§3.3 Constructing Examples

Shaoyun Yi

MATH 546/701I

University of South Carolina

May 20-21, 2020

Review

- Subgroup H: No worry about *associativity* $\begin{cases} \text{Closure} \\ \text{Identity} \\ \text{Inverses} \end{cases}$

Review

- Subgroup H: No worry about *associativity* $\begin{cases} \text{Closure} \\ \text{Identity} \\ \text{Inverses} \end{cases}$
  - **Corollary 7:** $\Leftrightarrow$ H is nonempty and $ab^{-1} \in H$ for all $a, b \in H$

Review

- Subgroup H: No worry about *associativity* $\begin{cases} \text{Closure} \\ \text{Identity} \\ \text{Inverses} \end{cases}$
  - **Corollary 7:** $\Leftrightarrow$ H is nonempty and $ab^{-1} \in H$ for all $a, b \in H$
  - **Corollary 8:** add "H is finite" $\Leftrightarrow$ H is nonempty and $ab \in H, \forall a, b \in H$

Review

- Subgroup H: No worry about *associativity* $\begin{cases} \text{Closure} \\ \text{Identity} \\ \text{Inverses} \end{cases}$
  - **Corollary 7:** $\Leftrightarrow H$ is nonempty and $ab^{-1} \in H$ for all $a, b \in H$
  - **Corollary 8:** add "*H* is finite" $\Leftrightarrow H$ is nonempty and $ab \in H, \forall a, b \in H$
  - Examples: $\mathbf{Z} \subseteq \mathbf{Q} \subseteq \mathbf{R} \subseteq \mathbf{C}$; $\mathbf{R}^+ \subseteq \mathbf{R}^\times$; $n\mathbf{Z} \subseteq \mathbf{Z}$; $\mathrm{SL}_n(\mathbf{R}) \subseteq \mathrm{GL}_n(\mathbf{R})$.

Review

- Subgroup H: No worry about *associativity* $\begin{cases} \text{Closure} \\ \text{Identity} \\ \text{Inverses} \end{cases}$
  - **Corollary 7:** $\Leftrightarrow H$ is nonempty and $ab^{-1} \in H$ for all $a, b \in H$
  - **Corollary 8:** add "H is finite" $\Leftrightarrow H$ is nonempty and $ab \in H, \forall a, b \in H$
  - Examples: $\mathbf{Z} \subseteq \mathbf{Q} \subseteq \mathbf{R} \subseteq \mathbf{C}$; $\mathbf{R}^{+} \subseteq \mathbf{R}^{\times}$; $n\mathbf{Z} \subseteq \mathbf{Z}$; $\mathrm{SL}_n(\mathbf{R}) \subseteq \mathrm{GL}_n(\mathbf{R})$.
- Cyclic subgroup $\langle a \rangle$ is the **smallest** subgroup of G containing $a \in G$.

Review

- Subgroup H: No worry about *associativity* $\begin{cases} \text{Closure} \\ \text{Identity} \\ \text{Inverses} \end{cases}$
  - **Corollary 7:** $\Leftrightarrow$ H is nonempty and $ab^{-1} \in H$ for all $a, b \in H$
  - **Corollary 8:** add "H is finite"$\Leftrightarrow$ H is nonempty and $ab \in H, \forall a, b \in H$
  - Examples: $\mathbf{Z} \subseteq \mathbf{Q} \subseteq \mathbf{R} \subseteq \mathbf{C}$; $\mathbf{R}^+ \subseteq \mathbf{R}^\times$; $n\mathbf{Z} \subseteq \mathbf{Z}$; $\mathrm{SL}_n(\mathbf{R}) \subseteq \mathrm{GL}_n(\mathbf{R})$.
- Cyclic subgroup $\langle a \rangle$ is the **smallest** subgroup of G containing $a \in G$.
  For example, $\langle i \rangle \subseteq \mathbf{C}^\times; \langle 2i \rangle \subseteq \mathbf{C}^\times; \langle (123) \rangle \subseteq S_3; \langle (12) \rangle \subseteq S_3$.

Review

- Subgroup H: No worry about *associativity* $\begin{cases} \text{Closure} \\ \text{Identity} \\ \text{Inverses} \end{cases}$
  - **Corollary 7:** $\Leftrightarrow H$ is nonempty and $ab^{-1} \in H$ for all $a, b \in H$
  - **Corollary 8:** add "H is finite"$\Leftrightarrow H$ is nonempty and $ab \in H, \forall a, b \in H$
  - Examples: $\mathbf{Z} \subseteq \mathbf{Q} \subseteq \mathbf{R} \subseteq \mathbf{C}$; $\mathbf{R}^+ \subseteq \mathbf{R}^\times$; $n\mathbf{Z} \subseteq \mathbf{Z}$; $\mathrm{SL}_n(\mathbf{R}) \subseteq \mathrm{GL}_n(\mathbf{R})$.
- Cyclic subgroup $\langle a \rangle$ is the **smallest** subgroup of G containing $a \in G$.
  For example, $\langle i \rangle \subseteq \mathbf{C}^\times; \langle 2i \rangle \subseteq \mathbf{C}^\times; \langle (123) \rangle \subseteq S_3; \langle (12) \rangle \subseteq S_3$.
- G is cyclic if $G = \langle a \rangle$.

Review

- Subgroup H: No worry about *associativity* $\begin{cases} \text{Closure} \\ \text{Identity} \\ \text{Inverses} \end{cases}$
  - **Corollary 7:** $\Leftrightarrow H$ is nonempty and $ab^{-1} \in H$ for all $a, b \in H$
  - **Corollary 8:** add "H is finite"$\Leftrightarrow H$ is nonempty and $ab \in H, \forall a, b \in H$
  - Examples: $\mathbf{Z} \subseteq \mathbf{Q} \subseteq \mathbf{R} \subseteq \mathbf{C}$; $\mathbf{R}^+ \subseteq \mathbf{R}^\times$; $n\mathbf{Z} \subseteq \mathbf{Z}$; $\mathrm{SL}_n(\mathbf{R}) \subseteq \mathrm{GL}_n(\mathbf{R})$.
- Cyclic subgroup $\langle a \rangle$ is the **smallest** subgroup of G containing $a \in G$.
  For example, $\langle i \rangle \subseteq \mathbf{C}^\times; \langle 2i \rangle \subseteq \mathbf{C}^\times; \langle (123) \rangle \subseteq S_3; \langle (12) \rangle \subseteq S_3$.
- G is cyclic if $G = \langle a \rangle$.
  For example, $\mathbf{Z}; \mathbf{Z}_n; \mathbf{Z}_5^\times$. Not examples: $\mathbf{Z}_8^\times; S_3$.

Review

- Subgroup H: No worry about *associativity* $\begin{cases} \text{Closure} \\ \text{Identity} \\ \text{Inverses} \end{cases}$
  - **Corollary 7:** $\Leftrightarrow$ H is nonempty and $ab^{-1} \in H$ for all $a, b \in H$
  - **Corollary 8:** add "H is finite" $\Leftrightarrow$ H is nonempty and $ab \in H, \forall a, b \in H$
  - Examples: $\mathbf{Z} \subseteq \mathbf{Q} \subseteq \mathbf{R} \subseteq \mathbf{C}$; $\mathbf{R}^+ \subseteq \mathbf{R}^\times$; $n\mathbf{Z} \subseteq \mathbf{Z}$; $\mathrm{SL}_n(\mathbf{R}) \subseteq \mathrm{GL}_n(\mathbf{R})$.
- Cyclic subgroup $\langle a \rangle$ is the **smallest** subgroup of G containing $a \in G$.
  For example, $\langle i \rangle \subseteq \mathbf{C}^\times; \langle 2i \rangle \subseteq \mathbf{C}^\times; \langle (123) \rangle \subseteq S_3; \langle (12) \rangle \subseteq S_3$.
- G is cyclic if $G = \langle a \rangle$.
  For example, $\mathbf{Z}; \mathbf{Z}_n; \mathbf{Z}_5^\times$. Not examples: $\mathbf{Z}_8^\times; S_3$.
- $o(a) = |\langle a \rangle|$.

Review

- Subgroup H: No worry about *associativity* $\begin{cases} \text{Closure} \\ \text{Identity} \\ \text{Inverses} \end{cases}$
  - **Corollary 7:** $\Leftrightarrow H$ is nonempty and $ab^{-1} \in H$ for all $a, b \in H$
  - **Corollary 8:** add "H is finite" $\Leftrightarrow H$ is nonempty and $ab \in H, \forall a, b \in H$
  - Examples: $\mathbf{Z} \subseteq \mathbf{Q} \subseteq \mathbf{R} \subseteq \mathbf{C}$; $\mathbf{R}^{+} \subseteq \mathbf{R}^{\times}$; $n\mathbf{Z} \subseteq \mathbf{Z}$; $\mathrm{SL}_n(\mathbf{R}) \subseteq \mathrm{GL}_n(\mathbf{R})$.
- Cyclic subgroup $\langle a \rangle$ is the **smallest** subgroup of G containing $a \in G$.
  For example, $\langle i \rangle \subseteq \mathbf{C}^{\times}; \langle 2i \rangle \subseteq \mathbf{C}^{\times}; \langle (123) \rangle \subseteq S_3; \langle (12) \rangle \subseteq S_3$.
- G is cyclic if $G = \langle a \rangle$.
  For example, $\mathbf{Z}; \mathbf{Z}_n; \mathbf{Z}_5^{\times}$. Not examples: $\mathbf{Z}_8^{\times}; S_3$.
- $o(a) = |\langle a \rangle|$. If $o(a) = n$ is finite, then $a^k = e \Leftrightarrow n | k$ for $k \in \mathbf{Z}$.

- Subgroup H: No worry about *associativity* $\begin{cases} \text{Closure} \\ \text{Identity} \\ \text{Inverses} \end{cases}$
  - **Corollary 7:** $\Leftrightarrow$ H is nonempty and $ab^{-1} \in H$ for all $a, b \in H$
  - **Corollary 8:** add "H is finite" $\Leftrightarrow$ H is nonempty and $ab \in H, \forall a, b \in H$
  - Examples: $\mathbf{Z} \subseteq \mathbf{Q} \subseteq \mathbf{R} \subseteq \mathbf{C}$; $\mathbf{R}^+ \subseteq \mathbf{R}^\times$; $n\mathbf{Z} \subseteq \mathbf{Z}$; $\mathrm{SL}_n(\mathbf{R}) \subseteq \mathrm{GL}_n(\mathbf{R})$.
- Cyclic subgroup $\langle a \rangle$ is the **smallest** subgroup of G containing $a \in G$.
  For example, $\langle i \rangle \subseteq \mathbf{C}^\times; \langle 2i \rangle \subseteq \mathbf{C}^\times; \langle (123) \rangle \subseteq S_3; \langle (12) \rangle \subseteq S_3$.
- G is cyclic if $G = \langle a \rangle$.
  For example, $\mathbf{Z}; \mathbf{Z}_n; \mathbf{Z}_5^\times$. Not examples: $\mathbf{Z}_8^\times; S_3$.
- $o(a) = |\langle a \rangle|$. If $o(a) = n$ is finite, then $a^k = e \Leftrightarrow n|k$ for $k \in \mathbf{Z}$.
- Lagrange's Theorem: If $|G| = n < \infty$ and $H \subseteq G$, then $|H| \Big| n$.

Review

- Subgroup H: No worry about *associativity* $\begin{cases} \text{Closure} \\ \text{Identity} \\ \text{Inverses} \end{cases}$
  - **Corollary 7:** $\Leftrightarrow H$ is nonempty and $ab^{-1} \in H$ for all $a, b \in H$
  - **Corollary 8:** add "H is finite" $\Leftrightarrow H$ is nonempty and $ab \in H, \forall a, b \in H$
  - Examples: $\mathbf{Z} \subseteq \mathbf{Q} \subseteq \mathbf{R} \subseteq \mathbf{C}$; $\mathbf{R}^+ \subseteq \mathbf{R}^\times$; $n\mathbf{Z} \subseteq \mathbf{Z}$; $\mathrm{SL}_n(\mathbf{R}) \subseteq \mathrm{GL}_n(\mathbf{R})$.
- Cyclic subgroup $\langle a \rangle$ is the **smallest** subgroup of G containing $a \in G$.
  For example, $\langle i \rangle \subseteq \mathbf{C}^\times; \langle 2i \rangle \subseteq \mathbf{C}^\times; \langle (123) \rangle \subseteq S_3; \langle (12) \rangle \subseteq S_3$.
- G is cyclic if $G = \langle a \rangle$.
  For example, $\mathbf{Z}; \mathbf{Z}_n; \mathbf{Z}_5^\times$. Not examples: $\mathbf{Z}_8^\times; S_3$.
- $o(a) = |\langle a \rangle|$. If $o(a) = n$ is finite, then $a^k = e \Leftrightarrow n|k$ for $k \in \mathbf{Z}$.
- Lagrange's Theorem: If $|G| = n < \infty$ and $H \subseteq G$, then $|H| \big| n$.
  - **Corollary 20:** $o(a)|n$ for any $a \in G$.

Review

- Subgroup H: No worry about *associativity* $\begin{cases} \text{Closure} \\ \text{Identity} \\ \text{Inverses} \end{cases}$
  - **Corollary 7:** $\Leftrightarrow$ H is nonempty and $ab^{-1} \in H$ for all $a, b \in H$
  - **Corollary 8:** add "H is finite" $\Leftrightarrow$ H is nonempty and $ab \in H, \forall a, b \in H$
  - Examples: $\mathbf{Z} \subseteq \mathbf{Q} \subseteq \mathbf{R} \subseteq \mathbf{C}$; $\mathbf{R}^+ \subseteq \mathbf{R}^\times$; $n\mathbf{Z} \subseteq \mathbf{Z}$; $\mathrm{SL}_n(\mathbf{R}) \subseteq \mathrm{GL}_n(\mathbf{R})$.
- Cyclic subgroup $\langle a \rangle$ is the **smallest** subgroup of G containing $a \in G$.
  For example, $\langle i \rangle \subseteq \mathbf{C}^\times; \langle 2i \rangle \subseteq \mathbf{C}^\times; \langle (123) \rangle \subseteq S_3; \langle (12) \rangle \subseteq S_3$.
- G is cyclic if $G = \langle a \rangle$.
  For example, $\mathbf{Z}; \mathbf{Z}_n; \mathbf{Z}_5^\times$. Not examples: $\mathbf{Z}_8^\times; S_3$.
- $o(a) = |\langle a \rangle|$. If $o(a) = n$ is finite, then $a^k = e \Leftrightarrow n | k$ for $k \in \mathbf{Z}$.
- Lagrange's Theorem: If $|G| = n < \infty$ and $H \subseteq G$, then $|H| \big| n$.
  - **Corollary 20:** $o(a)|n$ for any $a \in G$. $\dashrightarrow$ Nice proof for Euler's thm.

Review

- Subgroup H: No worry about *associativity* $\begin{cases} \text{Closure} \\ \text{Identity} \\ \text{Inverses} \end{cases}$
  - **Corollary 7:** $\Leftrightarrow H$ is nonempty and $ab^{-1} \in H$ for all $a, b \in H$
  - **Corollary 8:** add "H is finite" $\Leftrightarrow H$ is nonempty and $ab \in H, \forall a, b \in H$
  - Examples: $\mathbf{Z} \subseteq \mathbf{Q} \subseteq \mathbf{R} \subseteq \mathbf{C}$; $\mathbf{R}^{+} \subseteq \mathbf{R}^{\times}$; $n\mathbf{Z} \subseteq \mathbf{Z}$; $\mathrm{SL}_n(\mathbf{R}) \subseteq \mathrm{GL}_n(\mathbf{R})$.
- Cyclic subgroup $\langle a \rangle$ is the **smallest** subgroup of G containing $a \in G$. For example, $\langle i \rangle \subseteq \mathbf{C}^{\times}; \langle 2i \rangle \subseteq \mathbf{C}^{\times}; \langle (123) \rangle \subseteq S_3; \langle (12) \rangle \subseteq S_3$.
- G is cyclic if $G = \langle a \rangle$. For example, $\mathbf{Z}; \mathbf{Z}_n; \mathbf{Z}_5^{\times}$. Not examples: $\mathbf{Z}_8^{\times}; S_3$.
- $o(a) = |\langle a \rangle|$. If $o(a) = n$ is finite, then $a^k = e \Leftrightarrow n | k$ for $k \in \mathbf{Z}$.
- Lagrange's Theorem: If $|G| = n < \infty$ and $H \subseteq G$, then $|H| \big| n$.
  - **Corollary 20:** $o(a) | n$ for any $a \in G$. $\dashrightarrow$ Nice proof for Euler's thm.
  - **Corollary 21:** Any group of prime order is cyclic (and so abelian).

$|G| = 4$

Any group of order 2, 3, or 5 must be cyclic. (Why?)

$|G| = 4$

Any group of order 2, 3, or 5 must be cyclic. (Why?)
Let $|G| = 4$ and $a \in G$ with $a \neq e$.

$|G| = 4$

Any group of order 2, 3, or 5 must be cyclic. (Why?)
Let $|G| = 4$ and $a \in G$ with $a \neq e$. Then $o(a) = 2$ or $o(a) = 4$. (Why?)

$|G| = 4$

Any group of order 2, 3, or 5 must be cyclic. (Why?)
Let $|G| = 4$ and $a \in G$ with $a \neq e$. Then $o(a) = 2$ or $o(a) = 4$. (Why?)

(a) If $o(a) = 4$, then $G = \langle a \rangle = \{e, a, a^2, a^3\}$.

$|G| = 4$

Any group of order 2, 3, or 5 must be cyclic. (Why?)

Let $|G| = 4$ and $a \in G$ with $a \neq e$. Then $o(a) = 2$ or $o(a) = 4$. (Why?)

(a) If $o(a) = 4$, then $G = \langle a \rangle = \{e, a, a^2, a^3\}$.

(b) If there is no element of order 4, then $o(a) = 2$ for all $a \neq e$.

$|G| = 4$

Any group of order 2, 3, or 5 must be cyclic. (Why?)

Let $|G| = 4$ and $a \in G$ with $a \neq e$. Then $o(a) = 2$ or $o(a) = 4$. (Why?)

(a) If $o(a) = 4$, then $G = \langle a \rangle = \{e, a, a^2, a^3\}$.

(b) If there is no element of order 4, then $o(a) = 2$ for all $a \neq e$. So in the multiplication table for G, e must occur down the main diagonal.

$|G| = 4$

Any group of order 2, 3, or 5 must be cyclic. (Why?)

Let $|G| = 4$ and $a \in G$ with $a \neq e$. Then $o(a) = 2$ or $o(a) = 4$. (Why?)

(a) If $o(a) = 4$, then $G = \langle a \rangle = \{e, a, a^2, a^3\}$.

(b) If there is no element of order 4, then $o(a) = 2$ for all $a \neq e$. So in the multiplication table for G, e must occur down the main diagonal.

Fact 1

Each element must occur exactly once in each row and column.

$|G| = 4$

Any group of order 2, 3, or 5 must be cyclic. (Why?)

Let $|G| = 4$ and $a \in G$ with $a \neq e$. Then $o(a) = 2$ or $o(a) = 4$. (Why?)

(a) If $o(a) = 4$, then $G = \langle a \rangle = \{e, a, a^2, a^3\}$.

(b) If there is no element of order 4, then $o(a) = 2$ for all $a \neq e$. So in the multiplication table for G, e must occur down the main diagonal.

Fact 1

Each element must occur exactly once in each row and column.

By Fact 1, there is only one possible pattern for the table. (eg. $\mathbf{Z}_8^\times$)

Table 3.3.1: Multiplication Tables for Groups of Order 4

	e	a	a^2	a^3
e	e	a	a^2	a^3
a	a	a^2	a^3	e
a^2	a^2	a^3	e	a
a^3	a^3	e	a	a^2

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

$|G| = 6$

We know of two basic examples of groups of order 6:

$|G| = 6$

We know of two basic examples of groups of order 6:

(1) $\mathbf{Z}_6$: cyclic group. Its multiplication table is easy. (Check it!)

$|G| = 6$

We know of two basic examples of groups of order 6:

(1) $\mathbf{Z}_6$: cyclic group. Its multiplication table is easy. (Check it!)

(2) S_3: nonabelian.

$|G| = 6$

We know of two basic examples of groups of order 6:

(1) $\mathbf{Z}_6$: cyclic group. Its multiplication table is easy. (Check it!)

(2) S_3: nonabelian. We have described it by explicitly listing the permutations that belong to it. Here we will give another description:

$|G| = 6$

We know of two basic examples of groups of order 6:

(1) $\mathbf{Z}_6$: cyclic group. Its multiplication table is easy. (Check it!)

(2) S_3: nonabelian. We have described it by explicitly listing the permutations that belong to it. Here we will give another description: Let $e = (1), a = (123)$ and $b = (12)$. $\Rightarrow a^2 = (132), a^3 = e, b^2 = e$.

$|G| = 6$

We know of two basic examples of groups of order 6:

(1) $\mathbf{Z}_6$: cyclic group. Its multiplication table is easy. (Check it!)

(2) S_3: nonabelian. We have described it by explicitly listing the permutations that belong to it. Here we will give another description: Let $e = (1), a = (123)$ and $b = (12)$. $\Rightarrow a^2 = (132), a^3 = e, b^2 = e$. Using the convention $a^0 = b^0 = e$, we can express each element of S_3 in a unique way in the form $a^i b^j$, for $i = 0, 1, 2$ and $j = 0, 1$.

$|G| = 6$

We know of two basic examples of groups of order 6:

(1) $\mathbf{Z}_6$: cyclic group. Its multiplication table is easy. (Check it!)

(2) S_3: nonabelian. We have described it by explicitly listing the permutations that belong to it. Here we will give another description: Let $e = (1), a = (123)$ and $b = (12)$. $\Rightarrow a^2 = (132), a^3 = e, b^2 = e$. Using the convention $a^0 = b^0 = e$, we can express each element of S_3 in a unique way in the form $a^i b^j$, for $i = 0, 1, 2$ and $j = 0, 1$. That is,

$$(1) = e,\ (123) = a,\ (132) = a^2,\ (12) = b,\ (13) = ab,\ (23) = a^2 b.$$

Question 1

$|G| = 6$

We know of two basic examples of groups of order 6:

(1) $\mathbf{Z}_6$: cyclic group. Its multiplication table is easy. (Check it!)

(2) S_3: nonabelian. We have described it by explicitly listing the permutations that belong to it. Here we will give another description: Let $e = (1), a = (123)$ and $b = (12)$. $\Rightarrow a^2 = (132), a^3 = e, b^2 = e$. Using the convention $a^0 = b^0 = e$, we can express each element of S_3 in a unique way in the form $a^i b^j$, for $i = 0, 1, 2$ and $j = 0, 1$. That is,

$$(1) = e,\ (123) = a,\ (132) = a^2,\ (12) = b,\ (13) = ab,\ (23) = a^2 b.$$

Question 1

Question: What is ba?

$|G| = 6$

We know of two basic examples of groups of order 6:

(1) $\mathbf{Z}_6$: cyclic group. Its multiplication table is easy. (Check it!)

(2) S_3: nonabelian. We have described it by explicitly listing the permutations that belong to it. Here we will give another description: Let $e = (1), a = (123)$ and $b = (12)$. $\Rightarrow a^2 = (132), a^3 = e, b^2 = e$. Using the convention $a^0 = b^0 = e$, we can express each element of S_3 in a unique way in the form $a^i b^j$, for $i = 0, 1, 2$ and $j = 0, 1$. That is,

$$(1) = e,\ (123) = a,\ (132) = a^2,\ (12) = b,\ (13) = ab,\ (23) = a^2 b.$$

Question 1

Question: What is ba? *A:* $ba = a^2 b$ *(Why?)*

$|G| = 6$

We know of two basic examples of groups of order 6:

(1) $\mathbf{Z}_6$: cyclic group. Its multiplication table is easy. (Check it!)

(2) S_3: nonabelian. We have described it by explicitly listing the permutations that belong to it. Here we will give another description: Let $e = (1), a = (123)$ and $b = (12)$. $\Rightarrow a^2 = (132), a^3 = e, b^2 = e$. Using the convention $a^0 = b^0 = e$, we can express each element of S_3 in a unique way in the form $a^i b^j$, for $i = 0, 1, 2$ and $j = 0, 1$. That is,

$$(1) = e,\ (123) = a,\ (132) = a^2,\ (12) = b,\ (13) = ab,\ (23) = a^2 b.$$

Question 1

Question: What is ba? *A:* $ba = a^2 b$ *(Why?)* $(12)(123) = (23)$

$|G| = 6$

We know of two basic examples of groups of order 6:

(1) $\mathbf{Z}_6$: cyclic group. Its multiplication table is easy. (Check it!)

(2) S_3: nonabelian. We have described it by explicitly listing the permutations that belong to it. Here we will give another description: Let $e = (1), a = (123)$ and $b = (12)$. $\Rightarrow a^2 = (132), a^3 = e, b^2 = e$. Using the convention $a^0 = b^0 = e$, we can express each element of S_3 in a unique way in the form $a^i b^j$, for $i = 0, 1, 2$ and $j = 0, 1$. That is,

$$(1) = e,\ (123) = a,\ (132) = a^2,\ (12) = b,\ (13) = ab,\ (23) = a^2 b.$$

Question 1

Question: What is ba? *A:* $ba = a^2 b$ *(Why?)* $(12)(123) = (23)$

$$S_3 = \{e, a, a^2, b, ab, a^2 b\}, \qquad \text{where } a^3 = e, b^2 = e, ba = a^2 b.$$

Question 2

$|G| = 6$

We know of two basic examples of groups of order 6:

(1) $\mathbf{Z}_6$: cyclic group. Its multiplication table is easy. (Check it!)

(2) S_3: nonabelian. We have described it by explicitly listing the permutations that belong to it. Here we will give another description: Let $e = (1), a = (123)$ and $b = (12)$. $\Rightarrow a^2 = (132), a^3 = e, b^2 = e$. Using the convention $a^0 = b^0 = e$, we can express each element of S_3 in a unique way in the form $a^i b^j$, for $i = 0, 1, 2$ and $j = 0, 1$. That is,

$$(1) = e,\ (123) = a,\ (132) = a^2,\ (12) = b,\ (13) = ab,\ (23) = a^2 b.$$

Question 1

Question: What is ba? *A:* $ba = a^2 b$ *(Why?)* $(12)(123) = (23)$

$$S_3 = \{e, a, a^2, b, ab, a^2 b\}, \qquad \text{where } a^3 = e, b^2 = e, ba = a^2 b.$$

Question 2

Question: What is ba^2*?*

$|G| = 6$

We know of two basic examples of groups of order 6:

(1) $\mathbf{Z}_6$: cyclic group. Its multiplication table is easy. (Check it!)

(2) S_3: nonabelian. We have described it by explicitly listing the permutations that belong to it. Here we will give another description: Let $e = (1), a = (123)$ and $b = (12)$. $\Rightarrow a^2 = (132), a^3 = e, b^2 = e$. Using the convention $a^0 = b^0 = e$, we can express each element of S_3 in a unique way in the form $a^i b^j$, for $i = 0, 1, 2$ and $j = 0, 1$. That is,

$$(1) = e,\ (123) = a,\ (132) = a^2,\ (12) = b,\ (13) = ab,\ (23) = a^2 b.$$

Question 1

Question: What is ba? *A:* $ba = a^2 b$ *(Why?)* $(12)(123) = (23)$

$$S_3 = \{e, a, a^2, b, ab, a^2 b\}, \qquad \text{where } a^3 = e, b^2 = e, ba = a^2 b.$$

Question 2

Question: What is ba^2*?* $ba^2 = (ba)a = (a^2 b)a = a^2(ba) = a^2(a^2 b) = ab$

$|G| = 6$

We know of two basic examples of groups of order 6:

(1) $\mathbf{Z}_6$: cyclic group. Its multiplication table is easy. (Check it!)

(2) S_3: nonabelian. We have described it by explicitly listing the permutations that belong to it. Here we will give another description: Let $e = (1), a = (123)$ and $b = (12)$. $\Rightarrow a^2 = (132), a^3 = e, b^2 = e$. Using the convention $a^0 = b^0 = e$, we can express each element of S_3 in a unique way in the form $a^i b^j$, for $i = 0, 1, 2$ and $j = 0, 1$. That is,

$$(1) = e,\ (123) = a,\ (132) = a^2,\ (12) = b,\ (13) = ab,\ (23) = a^2 b.$$

Question 1

Question: What is ba?   *A:* $ba = a^2 b$ *(Why?)* $(12)(123) = (23)$

$$S_3 = \{e, a, a^2, b, ab, a^2 b\}, \qquad \text{where } a^3 = e, b^2 = e, ba = a^2 b.$$

Question 2

Question: What is ba^2*?* $ba^2 = (ba)a = (a^2 b)a = a^2(ba) = a^2(a^2 b) = ab$

Find its multiplication table. (Check it!)

Multiplication Table for S_3

$$S_3 = \{e, a, a^2, b, ab, a^2b\}, \qquad \text{where } a^3 = e, b^2 = e, ba = a^2b.$$

We also calculated $ba^2 = (ba)a = (a^2b)a = a^2(ba) = a^2(a^2b) = ab$.

	e	a	a^2	b	ab	a^2b
e	e	a	a^2	b	ab	a^2b
a	a	a^2	e	ab	a^2b	b
a^2	a^2	e	a	a^2b	b	ab
b	b	a^2b	ab	e	a^2	a
ab	ab	b	a^2b	a	e	a^2
a^2b	a^2b	ab	b	a^2	a	e

Product of two subgroups

Product of two subgroups

Recall: *the intersection of subgroups of a group is again a subgroup*.

Product of two subgroups

Recall: *the intersection of subgroups of a group is again a subgroup*. If H and K are subgroups of a group G, then $H \cap K$ is the largest subgroup of G that is contained in both H and K.

Product of two subgroups

Recall: *the intersection of subgroups of a group is again a subgroup*.
If H and K are subgroups of a group G, then $H \cap K$ is the largest subgroup of G that is contained in both H and K. On the other hand, what is the smallest subgroup that contains both H and K?

Definition 2

Product of two subgroups

Recall: *the intersection of subgroups of a group is again a subgroup*. If H and K are subgroups of a group G, then $H \cap K$ is the largest subgroup of G that is contained in both H and K. On the other hand, what is the smallest subgroup that contains both H and K?

Definition 2

Let G be a group, and let S and T be subsets of G. Then

$$ST = \{x \in G \mid x = st \text{ for some } s \in S, t \in T\}.$$

Product of two subgroups

Recall: *the intersection of subgroups of a group is again a subgroup*. If H and K are subgroups of a group G, then $H \cap K$ is the largest subgroup of G that is contained in both H and K. On the other hand, what is the smallest subgroup that contains both H and K?

Definition 2

Let G be a group, and let S and T be subsets of G. Then

$$ST = \{x \in G \mid x = st \text{ for some } s \in S, t \in T\}.$$

If H and K are subgroups of G, then we call HK the **product** of H and K.

Question 3

Product of two subgroups

Recall: *the intersection of subgroups of a group is again a subgroup*. If H and K are subgroups of a group G, then $H \cap K$ is the largest subgroup of G that is contained in both H and K. On the other hand, what is the smallest subgroup that contains both H and K?

Definition 2

Let G be a group, and let S and T be subsets of G. Then

$$ST = \{x \in G \mid x = st \text{ for some } s \in S, t \in T\}.$$

If H and K are subgroups of G, then we call HK the **product** of H and K.

Question 3

Is the **product** *HK a subgroup?*

Product of two subgroups

Recall: *the intersection of subgroups of a group is again a subgroup*. If H and K are subgroups of a group G, then $H \cap K$ is the largest subgroup of G that is contained in both H and K. On the other hand, what is the smallest subgroup that contains both H and K?

Definition 2

Let G be a group, and let S and T be subsets of G. Then

$$ST = \{x \in G \mid x = st \text{ for some } s \in S, t \in T\}.$$

If H and K are subgroups of G, then we call HK the **product** of H and K.

Question 3

Is the **product** *HK a subgroup?* *A: NOT always.*

Product of two subgroups

Recall: *the intersection of subgroups of a group is again a subgroup*. If H and K are subgroups of a group G, then $H \cap K$ is the largest subgroup of G that is contained in both H and K. On the other hand, what is the smallest subgroup that contains both H and K?

Definition 2

Let G be a group, and let S and T be subsets of G. Then

$$ST = \{x \in G \mid x = st \text{ for some } s \in S, t \in T\}.$$

If H and K are subgroups of G, then we call HK the **product** of H and K.

Question 3

Is the **product** *HK a subgroup?   A: NOT always.   (When?)*

Product of two subgroups

Recall: *the intersection of subgroups of a group is again a subgroup*.
If H and K are subgroups of a group G, then $H \cap K$ is the largest subgroup of G that is contained in both H and K. On the other hand, what is the smallest subgroup that contains both H and K?

Definition 2

Let G be a group, and let S and T be subsets of G. Then

$$ST = \{x \in G \mid x = st \text{ for some } s \in S, t \in T\}.$$

If H and K are subgroups of G, then we call HK the **product** of H and K.

Question 3

Is the **product** *HK a subgroup? A: NOT always. (When?)*

If the operation of G is denoted additively, then we write $H + K$, and refer to the **sum** of H and K.

When the product HK is a subgroup?

Proposition 1

When the product HK is a subgroup?

Proposition 1

Let G be a group, and let H and K be subgroups of G. If $h^{-1}kh \in K$ for all $h \in H$ and $k \in K$, then HK is a subgroup of G

Proof.

When the product HK is a subgroup?

Proposition 1

Let G be a group, and let H and K be subgroups of G. If $h^{-1}kh \in K$ for all $h \in H$ and $k \in K$, then HK is a subgroup of G

Proof.

(i) Closure: Let $g_1, g_2 \in HK$. Then $g_1 = h_1 k_1$ and $g_2 = h_2 k_2$.

When the product HK is a subgroup?

Proposition 1

Let G be a group, and let H and K be subgroups of G. If $h^{-1}kh \in K$ for all $h \in H$ and $k \in K$, then HK is a subgroup of G

Proof.

(i) Closure: Let $g_1, g_2 \in HK$. Then $g_1 = h_1k_1$ and $g_2 = h_2k_2$.

$$g_1g_2 = (h_1k_1)(h_2k_2) = h_1(h_2h_2^{-1})k_1h_2k_2 = h_1h_2(h_2^{-1}k_1h_2)k_2 \overset{?}{\in} HK$$

We omit parentheses because of associativity.

When the product HK is a subgroup?

Proposition 1

Let G be a group, and let H and K be subgroups of G. If $h^{-1}kh \in K$ for all $h \in H$ and $k \in K$, then HK is a subgroup of G

Proof.

(i) Closure: Let $g_1, g_2 \in HK$. Then $g_1 = h_1 k_1$ and $g_2 = h_2 k_2$.

$$g_1 g_2 = (h_1 k_1)(h_2 k_2) = h_1 (h_2 h_2^{-1}) k_1 h_2 k_2 = h_1 h_2 (h_2^{-1} k_1 h_2) k_2 \overset{?}{\in} HK$$

We omit parentheses because of associativity.

(ii) Identity: $e = e \cdot e \in HK$. (Why?)

When the product HK is a subgroup?

Proposition 1

Let G be a group, and let H and K be subgroups of G. If $h^{-1}kh \in K$ for all $h \in H$ and $k \in K$, then HK is a subgroup of G

Proof.

(i) Closure: Let $g_1, g_2 \in HK$. Then $g_1 = h_1k_1$ and $g_2 = h_2k_2$.

$$g_1g_2 = (h_1k_1)(h_2k_2) = h_1(h_2h_2^{-1})k_1h_2k_2 = h_1h_2(h_2^{-1}k_1h_2)k_2 \overset{?}{\in} HK$$

We omit parentheses because of associativity.

(ii) Identity: $e = e \cdot e \in HK$. (Why?)

(iii) Inverses: If $g = hk$ for $h \in H$ and $k \in K$. Then

$$g^{-1} = k^{-1}h^{-1} = (h^{-1}h)k^{-1}h^{-1} = h^{-1}((h^{-1})^{-1}k^{-1}h^{-1}) \overset{?}{\in} HK$$

$\square$

When the product HK is a subgroup?

Proposition 1

Let G be a group, and let H and K be subgroups of G. If $h^{-1}kh \in K$ for all $h \in H$ and $k \in K$, then HK is a subgroup of G

Proof.

(i) Closure: Let $g_1, g_2 \in HK$. Then $g_1 = h_1k_1$ and $g_2 = h_2k_2$.

$$g_1g_2 = (h_1k_1)(h_2k_2) = h_1(h_2h_2^{-1})k_1h_2k_2 = h_1h_2(h_2^{-1}k_1h_2)k_2 \overset{?}{\in} HK$$

We omit parentheses because of associativity.

(ii) Identity: $e = e \cdot e \in HK$. (Why?)

(iii) Inverses: If $g = hk$ for $h \in H$ and $k \in K$. Then

$$g^{-1} = k^{-1}h^{-1} = (h^{-1}h)k^{-1}h^{-1} = h^{-1}((h^{-1})^{-1}k^{-1}h^{-1}) \overset{?}{\in} HK$$

$\square$

If G is abelian, then the product of any two subgroups is again a subgroup.

When the product HK is a subgroup?

Proposition 1

Let G be a group, and let H and K be subgroups of G. If $h^{-1}kh \in K$ for all $h \in H$ and $k \in K$, then HK is a subgroup of G

Proof.

(i) Closure: Let $g_1, g_2 \in HK$. Then $g_1 = h_1k_1$ and $g_2 = h_2k_2$.

$$g_1g_2 = (h_1k_1)(h_2k_2) = h_1(h_2h_2^{-1})k_1h_2k_2 = h_1h_2(h_2^{-1}k_1h_2)k_2 \overset{?}{\in} HK$$

We omit parentheses because of associativity.

(ii) Identity: $e = e \cdot e \in HK$. (Why?)

(iii) Inverses: If $g = hk$ for $h \in H$ and $k \in K$. Then

$$g^{-1} = k^{-1}h^{-1} = (h^{-1}h)k^{-1}h^{-1} = h^{-1}((h^{-1})^{-1}k^{-1}h^{-1}) \overset{?}{\in} HK$$

$\square$

If G is abelian, then the product of any two subgroups is again a subgroup.

If G is a finite group, then $|HK| = |H||K|/|H \cap K|$. (How to prove it?)

Proof of $|HK| = |H||K|/|H \cap K|$

Proof of $|HK| = |H||K|/|H \cap K|$

- $H \cap K$ is a subgroup of G. (Why?)

Proof of $|HK| = |H||K|/|H \cap K|$

- $H \cap K$ is a subgroup of G. (Why?)
- $H \cap K$ is a subgroup of H and a subgroup of K. (Why?)

Proof of $|HK| = |H||K|/|H \cap K|$

- $H \cap K$ is a subgroup of G. (Why?)
- $H \cap K$ is a subgroup of H and a subgroup of K. (Why?)
- For any element $t \in H \cap K$, if $hk \in HK$, then we can write
$$hk = (ht)(t^{-1}k) \in HK. \text{ (Why?)}$$

Proof of $|HK| = |H||K|/|H \cap K|$

- $H \cap K$ is a subgroup of G. (Why?)
- $H \cap K$ is a subgroup of H and a subgroup of K. (Why?)
- For any element $t \in H \cap K$, if $hk \in HK$, then we can write
$$hk = (ht)(t^{-1}k) \in HK. \text{ (Why?)}$$
This implies that every element in HK can be written in at least $|H \cap K|$ different ways.

Proof of $|HK| = |H||K|/|H \cap K|$

- $H \cap K$ is a subgroup of G. (Why?)
- $H \cap K$ is a subgroup of H and a subgroup of K. (Why?)
- For any element $t \in H \cap K$, if $hk \in HK$, then we can write

$$hk = (ht)(t^{-1}k) \in HK. \text{ (Why?)}$$

  This implies that every element in HK can be written in at least $|H \cap K|$ different ways.
- On the other hand, if $hk = h'k' \in HK$, then

$$h'^{-1}h = k'k^{-1} \in H \cap K. \text{ (Why?)}$$

Proof of $|HK| = |H||K|/|H \cap K|$

- $H \cap K$ is a subgroup of G. (Why?)
- $H \cap K$ is a subgroup of H and a subgroup of K. (Why?)
- For any element $t \in H \cap K$, if $hk \in HK$, then we can write
$$hk = (ht)(t^{-1}k) \in HK. \text{ (Why?)}$$
This implies that every element in HK can be written in at least $|H \cap K|$ different ways.
- On the other hand, if $hk = h'k' \in HK$, then
$$h'^{-1}h = k'k^{-1} \in H \cap K. \text{ (Why?)}$$
This means that there exists $t \in H \cap K$ such that $t = h'^{-1}h = k'k^{-1}$. So $h' = ht^{-1}$ and $k' = tk$, i.e., $h'k' = (ht^{-1})(tk)$ for some $t \in H \cap K$.

Proof of $|HK| = |H||K|/|H \cap K|$

- $H \cap K$ is a subgroup of G. (Why?)
- $H \cap K$ is a subgroup of H and a subgroup of K. (Why?)
- For any element $t \in H \cap K$, if $hk \in HK$, then we can write
$$hk = (ht)(t^{-1}k) \in HK. \text{ (Why?)}$$
This implies that every element in HK can be written in at least $|H \cap K|$ different ways.
- On the other hand, if $hk = h'k' \in HK$, then
$$h'^{-1}h = k'k^{-1} \in H \cap K. \text{ (Why?)}$$
This means that there exists $t \in H \cap K$ such that $t = h'^{-1}h = k'k^{-1}$. So $h' = ht^{-1}$ and $k' = tk$, i.e., $h'k' = (ht^{-1})(tk)$ for some $t \in H \cap K$.
- Thus, every element in HK can be written in exactly $|H \cap K|$ different ways.

Proof of $|HK| = |H||K|/|H \cap K|$

- $H \cap K$ is a subgroup of G. (Why?)
- $H \cap K$ is a subgroup of H and a subgroup of K. (Why?)
- For any element $t \in H \cap K$, if $hk \in HK$, then we can write
$$hk = (ht)(t^{-1}k) \in HK. \text{ (Why?)}$$
This implies that every element in HK can be written in at least $|H \cap K|$ different ways.
- On the other hand, if $hk = h'k' \in HK$, then
$$h'^{-1}h = k'k^{-1} \in H \cap K. \text{ (Why?)}$$
This means that there exists $t \in H \cap K$ such that $t = h'^{-1}h = k'k^{-1}$. So $h' = ht^{-1}$ and $k' = tk$, i.e., $h'k' = (ht^{-1})(tk)$ for some $t \in H \cap K$.
- Thus, every element in HK can be written in exactly $|H \cap K|$ different ways. Therefore,
$$|HK| = \frac{|H||K|}{|H \cap K|}.$$

Examples

Example 3

$G = \mathbf{Z}_{15}^{\times}, H = \{[1], [11]\}, K = \{[1], [4]\}$:

Examples

Example 3

$G = \mathbf{Z}_{15}^{\times}, H = \{[1],[11]\}, K = \{[1],[4]\}$: Then HK is a subgroup. (Why?)
[

Examples

Example 3

$G = \mathbf{Z}_{15}^{\times}, H = \{[1],[11]\}, K = \{[1],[4]\}$: Then HK is a subgroup. (Why?) [$\mathbf{Z}_{15}^{\times}$ is abelian] Computing all possible products in HK gives us

Examples

Example 3

$G = \mathbf{Z}_{15}^{\times}, H = \{[1], [11]\}, K = \{[1], [4]\}$: Then HK is a subgroup. (Why?) [$\mathbf{Z}_{15}^{\times}$ is abelian] Computing all possible products in HK gives us

$$[1][1] = [1], \qquad [1][4] = [4], \qquad [11][1] = [11], \qquad [11][4] = [14],$$

and so $HK = \{[1], [4], [11], [14]\}$ is a subgroup of order 4.

Example 3

$G = \mathbf{Z}_{15}^{\times}, H = \{[1],[11]\}, K = \{[1],[4]\}$: Then HK is a subgroup. (Why?) [$\mathbf{Z}_{15}^{\times}$ is abelian] Computing all possible products in HK gives us

$$[1][1] = [1], \qquad [1][4] = [4], \qquad [11][1] = [11], \qquad [11][4] = [14],$$

and so $HK = \{[1],[4],[11],[14]\}$ is a subgroup of order 4.
Let $L = \langle [7] \rangle = \{[1],[4],[7],[13]\}$. Listing all of the distinct products:

$$HL = \{[1],[2],[4],[7],[8],[11],[13],[14]\} = \mathbf{Z}_{15}^{\times}.$$

Example 4 ($a\mathbf{Z} + b\mathbf{Z} = (a,b)\mathbf{Z}$)

Examples

Example 3

$G = \mathbf{Z}_{15}^{\times}, H = \{[1],[11]\}, K = \{[1],[4]\}$: Then HK is a subgroup. (Why?) [$\mathbf{Z}_{15}^{\times}$ is abelian] Computing all possible products in HK gives us

$$[1][1] = [1], \qquad [1][4] = [4], \qquad [11][1] = [11], \qquad [11][4] = [14],$$

and so $HK = \{[1],[4],[11],[14]\}$ is a subgroup of order 4.
Let $L = \langle [7] \rangle = \{[1],[4],[7],[13]\}$. Listing all of the distinct products:

$$HL = \{[1],[2],[4],[7],[8],[11],[13],[14]\} = \mathbf{Z}_{15}^{\times}.$$

Example 4 ($a\mathbf{Z} + b\mathbf{Z} = (a,b)\mathbf{Z}$)

Let $h \in H = a\mathbf{Z}$ and $k \in K = b\mathbf{Z}$. Let $(a,b) = d$. Claim: $H + K = d\mathbf{Z}$.

Examples

Example 3

$G = \mathbf{Z}_{15}^{\times}, H = \{[1],[11]\}, K = \{[1],[4]\}$: Then HK is a subgroup. (Why?) [$\mathbf{Z}_{15}^{\times}$ is abelian] Computing all possible products in HK gives us

$$[1][1] = [1], \qquad [1][4] = [4], \qquad [11][1] = [11], \qquad [11][4] = [14],$$

and so $HK = \{[1],[4],[11],[14]\}$ is a subgroup of order 4.
Let $L = \langle[7]\rangle = \{[1],[4],[7],[13]\}$. Listing all of the distinct products:

$$HL = \{[1],[2],[4],[7],[8],[11],[13],[14]\} = \mathbf{Z}_{15}^{\times}.$$

Example 4 ($a\mathbf{Z} + b\mathbf{Z} = (a,b)\mathbf{Z}$)

Let $h \in H = a\mathbf{Z}$ and $k \in K = b\mathbf{Z}$. Let $(a,b) = d$. Claim: $H + K = d\mathbf{Z}$.

- $H + K \subseteq d\mathbf{Z}$: (Why?) [

Example 3

$G = \mathbf{Z}_{15}^{\times}, H = \{[1],[11]\}, K = \{[1],[4]\}$: Then HK is a subgroup. (Why?) [$\mathbf{Z}_{15}^{\times}$ is abelian] Computing all possible products in HK gives us

$$[1][1] = [1], \qquad [1][4] = [4], \qquad [11][1] = [11], \qquad [11][4] = [14],$$

and so $HK = \{[1],[4],[11],[14]\}$ is a subgroup of order 4.
Let $L = \langle [7] \rangle = \{[1],[4],[7],[13]\}$. Listing all of the distinct products:

$$HL = \{[1],[2],[4],[7],[8],[11],[13],[14]\} = \mathbf{Z}_{15}^{\times}.$$

Example 4 ($a\mathbf{Z} + b\mathbf{Z} = (a,b)\mathbf{Z}$)

Let $h \in H = a\mathbf{Z}$ and $k \in K = b\mathbf{Z}$. Let $(a,b) = d$. Claim: $H + K = d\mathbf{Z}$.

- $H + K \subseteq d\mathbf{Z}$: (Why?) [$h + k$ is a linear combination of a and b.]

Example 3

$G = \mathbf{Z}_{15}^{\times}, H = \{[1], [11]\}, K = \{[1], [4]\}$: Then HK is a subgroup. (Why?) [$\mathbf{Z}_{15}^{\times}$ is abelian] Computing all possible products in HK gives us

$$[1][1] = [1], \qquad [1][4] = [4], \qquad [11][1] = [11], \qquad [11][4] = [14],$$

and so $HK = \{[1], [4], [11], [14]\}$ is a subgroup of order 4.
Let $L = \langle [7] \rangle = \{[1], [4], [7], [13]\}$. Listing all of the distinct products:

$$HL = \{[1], [2], [4], [7], [8], [11], [13], [14]\} = \mathbf{Z}_{15}^{\times}.$$

Example 4 ($a\mathbf{Z} + b\mathbf{Z} = (a, b)\mathbf{Z}$)

Let $h \in H = a\mathbf{Z}$ and $k \in K = b\mathbf{Z}$. Let $(a, b) = d$. Claim: $H + K = d\mathbf{Z}$.

- $H + K \subseteq d\mathbf{Z}$: (Why?) [$h + k$ is a linear combination of a and b.]
- $d\mathbf{Z} \subseteq H + K$: (Why?) [

Examples

Example 3

$G = \mathbf{Z}_{15}^{\times}, H = \{[1],[11]\}, K = \{[1],[4]\}$: Then HK is a subgroup. (Why?) [$\mathbf{Z}_{15}^{\times}$ is abelian] Computing all possible products in HK gives us

$$[1][1] = [1], \qquad [1][4] = [4], \qquad [11][1] = [11], \qquad [11][4] = [14],$$

and so $HK = \{[1],[4],[11],[14]\}$ is a subgroup of order 4.
Let $L = \langle [7] \rangle = \{[1],[4],[7],[13]\}$. Listing all of the distinct products:

$$HL = \{[1],[2],[4],[7],[8],[11],[13],[14]\} = \mathbf{Z}_{15}^{\times}.$$

Example 4 ($a\mathbf{Z} + b\mathbf{Z} = (a,b)\mathbf{Z}$)

Let $h \in H = a\mathbf{Z}$ and $k \in K = b\mathbf{Z}$. Let $(a,b) = d$. Claim: $H + K = d\mathbf{Z}$.

- $H + K \subseteq d\mathbf{Z}$: (Why?) [$h + k$ is a linear combination of a and b.]
- $d\mathbf{Z} \subseteq H + K$: (Why?) [$d$ is a linear combination of a and b, so $d \in H + K$.

Examples

Example 3

$G = \mathbf{Z}_{15}^{\times}, H = \{[1],[11]\}, K = \{[1],[4]\}$: Then HK is a subgroup. (Why?) [$\mathbf{Z}_{15}^{\times}$ is abelian] Computing all possible products in HK gives us

$$[1][1] = [1], \qquad [1][4] = [4], \qquad [11][1] = [11], \qquad [11][4] = [14],$$

and so $HK = \{[1],[4],[11],[14]\}$ is a subgroup of order 4.
Let $L = \langle [7] \rangle = \{[1],[4],[7],[13]\}$. Listing all of the distinct products:

$$HL = \{[1],[2],[4],[7],[8],[11],[13],[14]\} = \mathbf{Z}_{15}^{\times}.$$

Example 4 ($a\mathbf{Z} + b\mathbf{Z} = (a,b)\mathbf{Z}$)

Let $h \in H = a\mathbf{Z}$ and $k \in K = b\mathbf{Z}$. Let $(a,b) = d$. Claim: $H + K = d\mathbf{Z}$.

- $H + K \subseteq d\mathbf{Z}$: (Why?) [$h + k$ is a linear combination of a and b.]
- $d\mathbf{Z} \subseteq H + K$: (Why?) [$d$ is a linear combination of a and b, so $d \in H + K$. It implies that $d\mathbf{Z} \subseteq H + K$.

Example 3

$G = \mathbf{Z}_{15}^{\times}, H = \{[1], [11]\}, K = \{[1], [4]\}$: Then HK is a subgroup. (Why?) [$\mathbf{Z}_{15}^{\times}$ is abelian] Computing all possible products in HK gives us

$$[1][1] = [1], \qquad [1][4] = [4], \qquad [11][1] = [11], \qquad [11][4] = [14],$$

and so $HK = \{[1], [4], [11], [14]\}$ is a subgroup of order 4.
Let $L = \langle [7] \rangle = \{[1], [4], [7], [13]\}$. Listing all of the distinct products:

$$HL = \{[1], [2], [4], [7], [8], [11], [13], [14]\} = \mathbf{Z}_{15}^{\times}.$$

Example 4 ($a\mathbf{Z} + b\mathbf{Z} = (a, b)\mathbf{Z}$)

Let $h \in H = a\mathbf{Z}$ and $k \in K = b\mathbf{Z}$. Let $(a, b) = d$. Claim: $H + K = d\mathbf{Z}$.

- $H + K \subseteq d\mathbf{Z}$: (Why?) [$h + k$ is a linear combination of a and b.]
- $d\mathbf{Z} \subseteq H + K$: (Why?) [$d$ is a linear combination of a and b, so $d \in H + K$. It implies that $d\mathbf{Z} \subseteq H + K$. (Proposition 2 in §3.2 (b))]

Direct product

Definition 5

Direct product

Definition 5

Let G_1 and G_2 be groups. The set of all ordered pairs (x_1, x_2) such that $x_1 \in G_1$ and $x_2 \in G_2$ is called the **direct product** of G_1 and G_2, denoted by $G_1 \times G_2$. That is,

$$G_1 \times G_2 = \{(x_1, x_2) \mid x_1 \in G_1 \text{ and } x_2 \in G_2\}$$

Proposition 2 (Let $(G_1, *)$ and $(G_2, \cdot)$ be groups.)

Direct product

Definition 5

Let G_1 and G_2 be groups. The set of all ordered pairs (x_1, x_2) such that $x_1 \in G_1$ and $x_2 \in G_2$ is called the **direct product** of G_1 and G_2, denoted by $G_1 \times G_2$. That is,

$$G_1 \times G_2 = \{(x_1, x_2) \mid x_1 \in G_1 \text{ and } x_2 \in G_2\}$$

Proposition 2 (Let $(G_1, *)$ and $(G_2, \cdot)$ be groups.)

(a) *The direct product $G_1 \times G_2$ is a group under the operation defined for all $(a_1, a_2), (b_1, b_2) \in G_1 \times G_2$ by*

$$(a_1, a_2)(b_1, b_2) = (a_1 * b_1, a_2 \cdot b_2).$$

Direct product

Definition 5

Let G_1 and G_2 be groups. The set of all ordered pairs (x_1, x_2) such that $x_1 \in G_1$ and $x_2 \in G_2$ is called the **direct product** of G_1 and G_2, denoted by $G_1 \times G_2$. That is,

$$G_1 \times G_2 = \{(x_1, x_2) \mid x_1 \in G_1 \text{ and } x_2 \in G_2\}$$

Proposition 2 (Let $(G_1, *)$ and $(G_2, \cdot)$ be groups.)

(a) *The direct product $G_1 \times G_2$ is a group under the operation defined for all $(a_1, a_2), (b_1, b_2) \in G_1 \times G_2$ by*

$$(a_1, a_2)(b_1, b_2) = (a_1 * b_1, a_2 \cdot b_2).$$

(b) *If $a_1 \in G_1$ and $a_2 \in G_2$ have orders n and m, respectively, then in $G_1 \times G_2$ the element (a_1, a_2) has order $\mathrm{lcm}[n, m]$.*

Remark 1

Direct product

Definition 5

Let G_1 and G_2 be groups. The set of all ordered pairs (x_1, x_2) such that $x_1 \in G_1$ and $x_2 \in G_2$ is called the **direct product** of G_1 and G_2, denoted by $G_1 \times G_2$. That is,

$$G_1 \times G_2 = \{(x_1, x_2) \mid x_1 \in G_1 \text{ and } x_2 \in G_2\}$$

Proposition 2 (Let $(G_1, *)$ and $(G_2, \cdot)$ be groups.)

(a) *The direct product $G_1 \times G_2$ is a group under the operation defined for all $(a_1, a_2), (b_1, b_2) \in G_1 \times G_2$ by*

$$(a_1, a_2)(b_1, b_2) = (a_1 * b_1, a_2 \cdot b_2).$$

(b) *If $a_1 \in G_1$ and $a_2 \in G_2$ have orders n and m, respectively, then in $G_1 \times G_2$ the element (a_1, a_2) has order $\mathrm{lcm}[n, m]$.*

Remark 1

If G_1, G_2 are finite groups, then $|G_1 \times G_2| = |G_1| \cdot |G_2|$.

Proof of Proposition 2

Proof of Proposition 2

(a) (i) Closure: The given operation defines a binary operation. (Check it!)

Proof of Proposition 2

(a) (i) Closure: The given operation defines a binary operation. (Check it!)
(ii) Associativity:

Proof of Proposition 2

(a) (i) Closure: The given operation defines a binary operation. (Check it!)

(ii) Associativity: For all $(a_1, a_2), (b_1, b_2), (c_1, c_2) \in G_1 \times G_2$ we have

$$\begin{aligned}
(a_1, a_2)((b_1, b_2)(c_1, c_2)) &= (a_1, a_2)(b_1 * c_1, b_2 \cdot c_2) \\
&= (a_1 * (b_1 * c_1), a_2 \cdot (b_2 \cdot c_2)) \\
&= ((a_1 * b_1) * c_1, (a_2 \cdot b_2) \cdot c_2) \\
&= (a_1 * b_1, a_2 \cdot b_2)(c_1, c_2) \\
&= ((a_1, a_2)(b_1, b_2))(c_1, c_2)
\end{aligned}$$

(iii) Identity:

Proof of Proposition 2

(a) (i) Closure: The given operation defines a binary operation. (Check it!)

(ii) Associativity: For all $(a_1, a_2), (b_1, b_2), (c_1, c_2) \in G_1 \times G_2$ we have

$$\begin{aligned}
(a_1, a_2)((b_1, b_2)(c_1, c_2)) &= (a_1, a_2)(b_1 * c_1, b_2 \cdot c_2) \\
&= (a_1 * (b_1 * c_1), a_2 \cdot (b_2 \cdot c_2)) \\
&= ((a_1 * b_1) * c_1, (a_2 \cdot b_2) \cdot c_2) \\
&= (a_1 * b_1, a_2 \cdot b_2)(c_1, c_2) \\
&= ((a_1, a_2)(b_1, b_2))(c_1, c_2)
\end{aligned}$$

(iii) Identity: (e_1, e_2), where e_i is the identity elements in $G_i, i = 1, 2$.

Proof of Proposition 2

(a) (i) Closure: The given operation defines a binary operation. (Check it!)

(ii) Associativity: For all $(a_1, a_2), (b_1, b_2), (c_1, c_2) \in G_1 \times G_2$ we have

$$\begin{aligned}(a_1, a_2)((b_1, b_2)(c_1, c_2)) =& (a_1, a_2)(b_1 * c_1, b_2 \cdot c_2) \\ =& (a_1 * (b_1 * c_1), a_2 \cdot (b_2 \cdot c_2)) \\ =& ((a_1 * b_1) * c_1, (a_2 \cdot b_2) \cdot c_2) \\ =& (a_1 * b_1, a_2 \cdot b_2)(c_1, c_2) \\ =& ((a_1, a_2)(b_1, b_2))(c_1, c_2)\end{aligned}$$

(iii) Identity: (e_1, e_2), where e_i is the identity elements in $G_i, i = 1, 2$.

(iv) Inverses: $(a_1, a_2)^{-1} = (a_1^{-1}, a_2^{-1})$. (Check it!)

Proof of Proposition 2

(a) (i) Closure: The given operation defines a binary operation. (Check it!)

(ii) Associativity: For all $(a_1, a_2), (b_1, b_2), (c_1, c_2) \in G_1 \times G_2$ we have

$$\begin{aligned}(a_1, a_2)((b_1, b_2)(c_1, c_2)) =&(a_1, a_2)(b_1 * c_1, b_2 \cdot c_2)\\ =&(a_1 * (b_1 * c_1), a_2 \cdot (b_2 \cdot c_2))\\ =&((a_1 * b_1) * c_1, (a_2 \cdot b_2) \cdot c_2)\\ =&(a_1 * b_1, a_2 \cdot b_2)(c_1, c_2)\\ =&((a_1, a_2)(b_1, b_2))(c_1, c_2)\end{aligned}$$

(iii) Identity: (e_1, e_2), where e_i is the identity elements in $G_i, i = 1, 2$.

(iv) Inverses: $(a_1, a_2)^{-1} = (a_1^{-1}, a_2^{-1})$. (Check it!)

(b) Let $o(a_1) = n, o(a_2) = m$. In $G_1 \times G_2$, $o((a_1, a_2))$ is the smallest positive power k s.t. $(a_1, a_2)^k = (e_1, e_2)$. *To show*: $k = \mathrm{lcm}[n, m]$.

Proof of Proposition 2

(a) (i) Closure: The given operation defines a binary operation. (Check it!)

(ii) Associativity: For all $(a_1, a_2), (b_1, b_2), (c_1, c_2) \in G_1 \times G_2$ we have

$$\begin{aligned}(a_1, a_2)((b_1, b_2)(c_1, c_2)) &= (a_1, a_2)(b_1 * c_1, b_2 \cdot c_2)\\ &= (a_1 * (b_1 * c_1), a_2 \cdot (b_2 \cdot c_2))\\ &= ((a_1 * b_1) * c_1, (a_2 \cdot b_2) \cdot c_2)\\ &= (a_1 * b_1, a_2 \cdot b_2)(c_1, c_2)\\ &= ((a_1, a_2)(b_1, b_2))(c_1, c_2)\end{aligned}$$

(iii) Identity: (e_1, e_2), where e_i is the identity elements in $G_i, i = 1, 2$.

(iv) Inverses: $(a_1, a_2)^{-1} = (a_1^{-1}, a_2^{-1})$. (Check it!)

(b) Let $o(a_1) = n, o(a_2) = m$. In $G_1 \times G_2$, $o((a_1, a_2))$ is the smallest positive power k s.t. $(a_1, a_2)^k = (e_1, e_2)$. *To show*: $k = \mathrm{lcm}[n, m]$.

$(a_1, a_2)^k = (a_1^k, a_2^k) = (e_1, e_2) \Rightarrow a_1^k = e_1, a_2^k = e_2 \Rightarrow n|k, m|k$.(*Why?*)

Proof of Proposition 2

(a) (i) Closure: The given operation defines a binary operation. (Check it!)
(ii) Associativity: For all $(a_1, a_2), (b_1, b_2), (c_1, c_2) \in G_1 \times G_2$ we have

$$\begin{aligned}(a_1, a_2)((b_1, b_2)(c_1, c_2)) =&(a_1, a_2)(b_1 * c_1, b_2 \cdot c_2)\\ =&(a_1 * (b_1 * c_1), a_2 \cdot (b_2 \cdot c_2))\\ =&((a_1 * b_1) * c_1, (a_2 \cdot b_2) \cdot c_2)\\ =&(a_1 * b_1, a_2 \cdot b_2)(c_1, c_2)\\ =&((a_1, a_2)(b_1, b_2))(c_1, c_2)\end{aligned}$$

(iii) Identity: (e_1, e_2), where e_i is the identity elements in $G_i, i = 1, 2$.
(iv) Inverses: $(a_1, a_2)^{-1} = (a_1^{-1}, a_2^{-1})$. (Check it!)

(b) Let $o(a_1) = n, o(a_2) = m$. In $G_1 \times G_2$, $o((a_1, a_2))$ is the smallest positive power k s.t. $(a_1, a_2)^k = (e_1, e_2)$. *To show*: $k = \mathrm{lcm}[n, m]$.

$(a_1, a_2)^k = (a_1^k, a_2^k) = (e_1, e_2) \Rightarrow a_1^k = e_1, a_2^k = e_2 \Rightarrow n|k, m|k$.(*Why?*)

k is the smallest positive integer s.t. $n|k$ and $m|k$,

Proof of Proposition 2

(a) (i) Closure: The given operation defines a binary operation. (Check it!)

(ii) Associativity: For all $(a_1, a_2), (b_1, b_2), (c_1, c_2) \in G_1 \times G_2$ we have

$$\begin{aligned}
(a_1, a_2)((b_1, b_2)(c_1, c_2)) &= (a_1, a_2)(b_1 * c_1, b_2 \cdot c_2) \\
&= (a_1 * (b_1 * c_1), a_2 \cdot (b_2 \cdot c_2)) \\
&= ((a_1 * b_1) * c_1, (a_2 \cdot b_2) \cdot c_2) \\
&= (a_1 * b_1, a_2 \cdot b_2)(c_1, c_2) \\
&= ((a_1, a_2)(b_1, b_2))(c_1, c_2)
\end{aligned}$$

(iii) Identity: (e_1, e_2), where e_i is the identity elements in $G_i, i = 1, 2$.

(iv) Inverses: $(a_1, a_2)^{-1} = (a_1^{-1}, a_2^{-1})$. (Check it!)

(b) Let $o(a_1) = n, o(a_2) = m$. In $G_1 \times G_2$, $o((a_1, a_2))$ is the smallest positive power k s.t. $(a_1, a_2)^k = (e_1, e_2)$. *To show*: $k = \mathrm{lcm}[n, m]$.

$(a_1, a_2)^k = (a_1^k, a_2^k) = (e_1, e_2) \Rightarrow a_1^k = e_1, a_2^k = e_2 \Rightarrow n|k, m|k$.(*Why?*)

k is the smallest positive integer s.t. $n|k$ and $m|k$, so $k = \mathrm{lcm}[n, m]$.

Example: Klein four-group

We give the addition table for $\mathbf{Z}_2 \times \mathbf{Z}_2 = \{([0],[0]),([1],[0]),([0],[1]),([1],[1])\}$:

Example: Klein four-group

We give the addition table for $\mathbf{Z}_2 \times \mathbf{Z}_2 = \{([0],[0]),([1],[0]),([0],[1]),([1],[1])\}$:

	$([0],[0])$	$([1],[0])$	$([0],[1])$	$([1],[1])$
$([0],[0])$	$([0],[0])$	$([1],[0])$	$([0],[1])$	$([1],[1])$
$([1],[0])$	$([1],[0])$	$([0],[0])$	$([1],[1])$	$([0],[1])$
$([0],[1])$	$([0],[1])$	$([1],[1])$	$([0],[0])$	$([1],[0])$
$([1],[1])$	$([1],[1])$	$([0],[1])$	$([1],[0])$	$([0],[0])$

Example: Klein four-group

We give the addition table for $\mathbf{Z}_2 \times \mathbf{Z}_2 = \{([0],[0]),([1],[0]),([0],[1]),([1],[1])\}$:

	$([0],[0])$	$([1],[0])$	$([0],[1])$	$([1],[1])$
$([0],[0])$	$([0],[0])$	$([1],[0])$	$([0],[1])$	$([1],[1])$
$([1],[0])$	$([1],[0])$	$([0],[0])$	$([1],[1])$	$([0],[1])$
$([0],[1])$	$([0],[1])$	$([1],[1])$	$([0],[0])$	$([1],[0])$
$([1],[1])$	$([1],[1])$	$([0],[1])$	$([1],[0])$	$([0],[0])$

This group is usually called the **Klein four-group**.

Example: Klein four-group

We give the addition table for $\mathbf{Z}_2 \times \mathbf{Z}_2 = \{([0],[0]),([1],[0]),([0],[1]),([1],[1])\}$:

	$([0],[0])$	$([1],[0])$	$([0],[1])$	$([1],[1])$
$([0],[0])$	$([0],[0])$	$([1],[0])$	$([0],[1])$	$([1],[1])$
$([1],[0])$	$([1],[0])$	$([0],[0])$	$([1],[1])$	$([0],[1])$
$([0],[1])$	$([0],[1])$	$([1],[1])$	$([0],[0])$	$([1],[0])$
$([1],[1])$	$([1],[1])$	$([0],[1])$	$([1],[0])$	$([0],[0])$

This group is usually called the **Klein four-group**.

The pattern in this table is the same as the table below.

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

Example: Klein four-group

We give the addition table for $\mathbf{Z}_2 \times \mathbf{Z}_2 = \{([0],[0]),([1],[0]),([0],[1]),([1],[1])\}$:

	$([0],[0])$	$([1],[0])$	$([0],[1])$	$([1],[1])$
$([0],[0])$	$([0],[0])$	$([1],[0])$	$([0],[1])$	$([1],[1])$
$([1],[0])$	$([1],[0])$	$([0],[0])$	$([1],[1])$	$([0],[1])$
$([0],[1])$	$([0],[1])$	$([1],[1])$	$([0],[0])$	$([1],[0])$
$([1],[1])$	$([1],[1])$	$([0],[1])$	$([1],[0])$	$([0],[0])$

This group is usually called the **Klein four-group**.

The pattern in this table is the same as the table below.

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

This group is characterized by the fact that it has order 4 and each element except the identity has order 2.

More Examples

Example 6

In the group $\mathbf{Z} \times \mathbf{Z}$,

More Examples

Example 6

In the group $\mathbf{Z} \times \mathbf{Z}$, the subgroup generated by an element (m, n) consists of all multiples $k(m, n)$.

More Examples

Example 6

In the group $\mathbf{Z} \times \mathbf{Z}$, the subgroup generated by an element (m, n) consists of all multiples $k(m, n)$.
This subgroup cannot contain both of $(1, 0)$ and $(0, 1)$. (Check it!)

More Examples

Example 6

In the group $\mathbf{Z} \times \mathbf{Z}$, the subgroup generated by an element (m, n) consists of all multiples $k(m, n)$.
This subgroup cannot contain both of $(1, 0)$ and $(0, 1)$. (Check it!)
So no single element generates $\mathbf{Z} \times \mathbf{Z}$.

More Examples

Example 6

In the group $\mathbf{Z} \times \mathbf{Z}$, the subgroup generated by an element (m, n) consists of all multiples $k(m, n)$.
This subgroup cannot contain both of $(1, 0)$ and $(0, 1)$. (Check it!)
So no single element generates $\mathbf{Z} \times \mathbf{Z}$. Thus, it is not cyclic.

More Examples

Example 6

In the group $\mathbf{Z} \times \mathbf{Z}$, the subgroup generated by an element (m, n) consists of all multiples $k(m, n)$.
This subgroup cannot contain both of $(1, 0)$ and $(0, 1)$. (Check it!)
So no single element generates $\mathbf{Z} \times \mathbf{Z}$. Thus, it is not cyclic.
Natural subgroups: $\langle(1, 0)\rangle$ and $\langle(0, 1)\rangle$.

More Examples

Example 6

In the group $\mathbf{Z} \times \mathbf{Z}$, the subgroup generated by an element (m, n) consists of all multiples $k(m, n)$.
This subgroup cannot contain both of $(1, 0)$ and $(0, 1)$. (Check it!)
So no single element generates $\mathbf{Z} \times \mathbf{Z}$. Thus, it is not cyclic.
Natural subgroups: $\langle(1, 0)\rangle$ and $\langle(0, 1)\rangle$. The "diagonal" subgroup $\langle(1, 1)\rangle$.

Example 7

More Examples

Example 6

In the group $\mathbf{Z} \times \mathbf{Z}$, the subgroup generated by an element (m, n) consists of all multiples $k(m, n)$.
This subgroup cannot contain both of $(1, 0)$ and $(0, 1)$. (Check it!)
So no single element generates $\mathbf{Z} \times \mathbf{Z}$. Thus, it is not cyclic.
Natural subgroups: $\langle(1, 0)\rangle$ and $\langle(0, 1)\rangle$. The "diagonal" subgroup $\langle(1, 1)\rangle$.

Example 7

$\mathbf{Z}_2 \times \mathbf{Z}_3$ is cyclic. (Why?) [

More Examples

Example 6

In the group $\mathbf{Z} \times \mathbf{Z}$, the subgroup generated by an element (m, n) consists of all multiples $k(m, n)$.
This subgroup cannot contain both of $(1, 0)$ and $(0, 1)$. (Check it!)
So no single element generates $\mathbf{Z} \times \mathbf{Z}$. Thus, it is not cyclic.
Natural subgroups: $\langle(1, 0)\rangle$ and $\langle(0, 1)\rangle$. The "diagonal" subgroup $\langle(1, 1)\rangle$.

Example 7

$\mathbf{Z}_2 \times \mathbf{Z}_3$ is cyclic. (Why?) [$(1, 1)$ has order 6 (Why?)order$= \mathrm{lcm}[2, 3] = 6$]

More Examples

Example 6

In the group $\mathbf{Z} \times \mathbf{Z}$, the subgroup generated by an element (m, n) consists of all multiples $k(m, n)$.
This subgroup cannot contain both of $(1, 0)$ and $(0, 1)$. (Check it!)
So no single element generates $\mathbf{Z} \times \mathbf{Z}$. Thus, it is not cyclic.
Natural subgroups: $\langle(1, 0)\rangle$ and $\langle(0, 1)\rangle$. The "diagonal" subgroup $\langle(1, 1)\rangle$.

Example 7

$\mathbf{Z}_2 \times \mathbf{Z}_3$ is cyclic. (Why?) [(1, 1) has order 6 (Why?)order$= \mathrm{lcm}[2, 3] = 6$]
$\mathbf{Z}_2 \times \mathbf{Z}_4$ is not cyclic. (Why?) [

More Examples

Example 6

In the group $\mathbf{Z} \times \mathbf{Z}$, the subgroup generated by an element (m, n) consists of all multiples $k(m, n)$.
This subgroup cannot contain both of $(1, 0)$ and $(0, 1)$. (Check it!)
So no single element generates $\mathbf{Z} \times \mathbf{Z}$. Thus, it is not cyclic.
Natural subgroups: $\langle(1, 0)\rangle$ and $\langle(0, 1)\rangle$. The "diagonal" subgroup $\langle(1, 1)\rangle$.

Example 7

$\mathbf{Z}_2 \times \mathbf{Z}_3$ is cyclic. (Why?) [$(1, 1)$ has order 6 (Why?)order$= \mathrm{lcm}[2, 3] = 6$]
$\mathbf{Z}_2 \times \mathbf{Z}_4$ is not cyclic. (Why?) [Note that $|\mathbf{Z}_2 \times \mathbf{Z}_4| = 2 \cdot 4 = 8$]

More Examples

Example 6

In the group $\mathbf{Z} \times \mathbf{Z}$, the subgroup generated by an element (m, n) consists of all multiples $k(m, n)$.
This subgroup cannot contain both of $(1, 0)$ and $(0, 1)$. (Check it!)
So no single element generates $\mathbf{Z} \times \mathbf{Z}$. Thus, it is not cyclic.
Natural subgroups: $\langle(1, 0)\rangle$ and $\langle(0, 1)\rangle$. The "diagonal" subgroup $\langle(1, 1)\rangle$.

Example 7

$\mathbf{Z}_2 \times \mathbf{Z}_3$ is cyclic. (Why?) [$(1, 1)$ has order 6 (Why?)order$= \mathrm{lcm}[2, 3] = 6$]
$\mathbf{Z}_2 \times \mathbf{Z}_4$ is not cyclic. (Why?) [Note that $|\mathbf{Z}_2 \times \mathbf{Z}_4| = 2 \cdot 4 = 8$]
In the first component the possible orders are 1 and 2.

More Examples

Example 6

In the group $\mathbf{Z} \times \mathbf{Z}$, the subgroup generated by an element (m, n) consists of all multiples $k(m, n)$.
This subgroup cannot contain both of $(1, 0)$ and $(0, 1)$. (Check it!)
So no single element generates $\mathbf{Z} \times \mathbf{Z}$. Thus, it is not cyclic.
Natural subgroups: $\langle(1, 0)\rangle$ and $\langle(0, 1)\rangle$. The "diagonal" subgroup $\langle(1, 1)\rangle$.

Example 7

$\mathbf{Z}_2 \times \mathbf{Z}_3$ is cyclic. (Why?) [$(1, 1)$ has order 6 (Why?)order$= \mathrm{lcm}[2, 3] = 6$]
$\mathbf{Z}_2 \times \mathbf{Z}_4$ is not cyclic. (Why?) [Note that $|\mathbf{Z}_2 \times \mathbf{Z}_4| = 2 \cdot 4 = 8$]
In the first component the possible orders are 1 and 2.
In the second component the possible orders are $1, 2,$ and 4.

More Examples

Example 6

In the group $\mathbf{Z} \times \mathbf{Z}$, the subgroup generated by an element (m, n) consists of all multiples $k(m, n)$.
This subgroup cannot contain both of $(1, 0)$ and $(0, 1)$. (Check it!)
So no single element generates $\mathbf{Z} \times \mathbf{Z}$. Thus, it is not cyclic.
Natural subgroups: $\langle(1, 0)\rangle$ and $\langle(0, 1)\rangle$. The "diagonal" subgroup $\langle(1, 1)\rangle$.

Example 7

$\mathbf{Z}_2 \times \mathbf{Z}_3$ is cyclic. (Why?) [$(1, 1)$ has order 6 (Why?)order$= \mathrm{lcm}[2, 3] = 6$]
$\mathbf{Z}_2 \times \mathbf{Z}_4$ is not cyclic. (Why?) [Note that $|\mathbf{Z}_2 \times \mathbf{Z}_4| = 2 \cdot 4 = 8$]
In the first component the possible orders are 1 and 2.
In the second component the possible orders are $1, 2,$ and 4.
The largest possible least common multiple we can have is 4,

More Examples

Example 6

In the group $\mathbf{Z} \times \mathbf{Z}$, the subgroup generated by an element (m, n) consists of all multiples $k(m, n)$.
This subgroup cannot contain both of $(1, 0)$ and $(0, 1)$. (Check it!)
So no single element generates $\mathbf{Z} \times \mathbf{Z}$. Thus, it is not cyclic.
Natural subgroups: $\langle(1, 0)\rangle$ and $\langle(0, 1)\rangle$. The "diagonal" subgroup $\langle(1, 1)\rangle$.

Example 7

$\mathbf{Z}_2 \times \mathbf{Z}_3$ is cyclic. (Why?) [$(1, 1)$ has order 6 (Why?)order$= \mathrm{lcm}[2, 3] = 6$]
$\mathbf{Z}_2 \times \mathbf{Z}_4$ is not cyclic. (Why?) [Note that $|\mathbf{Z}_2 \times \mathbf{Z}_4| = 2 \cdot 4 = 8$]
In the first component the possible orders are 1 and 2.
In the second component the possible orders are $1, 2,$ and 4.
The largest possible least common multiple we can have is 4, so there is no element of order 8 and the group is not cyclic.

Proposition 3

More Examples

Example 6

In the group $\mathbf{Z} \times \mathbf{Z}$, the subgroup generated by an element (m, n) consists of all multiples $k(m, n)$.
This subgroup cannot contain both of $(1, 0)$ and $(0, 1)$. (Check it!)
So no single element generates $\mathbf{Z} \times \mathbf{Z}$. Thus, it is not cyclic.
Natural subgroups: $\langle(1, 0)\rangle$ and $\langle(0, 1)\rangle$. The "diagonal" subgroup $\langle(1, 1)\rangle$.

Example 7

$\mathbf{Z}_2 \times \mathbf{Z}_3$ is cyclic. (Why?) [$(1, 1)$ has order 6 (Why?)order$= \mathrm{lcm}[2, 3] = 6$]
$\mathbf{Z}_2 \times \mathbf{Z}_4$ is not cyclic. (Why?) [Note that $|\mathbf{Z}_2 \times \mathbf{Z}_4| = 2 \cdot 4 = 8$]
In the first component the possible orders are 1 and 2.
In the second component the possible orders are $1, 2,$ and 4.
The largest possible least common multiple we can have is 4, so there is no element of order 8 and the group is not cyclic.

Proposition 3

$\mathbf{Z}_n \times \mathbf{Z}_m$ is cyclic if and only if $\gcd(n, m) = 1$.

Proof of Proposition 3: $\mathbf{Z}_n \times \mathbf{Z}_m$ is cyclic $\Leftrightarrow (n, m) = 1$.

Recall: A finite group G is cyclic if and only if $o(x) = |G|$ for some $x \in G$.
$\Rightarrow$: Assume $\mathbf{Z}_n \times \mathbf{Z}_m$ is cyclic, we need *to show* $(n, m) = 1$.

Proof of Proposition 3: $\mathbf{Z}_n \times \mathbf{Z}_m$ is cyclic $\Leftrightarrow (n, m) = 1$.

Recall: A finite group G is cyclic if and only if $o(x) = |G|$ for some $x \in G$.
$\Rightarrow$: Assume $\mathbf{Z}_n \times \mathbf{Z}_m$ is cyclic, we need *to show* $(n, m) = 1$. There is an element $(a, b) \in \mathbf{Z}_n \times \mathbf{Z}_m$ with $o((a, b)) = nm$ since $|\mathbf{Z}_n \times \mathbf{Z}_m| = nm$.

Proof of Proposition 3: $\mathbf{Z}_n \times \mathbf{Z}_m$ is cyclic $\Leftrightarrow (n, m) = 1$.

Recall: A finite group G is cyclic if and only if $o(x) = |G|$ for some $x \in G$.
$\Rightarrow$: Assume $\mathbf{Z}_n \times \mathbf{Z}_m$ is cyclic, we need *to show* $(n, m) = 1$. There is an element $(a, b) \in \mathbf{Z}_n \times \mathbf{Z}_m$ with $o((a, b)) = nm$ since $|\mathbf{Z}_n \times \mathbf{Z}_m| = nm$.
We also have $o(a)|n$ and $o(b)|m$. (Why?) [

Proof of Proposition 3: $\mathbf{Z}_n \times \mathbf{Z}_m$ is cyclic $\Leftrightarrow (n, m) = 1$.

Recall: A finite group G is cyclic if and only if $o(x) = |G|$ for some $x \in G$.
$\Rightarrow$: Assume $\mathbf{Z}_n \times \mathbf{Z}_m$ is cyclic, we need *to show* $(n, m) = 1$. There is an element $(a, b) \in \mathbf{Z}_n \times \mathbf{Z}_m$ with $o((a, b)) = nm$ since $|\mathbf{Z}_n \times \mathbf{Z}_m| = nm$.
We also have $o(a)|n$ and $o(b)|m$. (Why?) [Corollary 20 (a) in §3.2]

Proof of Proposition 3: $\mathbf{Z}_n \times \mathbf{Z}_m$ is cyclic $\Leftrightarrow (n, m) = 1$.

Recall: A finite group G is cyclic if and only if $o(x) = |G|$ for some $x \in G$.
$\Rightarrow$: Assume $\mathbf{Z}_n \times \mathbf{Z}_m$ is cyclic, we need *to show* $(n, m) = 1$. There is an element $(a, b) \in \mathbf{Z}_n \times \mathbf{Z}_m$ with $o((a, b)) = nm$ since $|\mathbf{Z}_n \times \mathbf{Z}_m| = nm$.
We also have $o(a)|n$ and $o(b)|m$. (Why?) [Corollary 20 (a) in §3.2]
And we have $o((a, b)) = \mathrm{lcm}[o(a), o(b)]$. (Why?) [

Proof of Proposition 3: $\mathbf{Z}_n \times \mathbf{Z}_m$ is cyclic $\Leftrightarrow (n, m) = 1$.

Recall: A finite group G is cyclic if and only if $o(x) = |G|$ for some $x \in G$.
$\Rightarrow$: Assume $\mathbf{Z}_n \times \mathbf{Z}_m$ is cyclic, we need *to show* $(n, m) = 1$. There is an element $(a, b) \in \mathbf{Z}_n \times \mathbf{Z}_m$ with $o((a, b)) = nm$ since $|\mathbf{Z}_n \times \mathbf{Z}_m| = nm$.
We also have $o(a)|n$ and $o(b)|m$. (Why?) [Corollary 20 (a) in §3.2]
And we have $o((a, b)) = \mathrm{lcm}[o(a), o(b)]$. (Why?) [Proposition 2 (b)]

Proof of Proposition 3: $\mathbf{Z}_n \times \mathbf{Z}_m$ is cyclic $\Leftrightarrow (n, m) = 1$.

Recall: A finite group G is cyclic if and only if $o(x) = |G|$ for some $x \in G$.
$\Rightarrow$: Assume $\mathbf{Z}_n \times \mathbf{Z}_m$ is cyclic, we need *to show* $(n, m) = 1$. There is an element $(a, b) \in \mathbf{Z}_n \times \mathbf{Z}_m$ with $o((a, b)) = nm$ since $|\mathbf{Z}_n \times \mathbf{Z}_m| = nm$.
We also have $o(a)|n$ and $o(b)|m$. (Why?) [Corollary 20 (a) in §3.2]
And we have $o((a, b)) = \mathrm{lcm}[o(a), o(b)]$. (Why?) [Proposition 2 (b)]
Therefore, we must have $o(a) = n$ and $o(b) = m$.

Proof of Proposition 3: $\mathbf{Z}_n \times \mathbf{Z}_m$ is cyclic $\Leftrightarrow (n, m) = 1$.

Recall: A finite group G is cyclic if and only if $o(x) = |G|$ for some $x \in G$.
$\Rightarrow$: Assume $\mathbf{Z}_n \times \mathbf{Z}_m$ is cyclic, we need *to show* $(n, m) = 1$. There is an element $(a, b) \in \mathbf{Z}_n \times \mathbf{Z}_m$ with $o((a, b)) = nm$ since $|\mathbf{Z}_n \times \mathbf{Z}_m| = nm$.
We also have $o(a)|n$ and $o(b)|m$. (Why?) [Corollary 20 (a) in §3.2]
And we have $o((a, b)) = \mathrm{lcm}[o(a), o(b)]$. (Why?) [Proposition 2 (b)]
Therefore, we must have $o(a) = n$ and $o(b) = m$. Otherwise,

$$nm = o((a, b)) = \mathrm{lcm}[o(a), o(b)] = \frac{o(a) \cdot o(b)}{\gcd(o(a), o(b))} \leq o(a) \cdot o(b) < nm$$

Proof of Proposition 3: $\mathbf{Z}_n \times \mathbf{Z}_m$ is cyclic $\Leftrightarrow (n, m) = 1$.

Recall: A finite group G is cyclic if and only if $o(x) = |G|$ for some $x \in G$.
$\Rightarrow$: Assume $\mathbf{Z}_n \times \mathbf{Z}_m$ is cyclic, we need *to show* $(n, m) = 1$. There is an element $(a, b) \in \mathbf{Z}_n \times \mathbf{Z}_m$ with $o((a, b)) = nm$ since $|\mathbf{Z}_n \times \mathbf{Z}_m| = nm$.
We also have $o(a)|n$ and $o(b)|m$. (Why?) [Corollary 20 (a) in §3.2]
And we have $o((a, b)) = \mathrm{lcm}[o(a), o(b)]$. (Why?) [Proposition 2 (b)]
Therefore, we must have $o(a) = n$ and $o(b) = m$. Otherwise,

$$nm = o((a, b)) = \mathrm{lcm}[o(a), o(b)] = \frac{o(a) \cdot o(b)}{\gcd(o(a), o(b))} \leq o(a) \cdot o(b) < nm$$

It implies that $\gcd(o(a), o(b)) = \gcd(n, m) = 1$. (Why?)
$\Leftarrow$:

Proof of Proposition 3: $\mathbf{Z}_n \times \mathbf{Z}_m$ is cyclic $\Leftrightarrow (n, m) = 1$.

Recall: A finite group G is cyclic if and only if $o(x) = |G|$ for some $x \in G$.
$\Rightarrow$: Assume $\mathbf{Z}_n \times \mathbf{Z}_m$ is cyclic, we need *to show* $(n, m) = 1$. There is an element $(a, b) \in \mathbf{Z}_n \times \mathbf{Z}_m$ with $o((a, b)) = nm$ since $|\mathbf{Z}_n \times \mathbf{Z}_m| = nm$.
We also have $o(a)|n$ and $o(b)|m$. (Why?) [Corollary 20 (a) in §3.2]
And we have $o((a, b)) = \mathrm{lcm}[o(a), o(b)]$. (Why?) [Proposition 2 (b)]
Therefore, we must have $o(a) = n$ and $o(b) = m$. Otherwise,

$$nm = o((a, b)) = \mathrm{lcm}[o(a), o(b)] = \frac{o(a) \cdot o(b)}{\gcd(o(a), o(b))} \leq o(a) \cdot o(b) < nm$$

It implies that $\gcd(o(a), o(b)) = \gcd(n, m) = 1$. (Why?)
$\Leftarrow$: Assume $(n, m) = 1$, consider the cyclic subgroup $\langle([1]_n, [1]_m)\rangle$.

Proof of Proposition 3: $\mathbf{Z}_n \times \mathbf{Z}_m$ is cyclic $\Leftrightarrow (n, m) = 1$.

Recall: A finite group G is cyclic if and only if $o(x) = |G|$ for some $x \in G$.
$\Rightarrow$: Assume $\mathbf{Z}_n \times \mathbf{Z}_m$ is cyclic, we need *to show* $(n, m) = 1$. There is an element $(a, b) \in \mathbf{Z}_n \times \mathbf{Z}_m$ with $o((a, b)) = nm$ since $|\mathbf{Z}_n \times \mathbf{Z}_m| = nm$.
We also have $o(a)|n$ and $o(b)|m$. (Why?) [Corollary 20 (a) in §3.2]
And we have $o((a, b)) = \mathrm{lcm}[o(a), o(b)]$. (Why?) [Proposition 2 (b)]
Therefore, we must have $o(a) = n$ and $o(b) = m$. Otherwise,

$$nm = o((a, b)) = \mathrm{lcm}[o(a), o(b)] = \frac{o(a) \cdot o(b)}{\gcd(o(a), o(b))} \leq o(a) \cdot o(b) < nm$$

It implies that $\gcd(o(a), o(b)) = \gcd(n, m) = 1$. (Why?)
$\Leftarrow$: Assume $(n, m) = 1$, consider the cyclic subgroup $\langle([1]_n, [1]_m)\rangle$. It is easy to see that $o([1]_n) = n$ and $o([1]_m) = m$.

Proof of Proposition 3: $\mathbf{Z}_n \times \mathbf{Z}_m$ is cyclic $\Leftrightarrow (n, m) = 1$.

Recall: A finite group G is cyclic if and only if $o(x) = |G|$ for some $x \in G$.
$\Rightarrow$: Assume $\mathbf{Z}_n \times \mathbf{Z}_m$ is cyclic, we need *to show* $(n, m) = 1$. There is an element $(a, b) \in \mathbf{Z}_n \times \mathbf{Z}_m$ with $o((a, b)) = nm$ since $|\mathbf{Z}_n \times \mathbf{Z}_m| = nm$.
We also have $o(a)|n$ and $o(b)|m$. (Why?) [Corollary 20 (a) in §3.2]
And we have $o((a, b)) = \mathrm{lcm}[o(a), o(b)]$. (Why?) [Proposition 2 (b)]
Therefore, we must have $o(a) = n$ and $o(b) = m$. Otherwise,

$$nm = o((a, b)) = \mathrm{lcm}[o(a), o(b)] = \frac{o(a) \cdot o(b)}{\gcd(o(a), o(b))} \leq o(a) \cdot o(b) < nm$$

It implies that $\gcd(o(a), o(b)) = \gcd(n, m) = 1$. (Why?)
$\Leftarrow$: Assume $(n, m) = 1$, consider the cyclic subgroup $\langle([1]_n, [1]_m)\rangle$. It is easy to see that $o([1]_n) = n$ and $o([1]_m) = m$. Again, we have

$$o(([1]_n, [1]_m)) = \mathrm{lcm}[o([1]_n), o([1]_m)] = \mathrm{lcm}[n, m] = \frac{nm}{(n, m)} = nm.$$

Proof of Proposition 3: $\mathbf{Z}_n \times \mathbf{Z}_m$ is cyclic $\Leftrightarrow (n, m) = 1$.

Recall: A finite group G is cyclic if and only if $o(x) = |G|$ for some $x \in G$.
$\Rightarrow$: Assume $\mathbf{Z}_n \times \mathbf{Z}_m$ is cyclic, we need *to show* $(n, m) = 1$. There is an element $(a, b) \in \mathbf{Z}_n \times \mathbf{Z}_m$ with $o((a, b)) = nm$ since $|\mathbf{Z}_n \times \mathbf{Z}_m| = nm$.
We also have $o(a)|n$ and $o(b)|m$. (Why?) [Corollary 20 (a) in §3.2]
And we have $o((a, b)) = \mathrm{lcm}[o(a), o(b)]$. (Why?) [Proposition 2 (b)]
Therefore, we must have $o(a) = n$ and $o(b) = m$. Otherwise,

$$nm = o((a, b)) = \mathrm{lcm}[o(a), o(b)] = \frac{o(a) \cdot o(b)}{\gcd(o(a), o(b))} \leq o(a) \cdot o(b) < nm$$

It implies that $\gcd(o(a), o(b)) = \gcd(n, m) = 1$. (Why?)
$\Leftarrow$: Assume $(n, m) = 1$, consider the cyclic subgroup $\langle([1]_n, [1]_m)\rangle$. It is easy to see that $o([1]_n) = n$ and $o([1]_m) = m$. Again, we have

$$o(([1]_n, [1]_m)) = \mathrm{lcm}[o([1]_n), o([1]_m)] = \mathrm{lcm}[n, m] = \frac{nm}{(n, m)} = nm.$$

Therefore, $\mathbf{Z}_n \times \mathbf{Z}_m = \langle([1]_n, [1]_m)\rangle$ since $|\mathbf{Z}_n \times \mathbf{Z}_m| = o(([1]_n, [1]_m))$.

Definition of a field

Definition 8

Definition of a field

Definition 8

Let F be a set with two binary operations $+$ and $\cdot$ with respective identity elements 0 and 1, where $0 \neq 1$. Then F is called a **field** if

(i) the set of all elements of F is an abelian group under $+$;

(ii) the set of all nonzero elements of F is an abelian group under $\cdot$;

(iii) $a(b+c) = ab + ac$ and $(a+b)c = ac + bc$ for all $a, b, c \in F$.

Definition of a field

Definition 8

Let F be a set with two binary operations $+$ and $\cdot$ with respective identity elements 0 and 1, where $0 \neq 1$. Then F is called a **field** if

(i) the set of all elements of F is an abelian group under $+$;

(ii) the set of all nonzero elements of F is an abelian group under $\cdot$;

(iii) $a(b+c) = ab + ac$ and $(a+b)c = ac + bc$ for all $a, b, c \in F$.

For example, $\mathbf{Q}, \mathbf{R}, \mathbf{C}, \mathbf{Z}_p$, when p is a prime number.

Definition of a field

Definition 8

Let F be a set with two binary operations $+$ and $\cdot$ with respective identity elements 0 and 1, where $0 \neq 1$. Then F is called a **field** if

(i) the set of all elements of F is an abelian group under $+$;

(ii) the set of all nonzero elements of F is an abelian group under $\cdot$;

(iii) $a(b+c) = ab + ac$ and $(a+b)c = ac + bc$ for all $a, b, c \in F$.

For example, $\mathbf{Q}, \mathbf{R}, \mathbf{C}, \mathbf{Z}_p$, when p is a prime number. But $\mathbf{Z}$ is not a field.

Definition of a field

Definition 8

Let F be a set with two binary operations $+$ and $\cdot$ with respective identity elements 0 and 1, where $0 \neq 1$. Then F is called a **field** if

(i) the set of all elements of F is an abelian group under $+$;

(ii) the set of all nonzero elements of F is an abelian group under $\cdot$;

(iii) $a(b+c) = ab + ac$ and $(a+b)c = ac + bc$ for all $a, b, c \in F$.

For example, $\mathbf{Q}, \mathbf{R}, \mathbf{C}, \mathbf{Z}_p$, when p is a prime number. But $\mathbf{Z}$ is not a field. Axiom (iii) lists the **distributive laws**, which give a connection between addition and multiplication.

Proposition 4

Definition of a field

Definition 8

Let F be a set with two binary operations $+$ and $\cdot$ with respective identity elements 0 and 1, where $0 \neq 1$. Then F is called a **field** if

(i) the set of all elements of F is an abelian group under $+$;

(ii) the set of all nonzero elements of F is an abelian group under $\cdot$;

(iii) $a(b+c) = ab + ac$ and $(a+b)c = ac + bc$ for all $a, b, c \in F$.

For example, $\mathbf{Q}, \mathbf{R}, \mathbf{C}, \mathbf{Z}_p$, when p is a prime number. But $\mathbf{Z}$ is not a field. Axiom (iii) lists the **distributive laws**, which give a connection between addition and multiplication.

Proposition 4

For any element $a \in F$, we have $a \cdot 0 = 0$ and $0 \cdot a = 0$.

Proof:

Definition of a field

Definition 8

Let F be a set with two binary operations $+$ and $\cdot$ with respective identity elements 0 and 1, where $0 \neq 1$. Then F is called a **field** if

(i) the set of all elements of F is an abelian group under $+$;

(ii) the set of all nonzero elements of F is an abelian group under $\cdot$;

(iii) $a(b+c) = ab + ac$ and $(a+b)c = ac + bc$ for all $a, b, c \in F$.

For example, $\mathbf{Q}, \mathbf{R}, \mathbf{C}, \mathbf{Z}_p$, when p is a prime number. But $\mathbf{Z}$ is not a field. Axiom (iii) lists the **distributive laws**, which give a connection between addition and multiplication.

Proposition 4

For any element $a \in F$, we have $a \cdot 0 = 0$ and $0 \cdot a = 0$.

Proof: Note that 0 is (not)in the multiplicative group $(F^{\times}, \cdot)$, but in $(F, +)$.

Definition of a field

Definition 8

Let F be a set with two binary operations $+$ and $\cdot$ with respective identity elements 0 and 1, where $0 \neq 1$. Then F is called a **field** if

(i) the set of all elements of F is an abelian group under $+$;

(ii) the set of all nonzero elements of F is an abelian group under $\cdot$;

(iii) $a(b+c) = ab + ac$ and $(a+b)c = ac + bc$ for all $a, b, c \in F$.

For example, $\mathbf{Q}, \mathbf{R}, \mathbf{C}, \mathbf{Z}_p$, when p is a prime number. But $\mathbf{Z}$ is not a field. Axiom (iii) lists the **distributive laws**, which give a connection between addition and multiplication.

Proposition 4

For any element $a \in F$, we have $a \cdot 0 = 0$ and $0 \cdot a = 0$.

Proof: Note that 0 is (not)in the multiplicative group $(F^{\times}, \cdot)$, but in $(F, +)$.

$$0 + a \cdot 0 = a \cdot 0 = a \cdot (0+0) = a \cdot 0 + a \cdot 0 \Rightarrow 0 = a \cdot 0 \ (\textit{Why?})$$

Definition of a field

Definition 8

Let F be a set with two binary operations $+$ and $\cdot$ with respective identity elements 0 and 1, where $0 \neq 1$. Then F is called a **field** if

(i) the set of all elements of F is an abelian group under $+$;

(ii) the set of all nonzero elements of F is an abelian group under $\cdot$;

(iii) $a(b+c) = ab + ac$ and $(a+b)c = ac + bc$ for all $a, b, c \in F$.

For example, $\mathbf{Q}, \mathbf{R}, \mathbf{C}, \mathbf{Z}_p$, when p is a prime number. But $\mathbf{Z}$ is not a field. Axiom (iii) lists the **distributive laws**, which give a connection between addition and multiplication.

Proposition 4

For any element $a \in F$, we have $a \cdot 0 = 0$ and $0 \cdot a = 0$.

Proof: Note that 0 is (not)in the multiplicative group $(F^{\times}, \cdot)$, but in $(F, +)$.

$$0 + a \cdot 0 = a \cdot 0 = a \cdot (0+0) = a \cdot 0 + a \cdot 0 \Rightarrow 0 = a \cdot 0 \ (\textit{Why?})$$

A similar argument shows that $0 \cdot a = 0$ for all $a \in F$. (Check it!)

$\mathrm{GL}_n(F)$

Definition 9

$\mathrm{GL}_n(F)$

Definition 9

Let F be a field. The set of all invertible $n \times n$ matrices with entries in F is called the **general linear group of degree n over F**, and is denoted by $\mathrm{GL}_n(F)$.

Proposition 5

$\mathrm{GL}_n(F)$

Definition 9

Let F be a field. The set of all invertible $n \times n$ matrices with entries in F is called the **general linear group of degree** n **over** F, and is denoted by $\mathrm{GL}_n(F)$.

Proposition 5

Let F be a field. Then $\mathrm{GL}_n(F)$ is a group under matrix multiplication.

$\mathrm{GL}_n(F)$

Definition 9

Let F be a field. The set of all invertible $n \times n$ matrices with entries in F is called the **general linear group of degree n over F**, and is denoted by $\mathrm{GL}_n(F)$.

Proposition 5

Let F be a field. Then $\mathrm{GL}_n(F)$ is a group under matrix multiplication.

(i) Well-definedness: If (a_{ij}) and (b_{ij}) are $n \times n$ matrices, then the product (c_{ij}) with (i,j)-entries $c_{ij} = \sum_{k=1}^{n} a_{ik} b_{kj}$.

$\mathrm{GL}_n(F)$

Definition 9

Let F be a field. The set of all invertible $n \times n$ matrices with entries in F is called the **general linear group of degree n over F**, and is denoted by $\mathrm{GL}_n(F)$.

Proposition 5

Let F be a field. Then $\mathrm{GL}_n(F)$ is a group under matrix multiplication.

(i) Well-definedness: If (a_{ij}) and (b_{ij}) are $n \times n$ matrices, then the product (c_{ij}) with (i, j)-entries $c_{ij} = \sum_{k=1}^{n} a_{ik} b_{kj}$.
If $A, B \in \mathrm{GL}_n(F)$, then $AB \in \mathrm{GL}_n(F)$. (Why?)

$\mathrm{GL}_n(F)$

Definition 9

Let F be a field. The set of all invertible $n \times n$ matrices with entries in F is called the **general linear group of degree n over F**, and is denoted by $\mathrm{GL}_n(F)$.

Proposition 5

Let F be a field. Then $\mathrm{GL}_n(F)$ is a group under matrix multiplication.

(i) Well-definedness: If (a_{ij}) and (b_{ij}) are $n \times n$ matrices, then the product (c_{ij}) with (i,j)-entries $c_{ij} = \sum_{k=1}^{n} a_{ik} b_{kj}$.
If $A, B \in \mathrm{GL}_n(F)$, then $AB \in \mathrm{GL}_n(F)$. (Why?)

(ii) Associativity: ✓

$\mathrm{GL}_n(F)$

Definition 9

Let F be a field. The set of all invertible $n \times n$ matrices with entries in F is called the **general linear group of degree** n **over** F, and is denoted by $\mathrm{GL}_n(F)$.

Proposition 5

Let F be a field. Then $\mathrm{GL}_n(F)$ is a group under matrix multiplication.

(i) Well-definedness: If (a_{ij}) and (b_{ij}) are $n \times n$ matrices, then the product (c_{ij}) with (i, j)-entries $c_{ij} = \sum_{k=1}^{n} a_{ik} b_{kj}$.

If $A, B \in \mathrm{GL}_n(F)$, then $AB \in \mathrm{GL}_n(F)$. (Why?)

(ii) Associativity: ✓

(iii) Identity: The identity matrix I_n

$\mathrm{GL}_n(F)$

Definition 9

Let F be a field. The set of all invertible $n \times n$ matrices with entries in F is called the **general linear group of degree n over F**, and is denoted by $\mathrm{GL}_n(F)$.

Proposition 5

Let F be a field. Then $\mathrm{GL}_n(F)$ is a group under matrix multiplication.

(i) Well-definedness: If (a_{ij}) and (b_{ij}) are $n \times n$ matrices, then the product (c_{ij}) with (i,j)-entries $c_{ij} = \sum_{k=1}^{n} a_{ik} b_{kj}$.
If $A, B \in \mathrm{GL}_n(F)$, then $AB \in \mathrm{GL}_n(F)$. (Why?)

(ii) Associativity: ✓

(iii) Identity: The identity matrix I_n

(iv) Inverses: $A^{-1} \in \mathrm{GL}_n(F)$. (Why?) [

$\mathrm{GL}_n(F)$

Definition 9

Let F be a field. The set of all invertible $n \times n$ matrices with entries in F is called the **general linear group of degree n over F**, and is denoted by $\mathrm{GL}_n(F)$.

Proposition 5

Let F be a field. Then $\mathrm{GL}_n(F)$ is a group under matrix multiplication.

(i) Well-definedness: If (a_{ij}) and (b_{ij}) are $n \times n$ matrices, then the product (c_{ij}) with (i,j)-entries $c_{ij} = \sum_{k=1}^{n} a_{ik} b_{kj}$.
If $A, B \in \mathrm{GL}_n(F)$, then $AB \in \mathrm{GL}_n(F)$. (Why?)

(ii) Associativity: ✓

(iii) Identity: The identity matrix I_n

(iv) Inverses: $A^{-1} \in \mathrm{GL}_n(F)$. (Why?) [definition of invertible matrix]

Example 1: $\mathrm{GL}_2(\mathbf{Z}_2)$

Example 1: $\mathrm{GL}_2(\mathbf{Z}_2)$

We can check that $|\mathrm{GL}_2(\mathbf{Z}_2)| = 6$.

Example 1: $\mathrm{GL}_2(\mathbf{Z}_2)$

We can check that $|\mathrm{GL}_2(\mathbf{Z}_2)| = 6$. These 6 elements are

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

Example 1: $\mathrm{GL}_2(\mathbf{Z}_2)$

We can check that $|\mathrm{GL}_2(\mathbf{Z}_2)| = 6$. These 6 elements are

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

We simply use 0 and 1 to denote the congruence classes $[0]_2$ and $[1]_2$.

Example 1: $\mathrm{GL}_2(\mathbf{Z}_2)$

We can check that $|\mathrm{GL}_2(\mathbf{Z}_2)| = 6$. These 6 elements are

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

We simply use 0 and 1 to denote the congruence classes $[0]_2$ and $[1]_2$. Note that the group $\mathrm{GL}_2(\mathbf{Z}_2)$ is not abelian.

Proposition 6

Example 1: $\mathrm{GL}_2(\mathbf{Z}_2)$

We can check that $|\mathrm{GL}_2(\mathbf{Z}_2)| = 6$. These 6 elements are

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

We simply use 0 and 1 to denote the congruence classes $[0]_2$ and $[1]_2$. Note that the group $\mathrm{GL}_2(\mathbf{Z}_2)$ is not abelian.

Proposition 6

$|\mathrm{GL}_2(\mathbf{Z}_p)| = (p^2 - 1)(p^2 - p)$, *where p is a prime number.*

Example 1: $\mathrm{GL}_2(\mathbf{Z}_2)$

We can check that $|\mathrm{GL}_2(\mathbf{Z}_2)| = 6$. These 6 elements are

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

We simply use 0 and 1 to denote the congruence classes $[0]_2$ and $[1]_2$. Note that the group $\mathrm{GL}_2(\mathbf{Z}_2)$ is not abelian.

Proposition 6

$|\mathrm{GL}_2(\mathbf{Z}_p)| = (p^2 - 1)(p^2 - p)$, *where p is a prime number.*

- For the first row, there are $p^2 - 1$ choices. (Why?)

Example 1: $\mathrm{GL}_2(\mathbf{Z}_2)$

We can check that $|\mathrm{GL}_2(\mathbf{Z}_2)| = 6$. These 6 elements are

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

We simply use 0 and 1 to denote the congruence classes $[0]_2$ and $[1]_2$. Note that the group $\mathrm{GL}_2(\mathbf{Z}_2)$ is not abelian.

Proposition 6

$|\mathrm{GL}_2(\mathbf{Z}_p)| = (p^2 - 1)(p^2 - p)$, *where p is a prime number.*

- For the first row, there are $p^2 - 1$ choices. (Why?)
  -1 is because $(0, 0)$ cannot be a choice.

Example 1: $\mathrm{GL}_2(\mathbf{Z}_2)$

We can check that $|\mathrm{GL}_2(\mathbf{Z}_2)| = 6$. These 6 elements are

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

We simply use 0 and 1 to denote the congruence classes $[0]_2$ and $[1]_2$. Note that the group $\mathrm{GL}_2(\mathbf{Z}_2)$ is not abelian.

Proposition 6

$|\mathrm{GL}_2(\mathbf{Z}_p)| = (p^2 - 1)(p^2 - p)$, *where p is a prime number.*

- For the first row, there are $p^2 - 1$ choices. (Why?)
  -1 is because $(0, 0)$ cannot be a choice.
- For the second row, there are $p^2 - p$ choices. (Why?)

Example 1: $\mathrm{GL}_2(\mathbf{Z}_2)$

We can check that $|\mathrm{GL}_2(\mathbf{Z}_2)| = 6$. These 6 elements are

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

We simply use 0 and 1 to denote the congruence classes $[0]_2$ and $[1]_2$. Note that the group $\mathrm{GL}_2(\mathbf{Z}_2)$ is not abelian.

Proposition 6

$|\mathrm{GL}_2(\mathbf{Z}_p)| = (p^2 - 1)(p^2 - p)$, *where p is a prime number.*

- For the first row, there are $p^2 - 1$ choices. (Why?)
  -1 is because $(0, 0)$ cannot be a choice.
- For the second row, there are $p^2 - p$ choices. (Why?)
  $-p$ is because the scalars of the first row cannot be choices.

Example 2: Quaternion group

Let Q be the following set of matrices in $\mathrm{GL}_2(\mathbf{C})$:

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

Example 2: Quaternion group

Let Q be the following set of matrices in $\mathrm{GL}_2(\mathbf{C})$:

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

If we let

$$1=\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix},\quad \mathbf{i}=\begin{bmatrix}i & 0\\ 0 & -i\end{bmatrix},\quad \mathbf{j}=\begin{bmatrix}0 & 1\\ -1 & 0\end{bmatrix},\quad \mathbf{k}=\begin{bmatrix}0 & i\\ i & 0\end{bmatrix}.$$

then computations show that we have the following identities:

Example 2: Quaternion group

Let Q be the following set of matrices in $\mathrm{GL}_2(\mathbf{C})$:

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

If we let

$$1=\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}, \quad \mathbf{i}=\begin{bmatrix}i & 0\\ 0 & -i\end{bmatrix}, \quad \mathbf{j}=\begin{bmatrix}0 & 1\\ -1 & 0\end{bmatrix}, \quad \mathbf{k}=\begin{bmatrix}0 & i\\ i & 0\end{bmatrix}.$$

then computations show that we have the following identities:

$$\mathbf{i}^2=\mathbf{j}^2=\mathbf{k}^2=-1;$$
$$\mathbf{ij}=\mathbf{k}, \quad \mathbf{jk}=\mathbf{i}, \quad \mathbf{ki}=\mathbf{j}; \qquad \mathbf{ji}=-\mathbf{k}, \quad \mathbf{kj}=-\mathbf{i}, \quad \mathbf{ik}=-\mathbf{j}.$$

Example 2: Quaternion group

Let Q be the following set of matrices in $\mathrm{GL}_2(\mathbf{C})$:

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

If we let

$$1 = \begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}, \quad \mathbf{i} = \begin{bmatrix}i & 0\\ 0 & -i\end{bmatrix}, \quad \mathbf{j} = \begin{bmatrix}0 & 1\\ -1 & 0\end{bmatrix}, \quad \mathbf{k} = \begin{bmatrix}0 & i\\ i & 0\end{bmatrix}.$$

then computations show that we have the following identities:

$$\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -1;$$
$$\mathbf{ij} = \mathbf{k}, \quad \mathbf{jk} = \mathbf{i}, \quad \mathbf{ki} = \mathbf{j}; \qquad \mathbf{ji} = -\mathbf{k}, \quad \mathbf{kj} = -\mathbf{i}, \quad \mathbf{ik} = -\mathbf{j}.$$

Q is a subgroup of $\mathrm{GL}_2(\mathbf{C})$. (Check it!) [Closure: ✓]

Example 2: Quaternion group

Let Q be the following set of matrices in $\mathrm{GL}_2(\mathbf{C})$:

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

If we let

$$1=\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix},\quad \mathbf{i}=\begin{bmatrix}i & 0\\ 0 & -i\end{bmatrix},\quad \mathbf{j}=\begin{bmatrix}0 & 1\\ -1 & 0\end{bmatrix},\quad \mathbf{k}=\begin{bmatrix}0 & i\\ i & 0\end{bmatrix}.$$

then computations show that we have the following identities:

$$\mathbf{i}^2=\mathbf{j}^2=\mathbf{k}^2=-1;$$
$$\mathbf{ij}=\mathbf{k},\quad \mathbf{jk}=\mathbf{i},\quad \mathbf{ki}=\mathbf{j};\qquad\qquad \mathbf{ji}=-\mathbf{k},\quad \mathbf{kj}=-\mathbf{i},\quad \mathbf{ik}=-\mathbf{j}.$$

Q is a subgroup of $\mathrm{GL}_2(\mathbf{C})$. (Check it!) [Closure: ✓]
Q is not abelian (Why?) and

Example 2: Quaternion group

Let Q be the following set of matrices in $\mathrm{GL}_2(\mathbf{C})$:

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

If we let

$$1 = \begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}, \quad \mathbf{i} = \begin{bmatrix}i & 0\\ 0 & -i\end{bmatrix}, \quad \mathbf{j} = \begin{bmatrix}0 & 1\\ -1 & 0\end{bmatrix}, \quad \mathbf{k} = \begin{bmatrix}0 & i\\ i & 0\end{bmatrix}.$$

then computations show that we have the following identities:

$$\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -1;$$
$$\mathbf{ij} = \mathbf{k}, \quad \mathbf{jk} = \mathbf{i}, \quad \mathbf{ki} = \mathbf{j}; \qquad \mathbf{ji} = -\mathbf{k}, \quad \mathbf{kj} = -\mathbf{i}, \quad \mathbf{ik} = -\mathbf{j}.$$

Q is a subgroup of $\mathrm{GL}_2(\mathbf{C})$. (Check it!) [Closure: ✓]
Q is not abelian (Why?) and is not cyclic (Why?).

Example 2: Quaternion group

Let Q be the following set of matrices in $\mathrm{GL}_2(\mathbf{C})$:

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

If we let

$$1=\begin{bmatrix}1 & 0\\0 & 1\end{bmatrix},\quad \mathbf{i}=\begin{bmatrix}i & 0\\0 & -i\end{bmatrix},\quad \mathbf{j}=\begin{bmatrix}0 & 1\\-1 & 0\end{bmatrix},\quad \mathbf{k}=\begin{bmatrix}0 & i\\i & 0\end{bmatrix}.$$

then computations show that we have the following identities:

$$\mathbf{i}^2=\mathbf{j}^2=\mathbf{k}^2=-1;$$
$$\mathbf{ij}=\mathbf{k},\quad \mathbf{jk}=\mathbf{i},\quad \mathbf{ki}=\mathbf{j};\qquad\qquad \mathbf{ji}=-\mathbf{k},\quad \mathbf{kj}=-\mathbf{i},\quad \mathbf{ik}=-\mathbf{j}.$$

Q is a subgroup of $\mathrm{GL}_2(\mathbf{C})$. (Check it!) [Closure: ✓]
Q is not abelian (Why?) and is not cyclic (Why?).

- -1 has order 2

Example 2: Quaternion group

Let Q be the following set of matrices in $\mathrm{GL}_2(\mathbf{C})$:

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

If we let

$$1=\begin{bmatrix}1 & 0\\0 & 1\end{bmatrix},\quad \mathbf{i}=\begin{bmatrix}i & 0\\0 & -i\end{bmatrix},\quad \mathbf{j}=\begin{bmatrix}0 & 1\\-1 & 0\end{bmatrix},\quad \mathbf{k}=\begin{bmatrix}0 & i\\i & 0\end{bmatrix}.$$

then computations show that we have the following identities:

$$\mathbf{i}^2=\mathbf{j}^2=\mathbf{k}^2=-1;$$
$$\mathbf{ij}=\mathbf{k},\quad \mathbf{jk}=\mathbf{i},\quad \mathbf{ki}=\mathbf{j};\qquad\qquad \mathbf{ji}=-\mathbf{k},\quad \mathbf{kj}=-\mathbf{i},\quad \mathbf{ik}=-\mathbf{j}.$$

Q is a subgroup of $\mathrm{GL}_2(\mathbf{C})$. (Check it!) [Closure: ✓]
Q is not abelian (Why?) and is not cyclic (Why?).

- -1 has order 2
- $\pm\mathbf{i}, \pm\mathbf{j}$, and $\pm\mathbf{k}$ have order 4

Subgroup generated by S

Definition 10

Subgroup generated by S

Definition 10

Let S be a nonempty subset of the group G. A finite product of elements of S and their inverses is called a **word** in S. The set of all words in S is denoted by $\langle S \rangle$.

Subgroup generated by S

Definition 10

Let S be a nonempty subset of the group G. A finite product of elements of S and their inverses is called a **word** in S. The set of all words in S is denoted by $\langle S \rangle$.

For example, for $a, b, c \in S$, the product $a^{-1}a^{-1}bab^{-1}acb^{-1}cbc^{-1}c^{-1}$.

Proposition 7

Subgroup generated by S

Definition 10

Let S be a nonempty subset of the group G. A finite product of elements of S and their inverses is called a **word** in S. The set of all words in S is denoted by $\langle S\rangle$.

For example, for $a, b, c \in S$, the product $a^{-1}a^{-1}bab^{-1}acb^{-1}cbc^{-1}c^{-1}$.

Proposition 7

Let S be a nonempty subset of the group G. Then $\langle S\rangle$ is a subgroup of G, and is equal to the intersection of all subgroups of G that contain S.

Subgroup generated by S

Definition 10

Let S be a nonempty subset of the group G. A finite product of elements of S and their inverses is called a **word** in S. The set of all words in S is denoted by $\langle S \rangle$.

For example, for $a, b, c \in S$, the product $a^{-1}a^{-1}bab^{-1}acb^{-1}cbc^{-1}c^{-1}$.

Proposition 7

Let S be a nonempty subset of the group G. Then $\langle S \rangle$ is a subgroup of G, and is equal to the intersection of all subgroups of G that contain S.

(i) If x and y are two words in S, then xy is again a word in S. ✓

Subgroup generated by S

Definition 10

Let S be a nonempty subset of the group G. A finite product of elements of S and their inverses is called a **word** in S. The set of all words in S is denoted by $\langle S \rangle$.

For example, for $a, b, c \in S$, the product $a^{-1}a^{-1}bab^{-1}acb^{-1}cbc^{-1}c^{-1}$.

Proposition 7

Let S be a nonempty subset of the group G. Then $\langle S \rangle$ is a subgroup of G, and is equal to the intersection of all subgroups of G that contain S.

(i) If x and y are two words in S, then xy is again a word in S. ✓

(ii) $e = aa^{-1} \in \langle S \rangle$. A element $a \in S$ always exists since S is nonempty.

Subgroup generated by S

Definition 10

Let S be a nonempty subset of the group G. A finite product of elements of S and their inverses is called a **word** in S. The set of all words in S is denoted by $\langle S \rangle$.

For example, for $a, b, c \in S$, the product $a^{-1}a^{-1}bab^{-1}acb^{-1}cbc^{-1}c^{-1}$.

Proposition 7

Let S be a nonempty subset of the group G. Then $\langle S \rangle$ is a subgroup of G, and is equal to the intersection of all subgroups of G that contain S.

(i) If x and y are two words in S, then xy is again a word in S. ✓
(ii) $e = aa^{-1} \in \langle S \rangle$. A element $a \in S$ always exists since S is nonempty.
(iii) $x^{-1} \in \langle S \rangle$: reverses the order and changes the sign of the exponent.

Subgroup generated by S

Definition 10

Let S be a nonempty subset of the group G. A finite product of elements of S and their inverses is called a **word** in S. The set of all words in S is denoted by $\langle S \rangle$.

For example, for $a, b, c \in S$, the product $a^{-1}a^{-1}bab^{-1}acb^{-1}cbc^{-1}c^{-1}$.

Proposition 7

Let S be a nonempty subset of the group G. Then $\langle S \rangle$ is a subgroup of G, and is equal to the intersection of all subgroups of G that contain S.

(i) If x and y are two words in S, then xy is again a word in S. ✓
(ii) $e = aa^{-1} \in \langle S \rangle$. A element $a \in S$ always exists since S is nonempty.
(iii) $x^{-1} \in \langle S \rangle$: reverses the order and changes the sign of the exponent.

If $S \subseteq H$, where H is a subgroup of G, then it contains all words in S.

Subgroup generated by S

Definition 10

Let S be a nonempty subset of the group G. A finite product of elements of S and their inverses is called a **word** in S. The set of all words in S is denoted by $\langle S\rangle$.

For example, for $a, b, c \in S$, the product $a^{-1}a^{-1}bab^{-1}acb^{-1}cbc^{-1}c^{-1}$.

Proposition 7

Let S be a nonempty subset of the group G. Then $\langle S\rangle$ is a subgroup of G, and is equal to the intersection of all subgroups of G that contain S.

(i) If x and y are two words in S, then xy is again a word in S. ✓
(ii) $e = aa^{-1} \in \langle S\rangle$. A element $a \in S$ always exists since S is nonempty.
(iii) $x^{-1} \in \langle S\rangle$: reverses the order and changes the sign of the exponent.

If $S \subseteq H$, where H is a subgroup of G, then it contains all words in S. Therefore, $\langle S\rangle \subseteq H$.

Subgroup generated by S

Definition 10

Let S be a nonempty subset of the group G. A finite product of elements of S and their inverses is called a **word** in S. The set of all words in S is denoted by $\langle S \rangle$.

For example, for $a, b, c \in S$, the product $a^{-1}a^{-1}bab^{-1}acb^{-1}cbc^{-1}c^{-1}$.

Proposition 7

Let S be a nonempty subset of the group G. Then $\langle S \rangle$ is a subgroup of G, and is equal to the intersection of all subgroups of G that contain S.

(i) If x and y are two words in S, then xy is again a word in S. ✓

(ii) $e = aa^{-1} \in \langle S \rangle$. A element $a \in S$ always exists since S is nonempty.

(iii) $x^{-1} \in \langle S \rangle$: reverses the order and changes the sign of the exponent.

If $S \subseteq H$, where H is a subgroup of G, then it contains all words in S. Therefore, $\langle S \rangle \subseteq H$. It follows that $\langle S \rangle$ is the intersection of all subgroups of G that contain S.

Subgroup generated by S

Definition 10

Let S be a nonempty subset of the group G. A finite product of elements of S and their inverses is called a **word** in S. The set of all words in S is denoted by $\langle S \rangle$.

For example, for $a, b, c \in S$, the product $a^{-1}a^{-1}bab^{-1}acb^{-1}cbc^{-1}c^{-1}$.

Proposition 7

Let S be a nonempty subset of the group G. Then $\langle S \rangle$ is a subgroup of G, and is equal to the intersection of all subgroups of G that contain S.

(i) If x and y are two words in S, then xy is again a word in S. ✓
(ii) $e = aa^{-1} \in \langle S \rangle$. A element $a \in S$ always exists since S is nonempty.
(iii) $x^{-1} \in \langle S \rangle$: reverses the order and changes the sign of the exponent.

If $S \subseteq H$, where H is a subgroup of G, then it contains all words in S. Therefore, $\langle S \rangle \subseteq H$. It follows that $\langle S \rangle$ is the intersection of all subgroups of G that contain S. That is, $\langle S \rangle$ is the smallest subgroup that contains S.