黄子豪

代数图论笔记

2022 年 10 月 22 日

Springer Nature

Foreword

本书是笔者本科阶段为日后做代数图论方向所做的学习笔记。主要参考教材包括 Algebraic Graph Theory by Godsil (GTM207) 、Introduction to Graph Theory by Douglas B.West、图论及其应用 by 徐俊明、有限群导引 by 徐明曜、Algebra by Hungerford (GTM 73)。

本书计划分作四部分：第一部分用于介绍图论中基本的概念和结论。第二部分用于介绍群论、有限群的结论。第三部分用于介绍代数图论中的相关内容。第四部分用于写一些论文综述。

2022 9 月于 CSU　　黄子豪

目录

Part I

有限群论

Chapter 1
群论的基本概念

1.1 群和子群

1.1.1 群的基本定义和等价定义

Definition 1.1 一个非空集合 G, 其上定义了一个二元运算, 称作乘法, 其满足

(1) 结合律

(2) 存在单位元

(3) 每一个元都存在逆元

则称 G 是一个群.

Theorem 1.1 (群的等价定义) *一个非空集合 G, 其上定义了一个二元运算, 称作乘法, 其满足*

(1) 结合律

(2) 存在左单位元

(3) 每一个元都存在左逆元

则称 G 是一个群.

Proof 我们只需从左单位元和左逆元的存在性推出一般单位元和一般逆元的存在性. 任取 $a \in G$ 设 a_L^{-1} 是它的左逆元, 则有

$$\begin{aligned} aa_L^{-1} =& eaa_L^{-1} \\ =& \left(a_L^{-1}\right)^{-1} a_L^{-1} aa_L^{-1} \\ =& e_L \end{aligned}$$

于是每一个左逆元同时还是右逆元. 又由于

$$ae = aa_L^{-1}a = a$$

于是每一个左单位元都是右单位元, 因此是群. □

需要指出的是, 若将条件全部换作“右”, 任然成立, 方法是一样的. 但若条件是：左单位元存在, 并且每个元都有右逆元, 此时不能保证 G 是一个群. 下面我们给出一个例子说明.

Example 1.1 (半群有左单位元和右逆元但不是群) 考虑 $\mathbb{R}^*$ 是除掉 0 外的实数集. 定义其上的二元运算 $*$ 为 $a*b=|a|b, \forall a,b\in\mathbb{R}^*$. 则是一个半群, 且有左单位元 $-1,1$, 每个元也都有右逆元. 但显然不是一个群, 因其单位元不唯一.

Theorem 1.2 (群的等价定义) 一个非空集合 G, 其上定义了一个二元运算, 称作乘法, 其满足

(1) 结合律

(2) $\forall a,b\in G$ 存在 $x,y\in G$, 使得 $ax=b, ya=b$

则称 G 是一个群.

上面两个等价定义对于任意群都成立, 下面的等价定义只对有限的集合 G 成立.

Theorem 1.3 (有限群的等价定义) 一个非空有限集合 G, 其上定义了一个二元运算, 称作乘法, 其满足

(1) 结合律

(2) 满足左右消去律

则称 G 是一个群.

Proof 证明主要用到 G 的有限性.

设 $G=\{a_1,\cdots,a_n\}$, 则 a_1a_i 是 n 个不同的元素 (由消去律保证), 因此一定存在某个元素 a_{i_0} , 满足 $a_1a_{i_0}=a_1$. 记此元素为 $a_{i_0}=e$. $\forall a_j\in G, a_1a_j=a_1ea_j$, 由消去律得到 $ea_j=a_j$. 说明 e 是 G 的左单位元. 又由于 $\forall a_j\in G, \exists a_i$ 使得 $a_ia_j=e$, 于是每个元素存在左逆元. 综上 G 是一个群. □

1.1.2 子群和子群的陪集

Definition 1.2 G 是一个群, 给定 $H\subseteq G$, 若 H 是群, 则称 H 是 G 的子群, 记作 $H\leq G$.

Theorem 1.4 (子群的等价定义) 给定群 G 和 G 的子集 H, 下面三个命题等价.

(1) $H\leq G$

(2) $\forall a,b\in H, ab^{-1}\in G$

(3) $\forall a,b\in H, a^{-1}\in G, ab\in G$

特别的对于有限子集, 其是子群还有一等价定义.

Theorem 1.5 H 是群 G 的有限子集, 其是子群当且仅当 $H^2\subseteq H$

Proof 这是由于 H 是满足消去律和结合律的有限集, 所以 H 是群. □

下面指出子群的运算何时是一个子群.

Theorem 1.6 *:*

(1) $H_i \leq G, i = 1, 2, \cdots, n$ *是群* G *的一列子群, 则* $\bigcap_i H_i \leq G$

(2) $H, K \leq G, H \bigcup K \leq G \iff H \leq K$ *或* $k \leq H$

(3) 子群的乘积是子群当且仅当它们可以交换, 即 $H, K \leq G, HK \leq G \iff HK = KH$

Theorem 1.7 *任一群* G *不可能表示作两个真子群的并*

Proof 若 G 有两个真子群 H 和 K, $G = H \bigcup K$. 由于二者是真子集，于是 $\exists a \in G - K,\ b \in K - H$, 此时 $ab \in G = H \bigcap K$. 但不管假设 ab 属于 H 还是 K 都会导出矛盾. □

有时候任给一个 G 的子集 M, 其不一定是子群, 但可以嵌入进子群里.

Definition 1.3 M 是 H 的子集, $\langle M \rangle = \left\{ a_1 \cdots a_n | a_i \in M \bigcup M^{-1}, n = 1, 2, \cdots \right\}$ 称作 M 的生成子群, 其是所有包含 M 的子群的交.

下面来介绍子群的陪集

给定群 G, $H \leq G, a \in G$, 称 aH 是子群 H 的一个陪集. 容易验证两个陪集要么不交, 要么相等, 相等当且仅当 $ab^{-1} \in H$, 并且陪集的元素个数都等于 H 的元素个数. 于是 G 可以作陪集分解, 即存在 $a_1, \cdots, a_n$, 使得

$$G = a_1 H \bigcup \cdots \bigcup a_n H$$

元素 $\{a_1, \cdots, a_n\}$ 称作 H 在 G 中的一个左陪集代表系. 类似的我们可以定义右陪集，并且对 G 作右陪集分解，得到右陪集代表系. 那么这样的左右陪集有什么关系呢?

Theorem 1.8 (左右陪集对应定理) *左陪集的集合和右陪集的集合之间存在一个双射，从而左右陪集的个数或都为无限或一样多.*

Proof 取映射

$$\varphi : aH \to Ha^{-1}$$

即可验证这是一个双射. □

由于 H 的左陪集和右陪集一样多，从而我们可以称 H 的左 (右) 陪集的个数，称作是 H 在 G 中的指数, 记作 $|G : H|$. 由群 G 的陪集分解立得:

Theorem 1.9 (Lagrange) G *是有限群,* $H \leq G$*, 则* $|G| = |H||G : H|$.

由此定理立得一个有限群的子集是子群的必要条件是其阶数是群阶数的因子, 以及任一元素的阶数是群阶数的因子, 从而 $a^{|G|} = e$. 于是素数阶群一定是循环群.

应用 *Lagrange* 定理, 我们还可以证明数论中的一个定理.

Theorem 1.10 (Euler Theorem) *设* m *是大于 1 的整数, 若* $(a, m) = 1$ *则*

$$a^{\varphi(m)} \equiv 1 (mod\ m)$$

Proof 由于 $(a,m)=1$, 于是 $\overline{a}\in\mathbb{Z}^*$, 由于 $|\mathbb{Z}^*|=\varphi(m)$, 由 *Larange* 定理的推论即得 $\overline{a}^{\varphi(m)}=\overline{1}$, 从而 $\overline{a^{\varphi(m)}}=\overline{1}$

$$a^{\varphi(m)}\equiv 1(mod\ m)$$

此外，我们还可以用此定理来研究非阿贝尔群的最小阶数. 为此需要准备一些引理.

Lemma 1.1 *若群中每一个非单位元的元素阶数都为 2，则 G 是阿贝尔群.*

Proof $\forall a,b\in G$，$abab=e$, 于是 $ba=a^{-1}b^{-1}=ab$. □

现在可以证明：

Theorem 1.11 *非阿贝尔群的最小阶数是 6*

Proof 由上一引理和 *Larange* 定理我们知道，1，2，3，4，5 阶群是阿贝尔群. 最后以 S_3 表示集合 $\{1,2,3\}$ 的对称群，它是 6 阶非对称群. □

Theorem 1.12 *设 H 和 K 是群 G 的两个有限子群, 则*

$$|HK|=\frac{|H||K|}{|H\bigcap K|}$$

Proof 由于 $H\bigcap K\leq K$, 因此 $|K:H\bigcap K|=\dfrac{|K|}{|H\bigcap K|}$. 另一方面, 由于 HK 可以作陪集分解作 Hk_i 的并, 并且陪集相等当且仅当 $k_1k_2^{-1}\in H\bigcap K$, 于是 $Hk_1=Hk_2\iff(H\bigcap K)k_1=(H\bigcap K)k_2$. 说明 HK 的陪集分解中的 Hk_i 的个数就是 $H\bigcap K$ 在 K 在陪集的个数, 即 $|K:H\bigcap K|$. 综上 $|HK|=|H||K:H\bigcap K|=\dfrac{|H||K|}{|H\bigcap K|}$ □

利用陪集分解，我们还可以给出群 G 等于两个子群乘积的一个充分条件是两个子群在 G 的指数互素. 为此我们需要先准备一个引理.

Lemma 1.2 *设 G 是有限群，$A\leq B\leq G$，则*

$$[G:A]=[G:B][B:A]$$

Proof 将 G 作 B 的陪集分解

$$G=\bigcup_{j=1}^{n}Bg_j,\ n=[G:B]$$

再对 B 作 A 的陪集分解

$$B=\bigcup_{i=1}^{m}Ab_i,\ m=[B:A]$$

则

$$G=\bigcup_{j=1}^{n}\bigcup_{i=1}^{m}Ab_ig_j$$

若 $Ab_ig_j = Ab_{i'}g_{j'}$, 则 $b_ig_j(b_{i'}g_{j'})^{-1} \in A$, 从而 $g_jg_{j'} \in b_i^{-1}Ab_{i'} \subset B$, 从而 $j = j'$, 于是 $i = i'$. 综上 $(i,j) \neq (i',j')$ 时，Ab_ig_j 两两不同. 于是将 G 分解作了 mn 个 A 的不同的陪集的并. 说明 $[G:A] = nm = [G:B][B:A]$. □

Corollary 1.1 对于群 G 的任意两个子群 A,B，$[G:A\bigcap B] \leq [G:A][G:B]$

Proof 为此我们只需证明 $[B:A\bigcap B] \leq [G:A]$ 对于 $\forall b,b' \in B$, 从 $A\bigcap Bb \neq A\bigcap Bb' \hookrightarrow b(b')^{-1} \notin A\bigcap B \subset A \hookrightarrow Ab \neq Ab'$, 于是 $[B:A\bigcap B] \leq [G:A]$ □

现在可以证明我们的定理

Theorem 1.13 给定群 G 的两个子群 A,B，若 $[G:A]$ 和 $[G:B]$ 互素，则 $[G:A\bigcap B] = [G:A][G:B]$, 且 $G = AB$

Proof 由前面我们可以看出 $[G:B] \mid [G:A\bigcap B]$, $[G:A] \mid [G:A\bigcap B]$, 再由二者互素就得到 $[G:A\bigcap B] = [G:A][G:B]$. 从而 $|G| = \dfrac{|A||B|}{|A\bigcap B|} = |AB|$，于是 $G = AB$. □

1.1.3 元素的阶

Theorem 1.14 *:*

(1) 设 G 是群，$a,b \in G$，则 $o(a) = o(a^{-1})$, $o(ab) = o(ba)$,

(2) 设 G 是群，$g \in G$, $o(g) = n$ 则 $o(g^m) = \dfrac{n}{(m,n)}$

(3) 设 G 是群，H 是 G 的子群, $g \in G$, $o(g) = n$, $g^m \in H$, $(n,m) = 1$，则 $g \in H$

(4) 设 G 是群，$g_1,g_2 \in G$, $o(g_1) = n_1$, $o(g_2) = n_2$, $(n_1,n_2) = 1$ 若 $g_1g_2 = g_2g_1$，则 $o(g_1g_2) = n_1n_2$，当二者不可交换时，无此结论。

1.1.4 共轭算子

Definition 1.4 设 G 是群，$a,g \in G$，我们规定

$$a^g = g^{-1}ag$$

称作是 a 在 g 下的共轭变形。类似的对于 G 的子群 H，我们同样规定

$$H^g = g^{-1}Hg$$

称作 H 在 g 下的共轭变形。称两个元素 $a,b \in G$ 是共轭的，如果存在 $g \in G$，使得 $a^g = b$.

可以验证，两个元素的共轭关系是一个等价关系，于是以此可以将 G 中所有元素划分为若干个不相交的等价类，称作共轭类。每个共轭类包含的元素的个数称作此共轭类的长度。

Definition 1.5 设 G 是群，H 是 G 的子集，$g \in G$，若 $H^g = H$，则称元素 g 正规化 H，称所有能够正规化 H 的元素的集合

$$N_G(H) = \{g \in G | H^g = H\}$$

是 H 在 G 中的正规化子。特别的若元素 g 满足 $\forall h \in H, h^g = h$, 则称 g 中心化 H，所有中心化 H 的元素的集合

$$C_G(H) = \{g \in G | h^g = h, \forall h \in H\}$$

为 H 在 G 中的中心化子。规定

$$Z(G) = C_G(G)$$

称作群 G 的中心

从定义我们可以看出，每个子集的正规化子都是 G 的一个子群. 一个群是阿贝尔群当且仅当它等于它的中心. 一个群的中心反映了群 G 的交换性的程度.

下面我们思考, 给定群 G 的一个子集 M, 与 M 共轭的子集的个数是多少?

Theorem 1.15 *M 是群 G 的子集, 与 M 共轭的子集数等于 $[G : N_G(M)]$*

Proof 任一与 M 共轭的子集形如 $g^{-1}Mg$.

$$\begin{aligned} g^{-1}Mg = g'^{-1}Mg' &\iff g'g^{-1}Mgg'^{-1} = M \\ &\iff gg'^{-1} \in N_G(M) \\ &\iff N_G(M)g = N_G(M)g' \end{aligned}$$

从而 M 的共轭集数等于 M 正规化子在 G 的陪集数. □

于是我们知道一个集合 M 的共轭集数一定是 |G| 的因子, 特别的, 取 M 是单点集, 则任意 G 中的元素, 与其共轭的元素的个数是 |G| 的因子. 下面定理就作为上定理的一个应用

Theorem 1.16 *设 p 是素数, G 是 p^n 阶群. 则 G 中存在非平凡的中心元.*

Proof $a \in G$ 是 G 的中心元当且仅当 a 只与自己共轭. 于是中心元等价于其共轭类阶数为 1. 由于每个元素的共轭元的个数都是 p^i. 于是将 G 拆分作共轭元素类的并时, 就有

$$p^n = 1 + 1 + \cdots + 1 + p^{i_1} + \cdots + p^{i_k}$$

由于等式左右两边 $mod\ p \equiv 0$, 于是最少有 p 个 1 阶共轭类, 即最少有 p 个中心元, 或者说有 p-1 个非平凡中心元. □

1.1.5 习题及解答

习题一： 设群 G 中两个元素 g,h 可交换，$o(g)=m,\ o(h)=n$ 则有

(1) $o(g^nh^m)=\dfrac{[m,n]}{(m,n)}$;

(2) G 中存在阶数为 (m,n) 的元素;

(3) G 中存在阶数为 $[m,n]$ 的元素;

Proof (1): 设

$$m=(m,n)m_1,\ n=(m,n)n_1$$

则

$$\frac{[m,n]}{(m,n)}=n_1m_1,\ (m_1,n_1)=1$$

由于 $(g^nh^m)^{n_1m_1)}=e$, 于是

$$o(g^nh^m)\ \Big|\ n_1m_1$$

反之，由于

$$(g^nh^m)^{o(g^nh^m)m_1}=g^{nm_1o(g^nh^m)}h^{mm_1o(g^nh^m)}=e$$

说明

$$h^{mm_1o(g^nh^m)}=e,\ n\ \Big|\ mm_1o(g^nh^m),\ n\ \Big|\ (n,m)o(g^nh^m)$$

类似的有

$$m\ \Big|\ (n,m)o(g^nh^m)$$

于是由 (n_1,m_1), 可得 $n_1m_1\ \Big|\ o(g^nh^m)$. 综上 $\dfrac{[m,n]}{(m,n)}=n_1m_1=o(g^nh^m)$

(2) 考虑元素 g^{m_1}. 由定理1.14的 (2) , 立得.

(3) 答案有点复杂，为了不搞混，我们重新做个记号。

$$m=(m,n)p,\ n=(m,n)q,\ (p,q)=1$$

我们对 (m,n) 进一步分解

$$(m,n)=r_1r_2r_3$$

其中 r_1 只包含那些出现在 p 中的素因子，r_2 只包含那些出现在 q 中的素因子, r_3 不包含 p 和 q 的因子. 那么 r_i 和 r_j 在 $i\neq j$ 时两两互素. 更进一步

$$r_1p,\ r_2q,\ r_3$$

三者两两互素. 现在，若我们能够找到三个元素，使得它们的阶数分别等于上面三个数，并且两两可交换，那么由定理1.14的 (4)，将它们乘起来我们就得到一个元素的阶数是 $r_1r_2r_3pq=[m,n]$

下面我们找出这样的三个元素.

$$o(g^{r_2r_3}) = r_1p$$
$$o(g^{r_1r_2p}) = r_3$$
$$o(h^{r_1r_3}) = r_2q$$

并且由于它们两两可交换，且阶数互素，由定理1.14可以验证, 它们乘起来得到的元素就是所求的满足条件的元素. □

习题二: 设 G 是一个群，任取 G 中元素 a,b . $o(a) = m$, $o(b) = n$, $(m, n) = 1$，若存在某个整数 k, 使得 $a^k = b^k$，证明 $mn \mid k$，若 m 和 n 不互素，举出例子说明结论不成立.

Proof 由于

$$(b^k)^m = (a^k)^m = e$$

于是 $n \mid mk$，由于 $(n, m) = 1$，于是 $n \mid k$. 类似可得 $m \mid k$. 再次由它们二者互素，于是 $mn \mid k$

反例：考虑 $(\mathbb{Z}_6, +)$ 中的元素 $\overline{1}$ 和 $\overline{2}$. 则 $m = o(\overline{1}) = 6$, $n = o(\overline{2}) = 3$, 存在 $k = 6$ 使得 $(\overline{2})^6 = (\overline{1})^6 = \overline{0}$, 但 mn 不整除 k. □

习题三: 除平凡子群外无其它子群的群必是素数阶循环群.

Proof 设 $o(G) = ab$，$\forall g \in G$, 由于 G 中无子群，于是 $o(g) = ab$，但我们任可取 g^a, $o(g^a) = b$. 此时 $\langle g^a \rangle$ 是 G 的非平凡子群, 矛盾. □

1.2 正规子群、商群、群同态

1.2.1 正规子群和商群

前言: 假设给定了 N 是群 G 的子群，对 G 作 N 的陪集分解，取 $\overline{G}$ 是 N 的全部右陪集构成的集合，即 $\overline{G} = \{Na | a \in R\}$, 其中 R 是右陪集代表系. 我们希望在 $\overline{G}$ 上定义运算赋予群结构. 最自然的是取运算 $(Na)(Nb) = Nab$. 为此我们需要检验此定义不依赖于代表元的选取，即对于每一个 $a' \in Na$, $b' \in Nb$ 都有 $Na'b' = Nab$. 这相当于要求

$$NaNb = Nab \iff NaN = Na \iff NaNa^{-1} = N \iff aNa^{-1} \subset N, \forall a \in G$$

换句话说，我们要求 N 是一个自共轭子群，即只有 N 自身是 N 的共轭子群. 于是我们引出正规子群的定义:

Definition 1.6 称群 G 的子群 N 是 G 的正规子群，如果 $N^g \subset N$, $\forall g \in G$. 记作 $N \trianglelefteq G$.

Example 1.2 :

如果 $H \leqslant G$ 且 $[G:H]=2$, 则 $H \trianglelefteq G$.

证: $\forall x \in G$, 若 $x \in H$, 则 $Hx = H = xH$; 若 $x \notin H$, 则 $Hx \bigcap H = \varnothing, xH \bigcap H = \varnothing$, 且此时有 $G = H \bigcup Hx = H \bigcup xH$, 于是 $Hx = xH$. 总之有 $Hx = xH$, 即 $H \trianglelefteq G$.

Remark: 注意 $aH = Ha$ 只是集合相等, 绝不意味着元素乘积可以交换.

Theorem 1.17 (正规子群的等价定义) 设 G 是群，下面六条等价

(1) N 是 G 的正规子群.

(2) $N^g = N$, $\forall g \in G$，因此正规子群也称自共轭子群，因其群中的所有元素的共轭仍在此群中.

(3) $N_G(N) = G$.

(4) 若 $n \in N$，则 n 所属的 G 的共轭元素类 $C(n) \subset N$，即 N 是由 G 的若干整数割共轭类组成.

(5) N 在 G 中的每个左陪集都是一个右陪集. $Ng = gN$.

由于正规子群的左陪集和右陪集重合，因此对于正规子群只讨论其陪集，而不用区分左右. 显然阿贝尔群的子群都是正规子群，每个群都有两个平凡的正规子群 G 和 $\{e\}$.. 有些群只有平凡的正规子群，于是我们定义：

Definition 1.7 若群 G 只有平凡的正规子群，称群 G 是单群.

我们知道一个交换群，若是单群，意味着其无非平凡子群，由上节习题1.1.5, 此时其一定是素数阶循环群. 然而非交换单群则十分复杂，决定所有有限非交换单群多年来一直是有限群论的一个核心问题. 在可解群一节我们可以获得非交换群是单群的一些必要条件.

下面阐述一些获得正规子群的方法.

Theorem 1.18 给定一列正规子群 $N_1 \cdots N_s$，则 $\bigcap_{i=1}^{s} N_i$ 和 $\langle N_1, \cdots, N_s \rangle$ 仍然是正规子群.

Proof

$$\forall g \in G,\ n \in \bigcap_{i=1}^{s} N_i,\ n^g \in N_i,\ i = 1, 2, \cdots, s.$$

于是是正规子群，另一个类似可证. □

下面我们思考，给定任意一个群 G 的子集 M, 怎么找到一个最小的正规子群包含这个子集 M 呢? 以 M^G 记作是包含 M 的最小正规子群, 则应有

$$\{m^g \mid \forall g \in G, m \in M\} \subset M^G$$

同时, 由于 M^G 是包含上述子集的最小群, 于是

$$\langle m^g \mid \forall g \in G, m \in M \rangle \subset M^G$$

到这里就足够使得其是正规的了, 于是包含任意集合 M 的最小正规子群就是

$$M^G = \langle m^g \mid \forall g \in G, m \in M \rangle.$$

称其是 M 在 G 中的**正规闭包**.

又我们思考，给定任意一个群 G，如何找到一个群，使得它在其中正规呢？回顾上一节提到的正规化子

Theorem 1.19 *设 G 为群, H 是 G 的子群. 定义 H 的*正规化子 *(normalizer) 为*

$$N(H) = \left\{ g \in G \mid gHg^{-1} = H \right\}.$$

则 $N(H)$ 是 G 的子群, H 是 $N(H)$ 的正规子群.

Proof (1) 对任意的 $x, y \in N(H)$, 有 $xHx^{-1} = H, yHy^{-1} = H$, 则

$$x^{-1}Hx = x^{-1}\left(xHx^{-1}\right)x = H,$$
$$(xy)H(xy)^{-1} = x\left(yHy^{-1}\right)x^{-1} = xHx^{-1} = H.$$

55 从而 $x^{-1}, xy \in N(H)$, 所以 $N(H)$ 是 G 的子群.

(2) 对任意的 $x \in N(H)$, 由 $N(H)$ 的定义知

$$xHx^{-1} = H,$$

所以 H 是 $N(H)$ 的正规子群. 由此可以看出, $N(H)$ 是将 H 作为正规子群的 G 的最大的子群。特别地, 若 $H \trianglelefteq G$, 则 $N(H) = G$ □

现在我们回到前言提到的内容, 有了正规子群我们就可以在正规子群陪集的集合上定义二元运算, 使得其是一个群, 并且此时不需要考虑到底是左陪集还是右陪集, 因其在正规子群下是一样的. 我们来正式的定义它.

Definition 1.8 给定 $N \trianglelefteq G$, 记 $\overline{G} = \{N^g | g \in G\}$. 定义其上乘法 $Na * Nb = aN * Nb = aNb = Nab$. 则 $\overline{G}$ 在运算 $(*)$ 下封闭, 并且成为一个群. 将其称作 G 对 N 的商群, 记作 $\overline{G} = G/N$.

如果 G 是有限群, 由 *Lagrange* 定理立马有 $|G/N| = [G : N] = \dfrac{|G|}{|N|}$.

我们将下定理作为商群应用的一个例子

Theorem 1.20 (A.L.Cauchy) *设 G 是一个 pn 阶有限交换群, 其中 p 是一个素数, 则 G 有 p 阶元素, 从而有 p 阶子群.*

Proof 对 n 用数学归纳法. 当 $n = 1$ 时, G 是 p 阶循环群, 则 G 的一个生成元就是一个 p 阶元, 定理成立.

假设定理对阶为 $pk(1 \leqslant k < n)$ 的交换群成立, 下证对阶为 pn 的交换群 G 定理成立.

在 G 中任取 $a \neq e$. 若 $p||a|$, 令

$$|a| = ps,$$

则 $|a^s| = p$, 定理成立.

若 $p \nmid |a|$, 令 $|a| = m > 1$, 则 $(m, p) = 1$. 由于

$$m \mid pn,$$

故 $m \mid n$. 令 $N = \langle a \rangle$, 则由于 G 是交换群, 故

$$|G/N| = p \cdot \frac{n}{m},\ 1 \leqslant \frac{n}{m} < n.$$

于是由归纳假设, 群 G/N 有 p 阶元, 任取其一, 设为 bN, 且 $|b| = r$, 则

$$(bN)^r = b^r N = N,$$

从而 $p \mid r$. 令 $r = pt$, 则 $|b^t| = p$. □

实际上, 当 G 是非交换群时, 这个定理仍成立. 此处不再赘述.

1.2.2 群同态和群同构

一个群到群的映射, 如果保持乘法运算, 则称该映射是一个群同态映射. 若该同态映射同时还是双射, 则称是群同构映射.

根据定义立马可以得到群同态的一些简单性质:

Theorem 1.21 设 ϕ 是群 G 到群 G' 的同态映射, e 与 e' 分别是 G 与 G' 的单位元, $a \in G$, 则

(1) ϕ 将 G 的单位元映到 G' 的单位元, 即 $\phi(e) = e'$;

(2) ϕ 将 a 的逆元映到 $\phi(a)$ 的逆元, 即 $\phi\left(a^{-1}\right) = (\phi(a))^{-1}$;

(3) 设 n 是任一整数, 则 $\phi\left(a^n\right) = (\phi(a))^n$;

(4) 如果 $|a|$ 有限, 则 $|\phi(a)||a|$.

Proof (1) 因 e 与 e' 分别是 G 与 G' 的单位元, 所以

$$e' \cdot \phi(e) = \phi(e) = \phi(e \cdot e) = \phi(e) \cdot \phi(e),$$

从而由消去律得

$$e' = \phi(e),$$

即 $\phi(e)$ 为 G' 的单位元.

(2) 直接计算可得

$$\phi(a) \cdot \phi\left(a^{-1}\right) = \phi\left(aa^{-1}\right) = \phi(e) = e' = \phi(a) \cdot (\phi(a))^{-1}.$$

65 从而又由消去律得

$$\phi\left(a^{-1}\right)=(\phi(a))^{-1}$$

即 $\phi\left(a^{-1}\right)$ 为 $\phi(a)$ 的逆元.

(3) 当 $n=0$ 时,

$$\phi\left(a^{0}\right)=\phi(e)=e'=(\phi(a))^{0}.$$

当 $n>0$ 时,

$$\phi\left(a^{n}\right)=\phi\left(a^{n-1}a\right)=\phi\left(a^{n-1}\right)\phi(a)=\cdots=(\phi(a))^{n-1}\phi(a)=(\phi(a))^{n}.$$

当 $n<0$ 时,

$$\phi\left(a^{n}\right)=\phi\left(\left(a^{-1}\right)^{-n}\right)=\left(\phi\left(a^{-1}\right)\right)^{-n}=\left(\phi(a)^{-1}\right)^{-n}=(\phi(a))^{n}.$$

(4) 设 $|a|=r$, 则

$$(\phi(a))^{r}=\phi\left(a^{r}\right)=\phi(e)=e',$$

所以 $|\phi(a)|\mid|a|$. □

Theorem 1.22 *设 ϕ 是群 G 到 G' 的同态映射, H 与 K 分别是 G 与 G' 的子群, 则*

(1) $\phi(H)$ 是 G' 的子群;

(2) $\phi^{-1}(K)$ 是 G 的子群;

(3) 如果 H 是 G 的正规子群, 则 $\phi(H)$ 是 $\phi(G)$ 的正规子群;

(4) 如果 K 是 G' 的正规子群, 则 $\phi^{-1}(K)$ 是 G 的正规子群.

Proof (1) 对任意的 $h_1,h_2\in H$, 有 $h_1h_2^{-1}\in H$, 所以

$$\phi\left(h_1\right)\left(\phi\left(h_2\right)\right)^{-1}=\phi\left(h_1\right)\phi\left(h_2^{-1}\right)=\phi\left(h_1h_2^{-1}\right)\in\phi(H),$$

所以 $\phi(H)$ 是 G' 的子群.

(2) 对任意的 $a,b\in\phi^{-1}(K)$, 有 $\phi(a),\phi(b)\in K$, 则

$$\phi\left(ab^{-1}\right)=\phi(a)\phi\left(b^{-1}\right)=\phi(a)\phi(b)^{-1}\in K,$$

于是 $ab^{-1}\in\phi^{-1}(K)$, 所以 $\phi^{-1}(K)$ 是 G 的子群.

(3) 由 (1) 知 $\phi(H)$ 是 $\phi(G)$ 的子群. 又对任意的 $a'\in\phi(G),h'\in\phi(H)$, 有 $a\in G,h\in H$, 使 $\phi(a)=a',\phi(h)=h'$, 则 $aha^{-1}\in H$. 于是

$$a'h'a'^{-1}=\phi(a)\phi(h)(\phi(a))^{-1}=\phi(a)\phi(h)\phi\left(a^{-1}\right)$$

$66=\phi\left(aha^{-1}\right)\in\phi(H)$, 所以 $\phi(H)$ 是 $\phi(G)$ 的正规子群.

(4) 由 (2) 知, $\phi^{-1}(K)$ 是 G 的子群. 又对任意的 $a\in G,h\in\phi^{-1}(K)$, 则 $\phi(h)\in K$, 而 K 是 G' 的正规子群, 故

$$\phi\left(aha^{-1}\right)=\phi(a)\phi(h)\phi(a)^{-1}\in K.$$

从而

$$aha^{-1} \in \phi^{-1}(K),$$

所以 $\phi^{-1}(K)$ 是 G 的正规子群. □

在开始同态基本定理前我们先定义一些类似与线性空间中线性映射相似的东西.

Definition 1.9 设 $\alpha : G \to H$ 是一个群同态映射, 则

$$Ker\ \alpha := \{g \in G \mid g^\alpha = 1_H\}$$

称作是该同态映射的核

$$G^\alpha := \{g^\alpha \mid g \in G\}$$

称作是同态映射的像集. 可以验证 $Ker\ \alpha \trianglelefteq G$, 而 $G^\alpha \leq H$.

Theorem 1.23 (同态基本定理) *:*

(1) 任给 G 的正规子群 N, 都对应一个 G 的 G/N 的同态映射, 称作是 G 到 G/N 的自然同态.

(2) 给定一个 $\alpha : G \to H$ 是同态映射. 则 $Ker\ \alpha \trianglelefteq G$, 且 $G^\alpha \cong G/Ker\ \alpha$

Proof 记 $K = ker\ \alpha$, 设 $G/K = \{gK \mid g \in G\}$, 作 $G/K \to G^\alpha$ 的映射

$$\sigma : gK \to g^\alpha$$

则由于

$$g_1K = g_2K \iff g_1^{-1}g_2 \in K \iff (g_1^{-1}g_2)^\alpha = 1_H \iff g_1^\alpha = g_2^\alpha$$

于是 σ 是一个单射. 显然也是一个满同态. 于是 $G^\alpha \cong G/K$ □

这个定理告诉我们: **群 G 的同态像在同构意义下只能是 G 的商群!** 定理中给出的 $\sigma : G/Ker\ \alpha \to G^\alpha$ 称作是正则同构.

下面我们给出几个同态基本定理应用的例子.

Example 1.3 不难验证

$$\alpha : \mathbb{Z} \to \mathbb{Z}_n$$
$$a^\alpha = \overline{a}$$

是两个加法群之间的满同态, $Ker\ \alpha = n\mathbb{Z}$, 于是我们得到加法群同构 $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$. 从而有时候我们可以整数模 n 加法群 $\mathbb{Z}_n$ 记作 $\mathbb{Z}/n\mathbb{Z}$ 的形式.

Example 1.4 映射 $det : GL(n, \mathbb{C}) \to \mathbb{C}^*$ 是乘法群的满同态, 它将每一个可逆复方阵 M 映作 M 的行列式. 从而

$$Ker(det) = \{M \in GL(n, \mathbb{C}) \mid det(M) = 1\} = SL(n, \mathbb{C})$$

因此 $SL(n, \mathbb{C})$ 是 $GL(n, \mathbb{C})$ 的正规子群, 并且有 $GL/SL \cong \mathbb{C}^*$.

Theorem 1.24 (第一同构定理) 设 φ 是群 G 到群 $\bar{G}$ 的一个同态满射, 又 $ker\ \varphi \subseteq N \trianglelefteq G$, $\bar{N} = \varphi(N)$, 则

$$G/N \cong \bar{G}/\bar{N}.$$

Proof 因为 $N \trianglelefteq G$, 又 φ 是满同态, 故 $\bar{N} = \varphi(N) \trianglelefteq \bar{G}$. 现在令

$$\tau : G/N \to \bar{G}/\bar{N},$$
$$xN \to \varphi(x)\varphi(N)(\forall x \in G).$$

下证 τ 是商群 G/N 到 $\bar{G}/\bar{N}$ 的一个同构映射.

(1) τ 是映射: 设 $aN = bN(a, b \in G)$, 则 $a^{-1}b \in N$. 但由于 φ 是同态映射, 故

$$\varphi\left(a^{-1}\right)\varphi(b) = \varphi\left(a^{-1}b\right) \in \varphi(N) = \bar{N}.$$

从而 $\varphi(a)\bar{N} = \varphi(b)\bar{N}$, 即 τ 是 G/N 到 $\bar{G}/\bar{N}$ 的映射.

(2) τ 是满射: 任取 $\bar{a}\bar{N} \in \bar{G}/\bar{N}(\bar{a} \in \bar{G})$, 则因 φ 是满同态, 故有 $a \in G$ 使 $\varphi(a) = \bar{a}$. 从而在 τ 之下 $\bar{a}\bar{N}$ 有逆像 aN, 即 τ 是满射.

(3) τ 是单射: 设 $\varphi(a)\bar{N} = \varphi(b)\bar{N}$, 则

$$\varphi\left(a^{-1}b\right) = \varphi(a)^{-1}\varphi(b) \in \bar{N}.$$

但 φ 为满同态且 $\bar{N} = \varphi(N)$, 故有 $c \in N$ 使

$$\varphi\left(a^{-1}b\right) = \varphi(c)$$

此即

$$varphi\left(c^{-1}a^{-1}b\right) = \bar{e},$$

其中 $\bar{e}$ 是 $\bar{G}$ 的单位元. 于是 $c^{-1}a^{-1}b \in \ker\varphi$. 但是 $\ker\varphi \subseteq N$, 故

$$a^{-1}b = c \cdot c^{-1}a^{-1}b \in N.$$

从而 $aN = bN$, 即 τ 是单射. 因此, τ 是双射. 又因为显然在 τ 之下有

$$aN \cdot bN = abN \to \varphi(ab)\bar{N} = \varphi(a)\varphi(b)\bar{N} = \varphi(a)\bar{N} \cdot \varphi(b)\bar{N},$$

故 τ 是 G/N 到 $\bar{G}/\bar{N}$ 的同构映射. 因此

$$G/N \cong \bar{G}/\bar{N}.$$

Theorem 1.25 (第二同构定理) 设 H 为 G 的子群, K 为 G 的正规子群, 则 $H \bigcap K$ 是 H 的正规子群且

$$H/(H\bigcap K) \cong HK/K.$$

Proof 令

$$\phi : H \to HK/K,$$
$$h \to hK$$

(1) 显然 ϕ 是 H 到 HK/K 的映射.

(2) 对任意的 $hkK \in HK/K$, 其中 $h \in H, k \in K$, 由于 $hkK = hK$, 故

$$\phi(h) = hK = hkK,$$

所以 ϕ 是 H 到 HK/K 的满映射.

(3) 对任意的 $h_1, h_2 \in H$,

$$\phi(h_1 h_2) = (h_1 h_2) K = h_1 K \cdot h_2 K = \phi(h_1)\phi(h_2),$$

所以 ϕ 是 H 到 HK/K 的满同态.

(4) 同态的核

$$\begin{aligned}\ker\phi &= \{h \in H \mid \phi(h) = K\} \\ &= \{h \in H \mid hK = K\} \\ &= \{h \in H \mid h \in K\} = H \bigcap K\end{aligned}$$

(5) 由同态基本定理知, $H \bigcap K = \ker\phi$ 为 H 的正规子群, 且

$$H/(H \bigcap K) \cong HK/K$$

1.2.3 习题及解答

习题一： 证明单群的同态像仍是单群.

Proof 设 G 是单群，α 是一个同态映射. 若 G^α 中有正规子群 H. 则 $\forall g \in G$

$$\begin{aligned}&g^\alpha H = Hg^\alpha \\ \Rightarrow\ &(g^\alpha H)^{\alpha^{-1}} = (Hg^\alpha)^{\alpha^{-1}} \\ \Rightarrow\ &gH^{\alpha^{-1}} = H^{\alpha^{-1}} g \\ \Rightarrow\ &H^{\alpha^{-1}} \text{是 G 中单群} \\ \Rightarrow &H = \{e\} \text{ or } G^\alpha \\ \Rightarrow &G^\alpha \text{是单群}\end{aligned}$$

习题二： 证明若 G 是一个 pn 阶群，p 是一个素数，证明 G 有 p 阶元.

Proof 对 n 作归纳法. 当 n=1 时结论显然成立.

现在假设 $n \leq k$ 时结论成立.

(1) 若有一个子群 H, $p \nmid [G:H]$. 则由于

$$|G| = |H|[G:H] \ , \ p \mid |H|$$

于是由假设知 H 有 p 阶元, 从而 G 中有 p 阶元.

(2) 若对任意子群 H, $p \nmid [G:H]$ 则考虑 $N(a_i)$, 其中 $N(a_i)$ 是 a_i 的正规化子. 则有共轭类分解, 导致

$$|G| = |C| + \sum_{i=1}^{m} [G : N(a_i]$$

进而 $p \mid |C|$ 于是 C 中有 p 阶元. □

习题三: 群 G 的变换

$$\phi : \ x \mapsto x^{-1} \quad (x \in G)$$

是 G 的自同构当且仅当 G 是阿贝尔群.

Proof 显然这样的映射是一个双射. 若是自同构, 则 $\forall a, b \in G, \phi(ab) = (ab)^{-1} = b^{-1}a^{-1}$, 又 $\phi(ab) = \phi(a)\phi(b) = a^{-1}b^{-1}$, 于是 G 是交换群. 反之若 G 是交换群, 则 $\phi(ab) = b^{-1}a^{-1} = a^{-1}b^{-1} = \phi(a)\phi(b)$, 于是是同态, 进而是自同构. □

习题四: 举例说明: 正规子群的正规子群不一定是正规子群

例: 对于交错群 A_4 , 我们知道: A_4 的非平凡正规子群只有克莱因群 $K_4 \cong \mathbb{Z}/2 \times \mathbb{Z}/2$. 但 K_4 有正规子群 $\mathbb{Z}/2$. 于是正规子群 K_4 的正规子群 $\mathbb{Z}/2$ 不是 A_4 的正规子群.

1.3 自同构群

1.3.1 自同构

一个 G 到 G 自身的群同构映射称作是自同构, 用 **Aut(G)** 表示 G 的所有自同构映射的集合. 讨论任意群上的任意一个自同构是抽象的，但我们可以找出一些具体的自同构. 在群 G 中任取一个元素 $a \in G$, 映射

$$\sigma_a(x) := axa^{-1}, \quad \forall x \in G$$

定义了一个 G 的自同构. 所有这样的自同构组成的集合在一般映射运算下构成群，称作内自同构群，记作 **InnG**.

$$InnG := \left\{ \sigma_a \mid a \in G, \ \forall x \in G, \ \sigma_a(x) = axa^{-1} \right\}$$

自同构映射和内自同构映射组成的集合在映射的运算下构成群，分别称作**自同构群**和**内自同构群**. 很快我们就可以发现,

$$InnG \trianglelefteq AutG$$

显然一个群的自同构群和该群自身有关，那么自然就想问：两个同构的群，它们的自同构群是否同构？答案是肯定的.

Theorem 1.26 设 G 和 H 是两个群，有 $G \cong H$, 则 $Aut(G) \cong Aut(H)$.

Proof 由于 $G \cong H$, 于是有一个同构映射

$$\alpha : G \to H$$

下面对于 $\forall \beta \in Aut(G)$ 考虑映射

$$f : Aut(G) \to Aut(H)$$
$$\beta \to \alpha\beta\alpha^{-1}$$

首先我们验证 $\alpha\beta\alpha^{-1}$ 确是一个 H 上的自同构.

$$H \xrightarrow{\alpha^{-1}} G \xrightarrow{\beta} G \xrightarrow{\alpha} H$$

由同构关系的传递性知，$\alpha\beta\alpha^{-1}$ 确是一个 H 上的自同构. 我们接下来只需验证 f 是一个保运算的双射即可. 若 $\alpha\beta\alpha^{-1} = \alpha\beta'\alpha^{-1}$，则有 $\beta = \beta'$, 于是 f 是单射. 对于 $\forall \mu \in Aut(H)$ 由于

$$G \xrightarrow{\alpha} H \xrightarrow{\mu} H \xrightarrow{\alpha^{-1}} G$$

于是 $\alpha^{-1}\mu\alpha$ 是一个 G 上的自同构，并且其在 f 下的像就是 μ. 于是 f 是双射. 容易验证 f 还保持运算，于是 f 是 Aut(G) 到 Aut(H) 的同构映射. □

但据此我们能说明，不同构的两个群它们的自同构群一定不同吗，这是不能的事实上我们有反例.

Example 1.5 (不同构的群有相同自同构群) 考虑 $G = \{e\}, H = \mathbb{Z}_2$，它们不同构，但自同构群中都只有恒等映射.

接下来再成列一些常用的相关定理

Theorem 1.27 (自同构诱导的商群上的自同构) $N \trianglelefteq G, \alpha \in AutG$, 若 $N^\alpha = N$，则

$$\overline{\alpha} : Ng \mapsto Ng^\alpha$$

是商群 G/N 上的一个自同构，我们称是 α 诱导的自同构.

Proof 显然这是一个满射，因为 $\forall Ng \in G/N$，存在 $g' \in G$, 使得 $(g')^\alpha = g$. (这是由 α 是自同构保证的.) 于是 $(Ng')^{\overline{\alpha}} = Ng' = Ng$. 同时这又是一个单射，因为若 $Ng_1^\alpha = Ng_2^\alpha$ 则我们有

$$\begin{aligned} & g_1^{\alpha}(g_2^{\alpha})^{-1} \in N \\ \Rightarrow & (g_1 g_2^{-1})^{\alpha} \in N \\ \Rightarrow & g_1 g_2^{-1} \in N \\ \Rightarrow & N g_1 = N g_2 \end{aligned}$$

因此是单射. 同时很容易验证保持运算，于是是同构. □

Theorem 1.28 (N/C 定理) $H \leq G$, $N_G(H)/C_G(H)$ 同构于 $AutG$ 的一个子群.

Proof

$$\forall g \in N_G(H) = \left\{ g \in G | g^{-1} H g = H \right\}$$

都对应一个 H 的自同构

$$\sigma_g : h \mapsto h^g \quad \in AutG$$

于是考虑同态映射

$$\begin{aligned} f : N_G(H) &\to Aut(H) \\ g &\mapsto \sigma_g \end{aligned}$$

显然 $C_G(H)$ 是此同态映射的核，于是由同态基本定理知，此定理得证. □

接下来我们研究内自同构群. 由于内自同构来源于 G 中的元素, 因此很容易建立二者之间的关系, 事实上我们有

Theorem 1.29 $InnG \cong G/C(G)$

Proof 考虑 G 到 InnG 的满同态, 在此同态下 C(G) 是同态核, 于是由同态基本定理即得. □

由此可以立得一个群同构与它的内自同构群的充分条件

Corollary 1.2 当 G 是非交换单群时, $C(G) = \{e\}$, $InnG \cong G$.

于是我们发现了一些有趣的问题, 我们可以问出很多类似的问题, 例如: 什么时候一个群的自同构只有内自同构? 一个自同构群的自同构群和它有什么关系? 一个群是否能同构与它的自同构群?... 为了探究这些问题, 我们需要从简单的开始着手, 锻炼我们的思维.

首先是, 如何确定一个群的自同构群? 我们以整数加群 $(\mathbb{Z}, +)$ 为例, 试确定其自同构群:

解: 设 f 是 $\mathbb{Z}$ 的任一自同构, 则它只能把 $0 \mapsto 0$. 设它把 1 映作 $f(1) = k$. 故对于 $\forall x \in \mathbb{Z}$, $f(x) = kx$. 由于是满射, 因此存在 x_0, $f(x_0) = kx = 1$. 由于 k 和 x 都是整数, 因此只能有 $k = \pm 1$. 说明其上只有两种自同构.

$$\begin{aligned} f_1(x) &= x, \quad x \in \mathbb{Z} \\ f_2(x) &= -x, \quad x \in \mathbb{Z} \end{aligned}$$

于是我们分析自同构时候, 可以考虑先分析群中生成元的像, 从而决定此同构映射的约束条件.

1.3.2 完全群

在前面我们实际上已经注意到这种特殊的群了.

Definition 1.10 称 G 是完全群，如果 $C_G = \{e\}$, $AutG = InnG$.

Remark 1.1 由定理1.29, 知一个群是完全群当且仅当 $C_G = \{e\}, AutG \cong G$.

我们可以很快举出例子

Example 1.6 S_3 是完全群. 证明只需说明 $|AutS_3| \leq 6$, 并且由于 $C = \{e\}$, 于是 $InnS_3 \cong S_3$.(Th1.29) 于是 $|InnS_3| = |S_3| = 6$. 说明 $AutS_3 = InnS_3$. 事实上我们可以说明 $n \neq 6$ 时 S_n 都是完全群.

下面定理给出了更丰富的完全群.

Theorem 1.30 设 G 是非交换单群，则 $Aut(G)$ 是完全群.

Proof 为了方便，我们简记 $I = InnG, A = AutG$. 我们将分三步证明:

(1): $C_A(I) = \{e\}$;

$\forall \xi \in C_A(I)$, $\sigma \in I, \xi^{-1}\sigma_g\xi = \sigma_g$, $\forall g \in G$. 其中 σ_g 是同前面定义的 g 诱导的内自同构. 则对于 $\forall x \in G$, $\exists y \in G$, $y^\xi = x$. 于是

$$x^{\xi^{-1}\sigma_g\xi} = y^{\sigma_g\xi} = (g^{-1}yg)^\xi = y^{\xi\sigma_{g^\xi}} = x^{\sigma_{g^\xi}}.$$

最终得到 $\xi^{-1}\sigma_g\xi = \sigma_{g^\xi}$, 即 $\sigma_g = sigma_{g^\xi}$. 由于 σ 是一个 $G \to I$ 的同构映射，于是 $g = g^\xi$, 从而 $\xi = 1$，是恒等映射.

(2): 设 $\alpha \in Aut(A)$, 则 $I^\alpha = I$; 此处暂略

(3): 设 $\alpha \in Aut(A)$, 则 $\alpha \in Inn(A)$; 此处暂略 □

1.4 可解群

1.4.1 可解群基本定义以及性质

引言: 我们探究回正规子群的商群. 现在有一个这样的问题，一个群可能不是交换群，但它的商群可能是交换群. 于是我们思考，什么样的正规子群的商群是交换群. 等价的，我们只需要去找同态映射 $\sigma: G \to \overline{G}$, $Im(\sigma)$ 是交换群的条件. (这是由同态基本定理 $Im(\sigma) \cong G/Ker(\sigma)$, 而 Ker 是 G 的正规子群).

$$\begin{aligned} Im\sigma\text{是交换群} &\iff \sigma(x)\sigma(y)=\sigma(y)\sigma(x), && \forall x,y\in G\\ &\iff \sigma(xyx^{-1}y^{-1})=\overline{e}, && \forall x,y\in G\\ &\iff xyx^{-1}y^{-1}\in Ker\sigma, && \forall x,y\in G\\ &\iff \left\{xyx^{-1}y^{-1}\mid \forall x,y\in G\right\}\subseteq Ker\sigma \end{aligned}$$

于是所有 $xyx^{-1}y^{-1}$ 都必须包含进同态核里. 又由于同态核是一个群，于是 $\left\{xyx^{-1}y^{-1}\mid \forall x,y\in G\right\}$ 生成的群也要包含在同态核里.

Definition 1.11 称 $xyx^{-1}y^{-1}$ 是 x,y 的换位子, 所有换位子生成的群称作是换位子群，或 G 的导群，记作 G'. 即

$$G'=<\left\{xyx^{-1}y^{-1}\mid \forall x,y\in G\right\}>$$

可以看出，一个群的导群越大，其越不可交换 (这与中心刚好相反). 根据定义立刻有:

Corollary 1.3：

(1) G 是交换群 $\iff$ $G'=\{e\}$.

(2) 同态映射 $\sigma: G\to\overline{G}$，其同态像是交换群 $\cong$ $G'\subseteq Ker\sigma$.

(3) $G'\trianglelefteq G$.

Proof 我们只证明 (3) . $\forall g\in G, z\in G', gzg^{-1}z\in G', gzg^{-1}\in G'$. 于是 G' 是正规子群. □

Proposition 1.1 $N\trianglelefteq G$, 则 G/N 是交换群 $\iff$ $G'\subseteq N$.

Proof 考虑自然同态 $G\to G/N$, 则 N 是此同态的核，又由于导群含于此核中，于是由上推论 (2) 即得. □

Remark 1.2 特别的取正规子群 $N=G'$ ，则 G/G' 是交换群，并且是 G 中最大的交换商群.

下面介绍一种特殊的由导群导出的群.

Definition 1.12 称 G 是可解群，如果存在正整数 k, 使得 $G^{(k)}=\{e\}$ ..

这个名称来源于高于四次的一般代数方程根式不可解, 我们有 $f(x)=0$ 在 $\mathbb{F}$ 上根式可解当且仅当 $f(x)$ 在 $\mathbb{F}$ 上的伽罗瓦群是可解群. 于是我们现在需要先认识了解它. 首先我们很容易看出，交换群都是可解群，因为它们的导群都只有单位元. 为了刻画可解群，我们需要找到它的充要条件. 首先我们思考必要条件:

G 是可解群 $\Rightarrow$ 有 G 的递降子群序列

$$G=G_0\trianglerighteq G_1\trianglerighteq G_2\trianglerighteq\cdots\trianglerighteq G_s=\{e\}$$

并且每一个 G_{i-1}/G_i 都是交换群. 这是因为，我们可以取一个导群列 $\left\{G^{(i)}\right\}$, 该导群列最终是单位元，并且每一个都是上一个的正规子群，$G^{(i)}/G^{(i+1)}$ 是交换群. 接下来我们可以证明这个条件是充分的，于是:

Theorem 1.31 *G 是可解群 $\iff$ 有 G 的递降子群序列*

$$G = G_0 \trianglerighteq G_1 \trianglerighteq G_2 \trianglerighteq \cdots \trianglerighteq G_s = \{e\}$$

Proof 我们证明它的充分性，必要性在上面已经说明了. 由于 G_0/G_1 是交换群，于是 $G' \subseteq G_1$. 又由于 G_1/G_2 是交换群, 进而 $G^{(2)} \subseteq (G_1)' \subseteq G_2$. 归纳的可以证明 $G^l \subseteq G_l$. 于是 $G^{(s)} \subseteq G_s = \{e\}$. 说明 G 是可解群. □

下面这些很容易可以验证

Theorem 1.32 *可解群的每一个子群和同态像都是可解群.*

Corollary 1.4 *可解群的商群是可解的. 因商群是自然同态的同态像.*

下面这个定理“听上去很合理”.

Theorem 1.33 *$N \trianglelefteq G$, 若 N 和 G/N 都是可解群，则 G 也是可解群.*

Proof 考虑 $G \to G/N$ 的自然满同态映射 π. 则很容易验证

$$\pi(G') = (G/N)'$$

同理有

$$\pi(G^{(2)} = \pi((G')') = (\pi(G))^{(2)}$$

进一步由归纳法可以说明

$$\pi(G^{(i)}) = (\pi(G))^{(i)}$$

于是存在某一个 $k, \pi(G^{(k)} = (\pi(G))^k = N$. 由商群的性质，得 $G^{(k)} \subseteq N$. 又由于 N 是可解群，存在 l. $G^{(k+l)} \subseteq N^{(l)} = \{e\}$. 说明 G 是可解群. □

Theorem 1.34 *非交换单群都是不可解群*

Proof 由于是单群，于是导群只能是 G 或者 e，由于 G 非交换，说明导群只能是 G. 这样的话 G 的任意阶导群仍然是 G，不可能是 e. 于是 G 不是可解群. □

Corollary 1.5 *非交换可解群不是单群.*

这启示我们，若想找非交换单群，只能从不可解群中找.

Theorem 1.35 *奇数阶群都是可解群*

此证明长达 255 页. 此定理进一步告诉我们若想找非交换单群，只能从偶数阶不可解群中找.

1.4.2 递降子群刻画一般群结构

在前面我们用递降的子群刻画了可解群，当时我们要求每一个商群都是交换群. 现在我们推广至任意群上.

Definition 1.13 群 G 的一个递降子群序列：

$$G = G_0 \trianglerighteq G_1 \trianglerighteq G_2 \trianglerighteq \cdots \trianglerighteq G_r = \{e\}$$

称作是 G 的次正规子群列. 其商群组

$$G_0/G_1, \cdots G_{r-1}/G_r$$

称作是因子群组，其中含非单位元的因子群个数称作组的长度.

注意： G 的次正规子群列中，后一个是前一个的正规子群，但不代表是 G 的正规子群. 事实上，正规子群的正规子群不一定是正规子群. 1.2.3.

我们应该指出每一个群都有次正规子群列，理由如下：若 G 是单群，则

$$G = G_0 \trianglerighteq G_1 = \{e\}$$

若 G 不是单群，我们可以在中间插入正规子群. 若插入的正规子群不是单群，此过程还可继续下次. 若我们要求次正规子群列中无重复项，那么对于有限群而言，群列的长度一定小于 $|G|$. 需要提醒，一个群的次正规群列并不唯一.

Definition 1.14 群 G 的次正规子群列如果满足：每一个因子群都是单群，那么称是 G 的一个合成群列.

Example 1.7 交错群 A_4 有三个合成群列：命 $V = \{(1), (12)(34), (13)(24), (14)(23)\}$, 则有

$$A_4 \trianglerighteq V \trianglerighteq [(12)(34)] \trianglerighteq \{1\}$$
$$A_4 \trianglerighteq V \trianglerighteq [(13)(24)] \trianglerighteq \{1\}$$
$$A_4 \trianglerighteq V \trianglerighteq [(14)(23)] \trianglerighteq \{1\}$$

那是否每一个有限群都有合成群列？答案是肯定的

Theorem 1.36 每个**有限群**都有至少应该合成群列

Proof 设 G 是有限群，则子群列长度不会超过 G 的阶. 不妨取 G 的应该无重复项的最长的次正规子群列，我们证明这就是一个合成序列. 若不是合成序列，说明某一个 G_i/G_{i+1} 不是单群，于是其有非平凡正规子群 H/G_{i+1} 其中 H 是 G_i 包含 G_{i+1} 的非平凡正规子群. 于是其可插入我们的次正规子群列中，使得长度增加，这与最长矛盾. 于是最长的次正规子群列一定是合成群列. □

Corollary 1.6 有限群是可解群当且仅当存在一个递降的子群列

$$G = G_0 \trianglerighteq G_1 \trianglerighteq G_2 \trianglerighteq \cdots \trianglerighteq G_r = \{e\}$$

其中的每一个因子群组都是有限可交换单群，因此是素数阶循环群.

在前面的 A_4 的三个合成群列中，我们还发现合成群列具有相同长度，这是由下面定理保证的：

Theorem 1.37 (Jordan-Holder 定理) 有限群 G 的任意两个无重复项的合成群列具有相同长度，并且因子群组可以用某种方式配对，使得对应的因子群同构.

Proof 证明参考丘维声近世代数 P66. □

1.4.2.1 习题及解答

习题一： $N \geq 5$ 时，求 S_n 的导群.
习题二： 证明 $N \geq 5$ 时，$A_n' = A_n$
习题三： 证明 $S_n, N \geq 5$ 时都是不可解群.
习题四： 证明 $N \geq 5$ 时，A_n 都是单群.

1.5 有限群的结构

1.5.1 群的直积

设 G 和 H 是两个群, 运算都为乘法运算，在 $G \times H$ 上规定

$$(g_1, h_1)(g_2, h_2) := (g_1 g_2, h_1 h_2)$$

这是 $(G \times H, G \times H$ 到 $G \times H$ 的映射. 容易验证在此运算下 $G \times H$ 是一个乘法群. 称它是 G 和 H 上的**直积**.

Remark 1.3 对于有限多个群的直积，我们都可以这样定义，但无限多个时不行. 为此我们需要范畴论的知识，所以在这里暂时不讲.

自然的我们会想问 G 是一个群，H, K 是它的两个子群. 什么时候有 $G \cong H \times K$? 下面定理给出了充要条件.

Theorem 1.38 $G \cong H \times K$ 当且仅当下列三条成立.

(1) $G = HK$;

(2) $H \bigcap K = \{e\}$;

(3) H 中的每一个元素和 K 都可交换;

Proof 考虑映射

$$\begin{aligned}\sigma:\ H\times K &\to G\\ (h,k) &\mapsto hk.\end{aligned}$$

$$\begin{aligned}\sigma\text{是满射} &\iff G\text{中每个元素}g\text{能表示作}g=hk,h\in H,k\in K\\ &\iff G=HK\\ \sigma\text{是单射} &\iff h_1k_1=h_2k_2\text{可推出}h_1=h_2,k_1=k_2\\ &\iff h_2^{-1}h_1=k_2k_1^{-1}\text{可推出}h_1=h_2,k_1=k_2\\ &\iff H\bigcap K=\{e\}\\ \sigma[(h_1,k_1)(h_2,k_2)=\sigma(h_1,k_1)\sigma(h_2,k_2),\forall h_i\in H,k_i\in K&\\ &\iff \text{H 中每个元素与 K 中每个元素可交换.}\end{aligned}$$

1.5.2 有限可换群的结构

Definition 1.15 设 n 是一个正整数.

(1) 若 n 可表示作

$$n=p_1^{\alpha_1}\cdots p_s^{\alpha_s}$$

其中 p_i 是素数，不要求彼此互异，$\alpha_i\geq 1$, 我们就称 $\left\{p_1^{\alpha_1},\cdots,p_s^{\alpha_s}\right\}$ 是 n 的一个**初等因子组**.

(2) 若 n 可表示作

$$n=h_1\cdots h_r$$

其中 $h_i|h_{i+1}$，则称 $\{h_1,\cdots,h_r\}$ 是 n 的一个**不变因子组**.

Theorem 1.39 (初等因子定理) *设 G 是有限阿贝尔群，其阶数为 n，则 G 可表示作*

$$G\cong C_{p_1^{\alpha_1}}\times\cdots\times C_{p_s^{\alpha_1}}$$

其中 $\left\{p_1^{\alpha_1},\cdots,p_s^{\alpha_s}\right\}$ 是 n 的一个初等因子组. (该表示除乘积顺序外唯一.)

思路： G 是有限群，于是 G 可以由有限多个元素生成. 如果 G 有一个生成元集 W，其中含有 r 个元素. 若 G 的任何 r-1 个元素都不能生成 W，则称 W 是**极小生成元集**. 对于有限群一定有极小生成元集，生成元集可以不同，但有一样的元素个数. 于是在证明时候我们可以对生成元集的元素个数作归纳法. 此外，我们若能证明对有限可交换 p-群 P 结论成立，那么根据定理1.38和 Sylow 第一定理，就可以知道对任意有限可交换群 G 成立.

Proof 我们着手证明此定理对有限可交换 p-群 P 成立. 对可交换 p-群 P 的极小生成元集含有的元素个数 n 做归纳法.

n=1 时，此 Abel p-群是循环群，结论成立.

设当 n=r-1 时，命题成立，下面验证 n=r 的情形. 设 P 是阶为 p^l 的阿贝尔 p-群, 它的极小生成元集含有 r 个元素. 为了使用归纳假设，我们希望将 P 分解作

$$P =< a > \times P_1, \quad a \in P,\ P_1 \leq P$$

并且 P_1 的极小生成元集含有 r-1 个元素. 若能找到这样的 a 和 P_1 就由归纳假设就证完了，于是我们去找这样的两个东西. 自然的我们会想到要去 P 的含 r 个元素的极小生成元集中找.

回顾定理1.38, 知道我们找的 a 和 P_1 应该满足：

(1) $< a > \bigcap\ P_1 = \{e\}$;

(2) $P =< a > \times P_1$;

(3) $< a >$ 和 P_1 中元素可以任意交换;

考虑 M 是这样的集合:

$$M = \left\{(j_1, \cdots, j_r) \mid x_1^{j_1} \cdots x_r^{j_r} = e,\ \{x_1, \cdots, x_r\} \text{是 P 的一个极小生成元集}\right\}$$

M' 是这样的集合

$$M' = \{min\{j_1, \cdots, j_r\} \mid (j_1, \cdots, j_r) \in M,\ j_i > 0\}$$

于是 M' 有最小正整数，记作 m. 因而有 P 的极小生成元集 $\{x_1, \cdots, x_r\}$, 使得

$$x_1^m x_2^{j_2} \cdots x_r^{j_r} = e \quad (1)$$

我们断言 $m \mid j_i,\ 2 \leq i \leq r$. 否则, 以 $i = 2$ 为例： $j_2 = q_2 m + u_2,\ 0 \leq u_2 \leq m$

$$e = (x_1 x_2^{q_2})^m x_2^{u_2} \cdots x_r^{j_r}$$

由于 $\left\{x_1 x_2^{q_2}, x_2, \cdots, x_r\right\}$ 也是 P 的一个极小生成元集，于是 $(m, u_2, \cdots, j_r) \in M,\ u_2 \in M'$, 由于 m 是 M' 中最小的，于是 $u_2 = 0$. 类似可证得 $m \mid j_i,\ 2 \leq i \leq r$.

因此 (1) 化作

$$(x_1 x_2^{q_2} \cdots x_r^{q_r})^m = e$$

我们命 $a = (x_1 x_2^{q_2} \cdots x_r^{q_r}),\ P_1 = < x_2, \cdots, x_r$.

我们可以验证：

(1) $< a > P_1 = P$

(2) $< a >$ 和 P_1 中元可任意交换

(3) 若 $< a > \bigcap P_1 = y$, 则 $\exists s < m\ a^s = x_2^{q_2} \cdots x_r^{q_r}$, 于是

$$a^s x_2^{-q_2} \cdots x_r^{-q_r}$$

导致 $s \in M'$, 这与 m 的选取有关，进而

$$< a > \bigcap P_1 = \{e\}.$$

从而 $G =< a > \times P_1$. 由归纳假设

$$P_1 \cong C_{p^{\alpha_2}} \times \cdots \times C_{p^{\alpha_r}}$$

再

$$< a > \cong C_{p^{\alpha_1}}$$

于是

$$G \cong C_{p^{\alpha_1}} \times \cdots \times C_{p^{\alpha_1}}.$$

其中 $\alpha_1 + \cdots + \alpha_r = l$

于是我们对可交换 p-群证明了结论正确. 再由于 G 可以分解作 Sylow-p 子群的乘积，Sylow-p 子群又可以分解，于是定理得证.

Theorem 1.40 (不变因子定理) 设 G 是有限阿贝尔群，其阶数为 n，则 G 可表示作

$$G \cong C_{h_1} \times \cdots \times C_{h_r}$$

其中 $\{h_1, \cdots, h_r\}$ 是 n 的一个不变因子组.

Theorem 1.41 每一个有限阿贝尔群的初等因子组唯一，两个有限阿贝尔群同构当且仅当它们有一样的初等因子组.

Proof 此证明有些复杂，具体参考丘维声近世代数 P93. □

1.6 群例

1.6.1 n 元对称群

Definition 1.16 :

(1) 给定一个集合 Ω, 其上全部自双射组成的集合记作 S_Ω, S_Ω 是一个群，称作 Ω 上的全变换群.

(2) 特别的当 Ω 基数有限时，称集合上的每一个自双射是一个置换，此时 S_Ω 称作是 n 元对称群，记作 S_n.

一个 n 元置换 σ 把 $i \mapsto a_i$, 记作

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ a_1 & a_2 & \cdots & a_n \end{pmatrix}$$

可以看出这样的置换一共有 $n!$ 个, 于是 $|S_n| = n!$.

S_n 中任意两个置换相乘是按照映射的乘法进行的, 以 S_4 中两个置换 σ, τ 为例. 设

$$\sigma = \begin{pmatrix} 1\ 2\ 3\ 4 \\ 2\ 3\ 4\ 1 \end{pmatrix}, \quad \tau = \begin{pmatrix} 1\ 2\ 3\ 4 \\ 4\ 3\ 2\ 1 \end{pmatrix}.$$

则

$$\sigma\tau = \begin{pmatrix} 1\ 2\ 3\ 4 \\ \downarrow\ \downarrow\ \downarrow\ \downarrow \\ 4\ 3\ 2\ 1 \\ \downarrow\ \downarrow\ \downarrow\ \downarrow \\ 1\ 4\ 3\ 2 \end{pmatrix} = \begin{pmatrix} 1\ 2\ 3\ 4 \\ 1\ 4\ 3\ 2 \end{pmatrix},$$

$$\tau\sigma = \begin{pmatrix} 1\ 2\ 3\ 4 \\ \downarrow\ \downarrow\ \downarrow\ \downarrow \\ 2\ 3\ 4\ 1 \\ \downarrow\ \downarrow\ \downarrow\ \downarrow \\ 3\ 2\ 1\ 4 \end{pmatrix} = \begin{pmatrix} 1\ 2\ 3\ 4 \\ 3\ 2\ 1\ 4 \end{pmatrix}.$$

我们还可以用一种更节省的方式写出置换. 例如, (4) 式中的 σ, 它把 $1 \mapsto 2, 2 \mapsto 3, 3 \mapsto 4, 4 \mapsto 1$, 于是可以把 σ 写成下述形式:

$$\sigma = (1 \quad 2 \quad 3 \quad 4)$$

类似地, (4) 式中的 τ, 它把 $1 \mapsto 4, 4 \mapsto 1, 2 \mapsto 3, 3 \mapsto 2$, 于是可以把 τ 写成下述形式: $\tau = (14)(23)$. 由此引出下述概念:

如果一个 n 元置换 σ 把 i_1 映成 i_2, 把 i_2 映成 $i_3, \cdots\cdots$, 把 i_{r-1} 映成 i_r, 把 i_r 映成 i_1, 并且 σ 保持其余元素不变, 那么称 σ 为一个 **r-轮换** ($r-$ cycle), 简称为轮换, 记做 $(i_1 i_2 i_3 \cdots i_{r-1} i_r)$, 也可以写成 $(i_2 i_3 \cdots i_{r-1} i_r i_1)$, 还可以写成 $(i_3 i_4 \cdots i_{r-1} i_r i_1 i_2)$, 等等. 特别地, 2 - 轮换也称为**对换**; 恒等映射 I 记做 (1). 两个轮换如果它们之间没有公共的元素, 那么称它们不相交 (disjoint).

例如, S_5 中, (134) 与 (25) 是不相交的两个轮换. 乘积 (134) (25) 把 $1 \mapsto 3, 2 \mapsto 5, 3 \mapsto 4, 4 \mapsto 1, 5 \mapsto 2$, 而乘积 (25) (134) 也是把 $1 \mapsto 3, 2 \mapsto 5, 3 \mapsto 4, 4 \mapsto 1, 5 \mapsto 2$. 因此, (134) (25) = (25)(134). 这种分析方法对于任意两个不相交的轮换都适用. 因此我们得到: **不相交的两个轮换对乘法是可交换的**.

从 (4) 式中的 σ, τ 写成轮换形式的过程, 容易猜想有下述结论:

Theorem 1.42 *S_n 中任一非单位元的置换都能表示成一些两两不相交的轮换的乘积, 并且除了轮换的排列次序外, 表示法是唯一的.*

Proof 设 $\sigma \in S_n$, 且 $\sigma \neq (1)$. 于是在 $\Omega = \{1, 2, \cdots, n\}$ 中至少有一个 i_1 使得 $\sigma(i_1) \neq i_1$. 设

$$\sigma(i_1) = i_2, \quad \sigma(i_2) = i_3, \quad \cdots.$$

由于 $|\Omega| = n$, 因此在有限步后所得的像必与前面的元素重复. 设 i_r 是第一个与前面的元素重复的元素, 设 $i_r = i_j, j < r$. 假如 $j > 1$, 由于 $\sigma(i_{r-1}) = i_r, \sigma(i_{j-1}) = i_j$, 因此

$$\sigma^{r-1}(i_1) = i_r = i_j = \sigma^{j-1}(i_1).$$

在上式两边用 σ^{-1} 作用得

$$\sigma^{r-2}(i_1) = \sigma^{j-2}(i_1).$$

即 $i_{r-1} = i_{j-1}$. 这与 i_r 的选择矛盾. 因此 $j = 1$. 从而 $i_r = i_1$. 于是得到一个轮换 $\sigma_1 = (i_1 i_2 \cdots i_{r-1})$. 在 $\Omega \setminus \{i_1, i_2, \cdots, i_{r-1}\}$ 中重复上述步骤, 便可得到 σ 表示成两两不相交轮换乘积的式子:

$$\sigma = \sigma_1 \sigma_2 \cdots \sigma_t.$$

唯一性假设 σ 还有一个表示成两两不相交轮换乘积的式子: $\sigma = \tau_1 \tau_2 \cdots \tau_s$. 任取在 σ 下变动的元素 a, 则在 $\sigma_1, \sigma_2, \cdots, \sigma_t$ 中存在唯一的 σ_l, 使得 $\sigma_l(a) \neq a$. 同理, 在 $\tau_1, \tau_2, \cdots, \tau_s$ 中存在唯一的 τ_k, 使得 $\tau_k(a) \neq a$. 我们有

$$\sigma_l^m(a) = \sigma^m(a) = \tau_k^m(a), \quad m = 0, 1, 2, \cdots.$$

$\sigma_l = \tau_k$. 继续这样的讨论, 可得 $t = s$, 并且在适当排列 $\tau_1, \tau_2, \cdots, \tau_s$ 的次序后, 有 $\sigma_i = \tau_i, i = 1, 2, \cdots, t$. 从而唯一性成立. □

现在对于前面 S_4 中的 σ, τ, 用它们的轮换分解式来做乘法:

$$\sigma\tau = (1234)(14)(23) = (1)(24)(3) = (24),$$
$$\tau\sigma = (14)(23)(1234) = (13)(2)(4) = (13).$$

像上两式那样, 在运算的结果中常常把 1-轮换省略不写.

现在我们来思考一共轮换的逆元. 对于 σ, 容易求出它的逆元:

$$\sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix} = (1432).$$

与 σ 的轮换表示式 $\sigma = (1234)$ 比较, 猜测有如下结论:

$$(i_1 i_2 \cdots i_{r-1} i_r)^{-1} = (i_1 i_r i_{r-1} \cdots i_2).$$

证明如下: 由于

$$(i_1 i_2 \cdots i_{r-1} i_r)(i_1 i_r i_{r-1} \cdots i_2) = (i_1)(i_2) \cdots (i_{r-1})(i_r),$$
$$(i_1 i_r i_{r-1} \cdots i_2)(i_1 i_2 \cdots i_{r-1} i_r) = (i_1)(i_2) \cdots (i_{r-1})(i_r),$$

因此

$$(i_1 i_2 \cdots i_{r-1} i_r)^{-1} = (i_1 i_r i_{r-1} \cdots i_2).$$

通过直接计算可知下式成立:

$$(1234) = (14)(13)(12).$$

一般地, 可以直接验证下式成立:

$$(i_1 i_2 i_3 \cdots i_{r-1} i_r) = (i_1 i_r)\,(i_1 i_{r-1}) \cdots (i_1 i_3)\,(i_1 i_2)\,.$$

再结合定理1.42, 以及 $(1) = (12)(12)$, 得

Corollary 1.7 *S_n 中每一个置换都可以表示成一些对换的乘积.*

注意: 把置换表示成对换的乘积, 其表示方式不唯一, 并且这些对换会相交. 例如:

$$(134) = (14)(13),$$
$$(134) = (12)(34)(24)(12).$$

从上式看出, 把 (134) 表示成对换的乘积, 对换的个数都是偶数. 由此猜测有下述结论:

Proposition 1.2 *S_n 中一个置换表示成对换的乘积, 其中对换的个数的奇偶性由这个置换本身决定, 与表示方式无关.*

Proof 任取 $\sigma \in S_n$, 设

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ a_1 & a_2 & \cdots & a_n \end{pmatrix}.$$

则 σ 把 n 元排列 $12\cdots n$ 变成 n 元排列 $a_1 a_2 \cdots a_n$. 可以证明, 把 n 元排列 $12\cdots n$ 变成 $a_1 a_2 \cdots a_n$ 可以经过一系列对换实现, 并且所做对换的次数与 n 元排列 $a_1 a_2 \cdots a_n$ 有相同的奇偶性. 因此 σ 可以表示成一些对换的乘积, 其中对换的个数由 σ 本身决定, 与表示方式无关. □

由于上命题, 我们引出下述概念:

如果一个置换可以分解做偶数个兑换的乘积, 称作偶置换, 否则称作奇置换. 可以证明偶置换全体构成偶置换群, 称作 **n 元交错群**, 记作 A_n.

1.6.2 习题及解答

习题一: 证明

(1) $S_n =< \{(12), (23), \cdots, (n-1, n)\} >$.

(2) $S_n =< \{(12), (12\cdots n)\} >$.

Chapter 2
群在集合上的作用以及其应用

2.1 群作用及 sylow 定理

2.1.1 群作用

引言：在 Galois 考虑方程根式可解的时候，其考虑导方程根的置换群到根集的作用，这个作用保持了根之间关系式的不变性，于是我们引入群作用的概念.

Definition 2.1 G 是一个群，Ω 是一个非空集合，若映射

$$\begin{aligned}\sigma:\ G\times\Omega &\to \Omega\\ (a,x) &\mapsto x^a\end{aligned}$$

满足

$$\begin{aligned}&x^{(ab)} = (x^b)^a, \quad \forall a,b\in G, \forall x\in\Omega;\\ &e(x) = x, \quad \forall x\in\Omega;\end{aligned}$$

那么称 G 在 Ω 上有一个作用.

我们怎么理解一个群作用呢? 实际上，若 G 在 Ω 上有一个群作用，就意味着每一个 G 中的元 $a\in G$ 都对应了 Ω 上的一个映射 ϕ_a. 由于 $\phi_a\phi_{a^{-1}} = \phi_e = 1_\Omega$, 说明 ϕ_a 是可逆的，进而是一个双射. 于是群中任意一个元素都对应了 Ω 上的一个变换，这种群到变换群的对应就是我们所说的群作用.

事实上我们可以更进一步的证明：

Proposition 2.1 *设 G 在集合 Ω 上有一个作用，则存在一个同态映射 ϕ.*

$$\begin{aligned}\phi: G &\to S_\Omega\\ a &\mapsto \phi_a\end{aligned}$$

其中 $\phi_a(x) = x^a$. 即群 G 中元素 a 作用在 $x\in\Omega$ 下的像.

在同态映射 ϕ 下的核称作这个群作用的核，我们有

$$\begin{aligned} a \in G\text{是这个作用的核} &\iff a \in Ker\phi \\ &\iff \phi_a = 1_\Omega \\ &\iff \phi_a(x) = x, \quad \forall x \in \Omega \\ &\iff x^a = x, \quad \forall x \in \Omega \end{aligned}$$

当 $Ker\phi = \{e\}$ 时，称这个作用是**忠实的**. 此时同态 $\phi : G \to S_\Omega$ 是单同态. 我们可以把命题2.1反过来. 即：若群 G 到 Ω 的变换群 S_Ω 有一个同态映射，则 G 在 Ω 上有一个作用.

下面介绍一些重要的群作用

1.

$$\begin{aligned} G \times G &\to G \\ (a, x) &\mapsto ax \end{aligned}$$

即群 G 在 G 上的作用，称作群 G 在 G 上的**左平移**. 由于 $ax = x,\ \forall x \in G \iff a = e$, 于是 $Ker\phi = \{e\}$, 说明左平移作用是忠实的. 于是 $\phi : G \to S_G$ 是单同态，$G \cong Im\phi \leq S_G$. 于是我们有下定理

Theorem 2.1 (Cayley 定理) *任意一个群都同构于某一个变换群，任意有限群同构于某一个置换群.*

2.

$$\begin{aligned} G \times G &\to G \\ (a, x) &\mapsto axa^{-1} \end{aligned}$$

称作共轭作用，本质上此作用是 G 到 G 的自同构群的一个双射.

群 G 在集合上的作用还可给出一个集合上的划分. 我们定义

$$x \sim y \iff \exists a \in G, x^a = y \quad \forall x, y \in \Omega$$

可以验证"~" 是等价关系. 于是可以据此等价关系划分出等价类：

$$\begin{aligned} \forall x \in \Omega, \overline{x} &= \{y \in \Omega | y \sim x\} \\ &= \{x^a | a \in G\} \\ &:= G(x) \end{aligned}$$

我们把包含 x 的等价类 $G(x)$ 称作是 x 的 G-轨道. x 的 G-轨道就是 x 在群 G 的作用下能到达的所有点的集合. 容易看出两条轨道要么不相交要么相等. 于是 Ω 可以写作不交轨道的并.

$$\Omega = \bigcup_{i=1}^{k} G(x_i)$$

我们称 $\{x_i\}$ 是 Ω 的 G-轨道的完全代表系.

下面我们分析一条轨道的长度，也就是 x 在群 G 作用下能到达的点的数量.

我们知道对于 $\forall a, b \in G,\ x, y \in \Omega, x^a = x^b \iff x^{ab^{-1}} = x$. 于是我们考虑这样的 G 的子集

$$G_x := \{g \in G | x^g = x\}$$

可以验证这是一个 G 的子群，称作点 x 的稳定子群. x 的稳定子群中的元素作用在 x 上保持 x 不变. 那么很快我们就可以猜想有

$$|G(x)| = [G : G_x]$$

事实上这是正确的，这是由于

$$\begin{aligned} x^a \neq x^b &\iff ab^{-1} \notin G_x \\ &\iff aG_x \neq bG_x \end{aligned}$$

因此不同的 x^a 的个数应该和不同的 G 在 G_x 下的陪集数一样多. 于是我们证明了:

Theorem 2.2 (轨道-稳定子定理) *设 G 在集合 Ω 上有一个作用，则对于 $\forall x \in \Omega$*

$$|G(x)| = [G : G_x]$$

Corollary 2.1 *对于有限群 G，若 G 在集合 Ω 上有一个作用，那么 $\forall x \in \Omega$ 有*

$$|G(x)| = \frac{|G|}{|G_x|}$$

从而轨道长度都是 G 的阶的因子.

Remark 2.1 注意区分 $G(x)$ 和 G_x, 前者是 Ω 的子集，表示 $x \in \Omega$ 在群作用下能到达的元素的集合，后者是 G 的子集, 表示 x 的稳定子群.

我们可以将此推论运用到共轭作用上，对共轭作用作 G-轨道划分就得到有限群的**类方程**:

$$|G| = |C_G| + \Sigma_{i=1}^{s} |G(x_i)| = |C_G| + \Sigma_{i=1}^{s} [G : C_G(x)]$$

其中 $G(x)$ 是 x 的共轭类.

接下来我们考虑 Ω 中 G-轨道数.

Definition 2.2 若 G 在 Ω 上的作用只有一条轨道，即对于 $\forall x, y \in \Omega,\ \exists g \in G$, 使得 $y = x^g$. 那么称 G 在 Ω 上的作用是传递的. 此时称 Ω 是群 G 的一个齐次空间.

现在考虑，若有限群 G 在有限集合 Ω 上的作用有 r 条轨道，则有 Ω 的 G-轨道完全代表系 $\{x_1, \cdots, x_r\}$, 使得

$$\Omega = \bigcup_{i=1}^{r} G(x_i)$$

于是

$$|\Omega| = \sum_{i=1}^{r} |G(x_i)| = \sum_{i=1}^{r} \frac{|G|}{|G_{x_i}|}$$

这启示我们，若 x, y 属于同一条轨道，则应有 $|G_x| = |G_y|$. 我们来验证一下.

$$\begin{aligned} \text{x 和 y 属于同一轨道} &\iff \exists a \in G, y = x^a \\ \forall g \in G_y, y^g = y &\Rightarrow x^{ag} = x^a \\ &\Rightarrow x^{aga^{-1}} = x \\ &\Rightarrow aga^{-1} \in G_x \\ &\Rightarrow aG_y a^{-1} \subseteq G_x. \end{aligned}$$

类似的可以得到 $a^{-1}G_x a \subseteq G_y$, 说明 $G_x = a^{-1}G_y a$. 于是我们证明了

Proposition 2.2 *G 在 Ω 上有一个作用，则同一条 G-轨道上的点，它们的稳定子群是共轭的，因此这些稳定子群的阶数相同.*

由此命题，G_{x_i} 中所有元素的稳定子群的阶的和就是

$$|G_{x_i}||G(x_i)| = |G| \quad \text{(由轨道稳定子定理)}$$

更近一步，所有 Ω 中元素的稳定子群的阶的和就是

$$\sum_{x\in\Omega} |G_x| = \sum_{i=1}^{r} |G(x_i)||G_{x_i}| = r|G|$$

为了求 r , 我们需要有另一种方法求 $\sum_{x\in\Omega} |G_x|$.

考虑 $G \times \Omega$ 的子集 $S = \{(g, x)|x^g = x\}$. 则

$$|S| = \sum_{x\in\Omega} |G_x| = r|G|.$$

另一方面，给定 $\forall g \in G$, 记 $F(g) := \{x \in \Omega|x^g = x\}$, 则

$$|S| = \sum_{g\in G} |F(g)|$$

从而

$$r|G| = \sum_{g\in G} |F(g)|$$

$$r = \frac{1}{|G|} \sum_{g\in G} |F(g)|$$

这就是著名的 *Burside* 引理.

Theorem 2.3 (Burside 定理) 对于有限群 G，有限集 Ω，Ω 在 G 的作用下有 r 条轨道，则

$$r = \frac{1}{|G|}\sum_{g\in G}|F(g)|.$$

我们接下来考虑群作用的一种情况，若 $\exists x \in \Omega,\ \forall g \in G,\ x^g = x$, 我们称 x 是群 G 作用下的不动点，以 Ω_0 记所有不动点的全体.

Proposition 2.3 *p-群 G 在有限集 Ω 上有作用，则*

$$|\Omega_0| \equiv |\Omega| \ (mod\ p)$$

Proof

$$|\Omega| = |\Omega_0| + \sum_{i=1}^{r}|G(x_i)|$$

由于 $|G(x_i)| = \dfrac{|G|}{|G_{x_i}|}$, 于是每一个 $|G(x_i)|$ 都被 p 整除，说明

$$|\Omega| = |\Omega_0| \ (mod\ p).$$

将此命题应用在群共轭作用上，我们可以得到 $|G| \equiv |Z(G)| \ (mod\ p)$. 这就是定理1.16.

关于传递作用，我们还有一个重要的定理：

Theorem 2.4 (Frattini 论断) *设 G 作用在 Ω 上，并且 G 包含一个子群 N，子群在 Ω 上的作用是传递的，则*

$$G = G_\alpha N \quad \forall \alpha \in \Omega$$

Proof $\forall \alpha \in \Omega,\ \forall g \in G.\ \alpha^g = \beta$. 由于 N 是传递的，于是存在 $n \in N,\ \alpha^n = \beta, \alpha^{gn^{-1}} = \alpha,\ gn^{-1} \in G_\alpha$. 于是 $g = gn^{-1}n \Rightarrow G = G_\alpha N$. □

2.1.2 sylow 定理

前言： *Larange* 定理指出，有限群的任一子群的阶数一定是群阶数的因子，很自然的我们会考虑这个定理的逆：群 G 的阶数 $|G|$ 的因子 d, 是否一定有 d 阶的子群. 对于循环群显然是成立的，很遗憾的是对于一般群此定理不成立. 我们有反例：

Example 2.1 $|A_4| = 4!$, 但 A_4 中只有 2 阶，3 阶和 2^2 阶子群，无 6 阶子群.

这个例子让我们不禁猜想: 若 p 是 $|G|$ 的素因子，是否一定有 p^k 阶子群.

我们正式的提出问题: $|G| = p^l m$, p 是素数，$(m, p) = 1$, 对于 $1 \le k \le l$, 是否一定有 p^k 阶子群?

思路： 首先 G 的 p^k 阶子群一定是 G 的 p^k 阶子集. 于是我们将所有 G 的 p^k 阶子集取出，命名作集合 Ω. 考虑 G 在 Ω 上的作用：

$$\forall g \in G,\ A = \left\{a_1, \cdots, a_{p^k}\right\} \in \Omega,\ gA := \left\{ga_1, \cdots, ga_{p^k}\right\}$$

那么 G_A (A 的稳定子群) 就是一个 G 的子群. 由于 $\forall a \in A,\ G_A a \subseteq A$, 于是

$$|G_A| = |G_A a| \leq |A| = p^k$$

也就是说，现在我们只需要找到一个 G_A, 满足 $|G_A| \geq p^k$ 即可. 或者更进一步，找到一个 G_A, 满足 $p^k | G_A$ 也可以.

由于

$$|G| = |G_A||G(A)|$$

于是若 $p^k || G_A|$, 那么 $p^{l-k+1} \nmid |G(A)|$. 于是我们去找一个 $G(A)$, $p^{l-k+1} \nmid |G(A)|$.

我们想到

$$|\Omega| = \sum_{i=1}^{r} |G(A_i)|$$

于是若 $p^{l-k+1} \nmid |\Omega|$, 那么我们就能找到一个 A_i, $p^{l-k+1} \nmid |G(A_i)|$.

事实上，

$$|\Omega| = C_n^{p^k} = \frac{n(n-1)\cdots(n-p^k+1)}{p^k(p^k-1)\cdots(p^k-p^k+1)}$$

我们比较每一个 $n-j$ 和 $p^k - j$, 命 $j = p^t t'$, $(p, t') = 1$, 那么

$$n - j = p^t(p^{l-t} - j')$$
$$p^k - j = p^t(p^{k-t} - j'$$

于是 $C_n^{p^k}$ 中，至多只 p 的 p^{l-s} 因子. 说明 $p^{l-k+1} \nmid C_n^{p^k} = |\Omega|$. 于是根据前面的思考，存在一个 $G(A_i)$, $p^{l-k+1} \nmid |G(A_i)|$, $p^k || G_{A_i}|$, $|G_{A_i}| = p^k$. 我们就找到了要求的 p^k 阶群.

这就是著名的

Theorem 2.5 (Sylow 第一定理) *设 G 的阶 $n = p^l m$, 其中 p 是素数，$(m, p) = 1$. 则对于 $1 \leq k \leq l$, 在 G 中比存在 p^k 阶子群，其中 p^l 阶子群我们称作 G 的* ***Sylow p-子群***.

现在我们知道，每一个 p^l 阶子群，其包含 p^k, $1 \leq k \leq l$ 阶子群，那么反过来，任意 p^k, $1 \leq k \leq l$ 阶子群，是否一定含于某一个 p^l 阶子群中呢?

首先给定一个 Sylow-p 子群 P, 容易验证所有 P 的共轭子群都是 G 的 Sylow-p 子群. 于是我们只需说明，任意 p^k 阶子群 H，一定含于 P 的某个共轭子群即可.

$$\begin{aligned}
\text{H 含于 P 的共轭子群中} &\iff \exists a \in G,\ H \subseteq aPa^{-1} \\
&\iff \exists a \in G,\ a^{-1}Ha \subseteq P \\
&\iff \exists a \in G,\ \forall h \in H,\ a^{-1}ha \in P \\
&\iff \exists a \in G,\ \forall h \in H,\ (ha)P = aP
\end{aligned}$$

于是我们考虑群 H 在集合 G/P 上的左平移作用

$$\phi:\ H\times(G/P)\to(G/P)$$
$$(h,gP)\mapsto(hg)P$$

为了证明前面 a 的存在性，我们只需说明在这个左平移作用下的不动点集不空就行.

由于 H 是 p-群，由2.3

$$|\Omega_0|\equiv|(G/P)|=\frac{|G|}{|P|}=m\neq 0\ (mod\ p)$$

于是不动点集非空，说明 $\exists a\in G, H\subseteq a^{-1}Pa$, 即含于某个 Sylow-p 子群中. 特别的取 $k=l$, 我们得到容易 Sylow-p 子群都是共轭的. 这就是：

Theorem 2.6 (Sylow 第二定理) *设 G 的阶 $n=p^lm$, 其中 p 是素数，$(m,p)=1$. 则对于 $1\leq k\leq l$, 任意 p^k 阶子群，其一定含于某一个 Sylow p-子群中. 特别的，两个 Sylow p-子群是共轭的.*

Corollary 2.2 *有限群 G 的 Sylow p-子群是正规子群当且仅当 G 中只有一个 Sylow p-子群.*

Proof 取 G 的一个 Sylow p-子群 P. 由于 $\forall a\in G, a^{-1}Pa$ 也是一个 Sylow p-子群，故 $a^{-1}Pa=P\Rightarrow aP=Pa$, 故 P 是正规子群. 必要性同理. □

自然的我们就会去思考，如何求一个 Sylow p-子群的个数?

命 $\Omega=\{P_1,\cdots,P_r\}$ 是所有 Sylow p-子群的集合. 由命题2.3, 我们可以考虑 p-群的群作用. 最自然的就是考虑 P_1 (Remark: 这是任意一个 Sylow p-子群). 规定群作用

$$\phi:\ P_1\times\Omega\to\Omega$$
$$(a,P_i)\mapsto a^{-1}P_ia$$

我们研究此作用的不动点:

$$\begin{aligned}Q\in\Omega_0&\iff a^{-1}Qa=Q,\ \forall a\in P_1\\&\iff a\in N_G(Q),\ \forall a\in P_1\\&\iff P_1\subseteq N_G(Q)\end{aligned}$$

显然 P_1,Q 都是 $N_G(Q)$ 的 Sylow-p 子群, 并且 $Q\trianglelefteq N_G(Q)$, 于是由上推论知, $P_1=Q$. 故

$$\Omega_0=\{P_1\}$$

于是由命题2.3

$$r=|\Omega|\equiv 1\ (mod\ p).$$

此外 P_1 在 G 中共轭子群的个数 $r=[G:N_G(P_1)]\ ||G|=p^lm$, 于是 $r|m$. 综上我们证明了:

Theorem 2.7 (Sylow 第三定理) *G 中 Sylow p-子群的个数 r, 满足*

$$r\equiv 1\ (mod\ p)$$

$|G|=p^lm,\ (m,p)=1$, 则 $r|m$.

2.1.3 习题及解答

习题一: G 在 Ω 上的作用是传递的，$N \trianglelefteq G$, 证明 N 在 Ω 上的轨道一样长.

Proof 任取 N 在 Ω 上的两条轨道

$$N(x) = \{x^n | n \in N\}$$
$$N(y) = \{y^n | n \in N\}$$

由于 G 是传递的，于是存在 $g \in G$, $x^g = y$. 又由于 N 是正规的，于是 $gNg^{-1} = N$. 从而

$$\begin{aligned} N(x) &= \left\{x^{gng^{-1}} | gng^{-1} \in N\right\} \\ &= \left\{x^{gng^{-1}} | n \in N\right\} \\ &= \left\{y^{ng^{-1}} | n \in N\right\} \end{aligned}$$

作映射

$$\begin{aligned} \sigma : N(x) &\to N(y) \\ y^{ng^{-1}} &\mapsto y^n \end{aligned}$$

容易验证这是一个双射，于是两个轨道一样长. □

习题二: 有限群 G 忠实的作用在 Ω 上，A 是 G 的交换子群, 且在 Ω 上传递. 证明 $C_G(A) = A$.

Proof 由于 A 是交换的，于是 $A \subseteq C_G(A)$. 下证反包含关系.

若 $b \in C_G(A)$, 由 Frattin 论断2.4,

$$\forall \alpha \in \Omega, \exists g_0 \in G_\alpha,\ a_0 \in A,\ b = g_0 a_0$$

由于 A 是传递的，于是 $\forall \beta \in \Omega$, $\exists a \in A$, 使得 $\beta = \alpha^a$. 此时

$$\begin{aligned} \alpha^{ab} = \beta^b &\Rightarrow \alpha^{ba} = \beta^b \\ &\Rightarrow \alpha^{g_0 a_0 a} = \beta^b \\ &\Rightarrow \alpha^{a_0 a} = \beta^b \\ &\Rightarrow \beta^{a_0} = \beta^b \\ &\Rightarrow b a_0^{-1} \in Ker\phi \\ &\Rightarrow b = a_0 \in A \end{aligned}$$

于是反包含关系得证. □

2.2 Sylow 定理在可解群、P-群上的应用

Recall 1: 一个群称作 p-群，若其所有元素的阶都是 p 的方幂. 若 G 是有限群，则这等价于 G 的阶数是 p 的方幂.

Recall 2: 我们用 $N < G$ 表示 N 是 G 的真子群，用 $N \subset G$ 表示 N 是 G 的真子集.

Recall 3: 一个群的子群 H，与 H 共轭的子群一共有 $[G : N_G(H)]$ 个.

下面我们来研究 p-群的可解性. 我们想说明，有限 p-群都是可解群.

Theorem 2.8 *有限 p-群都是可解群.*

Proof 设 $|G| = p^l$, 我们对 l 作归纳. 当 $l = 0$ 时，结论显然成立. 假设当 $l < n$ 时结论成立，考虑 $l = n$ 时. 若我们能在 G 中取出一个正规 p^{l-1} 阶群 P'，那么由归纳假设知 P' 和 G/P' 都是可解群，于是 G 也是可解群. 由于所求 P' 的存在性可由下引理保证. 于是 p-群都是可解群. □

Lemma 2.1 *G 是有限群，P 是 G 的 p-子群，但不是 Sylow p-子群，则 $P \subset N_G(P)$. 进一步，若 P 是 G 的极大子群，则 P 是正规子群，并且 $|P| = \dfrac{|G|}{p}$.*

Proof 对 G 作双陪集分解

$$G = \bigcup_{i=1}^{k} Px_iP$$

每一个双陪集，又可以分解作 $n_i = [P : P^{x_i} \bigcap P] = \dfrac{|P|}{|P^{x_i} \bigcap P|} = p^s$ 个 P 的右陪集的并. 于是，G 可以分解作 $n_1 + \cdots + n_k = [G : P]$ 个右陪集的并. 由于 $p|[G : P]$, 并且有一个 $Px_iP = P, n_i = 1$, 于是还有至少一个 $n_j = 1$. 说明存在 x_j

$$P^{x_j} \bigcap P = P,\ P^{x_j} = P$$

于是 $x_j \in N_G(P),\ x_j \notin P$, 从而 $P \subset N_G(P)$.

由于 $P < N_G(P)$, 由 P 的极大性，$G = N_G(P)$ ，说明其是正规子群. □

Remark 2.2 于是对于一个 p^l 阶的 p-群 G，其任意 p^{l-1} 阶子群是极大子群，进而是正规子群. 这就补完了上定理的证明.

Theorem 2.9 *pq 阶群 G 是可解群. 其中 p,q 是素数.*

Proof 不妨设 $p < q$, 则由 Sylow 第一定理指导其有 Sylow q-子群 Q. Q 是可解群，于是若我们能说明 Q 是正规子群即可. 对 G 作 Q 的共轭分解，假设 Q 有 n_q 个共轭类. 由 Sylow 第三定理

$$n_q \equiv 1\ (mod\ q),\ n_q = \frac{|G|}{|N_{G(Q)}|} \leq \frac{|G|}{|Q|} \leq p$$

于是 $n_q = 1$，由 Sylow 第二定理知 Q 是正规子群，于是 G/Q 是商群 $|G/Q| = p$ 是可解群，从而 G 是可解群. □

更进一步我们有

Theorem 2.10 $p^\alpha q$ 阶群 G 是可解群，其中 p,q 是素数，α 是正整数.

Proof 设 P 是 G 的 Sylow p-子群，若 P 是 G 的正规子群，则定理得证. 否则考虑 P 的所有共轭子群，即所有 Sylow p-子群:

$$p_1,\cdots,p_{n_p}.$$

我们有 $n_p=\dfrac{|G|}{|N_G(P_1|}=q$ 于是可以改写所有正规子群作:

$$P_1,\cdots,P_q$$

下面分情况考虑

(i) 若对于 $i\neq j$, $P_i\bigcap P_j=\{e\}$. 此时 $\bigcup_{i=1}^{q}P_i$ 包含 $(p^\alpha-1)q+1$ 个元素. 此时还剩下 $q-1$ 个元素为包含进去. 由于 G 中还有一个 q 阶子群，q 子群和 p 子群是不交的，于是这样的 q 子群只有一个，于是此 q 子群是正规的，那么由 q 子群可解，q 子群的商群可解，知 G 可解.

(ii) 若有 $P_i\bigcap P_j>1$. 选取 $i\neq j$, 使得 $|P_i\bigcap P_j|$ 最大. 令 $P_i\bigcap P_j=D$. 由于 $D<P_i$, 于是 $D<N_{P_i}(D)=H_i\leq P_i$ 由于 $D<P_j$, 于是 $D<N_{P_j}(D)=H_j\leq P_j$. 这时有 $H\trianglelefteq<H_i,H_j>=T$.

1) 若 T 是 p-子群, 则存在 G 的 Sylow p-子群 P_k 使得 $T\leq P_k$, 此时 $P_k\bigcap P_i\geq H_i>D\Rightarrow P_k=P_i$, 同理 $P_k=P_j\Rightarrow P_i=P_j$, 矛盾, 于是只能是情况 2).

2) $|T|=p^tq$. 令 Q 是 T 的 q 阶子群. 可以证明 $G=QP_i$, 令 $N=D^G$, 则 $N\trianglelefteq G$, N 是 G 的真子群，就证完了. □

这个定理还可推广作

Theorem 2.11 (Burnside) p,q 是素数，a,b 是正整数，则 p^aq^b 阶群必为可解群.

在这里我们略去证明，以后学了表示论再证.

Theorem 2.12 (Feit-Thompson) 奇数阶群必为可解群

此定理证明长达 150 页，一般避免使用此定理.

借助上定理，我们可以证明

Theorem 2.13 $|G|=2n$, 其中 n 是奇数，则 G 是可解群

Chapter 3
置换群

3.1 基本概念

Remark 3.1 在本节中我们只考虑有限集合上的置换，于是可以假定 $\Omega = \{1, 2, \cdots, n\}$.

考虑 G 是集合 Ω 上的置换群，$G \leq S_\Omega$，则每一个群元素就是集合 Ω 上的一个置换. 记 $i \in \Omega$ 在 G 中元素 g 的像是 i^g (这点类似于我们群作用中的记号，事实上 G 也可以看作是一个 Ω 上的群作用). 下面我们列举一些记号和定义

(1) 对于 $\Delta \subseteq \Omega$, 规定

$$\Delta^g = \{\delta^g | \delta \in \Delta\}$$

(2) 对于 $i, j \in \Omega$, 若 $\exists g \in G$, $i^g = j$, 则记作 $i \sim j$.

(3) "~" 是 Ω 上的等价关系，将 Ω 划分做数个等价类，每个等价类称一条轨道

$$i^G = \{i^g | g \in G\}$$

表示一条包含 i 的轨道.

(4) 若 G 在 Ω 上只有一条轨道，称其在 Ω 上是传递的. 或说 G 的传递置换的.

(5) $G \subseteq S_\Omega$, $\Delta \subseteq \Omega$，规定

$$G_{(\Delta)} = \{g \in G | \forall \delta \in \Delta, \delta^g = \delta\}$$

称作 G 对 Δ 的点型稳定子群.

(6) $G \subseteq S_\Omega$, $\Delta \subseteq \Omega$，规定

$$G_{\{\Delta\}} = \{g \in G | \Delta^g = \Delta\}$$

称作 G 对 Δ 的集型稳定子群.

Proposition 3.1 *两个稳定子群的关系:* $G_{(\Delta)} \trianglelefteq G_{\{\Delta\}}$

(7) 设 G 是 Ω 上的非传递群，取其中一条轨道 O, $\forall g \in G$, 以 g^O 记 g 在 O 上诱导的置换. 令

$$G^O = \left\{ g^O | g \in G \right\}$$

称 G^O 是 G 在 O 上的传递成分. 一个成分是忠实的，如果 $G_{(O)} = \{e\}$

(8) 若 $\exists i \in \Omega$, $\forall g \in G$, $i^g = i$, 则称 i 是一个 G 的不动点，以 $fix_\Omega(G)$ 表示所有 G 不动点集合. 特别的，$fix_\Omega(g)$ 表示 g 固定的点.

(9) 称 $|\Omega| - |fix_\Omega(G)|$ 称作 G 的级，表示 G 实际能够变换的元素个数，记作 $degG$. 类似的 $degg$ 表示 g 能够变动的元素个数. 称

$$min\{deg\ g | g \in G, g \neq e\}$$

是 G 的最小级或者最小次数.

Proposition 3.2 *$G \leq S_\Omega$ 是传递置换群. $\alpha \in \Omega$, $\Phi = fix_\Omega(G_\alpha)$, $N = N_G(G_\alpha)$. 则 N 在 Φ 上传递. 特别的，G_α 的不动点数是 $[N : G_\alpha]$.*

Proof 首先 $\alpha \in \Phi$, 于是 N 在 Φ 上传递当且仅当 $\Phi = \{\alpha^n | n \in N\}$.

(i) $\forall n \in N$, $n^{-1} G_\alpha n = G_\alpha$. 于是

$$\alpha^n = \alpha^{G_\alpha n} = \alpha^{nG_\alpha}$$

说明 $\alpha^n \in \Phi$.

(ii) $\forall \beta \in \Phi$, 由于 G 在 Ω 上传递，于是 $\exists g \in G$, $\beta^g = \alpha$. 于是

$$\beta = \beta^{G_\alpha} = \alpha^{g^{-1} G_\alpha}$$
$$\beta = \alpha^{g^{-1}} = \alpha^{G_\alpha g^{-1}}$$

说明

$$\alpha^{g^{-1} G_\alpha g} = \alpha^{G_\alpha},\ g \in N$$

于是 $\beta \in \{\alpha^n | n \in N\}$.

综上说明 $\Phi = \{\alpha^n | n \in N\}$, 即 N 在 Φ 上传递. 于是 $|fix_\Omega(G_\alpha)| = |\Phi| = |\{\alpha^n | n \in N\}$ 由于 $\alpha^{n_1} = \alpha^{n_2} \iff n_1 n_2^{-1} \in G_\alpha$, 于是 $|\Phi| = [N : G_\alpha]$. □

3.2 置换群的正则性