

§1 群
(G, ·) group of.

1. 结合律

2. 有左单位元 e : $ea = a \quad \forall a \in G$

3. 有左逆元 a^{-1} , $a^{-1}a = e$

群 $\leftrightarrow$ 对称 $\leftrightarrow$ 美

平面图形 M 的一个对称是指一个保距-变换: $f: P \rightarrow P$
s.t. $f(M) \in M, \forall M \in M$. $S(M) = \{M \text{ 的对称} \}$

$$S(\text{圆}) = \{e^{i\theta}, \theta \in [0, 2\pi)\} \quad S(\text{正方形}) = D_4 \quad (8 \text{ 个元素})$$

$$S_3 = \{(1), (12), (13), (23), (123), (132)\}$$

$(S_3, \cdot)$ 三次对称群

Lemma 2:

设 $(G, \cdot)$ 是半群, 则 $(G, \cdot)$ 是群 $\Leftrightarrow$

$\Leftrightarrow$ 方程 $ax = b$ 和方程 $ya = b$ 在 G 中有解.

证: " $\Rightarrow$ " 显然

" $\Leftarrow$ " 取 $a \in G$, 设 e 是 $ya = a$ 的一个解 (在 G 中)

$\forall g \in G$, 设 e 是 $ya = a$ 的一个解.

设 $g = ax$ 有解 $b \in G$.

$$\text{则 } eg = e(ab) = (ea)b = ab = g \Rightarrow \text{有左单位元.}$$

又 $yg = e$ 有解. $\Rightarrow$ 有右逆元.

综上, $(G, \cdot)$ 是群.

引理3. 设 $(G, \cdot)$ 有限半群, 则 $(G, \cdot)$ 是群.

($\Rightarrow$) $(G, \cdot)$ 有左、右消去律

证: " $\Rightarrow$ " 显然

" $\Leftarrow$ " 设 $G = \{a_1, \dots, a_n\}$

$$\forall a \in G, aG = \{aa_1, \dots, aa_n\} = G.$$

则 $ax=b$ 在 G 中有解. $\forall a, b \in G$

同理 $ya=b$ 在 G 中有解.

据引理2. (G) 是群.

§2 子群和 Lagrange 定理.

Def: 设 $(G, \cdot)$ 是群, $\emptyset \neq H \subseteq G$, 称 H 为 G 的子群.
若 $(H, \cdot)$ 也是群, 记为 $H \leq G$.

$S_n(R)$

引理. 设 $(G, \cdot)$ 是群, $\emptyset \neq H \subseteq G$, 则 $H \leq G$

$\Leftrightarrow$ 对 $\forall a, b \in H$, 均有 $a^{-1}b \in H$.

证: " $\Rightarrow$ " 显然

" $\Leftarrow$ " 取 $a \in H$. $a^{-1}a = e \in H$

$\forall g \in H$ 则 $g^{-1} \cdot e = g^{-1} \in H$.

$\forall a, b \in H$, $a^{-1} \in H, b \in H$. $(a^{-1})^{-1}b = ab \in H$.

故又知 $(H, \cdot)$ 是群. $\#$

引理: 设 G 是群, $H, K \leq G$, 则 $HK \leq G \Leftrightarrow HK = KH$

" $\Rightarrow$ " 设 $HK \leq G$, 则 $(HK)^{-1} = HK$. 即 $K^{-1}H^{-1} = HK$
即 $KH = HK$

" $\Leftarrow$ " 设 $h_1 k_1, h_2 k_2 \in HK, h_1, h_2 \in H; k_1, k_2 \in K$

$$(h_2 k_2)^{-1} (h_1 k_1) = k_2^{-1} (h_2^{-1} h_1) k_1 \in K \cdot H \cdot K = K(HK) = (KK)H \subseteq KH$$

同时 $G \cdot KH \cdot K = HK \subseteq HK$ #

P.17 / 4, 6, 7 P.11/13 (近世代数引理).

§2 子群和 Lagrange 定理.

宋林 1367184329

zhulinh2323@gmail.com

熊伟林 13585853915

xiongbaolin@gmail.com

设 $\sim$ 是 S 上一个关系. 称 $\sim$ 是等价关系, 如果

(1) 自反性: $a \sim a \quad \forall a \in S$

(2) 对称性: $a \sim b \Rightarrow b \sim a$

(3) 传递性 $a \sim b, b \sim c \Rightarrow a \sim c$.

引理: {集合 S 上的等价关系} $\longleftrightarrow$ {集合 S 上的划分}.

证: $\sim \mapsto S = \bigcup_{a \in S} \{x \in S \mid x \sim a\}$. 反之亦然

其实这个引理不证自明.

设 $H \leq G$ 在 G 上定义关系 $\sim: a \sim b \Leftrightarrow a^{-1}b \in H$.

验证 " $\sim$ " 是等价的. (1) $a^{-1}a \in H \quad \forall a \in G$.

(2) $a^{-1}b \in H \Rightarrow b^{-1}a \in H$.

(3) $a^{-1}b \in H, b^{-1}c \in H \Rightarrow a^{-1}c \in H$.

于是 " $\sim$ " 引起了一个划分.

$a \cdot H = \{ah / h \in H\}$
称为 H 的一个左陪集.

$$[a] = \{x \in G \mid a^{-1}x \in H\} = \{x \in G \mid x \in aH\}.$$

$G = \bigcup_{a \in G} aH$. (左陪集的无交之并) a 是一个左陪集的代表元
称为左陪集代表元系

即要么 $aH \cap bH = \emptyset$ 要么 $aH = bH$.

Lagrange 定理.

设 $H \leq G$, a 是 G 关于 H 的左陪集的代表元.

则 $|G| = |H| \cdot |L|$. 特别地 $|H| \mid |G|$. (无限群也对, 但对有限群有意义)

$$\text{证: } |G| = \sum_{a \in L} |aH| = \sum_{a \in L} |H| = |H| \cdot |L|. \quad \#$$

(所有组员数 = 每组组员数 · 组长数) #

即子群的阶 | 群的阶.

同样地我们可以定义右陪集

$$G \equiv \bigcup_{a \in R} Ha$$

$$G = \bigcup_{a \in L} aH \Leftrightarrow G = \bigcup_{a \in L} aHa^{-1}$$

特别地 $|L| = |R|$

例1. $G = GL_n(R)$ $H = \{ I_n \}$, $H \leq G$.

$$G = \bigcup_{a \in R^*} \begin{pmatrix} a & \\ & 1 \end{pmatrix} SL_n(R).$$

例2. 设 $G = S_3$ $H = \{ (1) (12) (13) (23) (123) (132) \}$.

$$H = \{ (1) (12) \} \leq G. \quad \cancel{H = H \cup \{ (12) \}}$$

$$G = H \cup (13)H \cup (12)H.$$

例3. 设 $H, K \leq G$. $|HK| = \frac{|H| \cdot |K|}{|H \cap K|}$

证: 令 $X = HK$ 则 $|X| = |H| \cdot |K|$

fibonacci

设 $h'k' = hk \Rightarrow h^{-1}h' = k k'^{-1} \in H \cap K$

即 $h' = ht, k' = t^{-1}k$.

$$(h', k') = (ht, t^{-1}k) \in H \cap K$$

反之亦然

$$\text{即有 } |HK| = \frac{|H| \cdot |K|}{|H \cap K|}$$

6

设 G 是群, $g \in G$ 定义 g 的阶 $o(g)$ 是使得 $g^{o(g)} = 1$ 的最小正整数.
若不存在, 则定义 $o(g) = \infty$.

引理. 设 g 是群, $g \in G$, 则 $o(g) \mid |G|$

$$\langle g \rangle = \{g^i \mid i = 0, \pm 1, \dots\} \leq G.$$

$$|\langle g \rangle| = o(g).$$

引理: 设 G 是群, $g \in G$, $m \in \mathbb{N}$

$$\text{则 (1) } o(g^m) = \frac{o(g)}{(o(g), m)}.$$

$$(2) o(a) = n, o(b) = m, (a, b) = 1 \quad ab = ba$$

$$\text{则 } o(ab) = n \cdot m$$

证. (1) 设 $o(g^m) = t, o(g) = n$.

$$(g^m)^t = 1 \Rightarrow g^{mt} = 1 \quad \text{由 } o(g) = n \quad \text{故 } n \mid mt.$$

$$\frac{n}{(n, m)} \mid \frac{m}{(n, m)} t \quad \text{故 } \frac{n}{(n, m)} \mid t.$$

$$\left(\frac{n}{(n, m)}, \frac{m}{(n, m)}\right) = 1.$$

$$(g^m)^{\frac{n}{(n, m)}} = (g^n)^{\frac{m}{(n, m)}} = 1 \quad \text{故 } o(g^m) = t$$

$$\text{所以 } t \mid \frac{m}{(n, m)} \quad \text{故 } t = \frac{n}{(n, m)} \quad \#$$

§3 类方程

$$a \sim b \Leftrightarrow \exists g \in G \text{ s.t. } b = g^{-1}ag \quad (\text{共轭关系})$$

$$[a] = \{g^{-1}ag \mid g \in G\} \quad \text{共轭类}$$

$$C_G(a) = \{x \in G \mid xa = ax\} \leq G \quad \text{称为 } a \text{ 在 } G \text{ 中的中心化子}$$

(验证 $C_G(a)$ 是子群)

$$| [a] | = [G : C_G(a)] = \frac{|G|}{|C_G(a)|}$$

$$\text{证: } g^{-1}ag = h^{-1}ah \Leftrightarrow (hg^{-1})a = a(hg^{-1}) \Leftrightarrow hg^{-1} \in C_G(a).$$

$$\Leftrightarrow C_G(a)h = C_G(a)g.$$

$$G = \bigcup_{a \in R} [a]$$

$$C(G) = \{g \in G \mid gx = xg, \forall x \in G\} \leq G. \quad \text{称为 } G \text{ 的中心}$$

$$G \text{ Abel} \Leftrightarrow C(G) = G.$$

$$C(G) = \bigcap_{a \in G} C_G(a). \quad a \in C(G) \Leftrightarrow |[a]| = 1$$

$$G = \bigcup_{a \in R} [a] = C(G) \bigcup_{\substack{a \in R \\ a \notin C(G)}} [a]$$

$$|G| = |C(G)| + \sum_{\substack{a \in R \\ a \notin C(G)}} \frac{|G|}{|C_G(a)|} \quad \text{这就是类方程.}$$

定理: p -群有非平凡的中心 ($|G|=p^n$, p 素数, $n \geq 1$ 称为 p -群)

非平凡就是严格包含单位元 (还有别的元)

证: 由类方程 $|G| = |C(G)| + \sum_{\substack{a \in R \\ a \notin C(G)}} \frac{p^n}{|C_G(a)|}$

若 $|C(G)|=1$, 则 $p^n = 1 + \sum_{\substack{a \in R \\ a \notin C(G)}} \frac{p^n}{|C_G(a)|}$ 矛盾! $\#$

例: p^2 阶群是 Abel 群, p 素

证: 设 $|G|=p^2$ 不妨设 G 中无 p^2 阶元.

取 $g \in C(G)$. ~~且 $g \neq 1$~~ 且 $g \neq 1$. (由 p -群有非平凡的中心)

令 $H = \langle g \rangle$, $|H|=p$ ($\because |H| \mid |G|$, $|H| \neq 1$, $|H| \neq p^2$).

取 $b \notin H$, $b \in G$. 则 $o(b) = p$.

则 $G = H \cup bH \cup b^2H \cup \dots \cup b^{p-1}H$

(设 $b^i H = H$ 则 $b^i \in H$, $0 \leq i \leq p-1$ (i, p)=1).

则 $\exists \cdot \lim$ 使 $il + pm = 1$, $b = (b^i)^l \cdot (b^p)^m \in H$

故 $\forall x \in G$, ~~$x = b^i g$~~ 可交换 $\#$

$x = b^i h$, $y = b^j h'$

$h \in H \subseteq C(G)$

为群)

§4 循环群

群 G 称为循环群, 如果 $\exists g \in G$ st $G = \langle g \rangle = \{g^i \mid i \in \mathbb{Z}\}$

$\neq G = \langle g \rangle$, 则 $|G| = o(g) = |\langle g \rangle|$

例 $(\mathbb{Z}, +, 0) = \langle 1 \rangle$

$$a \equiv b \pmod{n} \quad n > 0 \Leftrightarrow a \sim b$$

$$[a] = \{a + qn \mid q \in \mathbb{Z}\} \quad \mathbb{Z} = \{\bar{0}, \bar{1}, \dots, \overline{n-1}\}$$

商集.
($\mathbb{Z}$ 是 $\mathbb{Z}$ 的
剩余类)

$(\mathbb{Z}_n, +, \bar{0})$ 也是群.

定义 $\bar{a} + \bar{b} = \overline{a+b}$ (与代表元无关)

设 G, G' 是群. $f: G \rightarrow G'$ 映射.

称 f 为群同态, 如果 $f(ab) = f(a) \cdot f(b) \quad \forall a, b \in G$.

设 f 是群同态.

若 f 还是单射, 则称 f 是单同态

若 f 还是满射, 则称 f 是满同态 (homomorphism).

若 f 还是双射, 则称 f 是同构 (isomorphism).

例: $(GL_n(\mathbb{R}), \cdot, I) \longrightarrow (\mathbb{R}^*, \cdot, 1)$

$\downarrow$ 矩阵乘法 $\downarrow$ 单位矩阵 $\downarrow$ 正实乘法 $\downarrow$ 数 1.

$M \mapsto |M|$ 是满同态 (因为 $|M \cdot N| = |M| \cdot |N|$)

$(\mathbb{R}, +, 0) \xrightarrow{+} (\mathbb{R}^*, \cdot, 1) \quad x \mapsto e^x$ 是群同态

循环群的结构定理:

1. 无限循环群均同构于 $(\mathbb{Z}, +, 0)$.

n 阶循环群均同构于 $(\mathbb{Z}_n, +, 0)$ (剩余类加群)

2. 设 $G = \langle g \rangle$ 若 $o(g) = \infty$, 则 $\langle g^m \rangle, m = 0, 1, \dots$ 就是 G 的全部

两两不同的子群. 若 $o(g) = n$, 则 $\langle g^m \rangle, m = 0$ 或 $1 \leq m < n, m|n$

是 G 的全部两两不同的子群.

循环群的子群也是循环群.

例 $\mathbb{Z}_{12}$ 的子群: $\mathbb{Z}_{12} = \langle 1 \rangle$, 子群: $\{\bar{0}\}, \langle \bar{2} \rangle, \langle \bar{3} \rangle, \langle \bar{4} \rangle, \langle \bar{6} \rangle, \langle \bar{1} \rangle$
(这里 $\{\bar{0}\} = \langle \bar{12} \rangle$)

证. $H \leq G = \langle g \rangle$. 设 m 是使得 $g^m \in H$ 的最小正整数.

则 $H = \langle g^m \rangle$ (带余除法)

P20 / 1, 2, 7. P16 定理 5.

§5 正规子群. 商群. 群同态基本定理.

设 $H \leq G$. 一般地 $gH \neq Hg$. 其中 $g \in G$.

例 $G = S_3$, $H = \{(1), (12)\} = \langle (12) \rangle$

而 $(2,3)H \neq H(2,3)$

引理: 设 $N \leq G$, 则下述等价:

(1) $gN = Ng \quad \forall g \in G$.

(2) $g^{-1}Ng \leq N, \quad \forall g \in G$

(3) $gNg = N, \quad \forall g \in G$

(4) $gng \in N, \quad \forall g \in G \quad \forall n \in N$

(5) N 的任一左陪集均是右陪集.

若其中任一成立, 则称 N 是 G 的正规子群, 记为 $N \trianglelefteq G$

证: (1) $\Rightarrow$ (2) 显然

(2) $\Rightarrow$ (3) 由 (2) $gNg^{-1} \leq N \Rightarrow N \subseteq g^{-1}Ng$.

(3) $\Rightarrow$ (4) 显然.

(4) $\Rightarrow$ (1) 显然

(1) $\Rightarrow$ (5) 显然.

(5) $\Rightarrow$ (1) 设 $g \in G$, 则 $\exists h \in G$ 使 $gN = Nh$.

~~$h \in N$~~ 则 $g \in gN = Nh$. $\therefore g = n \cdot h$.

于是 $Ng = N(n \cdot h) = (N \cdot n) \cdot h = Nh = gN$ ~~Ng~~ ~~h~~ ~~$*$~~

例: (1) Abel 群中任何子群均正规

(2) $C(G) \trianglelefteq G$

(3) $S_n(R) \trianglelefteq GL_n(R)$

(4) 设 $N \leq G$. 且 $[G:N] = 2$ 则 $N \trianglelefteq G$

12

设 $N \leq G$, 考虑左陪集之集 $G/N = \{gN \mid g \in G\}$

希望 $(gN)(hN) = (gh)N \quad \forall g, h \in G$

7/10 $gN = g'N$; $hN = h'N$ $\Rightarrow (gh)N \neq (g'h')N$ (*)

~~is " " A A A~~

对于 $\begin{cases} gN = g'N \\ hN = h'N \end{cases}$ 有 $(gh)N = (g'h')N$

$$(g'h')N = (g_n, h_n)N = (g_n, h)N = (g_n h_3)N$$
$$= (gh)N.$$

" $\Leftarrow$ " 设 $gN = g'N$ 和 $hN = h'N$ 可以推出 $(gh)N = (g'h')N$

设 $n \in N, g \in G$, 则 $N = nN, \cancel{gNg^{-1}} \Rightarrow gN = (ng)N$
 $gN = gN$

即 $g^{-1}ng \in N$. 即 $N \triangleleft G$

引理. 设 $N \triangleleft G$. 则 $(G/N, \cdot)$ 是群. 称为 G 关于 N 的商群.

结合律. 显然

~~单位元~~ N . 逆元为 $(g^{-1}N)$

例: 设 $N \triangleleft G$. 则有群满同态 $G \xrightarrow{\pi} G/N$

$f: G \rightarrow G'$ 群同态.

定义 $\ker f = \{x \in G \mid f(x) = 1\}$. 容易验证 $\ker f \triangleleft G$

(先证 $\ker f \leq G$. $\forall f(n_1) = 1, f(n_2) = 1$

$$f(n_1^{-1}n_2) = f(n_1)^{-1} \cdot f(n_2) = 1.$$

$\forall n \in \ker f \quad \forall g \in G$ 则 $g^{-1}ng \in \ker f$:

$$f(g^{-1}ng) = f(g)^{-1} \cdot f(n) \cdot f(g) = f(n) = 1 \text{ 故 } \ker f \text{ 正规}$$

且 f 是单射 $\Leftrightarrow \ker f = \{1\}$

" $\Rightarrow$ " 显然

" $\Leftarrow$ " 设 $f(x) = f(y), x, y \in G$. 则 $f(x^{-1}y) = (f(x))^{-1}f(y) = 1$

于是 $x^{-1}y = 1 \Rightarrow x = y$

~~$\ker \pi = \{xN \mid xN = N\}$~~

$$\ker \pi = \{x \in G \mid xN = N\} = \{x \in G \mid x \in N\} = N$$

~~满同态~~ 群同态基本定理.

设 $f: G \rightarrow G'$ 是群同态.

$$\text{Im}(f) = \text{Im } f = \{f(x) \in G' \mid x \in G\}.$$

$$f \text{ 满} \Leftrightarrow \text{Im } f = G' \quad \text{Im } f \leq G'$$

~~则有群同态~~

定理: 设 $f: G \rightarrow G'$ 是群同态, 则 $\ker f \trianglelefteq G$

且有群同构 $\text{Im } f \cong G / \ker f$ 特别地, 若 f 满, 则 $G' \cong G / \ker f$

$$\text{例) (1) } \pi: GL_n(R) \longrightarrow R^* \\ m \longmapsto |m|$$

π 是群同态

$$\ker \pi = SL_n(R) \trianglelefteq GL_n(R).$$

$$\text{故 } GL_n(R) / SL_n(R) \cong (R^*, \cdot)$$

$$(2) \pi: (\mathbb{Z}, +, 0) \longrightarrow (\mathbb{Z}_n, +, \bar{0}) \\ m \longmapsto [m]$$

π 是群满同态 则 $\ker \pi = n\mathbb{Z}$.

$$\text{故 } \mathbb{Z}_n \cong \mathbb{Z} / n\mathbb{Z}.$$

定理的证明: 令 $\tilde{f}: G/\ker f \rightarrow \text{Im } f$

$$x \ker f \mapsto f(x)$$

则 $\tilde{f}$ 是映射

$\tilde{f}$ 是群同态

$\tilde{f}$ 满

$\tilde{f}$ 单

设 $x' \ker f = x \ker f$ 即 $x' = xn$

子群对应定理: 设 $N \trianglelefteq G$, 令 $\mathcal{P} = \{ G \text{ 的子群 } H, \text{ 且 } H \supseteq N \}$
 $\mathcal{Q} = \{ G/N \text{ 的子群} \}$

$$\psi: \mathcal{P} \xrightarrow{1-1} \mathcal{Q}$$

$$H \mapsto H/N$$

且 $H/N \trianglelefteq G/N \iff H \trianglelefteq G$

(1) ψ 是映射 (2) ψ 是单射 (3) ψ 是满射

$$\overline{H} \subseteq G/N \rightarrow G$$

设 $N \trianglelefteq G$, 则有商群 $G/N = \{ gN = Ng, g \in G \}$ 令 $\bar{g} = gN$.

G/N 乘法: $\bar{g} \cdot \bar{h} = \overline{gh}$

$G \rightarrow G/N$ 群满同态. $\ker \pi = N$

群同态基本定理: 设 $f: G \rightarrow G'$, 则 $\text{Im } f \cong G/\ker f$

特别地, 若 f 满, $G' \cong G/\ker f$.

子群对应定理, 设 $N \trianglelefteq G$, 令 $\mathcal{T} = \{ G \text{ 的子群 } H, H \supseteq N \}$

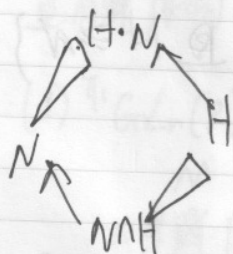
$\Omega = \{ \text{子群} \}$ 则有 1-1 对应.

$$\begin{aligned} \Gamma &\rightarrow \Omega \\ H &\mapsto H/N \end{aligned}$$

$$H/N \trianglelefteq G/N \iff H \trianglelefteq G$$

第一同构定理: 设 $N \trianglelefteq G, H \leq G$. 则 $N \cap H \trianglelefteq H, N \trianglelefteq NH = HN$.

且有群同构 $H \cdot N / N \cong H / (H \cap N)$



证: 考虑 $H \rightarrow H \cdot N / N$

$$h \mapsto h \cdot N \quad \pi \text{ 是群同态, 且满}$$

$$\text{由群同态基本定理 } H \cdot N / N \cong H / \ker \pi = H / (H \cap N) \neq$$

第二同构定理: 设 $A \trianglelefteq B, B \trianglelefteq G, A \trianglelefteq G$. 则:

$$B/A \trianglelefteq G/A \text{ 且有群同构 } (G/A) / (B/A) \cong G/B$$

(注意正规子群没有传递性)

证: 考虑 $\pi: G/A \rightarrow G/B$ π is well defined
 $gA \mapsto gB$

(因为若 $gA = g'A \Rightarrow g^{-1}g' \in A \Rightarrow g^{-1}g' \in B \text{ (} A \trianglelefteq B \text{)} \Rightarrow gB = g'B$)

$$\ker \pi: \{ gA \in G/A \mid gB = B \} \text{ 即 } \{ gA \in G/A \mid g \in B \} \\ = B/A$$

由同态基本定理知 $(G/A)/(B/A) \cong G/B$.

例 设 $m\mathbb{Z} \triangleleft n\mathbb{Z} \triangleleft \mathbb{Z}$. 其中 $n|m$, 则

$$(\mathbb{Z}/m\mathbb{Z}) / (\frac{n\mathbb{Z}}{m\mathbb{Z}}) \cong \mathbb{Z}/n\mathbb{Z} \quad \text{即} \quad \mathbb{Z}_n \cong \mathbb{Z}_m / \mathbb{Z}_{\frac{m}{n}}$$

$\mathbb{Z}_n$ 是 $\frac{m}{n}$ 阶循环群 $\cong \mathbb{Z}_{\frac{m}{n}}$

例: ~~$(\mathbb{Q}, +) \cong (\mathbb{Q}^*, \cdot)$~~

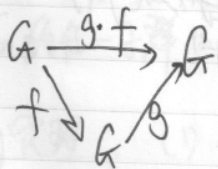
例 $(\mathbb{Q}, +) \not\cong (\mathbb{Q}^*, \cdot)$

证: 反设 $f: (\mathbb{Q}, +) \xrightarrow{\sim} (\mathbb{Q}^*, \cdot)$

则存在 $a \in \mathbb{Q}$, $2 = f(a)$ 于是 $2 = f(a) = f(\frac{a}{2} + \frac{a}{2})$

$$= f(\frac{a}{2}) f(\frac{a}{2}) = (f(\frac{a}{2}))^2 \quad \text{矛盾!} \quad \#$$

群 G , $\text{Aut}(G) = \{f: G \xrightarrow{\sim} G\}$, 称为 G 的自同构群.
(Automorphism) group. 单位元是恒等同构



例: 计算 $\text{Aut}(\mathbb{Q}, +) \cong (\mathbb{Q}^*, \cdot)$

一般地 $\text{Aut } G \not\cong G$ 不成立.

证: $\forall f \in \text{Aut}(\mathbb{Q}, +)$ 令 $f(1) = a \in \mathbb{Q}^*$

$$\text{则 } f(x) = ax, \forall x \in \mathbb{Q}$$

设 $a \in \mathbb{Q}^*$, 令 $f_a: (\mathbb{Q}, +) \rightarrow (\mathbb{Q}, +)$

$$x \mapsto ax$$

$$\text{即 } f_a(x) = xa.$$

$$\text{则 } f_a \in \text{Aut}(\mathbb{Q})$$

$$\text{综上, } \text{Aut}(\mathbb{Q}, +) = \{f_a \mid a \in \mathbb{Q}^*\}$$

$$\text{于是: } \text{Aut}(\mathbb{Q}, +) \xrightarrow{\sim} (\mathbb{Q}^*, \cdot) \quad *$$

$$f_a \mapsto a$$

内自同构: $p_g: G \rightarrow G$

$$x \mapsto g^{-1}xg$$

$$\text{令 } \text{Inn}(G) = \{p_g: G \xrightarrow{\sim} G \mid g \in G\} \subseteq \text{Aut}(G)$$

$$\text{且 } \text{Inn}(G) \leq \text{Aut}(G).$$

$$\cancel{p_h \cdot p_g = h^{-1}g^{-1}xgh = (gh)^{-1}x(gh) = p_{hg}}$$

$$p_h \cdot p_g: x \mapsto g^{-1}xg^{-1} \mapsto hg^{-1}xg^{-1}h^{-1} \quad \cancel{p_{hg}}$$

$$= (hg)^{-1}x(hg) = p_{hg}$$

$$\text{即 } p_h \cdot p_g = p_{hg}, \quad (p_g)^{-1} = p_{g^{-1}}$$

$$\text{Inn}(G) \cong \frac{G}{C(G)}$$

19

证: $G \xrightarrow{\pi} \text{Inn}(G)$
 $g \mapsto \rho_g$ 满.

$$\pi(gh) = \rho_{gh} \quad \Rightarrow \text{是同态}$$

$$\pi(g) \cdot \pi(h) = \rho_g \rho_h$$

$$\ker \pi = \{g \in G \mid \rho_g = \text{id}_G\} = c(G) \quad (x \mapsto g x g^{-1} = x \Rightarrow gx = xg)$$

由群同态基本定理 $\text{Inn}(G) \cong G/c(G)$.

例: G 不是 Abel 群, 则 $\text{Aut}(G)$ 不是循环群.

证: 反证: 若 $\text{Aut}(G)$ 是循环群, 则 $\text{Inn}(G)$ 是循环群.
 即 $G/c(G)$ 循环群. 即 G 是 Abel 群. $\text{Inn}(G) \leq \text{Aut}(G)$

§6 置换群 Permutation Group.
 变换群 $G \leq \text{GL}(V) = \text{GL}(n)$ $\dim V = n$

n 集合: $S(n) \stackrel{\text{def}}{=} \{f: X \rightarrow X, \text{ 且 } f \text{ 是 } 1-1 \text{ 映射}\}.$
 $(S(n), \cdot)$

$S(n)$ 的任一子群称为 n 的变换群.

若 n 有限 $n = \{1, \dots, n\}$ 记 $S(n)$ 为 S_n , 称为 n 次对称群.

S_n 的任一子群统称为置换群.

Cayley 定理: (1) 任一有限群均同构某置换群.
 (2) 任一有限群均同构某置换群.

20

证: (1) 设 G 是群, 考虑 $S(G) = \{f: G \rightarrow G, 1-1 \text{ 变换}\}$

$$\forall g \in G, \text{ 令 } l_g: G \rightarrow G \\ x \mapsto gx. \text{ 注意 } l_h \circ l_g = l_{hg}$$

$\angle G \stackrel{\text{def}}{=} \{l_g / g \in G\}$ $\angle(G)$ 是 $S(G)$ 的一个子群.

证 $G \cong \angle G$. π 是同构 (验证 (1) 单 (2) 满 (3) 群同态, 均显然). $\#$
 $g \mapsto l_g$.

$$\forall \sigma \in S_n, \sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix} \quad |S_n| = n!$$

l -轮换 $(i_1, i_2, \dots, i_l)$ 指 $i_1 \rightarrow i_2, i_2 \rightarrow i_3, \dots, i_{l-1} \rightarrow i_l, i_l \rightarrow i_1$.
 $(\text{length}) =$ 对换 (i, j)

定理: S_n 中任一置换均可写成互不相交的轮换的积. 且这种写法是唯一. 且因子之间是可换的.

证明: 任一轮换均可写成对换的乘积 (写法不唯一)

$$(i_1, \dots, i_l) = (1 \ i_1)(1 \ i_2)(1 \ i_3) \dots (1 \ i_l)$$

S_n 中元素写成对换之积时, 对换因子的个数的奇偶性不变

$$f = \prod_{1 \leq i < j \leq n} (x_i - x_j) \quad \forall \sigma \in S_n, \sigma = (s_1 \dots s_k) \text{ (对换)}$$

$$\sigma(f) = \prod (x_{\sigma(i)} - x_{\sigma(j)})$$

$$\text{验证 } \sigma(f) = \pm f$$

将能写成偶数个对换之积的置换称为偶置换.
将能写成奇数个对换之积的置换称为奇置换.

所有的偶置换作成 S_n 的一个子群, 记为 A_n , 称为 n 次交错群.

$|A_n| = \frac{n!}{2}$ 证: 设 σ 奇. 则任一奇置换 $\tau \in \sigma S_n$
 $\tau = \sigma(\sigma^{-1}\tau) \in \sigma S_n$

$[S_n : A_n] = 2$; $A_n \trianglelefteq S_n$

单群: 群 G 称为单群. 如果 $G \neq \{1\}$, G 只有两个平凡的正规子群.
 $\{1\}$ 和 G .

有限单群. 定理: 当 $n \geq 5$ 时, A_n 是单群 (书 P28 ~ 29 证明).

定理. Abel 单群必是素阶循环群.

• 阶 ≤ 1000 的非 Abel 单群只有 60, 168, 360, 504, 660 阶

• 阶 $\leq 10^6$ 的非 Abel 单群只有 53 个. 且阶均为偶数

• (W. Feit, J. Thompson) 非 Abel 单群的阶均为偶数.

Fields 奖. Abel 奖得主.

有限单群: (1) A_n : $n \geq 5$

(2) Lie 型单群.

(3) 26 个散在单群, 其中阶最大的称为魔群

阶为 $2^{46} \cdot 3^{20} \cdot 5^9 \cdot 7^6 \cdot 11^2 \cdot 13^2 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31$
 $A_1 \cdot 41 \cdot 59 \cdot 71 \sim 28 \times 10^{53}$

定理 (1) $S_n (n \geq 2)$ 由 $(12), \dots, (1n)$ 生成
 (2) $A_n (n \geq 3)$ 由 $(123), \dots, (12n)$ 生成
 3 轮换

作业: l -轮换的阶为 l

l -轮换是奇 $\Leftrightarrow l$ 偶

l -轮换是偶 $\Leftrightarrow l$ 奇

$$(ij)(st) = (isj)(st+i)$$

$$(ijk) = (12i)(12k)(12k)(12j)(12i)(12i)$$

书上有路勤作经. 学海无涯苦作舟 是不对的!

学习要有乐趣.

$$\sigma = \underbrace{(*) \dots (*)}_{\text{长度为 } l; m_1} \underbrace{(**) \dots (**)}_{\text{长度为 } 2; m_2} \dots \underbrace{(\dots)}_{\text{长度为 } n; m_n}$$

$1^{m_1} 2^{m_2} \dots n^{m_n}$ 称为 σ 的型 (type)

$$\text{且 } \sum_{i=1}^n i m_i = n$$

定理: 设 $\sigma, \tau \in S_n$ 则 σ 与 τ 共轭 $\Leftrightarrow \sigma$ 与 τ 的型相同

证: 设 σ 与 τ 的型相同. 设 $\sigma = (abc \dots) \dots (d\beta \gamma \dots)$
 $\tau = (a'b'c' \dots) \dots (d'\beta' \gamma' \dots)$
 充分性.

是互不相交轮换的分解. 于是 $\tau = ()^{-1} (abc \dots) \dots (\alpha\beta r \dots) ()$

$$\text{其中 } () = \begin{pmatrix} \alpha' b' c' \dots \alpha' \beta' r' \dots \\ a b c \dots \alpha \beta r \dots \end{pmatrix}$$

必要性: 设 σ 与 τ 共轭, 设 $\tau = \alpha^{-1} \sigma \alpha$
若 $\sigma(i) = j$, 则 τ 将 $\alpha(i)$ 变成 $\alpha(j)$

故 σ 与 τ 型相同 (你意识到了么?)

$$\sigma = \begin{pmatrix} i & s & \dots \\ j & t & \dots \end{pmatrix} \quad \tau = \begin{pmatrix} \alpha(i) & \alpha(s) & \dots \\ \alpha(j) & \alpha(t) & \dots \end{pmatrix}$$

细心是做科学的必要品质, 但不是充分的.

例: 求 S_4 中的所有正规子群.

解: 设 $H \trianglelefteq S_4$. 则由 Lagrange 定理知 $|H| = 1, 2, 3, 4, 6, 8, 12, 24$.

设 $|H| \neq 1, 24$. 则 $|H| \neq 2, 3, 6, 8$

若 $|H| = 4$, $H = \{ \{1\}, \{(12)(34), (13)(24), (14)(23)\} \}$

$|H| = 12$, $H = A_4$.

$|H| = 1$

$|H| = 2$: $(12), (13), (14), (23), (24), (34)$

$|H| = 3$: $(12)(34), (13)(24), (14)(23)$

$|H| = 4$: $(123), (134), (124), (142), (134), (143), (234), (243)$

$|H| = 6$: $(1234), (1243), (1324), (1342), (1423), (1432)$

正规子群是一些共轭类的完整并.

美题

$$24 = 1 + 6 + 3 + 8 + 6$$

24

大学要培养慧心

例 A_4 的正规子群: $\{1\}, K_4, A_4$.例 求 S_n 的正规子群 ($n \geq 5$): $\{1\}, A_n, S_n$ 设 $N \triangleleft S_n$, 且 $N \neq \{1\}, S_n$
断言 $N = A_n$ 事实上 $N \leq A_n$.(例 $N \neq A_n$ 则 $N \cdot A_n = S_n$, $Z_2 \cong S_n/A_n = N \cdot A_n/A_n \cong N/(N \cap A_n)$
(第一同构定理))又 $N \cap A_n \triangleleft A_n$. 但 A_n 是单群.故 $N \cap A_n = A_n$ 或 $N \cap A_n = \{1\}$ 但 ~~又因 $N \neq A_n$~~ 若 $N \cap A_n = A_n \Rightarrow A_n \leq N \neq A_n$ 矛盾 ~~$N = S_n$~~
若 $N \cap A_n = \{1\}$ 则 $N \cong Z_2$. 即 $|N| = 2$
(不可能是正规子群)作业, 求 A_4 的全部子群 (10 分)例 $S_4/K_4 \cong S_3$ (Klein 4 元群 $\{1, (12)(34), (13)(24), (14)(23)\}$)法 1: $S_4 = (1)K_4 \cup (12)K_4 \cup (13)K_4 \cup (123)K_4 \cup (132)K_4$ 故 $S_4/K_4 = \{1, (12), (13), (23), (123), (132)\} \cong S_3$ 法 2: 验证 $K_4 \cdot S_3 = S_4$ ($|K_4 \cdot S_3| = \frac{|K_4| |S_3|}{|K_4 \cap S_3|} = \frac{4 \cdot 6}{1} = 24$)有 $S_4/K_4 = K_4 S_3 / K_4 \cong K_4 S_3 / (S_3 \cap K_4) = S_3$

§1.7 群在集合上的作用.

G : 群, Ω : 集合. $S(\Omega)$: Ω 的对称群.
 $|\Omega| = n, |S(\Omega)| = S_n$

定义1: 将群同态 $f: G \rightarrow S(\Omega)$ 称为群 G 在集合 Ω 上的一个作用.
 特别地, 将群同态 $f: G \rightarrow S_n$ 在 n 元集上的一个作用.

定义2: 将映射 $G \times \Omega \rightarrow \Omega$ 称为群 G 在集合 Ω 上的一个作用, 满足:
 $(g, x) \mapsto g \cdot x, \forall g \in G, \forall x \in \Omega$.

$$(1) 1 \cdot x = x, \forall x \in \Omega$$

$$(2) (gh)x = g(hx), \forall g, h \in G, \forall x \in \Omega.$$

下证这两个定义等价: 定义1 $\Rightarrow$ 定义2, 设 $f: G \rightarrow S(\Omega)$.

定义映射: $G \times \Omega \rightarrow \Omega$
 $(g, x) \mapsto f(g)(x)$ 验证 (1)(2) 是显然成立的.

定义2 $\Rightarrow$ 定义1. 设映射 $G \times \Omega \rightarrow \Omega$ 满足上述两条性质.

定义映射 $f: G \rightarrow S(\Omega)$

$g \mapsto f(g): "x \mapsto gx"$ (单. 满) (f 是群同态). #

$\ker f = \{g \in G \mid f(g) = Id\}$ 称为作用的核.

若 $\ker f = \{1\}$, 称 g 在 Ω 的作用是忠实的 (faithful).

或 $\ker f = \{g \in G, gx = x, \forall x \in \Omega\} \triangleleft G$.

例1. $G, \Omega = G$.

$$G \times \Omega \rightarrow \Omega$$

$$(g, x) \mapsto gx$$

此作用称为 G 的左正则作用.

这个作用是忠实的.

例2: 设 $H \leq G$, $G/H = \{gH \mid g \in G\}$, $G \times \Omega \rightarrow \Omega$
 $(g, xH) \mapsto (gx)H$

这个作用称为左陪集作用

作用的核: $\bigcap_{g \in G} g^{-1}Hg \trianglelefteq G$

例3: $G, A \subseteq \mathbb{R}^n$ 子集, $\Omega = \{g^{-1}Ag \mid g \in G\}$

~~$G \curvearrowright \Omega: g(A) = gAg^{-1} \stackrel{\text{def}}{=} g^{-1}Ag$~~

$G \curvearrowright \Omega: g(A) = g(Ag^{-1}) \stackrel{\text{def}}{=} gAg^{-1}$

称为共轭作用: 核 $\bigcap_{g \in G} g^{-1}N_G(A)g \trianglelefteq G$.

$N_G(A) = \{h \in G \mid hAh^{-1} \subseteq A\}$ 正规化子

例4: $G = GL_n(\mathbb{R})$ $\Omega = \left\{ \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in \mathbb{R}^n \right\} = \mathbb{R}^n$.

$G \curvearrowright \Omega: A \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \stackrel{\text{def}}{=}} A_{n \times n} \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$ (矩阵乘法) 是忠实的

设 $G \curvearrowright \Omega$ (G 在 Ω 上的作用), $\forall x \in \Omega$. 令 $Gx = \{gx \mid g \in G\} \subseteq \Omega$
 称为 x 的 G -轨道.

令 $G_x \stackrel{\text{def}}{=} \{g \in G \mid gx = x\}$, 则 $G_x \leq G$, 称为 x 的稳定子群或不动点群

注意到 $\ker = \bigcap_{x \in \Omega} G_x$.

定理: (轨道公式 Orbit Formula) 设 $G \curvearrowright \Omega$, 则 $\forall x \in \Omega$.

$$|Gx| = [G : G_x] = \frac{|G|}{|G_x|}$$

27

$$g \cdot x = h \cdot x \Leftrightarrow (g^{-1}h) \cdot x = x \Leftrightarrow g^{-1}h \in G_x \Leftrightarrow g G_x = h G_x$$

$$\text{故 } |Gx| = [G : G_x] \quad \#$$

特别地, 若 G 在 Ω 上的作用是可迁的 (设 $G \curvearrowright \Omega$, 称此作用是可迁的, 如果 Ω 只有一个 ~~轨道~~ G -轨道: $\Omega = Gx = Gy \quad \forall y$)

$$\text{则 } |\Omega| = [G : G_x] \quad \forall x \in \Omega, \text{ 即有 } |\Omega| \mid |G|$$

正则作用是可迁的. $|Gx| = [G : G_x] = |G|$

$$\text{诱导作用 } \forall xH \in \Omega, \quad G_{xH} = \{g \in G \mid gxH = xH\} = \{g \in G \mid g \in xHx^{-1}\} \\ = xHx^{-1}$$

$$\text{也是可迁的. } G(xH) = \Omega. \quad |\Omega| = [G : H] = [G : xHx^{-1}] \\ = \frac{|G|}{|xHx^{-1}|} = \frac{|G|}{|H|}$$

共轭作用:
 $\forall xAx^{-1} \in \Omega.$

$$G(xAx^{-1}) = \{gxAx^{-1}g^{-1} \mid g \in G\} = \Omega. \text{ 也是可迁的.}$$

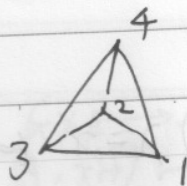
$$|\Omega| = [G : G_{xAx^{-1}}] = \frac{|G|}{|N_G(A)|} \quad \text{子集 } A \text{ 的共轭子集个数是 } \frac{|G|}{|N_G(A)|}$$

$$G_{xAx^{-1}} = \{g \in G \mid \underset{\substack{\uparrow \\ \text{此处是作用的意思}}}{g \cdot (xAx^{-1})} = xAx^{-1} : gxAx^{-1}g^{-1} = xAx^{-1}\}$$

$$= \{g \in G \mid (x^{-1}gx)A(x^{-1}g^{-1}x) = A\} = \{g \in G \mid x^{-1}gx \in N_G(A)\} \\ = xN_G(A)x^{-1}$$

28

例: 求正四面体的旋转群 G 的阶.



解: $G \curvearrowright \Omega = \{1, 2, 3, 4\}$.

$$4 = |\Omega| = [G : G_4] = \frac{|G|}{|G_4|} = \frac{|G|}{3} \Rightarrow |G| = 12$$

例: 设 G 是 $2n$ 阶群, n 奇, 则 G 有指数为 2 的正规子群 H .

且若 $|G| \geq 4$, 则 G 非单. (例: 14 阶群非单)

证: $\rho: G \hookrightarrow S_{2n}$ 左正则表示

G 有 2 阶元 g , $g = (x_1 \dots x_n)(y_1 \dots y_n) = \underbrace{(x_1 g x_1)(y_1 g y_1)}_{2n \text{ 个字母}} = \text{奇置换}$

$H = G \cap A_{2n}$ 则 $H \neq G$. 则 $g \notin H$, $H \neq G$

$$[G : H] = \frac{|G|}{|G \cap A_{2n}|} = \frac{|G \cdot A_{2n}|}{|A_{2n}|} = \frac{|S_{2n}|}{|A_{2n}|} = 2$$

§8 应用举例.

n 次二面体群 D_n . def 正 n 边形的对称群.

$$|D_n| = 2n \quad \text{令 } \Omega = \{1, \dots, n\} \quad D_n \curvearrowright \Omega$$

$$n = |\Omega| = \frac{|D_n|}{|D_n|} = \frac{|D_n|}{2} \Rightarrow |D_n| = 2n.$$

特别地, $D_6 = \{ (1), (12345), (135)(246), (14)(25)(36), (153)(264), (165432), (26)(35), (13)(46), (24)(15), (12)(36)(45), (23)(14)(56), (16)(25)(34) \}$. ~~其中~~, $|D_6| = 12$

Burnside 引理: ~~问题~~ 问题: 群作用 $G \curvearrowright \Omega$ 有多少个轨道?

轨道数 $t = \frac{1}{|G|} \cdot \sum_{g \in G} |F_g|$, 其中 $F_g = \{x \in \Omega \mid gx = x\}$ 是 g 的不动点集.

注意 $|F_g| \leq |\Omega|$. (平均使得几个点不动即为轨道数).

证: $\Omega = Gx_1 \cup Gx_2 \cup \dots \cup Gx_t$ (无交之并).

令 $\Gamma = \{(g, x) \in G \times \Omega \mid gx = x\}$ $|\Gamma| = ?$

方法 1: $|\Gamma| = \sum_{g \in G} |F_g|$ (固定 g , 再令 x 遍历).

方法 2: $|\Gamma| = \sum_{x \in \Omega} |G_x|$ (固定 x , 再令 g 遍历).

$$= \sum_{x \in \Omega} \frac{|G|}{|G_x|} = \sum_{i=1}^t \sum_{x \in Gx_i} \frac{|G|}{|Gx_i|} = \sum_{i=1}^t \sum_{x \in Gx_i} \frac{|G|}{|Gx_i|} = t|G|$$

故 $t = \frac{1}{|G|} \sum_{g \in G} |F_g|$ # 漂亮的算两次证明.

30

项链问题 (Necklace Problem)

设有 n 颗珠子, r 种颜色, 共配成多少种项链.

$$\Omega = B = \{1, 2, \dots, n\} \quad C = \{c_1, \dots, c_r\}$$

$$f: B \rightarrow C. \quad f = \begin{pmatrix} 1 & 2 & \dots & n \\ y_1 & y_2 & \dots & y_n \end{pmatrix}, \quad \overline{c_1}, \dots, \overline{c_n} \in C.$$

$$f = \begin{pmatrix} i_1 & \dots & i_n \\ y_{i_1} & \dots & y_{i_n} \end{pmatrix} \quad i_1, \dots, i_n \text{ 是 } 1, \dots, n \text{ 的一个排列}$$

这样的映射共有 r^n 个标号项链, 即共有 r^n 个标号项链考虑 $D_n \curvearrowright \Omega = \{f: B \rightarrow C\} = \{\text{标号项链}\}.$

$$\forall f = \begin{pmatrix} 1 & 2 & \dots & n \\ y_1 & y_2 & \dots & y_n \end{pmatrix} \in \Omega, \quad \forall \alpha = \begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & \dots & i_n \end{pmatrix} \in D_n$$

$$\alpha f = \begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix} \begin{pmatrix} 1 & 2 & \dots & n \\ y_1 & y_2 & \dots & y_n \end{pmatrix} \stackrel{\text{def}}{=} \begin{pmatrix} i_1 & \dots & i_n \\ y_1 & \dots & y_n \end{pmatrix} = f \alpha^{-1}$$

这是一个群作用.

$$\text{验证: } (\beta \alpha) f = f (\beta \alpha)^{-1} = f (\alpha^{-1} \beta^{-1}) = (f \alpha^{-1}) \beta^{-1} = \beta (\alpha f)$$

要求的项链的种数 = 群作用 $D_n \curvearrowright \Omega$ 的轨道的个数 +

Burnside 引理

$$t = \frac{1}{2n} \sum_{\alpha \in D_n} |F_\alpha| \quad \text{其中 } F_\alpha = \{f \in \mathcal{F} \mid \alpha \cdot f = f\}$$

α 的型 $(\lambda_1, \lambda_2, \dots, \lambda_n)$

引理. 设 $\alpha \in D_n$, $f \in \mathcal{F}$, 则 $\alpha f = f \iff$ 若 ij 位于 α 的同一轮换因子, 则 $f(i) = f(j)$. (把 i 和 j 的珠子颜色变成一样的, 也位于同一轮换因子中).

证: $\Rightarrow$ 设 $\alpha f = f$, 则 $y_j = y_{ij} \quad (j=1, 2, \dots, n)$

$$\alpha = (j \ i_j)$$

$\Leftarrow$ 也一样. (自己想吧)

$$|F_\alpha| = r^{\lambda_1 + \lambda_2 + \dots + \lambda_n}$$

$$t = \frac{1}{2n} \sum_{\substack{\alpha \in D_n \\ \alpha \text{ 的型为 } (\lambda_1, \lambda_2, \dots, \lambda_n)}} r^{\lambda_1 + \dots + \lambda_n} = \frac{1}{2n} \sum_{(\lambda_1, \dots, \lambda_n)} \frac{C(\lambda_1, \dots, \lambda_n)}{r^{\lambda_1 + \dots + \lambda_n}}$$

$C(\lambda_1, \dots, \lambda_n)$ 是 D_n 中型为 $(\lambda_1, \dots, \lambda_n)$ 的元素个数 #

特别地, $n=6$ 时. 看 D_6 : $t = \frac{1}{12} (3^6 + 2 \cdot 3^1 + 2 \cdot 3^2 + 4 \cdot 3^3 + 3 \cdot 3^4)$

(6颗珠子, 3种颜色)

$= 92$

32

作业题: 4颗珠子, 2种颜色. 几种项链.

§9 Sylow定理.

Lagrange定理之逆不成立: 设正整数 $d \mid |G|$, 则 G 未必有 d 阶子群.

Sylow I:

设 G 是群. $|G| = p^r \cdot m$, $r \geq 1$, p 是素数 (不一定要 r 最大).

用 $N(p^r)$ 表示 G 的阶为 p^r 的子群的个数. 则 $N(p^r) \equiv 1 \pmod{p}$.

证明略, 主要思想是群在集合上的应用.

Sylow II: 设 G 是群. $|G| = p^r \cdot m$, $r \geq 1$ 素数, $p \nmid m$.

用 G 的 p^r 阶子群称为 G 的 Sylow p -子群.

Sylow III: 有限群 G 的 Sylow p -子群互相共轭!

特别地 $N(p^r) \equiv 1 \pmod{p}$; $N(p^r) = [G : N_G(p^r)]$

~~G 的 Sylow p -子群~~

pf. 令 $\Omega = \{G \text{ 的 Sylow } p\text{-子群}\}$, 令 $\Gamma = \{gpg^{-1} \mid g \in G\}$
其中 p 是某个 Sylow p -子群. 要证 $\Gamma = \Omega$ (已知 $p \in \Omega$).

考虑 p 的共轭作用. 计算 $|\Omega|$.

$$|\Omega| = \sum_{j=1}^t |O_j| = \sum_{j=1}^t \frac{|P|}{|P_j|}$$

首先 P 是 G 的长为 1 的 p -轨道.

设 $\{M\}$ 是 G 的长为 1 的 p -轨道.

则 $m = p$. 因而 $|M| \equiv 1 \pmod{p}$.

$\forall p \in P, pMp^{-1} = M, pM = Mp$. 故 $mp \leq G$.

$$|mp| = |P| \cdot \frac{|M|}{|M \cap P|}, \quad m = m \cap p.$$

即 M 的长为 1 的 p -轨道只有一条, 故 $|M| \equiv 1 \pmod{p}$.

(反设) 设 P' 是 G 的一个 Sylow p -子群且 $P' \notin P$.

考虑 P' 在 P 上的作用.

$$|P| = \sum_{j=1}^t |O_j| = \sum_{j=1}^t \frac{|P'|}{|P'_j|} \quad \text{由此可见 } |P| \equiv 0 \pmod{p} \text{ 矛盾!}$$

例 1. p -群不是单群.

pf. 设 $|G| = p^m, m \geq 1, p$ 素.

$$C(G) \neq \{1\}.$$

$C(G) \triangleleft G$, 若 $C(G) \neq G$, 则 G 非单.

$C(G) = G$, 则 G 是 Abel 群.

由 Sylow 知 G 有 p 阶子群 $N \triangleleft G$.

所以 G 非单. #

例 2. p 阶群不是单群, p 素.

34

证: 分情况考虑. 若 $p=q$, OK; 若 $p < q$, 则

$$N(p^2) = kp + 1 \mid q.$$

故 $N(p^2) = 1$ 故 G 非单 (

若 $p < q$, 则 $N(q) = kq + 1 \mid p^2$.

$$\therefore N(q) = 1 \text{ or } N(q) = p^2$$

若 $N(q) = 1$, OK.

设 $N(q) = p^2$, 则 p 个 q 阶子群共占去了 $(q-1)p^2 + 1$ 个元.

还剩下 $p^2q - q p^2 + p^2 - 1 = p^2 - 1$ 个元

注: $p^2 - 1$ 连同单位元恰好作成唯一的一个 Sylow p -子群.

故 G 非单 #

错误的作法:

例: 40 阶群非单

56 阶群非单

36 阶群非单

48 阶群非单

24 阶群非单

35

p.f. $|G| = 24 = 2^3 \cdot 3$.

不妨设 Sylow 2-子群不是正规的.

则 ~~$N(8) = 3$~~ $N(8) = 3$. 设 G 的 3 个 8 阶子群 P_1, P_2, P_3
考虑 G 关于 $\{P_1, P_2, P_3\}$

有群同态 $\rho: G \rightarrow S_3$.

$\ker \rho \triangleleft G$. 且 $\ker \rho \neq 1$ (否则 $G \leq S_3$, 矛盾!)

$\ker \rho \neq G$ (否则与 Sylow I 矛盾).

故 G 非单.

作业 2.3.4.

Sylow I. 设群 G 的阶被 p^r 整除, 其中 p 素, $r \geq 1$. 则 G 的 p^r 阶子群
的个数 $n(p^r) \equiv 1 \pmod{p} = kp+1, k \in \mathbb{Z}^+ \cup \{0\}$.

Sylow I. 有限群的 Sylow p -子群彼此共轭.

推论: ~~有群 G 设~~ 设 $|G| = p^r \cdot m, p \nmid m$. 则 G 的 Sylow p -子群
(p 素, $r \geq 1$)

的个数 $n(p^r) = kp+1$. 且 $n(p^r) = [G : N_G(P)] \mid m$.

Sylow II: 有限群的任一 p^i 阶子群 $B (i \geq 1)$ 必含于某一 Sylow p -子群

36

证明 Sylow II: 设 $\Omega = \{G \text{ 的 Sylow } p\text{-子群}\}$.

考虑 $B \curvearrowright \Omega$. $\forall b \in B \forall P \in \Omega, b \cdot P \triangleq b \circ P b^{-1}$

$$|\Omega| \equiv 1 \pmod{p} \quad |\Omega| = \sum_{j=1}^t |O_j| = \sum_{j=1}^t \frac{|B|}{|B_j|}$$

~~故~~ Ω 中必有一个长为 1. B 轨道 $\{P\}$

故 $b P b^{-1} = P, \forall b \in B$

即 $b P = P b$, $B P = P B, B P \leq G$.

~~故~~ $P \leq B P$. $|B P|$ 的阶也是 p 的幂.

$|P| = |B P|$ 即 $B \subseteq P$. 证完.

例: 设 P 是有限 G 的 Sylow p -子群, $N_G(P) \triangleleft G$, 则 $P \triangleleft G$
 $\{x \in G \mid x P x^{-1} = P\}$.

注意 $P \triangleleft N_G(P)$. 但正规子群不具有传递性.

证: $\forall g \in G$, 要证 $g^{-1} P g = P$

易见 $g^{-1} P g \leq g^{-1} N_G(P) g = N_G(P)$.

故 P 与 $g^{-1} P g$ 均为 $N_G(P)$ 的 Sylow p -子群.

由 Sylow II: $\exists n \in N_G(P), g^{-1} P g = n^{-1} P n = P$. #
 ~~$\Rightarrow n g$~~

37

例: 非 Abel 的单群最小阶为 60. 并且 60 阶非 Abel 单群 ~~为~~ 必同构为 A_5

证: (1) p -群不是 ~~非~~ 非阿单群.

(2) p^2 -群不是非 Abel 单群.

(3) p^3 -群不是单群

(4) 2^m 阶群 (m 奇) 不是 ~~非~~ 非 Abel 单群.

1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15,
16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30,
~~31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44~~

31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45,
46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59

其中 24, 36, 40, 48, 56 阶群非单为前述所证, 不在 (1)~(4) 之列

S_3 群的直积.

设 $G_1, \dots, G_n$ 是群, $n \geq 2$. 令 $G \stackrel{\text{def}}{=} G_1 \times \dots \times G_n = \{(g_1, \dots, g_n) \mid g_i \in G_i, i=1, \dots, n\}$

定义 G 的运算 $(g_1, \dots, g_n)(h_1, \dots, h_n) = (g_1h_1, \dots, g_nh_n)$.

容易验证 $(G, \times G_1 \times \dots \times G_n, \cdot)$ 是群. 称之为 $G_1, \dots, G_n$ 的直积.

$(1, \dots, 1)$ 是其单位元. (每一个 1 是对应的 G_i 的单位元).

$(g_1, \dots, g_n)^{-1} = (g_1^{-1}, \dots, g_n^{-1})$.

问题: 给一个群 G , 何时能将这个群分解为: $G \cong G_1 \times \dots \times G_n$

38

$$\cancel{G_1 \times \dots \times G_n} = \{ (g_1, \dots, g_n) \in G_1 \times \dots \times G_n \}$$

$$\text{令 } G'_i = \{ (g_1, 1, \dots, 1) \mid g_1 \in G_i \}$$

类似定义 $G'_2, \dots, G'_n$

$$\text{则 } G'_i \triangleleft G_1 \times G_2 \times \dots \times G_n, \quad 1 \leq i \leq n.$$

$$\text{易见 } G'_i \cong G_i, \quad G_1 \times \dots \times G_n = \cancel{G'_1 \times \dots \times G'_n}$$

$$= G'_1 \dots G'_n$$

$$G'_i \cap G'_{i+1} \dots G'_n = \{1\} \quad | \leq i \leq n-1$$

G'_i 与 G'_j ($i \neq j$) 中的元素乘法可交换.

~~$G_1 \times \dots \times G_n$ 中~~ $G_1 \times \dots \times G_n$ 中任意元均可唯一写成:

$$x = x_1 \dots x_n, \quad x_i \in G'_i$$

重述一下性质:

$$\bullet G'_i \triangleleft G_1 \times \dots \times G_n, \quad 1 \leq i \leq n.$$

$$\bullet G'_i \cong G_i$$

$$\bullet G_1 \times \dots \times G_n = G'_1 \dots G'_n$$

$$\bullet G'_i \cap G'_{i+1} \dots G'_n = \{1\}, \quad | \leq i \leq n-1.$$

G'_i 与 G'_j ($i \neq j$) 乘法可换.

$G_1 \times \dots \times G_n$ 中任意元 x 均可唯一写成 $x = x_1 \dots x_n$, $x_i \in G'_i$

定理: 设 $G_1, \dots, G_n \trianglelefteq G$, 则下述等价.

- (1) $G \cong G_1 \times \dots \times G_n$
- (2) G 的任意元 ~~均可~~ g 均可唯一写成 $g = g_1 \dots g_n$ ($g_i \in G_i, i=1, \dots, n$)
- (3) $G = G_1 \dots G_n, G_i \cap G_{i+1} \dots G_n = \{1\}, i=1, \dots, n-1$
(可表性) (唯一性)
- (4) $G = G_1 \dots G_n, G_i \cap G_j = \{1\}, i \neq j$

且 G_i 中的元与 G_j 中的元可换 $\forall i \neq j$

证: (1) $\Rightarrow$ (2) $\Rightarrow$ (3) $\Rightarrow$ (4) $\Rightarrow$ (1).

(1) $\Rightarrow$ (2) $\Rightarrow$ (3) 显然

$$(3) \Rightarrow (4): \# g_i g_j = g_j g_i \Rightarrow g_j^{-1} g_i g_j = g_i$$

$$\Rightarrow g_i^{-1} g_i g_j g_i^{-1} = g_i^{-1} (g_i g_j g_i^{-1}) = (g_i^{-1} g_i g_j) g_i^{-1} = G_i \cap G_j = \{1\}$$

$$(4) \Rightarrow (1) \quad g = g_1 \dots g_n \longrightarrow (g_1, \dots, g_n)$$

$$\text{唯一性: } h_1^{-1} g_1 = h_1 h_2 g_2^{-1} \dots g_1^{-1} = (h_2 g_2^{-1}) \dots (h_n g_n^{-1}) = \{1\}$$

$$\text{同理得: } h_i = g_i \quad (1 \leq i \leq n)$$

$$\text{例: } P_{39}/5, 7 \cdot P_{44}/5, 6, 9, 4$$

40

$$\text{例: } \mathbb{Z}_n \oplus \mathbb{Z}_m \cong \mathbb{Z}_{nm} \Leftrightarrow (m, n) = 1$$

$$\begin{aligned} \text{例 } \mathbb{Z}_2 \oplus \mathbb{Z}_2 &\cong \{(1), (12)(34), (13)(24), (14)(23)\} \\ &\cong \{(1), (12), (34), (12)(34)\} \\ &\cong \{(\bar{0}, \bar{0}), (\bar{0}, \bar{1}), (\bar{1}, \bar{0}), (\bar{1}, \bar{1})\} \end{aligned}$$

证: " $\Leftarrow$ ": 设 $(n, m) = 1$. 设 $\mathbb{Z}_n = \langle x \rangle$, $\mathbb{Z}_m = \langle y \rangle$.

$$\text{令 } (x, y) \in \mathbb{Z}_n \oplus \mathbb{Z}_m \text{ 则 } xy \in \mathbb{Z}_n \oplus \mathbb{Z}_m$$

$$o(xy) = nm = |\mathbb{Z}_n \oplus \mathbb{Z}_m|$$

$$\text{故 } \mathbb{Z}_n \oplus \mathbb{Z}_m \cong \mathbb{Z}_{nm}$$

$$(u, v) \mapsto (u^s, v^t)$$

$$(\exists s, t, su + tv = 1)$$

" $\Rightarrow$ " 设 $\mathbb{Z}_n \oplus \mathbb{Z}_m \cong \mathbb{Z}_{nm} = \langle x \rangle$

$$\exists d = (n, m) \cdot \text{则 } n = ds, m = dt$$

$$\text{则 } o(x^m) = \frac{nm}{(m, nm)} = n. \text{ 同理 } o(x^n) = m$$

$$\langle x^m \rangle = \mathbb{Z}_n, \langle x^n \rangle = \mathbb{Z}_m$$

$$\underline{\text{证}} \quad \langle x^m \rangle \cap \langle x^n \rangle = \{1\}$$

$$x^{dst} = x^{nt} = x^{ms} \in \{1\}.$$

引理:

例: pq 阶群是循环群, 其中 $p < q$, $p \nmid q-1$, p, q 素数

证: $|G| = pq$, $p < q$, $p \nmid q-1$

则有 2 个 Sylow 子群: $N(q) = kq + 1 \mid p \Rightarrow N(q) = 1$

$\Rightarrow \mathbb{Z}_q \triangleleft G$

$N(p) = kp + 1 \mid q \Rightarrow N(p) = 1 \Rightarrow \mathbb{Z}_p \triangleleft G$

$G \cong \mathbb{Z}_p \oplus \mathbb{Z}_q \cong \mathbb{Z}_{pq}$ #

例: $5 \cdot 7 \cdot 13$ 阶群是循环群

证: $|G| = 5 \cdot 7 \cdot 13$, $N(13) = 13k + 1 \mid 5 \cdot 7 \Rightarrow N(13) = 1$

$\Rightarrow \mathbb{Z}_{13} = \langle z \rangle \triangleleft G$

$N(7) = 7k + 1 \mid 5 \cdot 13 \Rightarrow \mathbb{Z}_7 = \langle y \rangle \triangleleft G$

$N(5) = 5k + 1 \mid 7 \cdot 13 \Rightarrow \mathbb{Z}_5 = \langle x \rangle \leq G$

$\langle x \rangle \langle y \rangle$ 是 $5 \cdot 7$ 阶 Abel 子群 (引理)

$\langle x \rangle \langle z \rangle$ 是 G 的 $5 \cdot 13$ 阶 Abel 子群 (引理)

$\langle y \rangle \langle z \rangle$ 是 G 的 $7 \cdot 13$ 阶 Abel 子群 (引理)

故 x, y, z 两两可换

又 $G = \langle x \rangle \langle y \rangle \langle z \rangle$ 故 G 可换 $\Rightarrow G \cong \mathbb{Z}_{5 \cdot 7 \cdot 13}$

正规子群乘任一子群还是子群

42

§11 群的表现

集合 S 生成的自由群 $F(S)$ S 集合, $S^{-1} = \{s^{-1} \mid s \in S\}$ (硬规定形式逆)以 $S \cup S^{-1}$ (注意 $S \cap S^{-1} = \emptyset$) 为字母的集合记为 $F(S)$ 例 $S = \{a, b, c, \dots, x, y, z\}$ $F(S)$ 含 brave, love, love, 空字 ϕ (单位元). $F(S)$ 的乘法: 字的连接, 规定 $ss^{-1} = s^{-1}s = \phi$

$$\phi s = s\phi = s$$

 $F(S)$ 是群, 每个元的阶都是无限的

定理 (1) 任一群是自由群的商群.

(2) 任一有限群是有限生成自由群的商群.

证: $\pi: F(G) \rightarrow G$

$$\begin{aligned} g &\mapsto g \\ g^{-1} &\mapsto g^{-1} \end{aligned}$$

$$G \cong F(S)/K$$

$$G = \langle s \in S \mid k = k, \forall k \in K \rangle$$

$$= \langle s \in S \mid \text{若 } k \text{ 是由 } s \text{ 生成} \\ \text{的正规子群} \rangle$$

例: ~~已知~~ D_n (正 n 边形对称群) $= \{ \sigma^i \tau^j, 0 \leq i \leq n-1, j=0,1 \}$

$$|D_n| = 2n. \quad \sigma^n = 1, \tau^2 = 1, \tau\sigma = \sigma^{n-1}\tau$$

(σ 为旋转, τ 为翻折)

想象

证明: $D_n = \langle a, b \mid a^n = 1, b^2 = 1, ba = a^{n-1}b \rangle$

$$\pi: F(\{a, b\}) \longrightarrow D_n, \quad a \mapsto \sigma, \quad b \mapsto \tau.$$

$$\{ a^{m_1} b^{n_1} a^{m_2} b^{n_2} \dots a^{m_t} b^{n_t} \mid m_1, \dots, m_t, n_1, \dots, n_t \in \mathbb{Z}, t=0,1,\dots \}$$

$$D_n \cong F(\{a, b\}) / \ker \pi, \text{ 且由 } a^n, b^2, (ba)^2 \text{ 生成}$$

即 $F(\{a, b\})$ 的正规子群

$$K = \ker \pi$$

$$a^n = 1, b^2 = 1, (ba)^2 = 1$$

$$\Rightarrow K \subseteq \ker \pi, \quad 2n = |D_n| = |F(S)/\ker \pi| = \frac{|F(S)|}{|K|}$$

$$\text{从而 } \frac{|F(S)|}{|K|} \leq 2n. \Rightarrow \ker \pi = K$$

$$G = \mathbb{Z}_n \oplus \mathbb{Z}_m = \{(\bar{i}, \bar{j}) \mid \bar{i} \in \mathbb{Z}_n, \bar{j} \in \mathbb{Z}_m\}$$

$\mathbb{Z}_n$ 有限 Abel 群的结构.

设 G 是有限 Abel 群, $|G| = n = p_1^{r_1} \cdots p_k^{r_k}$, $p_1, \dots, p_k$ 素数两两不同

用 G_i 表示 G 的 Sylow p_i -子群, $i=1, \dots, k$ $r_1, \dots, r_k \geq 1$

则 $G_1, \dots, G_k \triangleleft G$.

$$|G_1 \cdots G_k| = |G| \text{ 且 } G_1 \cdots G_k = G$$

$$G_i \cap G_{i+1} \cdots G_k = \{1\}$$

$$\text{故 } G = G_1 \oplus \cdots \oplus G_k.$$

设 G 是 Abel 群且 $|G| = p^n$, p 素数, $n \geq 1$.

正整数 n 的划分 (partition) $n = n_1 + n_2 + \cdots + n_l$ $0 < n_1 \leq \cdots \leq n_l$

用 $p(n)$ 表示 n 的所有划分的个数. 例 $p(5) = 7$

$$5 = 5$$

$$= 1+4$$

$$= 2+3$$

$$= 1+1+3$$

$$= 1+2+2$$

$$= 1+1+1+2$$

$$= 1+1+1+1+1$$

定理: 用 Ω 表示正整数 n 的划分的集合

用 Γ 表示 p^n 阶 Abel 群同构类的集合

$$\text{则 } \Omega \longrightarrow \Gamma$$

$$n = n_1 + \cdots + n_l \longmapsto \mathbb{Z}_{p^{n_1}} \oplus \cdots \oplus \mathbb{Z}_{p^{n_l}}$$

是双射.

定理: 设 $n = p_1^{r_1} \cdots p_t^{r_t}$ 是标准素分解. 则在 n 阶 Abel 群必同构于

$$(\mathbb{Z}_{p_1^{r_{1,1}}} \oplus \cdots \oplus \mathbb{Z}_{p_1^{r_{1,s_1}}}) \oplus (\mathbb{Z}_{p_2^{r_{2,1}}} \oplus \cdots \oplus \mathbb{Z}_{p_2^{r_{2,s_2}}}) \oplus \cdots$$

$$\oplus (\mathbb{Z}_{p_t^{r_{t,1}}} \oplus \cdots \oplus \mathbb{Z}_{p_t^{r_{t,s_t}}})$$

其中 $r_i = r_{i,1} + \cdots + r_{i,s_i}$
 $r_t = r_{t,1} + \cdots + r_{t,s_t}$ (分别) 是 $r_1, \dots, r_t$ 的划分.

反之, 上述形式的直和是 n 阶 Abel 群.
 上述分解方式是唯一的.

将 $p_1^{r_{1,1}}, \dots, p_1^{r_{1,s_1}}, \dots, p_t^{r_{t,1}}, \dots, p_t^{r_{t,s_t}}$
 称为 n 阶 Abel 群的初等因子.

两个 n 阶 Abel 群同构 $\Leftrightarrow$ 其初等因子组相同.

例 $\mathbb{Z}_{2^3} \oplus \mathbb{Z}_{3^2} \not\cong \mathbb{Z}_{2^2} \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{3^2}$

定理: 在 n 阶 Abel 群 G 必同构于 $G \cong \mathbb{Z}_{n_1} \oplus \cdots \oplus \mathbb{Z}_{n_{s-1}} \oplus \mathbb{Z}_{n_s}$
 其中 $n_1 | n_2 | \cdots | n_s$ $n_1 \cdots n_s = n$.

称 $n_1, \dots, n_s$ 是 G 的不变因子组.

两个 n 阶 Abel 群同构 $\Leftrightarrow$ 其不变因子组相同

故若有 $P(r_1) \neq P(r_t)$ 个两两不同构的 n 阶 Abel 群.

46

例: 写出所有两两不同构的 1500 阶 Abel 群.

解: $1500 = 3 \times 5^3 \times 2^2 = 2^2 \cdot 3 \cdot 5^3$.

故共有 $p(2) \cdot p(1) \cdot p(3) = 6$ 个两两不同构的 1500 阶 Abel 群.

$$\begin{array}{c|c|c} 2=2 & 1=1 & 3=3 \\ =1+1 & & =1+2 \\ & & =1+1+1 \end{array}$$

$$\mathbb{Z}_{2^2} \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_{5^3} \cong \mathbb{Z}_{1500}$$

$$\mathbb{Z}_{2^2} \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_{5^2} \cong \mathbb{Z}_5 \oplus \mathbb{Z}_{300}$$

$$\mathbb{Z}_{2^2} \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5 \cong \mathbb{Z}_{60} \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5$$

$$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_{5^3} \cong \mathbb{Z}_2 \oplus \mathbb{Z}_{750}$$

$$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_{5^2} \cong \mathbb{Z}_{10} \oplus \mathbb{Z}_{300}$$

$$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5$$

$$\cong \mathbb{Z}_{30} \oplus \mathbb{Z}_{10} \oplus \mathbb{Z}_5$$

即有 6 个两两不同构的 1500 阶 Abel 群:

$$\mathbb{Z}_{1500}, \mathbb{Z}_5 \oplus \mathbb{Z}_{300}, \mathbb{Z}_{60} \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5, \mathbb{Z}_2 \oplus \mathbb{Z}_{750}, \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_{5^2}, \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5$$

47

$$\mathbb{Z}_{10} \oplus \mathbb{Z}_{300}, \mathbb{Z}_{30} \oplus \mathbb{Z}_{10} \oplus \mathbb{Z}_5.$$

写出所有两两不同构的900阶群.

例: Lagrange定理之逆对有限 Abel 群成立.

证: 设 $n = p_1^{r_1} \cdots p_t^{r_t}$ G 是 n 阶 Abel 群.

$$d \mid n, d = p_1^{r'_1} \cdots p_t^{r'_t}, r'_1, \dots, r'_t \geq 0. (\text{可以等于 } 0).$$

$$r'_1 = r'_{1,1} + \cdots + r'_{1,s'_1}, \dots, r'_t = r'_{t,1} + \cdots + r'_{t,s'_t}$$

$$\text{st. } r'_{1,1} \leq r_{1,1}, \dots, s'_1 \leq s_1, \dots$$

$$\bigoplus (\mathbb{Z}_{p_1^{r'_{1,1}}} \oplus \cdots \oplus \mathbb{Z}_{p_1^{r'_{1,s'_1}}})$$

$$\oplus \cdots \oplus (\mathbb{Z}_{p_t^{r'_{t,1}}} \oplus \cdots \oplus \mathbb{Z}_{p_t^{r'_{t,s'_t}}}).$$

为 G 的 d 阶子群.

确定互不同构的非Abel群.

例: 令 G 是 $S_3 \times \mathbb{Z}_4$ 由 $(123), \alpha^2$ 和 $(12), \alpha$ 生成的子群.

其中 $\mathbb{Z}_4 = \langle \alpha \rangle$

$$o(a) = 6, o(b) = 4.$$

$$a^3 = (11, \alpha^6) = (11, \alpha^2)$$

$$b^2 = (11, \alpha^2).$$

$$b^2 = \alpha^3$$

$$ba = ((12)(123), \alpha^3) = ((23), \alpha^3)$$

$$a^5 b = ((132), \alpha^2)(123, \alpha^3) = ((123), \alpha^3).$$

由直接计算可见

$$|G| = 12 \quad \therefore G = \langle a, b \mid a^6, b^2 = a^3, ba = a^5 b \rangle$$

$$= T$$

4次对称群 A_4 , 6次二面体群 $D_6 = \langle a, b \mid a^6 = 1, b^2 = 1, ba = ab \rangle$

和 $T = \langle a, b \mid a^6 = 1, b^2 = a^3, ba = a^5 b \rangle$

均为12阶非Abel群.

D_6 与 T 均有6阶元; 但 A_4 无6阶元;

又 T 中有4阶元; 但 D_4 无4阶元.

Campus

故 $A_4 \not\cong D_6, A_4 \not\cong T, D_6 \not\cong T$

$12 = 2^2 \cdot 3$. 设 $p = \langle c \rangle$ 是 G 的 Sylow 3-子群.

考虑 G 在 G/p (左陪集集合) 的左诱导作用

故有群同态 $\rho: G \rightarrow S_4 \dots (S_{p-1})$.

S_4 可解群.

设 G 是群, $a, b \in G$, 用 $[a, b] = aba^{-1}b^{-1}$ commutator

注意到 $ab = [a, b]ba$.

$[a, b]^{-1} = b a b^{-1} a^{-1}$ 也是交换子
 $= [b, a]$

但两个交换子乘积未必是交换子.

令 G' 是 G 的全部交换子生成的子群, 称为 G 的换位子群或导群.

$\angle: G' \triangleleft G$.

$\forall x \in G' \forall g \in G$. 要证. $g x g^{-1} \in G'$

则 $x = a_1 b_1 a_1^{-1} b_1^{-1} \dots a_m b_m a_m^{-1} b_m^{-1}$

故 $g x g^{-1} = g a_1 g^{-1} g b_1 g^{-1} g a_1^{-1} g^{-1} g b_1^{-1} g^{-1} \dots g a_m g^{-1} g b_m g^{-1} g a_m^{-1} g^{-1} g b_m^{-1} g^{-1}$
 也是换位子群中的元.

50

Remark: $G \text{ Abel} \Leftrightarrow G' = \{1\}$.

~~$G'_n = A_n$~~

定理: 设 $N \trianglelefteq G$. G/N 是 Abel 群 $\Leftrightarrow G' \leq N$

换言之, G' 是 S 中 G/N 是 Abel 群的最小正规子群 N

证: $\Rightarrow$ $G/N \text{ Abel} \Rightarrow a\bar{b}\bar{a}^{-1}\bar{b}^{-1} = \bar{1} \Rightarrow \overline{aba^{-1}b^{-1}} = \bar{1}$

$\Leftrightarrow aba^{-1}b^{-1} \in N$. 即在换位子 $\in N$. 即证.

例: $S'_n = A_n$

$S_n/A_n \text{ Abel}$. 故 $S'_n \leq A_n$

$n \geq 5$. $S'_n \trianglelefteq A_n$, A_n 是单群. 故 $S'_n = A_n$

~~$n \geq 5$~~

$n \leq 4$ 留给读者

$$A'_n = \begin{cases} A_n, & n \geq 5 \\ K_4, & n = 4 \\ A_3, & n \leq 3 \end{cases}$$

~~A~~

(~~若 $S'_n \neq \{1\}$~~)
导致 $S_n \text{ Abel}$
矛盾!

定义: 设 G 是群, 称 G 是可解群, 如果 $\exists n \in \mathbb{N}$ 使得 $G^{(n)} = \{1\}$

归纳定义 $G^{(1)} = G'$, $G^{(2)} = G^{(1)'} \dots, G^{(n)} = G^{(n-1)'}$

$$(n) \quad G \supset G^{(1)} \supset G^{(2)} \supset \dots \supset G^{(n-1)} \supset G^{(n)} \supset \dots$$

~~$S_n \leq 4$ 定理~~

结论: S_n 是可解群 $\Leftrightarrow n \leq 4$

A_n 是可解群 $\Leftrightarrow n \leq 4$

定理: 可解群的子群与商群均是可解群

设 $N \trianglelefteq G$. 若 N 与 G/N 均是可解群. 则 G 可解.

定理: p 群是可解群.

设 $|G| = p^n$, $n \geq 1$. 对 n 归纳.

(1) $n=1$, G Abelian $\checkmark$.

(2) $n > 1$. $C(G)$, $G/C(G)$ 可解. 故 G 可解.

($C(G) \neq \{1\}$). (归纳法假设)

作业:

(1) 证明: $G^{(n)} \trianglelefteq G$.

(2) 求 D_n (二面体群) 的换位子群并判断其可解性.

步 (3). pq , p^2q 均为可解群

§2

群 G 可解 $\Leftrightarrow \exists n \in \mathbb{N}, G^{(n)} = \{1\}$.

定理. 设 G 是有限群, 则下述等价

(1) G 是可解群. (2) G 有 ~~正规群列~~ ^{有限} 终止于 1 的正规群列

~~且每个因子群都是 Abel 群~~ 且每个因子群都是 Abel 群

即 $\exists G = G_0 \supset G_1 \supset G_2 \supset \dots \supset G_n = \{1\}, G_i \triangleleft G_{i+1}$

且 G_i/G_{i+1} 是 Abel. $0 \leq i \leq n-1$.

3. G 有终止于 $\{1\}$ 的有限长的次正规群列

且每个因子群是 Abel 群

4. G 有终止于有限长的次正规群列, 且每个因子群都是循环群

5. ————— 素阶循环群

6. ————— p -群

证:

(1) $\Rightarrow$ (2) $\bullet G \supset G^{(1)} \supset \dots \supset G^{(n)} = \{1\}, G^{(i)} \triangleleft G, \forall i \geq 1$

$G^{(i)}/G^{(i+1)} = G^{(i)}/G^{(i+1)}$ 为 Abel 群

(2) $\Rightarrow$ (3) 显然

(3) $\Rightarrow$ (4)

53

加细. G_i/G_{i+1} 有限 Abe(群).

$$G_i/G_{i+1} = G_i/G_{i+1} \oplus \dots \oplus G_{i+m_i}/G_{i+1} \oplus \dots \oplus G_i/G_{i+1} \text{ 循环群.}$$

$$G = G_{i_1} \dots G_{i_{m_1}} \triangleright G_{i_2} \dots G_{i_{m_2}} \triangleright \dots \triangleright G_{i_r}$$

(4) $\Rightarrow$ (5) 加细. 使用 Lagrange 定理之友

(5) $\Rightarrow$ (6) 显然

(6) $\Rightarrow$ (1) G_i/G_{i+1} 是 p -群. p -群可解. G_{i+1} 可解
故 G_i 可解

从后向前推即可

群. 很美的代数结论.

基本概念. 群. $GL_n(R)$ $SL_n(R)$. $\mathbb{Z}_n, \mathbb{Z}; S_n, A_n, \dots$

子群. 正规子群. p -群. 可解群. 循环群. S_n, A_n .

内部 - 阶. 子群. 正规. Lagrange. Sylow.

外部: p -群有非平凡的中心
Burnside 引理. 项链问题
群在集合上的作用. 对称性.

群类: S_n, A_n, D_n . 有限 Abe(群).

§2 环论 (ring)

$(\mathbb{Z}, +, 0, \cdot, 1)$: $(\mathbb{Z}, +, 0)$ 是加群
 $(\mathbb{Z}, \cdot, 1)$ 是含么群，但 $\mathbb{Z}$ 无逆元
 故非群

• 乘对加的分配律:

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

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

Def: 环 R 是带有两个二元运算, 记号 $+$, $\cdot$ (分别称为加法、乘法) 的集合. 其中 $(R, +)$ 是 Abel 群, $(R, \cdot)$ 是半群.
 并且乘法对加法有左右分配律.

Dictionary. ~~交换~~ 交换环: 对乘法满足交换律.
 含么环: 对乘法有单位元的环.
 零环

环 $(R, +, \cdot)$ 加群 $(R, +)$ 单位元记为 0 .

性质. $0 \cdot r = r \cdot 0 = 0 \quad \forall r \in R$.

证: 记 r 在 $(R, +)$ 中的逆元为 $-r$. 即 $r + (-r) = 0$
 简记为 $r - r = 0$

55

~~$$0 \cdot r = 0(r+0) = 0 \cdot r$$~~

$$0 \cdot r = (0+0)r = 0 \cdot r + 0 \cdot r \Rightarrow 0 \cdot r = 0$$

$$\text{同理可证 } 0 \cdot r = r \cdot 0 = 0$$

~~同样~~ 类似可证 $(-a)b = a(-b) = -ab$

$$(-a)(-b) = ab$$

$$\text{左零因子 } a: a \neq 0 \exists b \neq 0 \text{ s.t. } ab = 0$$

$$\text{右零因子 } a: a \neq 0 \exists b \neq 0 \text{ s.t. } ba = 0$$

左零因子与右零因子统称为零因子。

无零因子环：既无左零因子，又无右零因子的环。

作业： $\mathbb{Z}_n$ 无零因子环 $\Leftrightarrow n = p$ 素数

有 1 无零因子的交换环称为整环

可降环 (降)

$$(R^*, \cdot) = (R - \{0\}, \cdot) \text{ 是群}$$

skew field.

R 上任意非 0 元均有逆元

域：交换的可降环， $(R^*, \cdot)$ 是 Abel 群，例如 $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_p$ (p 素)

$$\text{例：} H = \{ae + bi + cj + dk \mid a, b, c, d \in \mathbb{R}\} \quad (p \text{ 素})$$

以 e, i, j, k 四个元素为基的 $\mathbb{R}$ 线性空间。

定义乘法为 $ri = ir, tj = jt, rk = kr$ ($k \in \mathbb{R}$)

$$i^2 = j^2 = k^2 = -1, \quad ij = -ji = k, \quad jk = -kj = i, \quad ki = -ik = j$$

56

设 $x \neq 0$, 设 $0 \neq x = ae + bi + cj + dk$

$$x^{-1} = \frac{1}{x} \text{ (自证)}$$

H 是可除环但不是域.

子环: $H \subseteq R$. 且 $(H, +) \leq (R, +)$, $(H, \cdot) \leq (R, \cdot)$

$$H \leq R \Leftrightarrow \forall a, b \in H, a-b \in H, a \cdot b \in H$$

子域: $H \subseteq R$ 且 $(H, +) \leq (R, +)$; $(H^*, \cdot) \leq (R^*, \cdot)$

设 $H \subseteq R$ 域, 则 $H \leq R$

$$\Leftrightarrow \forall a, b \in H, a-b \in H, a \cdot b^{-1} \in H$$

§2. 环同态基本定理.

群 环
子群 子环
正规子群 理想 (idea)

$$G/H = \{gH \mid g \in G\}. \quad \bar{g} \cdot \bar{h} = \overline{g \cdot h} \quad (\bar{g} = gH)$$

(正规子群才可以这么定义)

R/I 对加法已是正规子群.

$$\bar{r} = r + I \text{ (用加法作陪集)}$$

$\bar{r} + \bar{s} = \overline{r+s}$ 总是对的, 但 $\bar{r} \cdot \bar{s} = \overline{r \cdot s}$ 并不一定是对的.

57

引理: 设 I 是 R 的子环. 则 $\bar{r} \cdot \bar{s} = \overline{rs} \quad \forall \bar{r}, \bar{s} \in R/I$

是 well-defined $\Leftrightarrow I \triangleleft R$. (I 是 R 的理想)

设 $I \triangleleft R$ R/I 是环 R 关于 I 的商环.

$$R/I = \{r+I \mid r \in R\}$$

定义: 设 R 是环, $(I, +)$ ^{子环} 是 R 的理想:

$$\forall a, b \in I, a-b \in I.$$

$$\forall r \in R, \forall a \in I, \text{ 则 } ra, ar \in I.$$

例 $n\mathbb{Z} \triangleleft \mathbb{Z}$, $\mathbb{Z}$ 的任一子环均形如 $n\mathbb{Z}$, $n \geq 0$.
——理想 —— $n\mathbb{Z}'$, $n \geq 0$.

即 $\mathbb{Z}$ 的理想与子环是一样的.

理想的构造: 设 R 环. $\forall a \in R$, 用 $\langle a \rangle$ 表示 R 的包含 a 的最小的理想

$$\langle a \rangle = \mathbb{Z}a + aR + Ra + RaR$$

$$= \left\{ na + ar + ra + \sum_{i=1}^m s_i a t_i \mid n \in \mathbb{Z}, r, r', s, t \in R, m=1, 2, \dots \right\}$$

如果 R 交换环. 则 $\langle a \rangle = \mathbb{Z}a + aR$.

如果 R 有 1. 则 $\langle a \rangle = RaR$

如果 R 是交换环且有 1, 则 $\langle a \rangle = aR = Ra$.

58
 整环 R 称为主理想整环. 如果 R 中任一理想均是主理想.
 (主理想: 由一个元生成的理想)

$\mathbb{Z}$ p.i.d.

$R[x]$ ~~p.i.d.~~

∇
 $0 \neq I = \langle f(x) \rangle$ $f(x)$ 是 I 中次数最低的非 0 多项式

显然 $\langle f(x) \rangle \subseteq I$.

$\forall g(x) \in I$ 则 $g(x) = q(x)f(x) + r(x)$ (带余除法).

则 $r(x) \in I$ ~~矛盾~~ 故 $r(x) = 0$.

子集

$I + J = \{i+j \mid i \in I, j \in J\}$

$I \cdot J = \left\{ \sum_{i=1}^m a_i b_i \mid a_i, b_i \in I, m=1, 2, \dots \right\}$

环 R 称为单环

若 $R \neq \{0\}$ 且 R 仅有 $\{0\}$ 与 R 两个理想

例: $M_n(D)$ 是单环. D 是除环.

环同态基本定理: $f: R \rightarrow R'$, 满足

$$f(a+b) = f(a) + f(b)$$

$$f(ab) = f(a)f(b)$$

称 f 为环同态.

设 $f: R \rightarrow R'$ 环同态. 则 $\ker f \triangleleft R$. $\text{Im } f \leq R'$

$$\ker f = \{r \in R \mid f(r) = 0\}$$

$$\text{Im } f \cong \frac{R'}{\ker f}$$

环同构

子环对应定理: 设 $N \triangleleft R$, 则有一一对应
 $P = \{R \text{ 的子环 } H, H \supseteq N\}$.

$$\Omega = \{R/N \text{ 的子环}\} \quad H \longrightarrow H/N$$

$$R/N \text{ 的子环形如 } H/N. \quad H \leq R. \quad H \supseteq N.$$

$$\textcircled{1} \quad H/N \triangleleft R/N \iff H \triangleleft R.$$

第一同构定理. 设 $H \leq R, N \triangleleft R$. 则 $N \triangleleft H + N$, $H \cap N \triangleleft H$.

$$\textcircled{2} \text{ 且有环同构 } \frac{H+N}{N} \cong \frac{H}{H \cap N}.$$

第二同构定理: 设 $A \triangleleft R, B \triangleleft R$ 且 $A \triangleleft B$. 则有 $\frac{B}{A} \triangleleft \frac{R}{A}$.

$$\text{且 } \frac{(\frac{R}{A})}{(\frac{B}{A})} \cong \frac{R}{B}$$

60

§3 无零因子环的特征.

定义: 设 R 是有 1. 无零因子的非零环. ~~设 $a \neq 0$~~ . 设 $a \in R$.

用 $o(a)$ 表示 $o(a)$ 的加法阶.

~~定理~~: R 中任何非零元有相同的加法阶, 这个加法阶或者为 ∞

或者为素数 p . ~~如果~~ 定义 R 的特征 $\text{char } R \triangleq \begin{cases} R, & \text{if } o(1) = p \\ 0, & \text{if } o(1) = \infty \end{cases}$

证: 设 $o(1) = n < \infty$, 设 $a \neq 0$.
 $na = \underbrace{(n \cdot 1)}_{(n \text{ 倍的 } 1)} a = 0$. 说明 $o(a) | n$.

设 $o(a) = m$. $0 = ma = (m \cdot 1) a \Rightarrow m \cdot 1 = 0 \Rightarrow m | n$

$\Rightarrow m = n$.

若 $o(a) = \infty$. 设 $a \neq 0$. 若 $ma = 0$ 则 $(m \cdot 1) a = 0$
 $\Rightarrow m \cdot 1 = 0$ 矛盾! 即 $o(a) = \infty$.

设 $o(1) = n < \infty$. 若 $n = s \cdot t$ ($2 \leq s, t \leq n-1$).

则 $0 = n \cdot 1 = (st) \cdot 1 = (s \cdot 1) (t \cdot 1)$

$\Rightarrow s \cdot 1 = 0$ 或 $t \cdot 1 = 0$ 矛盾!

推论. 设 R 是有 1 的无 0 因子环, 特征为 p , $a, b \in R$ 且 $ab = ba$.

$$(a+b)^p = a^p + b^p \quad \text{一般地} \quad (a+b)^{p^n} = a^{p^n} + b^{p^n}.$$

特别地. 若 R 是域, 则特征 p $(a+b)^{p^n} = a^{p^n} + b^{p^n}$
($\forall a, b \in R$)

$$\text{证: } (a+b)^p = a^p + \sum_{i=1}^{p-1} \binom{p}{i} a^{p-i} b^i + b^p.$$

但 $p \mid \binom{p}{i}$ 故 $\binom{p}{i} a^{p-i} b^i = 0$.

$$\text{故 } (a+b)^p = a^p + b^p.$$

对 n 归纳即可.

§ 4. 整环的商域.

设 D 是整环 (即有 1 无 0 因子的交换环, 且非零环).

问题: 是否能将 D 嵌入到一个域 K 中?

即 $\exists$ 单同态 $D \hookrightarrow K$. 例如 $\mathbb{Z} \hookrightarrow \mathbb{Q}$

$$\text{令 } D^* = D - \{0\}, \quad D \times D^* = \{(s, t) \mid s \in D, t \in D^*\}$$

$\longleftrightarrow$

定义 $D \times D^*$ 上的一个关系 " $\sim$ ":

$$(s, t) \sim (s', t') \iff st' = s't$$

易证 $\sim$ 是等价关系 (自反性, 对称性, 传递性).

用 $\bar{s}$ 表示 (s, t) 所在的等价类

~~表示所有~~ 令 $K = \left\{ \frac{s}{t} \mid s \in D, t \in D^* \right\}$

① 先把 K 作成一域, 定义 $\frac{s}{t} + \frac{s'}{t'} = \frac{st' + ts'}{tt'}$ (*)

~~验证~~ (*) $\frac{s}{t} \cdot \frac{s'}{t'} = \frac{ss'}{tt'}$ (**)

验证 (*), (**) 是 well-defined. 则 $(K, +, \cdot)$ 是域
也就是说, 加法与乘法与代表元无关.

小学里会不会有小孩问为什么 $\frac{1}{3} + \frac{2}{5} = \frac{2}{6} + \frac{4}{10}$ 这才是天才
当然, 小学老师不会表扬这样的孩子.

$D \hookrightarrow K$

$d \mapsto \frac{d}{1}$ 验证是单同态.

K 是最小的

$D \hookrightarrow K' \text{ 域}$
 $\searrow$
 K

定义. 域 K 称为环 R 的高域

$\mathfrak{p}$ 极大理想. 素理想.

定义. 设 $I \triangleleft R$. 且 $I \neq R$.

(1) I 称为 R 的极大理想, 如果 $I \subseteq J \triangleleft R$. 则 $J = I$ or $J = R$
(极大理想可能有很多个)

(2) I 称为 R 的素理想. 如果 $A, B \triangleleft R$ 且 $AB \subseteq I$.

$\Rightarrow A \subseteq I$ 或 $B \subseteq I$ (理想之乘越来越小)

$$A \cdot B = \left\{ \sum_{\text{有限和}} a_i b_i \mid a_i \in A, b_i \in B \right\} \subseteq A \cap B.$$

例: $R = \mathbb{Z}$, $\mathbb{Z}$ 的极大理想是 $\langle p \rangle$, p 素数.

$\mathbb{Z}$ 的素理想是 $\langle p \rangle$, p 素数和 $\{0\}$.

定理: 设 $I \triangleleft R$, $I \neq R$, R 是有 1 的交换的(非零)环.

(1) I 极大 $\Leftrightarrow R/I$ 是域, 特别地 $\{0\}$ 是 R 的极大理想 $\Leftrightarrow R$ 是域

(2) I 素 $\Leftrightarrow R/I$ 是整环

特别地 $\{0\}$ 是素理想 $\Leftrightarrow R$ 是整环

证: (1) 设 I 极大. 则 R/I 有 1 的交换非零环

设 $\bar{r} = r + I \neq 0$ in R/I . 则 $r \notin I$.

$I \subseteq \langle r \rangle + I \triangleleft R$. 由 I 的极大性, $\langle r \rangle + I = R$

故 $\exists s \in R, i \in I$ 使 $1 = rs + i$. 则 $\bar{1} = \bar{r} \cdot \bar{s}$ in R/I

即 $\bar{r}$ 可逆 in R/I . 即 R/I 是域.

64

反之, 设 R/I 是域, 设 $I \subseteq J \triangleleft R$.

取 $j \in J, j \notin I$. 则 $\bar{j} \neq 0$ in R/I .

$\exists \bar{s} \in R/I$ s.t. $\bar{j} \cdot \bar{s} = 1$ 即 $1-j \in I$.

$1 \in j+I \subseteq J$ 故 $J = R$ 即 I 极大 $\square$

(2) 设 I 是 R 的极大理想, 则 R/I 是域

设 $\bar{r} = r+I \neq 0$ in R/I

$\bar{s} = s+I \neq 0$ in R/I .

(反证) 设 $\bar{r} \cdot \bar{s} = 0$ in R/I .

$rs \in I$. 即 $\langle r \rangle \cdot \langle s \rangle \subseteq I$.

因为 I 是极大理想, 故 $\langle r \rangle \subseteq I$ 或 $\langle s \rangle \subseteq I$

即 $r \in I$ 或 $s \in I$ 矛盾!

反之, 设 R/I 是整环. 设 $A, B \triangleleft I$ 且 $A, B \subseteq I$.

且 $A \neq \{0\}$. 往证 $B \subseteq I$.

任取 $b \in B$. 取 $a \in A$ 但 $a \notin I$.

$ab \in I$ $a\bar{b} = 0$ in R/I .

因为 R/I 是整环, 且 $a \neq 0$.

于是 $\bar{b} = 0$

故 $b \in I$ 即 $b \in I$

(1) 极大理想是素理想; 反之不对.

(2) 主理想非0. 素理想一定是极大理想. (作业)

证: (1) 设 M 极大 设 $A, B \triangleleft R$ 且 $AB \subseteq M$.
要证 $A \subseteq M$ 或 $B \subseteq M$.

(反证) 若 $A \not\subseteq M$ 且 $B \not\subseteq M$.

$$R = R^2 = (A+M)(B+M) = AB + AM + MB + M^2 \subseteq M \\ \Rightarrow M = R. \text{ 矛盾!}$$

$\mathbb{Z}[x]$ (整数环上的多项式环) $\langle x \rangle$ 是素理想

$$\mathbb{Z}[x]/\langle x \rangle \cong \mathbb{Z}$$

但 $\langle x \rangle$ 不是极大理想.

$$\langle x \rangle \subsetneq \langle 2, x \rangle \subsetneq \mathbb{Z}[x]$$

(带表证为偶数)

~~极大~~

故 $\langle x \rangle$ 非极大.

§6. 环的直和.

$R_1, \dots, R_n$ 都是环. 令 $R_1 \times \dots \times R_n = \{ (r_1, \dots, r_n) \mid r_i \in R_i, 1 \leq i \leq n \}$

定义 "+": $(r_1, \dots, r_n) + (r'_1, \dots, r'_n) = (r_1 + r'_1, \dots, r_n + r'_n)$ 第 i 个环中的加法

"·": $(r_1, \dots, r_n) \cdot (r'_1, \dots, r'_n) = (r_1 r'_1, \dots, r_n r'_n)$ 第 i 个环中的乘法

则 $(R_1 \times R_2 \times \dots \times R_n, +, \cdot)$ 为环, 称为 $R_1, \dots, R_n$ 的直和.

记为 $R_1 \oplus \dots \oplus R_n$

66

$$\text{令 } R' = \{(0, 0, \dots, r_i, \dots, 0) \mid r_i \in R_i\}$$

$$\text{则 } R' \triangleleft R \quad (r=1, \dots, n)$$

$$R'_i \cong R_i \text{ 环同构}$$

problem. ~~如何分解一个环R~~ 给定一个环R, ~~如何~~^{何时}将R

分解成R的一些理想 $I_1, \dots, I_n$ 的直和.

定理: 设 $I_1, \dots, I_n \triangleleft R$. 则 $R = I_1 \oplus \dots \oplus I_n$

$\Leftrightarrow$ R 的任一元素均可唯一地写成

$$r = r_1 + \dots + r_n, \quad r_i \in I_i$$

§ 7. 中国剩余定理 (CRT)

设 $m_1, \dots, m_n$ 两两互素, $m_i \in \mathbb{Z} \quad (i=1, \dots, n)$

$$\text{不定方程} \begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \vdots \\ x \equiv a_n \pmod{m_n} \end{cases}$$

如何求解.

环论中的 CRT:

设 R 有非 0 环, $I, J \triangleleft R$ 且 I, J 互素, 若 $I+J=R$

67

中国剩余定理 Chinese Remainder Theorem

设 R 是有单位元的非零环. 设 $I_1, \dots, I_n$ 是 R 的两两互素的理想, 则有环同构:

$$R / I_1 \cap \dots \cap I_n \cong R / I_1 \oplus \dots \oplus R / I_n \quad (\text{典范同构, 映射是固定的})$$

$$r + I_1 \cap \dots \cap I_n \mapsto (r + I_1, \dots, r + I_n)$$

$$\text{即 } \bar{r} \mapsto (\bar{r}_1, \dots, \bar{r}_n)$$

- 证: (1) well-defined. 显然 (设 $r - r' \in I_1 \cap \dots \cap I_n, R \mid r - r' \in I_i$
 (2) 环同态. 显然. 原像
 (3) 单射. 只需验证映成像是 0. 显然.
 (4) 满射

要证: $(a_1 + I_1, \dots, a_n + I_n) \in R / I_1 \oplus \dots \oplus R / I_n, \exists r \in R$
 $(r + I_1, \dots, r + I_n) = (a_1 + I_1, \dots, a_n + I_n)$

$$R \mid \begin{cases} r - a_1 \in I_1 \\ \vdots \\ r - a_n \in I_n \end{cases}$$

这是中国剩余定理高超之处

$$\text{即 } \begin{cases} x \equiv a_1 \pmod{I_1} \\ \vdots \\ x \equiv a_n \pmod{I_n} \end{cases} \text{ 有解.}$$

68

$$R = R^2 = (I_1 + I_2)(I_1 + I_3) \subseteq I_1 + I_2 I_3 \subseteq R$$

$$\text{故 } I_1 + I_2 I_3 = R$$

$$R = R^2 = (I_1 + I_2 I_3)(I_1 + I_4) \subseteq I_1 + I_2 I_3 I_4 \subseteq R$$

$$\text{故 } I_1 + I_2 I_3 I_4 = R$$

$$\text{一般地, } I_1 + I_2 I_3 \cdots I_n = R$$

$$\text{一般地, } I_i + \prod_{\substack{j \neq i \\ \text{按顺序乘}}} I_j = R \quad (1 \leq i \leq n)$$

$$\text{故 } \exists s_i + r_i = 1 \quad s_i \in I_i$$

$$r_i \in \prod_{\substack{j \neq i \\ \text{按顺序}}} I_j$$

$$\text{故 } r_{i-1} \in I_i$$

$$\text{显然 } r_i \notin I_i \text{ 否则 } 1 \in I_i \Rightarrow I_i = R \text{ 矛盾!}$$

$$r_i \in I_j \quad (j \neq i)$$

令 $r = a_1 r_1 + \dots + a_n r_n$ 具有 $\begin{cases} r - a_i \in I_i \\ r - a_n \in I_n \end{cases}$ 的性质.

$$r - a_i = a_1 r_1 + \dots + a_n r_n - a_i$$

$$= a_i(r_i - 1) + \sum_{j \neq i} a_j r_j \quad \rightarrow \text{也属于 } I_i$$

$\leftarrow \in I_i \quad (i=1, \dots, n) \quad \text{证完}$
属于 I_i

例一. 今有物不知数, 三三数之剩二, 五五数之剩三, 七七数之剩二.
问物几何?

解: $\begin{cases} x \equiv 2 \pmod{3} \\ x \equiv 3 \pmod{5} \\ x \equiv 2 \pmod{7} \end{cases}$ ~~$x = r = 2r_1 + 5r_2 + 7r_3$~~
 $x = r = 2r_1 + 3r_2 + 2r_3$

$$Z = I_i + \prod_{j \neq i} I_j = \langle m_i \rangle + \langle \frac{m_1 \dots m_n}{m_i} \rangle$$

$$1 = s_i + r_i$$

$$(3, 35) = 1, \quad 3(-23) + 35(2) = 1 \quad r_1 = 70$$

$$(5, 21) = 1 \quad 5(-4) + 21(1) = 1 \quad r_2 = 21$$

$$(7, 15) = 1 \quad 7(-2) + 15(1) = 1 \quad r_3 = 15$$

70

$$r = \cancel{2 \times 70} + 3 \cdot 21 + 2 \cdot 15$$

$$= 233 \equiv 23 \pmod{105}$$

秘密共享: $S = r$.

problem: 秘密 S - n 个人联手可解.

任何 $(n-1)$ 个联手均不可解.

用的是公开密钥算法. 安全 ~~性~~ 建立在计算的困难上.

one-way function.

取 $m_1, \dots, m_n$ 两两互素的整数, 公开

$$a_1, \dots, a_n, \text{ 令 } S_i < m_1 \dots m_n \text{ 且 } S_i \equiv \frac{m_1 \dots m_n}{m_i}$$

$$(i=1, \dots, n)$$

用 S 降以 $\frac{m_1 \dots m_n}{m_i} (i=1, \dots, n)$ 得到的余数为 a_i :

$$r = a_1 r_1 + a_2 r_2 + \dots + a_n r_n$$

$$r \equiv a_i \pmod{m_i}$$

把 a_i 给第 i 个人 (子密钥) 如此加密

$R = R_1 \oplus \dots \oplus R_n$. 则环的单位群 $U(R) = U(R_1) \times \dots \times U(R_n)$

$n = p_1^{r_1} \dots p_m^{r_m}$ 素分解. $U(R) = \{R \text{ 的可逆元}\}$

$$I_1 = \langle p_1^{r_1} \rangle, \dots, I_m = \langle p_m^{r_m} \rangle$$

$$\cancel{I_1 I_n = \langle n \rangle} \quad I_1 \cap \dots \cap I_m = \langle n \rangle.$$

$$\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{r_1}} \oplus \dots \oplus \mathbb{Z}_{p_m^{r_m}}.$$

$$U(\mathbb{Z}_n) \cong U(\mathbb{Z}_{p_1^{r_1}}) \times \dots \times U(\mathbb{Z}_{p_m^{r_m}}).$$

$$U(\mathbb{Z}_n) \quad \exists \cdot \bar{t} = \bar{1} \Rightarrow 1 - st \in n\mathbb{Z} \quad st + nm = 1.$$

$$\Leftrightarrow (s, n) = 1.$$

两边 $\cdot 1$

$$\text{则有 } \varphi(n) = \varphi(p_1^{r_1}) \dots \varphi(p_m^{r_m})$$

$$= (p_1^{r_1} - p_1^{r_1-1}) \dots (p_m^{r_m} - p_m^{r_m-1})$$

$$= \prod_{i=1}^m p_i^{r_i-1} (p_i - 1) = n \prod_{i=1}^m (1 - \frac{1}{p_i})$$

Euler 数公式.

复习

设 G 是群, Ω 是一集合, 如果有在群同态 $G \rightarrow S(\Omega)$,
 其中 $S(\Omega) = \{g: \Omega \rightarrow \Omega \text{ 一一映射}\}$ 是 Ω 的对称群, 则称 G 在 Ω
 上有一个群作用.

S_n 是可解群 $\Leftrightarrow n \leq 4$.

A_4 是可解群 $\Leftrightarrow n \leq 4$.

§7. 整环中的因子分解理论.

D 整环. $u(D) = \{a \in D \mid a \neq 0, a \text{ 可逆}\}$. 即 D 的单位群.

$a, b \in D$.

$a \mid b \Leftrightarrow \exists c \in D \text{ s.t. } b = ac$ 即 a 是 b 的因子.

单位是任一元的因子. $u(\mathbb{Z}) = \{\pm 1\}$

称 $a \sim b \Leftrightarrow \exists c \in u(D), \text{ s.t. } b = a \cdot c$.

$\sim$ 等价关系. a 的相伴称为是 a 的因子

a 是 b 的真因子. 如果 $a \mid b, a \notin u(D)$. a 与 b 不相伴

素元 p . $p \neq 0, p \notin u(D)$. 若 $p \mid ab$ 则 $p \mid a$ 或 $p \mid b$.

不可约元 p . $p \neq 0, p \notin u(D)$. p 无真因子 (若 $a \mid p$, 则 $a \in u(D)$ 或 $a \sim p$)

$$D = \mathbb{Z}[\sqrt{-3}] = \{a + b\sqrt{-3} \mid a, b \in \mathbb{Z}\}.$$

$$\text{则 } U(D) = \{1, -1\} \quad (|(a+b\sqrt{-3})(c+d\sqrt{-3})| = 1 \Rightarrow (a^2+3b^2)(c^2+3d^2)=1)$$

~~2是不可约元~~ $\pm 2, 1 \pm \sqrt{-3}$ 是不可约元.

但它们均不是素元. $2 \mid (1+\sqrt{-3})(1-\sqrt{-3})$

但 $2 \nmid 1 \pm \sqrt{-3}$.

于是在一般的整环中, 不可约元与素元不等价; 素元更强.

Def: 整环 D 称为 UFD (唯一 ~~分解~~ 因子分解整环). 如果我们要用不可约元写成 UFD.

(1) 任一非 0 非单位元的元均可写成有限个不可约元的乘积.

(2) 设 $a = p_1 \cdots p_s = q_1 \cdots q_t$ 且 $p_1, \dots, p_s; q_1, \dots, q_t$ 均为不可约元.

则 $s=t$, 且 $\exists \{1, \dots, s\}$ 的置换 σ s.t. $q_i \sim p_{\sigma(i)}$
 $i=1, \dots, s$.

例 10 $6 = 2 \cdot 3 = (-3)(-2)$ 为唯一分解.

例: $\mathbb{Z}[\sqrt{-3}]$ 非 UFD: $4 = 2 \cdot 2 = (1+\sqrt{-3})(1-\sqrt{-3})$

74

引理: (1) 素元是不可约元. 反之未必

(2) p 素元 $\Leftrightarrow \langle p \rangle$ 是非 0 素理想

(3) p 不可约元 $\Leftrightarrow \{ \langle a \rangle \mid a \neq 0, a \in U(D) \}$ 中极大元

(4) 若 D 是 ~~主理想~~ PID, 则不可约元也是素元

证 (4), 其余留给读者.

设 p 是不可约元, 设 $p \mid ab$ 且 $p \nmid a, p \nmid b$

则 $\langle a \rangle \not\subseteq \langle p \rangle, \langle b \rangle \not\subseteq \langle p \rangle$.

$\langle a \rangle + \langle p \rangle \not\subseteq \langle p \rangle$ 且 $\langle b \rangle + \langle p \rangle \not\subseteq \langle p \rangle$

令 $\langle a \rangle + \langle p \rangle = \langle c \rangle, \langle b \rangle + \langle p \rangle = \langle d \rangle$

则 $\langle c \rangle \langle d \rangle = (\langle a \rangle + \langle p \rangle)(\langle b \rangle + \langle p \rangle)$

$= \langle ab \rangle + \langle p \rangle \subseteq \langle p \rangle$. 于是

于是可取 $x \in \langle c \rangle, x \notin \langle p \rangle$.

$y \in \langle d \rangle, y \notin \langle p \rangle$

于是 $\langle x \rangle \langle y \rangle \subseteq \langle p \rangle$

~~于是~~

$\langle a \rangle + \langle p \rangle = \langle c \rangle \Rightarrow \langle p \rangle \subseteq \langle c \rangle \Rightarrow c \mid p$

~~$\langle b \rangle + \langle p \rangle = \langle d \rangle$~~ $\Rightarrow \langle p \rangle \subseteq \langle d \rangle \Rightarrow d \mid p$

p 是真因子，故 $c \in U(D)$ 或 $c \sim p$.

若 $c \sim p$ ，则 $\langle c \rangle = \langle p \rangle$ 与 $\langle c \rangle = \langle a \rangle + \langle p \rangle \not\subseteq \langle p \rangle$ 矛盾！

同理 $d \not\sim p$ ，从而 ~~$c \in U(D)$~~ $c \in U(D)$
 $d \in U(D)$

故 $\langle cd \rangle = D$ (因为 cd 是单位) $\left(\begin{array}{l} D = \langle c \rangle \langle d \rangle \subseteq \langle p \rangle \\ \Rightarrow \langle p \rangle = D \\ \Rightarrow p \text{ 是单位} \end{array} \right)$

于是 p 是单位，矛盾！

定理：~~下述等价~~ 设 D 是整环，则下述等价

- (1) D 是 UFD
- (2) (P1) 不存在无限长的链，使 $a_1, \dots, a_n, \dots$ 使 a_{i+1} 是 a_i 的真因子
 (P2) 不可约元也是素元

- (3) (P1) 与上述 (P1) 相同
 (P3) 任意两个非零元均有最大公因子 (a, b)

- (4) (P1) 与上述 (P1) 相同
 (P4) 任意两个非零元均有最小公倍元 $[a, b]$

76

若 $a, b \neq 0$. d 称为 a, b 的最大公因子.

如果 $d|a, d|b$.

② 若 $d'|a$ 且 $d'|b$ 则 $d'|d$.

性质: (a, b) 若存在, 则 "唯一" (相伴的意义下)

$\neq (a, b)$ 不一定存在.

类似定义最小公倍元

推论: PID 一定是 UFD.

证: 在 PID 中, 不可约元是素元.

设 $\exists \langle a_1 \rangle \subsetneq \langle a_2 \rangle \subsetneq \langle a_3 \rangle \subsetneq \dots$

$\bigcup_{i=1}^{\infty} \langle a_i \rangle$ 也是理想. $= \langle c \rangle$

即 $c \in \langle a_n \rangle \Rightarrow \langle c \rangle \subseteq \langle a_n \rangle$

$\langle a_{n+1} \rangle \subseteq \langle a_n \rangle, \langle a_{n+2} \rangle \subseteq \langle a_n \rangle, \dots$

即 $\langle a_n \rangle \subsetneq \langle a_{n+1} \rangle$ 矛盾!

§ 6 UFD.

定理: 设 D 是整环, 则下述等价.

1. D 是 UFD

2. D 满足性质 (P1) 与 (P2)

(P1): 不存在无限长的链 $a_1, a_2, \dots$, 使得 a_{i+1} 是 a_i 的真因子

(P2): 不可约元都是素元.

3. D 满足性质 (P1) 与 (P3)

(P3) 任意两非零元都有最大公因子

4. D 满足性质 (P1) 与 (P4)

(P4) 任意两非零元都有最小公倍元

证: (1) $\Rightarrow$ (2) 先证 (P1) ~~设 a 是 a 的真因子~~. (P1) 是相当显然的

设 p 是不可约元. 设 $p|ab$. $ab = pc$

$$(a_1 \dots a_s)(b_1 \dots b_t) = p(c_1 \dots c_l)$$

$\Rightarrow p|a$ 或 $p|b$ (因为 p 与某个 a_i 或 b_j 相伴. 这是定义保证的)

(2) $\Rightarrow$ (1) 断言 1: 设 $a \neq 0$. ~~若 $a \in U(D)$~~ 则 a 必有不可约因子.

证: 若 a 不可约 则 ok

若 a 可约. 则 a 存在真因子 a_1

若 a_1 不可约 则 ok

若 a_1 可约. 则 a_1 有真因子 a_2

由 (P1) 保证有步骤终止. 则 a 有不可约因子

78

设 $a \neq 0, a \notin U(D)$. 由断言知 $a = p_1 a_1$, p_1 是不可约元.

若 $a_1 \in U(D)$, 则 OK

若 $a_1 \notin U(D)$, 则 $a = p_1 (p_2 a_2)$

若 $a_2 \in U(D)$, 则 OK

若 $a_2 \notin U(D)$ 则 $a = p_1 p_2 (p_3 a_3)$

(P1) 设 $a_1, a_2, \dots$ 满足 $a_2 | a_1, a_3 | a_2, \dots$

则 $\exists N, \forall n > N, a_n \sim a_{n+1} \sim \dots$

(P1) $\Leftrightarrow$ (P1') 显然

这一过程不可能无限下去, 否则取 $a, p_2 p_3, p_3 p_4, \dots$, 满足 (P1'), 产生矛盾! (璋璞认为 $p_2 p_3 \dots$ 写法并不好, 但没有想出更好的办法).

设 $a_1 \dots a_s = b_1 \dots b_t$, $a_1, \dots, a_s, b_1, \dots, b_t$ 不可约.

a_i 是素元, $a_i | b_1 \dots b_t \Rightarrow a_i | b_{t_i}$

由此易知唯一性成立.

$$a = c_1^{m_1} \dots c_l^{m_l}$$

$$b = c_1^{m'_1} \dots c_l^{m'_l}$$

$$m_1, \dots, m_l \geq 0$$

$$m'_1, \dots, m'_l \geq 0.$$

$$\text{取 } n_i = \min \{ m_i, m'_i \}$$

$$\text{则 } (a, b) = c_1^{n_1} \dots c_l^{n_l}. \text{ 易验证此式成立.}$$

79

高斯定理: 设 D 是 UFD. 则多项式环 $D[x]$ 是 UFD.
 $D[x_1, \dots, x_n]$ 是 UFD.

例: $\mathbb{Z}[x]$ 是 UFD, 但 $\mathbb{Z}[x]$ 不是 PID.

§ 7 ED. (欧几里德整环)

设 D 是整环, 如果 $\exists \varphi: D^* = D - \{0\} \rightarrow \mathbb{N} = \{0, 1, 2, \dots\}$

s.t. $\forall a, b. b \neq 0. \exists q, r \in D$ 满足

$$a = qb + r, \quad r = 0 \text{ 或 } \varphi(r) < \varphi(b).$$

则称 D 是欧几里德整环, 简称 ED. (其实 φ 为一范数
在范数意义下带余除法)

例: $\mathbb{Q}$ 是 ED. 取 $\varphi = |\cdot|$

• 域是 ED. 因为 $r = 0$.

• $F[x]$ 是 ED. F 是域. $\varphi = \deg(F[x])$

例: $\mathbb{Z}[\sqrt{-1}] = \{a + b\sqrt{-1} \mid a, b \in \mathbb{Z}\}$ 是 ED.

证: $\varphi: \mathbb{Z}[\sqrt{-1}] \rightarrow \mathbb{N}$

$$\alpha \mapsto |\alpha|^2 \text{ 范数平方}$$

$$a + b\sqrt{-1} \mapsto a^2 + b^2$$

α, β s.t. $\beta \neq 0. \in \mathbb{Z}[\sqrt{-1}]$

$$\boxed{\alpha = \frac{\alpha}{\beta} \cdot \beta}$$

但 $\frac{\alpha}{\beta}$ 不一定 $\in \mathbb{Z}[\sqrt{-1}]$

设 $\frac{\alpha}{\beta} = a+bi \in \mathbb{Q}[\sqrt{-1}]$

取 $c+di \in \mathbb{Z}[i]$

s.t. $|a-c| \leq \frac{1}{2} \quad |b-d| \leq \frac{1}{2}$

则 $\alpha = (c+di)\beta + \underbrace{(a-c) + (b-d)i}_{\downarrow}$

则 $\varphi(r) = \left| (a-c) + (b-d)i \right| \leq \frac{1}{2} \varphi(\beta) < \varphi(\beta)$

需要验证. $r \in \mathbb{Z}[i]$ 这是因为 $\alpha = \underbrace{\alpha}_{\in \mathbb{Z}[i]} - \underbrace{(c+di)\beta}_{\in \mathbb{Z}[i]} \in \mathbb{Z}[i]$

作业. $\mathbb{Z}[\sqrt{-1}]$ 也是 ED.

定理: ED 是 PID.

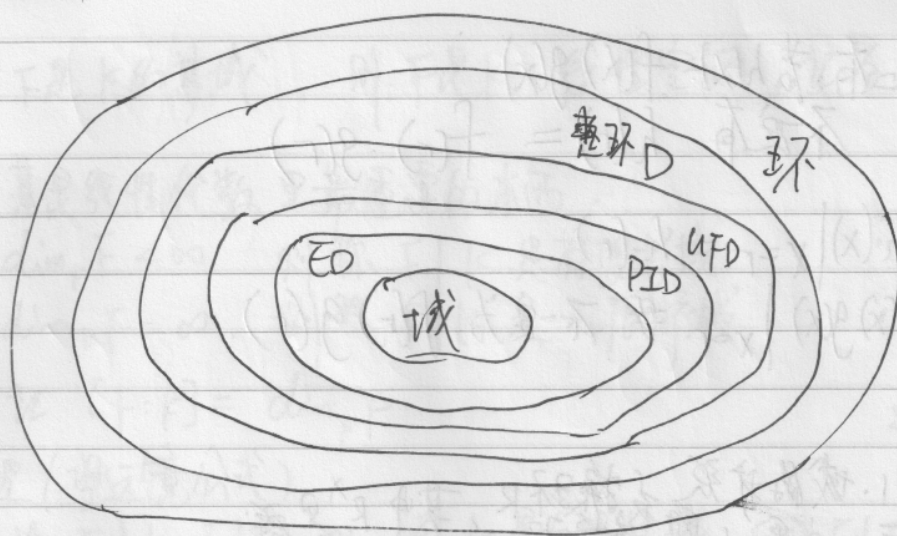
证: 设 D 是 ED. 为 D 的非 0 理想.

令 $a \neq 0, a \in I$ 且 $\varphi(a) = \min \{ \varphi(x) \mid x \in I, x \neq 0 \}$

则 $I = \langle a \rangle$. 这是因为 $\langle a \rangle \subseteq I \quad \forall b \in I \quad b = qa + r$.

因为 $\varphi(r) < \varphi(a)$, 故 $r=0$
或 $r=0$, 由 a 的选法知, $r=0$

即 $b \in \langle a \rangle$ 即 $I = \langle a \rangle$



是环不是整环: n 阶全矩阵环.

是D不是UFD: $\mathbb{Z}[\sqrt{5}]$

是UFD不是PID: 自己想

是PID不是ED: 1949年一篇文章中, 比较困难.

是域不是域: 自己想

多项式环

R 是环 $R[X]$ 为 R 上的多项式环.

$$R[X] \triangleq \left\{ a_0 + a_1x + \dots + a_nx^n \mid \begin{array}{l} n=1,2,\dots \\ a_0, \dots, a_n \in R \end{array} \right\}.$$

例: $\mathbb{Z}_2 = \{0, 1\}$ $x^2+1 \neq x+1$ 令 $f = x^2+1$, $g = x+1$ 即 $f \neq g$
 但 $f(0) = g(0) = 1$, $f(1) = g(1) = 0$.

我们规定 $f = g \iff$ 每一项系数均相同.

非交换环上有: 若 $h(x) = f(x)g(x)$

$$\text{不一定有 } h(r) = f(r) \cdot g(r)$$

$$\text{因为 } h(x)|_{x=r} = h(r)$$

$$f(x)g(x)|_{x=r} \text{ 不一定为 } f(r)g(r)$$

第三章 §1. 域的扩张 (交换环 R , 其中 R^* 是群)
域至少有两个元: 0 和 1. ~~的交换环~~

例如 $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_p$.

$F \subseteq K$, 记为 $K|F$. K 是 F 的扩张.

F 素域: 没有真子域的域称为素域
即 F 的任何真子集均不是域.

$$\text{char } F = 0 \Rightarrow \frac{m \cdot 1}{n \cdot 1} \in F. \text{ (因为 } n \cdot 1 \neq 0)$$

$$\text{即 } F \cong \mathbb{Q}.$$

$$\text{char } F = p. F = \{1, \dots, p-1\} \cong \mathbb{Z}_p.$$

命题: (1) 特征为 0 的素域同构于 $\mathbb{Q}$

特征为 p 的素域同构于 $\mathbb{Z}_p$

(2) 任何一个域均包含唯一的素域

$$F \supseteq \{1 \text{ 生成的子域} \}$$

设 F 是 K 的扩域, 则 F 是 K -线性空间, 记为 ${}_K F$

基是线性代数里最重要的东西.

若 $\dim_K F < \infty$ 则称 $F|K$ 是有限扩域

若 $\dim_K F = \infty$ 则称 $F|K$ 是无限扩域

$$\text{记 } [F:K] = \dim_K F$$

• $(F, +)$ 是 Abel 群

• $K \times F \rightarrow F$
 $\downarrow$
 $\lambda \cdot a \in F$
 数域.

引理 (塔远镜公式)

设 $F|K, E|F$, 则 $E|K$ 是有限扩域 $\Leftrightarrow E|F, F|K$ 均是有限扩域

$$[E:K] = [E:F][F:K]$$

证: 设 $\{a_i | i \in I\}$ 是 $E|F$ 的一组基. $[E:F] = |I|$

$\{b_j | j \in J\}$ 是 $F|K$ 的一组基. $[F:K] = |J|$

要证 $\{a_i b_j | i \in I, j \in J\}$ 是 $E|K$ 的一组基

(• $\{a_i b_j | i \in I, j \in J\}$ 是 K -无关

• $\forall x \in E, x$ 均可写成这组元的 K -组合

设 $F|K$. 设 $S \subseteq F$, $K(S)$ 是 F 的包含 S 和 K 的最小域

$$\bigcap \{L \mid L \text{ 是 } F \text{ 的子域, } L \supseteq S\}$$

$F \supseteq$

$$K(S) = \left\{ \frac{f(s_1, \dots, s_m)}{g(s_1, \dots, s_m)} \mid \begin{array}{l} f(x_1, \dots, x_m), g(x_1, \dots, x_m) \in K[x_1, \dots, x_m] \\ s_1, \dots, s_m \in S; n=1, 2, \dots \\ g(s_1, \dots, s_m) \neq 0 \end{array} \right\}$$

Boshi

性质: (1) 设 $S_1, S_2 \subseteq F$. 则 $k(S_1 \cup S_2) = (k(S_1))(S_2)$

我们约定: $k(a_1, \dots, a_n) = k(a_1)(a_2) \dots (a_n)$ 依次累加.

由上述性质得证.

(2) ~~设~~ 设 $a \in k(S)$, 则存在 S 的有限子集 S'

s.t.: $a \in k(S')$

设 $F \subseteq k$. $a \in k$. 考虑折线 $F(a) = \left\{ \frac{f(a)}{g(a)} \mid \begin{array}{l} f(x), g(x) \in F[x], \\ g(a) \neq 0 \end{array} \right\}$

a 是 F 上代数元. ~~若~~ 若 $\exists$ 非 0 多项式 $f(x) \in F[x]$. s.t. $f(a) = 0$.
 a 是 F 上超越元. 否则

设 a 是 F 上的代数元. 将 $F[x]$ 中首 1 的, 以 a 为根的次数最低的非 0 多项式 $f(x)$. 称为 a 在 F 上的极(小)多项式.

⌋. 设 a 是 F 上的代数元. 则下述等价.

(1) $f(x)$ 是 a 在 F 上的极小多项式.

(2) $f(x)$ 首 1. $f(a) = 0$. $f(x)$ 是 $F[x]$ 中不可约多项式.
 (不能写成次数更低的多项式之积)

(3) $f(x)$ 首 1. $f(a) = 0$.

若 $g(x) \in F[x]$. 且 $g(a) = 0$.

则 $f(x) \mid g(x)$

例. 求 $\sqrt{2} + \sqrt{3}$ 在 $\mathbb{Q}[\sqrt{6}]$ 上的极小多项式

$$(\sqrt{2} + \sqrt{3})^2 = 5 + 2\sqrt{6}$$

$$x^2 - (5 + 2\sqrt{6}) \in \mathbb{Q}(\sqrt{6})[x]$$

是 $\sqrt{2} + \sqrt{3}$ 在 $\mathbb{Q}(\sqrt{6})$ 的极小多项式.

定理: 设 $F \subseteq K$, $a \in K$.

(1) 若 a 在 F 上代数, 则 $F(a) \cong \frac{F[x]}{\langle f(x) \rangle}$, 其中 $f(x)$ 是在 F 上的极小多项式

$$\text{且 } [F(a):F] = n = \deg f(x).$$

且 $1, a, \dots, a^{n-1}$ 是 $F(a)$ 在 F 上的一组基.

$$\text{即 } F(a) = \{C_0 + C_1 a + \dots + C_{n-1} a^{n-1} \mid C_i \in F\}$$

且表达唯一.

(2) 若 a 在 F 上超越

$$\text{则 } F(a) \cong F(x) = \left\{ \frac{f(x)}{g(x)} \mid f(x), g(x) \in F[x], g(x) \neq 0 \right\}$$

有限整环必是域

$$\text{设 } P = \{0, a_1, \dots, a_n\}$$

$$a_i R = \{0, a_1 a_i, a_2 a_i, \dots, a_n a_i\} \quad (*)$$

$$a_i a_i = a_i a_j \Leftrightarrow a_i (a_i - a_j) = 0 \Leftrightarrow a_i = a_j \Leftrightarrow i = j$$

故 (*) 中元素两两相异. 必 $\exists a_k$ 使 $a_i a_k = 1$ 即 $a_i^{-1} = a_k$

PID 中, 非零素理想 = 极大理想

" $\supseteq$ " $\overset{\text{IAP}}{\text{I 极大}} \Rightarrow R/I \text{ 是域} \Rightarrow R/I \text{ 是整环} \Rightarrow I \text{ 非零素理想}$

" $\subseteq$ " $I \text{ 非零素理想}$

$$I \neq (x) \subseteq (y)$$

$$x = yz, yz \in (x)$$

由于 (x) 素, 故 $y \in (x)$ 或 $z \in (x)$

$$(1) y \in (x)$$

$$y = xw \text{ 或 } y = yzw \Rightarrow zw = 1 \Rightarrow \cancel{x \sim y}, z \in U(R)$$

$$\Rightarrow x \sim (y)$$

$$\Rightarrow (x) = (y)$$

$$(2) z \in (x)$$

$$z = xu, x = yxu = xyu \Rightarrow yu = 1 \Rightarrow (y) = R$$

$$\text{即 } (y) = (x) \text{ 或 } (y) = R$$

故 I 极大

$K|F$. ~~$F|K$~~ $\dim_F F$.

$$F \subseteq K, u \in K, F(u)$$

$$\pi: F[x] \rightarrow F[u] \subseteq F(u) \subseteq K,$$

$$g(x) \mapsto g(u).$$

Case 1. 设 u/F 代数, $f(x)$ 是 u 在 F 上的极小多项式.

$$\ker \pi = \langle f(x) \rangle$$

~~$F[x]$~~ 故 $F(u) \cong F[x] / \langle f(x) \rangle$. 因为 $f(x)$ 在 F 上不可约

故 $\langle f(x) \rangle$ 是 $F[x]$ 的极大理想.

即 $F[x] / \langle f(x) \rangle$ 是域 即 $F(u)$ 是域.

$$\text{于是 } F(u) = F(u) = \{a_0 + a_1 u + \dots + a_{n-1} u^{n-1} \mid a_i \in F, n = \deg f(x)\}$$

即 $1, u, \dots, u^{n-1}$ 是 $F(u)$ 的一组 F -基.

Case 2. 设 u/F 超越 $\ker \pi = \{0\}$.

$$F(u) \cong F[x] / \{0\} \cong F[x].$$

$$\text{即 } F(u) \cong F(x)$$

单扩域结构定理. 设 $K|F, u \in K$

1) 若 u/F 代数, 则 $[F(u):F] = n$.

n 是 u 在 F 上的极小多项式的次数.

且 $1, \dots, u^{n-1}$ 是 $F(u)$ 的一组 F -基.

$$a_i \in F, F(u) \cong F[x] / \langle f(x) \rangle$$

12) u 在 F 上超越. 则 $F(u) \cong F(x)$.

例: 设 u 是 $f(x) = x^3 + 2x + 1 \in \mathbb{Q}[x]$ 的一个实根.
 则 $f(x)$ 是 u 在 $\mathbb{Q}$ 上的极小多项式 (验证之)
 $[\mathbb{Q}(u) : \mathbb{Q}] = 3$

$$\text{设 } \frac{1}{u+1} = a_0 + a_1 u + a_2 u^2 \quad (\text{待定系数})$$

$$1 = (u+1)(a_0 + a_1 u + a_2 u^2)$$

$$\Leftrightarrow 1 = a_2 u^3 + (a_1 + a_2) u^2 + (a_0 + a_1) u + a_0$$

$$\Rightarrow a_2 u^3 + (a_1 + a_2) u^2 + (a_0 + a_1) u + a_0 = 0$$

$$\Rightarrow \begin{cases} a_2 = 0 \\ a_1 + a_2 = 0 \\ a_0 + a_1 = 2 \\ a_0 = -1 \end{cases} \Rightarrow \begin{cases} a_0 = 0 \\ a_1 = 0 \\ a_2 = 0 \end{cases} \quad \begin{cases} a_0 = 0 \\ a_1 = 2 \end{cases}$$

$$\Leftrightarrow 1 = a_2(1 - 2u) + (a_1 + a_2)u^2 + (a_0 + a_1)u + a_0$$

$$\Rightarrow 1 = a_0 + a_2 + (a_1 + a_0 - 2a_2)u + (a_2 + a_1)u^2$$

$$\Rightarrow \begin{cases} a_0 + a_2 = 1 \\ a_0 + a_1 - 2a_2 = 0 \\ a_1 + a_2 = 0 \end{cases}$$

$$\Rightarrow \begin{cases} a_0 = \frac{3}{4} \\ a_1 = -\frac{1}{4} \\ a_2 = \frac{1}{4} \end{cases}$$

设 $K|F$. $\text{Aut } K = \{ f: K \rightarrow K \text{ 域同构} \}$ is a group?

$$\text{Gal}(K|F) \triangleq \{ f: K \rightarrow K \mid f|_F = \text{Id}_F \}$$

$$= \{ f: K \rightarrow K \mid f(a) = a, \forall a \in F \} \leq \text{Aut}(K)$$

称为 F -自同构, 也称 K 在 F 上的伽罗瓦群.

设 $K|F$. $u \in F$.

若 $\text{Gal}(F(u)|F) = ?$

Case 1: $u|F$ 超越. $\text{Gal}(F(u)|F) = \frac{\text{GL}_2(F)}{\left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \mid a \in F^* \right\}}$
 $= \text{PGL}_2(F)$

Case 2: $u|F$ 代数. $f(x)$ 是 u 在 F 上的极小多项式.

$\text{Gal}(F(u)|F)$ 比较复杂.

但 我们知道 $|\text{Gal}(F(u)|F)| = f(x)$ 在 $F(u)$ 中互异根的个数

$$\leq [F(u):F]$$

证: $\sigma: F(u) \rightarrow F(u)$

$$u \mapsto u' = \sigma(u)$$

$$f(u) = 0.$$

~~$\sigma(u)$~~

$$\sigma(u^n + a_{n-1}u^{n-1} + \dots + a_1u + a_0) = \sigma(0) = 0$$

$$\Rightarrow \sigma(u)^n + a_{n-1} \sigma(u)^{n-1} + \dots + a_0 = 0$$

$\Rightarrow u'$ 也是 $f(x)$ 的根.

定义: 域扩张 $K|F$ 称为代数扩张. 如果

$\forall u \in K, u$ 在 F 上代数.

定理 1. 设 $K|F$ 是有根扩张, 则 $K|F$ 是代数扩张.

$\forall u \in F. 1, u, \dots, u^{n-1}, u^n$ 是 F -相关.

即不全为 0 的 $a_0, \dots, a_n \in F$

$$\text{使 } a_0 \cdot 1 + a_1 u + \dots + a_n u^n = 0$$

故 u 在 F 上代数.

2. 设 $K|F. u_1, \dots, u_n \in K$. 且每个 $u_i|F$ 均代数.

$$\text{则 } [F(u_1, \dots, u_n) : F] < \infty.$$

于是 $F(u_1, \dots, u_n)|F$ 是代数扩张, 由塔式公式
之得.

有限扩张必是代数扩张. 反之未必

特别地, 若 $u, v \in K$ 且均在 F 上代数. 则

$u \pm v, u \cdot v, \frac{u}{v} (v \neq 0)$ 均在 F 上代数.

3. $u|k$ 代数. $k|F$ 代数扩张. 则 $u|F$ 代数.

证: 设 $g(u)=0$. $g(x)=a_0+a_1x+\dots+a_{n-1}x^{n-1}+x^n$
 $\in k[x]$.

故 u 在 $F(a_0, \dots, a_{n-1})$ 上代数.

故 $[F(a_0, a_1, \dots, a_{n-1}, u) : F] < \infty$.

故 $F(a_0, \dots, a_{n-1}, u) | F$ 为代数扩张.

即 $u|F$ 代数.

4. 设有域扩张 $E|k$, $k|F$. 则 $E|F$ 代数扩张.

① ② $\Leftrightarrow E|k, k|F$ 均为代数扩张.

证: " $\Rightarrow$ " 设 $E|F$ 代数. 则 $E|k, k|F$ 代数. 显然.

" $\Leftarrow$ " $\forall u \in E$, $u|k$ 代数, $k|F$ 代数.

由定理 3. $u|F$ 代数.

§2. 分裂域

 $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_p$

$$\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}.$$

设 F 域, $f(x) \in F[x]$ $\deg f(x) \geq 1$

域扩张 E/F 称为 $f(x)$ 在 F 上的分裂域, 满足

• 如果 $f(x) = c(x-c_1)\cdots(x-c_n)$, $c_1, \dots, c_n \in E$
 $c \in F$.

• $E = F(c_1, \dots, c_n)$

例: $f(x) = x^3 - 2 \in \mathbb{Q}[x]$

$f(x)$ 在 $\mathbb{Q}$ 上的分裂域 $\mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2)$

$$= \mathbb{Q}(\sqrt[3]{2}, \omega) = \mathbb{Q}(\sqrt[3]{2}, \sqrt{3}i)$$

$$[\mathbb{Q}(\sqrt[3]{2}, \sqrt{3}i) : \mathbb{Q}] = 2 \times 3 = 6.$$

(望远镜公式)

定理: 设 F 域, $f(x) \in F[x]$, $\deg f(x) \geq 1$.

例 $f(x)$ 在 F 的分裂域是存在的

证: 对 $\deg f(x)$ 归纳.

(1) 任意域 F 上多项式在该域上的分裂域是存在的
假设 ———— $(n-1)$ 次 ————

设 $f(x) \in F[x]$. $\deg f(x) = n \geq 1$.

取 $f(x)$ 在 $F[x]$ 中的不可约因子 $g(x)$.

令 $K = \frac{F[x]}{\langle g(x) \rangle}$ 则 K 是域. $K \supseteq F$

令 $u = x + \langle g(x) \rangle \in K$

$$\begin{aligned} \text{则 } g(u) &= 0 \quad \text{因为 } g(x) = a_0 + a_1 x + \cdots + a_n x^n \\ &= (a_0 + a_1 u + \cdots + a_n u^n) - \langle g(x) \rangle \\ &= 0 \end{aligned}$$

$$f(x) = (x-u) \cdot h(x) \text{ in } K[x]$$

$$\deg h(x) = n-1.$$

$h(x)$ 在 K 上的分裂域存在. 设为 $E = K(u_1, \dots, u_{n-1})$

$$E = K(u_1, \dots, u_{n-1})$$

故 $F(u_1, \dots, u_{n-1}, u)$ 是 $f(x)$ 在 F 上的分裂域

同构延拓定理.

定理: 设 $\sigma: F \rightarrow F'$ 是同构, $f(x) \in F[x]$, $\deg f(x) \geq 1$
 设 E 和 E' 分别是 $f(x)$ 和 $f^\sigma(x)$ 在 $F(x)$ 和 F' 上的分裂域

则 σ 可以延拓成域同构 $\tau: E \xrightarrow{\sim} E'$ (即 $\tau|_F = \sigma$).
 $\sigma: F \xrightarrow{\sim} F'$

$$\sigma: F \xrightarrow{\sim} F'$$

这样的延拓的个数 m 满足:

$$\text{认为 } \sigma: F[x] \xrightarrow{\sim} F'[x]$$

$$1 \leq m \leq [E:F]$$

$$f(x) = a_0 + a_1x + \dots + a_nx^n$$

$$\mapsto f^\sigma(x) = \sigma(a_0) + \sigma(a_1)x + \dots + \sigma(a_n)x^n$$

并且 $m = [E:F]$ 当且仅当 $f(x)$ 是 F 上的可分多项式

设 $f(x) \in F[x]$, $f(x)$ 称为 F 上的可分多项式.
 如果 $f(x)$ 在 F 上的每个不可约因子都没有重根.

证明近世代数三问题

(or 1. 设 $f(x) \in F[x]$, $\deg f(x) \geq 1$. 则 $f(x)$ 在 F 上的分裂域是唯一的 (同构意义下)

证: 设 E 和 E' 均是 $f(x)$ 在 F 上的分裂域

$$\sigma = \text{id}: F \xrightarrow{\sim} F$$

(恒等)

$$f(x) \mapsto f(x)$$

$$\text{延拓成: } E \xrightarrow{\sim} E'$$

即证

$$\text{Gal}(K|F) = \{f: K \rightarrow K \mid f|_F = 1_K\}$$

Cor: 设 $f(x) \in F[x]$, $\deg f(x) \geq 1$. E 是 f ~~在 F 上~~ ^在 的分裂域. 则 $|\text{Gal}(E:F)| \leq [E:F]$.
等号成立当且仅当 $f(x)$ 在 F 上可分.

证: 这由同构延拓定理立得.

§3 有限域.

设 F 是有限域, 则 $\text{char } F = p$ (素数). $F \supseteq \mathbb{Z}_p$.

设 $[F:\mathbb{Z}_p] = n < \infty$, 设 $v_1, \dots, v_n$ 是 F 的一组 $\mathbb{Z}_p$ -基.

$$\begin{aligned} \text{则 } F &\cong \mathbb{Z}_p \cdot v_1 \oplus \mathbb{Z}_p \cdot v_2 \oplus \dots \oplus \mathbb{Z}_p \cdot v_n \\ &\cong \mathbb{Z}_p^n (\text{加法群}). \end{aligned}$$

定理(有限域的结构定理)

(1) 设 F 是有限域, 则 $\text{char } F = p$; 且 $|F| = p^n$, $n = [F:\mathbb{Z}_p]$
且有加群同构 $(F, +) \cong \mathbb{Z}_p^n$

(2) 设 F 是 p^n -元域. F_{p^n} , 则 $(F^*, \cdot)$ 是 $p^n - 1$ 阶循环群.
特别地, $F_{p^n} = \mathbb{Z}_p(n)$.

设 $p^n - 1 > 1$, $p^n - 1 = p_1^{r_1} \cdots p_m^{r_m}$ (素数分解).

$$x^{\frac{p^n-1}{p_i}} - 1 \in \mathbb{F}_{p^n}[x], \text{ 因 } \frac{p^n-1}{p_i} < p^n-1$$

故 $\mathbb{F}^*$ 中一定存在 u_i 不是 $f_i(x)$ 的根.

$$\text{令 } v_i = u_i^{(p^n-1)/p_i^{r_i}}$$

$$v_i^{p_i^{r_i}} = u_i^{p^n-1} = 1 \text{ 但 } v_i^{p_i^{r_i-1}} = u_i^{\frac{p^n-1}{p_i}} \neq 1$$

这说明 $o(v_i) = p_i^{r_i}$ 令 $v = v_1 \cdots v_m \in \mathbb{F}^*$

$$\text{故 } o(v) = p_1^{r_1} \cdots p_m^{r_m} = p^n - 1$$

(3) p^n 元域 $\mathbb{F}_{p^n}$ 是 $f(x) = x^{p^n} - x \in \mathbb{Z}_p[x]$ 的根集.

又

在 $\mathbb{Z}_p$ 上的分裂域

因此, 对于任一素数 p 和任一正整数 n , 存在唯一 p^n 元域

$$\text{证: } f(x) = x^{p^n} - x, \quad f'(x) = p^n x^{p^n-1} - 1 \quad (\text{形式上求导})$$

$$= -1$$

$$(f, f') = 1$$

$f(x)$ 无重根.

$f(x)$ 有 p^n 个不同根.

由此 $\forall a, b$ 是 $f(x)$ 的根. 则 $a-b, ab^{-1}$ 也是 $f(x)$ 的根.

$$(a-b)^{p^n} - (a-b) = a^{p^n} - b^{p^n} - (a-b) = 0.$$

$$p^n \text{ 奇则 } (a-b)^{p^n} = a^{p^n} - b^{p^n}$$

p^n 偶则 止的就是负的. $a-b = a+b$

$$|F| = p^n, a \in F^*. a^{p^n-1} = 1. \Rightarrow a^{p^n} = a.$$

域中任一元均是 $x^{p^n} - x$ 的根.

$$\mathbb{Z}_p \subseteq \{ \text{根} \}$$

$$(4) \text{Aut}(F_{p^n}) = \text{Gal}(F_{p^n}/\mathbb{Z}_p) = \langle \sigma \rangle \text{ 是 } n \text{ 阶循环群.}$$

$$\sigma: a \mapsto a^p, \forall a \in F_{p^n}.$$

为 F_{p^n} 的 Frobenius 自同构.

$$\text{证: } \text{Aut}(F_{p^n}) \supseteq \text{Gal}(F_{p^n}/\mathbb{Z}_p).$$

$$\forall f \in \text{Aut}(F_{p^n}), f(u) = 1, \text{ 故 } f(a) = a, \forall a \in \mathbb{Z}_p.$$

$$\Rightarrow f \in \text{Gal}(F_{p^n}/\mathbb{Z}_p)$$

$$\text{于是 } \text{Aut}(F_{p^n}) \subseteq \text{Gal}(F_{p^n}/\mathbb{Z}_p)$$

$$\sigma \in \text{Gal}(F_p^n | \mathbb{Z}_p).$$

$$F_p^n \rightarrow F_p^n$$

$$\sigma: a \mapsto a^p$$

$$\sigma \text{ 同态: } \sigma(ab) = \sigma(a)\sigma(b) \Leftrightarrow (ab)^p = a^p b^p$$

$$\sigma(a+b) = \sigma(a) + \sigma(b) \Leftrightarrow (a+b)^p = a^p + b^p$$

σ 单射. 只需 $\sigma(a) = 0$ 的像是 0 . 这由 F_p^n 无 0 因子律证
 σ 满射 不证自明, 因为 F_p^n 为有限域线性空间.

线性变换单射即满射

$$\sigma: a \mapsto a^p$$

$$\sigma^2: a \mapsto a^{p^2}$$

$$\sigma^n: a \mapsto a^{p^n} = a.$$

$$\sigma, \sigma^2, \dots, \sigma^n = \text{Id}$$

$$F \text{ 有 } p^n - 1 \text{ 个元 } u, u^{p^n-1} = 1.$$

$$\text{若 } \sigma^i = \sigma^j$$

$$\text{则 } a u^{p^i} = u^{p^j}$$

$$\Rightarrow u^{p^i - p^j} = 1$$

与 u 的取法矛盾!

$$|\text{Gal}(F_p^n | \mathbb{Z}_p)| \leq [F_p^n : \mathbb{Z}_p] = n.$$

但 $\alpha, \alpha^2, \dots, \alpha^n$ 已找到.

$$\text{故 } |\text{Gal}(F_{p^n} | \mathbb{Z}_p)| = n$$

(5) 给定正整数 n . 当 d 取遍 n 的正因子时.

F_{p^d} 就是 F_{p^n} 的 ~~全部~~ 所有子域

设 $d|n$ F_{p^d} 是 F_{p^n} 的唯一的子域 (集合意义下, 绝对意义下)

命题 $(p^d - 1) | (p^n - 1) \Leftrightarrow d | n$ (整数) 易证

证: 设 $d|n$. $F_{p^d} = x^{p^d} - x$ 的根集.

$$= x(x^{p^d-1} - 1)$$

$F_{p^n} \quad x^{p^n} - x = x(x^{p^n-1} - 1)$ 的根集.

反之. K 是 F_{p^n} 的一个子域. $|K| = p^d$.

则 $p^d - 1 | p^n - 1 \Rightarrow d | n$

$$\{0, 1, u, \dots, u^{p^n-2}\} \quad (\text{注意 } u^{p^n-1} = 1)$$

$\cong \mathbb{F}_{p^n}$ 加法怎么办?

找首1的n次不可约多项式

$f(x) \in \mathbb{Z}_p[x]$. 设 u 是 $f(x)$ 的一个根.

$$[\mathbb{Z}_p(u) : \mathbb{Z}_p] = n.$$

$$|\mathbb{Z}_p(u)| = p^n.$$

$$\mathbb{Z}_p(u) = \{a_0 + a_1 u + \dots + a_{n-1} u^{n-1} \mid a_i \in \mathbb{Z}_p\}$$

例: 9元域 ($9=3^2$)

$$\begin{array}{l} \cancel{x^2+1} \\ x^2+x+2 \\ x^2+2x+2 \end{array} \in \mathbb{Z}_3[x]$$

设 u 是 $f(x) = x^2+x+2 \in \mathbb{Z}_3[x]$ 的一个根.

则 $f(x)$ 是 u 在 $\mathbb{Z}_3$ 上的极小多项式

$$[\mathbb{Z}_3(u) : \mathbb{Z}_3] = 2.$$

$\therefore |\mathbb{Z}_3(u)| = 3^2$. 即 $\mathbb{Z}_3(u)$ 是9元域

$$\mathbb{Z}_3(u) = \{0, 1, 2, u, u+1, u+2, 2u, 2u+1, 2u+2\}$$

造 p^n 元域. ~~选择~~ 在 $\mathbb{Z}_p$ 上选一个 (首1) 不可约多项式 $f(x)$ 令 u 是 $f(x)$ 的一个根. 则 $\mathbb{Z}_p(u) = \{a_0 + a_1 u + \dots + a_{n-1} u^{n-1} \mid a_i \in \mathbb{Z}_p\}$.

$\mathbb{Z}_p(u)$ 是 p^n 元域. 加法: 按系数相加. 乘法: 按多项式乘法. 用 $f(u) = 0$ 进位.

(首1) n 次不可约多项式 $g(x) \in \mathbb{Z}_p[x]$. $g(u) = 0$.

$$|\mathbb{Z}_p(u)| = p^n. \quad \sigma: \mathbb{Z}_p(u) \xrightarrow{\sim} \mathbb{Z}_p(v)$$

故有 $\sigma(u) = v \Leftrightarrow u, v$ 是同一不可约多项式的根.

构造 27 元域. $27 = 3^3$.

$$f(x) = x^3 + ax^2 + bx + c$$

$f(x) = x^3 + 2x + 1$ ~~不可约~~ 在 $\mathbb{Z}_3[x]$ 上不可约. ($p=3$)

$$\text{令 } f(u) = 0. \quad \mathbb{Z}_3(u) = \{a_0 + a_1 u + a_2 u^2 \mid a_0, a_1, a_2 \in \mathbb{Z}_3\}$$

$$u^3 = -2u - 1 = u + 2. \quad u^5 = 2u^2 + u + 2, \quad u^8 = 2u^2 + 2.$$

$$u^{13} \neq 1$$

$$\text{取 } g(x) = x^3 + 2x + 2 \in \mathbb{Z}_3[x] \quad g(u) = 0.$$

$$\mathbb{Z}_3(u) = \{a_0 + a_1 v + a_2 v^2 \mid a_1, a_2, a_3 \in \mathbb{Z}_3\} \text{ 是 } 27 \text{ 元域}$$

$$v^3 = v + 1, \quad v^5 = v^2 + v + 1, \quad v^8 = 2v^2 + 2$$

$$v^{13} = 1 \quad (\text{注意到 } v \text{ 是 } 13 \text{ 阶, 非 } 26 \text{ 阶元})$$

~~故~~ 故不存在 σ . 且 $\sigma(u) = v$.

$$\sigma: \mathbb{Z}_3(u) \rightarrow \mathbb{Z}_3(v)$$

$$u \rightarrow 2v+1$$

$$f(2v+1) = (2v+1)^3 + 2(2v+1) + 1$$

$$= 8v^3 + 1 + 4v$$

$$= v^3 + 4v + 1$$

$$= 2(v^3 + 2v + 1) = 0$$

$$\text{例} \quad |GL_m(\mathbb{F}_q)| = ? \quad q = p^n$$

解: $M \in GL_m(\mathbb{F}_q) \Leftrightarrow M$ 的 m 行 $\alpha_1, \dots, \alpha_m$ 是 $\mathbb{F}_q$ -线性无关

$$\Rightarrow \alpha_1 \neq 0, \alpha_2 \neq k_1 \alpha_1, \alpha_3 \neq k_1 \alpha_1 + k_2 \alpha_2, \dots,$$

$$\alpha_n \neq k_1 \alpha_1 + \dots + k_{n-1} \alpha_{n-1}, \quad \alpha_i \in \mathbb{F}_q.$$

$$\begin{aligned} \Rightarrow |GL_m(\mathbb{F}_q)| &= (q^m - 1)(q^m - q) \cdots (q^m - q^{m-1}) \\ &= (p^{nm} - 1)(p^{nm} - p^n)(p^{nm} - p^{n(m-1)}) \end{aligned}$$

例: 代数闭域不能是有限域.

(下证代数闭域. 若 $F[x]$ 中任意次数多项式 $f(x)$ 均有一个根在 F 中.)

(反证).

证: 设 F_q 是代数闭域

$$x^{q^m} - x \in F_q[x] \text{ 的根在 } F_q \text{ 中.}$$

$$x^{q^m} - x \text{ 的根集为 } F_{q^m} \subseteq F_q. \text{ 导出矛盾!}$$

§4. 可分扩张.

代数扩张 K/F 称为可分扩张. 如果 K 中的任一元素在 F 上的极小多项式均无重根.

引理: 设 $f(x)$ 是 F 上的不可约多项式, 则 $f(x)$ 无重根.

(1) 若 $\text{char } F = 0$. 则 $f(x)$ 必无重根.

(2) 若 $\text{char } F = p$. 则 $f(x)$ 有重根 $\Leftrightarrow f(x) = g(x^p)$.

$$\text{证: } f(x) \text{ 有重根} \Leftrightarrow (f(x), f'(x)) \neq 1 \xLeftrightarrow^{f \text{ 不可约}} (f(x), f'(x)) = f(x)$$

$$\Leftrightarrow f'(x) = 0$$

$$(1) \text{ 若 } \text{char } F = 0. \quad f(x) \neq 0 \Rightarrow f'(x) \neq 0$$

$$\left(\begin{array}{l} \text{因为 } a_n x^n + \dots \neq 0, \\ (a_n \neq 0) \end{array} \Rightarrow n a_n x^{n-1} + \dots \neq 0 \right.$$

$$\left. \begin{array}{l} \text{因为 } n a_n \neq 0. \end{array} \right) \cdot \text{Boshi}$$

$$12) \text{char } F = p. f'(x) = 0 \Leftrightarrow f(x) = g(x^p)$$

$$f(x) = a_n x^n + \dots + a_i x^i + \dots$$

$$f'(x) = n a_n x^{n-1} + \dots + i a_i x^{i-1} + \dots$$

因为 $\text{char } F = p$. 故若 $p \mid i$. 必有 $a_i = 0$.

~~即~~ 即 $f(x)$ 只有 x^p 的项
 $\Rightarrow f(x) = g(x^p)$.

Cor: $\text{char} = 0$ 的域任一代数扩张是可分扩张.

~~(1) 若~~

例: 设 $\text{char } F = p$, $f(x) = x^p - a \in F[x]$ 设 $b^p = a$.

(1) 若 $b \in F$. 则 $f(x) = x^p - b^p = (x-b)^p \in F[x]$.

(2) 若 $b \notin F$. 则 ~~$f(x) = x^p - b^p$~~
 $f(x)$ 是 F 上的不可约多项式.

$$(x-b)^p = f(x) = g(x)h(x) \in F[x]$$

$$g(x) = (x-b)^m, 1 \leq m \leq p-1$$

但 $(x-b)^m$ 的 $(m-1)$ 次项系数为 $-mb \in F$.

但 $b \notin F$ 矛盾!

Cor: t 是不可分元; $f(x) = x^p - t \in \mathbb{Z}_p(t)[x]$.

令 K 是 $f(x)$ 在 $\mathbb{Z}_p(t)$ 上的分裂域.

例 ~~$K/\mathbb{Z}_p(t)$ 是不可分扩张~~

例 $K/\mathbb{Z}_p(t)$ 是不可分扩张.

$t^{1/p}$ 是不可分元 (因为 $t^{1/p}$ 在 $\mathbb{Z}_p(t)$ 上的极小多项式为 $f(x)$ 但 $t^{1/p} \notin \mathbb{Z}_p(t)$)

域 F 称为完备域 (perfect), 如果 F 的任一个代数扩张都是可分扩张.

事实: 特征 0 的域是完备的.

引理: 特征 p 的域 F 是完备的 $\Leftrightarrow F = F^p = \{a^p \mid a \in F\}$
(注意 $F^p \subseteq F$)

证: 设 F 完备. 则 $F = F^p$ (否则 $\exists \alpha \in F, \alpha \notin F^p$. 则 $x^p - \alpha \in F[x]$

为不可约多项式 ($x^p - \alpha$ 有 p 重根))

设 $F = F^p$ 只要证 $F[x]$ 中任一不可约多项式 $f(x)$ 均无重根

否则 $f(x) = g(x^p)$

NO. 106

$$= a_0 + a_1 X^p + \sqrt{a_2 X^{2p} + \dots + a_m X^{mp}}$$

$$= b_0^p + b_1^p X^p + b_2^p X^{2p} + \dots + b_m^p X^{mp}$$

$$= (b_0 + b_1 X + \dots + b_m X^m)^p \quad \text{与 } f(x) \text{ 不可约矛盾!}$$

Cor: 有限域是完备域. (Frobenius 自同构 $\Rightarrow F^p = F$)

定理: 设 $K|F$ 代数扩张. $\alpha_1, \dots, \alpha_n \in K$.

则 $F(\alpha_1, \dots, \alpha_n) | F$ 是可分扩张

$\Rightarrow \alpha_1, \dots, \alpha_n$ 是 F 上的可分元

定理: 有限可分扩张是单扩张

证: 设 $E|F$ 是有限可分扩张, 则 $E = F(\alpha_1, \dots, \alpha_m)$.

其中 α_i 都是 F 上的代数元.

只要证 $E = F(\alpha, \beta)$ 是 F 的单扩张

下设 F 是无限域

取 $r = \alpha + c\beta$ (线性式) $c \in F$

令 $f(x)$ 是 α 在 F 上的极小多项式, 全部根为 $\alpha_1, \dots, \alpha_n$ ($\alpha_i = \alpha$)

$g(x)$ 是 β 在 F 上的极小多项式, 全部根为 $\beta_1, \dots, \beta_m$ ($\beta_i = \beta$)

$$\text{令 } h(x) \triangleq f(r - cx) \in F(r)[x]$$

注意到 $h(\beta) = f(r - c\beta) = f(\alpha) = 0$

即 β 是 $h(x)$ 与 $g(x)$ 的一个公共根.

只要证: $h(x)$ 与 $g(x)$ 的公共根只有 β .

(why? 设 $h(x)$ 与 $g(x)$ 仅有一个公共根, 则 $(h(x), g(x)) = x - \beta$.

$(h(x), g(x)) \in F[x] \subseteq F(r)[x] \Rightarrow \beta \in F(r)[x]$
(辗转相除) $\alpha \in F(r)[x]$

只要证 $c \in F$ s.t. $\beta_1, \dots, \beta_m$ 均不是 $h(x)$ 的根即可 $\alpha = r - c\beta$

即 $f(r - c\beta_j) \neq 0, j = 2, \dots, m.$

即 $r - c\beta_j \neq \alpha_1, \dots, \alpha_n.$

即 $\alpha + c\beta - c\beta_j \neq \alpha_i, i = 1, \dots, n.$

即 $c = \frac{\alpha_i - \alpha}{\beta - \beta_j}, i = 1, \dots, n, j = 2, \dots, m$

总能取到 (因为 F 无限)

§5. 正规扩域.

定义. 代数扩域 $E|F$ 称为正规的, 如果:

若 $F[x]$ 中有一个不可约多项式 $p(x)$ 的一个根在 E 中,
则 $p(x)$ 的全部根均在 E 中. (不能同时脚踏两只船)

例 $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ 不是正规的

因为 $x^3 - 2 \in \mathbb{Q}[x]$ 不可约

有一个根 $\sqrt[3]{2} \in \mathbb{Q}(\sqrt[3]{2})$, 其余两根 $\sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2 \notin \mathbb{Q}(\sqrt[3]{2})$

定理. 设 E/F 是有限扩域. 则 E/F 是正规扩域

$\Leftrightarrow E$ 是 F 上某个多项式的分裂域

证: " $\Rightarrow$ " 设 E/F 是正规的. $E = F(\alpha_1, \dots, \alpha_m)$

令 $f_i(x)$ 是 α_i 在 F 上的极小多项式

E 是 $f(x) = f_1(x) \cdots f_m(x)$ 在 F 上的 ~~根域~~
 分裂域

" $\Leftarrow$ " 设 E 是 $f(x) \in F[x]$ 在 F 上的分裂域

要证 E/F 是正规的

设有 $F[x]$ 中不可约多项式 $p(x)$ 有一个根 α 在 E 中

要证 $p(x)$ 的任一根 β 也在 E 中

α, β 在 F 上的极小多项式为 ~~$p(x)$~~ $p(x)$

则 $\sigma: F(\alpha) \xrightarrow{\sim} F(\beta)$ $\sigma|_F = 1_d$

$\alpha \mapsto \beta$

$p(x) \mapsto p(x)$

$E(\alpha)$ 是 $p(x)$ 在 $F(\alpha)$ 上的分裂域

$E(\beta)$ 是 $p(x)$ 在 $F(\beta)$ 上的分裂域

则由同构扩张定理知有域同构 $E(\alpha) \cong E(\beta)$
 $\uparrow$
 E

即 $\beta \in E$

定义: 代数扩张 $E|F$ 称为有限 Galois 扩张, 若

(1) $E|F$ 是有限扩张

(2) $E|F$ 是可分扩张

(3) $E|F$ 是正规扩张

定理: 设 $E|F$ 是代数扩张, 则 $E|F$ 是有限 Galois 扩张

当且仅当 E 是 $F[x]$ 某个多项式的分裂域

可分

证: " $\Leftarrow$ " 留给读者

" $\Rightarrow$ " 留给读者

(由上页定理和上上页定理可推出)

我们以后常用

$$|\text{Gal}(E|F)| = [E:F] \quad \text{若 } E|F \text{ 是有限 Galois 扩张}$$

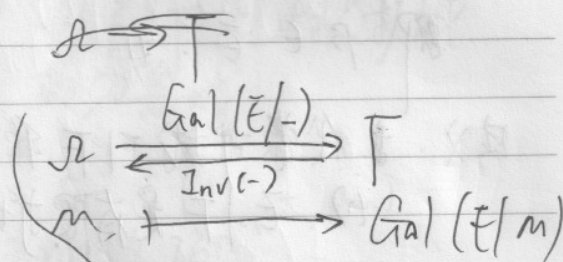
Chap. 4. Galois 理论

§1. Galois 对应.

E/F 是有限 Galois 扩张 $G = \text{Gal}(E/F)$.

令 $\mathcal{L} = \{E/F \text{ 的中间域 } m\}$

$\Gamma = \{G \text{ 的子群 } H\}$



$$\begin{array}{ccc}
 \text{Inv}(H) & & \\
 \parallel & & \text{Inv}(H) \leftarrow H
 \end{array}$$

$$\{x \in E \mid h(x) = x, \forall h \in H\}$$

$$h: E \rightarrow E$$

$$h|_F = \text{Id}.$$

设 $E|F$ 是扩域, $G = \text{Gal}(E|F)$

令 $\Omega = \{E|F \text{ 的中间域}\}$

$\Gamma = \{G \text{ 的子群 } H\}$

$$\Omega \xrightarrow{\text{Gal}(E/-)} \Gamma$$

$$\xleftarrow{\text{Inv}(-)}$$

$$M \longmapsto \text{Gal}(E|M) \leq G = \text{Gal}(E|F)$$

$$\text{Inv}(H) \longleftarrow H$$

$$= \{x \in E \mid h(x) = x, \forall h \in H\}$$

引理: 设 $E|F$ 是扩域, $G = \text{Gal}(E|F)$

$\Omega = \{E|F \text{ 的中间域}\}$ $\Gamma = \{G \text{ 的子群 } H\}$

$$\text{Gal}(E/-) : \Omega \rightarrow \Gamma$$

$$M \mapsto \text{Gal}(E|M)$$

$$\text{Inv} : \Gamma \rightarrow \Omega$$

$$H \mapsto \text{Inv}(H) = \{x \in E \mid h(x) = x, \forall h \in H\}$$

例 (1) $\text{Gal}(E/-) : \Omega \rightarrow \Gamma$ 是反序对应.

$\text{Inv} : \Gamma \rightarrow \Omega$ 是反序对应.

证: $M_1 \subseteq M_2 \Rightarrow \text{Gal}(E/M_1) \supseteq \text{Gal}(E/M_2)$

$H_1 \subseteq H_2 \Rightarrow \text{Inv}(H_1) \supseteq \text{Inv}(H_2)$

(2) $\text{Inv}(\text{Gal}(E/M)) \supseteq M \quad \forall M \in \Omega$

$\text{Gal}(E/\text{Inv}(H)) \supseteq H \quad \forall H \in \Gamma$ (两次不小)

(3) $\text{Gal}(E/\text{Inv}(\text{Gal}(E/M))) = \text{Gal}(E/M) \quad \forall M \in \Omega$ (~~三次不小~~)

$\text{Inv}(\text{Gal}(E/\text{Inv}(H))) = \text{Inv}(H) \quad \forall H \in \Gamma$ (三次不小)

" $\xrightarrow{\text{Inv}}$ " = " $\rightarrow$ "

证 (3): 令 $H = \text{Gal}(E/M)$

$H \subseteq \text{Gal}(E/\text{Inv}(H))$

由 (2) $\text{Inv}(\text{Gal}(E/M)) \supseteq M$

再由 (1) $\text{Gal}(E/\text{Inv}(\text{Gal}(E/M))) \supseteq \text{Gal}(E/M)$

即证 $\text{Gal}(E/\text{Inv}(\text{Gal}(E/M))) = \text{Gal}(E/M)$

同理可得 $\text{Inv}(\text{Gal}(\bar{E} | \text{Inv}(H))) = \text{Inv}(H)$.

中3-404 周五十点

§2. Galois理论基本定理.

Galois理论基本定理 (Galois大定理):

设 E/F 是有限 Galois 扩张. 令 $G = \text{Gal}(E/F)$

$\Omega = \{E/F \text{ 中间域 } M\}$ $\Gamma = \{G \text{ 的子群 } H\}$

令 $\text{Gal}(E/-): \Omega \rightarrow \Gamma$
 $M \mapsto \text{Gal}(E/M)$

令 $\text{Inv}: \Gamma \rightarrow \Omega$

~~令 Inv~~ : $H \mapsto \text{Inv}(H)$

$= \{x \in E \mid h(x) = x, \forall h \in H\}$

则 (1) $\text{Gal}(E/-)$ 和 Inv 是反序的互逆映射.

故 $\text{Inv}(\text{Gal}(E/M)) = M, \forall M \in \Omega$

$\text{Gal}(E | \text{Inv}(H)) = H, \forall H \in \Gamma$

特别地 $[E: \text{Inv}(H)] = |H|$

E/M 也是有限 Galois 扩张.

$$\text{又 } [E:F] = |G| = |\text{Gal}(E/F)|$$

$$\text{故 } [\text{Inv}(H), F] = [G, H]$$

设 E/F 是有限 Galois 扩张 $\Rightarrow |\text{Gal}(E/F)| = [E:F]$

$\Downarrow$

E 是 F 上某个 ^{可分} 多项式 $f(x)$ 的分裂域

(2) G 的两个子群 H 与 H' 共轭

$\Leftrightarrow \text{Inv}(H)$ 和 $\text{Inv}(H')$ 共轭

定义: m 与 m' 共轭 $\Leftrightarrow \exists \sigma \in \text{Gal}(E/F)$ s.t. $m' = \sigma(m)$

特别地: $H \triangleleft G \Leftrightarrow \text{Inv}(H)/F$ 正规

此时: $G/H \cong \text{Gal}(\text{Inv}(H)/F)$

$\parallel$

$$\frac{|\text{Gal}(E/F)|}{|\text{Gal}(E/\text{Inv}(H))|}$$

Artin 引理. 设 Q 是域 K 的自同构群的一个有限子群.

$$[K: \text{Inv}(Q)] \leq |Q|.$$

$$\text{其中 } \text{Inv}(Q) = \{x \in K \mid f(x) = x, \forall f \in Q\}.$$

$F) = (E:F)$

证: 设 $|Q| = n$. 要证 K 中任意 $(n+1)$ 个元 $u_1, \dots, u_{n+1}$.

必是 $\text{Inv}(Q)$ -相关的:

$$\text{令 } Q = \{f_1, \dots, f_n\}.$$

1_d .

考虑

$$(*) \begin{cases} u_1 x_1 + \dots + u_{n+1} x_{n+1} = 0 & (1) \\ f_2(u_1) x_1 + \dots + f_2(u_{n+1}) x_{n+1} = 0 \\ \vdots \\ f_n(u_1) x_1 + \dots + f_n(u_{n+1}) x_{n+1} = 0 \end{cases} \quad \text{系数 } \in K$$

必有非零解. 设 $(a_1, \dots, a_{n+1})$ 是其非零分量个数最小的一个非零解.

不妨设 $a_1 = 1$.

~~于是~~ $a_1, \dots, a_{n+1} \in \text{Inv}(Q)$ 则可由 (1) 式推出 Artin 引理.
只要证.

(反证) 假设 $\exists a_i \notin \text{Inv}(Q)$ 不妨设 $a_2 \notin \text{Inv}(Q)$

$(1 \leq t \leq n)$

故 $\exists f_t \in Q$. 使 $a_t \neq f_t(a_t)$

将 f_t 作用在 (*) 上: $\sum_{j=1}^{n+1} f_t(v_j) x_j = 0, i=1, \dots, n$

即有 $\sum_{j=1}^{n+1} f_t f_i(v_j) \cdot f_i(a_j) = 0$ (注意到 a_i 是 f_i)
(**)

又 $\{f_t f_i | i=1, \dots, n\} = \alpha$.

即 (**) 是 (*) 的一个重排.

故 $f_t(a_j)$ ~~也是~~

$= \{1, f_t(a_2), \dots, f_t(a_{n+1})\}$ 也是 (*) 的一个解.

注意 $\{0, a_2, \dots, a_{n+1}\}$ 也是 (*) 的解

故 $\{0, f_t(a_2) - a_2, \dots, f_t(a_{n+1}) - a_{n+1}\}$
也是 (*) 的解.

这与 $(a_1, \dots, a_{n+1})$ 的取法相矛盾 (非0分量最小) #

引理2. 设 M 是有限正规扩张 E/F 则 M/F 正规

$$\Leftrightarrow \sigma(M) = M, \forall \sigma \in \text{Gal}(E/F)$$

证: $\Rightarrow$ 设 M/F 正规, 则 M 是 F 的某个多项式 $f(x)$ 在 F 上的分裂域, $M = F(\alpha_1, \dots, \alpha_m)$.

其中 $\alpha_1, \dots, \alpha_m$ 是 $f(x)$ 的互异根.

$$\begin{aligned} \sigma(M) &= (\sigma F)(\sigma(\alpha_1), \sigma(\alpha_2), \dots, \sigma(\alpha_m)) \\ &= F(\sigma(\alpha_1), \dots, \sigma(\alpha_m)) \\ &= F(\alpha_1, \dots, \alpha_m) = M \end{aligned}$$

$$\begin{aligned} &\text{但 } \{\sigma(\alpha_1), \dots, \sigma(\alpha_m)\} \\ &= \{\alpha_1, \dots, \alpha_m\}. \end{aligned}$$

$$(\text{因 } 0 = f(\alpha_i))$$

$$\Rightarrow \underset{0}{\sigma(0)} = f(\sigma(\alpha_i))$$

$$\Leftarrow \text{设 } \sigma(M) = M, \forall \sigma \in \text{Gal}(E/F)$$

设 $p(x)$ 是 $M[x]$ 中不可约多项式

$\alpha \in M$ 是 $p(x)$ 的一根. 求证 $p(x)$ 的任一根 $\beta \in M$.

因为 E/F 有限正规

设 F 中多项式 $f(x)$ 在 F 上的分裂域

$$\begin{aligned} \sigma: F(\alpha) &\xrightarrow{\sim} F(\beta) \\ \sigma|_F = \text{id}, \alpha &\mapsto \beta = \sigma(\alpha) \end{aligned}$$

$$\begin{aligned} \tau: E(\alpha) &\xrightarrow{\sim} E(\beta) \\ \tau|_{F(\alpha)} &= \sigma \end{aligned}$$

$E(\alpha)$ 是 $F(\alpha)$ 中多项式 $f(x)$ 在 $F(\alpha)$ 上的分裂域

$E(\beta)$ 是 $F(\beta)$ 中多项式 $f(\beta)$ 在 $F(\beta)$ 上的分裂域

$$\beta = \sigma(\alpha) = \tau(\alpha) \in \tau(M) = M \quad \#$$

$$\tau: \tau \rightarrow E(\beta) = E, \tau \in \text{Gal}(E/F) \quad \circ$$

Galois

基本定理的证明:

$$(1) \quad M \subseteq \text{Inv}(\text{Gal}(E/M))$$

因为 E/M , $E/\text{Inv}(\text{Gal}(E/M))$ 是有 Galois 扩张

$$[E: \text{Inv}(\text{Gal}(E|M))] = |\text{Gal}(E | \text{Inv}(\text{Gal}(E|M)))|$$

" $\equiv$ " " $\sim$ "

$$|\text{Gal}(E|M)| = [E:M]$$

$$\text{故 } \cancel{M} \text{ 在 } [M: \text{Inv}(\text{Gal}(E|M))] = 1 \quad (\text{调运境公式})$$

$$\text{即 } M = \text{Inv}(\text{Gal}(E|M))$$

$$H \subseteq \text{Gal}(E | \text{Inv}(H))$$

$$|H| \leq |\text{Gal}(E | \text{Inv}(H))| = [E: \text{Inv}(H)] \stackrel{\text{Artin}}{\leq} |H|$$

上式必须全取等号.

$$\text{即有 } \text{Gal}(E | \text{Inv}(H)) = H. \quad \#$$

$$(v) \text{Inv}(\sigma H \sigma^{-1}) = \{x \in E \mid \sigma h \sigma^{-1}(x) = x, \forall h \in H\}$$

$$= \{x \in E \mid h \sigma^{-1}(x) = \sigma^{-1}(x), \forall h \in H\}$$

$$= \{x \in E \mid \sigma^{-1}(x) \in \text{Inv}(H)\}$$

$$= \sigma(\text{Inv}(H)) \quad \text{即证.} \quad \#$$

$$(3) \quad \cancel{\sigma(H)} \quad H \trianglelefteq G, \quad \sigma(\text{Inv}(H)) = \text{Inv}(H)$$

由引理 2: $\text{Inv}(H)/F$ 正规

设 $H \trianglelefteq G$, $\text{Inv}(H)/F$ 是正规子域 $\therefore \sigma(\text{Inv}(H)) = \text{Inv}(H)$

$$\pi: \begin{array}{ccc} G & \xrightarrow{\quad} & \text{Gal}(\text{Inv}(H)/F) \\ \downarrow & & \downarrow \\ G & \xrightarrow{\quad} & \sigma|_{\text{Inv}(H)} \end{array}$$

$$\ker \pi: \left\{ \sigma \in G \mid \sigma|_{\text{Inv}(H)} = 1_{\text{Inv}(H)} \right\}$$

$$= \text{Gal}(E/\text{Inv}(H)) = H \trianglelefteq G.$$

$$\text{于是 } G/H \hookrightarrow \text{Gal}(\text{Inv}(H)/F)$$

$$\cancel{|\text{Gal}(\text{Inv}(H)/F)|}$$

$$|\text{Gal}(\text{Inv}(H)/F)| = [\text{Inv}(H):F]$$

$$= \frac{[E:F]}{[E:\text{Inv}(H)]} = \frac{|\text{Gal}(E/F)|}{|\text{Gal}(E/\text{Inv}(H))|}$$

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

$$\text{故 } G/H \cong \text{Gal}(Z(H)/F) \quad \#$$

$Z(H)$
 $\in G$
 (F)

$$\begin{array}{ccc} E & \xrightarrow{\text{Gal}(E/-)} & \{1\} \\ \uparrow & & \downarrow \\ M & \xrightarrow{\text{Gal}(E/-)} & \text{Gal}(E/M) \\ \uparrow & & \downarrow \\ F & \xrightarrow{\text{Gal}(E/-)} & G = \text{Gal}(E/F) \end{array}$$

§3 Galois 群的计算

设 F 是域, $f(x) \in F[x]$. 令 E 是 $f(x)$ 在 F 上的分裂域.

$E = F(r_1, \dots, r_n)$, 其中 $r_1, \dots, r_n$ 是 $f(x)$ 的全部根.

$$\text{则 } f(x) = (x-r_1)(x-r_2)\cdots(x-r_n).$$

将 $G = \text{Gal}(E/F)$ 称为多项式 $f(x)$ 或方程 $f(x)=0$

的 Galois 群. 记为 $\text{Gal}(f(x), F)$ 或 G_F .

S_n 是 $\{1, \dots, n\}$ 的对称群.

设 $G \subseteq S_n$, 称 G 是 S_n 的一个可迁子群. 或 G 是

$\Omega = \{1, 2, \dots, n\}$ 上的一个可迁置换, 如果对于任意 $i, j \in \Omega$ 均 $\exists \sigma \in G$, s.t. $\sigma(i) = j$

设 $t \in \Omega$ (固定) 则 G 是 S_n 的可迁子群 $\Leftrightarrow \forall j \in \Omega$ 均 $\exists \sigma \in G$, s.t. $\sigma(t) = j$. (证明显然)

例: $K_4 = \{(1), (12)(34), (13)(24), (14)(23)\}$ 是 S_4 的一个可迁子群.

$\{(1), (12), (34), (12)(34)\}$ 不是 S_4 的可迁置换群, 但却同构于 K_4 .

定理: 设 F 是域, $f(x) \in F[x]$ 是无重根多项式, $n = \deg f(x)$

则 (1) G_f 是 S_n 的子群; $|G_f| = [E:F]$

$$f(x) = c(x-r_1) \cdots (x-r_n)$$

$$E = F(r_1, \dots, r_n)$$

$$\forall \sigma \in G_f \quad G_f = \text{Gal}(E/F)$$

$$= \text{Gal}(F(r_1, \dots, r_n)/F).$$

$$\sigma: \text{环同构} E[x] \xrightarrow{\sim} E[x]$$

$$g(x) \mapsto \sigma(g_0) + \sigma(g_1)x + \dots + \sigma(g_n)x^n$$

$$= g_0 + g_1x + \dots + g_nx^n$$

$$f(x) = \sigma(f(x)) = c(x - \sigma(r_1)) \dots (x - \sigma(r_n))$$

(因 $f(x) \in F[x]$)

即 $\sigma(r_1), \dots, \sigma(r_n)$ 是 $f(x)$ 的 n 个根

即 $\sigma(r_1), \dots, \sigma(r_n)$ 是 $1, \dots, n$ 的一个置换.

$$\text{2) } G_f \hookrightarrow \pi \rightarrow S_n$$

$$\sigma \mapsto \begin{pmatrix} r_1 & \dots & r_n \\ \sigma(r_1) & \dots & \sigma(r_n) \end{pmatrix}$$

π 是群同态

$$(2) \sigma \in S_n \cdot (2) \sigma \in G_f \Leftrightarrow \sigma \text{ 保持 } f(x) \text{ 的根集}$$

$\{r_1, \dots, r_n\}$ 上的 ~~所有~~ 代数关系

证: 设有 $g(x) \in F[x_1, \dots, x_n]$ 使 $g(r_1, \dots, r_n) = 0$
(将 $r_1, \dots, r_n$ 代入 $g(x)$)

$$0 = \sigma(0) = \sigma(g(r_1, \dots, r_n))$$

$$= g(\sigma(r_1), \dots, \sigma(r_n)) \quad (\sigma g = g, \text{ 因 } g \text{ 的系数在 } F)$$

反之. 设 σ 保持 $f(x)$ 的根之间的所有代数关系

$$\text{令 } \sigma: E \rightarrow E.$$

$$F(r_1, \dots, r_n)$$

$$\forall a \in E. a = \psi(r_1, \dots, r_n), \psi(r_1, \dots, r_n)$$

$$\in F[x_1, \dots, x_n]$$

$$\text{令 } \sigma(a) = \psi(\sigma(r_1), \dots, \sigma(r_n))$$

这是 well-defined. $\sigma|_F = \text{Id}$

σ 是域同态

$$\sigma: E \rightarrow E.$$

$\ker \sigma \triangleleft E$. (域的理想只有 $\{0\}$ 和 E)

$$\ker \sigma \neq E.$$

$$\ker \sigma = \{0\}.$$

(3) $f(x)$ 在 F 不可约 $\Leftrightarrow G_f$ 是 E 的一个可迁置换群.

证: " $\Rightarrow$ " 设 $f(x)$ 不可约. 设 r_i, r_j 是 $f(x)$ 的任意两根
 r_i, r_j 在 F 上有相同的根 + 多项式 $f(x)$

$$\sigma: F(r_i) \xrightarrow{\sim} F(r_j)$$

$$\sigma|_F = \text{Id}, \sigma(r_i) = r_j$$

σ 可延拓成: $E \rightarrow E$. 故 $\sigma \in G_f$.

反之. 设 G_f 是 S_n 的一个可迁子群. 设 r_j 是 $f(x)$ 的一个根. 是 $f_1(x)$ 是 r_i 在 F 上的根 + 多项式.

$$0 = f_1(r_i) \Rightarrow 0 = \sigma(0)$$

$$\text{故 } \exists \sigma \in G_f \text{ s.t. } \sigma(r_i) = r_j$$

$$0 = f_1(r_i) \Rightarrow 0 = \sigma(0) = f_1(\sigma(r_i)) = f_1(r_j)$$

$$\Rightarrow f_1(r_j) = 0 \quad \text{即 } r_j \text{ 也是 } f_1(x) \text{ 的根.}$$

$$\text{故 } f_1(x) = f(x) \text{ (最多差一个首项系数)}$$

例 $E = \mathbb{Q}(\sqrt[4]{5}, i)$ 求 $G = \text{Gal}(E/\mathbb{Q})$

E 是 $X^4 - 5 \in \mathbb{Q}[X]$ 在 $\mathbb{Q}$ 上的分裂域

$$G = G_f \quad E = \mathbb{Q}(\sqrt[4]{5}, i)$$

$$\forall \sigma \in G_f \quad \sigma(\sqrt[4]{5}) = \begin{cases} \sqrt[4]{5} \\ -\sqrt[4]{5} \\ \sqrt[4]{5}i \\ -\sqrt[4]{5}i \end{cases}$$

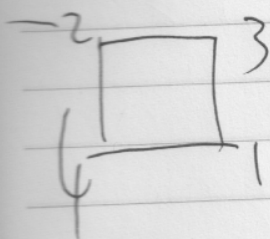
$$\sigma(i) = \begin{cases} i \\ -i \end{cases}$$

$$\begin{aligned} [E:\mathbb{Q}] &= [\mathbb{Q}(\sqrt[4]{5}i) : \mathbb{Q}(\sqrt[4]{5})] \cdot [\mathbb{Q}(\sqrt[4]{5}) : \mathbb{Q}] \\ &= 2 \cdot 4 = 8 \end{aligned}$$

$$|G| = 8 \quad G \leq S_4$$

	$r_1 = \sqrt[4]{5}$	$r_2 = -\sqrt[4]{5}$	$r_3 = \sqrt[4]{5}i$	$r_4 = -\sqrt[4]{5}i$	i	S_4
$G_1 = Id$	r_1	r_2	r_3	r_4	i	(1)
G_2	r_2	r_1	r_4	r_3	i	(12) (34)
G_3	r_3	r_4	r_2	r_1	i	(13) (24) (13 24)
G_4	r_4	r_3	r_1	r_2	i	(14 23)
G_5	r_1	r_2	r_4	r_3	$-i$	(34)
G_6	r_2	r_1	r_3	r_4	$-i$	(12)
G_7	r_3	r_4	r_1	r_2	$-i$	(13) (24)
G_8	r_4	r_3	r_2	r_1	$-i$	(14) (23)

$$G_f = D_4 \leq S_4 \quad (|D_4| = 8, |S_4| = 24)$$



定理: 设 $f(x) \in \mathbb{Q}[x]$ 是 p 次不可约多项式. p 素数.

设 $f(x)$ 仅有 2 个非实的复根 (其它根均为实数).

$$\text{则 } G_f = S_p.$$

$$\text{例: } f(x) = x^5 - 15x^2 + 9 \in \mathbb{Q}[x]$$

$$\text{求 } G_f = ?$$

$f(x) \in \mathbb{Q}[x]$ 不可约. (因 $f(x) \in \mathbb{Z}[x]$ 不可约)

$f(x)$ 有 3 个实根. 即 $f(x)$ 有 2 个非实的复根

$$\text{则 } G_f = S_5$$