西罗定理

2024 年 5 月 12 日

目录

现在，我们把目标转向非阿贝尔群，由于在上一章使用的是加法，则现在我们继续把符号用回乘法。

西罗定理告诉了我们一些类似于有限阿贝尔群的初等分解的一些类比。

回想一下单群的定义，若$G \neq 1$且G除了$\{1\}$和自身之外不存在其他的正规子群。对于阿贝尔群，它是单群意味着其是某个阶为素数p的循环群。由拉格朗日定理，对$n \geq 5$，A_n是非阿贝尔单群。实际上，A_5是最小的非阿贝尔单群。问题是，我们如何证明阶小于$60 =\mid A_5 \mid$的群不是单的呢？下面的这个习题告诉了我们一些东西：若G是一个阶为$\mid G \mid = mp$的群，其中p是素数，$1 < m < p$，则G不是单群。当我们去除了一些素数的方幂后，剩下的有可能为单群的阶的数是：

$$12\ \ 18\ \ 24\ \ 30\ \ 36\ \ 40\ \ 45\ \ 48\ \ 50\ \ 54\ \ 56$$

但对于这个习题的解决需要用到柯西定理，柯西定理说：G有p阶的子群。我们将看到，若G有一个阶是p^l而不是p的子群我们将看到，若G有一个阶为p^l而不是p的群，其p^l 是整除$\mid G \mid$的p的最高次幂。则我们可以推广上述习题，那么剩下的候选就只有 $30, 40, 56$。这是之后的一个定理-西罗定理。西罗证明了对每个有限群G及任意一个素数p，若p^l是能整除$\mid G \mid$的最大的p的方幂，则G也有一个阶为p^l的子群。

0.1 定义：

设p是素数，有限群G的西罗$p-$子群指的是G的最大的$p-$子群P 最大的意思是，若Q是G的一个$p-$子群且$P \leq Q$，则$P = Q$。

我们现在来证明一个事情，若S是一个G的任一$p-$子群，则存在一个包含S的西罗$p-$子群。否则S本身就是这么一个西罗子群。

0.1.1 例子

令G是阶为$\mid G \mid = p^e m$的有限群，其中p是素数且$p \nmid m$。我们来证明若存在阶为p^e的子群P，则P是一个G的西罗$p-$子群。若Q是一个$p-$子群使得$P \leq Q \leq G$，则$\mid P \mid = p^e \mid\mid Q \mid$。但是，若$\mid Q \mid = p^k$，则$p^k \mid p^e m$和$k \leq e$。因此$\mid Q \mid = p^e$使得$Q = P$

这个章节会使用很多群作用的东西。我们先来回顾一些定义。

0.2 定义：共轭

若H是G的子群，则H的共轭指的是G的子群具有如下形状：

$$aHa^{-1} = \{aha^{-1} : h \in H\}$$

其中$a \in G$

共轭子群是同构的，若$H \leq G$，则$h \to aha^{-1}$是单射同态$H \to G$使得象是aHa^{-1}。反之不成立。四元群V包含几个阶为2的子群。当然它们都是同构的，但不可能是共轭的，原因在于V是阿贝尔群。另一方面，在S_2中，所有2阶子群都是共轭的，因为$\langle(1\ 3)\rangle = g\langle(1\ 2)g^{-1}\rangle$，其中$g = (2\ 3)$

接下来我们讨论一下轨道和稳定子的概念。

0.3 定义：群作用

设X是一个集合，G是一个群，称G作用在X上，若对每一个$g \in G$存在函数$\alpha_g : X \to X$使得

1. $\alpha_g \circ \alpha_h = \alpha_{gh}$对所有$g, h \in G$
2. $\alpha_1 = 1_X$是恒等函数。

0.4 定义：轨道

若G作用在X上且$x \in X$，则x的轨道我们记为$\mathcal{O}(x)$，它是X的子集

$$\mathcal{O}(x) = \{\alpha_g(x) : g \in G\} \subseteq X$$

x的稳定化子记为G_x，它是G的子群

$$G_x = \{g \in G : \alpha_g(x) = x\} \leq G$$

一个群通过共轭作用在其所有子群构成的集合$X = \mathbf{Sub}(G)$上；若$g \in G$，则g的作用是$\alpha_g(H) = gHg^{-1}$，其中$H \leq G$，子群H的轨道由它所有共轭组成。H的稳定化子是$\{g \in G : gHg^{-1}\}$，则它的子群有一个称呼。

0.5 定义：正规化子

若H是群G的子群，则G中的正规化子H是子群

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

由定义，$hHh^{-1} = H$可以证明$H < N_G(H)$，然后$g \in G$使得$gHg^{-1} = H$可知H其是正规子群

0.6 命题

若H是有限群G的子群，则H在G中共轭的数量是$[G : N_G(H)]$

证明： 我们引入如下定理：

> 若G在集合X上作用且$x \in X$，则
>
> $$\mid \mathcal{O}(x) \mid = [G : G_x]$$
>
> 其中G_x是稳定化子。

而共轭是稳定化子的一个特殊的例子。再利用上述定义，做$G_x = N_G(H)$的替换，Q.E.D

0.7 引理

令P是有限群G的西罗$p-$子群。

1. 每个P的共轭也是G的西罗$p-$子群。
2. $\mid N_G(P)/P \mid$与p互素。
3. 若$g \in G$的阶为某个素数p的幂次且$gPg^{-1} = P$，则$g \in P$

证明1： 若$g \in G$，则gPg^{-1}是G的$p-$子群，因为共轭的阶是相同的。如果不是最大的，则存在$p-$群Q使得$gPg^{-1} < Q$。因此$P < g^{-1}Qg$与P是西罗p群矛盾。

证明2： 若p整除$\mid N_G(P)/P$，则柯西定理告诉我们$N_G(P)/P$包含一个阶为p的元gP，藉此有$N_G(P)/P$包含一个阶为p的循环子群$S^* = \langle gP \rangle$。由对应定理就有一个子群S使得$P \leq S \leq N_G(P)$使得$S/P \cong S^*$。那么S是一个$N_G(P)$上的p群，且S包含P，那么就与P是最大的矛盾。因此p不整除$\mid N_G(P)/P \mid$

证明3： 由正规化子的定义，$g \in N_G(P)$。若$g \notin P$，则陪集gP是$N_G(P)/P$中一个非平凡元素且阶为p的某方幂、结合命题2和拉格朗日定理可知矛盾。所以$g \in P$

0.8 定理(Sylow)

令G是阶为$p^e m$的有限群，其中p是素数且$p \neq m$，再令P是G的西罗$p-$子群。

1. 每个西罗$p-$子群是P的共轭
2. 若有r个西罗$p-$子群，则r是$\mid G \mid /p^e$的因子，且

$$r \equiv 1 \mod p$$

证明： 令$X = \{P_1, \cdots, P_r\}$是P是所有共轭的集合。其中我们把P记为P_1。若Q是任意G的西罗$p-$子群，如果Q通过共轭作用在X上。则

$$\alpha_a(P_i) = \alpha_a(g_i P g^{-1}) = (ag_i)P(ag_i)^{-1} \in X$$

由于轨道的并构成Q，所以任一轨道都是$\mid Q \mid$的因子。则这些轨道的阶都为p的某个幂次。如果有一轨道阶为1，那么这里就有某个P_i使得$aP_i a^{-1} = P_i$对所有$a \in Q$成立。利用引理0.7，则$a \in P_i$对所有$a \in Q$成立。因此$Q \leq P_i$，但是Q是西罗$p-$子群。因此$Q = P_i$，特别的若$Q = P_i$，则所有轨道都是p的方幂，除了这个轨道为1的。因此$\mid X \mid = r \equiv 1 \mod p$

其次，假设有一西罗$p-$子群Q，它不是和P共轭的，因此对任意i，$Q \neq P_i$。我们再一次把Q作用在X上，并再次设若有一轨道的阶为1，记为$\{P_j\}$。就跟我们刚才说的一样，这里可以推出$Q = P_i$。这和我们一开始的假设$Q \notin X$矛盾。因此，若不存在肠胃1的轨道，这就是说每个轨道的长度都是p的方幂，从而$\mid X \mid = r \mid p$有$r \equiv 0 \mod p$，这与r, p互素矛盾。这种Q是不存在的，所以所有的西罗$p-$子群是与P共轭的，我们有$r = [G : N_G(P)]$，所以$r \mid\mid G \mid = p^e m$，但$(r, p) = 1$，所以有$r \mid\mid G \mid /p^e$

0.9 推论

有限群G对某素数p有唯一的西罗$p-$子群P当且仅当$P \lhd G$

证明： 我们设G有唯一的西罗$p-$子群。对每个$a \in G$，它的共轭aPa^{-1}也是西罗$p-$子群。因为唯一，则$aPa^{-1} = P$对每个$a \in G$成立，因此$P \lhd G$

反之，设$P \lhd G$是西罗$p-$子群，若Q是任意的西罗$p-$子群，则$Q = aPa^{-1}$对某个$a \in G$成立。但$aPa^{-1} = P$，但P是正规子群，有$aPa^{-1} = P$，所以$Q = P$

0.10 定理(Sylow)

若G是阶为$p^e m$的有限群，其中p是素数且$p \nmid m$，则每个G的西罗$p-$子群的阶是p^e

证明： 我们首先证明$p \nmid [G : P]$。注意

$$[G : P] = [G : N_G(P)][N_G(P) : P]^{[1]}$$

对于上述第一个因子，$[G : N_G(P)] = r$是P在G中的共轭的数量,我们知道$r \equiv 1 \mod p$，所以p不整除$[G : N_G(P)]$。而第二个因子$[N_G(P) : P] = \mid N_G(P)/P \mid$，由引理0.7，$p \nmid [N_G(P) : P]$。

现在$\mid P \mid = p^k$对某个$k \leq e$成立。那么

$$[G : P] = \mid G \mid / \mid P \mid = p^e m/p^k = p^{e-k}m$$

由于$p \nmid [G : P]$，所以上面的式子成立当且仅当$e = k$，注意$p \nmid m$。因此$\mid P \mid = p^e$

0.10.1 例子

1. 利用推论0.9，我们知道阿贝尔群G的西罗$p-$子群其一个$p-$准素分支。由于G的子群是正规的，G对每个素数p就有唯一的西罗p子群

[1]注意，由定义可知$P \lhd N_G(P)$，其次这是我在《子群与拉格朗日》第一道习题就证明完的定理。

0.11 西罗定理(第二种)

令G是阶为$p^e m$的有限群，其中p是素数且$p \nmid m$，则G有阶为p^e的子群。

证明： 若X是G中所有p^e个元素的子集族，则$|X| = \binom{n}{p^e}$，但，$p \nmid \binom{n}{p^e}$，因为分子分母有同样的因子去掉剩下p不整除的。现在G作用在X上，定义$\alpha_g(B) = gB$，其中$g \in G, B \in X$，而$gB = \{gb : b \in B\}$。对每个$B \in X$，若$p \mid\mid \mathcal{O}(B)$，则$p$就是$|X|$的因子。但由于轨道构成$X$的无交并，因此$p \nmid\mid X |$就有$p \nmid\mid \mathcal{O}(B)|$，也就是说，这里就存在一个集合元素的数量为$p^e$且$p \nmid\mid \mathcal{O}(x)$的集合。不妨记为$|B| = p^e$。然后我们设$G_B$是集合$B$的稳定化子，由于$[G : G_B] = |\mathcal{O}(B)| \Rightarrow |G| = |G_B| \mid\mid \mathcal{O}(x)|$，因为$p^e \mid |G|$但$p \nmid\mid \mathcal{O}(x)|$，利用欧几里得引理就有$p^e \mid\mid |G_B|$。就有$p^e \leq |G_B|$

反过来，选择$b \in B$定义函数$\tau : G_B \to B$由$g \to gB$定义。对$g \in G_B$，则$\tau(g) = gB \in gB = B$。由于g在B的稳定化子G_B中，若$g, h \in G_B$且$h \neq g$，则$\tau(h) = hb \neq gb = \tau(g)$。从而$\tau$是单射，因此$|G_B| \leq |B| = p^e$，从而$G_B$就是一个阶为$p^e$的子群

0.12 引理

这里不存在一阶为$|G| = p^e m$的简单群G，其中p是素数且$m > 1$，$p \nmid m$和$p^e \nmid (m-1)!$

证明： 设这样的简单群G是存在的，由西罗定理，G包含一个阶为p^e的群P。可以得到P在G中的指数为m。利用凯莱定理，这里存在一个同态$\varphi : G \to S_m$成立。并且$\ker\varphi \leq P$由于G是单群，他没有其他的正规子群，因此$\ker\varphi = \{1\}$，所以映射是单射。利用鸽笼定理，我们就有$G \cong \varphi(G) \leq S_m$。利用拉格朗日定理，$p^e m \mid m!$，就有$p^e \mid (m-1)!$矛盾。

0.13 命题

不存在阶小于60的非阿贝尔单群。

证明： 若p是素数，则我们引入一个习题说明对每个$|G| > p$的$p-$群G不是单群。

首先，引入H为G的$p-$子群，则$[G:H]=[N_G(H):H]$
定理：有限$p-$群G是单群当且仅当$|\ G\ |=p$

证明： 设$|\ G\ |=p^e$，$e\geq 1$，由于G是单的，那么G的正规子群只有$\{1\}$和G。我们通过对$e\geq 1$进行归纳证明每个p^i阶的子群都是一个p^{i+1}阶子群的正规子群，由柯西定理，那么就有一个p阶子群。设$|\ H\ |=p^i$，$i<e$,那么$p\mid [G:H]$。定义$N_G(H)$，那么H就是其的正规子群，存在商群$N_G(H)/H$。由归纳法，$N_G(H)/H$存在一个p阶子群K^*。再利用对应定理，这里就存在一个包含H的子群L存在使得$[L:H]=p$，因此我们得到了一个p^{i+1}的子群L。证明完毕。

[2] 我们检查2到59阶的群，利用上面的定理，去除素数阶幂和不是形如p^em的分解，那么剩下$n=30,40,56$。利用定理0.9，

我们设存在阶为30的单群，令P是西罗$5-$子群，则$|\ P\ |=5$，P的共轭个数r_5为$30/5=6$，这是利用定理0.8的得到的并且$r_5\equiv 1\mod 5$，又因为$r_5\neq 1$，否则$P\lhd G$。所以$r_5=6$。由拉格朗日定理，这些群的交集是$\{1\}$，其次，这些群里面都含有4个非单位元，所以就有$4\times 6-24$个非单位元。然后我们找关于西罗$3-$子群的。容易得到$30/3=10$，为了满足$r\equiv 1\mod 3$，r只能是10，非单位元一共有20个，加起来是$20+24>|\ G\ |=30$，利用定理0.9这是一个矛盾。

然后我们来数40的。令P是西罗$5-$子群，那么$r_5\mid 40/5$并且满足$r_5\equiv 1\mod 5$。那么只有$r_5=1$，利用定理0.9$P\lhd G$，不存在这种单群

最后，我们设存在阶为56的单群。我们取P是西罗$7-$子群，那么$56/7$，满足$r_7\mid 56/7$且$r_7\equiv 1\mod 7$只有$r_7=8$，如法炮制，非单位元只有49个，除非$Q\lhd G$，否则还有一些西罗$2-$子群，这样子又超过了$|\ G\ |$，因此阶为56的单群不存在。

0.14 命题

若G是有限群，设p是素数且$p^k\ ||\ G\ |$，则G存在阶为p^k的子群

证明： 我们已经知道阶为p^e的群存在p^k的群。令$|\ G\ |=p^em$，则p^e阶的群

[2]这是西罗第一定理的内容

是一个G的西罗$p-$子群。综上所述，G存在一个阶为p^k的子群。

0.15 定义：严格上三角矩阵

设k是域，k上的一个$n\times n$单位三角矩阵指的是主对角线上元素均为1的上三角矩阵。用$\mathrm{UT}(n,k)$来表示k上所有$n\times n$的单位三角矩阵构成的集合。

0.16 命题：

对任意域k，$\mathrm{UT}(n,k)$是$\mathrm{GL}(n,k)$的子群。

证明： 若$A\in \mathrm{UT}(n,k)$，那么$A=I+N$，其中N是一个严格的上三角。那么N就是一个主对角线为0的矩阵，注意严格上三角的矩阵和还有积都是严格上三角。

令$e_1,\cdots,e_n$是k^n的一组标准基，定义$T:k^n\to k^n$由函数$T(e_i)=Ne_i$给出。其中e_i我们看成是列向量。那么e_i满足下列方程

$$T(e_1)=0 \quad 且 \quad T(e_{i+1})\in\langle e_1,\cdots,e_i\rangle$$

现在我们开始对i归纳，由归纳假设我们有$T^i(e_j)=N^ie_j=0$对每个$j\le i$成立。则$A=I+N$，其中$N^n=0$

我们现在证明$\mathrm{UT}(n,k)$是$\mathrm{GL}(n,k)$的子群。若A是单位三角的，则它是非退化的，类似于$1/(1+x)$的幂级数展开，我们来看$B=I-N+N^2-N^3+\cdots$是不是$A=I+N$的逆矩阵，做$BA=\left(\sum_{i=1}^{n-1}(-1)^{n-1}N\right)(I+N)$，左边是$\sum_{i=1}^{n-1}(-1)^{n-1}N$，右边是$\sum_{i=2}^{n-1}(-1)^{n-1}N$，注意$N^n=0$，那么就剩下了$I$，因此$BA=I$成立。所以$A$非退化，其次，由于$B$是严格上三角的，所以$A^{-1}$也是严格上三角的。最后，$(I+N)(I+M)=I+(N+M+NM)$也是单位三角形，证毕

0.17 命题：

令$q=p^e$，其中p是素数，对每个$n\ge 2$，$\mathrm{UT(n,\mathbb{F}_q)}$是阶为$q^{n(n-1)/2}$的$p-$子群

证明： 主对角线外的元素刚刚好是$1/2(n^2-n)=n(n-1)/2$个，每个元素都可以是F_q中任一一个元素，那么$n\times n$的单位三角矩阵恰好就有$q^{n(n-1)/2}$个。

0.18 命题

若p是奇素数，则这里存在阶为p^3且满足$x^p=1, x\in G$的非阿贝尔群G

证明： 若$G=\mathrm{UT}(3,\mathbb{F}_p)$，则$|\ G\ |=p^3$，若$A\in G$，则$A=I+N$，其中$N^3=0$。因此$N^p=0$对所有$p\geq 3$成立。再验证一下，$IN=NI=N$，二项式定理给出$A^p=(I+N)^p=I^p+N^p=I$。证毕。

0.19 定理：

令$\mathbb{F}_q$是有q个元的有限域，那么

$$|\ \mathrm{GL}(n,\mathbb{F}_q)\ |=(q^n-1)(q^n-q)(q^n-q^2)\cdots(q^n-q^{n-1})$$

证明： 令V是F_q上的n维线性空间。则这里存在一个双射Φ: $\mathrm{GL}(n,\mathbb{F}_q)\to\mathcal{B}$，其中$\mathcal{B}$是$V$的所有基的集合。我们一次性选取$V$的基$e_1,\cdots,e_n$。若$T\in\in\mathrm{GL}(n,\mathbb{F}_q)$,。然后我们定义$\Phi(T)=Te_1,\cdots,Te_n$，由于$T$非退化，那么$T$将一个基映射到一个基，因此$\Phi(T)\in\mathcal{B}$由于它是非退化的，因此存在唯一的逆的线性变换$S$使得$S(Te_i)=e_i$，综上所述，$\Phi$是双射。

V中有q^n个向量，故v_1存在q^n-1种选择，由于v_1选择了一个元，那么v_2就不能选择v_1张成的元了，因此可能的选择就剩下q^n-q个。以此类推在$v_1,\cdots,v_t$之后，v_{t+1}只能选择前面没选择过的，简单的归纳之后。我们就得出结论

$$|\ \mathrm{GL}(n,\mathrm{F}_q)\ |=(q^n-1)(q^n-q)(q^n-q^2)\cdots(q^n-q^{n-1})$$

0.20 推论

$$|\ \mathrm{GL}(n,\mathrm{F}_q)\ |=q^{n(n-1)/2}(q^n-1)(q^{n-1}-1)\cdots(q^2-1)(q-1)$$

证明： 很简单，注意$q^n-q^2=q^2(q^{n-2-1})$，我们只需要简单的提取公因式，并且注意提取完后就有$q^{1+2+\cdots+(n-1)}$和$1+2+\cdots+(n-1)=\frac{1}{2}n(n-1)$

0.21 定理：

若p是素数且$q = p^m$，则$\mathrm{UT}(n, \mathbb{F}_q)$是$\mathrm{GL}(n, \mathbb{F}_q)$的西罗$p$子群。

证明： 利用推论0.20我们可以知道p幂次最高的是$p^{n(n-1)/2}$。然后利用0.17，我们就证明完了。

0.22 推论：

若p是素数，则每一个有限$p-$群G同构于某三角单位群$\mathrm{UT}(m, \mathbb{F}_p)$的一个子群，其中$\mid G \mid = m$

证明： 我们首先对每个$m \geq 1$，对成群S_m都可以嵌入$\mathrm{GL}(m, k)$中，其中k是域。设V是k上的m维线性空间，基是$v_1, \cdots, v_m$。定义$\varphi : S_m \to \mathrm{GL}(V)$由函数$\sigma \to T_\sigma$定义。其中$T_\sigma : v_i \to v_{\sigma(i)}$[3]，我们可以快速的检验这是一个单同态。

利用凯莱定理，我们知道G可以被嵌入到S_G中，因此G就可以被嵌入到$\mathrm{GL}(m, \mathbb{F}_p)$，其中$\mid G \mid = m$。由于每个$p-$子群被包含在西罗$p$子群内，因此$G \subseteq \mathrm{UT}(V)$。其次，由于所有西罗$p-$子群是共轭的，那么就存在$a \in \mathrm{GL}(m, \mathbb{F}_p)$。使得$P = a(\mathrm{UT}(m, \mathbb{F}_p))a^{-1}$，因此这样子的群总是能找到的。那么

$$G \cong aGa^{-1} \leq a^{-1}Pa \leq \mathrm{UT}(m, \mathbb{F}_p)$$

[3]其实就是单位矩阵做行列互换。