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，$H\le G$, $a\in G$,

称$Ha = \{ha \mid h\in H\}$是子群H在G中的一个右陪集。

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

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) 等价关系易证，下证$Ha=[a]$

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 的左陪集和右陪集个数相等。

证： $f: T \to S$, $f(Ha) = a^{-1}H$,

T, S分别为右和左陪集的集合

f 的良定义性与单射性：

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

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

f 满射 …

H 在 G 中的指数$[G:H]$定义为

H 在G中的右（或者左）陪集个数

Lagrange定理及其推论

Lagrange定理：G是有限群，$H\le G$, 则$|G| = |H|[G:H]$

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

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

说明：仅适用于有限群，逆不一定为真.

推论

(1) 有限群中，元素的阶是群的阶的因子.

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

(2) 素数阶群一定是循环群.

证：$|G| = p$, $p>1$, 存在非单位元 a,

$|a|$的阶是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G的子群，

与Lagrange定理矛盾.

Lagrange定理的应用(续)

例2 6 阶群在同构意义下只有 2 个.

证明思路:

若G含6阶元，是循环群Z_6.

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，2p阶群只有2个.

4 阶群只有2个：循环群Z_4和 Klein 四元群.

小群

Numbers of isomorphism types of finite groups of given order

+++	+0	+1	+2	+3	+4	+5	+6	+7	+8	+9	+10	+11	+12	+13	+14	+15	+16	+17	+18	+19
0+	.	1	1	1	2	1	2	1	5	2	2	1	5	1	2	1	14	1	5	1
20+	5	2	2	1	15	2	2	5	4	1	4	1	51	1	2	1	14	1	2	2
40+	14	1	6	1	4	2	2	1	52	2	5	1	5	1	15	2	13	2	2	1
60+	13	1	2	4	267	1	4	1	5	1	4	1	50	1	2	3	4	1	6	1
80+	52	15	2	1	15	1	2	1	12	1	10	1	4	2	2	1	231	1	5	2
100+	16	1	4	1	14	2	2	1	45	1	6	2	43	1	6	1	5	4	2	1
120+	47	2	2	1	4	5	16	1	2328	2	4	1	10	1	2	5	15	1	4	1
140+	11	1	2	1	197	1	2	6	5	1	13	1	12	2	4	2	18	1	2	1
160+	238	1	55	1	5	2	2	1	57	2	4	5	4	1	4	2	42	1	2	1
180+	37	1	4	2	12	1	6	1	4	13	4	1	1543	1	2	2	12	1	10	1

http://www.icm.tu-bs.de/ag_algebra/software/small/

https://en.wikipedia.org/wiki/List_of_small_groups

1024阶的非同构的群有49487365422个！

共轭关系与共轭类

定义 设G为群，定义G上二元关系R，

$$aRb \Leftrightarrow \exists\, x\in G \text{ 使得 } b = x^{-1}ax$$

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$\bar{a}$

共轭类的性质：

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

$$|\bar{a}| = [G:N(a)],\ \text{其中} N(a) = \{x\in G \mid xa = ax\}$$

证明

证明 $|\bar{a}|=[G:N(a)]$

其中 $N(a)=\{x\in G|xa=ax\}$

证 $\forall x, y\in G$,

$xax^{-1}=yay^{-1} \Leftrightarrow ax^{-1}y=x^{-1}ya$

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

故存在双射：$\{xax^{-1}|x\in G\} \leftrightarrow \{xN(a)|\ x\in G\}$

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，共轭类分解一般不等势

(2) 共轭类中置换的轮换结构相同(练习34；反过来也对)，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为有限群，C为中心，G中至少含两个元素的共轭类有k个，$a_1, a_2, ..., a_k$为代表元素，则

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

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

$$G = \bar{a}_1 \cup \bar{a}_2 \cup \cdots \cup \bar{a}_k \cup \{a_{k+1}\} \cup \{a_{k+2}\} \cup \cdots \cup \{a_{k+l}\}$$

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

注：对任意i=1, 2,…, k, $N(a_i)<G$.

(否则$N(a_i)=G$, $|\bar{a}_i|=[G:N(a_i)]=1$)

群分类方程的应用

例3 $|G|=p^s$，p为素数，则$p||C|$.

证:

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

对于$i = 1, 2, \ldots, k$,

$[G:N(a_i)]$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

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

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

对一般的群G及$N \leq G$，左、右陪集不一定相等，即一般$gN \neq Ng$，但对某些群及其子群，总有性质：

$\forall g \in G$，$gN=Ng$

例如：G是Abel群；

$N=\{e\}$, C, 或 G

……

正规子群 (Normal subgroup)：

设G是群，$N \leq G$, 且$\forall g \in G$，$gN=Ng$，则称N是G的<u>正规子群</u>，记为$N \trianglelefteq G$.

正规子群及其判定

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)⇒(2): $gN=Ng \Rightarrow gNg^{-1}=N$

(2)⇒(3): $gng^{-1}\in gNg^{-1}=N$

(3)⇒(1): $\forall ng\in Ng \Rightarrow n\in N, g^{-1}\in G \Rightarrow$
$g^{-1}ng\in N \Rightarrow ng\in gN$

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

正规子群及其判定

判定方法: (1) 判定定理

例1：若$N\trianglelefteq G$，$H\trianglelefteq G$，则$N\cap H \trianglelefteq G$.

证： 因为$N\leq G$，$H\leq G$，故$N \cap H\leq G$.

又$\forall g\in G$, $\forall x\in N\cap H$, 有$x\in N$且$x\in H$. 因为$N\trianglelefteq G$，$H\trianglelefteq G$, 所以$gxg^{-1}\in N$且$gxg^{-1}\in H$，即$gxg^{-1}\in N\cap H$.

正规子群及其判定

例2：设H是群G的子群，假设H的任意两个左陪集的乘积仍是一个左陪集，证明：H是G的正规子群。

证：任取$a \in G$，由于H是G的左陪集，因此存在H的左陪集bH，使得$(Ha)H = H(aH) = bH$，由此可见$Ha \subseteq bH, \underline{a \in bH}$，从而$aH = bH$，所以$Ha \subseteq aH$，于是$a^{-1}Ha \subseteq H$. 由于$a$的任意性，$H$是$G$的正规子群。

正规子群及其判定

判定方法：

(1) 判定定理

(2) $|N|=n$，N是G的唯一n阶子群

(3) 指数为2的子群

证明

例3：N是G的唯一的 n 阶子群，则$N \trianglelefteq G$.

证：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.

例4： N是G的子群，且$[G:N]=2$, 则$N \trianglelefteq G$.

证：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.

证明

例5：A_4没有6阶子群.

证：A_4={(1), (123), (132), (124), (142), (134), (143), (234), (243), (12)(34), (13)(24), (14)(23)}.

假设A_4有6阶子群N, 则有$[A_4:N]=2$，故N是正规的，并且N中一定有3阶元，从而可以验证N包含所有的3阶元。事实上，A_4中的3阶元分成两个共轭类(see W. R. Scott, Group Theory, 1987，§11.1, p. 299)：

T ={(123), (142), (134), (243)}, T' ={(132), (124), (143), (234)}。不妨设T中某个3阶元$a \in N$，则知$a^2 \in T'$，且$T \subseteq N, T' \subseteq N$, 所以$|N|>8$，矛盾！

证明

例5：A_4没有6阶子群.

证：也可以利用事实：“6阶群，在同构的意义下只有Z_6和S_3”去证明。

注：1）由习题十七，p. 283第34题的逆命题：“S_n中轮换指数相同的置换在同一个共轭类中”知，(123)和 (132)在S_4中是共轭的，但不能得出它们在A_4中是共轭的。实际上，这两个置换在A_4中不共轭！

2）A_4是说明拉格朗日定理的逆命题一般不成立的最小群：给定一个有限群G和$|G|$的一个因子d，不一定存在G的一个d阶子群。

商群定义

商群 G是群，$N \trianglelefteq G$, 定义：$G/N = \{Na \mid a \in G\}$

$(Na)(Nb)=Nab$

说明：

良定义性质：$Na=Nx,\ Nb=Ny \Rightarrow Nab=Nxy$

G/N关于上面的运算构成群，称为G关于N的商群

商群G/N 就是商代数

$$aRb \Leftrightarrow Na=Nb \Leftrightarrow ab^{-1} \in N$$

$$aRb,\ cRd \Rightarrow ac(bd)^{-1} \in N \Rightarrow acRbd$$

$$aRb \Rightarrow ab^{-1} \in N \Rightarrow a^{-1}(b^{-1})^{-1} \in N \Rightarrow a^{-1}Rb^{-1}$$

商群实例

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

子群$H=<3>=\{0, 3, 6, 9\}$

商群$G/H=\{H, H+1, H+2\}$

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

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

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

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

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

商群实例

命题： 设G是一个群，N是G的正规子群.

(1) 若H是G的子群且$N \subseteq H$，则N是H的正规子群，H/N是G/N的子群.

(2) 若L是G/N的子群，则存在G的子群H，使得$N \subseteq H$且$L = H/N$.

商群实例

(1) 若 H 是 G 的子群且 $N \subseteq H$，则 N 是 H 的正规子群，H/N 是 G/N 的子群；

证 (1) 假设H是G的子群且$N \subseteq H$. 显然N是H的正规子群，并且$H/N \subseteq G/N$. 对于任意的$Na, Nb \in H/N$，我们有

$$(Na)(Nb)^{-1} = (Na)\left(Nb^{-1}\right) = N\left(ab^{-1}\right) \in H/N$$

所以H/N是G/N的子群。

也可直接由
$H/N \subseteq G/N$， H/N 是与 G/N 运算相同的商群知，H/N 是G/N的子群。

商群实例

(2) 若 L 是 G/N 的子群, 则存在 G 的子群 H, 使得 $N \subseteq H$ 且 $L = H/N$.

(2) 假设L是G/N的子群. 令

$$H = \{a \in G | Na \in L\}.$$

显然$N \subseteq H \subseteq G$，从而，$H \neq \emptyset$. 对于任意的$a, b \in H$，我们有

$$N(ab^{-1}) = (Na)(Nb^{-1}) = (Na)(Nb)^{-1} \in L,$$

从而, $ab^{-1} \in H$. 所以H是G的子群. 根据(1), N是H的正规子群, 从而, H/N有意义. 最后, 根据H的定义, 我们有$H/N = L$.

商群的性质

$|G/H|=[G:H]$，商群的阶是$|G|$的因子

保持群G的性质：交换性，循环性等

对一般有限群都是成立的，柯西定理

例6 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——商群满足性质推出原来群中性质.

归纳步骤. 假设对一切$m<n$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, $|G/H|=m$, $p|m$.

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

商群的性质

(4) $|a|=n, |b|=m, ab=ba \Rightarrow |ab| \mid [n,m]$,

若$(n,m)=1$, $|ab|=nm$

推论 设p, q为互异素数，则pq阶Abel群必为循环群。

证：设$|G|=pq$，G为Abel群。由前面例6知, G中有p阶元a和q阶元b.

又因为p, q为互异素数，且$ab=ba$，所以$|ab|=pq=|G|$，从而G是由ab生成的循环群。

例如，6=2×3阶交换群只能是6阶循环群；10=2×5阶交换群只能是10阶循环群，…

注意：推论对非交换群不成立。例如，

$|S_3|=6=2\times3$, S_3不是循环群。