4th abstract algebra

Sunday, 26. September 2021 13:28

$(ab)^{-1} = h$ abelian group

$h \cdot ab = e$

$h \cdot a = b^{-1}$

$h = b^{-1} \cdot a^{-1}$

Cyclic group.

Lemma: Let G be a group, Let H_i $i \in I$ be a collection of subgroup of G.

Then the intersection: $H = \bigcap_{i \in I} H_i$

is a subgroup of G.

H_1: a, b, ab H_2: a, b, ab

H: ab

Proof: H is not empty. $e \in H_i$, $i \in I$.

H is a subgroup iff H is closed under multiplication and inverse

Suppose $g, h \in H$ $g, h \in H_i$, $i \in I$

$hg \in H$ $hg \in H_i$

$gh \in H$ gh

Suppose $g \in H$ $g \in H_i$ $i \in I$

$g^{-1} \in H$ $g^{-1} \in H_i$ $i \in I$

$G \supseteq H_1 \supseteq H_2 \supseteq H_3$

$\{s\} \in G$ $H_1 = G$ $H_4 = \{s\}/\{s\}$

$\{s\} \in H_1$ $\{s\} \in H_2$ $\{s\} \in H_2$

Definition: Let G be a group and let S be a subset of G.

– Lemma

subgroup $H = \langle S \rangle$ generated by S is equal to

$\{\emptyset\} \leftarrow \{\emptyset\} \times \{e\}$ ✓

$\{e\}$ ✗

the smallest subgroup of G that contains S. $H_1 \cap H_2 \cap H_3$

the smallest subgroup of G that contains S. $H_1 \cap H_2 \cap H_3$

$S=\{a\}$ $H=\{a, a^{-1}, e\}$ $H=\langle S\rangle$

proof: Suppose H_i $i \in I$ is the collection of subgroups that contains S $H = \bigcap_{i \in I} H_i$ is a subgroup of G.

$\{e\}$

H contains S.

H is the smallest subgroup of G that contains S. □

Lemma: Let G be a group. S be a non-empty subset of G.

The subgroup H generated by S is equal to the (smallest subset of G, containing S, that is closed under multiplication and inverses condition. taking.)

$\{a\}$ $\{a\} \times \{a, a^{-1}\}$ $\{a, a^{-1}, e\}$

Proof: Let K be the smallest subset of G. closed under multiplication and taking inverses. $\Rightarrow$ subgroup

H is closed under multiplication and taking inverses.

① $K \subseteq H$

H is smallest subgroup of G. K is a subgroup of G.

② $H \subseteq K$.

$H = K$ ✓ □

Definition: Let G be a group. we say that a subset S of G generates G. if the smallest subgroup of G that contains S is G.

Definition: Let G be a group. we say that G is cyclic if it is generated by one element.

it is generated by one element.

Example. $G = \langle a \rangle$ be a cyclic group. $a \in G$, $a \cdot a \in G$, $a \cdot a \cdot a \in G$

$G = \{a^i \mid i \in \mathbb{Z}\}$ $\quad a^i a^j = a^{i+j} = a^j \cdot a^i$

Definition: Let G be a group, let $g \in G$ be an element of G

The order of g = cardinality of the subgroup generated by g.

$\mathrm{Ord}(g)$

$a \neq b$

$A = \{a, a^2, \dots, a^5 = e\}$ subgroup

$B = \{b, b^2, \dots, b^7 = e\}$ subgroup

$G: \{A, B, ab, ab^2 \dots a^2b, \dots, a^5b^7\}$ ★

$a \in G \quad \mathrm{Ord}(a) = 5 \quad \mathrm{Ord}(b) = 7.$

$\langle a^m b^n \rangle$, $0 \le m \le 5$, $0 \le n \le 7$

Lemma: Let G be a finite group. and $g \in G$.
Then the order of g divides the order of G.

proof: Langrange's theorem.

Lemma: Let G be a group of prime order. Then G is cyclic.

proof. $|G| = 1$ ✓

pick $a \in G$. $a \neq e$. $\mathrm{Ord}(a) \neq 1$

$e \cdot e = e$ $\{e\}$

$a \cdot a = e$ $\{a, a, e\}$.

$a \cdot a = *$ $\{a, a, *, \Delta, e\}$

$*\cdot\Delta = e$

$|a| \mid |G|$ — prime.

$|a| = 1$ or $|G|$

$|a| = |G| \Rightarrow |G|$ cyclic.

7

$b \to 1, 7$

□

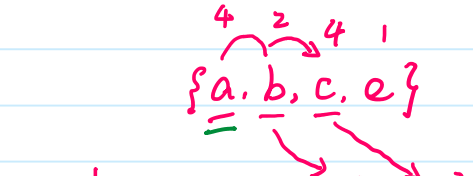
4 2 4 1

$|G| = |G| \Rightarrow |G|$ cyclic. 4

1 2 3 5 7 $\cdots \Rightarrow$ Cyclic

4. = Ord (G) cyclic

2×2.



*	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 ✓

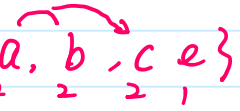
not cyclic

1, 2, 4

△ |G| | |G| 4

$\frac{4}{0} = \mathbb{Z}$

*	e	a	b	c
e	e	a	b	c
a	a	e	c ax	b
b	b	c	e bx	a
c	c	b	a	e ✓



1 2 3 4 5 6 7 $\cdots$ smallest non-abelian group

Abelian group $ab \neq ba$

Lemma. Let G be a group. $g \in G$. be an element of G.
Then the order of g is the smallest positive number k. such that $g^k = e$.

Finite: l is finite

proof: $B = \langle g \rangle \quad \{g^i, i \in \mathbb{Z}\}$.

$g^l = e \quad B = \{e, g, g^2 \cdots g^{l-1}\}$. closed under multiplication and taking inverses.

1) $g^i, g^j \in B \quad g^i g^j = g^{i+j} \quad i+j < l \quad g^{i+j} \in B$.

$i+j \geq l \quad g^l = e \Rightarrow g^{i+j} = g^{i+j-l} g^l = g^{i+j-l}$ ($g^l = e$). $0 \leq i+j-l < l$

$g^{i+j-l} \in B$.

2) $g^i \quad g^{l-i} g^i = g^l = e \quad g^{l-i} = (g^i)^{-1}$

$g^{l-i} \in B$.

infinite.

infinite:

$a^k = e$. k, infinite number

$\mathbb{Z}$: $\text{ord}(1) = \text{infinity}$.

$\text{Ord}(g) = \text{infinity}$.

k smallest

$|B| < k$ $\{e, g, g^2 \cdots g^{k-1}\}$ must have some repetitions.

$g^a = g^b$ $a \neq b$ g

$a, b \in [0, k-1]$ $a < b$.

$g^{b-a} = e$. $b-a < k$. this contradicts. $g^k = e$.

$g^* = e$ k smallest. □

Lemma: Let G be a finite group of order n. g be an element of G

$g^n = e$

proof: $g^k = e$ $k = |g|$, $k \mid \text{ord}(g) \Rightarrow k \mid n$. $n = km$

$g^n = g^{km} = (g^k)^m = e^m = e$. □

下下周 23.10