17.5 群的分解

- 陪集及其性质
- Lagrange定理
- Lagrange定理的应用
- 共轭关系与共轭类
- 群的分类方程

陪集定义及其实例

陪集定义 G 为群，$H \le G$, $a \in G$,

右陪集 $Ha = \{ ha \mid h \in H \}$

Ha 中的 a 称为该陪集的代表元素

实例：

S_3, $H = \{ (1), (12) \}$

$H(1) = H(12)$

$H(13) = H(132) = \{ (13), (132) \}$

$H(23) = H(123) = \{ (23), (123) \}$

陪集的性质

定理 G 为群，H 是 G 的子群，则

(1) $He = H$;

(2) $a \in Ha$;

(3) $Ha \approx H$;

(4) $a \in Hb \Leftrightarrow Ha = Hb \Leftrightarrow ab^{-1} \in H$

(5) 在G上定义二元关系 R, $aRb \Leftrightarrow ab^{-1} \in H$，则 R 为等价关系，且 $[a]_R = Ha$

(6) $a, b \in G$, $Ha \cap Hb = \varnothing$ 或 $Ha = Hb$，$\cup Ha = G$

说明：定义左陪集 $aH = \{ ah \mid h \in H \}$

性质类似 $a \in bH \Leftrightarrow aH = bH \Leftrightarrow a^{-1}b \in H$

陪集性质的证明

(4) $a \in Hb \Leftrightarrow Ha = Hb$

证 必要性. $a \in Hb \Leftrightarrow a = h'b \Leftrightarrow b = h'^{-1}a$

$$ha \in Ha \Rightarrow ha = hh'b \in Hb$$

$$hb \in Hb \Rightarrow hb = hh'^{-1}a \in Ha$$

(5) $Ha = [a]$

证 $b \in [a] \Leftrightarrow aRb \Leftrightarrow ab^{-1} \in H$

$$\Leftrightarrow Ha = Hb \Leftrightarrow b \in Ha$$

Lagrange定理的引理

引理　H 的左陪集和右陪集数相等

$$f: T \to S,\ f(Ha) = a^{-1}H,$$

T, S 分别为右和左陪集的集合

f 的良定义性与单射性:

$$Ha = Hb \Leftrightarrow ab^{-1} \in H \Leftrightarrow (a^{-1})^{-1}b^{-1} \in H$$

$$\Leftrightarrow a^{-1}H = b^{-1}H \Leftrightarrow f(Ha) = f(Hb)$$

H 在 G 中的 **指数** $[G:H]$:

H 在 G 中的右（或者左）陪集数

Lagrange定理及推论

lagrange定理： $|G| = |H|[G:H]$

证明：令 G 的不同的陪集为 $Ha_1, Ha_2, \ldots, Ha_r$，

$$|G| = |Ha_1| + |Ha_2| + \ldots + |Ha_r| = |H|\, r = |H|\,[G:H]$$

说明：适用于有限群，逆不一定为真.

推论

(1) 群的元素的阶是群的阶的因子.

证明：构造子群 $\langle a \rangle$，$|\langle a \rangle| = |a|$.

(2) 素数阶群一定是循环群.

证明：$|G| = p$，$p>1$，存在非单位元 a，

$|a|$ 是 p的因子，只能是 $|a| = p$. 故$G = \langle a \rangle$.

Lagrange定理的应用

例1 6 阶群必含3 阶元.

证 若存在 a，$|a| = 6$, 则 a^2为3 阶元.

假若没有6 阶元. 如果没有3 阶元，则$\forall a \in G$, $a^2 = e$, 则 G 为Abel 群，$\{a, b, ab, e\}$为子群，与 Lagrange 定理矛盾.

Lagrange定理的应用

例2 6 阶群在同构意义上只有 2 个.

证明思路：

若 G 含6 阶元，是循环群.

若不含 6 阶元，则含 3 阶元 a,

取 $c\notin\{e, a, a^2\}$, 则 c, ac, a^2c 两两不等（消去律）

可以证明 $G=\{e, a, a^2, c, ac, a^2c\}$ 同构于S_3.

推广

10 阶群只有 2 个，2 p 阶群只有 2 个.

4 阶群只有 2个：循环群和 Klein 四元群.

共轭关系与共轭类

定义 设 G 为群，定义 G 上二元关系 R，

$$aRb \Leftrightarrow \exists x\,(x\in G,\ b = xax^{-1})$$

称 R 为 G 上的共轭关系

共轭关系是 G上等价关系，等价类为共轭类

共轭类的性质：

$$a\in C \Leftrightarrow \bar{a} = \{a\}$$

$$|\bar{a}| = [G : N(a)],$$

其中

$$N(a) = \{x \mid x\in G,\ xa = ax\}$$

证明

证明 $|\bar{a}| = [G : N(a)]$

其中 $N(a) = \{ x \mid x \in G,\ xa = ax \}$

证 $\forall x, y \in G$,

$$x\,a\,x^{-1} = y\,a\,y^{-1} \Leftrightarrow a\,x^{-1}y = x^{-1}y\,a$$

$$\Leftrightarrow x^{-1}y \in N(a) \ \Leftrightarrow x\,N(a) = y\,N(a)$$

两种分解的实例

S_3={ (1), (12), (13), (23), (123), (132) }, H={ (1), (12) },

按照陪集分解：

H (13) = { (13), (132) }，H (23) = { (23), (123) }

{ { (1), (12) }, { (13), (132) }, { (23), (123) } }

按照共轭类分解：

{ { (1) }, { (12), (13), (23) }, { (123), (132) } }

区别：

(1) 陪集分解等价类等势，共轭类分解不等势

(2) 共轭类中置换的轮换结构相同，陪集分解不是

(3) 陪集分解计数导致 Lagrange定理，共轭类分解计数导致群的分类方程

群的分类方程

群的分类方程

G 为群，C 为中心，G 中至少含两个元素的共轭类有 k 个，$a_1, a_2, \ldots, a_k$为代表元素，则

$$|G| = |C| + [G:N(a_1)] + [G:N(a_2)] + \ldots + [G:N(a_k)]$$

证明：$|C| = l,\ C = \{ a_{k+1}, a_{k+2}, \ldots, a_{k+l} \}$

$$G = \overline{a_1} \cup \overline{a_2} \cup \ldots \cup \overline{a_k} \cup \{a_{k+1}\} \cup \{a_{k+2}\} \cup \ldots \cup \{a_{k+l}\}$$

$$|G| = [G:N(a_1)] + [G:N(a_2)] + \ldots + [G:N(a_k)] + |C|$$

注：$N(a_i) < G$

群分类方程的应用

例3 $|G|=p^s$，p为素数，则 $p \mid |C|$.

证明

$$|G|=|C|+[G:N(a_1)]+[G:N(a_2)]+\dots+[G:N(a_k)]$$

对于$i=1, 2, \dots, k$,

$[G:N(a_i)]$是$|G|$的因子，$|G|=p^s$,

$[G:N(a_i)]=p^t$ 或者 $[G:N(a_i)]=1$

$[G:N(a_i)]=1 \Rightarrow \bar{a}_i=\{a_i\} \Rightarrow a_i \in C$，矛盾

$p \mid [G:N(a_i)] \Rightarrow p \mid |C|$

17.6 正规子群与商群

- 正规子群及判定
  - 定义
  - 判别定理
  - 判别法
- 商群
  - 定义及其实例
  - 性质

正规子群及其判定

正规子群：$H \le G$,，且$\forall a \in G$，$aH = Ha$. 记为 $H \trianglelefteq G$.

判定定理： $N \le G$, 则下述条件等价

(1) N 是 G 的正规子群

(2) $\forall g \in G$, $gNg^{-1} = N$

(3) $\forall g \in G$, $\forall n \in N$, $gng^{-1} \in N$

证：(1) $\Rightarrow$(2): $gN = Ng \Rightarrow gNg^{-1} = N$

(2) $\Rightarrow$(3): $gng^{-1} \in gNg^{-1} = N$

(3)$\Rightarrow$(1):

$ng \in Ng \Rightarrow n \in N, g^{-1} \in G \Rightarrow g^{-1}ng \in N \Rightarrow ng \in gN$

$gn \in gN \Rightarrow n \in N, g \in G \Rightarrow gng^{-1} \in N \Rightarrow gn \in Ng$

正规子群及其判定

判定方法：

(1) 判定定理

(2) $|N| = t$, N 是G 的唯一 t 阶子群

(3) 指数为2 的子群

证 (2) 任取 $g \in G$, $gNg^{-1} \leq G$, 且$|gNg^{-1}| = |N|$，从而得到 $gNg^{-1} = N$，因此 N 是正规的.

(3) 任取 $g \in G$, 若 $g \in N$, 则 $gN = N = Ng$；若 $g \notin N$, 则 $gN = G - N = Ng$, 因此 N 是正规的.

商群定义

商群 $G/H = \{ Ha \mid a \in G \}$

$$Ha\,Hb = Hab$$

说明：

良定义性质：

$$Ha = Hx,\ Hb = Hy \Rightarrow Hab = Hxy$$

商群 G/H 就是商代数

$$a\,R\,b \Leftrightarrow Ha = Hb \Leftrightarrow ab^{-1} \in H$$

$$a\,R\,b,\ c\,R\,d \Rightarrow ac\,(bd)^{-1} \in H \Rightarrow ac\,R\,bd$$

$$a\,R\,b \Rightarrow ab^{-1} \in H \Rightarrow (a^{-1})^{-1}b^{-1} \in H \Rightarrow a^{-1}\,R\,b^{-1}$$

商群实例

$G = \langle Z_{12}, \oplus \rangle$, $Z_{12} = \{ 0, 1, \ldots, 11\}$, 模12加群

子群 $H = \langle 3 \rangle = \{ 0, 3, 6, 9 \}$

商群 $G / H = \{ H, H+1, H+2 \}$

$H+1 = \{ 1, 4, 7, 10 \}$, $H+2 = \{ 2, 5, 8, 11 \}$

$S_3 = \{ (1), (12), (13), (23), (123), (132) \}$

$A_3 = \{ (1), (123), (132) \}$

$S_3/A_3 = \{ A_3, A_3(12) \}$,

$A_3(12) = \{ (12), (13), (23) \}$

商群的性质

性质： $|G/H| = [G:H]$，商群的阶是 $|G|$ 的因子
保持群 G 的性质：交换性，循环性等.

例1 G为Abel 群，$|G| = n$, 素数 p 整除 n, 则 G 中有 p 阶元.

证明思路：归纳法. 归纳基础是显然的. 假设对一切 $m < n$ 命题为真，证明对于 n 为真.

设 $|G| = n$, 取 $a \in G$, $a \neq e$, 寻找 p 阶元.

① p 整除 $|a|$, 则$a^{|a|/p}$ 为 p 阶元.

② p不整除 $|a|$, 令$H = \langle a \rangle$, 构造G/H, $|G/H| = m$, p 整除 m.
G/H 中有 p 阶元 Hb, 导出 b 与 a 的关系

$$(Hb)^p = H \Rightarrow b^p \in H \Rightarrow b^p = a^t$$

$(b^{|a|})^p = e \Rightarrow b^{|a|}$ 为 p 阶元（$b^{|a|} = e \Rightarrow (Hb)^{|a|} = H \Rightarrow p \mid |a|$）

17.7 群的同态与同构

定义 f 为 G_1 到 G_2 的同态当且仅当

$f: G_1 \to G_2$, 且$\forall x, y \in G_1$，$f(x\,y) = f(x)\,f(y)$

实例: (1) 整数加群 $<Z,+>$ 的自同态:

$f_c(x) = c\,x$，c为给定整数

(2) 模 n 加群 $<Z_n,\oplus>$ 的自同态:

$f_p(x) = (px) \bmod n$, $p = 0, 1, \ldots, n-1$

(3) $G_1 = <Z,+>, G_2 = <Z_n,\oplus>$, G_1到 G_2 的满同态

$f : Z \to Z_n$, $f(x) = (x) \bmod n$

说明:将群看成代数系统 $< G, \circ, ^{-1}, e >$，则同态 f 满足:

$f(e_1) = e_2$ ， $f(x^{-1}) = f(x)^{-1}$

同态映射的性质

同态保持元素的性质

$f(e_1)=e_2$，$f(x^{-1})=f(x)^{-1}$，满同态 f 将生成元映到生成元

$|f(a)|$ 整除 $|a|$，同构条件下$|f(a)| = |a|$

同态保持子代数的性质

$H \leq G_1 \Rightarrow f(H) \leq G_2$

$H \trianglelefteq G_1$, f 为满同态，$f(H) \trianglelefteq G_2$

同态核的性质，$\ker f = \{\, x \mid x \in G,\ f(x) = e_2 \,\}$

$\ker f = \{e_1\} \Leftrightarrow f$ 为单同态

$\ker f \trianglelefteq G_1$，$\forall a, b \in G_1$，$f(a) = f(b) \Leftrightarrow a \ker f = b \ker f$

同态基本定理

(1) H 为G 的正规子群，则 G/H 是 G 的同态像

(2) 若 G' 为 G 的同态像（$f(G) = G'$），则 $G/\ker f \cong G'$.

同态性质的证明

证明

(1) $\ker f \trianglelefteq G_1$

(2) $\forall a,b\in G_1,\ f(a)=f(b) \Leftrightarrow a\ker f = b\ker f$

证: (1) 证子群. 显然 $\ker f$ 非空. $\forall a, b\in \ker f$,

$$f(ab^{-1}) = f(a)\,f(b)^{-1} = e_2\,e_2^{-1} = e_2 \Rightarrow ab^{-1}\in \ker f$$

正规性证明. $\forall g\in G_1$, $\forall a\in \ker f$,

$$f(gag^{-1}) = f(g)\,f(a)\,f(g^{-1}) = f(g)\,f(g^{-1}) = f(e_1) = e_2$$

$$gag^{-1}\in \ker f$$

(2) $f(a)=f(b) \Leftrightarrow f(a)^{-1}f(b) = e_2 \Leftrightarrow f(a^{-1}b) = e_2$

$$\Leftrightarrow a^{-1}b\in \ker f \Leftrightarrow a\ker f = b\ker f$$

自同态与自同构

End$G$：G 的自同态的集合

Aut$G$：G 的自同构的集合

Inn$G$：G 的内自同构的集合

内自同构 f_x：$G \to G$，$f_x(a) = x\,a\,x^{-1}$

关系：Inn$G$ $\subseteq$ Aut$G$ $\subseteq$ End$G$

End$G$ 为独异点

Aut$G$ 为群

Inn$G$ 为 Aut$G$ 的正规子群

$I_G = f_e$ 属于 Inn$G$

实例

$Z_6=\{0, 1, 2, 3, 4, 5\}$， $G = < Z_6, \oplus >$,

$f_p : Z_6 \to Z_6$, $f_p(x) = (px) \bmod 6$

$f_0(x)=0$, $f_1=I_G$,

$f_2(0)=f_2(3)=0$, $f_2(1)=f_2(4)=2$, $f_2(2)=f_2(5)=4$

$f_3(0)=f_3(2)=f_3(4)=0$, $f_3(1)=f_3(3)=f_3(5)=3$

$f_4(0)=f_4(3)=0$, $f_4(1)=f_4(4)=4$, $f_4(2)=f_4(5)=2$

$f_5(0)=0, f_5(1)=5, f_5(2)=4, f_5(3)=3, f_5(4)=2, f_5(5)=1$

$\mathrm{End}G = \{ f_0, f_1, \ldots, f_5 \}$,

$\mathrm{Aut}G = \{ f_1, f_5 \}$

$\mathrm{Inn}G = \{ f_1 \}$