Modern Algebra I

Lecture 1

Jung-Chen Liu

liujc@math.ntnu.edu.tw

2009, Fall

Text Book:

Text Book: Algebra

Text Book: Algebra

Author: Thomas W. Hungerford

Text Book: Algebra

Author: Thomas W. Hungerford

Publisher: Springer

Chapter I: Groups

Chapter I: Groups

Section I.1: Semigroups, Monoids, and Groups

Chapter I: Groups

Section I.1: Semigroups, Monoids, and Groups

Definition. Let G be a nonempty set.

Chapter I: Groups

Section I.1: Semigroups, Monoids, and Groups

Definition. Let G be a nonempty set. A **binary operation on** G is a function $G \times G \to G$.

Chapter I: Groups

Section I.1: Semigroups, Monoids, and Groups

Definition. Let G be a nonempty set. A **binary operation on G** is a function $G \times G \to G$.

Remark. There are several commonly used notations for the image of (a, b) under a binary operation:

Chapter I: Groups

Section I.1: Semigroups, Monoids, and Groups

Definition. Let G be a nonempty set. A **binary operation on** G is a function $G \times G \to G$.

Remark. There are several commonly used notations for the image of (a, b) under a binary operation:

$$\begin{array}{ccc} G \times G & \longrightarrow & G \\ (a, b) & \longmapsto & ?? \end{array}$$

Chapter I: Groups

Section I.1: Semigroups, Monoids, and Groups

Definition. Let G be a nonempty set. A **binary operation on** G is a function $G \times G \to G$.

Remark. There are several commonly used notations for the image of (a, b) under a binary operation:

$$\begin{array}{ccc} G \times G & \longrightarrow & G \\ (a, b) & \longmapsto & a * b \end{array}$$

Chapter I: Groups

Section I.1: Semigroups, Monoids, and Groups

Definition. Let G be a nonempty set. A **binary operation on** G is a function $G \times G \to G$.

Remark. There are several commonly used notations for the image of (a, b) under a binary operation:

$$\begin{array}{ccc} G \times G & \longrightarrow & G \\ (a, b) & \longmapsto & a \cdot b \end{array}$$

Chapter I: Groups

Section I.1: Semigroups, Monoids, and Groups

Definition. Let G be a nonempty set. A **binary operation on G** is a function $G \times G \to G$.

Remark. There are several commonly used notations for the image of (a, b) under a binary operation:

$$\begin{array}{ccc} G \times G & \longrightarrow & G \\ (a, b) & \longmapsto & ab \end{array}$$

Chapter I: Groups

Section I.1: Semigroups, Monoids, and Groups

Definition. Let G be a nonempty set. A **binary operation on** G is a function $G \times G \to G$.

Remark. There are several commonly used notations for the image of (a, b) under a binary operation:

$$\begin{array}{ccc} G \times G & \longrightarrow & G \\ (a, b) & \longmapsto & ab \text{ (multiplicative notation)} \end{array}$$

Chapter I: Groups

Section I.1: Semigroups, Monoids, and Groups

Definition. Let G be a nonempty set. A **binary operation on G** is a function $G \times G \to G$.

Remark. There are several commonly used notations for the image of (a, b) under a binary operation:

$$\begin{array}{ccc} G \times G & \longrightarrow & G \\ (a, b) & \longmapsto & a + b \end{array}$$

Chapter I: Groups

Section I.1: Semigroups, Monoids, and Groups

Definition. Let G be a nonempty set. A **binary operation on** G is a function $G \times G \to G$.

Remark. There are several commonly used notations for the image of (a, b) under a binary operation:

$$\begin{array}{ccc} G \times G & \longrightarrow & G \\ (a, b) & \longmapsto & a + b \text{ (additive notation)} \end{array}$$

Chapter I: Groups

Section I.1: Semigroups, Monoids, and Groups

Definition. Let G be a nonempty set. A **binary operation on G** is a function $G \times G \to G$.

Remark. There are several commonly used notations for the image of (a, b) under a binary operation:

$$\begin{array}{ccc} G \times G & \longrightarrow & G \\ (a, b) & \longmapsto & ab \end{array}$$

We usually use the multiplicative notation

Chapter I: Groups

Section I.1: Semigroups, Monoids, and Groups

Definition. Let G be a nonempty set. A **binary operation on** G is a function $G \times G \to G$.

Remark. There are several commonly used notations for the image of (a, b) under a binary operation:

$$\begin{array}{ccc} G \times G & \longrightarrow & G \\ (a, b) & \longmapsto & ab \end{array}$$

We usually use the multiplicative notation and refer to ab as the **product** of a and b.

Definition (1.1)

Definition (1.1)

Let G be a nonempty set together with a binary operation on G,

Definition (1.1)

Let G be a nonempty set together with a binary operation on G, i.e., $\forall a, b \in G$, $ab \in G$.

Definition (1.1)

Let G be a nonempty set together with a binary operation on G, i.e., $\forall a, b \in G$, $ab \in G$.

- G is a semigroup

Definition (1.1)

Let G be a nonempty set together with a binary operation on G, i.e., $\forall a, b \in G$, $ab \in G$.

- G is a semigroup if its binary operation is associative,

Definition (1.1)

Let G be a nonempty set together with a binary operation on G, i.e., $\forall a, b \in G$, $ab \in G$.

- G is a semigroup if its binary operation is associative, i.e., $\forall a, b, c \in G$, $(ab)c = a(bc)$.

Definition (1.1)

Let G be a nonempty set together with a binary operation on G, i.e., $\forall a, b \in G$, $ab \in G$.

- G is a semigroup if its binary operation is associative, i.e., $\forall a, b, c \in G$, $(ab)c = a(bc)$.
- G is a monoid

Definition (1.1)

Let G be a nonempty set together with a binary operation on G, i.e., $\forall a, b \in G$, $ab \in G$.

- G is a semigroup if its binary operation is associative, i.e., $\forall a, b, c \in G$, $(ab)c = a(bc)$.
- G is a monoid if it is a semigroup and

Definition (1.1)

Let G be a nonempty set together with a binary operation on G, i.e., $\forall a, b \in G$, $ab \in G$.

- G is a semigroup if its binary operation is associative, i.e., $\forall a, b, c \in G$, $(ab)c = a(bc)$.
- G is a monoid if it is a semigroup and it contains an identity element,

Definition (1.1)

Let G be a nonempty set together with a binary operation on G, i.e., $\forall a, b \in G$, $ab \in G$.

- G is a semigroup if its binary operation is associative, i.e., $\forall a, b, c \in G$, $(ab)c = a(bc)$.
- G is a monoid if it is a semigroup and it contains an identity element, i.e., $\exists e \in G$ such that $ae = ea = a \; \forall a \in G$.

Definition (1.1)

Let G be a nonempty set together with a binary operation on G, i.e., $\forall a, b \in G$, $ab \in G$.

- G is a semigroup if its binary operation is associative, i.e., $\forall a, b, c \in G$, $(ab)c = a(bc)$.
- G is a monoid if it is a semigroup and it contains an identity element, i.e., $\exists e \in G$ such that $ae = ea = a \; \forall a \in G$.
- G is a group

Definition (1.1)

Let G be a nonempty set together with a binary operation on G, i.e., $\forall a, b \in G$, $ab \in G$.

- G is a semigroup if its binary operation is associative, i.e., $\forall a, b, c \in G$, $(ab)c = a(bc)$.
- G is a monoid if it is a semigroup and it contains an identity element, i.e., $\exists e \in G$ such that $ae = ea = a \; \forall a \in G$.
- G is a group if it is a monoid and

Definition (1.1)

Let G be a nonempty set together with a binary operation on G, i.e., $\forall a, b \in G$, $ab \in G$.

- G is a semigroup if its binary operation is associative, i.e., $\forall a, b, c \in G$, $(ab)c = a(bc)$.
- G is a monoid if it is a semigroup and it contains an identity element, i.e., $\exists e \in G$ such that $ae = ea = a \; \forall a \in G$.
- G is a group if it is a monoid and every element in G has an inverse element,

Definition (1.1)

Let G be a nonempty set together with a binary operation on G, i.e., $\forall a, b \in G$, $ab \in G$.

- G is a semigroup if its binary operation is associative, i.e., $\forall a, b, c \in G$, $(ab)c = a(bc)$.
- G is a monoid if it is a semigroup and it contains an identity element, i.e., $\exists e \in G$ such that $ae = ea = a \; \forall a \in G$.
- G is a group if it is a monoid and every element in G has an inverse element, i.e., $\forall a \in G$, $\exists a^{-1} \in G$ such that $aa^{-1} = a^{-1}a = e$.

Definition (1.1)

Let G be a nonempty set together with a binary operation on G, i.e., $\forall a, b \in G$, $ab \in G$.

- G is a semigroup if its binary operation is associative, i.e., $\forall a, b, c \in G$, $(ab)c = a(bc)$.
- G is a monoid if it is a semigroup and it contains an identity element, i.e., $\exists e \in G$ such that $ae = ea = a \; \forall a \in G$.
- G is a group if it is a monoid and every element in G has an inverse element, i.e., $\forall a \in G$, $\exists a^{-1} \in G$ such that $aa^{-1} = a^{-1}a = e$.
- A semigroup G is said to be abelian or commutative

Definition (1.1)

Let G be a nonempty set together with a binary operation on G, i.e., $\forall a, b \in G$, $ab \in G$.

- G is a semigroup if its binary operation is associative, i.e., $\forall a, b, c \in G$, $(ab)c = a(bc)$.
- G is a monoid if it is a semigroup and it contains an identity element, i.e., $\exists e \in G$ such that $ae = ea = a \; \forall a \in G$.
- G is a group if it is a monoid and every element in G has an inverse element, i.e., $\forall a \in G$, $\exists a^{-1} \in G$ such that $aa^{-1} = a^{-1}a = e$.
- A semigroup G is said to be abelian or commutative if its binary operation is commutative,

Definition (1.1)

Let G be a nonempty set together with a binary operation on G, i.e., $\forall a, b \in G$, $ab \in G$.

- G is a semigroup if its binary operation is associative, i.e., $\forall a, b, c \in G$, $(ab)c = a(bc)$.
- G is a monoid if it is a semigroup and it contains an identity element, i.e., $\exists e \in G$ such that $ae = ea = a \; \forall a \in G$.
- G is a group if it is a monoid and every element in G has an inverse element, i.e., $\forall a \in G$, $\exists a^{-1} \in G$ such that $aa^{-1} = a^{-1}a = e$.
- A semigroup G is said to be abelian or commutative if its binary operation is commutative, i.e., $\forall a, b \in G$, $ab = ba$.

Definition (1.1)

Let G be a nonempty set together with a binary operation on G, i.e., $\forall a, b \in G$, $ab \in G$.

- G is a semigroup if its binary operation is associative, i.e., $\forall a, b, c \in G$, $(ab)c = a(bc)$.
- G is a monoid if it is a semigroup and it contains an identity element, i.e., $\exists e \in G$ such that $ae = ea = a \; \forall a \in G$.
- G is a group if it is a monoid and every element in G has an inverse element, i.e., $\forall a \in G$, $\exists a^{-1} \in G$ such that $aa^{-1} = a^{-1}a = e$.
- A semigroup G is said to be abelian or commutative if its binary operation is commutative, i.e., $\forall a, b \in G$, $ab = ba$.
- The order of a group G is the cardinal number $|G|$.

Definition (1.1)

Let G be a nonempty set together with a binary operation on G, i.e., $\forall a, b \in G$, $ab \in G$.

- G is a semigroup if its binary operation is associative, i.e., $\forall a, b, c \in G$, $(ab)c = a(bc)$.
- G is a monoid if it is a semigroup and it contains an identity element, i.e., $\exists e \in G$ such that $ae = ea = a \; \forall a \in G$.
- G is a group if it is a monoid and every element in G has an inverse element, i.e., $\forall a \in G$, $\exists a^{-1} \in G$ such that $aa^{-1} = a^{-1}a = e$.
- A semigroup G is said to be abelian or commutative if its binary operation is commutative, i.e., $\forall a, b \in G$, $ab = ba$.
- The order of a group G is the cardinal number $|G|$. G is finite if $|G|$ is finite;

Definition (1.1)

Let G be a nonempty set together with a binary operation on G, i.e., $\forall a, b \in G$, $ab \in G$.

- G is a semigroup if its binary operation is associative, i.e., $\forall a, b, c \in G$, $(ab)c = a(bc)$.
- G is a monoid if it is a semigroup and it contains an identity element, i.e., $\exists e \in G$ such that $ae = ea = a \; \forall a \in G$.
- G is a group if it is a monoid and every element in G has an inverse element, i.e., $\forall a \in G$, $\exists a^{-1} \in G$ such that $aa^{-1} = a^{-1}a = e$.
- A semigroup G is said to be abelian or commutative if its binary operation is commutative, i.e., $\forall a, b \in G$, $ab = ba$.
- The order of a group G is the cardinal number $|G|$. G is finite if $|G|$ is finite; otherwise, G is infinite.

Theorem (1.2)

Theorem (1.2)

If G is a monoid,

Theorem (1.2)

If G is a monoid, then the identity element e is unique.

Theorem (1.2)

If G is a monoid, then the identity element e is unique.

Proof. If e_1 and e_2 are both identities,

Theorem (1.2)

If G is a monoid, then the identity element e is unique.

Proof. If e_1 and e_2 are both identities, then $e_1 = e_1 e_2 = e_2$.

Theorem (1.2)

If G is a monoid, then the identity element e is unique.

Proof. If e_1 and e_2 are both identities, then $e_1 = e_1 e_2 = e_2$.

because e_2 is an identity

Theorem (1.2)

If G is a monoid, then the identity element e is unique.

Proof. If e_1 and e_2 are both identities, then $e_1 = e_1 e_2 = e_2$.

because e_1 is an identity

Theorem (1.2)

If G is a monoid, then the identity element e is unique.

Furthermore, if G is a group, then

Theorem (1.2)

If G is a monoid, then the identity element e is unique.

Furthermore, if G is a group, then

- $\forall a \in G$, the inverse element a^{-1} is unique.

Theorem (1.2)

If G is a monoid, then the identity element e is unique.

Furthermore, if G is a group, then

- $\forall a \in G$, the inverse element a^{-1} is unique.

Proof. If a_1 and a_2 are both inverses of a,

Theorem (1.2)

If G is a monoid, then the identity element e is unique.

Furthermore, if G is a group, then

- $\forall a \in G$, the inverse element a^{-1} is unique.

Proof. If a_1 and a_2 are both inverses of a, i.e., $aa_1 = a_1a = e$

Theorem (1.2)

If G is a monoid, then the identity element e is unique.

Furthermore, if G is a group, then

- $\forall a \in G$, the inverse element a^{-1} is unique.

Proof. If a_1 and a_2 are both inverses of a, i.e., $aa_1 = a_1a = e$ and $aa_2 = a_2a = e$,

Theorem (1.2)

If G is a monoid, then the identity element e is unique.

Furthermore, if G is a group, then

- $\forall a \in G$, the inverse element a^{-1} is unique.

Proof. If a_1 and a_2 are both inverses of a, i.e., $aa_1 = a_1a = e$ and $aa_2 = a_2a = e$, then

Theorem (1.2)

If G is a monoid, then the identity element e is unique.

Furthermore, if G is a group, then

- $\forall a \in G$, the inverse element a^{-1} is unique.

Proof. If a_1 and a_2 are both inverses of a, i.e., $aa_1 = a_1a = e$ and $aa_2 = a_2a = e$, then

$$a_1$$

Theorem (1.2)

If G is a monoid, then the identity element e is unique.

Furthermore, if G is a group, then

- $\forall a \in G$, the inverse element a^{-1} is unique.

Proof. If a_1 and a_2 are both inverses of a, i.e., $aa_1 = a_1a = e$ and $aa_2 = a_2a = e$, then

$$a_1 = a_1e$$

Theorem (1.2)

If G is a monoid, then the identity element e is unique.

Furthermore, if G is a group, then

- $\forall a \in G$, the inverse element a^{-1} is unique.

Proof. If a_1 and a_2 are both inverses of a, i.e., $aa_1 = a_1a = e$ and $aa_2 = a_2a = e$, then

$$a_1 = a_1e = a_1(aa_2)$$

Theorem (1.2)

If G is a monoid, then the identity element e is unique.

Furthermore, if G is a group, then

- $\forall a \in G$, the inverse element a^{-1} is unique.

Proof. If a_1 and a_2 are both inverses of a, i.e., $aa_1 = a_1a = e$ and $aa_2 = a_2a = e$, then

$$a_1 = a_1e = a_1(aa_2) = (a_1a)a_2$$

Theorem (1.2)

If G is a monoid, then the identity element e is unique.

Furthermore, if G is a group, then

- $\forall a \in G$, the inverse element a^{-1} is unique.

Proof. If a_1 and a_2 are both inverses of a, i.e., $aa_1 = a_1a = e$ and $aa_2 = a_2a = e$, then

$$a_1 = a_1e = a_1(aa_2) = (a_1a)a_2 = ea_2$$

Theorem (1.2)

If G is a monoid, then the identity element e is unique.

Furthermore, if G is a group, then

- $\forall a \in G$, the inverse element a^{-1} is unique.

Proof. If a_1 and a_2 are both inverses of a, i.e., $aa_1 = a_1a = e$ and $aa_2 = a_2a = e$, then

$$a_1 = a_1e = a_1(aa_2) = (a_1a)a_2 = ea_2 = a_2.$$

Theorem (1.2)

If G is a monoid, then the identity element e is unique.

Furthermore, if G is a group, then

- $\forall a \in G$, the inverse element a^{-1} is unique.
- $\forall a \in G$, $(a^{-1})^{-1} = a$.

Theorem (1.2)

If G is a monoid, then the identity element e is unique.

Furthermore, if G is a group, then

- $\forall a \in G$, the inverse element a^{-1} is unique.
- $\forall a \in G$, $(a^{-1})^{-1} = a$.

Proof. We need to show that

Theorem (1.2)

If G is a monoid, then the identity element e is unique.

Furthermore, if G is a group, then

- $\forall a \in G$, the inverse element a^{-1} is unique.
- $\forall a \in G$, $(a^{-1})^{-1} = a$.

Proof. We need to show that a is the inverse of a^{-1},

Theorem (1.2)

If G is a monoid, then the identity element e is unique.

Furthermore, if G is a group, then

- $\forall a \in G$, the inverse element a^{-1} is unique.
- $\forall a \in G$, $(a^{-1})^{-1} = a$.

Proof. We need to show that a is the inverse of a^{-1}, i.e., $a^{-1}a = aa^{-1} = e$.

Theorem (1.2)

If G is a monoid, then the identity element e is unique.

Furthermore, if G is a group, then

- $\forall a \in G$, the inverse element a^{-1} is unique.
- $\forall a \in G$, $(a^{-1})^{-1} = a$.

Proof. We need to show that a is the inverse of a^{-1}, i.e., $a^{-1}a = aa^{-1} = e$. However, this is clearly true.

Theorem (1.2)

If G is a monoid, then the identity element e is unique.

Furthermore, if G is a group, then

- $\forall a \in G$, the inverse element a^{-1} is unique.
- $\forall a \in G$, $(a^{-1})^{-1} = a$.
- $\forall a, b \in G$, $(ab)^{-1} = b^{-1}a^{-1}$.

Theorem (1.2)

If G is a monoid, then the identity element e is unique.

Furthermore, if G is a group, then

- $\forall a \in G$, the inverse element a^{-1} is unique.
- $\forall a \in G$, $(a^{-1})^{-1} = a$.
- $\forall a, b \in G$, $(ab)^{-1} = b^{-1}a^{-1}$.

Proof. As above, we only need to show that

Theorem (1.2)

If G is a monoid, then the identity element e is unique.

Furthermore, if G is a group, then

- $\forall a \in G$, the inverse element a^{-1} is unique.
- $\forall a \in G$, $(a^{-1})^{-1} = a$.
- $\forall a, b \in G$, $(ab)^{-1} = b^{-1}a^{-1}$.

Proof. As above, we only need to show that

$$(b^{-1}a^{-1})(ab) = (ab)(b^{-1}a^{-1}) = e.$$

Theorem (1.2)

If G is a monoid, then the identity element e is unique.

Furthermore, if G is a group, then

- $\forall a \in G$, the inverse element a^{-1} is unique.
- $\forall a \in G$, $(a^{-1})^{-1} = a$.
- $\forall a, b \in G$, $(ab)^{-1} = b^{-1}a^{-1}$.

Proof. As above, we only need to show that

$$(b^{-1}a^{-1})(ab) = (ab)(b^{-1}a^{-1}) = e.$$

However, we have

Theorem (1.2)

If G is a monoid, then the identity element e is unique.

Furthermore, if G is a group, then

- $\forall a \in G$, the inverse element a^{-1} is unique.
- $\forall a \in G$, $(a^{-1})^{-1} = a$.
- $\forall a, b \in G$, $(ab)^{-1} = b^{-1}a^{-1}$.

Proof. As above, we only need to show that

$$(b^{-1}a^{-1})(ab) = (ab)(b^{-1}a^{-1}) = e.$$

However, we have

$$(b^{-1}a^{-1})(ab)$$

Theorem (1.2)

If G is a monoid, then the identity element e is unique.

Furthermore, if G is a group, then

- $\forall a \in G$, the inverse element a^{-1} is unique.
- $\forall a \in G$, $(a^{-1})^{-1} = a$.
- $\forall a, b \in G$, $(ab)^{-1} = b^{-1}a^{-1}$.

Proof. As above, we only need to show that

$$(b^{-1}a^{-1})(ab) = (ab)(b^{-1}a^{-1}) = e.$$

However, we have

$$(b^{-1}a^{-1})(ab) = b^{-1}(a^{-1}a)b$$

Theorem (1.2)

If G is a monoid, then the identity element e is unique.

Furthermore, if G is a group, then

- $\forall a \in G$, the inverse element a^{-1} is unique.
- $\forall a \in G$, $(a^{-1})^{-1} = a$.
- $\forall a, b \in G$, $(ab)^{-1} = b^{-1}a^{-1}$.

Proof. As above, we only need to show that

$$(b^{-1}a^{-1})(ab) = (ab)(b^{-1}a^{-1}) = e.$$

However, we have

$$(b^{-1}a^{-1})(ab) = b^{-1}(a^{-1}a)b = b^{-1}eb$$

Theorem (1.2)

If G is a monoid, then the identity element e is unique.

Furthermore, if G is a group, then

- $\forall a \in G$, the inverse element a^{-1} is unique.
- $\forall a \in G$, $(a^{-1})^{-1} = a$.
- $\forall a, b \in G$, $(ab)^{-1} = b^{-1}a^{-1}$.

Proof. As above, we only need to show that

$$(b^{-1}a^{-1})(ab) = (ab)(b^{-1}a^{-1}) = e.$$

However, we have

$$(b^{-1}a^{-1})(ab) = b^{-1}(a^{-1}a)b = b^{-1}eb = b^{-1}b$$

Theorem (1.2)

If G is a monoid, then the identity element e is unique.

Furthermore, if G is a group, then

- $\forall a \in G$, the inverse element a^{-1} is unique.
- $\forall a \in G$, $(a^{-1})^{-1} = a$.
- $\forall a, b \in G$, $(ab)^{-1} = b^{-1}a^{-1}$.

Proof. As above, we only need to show that

$$(b^{-1}a^{-1})(ab) = (ab)(b^{-1}a^{-1}) = e.$$

However, we have

$$(b^{-1}a^{-1})(ab) = b^{-1}(a^{-1}a)b = b^{-1}eb = b^{-1}b = e,$$

Theorem (1.2)

If G is a monoid, then the identity element e is unique.

Furthermore, if G is a group, then

- $\forall a \in G$, the inverse element a^{-1} is unique.
- $\forall a \in G$, $(a^{-1})^{-1} = a$.
- $\forall a, b \in G$, $(ab)^{-1} = b^{-1}a^{-1}$.

Proof. As above, we only need to show that

$$(b^{-1}a^{-1})(ab) = (ab)(b^{-1}a^{-1}) = e.$$

However, we have

$$(b^{-1}a^{-1})(ab) = b^{-1}(a^{-1}a)b = b^{-1}eb = b^{-1}b = e,$$

and

Theorem (1.2)

If G is a monoid, then the identity element e is unique.

Furthermore, if G is a group, then

- $\forall a \in G$, the inverse element a^{-1} is unique.
- $\forall a \in G$, $(a^{-1})^{-1} = a$.
- $\forall a, b \in G$, $(ab)^{-1} = b^{-1}a^{-1}$.

Proof. As above, we only need to show that

$$(b^{-1}a^{-1})(ab) = (ab)(b^{-1}a^{-1}) = e.$$

However, we have

$$(b^{-1}a^{-1})(ab) = b^{-1}(a^{-1}a)b = b^{-1}eb = b^{-1}b = e,$$

and

$$(ab)(b^{-1}a^{-1})$$

Theorem (1.2)

If G is a monoid, then the identity element e is unique.

Furthermore, if G is a group, then

- $\forall a \in G$, the inverse element a^{-1} is unique.
- $\forall a \in G$, $(a^{-1})^{-1} = a$.
- $\forall a, b \in G$, $(ab)^{-1} = b^{-1}a^{-1}$.

Proof. As above, we only need to show that

$$(b^{-1}a^{-1})(ab) = (ab)(b^{-1}a^{-1}) = e.$$

However, we have

$$(b^{-1}a^{-1})(ab) = b^{-1}(a^{-1}a)b = b^{-1}eb = b^{-1}b = e,$$

and

$$(ab)(b^{-1}a^{-1}) = a^{-1}(b^{-1}b)a$$

Theorem (1.2)

If G is a monoid, then the identity element e is unique.

Furthermore, if G is a group, then

- $\forall a \in G$, the inverse element a^{-1} is unique.
- $\forall a \in G$, $(a^{-1})^{-1} = a$.
- $\forall a, b \in G$, $(ab)^{-1} = b^{-1}a^{-1}$.

Proof. As above, we only need to show that

$$(b^{-1}a^{-1})(ab) = (ab)(b^{-1}a^{-1}) = e.$$

However, we have

$$(b^{-1}a^{-1})(ab) = b^{-1}(a^{-1}a)b = b^{-1}eb = b^{-1}b = e,$$

and

$$(ab)(b^{-1}a^{-1}) = a^{-1}(b^{-1}b)a = a^{-1}ea$$

Theorem (1.2)

If G is a monoid, then the identity element e is unique.

Furthermore, if G is a group, then

- $\forall a \in G$, the inverse element a^{-1} is unique.
- $\forall a \in G$, $(a^{-1})^{-1} = a$.
- $\forall a, b \in G$, $(ab)^{-1} = b^{-1}a^{-1}$.

Proof. As above, we only need to show that

$$(b^{-1}a^{-1})(ab) = (ab)(b^{-1}a^{-1}) = e.$$

However, we have

$$(b^{-1}a^{-1})(ab) = b^{-1}(a^{-1}a)b = b^{-1}eb = b^{-1}b = e,$$

and

$$(ab)(b^{-1}a^{-1}) = a^{-1}(b^{-1}b)a = a^{-1}ea = a^{-1}a$$

Theorem (1.2)

If G is a monoid, then the identity element e is unique.

Furthermore, if G is a group, then

- $\forall a \in G$, the inverse element a^{-1} is unique.
- $\forall a \in G$, $(a^{-1})^{-1} = a$.
- $\forall a, b \in G$, $(ab)^{-1} = b^{-1}a^{-1}$.

Proof. As above, we only need to show that

$$(b^{-1}a^{-1})(ab) = (ab)(b^{-1}a^{-1}) = e.$$

However, we have

$$(b^{-1}a^{-1})(ab) = b^{-1}(a^{-1}a)b = b^{-1}eb = b^{-1}b = e,$$

and

$$(ab)(b^{-1}a^{-1}) = a^{-1}(b^{-1}b)a = a^{-1}ea = a^{-1}a = e.$$

Theorem (1.2)

If G is a monoid, then the identity element e is unique.

Furthermore, if G is a group, then

- $\forall a \in G$, the inverse element a^{-1} is unique.
- $\forall a \in G$, $(a^{-1})^{-1} = a$.
- $\forall a, b \in G$, $(ab)^{-1} = b^{-1}a^{-1}$.
- $c \in G$ and $cc = c$

Theorem (1.2)

If G is a monoid, then the identity element e is unique.

Furthermore, if G is a group, then

- $\forall a \in G$, the inverse element a^{-1} is unique.
- $\forall a \in G$, $(a^{-1})^{-1} = a$.
- $\forall a, b \in G$, $(ab)^{-1} = b^{-1}a^{-1}$.
- $c \in G$ and $cc = c \implies c = e$.

Theorem (1.2)

If G is a monoid, then the identity element e is unique.

Furthermore, if G is a group, then

- $\forall a \in G$, the inverse element a^{-1} is unique.
- $\forall a \in G$, $(a^{-1})^{-1} = a$.
- $\forall a, b \in G$, $(ab)^{-1} = b^{-1}a^{-1}$.
- $c \in G$ and $cc = c \implies c = e$.

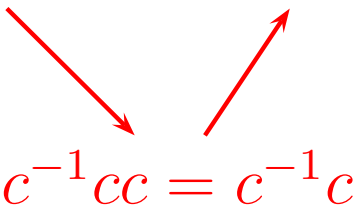
$$c^{-1}cc = c^{-1}c$$

Theorem (1.2)

If G is a monoid, then the identity element e is unique.

Furthermore, if G is a group, then

- $\forall a \in G$, the inverse element a^{-1} is unique.
- $\forall a \in G$, $(a^{-1})^{-1} = a$.
- $\forall a, b \in G$, $(ab)^{-1} = b^{-1}a^{-1}$.
- $c \in G$ and $cc = c \implies c = e$.



Theorem (1.2)

If G is a monoid, then the identity element e is unique.

Furthermore, if G is a group, then

- $\forall a \in G$, the inverse element a^{-1} is unique.
- $\forall a \in G$, $(a^{-1})^{-1} = a$.
- $\forall a, b \in G$, $(ab)^{-1} = b^{-1}a^{-1}$.
- $c \in G$ and $cc = c \implies c = e$.
- $\forall a, b, c \in G$,

Theorem (1.2)

If G is a monoid, then the identity element e is unique.

Furthermore, if G is a group, then

- $\forall a \in G$, the inverse element a^{-1} is unique.
- $\forall a \in G$, $(a^{-1})^{-1} = a$.
- $\forall a, b \in G$, $(ab)^{-1} = b^{-1}a^{-1}$.
- $c \in G$ and $cc = c \implies c = e$.
- $\forall a, b, c \in G$, $ab = ac$

Theorem (1.2)

If G is a monoid, then the identity element e is unique.

Furthermore, if G is a group, then

- $\forall a \in G$, the inverse element a^{-1} is unique.
- $\forall a \in G$, $(a^{-1})^{-1} = a$.
- $\forall a, b \in G$, $(ab)^{-1} = b^{-1}a^{-1}$.
- $c \in G$ and $cc = c \implies c = e$.
- $\forall a, b, c \in G$, $ab = ac \implies b = c$

Theorem (1.2)

If G is a monoid, then the identity element e is unique.

Furthermore, if G is a group, then

- $\forall a \in G$, the inverse element a^{-1} is unique.
- $\forall a \in G$, $(a^{-1})^{-1} = a$.
- $\forall a, b \in G$, $(ab)^{-1} = b^{-1}a^{-1}$.
- $c \in G$ and $cc = c \implies c = e$.
- $\forall a, b, c \in G$, $ab = ac \implies b = c$ (left cancelation)

Theorem (1.2)

If G is a monoid, then the identity element e is unique.

Furthermore, if G is a group, then

- $\forall a \in G$, the inverse element a^{-1} is unique.
- $\forall a \in G$, $(a^{-1})^{-1} = a$.
- $\forall a, b \in G$, $(ab)^{-1} = b^{-1}a^{-1}$.
- $c \in G$ and $cc = c \implies c = e$.
- $\forall a, b, c \in G$, $ab = ac \implies b = c$ (left cancelation)

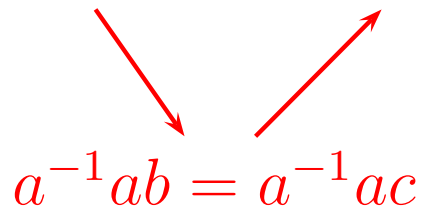
$a^{-1}ab = a^{-1}ac$

Theorem (1.2)

If G is a monoid, then the identity element e is unique.

Furthermore, if G is a group, then

- $\forall a \in G$, the inverse element a^{-1} is unique.
- $\forall a \in G$, $(a^{-1})^{-1} = a$.
- $\forall a, b \in G$, $(ab)^{-1} = b^{-1}a^{-1}$.
- $c \in G$ and $cc = c \implies c = e$.
- $\forall a, b, c \in G$, $ab = ac \implies b = c$ (left cancelation)



Theorem (1.2)

If G is a monoid, then the identity element e is unique.

Furthermore, if G is a group, then

- $\forall a \in G$, the inverse element a^{-1} is unique.
- $\forall a \in G$, $(a^{-1})^{-1} = a$.
- $\forall a, b \in G$, $(ab)^{-1} = b^{-1}a^{-1}$.
- $c \in G$ and $cc = c \implies c = e$.
- $\forall a, b, c \in G$, $ab = ac \implies b = c$ (left cancelation)
  $ba = ca \implies b = c$ (right cancelation).

Theorem (1.2)

If G is a monoid, then the identity element e is unique.

Furthermore, if G is a group, then

- $\forall a \in G$, the inverse element a^{-1} is unique.
- $\forall a \in G$, $(a^{-1})^{-1} = a$.
- $\forall a, b \in G$, $(ab)^{-1} = b^{-1}a^{-1}$.
- $c \in G$ and $cc = c \implies c = e$.
- $\forall a, b, c \in G$, $ab = ac \implies b = c$ (left cancelation)
  $ba = ca \implies b = c$ (right cancelation).

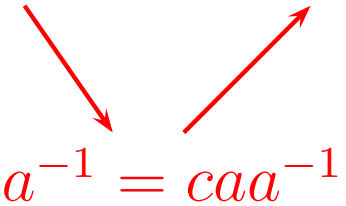
$baa^{-1} = caa^{-1}$

Theorem (1.2)

If G is a monoid, then the identity element e is unique.

Furthermore, if G is a group, then

- $\forall a \in G$, the inverse element a^{-1} is unique.
- $\forall a \in G$, $(a^{-1})^{-1} = a$.
- $\forall a, b \in G$, $(ab)^{-1} = b^{-1}a^{-1}$.
- $c \in G$ and $cc = c \implies c = e$.
- $\forall a, b, c \in G$, $ab = ac \implies b = c$ (left cancelation)
  $ba = ca \implies b = c$ (right cancelation).



Theorem (1.2)

If G is a monoid, then the identity element e is unique.

Furthermore, if G is a group, then

- $\forall a \in G$, the inverse element a^{-1} is unique.
- $\forall a \in G$, $(a^{-1})^{-1} = a$.
- $\forall a, b \in G$, $(ab)^{-1} = b^{-1}a^{-1}$.
- $c \in G$ and $cc = c \implies c = e$.
- $\forall a, b, c \in G$, $ab = ac \implies b = c$ (left cancelation)
  $ba = ca \implies b = c$ (right cancelation).

Proposition (1.3)

Proposition (1.3)

Suppose G is a semigroup.

Proposition (1.3)

Suppose G is a semigroup. Then G is a group

Proposition (1.3)

Suppose G is a semigroup. Then G is a group if and only if the following conditions hold:

Proposition (1.3)

Suppose G is a semigroup. Then G is a group if and only if the following conditions hold:

1. $\exists e \in G$ such that $ea = a, \forall a \in G$

Proposition (1.3)

Suppose G is a semigroup. Then G is a group if and only if the following conditions hold:

1. $\exists e \in G$ such that $ea = a, \forall a \in G$ (left identity).

Proposition (1.3)

Suppose G is a semigroup. Then G is a group if and only if the following conditions hold:

1. $\exists e \in G$ such that $ea = a, \forall a \in G$ (left identity).
2. $\forall a \in G, \exists a^{-1} \in G$ such that $a^{-1}a = e$

Proposition (1.3)

Suppose G is a semigroup. Then G is a group if and only if the following conditions hold:

1. $\exists e \in G$ such that $ea = a, \forall a \in G$ (left identity).
2. $\forall a \in G, \exists a^{-1} \in G$ such that $a^{-1}a = e$ (left inverse).

Proposition (1.3)

Suppose G is a semigroup. Then G is a group if and only if the following conditions hold:

1. $\exists e \in G$ such that $ea = a, \forall a \in G$ (left identity).
2. $\forall a \in G, \exists a^{-1} \in G$ such that $a^{-1}a = e$ (left inverse).

Proof. We need to show (1) $ae = a, \forall a \in G$, and

Proposition (1.3)

Suppose G is a semigroup. Then G is a group if and only if the following conditions hold:

1. $\exists e \in G$ such that $ea = a, \forall a \in G$ (left identity).
2. $\forall a \in G, \exists a^{-1} \in G$ such that $a^{-1}a = e$ (left inverse).

Proof. We need to show (1) $ae = a, \forall a \in G$, and (2) $aa^{-1} = e, \forall a \in G$.

Proposition (1.3)

Suppose G is a semigroup. Then G is a group if and only if the following conditions hold:

1. $\exists e \in G$ such that $ea = a, \forall a \in G$ (left identity).
2. $\forall a \in G, \exists a^{-1} \in G$ such that $a^{-1}a = e$ (left inverse).

Proof. We need to show (1) $ae = a, \forall a \in G$, and (2) $aa^{-1} = e, \forall a \in G$. Note that

Proposition (1.3)

Suppose G is a semigroup. Then G is a group if and only if the following conditions hold:

1. $\exists e \in G$ such that $ea = a, \forall a \in G$ (left identity).
2. $\forall a \in G, \exists a^{-1} \in G$ such that $a^{-1}a = e$ (left inverse).

Proof. We need to show (1) $ae = a, \forall a \in G$, and (2) $aa^{-1} = e, \forall a \in G$. Note that

$$(aa^{-1})(aa^{-1})$$

Proposition (1.3)

Suppose G is a semigroup. Then G is a group if and only if the following conditions hold:

1. $\exists e \in G$ such that $ea = a, \forall a \in G$ (left identity).
2. $\forall a \in G, \exists a^{-1} \in G$ such that $a^{-1}a = e$ (left inverse).

Proof. We need to show (1) $ae = a, \forall a \in G$, and (2) $aa^{-1} = e, \forall a \in G$. Note that

$$(aa^{-1})(aa^{-1}) = a(a^{-1}a)a^{-1}$$

Proposition (1.3)

Suppose G is a semigroup. Then G is a group if and only if the following conditions hold:

1. $\exists e \in G$ such that $ea = a, \forall a \in G$ (left identity).
2. $\forall a \in G, \exists a^{-1} \in G$ such that $a^{-1}a = e$ (left inverse).

Proof. We need to show (1) $ae = a, \forall a \in G$, and (2) $aa^{-1} = e, \forall a \in G$. Note that

$$(aa^{-1})(aa^{-1}) = a(a^{-1}a)a^{-1} = aea^{-1}$$

Proposition (1.3)

Suppose G is a semigroup. Then G is a group if and only if the following conditions hold:

1. $\exists e \in G$ such that $ea = a, \forall a \in G$ (left identity).
2. $\forall a \in G, \exists a^{-1} \in G$ such that $a^{-1}a = e$ (left inverse).

Proof. We need to show (1) $ae = a, \forall a \in G$, and (2) $aa^{-1} = e, \forall a \in G$. Note that

$$(aa^{-1})(aa^{-1}) = a(a^{-1}a)a^{-1} = aea^{-1}$$

because a^{-1} is a left inverse of a

Proposition (1.3)

Suppose G is a semigroup. Then G is a group if and only if the following conditions hold:

1. $\exists e \in G$ such that $ea = a, \forall a \in G$ (left identity).
2. $\forall a \in G, \exists a^{-1} \in G$ such that $a^{-1}a = e$ (left inverse).

Proof. We need to show (1) $ae = a, \forall a \in G$, and (2) $aa^{-1} = e, \forall a \in G$. Note that

$$(aa^{-1})(aa^{-1}) = a(a^{-1}a)a^{-1} = aea^{-1} = a(ea^{-1})$$

Proposition (1.3)

Suppose G is a semigroup. Then G is a group if and only if the following conditions hold:

1. $\exists e \in G$ such that $ea = a, \forall a \in G$ (left identity).
2. $\forall a \in G, \exists a^{-1} \in G$ such that $a^{-1}a = e$ (left inverse).

Proof. We need to show (1) $ae = a, \forall a \in G$, and (2) $aa^{-1} = e, \forall a \in G$. Note that

$$(aa^{-1})(aa^{-1}) = a(a^{-1}a)a^{-1} = aea^{-1} = a(ea^{-1}) = aa^{-1}.$$

Proposition (1.3)

Suppose G is a semigroup. Then G is a group if and only if the following conditions hold:

1. $\exists e \in G$ such that $ea = a, \forall a \in G$ (left identity).
2. $\forall a \in G, \exists a^{-1} \in G$ such that $a^{-1}a = e$ (left inverse).

Proof. We need to show (1) $ae = a, \forall a \in G$, and (2) $aa^{-1} = e, \forall a \in G$. Note that

$$(aa^{-1})(aa^{-1}) = a(a^{-1}a)a^{-1} = aea^{-1} = a(ea^{-1}) = aa^{-1}.$$

because e is a left identity

Proposition (1.3)

Suppose G is a semigroup. Then G is a group if and only if the following conditions hold:

1. $\exists e \in G$ such that $ea = a, \forall a \in G$ (left identity).
2. $\forall a \in G, \exists a^{-1} \in G$ such that $a^{-1}a = e$ (left inverse).

Proof. We need to show (1) $ae = a, \forall a \in G$, and (2) $aa^{-1} = e, \forall a \in G$. Note that

$$(aa^{-1})(aa^{-1}) = a(a^{-1}a)a^{-1} = aea^{-1} = a(ea^{-1}) = aa^{-1}.$$

Hence, if we let $b = (aa^{-1})$ then

Proposition (1.3)

Suppose G is a semigroup. Then G is a group if and only if the following conditions hold:

1. $\exists e \in G$ such that $ea = a, \forall a \in G$ (left identity).
2. $\forall a \in G, \exists a^{-1} \in G$ such that $a^{-1}a = e$ (left inverse).

Proof. We need to show (1) $ae = a, \forall a \in G$, and (2) $aa^{-1} = e, \forall a \in G$. Note that

$$(aa^{-1})(aa^{-1}) = a(a^{-1}a)a^{-1} = aea^{-1} = a(ea^{-1}) = aa^{-1}.$$

Hence, if we let $b = (aa^{-1})$ then we have $bb = b$.

Proposition (1.3)

Suppose G is a semigroup. Then G is a group if and only if the following conditions hold:

1. $\exists e \in G$ such that $ea = a, \forall a \in G$ (left identity).
2. $\forall a \in G, \exists a^{-1} \in G$ such that $a^{-1}a = e$ (left inverse).

Proof. We need to show (1) $ae = a, \forall a \in G$, and (2) $aa^{-1} = e, \forall a \in G$. Note that

$$(aa^{-1})(aa^{-1}) = a(a^{-1}a)a^{-1} = aea^{-1} = a(ea^{-1}) = aa^{-1}.$$

Hence, if we let $b = (aa^{-1})$ then we have $bb = b$. Since

$$bb = b \Rightarrow b^{-1}bb = b^{-1}b$$

Proposition (1.3)

Suppose G is a semigroup. Then G is a group if and only if the following conditions hold:

1. $\exists e \in G$ such that $ea = a, \forall a \in G$ (left identity).
2. $\forall a \in G, \exists a^{-1} \in G$ such that $a^{-1}a = e$ (left inverse).

Proof. We need to show (1) $ae = a, \forall a \in G$, and (2) $aa^{-1} = e, \forall a \in G$. Note that

$$(aa^{-1})(aa^{-1}) = a(a^{-1}a)a^{-1} = aea^{-1} = a(ea^{-1}) = aa^{-1}.$$

Hence, if we let $b = (aa^{-1})$ then we have $bb = b$. Since

$$bb = b \Rightarrow b^{-1}bb = b^{-1}b \Rightarrow (b^{-1}b)b = e$$

because b^{-1} is a left inverse of b

Proposition (1.3)

Suppose G is a semigroup. Then G is a group if and only if the following conditions hold:

1. $\exists e \in G$ such that $ea = a, \forall a \in G$ (left identity).
2. $\forall a \in G, \exists a^{-1} \in G$ such that $a^{-1}a = e$ (left inverse).

Proof. We need to show (1) $ae = a, \forall a \in G$, and (2) $aa^{-1} = e, \forall a \in G$. Note that

$$(aa^{-1})(aa^{-1}) = a(a^{-1}a)a^{-1} = aea^{-1} = a(ea^{-1}) = aa^{-1}.$$

Hence, if we let $b = (aa^{-1})$ then we have $bb = b$. Since

$$bb = b \Rightarrow b^{-1}bb = b^{-1}b \Rightarrow (b^{-1}b)b = e \Rightarrow eb = e$$

because b^{-1} is a left inverse of b

Proposition (1.3)

Suppose G is a semigroup. Then G is a group if and only if the following conditions hold:

1. $\exists e \in G$ such that $ea = a, \forall a \in G$ (left identity).
2. $\forall a \in G, \exists a^{-1} \in G$ such that $a^{-1}a = e$ (left inverse).

Proof. We need to show (1) $ae = a, \forall a \in G$, and (2) $aa^{-1} = e, \forall a \in G$. Note that

$$(aa^{-1})(aa^{-1}) = a(a^{-1}a)a^{-1} = aea^{-1} = a(ea^{-1}) = aa^{-1}.$$

Hence, if we let $b = (aa^{-1})$ then we have $bb = b$. Since

$$bb = b \Rightarrow b^{-1}bb = b^{-1}b \Rightarrow (b^{-1}b)b = e \Rightarrow eb = e \Rightarrow b = e,$$

because e is a left identity

Proposition (1.3)

Suppose G is a semigroup. Then G is a group if and only if the following conditions hold:

1. $\exists e \in G$ such that $ea = a, \forall a \in G$ (left identity).
2. $\forall a \in G, \exists a^{-1} \in G$ such that $a^{-1}a = e$ (left inverse).

Proof. We need to show (1) $ae = a, \forall a \in G$, and (2) $aa^{-1} = e, \forall a \in G$. Note that

$$(aa^{-1})(aa^{-1}) = a(a^{-1}a)a^{-1} = aea^{-1} = a(ea^{-1}) = aa^{-1}.$$

Hence, if we let $b = (aa^{-1})$ then we have $bb = b$. Since

$$bb = b \Rightarrow b^{-1}bb = b^{-1}b \Rightarrow (b^{-1}b)b = e \Rightarrow eb = e \Rightarrow b = e,$$

i.e., $aa^{-1} = e$,

Proposition (1.3)

Suppose G is a semigroup. Then G is a group if and only if the following conditions hold:

1. $\exists e \in G$ such that $ea = a, \forall a \in G$ (left identity).
2. $\forall a \in G, \exists a^{-1} \in G$ such that $a^{-1}a = e$ (left inverse).

Proof. We need to show (1) $ae = a, \forall a \in G$, and (2) $aa^{-1} = e, \forall a \in G$. Note that

$$(aa^{-1})(aa^{-1}) = a(a^{-1}a)a^{-1} = aea^{-1} = a(ea^{-1}) = aa^{-1}.$$

Hence, if we let $b = (aa^{-1})$ then we have $bb = b$. Since

$$bb = b \Rightarrow b^{-1}bb = b^{-1}b \Rightarrow (b^{-1}b)b = e \Rightarrow eb = e \Rightarrow b = e,$$

i.e., $aa^{-1} = e$, and this shows (2).

Proposition (1.3)

Suppose G is a semigroup. Then G is a group if and only if the following conditions hold:

1. $\exists e \in G$ such that $ea = a, \forall a \in G$ (left identity).
2. $\forall a \in G, \exists a^{-1} \in G$ such that $a^{-1}a = e$ (left inverse).

Proof. We need to show (1) $ae = a, \forall a \in G$, and (2) $aa^{-1} = e, \forall a \in G$. Note that

$$(aa^{-1})(aa^{-1}) = a(a^{-1}a)a^{-1} = aea^{-1} = a(ea^{-1}) = aa^{-1}.$$

Hence, if we let $b = (aa^{-1})$ then we have $bb = b$. Since

$$bb = b \Rightarrow b^{-1}bb = b^{-1}b \Rightarrow (b^{-1}b)b = e \Rightarrow eb = e \Rightarrow b = e,$$

i.e., $aa^{-1} = e$, and this shows (2). On the other hand,

Proposition (1.3)

Suppose G is a semigroup. Then G is a group if and only if the following conditions hold:

1. $\exists e \in G$ such that $ea = a, \forall a \in G$ (left identity).
2. $\forall a \in G, \exists a^{-1} \in G$ such that $a^{-1}a = e$ (left inverse).

Proof. We need to show (1) $ae = a, \forall a \in G$, and (2) $aa^{-1} = e, \forall a \in G$. Note that

$$(aa^{-1})(aa^{-1}) = a(a^{-1}a)a^{-1} = aea^{-1} = a(ea^{-1}) = aa^{-1}.$$

Hence, if we let $b = (aa^{-1})$ then we have $bb = b$. Since

$$bb = b \Rightarrow b^{-1}bb = b^{-1}b \Rightarrow (b^{-1}b)b = e \Rightarrow eb = e \Rightarrow b = e,$$

i.e., $aa^{-1} = e$, and this shows (2). On the other hand,

$$ae = a(a^{-1}a)$$

because a^{-1} is an inverse of a

Proposition (1.3)

Suppose G is a semigroup. Then G is a group if and only if the following conditions hold:

1. $\exists e \in G$ such that $ea = a, \forall a \in G$ (left identity).
2. $\forall a \in G, \exists a^{-1} \in G$ such that $a^{-1}a = e$ (left inverse).

Proof. We need to show (1) $ae = a, \forall a \in G$, and (2) $aa^{-1} = e, \forall a \in G$. Note that

$$(aa^{-1})(aa^{-1}) = a(a^{-1}a)a^{-1} = aea^{-1} = a(ea^{-1}) = aa^{-1}.$$

Hence, if we let $b = (aa^{-1})$ then we have $bb = b$. Since

$$bb = b \Rightarrow b^{-1}bb = b^{-1}b \Rightarrow (b^{-1}b)b = e \Rightarrow eb = e \Rightarrow b = e,$$

i.e., $aa^{-1} = e$, and this shows (2). On the other hand,

$$ae = a(a^{-1}a) = (aa^{-1})a$$

Proposition (1.3)

Suppose G is a semigroup. Then G is a group if and only if the following conditions hold:

1. $\exists e \in G$ such that $ea = a, \forall a \in G$ (left identity).
2. $\forall a \in G, \exists a^{-1} \in G$ such that $a^{-1}a = e$ (left inverse).

Proof. We need to show (1) $ae = a, \forall a \in G$, and (2) $aa^{-1} = e, \forall a \in G$. Note that

$$(aa^{-1})(aa^{-1}) = a(a^{-1}a)a^{-1} = aea^{-1} = a(ea^{-1}) = aa^{-1}.$$

Hence, if we let $b = (aa^{-1})$ then we have $bb = b$. Since

$$bb = b \Rightarrow b^{-1}bb = b^{-1}b \Rightarrow (b^{-1}b)b = e \Rightarrow eb = e \Rightarrow b = e,$$

i.e., $aa^{-1} = e$, and this shows (2). On the other hand,

$$ae = a(a^{-1}a) = (aa^{-1})a = ea$$

because a^{-1} is an inverse of a

Proposition (1.3)

Suppose G is a semigroup. Then G is a group if and only if the following conditions hold:

1. $\exists e \in G$ such that $ea = a, \forall a \in G$ (left identity).
2. $\forall a \in G, \exists a^{-1} \in G$ such that $a^{-1}a = e$ (left inverse).

Proof. We need to show (1) $ae = a, \forall a \in G$, and (2) $aa^{-1} = e, \forall a \in G$. Note that

$$(aa^{-1})(aa^{-1}) = a(a^{-1}a)a^{-1} = aea^{-1} = a(ea^{-1}) = aa^{-1}.$$

Hence, if we let $b = (aa^{-1})$ then we have $bb = b$. Since

$$bb = b \Rightarrow b^{-1}bb = b^{-1}b \Rightarrow (b^{-1}b)b = e \Rightarrow eb = e \Rightarrow b = e,$$

i.e., $aa^{-1} = e$, and this shows (2). On the other hand,

$$ae = a(a^{-1}a) = (aa^{-1})a = ea = a$$

because e is a left identity

Proposition (1.3)

Suppose G is a semigroup. Then G is a group if and only if the following conditions hold:

1. $\exists e \in G$ such that $ea = a, \forall a \in G$ (left identity).
2. $\forall a \in G, \exists a^{-1} \in G$ such that $a^{-1}a = e$ (left inverse).

Proof. We need to show (1) $ae = a, \forall a \in G$, and (2) $aa^{-1} = e, \forall a \in G$. Note that

$$(aa^{-1})(aa^{-1}) = a(a^{-1}a)a^{-1} = aea^{-1} = a(ea^{-1}) = aa^{-1}.$$

Hence, if we let $b = (aa^{-1})$ then we have $bb = b$. Since

$$bb = b \Rightarrow b^{-1}bb = b^{-1}b \Rightarrow (b^{-1}b)b = e \Rightarrow eb = e \Rightarrow b = e,$$

i.e., $aa^{-1} = e$, and this shows (2). On the other hand,

$$ae = a(a^{-1}a) = (aa^{-1})a = ea = a$$

and this shows (1).

Notation

Definition (1.8)**.** Let G be a semigroup.

Notation

Definition (1.8)**.** Let G be a semigroup.

- $\forall n \in \mathbb{N}, \forall a \in G,$

Notation

Definition (1.8)**.** Let G be a semigroup.

- $\forall n \in \mathbb{N}, \forall a \in G,\ a^n := \underbrace{aa \cdots a}_{n \text{ times}}$.

Notation

Definition (1.8)**.** Let G be a semigroup.

- $\forall n \in \mathbb{N}, \forall a \in G,\ a^n := \underbrace{aa \cdots a}_{n \text{ times}}$.
- If G is a monoid, then $\forall a \in G$,

Notation

Definition (1.8)**.** Let G be a semigroup.

- $\forall n \in \mathbb{N}, \forall a \in G,\ a^n := \underbrace{aa \cdots a}_{n \text{ times}}$.
- If G is a monoid, then $\forall a \in G,\ a^0 := e$.

Notation

Definition (1.8)**.** Let G be a semigroup.

- $\forall n \in \mathbb{N}, \forall a \in G,\ a^n := \underbrace{aa \cdots a}_{n \text{ times}}$.
- If G is a monoid, then $\forall a \in G,\ a^0 := e$.
- If G is a group, then $\forall n \in \mathbb{N}, \forall a \in G,$

Notation

Definition (1.8)**.** Let G be a semigroup.

- $\forall n \in \mathbb{N}, \forall a \in G,\ a^n := \underbrace{aa \cdots a}_{n \text{ times}}$.
- If G is a monoid, then $\forall a \in G,\ a^0 := e$.
- If G is a group, then $\forall n \in \mathbb{N}, \forall a \in G,\ a^{-n} := (a^{-1})^n$.

Notation

Definition (1.8)**.** Let G be a semigroup.

- $\forall n \in \mathbb{N}, \forall a \in G,\ a^n := \underbrace{aa \cdots a}_{n \text{ times}}$.
- If G is a monoid, then $\forall a \in G,\ a^0 := e$.
- If G is a group, then $\forall n \in \mathbb{N}, \forall a \in G,\ a^{-n} := (a^{-1})^n$.

Theorem (1.9)**.** If G is a group

Notation

Definition (1.8)**.** Let G be a semigroup.

- $\forall n \in \mathbb{N}, \forall a \in G,\ a^n := \underbrace{aa \cdots a}_{n \text{ times}}$.
- If G is a monoid, then $\forall a \in G,\ a^0 := e$.
- If G is a group, then $\forall n \in \mathbb{N}, \forall a \in G,\ a^{-n} := (a^{-1})^n$.

Theorem (1.9)**.** If G is a group
and if $a \in G$,

Notation

Definition (1.8)**.** Let G be a semigroup.

- $\forall n \in \mathbb{N}, \forall a \in G,\ a^n := \underbrace{aa \cdots a}_{n \text{ times}}$.
- If G is a monoid, then $\forall a \in G,\ a^0 := e$.
- If G is a group, then $\forall n \in \mathbb{N}, \forall a \in G,\ a^{-n} := (a^{-1})^n$.

Theorem (1.9)**.** If G is a group
and if $a \in G$, then $\forall m, n \in \mathbb{Z}$

Notation

Definition (1.8)**.** Let G be a semigroup.

- $\forall n \in \mathbb{N}, \forall a \in G,\ a^n := \underbrace{aa \cdots a}_{n \text{ times}}$.
- If G is a monoid, then $\forall a \in G,\ a^0 := e$.
- If G is a group, then $\forall n \in \mathbb{N}, \forall a \in G,\ a^{-n} := (a^{-1})^n$.

Theorem (1.9)**.** If G is a group
and if $a \in G$, then $\forall m, n \in \mathbb{Z}$

- $a^m a^n = a^{m+n}$,

Notation

Definition (1.8). Let G be a semigroup.

- $\forall n \in \mathbb{N}, \forall a \in G,\ a^n := \underbrace{aa \cdots a}_{n \text{ times}}$.
- If G is a monoid, then $\forall a \in G,\ a^0 := e$.
- If G is a group, then $\forall n \in \mathbb{N}, \forall a \in G,\ a^{-n} := (a^{-1})^n$.

Theorem (1.9). If G is a group
and if $a \in G$, then $\forall m, n \in \mathbb{Z}$

- $a^m a^n = a^{m+n}$,
- $(a^m)^n = a^{mn}$.

Notation

Definition (1.8). Let G be a semigroup.

- $\forall n \in \mathbb{N}, \forall a \in G,\ a^n := \underbrace{aa \cdots a}_{n \text{ times}}$.
- If G is a monoid, then $\forall a \in G,\ a^0 := e$.
- If G is a group, then $\forall n \in \mathbb{N}, \forall a \in G,\ a^{-n} := (a^{-1})^n$.

Theorem (1.9). If G is a group (resp. semigroup, and if $a \in G$, then $\forall m, n \in \mathbb{Z}$

- $a^m a^n = a^{m+n}$,
- $(a^m)^n = a^{mn}$.

Notation

Definition (1.8). Let G be a semigroup.

- $\forall n \in \mathbb{N}, \forall a \in G,\ a^n := \underbrace{aa \cdots a}_{n \text{ times}}$.
- If G is a monoid, then $\forall a \in G,\ a^0 := e$.
- If G is a group, then $\forall n \in \mathbb{N}, \forall a \in G,\ a^{-n} := (a^{-1})^n$.

Theorem (1.9). If G is a group (resp. semigroup, and if $a \in G$, then $\forall m, n \in \mathbb{Z}$ (resp. $\mathbb{N}$,

- $a^m a^n = a^{m+n}$,
- $(a^m)^n = a^{mn}$.

Notation

Definition (1.8)**.** Let G be a semigroup.

- $\forall n \in \mathbb{N}, \forall a \in G,\ a^n := \underbrace{aa \cdots a}_{n \text{ times}}$.
- If G is a monoid, then $\forall a \in G,\ a^0 := e$.
- If G is a group, then $\forall n \in \mathbb{N}, \forall a \in G,\ a^{-n} := (a^{-1})^n$.

Theorem (1.9)**.** If G is a group (resp. semigroup, monoid) and if $a \in G$, then $\forall m, n \in \mathbb{Z}$ (resp. $\mathbb{N}$,

- $a^m a^n = a^{m+n}$,
- $(a^m)^n = a^{mn}$.

Notation

Definition (1.8). Let G be a semigroup.

- $\forall n \in \mathbb{N}, \forall a \in G,\ a^n := \underbrace{aa \cdots a}_{n \text{ times}}$.
- If G is a monoid, then $\forall a \in G,\ a^0 := e$.
- If G is a group, then $\forall n \in \mathbb{N}, \forall a \in G,\ a^{-n} := (a^{-1})^n$.

Theorem (1.9). If G is a group (resp. semigroup, monoid) and if $a \in G$, then $\forall m, n \in \mathbb{Z}$ (resp. $\mathbb{N}$, $\mathbb{N} \cup \{0\}$),

- $a^m a^n = a^{m+n}$,
- $(a^m)^n = a^{mn}$.

Section I.2: Homomorphisms and Subgroups

Section I.2: Homomorphisms and Subgroups

Definition (2.1)**.** Let G and H be semigroups.

Section I.2: Homomorphisms and Subgroups

Definition (2.1)**.** Let G and H be semigroups.

A function $f : G \to H$

Section I.2: Homomorphisms and Subgroups

Definition (2.1)**.** Let G and H be semigroups.

A function $f : G \to H$ is called a homomorphism

Section I.2: Homomorphisms and Subgroups

Definition (2.1)**.** Let G and H be semigroups.

A function $f : G \to H$ is called a homomorphism (or said to be homomorphic)

Section I.2: Homomorphisms and Subgroups

Definition (2.1)**.** Let G and H be semigroups.

A function $f : G \to H$ is called a homomorphism (or said to be homomorphic) if

$$f(ab) = f(a)f(b), \quad \forall a, b \in G.$$

Section I.2: Homomorphisms and Subgroups

Definition (2.1)**.** Let G and H be semigroups.

A function $f : G \to H$ is called a homomorphism (or said to be homomorphic) if

$$f(ab) = f(a)f(b), \quad \forall a, b \in G.$$

Furthermore,

Section I.2: Homomorphisms and Subgroups

Definition (2.1)**.** Let G and H be semigroups.

A function $f : G \to H$ is called a homomorphism (or said to be homomorphic) if

$$f(ab) = f(a)f(b), \quad \forall a, b \in G.$$

Furthermore,

- if f is 1-1,

Section I.2: Homomorphisms and Subgroups

Definition (2.1)**.** Let G and H be semigroups.

A function $f : G \to H$ is called a homomorphism (or said to be homomorphic) if

$$f(ab) = f(a)f(b), \quad \forall a, b \in G.$$

Furthermore,

- if f is 1-1, i.e., injective,

Section I.2: Homomorphisms and Subgroups

Definition (2.1)**.** Let G and H be semigroups.

A function $f : G \to H$ is called a homomorphism (or said to be homomorphic) if

$$f(ab) = f(a)f(b), \quad \forall a, b \in G.$$

Furthermore,

- if f is 1-1, i.e., injective, f is called a monomorphism;

Section I.2: Homomorphisms and Subgroups

Definition (2.1)**.** Let G and H be semigroups.

A function $f : G \to H$ is called a homomorphism (or said to be homomorphic) if

$$f(ab) = f(a)f(b), \quad \forall a, b \in G.$$

Furthermore,

- if f is 1-1, i.e., injective, f is called a monomorphism;
- if f is onto,

Section I.2: Homomorphisms and Subgroups

Definition (2.1)**.** Let G and H be semigroups.

A function $f : G \to H$ is called a homomorphism (or said to be homomorphic) if

$$f(ab) = f(a)f(b), \quad \forall a, b \in G.$$

Furthermore,

- if f is 1-1, i.e., injective, f is called a monomorphism;
- if f is onto, i.e., surjective,

Section I.2: Homomorphisms and Subgroups

Definition (2.1)**.** Let G and H be semigroups.

A function $f : G \to H$ is called a homomorphism (or said to be homomorphic) if

$$f(ab) = f(a)f(b), \quad \forall a, b \in G.$$

Furthermore,

- if f is 1-1, i.e., injective, f is called a monomorphism;
- if f is onto, i.e., surjective, f is called an epimorphism;

Section I.2: Homomorphisms and Subgroups

Definition (2.1)**.** Let G and H be semigroups.

A function $f : G \to H$ is called a homomorphism (or said to be homomorphic) if

$$f(ab) = f(a)f(b), \quad \forall a, b \in G.$$

Furthermore,

- if f is 1-1, i.e., injective, f is called a monomorphism;
- if f is onto, i.e., surjective, f is called an epimorphism;
- if f is 1-1 and onto,

Section I.2: Homomorphisms and Subgroups

Definition (2.1)**.** Let G and H be semigroups.

A function $f : G \to H$ is called a homomorphism (or said to be homomorphic) if

$$f(ab) = f(a)f(b), \quad \forall a, b \in G.$$

Furthermore,

- if f is 1-1, i.e., injective, f is called a monomorphism;
- if f is onto, i.e., surjective, f is called an epimorphism;
- if f is 1-1 and onto, i.e., bijective,

Section I.2: Homomorphisms and Subgroups

Definition (2.1)**.** Let G and H be semigroups.

A function $f : G \to H$ is called a homomorphism (or said to be homomorphic) if

$$f(ab) = f(a)f(b), \quad \forall a, b \in G.$$

Furthermore,

- if f is 1-1, i.e., injective, f is called a monomorphism;
- if f is onto, i.e., surjective, f is called an epimorphism;
- if f is 1-1 and onto, i.e., bijective, f is called an isomorphism

Section I.2: Homomorphisms and Subgroups

Definition (2.1)**.** Let G and H be semigroups.
A function $f : G \to H$ is called a homomorphism (or said to be homomorphic) if

$$f(ab) = f(a)f(b), \quad \forall a, b \in G.$$

Furthermore,

- if f is 1-1, i.e., injective, f is called a monomorphism;
- if f is onto, i.e., surjective, f is called an epimorphism;
- if f is 1-1 and onto, i.e., bijective, f is called an isomorphism (or said to be isomorphic),

Section I.2: Homomorphisms and Subgroups

Definition (2.1)**.** Let G and H be semigroups.
A function $f : G \to H$ is called a homomorphism (or said to be homomorphic) if

$$f(ab) = f(a)f(b), \quad \forall a, b \in G.$$

Furthermore,

- if f is 1-1, i.e., injective, f is called a monomorphism;
- if f is onto, i.e., surjective, f is called an epimorphism;
- if f is 1-1 and onto, i.e., bijective, f is called an isomorphism (or said to be isomorphic), and we write $G \simeq H$.

Section I.2: Homomorphisms and Subgroups

Definition (2.1)**.** Let G and H be semigroups.
A function $f : G \to H$ is called a homomorphism (or said to be homomorphic) if

$$f(ab) = f(a)f(b), \quad \forall a, b \in G.$$

Furthermore,

- if f is 1-1, i.e., injective, f is called a monomorphism;
- if f is onto, i.e., surjective, f is called an epimorphism;
- if f is 1-1 and onto, i.e., bijective, f is called an isomorphism (or said to be isomorphic), and we write $G \simeq H$.

In particular,

Section I.2: Homomorphisms and Subgroups

Definition (2.1)**.** Let G and H be semigroups.
A function $f : G \to H$ is called a homomorphism (or said to be homomorphic) if

$$f(ab) = f(a)f(b), \quad \forall a, b \in G.$$

Furthermore,

- if f is 1-1, i.e., injective, f is called a monomorphism;
- if f is onto, i.e., surjective, f is called an epimorphism;
- if f is 1-1 and onto, i.e., bijective, f is called an isomorphism (or said to be isomorphic), and we write $G \simeq H$.

In particular,

- a homomorphism $f : G \to G$ is called an

Section I.2: Homomorphisms and Subgroups

Definition (2.1)**.** Let G and H be semigroups.
A function $f : G \to H$ is called a homomorphism (or said to be homomorphic) if

$$f(ab) = f(a)f(b), \quad \forall a, b \in G.$$

Furthermore,

- if f is 1-1, i.e., injective, f is called a monomorphism;
- if f is onto, i.e., surjective, f is called an epimorphism;
- if f is 1-1 and onto, i.e., bijective, f is called an isomorphism (or said to be isomorphic), and we write $G \simeq H$.

In particular,

- a homomorphism $f : G \to G$ is called an endomorphism;

Section I.2: Homomorphisms and Subgroups

Definition (2.1)**.** Let G and H be semigroups.
A function $f : G \to H$ is called a homomorphism (or said to be homomorphic) if

$$f(ab) = f(a)f(b), \quad \forall a, b \in G.$$

Furthermore,

- if f is 1-1, i.e., injective, f is called a monomorphism;
- if f is onto, i.e., surjective, f is called an epimorphism;
- if f is 1-1 and onto, i.e., bijective, f is called an isomorphism (or said to be isomorphic), and we write $G \simeq H$.

In particular,

- a homomorphism $f : G \to G$ is called an endomorphism;
- an isomorphism $f : G \to G$ is called an

Section I.2: Homomorphisms and Subgroups

Definition (2.1)**.** Let G and H be semigroups.
A function $f : G \to H$ is called a homomorphism (or said to be homomorphic) if

$$f(ab) = f(a)f(b), \quad \forall a, b \in G.$$

Furthermore,

- if f is 1-1, i.e., injective, f is called a monomorphism;
- if f is onto, i.e., surjective, f is called an epimorphism;
- if f is 1-1 and onto, i.e., bijective, f is called an isomorphism (or said to be isomorphic), and we write $G \simeq H$.

In particular,

- a homomorphism $f : G \to G$ is called an endomorphism;
- an isomorphism $f : G \to G$ is called an automorphism.

Remarks on Compositions

If $f : G \to H$ and $g : H \to K$ are homomorphisms of semigroups,

Remarks on Compositions

If $f : G \to H$ and $g : H \to K$ are homomorphisms of semigroups, then their composition $gf : G \to K$

Remarks on Compositions

If $f : G \to H$ and $g : H \to K$ are homomorphisms of semigroups, then their composition $gf : G \to K$ is also a homomorphism.

Remarks on Compositions

If $f : G \to H$ and $g : H \to K$ are homomorphisms of semigroups, then their composition $gf : G \to K$ is also a homomorphism.

This is because for all $a, b \in G$,

Remarks on Compositions

If $f : G \to H$ and $g : H \to K$ are homomorphisms of semigroups, then their composition $gf : G \to K$ is also a homomorphism.

This is because for all $a, b \in G$,

$$gf(ab) = g\big(f(ab)\big)$$

Remarks on Compositions

If $f : G \to H$ and $g : H \to K$ are homomorphisms of semigroups, then their composition $gf : G \to K$ is also a homomorphism.

This is because for all $a, b \in G$,

$$gf(ab) = g\big(f(ab)\big) = g\big(f(a)f(b)\big)$$

because f is homomorphic

Remarks on Compositions

If $f : G \to H$ and $g : H \to K$ are homomorphisms of semigroups, then their composition $gf : G \to K$ is also a homomorphism.

This is because for all $a, b \in G$,

$$gf(ab) = g\big(f(ab)\big) = g\big(f(a)f(b)\big) = g\big(f(a)\big)g\big(f(b)\big)$$

because g is homomorphic

Remarks on Compositions

If $f : G \to H$ and $g : H \to K$ are homomorphisms of semigroups, then their composition $gf : G \to K$ is also a homomorphism.

This is because for all $a, b \in G$,

$$gf(ab) = g\big(f(ab)\big) = g\big(f(a)f(b)\big) = g\big(f(a)\big)g\big(f(b)\big)$$
$$= gf(a)gf(b).$$

Remarks on Compositions

If $f : G \to H$ and $g : H \to K$ are homomorphisms of semigroups, then their composition $gf : G \to K$ is also a homomorphism.

Likewise,

Remarks on Compositions

If $f : G \to H$ and $g : H \to K$ are homomorphisms of semigroups, then their composition $gf : G \to K$ is also a homomorphism.

Likewise, because the composition of two one-to-one functions is again one-to-one

Remarks on Compositions

If $f : G \to H$ and $g : H \to K$ are homomorphisms of semigroups, then their composition $gf : G \to K$ is also a homomorphism.

Likewise, because the composition of two one-to-one functions is again one-to-one and because the composition of two onto functions is again onto,

Remarks on Compositions

If $f : G \to H$ and $g : H \to K$ are homomorphisms of semigroups, then their composition $gf : G \to K$ is also a homomorphism.

Likewise, because the composition of two one-to-one functions is again one-to-one and because the composition of two onto functions is again onto,

- the composition of monomorphisms is a monomorphism;

Remarks on Compositions

If $f : G \to H$ and $g : H \to K$ are homomorphisms of semigroups, then their composition $gf : G \to K$ is also a homomorphism.

Likewise, because the composition of two one-to-one functions is again one-to-one and because the composition of two onto functions is again onto,

- the composition of monomorphisms is a monomorphism;
- the composition of epimorphisms is an epimorphism;

Remarks on Compositions

If $f : G \to H$ and $g : H \to K$ are homomorphisms of semigroups, then their composition $gf : G \to K$ is also a homomorphism.

Likewise, because the composition of two one-to-one functions is again one-to-one and because the composition of two onto functions is again onto,

- the composition of monomorphisms is a monomorphism;
- the composition of epimorphisms is an epimorphism;
- the composition of isomorphisms is an isomorphism;

Remarks on Compositions

If $f : G \to H$ and $g : H \to K$ are homomorphisms of semigroups, then their composition $gf : G \to K$ is also a homomorphism.

Likewise, because the composition of two one-to-one functions is again one-to-one and because the composition of two onto functions is again onto,

- the composition of monomorphisms is a monomorphism;
- the composition of epimorphisms is an epimorphism;
- the composition of isomorphisms is an isomorphism;
- the composition of endomorphisms is an endomorphism;

Remarks on Compositions

If $f : G \to H$ and $g : H \to K$ are homomorphisms of semigroups, then their composition $gf : G \to K$ is also a homomorphism.

Likewise, because the composition of two one-to-one functions is again one-to-one and because the composition of two onto functions is again onto,

- the composition of monomorphisms is a monomorphism;
- the composition of epimorphisms is an epimorphism;
- the composition of isomorphisms is an isomorphism;
- the composition of endomorphisms is an endomorphism;
- the composition of automorphisms is an automorphism.

Homomorphisms vs Identities and Inverses

Remark. If G and H are groups

Homomorphisms vs Identities and Inverses

Remark. If G and H are groups with identities e_G and e_H respectively,

Homomorphisms vs Identities and Inverses

Remark. If G and H are groups with identities e_G and e_H respectively, and if $f : G \to H$ is a homomorphism,

Homomorphisms vs Identities and Inverses

Remark. If G and H are groups with identities e_G and e_H respectively, and if $f : G \to H$ is a homomorphism, then

$$f(e_G) = e_H$$

Homomorphisms vs Identities and Inverses

Remark. If G and H are groups with identities e_G and e_H respectively, and if $f : G \to H$ is a homomorphism, then

$f(e_G)=e_H$ and

Homomorphisms vs Identities and Inverses

Remark. If G and H are groups with identities e_G and e_H respectively, and if $f : G \to H$ is a homomorphism, then

$$f(e_G)=e_H \quad \text{and} \quad f(a^{-1})=f(a)^{-1}, \forall a \in G.$$

Homomorphisms vs Identities and Inverses

Remark. If G and H are groups with identities e_G and e_H respectively, and if $f : G \to H$ is a homomorphism, then

$$f(e_G)=e_H \quad \text{and} \quad f(a^{-1})=f(a)^{-1}, \forall a \in G.$$

because $f(e_G)f(e_G)$

Homomorphisms vs Identities and Inverses

Remark. If G and H are groups with identities e_G and e_H respectively, and if $f : G \to H$ is a homomorphism, then

$$f(e_G)=e_H \quad \text{and} \quad f(a^{-1})=f(a)^{-1}, \forall a \in G.$$

because $f(e_G)f(e_G) = f(e_G e_G)$

Homomorphisms vs Identities and Inverses

Remark. If G and H are groups with identities e_G and e_H respectively, and if $f : G \to H$ is a homomorphism, then

$$f(e_G)=e_H \quad \text{and} \quad f(a^{-1})=f(a)^{-1}, \forall a \in G.$$

because $f(e_G)f(e_G) = f(e_G e_G) = f(e_G)$

Homomorphisms vs Identities and Inverses

Remark. If G and H are groups with identities e_G and e_H respectively, and if $f : G \to H$ is a homomorphism, then

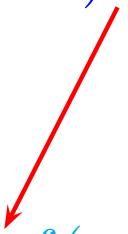
$$f(e_G)=e_H \quad \text{and} \quad f(a^{-1})=f(a)^{-1}, \forall a \in G.$$

because $f(e_G)f(e_G) = f(e_Ge_G) = f(e_G) \implies f(e_G) = e_H$

Homomorphisms vs Identities and Inverses

Remark. If G and H are groups with identities e_G and e_H respectively, and if $f : G \to H$ is a homomorphism, then

$$f(e_G)=e_H \quad \text{and} \quad f(a^{-1})=f(a)^{-1}, \forall a \in G.$$

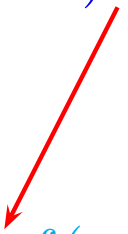


because $f(a^{-1})f(a)$

Homomorphisms vs Identities and Inverses

Remark. If G and H are groups with identities e_G and e_H respectively, and if $f : G \to H$ is a homomorphism, then

$$f(e_G)=e_H \quad \text{and} \quad f(a^{-1})=f(a)^{-1}, \forall a \in G.$$

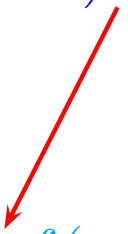


because $f(a^{-1})f(a) = f(a^{-1}a)$

Homomorphisms vs Identities and Inverses

Remark. If G and H are groups with identities e_G and e_H respectively, and if $f : G \to H$ is a homomorphism, then

$$f(e_G)=e_H \quad \text{and} \quad f(a^{-1})=f(a)^{-1}, \forall a \in G.$$

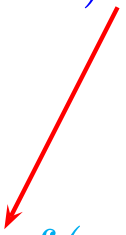


because $f(a^{-1})f(a) = f(a^{-1}a) = f(e_G)$

Homomorphisms vs Identities and Inverses

Remark. If G and H are groups with identities e_G and e_H respectively, and if $f : G \to H$ is a homomorphism, then

$$f(e_G)=e_H \quad \text{and} \quad f(a^{-1})=f(a)^{-1}, \forall a \in G.$$



because $f(a^{-1})f(a) = f(a^{-1}a) = f(e_G) = e_H$

Homomorphisms vs Identities and Inverses

Remark. If G and H are groups with identities e_G and e_H respectively, and if $f : G \to H$ is a homomorphism, then

$$f(e_G)=e_H \text{ and } f(a^{-1})=f(a)^{-1}, \forall a \in G.$$

WARNING:

Homomorphisms vs Identities and Inverses

Remark. If G and H are groups with identities e_G and e_H respectively, and if $f : G \to H$ is a homomorphism, then

$$f(e_G)=e_H \text{ and } f(a^{-1})=f(a)^{-1}, \forall a \in G.$$

WARNING: If G and H are just monoids, not groups,

Homomorphisms vs Identities and Inverses

Remark. If G and H are groups with identities e_G and e_H respectively, and if $f : G \to H$ is a homomorphism, then

$$f(e_G)=e_H \text{ and } f(a^{-1})=f(a)^{-1}, \forall a \in G.$$

WARNING: If G and H are just monoids, not groups, $f(e_G)$ may NOT equal e_H.

Homomorphisms vs Identities and Inverses

Remark. If G and H are groups with identities e_G and e_H respectively, and if $f : G \to H$ is a homomorphism, then

$$f(e_G)=e_H \text{ and } f(a^{-1})=f(a)^{-1}, \forall a \in G.$$

WARNING: If G and H are just monoids, not groups, $f(e_G)$ may NOT equal e_H.

EXAMPLE: $G = \mathbb{Z}$ and $H = \mathbb{Z} \times \mathbb{Z}$ are multiplicative monoids

Homomorphisms vs Identities and Inverses

Remark. If G and H are groups with identities e_G and e_H respectively, and if $f : G \to H$ is a homomorphism, then

$$f(e_G)=e_H \text{ and } f(a^{-1})=f(a)^{-1}, \forall a \in G.$$

WARNING: If G and H are just monoids, not groups, $f(e_G)$ may NOT equal e_H.

EXAMPLE: $G = \mathbb{Z}$ and $H = \mathbb{Z} \times \mathbb{Z}$ are multiplicative monoids with $e_G = 1$

Homomorphisms vs Identities and Inverses

Remark. If G and H are groups with identities e_G and e_H respectively, and if $f : G \to H$ is a homomorphism, then

$$f(e_G)=e_H \text{ and } f(a^{-1})=f(a)^{-1}, \forall a \in G.$$

WARNING: If G and H are just monoids, not groups, $f(e_G)$ may NOT equal e_H.

EXAMPLE: $G = \mathbb{Z}$ and $H = \mathbb{Z} \times \mathbb{Z}$ are multiplicative monoids with $e_G = 1$ and $e_H = (1, 1)$.

Homomorphisms vs Identities and Inverses

Remark. If G and H are groups with identities e_G and e_H respectively, and if $f : G \to H$ is a homomorphism, then

$$f(e_G)=e_H \text{ and } f(a^{-1})=f(a)^{-1}, \forall a \in G.$$

WARNING: If G and H are just monoids, not groups, $f(e_G)$ may NOT equal e_H.

EXAMPLE: $G = \mathbb{Z}$ and $H = \mathbb{Z} \times \mathbb{Z}$ are multiplicative monoids with $e_G = 1$ and $e_H = (1, 1)$. Consider

$$\begin{array}{ccccc} f & : & G = \mathbb{Z} & \longrightarrow & H = \mathbb{Z} \times \mathbb{Z} \\ & & a & \longmapsto & (a, 0) \end{array}$$

Homomorphisms vs Identities and Inverses

Remark. If G and H are groups with identities e_G and e_H respectively, and if $f : G \to H$ is a homomorphism, then

$$f(e_G)=e_H \text{ and } f(a^{-1})=f(a)^{-1}, \forall a \in G.$$

WARNING: If G and H are just monoids, not groups, $f(e_G)$ may NOT equal e_H.

EXAMPLE: $G = \mathbb{Z}$ and $H = \mathbb{Z} \times \mathbb{Z}$ are multiplicative monoids with $e_G = 1$ and $e_H = (1, 1)$. Consider

$$\begin{array}{ccccc} f & : & G = \mathbb{Z} & \longrightarrow & H = \mathbb{Z} \times \mathbb{Z} \\ & & a & \longmapsto & (a, 0) \end{array}$$

Then f is a homomorphism,

Homomorphisms vs Identities and Inverses

Remark. If G and H are groups with identities e_G and e_H respectively, and if $f : G \to H$ is a homomorphism, then

$$f(e_G)=e_H \text{ and } f(a^{-1})=f(a)^{-1}, \forall a \in G.$$

WARNING: If G and H are just monoids, not groups, $f(e_G)$ may NOT equal e_H.

EXAMPLE: $G = \mathbb{Z}$ and $H = \mathbb{Z} \times \mathbb{Z}$ are multiplicative monoids with $e_G = 1$ and $e_H = (1, 1)$. Consider

$$\begin{array}{ccccc} f & : & G = \mathbb{Z} & \longrightarrow & H = \mathbb{Z} \times \mathbb{Z} \\ & & a & \longmapsto & (a, 0) \end{array}$$

Then f is a homomorphism, but

Homomorphisms vs Identities and Inverses

Remark. If G and H are groups with identities e_G and e_H respectively, and if $f : G \to H$ is a homomorphism, then

$$f(e_G) = e_H \quad \text{and} \quad f(a^{-1}) = f(a)^{-1}, \forall a \in G.$$

WARNING: If G and H are just monoids, not groups, $f(e_G)$ may NOT equal e_H.

EXAMPLE: $G = \mathbb{Z}$ and $H = \mathbb{Z} \times \mathbb{Z}$ are multiplicative monoids with $e_G = 1$ and $e_H = (1, 1)$. Consider

$$\begin{array}{ccccc} f & : & G = \mathbb{Z} & \longrightarrow & H = \mathbb{Z} \times \mathbb{Z} \\ & & a & \longmapsto & (a, 0) \end{array}$$

Then f is a homomorphism, but

$$f(e_G) = f(1)$$

Homomorphisms vs Identities and Inverses

Remark. If G and H are groups with identities e_G and e_H respectively, and if $f : G \to H$ is a homomorphism, then

$$f(e_G)=e_H \text{ and } f(a^{-1})=f(a)^{-1}, \forall a \in G.$$

WARNING: If G and H are just monoids, not groups, $f(e_G)$ may NOT equal e_H.

EXAMPLE: $G = \mathbb{Z}$ and $H = \mathbb{Z} \times \mathbb{Z}$ are multiplicative monoids with $e_G = 1$ and $e_H = (1, 1)$. Consider

$$\begin{array}{ccccc} f & : & G = \mathbb{Z} & \longrightarrow & H = \mathbb{Z} \times \mathbb{Z} \\ & & a & \longmapsto & (a, 0) \end{array}$$

Then f is a homomorphism, but

$$f(e_G) = f(1) = (1, 0)$$

Homomorphisms vs Identities and Inverses

Remark. If G and H are groups with identities e_G and e_H respectively, and if $f : G \to H$ is a homomorphism, then

$$f(e_G)=e_H \text{ and } f(a^{-1})=f(a)^{-1}, \forall a \in G.$$

WARNING: If G and H are just monoids, not groups, $f(e_G)$ may NOT equal e_H.

EXAMPLE: $G = \mathbb{Z}$ and $H = \mathbb{Z} \times \mathbb{Z}$ are multiplicative monoids with $e_G = 1$ and $e_H = (1, 1)$. Consider

$$\begin{array}{ccccc} f & : & G = \mathbb{Z} & \longrightarrow & H = \mathbb{Z} \times \mathbb{Z} \\ & & a & \longmapsto & (a, 0) \end{array}$$

Then f is a homomorphism, but

$$f(e_G) = f(1) = (1, 0) \neq (1, 1) = e_H.$$

Definition (2.2)

Let $f : G \to H$ be a homomorphism of groups.

Definition (2.2)

Let $f : G \to H$ be a homomorphism of groups.

- The kernel of f is

Definition (2.2)

Let $f : G \to H$ be a homomorphism of groups.

- The kernel of f is $\mathrm{Ker}\ f$

Definition (2.2)

Let $f : G \to H$ be a homomorphism of groups.

- The kernel of f is $\operatorname{Ker} f = \{a \in G \mid f(a) = e_H\}$.

Definition (2.2)

Let $f : G \to H$ be a homomorphism of groups.

- The kernel of f is $\operatorname{Ker} f = \{a \in G \mid f(a) = e_H\}$.

Note that

Definition (2.2)

Let $f : G \to H$ be a homomorphism of groups.

- The kernel of f is $\operatorname{Ker} f = \{a \in G \mid f(a) = e_H\}$.

  Note that $f(e_G) = e_H$

Definition (2.2)

Let $f : G \to H$ be a homomorphism of groups.

- The kernel of f is $\operatorname{Ker} f = \{a \in G \mid f(a) = e_H\}$.

  Note that $f(e_G) = e_H \implies e_G \in \operatorname{Ker} f$.

Definition (2.2)

Let $f : G \to H$ be a homomorphism of groups.

- The kernel of f is $\operatorname{Ker} f = \{a \in G \mid f(a) = e \ \}$.

  Note that $f(e_G) = e_H \implies e_G \in \operatorname{Ker} f$.

Definition (2.2)

Let $f : G \to H$ be a homomorphism of groups.

- The kernel of f is $\operatorname{Ker} f = \{a \in G \mid f(a) = e \ \}$.

  Note that $f(e_G) = e_H \implies e_G \in \operatorname{Ker} f$.

- For a subset $A \subseteq G$,

Definition (2.2)

Let $f : G \to H$ be a homomorphism of groups.

- The kernel of f is $\operatorname{Ker} f = \{a \in G \mid f(a) = e \ \}$.

  Note that $f(e_G) = e_H \implies e_G \in \operatorname{Ker} f$.

- For a subset $A \subseteq G$, the image of A is

Definition (2.2)

Let $f : G \to H$ be a homomorphism of groups.

- The kernel of f is $\operatorname{Ker} f = \{a \in G \mid f(a) = e \ \}$.

  Note that $f(e_G) = e_H \implies e_G \in \operatorname{Ker} f$.

- For a subset $A \subseteq G$, the image of A is

  $f(A)$

Definition (2.2)

Let $f : G \to H$ be a homomorphism of groups.

- The kernel of f is $\operatorname{Ker} f = \{a \in G \mid f(a) = e \ \}$.

  Note that $f(e_G) = e_H \implies e_G \in \operatorname{Ker} f$.

- For a subset $A \subseteq G$, the image of A is

$$f(A) = \{b \in H \mid b = f(a) \text{ for some } a \in A\}$$

Definition (2.2)

Let $f : G \to H$ be a homomorphism of groups.

- The kernel of f is $\operatorname{Ker} f = \{a \in G \mid f(a) = e \ \}$.

  Note that $f(e_G) = e_H \implies e_G \in \operatorname{Ker} f$.

- For a subset $A \subseteq G$, the image of A is

$$f(A) = \{b \in H \mid b = f(a) \text{ for some } a \in A\}$$
$$= \{f(a) \mid a \in A\}.$$

Definition (2.2)

Let $f : G \to H$ be a homomorphism of groups.

- The kernel of f is $\operatorname{Ker} f = \{a \in G \mid f(a) = e \ \}$.

  Note that $f(e_G) = e_H \implies e_G \in \operatorname{Ker} f$.

- For a subset $A \subseteq G$, the image of A is

$$f(A) = \{b \in H \mid b = f(a) \text{ for some } a \in A\}$$
$$= \{f(a) \mid a \in A\}.$$

  $f(G)$ is called the image of f

Definition (2.2)

Let $f : G \to H$ be a homomorphism of groups.

- The kernel of f is $\operatorname{Ker} f = \{a \in G \mid f(a) = e \ \}$.

  Note that $f(e_G) = e_H \implies e_G \in \operatorname{Ker} f$.

- For a subset $A \subseteq G$, the image of A is

$$f(A) = \{b \in H \mid b = f(a) \text{ for some } a \in A\}$$
$$= \{f(a) \mid a \in A\}.$$

  $f(G)$ is called the image of f and denoted $\operatorname{Im} f$.

Definition (2.2)

Let $f : G \to H$ be a homomorphism of groups.

- The kernel of f is $\operatorname{Ker} f = \{a \in G \mid f(a) = e \ \}$.

  Note that $f(e_G) = e_H \implies e_G \in \operatorname{Ker} f$.

- For a subset $A \subseteq G$, the image of A is

$$f(A) = \{b \in H \mid b = f(a) \text{ for some } a \in A\}$$
$$= \{f(a) \mid a \in A\}.$$

  $f(G)$ is called the image of f and denoted $\operatorname{Im} f$.

  Note that

Definition (2.2)

Let $f : G \to H$ be a homomorphism of groups.

- The kernel of f is $\operatorname{Ker} f = \{a \in G \mid f(a) = e \ \}$.

  Note that $f(e_G) = e_H \implies e_G \in \operatorname{Ker} f$.

- For a subset $A \subseteq G$, the image of A is

$$f(A) = \{b \in H \mid b = f(a) \text{ for some } a \in A\}$$
$$= \{f(a) \mid a \in A\}.$$

  $f(G)$ is called the image of f and denoted $\operatorname{Im} f$.

  Note that $\operatorname{Im} f = H$

Definition (2.2)

Let $f : G \to H$ be a homomorphism of groups.

- The kernel of f is $\operatorname{Ker} f = \{a \in G \mid f(a) = e \ \}$.

  Note that $f(e_G) = e_H \implies e_G \in \operatorname{Ker} f$.

- For a subset $A \subseteq G$, the image of A is

$$f(A) = \{b \in H \mid b = f(a) \text{ for some } a \in A\}$$
$$= \{f(a) \mid a \in A\}.$$

  $f(G)$ is called the image of f and denoted $\operatorname{Im} f$.

  Note that $\operatorname{Im} f = H \iff f$ is onto.

Definition (2.2)

Let $f : G \to H$ be a homomorphism of groups.

- The kernel of f is $\operatorname{Ker} f = \{a \in G \mid f(a) = e \ \}$.

  Note that $f(e_G) = e_H \implies e_G \in \operatorname{Ker} f$.

- For a subset $A \subseteq G$, the image of A is

$$f(A) = \{b \in H \mid b = f(a) \text{ for some } a \in A\}$$
$$= \{f(a) \mid a \in A\}.$$

  $f(G)$ is called the image of f and denoted $\operatorname{Im} f$.

  Note that $\operatorname{Im} f = H \iff f$ is onto.

- For a subset $B \subseteq H$,

Definition (2.2)

Let $f : G \to H$ be a homomorphism of groups.

- The kernel of f is $\operatorname{Ker} f = \{a \in G \mid f(a) = e \ \}$.

  Note that $f(e_G) = e_H \implies e_G \in \operatorname{Ker} f$.

- For a subset $A \subseteq G$, the image of A is

$$f(A) = \{b \in H \mid b = f(a) \text{ for some } a \in A\}$$
$$= \{f(a) \mid a \in A\}.$$

  $f(G)$ is called the image of f and denoted $\operatorname{Im} f$.

  Note that $\operatorname{Im} f = H \iff f$ is onto.

- For a subset $B \subseteq H$, the inverse image

Definition (2.2)

Let $f : G \to H$ be a homomorphism of groups.

- The kernel of f is $\operatorname{Ker} f = \{a \in G \mid f(a) = e \ \}$.

  Note that $f(e_G) = e_H \implies e_G \in \operatorname{Ker} f$.

- For a subset $A \subseteq G$, the image of A is

$$f(A) = \{b \in H \mid b = f(a) \text{ for some } a \in A\}$$
$$= \{f(a) \mid a \in A\}.$$

  $f(G)$ is called the image of f and denoted $\operatorname{Im} f$.

  Note that $\operatorname{Im} f = H \iff f$ is onto.

- For a subset $B \subseteq H$, the inverse image or preimage of B is

Definition (2.2)

Let $f : G \to H$ be a homomorphism of groups.

- The kernel of f is $\operatorname{Ker} f = \{a \in G \mid f(a) = e \ \}$.

  Note that $f(e_G) = e_H \implies e_G \in \operatorname{Ker} f$.

- For a subset $A \subseteq G$, the image of A is

$$f(A) = \{b \in H \mid b = f(a) \text{ for some } a \in A\}$$
$$= \{f(a) \mid a \in A\}.$$

  $f(G)$ is called the image of f and denoted $\operatorname{Im} f$.

  Note that $\operatorname{Im} f = H \iff f$ is onto.

- For a subset $B \subseteq H$, the inverse image or preimage of B is

$$f^{-1}(B)$$

Definition (2.2)

Let $f : G \to H$ be a homomorphism of groups.

- The kernel of f is $\operatorname{Ker} f = \{a \in G \mid f(a) = e \ \}$.

  Note that $f(e_G) = e_H \implies e_G \in \operatorname{Ker} f$.

- For a subset $A \subseteq G$, the image of A is

$$f(A) = \{b \in H \mid b = f(a) \text{ for some } a \in A\}$$
$$= \{f(a) \mid a \in A\}.$$

  $f(G)$ is called the image of f and denoted $\operatorname{Im} f$.

  Note that $\operatorname{Im} f = H \iff f$ is onto.

- For a subset $B \subseteq H$, the inverse image or preimage of B is

$$f^{-1}(B) = \{a \in G \mid f(a) \in B\}.$$

Theorem (2.3)

Let $f : G \to H$ be a homomorphism of groups.

Theorem (2.3)

Let $f : G \to H$ be a homomorphism of groups. Then

- f is a monomorphism

Theorem (2.3)

Let $f : G \to H$ be a homomorphism of groups. Then

- f is a monomorphism $\iff$ $\mathrm{Ker}\, f = \{e\}$.

Theorem (2.3)

Let $f : G \to H$ be a homomorphism of groups. Then

- f is a monomorphism $\iff$ $\operatorname{Ker} f = \{e\}$.

Proof.

Theorem (2.3)

Let $f : G \to H$ be a homomorphism of groups. Then

- f is a monomorphism $\iff$ $\mathrm{Ker}\, f = \{e\}$.

Proof. "$\Rightarrow$":

Theorem (2.3)

Let $f : G \to H$ be a homomorphism of groups. Then

- f is a monomorphism $\iff$ $\mathrm{Ker}\, f = \{e\}$.

Proof. "$\Rightarrow$": We already see that $e \in \mathrm{Ker}\, f$ is always true.

Theorem (2.3)

Let $f : G \to H$ be a homomorphism of groups. Then

- f is a monomorphism $\iff \operatorname{Ker} f = \{e\}$.

Proof. "$\Rightarrow$": We already see that $e \in \operatorname{Ker} f$ is always true. Conversely,

Theorem (2.3)

Let $f : G \to H$ be a homomorphism of groups. Then

- f is a monomorphism $\iff \operatorname{Ker} f = \{e\}$.

Proof. "$\Rightarrow$": We already see that $e \in \operatorname{Ker} f$ is always true.
Conversely, $a \in \operatorname{Ker} f$

Theorem (2.3)

Let $f : G \to H$ be a homomorphism of groups. Then

- f is a monomorphism $\iff$ $\mathrm{Ker}\, f = \{e\}$.

Proof. "$\Rightarrow$": We already see that $e \in \mathrm{Ker}\, f$ is always true.
Conversely, $a \in \mathrm{Ker}\, f \implies f(a) = e$

Theorem (2.3)

Let $f : G \to H$ be a homomorphism of groups. Then

- f is a monomorphism $\iff \operatorname{Ker} f = \{e\}$.

Proof. "$\Rightarrow$": We already see that $e \in \operatorname{Ker} f$ is always true.
Conversely, $a \in \operatorname{Ker} f \implies f(a) = e = f(e)$

Theorem (2.3)

Let $f : G \to H$ be a homomorphism of groups. Then

- f is a monomorphism $\iff \operatorname{Ker} f = \{e\}$.

Proof. "$\Rightarrow$": We already see that $e \in \operatorname{Ker} f$ is always true.
Conversely, $a \in \operatorname{Ker} f \implies f(a) = e = f(e) \implies a = e$

because f is one-to-one

Theorem (2.3)

Let $f : G \to H$ be a homomorphism of groups. Then

- f is a monomorphism $\iff$ $\mathrm{Ker}\, f = \{e\}$.

Proof. "$\Rightarrow$": We already see that $e \in \mathrm{Ker}\, f$ is always true.
Conversely, $a \in \mathrm{Ker}\, f \implies f(a) = e = f(e) \implies a = e$

"$\Leftarrow$":

Theorem (2.3)

Let $f : G \to H$ be a homomorphism of groups. Then

- f is a monomorphism $\iff$ $\mathrm{Ker}\, f = \{e\}$.

Proof. "$\Rightarrow$": We already see that $e \in \mathrm{Ker}\, f$ is always true.
Conversely, $a \in \mathrm{Ker}\, f \implies f(a) = e = f(e) \implies a = e$

"$\Leftarrow$": $f(a) = f(b)$

Theorem (2.3)

Let $f : G \to H$ be a homomorphism of groups. Then

- f is a monomorphism $\iff \operatorname{Ker} f = \{e\}$.

Proof. "$\Rightarrow$": We already see that $e \in \operatorname{Ker} f$ is always true.
Conversely, $a \in \operatorname{Ker} f \implies f(a) = e = f(e) \implies a = e$

"$\Leftarrow$": $f(a) = f(b) \implies f(a)f(b)^{-1} = e$

Theorem (2.3)

Let $f : G \to H$ be a homomorphism of groups. Then

- f is a monomorphism $\iff \operatorname{Ker} f = \{e\}$.

Proof. "$\Rightarrow$": We already see that $e \in \operatorname{Ker} f$ is always true.
Conversely, $a \in \operatorname{Ker} f \implies f(a) = e = f(e) \implies a = e$

"$\Leftarrow$": $f(a) = f(b) \implies f(a)f(b)^{-1} = e$
$\implies f(a)f(b^{-1}) = e$

Theorem (2.3)

Let $f : G \to H$ be a homomorphism of groups. Then

- f is a monomorphism $\iff \operatorname{Ker} f = \{e\}$.

Proof. "$\Rightarrow$": We already see that $e \in \operatorname{Ker} f$ is always true.
Conversely, $a \in \operatorname{Ker} f \implies f(a) = e = f(e) \implies a = e$

"$\Leftarrow$": $f(a) = f(b) \implies f(a)f(b)^{-1} = e$
$\implies f(a)f(b^{-1}) = e$
$\implies f(ab^{-1}) = e$

Theorem (2.3)

Let $f : G \to H$ be a homomorphism of groups. Then

- f is a monomorphism $\iff \operatorname{Ker} f = \{e\}$.

Proof. "$\Rightarrow$": We already see that $e \in \operatorname{Ker} f$ is always true.
Conversely, $a \in \operatorname{Ker} f \implies f(a) = e = f(e) \implies a = e$

"$\Leftarrow$": $f(a) = f(b) \implies f(a)f(b)^{-1} = e$
$\implies f(a)f(b^{-1}) = e$
$\implies f(ab^{-1}) = e$
$\implies ab^{-1} \in \operatorname{Ker} f$

Theorem (2.3)

Let $f : G \to H$ be a homomorphism of groups. Then

- f is a monomorphism $\iff$ $\operatorname{Ker} f = \{e\}$.

Proof. "$\Rightarrow$": We already see that $e \in \operatorname{Ker} f$ is always true.
Conversely, $a \in \operatorname{Ker} f \implies f(a) = e = f(e) \implies a = e$

"$\Leftarrow$": $f(a) = f(b) \implies f(a)f(b)^{-1} = e$
$\implies f(a)f(b^{-1}) = e$
$\implies f(ab^{-1}) = e$
$\implies ab^{-1} \in \operatorname{Ker} f$
$\implies ab^{-1} = e$

Theorem (2.3)

Let $f : G \to H$ be a homomorphism of groups. Then

- f is a monomorphism $\iff$ $\operatorname{Ker} f = \{e\}$.

Proof. "$\Rightarrow$": We already see that $e \in \operatorname{Ker} f$ is always true.
Conversely, $a \in \operatorname{Ker} f \implies f(a) = e = f(e) \implies a = e$

"$\Leftarrow$": $f(a) = f(b) \implies f(a)f(b)^{-1} = e$

$$\begin{aligned}
&\implies f(a)f(b^{-1}) = e \\
&\implies f(ab^{-1}) = e \\
&\implies ab^{-1} \in \operatorname{Ker} f \\
&\implies ab^{-1} = e \\
&\implies a = b.
\end{aligned}$$

Theorem (2.3)

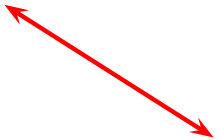
Let $f : G \to H$ be a homomorphism of groups. Then

- f is a monomorphism $\iff \operatorname{Ker} f = \{e\}$.
- f is an epimorphism $\iff \operatorname{Im} f = H$.

Theorem (2.3)

Let $f : G \to H$ be a homomorphism of groups. Then

- f is a monomorphism $\iff \operatorname{Ker} f = \{e\}$.
- f is an epimorphism $\iff \operatorname{Im} f = H$.



f is onto

Theorem (2.3)

Let $f : G \to H$ be a homomorphism of groups. Then

- f is a monomorphism $\iff \operatorname{Ker} f = \{e\}$.
- f is an epimorphism $\iff \operatorname{Im} f = H$.

f is onto

Theorem (2.3)

Let $f : G \to H$ be a homomorphism of groups. Then

- f is a monomorphism $\iff \operatorname{Ker} f = \{e\}$.
- f is an epimorphism $\iff \operatorname{Im} f = H$.
- f is an isomorphism $\iff$

Theorem (2.3)

Let $f : G \to H$ be a homomorphism of groups. Then

- f is a monomorphism $\iff \operatorname{Ker} f = \{e\}$.
- f is an epimorphism $\iff \operatorname{Im} f = H$.
- f is an isomorphism $\iff$ there is a homomorphism $f^{-1} : H \to G$ such that

Theorem (2.3)

Let $f : G \to H$ be a homomorphism of groups. Then

- f is a monomorphism $\iff \operatorname{Ker} f = \{e\}$.
- f is an epimorphism $\iff \operatorname{Im} f = H$.
- f is an isomorphism $\iff$ there is a homomorphism $f^{-1} : H \to G$ such that $f f^{-1} = 1_H$ and $f^{-1} f = 1_G$.

Theorem (2.3)

Let $f : G \to H$ be a homomorphism of groups. Then

- f is a monomorphism $\iff \operatorname{Ker} f = \{e\}$.
- f is an epimorphism $\iff \operatorname{Im} f = H$.
- f is an isomorphism $\iff$ there is a homomorphism $f^{-1} : H \to G$ such that $f f^{-1} = 1_H$ and $f^{-1} f = 1_G$.

Because

Theorem (2.3)

Let $f : G \to H$ be a homomorphism of groups. Then

- f is a monomorphism $\iff \operatorname{Ker} f = \{e\}$.
- f is an epimorphism $\iff \operatorname{Im} f = H$.
- f is an isomorphism $\iff$ there is a homomorphism $f^{-1} : H \to G$ such that $f f^{-1} = 1_H$ and $f^{-1} f = 1_G$.

Because f is bijective

$\iff \exists\, f^{-1} : H \to G$ such that $f f^{-1} = 1_H$ and $f^{-1} f = 1_G$,

Theorem (2.3)

Let $f : G \to H$ be a homomorphism of groups. Then

- f is a monomorphism $\iff \operatorname{Ker} f = \{e\}$.
- f is an epimorphism $\iff \operatorname{Im} f = H$.
- f is an isomorphism $\iff$ there is a homomorphism $f^{-1} : H \to G$ such that $f f^{-1} = 1_H$ and $f^{-1} f = 1_G$.

Because f is bijective

$\iff \exists\, f^{-1} : H \to G$ such that $f f^{-1} = 1_H$ and $f^{-1} f = 1_G$,

we only need to show that f^{-1} is homomorphic,

Theorem (2.3)

Let $f : G \to H$ be a homomorphism of groups. Then

- f is a monomorphism $\iff$ $\operatorname{Ker} f = \{e\}$.
- f is an epimorphism $\iff$ $\operatorname{Im} f = H$.
- f is an isomorphism $\iff$ there is a homomorphism $f^{-1} : H \to G$ such that $f f^{-1} = 1_H$ and $f^{-1} f = 1_G$.

Because f is bijective

$\iff$ $\exists\, f^{-1} : H \to G$ such that $f f^{-1} = 1_H$ and $f^{-1} f = 1_G$,

we only need to show that f^{-1} is homomorphic, i.e.,

$f^{-1}(a) f^{-1}(b) = f^{-1}(ab)$, for all $a, b \in H$.

Theorem (2.3)

Let $f : G \to H$ be a homomorphism of groups. Then

- f is a monomorphism $\iff \operatorname{Ker} f = \{e\}$.
- f is an epimorphism $\iff \operatorname{Im} f = H$.
- f is an isomorphism $\iff$ there is a homomorphism $f^{-1} : H \to G$ such that $f f^{-1} = 1_H$ and $f^{-1} f = 1_G$.

Because f is bijective

$\iff \exists\, f^{-1} : H \to G$ such that $f f^{-1} = 1_H$ and $f^{-1} f = 1_G$,

we only need to show that f^{-1} is homomorphic, i.e.,

$f^{-1}(a) f^{-1}(b) = f^{-1}(ab)$, for all $a, b \in H$.

Note that

Theorem (2.3)

Let $f : G \to H$ be a homomorphism of groups. Then

- f is a monomorphism $\iff \operatorname{Ker} f = \{e\}$.
- f is an epimorphism $\iff \operatorname{Im} f = H$.
- f is an isomorphism $\iff$ there is a homomorphism $f^{-1} : H \to G$ such that $f f^{-1} = 1_H$ and $f^{-1} f = 1_G$.

Because f is bijective

$\iff \exists\, f^{-1} : H \to G$ such that $f f^{-1} = 1_H$ and $f^{-1} f = 1_G$,

we only need to show that f^{-1} is homomorphic, i.e.,

$f^{-1}(a) f^{-1}(b) = f^{-1}(ab)$, for all $a, b \in H$.

Note that $f(f^{-1}(a) f^{-1}(b)) = f(f^{-1}(a)) f(f^{-1}(b))$

f is homomorphic

Theorem (2.3)

Let $f : G \to H$ be a homomorphism of groups. Then

- f is a monomorphism $\iff$ $\operatorname{Ker} f = \{e\}$.
- f is an epimorphism $\iff$ $\operatorname{Im} f = H$.
- f is an isomorphism $\iff$ there is a homomorphism $f^{-1} : H \to G$ such that $f f^{-1} = 1_H$ and $f^{-1} f = 1_G$.

Because f is bijective

$\iff \exists\, f^{-1} : H \to G$ such that $f f^{-1} = 1_H$ and $f^{-1} f = 1_G$,

we only need to show that f^{-1} is homomorphic, i.e.,

$f^{-1}(a) f^{-1}(b) = f^{-1}(ab)$, for all $a, b \in H$.

Note that $f(f^{-1}(a)f^{-1}(b)) = f(f^{-1}(a))f(f^{-1}(b)) = ab$.

$f f^{-1} = 1_H$

Theorem (2.3)

Let $f : G \to H$ be a homomorphism of groups. Then

- f is a monomorphism $\iff$ $\mathrm{Ker}\, f = \{e\}$.
- f is an epimorphism $\iff$ $\mathrm{Im}\, f = H$.
- f is an isomorphism $\iff$ there is a homomorphism $f^{-1} : H \to G$ such that $f f^{-1} = 1_H$ and $f^{-1} f = 1_G$.

Because f is bijective

$\iff \exists\, f^{-1} : H \to G$ such that $f f^{-1} = 1_H$ and $f^{-1} f = 1_G$,

we only need to show that f^{-1} is homomorphic, i.e.,

$f^{-1}(a) f^{-1}(b) = f^{-1}(ab)$, for all $a, b \in H$.

Note that $f(f^{-1}(a)f^{-1}(b)) = f(f^{-1}(a))f(f^{-1}(b)) = ab$.

Hence, by the definition of f^{-1},

Theorem (2.3)

Let $f : G \to H$ be a homomorphism of groups. Then

- f is a monomorphism $\iff$ $\mathrm{Ker}\, f = \{e\}$.
- f is an epimorphism $\iff$ $\mathrm{Im}\, f = H$.
- f is an isomorphism $\iff$ there is a homomorphism $f^{-1} : H \to G$ such that $f f^{-1} = 1_H$ and $f^{-1} f = 1_G$.

Because f is bijective

$\iff \exists\, f^{-1} : H \to G$ such that $f f^{-1} = 1_H$ and $f^{-1} f = 1_G$,

we only need to show that f^{-1} is homomorphic, i.e.,

$f^{-1}(a) f^{-1}(b) = f^{-1}(ab)$, for all $a, b \in H$.

Note that $f(f^{-1}(a)f^{-1}(b)) = f(f^{-1}(a))f(f^{-1}(b)) = ab$.

Hence, by the definition of f^{-1}, we get $f^{-1}(a)f^{-1}(b) = f^{-1}(ab)$.

Subgroups

Remark. Let G be a semigroup

Subgroups

Remark. Let G be a semigroup and let H be a nonempty subset of G.

Subgroups

Remark. Let G be a semigroup and let H be a nonempty subset of G. We say that H is closed under the product in G

Subgroups

Remark. Let G be a semigroup and let H be a nonempty subset of G. We say that H is closed under the product in G if $\forall a, b \in H, ab \in H$.

Subgroups

Remark. Let G be a semigroup and let H be a nonempty subset of G. We say that H is closed under the product in G if $\forall a, b \in H$, $ab \in H$. This means that the binary operation on G,

Subgroups

Remark. Let G be a semigroup and let H be a nonempty subset of G. We say that H is closed under the product in G if $\forall a, b \in H$, $ab \in H$. This means that the binary operation on G, when restricted to H,

Subgroups

Remark. Let G be a semigroup and let H be a nonempty subset of G. We say that H is closed under the product in G if $\forall a, b \in H$, $ab \in H$. This means that the binary operation on G, when restricted to H, is in fact a binary operation on H.

Subgroups

Remark. Let G be a semigroup and let H be a nonempty subset of G. We say that H is closed under the product in G if $\forall a, b \in H$, $ab \in H$. This means that the binary operation on G, when restricted to H, is in fact a binary operation on H.

Definition (2.4)**.** Let G be a group.

Subgroups

Remark. Let G be a semigroup and let H be a nonempty subset of G. We say that H is closed under the product in G if $\forall a, b \in H$, $ab \in H$. This means that the binary operation on G, when restricted to H, is in fact a binary operation on H.

Definition (2.4)**.** Let G be a group.

- Let H be a nonempty subset.

Subgroups

Remark. Let G be a semigroup and let H be a nonempty subset of G. We say that H is closed under the product in G if $\forall a, b \in H$, $ab \in H$. This means that the binary operation on G, when restricted to H, is in fact a binary operation on H.

Definition (2.4)**.** Let G be a group.

- Let H be a nonempty subset. If H is closed under the product in G

Subgroups

Remark. Let G be a semigroup and let H be a nonempty subset of G. We say that H is closed under the product in G if $\forall a, b \in H$, $ab \in H$. This means that the binary operation on G, when restricted to H, is in fact a binary operation on H.

Definition (2.4)**.** Let G be a group.

- Let H be a nonempty subset. If H is closed under the product in G and if H is a group under the product in G,

Subgroups

Remark. Let G be a semigroup and let H be a nonempty subset of G. We say that H is closed under the product in G if $\forall a, b \in H$, $ab \in H$. This means that the binary operation on G, when restricted to H, is in fact a binary operation on H.

Definition (2.4)**.** Let G be a group.

- Let H be a nonempty subset. If H is closed under the product in G and if H is a group under the product in G, H is called a subgroup of G

Subgroups

Remark. Let G be a semigroup and let H be a nonempty subset of G. We say that H is closed under the product in G if $\forall a, b \in H$, $ab \in H$. This means that the binary operation on G, when restricted to H, is in fact a binary operation on H.

Definition (2.4)**.** Let G be a group.

- Let H be a nonempty subset. If H is closed under the product in G and if H is a group under the product in G, H is called a subgroup of G and we write $H \leq G$.

Subgroups

Remark. Let G be a semigroup and let H be a nonempty subset of G. We say that H is closed under the product in G if $\forall a, b \in H$, $ab \in H$. This means that the binary operation on G, when restricted to H, is in fact a binary operation on H.

Definition (2.4)**.** Let G be a group.

- Let H be a nonempty subset. If H is closed under the product in G and if H is a group under the product in G, H is called a subgroup of G and we write $H \leq G$.
- If G is nontrivial,

Subgroups

Remark. Let G be a semigroup and let H be a nonempty subset of G. We say that H is closed under the product in G if $\forall a, b \in H$, $ab \in H$. This means that the binary operation on G, when restricted to H, is in fact a binary operation on H.

Definition (2.4)**.** Let G be a group.

- Let H be a nonempty subset. If H is closed under the product in G and if H is a group under the product in G, H is called a subgroup of G and we write $H \leq G$.
- If G is nontrivial, i.e., $G \neq \{e\}$,

Subgroups

Remark. Let G be a semigroup and let H be a nonempty subset of G. We say that H is closed under the product in G if $\forall a, b \in H$, $ab \in H$. This means that the binary operation on G, when restricted to H, is in fact a binary operation on H.

Definition (2.4)**.** Let G be a group.

- Let H be a nonempty subset. If H is closed under the product in G and if H is a group under the product in G, H is called a subgroup of G and we write $H \leq G$.
- If G is nontrivial, i.e., $G \neq \{e\}$, then G has at least two subgroups,

Subgroups

Remark. Let G be a semigroup and let H be a nonempty subset of G. We say that H is closed under the product in G if $\forall a, b \in H$, $ab \in H$. This means that the binary operation on G, when restricted to H, is in fact a binary operation on H.

Definition (2.4)**.** Let G be a group.

- Let H be a nonempty subset. If H is closed under the product in G and if H is a group under the product in G, H is called a subgroup of G and we write $H \leq G$.
- If G is nontrivial, i.e., $G \neq \{e\}$, then G has at least two subgroups, namely G itself

Subgroups

Remark. Let G be a semigroup and let H be a nonempty subset of G. We say that H is closed under the product in G if $\forall a, b \in H$, $ab \in H$. This means that the binary operation on G, when restricted to H, is in fact a binary operation on H.

Definition (2.4)**.** Let G be a group.

- Let H be a nonempty subset. If H is closed under the product in G and if H is a group under the product in G, H is called a subgroup of G and we write $H \leq G$.
- If G is nontrivial, i.e., $G \neq \{e\}$, then G has at least two subgroups, namely G itself and the trivial subgroup $\{e\}$.

Subgroups

Remark. Let G be a semigroup and let H be a nonempty subset of G. We say that H is closed under the product in G if $\forall a, b \in H$, $ab \in H$. This means that the binary operation on G, when restricted to H, is in fact a binary operation on H.

Definition (2.4)**.** Let G be a group.

- Let H be a nonempty subset. If H is closed under the product in G and if H is a group under the product in G, H is called a subgroup of G and we write $H \leq G$.
- If G is nontrivial, i.e., $G \neq \{e\}$, then G has at least two subgroups, namely G itself and the trivial subgroup $\{e\}$.
- A subgroup H of G is called a proper subgroup

Subgroups

Remark. Let G be a semigroup and let H be a nonempty subset of G. We say that H is closed under the product in G if $\forall a, b \in H$, $ab \in H$. This means that the binary operation on G, when restricted to H, is in fact a binary operation on H.

Definition (2.4)**.** Let G be a group.

- Let H be a nonempty subset. If H is closed under the product in G and if H is a group under the product in G, H is called a subgroup of G and we write $H \leq G$.
- If G is nontrivial, i.e., $G \neq \{e\}$, then G has at least two subgroups, namely G itself and the trivial subgroup $\{e\}$.
- A subgroup H of G is called a proper subgroup if $\{e\} \neq H \neq G$.

Subgroups

Remark. Let G be a semigroup and let H be a nonempty subset of G. We say that H is closed under the product in G if $\forall a, b \in H$, $ab \in H$. This means that the binary operation on G, when restricted to H, is in fact a binary operation on H.

Definition (2.4)**.** Let G be a group.

- Let H be a nonempty subset. If H is closed under the product in G and if H is a group under the product in G, H is called a subgroup of G and we write $H \leq G$.
- If G is nontrivial, i.e., $G \neq \{e\}$, then G has at least two subgroups, namely G itself and the trivial subgroup $\{e\}$.
- A subgroup H of G is called a proper subgroup if $\{e\} \neq H \neq G$.

Theorem (2.5)

Let H be a nonempty subset of a group G.

Theorem (2.5)

Let H be a nonempty subset of a group G.

Then H is a subgroup of G

Theorem (2.5)

Let H be a nonempty subset of a group G.

Then H is a subgroup of $G \iff ab^{-1} \in H, \forall a, b \in H$.

Theorem (2.5)

Let H be a nonempty subset of a group G.

Then H is a subgroup of $G \iff ab^{-1} \in H, \forall a, b \in H$.

Proof. We need to show

Theorem (2.5)

Let H be a nonempty subset of a group G.

Then H is a subgroup of $G \iff ab^{-1} \in H, \forall a, b \in H$.

Proof. We need to show

$$\left.\begin{array}{l} (1)\ ab \in H \quad \forall a, b \in H \\ (2)\ e \in H \\ (3)\ a^{-1} \in H \quad \forall a \in H \end{array}\right\} \iff (4)\ ab^{-1} \in H, \forall a, b \in H.$$

Theorem (2.5)

Let H be a nonempty subset of a group G.

Then H is a subgroup of $G \iff ab^{-1} \in H, \forall a, b \in H$.

Proof. We need to show

$$\left.\begin{array}{l} (1)\ ab \in H \quad \forall a, b \in H \\ (2)\ e \in H \\ (3)\ a^{-1} \in H \quad \forall a \in H \end{array}\right\} \iff (4)\ ab^{-1} \in H, \forall a, b \in H.$$

"$\Rightarrow$":

Theorem (2.5)

Let H be a nonempty subset of a group G.

Then H is a subgroup of $G \iff ab^{-1} \in H, \forall a, b \in H$.

Proof. We need to show

$$\left.\begin{array}{l} (1)\ ab \in H \quad \forall a, b \in H \\ (2)\ e \in H \\ (3)\ a^{-1} \in H \quad \forall a \in H \end{array}\right\} \iff (4)\ ab^{-1} \in H, \forall a, b \in H.$$

"$\Rightarrow$": $a, b \in H \implies a, b^{-1} \in H$

because (3)

Theorem (2.5)

Let H be a nonempty subset of a group G.

Then H is a subgroup of $G \iff ab^{-1} \in H, \forall a, b \in H$.

Proof. We need to show

$$\left.\begin{array}{l} (1)\ ab \in H \quad \forall a, b \in H \\ (2)\ e \in H \\ (3)\ a^{-1} \in H \quad \forall a \in H \end{array}\right\} \iff (4)\ ab^{-1} \in H, \forall a, b \in H.$$

"$\Rightarrow$": $a, b \in H \implies a, b^{-1} \in H \implies ab^{-1} \in H$.

because (1)

Theorem (2.5)

Let H be a nonempty subset of a group G.

Then H is a subgroup of $G \iff ab^{-1} \in H, \forall a, b \in H$.

Proof. We need to show

$$\left.\begin{array}{l} (1)\ ab \in H \quad \forall a, b \in H \\ (2)\ e \in H \\ (3)\ a^{-1} \in H \quad \forall a \in H \end{array}\right\} \iff (4)\ ab^{-1} \in H, \forall a, b \in H.$$

"$\Rightarrow$": $a, b \in H \implies a, b^{-1} \in H \implies ab^{-1} \in H$.

"$\Leftarrow$":

Theorem (2.5)

Let H be a nonempty subset of a group G.

Then H is a subgroup of $G \iff ab^{-1} \in H, \forall a, b \in H$.

Proof. We need to show

$$\left.\begin{array}{l} (1)\ ab \in H \quad \forall a, b \in H \\ (2)\ e \in H \\ (3)\ a^{-1} \in H \quad \forall a \in H \end{array}\right\} \iff (4)\ ab^{-1} \in H, \forall a, b \in H.$$

"$\Rightarrow$": $a, b \in H \implies a, b^{-1} \in H \implies ab^{-1} \in H$.

"$\Leftarrow$": Because $H \neq \varnothing$,

Theorem (2.5)

Let H be a nonempty subset of a group G.

Then H is a subgroup of $G \iff ab^{-1} \in H, \forall a, b \in H$.

Proof. We need to show

$$\left.\begin{array}{l} (1)\ ab \in H \quad \forall a, b \in H \\ (2)\ e \in H \\ (3)\ a^{-1} \in H \quad \forall a \in H \end{array}\right\} \iff (4)\ ab^{-1} \in H, \forall a, b \in H.$$

"$\Rightarrow$": $a, b \in H \implies a, b^{-1} \in H \implies ab^{-1} \in H$.

"$\Leftarrow$": Because $H \neq \varnothing$, $\exists a \in H$.

Theorem (2.5)

Let H be a nonempty subset of a group G.

Then H is a subgroup of $G \iff ab^{-1} \in H, \forall a, b \in H$.

Proof. We need to show

$$\left.\begin{array}{l} (1)\ ab \in H \quad \forall a, b \in H \\ (2)\ e \in H \\ (3)\ a^{-1} \in H \quad \forall a \in H \end{array}\right\} \iff (4)\ ab^{-1} \in H, \forall a, b \in H.$$

"$\Rightarrow$": $a, b \in H \implies a, b^{-1} \in H \implies ab^{-1} \in H$.

"$\Leftarrow$": Because $H \neq \varnothing$, $\exists a \in H$. Then $e = aa^{-1} \in H$

because (4)

Theorem (2.5)

Let H be a nonempty subset of a group G.

Then H is a subgroup of $G \iff ab^{-1} \in H, \forall a, b \in H$.

Proof. We need to show

$$\left.\begin{array}{l} (1)\ ab \in H \quad \forall a, b \in H \\ (2)\ e \in H \\ (3)\ a^{-1} \in H \quad \forall a \in H \end{array}\right\} \iff (4)\ ab^{-1} \in H, \forall a, b \in H.$$

"$\Rightarrow$": $a, b \in H \implies a, b^{-1} \in H \implies ab^{-1} \in H$.

"$\Leftarrow$": Because $H \neq \varnothing$, $\exists a \in H$. Then $e = aa^{-1} \in H$ and this proves (2).

Theorem (2.5)

Let H be a nonempty subset of a group G.

Then H is a subgroup of $G \iff ab^{-1} \in H, \forall a, b \in H$.

Proof. We need to show

$$\left.\begin{array}{l} (1)\ ab \in H \quad \forall a, b \in H \\ (2)\ e \in H \\ (3)\ a^{-1} \in H \quad \forall a \in H \end{array}\right\} \iff (4)\ ab^{-1} \in H, \forall a, b \in H.$$

"$\Rightarrow$": $a, b \in H \implies a, b^{-1} \in H \implies ab^{-1} \in H$.

"$\Leftarrow$": Because $H \neq \varnothing$, $\exists a \in H$. Then $e = aa^{-1} \in H$ and this proves (2). Next, $a \in H \implies e, a \in H$

because (2) $e \in H$

Theorem (2.5)

Let H be a nonempty subset of a group G.

Then H is a subgroup of $G \iff ab^{-1} \in H, \forall a, b \in H$.

Proof. We need to show

$$\left.\begin{array}{l} (1)\ ab \in H \quad \forall a, b \in H \\ (2)\ e \in H \\ (3)\ a^{-1} \in H \quad \forall a \in H \end{array}\right\} \iff (4)\ ab^{-1} \in H, \forall a, b \in H.$$

"$\Rightarrow$": $a, b \in H \implies a, b^{-1} \in H \implies ab^{-1} \in H$.

"$\Leftarrow$": Because $H \neq \varnothing$, $\exists a \in H$. Then $e = aa^{-1} \in H$ and this proves (2). Next, $a \in H \implies e, a \in H \implies a^{-1} = ea^{-1} \in H$.

because (4)

Theorem (2.5)

Let H be a nonempty subset of a group G.

Then H is a subgroup of $G \iff ab^{-1} \in H, \forall a, b \in H$.

Proof. We need to show

$$\left.\begin{array}{l} (1)\ ab \in H \quad \forall a, b \in H \\ (2)\ e \in H \\ (3)\ a^{-1} \in H \quad \forall a \in H \end{array}\right\} \iff (4)\ ab^{-1} \in H, \forall a, b \in H.$$

"$\Rightarrow$": $a, b \in H \implies a, b^{-1} \in H \implies ab^{-1} \in H$.

"$\Leftarrow$": Because $H \neq \varnothing$, $\exists a \in H$. Then $e = aa^{-1} \in H$ and this proves (2). Next, $a \in H \implies e, a \in H \implies a^{-1} = ea^{-1} \in H$. This shows (3).

Theorem (2.5)

Let H be a nonempty subset of a group G.

Then H is a subgroup of $G \iff ab^{-1} \in H, \forall a, b \in H$.

Proof. We need to show

$$\left.\begin{array}{l} (1)\ ab \in H \quad \forall a, b \in H \\ (2)\ e \in H \\ (3)\ a^{-1} \in H \quad \forall a \in H \end{array}\right\} \iff (4)\ ab^{-1} \in H, \forall a, b \in H.$$

"$\Rightarrow$": $a, b \in H \implies a, b^{-1} \in H \implies ab^{-1} \in H$.

"$\Leftarrow$": Because $H \neq \varnothing$, $\exists a \in H$. Then $e = aa^{-1} \in H$ and this proves (2). Next, $a \in H \implies e, a \in H \implies a^{-1} = ea^{-1} \in H$. This shows (3). Finally,

Theorem (2.5)

Let H be a nonempty subset of a group G.

Then H is a subgroup of $G \iff ab^{-1} \in H, \forall a, b \in H$.

Proof. We need to show

$$\left.\begin{array}{l} (1)\ ab \in H \quad \forall a, b \in H \\ (2)\ e \in H \\ (3)\ a^{-1} \in H \quad \forall a \in H \end{array}\right\} \iff (4)\ ab^{-1} \in H, \forall a, b \in H.$$

"$\Rightarrow$": $a, b \in H \implies a, b^{-1} \in H \implies ab^{-1} \in H$.

"$\Leftarrow$": Because $H \neq \varnothing$, $\exists a \in H$. Then $e = aa^{-1} \in H$ and this proves (2). Next, $a \in H \implies e, a \in H \implies a^{-1} = ea^{-1} \in H$. This shows (3). Finally, $a, b \in H \implies a, b^{-1} \in H$

because (3)

Theorem (2.5)

Let H be a nonempty subset of a group G.

Then H is a subgroup of $G \iff ab^{-1} \in H, \forall a, b \in H$.

Proof. We need to show

$$\left.\begin{array}{l} (1)\ ab \in H \quad \forall a, b \in H \\ (2)\ e \in H \\ (3)\ a^{-1} \in H \quad \forall a \in H \end{array}\right\} \iff (4)\ ab^{-1} \in H, \forall a, b \in H.$$

"$\Rightarrow$": $a, b \in H \implies a, b^{-1} \in H \implies ab^{-1} \in H$.

"$\Leftarrow$": Because $H \neq \varnothing$, $\exists a \in H$. Then $e = aa^{-1} \in H$ and this proves (2). Next, $a \in H \implies e, a \in H \implies a^{-1} = ea^{-1} \in H$. This shows (3). Finally, $a, b \in H \implies a, b^{-1} \in H \implies$ $ab = a(b^{-1})^{-1} \in H$.

because (4)

Theorem (2.5)

Let H be a nonempty subset of a group G.

Then H is a subgroup of $G \iff ab^{-1} \in H, \forall a, b \in H$.

Proof. We need to show

$$\left.\begin{array}{l} (1)\ ab \in H \quad \forall a, b \in H \\ (2)\ e \in H \\ (3)\ a^{-1} \in H \quad \forall a \in H \end{array}\right\} \iff (4)\ ab^{-1} \in H, \forall a, b \in H.$$

"$\Rightarrow$": $a, b \in H \implies a, b^{-1} \in H \implies ab^{-1} \in H$.

"$\Leftarrow$": Because $H \neq \varnothing$, $\exists a \in H$. Then $e = aa^{-1} \in H$ and this proves (2). Next, $a \in H \implies e, a \in H \implies a^{-1} = ea^{-1} \in H$. This shows (3). Finally, $a, b \in H \implies a, b^{-1} \in H \implies$ $ab = a(b^{-1})^{-1} \in H$. This shows (1).

Theorem (2.5)

Let H be a nonempty subset of a group G.

Then H is a subgroup of $G \iff ab^{-1} \in H, \forall a, b \in H$.

Corollary (2.6)**.** If G is a group

Theorem (2.5)

Let H be a nonempty subset of a group G.
Then H is a subgroup of $G \iff ab^{-1} \in H, \forall a, b \in H$.

Corollary (2.6)**.** If G is a group and if $\{H_i \mid i \in I\}$ is a family of subgroups of G,

Theorem (2.5)

Let H be a nonempty subset of a group G.
Then H is a subgroup of $G \iff ab^{-1} \in H, \forall a, b \in H$.

Corollary (2.6)**.** If G is a group and if $\{H_i \mid i \in I\}$ is a family of subgroups of G, then $\bigcap_{i \in I} H_i$ is a subgroup of G.

Theorem (2.5)

Let H be a nonempty subset of a group G.
Then H is a subgroup of $G \iff ab^{-1} \in H, \forall a, b \in H$.

Corollary (2.6)**.** If G is a group and if $\{H_i \mid i \in I\}$ is a family of subgroups of G, then $\bigcap_{i \in I} H_i$ is a subgroup of G.

Proof.

Theorem (2.5)

Let H be a nonempty subset of a group G.
Then H is a subgroup of $G \iff ab^{-1} \in H, \forall a, b \in H$.

Corollary (2.6)**.** If G is a group and if $\{H_i \mid i \in I\}$ is a family of subgroups of G, then $\bigcap_{i \in I} H_i$ is a subgroup of G.

Proof. Because $e \in H_i$ for all $i \in I$,

Theorem (2.5)

Let H be a nonempty subset of a group G.
Then H is a subgroup of $G \iff ab^{-1} \in H, \forall a, b \in H$.

Corollary (2.6)**.** If G is a group and if $\{H_i \mid i \in I\}$ is a family of subgroups of G, then $\bigcap_{i \in I} H_i$ is a subgroup of G.

Proof. Because $e \in H_i$ for all $i \in I$, $e \in H$

Theorem (2.5)

Let H be a nonempty subset of a group G.
Then H is a subgroup of $G \iff ab^{-1} \in H, \forall a, b \in H$.

Corollary (2.6)**.** If G is a group and if $\{H_i \mid i \in I\}$ is a family of subgroups of G, then $\bigcap_{i \in I} H_i$ is a subgroup of G.

Proof. Because $e \in H_i$ for all $i \in I$, $e \in H$ and so $H \neq \varnothing$.

Theorem (2.5)

Let H be a nonempty subset of a group G.
Then H is a subgroup of $G \iff ab^{-1} \in H, \forall a, b \in H$.

Corollary (2.6)**.** If G is a group and if $\{H_i \mid i \in I\}$ is a family of subgroups of G, then $\bigcap_{i \in I} H_i$ is a subgroup of G.

Proof. Because $e \in H_i$ for all $i \in I$, $e \in H$ and so $H \neq \varnothing$.
Moreover, $a, b \in H$

Theorem (2.5)

Let H be a nonempty subset of a group G.
Then H is a subgroup of $G \iff ab^{-1} \in H, \forall a, b \in H$.

Corollary (2.6)**.** If G is a group and if $\{H_i \mid i \in I\}$ is a family of subgroups of G, then $\bigcap_{i \in I} H_i$ is a subgroup of G.

Proof. Because $e \in H_i$ for all $i \in I$, $e \in H$ and so $H \neq \varnothing$.
Moreover, $a, b \in H \implies a, b \in H_i, \ \forall i \in I$

Theorem (2.5)

Let H be a nonempty subset of a group G.
Then H is a subgroup of $G \iff ab^{-1} \in H, \forall a, b \in H$.

Corollary (2.6). If G is a group and if $\{H_i \mid i \in I\}$ is a family of subgroups of G, then $\bigcap_{i \in I} H_i$ is a subgroup of G.

Proof. Because $e \in H_i$ for all $i \in I$, $e \in H$ and so $H \neq \varnothing$.
Moreover, $a, b \in H \implies a, b \in H_i, \ \forall i \in I$
$\implies ab^{-1} \in H_i, \ \forall i \in I$

Theorem (2.5)

Let H be a nonempty subset of a group G.
Then H is a subgroup of $G \iff ab^{-1} \in H, \forall a, b \in H$.

Corollary (2.6)**.** If G is a group and if $\{H_i \mid i \in I\}$ is a family of subgroups of G, then $\bigcap_{i \in I} H_i$ is a subgroup of G.

Proof. Because $e \in H_i$ for all $i \in I$, $e \in H$ and so $H \neq \varnothing$.
Moreover, $a, b \in H \implies a, b \in H_i, \ \forall i \in I$
$\implies ab^{-1} \in H_i, \ \forall i \in I$
$\implies ab^{-1} \in H.$

Theorem (2.5)

Let H be a nonempty subset of a group G.
Then H is a subgroup of $G \iff ab^{-1} \in H, \forall a, b \in H$.

Corollary (2.6). If G is a group and if $\{H_i \mid i \in I\}$ is a family of subgroups of G, then $\bigcap_{i \in I} H_i$ is a subgroup of G.

Proof. Because $e \in H_i$ for all $i \in I$, $e \in H$ and so $H \neq \varnothing$.
Moreover, $a, b \in H \implies a, b \in H_i, \ \forall i \in I$
$\implies ab^{-1} \in H_i, \ \forall i \in I$
$\implies ab^{-1} \in H.$
Hence, by Theorem (2.5), H is a subgroup of G.

Example

Let $f : G \to H$ be a homomorphism of groups.

Example

Let $f : G \to H$ be a homomorphism of groups.

- If A is a subgroup of G, then $f(A)$ is a subgroup of H.

Example

Let $f : G \to H$ be a homomorphism of groups.

- If A is a subgroup of G, then $f(A)$ is a subgroup of H.

Proof. Note that

Example

Let $f : G \to H$ be a homomorphism of groups.

- If A is a subgroup of G, then $f(A)$ is a subgroup of H.

Proof. Note that $f(A) = \{f(a) \mid a \in A\}$.

Example

Let $f : G \to H$ be a homomorphism of groups.

- If A is a subgroup of G, then $f(A)$ is a subgroup of H.

Proof. Note that $f(A) = \{f(a) \mid a \in A\}$. Since A is a subgroup of G,

Example

Let $f : G \to H$ be a homomorphism of groups.

- If A is a subgroup of G, then $f(A)$ is a subgroup of H.

Proof. Note that $f(A) = \{f(a) \mid a \in A\}$. Since A is a subgroup of G, $A \neq \varnothing$

Example

Let $f : G \to H$ be a homomorphism of groups.

- If A is a subgroup of G, then $f(A)$ is a subgroup of H.

Proof. Note that $f(A) = \{f(a) \mid a \in A\}$. Since A is a subgroup of G, $A \neq \varnothing$ and so $f(A) \neq \varnothing$.

Example

Let $f : G \to H$ be a homomorphism of groups.

- If A is a subgroup of G, then $f(A)$ is a subgroup of H.

Proof. Note that $f(A) = \{f(a) \mid a \in A\}$. Since A is a subgroup of G, $A \neq \varnothing$ and so $f(A) \neq \varnothing$. Moreover,

Example

Let $f : G \to H$ be a homomorphism of groups.

- If A is a subgroup of G, then $f(A)$ is a subgroup of H.

Proof. Note that $f(A) = \{f(a) \mid a \in A\}$. Since A is a subgroup of G, $A \neq \varnothing$ and so $f(A) \neq \varnothing$. Moreover,

$\alpha, \beta \in f(A)$

Example

Let $f : G \to H$ be a homomorphism of groups.

- If A is a subgroup of G, then $f(A)$ is a subgroup of H.

Proof. Note that $f(A) = \{f(a) \mid a \in A\}$. Since A is a subgroup of G, $A \neq \varnothing$ and so $f(A) \neq \varnothing$. Moreover,

$$\alpha, \beta \in f(A) \implies \alpha = f(a) \text{ and } \beta = f(b) \text{ for some } a, b \in A$$

Example

Let $f : G \to H$ be a homomorphism of groups.

- If A is a subgroup of G, then $f(A)$ is a subgroup of H.

Proof. Note that $f(A) = \{f(a) \mid a \in A\}$. Since A is a subgroup of G, $A \neq \varnothing$ and so $f(A) \neq \varnothing$. Moreover,

$$\alpha, \beta \in f(A) \implies \alpha = f(a) \text{ and } \beta = f(b) \text{ for some } a, b \in A$$
$$\implies \alpha\beta^{-1} = f(a)f(b)^{-1}$$

Example

Let $f : G \to H$ be a homomorphism of groups.

- If A is a subgroup of G, then $f(A)$ is a subgroup of H.

Proof. Note that $f(A) = \{f(a) \mid a \in A\}$. Since A is a subgroup of G, $A \neq \varnothing$ and so $f(A) \neq \varnothing$. Moreover,

$$\alpha, \beta \in f(A) \implies \alpha = f(a) \text{ and } \beta = f(b) \text{ for some } a, b \in A$$
$$\implies \alpha\beta^{-1} = f(a)f(b)^{-1} = f(ab^{-1})$$

because f is homomorphic

Example

Let $f : G \to H$ be a homomorphism of groups.

- If A is a subgroup of G, then $f(A)$ is a subgroup of H.

Proof. Note that $f(A) = \{f(a) \mid a \in A\}$. Since A is a subgroup of G, $A \neq \varnothing$ and so $f(A) \neq \varnothing$. Moreover,

$$\alpha, \beta \in f(A) \implies \alpha = f(a) \text{ and } \beta = f(b) \text{ for some } a, b \in A$$
$$\implies \alpha\beta^{-1} = f(a)f(b)^{-1} = f(ab^{-1}) \in f(A).$$

because A is a subgroup

Example

Let $f : G \to H$ be a homomorphism of groups.

- If A is a subgroup of G, then $f(A)$ is a subgroup of H.

Proof. Note that $f(A) = \{f(a) \mid a \in A\}$. Since A is a subgroup of G, $A \neq \varnothing$ and so $f(A) \neq \varnothing$. Moreover,

$$\alpha, \beta \in f(A) \implies \alpha = f(a) \text{ and } \beta = f(b) \text{ for some } a, b \in A$$
$$\implies \alpha\beta^{-1} = f(a)f(b)^{-1} = f(ab^{-1}) \in f(A).$$

Hence by Theorem (2.5),

Example

Let $f : G \to H$ be a homomorphism of groups.

- If A is a subgroup of G, then $f(A)$ is a subgroup of H.

Proof. Note that $f(A) = \{f(a) \mid a \in A\}$. Since A is a subgroup of G, $A \neq \varnothing$ and so $f(A) \neq \varnothing$. Moreover,

$$\alpha, \beta \in f(A) \implies \alpha = f(a) \text{ and } \beta = f(b) \text{ for some } a, b \in A$$
$$\implies \alpha\beta^{-1} = f(a)f(b)^{-1} = f(ab^{-1}) \in f(A).$$

Hence by Theorem (2.5), $f(A)$ is a subgroup of H.

Example

Let $f : G \to H$ be a homomorphism of groups.

- If A is a subgroup of G, then $f(A)$ is a subgroup of H.
  In particular, $\mathrm{Im}\, f$ is a subgroup of H.

Proof. Note that $f(A) = \{f(a) \mid a \in A\}$. Since A is a subgroup of G, $A \neq \varnothing$ and so $f(A) \neq \varnothing$. Moreover,

$$\alpha, \beta \in f(A) \implies \alpha = f(a) \text{ and } \beta = f(b) \text{ for some } a, b \in A$$
$$\implies \alpha\beta^{-1} = f(a)f(b)^{-1} = f(ab^{-1}) \in f(A).$$

Hence by Theorem (2.5), $f(A)$ is a subgroup of H.

Example

Let $f : G \to H$ be a homomorphism of groups.

- If A is a subgroup of G, then $f(A)$ is a subgroup of H.
  In particular, $\mathrm{Im}\, f$ is a subgroup of H.

Proof. This is because $\mathrm{Im}\, f = f(G)$.

Example

Let $f : G \to H$ be a homomorphism of groups.

- If A is a subgroup of G, then $f(A)$ is a subgroup of H.
  In particular, $\mathrm{Im}\, f$ is a subgroup of H.
- If B is a subgroup of H, then $f^{-1}(B)$ is a subgroup of G.

Example

Let $f : G \to H$ be a homomorphism of groups.

- If A is a subgroup of G, then $f(A)$ is a subgroup of H.
  In particular, $\mathrm{Im}\, f$ is a subgroup of H.
- If B is a subgroup of H, then $f^{-1}(B)$ is a subgroup of G.

Proof. Note that

Example

Let $f : G \to H$ be a homomorphism of groups.

- If A is a subgroup of G, then $f(A)$ is a subgroup of H.
  In particular, $\mathrm{Im}\, f$ is a subgroup of H.
- If B is a subgroup of H, then $f^{-1}(B)$ is a subgroup of G.

Proof. Note that $f^{-1}(B) = \{a \in G \mid f(a) \in B\}$.

Example

Let $f : G \to H$ be a homomorphism of groups.

- If A is a subgroup of G, then $f(A)$ is a subgroup of H.
  In particular, $\mathrm{Im}\, f$ is a subgroup of H.
- If B is a subgroup of H, then $f^{-1}(B)$ is a subgroup of G.

Proof. Note that $f^{-1}(B) = \{a \in G \mid f(a) \in B\}$. Since B is a subgroup of H,

Example

Let $f : G \to H$ be a homomorphism of groups.

- If A is a subgroup of G, then $f(A)$ is a subgroup of H.
  In particular, $\mathrm{Im}\, f$ is a subgroup of H.
- If B is a subgroup of H, then $f^{-1}(B)$ is a subgroup of G.

Proof. Note that $f^{-1}(B) = \{a \in G \mid f(a) \in B\}$. Since B is a subgroup of H, $e \in B$

Example

Let $f : G \to H$ be a homomorphism of groups.

- If A is a subgroup of G, then $f(A)$ is a subgroup of H.
  In particular, $\mathrm{Im}\, f$ is a subgroup of H.
- If B is a subgroup of H, then $f^{-1}(B)$ is a subgroup of G.

Proof. Note that $f^{-1}(B) = \{a \in G \mid f(a) \in B\}$. Since B is a subgroup of H, $e \in B \implies f(e) \in B$

Example

Let $f : G \to H$ be a homomorphism of groups.

- If A is a subgroup of G, then $f(A)$ is a subgroup of H.
  In particular, $\mathrm{Im}\, f$ is a subgroup of H.
- If B is a subgroup of H, then $f^{-1}(B)$ is a subgroup of G.

Proof. Note that $f^{-1}(B) = \{a \in G \mid f(a) \in B\}$. Since B is a subgroup of H, $e \in B \implies f(e) \in B \implies e \in f^{-1}(B)$.

Example

Let $f : G \to H$ be a homomorphism of groups.

- If A is a subgroup of G, then $f(A)$ is a subgroup of H.
  In particular, $\mathrm{Im}\, f$ is a subgroup of H.
- If B is a subgroup of H, then $f^{-1}(B)$ is a subgroup of G.

Proof. Note that $f^{-1}(B) = \{a \in G \mid f(a) \in B\}$. Since B is a subgroup of H, $e \in B \implies f(e) \in B \implies e \in f^{-1}(B)$.
Hence $f^{-1}(B) \neq \varnothing$.

Example

Let $f : G \to H$ be a homomorphism of groups.

- If A is a subgroup of G, then $f(A)$ is a subgroup of H.
  In particular, $\mathrm{Im}\, f$ is a subgroup of H.
- If B is a subgroup of H, then $f^{-1}(B)$ is a subgroup of G.

Proof. Note that $f^{-1}(B) = \{a \in G \mid f(a) \in B\}$. Since B is a subgroup of H, $e \in B \implies f(e) \in B \implies e \in f^{-1}(B)$.
Hence $f^{-1}(B) \neq \varnothing$. Moreover,

Example

Let $f : G \to H$ be a homomorphism of groups.

- If A is a subgroup of G, then $f(A)$ is a subgroup of H.
  In particular, $\mathrm{Im}\, f$ is a subgroup of H.
- If B is a subgroup of H, then $f^{-1}(B)$ is a subgroup of G.

Proof. Note that $f^{-1}(B) = \{a \in G \mid f(a) \in B\}$. Since B is a subgroup of H, $e \in B \implies f(e) \in B \implies e \in f^{-1}(B)$.
Hence $f^{-1}(B) \neq \varnothing$. Moreover,

$a, b \in f^{-1}(B)$

Example

Let $f : G \to H$ be a homomorphism of groups.

- If A is a subgroup of G, then $f(A)$ is a subgroup of H.
  In particular, $\mathrm{Im}\, f$ is a subgroup of H.
- If B is a subgroup of H, then $f^{-1}(B)$ is a subgroup of G.

Proof. Note that $f^{-1}(B) = \{a \in G \mid f(a) \in B\}$. Since B is a subgroup of H, $e \in B \implies f(e) \in B \implies e \in f^{-1}(B)$.
Hence $f^{-1}(B) \neq \varnothing$. Moreover,

$$a, b \in f^{-1}(B) \implies f(a), f(b) \in B$$

Example

Let $f : G \to H$ be a homomorphism of groups.

- If A is a subgroup of G, then $f(A)$ is a subgroup of H.
  In particular, $\mathrm{Im}\, f$ is a subgroup of H.
- If B is a subgroup of H, then $f^{-1}(B)$ is a subgroup of G.

Proof. Note that $f^{-1}(B) = \{a \in G \mid f(a) \in B\}$. Since B is a subgroup of H, $e \in B \implies f(e) \in B \implies e \in f^{-1}(B)$.
Hence $f^{-1}(B) \neq \varnothing$. Moreover,

$$a, b \in f^{-1}(B) \implies f(a), f(b) \in B \implies f(a)f(b)^{-1} \in B$$

because B is a subgroup

Example

Let $f : G \to H$ be a homomorphism of groups.

- If A is a subgroup of G, then $f(A)$ is a subgroup of H.
  In particular, $\mathrm{Im}\, f$ is a subgroup of H.
- If B is a subgroup of H, then $f^{-1}(B)$ is a subgroup of G.

Proof. Note that $f^{-1}(B) = \{a \in G \mid f(a) \in B\}$. Since B is a subgroup of H, $e \in B \implies f(e) \in B \implies e \in f^{-1}(B)$.
Hence $f^{-1}(B) \neq \varnothing$. Moreover,

$$a, b \in f^{-1}(B) \implies f(a), f(b) \in B \implies f(a)f(b)^{-1} \in B$$
$$\implies f(ab^{-1}) \in B$$

because f is homomorphic

Example

Let $f : G \to H$ be a homomorphism of groups.

- If A is a subgroup of G, then $f(A)$ is a subgroup of H.
  In particular, $\mathrm{Im}\, f$ is a subgroup of H.
- If B is a subgroup of H, then $f^{-1}(B)$ is a subgroup of G.

Proof. Note that $f^{-1}(B) = \{a \in G \mid f(a) \in B\}$. Since B is a subgroup of H, $e \in B \implies f(e) \in B \implies e \in f^{-1}(B)$.
Hence $f^{-1}(B) \neq \varnothing$. Moreover,

$$a, b \in f^{-1}(B) \implies f(a), f(b) \in B \implies f(a)f(b)^{-1} \in B$$
$$\implies f(ab^{-1}) \in B \implies ab^{-1} \in f^{-1}(B).$$

Example

Let $f : G \to H$ be a homomorphism of groups.

- If A is a subgroup of G, then $f(A)$ is a subgroup of H.
  In particular, $\mathrm{Im}\, f$ is a subgroup of H.
- If B is a subgroup of H, then $f^{-1}(B)$ is a subgroup of G.

Proof. Note that $f^{-1}(B) = \{a \in G \mid f(a) \in B\}$. Since B is a subgroup of H, $e \in B \implies f(e) \in B \implies e \in f^{-1}(B)$.
Hence $f^{-1}(B) \neq \varnothing$. Moreover,

$$a, b \in f^{-1}(B) \implies f(a), f(b) \in B \implies f(a)f(b)^{-1} \in B$$
$$\implies f(ab^{-1}) \in B \implies ab^{-1} \in f^{-1}(B).$$

Hence by Theorem (2.5), $f^{-1}(B)$ is a subgroup of G.

Example

Let $f : G \to H$ be a homomorphism of groups.

- If A is a subgroup of G, then $f(A)$ is a subgroup of H.
  In particular, $\mathrm{Im}\, f$ is a subgroup of H.
- If B is a subgroup of H, then $f^{-1}(B)$ is a subgroup of G.
  In particular, $\mathrm{Ker}\, f$ is a subgroup of G.

Proof. Note that $f^{-1}(B) = \{a \in G \mid f(a) \in B\}$. Since B is a subgroup of H, $e \in B \implies f(e) \in B \implies e \in f^{-1}(B)$.
Hence $f^{-1}(B) \neq \varnothing$. Moreover,

$$a, b \in f^{-1}(B) \implies f(a), f(b) \in B \implies f(a)f(b)^{-1} \in B$$
$$\implies f(ab^{-1}) \in B \implies ab^{-1} \in f^{-1}(B).$$

Hence by Theorem (2.5), $f^{-1}(B)$ is a subgroup of G.

Example

Let $f : G \to H$ be a homomorphism of groups.

- If A is a subgroup of G, then $f(A)$ is a subgroup of H.
  In particular, $\mathrm{Im}\ f$ is a subgroup of H.
- If B is a subgroup of H, then $f^{-1}(B)$ is a subgroup of G.
  In particular, $\mathrm{Ker}\ f$ is a subgroup of G.

Proof. This is because $\mathrm{Ker}\ f = f^{-1}(\{e\})$.

Definition (2.7)

Let G be a group and let X be a subset of G.

Definition (2.7)

Let G be a group and let X be a subset of G.

- Let $\{H_i \mid i \in I\}$ be the family of all subgroups of G which contain X.

Definition (2.7)

Let G be a group and let X be a subset of G.

- Let $\{H_i \mid i \in I\}$ be the family of all subgroups of G which contain X.

Corollary (2.6). If G is a group and if $\{H_i \mid i \in I\}$ is a family of subgroups of G, then $\bigcap_{i \in I} H_i$ is a subgroup of G.

Definition (2.7)

Let G be a group and let X be a subset of G.

- Let $\{H_i \mid i \in I\}$ be the family of all subgroups of G which contain X. Then $\bigcap_{i \in I} H_i$ is called the subgroup of G generated by the set X

Corollary (2.6). If G is a group and if $\{H_i \mid i \in I\}$ is a family of subgroups of G, then $\bigcap_{i \in I} H_i$ is a subgroup of G.

Definition (2.7)

Let G be a group and let X be a subset of G.

- Let $\{H_i \mid i \in I\}$ be the family of all subgroups of G which contain X. Then $\bigcap_{i \in I} H_i$ is called the subgroup of G generated by the set X and denoted $\langle X \rangle$.

Corollary (2.6). If G is a group and if $\{H_i \mid i \in I\}$ is a family of subgroups of G, then $\bigcap_{i \in I} H_i$ is a subgroup of G.

Definition (2.7)

Let G be a group and let X be a subset of G.

- Let $\{H_i \mid i \in I\}$ be the family of all subgroups of G which contain X. Then $\bigcap_{i \in I} H_i$ is called the subgroup of G generated by the set X and denoted $\langle X \rangle$.

Question. What is $\langle \varnothing \rangle$?

Definition (2.7)

Let G be a group and let X be a subset of G.

- Let $\{H_i \mid i \in I\}$ be the family of all subgroups of G which contain X. Then $\bigcap_{i \in I} H_i$ is called the subgroup of G generated by the set X and denoted $\langle X \rangle$.

Question. What is $\langle \varnothing \rangle$? **Answer.** $\langle \varnothing \rangle = \{e\}$.

Definition (2.7)

Let G be a group and let X be a subset of G.

- Let $\{H_i \mid i \in I\}$ be the family of all subgroups of G which contain X. Then $\bigcap_{i \in I} H_i$ is called the subgroup of G generated by the set X and denoted $\langle X \rangle$.
- The elements of X are the generators of the subgroup $\langle X \rangle$.

Definition (2.7)

Let G be a group and let X be a subset of G.

- Let $\{H_i \mid i \in I\}$ be the family of all subgroups of G which contain X. Then $\bigcap_{i \in I} H_i$ is called the subgroup of G generated by the set X and denoted $\langle X \rangle$.
- The elements of X are the generators of the subgroup $\langle X \rangle$. Note that $\langle X \rangle$ may also be generated by other subsets,

Definition (2.7)

Let G be a group and let X be a subset of G.

- Let $\{H_i \mid i \in I\}$ be the family of all subgroups of G which contain X. Then $\bigcap_{i \in I} H_i$ is called the subgroup of G generated by the set X and denoted $\langle X \rangle$.
- The elements of X are the generators of the subgroup $\langle X \rangle$. Note that $\langle X \rangle$ may also be generated by other subsets, i.e., it is possible that $\langle X \rangle = \langle Y \rangle$ while $X \neq Y$.

Definition (2.7)

Let G be a group and let X be a subset of G.

- Let $\{H_i \mid i \in I\}$ be the family of all subgroups of G which contain X. Then $\bigcap_{i \in I} H_i$ is called the subgroup of G generated by the set X and denoted $\langle X \rangle$.
- The elements of X are the generators of the subgroup $\langle X \rangle$. Note that $\langle X \rangle$ may also be generated by other subsets, i.e., it is possible that $\langle X \rangle = \langle Y \rangle$ while $X \neq Y$.
- If $X = \{a_1, \ldots, a_n\}$,

Definition (2.7)

Let G be a group and let X be a subset of G.

- Let $\{H_i \mid i \in I\}$ be the family of all subgroups of G which contain X. Then $\bigcap_{i \in I} H_i$ is called the subgroup of G generated by the set X and denoted $\langle X \rangle$.
- The elements of X are the generators of the subgroup $\langle X \rangle$. Note that $\langle X \rangle$ may also be generated by other subsets, i.e., it is possible that $\langle X \rangle = \langle Y \rangle$ while $X \neq Y$.
- If $X = \{a_1, \ldots, a_n\}$, we write $\langle a_1, \ldots, a_n \rangle$ in place of $\langle X \rangle$.

Definition (2.7)

Let G be a group and let X be a subset of G.

- Let $\{H_i \mid i \in I\}$ be the family of all subgroups of G which contain X. Then $\bigcap_{i \in I} H_i$ is called the subgroup of G generated by the set X and denoted $\langle X \rangle$.
- The elements of X are the generators of the subgroup $\langle X \rangle$. Note that $\langle X \rangle$ may also be generated by other subsets, i.e., it is possible that $\langle X \rangle = \langle Y \rangle$ while $X \neq Y$.
- If $X = \{a_1, \ldots, a_n\}$, we write $\langle a_1, \ldots, a_n \rangle$ in place of $\langle X \rangle$.
- If $G = \langle a_1, \ldots, a_n \rangle$ for some $a_1, \ldots, a_n \in G$,

Definition (2.7)

Let G be a group and let X be a subset of G.

- Let $\{H_i \mid i \in I\}$ be the family of all subgroups of G which contain X. Then $\bigcap_{i \in I} H_i$ is called the subgroup of G generated by the set X and denoted $\langle X \rangle$.
- The elements of X are the generators of the subgroup $\langle X \rangle$. Note that $\langle X \rangle$ may also be generated by other subsets, i.e., it is possible that $\langle X \rangle = \langle Y \rangle$ while $X \neq Y$.
- If $X = \{a_1, \ldots, a_n\}$, we write $\langle a_1, \ldots, a_n \rangle$ in place of $\langle X \rangle$.
- If $G = \langle a_1, \ldots, a_n \rangle$ for some $a_1, \ldots, a_n \in G$, G is said to be finitely generated.

Definition (2.7)

Let G be a group and let X be a subset of G.

- Let $\{H_i \mid i \in I\}$ be the family of all subgroups of G which contain X. Then $\bigcap_{i \in I} H_i$ is called the subgroup of G generated by the set X and denoted $\langle X \rangle$.
- The elements of X are the generators of the subgroup $\langle X \rangle$. Note that $\langle X \rangle$ may also be generated by other subsets, i.e., it is possible that $\langle X \rangle = \langle Y \rangle$ while $X \neq Y$.
- If $X = \{a_1, \ldots, a_n\}$, we write $\langle a_1, \ldots, a_n \rangle$ in place of $\langle X \rangle$.
- If $G = \langle a_1, \ldots, a_n \rangle$ for some $a_1, \ldots, a_n \in G$, G is said to be finitely generated.
- If $a \in G$,

Definition (2.7)

Let G be a group and let X be a subset of G.

- Let $\{H_i \mid i \in I\}$ be the family of all subgroups of G which contain X. Then $\bigcap_{i \in I} H_i$ is called the subgroup of G generated by the set X and denoted $\langle X \rangle$.
- The elements of X are the generators of the subgroup $\langle X \rangle$. Note that $\langle X \rangle$ may also be generated by other subsets, i.e., it is possible that $\langle X \rangle = \langle Y \rangle$ while $X \neq Y$.
- If $X = \{a_1, \ldots, a_n\}$, we write $\langle a_1, \ldots, a_n \rangle$ in place of $\langle X \rangle$.
- If $G = \langle a_1, \ldots, a_n \rangle$ for some $a_1, \ldots, a_n \in G$, G is said to be finitely generated.
- If $a \in G$, the subgroup $\langle a \rangle$ is called

Definition (2.7)

Let G be a group and let X be a subset of G.

- Let $\{H_i \mid i \in I\}$ be the family of all subgroups of G which contain X. Then $\bigcap_{i \in I} H_i$ is called the subgroup of G generated by the set X and denoted $\langle X \rangle$.
- The elements of X are the generators of the subgroup $\langle X \rangle$. Note that $\langle X \rangle$ may also be generated by other subsets, i.e., it is possible that $\langle X \rangle = \langle Y \rangle$ while $X \neq Y$.
- If $X = \{a_1, \ldots, a_n\}$, we write $\langle a_1, \ldots, a_n \rangle$ in place of $\langle X \rangle$.
- If $G = \langle a_1, \ldots, a_n \rangle$ for some $a_1, \ldots, a_n \in G$, G is said to be finitely generated.
- If $a \in G$, the subgroup $\langle a \rangle$ is called the cyclic (sub)group generated by a.

Theorem (2.8)

Let G be a group and let X be a nonempty subset of G.

Theorem (2.8)

Let G be a group and let X be a nonempty subset of G. Then the subgroup $\langle X \rangle$ consists of all finite products

Theorem (2.8)

Let G be a group and let X be a nonempty subset of G. Then the subgroup $\langle X \rangle$ consists of all finite products $a_1^{n_1} a_2^{n_2} \cdots a_t^{n_t}$ with $a_i \in X$ and $n_i \in \mathbb{Z}$,

Theorem (2.8)

Let G be a group and let X be a nonempty subset of G. Then the subgroup $\langle X \rangle$ consists of all finite products $a_1^{n_1} a_2^{n_2} \cdots a_t^{n_t}$ with $a_i \in X$ and $n_i \in \mathbb{Z}$, i.e.,

$$\langle X \rangle = \left\{ a_1^{n_1} a_2^{n_2} \cdots a_t^{n_t} \right|$$

Theorem (2.8)

Let G be a group and let X be a nonempty subset of G. Then the subgroup $\langle X \rangle$ consists of all finite products $a_1^{n_1} a_2^{n_2} \cdots a_t^{n_t}$ with $a_i \in X$ and $n_i \in \mathbb{Z}$, i.e.,

$$\langle X \rangle = \left\{ a_1^{n_1} a_2^{n_2} \cdots a_t^{n_t} \;\middle|\; t \in \mathbb{N}, \right.$$

Theorem (2.8)

Let G be a group and let X be a nonempty subset of G. Then the subgroup $\langle X \rangle$ consists of all finite products $a_1^{n_1} a_2^{n_2} \cdots a_t^{n_t}$ with $a_i \in X$ and $n_i \in \mathbb{Z}$, i.e.,

$$\langle X \rangle = \left\{ a_1^{n_1} a_2^{n_2} \cdots a_t^{n_t} \;\middle|\; t \in \mathbb{N},\ a_1, \ldots, a_t \in X, \right.$$

Theorem (2.8)

Let G be a group and let X be a nonempty subset of G. Then the subgroup $\langle X \rangle$ consists of all finite products $a_1^{n_1} a_2^{n_2} \cdots a_t^{n_t}$ with $a_i \in X$ and $n_i \in \mathbb{Z}$, i.e.,

$$\langle X \rangle = \left\{ a_1^{n_1} a_2^{n_2} \cdots a_t^{n_t} \;\middle|\; \begin{array}{r} t \in \mathbb{N},\ a_1, \ldots, a_t \in X, \\ \text{and } n_1, \ldots, n_t \in \mathbb{Z} \end{array} \right\}.$$

Theorem (2.8)

Let G be a group and let X be a nonempty subset of G. Then the subgroup $\langle X \rangle$ consists of all finite products $a_1^{n_1} a_2^{n_2} \cdots a_t^{n_t}$ with $a_i \in X$ and $n_i \in \mathbb{Z}$, i.e.,

$$\langle X \rangle = \left\{ a_1^{n_1} a_2^{n_2} \cdots a_t^{n_t} \;\middle|\; \begin{array}{r} t \in \mathbb{N},\ a_1, \ldots, a_t \in X, \\ \text{and } n_1, \ldots, n_t \in \mathbb{Z} \end{array} \right\}.$$

In particular, for every $a \in G$,

Theorem (2.8)

Let G be a group and let X be a nonempty subset of G. Then the subgroup $\langle X \rangle$ consists of all finite products $a_1^{n_1} a_2^{n_2} \cdots a_t^{n_t}$ with $a_i \in X$ and $n_i \in \mathbb{Z}$, i.e.,

$$\langle X \rangle = \left\{ a_1^{n_1} a_2^{n_2} \cdots a_t^{n_t} \;\middle|\; \begin{array}{r} t \in \mathbb{N},\ a_1, \ldots, a_t \in X, \\ \text{and } n_1, \ldots, n_t \in \mathbb{Z} \end{array} \right\}.$$

In particular, for every $a \in G$, $\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$.

Theorem (2.8)

Let G be a group and let X be a nonempty subset of G. Then the subgroup $\langle X \rangle$ consists of all finite products $a_1^{n_1} a_2^{n_2} \cdots a_t^{n_t}$ with $a_i \in X$ and $n_i \in \mathbb{Z}$, i.e.,

$$\langle X \rangle = \left\{ a_1^{n_1} a_2^{n_2} \cdots a_t^{n_t} \;\middle|\; \begin{array}{r} t \in \mathbb{N},\ a_1, \ldots, a_t \in X, \\ \text{and } n_1, \ldots, n_t \in \mathbb{Z} \end{array} \right\}.$$

In particular, for every $a \in G$, $\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$.

Proof. Since $\langle X \rangle$ is a subgroup of G,

Theorem (2.8)

Let G be a group and let X be a nonempty subset of G. Then the subgroup $\langle X \rangle$ consists of all finite products $a_1^{n_1} a_2^{n_2} \cdots a_t^{n_t}$ with $a_i \in X$ and $n_i \in \mathbb{Z}$, i.e.,

$$\langle X \rangle = \left\{ a_1^{n_1} a_2^{n_2} \cdots a_t^{n_t} \;\middle|\; \begin{array}{r} t \in \mathbb{N},\ a_1, \ldots, a_t \in X, \\ \text{and } n_1, \ldots, n_t \in \mathbb{Z} \end{array} \right\}.$$

In particular, for every $a \in G$, $\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$.

Proof. Since $\langle X \rangle$ is a subgroup of G, the direction $\supseteq$ is easy to see.

Theorem (2.8)

Let G be a group and let X be a nonempty subset of G. Then the subgroup $\langle X \rangle$ consists of all finite products $a_1^{n_1} a_2^{n_2} \cdots a_t^{n_t}$ with $a_i \in X$ and $n_i \in \mathbb{Z}$, i.e.,

$$\langle X \rangle = \left\{ a_1^{n_1} a_2^{n_2} \cdots a_t^{n_t} \;\middle|\; \begin{array}{r} t \in \mathbb{N},\ a_1, \ldots, a_t \in X, \\ \text{and } n_1, \ldots, n_t \in \mathbb{Z} \end{array} \right\}.$$

In particular, for every $a \in G$, $\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$.

Proof. Since $\langle X \rangle$ is a subgroup of G, the direction $\supseteq$ is easy to see. Next, it is not difficult to check that R.H.S is indeed a subgroup containing X.

Theorem (2.8)

Let G be a group and let X be a nonempty subset of G. Then the subgroup $\langle X \rangle$ consists of all finite products $a_1^{n_1} a_2^{n_2} \cdots a_t^{n_t}$ with $a_i \in X$ and $n_i \in \mathbb{Z}$, i.e.,

$$\langle X \rangle = \left\{ a_1^{n_1} a_2^{n_2} \cdots a_t^{n_t} \;\middle|\; \begin{array}{r} t \in \mathbb{N},\ a_1, \ldots, a_t \in X, \\ \text{and } n_1, \ldots, n_t \in \mathbb{Z} \end{array} \right\}.$$

In particular, for every $a \in G$, $\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$.

Proof. Since $\langle X \rangle$ is a subgroup of G, the direction $\supseteq$ is easy to see. Next, it is not difficult to check that R.H.S is indeed a subgroup containing X. Since L.H.S is the intersection of all subgroups containing X,

Theorem (2.8)

Let G be a group and let X be a nonempty subset of G. Then the subgroup $\langle X \rangle$ consists of all finite products $a_1^{n_1} a_2^{n_2} \cdots a_t^{n_t}$ with $a_i \in X$ and $n_i \in \mathbb{Z}$, i.e.,

$$\langle X \rangle = \left\{ a_1^{n_1} a_2^{n_2} \cdots a_t^{n_t} \;\middle|\; \begin{array}{r} t \in \mathbb{N},\ a_1, \ldots, a_t \in X, \\ \text{and } n_1, \ldots, n_t \in \mathbb{Z} \end{array} \right\}.$$

In particular, for every $a \in G$, $\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$.

Proof. Since $\langle X \rangle$ is a subgroup of G, the direction $\supseteq$ is easy to see. Next, it is not difficult to check that R.H.S is indeed a subgroup containing X. Since L.H.S is the intersection of all subgroups containing X, we have the direction $\subseteq$.

Theorem (2.8)

Let G be a group and let X be a nonempty subset of G. Then the subgroup $\langle X \rangle$ consists of all finite products $a_1^{n_1} a_2^{n_2} \cdots a_t^{n_t}$ with $a_i \in X$ and $n_i \in \mathbb{Z}$, i.e.,

$$\langle X \rangle = \left\{ a_1^{n_1} a_2^{n_2} \cdots a_t^{n_t} \;\middle|\; \begin{array}{r} t \in \mathbb{N},\ a_1, \ldots, a_t \in X, \\ \text{and } n_1, \ldots, n_t \in \mathbb{Z} \end{array} \right\}.$$

In particular, for every $a \in G$, $\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$.

Proof. Since $\langle X \rangle$ is a subgroup of G, the direction $\supseteq$ is easy to see. Next, it is not difficult to check that R.H.S is indeed a subgroup containing X. Since L.H.S is the intersection of all subgroups containing X, we have the direction $\subseteq$. Therefore, we have the equality.

Remark.

Let $\{H_i \mid i \in I\}$ be a family of subgroups of a group G.

Remark.

Let $\{H_i \mid i \in I\}$ be a family of subgroups of a group G.

We have seen that $\bigcap_{i \in I} H_i$ is a subgroup of G.

Remark.

Let $\{H_i \mid i \in I\}$ be a family of subgroups of a group G.

We have seen that $\bigcap_{i \in I} H_i$ is a subgroup of G. In other words,

Remark.

Let $\{H_i \mid i \in I\}$ be a family of subgroups of a group G.

We have seen that $\bigcap_{i \in I} H_i$ is a subgroup of G. In other words,
an intersection of subgroups of a group G

Remark.

Let $\{H_i \mid i \in I\}$ be a family of subgroups of a group G.

We have seen that $\bigcap_{i \in I} H_i$ is a subgroup of G. In other words, an intersection of subgroups of a group G is always a subgroup of G.

Remark.

Let $\{H_i \mid i \in I\}$ be a family of subgroups of a group G.

We have seen that $\bigcap_{i \in I} H_i$ is a subgroup of G. In other words, an intersection of subgroups of a group G is always a subgroup of G.

However, $\bigcup_{i \in I} H_i$ is usually NOT a subgroup of G.

Remark.

Let $\{H_i \mid i \in I\}$ be a family of subgroups of a group G.

We have seen that $\bigcap_{i \in I} H_i$ is a subgroup of G. In other words, an intersection of subgroups of a group G is always a subgroup of G.

However, $\bigcup_{i \in I} H_i$ is usually NOT a subgroup of G. In other words,

Remark.

Let $\{H_i \mid i \in I\}$ be a family of subgroups of a group G.

We have seen that $\bigcap_{i \in I} H_i$ is a subgroup of G. In other words, an intersection of subgroups of a group G is always a subgroup of G.

However, $\bigcup_{i \in I} H_i$ is usually NOT a subgroup of G. In other words, a union of subgroups of G

Remark.

Let $\{H_i \mid i \in I\}$ be a family of subgroups of a group G.

We have seen that $\bigcap_{i \in I} H_i$ is a subgroup of G. In other words, an intersection of subgroups of a group G is always a subgroup of G.

However, $\bigcup_{i \in I} H_i$ is usually NOT a subgroup of G. In other words, a union of subgroups of G is NOT a subgroup of G, in general.

Remark.

Let $\{H_i \mid i \in I\}$ be a family of subgroups of a group G.

We have seen that $\bigcap_{i \in I} H_i$ is a subgroup of G. In other words, an intersection of subgroups of a group G is always a subgroup of G.

However, $\bigcup_{i \in I} H_i$ is usually NOT a subgroup of G. In other words, a union of subgroups of G is NOT a subgroup of G, in general.

Definition. Let $\{H_i \mid i \in I\}$ be a family of subgroups of a group G.

Remark.

Let $\{H_i \mid i \in I\}$ be a family of subgroups of a group G.

We have seen that $\bigcap_{i \in I} H_i$ is a subgroup of G. In other words, an intersection of subgroups of a group G is always a subgroup of G.

However, $\bigcup_{i \in I} H_i$ is usually NOT a subgroup of G. In other words, a union of subgroups of G is NOT a subgroup of G, in general.

Definition. Let $\{H_i \mid i \in I\}$ be a family of subgroups of a group G. The subgroup $\langle \bigcup_{i \in I} H_i \rangle$,

Remark.

Let $\{H_i \mid i \in I\}$ be a family of subgroups of a group G.

We have seen that $\bigcap_{i \in I} H_i$ is a subgroup of G. In other words, an intersection of subgroups of a group G is always a subgroup of G.

However, $\bigcup_{i \in I} H_i$ is usually NOT a subgroup of G. In other words, a union of subgroups of G is NOT a subgroup of G, in general.

Definition. Let $\{H_i \mid i \in I\}$ be a family of subgroups of a group G. The subgroup $\langle \bigcup_{i \in I} H_i \rangle$, generated by the set $\bigcup_{i \in I} H_i$,

Remark.

Let $\{H_i \mid i \in I\}$ be a family of subgroups of a group G.

We have seen that $\bigcap_{i \in I} H_i$ is a subgroup of G. In other words, an intersection of subgroups of a group G is always a subgroup of G.

However, $\bigcup_{i \in I} H_i$ is usually NOT a subgroup of G. In other words, a union of subgroups of G is NOT a subgroup of G, in general.

Definition. Let $\{H_i \mid i \in I\}$ be a family of subgroups of a group G. The subgroup $\langle \bigcup_{i \in I} H_i \rangle$, generated by the set $\bigcup_{i \in I} H_i$, is called the subgroup generated by the groups $\{H_i \mid i \in I\}$.

Remark.

Let $\{H_i \mid i \in I\}$ be a family of subgroups of a group G.

We have seen that $\bigcap_{i \in I} H_i$ is a subgroup of G. In other words, an intersection of subgroups of a group G is always a subgroup of G.

However, $\bigcup_{i \in I} H_i$ is usually NOT a subgroup of G. In other words, a union of subgroups of G is NOT a subgroup of G, in general.

Definition. Let $\{H_i \mid i \in I\}$ be a family of subgroups of a group G. The subgroup $\langle \bigcup_{i \in I} H_i \rangle$, generated by the set $\bigcup_{i \in I} H_i$, is called the subgroup generated by the groups $\{H_i \mid i \in I\}$. In particular, if H and K are subgroups of G,

Remark.

Let $\{H_i \mid i \in I\}$ be a family of subgroups of a group G.

We have seen that $\bigcap_{i \in I} H_i$ is a subgroup of G. In other words, an intersection of subgroups of a group G is always a subgroup of G.

However, $\bigcup_{i \in I} H_i$ is usually NOT a subgroup of G. In other words, a union of subgroups of G is NOT a subgroup of G, in general.

Definition. Let $\{H_i \mid i \in I\}$ be a family of subgroups of a group G. The subgroup $\langle \bigcup_{i \in I} H_i \rangle$, generated by the set $\bigcup_{i \in I} H_i$, is called the subgroup generated by the groups $\{H_i \mid i \in I\}$. In particular, if H and K are subgroups of G, the subgroup $\langle H \cup K \rangle$

Remark.

Let $\{H_i \mid i \in I\}$ be a family of subgroups of a group G.

We have seen that $\bigcap_{i\in I} H_i$ is a subgroup of G. In other words, an intersection of subgroups of a group G is always a subgroup of G.

However, $\bigcup_{i\in I} H_i$ is usually NOT a subgroup of G. In other words, a union of subgroups of G is NOT a subgroup of G, in general.

Definition. Let $\{H_i \mid i \in I\}$ be a family of subgroups of a group G. The subgroup $\langle \bigcup_{i\in I} H_i \rangle$, generated by the set $\bigcup_{i\in I} H_i$, is called the subgroup generated by the groups $\{H_i \mid i \in I\}$. In particular, if H and K are subgroups of G, the subgroup $\langle H \cup K \rangle$ is called the join of H and K

Remark.

Let $\{H_i \mid i \in I\}$ be a family of subgroups of a group G.

We have seen that $\bigcap_{i\in I} H_i$ is a subgroup of G. In other words, an intersection of subgroups of a group G is always a subgroup of G.

However, $\bigcup_{i\in I} H_i$ is usually NOT a subgroup of G. In other words, a union of subgroups of G is NOT a subgroup of G, in general.

Definition. Let $\{H_i \mid i \in I\}$ be a family of subgroups of a group G. The subgroup $\langle \bigcup_{i\in I} H_i \rangle$, generated by the set $\bigcup_{i\in I} H_i$, is called the subgroup generated by the groups $\{H_i \mid i \in I\}$. In particular, if H and K are subgroups of G, the subgroup $\langle H \cup K \rangle$ is called the join of H and K and is denoted by $H \vee K$.

Section I.3: Cyclic Groups

Section I.3: Cyclic Groups

Theorem (3.1)**.** Let H be a subgroup of the additive group $\mathbb{Z}$.

Section I.3: Cyclic Groups

Theorem (3.1)**.** Let H be a subgroup of the additive group $\mathbb{Z}$.

- Either $H = \{0\}$

Section I.3: Cyclic Groups

Theorem (3.1)**.** Let H be a subgroup of the additive group $\mathbb{Z}$.

- Either $H = \{0\} = \langle 0 \rangle$

Section I.3: Cyclic Groups

Theorem (3.1)**.** Let H be a subgroup of the additive group $\mathbb{Z}$.

- Either $H = \{0\} = \langle 0 \rangle$
  or $H = \langle m \rangle$,

Section I.3: Cyclic Groups

Theorem (3.1)**.** Let H be a subgroup of the additive group $\mathbb{Z}$.

- Either $H = \{0\} = \langle 0 \rangle$
  or $H = \langle m \rangle$, where $m = \min\{k \mid k \in \mathbb{N} \cap H\}$.

Section I.3: Cyclic Groups

Theorem (3.1)**.** Let H be a subgroup of the additive group $\mathbb{Z}$.

- Either $H = \{0\} = \langle 0 \rangle$
  or $H = \langle m \rangle$, where $m = \min\{k \mid k \in \mathbb{N} \cap H\}$.
- H is cyclic.

Section I.3: Cyclic Groups

Theorem (3.1)**.** Let H be a subgroup of the additive group $\mathbb{Z}$.

- Either $H = \{0\} = \langle 0 \rangle$
  or $H = \langle m \rangle$, where $m = \min\{k \mid k \in \mathbb{N} \cap H\}$.
- H is cyclic.
- If $H \neq \{0\}$, then H is infinite.

Section I.3: Cyclic Groups

Theorem (3.1)**.** Let H be a subgroup of the additive group $\mathbb{Z}$.

- Either $H = \{0\} = \langle 0 \rangle$
  or $H = \langle m \rangle$, where $m = \min\{k \mid k \in \mathbb{N} \cap H\}$.
- H is cyclic.
- If $H \neq \{0\}$, then H is infinite.

Proof. We only need to show that

Section I.3: Cyclic Groups

Theorem (3.1)**.** Let H be a subgroup of the additive group $\mathbb{Z}$.

- Either $H = \{0\} = \langle 0 \rangle$
  or $H = \langle m \rangle$, where $m = \min\{k \mid k \in \mathbb{N} \cap H\}$.
- H is cyclic.
- If $H \neq \{0\}$, then H is infinite.

Proof. We only need to show that if $H \neq \{0\}$

Section I.3: Cyclic Groups

Theorem (3.1)**.** Let H be a subgroup of the additive group $\mathbb{Z}$.

- Either $H = \{0\} = \langle 0 \rangle$
  or $H = \langle m \rangle$, where $m = \min\{k \mid k \in \mathbb{N} \cap H\}$.
- H is cyclic.
- If $H \neq \{0\}$, then H is infinite.

Proof. We only need to show that if $H \neq \{0\}$ and if $m = \min\{k \mid k \in \mathbb{N} \cap H\}$,

Section I.3: Cyclic Groups

Theorem (3.1)**.** Let H be a subgroup of the additive group $\mathbb{Z}$.

- Either $H = \{0\} = \langle 0 \rangle$
  or $H = \langle m \rangle$, where $m = \min\{k \mid k \in \mathbb{N} \cap H\}$.
- H is cyclic.
- If $H \neq \{0\}$, then H is infinite.

Proof. We only need to show that if $H \neq \{0\}$ and if $m = \min\{k \mid k \in \mathbb{N} \cap H\}$, then $H = \langle m \rangle$.

Section I.3: Cyclic Groups

Theorem (3.1)**.** Let H be a subgroup of the additive group $\mathbb{Z}$.

- Either $H = \{0\} = \langle 0 \rangle$
  or $H = \langle m \rangle$, where $m = \min\{k \mid k \in \mathbb{N} \cap H\}$.
- H is cyclic.
- If $H \neq \{0\}$, then H is infinite.

Proof. We only need to show that if $H \neq \{0\}$ and if $m = \min\{k \mid k \in \mathbb{N} \cap H\}$, then $H = \langle m \rangle$.
Since $m \in H$,

Section I.3: Cyclic Groups

Theorem (3.1)**.** Let H be a subgroup of the additive group $\mathbb{Z}$.

- Either $H = \{0\} = \langle 0 \rangle$
  or $H = \langle m \rangle$, where $m = \min\{k \mid k \in \mathbb{N} \cap H\}$.
- H is cyclic.
- If $H \neq \{0\}$, then H is infinite.

Proof. We only need to show that if $H \neq \{0\}$ and if $m = \min\{k \mid k \in \mathbb{N} \cap H\}$, then $H = \langle m \rangle$.
Since $m \in H$, $\langle m \rangle \subseteq H$.

Section I.3: Cyclic Groups

Theorem (3.1)**.** Let H be a subgroup of the additive group $\mathbb{Z}$.

- Either $H = \{0\} = \langle 0 \rangle$
  or $H = \langle m \rangle$, where $m = \min\{k \mid k \in \mathbb{N} \cap H\}$.
- H is cyclic.
- If $H \neq \{0\}$, then H is infinite.

Proof. We only need to show that if $H \neq \{0\}$ and if $m = \min\{k \mid k \in \mathbb{N} \cap H\}$, then $H = \langle m \rangle$.
Since $m \in H$, $\langle m \rangle \subseteq H$. Conversely, let $n \in H$.

Section I.3: Cyclic Groups

Theorem (3.1)**.** Let H be a subgroup of the additive group $\mathbb{Z}$.

- Either $H = \{0\} = \langle 0 \rangle$
  or $H = \langle m \rangle$, where $m = \min\{k \mid k \in \mathbb{N} \cap H\}$.
- H is cyclic.
- If $H \neq \{0\}$, then H is infinite.

Proof. We only need to show that if $H \neq \{0\}$ and if $m = \min\{k \mid k \in \mathbb{N} \cap H\}$, then $H = \langle m \rangle$.
Since $m \in H$, $\langle m \rangle \subseteq H$. Conversely, let $n \in H$. By the division algorithm on $\mathbb{Z}$,

Section I.3: Cyclic Groups

Theorem (3.1)**.** Let H be a subgroup of the additive group $\mathbb{Z}$.

- Either $H = \{0\} = \langle 0 \rangle$
  or $H = \langle m \rangle$, where $m = \min\{k \mid k \in \mathbb{N} \cap H\}$.
- H is cyclic.
- If $H \neq \{0\}$, then H is infinite.

Proof. We only need to show that if $H \neq \{0\}$ and if $m = \min\{k \mid k \in \mathbb{N} \cap H\}$, then $H = \langle m \rangle$.
Since $m \in H$, $\langle m \rangle \subseteq H$. Conversely, let $n \in H$. By the division algorithm on $\mathbb{Z}$, there exists $q, r \in \mathbb{Z}$ such that $n = qm + r$ and $0 \leq r < m$.

Section I.3: Cyclic Groups

Theorem (3.1). Let H be a subgroup of the additive group $\mathbb{Z}$.

- Either $H = \{0\} = \langle 0 \rangle$
  or $H = \langle m \rangle$, where $m = \min\{k \mid k \in \mathbb{N} \cap H\}$.
- H is cyclic.
- If $H \neq \{0\}$, then H is infinite.

Proof. We only need to show that if $H \neq \{0\}$ and if $m = \min\{k \mid k \in \mathbb{N} \cap H\}$, then $H = \langle m \rangle$.
Since $m \in H$, $\langle m \rangle \subseteq H$. Conversely, let $n \in H$. By the division algorithm on $\mathbb{Z}$, there exists $q, r \in \mathbb{Z}$ such that $n = qm + r$ and $0 \leq r < m$. Since $r = n - qm$

Section I.3: Cyclic Groups

Theorem (3.1)**.** Let H be a subgroup of the additive group $\mathbb{Z}$.

- Either $H = \{0\} = \langle 0 \rangle$
  or $H = \langle m \rangle$, where $m = \min\{k \mid k \in \mathbb{N} \cap H\}$.
- H is cyclic.
- If $H \neq \{0\}$, then H is infinite.

Proof. We only need to show that if $H \neq \{0\}$ and if $m = \min\{k \mid k \in \mathbb{N} \cap H\}$, then $H = \langle m \rangle$.
Since $m \in H$, $\langle m \rangle \subseteq H$. Conversely, let $n \in H$. By the division algorithm on $\mathbb{Z}$, there exists $q, r \in \mathbb{Z}$ such that $n = qm + r$ and $0 \leq r < m$. Since $r = n - qm$ and since $n, m \in H$,

Section I.3: Cyclic Groups

Theorem (3.1)**.** Let H be a subgroup of the additive group $\mathbb{Z}$.

- Either $H = \{0\} = \langle 0 \rangle$
  or $H = \langle m \rangle$, where $m = \min\{k \mid k \in \mathbb{N} \cap H\}$.
- H is cyclic.
- If $H \neq \{0\}$, then H is infinite.

Proof. We only need to show that if $H \neq \{0\}$ and if $m = \min\{k \mid k \in \mathbb{N} \cap H\}$, then $H = \langle m \rangle$.
Since $m \in H$, $\langle m \rangle \subseteq H$. Conversely, let $n \in H$. By the division algorithm on $\mathbb{Z}$, there exists $q, r \in \mathbb{Z}$ such that $n = qm + r$ and $0 \leq r < m$. Since $r = n - qm$ and since $n, m \in H$, $r \in H$.

Section I.3: Cyclic Groups

Theorem (3.1). Let H be a subgroup of the additive group $\mathbb{Z}$.

- Either $H = \{0\} = \langle 0 \rangle$
  or $H = \langle m \rangle$, where $m = \min\{k \mid k \in \mathbb{N} \cap H\}$.
- H is cyclic.
- If $H \neq \{0\}$, then H is infinite.

Proof. We only need to show that if $H \neq \{0\}$ and if $m = \min\{k \mid k \in \mathbb{N} \cap H\}$, then $H = \langle m \rangle$.
Since $m \in H$, $\langle m \rangle \subseteq H$. Conversely, let $n \in H$. By the division algorithm on $\mathbb{Z}$, there exists $q, r \in \mathbb{Z}$ such that $n = qm + r$ and $0 \leq r < m$. Since $r = n - qm$ and since $n, m \in H$, $r \in H$.
By the minimality of m,

Section I.3: Cyclic Groups

Theorem (3.1). Let H be a subgroup of the additive group $\mathbb{Z}$.

- Either $H = \{0\} = \langle 0 \rangle$
  or $H = \langle m \rangle$, where $m = \min\{k \mid k \in \mathbb{N} \cap H\}$.
- H is cyclic.
- If $H \neq \{0\}$, then H is infinite.

Proof. We only need to show that if $H \neq \{0\}$ and if $m = \min\{k \mid k \in \mathbb{N} \cap H\}$, then $H = \langle m \rangle$.
Since $m \in H$, $\langle m \rangle \subseteq H$. Conversely, let $n \in H$. By the division algorithm on $\mathbb{Z}$, there exists $q, r \in \mathbb{Z}$ such that $n = qm + r$ and $0 \leq r < m$. Since $r = n - qm$ and since $n, m \in H$, $r \in H$.
By the minimality of m, $r = 0$

Section I.3: Cyclic Groups

Theorem (3.1). Let H be a subgroup of the additive group $\mathbb{Z}$.

- Either $H = \{0\} = \langle 0 \rangle$
  or $H = \langle m \rangle$, where $m = \min\{k \mid k \in \mathbb{N} \cap H\}$.
- H is cyclic.
- If $H \neq \{0\}$, then H is infinite.

Proof. We only need to show that if $H \neq \{0\}$ and if $m = \min\{k \mid k \in \mathbb{N} \cap H\}$, then $H = \langle m \rangle$.
Since $m \in H$, $\langle m \rangle \subseteq H$. Conversely, let $n \in H$. By the division algorithm on $\mathbb{Z}$, there exists $q, r \in \mathbb{Z}$ such that $n = qm + r$ and $0 \leq r < m$. Since $r = n - qm$ and since $n, m \in H$, $r \in H$.
By the minimality of m, $r = 0$ and so $n = qm \in \langle m \rangle$.

Section I.3: Cyclic Groups

Theorem (3.1). Let H be a subgroup of the additive group $\mathbb{Z}$.

- Either $H = \{0\} = \langle 0 \rangle$
  or $H = \langle m \rangle$, where $m = \min\{k \mid k \in \mathbb{N} \cap H\}$.
- H is cyclic.
- If $H \neq \{0\}$, then H is infinite.

Proof. We only need to show that if $H \neq \{0\}$ and if $m = \min\{k \mid k \in \mathbb{N} \cap H\}$, then $H = \langle m \rangle$.
Since $m \in H$, $\langle m \rangle \subseteq H$. Conversely, let $n \in H$. By the division algorithm on $\mathbb{Z}$, there exists $q, r \in \mathbb{Z}$ such that $n = qm + r$ and $0 \leq r < m$. Since $r = n - qm$ and since $n, m \in H$, $r \in H$.
By the minimality of m, $r = 0$ and so $n = qm \in \langle m \rangle$.
Therefore $H \subseteq \langle m \rangle$

Section I.3: Cyclic Groups

Theorem (3.1). Let H be a subgroup of the additive group $\mathbb{Z}$.

- Either $H = \{0\} = \langle 0 \rangle$
  or $H = \langle m \rangle$, where $m = \min\{k \mid k \in \mathbb{N} \cap H\}$.
- H is cyclic.
- If $H \neq \{0\}$, then H is infinite.

Proof. We only need to show that if $H \neq \{0\}$ and if $m = \min\{k \mid k \in \mathbb{N} \cap H\}$, then $H = \langle m \rangle$.
Since $m \in H$, $\langle m \rangle \subseteq H$. Conversely, let $n \in H$. By the division algorithm on $\mathbb{Z}$, there exists $q, r \in \mathbb{Z}$ such that $n = qm + r$ and $0 \leq r < m$. Since $r = n - qm$ and since $n, m \in H$, $r \in H$.
By the minimality of m, $r = 0$ and so $n = qm \in \langle m \rangle$.
Therefore $H \subseteq \langle m \rangle$ and this implies $H = \langle m \rangle$.

Remark

Let G be a group and let $a \in G$.

Remark

Let G be a group and let $a \in G$.

Consider the map $\phi : \mathbb{Z} \to G$ defined by $k \mapsto a^k$.

Remark

Let G be a group and let $a \in G$.

Consider the map $\phi : \mathbb{Z} \to G$ defined by $k \mapsto a^k$.

- $\operatorname{Im} \phi = \langle a \rangle$.

Remark

Let G be a group and let $a \in G$.

Consider the map $\phi : \mathbb{Z} \to G$ defined by $k \mapsto a^k$.

- $\operatorname{Im} \phi = \langle a \rangle$.
- $\forall m, n \in \mathbb{Z}$,

Remark

Let G be a group and let $a \in G$.

Consider the map $\phi : \mathbb{Z} \to G$ defined by $k \mapsto a^k$.

- $\operatorname{Im} \phi = \langle a \rangle$.
- $\forall m, n \in \mathbb{Z},\ \phi(m+n) = a^{m+n}$

Remark

Let G be a group and let $a \in G$.

Consider the map $\phi : \mathbb{Z} \to G$ defined by $k \mapsto a^k$.

- $\operatorname{Im} \phi = \langle a \rangle$.
- $\forall m, n \in \mathbb{Z},\ \phi(m+n) = a^{m+n} = a^m a^n$

Remark

Let G be a group and let $a \in G$.

Consider the map $\phi : \mathbb{Z} \to G$ defined by $k \mapsto a^k$.

- $\operatorname{Im} \phi = \langle a \rangle$.
- $\forall m, n \in \mathbb{Z},\ \phi(m+n) = a^{m+n} = a^m a^n = \phi(m)\phi(n)$.

Remark

Let G be a group and let $a \in G$.

Consider the map $\phi : \mathbb{Z} \to G$ defined by $k \mapsto a^k$.

- $\operatorname{Im} \phi = \langle a \rangle$.
- $\forall m, n \in \mathbb{Z},\ \phi(m+n) = a^{m+n} = a^m a^n = \phi(m)\phi(n)$.
  Thus ϕ is a homomorphism.

Remark

Let G be a group and let $a \in G$.

Consider the map $\phi : \mathbb{Z} \to G$ defined by $k \mapsto a^k$.

- $\operatorname{Im} \phi = \langle a \rangle$.
- $\forall m, n \in \mathbb{Z},\ \phi(m+n) = a^{m+n} = a^m a^n = \phi(m)\phi(n)$. Thus ϕ is a homomorphism.
- $\operatorname{Ker} \phi$ is a subgroup of $\mathbb{Z}$.

Remark

Let G be a group and let $a \in G$.

Consider the map $\phi : \mathbb{Z} \to G$ defined by $k \mapsto a^k$.

- $\operatorname{Im} \phi = \langle a \rangle$.
- $\forall m, n \in \mathbb{Z},\ \phi(m+n) = a^{m+n} = a^m a^n = \phi(m)\phi(n)$. Thus ϕ is a homomorphism.
- $\operatorname{Ker} \phi$ is a subgroup of $\mathbb{Z}$. Hence by Theorem (3.1),

Theorem (3.1). Let H be a subgroup of the additive group $\mathbb{Z}$. Either $H = \{0\}$ or $H = \langle m \rangle$, where $m = \min\{k \mid k \in \mathbb{N} \cap H\}$.

Remark

Let G be a group and let $a \in G$.

Consider the map $\phi : \mathbb{Z} \to G$ defined by $k \mapsto a^k$.

- $\operatorname{Im} \phi = \langle a \rangle$.
- $\forall m, n \in \mathbb{Z},\ \phi(m+n) = a^{m+n} = a^m a^n = \phi(m)\phi(n)$.
  Thus ϕ is a homomorphism.
- $\operatorname{Ker} \phi$ is a subgroup of $\mathbb{Z}$. Hence by Theorem (3.1),
  $\operatorname{Ker} \phi = \{0\}$

Theorem (3.1). Let H be a subgroup of the additive group $\mathbb{Z}$. Either $H = \{0\}$ or $H = \langle m \rangle$, where $m = \min\{k \mid k \in \mathbb{N} \cap H\}$.

Remark

Let G be a group and let $a \in G$.

Consider the map $\phi : \mathbb{Z} \to G$ defined by $k \mapsto a^k$.

- $\operatorname{Im} \phi = \langle a \rangle$.
- $\forall m, n \in \mathbb{Z},\ \phi(m+n) = a^{m+n} = a^m a^n = \phi(m)\phi(n)$.
  Thus ϕ is a homomorphism.
- $\operatorname{Ker} \phi$ is a subgroup of $\mathbb{Z}$. Hence by Theorem (3.1),
  $\operatorname{Ker} \phi = \{0\}$ or $\operatorname{Ker} \phi = \langle m \rangle$

Theorem (3.1). Let H be a subgroup of the additive group $\mathbb{Z}$.
Either $H = \{0\}$ or $H = \langle m \rangle$, where $m = \min\{k \mid k \in \mathbb{N} \cap H\}$.

Remark

Let G be a group and let $a \in G$.

Consider the map $\phi : \mathbb{Z} \to G$ defined by $k \mapsto a^k$.

- $\operatorname{Im} \phi = \langle a \rangle$.
- $\forall m, n \in \mathbb{Z},\ \phi(m+n) = a^{m+n} = a^m a^n = \phi(m)\phi(n)$.
  Thus ϕ is a homomorphism.
- $\operatorname{Ker} \phi$ is a subgroup of $\mathbb{Z}$. Hence by Theorem (3.1),
  $\operatorname{Ker} \phi = \{0\}$ or $\operatorname{Ker} \phi = \langle m \rangle$ where
  $m = \min\{k \mid k \in \mathbb{N} \cap \operatorname{Ker} \phi\}$

Theorem (3.1). Let H be a subgroup of the additive group $\mathbb{Z}$. Either $H = \{0\}$ or $H = \langle m \rangle$, where $m = \min\{k \mid k \in \mathbb{N} \cap H\}$.

Remark

Let G be a group and let $a \in G$.

Consider the map $\phi : \mathbb{Z} \to G$ defined by $k \mapsto a^k$.

- $\operatorname{Im} \phi = \langle a \rangle$.
- $\forall m, n \in \mathbb{Z},\ \phi(m+n) = a^{m+n} = a^m a^n = \phi(m)\phi(n)$.
  Thus ϕ is a homomorphism.
- $\operatorname{Ker} \phi$ is a subgroup of $\mathbb{Z}$. Hence by Theorem (3.1),
  $\operatorname{Ker} \phi = \{0\}$ or $\operatorname{Ker} \phi = \langle m \rangle$ where
  $m = \min\{k \mid k \in \mathbb{N} \cap \operatorname{Ker} \phi\} = \min\{k \in \mathbb{N} \mid a^k = e\}$.

Theorem (3.1). Let H be a subgroup of the additive group $\mathbb{Z}$.
Either $H = \{0\}$ or $H = \langle m \rangle$, where $m = \min\{k \mid k \in \mathbb{N} \cap H\}$.

Case 1: $\mathrm{Ker}\,\phi = \{0\}$.

Case 1: $\mathrm{Ker}\,\phi = \{0\}$.

- G is a group and $a \in G$.

Case 1: $\mathrm{Ker}\,\phi = \{0\}$.

- G is a group and $a \in G$.
- The homomorphism $\phi : \mathbb{Z} \to G$ is defined by $k \mapsto a^k$.

Case 1: $\mathrm{Ker}\,\phi = \{0\}$.

- G is a group and $a \in G$.
- The homomorphism $\phi : \mathbb{Z} \to G$ is defined by $k \mapsto a^k$.
- $\mathrm{Im}\,\phi = \langle a \rangle$.

Case 1: $\mathrm{Ker}\,\phi = \{0\}$.

- G is a group and $a \in G$.
- The homomorphism $\phi : \mathbb{Z} \to G$ is defined by $k \mapsto a^k$.
- $\mathrm{Im}\,\phi = \langle a \rangle$.

Because $\mathrm{Ker}\,\phi = \{0\}$, we have

Case 1: $\mathrm{Ker}\,\phi = \{0\}$.

- G is a group and $a \in G$.
- The homomorphism $\phi : \mathbb{Z} \to G$ is defined by $k \mapsto a^k$.
- $\mathrm{Im}\,\phi = \langle a \rangle$.

Because $\mathrm{Ker}\,\phi = \{0\}$, we have

- $a^k = e \iff k = 0$,

Case 1: $\mathrm{Ker}\,\phi = \{0\}$.

- G is a group and $a \in G$.
- The homomorphism $\phi : \mathbb{Z} \to G$ is defined by $k \mapsto a^k$.
- $\mathrm{Im}\,\phi = \langle a \rangle$.

Because $\mathrm{Ker}\,\phi = \{0\}$, we have

- $a^k = e \iff k = 0$,
- ϕ is one-to-one,

Case 1: $\mathrm{Ker}\,\phi = \{0\}$.

- G is a group and $a \in G$.
- The homomorphism $\phi : \mathbb{Z} \to G$ is defined by $k \mapsto a^k$.
- $\mathrm{Im}\,\phi = \langle a \rangle$.

Because $\mathrm{Ker}\,\phi = \{0\}$, we have

- $a^k = e \iff k = 0$,
- ϕ is one-to-one, i.e., $a^k = a^\ell \iff k = \ell$,

Case 1: $\mathrm{Ker}\,\phi = \{0\}$.

- G is a group and $a \in G$.
- The homomorphism $\phi : \mathbb{Z} \to G$ is defined by $k \mapsto a^k$.
- $\mathrm{Im}\,\phi = \langle a \rangle$.

Because $\mathrm{Ker}\,\phi = \{0\}$, we have

- $a^k = e \iff k = 0$,
- ϕ is one-to-one, i.e., $a^k = a^\ell \iff k = \ell$,
- $\mathbb{Z} \cong \mathrm{Im}\,\phi$

Case 1: $\mathrm{Ker}\,\phi = \{0\}$.

- G is a group and $a \in G$.
- The homomorphism $\phi : \mathbb{Z} \to G$ is defined by $k \mapsto a^k$.
- $\mathrm{Im}\,\phi = \langle a \rangle$.

Because $\mathrm{Ker}\,\phi = \{0\}$, we have

- $a^k = e \iff k = 0$,
- ϕ is one-to-one, i.e., $a^k = a^\ell \iff k = \ell$,
- $\mathbb{Z} \cong \mathrm{Im}\,\phi = \langle a \rangle$,

Case 1: $\mathrm{Ker}\,\phi = \{0\}$.

- G is a group and $a \in G$.
- The homomorphism $\phi : \mathbb{Z} \to G$ is defined by $k \mapsto a^k$.
- $\mathrm{Im}\,\phi = \langle a \rangle$.

Because $\mathrm{Ker}\,\phi = \{0\}$, we have

- $a^k = e \iff k = 0$,
- ϕ is one-to-one, i.e., $a^k = a^\ell \iff k = \ell$,
- $\mathbb{Z} \cong \mathrm{Im}\,\phi = \langle a \rangle$,
- $|\langle a \rangle| = |\mathbb{Z}|$

Case 1: $\mathrm{Ker}\,\phi = \{0\}$.

- G is a group and $a \in G$.
- The homomorphism $\phi : \mathbb{Z} \to G$ is defined by $k \mapsto a^k$.
- $\mathrm{Im}\,\phi = \langle a \rangle$.

Because $\mathrm{Ker}\,\phi = \{0\}$, we have

- $a^k = e \iff k = 0$,
- ϕ is one-to-one, i.e., $a^k = a^\ell \iff k = \ell$,
- $\mathbb{Z} \cong \mathrm{Im}\,\phi = \langle a \rangle$,
- $|\langle a \rangle| = |\mathbb{Z}| = \infty$.

Case 2: $\mathrm{Ker}\,\phi \neq \{0\}$.

Case 2: $\mathrm{Ker}\,\phi \neq \{0\}$.

- G is a group and $a \in G$.
- The homomorphism $\phi : \mathbb{Z} \to G$ is defined by $k \mapsto a^k$.
- $\mathrm{Im}\,\phi = \langle a \rangle$.

Case 2: $\mathrm{Ker}\,\phi \neq \{0\}$.

- G is a group and $a \in G$.
- The homomorphism $\phi : \mathbb{Z} \to G$ is defined by $k \mapsto a^k$.
- $\mathrm{Im}\,\phi = \langle a \rangle$.
- $\mathrm{Ker}\,\phi = \langle m \rangle$, where $m = \min\{k \in \mathbb{N} \mid a^k = e\}$.

Case 2: $\operatorname{Ker}\phi \neq \{0\}$.

- G is a group and $a \in G$.
- The homomorphism $\phi : \mathbb{Z} \to G$ is defined by $k \mapsto a^k$.
- $\operatorname{Im}\phi = \langle a \rangle$.
- $\operatorname{Ker}\phi = \langle m \rangle$, where $m = \min\{k \in \mathbb{N} \mid a^k = e\}$.

Consider the map $\varphi : \mathbb{Z}_m \to G$

Case 2: $\operatorname{Ker}\phi \neq \{0\}$.

- G is a group and $a \in G$.
- The homomorphism $\phi : \mathbb{Z} \to G$ is defined by $k \mapsto a^k$.
- $\operatorname{Im}\phi = \langle a \rangle$.
- $\operatorname{Ker}\phi = \langle m \rangle$, where $m = \min\{k \in \mathbb{N} \mid a^k = e\}$.

Consider the map $\varphi : \mathbb{Z}_m \to G$ defined by $\overline{k} \mapsto a^k$.

Case 2: $\operatorname{Ker}\phi \neq \{0\}$.

- G is a group and $a \in G$.
- The homomorphism $\phi : \mathbb{Z} \to G$ is defined by $k \mapsto a^k$.
- $\operatorname{Im}\phi = \langle a \rangle$.
- $\operatorname{Ker}\phi = \langle m \rangle$, where $m = \min\{k \in \mathbb{N} \mid a^k = e\}$.

Consider the map $\varphi : \mathbb{Z}_m \to G$ defined by $\overline{k} \mapsto a^k$.

- Note that $\overline{k} = \overline{\ell}$

Case 2: $\operatorname{Ker}\phi \neq \{0\}$.

- G is a group and $a \in G$.
- The homomorphism $\phi : \mathbb{Z} \to G$ is defined by $k \mapsto a^k$.
- $\operatorname{Im}\phi = \langle a \rangle$.
- $\operatorname{Ker}\phi = \langle m \rangle$, where $m = \min\{k \in \mathbb{N} \mid a^k = e\}$.

Consider the map $\varphi : \mathbb{Z}_m \to G$ defined by $\overline{k} \mapsto a^k$.

- Note that $\overline{k} = \overline{\ell} \implies m \mid k - \ell$

Case 2: $\operatorname{Ker}\phi \neq \{0\}$.

- G is a group and $a \in G$.
- The homomorphism $\phi : \mathbb{Z} \to G$ is defined by $k \mapsto a^k$.
- $\operatorname{Im}\phi = \langle a \rangle$.
- $\operatorname{Ker}\phi = \langle m \rangle$, where $m = \min\{k \in \mathbb{N} \mid a^k = e\}$.

Consider the map $\varphi : \mathbb{Z}_m \to G$ defined by $\overline{k} \mapsto a^k$.

- Note that $\overline{k} = \overline{\ell} \implies m \mid k - \ell \implies k - \ell \in \langle m \rangle = \operatorname{Ker}\phi$

Case 2: $\operatorname{Ker}\phi \neq \{0\}$.

- G is a group and $a \in G$.
- The homomorphism $\phi : \mathbb{Z} \to G$ is defined by $k \mapsto a^k$.
- $\operatorname{Im}\phi = \langle a \rangle$.
- $\operatorname{Ker}\phi = \langle m \rangle$, where $m = \min\{k \in \mathbb{N} \mid a^k = e\}$.

Consider the map $\varphi : \mathbb{Z}_m \to G$ defined by $\overline{k} \mapsto a^k$.

- Note that $\overline{k} = \overline{\ell} \implies m \mid k - \ell \implies k - \ell \in \langle m \rangle = \operatorname{Ker}\phi$
  $\implies a^{k-\ell} = e$

Case 2: $\operatorname{Ker}\phi \neq \{0\}$.

- G is a group and $a \in G$.
- The homomorphism $\phi : \mathbb{Z} \to G$ is defined by $k \mapsto a^k$.
- $\operatorname{Im}\phi = \langle a \rangle$.
- $\operatorname{Ker}\phi = \langle m \rangle$, where $m = \min\{k \in \mathbb{N} \mid a^k = e\}$.

Consider the map $\varphi : \mathbb{Z}_m \to G$ defined by $\overline{k} \mapsto a^k$.

- Note that $\overline{k} = \overline{\ell} \implies m \mid k - \ell \implies k - \ell \in \langle m \rangle = \operatorname{Ker}\phi$
  $\implies a^{k-\ell} = e \implies a^k = a^\ell$.

Case 2: $\operatorname{Ker}\phi \neq \{0\}$.

- G is a group and $a \in G$.
- The homomorphism $\phi : \mathbb{Z} \to G$ is defined by $k \mapsto a^k$.
- $\operatorname{Im}\phi = \langle a \rangle$.
- $\operatorname{Ker}\phi = \langle m \rangle$, where $m = \min\{k \in \mathbb{N} \mid a^k = e\}$.

Consider the map $\varphi : \mathbb{Z}_m \to G$ defined by $\overline{k} \mapsto a^k$.

- Note that $\overline{k} = \overline{\ell} \implies m \mid k - \ell \implies k - \ell \in \langle m \rangle = \operatorname{Ker}\phi$ $\implies a^{k-\ell} = e \implies a^k = a^\ell$. Thus φ is well-defined.

Case 2: $\operatorname{Ker}\phi \neq \{0\}$.

- G is a group and $a \in G$.
- The homomorphism $\phi : \mathbb{Z} \to G$ is defined by $k \mapsto a^k$.
- $\operatorname{Im}\phi = \langle a \rangle$.
- $\operatorname{Ker}\phi = \langle m \rangle$, where $m = \min\{k \in \mathbb{N} \mid a^k = e\}$.

Consider the map $\varphi : \mathbb{Z}_m \to G$ defined by $\overline{k} \mapsto a^k$.

- Note that $\overline{k} = \overline{\ell} \implies m \mid k - \ell \implies k - \ell \in \langle m \rangle = \operatorname{Ker}\phi$ $\implies a^{k-\ell} = e \implies a^k = a^\ell$. Thus φ is well-defined.
- Note that $\varphi(\overline{k} + \overline{\ell})$

Case 2: $\operatorname{Ker}\phi \neq \{0\}$.

- G is a group and $a \in G$.
- The homomorphism $\phi : \mathbb{Z} \to G$ is defined by $k \mapsto a^k$.
- $\operatorname{Im}\phi = \langle a \rangle$.
- $\operatorname{Ker}\phi = \langle m \rangle$, where $m = \min\{k \in \mathbb{N} \mid a^k = e\}$.

Consider the map $\varphi : \mathbb{Z}_m \to G$ defined by $\overline{k} \mapsto a^k$.

- Note that $\overline{k} = \overline{\ell} \implies m \mid k - \ell \implies k - \ell \in \langle m \rangle = \operatorname{Ker}\phi$ $\implies a^{k-\ell} = e \implies a^k = a^\ell$. Thus φ is well-defined.
- Note that $\varphi(\overline{k} + \overline{\ell}) = \varphi(\overline{k + \ell})$

Case 2: $\operatorname{Ker}\phi \neq \{0\}$.

- G is a group and $a \in G$.
- The homomorphism $\phi : \mathbb{Z} \to G$ is defined by $k \mapsto a^k$.
- $\operatorname{Im}\phi = \langle a \rangle$.
- $\operatorname{Ker}\phi = \langle m \rangle$, where $m = \min\{k \in \mathbb{N} \mid a^k = e\}$.

Consider the map $\varphi : \mathbb{Z}_m \to G$ defined by $\overline{k} \mapsto a^k$.

- Note that $\overline{k} = \overline{\ell} \implies m \mid k - \ell \implies k - \ell \in \langle m \rangle = \operatorname{Ker}\phi$ $\implies a^{k-\ell} = e \implies a^k = a^\ell$. Thus φ is well-defined.
- Note that $\varphi(\overline{k} + \overline{\ell}) = \varphi(\overline{k + \ell}) = a^{k+\ell}$

Case 2: $\operatorname{Ker}\phi \neq \{0\}$.

- G is a group and $a \in G$.
- The homomorphism $\phi : \mathbb{Z} \to G$ is defined by $k \mapsto a^k$.
- $\operatorname{Im}\phi = \langle a \rangle$.
- $\operatorname{Ker}\phi = \langle m \rangle$, where $m = \min\{k \in \mathbb{N} \mid a^k = e\}$.

Consider the map $\varphi : \mathbb{Z}_m \to G$ defined by $\overline{k} \mapsto a^k$.

- Note that $\overline{k} = \overline{\ell} \implies m \mid k - \ell \implies k - \ell \in \langle m \rangle = \operatorname{Ker}\phi$ $\implies a^{k-\ell} = e \implies a^k = a^\ell$. Thus φ is well-defined.
- Note that $\varphi(\overline{k} + \overline{\ell}) = \varphi(\overline{k + \ell}) = a^{k+\ell} = a^k a^\ell$

Case 2: $\operatorname{Ker}\phi \neq \{0\}$.

- G is a group and $a \in G$.
- The homomorphism $\phi : \mathbb{Z} \to G$ is defined by $k \mapsto a^k$.
- $\operatorname{Im}\phi = \langle a \rangle$.
- $\operatorname{Ker}\phi = \langle m \rangle$, where $m = \min\{k \in \mathbb{N} \mid a^k = e\}$.

Consider the map $\varphi : \mathbb{Z}_m \to G$ defined by $\overline{k} \mapsto a^k$.

- Note that $\overline{k} = \overline{\ell} \implies m \mid k - \ell \implies k - \ell \in \langle m \rangle = \operatorname{Ker}\phi$ $\implies a^{k-\ell} = e \implies a^k = a^\ell$. Thus φ is well-defined.
- Note that $\varphi(\overline{k} + \overline{\ell}) = \varphi(\overline{k+\ell}) = a^{k+\ell} = a^k a^\ell = \varphi(\overline{k})\varphi(\overline{\ell})$.

Case 2: $\operatorname{Ker}\phi \neq \{0\}$.

- G is a group and $a \in G$.
- The homomorphism $\phi : \mathbb{Z} \to G$ is defined by $k \mapsto a^k$.
- $\operatorname{Im}\phi = \langle a \rangle$.
- $\operatorname{Ker}\phi = \langle m \rangle$, where $m = \min\{k \in \mathbb{N} \mid a^k = e\}$.

Consider the map $\varphi : \mathbb{Z}_m \to G$ defined by $\overline{k} \mapsto a^k$.

- Note that $\overline{k} = \overline{\ell} \implies m \mid k - \ell \implies k - \ell \in \langle m \rangle = \operatorname{Ker}\phi$ $\implies a^{k-\ell} = e \implies a^k = a^\ell$. Thus φ is well-defined.
- Note that $\varphi(\overline{k} + \overline{\ell}) = \varphi(\overline{k+\ell}) = a^{k+\ell} = a^k a^\ell = \varphi(\overline{k})\varphi(\overline{\ell})$. Thus φ is a homomorphism.

Case 2: $\operatorname{Ker}\phi \neq \{0\}$.

- G is a group and $a \in G$.
- The homomorphism $\phi : \mathbb{Z} \to G$ is defined by $k \mapsto a^k$.
- $\operatorname{Im}\phi = \langle a \rangle$.
- $\operatorname{Ker}\phi = \langle m \rangle$, where $m = \min\{k \in \mathbb{N} \mid a^k = e\}$.

Consider the map $\varphi : \mathbb{Z}_m \to G$ defined by $\overline{k} \mapsto a^k$.

- Note that $\overline{k} = \overline{\ell} \implies m \mid k - \ell \implies k - \ell \in \langle m \rangle = \operatorname{Ker}\phi$ $\implies a^{k-\ell} = e \implies a^k = a^\ell$. Thus φ is well-defined.
- Note that $\varphi(\overline{k} + \overline{\ell}) = \varphi(\overline{k+\ell}) = a^{k+\ell} = a^k a^\ell = \varphi(\overline{k})\varphi(\overline{\ell})$. Thus φ is a homomorphism.
- Note that $\overline{k} \in \operatorname{Ker}\varphi$

Case 2: $\operatorname{Ker}\phi \neq \{0\}$.

- G is a group and $a \in G$.
- The homomorphism $\phi : \mathbb{Z} \to G$ is defined by $k \mapsto a^k$.
- $\operatorname{Im}\phi = \langle a \rangle$.
- $\operatorname{Ker}\phi = \langle m \rangle$, where $m = \min\{k \in \mathbb{N} \mid a^k = e\}$.

Consider the map $\varphi : \mathbb{Z}_m \to G$ defined by $\overline{k} \mapsto a^k$.

- Note that $\overline{k} = \overline{\ell} \implies m \mid k - \ell \implies k - \ell \in \langle m \rangle = \operatorname{Ker}\phi$ $\implies a^{k-\ell} = e \implies a^k = a^\ell$. Thus φ is well-defined.
- Note that $\varphi(\overline{k} + \overline{\ell}) = \varphi(\overline{k+\ell}) = a^{k+\ell} = a^k a^\ell = \varphi(\overline{k})\varphi(\overline{\ell})$. Thus φ is a homomorphism.
- Note that $\overline{k} \in \operatorname{Ker}\varphi \iff a^k = e$

Case 2: $\operatorname{Ker}\phi \neq \{0\}$.

- G is a group and $a \in G$.
- The homomorphism $\phi : \mathbb{Z} \to G$ is defined by $k \mapsto a^k$.
- $\operatorname{Im}\phi = \langle a \rangle$.
- $\operatorname{Ker}\phi = \langle m \rangle$, where $m = \min\{k \in \mathbb{N} \mid a^k = e\}$.

Consider the map $\varphi : \mathbb{Z}_m \to G$ defined by $\overline{k} \mapsto a^k$.

- Note that $\overline{k} = \overline{\ell} \implies m \mid k - \ell \implies k - \ell \in \langle m \rangle = \operatorname{Ker}\phi$ $\implies a^{k-\ell} = e \implies a^k = a^\ell$. Thus φ is well-defined.
- Note that $\varphi(\overline{k} + \overline{\ell}) = \varphi(\overline{k+\ell}) = a^{k+\ell} = a^k a^\ell = \varphi(\overline{k})\varphi(\overline{\ell})$. Thus φ is a homomorphism.
- Note that $\overline{k} \in \operatorname{Ker}\varphi \iff a^k = e \iff k \in \operatorname{Ker}\phi = \langle m \rangle$

Case 2: $\operatorname{Ker}\phi \neq \{0\}$.

- G is a group and $a \in G$.
- The homomorphism $\phi : \mathbb{Z} \to G$ is defined by $k \mapsto a^k$.
- $\operatorname{Im}\phi = \langle a \rangle$.
- $\operatorname{Ker}\phi = \langle m \rangle$, where $m = \min\{k \in \mathbb{N} \mid a^k = e\}$.

Consider the map $\varphi : \mathbb{Z}_m \to G$ defined by $\overline{k} \mapsto a^k$.

- Note that $\overline{k} = \overline{\ell} \implies m \mid k - \ell \implies k - \ell \in \langle m \rangle = \operatorname{Ker}\phi$ $\implies a^{k-\ell} = e \implies a^k = a^\ell$. Thus φ is well-defined.
- Note that $\varphi(\overline{k} + \overline{\ell}) = \varphi(\overline{k+\ell}) = a^{k+\ell} = a^k a^\ell = \varphi(\overline{k})\varphi(\overline{\ell})$. Thus φ is a homomorphism.
- Note that $\overline{k} \in \operatorname{Ker}\varphi \iff a^k = e \iff k \in \operatorname{Ker}\phi = \langle m \rangle$ $\iff m \mid k$

Case 2: $\operatorname{Ker}\phi \neq \{0\}$.

- G is a group and $a \in G$.
- The homomorphism $\phi : \mathbb{Z} \to G$ is defined by $k \mapsto a^k$.
- $\operatorname{Im}\phi = \langle a \rangle$.
- $\operatorname{Ker}\phi = \langle m \rangle$, where $m = \min\{k \in \mathbb{N} \mid a^k = e\}$.

Consider the map $\varphi : \mathbb{Z}_m \to G$ defined by $\overline{k} \mapsto a^k$.

- Note that $\overline{k} = \overline{\ell} \implies m \mid k - \ell \implies k - \ell \in \langle m \rangle = \operatorname{Ker}\phi$ $\implies a^{k-\ell} = e \implies a^k = a^\ell$. Thus φ is well-defined.
- Note that $\varphi(\overline{k} + \overline{\ell}) = \varphi(\overline{k+\ell}) = a^{k+\ell} = a^k a^\ell = \varphi(\overline{k})\varphi(\overline{\ell})$. Thus φ is a homomorphism.
- Note that $\overline{k} \in \operatorname{Ker}\varphi \iff a^k = e \iff k \in \operatorname{Ker}\phi = \langle m \rangle$ $\iff m \mid k \iff \overline{k} = \overline{0}$ in $\mathbb{Z}_m$.

Case 2: $\operatorname{Ker}\phi \neq \{0\}$.

- G is a group and $a \in G$.
- The homomorphism $\phi : \mathbb{Z} \to G$ is defined by $k \mapsto a^k$.
- $\operatorname{Im}\phi = \langle a \rangle$.
- $\operatorname{Ker}\phi = \langle m \rangle$, where $m = \min\{k \in \mathbb{N} \mid a^k = e\}$.

Consider the map $\varphi : \mathbb{Z}_m \to G$ defined by $\overline{k} \mapsto a^k$.

- Note that $\overline{k} = \overline{\ell} \implies m \mid k - \ell \implies k - \ell \in \langle m \rangle = \operatorname{Ker}\phi$ $\implies a^{k-\ell} = e \implies a^k = a^\ell$. Thus φ is well-defined.
- Note that $\varphi(\overline{k} + \overline{\ell}) = \varphi(\overline{k+\ell}) = a^{k+\ell} = a^k a^\ell = \varphi(\overline{k})\varphi(\overline{\ell})$. Thus φ is a homomorphism.
- Note that $\overline{k} \in \operatorname{Ker}\varphi \iff a^k = e \iff k \in \operatorname{Ker}\phi = \langle m \rangle$ $\iff m \mid k \iff \overline{k} = \overline{0}$ in $\mathbb{Z}_m$. Hence φ is one-to-one.

Case 2: $\operatorname{Ker}\phi \neq \{0\}$.

- G is a group and $a \in G$.
- The homomorphism $\phi : \mathbb{Z} \to G$ is defined by $k \mapsto a^k$.
- $\operatorname{Im}\phi = \langle a \rangle$.
- $\operatorname{Ker}\phi = \langle m \rangle$, where $m = \min\{k \in \mathbb{N} \mid a^k = e\}$.

Consider the map $\varphi : \mathbb{Z}_m \to G$ defined by $\overline{k} \mapsto a^k$.

- Note that $\overline{k} = \overline{\ell} \implies m \mid k - \ell \implies k - \ell \in \langle m \rangle = \operatorname{Ker}\phi$ $\implies a^{k-\ell} = e \implies a^k = a^\ell$. Thus φ is well-defined.
- Note that $\varphi(\overline{k} + \overline{\ell}) = \varphi(\overline{k+\ell}) = a^{k+\ell} = a^k a^\ell = \varphi(\overline{k})\varphi(\overline{\ell})$. Thus φ is a homomorphism.
- Note that $\overline{k} \in \operatorname{Ker}\varphi \iff a^k = e \iff k \in \operatorname{Ker}\phi = \langle m \rangle$ $\iff m \mid k \iff \overline{k} = \overline{0}$ in $\mathbb{Z}_m$. Hence φ is one-to-one.

Therefore, $\mathbb{Z}_m \cong \operatorname{Im}\varphi$

Case 2: $\operatorname{Ker}\phi \neq \{0\}$.

- G is a group and $a \in G$.
- The homomorphism $\phi : \mathbb{Z} \to G$ is defined by $k \mapsto a^k$.
- $\operatorname{Im}\phi = \langle a \rangle$.
- $\operatorname{Ker}\phi = \langle m \rangle$, where $m = \min\{k \in \mathbb{N} \mid a^k = e\}$.

Consider the map $\varphi : \mathbb{Z}_m \to G$ defined by $\overline{k} \mapsto a^k$.

- Note that $\overline{k} = \overline{\ell} \implies m \mid k - \ell \implies k - \ell \in \langle m \rangle = \operatorname{Ker}\phi$ $\implies a^{k-\ell} = e \implies a^k = a^\ell$. Thus φ is well-defined.
- Note that $\varphi(\overline{k} + \overline{\ell}) = \varphi(\overline{k+\ell}) = a^{k+\ell} = a^k a^\ell = \varphi(\overline{k})\varphi(\overline{\ell})$. Thus φ is a homomorphism.
- Note that $\overline{k} \in \operatorname{Ker}\varphi \iff a^k = e \iff k \in \operatorname{Ker}\phi = \langle m \rangle$ $\iff m \mid k \iff \overline{k} = \overline{0}$ in $\mathbb{Z}_m$. Hence φ is one-to-one.

Therefore, $\mathbb{Z}_m \cong \operatorname{Im}\varphi = \langle a \rangle$

Case 2: $\operatorname{Ker}\phi \neq \{0\}$.

- G is a group and $a \in G$.
- The homomorphism $\phi : \mathbb{Z} \to G$ is defined by $k \mapsto a^k$.
- $\operatorname{Im}\phi = \langle a \rangle$.
- $\operatorname{Ker}\phi = \langle m \rangle$, where $m = \min\{k \in \mathbb{N} \mid a^k = e\}$.

Consider the map $\varphi : \mathbb{Z}_m \to G$ defined by $\overline{k} \mapsto a^k$.

- Note that $\overline{k} = \overline{\ell} \implies m \mid k - \ell \implies k - \ell \in \langle m \rangle = \operatorname{Ker}\phi$ $\implies a^{k-\ell} = e \implies a^k = a^\ell$. Thus φ is well-defined.
- Note that $\varphi(\overline{k} + \overline{\ell}) = \varphi(\overline{k+\ell}) = a^{k+\ell} = a^k a^\ell = \varphi(\overline{k})\varphi(\overline{\ell})$. Thus φ is a homomorphism.
- Note that $\overline{k} \in \operatorname{Ker}\varphi \iff a^k = e \iff k \in \operatorname{Ker}\phi = \langle m \rangle$ $\iff m \mid k \iff \overline{k} = \overline{0}$ in $\mathbb{Z}_m$. Hence φ is one-to-one.

Therefore, $\mathbb{Z}_m \cong \operatorname{Im}\varphi = \langle a \rangle$ and $|\langle a \rangle| = m$.

The order of an element a in G

The order of an element a in G

Definition (3.3)**.** Let G be a group

The order of an element a in G

Definition (3.3)**.** Let G be a group and let $a \in G$.

The order of an element a in G

Definition (3.3)**.** Let G be a group and let $a \in G$.

The order of a

The order of an element a in G

Definition (3.3)**.** Let G be a group and let $a \in G$.

The order of a is defined as the order of the cyclic subgroup $\langle a \rangle$

The order of an element a in G

Definition (3.3)**.** Let G be a group and let $a \in G$.

The order of a is defined as the order of the cyclic subgroup $\langle a \rangle$ and denoted by $|a|$,

The order of an element a in G

Definition (3.3)**.** Let G be a group and let $a \in G$.

The order of a is defined as the order of the cyclic subgroup $\langle a \rangle$ and denoted by $|a|$, i.e., $|a| = |\langle a \rangle|$.

The order of an element a in G

Definition (3.3)**.** Let G be a group and let $a \in G$.

The order of a is defined as the order of the cyclic subgroup $\langle a \rangle$ and denoted by $|a|$, i.e., $|a| = |\langle a \rangle|$.

Recall:

The order of an element a in G

Definition (3.3)**.** Let G be a group and let $a \in G$.

The order of a is defined as the order of the cyclic subgroup $\langle a \rangle$ and denoted by $|a|$, i.e., $|a| = |\langle a \rangle|$.

Recall: We consider the homomorphism $\phi : \mathbb{Z} \to G$ defined by $\phi(n) = a^n$,

The order of an element a in G

Definition (3.3)**.** Let G be a group and let $a \in G$.
The order of a is defined as the order of the cyclic subgroup $\langle a \rangle$ and denoted by $|a|$, i.e., $|a| = |\langle a \rangle|$.

Recall: We consider the homomorphism $\phi : \mathbb{Z} \to G$ defined by $\phi(n) = a^n$, and showed that

The order of an element a in G

Definition (3.3)**.** Let G be a group and let $a \in G$.
The order of a is defined as the order of the cyclic subgroup $\langle a \rangle$ and denoted by $|a|$, i.e., $|a| = |\langle a \rangle|$.

Recall: We consider the homomorphism $\phi : \mathbb{Z} \to G$ defined by $\phi(n) = a^n$, and showed that

- if $\operatorname{Ker} \phi = \{0\}$,

The order of an element a in G

Definition (3.3)**.** Let G be a group and let $a \in G$.
The order of a is defined as the order of the cyclic subgroup $\langle a \rangle$ and denoted by $|a|$, i.e., $|a| = |\langle a \rangle|$.

Recall: We consider the homomorphism $\phi : \mathbb{Z} \to G$ defined by $\phi(n) = a^n$, and showed that

- if $\operatorname{Ker} \phi = \{0\}$, then $|a| = \infty$;

The order of an element a in G

Definition (3.3)**.** Let G be a group and let $a \in G$.
The order of a is defined as the order of the cyclic subgroup $\langle a \rangle$ and denoted by $|a|$, i.e., $|a| = |\langle a \rangle|$.

Recall: We consider the homomorphism $\phi : \mathbb{Z} \to G$ defined by $\phi(n) = a^n$, and showed that

- if $\operatorname{Ker} \phi = \{0\}$, then $|a| = \infty$;
- if $\operatorname{Ker} \phi \neq \{0\}$,

The order of an element a in G

Definition (3.3). Let G be a group and let $a \in G$.
The order of a is defined as the order of the cyclic subgroup $\langle a \rangle$ and denoted by $|a|$, i.e., $|a| = |\langle a \rangle|$.

Recall: We consider the homomorphism $\phi : \mathbb{Z} \to G$ defined by $\phi(n) = a^n$, and showed that

- if $\operatorname{Ker} \phi = \{0\}$, then $|a| = \infty$;
- if $\operatorname{Ker} \phi \neq \{0\}$, then $\operatorname{Ker} \phi = \langle m \rangle$, where $m = \min\{k \in \mathbb{N} \mid a^k = e\}$

The order of an element a in G

Definition (3.3). Let G be a group and let $a \in G$.
The order of a is defined as the order of the cyclic subgroup $\langle a \rangle$ and denoted by $|a|$, i.e., $|a| = |\langle a \rangle|$.

Recall: We consider the homomorphism $\phi : \mathbb{Z} \to G$ defined by $\phi(n) = a^n$, and showed that

- if $\operatorname{Ker} \phi = \{0\}$, then $|a| = \infty$;
- if $\operatorname{Ker} \phi \neq \{0\}$, then $\operatorname{Ker} \phi = \langle m \rangle$, where $m = \min\{k \in \mathbb{N} \mid a^k = e\}$ and $|a| = m$.

The order of an element a in G

Definition (3.3). Let G be a group and let $a \in G$.
The order of a is defined as the order of the cyclic subgroup $\langle a \rangle$ and denoted by $|a|$, i.e., $|a| = |\langle a \rangle|$.

Recall: We consider the homomorphism $\phi : \mathbb{Z} \to G$ defined by $\phi(n) = a^n$, and showed that

- if $\operatorname{Ker} \phi = \{0\}$, then $|a| = \infty$;
- if $\operatorname{Ker} \phi \neq \{0\}$, then $\operatorname{Ker} \phi = \langle m \rangle$, where $m = \min\{k \in \mathbb{N} \mid a^k = e\}$ and $|a| = m$.

Therefore, we have two cases:

The order of an element a in G

Definition (3.3). Let G be a group and let $a \in G$.
The order of a is defined as the order of the cyclic subgroup $\langle a \rangle$ and denoted by $|a|$, i.e., $|a| = |\langle a \rangle|$.

Recall: We consider the homomorphism $\phi : \mathbb{Z} \to G$ defined by $\phi(n) = a^n$, and showed that

- if $\operatorname{Ker} \phi = \{0\}$, then $|a| = \infty$;
- if $\operatorname{Ker} \phi \neq \{0\}$, then $\operatorname{Ker} \phi = \langle m \rangle$, where $m = \min\{k \in \mathbb{N} \mid a^k = e\}$ and $|a| = m$.

Therefore, we have two cases:

Case 1: $|a| = \infty$,

The order of an element a in G

Definition (3.3). Let G be a group and let $a \in G$.
The order of a is defined as the order of the cyclic subgroup $\langle a \rangle$ and denoted by $|a|$, i.e., $|a| = |\langle a \rangle|$.

Recall: We consider the homomorphism $\phi : \mathbb{Z} \to G$ defined by $\phi(n) = a^n$, and showed that

- if $\operatorname{Ker} \phi = \{0\}$, then $|a| = \infty$;
- if $\operatorname{Ker} \phi \neq \{0\}$, then $\operatorname{Ker} \phi = \langle m \rangle$, where $m = \min\{k \in \mathbb{N} \mid a^k = e\}$ and $|a| = m$.

Therefore, we have two cases:

Case 1: $|a| = \infty$, i.e., $\operatorname{Ker} \phi = \{0\}$;

The order of an element a in G

Definition (3.3). Let G be a group and let $a \in G$.
The order of a is defined as the order of the cyclic subgroup $\langle a \rangle$ and denoted by $|a|$, i.e., $|a| = |\langle a \rangle|$.

Recall: We consider the homomorphism $\phi : \mathbb{Z} \to G$ defined by $\phi(n) = a^n$, and showed that

- if $\operatorname{Ker} \phi = \{0\}$, then $|a| = \infty$;
- if $\operatorname{Ker} \phi \neq \{0\}$, then $\operatorname{Ker} \phi = \langle m \rangle$, where $m = \min\{k \in \mathbb{N} \mid a^k = e\}$ and $|a| = m$.

Therefore, we have two cases:

Case 1: $|a| = \infty$, i.e., $\operatorname{Ker} \phi = \{0\}$;

Case 2: $|a| = m < \infty$,

The order of an element a in G

Definition (3.3). Let G be a group and let $a \in G$.
The order of a is defined as the order of the cyclic subgroup $\langle a \rangle$ and denoted by $|a|$, i.e., $|a| = |\langle a \rangle|$.

Recall: We consider the homomorphism $\phi : \mathbb{Z} \to G$ defined by $\phi(n) = a^n$, and showed that

- if $\operatorname{Ker} \phi = \{0\}$, then $|a| = \infty$;
- if $\operatorname{Ker} \phi \neq \{0\}$, then $\operatorname{Ker} \phi = \langle m \rangle$, where $m = \min\{k \in \mathbb{N} \mid a^k = e\}$ and $|a| = m$.

Therefore, we have two cases:

Case 1: $|a| = \infty$, i.e., $\operatorname{Ker} \phi = \{0\}$;

Case 2: $|a| = m < \infty$, where $m = \min\{k \in \mathbb{N} \mid a^k = e\}$,

The order of an element a in G

Definition (3.3). Let G be a group and let $a \in G$.
The order of a is defined as the order of the cyclic subgroup $\langle a \rangle$ and denoted by $|a|$, i.e., $|a| = |\langle a \rangle|$.

Recall: We consider the homomorphism $\phi : \mathbb{Z} \to G$ defined by $\phi(n) = a^n$, and showed that

- if $\operatorname{Ker}\phi = \{0\}$, then $|a| = \infty$;
- if $\operatorname{Ker}\phi \neq \{0\}$, then $\operatorname{Ker}\phi = \langle m \rangle$, where $m = \min\{k \in \mathbb{N} \mid a^k = e\}$ and $|a| = m$.

Therefore, we have two cases:

Case 1: $|a| = \infty$, i.e., $\operatorname{Ker}\phi = \{0\}$;

Case 2: $|a| = m < \infty$, where $m = \min\{k \in \mathbb{N} \mid a^k = e\}$,
i.e., $\operatorname{Ker}\phi = \langle m \rangle \neq \{0\}$.

Theorem (3.4)

Theorem (3.4)

Let G be a group and let $a \in G$.

Theorem (3.4)

Let G be a group and let $a \in G$. Let $\phi : \mathbb{Z} \to G$ with $\phi(n) = a^n$.

Theorem (3.4)

Let G be a group and let $a \in G$. Let $\phi : \mathbb{Z} \to G$ with $\phi(n) = a^n$.

- If a has infinite order, i.e., $|a| = \infty$, then

Theorem (3.4)

Let G be a group and let $a \in G$. Let $\phi : \mathbb{Z} \to G$ with $\phi(n) = a^n$.

- If a has infinite order, i.e., $|a| = \infty$, then
  - $a^k = e \iff k = 0$;

Theorem (3.4)

Let G be a group and let $a \in G$. Let $\phi : \mathbb{Z} \to G$ with $\phi(n) = a^n$.

- If a has infinite order, i.e., $|a| = \infty$, then
  - $a^k = e \iff k = 0$;

Proof. Because $|a| = \infty$,

Theorem (3.4)

Let G be a group and let $a \in G$. Let $\phi : \mathbb{Z} \to G$ with $\phi(n) = a^n$.

- If a has infinite order, i.e., $|a| = \infty$, then
  - $a^k = e \iff k = 0$;

Proof. Because $|a| = \infty$, $\operatorname{Ker} \phi = \{0\}$.

Theorem (3.4)

Let G be a group and let $a \in G$. Let $\phi : \mathbb{Z} \to G$ with $\phi(n) = a^n$.

- If a has infinite order, i.e., $|a| = \infty$, then
  - $a^k = e \iff k = 0$;

Proof. Because $|a| = \infty$, $\operatorname{Ker} \phi = \{0\}$. Thus,

$$a^k = e$$

Theorem (3.4)

Let G be a group and let $a \in G$. Let $\phi : \mathbb{Z} \to G$ with $\phi(n) = a^n$.

- If a has infinite order, i.e., $|a| = \infty$, then
  - $a^k = e \iff k = 0$;

Proof. Because $|a| = \infty$, $\operatorname{Ker} \phi = \{0\}$. Thus,

$$a^k = e \iff k \in \operatorname{Ker} \phi$$

Theorem (3.4)

Let G be a group and let $a \in G$. Let $\phi : \mathbb{Z} \to G$ with $\phi(n) = a^n$.

- If a has infinite order, i.e., $|a| = \infty$, then
  - $a^k = e \iff k = 0$;

Proof. Because $|a| = \infty$, $\operatorname{Ker} \phi = \{0\}$. Thus,

$$a^k = e \iff k \in \operatorname{Ker} \phi \iff k = 0.$$

Theorem (3.4)

Let G be a group and let $a \in G$. Let $\phi : \mathbb{Z} \to G$ with $\phi(n) = a^n$.

- If a has infinite order, i.e., $|a| = \infty$, then
  - $a^k = e \iff k = 0$;
  - the elements a^k, $k \in \mathbb{Z}$, are all distinct.

Proof. Because $|a| = \infty$, $\operatorname{Ker} \phi = \{0\}$. Thus,

$$a^k = e \iff k \in \operatorname{Ker} \phi \iff k = 0.$$

Theorem (3.4)

Let G be a group and let $a \in G$. Let $\phi : \mathbb{Z} \to G$ with $\phi(n) = a^n$.

- If a has infinite order, i.e., $|a| = \infty$, then
  - $a^k = e \iff k = 0$;
  - the elements a^k, $k \in \mathbb{Z}$, are all distinct.

Proof. Because $|a| = \infty$, $\operatorname{Ker} \phi = \{0\}$. Thus,

$$a^k = e \iff k \in \operatorname{Ker} \phi \iff k = 0.$$

Moreover, since $\operatorname{Ker} \phi = \{0\}$,

Theorem (3.4)

Let G be a group and let $a \in G$. Let $\phi : \mathbb{Z} \to G$ with $\phi(n) = a^n$.

- If a has infinite order, i.e., $|a| = \infty$, then
  - $a^k = e \iff k = 0$;
  - the elements a^k, $k \in \mathbb{Z}$, are all distinct.

Proof. Because $|a| = \infty$, $\operatorname{Ker} \phi = \{0\}$. Thus,

$$a^k = e \iff k \in \operatorname{Ker} \phi \iff k = 0.$$

Moreover, since $\operatorname{Ker} \phi = \{0\}$, ϕ is one-to-one,

Theorem (3.4)

Let G be a group and let $a \in G$. Let $\phi : \mathbb{Z} \to G$ with $\phi(n) = a^n$.

- If a has infinite order, i.e., $|a| = \infty$, then
  - $a^k = e \iff k = 0$;
  - the elements a^k, $k \in \mathbb{Z}$, are all distinct.

Proof. Because $|a| = \infty$, $\operatorname{Ker} \phi = \{0\}$. Thus,

$$a^k = e \iff k \in \operatorname{Ker} \phi \iff k = 0.$$

Moreover, since $\operatorname{Ker} \phi = \{0\}$, ϕ is one-to-one, and so $a^k = \phi(k)$, $k \in \mathbb{Z}$, are all distinct.

Theorem (3.4)

Let G be a group and let $a \in G$. Let $\phi : \mathbb{Z} \to G$ with $\phi(n) = a^n$.

- If a has infinite order, i.e., $|a| = \infty$, then
  - $a^k = e \iff k = 0$;
  - the elements a^k, $k \in \mathbb{Z}$, are all distinct.
- If a has finite order m,

Theorem (3.4)

Let G be a group and let $a \in G$. Let $\phi : \mathbb{Z} \to G$ with $\phi(n) = a^n$.

- If a has infinite order, i.e., $|a| = \infty$, then
  - $a^k = e \iff k = 0$;
  - the elements a^k, $k \in \mathbb{Z}$, are all distinct.
- If a has finite order m, i.e., $|a| = m$,

Theorem (3.4)

Let G be a group and let $a \in G$. Let $\phi : \mathbb{Z} \to G$ with $\phi(n) = a^n$.

- If a has infinite order, i.e., $|a| = \infty$, then
  - $a^k = e \iff k = 0$;
  - the elements a^k, $k \in \mathbb{Z}$, are all distinct.
- If a has finite order m, i.e., $|a| = m$, then $\operatorname{Ker} \phi = \langle m \rangle$ and

Theorem (3.4)

Let G be a group and let $a \in G$. Let $\phi : \mathbb{Z} \to G$ with $\phi(n) = a^n$.

- If a has infinite order, i.e., $|a| = \infty$, then
  - $a^k = e \iff k = 0$;
  - the elements a^k, $k \in \mathbb{Z}$, are all distinct.
- If a has finite order m, i.e., $|a| = m$, then $\operatorname{Ker} \phi = \langle m \rangle$ and
  - $m = \min\{n \in \mathbb{N} \mid a^n = e\}$;

Theorem (3.4)

Let G be a group and let $a \in G$. Let $\phi : \mathbb{Z} \to G$ with $\phi(n) = a^n$.

- If a has infinite order, i.e., $|a| = \infty$, then
  - $a^k = e \iff k = 0$;
  - the elements a^k, $k \in \mathbb{Z}$, are all distinct.
- If a has finite order m, i.e., $|a| = m$, then $\operatorname{Ker} \phi = \langle m \rangle$ and
  - $m = \min\{n \in \mathbb{N} \mid a^n = e\}$;
  - $a^k = e \iff m \mid k$;

Theorem (3.4)

Let G be a group and let $a \in G$. Let $\phi : \mathbb{Z} \to G$ with $\phi(n) = a^n$.

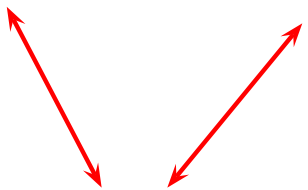
- If a has infinite order, i.e., $|a| = \infty$, then
  - $a^k = e \iff k = 0$;
  - the elements a^k, $k \in \mathbb{Z}$, are all distinct.
- If a has finite order m, i.e., $|a| = m$, then $\operatorname{Ker}\phi = \langle m \rangle$ and
  - $m = \min\{n \in \mathbb{N} \mid a^n = e\}$;
  - $a^k = e \iff m \mid k$;

$k \in \operatorname{Ker}\phi = \langle m \rangle$

Theorem (3.4)

Let G be a group and let $a \in G$. Let $\phi : \mathbb{Z} \to G$ with $\phi(n) = a^n$.

- If a has infinite order, i.e., $|a| = \infty$, then
  - $a^k = e \iff k = 0$;
  - the elements a^k, $k \in \mathbb{Z}$, are all distinct.
- If a has finite order m, i.e., $|a| = m$, then $\operatorname{Ker} \phi = \langle m \rangle$ and
  - $m = \min\{n \in \mathbb{N} \mid a^n = e\}$;
  - $a^k = e \iff m \mid k$;



$k \in \operatorname{Ker} \phi = \langle m \rangle$

Theorem (3.4)

Let G be a group and let $a \in G$. Let $\phi : \mathbb{Z} \to G$ with $\phi(n) = a^n$.

- If a has infinite order, i.e., $|a| = \infty$, then
  - $a^k = e \iff k = 0$;
  - the elements a^k, $k \in \mathbb{Z}$, are all distinct.
- If a has finite order m, i.e., $|a| = m$, then $\operatorname{Ker} \phi = \langle m \rangle$ and
  - $m = \min\{n \in \mathbb{N} \mid a^n = e\}$;
  - $a^k = e \iff m \mid k$;
  - $a^r = a^s \iff r \equiv s \mod m$;

Theorem (3.4)

Let G be a group and let $a \in G$. Let $\phi : \mathbb{Z} \to G$ with $\phi(n) = a^n$.

- If a has infinite order, i.e., $|a| = \infty$, then
  - $a^k = e \iff k = 0$;
  - the elements a^k, $k \in \mathbb{Z}$, are all distinct.
- If a has finite order m, i.e., $|a| = m$, then $\operatorname{Ker} \phi = \langle m \rangle$ and
  - $m = \min\{n \in \mathbb{N} \mid a^n = e\}$;
  - $a^k = e \iff m \mid k$;
  - $a^r = a^s \iff r \equiv s \mod m$;

$a^{r-s} = e$

Theorem (3.4)

Let G be a group and let $a \in G$. Let $\phi : \mathbb{Z} \to G$ with $\phi(n) = a^n$.

- If a has infinite order, i.e., $|a| = \infty$, then
  - $a^k = e \iff k = 0$;
  - the elements a^k, $k \in \mathbb{Z}$, are all distinct.
- If a has finite order m, i.e., $|a| = m$, then $\operatorname{Ker} \phi = \langle m \rangle$ and
  - $m = \min\{n \in \mathbb{N} \mid a^n = e\}$;
  - $a^k = e \iff m \mid k$;
  - $a^r = a^s \iff r \equiv s \mod m$;

$a^{r-s} = e \iff m \mid r - s$

Theorem (3.4)

Let G be a group and let $a \in G$. Let $\phi : \mathbb{Z} \to G$ with $\phi(n) = a^n$.

- If a has infinite order, i.e., $|a| = \infty$, then
  - $a^k = e \iff k = 0$;
  - the elements a^k, $k \in \mathbb{Z}$, are all distinct.
- If a has finite order m, i.e., $|a| = m$, then $\operatorname{Ker} \phi = \langle m \rangle$ and
  - $m = \min\{n \in \mathbb{N} \mid a^n = e\}$;
  - $a^k = e \iff m \mid k$;
  - $a^r = a^s \iff r \equiv s \mod m$;

$a^{r-s} = e \iff m \mid r - s$

Theorem (3.4)

Let G be a group and let $a \in G$. Let $\phi : \mathbb{Z} \to G$ with $\phi(n) = a^n$.

- If a has infinite order, i.e., $|a| = \infty$, then
  - $a^k = e \iff k = 0$;
  - the elements a^k, $k \in \mathbb{Z}$, are all distinct.
- If a has finite order m, i.e., $|a| = m$, then $\operatorname{Ker} \phi = \langle m \rangle$ and
  - $m = \min\{n \in \mathbb{N} \mid a^n = e\}$;
  - $a^k = e \iff m \mid k$;
  - $a^r = a^s \iff r \equiv s \mod m$;
  - $\langle a \rangle = \{e, a, a^2, \ldots, a^{m-1}\}$ and these elements are distinct;

Theorem (3.4)

Let G be a group and let $a \in G$. Let $\phi : \mathbb{Z} \to G$ with $\phi(n) = a^n$.

- If a has infinite order, i.e., $|a| = \infty$, then
  - $a^k = e \iff k = 0$;
  - the elements a^k, $k \in \mathbb{Z}$, are all distinct.
- If a has finite order m, i.e., $|a| = m$, then $\operatorname{Ker} \phi = \langle m \rangle$ and
  - $m = \min\{n \in \mathbb{N} \mid a^n = e\}$;
  - $a^k = e \iff m \mid k$;
  - $a^r = a^s \iff r \equiv s \mod m$;
  - $\langle a \rangle = \{e, a, a^2, \ldots, a^{m-1}\}$ and these elements are distinct;
  - for each k such that $k \mid m$,

Theorem (3.4)

Let G be a group and let $a \in G$. Let $\phi : \mathbb{Z} \to G$ with $\phi(n) = a^n$.

- If a has infinite order, i.e., $|a| = \infty$, then
  - $a^k = e \iff k = 0$;
  - the elements a^k, $k \in \mathbb{Z}$, are all distinct.
- If a has finite order m, i.e., $|a| = m$, then $\operatorname{Ker} \phi = \langle m \rangle$ and
  - $m = \min\{n \in \mathbb{N} \mid a^n = e\}$;
  - $a^k = e \iff m \mid k$;
  - $a^r = a^s \iff r \equiv s \mod m$;
  - $\langle a \rangle = \{e, a, a^2, \ldots, a^{m-1}\}$ and these elements are distinct;
  - for each k such that $k \mid m$, $|a^k| = \frac{m}{k}$.

Theorem (3.4)

Let G be a group and let $a \in G$. Let $\phi : \mathbb{Z} \to G$ with $\phi(n) = a^n$.

- If a has infinite order, i.e., $|a| = \infty$, then
  - $a^k = e \iff k = 0$;
  - the elements a^k, $k \in \mathbb{Z}$, are all distinct.
- If a has finite order m, i.e., $|a| = m$, then $\operatorname{Ker} \phi = \langle m \rangle$ and
  - $m = \min\{n \in \mathbb{N} \mid a^n = e\}$;
  - $a^k = e \iff m \mid k$;
  - $a^r = a^s \iff r \equiv s \mod m$;
  - $\langle a \rangle = \{e, a, a^2, \ldots, a^{m-1}\}$ and these elements are distinct;
  - for each k such that $k \mid m$, $|a^k| = \frac{m}{k}$.

$m = \min\{n \in \mathbb{N} \mid a^n = e\}$,

Theorem (3.4)

Let G be a group and let $a \in G$. Let $\phi : \mathbb{Z} \to G$ with $\phi(n) = a^n$.

- If a has infinite order, i.e., $|a| = \infty$, then
  - $a^k = e \iff k = 0$;
  - the elements a^k, $k \in \mathbb{Z}$, are all distinct.
- If a has finite order m, i.e., $|a| = m$, then $\operatorname{Ker} \phi = \langle m \rangle$ and
  - $m = \min\{n \in \mathbb{N} \mid a^n = e\}$;
  - $a^k = e \iff m \mid k$;
  - $a^r = a^s \iff r \equiv s \mod m$;
  - $\langle a \rangle = \{e, a, a^2, \ldots, a^{m-1}\}$ and these elements are distinct;
  - for each k such that $k \mid m$, $|a^k| = \frac{m}{k}$.

$m = \min\{n \in \mathbb{N} \mid a^n = e\}$, so $\frac{m}{k} = \min\{n \in \mathbb{N} \mid (a^k)^n = e\}$.

Theorem (3.2)

Theorem (3.2)

Let G be a cyclic group.

Theorem (3.2)

Let G be a cyclic group.

- If G is infinite,

Theorem (3.2)

Let G be a cyclic group.

- If G is infinite, then G is isomorphic to $\langle \mathbb{Z}, + \rangle$.

Theorem (3.2)

Let G be a cyclic group.

- If G is infinite, then G is isomorphic to $\langle \mathbb{Z}, + \rangle$.
- If G is finite with order m,

Theorem (3.2)

Let G be a cyclic group.

- If G is infinite, then G is isomorphic to $\langle \mathbb{Z}, + \rangle$.
- If G is finite with order m, then G is isomorphic to $\langle \mathbb{Z}_m, + \rangle$.

Theorem (3.2)

Let G be a cyclic group.

- If G is infinite, then G is isomorphic to $\langle \mathbb{Z}, + \rangle$.
- If G is finite with order m, then G is isomorphic to $\langle \mathbb{Z}_m, + \rangle$.

Proof.

Theorem (3.2)

Let G be a cyclic group.

- If G is infinite, then G is isomorphic to $\langle \mathbb{Z}, + \rangle$.
- If G is finite with order m, then G is isomorphic to $\langle \mathbb{Z}_m, + \rangle$.

Proof. Since G is cyclic,

Theorem (3.2)

Let G be a cyclic group.

- If G is infinite, then G is isomorphic to $\langle \mathbb{Z}, + \rangle$.
- If G is finite with order m, then G is isomorphic to $\langle \mathbb{Z}_m, + \rangle$.

Proof. Since G is cyclic, there exists $a \in G$ such that $G = \langle a \rangle$.

Theorem (3.2)

Let G be a cyclic group.

- If G is infinite, then G is isomorphic to $\langle \mathbb{Z}, + \rangle$.
- If G is finite with order m, then G is isomorphic to $\langle \mathbb{Z}_m, + \rangle$.

Proof. Since G is cyclic, there exists $a \in G$ such that $G = \langle a \rangle$. Consider the map $\phi : \mathbb{Z} \to G$ defined by $n \mapsto a^n$.

Theorem (3.2)

Let G be a cyclic group.

- If G is infinite, then G is isomorphic to $\langle \mathbb{Z}, + \rangle$.
- If G is finite with order m, then G is isomorphic to $\langle \mathbb{Z}_m, + \rangle$.

Proof. Since G is cyclic, there exists $a \in G$ such that $G = \langle a \rangle$. Consider the map $\phi : \mathbb{Z} \to G$ defined by $n \mapsto a^n$.

- If $|G| = \infty$,

Theorem (3.2)

Let G be a cyclic group.

- If G is infinite, then G is isomorphic to $\langle \mathbb{Z}, + \rangle$.
- If G is finite with order m, then G is isomorphic to $\langle \mathbb{Z}_m, + \rangle$.

Proof. Since G is cyclic, there exists $a \in G$ such that $G = \langle a \rangle$. Consider the map $\phi : \mathbb{Z} \to G$ defined by $n \mapsto a^n$.

- If $|G| = \infty$, i.e., $|a| = \infty$,

Theorem (3.2)

Let G be a cyclic group.

- If G is infinite, then G is isomorphic to $\langle \mathbb{Z}, + \rangle$.
- If G is finite with order m, then G is isomorphic to $\langle \mathbb{Z}_m, + \rangle$.

Proof. Since G is cyclic, there exists $a \in G$ such that $G = \langle a \rangle$. Consider the map $\phi : \mathbb{Z} \to G$ defined by $n \mapsto a^n$.

- If $|G| = \infty$, i.e., $|a| = \infty$, i.e., $\operatorname{Ker} \phi = \{0\}$,

Theorem (3.2)

Let G be a cyclic group.

- If G is infinite, then G is isomorphic to $\langle \mathbb{Z}, + \rangle$.
- If G is finite with order m, then G is isomorphic to $\langle \mathbb{Z}_m, + \rangle$.

Proof. Since G is cyclic, there exists $a \in G$ such that $G = \langle a \rangle$. Consider the map $\phi : \mathbb{Z} \to G$ defined by $n \mapsto a^n$.

- If $|G| = \infty$, i.e., $|a| = \infty$, i.e., $\operatorname{Ker} \phi = \{0\}$, we have shown $\langle a \rangle \cong \mathbb{Z}$,

Theorem (3.2)

Let G be a cyclic group.

- If G is infinite, then G is isomorphic to $\langle \mathbb{Z}, + \rangle$.
- If G is finite with order m, then G is isomorphic to $\langle \mathbb{Z}_m, + \rangle$.

Proof. Since G is cyclic, there exists $a \in G$ such that $G = \langle a \rangle$. Consider the map $\phi : \mathbb{Z} \to G$ defined by $n \mapsto a^n$.

- If $|G| = \infty$, i.e., $|a| = \infty$, i.e., $\operatorname{Ker} \phi = \{0\}$, we have shown $\langle a \rangle \cong \mathbb{Z}$, i.e., $G \cong \mathbb{Z}$.

Theorem (3.2)

Let G be a cyclic group.

- If G is infinite, then G is isomorphic to $\langle \mathbb{Z}, + \rangle$.
- If G is finite with order m, then G is isomorphic to $\langle \mathbb{Z}_m, + \rangle$.

Proof. Since G is cyclic, there exists $a \in G$ such that $G = \langle a \rangle$. Consider the map $\phi : \mathbb{Z} \to G$ defined by $n \mapsto a^n$.

- If $|G| = \infty$, i.e., $|a| = \infty$, i.e., $\operatorname{Ker} \phi = \{0\}$, we have shown $\langle a \rangle \cong \mathbb{Z}$, i.e., $G \cong \mathbb{Z}$.
- If $|G| = m$,

Theorem (3.2)

Let G be a cyclic group.

- If G is infinite, then G is isomorphic to $\langle \mathbb{Z}, + \rangle$.
- If G is finite with order m, then G is isomorphic to $\langle \mathbb{Z}_m, + \rangle$.

Proof. Since G is cyclic, there exists $a \in G$ such that $G = \langle a \rangle$. Consider the map $\phi : \mathbb{Z} \to G$ defined by $n \mapsto a^n$.

- If $|G| = \infty$, i.e., $|a| = \infty$, i.e., $\operatorname{Ker} \phi = \{0\}$, we have shown $\langle a \rangle \cong \mathbb{Z}$, i.e., $G \cong \mathbb{Z}$.
- If $|G| = m$, i.e., $|a| = m$,

Theorem (3.2)

Let G be a cyclic group.

- If G is infinite, then G is isomorphic to $\langle \mathbb{Z}, + \rangle$.
- If G is finite with order m, then G is isomorphic to $\langle \mathbb{Z}_m, + \rangle$.

Proof. Since G is cyclic, there exists $a \in G$ such that $G = \langle a \rangle$. Consider the map $\phi : \mathbb{Z} \to G$ defined by $n \mapsto a^n$.

- If $|G| = \infty$, i.e., $|a| = \infty$, i.e., $\operatorname{Ker} \phi = \{0\}$, we have shown $\langle a \rangle \cong \mathbb{Z}$, i.e., $G \cong \mathbb{Z}$.
- If $|G| = m$, i.e., $|a| = m$, i.e., $\operatorname{Ker} \phi = \langle m \rangle$

Theorem (3.2)

Let G be a cyclic group.

- If G is infinite, then G is isomorphic to $\langle \mathbb{Z}, + \rangle$.
- If G is finite with order m, then G is isomorphic to $\langle \mathbb{Z}_m, + \rangle$.

Proof. Since G is cyclic, there exists $a \in G$ such that $G = \langle a \rangle$. Consider the map $\phi : \mathbb{Z} \to G$ defined by $n \mapsto a^n$.

- If $|G| = \infty$, i.e., $|a| = \infty$, i.e., $\operatorname{Ker} \phi = \{0\}$, we have shown $\langle a \rangle \cong \mathbb{Z}$, i.e., $G \cong \mathbb{Z}$.
- If $|G| = m$, i.e., $|a| = m$, i.e., $\operatorname{Ker} \phi = \langle m \rangle$ we have shown $\langle a \rangle \cong \mathbb{Z}_m$,

Theorem (3.2)

Let G be a cyclic group.

- If G is infinite, then G is isomorphic to $\langle \mathbb{Z}, + \rangle$.
- If G is finite with order m, then G is isomorphic to $\langle \mathbb{Z}_m, + \rangle$.

Proof. Since G is cyclic, there exists $a \in G$ such that $G = \langle a \rangle$. Consider the map $\phi : \mathbb{Z} \to G$ defined by $n \mapsto a^n$.

- If $|G| = \infty$, i.e., $|a| = \infty$, i.e., $\operatorname{Ker} \phi = \{0\}$, we have shown $\langle a \rangle \cong \mathbb{Z}$, i.e., $G \cong \mathbb{Z}$.
- If $|G| = m$, i.e., $|a| = m$, i.e., $\operatorname{Ker} \phi = \langle m \rangle$ we have shown $\langle a \rangle \cong \mathbb{Z}_m$, i.e., $G \cong \mathbb{Z}_m$.

Theorem (3.5)

Let $G = \langle a \rangle$ be a cyclic group, i.e., $G = \{a^n \mid n \in \mathbb{Z}\}$.

Theorem (3.5)

Let $G = \langle a \rangle$ be a cyclic group, i.e., $G = \{a^n \mid n \in \mathbb{Z}\}$.

- If $f : G \to K$ is a group homomorphism,

Theorem (3.5)

Let $G = \langle a \rangle$ be a cyclic group, i.e., $G = \{a^n \mid n \in \mathbb{Z}\}$.

- If $f : G \to K$ is a group homomorphism, then $\mathrm{Im}\, f$ is a cyclic group.

Theorem (3.5)

Let $G = \langle a \rangle$ be a cyclic group, i.e., $G = \{a^n \mid n \in \mathbb{Z}\}$.

- If $f : G \to K$ is a group homomorphism, then $\mathrm{Im}\, f$ is a cyclic group. In fact, $\mathrm{Im}\, f = \langle f(a) \rangle$.

Theorem (3.5)

Let $G = \langle a \rangle$ be a cyclic group, i.e., $G = \{a^n \mid n \in \mathbb{Z}\}$.

- If $f : G \to K$ is a group homomorphism, then $\operatorname{Im} f$ is a cyclic group. In fact, $\operatorname{Im} f = \langle f(a) \rangle$.

Proof.

Theorem (3.5)

Let $G = \langle a \rangle$ be a cyclic group, i.e., $G = \{a^n \mid n \in \mathbb{Z}\}$.

- If $f : G \to K$ is a group homomorphism, then $\mathrm{Im}\, f$ is a cyclic group. In fact, $\mathrm{Im}\, f = \langle f(a) \rangle$.

Proof. Since $G = \{a^n \mid n \in \mathbb{Z}\}$,

Theorem (3.5)

Let $G = \langle a \rangle$ be a cyclic group, i.e., $G = \{a^n \mid n \in \mathbb{Z}\}$.

- If $f : G \to K$ is a group homomorphism, then $\mathrm{Im}\, f$ is a cyclic group. In fact, $\mathrm{Im}\, f = \langle f(a) \rangle$.

Proof. Since $G = \{a^n \mid n \in \mathbb{Z}\}$,
$\mathrm{Im}\, f = f(G)$

Theorem (3.5)

Let $G = \langle a \rangle$ be a cyclic group, i.e., $G = \{a^n \mid n \in \mathbb{Z}\}$.

- If $f : G \to K$ is a group homomorphism, then $\operatorname{Im} f$ is a cyclic group. In fact, $\operatorname{Im} f = \langle f(a) \rangle$.

Proof. Since $G = \{a^n \mid n \in \mathbb{Z}\}$,
$\operatorname{Im} f = f(G) = \{f(a^n) \mid n \in \mathbb{Z}\}$

Theorem (3.5)

Let $G = \langle a \rangle$ be a cyclic group, i.e., $G = \{a^n \mid n \in \mathbb{Z}\}$.

- If $f : G \to K$ is a group homomorphism, then $\operatorname{Im} f$ is a cyclic group. In fact, $\operatorname{Im} f = \langle f(a) \rangle$.

Proof. Since $G = \{a^n \mid n \in \mathbb{Z}\}$,
$\operatorname{Im} f = f(G) = \{f(a^n) \mid n \in \mathbb{Z}\} = \{f(a)^n \mid n \in \mathbb{Z}\}$

Theorem (3.5)

Let $G = \langle a \rangle$ be a cyclic group, i.e., $G = \{a^n \mid n \in \mathbb{Z}\}$.

- If $f : G \to K$ is a group homomorphism, then $\operatorname{Im} f$ is a cyclic group. In fact, $\operatorname{Im} f = \langle f(a) \rangle$.

Proof. Since $G = \{a^n \mid n \in \mathbb{Z}\}$,
$\operatorname{Im} f = f(G) = \{f(a^n) \mid n \in \mathbb{Z}\} = \{f(a)^n \mid n \in \mathbb{Z}\} = \langle f(a) \rangle$

Theorem (3.5)

Let $G = \langle a \rangle$ be a cyclic group, i.e., $G = \{a^n \mid n \in \mathbb{Z}\}$.

- If $f : G \to K$ is a group homomorphism, then $\operatorname{Im} f$ is a cyclic group. In fact, $\operatorname{Im} f = \langle f(a) \rangle$.

Proof. Since $G = \{a^n \mid n \in \mathbb{Z}\}$,
$\operatorname{Im} f = f(G) = \{f(a^n) \mid n \in \mathbb{Z}\} = \{f(a)^n \mid n \in \mathbb{Z}\} = \langle f(a) \rangle$
is a cyclic group.

Theorem (3.5)

Let $G = \langle a \rangle$ be a cyclic group, i.e., $G = \{a^n \mid n \in \mathbb{Z}\}$.

- If $f : G \to K$ is a group homomorphism, then $\operatorname{Im} f$ is a cyclic group. In fact, $\operatorname{Im} f = \langle f(a) \rangle$.
- If H is a subgroup of G,

Proof. Since $G = \{a^n \mid n \in \mathbb{Z}\}$,
$\operatorname{Im} f = f(G) = \{f(a^n) \mid n \in \mathbb{Z}\} = \{f(a)^n \mid n \in \mathbb{Z}\} = \langle f(a) \rangle$
is a cyclic group.

Theorem (3.5)

Let $G = \langle a \rangle$ be a cyclic group, i.e., $G = \{a^n \mid n \in \mathbb{Z}\}$.

- If $f : G \to K$ is a group homomorphism, then $\operatorname{Im} f$ is a cyclic group. In fact, $\operatorname{Im} f = \langle f(a) \rangle$.
- If H is a subgroup of G, then H is cyclic.

Proof. Since $G = \{a^n \mid n \in \mathbb{Z}\}$,
$\operatorname{Im} f = f(G) = \{f(a^n) \mid n \in \mathbb{Z}\} = \{f(a)^n \mid n \in \mathbb{Z}\} = \langle f(a) \rangle$
is a cyclic group.

Theorem (3.5)

Let $G = \langle a \rangle$ be a cyclic group, i.e., $G = \{a^n \mid n \in \mathbb{Z}\}$.

- If $f : G \to K$ is a group homomorphism, then $\operatorname{Im} f$ is a cyclic group. In fact, $\operatorname{Im} f = \langle f(a) \rangle$.
- If H is a subgroup of G, then H is cyclic.
  In particular, if H is a nontrivial subgroup of G and

Proof. Since $G = \{a^n \mid n \in \mathbb{Z}\}$,
$\operatorname{Im} f = f(G) = \{f(a^n) \mid n \in \mathbb{Z}\} = \{f(a)^n \mid n \in \mathbb{Z}\} = \langle f(a) \rangle$
is a cyclic group.

Theorem (3.5)

Let $G = \langle a \rangle$ be a cyclic group, i.e., $G = \{a^n \mid n \in \mathbb{Z}\}$.

- If $f : G \to K$ is a group homomorphism, then $\operatorname{Im} f$ is a cyclic group. In fact, $\operatorname{Im} f = \langle f(a) \rangle$.
- If H is a subgroup of G, then H is cyclic.
  In particular, if H is a nontrivial subgroup of G and if $m = \min\{n \in \mathbb{N} \mid a^n \in H\}$,

Proof. Since $G = \{a^n \mid n \in \mathbb{Z}\}$,
$\operatorname{Im} f = f(G) = \{f(a^n) \mid n \in \mathbb{Z}\} = \{f(a)^n \mid n \in \mathbb{Z}\} = \langle f(a) \rangle$
is a cyclic group.

Theorem (3.5)

Let $G = \langle a \rangle$ be a cyclic group, i.e., $G = \{a^n \mid n \in \mathbb{Z}\}$.

- If $f : G \to K$ is a group homomorphism, then $\operatorname{Im} f$ is a cyclic group. In fact, $\operatorname{Im} f = \langle f(a) \rangle$.
- If H is a subgroup of G, then H is cyclic.
  In particular, if H is a nontrivial subgroup of G and if $m = \min\{n \in \mathbb{N} \mid a^n \in H\}$, then $H = \langle a^m \rangle$.

Proof. Since $G = \{a^n \mid n \in \mathbb{Z}\}$,
$\operatorname{Im} f = f(G) = \{f(a^n) \mid n \in \mathbb{Z}\} = \{f(a)^n \mid n \in \mathbb{Z}\} = \langle f(a) \rangle$
is a cyclic group.

Theorem (3.5)

Let $G = \langle a \rangle$ be a cyclic group, i.e., $G = \{a^n \mid n \in \mathbb{Z}\}$.

- If $f : G \to K$ is a group homomorphism, then $\operatorname{Im} f$ is a cyclic group. In fact, $\operatorname{Im} f = \langle f(a) \rangle$.
- If H is a subgroup of G, then H is cyclic.
  In particular, if H is a nontrivial subgroup of G and if $m = \min\{n \in \mathbb{N} \mid a^n \in H\}$, then $H = \langle a^m \rangle$.

Proof. If H is the trivial subgroup of G,

Theorem (3.5)

Let $G = \langle a \rangle$ be a cyclic group, i.e., $G = \{a^n \mid n \in \mathbb{Z}\}$.

- If $f : G \to K$ is a group homomorphism, then $\operatorname{Im} f$ is a cyclic group. In fact, $\operatorname{Im} f = \langle f(a) \rangle$.
- If H is a subgroup of G, then H is cyclic.
  In particular, if H is a nontrivial subgroup of G and if $m = \min\{n \in \mathbb{N} \mid a^n \in H\}$, then $H = \langle a^m \rangle$.

Proof. If H is the trivial subgroup of G, then $H = \langle e \rangle$

Theorem (3.5)

Let $G = \langle a \rangle$ be a cyclic group, i.e., $G = \{a^n \mid n \in \mathbb{Z}\}$.

- If $f : G \to K$ is a group homomorphism, then $\operatorname{Im} f$ is a cyclic group. In fact, $\operatorname{Im} f = \langle f(a) \rangle$.
- If H is a subgroup of G, then H is cyclic.
  In particular, if H is a nontrivial subgroup of G and if $m = \min\{n \in \mathbb{N} \mid a^n \in H\}$, then $H = \langle a^m \rangle$.

Proof. If H is the trivial subgroup of G, then $H = \langle e \rangle$ is cyclic.

Theorem (3.5)

Let $G = \langle a \rangle$ be a cyclic group, i.e., $G = \{a^n \mid n \in \mathbb{Z}\}$.

- If $f : G \to K$ is a group homomorphism, then $\operatorname{Im} f$ is a cyclic group. In fact, $\operatorname{Im} f = \langle f(a) \rangle$.
- If H is a subgroup of G, then H is cyclic.
  In particular, if H is a nontrivial subgroup of G and if $m = \min\{n \in \mathbb{N} \mid a^n \in H\}$, then $H = \langle a^m \rangle$.

Proof. Consider the homomorphism $\phi : \mathbb{Z} \to G$ defined by $\phi(n) = a^n$.

Theorem (3.5)

Let $G = \langle a \rangle$ be a cyclic group, i.e., $G = \{a^n \mid n \in \mathbb{Z}\}$.

- If $f : G \to K$ is a group homomorphism, then $\operatorname{Im} f$ is a cyclic group. In fact, $\operatorname{Im} f = \langle f(a) \rangle$.
- If H is a subgroup of G, then H is cyclic.
  In particular, if H is a nontrivial subgroup of G and if $m = \min\{n \in \mathbb{N} \mid a^n \in H\}$, then $H = \langle a^m \rangle$.

Proof. Consider the homomorphism $\phi : \mathbb{Z} \to G$ defined by $\phi(n) = a^n$. Since $G = \langle a \rangle$,

Theorem (3.5)

Let $G = \langle a \rangle$ be a cyclic group, i.e., $G = \{a^n \mid n \in \mathbb{Z}\}$.

- If $f : G \to K$ is a group homomorphism, then $\operatorname{Im} f$ is a cyclic group. In fact, $\operatorname{Im} f = \langle f(a) \rangle$.
- If H is a subgroup of G, then H is cyclic.
  In particular, if H is a nontrivial subgroup of G and if $m = \min\{n \in \mathbb{N} \mid a^n \in H\}$, then $H = \langle a^m \rangle$.

Proof. Consider the homomorphism $\phi : \mathbb{Z} \to G$ defined by $\phi(n) = a^n$. Since $G = \langle a \rangle$, ϕ is onto.

Theorem (3.5)

Let $G = \langle a \rangle$ be a cyclic group, i.e., $G = \{a^n \mid n \in \mathbb{Z}\}$.

- If $f : G \to K$ is a group homomorphism, then $\operatorname{Im} f$ is a cyclic group. In fact, $\operatorname{Im} f = \langle f(a) \rangle$.
- If H is a subgroup of G, then H is cyclic.
  In particular, if H is a nontrivial subgroup of G and if $m = \min\{n \in \mathbb{N} \mid a^n \in H\}$, then $H = \langle a^m \rangle$.

Proof. Consider the homomorphism $\phi : \mathbb{Z} \to G$ defined by $\phi(n) = a^n$. Since $G = \langle a \rangle$, ϕ is onto. If H is a nontrivial subgroup of G,

Theorem (3.5)

Let $G = \langle a \rangle$ be a cyclic group, i.e., $G = \{a^n \mid n \in \mathbb{Z}\}$.

- If $f : G \to K$ is a group homomorphism, then $\operatorname{Im} f$ is a cyclic group. In fact, $\operatorname{Im} f = \langle f(a) \rangle$.
- If H is a subgroup of G, then H is cyclic.
  In particular, if H is a nontrivial subgroup of G and if $m = \min\{n \in \mathbb{N} \mid a^n \in H\}$, then $H = \langle a^m \rangle$.

Proof. Consider the homomorphism $\phi : \mathbb{Z} \to G$ defined by $\phi(n) = a^n$. Since $G = \langle a \rangle$, ϕ is onto. If H is a nontrivial subgroup of G, then $\phi^{-1}(H)$ is a nontrivial subgroup of $\mathbb{Z}$

Theorem (3.5)

Let $G = \langle a \rangle$ be a cyclic group, i.e., $G = \{a^n \mid n \in \mathbb{Z}\}$.

- If $f : G \to K$ is a group homomorphism, then $\operatorname{Im} f$ is a cyclic group. In fact, $\operatorname{Im} f = \langle f(a) \rangle$.
- If H is a subgroup of G, then H is cyclic.
  In particular, if H is a nontrivial subgroup of G and if $m = \min\{n \in \mathbb{N} \mid a^n \in H\}$, then $H = \langle a^m \rangle$.

Proof. Consider the homomorphism $\phi : \mathbb{Z} \to G$ defined by $\phi(n) = a^n$. Since $G = \langle a \rangle$, ϕ is onto. If H is a nontrivial subgroup of G, then $\phi^{-1}(H)$ is a nontrivial subgroup of $\mathbb{Z}$ and so $\phi^{-1}(H) = \langle m \rangle$,

Theorem (3.5)

Let $G = \langle a \rangle$ be a cyclic group, i.e., $G = \{a^n \mid n \in \mathbb{Z}\}$.

- If $f : G \to K$ is a group homomorphism, then $\operatorname{Im} f$ is a cyclic group. In fact, $\operatorname{Im} f = \langle f(a) \rangle$.
- If H is a subgroup of G, then H is cyclic.
  In particular, if H is a nontrivial subgroup of G and if $m = \min\{n \in \mathbb{N} \mid a^n \in H\}$, then $H = \langle a^m \rangle$.

Proof. Consider the homomorphism $\phi : \mathbb{Z} \to G$ defined by $\phi(n) = a^n$. Since $G = \langle a \rangle$, ϕ is onto. If H is a nontrivial subgroup of G, then $\phi^{-1}(H)$ is a nontrivial subgroup of $\mathbb{Z}$ and so $\phi^{-1}(H) = \langle m \rangle$, where $m = \min\{n \in \mathbb{N} \mid n \in \phi^{-1}(H)\}$.

Theorem (3.5)

Let $G = \langle a \rangle$ be a cyclic group, i.e., $G = \{a^n \mid n \in \mathbb{Z}\}$.

- If $f : G \to K$ is a group homomorphism, then $\operatorname{Im} f$ is a cyclic group. In fact, $\operatorname{Im} f = \langle f(a) \rangle$.
- If H is a subgroup of G, then H is cyclic.
  In particular, if H is a nontrivial subgroup of G and if $m = \min\{n \in \mathbb{N} \mid a^n \in H\}$, then $H = \langle a^m \rangle$.

Proof. Consider the homomorphism $\phi : \mathbb{Z} \to G$ defined by $\phi(n) = a^n$. Since $G = \langle a \rangle$, ϕ is onto. If H is a nontrivial subgroup of G, then $\phi^{-1}(H)$ is a nontrivial subgroup of $\mathbb{Z}$ and so $\phi^{-1}(H) = \langle m \rangle$, where $m = \min\{n \in \mathbb{N} \mid n \in \phi^{-1}(H)\}$. Since $n \in \phi^{-1}(H)$

Theorem (3.5)

Let $G = \langle a \rangle$ be a cyclic group, i.e., $G = \{a^n \mid n \in \mathbb{Z}\}$.

- If $f : G \to K$ is a group homomorphism, then $\operatorname{Im} f$ is a cyclic group. In fact, $\operatorname{Im} f = \langle f(a) \rangle$.
- If H is a subgroup of G, then H is cyclic.
  In particular, if H is a nontrivial subgroup of G and if $m = \min\{n \in \mathbb{N} \mid a^n \in H\}$, then $H = \langle a^m \rangle$.

Proof. Consider the homomorphism $\phi : \mathbb{Z} \to G$ defined by $\phi(n) = a^n$. Since $G = \langle a \rangle$, ϕ is onto. If H is a nontrivial subgroup of G, then $\phi^{-1}(H)$ is a nontrivial subgroup of $\mathbb{Z}$ and so $\phi^{-1}(H) = \langle m \rangle$, where $m = \min\{n \in \mathbb{N} \mid n \in \phi^{-1}(H)\}$. Since $n \in \phi^{-1}(H) \iff \phi(n) \in H$

Theorem (3.5)

Let $G = \langle a \rangle$ be a cyclic group, i.e., $G = \{a^n \mid n \in \mathbb{Z}\}$.

- If $f : G \to K$ is a group homomorphism, then $\operatorname{Im} f$ is a cyclic group. In fact, $\operatorname{Im} f = \langle f(a) \rangle$.
- If H is a subgroup of G, then H is cyclic.
  In particular, if H is a nontrivial subgroup of G and if $m = \min\{n \in \mathbb{N} \mid a^n \in H\}$, then $H = \langle a^m \rangle$.

Proof. Consider the homomorphism $\phi : \mathbb{Z} \to G$ defined by $\phi(n) = a^n$. Since $G = \langle a \rangle$, ϕ is onto. If H is a nontrivial subgroup of G, then $\phi^{-1}(H)$ is a nontrivial subgroup of $\mathbb{Z}$ and so $\phi^{-1}(H) = \langle m \rangle$, where $m = \min\{n \in \mathbb{N} \mid n \in \phi^{-1}(H)\}$. Since $n \in \phi^{-1}(H) \iff \phi(n) \in H \iff a^n \in H$,

Theorem (3.5)

Let $G = \langle a \rangle$ be a cyclic group, i.e., $G = \{a^n \mid n \in \mathbb{Z}\}$.

- If $f : G \to K$ is a group homomorphism, then $\operatorname{Im} f$ is a cyclic group. In fact, $\operatorname{Im} f = \langle f(a) \rangle$.
- If H is a subgroup of G, then H is cyclic.
  In particular, if H is a nontrivial subgroup of G and if $m = \min\{n \in \mathbb{N} \mid a^n \in H\}$, then $H = \langle a^m \rangle$.

Proof. Consider the homomorphism $\phi : \mathbb{Z} \to G$ defined by $\phi(n) = a^n$. Since $G = \langle a \rangle$, ϕ is onto. If H is a nontrivial subgroup of G, then $\phi^{-1}(H)$ is a nontrivial subgroup of $\mathbb{Z}$ and so $\phi^{-1}(H) = \langle m \rangle$, where $m = \min\{n \in \mathbb{N} \mid n \in \phi^{-1}(H)\}$. Since $n \in \phi^{-1}(H) \iff \phi(n) \in H \iff a^n \in H$, we have $m = \min\{n \in \mathbb{N} \mid a^n \in H\}$.

Theorem (3.5)

Let $G = \langle a \rangle$ be a cyclic group, i.e., $G = \{a^n \mid n \in \mathbb{Z}\}$.

- If $f : G \to K$ is a group homomorphism, then $\operatorname{Im} f$ is a cyclic group. In fact, $\operatorname{Im} f = \langle f(a) \rangle$.
- If H is a subgroup of G, then H is cyclic.
  In particular, if H is a nontrivial subgroup of G and if $m = \min\{n \in \mathbb{N} \mid a^n \in H\}$, then $H = \langle a^m \rangle$.

Proof. Consider the homomorphism $\phi : \mathbb{Z} \to G$ defined by $\phi(n) = a^n$. Since $G = \langle a \rangle$, ϕ is onto. If H is a nontrivial subgroup of G, then $\phi^{-1}(H)$ is a nontrivial subgroup of $\mathbb{Z}$ and so $\phi^{-1}(H) = \langle m \rangle$, where $m = \min\{n \in \mathbb{N} \mid n \in \phi^{-1}(H)\}$. Since $n \in \phi^{-1}(H) \iff \phi(n) \in H \iff a^n \in H$, we have $m = \min\{n \in \mathbb{N} \mid a^n \in H\}$. Moreover, because ϕ is onto,

Theorem (3.5)

Let $G = \langle a \rangle$ be a cyclic group, i.e., $G = \{a^n \mid n \in \mathbb{Z}\}$.

- If $f : G \to K$ is a group homomorphism, then $\operatorname{Im} f$ is a cyclic group. In fact, $\operatorname{Im} f = \langle f(a) \rangle$.
- If H is a subgroup of G, then H is cyclic.
  In particular, if H is a nontrivial subgroup of G and if $m = \min\{n \in \mathbb{N} \mid a^n \in H\}$, then $H = \langle a^m \rangle$.

Proof. Consider the homomorphism $\phi : \mathbb{Z} \to G$ defined by $\phi(n) = a^n$. Since $G = \langle a \rangle$, ϕ is onto. If H is a nontrivial subgroup of G, then $\phi^{-1}(H)$ is a nontrivial subgroup of $\mathbb{Z}$ and so $\phi^{-1}(H) = \langle m \rangle$, where $m = \min\{n \in \mathbb{N} \mid n \in \phi^{-1}(H)\}$. Since $n \in \phi^{-1}(H) \iff \phi(n) \in H \iff a^n \in H$, we have $m = \min\{n \in \mathbb{N} \mid a^n \in H\}$. Moreover, because ϕ is onto, $H = \phi(\phi^{-1}(H))$

Theorem (3.5)

Let $G = \langle a \rangle$ be a cyclic group, i.e., $G = \{a^n \mid n \in \mathbb{Z}\}$.

- If $f : G \to K$ is a group homomorphism, then $\operatorname{Im} f$ is a cyclic group. In fact, $\operatorname{Im} f = \langle f(a) \rangle$.
- If H is a subgroup of G, then H is cyclic.
  In particular, if H is a nontrivial subgroup of G and if $m = \min\{n \in \mathbb{N} \mid a^n \in H\}$, then $H = \langle a^m \rangle$.

Proof. Consider the homomorphism $\phi : \mathbb{Z} \to G$ defined by $\phi(n) = a^n$. Since $G = \langle a \rangle$, ϕ is onto. If H is a nontrivial subgroup of G, then $\phi^{-1}(H)$ is a nontrivial subgroup of $\mathbb{Z}$ and so $\phi^{-1}(H) = \langle m \rangle$, where $m = \min\{n \in \mathbb{N} \mid n \in \phi^{-1}(H)\}$. Since $n \in \phi^{-1}(H) \iff \phi(n) \in H \iff a^n \in H$, we have $m = \min\{n \in \mathbb{N} \mid a^n \in H\}$. Moreover, because ϕ is onto, $H = \phi(\phi^{-1}(H)) = \langle \phi(m) \rangle$

Theorem (3.5)

Let $G = \langle a \rangle$ be a cyclic group, i.e., $G = \{a^n \mid n \in \mathbb{Z}\}$.

- If $f : G \to K$ is a group homomorphism, then $\operatorname{Im} f$ is a cyclic group. In fact, $\operatorname{Im} f = \langle f(a) \rangle$.
- If H is a subgroup of G, then H is cyclic.
  In particular, if H is a nontrivial subgroup of G and if $m = \min\{n \in \mathbb{N} \mid a^n \in H\}$, then $H = \langle a^m \rangle$.

Proof. Consider the homomorphism $\phi : \mathbb{Z} \to G$ defined by $\phi(n) = a^n$. Since $G = \langle a \rangle$, ϕ is onto. If H is a nontrivial subgroup of G, then $\phi^{-1}(H)$ is a nontrivial subgroup of $\mathbb{Z}$ and so $\phi^{-1}(H) = \langle m \rangle$, where $m = \min\{n \in \mathbb{N} \mid n \in \phi^{-1}(H)\}$. Since $n \in \phi^{-1}(H) \iff \phi(n) \in H \iff a^n \in H$, we have $m = \min\{n \in \mathbb{N} \mid a^n \in H\}$. Moreover, because ϕ is onto, $H = \phi(\phi^{-1}(H)) = \langle \phi(m) \rangle = \langle a^m \rangle$.

Theorem (3.6)

Let $G = \langle a \rangle$ be a cyclic group.

Theorem (3.6)

Let $G = \langle a \rangle$ be a cyclic group.

- If G is infinite,

Theorem (3.6)

Let $G = \langle a \rangle$ be a cyclic group.

- If G is infinite, then a and a^{-1} are the only generators of G,

Theorem (3.6)

Let $G = \langle a \rangle$ be a cyclic group.

- If G is infinite, then a and a^{-1} are the only generators of G, i.e., $G = \langle b \rangle \iff b \in \{a, a^{-1}\}$.

Theorem (3.6)

Let $G = \langle a \rangle$ be a cyclic group.

- If G is infinite, then a and a^{-1} are the only generators of G, i.e., $G = \langle b \rangle \iff b \in \{a, a^{-1}\}$.

Proof. "$\Leftarrow$" is clear.

Theorem (3.6)

Let $G = \langle a \rangle$ be a cyclic group.

- If G is infinite, then a and a^{-1} are the only generators of G, i.e., $G = \langle b \rangle \iff b \in \{a, a^{-1}\}$.

Proof. "$\Leftarrow$" is clear. For "$\Rightarrow$",

Theorem (3.6)

Let $G = \langle a \rangle$ be a cyclic group.

- If G is infinite, then a and a^{-1} are the only generators of G, i.e., $G = \langle b \rangle \iff b \in \{a, a^{-1}\}$.

Proof. "$\Leftarrow$" is clear. For "$\Rightarrow$", $b \in G = \langle a \rangle$,

Theorem (3.6)

Let $G = \langle a \rangle$ be a cyclic group.

- If G is infinite, then a and a^{-1} are the only generators of G, i.e., $G = \langle b \rangle \iff b \in \{a, a^{-1}\}$.

Proof. "$\Leftarrow$" is clear. For "$\Rightarrow$", $b \in G = \langle a \rangle$, so $b = a^n$ for some $n \in \mathbb{Z}$.

Theorem (3.6)

Let $G = \langle a \rangle$ be a cyclic group.

- If G is infinite, then a and a^{-1} are the only generators of G, i.e., $G = \langle b \rangle \iff b \in \{a, a^{-1}\}$.

Proof. "$\Leftarrow$" is clear. For "$\Rightarrow$", $b \in G = \langle a \rangle$, so $b = a^n$ for some $n \in \mathbb{Z}$. Conversely, $a \in G = \langle b \rangle$,

Theorem (3.6)

Let $G = \langle a \rangle$ be a cyclic group.

- If G is infinite, then a and a^{-1} are the only generators of G, i.e., $G = \langle b \rangle \iff b \in \{a, a^{-1}\}$.

Proof. "$\Leftarrow$" is clear. For "$\Rightarrow$", $b \in G = \langle a \rangle$, so $b = a^n$ for some $n \in \mathbb{Z}$. Conversely, $a \in G = \langle b \rangle$, so $a = b^k$ for some $k \in \mathbb{Z}$.

Theorem (3.6)

Let $G = \langle a \rangle$ be a cyclic group.

- If G is infinite, then a and a^{-1} are the only generators of G, i.e., $G = \langle b \rangle \iff b \in \{a, a^{-1}\}$.

Proof. "$\Leftarrow$" is clear. For "$\Rightarrow$", $b \in G = \langle a \rangle$, so $b = a^n$ for some $n \in \mathbb{Z}$. Conversely, $a \in G = \langle b \rangle$, so $a = b^k$ for some $k \in \mathbb{Z}$. Hence, $a = b^k$

Theorem (3.6)

Let $G = \langle a \rangle$ be a cyclic group.

- If G is infinite, then a and a^{-1} are the only generators of G, i.e., $G = \langle b \rangle \iff b \in \{a, a^{-1}\}$.

Proof. "$\Leftarrow$" is clear. For "$\Rightarrow$", $b \in G = \langle a \rangle$, so $b = a^n$ for some $n \in \mathbb{Z}$. Conversely, $a \in G = \langle b \rangle$, so $a = b^k$ for some $k \in \mathbb{Z}$. Hence, $a = b^k = (a^n)^k$

Theorem (3.6)

Let $G = \langle a \rangle$ be a cyclic group.

- If G is infinite, then a and a^{-1} are the only generators of G, i.e., $G = \langle b \rangle \iff b \in \{a, a^{-1}\}$.

Proof. "$\Leftarrow$" is clear. For "$\Rightarrow$", $b \in G = \langle a \rangle$, so $b = a^n$ for some $n \in \mathbb{Z}$. Conversely, $a \in G = \langle b \rangle$, so $a = b^k$ for some $k \in \mathbb{Z}$. Hence, $a = b^k = (a^n)^k = a^{nk}$.

Theorem (3.6)

Let $G = \langle a \rangle$ be a cyclic group.

- If G is infinite, then a and a^{-1} are the only generators of G, i.e., $G = \langle b \rangle \iff b \in \{a, a^{-1}\}$.

Proof. "$\Leftarrow$" is clear. For "$\Rightarrow$", $b \in G = \langle a \rangle$, so $b = a^n$ for some $n \in \mathbb{Z}$. Conversely, $a \in G = \langle b \rangle$, so $a = b^k$ for some $k \in \mathbb{Z}$. Hence, $a = b^k = (a^n)^k = a^{nk}$. Thus, $nk = 1$

Theorem (3.6)

Let $G = \langle a \rangle$ be a cyclic group.

- If G is infinite, then a and a^{-1} are the only generators of G, i.e., $G = \langle b \rangle \iff b \in \{a, a^{-1}\}$.

Proof. "$\Leftarrow$" is clear. For "$\Rightarrow$", $b \in G = \langle a \rangle$, so $b = a^n$ for some $n \in \mathbb{Z}$. Conversely, $a \in G = \langle b \rangle$, so $a = b^k$ for some $k \in \mathbb{Z}$. Hence, $a = b^k = (a^n)^k = a^{nk}$. Thus, $nk = 1$ and this implies $n = 1$ or -1,

Theorem (3.6)

Let $G = \langle a \rangle$ be a cyclic group.

- If G is infinite, then a and a^{-1} are the only generators of G, i.e., $G = \langle b \rangle \iff b \in \{a, a^{-1}\}$.

Proof. "$\Leftarrow$" is clear. For "$\Rightarrow$", $b \in G = \langle a \rangle$, so $b = a^n$ for some $n \in \mathbb{Z}$. Conversely, $a \in G = \langle b \rangle$, so $a = b^k$ for some $k \in \mathbb{Z}$. Hence, $a = b^k = (a^n)^k = a^{nk}$. Thus, $nk = 1$ and this implies $n = 1$ or -1, i.e., $b = a$ or a^{-1}.

Theorem (3.6)

Let $G = \langle a \rangle$ be a cyclic group.

- If G is infinite, then a and a^{-1} are the only generators of G, i.e., $G = \langle b \rangle \iff b \in \{a, a^{-1}\}$.
- If G is finite of order m,

Proof. "$\Leftarrow$" is clear. For "$\Rightarrow$", $b \in G = \langle a \rangle$, so $b = a^n$ for some $n \in \mathbb{Z}$. Conversely, $a \in G = \langle b \rangle$, so $a = b^k$ for some $k \in \mathbb{Z}$. Hence, $a = b^k = (a^n)^k = a^{nk}$. Thus, $nk = 1$ and this implies $n = 1$ or -1, i.e., $b = a$ or a^{-1}.

Theorem (3.6)

Let $G = \langle a \rangle$ be a cyclic group.

- If G is infinite, then a and a^{-1} are the only generators of G, i.e., $G = \langle b \rangle \iff b \in \{a, a^{-1}\}$.
- If G is finite of order m, then

Proof. "$\Leftarrow$" is clear. For "$\Rightarrow$", $b \in G = \langle a \rangle$, so $b = a^n$ for some $n \in \mathbb{Z}$. Conversely, $a \in G = \langle b \rangle$, so $a = b^k$ for some $k \in \mathbb{Z}$. Hence, $a = b^k = (a^n)^k = a^{nk}$. Thus, $nk = 1$ and this implies $n = 1$ or -1, i.e., $b = a$ or a^{-1}.

Theorem (3.6)

Let $G = \langle a \rangle$ be a cyclic group.

- If G is infinite, then a and a^{-1} are the only generators of G, i.e., $G = \langle b \rangle \iff b \in \{a, a^{-1}\}$.
- If G is finite of order m, then
  - $\langle a^k \rangle = \langle a^d \rangle$,

Proof. "$\Leftarrow$" is clear. For "$\Rightarrow$", $b \in G = \langle a \rangle$, so $b = a^n$ for some $n \in \mathbb{Z}$. Conversely, $a \in G = \langle b \rangle$, so $a = b^k$ for some $k \in \mathbb{Z}$. Hence, $a = b^k = (a^n)^k = a^{nk}$. Thus, $nk = 1$ and this implies $n = 1$ or -1, i.e., $b = a$ or a^{-1}.

Theorem (3.6)

Let $G = \langle a \rangle$ be a cyclic group.

- If G is infinite, then a and a^{-1} are the only generators of G, i.e., $G = \langle b \rangle \iff b \in \{a, a^{-1}\}$.
- If G is finite of order m, then
  - $\langle a^k \rangle = \langle a^d \rangle$, where $d = (k, m)$;

Proof. "$\Leftarrow$" is clear. For "$\Rightarrow$", $b \in G = \langle a \rangle$, so $b = a^n$ for some $n \in \mathbb{Z}$. Conversely, $a \in G = \langle b \rangle$, so $a = b^k$ for some $k \in \mathbb{Z}$. Hence, $a = b^k = (a^n)^k = a^{nk}$. Thus, $nk = 1$ and this implies $n = 1$ or -1, i.e., $b = a$ or a^{-1}.

Theorem (3.6)

Let $G = \langle a \rangle$ be a cyclic group.

- If G is infinite, then a and a^{-1} are the only generators of G, i.e., $G = \langle b \rangle \iff b \in \{a, a^{-1}\}$.
- If G is finite of order m, then
  - $\langle a^k \rangle = \langle a^d \rangle$, where $d = (k, m)$;

Proof. Because $d = (k, m)$,

Theorem (3.6)

Let $G = \langle a \rangle$ be a cyclic group.

- If G is infinite, then a and a^{-1} are the only generators of G, i.e., $G = \langle b \rangle \iff b \in \{a, a^{-1}\}$.
- If G is finite of order m, then
  - $\langle a^k \rangle = \langle a^d \rangle$, where $d = (k, m)$;

Proof. Because $d = (k, m)$, $\exists s, t \in \mathbb{Z}$ such that $sk + tm = d$.

Theorem (3.6)

Let $G = \langle a \rangle$ be a cyclic group.

- If G is infinite, then a and a^{-1} are the only generators of G, i.e., $G = \langle b \rangle \iff b \in \{a, a^{-1}\}$.
- If G is finite of order m, then
  - $\langle a^k \rangle = \langle a^d \rangle$, where $d = (k, m)$;

Proof. Because $d = (k, m)$, $\exists s, t \in \mathbb{Z}$ such that $sk + tm = d$.
Hence, $a^d = a^{sk+tm}$

Theorem (3.6)

Let $G = \langle a \rangle$ be a cyclic group.

- If G is infinite, then a and a^{-1} are the only generators of G, i.e., $G = \langle b \rangle \iff b \in \{a, a^{-1}\}$.
- If G is finite of order m, then
  - $\langle a^k \rangle = \langle a^d \rangle$, where $d = (k, m)$;

Proof. Because $d = (k, m)$, $\exists s, t \in \mathbb{Z}$ such that $sk + tm = d$.
Hence, $a^d = a^{sk+tm} = (a^k)^s (a^m)^t$

Theorem (3.6)

Let $G = \langle a \rangle$ be a cyclic group.

- If G is infinite, then a and a^{-1} are the only generators of G, i.e., $G = \langle b \rangle \iff b \in \{a, a^{-1}\}$.
- If G is finite of order m, then
  - $\langle a^k \rangle = \langle a^d \rangle$, where $d = (k, m)$;

Proof. Because $d = (k, m)$, $\exists s, t \in \mathbb{Z}$ such that $sk + tm = d$.
Hence, $a^d = a^{sk+tm} = (a^k)^s (a^m)^t = (a^k)^s e^t$

Theorem (3.6)

Let $G = \langle a \rangle$ be a cyclic group.

- If G is infinite, then a and a^{-1} are the only generators of G, i.e., $G = \langle b \rangle \iff b \in \{a, a^{-1}\}$.
- If G is finite of order m, then
  - $\langle a^k \rangle = \langle a^d \rangle$, where $d = (k, m)$;

Proof. Because $d = (k, m)$, $\exists s, t \in \mathbb{Z}$ such that $sk + tm = d$.
Hence, $a^d = a^{sk+tm} = (a^k)^s (a^m)^t = (a^k)^s e^t = (a^k)^s$

Theorem (3.6)

Let $G = \langle a \rangle$ be a cyclic group.

- If G is infinite, then a and a^{-1} are the only generators of G, i.e., $G = \langle b \rangle \iff b \in \{a, a^{-1}\}$.
- If G is finite of order m, then
  - $\langle a^k \rangle = \langle a^d \rangle$, where $d = (k, m)$;

Proof. Because $d = (k, m)$, $\exists s, t \in \mathbb{Z}$ such that $sk + tm = d$.
Hence, $a^d = a^{sk+tm} = (a^k)^s (a^m)^t = (a^k)^s e^t = (a^k)^s \in \langle a^k \rangle$.

Theorem (3.6)

Let $G = \langle a \rangle$ be a cyclic group.

- If G is infinite, then a and a^{-1} are the only generators of G, i.e., $G = \langle b \rangle \iff b \in \{a, a^{-1}\}$.
- If G is finite of order m, then
  - $\langle a^k \rangle = \langle a^d \rangle$, where $d = (k, m)$;

Proof. Because $d = (k, m)$, $\exists s, t \in \mathbb{Z}$ such that $sk + tm = d$.
Hence, $a^d = a^{sk+tm} = (a^k)^s (a^m)^t = (a^k)^s e^t = (a^k)^s \in \langle a^k \rangle$.
Conversely, since $d \mid k$,

Theorem (3.6)

Let $G = \langle a \rangle$ be a cyclic group.

- If G is infinite, then a and a^{-1} are the only generators of G, i.e., $G = \langle b \rangle \iff b \in \{a, a^{-1}\}$.
- If G is finite of order m, then
  - $\langle a^k \rangle = \langle a^d \rangle$, where $d = (k, m)$;

Proof. Because $d = (k, m)$, $\exists s, t \in \mathbb{Z}$ such that $sk + tm = d$.
Hence, $a^d = a^{sk+tm} = (a^k)^s (a^m)^t = (a^k)^s e^t = (a^k)^s \in \langle a^k \rangle$.
Conversely, since $d \mid k$, $a^k \in \langle a^d \rangle$.

Theorem (3.6)

Let $G = \langle a \rangle$ be a cyclic group.

- If G is infinite, then a and a^{-1} are the only generators of G, i.e., $G = \langle b \rangle \iff b \in \{a, a^{-1}\}$.
- If G is finite of order m, then
  - $\langle a^k \rangle = \langle a^d \rangle$, where $d = (k, m)$;

Proof. Because $d = (k, m)$, $\exists s, t \in \mathbb{Z}$ such that $sk + tm = d$.
Hence, $a^d = a^{sk+tm} = (a^k)^s (a^m)^t = (a^k)^s e^t = (a^k)^s \in \langle a^k \rangle$.
Conversely, since $d \mid k$, $a^k \in \langle a^d \rangle$. Therefore, $\langle a^k \rangle = \langle a^d \rangle$.

Theorem (3.6)

Let $G = \langle a \rangle$ be a cyclic group.

- If G is infinite, then a and a^{-1} are the only generators of G, i.e., $G = \langle b \rangle \iff b \in \{a, a^{-1}\}$.
- If G is finite of order m, then
  - $\langle a^k \rangle = \langle a^d \rangle$, where $d = (k, m)$;

Proof. Because $d = (k, m)$, $\exists s, t \in \mathbb{Z}$ such that $sk + tm = d$. Hence, $a^d = a^{sk+tm} = (a^k)^s (a^m)^t = (a^k)^s e^t = (a^k)^s \in \langle a^k \rangle$. Conversely, since $d \mid k$, $a^k \in \langle a^d \rangle$. Therefore, $\langle a^k \rangle = \langle a^d \rangle$. Moreover,

Theorem (3.6)

Let $G = \langle a \rangle$ be a cyclic group.

- If G is infinite, then a and a^{-1} are the only generators of G, i.e., $G = \langle b \rangle \iff b \in \{a, a^{-1}\}$.
- If G is finite of order m, then
  - $\langle a^k \rangle = \langle a^d \rangle$, where $d = (k, m)$;

Proof. Because $d = (k, m)$, $\exists s, t \in \mathbb{Z}$ such that $sk + tm = d$.
Hence, $a^d = a^{sk+tm} = (a^k)^s (a^m)^t = (a^k)^s e^t = (a^k)^s \in \langle a^k \rangle$.
Conversely, since $d \mid k$, $a^k \in \langle a^d \rangle$. Therefore, $\langle a^k \rangle = \langle a^d \rangle$.
Moreover, $|a^k| = |a^d|$

Theorem (3.6)

Let $G = \langle a \rangle$ be a cyclic group.

- If G is infinite, then a and a^{-1} are the only generators of G, i.e., $G = \langle b \rangle \iff b \in \{a, a^{-1}\}$.
- If G is finite of order m, then
  - $\langle a^k \rangle = \langle a^d \rangle$, where $d = (k, m)$;

Proof. Because $d = (k, m)$, $\exists s, t \in \mathbb{Z}$ such that $sk + tm = d$.
Hence, $a^d = a^{sk+tm} = (a^k)^s (a^m)^t = (a^k)^s e^t = (a^k)^s \in \langle a^k \rangle$.
Conversely, since $d \mid k$, $a^k \in \langle a^d \rangle$. Therefore, $\langle a^k \rangle = \langle a^d \rangle$.
Moreover, $|a^k| = |a^d| = \frac{m}{d}$.

by Theorem 3.4

Theorem (3.6)

Let $G = \langle a \rangle$ be a cyclic group.

- If G is infinite, then a and a^{-1} are the only generators of G, i.e., $G = \langle b \rangle \iff b \in \{a, a^{-1}\}$.
- If G is finite of order m, then
  - $\langle a^k \rangle = \langle a^d \rangle$, where $d = (k, m)$;

Proof. Because $d = (k, m)$, $\exists s, t \in \mathbb{Z}$ such that $sk + tm = d$.
Hence, $a^d = a^{sk+tm} = (a^k)^s (a^m)^t = (a^k)^s e^t = (a^k)^s \in \langle a^k \rangle$.
Conversely, since $d \mid k$, $a^k \in \langle a^d \rangle$. Therefore, $\langle a^k \rangle = \langle a^d \rangle$.
Moreover, $|a^k| = |a^d| = \frac{m}{d}$.
Hence, a^k is a generator of G

Theorem (3.6)

Let $G = \langle a \rangle$ be a cyclic group.

- If G is infinite, then a and a^{-1} are the only generators of G, i.e., $G = \langle b \rangle \iff b \in \{a, a^{-1}\}$.
- If G is finite of order m, then
  - $\langle a^k \rangle = \langle a^d \rangle$, where $d = (k, m)$;

Proof. Because $d = (k, m)$, $\exists s, t \in \mathbb{Z}$ such that $sk + tm = d$.
Hence, $a^d = a^{sk+tm} = (a^k)^s (a^m)^t = (a^k)^s e^t = (a^k)^s \in \langle a^k \rangle$.
Conversely, since $d \mid k$, $a^k \in \langle a^d \rangle$. Therefore, $\langle a^k \rangle = \langle a^d \rangle$.
Moreover, $|a^k| = |a^d| = \frac{m}{d}$.
Hence, a^k is a generator of $G \iff |a^k| = m$

Theorem (3.6)

Let $G = \langle a \rangle$ be a cyclic group.

- If G is infinite, then a and a^{-1} are the only generators of G, i.e., $G = \langle b \rangle \iff b \in \{a, a^{-1}\}$.
- If G is finite of order m, then
  - $\langle a^k \rangle = \langle a^d \rangle$, where $d = (k, m)$;

Proof. Because $d = (k, m)$, $\exists s, t \in \mathbb{Z}$ such that $sk + tm = d$.
Hence, $a^d = a^{sk+tm} = (a^k)^s (a^m)^t = (a^k)^s e^t = (a^k)^s \in \langle a^k \rangle$.
Conversely, since $d \mid k$, $a^k \in \langle a^d \rangle$. Therefore, $\langle a^k \rangle = \langle a^d \rangle$.
Moreover, $|a^k| = |a^d| = \frac{m}{d}$.
Hence, a^k is a generator of $G \iff |a^k| = m \iff (k, m) = 1$.

Theorem (3.6)

Let $G = \langle a \rangle$ be a cyclic group.

- If G is infinite, then a and a^{-1} are the only generators of G, i.e., $G = \langle b \rangle \iff b \in \{a, a^{-1}\}$.
- If G is finite of order m, then
  - $\langle a^k \rangle = \langle a^d \rangle$, where $d = (k, m)$;
  - a^k is a generator of G

Proof. Because $d = (k, m)$, $\exists s, t \in \mathbb{Z}$ such that $sk + tm = d$.
Hence, $a^d = a^{sk+tm} = (a^k)^s (a^m)^t = (a^k)^s e^t = (a^k)^s \in \langle a^k \rangle$.
Conversely, since $d \mid k$, $a^k \in \langle a^d \rangle$. Therefore, $\langle a^k \rangle = \langle a^d \rangle$.
Moreover, $|a^k| = |a^d| = \frac{m}{d}$.
Hence, a^k is a generator of $G \iff |a^k| = m \iff (k, m) = 1$.

Theorem (3.6)

Let $G = \langle a \rangle$ be a cyclic group.

- If G is infinite, then a and a^{-1} are the only generators of G, i.e., $G = \langle b \rangle \iff b \in \{a, a^{-1}\}$.
- If G is finite of order m, then
  - $\langle a^k \rangle = \langle a^d \rangle$, where $d = (k, m)$;
  - a^k is a generator of $G \iff (k, m) = 1$.

Proof. Because $d = (k, m)$, $\exists s, t \in \mathbb{Z}$ such that $sk + tm = d$.
Hence, $a^d = a^{sk+tm} = (a^k)^s (a^m)^t = (a^k)^s e^t = (a^k)^s \in \langle a^k \rangle$.
Conversely, since $d \mid k$, $a^k \in \langle a^d \rangle$. Therefore, $\langle a^k \rangle = \langle a^d \rangle$.
Moreover, $|a^k| = |a^d| = \frac{m}{d}$.
Hence, a^k is a generator of $G \iff |a^k| = m \iff (k, m) = 1$.