

: رياضيات 6 (نظرية الزمرة)

: كيمياء (تربية عام)

7 :

: د. هدير الجندی

Then H is not a subgroup of G , since $\sqrt{2} \in H$ but $\sqrt{2} \cdot \sqrt{2} = 2 \notin H$. Also K is not a subgroup, since $z \in K$ but $z^{-1} \notin K$.

Definition (Center of a group)

The center $Z(G)$ of a group G is

$$Z(G) = \{a \in G \mid ax = xa \text{ for all } x \in G\}$$

Theorem

The center of a group G is a subgroup of G .

Proof

(1) $Z(G)$ is a non-empty set:
since $ex = xe$ for all $x \in G$, then $e \in Z(G)$.

(2) Let $a, b \in Z(G)$. Then

$$ax = xa \text{ for all } x \in G,$$

$$bx = xb \text{ for all } x \in G.$$

Hence
$$x(ab^{-1}) = (xa)b^{-1} = (ax)b^{-1} = (a(b^{-1}b)x)b^{-1}$$

Then H is not a subgroup of G , since $\sqrt{2} \in H$ but $\sqrt{2} \cdot \sqrt{2} = 2 \notin H$. Also K is not a subgroup, since $z \in K$ but $z^{-1} \notin K$.

Definition (Center of a group)

The center $Z(G)$ of a group G is

$$Z(G) = \{a \in G \mid ax = xa \text{ for all } x \in G\}$$

Theorem

The center of a group G is a subgroup of G .

Proof

(1) $Z(G)$ is a non-empty set:

since $ex = xe$ for all $x \in G$, then $e \in Z(G)$

(2) Let $a, b \in Z(G)$. Then

$$ax = xa \text{ for all } x \in G,$$

$$bx = xb \text{ for all } x \in G.$$

Hence

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

$$\begin{aligned} &= a(b^{-1}(xb))b^{-1} = a(b^{-1}(xb)b^{-1}) \\ &= a(b^{-1}x) = (ab^{-1})x. \end{aligned}$$

Thus $(ab^{-1}) \in Z(G)$.

Definition

Let a be a fixed element of a group G . The Centralizer of a in G , $C(a)$, is the set of all elements in G that commute with a :

$$C(a) = \{g \in G \mid ga = ag\}.$$

Theorem

For each a in a group G , the Centralizer of a is a subgroup of G .

Proof. A proof similar to that of the previous theorem ?!

Exercises

(1) If H and K are subgroups of G , show that $H \cap K$ is a subgroup of G .

(2) Let $G = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mid a, b, c, d \in \mathbb{Z} \right\}$ under addition.

Let $H = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in G \mid a+b+c+d=0 \right\}$.

Prove that H is a subgroup of G .

What if 0 is replaced by 1?

(3) Let $H = \{ A \in GL(2, \mathbb{R}) \mid \det A \text{ is a power of } 2 \}$

Show that H is a subgroup of $GL(2, \mathbb{R})$.

(4) Let H be a subgroup of \mathbb{R} under addition.

Let $K = \{ 2^a \mid a \in H \}$. Prove that K is

a subgroup of \mathbb{R}^* under multiplication.

(5) Let $G = GL(2, \mathbb{R})$ and let

$$H = \left\{ \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \mid a, b \text{ are nonzero integers} \right\}$$

Under the operation of matrix multiplication
Prove or disprove that H is a subgroup
of $GL(2, \mathbb{R})$.

(6) Let $H = \{a+bi \mid a, b \in \mathbb{R}, ab \geq 0\}$. Prove
or disprove that H is a subgroup
of $GL(2, \mathbb{R})$.

(7) Consider the elements

$$A = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \text{ and } B = \begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix} \text{ from}$$

$SL(2, \mathbb{R})$. Find $|A|$, $|B|$, and $|AB|$.

Chapter 4
Cyclic group

Definition

A group G is called cyclic if there is an element $a \in G$ such that

$$G = \{ a^n \mid n \in \mathbb{Z} \}.$$

Remarks

(1) The element a is called a generator

(2) We say G is cyclic group generated by a and write $G = \langle a \rangle$.

Example

The set of integers \mathbb{Z} under addition is cyclic.

Both 1 and -1 are generators.

Example

The set $\mathbb{Z}_n = \{0, 1, \dots, n-1\}$ for $n \neq 1$ is cyclic group under addition modulo n . 1 and -1 are generators.

Example

$$\mathbb{Z}_8 = \langle 1 \rangle = \langle 3 \rangle = \langle 5 \rangle = \langle 7 \rangle.$$

Note 2 is not generator, since

$$\langle 2 \rangle = \{0, 2, 4, 6\} \neq \mathbb{Z}_8.$$

Theorem

Let G be a group and let $a \in G$. If a has infinite order, then all distinct powers of a are distinct group elements. If a has finite order, say n , then $\langle a \rangle = \{e, a, a^2, \dots, a^{n-1}\}$ and $a^i = a^j$ if and only if n divides $i-j$.

Proof

If a has infinite order, there is no nonzero n such that $a^n = e$.

Since $a^i = a^j$ implies $a^{i-j} = e$, we must have $i-j=0$ and the first statement of the theorem is proved.

Now assume that $|a| = n$. We will prove that $\langle a \rangle = \{e, a, a^2, \dots, a^{n-1}\}$.

We first note that the elements $e, a, a^2, \dots, a^{n-1}$ are distinct. For if $a^i = a^j$, $0 \leq j < i \leq n-1$, then $a^{i-j} = e$. But this contradicts the fact that n is the least positive integer such that $a^n = e$.

Now suppose that $a^k \in \langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$. By division algorithm, there exist integers q and r such that

$$k = qn + r \text{ with } 0 \leq r < n.$$

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

Thus $a^k \in \{e, a, a^2, \dots, a^{n-1}\}$.

This shows that $\langle a \rangle \subseteq \{e, a, a^2, \dots, a^{n-1}\}$.

Hence $\langle a \rangle = \{e, a, a^2, \dots, a^{n-1}\}$.

Next, we assume that $a^i = a^j$ and prove that n divides $i-j$. We first observe that $a^i = a^j$ implies $a^{i-j} = e$. Again, by the division algorithm, there are integers q and r such that

$$i-j = qn + r \quad \text{with } 0 \leq r < n.$$

Then, $a^{i-j} = a^{qn+r}$. Hence

$$e = a^{i-j} = a^{qn+r} = (a^n)^q a^r = a^r.$$

Since n is the least positive integer such that $a^n = e$, we must have $r=0$, so that n divides $i-j$.

Conversely, if $i-j = nq$, then

$$a^{i-j} = a^{nq} = (a^n)^q = e, \text{ so that } a^i = a^j.$$

Corollary 1

For any group element
 $|a| = |\langle a \rangle|$

Corollary 2

Let G be a group and let a
be an element of order n in G . If
 $a^k = e$, then n divides k .

Proof. Since $a^k = e = a^0$, then the
previous theorem implies that
 n divides $k - 0$.

Exercises

- (1) List the elements of the subgroups $\langle 20 \rangle$ and $\langle 10 \rangle$ in \mathbb{Z}_{30} .
 - (2) List the elements of the subgroups $\langle 3 \rangle$ and $\langle 15 \rangle$ in \mathbb{Z}_{30} .
 - (3) Let $G = \langle a \rangle$ and let $|a| = 24$. List all generators for the subgroup of order 8.
 - (4) Let G be a group and let $a \in G$. Prove that $\langle a^{-1} \rangle = \langle a \rangle$.
 - (5) Let G be a finite group. Show that there exist a fixed positive integer n such that $a^n = e$ for all $a \in G$.
-
-