0 Group Theory   2019-03-18 周一.

$\boxed{\text{Group}}$, Ring、Field.   (Abstract Algebra)
($G, \circ$) ($G, +, \times$)   (Modern Algebra)
近世.

- What is a group?
- 什么是群?
- "群论"有什么用?
  - 指定研究领域 (PL; Automata Theory)
  - 深入研究领域.

~~Sp.~~ Groups:

- Cyclic Group
- Permutation Groups
- D_n (Dihedral Group)
  (Tetrahedron)
- S_n; A_n
- Groups of small orders
  (≤ 8.)

(1) order of G
(2) Order of element of G
(3) subgroups of G
(4) Normal subgroups of G.

Applications.

- 15-puzzle
- Cube (Rubik cube).

① Cyclic Group. $G = \langle g \rangle = \{ g^k : k \in \mathbb{Z} \}$

Thm 9.7 All cyclic groups of infinite

$G_\infty \cong \mathbb{Z}$

$|G| = \infty \Rightarrow G \cong \mathbb{Z} \quad (\mathbb{Z}, +)$

$(g^0 = e, g^1, g^2, \dots)$

$(0, 1, 2, \dots)$

Thm 9.8 $|G| = n \Rightarrow G_n \cong \mathbb{Z}_n \quad (\mathbb{Z}_n, +)$.

$(g^0 = e, g^1, \dots g^{n-1})$

$(0, 1, \dots n-1)$

We want to know. ① generators of G; ② order of element in G

③ Subgroups of G.

$G \cong \mathbb{Z}$.:

① Thm. ~~Infinite~~ and only has.

$(\mathbb{Z}, +)$ has two generators: g and g^{-1}.

$G = \langle g \rangle$, $|G| = \infty$.

Pf. (1) g and g^{-1} are generators of G.

(2) Suppose g^k $(k \neq \pm 1)$ is also a generator of G.

$G = \langle g^k \rangle$.

$g \in G \Rightarrow \exists\, l \in \mathbb{Z}.\ g = g^{kl} \Rightarrow kl = 1$

$\Rightarrow k = \pm 1,\ l = \pm 1.$ $\boxtimes$

---

② Orders of elements in $G = \langle g \rangle$.

Thm. ~~Each element~~ The order of each element of $G_\infty = \langle g \rangle$ ~~has~~ is infinite.

Pf. By contradiction.

$|(g^k)| = l. \Rightarrow g^{kl} = e.$ $\boxtimes$

$k \in \mathbb{Z}. \quad (l > 0, l \in \mathbb{Z})$

③ Subgraphs of $G_\infty = \langle g \rangle$.

2

Thm 4.10: Every subgroup of a cyclic group is cyclic.

In its proof: we know that

$\Rightarrow k \in \mathbb{N}$.

Any subgroup has the form $\langle g^k \rangle$ for $k \in \mathbb{Z}$.

Valid for both G_∞ and G_n. $\langle g^k \rangle = \langle g^{-k} \rangle$

Thm. For $G_\infty = \langle g \rangle$, each subgroup has the ~~form~~ $\langle g^k \rangle$ for ~~each~~ $n \in \mathbb{N}$.

pf:

(1) $\langle g^0 \rangle$, $\langle g^1 \rangle$, $\langle g^2 \rangle$, $\langle g^3 \rangle$ ... $\langle g^k \rangle$ ... for $k \in \mathbb{Z}$.

for $\mathbb{Z}$: $\{0\}$. $\mathbb{Z}$. $2\mathbb{Z}$. $3\mathbb{Z}$. ... $k\mathbb{Z}$, ... for $k \in \mathbb{Z}$.

(2) ~~$\langle g^k \rangle \neq \langle g^l \rangle$ if $k \neq l$. $k, l \in \mathbb{N}$.~~

We need to show that:

$$\text{if } k \neq l,\ (k,l) \in \mathbb{N} \Rightarrow \langle g^k \rangle \neq \langle g^l \rangle.$$

pf. By contradiction.

$\langle g^k \rangle = \langle g^l \rangle$.

(1) $g^k \in \langle g^l \rangle$. (2) $g^l \in \langle g^k \rangle$

$\exists t \in \mathbb{N}, k = lt$ $\Rightarrow k \mid l$.

$\Rightarrow l \mid k$

$\Rightarrow l = k$. $\boxtimes$.

3 Exercises: ~~Problem~~ 4.4

4.4 -1: (c) $(\mathbb{Q},+)$ is cyclic. (X)

Pf. By contradiction.

Suppose that : $\mathbb{Q} = \langle \frac{a}{b} \rangle$.

$\frac{a}{2b} \notin \langle \frac{a}{b} \rangle$. ($(\frac{a}{b})$ is arbitrary.)

(d) If every proper subgroup of a group G is cyclic, then G is a cyclic group. (X)

Pf. Counterexamples:

- Example 4.7 (S_3).
- $G = \langle e, a, b, ab = ba \rangle$

$a^2 = b^2 = e$,

$ab = ba$.

(e). A group with a finite number of subgroups is finite. (✓)

Pf. By contradiction.

To show: If G is infinite, then G has an infinite number of subgroups. ($G = \{a_1, a_2, \dots\}$)

(1) If some element $a \in G$ ~~has~~: $|a| = \infty$.

$\exists a \in G$: $|a| = \infty$. $\langle a \rangle \cong \mathbb{Z}$.

$\Rightarrow$ has an infinite number of subgroups.

(2) $\forall a \in G$: ~~|a| = n.~~ $|a|$ is finite.

~~$G = \{a_1$~~ $\langle a_1 \rangle$.

Infinite number. $\left\{ \begin{array}{l} \langle a_2 \rangle \\ \vdots \\ \langle a_k \rangle \dots \end{array} \right.$

There are infinite groups where each element has finite order,

(f) Additional

(4f) There are infinite groups where each element has finite order.

pf.

(1) $\mathbb{Q}/\mathbb{Z}$.

(2) $\{ z \in \mathbb{C} : z^n = 1 \text{ for some } n \in \mathbb{N}\}$.

$$\left| z = \operatorname{cis}\left(\frac{2k\pi}{n}\right) \right| = n.$$

Explanation:

$(\mathbb{Q}, +)$ is a group.

$(\mathbb{Z}, +) \leq (\mathbb{Q}, +)$, $(\mathbb{Z}, +) \trianglelefteq (\mathbb{Q}, +)$.

$\mathbb{Q}/\mathbb{Z}$.

- Each element of $\mathbb{Q}/\mathbb{Z}$ is of the form: $\frac{m}{n} + \mathbb{Z}$. $m, n \in \mathbb{Z}$.
- The representatives of $\mathbb{Q}/\mathbb{Z}$ are rational numbers in $[0,1) \Rightarrow \mathbb{Q}/\mathbb{Z}$ is infinite.
- $n \cdot \left(\frac{m}{n} + \mathbb{Z}\right) \overset{?}{=} m + \mathbb{Z} \overset{?}{=} 0 + \mathbb{Z}$.

$\Rightarrow$ The order of $\frac{m}{n} + \mathbb{Z}$ is at most n.

(5) $G_n = \langle g \rangle \cong \mathbb{Z}_n \quad (\mathbb{Z}_n, +)$.

① Generators,

② order of element in G

③ subgroups of G_n

Thm 4.13 $G_n = \langle g \rangle$. Then

$$|g^k| = \frac{n}{(k,n)}.$$

Pf. $|g^k| = t$ is the $\boxed{\text{smallest}}$ positive integer that

$$g^{kt} = e.$$

Goal: $t = \dfrac{n}{(k,n)}$.

(1) $t \mid \dfrac{n}{(k,n)}$

$$(g^k)^{\frac{n}{(k,n)}} = g^{\frac{k}{(k,n)} \cdot n}$$

$$= (g^n)^{\frac{k}{(k,n)}}$$

$$= e$$

$$\Rightarrow t \le \frac{n}{(k,n)}.$$

(2) $\dfrac{n}{(k,n)} \mid t$.

$$g^{kt} = e$$

$$\Rightarrow n \mid kt.$$

$$\Rightarrow \frac{n}{(k,n)} \mid \frac{k}{(k,n)} t$$

$$\Rightarrow \frac{n}{(k,n)} \mid t \quad \because \left(\left(\frac{n}{(k,n)}, \frac{k}{(k,n)}\right) = 1\right)$$

$$\boxed{\Rightarrow \frac{n}{(k,n)} \le t}$$

$$\Rightarrow t = \frac{n}{(k,n)}.$$

~~Thm~~ Corollary 4.14: The generator of $G_n = \langle g \rangle$ ($\mathbb{Z}_n$): g^k.

$$1 \le \boxed{k} < n, \quad (k, n) = 1$$

Ex 4.12.

6 Find a cyclic group with exactly one generator. $\{e\}$.

two $\mathbb{Z}$. 1

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

n. $\phi(m) = n$. $|G| = m$.

Ex. 4-24

p, q : primes

$\mathbb{Z}_{pq}$. $\phi(pq) = \phi(p)\phi(q) = (p-1)(q-1)$.

Thm. (ϕ function formulas)

① $(m,n)=1 \Rightarrow \phi(mn) = \phi(m)\phi(n)$

② p is a prime, $k \geq 1$

$$\phi(p^k) = p^k - p^{k-1}.$$

$$n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$$

$$\phi(n) = \phi(p_1^{k_1}) \cdot \phi(p_2^{k_2}) \cdots \phi(p_r^{k_r})$$

$$= \phi(p_1^{k_1} - p_1^{k_1-1}).$$

$$n = \prod_{1 \le i \le r} p_i^{k_i}$$

$$\phi(n) = \prod_{1 \le i \le r} \phi(p_i^{k_i})$$

$$= \prod_{1 \le i \le r} (p_i^{k_i} - p_i^{k_i-1})$$

Pf. Chapter 11. of "A Friendly Introduction to Number theory" (Joseph H. Silverman)

Thm 11-1 of

7 Subgroups of $C_n = \langle g \rangle$, $(\mathbb{Z}_n, +)$.

Example: $\mathbb{Z}_6 = \langle 0, 1, 2, 3, 4, 5 \rangle$

$\langle 0 \rangle = \{0\}$.

$\langle 1 \rangle = \mathbb{Z}_6$

$\langle 2 \rangle = \{0, 2, 4\} = 2\mathbb{Z}_6$

$\langle 3 \rangle = \{0, 3\} = 3\mathbb{Z}_6$

$\langle 4 \rangle = \{0, 2, 4\} = 4\mathbb{Z}_6 = 2\mathbb{Z}_6$

$\langle 5 \rangle = \{0, 1, 2, 3, 4, 5\} = \mathbb{Z}_6$.

$\langle 6 \rangle = \{0\}$

$\langle 1 \rangle, \langle 2 \rangle, \langle 3 \rangle, \langle 6 \rangle$.

$\langle 5 \rangle, \langle 4 \rangle, 6$.

How many subgroups?

$6 = 2^1 \times 3^1$

$\# = 2 \times 2 = 4$

$\boxed{1 \quad 2 \quad 3 \quad 6}$

$12 = 2^2 \times 3^1$

$\# = 3 \times 2 = 6$

1 2 3 4 6 12

~~Try!~~

$\langle g^k \rangle = \langle g^l \rangle$ (To find the relation between k, l)

$g^k \in \langle g^l \rangle$ and $g^l \in \langle g^k \rangle$.

$\exists t: g^k = g^{lt}$. $\quad \exists s: g^l = g^{ks}$

$k \equiv lt \pmod{n}$ $\quad l \equiv ks \pmod{n}$.

Each subgroup of C_n has the form $\langle g^k \rangle$ where $0 \le k \le n-1$.

Thm: 8 $G_n = \langle g \rangle$. $\langle g^k \rangle = \langle g^{(k,n)} \rangle$.

pf. (1) $g^k \in \langle g^{(k,n)} \rangle$

$\because (k,n) \mid k$.

(2) $g^{(k,n)} \in \langle g^k \rangle$

Bezout's Identity. (Thm 2.10).

$(k,n) = kx + ny$ for some $x, y \in \mathbb{Z}$.

$$g^{(k,n)} = g^{(kx+ny)} = g^{kx} \cdot g^{ny} = g^{kx}.$$

Col. ~~Thm~~: ~~Any~~ Each subgroup of C_n has the form ~~is generated by~~ $\langle g^d \rangle$, where d is ~~some~~ a positive divisor of n.

~~Duplication?~~

(逆命题)

(1) For every positive divisor d of n, there is a subgroup of the form $\langle g^d \rangle$. $\Longrightarrow$ $\langle g^d, g^{2d}, \dots g^{\frac{n}{d}\cdot d} \rangle$, $g^{\frac{n}{d}\cdot d} = e$.

(2) Duplication?

~~For a~~ For two positive divisors d_1, d_2 of n.

$d_1 \neq d_2$, $\langle g^{d_1} \rangle \neq \langle g^{d_2} \rangle$.

$$|\langle g^{d_1} \rangle| = \frac{n}{d_1}$$

$$|\langle g^{d_2} \rangle| = \frac{n}{d_2}.$$

Thm: ~~$G_n = \langle g \rangle$~~. Each subgroup of C_n has the form $\langle g^d \rangle$, where d is a unique positive divisor of n.

$\langle g^k \rangle = \langle g^{(k,n)} \rangle$.

Thm 9: # subgroups of C_n = # of positive divisors of n.

$n = \prod_{1 \le i \le r} p_i^{k_i}$.

$\# = \Sigma (k_i + 1)$.

$12 = 2^2 \times 3$.

$\# = 3 \times 2 = 6$

~~In an infinite cyclic group, w~~

Q1: Thm: $C_\infty = \langle g \rangle$.

$\langle g^k \rangle \subseteq \langle g^l \rangle \iff l \mid k$.

$(\langle g^k \rangle \le \langle g^l \rangle)$

Q2: Thm: $C_n = \langle g \rangle$

$\langle g^k \rangle \subseteq \langle g^l \rangle \iff (l, n) \mid (k, n)$.

$(\langle g^k \rangle \le \langle g^l \rangle)$