

第十一次习题课讲义

1. 上节课内容回顾

① 群定义

1. 结合律 4^* 交换性

2. 单位元

3. 可逆元

② 用乘法表描述有限群

③ 群同态 $\xrightarrow{+}$ 单射 $\xrightarrow{+}$ 单同态

$\xrightarrow{+}$ 满射 $\xrightarrow{+}$ 满同态

$\xrightarrow{+}$ 双射 $\xrightarrow{+}$ 同构

④ 低阶群分类

⑤ 子群定义和性质 (Lagrange 定理)

⑥ 一类特殊子群——循环子群 结构是怎样的?

⑦ Cayley 定理

2. 习题内容解答

3. 拓展内容

① 群的作用 (主要讲作用在集合上)

② 群作用实例 1. $\text{Int}(G)$ 与 $\text{Aut}(G)$

2. 子群在 G 上的作用 (商群)

群在集合上的作用

定义: 记 G 为群, X 为集合

G 在 X 上的作用是群族 $\{L_g: X \rightarrow X \mid L_g \text{ 为双射 } g \in G\}$

$$\text{满足 } L_{g' \circ g} = L_{g'g} \quad \forall g, g' \in G$$

一般记 $g \cdot x \triangleq L_g(x)$ 即为 g 在 x 上的作用

例子 1: 取 $X = G$ 本身

$$L_g: X \rightarrow X \text{ 为左平移}$$

$$\text{由结合律知 } L_{g' \circ g} = L_{g'g}$$

这说明 G 在自身上有一个左平移作用

例子 2: 取 $X = \{1, 2, \dots, n\}$ $G = S_n$

$$L_g: X \rightarrow X$$

$$i \mapsto g(i)$$

$$\text{由于 } g' \circ g(i) = g'(g(i)) \quad (\text{置换定义})$$

故说明 S_n 在 $\{1, 2, \dots, n\}$ 有一个置换作用

为了描述群在集合上的作用的好处, 我们还需要其它概念.

定义: 轨道: $\forall x \in X$, 我们称 x 所在的轨道为 x 的子集 $\{L_g(x) \mid g \in G\} = L_x$

显然利用 G 在 X 上的作用, 我们可以给出一个 X 的分划 $\bigcup_{x \in X} L_x$ (等价关系为 $x \sim y \Leftrightarrow \exists g \in G \text{ s.t. } L_g(x) = y$)

我们称其为 x 关于 G 的作用的轨道分解

稳定子群: $\forall x \in X$, 我们称 G 的子群 $\{g \in G \mid g \cdot x = x\}$ 为 x 关于这个作用的稳定子群.

Lemma: $|Gx| \mid |G|$ 若 G 为有限群

$$\text{且 } |G|/|Gx| = |L_x| \quad (\text{在 } G \text{ 上定义等价关系 } g_1 \sim g_2 \Leftrightarrow L_{g_1}(x) = L_{g_2}(x))$$

从而我们有了轨道公式 (针对右陪集 G)

$$|G| = \sum_{x \in X/\sim} |Gx| = \sum_{x \in X/\sim} |G|/|Gx|$$

而我们为什么要研究 G 在 X 上的作用, 因为它对研究 G 本身的结构有重要意义! (著名的 Sylow 定理就是用此证明的!)

这里举一个简单的应用

Thm: P -群有非平凡中心 (G 为 P -群是指 $|G| = p^n$)

pf 考察 G 在 G 上的共轭作用

$$L_g: G \rightarrow G$$

$$x \mapsto gxg^{-1}$$

$$G_x = \{ g \in G \mid gxg^{-1} = x \} \quad \text{而 } |G_x| = |G| \iff x \text{ 为中心}$$

从而由轨道公式立刻得到结论。

2. 接下来举 n 个 X 拥有比集合 ~~结构~~ 更多的结构时, 群在 X 上的作用有什么特点。

$$\textcircled{1} \text{Int}(G), \text{Aut}(G)$$

我们定义所有 $G \rightarrow G$ 的自同构为 $\text{Aut}(G)$

而利用某些元素诱导的共轭同构 $G \rightarrow G$, 把这些共轭同构放在一起组成 $\text{Int}(G)$

$$g \cdot x \mapsto gxg^{-1}$$

群理论的一个基本问题是说何时 $\text{Int}(G) = \text{Aut}(G)$, 然后判断 $\varphi: G \rightarrow G$ 是不是共轭同构也需要花一番功夫。

即看 $g \varphi g^{-1} = \varphi$ 是否存在这样的 g

那么很自然的状态就可以在 $\text{Aut}(G)$ 上有一个 G -作用

$$g \cdot \varphi = \varphi \circ g$$

$$\text{其中 } Lg(x) = g \circ g^{-1}$$

从而立刻得到 $\text{Aut}(G)$ 即为 G 在这个作用下的轨道

$$\text{所以 } \text{Ind}(G) = \text{Aut}(G) \iff \text{轨道仅一个}$$

而 G 在 X 上的作用轨道仅一个的情况我们称 G 作用是传递的

$$\text{即 } \forall x \in X, \text{ 存在 } x_0 \in X \text{ 有 } g_x \in G \text{ s.t. } g_x \cdot x_0 = x$$

② ~~子群在商集上的作用~~

本节最终目标是证明 Γ^2 所导一一定是交换群 (Γ 为素数)
和 Γ^3 所导的结构

记 $C(G)$ 为 G 的中心

Lemma: $G/C(G)$ 如果是有限循环群, 那么 G abelian.

首先 $G/C(G)$ 是什么?

作为集合它是 $G/\sim$ 等价关系为 $g_1 \sim g_2 \iff g_1 g_2^{-1} \in C(G)$

而它还有乘法结构 $\overline{g_1 g_2} = \overline{g_1} \overline{g_2}$

这是良定义的因为 $g_1 g_2 (g'_1 g'_2)^{-1} = g_1 g_2 g'_2{}^{-1} g'_1{}^{-1}$

$$\text{由于 } g_2 \sim g'_2 \Rightarrow g_2 g'_2{}^{-1} \in C(G) \Rightarrow (g_1 g_2)(g'_2 g'_2{}^{-1}) \in C(G)$$

进一步它还构成一个群.

再来看引理的证明 $G/C(G) = \langle a \rangle$

那么 G 中元素可写为 $a^n t$ $n \in \mathbb{N}, t \in C(G)$

$$\text{由于 } (a^n t)(a^{n'} t') = (a^{n+n'}) (a^n t a^{n'} t') \text{ 故 } G \text{ 交换}$$

之前证明 p^2 -阶群 $|C(G)| \neq 1$

$|C(G) \cap C(G)| = 1$ or p 均为循环群

从而 G 为交换群

但是到了 p^3 阶群，就不一定交换了

比如 8 阶群 Q_8, D_8 均不是交换群

在以后学习半直积之后，我们可以对 p^3 阶群进行完全分类

现在我想说 ~~最多只有 2 种非交换 p^3 阶群~~ (在同构意义下). (当然 $p=2$ 时还有 2 种 Q_8 与 D_8)

若 $|C(G)| = p$ 如果 G 不是 abelian 的 p^3 阶群 接下来利用以下引理即可得到 p^3 阶群的表示

Lemma. p^3 阶非交换群的 $C(G)$ 由 $\langle aba^{-1}b^{-1}, a, b \rangle$ 生成

$$\text{即 } C(G) = \langle a, b \rangle$$

即 $G/\langle a, b \rangle$ 交换 $\Rightarrow [a, a] \neq 1$ 而 $[a, b] \neq 1$

现在我们先对 $p=2$ 来进行粗略地研究

证明最多有 2 种非交换 p^3 阶群 (在同构意义下)

首先 $|C(G)| = p$ 如果 G 不交换的话

再说明 $[a, a] = \langle aba^{-1}b^{-1}, a, b \rangle$ 生成的子群 $= C(G)$

因为 $G/\langle a, a \rangle$ p^2 阶群 交换 故 $C(G) \supset \langle a, a \rangle$

假设 G 无 p^2 阶元 那么全是 p 阶元或单位元, 记 $C(G) = \langle c \rangle$, a, b 为不在 $C(G)$ 中的 p 阶元

由于 $aba^{-1}b^{-1} = c^k$ 也为 p 阶元 故 $k \neq 1$

从而 $G = \langle a, b, c \mid aba^{-1}b^{-1} = c, a^p = ca, b^p = bc \rangle$

若 G 有 p^2 阶元 设 a 记 $C(a) = \langle b \rangle$ b 为不在 $\langle a \rangle$ 中 $C(a)$ 中的元素.

由于 $b \notin \langle a \rangle$ 故 b 不可能是 p 阶元

$$aba^{-1}b^{-1} \in \langle C \rangle \quad \text{于是 } aba^{-1}b^{-1} = c \Rightarrow ab = cba$$

~~$$aba^{-1}b^{-1} = c \Rightarrow ab = cba$$~~

$$aba^{-1} = cb$$

$$bab^{-1} = a^{-1}c$$

~~$$bab^{-1} = a^{-1}c$$~~

若 $\forall b \in \langle a \rangle + C(a) \quad aba^{-1}b^{-1} = 1 \Rightarrow a \in C(a)$ 矛盾

故我们取 $aba^{-1}b^{-1} \neq 1 \in \langle C \rangle$ 不妨记 $c = aba^{-1}b^{-1}$

这里我们需要说明 $bab^{-1} \in \langle a \rangle$ (这用到 Sylow 定理)

$$\text{从而 } bab^{-1} = a^k \quad 1 \leq k \leq p^2 \quad \text{代入 } c = aba^{-1}b^{-1} = a^{k-1} \text{ 为 } p \text{ 阶元} \in C(a)$$

~~$$\Rightarrow p(k-1) \text{ 是 } p^2 \text{ 的倍数}$$~~ or

$$\Rightarrow \frac{p^2}{(p^2, k-1)} = p \Rightarrow (p^2, k-1) = p \Rightarrow p | k-1 \quad \text{但 } p \nmid k-1 \Rightarrow k = p+1 \quad 1 \leq k \leq p-1$$

而 $l = | \sim p-1$ 个输出的群是同构的

$$\text{故 } C(a) = 1$$

$$\text{从而 } \text{这个非交换群为 } \{ \langle a, b \mid b^p ab = a^{p+1}, |a| = p^2, |b| = p \rangle \}$$