Week 7 摘要

本周的主要内容是Sylow Thm.的表述，第一部分的证明梗概，以及为了完成整个证明而引入的"群作用"的概念.

* 我们始终强调，研究子结构是代数研究中的重要方法. Week 3引入的 Lagrange Thm. 给出了子群构成的一个必要条件，即阶数整除"母群"的阶；那么自然要问，这个条件在什么情况下是充分的？Sylow Thm. 对阶为素数幂的群给出了回答，并对各素数幂阶的子群的数量给出了估计(同余的形式). 同时给出了这些子群之间的共轭、包含关系.
* 对于Sylow Thm.的第一部分(即子群数量的同余估计)，我们的主要证明思路如下：
  - 为估计群G中d阶子群的总数，首先去考虑所有的d阶子集，记后者全体构成集合T.
  - 将群G作用在T上，据此给出T的一个分划.
  - 给出上述分划中每块的阶的估计，最终得到d阶子群个数的一个估计式④

  值得指出，上述步骤对于任意的群G和因子d都是成立的. Sylow Thm.的第一部分，是借由其素数幂条件的良好数论性质，由④给出的直接推论.
* 我们在本周给出的基于上述思路的证明并不完整，主要是对划分中每一块的阶的估计没有给出证明. 为此，我们引入**群作用**的概念. 通过群在其他集合上的作用来研究群自身的性质是常见的想法. 我们在Sylow Thm.的证明中将应用这个想法.

Def. (Sylow 子群)

设G为有限群，$|G|=n$，p为素数. $k=v_p(n)$ (即 $p^k \mid n$ 且 $p^{k+1} \nmid n$)

考虑 $H \le G$.

(1) 若$|H|$为p的幂，则称H为G的p-子群.

(2) 若$|H|=p^k$，则称H为G的Sylow p-子群.

由Lagrange Thm.，我们知道p-子群的阶的p幂次$\le k$.

故Sylow p-子群也可理解为阶最大的p-子群.

Sylow Thm. 断言：Sylow p-子群存在.

Sylow 子群的例子：

1) 12阶循环群的Sylow 2-子群.

$G=\langle a\rangle \quad o(a)=12 \rightarrow H=\langle a^3\rangle$

2) A_4的Sylow 2-子群

$H=\{id, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$

(还有 $H \lhd A_4$, $H \lhd S_4$)

Sylow Thm.

对有限群$G(|G|=n)$及素数p，则有：

(1) G有Sylow p-子群，且个数模p余1.

(2) 设H、K都是G的Sylow p-子群，则$\exists g\in G$使$K=gHg^{-1}$

(即任何两个Sylow p-子群共轭)

(3) 对G的p-子群A，总存在Sylow p-子群H使$A\subseteq H$.

事实上，(1)可加强为：对$p^l \mid n$，有

$$\left|\{A\le G, |A|=p^l\}\right| \equiv 1 \pmod p$$

我们将证明加强的(1).

Sylow Thm.的证明：

证明思路：

(1) 为了寻找p^l阶子群，我们首先考虑所有的p^l阶子集，将所有这些子集构成的集合作分划，以导出我们需要的数量关系.

(2)(3) 从群作用的角度证明.

我们首先考虑一个特殊情况，以理解上述的证明思路.(这里$p=2$, $l=1$)

对偶数阶群G，考虑$p=2$，则有：

$\left|\{a\in G \mid a^2=e\}\right| \equiv 0 \pmod 2$ (即G中二阶元的个数都是奇数)

从而有：$\left|\{A \mid A\le G, |A|=2\}\right| \equiv 1 \pmod 2$ (因为每个二阶元对应一个二阶子群)

Pf: 定义等价关系$\sim$：$\forall a,b\in G$，$a\sim b \overset{\Delta}{\Longleftrightarrow} a=b$ 或 $a=b^{-1}$.

(需要验证$\sim$确实是等价关系，这是显然的)

则对任意$a\in G$，a所在的等价类为$\{a,a^{-1}\}$

$\left|\{a,a^{-1}\}\right|=1 \Leftrightarrow a=a^{-1} \Leftrightarrow a^2=e$

$\left|\{a,a^{-1}\}\right|=2 \Leftrightarrow a\ne a^{-1} \Leftrightarrow a^2\ne e$.

记T为G在$\sim$下的全体等价类.

则有

$$\begin{aligned}|G| &= \sum_{A\in T}|A| \\ &= \sum_{A\in T,|A|=1}|A| + \sum_{A\in T,|A|=2}|A| \\ &= \left|\{A\in T \mid |A|=1\}\right| + 2\left|\{A\in T \mid |A|=2\}\right| \\ &= \left|\{a\in G \mid a^2=e\}\right| + 2\left|\{A\in T \mid |A|=2\}\right| \\ &\equiv 0 \pmod 2\end{aligned}$$

即 $\left|\{a\in G \mid a^2=e\}\right| \equiv 0 \pmod 2$

上述证明的思路与一般情形下的(1)证明思路类似：

通过对G的分划，及分划中若干已知的集合的阶，

去导出目标的集合的阶的信息.

接下来我们回到一般情形的证明思路：

值得注意的是，该证明的绝大部分讨论都与素数幂的条件无关.

命题 设G为n阶群，$d \mid n$. G的d阶子群的个数为k. 则有：

(1) 存在d的一些不小于2的因子$w_1,w_2,\dots,w_s$使得：

$$\binom{n-1}{d-1}=k+w_1+w_2+\cdots+w_s \quad ④$$

(2) 若$d=p^l$，则$k\ge 1$ (我们总认为符号p表示素数，以下不再说明)

(3) 若$d=p^l$，则$k\equiv 1 \pmod p$

Pf: 我们先说明，(1)⇒(2)(3)

将$d=p^l$代入④式，有：

$$\binom{n-1}{p^l-1}=k+w_1+\cdots+w_s$$

由$w_i \mid p^l$，$w_i\ge 2$，$i=1,2,\dots,s$

有 $w_i=p^{t_i}$ $1\le t_i\le l$. $i=1,2,\dots,s$

$\Rightarrow p \mid w_i$ $i=1,2,\dots,s$. 在④两边模p

则有 $\binom{n-1}{p^l-1}\equiv k \pmod p$

由数论中的相关结果有 $\binom{n-1}{p^l-1}\equiv 1 \pmod p$

故 $k\equiv 1 \pmod p$

接下来我们证明一般性的结果(1)

对n阶群G，$d \mid n$，希望考察G中有无d阶子群.

记T为G的所有d阶子集构成的集合.

定义T上的等价关系$\sim$. $A\sim B \overset{\Delta}{\Longleftrightarrow} \exists g\in G$使$B=gA$.(仍需验证，这是平凡的) 群作用：群G作用在T上

对$A\in T$，有$[A]=\{B\in T \mid A\sim B\}=\{gA \mid g\in G\}$

$[A]$：A所在的等价类 我们可以断言：

(1) 若$[A]$中含有子群，则子群的数量为1，且$|[A]|=\frac{n}{d}$

(2) 若$[A]$中不含子群，则$|[A]|=\frac{n}{d}\cdot w_A$，其中$w_A\ge 2$且$w_A \mid d$

设$L_1,L_2,\dots,L_m$为全体等价类. $L_1,\dots,L_k$含有子群；$L_{k+1},\dots,L_m$不含子群.

从而G恰有k个d阶子群.

由(1),(2)，有$|L_1|=|L_2|=\cdots=|L_k|=\frac{n}{d}$，$|L_i|=\frac{n}{d}\cdot w_i$. $k+1\le i\le m$

$\Rightarrow |T|=\sum_{i=1}^{m}|L_i|=\frac{n}{d}\cdot k+\frac{n}{d}\sum_{i=k+1}^{m}w_i$

又有 $|T|=\binom{n}{d}=\binom{n-1}{d-1}\frac{n}{d}$

则有 $\binom{n-1}{d-1}=k+\sum_{i=k+1}^{m}w_i$. 这就是④式.

为了给出对断言(1)(2)的证明，我们先讨论群作用的若干性质.

引入：我们并非没有见过类似的东西.(作用)

例如向量的数乘，就是$\mathbb{R}$作用在$\mathbb{R}^n$上(又得到了$\mathbb{R}^n$)

这个作用有两条性质 $\begin{cases}(\lambda\mu)\vec{v}=\lambda(\mu\vec{v})\\ 1\vec{v}=\vec{v}\end{cases}$

我们将上述性质抽象为下面的定义.

Def.

(幺半群在集合上的作用)

对幺半群G与集合X. $\rightarrow$是$G\times X$到X上的一个映射. $g\rightarrow x := \rightarrow(g,x)$.

若$\forall g,h\in G$，$\forall x\in X$，有 $\begin{cases}gh\rightarrow x=g\rightarrow(h\rightarrow x)\\ e_G\rightarrow x=x\end{cases}$

则称$\rightarrow$是幺半群G在X上的一个作用

群作用的例子.

1. 我们在Sylow Thm.定理的证明中定义的等价关系，就是基于群在其子集上的作用.

   可以验证它满足群作用的两个条件：

   $\begin{cases}e_G\rightarrow A=e_GA=A\\ (gh)\rightarrow A=\{gha \mid a\in A\}=g\rightarrow(h\rightarrow A)\end{cases}$

2. 给定集合X，$G:=Sym(X)$ $\sigma\rightarrow x:=\sigma(x)$

   验证条件 $\begin{cases}id\rightarrow x=id(x)=x\\ (\sigma\tau)\rightarrow x=(\sigma\tau)(x)=\sigma(\tau(x))=\sigma\rightarrow(\tau\rightarrow x)\end{cases}$

3. 共轭作用 —— G在自身上的作用 $g\rightarrow x$，${}^gx:=gxg^{-1}$

   验证条件 $\begin{cases}e\rightarrow x=exe^{-1}=x\\ (gh)\rightarrow x=ghx(gh)^{-1}=ghxh^{-1}g^{-1}=g(hxh^{-1})g^{-1}=g\rightarrow(h\rightarrow x)\end{cases}$

   这里还有一个附加的性质 —— $g\rightarrow(xy)=(g\rightarrow x)(g\rightarrow y)$

4. 群在其子集上的共轭作用.

   G. $X=2^G$. $g\rightarrow A:=gAg^{-1}:=\{gag^{-1} \mid a\in A\}$

   性质验证也是类似的.

   对$H\le G$，有$H\lhd G \Leftrightarrow \forall g\in G, gHg^{-1}=H$

   $\Leftrightarrow \forall g\in G, g\rightarrow H=H$.

   (正规子群在共轭作用下不变)

5. $G=GL_2(\mathbb{R})$ ($\mathbb{R}$上所有2阶可逆矩阵)

   $X=\mathbb{R}^2$ $A\rightarrow\beta:=A\beta$. (矩阵在列向量上的作用)

   性质：$\forall\alpha,\beta\in X$，$\alpha,\beta\ne 0$. $\exists A\in G$使$\beta=A\alpha$

   (该性质称为作用的传递性).

考虑群G以$\rightarrow$作用在X上，可在X上定义等价关系$\sim$：

$x\sim y \overset{\Delta}{\Longleftrightarrow} \exists g\in G$. s.t. $y=g\rightarrow x$

等价关系的验证：

$x\sim x$：因为 $x=e\rightarrow x$

$x\sim y\Rightarrow y\sim x$：由$x\sim y$，$\exists g\in G$，$y=g\rightarrow x$

那么 $g^{-1}\rightarrow y=g^{-1}\rightarrow(g\rightarrow x)=(g^{-1}g)\rightarrow x=x$

即 $y\sim x$

$x\sim y \wedge y\sim z\Rightarrow x\sim z$：$\exists g,h\in G$，$y=g\rightarrow x$，$z=h\rightarrow y$

$\Rightarrow z=h\rightarrow y=h\rightarrow(g\rightarrow x)=(hg)\rightarrow x$

$\Leftrightarrow x\sim z$

课上布置，并说可能要考的一个题目：

对群G，$g\in G$，如下定义$f: G\rightarrow G$.

$\forall a\in G$，$f(a)=gag^{-1}$.

求证：f是G到自身的同构，并且$f^{-1}(a)=g^{-1}ag$. $\forall a\in G$.

(此处的f称为由g诱导的内自同构)

Pf: 先证f为$G\rightarrow G$的同态.

任取$a,b\in G$，有 $f(ab)=gabg^{-1}$

$f(a)f(b)=(gag^{-1})(gbg^{-1})$

$=ga(g^{-1}g)bg^{-1}=gabg^{-1}$

即有$f(ab)=f(a)f(b)$，即f为同态.

再证f为单射. 对$a,b\in G$，$f(a)=f(b)$

有$gag^{-1}=gbg^{-1}$. 两边右乘g，左乘g^{-1}有$a=b$

最后证f为满射. 任取$a\in G$，都存在$x=g^{-1}ag$，使得：

$f(x)=g(g^{-1}ag)g^{-1}=a$

故f为同构. $f^{-1}(a)=g^{-1}ag$