Group Theory Notes

Jason Sass

July 24, 2023

Binary Operations

Definition 1. binary operation on a set

A **binary operation on a set** S is a function from $S \times S$ to S.
Therefore $*$ is a **binary operation on** S iff $* : S \times S \to S$ is a function.

Let S be a set.
Let $*$ be a binary operation on S.
Then $* : S \times S \to S$ is a function.
Let $(a, b) \in S \times S$.
The image of (a, b) under $*$ is denoted $a * b$.
Therefore $(a, b) \mapsto a * b$ for each $(a, b) \in S \times S$.
Thus, $*$ assigns the unique element $a * b \in S$ to each ordered pair of elements $(a, b) \in S \times S$.
Hence, $*$ assigns the unique element $a * b \in S$ for every $a, b \in S$.
Therefore, a binary operation on a set S is a rule for combining two elements of S to produce a third element of S.

Definition 2. closure of a set

Let $*$ be a binary operation defined on a set S.
Then S is **closed under** $*$ iff $(\forall a, b \in S)(a * b \in S)$.

Therefore, S is not closed under $*$ iff $(\exists a, b \in S)(a * b \notin S)$.

Theorem 3. *Properties of binary operations*

Let $*$ be a binary operation on a set S. Then
1. ***Closure**: S is closed under $*$.*
2. ***Well defined**: $(\forall a, b, c, d \in S)(a = c \land b = d \to a * b = c * d)$. Law of Substitution.*
3. ***Left multiply** $(\forall a, b, c \in S)(a = b \to c * a = c * b)$.*
4. ***Right multiply** $(\forall a, b, c \in S)(a = b \to a * c = b * c)$.*

Let $* : S \times S \to S$ be a binary relation from $S \times S$ to S defined by $a * b$ for all $(a, b) \in S \times S$.
Then $*$ is a binary operation on S iff $* : S \times S \to S$ is **well defined**.

Therefore, $*$ is a binary operation on S iff

1. Existence: $a * b \in S$ for every $(a, b) \in S \times S$.

This is the same as:

Closure: $(\forall a, b \in S)(a * b \in S)$.

2. Uniqueness: $a * b$ is unique for every $(a, b) \in S \times S$.

This is the same as: $(\forall a, b \in S)(a * b$ is unique$)$.

If $(a, b), (c, d) \in S \times S$ such that $(a, b) = (c, d)$, then $a = c$ and $b = d$, so $a * b = c * d$.

Definition 4. binary algebraic structure

A **binary structure** $(S, *)$ is a nonempty set S with a binary operation $*$ defined on S.

Let $(S, *)$ be a binary structure.

Since $*$ is a binary operation on set S, then S is closed under $*$.

Therefore, a binary structure is closed under its binary operation.

Definition 5. Atttributes of binary operations

Let $*$ be a binary operation defined over a set S.

1. $*$ is **associative** iff $(a * b) * c = a * (b * c)$ for all $a, b, c \in S$.
2. $*$ is **commutative** iff $a * b = b * a$ for all $a, b \in S$.

Let $*$ be a binary operation defined over a set S.

The binary operation $*$ is not associative iff $(\exists, a, b, c \in S)$ such that $(a*b)c \neq a * (b * c)$.

The binary operation $*$ is not commutative iff $(\exists a, b \in S)$ such that $a * b \neq b * a$.

Let S be finite, $|S| = n, n \in \mathbb{Z}^+$.

Since $\exists n^{n^2}$ binary operations on S, then $\exists n^{n^2}$ finite binary structures.

Since $\exists n^{n(n+1)/2}$ commutative binary operations on S, then $\exists n^{n(n+1)/2}$ finite commutative binary structures.

Let S be a finite set with $|S| = n, n \in \mathbb{Z}^+$.

Then there are $n^{(n^2)}$ binary operations on S.

There are $n^{n(n+1)/2}$ commutative binary operations on S.

How many associative binary operations exist?

Definition 6. left and right identity elements

Let $(S, *)$ be a binary structure.

An element $e \in S$ is a **left identity** with respect to $*$ iff $(\forall a \in S)(e * a = a)$.

An element $e \in S$ is a **right identity** with respect to $*$ iff $(\forall a \in S)(a*e = a)$.

Definition 7. identity element

Let $(S, *)$ be a binary structure.

An element $e \in S$ is an **identity** with respect to $*$ iff $(\forall a \in S)(e*a = a*e = a)$.

Proposition 8. *If a binary structure has an identity element, then the identity element is unique.*

Let $(S, *)$ be a binary structure with identity $e \in S$.
Then e is unique.

Definition 9. left and right inverse elements
Let $(S, *)$ be a binary structure with identity $e \in S$.
Let $a \in S$.
An element $b \in S$ is a **left inverse** of a iff $b * a = e$.
An element $b \in S$ is a **right inverse** of a iff $a * b = e$.

Definition 10. inverse element
Let $(S, *)$ be a binary structure with identity $e \in S$.
Let $a \in S$.
Then a is **invertible** iff there exists $b \in S$ such that $a * b = b * a = e$.
Therefore a is invertible iff $(\exists b \in S)(a * b = b * a = e)$.

Let $(S, *)$ be a binary structure with identity $e \in S$.
Let $a \in S$.
We say that a is invertible iff a has an inverse in S.
Therefore, a is invertible iff $(\exists b \in S)(a * b = b * a = e)$ and we say that b is an inverse of a.

Proposition 11. *Let $(S, *)$ be an associative binary structure with identity.*
Then
1. The inverse of every invertible element of S is unique.
2. Let $a \in S$.
If a is invertible, then $(a^{-1})^{-1} = a$. ***inverse of an inverse***
3. Let $a, b \in S$.
If a and b are invertible, then $(a * b)^{-1} = b^{-1} * a^{-1}$. ***inverse of a product***

Let $(S, *)$ be an associative binary structure with identity e.
Let a be an invertible element of S.
Then $a \in S$ and the inverse of a is unique.
The inverse of a is denoted a^{-1}.
Therefore, $a^{-1} \in S$ and $a * a^{-1} = a^{-1} * a = e$.

Definition 12. left and right cancellation laws
Let $(S, *)$ be a binary structure.
The **left cancellation law** holds iff $c * a = c * b$ implies $a = b$ for all $a, b, c \in S$.
The **right cancellation law** holds iff $a * c = b * c$ implies $a = b$ for all $a, b, c \in S$.

Proposition 13. *Let $(S, *)$ be an associative binary structure with a left identity such that each element has a left inverse.*
Then the left cancellation law holds.

Let $(S, *)$ be an associative binary structure with a left identity such that each element has a left inverse.

Then the left cancellation law holds, so $c * a = c * b$ implies $a = b$ for all $a, b, c \in S$.

Proposition 14. *Let $(S, *)$ be an associative binary structure with a right identity such that each element has a right inverse.*

Then the right cancellation law holds.

Let $(S, *)$ be an associative binary structure with a right identity such that each element has a right inverse.

Then the right cancellation law holds, so $a * c = b * c$ implies $a = b$ for all $a, b, c \in S$.

Definition 15. idempotent element

Let $(S, *)$ be a binary structure.

An element $a \in S$ is an **idempotent** with respect to $*$ iff $a * a = a$.

Definition 16. zero element

Let $(S, *)$ be a binary structure.

An element $z \in S$ is a **zero** with respect to $*$ iff $(\forall x \in S)(z * x = x * z = z)$.

Proposition 17. *If a binary structure has a zero element, then the zero element is unique.*

Let $(S, *)$ be a binary structure with a zero element $z \in S$.

Then z is unique, so there is exactly one element of S that is a zero.

Groups

A group is an algebraic structure upon which a single binary operation is defined.

Groups describe symmetries of objects.

A symmetry is an undetectable motion.

An object is symmetric if it has symmetries.

Definition 18. Group

Let G be a set.

Define binary operation $* : G \times G \to G$ by $a * b \in G$ for all $a, b \in G$.

A **group** $(G, *)$ is a set G with a binary operation $*$ defined on G such that the following axioms hold:

G1. $*$ is associative.

$(a * b) * c = a * (b * c)$ for all $a, b, c \in G$.

G2. There is an identity element for $*$.

$(\exists e \in G)(\forall a \in G)(e * a = a * e = a)$.

G3. Each element has an inverse for $*$.

$(\forall a \in G)(\exists b \in G)(a * b = b * a = e)$.

Let $(G, *)$ be a group.
Since $*$ is a binary operation on G, then G is closed under $*$.
Since $(G, *)$ is a group and G is closed under $*$, then G satisfies the following axioms:
G1 **Closure** $a * b \in G$ for all $a, b \in G$.
G2. **Associative** $(a * b) * c = a * (b * c)$ for all $a, b, c \in G$.
G3. **Identity** $(\exists e \in G)(\forall a \in G)(e * a = a * e = a)$.
G4. **Inverses** $(\forall a \in G)(\exists b \in G)(a * b = b * a = e)$.

Since there exists an identity element in a group, then G contains at least one element.
Therefore, any group contains at least one element.

By axiom $G4$, every element of a group has an inverse, so every element of a group is invertible.

Theorem 19. ***Uniqueness of group identity***
The identity element of a group is unique.

Let $(G, *)$ be a group with identity $e \in G$.
Then e is unique, so there is exactly one element of G that is identity.

Let $(G, \cdot)$ be a multiplicative group with identity $e \in G$.
Then e is unique and $ea = ae = a$ for all $a \in G$.

Let $(G, +)$ be an additive group with identity $0 \in G$.
Then 0 is unique and $0 + a = a + 0 = a$ for all $a \in G$.

Theorem 20. ***Uniqueness of group inverses***
The inverse of each element in a group is unique.

Let $(G, *)$ be a group with identity $e \in G$.
Let $a \in G$.
The inverse of a is unique and is denoted a^{-1}.
Hence, $a * a^{-1} = a^{-1} * a = e$.
Therefore, $a * a^{-1} = a^{-1} * a = e$ for all $a \in G$.

Let $(G, \cdot)$ be a multiplicative group with identity $e \in G$.
The inverse of element $a \in G$ is $a^{-1} \in G$ and a^{-1} is unique and $aa^{-1} = a^{-1}a = e$ for all $a \in G$.

Let $(G, +)$ be an additive group with identity $0 \in G$.
The inverse of element $a \in G$ is $-a \in G$ and $-a$ is unique and $a + (-a) = (-a) + a = 0$ for all $a \in G$.

Proposition 21. *The identity element in a group is its own inverse.*

Let $(G, *)$ be a group with identity $e \in G$.
Since the identity element is its own inverse, then $e^{-1} = e$.

Theorem 22. ***Group inverse properties***
Let $(G, *)$ be a group. Then
1) $(a^{-1})^{-1} = a$ for all $a \in G$. ***inverse of an inverse***
2) $(a * b)^{-1} = b^{-1} * a^{-1}$ for all $a, b \in G$. ***inverse of a product***

Let $(G, \cdot)$ be a multiplicative group.
Then $(a^{-1})^{-1} = a$ for all $a \in G$ and $(ab)^{-1} = b^{-1}a^{-1}$ for all $a, b \in G$.

Let $(G, +)$ be an additive group.
Then $-(-a) = a$ for all $a \in G$ and $-(a + b) = (-b) + (-a)$ for all $a, b \in G$.

Proposition 23. ***inverse of a finite product***
Let $g_1, g_2, ..., g_n$ be elements of a group $(G, *)$.
Then $(g_1g_2...g_n)^{-1} = g_n^{-1}g_{n-1}^{-1}...g_2^{-1}g_1^{-1}$ for all $n \in \mathbb{Z}^+$.

Let $(G, \cdot)$ be a multiplicative group.
Let $g_1, g_2, ..., g_n$ be elements of G.
Then $(g_1 \cdot g_2 \cdot ... \cdot g_n)^{-1} = g_n^{-1} \cdot g_{n-1}^{-1} \cdot ... \cdot g_2^{-1} \cdot g_1^{-1}$.

Let $(G, +)$ be an additive group.
Let $g_1, g_2, ..., g_n$ be elements of G.
Then $-(g_1 + g_2 + ... + g_n) = (-g_n) + (-g_{n-1}) + ... + (-g_2) + (-g_1)$.

Theorem 24. ***Group Cancellation Laws***
Let $(G, *)$ be a group.
For all $a, b, c \in G$
*1. if $c * a = c * b$ then $a = b$. (**left cancellation law**)*
*2. if $a * c = b * c$ then $a = b$. (**right cancellation law**)*

Corollary 25. ***Unique solutions to linear equations***
Let $(G, *)$ be a group.
Let $a, b \in G$.
1. The linear equation $a * x = b$ has a unique solution in G.
2. The linear equation $x * a = b$ has a unique solution in G.

Proposition 26. *A group has exactly one idempotent element, the identity element.*

Therefore, if $(G, *)$ is a group with identity $e \in G$, then $e * e = e$.

Proposition 27. ***left sided definition of a group***
*A **group** $(G, *)$ is a set G with a binary operation $*$ defined on G such that the following axioms hold:*
G1. $*$ is associative.
$(a * b) * c = a * (b * c)$ for all $a, b, c \in G$.
G2. There is a left identity element for $*$.

$(\exists e \in G)(\forall a \in G)(e * a = a)$.
G3. Each element has a left inverse for $*$.
$(\forall a \in G)(\exists b \in G)(b * a = e)$.

Let $(G, *)$ be an associative binary structure with a left identity such that each element has a left inverse.
Then $(G, *)$ is a group.

Proposition 28. ***right sided definition of a group***
*A **group** $(G, *)$ is a set G with a binary operation $*$ defined on G such that the following axioms hold:*
G1. $*$ is associative.
$(a * b) * c = a * (b * c)$ for all $a, b, c \in G$.
G2. There is a right identity element for $*$.
$(\exists e \in G)(\forall a \in G)(a * e = a)$.
G3. Each element has a right inverse for $*$.
$(\forall a \in G)(\exists b \in G)(a * b = e)$.

Let $(G, *)$ be an associative binary structure with a right identity such that each element has a right inverse.
Then $(G, *)$ is a group.

Definition 29. abelian group
A group $(G, *)$ is **abelian** iff $*$ is commutative.

multiplicative group notation

Let $(G, \cdot)$ be a **multiplicative group**.
G1. Multiplication $\cdot$ is associative.
Therefore, $(ab)c = a(bc)$ for all $a, b, c \in G$.
G2. Let $e \in G$ be the multiplicative identity element.
Then $(\forall a \in G)(ea = ae = a)$.
G3. Each element a has a multiplicative inverse a^{-1}.
Therefore, $(\forall a \in G)(\exists a^{-1} \in G)(aa^{-1} = a^{-1}a = e)$.

Definition 30. powers of an element in a multiplicative group
Let $(G, \cdot)$ be a multiplicative group with multiplicative identity $e \in G$.
Let $a \in G, n \in \mathbb{Z}$.
Define $a^0 = e$.
Define $a^n = a^{n-1} \cdot a$ if $n > 0$.
Define $a^{-n} = (a^{-1})^n$ if $n > 0$.

Let $(G, \cdot)$ be a multiplicative group with multiplicative identity $e \in G$.
Let $a \in G$.

Observe that
$a^1 = a^{1-1} \cdot a = a^0 \cdot a = e \cdot a = a.$
Hence, $a^1 = a$.
Therefore, $a^1 = a$ for all $a \in G$.
This means a raised to the first power is a for all $a \in G$.
In particular, $e^1 = e$ for multiplicative identity $e \in G$.

Observe that
$a^{-1} = (a^{-1})^1 = a^{-1}$.
Therefore, $a^{-1} = a^{-1}$.
This means a raised to the negative 1 power is the multiplicative inverse of a for all $a \in G$.

Observe that a^n is the product of a with itself n times when $n > 0$.
Observe that a^{-n} is the product of a^{-1} with itself n times when $n > 0$.

Lemma 31. *Let $(G, \cdot)$ be a multiplicative group.*
Let $a \in G$.
Then $a^n \cdot a = a \cdot a^n$ for all $n \in \mathbb{Z}^+$.

Theorem 32. ***Laws of Exponents for a multiplicative group***
Let $(G, \cdot)$ be a multiplicative group.
1. If $a \in G$, then $a^{-n} = (a^{-1})^n = (a^n)^{-1}$ for all $n \in \mathbb{Z}^+$.
2. If $a \in G$, then $a^n \in G$ for all $n \in \mathbb{Z}$.
3. If $a \in G$, then $a^m \cdot a^n = a^{m+n}$ for all $m, n \in \mathbb{Z}$.
4. If $a \in G$, then $(a^m)^n = a^{mn}$ for all $m, n \in \mathbb{Z}$.
5. If $a, b \in G$ and G is abelian, then $(ab)^n = a^n \cdot b^n$ for all $n \in \mathbb{Z}$.

Proposition 33. *Let $(G, \cdot)$ be a multiplicative group with multiplicative identity $e \in G$.*
$(\forall n \in \mathbb{Z})(e^n = e)$.

Therefore, if $(G, \cdot)$ is a multiplicative group with identity $e \in G$, then $e^{-1} = e$.

additive group notation

Let $(G, +)$ be an **additive group**.
G1. Addition $+$ is associative.
Therefore, $(a + b) + c = a + (b + c)$ for all $a, b, c \in G$.
G2. Let $0 \in G$ be the additive identity element.
Then $(\forall a \in G)(0 + a = a + 0 = a)$.
G3. Each element a has an additive inverse $-a$.
Therefore, $(\forall a \in G)(\exists -a \in G)(a + (-a) = -a + a = 0)$.

Definition 34. multiples of an element in an additive group
Let $(G, +)$ be an additive group with additive identity $0 \in G$.
Let $a \in G, n \in \mathbb{Z}$.
Define $0a = 0$.
Define $na = (n-1)a + a$ if $n > 0$.
Define $(-n)a = n(-a)$ if $n > 0$.

Let $(G, +)$ be an additive group with additive identity $0 \in G$.
Let $a \in G$.

Observe that
$1a = (1-1)a + a = 0a + a = 0 + a = a$.
Hence, $1a = a$.
Therefore, $1a = a$ for all $a \in G$.
This means positive 1 times a is a for all $a \in G$.
In particular, $1 \cdot 0 = 0$ for additive identity $0 \in G$.

Observe that
$(-1)a = 1(-a) = -a$.
Therefore, $(-1)a = -a$.
This means negative 1 times a is the additive inverse of a for all $a \in G$.

Observe that na is the sum of a with itself n times when $n > 0$.
Observe that $(-n)a$ is the sum of $-a$ with itself n times when $n > 0$.

Lemma 35. *Let $(G, +)$ be an additive group.*
Let $a \in G$.
Then $na + a = a + na$ for all $n \in \mathbb{Z}^+$.

Theorem 36. ***Laws of Exponents for an additive group***
Let $(G, +)$ be an additive group.
1. *If $a \in G$, then $(-n)a = n(-a) = -(na)$ for all $n \in \mathbb{Z}^+$.*
2. *If $a \in G$, then $na \in G$ for all $n \in \mathbb{Z}$.*
3. *If $a \in G$, then $ma + na = (m+n)a$.*
4. *If $a \in G$, then $n(ma) = (mn)a$ for all $m, n \in \mathbb{Z}$.*
5. *If $a, b \in G$ and G is abelian, then $n(a+b) = na + nb$ for all $n \in \mathbb{Z}$.*

Proposition 37. *Let $(G, +)$ be an additive group with additive identity $0 \in G$.*
$(\forall n \in \mathbb{Z})(n0 = 0)$.

Therefore, if $(G, +)$ is an additive group with identity $0 \in G$, then $-0 = 0$.

Definition 38. Order of a Group
Let $(G, *)$ be a group.
The **order of** G, denoted $|G|$, is the cardinality of the set G.
If G is finite, then $|G|$ is the number of elements in G.
If G is not finite, then the group is of **infinite order**.
A **finite group** is a group whose order is finite.
An **infinite group** is a group whose order is infinite.

Finite Groups of small order

Let $(G, *)$ be a group.

Each $g \in G$ appears exactly once in each row and exactly once in each column of the group's Cayley table.

The order of a finite group with n elements is n.

Group of order 1 (**trivial group**)

*	e
e	e

A group of order 1 is abelian.

The trivial group is cyclic.

$G_1 = \langle e \rangle$

subgroup of G_1 is $\{e\}$

Group of order 2

*	e	a
e	e	a
a	a	e

A group of order 2 is abelian and cyclic and each element is its own inverse.

$G_2 = \langle a \rangle \cong (\mathbb{Z}_2, +)$

subgroups of G_2 are $G_2, \{e\}$

Group of order 3

*	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

A group of order 3 is abelian and cyclic and a and b are inverses of each other.

$G_3 = \langle a \rangle = \langle b \rangle \cong (\mathbb{Z}_3, +)$

subgroups of G_3 are $G_3, \{e\}$

Group of Order 4

A group of order 4 is abelian.

Klein 4-group $(V_4, *)$

*	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Klein 4-group has property $\forall x \in V . x * x = e$.

The product of any two distinct elements other than e is the third such element.

Klein 4-group has exactly 3 nontrivial proper subgroups: $\{e, a\}, \{e, b\}, \{e, c\}$

Klein 4-group is not cyclic.

Klein 4-group is isomorphic to the group of symmetries of a rectangle.

$(\mathbb{Z}_4, +)$

*	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

$\{0, 2\}$ is the only nontrivial proper subgroup of $(\mathbb{Z}_4, +)$.
$(\mathbb{Z}_4, +)$ is cyclic.
$\mathbb{Z}_4 = \langle 1 \rangle = \langle 3 \rangle$.

Subgroups

Definition 39. Subgroup
Let $(G, *)$ be a group.
A **subgroup of** G is a subset of G that is a group under the binary operation of G.

Therefore H is a subgroup of $(G, *)$ iff
1. $H \subset G$
2. $(H, *)$ is a group under the operation induced by G.

$H < G$ denotes that H is a subgroup of G.

Let $(G, *)$ be an arbitrary group with identity $e \in G$.
Since $G \subset G$ and $(G, *)$ is a group, then $G < G$.
Therefore every group is a subgroup of itself.

Since $e \in G$, then $\{e\} \subset G$, so $\{e\} < G$.
Therefore the **trivial group** is a subgroup of every group.

Let H be a subgroup of a group $(G, *)$ with identity $e \in G$.
Since $\{e\}$ is a subgroup of every group and H is a group, then $\{e\}$ is a subgroup of H.
Therefore, $\{e\} \subset H$, so $e \in H$.

A **proper subgroup** is a subgroup of G other than G.
Let $H < G$.
Then H is a proper subgroup of G iff $H \neq G$.

Theorem 40. *Two-Step Subgroup Test*
Let H be a nonempty subset of a group $(G, *)$.
Then $H < G$ iff
1. Closed under $*$: $(\forall a, b \in H)(a * b \in H)$.
2. Closed under inverses: $(\forall a \in H)(a^{-1} \in H)$.

Theorem 41. ***One-Step Subgroup Test***

Let H be a nonempty subset of a group $(G, *)$.
Then $H < G$ iff
1. $(\forall a, b \in H)(a * b^{-1} \in H)$.

Theorem 42. ***Subgroup relation is transitive.***

Let $(G, *)$ be a group.
If $H < K$ and $K < G$, then $H < G$.

Since every group is a subgroup of itself, then $G < G$, so the subgroup relation is reflexive.

Suppose $G < H$ and $H < G$.
Then $G \subset H$ and $H \subset G$, so $G = H$.
Therefore, the subgroup relation is anti-symmetric.

Since $<$ is reflexive, anti-symmetric, and transitive, then the subgroup relation is a partial order.
Therefore, we can create subgroup lattice diagrams of a given group.

Theorem 43. ***The intersection of subgroups is a subgroup.***

The intersection of a family of subgroups is a subgroup.

Let $(G, *)$ be a group.
Let $\{H_i : i \in I\}$ be a collection of subgroups of G for some index set I.
Each H_i is a subgroup of G.
Let $H = \cap_{i \in I} H_i$.
Then $H < G$.

In particular, the intersection of any two subgroups is a subgroup.
Therefore, if $H < G$ and $K < G$, then $H \cap K < G$.

The union of subgroups is not necessarily a subgroup.

Cyclic Groups

Order of a group element

Definition 44. Order of an element

Let $(G, *)$ be a group with identity $e \in G$.
An element $a \in G$ has **finite order** iff $(\exists n \in \mathbb{Z}^+)(a^n = e)$.
The **order of** a, denoted $|a|$, is the smallest positive integer k such that $a^k = e$.
An element $a \in G$ has **infinite order** iff $\neg(\exists n \in \mathbb{Z}^+)(a^n = e)$.

Let G be a group with identity $e \in G$.
Let $a \in G$.
Either there exists a positive integer n such that $a^n = e$ or there does not exist a positive integer n such that $a^n = e$.
Hence, either a has finite order or a has infinite order.
Therefore, every element of a group has either finite order or infinite order.
Since $e^1 = e$, then the order of the identity element of a group is 1.

Let G be a group with identity $e \in G$.
Suppose $a \neq e$ has finite order n.
Then n is the least positive integer such that $a^n = e$.
If $n = 1$, then $e = a^n = a^1 = a$, so $a = e$.
But, $a \neq e$, so $n \neq 1$.
Hence, $n > 1$.
Therefore, if $a \neq e$ has finite order n, then $n > 1$.

If $(G, +)$ is an additive group with identity $0 \in G$, then
An element $a \in G$ has **finite order** iff $(\exists n \in \mathbb{Z}^+)(na = 0)$.
The **order of** a, denoted $|a|$, is the smallest positive integer k such that $ka = 0$.
An element $a \in G$ has **infinite order** iff $\neg(\exists n \in \mathbb{Z}^+)(na = 0)$.

Theorem 45. *Let $(G, *)$ be a group.*
Let $a \in G$.
If $a^s = a^t$ and $s \neq t$ for some $s, t \in \mathbb{Z}$, then a has finite order.

Suppose a has infinite order.
Then a does not have finite order.
Hence, there does not exist distinct $s, t \in \mathbb{Z}$ such that $a^s = a^t$.
Therefore, $a^s \neq a^t$ for every distinct $s, t \in \mathbb{Z}$.
Consequently, all elements a^k are distinct, so every power of a is distinct.
Therefore, if a has infinite order, then every power of a is distinct.

Let $(G, +)$ be an additive group.
Let $a \in G$.
If $sa = ta$ and $s \neq t$ for some $s, t \in \mathbb{Z}$, then a has finite order.

Therefore, if a has infinite order, then every multiple of a is distinct.

Theorem 46. *Let $(G, *)$ be a group with identity $e \in G$.*
If $a \in G$ has finite order n, then $a^k = e$ iff $n|k$ for all $k \in \mathbb{Z}$.

Let $(G, +)$ be an additive group with identity $0 \in G$.
If $a \in G$ has finite order n, then $ka = 0$ iff $n|k$ for all $k \in \mathbb{Z}$.

Corollary 47. *Let $(G, *)$ be a group with identity $e \in G$.*
If $a \in G$ has finite order n, then $a^s = a^t$ iff $s \equiv t \pmod{n}$ for all $s, t \in \mathbb{Z}$.

Let $(G, +)$ be an additive group with identity $0 \in G$.
If $a \in G$ has finite order n, then $sa = ta$ iff $s \equiv t \pmod{n}$ for all $s, t \in \mathbb{Z}$.

Theorem 48. *Let $(G, *)$ be a group with identity $e \in G$.*
If $a \in G$ has finite order n, then the order of a^s is $\frac{n}{\gcd(s,n)}$ for all $s \in \mathbb{Z}$.

Let $(G, +)$ be an additive group with identity $0 \in G$.
If $a \in G$ has finite order n, then the order of sa is $\frac{n}{\gcd(s,n)}$ for all $s \in \mathbb{Z}$.

Corollary 49. *Let $(G, *)$ be a group.*
Let $a \in G$ have order n.
Let $s \in \mathbb{Z}$.
If s and n are relatively prime, then a^s has order n.

Corollary 50. *Let $(G, *)$ be a group.*
Let $a \in G$ have order n.
Let $s \in \mathbb{Z}$.
If s divides n, then a^s has order $\frac{n}{s}$.

Proposition 51. ***The order of a is the same as the order of a^{-1}.***
Let $(G, *)$ be a group.
Let $a \in G$.
Then $|a| = |a^{-1}|$.

Therefore, the order of an element is the order of its inverse.

Proposition 52. ***The order of ab is the same as the order of ba.***
Let $(G, *)$ be a group.
Let $a, b \in G$.
Then $|ab| = |ba|$.

Therefore, if ab has finite order n, then ba has finite order n.

Proposition 53. ***Every element of a finite group has finite order.***
Let $(G, *)$ be a finite group with identity $e \in G$.
Then $(\forall a \in G)(\exists k \in \mathbb{Z}^+)(a^k = e)$.

Let $(G, *)$ be a finite group with identity $e \in G$.
Let $a \in G$.
Then there exists $k \in \mathbb{Z}^+$ such that $a^k = e$, so a has finite order.
Hence, every element of G has finite order.
Therefore, every element of a finite group has finite order.

Theorem 54. ***Finite Subgroup Test***
Let H be a nonempty finite subset of a group $(G, *)$.
Then $H < G$ iff H is closed under $*$ of G.

Cyclic subgroups

Definition 55. Cyclic subgroup of G
Let $(G, *)$ be a group.
Let $g \in G$.
Let $\langle g \rangle = \{g^n : n \in \mathbb{Z}\}$.
Then $\langle g \rangle$ is called the **cyclic subgroup of G generated by g**.

Every element of a group G generates a cyclic subgroup of G.
If $(G, +)$ is an additive group, then $\langle g \rangle = \{ng : n \in \mathbb{Z}\}$.

Theorem 56. ***The cyclic subgroup of a group G generated by $g \in G$ is the smallest subgroup of G that contains g.***
Let $(G, *)$ be a group.
Let $g \in G$.
Then $\langle g \rangle = \{g^n : n \in \mathbb{Z}\}$ is a subgroup of G.
Moreover, $\langle g \rangle$ is the smallest subgroup of G that contains g.

Let $(G, *)$ be a group with identity $e \in G$.
The cyclic subgroup generated by $g \in G$ is $\langle g \rangle = \{g^n : n \in \mathbb{Z}\}$.
The identity of $\langle g \rangle$ is $g^0 = e$.
The inverse of g^k is g^{-k} for $k \in \mathbb{Z}$, since $g^k * g^{-k} = g^{k-k} = g^0$.

$\langle g \rangle$ is the smallest subgroup of G that contains g.
Therefore any subgroup of G that contains g must contain $\langle g \rangle$.
Hence, $\langle g \rangle$ must be a subgroup of any group that contains g.
Therefore, for every $K < G$ such that $g \in K$, then $\langle g \rangle < K$.
Therefore, if $K < G$ and $g \in K$, then $\langle g \rangle < K$.

Definition 57. cyclic group
A group $(G, *)$ is **cyclic** iff $(\exists g \in G)(G = \langle g \rangle)$.
The element g is a **generator of** G.

Theorem 58. *Every cyclic group is abelian.*

Let $(G, *)$ be a group.
If G is cyclic, then G is abelian.

Example 59. abelian group is not necessarily cyclic
1. The Klein-4 group $(V_4, +)$ is abelian, but it is not cyclic.
2. The circle group $(\mathbb{T}, \cdot)$ is abelian, but it is not cyclic.

Theorem 60. *Every subgroup of a cyclic group is cyclic.*

Let G be a cyclic group.
If $H < G$, then H is cyclic.

Corollary 61. *The only subgroups of $(\mathbb{Z}, +)$ are $(n\mathbb{Z}, +)$ for all $n \in \mathbb{Z}$.*

Let $n \in \mathbb{Z}$.
Then $(n\mathbb{Z}, +)$ is a subgroup of $(\mathbb{Z}, +)$.
Since $\mathbb{Z}$ is cyclic and $n\mathbb{Z} < \mathbb{Z}$, then $n\mathbb{Z}$ is cyclic.

Example 62. 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 $\gcd(a, b)$.

Let $a, b \in \mathbb{Z}^+$ be fixed.
Let $G = \{ma + nb : m, n \in \mathbb{Z}\}$.
Then $(G, +)$ is a cyclic group with generator $\gcd(a, b)$ and $G = \{kd : k \in \mathbb{Z}\}$.
additive identity is $0 = 0a + 0b$.
additive inverse of $ma + nb$ is $-ma - nb$.

Theorem 63. ***Characterization of cyclic subgroup***
Let $(G, *)$ be a group.
Let $a \in G$.
The order of a is the order of the cyclic subgroup of G generated by a.
1. If a has finite order n, then $\langle a \rangle$ is finite and $\langle a \rangle = \{e, a^1, a^2, ..., a^{n-1}\}$.
2. If a has infinite order, then $\langle a \rangle$ is infinite and $\langle a \rangle = \{..., a^{-2}, a^{-1}, e, a^1, a^2, ...\}$ and each power of a is distinct.

Let $(G, +)$ be an additive group.
Let $a \in G$.
The order of a is the order of the cyclic subgroup of G generated by a.
1. If a has finite order n, then $\langle a \rangle$ is finite and $\langle a \rangle = \{0, 1a, 2a, ..., (n-1)a\}$.
2. If a has infinite order, then $\langle a \rangle$ is infinite and $\langle a \rangle = \{..., -2a, -1a, 0, 1a, 2a, ...\}$.

Proposition 64. ***Generators of a finite cyclic group***
Let $n \in \mathbb{Z}^+$.
Let G be a cyclic group of order n.
If $g \in G$ is a generator of G, then the generators of G are elements g^k such that $\gcd(k, n) = 1$.

Corollary 65. *The generators of $(\mathbb{Z}_n, +)$ are congruence classes $[k]$ such that $k \in \mathbb{Z}^+$ and $1 \leq k \leq n$ and $\gcd(k, n) = 1$.*

Therefore there are $\phi(n)$ generators of $(\mathbb{Z}_n, +)$ where ϕ is Euler's totient function.
The generators of $(\mathbb{Z}_n, +)$ are positive integers that are relatively prime to the modulus n.

Definition 66. Subgroup of G generated by $a_1, ..., a_n$
Let $(G, *)$ be a group with identity e and $a_1, a_2, ..., a_n \in G$.
Let $\langle a_1, a_2, ..., a_n \rangle$ be the set of all finite products of integer powers of $a_1, ..., a_n$.
Let $N_0 = \{0, 1, 2, 3, ...\}$.

Then $\langle a_1, a_2, ..., a_n \rangle = \{b_1^{\epsilon_1} \cdot b_2^{\epsilon_2} \cdots b_k^{\epsilon_k} : k \in N_0, b_i \in \{a_1, ..., a_n\}, \epsilon_i \in \mathbb{Z}\}$

Whenever $k = 0$ then $b_1^{\epsilon_1} \cdot b_2^{\epsilon_2} \cdots b_k^{\epsilon_k}$ is the empty product and is defined to be e.

Therefore, $b_1^{\epsilon_1} \cdot b_2^{\epsilon_2} \cdots b_k^{\epsilon_k} = e$ iff $k = 0$.

$\langle a_1, a_2, ..., a_n \rangle$ is called the **subgroup of G generated by the set** $\{a_1, a_2, ..., a_n\}$.

Theorem 67. *Let $(G, *)$ be a group.*

Let $a_1, a_2, ..., a_n \in G$.

Then $\langle a_1, a_2, ..., a_n \rangle$ is a subgroup of G.

Moreover, $\langle a_1, a_2, ..., a_n \rangle$ is the smallest subgroup of G that contains $\{a_1, a_2, ..., a_n\}$.

Therefore any subgroup of G that contains $\{a_1, a_2, ..., a_n\}$ must contain $\langle a_1, a_2, ..., a_n \rangle$.

Theorem 68. *Let $(G, *)$ be a group.*

Let $S \subset G$.

The smallest subgroup that contains S is the intersection of all subgroups that contain S.

Definition 69. Subgroup Generated by a subset of a group

Let $(G, *)$ be a group.

Let $X \subset G$.

Let H_i be a subgroup of G such that $X \subset H_i$.

Let I be some index set.

Let $\{H_i : i \in I\}$ be the collection of all subgroups of G that contain X.

Let $\langle X \rangle = \cap_{i \in I} H_i$.

Then $\langle X \rangle$ is called the **subgroup of G generated by** X.

$\langle X \rangle$ is the smallest subgroup of G containing X.

We say that X **generates** $\langle X \rangle$.

If $\langle X \rangle = G$, then X generates G.

If X is finite, we say that G is **finitely generated**.

Let $\langle X \rangle$ be the subgroup of G generated by $X \subset G$.

$\langle X \rangle$ is the smallest subgroup of G containing X means:

For every $K < G$ such that $X \subset K$, $\langle X \rangle < K$.

If X consists of a single element $a \in G$, then $\langle X \rangle = \langle a \rangle$, the cyclic subgroup of G generated by a.

If X is a finite set, then there exist $a_1, a_2, ..., a_n \in G$ such that $X = \{a_1, a_2, ..., a_n\}$ and $\langle X \rangle = \langle a_1, a_2, ..., a_n \rangle$.

Additive Number Groups

Integers under addition $(\mathbb{Z}, +)$

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

Additive identity is 0.

Additive inverse of a is $-a$.

$(\mathbb{Z}, +)$ is cyclic.
$\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$ with generators 1 and -1.
Since $n\mathbb{Z} < \mathbb{Z}$ and $\mathbb{Z}$ is abelian, then $n\mathbb{Z} \lhd \mathbb{Z}$, so $n\mathbb{Z}$ is normal in $\mathbb{Z}$.

Multiples of integer n under addition $(n\mathbb{Z}, +)$

Let $n \in \mathbb{Z}$.
$(n\mathbb{Z}, +)$ is an abelian group.
Additive identity is 0.
Additive inverse of nk is $-nk$.
$(n\mathbb{Z}, +)$ is cyclic.
$n\mathbb{Z} = \{nk : k \in \mathbb{Z}\} = \langle n \rangle = \langle -n \rangle$ with generators n and $-n$.

Integers modulo n under addition $(\mathbb{Z}_n, +)$ of order n

Let $n \in \mathbb{Z}^+$.
$(\mathbb{Z}_n, +)$ is an abelian group and $|\mathbb{Z}_n| = n$.
Additive identity is $[0]$.
Additive inverse of $[a]$ is $-[a] = [n - a]$.
$(\mathbb{Z}_n, +)$ is cyclic.
$\mathbb{Z}_n = \{[0], [1], ..., [n-1]\} = \langle [1] \rangle = \{a[1] : a \in \mathbb{Z}\} = \{[a] : a \in \mathbb{Z}\}$ with generators $[k]$ such that $1 \leq k \leq n$ and $\gcd(k, n) = 1$.

Let $p \in \mathbb{Z}^+$ be prime.
Then $(\mathbb{Z}_p, +)$ has no proper nontrivial subgroups.

Rational numbers under addition $(\mathbb{Q}, +)$

$(\mathbb{Q}, +)$ is an abelian group.
Additive identity is $0 = \frac{0}{1}$.
Additive inverse of $\frac{a}{b}$ is $-\frac{a}{b} = \frac{-a}{b}$.
$(\mathbb{Q}, +)$ is not cyclic.

Real numbers under addition $(\mathbb{R}, +)$

$(\mathbb{R}, +)$ is an abelian group.
Additive identity is 0.
Additive inverse of a is $-a$.
$(\mathbb{R}, +)$ is not cyclic.

Complex numbers under addition $(\mathbb{C}, +)$

$(\mathbb{C}, +)$ is an abelian group.
Additive identity is $0 = 0 + 0i$.
Let $x, y \in \mathbb{R}$.
Additive inverse of $z = x + yi$ is $-z = -x - yi$.

Example 70. 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.

Multiplicative Number Groups

Nonzero rational numbers under multiplication $(\mathbb{Q}^*, \cdot)$

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

Multiplicative identity is $1 = \frac{1}{1}$.

Multiplicative inverse of $\frac{a}{b}$ is $\frac{b}{a}$.

Nonzero real numbers under multiplication $(\mathbb{R}^*, \cdot)$

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

Multiplicative identity is 1.

Multiplicative inverse of a is $\frac{1}{a}$.

Nonzero complex numbers under multiplication $(\mathbb{C}^*, \cdot)$

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

Multiplicative identity is $1 = 1 + 0i$.

Multiplicative inverse of $z \in \mathbb{C}^*$ is $\frac{1}{z} = \frac{\bar{z}}{|z|^2}$, where $\bar{z}$ is the complex conjugate of z and $|z|$ is the modulus of z.

Positive rational numbers under multiplication $(\mathbb{Q}^+, \cdot)$

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

Multiplicative identity is $1 = \frac{1}{1}$.

Multiplicative inverse of $\frac{a}{b}$ is $\frac{b}{a}$.

Positive real numbers under multiplication $(\mathbb{R}^+, \cdot)$

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

Multiplicative identity is 1.

Multiplicative inverse of a is $\frac{1}{a}$.

Subgroup Relationships of number groups

$(n\mathbb{Z}, +) < (\mathbb{Z}, +) < (\mathbb{Q}, +) < (\mathbb{R}, +) < (\mathbb{C}, +)$

$(\mathbb{Z}[i], +) < (\mathbb{C}, +)$

$(\mathbb{Q}^*, \cdot) < (\mathbb{R}^*, \cdot) < (\mathbb{C}^*, \cdot)$

$(\mathbb{Q}^+, \cdot) < (\mathbb{R}^+, \cdot) < (\mathbb{R}^*, \cdot)$

$(U_n, \cdot) < (\mathbb{T}, \cdot) < (\mathbb{C}^*, \cdot)$

Group of Units of Integers modulo n

Definition 71. Group of Units of $\mathbb{Z}_n$ of order $\phi(n)$

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

Let $\mathbb{Z}_n^*$ be the set of all units of $\mathbb{Z}_n$.

Then $\mathbb{Z}_n^*$ is the set of all congruence classes of $\mathbb{Z}_n$ which have multiplicative inverses in $\mathbb{Z}_n$.

$$\begin{aligned} \mathbb{Z}_n^* &= \{[a] \in \mathbb{Z}_n : [a] \text{ is a unit}\} \\ &= \{[a] \in \mathbb{Z}_n : [a] \text{ has a multiplicative inverse}\} \\ &= \{[a] \in \mathbb{Z}_n : \gcd(a, n) = 1\} \\ &= \{[a] : a \in \mathbb{Z}, 1 \leq a < n \wedge \gcd(a, n) = 1\} \end{aligned}$$

Lemma 72. *Let $a, b \in \mathbb{Z}$ and $n \in \mathbb{Z}^+$.*

If $\gcd(a, n) = \gcd(b, n) = 1$, then $\gcd(ab, n) = 1$.

Proposition 73. ***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.

$(\mathbb{Z}_n^*, \cdot)$ is an abelian group under multiplication modulo n.

Multiplicative identity is $[1]$.

Multiplicative inverse of $[x]$ is $[y]$ such that $[x][y] = [y][x] = [1]$.

Multiplicative inverse of $[1]$ is $[1]$ since $[1][1] = [1 \cdot 1] = [1]$.

Multiplicative inverse of $[n-1]$ is $[n-1]$ since $[n-1][n-1] = [(n-1)(n-1)] = [n^2-2n+1] = [n(n-2)+1] = [n(n-2)]+[1] = [n][n-2]+[1] = [0][n-2]+[1] = [0] + [1] = [1]$.

If $n > 1$, then $[0]$ has no multiplicative inverse, so $[0] \notin \mathbb{Z}_n^*$.

$[1] \in \mathbb{Z}_n^*$ and $[n-1] \in \mathbb{Z}_n^*$ for all $n \in \mathbb{Z}^+$.

Proposition 74. *Let $n \in \mathbb{Z}^+$.*

Let $\mathbb{Z}_n^*$ be the group of units of $\mathbb{Z}_n$.

Then $|\mathbb{Z}_n^*| = \phi(n)$.

Complex Number Groups

Example 75. Circle Group $(\mathbb{T}, \cdot)$

Let $\mathbb{T}$ be the unit circle in the complex plane.

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

$(\mathbb{T}, \cdot)$ is an abelian group.

Multiplicative identity is $1 = 1 + 0i$.

Multiplicative inverse of $z \in \mathbb{T}$ is $\frac{1}{z} = \bar{z}$, where $\bar{z}$ is the complex conjugate of z.

Hence, if $z \in \mathbb{T}$ and $z = cis(\theta)$, then $z^{-1} = \frac{1}{z} = cis(-\theta)$ for some $\theta \in \mathbb{R}$.

Therefore, if $z \in \mathbb{T}$ and $z = e^{i\theta}$, then $z^{-1} = \frac{1}{z} = e^{-i\theta}$ for some $\theta \in \mathbb{R}$.

$(\mathbb{T}, \cdot)$ is a subgroup of the group $(\mathbb{C}^*, \cdot)$.

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

Example 76. n^{th} **Roots of Unity of order** n **is** $(U_n, \cdot)$

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

Let $U_n = \{z \in \mathbb{C} : z^n = 1\}$.

Then $(U_n, \cdot)$ is an abelian group and $|U_n| = n$.

Multiplicative identity is $1 = 1 + 0i$.

$(U_n, \cdot)$ is a subgroup of the circle group $(\mathbb{T}, \cdot)$.

$(U_n, \cdot)$ is cyclic with generator $g \in U_n$ and $g = \cos(\frac{2\pi}{n}) + i\sin(\frac{2\pi}{n}) = e^{i\frac{2\pi}{n}}$.

Observe that

$$\begin{aligned}
U_n &= \{z \in \mathbb{C} : z^n = 1\} \\
&= \langle g \rangle \\
&= \langle \cos(\frac{2\pi}{n}) + i\sin(\frac{2\pi}{n}) \rangle \\
&= \langle e^{i\frac{2\pi}{n}} \rangle \\
&= \{(e^{i\frac{2\pi}{n}})^k : k \in \mathbb{Z}\} \\
&= \{e^{i\frac{2k\pi}{n}} : k \in \mathbb{Z}\}.
\end{aligned}$$

Examples of roots of unity.

$U_1 = \{1\}$

$U_2 = \{1, -1\}$

$U_3 = \{1, e^{i2\pi/3}, e^{i4\pi/3}\} = \{1, \frac{-1+i\sqrt{3}}{2}, \frac{-1-i\sqrt{3}}{2}\}$

$U_4 = \{1, i, -1, -i\}$

$U_6 = \{1, e^{i\pi/3}, e^{i2\pi/3}, e^{i\pi}, e^{i4\pi/3}, e^{i5\pi/3}\} = \{1, \frac{1+i\sqrt{3}}{2}, \frac{-1+i\sqrt{3}}{2}, -1, \frac{-1-i\sqrt{3}}{2}, \frac{1-i\sqrt{3}}{2}\}$

Example 77. 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 $\mathbb{C}$.
$|Q_8| = 8$
$(Q_8, \cdot)$ is not cyclic.

·	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

Function Groups

Example 78. Let S be a set.
Let $F = \{f : S \to S | f \text{ is a function}\}$.
Then $(F, +)$ is an abelian group, additive identity is zero function $f(x) = 0$, additive inverse of $f(x)$ is $-f(x) = (-f)(x)$.

Example 79. Let $G = \{f : \mathbb{R} \to \mathbb{R} | f \text{ is a function}\}$.
Then $(G, +)$ is an abelian group, additive identity is zero function $f(x) = 0$,
additive inverse of $f(x)$ is $-f(x) = (-f)(x)$.
Let $C = \{f \in G : f \text{ is a continuous function}\}$.
Then $(C, +) < (G, +)$.
Let $C_{[0,1]} = \{f \in C : f \text{ is a continuous function on unit interval } [0, 1]\}$.
Then $(C_{[0,1]}, +) < (C, +)$.
Let $D = \{f \in G : f \text{ is a differentiable function}\}$.
Then $(D, +) < (C, +)$.

Additive Matrix Groups

Example 80. $M_{m\times n}(\mathbb{R}) = m \times n$ real matrices
Then $(M_{m\times n}(\mathbb{R}), +) =$ abelian group, additive identity=zero matrix, $-A =$ additive inverse of matrix A.

Example 81. $M_{m \times n}(\mathbb{C}) = m \times n$ complex matrices

Then $(M_{m \times n}(\mathbb{C}), +) =$ abelian group, additive identity=zero matrix, $-A =$ additive inverse of matrix A.

Multiplicative Matrix Groups

Definition 82. $M_n(\mathbb{R})$

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

The set of all $n \times n$ matrices over $\mathbb{R}$ is denoted $M_n(\mathbb{R})$.

Therefore $M_n(\mathbb{R})$ is the set of all $n \times n$ matrices with entries in $\mathbb{R}$.

Definition 83. $M_n(\mathbb{C})$

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

The set of all $n \times n$ matrices over $\mathbb{C}$ is denoted $M_n(\mathbb{C})$.

Therefore $M_n(\mathbb{C})$ is the set of all $n \times n$ matrices with entries in $\mathbb{C}$.

Definition 84. general linear group

Let F be a field.

Let $GL_n(F)$ be the set of all $n \times n$ invertible matrices with entries in F.

Then $GL_n(F) = \{A : A \text{ is an invertible square matrix } \}$.

$GL_n(F)$ is called the **general linear group of degree** n **over** F.

Example 85. General linear group is a group under matrix multiplication

Let F be a field.

Then $GL_n(F)$ is a group under matrix multiplication.

Let $GL_n(F)$ be the general linear group over a field F under matrix multiplication.

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

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

The product AB is an invertible square matrix and $(AB)^{-1} = B^{-1}A^{-1}$.

The identity $n \times n$ matrix I is multiplicative identity.

The matrix A^{-1} is the multiplicative inverse of matrix A and $AA^{-1} = I = A^{-1}A$.

In general matrix multiplication is not commutative, so in general $GL_n(F)$ is non-abelian.

Example 86. (special linear group)

$SL_n(\mathbb{R}) = \{A \in GL_n(\mathbb{R}) : \text{det A} = 1\}$

$(SL_n, \cdot) < (GL_n, \cdot)$

Therefore, the special linear group is a subgroup of the general linear group.

Example 87. (orthogonal group)

$O_n = \{A \in GL_n(\mathbb{R}) : A^{-1} = A^T\}$

Example 88. (special orthogonal group)
$SO_n = \{A \in O_n : \det \text{A} = 1\}$

Example 89. (unitary group)
$U_n = \{A \in GL_n(\mathbb{C}) : A^{-1} = A^{-T}\}$

Example 90. (special unitary group)
$SU_n = \{A \in U_n : \det \text{A} = 1\}$
special case:

$$SO_2 = \{ \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix} : \theta \in \mathbb{R}\} \text{ is abelian}$$

Example 91. $GL_n(\mathbb{R}) \subset M_n(\mathbb{R})$
$GL_n(\mathbb{R}) = n \times n$ real invertible matrices, non-abelian
$GL_n(\mathbb{C}) = n \times n$ complex invertible matrices, non-abelian
$GL_n(\mathbb{Z}_p) = n \times n$ invertible matrices with entries in $\mathbb{Z}_p$, p prime

if A represents $T : \mathbb{R}^n \mapsto \mathbb{R}^n$ and B represents $S : \mathbb{R}^n \mapsto \mathbb{R}^n$ then AB represents composition $T \circ S$
$A + B = B + A$, but $AB \neq BA$
Associative law: $A(BC) = (AB)C$
$I =$ identity matrix and $AI = IA = A$
Distributive law: $A(B + C) = AB + AC$
A is invertible $\leftrightarrow \exists B$ s.t. $AB = BA = I$
I is invertible. Take $B = I$.
Not all matrices are invertible.
e.g. 0 is not invertible since $0A = 0 = A0$ and $B = \frac{1}{a}$
1×1 matrices $[a]$ is invertible $\leftrightarrow a \neq 0$
2×2 matrices

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

invertible $\leftrightarrow ad - bc \neq 0$
Then

$$A^{-1} = \frac{1}{\det(A)} = \frac{1}{ad - bc} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$$

A is invertible $\leftrightarrow \det(A) \neq 0$
If inverse exists, then it is unique.
Suppose $AB = AC = I$.
Then $B(AB) = B(AC) = BI$, so $(BA)B = (BA)C$ so $IB = IC$ so $B = C$.
GL_n is closed under $\cdot$.
Two proofs: Suppose A, B are invertible.
Then AB is invertible since $(B^{-1}A^{-1})(AB) = B^{-1}(A^{-1}A)B = B^{-1}IB = I$.
Alt pf:
$\det(AB) = \det(A) \cdot \det(B)$ and $GL_n(\mathbb{R}) = \{A : \det(\text{A}) \neq 0\}$

Permutation Groups

A permutation is a symmetry of a configuration of identical objects.

A **permutation** of a sequence of symbols is a rearrangement of the order of the symbols.

Definition 92. permutation map

A **permutation** of a set S is a bijection $\sigma : S \to S$.

A permutation is an ordered arrangement of symbols.

Definition 93. S_n is the set of all permutations of a finite set.

Let $n \in \mathbb{Z}^+$.
Let $S = \{1, 2, ..., n\}$ be a set.
Let S_n be the set of all permutations of S.
Then $S_n = \{\sigma : S \to S | \ \sigma \text{ is a permutation } \}$.

Let $\sigma \in S_n$.

Then $\sigma : S \to S$ is a permutation, so σ is an ordered arrangement of n symbols.

Thus, σ is a sequence of n elements.

By the multiplication principle, there are n choices to place a symbol into the first slot, $n - 1$ choices to place a symbol into the second slot, ..., 1 choice to place a symbol in the n^{th} slot.

Hence, there are $n!$ different permutations of S, so there are $n!$ different permutations in S_n.

Therefore, $|S_n| = n!$.

Definition 94. symmetric group S_n of degree n

Let $n \in \mathbb{Z}^+$.
Let $\{1, 2, ..., n\}$ be a set.
Let S_n be the set of all permutations of $\{1, 2, ..., n\}$.
Then $S_n = \{\sigma : \sigma \text{ is a permutation of } n \text{ symbols}\}$.
S_n is called the **symmetric group on n symbols**.

Let $n \in \mathbb{Z}^+$.
Let $S = \{1, 2, ..., n\}$.
Let S_n be the symmetric group on n symbols.
Then $S_n = \{\sigma : S \to S | \ \sigma \text{ is a permutation } \}$.
Let $\sigma : S \to S$ be an element of S_n.
Then $\sigma : S \to S$ is a permutation, so $\sigma : S \to S$ is a bijective function.

Definition 95. symmetric group on a set

Let X be a set.
Let S_X be the set of all permutations of X.
S_X is called the **symmetric group on X**.

Let X be a nonempty set.
Let S_X be the symmetric group on X.
Then $S_X = \{\sigma : X \to X | \ \sigma \text{ is a permutation } \}$.
Let $\sigma : X \to X$ be an element of S_X.
Then $\sigma : X \to X$ is a permutation, so $\sigma : X \to X$ is a bijective function.

Theorem 96. $(S_X, \circ)$ ***is a group under function composition***
Let X be a nonempty set.
Let S_X be the set of all permutations of X.
Define $\circ$ to be function composition on S_X.
*Then $(S_X, \circ)$ is a group, called the **symmetric group on** X.*

Therefore, $(S_X, \circ)$ is the symmetric group on a set X under function composition.
The identity of S_X is the identity map $id : X \to X$ defined by $x \mapsto x$.
The inverse of permutation $\sigma : X \to X$ is the permutation $\sigma^{-1} : X \to X$ defined by $\sigma^{-1}(y) = x$ iff $\sigma(x) = y$.
Therefore, $\sigma \circ \sigma^{-1} = \sigma^{-1} \circ \sigma = id$.

Let $\sigma \in S_X$.
Then $\sigma : X \to X$ is a permutation, so σ is a bijective function.
Since function composition is generally not commutative, then $(S_X, \circ)$ is a generally nonabelian group.

Subgroups:
X = vector space : Iso(X) = all isomorphisms of X onto X
X = topological space : Homeo(X) = all homeomorphisms of X onto X

Corollary 97. $(S_n, \circ)$ ***is a group under function composition***
Let $n \in \mathbb{Z}^+$.
The symmetric group on n symbols is a group under function composition.

Therefore, the symmetric group $(S_n, \circ)$ is the group of all permutations of n symbols under function composition.
$(S_n, \circ)$ is the group of all permutations on a set of n elements.
The identity map id is the identity of S_n.
The number of permutations of n distinct objects taken n at a time is $P(n, n) = n!$.
Therefore, the number of permutations in S_n is $|S_n| = n!$.
Since the order of S_n is a finite number, then S_n is a finite group.

Let $\sigma \in S_n$.
Then $\sigma : i \mapsto \sigma(i)$ for all $i \in \{1, 2, ..., n\}$.

Let $\sigma\tau = \sigma \circ \tau$.
Then $(\sigma \circ \tau)(x) = \sigma(\tau(x))$ for all $x \in X$.
Hence, $\sigma\tau = \sigma \circ \tau$ means do τ first and then do σ second.
Therefore, our convention is to perform permutation multiplication(function composition) from right to left.

Definition 98. permutation group
Let X be a nonempty set.
Let $(S_X, \circ)$ be the symmetric group on X under function composition.
A subgroup of $(S_X, \circ)$ is called a **permutation group on** X.

A permutation group preserves the structure of the set X ("symmetries").

Let $n \in \mathbb{Z}^+$.
A subgroup of $(S_n, \circ)$ is called a **permutation group**.
Therefore, a permutation group is a subgroup of the symmetric group.

Example 99. $(S_3, \circ)$ **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)

Proposition 100. *Let $n \in \mathbb{Z}^+$.*
If $n \geq 3$, then $(S_n, \circ)$ is non-abelian.

$S_1 = \{id\}$ is abelian (trivial group).
$S_2 = \{id, (1\ 2)\}$ is abelian and $(S_2, \circ) \cong (\mathbb{Z}_2, +)$.
$S_3 = \{(1), (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)\}$ and S_3 is non-abelian.

Theorem 101. ***Cayley's Theorem***
Every group G is isomorphic to a subgroup of the symmetric group on G.

Therefore, every group is isomorphic to a permutation group.
For each $g \in G$ define the permutation $\lambda_g : G \to G$ by $\lambda_g(x) = gx$ for all $x \in G$.
The isomorphism $g \mapsto \lambda_g$ is called the **left regular representation of** G.
For each $g \in G$ define the permutation $\rho_g : G \to G$ by $\rho_g(x) = xg$ for all $x \in G$.
The isomorphism $g \mapsto \rho_g$ is called the **right regular representation of** G.

Corollary 102. *Every finite group of order n is isomorphic to a subgroup of S_n.*

Cycle notation for permutations

Cycle notation is a compact way to write permutations.

Definition 103. k **cycle**
Let X be a nonempty set.
Let $(S_X, \circ)$ be the symmetric group on X.
Let $\sigma \in S_X$.
Then $\sigma : X \to X$ is a permutation of X.
Let k be a positive integer with $k \geq 2$.
Let $S = \{a_1, a_2, ..., a_k\}$ be a subset of X such that
1. $\sigma(a_i) = a_{i \pmod{k}+1}$ for all $a_i \in S$.
This means

$$\begin{aligned}\sigma(a_1) &= a_2\\ \sigma(a_2) &= a_3\\ &\vdots\\ \sigma(a_k) &= a_1\end{aligned}$$

2. $(\forall x \in X - S)(\sigma(x) = x)$.
Then σ is a **cycle of length** k.
σ is called a k cycle.
k represents the number of elements moved by σ.
$(a_1\ a_2\ ...\ a_k)$ denotes a cycle of length k.

Let X be a nonempty set.
Let $S = \{a_1, a_2, ..., a_k\}$ be a subset of X.
Let $\sigma = (a_1\ a_2\ ...\ a_k)$.
Then σ is a k cycle.
Therefore, $a_1 \mapsto a_2 \mapsto a_3 ... \mapsto a_k \mapsto a_1$ and $\sigma(x) = x$ for all $x \in X - S$.

Denote the identity permutation by $id = (1)$ in cycle notation.

A cycle is a type of permutation.
A cycle can be written in several different ways.

Proposition 104. ***inverse of a cycle***
Let $\{a_1, a_2, ..., a_k\}$ be a subset of a nonempty set X.
Let σ be a k cycle in the symmetric group on X.
If $\sigma = (a_1\ a_2\ ...\ a_k)$, then $\sigma^{-1} = (a_k\ a_{k-1}\ ...\ a_2\ a_1)$.

The inverse of a cycle is the same elements written in reverse order.

Since there are several ways to represent the same cycle, the following is also true.
Observe that

$$\begin{aligned}
\sigma^{-1} &= (a_k\ a_{k-1}\ ...\ a_2\ a_1) \\
&= (a_1\ a_k\ a_{k-1}\ ...\ a_3\ a_2) \\
&= (a_2\ a_1\ a_k\ a_{k-1}\ ...\ a_4\ a_3) \\
&= ... \\
&= (a_{k-1}\ a_{k-2}\ ...\ a_2\ a_1\ a_k).
\end{aligned}$$

Proposition 105. ***order of a cycle***
Let $k \in \mathbb{Z}^+$.
A cycle of length k has order k.

Let $n \in \mathbb{Z}$ with $n \geq 2$.
Let $k \in \mathbb{Z}^+$ such that $2 \leq k \leq n$.
Let σ be a k cycle in the symmetric group $(S_n, \circ)$.
Let $id \in S_n$ be the identity permutation.
Then $|\sigma| = k$, so k is the least positive integer such that $\sigma^k = id$.

Definition 106. Disjoint cycle
Let $\alpha = (a_1\ a_2\ ...\ a_m)$ and $\beta = (b_1\ b_2\ ...\ b_n)$ be two cycles in the symmetric group on set X.
Then α and β are **disjoint** iff $a_i \neq b_j$ for all i, j.

Let $\alpha = (a_1\ a_2\ ...\ a_m)$ and $\beta = (b_1\ b_2\ ...\ b_n)$ be disjoint cycles.
Let $A = \{a_1, a_2, ..., a_m\}$ and $B = \{b_1, b_2, ..., b_n\}$.
Then $A \cap B = \emptyset$.
Therefore, disjoint cycles have no elements in common.

Theorem 107. ***Disjoint cycles commute.***
Let α and β be disjoint cycles in the symmetric group on set X.
Then $\alpha\beta = \beta\alpha$.

Therefore cycles with no elements in common commute with each other.
However, cycles with an element in common do not commute.

Theorem 108. ***Cycle Decomposition Theorem***
Every permutation of a nonempty finite set can be written as a finite product of disjoint cycles.

Let $n \in \mathbb{Z}+$.
Every permutation in $(S_n, \circ)$ can be written as a finite product of disjoint cycles.
Moreover, the decomposition of a permutation into disjoint cycles is unique up to the order and representation of cycles.

Since every permutation on a nonempty finite set can be decomposed into a product of cycles, then cycles are the building blocks of all permutations.

Corollary 109. *The order of a permutation is the least common multiple of the orders of its disjoint cycles.*

Let $\sigma \in (S_n, \circ)$.
Since every permutation is a finite product of disjoint cycles, then there exist $k \in \mathbb{Z}^+$ and disjoint cycles $\alpha_1, \alpha_2, ..., \alpha_k$ such that $\sigma = \alpha_1 \circ \alpha_2 \circ ... \circ \alpha_k$.
Let $|\alpha_1| = m_1$ and $|\alpha_2| = m_2$ and ... $|\alpha_k| = m_k$.
Then $|\sigma| = lcm(m_1, m_2, ..., m_k)$.

Proposition 110. *Let τ be a k cycle.*
If σ is a permutation, then $\sigma\tau\sigma^{-1}$ is a k cycle.

Parity of a permutation

Definition 111. transposition
A **transposition** is a permutation that swaps two elements and leaves everything else fixed.
A transposition is a 2-cycle.

Let $n \in \mathbb{Z}^+$ and $n \geq 2$.
Let X be a set of n elements.
Let id be the identity permutation of S_n.
Let $\{a, b\}$ be a subset of X.
Let $\tau \in S_n$ be a transposition of X defined by $\tau = (a, b)$.

Since τ is a 2 cycle, then $\tau(a) = b$ and $\tau(b) = a$ and $\tau(x) = x$ for $x \in X - \{a, b\}$.

Therefore $a \mapsto b \mapsto a$ and $b \mapsto a \mapsto b$, so $(b\ a) = (a\ b)$.

Since a transposition is a 2 cycle, then a transposition is a cycle of length 2, so a transposition has order 2.

Since τ has finite order $|\tau| = 2$, then 2 is the least positive integer such that $\tau^2 = id$.

Since $\tau^2 = id$, then $\tau^{-1} = \tau$.

Observe that $\tau^2 = (a\ b)(a\ b) = id$ and $(a\ b) = \tau = \tau^{-1} = (a\ b)^{-1} = (b\ a)$.

Theorem 112. ***A permutation is a product of transpositions***

Every permutation of a finite set containing at least two elements can be written as a finite product of transpositions.

Therefore, for $n \geq 2$, every permutation in $(S_n, \circ)$ can be written as a finite product of transpositions.

Hence, every permutation of a finite set can be written as a product of transpositions.

However, the decomposition of a permutation as a product of transpositions is not unique.

To decompose a permutation into a product of transpositions

1. Write the permutation as a product of disjoint cycles.
2. Decompose each cycle into a product of transpositions.

Observe that

$$\begin{aligned}(a_1\ a_2\ ...\ a_k) &= (a_1\ a_2)(a_2\ a_3)...(a_{k-1}\ a_k) \\ &= (a_1\ a_k)(a_1\ a_{k-1})\ ...(a_1\ a_3)(a_1\ a_2).\end{aligned}$$

Definition 113. even and odd permutation

Let X be a finite set of at least two elements.

Let σ be a permutation of X.

The permutation σ is **even** iff σ can be written as a product of an even number of transpositions.

The permutation σ is **odd** iff σ can be written as a product of an odd number of transpositions.

Lemma 114. ***Reduction Lemma***

If the identity permutation id can be written as a product of k transpositions, then id can be written as a product of $k - 2$ transpositions.

Lemma 115. ***Even Identity Lemma***

If the identity permutation is a product of k transpositions, then k is even.

Theorem 116. ***Parity Theorem***

If a permutation is a product of k and m transpositions, then either k and m are both even or k and m are both odd.

Therefore, if a permutation is a product of k and m transpositions, then k and m must have the same parity.

Hence, a permutation cannot be both even and odd.

Thus, a permutation must be either even or odd, but not both.

Let $n \in \mathbb{Z}^+$ and $n \geq 2$.

Let $X = \{1, 2, ..., n\}$ be a set of n elements.

Then $\{1, 2\}$ is a subset of X.

Since $id = (1\ 2)(1\ 2)$ is a product of 2 transpositions and 2 is even, then the identity permutation is an even permutation.

Since $(1, 2)(1, 2) = id$, then the identity map is an even permutation.

Theorem 117. *A cycle of even length is odd and a cycle of odd length is even.*

Since a transposition is a 2 cycle and 2 is even, then a transposition is an odd permutation.

Therefore, every transposition is an odd permutation.

Theorem 118. *The parity of a permutation is the same as the parity of its inverse.*

Let $n \geq 2$.

Let $\alpha \in S_n$.

Then $\alpha^{-1} \in S_n$ and the parity of α is the same as the parity of α^{-1}.

Thus, if α is an even permutation, then α^{-1} is an even permutation.

If α is an odd permutation, then α^{-1} is an odd permutation.

Theorem 119. *The composition of two permutations of the same parity is even.*

Let $n \geq 2$.

Let $\sigma, \tau \in S_n$ such that σ and τ have the same parity.

Then $\sigma\tau$ is an even permutation.

Thus, if σ and τ are both even, then $\sigma\tau$ is even.

If σ and τ are both odd, then $\sigma\tau$ is even.

Theorem 120. *The composition of two permutations of opposite parity is odd.*

Let $n \geq 2$.

Let $\sigma, \tau \in S_n$ such that σ and τ have opposite parity.

Then $\sigma\tau$ is an odd permutation.

Thus, if σ is even and τ is odd, then $\sigma\tau$ is an odd.

If σ is odd and τ is even, then $\sigma\tau$ is an odd.

Definition 121. signature of a permutation

The signature of a permutation σ, denoted $sgn(\sigma)$, is 1 if σ is even and -1 if σ is odd.

Since a permutation is either even or odd, but not both, then its signature is unique.

Proposition 122. *The function $S_n \to \{-1, 1\}$ that assigns to each permutation of S_n its signature is a group homomorphism.*

Theorem 123. *Let $(S_n, \circ)$ be the symmetric group on n symbols.*
Let $A_n = \{\sigma \in S_n : \sigma$ is an even permutation $\}$.
Then $A_n < S_n$.

Definition 124. Alternating Group A_n of order $\frac{n!}{2}$
Let $n \geq 2$.
Let $(S_n, \circ)$ be the symmetric group on n symbols.
Let $A_n = \{\sigma \in S_n : \sigma$ is an even permutation $\}$.
$(A_n, \circ)$ is called the **alternating group**.

Since $A_n < S_n$, then the alternating group is a subgroup of the symmetric group.

Theorem 125. *For $n \geq 2$, the number of even permutations in S_n equals the number of odd permutations.*
Moreover, the order of A_n is $\frac{n!}{2}$.

Proposition 126. *Let H be a subgroup of G such that $[G : H] = 2$.*
Then $H \lhd G$.

Since $[S_n : A_n] = \frac{|S_n|}{|A_n|} = \frac{|S_n|}{|S_n|/2} = 2$, then this implies $A_n \lhd S_n$.
Hence, S_n is not simple.

Symmetric group S_4

$(S_4, \circ)$ = nonabelian group of order $4! = 24$
identity = id
The elements in S_4 are:
$id, (34), (23), (234), (243), (24),$
$(12), (12)(34), (123), (1234), (1243), (124),$
$(132), (1342), (13), (134), (13)(24), (1324),$
$(1432), (142), (143), (14), (1423), (14)(23).$

Alternating group A_4

$(A_4, \circ)$ = nonabelian group of order $\frac{4!}{2} = 12$
identity = id
The elements in A_4 are:
$id, (234), (243), (12)(34),$
$(123), (124), (132), (134),$
$(13)(24), (142), (143), (14)(23).$

Symmetry Groups

Theorem 127. *The set of all geometric transformations of n dimensional space is a group under function composition.*

Let $Sym(\mathbb{R}^n)$ be the set of all geometric transformations of the n dimensional vector space $\mathbb{R}^n$.

Then $Sym(\mathbb{R}^n) = \{T | T : \mathbb{R}^n \to \mathbb{R}^n \text{ is a bijective map}\}$.

Let $\circ$ be function composition.

Then $(Sym(\mathbb{R}^n), \circ)$ is the symmetric group on $\mathbb{R}^n$.

The identity element is the identity map id.

The inverse of the transformation $\alpha : \mathbb{R}^2 \to \mathbb{R}^2$ is the inverse transformation $\alpha^{-1} : \mathbb{R}^2 \to \mathbb{R}^2$.

$Sym(\mathbb{R}^2)$ is the group of all transformations of $\mathbb{R}^2$.

$Sym(\mathbb{R}^3)$ is the group of all transformations of $\mathbb{R}^3$.

Theorem 128. *The set of all bijective isometries of* 2 *dimensional space is a subgroup of $Sym(\mathbb{R}^2)$.*

$Iso(\mathbb{R}^2) < Sym(\mathbb{R}^2)$.

Definition 129. The **isometry group of** $\mathbb{R}^2$ is the group of all bijective isometries from $\mathbb{R}^2$ onto $\mathbb{R}^2$ under function composition.

Let $(Iso(\mathbb{R}^2), \circ)$ be the isometry group of $\mathbb{R}^2$.

Then $Iso(\mathbb{R}^2) = \{\sigma | \sigma : \mathbb{R}^2 \to \mathbb{R}^2 \text{ is a bijective isometry}\}$.

The identity element is the identity map id.

The inverse of the bijective isometry $\alpha : \mathbb{R}^2 \to \mathbb{R}^2$ is the inverse isometry $\alpha^{-1} : \mathbb{R}^2 \to \mathbb{R}^2$.

Definition 130. A **regular n-gon** is a closed, convex polygon with n equal sides in the plane.

Definition 131. A **rigid motion** of the plane is a bijective map $\mathbb{R}^2 \to \mathbb{R}^2$ that preserves distance.

Therefore a rigid motion is a bijective isometry.

Definition 132. A **symmetry** of a figure is an undetectable rigid motion that preserves distance.

Therefore, a symmetry of a figure is a bijective isometry that preserves the figure.

Let $X \subset \mathbb{R}^2$.

Let $f : \mathbb{R}^2 \to \mathbb{R}^2$ be an isometry.

Then f is a **symmetry of** X iff $f(X) = X$.

Therefore a symmetry of X is a distance preserving function $f : \mathbb{R}^2 \to \mathbb{R}^2$ such that $f(X) = X$.

Theorem 133. *The set of all symmetries of a regular n-gon in $\mathbb{R}^2$ under function composition is a subgroup of the isometry group of $\mathbb{R}^2$.*

Therefore, $D_n < Iso(\mathbb{R}^2)$.
A geometric object is symmetric iff it has symmetries.
Let a, b be symmetries of a geometric object.
Define $a * b$ by do motion b first followed by do motion a.

Definition 134. Dihedral group D_n of order $2n$
The **dihedral group**, denoted $(D_n, \circ)$, is the set of all symmetries of a regular n sided polygon under function composition.
Therefore, D_n is the group of symmetries of a regular n-gon under function composition.
Hence, D_n is the group of undetectable rigid motions of a regular n-sided polygon.
$D_n = \{\rho : \rho($ is a symmetry of X $\} = \{\rho : \mathbb{R}^2 \to \mathbb{R}^2 \in Iso(\mathbb{R}^2) | \rho(X) = X\}$.
D_n consists of n rotations and n reflections.

There are n vertices to relabel to determine the number of rigid motions of D_n.
There are n choices to replace the first vertex.
If we replace the first vertex by k, then the second vertex must be replaced by either vertex $k+1$ or vertex $k-1$.
Hence, there are $2n$ choices for the given vertex to relabel, so there are $2n$ possible rigid motions of D_n.
$|D_n| = 2n$
Since $D_n < Iso(\mathbb{R}^2)$ and $Iso(\mathbb{R}^2) < Sym(\mathbb{R}^2)$, then $D_n < Sym(\mathbb{R}^2)$.

Theorem 135. *$(D_n, \circ)$ is isomorphic to a subgroup of $(S_n, \circ)$.*

Thus, there exists $H < S_n$ such that $D_n \cong H$, where n is the number of vertices of a regular n-sided polygon.

Definition 136. The **Euclidean group**, denoted $E(n)$, is the symmetry group of n dimensional Euclidean space.

Symmetries of a rectangle that is not a square (D_2)

Define the following symmetries of a non square rectangle with vertices $1, 2, 3, 4$ labeled counterclockwise.
Let $D_2 = \{e, r, s_h, s_v\}$.
Let e = do nothing motion (no rotation)
Let r = rotate by π
Let s_h = reflect about the horizontal line through the center of the rectangle
Let s_v = reflect about the vertical line through the center of the rectangle

*	e	r	s_h	s_v
e	e	r	s_h	s_v
r	r	e	s_v	s_h
s_h	s_h	s_v	e	r
s_v	s_v	s_h	r	e

D_2 is abelian.

$$
\begin{aligned}
e &\mapsto (1)\\
r &\mapsto (13)(24)\\
s_h &\mapsto (12)(34)\\
s_v &\mapsto (14)(23).
\end{aligned}
$$

$D_2 < A_4$.
D_2 is isomorphic to the Klein-4 group $V = \{e, a, b, c\}$.
An isomorphism from D_2 to V is:

$$
\begin{aligned}
e &\mapsto e\\
r &\mapsto a\\
s_h &\mapsto b\\
s_v &\mapsto c.
\end{aligned}
$$

Symmetries of an Equilateral Triangle (D_3)

Define the following symmetries of a triangle with vertices $1, 2, 3$ labeled counterclockwise.
Let $D_3 = \{e, r, r^2, a, b, c\}$.
Let $e =$ do nothing motion (no rotation)
Let $r =$ rotate by $\frac{2\pi}{3}$ ccw
Let $r^2 =$ rotate by $\frac{2\pi}{3}$ ccw twice
Let $a =$ reflect about the line through the center containing vertex 1
Let $b =$ reflect about the line through the center containing vertex 2
Let $c =$ reflect about the line through the center containing vertex 3

*	e	r	r^2	a	b	c
e	e	r	r^2	a	b	c
r	r	r^2	e	c	a	b
r^2	r^2	e	r	b	c	a
a	a	b	c	e	r	r^2
b	b	c	a	r^2	e	r
c	c	a	b	r	r^2	e

D_3 is not abelian.
$(D_3, *) \cong (S_3, \circ)$ and $|D_3| = 2 * 3 = 6$ and $|S_3| = 3! = 6$.
Let $S_3 = \{(1), (12), (13), (23), (123), (132)\}$.
An isomorphism from D_3 to S_3 is:

$$
\begin{aligned}
e &\mapsto (1)\\
r &\mapsto (123)\\
r^2 &\mapsto (132)\\
a &\mapsto (23)\\
b &\mapsto (13)\\
c &\mapsto (12).
\end{aligned}
$$

Proper subgroups of D_3:
$\langle a\rangle = \{a, e\}$
$\langle b\rangle = \{b, e\}$
$\langle c\rangle = \{c, e\}$
$\langle r\rangle = \langle r^2\rangle = \{e, r, r^2\}$
$\langle a\rangle \cong \langle b\rangle \cong \langle c\rangle$.

Symmetries of a Square (Octic group D_4)

Define the following symmetries of a square with vertices $1, 2, 3, 4$ labeled counterclockwise.
Let $D_4 = \{e, r, r^2, r^3, a, b, c, d\}$.
$|D_4| = 2 * 4 = 8$
Let $e =$ do nothing motion (no rotation)
Let $r =$ rotate by $\frac{\pi}{2}$ ccw
Let $r^2 =$ rotate by $\frac{\pi}{2}$ 2 times ccw
Let $r^3 =$ rotate by $\frac{\pi}{2}$ 3 times ccw
Let $a =$ reflect about the horizontal line through the center
Let $b =$ reflect about the vertical line through the center
Let $c =$ reflect about the main diagonal (NW to SE)
Let $d =$ reflect about the secondary diagonal (SW to NE)

*	e	r	r^2	r^3	a	b	c	d
e	e	r	r^2	r^3	a	b	c	d
r	r	r^2	r^3	e	d	c	a	b
r^2	r^2	r^3	e	r	b	a	d	c
r^3	r^3	e	r	r^2	c	d	b	a
a	a	c	b	d	e	r^2	r	r^3
b	b	d	a	c	r^2	e	r^3	r
c	c	b	d	a	r^3	r	e	r^2
d	d	a	c	b	r	r^3	r^2	e

D_4 is not abelian.

$$\begin{aligned}
e &\mapsto (1) \\
r &\mapsto (1234) \\
r^2 &\mapsto (13)(24) \\
r^3 &\mapsto (1432) \\
a &\mapsto (12)(34) \\
b &\mapsto (14)(23) \\
c &\mapsto (24) \\
d &\mapsto (13).
\end{aligned}$$

Cosets

Definition 137. Coset

Let $(H, *)$ be a subgroup of group $(G, *)$.
Define relation $\sim_L$ on G for all $a, b \in G$ by $a \sim_L b$ iff $a^{-1}b \in H$.
Then $\sim_L$ is an equivalence relation on G.
Define relation $\sim_R$ on G for all $a, b \in G$ by $a \sim_R b$ iff $ab^{-1} \in H$.
Then $\sim_R$ is an equivalence relation on G.
Let $g \in G$.
Then

$$\begin{aligned} gH &= \{x \in G : x \sim_L g\} \\ &= \{x \in G : g \sim_L x\} \\ &= \{x \in G : g^{-1}x \in H\} \\ &= \{gh \in G : h \in H\} \end{aligned}$$

gH is defined to be the left coset of H with representative $g \in G$.
Observe that

$$\begin{aligned} Hg &= \{x \in G : x \sim_R g\} \\ &= \{x \in G : xg^{-1} \in H\} \\ &= \{hg \in G : h \in H\} \end{aligned}$$

Hg is defined to be the right coset of H with representative $g \in G$.

Let $(H, *)$ be a subgroup of group $(G, *)$.
Let $g \in G$ be fixed.
The **left coset of H containing** g is $g * H = \{g * h : h \in H\}$.
The **right coset of H containing** g is $H * g = \{h * g : h \in H\}$.

Let $(H, +)$ be a subgroup of additive group $(G, +)$.
Let $g \in G$ be fixed.
The **left coset of H containing** g is $g + H = \{g + h : h \in H\}$.
The **right coset of H containing** g is $H + g = \{h + g : h \in H\}$.

Let $H < G$.
Let e be the identity of G.
Since $e \in H$ and $g = ge$, then $g \in gH$.
Therefore $(\forall g \in G)(g \in gH)$.
Since $e \in H$ and $g = eg$, then $g \in Hg$.
Therefore $(\forall g \in G)(g \in Hg)$.
Since $e \in G$, then $eH = \{eh : h \in H\} = \{h : h \in H\} = H$ and $He = \{he : h \in H\} = \{h : h \in H\} = H$.
Therefore, $eH = H = He$.

Since $\sim_L$ is an equivalence relation on G, then a left coset is an equivalence class and each element of G lies in exactly one left coset of H in G.

Therefore $a \sim_L b$ iff $aH = bH$.

Since $\sim_R$ is an equivalence relation on G, then a right coset is an equivalence class and each element of G lies in exactly one right coset of H in G.

Therefore $a \sim_R b$ iff $Ha = Hb$.

Example 138. Consider $(n\mathbb{Z}, +) < (\mathbb{Z}, +)$.

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

The left coset of $(n\mathbb{Z}, +)$ containing a is $a + n\mathbb{Z} = [a]_n$.

The right coset of $(n\mathbb{Z}, +)$ containing a is $n\mathbb{Z} + a = [a]_n$.

Thus, $a + n\mathbb{Z} = n\mathbb{Z} + a$.

The collection of all left cosets of $n\mathbb{Z}$ in $\mathbb{Z}$ is $\mathbb{Z}_n = \{[0], [1], [2], ..., [n-1]\}$.

The collection of all right cosets of $n\mathbb{Z}$ in $\mathbb{Z}$ is $\mathbb{Z}_n = \{[0], [1], [2], ..., [n-1]\}$.

Thus, the collection of all cosets of $n\mathbb{Z}$ in $\mathbb{Z}$ is $\mathbb{Z}_n = \{[0], [1], [2], ..., [n-1]\}$.

Thus, $\mathbb{Z}_n$ is a partition of $\mathbb{Z}$ and $[\mathbb{Z} : n\mathbb{Z}] = n$.

$[a]_n$ is an equivalence class of $\mathbb{Z}_n$.

Theorem 139. *Let $H < G$.*

Let $a, b \in G$.

Then the following are equivalent:

1. $a^{-1}b \in H$.

2. $(\exists h \in H)(a = bh)$.

3. $a \in bH$.

4. $aH = bH$.

Therefore, $a \sim_L b$ iff $a^{-1}b \in H$ iff a and b belong to the same left coset of H in G iff any of the 4 conditions above hold true.

Theorem 140. *Let $H < G$.*

Let $a, b \in G$.

Then the following are equivalent:

1. $ab^{-1} \in H$.

2. $(\exists h \in H)(a = hb)$.

3. $a \in Hb$.

4. $Ha = Hb$.

Therefore, $a \sim_R b$ iff $ab^{-1} \in H$ iff a and b belong to the same right coset of H in G iff any of the 4 conditions above hold true.

Lemma 141. *Let $H < G$.*

Let $a, b \in G$.

Then $aH = bH$ iff $Ha^{-1} = Hb^{-1}$.

Since $\sim_L$ is an equivalence relation defined on G, then the collection of all left cosets of H in G forms a partition of G.

Since $\sim_R$ is an equivalence relation defined on G, then the collection of all right cosets of H in G forms a partition of G.

Theorem 142. *Let H be a subgroup of a group G.*

The number of left cosets of H in G equals the number of right cosets of H in G.

Let $\frac{G}{\sim_L} = \{gH : g \in G\}$ be the collection of all left cosets of H in G.
Let $\frac{G}{\sim_R} = \{Hg : g \in G\}$ be the collection of all right cosets of H in G.
$\frac{G}{\sim_L}$ is a partition of G under $\sim_L$.
$\frac{G}{\sim_R}$ is a partition of G under $\sim_R$.
$|\frac{G}{\sim_L}| = |\frac{G}{\sim_R}|$.

Theorem 143. *Let H be a subgroup of a group G.*
Let $g \in G$ be fixed.
Then $|gH| = |H|$ and $|Hg| = |H|$.

Let $g \in G$.
Then $|gH| = |H| = |Hg|$.
Moreover, if $a, b \in G$, then $|aH| = |bH| = |Ha| = |Hb|$.

Hence, any two left cosets have the same cardinality and any two right cosets have the same cardinality and the cardinality of a left coset equals the cardinality of a right coset.

Definition 144. Index of H in G
Let H be a subgroup of group G.
The **index of H in G**, denoted $[G : H]$, is the number of distinct left cosets of H in G.

Let $\frac{G}{\sim_L} = \{gH : g \in G\}$ be the collection of all distinct left cosets of H in G.
Let $\frac{G}{\sim_R} = \{Hg : g \in G\}$ be the collection of all distinct right cosets of H in G.
Then $[G : H] = |\frac{G}{\sim_L}|$.
Since $|\frac{G}{\sim_L}| = |\frac{G}{\sim_R}|$, then $[G : H]$ equals the number of distinct right cosets of H in G.
Therefore $[G : H] = |\frac{G}{\sim_R}|$.

Finite Groups

Theorem 145. ***Lagrange's Theorem***
The order of a subgroup of a finite group divides the order of the group.

Let H be a subgroup of a finite group G.
Then $|H|$ divides $|G|$.

Let $[G : H] =$ the number of distinct left cosets of H in G.
Then $|G| = |H| * [G : H]$, so $|H|$ divides $|G|$.
Since H is a left coset of H in G, then $[G : H] > 0$, so $[G : H]$ divides $|G|$.
Therefore, the number of elements in $G =$ number of elements per left coset * number of left cosets.

Corollary 146. *The order of an element of a finite group divides the order of the group.*

Let G be a finite group.
Let $g \in G$.
Then $|g|$ divides $|G|$.

Corollary 147. *Let G be a finite group.*
If $H < K < G$, then $[G : H] = [G : K][K : H]$.

Corollary 148. *Let G be a finite group of order n.*
Then $g^n = e$ for all $g \in G$.

Corollary 149. *Every group of prime order is cyclic.*

Let G be a group of prime order.
Then the only subgroups of G are the trivial subgroup and G itself.
Any $a \in G$ such that $a \neq e$ is a generator of G.

Direct Products

Definition 150. External direct product of groups
Let $(A, \cdot)$ and $(B, *)$ be groups.
Let G be the Cartesian product $A \times B = \{(a, b) : a \in A, b \in B\}$.
Define component wise multiplication $\circ : G \times G \to G$ by $(a_1, b_1) \circ (a_2, b_2) = (a_1 \cdot a_2, b_1 * b_2)$ for all $(a_1, b_1), (a_2, b_2) \in A \times B$.
Then $(A \times B, \circ)$ is a group, called the **external direct product of** A **and** B.
The identity of $A \times B$ is (e, e') where e is identity of A and e' is identity of B.
The inverse of (a, b) is (a^{-1}, b^{-1}).

Let $G \times H$ be the direct product of finite groups G, H.
Then $|G \times H| = |G||H|$.

Example 151. Let $(\mathbb{R}, +)$. Define addition on $\mathbb{R} \times \mathbb{R} = \mathbb{R}^2$ by $(a, b) + (c, d) = (a + c, b + d)$. Then $(\mathbb{R}^2, +)$ is an abelian group with identity $(0, 0)$ and the additive inverse of (a, b) is $(-a, -b)$.

Example 152. $(\mathbb{Z}_2 \times \mathbb{Z}_2, +)$ is an abelian group of order 4 and $\mathbb{Z}_2 \times \mathbb{Z}_2 = \{(0, 0), (0, 1), (1, 0), (1, 1)\}$. Each element of $\mathbb{Z}_2 \times \mathbb{Z}_2$ has order 2, so there is no element of order 4. Thus, $\mathbb{Z}_2 \times \mathbb{Z}_2$ is not cyclic. Since there are only 2 groups of order 4 up to isomorphism, then $\mathbb{Z}_2 \times \mathbb{Z}_2 \cong V$. Hence, $\mathbb{Z}_2 \times \mathbb{Z}_2$ is isomorphic to the Klein 4 group which is isomorphic to D_2. Furthermore, $\mathbb{Z}_2 \times \mathbb{Z}_2 \ncong \mathbb{Z}_4$.

Definition 153. External direct product of n groups
Let $n \in \mathbb{Z}^+, n \geq 2$.
Let $G_1, G_2, ..., G_n$ be groups.
Then

$$\begin{aligned}\prod_{i=1}^{n} G_i &= G_1 \times G_2 \times ... \times G_n \\ &= \{(g_1, g_2, ..., g_n) : g_1 \in G_1 \wedge g_2 \in G_2 \wedge ... \wedge g_n \in G_n\} \\ &= \{(g_1, g_2, ..., g_n) : g_i \in G_i \text{ for each } i \in \{1, 2, ..., n\}\} \\ &= \{(g_1, g_2, ..., g_n) : (\forall i \in \{1, 2, ..., n\})(g_i \in G_i)\}.\end{aligned}$$

Let $G = G_1 \times G_2 \times ... \times G_n$.
Let $a, b \in G$. Then for each $i \in \{1, 2, ..., n\}$ there exist $a_i, b_i \in G_i$ such that $a = (a_1, a_2, ..., a_n)$ and $b = (b_1, b_2, ..., b_n)$.
Define component wise multiplication on G by the n tuple whose i^{th} component is $a_i b_i$ for each i.
Then $ab = (a_1, a_2, ..., a_n)(b_1, b_2, ..., b_n) = (a_1 b_1, a_2 b_2, ..., a_n b_n)$.

Theorem 154. *Let $n \in \mathbb{Z}^+, n \geq 2$.*
The external direct product of n groups is a group.

Therefore, the direct product of n groups is a group.

Theorem 155. *A direct product of abelian groups is an abelian group.*

Let $G_1, G_2, ..., G_n$ be additive abelian groups. Then the direct product $G = G_1 \times G_2 \times ... \times G_n$ is called the **direct sum of n groups** and is denoted $\bigoplus_{i=1}^{n}$.
Therefore, $G = \bigoplus_{i=1}^{n} G_i = G_1 \oplus G_2 \oplus ... \oplus G_n$.
Hence, the direct sum of abelian groups is an abelian group.

Definition 156. External direct product of a group with itself n times
Let $n \in \mathbb{Z}^+, n \geq 2$.
Let G be a group. Then

$$\begin{aligned}G^n &= G \times G \times ... \times G \\ &= \{(g_1, g_2, ..., g_n) : g_1 \in G \wedge g_2 \in G ... \wedge g_n \in G\} \\ &= \{(g_1, g_2, ..., g_n) : g_i \in G \text{ for each } i \in \{1, 2, ..., n\}\} \\ &= \{(g_1, g_2, ..., g_n) : (\forall i \in \{1, 2, ..., n\})(g_i \in G)\}\end{aligned}$$

Example 157. Let $(\mathbb{Z}_2, +)$ be the cyclic group of integers modulo 2. Let $n \in \mathbb{Z}^+$.
Then

$$\begin{aligned}\mathbb{Z}_2^n &= \mathbb{Z}_2 \times \mathbb{Z}_2 \times ... \times \mathbb{Z}_2 \\ &= \{(a_1, a_2, ..., a_n) : a_1 \in \mathbb{Z}_2 \wedge a_2 \in \mathbb{Z}_2 ... \wedge a_n \in \mathbb{Z}_2\} \\ &= \{(a_1, a_2, ..., a_n) : a_i \in \mathbb{Z}_2 \text{ for each } i \in \{1, 2, ..., n\}\} \\ &= \{(a_1, a_2, ..., a_n) : (\forall i \in \{1, 2, ..., n\})(a_i \in \mathbb{Z}_2)\}\end{aligned}$$

Thus, $\mathbb{Z}_2^n$ is a group of all n tuples consisting of 0 or 1 (binary n tuples).

Let $\mathbb{Z}_2 = \{0,1\}$ and $S = \{T, F\}$. Then $(S, \oplus) \cong (\mathbb{Z}_2, +)$ since $\phi : S \to \mathbb{Z}_2$ defined by $\phi(F) = 0$ and $\phi(T) = 1$ is an isomorphism. Therefore, addition modulo 2 corresponds to logical XOR operation ($\oplus$).

Hence, $\mathbb{Z}_2^n$ is a group of binary n tuples with binary operation logical XOR.

Let $a = (0,1,0,1,1,1,0,1)$ and $b = (0,1,0,0,1,0,1,1)$ in $\mathbb{Z}_2^8$.

Then $ab = (0,1,0,1,1,1,0,1) + (0,1,0,0,1,0,1,1) = (0,0,0,1,0,1,1,0)$.

Theorem 158. *Let $G \times H$ be the external direct product of groups G, H. Let $(g,h) \in G \times H$. If g and h have finite order, then the order of (g,h) in $G \times H$ is the least common multiple of the orders of g and h.*

Let $(g,h) \in G \times H$.

Then $|(g,h)| = lcm(|g|, |h|)$.

Corollary 159. *Let $n \in \mathbb{Z}^+, n \geq 2$. Let $\prod_{i=1}^n G_i$ be the external direct product of n groups. Let $(g_1, g_2, ..., g_n) \in \prod_{i=1}^n G_i$. If each g_i has finite order a_i in G_i, then the order of $(g_1, g_2, ..., g_n)$ in $\prod_{i=1}^n G_i$ is the least common multiple of $a_1, a_2, ..., a_n$.*

Theorem 160. *Let $m, n \in \mathbb{Z}^+$.*

Then $(\mathbb{Z}_m \times \mathbb{Z}_n, +) \cong (\mathbb{Z}_{mn}, +)$ iff $\gcd(m,n) = 1$.

Corollary 161. *Let $n_1, ..., n_k$ be positive integers.*

Then $\prod_{i=1}^k \mathbb{Z}_{n_i} \cong \mathbb{Z}_{n_1 ... n_k}$.

Corollary 162. *Let $p_1, ..., p_k$ be distinct primes. Let $n = p_1^{e_1} ... p_k^{e_k}$.*

Then $\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{e_1}} \times ... \times \mathbb{Z}_{p_k^{e_k}}$.

Definition 163. product of sets

Let H and K be subsets in a group G.

The **product of H and K** is the set $HK = \{hk : h \in H, k \in K\}$.

Let $x \in HK$. Then there exists $h \in H$ and $k \in K$ such that $x = hk$. Since $h \in H$ and $H \subset G$, then $h \in G$. Since $k \in K$ and $K \subset G$, then $k \in G$. Since $hk \in G$, then $x \in G$, so $HK \subset G$.

Proposition 164. *If H and K are subgroups of an abelian group G, then $HK < G$.*

Proposition 165. *Let H and K be subgroups of a group G.*

If $h^{-1}kh \in K$ for all $h \in H$ and all $k \in K$, then $HK < G$.

Proposition 166. *Let H and K be subgroups of a group G.*

Then $HK < G$ iff $KH \subset HK$.

Definition 167. Internal direct product of groups

Let G be a group with subgroups H, K such that

1. $G = HK = \{hk : h \in H, k \in K\}$.
2. $H \cap K = \{e\}$.
3. $hk = kh$ for all $h \in H, k \in K$.

Then G is called the **internal direct product of H and K** .

Normal Subgroups

Definition 168. Normal subgroup

Let H be a subgroup of a group G.
Then H is **normal in** G iff $(\forall g \in G)(\forall h \in H)(ghg^{-1} \in H)$.
$H \triangleleft G$ means H is normal in G.

Let G be a group with identity e.
Since $G < G$ and $ghg^{-1} \in G$ for all $g, h \in G$, then $G \triangleleft G$.
Therefore, every group is a normal subgroup of itself.
Since $geg^{-1} = gg^{-1} = e \in \{e\}$ for all $g \in G$, then $\{e\} \triangleleft G$.
Therefore, the trivial subgroup is a normal subgroup of every group.

Definition 169. conjugate

Let G be a group.
Let $x \in G$.
Then y is a **conjugate to** x **in** G iff $(\exists a \in G)(y = axa^{-1})$.

Definition 170. Set gHg^{-1}

Let G be a group.
Let $H < G$.
Let $g \in G$.
Then $gHg^{-1} = \{ghg^{-1} : h \in H\}$.

Theorem 171. *Let $H < G$. Then the following are equivalent:*

1. $H \triangleleft G$.
2. $gHg^{-1} \subset H$ *for all* $g \in G$.
3. $gHg^{-1} = H$ *for all* $g \in G$.

Theorem 172. *Let $H < G$.*
Then $H \triangleleft G$ iff $gH = Hg$ for all $g \in G$.

Therefore, a normal group H is a subgroup of G in which the left and right cosets of H in G are equal for each $g \in G$.

Thus, the left and right cosets of H in G are equal for each $g \in G$.

Hence, the partition of G into left cosets of H equals the partition of G into right cosets of H.

Therefore, in any normal subgroup H of G, $L_H = R_H$ where L_H is the collection of all distinct left cosets of H in G and R_H is the collection of all distinct right cosets of H in G.

Theorem 173. *Every subgroup of an abelian group is normal.*

Let H be a subgroup of an abelian group G.
Then $H \triangleleft G$.

Theorem 174. *The intersection of two normal subgroups is a normal subgroup.*

Let G be a group.
If $H \triangleleft G$ and $K \triangleleft G$, then $H \cap K \triangleleft G$.

Proposition 175. *If G is a group and $H < G$, then $gHg^{-1} < G$ and $gHg^{-1} \cong H$ for all $g \in G$.*

Definition 176. Normalizer of a subgroup

Let G be a group.

Let $H < G$.

The **normalizer of H in G**, denoted $N(H)$, is the set $N(H) = \{g \in G : gHg^{-1} = H\}$.

Proposition 177. *Let H be a subgroup of group G.*

Let $N(H) = \{g \in G : (\forall h \in H)(gh = hg)\}$.

*Then $N(H)$ is a subgroup of G, called the **normalizer of H in G**.*

Proposition 178. *If G is a group and $H < G$, then $N(H) < G$ and $H \subset N(H)$.*

Definition 179. Centralizer of an element

Let G be a group.

Let $g \in G$.

The **centralizer of** g, denoted $C(g)$, is the set of elements of G that commute with g.

Therefore $C(g) = \{x \in G : xg = gx\}$.

Theorem 180. *Let G be a group.*

Let $g \in G$.

Then $C(g) < G$.

If g generates a normal subgroup of G, then $C(g) \lhd G$. We're stuck in this part of the proof!

Definition 181. Center of a group

Let $(G, *)$ be a group.

Let $a, b \in G$.

We say that a and b **commute** iff $ab = ba$.

The **center of** G, denoted $Z(G)$, is the set of elements of G that commute with all elements of G.

Therefore, $Z(G) = \{x \in G : (\forall g \in G)(xg = gx)\}$.

Theorem 182. ***The center of a group G is a normal subgroup of G.***

Let G be a group.

Then $Z(G) \lhd G$.

Definition 183. Commutator

Let $(G, *)$ be a group.

Let $a, b \in G$.

The **commutator of a and b**, denoted by $[a, b]$, is $aba^{-1}b^{-1}$.

Therefore, $[a, b] = aba^{-1}b^{-1}$.

Definition 184. Commutator subgroup
Let $(G, *)$ be a group.
Let $a, b \in G$.
The **commutator subgroup of** G, denoted by G', is the subgroup of G generated by all the commutators.

Definition 185. simple group
A group G is **simple** if its only normal subgroups are $\{e\}$ and G.

A simple group cannot be decomposed any further.

Example 186. Any group of prime order is simple.
If G is a group of prime order, then its only subgroups are $\{e\}$ and G itself.
Hence, these are the only normal subgroups of G.
In particular, $(\mathbb{Z}_p, +)$ is simple for prime p.

Definition 187. Quotient Group $\frac{G}{N}$ of order $[G : N]$
Let G be a group and $N \lhd G$.
Let $\frac{G}{N}$ be the set of all cosets of N in G.
Then $\frac{G}{N} = \{aN : a \in G\}$.
Define $(aN)(bN) = (ab)N$ for all $aN, bN \in \frac{G}{N}$.
Then $(\frac{G}{N}, *)$ is a group and $|\frac{G}{N}| = [G : N]$.
The identity is N and $(aN)^{-1} = a^{-1}N$.
$(\frac{G}{N}, *)$ is the **factor group** or **quotient group of** G **modulo** N.
Each aN is called a **coset modulo** N.

If G is finite, then $|\frac{G}{N}| = [G : N] = \frac{|G|}{|N|}$.

Example 188. $\frac{\mathbb{Z}}{n\mathbb{Z}} = \{n\mathbb{Z}, 1+n\mathbb{Z}, 2+n\mathbb{Z}, 3+n\mathbb{Z}, ..., (n-1)+n\mathbb{Z}\} = \{[0]_n, [1]_n, [2]_n, ..., [n-1]_n\} = \mathbb{Z}_n$.
$|\frac{\mathbb{Z}}{n\mathbb{Z}}| = [\mathbb{Z} : n\mathbb{Z}] = n$.
$(k + \mathbb{Z}) + (m + \mathbb{Z}) = (k + m) + \mathbb{Z}$.

Theorem 189. *If N is a subgroup of an abelian group G, then $\frac{G}{N}$ is abelian.*

Theorem 190. *If N is a subgroup of a cyclic group G, then $\frac{G}{N}$ is cyclic.*

If $g \in G$ is a generator of G, then gN is a generator of $\frac{G}{N}$.

Theorem 191. *Let G be a group and let $Z(G)$ be the center of G.*
If $\frac{G}{Z(G)}$ is cyclic, then G is abelian.

Homomorphisms

Homomorphisms are maps that preserve algebraic structure.

Definition 192. Group Homomorphism

Let $(G, *)$ and $(H, \star)$ be groups.
Let $\phi : G \to H$ be a function.
Then ϕ is a **homomorphism** iff $\phi(a * b) = \phi(a) \star \phi(b)$ for all $a, b \in G$.

A homomorphism preserves the binary operation of G.

Example 193. trivial homomorphism

The **trivial homomorphism** is the group homomorphism $\phi : G \to G'$ such that $\ker(\phi) = G$ and $Im(\phi) = \{e'\}$.

Thus, ϕ maps every element of G to the identity $e'$of G' and $Im(\phi) = \phi(G) = \{e'\}$.

Example 194. Let $(\mathbb{Z}, +)$ and $(G, *)$ be groups.
Let $g \in G$.
Let $\phi : \mathbb{Z} \to G$ be defined by $\phi(n) = g^n$ for all $n \in \mathbb{Z}$.
Let $m, n \in \mathbb{Z}$.
Then

$$\begin{aligned} \phi(m+n) &= g^{m+n} \\ &= g^m g^n \\ &= \phi(m)\phi(n). \end{aligned}$$

Therefore, ϕ is a homomorphism.
Either g has finite order or g has infinite order.

Suppose g has infinite order.
Then $g^n = e$ implies $n = 0$.
Hence, $\ker(\phi) = \{0\} = \langle 0 \rangle$, so ϕ is injective.
The image is $Im(\phi) = \{\phi(g) : g \in \mathbb{Z}\} = \{g^n : n \in \mathbb{Z}\}$.
Since ϕ is injective, then $\mathbb{Z} \cong Im(\phi) = \{..., g^{-2}, g^{-1}, g^0, g, g^2, ...\}$.

Suppose g has finite order n.
Then $g^k = e$ iff $n|k$ for integer k.
Hence, $\ker(\phi) = \{k \in \mathbb{Z} : n|k\} = \{nm : m \in \mathbb{Z}\} = n\mathbb{Z} = \langle n \rangle$.
The image is $Im(\phi) = \{\phi(g) : g \in \mathbb{Z}\} = \{g^n : n \in \mathbb{Z}\} = \langle g \rangle$.
Let $\langle g \rangle$ be the cyclic subgroup of G generated by $g \in G$.
Then $\langle g \rangle = \{g^k : k \in \mathbb{Z}\}$ and $\langle g \rangle < G$.

Let $f : \mathbb{Z} \to \langle g \rangle$ be the restriction of ϕ to $\langle g \rangle$.
Let $g^k \in \langle g \rangle$.
Then $k \in \mathbb{Z}$.
Therefore, f is surjective.

Example 195. Let $(GL_2(\mathbb{R}), \cdot)$ and $(\mathbb{R}^*, \cdot)$ be groups.

Let $f : GL_2(\mathbb{R}) \to \mathbb{R}^*$ be defined by $f(A) = \det A$ for all $A \in GL_2(\mathbb{R})$. Let $A \in GL_2(\mathbb{R})$. Then there exist $a, b, c, d \in \mathbb{R}$ such that

$$\text{A} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

and A is invertible. Thus, $\det(A) = ad - bc \neq 0$. Hence, $f(A) \in \mathbb{R}^*$.

Let $A, B \in GL_2(\mathbb{R})$.

Then

$$\begin{aligned} f(AB) &= \det(AB) \\ &= \det(A)\det(B) \\ &= f(A)f(B). \end{aligned}$$

Hence, f is a homomorphism.

Observe that

$$\begin{aligned} \ker(f) &= \{A \in GL_2(\mathbb{R}) : f(A) = 1\} \\ &= \{A \in GL_2(\mathbb{R}) : \det(A) = 1\} \\ &= SL_2(\mathbb{R}). \end{aligned}$$

Example 196. Let $(\mathbb{R}, +)$ and $(\mathbb{C}^*, \cdot)$ be groups.

Let $f : \mathbb{R} \to \mathbb{C}^*$ be defined by $f(\theta) = cis(\theta)$ for all $\theta \in \mathbb{R}$.

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

$$\begin{aligned} f(a+b) &= cis(a+b) \\ &= \cos(a+b) + i\sin(a+b) \\ &= \cos(a)\cos(b) - \sin(a)\sin(b) + i(\sin(a)\cos(b) + \cos(a)\sin(b)) \\ &= \cos(b)(\cos(a) + i\sin(a)) - \sin(a)\sin(b) + i\cos(a)\sin(b) \\ &= \cos(b)cis(a) + i\sin(b)(i\sin(a) + \cos(a)) \\ &= \cos(b)cis(a) + i\sin(b)cis(a) \\ &= cis(a)(\cos(b) + i\sin(b)) \\ &= cis(a)cis(b) \\ &= f(a)f(b). \end{aligned}$$

Hence, f is a homomorphism.

Let $T = \{z \in \mathbb{C} : |z| = 1\}$ be the circle group.

Observe that

$$\begin{aligned} Im(f) &= f(\mathbb{R}) \\ &= \{f(\theta) \in \mathbb{C}^* : \theta \in \mathbb{R}\} \\ &= \{cis(\theta) \in \mathbb{C}^* : \theta \in \mathbb{R}\} \\ &= \{z \in \mathbb{C}^* : |z| = 1\} \\ &= T. \end{aligned}$$

Observe that

$$\begin{aligned}
\ker(f) &= \{\theta \in \mathbb{R} : f(\theta) = 1\} \\
&= \{\theta \in \mathbb{R} : cis(\theta) = 1\} \\
&= \{2\pi k : k \in \mathbb{Z}\} \\
&= \langle 2\pi \rangle.
\end{aligned}$$

Note that $\langle 2\pi \rangle \cong (\mathbb{Z}, +)$.

Definition 197. Types of homomorphisms
An injective homomorphism is called a **monomorphism**.
A surjective homomorphism is called an **epimorphism**.
A bijective homomorphism is called an **isomorphism**.
An **endomorphism** is a homomorphism of a group with itself.
Therefore, the homomorphism $\phi : G \to G$ is called an endomorphism.
An **automorphism** is an isomorphism of a group with itself.
Therefore, the isomorphism $\phi : G \to G$ is called an automorphism.

Definition 198. Image of a Homomorphism
Let $\phi : G \to G'$ be a group homomorphism.
The **image of** ϕ, denoted $Im(\phi)$, is the set $\phi(G) = \{\phi(g) \in G' : g \in G\}$.

Theorem 199. ***preservation properties of a group homomorphism***
Let $(G, *)$ be a group with identity e.
Let $(G', \star)$ be a group with identity e'.
Let $\phi : G \to G'$ be a homomorphism.
Then
1. $\phi(e) = e'$. preserves identity
2. $(\forall a \in G)[\phi(a^{-1}) = (\phi(a))^{-1}]$. preserves inverses
3. $(\forall k \in \mathbb{Z})[\phi(a^k) = (\phi(a))^k]$. preserves powers of a
4. If $H < G$, then $\phi(H) < G'$. preserves subgroups of G
In particular, since $G < G$, then $\phi(G) < G'$.
This means the image of a homomorphism is a subgroup of G'.
5. If $K' < G'$, then $\phi^{-1}(K') < G$. preserves subgroups of G'
Moreover, if $K' \lhd G'$, then $\phi^{-1}(K') \lhd G$.

Definition 200. Kernel of a Homomorphism
Let $\phi : G \to G'$ be a group homomorphism.
Let e be the identity of G.
Let e' be the identity of G'.
The **kernel of** ϕ, denoted $\ker(\phi)$, is the set $\{g \in G : \phi(g) = e'\}$.
Therefore, $\ker(\phi) = \{g \in G : \phi(g) = e'\}$.

Since $e \in G$ and $\phi(e) = e'$, then $e \in \ker(\phi)$.
The group $\{e'\}$ is the trivial subgroup of G'.
Hence, the kernel of ϕ is the preimage of the trivial subgroup of G'.
Therefore, $\ker(\phi) = \phi^{-1}\{e'\}$.

Theorem 201. *Let $\phi : G \to G'$ be a group homomorphism.*
Then $\ker(\phi) \lhd G$.

Therefore the kernel of a group homomorphism $\phi : G \to G'$ is a normal subgroup of G.

Theorem 202. *Let $\phi : G \to G'$ be a group homomorphism.*
Let e be the identity of G. Then
1. If ϕ is injective, then $G \cong \phi(G)$.
2. ϕ is injective iff $\ker(\phi) = \{e\}$.

Theorem 203. *Let $\phi : G \to G'$ be a group homomorphism.*
Let e be the identity of G. Then
1. ϕ is an epimorphism iff $Im(\phi) = G'$.
2. ϕ is a monomorphism iff $\ker(\phi) = \{e\}$.
3. ϕ is an isomorphism iff $\ker(\phi) = \{e\}$ *and $Im(\phi) = G'$.*

Theorem 204. *The composition of group homomorphisms is a group homomorphism.*

Let $f_1 : G \to G'$ be a group homomorphism.
Let $f_2 : G' \to G''$ be a group homomorphism.
Let $f_2 \circ f_1 : G \to G''$ be the composition of f_1 and f_2.
Then $f_2 \circ f_1$ is a group homomorphism.

Theorem 205. *Let $\phi : G \to G'$ be a group homomorphism with kernel K.*
Then $xK = Kx = \phi^{-1}(\phi(x))$ for all $x \in G$.

The coset of the kernel with representative $x \in G$ is the preimage of x under ϕ.
Therefore, $xK = \phi^{-1}(\phi(x)) = \{a \in G : \phi(a) = \phi(x)\}$.

Corollary 206. *If G is a finite group and $\phi : G \to G'$ is a group homomorphism, then* $|G| = |\ker(\phi)||Im(\phi)|$.

$|Im(\phi)|$ is the number of distinct cosets of $\ker(\phi)$ in G.

Theorem 207. *Let G be a group.*
If $N \lhd G$, then $\eta : G \to \frac{G}{N}$ defined by $\eta(a) = aN$ for all $a \in G$ is a homomorphism such that $\ker(\eta) = N$.

We call η the **natural surjective homomorphism** from G onto $\frac{G}{N}$ with kernel N.
$\eta : G \to \frac{G}{N}$ is surjective.

Isomorphisms

Definition 208. Isomorphism

Let $(G, *)$ and $(H, \star)$ be groups.
Let $\phi : G \to H$ be a function.
Then ϕ is an **isomorphism** of G with H iff
1. ϕ is a homomorphism
2. ϕ is bijective.

Therefore, an isomorphism is a bijective homomorphism.

$(G, *)$ is **isomorphic to** $(H, \star)$ iff there exists an isomorphism $\phi : G \to H$.
$(G, *) \cong (H, \star)$ means $(G, *)$ is isomorphic to $(H, \star)$

Isomorphic algebraic structures are structurally identical.

If $(G, *) \cong (H, \star)$ then any algebraic property that is preserved by isomorphism and which is true of $(G, *)$ is also true of $(H, \star)$.

Algebraic properties preserved by isomorphism:
1. closure is preserved.
2. associativity of $*$ is preserved.
3. commutativity of $*$ is preserved.
4. identity element is preserved.
5. invertible elements are preserved.
6. subgroups are preserved.

Example 209. 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 $(\mathbb{Z}_4, +) \cong (U_4, \cdot)$.

Example 210. $(\mathbb{R}, +) \cong (\mathbb{R}^+, \cdot)$ since $\phi : \mathbb{R} \to \mathbb{R}^+$ defined by $\phi(x) = e^x$ for all $x \in \mathbb{R}$ is an isomorphism.

Example 211. For $n \neq 0, (\mathbb{Z}, +) \cong (n\mathbb{Z}, +)$ since $\phi : \mathbb{Z} \to n\mathbb{Z}$ defined by $\phi(k) = nk$ for all $k \in \mathbb{Z}$ is an isomorphism.

Example 212. Let $S = \{2^k : k \in \mathbb{Z}\}$.
Then $(S, \cdot) < (\mathbb{Q}^+, \cdot)$.
$(\mathbb{Z}, +) \cong (S, *)$ since $\phi : \mathbb{Z} \to S$ defined by $\phi(n) = 2^n$ for all $n \in \mathbb{Z}$ is an isomorphism.

Example 213. Let $M_2(\mathbb{R})$ = the set of all 2x2 matrices with real entries.

$$\text{Let } H = \text{the set of all matrices of the form } \begin{bmatrix} a & -b \\ b & a \end{bmatrix} \text{ where } a, b \in \mathbb{R}$$

Then $H \subset M_2(\mathbb{R})$ and $(H, +)$ and $(H, \cdot)$ are binary structures.

Let $\phi : \mathbb{C} \mapsto H$ such that $\phi(a+bi) = \begin{bmatrix} a & -b \\ b & a \end{bmatrix}$ where $a, b \in \mathbb{R}$.

Then $(\mathbb{C}, +) \cong (H, +)$ and $(\mathbb{C}, \cdot) \cong (H, \cdot)$.
H is a matrix representation of the complex numbers.

Lemma 214. *The isomorphism relation on groups is reflexive.*

Let $(G, *)$ be a group.
Then $G \cong G$.
Therefore, every group is isomorphic to itself.
The identity map $\phi : G \to G$ be defined by $\phi(x) = x$ for all $x \in G$ is an isomorphism.

Lemma 215. *The isomorphism relation on groups is symmetric.*

Let $(G, *)$ and $(H, \cdot)$ be groups.
If $G \cong H$, then $H \cong G$.
Therefore, if $\phi : G \to H$ is an isomorphism, then the inverse map $\phi^{-1} : H \to G$ is an isomorphism.

Lemma 216. *The isomorphism relation on groups is transitive.*

Let $(G, *), (H, \cdot), (K, \diamond)$ be groups.
If $G \cong H$ and $H \cong K$, then $G \cong K$.
Therefore, if $\phi : G \to H$ and $\psi : H \to K$ are isomorphisms, then $\psi \circ \phi : G \to K$ is an isomorphism.

Theorem 217. *The isomorphism relation on groups is an equivalence relation on the class of all groups.*

Let $\cong$ be the isomorphism relation on the class of all groups.
Then $\cong$ is reflexive, symmetric, and transitive.

Theorem 218. ***preservation properties of a group isomorphism***
Let $\phi : G \to G'$ be a group isomorphism. Then
1. $|G| = |G'|$. preserves cardinality
2. If G is abelian, then G' is abelian. preserves commutativity
3. If G is cyclic, then G' is cyclic. preserves cyclic property
4. If H is a subgroup of G of order n, then $\phi(H)$ is a subgroup of G' of order n. preserves finite subgroups
5. $(\forall a \in G, n \in \mathbb{Z}^+)(|a| = n \to |\phi(a)| = n)$. preserves finite order of an element

In particular, if G is finite, then if $|a| = |G|$, then $|\phi(a)| = |G|$.
Therefore, if G is a finite group and if a is a generator, then $\phi(a)$ is a generator.

Isomorphic cyclic groups

Theorem 219. *Every cyclic group of infinite order is isomorphic to* $(\mathbb{Z}, +)$.

Theorem 220. *Every cyclic group of finite order* n *is isomorphic to* $(\mathbb{Z}_n, +)$.

Since a cyclic group is either finite or infinite, then every cyclic group is isomorphic to either $\mathbb{Z}_n$ or $\mathbb{Z}$.

Thus, up to isomorphism, the only cyclic groups are $\mathbb{Z}$ and $\mathbb{Z}_n$.

Corollary 221. *Every group of prime order* p *is isomorphic to* $(\mathbb{Z}_p, +)$.

Proposition 222. *Let* G *be an abelian group with subgroups* H *and* K.
If $HK = G$ *and* $H \cap K = \{e\}$, *then* $G \cong H \times K$.

Proposition 223. *The identity map is an automorphism in any group.*

Let $(G, *)$ be a group.

The identity map $I_G : G \to G$ defined by $I_G(x) = x$ for all $x \in G$ is an automorphism.

Example 224. 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 $\mathbb{C}$.

Example 225. 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 $\mathbb{C}^*$.

Theorem 226. *Let* $Aut(G)$ *be the set of all automorphisms of a group* G.
Then $(Aut(G), \circ)$ *is a subgroup of* $(S_G, \circ)$.

Definition 227. Group of Automorphisms $Aut(G)$
Let $Aut(G)$ be the set of all automorphisms of a group G.
Then $Aut(G) = \{\alpha : G \to G | \alpha \text{ is an isomorphism}\}$.
$(Aut(G), \circ)$ is called the **group of automorphisms of** G.
$\circ$ is function composition
$Aut(G) < S_G$.
identity is the identity map $I_G : G \to G$ defined by $I_G(x) = x$ for all $x \in G$.

Proposition 228. ***inner automorphism***
Let $\langle G, * \rangle$ *be a group.*
Let $g \in G$ *be a fixed element.*
Then the map $i_g : G \to G$ *defined by* $i_g(x) = g * x * g^{-1}$ *for all* $x \in G$ *is an isomorphism of* G *with itself.*

Theorem 229. ***First Isomorphism Theorem***
Let $\phi : G \to G'$ *be a group homomorphism with kernel* K.
Then there exists a group isomorphism $\psi : \frac{G}{K} \to \phi(G)$ *defined by* $\psi(gK) = \phi(g)$ *for all* $g \in G$ *such that* $\psi \circ \eta = \phi$, *where* $\eta : G \to \frac{G}{K}$ *is the natural homomorphism.*

Therefore, the image of any group G under a homomorphism with kernel K is isomorphic to the quotient group $\frac{G}{K}$.

Thus, $\frac{G}{\ker(\phi)} \cong Im(\phi)$.

Theorem 230. ***Second Isomorphism Theorem***

Let H be a subgroup of G and let N be a normal subgroup of G.

Let $HN = \{hk : h \in H \wedge k \in N\}$.

Then $HN < G$ and $N \lhd HN$ and $H \cap N \lhd H$ and $\frac{H}{H \cap N} \cong \frac{HN}{N}$.