2024-12-06

习题课讲义：子群，陪集，拉格朗日定理与循环群结构

1) 群是有理数集，实数集，复数集关于乘法构成代数结构的抽象。设 $*$ 为集合 G 上的二元运算，$(G,*)$ 称为一个群若满足

G1 G 关于运算 $*$ 封闭。$\forall a,b\in G \Rightarrow a*b\in G$

G2 结合律：$\forall a,b,c\in G$，$(a*b)*c=a*(b*c)$

G3 单位元：存在 $e\in G$ 使得 $e*a=a*e=a$ $\forall a\in G$.

G4 逆元存在：对任意 $a\in G$，存在 $b\in G$ 使得 $a*b=b*a=e$.

例

1. $(\mathbb{Z},+)$，$(\mathbb{Q},+)$，$(\mathbb{R},+)$，$(\mathbb{C},+)$

2. $(\mathbb{Q}^\times,*)$，$(\mathbb{R}^\times,*)$，$(\mathbb{C}^\times,*)$ $\mathbb{Q}^\times=\mathbb{Q}\setminus\{0\}$.

3. $(S_n,\circ)$ 置换群

   $(A_n,\circ)$ 偶置换构成的交错群

4. $(GL_n(\mathbb{R}),\cdot)$ 一般线性群，由所有 $n\times n$ 可逆矩阵构成

5. $S(A):=\{\phi: A\to A \mid \phi \text{ 为双射}\}$

   称为集合 A 的变换群

6. 单位根群：$U_n=\{x\in\mathbb{C} \mid x^n=1\}$

7. $(\mathbb{Z}_n,+)$ 模 n 剩余类群

   $\bar{a}=\{a+nk \mid k\in\mathbb{Z}\}$

   $\bar{a}+\bar{b}=\overline{a+b}$.

2) 子群：设 $(G,*)$ 为一个群，H 为 G 的子集，假如 H 对于运算 $*$ 也构成一个群，则称 H 为 G 的子群。

定理：设 H 为群 $(G,*)$ 的一个子集，H 构成 G 的一个子群的充分必要条件为 (i) $a,b\in H \Rightarrow a*b\in H$

(ii) $a\in H \Rightarrow a^{-1}\in H$

注：(i)(ii) 两个条件不仅用一个条件代替，(iii) $a,b\in H \Rightarrow ab^{-1}\in H$。当 H 为有限子集时，该条件不仅可减弱为 (i)，即

命题：一个群 G 的一个不空有限子集 H 构成 G 的一个子群的充分必要条件为：$\forall a,b\in H \Rightarrow a*b\in H$ (*)

证明：只需证明充分性。假设有限集合 $H\subseteq G$ 满足条件 (*)。我们只需推导条件 (ii)。$\forall a\overset{\neq e}{\in} H$，考虑序列

$$a, a^2, a^3, \cdots \in H$$

因为 H 为有限集合，存在 $m>n$ 使得 $a^n=a^m$

因为 $a\in G$，则有 $a^{m-n}=e \Rightarrow a^{-1}=a^{m-n-1}\in H$ 图

3) 拉格朗日定理 (Lagrange theorem)

设 G 为一个有限群，且 H 为 G 的子群，则

$$\mathrm{card}(H) \mid \mathrm{card}(G)$$

整除

证明该定理之前，先介绍陪集的概念。

注：$\mathrm{card}(G)$ 为 G 的元素个数，有时记为 $|G|$

设 H 为 G 的子群，定义关系 $\sim_H$：

$$\forall a,b\in G,\quad a\sim_H b \Leftrightarrow a^{-1}b\in H$$

Claim 1. $\sim_H$ 是 G 上等价关系.

证明. 自反性：

① 因为 $a^{-1}a=e\in H$，所以 $a\sim_H a$

② 对称性：

若 $a\sim_H b$，即 $a^{-1}b\in H \Rightarrow (a^{-1}b)^{-1}=ba^{-1}\in H$

所以 $b\sim_H a$.

③ 传递性：假设 $a\sim_H b$，$b\sim_H c$，即

$a^{-1}b\in H$ 且 $b^{-1}c\in H$，则 $a^{-1}bb^{-1}c=a^{-1}c\in H$

$\Rightarrow a\sim_H c$. 图

定义：(左陪集)

$\forall a\in G$，由 a 所在的等价类 $\bar{a}=\{b\in G \mid a\sim_H b\}$

称 a 的左陪集.

设 H_1,H_2 为 G 的两个子集，定义：$H_1\cdot H_2=\{$  $\mid a_1\in H_1, a_2\in H_2\}$

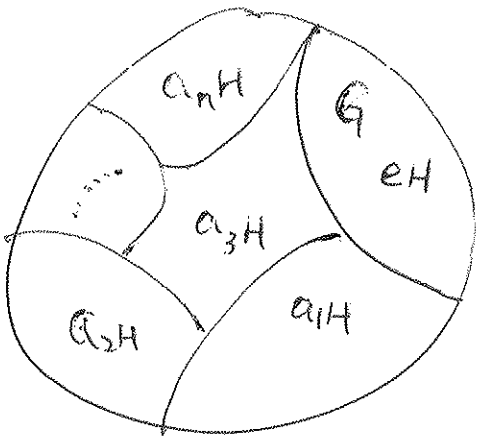
Claim 2. $\bar{a}=a\cdot H=\{ah\mid h\in H\}$

证明. $\forall b\in\bar{a}$，即 $a^{-1}b\in H$，$a^{-1}b=h \Rightarrow b=ah\in aH$

$\Rightarrow \bar{a}\subseteq aH$

$\forall g\in aH$，$g=ah \Rightarrow a^{-1}g\in H \Rightarrow a\sim_H g \Rightarrow g\in\bar{a}$

$\Rightarrow aH\subseteq\bar{a}$. 图



所以 $G = \bigcup_{a\in G} \bar{a} = \bigcup_{a\in G} aH$.

下面证明，任意两个陪集之间都存在双射

Lemma 1. $\forall a, b \in G$，存在双射

$$\varphi: aH \longrightarrow bH.$$
$$g \longmapsto ba^{-1}g.$$

证明 良定义：$g = ah \Rightarrow ba^{-1}g = ba^{-1}ah = bh \in bH$

单射：若 $\varphi(g_1) = \varphi(g_2)$ 即 $ba^{-1}g_1 = ba^{-1}g_2$，由左消去律

$$\Rightarrow g_1 = g_2,$$

满射：$\forall g \in bH$，$g = bh$，其中 $h \in H$，则有 $ah \in aH$

$$\varphi(ah) = g.$$

Lagrange定理证明：

因为 H 为 G 的子群，则 G 关于等价关系 $\sim_H$ 的分划为 $|G/\sim_H|$ 个元素个数相同的左陪集，因为 $H = eH$ 也为一个左陪集，所以

$$|G| = |H| \cdot |G/\sim_H|.$$

推论1. 设 G 为有限群，对任意 $a \in G$，a 的阶数必为 $|G|$ 的因子.

证明：a 的阶数 $= |\langle a \rangle|$，$|\langle a \rangle|$ 整除 $|G|$.

↳由 a 生成的 G 的子群

推论2. 设 G 为有限群，且 $|G|$ 为素数，则 G 为循环群.

证明：任取 $g^{\neq e} \in G$，考虑子群 $H = \langle g \rangle$，由于 $|H| \mid |G|$

$$\Rightarrow |H| = |G| \Rightarrow G = H = \langle g \rangle.$$

循环群的结构：

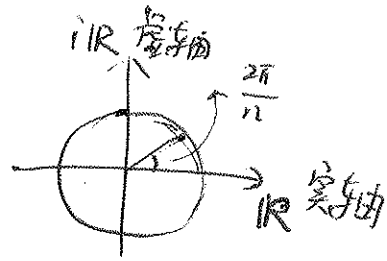
定义：若一个群 G 的每一个元素都是 G 的一某固定元 a 的乘方，则 G 叫做循环群，即 $G=\langle a\rangle$. a 称为 G 的生成元.

例子：

① $(\mathbb{Z},+)=\langle 1\rangle$

② $(\mathbb{Z}_n,+)=\langle \bar{1}\rangle$

③ $(U_n,\cdot)=\langle e^{\frac{2\pi i}{n}}\rangle$



定理：设 G 是由 a 生成的循环群. 则

1) 若 a 的阶数为无限的，$G\cong(\mathbb{Z},+)$ 同构；

2) 若 a 的阶数为整数 n，$G\cong(\mathbb{Z}_n,+)$ 同构.

证明：1). 设 a 的阶数是无限的，这时

$$a^h=a^k \iff h=k \qquad (*)$$

这样定义映射：

$$\varphi:\ G\to\mathbb{Z},\quad a^k\mapsto k$$

φ 是同态，因为 $a^k a^h=a^{k+h}$ 即 $\varphi(a^k\cdot a^h)=k+h=\varphi(a^k)+\varphi(a^h)$

由(*)，φ 为单射，φ 显然为满射. 所以 φ 是 G 到 $(\mathbb{Z},+)$ 的同构.

2). 设 a 的阶数为 n, 即 $a^n = e$. 则有

$$a^h = a^k \iff n \mid h-k. \qquad (*)$$

因为 $a^h = a^k \iff a^{h-k} = e \iff n \mid h-k$
(n 为最小整数使 $a^n = e$)

定义: $\varphi: G \to (\mathbb{Z}_n, +)$

$$a^k \mapsto \bar{k}$$

良定义: $a^{k+nm} = a^k \cdot (a^n)^m = a^k \cdot e^m = a^k$

$a^h \cdot a^k = a^{h+k} \to [h+k] = \bar{h} + \bar{k} \Rightarrow \varphi$ 是同态

φ 显然为满射, 由 $(*)$ 知 φ 为单射.

所以 $G \cong (\mathbb{Z}_n, +)$. ☐

命题: 设 $G = \langle g \rangle$, 且 $|G| = n$

若 $b = g^m$ 且 $\gcd(m, n) = 1$, 则 $G = \langle b \rangle$

证明: $b \in G \Rightarrow \langle b \rangle \subseteq G$

$\forall g \in G$, 因为 $\gcd(m, n) = 1$, 则存在整数 u, v 使得

$$um + vn = 1$$

则

$$g^1 = g^{um+vn} = (g^m)^u (g^n)^v = b^u \in \langle b \rangle$$

$$\Rightarrow G \subseteq \langle b \rangle \quad \text{所以} \quad G = \langle b \rangle$$ ☐

命题：若 G 为循环群，则 G 的任意子群 H 也是循环群。

证明：设 $G=\langle g\rangle$，则 H 中的所有元素皆为形如 g^z。

我们取 z_0 为绝对值最小的正整数使得 $g^{z_0}\in H$。

$\forall b\in H$，$b=g^z$，由带余除法知：$z=q\cdot z_0+r$

其中 $|r|<|z_0|$。$g^r=g^{z-q\cdot z_0}=g^z\cdot(g^{z_0})^{-q}\in H$

由 z_0 的极小性，知 $r=0$，则 $g^z=(g^{z_0})^q$。

$\Rightarrow b=(g^{z_0})^q \Rightarrow H=\langle g^{z_0}\rangle$。

注：由上命题可以知道，循环群的子群结构是完全清楚的。

若 G 为无限循环群，其所有子群也是无限循环群

若 G 为有限群，由 Lagrange 定理，其子群的阶数整除 $|G|$。例如 $|G|=12$，则 G 的所有子群为：

$G=\langle g\rangle$，$g^{12}=e$

$H_1=\langle e\rangle$

$H_2=G$

$H_3=\langle g^2\rangle$ $|H_3|=6$

$H_4=\langle g^3\rangle$ $|H_4|=4$

$H_5=\langle g^4\rangle$ $|H_4|=3$

$H_6=\langle g^6\rangle$ $|H_6|=2$

不可能有阶为 7 阶，8，9，10，11 阶子群 $\Rightarrow$