§3.2 Subgroups

Shaoyun Yi

MATH 546/701I

University of South Carolina

May 18-19, 2020

Review

- Group $(G, *)$ $\begin{cases} \text{(i)} & \text{Closure} \leftrightarrow * \\ \text{(ii)} & \text{Associativity} \leftrightarrow \text{parentheses} \\ \text{(iii)} & \text{Identity: Uniqueness by Associativity} \\ \text{(iv)} & \text{Inverses: } (a^{-1})^{-1} = a \end{cases}$

Review

- Group $(G, *)$ $\begin{cases} \text{(i)} & \text{Closure} \leftrightarrow * \\ \text{(ii)} & \text{Associativity} \leftrightarrow \text{parentheses} \\ \text{(iii)} & \text{Identity: Uniqueness by Associativity} \\ \text{(iv)} & \text{Inverses: } (a^{-1})^{-1} = a \end{cases}$
- Examples: $(\mathbf{R}^\times, \cdot)$, $(\mathrm{Sym}(S), \circ)$, $(M_n(\mathbf{R}), +_{\text{matrix}})$, $(\mathrm{GL}_n(\mathbf{R}), \cdot_{\text{matrix}})$

Review

- Group $(G, *)$ $\begin{cases} \text{(i)} & \text{Closure} \leftrightarrow * \\ \text{(ii)} & \text{Associativity} \leftrightarrow \text{parentheses} \\ \text{(iii)} & \text{Identity: Uniqueness by Associativity} \\ \text{(iv)} & \text{Inverses: } (a^{-1})^{-1} = a \end{cases}$
- Examples: $(\mathbf{R}^{\times}, \cdot)$, $(\mathrm{Sym}(S), \circ)$, $(M_n(\mathbf{R}), +_{\text{matrix}})$, $(\mathrm{GL}_n(\mathbf{R}), \cdot_{\text{matrix}})$
- Cancellation law

Review

- Group $(G, *)$ $\begin{cases} \text{(i)} & \text{Closure} \leftrightarrow * \\ \text{(ii)} & \text{Associativity} \leftrightarrow \text{parentheses} \\ \text{(iii)} & \text{Identity: Uniqueness by Associativity} \\ \text{(iv)} & \text{Inverses: } (a^{-1})^{-1} = a \end{cases}$

- Examples: $(\mathbf{R}^\times, \cdot)$, $(\mathrm{Sym}(S), \circ)$, $(M_n(\mathbf{R}), +_{\text{matrix}})$, $(\mathrm{GL}_n(\mathbf{R}), \cdot_{\text{matrix}})$

- Cancellation law

- Abelian group: eg. $(\mathbf{Z}, +)$, $(\pm 1, \cdot)$, $(\mathbf{Q}^\times, \cdot)$, $(\mathbf{Z}_n, +_{[a]_n})$, $(\mathbf{Z}_n^\times, \cdot_{[a]_n})$

Review

- Group $(G, *)$ $\begin{cases} \text{(i)} & \text{Closure} \leftrightarrow * \\ \text{(ii)} & \text{Associativity} \leftrightarrow \text{parentheses} \\ \text{(iii)} & \text{Identity: Uniqueness by Associativity} \\ \text{(iv)} & \text{Inverses: } (a^{-1})^{-1} = a \end{cases}$

- Examples: $(\mathbf{R}^\times, \cdot)$, $(\mathrm{Sym}(S), \circ)$, $(M_n(\mathbf{R}), +_{\text{matrix}})$, $(\mathrm{GL}_n(\mathbf{R}), \cdot_{\text{matrix}})$

- Cancellation law

- Abelian group: eg. $(\mathbf{Z}, +)$, $(\pm 1, \cdot)$, $(\mathbf{Q}^\times, \cdot)$, $(\mathbf{Z}_n, +_{[a]_n})$, $(\mathbf{Z}_n^\times, \cdot_{[a]_n})$

- Finite group (**order**) vs. Infinite group

Review

- Group $(G, *)$ $\begin{cases} \text{(i)} & \text{Closure} \leftrightarrow * \\ \text{(ii)} & \text{Associativity} \leftrightarrow \text{parentheses} \\ \text{(iii)} & \text{Identity: Uniqueness by Associativity} \\ \text{(iv)} & \text{Inverses: } (a^{-1})^{-1} = a \end{cases}$
- Examples: $(\mathbf{R}^\times, \cdot)$, $(\mathrm{Sym}(S), \circ)$, $(M_n(\mathbf{R}), +_{\text{matrix}})$, $(\mathrm{GL}_n(\mathbf{R}), \cdot_{\text{matrix}})$
- Cancellation law
- Abelian group: eg. $(\mathbf{Z}, +)$, $(\pm 1, \cdot)$, $(\mathbf{Q}^\times, \cdot)$, $(\mathbf{Z}_n, +_{[a]_n})$, $(\mathbf{Z}_n^\times, \cdot_{[a]_n})$
- Finite group (**order**) vs. Infinite group
- Eg. Conjugacy $\leftrightarrow$ Equivalence relation

Definition

Definition 1

Let G be a group, and let H be a subset of G. Then H is called a **subgroup** of G if H is itself a group, under the operation induced by G.

Definition

Definition 1

Let G be a group, and let H be a subset of G. Then H is called a **subgroup** of G if H is itself a group, under the operation induced by G.

Example 2

$\mathbf{Z} \subseteq \mathbf{Q} \subseteq \mathbf{R} \subseteq \mathbf{C}$: each group is a subgroup of the next under ordinary addition.

Definition

Definition 1

Let G be a group, and let H be a subset of G. Then H is called a **subgroup** of G if H is itself a group, under the operation induced by G.

Example 2

$\mathbf{Z} \subseteq \mathbf{Q} \subseteq \mathbf{R} \subseteq \mathbf{C}$: each group is a subgroup of the next under ordinary addition.

Example 3

multiplicative (sub)groups of nonzero elements: $\{\pm 1\} \subseteq \mathbf{Q}^\times \subseteq \mathbf{R}^\times \subseteq \mathbf{C}^\times$.

We cannot include the set of nonzero integers in this diagram. (Why?)

More examples

Example 4

The set of all multiples of a fixed positive integer n, denoted by

$n\mathbf{Z} = \{x \in \mathbf{Z} \mid x = nk \text{ for some } k \in \mathbf{Z}\}$ is a subgroup of $\mathbf{Z}$ under addition.

More examples

Example 4

The set of all multiples of a fixed positive integer n, denoted by

$n\mathbf{Z} = \{x \in \mathbf{Z} \mid x = nk \text{ for some } k \in \mathbf{Z}\}$ is a subgroup of $\mathbf{Z}$ under addition.

(i) Closure: (Check it!) [

More examples

Example 4

The set of all multiples of a fixed positive integer n, denoted by

$n\mathbf{Z} = \{x \in \mathbf{Z} \mid x = nk \text{ for some } k \in \mathbf{Z}\}$ is a subgroup of $\mathbf{Z}$ under addition.

(i) Closure: (Check it!) [$a + b = nq + nk = n(q + k)$ for some $q, k \in \mathbf{Z}$]

More examples

Example 4

The set of all multiples of a fixed positive integer n, denoted by

$n\mathbf{Z} = \{x \in \mathbf{Z} \mid x = nk \text{ for some } k \in \mathbf{Z}\}$ is a subgroup of $\mathbf{Z}$ under addition.

(i) Closure: (Check it!) [$a + b = nq + nk = n(q + k)$ for some $q, k \in \mathbf{Z}$]
(ii) Associative law: ✓;

More examples

Example 4

The set of all multiples of a fixed positive integer n, denoted by

$n\mathbf{Z} = \{x \in \mathbf{Z} \mid x = nk \text{ for some } k \in \mathbf{Z}\}$ is a subgroup of $\mathbf{Z}$ under addition.

(i) Closure: (Check it!) $[a + b = nq + nk = n(q + k)$ for some $q, k \in \mathbf{Z}]$
(ii) Associative law: ✓; (iii) Identity: $0 = n \cdot 0$;

More examples

Example 4

The set of all multiples of a fixed positive integer n, denoted by

$n\mathbf{Z} = \{x \in \mathbf{Z} \mid x = nk \text{ for some } k \in \mathbf{Z}\}$ is a subgroup of $\mathbf{Z}$ under addition.

(i) Closure: (Check it!) $[a + b = nq + nk = n(q + k)$ for some $q, k \in \mathbf{Z}]$
(ii) Associative law: ✓; (iii) Identity: $0 = n \cdot 0$; (iv) Inverses: its negative.

Example 5

More examples

Example 4

The set of all multiples of a fixed positive integer n, denoted by

$n\mathbf{Z} = \{x \in \mathbf{Z} \mid x = nk \text{ for some } k \in \mathbf{Z}\}$ is a subgroup of $\mathbf{Z}$ under addition.

(i) Closure: (Check it!) $[a + b = nq + nk = n(q + k)$ for some $q, k \in \mathbf{Z}]$
(ii) Associative law: ✓; (iii) Identity: $0 = n \cdot 0$; (iv) Inverses: its negative.

Example 5

$\mathbf{R}^+ = \{x \in \mathbf{R} | x > 0\}$ is a subgroup of $\mathbf{R}^\times$ under multiplication. (Check it!)

More examples

Example 4

The set of all multiples of a fixed positive integer n, denoted by

$n\mathbf{Z} = \{x \in \mathbf{Z} \mid x = nk \text{ for some } k \in \mathbf{Z}\}$ is a subgroup of $\mathbf{Z}$ under addition.

(i) Closure: (Check it!) $[a + b = nq + nk = n(q + k)$ for some $q, k \in \mathbf{Z}]$
(ii) Associative law: $\checkmark$; (iii) Identity: $0 = n \cdot 0$; (iv) Inverses: its negative.

Example 5

$\mathbf{R}^+ = \{x \in \mathbf{R} | x > 0\}$ is a subgroup of $\mathbf{R}^\times$ under multiplication. (Check it!)
(i) if $x, y > 0$, then $xy > 0$;

More examples

Example 4

The set of all multiples of a fixed positive integer n, denoted by

$n\mathbf{Z} = \{x \in \mathbf{Z} \mid x = nk \text{ for some } k \in \mathbf{Z}\}$ is a subgroup of $\mathbf{Z}$ under addition.

(i) Closure: (Check it!) [$a + b = nq + nk = n(q + k)$ for some $q, k \in \mathbf{Z}$]
(ii) Associative law: ✓; (iii) Identity: $0 = n \cdot 0$; (iv) Inverses: its negative.

Example 5

$\mathbf{R}^+ = \{x \in \mathbf{R} | x > 0\}$ is a subgroup of $\mathbf{R}^\times$ under multiplication. (Check it!)
(i) if $x, y > 0$, then $xy > 0$; (ii) ✓;

More examples

Example 4

The set of all multiples of a fixed positive integer n, denoted by

$n\mathbf{Z} = \{x \in \mathbf{Z} \mid x = nk \text{ for some } k \in \mathbf{Z}\}$ is a subgroup of $\mathbf{Z}$ under addition.

(i) Closure: (Check it!) $[a + b = nq + nk = n(q + k)$ for some $q, k \in \mathbf{Z}]$
(ii) Associative law: ✓; (iii) Identity: $0 = n \cdot 0$; (iv) Inverses: its negative.

Example 5

$\mathbf{R}^+ = \{x \in \mathbf{R} | x > 0\}$ is a subgroup of $\mathbf{R}^\times$ under multiplication. (Check it!)
(i) if $x, y > 0$, then $xy > 0$; (ii) ✓; (iii) 1;

More examples

Example 4

The set of all multiples of a fixed positive integer n, denoted by

$n\mathbf{Z} = \{x \in \mathbf{Z} \mid x = nk \text{ for some } k \in \mathbf{Z}\}$ is a subgroup of $\mathbf{Z}$ under addition.

(i) Closure: (Check it!) $[a + b = nq + nk = n(q + k)$ for some $q, k \in \mathbf{Z}]$
(ii) Associative law: ✓; (iii) Identity: $0 = n \cdot 0$; (iv) Inverses: its negative.

Example 5

$\mathbf{R}^+ = \{x \in \mathbf{R} | x > 0\}$ is a subgroup of $\mathbf{R}^\times$ under multiplication. (Check it!)
(i) if $x, y > 0$, then $xy > 0$; (ii) ✓; (iii) 1; (iv) $1/x > 0$, since $x > 0$.

Example 6

More examples

Example 4

The set of all multiples of a fixed positive integer n, denoted by

$n\mathbf{Z} = \{x \in \mathbf{Z} \mid x = nk \text{ for some } k \in \mathbf{Z}\}$ is a subgroup of $\mathbf{Z}$ under addition.

(i) Closure: (Check it!) $[a + b = nq + nk = n(q + k)$ for some $q, k \in \mathbf{Z}]$
(ii) Associative law: ✓; (iii) Identity: $0 = n \cdot 0$; (iv) Inverses: its negative.

Example 5

$\mathbf{R}^+ = \{x \in \mathbf{R} | x > 0\}$ is a subgroup of $\mathbf{R}^\times$ under multiplication. (Check it!)
(i) if $x, y > 0$, then $xy > 0$; (ii) ✓; (iii) 1; (iv) $1/x > 0$, since $x > 0$.

Example 6

The **special linear group over R:** $\mathrm{SL}_n(\mathbf{R}) = \{A \in \mathrm{GL}_n(\mathbf{R}) | \det(A) = 1\}$ is a subgroup of $\mathrm{GL}_n(\mathbf{R})$ under matrix multiplication. (Check it!)

More examples

Example 4

The set of all multiples of a fixed positive integer n, denoted by

$n\mathbf{Z} = \{x \in \mathbf{Z} \mid x = nk$ for some $k \in \mathbf{Z}\}$ is a subgroup of $\mathbf{Z}$ under addition.

(i) Closure: (Check it!) [$a + b = nq + nk = n(q + k)$ for some $q, k \in \mathbf{Z}$]
(ii) Associative law: ✓; (iii) Identity: $0 = n \cdot 0$; (iv) Inverses: its negative.

Example 5

$\mathbf{R}^+ = \{x \in \mathbf{R} | x > 0\}$ is a subgroup of $\mathbf{R}^\times$ under multiplication. (Check it!)
(i) if $x, y > 0$, then $xy > 0$; (ii) ✓; (iii) 1; (iv) $1/x > 0$, since $x > 0$.

Example 6

The **special linear group over R:** $\mathrm{SL}_n(\mathbf{R}) = \{A \in \mathrm{GL}_n(\mathbf{R}) | \det(A) = 1\}$ is a subgroup of $\mathrm{GL}_n(\mathbf{R})$ under matrix multiplication. (Check it!)
(i) $\det(AB) = \det(A)\det(B)$;

More examples

Example 4

The set of all multiples of a fixed positive integer n, denoted by

$n\mathbf{Z} = \{x \in \mathbf{Z} \mid x = nk \text{ for some } k \in \mathbf{Z}\}$ is a subgroup of $\mathbf{Z}$ under addition.

(i) Closure: (Check it!) $[a + b = nq + nk = n(q + k)$ for some $q, k \in \mathbf{Z}]$
(ii) Associative law: ✓; (iii) Identity: $0 = n \cdot 0$; (iv) Inverses: its negative.

Example 5

$\mathbf{R}^+ = \{x \in \mathbf{R} | x > 0\}$ is a subgroup of $\mathbf{R}^\times$ under multiplication. (Check it!)
(i) if $x, y > 0$, then $xy > 0$; (ii) ✓; (iii) 1; (iv) $1/x > 0$, since $x > 0$.

Example 6

The **special linear group over R:** $\mathrm{SL}_n(\mathbf{R}) = \{A \in \mathrm{GL}_n(\mathbf{R}) | \det(A) = 1\}$ is a subgroup of $\mathrm{GL}_n(\mathbf{R})$ under matrix multiplication. (Check it!)
(i) $\det(AB) = \det(A)\det(B)$; (ii) ✓;

More examples

Example 4

The set of all multiples of a fixed positive integer n, denoted by

$n\mathbf{Z} = \{x \in \mathbf{Z} \mid x = nk \text{ for some } k \in \mathbf{Z}\}$ is a subgroup of $\mathbf{Z}$ under addition.

(i) Closure: (Check it!) $[a + b = nq + nk = n(q + k)$ for some $q, k \in \mathbf{Z}]$
(ii) Associative law: ✓; (iii) Identity: $0 = n \cdot 0$; (iv) Inverses: its negative.

Example 5

$\mathbf{R}^+ = \{x \in \mathbf{R} | x > 0\}$ is a subgroup of $\mathbf{R}^\times$ under multiplication. (Check it!)
(i) if $x, y > 0$, then $xy > 0$; (ii) ✓; (iii) 1; (iv) $1/x > 0$, since $x > 0$.

Example 6

The **special linear group over R:** $\mathrm{SL}_n(\mathbf{R}) = \{A \in \mathrm{GL}_n(\mathbf{R}) | \det(A) = 1\}$ is a subgroup of $\mathrm{GL}_n(\mathbf{R})$ under matrix multiplication. (Check it!)
(i) $\det(AB) = \det(A)\det(B)$; (ii) ✓; (iii) I_n;

More examples

Example 4

The set of all multiples of a fixed positive integer n, denoted by

$n\mathbf{Z} = \{x \in \mathbf{Z} \mid x = nk \text{ for some } k \in \mathbf{Z}\}$ is a subgroup of $\mathbf{Z}$ under addition.

(i) Closure: (Check it!) $[a + b = nq + nk = n(q + k)$ for some $q, k \in \mathbf{Z}]$
(ii) Associative law: ✓; (iii) Identity: $0 = n \cdot 0$; (iv) Inverses: its negative.

Example 5

$\mathbf{R}^+ = \{x \in \mathbf{R} | x > 0\}$ is a subgroup of $\mathbf{R}^\times$ under multiplication. (Check it!)
(i) if $x, y > 0$, then $xy > 0$; (ii) ✓; (iii) 1; (iv) $1/x > 0$, since $x > 0$.

Example 6

The **special linear group over R:** $\mathrm{SL}_n(\mathbf{R}) = \{A \in \mathrm{GL}_n(\mathbf{R}) | \det(A) = 1\}$ is a subgroup of $\mathrm{GL}_n(\mathbf{R})$ under matrix multiplication. (Check it!)
(i) $\det(AB) = \det(A)\det(B)$; (ii) ✓; (iii) I_n; (iv) A^{-1}, since $\det(A^{-1}) = 1$.

A simpler way

Proposition 1

Let G be a group with identity element e, and let H be a subset of G. Then H is a subgroup of G if and only if the following conditions hold:

(i) $ab \in H$ *for all* $a, b \in H$;

(ii) $e \in H$;

(iii) $a^{-1} \in H$ *for all* $a \in H$.

A simpler way

Proposition 1

Let G be a group with identity element e, and let H be a subset of G. Then H is a subgroup of G if and only if the following conditions hold:

(i) $ab \in H$ *for all* $a, b \in H$;

(ii) $e \in H$;

(iii) $a^{-1} \in H$ *for all* $a \in H$.

$(\Rightarrow)$:

A simpler way

Proposition 1

Let G be a group with identity element e, and let H be a subset of G. Then H is a subgroup of G if and only if the following conditions hold:

(i) $ab \in H$ *for all* $a, b \in H$;

(ii) $e \in H$;

(iii) $a^{-1} \in H$ *for all* $a \in H$.

($\Rightarrow$): (i) is trivial. (Why?);

Proposition 1

Let G be a group with identity element e, and let H be a subset of G. Then H is a subgroup of G if and only if the following conditions hold:

(i) $ab \in H$ *for all* $a, b \in H$;

(ii) $e \in H$;

(iii) $a^{-1} \in H$ *for all* $a \in H$.

($\Rightarrow$): (i) is trivial. (Why?);
(ii) Let e' be an identity element for H. *To show*: $e' = e$.

A simpler way

Proposition 1

Let G be a group with identity element e, and let H be a subset of G. Then H is a subgroup of G if and only if the following conditions hold:

(i) $ab \in H$ *for all* $a, b \in H$;

(ii) $e \in H$;

(iii) $a^{-1} \in H$ *for all* $a \in H$.

($\Rightarrow$): (i) is trivial. (Why?);
(ii) Let e' be an identity element for H. *To show*: $e' = e$.

$e'e' = e'$ (Why?)

A simpler way

Proposition 1

Let G be a group with identity element e, and let H be a subset of G. Then H is a subgroup of G if and only if the following conditions hold:

(i) $ab \in H$ *for all* $a, b \in H$;

(ii) $e \in H$;

(iii) $a^{-1} \in H$ *for all* $a \in H$.

($\Rightarrow$): (i) is trivial. (Why?);
(ii) Let e' be an identity element for H. *To show*: $e' = e$.

$e'e' = e'$ (Why?) and $e'e = e'$ (Why?)

A simpler way

Proposition 1

Let G be a group with identity element e, and let H be a subset of G. Then H is a subgroup of G if and only if the following conditions hold:

(i) $ab \in H$ *for all* $a, b \in H$;

(ii) $e \in H$;

(iii) $a^{-1} \in H$ *for all* $a \in H$.

($\Rightarrow$): (i) is trivial. (Why?);
(ii) Let e' be an identity element for H. *To show*: $e' = e$.

$e'e' = e'$ (Why?) and $e'e = e'$ (Why?) $\Rightarrow e'e' = e'e \Rightarrow e' = e$. (Why?)

A simpler way

Proposition 1

Let G be a group with identity element e, and let H be a subset of G. Then H is a subgroup of G if and only if the following conditions hold:

(i) $ab \in H$ *for all* $a, b \in H$;

(ii) $e \in H$;

(iii) $a^{-1} \in H$ *for all* $a \in H$.

($\Rightarrow$): (i) is trivial. (Why?);
(ii) Let e' be an identity element for H. *To show*: $e' = e$.

$e'e' = e'$ (Why?) and $e'e = e'$ (Why?) $\Rightarrow e'e' = e'e \Rightarrow e' = e$. (Why?)

(iii) If $a \in H$, then a must have an inverse $b \in H$. *To show*: $a^{-1} = b$.

A simpler way

Proposition 1

Let G be a group with identity element e, and let H be a subset of G. Then H is a subgroup of G if and only if the following conditions hold:

(i) $ab \in H$ *for all* $a, b \in H$;

(ii) $e \in H$;

(iii) $a^{-1} \in H$ *for all* $a \in H$.

($\Rightarrow$): (i) is trivial. (Why?);
(ii) Let e' be an identity element for H. *To show*: $e' = e$.

$e'e' = e'$ (Why?) and $e'e = e'$ (Why?) $\Rightarrow e'e' = e'e \Rightarrow e' = e$. (Why?)

(iii) If $a \in H$, then a must have an inverse $b \in H$. *To show*: $a^{-1} = b$.

In G, we have $ab = e = aa^{-1}$,

A simpler way

Proposition 1

Let G be a group with identity element e, and let H be a subset of G. Then H is a subgroup of G if and only if the following conditions hold:

(i) $ab \in H$ *for all* $a, b \in H$;

(ii) $e \in H$;

(iii) $a^{-1} \in H$ *for all* $a \in H$.

($\Rightarrow$): (i) is trivial. (Why?);

(ii) Let e' be an identity element for H. *To show*: $e' = e$.

$e'e' = e'$ (Why?) and $e'e = e'$ (Why?) $\Rightarrow e'e' = e'e \Rightarrow e' = e$. (Why?)

(iii) If $a \in H$, then a must have an inverse $b \in H$. *To show*: $a^{-1} = b$.

In G, we have $ab = e = aa^{-1}$, and then $a^{-1} = b$. $\Rightarrow a^{-1} \in H$.

A simpler way

Proposition 1

Let G be a group with identity element e, and let H be a subset of G. Then H is a subgroup of G if and only if the following conditions hold:

(i) $ab \in H$ *for all* $a, b \in H$;

(ii) $e \in H$;

(iii) $a^{-1} \in H$ *for all* $a \in H$.

($\Rightarrow$): (i) is trivial. (Why?);

(ii) Let e' be an identity element for H. *To show*: $e' = e$.

$e'e' = e'$ (Why?) and $e'e = e'$ (Why?) $\Rightarrow e'e' = e'e \Rightarrow e' = e$. (Why?)

(iii) If $a \in H$, then a must have an inverse $b \in H$. *To show*: $a^{-1} = b$.

In G, we have $ab = e = aa^{-1}$, and then $a^{-1} = b$. $\Rightarrow a^{-1} \in H$.

($\Leftarrow$):

A simpler way

Proposition 1

Let G be a group with identity element e, and let H be a subset of G. Then H is a subgroup of G if and only if the following conditions hold:

(i) $ab \in H$ *for all* $a, b \in H$;

(ii) $e \in H$;

(iii) $a^{-1} \in H$ *for all* $a \in H$.

($\Rightarrow$): (i) is trivial. (Why?);
(ii) Let e' be an identity element for H. *To show*: $e' = e$.

$e'e' = e'$ (Why?) and $e'e = e'$ (Why?) $\Rightarrow e'e' = e'e \Rightarrow e' = e$. (Why?)

(iii) If $a \in H$, then a must have an inverse $b \in H$. *To show*: $a^{-1} = b$.

In G, we have $ab = e = aa^{-1}$, and then $a^{-1} = b$. $\Rightarrow a^{-1} \in H$.

($\Leftarrow$): (i) Closure ✓;

A simpler way

Proposition 1

Let G be a group with identity element e, and let H be a subset of G. Then H is a subgroup of G if and only if the following conditions hold:

(i) $ab \in H$ *for all* $a, b \in H$*;*

(ii) $e \in H$*;*

(iii) $a^{-1} \in H$ *for all* $a \in H$*.*

($\Rightarrow$): (i) is trivial. (Why?);
(ii) Let e' be an identity element for H. *To show*: $e' = e$.

$e'e' = e'$ (Why?) and $e'e = e'$ (Why?) $\Rightarrow e'e' = e'e \Rightarrow e' = e$. (Why?)

(iii) If $a \in H$, then a must have an inverse $b \in H$. *To show*: $a^{-1} = b$.

In G, we have $ab = e = aa^{-1}$, and then $a^{-1} = b$. $\Rightarrow a^{-1} \in H$.

($\Leftarrow$): (i) Closure ✓; (ii) Associativity:

A simpler way

Proposition 1

Let G be a group with identity element e, and let H be a subset of G. Then H is a subgroup of G if and only if the following conditions hold:

(i) $ab \in H$ *for all* $a, b \in H$;

(ii) $e \in H$;

(iii) $a^{-1} \in H$ *for all* $a \in H$.

($\Rightarrow$): (i) is trivial. (Why?);
(ii) Let e' be an identity element for H. *To show*: $e' = e$.

$e'e' = e'$ (Why?) and $e'e = e'$ (Why?) $\Rightarrow e'e' = e'e \Rightarrow e' = e$. (Why?)

(iii) If $a \in H$, then a must have an inverse $b \in H$. *To show*: $a^{-1} = b$.

In G, we have $ab = e = aa^{-1}$, and then $a^{-1} = b$. $\Rightarrow a^{-1} \in H$.

($\Leftarrow$): (i) Closure ✓; (ii) Associativity: If $a, b, c \in H$, then in G we have $a(bc) = (ab)c$, and so also in H;

A simpler way

Proposition 1

Let G be a group with identity element e, and let H be a subset of G. Then H is a subgroup of G if and only if the following conditions hold:

(i) $ab \in H$ *for all* $a, b \in H$;

(ii) $e \in H$;

(iii) $a^{-1} \in H$ *for all* $a \in H$.

($\Rightarrow$): (i) is trivial. (Why?);
(ii) Let e' be an identity element for H. *To show*: $e' = e$.

$e'e' = e'$ (Why?) and $e'e = e'$ (Why?) $\Rightarrow e'e' = e'e \Rightarrow e' = e$. (Why?)

(iii) If $a \in H$, then a must have an inverse $b \in H$. *To show*: $a^{-1} = b$.

In G, we have $ab = e = aa^{-1}$, and then $a^{-1} = b$. $\Rightarrow a^{-1} \in H$.

($\Leftarrow$): (i) Closure ✓; (ii) Associativity: If $a, b, c \in H$, then in G we have $a(bc) = (ab)c$, and so also in H; (iii) Identity ✓;

A simpler way

Proposition 1

Let G be a group with identity element e, and let H be a subset of G. Then H is a subgroup of G if and only if the following conditions hold:

(i) $ab \in H$ *for all* $a, b \in H$;

(ii) $e \in H$;

(iii) $a^{-1} \in H$ *for all* $a \in H$.

($\Rightarrow$): (i) is trivial. (Why?);
(ii) Let e' be an identity element for H. *To show*: $e' = e$.

$e'e' = e'$ (Why?) and $e'e = e'$ (Why?) $\Rightarrow e'e' = e'e \Rightarrow e' = e$. (Why?)

(iii) If $a \in H$, then a must have an inverse $b \in H$. *To show*: $a^{-1} = b$.

In G, we have $ab = e = aa^{-1}$, and then $a^{-1} = b$. $\Rightarrow a^{-1} \in H$.

($\Leftarrow$): (i) Closure ✓; (ii) Associativity: If $a, b, c \in H$, then in G we have $a(bc) = (ab)c$, and so also in H; (iii) Identity ✓; (iv) Inverses ✓.

Consequences of Proposition 1

For any group G,

- the entire set G is certainly a subgroup;

Consequences of Proposition 1

For any group G,

- the entire set G is certainly a subgroup;
- the set $\{e\}$ is always a subgroup of G, called the **trivial subgroup**.

Corollary 7

Consequences of Proposition 1

For any group G,

- the entire set G is certainly a subgroup;
- the set $\{e\}$ is always a subgroup of G, called the **trivial subgroup**.

Corollary 7

Let G be a group and let H be a subset of G. Then H is a subgroup of G if and only if H is nonempty and $ab^{-1} \in H$ for all $a, b \in H$.

$(\Rightarrow)$:

Consequences of Proposition 1

For any group G,

- the entire set G is certainly a subgroup;
- the set $\{e\}$ is always a subgroup of G, called the **trivial subgroup**.

Corollary 7

Let G be a group and let H be a subset of G. Then H is a subgroup of G if and only if H is nonempty and $ab^{-1} \in H$ for all $a, b \in H$.

$(\Rightarrow)$: Nonempty: $e \in H$;

Consequences of Proposition 1

For any group G,

- the entire set G is certainly a subgroup;
- the set $\{e\}$ is always a subgroup of G, called the **trivial subgroup**.

Corollary 7

Let G be a group and let H be a subset of G. Then H is a subgroup of G if and only if H is nonempty and $ab^{-1} \in H$ for all $a, b \in H$.

($\Rightarrow$): Nonempty: $e \in H$; If $a, b \in H$, then $b^{-1} \in H$ and $ab^{-1} \in H$ (Why?).
($\Leftarrow$):

Consequences of Proposition 1

For any group G,

- the entire set G is certainly a subgroup;
- the set $\{e\}$ is always a subgroup of G, called the **trivial subgroup**.

Corollary 7

Let G be a group and let H be a subset of G. Then H is a subgroup of G if and only if H is nonempty and $ab^{-1} \in H$ for all $a, b \in H$.

$(\Rightarrow)$: Nonempty: $e \in H$; If $a, b \in H$, then $b^{-1} \in H$ and $ab^{-1} \in H$ (Why?).
$(\Leftarrow)$: Since H is nonempty, there is at least $a \in H$. Then $e \in H$ (Why?).

Consequences of Proposition 1

For any group G,

- the entire set G is certainly a subgroup;
- the set $\{e\}$ is always a subgroup of G, called the **trivial subgroup**.

Corollary 7

Let G be a group and let H be a subset of G. Then H is a subgroup of G if and only if H is nonempty and $ab^{-1} \in H$ for all $a, b \in H$.

($\Rightarrow$): Nonempty: $e \in H$; If $a, b \in H$, then $b^{-1} \in H$ and $ab^{-1} \in H$ (Why?).
($\Leftarrow$): Since H is nonempty, there is at least $a \in H$. Then $e \in H$ (Why?).
So $a^{-1} \in H$ since

Consequences of Proposition 1

For any group G,

- the entire set G is certainly a subgroup;
- the set $\{e\}$ is always a subgroup of G, called the **trivial subgroup**.

Corollary 7

Let G be a group and let H be a subset of G. Then H is a subgroup of G if and only if H is nonempty and $ab^{-1} \in H$ for all $a, b \in H$.

($\Rightarrow$): Nonempty: $e \in H$; If $a, b \in H$, then $b^{-1} \in H$ and $ab^{-1} \in H$ (Why?).
($\Leftarrow$): Since H is nonempty, there is at least $a \in H$. Then $e \in H$ (Why?).
So $a^{-1} \in H$ since $a^{-1} = ea^{-1} \in H$.

Consequences of Proposition 1

For any group G,

- the entire set G is certainly a subgroup;
- the set $\{e\}$ is always a subgroup of G, called the **trivial subgroup**.

Corollary 7

Let G be a group and let H be a subset of G. Then H is a subgroup of G if and only if H is nonempty and $ab^{-1} \in H$ for all $a, b \in H$.

($\Rightarrow$): Nonempty: $e \in H$; If $a, b \in H$, then $b^{-1} \in H$ and $ab^{-1} \in H$ (Why?).
($\Leftarrow$): Since H is nonempty, there is at least $a \in H$. Then $e \in H$ (Why?). So $a^{-1} \in H$ since $a^{-1} = ea^{-1} \in H$. Finally, it follows from Proposition 1 that we must *show that* $ab \in H$ for all $a, b \in H$.

Consequences of Proposition 1

For any group G,

- the entire set G is certainly a subgroup;
- the set $\{e\}$ is always a subgroup of G, called the **trivial subgroup**.

Corollary 7

Let G be a group and let H be a subset of G. Then H is a subgroup of G if and only if H is nonempty and $ab^{-1} \in H$ for all $a, b \in H$.

$(\Rightarrow)$: Nonempty: $e \in H$; If $a, b \in H$, then $b^{-1} \in H$ and $ab^{-1} \in H$ (Why?).
$(\Leftarrow)$: Since H is nonempty, there is at least $a \in H$. Then $e \in H$ (Why?). So $a^{-1} \in H$ since $a^{-1} = ea^{-1} \in H$. Finally, it follows from Proposition 1 that we must *show that* $ab \in H$ for all $a, b \in H$. It can be achieved by

$$ab = a(b^{-1})^{-1} \in H. \quad \text{(Why?)}$$

Consequences of Proposition 1

For any group G,

- the entire set G is certainly a subgroup;
- the set $\{e\}$ is always a subgroup of G, called the **trivial subgroup**.

Corollary 7

Let G be a group and let H be a subset of G. Then H is a subgroup of G if and only if H is nonempty and $ab^{-1} \in H$ for all $a, b \in H$.

($\Rightarrow$): Nonempty: $e \in H$; If $a, b \in H$, then $b^{-1} \in H$ and $ab^{-1} \in H$ (Why?).
($\Leftarrow$): Since H is nonempty, there is at least $a \in H$. Then $e \in H$ (Why?). So $a^{-1} \in H$ since $a^{-1} = ea^{-1} \in H$. Finally, it follows from Proposition 1 that we must *show that* $ab \in H$ for all $a, b \in H$. It can be achieved by

$$ab = a(b^{-1})^{-1} \in H. \quad \text{(Why?)}$$

Note 1 (To show that the subset H is nonempty:)

The easiest way to do this is to show that H **contains the identity element** *e.*

Finite subgroup

Corollary 8

Let G be a group, and let H be a finite, nonempty subset of G. Then H is a subgroup of G if and only if $ab \in H$ for all $a, b \in H$.

Finite subgroup

Corollary 8

Let G be a group, and let H be a finite, nonempty subset of G. Then H is a subgroup of G if and only if $ab \in H$ for all $a, b \in H$.

Proof.

($\Rightarrow$): Trivial.
($\Leftarrow$):

Finite subgroup

Corollary 8

Let G be a group, and let H be a finite, nonempty subset of G. Then H is a subgroup of G if and only if $ab \in H$ for all $a, b \in H$.

Proof.

($\Rightarrow$): Trivial.
($\Leftarrow$): By previous corollary, it suffices to show $b^{-1} \in H$ for all $b \in H$.

Finite subgroup

Corollary 8

Let G be a group, and let H be a finite, nonempty subset of G. Then H is a subgroup of G if and only if $ab \in H$ for all $a, b \in H$.

Proof.

$(\Rightarrow)$: Trivial.
$(\Leftarrow)$: By previous corollary, it suffices to show $b^{-1} \in H$ for all $b \in H$.
Given $b \in H$, consider the powers of b:

$$\{b, b^2, b^3, \ldots\}$$

Finite subgroup

Corollary 8

Let G be a group, and let H be a finite, nonempty subset of G. Then H is a subgroup of G if and only if $ab \in H$ for all $a, b \in H$.

Proof.

($\Rightarrow$): Trivial.
($\Leftarrow$): By previous corollary, it suffices to show $b^{-1} \in H$ for all $b \in H$.
Given $b \in H$, consider the powers of b:

$$\{b, b^2, b^3, \ldots\}$$

These must all belong to H. (Why?)

Finite subgroup

Corollary 8

Let G be a group, and let H be a finite, nonempty subset of G. Then H is a subgroup of G if and only if $ab \in H$ for all $a, b \in H$.

Proof.

($\Rightarrow$): Trivial.
($\Leftarrow$): By previous corollary, it suffices to show $b^{-1} \in H$ for all $b \in H$.
Given $b \in H$, consider the powers of b:

$$\{b, b^2, b^3, \ldots\}$$

These must all belong to H. (Why?)
But since H is a finite set, they cannot all be distinct. There must be some repetition, say $b^n = b^m$ for some positive integers $n > m$.

Finite subgroup

Corollary 8

Let G be a group, and let H be a finite, nonempty subset of G. Then H is a subgroup of G if and only if $ab \in H$ for all $a, b \in H$.

Proof.

($\Rightarrow$): Trivial.
($\Leftarrow$): By previous corollary, it suffices to show $b^{-1} \in H$ for all $b \in H$.
Given $b \in H$, consider the powers of b:

$$\{b, b^2, b^3, \ldots\}$$

These must all belong to H. (Why?)
But since H is a finite set, they cannot all be distinct. There must be some repetition, say $b^n = b^m$ for some positive integers $n > m$. Then $b^{n-m} = e$. (Why?)

Finite subgroup

Corollary 8

Let G be a group, and let H be a finite, nonempty subset of G. Then H is a subgroup of G if and only if $ab \in H$ for all $a, b \in H$.

Proof.

($\Rightarrow$): Trivial.
($\Leftarrow$): By previous corollary, it suffices to show $b^{-1} \in H$ for all $b \in H$.
Given $b \in H$, consider the powers of b:

$$\{b, b^2, b^3, \ldots\}$$

These must all belong to H. (Why?)
But since H is a finite set, they cannot all be distinct. There must be some repetition, say $b^n = b^m$ for some positive integers $n > m$. Then $b^{n-m} = e$. (Why?) Either $b = e$ or $n - m > 1$, and in the second case we then have

Finite subgroup

Corollary 8

Let G be a group, and let H be a finite, nonempty subset of G. Then H is a subgroup of G if and only if $ab \in H$ for all $a, b \in H$.

Proof.

($\Rightarrow$): Trivial.
($\Leftarrow$): By previous corollary, it suffices to show $b^{-1} \in H$ for all $b \in H$.
Given $b \in H$, consider the powers of b:

$$\{b, b^2, b^3, \ldots\}$$

These must all belong to H. (Why?)
But since H is a finite set, they cannot all be distinct. There must be some repetition, say $b^n = b^m$ for some positive integers $n > m$. Then $b^{n-m} = e$. (Why?) Either $b = e$ or $n - m > 1$, and in the second case we then have $bb^{n-m-1} = e$, which shows that $b^{-1} = b^{n-m-1}$.

Finite subgroup

Corollary 8

Let G be a group, and let H be a finite, nonempty subset of G. Then H is a subgroup of G if and only if $ab \in H$ for all $a, b \in H$.

Proof.

($\Rightarrow$): Trivial.
($\Leftarrow$): By previous corollary, it suffices to show $b^{-1} \in H$ for all $b \in H$.
Given $b \in H$, consider the powers of b:

$$\{b, b^2, b^3, \dots\}$$

These must all belong to H. (Why?)
But since H is a finite set, they cannot all be distinct. There must be some repetition, say $b^n = b^m$ for some positive integers $n > m$. Then $b^{n-m} = e$. (Why?) Either $b = e$ or $n - m > 1$, and in the second case we then have $bb^{n-m-1} = e$, which shows that $b^{-1} = b^{n-m-1}$.
Thus b^{-1} can be expressed as a positive power of b, which must belong to H. $\square$

Examples

Example 9 (Subgroups of S_3)

- The subset $\{(1), (123), (132)\}$ is closed under multiplication. It follows from Corollary 8 that this subset is a subgroup.

Examples

Example 9 (Subgroups of S_3)

- The subset $\{(1), (123), (132)\}$ is closed under multiplication. It follows from Corollary 8 that this subset is a subgroup.
- Some other subgroups: $\{(1), (12)\}$, $\{(1), (13)\}, \{(1), (23)\}$. (Why?)

Example 10

Examples

Example 9 (Subgroups of S_3)

- The subset $\{(1), (123), (132)\}$ is closed under multiplication. It follows from Corollary 8 that this subset is a subgroup.
- Some other subgroups: $\{(1), (12)\}$, $\{(1), (13)\}, \{(1), (23)\}$. (Why?)

Example 10

In the group $\mathrm{GL}_2(\mathbf{R})$, let H be the following set of matrices:

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}, \quad \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \quad \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}.$$

Examples

Example 9 (Subgroups of S_3)

- The subset $\{(1), (123), (132)\}$ is closed under multiplication. It follows from Corollary 8 that this subset is a subgroup.
- Some other subgroups: $\{(1), (12)\}$, $\{(1), (13)\}, \{(1), (23)\}$. (Why?)

Example 10

In the group $\mathrm{GL}_2(\mathbf{R})$, let H be the following set of matrices:

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}, \quad \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \quad \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}.$$

The product of any two of these matrices is again in the set H. (Check it!)

Examples

Example 9 (Subgroups of S_3)

- The subset $\{(1), (123), (132)\}$ is closed under multiplication. It follows from Corollary 8 that this subset is a subgroup.
- Some other subgroups: $\{(1), (12)\}$, $\{(1), (13)\}, \{(1), (23)\}$. (Why?)

Example 10

In the group $\mathrm{GL}_2(\mathbf{R})$, let H be the following set of matrices:

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}, \quad \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \quad \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}.$$

The product of any two of these matrices is again in the set H. (Check it!) Since the set is finite and closed under matrix multiplication, Corollary 8 implies that it is a subgroup of $\mathrm{GL}_2(\mathbf{R})$.

One more example

Let H be the set of all diagonal matrices in the group $G = \mathrm{GL}_n(\mathbf{R})$.

The diagonal entries of any element in H must all be nonzero. (Why?)

One more example

Let H be the set of all diagonal matrices in the group $G = \mathrm{GL}_n(\mathbf{R})$.

The diagonal entries of any element in H must all be nonzero. (Why?)

To show that H is a subgroup, we can no longer apply Corollary 8. (Why?)

One more example

Let H be the set of all diagonal matrices in the group $G = \mathrm{GL}_n(\mathbf{R})$.

The diagonal entries of any element in H must all be nonzero. (Why?)

To show that H is a subgroup, we can no longer apply Corollary 8. (Why?)

It is probably easiest to just use Proposition 1.

One more example

Let H be the set of all diagonal matrices in the group $G = \mathrm{GL}_n(\mathbf{R})$.

The diagonal entries of any element in H must all be nonzero. (Why?)

To show that H is a subgroup, we can no longer apply Corollary 8. (Why?)

It is probably easiest to just use Proposition 1.

(i) If $a, b \in H$, then $ab \in H$. (Check it!)

One more example

Let H be the set of all diagonal matrices in the group $G = \mathrm{GL}_n(\mathbf{R})$.

The diagonal entries of any element in H must all be nonzero. (Why?)

To show that H is a subgroup, we can no longer apply Corollary 8. (Why?)

It is probably easiest to just use Proposition 1.

(i) If $a, b \in H$, then $ab \in H$. (Check it!)

(ii) The identity matrix $I_n \in H$.

One more example

Let H be the set of all diagonal matrices in the group $G = \mathrm{GL}_n(\mathbf{R})$.

The diagonal entries of any element in H must all be nonzero. (Why?)

To show that H is a subgroup, we can no longer apply Corollary 8. (Why?)

It is probably easiest to just use Proposition 1.

(i) If $a, b \in H$, then $ab \in H$. (Check it!)

(ii) The identity matrix $I_n \in H$.

(iii) The inverse of a diagonal matrix a with nonzero entries is again a diagonal matrix with nonzero entries. That is, $a^{-1} \in H$.

Cyclic subgroup

Definition 11

Let G be a group, and let a be any element of G.
The set
$$\langle a \rangle = \{x \in G \mid x = a^n \text{ for some } n \in \mathbf{Z}\}$$
is called the **cyclic subgroup generated by** a.

Cyclic subgroup

Definition 11

Let G be a group, and let a be any element of G.
The set

$$\langle a \rangle = \{x \in G \mid x = a^n \text{ for some } n \in \mathbf{Z}\}$$

is called the **cyclic subgroup generated by** a.
The group G is called a **cyclic group** if there exists an element $a \in G$ such that $G = \langle a \rangle$. In this case a is called a **generator** of G.

Cyclic subgroup

Definition 11

Let G be a group, and let a be any element of G.
The set

$$\langle a \rangle = \{x \in G \mid x = a^n \text{ for some } n \in \mathbf{Z}\}$$

is called the **cyclic subgroup generated by** a.
The group G is called a **cyclic group** if there exists an element $a \in G$ such that $G = \langle a \rangle$. In this case a is called a **generator** of G.

Proposition 2

Let G be a group, and let $a \in G$.

(a) *The set $\langle a \rangle$ is a subgroup of G.*

(b) *If K is any subgroup of G such that $a \in K$, then $\langle a \rangle \subseteq K$.*

(a): (i)

Cyclic subgroup

Definition 11

Let G be a group, and let a be any element of G.
The set
$$\langle a \rangle = \{x \in G \mid x = a^n \text{ for some } n \in \mathbf{Z}\}$$
is called the **cyclic subgroup generated by** a.
The group G is called a **cyclic group** if there exists an element $a \in G$ such that $G = \langle a \rangle$. In this case a is called a **generator** of G.

Proposition 2

Let G be a group, and let $a \in G$.

(a) *The set $\langle a \rangle$ is a subgroup of G.*

(b) *If K is any subgroup of G such that $a \in K$, then $\langle a \rangle \subseteq K$.*

(a): (i) $a^m, a^n \in \langle a \rangle \Rightarrow a^m a^n = a^{m+n} \in \langle a \rangle$; (ii)

Cyclic subgroup

Definition 11

Let G be a group, and let a be any element of G.
The set
$$\langle a \rangle = \{x \in G \mid x = a^n \text{ for some } n \in \mathbf{Z}\}$$
is called the **cyclic subgroup generated by** a.
The group G is called a **cyclic group** if there exists an element $a \in G$ such that $G = \langle a \rangle$. In this case a is called a **generator** of G.

Proposition 2

Let G be a group, and let $a \in G$.

(a) *The set $\langle a \rangle$ is a subgroup of G.*

(b) *If K is any subgroup of G such that $a \in K$, then $\langle a \rangle \subseteq K$.*

(a): (i) $a^m, a^n \in \langle a \rangle \Rightarrow a^m a^n = a^{m+n} \in \langle a \rangle$; (ii) $a^0 = e$; (iii)

Cyclic subgroup

Definition 11

Let G be a group, and let a be any element of G.
The set
$$\langle a \rangle = \{x \in G \mid x = a^n \text{ for some } n \in \mathbf{Z}\}$$
is called the **cyclic subgroup generated by** a.
The group G is called a **cyclic group** if there exists an element $a \in G$ such that $G = \langle a \rangle$. In this case a is called a **generator** of G.

Proposition 2

Let G be a group, and let $a \in G$.

(a) *The set $\langle a \rangle$ is a subgroup of G.*

(b) *If K is any subgroup of G such that $a \in K$, then $\langle a \rangle \subseteq K$.*

(a): (i) $a^m, a^n \in \langle a \rangle \Rightarrow a^m a^n = a^{m+n} \in \langle a \rangle$; (ii) $a^0 = e$; (iii) $(a^n)^{-1} = a^{-n}$.
(b):

Cyclic subgroup

Definition 11

Let G be a group, and let a be any element of G.
The set
$$\langle a \rangle = \{x \in G \mid x = a^n \text{ for some } n \in \mathbf{Z}\}$$
is called the **cyclic subgroup generated by** a.
The group G is called a **cyclic group** if there exists an element $a \in G$ such that $G = \langle a \rangle$. In this case a is called a **generator** of G.

Proposition 2

Let G be a group, and let $a \in G$.

(a) *The set $\langle a \rangle$ is a subgroup of G.*

(b) *If K is any subgroup of G such that $a \in K$, then $\langle a \rangle \subseteq K$.*

(a): (i) $a^m, a^n \in \langle a \rangle \Rightarrow a^m a^n = a^{m+n} \in \langle a \rangle$; (ii) $a^0 = e$; (iii) $(a^n)^{-1} = a^{-n}$.
(b): If K is any subgroup that contains a, then it must contain all positive powers of a. (Why?)

Cyclic subgroup

Definition 11

Let G be a group, and let a be any element of G.
The set
$$\langle a \rangle = \{x \in G \mid x = a^n \text{ for some } n \in \mathbf{Z}\}$$
is called the **cyclic subgroup generated by** a.
The group G is called a **cyclic group** if there exists an element $a \in G$ such that $G = \langle a \rangle$. In this case a is called a **generator** of G.

Proposition 2

Let G be a group, and let $a \in G$.

(a) *The set $\langle a \rangle$ is a subgroup of G.*

(b) *If K is any subgroup of G such that $a \in K$, then $\langle a \rangle \subseteq K$.*

(a): (i) $a^m, a^n \in \langle a \rangle \Rightarrow a^m a^n = a^{m+n} \in \langle a \rangle$; (ii) $a^0 = e$; (iii) $(a^n)^{-1} = a^{-n}$.
(b): If K is any subgroup that contains a, then it must contain all positive powers of a. (Why?) It also contains $e = a^0$, and

Cyclic subgroup

Definition 11

Let G be a group, and let a be any element of G.
The set
$$\langle a \rangle = \{x \in G \mid x = a^n \text{ for some } n \in \mathbf{Z}\}$$
is called the **cyclic subgroup generated by** a.
The group G is called a **cyclic group** if there exists an element $a \in G$ such that $G = \langle a \rangle$. In this case a is called a **generator** of G.

Proposition 2

Let G be a group, and let $a \in G$.

(a) *The set $\langle a \rangle$ is a subgroup of G.*

(b) *If K is any subgroup of G such that $a \in K$, then $\langle a \rangle \subseteq K$.*

(a): (i) $a^m, a^n \in \langle a \rangle \Rightarrow a^m a^n = a^{m+n} \in \langle a \rangle$; (ii) $a^0 = e$; (iii) $(a^n)^{-1} = a^{-n}$.
(b): If K is any subgroup that contains a, then it must contain all positive powers of a. (Why?) It also contains $e = a^0$, and if $n < 0$ then $a^n \in K$. (Why?)

Examples

The intersection of any collection of subgroups is again a subgroup.

Examples

The intersection of any collection of subgroups is again a subgroup. Given any subset S of a group G, the intersection of all subgroups of G that contain S is in fact the **smallest subgroup that contains** S.

Example 12

Examples

The intersection of any collection of subgroups is again a subgroup. Given any subset S of a group G, the intersection of all subgroups of G that contain S is in fact the **smallest subgroup that contains** S.

Example 12

In the case $S = \{a\}$, by the previous proposition we obtain $\langle a \rangle$.

Examples

The intersection of any collection of subgroups is again a subgroup.
Given any subset S of a group G, the intersection of all subgroups of G that contain S is in fact the **smallest subgroup that contains** S.

Example 12

In the case $S = \{a\}$, by the previous proposition we obtain $\langle a \rangle$.
But, in the case $S = \{a, b\}$ of a nonabelian group G, it becomes much more complicated to describe the smallest subgroup of G that contains S.

Example 13

Examples

The intersection of any collection of subgroups is again a subgroup. Given any subset S of a group G, the intersection of all subgroups of G that contain S is in fact the **smallest subgroup that contains** S.

Example 12

In the case $S = \{a\}$, by the previous proposition we obtain $\langle a \rangle$.
But, in the case $S = \{a, b\}$ of a nonabelian group G, it becomes much more complicated to describe the smallest subgroup of G that contains S.

Example 13

In the multiplicative group $\mathbf{C}^{\times}$, consider the powers of i. We can easily get

$$\langle i \rangle = \{1, i, -1, -i\},$$

Examples

The intersection of any collection of subgroups is again a subgroup. Given any subset S of a group G, the intersection of all subgroups of G that contain S is in fact the **smallest subgroup that contains** S.

Example 12

In the case $S = \{a\}$, by the previous proposition we obtain $\langle a \rangle$. But, in the case $S = \{a, b\}$ of a nonabelian group G, it becomes much more complicated to describe the smallest subgroup of G that contains S.

Example 13

In the multiplicative group $\mathbf{C}^\times$, consider the powers of i. We can easily get

$$\langle i \rangle = \{1, i, -1, -i\}, \quad \text{which is a cyclic subgroup of } \mathbf{C}^\times \text{ of order } 4.$$

Examples

The intersection of any collection of subgroups is again a subgroup. Given any subset S of a group G, the intersection of all subgroups of G that contain S is in fact the **smallest subgroup that contains** S.

Example 12

In the case $S = \{a\}$, by the previous proposition we obtain $\langle a \rangle$. But, in the case $S = \{a, b\}$ of a nonabelian group G, it becomes much more complicated to describe the smallest subgroup of G that contains S.

Example 13

In the multiplicative group $\mathbf{C}^{\times}$, consider the powers of i. We can easily get

$$\langle i \rangle = \{1, i, -1, -i\}, \quad \text{which is a cyclic subgroup of } \mathbf{C}^{\times} \text{ of order } 4.$$

The situation is quite different if we consider $\langle 2i \rangle$,

Examples

The intersection of any collection of subgroups is again a subgroup. Given any subset S of a group G, the intersection of all subgroups of G that contain S is in fact the **smallest subgroup that contains** S.

Example 12

In the case $S = \{a\}$, by the previous proposition we obtain $\langle a \rangle$.
But, in the case $S = \{a, b\}$ of a nonabelian group G, it becomes much more complicated to describe the smallest subgroup of G that contains S.

Example 13

In the multiplicative group $\mathbf{C}^\times$, consider the powers of i. We can easily get

$$\langle i \rangle = \{1, i, -1, -i\}, \quad \text{which is a cyclic subgroup of } \mathbf{C}^\times \text{ of order } 4.$$

The situation is quite different if we consider $\langle 2i \rangle$, which is infinite:

$$\langle 2i \rangle = \{\ldots, \tfrac{1}{16}, \tfrac{1}{8}i, -\tfrac{1}{4}, -\tfrac{1}{2}i, 1, 2i, -4, -8i, 16, \ldots\}.$$

Examples

The intersection of any collection of subgroups is again a subgroup. Given any subset S of a group G, the intersection of all subgroups of G that contain S is in fact the **smallest subgroup that contains** S.

Example 12

In the case $S = \{a\}$, by the previous proposition we obtain $\langle a\rangle$. But, in the case $S = \{a, b\}$ of a nonabelian group G, it becomes much more complicated to describe the smallest subgroup of G that contains S.

Example 13

In the multiplicative group $\mathbf{C}^\times$, consider the powers of i. We can easily get

$$\langle i\rangle = \{1, i, -1, -i\}, \quad \text{which is a cyclic subgroup of } \mathbf{C}^\times \text{ of order } 4.$$

The situation is quite different if we consider $\langle 2i\rangle$, which is infinite:

$$\langle 2i\rangle = \{\dots, \tfrac{1}{16}, \tfrac{1}{8}i, -\tfrac{1}{4}, -\tfrac{1}{2}i, 1, 2i, -4, -8i, 16, \dots\}.$$

Let $z = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$.

Examples

The intersection of any collection of subgroups is again a subgroup. Given any subset S of a group G, the intersection of all subgroups of G that contain S is in fact the **smallest subgroup that contains** S.

Example 12

In the case $S = \{a\}$, by the previous proposition we obtain $\langle a \rangle$.
But, in the case $S = \{a, b\}$ of a nonabelian group G, it becomes much more complicated to describe the smallest subgroup of G that contains S.

Example 13

In the multiplicative group $\mathbf{C}^\times$, consider the powers of i. We can easily get

$$\langle i \rangle = \{1, i, -1, -i\}, \quad \text{which is a cyclic subgroup of } \mathbf{C}^\times \text{ of order } 4.$$

The situation is quite different if we consider $\langle 2i \rangle$, which is infinite:

$$\langle 2i \rangle = \{\ldots, \tfrac{1}{16}, \tfrac{1}{8}i, -\tfrac{1}{4}, -\tfrac{1}{2}i, 1, 2i, -4, -8i, 16, \ldots\}.$$

Let $z = \cos\frac{2\pi}{n} + i \sin\frac{2\pi}{n}$. We can show that $\langle z \rangle = \{z^k \mid k \in \mathbf{Z}\}$ is the set of complex nth roots of unity,

Examples

The intersection of any collection of subgroups is again a subgroup. Given any subset S of a group G, the intersection of all subgroups of G that contain S is in fact the **smallest subgroup that contains** S.

Example 12

In the case $S = \{a\}$, by the previous proposition we obtain $\langle a \rangle$.
But, in the case $S = \{a, b\}$ of a nonabelian group G, it becomes much more complicated to describe the smallest subgroup of G that contains S.

Example 13

In the multiplicative group $\mathbf{C}^\times$, consider the powers of i. We can easily get

$$\langle i \rangle = \{1, i, -1, -i\}, \quad \text{which is a cyclic subgroup of } \mathbf{C}^\times \text{ of order } 4.$$

The situation is quite different if we consider $\langle 2i \rangle$, which is infinite:

$$\langle 2i \rangle = \{\ldots, \tfrac{1}{16}, \tfrac{1}{8}i, -\tfrac{1}{4}, -\tfrac{1}{2}i, 1, 2i, -4, -8i, 16, \ldots\}.$$

Let $z = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$. We can show that $\langle z \rangle = \{z^k \mid k \in \mathbf{Z}\}$ is the set of complex nth roots of unity, which is a cyclic subgroup of $\mathbf{C}^\times$ of order n.

More examples

When the operation is denoted additively rather than multiplicatively, we must consider multiples rather than powers.

More examples

When the operation is denoted additively rather than multiplicatively, we must consider multiples rather than powers.

Example 14 ($(\mathbf{Z}, +)$ is cyclic)

$\mathbf{Z} = \langle 1 \rangle = \langle -1 \rangle$. (Check it!)

More examples

When the operation is denoted additively rather than multiplicatively, we must consider multiples rather than powers.

Example 14 ($(\mathbf{Z}, +)$ is cyclic)

$\mathbf{Z} = \langle 1 \rangle = \langle -1 \rangle$. (Check it!) $\mathbf{Z} = \langle a \rangle = \{na \mid n \in \mathbf{Z}\} \Rightarrow a = \pm 1$.

Example 15 ($(\mathbf{Z}_n, +_{[a]_n})$ is cyclic)

More examples

When the operation is denoted additively rather than multiplicatively, we must consider multiples rather than powers.

Example 14 ($(\mathbf{Z}, +)$ is cyclic)

$\mathbf{Z} = \langle 1 \rangle = \langle -1 \rangle$. (Check it!) $\mathbf{Z} = \langle a \rangle = \{na \mid n \in \mathbf{Z}\} \Rightarrow a = \pm 1$.

Example 15 ($(\mathbf{Z}_n, +_{[a]_n})$ is cyclic)

$\mathbf{Z}_n = \langle [1]_n \rangle$.

More examples

When the operation is denoted additively rather than multiplicatively, we must consider multiples rather than powers.

Example 14 (($\mathbf{Z}, +$) is cyclic)

$\mathbf{Z} = \langle 1 \rangle = \langle -1 \rangle$. (Check it!) $\quad \mathbf{Z} = \langle a \rangle = \{na \mid n \in \mathbf{Z}\} \Rightarrow a = \pm 1$.

Example 15 (($\mathbf{Z}_n, +_{[a]_n}$) is cyclic)

$\mathbf{Z}_n = \langle [1]_n \rangle$. $\quad$ In fact, we can determine all possible generators. (How?)

More examples

When the operation is denoted additively rather than multiplicatively, we must consider multiples rather than powers.

Example 14 ($(\mathbf{Z}, +)$ is cyclic)

$\mathbf{Z} = \langle 1 \rangle = \langle -1 \rangle$. (Check it!) $\mathbf{Z} = \langle a \rangle = \{na \mid n \in \mathbf{Z}\} \Rightarrow a = \pm 1$.

Example 15 ($(\mathbf{Z}_n, +_{[a]_n})$ is cyclic)

$\mathbf{Z}_n = \langle [1]_n \rangle$. In fact, we can determine all possible generators. (How?)
Claim: $\mathbf{Z}_n = \langle [a]_n \rangle$ if and only if $[1]_n$ is a multiple of $[a]_n$. (Check it!)

More examples

When the operation is denoted additively rather than multiplicatively, we must consider multiples rather than powers.

Example 14 ($(\mathbf{Z}, +)$ is cyclic)

$\mathbf{Z} = \langle 1 \rangle = \langle -1 \rangle$. (Check it!) $\mathbf{Z} = \langle a \rangle = \{na \mid n \in \mathbf{Z}\} \Rightarrow a = \pm 1$.

Example 15 ($(\mathbf{Z}_n, +_{[a]_n})$ is cyclic)

$\mathbf{Z}_n = \langle [1]_n \rangle$. In fact, we can determine all possible generators. (How?)
Claim: $\mathbf{Z}_n = \langle [a]_n \rangle$ if and only if $[1]_n$ is a multiple of $[a]_n$. (Check it!)
Equivalently, $ba \equiv 1 \pmod{n}$ for some $b \in \mathbf{Z}$

More examples

When the operation is denoted additively rather than multiplicatively, we must consider multiples rather than powers.

Example 14 ($(\mathbf{Z}, +)$ is cyclic)

$\mathbf{Z} = \langle 1 \rangle = \langle -1 \rangle$. (Check it!) $\mathbf{Z} = \langle a \rangle = \{na \mid n \in \mathbf{Z}\} \Rightarrow a = \pm 1$.

Example 15 ($(\mathbf{Z}_n, +_{[a]_n})$ is cyclic)

$\mathbf{Z}_n = \langle [1]_n \rangle$. In fact, we can determine all possible generators. (How?)
Claim: $\mathbf{Z}_n = \langle [a]_n \rangle$ if and only if $[1]_n$ is a multiple of $[a]_n$. (Check it!)
Equivalently, $ba \equiv 1 \pmod{n}$ for some $b \in \mathbf{Z} \Leftrightarrow (a, n) = 1$, i.e., $[a]_n \in \mathbf{Z}_n^\times$.

Example 16 (Sometimes $(\mathbf{Z}_n^\times, \cdot_{[a]_n})$ is cyclic, sometimes not)

More examples

When the operation is denoted additively rather than multiplicatively, we must consider multiples rather than powers.

Example 14 ($(\mathbf{Z}, +)$ is cyclic)

$\mathbf{Z} = \langle 1 \rangle = \langle -1 \rangle$. (Check it!) $\mathbf{Z} = \langle a \rangle = \{na \mid n \in \mathbf{Z}\} \Rightarrow a = \pm 1$.

Example 15 ($(\mathbf{Z}_n, +_{[a]_n})$ is cyclic)

$\mathbf{Z}_n = \langle [1]_n \rangle$. In fact, we can determine all possible generators. (How?)
Claim: $\mathbf{Z}_n = \langle [a]_n \rangle$ if and only if $[1]_n$ is a multiple of $[a]_n$. (Check it!)
Equivalently, $ba \equiv 1 \pmod{n}$ for some $b \in \mathbf{Z} \Leftrightarrow (a, n) = 1$, i.e., $[a]_n \in \mathbf{Z}_n^\times$.

Example 16 (Sometimes $(\mathbf{Z}_n^\times, \cdot_{[a]_n})$ is cyclic, sometimes not)

(a) $\mathbf{Z}_5^\times = \langle [2]_5 \rangle = \langle [3]_5 \rangle$ (Check it!)

More examples

When the operation is denoted additively rather than multiplicatively, we must consider multiples rather than powers.

Example 14 ($(\mathbf{Z}, +)$ is cyclic)

$\mathbf{Z} = \langle 1 \rangle = \langle -1 \rangle$. (Check it!) $\mathbf{Z} = \langle a \rangle = \{na \mid n \in \mathbf{Z}\} \Rightarrow a = \pm 1$.

Example 15 ($(\mathbf{Z}_n, +_{[a]_n})$ is cyclic)

$\mathbf{Z}_n = \langle [1]_n \rangle$. In fact, we can determine all possible generators. (How?)
Claim: $\mathbf{Z}_n = \langle [a]_n \rangle$ if and only if $[1]_n$ is a multiple of $[a]_n$. (Check it!)
Equivalently, $ba \equiv 1 \pmod{n}$ for some $b \in \mathbf{Z} \Leftrightarrow (a, n) = 1$, i.e., $[a]_n \in \mathbf{Z}_n^{\times}$.

Example 16 (Sometimes $(\mathbf{Z}_n^{\times}, \cdot_{[a]_n})$ is cyclic, sometimes not)

(a) $\mathbf{Z}_5^{\times} = \langle [2]_5 \rangle = \langle [3]_5 \rangle$ (Check it!) But $[4]_5$ is not a generator. (Why?)

More examples

When the operation is denoted additively rather than multiplicatively, we must consider multiples rather than powers.

Example 14 ($(\mathbf{Z}, +)$ is cyclic)

$\mathbf{Z} = \langle 1 \rangle = \langle -1 \rangle$. (Check it!) $\mathbf{Z} = \langle a \rangle = \{na \mid n \in \mathbf{Z}\} \Rightarrow a = \pm 1$.

Example 15 ($(\mathbf{Z}_n, +_{[a]_n})$ is cyclic)

$\mathbf{Z}_n = \langle [1]_n \rangle$. In fact, we can determine all possible generators. (How?)
Claim: $\mathbf{Z}_n = \langle [a]_n \rangle$ if and only if $[1]_n$ is a multiple of $[a]_n$. (Check it!)
Equivalently, $ba \equiv 1 \pmod{n}$ for some $b \in \mathbf{Z} \Leftrightarrow (a, n) = 1$, i.e., $[a]_n \in \mathbf{Z}_n^{\times}$.

Example 16 (Sometimes $(\mathbf{Z}_n^{\times}, \cdot_{[a]_n})$ is cyclic, sometimes not)

(a) $\mathbf{Z}_5^{\times} = \langle [2]_5 \rangle = \langle [3]_5 \rangle$ (Check it!) But $[4]_5$ is not a generator. (Why?)
(b) $\mathbf{Z}_8^{\times} = \{[1]_8, [3]_8, [5]_8, [7]_8\}$ is not cyclic. (Why?)

More examples

When the operation is denoted additively rather than multiplicatively, we must consider multiples rather than powers.

Example 14 ($(\mathbf{Z}, +)$ is cyclic)

$\mathbf{Z} = \langle 1 \rangle = \langle -1 \rangle$. (Check it!) $\mathbf{Z} = \langle a \rangle = \{na \mid n \in \mathbf{Z}\} \Rightarrow a = \pm 1$.

Example 15 ($(\mathbf{Z}_n, +_{[a]_n})$ is cyclic)

$\mathbf{Z}_n = \langle [1]_n \rangle$. In fact, we can determine all possible generators. (How?)
Claim: $\mathbf{Z}_n = \langle [a]_n \rangle$ if and only if $[1]_n$ is a multiple of $[a]_n$. (Check it!)
Equivalently, $ba \equiv 1 \pmod{n}$ for some $b \in \mathbf{Z} \Leftrightarrow (a, n) = 1$, i.e., $[a]_n \in \mathbf{Z}_n^\times$.

Example 16 (Sometimes $(\mathbf{Z}_n^\times, \cdot_{[a]_n})$ is cyclic, sometimes not)

(a) $\mathbf{Z}_5^\times = \langle [2]_5 \rangle = \langle [3]_5 \rangle$ (Check it!) But $[4]_5$ is not a generator. (Why?)

(b) $\mathbf{Z}_8^\times = \{[1]_8, [3]_8, [5]_8, [7]_8\}$ is not cyclic. (Why?) The square of each element is $[1]$,

More examples

When the operation is denoted additively rather than multiplicatively, we must consider multiples rather than powers.

Example 14 (($\mathbf{Z}, +$) is cyclic)

$\mathbf{Z} = \langle 1 \rangle = \langle -1 \rangle$. (Check it!) $\mathbf{Z} = \langle a \rangle = \{na \mid n \in \mathbf{Z}\} \Rightarrow a = \pm 1$.

Example 15 (($\mathbf{Z}_n, +_{[a]_n}$) is cyclic)

$\mathbf{Z}_n = \langle [1]_n \rangle$. In fact, we can determine all possible generators. (How?)
Claim: $\mathbf{Z}_n = \langle [a]_n \rangle$ if and only if $[1]_n$ is a multiple of $[a]_n$. (Check it!)
Equivalently, $ba \equiv 1 \pmod{n}$ for some $b \in \mathbf{Z} \Leftrightarrow (a, n) = 1$, i.e., $[a]_n \in \mathbf{Z}_n^\times$.

Example 16 (Sometimes ($\mathbf{Z}_n^\times, \cdot_{[a]_n}$) is cyclic, sometimes not)

(a) $\mathbf{Z}_5^\times = \langle [2]_5 \rangle = \langle [3]_5 \rangle$ (Check it!) But $[4]_5$ is not a generator. (Why?)

(b) $\mathbf{Z}_8^\times = \{[1]_8, [3]_8, [5]_8, [7]_8\}$ is not cyclic. (Why?) The square of each element is $[1]$, so $\langle [3] \rangle = \{[1], [3]\}, \langle [5] \rangle = \{[1], [5]\}, \langle [7] \rangle = \{[1], [7]\}$.

Revisit Example 9

The group S_3 is not cyclic.

Revisit Example 9

The group S_3 is not cyclic. We can list all cyclic subgroups as follows:

$$\begin{aligned}
\langle(1)\rangle =& \{(1)\};\\
\langle(12)\rangle =& \{(1),(12)\};\\
\langle(13)\rangle =& \{(1),(13)\};\\
\langle(23)\rangle =& \{(1),(23)\};\\
\langle(123)\rangle =& \{(1),(123),(132)\};\\
\langle(132)\rangle =& \{(1),(132),(123)\}.
\end{aligned}$$

Revisit Example 9

The group S_3 is not cyclic. We can list all cyclic subgroups as follows:

$$\begin{aligned}\langle(1)\rangle =&\{(1)\};\\ \langle(12)\rangle =&\{(1),(12)\};\\ \langle(13)\rangle =&\{(1),(13)\};\\ \langle(23)\rangle =&\{(1),(23)\};\\ \langle(123)\rangle =&\{(1),(123),(132)\};\\ \langle(132)\rangle =&\{(1),(132),(123)\}.\end{aligned}$$

Since no cyclic subgroup is equal to all of S_3, it is not cyclic. $\square$

Revisit Example 9

The group S_3 is not cyclic. We can list all cyclic subgroups as follows:

$$\begin{aligned}
\langle(1)\rangle =& \{(1)\};\\
\langle(12)\rangle =& \{(1),(12)\};\\
\langle(13)\rangle =& \{(1),(13)\};\\
\langle(23)\rangle =& \{(1),(23)\};\\
\langle(123)\rangle =& \{(1),(123),(132)\};\\
\langle(132)\rangle =& \{(1),(132),(123)\}.
\end{aligned}$$

Since no cyclic subgroup is equal to all of S_3, it is not cyclic. $\square$

Remark 1

Every proper subgroup of S_3 is cyclic, but S_3 is not cyclic. Same with $\mathbf{Z}_8^\times$.

Order of an element

Definition 17 (Let a be an element of the group G.)

If there exists a positive integer n such that $a^n = e$, then a is said to have **finite order**, and the smallest such positive integer is called the **order** of a, denoted by $o(a)$.

Order of an element

Definition 17 (Let a be an element of the group G.)

If there exists a positive integer n such that $a^n = e$, then a is said to have **finite order**, and the smallest such positive integer is called the **order** of a, denoted by $o(a)$.
If there does not exist a positive integer n such that $a^n = e$, then a is said to have **infinite order**.

Order of an element

Definition 17 (Let a be an element of the group G.)

If there exists a positive integer n such that $a^n = e$, then a is said to have **finite order**, and the smallest such positive integer is called the **order** of a, denoted by $o(a)$.
If there does not exist a positive integer n such that $a^n = e$, then a is said to have **infinite order**.

Every element of a finite group must have finite order. (Why?)

Proposition 3 (Let a be an element of the group G.)

Order of an element

Definition 17 (Let a be an element of the group G.)

If there exists a positive integer n such that $a^n = e$, then a is said to have **finite order**, and the smallest such positive integer is called the **order** of a, denoted by $o(a)$.
If there does not exist a positive integer n such that $a^n = e$, then a is said to have **infinite order**.

Every element of a finite group must have finite order. (Why?)

Proposition 3 (Let a be an element of the group G.)

(a) *If a has infinite order, then $a^k \neq a^m$ for all integers $k \neq m$.*

Order of an element

Definition 17 (Let a be an element of the group G.)

If there exists a positive integer n such that $a^n = e$, then a is said to have **finite order**, and the smallest such positive integer is called the **order** of a, denoted by $o(a)$.
If there does not exist a positive integer n such that $a^n = e$, then a is said to have **infinite order**.

Every element of a finite group must have finite order. (Why?)

Proposition 3 (Let a be an element of the group G.)

(a) *If a has infinite order, then $a^k \neq a^m$ for all integers $k \neq m$.*

(b) *If a has finite order and $k \in \mathbf{Z}$, then $a^k = e$ if and only if $o(a) | k$.*

Order of an element

Definition 17 (Let a be an element of the group G.)

If there exists a positive integer n such that $a^n = e$, then a is said to have **finite order**, and the smallest such positive integer is called the **order** of a, denoted by $o(a)$.
If there does not exist a positive integer n such that $a^n = e$, then a is said to have **infinite order**.

Every element of a finite group must have finite order. (Why?)

Proposition 3 (Let a be an element of the group G.)

(a) *If a has infinite order, then $a^k \neq a^m$ for all integers $k \neq m$.*

(b) *If a has finite order and $k \in \mathbf{Z}$, then $a^k = e$ if and only if $o(a) | k$.*

(c) *If a has finite order $o(a) = n$, then for all integers k, m, we have*

$$a^k = a^m \text{ if and only if } k \equiv m \pmod{n}.$$

Furthermore, $|\langle a \rangle| = o(a)$.

Proof of Proposition 3

(a) Let a have infinite order. Suppose that $a^k = a^m$ for $k, m \in \mathbf{Z}$, with $k \geq m$.

Proof of Proposition 3

(a) Let a have infinite order. Suppose that $a^k = a^m$ for $k, m \in \mathbf{Z}$, with $k \geq m$. Then $a^{k-m} = e$. (Why?)

Proof of Proposition 3

(a) Let a have infinite order. Suppose that $a^k = a^m$ for $k, m \in \mathbf{Z}$, with $k \geq m$. Then $a^{k-m} = e$. (Why?) Thus, we must have $k - m = 0$. (Why?)

(b) $\Rightarrow$: Let $o(a) = n$, and suppose that $a^k = e$. *To show*: $n|k$.

Proof of Proposition 3

(a) Let a have infinite order. Suppose that $a^k = a^m$ for $k, m \in \mathbf{Z}$, with $k \geq m$. Then $a^{k-m} = e$. (Why?) Thus, we must have $k - m = 0$. (Why?)

(b) $\Rightarrow$: Let $o(a) = n$, and suppose that $a^k = e$. *To show*: $n|k$.
Write $k = nq + r$, where $0 \leq r < n$. (Why?)

Proof of Proposition 3

(a) Let a have infinite order. Suppose that $a^k = a^m$ for $k, m \in \mathbf{Z}$, with $k \geq m$. Then $a^{k-m} = e$. (Why?) Thus, we must have $k - m = 0$. (Why?)

(b) $\Rightarrow$: Let $o(a) = n$, and suppose that $a^k = e$. *To show*: $n|k$.
Write $k = nq + r$, where $0 \leq r < n$. (Why?) Thus,

$$a^r = a^{k-nq} = a^k a^{-nq} = a^k (a^n)^{-q} = e \cdot e^{-q} = e.$$

Proof of Proposition 3

(a) Let a have infinite order. Suppose that $a^k = a^m$ for $k, m \in \mathbf{Z}$, with $k \geq m$. Then $a^{k-m} = e$. (Why?) Thus, we must have $k - m = 0$. (Why?)

(b) $\Rightarrow$: Let $o(a) = n$, and suppose that $a^k = e$. *To show*: $n|k$.
Write $k = nq + r$, where $0 \leq r < n$. (Why?) Thus,

$$a^r = a^{k-nq} = a^k a^{-nq} = a^k (a^n)^{-q} = e \cdot e^{-q} = e.$$

We must have $r = 0$. (Why?)

Proof of Proposition 3

(a) Let a have infinite order. Suppose that $a^k = a^m$ for $k, m \in \mathbf{Z}$, with $k \geq m$. Then $a^{k-m} = e$. (Why?) Thus, we must have $k - m = 0$. (Why?)

(b) $\Rightarrow$: Let $o(a) = n$, and suppose that $a^k = e$. *To show*: $n|k$.
Write $k = nq + r$, where $0 \leq r < n$. (Why?) Thus,

$$a^r = a^{k-nq} = a^k a^{-nq} = a^k (a^n)^{-q} = e \cdot e^{-q} = e.$$

We must have $r = 0$. (Why?) Therefore $k = nq$.
$\Leftarrow$:

Proof of Proposition 3

(a) Let a have infinite order. Suppose that $a^k = a^m$ for $k, m \in \mathbf{Z}$, with $k \geq m$. Then $a^{k-m} = e$. (Why?) Thus, we must have $k - m = 0$. (Why?)

(b) $\Rightarrow$: Let $o(a) = n$, and suppose that $a^k = e$. *To show*: $n|k$.
Write $k = nq + r$, where $0 \leq r < n$. (Why?) Thus,

$$a^r = a^{k-nq} = a^k a^{-nq} = a^k (a^n)^{-q} = e \cdot e^{-q} = e.$$

We must have $r = 0$. (Why?) Therefore $k = nq$.
$\Leftarrow$: If $o(a)|k$, then $k = o(a) \cdot q$. Thus $a^k = (a^{o(a)})^q = e^q = e$.

(c) Let $o(a) = n$.

Proof of Proposition 3

(a) Let a have infinite order. Suppose that $a^k = a^m$ for $k, m \in \mathbf{Z}$, with $k \geq m$. Then $a^{k-m} = e$. (Why?) Thus, we must have $k - m = 0$. (Why?)

(b) $\Rightarrow$: Let $o(a) = n$, and suppose that $a^k = e$. *To show*: $n | k$.
Write $k = nq + r$, where $0 \leq r < n$. (Why?) Thus,

$$a^r = a^{k-nq} = a^k a^{-nq} = a^k (a^n)^{-q} = e \cdot e^{-q} = e.$$

We must have $r = 0$. (Why?) Therefore $k = nq$.
$\Leftarrow$: If $o(a)|k$, then $k = o(a) \cdot q$. Thus $a^k = (a^{o(a)})^q = e^q = e$.

(c) Let $o(a) = n$. $a^k = a^m \Leftrightarrow a^{k-m} = e$

Proof of Proposition 3

(a) Let a have infinite order. Suppose that $a^k = a^m$ for $k, m \in \mathbf{Z}$, with $k \geq m$. Then $a^{k-m} = e$. (Why?) Thus, we must have $k - m = 0$. (Why?)

(b) $\Rightarrow$: Let $o(a) = n$, and suppose that $a^k = e$. *To show*: $n|k$.
Write $k = nq + r$, where $0 \leq r < n$. (Why?) Thus,

$$a^r = a^{k-nq} = a^k a^{-nq} = a^k (a^n)^{-q} = e \cdot e^{-q} = e.$$

We must have $r = 0$. (Why?) Therefore $k = nq$.
$\Leftarrow$: If $o(a)|k$, then $k = o(a) \cdot q$. Thus $a^k = (a^{o(a)})^q = e^q = e$.

(c) Let $o(a) = n$. $a^k = a^m \Leftrightarrow a^{k-m} = e \Leftrightarrow n|(k - m)$

Proof of Proposition 3

(a) Let a have infinite order. Suppose that $a^k = a^m$ for $k, m \in \mathbf{Z}$, with $k \geq m$. Then $a^{k-m} = e$. (Why?) Thus, we must have $k - m = 0$. (Why?)

(b) $\Rightarrow$: Let $o(a) = n$, and suppose that $a^k = e$. *To show*: $n | k$.
Write $k = nq + r$, where $0 \leq r < n$. (Why?) Thus,

$$a^r = a^{k-nq} = a^k a^{-nq} = a^k (a^n)^{-q} = e \cdot e^{-q} = e.$$

We must have $r = 0$. (Why?) Therefore $k = nq$.
$\Leftarrow$: If $o(a)|k$, then $k = o(a) \cdot q$. Thus $a^k = (a^{o(a)})^q = e^q = e$.

(c) Let $o(a) = n$. $a^k = a^m \Leftrightarrow a^{k-m} = e \Leftrightarrow n|(k-m) \Leftrightarrow k \equiv m \pmod{n}$.

Proof of Proposition 3

(a) Let a have infinite order. Suppose that $a^k = a^m$ for $k, m \in \mathbf{Z}$, with $k \geq m$. Then $a^{k-m} = e$. (Why?) Thus, we must have $k - m = 0$. (Why?)

(b) $\Rightarrow$: Let $o(a) = n$, and suppose that $a^k = e$. *To show*: $n|k$.
Write $k = nq + r$, where $0 \leq r < n$. (Why?) Thus,

$$a^r = a^{k-nq} = a^k a^{-nq} = a^k (a^n)^{-q} = e \cdot e^{-q} = e.$$

We must have $r = 0$. (Why?) Therefore $k = nq$.
$\Leftarrow$: If $o(a)|k$, then $k = o(a) \cdot q$. Thus $a^k = (a^{o(a)})^q = e^q = e$.

(c) Let $o(a) = n$. $a^k = a^m \Leftrightarrow a^{k-m} = e \Leftrightarrow n|(k-m) \Leftrightarrow k \equiv m \pmod{n}$.
Claim: The subset $S = \{e, a, \ldots, a^{n-1}\}$ is a subgroup. (Why?)[

Proof of Proposition 3

(a) Let a have infinite order. Suppose that $a^k = a^m$ for $k, m \in \mathbf{Z}$, with $k \geq m$. Then $a^{k-m} = e$. (Why?) Thus, we must have $k - m = 0$. (Why?)

(b) $\Rightarrow$: Let $o(a) = n$, and suppose that $a^k = e$. *To show*: $n|k$.
Write $k = nq + r$, where $0 \leq r < n$. (Why?) Thus,

$$a^r = a^{k-nq} = a^k a^{-nq} = a^k (a^n)^{-q} = e \cdot e^{-q} = e.$$

We must have $r = 0$. (Why?) Therefore $k = nq$.
$\Leftarrow$: If $o(a)|k$, then $k = o(a) \cdot q$. Thus $a^k = (a^{o(a)})^q = e^q = e$.

(c) Let $o(a) = n$. $a^k = a^m \Leftrightarrow a^{k-m} = e \Leftrightarrow n|(k - m) \Leftrightarrow k \equiv m \pmod{n}$.
Claim: The subset $S = \{e, a, \ldots, a^{n-1}\}$ is a subgroup. (Why?)[Cor. 8]

Proof of Proposition 3

(a) Let a have infinite order. Suppose that $a^k = a^m$ for $k, m \in \mathbf{Z}$, with $k \geq m$. Then $a^{k-m} = e$. (Why?) Thus, we must have $k - m = 0$. (Why?)

(b) $\Rightarrow$: Let $o(a) = n$, and suppose that $a^k = e$. *To show*: $n|k$.
Write $k = nq + r$, where $0 \leq r < n$. (Why?) Thus,

$$a^r = a^{k-nq} = a^k a^{-nq} = a^k (a^n)^{-q} = e \cdot e^{-q} = e.$$

We must have $r = 0$. (Why?) Therefore $k = nq$.
$\Leftarrow$: If $o(a)|k$, then $k = o(a) \cdot q$. Thus $a^k = (a^{o(a)})^q = e^q = e$.

(c) Let $o(a) = n$. $a^k = a^m \Leftrightarrow a^{k-m} = e \Leftrightarrow n|(k-m) \Leftrightarrow k \equiv m \pmod{n}$.
Claim: The subset $S = \{e, a, \ldots, a^{n-1}\}$ is a subgroup. (Why?)[Cor. 8]
To show: $S = \langle a \rangle$.

Proof of Proposition 3

(a) Let a have infinite order. Suppose that $a^k = a^m$ for $k, m \in \mathbf{Z}$, with $k \geq m$. Then $a^{k-m} = e$. (Why?) Thus, we must have $k - m = 0$. (Why?)

(b) $\Rightarrow$: Let $o(a) = n$, and suppose that $a^k = e$. *To show*: $n|k$.
Write $k = nq + r$, where $0 \leq r < n$. (Why?) Thus,

$$a^r = a^{k-nq} = a^k a^{-nq} = a^k (a^n)^{-q} = e \cdot e^{-q} = e.$$

We must have $r = 0$. (Why?) Therefore $k = nq$.
$\Leftarrow$: If $o(a)|k$, then $k = o(a) \cdot q$. Thus $a^k = (a^{o(a)})^q = e^q = e$.

(c) Let $o(a) = n$. $a^k = a^m \Leftrightarrow a^{k-m} = e \Leftrightarrow n|(k-m) \Leftrightarrow k \equiv m \pmod{n}$.
Claim: The subset $S = \{e, a, \ldots, a^{n-1}\}$ is a subgroup. (Why?)[Cor. 8]
To show: $S = \langle a \rangle$.

- Since $a \in S$, then $\langle a \rangle \subseteq S$. (Why?) [Proposition 2]

Proof of Proposition 3

(a) Let a have infinite order. Suppose that $a^k = a^m$ for $k, m \in \mathbf{Z}$, with $k \geq m$. Then $a^{k-m} = e$. (Why?) Thus, we must have $k - m = 0$. (Why?)

(b) $\Rightarrow$: Let $o(a) = n$, and suppose that $a^k = e$. *To show*: $n|k$.
Write $k = nq + r$, where $0 \leq r < n$. (Why?) Thus,

$$a^r = a^{k-nq} = a^k a^{-nq} = a^k(a^n)^{-q} = e \cdot e^{-q} = e.$$

We must have $r = 0$. (Why?) Therefore $k = nq$.
$\Leftarrow$: If $o(a)|k$, then $k = o(a) \cdot q$. Thus $a^k = (a^{o(a)})^q = e^q = e$.

(c) Let $o(a) = n$. $a^k = a^m \Leftrightarrow a^{k-m} = e \Leftrightarrow n|(k-m) \Leftrightarrow k \equiv m \pmod{n}$.
Claim: The subset $S = \{e, a, \ldots, a^{n-1}\}$ is a subgroup. (Why?)[Cor. 8]
To show: $S = \langle a \rangle$.

- Since $a \in S$, then $\langle a \rangle \subseteq S$. (Why?) [Proposition 2]
- On the other hand, $S \subseteq \langle a \rangle$ by the definition of $\langle a \rangle$.

Proof of Proposition 3

(a) Let a have infinite order. Suppose that $a^k = a^m$ for $k, m \in \mathbf{Z}$, with $k \geq m$. Then $a^{k-m} = e$. (Why?) Thus, we must have $k - m = 0$. (Why?)

(b) $\Rightarrow$: Let $o(a) = n$, and suppose that $a^k = e$. *To show*: $n|k$.
Write $k = nq + r$, where $0 \leq r < n$. (Why?) Thus,

$$a^r = a^{k-nq} = a^k a^{-nq} = a^k (a^n)^{-q} = e \cdot e^{-q} = e.$$

We must have $r = 0$. (Why?) Therefore $k = nq$.
$\Leftarrow$: If $o(a)|k$, then $k = o(a) \cdot q$. Thus $a^k = (a^{o(a)})^q = e^q = e$.

(c) Let $o(a) = n$. $a^k = a^m \Leftrightarrow a^{k-m} = e \Leftrightarrow n|(k-m) \Leftrightarrow k \equiv m \pmod{n}$.
Claim: The subset $S = \{e, a, \ldots, a^{n-1}\}$ is a subgroup. (Why?)[Cor. 8]
To show: $S = \langle a \rangle$.

- Since $a \in S$, then $\langle a \rangle \subseteq S$. (Why?) [Proposition 2]
- On the other hand, $S \subseteq \langle a \rangle$ by the definition of $\langle a \rangle$.

Thus $|\langle a \rangle| = |S| = o(a)$.

Lagrange's Theorem

Theorem 18 (Lagrange)

If H is a subgroup of the finite group G, then $|H|$ is a divisor of $|G|$.

Lagrange's Theorem

Theorem 18 (Lagrange)

If H is a subgroup of the finite group G, then $|H|$ is a divisor of $|G|$.

To prove it, we need the following lemma:

Lemma 19 (Let H be a subgroup of the group G.)

Lagrange's Theorem

Theorem 18 (Lagrange)

If H is a subgroup of the finite group G, then $|H|$ is a divisor of $|G|$.

To prove it, we need the following lemma:

Lemma 19 (Let H be a subgroup of the group G.)

For $a, b \in G$ define $a \sim b$ if $ab^{-1} \in H$. Then $\sim$ is an equivalence relation.

Proof of Lemma 19:

Lagrange's Theorem

Theorem 18 (Lagrange)

If H is a subgroup of the finite group G, then $|H|$ is a divisor of $|G|$.

To prove it, we need the following lemma:

Lemma 19 (Let H be a subgroup of the group G.)

For $a, b \in G$ define $a \sim b$ if $ab^{-1} \in H$. Then $\sim$ is an equivalence relation.

Proof of Lemma 19:

(i) Reflexive: $a \sim a$

Theorem 18 (Lagrange)

If H is a subgroup of the finite group G, then $|H|$ is a divisor of $|G|$.

To prove it, we need the following lemma:

Lemma 19 (Let H be a subgroup of the group G.)

For $a, b \in G$ define $a \sim b$ if $ab^{-1} \in H$. Then $\sim$ is an equivalence relation.

Proof of Lemma 19:

(i) Reflexive: $a \sim a$ since $aa^{-1} = e \in H$.

(ii) Symmetric:

Lagrange's Theorem

Theorem 18 (Lagrange)

If H is a subgroup of the finite group G, then $|H|$ is a divisor of $|G|$.

To prove it, we need the following lemma:

Lemma 19 (Let H be a subgroup of the group G.)

For $a, b \in G$ define $a \sim b$ if $ab^{-1} \in H$. Then $\sim$ is an equivalence relation.

Proof of Lemma 19:

(i) Reflexive: $a \sim a$ since $aa^{-1} = e \in H$.

(ii) Symmetric: If $a \sim b$, then $ab^{-1} \in H$.

Lagrange's Theorem

Theorem 18 (Lagrange)

If H is a subgroup of the finite group G, then $|H|$ is a divisor of $|G|$.

To prove it, we need the following lemma:

Lemma 19 (Let H be a subgroup of the group G.)

For $a, b \in G$ define $a \sim b$ if $ab^{-1} \in H$. Then $\sim$ is an equivalence relation.

Proof of Lemma 19:

(i) Reflexive: $a \sim a$ since $aa^{-1} = e \in H$.

(ii) Symmetric: If $a \sim b$, then $ab^{-1} \in H$. $\Rightarrow ba^{-1} = (ab^{-1})^{-1} \in H$.

(iii) Transitive:

Theorem 18 (Lagrange)

If H is a subgroup of the finite group G, then $|H|$ is a divisor of $|G|$.

To prove it, we need the following lemma:

Lemma 19 (Let H be a subgroup of the group G.)

For $a, b \in G$ define $a \sim b$ if $ab^{-1} \in H$. Then $\sim$ is an equivalence relation.

Proof of Lemma 19:

(i) Reflexive: $a \sim a$ since $aa^{-1} = e \in H$.

(ii) Symmetric: If $a \sim b$, then $ab^{-1} \in H$. $\Rightarrow ba^{-1} = (ab^{-1})^{-1} \in H$.

(iii) Transitive: If $a \sim b$ and $b \sim c$,

Lagrange's Theorem

Theorem 18 (Lagrange)

If H is a subgroup of the finite group G, then $|H|$ is a divisor of $|G|$.

To prove it, we need the following lemma:

Lemma 19 (Let H be a subgroup of the group G.)

For $a, b \in G$ define $a \sim b$ if $ab^{-1} \in H$. Then $\sim$ is an equivalence relation.

Proof of Lemma 19:

(i) Reflexive: $a \sim a$ since $aa^{-1} = e \in H$.

(ii) Symmetric: If $a \sim b$, then $ab^{-1} \in H$. $\Rightarrow ba^{-1} = (ab^{-1})^{-1} \in H$.

(iii) Transitive: If $a \sim b$ and $b \sim c$, then $ab^{-1} \in H$ and $bc^{-1} \in H$.

Lagrange's Theorem

Theorem 18 (Lagrange)

If H is a subgroup of the finite group G, then $|H|$ is a divisor of $|G|$.

To prove it, we need the following lemma:

Lemma 19 (Let H be a subgroup of the group G.)

For $a, b \in G$ define $a \sim b$ if $ab^{-1} \in H$. Then $\sim$ is an equivalence relation.

Proof of Lemma 19:

(i) Reflexive: $a \sim a$ since $aa^{-1} = e \in H$.

(ii) Symmetric: If $a \sim b$, then $ab^{-1} \in H$. $\Rightarrow ba^{-1} = (ab^{-1})^{-1} \in H$.

(iii) Transitive: If $a \sim b$ and $b \sim c$, then $ab^{-1} \in H$ and $bc^{-1} \in H$. Thus,
$$ac^{-1} = (ab^{-1})(bc) \in H. \text{ (Why?)}$$

$\square$

Lagrange's Theorem

Theorem 18 (Lagrange)

If H is a subgroup of the finite group G, then $|H|$ is a divisor of $|G|$.

To prove it, we need the following lemma:

Lemma 19 (Let H be a subgroup of the group G.)

For $a, b \in G$ define $a \sim b$ if $ab^{-1} \in H$. Then $\sim$ is an equivalence relation.

Proof of Lemma 19:

(i) Reflexive: $a \sim a$ since $aa^{-1} = e \in H$.

(ii) Symmetric: If $a \sim b$, then $ab^{-1} \in H$. $\Rightarrow ba^{-1} = (ab^{-1})^{-1} \in H$.

(iii) Transitive: If $a \sim b$ and $b \sim c$, then $ab^{-1} \in H$ and $bc^{-1} \in H$. Thus,

$$ac^{-1} = (ab^{-1})(bc) \in H. \text{ (Why?)}$$

$\square$

If the operation is denoted additively, then define $a \sim b$ if $a + (-b) \in H$.

Lagrange's Theorem

Theorem 18 (Lagrange)

If H is a subgroup of the finite group G, then $|H|$ is a divisor of $|G|$.

To prove it, we need the following lemma:

Lemma 19 (Let H be a subgroup of the group G.)

For $a, b \in G$ define $a \sim b$ if $ab^{-1} \in H$. Then $\sim$ is an equivalence relation.

Proof of Lemma 19:

(i) Reflexive: $a \sim a$ since $aa^{-1} = e \in H$.

(ii) Symmetric: If $a \sim b$, then $ab^{-1} \in H$. $\Rightarrow ba^{-1} = (ab^{-1})^{-1} \in H$.

(iii) Transitive: If $a \sim b$ and $b \sim c$, then $ab^{-1} \in H$ and $bc^{-1} \in H$. Thus,

$$ac^{-1} = (ab^{-1})(bc) \in H. \text{ (Why?)}$$

$\square$

If the operation is denoted additively, then define $a \sim b$ if $a + (-b) \in H$. This is usually written as $a \sim b$ if $a - b \in H$.

Lagrange's Theorem

Theorem 18 (Lagrange)

If H is a subgroup of the finite group G, then $|H|$ is a divisor of $|G|$.

To prove it, we need the following lemma:

Lemma 19 (Let H be a subgroup of the group G.)

For $a, b \in G$ define $a \sim b$ if $ab^{-1} \in H$. Then $\sim$ is an equivalence relation.

Proof of Lemma 19:

(i) Reflexive: $a \sim a$ since $aa^{-1} = e \in H$.

(ii) Symmetric: If $a \sim b$, then $ab^{-1} \in H$. $\Rightarrow ba^{-1} = (ab^{-1})^{-1} \in H$.

(iii) Transitive: If $a \sim b$ and $b \sim c$, then $ab^{-1} \in H$ and $bc^{-1} \in H$. Thus,
$$ac^{-1} = (ab^{-1})(bc) \in H. \text{ (Why?)}$$

$\square$

If the operation is denoted additively, then define $a \sim b$ if $a + (-b) \in H$. This is usually written as $a \sim b$ if $a - b \in H$. For example, consider $G = \mathbf{Z}$ and H is the subgroup $n\mathbf{Z}$:

Lagrange's Theorem

Theorem 18 (Lagrange)

If H is a subgroup of the finite group G, then $|H|$ is a divisor of $|G|$.

To prove it, we need the following lemma:

Lemma 19 (Let H be a subgroup of the group G.)

For $a, b \in G$ define $a \sim b$ if $ab^{-1} \in H$. Then $\sim$ is an equivalence relation.

Proof of Lemma 19:

(i) Reflexive: $a \sim a$ since $aa^{-1} = e \in H$.

(ii) Symmetric: If $a \sim b$, then $ab^{-1} \in H$. $\Rightarrow ba^{-1} = (ab^{-1})^{-1} \in H$.

(iii) Transitive: If $a \sim b$ and $b \sim c$, then $ab^{-1} \in H$ and $bc^{-1} \in H$. Thus,

$$ac^{-1} = (ab^{-1})(bc) \in H. \text{ (Why?)}$$

$\square$

If the operation is denoted additively, then define $a \sim b$ if $a + (-b) \in H$. This is usually written as $a \sim b$ if $a - b \in H$. For example, consider $G = \mathbf{Z}$ and H is the subgroup $n\mathbf{Z}$: $a \equiv b \pmod{n} \Leftrightarrow n|(a-b) \Leftrightarrow a - b \in n\mathbf{Z}$.

Proof of Lagrange's Theorem

Let H be a subgroup of the finite group G, with $|G| = n$ and $|H| = m$.

Proof of Lagrange's Theorem

Let H be a subgroup of the finite group G, with $|G| = n$ and $|H| = m$.
Let $\sim$ denote the equivalence relation defined in the previous lemma, i.e.,

$$\text{For } a, b \in G, \text{ define } a \sim b \text{ if } ab^{-1} \in H.$$

Proof of Lagrange's Theorem

Let H be a subgroup of the finite group G, with $|G| = n$ and $|H| = m$.
Let $\sim$ denote the equivalence relation defined in the previous lemma, i.e.,

$$\text{For } a, b \in G, \text{ define } a \sim b \text{ if } ab^{-1} \in H.$$

For any $a \in G$, let $[a] = \{b \in G | b \sim a\}$ denote the equivalence class of a.

Proof of Lagrange's Theorem

Let H be a subgroup of the finite group G, with $|G| = n$ and $|H| = m$. Let $\sim$ denote the equivalence relation defined in the previous lemma, i.e.,

$$\text{For } a, b \in G, \text{ define } a \sim b \text{ if } ab^{-1} \in H.$$

For any $a \in G$, let $[a] = \{b \in G | b \sim a\}$ denote the equivalence class of a. Consider the function $\rho_a : H \to [a]$ defined by $\rho_a(h) = ha$ for all $h \in H$.
Claim:

Proof of Lagrange's Theorem

Let H be a subgroup of the finite group G, with $|G| = n$ and $|H| = m$. Let $\sim$ denote the equivalence relation defined in the previous lemma, i.e.,

$$\text{For } a, b \in G, \text{ define } a \sim b \text{ if } ab^{-1} \in H.$$

For any $a \in G$, let $[a] = \{b \in G | b \sim a\}$ denote the equivalence class of a. Consider the function $\rho_a : H \to [a]$ defined by $\rho_a(h) = ha$ for all $h \in H$.
Claim: The function ρ_a a one-to-one correspondence between H and $[a]$.

Proof of Lagrange's Theorem

Let H be a subgroup of the finite group G, with $|G| = n$ and $|H| = m$. Let $\sim$ denote the equivalence relation defined in the previous lemma, i.e.,

$$\text{For } a, b \in G, \text{ define } a \sim b \text{ if } ab^{-1} \in H.$$

For any $a \in G$, let $[a] = \{b \in G | b \sim a\}$ denote the equivalence class of a. Consider the function $\rho_a : H \to [a]$ defined by $\rho_a(h) = ha$ for all $h \in H$. *Claim*: The function ρ_a a one-to-one correspondence between H and $[a]$.

(i) The codomain of ρ_a is correct:

Proof of Lagrange's Theorem

Let H be a subgroup of the finite group G, with $|G| = n$ and $|H| = m$. Let $\sim$ denote the equivalence relation defined in the previous lemma, i.e.,

$$\text{For } a, b \in G, \text{ define } a \sim b \text{ if } ab^{-1} \in H.$$

For any $a \in G$, let $[a] = \{b \in G | b \sim a\}$ denote the equivalence class of a. Consider the function $\rho_a : H \to [a]$ defined by $\rho_a(h) = ha$ for all $h \in H$.
Claim: The function ρ_a a one-to-one correspondence between H and $[a]$.

(i) The codomain of ρ_a is correct: If $h \in H$, then $\rho_a(h) = ha \in [a]$. (Why?)

(ii) one-to-one:

Proof of Lagrange's Theorem

Let H be a subgroup of the finite group G, with $|G| = n$ and $|H| = m$. Let $\sim$ denote the equivalence relation defined in the previous lemma, i.e.,

$$\text{For } a, b \in G, \text{ define } a \sim b \text{ if } ab^{-1} \in H.$$

For any $a \in G$, let $[a] = \{b \in G | b \sim a\}$ denote the equivalence class of a. Consider the function $\rho_a : H \to [a]$ defined by $\rho_a(h) = ha$ for all $h \in H$.
Claim: The function ρ_a a one-to-one correspondence between H and $[a]$.

(i) The codomain of ρ_a is correct: If $h \in H$, then $\rho_a(h) = ha \in [a]$. (Why?)

(ii) one-to-one: For $h, k \in H$, if $\rho_a(h) = \rho_a(k)$,

Proof of Lagrange's Theorem

Let H be a subgroup of the finite group G, with $|G| = n$ and $|H| = m$.
Let $\sim$ denote the equivalence relation defined in the previous lemma, i.e.,

$$\text{For } a, b \in G, \text{ define } a \sim b \text{ if } ab^{-1} \in H.$$

For any $a \in G$, let $[a] = \{b \in G | b \sim a\}$ denote the equivalence class of a.
Consider the function $\rho_a : H \to [a]$ defined by $\rho_a(h) = ha$ for all $h \in H$.
Claim: The function ρ_a a one-to-one correspondence between H and $[a]$.

(i) The codomain of ρ_a is correct: If $h \in H$, then $\rho_a(h) = ha \in [a]$. (Why?)

(ii) one-to-one: For $h, k \in H$, if $\rho_a(h) = \rho_a(k)$, then $ha = ka$. $\Rightarrow h = k$.

(iii) onto:

Proof of Lagrange's Theorem

Let H be a subgroup of the finite group G, with $|G| = n$ and $|H| = m$.
Let $\sim$ denote the equivalence relation defined in the previous lemma, i.e.,

$$\text{For } a, b \in G, \text{ define } a \sim b \text{ if } ab^{-1} \in H.$$

For any $a \in G$, let $[a] = \{b \in G | b \sim a\}$ denote the equivalence class of a.
Consider the function $\rho_a : H \to [a]$ defined by $\rho_a(h) = ha$ for all $h \in H$.
Claim: The function ρ_a a one-to-one correspondence between H and $[a]$.

(i) The codomain of ρ_a is correct: If $h \in H$, then $\rho_a(h) = ha \in [a]$. (Why?)

(ii) one-to-one: For $h, k \in H$, if $\rho_a(h) = \rho_a(k)$, then $ha = ka$. $\Rightarrow h = k$.

(iii) onto: If $b \in [a]$,

Proof of Lagrange's Theorem

Let H be a subgroup of the finite group G, with $|G| = n$ and $|H| = m$.
Let $\sim$ denote the equivalence relation defined in the previous lemma, i.e.,

$$\text{For } a, b \in G, \text{ define } a \sim b \text{ if } ab^{-1} \in H.$$

For any $a \in G$, let $[a] = \{b \in G | b \sim a\}$ denote the equivalence class of a.
Consider the function $\rho_a : H \to [a]$ defined by $\rho_a(h) = ha$ for all $h \in H$.
Claim: The function ρ_a a one-to-one correspondence between H and $[a]$.

(i) The codomain of ρ_a is correct: If $h \in H$, then $\rho_a(h) = ha \in [a]$. (Why?)

(ii) one-to-one: For $h, k \in H$, if $\rho_a(h) = \rho_a(k)$, then $ha = ka$. $\Rightarrow h = k$.

(iii) onto: If $b \in [a]$, then $ba^{-1} = h$ for some $h \in H$.

Proof of Lagrange's Theorem

Let H be a subgroup of the finite group G, with $|G| = n$ and $|H| = m$. Let $\sim$ denote the equivalence relation defined in the previous lemma, i.e.,

$$\text{For } a, b \in G, \text{ define } a \sim b \text{ if } ab^{-1} \in H.$$

For any $a \in G$, let $[a] = \{b \in G | b \sim a\}$ denote the equivalence class of a. Consider the function $\rho_a : H \to [a]$ defined by $\rho_a(h) = ha$ for all $h \in H$. *Claim*: The function ρ_a a one-to-one correspondence between H and $[a]$.

(i) The codomain of ρ_a is correct: If $h \in H$, then $\rho_a(h) = ha \in [a]$. (Why?)

(ii) one-to-one: For $h, k \in H$, if $\rho_a(h) = \rho_a(k)$, then $ha = ka$. $\Rightarrow h = k$.

(iii) onto: If $b \in [a]$, then $ba^{-1} = h$ for some $h \in H$. $\Rightarrow b = ha = \rho_a(h)$.

Proof of Lagrange's Theorem

Let H be a subgroup of the finite group G, with $|G| = n$ and $|H| = m$. Let $\sim$ denote the equivalence relation defined in the previous lemma, i.e.,

$$\text{For } a, b \in G, \text{ define } a \sim b \text{ if } ab^{-1} \in H.$$

For any $a \in G$, let $[a] = \{b \in G | b \sim a\}$ denote the equivalence class of a. Consider the function $\rho_a : H \to [a]$ defined by $\rho_a(h) = ha$ for all $h \in H$. *Claim*: The function ρ_a a one-to-one correspondence between H and $[a]$.

(i) The codomain of ρ_a is correct: If $h \in H$, then $\rho_a(h) = ha \in [a]$. (Why?)

(ii) one-to-one: For $h, k \in H$, if $\rho_a(h) = \rho_a(k)$, then $ha = ka$. $\Rightarrow h = k$.

(iii) onto: If $b \in [a]$, then $ba^{-1} = h$ for some $h \in H$. $\Rightarrow b = ha = \rho_a(h)$.

Since the equivalence classes of $\sim$ partition G, each element of G belongs to precisely one of the equivalence classes.

Proof of Lagrange's Theorem

Let H be a subgroup of the finite group G, with $|G| = n$ and $|H| = m$. Let $\sim$ denote the equivalence relation defined in the previous lemma, i.e.,

$$\text{For } a, b \in G, \text{ define } a \sim b \text{ if } ab^{-1} \in H.$$

For any $a \in G$, let $[a] = \{b \in G | b \sim a\}$ denote the equivalence class of a. Consider the function $\rho_a : H \to [a]$ defined by $\rho_a(h) = ha$ for all $h \in H$.
Claim: The function ρ_a a one-to-one correspondence between H and $[a]$.

(i) The codomain of ρ_a is correct: If $h \in H$, then $\rho_a(h) = ha \in [a]$. (Why?)

(ii) one-to-one: For $h, k \in H$, if $\rho_a(h) = \rho_a(k)$, then $ha = ka$. $\Rightarrow h = k$.

(iii) onto: If $b \in [a]$, then $ba^{-1} = h$ for some $h \in H$. $\Rightarrow b = ha = \rho_a(h)$.

Since the equivalence classes of $\sim$ partition G, each element of G belongs to precisely one of the equivalence classes. We have shown that each equivalence class $[a]$ has m elements. (Why?)

Proof of Lagrange's Theorem

Let H be a subgroup of the finite group G, with $|G| = n$ and $|H| = m$.
Let $\sim$ denote the equivalence relation defined in the previous lemma, i.e.,

$$\text{For } a, b \in G, \text{ define } a \sim b \text{ if } ab^{-1} \in H.$$

For any $a \in G$, let $[a] = \{b \in G | b \sim a\}$ denote the equivalence class of a.
Consider the function $\rho_a : H \to [a]$ defined by $\rho_a(h) = ha$ for all $h \in H$.
Claim: The function ρ_a a one-to-one correspondence between H and $[a]$.

(i) The codomain of ρ_a is correct: If $h \in H$, then $\rho_a(h) = ha \in [a]$. (Why?)

(ii) one-to-one: For $h, k \in H$, if $\rho_a(h) = \rho_a(k)$, then $ha = ka$. $\Rightarrow h = k$.

(iii) onto: If $b \in [a]$, then $ba^{-1} = h$ for some $h \in H$. $\Rightarrow b = ha = \rho_a(h)$.

Since the equivalence classes of $\sim$ partition G, each element of G belongs to precisely one of the equivalence classes. We have shown that each equivalence class $[a]$ has m elements. (Why?)
Counting the elements of G according to the distinct equivalence classes,

Proof of Lagrange's Theorem

Let H be a subgroup of the finite group G, with $|G| = n$ and $|H| = m$.
Let $\sim$ denote the equivalence relation defined in the previous lemma, i.e.,

$$\text{For } a, b \in G, \text{ define } a \sim b \text{ if } ab^{-1} \in H.$$

For any $a \in G$, let $[a] = \{b \in G | b \sim a\}$ denote the equivalence class of a.
Consider the function $\rho_a : H \to [a]$ defined by $\rho_a(h) = ha$ for all $h \in H$.
Claim: The function ρ_a a one-to-one correspondence between H and $[a]$.

(i) The codomain of ρ_a is correct: If $h \in H$, then $\rho_a(h) = ha \in [a]$. (Why?)

(ii) one-to-one: For $h, k \in H$, if $\rho_a(h) = \rho_a(k)$, then $ha = ka$. $\Rightarrow h = k$.

(iii) onto: If $b \in [a]$, then $ba^{-1} = h$ for some $h \in H$. $\Rightarrow b = ha = \rho_a(h)$.

Since the equivalence classes of $\sim$ partition G, each element of G belongs to precisely one of the equivalence classes. We have shown that each equivalence class $[a]$ has m elements. (Why?)
Counting the elements of G according to the distinct equivalence classes, then we get $n = mt$, where t is the number of distinct equivalence classes.

Example: $G = S_3$

(1) Let $H = \langle (123) \rangle = \{(1), (123), (132)\}$.

Example: $G = S_3$

(1) Let $H = \langle (123) \rangle = \{(1), (123), (132)\}$.
By definition, the elements of H form the first equivalence class.

Example: $G = S_3$

(1) Let $H = \langle (123) \rangle = \{(1), (123), (132)\}$.
By definition, the elements of H form the first equivalence class.
Any other equivalence class must be disjoint from the first one and have the same number of elements,

Example: $G = S_3$

(1) Let $H = \langle(123)\rangle = \{(1), (123), (132)\}$.
By definition, the elements of H form the first equivalence class.
Any other equivalence class must be disjoint from the first one and have the same number of elements, so the only possibility is that the remaining elements of G must form a second equivalence class:

$$\{(12), (13), (23)\}.$$

Example: $G = S_3$

(1) Let $H = \langle(123)\rangle = \{(1), (123), (132)\}$.
By definition, the elements of H form the first equivalence class.
Any other equivalence class must be disjoint from the first one and have the same number of elements, so the only possibility is that the remaining elements of G must form a second equivalence class:

$$\{(12), (13), (23)\}.$$

(2) Let $K = \langle(12)\rangle = \{(1), (12)\}$.

Example: $G = S_3$

(1) Let $H = \langle (123) \rangle = \{(1), (123), (132)\}$.
By definition, the elements of H form the first equivalence class.
Any other equivalence class must be disjoint from the first one and have the same number of elements, so the only possibility is that the remaining elements of G must form a second equivalence class:

$$\{(12), (13), (23)\}.$$

(2) Let $K = \langle (12) \rangle = \{(1), (12)\}$.
So the equivalence classes must each contain two elements.

Example: $G = S_3$

(1) Let $H = \langle(123)\rangle = \{(1), (123), (132)\}$.
By definition, the elements of H form the first equivalence class.
Any other equivalence class must be disjoint from the first one and have the same number of elements, so the only possibility is that the remaining elements of G must form a second equivalence class:

$$\{(12), (13), (23)\}.$$

(2) Let $K = \langle(12)\rangle = \{(1), (12)\}$.
So the equivalence classes must each contain two elements.
We can find the equivalence class of $a \in G$ by multiplying it on the left by all elements of K. (Why?) [

Example: $G = S_3$

(1) Let $H = \langle(123)\rangle = \{(1), (123), (132)\}$.
By definition, the elements of H form the first equivalence class.
Any other equivalence class must be disjoint from the first one and have the same number of elements, so the only possibility is that the remaining elements of G must form a second equivalence class:
$$\{(12), (13), (23)\}.$$

(2) Let $K = \langle(12)\rangle = \{(1), (12)\}$.
So the equivalence classes must each contain two elements.
We can find the equivalence class of $a \in G$ by multiplying it on the left by all elements of K. (Why?) $[\rho_a : H \to [a];\ \rho_a(h) = ha, \forall h \in H.]$

Example: $G = S_3$

(1) Let $H = \langle(123)\rangle = \{(1), (123), (132)\}$.
By definition, the elements of H form the first equivalence class.
Any other equivalence class must be disjoint from the first one and have the same number of elements, so the only possibility is that the remaining elements of G must form a second equivalence class:

$$\{(12), (13), (23)\}.$$

(2) Let $K = \langle(12)\rangle = \{(1), (12)\}$.
So the equivalence classes must each contain two elements.
We can find the equivalence class of $a \in G$ by multiplying it on the left by all elements of K. (Why?) [$\rho_a : H \to [a]$; $\rho_a(h) = ha, \forall h \in H$.]
If $a = (123)$, then $(1)(123) = (123)$ and $(12)(123) = (23)$.

Example: $G = S_3$

(1) Let $H = \langle(123)\rangle = \{(1), (123), (132)\}$.
By definition, the elements of H form the first equivalence class.
Any other equivalence class must be disjoint from the first one and have the same number of elements, so the only possibility is that the remaining elements of G must form a second equivalence class:

$$\{(12), (13), (23)\}.$$

(2) Let $K = \langle(12)\rangle = \{(1), (12)\}$.
So the equivalence classes must each contain two elements.
We can find the equivalence class of $a \in G$ by multiplying it on the left by all elements of K. (Why?) [$\rho_a : H \to [a]$; $\rho_a(h) = ha, \forall h \in H$.]
If $a = (123)$, then $(1)(123) = (123)$ and $(12)(123) = (23)$.
And the remaining two elements form the third equivalence class.

Example: $G = S_3$

(1) Let $H = \langle(123)\rangle = \{(1), (123), (132)\}$.
By definition, the elements of H form the first equivalence class.
Any other equivalence class must be disjoint from the first one and have the same number of elements, so the only possibility is that the remaining elements of G must form a second equivalence class:

$$\{(12), (13), (23)\}.$$

(2) Let $K = \langle(12)\rangle = \{(1), (12)\}$.
So the equivalence classes must each contain two elements.
We can find the equivalence class of $a \in G$ by multiplying it on the left by all elements of K. (Why?) $[\rho_a : H \to [a];\ \rho_a(h) = ha, \forall h \in H.]$
If $a = (123)$, then $(1)(123) = (123)$ and $(12)(123) = (23)$.
And the remaining two elements form the third equivalence class. So the $\sim$ defined by the subgroup K determines three equivalence classes:

$$\{(1), (12)\}, \qquad \{(123), (23)\}, \qquad \{(132), (13)\}.$$

Corollaries

The converse of Lagrange's theorem is false. (See an example in §3.6.)

Corollary 20

Corollaries

The converse of Lagrange's theorem is false. (See an example in §3.6.)

Corollary 20

Let G be a finite group of order n.

(a) *For any $a \in G$, $o(a)$ is a divisor of n.*

(b) *For any $a \in G, a^n = e$.*

Corollaries

The converse of Lagrange's theorem is false. (See an example in §3.6.)

Corollary 20

Let G be a finite group of order n.

(a) *For any $a \in G$, $o(a)$ is a divisor of n.*

(b) *For any $a \in G, a^n = e$.*

(a) $\langle a \rangle$ is a subgroup and $|\langle a \rangle| = o(a)$

Corollaries

The converse of Lagrange's theorem is false. (See an example in §3.6.)

Corollary 20

Let G be a finite group of order n.

(a) *For any $a \in G$, $o(a)$ is a divisor of n.*

(b) *For any $a \in G, a^n = e$.*

(a) $\langle a \rangle$ is a subgroup and $|\langle a \rangle| = o(a) \Rightarrow o(a)|n$. (Why?)

Corollaries

The converse of Lagrange's theorem is false. (See an example in §3.6.)

Corollary 20

Let G be a finite group of order n.

(a) *For any $a \in G$, $o(a)$ is a divisor of n.*

(b) *For any $a \in G, a^n = e$.*

(a) $\langle a \rangle$ is a subgroup and $|\langle a \rangle| = o(a) \Rightarrow o(a)|n$. (Why?)

(b) It follows from part (a) immediately.

Corollary 21

Corollaries

The converse of Lagrange's theorem is false. (See an example in §3.6.)

Corollary 20

Let G be a finite group of order n.

(a) *For any $a \in G$, $o(a)$ is a divisor of n.*

(b) *For any $a \in G, a^n = e$.*

(a) $\langle a \rangle$ is a subgroup and $|\langle a \rangle| = o(a) \Rightarrow o(a)|n$. (Why?)
(b) It follows from part (a) immediately.

Corollary 21

Any group of prime order is cyclic.

Proof.

Let G be a group of order p, where p is a prime number.

Corollaries

The converse of Lagrange's theorem is false. (See an example in §3.6.)

Corollary 20

Let G be a finite group of order n.

(a) *For any $a \in G$, $o(a)$ is a divisor of n.*

(b) *For any $a \in G, a^n = e$.*

(a) $\langle a \rangle$ is a subgroup and $|\langle a \rangle| = o(a) \Rightarrow o(a)|n$. (Why?)
(b) It follows from part (a) immediately.

Corollary 21

Any group of prime order is cyclic.

Proof.

Let G be a group of order p, where p is a prime number. Let $a \in G$ and $a \neq e$.

Corollaries

The converse of Lagrange's theorem is false. (See an example in §3.6.)

Corollary 20

Let G be a finite group of order n.

(a) *For any $a \in G$, $o(a)$ is a divisor of n.*

(b) *For any $a \in G, a^n = e$.*

(a) $\langle a \rangle$ is a subgroup and $|\langle a \rangle| = o(a) \Rightarrow o(a)|n$. (Why?)
(b) It follows from part (a) immediately.

Corollary 21

Any group of prime order is cyclic.

Proof.

Let G be a group of order p, where p is a prime number. Let $a \in G$ and $a \neq e$. Then $|\langle a \rangle| \neq 1$,

Corollaries

The converse of Lagrange's theorem is false. (See an example in §3.6.)

Corollary 20

Let G be a finite group of order n.

(a) *For any $a \in G$, $o(a)$ is a divisor of n.*

(b) *For any $a \in G, a^n = e$.*

(a) $\langle a \rangle$ is a subgroup and $|\langle a \rangle| = o(a) \Rightarrow o(a)|n$. (Why?)
(b) It follows from part (a) immediately.

Corollary 21

Any group of prime order is cyclic.

Proof.

Let G be a group of order p, where p is a prime number. Let $a \in G$ and $a \neq e$. Then $|\langle a \rangle| \neq 1$, and so $|\langle a \rangle|$ must be p. (Why?)

Corollaries

The converse of Lagrange's theorem is false. (See an example in §3.6.)

Corollary 20

Let G be a finite group of order n.

(a) *For any $a \in G$, $o(a)$ is a divisor of n.*

(b) *For any $a \in G, a^n = e$.*

(a) $\langle a \rangle$ is a subgroup and $|\langle a \rangle| = o(a) \Rightarrow o(a)|n$. (Why?)

(b) It follows from part (a) immediately.

Corollary 21

Any group of prime order is cyclic.

Proof.

Let G be a group of order p, where p is a prime number. Let $a \in G$ and $a \neq e$. Then $|\langle a \rangle| \neq 1$, and so $|\langle a \rangle|$ must be p. (Why?)
This implies that $\langle a \rangle = G$, and thus G is cyclic. $\square$

Examples

Example 22 (Euler's theorem: If $(a, n) = 1$, then $a^{\varphi(n)} \equiv 1 \pmod{n}$)

Examples

Example 22 (Euler's theorem: If $(a, n) = 1$, then $a^{\varphi(n)} \equiv 1 \pmod{n}$)

Let $G = \mathbf{Z}_n^\times$, the group of units modulo n.

Examples

Example 22 (Euler's theorem: If $(a, n) = 1$, then $a^{\varphi(n)} \equiv 1 \pmod{n}$)

Let $G = \mathbf{Z}_n^\times$, the group of units modulo n. We know that $|G| = \varphi(n)$. It follows from Corollary 20 (b) that $[a]^{\varphi(n)} = [1]$ for any $[a] \in G$. $\square$

Example 23 (aHa^{-1} is a subgroup of G.)

Examples

Example 22 (Euler's theorem: If $(a, n) = 1$, then $a^{\varphi(n)} \equiv 1 \pmod{n}$)

Let $G = \mathbf{Z}_n^\times$, the group of units modulo n. We know that $|G| = \varphi(n)$. It follows from Corollary 20 (b) that $[a]^{\varphi(n)} = [1]$ for any $[a] \in G$. $\square$

Example 23 (aHa^{-1} is a subgroup of G.)

Let H be any subgroup of G and a fixed element $a \in G$. We will show that $aHa^{-1} = \{g \in G \mid g = aha^{-1} \text{ for some } h \in H\}$ is a subgroup of G.

Examples

Example 22 (Euler's theorem: If $(a, n) = 1$, then $a^{\varphi(n)} \equiv 1 \pmod{n}$)

Let $G = \mathbf{Z}_n^\times$, the group of units modulo n. We know that $|G| = \varphi(n)$. It follows from Corollary 20 (b) that $[a]^{\varphi(n)} = [1]$ for any $[a] \in G$. □

Example 23 (aHa^{-1} is a subgroup of G.)

Let H be any subgroup of G and a fixed element $a \in G$. We will show that $aHa^{-1} = \{g \in G \mid g = aha^{-1} \text{ for some } h \in H\}$ is a subgroup of G.

(i) Closure:

Examples

Example 22 (Euler's theorem: If $(a, n) = 1$, then $a^{\varphi(n)} \equiv 1 \pmod{n}$)

Let $G = \mathbf{Z}_n^{\times}$, the group of units modulo n. We know that $|G| = \varphi(n)$. It follows from Corollary 20 (b) that $[a]^{\varphi(n)} = [1]$ for any $[a] \in G$. $\square$

Example 23 (aHa^{-1} is a subgroup of G.)

Let H be any subgroup of G and a fixed element $a \in G$. We will show that $aHa^{-1} = \{g \in G \mid g = aha^{-1} \text{ for some } h \in H\}$ is a subgroup of G.

(i) Closure: Let $g_i = ah_ia^{-1}, i = \{1, 2\}$.

Examples

Example 22 (Euler's theorem: If $(a, n) = 1$, then $a^{\varphi(n)} \equiv 1 \pmod{n}$)

Let $G = \mathbf{Z}_n^\times$, the group of units modulo n. We know that $|G| = \varphi(n)$. It follows from Corollary 20 (b) that $[a]^{\varphi(n)} = [1]$ for any $[a] \in G$. □

Example 23 (aHa^{-1} is a subgroup of G.)

Let H be any subgroup of G and a fixed element $a \in G$. We will show that $aHa^{-1} = \{g \in G \mid g = aha^{-1} \text{ for some } h \in H\}$ is a subgroup of G.

(i) Closure: Let $g_i = ah_ia^{-1}, i = \{1, 2\}. \Rightarrow g_1g_2 = a(h_1h_2)a^{-1} \in aHa^{-1}$

(ii) Identity:

Examples

Example 22 (Euler's theorem: If $(a, n) = 1$, then $a^{\varphi(n)} \equiv 1 \pmod{n}$)

Let $G = \mathbf{Z}_n^\times$, the group of units modulo n. We know that $|G| = \varphi(n)$. It follows from Corollary 20 (b) that $[a]^{\varphi(n)} = [1]$ for any $[a] \in G$. □

Example 23 (aHa^{-1} is a subgroup of G.)

Let H be any subgroup of G and a fixed element $a \in G$. We will show that $aHa^{-1} = \{g \in G \mid g = aha^{-1} \text{ for some } h \in H\}$ is a subgroup of G.

(i) Closure: Let $g_i = ah_ia^{-1}, i = \{1, 2\}$. $\Rightarrow g_1g_2 = a(h_1h_2)a^{-1} \in aHa^{-1}$

(ii) Identity: $e = aea^{-1} \in aHa^{-1}$

(iii) Inverses:

Examples

Example 22 (Euler's theorem: If $(a, n) = 1$, then $a^{\varphi(n)} \equiv 1 \pmod{n}$)

Let $G = \mathbf{Z}_n^{\times}$, the group of units modulo n. We know that $|G| = \varphi(n)$. It follows from Corollary 20 (b) that $[a]^{\varphi(n)} = [1]$ for any $[a] \in G$. $\square$

Example 23 (aHa^{-1} is a subgroup of G.)

Let H be any subgroup of G and a fixed element $a \in G$. We will show that $aHa^{-1} = \{g \in G \mid g = aha^{-1} \text{ for some } h \in H\}$ is a subgroup of G.

(i) Closure: Let $g_i = ah_ia^{-1}, i = \{1, 2\}$. $\Rightarrow g_1g_2 = a(h_1h_2)a^{-1} \in aHa^{-1}$

(ii) Identity: $e = aea^{-1} \in aHa^{-1}$

(iii) Inverses: $g = aha^{-1} \in aHa^{-1}$

Examples

Example 22 (Euler's theorem: If $(a, n) = 1$, then $a^{\varphi(n)} \equiv 1 \pmod{n}$)

Let $G = \mathbf{Z}_n^\times$, the group of units modulo n. We know that $|G| = \varphi(n)$. It follows from Corollary 20 (b) that $[a]^{\varphi(n)} = [1]$ for any $[a] \in G$. $\square$

Example 23 (aHa^{-1} is a subgroup of G.)

Let H be any subgroup of G and a fixed element $a \in G$. We will show that $aHa^{-1} = \{g \in G \mid g = aha^{-1} \text{ for some } h \in H\}$ is a subgroup of G.

(i) Closure: Let $g_i = ah_ia^{-1}, i = \{1, 2\}$. $\Rightarrow g_1g_2 = a(h_1h_2)a^{-1} \in aHa^{-1}$

(ii) Identity: $e = aea^{-1} \in aHa^{-1}$

(iii) Inverses: $g = aha^{-1} \in aHa^{-1} \Rightarrow g^{-1} = ah^{-1}a^{-1} \in aHa^{-1}$. (Why?)

One more example: nth powers

Let G be an abelian group, and let n be a fixed positive integer. Define

$$N = \{g \in G \mid g = a^n \text{ for some } a \in G\}.$$

We will show that N is a subgroup of G.

One more example: nth powers

Let G be an abelian group, and let n be a fixed positive integer. Define

$$N = \{g \in G \mid g = a^n \text{ for some } a \in G\}.$$

We will show that N is a subgroup of G.

Proof.

Use Corollary 7: *To show* N is nonempty and $g_1 g_2^{-1} \in N, \forall g_1, g_2 \in N$.

One more example: nth powers

Let G be an abelian group, and let n be a fixed positive integer. Define

$$N = \{g \in G \mid g = a^n \text{ for some } a \in G\}.$$

We will show that N is a subgroup of G.

Proof.

Use Corollary 7: *To show* N is nonempty and $g_1 g_2^{-1} \in N, \forall g_1, g_2 \in N$.

- The identity element $e \in N$ since $e = e^n$.

One more example: nth powers

Let G be an abelian group, and let n be a fixed positive integer. Define

$$N = \{g \in G \mid g = a^n \text{ for some } a \in G\}.$$

We will show that N is a subgroup of G.

Proof.

Use Corollary 7: *To show* N is nonempty and $g_1 g_2^{-1} \in N, \forall g_1, g_2 \in N$.

- The identity element $e \in N$ since $e = e^n$.
- Let $g_1 = a_1^n$ and $g_2 = a_2^n$ for some $a_1, a_2 \in G$.

One more example: nth powers

Let G be an abelian group, and let n be a fixed positive integer. Define

$$N = \{g \in G \mid g = a^n \text{ for some } a \in G\}.$$

We will show that N is a subgroup of G.

Proof.

Use Corollary 7: *To show* N is nonempty and $g_1 g_2^{-1} \in N, \forall g_1, g_2 \in N$.

- The identity element $e \in N$ since $e = e^n$.
- Let $g_1 = a_1^n$ and $g_2 = a_2^n$ for some $a_1, a_2 \in G$. So

$$g_1 g_2^{-1} = a_1^n (a_2^n)^{-1} = a_1^n (a_2^{-1})^n \overset{!}{=} (a_1 a_2^{-1})^n \in N.$$

One more example: nth powers

Let G be an abelian group, and let n be a fixed positive integer. Define

$$N = \{g \in G \mid g = a^n \text{ for some } a \in G\}.$$

We will show that N is a subgroup of G.

Proof.

Use Corollary 7: *To show* N is nonempty and $g_1 g_2^{-1} \in N, \forall g_1, g_2 \in N$.

- The identity element $e \in N$ since $e = e^n$.
- Let $g_1 = a_1^n$ and $g_2 = a_2^n$ for some $a_1, a_2 \in G$. So

$$g_1 g_2^{-1} = a_1^n (a_2^n)^{-1} = a_1^n (a_2^{-1})^n \overset{!}{=} (a_1 a_2^{-1})^n \in N.$$

The last equality "$\overset{!}{=}$" holds. (Why?)

$\square$