抽象代数(群论)

数62 谭泽睿

2017 年 11 月 11 日

Abstract

内容概要：

- 群作用的概念理解
- 三个典型重要的群作用：正则表示，诱导表示，共轭作用
- Sylow定理的常见用法
- 对应定理，一些其它的东西
- 一些作业题，常见坑

Contents

1 群作用

群本质上是对称群/变换群/作用群的抽象结构。所谓群的作用，就是将抽象的群的元素实现为具体的变换/作用。比方说，循环群这种对称结构如何作用在各种对象上？我们知道，它可以实现为正多边形的旋转，即有群同态

$$\mathbb{Z}_n \to \{正n边形的旋转群\}$$

其中$\mathbb{Z}_n$的生成元被映射到某个单位旋转。也可以这样描述这种作用：将正n边形的旋转理解为顶点集$\{1, 2, \ldots, n\}$上的一个置换，从而得到(单)同态

$$\mathbb{Z}_n \to S_n$$

其中$\mathbb{Z}_n$的生成元被映射到轮换$(123 \ldots n)$.

我们研究群的尽可能广泛的作用，就是考虑群G到尽可能大的一类变换群的同态。一般考虑的大的一类变换群主要是两类：置换群和矩阵群。研究到矩阵群的同态的是群的线性表示论(简称群表示论)。我们研究群在集合上的作用时，就主要是研究的到置换群的同态。以$\mathrm{Sym}(X)$或$A(X)$或S_X 记集合X 上的所有置换，即所有单满映射，(**徐帆老师的记号是**$A(X)$,但$\mathrm{Sym}(X)$是标准的记号), 称之为X 的对称群。那么我们称群G 在集合X 上的一个作用就是指一个同态

$$\rho : G \to \mathrm{Sym}(X).$$

这也称为群G的一个置换表示，也就是说，$\rho(g)$将成为集合X上的一个变换(置换)，单满射，即

$$\rho(g) : X \to X.$$

这个变换可以作用在$x \in X$ 上得到$\rho(g)(x)$。给定了同态ρ后不妨把G中元素想象为一堆作用在X上的“算子”，直接用$g * x$或gx表示$\rho(g)(x)$.

我们先来复习群作用基本的术语。如果ρ是单同态，就称这个作用是**忠实的(faithful)**。
对于$x \in X$，集合

$$Gx = \{gx | g \in G\}$$

称为x的**轨道(Orbit)**。容易证明，a, b属于同一个轨道，也就是存在g使得$a = gb$,是一个等价关系，这一点与G是群密切相关。如此而来，X中的元素划分为一些不相交的等价类的并，也就是不相交的轨道的并。如果X只有一个轨道，我们就称这个作用是**传递的(transitive)**，这也就是说，任何一个x 都可以被G中的某一个作用映到任何一个给定的y.

定义1. 给定了群G在集合X上的作用，我们用

$$\mathrm{Stab}(x) = \{g \in G | gx = x\}$$

记G中所有保持x不动的变换。这是G的一个子群，称之为x的**稳定化子(Stabilizer)**.

既然$\mathrm{Stab}(x)$是个子群，我们就可以作陪集分解

$$G = \bigcup_i g_i \mathrm{Stab}(x)$$

其中，每个陪集在x上的作用全部一致，都是$g_i x$.并且不同的陪集显然给出在x上不同的作用，否则$ax = bx \Leftrightarrow a^{-1}b \in \mathrm{Stab}(x) \Leftrightarrow a\mathrm{Stab}(x) = b\mathrm{Stab}(x)$.我们立马得到了如下简单而基本的轨道公式(计算轨道长度)

定理2 (轨道公式)**.**

$$|Gx| = [G : \mathrm{Stab}(x)]$$

由于X划分为一些轨道，我们以x_i记每个轨道的代表元素，则显然必须有

$$|X| = \sum |\text{轨道}| = \sum_i [G : \mathrm{Stab}(x_i)].$$

轨道公式虽然简单，但必须熟练掌握。我们举一个计算对称群阶数的例子：

例1. *我们计算正四面体群的对称群$|G|$(就是正四面体上的刚体变换群).取正四面体的某一个顶点x,由于群作用是传递的，$|Gx| = 4$.而G中有6个变换保持x 不变，三个以x为轴的旋转变换和3个反射面经过x的反射变换。故*

$$|G| = |Gx||\mathrm{Stab}(x)| = 4 \times 6 = 24.$$

另外，我们马上能得到如下计算轨道个数的公式

定理3 (Burnside)**.** *轨道的个数N有如下公式*

$$N = \frac{1}{|G|} \sum_{g \in G} (\text{被}g\text{固定的元素}x \in X\text{的个数}).$$

$$\begin{aligned} N &= \sum_{\text{轨道}} 1 = \sum_{\text{轨道}} \left(\sum_{x \in \text{轨道}} \frac{1}{|Gx|} \right) \\ &= \sum_{x \in X} \frac{1}{|Gx|} = \sum_{x \in X} \frac{|\mathrm{Stab}(x)|}{|G|} \\ &= \frac{1}{|G|} \sum_{x \in X} \sum_{g \in G} 1_{gx=x} = \frac{1}{|G|} \sum_{g \in G} \sum_{x \in X} 1_{gx=x}. \end{aligned}$$

1.1 表示/作用的核

给定一个作用，我们来求$\ker\rho$，这一般是重要的，因为这样，由同态基本定理，$G/\ker\rho$将会同构于变换群$\mathrm{Sym}(X)$的某个子群。

$\ker\rho$是什么呢？就是那些固定所有元素的g,因此

$$\ker\rho=\bigcap_{x\in X}\mathrm{Stab}(x).$$

如果这个作用是传递的，就有

$$\ker\rho=\bigcap_{g\in G}\mathrm{Stab}(gx).$$

$\mathrm{Stab}(x)$与$\mathrm{Stab}(gx)$有自然的关系。固定x的那些变换，稍微改一改，也可以拿去固定gx.这只需要先复合一个g^{-1},再施加$\mathrm{Stab}(x)$,再复合g.换而言之我们发现

$$g\mathrm{Stab}(x)g^{-1}\subset\mathrm{Stab}(gx).$$

反过来一样有

$$g^{-1}\mathrm{Stab}(gx)g\subset\mathrm{Stab}(x).$$

因此我们发现

$$\mathrm{Stab}(gx)=g\mathrm{Stab}(x)g^{-1}.$$

因而，在作用是传递的时，有

$$\ker\rho=\bigcap_{g\in G}g\mathrm{Stab}(x)g^{-1}.$$

这是一个正规子群。这事实上也启示我们如下平凡的命题：设$H\leq G$，则

$$\bigcap_{g\in G}gHg^{-1}\triangleleft G$$

群不光可以作用在其它对象X上，它很多时候可以自然地作用在自己的某些结构上。在群论的研究中，这是一种极为重要，朴素而强大的方法。我们将重点讨论以下几个典型的群作用

- 在元素上的共轭作用
- 在子群上的共轭作用
- (左)正则表示
- (左)诱导表示

1.2 正则表示

群G以(左)乘法作用在群G上，也即

$$\rho: G \to \mathrm{Sym}(G)$$
$$g \mapsto (a \mapsto ga)$$

$$\rho(g)(a) := ga.$$

即将g以左乘法自然地视为一个集合G上的置换$\rho(g)$.因为G是群，这显然是一个忠实，传递的表示。我们马上得出Cayley定理：每个群都同构于某个置换群的子群。这看起来似乎弱智无比，但是就是这样朴素的观点我们可以得到非平凡的结论，我们举一个例子。

命题4. *设G是$4k+2$阶群，那么它一定有一个指数为2的正规子群。(因而不是单群)*

Proof. 考虑群的左正则作用

$$\rho: G \to \mathrm{Sym}(G)$$

由于这是忠实表示，我们可以把G与$\rho(G)$等同起来。那么，每个$\rho(g)$都是一个G上的置换，由于群乘法具有逆的原因，除非$g=1$,这个置换不可能固定任何群中的元素($ga = a \Leftrightarrow g = 1.$) 因此可以将$\rho(g)$写为一些长度大于1的不相交轮换的乘积。现取$g$为群中的一个二阶元素，由前面的习题我们知道在偶数阶群中这是一定可以取到的。因此，$\rho(g)$分解成$2n+1$个不相交的对换的乘积，因而是奇置换。于是我们证明了G中有奇置换，因而G中的所有偶置换构成一个指数为2 的正规子群。 □

1.3 诱导表示

给定了群G的一个子群H后，有(左)陪集集合G/H，群G可以以左乘法自然地作用在G/H上。

$$\rho: G \to \mathrm{Sym}(G/H)$$
$$g \mapsto (aH \mapsto gaH)$$

这称为(左)诱导表示。它显然是传递的。事实上，诱导表示又称为传递置换表示，因为从而它的核是

$$\ker \rho = \bigcap_{g \in G} gHg^{-1}$$

并注意(重要!)事实上有$\ker\rho \triangleleft H$.运用这个表示可以得到很多厉害(其实很简单)的结论。

例2. *单群不可能有太大的子群：若G是大于3阶的单群，$H \leq G$,证明$[G:H] \geq 4$.*

Proof. 考虑G在陪集集合G/H上的诱导表示

$$\rho : G \to \mathrm{Sym}(G/H)$$

由于G是单群，而这个作用是传递的，必须有$\ker\rho = e$.从而G同构于$S_{[G:H]}$的子群，从而$[G:H]! \geq |G| \geq 4$,故$[G:H] \geq 3$.但是S_3中的单子群只有2阶和3阶的，不可能是G.因而只能有$[G:H] \geq 4$. □

例3. *设$|G| = mp, 1 < m < p$,其中p是素数。证明$\mathbb{Z}_p \triangleleft G$.*

这个命题可以由Sylow定理得到，我们这里展示一个用群的诱导表示的证明：

Proof. 柯西定理表明有p阶元素a，记$H = \mathbb{Z}_p = \langle a \rangle$，考虑$G$在陪集集合$G/H$上的诱导表示

$$\rho : G \to \mathrm{Sym}(G/H) \cong S_m$$

由$\ker\rho \leq H$, $\ker\rho = e$或H.前者是不可能的，否则由同态基本定理有$p|m!$，但事实上$m < p$. □

例4. *设H是无限群G的一个具有有限指数的真子群，那么G一定有一个具有有限指数的真正规子群。*

Proof. 考虑G在陪集G/H上的诱导表示

$$\rho : G \to \mathrm{Sym}(G/H)$$

由于$[G:\ker\rho] \leq |\mathrm{Sym}(G/H)| = [G:H]!$是有限的，我们完成了命题的证明。 □

命题5. *设p是$|G|$最小的素因子，那么若$H \leq G$且$[G:H] = p$则有$H \triangleleft G$.*

Proof. 考虑在陪集集合G/H上的诱导表示$\rho : G \to \mathrm{Sym}(G/H)$，由于有$G/\ker\rho$同构于$\mathrm{Sym}(G/H)$的一个子群，因而必须有$|G/\ker\rho|$是$[G:H]!$的因数。现在由于$\ker\rho \leq H$,我们有

$$[G:\ker\rho] = [G:H][H:\ker\rho]$$

是$[G:H]=p$的倍数。由于p是$|G|$的最小素因子，我们知道$[H:\ker\rho]$是1或p的倍数。若不是1，必有$p^2|p!$，这不可能，故

$$H=\ker\rho\lhd G.$$

□

1.4 循环群的作用

我们看一个群作用的强大威力的例子，我们证明如下的柯西定理：

定理6 (Cauchy). 设p是$|G|$的一个素因数，则G中有p阶元素。

在开始看证明之前我们来理解一下思路。$p=2$的情形已经作为一道作业题做过了，还记得做法吗？大家的做法，估计就是对G中的元素配对，g和g^{-1}配一对，二阶元素g和g^{-1}是相同的，就无法配对，最后因为群的阶数是2的倍数，配了对的元素个数也是2的倍数，我们得出满足$x^2=1$的元素个数有偶数个。由于$1^2=1$，我们知道一定有二阶元素。

不过，这个证明初看起来似乎并不能推广到$p>2$的情形。但是，如果你用群与对称的观点重新叙述上面的证明，你马上就可以看出如何作推广。我们要将上述证明中出现的现象理解为一种对称性，那么就一定要有对称变换。我们观察到的现象是什么呢？那就是在所有的有序对$X=\{(g,g^{-1})|g\in G\}$集合上，有一种对称变换$(x,y)\mapsto(y,x)$.这就是群$\mathbb{Z}_2$在该集合上的作用。那么X拆分为一些轨道的并。而在该作用下轨道的长度为1等价于说$g=g^{-1}$也就是$g^2=1$,由轨道方程

$$|X|=|\{(g,g)|g^2=1\}|+\sum|\text{其它长为2的轨道}|$$

轨道公式表明轨道的长度只能是1或2,我们立刻得出$|\{g|g^2=1\}|$是2的倍数。现在，我想，如何推广这个证明已经至为显然。

设$X=\{(g_1,g_2,\ldots,g_p)|g_1g_2\ldots g_p=1\}$,并设$a$是群$\mathbb{Z}_p$的生成元，考虑群$\mathbb{Z}_p$在$X$上的如下作用

$$\rho:\mathbb{Z}_p\to\mathrm{Sym}(X)$$
$$a\mapsto f$$

其中$f:X\to X$是把$(g_1,g_2,\ldots,g_p)$映到$(g_2,g_3,\ldots,g_p,g_1)$的映射。

我们需要验证$g_2g_3\ldots g_pg_1=1$,这可由$ab=1\Leftrightarrow ba=1$得到。现在由轨道方程

$$|G|^{p-1}=|X|=|\{g\in G|g^p=1\}|+\sum|\text{其它长为}p\text{的轨道}|$$

我们立得$|\{g \in G | g^p = 1\}|$是p的倍数，由$1^p = 1$立即知道群G中存在p阶元素，而且至少有$p-1$个。事实上，可以得到更强的结论：(p阶元素个数+1)是p的倍数。

1.5 共轭作用

群G以共轭作用作用在集合G上，也即

$$\begin{aligned} \rho : G &\to \mathrm{Sym}(G) \\ x &\mapsto (g \mapsto x^{-1}gx) \end{aligned}$$

$$\rho(g)(x) := x^{-1}gx.$$

关于这个作用的轨道就是共轭类，容易看出，作用的核$\ker\rho = Z(G)$.对于$g \in G$,其稳定化子$\mathrm{Stab}(g)$我们记作$C_G(g) = \{h \in G | gh = hg\}$称为$S$的**中心化子**，这是$G$ 的一个子群。我们把这个情形下的轨道方程

$$|G| = \sum_i [G : C_G(g_i)]$$

称之为群G的**类方程**。值得注意的是，有些元素$g \in G$可能轨道长度为1，也就是只与自己共轭的，中心元素，$Z(G)$.如果设$|G| = p^n$，其中p是某个素数，则有

$$p^n = |Z(G)| + \sum_{i, g_i \notin Z(G)} [G : C_G(g_i)]$$

易知$[G : C_G(g_i)]$必是p的倍数。故此时的$|Z(G)|$必须是p的倍数，因此$|Z(G)| > 1$.换而言之我们得到了结论

推论7. 设$|G| = p^n, n > 1$，则G有非平凡的中心$Z(G)$.

例5. 设G是6阶非$Abel$群，我们用群作用的方法证明$G \cong S_3$. 首先，我们知道必有$Z(G) = e$.否则$G/Z(G)$是循环群将推出G是交换的。由柯西定理，(2阶元的个数$+1$)是2的倍数，因而可能是$1, 3, 5$.5 是不可能的，否则群G中只有e和二阶元素从而交换。1也是不可能的，否则这个二阶元素就是中心元素，与$Z(G) = 1$矛盾。因而可设a, b, c是群G中三个不同的二阶元素。现在考虑G在集合$X = \{a, b, c\}$上的共轭作用

$$\rho : G \to S_3$$

$$\rho(g)(x) = g^{-1}xg.$$

由于$\langle a,b,c\rangle = G$,因此若$g\in\ker\rho$,即g与a,b,c都交换，则$g\in Z(G)=e$.故这个作用是忠实的，从而得出

$$G\cong S_3.$$

设$A\le G$是一个子群，容易发现，$g^{-1}Ag$也是一个子群。因为映射$x\mapsto g^{-1}xg$是自同构，而自同构限制在子群上还是同构，其像必然为群。我们称子群A与B共轭，如果$A=g^{-1}Bg$.那么容易看出，G可以以共轭作用作用在它的一些子群上。容易看出，一个子群可以有很多个共轭子群，而G的正规子群就是那些在G 的共轭作用下不变的子群，也就是只与自己共轭的子群，这时它单独组成一个共轭类。

对于$S\subset G$,我们以记号$N_G(S)$表示$\{g\in G|gS=Sg\}$,称为S的**正规化子**。容易看出，$A\le G$的稳定化子是$N_G(A)$，从而有共轭类的大小为

$$[G:N_G(A)].$$

例6. 设$|G|=p^n$，则G的非正规子群个数是p的倍数。

Proof. 考虑在所有子群上的共轭作用，轨道长度是1(正规)或是p的倍数。 □

1.5.1 一些作业题

我们可以举出更多有趣的例子。这里我们给出几道作业题的群作用方法的解答

问题1. 作业题：证明36阶群不是单群。

原来的做法是证明其两个9阶群的交是一个三阶正规子群，过程比较复杂。这里我们给出一个相对更自然的，运用群作用的证明：

Proof. 由Sylow定理，其Sylow-3子群，即9阶子群的个数只能为1或4.若有4个，考虑G在这4个子群$X=\{P_1,P_2,P_3,P_4\}$上的共轭作用，Sylow定理表明这个作用是传递的，即只有一个轨道，因而作用非平凡。但是$\rho: G\to \mathrm{Sym}(X)$不可能是忠实的，因为$36=|G|>|S_4|=24$.从而$\ker\rho\lhd G$ 是一个非平凡的正规子群。 □

问题2. 若G是p^n阶的群，$H<G$，证明$H<N(H)$.

这道题的标准做法是归纳，但也可以用群作用证明：

Proof. 设$X=\{H=H_1,H_2,\ldots,H_m\}$是$H$在$G$中所有的共轭，$H_i=g_i^{-1}Hg_i$,共有$[G:N(H)]$个。若$N(H)=G$则无需作任何证明。故设$N(H)<G$，$|X|$是$p$的倍数。现在用$H$ 作用在该集合上，并注意在此作用下$\{H\}$ 单独组成一个轨道，从而存在别的H_i也单独组成一个轨道，即对任意$h\in H$有$g_i^{-1}Hg_i=H_i=h^{-1}H_ih=h^{-1}g_i^{-1}Hg_ih$. 故$H=g_ih^{-1}g_i^{-1}Hg_ihg_i^{-1}$

$$g_ihg_i^{-1}\in N(H).$$

如果$N(H)=H$，我们将得到对任意$h\in H$有$h\in H_i$，从而$H=H_i$,这是不可能的。 □

问题3. *给出S_4中的所有Sylow-2子群(8阶子群)*

容易知道，一共有1或3个Sylow-2子群。我们现在用群作用的观点和对应定理来寻找这样的8阶子群，设

$$\alpha=(12)(34),\beta=(13)(24),\gamma=(14)(23)$$

由于$K=\{1,\alpha,\beta,\gamma\}\lhd S_4$，我们可考虑如下群$G=S_4$在集合$X=\{\alpha,\beta,\gamma\}$上的共轭作用

$$\rho:S_4\to\mathrm{Sym}(X)\cong S_3$$

易知这是一个满同态，且$K\le\ker\rho$从而有$K=\ker\rho$,则ρ诱导了一个同构

$$\rho':S_4/K\to S_3$$

因而根据对应定理，S_3的三个2阶子群$\langle(\alpha\beta)\rangle,\langle(\beta\gamma)\rangle,\langle(\alpha\gamma)\rangle$对应于$S_4$的三个8阶子群，它们是

$$\langle K,(23)\rangle,\langle K,(34)\rangle,\langle K,(24)\rangle.$$

2 关于直积/直和

关于直积这个相对简单的构造，大家容易产生跟直积有关的东西都是直积的幻觉。常见幻觉有：

问题4. *$G_1\times G_2$的子群一定形如$H_1\times H_2$吗？*

答案是否定的，反例数不胜数，比如$\{(0,0),(1,1)\}\le\mathbb{Z}_2\times\mathbb{Z}_2$.

问题5. *$\mathrm{Aut}(G\times H)=\mathrm{Aut}(G)\times\mathrm{Aut}(H)$是否成立？*

事实上，绝不成立。比如$\mathrm{Aut}(\mathbb{Z}_2\times\mathbb{Z}_2)\cong S_3$.事实上，即使是有限Abel群，决定它们的自同构群也是极为复杂的问题。比如无聊时，曾计算过这样一些例子：

$$\mathrm{Aut}(\mathbb{Z}_2\times\mathbb{Z}_4)\cong D_4$$

$$\mathrm{Aut}(\mathbb{Z}_p\times\mathbb{Z}_{p^2})\cong\left(\mathbb{Z}_p^2\rtimes\mathbb{Z}_p\right)\rtimes\mathbb{Z}_{p-1}^2.$$

问题6. *S_n是否同构于$A_n\times\mathbb{Z}_2$？*

调查显示，超过三分之二的同学认同这个观点。而这绝对是不成立的。事实上，我们有$A_3\times\mathbb{Z}_2\cong\mathbb{Z}_3\times\mathbb{Z}_2\cong\mathbb{Z}_6$.千万不要认为，如果$G/N\cong Q$, 则$G\cong N\times Q$, 绝大多数时候这不成立。

我们现在来看一个跟直积的子群有关的计算例子：

问题7. *$G=\mathbb{Z}_{p^3}\oplus\mathbb{Z}_{p^2}$有多少个$p^2$阶子群？*

p^2阶群只有两种：$\mathbb{Z}_{p^2}$或$\mathbb{Z}_p\oplus\mathbb{Z}_p$.我们先来数同构于$\mathbb{Z}_{p^2}$的子群的个数。我们知道，$G$中的$p^2$阶元素具有如下形状：

$$(pa,b)$$

其中a,b不同时为p的倍数。这样的话就有$p^2\cdot p^2-p^2$个p^2阶元素。每个p^2阶元素都生成一个循环群，而每个这样的循环群恰好具有$\varphi(p^2)$个生成元，因而形如$\mathbb{Z}_{p^2}$的子群的个数就是

$$\frac{p^4-p^2}{\varphi(p^2)}=p^2+p$$

同构于$\mathbb{Z}_p\oplus\mathbb{Z}_p$的子群，容易看出，只有一个。因而所求的群总共有$p^2+p+1$个。

3 Sylow定理

就像我们已经看到的那样，Sylow定理经常和共轭作用联合使用，这是因为它们之间有天然的关系：Sylow-p子群是互相共轭的。除了Sylow定理最常见的数字上的应用必须熟练掌握以外，和共轭作用联合使用往往能得出非平凡的结论。

定理8 (Sylow)**.** *设$p^r|n=|G|$, 则*

- *存在p^r阶子群*
- *若$p^{r+1}\nmid n$则它们互相共轭，个数为$[G:N_G(P)]\equiv 1\mod p$*

- *事实上，p^r阶子群的个数也是$\equiv 1 \mod p$的，这也是Sylow定理的一部分（徐帆补充习题）*

值得注意的是，一般的p子群未必是互相共轭的。

3.1 运用Sylow定理寻找正规子群

寻找正规子群很重要，通常可以用来分类群的结构/证明一个群不是单群。而Sylow定理一个常见的应用是用Sylow定理来寻找正规子群，以下是利用Sylow定理寻找正规子群的常见的方法。

- 取$p^r|n$使$p^{r+1} \nmid n$, 计算Sylow-p子群P的可能个数N,它满足

$$\begin{cases} N \equiv 1 \mod p \\ N\text{是}|G|\text{的因数} \end{cases}$$

- 如果$N=1$，则由Sylow定理我们知道$P \lhd G$.
- 若$r=1$, 则可考虑对每个$r=1$的素数p,对应的所有P所占的元素个数至少为$N(p-1)+1$, 有可能利用这一点说明不可能有这么多Sylow子群。
- 若$r=2$, 还可考虑两个Sylow子群的交$H=P_1\cap P_2$, 如果$|P|^2>|G|$则一定有$|H|=p$(因为$|P_1P_2|=|P|^2/|P_1\cap P_2|$), 并且有$P_1,P_2\leq N_G(H)$ 从而$G=N_G(H)$, $H\lhd N_G(H)=G$.
- 还可考虑群G在$X=\{P_1,P_2,\dots,P_N\}$上的共轭作用$\rho: G\to \mathrm{Sym}(X)$,其核$\ker\rho$可能为$G$的非平凡正规子群。

3.2 运用Sylow定理与共轭作用

如何来综合运用Sylow定理与共轭作用呢？如下引理描述了共轭作用如何与Sylow子群相互作用。

引理9. *设H是某个p子群，作用在所有的Sylow-p子群上，则P_i单独组成一个轨道$\Leftrightarrow H\leq P_i$*

Proof. 有一边是显然的，我们来证明另一边。设$a^{-1}Pa=P$且a是p^k阶元素，则$a\in N_G(P)$.由于$P\lhd N_G(P)$, 考虑a在投射

$$N_G(P)\to N_G(P)/P$$

下的像，由于$|N_G(P)/P|$显然与p互素，其像只能为单位元，故$a\in P$. 这足以证明命题。 □

命题10. *G的每个p方幂阶的子群H被某个Sylow-p子群包含。*

Proof. 考虑用H共轭作用在G的所有Sylow-p子群上，则其轨道长度为1或p的倍数。由于Sylow-p子群的个数是$\equiv 1 \mod p$, 我们知道一定有一个P单独组成一个轨道，因而由引理$H \leq P$. □

命题11. *设H是一个p子群，则包含它的Sylow-p子群的个数$a \equiv 1 \mod p$.*

Proof. 让H作用在所有Sylow-p子群上，$H \leq P$等价于P的轨道长度为1. 由于所有Sylow-p子群的个数$\equiv 1 \mod p$, 我们有

$$a \equiv a + \text{其它轨道} = N \equiv 1 \mod p.$$

□