第二章　群在集合上的作用

数学研究对象中, 常常需要研究集合的性质, 但集合本身并不是孤立的, 从代数的观点而言, 群在集合上的作用是研究集合的最主要的代数方法.

我们首先给出定义.

定义2.1. 设 X 是集合, G 为群. G **在** X **上的作用** (action of G on the set X)是指映射

$$G \times X \to X, \quad (g, x) \mapsto g \cdot x,$$

且满足条件

(1) 对任意的 $x \in X$, $1 \cdot x = x$.

(2) (结合律) 对任意 $x \in X, g, h \in G$,

$$g(hx) = (gh)x.$$

此时, 我们亦称 X 为 G**-集** (G-set).

§2.1　对称群

我们首先以**对称群** (置换群) S_n 作为例子来考虑一下群在集合上的作用. 令 $X_n = \{1, \ldots, n\}$, 则 $S_n = S_{X_n}$ 自然作用在 X_n 上.

§2.1.1　置换及其表示

对置换 $\sigma \in S_n$, 我们一方面可以用**两行式**来表示 σ, 即

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}. \tag{2.1}$$

另一方面, 我们可以用另外一种方式来表示 σ:

定义2.2. 设 $k \leqslant n$, $\{a_1, \ldots, a_k\} \subseteq X_n$, 若置换$\sigma$满足**:**

- $\sigma(a_1) = a_2$, $\sigma(a_2) = a_3$, $\ldots, \sigma(a_k) = a_1$;
- 对于 $i \in X_n \setminus \{a_1, \ldots, a_k\}$, $\sigma(i) = i$.

则置换 σ 称为一个 k **轮换** (k-cycle)。此时记 $\sigma = (a_1 a_2 \cdots a_k)$.

特别地, 2 轮换也称作**对换** (transposition).

注记. (1) 任何一个1 轮换都是恒等置换, 即S_n 中的单位元 1.

(2) k 轮换 $(a_1 a_2 \cdots a_k) = (a_2 \cdots a_k a_1) = \cdots = (a_k a_1 a_2 \cdots a_{k-1})$.

(3) 对于k 轮换 $\sigma = (a_1 a_2 \cdots a_k)$, 若$a \in X_n$ 满足$\sigma(a) \neq a$, 则

$$\sigma = (a\ \sigma(a)\ \sigma^2(a) \cdots \sigma^{k-1}(a)).$$

定义2.3. 如果 $\{a_1,\dots,a_k\}\cap\{b_1,\dots,b_j\}=\emptyset$, 称轮换 $(a_1a_2\cdots a_k)$ 与 $(b_1b_2\cdots b_j)$ **不相交** (disjoint).

定理2.4. (1) 两个不相交轮换必交换, 即 $\sigma\tau=\tau\sigma$ 对不相交轮换 σ,τ 恒成立.

(2) 任意置换 $\sigma\in S_n$ 均可写为两两不相交轮换的乘积, 且在不计先后次序并去除1 轮换的情况下方式唯一.

证明. (1) 设 $\sigma=(i_1\ i_2\cdots i_k)$, $\tau=(j_1\ j_2\cdots j_l)$, 则

$$\begin{gathered}\sigma\tau(i_1)=\sigma(i_1)=i_2=\tau\sigma(i_1)\\ \cdots\\ \sigma\tau(i_k)=\sigma(i_k)=i_1=\tau\sigma(i_k)\\ \sigma\tau(j_1)=\sigma(j_2)=j_2=\tau\sigma(j_1)\\ \cdots\\ \sigma\tau(j_l)=\sigma(j_1)=j_1=\tau\sigma(j_l)\\ \sigma\tau(\alpha)=\alpha=\tau\sigma(\alpha),\forall\alpha\notin\{i_1,\dots,i_k,j_1,\dots,j_l\}\end{gathered}$$

故$\sigma\tau=\tau\sigma$.

(2) 对于给定的$\sigma\in S_n$, 我们在$X_n=\{1,2,\dots,n\}$ 上定义关系 $\sim$ 如下:

$$a\sim b\quad\Leftrightarrow\quad\text{存在}k\in\mathbb{Z},\ \text{使得}\sigma^k(a)=b.$$

容易验证, $\sim$ 是一个等价关系, 从而诱导出分拆:

$$\{1,2,\dots,n\}=\bigsqcup_{1\le j\le s}T_j.$$

设$k_j=|T_j|$ 为集合的阶. 对于任意$a\in T_j$, 由等价定义我们有$\sigma^i(a)\in T_j$, 从而存在整数$i<j$使得$\sigma^i(a)=\sigma^j(a)$, 也就是$\sigma^{j-i}(a)=a$. 令k为使$\sigma^k(a)=a$的最小正整数. 记

$$T_j'=\{a,\ \sigma(a),\ \sigma^2(a),\dots,\sigma^{k-1}(a)\}\subseteq T_j.$$

另一方面, 若$b\in T_j$, 则$b=\sigma^l(a)$, 由$\sigma^k(a)=a=\sigma^{-k}(a)$立即有$b\in T_j'$. 故

$$T_j=T_j'=\{a,\ \sigma(a),\ \sigma^2(a),\dots,\sigma^{k-1}(a)\},\ k_j=k,$$

也就是, 对任意$a\in T_j$, k_j 是使得$\sigma^k(a)=a$的最小正整数. 对于每个j, 我们定义k_j 轮换$\sigma_j=(a\ \sigma(a)\ \sigma^2(a)\ \cdots\ \sigma^{k_j-1}(a))$, 记$\tau=\sigma_1\sigma_2\cdots\sigma_s$. 注意到定义右边的这些轮换两两不相交, 从而可交换. 对任意$b\in X_n=\{1,2,\dots,n\}=\bigsqcup_{1\le j\le s}T_j$, 不妨设$b\in T_j$. 则对任意$i\neq j$, $\sigma_i(b)=b$, 从而$\tau(b)=\sigma_j(b)=\sigma(b)$. 故有

$$\sigma=\sigma_1\sigma_2\cdots\sigma_s.\tag{2.2}$$

存在性得证.

设$1 \neq \sigma = \tau_1\tau_2\cdots\tau_t$, 其中$\tau_j$是$l_j$-轮换($l_j > 1$) 且两两不交. 对于$a$, 若$\tau_j(a) \neq a$, 由不相交性知：对于$j' \neq j$, $\tau_{j'}(a) = a$, 故$\tau_j = (a\,\sigma(a)\cdots\ \sigma^{l_j-1}(a))$. 如果$a \in T_l$, 则由上述讨论$\tau_j = \sigma_l$. 唯一性得证. □

例2.5. 对于 $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 4 & 2 & 3 & 5 & 1 \end{pmatrix}$, 则 $\sigma = (1\ 6)(2\ 4\ 3)(5) = (1\ 6)(2\ 4\ 3) = (2\ 4\ 3)(1\ 6)$.

例2.6. 对于小的n, 对称群 S_n 可以如下详细给出.

(1) 对于 $n = 2$, $S_2 = \{1, (12)\}$.

(2) 对于 $n = 3$, $S_3 = \{1, (12), (13), (23), (123), (132)\}$.

(3) 对于 $n = 4$, 则

$$\begin{aligned} S_4 = \{&1, (12), (13), (14), (23), (24), (34),\\ &(123), (132), (124), (142), (134), (143), (234), (243),\\ &(1234), (1243), (1324), (1342), (1423), (1432),\\ &(12)(34), (13)(24), (14)(23)\}. \end{aligned}$$

由于 k 轮换 $(i_1\cdots i_k)$ 中哪个元素放在首位不是本质的, 将$i_1, \cdots i_k$ 这k 个点依顺时针次序均匀放置在时钟上, 则k 轮换可以看做是将时钟顺时针转动角度 $2\pi/k$, 其逆也就是逆时钟转动相同角度. 即有

引理2.7. 如 $\sigma = (i_1\cdots i_k)$ 为 k 轮换, 则 σ 的阶为 k, 且 $\sigma^{-1} = (i_k\ i_{k-1}\cdots i_1)$.

定义2.8. 设 $\sigma \in S_n$. 当置换 σ 写为不交轮换乘积时, 若k 轮换的个数为 λ_k (当$k = 1$, 设λ_1为$\{1, \cdots, n\}$中被σ固定的元素个数), 则称 σ 的**型** (type) 为 $1^{\lambda_1}2^{\lambda_2}\cdots n^{\lambda_n}$.

由型的定义, 整数 $\lambda_1, \ldots, \lambda_n \geq 0$, 满足方程

$$\sum_{i=1}^{n} i\lambda_i = n. \tag{2.3}$$

所以S_n 中置换的型的个数即为满足 (2.3) 的非负整数组 $\lambda_1, \ldots, \lambda_n$ 的个数. 在组合数学中, 这样的数组称为正整数 n 的一个**分拆** (partition). n 的分拆个数常用$p(n)$ 表示, 函数$n \mapsto p(n)$ 称为**分拆函数**.

例2.9. 由$p(2) = 2$, $p(3) = 3$, $p(4) = 5$ 知对称群 S_2, S_3 和S_4 中元素的型分别有2, 3 和5 种, 这与例 2.6 一致.

命题2.10. 置换 σ 与 σ' 的型相同当且仅当 σ 与 σ' 在 S_n 中共轭, 即存在 $\tau \in S_n$, $\sigma' = \tau\sigma\tau^{-1}$. 故对称群$S_n$ 中共轭类的个数等于n的分拆个数$p(n)$.

证明. 设 $\sigma=(i_1\cdots i_k)(j_1\cdots j_l)\cdots$, 直接计算有$\tau\sigma\tau^{-1}\big(\tau(i_s)\big)=\tau(i_{s+1})$, 从而

$$\tau\sigma\tau^{-1}=(\tau(i_1)\cdots\tau(i_k))(\tau(j_1)\cdots\tau(j_l))\cdots,$$

它的型与 σ 一致.

反过来, 如 $\sigma=(i_1\cdots i_k)(j_1\cdots j_l)\cdots$, $\sigma'=(i'_1\cdots i'_k)(j'_1\cdots j'_l)\cdots$. 令

$$\tau=\begin{pmatrix} i_1 & \cdots & i_k & j_1 & \cdots & j_l & \cdots \\ i'_1 & \cdots & i'_k & j'_1 & \cdots & j'_l & \cdots \end{pmatrix}$$

则

$$\tau^{-1}=\begin{pmatrix} i'_1 & \cdots & i'_k & j'_1 & \cdots & j'_l & \cdots \\ i_1 & \cdots & i_k & j_1 & \cdots & j_l & \cdots \end{pmatrix}$$

故有 $\tau\sigma\tau^{-1}=\sigma'$, 即 σ 与 σ' 共轭. □

§2.1.2 奇置换与偶置换

命题2.11. (1) 任何k 轮换均可写为$k-1$ 个对换的乘积.

(2) S_n 由对换生成. 更一般地, S_n 可由对换 $(12),(13),\ldots,(1n)$ 生成.

证明. (1) 这是由于$(i_1\cdots i_k)=(i_1i_k)(i_1i_{k-1})(i_1i_2)$.

(2) 由于每个置换都是轮换的乘积, 故由(1), S_n 由对换生成. 由于对每个对换

$$(ij)=(1i)(1j)(1i)=(1j)(1i)(1j),$$

故S_n 可由对换 $(12),(13),\ldots,(1n)$ 生成. □

设 $f=f(x_1,\ldots,x_n)$ 是 $\mathbb{Z}^n$ 到 $\mathbb{Z}$ 的 n 变量函数, 对于 $\sigma\in S_n$ 定义

$$\sigma(f)(x_1,\ldots,x_n)=f(x_{\sigma(1)},\ldots,x_{\sigma(n)}). \tag{2.4}$$

故 $\sigma(f)$ 也是 $\mathbb{Z}^n$ 到 $\mathbb{Z}$ 上的 n 变量函数.

例2.12. 设 $n=3$, $\sigma=(123)$, $f(x_1,x_2,x_3)=x_3^2-x_1$, 则

$$\sigma(f)(x_1,x_2,x_3)=x_1^2-x_2.$$

引理2.13. 我们有

(1) 如 $\sigma=1$, 则 $\sigma(f)=f$.

(2) 如 $\sigma,\tau\in S_n$, 则 $\sigma\tau(f)=\sigma(\tau(f))$.

(3) 如 f,g 为 n 变量函数, c 为整常数, 则

$$\sigma(f+g)=\sigma(f)+\sigma(g),\quad \sigma(cf)=c\sigma(f),\quad \sigma(fg)=\sigma(f)\sigma(g).$$

证明. (1), (3) 留给读者.

(2) 一方面,

$$\sigma\tau(f)(x_1,\ldots,x_n)=f(x_{\sigma\tau(1)},\ldots,x_{\sigma\tau(n)}).$$

另一方面, 由$\tau(f)(x)=f(x_{\tau(1)},\ldots,x_{\tau(n)})$ 得

$$\sigma(\tau(f))(x)=f(x_{\sigma(\tau(1))},\ldots,x_{\sigma(\tau(n))})=f(x_{\sigma\tau(1)},\ldots,x_{\sigma\tau(n)}).$$

故 $\sigma\tau(f)=\sigma(\tau(f))$. □

定理2.14. 存在唯一的群同态 $\varepsilon: S_n\to\{\pm1\}$, 使得对所有对换 τ 有

$$\varepsilon(\tau)=-1.$$

证明. 令 $\Delta(x_1,\ldots,x_n)=\prod\limits_{1\le i<j\le n}(x_i-x_j)$. 由置换的定义, 对$\sigma\in S_n$, 易知有$\sigma(\Delta)=\pm\Delta$, 也就是$\sigma(\Delta)/\Delta\in\{\pm1\}$. 令$\varepsilon(\sigma)\triangleq\sigma(\Delta)/\Delta$. 对任意$\sigma,\tau\in S_n$,

$$\varepsilon(\sigma\tau)=\frac{(\sigma\tau)(\Delta)}{\Delta}=\frac{\sigma(\tau(\Delta))}{\Delta}=\frac{\sigma(\varepsilon(\tau)\Delta)}{\Delta}=\frac{\varepsilon(\tau)\sigma(\Delta)}{\Delta}=\varepsilon(\sigma)\varepsilon(\tau).$$

故 ε 为群同态.

对于$\sigma=(1k)$, 经计算即得

$$\sigma\Delta=-\Delta,$$

也就是$\varepsilon(1k)=-1$. 从而对换$(ij)=(1i)(1j)(1i)$ 有$\varepsilon(ij)=(-1)^3=-1$.

唯一性显然, 因为所有置换均由对换生成. □

由定理知, 一个置换写成对换乘积时, 对换个数的奇偶性不变. 我们有如下定义.

定义2.15. 如果置换 σ 为偶数个对换的乘积, 称 σ 为**偶置换** (even permutation). 如果 σ 为奇数个对换的乘积, 称 σ 为**奇置换** (odd permutation).

下面命题给出置换奇偶性的一个简单判定:

命题2.16. 如果置换 $\sigma\in S_n$的型为$1^{\lambda_1}2^{\lambda_2}\cdots n^{\lambda_n}$, 则$\sigma$ 的奇偶性与$\sum\limits_{i=1}^{n}\lambda_i(i-1)$ 的奇偶性一致.

证明. 由于每个k 轮换均是$k-1$ 个对换的乘积, 从而σ可以写成$\sum\limits_{k=1}^{n}\lambda_k(k-1)$个轮换的乘积. □

§2.1.3 交错群

定义2.17. S_n 中所有偶置换构成的子群, 即 $\ker\varepsilon$, 称为 n 阶**交错群** (alternating group), 记为 A_n.

由置换的奇偶性讨论即知, A_n 是 S_n 的正规子群, 且如$n \geq 2$, A_n 的阶为 $\frac{n!}{2}$. 事实上, $n \geq 2$时显然有$(12) \notin A_n$. 对任意$\sigma \notin A_n$也就是σ是一个奇置换, 都有$(12)\sigma \in A_n$, 也就是$\sigma \in (12)A_n$, 从而有$S_n = A_n \sqcup (12)A_n$.

定义2.18. 没有非平凡正规子群的非平凡群称为**单群** (simple group). 也就是说, 如果群$G \neq \{1\}$, 并且除去子群$\{1\}$和G外没有别的正规子群, 则G 称为单群.

例2.19. 最简单的单群是素数阶群. 事实上, 素数阶群是仅有的阿贝尔单群. 如 $G \neq \{1\}$ 是阿贝尔群, $1 \neq g \in G$. 设 g 的阶为 n 而 p 是 n 的素因子, 则 $\langle g^{n/p}\rangle$ 是 G 的 p 阶正规子群(阿贝尔群的所有子群都是正规子群). 要使 G 为单群, 则必有$g \in \langle g^{n/p}\rangle = G$, 也就是$n = p$, 并且$G = \langle g^{n/p}\rangle = \langle g\rangle$为$p$阶循环群.

本节剩余内容将致力于证明下述著名定理:

定理2.20. $A_n (n \geqslant 5)$ 是单群.

注记. $A_2 = \{1\}, A_3$ 的阶为3, 显然是单群. 但 A_4 不是单群, 事实上Klein四元群

$$K_4 = \{1, (12)(34), (13)(24), (14)(23)\} \lhd S_4,$$

自然也是 A_4 的正规子群.

Galois 利用定理 2.20 证明了五次以上多项式没有求根公式, 这是群论诞生的标志. 我们将在第六章阐述 Galois 的著名结果.

引理2.21. A_n 由 3 轮换生成.

证明. 由于A_n中的置换都是偶置换, 并且偶置换都可以写成偶数个对换的乘积, 从而我们只需要证明任何两个对换的乘积可以由3轮换生成即可.

事实上, 我们有

$$(ij)(rs) = \begin{cases} 1 & \text{如 } (ij) = (rs), \\ (jsi) & \text{如 } j = r, i \neq s, \\ (ris)(ijr) & \text{如 } \{i, j\} \cap \{r, s\} = \emptyset. \end{cases}$$

故引理得证. □

引理2.22. 如果 $n \geqslant 5$, 则对于 3 轮换 (ijk) 和 $(i'j'k')$, 存在 $\gamma \in A_n$, 使得

$$\gamma(ijk)\gamma^{-1} = (i'j'k').$$

证明. 由命题 2.10, 存在 $\gamma \in S_n$, 使得

$$\gamma(ijk)\gamma^{-1} = (i'j'k').$$

如果 γ 是偶置换, 引理自然成立; 如果 γ 是奇置换, 由于$n \geq 5$, 我们取 $r, s \neq i', j', k'$, 则 $(rs)\gamma \in A_n$, 且 $(rs)\gamma(ijk)\gamma^{-1}(rs)^{-1} = (rs)(i'j'k')(rs) = (i'j'k')$. □

定理 *2.20* 的证明. 设 $\{1\} \neq N \lhd A_n$. 我们要证明 $N = A_n$. 由正规子群定义知, 如 $x \in N$, $g \in A_n$, 则 $gxg^{-1} \in N$, 故由引理 2.21 和引理 2.22. 我们只需证明 N 中包含一个 3 轮换.

设 $1 \neq \sigma \in N$, 且 σ 保持 X_n 中尽可能多的元素不动. 我们证明 σ 至多变动三个元素, 故σ可以看作S_3中的偶置换, 即为 3 轮换.

注意到 σ 至少变动三个元素, 我们只需证明如果 σ 变动超过了三个元素, 则存在 $\sigma' \in N$ 变动元素个数比 σ 少. 记 σ 为不相交轮换之积, 且最长轮换在左边. 我们将选取恰当的 $\tau \in A_n$, 比较 N 中新元素 $\tau\sigma\tau^{-1}\sigma^{-1}$ 与 σ. (由于$N \lhd A_n$, 有$\tau\sigma\tau^{-1} \in N$, 又有$\sigma^{-1} \in N$, 故$\tau\sigma\tau^{-1}\sigma^{-1} \in N$成立.)

(i) 如果σ恰好变动4个元素, 又是偶置换, 故$\sigma = (a_1a_2)(a_3a_4)$. 令 $\tau = (a_3a_4a_5)$, 则

$$\tau\sigma\tau^{-1}\sigma^{-1} = (a_3a_5a_4) \in N.$$

(ii) 如果σ 至少变动 5 个元素, 我们考虑σ 中最长轮换(最左边的轮换)的长度.

- 若最长轮换长度至少是5, $\sigma = (a_1a_2a_3a_4a_5\cdots)\sigma_1$. 令 $\tau = (a_2a_3a_4)$, 则

$$\tau\sigma\tau^{-1}\sigma^{-1} = (a_2a_3a_5) \in N.$$

- 若最长轮换长度为4, $\sigma = (a_1a_2a_3a_4)\sigma_1$. 令 $\tau = (a_2a_3a_4)$, 则

$$\tau\sigma\tau^{-1}\sigma^{-1} = (a_1a_2a_3) \in N.$$

- 若最长轮换长度为3, 则$\sigma = (a_1a_2a_3)(a_4a_5a_6)\sigma_1$或$(a_1a_2a_3)(a_4a_5)(a_6a_7)\sigma_1$，最少变动6个元素. 令$\tau = (a_2a_3a_4)$, 则总有

$$\tau\sigma\tau^{-1}\sigma^{-1} = (a_1a_4a_2a_3a_5) \in N,$$

且最多变动 5 个元素.

- 若最长轮换长度为2, 则$\sigma = (a_1a_2)(a_3a_4)(a_5a_6)\sigma_1$. 令$\tau = (a_2a_3a_4)$, 则有

$$\tau\sigma\tau^{-1}\sigma^{-1} = (a_1a_4)(a_2a_3) \in N,$$

且变动 4 个元素.

综上所述, 定理得证. □

单群就如整数中的素数, 是群的建筑基块. 对于单群, 特别是有限单群的研究, 在上个世纪五十年代到八十年代是数学研究的一个热点. 近百名群论学家发表了500多篇期刊文章上万页论文, 最终在本世纪初成功将所有有限单群进行了分类, 这就是著名的**有限单群分类定理** (Classification Theorem of the finite simple groups). 它声称所有的有限单群只有四类:

(1) 素数阶循环群;

(2) 交错群$A_n\,(n \geq 5)$;

(3) 李型单群(simple groups of Lie type);

(4) 26 个散在单群(sporadic simple groups).

有限单群分类定理的证明是群论研究的一个高峰, 这个定理被广泛应用到数学研究的各个方面.

习　　题

习题2.1.1. 把置换 $\sigma = (456)(567)(761)$ 写成不相交轮换的积.

习题2.1.2. 直接证明置换 $(123)(45)$ 与 $(241)(35)$ 共轭.

习题2.1.3. 讨论置换

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ n & n-1 & \cdots & 1 \end{pmatrix}$$

的奇偶性.

习题2.1.4. 一个置换的阶等于它的轮换表示中各个轮换的长度的最小公倍数.

习题2.1.5. 证明 S_n 中型为 $1^{\lambda_1}2^{\lambda_2}\cdots n^{\lambda_n}$ 的置换共有 $n!/\prod\limits_{i=1}^{n}\lambda_i!i^{\lambda_i}$ 个. 由此证明

$$\sum_{\substack{\lambda_i \geqslant 0 \\ \lambda_1+2\lambda_2+\cdots+n\lambda_n=n}} \frac{1}{\prod\limits_{i=1}^{n}\lambda_i!i^{\lambda_i}} = 1.$$

习题2.1.6. 试确定 $S_n(n \geqslant 2)$ 的全部正规子群.

习题2.1.7. 置换 σ 的**交错数** $n(\sigma)$ 定义为集合$\{(i,j) \mid \sigma(i) > \sigma(j)$ 但 $i < j\}$ 的阶.

(1) 证明 $n(\sigma) = \sum\limits_{i=1}^{n}\Big|\{j \mid \sigma(j) > i$ 且 $j < \sigma^{-1}(i)\}\Big|$.

(2) 证明置换 σ 可以写为 $n(\sigma)$ 个对换的乘积. 故置换的奇偶性和它的交错数的奇偶性相同.

习题2.1.8. (1) 试证 A_5 中置换的型为 1^5, $2^2\cdot 1^1$, $3^1\cdot 1^2$ 和 5^1.

(2) 证明 A_5 中型为 $2^2\cdot 1^1$ 的置换共轭, 型为 $3\cdot 1^2$ 的置换也共轭.

(3) 试求 A_5 中型为 5^1 的置换的共轭类.

(4) 由此证明 A_5 是单群.

习题2.1.9. 试证: 当 $n\geq 3$时, $Z(S_n)=1$.

习题2.1.10. 试证 A_4 没有 6 阶子群.

习题2.1.11. 试计算:

(1) S_6 中 2 阶元的个数.

(2) A_8 中阶最大的元素个数.

习题2.1.12. 计算 S_n 中使任意指标都变动的置换的个数.

习题2.1.13. 证明当$n\geq 2$ 时, A_n 是 S_n 唯一的指数为 2 的子群.

习题2.1.14. 当 $n\geqslant 2$ 时, (12) 和 $(123\cdots n)$ 是 S_n 的一组生成元.

§2.2 群在集合上的作用

§2.2.1 轨道与稳定子群

我们再回顾一下群在集合上的作用的定义.

定义2.23. 设 X 是集合, G 为群. G 在 X 上的作用是指映射

$$G\times X\to X,\quad (g,x)\mapsto g\cdot x,$$

且满足条件

(1) 对任意的 $x\in X, 1\cdot x=x$.

(2) (结合律) 对任意 $x\in X, g,h\in G$,

$$g(hx)=(gh)x.$$

此时, 我们亦称 X 为 G-**集**.

定义2.24. 如果 X 为 G-集, $x\in X$. 则

$$O_x=Gx=\{gx\mid g\in G\}\subseteq X \tag{2.5}$$

称为 x 所在的**轨道** (orbit). 如果存在 $x\in X$ 使得 $O_x=X$, 称 G 在 X 上的作用**可迁** (transitive).

注记. 由于G是群, 其中任何元素都有逆, 并且群作用满足结合性以及$1 \cdot x = x$可知 X 上不同的轨道不相交, 且 X 是 G 作用下所有轨道的不交并. 由此我们可以定义 X 上的等价关系

$$x \sim y \qquad \text{如果存在 } g \in G,\ y = gx,\ \text{即 } y \in O_x.$$

令 $\{O_x \mid x \in I\}$ 为 X 上所有轨道构成的集合, 则

$$X = \bigsqcup_{x \in I} O_x. \tag{2.6}$$

定义2.25. 设 X 为 G-集, $x \in X$. 定义

$$G_x = \{g \in G \mid gx = x\}, \tag{2.7}$$

即 G 中所有在 x 上作用平凡的元素的集合, 容易验证 G_x 是 G 的子群. G_x 称为 x 的**稳定子群** (stabilizer).

例2.26. 设 $\mathcal{H}$ 为上半平面 $\{z \in \mathbb{C} \mid \operatorname{im} z > 0\}$. 则群 $G = \mathrm{SL}_2(\mathbb{R})$ 作用在 $\mathcal{H}$ 上: 对于 $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in G$, 令

$$\gamma z = \frac{az + b}{cz + d}. \tag{2.8}$$

此作用称为**分式线性变换** 或**Möbius 变换**.

由计算易知 i 的稳定子群是 $SO_2(\mathbb{R})$. 对于$z = x + yi \in \mathcal{H}$, 令

$$\gamma = \frac{1}{\sqrt{y}} \begin{pmatrix} 1 & -x \\ 0 & y \end{pmatrix},$$

则$\gamma z = i$. 故 G 在 $\mathcal{H}$ 上的作用是可迁的.

例2.27. 设 M 是平面上刚体运动构成的群. 我们由解析几何知 M 是由平移、旋转与反射生成. 如果在平面上建立坐标系, 则 M 中一个元素可以如此表出

$$\begin{pmatrix} x \\ y \end{pmatrix} \longmapsto \begin{pmatrix} \cos\theta & -\sin\theta \\ \pm\sin\theta & \pm\cos\theta \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} x_0 \\ y_0 \end{pmatrix}.$$

特别地, **旋转**为

$$\rho_\theta : \begin{pmatrix} x \\ y \end{pmatrix} \longmapsto \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}; \tag{2.9}$$

平移为

$$\tau_P : \begin{pmatrix} x \\ y \end{pmatrix} \longmapsto \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} x_0 \\ y_0 \end{pmatrix},\ \text{其中 } P = (x_0, y_0); \tag{2.10}$$

反射为

$$r : \begin{pmatrix} x \\ y \end{pmatrix} \longmapsto \begin{pmatrix} x \\ -y \end{pmatrix}. \tag{2.11}$$

则 M 作用在平面上的点集上, 平面上的直线集上, 和平面上的三角形集上.

如果 X 是平面上的点集, 则 M 在 X 上的作用是可迁的, 且原点 O 的稳定子群是 $M_O = \mathrm{O}_2(\mathbb{R})$, 即正交群.

例2.28. 设 $H \leqslant G$, 设 $G/H = \{aH \mid a \in G\}$ 是 G 关于 H 的左陪集的集合, 则

$$G \times G/H \to G/H, \qquad (g, aH) \mapsto gaH$$

是 G 在 G/H 上的左乘作用, 我们称为 G 关于 H 的**左诱导表示** (left induced representation). 容易看出 G 在 G/H 上的作用是可迁的, 且对于陪集 $H \in G/H$, 稳定子群

$$G_H = \{g \in G \,|\, g \cdot H = 1 \cdot H\} = \{g \in G \,|\, g \in H\} = H \leq G.$$

以及对任意$a \in G$, 有

$$G_{aH} = \{g \in G \,|\, g \cdot aH = 1 \cdot aH\} = \{g \in G \,|\, a^{-1}ga \in H\} = aHa^{-1} \leq G.$$

例2.29. 设 $G = \mathbb{R}$, X 为 $\mathbb{R}$ 上连续函数的集合. 对于 $f \in X$, $a \in \mathbb{R}$, 定义

$$(a \circ f)(x) = f(x + a).$$

则加法群 $\mathbb{R}$ 作用在连续函数集合上. 注意到:

(1) f 的稳定子群 $G_f = \mathbb{R}$ 当且仅当 f 是常值函数.

(2) f 的稳定子群 $G_f = t\mathbb{Z}$ $(t > 0)$ 当且仅当 f 为具有最小正周期 t 的连续周期函数.

命题2.30. 设 X 是 G-集, $x \in X$, O_x 是 x 所在的轨道, 稳定子群 G_x 为 G 的子群, 记为$H = G_x$. 则存在自然的双射

$$\varphi : G/H \to O_x, \quad aH \mapsto ax.$$

此映射与 G 的作用相洽(compatible), 即对于 $g \in G$, $\varphi(gaH) = g\varphi(aH)$.

证明. 首先, 如果 $aH = bH$, 则 $b = ah, bx = ahx = ax$, 也就是

$$\varphi(aH) = ax = bx = \varphi(bH),$$

故 φ 的定义与 a 的选取无关(well-defined). 另由定义, φ 与 G 相洽. 其次, 如果 $ax = bx$, 则 $x = a^{-1}ax = a^{-1}bx$, 所以 $a^{-1}b \in G_x = H$, 即 $aH = bH$, 故 φ 是单射. 又由于 φ 显然是满射, 故 φ 是双射. □

推论2.31 (计数公式)**.** 设 X 为 G-集.

(1) 如果 $x \in X$, 则 $|O_x| = (G : G_x)$.

(2) 如果X 为有限集, 则

$$|X| = \sum_{x \in I} |O_x| = \sum_{x \in I} (G : G_x). \tag{2.12}$$

证明. 由命题 2.30, $|O_x| = |G/G_x| = (G : G_x)$, 故(1)成立. (2) 由(1) 及(2.6) 即得. □

命题2.32. 设 X 为 G-集, $x \in X, x' = ax \in O_x$, 则

(1) $\{g \in G \mid gx = x'\} = aG_x$.

(2) $G_{x'} = aG_xa^{-1} = \{g \in G \mid g = aha^{-1}, h \in G_x\}$.

证明. (1) 注意到 $gx = x' = ax$ 当且仅当 $a^{-1}gx = x$, 即 $a^{-1}g \in G_x$, 换言之 $g \in aG_x$.

(2) $gx' = x'$ 即 $gax = ax$, 亦即 $a^{-1}gax = x$, 亦即 $a^{-1}ga \in G_x$, 换言之$g \in aG_xa^{-1}$. □

例2.33. 在例 2.27 中, 对于平面上的任意一点 P, 稳定子群

$$M_P = \tau_P \, \mathrm{O}_2(\mathbb{R}) \, \tau_P^{-1} = \tau_P \, \mathrm{O}_2(\mathbb{R}) \, \tau_{-P}.$$

例2.34. 我们再次说明二面体群 D_n 的阶为 $2n$. 事实上, D_n 在正 n 边形的 n 个顶点上的作用可迁, 且固定某一顶点的元素恰好为两个: 单位元和沿过此顶点和对称中心的直线的反射. 记X为正 n 边形的 n 个顶点, $G = D_n$, 则有

$$|X| = |O_x| = (G : G_x),$$

其中$|G_x| = 2$, $|X| = n$, 因此$|D_n| = |G| = 2n$.

§2.2.2 G 在集合 X 上的作用与 G 到群 S_X 的群同态的关系

设 X 是 G-集, 对于 $g \in G$,

$$\rho_g : X \longrightarrow X, \quad x \longmapsto gx$$

是 X 的双射, 事实上 $\rho_{g^{-1}}$ 是 ρ_g 的逆. 故 $\rho \in S_X$ (X 的对称群). 由此, 我们有映射

$$\rho : G \longrightarrow S_X, \quad g \longmapsto \rho_g, \tag{2.13}$$

并且由 $(gh)(x) = g(h(x))$, 我们有 $\rho_{gh}(x) = \rho_g \circ \rho_h(x)$, 也就是$\rho_{gh} = \rho_g\rho_h(x)$, 故 ρ 为群同态. 我们称 ρ 为**群作用诱导的同态** 或者说 ρ 为 G的一个**表示**.

反过来, 给定群同态 $\rho : G \to S_X$, 则对 $g \in G, x \in X$, 令 $gx = \rho(g)x$, 则我们定义了群 G 在 X 上的作用.

我们来讨论一下 ρ 的核. 如果 $\rho_g = 1$, 则对于所有的 $x \in X, gx = x$, 即 $g \in G_x$, 所以

$$\ker \rho = \bigcap_{x \in X} G_x. \tag{2.14}$$

由同态基本定理, 我们得到单同态

$$\bar{\rho} : G \Big/ \bigcap_{x \in X} G_x \longrightarrow S_X. \tag{2.15}$$

例2.35. 设 H 是 G 的子群, G/H 为 H 的左陪集集合, 则 G 在 H 上的左诱导表示的诱导映射为

$$\rho : G \longrightarrow S_{G/H},$$

其核为 $\ker\rho = \bigcap\limits_{g\in G} G_{gH} = \bigcap\limits_{g\in G} g(G_H)g^{-1} = \bigcap\limits_{g\in G} gHg^{-1}$.

命题2.36. $\mathrm{GL}_2(\mathbb{F}_2) \cong S_3$.

证明. 令向量空间 $V = \mathbb{F}_2^2 = \{ae_1 + be_2, \mid a, b \in \mathbb{F}_2\} = \{0, e_1, e_2, e_1 + e_2\}$, 则二阶可逆方阵 $A \in \mathrm{GL}_2(\mathbb{F}_2)$ 通过$v \mapsto Av$ 作用在 V 上, 故也作用在 $X = V \setminus \{0\}$ 上, 由此我们有同态

$$\rho : \mathrm{GL}_2(\mathbb{F}_2) \longrightarrow S_X \cong S_3.$$

如果 $\rho_A = 1$, 则 $Ae_1 = e_1, Ae_2 = e_2$, 故 $A = I_2$, 所以 ρ 是单同态. 由于 $|\mathrm{GL}_2(\mathbb{F}_2)| = (2^2 - 2^0)(2^2 - 2^1) = 6$, 并且$|S_3| = 3! = 6$, 故 ρ 是同构. □

习　　题

习题2.2.1. 设群 G 在集合 Σ 上的作用是传递的, N 是 G 的正规子群, 则 Σ 在 N 作用下的每个轨道有同样多的元素.

习题2.2.2. 设X 是$\mathbb{R}$ 上所有函数的集合. 验证

$$a \circ f(x) = f(ax)\ (a \in \mathbb{R}^\times)$$

给出乘法群$\mathbb{R}^\times$ 在X 上的作用, 并确定所有稳定子群为$\mathbb{R}_+^\times$ 的函数f.

习题2.2.3. 集合 $A \subseteq \mathbb{R}^n$ 的对称群是指将 A 映为自身的所有刚体变换得到的群.

(1) 求正方形, 除正方形外的长方形, 除正方形外的菱形, 圆的对称群.

(2) 求正四面体, 正立方体, 正八面体, 正十二面体, 正二十面体的对称群各有多少元素? 这五个对称群当中是否有同构的?

习题2.2.4. 设群 G 作用在集合Σ 上. 令 t 表示 Σ 在 G 作用下的轨道个数. 对任意 $g \in G$, 令$f(g)$ 表示 Σ 在 g 作用下的不动点个数. 试证

$$\sum_{g\in G} f(g) = t|G|.$$

这就是说, G 的每个元素在 Σ 上的作用平均使得 t 个元素不动.

习题2.2.5. 例 2.26 诱导了 $\mathrm{SL}_2(\mathbb{Z})$ 在 $\mathcal{H}$ 上的作用. 哪些点的稳定子群非平凡? 共有几个这样的轨道?

习题2.2.6. 设群 H 作用在群 N 上, 且每个元素 $g \in H$ 诱导了 N 上的群同构, 即有群同态 $\varphi(g) : H \to \mathrm{Aut}(N)$. 令集合 $G = N \times H$, 定义运算

$$(x_1, y_1)(x_2, y_2) = (x_1 \cdot \varphi(y_1)(x_2), y_1 y_2).$$

(1) 证明 G 在此运算下成为群, 称为 N 和 H 的**半直积** (semidirect product), 记为 $G = N \rtimes H$.

(2) N 同构于 G 的一个正规子群, H 同构于 G 的一个子群. 由此说明上述定义等价于

$$N \lhd G,\ H \leqslant G,\ G = NH,\ N \cap H = \{1\},$$

此时 H 在 N 上的作用为内自同构.

(3) 证明 $G/N \cong H$.

(4) 证明 $S_n = A_n \rtimes \langle (12) \rangle$, 其中 $n \geqslant 3$.

习题2.2.7. 正四面体的 4 个顶点用 4 种颜色染色, 求真正不同的染色的方案个数.

§2.3 群在自身上的作用

§2.3.1 左乘作用

设 G 为群, 则群的乘法自然诱导 G 在自身上的作用

$$G \times G \to G, \quad (g, x) \mapsto gx, \tag{2.16}$$

此作用称为**左乘作用** (action by left multiplication). 由此诱导同态 $\rho : G \to S_G$. 由于对于 $x \in G$, $gx = x$ 当且仅当 $g = 1$, 故 $G_x = \{1\}$, ρ 为单同态. 由此, 我们有

定理2.37 (Caylay)**.** 每个有限群均是对称群的子群. 如果 G 的阶为 n, 则 G 是 S_n 的子群.

注记. 由于 $n!$ 随着 n 的增大而迅速增大, 这个定理在实际中的作用并不大.

命题2.38. 设 G 的阶为 $2n$, 其中 n 为奇数, 则 G 有指数为 2 的子群, 故$n \geq 3$时 G 不是单群.

证明. 考虑 G 的左乘表示 $\rho : G \hookrightarrow S_{2n}$, 由于是群的左乘作用, 从而对于任意$1 \neq g \in G$, 对应的置换$\rho_g \in S_{2n}$ 都变动了所有$2n$个元素($\rho_g(x) \neq x$), 也就是ρ_g中不存在1轮换. 现在我们可以将 G 视为 S_{2n} 的子群, 即将 ρ_g 与 g 视为同一元素. 令 $H = G \cap A_{2n}$, 则

$$G/(G \cap A_{2n}) \cong (G \cdot A_{2n})/A_{2n},$$

从而有

$$(G : H) = \Big((G \cdot A_{2n}) : A_{2n}\Big) \leqslant (S_{2n} : A_{2n}) = 2.$$

我们要证明 $(G:H)=2$, 即 G 中存在奇置换.

事实上, 由于偶数阶群 G 中满足 $x^2=1$ 的元素为偶数(不满足等式的元素y与y^{-1}成对出现), 故 G 中存在 2 阶元 g. 从而ρ_g为S_{2n}中的2阶元, 由上述讨论知道ρ_g变动了所有$2n$个元素, 而且阶数为2只能为n个不相交对换的乘积, 而n为奇数, 故$\rho_g \in \rho(G)$为奇置换.

设 $H \leqslant G$, $(G:H)=2$. 对于任意 $g \notin H$, 则 $G = H \bigsqcup Hg = H \bigsqcup gH$, 所以 $Hg = gH$; 而对于$g \in H$, 总有$Hg = H = gH$, 所以H 为 G 的正规子群. 故 $n \geq 3$时 G 不是单群. □

例2.39. 由上述命题立即可知: $150 = 2 \cdot 75$阶群不是单群.

§2.3.2 共轭作用

群对自身的作用中, 更有意义的作用是**共轭作用** (action by conjugation), 即映射

$$G \times G \to G, \quad (g,x) \mapsto gxg^{-1}. \tag{2.17}$$

容易验证上述作用的确是群的作用. 对于 $x \in G$, 我们记

- $Z(x) = G_x = \{g \in G \mid gxg^{-1} = x\} = \{g \in G \mid gx = xg\}$,
- $C_x = O_x = \{x' \in G \mid x' = gxg^{-1}\}$.

子群 $Z(x)$ 是 G 中所有与x 可交换的元素的集合, 称为 x 的**中心化子** (centralizer), 集合C_x即 x 所在的**共轭类** (conjugate class).

由元素 x 的中心化子的定义, 可以定义 G 的任意子集 T 的中心化子

$$Z_G(T) = \bigcap_{x \in T} Z(x) = \{g \in G \mid gx = xg, \text{ 对任意 } x \in T \text{ 成立}\}.$$

特别地, 对于群 G 的中心 $Z(G)$ 有

$$Z(G) = Z_G(G) = \bigcap_{x \in G} Z(x) = \{g \in G \mid gx = xg, \text{ 对任意 } x \in G \text{ 成立}\}. \tag{2.18}$$

再由式 (2.14), 它就是共轭作用所诱导的同态 $\pi : G \to S_G$ 的核 $\ker \pi$.

由推论 2.31 的计数公式, 我们有

命题2.40. 设 G 为有限群, 则

(1) $|G| = |O_x| \cdot |G_x| = |C_x| \cdot |Z(x)|$.

(2) **类方程** (class equation) 成立:

$$|G| = \sum_{G \text{ 中共轭类}} |C_x| = |Z(G)| + \sum_{|C_x| \neq 1} |C_x|. \tag{2.19}$$

证明. 只需要证明类方程的第二个等式. 这是由于元素

$$x \in Z(G) \Longleftrightarrow gxg^{-1} = x, \ \forall\, g \in G \Longleftrightarrow \{x\} = C_x,$$

亦或 $Z(x) = G$. □

我们下面给出类方程的一些应用.

定义2.41. 如果有限群 G 的阶是素数 p 的方幂($|G|=p^r, r\geq 1$), 则称 G 为 p **群** (p-group).

命题2.42. p 群的中心非平凡, 即$|Z(G)|>1$.

证明. 由类方程

$$p^r=|G|=|Z(G)|+\sum_{|C_x|\neq 1}|C_x|.$$

又$|C_x|\cdot|Z(x)|=|G|=p^r$, 从而$C_x=p^{k_x}$. 若$|C_x|>1$, 则有$p\big||C_x|$, 故p乘除$\sum\limits_{|C_x|\neq 1}|C_x|$. 由类方程立即有 p 整除 $|Z(G)|\geq 1$, 所以 $Z(G)$ 非平凡. □

同理, 由公式 (2.12), 可以证明 (留作练习):

命题2.43. 设 G 为 p 群, X 是有限 G-集, 且 $p\nmid|X|$, 则存在 $x\in X$, 对所有 $g\in G, gx=x$, 即 X 中存在 G 作用下的不动点.

证明. 直接考虑推论 2.31 计数公式(2.12). □

命题2.44. p^2 阶群 G 必为阿贝尔群.

证明. 令 Z 为 G 的中心. (反证法)设 $Z\neq G$, 由命题 2.42, Z 非平凡, 故 $|Z|=p$. 令 $x\in G$ 但 $x\notin Z$, 则 $Z\subseteq Z(x)$ 且 $x\in Z(x)$, 故子群$Z(x)$的阶 $|Z(x)|>p$. 所以 $Z(x)=G$, 我们得到 $x\in Z$, 矛盾. 于是假设不成立, 所以 $Z=G$, 即 G 为阿贝尔群. □

命题2.45. p^2 阶群或为循环群, 或为两个 p 阶循环群的乘积.

证明. 如果 G 中包含 p^2 阶元, 则 G 为该元素生成的p^2阶循环群. 否则 G 中所有非单位元的阶均为 p. 令 $1\neq x\in G$, 且 $y\in G\backslash\langle x\rangle$. 则 $\langle x\rangle\cap\langle y\rangle=\{1\}$. 考虑映射

$$\varphi:\mathbb{Z}/p\mathbb{Z}\times\mathbb{Z}/p\mathbb{Z}\to G,\quad (m,n)\mapsto x^my^n.$$

由于G是阿贝尔群, 我们容易验证 φ 为同态. 如果$\varphi(m,n)=1$, 则 $x^m=y^{-n}\in\langle x\rangle\cap\langle y\rangle=\{1\}$, 故 $m=n=0$, 所以 φ 为单同态. 由于 $|\mathbb{Z}/p\mathbb{Z}\times\mathbb{Z}/p\mathbb{Z}|=p^2=|G|$, 所以 φ 为同构. □

§2.3.3 G 在子群 H 上的共轭作用

设 H 为 G 的子群. 令 $X_H=\{gHg^{-1}\mid g\in G\}$, 即 X_H 为所有与 H 共轭的群的集合. 注意到

$$X_H=\{H\}\text{ 当且仅当 }H\lhd G. \tag{2.20}$$

G 在 X_H 上的**共轭作用**为

$$\begin{aligned}G\times X_H&\longrightarrow X_H\\(g,aHa^{-1})&\longmapsto gaHa^{-1}g^{-1}=(ga)H(ga)^{-1}.\end{aligned}$$

我们容易验证, G 在 X_H 上的作用可迁.

定义2.46. H 关于 G 的**正规化子** (normalizer)为

$$N_G(H) = \{g \in G \mid gHg^{-1} = H\}, \tag{2.21}$$

即为 H 在共轭作用下的稳定子群. 特别地, $H \lhd N_G(H)$.

由计数公式 (2.12), 我们有

$$|G| = |N_G(H)| \cdot |X_H|,$$

故由公式 (2.20)有

$$N_G(H) = G \text{ 当且仅当 } H \lhd G. \tag{2.22}$$

令 $\pi_H : G \to S_{X_H}$ 为 G 在 X_H 上的共轭作用诱导的同态, 则

$$\ker \pi_H = \bigcap_{a\in G} G_{aHa^{-1}} = \bigcap_{a\in G} a(G_H)a^{-1} = \bigcap_{a\in G} aN_G(H)a^{-1}. \tag{2.23}$$

例2.47. 如果 $(G : N) = p$, 且 p 为 $|G|$ 的最小素因子, 则 $N \lhd G$.

证明. 考虑 G 在 N 的左陪集表示, 我们得到群同态

$$\rho_N : G \longrightarrow S_{G/N} \cong S_p.$$

其核 $\ker \rho_N = \bigcap\limits_{a\in G} a^{-1}Na \lhd N$. 首先, 由同态基本定理, $G/\ker \rho_N$ 为 S_p 的子群, 故 $(G : \ker \rho_N)$ 是 $p!$ 的因子. 设q为$(G : \ker \rho_N) \geq p$的任意素因子, 则首先q为$|G|$的素因子, 从而有$q \geq p$. 又q是p !的因子，故$q \leq p$. 立即有$p^r = (G : \ker \rho_N)$为$p!$ 的因子. 从而$r = 1$并且$(G : \ker \rho_N) = p$. 此时 $N = \ker \rho_N \lhd G$. □

习　　题

习题2.3.1. 确定 $\mathrm{GL}_2(\mathbb{F}_5)$ 中 $\begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}$ 的共轭类的阶.

习题2.3.2. 设 p 是素数, G 是 p 的方幂阶的群. 试证 G 子群中非正规子群的个数一定是 p 的倍数.

习题2.3.3. 令 G 是单群, 如果存在 G 的真子群 H 使得 $[G : H] \leqslant 4$, 则 $|G| \leqslant 3$.

习题2.3.4. 设 H 是无限群 G 的有限指数真子群, 则 G 一定含有一个有限指数的真正规子群.

习题2.3.5. 证明$\mathrm{GL}_n(\mathbb{R})$ 的上三角矩阵构成的子群与下三角矩阵构成的子群共轭.

习题2.3.6. 证明命题 2.43.

习题2.3.7. 一般线性群 $\mathrm{GL}_n(\mathbb{C})$ 不含有指数有限的真子群.

习题2.3.8. 令 G 是阶数为 $2^n m$ 的群, 其中 m 是奇数. 如果 G 含有一个 2^n 阶的元素, 则 G 含有一个指数为 2^n 的正规子群.

习题2.3.9. 将S_n 视为 $\mathrm{GL}_n(\mathbb{R})$ 的置换矩阵构成的子群. 确定 S_n 在 $\mathrm{GL}_n(\mathbb{R})$中的正规化子.

习题2.3.10. 求对称群 S_3 的自同构群 $\mathrm{Aut}(S_3)$.

习题2.3.11. 设 α 是有限群 G 的自同构. 若 α 把每个元素都变到它在 G 中的共轭元素, 即对任意 $g \in G$, g 和 $\alpha(g)$ 共轭, 则 α 的阶的素因子都是 $|G|$ 的因子.

习题2.3.12. 设 p 是 $|G|$ 的最小素因子. 若 p 阶子群 $A \lhd G$, 则 $A \leqslant Z(G)$.

习题2.3.13. 试求中心化子:

(1) 群S_4 中元素$(12)(34)$;

(2) 群S_n 中元素$(123\cdots n)$.

习题2.3.14. 试求非交换 p^3 阶群的共轭类个数以及每个共轭类元素个数.

习题2.3.15. 令 $G = \mathrm{GL}_n(\mathbb{C})$, $T = T_n(\mathbb{C})$ 为 G 中对角线元全为 1 的上三角阵构成的子群. 确定 $N_G(T)$, $Z_G(T)$ 和 T 的中心 $Z(T)$.

习题2.3.16. 设 $N \lhd G$, M 是 G 的子群且 $N \leq M$, 则 $N_G(M)/N = N_{\overline{G}}(\overline{M})$, 这里 $\overline{G} = G/N$, $\overline{M} = M/N$.

习题2.3.17. 试证有限群 G 的一个真子群的全部共轭子群不能覆盖整个群 G. 结论对无限群是否成立?

习题2.3.18. 设 K是群 G的一个 2 阶正规子群, 且设 $\overline{G} = G/K$. 设 $\overline{C}$ 是 $\overline{G}$ 的一个共轭类. 设 S是 $\overline{C}$ 在 G 中的逆像. 证明下列两种情形之一必成立:

(1) $S = C$ 是单独一个共轭类且 $|C| = 2|\overline{C}|$。

(2) $S = C_1 \bigcup C_2$ 由两个共轭类组成且 $|C_1| = |C_2| = |\overline{C}|$。

习题2.3.19. (1) 若 $G/Z(G)$ 是循环群, 证明 G 为阿贝尔群, 故非交换有限群 G 的中心 $Z(G)$ 的指数 $\geqslant 4$.

(2) 如果 G 为 n 阶有限群, t 为 G 中共轭类的个数, $c = \frac{t}{n}$. 证明 $c = 1$ 或者 $c \leqslant \frac{5}{8}$.

§2.4 西罗定理及其应用

本节将讨论有限群论中最主要的一个定理: 西罗定理.

§2.4.1 西罗定理

设 G 为 n 阶有限群. 设 p 为 n 的一个素因子, 记 $n = p^r m$, 其中 p 与 m 互素. 我们称 p^r 为 n 的 p 部分, m 为 n 的非 p 部分. 一个自然的问题是, G 中是否含有 p 阶元? 更进一步地, G 中是否存在 p^r 阶子群?

定义2.48. 阶为 p^r 的子群称为 G 的 **西罗p-子群** (Sylow p-subgroup).

定理2.49 (西罗第一定理)**.** G 中存在西罗p-子群.

证明. 设 X 为 G 中所有 p^r 元子集构成的族, 即

$$X = \{U \subseteq G \mid |U| = p^r\}.$$

则

$$N = |X| = \binom{mp^r}{p^r} = \frac{mp^r \cdot (mp^r - 1) \cdots (mp^r - p^r + 1)}{1 \cdot 2 \cdots p^r},$$

也就是

$$N \cdot 1 \cdot 2 \cdots (p^r - 2)(p^r - 1) = m \cdot (mp^r - 1) \cdots (mp^r - (p^r - 1)),$$

由于 i 与 $mp^r - i (1 \leqslant i \leqslant p^r - 1)$ 被 p 整除的次数一样, 比较上式两端素数p的因子个数立即有 $(p, N) = 1$.

考虑 G 在 X 上的左乘作用, 由于 $p \nmid N$, 由计数公式, 故必存在一个轨道, 它的阶与p互素. 不妨设 $U \in X$ 所在的轨道O_U 的阶 $|O_U|$ 与 p 互素. 由稳定子群定义, $U = \bigcup\limits_{x \in U} G_U\, x$, 也就是$U$是$G$的子群 G_U 的一些右陪集的并, 从而是一些右陪集的无交并, 故 $|G_U|$ 是 $|U| = p^r$ 的因子, 故 $|G_U|$ 也是p的方幂. 由公式 (2.12),

$$n = m \cdot p^r = |G| = |G_U| \cdot |O_U| = p^k \cdot |O_U|,$$

由于 $|O_U|$ 与 p 互素, 故 $|G_U| = p^r$, 所以 G_U 是 G 的西罗 p-子群. □

定理2.50 (西罗第二定理)**.** 设 K 为 G 的子群, 且 p 整除 K 的阶, H 是 G 的一个西罗 p-子群. 则存在 $H' = gHg^{-1}$ 使得 $H' \cap K$ 是 K 的西罗子群.

证明. 我们知道 G 在 $X = G/H = \{gH \mid g \in G\}$ 上的左诱导作用可迁, 且对于 $x = aH \in X$, 它的稳定子群是 aHa^{-1}.

将 G 在 X 上的作用限制到 K 在 X 上的作用. 由于 $|X| = m$ 与p互素, 故存在X中的元素$x = aH$对应的 K-轨道 O_x, 使得$|O_x|$ 与 p 互素, 此时

$$K_x = G_x \cap K = aHa^{-1} \cap K \leq aHa^{-1},$$

从而相应的稳定子群K_x的阶为 p 的幂次. 由于 $|O_x| \cdot |K_x| = |K|$以及 $|O_x|$ 与 p 互素, 从而 K_x 的阶恰好为 $|K|$ 的 p 部分, 即 $K_x = aHa^{-1} \cap K$ 是 K 的西罗p-子群. □

由西罗第二定理, 我们有

推论2.51. (1) 如果 $K \leqslant G$ 是 p 群, 则 K 是 G 的某个西罗 p-子群 H 的子群.

(2) 所有 G 的西罗p-子群共轭.

证明. (1) 由于 K 是 p 群, 因此 K 的西罗 p 子群是自身, 故 $H' \cap K = K$, 即 $K \leqslant H'$.

(2) 设 H, H_1 为 G 的两个西罗p-子群. 由西罗第二定理, 存在 $H' = gHg^{-1}$ 使得 $H' \cap H_1 = H_1$, 但由于 $|H_1| = |H| = |H'| = p^r$, 我们有 $H_1 = H' = gHg^{-1}$, 它与 H 共轭. □

定理2.52 (西罗第三定理)**.** 令H 是G 的西罗p-子群, $X_H = \{aHa^{-1} \mid a \in G\}$, 且记

$$N(p) = |X_H| = G \text{ 的西罗 } p \text{ 子群的个数}. \tag{2.24}$$

则$N(p) \,\big|\, m$ 并且 $N(p) \equiv 1 \mod p$.

证明. 由上述推论我们知道 G 在 X_H 上的共轭作用可迁($O_H = X_H$), 又

$$G_H = \{g \in G \,|\, gHg^{-1} = H\} = N_G(H),$$

故 $N(p) = (G : N)$, 其中 $N = N_G(H)$.

考虑G的子群H在X_H上的共轭作用, 将 X_H 分解为 H 作用的轨道:

$$X_H = \bigsqcup_{i \in I} O_{H_i} \Longrightarrow N(p) = |X_H| = \sum_{i \in I} |O_{H_i}|.$$

(1) 如果$|O_{H_i}| = 1$, 即$O_{H_i} = \{H_i\}$, 则$hH_ih^{-1} = H_i$对所有$h \in H$成立, 故 $H \leqslant N_G(H_i)$, 由于H是G的西罗子群, 从而也是G的子群$N_H(H_i)$的西罗p子群. 另一方面, 由正规化子的定义有$H_i \lhd N_G(H_i)$, 再由推论2.51 可知G的西罗p子群H_i是 $N_G(H_i)$ 唯一的西罗 p-子群, 故 $H = H_i$. 这说明仅包含一个元素的轨道只有 $O_H = \{H\}$.

(2) 如果$|O_{H_i}| > 1$, 由$|O_{H_i}| \cdot |N_G(H_i) \cap H| = |H| = p^r$, 知$p \,\big|\, |O_{H_i}|$. 从而

$$N(p) = |X_H| = \sum_{i \in I} |O_{H_i}| = |O_H| + \sum_{i \in I, H_i \neq H} |O_{H_i}| = 1 + \sum_{i \in I, |O_{H_i}| > 1} |O_{H_i}|,$$

故$N(p) \equiv 1 \mod p$. 现在由$(N(p), p) = 1$以及$N(p) \big|\big| G| = m \cdot p^r$立即有$N(p) \,\big|\, m$. □

类似西罗定理的证明, 更一般地, 我们可以证明（留作练习）:

定理2.53. 设$p^k \big|\big| G|$, 其中p为素数. 则 G 中存在 p^k 阶子群, 且其个数模 p 余 1.

上面的西罗第一, 第二, 第三定理常常综合为如下定理:

定理2.54 (西罗定理)**.** 设 G 为有限群, 其阶为 $p^r m$, 其中 $(m, p) = 1$, 则

(1) G 中存在西罗p-子群, 即阶为 p^r 的子群.

(2) 所有 G 中的西罗p-子群共轭.

(3) G 的西罗p-子群个数 $N(p) \equiv 1 \mod p$ 且 $N(p) \mid m$.

注记. 如果$N(p)=1$, 则G唯一的西罗p-子群是G的正规子群.

路德维希 · 西罗(Ludwig Sylow, 1832年12月12日－1918 年9 月7日, 图 2.1)是挪威数学家, 长期担任高中数学教师. 1862年在克里斯蒂安尼亚大学(现奥斯陆大学) 当代课讲师, 教授伽罗瓦理论时, 他提出的问题最终导致他发现西罗子群和西罗定理, 西罗定理在1872年发表. 西罗还花了8年时间和索福斯 · 李(Sophus Lie, 李群李代数的发现者) 一起编辑阿贝尔的数学全集.

图 2.1: 西罗像

§2.4.2 西罗定理的应用

西罗定理在研究有限群的结构中起着关键作用. 下面我们举例说明它的一些应用.

例2.55. 我们再次证明150 阶群G 不是单群. 事实上, 设 H 为 G 的一个西罗5-子群, 即阶为25的子群, 则 G 在 H 的左陪集作用诱导同态

$$\rho : G \longrightarrow S_{G/H} \cong S_6.$$

首先有,

$$\ker\rho = \bigcap_{a\in G} G_{aH} = \bigcap_{a\in G} aG_Ha^{-1} = \bigcap_{a\in G} aHa^{-1} \leq H.$$

另一方面，如果$\ker\rho = \{1\}$, 则$G \cong \rho(G) \leq S_6$. 但由于 $|G| = 150 \nmid 6!$, 故 $\rho(G)$不是S_6的子群, 即$\{1\} \neq \ker\rho \leq H$, 因此 $\ker\rho$ 为 G 的非平凡正规子群.

命题2.56. 设 p,q 为素数, 则

(1) pq 阶群不是单群.

(2) p^2q 阶群也不是单群.

证明. 由于素数幂次群有非平凡中心, 故p^2和p^3阶群均不是单群. 不妨假设 $p\neq q$.

(1) 不妨设 $p<q$, 则由 $N(q)|p$ (故$N(q)=1$ 或 p) 且 $N(q)\equiv 1 \pmod q$ 有 $N(q)=1$, 即西罗q-子群是 G 的正规子群.

(2) 如果 $p>q$, 则同上推理 $N(p)=1$, G 不是单群. 如果 $p<q$, 则 $N(p)=1$ 或 q 且 $N(q)=1$ 或 p^2(由于 $p\not\equiv 1 \mod q$, $N(q)$ 不可能等于p). 如果 $N(q)=p^2$, 则 G 中有 p^2 个 q 阶循环群, 又两个不同的q阶群的交是$\{1\}$, 从而G 的 q 阶元个数为 $p^2(q-1)$. 由此知 G 中 p 幂次元最多有 $p^2q-p^2(q-1)=p^2$ 个, 也就是G中最多一个p^2阶群, 由西罗定理知G中恰好有一个p^2阶群, 即$N(p)=1$. □

注记. 著名的Burnside 定理即是说对于 p,q 为不同素数, $a,b\geq 1$, 则 p^aq^b 阶群都不是单群. Butnside定理是有限群表示论的著名结果, 但迄今为止尚未有使用纯粹群论方法的证明.

定理2.57. 最小有限非阿贝尔单群 G 同构于 A_5, 即

(1) 如果 $|G|<60$, G 不是非阿贝尔单群.

(2) 如果 $|G|=60$ 且 G 为单群, 则 $G\cong A_5$.

证明. (1) 我们已知$\{1\}$不是单群, 并且:

(i) 素数阶群均是循环群(推论 1.62);

$$|G|=2,3,5,7,11,13,17,19,23,29,31,37,41,43,47,53,59;$$

(ii) $2m$ ($m\geq 2$ 为奇数) 阶群不是单群(命题 2.38);

$$|G|=6,10,14,18,22,26,30,34,38,42,46,50,54,58;$$

(iii) 素数幂次(次数$\geqslant 2$)阶群不是单群(命题 2.42);

$$|G|=4,8,9,16,25,27,32,49;$$

(iv) pq, p^2q 阶群(p,q 为不相同的素数) 不是单群(命题 2.56);

$$|G|=6,10,12,14,15,18,20,21,22,26,28,33,34,35,38,39,44,45,46,50,51,52,55,57,58.$$

故只需考虑 $n=|G|=24,36,40,48,56$.

(a) $n=24=2^3\cdot 3$, (或$n=48=2^4\cdot 3$), 设 H 为 G 的西罗2-子群. G 在 G/H 上的左诱导表示诱导同态 $\rho: G\longrightarrow S_{G/H}\cong S_3$. 由于 $\ker\rho\leq H$, 且 $n>6=|S_3|$, 故 $\ker\rho\neq\{1\}$ 是 G 的真正规子群, 故G 非单.

(b) $n=36=3^2\cdot 4$, 类似于(a) 取G 的西罗3-子群H. G 在 G/H 上的左诱导表示诱导同态 $\rho: G\longrightarrow S_{G/H}\cong S_4$. 由于 $\ker\rho\leq H$, 且 $n=36>24=|S_4|$, 故 $\ker\rho\neq\{1\}$ 是 G 的真正规子群, 故G 非单.

(c) $n=40$, 则 $N(5)\big|8$ 且 $N(5)\equiv 1\pmod 5$, 我们有 $N(5)=1$.

(d) $n=56=7\times 8$, $N(7)=1$ 或 8. 如果 $N(7)=8$, 则 G 中 7 阶元素有 $8\times(7-1)=48$个, 其它阶元素只有 8个, 则G至多一个8阶子群, 故 $N(2)=1$, G 不是单群.

(2) 我们现在假设 $|G|=60=2^2\cdot 3\cdot 5$ 且 G 为单群. 首先我们知道$N(2)$, $N(3)$和$N(5)$都不等于1. 我们分三步来证明$G\cong A_5$.

(a)首先断言 G 中没有指数 $\leqslant 4$ 的真子群. 事实上, 如果 $[G:H]=m\leq 4$, 则G 在 H 的左陪集上的表示诱导非平凡同态 $\rho: G\to S_m$. 如果 $1<m\leqslant 4$, 则$|G|=60>24\geq m!=|S_m|$, 从而$\{1\}\neq\ker\rho\leq H$ 为G 的非平凡正规子群.

(b) 我们断言 G 中有指数为 5 的子群 H, 即 $|H|=12$. 事实上, 考虑 G 的西罗2-子群, 若N是G的一个西罗2-子群, 则有$N(2)=(G:N_G(N))$, 由(a)知$N(2)\neq 2$, 故$N(2)=5$ 或15.

如果 $N(2)=5$, 则可取 H 为西罗2-子群N的正规化子$N_G(N)$.

如果 $N(2)=15$. 由于 $N(5)\big|12$, $N(5)\equiv 1\pmod 5$, 故有$N(5)=6$. 由(a)知$N(3)\neq 4$, 且 $N(3)\big|20$, $N(3)\equiv 1\pmod 3$, 故有$N(3)=10$. 从而G 中 5 阶元和 3 阶元有 $6\cdot(5-1)+10\cdot(3-1)=24+20=44$ 个元素. G的15个西罗2-子群(4阶子群)的所有元素只能在剩余$60-44=16$个元素中, 故必存在 G 的西罗2-子群 P_1, P_2, 它们的交非平凡, 也就是为一个2阶子群. 记P_1与P_2 的交为$K=\{1,x\}$, 它们生成的群为H. 由于 P_1,P_2 均为阿贝尔群, x与$P_1\bigcup P_2$中所有元素可交换, 故x与P_1 与P_2 生成的子群H中所有元素可交换, 即有$H\leq Z_G(x)$. 又由G单群可知$Z_G(x)\neq G$ (G的中心是平凡的). 由于H有子群P_1和P_2并且$P_1\bigcup P_2\subseteq H$, 立即有

$$4\big||H|,\ |H|\big||G|=60,\ 6\leq|H|<60$$

故 H 的阶只能是 12 或 20, 但由(a)知 H 只能是 12 阶群.

(c) 考虑 G 在12阶子群 H 的左陪集上的表示, 则有非平凡同态 $\rho: G\to S_5$, 故 $\ker\rho=\{1\}$, 即ρ 为单同态. 因此G 同构于 S_5 的一个 60 阶子群 M, M在S_5指数为2故为正规子群. 由置换群S_n中置换奇偶的定义知M中至少有一半的偶置换, 故 $\{1\}\neq M\cap A_5\lhd A_5$. 由于$A_5$是单群知 $M=A_5$. □

习　　题

习题2.4.1. 若 p 是 $|G|$ 的素因子, 则群 G 必有 p 阶元素.

习题2.4.2. 给出 $\mathrm{GL}_n(\mathbb{F}_p)$ 的一个西罗p-子群, 并求出 $\mathrm{GL}_n(\mathbb{F}_p)$ 中西罗 p 子群的个数.

习题2.4.3. 证明定理2.53.

习题2.4.4. 设 G 是 n 阶群, p 是 n 的素因子. 证明方程 $x^p = 1$ 在群 G 中的解的个数是 p 的倍数.

习题2.4.5. 证明 6 阶非阿贝尔群只有 S_3.

习题2.4.6. 证明 148, 200, 224 阶群不是单群.

习题2.4.7. 求对称群 S_4 的自同构群 $\mathrm{Aut}(S_4)$.

习题2.4.8. 设 N 是有限群 G 的正规子群. 如果 p 和 $|G/N|$ 互素, 则 N 包含 G 的所有西罗p-子群.

习题2.4.9. 设 G 是有限群, N 是 G 的正规子群, P 是 G 的一个西罗p-子群. 证明:

(1) $N \cap P$ 是 N 的西罗p-子群;

(2) PN/N 是 G/N 的西罗p-子群;

(3) $N_G(P)N/N \cong N_{G/N}(PN/N)$.

习题2.4.10. 令 $P_1, \ldots, P_N$ 是有限群 G 的全部西罗p-子群. 如果对任意 $i \neq j$, 总有

$$|P_i : P_i \cap P_j| \geqslant p^r,$$

则 $N \equiv 1 (\mathrm{mod}\ p^r)$.

习题2.4.11. 证明: 若 G 的阶为 $n = p^e a$, 其中 $1 \leq a < p$, 且 $e \geq 1$, 则 G 一定有真正规子群.

习题2.4.12. 令 G 是集合 Σ 上的对称群, P 是 G 的西罗p-子群, $a \in \Sigma$. 如果 p^m 整除 $|Ga|$, 则 p^m 整除 $|Pa|$.

习题2.4.13. 令 G 是集合 Σ 上的对称群. 对任意 $a \in \Sigma$, 设 P 是稳定子群 G_a 的西罗p-子群, Δ 是轨道 Ga 在 P 作用下的全部不动点的集合. 证明 $N_G(P)$ 在 Δ 上的作用是传递的.

习题2.4.14. 设群 G 是 24 阶群且其中心平凡, 证明 G 同构于 S_4.

习题2.4.15. 设 P 是 G 的西罗p-子群且 $N_G(P)$ 是 G 的正规子群. 证明 P 是 G 的正规子群.

§2.5 自由群与群的表现

§2.5.1 自由群

设 S 为任意集合。我们期望由 S 来生成一个群 $F(S)$. 对于集合S, 定义集合$S^{-1} = \{x^{-1} \,|\, x \in S\}$, 其中元素没有实际意义, 只是一个和$S$之间存在一一映射的集合.

首先, 我们来看由字母生成字的过程: 将一串字母串起来, 就构成了一个字。如此类比, 可以认为 $\widetilde{F(S)}$ 是由 $S\bigcup S^{-1}$ 中的元素作为字母生成的字的全体, 首先希望在 $\widetilde{F(S)}$ 上定义一些运算:

(i) $\widetilde{F(S)}$ 上的二元运算。如果 $w_1 = x_1\cdots x_n, w_2 = y_1\cdots y_m$, 则该运算是将 w_1 与 w_2 串联起来, 得到

$$w_1 \cdot w_2 = x_1\cdots x_n y_1\cdots y_m.$$

显然二元运算满足结合律.

(ii) $\widetilde{F(S)}$ 中的**单位元**。它与任何字 w 串联起来还是 w, 可以认为它就是“空字”。

由(i)-(ii), 我们可以令

$$\widetilde{F(S)} = \{1\} \cup \{x_1x_2\cdots x_n \mid x_i \in S\cup S^{-1}, 1 \leqslant i \leqslant n\} \tag{2.25}$$

其中1就是单位元.

注记. 作为集合$\widetilde{F(S)}$中的元素没有任何关系. 在$\widetilde{F(S)}$中, 对$w = x_1\cdots x_n$形式定义$w^{-1} = x_n^{-1}\cdots x_1^{-1}$. 其中若$x_i = y^{-1} \in S^{-1}$则定义$x_i^{-1} = y$.

定义2.58. 对于$w, u \in \widetilde{F(S)}$, 称$w$与$u$**等价**（记作$w \sim u$）如果通过有限次下述变换可以从$w$得到$u$或者从$u$得到$w$：

(1) 插入xx^{-1} 或者$x^{-1}x$ $(x \in S)$；

(2) 删去（消去）xx^{-1} 或者$x^{-1}x$ $(x \in S)$。

显然(1)和(2)是互逆的过程，从而上述关系是$\widetilde{F(S)}$字之间的等价关系。令$\widetilde{F(S)}/\sim$是相应等价类的集合，记$w \in \widetilde{F(S)}$所在的等价类为$[w]$，即

$$[w] = \{u \in \widetilde{F(S)} \mid w \sim u\}.$$

首先等价关系有以下性质：

命题2.59. 若$w \sim w'$，并且$u \sim u'$，则$wu \sim w'u'$。

证明. 由等价的定义我们有：$wu \sim w'u \sim w'u'$。 □

我们在$F(S)$上定义乘法：对于$[w], [u] \in F(S)$，令$[w]\cdot[u] \triangleq [wu]$。由上述命题，我们知道乘法是well-defined（和等价类的代表元选取无关），并且有

$$[w][1] = [w] = [1][w], \quad [w][w^{-1}] = [1] = [w^{-1}][w], \quad ([w][u])[v] = [w]([u][v]).$$

也就是$F(S)$在上述乘法下构成群，称为集合S生成的自由群。

定义2.60. 字 w 称为**简化字**(或称**既约字**), 如果 w 中没有形如 $a^{-1}a(a \in S\cup S^{-1})$ 的字串。

首先，字$w \in \widetilde{F(S)}$，对字的长度进行归纳，通过上面等价定义的(2)将w变成长度更短的字，直到不能消去，从而得到$[w]$一定含有简化字。特别地，我们有

命题2.61. 对$w \in \widetilde{F(S)}$, $[w]$含有唯一一个简化字。

证明. 令R是$\widetilde{F(S)}$中所有简化字组成的集合。下面我们来定义群$F(S)$在R上的作用，首先定义$\widetilde{F(S)}$在R上的作用，对于$x \in S \cup S^{-1}$，定义$f_x : R \longrightarrow R$如下

$$f_x(x_1x_2\cdots x_n) = \begin{cases} xx_1\cdots x_n, & \text{若 } x \neq x_1^{-1}, \\ x_2x_3\cdots x_n, & \text{若 } x = x_1^{-1}. \end{cases}$$

特别地，我们有$f_{x^{-1}} \circ f_x = \mathrm{id}_R = f_1$，从而映射$f_x \in S_R$，也就是$R$上的一个置换。对$w = x_1\cdots x_n \in \widetilde{F(S)}$，令

$$f_w \triangleq f_{x_1} \circ f_{x_2} \circ \cdots \circ f_{x_n} \in S_R.$$

由定义我们有：若$w \sim u$，则$f_w = f_u$。从而可以定义$f : F(S) \longrightarrow S_R$，$[w] \mapsto f_w$，并且$f$是群同态。

如果$w \sim u$并且均为简化字，则$[w] = [u]$，故有$f_w = f([w]) = f([u]) = f_u$。如果简化字$w = x_1x_2\cdots x_n$，则$f_w = f_{x_1} \circ f_{x_2} \circ \cdots \circ f_{x_n}$，从而

$$f_w(1) = f_{x_1} \circ \cdots \circ f_{x_n}(1) = f_{x_1} \circ \cdots \circ f_{x_{n-1}}(x_n) = \cdots = x_1\cdots x_{n-1}x_n = w.$$

类似的，对u我们有$f_u(1) = u$。从而$w = f_w(1) = f_u(1) = u$。 □

现在我们可以重新如下定义自由群：

定义2.62. 群

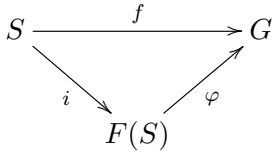
$$F(S) = \{1\} \cup \{x_1x_2\cdots x_n \mid x_i \in S \cup S^{-1}\} \tag{2.26}$$

称为由 S 生成的**自由群** (free group), 其乘法为字的串联, 且两个字相等当且仅当它们有相同的简化形式(当且仅当他们等价). 如果 S 有限, 称 $F(S)$ 为**有限生成自由群** (finitely generated free group).

注记. 由于上述定义中的相等等同于$\widetilde{F(S)}$上的等价，从而两种定义是等价的.

例如 $S = \{a\}$, 则 $F(S) = \langle a\rangle = \{a^n \mid n \in \mathbb{Z}\}$ 为无限循环群. 如果 $|S| \geqslant 2$, $F(S)$ 为无限非阿贝尔群.

定理2.63 (自由群的泛性质)**.** 设 G 为群, S 为集合, $f : S \to G$ 为集合间的映射, 则 f 可以唯一扩充为群同态 $\varphi : F(S) \to G$; 换言之, 即存在唯一的群同态 $\varphi : F(S) \to G$, 使得图表



交换, 这里$i : S \to F(S)$ 为自然的包含映射.

证明. 显然$\varphi(1)=1_G$. 对 $w=a_1\cdots a_n, a_i\in S\cup S^{-1}$, 只需定义

$$\varphi(a_1\cdots a_n)=\varphi(a_1)\cdots\varphi(a_n)$$

且我们应该有

$$\varphi(a_i)=\begin{cases} f(a_i), & \text{若 } a_i\in S,\\ f(x)^{-1}, & \text{若 } a_i=x^{-1}\in S^{-1}. \end{cases}$$

则 φ 为唯一的延拓 f 的群同态。由于$\varphi(x)\varphi(x^{-1})=1_G$，因此$F(S)$中相等的字定义的像是一样的。 □

在定理 2.63的条件中取 $S\subseteq G$, f是嵌入映射, 如果 S 生成 G, 则 $\varphi: F(S)\to G$ 是群的满同态, 即 G 为 $F(S)$ 的商群. 特别地

(1) 取 $S=G$, 我们得到 G 是自由群的商群.

(2) 如果 S 有限, 即 G 为有限生成群, 则 G 是有限生成自由群的商群.

综上所述, 我们有定理

定理2.64. 每个群都是自由群的商群, 每个有限生成群都是有限生成自由群的商群.

§2.5.2 群的表现

设 G 为群, 根据定理 2.64, 存在集合 $S\subseteq G$ 使得 G 是自由群 $F(S)$ 的商群, 即 $G=F(S)/N$. 如果 G 是有限生成的, 我们可以假设 S 为有限集.

定义2.65. 如果 $G=F(S)/N$, 则 G 的**表现** (presentation)记为

$$\langle S\mid r=1,\ \text{其中 } r\in N\rangle.$$

N就是$F(S)$中一些字的集合，本来S里的元素没有关系（自由的），对于$r\in N$，$r=1$，就是S里的元素有了约束，模掉这些约束关系，可以理解为商群里的元素比$F(S)$少了很多，具体看后面的例子理解。特别地, 如果 $R=\{r_1,\cdots,r_n\}\subseteq N$ 且包含 R 的最小正规子群为 N （也就是$r_1,\cdots,r_n$生成的正规子群，即包含这些元的正规子群的交）, 则 G 的表现为

$$G=\langle S\mid r_1=r_2=\cdots=r_n=1\rangle.$$

S 中的元素称为 G 的**生成元** (generator), N 中的元素(或 R 中的元素)构成生成元的**生成关系** (relation).

注记. $S\subseteq G$，则由S生成的G的正规子群是

$$\{(g_1x_1g_1^{-1})(g_2x_2g_2^{-1})\cdots(g_nx_ng_n^{-1})\mid x_i\in S\cup S^{-1},\ g_i\in G,\ n\in\mathbb{Z}_{\geq 0}\}.$$

例2.66. 循环群 $\mathbb{Z}/n\mathbb{Z}\cong\langle a\rangle/\langle a^n\rangle$, 从而可以表现为 $\langle a\mid a^n=1\rangle$.

例2.67. 二面体群 D_n 的表现. 首先二面体群有生成元 σ(旋转), τ(反射), 其中 $\sigma^n=\tau^2=1$ 且 $(\sigma\tau)^2=1$. 令 $S=\{\sigma,\tau\}$, 则 $S\hookrightarrow D_n$ 诱导 $F(S)\to D_n$ 的满同态 φ. 令 $N=\ker\varphi$, 则我们有 $\sigma^n,\tau^2,(\sigma\tau)^2\in N$. 令 K 是由 $\sigma^n,\tau^2,(\sigma\tau)^2$ 生成的正规子群, 则 $K\subseteq N$, 即有

$$F(S)/K\twoheadrightarrow F(S)/N\twoheadrightarrow D_n.$$

另一方面, $F(S)/K$ 中的元素均可写为 $\sigma^i\tau^j(0\leqslant i\leqslant n-1,0\leqslant j\leqslant 1)$ 的形式, 故 $|F(S)/K|\leqslant 2n$, 所以我们必有 $K=N$, 于是

$$D_n=\langle\sigma,\tau\mid\sigma^n=\tau^2=(\sigma\tau)^2=1\rangle.$$

由前面的讨论$F(S)$中的每个元素都可以写成唯一简化字的形式，如果再合并同类项，则有

$$w=x_1^{m_1}x_2^{m_2}\cdots x_r^{m_r},\ \text{其中}x_i\in S,\ m_i\in\mathbb{Z}\setminus\{0\}\ \text{并且}x_i\neq x_{i+1}.$$

上述表达称为**正则形式**。从而$F(\sigma,\tau)$中元素的一般形式为：

$$\tau^{j_0}\sigma^{i_1}\tau^{j_1}\sigma^{i_2}\tau^{j_2}\cdots\sigma^{i_r}\tau^{j_r}\sigma^{i_0}$$

其中i_k,j_k是非零整数，$1\leq k\leq r$，而i_0和j_0可以取任意整数。进而我们可以讨论关系K对元素形式的影响。 □

我们下面来讨论群 G 的换位子群.

定义2.68. 设 G 为群. 对于 $a,b\in G$, a 与 b 的**换位子** (commutator) $[a,b]$ 定义为 $aba^{-1}b^{-1}$. 由 G 中所有换位子生成的子群称为 G 的**换位子群** (commutator subgroup), 记为 $G'=[G,G]$.

命题2.69. (1) G' 是 G 的正规子群, G/G' 为阿贝尔群.

(2) 设 A 为阿贝尔群, $\varphi:G\to A$ 为同态, 则 $\ker\varphi\supseteq G'$, 且 φ 诱导同态

$$\overline{\varphi}:G/G'\to A,\quad \overline{\varphi}(\overline{g})=\varphi(g).$$

也就是说, G到阿贝尔群的任何同态均通过自然商映射$\pi:G\to G/G'$ 分解.

注记. 由命题可知 G/G' 是 G 的最大阿贝尔商群.

证明. (1) 我们有

$$g[a,b]g^{-1}=gaba^{-1}b^{-1}g^{-1}=\big((ga)b(a^{-1}g^{-1})b^{-1}\big)(bgb^{-1}g^{-1})=[ga,b][b,g],$$

故 $G'\lhd G$. 由 $\overline{a}\,\overline{b}\,\overline{a^{-1}}\,\overline{b^{-1}}=1$, 故 $\overline{a}\,\overline{b}=\overline{b}\,\overline{a}$, 即 G/G' 是阿贝尔群.

(2) 由 φ 为同态知

$$\varphi([a,b])=\varphi(a)\varphi(b)\varphi(a)^{-1}\varphi(b)^{-1}=1,$$

故 $[a,b]\in\ker\varphi$, 从而$G'\lhd\ker\varphi$, 所以我们有

$$\varphi:G\to G/G'\to G/\ker\varphi\to A,$$

得到诱导同态 $\overline{\varphi}:G/G'\to A$. □

命题2.70. 设 $\varphi : F(S) \to G$ 为满同态. 则 φ 诱导满同态

$$\overline{\varphi} : F(S)/F(S)' \to G/G', \quad \overline{\varphi}(\overline{g}) = \overline{\varphi(g)}.$$

换言之, 我们有交换图表

$$\begin{array}{ccc} F(S) & \xrightarrow{\varphi} & G \\ \downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle \pi} \\ F(S)/F(S)' & \xrightarrow{\overline{\varphi}} & G/G'. \end{array}$$

证明. 我们有满同态

$$\widetilde{\varphi} : F(S) \to G \to G/G', \quad \widetilde{\varphi}(g) = \overline{\varphi(g)}.$$

由命题 2.69(2) , 诱导了满同态

$$\overline{\varphi} : F(S)/F(S)' \to G/G', \quad \overline{\varphi}(\overline{g}) = \overline{\varphi(g)}. \qquad \square$$

由命题 2.70 可知, 如果 G 的表现为

$$G = \langle S \mid r_1 = r_2 = \cdots = r_n = 1 \rangle,$$

则G/G' 的表现为

$$G/G' = \langle S \mid r_1 = r_2 = \cdots = r_n = 1, xy = yx, \text{ 对任意的 } x, y \in S \rangle.$$

特别地, $F(S)/F(S)'$ 的表现为

$$F(S)/F(S)' = \langle S \mid xy = yx, \text{ 对任意的 } x, y \in S \rangle.$$

我们将在下节详细讨论此群.

习　　题

习题2.5.1. 证明或否定: 两个生成元的自由群同构于两个无限循环群的积.

习题2.5.2. 设 F 是 x, y 生成的自由群.

(1) 证明两个元素 $u = x^2$ 和 $v = y^3$ 生成 F 的一个子群, 它同构于 u, v 上的自由群.

(2) 证明三个元素 $u = x^2$, $v = y^2$ 和 $z = xy$ 生成 F 的一个子群, 它同构于 u, v, z 上的自由群.

习题2.5.3. 若 n 为正奇数,求证: $D_{2n} \cong D_n \times \mathbb{Z}/2\mathbb{Z}$.

习题2.5.4. 若 $n \geq 3$, $A_n \times \mathbb{Z}/2\mathbb{Z}$ 与 S_n 是否同构?

习题2.5.5. 设 $G = G_1 \times \cdots \times G_n$, H 为 G 的子群. 问 H 是否一定形如 $H = H_1 \times \cdots \times H_n$, 其中 $H_i \leqslant G_i, 1 \leqslant i \leqslant n$.

习题2.5.6. 设 G_1 和 G_2 是两个非交换单群. 证明 $G_1 \times G_2$ 的非平凡正规子群只有 G_1 和 G_2.

习题2.5.7. 证明 $5 \cdot 7 \cdot 13$ 阶群一定是循环群.

习题2.5.8. (1) 求出圆的对称群.

(2) 求出球的对称群.

(3) 试求出圆柱体的对称群.

习题2.5.9. 给定两个水平平面, 在顶面有三个点, 它们在底面有正投影. 把顶面的三个点与底面的正投影分别用三根不相交的绳子连接起来, 且每根绳子与两平面之间的每一个水平面恰好相交一次, 这样的三根绳子称为一个 3- **辫子**. 给定两个 3-辫子 a, b, 将 b 放在 a 下面连接起来得到一个新的辫子, 称为 a 和 b 的乘法. 试证明所有的 3-辫子构成一个群, 并确定它的表现.

习题2.5.10. 设 G 由 n 个元素生成, 而 G 的子群 A 具有有限指数. 求证: A 可以由 $2n(G : A)$ 个元素生成.

习题2.5.11. 令 $G = G_1 \times G_2 \times \cdots \times G_n$, 且对任意 $i \neq j$, $|G_i|$ 和 $|G_j|$ 互素. 证明 G 的任意子群 H 都是它的子群 $H \cap G_i$ $(i = 1, 2, \cdots, n)$ 的直积.

§2.6 有限生成阿贝尔群的结构

§2.6.1 有限生成自由阿贝尔群

定义2.71. 对于集合 S, 群

$$\mathbb{Z}(S) = F(S)/F(S)' = \langle S \mid xy = yx,\ x, y \in S \rangle \tag{2.27}$$

称为由 S 生成的**自由阿贝尔群** (free abelian group).

如果 S 为有限集, 称 $\mathbb{Z}(S)$ 为**有限生成自由阿贝尔群** (finitely generated free abelian group).

定义2.72. 设 S 为集合, **直和** (direct sum) $\bigoplus\limits_{x \in S} \mathbb{Z}$ 定义为

$$\bigoplus_{x \in S} \mathbb{Z} = \{a = (a_x)_{x \in S} \mid a_x \in \mathbb{Z} \text{ 且只有有限个 } a_x \neq 0\}.$$

由定义知 $\bigoplus\limits_{x \in S} \mathbb{Z}$ 在加法意义下构成阿贝尔群, 且当 S 为有限集时, $\bigoplus\limits_{x \in S} \mathbb{Z} \cong \mathbb{Z}^{|S|}$.

定理2.73. (1) $\mathbb{Z}(S) \cong \bigoplus_{x\in S} \mathbb{Z}$.

(2) 如果 $m \neq n$, 则 $\mathbb{Z}^m$ 与 $\mathbb{Z}^n$ 不同构.

证明. 令

$$f : S \longrightarrow \bigoplus_{x\in S} \mathbb{Z}, \quad x \longmapsto f(x) = (a_{x,y})_{y\in S}$$

为映射, 其中 $a_{x,x} = 1$ 且 $a_{x,y} = 0$ 如果 $x \neq y$ (也就是x的位置是1其他位置是0的元素, 由 $\bigoplus_{x\in S} \mathbb{Z}$定义可知这些元素生成整个群 $\bigoplus_{x\in S} \mathbb{Z}$). 由自由群的泛性质(定理 2.63), f 可以唯一扩充为满同态

$$\varphi : F(S) \longrightarrow \bigoplus_{x\in S} \mathbb{Z}.$$

再由于 $\bigoplus_{x\in S} \mathbb{Z}$ 是阿贝尔群, 由命题 2.69, 我们得到满同态

$$\overline{\varphi} : \mathbb{Z}(S) = F(S)/F(S)' \longrightarrow \bigoplus_{x\in S} \mathbb{Z}.$$

再由 $\mathbb{Z}(S)$ 的定义, 任何 $\mathbb{Z}(S)$ 中的元素可以写成 $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ 的形式, 其中 $\alpha_i \in \mathbb{Z}, x_i$ 两两不同, 故

$$\overline{\varphi}(x_1^{\alpha_1} \cdots x_n^{\alpha_n}) = \alpha_1 f(x_1) + \cdots + \alpha_n f(x_n).$$

由$f(x)$的定义知 $\overline{\varphi}(x_1^{\alpha_1} \cdots x_n^{\alpha_n}) = 0$ 等价于 $\alpha_1 = \cdots = \alpha_n = 0$, 即 $x_1^{\alpha_1} \cdots x_n^{\alpha_n} = 1$, 故 $\overline{\varphi}$ 为单同态, 所以

$$\overline{\varphi} : \mathbb{Z}(S) \xrightarrow{\sim} \bigoplus_{x\in S} \mathbb{Z}.$$

(2) 如果 $m \neq n$, 且有同构 $\tau : \mathbb{Z}^m \to \mathbb{Z}^n$, 则 $\tau((k\mathbb{Z})^m) = (k\mathbb{Z})^n$ 对所有 $k \geqslant 2$ 成立, $(\tau(kx) = \tau(x + \cdots + x) = \tau(x) + \cdots + \tau(x) = k\tau(x))$ 故 τ 诱导同构

$$\mathbb{Z}^m/(k\mathbb{Z})^m \xrightarrow{\sim} \mathbb{Z}^n/(k\mathbb{Z})^n.$$

但上式左边元素个数等于 k^m, 右边元素个数等于 k^n, 矛盾! □

由定理 2.73, 立知

推论2.74. 有限生成自由阿贝尔群 $\mathbb{Z}(S)$ 同构于 $\mathbb{Z}^{|S|}$, 且在同构意义下, $\mathbb{Z}(S)$ 由 $|S|$ 唯一确定.

定义2.75. 有限生成自由阿贝尔群 $G = \mathbb{Z}(S)$ 的**秩** (rank) 定义为$|S|$, 记为 rank G.

如果存在G 的子集合B, 使得$G \cong \mathbb{Z}(B)$, 则称B 为 G 的一组**基** (basis).

注记. 由定义立知S 是$\mathbb{Z}(S)$ 的基. 另一方面, 若G为有限生成阿贝尔群, 则由定理 2.73, 知G不同的基所含的元素个数相等并且等于有限生成阿贝尔群G的秩.

§2.6.2 有限生成阿贝尔群的结构定理

我们假设 G 是有限生成阿贝尔群, 记 G 的运算为加法.

定理2.76. 设 G 是有限生成自由阿贝尔群, H 为 G 的非零子群, 则 H 也是有限生成自由阿贝尔群, 且 $\mathrm{rank}(H) \leqslant \mathrm{rank}(G)$. 更具体地说, 存在 G 的一组基 $\{x_1, \cdots, x_n\}$, 正整数 $r \leqslant n$, 正整数 $d_1 \mid d_2 \mid \cdots \mid d_r$, 使得 H 是以 $\{d_1x_1, \cdots, d_rx_r\}$ 为基的自由阿贝尔群.

证明. 令集合

$$I = \{s \in \mathbb{Z} \mid 存在G的一组基y_1, \cdots, y_n, \alpha \in H, \alpha = sy_1 + k_2y_2 + \cdots + k_ny_n\}.$$

我们注意到如果 $H \neq 0$, 则 $I \neq 0$ 且

- 如果 $s \in I$, $m \in \mathbb{Z}$, 则$m\alpha \in H$, 故有$ms \in I$. 从而 I 中有正整数.
- 由于 $\{y_2, y_1, \cdots, y_n\}$ 也是一组基, 故 $k_2 \in I$. 同理 $k_i \in I$.

由此, 令 d_1 为 I 中最小正整数, 则存在 $\alpha \in H$, 基 $\{y_1, y_2, \cdots, y_n\}$ 使得 $\alpha = d_1y_1 + k_2y_2 + \cdots + k_ny_n$. 令 $k_i = q_id_1 + r_i$ $(0 \leq r_i < d_1)$, 则

$$\alpha = d_1(y_1 + q_2y_2 + \cdots + q_ny_n) + r_2y_2 + \cdots + r_ny_n.$$

由于 $\{y_1 + q_2y_2 + \cdots + q_ny_n, y_2, \cdots, y_n\}$ 还是一组基, 故 $r_i \in I$. 由 d_1 的最小性知 $r_i = 0$. 即存在 $\alpha \in H$, 基 $\{x_1, y_2, \cdots, y_n\}$ 使得 $\alpha = d_1x_1$. 固定此 x_1, 对于 G 的任何一组基$\{x_1, x_2, \cdots, x_n\}$ 及元素$\beta \in H$, 记 $\beta = s_1x_1 + s_2x_2 + \cdots + s_nx_n$, 由于$\beta + \mathbb{Z}\alpha \subseteq H$, 立即有$d_1 \big| s_1$, 故

$$\beta' = d_1x_1 + s_2x_2 + \cdots + s_nx_n = \beta - (\frac{s_1}{d_1} - 1)\alpha \in H,$$

由上述同样讨论知 $d_1 \mid s_i$ 对所有$1 \leq i \leq n$ 成立.

我们现在对 G 的秩作归纳. 如果 $n = 1$, 定理显然成立. 假设定理对任意秩 $< n$ 的有限生成自由阿贝尔群成立, 当$\mathrm{rank}G = n$, $\{0\} \neq H \leqslant G$时取上述d_1和x_1, 并固定G的一组基$\{x_1, y_2, \cdots, y_n\}$. 令 $G_1 = \langle y_2, \cdots, y_n\rangle$, 我们断言

$$H = \langle\alpha\rangle \oplus (H \cap G_1).$$

事实上, 由于 $x_1, y_2, \cdots, y_n$ 为 G 的基, $\langle x_1\rangle \cap G_1 = \{0\}$, 故 $\langle\alpha\rangle \cap (H \cap G_1) = \{0\}$. 又若 $x \in H$,

$$x = k_1x_1 + k_2y_2 + \cdots + k_ny_n,$$

由于 $d_1 \mid k_1$, 故$k_1x_1 \in \langle\alpha\rangle \subseteq H$. 从而$k_2y_2 + \cdots + k_ny_n = x - k_1x_1 \in H$, 故$x \in \langle\alpha\rangle + (H \cap G_1)$, 断言证毕.

现在如果 $G_1 \cap H = \{0\}$, 则 $H = \langle d_1x_1\rangle$, 定理成立. 如果$G_1 \cap H \neq \{0\}$, 则 $G_1 \cap H$ 是有限生成自由阿贝尔群 G_1 的子群. 由于 $\mathrm{rank}G_1 = n - 1$, 由归纳假设, 存在 G_1 的一组基 $\{x_2, \cdots, x_n\}, d_2 \mid d_3 \mid \cdots \mid d_r$, 使得 $G_1 \cap H = \langle d_2x_2, \cdots, d_rx_r\rangle$, 则 $\{x_1, \cdots, x_n\}$ 为 G 的一组基, 使得 $\{d_1x_1, \cdots, d_rx_r\}$ 为 H 的基, 且由 d_1 的性质, $d_1 \mid d_2$, 定理证毕. □

定理2.77. 有限生成阿贝尔群 A 均有如下结构

$$A \cong \mathbb{Z}^r \oplus \mathbb{Z}/m_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/m_s\mathbb{Z},$$

其中 $m_1 \mid m_2 \mid \cdots \mid m_s$ 为正整数.

证明. 设 $F(S) \to A$ 为满同态, 其中 S 为有限集. 由于 A 为阿贝尔群, φ 诱导满同态

$$\varphi : \mathbb{Z}(S) = F(S)/F(S)' \to A.$$

则 $\ker\varphi$ 是 $\mathbb{Z}(S)$ 的子群. 由定理 2.76, 存在 $\mathbb{Z}(S)$ 的一组基 $\{x_1, \cdots, x_n\}$ 及正整数 $m_1 \mid m_2 \mid \cdots \mid m_s$, 使得 $\{m_1x_1, \cdots, m_sx_s\}$ 是 $\ker\varphi$ 的基, 故

$$A = \mathbb{Z}(S)/\ker\varphi = \mathbb{Z}^{n-s} \oplus \mathbb{Z}/m_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/m_s\mathbb{Z}.$$

定理证毕. □

定义2.78. 设 A 是有限生成阿贝尔群, 定义它的**扭子群** (torsion subgroup)

$$A_t = \{a \in A \mid a\text{的阶有限}\}. \tag{2.28}$$

容易看出 A_t 的确是 A 的子群, 且对于群

$$\mathbb{Z}^r \oplus \mathbb{Z}/m_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/m_s\mathbb{Z},$$

其扭子群为 $\mathbb{Z}/m_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/m_s\mathbb{Z} = T$, 为有限群. 事实上, 考虑元素

$$(a_1, a_2, \ldots, a_r, b_1, b_2, \ldots, b_s) \in \mathbb{Z}^r \oplus \mathbb{Z}/m_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/m_s\mathbb{Z},$$

就可以确定其扭子群. 由上述定理, 我们有

推论2.79. (1) $A = A_t \oplus A_f$, 其中 A_f 是有限生成自由阿贝尔群.

(2) $A \cong B$ 当且仅当 $A_t \cong B_t$ 且 $\mathrm{rank}A_f = \mathrm{rank}B_f$.

证明. (1) 设 $\varphi : A \cong \mathbb{Z}^r \oplus T$, 令 $A_f = \varphi^{-1}(\mathbb{Z}^r), A_t = \varphi^{-1}(T)$, 则 A_t 为 A 的扭子群, 且 A_f 为秩为 r 的自由群. 由于φ是群同构, 从而得到(1)要求的直和分解.

(2) 设 $\varphi : A \cong B$, 则由扭子群定义有$\varphi(A_t) = B_t$ (有限阶元映到有限阶元)，故$A_t \cong B_t$. 设有限群的阶$|A_t| = |B_t| = k$，则由$A \cong B$得到$kA \cong kB$，也就是$kA_f \cong kB_f$，而对于自由群有$\mathrm{rank}(kA_f) = \mathrm{rank}A_f$，$\mathrm{rank}(kB_f) = \mathrm{rank}B_f$, 因此得到$\mathrm{rank}A_f = \mathrm{rank}B_f$。命题的充分性是显然的。 □

注记. 若阿贝尔群A, B有$A \cong B$，而且$C \le A$, $D \le B$，满足$C \cong D$，也不能得到$A/C \cong B/D$. 例如$A = B = \mathbb{Z}_2 \oplus \mathbb{Z}_4$, 令$C = \mathbb{Z}_2 \oplus \{0\} \cong \mathbb{Z}_2$，$D = \{0\} \oplus 2\mathbb{Z}_4 \cong \mathbb{Z}_2$, 但是

$$A/C \cong \mathbb{Z}_4 \ncong \mathbb{Z}_2 \oplus \mathbb{Z}_2 \cong B/D.$$

定理2.80. 设 $A \neq \{0\}$ 为有限阿贝尔群, 则

(1) $A \cong \mathbb{Z}/m_1\mathbb{Z} \oplus \cdots \mathbb{Z}/m_s\mathbb{Z}$, 正整数 $1 < m_1 \big| \cdots \big| m_s$ 由 A 唯一确定.

(2) $A \cong \mathbb{Z}/p_1^{\alpha_1}\mathbb{Z} \oplus \cdots \mathbb{Z}/p_t^{\alpha_t}\mathbb{Z}$, 其中 $p_1, \cdots, p_t$ 为素数, $\alpha_i \geq 1$, 且 $p_1^{\alpha_1}, \cdots, p_t^{\alpha_t}$ 由 A 唯一确定.

证明. 由于 A 有限, 则 $A = A_t$ 没有无限阶元, 故 A 有(1)的形式, 又由中国剩余定理, 如果 $m = p_1^{\alpha_1} \cdots p_s^{\alpha_s}$, 则

$$\mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}/p_1^{\alpha_1}\mathbb{Z} \oplus \cdots \mathbb{Z}/p_s^{\alpha_s}\mathbb{Z}.$$

故 A 有(2)的形式. 我们需要证明唯一性.

首先我们证明(2)的唯一性. 由于 A 是阿贝尔群, 它的所有子群都是正规子群, 从而对$|A|$的任意素因子p, A都有唯一的西罗p-子群. 我们有

$$A = \bigoplus_p A_p = A_{p_1} \oplus \cdots \oplus A_{p_t}$$

的形式, 其中 A_p 是 A 的Sylow p 子群, 由A唯一确定. 故不妨假设 A 本身是 p 群, 我们要证明

$$A \cong \mathbb{Z}/p^{\alpha_1}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p^{\alpha_r}\mathbb{Z} \ (1 \leq \alpha_1 \leqslant \cdots \leqslant \alpha_r) \tag{2.29}$$

唯一. 如不然, 令

$$A \cong \mathbb{Z}/p^{\beta_1}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p^{\beta_{r'}}\mathbb{Z} \ (1 \leq \beta_1 \leqslant \cdots \leqslant \beta_{r'}). \tag{2.30}$$

考虑 A/pA, 式(2.29)说明 $|A/pA| = p^r$, 式(2.30)说明 $|A/pA| = p^{r'}$, 故 $r = r'$. (也可以对r归纳! 由$p^{\alpha_1}A$和$p^{\beta_1}A$的两种同构形式，有$\alpha_1 = \beta_1$，并且由归纳知道剩下的一样，从而$\alpha_1 = \beta_1$出现的次数也相同。) 我们对 k 作归纳证明 $\alpha_k = \beta_k$. 如果 $\alpha_1 = \beta_1, \cdots, \alpha_{k-1} = \beta_{k-1}$ 但 $\alpha_k < \beta_k$, 则由式(2.29), $|p^{\alpha_k}A/p^{\alpha_k+1}A| \leqslant p^{r-k}$, 但由式(2.30), $|p^{\alpha_k}A/p^{\alpha_k+1}A| = p^{r-k+1}$, 矛盾. 故 $\alpha_k = \beta_k$, 即(2.29)与(2.30)形状一样, (2)的唯一性证毕.

对于(1)的唯一性, 对任何 p, 考虑 A 的Sylow p子群. 由(2)

$$A_p \cong \mathbb{Z}/p^{\alpha_1}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p^{\alpha_r}\mathbb{Z}, \ \alpha_1 \leqslant \cdots \leqslant \alpha_r.$$

由(1)以及Sylow p 子群的阶数有,

$$A_p = (\mathbb{Z}/m_1\mathbb{Z})_p \oplus \cdots \oplus (\mathbb{Z}/m_s\mathbb{Z})_p$$

由于 $m_1 \big| m_2 \big| \cdots \big| m_s$, 且 $(\mathbb{Z}/m\mathbb{Z})_p$ 为循环群, 故必有

$$(\mathbb{Z}/m_s\mathbb{Z})_p \cong \mathbb{Z}/p^{\alpha_r}\mathbb{Z}, \quad (\mathbb{Z}/m_{s-1}\mathbb{Z})_p \cong \mathbb{Z}/p^{\alpha_{r-1}}\mathbb{Z}, \quad \cdots.$$

也就是$m_s = p^{\alpha_r}n_s$, $(n_s, p) = 1$. 由此, $m_s, m_{s-1}, \cdots$ 均唯一确定. □

也可以先证明(1)的唯一性. 若有$A \cong \mathbb{Z}/n_1\mathbb{Z} \oplus \cdots \mathbb{Z}/n_s\mathbb{Z}$, 正整数 $1 < n_1 \big| \cdots \big| n_k$. 首先，对于$a, b \in \mathbb{Z}$, 关于循环群我们有如下结果：

$$a(\mathbb{Z}/b\mathbb{Z}) \cong (a,b)\mathbb{Z}/b\mathbb{Z} \cong \mathbb{Z}/\tfrac{b}{(a,b)}\mathbb{Z}.$$

从而由$m_sA = 0$, 可以得到$m_s(\mathbb{Z}/n_i\mathbb{Z}) = 0$，故有$n_k \big| m_s$. 而$n_kA = 0$使得$m_s \big| n_k$，从而有$m_s = n_k$。然后再考虑$n_{k-1}$与$m_{s-1}$分别作用到$A$上，首先$|m_{s-1}A| = \frac{m_s}{m_{s-1}}$, 而同时有$|m_{s-1}A| \geq \frac{n_k}{(n_k, m_{s-1})} = \frac{m_s}{m_{s-1}}$. 故得到$m_{s-1}(\mathbb{Z}/n_{k-1}\mathbb{Z}) = 0$，从而有$n_{k-1} \big| m_{s-1}$. 类似有$m_{s-1} \big| n_{k-1}$，则有$n_{k-1} = m_{s-1}$. 然后由$|m_{s-2}A| = \frac{m_{s-1}}{m_{s-2}} \cdot \frac{m_s}{m_{s-2}}$, 以及$|m_{s-2}A| \geq \frac{n_{k-1}}{(n_{k-1}, m_{s-2})} \frac{n_k}{(n_k, m_{s-2})}$，得到$m_{s-2} \big| n_{k-2}$, ... 依次类推，有$m_{s-i} = n_{k-i}$, $i = 0, 1, \ldots$. 另外由于$|A| = m_1 m_2 \cdots m_s = n_1 n_2 \cdots n_k$，从而得到$k = s$，并且$m_i = n_i$，$1 \leq i \leq s$.

定义2.81. 上述定理中 $\{p_1^{\alpha_1}, \cdots, p_t^{\alpha_t}\}$ 称为 A 的**初等因子组**, 其中元素称为**初等因子** (elementary divisors); $\{m_1, \cdots, m_s\}$ 称为 A 的**不变因子组**, 其中元素称为**不变因子** (invariant factors).

我们可以综合上述定理得到

定理2.82 (**有限生成阿贝尔群的结构定理**). (1) 设 A 为有限生成阿贝尔群, 则

$$A \cong \mathbb{Z}^r \oplus \mathbb{Z}/m_1\mathbb{Z} \oplus \cdots \mathbb{Z}/m_s\mathbb{Z} \cong \mathbb{Z}^r \oplus \mathbb{Z}/p_1^{\alpha_1}\mathbb{Z} \oplus \cdots \mathbb{Z}/p_t^{\alpha_t}\mathbb{Z}$$

其中

(i) r 称为 A 的秩, 由 A 唯一确定.

(ii) $1 < m_1 \big| m_2 \big| \cdots \big| m_s$ 由 A 唯一确定.

(iii) $\{p_1^{\alpha_1}, \cdots, p_t^{\alpha_t}\}$ 由 A 唯一确定.

(2) 有限生成阿贝尔群 A 与 B 同构当且仅当其秩相同, 且其初等因子或不变因子也相同.

例2.83. 我们来讨论一下8 阶群G 的结构.

(1) 阿贝尔群. 此时初等因子可能有3 种情况: $\{8\}$, $\{2, 4\}$ 和$\{2, 2, 2\}$, 故共有3 种8 阶阿贝尔群: $\mathbb{Z}/8\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ 和$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$.

(2) 非阿贝尔群. 如果G中有8 阶元, 则G 是循环群; 如果其元素阶只为1 和2, 则G 为阿贝尔群(引理 1.66). 我们可以假设x 是G 的一个4 阶元, 则$(G : \langle x \rangle) = 2$, $\langle x \rangle$ 是G 的正规子群(命题 2.38). 令$y \in G \setminus \langle x \rangle$, 则$G = \{x^i, x^i y \big| i = 0, 1, 2, 3\}$.

考虑元素$y^{-1}xy \in \langle x \rangle$. 由于它与$x$ 同阶, 故$y^{-1}xy = x$ 或者x^3. 但由于x 与y 不交换, 故$y^{-1}xy = x^3 = x^{-1}$. 如果y 的阶为2, 则

$$G = \langle x,\ y \big| x^4 = y^2 = 1,\ yxy = x^{-1} \rangle \cong D_4.$$

如果y 的阶为4, 则(注意到$y^2 \in \langle x \rangle$并且为2阶元)

$$G = \langle x,\ y \big| x^4 = 1,\ x^2 = y^2,\ y^{-1}xy = x^{-1} \rangle.$$

我们考虑4**元数群**

$$Q_8 := \left\{ \pm I_2,\ \pm \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix},\ \pm \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},\ \pm \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \right\}. \tag{2.31}$$

则G 与Q_8 通过映射$x \mapsto \left(\begin{smallmatrix} i & 0 \\ 0 & -i \end{smallmatrix}\right)$, $y \mapsto \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$ 同构.

另外, 易知Q_8中$-I_2$是唯一的2阶元，而D_4中，至少x^2和y都是2阶元，故两个群不同构. 综上所述, 在同构意义下 8阶非阿贝尔群共有两个: D_4 和Q_8.

例2.84. 1500 阶阿贝尔群 A 的结构. 由$1500 = 2^2 \times 3 \times 5^3$, 它的初等因子组有如下可能: $\{2,2,3,5,5,5\}$, $\{2,2,3,5,25\}$, $\{2,2,3,125\}$, $\{4,3,5,5,5\}$, $\{4,3,5,25\}$, $\{4,3,125\}$, 故共有六种阿贝尔群($6 = P(2)\cdot P(1)\cdot P(3)$, 参考习题6.12), 其阶为 1500.

习　　题

习题2.6.1. 将 33 阶群和 18 阶群分类.

习题2.6.2. 有限生成阿贝尔群 G 是自由阿贝尔群当且仅当 G 的每个非零元素都是无限阶元素.

习题2.6.3. (1) 正有理数乘法群 $\mathbb{Q}^+$ 是自由阿贝尔群, 全部素数是它的一组基.

(2) $\mathbb{Q}^+$ 不是有限生成的.

习题2.6.4. $\mathbb{Q}$ 不是自由阿贝尔群.

习题2.6.5. 设有限阿贝尔群

$$A \cong \mathbb{Z}/p_1^{\alpha_1}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p_s^{\alpha_s}\mathbb{Z}, \quad (p_i \text{ 为素数}, \alpha_i \in \mathbb{Z}_+).$$

证明A 的任何子群B 均同构于$\mathbb{Z}/p_1^{\beta_1}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p_s^{\beta_s}\mathbb{Z}$, 其中$0 \le \beta_i \le \alpha_i$.

习题2.6.6. 设 G 是有限生成的自由阿贝尔群, $\mathrm{rank}(G) = r$. 如果 $g_1, g_2, \cdots, g_n$ 是 G 的一组生成元,则 $n \ge r$.

习题2.6.7. 设 A 为有限阿贝尔群, 对于 $|A|$ 的每个正因子 d, A 均有 d 阶子群和 d 阶商群.

习题2.6.8. 设 H 是有限阿贝尔群 A 的子群, 则存在 A 的子群同构于 A/H.

习题2.6.9. 如果有限阿贝尔群 A 不是循环群, 则存在素数 p 使得 A 有子群同构于 $(\mathbb{Z}/p\mathbb{Z})^2$.

习题2.6.10. 求出 $\mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$ 的不变因子和初等因子.

习题2.6.11. 求出 $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/9\mathbb{Z} \oplus \mathbb{Z}/35\mathbb{Z}$ 的不变因子和初等因子.

习题2.6.12. 设 n 为正整数, 问有多少个 n 阶阿贝尔群?

习题2.6.13. 设 p 是一个素数, 问 $\mathbb{Z}/p^2\mathbb{Z}\oplus\mathbb{Z}/p^3\mathbb{Z}$ 有多少个 p^2 阶子群?

习题2.6.14. $\mathbb{C}^\times$ 的每个有限子群都是循环群. 由此求出 $\mathbb{Z}/n\mathbb{Z}$ 到 $\mathbb{C}^\times$ 的所有群同态.

习题2.6.15. 设 G, A, B 均为有限阿贝尔群. 如果 $G\oplus A\cong G\oplus B$, 证明 $A\cong B$.

习题2.6.16. 设有限生成阿贝尔群 G 的秩为 1, $f: G\to\mathbb{Z}$ 为满同态, 则 $G\cong\mathbb{Z}\oplus\ker f$, 即 $\ker f$ 是 G 的扭子群.

习题2.6.17. 有限生成自由阿贝尔群有什么样的泛性质?

习题2.6.18. 将 $\mathbb{F}_p$ 上的 n 维向量空间 $\mathbb{F}_p^n$ 作为加法群.

(1) 试求 $\mathbb{F}_p^n$ 中 p^{n-1} 阶子群的个数.

(2) 证明 $\mathbb{F}_p^n$ 中 p^k 阶子群的个数等于 p^{n-k} 阶子群的个数.

§2.7 西罗定理续

定理2.85. 设$p^r||G|$，其中p为素数。以$\mathcal{N}(n)$表示G中n阶子群的个数，则$\mathcal{N}(p^r)\equiv 1(\mathrm{mod}\,p)$。

证明. 设$|G|=p^rn$。设 X 为 G 中所有 p^r 元子集构成的族, 即

$$X=\{U\subseteq G\mid |U|=p^r\}.$$

则

$$N=|X|=\binom{np^r}{p^r}.$$

考虑 G 在 X 上的左乘作用, 从而有

$$X=\bigcup_{U\in I}O_U,\ N=|X|=\sum_{U\in I}|O_U|,\ |O_U|=(G:G_U).$$

由于$G_UU=U$，现在考虑G的子群G_U左乘作用在U上，由轨道分解公式(2.6)，$U=\bigcup\limits_{x\in U}G_Ux$ 是 G_U 的一些右陪集的并, 从而是子群G_U的一些陪集的无交并，故 $|G_U||U|=p^r$ 是 p 的方幂，设$|G_U|=p^{r_U}$，$r_U\le r$。

(1). 如果$r_U<r$，则$|O_U|=(G:G_U)=np^{r-r_U}\equiv 0\,(\mathrm{mod}\,p)$；

(2). 否则$r_U=r$，则$|O_U|=n$，从而有

$$N=|X|=\sum_{U\in I}|O_U|\equiv\sum_{|O_U|=n}|O_U|=n\sum_{|O_U|=n}1\,(\mathrm{mod}\,p).$$

现在我们来计算 $\sum_{|O_U|=n} 1$，即长为n的轨道O_U的个数。由于$|O_U| = n$，从而有$|G_U| = p^r = |U|$，我们立即得到U等于G_U一个右陪集，也就是$U = G_U g$对于某个$g \in G$。现在我们得到G的p^r阶子群$B = g^{-1}G_U g = g^{-1}U \in O_U$，也就是如果$|O_U| = n$则$O_U$含有$G$的一个$p^r$阶的子群；另外如果$Y \leq G$并且有$Y \in O_U = O_B$，也就是$Y = g_1 B$对于某个$g_1 \in G$。由于$Y$是子群$B$的左陪集，又含有单位，自然有$Y = B$；最后，若$Y$是$G$的一个$p^r$阶子群，则$G_Y = Y$，从而有$O_Y = (G : G_Y) = n$。综上有，$G$的每个$p^r$阶子群均恰好在一个长为$n$的轨道之中，也就是有 $\sum_{|O_U|=n} 1 = \mathcal{N}(p^r)$。从而

$$\binom{np^r}{p^r} \equiv n\mathcal{N}(p^r) \,(\mathrm{mod}\, np).$$

这个同余式对任意np^r阶群G都成立，特别取G是循环群，则G只有一个p^r阶子群，代入立即有$\binom{np^r}{p^r} \equiv n \,(\mathrm{mod}\, np)$。再带回上式得到$n \equiv n\mathcal{N}(p^r) \,(\mathrm{mod}\, np)$，也就是$\mathcal{N}(p^r) \equiv 1(\mathrm{mod}\, p)$。

由公式 (2.12), $|G_U| \cdot |O_U| = |G|$, 由于 $|G_U|$ 是 p 的幂, $|O_U|$ 与 p 互素, 故 $|G_U| = p^r$, 所以 G_U 是 G 的 西罗 p 子群。 □

推论2.86. 设H是G的西罗 p-子群，并且$N_G(H) \leq A \leq G$，则$N_G(A) = A$ (**即A自正规**)。

证明. 设$gAg^{-1} = A$也就是$g \in N_G(A)$，从而$gHg^{-1} \leq gAg^{-1} = A$。由于$H \leq N_G(H) \leq A \leq G$，并且$H$是$G$的西罗 p-子群，从而H和gHg^{-1}都是A的 p-子群。由西罗定理即知存在$a \in A$使得$agHg^{-1}a^{-1} = H$，也就是$ag \in N_G(H) \leq A$，于是$g \in A$。 □

推论2.87. 设$M \lhd G$，H是M的西罗 p-子群，则

$$G = MN_G(H).$$

证明. 对任意的$g \in G$，由于$gMg^{-1} = M$，从而$gHg^{-1} \leq gMg^{-1} = M$。立即有$H$和$gHg^{-1}$都是$M$的 p-子群。由西罗定理即知存在$k \in M$使得$kgHg^{-1}k^{-1} = H$，也就是$kg \in N_G(H)$，于是$g \in MN_G(H)$。 □