第十周周一期中考试.

回顾：群作用的定义

设 G 为么半群，X 为集合. $\to: G\times X\to X$

若 (1) $\forall x\in X$，$e_G\to x = x$

(2) $\forall g,h\in G$，$x\in X$，有 $g\to(h\to x)=(gh)\to x$，

则称 $\to$ 为一个作用.

引入"作用"的概念，是为了通过群在集合上的作用研究导出群自身的结论.

Sylow Thm. 的证明就是这种研究思路的经典例子.

设群 G 依 $\to$ 作用在 X 上. 在 X 上定义关系 $\sim$：$x\sim y \overset{\wedge}{\iff} \exists g\in G$, s.t. $g\to x=y$

则 $\sim$ 是一个等价关系. 如果 X 有限，设 $U_1,U_2,\dots,U_m$ 为 $\sim$ 在 X 上诱导的等价类全体. 则有 $|X|=\sum_{i=1}^{m}|U_i|$ ㊅

对于一般的等价关系，我们对 $|X|$ 的表达到此为止。但对于群作用，我们能给出更好的结果.

$\forall x\in X$，$[x]=\{g\to x \mid g\in G\}=:\underline{G_x}$ 称为 x 在作用 $\sim$ 下的轨道.

$\mathrm{Stab}(x):=\{g\in G \mid g\to x=x\}$，称为稳定化子.（$x$ 所在的稳定化子）.

我们可以给出 x 的轨道的阶的一个结论：（轨道公式）

命题. 设群 G 依 $\sim$ 作用在 X 上. $x\in X$. $H=\mathrm{Stab}(x)$. 则有：

(1) $H\leq G$.

(2) $\forall a,b\in G$，$a\to x=b\to x \iff a^{-1}b\in H \iff aH=bH$

(3) 定义 $\varphi: G/H\to G_x$. $\forall a\in G$，$\varphi(aH):=a\to x$

则 φ 是 well-defined 一一对应.

(4)（轨道公式）若 G，X 都有限，则

$$|G_x|=\frac{|G|}{|H|}=|G/H|$$

Pf：

(1) 由 $e_G\to x=x$. 故 $e_G\in H$

设有 $a\in H$，$b\in H$. 则有 $(ab)\to x=a\to(b\to x)=a\to x=x$. 故 $ab\in H$

设有 $a\in H$. 则有 $a^{-1}\to x=a^{-1}\to(a\to x)=(a^{-1}a)\to x=e_G\to x=x$. 故 $a^{-1}\in H$

综上有 $H\leq G$

(2) 设有 $a\to x=b\to x$. 则有 $(a^{-1}b)\to x=a^{-1}\to(b\to x)=a^{-1}\to(a\to x)=(a^{-1}a)\to x=e_G\to x=x$. 即 $a^{-1}b\in H$

反之，若有 $a^{-1}b\in H$. 则有 $a\to x=a\to(a^{-1}b\to x)=(aa^{-1}b)\to x=b\to x$.

后面的一个等价是熟知的.（可参阅 week 3）

(3) φ is well-defined：

若 $aH=bH$. 则 $\varphi(aH)=a\to x=b\to x=\varphi(bH)$

即映射的结果与陪集的表述方式无关.

- φ 单射：若有 $\varphi(aH)=\varphi(bH)$. 即 $a\to x=b\to x$. 由 (2) 知 $aH=bH$
- φ 满射：任取 $g\in G_x$. 有 $g=a\to x$. $\exists a\in G$. 则有 $\varphi(aH)=g$. $aH\in G/H$.

(4) 是 (3) 的直接推论.

由上面的结论，我们就能基于㊅给出更好的表达式：

设有限群 G 依 $\to$ 作用在有限集 X 上. $U_1,\dots,U_m$ 是该作用下两两不同的轨道全体

记 $U_i=G_{x_i}$ $(x_i\in X,\ i=1,\dots,m)$，则有：

$$|X|=\sum_{i=1}^{m}\frac{|G|}{|\mathrm{Stab}(x_i)|}$$（轨道公式的直接推论）.

对于更特殊的群 G，我们能够得到更特殊的结论：

定义：设 G 依 $\to$ 作用在 X 上，$x\in X$. 若 $\forall g\in G$，有 $g\to x=x$. 则称 x 是该作用下的不动点.

等价地说，$\{x\}=G_x$，$G=\mathrm{Stab}(x)$

我们接下来看一些具体的不动点.

G 共轭作用在 G 上 $(g\to x:=gxg^{-1})$

对 $x\in G$. x 为不动点 $\iff \forall g\in G$，$g\to x=gxg^{-1}=x$

$\iff \forall g\in G$，$gx=xg$

即 x 与 G 中任意元素都乘法可交换.

（$Z(G):=\{x\in G \mid gx=xg,\ \forall g\in G\}$ 称为群的中心）

例如，$Z(GL_2(\mathbb{R}))=\left\{\begin{pmatrix}a&0\\0&a\end{pmatrix} \middle| a\neq 0\right\}$（即和任意 2 阶可逆实矩阵都可交换的 2 阶可逆实矩阵）

命题（不动点定理）. 设 p 为素数，有限群 G 的阶是 p 的幂. 设 G 依 $\to$ 作用在有限集 X 上.

Y 为全体不动点. 则有 $|X|\equiv|Y| \pmod p$. 特别地，若 $p\nmid |X|$. 则该作用存在不动点.

在证明 Sylow Thm. 时我们将会用到这一结论.

Pf：设 $U_1,\dots,U_m$ 为全体轨道. $U_i=G_{x_i}$ $(x_i\in X,\ i=1,\dots,m)$

不妨设 $U_1,\dots,U_k$ 恰含一个元素，$U_{k+1},\dots,U_m$ 至少含两个元素.

由轨道公式，我们有：

$|X|=\sum_{i=1}^{m}|U_i|=\sum_{i=1}^{k}|U_i|+\sum_{i=k+1}^{m}|U_i|$ ㊅

对 $i=1,\dots,k$. $|U_i|=\frac{|G|}{|\mathrm{Stab}(x_i)|}=1$.

对 $i=k+1,\dots,m$，$|U_i|=\frac{|G|}{|\mathrm{Stab}(x_i)|}\geq 2$. 又由 $|G|$ 为 p 的幂，

故 $|U_i|$ 也为 p 的幂.

则由㊅式有 $|X|\equiv k \pmod p$

又每一个阶为 1 的轨道对应一个不动点. 则 $|Y|=k$

综上有 $|X|\equiv|Y| \pmod p$.

接下来回到 Sylow Thm. 的后半部分.

命题. 设 G 为有限群. p 为素数. A 为 G 的 p-子群. $H\leq G$. $\underline{p\nmid\frac{|G|}{|H|}}$

则 $\exists g\in G$, s.t. $A\subseteq gHg^{-1}$ 即 $|G|$，$|H|$ 的分解中 p 的指数相同.

Pf：考虑 A 依左乘作用在 G/H 上.（$a\in A$，$g\in G$. $a\to(gH):=agH$）

由 $|A|$ 为 p 的幂. $p\nmid|G/H|$. 由不动点定理知该作用有不动点.

任取 $g\in G$ 为该作用的不动点. 则有 $\forall a\in A$. $a\to gH=agH=gH$.

由 $agH=gH \Rightarrow ag\in gH \Rightarrow a\in gHg^{-1}$. 知 $A\subseteq gHg^{-1}$.

Sylow Thm. 的第二部分：

设 G 为有限群. p 为素数. $v_p(|G|)=k$

(1) 若 H、K 是 Sylow p-子群. 则它们共轭. 即 $\exists g\in G$ 使 $K=gHg^{-1}$

(2) 设 A 是 G 的 p-子群. 则 $\exists$ G 的 Sylow p-子群 H 使 $A\subseteq H$.

Pf：(1) K 是 p-子群. $p\nmid\frac{|G|}{|H|}$

$\Rightarrow \exists g\in G$ 使 $K\subseteq gHg^{-1}$ 又有 $|gHg^{-1}|=|H|=|K|$

故 $K=gHg^{-1}$.

(2) 任取 G 的 Sylow p-子群 L. A 为 p-子群. $p\nmid\frac{|G|}{|L|}$

则 $\exists g\in G$ 使 $A\subseteq \underline{gLg^{-1}}$ 它也是 Sylow p-子群！

Sylow Thm. 第一部分的详细证明.

设 G 为有限群，p 为素数，$p^l \mid |G|$，$l\geq 1$. 则有：

$$\left|\{H\leq G \mid |H|=p^l\}\right|\equiv 1 \pmod p$$

Pf：

记 $T:=\{A\subseteq G \mid |A|=p^l\}$

考虑 G 依左乘作用在 T 上. 记 $L_1,L_2,\dots,L_m$ 为该作用下的两两不同的轨道全体. 对任意轨道 U，我们说明下面两种情况之一成立.

1° U 中恰含一个 p^l 阶子群. 且 $|U|=\frac{n}{p^l}$（其中 $n=|G|$）

2° U 中不含 p^l 阶子群. 且 $\frac{n}{p^{l-1}} \mid |U|$.

在上述断言成立的假设下，不妨设轨道 $L_1,\dots,L_k$ 恰含一个子群.

$L_{k+1},\dots,L_m$ 中均不含子群. 则有：

对 $1\leq i\leq k$，有 $|L_i|=\frac{n}{p^l}$

对 $k+1\leq i\leq m$，有 $\frac{n}{p^{l-1}} \mid |L_i|$

则有 $|T|=\sum_{i=1}^{m}|L_i|=k\cdot\frac{n}{p^l}+\sum_{i=k+1}^{m}w_i\frac{n}{p^{l-1}}$. $w_i\in\mathbb{Z}^+$，$i=k+1,\dots,m$

另一方面，有 $|T|=\binom{n}{p^l}$

则有 $\binom{n}{p^l}=\frac{n}{p^l}\binom{n-1}{p^l-1}=k\cdot\frac{n}{p^l}+\sum_{i=k+1}^{m}w_i\frac{n}{p^{l-1}}$

即 $\underline{\binom{n-1}{p^l-1}}=k+p\sum_{i=k+1}^{m}w_i$ 模 p 有：

$k\equiv 1 \pmod p$

它模 p 余 1，这是数论性质.

接下来证明 1°，2°. 需要一些背景知识.

群在子集上的作用.

设 G 为群. G 依左乘作用在其子集上. 对 $A\subseteq G$，A 所在的轨道 $=\{gA \mid g\in G\}$.

对于子群 H，有 H 所在的轨道 $=\{gH \mid g\in G\}=G/H$.

$\mathrm{Stab}(H)=H$（这是因为 $\forall g\in G$，$gH=H \iff g\in H$）

事实上我们有：$H\leq G \iff \mathrm{Stab}(H)=H$.（$\Leftarrow$：$\mathrm{Stab}(H)\leq G$）.

Fact.

设 $A\subseteq G$，$H=\mathrm{Stab}(A)$. 则 $A=HA$.（对于左乘作用）

Pf：$HA=\{ha \mid h\in H, a\in A\}=\bigcup_{h\in H}hA$.

由稳定化子的定义，总有 $hA=A$，$\forall h\in H$. 故上式 $=A$.

基于此，我们有：

$HA=\{ha \mid h\in H, a\in A\}=\bigcup_{a\in A}Ha$ 即一些右陪集之并.

对于陪集，总有：$\forall a,b\in A$，或者 $Ha=Hb$，或者 $Ha\cap Hb=\varnothing$.

因此 $HA=\bigcup_{a\in A}Ha$ 本质上是不交并. 基于此，进一步有：

Fact. 设 $A\subseteq G$，A 有限. $H=\mathrm{Stab}(A)$. 则有：

(1) $|H| \mid |A|$.   (2) $A\leq G \iff e_G\in A$ 且 $|H|=|A|$

Pf：(1) $|A|=\left|\bigcup_{a\in A}Ha\right|$ 则 $|A|$ 是若干两两不交的 $|Ha|$ 之和. 又 $|Ha|=|H|$.

则 $|H| \mid |A|$.

(2) $\Rightarrow$：若 $A\leq G$，则有 $e_G\in A$. 且有 $A=H$. 结论显然

$\Leftarrow$：若 $e_G\in A$，$|H|=|A|$. 则由 $A=\bigcup_{a\in A}Ha$，

及 $\underline{\forall a\in A,\ Ha\subseteq A}$. 又 $|H|=|Ha|=|A|$. 故 $Ha=A$

因为 $H=\mathrm{Stab}(A)$，所以对 A 中元素作用不可能出去.

基于上述结论，考虑轨道 U.

(1) 设 U 中有一个子群 $H\leq G$.

那么 $U=\{gH \mid g\in G\}=G/H$.

假设有 $\exists g\in G$，$gH\leq G \Rightarrow e_G\in gH \Rightarrow gH=H$.

此时 $|U|=|G/H|=\frac{|G|}{|H|}$ 这就是论断 1°.

(2) 设 U 中不含 G 的子群. 我们总可以取 $A\in U$，使 $e_G\in A$.

（任取 $A'\in U$. $a\in A'$. 则取 $A=a^{-1}A'$，有 $e_G\in A$）.

$U=\{gA \mid g\in G\}$. $|U|=\frac{|G|}{|\mathrm{Stab}(A)|}$

又有 $|\mathrm{Stab}(A)| \mid |A|$，$|\mathrm{Stab}(A)|\neq|A|$（因为 A 不是子群）

另一种处理：对群的阶归纳.

群论的内容到此为止. 接下来进入环论的部分.

一些例子.

我们考虑一个熟知的结构 $(\mathbb{Z};+;\cdot)$.

$(\mathbb{Z};+)$ 构成交换群. $(\mathbb{Z};\cdot)$ 构成么半群. $(+;\cdot)$ 之间有左右分配律.

Def. 将这样的结构抽象出来，我们称之为环.

称代数结构 $(R;+;\cdot)$ 是环，若：

1° $(R,+)$ 构成交换群，么元为 0.

2° $(R,\cdot)$ 构成么半群、么元为 1_R.

3° 分配律. $\forall a,b,c\in R$，有：$a\cdot(b+c)=a\cdot b+a\cdot c$，

$(a+b)\cdot c=a\cdot c+b\cdot c$

若 $\forall a,b\in R$，有 $ab=ba$，则称 $(R;+;\cdot)$ 为交换环.

既然环的结构建立在群的基础上，我们可以预想到一些性质的联系

更多的例子：$(M_n(\mathbb{R});+;\cdot)$：$\mathbb{R}$ 上的所有上三角矩阵.

事实上，若在上述定义的 1° 中不要求 $(R;+)$ 为 Abel 群（记为 1°'），该定义仍然是等价的（换句话说，$1^{\circ\prime}+2^\circ+3^\circ \Rightarrow 1^\circ+2^\circ+3^\circ$）

有限环的例子：$(\mathbb{Z}_n;\oplus;\odot)$.

考虑 $R=\{(a_0,a_1,a_2,\dots,a_i,\dots) \mid a_i\in\mathbb{R},\ i\in\mathbb{N}\}$.

$(a_0,a_1,\dots)+(b_0,b_1,\dots):=(a_0+b_0,a_1+b_1,\dots)$

$(a_0,a_1,\dots)\cdot(b_0,b_1,\dots):=(c_0,c_1,\dots)$

其中 $c_k=\sum_{i=0}^{k}a_ib_{k-i}$

（本质上就是形式幂级数的定义）.