

设  $G$  是一个幺半群,  $X$  集合

$$\rightarrow: G \times X \rightarrow X \quad (\forall g \in G, x \in X, g \rightarrow x = \neg(g, x))$$

$$\text{若 (i) } \forall x \in X, \underset{| \cdot x = x}{\text{Id}} \rightarrow x = x.$$

$$\text{(ii) } \forall g, h \in G, x \in X, g \rightarrow (h \rightarrow x) = (gh) \rightarrow x \quad (ab)x = a(bx)$$

群  $G$  依  $\rightarrow$  作用在  $X$  上.

在  $X$  上定义关系  $\sim$   $x \sim y \Leftrightarrow \exists g \in G, \text{s.t. } g \rightarrow x$

$$\left( \begin{array}{l} \text{自反: } x = \text{Id} \rightarrow x \\ \text{对称: } y = g \rightarrow x \Leftrightarrow x = g^{-1} \rightarrow y \\ \text{传递: } y = g \rightarrow x, z = h \rightarrow y \Rightarrow z = (hg) \rightarrow x. \end{array} \right) \text{ 叫做关系}$$

如果  $X$  有限, 设  $U_1, U_2, \dots, U_m$  是  $(X, \sim)$  的两个不同的等价类全体, 则:

$$|X| = |U_1| + |U_2| + \dots + |U_m|$$

$$\forall x \in X, \{y | y \in X, x \sim y\} = \{g \rightarrow x | g \in G\} = \underline{G_x / \text{orbit}(x) / G(x)}$$

$G_x$  称为  $x$  在作用  $\rightarrow$  下的轨道.  $\text{stab}(x) = \{g | g \in G, g \rightarrow x = x\}$  稳定化子

命题. 设  $G$  依  $\rightarrow$  作用在  $X$  上,  $x \in X$ , 记:  $G_x = \{g \rightarrow x | g \in G\}$ ,

$H = \text{stab}(x) = \{g | g \in G, g \rightarrow x = x\}$ , 则:

(i)  $H \leq G$  ( $H$  是子群)

$$(i) \forall a, b \in G, a \rightarrow x = b \rightarrow x \Leftrightarrow a^{-1}b \in H \Leftrightarrow aH = bH.$$

(ii) 定义  $\varphi: G/H \rightarrow G_x: \forall a \in G, \varphi(aH) = a \rightarrow x$ , 则  $\varphi$  是合理的--对应.

(iii) 若  $G, X$  都有限, 则  $|G_x| = |G/H| = \frac{|G|}{|H|}$  (轨道公式)

证: (i)  $\because \text{Id} \rightarrow x = x, \therefore \text{Id} \in H$

$$a, b \in H, \therefore a \rightarrow x = b \rightarrow x = x$$

$$(ab) \rightarrow x = a \rightarrow (b \rightarrow x) = a \rightarrow x = x, \therefore ab \in H$$

$$a^{-1} \rightarrow x = a^{-1} \rightarrow (a \rightarrow x) = (a^{-1}a) \rightarrow x = 1_G \rightarrow x = x. \quad \therefore a^{-1} \in H$$

(2) 若  $a \rightarrow x = b \rightarrow x$

$$\therefore (a^{-1}b) \rightarrow x = a^{-1} \rightarrow (b \rightarrow x) = a^{-1} \rightarrow (a \rightarrow x) = (a^{-1}a) \rightarrow x = 1_G \rightarrow x = x.$$

若  $(a^{-1}b) \rightarrow x = x$ ,

$$a \rightarrow x = a \rightarrow ((a^{-1}b) \rightarrow x) = (a(a^{-1}b)) \rightarrow x = b \rightarrow x.$$

$\therefore a \rightarrow x = b \rightarrow x \Leftrightarrow a^{-1}b \in H \Leftrightarrow aH = bH$ . // 陪集的时候说过

(3)  $\varphi$  是合理定义的:

$$\text{由(2), } aH = bH \Rightarrow a \rightarrow x = b \rightarrow x$$

$\varphi$  是单射: 若  $\varphi(aH) = \varphi(bH)$ , 则  $a \rightarrow x = b \rightarrow x$ . 由(4) 和  $aH = bH$ .

$$\text{ran}(\varphi) = G_x: \forall a \in G: a \rightarrow x = \varphi(aH) \in \text{ran}(\varphi).$$

$$(4) |Gx| = |G/H| = \frac{|G|}{|H|}. \quad \text{因为双射}$$

★ 命题. 设有限群  $G$  依一作用在有限集  $X$  上,  $U_1, U_2, \dots, U_m$  是该作用下的两个不同的轨道全体, 记  $U_i = Gx_i$  ( $x_i \in X$ ,  $i=1, 2, \dots, m$ ), 则:  $|X| = \sum_{i=1}^m \frac{|G|}{|\text{stab}(x_i)|}$

$$\text{证: } |X| = \sum_{i=1}^m |U_i| \quad \text{[由(4)]} \quad |Gx| = \frac{|G|}{|\text{stab}(x)|}$$

$$\forall i: U_i = Gx_i \quad |U_i| = |Gx_i| = \frac{|G|}{|\text{stab}(x_i)|} \quad \#.$$

定义. 设  $G$  依一作用在  $X$  上,  $x \in X$ . 若  $\forall g \in G$ , 都有  $g \rightarrow x = x$ , 则称  $x$  是该作用下的不动点. ( $x$  是不动点  $\Leftrightarrow G_x = \{x\} \Leftrightarrow \text{stab}(x) = G$ )

$$G$$
 共轭作用在  $G$  上.  $g \rightarrow x = gxg^{-1}$

$$\begin{aligned} x \in G, x \text{ 是共轭作用下的不动点} &\Leftrightarrow \forall g \in G, g \rightarrow x = x \Leftrightarrow \forall g \in G, gxg^{-1} = x \\ &\Leftrightarrow \forall g \in G, gx = xg \end{aligned}$$

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

$\Leftrightarrow G = GL_2(\mathbb{R}) = \{\text{所有二阶可逆实矩阵}\}$

$$Z(G) = \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \mid a \neq 0 \right\} \quad || \text{对 } n \text{ 阶都行.}$$

\* 命题. 设  $p$  是素数, 有限群  $G$  的阶数是  $p$  的幂次. 令  $G$  依一作用在有限集  $X$  上,  $Y$  是该作用下的全体不动点.  $Y = \{x \mid x \in X: \forall g \in G, g \cdot x = x\}$ . 则  $|X| \equiv |Y| \pmod{p}$ . 特别地, 若  $p \nmid |X|$ , 则该作用有不动点. 即  $x \neq 0$ .  $|x| \equiv k \pmod{p}$ .

证: 记  $U_1, \dots, U_m$  是全体轨道.  $U_i = Gx_i$  ( $i=1, \dots, m$ )

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

$$\therefore |X| = \sum_{i=1}^m \frac{|G|}{|\text{stab}(x_i)|} \quad \hookrightarrow |x| ?$$

$$\text{对 } i=1, \dots, k, \quad |U_i| = \frac{|G|}{|\text{stab}(x_i)|} = 1$$

$$\text{对 } i=k+1, \dots, m, \quad |U_i| = \frac{|G|}{|\text{stab}(x_i)|} \geq 2$$

$\because |G|$  是  $p$  的幂次,  $|\text{stab}(x_i)| \mid |G|$ .

$\rightarrow |U_i|$  是  $p$  的幂次, 而  $|U_i| \geq 2$ .  $\therefore p \mid |U_i|, k+1 \leq i \leq m$ .

$$\therefore |X| \equiv k \pmod{p}$$

$$|Y| = k. \rightarrow k \nmid, \text{ 每 } U_i - U_k \rightarrow$$

$$2^3 \times 3^2 = 36$$

$$p=2, \quad 2 \nmid \frac{36}{|H|}$$

$$|H|=4, 12, 36$$

命题. 设  $G$  是有限群,  $p$  是素数,  $A$  是  $G$  的  $p$  7 群 ( $|A|=p^k$ ),  $H \leq G$ ,  $p \nmid \frac{|G|}{|H|}$ .

则  $\exists g \in G$ , st.  $A \subseteq gHg^{-1}$  ( $gHg^{-1} = \{ghg^{-1} \mid h \in H\}$ )

证: 考虑  $G/H$ . 令  $A$  依左乘作用在  $G/H$  上 ( $\forall a \in A, \forall g \in G, a \cdot (gh) =agh$ )

$\because |A|$  是  $p$  的幂次,  $p \nmid |G|/|H|$  上个命题中的  $X$

$\therefore$  该作用具有不动点, 取  $g \in G$ , st.  $gH$  是不动点.

$$\forall a \in A, a \cdot (gh) = gh. \quad \therefore (agh) = gh$$

$$\therefore ag \in gH \quad a \in gHg^{-1}$$

后来  $g^{-1}$

$$\therefore A \subseteq gHg^{-1}$$

$$aH = bH, \quad \text{即 } a \in bH$$

### Sylow 定理的第二部分

$G$  是有限群,  $p$  是素数,  $p^k \mid |G|$ ,  $p^{k+1} \nmid |G|$ , ( $G$  的任一  $p^k$  阶子群称为  $G$  的一个 Sylow- $p$  子群), 则:

(1) 若  $H, K$  是两个 Sylow- $p$  子群, 则  $\exists g \in G$ , s.t.  $K = gHg^{-1}$ .

(2) 设  $A$  是  $G$  的  $p$ -子群, 则  $\exists H$  是  $G$  的 Sylow- $p$  子群, s.t.  $A \leq H$ .

证: (1)  $K$  是  $p$ -子群,  $p \nmid \frac{|G|}{|H|}$ . 则  $\exists g \in G$ , s.t.  $K \leq gHg^{-1}$ .

$$\text{但 } |K| = |gHg^{-1}| = |H| \quad \therefore K = gHg^{-1}$$

(2) 取一个  $G$  的 Sylow- $p$  子群  $L$ ,  $A$  是  $p$ -子群,  $p \nmid \frac{|G|}{|L|}$ .

$$\therefore \exists g \in G, \text{s.t. } A \leq gLg^{-1} \rightarrow \text{Sylow-}p \text{ 子群.}$$

$$|K| = |H| = p^k$$

	<p>Sylow 定理第一部分</p> <p>设 <math>G</math> 是有限群, <math>p</math> 是素数, <math>p^l \mid  G </math>, <math>l \geq 1</math>.</p> <p>则 <math>G</math> 的 <math>p^l</math> 阶子群的个数模 <math>p</math> 余 1, 即 <math> \{A \mid A \leq G,  A =p^l\}  \equiv 1 \pmod{p}</math>. <math> G =n</math>.</p> <p>证: <math>T = \{A \mid A \leq G,  A =p^l\}</math></p> <p><math>G</math> 依左乘作用在 <math>T</math> 上. <math>(g \rightarrow A = gA = \{ga \mid a \in A\})</math></p> <p>记 <math>L_1, L_2, \dots, L_m</math> 为该作用下的轨道全体.</p> <p>对任一轨道 <math>U</math>, 下面2种情况之一成立.</p> <p>(1) <math>U</math> 中恰含一个 <math>p^l</math> 阶子群, 并且 <math> U  = \frac{n}{p^l}</math>.</p> <p>(2) <math>U</math> 中不含 <math>p^l</math> 阶子群, 并且 <math>\frac{n}{p^{l-1}} \mid  U </math>.</p> <p>不妨设 <math>L_1, \dots, L_k</math> 中每个恰含一个子群, <math>L_{k+1}, \dots, L_m</math> 中均不含子群 (故 <math>G</math> 恰有 <math>k</math> 个 <math>p^l</math> 阶子群)</p> <p><math>\forall 1 \leq i \leq k,  L_i  = \frac{n}{p^l}, \forall k+1 \leq i \leq m \quad \frac{n}{p^{l-1}} \mid  L_i </math></p> <p><math> T  =  L_1  +  L_2  + \dots +  L_m  = k \frac{n}{p^l} + w \frac{n}{p^{l-1}}, w \in \mathbb{N}</math>.</p> <p>另一方面, <math> T  = C(n, p^l)</math></p> <p><math>C(n, p^l) = k \frac{n}{p^l} + w \frac{n}{p^{l-1}}</math>, 两边同 <math>\div \frac{n}{p^l}</math></p> <p><math>C(n-1, p^l-1) = k + wp</math>, 两边 mod <math>p</math>.</p> <p><math>k \equiv C(n-1, p^l-1) \equiv 1 \pmod{p}</math></p> <p>#.</p>
任何群作用共有 左乘特有	<p><math>G</math> 群, <math>G</math> 依左乘作用在其子集上. <math>g \rightarrow A = \{ga \mid a \in A\} = gA</math>.</p> <p>对 <math>A \leq G</math>, <math>A</math> 所在的轨道 <math>= \{gA \mid g \in G\}</math></p> <p><math>\text{stab}(A) = \{g \mid g \in G, gA = A\}</math></p> <p>对 <math>H \leq G</math>, <math>H</math> 所在的轨道 <math>= \{gH \mid g \in G\}</math></p> <p><math>\text{stab}(H) = H</math></p>

$(\forall g \in G, gH = H \Leftrightarrow g \in H)$   
对  $A \subseteq G, A \leq G \Leftrightarrow A = \text{stab}(A)$  ( $\Rightarrow \vee$   
 $\Leftarrow \text{stab}(A) \leq G$ )

事实.  $A \subseteq G$ , 令  $H = \text{stab}(A)$ , 则  $A = HA$ .

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

而  $\forall h \in H, ha = a$ . ( $H = \text{stab}(A)$ ,  $ha = a$ ).

$A \subseteq G, H = \text{stab}(A)$ , 则  $A = HA$  ( $H \leq G$ )

$$HA = \{ha \mid h \in H, a \in A\} = \bigcup_{a \in A} Ha \rightarrow -\text{一些右陪集 (与左陪集完全对称)}$$

且  $\forall a, b \in A$ , 要么  $Ha = Hb$ , 要么  $Ha \cap Hb = \emptyset$

$$A = \bigcup_{a \in A} Ha \text{ 不交并}$$

事实. 设  $A \subseteq G$ ,  $A$  有限,  $H = \text{stab}(A)$ , 则  $|H| \mid |A|$ .

进一步地,  $A \subseteq G$  当且仅当  $\{g \in A\}$  并且  $|H| = |A|$ .

$$|A| = \text{若干个 } |Ha| \text{ 之和, 每个 } |Ha| = |H| \Rightarrow |H| \mid |A|$$

若  $A \subseteq G, \{g \in A\} = \text{stab}(A) = H$ .

若  $\{g \in A\} = |H|$ ,  $A = \bigcup_{a \in A} Ha \text{ 不交并}, |H| = |A|$

对每个  $a \in A, Ha \subseteq A, |A| = |Ha| \therefore A = Ha$ .

$$\{g \in A\} = H \quad \therefore A = H$$

看轨道  $U$  ( $U = \{ga \mid g \in G\}$  对某个  $A \subseteq G$ )  $U \neq \emptyset$

设  $U$  中有一个  $G$  的子群  $H$   $U = \{gh \mid g \in G\} = G/H$

若  $g \in G, gh \in G \Rightarrow \{g\} \in gh \Rightarrow gh = H$  // $\exists$  有一个子群, 无 2 个及以上

此时  $|U| = |G/H| = \frac{|G|}{|H|}$

书上 Sylow 定理证明：

对  $|G|$  归纳

设  $U$  中不含  $G$  的子群。

可以取到  $A \in U$ , s.t.  $\{g \in A \mid A' \subseteq U, \forall a \in A', g^{-1}A' \subseteq U, |g \in g^{-1}A'\}$

$$U = \{gA \mid g \in G\}, |U| = \frac{|G|}{|\text{stab}(A)|}, \text{而 } |\text{stab}(A)| \mid |A|. |\text{stab}(A)| \neq |A|$$

真因子

$U$  无子群,  $A$  不是子群

### 环

$(\mathbb{Z}, +, \cdot)$

$(\mathbb{Z}, +)$  是交换群

$(\mathbb{Z}, \cdot)$  么半群

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

$$(ab) \cdot c = a(bc)$$

$$a+0 = 0+a=a$$

$$a \cdot 1 = 1 \cdot a$$

$$a+(-a) = (-a)+a = 0$$

// 做不到群，除 1, -1 外无逆元

$$a+b=b+a$$

分配律

$$a(b+c) = ab+ac$$

$$(a+b)c = ac+bc$$

定义。称代数结构  $(R, +, \cdot)$  是环，若：

(1)  $(R, +)$  是交换群，其么元记为  $0$  // 若仅要求群，记为 (1)

(2)  $(R, \cdot)$  是么半群，其么元记为  $1_r$  // 各书 def 不同，有些不要求么元

(3) 分配律  $\forall a, b, c \in R$

$$a(b+c) = ab+ac \quad (a+b)c = ac+bc.$$

(4) 若  $\forall a, b \in R$ , 均有  $ab=ba$ , 则称  $(R, +, \cdot)$  是交换环

则 (1)+(2)+(1)  $\Rightarrow (R, +)$  是交换群

即 (1)+(2)+(3)  $\Rightarrow (1)+(2)+(3)$

e.g. 偶数全体  $\{2a \mid a \in \mathbb{Z}\}$

无么元，其余均满足

\* 任何环可通过单同态映射到有么元的环上，于是 def 有么元不失一般性

若和所有矩阵都可交换, $\begin{pmatrix} a & a & 0 \\ 0 & a & a \\ 0 & 0 & \dots \end{pmatrix}$		eg. $M_n(\mathbb{R})$ : $\mathbb{R}$ 上全体n阶矩阵 ( $M_n(\mathbb{R}), +, \cdot$ ) 环 $n \geq 2$ , 不是交换环 eg. $n \in \mathbb{Z}^+$ , $(\{0, 1, \dots, n-1\}, \oplus, \otimes)$ //有限环位数例子 $a \oplus b = (a+b) \% n$ 有限群 ✓ 但无限环常见 $a \otimes b = (ab) \% n$
费马大定理: $x^n + y^n = z^n$		$n \geq 3$ 无整数解
群	环	$n \geq 2$ 时, 做成交换环
子群	子环	eg. $\mathbb{R}$ 上的n阶上三角矩阵 $\begin{pmatrix} * & * & * \\ 0 & * & * \\ * & 0 & * \end{pmatrix}$ //矩阵环的子环
商群	商环	eg. 实数序列 $(a_0, a_1, a_2, \dots, a_n, \dots)$
同态	同态	$R = \{(a_0, a_1, \dots, a_n, \dots) \mid \text{每 } a_i \in \mathbb{R}\}$
正规子群	理想	$(a_0, a_1, \dots) + (b_0, b_1, \dots) = (a_0+b_0, a_1+b_1, \dots)$ 交换群 ✓
多项式环		$(a_0, a_1, \dots)(b_0, b_1, \dots) = (c_0, c_1, \dots)$
$c_0 = a_0 b_0$		
$c_1 = a_0 b_1 + a_1 b_0$		
$c_2 = a_0 b_2 + a_1 b_1 + a_2 b_0$		
- - - -		
$c_n = \sum_{i=0}^n a_i b_{n-i} = a_0 b_n + a_1 b_{n-1} + \dots + a_{n-1} b_1 + a_n b_0$		
$(\sum_{i=0}^{\infty} a_i x^i) + (\sum_{i=0}^{\infty} b_i x^i)$		
$(1, 0, 0, \dots)$ 不是元可以写成 $x = (0, 1, 0, \dots)$		