离散数学习题课

第七讲 —— 群论（一）

Subgroups

- Three theorems on identifying subgroups:

  Let G be a group, H be a <u>nonempty subset</u> of G.

  (1) $H \leq G$ if and only if

  a) $\forall a, b \in H$, we have $ab \in H$, and

  b) $\forall a \in H$, we have $a^{-1} \in H$.

  (2) $H \leq G$ if and only if

  $\forall a, b \in H$, we have $ab^{-1} \in H$.

  (3) If H is <u>finite</u>, then $H \leq G$ if and only if

  $\forall a, b \in H$, we have $ab \in H$.

Cosets

Important results on cosets:

For any group G, and subgroup $H \leq G$, we have

(1) $eH = He = H$;

(2) $\forall a \in G, a \in aH \cap Ha$;

(3) $\forall a \in G, aH \approx H \approx Ha$;

(4) $\forall a, b \in G, a \in bH \iff aH = bH \iff a^{-1}b \in H$;

(5) $\forall a, b \in G, a \in Hb \iff Ha = Hb \iff ab^{-1} \in H$;

(6) Let $S = \{aH \mid a \in G\}, T = \{Ha \mid a \in G\}$, then S and T are both partitions of G, and $|S| = |T|$.

Lagrange's Theorem

- Let G be a <u>finite</u> group, $H \leq G$, then

$$|G| = |H| \cdot [G : H]$$

  where $[G : H] = |\{aH \mid a \in G\}|$.

Comments:

Let G be a finite group,

- For any $H \leq G$, we have $|H| \mid |G|$
- For any $a \in G$, since $\langle a \rangle \leq G$ and $|a| = |\langle a \rangle|$, we have

$$|a| \mid |G|$$

- Every group with a prime order is a cyclic group

Coset decomposition

- Let G be a group, $H \leq G$, with $[G:H] = n$, then

  $$G = a_1H \cup a_2H \cup \cdots \cup a_nH$$

  where, for all $1 \leq i,j \leq n, a_i \in G, a_i^{-1}a_j \notin H (i \neq j)$.

  Similarly, we have

  $$G = Ha_1 \cup Ha_2 \cup \cdots \cup Ha_n$$

  where, for all $1 \leq i,j \leq n, a_i \in G, a_i a_j^{-1} \notin H (i \neq j)$.
- For any group G and $H \leq G$, we have

  $$G = \bigcup_{g \in G} gH = \bigcup_{g \in G} Hg$$

Problems

1. Let A, B be two subgroups of G, show that

$$AB \leq G \iff AB = BA$$

where $AB = \{ab \mid a \in A \wedge b \in B\}$

2. Let G be a group, $a, b \in G, |a| = p,$ where *p* is prime, show that

$$a \notin \langle b \rangle \implies \langle a \rangle \cap \langle b \rangle = \{e\}$$

3. Let A, B be finite subgroups of G, show that

$$|AB| = \frac{|A|\,|B|}{|A \cap B|}$$

Problems (cont.)

4. Let G be a group, define a binary relation (called the <u>conjugacy</u> relation) as follow:

$$\forall a, b \in G, aRb \iff \exists x(x \in G \land a = xbx^{-1})$$

Show that

(1) The conjugacy relation is an equivalence;

(2) For all $a \in G, |[a]_R| = [G : Z(a)]$

where $Z(a) = \{x \mid x \in G \land xa = ax\}$ (called the <u>centralizer</u> of a), and $[a]_R$ is called the <u>conjugacy class</u> of a, denoted as $\bar{a}$.

Comments

- 群的中心(The center of a group):

$$Z(G) = \{a \mid \forall x(x \in G \rightarrow xa = ax)\}$$

- 群的分类方程(Conjugacy class equation)：

设 G 是有限群，$Z(G)$ 是 G 的中心。设 G 中至少含有两个元素的共轭类有 k 个，且 $a_1, a_2, \cdots, a_k$ 分别为这 k 个共轭类的代表元素，则

$$|G| = |Z(G)| + [G : Z(a_1)] + [G : Z(a_2)] + \cdots + [G : Z(a_k)]$$

Problems (cont.)

5. Show that

$$|\bar{a}| = 1 \iff a \in Z(G)$$

6. Let G be a group with $|G| = p^s$, where p is prime, and $s \in \mathbb{Z}^+$, show that $p \mid |Z(G)|$.
7. Let G be an abelian group, show that

$$H = \{x \mid \exists n \in \mathbb{N}(x^n = e)\} \leq G$$

8. Let G be a group, $a \in G, |a| = mn, (m,n) = 1$, show that

$$\exists b, c \in G(a = bc = cb \wedge |b| = m \wedge |c| = n)$$

Problems (cont.)

9. Let G be a finite group with $|G| = n$, show that

$$n \text{ is odd} \iff \forall a \in G, \exists b \in G(b^2 = a)$$

Thank you

Any questions?