Group Theory

Jason Sass

July 24, 2023

Binary Operations

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

Proof. We prove 1.
Let $a, b \in S$.
Then $(a, b) \in S \times S$.
Since $*$ is a binary operation on S, then $* : S \times S \rightarrow S$ is a function.
Therefore, $x * y \in S$ for every $(x, y) \in S \times S$.
In particular, $a * b \in S$. $\square$

Proof. We prove 2.
Let $a, b, c, d \in S$ such that $a = c$ and $b = d$.
Since $a, b \in S$, then $(a, b) \in S \times S$.
Since $c, d \in S$, then $(c, d) \in S \times S$.
By definition of equality of ordered pairs, $(a, b) = (c, d)$ iff $a = c$ and $b = d$.
Therefore, $(a, b) = (c, d)$.
Since $*$ is a binary operation on S, then $* : S \times S \rightarrow S$ is a function.
Since every function is well defined, then for every $(w, x), (y, z) \in S \times S$ such that $(w, x) = (y, z)$, we have $w * x = y * z$.
Since, $(a, b) = (c, d)$, then we conclude $a * b = c * d$. $\square$

Proof. We prove 3.
Let $a, b, c \in S$ such that $a = b$.
Since equality is reflexive, then $x = x$ for every $x \in S$.
Since $c \in S$, then this implies $c = c$.
Thus, by statement 2, $c = c$ and $a = b$ imply $c * a = c * b$.
Since $c = c$ and $a = b$, then we conclude $c * a = c * b$. $\square$

Proof. We prove 4.

Let $a, b, c \in S$ such that $a = b$.

Since equality is reflexive, then $x = x$ for every $x \in S$.

Since $c \in S$, then this implies $c = c$.

Thus, by statement 2, $a = b$ and $c = c$ imply $a * c = b * c$.

Since $a = b$ and $c = c$, then we conclude $a * c = b * c$. $\square$

Proposition 2. *If a binary structure has an identity element, then the identity element is unique.*

Proof. Let $(S, *)$ be a binary structure with an identity element $e \in S$.

Since $e \in S$ is an identity element, then $e * a = a * e = a$ for every $a \in S$.

Suppose e' is an identity element of S.

Then $e' \in S$ and $e' * a = a * e' = a$ for every $a \in S$.

Since $e' \in S$ and $e * a = a * e = a$ for every $a \in S$, then in particular, $e * e' = e'$.

Since $e \in S$ and $e' * a = a * e' = a$ for every $a \in S$, then in particular, $e * e' = e$.

Hence, $e = e * e' = e'$, so $e = e'$.

Therefore, the identity element in S is unique. $\square$

Proposition 3. *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***

Proof. We prove 1.

Let e be the identity element of the set S.

Let a be an arbitrary invertible element of S.

Then $a \in S$.

Since a is invertible, then there exists $b \in S$ such that $ab = ba = e$.

Therefore, at least one inverse of a exists in S.

Suppose b' is an inverse of a.

Then $b \in S$ and $b'a = e$.

Observe that

$$\begin{aligned} b' &= b'e \\ &= b'(ab) \\ &= (b'a)b \\ &= eb \\ &= b. \end{aligned}$$

Hence, $b' = b$, so at most one inverse of a exists.

Since at least one inverse of a exists and at most one inverse of a exists, then exactly one inverse of a exists, so the inverse of a is unique.

Since a is arbitrary, then the inverse of every invertible element of S is unique. $\square$

Proof. We prove 2.

Let $a \in S$.

Suppose a is invertible.

Then there exists a unique $a^{-1} \in S$ such that $a * a^{-1} = a^{-1} * a = e$.

Since $a * a^{-1} = a^{-1} * a = e$, then $a^{-1} * a = a * a^{-1} = e$.

Hence, a is an inverse of a^{-1}, by definition of inverse element.

Thus, a^{-1} is invertible.

From statement 1, we know that the inverse of each invertible element of an associative binary structure with identity is unique, so the inverse of a^{-1} is unique.

Therefore, the inverse of a^{-1} must be a, so $(a^{-1})^{-1} = a$. $\square$

Proof. We prove 3.

Let $a, b \in S$.

Suppose a and b are invertible.

Then there exist unique $a^{-1} \in S$ and $b^{-1} \in S$ such that $a * a^{-1} = a^{-1} * a = e$ and $b * b^{-1} = b^{-1} * b = e$.

Since $(S, *)$ is a binary structure, then S is closed under $*$.

Since $a \in S$ and $b \in S$, then $a * b \in S$.

Since $a^{-1} \in S$ and $b^{-1} \in S$, then $b^{-1} * a^{-1} \in S$.

Observe that

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

and

$$\begin{aligned}
(b^{-1} * a^{-1}) * (a * b) &= b^{-1} * (a^{-1} * a) * b \\
&= b^{-1} * e * b \\
&= b^{-1} * b \\
&= e.
\end{aligned}$$

Hence, $b^{-1} * a^{-1}$ is an inverse of $a * b$, by definition of inverse element.

Thus, $a * b$ is invertible.

From statement 1, we know that the inverse of each invertible element of an associative binary structure with identity is unique, so the inverse of $a * b$ is unique.

Therefore, $b^{-1} * a^{-1}$ must be the inverse of $a * b$, so $(a * b)^{-1} = b^{-1} * a^{-1}$. $\square$

Proposition 4. *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.

Proof. Let e be a left identity of S.

Let $a, b, c \in S$ such that $ca = cb$.

Since e is a left identity and $a \in S$ and $b \in S$, then $a = ea$ and $b = eb$.

Since each element of S has a left inverse and $c \in S$, then then there exists $c' \in S$ such that $c'c = e$.

Observe that

$$\begin{aligned} a &= ea \\ &= (c'c)a \\ &= c'(ca) \\ &= c'(cb) \\ &= (c'c)b \\ &= eb \\ &= b. \end{aligned}$$

Therefore, $ca = cb$ implies $a = b$, so the left cancellation law holds. ☐

Proposition 5. *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.

Proof. Let e be a right identity of S.

Let $a, b, c \in S$ such that $ac = bc$.

Since e is a right identity and $a \in S$ and $b \in S$, then $a = ae$ and $b = be$.

Since each element of S has a right inverse and $c \in S$, then then there exists $c' \in S$ such that $cc' = e$.

Observe that

$$\begin{aligned} a &= ae \\ &= a(cc') \\ &= (ac)c' \\ &= (bc)c' \\ &= b(cc') \\ &= be \\ &= b. \end{aligned}$$

Therefore, $ac = bc$ implies $a = b$, so the right cancellation law holds. ☐

Proposition 6. *If a binary structure has a zero element, then the zero element is unique.*

Proof. Let $(S, *)$ be a binary structure with a zero element.

Let z be a zero element of S.

Then $z \in S$ and $zx = xz = z$ for all $x \in S$.

Suppose z' is a zero element of S.

Then $z' \in S$ and $z'x = xz' = z'$ for all $x \in S$.

Since $z \in S$ and $z'x = xz' = z'$ for all $x \in S$, then we conclude $zz' = z'$.

Since $z' \in S$ and $zx = xz = z$ for all $x \in S$, then we conclude $zz' = z$.

Therefore, $z = zz' = z'$, so $z = z'$.

Therefore, at most one zero element exists in S.

Since at least one zero element exists in S and at most one zero element exists in S, then exactly one zero element exists in S.

Therefore, the zero element in S is unique. $\square$

Groups

Theorem 7. ***Uniqueness of group identity***

The identity element of a group is unique.

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

Then there exists an identity element for $*$ in G.

Let e be an identity element of G.

Since $(G, *)$ is a group, then G is a set with a binary operation $*$ defined on G, so $(G, *)$ is a binary structure.

Thus, $(G, *)$ is a binary structure with identity e.

If a binary structure has an identity element, then the identity element is unique, by proposition 2

Therefore, we conclude the identity element is unique, so e is unique. $\square$

Theorem 8. ***Uniqueness of group inverses***

The inverse of each element in a group is unique.

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

Let a be an arbitrary element of G.

Since each element of G has an inverse in G, then in particular, a has an inverse in G, so a is invertible.

Let b be an inverse of a in G.

Since $(G, *)$ is a group, then $(G, *)$ is an associative binary structure with identity.

The inverse of every invertible element of an associative binary structure with identity is unique, by proposition 3.

Hence, the inverse of every invertible element of $(G, \cdot)$ is unique.

Since a is an invertible element of G, then we conclude the inverse of a is unique, so b is unique. $\square$

Proposition 9. *The identity element in a group is its own inverse.*

Proof. Let $(G, *)$ be a group with identity $e \in G$.

Since G is a group and $e \in G$, then e has an inverse in G.

Let $e^{-1} \in G$ be the inverse of e.

Then by definition of inverse, $ee^{-1} = e$.

Since $e = ee^{-1} = e^{-1}$, then $e = e^{-1}$.

Therefore, e is the inverse of e. □

Theorem 10. ***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***

Proof. We prove 1.

Let $a \in G$.

Each element in a group has an inverse, by definition of group.

Hence, a has an inverse $a^{-1} \in G$, so a is invertible.

Since $(G, *)$ is a group, then $(G, *)$ is an associative binary structure with identity.

Since $(G, *)$ is an associative binary structure with identity and a is invertible, then by proposition 3, we conclude $(a^{-1})^{-1} = a$. □

Proof. We prove 2.

Let $a, b \in G$.

Since $(G, *)$ is a group, then $(G, *)$ is an associative binary structure with identity.

By definition of a group, every element of G is invertible, so a is invertible and b is invertible.

Since $(G, *)$ is an associative binary structure with identity and a is invertible and b is invertible, then by proposition 3, we conclude $(a * b)^{-1} = b^{-1} * a^{-1}$. □

Proposition 11. ***inverse of a finite product***

Let $g_1, g_2, ..., g_n$ be elements of a group $(G, *)$.

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

Proof. To prove $(g_1 g_2 ... g_n)^{-1} = g_n^{-1} g_{n-1}^{-1} ... g_2^{-1} g_1^{-1}$ for all $n \in \mathbb{Z}^+$, let $S_n : (g_1 g_2 ... g_n)^{-1} = g_n^{-1} g_{n-1}^{-1} ... g_2^{-1} g_1^{-1}$.

We must prove

1. S_n is true for all $n \in \mathbb{Z}^+$.

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

Basis:

Since $(g_1)^{-1} = g_1^{-1}$, then S_1 is true.

Induction:

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

Then $(g_1 g_2 ... g_k)^{-1} = g_k^{-1} g_{k-1}^{-1} ... g_2^{-1} g_1^{-1}$.

Observe that

$$\begin{aligned}(g_1 g_2 ... g_k g_{k+1})^{-1} &= [(g_1 g_2 ... g_k) g_{k+1}]^{-1} \\ &= g_{k+1}^{-1} * (g_1 g_2 ... g_k)^{-1} \\ &= g_{k+1}^{-1} * (g_k^{-1} g_{k-1}^{-1} * ... * g_2^{-1} g_1^{-1}) \\ &= g_{k+1}^{-1} * g_k^{-1} * g_{k-1}^{-1} * ... * g_2^{-1} * g_1^{-1}.\end{aligned}$$

Therefore, $(g_1 g_2 ... g_k g_{k+1})^{-1} = g_{k+1}^{-1} * g_k^{-1} * g_{k-1}^{-1} ... * g_2^{-1} g_1^{-1}$, so S_{k+1} is true.

Hence, S_k implies S_{k+1} for all $k \in \mathbb{Z}^+$.

Since S_1 is true and S_k implies S_{k+1} for all $k \in \mathbb{Z}^+$, then by induction, S_n is true for all $n \in \mathbb{Z}^+$. ☐

Theorem 12. ***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)***

Proof. We prove the left cancellation law holds in a group.

Since $(G, *)$ is a group, then $*$ is a binary operation on G and $*$ is associative, so $(G, *)$ is an associative binary structure.

Since $(G, *)$ is a group, then an identity element exists in G.

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

Then $e * a = a * e = a$ for all $a \in G$, so $e * a = a$ for all $a \in G$.

Hence, e is a left identity with respect to $*$, so $(G, *)$ has a left identity.

Let $a \in G$ be arbitrary.

By definition of a group, a has an inverse in G, so there exists $b \in G$ such that $a * b = b * a = e$.

Hence, there exists $b \in G$ such that $b * a = e$, so b is a left inverse of a.

Thus, a has a left inverse.

Since a is arbitrary, then each element of G has a left inverse.

Since $(G, *)$ is an associative binary structure and $(G, *)$ has a left identity and each element of G has a left inverse, then by proposition 4, we conclude the left cancellation law holds in $(G, *)$. ☐

Proof. We prove the right cancellation law holds in a group.

Since $(G, *)$ is a group, then $*$ is a binary operation on G and $*$ is associative, so $(G, *)$ is an associative binary structure.

Since $(G, *)$ is a group, then an identity element exists in G.

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

Then $e * a = a * e = a$ for all $a \in G$, so $a * e = a$ for all $a \in G$.

Hence, e is a right identity with respect to $*$, so $(G, *)$ has a right identity.

Let $a \in G$ be arbitrary.

By definition of a group, a has an inverse in G, so there exists $b \in G$ such that $a * b = b * a = e$.

Hence, there exists $b \in G$ such that $a * b = e$, so b is a right inverse of a.

Thus, a has a right inverse.

Since a is arbitrary, then each element of G has a right inverse.

Since $(G, *)$ is an associative binary structure and $(G, *)$ has a right identity and each element of G has a right inverse, then by proposition 5, we conclude the right cancellation law holds in $(G, *)$. $\square$

Corollary 13. ***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.

Proof. We prove a solution to the linear equation $a * x = b$ is unique.

Let $a, b \in G$.

Since G is a group, then the inverse of a exists in G, so $a^{-1} \in G$.

Existence:

Let $x = a^{-1} * b$.

Since G is closed under $*$, then $a^{-1} * b \in G$, so $x \in G$.

Observe that $a * (a^{-1} * b) = (a * a^{-1}) * b = e * b = b$.

Hence, $a^{-1} * b \in G$ is a solution to the equation $a * x = b$.

Therefore, at least one solution exists.

Uniqueness:

Suppose $x_1, x_2 \in G$ are solutions to the equation $a * x = b$.

Then $a * x_1 = b$ and $a * x_2 = b$, so $b = a * x_1 = a * x_2$.

By the left cancellation law for groups we obtain $x_1 = x_2$.

Therefore, at most one solution exists.

Since at least one solution exists and at most one solution exists, then exactly one solution exists.

Therefore, a solution to the equation $a * x = b$ is unique. $\square$

Proof. We prove a solution to the linear equation $x * a = b$ is unique.

Let $a, b \in G$.

Since G is a group, then the inverse of a exists in G, so $a^{-1} \in G$.

Existence:

Let $x = b * a^{-1}$.

Since G is closed under $*$, then $b * a^{-1} \in G$, so $x \in G$.

Observe that $(b * a^{-1}) * a = b * (a^{-1} * a) = b * e = b$.

Hence, $b * a^{-1} \in G$ is a solution to the equation $x * a = b$.

Therefore, at least one solution exists.

Uniqueness:

Suppose $x_1, x_2 \in G$ are solutions to the equation $x * a = b$.
Then $x_1 * a = b$ and $x_2 * a = b$, so $b = x_1 * a = x_2 * a$.
By the right cancellation law for groups we obtain $x_1 = x_2$.
Therefore, at most one solution exists.

Since at least one solution exists and at most one solution exists, then exactly one solution exists.

Therefore, a solution to the equation $x * a = b$ is unique. □

Proposition 14. *A group has exactly one idempotent element, the identity element.*

Proof. Let $(G, *)$ be a group with identity $e \in G$.

Existence:

Then $e * e = e$, by definition of identity element.
Hence, e is an idempotent element, by definition of idempotent element.
Thus, there is at least one idempotent element in G.

Uniqueness:

Suppose x is an idempotent element of G.
Then $x * x = x = x * e$.
By the left cancellation law for groups we obtain $x = e$.
Therefore, there is at most one idempotent element in G.

Since there is at least one idempotent element in G and there is at most one idempotent element in G, then there is exactly one idempotent element in G. □

Proposition 15. ***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 $*$.
$(\forall a \in G)(\exists b \in G)(b * a = e)$.

Proof. Let G be a set with a binary operation $*$ defined on G such that $*$ is associative and there is a left identity element for $*$ and each element has a left inverse.

Since G is a set and $*$ is a binary operation on G and $*$ is associative, then G is an associative binary structure, so G is an associative binary structure with a left identity and each element has a left inverse.

Let e be a left identity of G.

Let $a \in G$.

Since e is a left identity, then $e \in G$ and $ex = x$ for all $x \in G$.

In particular, $ea = a$ and $ee = e$.

Since $a \in G$ and each element of G has a left inverse, then there exists $a' \in G$ such that $a'a = e$.

Observe that

$$\begin{aligned} a'a &= e \\ &= ee \\ &= (a'a)e \\ &= a'(ae). \end{aligned}$$

Thus, $a'a = a'(ae)$.

Since G is an associative binary structure with a left identity and each element has a left inverse, then by proposition 4, the left cancellation law holds.

Therefore, $a = ae$.

Hence, $ea = a = ae$.

Since a is arbitrary, then $ea = ae = a$ for all $a \in G$, so e is an identity for $*$.

Since e is an identity for $*$, then $ex = xe = x$ for all $x \in G$.

Since $a' \in G$, then we conclude $ea' = a'e = a'$.

Observe that

$$\begin{aligned} a'e &= a' \\ &= ea' \\ &= (a'a)a' \\ &= a'(aa'). \end{aligned}$$

Thus, $a'e = a'(aa')$.

By the left cancellation law, we have $e = aa'$.

Hence, $a'a = e = aa'$.

Since $a' \in G$ and $aa' = a'a = e$, then a' is an inverse of a, so a has an inverse for $*$.

Since a is arbitrary, then every element of G has an inverse for $*$.

Since $*$ is a binary operation on G and $*$ is associative and e is an identity element for $*$ and every element of G has an inverse for $*$, then by definition of group, $(G, *)$ is a group. $\square$

Proposition 16. ***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 $*$.
$(\forall a \in G)(\exists b \in G)(a * b = e)$.

Proof. Let G be a set with a binary operation $*$ defined on G such that $*$ is associative and there is a right identity element for $*$ and each element has a right inverse.

Since G is a set and $*$ is a binary operation on G and $*$ is associative, then G is an associative binary structure, G is an associative binary structure with a right identity and each element has a right inverse.

Let e be a right identity of G.

Let $a \in G$.

Since e is a right identity, then $e \in G$ and $xe = x$ for all $x \in G$.

In particular, $ae = a$ and $ee = e$.

Since $a \in G$ and each element of G has a right inverse, then there exists $a' \in G$ such that $aa' = e$.

Observe that

$$\begin{aligned} aa' &= e \\ &= ee \\ &= e(aa') \\ &= (ea)a'. \end{aligned}$$

Thus, $aa' = (ea)a'$.

Since G is an associative binary structure with a right identity and each element has a right inverse, then by proposition 5, the right cancellation law holds.

Therefore, $a = ea$.

Hence, $ae = a = ea$.

Since a is arbitrary, then $ea = ae = a$ for all $a \in G$, so e is an identity for $*$.

Since e is an identity for $*$, then $ex = xe = x$ for all $x \in G$.

Since $a' \in G$, then we conclude $ea' = a'e = a'$.

Observe that

$$\begin{aligned} ea' &= a' \\ &= a'e \\ &= a'(aa') \\ &= (a'a)a'. \end{aligned}$$

Thus, $ea' = (a'a)a'$.

By the right cancellation law, we have $e = a'a$.

Hence, $aa' = e = a'a$.

Since $a' \in G$ and $aa' = a'a = e$, then a' is an inverse of a, so a has an inverse for $*$.

Since a is arbitrary, then every element of G has an inverse for $*$.

Since $*$ is a binary operation on G and $*$ is associative and e is an identity element for $*$ and every element has an inverse for $*$, then by definition of group, $(G, *)$ is a group. ☐

multiplicative group notation

Lemma 17. *Let $(G, \cdot)$ be a multiplicative group.*

Let $a \in G$.

Then $a^n \cdot a = a \cdot a^n$ for all $n \in \mathbb{Z}^+$.

Proof. To prove $a^n \cdot a = a \cdot a^n$ for all $n \in \mathbb{Z}^+$, let $S_n : a^n \cdot a = a \cdot a^n$.

We must prove

1. S_n is true for all $n \in \mathbb{Z}^+$.

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

Basis:

Observe that

$$\begin{aligned}
a^1 \cdot a &= (a^{1-1} \cdot a) \cdot a \\
&= (a^0 \cdot a) \cdot a \\
&= (a^0 \cdot a) \cdot (e \cdot a) \\
&= (a^0 \cdot a) \cdot (a^0 \cdot a) \\
&= (e \cdot a) \cdot (a^{1-1} \cdot a) \\
&= a \cdot a^1.
\end{aligned}$$

Therefore, $a^1 \cdot a = a \cdot a^1$, so S_1 is true.

Induction:

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

Then $a^k \cdot a = a \cdot a^k$ and $k > 0$, so $k + 1 > 0$.

Observe that

$$\begin{aligned}
a^{k+1} \cdot a &= (a^k \cdot a) \cdot a \\
&= (a \cdot a^k) \cdot a \\
&= a \cdot (a^k \cdot a) \\
&= a \cdot a^{k+1}.
\end{aligned}$$

Hence, $a^{k+1} \cdot a = a \cdot a^{k+1}$, so S_{k+1} is true.

Thus, S_k implies S_{k+1} for all $k \in \mathbb{Z}^+$.

Since S_1 is true and S_k implies S_{k+1} for all $k \in \mathbb{Z}^+$, then by induction, S_n is true for all $n \in \mathbb{Z}^+$. ☐

Theorem 18. ***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 $n \in \mathbb{Z}$.

Proof. We prove 1.

If $a \in G$, then $a^{-n} = (a^{-1})^n = (a^n)^{-1}$ for all $n \in \mathbb{Z}^+$.

Let $a \in G$ be arbitrary.

To prove $a^{-n} = (a^{-1})^n = (a^n)^{-1}$ for all $n \in \mathbb{Z}^+$, let $n \in \mathbb{Z}^+$.

Then $n \in \mathbb{Z}$ and $n > 0$, so $a^{-n} = (a^{-1})^n$.

Since $n \in \mathbb{Z}^+$, then $(a^{-1})^n$ is a product of a^{-1} with itself n times.

Hence, $(a^{-1})^n = (a^{-1}) \cdot (a^{-1}) \cdot ... \cdot (a^{-1})$.

The expression $(a^{-1}) \cdot (a^{-1}) \cdot ... \cdot (a^{-1})$ is the same as the inverse of the product of a with itself n times, by proposition 11 .

Thus, $(a^{-1}) \cdot (a^{-1}) \cdot ... \cdot (a^{-1}) = (a \cdot a ... \cdot a)^{-1} = (a^n)^{-1}$.

Hence, $(a^{-1})^n = (a^{-1}) \cdot (a^{-1}) \cdot ... \cdot (a^{-1}) = (a \cdot a ... \cdot a)^{-1} = (a^n)^{-1}$, so $(a^{-1})^n = (a^n)^{-1}$.

Therefore, $a^{-n} = (a^{-1})^n$ and $(a^{-1})^n = (a^n)^{-1}$, so $a^{-n} = (a^{-1})^n = (a^n)^{-1}$. □

Proof. We prove 2.

If $a \in G$, then $a^n \in G$ for all $n \in \mathbb{Z}$.

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

Let $a \in G$ be arbitrary.

To prove $a^n \in G$ for all $n \in \mathbb{Z}$, let $S_n : a^n \in G$ and let $T_n : a^{-n} \in G$.

We must prove

1. $a^0 \in G$.
2. S_n is true for all $n \in \mathbb{Z}^+$.
3. T_n is true for all $n \in \mathbb{Z}^+$. □

Proof. We first prove $a^0 \in G$.

Since $a^0 = e$ and $e \in G$, then $a^0 \in G$. □

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

Basis:

Since $a \in G$ and $a^1 = a^{1-1} \cdot a = a^0 \cdot a = e \cdot a = a$, then $a^1 \in G$, so S_1 is true.

Induction:

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

Since $k \in \mathbb{Z}^+$, then $k > 0$, so $k + 1 > 0$.

Since S_k is true, then $a^k \in G$.

Since $a^{k+1} = a^k \cdot a$ and $a^k \in G$ and $a \in G$, then by closure of G under $\cdot$, the product a^{k+1} is an element of G, so $a^{k+1} \in G$.

Therefore, S_{k+1} is true.

Thus, S_k implies S_{k+1} for all $k \in \mathbb{Z}^+$.

Since S_1 is true and S_k implies S_{k+1} for all $k \in \mathbb{Z}^+$, then by induction, S_n is true for all $n \in \mathbb{Z}^+$. $\square$

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

Basis:

Since $a \in G$ and every element in G is invertible by definition of a group, then its inverse a^{-1} is in G, so $a^{-1} \in G$.

Therefore, T_1 is true.

Induction:

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

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

Since $k > 0$, then $a^{-k} = (a^{-1})^k$.

Since T_k is true, then $a^{-k} \in G$.

Observe that

$$\begin{aligned} a^{-(k+1)} &= (a^{-1})^{(k+1)} \\ &= (a^{-1})^k \cdot (a^{-1}) \\ &= (a^{-k}) \cdot (a^{-1}). \end{aligned}$$

Since $a^{-k} \in G$ and $a^{-1} \in G$, then by closure of G under $\cdot$, we have $a^{-k} \cdot a^{-1} \in G$, so $a^{-(k+1)} \in G$.

Therefore, T_{k+1} is true.

Thus, T_k implies T_{k+1} for all $k \in \mathbb{Z}^+$.

Since T_1 is true and T_k implies T_{k+1} for all $k \in \mathbb{Z}^+$, then by induction, T_n is true for all $n \in \mathbb{Z}^+$. $\square$

Proof. We prove 3.

If $a \in G$, then $a^m \cdot a^n = a^{m+n}$ for all $m, n \in \mathbb{Z}$.

Let $a \in G$ be arbitrary.

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

To prove $a^m \cdot a^n = a^{m+n}$ for all $n \in \mathbb{Z}$, let $S_n : a^m \cdot a^n = a^{m+n}$ and let $T_n : a^m \cdot a^{-n} = a^{m-n}$.

We must prove

1. $a^m \cdot a^0 = a^{m+0}$.
2. S_n is true for all $n \in \mathbb{Z}^+$.
3. T_n is true for all $n \in \mathbb{Z}^+$. $\square$

Proof. We prove $a^m \cdot a^0 = a^{m+0}$.

Since $a^{m+0} = a^m = a^m \cdot e = a^m \cdot a^0$, then $a^m \cdot a^0 = a^{m+0}$. $\square$

Proof. We prove T_1 is true.

Basis:

Either $m - 1 > 0$ or $m - 1 = 0$ or $m - 1 < 0$.

We consider these cases separately.

Case 1: Suppose $m - 1 > 0$.

Then $m > 1$, so $m > 0$.

Since $a^m \cdot a^{-1} = (a^{m-1} \cdot a) \cdot a^{-1} = a^{m-1} \cdot (a \cdot a^{-1}) = a^{m-1} \cdot e = a^{m-1}$, then $a^m \cdot a^{-1} = a^{m-1}$.

Therefore, T_1 is true.

Case 2: Suppose $m - 1 = 0$.

Then $m = 1$.

Since $a^m \cdot a^{-1} = a^1 \cdot a^{-1} = a \cdot a^{-1} = e = a^0 = a^{m-1}$, then $a^m \cdot a^{-1} = a^{m-1}$.

Therefore, T_1 is true.

Case 3: Suppose $m - 1 < 0$.

Then $m < 1$.

We must prove $a^m \cdot a^{-1} = a^{m-1}$ for all integers $m < 1$.

The statement $a^m \cdot a^{-1} = a^{m-1}$ for all integers $m < -1$ is equivalent to the statement $a^m \cdot a^{-1} = a^{m-1}$ for all integers $m \leq -2$ which is equivalent to the statement $a^{-k} \cdot a^{-1} = a^{-k-1}$ for all integers $k \geq 2$.

So, to prove the statement $a^m \cdot a^{-1} = a^{m-1}$ for all integers $m < -1$, we prove the equivalent statement $a^{-k} \cdot a^{-1} = a^{-k-1}$ for all integers $k \geq 2$.

Let $k \in \mathbb{Z}$ and $k \geq 2$.

Since $k \geq 2$ and $2 > 0$, then $k > 0$.

Since $k > 0$ and $1 > 0$, we add to obtain $k + 1 > 0$.

Observe that

$$\begin{aligned}
a^{-k} \cdot a^{-1} &= (a^k)^{-1} \cdot a^{-1} \\
&= (a \cdot a^k)^{-1} \\
&= (a^k \cdot a)^{-1} \\
&= (a^{k+1})^{-1} \\
&= a^{-(k+1)} \\
&= a^{-k-1}.
\end{aligned}$$

Hence, $a^{-k} \cdot a^{-1} = a^{-k-1}$, so $a^m \cdot a^{-1} = a^{m-1}$ for all integers $m < -1$.

Therefore, T_1 is true.

In all cases, T_1 is true.

Therefore, $a^m \cdot a^{-1} = a^{m-1}$ for all $m \in \mathbb{Z}$. $\square$

Proof. **Induction:**

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

Since $k \in \mathbb{Z}^+$, then $k > 0$, so $k + 1 > 0$.

Since T_k is true, then $a^m \cdot a^{-k} = a^{m-k}$.

Either $m - k - 1 > 0$ or $m - k - 1 = 0$ or $m - k - 1 < 0$.

We consider these cases separately.

Case 1: Suppose $m - k - 1 > 0$.

Then $m - k > 1$, so $m - k > 0$.

Observe that

$$\begin{aligned}
a^m \cdot a^{-(k+1)} &= a^m \cdot (a^{-1})^{k+1} \\
&= a^m \cdot ((a^{-1})^k \cdot a^{-1}) \\
&= a^m \cdot (a^{-k} \cdot a^{-1}) \\
&= (a^m \cdot a^{-k}) \cdot a^{-1} \\
&= a^{m-k} \cdot a^{-1} \\
&= (a^{m-k-1} \cdot a) \cdot a^{-1} \\
&= a^{m-k-1} \cdot (a \cdot a^{-1}) \\
&= a^{m-k-1} \cdot e \\
&= a^{m-k-1} \\
&= a^{m-(k+1)}.
\end{aligned}$$

Thus, $a^m \cdot a^{-(k+1)} = a^{m-(k+1)}$.
Therefore, T_{k+1} is true.
Case 2: Suppose $m - k - 1 = 0$.
Then $m - k = 1$.
Observe that

$$\begin{aligned}
a^m \cdot a^{-(k+1)} &= a^m \cdot (a^{-1})^{k+1} \\
&= a^m \cdot ((a^{-1})^k \cdot a^{-1}) \\
&= a^m \cdot (a^{-k} \cdot a^{-1}) \\
&= (a^m \cdot a^{-k}) \cdot a^{-1} \\
&= a^{m-k} \cdot a^{-1} \\
&= a^1 \cdot a^{-1} \\
&= a \cdot a^{-1} \\
&= e \\
&= a^0 \\
&= a^{m-k-1} \\
&= a^{m-(k+1)}.
\end{aligned}$$

Thus, $a^m \cdot a^{-(k+1)} = a^{m-(k+1)}$.
Therefore, T_{k+1} is true.
Case 3: Suppose $m - k - 1 < 0$.

Observe that

$$\begin{aligned} a^m \cdot a^{-(k+1)} &= a^m \cdot (a^{-1})^{k+1} \\ &= a^m \cdot ((a^{-1})^k \cdot a^{-1}) \\ &= a^m \cdot (a^{-k} \cdot a^{-1}) \\ &= (a^m \cdot a^{-k}) \cdot a^{-1} \\ &= a^{m-k} \cdot a^{-1} \\ &= a^{m-k-1} \\ &= a^{m-(k+1)}. \end{aligned}$$

Thus, $a^m \cdot a^{-(k+1)} = a^{m-(k+1)}$.

Therefore, T_{k+1} is true.

In all cases, T_{k+1} is true.

Hence, T_k implies T_{k+1} for all $k \in \mathbb{Z}^+$.

Since T_1 is true and T_k implies T_{k+1} for all $k \in \mathbb{Z}^+$, then by induction, T_n is true for all $n \in \mathbb{Z}^+$. $\square$

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

Basis:

Either $m+1 > 0$ or $m+1 = 0$ or $m+1 < 0$.

We consider these cases separately.

Case 1: Suppose $m+1 > 0$.

Since $a^m \cdot a^1 = a^m \cdot a = a^{m+1-1} \cdot a = a^{m+1}$, then $a^m \cdot a^1 = a^{m+1}$.

Therefore, S_1 is true.

Case 2: Suppose $m+1 = 0$.

Then $m = -1$.

Since $a^m \cdot a^1 = a^{-1} \cdot a^1 = a^{-1} \cdot a = e = a^0 = a^{m+1}$, then $a^m \cdot a^1 = a^{m+1}$.

Therefore, S_1 is true.

Case 3: Suppose $m+1 < 0$.

Then $m < -1$.

We must prove $a^m \cdot a^1 = a^{m+1}$ for all integers $m < -1$.

The statement $a^m \cdot a^1 = a^{m+1}$ for all integers $m < -1$ is equivalent to the statement $a^m \cdot a^1 = a^{m+1}$ for all integers $m \leq -2$ which is equivalent to the statement $a^{-k} \cdot a^1 = a^{-k+1}$ for all integers $k \geq 2$.

So, to prove the statement $a^m \cdot a^1 = a^{m+1}$ for all integers $m < -1$, we prove the equivalent statement $a^{-k} \cdot a^1 = a^{-k+1}$ for all integers $k \geq 2$.

Let $k \in \mathbb{Z}$ and $k \geq 2$.

Since $k \geq 2$ and $2 > 0$, then $k > 0$.

Since $k \geq 2$, then $k - 1 \geq 1$, so $k - 1 > 0$.

Observe that

$$\begin{aligned}
a^{-k} \cdot a^1 &= a^{-k} \cdot a \\
&= (a^{-1})^k \cdot a \\
&= [(a^{-1})^{k-1} \cdot a^{-1}] \cdot a \\
&= (a^{-1})^{k-1} \cdot (a^{-1} \cdot a) \\
&= (a^{-1})^{k-1} \cdot e \\
&= (a^{-1})^{k-1} \\
&= a^{-(k-1)} \\
&= a^{-k+1}.
\end{aligned}$$

Hence, $a^{-k} \cdot a^1 = a^{-k+1}$, so $a^m \cdot a^1 = a^{m+1}$ for all integers $m < -1$.
Therefore, S_1 is true.

In all cases, S_1 is true. □

Proof. **Induction:**
Let $k \in \mathbb{Z}^+$ such that S_k is true.
Since $k \in \mathbb{Z}^+$, then $k > 0$.
Since S_k is true, then $a^m \cdot a^k = a^{m+k}$.
Either $m + k + 1 > 0$ or $m + k + 1 = 0$ or $m + k + 1 < 0$.
We consider these cases separately.
Case 1: Suppose $m + k + 1 > 0$.
Observe that

$$\begin{aligned}
a^m \cdot a^{k+1} &= a^m \cdot (a^k \cdot a) \\
&= (a^m \cdot a^k) \cdot a \\
&= a^{m+k} \cdot a \\
&= a^{m+k+1-1} \cdot a \\
&= a^{m+k+1} \\
&= a^{m+(k+1)}.
\end{aligned}$$

Thus, $a^m \cdot a^{k+1} = a^{m+(k+1)}$.
Therefore, S_{k+1} is true.
Case 2: Suppose $m + k + 1 = 0$.
Then $m + k = -1$.

Observe that

$$\begin{aligned} a^m \cdot a^{k+1} &= a^m \cdot (a^k \cdot a) \\ &= (a^m \cdot a^k) \cdot a \\ &= a^{m+k} \cdot a \\ &= a^{-1} \cdot a \\ &= e \\ &= a^0 \\ &= a^{m+k+1} \\ &= a^{m+(k+1)}. \end{aligned}$$

Thus, $a^m \cdot a^{k+1} = a^{m+(k+1)}$.
Therefore, S_{k+1} is true.
Case 3: Suppose $m + k + 1 < 0$.
Then $m + k < -1$.
Since S_1 is true, then $a^m \cdot a^1 = a^{m+1}$ for all integers $m < -1$.
Hence, $a^{m+k} \cdot a^1 = a^{(m+k)+1}$.
Observe that

$$\begin{aligned} a^m \cdot a^{k+1} &= a^m \cdot (a^k \cdot a) \\ &= (a^m \cdot a^k) \cdot a \\ &= a^{m+k} \cdot a \\ &= a^{m+k} \cdot a^1 \\ &= a^{(m+k)+1} \\ &= a^{m+(k+1)}. \end{aligned}$$

Thus, $a^m \cdot a^{k+1} = a^{m+(k+1)}$.
Therefore, S_{k+1} is true.

In all cases, S_{k+1} is true.
Hence, S_k implies S_{k+1} for all $k \in \mathbb{Z}^+$.
Since S_1 is true and S_k implies S_{k+1} for all $k \in \mathbb{Z}^+$, then by induction, S_n is true for all $n \in \mathbb{Z}^+$. □

Proof. We prove 4.
If $a \in G$, then $(a^m)^n = a^{mn}$ for all $m, n \in \mathbb{Z}$.
Let $a \in G$.
Let $m \in \mathbb{Z}$.
To prove $(a^m)^n = a^{mn}$ for all $n \in \mathbb{Z}$, let $S_n : (a^m)^n = a^{mn}$ and let $T_n : (a^m)^{-n} = a^{m(-n)}$.
We must prove
1. $(a^m)^0 = a^{m0}$.
2. S_n is true for all $n \in \mathbb{Z}^+$.
3. T_n is true for all $n \in \mathbb{Z}^+$. □

Proof. We prove $(a^m)^0 = a^{m0}$.

Since $a \in G$ and $m \in \mathbb{Z}$, then $a^m \in G$, so $(a^m)^0 = e = a^0 = a^{m \cdot 0}$.

Therefore, $(a^m)^0 = a^{m0}$. $\square$

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

Basis:

Since $(a^m)^1 = a^m = a^{m1}$, then $(a^m)^1 = a^{m1}$, so S_1 is true.

Induction:

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

Then $(a^m)^k = a^{mk}$.

Observe that

$$\begin{array}{rcl} (a^m)^{k+1} & = & (a^m)^k \cdot a^m \\ & = & a^{mk} \cdot a^m \\ & = & a^{mk+m} \\ & = & a^{m(k+1)}. \end{array}$$

Thus, $(a^m)^{k+1} = a^{m(k+1)}$, so S_{k+1} is true.

Therefore, S_k implies S_{k+1} for all $k \in \mathbb{Z}^+$.

Since S_1 is true and S_k implies S_{k+1} for all $k \in \mathbb{Z}^+$, then by induction, S_n is true for all $n \in \mathbb{Z}^+$. $\square$

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

Basis:

Since $m \in \mathbb{Z}$, then either $m > 0$ or $m = 0$ or $m < 0$.

We consider these cases separately.

Case 1: Suppose $m > 0$.

Then $(a^m)^{-1} = a^{-m} = a^{m(-1)}$, so $(a^m)^{-1} = a^{m(-1)}$.

Therefore, T_1 is true.

Case 2: Suppose $m = 0$.

Then $(a^m)^{-1} = (a^0)^{-1} = e^{-1} = e = a^0 = a^{0(-1)} = a^{m(-1)}$, so $(a^m)^{-1} = a^{m(-1)}$.

Therefore, T_1 is true.

Case 3: Suppose $m < 0$.

Then $-m > 0$, so $a^{-(-m)} = (a^{-m})^{-1}$.

Observe that

$$\begin{array}{rcl} (a^m)^{-1} & = & [a^{-(-m)}]^{-1} \\ & = & [(a^{-m})^{-1}]^{-1} \\ & = & a^{-m} \\ & = & a^{m(-1)}. \end{array}$$

Thus, $(a^m)^{-1} = a^{m(-1)}$, so T_1 is true.

In all cases, T_1 is true.

Therefore, $(a^m)^{-1} = a^{m(-1)}$ for all $m \in \mathbb{Z}$.

Induction:

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

Then $(a^m)^{-k} = a^{m(-k)}$.

Observe that

$$\begin{aligned}
(a^m)^{-(k+1)} &= (a^m)^{(k+1)(-1)} \\
&= [(a^m)^{k+1}]^{-1} \\
&= [(a^m)^k \cdot a^m]^{-1} \\
&= (a^m)^{-1} \cdot [(a^m)^k]^{-1} \\
&= (a^m)^{-1} \cdot (a^m)^{k(-1)} \\
&= (a^m)^{-1} \cdot (a^m)^{-k} \\
&= (a^m)^{-1} \cdot a^{m(-k)} \\
&= a^{m(-1)} \cdot a^{m(-k)} \\
&= a^{-m} \cdot a^{-mk} \\
&= a^{-m-mk} \\
&= a^{-m(1+k)} \\
&= a^{-m(k+1)}.
\end{aligned}$$

Thus, $(a^m)^{-(k+1)} = a^{-m(k+1)}$, so T_{k+1} is true.

Therefore, T_k implies T_{k+1} for all $k \in \mathbb{Z}^+$.

Since T_1 is true and T_k implies T_{k+1} for all $k \in \mathbb{Z}^+$, then by induction, T_n is true for all $n \in \mathbb{Z}^+$. □

Proof. We prove 5.

If $a, b \in G$ and G is abelian, then $(ab)^n = a^n b^n$ for all $n \in \mathbb{Z}$.

Suppose $a, b \in G$ and G is abelian.

To prove $(ab)^n = a^n b^n$ for all $n \in \mathbb{Z}$, let $S_n : (ab)^n = a^n b^n$ and let $T_n : (ab)^{-n} = a^{-n} b^{-n}$.

We must prove

1. $(ab)^0 = a^0 b^0$.
2. S_n is true for all $n \in \mathbb{Z}^+$.
3. T_n is true for all $n \in \mathbb{Z}^+$. □

Proof. We prove $(ab)^0 = a^0 b^0$.

Since $a \in G$ and $b \in G$, then by closure of G under $\cdot$, we have $ab \in G$.

Therefore, $(ab)^0 = e = ee = a^0 b^0$, so $(ab)^0 = a^0 b^0$, as desired. □

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

Basis:

Since $(ab)^1 = ab = a^1 b^1$, then $(ab)^1 = a^1 b^1$, so S_1 is true.

Induction:

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

Since $k \in \mathbb{Z}^+$, then $k \in \mathbb{Z}$ and $k > 0$.
Since S_k is true, then $(ab)^k = a^k b^k$.
Observe that

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

Therefore, $(ab)^{k+1} = a^{k+1}b^{k+1}$, so S_{k+1} is true.
Hence, S_k implies S_{k+1} for all $k \in \mathbb{Z}^+$.
Since S_1 is true and S_k implies S_{k+1} for all $k \in \mathbb{Z}^+$, then by induction, S_n is true for all $n \in \mathbb{Z}^+$. □

Proof. We prove T_n is true for all $n \in \mathbb{Z}^+$ by induction on n.
Basis:
Since $(ab)^{-1} = b^{-1}a^{-1} = a^{-1}b^{-1}$, then $(ab)^{-1} = a^{-1}b^{-1}$, so T_1 is true.
Induction:
Let $k \in \mathbb{Z}^+$ such that T_k is true.
Since $k \in \mathbb{Z}^+$, then $k \in \mathbb{Z}$ and $k > 0$.
Since T_k is true, then $(ab)^{-k} = a^{-k}b^{-k}$.
Observe that

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

Hence, $(ab)^{-(k+1)} = a^{-(k+1)}b^{-(k+1)}$, so T_{k+1} is true.
Therefore, T_k implies T_{k+1} for all $k \in \mathbb{Z}^+$.
Since T_1 is true and T_k implies T_{k+1} for all $k \in \mathbb{Z}^+$, then by induction, T_n is true for all $n \in \mathbb{Z}^+$ □

Proposition 19. *Let $(G, \cdot)$ be a multiplicative group with multiplicative identity $e \in G$.*
$(\forall n \in \mathbb{Z})(e^n = e)$.

Proof. To prove $(\forall n \in \mathbb{Z})(e^n = e)$, let $S_n : e^n = e$ and let $T_n : e^{-n} = e$.

We must prove

1. $e^0 = e$.
2. S_n is true for all $n \in \mathbb{Z}^+$.
3. T_n is true for all $n \in \mathbb{Z}^+$. □

Proof. We prove $e^0 = e$.

Since G is a multiplicative group and $a^0 = e$ for all $a \in G$ and $e \in G$, then $e^0 = e$. □

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

Basis:

Since G is a multiplicative group and $e \in G$, then $e^1 = e^{1-1} \cdot e = e^0 \cdot e = e \cdot e = e$, so S_1 is true.

Induction:

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

Since $k \in \mathbb{Z}^+$, then $k > 0$, so $k + 1 > 0$.

Since S_k is true, then $e^k = e$.

Since $e^{k+1} = e^k \cdot e = e \cdot e = e$, then S_{k+1} is true.

Therefore, S_k implies S_{k+1} for all $k \in \mathbb{Z}^+$.

Since S_1 is true and S_k implies S_{k+1} for all $k \in \mathbb{Z}^+$, then by induction S_n is true for all $n \in \mathbb{Z}^+$. □

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

Basis:

Since the identity element of a group is its own inverse, then $e^{-1} = e$, so T_1 is true.

Induction:

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

Then $e^{-k} = e$.

Since $e^{-(k+1)} = e^{-k-1} = e^{-k}e^{-1} = ee^{-1} = ee = e$, then T_{k+1} is true..

Therefore, T_k implies T_{k+1} for all $k \in \mathbb{Z}^+$.

Since T_1 is true and T_k implies T_{k+1} for all $k \in \mathbb{Z}^+$, then by induction T_n is true for all $n \in \mathbb{Z}^+$. □

additive group notation

Lemma 20. *Let $(G, +)$ be an additive group.*

Let $a \in G$.

Then $na + a = a + na$ for all $n \in \mathbb{Z}^+$.

Proof. To prove $na + a = a + na$ for all $n \in \mathbb{Z}^+$, let $S_n : na + a = a + na$.

We must prove

1. S_n is true for all $n \in \mathbb{Z}^+$.

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

Basis:

Observe that

$$\begin{aligned}
1a + a &= [(1-1)a + a] + a \\
&= (0a + a) + a \\
&= (0a + a) + (0 + a) \\
&= (0a + a) + (0a + a) \\
&= (0 + a) + [(1-1)a + a] \\
&= a + 1a.
\end{aligned}$$

Therefore, $1a + a = a + 1a$, so S_1 is true.

Induction:

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

Then $ka + a = a + ka$ and $k > 0$, so $k + 1 > 0$.

Observe that

$$\begin{aligned}
(k+1)a + a &= (ka + a) + a \\
&= (a + ka) + a \\
&= a + (ka + a) \\
&= a + (k+1)a.
\end{aligned}$$

Hence, $(k+1)a + a = a + (k+1)a$, so S_{k+1} is true.

Thus, S_k implies S_{k+1} for all $k \in \mathbb{Z}^+$.

Since S_1 is true and S_k implies S_{k+1} for all $k \in \mathbb{Z}^+$, then by induction, S_n is true for all $n \in \mathbb{Z}^+$. ☐

Theorem 21. ***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 $n \in \mathbb{Z}$.

Proof. We prove 1.

If $a \in G$, then $(-n)a = n(-a) = -(na)$ for all $n \in \mathbb{Z}^+$.

Let $a \in G$ be arbitrary.

To prove $(-n)a = n(-a) = -(na)$ for all $n \in \mathbb{Z}^+$, let $n \in \mathbb{Z}^+$.

Then $n \in \mathbb{Z}$ and $n > 0$, so $(-n)a = n(-a)$.

Since $n \in \mathbb{Z}^+$, then $n(-a)$ is a sum of $-a$ with itself n times.

Hence, $n(-a) = (-a) + (-a) + ... + (-a)$.

The expression $(-a) + (-a) + ... + (-a)$ is the same as the inverse of the sum of a with itself n times, by proposition 11 .

Thus, $(-a) + (-a) + ... + (-a) = -(a + a + ... + a) = -(na)$.

Hence, $n(-a) = (-a) + (-a) + ... + (-a) = -(a + a + ... + a) = -(na)$, so $n(-a) = -(na)$.

Therefore, $(-n)a = n(-a)$ and $n(-a) = -(na)$, so $(-n)a = n(-a) = -(na)$. ☐

Proof. We prove 2.

If $a \in G$, then $na \in G$ for all $n \in \mathbb{Z}$.

Let $0 \in G$ be the identity of G.

Let $a \in G$ be arbitrary.

To prove $na \in G$ for all $n \in \mathbb{Z}$, let $S_n : na \in G$ and let $T_n : (-n)a \in G$.

We must prove

1. $0a \in G$.
2. S_n is true for all $n \in \mathbb{Z}^+$.
3. T_n is true for all $n \in \mathbb{Z}^+$. ☐

Proof. We first prove $0a \in G$.

Since $0a = 0$ and $0 \in G$, then $0a \in G$. ☐

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

Basis:

Since $a \in G$ and $1a = (1-1)a + a = 0a + a = 0 + a = a$, then $1a \in G$, so S_1 is true.

Induction:

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

Since $k \in \mathbb{Z}^+$, then $k > 0$, so $k + 1 > 0$.

Since S_k is true, then $ka \in G$.

Since $(k+1)a = ka + a$ and $ka \in G$ and $a \in G$, then by closure of G under $+$, the sum $(k+1)a$ is an element of G, so $(k+1)a \in G$.

Therefore, S_{k+1} is true.

Thus, S_k implies S_{k+1} for all $k \in \mathbb{Z}^+$.

Since S_1 is true and S_k implies S_{k+1} for all $k \in \mathbb{Z}^+$, then by induction, S_n is true for all $n \in \mathbb{Z}^+$. ☐

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

Basis:

Since $a \in G$ and every element in G is invertible by definition of a group, then its inverse $-a$ is in G, so $-a \in G$.

Since $(-1)a = -a$ and $-a \in G$, then T_1 is true.

Induction:

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

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

Since T_k is true, then $(-k)a \in G$.

Observe that

$$\begin{aligned} -(k+1)a &= (k+1)(-a) \\ &= k(-a) + (-a) \\ &= (-k)a + (-a). \end{aligned}$$

Since $(-k)a \in G$ and $-a \in G$, then by closure of G under $+$, we have $(-k)a + (-a) \in G$, so $-(k+1)a \in G$.

Therefore, T_{k+1} is true.

Thus, T_k implies T_{k+1} for all $k \in \mathbb{Z}^+$.

Since T_1 is true and T_k implies T_{k+1} for all $k \in \mathbb{Z}^+$, then by induction, T_n is true for all $n \in \mathbb{Z}^+$. $\square$

Proof. We prove 3.

If $a \in G$, then $ma + na = (m+n)a$ for all $m, n \in \mathbb{Z}$.

Let $a \in G$ be arbitrary.

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

To prove $ma + na = (m+n)a$ for all $n \in \mathbb{Z}$, let $S_n : ma + na = (m+n)a$ and let $T_n : ma + (-n)a = (m-n)a$.

We must prove

1. $ma + 0a = (m+0)a$.
2. S_n is true for all $n \in \mathbb{Z}^+$.
3. T_n is true for all $n \in \mathbb{Z}^+$. $\square$

Proof. We prove $ma + 0a = (m+0)a$.

Since $(m+0)a = ma = ma + 0 = ma + 0a$, then $ma + 0a = (m+0)a$. $\square$

Proof. We prove T_1 is true.

Basis:

Either $m - 1 > 0$ or $m - 1 = 0$ or $m - 1 < 0$.

We consider these cases separately.

Case 1: Suppose $m - 1 > 0$.

Then $m > 1$, so $m > 0$.

Since $ma+(-1)a = ma+(-a) = [(m-1)a+a]+(-a) = (m-1)a+[a+(-a)] = (m-1)a + 0 = (m-1)a$, then $ma + (-1)a = (m-1)a$.

Therefore, T_1 is true.

Case 2: Suppose $m - 1 = 0$.

Then $m = 1$.

Since $ma+(-1)a = 1a+(-1)a = a+(-1)a = a+(-a) = 0 = 0a = (m-1)a$, then $ma + (-1)a = (m-1)a$.

Therefore, T_1 is true.

Case 3: Suppose $m - 1 < 0$.

Then $m < 1$.

We must prove $ma + (-1)a = (m-1)a$ for all integers $m < 1$.

The statement $ma + (-1)a = (m-1)a$ for all integers $m < -1$ is equivalent to the statement $ma + (-1)a = (m-1)a$ for all integers $m \leq -2$ which is equivalent to the statement $(-k)a + (-1)a = (-k-1)a$ for all integers $k \geq 2$.

So, to prove the statement $ma + (-1)a = (m-1)a$ for all integers $m < -1$, we prove the equivalent statement $(-k)a + (-1)a = (-k-1)a$ for all integers $k \geq 2$.

Let $k \in \mathbb{Z}$ and $k \geq 2$.

Since $k \geq 2$ and $2 > 0$, then $k > 0$, so $-k < 0$.

Since $k > 0$ and $1 > 0$, then we add to obtain $k + 1 > 0$.

Observe that

$$\begin{aligned}
(-k)a + (-1)a &= (-k)a + (-a) \\
&= -(ka) + (-a) \\
&= -(a + ka) \\
&= -(ka + a) \\
&= -[(k+1)a] \\
&= -(k+1)a \\
&= (-k-1)a.
\end{aligned}$$

Hence, $(-k)a+(-1)a = (-k-1)a$, so $ma+(-1)a = (m-1)a$ for all integers $m < -1$.

Therefore, T_1 is true.

In all cases, T_1 is true.

Therefore, $ma + (-1)a = (m-1)a$ for all $m \in \mathbb{Z}$. □

Proof. **Induction:**

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

Since $k \in \mathbb{Z}^+$, then $k > 0$, so $k + 1 > 0$.

Since T_k is true, then $ma + (-k)a = (m-k)a$.

Either $m - k - 1 > 0$ or $m - k - 1 = 0$ or $m - k - 1 < 0$.

We consider these cases separately.

Case 1: Suppose $m - k - 1 > 0$.

Then $m - k > 1$, so $m - k > 0$.

Observe that

$$\begin{aligned}
ma + [-(k+1)]a &= ma + [(k+1)(-a)] \\
&= ma + [k(-a) + (-a)] \\
&= ma + [(-k)a + (-a)] \\
&= [ma + (-k)a] + (-a) \\
&= (m-k)a + (-a) \\
&= [(m-k-1)a + a] + (-a) \\
&= (m-k-1)a + [a + (-a)] \\
&= (m-k-1)a + 0 \\
&= (m-k-1)a \\
&= [m-(k+1)]a.
\end{aligned}$$

Thus, $ma + [-(k+1)]a = [m-(k+1)]a$.

Therefore, T_{k+1} is true.

Case 2: Suppose $m - k - 1 = 0$.

Then $m - k = 1$.

Observe that

$$\begin{aligned}
ma + [-(k+1)]a &= ma + (k+1)(-a) \\
&= ma + [k(-a) + (-a)] \\
&= ma + [(-k)a + (-a)] \\
&= [ma + (-k)a] + (-a) \\
&= (m-k)a + (-a) \\
&= 1a + (-a) \\
&= a + (-a) \\
&= 0 \\
&= 0a \\
&= (m-k-1)a \\
&= [m-(k+1)]a.
\end{aligned}$$

Thus, $ma + [-(k+1)]a = [m-(k+1)]a$.
Therefore, T_{k+1} is true.
Case 3: Suppose $m - k - 1 < 0$.
Observe that

$$\begin{aligned}
ma + [-(k+1)]a &= ma + (k+1)(-a) \\
&= ma + [k(-a) + (-a)] \\
&= ma + [(-k)a + (-a)] \\
&= [ma + (-k)a] + (-a) \\
&= (m-k)a + (-a) \\
&= (m-k)a + (-1)a \\
&= (m-k-1)a \\
&= [m-(k+1)]a.
\end{aligned}$$

Thus, $ma + [-(k+1)]a = [m-(k+1)]a$.
Therefore, T_{k+1} is true.

In all cases, T_{k+1} is true.
Hence, T_k implies T_{k+1} for all $k \in \mathbb{Z}^+$.
Since T_1 is true and T_k implies T_{k+1} for all $k \in \mathbb{Z}^+$, then by induction, T_n is true for all $n \in \mathbb{Z}^+$. $\square$

Proof. We prove S_n is true for all $n \in \mathbb{Z}^+$ by induction on n.
Basis:
Either $m + 1 > 0$ or $m + 1 = 0$ or $m + 1 < 0$.
We consider these cases separately.
Case 1: Suppose $m + 1 > 0$.
Since $ma+1a = ma+a = (m+1-1)a+a = (m+1)a$, then $ma+1a = (m+1)a$.
Therefore, S_1 is true.

Case 2: Suppose $m + 1 = 0$.
Then $m = -1$.
Since $ma + 1a = (-1)a + 1a = (-1)a + a = -a + a = 0 = 0a = (m + 1)a$, then $ma + 1a = (m + 1)a$.
Therefore, S_1 is true.
Case 3: Suppose $m + 1 < 0$.
Then $m < -1$.
We must prove $ma + 1a = (m + 1)a$ for all integers $m < -1$.
The statement $ma + 1a = (m + 1)a$ for all integers $m < -1$ is equivalent to the statement $ma + 1a = (m + 1)a$ for all integers $m \leq -2$ which is equivalent to the statement $(-k)a + 1a = (-k + 1)a$ for all integers $k \geq 2$.
So, to prove the statement $ma + 1a = (m + 1)a$ for all integers $m < -1$, we prove the equivalent statement $(-k)a + 1a = (-k + 1)a$ for all integers $k \geq 2$.
Let $k \in \mathbb{Z}$ and $k \geq 2$.
Since $k \geq 2$ and $2 > 0$, then $k > 0$.
Since $k \geq 2$, then $k - 1 \geq 1$, so $k - 1 > 0$.
Observe that

$$\begin{aligned}
(-k)a + 1a &= (-k)a + a \\
&= k(-a) + a \\
&= [(k-1)(-a) + (-a)] + a \\
&= (k-1)(-a) + [(-a) + a] \\
&= (k-1)(-a) + 0 \\
&= (k-1)(-a) \\
&= -(k-1)a \\
&= (-k+1)a.
\end{aligned}$$

Hence, $(-k)a + 1a = (-k + 1)a$, so $ma + 1a = (m + 1)a$ for all integers $m < -1$.
Therefore, S_1 is true.

In all cases, S_1 is true. □

Proof. **Induction:**
Let $k \in \mathbb{Z}^+$ such that S_k is true.
Since $k \in \mathbb{Z}^+$, then $k > 0$.
Since S_k is true, then $ma + ka = (m + k)a$.
Either $m + k + 1 > 0$ or $m + k + 1 = 0$ or $m + k + 1 < 0$.
We consider these cases separately.
Case 1: Suppose $m + k + 1 > 0$.

Observe that

$$\begin{aligned}
ma + (k+1)a &= ma + (ka + a) \\
&= (ma + ka) + a \\
&= (m + k)a + a \\
&= (m + k + 1 - 1)a + a \\
&= (m + k + 1)a \\
&= [m + (k + 1)]a.
\end{aligned}$$

Thus, $ma + (k+1)a = [m + (k+1)]a$.
Therefore, S_{k+1} is true.
Case 2: Suppose $m + k + 1 = 0$.
Then $m + k = -1$.
Observe that

$$\begin{aligned}
ma + (k+1)a &= ma + (ka + a) \\
&= (ma + ka) + a \\
&= (m + k)a + a \\
&= (-1)a + a \\
&= -a + a \\
&= 0 \\
&= 0a \\
&= (m + k + 1)a \\
&= [m + (k + 1)]a.
\end{aligned}$$

Thus, $ma + (k+1)a = [m + (k+1)]a$.
Therefore, S_{k+1} is true.
Case 3: Suppose $m + k + 1 < 0$.
Then $m + k < -1$.
Since S_1 is true, then $ma + 1a = (m+1)a$ for all integers $m < -1$.
Hence, $(m+k)a + 1a = [(m+k) + 1]a$.
Observe that

$$\begin{aligned}
ma + (k+1)a &= ma + (ka + a) \\
&= (ma + ka) + a \\
&= (m + k)a + a \\
&= (m + k)a + 1a \\
&= [(m + k) + 1]a \\
&= [m + (k + 1)]a.
\end{aligned}$$

Thus, $ma + (k+1)a = [m + (k+1)]a$.
Therefore, S_{k+1} is true.

In all cases, S_{k+1} is true.

Hence, S_k implies S_{k+1} for all $k \in \mathbb{Z}^+$.

Since S_1 is true and S_k implies S_{k+1} for all $k \in \mathbb{Z}^+$, then by induction, S_n is true for all $n \in \mathbb{Z}^+$. ☐

Proof. We prove 4.

If $a \in G$, then $n(ma) = (mn)a$ for all $m, n \in \mathbb{Z}$.

Let $a \in G$.

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

To prove $n(ma) = (mn)a$ for all $n \in \mathbb{Z}$, let $S_n : n(ma) = (mn)a$ and let $T_n : (-n)(ma) = [m(-n)]a$.

We must prove

1. $0(ma) = (m0)a$.
2. S_n is true for all $n \in \mathbb{Z}^+$.
3. T_n is true for all $n \in \mathbb{Z}^+$. ☐

Proof. We prove $0(ma) = (m0)a$.

Since $a \in G$ and $m \in \mathbb{Z}$, then $ma \in G$, so $0(ma) = 0 = 0a = (m0)a$.

Therefore, $0(ma) = (m0)a$. ☐

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

Basis:

Since $1(ma) = ma = (m1)a$, then $1(ma) = (m1)a$, so S_1 is true.

Induction:

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

Then $k(ma) = (mk)a$.

Observe that

$$\begin{aligned}
(k+1)(ma) &= k(ma) + (ma) \\
&= (mk)a + (ma) \\
&= (mk + m)a \\
&= m(k+1)a.
\end{aligned}$$

Thus, $(k+1)(ma) = m(k+1)a$, so S_{k+1} is true.

Therefore, S_k implies S_{k+1} for all $k \in \mathbb{Z}^+$.

Since S_1 is true and S_k implies S_{k+1} for all $k \in \mathbb{Z}^+$, then by induction, S_n is true for all $n \in \mathbb{Z}^+$. ☐

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

Basis:

Since $m \in \mathbb{Z}$, then either $m > 0$ or $m = 0$ or $m < 0$.

We consider these cases separately.

Case 1: Suppose $m > 0$.

Then $(-1)(ma) = -(ma) = [(-m)]a = [m(-1)]a$, so $(-1)(ma) = [m(-1)]a$.

Therefore, T_1 is true.

Case 2: Suppose $m = 0$.

Then $(-1)(ma) = (-1)(0a) = (-1)0 = 0 = 0a = [0(-1)]a = [m(-1)]a$, so $(-1)(ma) = [m(-1)]a$.

Therefore, T_1 is true.

Case 3: Suppose $m < 0$.

Then $-m > 0$, so $[-(-m)]a = -[(-m)a]$.

Observe that

$$\begin{aligned}
(-1)(ma) &= -(ma) \\
&= -[[-(-m)]a] \\
&= -[-[(-m)a]] \\
&= (-m)a \\
&= [m(-1)]a.
\end{aligned}$$

Thus, $(-1)(ma) = [m(-1)]a$, so T_1 is true.

In all cases, T_1 is true.

Therefore, $(-1)(ma) = [m(-1)]a$ for all $m \in \mathbb{Z}$.

Induction:

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

Then $(-k)(ma) = [m(-k)]a$.

Observe that

$$\begin{aligned}
[-(k+1)](ma) &= [(k+1)(-1)](ma) \\
&= (-1)[(k+1)(ma)] \\
&= (-1)[k(ma) + ma] \\
&= -[k(ma) + ma] \\
&= -(ma) + (-k)(ma) \\
&= -(ma) + [m(-k)]a \\
&= (-1)(ma) + [m(-k)]a \\
&= [m(-1)]a + [m(-k)]a \\
&= (-m)a + (-mk)a \\
&= (-m - mk)a \\
&= [-m(1+k)]a \\
&= [-m(k+1)]a \\
&= [m(-(k+1))]a.
\end{aligned}$$

Thus, $[-(k+1)](ma) = [m(-(k+1))]a$, so T_{k+1} is true.

Therefore, T_k implies T_{k+1} for all $k \in \mathbb{Z}^+$.

Since T_1 is true and T_k implies T_{k+1} for all $k \in \mathbb{Z}^+$, then by induction, T_n is true for all $n \in \mathbb{Z}^+$. $\square$

Proof. We prove 5.

If $a, b \in G$ and G is abelian, then $n(a+b) = na + nb$ for all $n \in \mathbb{Z}$.

Suppose $a, b \in G$ and G is abelian.

To prove $n(a+b) = na + nb$ for all $n \in \mathbb{Z}$, let $S_n : n(a+b) = na + nb$ and let $T_n : (-n)(a+b) = (-n)a + (-n)b$.

We must prove

1. $0(a+b) = 0a + 0b$.
2. S_n is true for all $n \in \mathbb{Z}^+$.
3. T_n is true for all $n \in \mathbb{Z}^+$. $\square$

Proof. We prove $0(a+b) = 0a + 0b$.

Since $a \in G$ and $b \in G$, then by closure of G under $+$, we have $a + b \in G$.

Therefore, $0(a+b) = 0 = 0+0 = 0a+0b$, so $0(a+b) = 0a+0b$, as desired. $\square$

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

Basis:

Since $1(a+b) = a+b = 1a+1b$, then $1(a+b) = 1a+1b$, so S_1 is true.

Induction:

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

Since $k \in \mathbb{Z}^+$, then $k \in \mathbb{Z}$ and $k > 0$.

Since S_k is true, then $k(a+b) = ka + kb$.

Observe that

$$\begin{aligned}
(k+1)(a+b) &= k(a+b) + (a+b) \\
&= (ka+kb) + (a+b) \\
&= ka + (kb+a) + b \\
&= ka + (a+kb) + b \\
&= (ka+a) + (kb+b) \\
&= (k+1)a + (k+1)b
\end{aligned}$$

Therefore, $(k+1)(a+b) = (k+1)a + (k+1)b$, so S_{k+1} is true.

Hence, S_k implies S_{k+1} for all $k \in \mathbb{Z}^+$.

Since S_1 is true and S_k implies S_{k+1} for all $k \in \mathbb{Z}^+$, then by induction, S_n is true for all $n \in \mathbb{Z}^+$. $\square$

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

Basis:

Since $(-1)(a+b) = -(a+b) = (-b)+(-a) = (-a)+(-b) = (-1)a+(-1)b$, then $(-1)(a+b) = (-1)a+(-1)b$, so T_1 is true.

Induction:

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

Since $k \in \mathbb{Z}^+$, then $k \in \mathbb{Z}$ and $k > 0$.

Since T_k is true, then $(-k)(a+b) = (-k)a + (-k)b$.

Observe that

$$\begin{aligned}
[-(k+1)](a+b) &= (-k-1)(a+b) \\
&= (-k)(a+b)+(-1)(a+b) \\
&= [(-k)a+(-k)b]+(-1)(a+b) \\
&= [(-k)a+(-k)b]+[-(a+b)] \\
&= [(-k)a+(-k)b]+[(-b)+(-a)] \\
&= (-k)a+[(-k)b+(-b)]+(-a) \\
&= [(-k)a+(-a)]+[(-k)b+(-b)] \\
&= (-k-1)a+(-k-1)b \\
&= [-(k+1)]a+[-(k+1)]b
\end{aligned}$$

Hence, $[-(k+1)](a+b) = [-(k+1)]a + [-(k+1)]b$, so T_{k+1} is true.

Therefore, T_k implies T_{k+1} for all $k \in \mathbb{Z}^+$.

Since T_1 is true and T_k implies T_{k+1} for all $k \in \mathbb{Z}^+$, then by induction, T_n is true for all $n \in \mathbb{Z}^+$ $\square$

Proposition 22. *Let $(G, +)$ be an additive group with additive identity $0 \in G$. $(\forall n \in \mathbb{Z})(n0 = 0)$.*

Proof. To prove $(\forall n \in \mathbb{Z})(n0 = 0)$, let $S_n : n0 = 0$ and let $T_n : (-n)0 = 0$.

We must prove

1. $00 = 0$.
2. S_n is true for all $n \in \mathbb{Z}^+$.
3. T_n is true for all $n \in \mathbb{Z}^+$. $\square$

Proof. We prove $00 = 0$.

Since G is an additive group and $0a = 0$ for all $a \in G$ and $0 \in G$, then $00 = 0$. $\square$

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

Basis:

Since G is an additive group and $0 \in G$, then $1 \cdot 0 = (1-1) \cdot 0 + 0 = (0 \cdot 0) + 0 = 0 + 0 = 0$, so S_1 is true.

Induction:

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

Since $k \in \mathbb{Z}^+$, then $k > 0$, so $k + 1 > 0$.

Since S_k is true, then $k0 = 0$.

Since $(k+1)0 = k0 + 0 = 0 + 0 = 0$, then S_{k+1} is true.

Therefore, S_k implies S_{k+1} for all $k \in \mathbb{Z}^+$.

Since S_1 is true and S_k implies S_{k+1} for all $k \in \mathbb{Z}^+$, then by induction S_n is true for all $n \in \mathbb{Z}^+$. $\square$

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

Basis:

Since the identity element of a group is its own inverse, then $-0 = 0$, so $(-1)0 = -0 = 0$.

Therefore, T_1 is true.

Induction:

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

Then $(-k)0 = 0$.

Since $[-(k+1)]0 = (-k-1)0 = (-k)0 + (-1)0 = 0 + (-1)0 = 0 + 0 = 0$, then T_{k+1} is true..

Therefore, T_k implies T_{k+1} for all $k \in \mathbb{Z}^+$.

Since T_1 is true and T_k implies T_{k+1} for all $k \in \mathbb{Z}^+$, then by induction T_n is true for all $n \in \mathbb{Z}^+$. $\square$

Subgroups

Theorem 23. ***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: $(\forall a \in H)(a^{-1} \in H)$.

Proof. Suppose $a * b \in H$ for all $a, b \in H$ and $a^{-1} \in H$ for all $a \in H$.

We must prove $H < G$.

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

We prove $e \in H$.

Since H is not empty, then there exists $a \in H$.

Since $a^{-1} \in H$ for all $a \in H$, then $a^{-1} \in H$.

Since $a * b \in H$ for all $a, b \in H$ and $a \in H$ and $a^{-1} \in H$, then $a * a^{-1} \in H$, so $e \in H$.

We prove $*$ is a binary operation on H.

Let $a, b \in H$.

By assumption, $a * b \in H$ for all $a, b \in H$, so we conclude $a * b \in H$.

Since $a \in H$ and $H \subset G$, then $a \in G$.

Since $b \in H$ and $H \subset G$, then $b \in G$.

Since G is a group, then $*$ is a binary operation on G, so $a * b$ is unique.

Therefore, $a * b \in H$ and $a * b$ is unique, so $*$ is a binary operation on H.

We prove the binary operation $*$ over H is associative.

Since $*$ over G is associative and $H \subset G$, then $*$ over H is associative.

We prove $e \in H$ is an identity for $*$.
Let $a \in H$.
Since $H \subset G$, then $a \in G$.
Since $e \in G$ is identity for $*$, then $a * e = e * a = a$ for all $a \in G$, so $a * e = e * a = a$.
Hence, $a * e = e * a = a$ for all $a \in H$.
Since $e \in H$ and $a * e = e * a = a$ for all $a \in H$, then $e \in H$ is an identity for $*$.

We prove for every element $a \in H$, there exists an inverse $a^{-1} \in H$.
Let $a \in H$.
By assumption $a^{-1} \in H$ for all $a \in H$.
In particular, $a^{-1} \in H$.
Since $(G, *)$ is a group, then $a * a^{-1} = a^{-1} * a = e$ for all $a \in G$.
Since $a \in H$ and $H \subset G$, then $a \in G$, so we conclude $a * a^{-1} = a^{-1} * a = e$.
Thus, for every $a \in H$ there exists $a^{-1} \in H$ such that $a * a^{-1} = a^{-1} * a = e$.
Therefore, for every $a \in H$, there exists an inverse $a^{-1} \in H$.

Since $*$ is a binary operation on H and $*$ over H is associative and $e \in H$ is an identity for $*$ and for every element $a \in H$, there exists an inverse $a^{-1} \in H$, then $(H, *)$ is a group.
Since $H \subset G$ and $(H, *)$ is a group, then H is a subgroup of G, so $H < G$. □

Proof. Conversely, suppose $H < G$.
Then $H \subset G$ and $(H, *)$ is a group under the binary operation of $(G, *)$.
We must prove $a * b \in H$ for all $a, b \in H$ and $a^{-1} \in H$ for all $a \in H$.

We prove $a * b \in H$ for all $a, b \in H$.
Since $(H, *)$ is a group under the binary operation of G, then $*$ is a binary operation on H, so H is closed under $*$ of G.
Therefore, $a * b \in H$ for all $a, b \in H$.

We prove $a^{-1} \in H$ for all $a \in H$.
Let $a \in H$.
Since $(H, *)$ is a group, then the inverse of a exists in H.
Let a^{-1} be the inverse of a.
Then $a^{-1} \in H$, so $a^{-1} \in H$ for all $a \in H$. □

Theorem 24. ***One-Step Subgroup Test***
Let H be a nonempty subset of a group $(G, *)$.
Then $H < G$ iff
1. $(\forall a, b \in H)(a * b^{-1} \in H)$.

Proof. Suppose $a * b^{-1} \in H$ for all $a, b \in H$.
We must prove $H < G$.
Let $e \in G$ be the identity of G.

We prove $a^{-1} \in H$ for all $a \in H$.
Let $a \in H$.
By assumption, $a * b^{-1} \in H$ for all $a, b \in H$.
Since $a \in H$ and $a \in H$, then we conclude $a * a^{-1} \in H$, so $e \in H$.
Since $e \in H$ and $a \in H$, then we conclude $e * a^{-1} \in H$, so $a^{-1} \in H$.
Therefore, $a^{-1} \in H$ for all $a \in H$.

We prove $a * b \in H$ for all $a, b \in H$.
Let $a, b \in H$.
Since $a^{-1} \in H$ for all $a \in H$ and $b \in H$, then $b^{-1} \in H$.
By assumption, $a * b^{-1} \in H$ for all $a, b \in H$.
Since $a \in H$ and $b^{-1} \in H$, then we conclude $a * (b^{-1})^{-1} \in H$, so $a * b \in H$.
Therefore, $a * b \in H$ for all $a, b \in H$.

Since H is a nonempty subset of G and $a*b \in H$ for all $a, b \in H$ and $a^{-1} \in H$ for all $a \in H$, then by the two-step subgroup test, H is a subgroup of G, so $H < G$. $\square$

Proof. Conversely, suppose $H < G$.
We must prove $a * b^{-1} \in H$ for all $a, b \in H$.
Let $a, b \in H$.
Since $H < G$, then H is a group, so for every $a \in H$, there exists an inverse $a^{-1} \in H$.
Since $b \in H$, then this implies there exists $b^{-1} \in H$.
Since $H < G$, then H is closed under the binary operation of G, so $a * b \in H$ for all $a, b \in H$.
Since $a \in H$ and $b^{-1} \in H$, then this implies $a * b^{-1} \in H$.
Therefore, $a * b^{-1} \in H$ for all $a, b \in H$. $\square$

Theorem 25. ***Subgroup relation is transitive.***
Let $(G, *)$ be a group.
If $H < K$ and $K < G$, then $H < G$.

Proof. Suppose $H < K$ and $K < G$.
We must prove $H < G$.

We prove $H \subset G$.
Since $H < K$, then $H \subset K$.
Since $K < G$, then $K \subset G$.
Since $H \subset K$ and $K \subset G$, then $H \subset G$.

We prove $a * b \in H$ for all $a, b \in H$.

Since $K < G$, then K is closed under the binary operation of G, so the binary operation of K is the same as the binary operation of G.

Since $H < K$, then H is closed under the binary operation of K.

Since the binary operation of K is the same as the binary operation of G and $*$ is the binary operation on G, then $*$ is the binary operation on K.

Since H is closed under the binary operation of K and $*$ is the binary operation on K, then H is closed under $*$.

Therefore, $a * b \in H$ for all $a, b \in H$.

We prove $e \in H$.

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

Since $K < G$ and $e \in G$, then K is closed under identity by the first subgroup test, so $e \in K$.

Since $H < K$ and $e \in K$, then H is closed under identity by the first subgroup test, so $e \in H$.

We prove $a^{-1} \in H$ for all $a \in H$.

Let $a \in H$.

Since $H < K$, then H is a subgroup of K, so H is a group.

Hence, every element of H has an inverse in H.

Since $a \in H$, then this implies $a^{-1} \in H$.

Therefore, $a^{-1} \in H$ for all $a \in H$.

Since $H \subset G$ and $a * b \in H$ for all $a, b \in H$ and $e \in H$ and $a^{-1} \in H$ for all $a \in H$, then by the first subgroup test, H is a subgroup of G, so $H < G$. □

Theorem 26. ***The intersection of subgroups is a subgroup.***

The intersection of a family of subgroups is a subgroup.

Proof. Let $(G, *)$ be a group with identity $e \in G$.

Let $\{H_i : i \in I\}$ be a collection of subgroups of G for some index set I.

Then each H_i is a subgroup of G, so $H_i < G$ for all $i \in I$.

Let $H = \cap_{i \in I} H_i$ be the intersection of all these subgroups.

Then $H = \{x : x \in H_i \text{ for all } i \in I\}$, by definition of intersection of a family of sets.

We must prove H is a subgroup of G.

We prove $H \subset G$.

Let $x \in H$.

Then $x \in H_i$ for all $i \in I$.

Let $i \in I$.

Then $x \in H_i$ and $H_i < G$.

Since $H_i < G$, then $H_i \subset G$.

Since $x \in H_i$ and $H_i \subset G$, then $x \in G$.

Therefore, $x \in H$ implies $x \in G$, so $H \subset G$.

We prove $H \neq \emptyset$.
Let $i \in I$.
Then $H_i < G$.
Since $H_i < G$, then H_i is closed under identity by the first subgroup test.
Since $e \in G$, then this implies $e \in H_i$.
Since i is arbitrary, then $e \in H_i$ for all $i \in I$.
Therefore, $e \in H$, so $H \neq \emptyset$.

We prove $a * b^{-1} \in H$ for all $a, b \in H$.
Let $a, b \in H$.
Then $a \in H_i$ for all $i \in I$ and $b \in H_i$ for all $i \in I$.
Let $i \in I$.
Then $a \in H_i$ and $b \in H_i$ and $H_i < G$.
Since $H_i < G$, then H_i is a subgroup of G, so H_i is a group.
Since H_i is a group and $b \in H_i$, then $b^{-1} \in H_i$.
Since H_i is a subgroup of G, then H_i is closed under $*$ of G.
Since $a \in H_i$ and $b^{-1} \in H_i$, then we conclude $a * b^{-1} \in H_i$.
Since i is arbitrary, then $a * b^{-1} \in H_i$ for all $i \in I$.
Therefore, $a * b^{-1} \in H$, so $a * b^{-1} \in H$ for all $a, b \in H$.

Since $H \subset G$ and $H \neq \emptyset$ and $a * b^{-1} \in H$ for all $a, b \in H$, then by the second subgroup test, $H < G$. ☐

Cyclic groups

Order of a group element

Theorem 27. *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.

Proof. Suppose there exist integers s and t such that $a^s = a^t$ and $s \neq t$.
Since $s \neq t$, then either $s < t$ or $s > t$.
Without loss of generality, assume $s < t$.
Then $0 < t - s$.
Let $e \in G$ be the identity of G.
Observe that

$$\begin{aligned} e &= a^0 \\ &= a^{s-s} \\ &= a^s * a^{-s} \\ &= a^t * a^{-s} \\ &= a^{t-s}. \end{aligned}$$

Since s and t are integers, then $t - s$ is an integer.

Since $t-s$ is an integer and $t-s>0$, then $t-s \in \mathbb{Z}^+$.
Since $t-s \in \mathbb{Z}^+$ and $a^{t-s}=e$, then a has finite order. □

Theorem 28. *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 $k \in \mathbb{Z}$.

Proof. Suppose $a \in G$ has finite order n.
Then n is the least positive integer such that $a^n = e$.

We must prove $a^k = e$ iff $n|k$ for all $k \in \mathbb{Z}$.
Let $k \in \mathbb{Z}$.

We prove if $n|k$, then $a^k = e$.
Suppose $n|k$.
Then $k = nm$ for some integer m.
Thus,

$$\begin{aligned} a^k &= a^{nm} \\ &= (a^n)^m \\ &= e^m \\ &= e. \end{aligned}$$

Therefore, $a^k = e$. □

Proof. Conversely, we prove if $a^k = e$, then $n|k$.
Suppose $a^k = e$.
We divide k by n
By the division algorithm, $k = nq + r$ for integers q, r with $0 \leq r < n$.
Thus,

$$\begin{aligned} e &= a^k \\ &= a^{nq+r} \\ &= a^{nq} * a^r \\ &= (a^n)^q * a^r \\ &= e^q * a^r \\ &= e * a^r \\ &= a^r. \end{aligned}$$

Hence, $a^r = e$.
Since $r \geq 0$, then either $r > 0$ or $r = 0$.

Suppose $r > 0$.

Since $r \in \mathbb{Z}$ and $r > 0$, then $r \in \mathbb{Z}^+$.

Since n is the least positive integer such that $a^n = e$, then $n \leq x$ for every $x \in \mathbb{Z}^+$ such that $a^x = e$.

Since $r \in \mathbb{Z}^+$ and $a^r = e$, then we conclude $n \leq r$, so $r \geq n$.

But, this contradicts $r < n$.

Hence, r cannot be greater than zero, so we must conclude $r = 0$.

Therefore, $k = nq + r = nq + 0 = nq$, so $n|k$, as desired. ☐

Corollary 29. *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 $s, t \in \mathbb{Z}$.

Proof. Suppose $a \in G$ has finite order n.

Then n is the least positive integer such that $a^n = e$.

Let s and t be arbitrary integers.

We must prove $a^s = a^t$ iff $s \equiv t \pmod{n}$.

We prove if $s \equiv t \pmod{n}$ then $a^s = a^t$.

Suppose $s \equiv t \pmod{n}$.

Then $n|s - t$, so there exists an integer k such that $s - t = nk$.

Observe that

$$\begin{aligned} a^s &= a^{nk+t} \\ &= a^{nk} * a^t \\ &= (a^n)^k * a^t \\ &= e^k * a^t \\ &= e * a^t \\ &= a^t. \end{aligned}$$

Therefore, $a^s = a^t$. ☐

Proof. Conversely, we prove if $a^s = a^t$ then $s \equiv t \pmod{n}$.

Suppose $a^s = a^t$.

Then

$$\begin{aligned} a^{s-t} &= a^s * a^{-t} \\ &= a^t * a^{-t} \\ &= a^{t-t} \\ &= a^0 \\ &= e. \end{aligned}$$

Thus, $a^{s-t} = e$.

Since a has finite order n and $s - t \in \mathbb{Z}$, then $a^{s-t} = e$ iff $n|(s - t)$.

Hence, $n|(s - t)$.

Therefore, $s \equiv t \pmod{n}$. ☐

Theorem 30. *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 $s \in \mathbb{Z}$.

Proof. Suppose $a \in G$ has finite order n.
Then n is the least positive integer such that $a^n = e$.
Let $s \in \mathbb{Z}$.
Observe that

$$\begin{aligned}(a^s)^n &= a^{sn} \\ &= a^{ns} \\ &= (a^n)^s \\ &= e^s \\ &= e.\end{aligned}$$

Hence, there exists a positive integer n such that $(a^s)^n = e$.
Therefore, a^s has finite order. $\square$

Proof. Let $d = \gcd(s, n)$.
Then d is a positive integer and $d|s$ and $d|n$.
Hence, $\frac{s}{d}$ is an integer and $\frac{n}{d}$ is a positive integer.

We prove the order of a^s is $\frac{n}{d}$.
Since a^s has finite order, let t be the order of a^s.
Then t is the least positive integer such that $(a^s)^t = e$, so $e = a^{st}$.
Since a has finite order n, then $a^{st} = e$ if and only if $n|st$.
Hence, $n|st$, so there exists an integer b such that $st = nb$.
Since $d > 0$, we divide by d to obtain $\frac{s}{d}t = \frac{n}{d}b$.
Since $\frac{s}{d}$ and t are integers, then the product $\frac{s}{d}t$ is an integer.
Since $\frac{n}{d}$ and b are integers, then $\frac{n}{d}$ divides $\frac{s}{d}t$.

Since $d = \gcd(s, n)$, then $\gcd(\frac{s}{d}, \frac{n}{d}) = 1$, so $\gcd(\frac{n}{d}, \frac{s}{d}) = 1$.
Since $\frac{n}{d}$ divides $\frac{s}{d}t$ and $\gcd(\frac{n}{d}, \frac{s}{d}) = 1$, then $\frac{n}{d}$ divides t.
Observe that

$$\begin{aligned}(a^s)^{\frac{n}{d}} &= a^{\frac{sn}{d}} \\ &= (a^n)^{\frac{s}{d}} \\ &= e^{\frac{s}{d}} \\ &= e.\end{aligned}$$

Since a^s has finite order t, then $(a^s)^m = e$ iff $t|m$ for all integers m.
Since $\frac{n}{d}$ is an integer, then we conclude $(a^s)^{\frac{n}{d}} = e$ iff t divides $\frac{n}{d}$.
Hence, t divides $\frac{n}{d}$.
Since $t \in \mathbb{Z}^+$ and $\frac{n}{d} \in \mathbb{Z}^+$ and t divides $\frac{n}{d}$ and $\frac{n}{d}$ divides t, then $t = \frac{n}{d}$, by the anti-symmetric property of the divides relation on $\mathbb{Z}^+$. $\square$

Corollary 31. *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.

Proof. Suppose s and n are relatively prime.
Then $\gcd(s, n) = 1$.
Observe that

$$\begin{aligned} |a^s| &= \frac{n}{\gcd(s,n)} \\ &= \frac{n}{1} \\ &= n. \end{aligned}$$

Therefore, a^s has order n. $\square$

Corollary 32. *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 $\frac{n}{s}$.

Proof. Suppose s divides n.
Then there exists $t \in \mathbb{Z}$ such that $n = st$.
Thus, $t = \frac{n}{s}$.
Since a has order n, then n is a positive integer, so $n \neq 0$.

Suppose $s = 0$.
Then $n = st = 0t = 0$.
Thus, $n = 0$ and $n \neq 0$, a contradiction.
Therefore, $s \neq 0$.

Observe that

$$\begin{aligned} |a^s| &= \frac{n}{\gcd(s,n)} \\ &= \frac{st}{\gcd(s,st)} \\ &= \frac{st}{s\gcd(1,t)} \\ &= \frac{t}{\gcd(1,t)} \\ &= \frac{t}{1} \\ &= t \\ &= \frac{n}{s}. \end{aligned}$$

Therefore, a^s has order $\frac{n}{s}$. $\square$

Proposition 33. ***The order of*** a ***is the same as the order of*** a^{-1}***.***

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

Let $a \in G$.

Then $|a| = |a^{-1}|$.

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

Suppose a has finite order.

Let n be the order of a.

Then n is the least positive integer such that $a^n = e$ and $a^k = e$ iff $n|k$ for all $k \in \mathbb{Z}$.

Observe that $(a^{-1})^n = (a^n)^{-1} = e^{-1} = e$.

Since $n \in \mathbb{Z}^+$ and $(a^{-1})^n = e$, then a^{-1} has finite order.

Let m be the order of a^{-1}.

Then m is the least positive integer such that $(a^{-1})^m = e$ and $(a^{-1})^k = e$ iff $m|k$ for all $k \in \mathbb{Z}$.

Since $n \in \mathbb{Z}$, then $(a^{-1})^n = e$ iff $m|n$.

Since $(a^{-1})^n = e$, then we conclude $m|n$.

Observe that $e = (a^{-1})^m = a^{-m}$.

Since $a^k = e$ iff $n|k$ for all $k \in \mathbb{Z}$ and $-m \in \mathbb{Z}$, then $a^{-m} = e$ iff $n|(-m)$.

Since $a^{-m} = e$, then we conclude $n|(-m)$, so $n|m$.

Since $m|n$ and $n|m$, then $m = n$.

Therefore, $|a| = n = m = |a^{-1}|$, so $|a| = |a^{-1}|$, as desired. $\square$

Proposition 34. ***The order of*** ab ***is the same as the order of*** ba***.***

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

Let $a, b \in G$.

Then $|ab| = |ba|$.

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

Suppose ab has finite order.

Let n be the order of ab.

Then n is the least positive integer such that $(ab)^n = e$ and $(ab)^k = e$ iff $n|k$ for all integers k.

Right multiply by a to obtain $(ab)^n a = ea = a$.

Thus, $(ab)(ab)...(ab)a = a$, so $a(ba)(ba)...(ba) = a$.

Hence, $a(ba)^n = a = ae$, so by left cancellation we obtain $(ba)^n = e$.

Since $n \in \mathbb{Z}^+$ and $(ba)^n = e$, then ba has finite order.

Let m be the order of ba.

Then m is the least positive integer such that $(ba)^m = e$ and $(ba)^n = e$ iff $m|n$.

Since $(ba)^n = e$, then we conclude $m|n$.

Since $(ba)^m = e$, left multiply by a to obtain $a(ba)^m = ae = a$.

Thus, $a(ba)(ba)...(ba) = a$, so $(ab)(ab)...(ab)a = a$.

Hence, $(ab)^m a = a = ea$, so by right cancellation we obtain $(ab)^m = e$.

Since $m \in \mathbb{Z}$ and $(ab)^m = e$ iff $n|m$, then we conclude $n|m$.

Since $m|n$ and $n|m$, then $m = n$.
Therefore, $|ab| = n = m = |ba|$, so $|ab| = |ba|$. $\square$

Proposition 35. ***Every element of a finite group has finite order.***
Let $(G, *)$ be a finite group with identity $e \in G$.
Then $(\forall a \in G)(\exists k \in \mathbb{Z}^+)(a^k = e)$.

Proof. Since G is finite, let n be the number of elements in G.
Then $|G| = n$.
Since G is a group, then $G \neq \emptyset$, so n is a positive integer.
Let $a \in G$.
Either all distinct positive integer powers of a are distinct or not.
We consider these cases separately.
Case 1: Suppose all distinct positive integer powers of a are distinct.
Let $S = \{a, a^2, a^3, ..., a^n\}$.
Then $S = \{a^k : 1 \leq k \leq n, k \in \mathbb{Z}\}$.
By the laws of exponents, $a^n \in G$ for all $n \in \mathbb{Z}$, so $S \subset G$.
Since G is finite and $|S| = n = |G|$ and $S \subset G$, then $S = G$.
Since $e \in G$, then this implies $e \in S$.
Hence, there exists an integer k such that $1 \leq k \leq n$ and $e = a^k$.
Therefore, there exists a positive integer k such that $a^k = e$.
Case 2: Suppose not all distinct positive integer powers of a are distinct.
Then there exist distinct positive integer powers of a that are the same.
Hence, there exist distinct positive integers s and t such that $a^s = a^t$.
Thus, $s \neq t$ and $a^s = a^t$.
Since $s \neq t$, then either $s < t$ or $s > t$.
Without loss of generality, assume $s < t$.
Then $t > s$, so $t - s > 0$.
Hence, $t - s$ is a positive integer.
Observe that

$$\begin{aligned} a^{t-s} &= a^t * a^{-s} \\ &= a^s * a^{-s} \\ &= a^{s-s} \\ &= a^0 \\ &= e. \end{aligned}$$

Therefore, there exists a positive integer $t - s$ such that $a^{t-s} = e$. $\square$

Theorem 36. ***Finite Subgroup Test***
Let H be a nonempty finite subset of a group $(G, *)$.
Then $H < G$ iff H is closed under $*$ of G.

Proof. We prove if $H < G$, then H is closed under $*$ of G.
Suppose $H < G$.
Then H is a subgroup of G, so H is a group under the binary operation of G.
Hence, $*$ is a binary operation on H, so H is closed under $*$ of G. $\square$

Proof. Conversely, we prove if H is closed under $*$ of G, then $H < G$.

Suppose H is closed under $*$ of G.
Then $a * b \in H$ for all $a, b \in H$.
Since H is a nonempty set, then there exists an element $a \in H$.

We first prove $a^k \in H$ for all $k \in \mathbb{Z}^+$ by induction on k.
Define predicate $p(k) : a^k \in H$ over $\mathbb{Z}^+$.
Basis:
Since $a \in H$ and $a^1 = a$, then $a^1 \in H$, so $p(1)$ is true.
Induction:
Let $k \in \mathbb{Z}^+$ such that $p(k)$ is true.
Then $a^k \in H$.
Since $a * b \in H$ for all $a, b \in H$ and $a^k \in H$ and $a \in H$, then $a^k * a \in H$, so $a^{k+1} \in H$.
Hence, $p(k+1)$ is true.
Thus, $p(k)$ implies $p(k+1)$ for all $k \in \mathbb{Z}^+$.
Since $p(1)$ is true and $p(k)$ implies $p(k+1)$ for all $k \in \mathbb{Z}^+$, then by induction, $p(k)$ is true for all $k \in \mathbb{Z}^+$.
Therefore, $a^k \in H$ for all $k \in \mathbb{Z}^+$.

Since H is finite, then H contains a finite number of elements.
Let n be the number of elements in H.
Then $n \in \mathbb{Z}$.
Since H is not empty, then $n \geq 1$.
Since $a^k \in H$ for all $k \in \mathbb{Z}^+$ and H contains exactly n elements, then H consists of n distinct powers of a, so $H = \{a, a^2, a^3, ..., a^n\} = \{a^i : 1 \leq i \leq n\}$.
Since $a^k \in H$ for all $k \in \mathbb{Z}^+$ and $n + 1 \in \mathbb{Z}^+$, then $a^{n+1} \in H$, so $a^{n+1} = a^k$ for some integer k with $1 \leq k \leq n$.
Since $1 \leq k \leq n$ and $n < n + 1$, then $1 \leq k \leq n < n + 1$, so $1 \leq k < n + 1$.
Thus, $k < n + 1$, so $k \neq n + 1$.
Since $a \in H$ and $H \subset G$, then $a \in G$.
Since G is a group and $a \in G$ and $a^k = a^{n+1}$ and k and $n + 1$ are integers and $k \neq n + 1$, then a has finite order.
Let m be the order of a.
Then m is the least positive integer such that $a^m = e$.
Since $a^k \in H$ for all $k \in \mathbb{Z}^+$ and $m \in \mathbb{Z}^+$, then $a^m \in H$, so $e \in H$.
Since $a^m \in H$, then $1 \leq m \leq n$.

Suppose $m < n$.
Then $n - m > 0$.
Since $a^k \in H$ for all $k \in \mathbb{Z}^+$ and $n - m \in \mathbb{Z}^+$, then $a^{n-m} \in H$.

Observe that

$$\begin{aligned}
a^{n-m} &= e * a^{n-m} \\
&= a^m * a^{n-m} \\
&= a^{m+n-m} \\
&= a^n.
\end{aligned}$$

Since $a^{n-m} = a^n$ and $a^{n-m} \in H$ and $a^n \in H$, then we must conclude $n - m = n$.

Hence, $n - n = m$, so $m = 0$.

But, this contradicts that m is positive, so m cannot be less than n.

Since $m \leq n$ and m is not less than n, then m must equal n, so $m = n$.

Therefore, the order of a is n, so $a^n = e$.

Since $n \in \mathbb{Z}^+$, then either $n > 1$ or $n = 1$.

We consider these cases separately.

Case 1: Suppose $n = 1$.

Then $e = a^1 = a$.

Thus, $a \in H$ implies $a \in \{e\}$.

Hence, $H \subset \{e\}$.

Since $e \in H$, then $\{e\} \subset H$.

Thus, $H \subset \{e\}$ and $\{e\} \subset H$, so $H = \{e\}$.

Since the trivial group is a subgroup of every group, then $H < G$.

Case 2: Suppose $n > 1$.

Observe that

$$\begin{aligned}
a * a^{n-1} &= a^{1+n-1} \\
&= a^n \\
&= e \\
&= a^n \\
&= a^{n-1+1} \\
&= a^{n-1} * a.
\end{aligned}$$

Since $a * a^{n-1} = e = a^{n-1} * a$, then a^{n-1} is the inverse of a.

Therefore, $a^{-1} = a^{n-1}$.

Since $n \in \mathbb{Z}$ and $n > 1$, then $n \geq 2$, so $n - 1 \geq 1$.

Since $1 \leq n - 1$ and $n - 1 < n$, then $1 \leq n - 1 < n$.

Since $n - 1 \in \mathbb{Z}$ and $1 \leq n - 1 < n$, then $a^{n-1} \in H$, so $a^{-1} \in H$.

Since a is arbitrary, then $a^{-1} \in H$ for all $a \in H$.

Since H is a nonempty subset of G and $a * b \in H$ for all $a, b \in H$ and $a^{-1} \in H$ for all $a \in H$, then by the two-step subgroup test, H is a subgroup of G, so $H < G$.

Therefore, in all cases, $H < G$, as desired. $\square$

Cyclic subgroups

Theorem 37. ***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.

Proof. Let $H = \{g^n : n \in \mathbb{Z}\}$.
Let $e \in G$ be the identity element of G.
We must prove $H < G$.

Since $g^0 = e$ and $0 \in \mathbb{Z}$, then $e \in H$, so $H \neq \emptyset$.

We prove $H \subset G$.
Let $h \in H$.
Then $h = g^k$ for some $k \in \mathbb{Z}$.
By the law of exponents for a group G, if $a \in G$, then $a^n \in G$ for all $n \in \mathbb{Z}$.
Since G is a group and $g \in G$ and $k \in \mathbb{Z}$, then we conclude $g^k \in G$, so $h \in G$.
Therefore, $h \in H$ implies $h \in G$, so $H \subset G$.

Since $H \subset G$ and $H \neq \emptyset$, then H is a nonempty subset of G.

We prove H is closed under the binary operation of G.
Let $g^i, g^j \in H$.
Then $i, j \in \mathbb{Z}$.
Since $g^i * g^j = g^{i+j}$ and $i + j \in \mathbb{Z}$, then $g^{i+j} \in H$, so $g^i * g^j \in H$.
Therefore, $g^i * g^j \in H$ for all $g^i, g^j \in H$.

We prove H is closed under inverses.
Let $g^m \in H$.
Then $m \in \mathbb{Z}$.
Since $g^m \in H$ and $H \subset G$, then $g^m \in G$.
Since G is a group and $g^m \in G$, then the inverse of g^m exists.
Let $(g^m)^{-1} \in G$ be the inverse of g^m.
Then $(g^m)^{-1} = g^{-m}$ and $g^m * g^{-m} = g^{m-m} = g^0 = e = g^{-m+m} = g^{-m} * g^m$.
Since $-m \in \mathbb{Z}$, then $g^{-m} \in H$, so $(g^m)^{-1} \in H$.
Therefore, $(g^m)^{-1} \in H$ for all $g^m \in H$.

Since H is a nonempty subset of G and $g^i * g^j \in H$ for all $g^i, g^j \in H$ and $(g^m)^{-1} \in H$ for all $g^m \in H$, then by the two-step subgroup test, H is a subgroup of G, so $H < G$. $\square$

Proof. To prove H is the smallest subgroup of G containing g, let $K < G$ and $g \in K$.

We must prove $H < K$.

We prove $H \subset K$.

Let $h \in H$.

Then $h = g^k$ for some $k \in \mathbb{Z}$.

By the law of exponents for a group K, if $a \in K$, then $a^n \in K$ for all $n \in \mathbb{Z}$.

Since $K < G$, then K is a subgroup of G, so K is a group.

Since $g \in K$ and $k \in \mathbb{Z}$, then we conclude $g^k \in K$, so $h \in K$.

Therefore, $h \in H$ implies $h \in K$, so $H \subset K$.

Since $H \subset K$ and $H \neq \emptyset$, then H is a nonempty subset of K.

We prove H is closed under the binary operation on K.

Since $K < G$, then K is closed under the binary operation on G, so the binary operation on K is the binary operation on G.

Since $H < G$, then H is closed under the binary operation on G, so the binary operation on H is the binary operation on G.

Since the binary operation on H is the binary operation on G and the binary operation on G is the binary operation on K, then the binary operation on H is the binary operation on K.

Therefore, H is closed under the binary operation on K.

We prove $a^{-1} \in H$ for all $a \in H$.

Since $H < G$, then H is a group under the binary operation of G, so for every $a \in H$, there exists $a^{-1} \in H$ such that $a * a^{-1} = a^{-1} * a = e$.

Therefore, $a^{-1} \in H$ for all $a \in H$.

Since H is a nonempty subset of K and H is closed under the binary operation on K and $a^{-1} \in H$ for all $a \in H$, then by the two-step subgroup test, H is a subgroup of K, so $H < K$. $\square$

Theorem 38. *Every cyclic group is abelian.*

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

Then $G = \{g^n : n \in \mathbb{Z}\}$ for some generator $g \in G$.

Let $a, b \in G$.

Since $a \in G$, then $a = g^k$ for some $k \in \mathbb{Z}$.

Since $b \in G$, then $b = g^m$ for some $m \in \mathbb{Z}$.

Observe that

$$\begin{aligned} a * b &= g^k * g^m \\ &= g^{k+m} \\ &= g^{m+k} \\ &= g^m * g^k \\ &= b * a. \end{aligned}$$

Since $a * b = b * a$, then $*$ is commutative, so G is abelian. ◻

Theorem 39. *Every subgroup of a cyclic group is cyclic.*

Proof. Let $(G, *)$ be a cyclic group.
Let $(H, *)$ be an arbitrary subgroup of $(G, *)$.
We must prove H is cyclic.

Let $e \in G$ be the identity of G.
Since H is a subgroup of G, then either H is the trivial group or H is not the trivial group.
We consider these cases separately.
Case 1: Suppose H is the trivial group.
Then $H = \{e\}$.
Since $e^n = e$ for all $n \in \mathbb{Z}$, then the cyclic group generated by e is $\langle e \rangle = \{e^n : n \in \mathbb{Z}\} = \{e\} = H$.
Therefore, H is cyclic.
Case 2: Suppose H is not the trivial group.
Then H contains at least one element that is not the identity element of G.
Hence, there exists $a \in H$ such that $a \neq e$.
Since G is cyclic, then there exists $g \in G$ such that $G = \{g^k : k \in \mathbb{Z}\}$.
Since $H < G$, then $H \subset G$.
Since $a \in H$ and $H \subset G$, then $a \in G$, so there exists $k \in \mathbb{Z}$ such that $a = g^k$.

Since $g^0 = e \neq a = g^k$, then $k \neq 0$, so either $k < 0$ or $k > 0$.
Without loss of generality, assume $k > 0$.
Then there exists $k \in \mathbb{Z}^+$ such that $a = g^k$.
Since $a \in H$ and $a = g^k$, then $g^k \in H$.

Let $S = \{n \in \mathbb{Z}^+ : g^n \in H\}$.
Then $S \subset \mathbb{Z}^+$
Since $k \in \mathbb{Z}^+$ and $g^k \in H$, then $k \in S$, so $S \neq \emptyset$.
Since $S \subset \mathbb{Z}^+$ and $S \neq \emptyset$, then S contains a least element by the well ordering property of $\mathbb{Z}^+$.
Let m be the least element of S.
Then $m \in S$ and $m \leq n$ for all $n \in S$.
Since $m \in S$, then $m \in \mathbb{Z}^+$ and $g^m \in H$.

Let $b \in H$ be arbitrary.

Since $b \in H$ and $H \subset G$, then $b \in G$, so there exists $s \in \mathbb{Z}$ such that $b = g^s$.

Since $b \in H$ and $b = g^s$, then $g^s \in H$.

We divide s by m.

By the division algorithm, there exist unique integers q, r such that $s = mq + r$ and $0 \leq r < m$.

Observe that

$$\begin{aligned} b &= g^s \\ &= g^{mq+r} \\ &= g^{mq} * g^r \\ &= (g^m)^q * g^r. \end{aligned}$$

Hence, $g^s = (g^m)^q * g^r$.

We left multiply by $[(g^m)^q]^{-1}$ to obtain $g^r = [(g^m)^q]^{-1} * g^s = (g^m)^{-q} * g^s$.

By the laws of exponents for a multiplicative group, if G is a group and $a \in G$, then $a^n \in G$ for all $n \in \mathbb{Z}$.

Since H is a group and $g^m \in H$ and $-q \in \mathbb{Z}$, then we conclude $(g^m)^{-q} \in H$.

Since H is a group, then H is closed under its binary operation $*$.

Since $(g^m)^{-q} \in H$ and $g^s \in H$, then we conclude $g^r \in H$.

Since $0 \leq r < m$, then $0 \leq r$ and $r < m$.

Since $0 \leq r$, then either $r > 0$ or $r = 0$.

Suppose $r > 0$.

Since r is an integer and $r > 0$, then $r \in \mathbb{Z}^+$.

Since $r \in \mathbb{Z}^+$ and $g^r \in H$, then $r \in S$, so $m \leq r$.

Thus, we have $r < m$ and $r \geq m$, a violation of trichotomy law for integers.

Therefore, r cannot be greater than zero.

Since either $r > 0$ or $r = 0$, we must conclude $r = 0$, so $s = mq + r = mq + 0 = mq$.

Thus,

$$\begin{aligned} b &= g^s \\ &= g^{mq} \\ &= (g^m)^q. \end{aligned}$$

Let $H' = \{(g^m)^n : n \in \mathbb{Z}\}$.

Since $b = (g^m)^q$ and $q \in \mathbb{Z}$, then $b \in H'$.

Therefore, $b \in H$ implies $b \in H'$, so $H \subset H'$.

We prove $H' \subset H$.

Let $h' \in H'$.

Then $h' = (g^m)^n$ for some $n \in \mathbb{Z}$.

By the laws of exponents for a multiplicative group, if G is a group and $a \in G$, then $a^n \in G$ for all $n \in \mathbb{Z}$.

Since H is a group and $g^m \in H$ and $n \in \mathbb{Z}$, then we conclude $(g^m)^n \in H$, so $h' \in H$.

Therefore, $h' \in H'$ implies $h' \in H$, so $H' \subset H$.

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

Therefore, $H = H' = \{(g^m)^n : n \in \mathbb{Z}\}$ is the cyclic subgroup generated by the element $g^m \in H$, so H is cyclic. □

Corollary 40. *The only subgroups of* $(\mathbb{Z}, +)$ *are* $(n\mathbb{Z}, +)$ *for all* $n \in \mathbb{Z}$.

Proof. To prove the only subgroups of $\mathbb{Z}$ are $n\mathbb{Z}$ for all $n \in \mathbb{Z}$, we prove the set of all subgroups of $\mathbb{Z}$ is the set of all $n\mathbb{Z}$.

Let S be the set of all subgroups of $\mathbb{Z}$.

Then $S = \{H : H < \mathbb{Z}\}$.

Let $T = \{n\mathbb{Z} : n \in \mathbb{Z}\}$.

We must prove $S = T$.

We prove $S \subset T$.

Let $H \in S$.

Then $H < \mathbb{Z}$, so H is a subgroup of $\mathbb{Z}$.

Thus, $H \subset \mathbb{Z}$.

Every subgroup of a cyclic group is cyclic.

Since H is a subgroup of $\mathbb{Z}$ and $\mathbb{Z}$ is cyclic, then H is cyclic.

Therefore, there exists $h \in H$ such that $H = \{nh : n \in \mathbb{Z}\} = h\mathbb{Z}$.

Since $h \in H$ and $H \subset \mathbb{Z}$, then $h \in \mathbb{Z}$.

Since $H = h\mathbb{Z}$ and $h \in \mathbb{Z}$, then $H \in T$.

Therefore, $H \in S$ implies $H \in T$, so $S \subset T$.

We prove $T \subset S$.

Let $G \in T$.

Then $G = n\mathbb{Z}$ for some $n \in \mathbb{Z}$.

Since $n\mathbb{Z}$ is a subgroup of $\mathbb{Z}$, then $G < \mathbb{Z}$, so $G \in S$.

Therefore, $G \in T$ implies $G \in S$, so $T \subset S$.

Since $S \subset T$ and $T \subset S$, then $S = T$. □

Theorem 41. ***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.*

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

Since G is a group and $a \in G$, then a generates a cyclic subgroup of G.

Let H be the cyclic subgroup of G generated by a.

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

Either there exists $k \in \mathbb{Z}^+$ such that $a^k = e$ or there does not exist $k \in \mathbb{Z}^+$ such that $a^k = e$.

We consider these cases separately.

Case 1: Suppose there exists $k \in \mathbb{Z}^+$ such that $a^k = e$.

Then a has finite order.

Let n be the order of a.

Then n is the least positive integer such that $a^n = e$.

Let $H' = \{a^0, a^1, a^2, ..., a^{n-1}\} = \{a^k : k \in \mathbb{Z} \wedge 0 \leq k < n\}$.

Then $|H'| = n$ and $H' \subset H$.

We must prove $H = H'$ and $|H| = n$.

Let $a^k \in H$.

Then k is an integer.

We divide k by n.

By the division algorithm, there exist unique integers q, r such that $k = nq+r$ and $0 \leq r < n$.

Observe that

$$\begin{aligned} a^k &= a^{nq+r} \\ &= a^{nq} * a^r \\ &= (a^n)^q * a^r \\ &= e^q * a^r \\ &= e * a^r \\ &= a^r. \end{aligned}$$

Hence, there exists an integer r such that $0 \leq r < n$ and $a^k = a^r$, so $a^k \in H'$.

Thus, $a^k \in H$ implies $a^k \in H'$, so $H \subset H'$.

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

Therefore, $|H| = |H'| = n$, so $|H| = n$.

Case 2: Suppose there does not exist $k \in \mathbb{Z}^+$ such that $a^k = e$.

Then a has infinite order, so a does not have finite order.

If $a^s = a^t$ and $s \neq t$ for some $s, t \in \mathbb{Z}$, then a has finite order.

Hence, if a does not have finite order, then there does not exist $s, t \in \mathbb{Z}$ with $s \neq t$ and $a^s = a^t$.

Since a does not have finite order, then we conclude there does not exist $s, t \in \mathbb{Z}$ with $s \neq t$ and $a^s = a^t$.

Hence, $a^s \neq a^t$ for every distinct $s, t \in \mathbb{Z}$, so every integer power of a is distinct.

Therefore, the cyclic subgroup generated by a is $\langle a \rangle = \{a^k : k \in \mathbb{Z}\} = \{..., a^{-2}, a^{-1}, a^0, a^1, a^2, a^3, ..., \}$, so $\langle a \rangle$ is infinite. $\square$

Proposition 42. ***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 $\gcd(k,n) = 1$.

Proof. Suppose $g \in G$ is a generator of G.
Then $G = \{g^k : k \in \mathbb{Z}\}$.
Let S be the set of all generators of G.
Then $S = \{s \in G : G = \langle s \rangle\}$.
Let $T = \{g^k : \gcd(k,n) = 1, k \in \mathbb{Z}\}$.
We must prove $S = T$.

We prove $S \subset T$.
Since $g \in G$ and $G = \{g^k : k \in \mathbb{Z}\} = \langle g \rangle$, then $g \in S$, so $S \neq \emptyset$.
The order of g is the order of the cyclic subgroup generated by g.
Therefore, $|g| = |\langle g \rangle| = |\{g^k : k \in \mathbb{Z}\}| = |G| = n$, so g has finite order n.
Let $s \in S$.
Then $s \in G$ and $G = \langle s \rangle$.
Since $s \in G$, then there exists $k \in \mathbb{Z}$ such that $s = g^k$.
The order of s is the order of the cyclic subgroup generated by s.
Hence, $|s| = |\langle s \rangle| = |G| = n$.
Since g has finite order n, then $|s| = |g^k| = \frac{n}{\gcd(k,n)}$.
Thus, $n = |s| = \frac{n}{\gcd(k,n)}$, so $n \gcd(k,n) = n$.
Consequently, $\gcd(k,n) = 1$.
Since there exists $k \in \mathbb{Z}$ such that $s = g^k$ and $\gcd(k,n) = 1$, then $s \in T$, so $S \subset T$.

We prove $T \subset S$.
Let $t \in T$.
Then there exists $m \in \mathbb{Z}$ such that $t = g^m$ and $\gcd(m,n) = 1$.
By the law of exponents, $g^n \in G$ for all $n \in \mathbb{Z}$.
Since $m \in \mathbb{Z}$, then $g^m \in G$, so $t \in G$.
Every element of a group G generates a cyclic subgroup of G.
Since $t \in G$, then t generates a cyclic subgroup of G, so $\langle t \rangle$ is a subgroup of G.
Hence, $\langle t \rangle$ is a subset of G.
Since $|G| = n$, then G is a finite group.
Every element of a finite group has finite order.
Thus, every element of G has finite order.
Since $t \in G$, then t has finite order.
Thus, $|t| = |g^m| = \frac{n}{\gcd(m,n)} = \frac{n}{1} = n = |G|$.
The order of t is the order of the cyclic subgroup generated by t.
Hence, $|t| = |\langle t \rangle|$.
Thus, $|G| = |t| = |\langle t \rangle|$.

Since $\langle t\rangle$ is a subset of G and G is finite and $|G| = |\langle t\rangle|$, then $G = \langle t\rangle$.
Since $t \in G$ and $G = \langle t\rangle$, then $t \in S$, so $T \subset S$.

Since $S \subset T$ and $T \subset S$, then $S = T$, as desired. $\square$

Corollary 43. *The generators of* $(\mathbb{Z}_n, +)$ *are congruence classes* $[k]$ *such that* $k \in \mathbb{Z}^+$ *and* $1 \leq k \leq n$ *and* $\gcd(k, n) = 1$.

Proof. Let $n \in \mathbb{Z}^+$.
Observe that $(\mathbb{Z}_n, +)$ is a cyclic group of order n.
Since $[1] \in \mathbb{Z}_n$ is a generator of $\mathbb{Z}_n$, then by the previous proposition 42, the generators of $\mathbb{Z}_n$ are elements $k[1]$ such that $\gcd(k, n) = 1$ for $k \in \mathbb{Z}$.
Since $k \in \mathbb{Z}$, then $k[1] = [k]$.
Since $\mathbb{Z}_n = \{[1], [2], ..., [n-1], [n]\} = \{[k] : 1 \leq k \leq n\}$, then $k \in \mathbb{Z}^+$.
Therefore, the generators of $\mathbb{Z}_n$ are congruence classes $[k] \in \mathbb{Z}_n$ such that $k \in \mathbb{Z}^+$ and $1 \leq k \leq n$ and $\gcd(k, n) = 1$. $\square$

Theorem 44. *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* $\{a_1, a_2, ..., a_n\}$.

Solution. We must prove
1. $\langle a_1, a_2, ..., a_n\rangle$ is a subgroup of $(G, *)$.
2. To prove $\langle a_1, a_2, ..., a_n\rangle$ is the smallest subgroup of G that contains $\{a_1, a_2, ..., a_n\}$, we must prove for every subgroup K of G such that $\{a_1, a_2, ..., a_n\} \subset K$, $\langle a_1, a_2, ..., a_n\rangle \subset K$. $\square$

Proof. Let $H = \langle a_1, a_2, ..., a_n\rangle$. Let $N_0 = \{0, 1, 2, 3, ...\}$.
Then $H = \{b_1^{\epsilon_1} \cdot b_2^{\epsilon_2} \cdots b_k^{\epsilon_k} : k \in N_0, b_i \in \{a_1, ..., a_n\}, \epsilon_i \in \mathbb{Z}\}$.
Let $x \in H$. Then there exists $k \in N_0$ and for each $i \in \{1, ..., k\}$ there exists $b_i \in \{a_1, ..., a_n\}$ and integer ϵ_i such that $x = b_1^{\epsilon_1} b_2^{\epsilon_2} \cdots b_k^{\epsilon_k}$. Let i be an arbitrary integer in $\{1, 2, ..., k\}$. Since $b_i \in \{a_1, ..., a_n\}$ and $\{a_1, ..., a_n\} \subset G$, then $b_i \in G$. Every integer power of b_i is an element of the group that contains b_i. Thus, $b_i^{\epsilon_i} \in G$. Since i is arbitrary, then $b_i^{\epsilon_i} \in G$ for each i. By closure of G we have $b_1^{\epsilon_1} b_2^{\epsilon_2} \cdots b_k^{\epsilon_k} \in G$, so $x \in G$. Hence, $x \in H$ implies $x \in G$, so $H \subset G$.
Let e be the identity element of G. If $k = 0$, then $b_1^{\epsilon_1} \cdot b_2^{\epsilon_2} \cdots b_k^{\epsilon_k}$ is a product of zero factors. By definition, this implies $b_1^{\epsilon_1} \cdot b_2^{\epsilon_2} \cdots b_k^{\epsilon_k} = e$. Thus, $e \in H$, so $H \neq \emptyset$.
Let $x, y \in H$. Then there exists $k \in N_0$ and for each i in $\{1, ..., k\}$ there exist $b_i \in \{a_1, ..., a_n\}$ and integer ϵ_i such that $x = b_1^{\epsilon_1} b_2^{\epsilon_2} \ldots b_k^{\epsilon_k}$ and there exists $m \in N_0$ and for each j in $\{1, ..., m\}$ there exist $c_j \in \{a_1, ..., a_n\}$ and integer δ_j such that $y = c_1^{\delta_1} c_2^{\delta_2} \ldots c_m^{\delta_m}$. Observe that

$$\begin{aligned}
xy^{-1} &= (b_1^{\epsilon_1} b_2^{\epsilon_2} \ldots b_k^{\epsilon_k})(c_1^{\delta_1} c_2^{\delta_2} \ldots c_m^{\delta_m})^{-1} \\
&= (b_1^{\epsilon_1} b_2^{\epsilon_2} \ldots b_k^{\epsilon_k})(c_m^{-\delta_m} c_{m-1}^{-\delta_{m-1}} \ldots c_1^{-\delta_1}) \\
&= b_1^{\epsilon_1} b_2^{\epsilon_2} \ldots b_k^{\epsilon_k} c_m^{-\delta_m} c_{m-1}^{-\delta_{m-1}} \ldots c_1^{-\delta_1}.
\end{aligned}$$

Hence, xy^{-1} is a product of $k+m$ factors and $k+m \in N_0$ and each factor has a base in $\{a_1, ..., a_n\}$ and an integer exponent. Therefore, $xy^{-1} \in H$.

Hence, H is a subgroup of G.

To prove H is the smallest subgroup of G containing $\{a_1, a_2, ..., a_n\}$, let K be an arbitrary subgroup of G such that $\{a_1, a_2, ..., a_n\} \subset K$.

We must prove $H \subset K$.

Let $x \in H$. Then there exists $k \in N_0$ and for each i in $\{1, 2, ..., k\}$ there exist $b_i \in \{a_1, a_2, ..., a_n\}$ and integer ϵ_i such that $x = b_1^{\epsilon_1} b_2^{\epsilon_2} \cdots b_k^{\epsilon_k}$.

Let i be an arbitrary element of $\{1, 2, ..., k\}$. Since $b_i \in \{a_1, a_2, ..., a_n\}$ and $\{a_1, a_2, ..., a_n\} \subset K$, then $b_i \in K$. Every integer power of b_i is an element of the group that contains b_i. Thus, $b_i^{\epsilon_i} \in K$. Since i is arbitrary, then $b_i^{\epsilon_i} \in K$ for every i in $\{1, 2, ..., k\}$. Since K is a subgroup of G, then K is closed under the binary operation of G. Hence, $b_1^{\epsilon_1} b_2^{\epsilon_2} \cdots b_k^{\epsilon_k} \in K$, so $x \in K$.

Thus, $x \in H$ implies $x \in K$, so $H \subset K$, as desired. $\square$

Theorem 45. *Let $(G, *)$ be a group.*

Let $S \subset G$.

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

Proof. Let H_i be a subgroup of G such that $S \subset H_i$. Let I be some index set. Then $T = \{H_i : i \in I\}$ is the collection of all subgroups of G that contain S. Since $G < G$ and $S \subset G$, then $G \in T$. Hence, T is not empty.

Let H be the intersection of all the subgroups in T. Then $H = \cap_{i \in I} H_i = \{x : x \in H_i \text{ for all } i \in I\}$.

The intersection of a collection of subgroups is a subgroup. Hence, $H < G$.

We prove $S \subset H$. Let $x \in S$. To prove $x \in H$, we must prove $x \in H_i$ for all $i \in I$. Let $i \in I$. Then H_i is an arbitrary subgroup of G that contains S. Thus, $S \subset H_i$. Since $x \in S$ and $S \subset H_i$, then $x \in H_i$. Since i is arbitrary, then $x \in H_i$ for all $i \in I$. Thus, $x \in H$. Hence, $x \in S$ implies $x \in H$, so $S \subset H$.

To prove H is the smallest subgroup of G that contains S, we must prove $H < K$ for every subgroup K that contains S.

Let $i \in I$. Then H_i is an arbitrary subgroup of G that contains S.

We prove $H < H_i$.

We prove $H \subset H_i$. Let $x \in H$. Then $x \in H_i$ for all $i \in I$. In particular, $x \in H_i$. Hence, $x \in H$ implies $x \in H_i$, so $H \subset H_i$.

We prove H is closed under the binary operation of H_i. Since $H_i < G$, then H_i is closed under the binary operation of G. Thus, the binary operation of H_i is the same as in G. Since $H < G$, then H is closed under the binary operation of G. Hence, H is closed under the binary operation of H_i.

Let e be the identity of G. Since $H_i < G$, then $e \in H_i$. Since $H < G$, then $e \in H$. Thus, the identity of H_i is contained in H.

Let $a \in H$. We prove the inverse of a is in H. Since $H < G$, then $H \subset G$. Thus, $a \in G$. Since G is a group, then the inverse of a exists in G. Let b be the inverse of a in G. Then $b \in G$ and $ab = e$. Since $H < G$, then $b \in H$.

Since $a \in H$ and $H \subset H_i$, then $a \in H_i$. Since H_i is a group, then the inverse of a exists in H_i. Let b' be the inverse of a in H_i. Then $b' \in H_i$ and $ab' = e$.

Thus, $ab = e = ab'$, so $ab = ab'$. Since $b' \in H_i$ and $H_i \subset G$, then $b' \in G$. Hence, $a, b, b' \in G$, so by the left cancellation law, we have $b = b'$. Since $b' = b$ and $b \in H$, then $b' \in H$. Thus, the inverse of a in H_i is in H.

Therefore, $H < H_i$. ☐

Permutation Groups

Theorem 46. $(S_X, \circ)$ ***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.*

Proof. We prove $\circ$ is a binary operation on S_X.

Let $\sigma : X \to X$ and $\tau : X \to X$ be elements of S_X.

Then $\sigma : X \to X$ and $\tau : X \to X$ are permutations of X.

Hence, σ and τ are bijective functions, so σ and τ are bijections.

Let $\sigma \circ \tau : X \to X$ be the function defined by $(\sigma \circ \tau)(x) = \sigma(\tau(x))$ for all $x \in X$.

Since the composition of functions is a function and σ is a function and τ is a function, then $\sigma \circ \tau$ is a function and $\sigma \circ \tau$ is unique.

Since the composition of bijections is a bijection and σ is a bijection and τ is a bijection, then $\sigma \circ \tau$ is a bijection, so $\sigma \circ \tau$ is a permutation.

Therefore, $\sigma \circ \tau$ is an element of S_X, so $\circ$ is a binary operation on S_X.

We prove $\circ$ is associative.

Since function composition is associative, then $(\sigma \circ \tau) \circ \mu = \sigma \circ (\tau \circ \mu)$ for all $\sigma, \tau, \mu \in S_X$.

Therefore, $\circ$ is associative.

We prove the identity map is an identity for $\circ$.

Let $id : X \to X$ be the identity map defined by $id(x) = x$ for all $x \in X$.

Since the identity map is a bijection of X, then the identity map is a permutation of X, so $id \in S_X$.

Let $\sigma \in S_X$.

Let $x \in X$.

Observe that

$$\begin{aligned}
(id \circ \sigma)(x) &= id(\sigma(x)) \\
&= \sigma(x) \\
&= \sigma(id(x)) \\
&= (\sigma \circ id)(x).
\end{aligned}$$

Thus, $(id \circ \sigma)(x) = \sigma(x) = (\sigma \circ id)(x)$ for all $x \in X$, so $id \circ \sigma = \sigma = \sigma \circ id$.

Since $id \in S_X$ and $id \circ \sigma = \sigma = \sigma \circ id$, then the identity map id is an identity for $\circ$.

We prove every permutation in S_X has an inverse in S_X.

Let $\sigma \in S_X$.

Then σ is a permutation of X, so $\sigma : X \to X$ is a bijective function.

A function is invertible iff it is bijective.

Hence, σ is invertible, so the inverse function of σ exists and is unique.

Let $\tau : X \to X$ defined by $\tau(y) = x$ iff $\sigma(x) = y$ be the inverse function of σ.

Let $x \in X$.

Then $\tau(x) = y$ iff $\sigma(y) = x$.

Observe that

$$\begin{aligned}(\sigma \circ \tau)(x) &= \sigma(\tau(x)) \\ &= \sigma(y) \\ &= x \\ &= id(x).\end{aligned}$$

Thus, $(\sigma \circ \tau)(x) = id(x)$ for all $x \in X$, so $\sigma \circ \tau = id$.

Let $x \in X$.

Then $\sigma(x) = y$ iff $\tau(y) = x$.

Observe that

$$\begin{aligned}(\tau \circ \sigma)(x) &= \tau(\sigma(x)) \\ &= \tau(y) \\ &= x \\ &= id(x).\end{aligned}$$

Thus, $(\tau \circ \sigma)(x) = id(x)$ for all $x \in X$, so $\tau \circ \sigma = id$.

Hence, $\tau \circ \sigma = id = \sigma \circ \tau$, so σ is an inverse of τ.

Consequently, τ is invertible, so τ is bijective.

Therefore, τ is a permutation of X, so $\tau \in S_X$.

Therefore, for every permutation σ, there exists a permutation τ in S_X such that $\sigma \circ \tau = \tau \circ \sigma = id$, so every permutation in S_X has an inverse in S_X.

Since $\circ$ is a binary operation on S_X and $\circ$ is associative and the identity map id is an identity for $\circ$ and every permutation in S_X has an inverse in S_X, then $(S_X, \circ)$ is a group. $\square$

Corollary 47. *Let $n \in \mathbb{Z}^+$.*

The symmetric group on n symbols is a group under function composition.

Proof. Let $X = \{1, 2, ..., n\}$.

Let S_n be the set of all permutations on the set X.

Since $n \in \mathbb{Z}^+$, then $n \geq 1$, so $1 \in X$.

Hence, X is not empty.

Let $\circ$ be function composition on S_n.

Since the set X is not empty and S_n is the set of all permutations of X, then by the previous theorem, $(S_n, \circ)$ is a group under function composition. $\square$

Proposition 48. *Let $n \in \mathbb{Z}^+$.*

If $n \geq 3$, then $(S_n, \circ)$ is non-abelian.

Proof. Let X be a finite set of n symbols.

Since $n \geq 3$, let a, b, c be distinct elements of X.

Let $\sigma : X \to X$ be the function defined by $\sigma(a) = b$ and $\sigma(b) = a$ and $\sigma(x) = x$ for every other $x \in X$.

Then σ is a one to one and onto function, so $\sigma \in S_n$.

Let $\tau : X \to X$ be the function defined by $\tau(a) = b$ and $\tau(b) = c$ and $\tau(c) = a$ and $\tau(x) = x$ for every other $x \in X$.

Then τ is a one to one and onto function, so $\tau \in S_n$.

Since $(\sigma \circ \tau)(a) = \sigma((\tau(a)) = \sigma(b) = a$ and $(\tau \circ \sigma)(a) = \tau(\sigma(a)) = \tau(b) = c$ and $a \neq c$, then $(\sigma \circ \tau)(a) \neq (\tau \circ \sigma)(a)$, so $\sigma \circ \tau \neq \tau \circ \sigma$,

Since there exist $\sigma, \tau \in S_n$ such that $\sigma \circ \tau \neq \tau \circ \sigma$, then $\circ$ is not commutative, so S_n is not abelian. $\square$

Proof. Let n be an integer greater than or equal to 3.

Let $X = \{1, 2, 3, ..., n\}$ be a finite set of n symbols.

Let S_n be the symmetric group on n symbols of X.

Then there exist transpositions $(1, 2)$ and $(1, 3)$ in S_n.

Let $\sigma = (1, 2)$ and $\tau = (1, 3)$.

Then $\sigma, \tau \in S_n$ and $\sigma\tau = (1\ 2)(1\ 3) = (1\ 3\ 2) \neq (1\ 2\ 3) = (1\ 3)(1\ 2) = \tau\sigma$.

Therefore, there exist a distinct pair of elements in S_n that do not commute, so S_n is not abelian. $\square$

Theorem 49. ***Cayley's Theorem***

Every group G is isomorphic to a subgroup of the symmetric group on G.

Solution. Let $(G, *)$ and $(S_G, \circ)$ be groups.

We need to devise an bijective map from G to S_G that satisfies the homomorphism property $\phi(gh) = \phi(g) \circ \phi(h)$.

The key insight is to break down the problem and first devise a bijective function from G to G.

We have to devise a suitable bijective function.

We can look at the Cayley multiplication table for a group to devise a bijection.

We can let $\lambda_g(x) = gx$ for all $x \in G$ (left multiply by g).

When we left multiply we have the **left representation of** G.

We could also let $\rho_g(x) = xg$ for all $x \in G$ (right multiply by g).

When we right multiply we have the **right representation of** G.
Either choice is fine in the proof. $\square$

Proof. Let $(G, *)$ be a group.
Let $(S_G, \circ)$ be the symmetric group on G.
Define for each $g \in G$ the function $\lambda_g : G \to G$ by $\lambda_g(x) = gx$ for all $x \in G$.
Let $g \in G$.

We prove λ_g is a permutation of G.
We first prove λ_g is injective.
Let $x, y \in G$ such that $\lambda_g(x) = \lambda_g(y)$.
Then $gx = gy$.
By the cancellation law for groups, we have $x = y$.
Hence, $\lambda_g(x) = \lambda_g(y)$ implies $x = y$, so λ_g is injective.

We prove λ_g is surjective.
Let $y \in G$.
Let g^{-1} be the inverse of g.
Let $x = g^{-1}y$.
Since G is closed under its binary operation and $g^{-1}, y \in G$, then $x \in G$.
Let e be the identity of G.
Observe that

$$\begin{aligned} \lambda_g(x) &= \lambda_g(g^{-1}y) \\ &= g(g^{-1}y) \\ &= (gg^{-1})y \\ &= ey \\ &= y. \end{aligned}$$

Hence, there exists $x \in G$ such that $\lambda_g(x) = y$, so λ_g is surjective.
Thus, λ_g is bijective, so λ_g is a permutation of G.
Let $G' = \{\lambda_g : g \in G\}$.
Then $G' \subset S_G$.

We prove $G' < S_G$ by the subgroup test.
Let id be the identity of S_G.
Then $id : G \to G$ is the identity map on G defined by $id(x) = x$ for all $x \in G$.
Since $e \in G$, then $\lambda_e(x) = ex = x = id(x)$ for all $x \in G$.
Hence, $\lambda_e = id$.
Since $\lambda_e \in G'$, then $id \in G'$.
Let $\lambda_a, \lambda_b \in G'$.
Then $a, b \in G$.
Let $x \in G$.

Observe that

$$\begin{aligned}(\lambda_a \circ \lambda_b)(x) &= \lambda_a[\lambda_b(x)] \\ &= \lambda_a(bx) \\ &= a(bx) \\ &= (ab)x \\ &= \lambda_{ab}(x).\end{aligned}$$

Hence, $\lambda_a\lambda_b = \lambda_{ab}$.

Since $a, b \in G$ and G is closed under $*$, then $ab \in G$.

Thus, $\lambda_{ab} \in G'$, so $\lambda_a\lambda_b \in G'$.

Therefore, G' is closed under $\circ$.

Let λ_g^{-1} be the inverse of λ_g in S_G.

Then $\lambda_g\lambda_g^{-1} = id$.

Since $g^{-1} \in G$, then $\lambda_{g^{-1}} \in G'$.

Since $G' \subset S_G$, then $\lambda_{g^{-1}} \in S_G$.

Let $x \in G$. Then

$$\begin{aligned}\lambda_g\lambda_{g^{-1}}(x) &= \lambda_g(\lambda_{g^{-1}}(x)) \\ &= \lambda_g(g^{-1}x) \\ &= g(g^{-1}x) \\ &= (gg^{-1})x \\ &= ex \\ &= x \\ &= id(x).\end{aligned}$$

Hence, $\lambda_g\lambda_{g^{-1}} = id$.

Thus, $\lambda_g\lambda_g^{-1} = \lambda_g\lambda_{g^{-1}}$.

By the cancellation law for groups, we have $\lambda_g^{-1} = \lambda_{g^{-1}}$.

Thus, $\lambda_g^{-1} \in G'$, so G' is closed under taking inverses.

Therefore, $G' < S_G$.

Let $\phi : G \to G'$ be a function defined by $\phi(g) = \lambda_g$ for all $g \in G$.

To prove $G \cong G'$, we prove ϕ is an isomorphism.

Let $g, h \in G$ such that $\phi(g) = \phi(h)$.

Then $\lambda_g = \lambda_h$.

Let $x \in G$.

Then $\lambda_g(x) = \lambda_h(x)$, so $gx = hx$.

By the cancellation law for groups, we have $g = h$.

Thus, $\phi(g) = \phi(h)$ implies $g = h$, so ϕ is injective.

Let $\lambda_g \in G'$.
Then by definition of G', $g \in G$.
Hence, there exists $g \in G$ such that $\phi(g) = \lambda_g$.
Therefore, ϕ is surjective.
Hence, ϕ is a bijective function.
Since $\lambda_{ab} = \lambda_a \lambda_b$ for all $a, b \in G$, then $\phi(ab) = \phi(a)\phi(b)$ for all $a, b \in G$.
Therefore, ϕ is a homomorphism.
Hence, ϕ is a bijective homomorphism, so $\phi : G \to G'$ is an isomorphism.
Thus, $G \cong G'$. □

Corollary 50. *Every finite group of order n is isomorphic to a subgroup of S_n.*

Proof. TODO □

Cycle notation for permutations

Proposition 51. ***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 $\sigma^{-1} = (a_k\ a_{k-1}\ ...\ a_2\ a_1)$.

Proof. Suppose $\sigma = (a_1\ a_2\ ...\ a_k)$.
Let id be the identity permutation in the symmetric group on X.
Observe that

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

Hence, $\sigma(a_k\ a_{k-1}\ ...\ a_2\ a_1) = id = (a_k\ a_{k-1}\ ...\ a_2\ a_1)\sigma$, so $(a_k\ a_{k-1}\ ...\ a_2\ a_1)$ is the inverse of σ.
Therefore, $(a_k\ a_{k-1}\ ...\ a_2\ a_1) = \sigma^{-1}$. □

Proposition 52. ***order of a cycle***
Let $k \in \mathbb{Z}^+$.
A cycle of length k has order k.

Proof. Let $n \in \mathbb{Z}$ with $n \geq 2$.
Let $X = \{1, 2, ..., n\}$.
Let $k \in \mathbb{Z}^+$ such that $2 \leq k \leq n$.
Let σ be a cycle of length k in the symmetric group $(S_n, \circ)$.
Then $\sigma = (a_1\ a_2\ ...\ a_k)$.
Let $S = \{a_1, a_2, ..., a_k\}$ be a subset of X.
Then $\sigma(a_i) = a_{i \pmod k)+1}$ for all $a_i \in S$ and $\sigma(x) = x$ for all $x \in X - S$.
Let $id \in S_n$ be the identity permutation.

Let $x \in X$.

Then either $x \in S$ or $x \notin S$.

We consider these cases separately.

Case 1: Suppose $x \in S$.

Let a_1 be an arbitrary element of S.

Then $\sigma(a_1) = a_2$ and $\sigma(a_2) = a_3$ and $\sigma(a_3) = a_4$ and ... and $\sigma(a_k) = a_1$.

Since $a_1 \neq a_2$, then $\sigma \neq id$.

Observe that $\sigma^2(a_1) = \sigma(\sigma(a_1)) = \sigma(a_2) = a_3$.

Since $a_1 \neq a_3$, then $\sigma^2 \neq id$.

Observe that $\sigma^3(a_1) = \sigma^2(\sigma(a_1)) = \sigma^2(a_2) = \sigma(\sigma(a_2)) = \sigma(a_3) = a_4$.

Since $a_1 \neq a_4$, then $\sigma^3 \neq id$.

We repeat this process.

Observe that $\sigma^{k-1}(a_1) = \sigma^{k-2}(\sigma(a_1)) = \sigma(a_{k-1}) = a_k$.

Since $a_1 \neq a_k$, then $\sigma^{k-1} \neq id$.

Observe that $\sigma^k(a_1) = \sigma^{k-1}(\sigma(a_1)) = \sigma(a_k) = a_1$.

Thus, $\sigma^k(a_1) = a_1$.

Since a_1 is arbitrary, then $\sigma^k(x) = x$ for all $x \in S$.

Since $\sigma \neq id$ and $\sigma^2 \neq id$ and ... and $\sigma^{k-1} \neq id$, then $\sigma^s \neq id$ for each s with $s \in \{1, 2, ..., k-1\}$.

Case 2: Suppose $x \notin S$.

Since $x \in X$ and $x \notin S$, then $x \in X - S$.

Thus, $\sigma(x) = x$.

Since x is arbitrary, then $\sigma(x) = x$ for all $x \in X - S$.

Thus, $\sigma = id$ for all $x \in X - S$.

In any group with identity e, $e^t = e$ for all $t \in \mathbb{Z}$.

Since $k \in \mathbb{Z}$, then this implies $id^k = id$, so $\sigma^k = id$.

Hence, $(\sigma^k)(x) = x$ for all $x \in X - S$.

Since $\sigma^k(x) = x$ for all $x \in S$ and $(\sigma^k)(x) = x$ for all $x \in X - S$, then $(\sigma^k)(x) = x$ for all $x \in X$, so $\sigma^k = id$.

Since $\sigma^s \neq id$ for each s with $s \in \{1, 2, ..., k-1\}$ and $\sigma^k = id$, then k is the least positive integer such that $\sigma^k = id$, so the order of σ is k. ☐

Theorem 53. ***Disjoint cycles commute.***

Let α and β be disjoint cycles in the symmetric group on set X.

Then $\alpha\beta = \beta\alpha$.

Proof. Let X be a nonempty set.

Let $(S_X, \circ)$ be the symmetric group on X.

Let α and β be disjoint cycles in $(S_X, \circ)$.

Since α is a cycle, then there exist distinct $a_1, a_2, ..., a_k \in X$ for some integer $k \geq 2$ such that $\alpha = (a_1\ a_2\ ...\ a_k)$.

Since β is a cycle, then there exist distinct $b_1, b_2, ..., b_m \in X$ for some integer $m \geq 2$ such that $\beta = (b_1\ b_2\ ...\ b_m)$.

Let $A = \{a_1, a_2, ..., a_k\}$ be a subset of X.

Let $B = \{b_1, b_2, ..., b_m\}$ be a subset of X.
Since α and β are disjoint cycles, then A and B are disjoint sets, so $A \cap B = \emptyset$.
Since α is a cycle, then for every $x \in X$, $\alpha(x) \in A$ iff $x \in A$ and $\alpha(x) = x$ iff $x \notin A$.
Since β is a cycle, then for every $x \in X$, $\beta(x) \in B$ iff $x \in B$ and $\beta(x) = x$ iff $x \notin B$.

To prove $\alpha\beta = \beta\alpha$, we must prove $(\alpha\beta)(x) = (\beta\alpha)(x)$ for all $x \in X$.
Let $x \in X$.
We must prove $(\alpha\beta)(x) = (\beta\alpha)(x)$.
Either $x \in A \cup B$ or $x \notin A \cup B$.
Thus, either $x \in A$ or $x \in B$ or x is in neither A nor in B.
We consider these cases separately.
Case 1: Suppose $x \in A$.
Since $x \in A$ iff $\alpha(x) \in A$, then $\alpha(x) \in A$.
Since $\alpha(x) \in A$ and A and B are disjoint, then $\alpha(x) \notin B$.
Since $\beta(\alpha(x)) = \alpha(x)$ iff $\alpha(x) \notin B$, then $\beta(\alpha(x)) = \alpha(x)$.
Since $x \in A$ and A and B are disjoint, then $x \notin B$.
Since $\beta(x) = x$ iff $x \notin B$, then $\beta(x) = x$.
Observe that

$$\begin{aligned}
(\alpha\beta)(x) &= \alpha(\beta(x)) \\
&= \alpha(x) \\
&= \beta(\alpha(x)) \\
&= (\beta\alpha)(x).
\end{aligned}$$

Therefore, $(\alpha\beta)(x) = (\beta\alpha)(x)$.
Case 2: Suppose $x \in B$.
Since $x \in B$ iff $\beta(x) \in B$, then $\beta(x) \in B$.
Since $\beta(x) \in B$ and A and B are disjoint, then $\beta(x) \notin A$.
Since $\alpha(\beta(x)) = \beta(x)$ iff $\beta(x) \notin A$, then $\alpha(\beta(x)) = \beta(x)$.
Since $x \in B$ and A and B are disjoint, then $x \notin A$.
Since $\alpha(x) = x$ iff $x \notin A$, then $\alpha(x) = x$.
Observe that

$$\begin{aligned}
(\alpha\beta)(x) &= \alpha(\beta(x)) \\
&= \beta(x) \\
&= \beta(\alpha(x)) \\
&= (\beta\alpha)(x).
\end{aligned}$$

Therefore, $(\alpha\beta)(x) = (\beta\alpha)(x)$.
Case 3: Suppose x is in neither A nor in B.
Then $x \notin A$ and $x \notin B$.
Since $x \notin A$ and $\alpha(x) = x$ iff $x \notin A$, then $\alpha(x) = x$.
Since $x \notin B$ and $\beta(x) = x$ iff $x \notin B$, then $\beta(x) = x$.

Observe that

$$\begin{aligned}(\alpha\beta)(x) &= \alpha(\beta(x)) \\ &= \alpha(x) \\ &= x \\ &= \beta(x) \\ &= \beta(\alpha(x)) \\ &= (\beta\alpha)(x).\end{aligned}$$

Therefore, $(\alpha\beta)(x) = (\beta\alpha)(x)$.

Hence, in all cases $(\alpha\beta)(x) = (\beta\alpha)(x)$, as desired. ☐

Theorem 54. ***Cycle Decomposition Theorem***

Every permutation of a nonempty finite set can be written as a finite product of disjoint cycles.

Proof. Define predicate $p(n)$: every permutation of a set of size n is a finite product of disjoint cycles.

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

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

Basis:

Let $X = \{x\}$ be a set of size 1.

The only permutation of X is the identity map $id : X \to X$ defined by $id(x) = x$.

The identity map in cycle notation is the 1 cycle (1), so (1) is a single product of a cycle.

Hence, the only permutation of X is a single product of a cycle.

Thus, every permutation of X is a single product of a cycle, so every permutation of a set of size 1 is a single product of a cycle.

Therefore, $p(1)$ is true.

Induction:

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

Suppose $p(k)$ is true for every $1 \leq k \leq m$.

Then $p(1)$ and $p(2)$ and ... and $p(m)$ are true.

Thus, every permutation of a finite set of size between 1 and m is a finite product of disjoint cycles.

To prove $p(m+1)$ is true, we must prove every permutation of a set of size $m+1$ is a finite product of disjoint cycles.

Let $(S_{m+1}, \circ)$ be the symmetric group on a set X of size $m+1$.

Let $X = \{1, 2, ..., m, m+1\}$.

Then $|X| = m+1$.

Let σ be an arbitrary element of S_{m+1}.
Then σ is an arbitrary permutation of X.
We must prove σ can be written as a finite product of disjoint cycles.
Let id be the identity permutation in S_{m+1}.
Every element of a finite group has finite order.
Since S_{m+1} is a finite group and $\sigma \in S_{m+1}$, then σ has finite order.
Let s be the order of σ.
Then s is the least positive integer such that $\sigma^s = id$.
Let $S = \{1, \sigma(1), \sigma^2(1), \sigma^3(1), ..., \sigma^{s-1}(1)\}$.
Then $S \subset X$ and $|S| = s$ and $(1\ \sigma(1)\ \sigma^2(1)\ ...\ \sigma^{s-1}(1))$ is a cycle of length s.
Since X is finite and $|X| = m+1$ and $S \subset X$ and $|S| = s$, then either $s = m+1$ or $s < m+1$.
We consider these cases separately.
Case 1: Suppose $s = m+1$.
Then $S = \{1, \sigma(1), \sigma^2(1), \sigma^3(1), ..., \sigma^m(1)\}$.
Thus, σ is the cycle $(1\ \sigma(1)\ \sigma^2(1)\ ...\ \sigma^m(1))$ of length $m+1$.
Therefore, σ is a single product of a cycle.
Case 2: Suppose $s < m+1$.
Then $0 < m+1-s$.
Since $X = S \cup (X - S)$ and S and $X - S$ are disjoint sets, then

$$\begin{aligned} m+1 &= |X| \\ &= |S \cup (X-S)| \\ &= |S| + |X - S| \\ &= s + |X - S|. \end{aligned}$$

Thus, $m+1 = s + |X-S|$, so $|X-S| = m+1-s$.
Since s is positive, then $s > 0$, so $-s < 0$.
Thus, $m+1-s < m+1$.
Therefore, $0 < m+1-s$ and $m+1-s < m+1$, so $0 < m+1-s < m+1$.
Hence, $1 \leq m+1-s \leq m$, so $1 \leq |X-S| \leq m$.
Consequently, $X - S$ is a set of size between 1 and m.
By the induction hypothesis, every permutation of $X - S$ is a finite product of disjoint cycles.

Let τ be an arbitrary permutation of the set $X - S$.
Then τ is a finite product of disjoint cycles.
Thus, there exists a positive integer t such that $\tau = \tau_1\tau_2\ldots\tau_t$ and τ_i is a disjoint cycle for each $i \in \{1, 2, ..., t\}$.
Since S and $X - S$ are disjoint sets, then the cycles
$(1\ \sigma(1)\ \sigma^2(1)\ ...\ \sigma^{s-1}(1))$
and τ_i are disjoint for each $i \in \{1, 2, ..., t\}$.
Hence, $(1\ \sigma(1)\ \sigma^2(1)\ ...\ \sigma^{s-1}(1)), \tau_1, \tau_2, ...,$ and τ_t are all disjoint cycles.

Observe that

$$\begin{aligned}\sigma &= (1\ \sigma(1)\ \sigma^2(1)\ ...\ \sigma^{s-1}(1))\tau \\ &= (1\ \sigma(1)\ \sigma^2(1)\ ...\ \sigma^{s-1}(1))\tau_1\tau_2\ldots\tau_t.\end{aligned}$$

Thus, σ is a finite product of disjoint cycles.

In all cases, σ is a finite product of disjoint cycles, so every permutation of a set of size $m+1$ is a finite product of disjoint cycles.

Hence, $p(m+1)$ is true, so $p(1)$ and $p(2)$ and ... and $p(m)$ imply $p(m+1)$.

Since $p(1)$ is true and the statements $p(1)$ and $p(2)$ and ... and $p(m)$ imply $p(m+1)$, then by the principle of strong induction, $p(m)$ is true for all $m \in \mathbb{Z}^+$.

Therefore, every permutation of a set of size n is a finite product of disjoint cycles for all $n \in \mathbb{Z}^+$. □

Corollary 55. *The order of a permutation is the least common multiple of the orders of its disjoint cycles.*

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

Let σ be a permutation in the symmetric group $(S_n, \circ)$.

Let $id \in S_n$ be the identity permutation.

Every permutation in S_n can be written as a finite product of disjoint cycles.

Thus, there exist a positive integer k and disjoint cycles $\alpha_1, \alpha_2, ..., \alpha_k$ in S_n such that $\sigma = \alpha_1 \circ \alpha_2 \circ ... \circ \alpha_k$.

Every element of a finite group has finite order.

Since $\alpha_1, \alpha_2, ..., \alpha_k, \sigma \in S_n$ and S_n is a finite group, then each of $\alpha_1, \alpha_2, ..., \alpha_k$, and σ has a finite order.

Let m_1 be the finite order of α_1 and let m_2 be the finite order of α_2 and ... let m_k be the finite order of α_k and let m be the finite order of σ.

Since σ has finite order m, then m is the least positive integer such that $\sigma^m = id$.

Disjoint cycles commute, so $\alpha_i \circ \alpha_j = \alpha_j \circ \alpha_i$ for each $1 \leq i, j \leq k$.

Hence,

$$\begin{aligned} id &= \sigma^m \\ &= (\alpha_1 \circ \alpha_2 \circ ... \circ \alpha_k)^m \\ &= \alpha_1^m \circ \alpha_2^m \circ ... \circ \alpha_k^m.\end{aligned}$$

Thus, $\sigma^m = id$ iff $\alpha_i^m = id$ for each $i \in \{1, 2, ..., k\}$.

If an element α has finite order m, then $\alpha^N = id$ iff $m|N$.

Thus, $\alpha_1^m = id$ iff $m_1|m$ and $\alpha_2^m = id$ iff $m_2|m$ and ... and $\alpha_k^m = id$ iff $m_k|m$.

Hence, $\alpha_1^m = id$ and $\alpha_2^m = id$ and ... and $\alpha_k^m = id$ iff $m_1|m$ and $m_2|m$ and ... and $m_k|m$, so m must be a common multiple of $m_1, m_2, ..., m_k$.

Since m is the least positive integer such that $\sigma^m = id$, then this implies m must be the least common multiple of $m_1, m_2, ..., m_k$.

Therefore, $m = lcm(m_1, m_2, ..., m_k)$. □

Proposition 56. *Let τ be a k cycle.*

If σ is a permutation, then $\sigma\tau\sigma^{-1}$ is a k cycle.

Solution. To prove $\sigma\tau\sigma^{-1}$ is a k cycle, let $\alpha = \sigma\tau\sigma^{-1}$.

We must prove there exists $b_1, b_2, ..., b_k \in X$ such that $\alpha(b_1) = b_2$ and $\alpha(b_2) = b_3$ and ... and $\alpha(b_k) = b_1$ and for all other $x \in X$, $\alpha(x) = x$.

Since τ is a k cycle, then there exist $a_1, a_2, ..., a_k \in X$ such that $\tau = (a_1, a_2, ..., a_k)$.

Let $b_1 = \sigma(a_1)$. ☐

Proof. Let X be a nonempty set. Let τ be a k cycle. Then there exist distinct $a_1, a_2, ..., a_k \in X$ such that $\tau = (a_1, a_2, ..., a_k)$.

Let $A = \{a_1, a_2, ..., a_k\}$. Then $A \subset X$.

Let σ be an arbitrary permutation in S_X. Then $\sigma : X \to X$ is a bijective function. Thus, for every $x \in X$, $\sigma(x) \in X$. Hence, $\sigma(a_i) \in X$ for each $i \in \{1, 2, ..., k\}$. Let $b_i = \sigma(a_i)$ for each $i \in \{1, 2, ..., k\}$. Since σ is injective, then $a_i \neq a_j$ implies $\sigma(a_i) \neq \sigma(a_j)$ for all $i, j \in \{1, 2, ..., k\}$. Hence, for all $i, j \in \{1, 2, ..., k\}$, if $a_i \neq a_j$, then $b_i \neq b_j$. Thus, each b_i is distinct, so let $B = \{b_1, b_2, ..., b_k\}$.

Let $x \in X$. Either $x \in B$ or $x \notin B$.

Case 1: Suppose $x \in B$.

Let i be an arbitrary positive integer such that $x = b_i$.

Observe that

$$\begin{aligned}
\sigma\tau\sigma^{-1}(b_i) &= \sigma\tau(\sigma^{-1}(b_i)) \\
&= \sigma\tau(a_i) \\
&= \sigma(\tau(a_i)) \\
&= \sigma(a_{i \pmod k)+1}) \\
&= b_{i \pmod k)+1}).
\end{aligned}$$

Since i is arbitrary, then $\sigma\tau\sigma^{-1}(b_i) = b_{i \pmod k)+1})$ for all positive integers i.

Thus, in particular, $\sigma\tau\sigma^{-1}(b_1) = b_2$ and $\sigma\tau\sigma^{-1}(b_2) = b_3$ and ... and $\sigma\tau\sigma^{-1}(b_k) = b_{k \pmod k)+1} = b_{0+1} = b_1$.

Case 2: Suppose $x \notin B$.

Since σ is bijective, then σ is surjective. Hence, there exists $y \in X$ such that $\sigma(y) = x$. Thus, $\sigma(y) \notin B$. For every $x \in X$, $\sigma(x) \in B$ iff $x \in A$. Thus, for every $x \in X$, $\sigma(x) \notin B$ iff $x \notin A$. Hence, $\sigma(y) \notin B$ iff $y \notin A$. Therefore, $y \notin A$.

Observe that

$$\begin{aligned}
\sigma\tau\sigma^{-1}(x) &= \sigma\tau\sigma^{-1}(\sigma(y)) \\
&= (\sigma\tau\sigma^{-1})(\sigma(y)) \\
&= [\sigma\tau\sigma^{-1}\sigma](y) \\
&= [(\sigma\tau)(\sigma^{-1}\sigma)](y) \\
&= [(\sigma\tau)(id)](y) \\
&= (\sigma\tau)(y) \\
&= \sigma(\tau(y)) \\
&= \sigma(y) \\
&= x.
\end{aligned}$$

Therefore, if $x \notin B$, then $\sigma\tau\sigma^{-1}(x) = x$.

Since there exist $b_1, b_2, ..., b_k \in X$ such that $\sigma\tau\sigma^{-1}(b_1) = b_2$ and $\sigma\tau\sigma^{-1}(b_2) = b_3$ and ... and $\sigma\tau\sigma^{-1}(b_k) = b_{k \pmod k)+1} = b_{0+1} = b_1$ and $\sigma\tau\sigma^{-1}(x) = x$ for all other x, then $\sigma\tau\sigma^{-1}$ is a cycle of length k. $\square$

Parity of a permutation

Theorem 57. ***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.

Proof. Let n be a fixed integer greater than or equal to 2.

Let X be a set of n elements.

Since $n \geq 2$, then X is a nonempty finite set.

Let $\sigma : X \to X$ be an arbitrary permutation of X.

By the cycle decomposition theorem, every permutation of a nonempty finite set can be written as a finite product of disjoint cycles.

Since σ is a permutation of X and X is a nonempty finite set, then σ can be written as a finite product of disjoint cycles.

Hence, there exists a positive integer m such that $\alpha_1, \alpha_2, ..., \alpha_m$ are disjoint cycles and $\sigma = \alpha_1\alpha_2...\alpha_m$.

To prove σ can be written as a finite product of transpositions, we must prove an arbitrary cycle of σ can be written as a finite product of transpositions.

Let τ be an arbitrary cycle of length k in σ.

Then k is a positive integer such that $\tau = (a_1\ a_2\ ...\ a_k)$ and $\{a_1, a_2, ..., a_k\}$ is a subset of X.

Observe that

$$\begin{aligned}
(a_1\ a_2)(a_2\ a_3)(a_3\ a_4)...(a_{k-1}\ a_k) &= (a_1\ a_2)(a_2\ a_3)...(a_{k-3}\ a_{k-2})(a_{k-2}\ a_{k-1})(a_{k-1}\ a_k) \\
&= (a_1\ a_2)(a_2\ a_3)(a_3\ a_4)...(a_{k-3}\ a_{k-2})(a_{k-2}\ a_{k-1}\ a_k) \\
&= (a_1\ a_2)(a_2\ a_3)(a_3\ a_4)...(a_{k-3}\ a_{k-2}\ a_{k-1}\ a_k) \\
&= (a_1\ a_2)(a_2\ a_3)(a_3\ a_4\ ...a_{k-3}\ a_{k-2}\ a_{k-1}\ a_k) \\
&= (a_1\ a_2)(a_2\ a_3\ a_4\ ...\ a_{k-3}\ a_{k-2}\ a_{k-1}\ a_k) \\
&= (a_1\ a_2\ a_3\ a_4\ ...\ a_{k-3}\ a_{k-2}\ a_{k-1}\ a_k) \\
&= \tau.
\end{aligned}$$

Hence, $\tau = (a_1\ a_2\ ...\ a_k) = (a_1\ a_2)(a_2\ a_3)...(a_{k-1}\ a_k)$ is a product of $k-1$ transpositions.

Therefore, τ is a finite product of transpositions.

Since τ is an arbitrary cycle of σ, then every cycle of σ is a finite product of transpositions.

Thus, each α_i for $i \in \{1, 2, ..., m\}$ is a finite product of transpositions.

Since $\sigma = \alpha_1\alpha_2...\alpha_m$, then this implies σ is a finite product of transpositions.

□

Lemma 58. ***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.

Solution. The solution is a clever insight. We start with $e = \tau_1\tau_2...\tau_k$, where each τ_i is a transposition.

Let τ_1 and τ_2 be two transpositions.

We observe that the product of τ_1 and τ_2 can be categorized as one of 4 possibilities:

1. $\tau_1 = \tau_2$. So, if $\tau_1 = (a, b)$, then $\tau_2 = (a, b)$. And we know $(a, b)(a, b) = e$.

2. τ_1 and τ_2 are disjoint cycles. So, if $\tau_1 = (a, b)$, let $\tau_2 = (c, d)$. Since disjoint cycles commute, then we have $(a, b)(c, d) = (c, d)(a, b)$.

The other possibilities are when τ_1 and τ_2 share exactly one element in common.

Thus, if we let $\tau_2 = (a, b)$, then $\tau_1 = (a, c)$ or $\tau_1 = (c, b)$.

3. If $\tau_1 = (a, c)$ and $\tau_2 = (a, b)$, then $(a, c)(a, b) = (a, b)(b, c)$.

4. If $\tau_1 = (c, b)$ and $\tau_2 = (a, b)$, then $(c, b)(a, b) = (a, c)(b, c)$.

The key insight is that we may reduce a product of k transpositions for e into a product of $k-2$ transpositions by moving a given element a of a transposition to the left, preserving e. We see this after computing many different example products for e.

We keep moving a to the left and either obtain scenario 1 in which we have two identical transpositions which cancel each other, resulting in $k-2$ transpositions or we end up with k transpositions in which a is the only element in the left most transposition, say τ_1. □

Proof. Let X be a finite set of at least two elements. Let id be the identity permutation of X. Any permutation of a finite set containing at least two elements can be written as a finite product of transpositions. Therefore, id can be written as a finite product of transpositions. Hence, there exists a positive integer k such that $\tau_1, \tau_2, ..., \tau_k$ are transpositions and $id = \tau_1\tau_2...\tau_k$.

We must prove id can be written as a product of $k-2$ transpositions.

Let a, b, c, d be distinct elements of X. Let $\tau_k = (a, b)$. Since $(a, b) = (b, a)$, then we may arbitrarily choose either a or b. Without loss of generality, choose a. The product of two transpositions either has no elements in common, or has exactly one element in common, or has exactly two elements in common.

Hence, there are 4 possible scenarios for the product $\tau_{k-1}\tau_k$.

1. identical cycles (two elements in common): $(a, b)(a, b) = id$.
2. exactly one element in common c: $(a, c)(a, b) = (a, b)(b, c)$.
3. exactly one element in common c: $(c, b)(a, b) = (a, c)(b, c)$.
4. disjoint cycles (no elements in common): $(c, d)(a, b) = (a, b)(c, d)$.

If case 1 occurs, then we may delete $\tau_{k-1}\tau_k$ in the original product $id = \tau_1\tau_2...\tau_k$. We then obtain $id = \tau_1\tau_2...\tau_{k-2}$, so id is a product of $k-2$ transpositions, as desired.

If one of the other 3 cases occurs, then we replace $\tau_{k-1}\tau_k$ with what appears on the right to obtain a new product of k transpositions which equals id and for which the right most occurrence of a is moved one transposition to the left.

Repeat this process. At each stage, either we cancel the 2 transpositions (case 1) so we're done, or we form a new product of k transpositions in which a has moved to the left by another transposition.

The process must terminate since there are a finite number of transpositions.

Suppose for the sake of contradiction that the process terminates and id is not the product of $k-2$ transpositions. Then id is the product of k transpositions in which a is in the left most transposition τ_1. Thus, either $\tau_1 = (a, b)$ or $\tau_1 = (a, c)$. Hence, $\tau_1(a) \neq a$, Therefore, this product of k transpositions maps a to some element of X other than a. Thus, this product of k transpositions is not the identity map, which contradicts the statement that id equals this product.

Therefore, id must be the product of $k-2$ transpositions. ☐

Lemma 59. ***Even Identity Lemma***

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

Proof. Let X be a finite set of at least two elements. Let id be the identity permutation of X. Any permutation of a finite set containing at least two elements can be written as a finite product of transpositions. Therefore, id can be written as a finite product of transpositions. Hence, there exists a positive integer k such that $\tau_1, \tau_2, ..., \tau_k$ are transpositions and $id = \tau_1\tau_2...\tau_k$.

To prove k is even, suppose for the sake of contradiction that k is not even. Then k is odd.

By the reduction lemma, if id can be written as a product of k transpositions, then id can be written as a product of $k-2$ transpositions.

Since id is a product of k transpositions, then it follows that id can be written as a product of $k-2$ transpositions.

Repeat this process. At each stage id is a product of 2 fewer transpositions. Since the difference between an odd number and 2 is odd, then the number of transpositions remains odd. Hence, id remains a product of an odd number of transpositions at each stage.

Since k is finite, then this process must terminate.

Suppose the process terminates. Since k is a positive integer and id must be the product of an odd number of transpositions, then $k = 1$. Hence, id is a product of exactly one transposition. Thus, there exists a transposition equal to id.

Let $\tau = (i, j)$ be a transposition of distinct elements i and j in X such that $id = \tau$. Then $i \neq j$ and $\tau(i) = j$. Hence, $\tau(i) \neq i$. Since $\tau = id$, then $\tau(x) = x$ for all x. Hence, $\tau(i) = i$. Thus we have $\tau(i) = i$ and $\tau(i) \neq i$, a contradiction. Therefore, k cannot be odd, so k must be even. □

Theorem 60. ***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.

Solution. There are various proofs and approaches one can take. We take the approach to first prove a lemma: establish that identity permutation in S_n can be expressed as an even number of transpositions (not odd) because this will make the proof easier.

We can right multiply by the inverse of each σ in reverse order. □

Proof. Let $n \in \mathbb{Z}^+$ and $n \geq 2$. Let α be a permutation in the symmetric group $(S_n, \circ)$. Any permutation of a finite set containing at least two elements can be written as a finite product of transpositions. Since S_n is a finite set, then α can be written as a finite product of transpositions. Let $k, m \in \mathbb{Z}^+$. Suppose α is a finite product of k and m transpositions. Then there exist transpositions $\tau_1, \tau_2, ..., \tau_k$ and $\sigma_1, \sigma_2, ..., \sigma_m$ such that $\alpha = \tau_1\tau_2...\tau_k$ and $\alpha = \sigma_1\sigma_2...\sigma_m$.

Let id be the identity of S_n. Then id is the identity permutation and $id = \alpha \circ \alpha^{-1}$. Since the inverse of a sequence of transpositions is the composition of their inverses in reverse order, and since each transposition is its own inverse, then

$$\begin{aligned} id &= \alpha\alpha^{-1} \\ &= (\tau_1\tau_2...\tau_k) \circ (\sigma_1\sigma_2...\sigma_m)^{-1} \\ &= (\tau_1\tau_2...\tau_k) \circ (\sigma_m^{-1}\sigma_{m-1}^{-1}...\sigma_2^{-1}\sigma_1^{-1}) \\ &= (\tau_1\tau_2...\tau_k) \circ (\sigma_m\sigma_{m-1}...\sigma_1). \end{aligned}$$

Hence, the identity permutation is a product of $k+m$ transpositions. By the even identity lemma, if id is a product of $k+m$ transpositions, then $k+m$ is even. Thus, $k+m$ is even. The sum $k+m$ is even iff k and m are both even or both odd. Therefore, k and m are either both even or both odd, so k and m have the same parity. □

Theorem 61. *A cycle of even length is odd and a cycle of odd length is even.*

Proof. Let $n \in \mathbb{Z}, n \geq 2$. Let $X = \{1, 2, ..., n\}$. Let k be a positive integer such that $2 \leq k \leq n$. Let σ be a k cycle. Then there exist $a_1, a_2, ..., a_k \in \{1, 2, ..., k\}$ such that $\sigma = (a_1, a_2, ..., a_k)$ and $\sigma(x) = x$ for all $x \in X - \{1, 2, ..., k\}$.

Any permutation of a finite set containing at least two elements can be written as a finite product of transpositions. Thus, σ is a finite product of transpositions. Observe that

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

Thus, σ is a product of $k - 1$ transpositions.

Either k is even or k is odd.

We consider these cases separately.

Case 1: Suppose k is even.

Then $k-1$ is odd. Thus, σ is a product of an odd number of transpositions. By the parity theorem, a permutation is either even or odd, but not both. Therefore, σ must be odd.

Case 2: Suppose k is odd.

Then $k-1$ is even. Thus, σ is a product of an even number of transpositions. By the parity theorem, a permutation is either even or odd, but not both. Therefore, σ must be even. □

Theorem 62. *The parity of a permutation is the same as the parity of its inverse.*

Solution. This statement means: Let α be a permutation. Let α^{-1} be the inverse of α. Then if α is even, then α^{-1} is even and if α is odd, then α^{-1} is odd. □

Proof. Let n be an integer greater than or equal to 2. Let $(S_n, \circ)$ be the symmetric group of n symbols. Let α be a permutation of S_n. Since S_n is a group, then the inverse of α exists. Let α^{-1} be the inverse of α.

Any permutation in S_n can be written as a finite product of transpositions. Hence, α can be written as a finite product of transpositions. Thus, there exists a positive integer k such that $\alpha_1, \alpha_2, ..., \alpha_k$ are transpositions and $\alpha = \alpha_1 \alpha_2 \cdots \alpha_k$. Observe that

$$\begin{aligned} \alpha^{-1} &= (\alpha_1 \alpha_2 \cdots \alpha_k)^{-1} \\ &= \alpha_k^{-1} \alpha_{k-1}^{-1} \cdots \alpha_1^{-1} \\ &= \alpha_k \alpha_{k-1} \cdots \alpha_1. \end{aligned}$$

Hence, α^{-1} is a product of k transpositions. Since α is a product of k transpositions, then α and α^{-1} are each a product of k transpositions.

Either k is even or k is odd.

We consider these cases separately.

Case 1: Suppose k is even.

Then α and α^{-1} are each a product of an even number of transpositions. By the parity theorem, a permutation is either even or odd, but not both. Therefore, α and α^{-1} are each even permutations. Hence, the parity of α is the same as the parity of α^{-1}.

Case 2: Suppose k is odd.

Then α and α^{-1} are each a product of an odd number of transpositions. By the parity theorem, a permutation is either even or odd, but not both. Therefore, α and α^{-1} are each odd permutations. Hence, the parity of α is the same as the parity of α^{-1}.

Therefore, in all cases, α and α^{-1} have the same parity. $\square$

Theorem 63. *The composition of two permutations of the same parity is even.*

Proof. Let $n \in \mathbb{Z}^+, n \geq 2$. Let $\sigma, \tau \in S_n$ such that σ and τ have the same parity. We must prove $\sigma\tau$ is an even permutation.

For $n \geq 2$, any permutation in $(S_n, \circ)$ can be written as a finite product of transpositions. Thus, σ and τ each can be written as a finite product of transpositions. Hence, there exist positive integers k and m such that $\sigma = \sigma_1\sigma_2\cdots\sigma_k$ and for each $i \in \{1, 2, ..., k\}$, σ_i is a transposition and $\tau = \tau_1\tau_2\cdots\tau_m$ and for each $j \in \{1, 2, ..., m\}$, τ_j is a transposition. Thus, $\sigma\tau = (\sigma_1\sigma_2\cdots\sigma_k)(\tau_1\tau_2\cdots\tau_m)$. Hence, $\sigma\tau$ is a product of $k + m$ transpositions.

Since σ and τ have the same parity, then either k and m are both even or both odd.

We consider these cases separately.

Case 1: Suppose k and m are both even.

The sum of any two even integers is even. Hence, $k + m$ is even.

Case 2: Suppose k and m are both odd.

The sum of any two odd integers is even. Hence, $k + m$ is even.

Thus, in all cases $k + m$ is even. By the parity theorem, the parity of $\sigma\tau$ is either even or odd, but not both. Therefore, $\sigma\tau$ must be an even permutation. $\square$

Theorem 64. *The composition of two permutations of opposite parity is odd.*

Proof. Let $n \in \mathbb{Z}^+, n \geq 2$. Let $\sigma, \tau \in S_n$ such that σ and τ have opposite parity. We must prove $\sigma\tau$ is an odd permutation.

For $n \geq 2$, any permutation in $(S_n, \circ)$ can be written as a finite product of transpositions. Thus, σ and τ each can be written as a finite product of transpositions. Hence, there exist positive integers k and m such that $\sigma = \sigma_1\sigma_2\cdots\sigma_k$ and for each $i \in \{1, 2, ..., k\}$, σ_i is a transposition and $\tau = \tau_1\tau_2\cdots\tau_m$ and for each $j \in \{1, 2, ..., m\}$, τ_j is a transposition.

Thus, $\sigma\tau = (\sigma_1\sigma_2\cdots\sigma_k)(\tau_1\tau_2\cdots\tau_m)$. Hence, $\sigma\tau$ is a product of $k + m$ transpositions.

The sum of two integers of opposite parity is odd. Hence, $k + m$ is odd. By the parity theorem, the parity of $\sigma\tau$ is either even or odd, but not both. Therefore, $\sigma\tau$ must be an odd permutation. $\square$

Proposition 65. *The function $S_n \to \{-1, 1\}$ that assigns to each permutation of S_n its signature is a group homomorphism.*

Proof. Let S_n be the symmetric group on n symbols.

Let $f : S_n \to \{-1, 1\}$ be defined by $f(\sigma) = sgn(\sigma)$ for each $\sigma \in S_n$.

Let $\sigma \in S_n$. Then $f(\sigma) = sgn(\sigma)$ and $sgn(\sigma) \in \{-1, 1\}$. Since any permutation is either even or odd, but not both, then $sgn(\sigma)$ is either 1 or -1, but not both. Hence, $sgn(\sigma)$ is uniquely determined, so $f(\sigma)$ is unique. Thus, $f(\sigma)$ is unique for every $\sigma \in S_n$. Therefore, f is a function.

Observe that $\{-1, 1\}$ is a group under multiplication of integers.

Let $\alpha, \beta \in S_n$. Let $k = sgn(\alpha)$ and $m = sgn(\beta)$.

Since α, β are either even or odd we have 4 cases to consider.

Case 1: Suppose α, β are both even.

Then $sgn(\alpha) = 1$ and $sgn(\beta) = 1$. The composition of two permutations of the same parity is even. Hence, $\alpha\beta$ is even, so $sgn(\alpha\beta) = 1$.

Observe that

$$\begin{aligned} f(\alpha\beta) &= sgn(\alpha\beta) \\ &= 1 \\ &= (1)(1) \\ &= sgn(\alpha)sgn(\beta) \\ &= f(\alpha)f(\beta). \end{aligned}$$

Case 2: Suppose α, β are both odd.

Then $sgn(\alpha) = -1$ and $sgn(\beta) = -1$. The composition of two permutations of the same parity is even. Hence, $\alpha\beta$ is even, so $sgn(\alpha\beta) = 1$.

Observe that

$$\begin{aligned} f(\alpha\beta) &= sgn(\alpha\beta) \\ &= 1 \\ &= (-1)(-1) \\ &= sgn(\alpha)sgn(\beta) \\ &= f(\alpha)f(\beta). \end{aligned}$$

Case 3: Suppose α is even and β is odd.

Then $sgn(\alpha) = 1$ and $sgn(\beta) = -1$. The composition of two permutations of opposite parity is odd. Hence, $\alpha\beta$ is odd, so $sgn(\alpha\beta) = -1$.

Observe that

$$\begin{aligned} f(\alpha\beta) &= sgn(\alpha\beta) \\ &= -1 \\ &= (1)(-1) \\ &= sgn(\alpha)sgn(\beta) \\ &= f(\alpha)f(\beta). \end{aligned}$$

Case 4: Suppose α is odd and β is even.

Then $sgn(\alpha) = -1$ and $sgn(\beta) = 1$. The composition of two permutations of opposite parity is odd. Hence, $\alpha\beta$ is odd, so $sgn(\alpha\beta) = -1$.

Observe that

$$\begin{aligned} f(\alpha\beta) &= sgn(\alpha\beta) \\ &= -1 \\ &= (-1)(1) \\ &= sgn(\alpha)sgn(\beta) \\ &= f(\alpha)f(\beta). \end{aligned}$$

Therefore, in all cases, $f(\alpha\beta) = f(\alpha)f(\beta)$. Hence, f is a group homomorphism. □

Theorem 66. *Let $(S_n, \circ)$ be the symmetric group on n symbols.*

Let $A_n = \{\sigma \in S_n : \sigma$ is an even permutation $\}$.

Then $A_n < S_n$.

Solution. To prove A_n is a subgroup of S_n, we use the finite subgroup test:

Thus, we prove:

1. A_n is closed under $\circ$ of S_n: $(\forall \alpha, \beta \in A_n)(\alpha\beta \in A_n)$.

2. $A_n \neq \emptyset$. We prove this by proving $e \in A_n$, where $e \in S_n$ is identity map on a set of n symbols. □

Proof. Observe that $A_n \subset S_n$. Since $|S_n| = n!$, then S_n is finite. Every subset of a finite set is finite. Hence, A_n is finite.

Let id be the identity permutation in S_n. Since id is an even permutation, then $id \in A_n$. Hence, A_n is not empty.

Thus, A_n is a nonempty finite subset of S_n.

To prove $A_n < S_n$, we prove A_n is closed under $\circ$ of S_n.

Let $\alpha, \beta \in A_n$. Then $\alpha, \beta \in S_n$ and α and β are even. Thus, α and β have the same parity. Let $\alpha\beta$ be the composition of α and β. By closure of the symmetric group S_n, we have $\alpha\beta \in S_n$. The composition of two permutations of the same parity is even. Hence, $\alpha\beta$ is even. Since $\alpha\beta \in S_n$ and $\alpha\beta$ is even, then $\alpha\beta \in A_n$. Therefore, A_n is closed under $\circ$ of S_n.

Thus, by the finite subgroup test, $A_n < S_n$. □

Theorem 67. *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 $\frac{n!}{2}$.

Solution. Let $\sigma \in S_n$. Then σ is either an even permutation or an odd permutation, but not both, by the parity theorem. Hence, the set of even permutations is disjoint from the set of odd permutations, and the collection of even and odd permutations forms a partition of S_n. To prove the number of even permutations equals the number of odd permutations, we must prove $|A_n| = |\overline{A_n}|$. Hence, we must devise a bijection between A_n and $\overline{A_n}$.

How do we devise a bijective function? After working thru examples, such as S_1, S_2, S_3, S_4 we see that there does not exist an obvious pattern between a given even permutation and an odd permutation.

However, the key insight is to use the left or right representation of A_n just as was done in the proof of Cayley's theorem.

Thus, let $\phi(\sigma) = \tau\sigma$ be a function from A_n to $\overline{A_n}$ for a fixed $\tau \in S_n$. We must prove ϕ is one to one and onto.

Also, we note that if $n = 1$, then $S_1 = \{id\}$. Since id is even, then there is exactly one even permutation in S_1. However, there are no odd permutations in S_1. That's why we restrict n to $n \geq 2$. $\square$

Proof. Let n be an integer greater than or equal to 2.

Let $X = \{1, 2, ..., n\}$.

Let $(S_n, \circ)$ be the symmetric group on n symbols.

Then $S_n = \{\sigma : \sigma \text{ is a permutation of } X\ \}$.

Let id be the identity element of S_n. Then $id : X \to X$ is the identity permutation and id is even.

Let A be the set of all even permutations of S_n. Then $A = \{\sigma \in S_n : \sigma \text{ is even.}\}$.

Let B be the set of all odd permutations of S_n. Then $B = \{\sigma \in S_n : \sigma \text{ is odd.}\}$.

Thus, $A \subset S_n$ and $B \subset S_n$ and $A \cup B \subset S_n$.

Let $P = \{A, B\}$.

We prove P is a partition of S_n.

Since $id \in S_n$ and id is even, then $id \in A$. Hence, $A \neq \emptyset$.

Since $n \geq 2$, then a transposition exists in S_n. Let τ be a transposition in S_n. Since $\tau \in S_n$ and τ is odd, then $\tau \in B$. Hence, $B \neq \emptyset$.

We prove $A \cup B = S_n$.

Let $\sigma \in S_n$. By the parity theorem, either σ is even or odd, but not both even and odd. Hence, either $\sigma \in A$ or $\sigma \in B$ but $\sigma \notin A \cap B$. Thus, $\sigma \in A \cup B$ and $\sigma \notin A \cap B$.

Therefore $\sigma \in S_n$ implies $\sigma \in A \cup B$, so $S_n \subset A \cup B$.

Since $A \cup B \subset S_n$ and $S_n \subset A \cup B$, then $A \cup B = S_n$.

Since σ is arbitrary, then $\sigma \notin A \cap B$ for all $\sigma \in S_n$. Hence, there does not exist $\sigma \in S_n$ such that $\sigma \in A \cap B$. Therefore, $A \cap B = \emptyset$.

Thus, P is a partition of S_n.

To prove $|A| = |B|$, we must prove there exists a bijective function $f : A \to B$.

Let $\lambda_\tau : A \to B$ be defined by $\lambda_\tau(\sigma) = \tau\sigma$ for all $\sigma \in A$.

Let $\sigma \in A$. Then $\sigma \in S_n$ and σ is even.

By closure of S_n under $\circ$, we have $\tau\sigma \in S_n$. Since σ is even and τ is odd, then σ and τ have opposite parity. The composition of permutations of opposite parity is odd. Hence, $\tau\sigma$ is odd. Since $\tau\sigma \in S_n$ and $\tau\sigma$ is odd, then $\tau\sigma \in B$.

Since $\sigma, \tau \in S_n$ and $\circ$ is a binary operation on S_n, then the product $\tau\sigma$ is unique.

Therefore, $\tau\sigma \in B$ and is unique, so $\lambda_\tau(\sigma) \in B$ is unique.

Thus, λ is a function.

We prove λ is injective. Let $\sigma_1, \sigma_2 \in S_n$ such that $\lambda_\tau(\sigma_1) = \lambda_\tau(\sigma_2)$. Then $\tau\sigma_1 = \tau\sigma_2$. Since $\tau \in B$ and $B \subset S_n$, then $\tau \in S_n$. Since $\tau, \sigma_1, \sigma_2 \in S_n$ and S_n is a group, we apply the cancellation law to obtain $\sigma_1 = \sigma_2$. Therefore, $\lambda_\tau(\sigma_1) = \lambda_\tau(\sigma_2)$ implies $\sigma_1 = \sigma_2$, so λ is injective.

We prove λ is surjective. Let β be an arbitrary element of B. We must find some $\alpha \in A$ such that $\phi(\alpha) = \beta$.

Let $\alpha = \tau\beta$.

Since $\tau, \beta \in S_n$ and S_n is closed under $\circ$, then $\tau\beta \in S_n$.

Since τ and β are odd permutations, then τ and β have the same parity. The composition of two permutations of the same parity is even. Therefore, $\tau\beta$ is even.

Since $\tau\beta \in S_n$ and $\tau\beta$ is even, then $\tau\beta \in A$.

Hence, $\alpha \in A$. Observe that

$$\begin{aligned} \lambda_\tau(\alpha) &= \lambda_\tau(\tau\beta) \\ &= \tau(\tau\beta) \\ &= (\tau\tau)\beta \\ &= id\beta \\ &= \beta. \end{aligned}$$

Therefore, λ is surjective.

Since λ is injective and surjective, then $\lambda_\tau : A \to B$ is bijective. Thus, $\lambda_\tau : A \to B$ is a bijective function, so $|A| = |B|$.

Observe that

$$\begin{aligned} n! &= |S_n| \\ &= |A \cup B| \\ &= |A| + |B| - |A \cap B| \\ &= |A| + |A| - |\emptyset| \\ &= 2 * |A| - 0 \\ &= 2|A|. \end{aligned}$$

Therefore, $|A| = \frac{n!}{2}$. Since $A_n = A$, then $|A_n| = |A| = \frac{n!}{2}$, so $|A_n| = \frac{n!}{2}$. $\square$

Symmetry groups

Theorem 68. *The set of all geometric transformations of n dimensional space is a group under function composition.*

Proof. Let n be a positive integer. Let $X = \mathbb{R}^n$ be an n dimensional vector space. Since $(0, 0, ..., 0) \in \mathbb{R}^n$, then $\mathbb{R}^n \neq \emptyset$. Let S_X be the set of all geometric transformations of $\mathbb{R}^n$. Then S_X is the set of all bijective maps from $\mathbb{R}^n$ to $\mathbb{R}^n$. Hence, S_X is the set of all permutations of $\mathbb{R}^n$. Let $\circ$ be function composition on S_X. Then $(S_X, \circ)$ is the symmetric group on $\mathbb{R}^n$. $\square$

Theorem 69. *The set of all bijective isometries of* 2 *dimensional space is a subgroup of* $Sym(\mathbb{R}^2)$.

Proof. Let $\mathbb{R}^2$ be 2 dimensional space. Let $Sym(\mathbb{R}^2)$ be the symmetric group on $\mathbb{R}^2$ under function composition $\circ$. Then $Sym(\mathbb{R}^2)$ is the group of all permutations of $\mathbb{R}^2$. Hence, $Sym(\mathbb{R}^2)$ is the set of all bijective maps from $\mathbb{R}^2$ onto $\mathbb{R}^2$.

Let S be the set of all bijective isometries of $\mathbb{R}^2$.

Then $S = \{\alpha | \alpha : \mathbb{R}^2 \to \mathbb{R}^2 \text{is a bijective isometry}\}$.

We must prove $(S, \circ)$ is a subgroup of $Sym(\mathbb{R}^2)$.

Let $\alpha \in S$. Then $\alpha : \mathbb{R}^2 \to \mathbb{R}^2$ is a bijective isometry. Hence, α is a bijective function, so $\alpha \in Sym(\mathbb{R}^2)$. Thus, $\alpha \in S$ implies $\alpha \in Sym(\mathbb{R}^2)$, so $S \subset Sym(\mathbb{R}^2)$.

Let id be the identity of $Sym(\mathbb{R}^2)$. Then $id : \mathbb{R}^2 \to \mathbb{R}^2$ is the identity map and $id(P) = P$ for every point $P \in \mathbb{R}^2$. Since the identity map is bijective, then id is bijective.

We prove id is an isometry. Let $P, Q \in \mathbb{R}^2$. Let $d(P, Q)$ be the distance between points P and Q in $\mathbb{R}^2$. Then $d(id(P), id(Q)) = d(P, Q)$. Hence, id is an isometry. Since id is a bijective isometry, then $id \in S$.

Let $\alpha, \beta \in S$. Then $\alpha : \mathbb{R}^2 \to \mathbb{R}^2$ and $\beta : \mathbb{R}^2 \to \mathbb{R}^2$ are bijective isometries.

We prove $\beta\alpha$ is an isometry.

Let $P, Q \in \mathbb{R}^2$. Since α is an isometry, then the distance between the images of P and Q under α equals the distance between P and Q. Hence, $d(\alpha(P), \alpha(Q)) = d(P, Q)$.

Since β is an isometry, then the distance between the images of $\alpha(P)$ and $\alpha(Q)$ under β equals the distance between $\alpha(P)$ and $\alpha(Q)$. Hence, $d(\beta(\alpha(P)), \beta(\alpha(Q))) = d(\alpha(P), \alpha(Q))$.

Therefore, by transitivity of equality, we have

$d(\beta(\alpha(P)), \beta(\alpha(Q))) = d(P, Q)$.

Thus, $d((\beta\alpha)(P), (\beta\alpha)(Q)) = d(P, Q)$. Hence, the distance between the images of P and Q under $\beta\alpha$ equals the distance between P and Q. Therefore, $\beta\alpha$ is an isometry.

The composition of bijections is a bijection. Hence, $\beta\alpha$ is a bijection, so $\beta\alpha$ is bijective. Since $\beta\alpha$ is a bijective isometry, then $\beta\alpha \in S$.

Therefore, S is closed under function composition.

Let $\alpha \in S$. Then $\alpha : \mathbb{R}^2 \to \mathbb{R}^2$ is a bijective isometry. Let $\alpha^{-1} : \mathbb{R}^2 \to \mathbb{R}^2$ be the inverse of α in $Sym(\mathbb{R}^2)$. Then $\alpha\alpha^{-1} = \alpha^{-1}\alpha = id$, so $(\alpha^{-1})^{-1} = \alpha$. Thus, α^{-1} is invertible. A map is invertible iff it is bijective. Hence, α^{-1} is bijective.

To prove $\alpha^{-1} \in S$, we must prove α^{-1} is an isometry. To prove α^{-1} is an isometry, let $P, Q \in \mathbb{R}^2$ be arbitrary.

We must prove $d(\alpha^{-1}(P), \alpha^{-1}(Q)) = d(P, Q)$.

Since α is bijective, then α is surjective. Hence, there exist points $A, B \in \mathbb{R}^2$ such that $\alpha(A) = P$ and $\alpha(B) = Q$.

Observe that

$$\begin{aligned} d(\alpha^{-1}(P), \alpha^{-1}(Q) &= d(A, B) \\ &= d(\alpha(A), \alpha(B)) \\ &= d(P, Q). \end{aligned}$$

Hence, α^{-1} is an isometry. Since α^{-1} is a bijective isometry, then $\alpha^{-1} \in S$. Thus, S is closed under taking inverses.

Therefore, S is a subgroup of $Sym(\mathbb{R}^2)$. $\square$

Theorem 70. *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 $\mathbb{R}^2$.*

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

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

Let X be a regular $n-$ gon in $\mathbb{R}^2$.

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

Let G be the set of all symmetries of a regular n-gon.

Then $G = \{\sigma : \sigma(\text{ is a symmetry of } X \} = \{\sigma : \mathbb{R}^2 \to \mathbb{R}^2 \in Iso(\mathbb{R}^2) | \sigma(X) = X\}$.

Observe that $G \subset Iso(\mathbb{R}^2)$.

We apply the subgroup test.

Let id be the identity element of $Iso(\mathbb{R}^2)$. Then $id : \mathbb{R}^2 \to \mathbb{R}^2$ is the identity map and $id \in Iso(\mathbb{R}^2)$ and $id(P) = P$ for all points $P \in \mathbb{R}^2$.

Let $p \in X$. Since $X \subset \mathbb{R}^2$, then $p \in \mathbb{R}^2$. Hence, $id(p) = p$. Since p is arbitrary, then $id(p) = p$ for all points $p \in X$. Hence, $id(X) = X$.

Since $id \in Iso(\mathbb{R}^2)$ and $id(X) = X$, then $id \in G$. Therefore the identity of $Iso(\mathbb{R}^2)$ is in G.

Let $\alpha, \beta \in G$. Then α and β are symmetries of X. Hence, $\alpha : \mathbb{R}^2 \to \mathbb{R}^2$ is a bijective isometry such that $\alpha(X) = X$ and $\beta : \mathbb{R}^2 \to \mathbb{R}^2$ is a bijective isometry such that $\beta(X) = X$. Since $\alpha, \beta \in G$ and $G \subset Iso(\mathbb{R}^2)$, then $\alpha, \beta \in Iso(\mathbb{R}^2)$. By closure of $Iso(\mathbb{R}^2)$ under $\circ$, $\alpha\beta \in Iso(\mathbb{R}^2)$.

Observe that

$$\begin{aligned} (\alpha\beta)(X) &= \alpha(\beta(X)) \\ &= \alpha(X) \\ &= X. \end{aligned}$$

Hence, $(\alpha\beta)(X) = X$.

Since $\alpha\beta \in Iso(\mathbb{R}^2)$ and $(\alpha\beta)(X) = X$, then $\alpha\beta \in G$. Therefore, G is closed under $\circ$.

Let $\alpha \in G$. Then $\alpha : \mathbb{R}^2 \to \mathbb{R}^2$ is a bijective isometry such that $\alpha(X) = X$.

Let α^{-1} be the inverse of $\alpha \in Iso(\mathbb{R}^2)$. Then $\alpha^{-1} : \mathbb{R}^2 \to \mathbb{R}^2$ is a bijective isometry. Since $\alpha(X) = X$ and α^{-1} is the inverse of α, then $\alpha^{-1}(X) = X$. Since $\alpha^{-1} \in Iso(\mathbb{R}^2)$ and $\alpha^{-1}(X) = X$, then $\alpha^{-1} \in G$.

Therefore, $(G, \circ)$ is a subgroup of $(Iso(\mathbb{R}^2), \circ)$. $\square$

Theorem 71. *$(D_n, \circ)$ is isomorphic to a subgroup of $(S_n, \circ)$.*

Solution. We first construct a set H that is a subset of S_n and show that $H < S_n$. Then we show that $D_n \cong H$. $\square$

Proof. Let $f : D_n \to S_n$ be defined by $f(\alpha) = \beta$ for all $\alpha \in D_n$, where β is the unique permutation of the n vertices of the regular $n-$gon associated with the symmetry α. Clearly, f is a function. Since each distinct symmetry corresponds to a distinct permutation, then f is injective.

Let H be the set of all permutations of the n vertices associated with each symmetry of D_n. Then $H = \{f(\alpha) \in S_n : \alpha \in D_n\}$. Hence, $H \subset S_n$.

We prove $H < S_n$. Let id be the identity symmetry in D_n. Then $f(id) = (1)$, the identity permutation in S_n, so $(1) \in H$. Hence, H is not empty.

Every subset of a finite set is finite. Thus, H is finite since S_n is finite. Hence, H is a nonempty finite subset of S_n.

Let $\sigma, \tau \in H$. Then $\sigma = f(\alpha)$ for some $\alpha \in D_n$ and $\tau = f(\beta)$ for some $\beta \in D_n$. Multiplication of σ and τ in H corresponds to multiplication of α and β in D_n. Thus, $\sigma\tau = f(\alpha\beta)$. Since D_n is closed under function composition, then $\alpha\beta \in D_n$. Hence, there exists $\alpha\beta \in D_n$ such that $f(\alpha\beta) = \sigma\tau$, so $\sigma\tau \in H$. Therefore, H is closed under function composition.

Thus, by the finite subgroup test, $H < S_n$.

Let ϕ be the restriction of f to H. Then $\phi : D_n \to H$ is a function defined by $\phi(\alpha) = f(\alpha)$ for all $\alpha \in D_n$.

Let $\beta \in H$. Then there exists $\alpha \in D_n$ such that $f(\alpha) = \beta$. Observe that $\phi(\alpha) = f(\alpha) = \beta$. Hence, there exists $\alpha \in D_n$ such that $\phi(\alpha) = \beta$, so ϕ is surjective.

Let $\alpha, \beta \in D_n$ such that $\phi(\alpha) = \phi(\beta)$. Then $f(\alpha) = f(\beta)$. Since f is injective, then $\alpha = \beta$. Hence, $\phi(\alpha) = \phi(\beta)$ implies $\alpha = \beta$, so ϕ is injective. Thus, ϕ is bijective.

Let $\alpha, \beta \in D_n$ such that $\phi(\alpha) = \sigma$ and $\phi(\beta) = \tau$. Then $\sigma, \tau \in H$ since ϕ is a function. Multiplication of σ and τ in H corresponds to multiplication of α and β in D_n. Thus, $\sigma\tau = f(\alpha\beta)$.

Observe that

$$\begin{aligned} \phi(\alpha\beta) &= f(\alpha\beta) \\ &= \sigma\tau \\ &= \phi(\alpha)\phi(\beta). \end{aligned}$$

Therefore, ϕ is a homomorphism, so ϕ is a bijective homomorphism. Thus, $\phi : D_n \to H$ is an isomorphism, so $D_n \cong H$. $\square$

Cosets

Theorem 72. *Let H be a subgroup of a group G. Define relation $\sim_L$ on G for every $a, b \in G$ by $a \sim_L b$ iff $a^{-1}b \in H$ and $a \sim_R b$ iff $ab^{-1} \in H$. Then $\sim_L$ and $\sim_R$ are equivalence relations on G.*

Solution. To prove $\sim_L$ and $\sim_R$ are equivalence relations, we must prove each relation is reflexive, symmetric, and transitive. $\square$

Proof. Let a, b, and c be arbitrary elements of G.

We prove $\sim_L$ is reflexive. Observe that $a^{-1}a = e \in G$. Since H is a subgroup of G, then $e \in H$. Hence, $a^{-1}a \in H$, so $a \sim_L a$. Therefore, $\sim_L$ is reflexive.

We prove $\sim_L$ is symmetric. Suppose $a \sim_L b$. Then $a^{-1}b \in H$. Since H is a group, then the inverse of $a^{-1}b$ is in H. Hence, $(a^{-1}b)^{-1} = b^{-1}(a^{-1})^{-1} = b^{-1}a \in H$. Thus, $b \sim_L a$, so $\sim_L$ is symmetric.

We prove $\sim_L$ is transitive. Suppose $a \sim_L b$ and $b \sim_L c$. Then $a^{-1}b \in H$ and $b^{-1}c \in H$. Since H is closed under $\cdot$, then $(a^{-1}b)(b^{-1}c) \in H$. Hence, $(a^{-1}b)(b^{-1}c) = a^{-1}(bb^{-1})c = a^{-1}ec = a^{-1}c \in H$. Therefore, $a \sim_L c$, so $\sim_L$ is transitive.

Since $\sim_L$ is reflexive, symmetric, and transitive on G, then $\sim_L$ is an equivalence relation on G.

We prove $\sim_R$ is reflexive. Observe that $aa^{-1} = e \in G$. Since H is a subgroup of G, then $e \in H$. Hence, $aa^{-1} \in H$, so $a \sim_R a$. Therefore, $\sim_R$ is reflexive.

We prove $\sim_R$ is symmetric. Suppose $a \sim_R b$. Then $ab^{-1} \in H$. Since H is a group, then the inverse of ab^{-1} is in H. Hence, $(ab^{-1})^{-1} = (b^{-1})^{-1}a^{-1} = ba^{-1} \in H$. Thus, $b \sim_R a$, so $\sim_R$ is symmetric.

We prove $\sim_R$ is transitive. Suppose $a \sim_R b$ and $b \sim_R c$. Then $ab^{-1} \in H$ and $bc^{-1} \in H$. Since H is closed under $\cdot$, then $(ab^{-1})(bc^{-1}) \in H$. Hence, $(ab^{-1})(bc^{-1}) = a(b^{-1}b)c^{-1} = aec^{-1} = ac^{-1} \in H$. Therefore, $a \sim_R c$, so $\sim_R$ is transitive.

Since $\sim_R$ is reflexive, symmetric, and transitive on G, then $\sim_R$ is an equivalence relation on G. $\square$

Theorem 73. *Let H be a subgroup of 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. $aH = bH$.

Proof. We prove $a^{-1}b \in H \Rightarrow (\exists h \in H)(a = bh)$.

Suppose $a^{-1}b \in H$. Let $h = (a^{-1}b)^{-1}$. Since H is a group, then every element of H has an inverse in H. Since $a^{-1}b \in H$, then its inverse $(a^{-1}b)^{-1}$ is in H. Hence, $h \in H$. Observe that

$$\begin{aligned} bh &= b((a^{-1}b)^{-1}) \\ &= b(b^{-1}(a^{-1})^{-1}) \\ &= b(b^{-1}a) \\ &= (bb^{-1})a \\ &= ea \\ &= a. \end{aligned}$$

Therefore, there exists $h \in H$ such that $a = bh$, as desired.

We prove $(\exists h \in H)(a = bh) \Rightarrow a \in bH$.

Suppose there exists $h \in H$ such that $a = bh$. Then $a \in bH$, by definition of bH.

We prove $a \in bH \Rightarrow (aH = bH)$.

Suppose $a \in bH$. To prove $aH = bH$, we prove $aH \subset bH$ and $bH \subset aH$.

Let $x \in aH$. Then there exists $h_1 \in H$ such that $x = ah_1$, by definition of aH. Since $a \in bH$, then there exists $h_2 \in H$ such that $a = bh_2$, by definition of bH. Let $h = h_2h_1$. Since H is a group, then H is closed under its binary operation. Since $h_1, h_2 \in H$, then $h_2h_1 \in H$, so $h \in H$.

Observe that

$$\begin{aligned} bh &= b(h_2h_1) \\ &= (bh_2)h_1 \\ &= ah_1 \\ &= x. \end{aligned}$$

Hence, there exists $h \in H$ such that $x = bh$, so by definition of bH, $x \in bH$. Therefore, $x \in aH$ implies $x \in bH$, so $aH \subset bH$.

Let $y \in bH$. Then there exists $h_1 \in H$ such that $y = bh_1$, by definition of bH. Since $a \in bH$, then by definition of bH, there exists $h_2 \in H$ such that $a = bh_2$. Let $h = h_2^{-1}h_1$. Since H is closed under its binary operation and $h_1, h_2^{-1} \in H$, then $h \in H$. Observe that

$$\begin{aligned} ah &= (bh_2)(h_2^{-1}h_1) \\ &= b(h_2h_2^{-1})h_1 \\ &= beh_1 \\ &= bh_1 \\ &= y. \end{aligned}$$

Hence, there exists $h \in H$ such that $y = ah$, so by definition of aH, $y \in aH$. Therefore, $y \in bH$ implies $y \in aH$, so $bH \subset aH$.

Since $aH \subset bH$ and $bH \subset aH$, then $aH = bH$, as desired.

We prove $(aH = bH) \Rightarrow a^{-1}b \in H$.

Suppose $aH = bH$. Since $a \in aH$ and $aH = bH$, then $a \in bH$. Thus, there exists $h \in H$ such that $a = bh$, by definition of bH. Observe that

$$\begin{aligned} a^{-1}b &= (bh)^{-1}b \\ &= (h^{-1}b^{-1})b \\ &= h^{-1}(b^{-1}b) \\ &= h^{-1}e \\ &= h^{-1}. \end{aligned}$$

Since H is a group, then each element of H has an inverse in H. Therefore, since $h \in H$, then $h^{-1} \in H$. Hence, $a^{-1}b \in H$, as desired. $\square$

Theorem 74. *Let H be a subgroup of 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. $Ha = Hb$.

Proof. We prove $ab^{-1} \in H \Rightarrow (\exists h \in H)(a = hb)$.

Suppose $ab^{-1} \in H$. Let $h = ab^{-1}$. Then $h \in H$.

Observe that

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

Therefore, there exists $h \in H$ such that $a = hb$, as desired.

We prove $(\exists h \in H)(a = hb) \Rightarrow a \in Hb$.

Suppose there exists $h \in H$ such that $a = hb$. Then $a \in Hb$, by definition of Hb.

We prove $a \in Hb \Rightarrow (Ha = Hb)$.

Suppose $a \in Hb$. To prove $Ha = Hb$, we prove $Ha \subset Hb$ and $Hb \subset Ha$.

Let $x \in Ha$. Then there exists $h_1 \in H$ such that $x = h_1a$, by definition of Ha. Since $a \in Hb$, then there exists $h_2 \in H$ such that $a = h_2b$, by definition of Hb. Let $h = h_1h_2$. Since H is a group, then H is closed under its binary operation. Since $h_1, h_2 \in H$, then $h \in H$.

Observe that

$$\begin{aligned} hb &= (h_1h_2)b \\ &= h_1(h_2b) \\ &= h_1a \\ &= x. \end{aligned}$$

Hence, there exists $h \in H$ such that $x = hb$, so by definition of Hb, $x \in Hb$. Therefore, $x \in Ha$ implies $x \in Hb$, so $Ha \subset Hb$.

Let $y \in Hb$. Then there exists $h_1 \in H$ such that $y = h_1b$, by definition of Hb. Since $a \in Hb$, then by definition of Hb, there exists $h_2 \in H$ such that $a = h_2b$. Let $h = h_1h_2^{-1}$. Since H is closed under its binary operation and $h_1, h_2^{-1} \in H$, then $h \in H$.

Observe that

$$\begin{aligned} ha &= (h_1h_2^{-1})(h_2b) \\ &= h_1(h_2^{-1}h_2)b \\ &= h_1eb \\ &= h_1b \\ &= y. \end{aligned}$$

Hence, there exists $h \in H$ such that $y = ha$, so by definition of Ha, $y \in Ha$. Therefore, $y \in Hb$ implies $y \in Ha$, so $Hb \subset Ha$.

Since $Ha \subset Hb$ and $Hb \subset Ha$, then $Ha = Hb$, as desired.

We prove $(Ha = Hb) \Rightarrow ab^{-1} \in H$.

Suppose $Ha = Hb$. Since $a \in Ha$ and $Ha = Hb$, then $a \in Hb$. Thus, there exists $h \in H$ such that $a = hb$, by definition of Hb. Right multiply by b^{-1} to obtain $ab^{-1} = h$. Therefore, since $h \in H$, then $ab^{-1} \in H$, as desired. □

Lemma 75. *Let H be a subgroup of G. Let $a, b \in G$. Then $aH = bH$ iff $Ha^{-1} = Hb^{-1}$.*

Proof. Observe that

$$\begin{aligned} aH = bH &\Leftrightarrow a^{-1}b \in H \\ &\Leftrightarrow a^{-1}(b^{-1})^{-1} \in H \\ &\Leftrightarrow Ha^{-1} = Hb^{-1}. \end{aligned}$$

□

Theorem 76. *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.*

Solution. To prove the number of left cosets of H equals the number of right cosets of H, we let H_L be the collection of distinct left cosets of H and H_R be the collection of distinct right cosets of H. Thus $H_L = \{gH : g \in G\}$ and $H_R = \{Hg : g \in G\}$.

We must prove $|H_L| = |H_R|$.

To prove this, we must devise a bijective map $\phi : H_L \mapsto H_R$.

The key insight is to use figure out what map would work.

We try $\phi(gH) = Hg^{-1}$.

Thus, we must show that ϕ maps each $gH \in H_L$ to a unique $Hg^{-1} \in H_R$ and show that ϕ is injective and surjective. □

Proof. Let H_L be the collection of distinct left cosets of H in G. Let H_R be the collection of distinct right cosets of H in G. Then $H_L = \{gH : g \in G\}$ and $H_R = \{Hg : g \in G\}$.

Let $\phi : H_L \mapsto H_R$ be a binary relation defined by $\phi(gH) = Hg^{-1}$ for all $g \in G$.

Suppose $g \in G$. Then $gH \in H_L$, so $\phi(gH) = Hg^{-1}$. Since G is a group and $g \in G$, then $g^{-1} \in G$. Hence, $Hg^{-1} \in H_R$.

To prove ϕ is well-defined, let a and b be arbitrary elements of G. Then aH and bH are arbitrary left cosets in H_L. Suppose $aH = bH$. Then $\phi(aH) = Ha^{-1}$ and $\phi(bH) = Hb^{-1}$. Since $Ha^{-1} = Hb^{-1}$ iff $aH = bH$, then $Ha^{-1} = Hb^{-1}$. Hence, $\phi(aH) = \phi(bH)$. Therefore, $aH = bH$ implies $\phi(aH) = \phi(bH)$, so ϕ is a well defined map from H_L to H_R.

We prove ϕ is injective. Suppose aH and bH are arbitrary left cosets in H_L such that $\phi(aH) = \phi(bH)$. Then a and b are some elements in G and

$Ha^{-1} = Hb^{-1}$. By a previous lemma, $Ha^{-1} = Hb^{-1}$ iff $aH = bH$. Hence, we conclude $aH = bH$. Therefore, $\phi(aH) = \phi(bH)$ implies $aH = bH$, so ϕ is injective.

We prove ϕ is surjective. Suppose Hg is an arbitrary right coset in H_R. Then $g \in G$. Since G is a group, then $g^{-1} \in G$. Let $a = g^{-1}H$. Since there exists $g^{-1} \in G$ such that $a = g^{-1}H$, then $a \in H_L$. Observe that $\phi(a) = \phi(g^{-1}H) = H(g^{-1})^{-1} = Hg$. Therefore, there exists $a \in H_L$ such that $\phi(a) = Hg$, so ϕ is surjective.

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

Therefore, $\phi : H_L \mapsto H_R$ is a bijective map, so $|H_L| = |H_R|$, as desired. □

Theorem 77. *Let H be a subgroup of a group G.*

Let $g \in G$ be fixed.

Then $|gH| = |H|$ and $|Hg| = |H|$.

Solution. We must prove $|gH| = |H|$ and $|Hg| = |H|$.

To prove $|gH| = |H|$, we show there exists a bijection between gH and H.

To prove $|Hg| = |H|$, we show there exists a bijection between Hg and H.

To prove $|gH| = |H|$, we must devise a bijective map $\phi : H \mapsto gH$.

We know that the left coset $gH = \{gh : h \in H\}$.

Hence, let's try $\phi(h) = gh$ for all $h \in H$.

We observe this is similar to a left representation of H, except that g is not necessarily in H.

We must prove ϕ maps each $h \in H$ to some element in gH and show that ϕ is one to one and onto gH.

Since ϕ is bijective, then we conclude $|H| = |gH|$.

Hence, if H is of finite order, then gH is finite and gH has the same number of elements as H. □

Proof. To prove $|gH| = |H|$, let $\phi : H \mapsto gH$ be a binary relation defined by $\phi(h) = gh$ for all $h \in H$.

Let h be an arbitrary element of H.

Then $\phi(h) = gh$.

Since $gh \in gH$, then $\phi(h) \in gH$.

We prove ϕ is well defined.

Suppose h_1 and h_2 are arbitrary elements of H such that $h_1 = h_2$.

We must prove $\phi(h_1) = \phi(h_2)$.

Since $h_1, h_2 \in H$ and $H \subset G$, then $h_1, h_2 \in G$.

Since $g, h_1, h_2 \in G$ and G is a group, then we left multiply by g to obtain $gh_1 = gh_2$.

Observe that $\phi(h_1) = gh_1 = gh_2 = \phi(h_2)$.

Hence, ϕ is well defined, so $\phi : H \mapsto gH$ is a function.

Suppose h_1 and h_2 are arbitrary elements of H such that $\phi(h_1) = \phi(h_2)$.

Then $gh_1 = gh_2$.

Since $h_1, h_2 \in H$ and $H \subset G$, then $h_1, h_2 \in G$.

Since G is a group and $g, h_1, h_2 \in G$, then we apply the left cancellation law to obtain $h_1 = h_2$.

Hence, $\phi(h_1) = \phi(h_2)$ implies $h_1 = h_2$, so ϕ is injective.

Suppose k is an arbitrary element of gH.

Then there exists some $h \in H$ such that $k = gh$.

Observe that $\phi(h) = gh = k$.

Hence, there exists $h \in H$ such that $\phi(h) = k$, so ϕ is surjective.

Since ϕ is a function that is injective and surjective, then $\phi : H \mapsto gH$ is bijective.

Therefore, $|gH| = |H|$, as desired.

To prove $|Hg| = |H|$, let $\sigma : H \mapsto Hg$ be a binary relation defined by $\sigma(h) = hg$ for all $h \in H$.

Let h be an arbitrary element of H.

Then $\sigma(h) = hg$.

Since $hg \in Hg$, then $\sigma(h) \in Hg$.

We prove σ is well defined.

Suppose h_1 and h_2 are arbitrary elements of H such that $h_1 = h_2$.

We must prove $\sigma(h_1) = \sigma(h_2)$.

Since $h_1, h_2 \in H$ and $H \subset G$, then $h_1, h_2 \in G$.

Since $g, h_1, h_2 \in G$ and G is a group, then we right multiply by g to obtain $h_1 g = h_2 g$.

Observe that $\sigma(h_1) = h_1 g = h_2 g = \sigma(h_2)$.

Hence, σ is well defined, so $\sigma : H \mapsto Hg$ is a function.

Suppose h_1 and h_2 are arbitrary elements of H such that $\sigma(h_1) = \sigma(h_2)$.

Then $h_1 g = h_2 g$.

Since $h_1, h_2 \in H$ and $H \subset G$, then $h_1, h_2 \in G$.

Since G is a group and $g, h_1, h_2 \in G$, then we apply the right cancellation law to obtain $h_1 = h_2$.

Hence, σ is injective.

Suppose k is an arbitrary element of Hg.

Then there exists some $h \in H$ such that $k = hg$.

Observe that $\sigma(h) = hg = k$.

Hence, σ is surjective.

Since σ is a function that is injective and surjective, then $\sigma : H \mapsto Hg$ is bijective.

Therefore, $|Hg| = |H|$, as desired. $\square$

Finite Groups

Theorem 78. ***Lagrange's Theorem***
The order of a subgroup of a finite group divides the order of the group.

Proof. Let H be a subgroup of a finite group G.
We must prove $|H|$ divides $|G|$.
Since G is a finite group, then $|G| = n$ for some positive integer n.
Since G is finite and $H \subset G$, then H is finite.
Hence, $|H| = m$ for some positive integer m.

To prove $|H|$ divides $|G|$, we must prove $m|n$.
Let $g \in G$.
Let gH be the left coset of H in G with representative g.
Then $|gH| = |H| = m$.
Hence, each left coset of H in G contains the same number of elements as H.

Since G is finite, then there are a finite number of subsets of G.
In particular, there are a finite number of left cosets of H in G.
Let k be the number of left cosets of H in G.
Then k is an integer.
Since H is a left coset, then $k > 0$, so k is a positive integer.

Since the collection of left cosets of H in G is a partition of G, then the number of elements in G equals the number of left cosets times the number of elements in each left coset.
Thus, $|G| = km = k|H|$.
Therefore, $|H|$ divides $|G|$. $\square$

Corollary 79. *The order of an element of a finite group divides the order of the group.*

Solution. This means:
If G is a finite group, then the order of $g \in G$ divides the order of G. $\square$

Proof. Let G be a finite group.
Then there exists a positive integer n such that $|G| = n$.

Let $g \in G$.
Every element of a finite group has finite order.
In particular, g has finite order.
Let m be the order of g.
Then m is the order of the cyclic subgroup generated by g.
Let H be the cyclic subgroup of G generated by g.
Then $m = |H|$ and $H < G$.
Since $H < G$ and G is finite, then by LaGrange's theorem, $|H|$ divides $|G|$.

Therefore, $m|n$. $\square$

Corollary 80. *Let G be a finite group.*
If $H < K < G$, then $[G : H] = [G : K][K : H]$.

Proof. Suppose $H < K < G$.
Then $H < G$ and

$$\begin{aligned} [G : H] &= \frac{|G|}{|H|} \\ &= \frac{|G|}{|K|} * \frac{|K|}{|H|} \\ &= [G : K][K : H]. \end{aligned}$$

$\square$

Corollary 81. *Let G be a finite group of order n.*
Then $g^n = e$ for all $g \in G$.

Solution. Let $n \in \mathbb{Z}^+$. Let e be the identity of G.
We must prove $(\forall g \in G)(g^n = e)$. $\square$

Proof. Suppose G is a finite group of order n. Then n is a positive integer and $|G| = n$.
Let g be an arbitrary element of G with identity e.
Every element in a finite group has finite order.
In particular, g has finite order.
Let m be the order of g.
The order of g is the order of the cyclic subgroup generated by g.
Let H be the cyclic subgroup of G generated by g.
Then $m = |H|$ and $H < G$.
Since $H < G$ and G is finite, then by LaGrange's theorem, the order of H divides the order of G.
Hence, $m|n$.
Since the order of g is m, then $g^n = e$ iff $m|n$. Therefore, $g^n = e$. $\square$

Corollary 82. *Every group of prime order is cyclic.*

Solution. Let G be an arbitrary group of prime order.
To prove G is cyclic, we must find an element $a \in G$ such that $G = \{a^m : m \in \mathbb{Z}\}$.
How do we find a?
Consider the cyclic group generated by a. Then $\langle a \rangle = \{a^m : m \in \mathbb{Z}\}$. $\square$

Proof. Let G be an arbitrary group of prime order p.
Then $|G| = p$.
Since p is prime, then $p \geq 2$.
Therefore, there are at least two elements in G and G is finite.
Let e be the identity of G.

Since at least two elements exist in G, then there exists at least one element that is distinct from e.

Let a be an arbitrary element of G such that $a \neq e$.

Every element of a finite group has finite order.

In particular, a has finite order.

Let m be the order of a.

Then m is a positive integer.

The order of a is the order of the cyclic subgroup generated by a.

Let H be the cyclic subgroup of G generated by a.

Then $H = \{a^k : k \in \mathbb{Z}\}$ and $m = |H|$ and $H < G$.

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

Since $e = a^0$, then $e \in H$.

Since $a \neq e$, then this implies H contains at least two elements.

Hence, $|H| \geq 2$, so $|H| > 1$.

Therefore, $m > 1$.

Since $H < G$ and G is finite, then by LaGrange's theorem, the order of H divides the order of G.

Hence, $m|p$.

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

Thus, either $m = 1$ or $m = p$.

Since $m > 1$, then $m \neq 1$.

Therefore, $m = p$.

Hence, $|H| = p$.

Since $H \subset G$ and $|H| = p = |G|$ and G is finite, then $H = G$.

Thus, there exists $a \in G$ such that $G = H$.

Therefore, G is cyclic. $\square$

Direct Products

Theorem 83. *Let A, B be groups.*

Let G be the Cartesian product $A \times B = \{(a, b) : a \in A, b \in B\}$.

Define $\circ : G \times G \mapsto G$ by $(a_1, b_1) \circ (a_2, b_2) = (a_1 a_2, b_1 * b_2)$.

Then $(G, \circ)$ is a group, called the ***external direct product of*** *A* ***and*** *B.*

Proof. We prove $\circ$ is a binary operation.

We first prove G is closed under $\circ$.

Let $x, y \in G$.

Then there exist $a_1, a_2 \in A$ and $b_1, b_2 \in B$ such that $x = (a_1, b_1)$ and $y = (a_2, b_2)$.

Thus, $x \circ y = (a_1, b_1) \circ (a_2, b_2) = (a_1 a_2, b_1 b_2)$.

By closure of A and B, $a_1 a_2 \in A$ and $b_1 b_2 \in B$.

Hence, $xy \in G$, so G is closed under $\circ$.

We prove $\circ$ is well defined.

Suppose (x, y) and (z, w) are arbitrary elements of $G \times G$ such that $(x, y) = (z, w)$.

Then there exist $a_1, a_2, a_3, a_4 \in A$ and $b_1, b_2, b_3, b_4 \in B$ such that $x = (a_1, b_1)$ and $y = (a_2, b_2)$ and $z = (a_3, b_3)$ and $w = (a_4, b_4)$ and $x = z$ and $y = w$.

Thus, $a_1 = a_3$ and $b_1 = b_3$ and $a_2 = a_4$ and $b_2 = b_4$.

Observe that

$$\begin{aligned}
x \circ y &= (a_1, b_1) \circ (a_2, b_2) \\
&= (a_1 a_2, b_1 b_2) \\
&= (a_3 a_2, b_3 b_2) \\
&= (a_3 a_4, b_3 b_4) \\
&= (a_3, b_3) \circ (a_4, b_4) \\
&= z \circ w.
\end{aligned}$$

Therefore, $\circ$ is well defined.

Hence, $\circ$ is a binary operation on G.

Let $x, y, z \in G$. Then there exist $a_1, a_2, a_3 \in A$ and $b_1, b_2, b_3 \in B$ such that $x = (a_1, b_1)$ and $y = (a_2, b_2)$ and $z = (a_3, b_3)$. Observe that

$$\begin{aligned}
(xy)z &= [(a_1, b_1)(a_2, b_2)](a_3, b_3) \\
&= (a_1 a_2, b_1 b_2)(a_3, b_3) \\
&= ((a_1 a_2) a_3, (b_1 b_2) b_3) \\
&= (a_1 (a_2 a_3), b_1 (b_2 b_3)) \\
&= (a_1, b_1)(a_2 a_3, b_2 b_3) \\
&= (a_1, b_1)[(a_2, b_2)(a_3, b_3)] \\
&= x(yz).
\end{aligned}$$

Therefore, $\circ$ is associative.

Let e be the identity of A and e' be the identity of B.

Then $(e, e') \in G$.

Let x be an arbitrary element of G.

Then $x = (a, b)$ for some $a \in A$ and $b \in B$.

Observe that

$$\begin{aligned}
(e, e')(a, b) &= (ea, e'b) \\
&= (a, b) \\
&= (ae, be') \\
&= (a, b)(e, e').
\end{aligned}$$

Thus, (e, e') is an identity element of G.

Let $x \in G$. Then $x = (a, b)$ for some $a \in A$ and $b \in B$. Since A and B are groups, then $a^{-1} \in A$ and $b^{-1} \in B$. Hence, $(a^{-1}, b^{-1}) \in G$.

Observe that

$$\begin{aligned} (a,b)(a^{-1},b^{-1}) &= (aa^{-1}, bb^{-1}) \\ &= (e, e') \\ &= (a^{-1}a, b^{-1}b) \\ &= (a^{-1}, b^{-1})(a, b). \end{aligned}$$

Thus, the inverse of (a, b) is (a^{-1}, b^{-1}), so each element of G has an inverse in G.

Therefore, $(G, \circ)$ is a group. $\square$

Theorem 84. *Let $n \in \mathbb{Z}^+, n \geq 2$.*

The external direct product of n groups is a group.

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

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 $b = (b_1, b_2, ..., b_n)$. Thus, $a \circ b = (a_1, a_2, ..., a_n) \circ (b_1, b_2, ..., b_n) = (a_1b_1, a_2b_2, ..., a_nb_n)$. For each i, the group G_i is closed. Therefore, for each i, the product g_ih_i is in the group G_i. Hence, $ab \in G$, so G is closed under $\circ$.

Suppose (a, b) and (c, d) are arbitrary elements of $G \times G$ such that $(a, b) = (c, d)$. Then for each $i \in \{1, 2, ..., n\}$ there exist $a_i, b_i, c_i, d_i \in G_i$ such that $a = (a_1, a_2, ..., a_n)$ and $b = (b_1, b_2, ..., b_n)$ and $c = (c_1, c_2, ..., c_n)$ and $d = (d_1, d_2, ..., d_n)$ and $a = c$ and $b = d$. Thus, for each i, $a_i = c_i$ and $b_i = d_i$. Observe that

$$\begin{aligned} ab &= (a_1, a_2, ..., a_n)(b_1, b_2, ..., b_n) \\ &= (a_1b_1, a_2b_2, ..., a_nb_n) \\ &= (c_1b_1, c_2b_2, ..., c_nb_n) \\ &= (c_1d_1, c_2d_2, ..., c_nd_n) \\ &= (c_1, c_2, ..., c_n)(d_1, d_2, ..., d_n) \\ &= cd. \end{aligned}$$

Therefore, $\circ$ is well defined. Hence, $\circ$ is a binary operation on G.

Let $a, b, c \in G$. Then for each $i \in \{1, 2, ..., n\}$ there exist $a_i, b_i, c_i \in G_i$ such that $a = (a_1, a_2, ..., a_n)$ and $b = (b_1, b_2, ..., b_n)$ and $c = (c_1, c_2, ..., c_n)$. Observe that

$$\begin{aligned}
(ab)c &= [(a_1, a_2, ..., a_n)(b_1, b_2, ..., b_n)](c_1, c_2, ..., c_n) \\
&= (a_1b_1, a_2b_2, ..., a_nb_n)(c_1, c_2, ..., c_n) \\
&= ((a_1b_1)c_1, (a_2b_2)c_2, ..., (a_nb_n)c_n) \\
&= (a_1(b_1c_1), a_2(b_2c_2), ..., a_n(b_nc_n)) \\
&= (a_1, a_2, ..., a_n)(b_1c_1, b_2c_2, ..., b_nc_n) \\
&= (a_1, a_2, ..., a_n)[(b_1, b_2, ..., b_n)(c_1, c_2, ..., c_n)] \\
&= a(bc).
\end{aligned}$$

Therefore, $\circ$ is associative.

Let e_i be the identity of G_i for each $i \in \{1, 2, ..., n\}$. Then $(e_1, e_2, ..., e_n) \in G$. Let x be an arbitrary element of G. Then for each $i \in \{1, 2, ..., n\}$ there exist $a_i \in G_i$ such that $x = (a_1, a_2, ..., a_n)$. Observe that

$$\begin{aligned}
(e_1, e_2, ..., e_n)(a_1, a_2, ..., a_n) &= (e_1a_1, e_2a_2, ..., e_na_n) \\
&= (a_1, a_2, ..., a_n) \\
&= (a_1e_1, a_2e_2, ..., a_ne_n) \\
&= (a_1, a_2, ..., a_n)(e_1, e_2, ..., e_n).
\end{aligned}$$

Thus, $(e_1, e_2, ..., e_n)$ is an identity element of G.

Let a be an arbitrary element of G. Then for each $i \in \{1, 2, ..., n\}$ there exist $a_i \in G_i$ such that $a = (a_1, a_2, ..., a_n)$. Since each G_i is a group, then $a_i^{-1} \in G_i$ for each i. Hence, $(a_1^{-1}, a_2^{-1}, ..., a_n^{-1}) \in G$. Observe that

$$\begin{aligned}
(a_1, a_2, ..., a_n)(a_1^{-1}, a_2^{-1}, ..., a_n^{-1}) &= (a_1a_1^{-1}, a_2a_2^{-1}, ..., a_na_n^{-1}) \\
&= (e_1, e_2, ..., e_n) \\
&= (a_1^{-1}a_1, a_2^{-1}a_2, ..., a_n^{-1}a_n) \\
&= (a_1^{-1}, a_2^{-1}, ..., a_n^{-1})(a_1, a_2, ..., a_n).
\end{aligned}$$

Thus, the inverse of $(a_1, a_2, ..., a_n)$ is $(a_1^{-1}, a_2^{-1}, ..., a_n^{-1})$, so each element of G has an inverse in G.

Therefore, $(G, \circ)$ is a group. $\square$

Theorem 85. *A direct product of abelian groups is an abelian group.*

Proof. Let $n \in \mathbb{Z}^+, n \geq 2$. Let $G_1, G_2, ..., G_n$ be n abelian groups. Then $\prod_{i=1}^n G_i$ is the direct product of n groups. The direct product of n groups is a group. Therefore, $\prod_{i=1}^n G_i$ is a group.

Let $a, b \in \prod_{i=1}^n G_i$. 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 $b = (b_1, b_2, ..., b_n)$. Observe that

$$\begin{aligned}
ab &= (a_1, a_2, ..., a_n)(b_1, b_2, ..., b_n) \\
&= (a_1b_1, a_2b_2, ..., a_nb_n) \\
&= (b_1a_1, b_2a_2, ..., b_na_n) \\
&= (b_1, b_2, ..., b_n)(a_1, a_2, ..., a_n) \\
&= ba.
\end{aligned}$$

Therefore, component wise multiplication in $\prod_{i=1}^n G_i$ is commutative. Hence, $\prod_{i=1}^n G_i$ is abelian. Thus, $\prod_{i=1}^n G_i$ is an abelian group. $\square$

Theorem 86. *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.*

Solution. We must prove:
1. The order of (g, h) is finite.
2. The order of (g, h) equals $lcm(a, b)$. $\square$

Proof. Let e be the identity of G and e' be the identity of H. Then (e, e') is the identity of $G \times H$. Since $(g, h) \in G \times H$, then $g \in G$ and $h \in H$.

Suppose g and h have finite order. Let a be the order of g and let b be the order of h. Then a is the least positive integer such that $g^a = e$ and b is the least positive integer such that $h^b = e'$.

We prove the order of (g, h) is finite. Let $n = ab$. Then n is a positive integer and $a|n$ and $b|n$. For any integer M, $g^M = e$ iff $a|M$ and for any integer N, $h^N = e'$ iff $b|N$. Hence, $g^n = e$ iff $a|n$ and $h^n = e'$ iff $b|n$. Thus, $g^n = e$ and $h^n = e'$. Observe that

$$
\begin{aligned}
(g, h)^n &= (g, h)(g, h)...(g, h) \\
&= (g^n, h^n) \\
&= (e, e').
\end{aligned}
$$

Therefore, there exists a positive integer n such that $(g, h)^n = (e, e')$, so the order of (g, h) is finite.

Let k be the order of (g, h). Then k is the least positive integer such that $(g, h)^k = (e, e')$. Thus,

$$
\begin{aligned}
(e, e') &= (g, h)^k \\
&= (g, h)(g, h)...(g, h) \\
&= (g^k, h^k).
\end{aligned}
$$

Hence, $g^k = e$ and $h^k = e'$. Thus, $a|k$ and $b|k$.

Let m be the least common multiple of a and b. Then $a|m$ and $b|m$ and for every integer c, if $a|c$ and $b|c$, then $m|c$. Thus, if $a|k$ and $b|k$, then $m|k$. Since $a|k$ and $b|k$, then $m|k$.

Since $a|m$ and $b|m$, then $g^m = e$ and $h^m = e'$. Thus,

$$
\begin{aligned}
(e, e') &= (g^m, h^m) \\
&= (g, h)^m.
\end{aligned}
$$

For any integer N, $(g, h)^N = (e, e')$ iff $k|N$. Hence, in particular, $(g, h)^m = (e, e')$ iff $k|m$. Thus, $k|m$.

By the antisymmetric property of $\mathbb{Z}^+$, $k|m$ and $m|k$ implies $k = m$. Since $m, k \in \mathbb{Z}^+$ and $m|k$ and $k|m$, then we conclude $k = m$.

Therefore, the order of (g, h) is the least common multiple of a and b. $\square$

Corollary 87. *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 $a_1, a_2, ..., a_n$.*

Solution. We must prove:

1. The order of $(g_1, g_2, ..., g_n)$ is finite.
2. The order of $(g_1, g_2, ..., g_n)$ equals $lcm(a_1, a_2, ..., a_n)$. □

Proof. Let $G = G_1 \times G_2 \times ... \times G_n$. Then for each $i \in \{1, 2, ..., n\}$, G_i is a group. Let e_i be the identity of each group G_i. Then $(e_1, e_2, ..., e_n)$ is the identity of G. Since $(g_1, g_2, ..., g_n) \in G$, then each element g_i is in the group G_i.

Suppose each g_i has finite order a_i in G_i. Then for each i, a_i is the least positive integer such that $g_i^{a_i} = e_i$.

We prove the order of $(g_1, g_2, ..., g_n)$ is finite. Let $m = a_1 a_2 ... a_n$. Then m is a positive integer and for each i, $a_i | m$.

For each i and for any integer M, $g_i^M = e_i$ iff $a_i | M$. Hence, for each i, $g_i^m = e_i$ iff $a_i | m$. Thus, for each i, $g_i^m = e_i$. Observe that

$$\begin{aligned} (g_1, g_2, ..., g_n)^m &= (g_1^m, g_2^m, ..., g_n^m) \\ &= (e_1, e_2, ..., e_n). \end{aligned}$$

Therefore, there exists a positive integer m such that $(g_1, g_2, ..., g_n)^m = (e_1, e_2, ..., e_n)$, so the order of $(g_1, g_2, ..., g_n)$ is finite.

Let k be the order of $(g_1, g_2, ..., g_n)$. Then k is the least positive integer such that $(g_1, g_2, ..., g_n)^k = (e_1, e_2, ..., e_n)$. Thus,

$$\begin{aligned} (e_1, e_2, ..., e_n) &= (g_1, g_2, ..., g_n)^k \\ &= (g_1^k, g_2^k, ..., g_n^k). \end{aligned}$$

Hence, for each i, $g_i^k = e_i$. Thus, for each i, $a_i | k$.

Let s be the least common multiple of each a_i. Then for each i, $a_i | s$ and for every integer c, if each $a_i | c$, then $s | c$. Thus, if each $a_i | k$, then $s | k$. Since each a_i divides k, then $s | k$.

Since each a_i divides s, then $g_i^s = e_i$ for each i. Thus,

$$\begin{aligned} (e_1, e_2, ..., e_n) &= (g_1^s, g_2^s, ..., g_n^s) \\ &= (g_1, g_2, ..., g_n)^s. \end{aligned}$$

For any integer $N, (g_1, g_2, ..., g_n)^N = (e_1, e_2, ..., e_n)$ iff $k | N$. Hence, in particular, $(g_1, g_2, ..., g_n)^s = (e_1, e_2, ..., e_n)$ iff $k | s$. Thus, $k | s$.

By the antisymmetric property of $\mathbb{Z}^+$, $k | s$ and $s | k$ implies $k = s$. Since $s | k$ and $k | s$, then we conclude $k = s$.

Therefore, the order of
$(g_1, g_2, ..., g_n)$
is the least common multiple of $a_1, a_2, ..., a_n$. □

Theorem 88. *Let $m, n \in \mathbb{Z}^+$. Then $(\mathbb{Z}_m \times \mathbb{Z}_n, +) \cong (\mathbb{Z}_{mn}, +)$ iff $\gcd(m, n) = 1$.*

Proof. We prove $\gcd(m,n) = 1$ implies $(\mathbb{Z}_m \times \mathbb{Z}_n, +) \cong (\mathbb{Z}_{mn}, +)$.

Suppose $\gcd(m,n) = 1$. Observe that $(\mathbb{Z}_m, +)$ is a cyclic group with generator $[1]_m \in \mathbb{Z}_m$. Thus, the order of $[1]_m$ in $\mathbb{Z}_m$ is m. Observe that $(\mathbb{Z}_n, +)$ is a cyclic group with generator $[1]_n \in \mathbb{Z}_n$. Thus, the order of $[1]_n$ in $\mathbb{Z}_n$ is n. Therefore, the order of $([1]_m, [1]_n) \in \mathbb{Z}_m \times \mathbb{Z}_n$ is the least common multiple of m and n. Observe that

$$\begin{aligned} mn &= \gcd(m,n) * lcm(m,n) \\ &= 1 * lcm(m,n) \\ &= lcm(m,n). \end{aligned}$$

Hence, the order of $([1]_m, [1]_n)$ is mn.

The order of $([1]_m, [1]_n) \in \mathbb{Z}_m \times \mathbb{Z}_n$ is the order of the cyclic subgroup of $\mathbb{Z}_m \times \mathbb{Z}_n$ generated by $([1]_m, [1]_n)$. Let G be the cyclic subgroup of $\mathbb{Z}_m \times \mathbb{Z}_n$ generated by $([1]_m, [1]_n)$. Then $G \subset \mathbb{Z}_m \times \mathbb{Z}_n$ and $|G| = mn = |\mathbb{Z}_m||\mathbb{Z}_n| = |\mathbb{Z}_m \times \mathbb{Z}_n|$. If S is a finite set and T is a subset of S such that $|T| = |S|$, then $T = S$. Observe that $\mathbb{Z}_m \times \mathbb{Z}_n$ is a finite set and $G \subset \mathbb{Z}_m \times \mathbb{Z}_n$ and $|G| = |\mathbb{Z}_m \times \mathbb{Z}_n|$. Hence, $G = \mathbb{Z}_m \times \mathbb{Z}_n$. Thus, $([1]_m, [1]_n)$ is a generator of $\mathbb{Z}_m \times \mathbb{Z}_n$, so $\mathbb{Z}_m \times \mathbb{Z}_n$ is cyclic.

Every cyclic group of finite order n is isomorphic to $(\mathbb{Z}_n, +)$. Hence, every cyclic group of finite order mn is isomorphic to $(\mathbb{Z}_{mn}, +)$. Observe that $\mathbb{Z}_m \times \mathbb{Z}_n$ is a cyclic group of order mn. Therefore, $(\mathbb{Z}_m \times \mathbb{Z}_n, +)$ is isomorphic to $(\mathbb{Z}_{mn}, +)$.

Conversely, we prove $(\mathbb{Z}_m \times \mathbb{Z}_n, +) \cong (\mathbb{Z}_{mn}, +)$ implies $\gcd(m,n) = 1$. We prove by contrapositive. Suppose $\gcd(m,n) \neq 1$. Then $\gcd(m,n) > 1$. Let $d = \gcd(m,n)$. Then $d > 1$ and $d|m$ and $d|n$, so $d|mn$. Thus, $\frac{m}{d}$, $\frac{n}{d}$, and $\frac{mn}{d}$ are positive integers. Since $1|\frac{n}{d}$, then $m|\frac{mn}{d}$. Since $1|\frac{m}{d}$, then $n|\frac{mn}{d}$. Let $w = \frac{mn}{d}$. Then $m|w$ and $n|w$.

Let $(a,b) \in \mathbb{Z}_m \times \mathbb{Z}_n$. Then $a \in \mathbb{Z}_m$ and $b \in \mathbb{Z}_n$.

Every element of a finite group has finite order. Since $\mathbb{Z}_m$ and $\mathbb{Z}_n$ and $\mathbb{Z}_m \times \mathbb{Z}_n$ are finite groups, then every element of $\mathbb{Z}_m$ and $\mathbb{Z}_n$ and $\mathbb{Z}_m \times \mathbb{Z}_n$ has finite order. In particular, a and b and (a,b) have finite order. Let k be the order of a and l be the order of b and s be the order of (a,b).

The order of an element of a finite group G divides the order of G. Thus, the order of a divides $|\mathbb{Z}_m|$ and the order of b divides $|\mathbb{Z}_n|$, so $k|m$ and $l|n$. Since $k|m$ and $m|w$, then $k|w$. Since $l|n$ and $n|w$, then $l|w$. Thus, $k|w$ and $l|w$.

Since a has finite order k, then $wa = 0$ iff $k|w$. Since $k|w$, then $wa = 0$.

Since b has finite order l, then $wb = 0$ iff $l|w$. Since $l|w$, then $wb = 0$.

Thus, $w(a,b) = (wa, wb) = (0,0)$.

Since (a,b) has finite order s, then $w(a,b) = (0,0)$ iff $s|w$. Since $w(a,b) = (0,0)$, then $s|w$. Since s and w are positive integers, then this implies $s \leq w$.

Since $d > 1$, then $1 < d$, so $\frac{1}{d} < 1$. Thus, $\frac{mn}{d} < mn$, so $w < mn$. Since $s \leq w$ and $w < mn$, then $s < mn$. Hence, $s \neq mn$, so $|(a,b)| \neq |\mathbb{Z}_m \times \mathbb{Z}_n|$.

If a finite group G is cyclic, then there exists $g \in G$ such that $|g| = |G|$. Thus, if $|g| \neq |G|$ for all $g \in G$, then a finite group G is not cyclic. Hence, if g is an arbitrary element of a finite group G such that $|g| \neq |G|$, then G is not cyclic. Since (a, b) is an arbitrary element of the finite group $\mathbb{Z}_m \times \mathbb{Z}_n$ and $|(a, b)| \neq |\mathbb{Z}_m \times \mathbb{Z}_n|$, then we conclude $\mathbb{Z}_m \times \mathbb{Z}_n$ is not cyclic.

Suppose $\mathbb{Z}_{mn}$ is isomorphic to $\mathbb{Z}_m \times \mathbb{Z}_n$. Then there exists an isomorphism between $\mathbb{Z}_{mn}$ and $\mathbb{Z}_m \times \mathbb{Z}_n$. Let $\phi : \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n$ be an isomorphism. Since ϕ preserves the cyclic property of groups and $\mathbb{Z}_{mn}$ is cyclic, then $\mathbb{Z}_m \times \mathbb{Z}_n$ is cyclic. Thus, we have $\mathbb{Z}_m \times \mathbb{Z}_n$ is cyclic and $\mathbb{Z}_m \times \mathbb{Z}_n$ is not cyclic, a contradiction. Therefore, $\mathbb{Z}_{mn}$ is not isomorphic to $\mathbb{Z}_m \times \mathbb{Z}_n$. □

Corollary 89. *Let $n_1, ..., n_k$ be positive integers.*

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

Proof. □

Corollary 90. *Let $p_1, ..., p_k$ be distinct primes. Let $n = p_1^{e_1} ... p_k^{e_k}$.*

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

Proof. □

Proposition 91. *If H and K are subgroups of an abelian group G, then $HK < G$.*

Solution. Let $HK = \{hk : h \in H, k \in K\}$.

The hypothesis is:

G is an abelian group and $H < G$ and $K < G$.

The conclusion is: $HK < G$.

Suppose G is an abelian group and $H < G$ and $K < G$.

To prove $HK < G$, we use a subgroup test. □

Proof. Suppose G is an abelian group and $H < G$ and $K < G$.

Let $hk \in HK$. Then $h \in H$ and $k \in K$. Since $H < G$, then $H \subset G$, so $h \in G$. Since $K < G$, then $K \subset G$, so $k \in G$. By closure of $G, hk \in G$. Thus, $hk \in HK$ implies $hk \in G$, so $HK \subset G$.

Let $h_1k_1, h_2k_2 \in HK$. Then $h_1, h_2 \in H$ and $k_1, k_2 \in K$. Observe that

$$\begin{aligned}
(h_1k_1)(h_2k_2) &= h_1(k_1h_2)k_2 \\
&= h_1(h_2k_1)k_2 \\
&= (h_1h_2)(k_1k_2).
\end{aligned}$$

By closure of H and K, $h_1h_2 \in H$ and $k_1k_2 \in K$. Hence, $(h_1k_1)(h_2k_2) \in HK$. Therefore, HK is closed under the binary operation of G.

Let e be the identity of G. Since $H < G$ and $K < G$, then $e \in H$ and $e \in K$. Hence, $ee = e \in HK$. Therefore, HK contains the identity of G.

Let $hk \in HK$. Since $H < G$ and $K < G$, then $h^{-1} \in H$ and $k^{-1} \in K$. Observe that

$$\begin{aligned}
(hk)^{-1} &= k^{-1}h^{-1} \\
&= h^{-1}k^{-1}.
\end{aligned}$$

Hence, $(hk)^{-1} \in HK$.

Therefore, $HK < G$. □

Proposition 92. *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 $HK < G$.

Proof. Let G be a group and $H < G$ and $K < G$.
Suppose $h^{-1}kh \in K$ for all $h \in H$ and all $k \in K$.
Let $hk \in HK$. Then $h \in H$ and $k \in K$. Since $H < G$, the $H \subset G$, so $h \in G$. Since $K < G$, then $K \subset G$, so $k \in G$. By closure of $G, hk \in G$. Hence, $hk \in HK$ implies $hk \in G$, so $HK \subset G$.
Let $h_1k_1, h_2k_2 \in HK$. Then $h_1, h_2 \in H$ and $k_1, k_2 \in K$.
Since $h_2 \in H$ and $k_1 \in K$, then $h_2^{-1}k_1h_2 \in K$. Thus, there exists $k' \in K$ such that $k' = h_2^{-1}k_1h_2$. Hence, $h_2k' = k_1h_2$. Observe that

$$\begin{aligned}(h_1k_1)(h_2k_2) &= h_1(k_1h_2)k_2 \\ &= h_1(h_2k')k_2 \\ &= (h_1h_2)(k'k_2).\end{aligned}$$

By closure of H and K, $h_1h_2 \in H$ and $k'k_2 \in K$. Hence, $(h_1k_1)(h_2k_2) \in HK$. Therefore, HK is closed under the binary operation of G.
Let e be the identity of G. Since $H < G$ and $K < G$, then $e \in H$ and $e \in K$. Hence, $ee = e \in HK$. Therefore, HK contains the identity of G.
Let $hk \in HK$. Then $h \in H$ and $k \in K$. Since $H < G$, then $h^{-1} \in H$. Since $h^{-1} \in H$ and $k \in K$, then $(h^{-1})^{-1}k(h^{-1}) \in K$. Hence, there exists $k' \in K$ such that $k' = hkh^{-1}$. Thus, $k'h = hk$. Let $(hk)^{-1}$ be the inverse of hk in G. Then

$$\begin{aligned}(hk)^{-1} &= (k'h)^{-1} \\ &= h^{-1}k'^{-1}.\end{aligned}$$

Since $h^{-1} \in H$ and $k'^{-1} \in K$, then this implies $(hk)^{-1} \in HK$. Hence, HK is closed under inverses.
Therefore, $HK < G$. □

Proposition 93. *Let H and K be subgroups of a group G.*
Then $HK < G$ iff $KH \subset HK$.

Proof. We prove if $HK < G$, then $KH \subset HK$.
Suppose $HK < G$.
Let $kh \in KH$. Then $k \in K$ and $h \in H$. Since $H < G$ and $K < G$, then $e \in H$ and $e \in K$. Since $e \in H$ and $k \in K$, then $ek = k \in HK$. Since $h \in H$ and $e \in K$, then $he = h \in HK$. Since $HK < G$, then HK is closed, so $k \in HK$ and $h \in HK$ imply $kh \in HK$. Thus, $kh \in KH$ implies $kh \in HK$, so $KH \subset HK$.
Conversely, we prove if $KH \subset HK$, then $HK < G$.
Suppose $KH \subset HK$.
Let e be the identity of G. Since $H < G$ and $K < G$, then $e \in H$ and $e \in K$. Hence, $ee = e \in HK$. Therefore, HK contains the identity of G.
Let $hk \in HK$. Then $h \in H$ and $k \in K$. Since $H < G$, the $H \subset G$, so $h \in G$. Since $K < G$, then $K \subset G$, so $k \in G$. By closure of $G, hk \in G$. Hence, $hk \in HK$ implies $hk \in G$, so $HK \subset G$.

Let $h_1k_1, h_2k_2 \in HK$. Then $h_1, h_2 \in H$ and $k_1, k_2 \in K$.

Since $h_2 \in H$ and $k_1 \in K$, then $k_1h_2 \in KH$. Since $KH \subset HK$, then $k_1h_2 \in HK$. Thus, there exists $h' \in H$ and $k' \in K$ such that $h'k' = k_1h_2$. Observe that

$$\begin{aligned}(h_1k_1)(h_2k_2) &= h_1(k_1h_2)k_2 \\ &= h_1(h'k')k_2 \\ &= (h_1h')(k'k_2).\end{aligned}$$

By closure of H and K, $h_1h' \in H$ and $k'k_2 \in K$. Hence, $(h_1k_1)(h_2k_2) \in HK$. Therefore, HK is closed under the binary operation of G.

Let $hk \in HK$. Then $h \in H$ and $k \in K$. Since $H < G$ and $K < G$, then $h^{-1} \in H$ and $k^{-1} \in K$. Thus, $k^{-1}h^{-1} \in KH$. Since $KH \subset HK$, then $k^{-1}h^{-1} \in HK$. Since $(hk)^{-1} = k^{-1}h^{-1}$, then this implies $(hk)^{-1} \in HK$. Hence, HK is closed under inverses. Therefore, $HK < G$. $\square$

Normal Subgroups

Theorem 94. *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 $g \in G$.*

Proof. We prove 1 implies 2.

Suppose $H \triangleleft G$. Then $ghg^{-1} \in H$ for all $g \in G$ and all $h \in H$.

Let $g \in G$. Let $x \in gHg^{-1}$. Then $x = ghg^{-1}$ for some $h \in H$. Since $H \triangleleft G$, then $x \in H$. Hence, $x \in gHg^{-1}$ implies $x \in H$, so $gHg^{-1} \subset H$.

We prove 2 implies 3.

Suppose $gHg^{-1} \subset H$ for all $g \in G$. We prove $H \subset gHg^{-1}$ for all $g \in G$.

Let $g \in G$. Let $h \in H$. Let $h' = g^{-1}hg$. Since $g^{-1} \in G$, then $g^{-1}H(g^{-1})^{-1} \subset H$. Hence, $g^{-1}Hg \subset H$. Since $h' = g^{-1}hg$ for some $h \in H$, then $h' \in g^{-1}Hg$. Thus, $h' \in H$. Observe that

$$\begin{aligned}gh'g^{-1} &= g(g^{-1}hg)g^{-1} \\ &= (gg^{-1})h(gg^{-1}) \\ &= h.\end{aligned}$$

Hence, there exists $h' \in H$ such that $h = gh'g^{-1}$, so $h \in gHg^{-1}$. Thus, $h \in H$ implies $h \in gHg^{-1}$, so $H \subset gHg^{-1}$.

Since $gHg^{-1} \subset H$ and $H \subset gHg^{-1}$, then $gHg^{-1} = H$.

We prove 3 implies 1.

Suppose $gHg^{-1} = H$ for all $g \in G$. Let $g \in G$ and $h \in H$. Then $gHg^{-1} = H$. Thus, $gHg^{-1} \subset H$. Hence, $ghg^{-1} \in H$. $\square$

Theorem 95. *Let $H < G$. Then $H \triangleleft G$ iff $gH = Hg$ for all $g \in G$.*

Proof. Suppose $H \lhd G$. Then $ghg^{-1} \in H$ for all $g \in G$ and all $h \in H$.

Let $g \in G$.

Suppose $gh \in gH$. Then $h \in H$. Let $h' = ghg^{-1}$. Then $h'g = gh$. Since $g \in G$ and $h \in H$ and $H \lhd G$, then $h' \in H$. Observe that

$$\begin{aligned} gh \in gH &\Rightarrow h'g \in gH \\ &\Rightarrow h'g \in Hg \\ &\Rightarrow gh \in Hg. \end{aligned}$$

Hence, $gh \in gH$ implies $gh \in Hg$, so $gH \subset Hg$.

Suppose $hg \in Hg$. Then $h \in H$. Let $h'' = g^{-1}hg = g^{-1}h(g^{-1})^{-1}$. Then $gh'' = hg$. Since $g^{-1} \in G$ and $h \in H$ and $H \lhd G$, then $h'' \in H$. Observe that

$$\begin{aligned} hg \in Hg &\Rightarrow gh'' \in Hg \\ &\Rightarrow gh'' \in gH \\ &\Rightarrow hg \in gH. \end{aligned}$$

Hence, $hg \in Hg$ implies $hg \in gH$, so $Hg \subset gH$.

Since $gH \subset Hg$ and $Hg \subset gH$, then $gH = Hg$.

Conversely, suppose $gH = Hg$ for all $g \in G$. Let $g \in G$ and $h \in H$. Then $gH = Hg$, so $gh = h'g$ for some $h' \in H$. Thus, $ghg^{-1} = h'$, so $ghg^{-1} \in H$. Therefore, $H \lhd G$. ☐

Theorem 96. *Every subgroup of an abelian group is normal.*

Solution. To prove H is normal in G, we prove $ghg^{-1} \in H$ for all $g \in G$ and all $h \in H$. ☐

Proof. Let H be an arbitrary subgroup of an abelian group G.

Let $g \in G$ and $h \in H$. Since $h \in H$ and $H \subset G$, then $h \in G$. Thus,

$$\begin{aligned} ghg^{-1} &= (gh)g^{-1} \\ &= (hg)g^{-1} \\ &= h(gg^{-1}) \\ &= he \\ &= h. \end{aligned}$$

Hence, $ghg^{-1} \in H$, so $H \lhd G$. ☐

Proof. Let $g, h \in G$.

Observe that

$$\begin{aligned} gh \in gH &\Rightarrow hg \in gH \\ &\Rightarrow hg \in Hg \\ &\Rightarrow gh \in Hg. \end{aligned}$$

Therefore, $gH \subset Hg$.

Observe that

$$\begin{aligned} hg \in Hg &\Rightarrow gh \in Hg \\ &\Rightarrow gh \in gH \\ &\Rightarrow hg \in gH. \end{aligned}$$

Therefore, $Hg \subset gH$.

Thus, $gH \subset Hg$ and $Hg \subset gH$, so $gH = Hg$.

Hence, $H \lhd G$. ☐

Theorem 97. *The intersection of two normal subgroups is a normal subgroup.*

Solution. This statement means:

if H and K are normal subgroups of a group G, then $H \cap K \lhd G$.

Hence, we assume H and K are normal subgroups of a group G.

To prove $H \cap K \lhd G$, we must prove $ghg^{-1} \in H \cap K$ for all $g \in G$ and all $h \in H \cap K$. ☐

Proof. Let H and K be normal subgroups of a group G. Let $g \in G$ and $h \in H \cap K$. Since G is a group and $g \in G$, then $g^{-1} \in G$. Since $h \in H \cap K$, then $h \in H$ and $h \in K$.

Since $H \lhd G$, then $ghg^{-1} \in H$. Since $K \lhd G$, then $ghg^{-1} \in K$. Hence, $ghg^{-1} \in H$ and $ghg^{-1} \in K$, so $ghg^{-1} \in H \cap K$. Therefore, $H \cap K \lhd G$. ☐

Proposition 98. *If G is a group and $H < G$, then $gHg^{-1} < G$ and $gHg^{-1} \cong H$ for all $g \in G$.*

Proof. Suppose G is a group and $H < G$.

Let $g \in G$.

We first prove $gHg^{-1} < G$.

Let $x \in gHg^{-1}$.

Then there exists $h \in H$ such that $x = ghg^{-1}$.

Since $h \in H$ and $H \subset G$, then $h \in G$.

By closure of $G, x \in G$.

Hence, $x \in gHg^{-1}$ implies $x \in G$, so $gHg^{-1} \subset G$.

Let $x, y \in gHg^{-1}$.

Then $x = gh_1g^{-1}$ for some $h_1 \in H$ and $y = gh_2g^{-1}$ for some $h_2 \in H$.

Thus,

$$\begin{aligned} xy &= (gh_1g^{-1})(gh_2g^{-1}) \\ &= (gh_1)(g^{-1}g)(h_2g^{-1}) \\ &= (gh_1)(h_2g^{-1}) \\ &= g(h_1h_2)g^{-1}. \end{aligned}$$

By closure of $H, h_1h_2 \in H$.

Hence, there exists $h_1h_2 \in H$ such that $xy = g(h_1h_2)g^{-1}$, so $xy \in gHg^{-1}$.

Let e be the identity of G.
Since $H < G$, then $e \in H$.
Observe that $e = gg^{-1} = geg^{-1}$.
Hence, $e \in gHg^{-1}$.

Let $x \in gHg^{-1}$.
Then there exists $h \in H$ such that $x = ghg^{-1}$.
Since $H < G$, then $h^{-1} \in H$.
Thus, $x^{-1} = (ghg^{-1})^{-1} = gh^{-1}g^{-1}$.
Hence, there exists $h^{-1} \in H$ such that $x^{-1} = gh^{-1}g^{-1}$, so $x^{-1} \in gHg^{-1}$.
Therefore, by the subgroup test, $gHg^{-1} < G$. $\square$

Proof. Let $g \in G$.
We prove $gHg^{-1} \cong H$.
Define $\phi : H \to gHg^{-1}$ by $\phi(h) = ghg^{-1}$ for all $h \in H$.

Let $h_1, h_2 \in H$ such that $h_1 = h_2$. Then $gh_1 = gh_2$, so $gh_1g^{-1} = gh_2g^{-1}$. Hence, $\phi(h_1) = \phi(h_2)$. Thus, $h_1 = h_2$ implies $\phi(h_1) = \phi(h_2)$, so ϕ is well defined. Therefore, ϕ is a function.

Let $h_1, h_2 \in H$ such that $\phi(h_1) = \phi(h_2)$. Then $gh_1g^{-1} = gh_2g^{-1}$. By the right cancellation law, we have $gh_1 = gh_2$. By the left cancellation law, we have $h_1 = h_2$. Hence, $\phi(h_1) = \phi(h_2)$ implies $h_1 = h_2$, so ϕ is injective.

Let $ghg^{-1} \in gHg^{-1}$. Then $h \in H$. Hence, there exists $h \in H$ such that $ghg^{-1} \in gHg^{-1}$. Therefore, ϕ is surjective.

Thus, ϕ is a bijective function.
Let $h_1, h_2 \in H$. Then

$$\begin{aligned}
\phi(h_1h_2) &= g(h_1h_2)g^{-1} \\
&= (gh_1)(h_2g^{-1}) \\
&= (gh_1)(g^{-1}g)(h_2g^{-1}) \\
&= (gh_1g^{-1})(gh_2g^{-1}) \\
&= \phi(h_1)\phi(h_2).
\end{aligned}$$

Thus, ϕ is a group homomorphism, so $\phi : H \to gHg^{-1}$ is an isomorphism.
Therefore, $H \cong gHg^{-1}$. $\square$

Proof. Let $g \in G$.
Define $\phi : H \to G$ by $\phi(h) = ghg^{-1}$ for all $h \in H$.

Let $h_1, h_2 \in H$ such that $h_1 = h_2$. Then $gh_1 = gh_2$, so $gh_1g^{-1} = gh_2g^{-1}$. Hence, $\phi(h_1) = \phi(h_2)$. Thus, $h_1 = h_2$ implies $\phi(h_1) = \phi(h_2)$, so ϕ is well defined. Therefore, ϕ is a function.

Let $h_1, h_2 \in H$. Then

$$\begin{aligned}
\phi(h_1h_2) &= g(h_1h_2)g^{-1} \\
&= (gh_1)(h_2g^{-1}) \\
&= (gh_1)e(h_2g^{-1}) \\
&= (gh_1)(g^{-1}g)(h_2g^{-1}) \\
&= (gh_1g^{-1})(gh_2g^{-1}) \\
&= \phi(h_1)\phi(h_2).
\end{aligned}$$

Therefore, ϕ is a group homomorphism.

Since $\phi : H \to G$ is a group homomorphism, then $\phi(H) < G$.

We prove $\phi(H) = gHg^{-1}$.

Let $x \in \phi(H)$. Then there exists $h \in H$ such that $x = \phi(h)$. Thus, there exists $h \in H$ such that $x = ghg^{-1}$. Hence, $x \in gHg^{-1}$. Therefore, $x \in \phi(H)$ implies $x \in gHg^{-1}$, so $\phi(H) \subset gHg^{-1}$.

Let $y \in gHg^{-1}$. Then there exists $h \in H$ such that $y = ghg^{-1}$. Hence, there exists $h \in H$ such that $y = \phi(h)$. Thus, $y \in \phi(H)$. Therefore, $y \in gHg^{-1}$ implies $y \in \phi(H)$, so $gHg^{-1} \subset \phi(H)$.

Since $\phi(H) \subset gHg^{-1}$ and $gHg^{-1} \subset \phi(H)$, then $\phi(H) = gHg^{-1}$. Therefore, $gHg^{-1} < G$.

Let $h_1, h_2 \in H$ such that $\phi(h_1) = \phi(h_2)$. Then $gh_1g^{-1} = gh_2g^{-1}$. By the right cancellation law, we have $gh_1 = gh_2$. By the left cancellation law, we have $h_1 = h_2$. Hence, $\phi(h_1) = \phi(h_2)$ implies $h_1 = h_2$, so ϕ is injective.

Since ϕ is injective, then $H \cong \phi(H)$. Thus, $H \cong gHg^{-1}$, so $gHg^{-1} \cong H$. □

Proposition 99. *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.*

Proof. Observe that $N(H)$ is a subset of G.

Let e be the identity of G.

Let $h \in H$.

Then $eh = h = he$, so $e \in N(H)$.

Hence, $N(H)$ is not empty.

Let $a, b \in N(H)$.

Then $a \in G$ and for every $h \in H, ah = ha$ and $b \in G$ and for every $h \in H, bh = hb$.

Thus, $ah = ha$ and $bh = hb$.

Hence, $b = hbh^{-1}$.

Since G is a group, then $b^{-1} \in G$.

By closure of G, $ab^{-1} \in G$.

Observe that

$$\begin{aligned}
(ab^{-1})h &= (a(hbh^{-1})^{-1})h \\
&= (a(hb^{-1}h^{-1}))h \\
&= (ah)b^{-1}(h^{-1}h) \\
&= (ah)b^{-1}e \\
&= (ah)b^{-1} \\
&= (ha)b^{-1} \\
&= h(ab^{-1}).
\end{aligned}$$

Hence, $(ab^{-1})h = h(ab^{-1})$.

Therefore, $ab^{-1} \in N(H)$.

Thus, $N(H)$ is a subgroup of G. □

Proposition 100. *If G is a group and $H < G$, then $N(H) < G$ and $H \subset N(H)$.*

Proof. Suppose G is a group and $H < G$.

Let $x \in N(H)$.

Then $x \in G$.

Hence, $N(H) \subset G$.

Let e be the identity of G. To prove $e \in N(H)$, we must prove $eHe^{-1} = H$.

Let $h \in eHe^{-1}$. Then there exists $h' \in H$ such that $h = eh'e^{-1}$. Thus,

$$\begin{aligned}
h &= eh'e^{-1} \\
&= h'e^{-1} \\
&= h'e \\
&= h'.
\end{aligned}$$

Hence, $h \in H$. Therefore, $h \in eHe^{-1}$ implies $h \in H$, so $eHe^{-1} \subset H$.

Let $h \in H$. Then

$$\begin{aligned}
ehe^{-1} &= he^{-1} \\
&= he \\
&= h.
\end{aligned}$$

Hence, there exists $h \in H$ such that $h = ehe^{-1}$, so $h \in eHe^{-1}$. Therefore, $h \in H$ implies $h \in eHe^{-1}$, so $H \subset eHe^{-1}$.

Since $eHe^{-1} \subset H$ and $H \subset eHe^{-1}$, then $eHe^{-1} = H$. Since $e \in G$ and $eHe^{-1} = H$, then $e \in N(H)$.

Let $a, b \in N(H)$. Then $a, b \in G$ and $aHa^{-1} = H$ and $bHb^{-1} = H$. By closure of $G, ab \in G$.

We prove $(ab)H(ab)^{-1} = H$.

Let $x \in (ab)H(ab)^{-1}$. Then there exists $h \in H$ such that $x = (ab)h(ab)^{-1}$. Hence, $x = abhb^{-1}a^{-1}$. Let $h' = bhb^{-1}$. Since $h \in H$, then $h' \in bHb^{-1}$. Since $bHb^{-1} = H$, then $h' \in H$. Thus, $x = ah'a^{-1}$. Since $h' \in H$, then $x \in aHa^{-1}$. Since $aHa^{-1} = H$, then $x \in H$. Hence, $x \in (ab)H(ab)^{-1}$ implies $x \in H$, so $(ab)H(ab)^{-1} \subset H$.

Let $y \in H$. Since $H = aHa^{-1} = bHb^{-1}$, then $y \in aHa^{-1}$ and $y \in bHb^{-1}$. Hence, $y = aha^{-1}$ for some $h \in H$ and $y = bh'b^{-1}$ for some $h' \in H$.

Let $h'' = b^{-1}hb$.

We must prove $h'' \in H$!!!

Observe that

$$\begin{aligned}
(ab)h''(ab)^{-1} &= (ab)(b^{-1}hb)(ab)^{-1} \\
&= (ab)(b^{-1}hb)(b^{-1}a^{-1}) \\
&= a(bb^{-1})h(bb^{-1})a^{-1} \\
&= aha^{-1} \\
&= y.
\end{aligned}$$

Hence, $y \in (ab)H(ab)^{-1}$. Thus, $y \in H$ implies $y \in (ab)H(ab)^{-1}$, so $H \subset (ab)H(ab)^{-1}$.

Since $(ab)H(ab)^{-1} \subset H$ and $H \subset (ab)H(ab)^{-1}$, then $(ab)H(ab)^{-1} = H$.

Since $ab \in G$ and $(ab)H(ab)^{-1} = H$, then $ab \in N(H)$. Therefore, $N(H)$ is closed under the binary operation of G.

We prove $N(H)$ is closed under taking inverses. Let $a \in N(H)$. Then $a \in G$ and $aHa^{-1} = H$. By closure of $G, a^{-1} \in G$.

To prove $a^{-1} \in N(H)$, we must prove $a^{-1}Ha = H$. Thus, we must prove $aHa^{-1} = H$ implies $a^{-1}Ha = H$.

Suppose $aHa^{-1} = H$. To prove $a^{-1}Ha = H$, we must prove $a^{-1}Ha = aHa^{-1}$. Thus, we must prove $a^{-1}Ha \subset aHa^{-1}$ and $aHa^{-1} \subset a^{-1}Ha$. □

Theorem 101. *Let G be a group.*

Let $g \in G$.

Then $C(g) < G$.

If g generates a normal subgroup of G, then $C(g) \lhd G$.

Proof. Observe that $C(g)$ is a subset of G. Let e be the identity element of G. Since $e \in G$ and $eg = ge$, then $e \in C(g)$.

Let $a, b \in C(g)$. Then $a \in G$ and $ag = ga$ and $b \in G$ and $bg = gb$. By closure of $G, ab \in G$. Observe that

$$\begin{aligned}
(ab)g &= a(bg) \\
&= a(gb) \\
&= (ag)b \\
&= (ga)b \\
&= g(ab).
\end{aligned}$$

Since $ab \in G$ and $(ab)g = g(ab)$, then $ab \in C(g)$. Hence, $C(g)$ is closed under the binary operation of G.

Let $a \in C(g)$. Then $a \in G$ and $ag = ga$. Thus, $a = gag^{-1}$, so $a^{-1} = (gag^{-1})^{-1} = ga^{-1}g^{-1}$. Hence, $a^{-1}g = ga^{-1}$. Since $a^{-1} \in G$ and $a^{-1}g = ga^{-1}$, then $a^{-1} \in C(g)$. Hence, $C(g)$ is closed under taking inverses.

Therefore, by the subgroup test, $C(g) < G$.

Let $\langle g \rangle$ be the cyclic subgroup of G generated by g. Then $\langle g \rangle = \{g^k : k \in \mathbb{Z}\}$. Suppose $\langle g \rangle \lhd G$. Then $ag^k a^{-1} \in \langle g \rangle$ for all $a \in G$ and all $g^k \in \langle g \rangle$.

Let $H = C(g)$.

To prove $H \lhd G$, we prove $aha^{-1} \in H$ for all $a \in G$ and all $h \in H$.

Let $a \in G$.

Let $h \in H$.

Then $h \in G$ and $gh = gh$. $\square$

Theorem 102. ***The center of a group*** G ***is a normal subgroup of*** G**.**

Let G *be a group.*

Then $Z(G) \lhd G$.

Proof. We first prove $Z(G) < G$.

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

Let e be the identity of G.

By definition of group, $eg = ge$ for all $g \in G$.

Since $e \in G$ and $eg = ge$ for all $g \in G$, then $e \in Z(G)$, so $Z(G) \neq \emptyset$.

Since $Z(G) \subset G$ and $Z(G) \neq \emptyset$, then $Z(G)$ is a nonempty subset of G.

We prove $Z(G)$ is closed under the binary operation of G.

Let $a, b \in Z(G)$.

Then $a \in G$ and $ag = ga$ for all $g \in G$ and $b \in G$ and $bg = gb$ for all $g \in G$.

By closure of $G, a \in G$ and $b \in G$ implies $ab \in G$.

Let $g \in G$.

Observe that

$$\begin{aligned} (ab)g &= a(bg) \\ &= a(gb) \\ &= (ag)b \\ &= (ga)b \\ &= g(ab). \end{aligned}$$

Since $ab \in G$ and $(ab)g = g(ab)$, then $ab \in Z(G)$.

Therefore, $Z(G)$ is closed under the binary operation of G.

We prove $Z(G)$ is closed under inverses.

Let $a \in Z(G)$.

Then $a \in G$ and $ag = ga$ for all $g \in G$.

Since $a \in G$ and G is a group, then $a^{-1} \in G$.

Let $g \in G$.
Then $ag = ga$, so $a = gag^{-1}$.
Hence, $a^{-1} = (gag^{-1})^{-1} = ga^{-1}g^{-1}$, so $a^{-1}g = ga^{-1}$.
Thus, $a^{-1}g = ga^{-1}$ for all $g \in G$.
Since $a^{-1} \in G$ and $a^{-1}g = ga^{-1}$ for all $g \in G$, then $a^{-1} \in Z(G)$.
Therefore, $a^{-1} \in Z(G)$ for all $a \in Z(G)$.

Since $Z(G)$ is a nonempty subset of G and $Z(G)$ is closed under the binary operation of G and $a^{-1} \in Z(G)$ for all $a \in Z(G)$, then by the two-step subgroup test, $Z(G)$ is a subgroup of G, so $Z(G) < G$. ☐

Proof. We prove $Z(G) \triangleleft G$.

Let $g \in G$ and $h \in Z(G)$. Then $h \in G$ and $hx = xh$ for all $x \in G$. By closure of $G, ghg^{-1} \in G$. Let $x \in G$. Observe that

$$\begin{aligned}
(ghg^{-1})x &= (gh)(g^{-1}x) \\
&= (hg)(g^{-1}x) \\
&= h(gg^{-1})x \\
&= hx \\
&= xh \\
&= x(gg^{-1})h \\
&= (xg)(g^{-1}h) \\
&= (xg)(hg^{-1}) \\
&= x(ghg^{-1}).
\end{aligned}$$

Since $ghg^{-1} \in G$ and $(ghg^{-1})x = x(ghg^{-1})$ for all $x \in G$, then $ghg^{-1} \in Z(G)$. Therefore, $Z(G) \triangleleft G$. ☐

Theorem 103. *Let $H \triangleleft G$.*

Let $\frac{G}{H}$ be the set of all cosets of H in G.

Define $(aH)(bH) = (ab)H$ for all $aH, bH \in \frac{G}{H}$.

Then $(\frac{G}{H}, *)$ is a group and $|\frac{G}{H}| = [G : H]$.

Proof. Since $e \in G$, then $eH = H$ is a coset of H in G. Therefore, $H \in \frac{G}{H}$, so $\frac{G}{H}$ is not empty.

Let $aH, bH \in \frac{G}{H}$. Then $a, b \in G$ and $(aH)(bH) = (ab)H$. Since G is a group, then $ab \in G$, so $(ab)H \in \frac{G}{H}$. Therefore, $\frac{G}{H}$ is closed under multiplication of cosets.

We prove that multiplication of cosets is well defined.

Suppose $cH, dH \in \frac{G}{H}$ such that $aH = cH$ and $bH = dH$. Then $a, b, c, d \in G$. To prove coset multiplication is well defined, we must prove $(aH)(bH)$ is unique. Hence, we must prove $(aH)(bH) = (cH)(dH)$.

Since $aH = cH$ iff $a \in cH$, then $a \in cH$. Thus, there exists $h_1 \in H$ such that $a = ch_1$. Since $bH = dH$ iff $b \in dH$, then $b \in dH$. Thus, there exists $h_2 \in H$

such that $b = dh_2$. Since H is normal in G, then for every $g \in G$ and $h \in H$, $ghg^{-1} \in H$. Since $d^{-1} \in G$ and $h_1 \in H$, then $d^{-1}h_1(d^{-1})^{-1} = d^{-1}h_1d \in H$. Let $h_3 = d^{-1}h_1d$. Then $h_3 \in H$.

Let $h = h_3h_2$. Since H is a group, then H is closed under its binary operation. Hence, $h \in H$ since $h_2, h_3 \in H$.

Observe that

$$\begin{aligned}(cd)h &= (cd)(h_3h_2)\\ &= (cd)(d^{-1}h_1d)h_2\\ &= c(dd^{-1})h_1dh_2\\ &= (ch_1)(dh_2)\\ &= ab.\end{aligned}$$

Since $ab = (cd)h$ for some $h \in H$, then $ab \in (cd)H$. Since $ab \in (ab)H$ and $ab \in (cd)H$, then $(ab)H = (cd)H$. Therefore,

$$\begin{aligned}(aH)(bH) &= (ab)H\\ &= (cd)H\\ &= (cH)(dH).\end{aligned}$$

Therefore, multiplication of cosets is well defined, so multiplication of cosets is a binary operation on $\frac{G}{H}$.

Let $aH, bH, cH \in \frac{G}{H}$. Observe that

$$\begin{aligned}[(aH)(bH)](cH) &= (abH)(cH)\\ &= ((ab)c)H\\ &= (a(bc))H\\ &= (aH)(bcH)\\ &= (aH)[(bH)(cH)].\end{aligned}$$

Therefore, multiplication of cosets is associative.

Let $aH \in \frac{G}{H}$. Then $(aH)(H) = (aH)(eH) = (ae)H = aH = (ea)H = (eH)(aH) = (H)(aH)$. Since $H \in \frac{G}{H}$ and $(aH)(H) = (H)(aH) = aH$, then H is an identity element of $\frac{G}{H}$.

Since $a^{-1} \in G$, then $a^{-1}H \in \frac{G}{H}$. Observe that $(aH)(a^{-1}H) = (aa^{-1})H = eH = (a^{-1}a)H = (a^{-1}H)(aH)$. Hence, an inverse of aH is $a^{-1}H$, so each element of $\frac{G}{H}$ has an inverse.

Therefore, $(\frac{G}{H}, *)$ is a group.

The order of the group $\frac{G}{H}$ is the number of cosets of H in G. Since H is normal in G, then $gH = Hg$ for every $g \in G$. Thus, each left coset equals each right coset. Hence, the number of cosets equals the number of left cosets. Therefore, $|\frac{G}{H}| = [G : H]$. $\square$

Theorem 104. *If N is a subgroup of an abelian group G, then $\frac{G}{N}$ is abelian.*

Proof. Suppose G is an abelian group and $N < G$.

Every subgroup of an abelian group is normal, so $N \lhd G$.

Let $aN, bN \in \frac{G}{N}$.

Then $a, b \in G$.

Observe that

$$\begin{aligned} (aN)(bN) &= (ab)N \\ &= (ba)N \\ &= (bN)(aN). \end{aligned}$$

Therefore, $\frac{G}{N}$ is abelian. □

Theorem 105. *If N is a subgroup of a cyclic group G, then $\frac{G}{N}$ is cyclic.*

Proof. Suppose N is a subgroup of a cyclic group G. Every cyclic group is abelian, so G is abelian. Every subgroup of an abelian group is normal, so N is normal. Therefore, $\frac{G}{N}$ is a group and $\frac{G}{N} = \{aN : a \in G\}$.

Since G is cyclic, then there exists $g \in G$ such that $G = \{g^n : n \in \mathbb{Z}\}$. Since $g \in G$, then $gN \in \frac{G}{N}$. Every element of a group generates a cyclic subgroup. Let T be the cyclic subgroup of $\frac{G}{N}$ generated by gN. Then $T = \{(gN)^n : n \in \mathbb{Z}\}$.

Let $aN \in \frac{G}{N}$. Then $a \in G$. Since G is cyclic, then there exists an integer n such that $a = g^n$. Therefore, $aN = g^n N = (g * g * ... * g)N = (gN)(gN)...(gN) = (gN)^n$. Thus, there exists an integer n such that $aN = (gN)^n$, so $aN \in T$. Hence, $aN \in \frac{G}{N}$ implies $aN \in T$, so $\frac{G}{N} \subset T$.

Let $y \in T$. Then there exists an integer m such that $y = (gN)^m$. Thus, $y = (gN)(gN)...(gN) = (gg...g)N = (g^m)N$. Since $g^m \in G$, then $y = (g^m)N \in \frac{G}{N}$. Thus, $y \in T$ implies $y \in \frac{G}{N}$, so $T \subset \frac{G}{N}$.

Since $\frac{G}{N} \subset T$ and $T \subset \frac{G}{N}$, then $\frac{G}{N} = T$. Thus, $\frac{G}{N} = \{(gN)^n : n \in \mathbb{Z}\}$. Since there exists $gN \in \frac{G}{N}$ such that $\frac{G}{N} = \{(gN)^n : n \in \mathbb{Z}\}$, then $\frac{G}{N}$ is cyclic. □

Theorem 106. *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.

Proof. Let $H = Z(G) = \{x \in G : (\forall g \in G)(xg = gx)\}$.

Since $Z(G) \lhd G$, then $H \lhd G$, so $\frac{G}{H}$ exists.

Suppose $\frac{G}{H}$ is cyclic.

Then there exists $gH \in \frac{G}{H}$ such that $\frac{G}{H} = \{(gH)^k : k \in \mathbb{Z}\}$.

Hence, there exists $g \in G$ such that $\frac{G}{H} = \{g^k H : k \in \mathbb{Z}\}$.

Let $aH, bH \in \frac{G}{H}$.

Then $a, b \in G$ and there exist integers m and n such that $aH = g^m H$ and $bH = g^n H$.

Since $aH = g^m H$, then $a = g^m h_1$ for some $h_1 \in H$.

Since $bH = g^n H$, then $b = g^n h_2$ for some $h_2 \in H$.

Observe that

$$\begin{aligned}
ab &= (g^m h_1)(g^n h_2) \\
&= g^m (h_1 g^n) h_2 \\
&= g^m (g^n h_1) h_2 \\
&= (g^m g^n)(h_1 h_2) \\
&= (g^{m+n})(h_1 h_2) \\
&= (g^{n+m})(h_1 h_2) \\
&= (g^n g^m)(h_1 h_2) \\
&= (g^n g^m)(h_2 h_1) \\
&= g^n (g^m h_2) h_1 \\
&= g^n (h_2 g^m) h_1 \\
&= (g^n h_2)(g^m h_1) \\
&= ba.
\end{aligned}$$

Therefore, G is abelian. □

Homomorphisms

Theorem 107. *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 $\phi^{-1}(K') \lhd G$.

Proof. To prove 1: we must prove $\phi(e) = e'$.
Observe that

$$\begin{aligned}
e'\phi(e) &= \phi(e) \\
&= \phi(ee) \\
&= \phi(e)\phi(e).
\end{aligned}$$

Applying the right cancellation law, we obtain $e' = \phi(e)$, as desired. □

Proof. We prove 2.

Let $a \in G$.
We must prove $\phi(a^{-1}) = (\phi(a))^{-1}$.
Observe that

$$\begin{aligned} e' &= \phi(e) \\ &= \phi(aa^{-1}) \\ &= \phi(a)\phi(a^{-1}). \end{aligned}$$

Hence, $\phi(a)$ and $\phi(a^{-1})$ are inverses of each other in G'.
Therefore, $(\phi(a))^{-1} = \phi(a^{-1})$, as desired. $\square$

Proof. To prove 3: define predicate $p(k) : \phi(a^k) = (\phi(a))^k$ over $\mathbb{Z}$.
We must prove $(\forall k \in \mathbb{Z})(p(k))$.
Observe that $(\forall k \in \mathbb{Z})(p(k)) \Leftrightarrow (\forall k \in \mathbb{Z}^+)(p(k)) \wedge p(0) \wedge (\forall k \in \mathbb{Z}^+)(p(-k))$.
Thus, we must prove:
3a. $(\forall k \in \mathbb{Z}^+)(p(k))$.
3b. $p(0)$.
3c. $(\forall k \in \mathbb{Z}^+)(p(-k))$.

Observe that

$$\begin{aligned} \phi(a^0) &= \phi(e) \\ &= e' \\ &= (\phi(a))^0. \end{aligned}$$

Therefore, $p(0)$ is true.

We prove $(\forall k \in \mathbb{Z}^+)(p(k))$ by induction on k.
If $k = 1$, then $\phi(a^1) = \phi(a) = (\phi(a))^1$, so $p(1)$ is true.
Suppose $k \in \mathbb{Z}^+$ such that $p(k)$ is true.
Then $\phi(a^k) = (\phi(a))^k$.
Observe that

$$\begin{aligned} \phi(a^{k+1}) &= \phi(a^k a) \\ &= \phi(a^k)\phi(a) \\ &= (\phi(a))^k\phi(a) \\ &= (\phi(a))^{k+1}. \end{aligned}$$

Hence, $\phi(k+1)$ is true, so $p(k)$ implies $p(k+1)$.
Therefore, by induction, $p(k)$ is true for all $k \in \mathbb{Z}^+$.

We prove $(\forall k \in \mathbb{Z}^+)(p(-k))$ by induction on k.

Let $k = 1$.

Since a group homomorphism preserves inverses, then $\phi(a^{-1}) = (\phi(a))^{-1}$, so $p(-1)$ is true.

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

Then $\phi(a^{-k}) = (\phi(a))^{-k}$.

Observe that

$$\begin{aligned}
\phi(a^{-(k+1)}) &= \phi(a^{-k-1}) \\
&= \phi(a^{-k}a^{-1}) \\
&= \phi(a^{-k})\phi(a^{-1}) \\
&= (\phi(a))^{-k}\phi(a^{-1}) \\
&= (\phi(a))^{-k}(\phi(a))^{-1} \\
&= (\phi(a))^{-k-1} \\
&= (\phi(a))^{-(k+1)}.
\end{aligned}$$

Thus, $p(-(k+1))$ is true, so $p(-k)$ implies $p(-(k+1))$.

Hence, by induction, $p(-k)$ is true for all $k \in \mathbb{Z}^+$.

Therefore, $p(-k)$ is true for all $k \in \mathbb{Z}$. ∎

Proof. We prove 4.

Suppose $H < G$.

We must prove $\phi(H) < G'$.

Let $\phi(H)$ be the image of H under ϕ.

Then $\phi(H) = \{\phi(h) \in G' : h \in H\}$.

Thus, $\phi(H) \subset G'$, so $\phi(H)$ is a subset of G'.

Every subgroup of G contains the identity of G.

Since $H < G$ and $e \in G$, then $e \in H$.

Since $e \in H$ and $\phi(e) = e'$ and $e' \in G'$, then $e' \in \phi(H)$.

Therefore, $\phi(H)$ is closed under the identity of G'.

Let $\phi(a), \phi(b) \in \phi(H)$.

Since $\phi(a) \in \phi(H)$, then $\phi(a) \in G'$ and $a \in H$.

Since $\phi(b) \in \phi(H)$, then $\phi(b) \in G'$ and $b \in H$.

Since H is a group and $a \in H$ and $b \in H$, then by closure of H, we have $ab \in H$.

Since $\phi(a) \in G'$, then $a \in G$.

Since $\phi(b) \in G'$, then $b \in G$.

Since G is a group and $a \in G$ and $b \in G$, then by closure of G, we have $ab \in G$, so $\phi(ab) \in G'$.

Since $\phi(a)\phi(b) = \phi(ab)$ and $\phi(ab) \in G'$ and $ab \in H$, then $\phi(a)\phi(b) \in \phi(H)$.

Therefore, $\phi(H)$ is closed under the binary operation of G'.

Let $\phi(a) \in \phi(H)$.
Then $a \in H$ by definition of $\phi(H)$.
Since H is a group, then $a^{-1} \in H$.
Since $a^{-1} \in H$ and $\phi(a^{-1}) = (\phi(a))^{-1}$, then $(\phi(a))^{-1} \in \phi(H)$.
Consequently, $\phi(H)$ is closed under taking of inverses.

Since $\phi(H)$ is a subset of G' and is closed under the binary operation of G' and is closed under the identity of G' and is closed under inverses, then by the subgroup test, $\phi(H)$ is a subgroup of G'.
Therefore, $\phi(H) < G'$. □

Proof. We prove 5:
Suppose $K' < G'$.
We must prove the pre-image of K' is a subgroup of G.
Let K be the pre-image of K'.
Then $K = \phi^{-1}(K') = \{a \in G : \phi(a) \in K'\}$, so $K \subset G$.
Therefore, K is a subset of G.

Let $x, y \in K$.
Since $x \in K$, then $x \in G$ and $\phi(x) \in K'$.
Since $y \in K$, then $y \in G$ and $\phi(y) \in K'$.
Since G is a group and $x \in G$ and $y \in G$, then by closure of G, we have $xy \in G$.
Since $K' < G'$, then K' is a group.
Since K' is a group and $\phi(x) \in K'$ and $\phi(y) \in K'$, then by closure of K', we have $\phi(x)\phi(y) \in K'$.
Since $xy \in G$ and $\phi(xy) = \phi(x)\phi(y)$ and $\phi(x)\phi(y) \in K'$, then $xy \in K$.
Therefore, K is closed under the binary operation of G.

Since $K' < G'$, then $e' \in K'$.
Since $e' = \phi(e)$, then $\phi(e) \in K'$.
Since $e \in G$ and $\phi(e) \in K'$, then $e \in K$.
Therefore, K is closed under the identity of G.

Let $x \in K$.
Then $x \in G$ and $\phi(x) \in K'$.
Since G is a group and $x \in G$, then $x^{-1} \in G$.
Since K' is a group and $\phi(x) \in K'$, then $(\phi(x))^{-1} \in K'$.
Since $x^{-1} \in G$ and $\phi(x^{-1}) = (\phi(x))^{-1}$ and $(\phi(x))^{-1} \in K'$, then $x^{-1} \in K$.
Therefore, K is closed under inverses.

Since K is a subset of G and K is closed under the binary operation of G and K is closed under the identity of G and K is closed under inverses, then by the subgroup test, $K < G$.
Therefore, $\phi^{-1}(K') < G$.

Suppose $K' \lhd G'$.
Let $g \in G$ and $h \in K$.
Let $g' = ghg^{-1}$.
To prove $K \lhd G$, we must prove $g' \in K$, so we must prove $g' \in G$ and $\phi(g') \in K'$.

Since $g \in G$ and G is a group, then $g^{-1} \in G$.
Since K is a subgroup of G, then K is a subset of G.
Since $h \in K$ and $K \subset G$, then $h \in G$.
Since G is closed under its binary operation and $g, g^{-1}, h \in G$, then $g' \in G$.

Observe that

$$\begin{aligned} \phi(g') &= \phi(ghg^{-1}) \\ &= \phi(gh)\phi(g^{-1}) \\ &= \phi(g)\phi(h)\phi(g^{-1}) \\ &= \phi(g)\phi(h)(\phi(g))^{-1}. \end{aligned}$$

Since $h \in K$, then $\phi(h) \in K'$, by definition of K.
Since $K' \lhd G'$, then $aba^{-1} \in K'$ for every $a \in G'$ and every $b \in K'$.
Since $\phi(g) \in G'$ and $\phi(h) \in K'$, then this implies $\phi(g)\phi(h)(\phi(g))^{-1} \in K'$.
Since $\phi(g)\phi(h)(\phi(g))^{-1} = \phi(g')$, then $\phi(g') \in K'$.
Since $g' \in G$ and $\phi(g') \in K'$, then $g' \in K$.
Therefore, $K \lhd G$. □

Theorem 108. *Let $\phi : G \to G'$ be a group homomorphism.*
Then $\ker(\phi) \lhd G$.

Proof. We prove $K < G$.
Let e be the identity of G and e' be the identity of G'.
Let $K = \ker(\phi) = \{g \in G : \phi(g) = e'\}$.
Then $K \subset G$, so K is a subset of G.

Let $a, b \in K$.
Then $a, b \in G$ and $\phi(a) = \phi(b) = e'$. Thus,

$$\begin{aligned} \phi(ab) &= \phi(a)\phi(b) \\ &= e'e' \\ &= e'. \end{aligned}$$

Since $ab \in G$ and $\phi(ab) = e'$, then $ab \in K$.
Therefore, K is closed under the binary operation of G.

Since $e \in G$ and $\phi(e) = e'$, then $e \in K$.
Therefore, K is closed under the identity of G.

Let $a \in K$.

Then $a \in G$ and $\phi(a) = e'$.

Let $a^{-1} \in G$. Then

$$\begin{aligned} \phi(a^{-1}) &= (\phi(a))^{-1} \\ &= e'^{-1} \\ &= e'. \end{aligned}$$

Since $a^{-1} \in G$ and $\phi(a^{-1}) = e'$, then $a^{-1} \in K$.

Therefore, K is closed under inverses.

Since K is a subset of G and K is closed under the binary operation of G and K is closed under the identity of G and K is closed under inverses, then by the subgroup test, $K < G$. □

Proof. To prove K is normal in G, we must prove $(\forall g \in G)(\forall h \in K)(ghg^{-1} \in K)$.

Let $g \in G$ and $h \in K$.

Since $h \in K$, then $h \in G$ and $\phi(h) = e'$.

Since $g \in G$ and G is a group, then $g^{-1} \in G$.

Since $g, g^{-1}, h \in G$ and G is closed under its binary operation, then $ghg^{-1} \in G$.

Observe that

$$\begin{aligned} \phi(ghg^{-1}) &= \phi(g)\phi(h)\phi(g^{-1}) \\ &= \phi(g)e'\phi(g^{-1}) \\ &= \phi(g)\phi(g^{-1}) \\ &= \phi(gg^{-1}) \\ &= \phi(e) \\ &= e'. \end{aligned}$$

Since $ghg^{-1} \in G$ and $\phi(ghg^{-1}) = e'$, then $ghg^{-1} \in K$.

Therefore, $K \lhd G$. □

Theorem 109. *Let $\phi : G \to G'$ be a group homomorphism.*

If ϕ is injective, then $G \cong \phi(G)$.

Solution. Suppose ϕ is injective.

To prove $G \cong \phi(G)$, we must prove there exists an isomorphism $f : G \to \phi(G)$.

□

Proof. Suppose ϕ is injective.

Let $f : G \to \phi(G)$ be the restriction of ϕ to $\phi(G)$.

Then $f(g) = \phi(g)$ for all $g \in G$.

Clearly, f is a function.

Let $a, b \in G$.
Since ϕ is a homomorphism, then $\phi(ab) = \phi(a)\phi(b)$ and $\phi(G) < G'$.
Observe that

$$\begin{aligned} f(ab) &= \phi(ab) \\ &= \phi(a)\phi(b) \\ &= f(a)f(b). \end{aligned}$$

Hence, f is a group homomorphism.

Suppose $f(a) = f(b)$.
Then $\phi(a) = \phi(b)$.
Since ϕ is injective, then $\phi(a) = \phi(b)$ implies $a = b$.
Hence, $a = b$.
Therefore, $f(a) = f(b)$ implies $a = b$, so f is injective.

Let $b \in \phi(G)$.
By definition of $\phi(G)$, there exists $a \in G$ such that $\phi(a) = b$.
Since $f(a) = \phi(a) = b$, then there exists $a \in G$ such that $f(a) = b$.
Therefore, f is surjective.

Since f is injective and surjective, then f is bijective.
Thus, f is a bijective homomorphism, so $f : G \to \phi(G)$ is an isomorphism.
Therefore, $G \cong \phi(G)$. □

Theorem 110. *Let $\phi : G \to G'$ be a group homomorphism.*
Let e be the identity of G.
Then ϕ is injective if and only if $\ker(\phi) = \{e\}$.

Solution. Consider if the kernel of a homomorphism has more than one element, then by the pigeonhole principle there will be at least two elements in the kernel which map to $e' \in G'$.
Hence, ϕ would not be one to one.
Now, let's suppose the kernel has exactly one element in it.
Then the only element that maps to e' is $e \in G$.
We must prove $P \Leftrightarrow Q$:
1. Necessary ONLY IF $\Rightarrow$ ϕ is injective, then $\ker(\phi) = \{e\}$.
2. Sufficient IF $\ker(\phi) = \{e\}$, then ϕ is injective. □

Proof. Let e' be the identity of G'.
We prove if ϕ is injective, then $\ker(\phi) = \{e\}$.
Suppose ϕ is injective.
Let $a \in \ker(\phi)$.
Then $a \in G$ and $\phi(a) = e'$.
Observe that $\phi(e) = e' = \phi(a)$.
Since ϕ is injective, then $\phi(e) = \phi(a)$ implies $e = a$.

Hence, $e = a$, so $a \in \{e\}$.
Thus, $a \in \ker(\phi)$ implies $a \in \{e\}$, so $\ker(\phi) \subset \{e\}$.
Since $e \in G$ and $\phi(e) = e'$, then $e \in \ker(\phi)$.
Hence, $\{e\} \subset \ker(\phi)$.
Since $\ker(\phi) \subset \{e\}$ and $\{e\} \subset \ker(\phi)$, then $\ker(\phi) = \{e\}$, as desired. □

Proof. We prove if $\ker(\phi) = \{e\}$, then ϕ is injective.
Conversely, suppose $\ker(\phi) = \{e\}$.
To prove ϕ is injective, we must prove $(\forall a, b \in G)(\phi(a) = \phi(b) \to a = b)$.
Let $a, b \in G$ such that $\phi(a) = \phi(b)$.
Observe that

$$\begin{aligned} e' &= \phi(a)[\phi(a)]^{-1} \\ &= \phi(b)[\phi(a)]^{-1} \\ &= \phi(b)\phi(a^{-1}) \\ &= \phi(ba^{-1}). \end{aligned}$$

Since $\phi(ba^{-1}) = e'$ and $ba^{-1} \in G$, then $ba^{-1} \in \ker(\phi)$.
Since $\ker(\phi) = \{e\}$, then, $ba^{-1} \in \{e\}$, so $ba^{-1} = e$.
Observe that

$$\begin{aligned} a &= ea \\ &= (ba^{-1})a \\ &= b(a^{-1}a) \\ &= be \\ &= b. \end{aligned}$$

Therefore, $a = b$, as desired. □

Theorem 111. *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 $Im(\phi) = G'$.

Proof. We prove 1.
Suppose ϕ is an epimorphism.
Then ϕ is surjective, so the image of ϕ is G'.
Therefore, $Im(\phi) = G'$.

Conversely, suppose $Im(\phi) = G'$.Then ϕ is surjective, so ϕ is an epimorphism. □

Proof. We prove 2.
Suppose ϕ is a monomorphism.
Then ϕ is injective.
The homomorphism ϕ is injective iff $\ker(\phi) = \{e\}$.
Therefore, $\ker(\phi) = \{e\}$.

Conversely, suppose $\ker(\phi) = \{e\}$.

The homomorphism ϕ is injective iff $\ker(\phi) = \{e\}$.

Therefore, ϕ is injective, so ϕ is a monomorphism. $\square$

Proof. We prove 3.

Suppose ϕ is an isomorphism.

Then ϕ is bijective, so ϕ is injective and surjective.

Since ϕ is surjective, then $Im(\phi) = G'$.

Since ϕ is injective and a homomorphism ϕ is injective iff $\ker(\phi) = \{e\}$, then $\ker(\phi) = \{e\}$.

Therefore, $\ker(\phi) = \{e\}$ and $Im(\phi) = G'$.

Conversely, suppose $\ker(\phi) = \{e\}$ and $Im(\phi) = G'$.

Since $\ker(\phi) = \{e\}$ iff ϕ is injective and $\ker(\phi) = \{e\}$, then ϕ is injective.

Since $Im(\phi) = G'$, then ϕ is surjective.

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

Since ϕ is a homomorphism and ϕ is bijective, then ϕ is an isomorphism. $\square$

Theorem 112. *The composition of group homomorphisms is a group homomorphism.*

Proof. 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.

We must prove $f_2 \circ f_1$ is a group homomorphism.

Let $a, b \in G$.

Then

$$\begin{aligned}
(f_2 \circ f_1)(ab) &= f_2[f_1(ab)] \\
&= f_2[f_1(a)f_1(b)] \\
&= f_2[f_1(a)] * f_2[f_1(b)] \\
&= (f_2 \circ f_1)(a) * (f_2 \circ f_1)(b).
\end{aligned}$$

Hence, $(f_2 \circ f_1)(ab) = (f_2 \circ f_1)(a) * (f_2 \circ f_1)(b)$.

Therefore, $f_2 \circ f_1 : G \to G''$ is a group homomorphism. $\square$

Theorem 113. *Let $\phi : G \to G'$ be a group homomorphism with kernel K.*

Then $xK = Kx = \phi^{-1}(\phi(x))$ for all $x \in G$.

Proof. Let e' be the identity of G'.

Let $x \in G$.

Observe that $\phi^{-1}(\phi(x)) = \{a \in G : \phi(a) = \phi(x)\}$, by definition of preimage of an element.

Observe that $K = \ker(\phi) = \{a \in G : \phi(a) = e'\}$ and $xK = \{xk : k \in K\}$.

Let $xk \in xK$.

Then $k \in K$, so $k \in G$ and $\phi(k) = e'$.

Since $K < G$, then $K \subset G$.

Since $k \in K$ and $K \subset G$, then $k \in G$.

By closure of $G, xk \in G$.

Observe that

$$\begin{aligned} \phi(xk) &= \phi(x)\phi(k) \\ &= \phi(x)e' \\ &= \phi(x). \end{aligned}$$

Since $xk \in G$ and $\phi(xk) = \phi(x)$, then $xk \in \phi^{-1}(\phi(x))$.

Thus, $xk \in xK$ implies $xk \in \phi^{-1}(\phi(x))$, so $xK \subset \phi^{-1}(\phi(x))$.

Let $a \in \phi^{-1}(\phi(x))$.

Then $a \in G$ and $\phi(a) = \phi(x)$.

Let $k = x^{-1}a$.

Since $x^{-1}, a \in G$, then by closure of $G, k \in G$.

Observe that

$$\begin{aligned} \phi(k) &= \phi(x^{-1}a) \\ &= \phi(x^{-1})\phi(a) \\ &= (\phi(x))^{-1}\phi(a) \\ &= (\phi(a))^{-1}\phi(a) \\ &= e'. \end{aligned}$$

Since $k \in G$ and $\phi(k) = e'$, then $k \in K$.

Hence, there exists $k \in K$ such that $k = x^{-1}a$, so there exists $k \in K$ such that $xk = a$.

Thus, $a \in xK$.

Therefore, $a \in \phi^{-1}(\phi(x))$ implies $a \in xK$, so $\phi^{-1}(\phi(x)) \subset xK$.

Since $xK \subset \phi^{-1}(\phi(x))$ and $\phi^{-1}(\phi(x)) \subset xK$, then $xK = \phi^{-1}(\phi(x))$.

Since $K \lhd G$, then $xK = Kx$.

Therefore, $xK = Kx = \phi^{-1}(\phi(x))$. ☐

Corollary 114. *If G is a finite group and $\phi : G \to G'$ is a group homomorphism, then $|G| = |\ker(\phi)||Im(\phi)|$.*

Proof. Let G be a finite group and $\phi : G \to G'$ be a group homomorphism with kernel K.

Then $Im(\phi) = \phi(G) = \{\phi(g) \in G' : g \in G\}$.

Let $\phi(g) \in Im(\phi)$.

Then $g \in G$ and the preimage of $\phi(g)$ is the left coset gK.

Thus, $|Im(\phi)|$ is the number of distinct left cosets of K in G.

Therefore, $|Im(\phi)| = [G : K] = \frac{|G|}{|K|}$, so $|G| = |K||Im(\phi)|$. ☐

Theorem 115. *Let G be a group.*

If $N \lhd G$, then $\eta : G \mapsto \frac{G}{N}$ defined by $\eta(a) = aN$ for all $a \in G$ is a homomorphism such that $\ker(\eta) = N$.

We call η the ***natural homomorphism*** *from G onto $\frac{G}{N}$.*

Proof. Suppose N is a normal subgroup of G.
Then $\frac{G}{N}$ is a group under coset multiplication with identity N.

Suppose $a, b \in G$ such that $a = b$.
Then $\eta(a) = aN$ and $\eta(b) = bN$.
Since $a = b$ and $b \in bN$, then $a \in bN$.
Thus, $aN = bN$, so $\eta(a) = \eta(b)$.
Hence, $a = b$ implies $\eta(a) = \eta(b)$, so η is well defined.
Therefore, η is a function.

Let $a, b \in G$.
Then $\eta(ab) = (ab)N = (aN)(bN) = \eta(a)\eta(b)$.
Therefore, η is a homomorphism.

Let $bN \in \frac{G}{N}$.
Then $b \in G$, by definition of $\frac{G}{N}$.
Observe that $\eta(b) = bN$.
Hence, there exists $b \in G$ such that $\eta(b) = bN$, so η is surjective.
Observe that $\ker(\eta) = \{g \in G : \eta(g) = N\}$.

Let $x \in \ker(\eta)$.
Then $x \in G$ and $N = \eta(x) = xN$.
Since $x \in xN$ and $xN = N$, then $x \in N$.
Thus, $x \in \ker(\eta)$ implies $x \in N$, so $\ker(\eta) \subset N$.

Let $y \in N$.
Since N is a subgroup of G, then N is a subset of G.
Since $y \in N$ and $N \subset G$, then $y \in G$.
Since $y \in yN$ and $y \in N$, then $yN = N$.
Thus, $\eta(y) = yN = N$.
Since $y \in G$ and $\eta(y) = N$, then $y \in \ker(\eta)$.
Hence, $y \in N$ implies $y \in \ker(\eta)$, so $N \subset \ker(\eta)$.
Since $\ker(\eta) \subset N$ and $N \subset \ker(\eta)$, then $\ker(\eta) = N$. □

Isomorphisms

Lemma 116. *The isomorphism relation on groups is reflexive.*

Proof. Let $(G, *)$ be a group.
To prove the isomorphic relation is reflexive, we must prove $G \cong G$.
Let $\phi : G \to G$ be defined by $\phi(x) = x$ for all $x \in G$.
Then ϕ is the identity map and is bijective.

Let $a, b \in G$.
Then $\phi(ab) = ab = \phi(a)\phi(b)$.
Therefore, ϕ is a homomorphism.

Since ϕ is a homomorphism and ϕ is bijective, then $\phi : G \to G$ is an isomorphism.
Therefore, $G \cong G$. $\square$

Lemma 117. *The isomorphism relation on groups is symmetric.*

Proof. Let $(G, *)$ and $(H, \cdot)$ be a groups.
To prove is isomorphic to is symmetric, we must prove if $G \cong H$, then $H \cong G$.

Suppose $G \cong H$.
Then there exists an isomorphism from G to H.
Let $\phi : G \to H$ be an isomorphism.
Then ϕ is a bijective function and is a homomorphism.
Since ϕ is bijective, then the inverse function exists.
Let $\phi^{-1} : H \to G$ be the inverse function of ϕ.

Since $(\phi^{-1})^{-1} = \phi$, then ϕ^{-1} is invertible.
All invertible functions are bijective, so ϕ^{-1} is bijective.
Therefore, ϕ^{-1} is a bijective function.

We prove ϕ^{-1} is a homomorphism.
Let $b_1, b_2 \in H$.
Since ϕ is bijective, then ϕ is surjective.
Thus there exists $a_1, a_2 \in G$ such that $\phi(a_1) = b_1$ and $\phi(a_2) = b_2$.
Hence, $\phi^{-1}(b_1) = a_1$ and $\phi^{-1}(b_2) = a_2$.

Since ϕ and ϕ^{-1} are inverses, then $\phi^{-1} \circ \phi = id$.
Hence, $(\phi^{-1} \circ \phi)(x) = x$ for all $x \in G$.
Since G is closed under $*$ and $a_1, a_2 \in G$, then $a_1 a_2 \in G$.
Thus, $(\phi^{-1} \circ \phi)(a_1 a_2) = a_1 a_2$.

Observe that

$$\begin{aligned}
\phi^{-1}(b_1b_2) &= \phi^{-1}(\phi(a_1)\phi(a_2)) \\
&= \phi^{-1}(\phi(a_1a_2)) \\
&= (\phi^{-1}\circ\phi)(a_1a_2) \\
&= a_1a_2 \\
&= \phi^{-1}(b_1)\phi^{-1}(b_2).
\end{aligned}$$

Thus, $\phi^{-1}(b_1b_2) = \phi^{-1}(b_1)\phi^{-1}(b_2)$, so ϕ^{-1} is a homomorphism.

Since ϕ^{-1} is a bijective homomorphism, then $\phi^{-1} : H \to G$ is an isomorphism.

Therefore, $H \cong G$. ☐

Lemma 118. *The isomorphism relation on groups is transitive.*

Proof. Let $(G,*), (H,\cdot), (K,\diamond)$ be groups.

To prove is isomorphic to is transitive, we must prove if $G \cong H$ and $H \cong K$, then $G \cong K$.

Suppose $G \cong H$ and $H \cong K$.

Then there exist isomorphisms $\phi : G \to H$ and $\psi : H \to K$.

Thus, ϕ is a bijective homomorphism and ψ is a bijective homomorphism.

Since ϕ is a bijective homomorphism, then ϕ is a homomorphism and ϕ is a bijection.

Since ψ is a bijective homomorphism, then ψ is a homomorphism and ψ is a bijection.

Let $\psi\circ\phi : G \to K$ be the composition of ϕ and ψ.

The composition of bijections is a bijection.

Since ϕ is a bijection and ψ is a bijection, then $\psi\circ\phi$ is a bijection.

The composition of group homomorphisms is a group homomorphism.

Since ϕ is a homomorphism and ψ is a homomorphism, then $\psi\circ\phi$ is a homomorphism.

Since $\psi\circ\phi$ is a bijection and $\psi\circ\phi$ is a homomorphism, then $\psi\circ\phi : G \to K$ is an isomorphism.

Therefore, $G \cong K$. ☐

Theorem 119. *The isomorphism relation on groups is an equivalence relation on the class of all groups.*

Proof. The isomorphism relation on the class of all groups is reflexive, symmetric, and transitive.

Therefore, the isomorphism relation is an equivalence relation. ☐

Theorem 120. ***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

Proof. We prove 1.
Since ϕ is an isomorphism, then ϕ is a bijective homomorphism, so ϕ is a bijection.
Thus, ϕ is a bijective function from G to G'.
Since there exists a bijective function from G to G', then $|G| = |G'|$. □

Proof. We prove 2.
Suppose G is abelian.
Let $a', b' \in G'$.
Since ϕ is an isomorphism, then ϕ is a bijective homomorphism, so ϕ is a bijective function.
Hence, ϕ is surjective, so there exists $a \in G$ such that $\phi(a) = a'$ and there exists $b \in G$ such that $\phi(b) = b'$.
Observe that

$$\begin{aligned} a' \cdot b' &= \phi(a) \cdot \phi(b) \\ &= \phi(ab) \\ &= \phi(ba) \\ &= \phi(b) \cdot \phi(a) \\ &= b' \cdot a'. \end{aligned}$$

Therefore, $a'b' = b'a'$, so G' is abelian. □

Proof. We prove 3.
Suppose G is cyclic.
Then there exists $g \in G$ such that $G = \{g^k : k \in \mathbb{Z}\}$.
Since ϕ is a function, then there exists a unique $g' \in G'$ such that $\phi(g) = g'$.

Every element of a group generates a cyclic subgroup.
Since $g' \in G'$ and G' is a group, then g' generates a cyclic subgroup.
Let T be the cyclic subgroup of G' generated by g'.
Then $T = \{(g')^k : k \in \mathbb{Z}\}$.
Since T is a subgroup of G', then T is a subset of G', so $T \subset G'$.

Let $b \in G'$.
Since ϕ is surjective, then there exists $a \in G$ such that $\phi(a) = b$.
Since $a \in G$, then there exists $m \in \mathbb{Z}$ such that $a = g^m$.
Observe that

$$\begin{aligned} (g')^m &= (\phi(g))^m \\ &= \phi(g^m) \\ &= \phi(a) \\ &= b. \end{aligned}$$

Thus, there exists $m \in \mathbb{Z}$ such that $b = (g')^m$, so $b \in T$.
Hence, $b \in G'$ implies $b \in T$, so $G' \subset T$.
Since $G' \subset T$ and $T \subset G'$, then $G' = T$.
Therefore, there exists $g' \in G'$ such that $G' = T$, so G' is cyclic. □

Proof. We prove 4.
Suppose H is a subgroup of G of order n.
Then n is a positive integer and $|H| = n$.

Since ϕ is an isomorphism, then ϕ is a bijective homomorphism, so ϕ is a bijective function and ϕ is a homomorphism.
Every homomorphism preserves subgroups.
Since ϕ is a homomorphism, then ϕ preserves subgroups.
Thus, if H is a subgroup of G, then $\phi(H)$ is a subgroup of G'.
Since H is a subgroup of G, then we conclude $\phi(H)$ is a subgroup of G'.

Let $\phi' : H \to \phi(H)$ be the function defined by $\phi'(h) = \phi(h)$ for all $h \in H$.

We prove ϕ' is surjective.
Let $b \in \phi(H)$.
Then $b = \phi(a)$ for some $a \in H$, so $\phi'(a) = \phi(a) = b$.
Since $\phi'(a) = b$ for some $a \in H$, then ϕ' is surjective.

We prove ϕ' is injective.
Let $x, y \in H$ such that $\phi'(x) = \phi'(y)$.
Then $\phi(x) = \phi'(x) = \phi'(y) = \phi(y)$.
Since ϕ is bijective, then ϕ is injective, so for every $a, b \in G$, $\phi(a) = \phi(b)$ implies $a = b$.
Since $H < G$, then $H \subset G$.
Since $x \in H$ and $H \subset G$, then $x \in G$.
Since $y \in H$ and $H \subset G$, then $y \in G$.
Since $x \in G$ and $y \in G$, then $\phi(x) = \phi(y)$ implies $x = y$.
Since $\phi(x) = \phi(y)$, then we conclude $x = y$.
Therefore, ϕ' is injective.

Since ϕ' is injective and surjective, then ϕ' is bijective, so $|H| = |\phi(H)|$.
Thus, $n = |H| = |\phi(H)|$.

Since $\phi(H)$ is a subgroup of G' and $|\phi(H)| = n$, then $\phi(H)$ is a subgroup of G' of order n. $\square$

Proof. We prove 5.
Let a be an arbitrary element of G of finite order n.
Then $a \in G$ and $|a| = n$.
The order of a is the order of the cyclic group generated by a.
Let H be the cyclic subgroup of G generated by a.
Then $H = \{a^k : k \in \mathbb{Z}\}$ and $H < G$ and $|H| = n$ and $a \in H$.

Since ϕ is an isomorphism, then if H is a subgroup of G of order n, then the image of H is a subgroup of G' of order n.
Since H is a subgroup of G of order n, then we conclude the image of H is a subgroup of G' of order n.
Let $\phi(H)$ be the image of H under ϕ.
Then $\phi(H) = \{\phi(h) \in G' : h \in H\}$ and $\phi(H) < G'$ and $|\phi(H)| = n$.
Thus, $|H| = |\phi(H)|$.

Since G' is a group, then every element of G' generates a cyclic subgroup of G'.
Since $\phi(a) \in G'$, then $\phi(a)$ generates a cyclic subgroup of G'.
Let H' be the cyclic subgroup of G' generated by $\phi(a)$.
Then $H' = \{(\phi(a))^k : k \in \mathbb{Z}\}$.
The order of $\phi(a)$ is the order of the cyclic subgroup generated by $\phi(a)$.
Thus, $|\phi(a)| = |H'|$.

The cyclic subgroup of G' generated by $\phi(a)$ is the smallest subgroup of G' that contains $\phi(a)$.
Thus, if K is a subgroup of G' that contains $\phi(a)$, then $H' \subset K$.
Since $a \in H$ and $\phi(a) \in G'$, then $\phi(a) \in \phi(H)$.
Since $\phi(H)$ is a subgroup of G' that contains $\phi(a)$, then $H' \subset \phi(H)$.

Let $h' \in \phi(H)$.
Then there exists $h \in H$ such that $h' = \phi(h) \in G'$.
Since $h \in H$, then there exists $k \in \mathbb{Z}$ such that $h = a^k$.
Thus, $h' = \phi(h) = \phi(a^k) = (\phi(a))^k$.
Hence, there exists $k \in \mathbb{Z}$ such that $h' = (\phi(a))^k$, so $h' \in H'$.
Therefore, $h' \in \phi(H)$ implies $h' \in H'$, so $\phi(H) \subset H'$.
Since $\phi(H) \subset H'$ and $H' \subset \phi(H)$, then $\phi(H) = H'$.
Thus, $n = |H| = |\phi(H)| = |H'| = |\phi(a)|$.
Therefore, $|\phi(a)| = n$, as desired. $\square$

Theorem 121. *Every cyclic group of infinite order is isomorphic to* $(\mathbb{Z}, +)$.

Proof. Let $f : \mathbb{Z} \to H$ be a binary relation defined by $n \mapsto a^n$ for all $n \in \mathbb{Z}$.
Let $n \in \mathbb{Z}$.
Then $f(n) = a^n \in H$.
Let $n_1, n_2 \in \mathbb{Z}$ such that $n_1 = n_2$.
Then $f(n_1) = a^{n_1} = a^{n_2} = f(n_2)$.
Thus, $n_1 = n_2$ implies $f(n1) = f(n_2)$, so f is well defined.
Therefore, f is a function.

Let $s, t \in \mathbb{Z}$ such that $a^s = a^t$. Observe that $a^{s-t} = a^s a^{-t} = a^t a^{-t} = a^{t-t} = a^0 = e$. Thus, $a^{s-t} = e$. Since a is of infinite order and $s - t \in \mathbb{Z}$, then $a^{s-t} = e$ iff $s - t = 0$. Hence, $s - t = 0$, so $s = t$.

Thus, $a^s = a^t$ implies $s = t$, so f is injective. Since $a^s = a^t$ implies $s = t$, then $s \neq t$ implies $a^s \neq a^t$. Hence, each power of a is distinct.

Let $b \in H$. Then there exists $k \in \mathbb{Z}$ such that $b = a^k$. Observe that $f(k) = a^k = b$. Hence, there exists $k \in \mathbb{Z}$ such that $f(k) = b$. Therefore, f is surjective.

Since f is injective and surjective, then f is bijective. Thus, $f : \mathbb{Z} \mapsto H$ is a bijective function.

We prove f is a group homomorphism from $(\mathbb{Z}, +)$ to $(H, *)$. Let $m, n \in \mathbb{Z}$.
Observe that

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

Hence, $f(m+n) = f(m)f(n)$, so f is a group homomorphism. Since f is a bijective homomorphism, then $f : \mathbb{Z} \to H$ is an isomorphism. Therefore, $\mathbb{Z} \cong H$, so $H \cong \mathbb{Z}$. Since H is arbitrary, then every cyclic group of infinite order is isomorphic to $(\mathbb{Z}, +)$. Thus, $H = \{a^k : k \in \mathbb{Z}\} = \{..., a^{-3}, a^{-2}, a^{-1}, a^0, a^1, a^2, a^3, ...\}$ and $|H| = \infty$. $\square$

Theorem 122. *Every cyclic group of finite order n is isomorphic to $(\mathbb{Z}_n, +)$.*

Proof. Let $(G, *)$ be a cyclic group of finite order n.
Then $|G| = n$.
We must prove $G \cong \mathbb{Z}_n$.
Since G is cyclic, then there exists $a \in G$ such that $G = \{a^k : k \in \mathbb{Z}\}$.
Thus, $n = |G| = |\{a^k : k \in \mathbb{Z}\}|$.
The order of a is the order of the cyclic subgroup of G generated by a.
Thus, the order of a is the order of G, so $|a| = n$.

Let $\phi : \mathbb{Z}_n \to G$ be a binary relation defined by $\phi([k]) = a^k$ for all $[k] \in \mathbb{Z}_n$.
Let $[k] \in \mathbb{Z}_n$.
Then $\phi([k]) = a^k \in G$.
Suppose $[x], [y] \in \mathbb{Z}_n$ such that $[x] = [y]$.
Then $x \equiv y \pmod{n}$.

Since a has finite order n, then $x \equiv y \pmod{n}$ iff $a^x = a^y$.
Hence, $a^x = a^y$, so $\phi([x]) = \phi([y])$.
Thus, $[x] = [y]$ implies $\phi([x]) = \phi([y])$, so ϕ is well defined.
Therefore, ϕ is a function.
Let $[x], [y] \in \mathbb{Z}_n$.
Then

$$\begin{aligned} \phi([x]+[y]) &= \phi([x+y]) \\ &= a^{x+y} \\ &= a^x a^y \\ &= \phi([x])\phi([y]). \end{aligned}$$

Therefore, ϕ is a homomorphism.
Let $[x], [y] \in \mathbb{Z}_n$ such that $\phi([x]) = \phi([y])$.
Then $a^x = a^y$.
Since a has finite order, then $a^x = a^y$ iff $x \equiv y \pmod{n}$.
Thus, $x \equiv y \pmod{n}$, so $[x] = [y]$.
Hence, $\phi([x]) = \phi([y])$ implies $[x] = [y]$, so ϕ is injective.

Let $y \in G$.
Then there exists $k \in \mathbb{Z}$ such that $y = a^k$, by definition of G.
Thus, $[k] \in \mathbb{Z}_n$ and $\phi([k]) = a^k = y$.
Hence, there exists $[k] \in \mathbb{Z}_n$ such that $\phi([k]) = y$.
Therefore, ϕ is surjective.
Since ϕ is injective and surjective, then ϕ is bijective.
Thus, ϕ is a bijective homomorphism, so $\phi : \mathbb{Z}_n \to G$ is an isomorphism.
Therefore, $\mathbb{Z}_n \cong G$, so $G \cong \mathbb{Z}_n$. $\square$

Corollary 123. *Every group of prime order p is isomorphic to $(\mathbb{Z}_p, +)$.*

Proof. Let G be a group of prime order p.
Every group of prime order is cyclic.
Therefore, G is cyclic.
Every cyclic group of finite order n is isomorphic to $(\mathbb{Z}_n, +)$.
Thus, every cyclic group of finite order p is isomorphic to $(\mathbb{Z}_p, +)$.
Since G is a cyclic group of finite order p, then G is isomorphic to $\mathbb{Z}_p$. $\square$

Proposition 124. *Let G be an abelian group with subgroups H and K.
If $HK = G$ and $H \cap K = \{e\}$, then $G \cong H \times K$.*

Proof. Let e be the identity of G.
Suppose $HK = G$ and $H \cap K = \{e\}$.
Let $\phi : H \times K \to G$ be defined by $\phi(h,k) = hk$ for all $(h,k) \in H \times K$.
Clearly, ϕ is a function.

Let $(h_1, k_1), (h_2, k_2) \in H \times K$.
Then

$$\begin{aligned}
\phi((h_1,k_1)(h_2,k_2)) &= \phi(h_1h_2, k_1k_2) \\
&= (h_1h_2)(k_1k_2) \\
&= h_1(h_2k_1)k_2 \\
&= h_1(k_1h_2)k_2 \\
&= (h_1k_1)(h_2k_2) \\
&= \phi(h_1,k_1)\phi(h_2,k_2)
\end{aligned}$$

Therefore, ϕ is a group homomorphism.

Let $g \in G$.
Since $G = HK$, then there exist $h \in H$ and $k \in K$ such that $g = hk$.
Thus, there exists $(h,k) \in H \times K$ such that $g = \phi(h,k)$.
Hence, ϕ is surjective.

To prove ϕ is injective, we prove $\ker(\phi) = \{(e,e)\}$.
Let $(a,b) \in \ker(\phi)$. Then $(a,b) \in H \times K$ and $\phi(a,b) = e$. Thus, $a \in H$ and $b \in K$ and $ab = e$. Hence, $a = b^{-1}$ and $b = a^{-1}$. Since $a \in H$ and $H < G$, then $a^{-1} \in H$. Thus, $b \in H$. Since $b \in K$ and $K < G$, then $b^{-1} \in K$. Thus, $a \in K$. Since $a \in H$ and $a \in K$, then $a \in H \cap K$. Since $b \in H$ and $b \in K$, then $b \in H \cap K$. Since $a \in H \cap K$ and $H \cap K = \{e\}$, then $a \in \{e\}$, so $a = e$. Since $b \in H \cap K$ and $H \cap K = \{e\}$, then $b \in \{e\}$, so $b = e$. Thus, $(a,b) = (e,e)$, so $(a,b) \in \{(e,e)\}$. Therefore, $(a,b) \in \ker(\phi)$ implies $(a,b) \in \{(e,e)\}$, so $\ker(\phi) \subset \{(e,e)\}$.

Since ϕ is a group homomorphism, then $(e,e) \in \ker(\phi)$, so $\{(e,e)\} \subset \ker(\phi)$.
Thus, $\ker(\phi) \subset \{(e,e)\}$ and $\{(e,e)\} \subset \ker(\phi)$, so $\ker(\phi) = \{(e,e)\}$.
Since $\ker(\phi) = \{(e,e)\}$ iff ϕ is injective, then ϕ is injective.
Therefore, ϕ is a bijective homomorphism, so ϕ is an isomorphism.
Thus, $H \times K \cong G$, so $G \cong H \times K$. $\square$

Proposition 125. *The identity map is an automorphism in any group.*

Proof. Let $(G, *)$ be a group.
Let $I_G : G \to G$ be the identity map on G defined by $I_G(x) = x$ for all $x \in G$.
Then I_G is a bijection, so I_G is a bijective function.

Let $a, b \in G$.
Since $I_G(ab) = ab = I_G(a)I_G(b)$, then I_G is a homomorphism.
Since I_G is a homomorphism and I_G is bijective, then I_G is an isomorphism.
Therefore, $I_G : G \to G$ is an automorphism. $\square$

Theorem 126. *Let $Aut(G)$ be the set of all automorphisms of a group G.*
Then $(Aut(G), \circ)$ is a subgroup of $(S_G, \circ)$.

Proof. Let $\alpha \in Aut(G)$.

Then $\alpha : G \to G$ is an isomorphism, so α is a bijective homomorphism.

Thus, α is a bijective function, so α is a permutation of G.

Hence, $\alpha \in S_G$.

Therefore, $\alpha \in Aut(G)$ implies $\alpha \in S_G$, so $Aut(G) \subset S_G$.

Consequently, $Aut(G)$ is a subset of S_G.

Let $\alpha, \beta \in Aut(G)$.

Then $\alpha : G \to G$ and $\beta : G \to G$ are isomorphisms, so α and β are bijective homomorphisms.

Since α is a bijective homomorphism, then α is a homomorphism.

Since β is a bijective homomorphism, then β is a homomorphism.

Since $\alpha \in Aut(G)$ and $Aut(G) \subset S_G$, then $\alpha \in S_G$.

Since $\beta \in Aut(G)$ and $Aut(G) \subset S_G$, then $\beta \in S_G$.

Let $\alpha\beta : G \to G$ be the composition of α and β.

Since $\alpha \in S_G$ and $\beta \in S_G$ and S_G is a group, then by closure of S_G, we have $\alpha\beta \in S_G$, so $\alpha\beta$ is a permutation.

Hence, $\alpha\beta$ is a bijective function.

The composition of homomorphisms is a homomorphism.

Since α is a homomorphism and β is a homomorphism, then $\alpha\beta$ is a homomorphism.

Since $\alpha\beta$ is a bijective function and $\alpha\beta$ is a homomorphism, then $\alpha\beta$ is an isomorphism, so $\alpha\beta \in Aut(G)$.

Therefore, $Aut(G)$ is closed under function composition of S_G.

Let $id : G \to G$ be the identity element of S_G.

Then id is the identity map, so id is an isomorphism.

Hence, $id \in Aut(G)$, so $Aut(G)$ is closed under the identity of S_G.

Let $\alpha \in Aut(G)$.

Then $\alpha : G \to G$ is an isomorphism.

Since the isomorphism relation is an equivalence relation on the class of groups, then the isomorphism relation is symmetric.

Thus, for groups G and H, if $G \cong H$, then $H \cong G$.

Hence, if $\phi : G \to H$ is an isomorphism, then the inverse map $\phi^{-1} : H \to G$ is an isomorphism.

Since $\alpha : G \to G$ is an isomorphism, then we conclude the inverse map $\alpha^{-1} : G \to G$ is an isomorphism.

Therefore, $\alpha^{-1} \in Aut(G)$., so $Aut(G)$ is closed under taking inverses.

Since $Aut(G)$ is a subset of S_G and $Aut(G)$ is closed under function composition of S_G and $Aut(G)$ is closed under the identity of S_G and $Aut(G)$ is closed under inverses, then by the subgroup test, $Aut(G)$ is a subgroup of S_G. $\square$

Proposition 127. ***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.

Solution. We must prove i_g is an isomorphism of G with G.

Thus we must prove:

1) i_g is one to one.

To prove this we must show: $\forall a, b \in G. i_g(a) = i_g(b) \to a = b$.

2) i_g is onto. To prove this we must show: $\forall b \in G. \exists a \in G. i_g(a) = b$.

3) $(\forall a, b \in G)(i_g(a * b) = i_g(a) * i_g(b))$.

i_g is called an **inner automorphism**.

The set of all inner automorphisms of G is denoted $Inn(G)$. □

Proof. Since $g \in G$ and G is a group, then $g^{-1} \in G$.

Let $a, b \in G$.

Since G is closed under $*$ then $gag^{-1} \in G$ and $gbg^{-1} \in G$.

Suppose $i_g(a) = i_g(b)$.

Then $gag^{-1} = gbg^{-1}$.

By the left cancellation law of G, $ag^{-1} = bg^{-1}$.

By the right cancellation law of G, $a = b$.

Hence, $i_g(a) = i_g(b)$ implies $a = b$.

Since a, b are arbitrary then $i_g(a) = i_g(b)$ implies $a = b$ is true for all $a, b \in G$.

Therefore, i_g is one to one, by definition of injective function.

Suppose $b \in G$.

Since $g \in G$ by definition of group $g^{-1} \in G$.

Set $a = g^{-1}bg$.

Since G is closed under $*$, then $a \in G$.

Observe that

$$\begin{aligned} i_g(a) &= i_g(g^{-1}bg) \\ &= g(g^{-1}bg)g^{-1} \\ &= (gg^{-1})b(gg^{-1}) \\ &= ebe \\ &= b \end{aligned}$$

Thus, there exists $a \in G$ such that $i_g(a) = b$.

Since b is arbitrary then there exists $a \in G$ such that $i_g(a) = b$ for all $b \in G$.

Therefore, by definition of surjective function, i_g is onto.

Since i_g is one to one and onto, then i_g is a bijective map.

Let $a, b \in G$.

Observe that

$$\begin{aligned} i_g(a) * i_g(b) &= (g * a * g^{-1}) * (g * b * g^{-1}) \\ &= (g * a) * (g^{-1} * g) * (b * g^{-1}) \\ &= (g * a) * e * (b * g^{-1}) \\ &= (g * a) * (b * g^{-1}) \\ &= g * (a * b) * g^{-1} \\ &= i_g(a * b) \end{aligned}$$

Thus, $i_g(a) * i_g(b) = i_g(a * b)$.

Since a, b are arbitrary then $i_g(a) * i_g(b) = i_g(a * b)$ for all $a, b \in G$.

Therefore, by definition of isomorphism, $i_g : G \to G$ is an isomorphism. $\square$

Theorem 128. ***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.

Proof. Since ϕ is a group homomorphism, then $\phi(G) < G'$. Let e' be the identity of G'. Since K is the kernel of ϕ, then $K = \ker(\phi) = \{g \in G : \phi(g) = e'\}$. Since $K \lhd G$, then the quotient group $\frac{G}{K}$ exists.

Define binary relation $\psi : \frac{G}{K} \to \phi(G)$ by $\psi(gK) = \phi(g)$ for all $gK \in \frac{G}{K}$.

To prove ψ is an isomorphism, we must prove ψ is a function and ψ is a homomorphism and ψ is injective and ψ is surjective.

We prove the binary relation ψ is well defined. Let $aK, bK \in \frac{G}{K}$ such that $aK = bK$. Then $a, b \in G$. Since $aK = bK$ iff $a \in bK$, then $a \in bK$. Hence, $a = bk$ for some $k \in K$, by definition of bK. By definition of K, $k \in G$ and $\phi(k) = e'$. Observe that

$$\begin{aligned} \psi(aK) &= \phi(a) \\ &= \phi(bk) \\ &= \phi(b)\phi(k) \\ &= \phi(b)e' \\ &= \phi(b) \\ &= \psi(bK). \end{aligned}$$

Hence, $\psi(aK) = \psi(bK)$. Therefore, $aK = bK$ implies $\psi(aK) = \psi(bK)$. Thus, ψ is well defined, so ψ is a function from $\frac{G}{K}$ to $\phi(G)$.

Observe that

$$\begin{aligned} \psi((aK)(bK)) &= \psi((ab)K) \\ &= \phi(ab) \\ &= \phi(a)\phi(b) \\ &= \psi(aK)\psi(bK). \end{aligned}$$

Therefore, ψ is a homomorphism.

We prove ψ is injective. Let $aK, bK \in \frac{G}{K}$ such that $\psi(aK) = \psi(bK)$. Then $a, b \in G$ and $\phi(a) = \phi(b)$.

Observe that $\phi(a^{-1}b) = \phi(a^{-1})\phi(b) = \phi(a^{-1})\phi(a) = (\phi(a))^{-1}\phi(a) = e'$. Since $a^{-1}b \in G$ and $\phi(a^{-1}b) = e'$, then $a^{-1}b \in K$, by definition of K. Since $K < G$, then $a^{-1}b \in K$ iff $aK = bK$. Therefore, $aK = bK$.

Hence, $\psi(aK) = \psi(bK)$ implies $aK = bK$, so ψ is injective.

We prove ψ is surjective. Let $\phi(g) \in \phi(G)$. Then $g \in G$, by definition of $\phi(G)$. Thus, $gK \in \frac{G}{K}$. Observe that $\psi(gK) = \phi(g)$. Hence, there exists $gK \in \frac{G}{K}$ such that $\psi(gK) = \phi(G)$, so ψ is surjective.

Since ψ is injective and surjective, then ψ is bijective. Thus, ψ is a bijective homomorphism, so $\psi : \frac{G}{K} \to \phi(G)$ is an isomorphism. Hence, $\frac{G}{K} \cong \phi(G)$.

The composition of homomorphisms is a homomorphism. Since ψ is a homomorphism and η is the natural homomorphism from G onto $\frac{G}{K}$, then $\psi \circ \eta$ is a homomorphism. Hence, $\psi \circ \eta$ is a function. Observe that $\phi : G \to G'$ and $\psi \circ \eta : G \to G'$ have the same domain G and the same codomain G'.

Let $g \in G$. Then $(\psi \circ \eta)(g) = \psi(\eta(g)) = \psi(gK) = \phi(g)$. Since g is arbitrary, then $(\psi \circ \eta)(g) = \phi(g)$ for all $g \in G$.

Therefore, $\psi \circ \eta = \phi$. $\square$

Theorem 129. ***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 $\frac{H}{H \cap N} \cong \frac{HN}{N}$.

Solution. We must prove:

1. $HN < G$.
2. $N \lhd HN$.
3. $H \cap N \lhd H$.
4. $\frac{H}{H \cap N} \cong \frac{HN}{N}$.

$\square$

Proof. We first prove $HN < G$.

Let $x \in HN$. Then there exists $h \in H$ and $k \in N$ such that $x = hk$. Since $H < G$, then $H \subset G$. Since $h \in H$ and $H \subset G$, then $h \in G$. Since $N < G$, then $N \subset G$. Since $k \in N$ and $N \subset G$, then $k \in G$. Since G is a group, then G is closed under its binary operation. Thus, since $h, k \in G$, then $hk = x \in G$. Therefore, $x \in HN$ implies $x \in G$, so $HN \subset G$.

We apply a subgroup test.

Let e be the identity of G. Since $H < G$, then $e \in H$. Since $N < G$, then $e \in N$. Since $e = ee$, then $e \in HN$, by definition of HN. Therefore, $HN \neq \emptyset$.

Let $a, b \in HN$. Then there exist $h_1 \in H$ and $k_1 \in N$ such that $a = h_1k_1$ and there exist $h_2 \in H$ and $k_2 \in N$ such that $b = h_2k_2$, by definition of HN. Since $a, b \in HN$ and $HN \subset G$, then $a, b \in G$. Thus, $ab^{-1} = (h_1k_1)(h_2k_2)^{-1} = (h_1k_1)(k_2^{-1}h_2^{-1}) = h_1k_1k_2^{-1}h_2^{-1}$. Let $k = k_1k_2^{-1}$. Since N is a group, then $k \in N$ and $ab^{-1} = h_1kh_2^{-1}$.

Since $h_2 \in H$ and $H \subset G$, then $h_2 \in G$. Since $N \lhd G$, then for every $g \in G, h \in N, ghg^{-1} \in N$. Thus, in particular, if we let $g = h_2$ and $h = k$, then $h_2kh_2^{-1} \in N$. Let $k_3 = h_2kh_2^{-1}$. Then $k_3 \in N$ and $kh_2^{-1} = h_2^{-1}k_3$, so $ab^{-1} = h_1(h_2^{-1}k_3) = (h_1h_2^{-1})k_3$. Since H is a group, then H is closed under its binary operation. Therefore, since $h_1 \in H$ and $h_2^{-1} \in H$, then $h_1h_2^{-1} \in H$. Since $h_1h_2^{-1} \in H$ and $k_3 \in N$, then $ab^{-1} \in HN$, by definition of HN.

Therefore, HN is a subgroup of G.

We prove N is normal in HN. We first prove N is a subgroup of HN and then prove for every $g \in HN$ and $k \in N$, $gkg^{-1} \in N$.

Let $x \in N$. Then $x = ex$. Since $e \in H$ and $x \in N$, then $x \in HN$, by definition of HN. Thus, $x \in N$ implies $x \in HN$, so $N \subset HN$.

Since $N < G$, then $e \in N$, so $N \neq \emptyset$.

Let $a, b \in N$. Since N is a group, then $b^{-1} \in N$. Since N is closed under its binary operation, then $ab^{-1} \in N$.

Thus, N is a subgroup of HN.

Let $g \in HN$ and $k' \in N$. Then $g = hk$ for some $h \in H$ and $k \in N$. Observe that $gk'g^{-1} = (hk)k'(hk)^{-1} = hkk'k^{-1}h^{-1}$. Let $k'' = kk'k^{-1}$. Then $gk'g^{-1} = hk''h^{-1}$. Since $N \lhd G$, then $hk''h^{-1} \in N$, so $gk'g^{-1} \in N$. Therefore, N is a normal subgroup of HN.

Since N is normal in HN, then the quotient group $\frac{HN}{N}$ exists.

Let $\frac{HN}{N}$ be the set of all cosets of N in HN. Then $\frac{HN}{N} = \{aN : a \in HN\} = \{hnN : h \in H, n \in N\} = \{hN : h \in H\}$.

Define binary relation $\phi : H \mapsto \frac{HN}{N}$ by $\phi(h) = hN$ for all $h \in H$.

We prove ϕ is well defined. Let $h_1, h_2 \in H$ such that $h_1 = h_2$. Then $h_1N = h_2N$. Thus, $\phi(h_1) = h_1N = h_2N = \phi(h_2)$. Hence, $h_1 = h_2$ implies $\phi(h_1) = \phi(h_2)$, so ϕ is well defined. Therefore, ϕ is a function.

Let $y \in \frac{HN}{N}$. Then there exists $h \in H$ such that $y = hN$, by definition of $\frac{HN}{N}$. Thus, $\phi(h) = hN = y$, so there exists $h \in H$ such that $\phi(h) = y$. Hence, ϕ is surjective. Therefore, $\phi(H) = \frac{HN}{N}$.

Let $a, b \in H$. Then $\phi(ab) = (ab)N = (aN)(bN) = \phi(a)\phi(b)$. Thus, ϕ is a homomorphism.

We prove $\ker(\phi) = H \cap N$. Let $x \in \ker(\phi)$. Then $x \in H$ and $\phi(x) = N$, by definition of kernel of ϕ. Thus, $N = \phi(x) = xN$. Since $xN = N$ iff $x \in N$, then $x \in N$. Thus $x \in H$ and $x \in N$, so $x \in H \cap N$. Hence, $x \in \ker(\phi)$ implies $x \in H \cap N$, so $\ker(\phi) \subset H \cap N$.

Let $y \in H \cap N$. Then $y \in H$ and $y \in N$. Since $y \in H$ and $H \subset G$, then $y \in G$. Since $y \in N$ iff $yN = N$, then $yN = N$. Thus, $\phi(y) = yN = N$. Since $y \in H$ and $\phi(y) = N$, then $y \in \ker(\phi)$. Hence, $y \in H \cap N$ implies $y \in \ker(\phi)$, so $H \cap N \subset \ker(\phi)$.

Since $\ker(\phi) \subset H \cap N$ and $H \cap N \subset \ker(\phi)$, then $\ker(\phi) = H \cap N$. The kernel of ϕ is normal in H, so $H \cap N \lhd H$.

Hence, $\phi : H \mapsto \frac{HN}{N}$ is a homomorphism with kernel $H \cap N$ and $\phi(H) = \frac{HN}{N}$. Thus, by the first isomorphism theorem, $\frac{H}{H \cap N} \cong \frac{HN}{N}$. $\square$