Institute: University of Basrah

College of Sciences

Department of Mathematics

Email: mohna_l@yahoo.com

mohammed.ibrahim@uobasrah.edu.iq

Date: October 8, 2022

Mohammed Alabbood
MOHAMMED ALI IBRAHIM

Half of knowledge is to say "I do not know"

Contents

GROUP THEORY: PART II

Homomorphisms of groups

DEFINITION: Let $(G, \star)$ and $(G', \star')$ be two groups. A map $\varphi : G \to G'$ is said to be a **group homomorphism** if for all $a, b \in G$:

$$\varphi(a \star b) = \varphi(a) \star' \varphi(b).$$

A **kernel** of φ, denoted by $\ker(\varphi)$, is the set:

$$\ker(\varphi) = \{a \in G : \varphi(a) = e'\}$$

where e' is the identity of G'. The **image** of φ, denoted by $\mathsf{im}(\varphi)$, is the set:

$$\mathsf{im}(\varphi) = \{\varphi(a) \in G' : a \in G\}.$$

Note that $\ker(\varphi) \subseteq G$, while $\mathsf{im}(\varphi) \subseteq G'$.

THEOREM: Let $(G, \star)$ and $(G', \star')$ be two groups, and let $\varphi : G \to G'$ be a group homomorphism. Then

1. $\varphi(e) = e'$, where e and e' are the identities of G and G' respectively.
2. $\varphi(a^{-1}) = (\varphi(a))^{-1}$.
3. $\ker(\varphi) \leq G$.
4. $\mathsf{im}(\varphi) \leq G'$.
5. $\ker(\varphi) = \{e\} \iff \varphi$ is one-one.

Proof

1. $\varphi(e) = \varphi(e \star e) = \varphi(e) \star' \varphi(e)$. On the other hand, $\varphi(e) = \varphi(e) \star' e'$.

   So,
$$\varphi(e) \star' \varphi(e) = \varphi(e) \star' e'.$$
   By cancellation law, we get $\varphi(e) = e'$.

2. $\varphi(a \star a^{-1}) = \varphi(e) = e'$. Since φ is a group homomorphism, we have
$$\varphi(a \star a^{-1}) = \varphi(a) \star' \varphi(a^{-1}) = e' = \varphi(a) \star' (\varphi(a))^{-1}.$$
   By cancellation law, we get $\varphi(a^{-1}) = (\varphi(a))^{-1}$.

3. Let $x, y \in \ker(\varphi)$.
   (a). $e \in \ker(\varphi)$ since $\varphi(e) = e'$ [by (1)].
   (b). Since $x, y \in \ker(\varphi)$, we have $\varphi(x) = \varphi(y) = e'$. Want to show that $x \star y^{-1} \in \ker(\varphi)$, i.e. $\varphi(x \star y^{-1}) = e'$. Note that:
$$\begin{aligned}\varphi(x \star y^{-1}) &= \varphi(x) \star' \varphi(y) = \varphi(x) \star' \varphi(y^{-1}) \\ &= \varphi(x) \star' (\varphi(y))^{-1} = e' \star e'^{-1} = e' \star e' = e'.\end{aligned}$$
   Thus $\ker(\varphi) \leq G$.

4. Let $x', y' \in \mathsf{im}(\varphi)$.
   (a). $e' \in \mathsf{im}(\varphi)$ since $e' = \varphi(e) \in \mathsf{im}(\varphi)$ [by (1)].
   (b). Want to show that $x' \star' y'^{-1} \in \mathsf{im}(\varphi)$. We have $x' = \varphi(x)$ and $y' = \varphi(y)$ for some $x, y \in G$.
$$\varphi(x \star y^{-1}) = \varphi(x) \star' \varphi(y^{-1}) = \varphi(x) \star' (\varphi(y))^{-1} = x' \star' y'^{-1}.$$
   So, $x' \star' y'^{-1} \in \mathsf{im}(\varphi)$ [since $x \star y^{-1} \in G$]. Thus $\mathsf{im}(\varphi) \leq G'$.

5. Assume that $\ker(\varphi) = \{e\}$. Let $\varphi(x) = \varphi(y)$. Want to show that

$x = y$:

$$\varphi(x) = \varphi(y) \Longrightarrow \varphi(x) \star' (\varphi(y))^{-1} = \varphi(y) \star' (\varphi(y))^{-1} = e'$$

$$\Longrightarrow \varphi(x) \star' (\varphi(y))^{-1} = \varphi(x) \star' \varphi(y^{-1}) = e' \quad [\text{by } 2]$$

$$\Longrightarrow \varphi(x \star y^{-1}) = e' \quad \text{since } \varphi \text{ is group homomorphism}$$

$$\Longrightarrow x \star y^{-1} \in \ker(\varphi) = \{e\} \Longrightarrow x \star y^{-1} = e$$

$$\Longrightarrow x \star y^{-1} \star y = e \star y = y \Longrightarrow x \star e = y \Longrightarrow x = y.$$

Conversely, assume that φ is one-one, and let $x \in \ker(\varphi)$. Want to show that $x = e$.

$$x \in \ker(\varphi) \Longrightarrow \varphi(x) = e' = \varphi(e) \text{ [by (1)]}$$

$$\Longrightarrow x = e \quad [\text{ since } \varphi \text{ is one-one}].$$

Definition: A group homomorphism $\varphi : G \to G'$ is said to be

- **epimorphism** if it is onto, i.e. $\text{im}(\varphi) = \varphi(G) = G'$.
- **monomorphism** if it is one-one, i.e. $\ker(\varphi) = \{e\}$.
- **isomorphism** if it is epimorphism and monomorphism. In this case, we say G **isomorphic** to G', and we write $G \cong G'$.
- **automorphism** if it is isomorphism and $G = G'$.
- **trivial homomorphism** if $\varphi(a) = e'$ for all $a \in G$.
- **identity homomorphism** if $G = G'$ and $\varphi(a) = a$ for all $a \in G$.

Example: I. The map $\varphi : (\mathbb{R}, +) \to (\mathbb{R}^+, \cdot)$ defined by $\varphi(x) = e^x$ is an isomorphism and hence $\mathbb{R} \cong \mathbb{R}^+$.

Claim:

1. φ is a group homomorphism: Let $x, y \in \mathbb{R}$. Then

$$\varphi(x + y) = e^{x+y} = e^x \cdot e^y = \varphi(x) \cdot \varphi(y).$$

2. φ is one-one:

$$\ker(\varphi) = \{x \in \mathbb{R} : \varphi(x) = 1\} = \{x \in \mathbb{R} : e^x = 1\} = \{0\}.$$

3. φ is onto: Let $y \in \mathbb{R}^+$ (codomain). Want to find $x \in \mathbb{R}$ (domain) such that $\varphi(x) = y$. Since $y \in \mathbb{R}^+$, we can take $x = \ln(y) \in \mathbb{R}$. Note that

$$\varphi(x) = e^x = e^{\ln(y)} = y.$$

Thus $\mathbb{R} \cong \mathbb{R}^+$.

Example: II. Show that the map $\varphi : (\mathbb{R}\backslash\{0\}, \cdot) \to (\mathbb{R}^+, \cdot)$ defined by $\varphi(x) = |x|$ is an epimorphism. What is the kernel of φ?

Answer:

1. φ is a group homomorphism: Let $x, y \in \mathbb{R}$. Then

$$\varphi(x \cdot y) = |x \cdot y| = |x| \cdot |y| = \varphi(x) \cdot \varphi(y).$$

2. φ is onto: Let $y \in \mathbb{R}^+$ (codomain). Want to find $x \in \mathbb{R}\backslash\{0\}$ (domain) such that $\varphi(x) = y$. Since $y \in \mathbb{R}^+$, we can take $x = y \in \mathbb{R}\backslash\{0\}$. Note that

$$\varphi(x) = |x| = x = y.$$

Finally, let us find $\ker(\varphi)$:

$$\ker(\varphi) = \{x \in \mathbb{R}\backslash\{0\} : \varphi(x) = 1\} = \{x \in \mathbb{R} : |x| = 1\} = \{-1, 1\}.$$

Example: III. Let H be a subgroup of a group $(G, \star)$, and let $a \in G$. Prove that $H \cong a \star H \star a^{-1}$.

Proof Recall that $a \star H \star a^{-1} = \{a \star h \star a^{-1} : h \in H\}$.

Define a map $\varphi : H \to a \star H \star a^{-1}$ by $\varphi(h) = a \star h \star a^{-1}$ for all $h \in H$.

Now, we prove that φ is an isomorphism:

1. φ is a group homomorphism: Let $x, y \in H$. Then

$$\varphi(x \star y) = a \star (x \star y) \star a^{-1} = (a \star x \star a^{-1}) \star (a \star y \star a^{-1}) = \varphi(x) \star \varphi(y).$$

2. φ is one-one:

$$\ker(\varphi) = \{x \in H : \varphi(x) = e\} = \{x \in H : a \star x \star a^{-1} = e\} = \{e\}.$$

3. φ is onto: Let $y \in a \star H \star a^{-1}$ (codomain). Want to find $x \in H$ (domain) such that $\varphi(x) = y$. Since $y \in a \star H \star a^{-1}$, there is $h \in H$ such that $y = a \star h \star a^{-1}$. We can take $x = h \in H$. Note that

$$\varphi(x) = \varphi(h) = a \star h \star a^{-1} = y.$$

Thus $H \cong a \star H \star a^{-1}$.

Problems: Which of the following maps is an isomorphism/ a monomorphism/ an epimorphism:

1. $\varphi : (\mathbb{Z}, +) \to (2\mathbb{Z}, +)$ defined by $\varphi(x) = 2x$.
2. $\varphi_m : (\mathbb{Z}, +) \to (m\mathbb{Z}, +)$ defined by $\varphi(x) = mx$, where $m \in \mathbb{Z}^+$.
3. $\varphi : (\mathbb{Z}, +) \to (\mathbb{Z}_n, +)$ defined by

$$\varphi(x) = \text{the reminder when } x \text{ divided by } n.$$

Theorem: Let $\varphi : (G, \star) \to (G', \star')$ be a group homomorphism, and Let $H \leq G, H' \leq G'$. Then

1. $\varphi(H) \leq G'$, where

$$\varphi(H) = \{\varphi(h) : h \in H\} \qquad [\textbf{image of } H \textbf{ under } \varphi].$$

2. $\varphi^{-1}(H') \leq G$, where

$$\varphi^{-1}(H') = \{h \in G : \varphi(h) \in H'\} \qquad [\textbf{preimage of } H' \textbf{ under } \varphi].$$

Proof

1. Let $x', y' \in \varphi(H)$. Then

(a). $e' = \varphi(e) \in \varphi(H)$ since $e \in H$.

(b). $x', y' \in \varphi(H)$ implies $x' = \varphi(x), y' = \varphi(y)$ for some $x, y \in H$. Want to show $x' \star' y'^{-1} \in \varphi(H)$, i.e., we must find $h \in H$ such that $\varphi(h) = x' \star' y'^{-1}$. Take $h = x \star y^{-1} \in H$ (since $H \leq G$):

$$\varphi(h) = \varphi(x \star y^{-1}) = \varphi(x) \star' \varphi(y^{-1}) = \varphi(x) \star' (\varphi(y))^{-1} = x' \star' y'^{-1}.$$

2. Let $x, y \in \varphi^{-1}(H')$. Then

(a). $e \in \varphi^{-1}(H')$ since $e' = \varphi(e) \in H'$.

(b). $x, y \in \varphi^{-1}(H')$ implies $\varphi(x), \varphi(y) \in H'$. Want to show $x \star y^{-1} \in \varphi^{-1}(H')$, i.e., we must prove that $\varphi(x \star y^{-1}) \in H'$:

$$\varphi(x \star y^{-1}) = \varphi(x) \star' \varphi(y^{-1}) = \varphi(x) \star' (\varphi(y))^{-1} \in H'.$$

THEOREM: (Cayley) Let $(G, \star)$ be a group and $a \in G$. Then

1. The map $\lambda_a : G \to G$ defined by $\lambda_a(x) = a \star x$ is a permutation in S_G, where

$$S_G = \{\text{all bijections } f : G \to G\}.$$

2. $H = \{\lambda_a : a \in G\} \leq S_G$.
3. $G \cong H$.

Proof

1. It is enough to show that λ_a bijective:

(a). λ_a is onto: Let $y \in G$ (codomain). Want to find $x \in G$ (domain) such that $\lambda_a(x) = y$. Take $x = a^{-1} \star y \in G$. Then

$$\lambda_a(x) = \lambda_a(a^{-1} \star y) = a \star (a^{-1} \star y) = (a \star a^{-1}) \star y = e \star y = y.$$

(b). λ_a is one-one: Let $\lambda_a(x) = \lambda_a(x')$ for some $x, x' \in G$. Then

$$a \star x = a \star x' \Longrightarrow x = x' \text{ (by cancellation law)}.$$

So, $\lambda_a \in S_G$.

2. Let $\lambda_a, \lambda_b \in H$.

   (a). Since $\lambda_e(x) = e \star x = x$ for all $x \in G$. So, $\lambda_e \in H$ which is the identity of S_G.

   (b). Note that,

$$\lambda_{b^{-1}} \circ \lambda_b(x) = \lambda_{b^{-1}}(b \star x) = b^{-1} \star (b \star x) = \lambda_e(x).$$

   Thus, $(\lambda_b)^{-1} = \lambda_{b^{-1}}$. Also,

$$\lambda_a \circ \lambda_b(x) = \lambda_a(b \star x) = a \star (b \star x) = \lambda_{a\star b}(x).$$

   Thus, $\lambda_a \circ \lambda_b = \lambda_{a\star b}$. Now,

$$\lambda_a \circ (\lambda_b)^{-1} = \lambda_a \circ \lambda_{b^{-1}} = \lambda_{a\star b^{-1}} \in H.$$

   Hence, $H \leq S_G$.

3. Define the map $\varphi : G \to H$ by $\varphi(a) = \lambda_a$ for all $a \in G$.

   (a). φ is a group homomorphism: Let $a, b \in G$.

$$\varphi(a \star b) = \lambda_{a\star b} = \lambda_a \circ \lambda_b.$$

   (b). φ is onto:

$$\text{im}(\varphi) = \{\lambda_a : a \in G\} = H.$$

   (c). φ is one-one: Let $\varphi(a) = \varphi(b)$. Then, in particular $\lambda_a(e) = \lambda_b(e)$. That is,

$$a \star e = b \star e \Longrightarrow a = b.$$

   Thus, $G \cong H$.

Cosets and Lagrange's Theorem

Definition: Let $(G, \star)$ be a group, and let $H \leq G$, $a \in G$. The set

$$a \star H = \{a \star H : h \in H\}$$

is called the **left coset** of H that containing a. The set

$$H \star a = \{H \star a : h \in H\}$$

is called the **right coset** of H that containing a. The number of all distinct left cosets of H, denoted by $[G : H]$, is called the **index of** H in G.

Note that:

- $H \star e = e \star H = H$.
- If G is an abelian group, then $H \star a = H \star a$.

Example: I. Consider the symmetric group $(S_3, \circ)$. We know that

$$H = \langle(1\ 2\ 3)\rangle = \{e, (1\ 2\ 3), (1\ 3\ 2)\} \leq S_3.$$

Let us find $H \circ \sigma$ and $\sigma \circ H$ for all $\sigma \in S_3$. Recall,

$$S_3 = \{e, (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)\}.$$

The following are all left and right cosets of H:

$$(1\ 2\ 3) \circ H = (1\ 3\ 2) \circ H = H$$

$$(1\ 2) \circ H = (1\ 3) \circ H = (2\ 3) \circ H = \{(1\ 2), (1\ 3), (2\ 3)\}$$

$$H \circ (1\ 2\ 3) = H \circ (1\ 3\ 2) \circ H = H$$

$$H \circ (1\ 2) = H \circ (1\ 3) = H \circ (2\ 3) = \{(1\ 2), (1\ 3), (2\ 3)\}.$$

Note that, for all $\sigma \in S_3$, we get $\sigma \circ H = H \circ \sigma$.

Example: II. Let us find all the left and right cosets of $H = \langle(1\ 2)\rangle$ in the symmetric group $(S_3, \circ)$. The following are all left and right cosets of $H = \{e, (1\ 2)\}$:

$$(1\ 2) \circ H = H$$

$$(1\ 2\ 3) \circ H = (1\ 3) \circ H = \{(1\ 3), (1\ 2\ 3)\}$$

$$(1\ 3\ 2) \circ H = (2\ 3) \circ H = \{(2\ 3), (1\ 3\ 2)\}$$

$$H \circ (1\ 2) = H$$

$$H \circ (1\ 3) = H \circ (1\ 3\ 2) = \{(1\ 3), (1\ 3\ 2)\}$$

$$H \circ (2\ 3) = H \circ (1\ 2\ 3) = \{(2\ 3), (1\ 2\ 3)\}.$$

Note that, $(1\ 3) \circ H \neq H \circ (1\ 3)$.

Example: III. Let us find all the left and right cosets of $H = 3\mathbb{Z}$ as a subgroup of the group $(\mathbb{Z}, +)$. The following are all left and right cosets of $H = \{\ldots, -6, -3, 0, 3, 6, \ldots\}$:

$$0 + H = H = 0 + H = \{\ldots, -6, -3, 0, 3, 6, \ldots\}$$

$$1 + H = \{\ldots, -5, -2, 1, 4, 7, \ldots\} = H + 1$$

$$2 + H = \{\ldots, -4, -1, 2, 5, 8, \ldots\} = H + 2$$

$$3 + H = \{\ldots, -3, 0, 3, 6, 9, \ldots\} = H + 2 = H$$

$$4 + H = \{\ldots, -2, 1, 4, 7, 10, \ldots\} = H + 4 = 1 + H$$

So, the only distinct left cosets of H are $0 + H, 1 + H, 2 + H$, i.e., $[\mathbb{Z} : 3\mathbb{Z}] = 3$.

Theorem: Let $(G, \star)$ be a group, and let $H \leq G$. The set of all distinct left cosets of H forms a partition of G.

Proof First of all, we have $a \star H \neq \emptyset$ for all $a \in H$ since $a = a \star e \in a \star H$. Now, we need to prove that

1. If $a \star H$ and $b \star H$ are left cosets of H, then either $a \star H = b \star H$ or $a \star H \cap b \star H = \emptyset$.
2. $G = \bigcup_{a \in G} a \star H$.

Let us prove (1): Assume that $a \star H \cap b \star H \neq \emptyset$. Want to prove $a \star H = b \star H$.

Let $x \in (a \star H \cap b \star H)$. Then $x = a \star h_1$ and $x = b \star h_2$ for some $h_1, h_2 \in H$. Hence,

$$a \star h_1 = b \star h_2 \Longrightarrow b^{-1} \star a = \star h_2 \star h_1^{-1} \in H.$$

So, $b^{-1} \star a \star H = H \Longrightarrow b \star b^{-1} \star a \star H = b \star H \Longrightarrow e \star a \star H = b \star H \Longrightarrow a \star H = b \star H$.

Now, we prove (2): It is clear from definition of the left cosets, $\bigcup_{a \in G} a \star H \subseteq G$. On the other hand, assume that $a \in G$. Then $a \in a \star H$ (as we shown previously). So, $a \in \bigcup_{a \in G} a \star H$. It follows that $G \subseteq \bigcup_{a \in G} a \star H$.

THEOREM: Let $(G, \star)$ be a group, and let $H \leq G$. Then $|aH| = H$.

Proof Define a map $f : H \to a \star H$ by $f(h) = a \star h$ for all $h \in H$. We prove that f is bijection.

1. f is onto: Let $y \in a \star H$. Want to find $x \in H$ such that $f(y) = x$. Since $y \in a \star H$, there is $h \in H$ such that $y = a \star h$. So, we can take $x = h$. Note that

$$f(x) = f(h) = a \star h = y.$$

2. f is one-one: Let $f(h) = f(h')$. Then

$$a \star h = a \star h' \Longrightarrow h = h' \quad \text{(cancellation laws in a group)}.$$

THEOREM: [Lagrange Theorem] Let $(G, \star)$ be a finite group, and let $H \leq G$. Then $|H|$ divides $|G|$, and hence $|G| = [G : H]|H|$.

Proof Let $\{a_1 \star H, a_2 \star H, \ldots, a_k \star H\}$ be the set of all distinct left cosets of H in G. That is, $[G : H] = k$. Then

$$G = \bigcup_{j=1}^{k} a_j \star H \Longrightarrow |G| = |a_1 \star H| + |a_2 \star H| + \ldots + |a_k \star H|$$

$$\Longrightarrow |G| = |H| + \ldots + |H| \quad (k - \text{times})$$

$$\Longrightarrow |G| = k|H| = [G : H]|H|.$$

Thus, $|H|$ divides $|G|$.

PROBLEMS: [Applications on Lagrange Theorem] Let $(G, \star)$ be a finite group of order n. Then

1. If $a \in G$, then $a^n = e$.
2. If $n = p$ (prime number), then G is cyclic group.

Normal subgroups

DEFINITION: Let $(G, \star)$ be a group, and let $H \leq G$, $a \in G$. Then H is said to be a **normal subgroup** of G, written $H \trianglelefteq G$ if $a \star H = H \star a$ for all $a \in H$.

Note that:

- Any group $(G, \star)$ has $\{e\}$ and G as normal subgroups.
- If $(G, \star)$ is an abelian group, then any subgroup of G is normal.

Example: I. Consider the subgroup $H = 3\mathbb{Z}$ of the group $(\mathbb{Z}, +)$. Then $H \trianglelefteq \mathbb{Z}$ because $(\mathbb{Z}, +)$ is an abelian group. In fact, $3\mathbb{Z} + a = a + 3\mathbb{Z}$ for all $a \in \mathbb{Z}$.

Example: II. Consider the subgroup $H = \langle (1\ 2) \rangle$ of the group $(S_3, \circ)$. Then $H \ntrianglelefteq S_3$ because $(1\ 3) \circ H \neq H \circ (1\ 3)$. Note that, $H = \{e, (1\ 2)\}$ and

$$(1\ 3) \circ H = \{(1\ 3) \circ e, (1\ 3) \circ (1\ 2)\} = \{(1\ 3), (1\ 2\ 3)\}$$

$$H \circ (1\ 3) = \{e \circ (1\ 3), (1\ 2) \circ (1\ 3)\} = \{(1\ 3), (1\ 3\ 2)\}.$$

Hence, $(1\ 3) \circ H \neq H \circ (1\ 3)$.

Problems: Let $(G, \star)$ be a group, and let $H \leq G$. Then the following statements are equivalent

1. $H \trianglelefteq G$.
2. $x^{-1} \star h \star x \in H$ for all $x \in G$ and $h \in H$.
3. $x^{-1} \star H \star x \subseteq H$ for all $x \in G$.
4. $x^{-1} \star H \star x = H$ for all $x \in G$.

Example: Let $(G, \star)$ be a group. Let us show that $Z(G) \trianglelefteq G$.

1. First, we prove that $Z(G) \leq G$: it is clear that $e \in Z(G)$ since $xe = ex = x$ for all $x \in G$. Now, let $x, y \in Z(G)$. Want to prove that $x \star y^{-1} \in Z(G)$. Note that, for all $a \in G$:

$$(x \star y^{-1}) \star a = x \star a \star y^{-1} \quad \text{since } y^{-1} \star a = a \star y^{-1}$$

$$a \star (x \star y^{-1}) \quad \text{since } x \star a = a \star x.$$

2. Secondly, we prove that $Z(G) \trianglelefteq G$: it is enough to prove that $x^{-1} \star h \star x \in Z(G)$ for all $x \in G$ and $h \in Z(G)$. Note that for all $x \in G$ and $h \in Z(G)$, we have $x \star h = h \star x$ "Definition of $Z(G)$". Consequently,

$$x^{-1}\star x\star h = x^{-1}\star h\star x \Longrightarrow e\star h = x^{-1}\star h\star x \Longrightarrow h = x^{-1}\star h\star x.$$

So, $x^{-1}\star h\star x = h \in Z(G)$ for all $x \in G$ and $h \in Z(G)$.

THEOREM: Let $(G,\star)$ be a group, and let $H \leq G$ with $[G:H]=2$. Then $H \trianglelefteq G$.

Proof Let x be an element in G and $x \notin H$. Then $x\star H \neq H$ and $H\star x \neq H$. Since, there only two left cosets and two right cosets of H "$[G:H]=2$", we get $\{H, x\star H\} = \{H, H\star x\}$. It follows that $H\star x = x\star H$ for every $x \in G$. Thus, $H \trianglelefteq G$.

DEFINITION: A group $(G,\star)$ is said to be **simple** if the only normal subgroups G are $\{e\}$ and G itself.

EXAMPLE: I. The group $(\mathbb{Z}_5,+)$ is a simple group. In fact, the only normal subgroups of $(\mathbb{Z}_5,+)$ are $\{0\}$ and $\mathbb{Z}_5$.

EXAMPLE: II. The group $(\mathbb{R},+)$ is not simple group. In fact, $(\mathbb{Z},+)$ is normal subgroup of $(\mathbb{R},+)$ since $(\mathbb{R},+)$ is abelian group. Moreover, $\mathbb{Z}\neq\mathbb{R}$ and $\mathbb{Z}\neq\{0\}$.

Quotient groups

Assume that $(G,\star)$ is a group, and $H \trianglelefteq G$. Let G/H be the set of all distinct cosets of H in G. For all $a\star H$, $b\star H$ in G/H, define

$$(a\star H)\star(b\star H) = a\star b\star H.$$

Is $\star$ a binary operation on G/H?

Answer: Yes.

We must prove that $\star$ is well-defined binary operation on G/H as follows:

Let $a\star H = a'\star H$ and $b\star H = b'\star H$. Want to prove $a\star b\star H = a'\star b'\star H$.

Since $a \star H = a' \star H$ and $b \star H = b' \star H$, there are two element $h_1, h_2 \in H$ such that $a = a' \star h_1$ and $b = b' \star h_2$. Also, we have $b'^{-1} \star h_1 \star b' \star h_2 \in H$ because $H \trianglelefteq G$. Now,

$$\begin{aligned}(a' \star b')^{-1} \star (a \star b) &= b'^{-1} \star a'^{-1} \star a \star b \\ &= b'^{-1} \star a'^{-1} \star (a' \star h_1) \star (b' \star h_2) \\ &= b'^{-1} \star e \star h_1 \star b' \star h_2 \\ &= b'^{-1} \star h_1 \star b' \star h_2 \in H.\end{aligned}$$

Thus, $(a' \star b')^{-1} \star (a \star b) \in H$ and hence $a \star b \star H = a' \star b' \star H$.

In fact, $(G/H, \star)$ forms a group called the **quotient group (or factor group)** of G by H.

What is the identity of G/H?

Answer: $H = e \star H$, where e is the identity of G.

What is the inverse of $a \star H$ in G/H?

Answer: $(a \star H)^{-1} = a^{-1} \star H$, where a^{-1} is the inverse of a in G.

EXAMPLE: I. We know that $(\mathbb{Z},+)$ is an abelian group. So $6\mathbb{Z} \trianglelefteq \mathbb{Z}$. Let us find the quotient group $\mathbb{Z}/6\mathbb{Z}$:

$$0+6\mathbb{Z} = 6\mathbb{Z} = \{\ldots,-12,-6,0,6,12,\ldots\};$$

$$1+6\mathbb{Z} = \{\ldots,-11,-5,1,7,13,\ldots\};$$

$$2+6\mathbb{Z} = \{\ldots,-10,-4,2,8,14,\ldots\};$$

$$3+6\mathbb{Z} = \{\ldots,-9,-3,3,9,15,\ldots\};$$

$$4+6\mathbb{Z} = \{\ldots,-8,-2,4,10,16,\ldots\};$$

$$5+6\mathbb{Z} = \{\ldots,-7,-1,5,11,17,\ldots\};$$

$$6+6\mathbb{Z} = \{\ldots,-6,0,6,12,18,\ldots\} = 6\mathbb{Z}.$$

So, $\mathbb{Z}/6\mathbb{Z} = \{6\mathbb{Z}, 1+6\mathbb{Z}, 2+6\mathbb{Z}, 3+6\mathbb{Z}, 4+6\mathbb{Z}, 5+6\mathbb{Z}\}$.

EXAMPLE: II. In this example, we construct the quotient group of the abelian group $(\mathbb{Z}_{18},+)$ by the subgroup $H = \langle 6\rangle$. First of all, we have $H = \{0,6,12\}$. Now,

$$0+H = H = \{0,6,12\};$$

$$1+H = \{1,7,13\};$$

$$2+H = \{2,8,14\};$$

$$3+H = \{3,9,15\};$$

$$4+H = \{4,10,16\};$$

$$5+H = \{5,11,17\};$$

$$6+H = \{6,12,0\} = H.$$

So, $\mathbb{Z}_{18}/H = \{H, 1+H, 2+H, 3+H, 4+H, 5+H\}$.

PROBLEMS: Let $(G, \star)$ be a group, and let $H \trianglelefteq G$. Then

1. G is abelian $\Longrightarrow G/H$ is abelian.
2. $G = \langle a \rangle$ (cyclic generated by a) $\Longrightarrow G/H = \langle a \star H \rangle$ (cyclic generated by $a \star H$).
3. G is finite $\Longrightarrow |G/H| = [G : H] = \dfrac{|G|}{|H|}$.
4. There is an epimorphism φ with domain G and $\ker(\varphi) = H$ "such homomorphism is called **canonical or natural** homomorphism".

THEOREM: **[The fundamental theorem of group homomorphisms]** Let $\varphi : (G, \star) \to (G', \star')$ be a group homomorphism. Then $G/\ker(\varphi) \cong \mathrm{im}(\varphi)$.

Proof Let $K = \ker(\varphi)$. Define $\psi : G/K \to \mathrm{im}(\varphi)$ by $\psi(a \star K) = \varphi(a)$ for all $a \star K \in G/K$. First of all, we show that φ is well-defined as a map, i.e. $a \star K = b \star K$ implies $\varphi(a) = \varphi(b)$. Note that

$$\begin{aligned} a \star K = b \star K &\Longrightarrow a = b \star k \text{ for some } k \in K \\ &\Longrightarrow \varphi(a) = \varphi(b \star k) = \varphi(b) \star' \varphi(k) \\ &= \varphi(b) \star' e = \varphi(b) \text{ since } k \in K = \ker(\varphi). \end{aligned}$$

Now, we prove that ψ is an isomorphism

1. ψ is a homomorphism:
$$\begin{aligned} \psi((a \star K) \star (b \star K)) &= \psi(a \star b \star K) = \varphi(a \star b) \\ &= \varphi(a) \star' \varphi(b) = \psi(a \star K) \star' \psi(b \star K). \end{aligned}$$
2. ψ is onto: Clearly from the definition of ψ.
3. ψ is one-one: Want to show that $\ker(\psi) = \{K\}$. Note that
$$\begin{aligned} \ker(\psi) &= \{a \star K : \psi(a \star K) = e'\} = \{a \star K : \varphi(a) = e'\} \\ &= \{a \star K : a \in \ker(\varphi) = K\} = \{K\}. \end{aligned}$$

PROBLEMS: Let $\varphi : (G, \star) \to (G', \star')$ be a group homomorphism. Then

1. φ is onto $\Longrightarrow G/\ker(\varphi) \cong G'$.
2. G is finite $\Longrightarrow |\varphi(G)|$ divides $|G|$.

EXAMPLE: It is clear that $\{0\} \times \mathbb{Z}_2 \trianglelefteq \mathbb{Z}_4 \times \mathbb{Z}_2$ because $\mathbb{Z}_4 \times \mathbb{Z}_2$ is an abelian group. Let us show that $\mathbb{Z}_4 \times \mathbb{Z}_2/\{0\} \times \mathbb{Z}_2 \cong \mathbb{Z}_4$. Define a map $\varphi : \mathbb{Z}_4 \times \mathbb{Z}_2 \to \mathbb{Z}_4$ by $\varphi(m, n) = m$.

Note that

1. φ is a homomorphism: Let $(m, n), (m', n') \in \mathbb{Z}_4 \times \mathbb{Z}_2$. Then
$$\begin{aligned}\varphi((m, n) + (m', n')) &= \varphi(m + m', n + n') = m + m' \\ &= \varphi(m, n) + \varphi(m', n').\end{aligned}$$
2. φ is onto:
$$\begin{aligned}\mathsf{im}(\varphi) &= \{\varphi(m, n) : (m, n) \in \mathbb{Z}_4 \times \mathbb{Z}_2\} \\ &= \{m : (m, n) \in \mathbb{Z}_4 \times \mathbb{Z}_2\} = \mathbb{Z}_4.\end{aligned}$$
3. $\ker(\varphi) = \{0\} \times \mathbb{Z}_2$:
$$\begin{aligned}\ker(\varphi) &= \{(m, n) \in \mathbb{Z}_4 \times \mathbb{Z}_2 : \varphi(m, n) = 0\} \\ &= \{(m, n) \in \mathbb{Z}_4 \times \mathbb{Z}_2 : m = 0\} \\ &= \{(0, n) \in \mathbb{Z}_4 \times \mathbb{Z}_2\} = \{0\} \times \mathbb{Z}_2.\end{aligned}$$

Thus, $\mathbb{Z}_4 \times \mathbb{Z}_2/\ker(\varphi) \cong \mathbb{Z}_4$.

EXERCISES

1. Let $(G, \star)$ be a finite group of order n. Then
   (a). Let $n = pq$ (p, q are a prime numbers) and let $H, K \leq G$ (unique subgroups) such that $|H| = p, |K| = q$. Then G is cyclic group.
   (b). If $n = p^h$ (p is a prime number, and $h \in \mathbb{Z}^+$), then G has an

element of order p.

2. Which of the following maps is an isomorphism/ a monomorphism/ an epimorphism:

(a). $\varphi : (S_n, \circ) \to (\mathbb{Z}_2, +)$ defined by

$$\varphi(\sigma) = \begin{cases} 1, & \text{if } \sigma \text{ odd;} \\ 0, & \text{if } \sigma \text{ even.} \end{cases}$$

(b). $\varphi : (\mathbb{R}\backslash\{0\}, \cdot) \to (\{-1, 1\}, \cdot)$ defined by

$$\varphi(x) = \begin{cases} 1, & \text{if } x > 0; \\ -1, & \text{if } x < 0. \end{cases}$$

3. Let $\varphi : (G, \star) \to (G', \star')$ be a group homomorphism, and let $a \in G$. Prove that

(a). If G is an abelian group, then $\varphi(G)$ is an abelian group.

(b). If G is an abelian group, and φ is onto, then G' is an abelian group.

(c). If $o(a) = n$, then $o(\varphi(a))|n$.

4. Prove that $(\mathbb{C}, +) \cong (\mathbb{R} \times \mathbb{R}, +)$.

5. Let $(G, \star)$ be a cyclic group, namely $G = \langle a \rangle$. Prove that

(a). if G is finite of order n, then $G \cong \mathbb{Z}_n$.

(b). if G is infinite, then $G \cong \mathbb{Z}$.

6. Let $\varphi : (G, \star) \to (G', \star')$ be a group isomorphism, and let $a \in G$. Prove that

(a). G is abelian if and only if G' is abelian.

(b). $o(a) = o(\varphi(a))$.

(c). G is cyclic if and only if G' is cyclic.

7. Show that

(a). $(\mathbb{Z}, +) \ncong (\mathbb{Q}, +)$.

(b). $(\mathbb{Q},+) \ncong (\mathbb{Q}\backslash\{0\},\cdot)$.

(c). $(\mathbb{R}\backslash\{0\},\cdot) \ncong (\mathbb{Q}\backslash\{0\},\cdot)$.

(d). $(\mathbb{R}\backslash\{0\},\cdot) \ncong (\mathbb{C}\backslash\{0\},\cdot)$.

(e). $(D_4,\cdot) \ncong (\mathbb{Z}_8,+)$.

(f). $(\mathbb{Z}_2 \times \mathbb{Z}_2,+) \ncong (\mathbb{Z}_4,+)$.

8. Prove or disprove

(a). There is a homomorphism between any two groups.

(b). There is a finite group isomorphic to an infinite group.

(c). Any two finite groups of the same order are isomorphic.

(d). There is an abelian group isomorphic to a non-abelian group.

(e). The map $\varphi : G \to G$ defined by $\varphi(x) = x^{-1}$ is a homomorphism for any a group $(G,\star)$.

(f). For any two groups $(G,\star)$ and $(G',\star)$, we have $G \times G' \cong G' \times G$.

(g). The map $\varphi : (\mathbb{C},+) \to (\mathbb{R},+)$ defined by $\varphi(x+iy) = x+y$ is an epimorphism.

(h). There are 5 subgroups of $4\mathbb{Z}/64\mathbb{Z}$ under the usual addition.

(i). Let $(\mathbb{Z},+)$ be the group of integers. The map $\varphi : \mathbb{Z}\times\mathbb{Z} \to \mathbb{Z}$ defined by $\varphi(a,b) = a-b$ is a homomorphism and $\ker(\varphi) = \{(a,a) : a \in \mathbb{Z}\}$.

(j). $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$ for any positive integer n (under addition).

9. Let $(G,\star)$ be a finite group of order pq, where p and q are prime numbers. Prove that any non trivial subgroup of G is cyclic.

10. Let $(G,\star)$ be a group, and let $H \leq G$. Define

$$N(H) = \{x \in G : x^{-1} \star H \star x = H\} \text{ [}\textbf{Normalizer of } H \text{ in } G\text{]}.$$

Show that

(a). $N(H) \leq G$.

(b). $H \trianglelefteq N(H)$.

(c). $N(H) = G$ if and only if $H \trianglelefteq G$.

11. Let $\varphi : (G, \star) \to (G', \star')$ be a group homomorphism. Prove that

(a). $\ker(\varphi) \trianglelefteq G$.

(b). $H \trianglelefteq G \Longrightarrow \varphi(H) \trianglelefteq \varphi(G)$.

(c). $H' \trianglelefteq G' \Longrightarrow \varphi^{-1}(H') \trianglelefteq G$.

12. Prove that the intersection of any family of normal subgroups of a group $(G, \star)$ is again normal subgroup of G.

13. Let $(G, \star)$ be a group. Prove that

(a). $H, K \leq G$ and $H \trianglelefteq G \Longrightarrow H \star K \leq G$.

(b). $H \trianglelefteq G$ and $K \trianglelefteq G \Longrightarrow H \star K \trianglelefteq G$.

14. Prove or disprove

(a). $(H, \star) \leq (G, \star)$, and H is an abelian subgroup $\Longrightarrow H \trianglelefteq G$.

(b). $(H, \star) \leq (G, \star)$, and G is an abelian group $\Longrightarrow N(H) = G$.

(c). All subgroups of an abelian group are normals.

(d). All subgroups of group with prime order are normals.

(e). If $(G, \star)$ a group and $H \trianglelefteq G$ such that G/H is finite $\Longrightarrow G$ is finite.

(f). There are 6 normal subgroups in the dihedral group D_4.

15. Let $(G, \star)$ be a group, and let $H_1, H_2, \ldots, H_k$ be normal subgroups of G such that $H_1 \cap H_2 \cap \ldots \cap H_k = \{e\}$. Prove that there is a monomorphism $\varphi : G \to G/H_1 \times G/H_2 \times \ldots G/H_k$.

16. Let $(G, \star)$ be a group, and let $H \leq G, K \trianglelefteq G$. Prove that

$$H/(H \cap K) \cong H \star K/K.$$

17. Let $(G, \star)$ be a group, and let $H, K \trianglelefteq G, H \leq K$. Prove that

(a). $K/H \trianglelefteq G/H$

(b). $(G/H)/(K/H) \cong G/K$.

18. Which of the following groups are simple?

(a). $(\mathbb{Z}, +)$.

(b). $(\mathbb{Z}_p, +)$, where p is a prime number.

(c). $(S_3, \circ)$.

(d). $(D_4, \cdot)$.

(e). $(\mathbb{Z} \times \mathbb{Z}, +)$.