\mathbb{Q}$ is $-n$. Since $-n$ is also an integer, then $\mathbb{Z}$ is closed under taking of inverses.

Therefore, $\mathbb{Z}$ is a subgroup of the additive group $\mathbb{Q}$. $\square$

Cyclic Groups

Example 31. $(\mathbb{Z}, +)$ is a cyclic group.

Proof. The set of all integers under addition is the group $(\mathbb{Z}, +)$.

The cyclic subgroup generated by 1 is the set of all multiples of 1.

Therefore, $\langle 1 \rangle = \{k \cdot 1 : k \in \mathbb{Z}\} = \{k : k \in \mathbb{Z}\} = \mathbb{Z}$.

Since $1 \in \mathbb{Z}$ and $\mathbb{Z} = \langle 1 \rangle$, then $\mathbb{Z}$ is cyclic with generator 1.

The cyclic subgroup generated by -1 is the set of all multiples of -1.

Therefore, $\langle -1 \rangle = \{k(-1) : k \in \mathbb{Z}\} = \{-k : k \in \mathbb{Z}\} = \mathbb{Z}$.

Since $-1 \in \mathbb{Z}$ and $\mathbb{Z} = \langle -1 \rangle$, then $\mathbb{Z}$ is cyclic with generator -1.

Therefore, $\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$ and both 1 and -1 are generators of $\mathbb{Z}$. $\square$

Example 32. Let $n \in \mathbb{Z}$.

Then $(n\mathbb{Z}, +)$ is a cyclic group.

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

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

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

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

The cyclic subgroup generated by $-n$ is the set of all multiples of $-n$.

Therefore, $\langle -n \rangle = \{k(-n) : k \in \mathbb{Z}\} = \{-kn : k \in \mathbb{Z}\} = n\mathbb{Z}$.

Since $-n \in \mathbb{Z}$ and $n\mathbb{Z} = \langle -n \rangle$, then $n\mathbb{Z}$ is cyclic with generator $-n$.

Therefore, $n\mathbb{Z} = \langle n \rangle = \langle -n \rangle$ and both n and $-n$ are generators of $n\mathbb{Z}$. $\square$

Example 33. $(\mathbb{Z}_n, +)$ is a cyclic group.

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

The set of integers modulo n under addition is the group $(\mathbb{Z}_n, +)$ and $\mathbb{Z}_n = \{[0], [1], ..., [n-1]\}$.

The cyclic subgroup generated by $[1]$ is the set of all multiples of $[1]$ modulo n.

Therefore, $\langle [1] \rangle = \{k[1] : k \in \mathbb{Z}\} = \{[k] : k \in \mathbb{Z}\} = \{[0], [1], ..., [n-1]\} = \mathbb{Z}_n$.

Since $[1] \in \mathbb{Z}_n$ and $\mathbb{Z}_n = \langle [1] \rangle$, then $\mathbb{Z}_n$ is a cyclic group with generator $[1]$. $\square$

Example 34. The set of all linear combinations of positive integers a **and** b **under addition is a cyclic group with generator** $\gcd(a, b)$

Let $a, b \in \mathbb{Z}^+$.

Let $G = \{ma + nb : m, n \in \mathbb{Z}\}$.

Then $(G, +)$ is a cyclic group with generator $\gcd(a, b)$.

Proof. We prove $(G, +)$ is a group.

We prove addition is a binary operation on G.

Let $x, y \in G$.

Since $x \in G$ then there exist integers m_1 and n_1 such that $x = m_1 a + n_1 b$.

Since $y \in G$ then there exist integers m_2 and n_2 such that $y = m_2 a + n_2 b$.

Observe that

$$\begin{aligned} x + y &= (m_1 a + n_1 b) + (m_2 a + n_2 b) \\ &= m_1 a + (n_1 b + m_2 a) + n_2 b \\ &= m_1 a + (m_2 a + n_1 b) + n_2 b \\ &= (m_1 a + m_2 a) + (n_1 b + n_2 b) \\ &= (m_1 + m_2) a + (n_1 + n_2) b. \end{aligned}$$

Since $m_1, m_2 \in \mathbb{Z}$, then $m_1 + m_2 \in \mathbb{Z}$.

Since $n_1, n_2 \in \mathbb{Z}$, then $n_1 + n_2 \in \mathbb{Z}$.

Since $m_1 + m_2 \in \mathbb{Z}$ and $n_1 + n_2 \in \mathbb{Z}$ and $x + y = (m_1 + m_2)a + (n_1 + n_2)b$, then $x + y \in G$, so G is closed under addition.

Therefore, addition is a binary operation on G.

We prove addition over G is associative.

Since addition of integers is associative and $G \subset \mathbb{Z}$, then addition over G is associative.

We prove $0 \in G$ is an additive identity.

Since $0 \in \mathbb{Z}$ and $0 = 0 + 0 = 0a + 0b$, then $0 \in G$.

Let $x \in G$.

Then there exist integers m and n such that $x = ma + nb$.

Observe that

$$
\begin{aligned}
x+0 &= (ma+nb)+(0a+0b) \\
&= ma+(nb+0a)+0b \\
&= ma+(0a+nb)+0b \\
&= (ma+0a)+(nb+0b) \\
&= (m+0)a+(n+0)b \\
&= ma+nb \\
&= x \\
&= ma+nb \\
&= (0+m)a+(0+n)b \\
&= (0a+ma)+(0b+nb) \\
&= 0a+(ma+0b)+nb \\
&= 0a+(0b+ma)+nb \\
&= (0a+0b)+(ma+nb) \\
&= 0+x
\end{aligned}
$$

Thus, $x+0=x=0+x$.
Since $0 \in G$ and $x+0=x=0+x$, then $0 \in G$ is an additive identity.

We prove for every $ma+nb \in G$ there exists an inverse $-ma-nb \in G$.
Let $x \in G$.
Then there exist $m,n \in \mathbb{Z}$ such that $x=ma+nb$.
Since $m,n \in \mathbb{Z}$, then $-m,-n \in \mathbb{Z}$.
Let $y=-ma-nb$.
Since $y=-ma-nb=(-m)a+(-n)b$ and $m,-n \in \mathbb{Z}$, then $y \in G$.
Observe that

$$
\begin{aligned}
x+y &= (ma+nb)+(-ma-nb) \\
&= ma+(nb-ma)-nb \\
&= ma+(-ma+nb)-nb \\
&= (ma-ma)+(nb-nb) \\
&= 0+0 \\
&= 0 \\
&= 0+0 \\
&= (-ma+ma)+(-nb+nb) \\
&= -ma+(ma-nb)+nb \\
&= -ma+(-nb+ma)+nb \\
&= (-ma-nb)+(ma+nb) \\
&= y+x.
\end{aligned}
$$

Thus, $x + y = 0 = y + x$.

Therefore, for every $ma+nb \in G$ there exists an additive inverse $-ma-nb \in G$.

Since addition is a binary operation on G and addition over G is associative and $0 \in G$ is an additive identity and for every $ma + nb \in G$ there exists an additive inverse $-ma - nb \in G$, then $(G, +)$ is a group. □

Proof. We prove G is cyclic.

Let $d = \gcd(a, b)$.

Since d is the greatest common divisor of a and b, then d is the least positive linear combination of a and b, so there exist integers m and n such that $d = ma + nb$.

Therefore, $d \in G$.

Let G' be the cyclic subgroup generated by d.

Then $G' = \{kd : k \in \mathbb{Z}\}$.

We must prove $G = G'$.

We prove $G \subset G'$.

Let $x \in G$.

Then there exist integers r and s such that $x = ra + sb$, so x is a linear combination of a and b.

Since any common divisor of a and b divides any linear combination of a and b, then the greatest common divisor of a and b divides x, so $d|x$.

Hence, $x = dt$ for some integer t, so $x \in G'$.

Therefore, $G \subset G'$.

We prove $G' \subset G$.

Let $y \in G'$.

Then there exists an integer k such that $y = kd$.

Thus, $y = kd = k(ma + nb) = kma + knb = (km)a + (kn)b$.

Since $y = (km)a + (kn)b$ and $km, kn \in \mathbb{Z}$, then $y \in G$, so $G' \subset G$.

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

Therefore, there exists $d \in G$ such that $G = G' = \{kd : k \in \mathbb{Z}\}$, so G is cyclic. □

Example 35. The group $(\mathbb{Q}, +)$ is not cyclic.

Proof. Suppose $(\mathbb{Q}, +)$ is cyclic.

Then there exists $q \in \mathbb{Q}$ such that $\mathbb{Q} = \langle q \rangle = \{nq : n \in \mathbb{Z}\}$.

Since $q \in \mathbb{Q}$, then there exist integers a, b with $b \neq 0$ such that $q = \frac{a}{b}$.

Suppose $q = 0$.
Then $\mathbb{Q} = \{nq : n \in \mathbb{Z}\} = \{n0 : n \in \mathbb{Z}\} = \{0\}$, so $\mathbb{Q} = \{0\}$.
But, $\mathbb{Q} \neq \{0\}$, so $q \neq 0$.
Since $q = \frac{a}{b}$ and $b \neq 0$ and $q \neq 0$, then $a \neq 0$.

Either $b|a$ or $b \not| a$.
We consider these cases separately.
Case 1: Suppose $b|a$.
Then $\frac{a}{b} \in \mathbb{Z}$.
Since $q = \frac{a}{b}$, then $q \in \mathbb{Z}$.
Let $x = \frac{q}{2}$.
Since $q \in \mathbb{Z}$ and $2 \in \mathbb{Z}$ and $2 \neq 0$, then $\frac{q}{2} \in \mathbb{Q}$, so $x \in \mathbb{Q}$.
Since $\mathbb{Q} = \{nq : n \in \mathbb{Z}\}$, then there exists an integer n such that $x = nq$, so $\frac{q}{2} = nq$.
Hence, $q = 2nq$, so $2nq = q$.
Since $q \neq 0$, then $2n = 1$, so 1 is even.
But, this contradicts that 1 is odd.
Case 2: Suppose $b \not| a$.
Let $y = \frac{a}{2b}$.
Since $a \in \mathbb{Z}$ and $2b \in \mathbb{Z}$ and $2b \neq 0$, then $y \in \mathbb{Q}$.
Since $\mathbb{Q} = \{nq : n \in \mathbb{Z}\}$, then there exists an integer n such that $y = nq$, so $\frac{a}{2b} = y = nq = \frac{na}{b}$.
Thus, $\frac{a}{2b} = \frac{na}{b}$, so $ab = 2nab$.
Since $a, b \in \mathbb{Z}$ and $a \neq 0$ and $b \neq 0$, then $ab \neq 0$, so cancelling, we obtain $1 = 2n$.
But, $1 = 2n$ implies 1 is even which contradicts 1 is odd.

Therefore, in all cases, a contradiction is reached, so $(\mathbb{Q}, +)$ cannot be cyclic. $\square$

Example 36. The group $(\mathbb{R}, +)$ is not cyclic.

Proof. Suppose $(\mathbb{R}, +)$ is cyclic.
Then there exists $g \in \mathbb{R}$ such that $\mathbb{R} = \{ng : n \in \mathbb{Z}\}$.
Therefore, every real number is an integer multiple of g.
Since $g \in \mathbb{R}$, then either $g = 0$ or $g \neq 0$.
We consider these cases separately.
Case 1: Suppose $g = 0$.
Then $\mathbb{R} = \{ng : n \in \mathbb{Z}\} = \{n \cdot 0 : n \in \mathbb{Z}\} = \{0\}$.
But, $\mathbb{R} \neq \{0\}$.
Case 2: Suppose $g \neq 0$.
Since $g \in \mathbb{R}$, then $\frac{g}{2} \in \mathbb{R}$.
Since $\frac{1}{2} \notin \mathbb{Z}$, then $\frac{g}{2}$ is not an integer multiple of g.
Thus, there exists $\frac{g}{2} \in \mathbb{R}$ such that $\frac{g}{2}$ is not an integer multiple of g.
But, this contradicts the assumption that every real number is an integer multiple of g.

TODO THIS PROOF IS NOT CORRECT b/c we could have $g/2$ be an integer when g is even.

So, we need to re-work this proof!!!

Hence, in all cases, we have a contradiction.

Therefore, $(\mathbb{R}, +)$ is not cyclic. $\square$

Example 37. $(\mathbb{Q}^*, \cdot)$ is not a cyclic group.

Solution. We must disprove that $\mathbb{Q}^*$ is cyclic.

By definition of cyclic group $\mathbb{Q}^*$ is cyclic iff $\exists g \in \mathbb{Q}^*$ such that $\mathbb{Q}^* = \{g^n : n \in \mathbb{Z}\}$.

We know $\mathbb{Q}^* = \{\frac{a}{b} : a, b \in \mathbb{Z}^*\}$. $\square$

Proof. Suppose the group $(\mathbb{Q}^*, \cdot)$ is cyclic.

Then there is $g \in \mathbb{Q}^*$ such that $\mathbb{Q}^* = \{g^n : n \in \mathbb{Z}\}$.

Since $g \in \mathbb{Q}^*$, then $g = \frac{p}{q}$ and $p, q \in \mathbb{Z}^*$.

TODO RE work this proof b/c this is not correct.

Let $n \in \mathbb{Z}$.

Either $|(\frac{p}{q})^n| < 1$ or $|(\frac{p}{q})^n| \geq 1$.

There are two cases to consider.

Case 1: Suppose $|(\frac{p}{q})^n| < 1$.

Then no rational number greater than or equal to one can be represented by any power of g.

For example, 2 cannot be represented by any power of g.

Case 2: Suppose $|(\frac{p}{q})^n| \geq 1$.

Then no positive rational number less than one can be represented by any power of g.

For example, $\frac{1}{2}$ cannot be represented by any power of g.

Hence, in either case at least one nonzero rational number cannot be expressed as a power of g.

Therefore, $g \in \mathbb{Q}^*$ cannot be a generator of $\mathbb{Q}^*$.

Thus, there is no generator in $\mathbb{Q}^*$ that can generate all of $\mathbb{Q}^*$.

Hence, $(\mathbb{Q}^*, \cdot)$ is not cyclic. $\square$

Example 38. Circle group is not cyclic.

Let $\mathbb{T} = \{z \in \mathbb{C} : |z| = 1\}$.

Then $(\mathbb{T}, \cdot)$ is not cyclic.

Proof. We use proof by contradiction.

Suppose $(\mathbb{T}, \cdot)$ is cyclic.

Then there exists $g \in \mathbb{T}$ such that $\mathbb{T} = \{g^n : n \in \mathbb{Z}\}$.

Since $g \in \mathbb{T}$, then $g \in \mathbb{C}$ and $|g| = 1$.

Since $g \in \mathbb{C}$, then there exists $\theta \in \mathbb{R}$ such that $g = |g| \cdot \text{cis } \theta = 1 \cdot \text{cis } \theta = \text{cis } \theta = e^{i\theta}$, so $g = e^{i\theta}$.

We prove $\theta \neq 0$.
Suppose $\theta = 0$.
Then $g = e^{i\theta} = e^{i(0)} = e^0 = 1$, so $g = 1$.
Thus, $\mathbb{T} = \{g^n : n \in \mathbb{Z}\} = \{1^n : n \in \mathbb{Z}\} = \{1\}$, so $\mathbb{T} = \{1\}$.
Since $-1 = -1 + 0i$, then $-1 \in \mathbb{C}$.
Since $-1 \in \mathbb{C}$ and $|-1| = 1$, then $-1 \in \mathbb{T}$.
Since $\mathbb{T} = \{1\}$, then this implies $-1 \in \{1\}$, a contradiction.
Hence, $\theta \neq 0$.

Let $t = e^{i\frac{\theta}{2}}$.
Then $t \in \mathbb{C}$.
Since $\frac{\theta}{2} \in \mathbb{R}$, then $|e^{i\frac{\theta}{2}}| = 1$, so $|t| = 1$.
Since $t \in \mathbb{C}$ and $|t| = 1$, then $t \in \mathbb{T}$.
Hence, there exists an integer n such that $t = g^n$.
Observe that

$$\begin{aligned} e^{i\frac{\theta}{2}} &= t \\ &= g^n \\ &= (e^{i\theta})^n \\ &= e^{in\theta}. \end{aligned}$$

Thus, $e^{i\frac{\theta}{2}} = e^{in\theta}$, so $\frac{\theta}{2} = n\theta$.
Hence, $\theta = 2n\theta$.
Since $\theta \neq 0$, we divide to obtain $1 = 2n$.
Thus, 1 is even, a contradiction.
Consequently, there is no integer n such that $t = g^n$.
Thus, there is no $g \in \mathbb{T}$ such that $\mathbb{T} = \{g^n : n \in \mathbb{Z}\}$.
Therefore, $(\mathbb{T}, \cdot)$ is not cyclic. □

Example 39. The n^{th} roots of unity is a cyclic group.
The group $(U_n, \cdot)$ is cyclic with generator $e^{i\frac{2\pi}{n}}$ and has order $|U_n| = n$.

Proof. Let n be a positive integer.
Let $U_n = \{z \in \mathbb{C} : z^n = 1\}$ be the n^{th} roots of unity.
Let $g = \text{cis } \frac{2\pi}{n}$.
Then $g \in \mathbb{C}$ and $g = e^{i\frac{2\pi}{n}}$.
Observe that

$$\begin{aligned} g^n &= (e^{\frac{2\pi i}{n}})^n \\ &= e^{2\pi i} \\ &= 1. \end{aligned}$$

Since $g \in \mathbb{C}$ and $g^n = 1$, then $g \in U_n$.
Every element of a group G generates a cyclic subgroup of G.
Since U_n is a group and $g \in U_n$, then g generates a cyclic subgroup of U_n.
Let G be the cyclic subgroup of U_n generated by g.

Then

$$\begin{aligned} G &= \{g^k : k \in \mathbb{Z}\} \\ &= \{(e^{i\frac{2\pi}{n}})^k : k \in \mathbb{Z}\} \\ &= \{e^{i\frac{2k\pi}{n}} : k \in \mathbb{Z}\}. \end{aligned}$$

Since G is a subgroup of U_n, then G is a subset of U_n, so $G \subset U_n$.

We prove $|g| = n$.
For $k = 0$, $g^0 = e^{i0} = e^0 = 1$.
For $k = 1$, $g^1 = g = e^{i\frac{2\pi}{n}} = e^{i2\pi\frac{1}{n}}$.
For $k = 2$, $g^2 = (e^{i\frac{2\pi}{n}})^2 = e^{i2\pi\frac{2}{n}}$.
For $k = 3$, $g^3 = (e^{i\frac{2\pi}{n}})^3 = e^{i2\pi\frac{3}{n}}$.
...
For $k = n-1$, $g^{n-1} = (e^{i\frac{2\pi}{n}})^{n-1} = e^{i2\pi\frac{n-1}{n}}$.
For $k = n$, $g^n = (e^{i\frac{2\pi}{n}})^n = e^{i2\pi} = 1$.
Therefore, g has finite order n, so $|g| = n$.
Since the order of $g \in U_n$ is the order of the cyclic subgroup of U_n generated by g, then $n = |g| = |G|$, so $n = |G|$.

We prove $|U_n| = n$.
Since $U_n = \{z \in \mathbb{C} : z^n = 1\}$, then $z \in U_n$ iff $z^n = 1$ iff $z^n - 1 = 0$.
By the fundamental theorem of algebra, a polynomial of degree n has at most n zeros.
Hence, $z^n - 1$ has at most n zeroes, so there are at most n elements in U_n.
Therefore, $|U_n| \leq n$.

Since U_n has order at most n, then U_n is a finite group.
Since $G \subset U_n$ and U_n is finite and $|G| = n$, then U_n has at least n elements, so $|U_n| \geq n$.
Since $|U_n| \leq n$ and $n \leq |U_n|$, then $|U_n| = n$, so $|U_n| = |G|$.

Since U_n is finite and $G \subset U_n$ and $|G| = |U_n|$, then $G = U_n$.
Since $g \in U_n$ and $U_n = G$, then U_n is cyclic, as desired. □

Multiplicative Matrix Groups

Example 40. General linear group is a group under matrix multiplication
Let F be a field.
Then $GL_n(F)$ is a group under matrix multiplication.

Proof. We prove matrix multiplication is a binary operation on $GL_n(F)$.

Let $A, B \in GL_n(F)$.

Then A and B are $n \times n$ invertible matrices with entries in F.

The product of any two square matrices is a unique square matrix, so AB is a unique $n \times n$ matrix.

Since A and B are invertible, then A^{-1} and B^{-1} exist and are square matrices.

Thus, $B^{-1}A^{-1}$ is a square matrix.

Observe that

$$\begin{aligned} (AB)(B^{-1}A^{-1}) &= A(BB^{-1})A^{-1} \\ &= AIA^{-1} \\ &= AA^{-1} \\ &= I \end{aligned}$$

and

$$\begin{aligned} (B^{-1}A^{-1})(AB) &= B^{-1}(A^{-1}A)B \\ &= B^{-1}IB \\ &= B^{-1}B \\ &= I \end{aligned}$$

Hence, AB is invertible.

Since AB is an invertible square matrix, then $AB \in GL_n(F)$.

Since AB is a unique invertible square matrix in $GL_n(F)$, then matrix multiplication is a binary operation on $GL_n(F)$.

Matrix multiplication is associative.

In particular, matrix multiplication over $GL_n(F)$ is associative.

We prove I is an identity for matrix multiplication for $GL_n(F)$.

Let I be the identity $n \times n$ matrix.

Since $I^2 = I$, then I is invertible, so $I \in GL_n(F)$.

Since I is a square matrix and $AI = IA = A$ for all $A \in GL_n(F)$, then I is an identity for matrix multiplication in $GL_n(F)$.

We prove every $A \in GL_n(F)$ has a multiplicative inverse in $GL_n(F)$.

Let $A \in GL_n(F)$.

Then A is a square invertible matrix.

Since A is invertible, then its inverse exists.

Let A^{-1} be the inverse matrix of A.

Then A^{-1} is a square matrix and $AA^{-1} = A^{-1}A = I$.

Thus, $A^{-1}A = AA^{-1} = I$, so A^{-1} is invertible.

Therefore, A^{-1} is an invertible square matrix, so $A^{-1} \in GL_n(F)$.

Since matrix multiplication is a binary operation on $GL_n(F)$ and matrix multiplication over $GL_n(F)$ is associative and the identity matrix I is an identity for matrix multiplication and every square invertible matrix A has an inverse matrix $A^{-1} \in GL_n(F)$, then $(GL_n(F), \cdot)$ is a group. $\square$

Permutation Groups

Example 41. $(S_3, \circ)$ **is a non-abelian group.**

Let $S = \{1, 2, 3\}$.

Then $|S_3| = 3! = 6$, so there are 6 permutations of S.

The permutations are:

I. (1)

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = \text{ motion that does nothing (identity permutation)}$$

II. (2 3)

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \text{ keep position 1 fixed, and swap 2 and 3}$$

III. (1 2)

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \text{ keep position 3 fixed, and swap 1 and 2}$$

IV. (1 2 3)

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \text{ rotate each position once to the left}$$

V. (1 3 2)

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \text{ rotate each position once to the right}$$

VI. (1 3)

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \text{ keep position 2 fixed, and swap 1 and 3}$$

The Cayley table for $(S_3, \circ)$ is shown below.

$\circ$	(1)	(1 2)	(1 3)	(2 3)	(1 2 3)	(1 3 2)
(1)	(1)	(1 2)	(1 3)	(2 3)	(1 2 3)	(1 3 2)
(1 2)	(1 2)	(1)	(1 3 2)	(1 2 3)	(2 3)	(1 3)
(1 3)	(1 3)	(1 2 3)	(1)	(1 3 2)	(1 2)	(2 3)
(2 3)	(2 3)	(1 3 2)	(1 2 3)	(1)	(1 3)	(1 2)
(1 2 3)	(1 2 3)	(1 3)	(2 3)	(1 2)	(1 3 2)	(1)
(1 3 2)	(1 3 2)	(2 3)	(1 2)	(1 3)	(1)	(1 2 3)

Isomorphisms

Example 42. Let $(U_4, \cdot)$ be the fourth roots of unity with complex multiplication and $(\mathbb{Z}_4, +)$ be the group of integers modulo 4 under addition.

Then $(\mathbb{Z}_4, +) \cong (U_4, \cdot)$.

Proof. Let $\phi : \mathbb{Z}_4 \to U_4$ be a binary relation defined by $\phi([k]) = i^k$ for all $[k] \in \mathbb{Z}_4$.

The domain is $\mathbb{Z}_4 = \{[0], [1], [2], [3]\}$.

Observe that $U_4 = \{(\text{cis } \frac{2\pi}{4})^k : k \in \mathbb{Z}\} = \{(\text{cis } \frac{\pi}{2})^k : k \in \mathbb{Z}\} = \{i^k : k \in \mathbb{Z}\} = \{1, i, -1, -i\}$.

Observe that $\phi([0]) = i^0 = 1$ and $\phi([1]) = i^1 = i$ and $\phi([2]) = i^2 = -1$ and $\phi([3]) = i^3 = -i$.

Thus, ϕ is a function.

Since $\phi(\mathbb{Z}_4) = U_4$, then ϕ is surjective.

Clearly, ϕ is injective.

Since ϕ is injective and surjective, then ϕ is bijective.

Let $[a], [b] \in \mathbb{Z}_4$.

Then $a, b \in \mathbb{Z}$ and $\phi([a] + [b]) = \phi([a + b]) = i^{a+b} = i^a i^b = \phi([a])\phi([b])$.

Therefore, ϕ is a homomorphism.

Since ϕ is a bijective and ϕ is a homomorphism, then $\phi : \mathbb{Z}_4 \to U_4$ is an isomorphism.

Therefore, $(\mathbb{Z}_4, +) \cong (U_4, \cdot)$. ∎

Example 43. Complex conjugation is an automorphism of the additive group of complex numbers.

Let $(\mathbb{C}, +)$ be the additive group of complex numbers.

Then $\phi : \mathbb{C} \to \mathbb{C}$ defined by $\phi(a + bi) = a - bi$ is an automorphism of $\mathbb{C}$.

Proof. Let $a + bi, c + di \in \mathbb{C}$.

Then $a, b, c, d \in \mathbb{R}$.

Clearly, ϕ is a function.

Observe that

$$\begin{aligned}
\phi((a + bi) + (c + di)) &= \phi((a + c) + (b + d)i) \\
&= (a + c) - (b + d)i \\
&= (a - bi) + (c - di) \\
&= \phi(a + bi) + \phi(c + di).
\end{aligned}$$

Therefore, ϕ is a homomorphism.

Let $a+bi, c+di \in \mathbb{C}$.
Suppose $\phi(a+bi) = \phi(c+di)$.
Then $a-bi = c-di$, so $a=c$ and $b=d$.
If $z_1 = a+bi$ and $z_2 = c+di$, then $z_1 = z_2$ iff $a=c$ and $b=d$.
Hence, $z_1 = z_2$, so $a+bi = c+di$.
Thus, $\phi(a+bi) = \phi(c+di)$ implies $a+bi = c+di$, so ϕ is injective.

Let $a+bi \in \mathbb{C}$.
Then $a, b \in \mathbb{R}$, so $a-bi \in \mathbb{C}$.
Observe that $\phi(a-bi) = \phi(a+(-b)i) = a-(-b)i = a+bi$.
Hence, there exists $a-bi \in \mathbb{C}$ such that $\phi(a-bi) = a+bi$, so ϕ is surjective.
Since ϕ is injective and surjective, then ϕ is bijective.
Since ϕ is bijective and ϕ is a homomorphism, then $\phi : \mathbb{C} \to \mathbb{C}$ is an isomorphism, so ϕ is an automorphism of $\mathbb{C}$. ☐

Example 44. Complex conjugation is an automorphism of the multiplicative group of nonzero complex numbers.
Let $(\mathbb{C}^*, \cdot)$ be the multiplicative group of nonzero complex numbers.
Then $\phi : \mathbb{C}^* \to \mathbb{C}^*$ defined by $\phi(a+bi) = a-bi$ is an automorphism of $\mathbb{C}^*$.

Proof. Let $a+bi, c+di \in \mathbb{C}^*$.
Then $a, b, c, d \in \mathbb{R}$ and $a+bi \neq 0$ and $c+di \neq 0$.
Clearly, ϕ is a function.
Observe that

$$\begin{aligned}
\phi((a+bi)(c+di)) &= \phi(ac+adi+bci-bd) \\
&= \phi((ac-bd)+(ad+bc)i) \\
&= (ac-bd)-(ad+bc)i \\
&= ac-bd-adi-bci \\
&= a(c-di)-bci+bdi^2 \\
&= a(c-di)-bi(c-di) \\
&= (a-bi)(c-di) \\
&= \phi(a+bi)\phi(c+di).
\end{aligned}$$

Therefore, ϕ is a homomorphism.

Let $a+bi, c+di \in \mathbb{C}^*$.
Suppose $\phi(a+bi) = \phi(c+di)$.
Then $a-bi = c-di$, so $a=c$ and $b=d$.
If $z_1 = a+bi$ and $z_2 = c+di$, then $z_1 = z_2$ iff $a=c$ and $b=d$.
Hence, $z_1 = z_2$, so $a+bi = c+di$.
Thus, $\phi(a+bi) = \phi(c+di)$ implies $a+bi = c+di$, so ϕ is injective.

Let $a + bi \in \mathbb{C}^*$.

Then $a, b \in \mathbb{R}$ and a and b are not both zero.

A complex number $z = x - yi$ is zero iff $x = y = 0$.

Hence, a complex number $z = x - yi$ is nonzero iff either $x \neq 0$ or $y \neq 0$.

Since a and b are not both zero, then either a is nonzero or b is nonzero.

Thus, $a - bi \in \mathbb{C}^*$.

Observe that $\phi(a - bi) = \phi(a + (-b)i) = a - (-b)i = a + bi$.

Hence, there exists $a - bi \in \mathbb{C}^*$ such that $\phi(a - bi) = a + bi$, so ϕ is surjective.

Since ϕ is injective and surjective, then ϕ is bijective.

Since ϕ is bijective and ϕ is a homomorphism, then $\phi : \mathbb{C}^* \to \mathbb{C}^*$ is an isomorphism, so ϕ is an automorphism of $\mathbb{C}^*$. $\square$