

9.9

水课 .

代数整数环: $\mathcal{O}_K = \{\alpha \mid \alpha \text{是 } \mathbb{Q} \text{上的一个首-整系数多项式的根}\}$. \square

proposition: 以下命题等价: 设 $\alpha \in \mathbb{C}$

(i) α 是代数整数

(ii) $\mathbb{Z}[\alpha]$ 的加法群是有限生成的.

(iii) α 是 \mathbb{C} 中某个非零子环 R 中的元素且 R 的加法群是有限生成的.

(iv) 存在有限生成的非零加法群 $A \subset \mathbb{C}$ 使得 $\alpha A \subseteq A$.

Proof: (i) \Rightarrow (ii): 由定义, 存在 $f(x) = x^n + C_{n-1}x^{n-1} + \dots + C_1x + C_0 \in \mathbb{Z}[x]$

使得 $f(\alpha) = 0$. 则 $\mathbb{Z}[\alpha] = \mathbb{Z} \oplus \mathbb{Z}\alpha \oplus \dots \oplus \mathbb{Z}\alpha^{n-1}$ \square .

(ii) \Rightarrow (iii): 令 $R = \mathbb{Z}[\alpha]$

(iii) \Rightarrow (iv): 令 $A = R$.

(iv) \Rightarrow (i): 设加法群 A 由 a_1, \dots, a_n 生成, 则由 $\alpha A \subseteq A$

$$\text{知存在 } M_{n \times n} \text{ 使得 } \begin{pmatrix} \alpha a_1 \\ \vdots \\ \alpha a_n \end{pmatrix} = M \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}$$

从而 $(\alpha I - M) \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} = (0)$, α 是 n 次首-整系数多项式

$f(x) = \det(xI - M)$ 的根. 是代数整数

作业 (9.9)

1. (1) f 有左逆 $\Rightarrow g \circ f = \text{id}_X \Rightarrow \forall x_1 \neq x_2 \in X, g \circ f(x_1) \neq g \circ f(x_2)$
 $\Rightarrow f(x_1) \neq f(x_2) \Rightarrow f$ 单.

f 单, 由选择公理, 存在 $f^{-1}: f(X) \rightarrow X$, 则 $f^{-1} \circ f = \text{id}_X \quad \square$

(2) f 有右逆 $\Rightarrow f \circ g = \text{id}_Y \Rightarrow \forall y \in Y, \exists y' \text{ 使 } f(y') = y (y' = g(y))$.
 $\Rightarrow f$ 满

f 满, 由选择公理, $\forall y \in Y, \exists x \text{ 使 } f(x) = y, \text{ 令 } x = f^{-1}(y)$,

则 $f \circ f^{-1} = \text{id}_Y \quad \square$

(3) 由(1)(2) 显然

(4) $g \circ f \circ h = g \circ \text{id}_Y = g, g \circ f \circ h = \text{id}_X \circ h = h \Rightarrow g = h \quad \square$

(5) 设 g_1, g_2 为 f 的逆. 由(4) 知 $g_1 = g_2 \quad \square$

(6) 易知 f 是 f^{-1} 的逆. 由逆的唯一性知 $f = (f^{-1})^{-1} \quad \square$.

1. Lemma: 若 $x^2 = x$. 则 $x = e$.

pf: 由(3). 存在 y 使 $yx = e$. $x = ex = (yx) \cdot x$
 $= y \cdot x^2 = y \cdot x = e \quad \square$

设 $ba = e$, 则 $(ab)^2 = abab = a \cdot e \cdot b = ab \stackrel{\text{Lemma}}{\Rightarrow} ab = e$.

$\Rightarrow ae = aba = ea = a \Rightarrow e$ 为幺元. 又由于 $ba = e \Rightarrow ab = e$

故逆元存在. \square

2. 反例: $G = \{a, b, c, d, e\}$. 滿足任意 $x, y \in G$, $x * y = y$.

结合律: $(a * b) * c = b * c = c$, $a * (b * c) = a * c = c$.

左幺元: $e * x = x$, 右逆元: $a * e = e$

3. $\forall a \in G, \exists x$ 使 $ax = a$; $\forall b, \exists t: b = ta$, 则

$bx = tax = ta = b \Rightarrow \exists H \subseteq G, \forall x \in H, a \in G$ (H 是右
幺集,

$ax = a$ 同理存在 H' , $\forall y \in H', a \in G, ya = a$.

H' 是左
幺集)

且由 $ax = a$ 的 x 存在性 $\Rightarrow H \neq \emptyset$, 同理 $H' \neq \emptyset$

$\forall x \in H, y \in H', x = yx = y \Rightarrow H = H', \exists e \in H$.

则 $\forall x \in G, xe = ex = x$ 则 e 为单位元.

又 $xa = e$ 与 $ax = e$ 的解 x 存在, 故存在逆

综上得 G 为群

□

4. 由于 G 有限. 且消去律. 知 $aG = Ga = G$ for any $a \in G$.

故 $\forall b \in G$, $ax = b$ 有解 x , $ya = b$ 有解 y . 由 T₃ 得证. □.

9.12

WF2 代课.

置换群 $S_n: \{f: [n] \rightarrow [n], 双射\}$, 非交換 ($n \geq 3$)

称 n 元置换 α, τ 是不交的: α 变动的元在 τ 下不动

命题: 不交的置换可交换. 即: $\alpha\tau = \tau\alpha$

□

9.12 作业

P24 . T6.8.12.16.17.18.19.21.22

6. 反证 G 恰有 2 个非零元 $a \neq b$. 则 $a = a^{-1}$, $b = b^{-1}$

且 $(aba)^2 = abaaba = e$. 则 $aba = a \circ b$. 若 $aba = a \Rightarrow ab = e$

$\Rightarrow b = a^{-1} = a$. 矛盾! 故 $aba = b \Rightarrow ab = ba^{-1} = ba$

$\Rightarrow (ab)^2 = abab = abba = e$. 而 $ab \neq a, \neq b, \neq e$ 是非零元. 矛盾!

8. $(xy)^2 = x^2y^2 \Leftrightarrow xy \circ y \neq x \circ yy \Leftrightarrow xy \neq yx$.

取 $x = (13)$ $y = (12)$ $xy = (123)$ $yx = (132)$ 不同.

12. " \Rightarrow ": 若 $HK \leq G$. 若 HK 是子群, 则 $\forall kh \in KH$.

$kh = (h^{-1}k^{-1})^{-1} \in HK$, $\forall hk \in HK$, $e k^{-1} \cdot h^{-1} e \in HK$

即存在 $h_1 \in H$, $k_1 \in K$ 使 $k^{-1}h^{-1} = h_1k_1$. 即 $hk = k_1^{-1}h_1^{-1} \in KH$.

故 $HK \subseteq KH$ 且 $KH \subseteq HK \Rightarrow HK = KH$

□

" \Leftarrow ": 若 $HK = KH$. 则 $\forall h_1, h_2 \in H$, $k_1, k_2 \in K$, $h_1k_1(h_2k_2)^{-1}$

$= h_1k_1k_2^{-1}h_2^{-1} := h_1k_3h_2^{-1}$ 由 $HK = KH$ 知 $\exists h_4 \in H$

$k_4 \in K$ 使得 $k_3h_2^{-1} = h_4k_4 \Rightarrow h_1h_4k_4 \in HK \Rightarrow HK \leq G$. □

16. 考虑 $x \mapsto x^{-1}$ 不动元素 e . 至少还有一个. 否则

恰一个不动 \Rightarrow 阶奇数. 矛盾! 故 $a=a^{-1} \Rightarrow a^2=e$. ($a \neq e$)

17. $x \leftrightarrow x^{-1}$ $\text{ord}(x) = \text{ord}(x^{-1})$

□

18. 设 $r \in \mathbb{N}^*$ $\boxed{\text{R. } \overbrace{abab\dots ab}^{rt} = e}$

$$\text{若 } a(ba)^{r-1}b = e \Rightarrow (ba)^{r-1} = a^{-1}b^{-1} = (ba)^{-1}$$

$$\Rightarrow (ba)^r = e \quad \text{同理 } (ba)^r = e \Rightarrow (ab)^r = e.$$

故 $(ab)^r = e \Leftrightarrow (ba)^r = e$, 易得 $\text{ord}(ab) = \text{ord}(ba)$ □.

$$19. a^2 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \neq I_2, a \neq I_2$$

$$\text{且 } a^4 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I_2 \Rightarrow \text{ord}(a) = 4$$

$$b^2 = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix} = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}$$

$$b^3 = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I_2$$

$$\text{由于 } b \neq I_2 \Rightarrow \text{ord}(b) = 3.$$

□

21. 考虑 $\forall g \in G$, g 生成的群 G_g . 假设 $|G| = +\infty$

- 若存在 g 使 G_g 阶为无穷 $\Rightarrow G_g \cong \mathbb{Z}$, 显而有无穷多子群

从而 G 有无穷多子群

- 若 $\forall g \in G$, $|G_g| < \infty$, 归纳取 $g_i \in G \setminus \{g_1, \dots, g_{i-1}\}$

由于 $|G| = +\infty$ 知 g_i 存在，从而 $\{g_i\}$ 生成子群列

$\{G_{g_i}\}$ ，由于 G_{g_i} 均有限，故重复的群每类只有有限个。

知该子群列有无穷多个而不同子群。□。

22. 在 $H \times K$ 上定义等价关系 \sim : $(h_1, k_1) \sim (h_2, k_2) \Leftrightarrow h_1 k_1 = h_2 k_2$

下证每个等价类有 $|H \cap K|$ 个元素：考虑等价类 $\{h_1 k_1, h_2 k_2, \dots, h_t k_t\}$

一方面，取 $h_i^{-1} h_j = k_j k_i^{-1}$ 时， $h_i^{-1} h_j \in H \cap K \Rightarrow t \leq |H \cap K|$

另一方面对 $\forall h k$, 设 $H \cap K = \{a_1, \dots, a_n\}$ 取 (h_i, k_i) 使

$h_i^{-1} h = k_i k^{-1} = a_i \Rightarrow h_i k_i = h k$ 且两两不同，在等价类里

故每个等价类恰 $|H \cap K|$ 个元素 $\Rightarrow |H \cap K| |H K| = |H| |K|$ 。□。

(9.19) $P_{25}: T_{23, 24, 25, 29, 30, 39}$

$P_{35}: T_3, 8, 12, 13, 14, 15, 17$

T₂₃. 设 $H \leq G$, $G = H a H = H b H$ $\Rightarrow aH = Hb$

$\forall a \notin H \Rightarrow a \in Hb \Rightarrow Ha = Hb$ 由 $aH = Ha \Rightarrow H$ 正规. \square

T₂₄. 设 H_1, H_2 是唯二两个指数为 2 的子群, 则 $H_1 \leq H_1 H_2 \leq G$

由 $[G : H_1 H_2] \mid [G : H_1]$ 知 $H_1 H_2 = H_1$ 或 G . 若 $H_1 H_2 = H_1$, 由 $H_1 \triangleleft G$ 知

$H_2 \leq H_1 \Rightarrow \frac{G}{H_1} = \frac{G/H_2}{H_1/H_2} \cong \frac{G/H_1}{G/H_2} \cong \mathbb{Z}_2$

$\Rightarrow H_1 H_2 = \{e\} \Rightarrow H_1 = H_2$. 矛盾! 故 $H_1 H_2 = G$. 由 $H_1 \triangleleft G, H_2 \triangleleft G$

$H_1 H_2$ 知 $H_1 \cap H_2 \triangleleft G$. 且 $\frac{H_1 H_2}{H_1} \cong \frac{H_1 H_2 / H_1 \cap H_2}{H_1 / H_1 \cap H_2} \cong \mathbb{Z}_2$

$\Rightarrow \mathbb{Z}_2 \cong \frac{H_1 H_2 / H_1 \cap H_2}{\mathbb{Z}_2} \Rightarrow H_1 H_2 / H_1 \cap H_2$ 是 4 阶子群

\mathbb{Z}_4 或 $\mathbb{Z}_2 \times \mathbb{Z}_2$. 由于 $H_1 H_2 / H_1 \cap H_2$ 中的 2 阶子群 (非平凡子群)

与 $H_1 H_2$ 中包含 $H_1 \cap H_2$ 的非平凡子群一一对应, \mathbb{Z}_4 有 1 个非平凡子群, $\mathbb{Z}_2 \times \mathbb{Z}_2$ 有 3 个.

$\Rightarrow H_1 H_2 / H_1 \cap H_2 \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. 取其第三个二阶子群所对应的含 $H_1 \cap H_2$ 子群,

我们得到 H_3 . 满足 $[G : H_3] = 2$. 矛盾!

25. $D_{20} = \langle r, s \mid r^{10} = 1, s^2 = 1, srs = r^{-1} \rangle = \{sr^i, r^i \mid i=1, 2, \dots, 19\}$

设 H 是 D_{20} 的正规子群,

$$r^i \cdot sr^k \cdot r^{-i} = sr^{k-2i} \quad \text{--- ①} \quad r^i \cdot r^k \cdot r^{-i} = r^k \quad \text{--- ③}$$

$$sr^i \cdot sr^k \cdot r^{-i} \cdot s = sr^{2i-k} \quad \text{--- ②} \quad sr^i \cdot r^k \cdot r^{-i} \cdot s = r^{-k} \quad \text{--- ④}$$

因此 $H = \langle r^m \rangle$ 时，由③④知 H 是正规的。

$H = \langle r^m, s \rangle$ 时，①②要求 $m=1$ 或 2 ($\{r^{\frac{1}{2}}\}, \{r^{\frac{1}{3}}\}$ 同时出现)

故所有正规子群为 $\langle r^m \rangle$ ($m=1, 2, 5, 10$)， $\langle r^m, s \rangle$ ($m=1, 2$)。 \square

29. 记 $H = \langle a \rangle N$ ， $\langle a \rangle$ 是 a 生成的子群。由 G 有限 \Rightarrow

$$|G| = |N||G/N|. \text{ 由 } N \trianglelefteq G \Rightarrow H \leq G. \Rightarrow |H| \mid |G|$$

$$\text{而 } |H| \mid |\langle a \rangle| |N|, \text{ 且 } \langle a \rangle \mid |N| \Rightarrow |H| \mid |N|^2$$

$$\Rightarrow |H| \mid \gcd(|N|^2, |N||G/N|) = |N| \times |N| / |H|$$

$$\Rightarrow |N| = |H|. \text{ 由 } N \trianglelefteq H \text{ 且 } \langle a \rangle \subseteq N \Rightarrow a \in N$$

\square

30. 证： $aH \cap K = aH \cap ak$.

$$\text{一方面 } aH \cap K \subset aH, aH \cap K \subset ak$$

$$\Rightarrow aH \cap K \subset aH \cap ak$$

$$\text{另一方面 } \forall x \in aH \cap ak, \exists h \in H, k \in K, x = ah = ak$$

$$\Rightarrow h = k \in H \cap K \Rightarrow aH \cap ak \subset aH \cap K.$$

$$\text{综上 } aH \cap K = aH \cap ak$$

\square

39. 一方面 $\forall x \in AB \cap C$. $\exists a \in A, b \in B, c \in C$ 使 $x = ab = c = a(a^{-1}c)$

$$\text{则 } b \in B \text{ 且 } b = a^{-1}c \in C \Rightarrow b \in B \cap C \Rightarrow x = ab \in A(B \cap C)$$

$$\text{另一方面 } \forall x \in A(B \cap C), \exists a \in A, t \in B, t \in C \text{ 使 } x = at$$

$$\text{则 } at \in A \cap C. at \in AB \Rightarrow x = at \in AB \cap C$$

$$\text{综上 } AB \cap C = A(B \cap C)$$

\square

3. . 0元: R 中的 0 元 1: $a \oplus 1 = a + 1 - 1 = a$ 加法幺元

• $(a \oplus b) \oplus c = (a+b-1) \oplus c = a+b+c-2 = a \oplus (b+c-1)$
 $= a \oplus (b \oplus c)$ 加法结合

• a 的加法逆元: $-a+2: a + (-a+2) - 1 = 1 = 0_R$ 加法逆元

• $a \oplus b = a+b-1 = b+a-1 = b \oplus a$ 加法交换

综上加法构成 Abel 群.

• $(a \cdot b) \cdot c = (a+b-ab) \cdot c = a+b+c-ab-ac-bc = a \cdot (b \cdot c)$ 乘法结合

• 1元: R 中的 1 元: $a \cdot 0 = a+0-0 = a$ 乘法幺元

• $(a \oplus b) \cdot c = (a+b-1) \cdot c = a+b-1+c - ac-bc+c$

$= (a+c-ac) + (b+c-bc) - 1 = (a+c-ac) \oplus (b+c-bc)$

$= (a \cdot c) \oplus (b \cdot c)$ 乘法分配律①

• $a \cdot b = a+b-ab = b+a-ba = b \cdot a$ 乘法交换

乘法分配律

• $c \cdot (a \oplus b) = (a \oplus b) \cdot c = (a \cdot c) \oplus (b \cdot c) = (c \cdot a) \oplus (c \cdot b)$ ②

综上得证.

8. (1) $R = \mathbb{Z}$, $S = 2\mathbb{Z}$

(2) $R = 2\mathbb{Z}$, $S = \frac{2\mathbb{Z}}{6\mathbb{Z}}$

(3) $R = \mathbb{Z}/9\mathbb{Z}$, $S = \mathbb{Z}/3\mathbb{Z}$

(4) $R = GL_n(\mathbb{R})$ 所有可逆阵, $S = DL_n(\mathbb{R})$ 所有对角阵.

$$12. \ ab a = (ab)a = a \Rightarrow a(ba-1) = 0 \quad \text{且 } ba-1 \neq 0$$

我们证明 $\{x_n\} = \{(ba-1)a^n + b\}$ 是无穷多个解 of $ax=1$.

$$\text{一方面}, \ a[(ba-1)a^n + b] = (aba-a)a^n + ab = 0 + 1 = 1$$

$$\text{另一方面}, \text{若 } x_k = x_l \text{ for } k \neq l, \text{ 由 } (ba-1)(a^k - a^l) = 0, \text{ 且 } k > l$$

$$\text{由 } ba^{k+1} - a^k - ba^{l+1} + a^l = 0 \quad \text{两侧右乘 } b^{t+1}, t = k-l > 0.$$

$$\Rightarrow ba^t - a^{t-1} - b + b = 0 \Rightarrow ba^t - a^{t-1} = 0, \text{ 两侧右乘 } b^{t-1}$$

$$\Rightarrow ba-1 = 0. \text{ 矛盾! 故 } x_n \text{ 两两不同}$$

□

9.23 作业

$$13. \text{ 设 } a^n = 0, \text{ 由 } (1-a)(1+a+\dots+a^{n-1}) = 1-a^n = 1$$

$$(1+a+\dots+a^{n-1})(1-a) = 1-a^n = 1$$

从而 $1-a$ 可逆

□

14. 设零元组成集合 S :

① 关于加法封闭: $\forall a \in S \text{ with } a^n = 0, b \in S \text{ with } b^m = 0, (a+b)^{m+n} =$

-一些 $\deg(a) \geq m$ 的单项 + $\deg(b) \geq n$ 的单项 = 0. 则 $a+b \in S$.

从而 S 是 R 的加法子群.

② 理想: $\forall a \in S \text{ with } a^n = 0, \forall r \in R, (ra)^n = r^n a^n = r^n \cdot 0 = 0$

$$(ar)^n = a^n \cdot r^n = 0 \cdot r^n = 0 \Rightarrow ra \in S. ar \in S. \Rightarrow S \text{ 是 } R \text{ 的}$$

理想

□

15. 以下默认 $i_* \in I$, $j_* \in J$, $k_* \in K$, $r_* \in R$.

$\forall x \in (I+J)K$. 存在有限 i_m, j_m, k_m 使 $x = \sum_{m=1}^M (i_m + j_m) k_m$

$$= \left(\sum_{m=1}^M i_m k_m \right) + \left(\sum_{m=1}^M j_m k_m \right) \in IK + JK.$$

$\forall x \in IK + JK$. 存在有限 i_p, k_p, j_q, k_q 使 $x = \sum_{p=1}^P i_p k_p + \sum_{q=1}^Q j_q k_q$.

$$= \sum_{p=1}^P (i_p + 0) k_p + \sum_{q=1}^Q (0 + j_q) k_q \in (I+J)K.$$

对于 $K(I+J) = KI + KJ$. 同理 \square

17. 假设 $M_n(K)$ 有一个理想 I . 我们给 $M_n(K)$ 分类:

$S_i = \{A \in M_n(K) \mid \text{rank}(A) = i\}$. 由于矩阵等价 $\Rightarrow \text{rank}$ 相同.

我们容易得到: $S_i \cap I = \emptyset$ 或 S_i . 事实上, 若 $\exists A \in S_i \cap I$, 则 $\forall B \in S_i$,

存在可逆阵 T 使 $B = AT \in I$.

若 $\exists i > 1$ 使 $\exists A \in S_i \cap I$. 即 $I \neq \{0\}$. 我们有 $A \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} * & * & \cdots & * \\ 0 & 0 & \cdots & 0 \end{pmatrix}$

$\Leftarrow B$ 有 $\text{rank } 1$. $\Rightarrow S_1 \subseteq I \Rightarrow \begin{pmatrix} 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix}$ ($a_{ii} = 1, \text{else} = 0$)

的矩阵在 I 中 ($i=1, 2, \dots, n$). 它们张成 $M_n(K)$ 的一组基. 从而

$I = M_n(K)$. 得证 \square

Note: 险江子环: ① 加法群 ② 乘法封闭. ③ I_R 是子环的元

验证理想: ① 加法群 ② 乘法($I+I$)性质.

Theorem. $\forall n \in \mathbb{Z}_+$ 有限域 \mathbb{F}_p 上有 n 次不可约多项式.

Definition 设 F 是一个域, $f(x) \in F[x]$, 若 F 的域扩张 K 满足

(1) $f(x)$ 在 K 上完全分裂, 即 $f(x) = (x - \alpha_1) \cdots (x - \alpha_n)$, $\alpha_i \in K$.

(2) $K = F(\alpha_1, \dots, \alpha_n)$

则称 K 是 $f(x)$ 在 F 上的分裂域

Lemma 1: 分裂域的存在性: 即 $\forall F \ni f(x)$. $f(x)$ 在 F 上的分裂域存在.

Pf: 我们对 $\deg f$ 归纳. $\deg f = 1$ 时取 $K = F$. 显然成立.

假设 Lemma 1 对 $\forall \deg f = n-1$ 的 $f(x)$ 成立. 当 $\deg f = n$ 时,

我们取变元 θ 使 $f(\theta) = 0$. 令 $L = F(\theta)$ 是 F 的域扩张. 则在 L 中

$f(x) = (x - \theta)g(x)$, $\deg g = n-1$. 由归纳假设存在 $g(x)$ 在 L 上的分裂

$\rightarrow K$, 使 $| g(x) = (x - \alpha_1) \cdots (x - \alpha_{n-1}) \quad (\alpha_i \in K)$

$f(x) = (x - \theta)(x - \alpha_1) \cdots (x - \alpha_{n-1}) \quad (\alpha_i \in K, \theta \in L \subset K).$

$K = L(\alpha_1, \dots, \alpha_{n-1}) = F(\theta)(\alpha_1, \dots, \alpha_{n-1}) = F(\theta, \alpha_1, \dots, \alpha_{n-1})$

从而 K 是 $f(x)$ 在 F 上的分裂域

事实上我们还可归纳证 $[K:F] \leq n!$. 由于 $[L:F] = \deg_F(\theta) \leq \deg(f) = n$

故 $[K:F] = [K:L][L:F] \stackrel{\text{归假}}{\leq} (n-1)! [L:F] \leq (n-1)! \cdot n = n!$ \square

Lemma 2: 设 F 是域, $f(x) \in F[x]$. 则 $f(x)$ 在 F 上有至多 $\deg f$ 个不同的根.

Pf: 对 $n = \deg f$ 归纳, $n=1$ 显. 假设 $n-1$ 时成立. $\deg f = n$ 时,

若 f 在 F 无根, 证毕; 若有, 取出一个记为 α . f 对 $(x - \alpha)$ 作带余除法,

知 $(x - \alpha) | f(x)$. 设 $f(x) = (x - \alpha)g(x)$, 对 $g(x)$ 用归纳 \square .

Lemma 3: 设 G 是交换群, $a, b \in G$, $\text{ord}(a) = m$, $\text{ord}(b) = n$,
且 $(mn)^{-1} = 1$, 则 $\text{ord}(ab) = mn$.

Pf: 一方面 $(ab)^{mn} = (a^m)^n \cdot (a^n)^m = 1 \cdot 1 = 1$.

另一方面 若 $(ab)^t = 1$, $\Rightarrow (ab)^{tm} = 1 \Rightarrow b^{tm} = 1$

$$\Rightarrow n | tm \Rightarrow n | t \quad \text{同理 } m | t \Rightarrow mn | t. \quad \square$$

Lemma 4: 设 G 是有限 Abel 群, 则存在 $x \in G$ 使 $\forall g \in G$,

$$\text{ord}(g) | \text{ord}(x)$$

Pf: 选最大 ord 的 x . 反证若 $\exists g \in G$ 使 $\text{ord}(g) > \text{ord}(x)$

记 $\text{ord}(g) = a$, $\text{ord}(x) = b$. 则存在素数 p 使

$$\alpha = v_p(a) > v_p(b) = \beta. \quad \text{由于 } \text{ord}(g^{\frac{a}{p^\alpha}}) = p^\alpha, \text{ord}(x^{p^\beta}) = \frac{b}{p^\beta}$$

且两者互素. 由 Lemma 3 知 $x' = g^{\frac{a}{p^\alpha}} \cdot x^{p^\beta}$ 的阶为 $b \cdot p^{\alpha-\beta} > b$

与 $\text{ord}(x)$ 最大性矛盾: \square

Lemma 5: 设 F 是有限域, F^\times 是 F 的单位群即 $F \setminus \{0\}$, 则 F^\times 是乘法循环群

Pf: 显然 F^\times 是乘法群, 设 $n = |F^\times|$, 我们考虑 F^\times 中满足 $x^m = 1$ 的元素

个数: 由 Lemma 2 知至多 m 个. 再由 Lemma 4 知存在 x 使 \forall

$g \in F^\times$, $\text{ord}(g) | \text{ord}(x) \triangleq t$. 故有 n 个元素 (即 F^\times 全部) 满足

$$x^t = 1, \quad \text{且 } t \geq n \Rightarrow t = n. \quad \text{即 } \langle g \rangle = F^\times \quad \square.$$

Definition. 设 $f(x)$ 是多项式, $f(x) = a_n x^n + \dots + a_1 x + a_0$.

定义它的形式导数 $D(f(x)) = n a_n x^{n-1} + \dots + 2 a_2 x + a_1$.

Lemma 7. 设 $f(x) \in F[x]$, K 是 f 在 F 上的分裂域, 则 f 在 K 上无重根 $\Leftrightarrow (f(x), D(f(x))) = (1)$.

Pf. 一方面若 $(f(x), D(f(x))) = (1)$. |R| 由 Bezout 定理, 存在

$p(x) \in F[x]$, $q(x) \in F[x]$, 使 $p(x)f(x) + q(x)D(f(x)) = (1)$

若存在 α 使 $(x-\alpha)^2 \mid f(x)$. 则 $(x-\alpha) \mid D(f(x))$

$\Rightarrow (f(x)) \mid (1)$ 矛盾!

另一方面. 若 f 无重根. 设 $f(x) = (x-\alpha_1) \dots (x-\alpha_n)$

$(d(x)) = (f(x), D(f(x)))$. 若 $d(x) \neq 1$, 则存在 α 满足

$f(\alpha) = 0$ 且 $D(f(\alpha)) = 0 \Rightarrow (x-\alpha)^2 \mid f(x)$, 矛盾! \square

Lemma 8 (1) 任何一个有限域 F , 存在素数 p 与正整数 n , 使 $\#F = p^n$

(2) 对任意素数 p 与正整数 n , 同构意义下存在唯一有限域 F

满足 $\#F = p^n$. 且 F 是 $x^{p^n} - x$ 在 \bar{F}_p 的分裂域.

Pf of (1) : 设 $\text{Char}(F) = p$. 则 $\bar{F}_p \subset F$. F 是 \bar{F}_p 上的线性空间,

设 $n = \dim_{\bar{F}_p}(F)$. 则 $\#F = p^n$

Pf of (2) : 一方面, 取 $x^{p^n} - x$ 在 \bar{F}_p 的分裂域 F , 由于 $D(x^{p^n} - x) = -1$

$\Rightarrow (x^{p^n} - x, D(x^{p^n} - x)) = (1)$. 故 $x^{p^n} - x$ 在 F 上无重根.

且对 $\forall a, b \in F$, $a^{p^n} - a = 0$, $b^{p^n} - b = 0$. 有

$$(a+b)^{p^n} - a - b = a^{p^n} + b^{p^n} - a - b = 0$$

$$(a-b)^{p^n} - a + b = a^{p^n} - b^{p^n} - a + b = 0$$

$$(ab)^{p^n} - ab = a^{p^n} \cdot b^{p^n} - ab = ab - ab = 0$$

$$(\frac{a}{b})^{p^n} - \frac{a}{b} = \frac{a^{p^n}}{b^{p^n}} - \frac{a}{b} = \frac{a}{b} - \frac{a}{b} = 0.$$

$\forall a+b, a-b, ab, a/b \in F$. 故 F 恰由 $x^{p^n} - x$ 的 p^n 个根构成.

证 Theorem

(不必要的) 另一方面. 证明 F 的唯一性, 即 $\#F = p^n$ 的 F 唯一.

由于 F^\times 是乘法循环群, 存在一个生成元 g , $F = \mathbb{F}_p(g)$

且 g 满足 $g^{p^n} - g = 0$. 由于 F^\times 中元素都满足 $x^{p^n} - 1 = 0$ 且

$x^{p^n-1} - 1 = 0$ 在 F 上至多 $p^n - 1$ 根 (Lemma 2) 故 F^\times 恰含 $x^{p^n-1} - 1 = 0$

的所有根 $\Rightarrow F$ 是 $x^{p^n} - x$ 在 \mathbb{F}_p 上的分裂域. 这是唯一的. \square .

回到原题

取 $F = \mathbb{F}_{p^n}$ 是含 p^n 个元素的 $\text{Char} = p$ 的域 (Lemma 8 的存在性)

则 F^\times 是循环群 (Lemma 5) 存一个生成元 α , 则 $F = \mathbb{F}_p(\alpha)$

由 $[F : \mathbb{F}_p] = n \Rightarrow \deg_F(\alpha) = n$. 存 α 在 \mathbb{F}_p 的最小多项式 $f(x)$

$\Rightarrow f(x)$ 是 n 次不可约多项式, 符合题意.

9.26 课堂

设 A 是体， F 是 A 的子集， F 是域，且 F 中元素均与 A 交换，则 A 是 F 上的一个线性空间

四元数代数要么与 $M_2(F)$ 同构，要么是体

不一定都可逆

Vector space 不自带双线性映射
人为定义可以映射到 \mathbb{R} (内), V (外).

Definition

设 $a, b \in F$, A 是 F 上的 4 维向量空间， i, j, k 是一组基，

其双线性乘法由单位元 1 与下列条件确定

$$i^2 = a, j^2 = b, ij = -ji = k.$$

容易验证 A 在该双线性乘法下构成环，称为四元数代数。记为 $(\frac{a, b}{F})$

Theorem 四元数代数 $A = (\frac{a, b}{F})$ 为体 $\Leftrightarrow c_0^2 = ac_1^2 + bc_2^2$ 在 F 上只有零解。

Proof: 定义对 α : $\alpha = c_0 + c_1 i + c_2 j + c_3 k$, $\bar{\alpha} = c_0 - c_1 i - c_2 j - c_3 k$.

$$\alpha \bar{\alpha} = c_0^2 - ac_1^2 - bc_2^2 + ab c_3^2 \in F, \bar{\alpha} = \alpha.$$

• α 可逆 ($\text{in } A$) $\Leftrightarrow \alpha \bar{\alpha}$ 可逆 ($\text{in } F$) $\Leftrightarrow \alpha \neq 0$ 时 $\alpha \bar{\alpha} \neq 0$

$$\Leftrightarrow c_0^2 - ac_1^2 - bc_2^2 + ab c_3^2 = 0 \text{ 只有零解.}$$

$$\text{上式可写成 } b(c_2^2 - ac_3^2)^2 = (c_0^2 - ac_1^2)(c_2^2 - ac_3^2)$$

$$= (c_0 c_2 + ac_1 c_3)^2 - a(c_0 c_3 + c_1 c_2)^2 = b x^2 = Y^2 - a Z^2.$$

$$\text{若 } c_2^2 - ac_3^2 = 0 \Rightarrow c_2 = c_3 = 0 \Rightarrow c_0^2 - ac_1^2 = 0 \Rightarrow c_0 = c_1 = 0$$

Example $A = (\frac{-1, -1}{\mathbb{R}})$, $c_0^2 + c_1^2 + c_2^2 = 0$ 只有零解，为体

. 即 $\left\{ \begin{pmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{pmatrix} \mid \alpha, \beta \in \mathbb{C} \right\}$, 一组基为

$$1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, i = \begin{pmatrix} 0 & 1 \\ 0 & -1 \end{pmatrix}, j = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, k = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

$$A = \left(\frac{-1, -1}{\mathbb{C}} \right) \cong M_2(\mathbb{C}), \text{ 基同上}$$

$$A = \left(\frac{1, 1}{\mathbb{Q}} \right) \cong M_2(\mathbb{Q}), \text{ 基同上}$$

基为 $(1, 0), (0, 1), (0, 1), (-1, 0)$

9.27

P45 T9. 10. 11. 13. 14. 15.

9. $IH_0 \subseteq IH$, 我们只需验证运算是封闭的.

$$(a_1 + b_1 I + c_1 J + d_1 K)(a_2 + b_2 I + c_2 J + d_2 K) =$$

$$(a_1 a_2 - b_1 b_2 - c_1 c_2 - d_1 d_2) + (c_1 d_2 - d_1 c_2 + b_1 a_2 + a_1 b_2) I +$$

$$(d_1 b_2 - d_2 b_1 + a_2 c_1 + a_1 c_2) J + (b_1 c_2 - c_1 b_2 + a_2 d_1 + a_1 d_2) K. \quad \xi \text{数} \in \mathbb{Q}.$$

$$\Rightarrow \text{上式} \in IH_0.$$

$$(a_1 + b_1 I + c_1 J + d_1 K) + (a_2 + b_2 I + c_2 J + d_2 K)$$

$$= (a_1 + a_2) + (b_1 + b_2) I + (c_1 + c_2) J + (d_1 + d_2) K \quad \xi \text{数} \in \mathbb{Q}.$$

$$\Rightarrow \text{上式} \in IH_0.$$

10. 利用 T_9 的结果. $x, y \in IH$. (对应系数下标 1, 2), $xy = yx$, $\forall y \Leftrightarrow$

$$c_1 d_2 - d_1 c_2 = 0, \quad d_1 b_2 - d_2 b_1 = 0, \quad c_1 b_2 - c_2 b_1 = 0, \quad \forall b_2, c_2, d_2$$

$$\overline{y} \times c_2 = 0, \quad d_2 = 1 \Rightarrow c_1 = 0. \quad [\text{由} d_1 = b_1 = 0 \Rightarrow Z(IH) = \mathbb{R}].$$

$$= \{a + 0 + 0 + 0 \mid a \in \mathbb{R}\}.$$

11. $|Q_8| = 8$, 非平凡子群阶为 4 或 2. 设子群 $N \leq Q_8$

Case 1: 2 阶群: $(Q_8 \text{ 中 } 2 \text{ 阶元仅 } -1, \text{ 子群 } N \text{ 仅可能为 } \{1, -1\})$

考虑 $\varphi: Q_8 \rightarrow (\mathbb{Z}_2 \times \mathbb{Z}_2, +)$, $1, -1 \mapsto (0, 0)$, $\pm I \mapsto (1, 0)$

$\pm J \mapsto (0, 1)$, $\pm K \mapsto (1, 1)$ 易验证是同态. $\ker \varphi = \{1, -1\}$

故 $Q_8/\{1, -1\} \cong (\mathbb{Z}_2 \times \mathbb{Z}_2, +)$, $\{1, -1\} \triangleleft Q_8$.

Case 2: 4 阶群 由 $[Q_8 : N] = 2$ 及 $P_{25} T_{23}$ 结论知

指数为 2 的子群 N 必正规

□

(3) (1) 假设存在 $a_1, a_2 \in L$, $a_1, a_2 \neq 0$. $a_1 a_2 = 0$. 则 $\exists b$ 使 $a_1 b a_1 = a_1$

而由 $b + a_2 \neq b$ 且 $a_1(b + a_2)a_1 = (ab + a_1 a_2)a_1 = (ab + 0)a_1 = aba_1 = a_1$,
 $= a_1$, 矛盾! 故不存在非零零因子.

(2) $aba = a \Rightarrow abab = ab \Rightarrow a(bab - b) = 0 \Rightarrow bab - b = 0 \Rightarrow bab = b$

(3) 任一个非零 a , 依题找到 b 使 $aba = a$. 若 $b = f(a)$.

我们证明. $\forall a, b \in L$. $a f(a) = f(a) \cdot a = b f(b)$. 从而定义其为 1

事实上 $a f(a) a = a \dots (*)_1 \quad a = a f(a) a \dots (*)_2$ 从 $(*)_2$ 右乘 $(*)_1$

$\Rightarrow a f(a) a a = a a f(a) a \Rightarrow a (f(a) a - a f(a)) a = 0$

$\Rightarrow (f(a) a - a f(a)) a = 0 \Rightarrow f(a) a - a f(a) = 0 \Rightarrow f(a) a = a f(a)$

$b = b f(b) b \dots (*)_3$. $(*)_3$ 右乘上 $(*)_1$ 得

$a f(a) a b = a b f(b) b \Rightarrow f(a) a = b f(b)$. 从而 1 是良定义的.

另一方面我们验证 $\forall x \in L$. $1x = x1 = x$. 将 1 写成 $x f(x)$

则 $1x = x f(x) x = x$, 将 1 写成 $f(x) x$. 则 $x1 = x f(x) x = x$.

(4) 我们在(3)中证明了环 L 有乘法幺元且也有逆, 故 L 是体.

□

$$14. (b^{-1} - a)^{-1} = ((1-ab)b^{-1})^{-1} = b(1-ab)^{-1}$$

$$\begin{aligned} (a^{-1} + (b^{-1} - a)^{-1})^{-1} &= (a^{-1} + b(1-ab)^{-1})^{-1} = (a^{-1}(1 + ab(1-ab)^{-1}))^{-1} \\ &= (1 + ab(1-ab)^{-1})^{-1}a = (-c(1-ab)(1-ab)^{-1} + 1 + (1-ab)^{-1})^{-1}a \\ &= ((1-ab)^{-1})^{-1}a = (1-ab)a = a - aba, \text{ 整理即得原式.} \end{aligned}$$

$$15. (a+b)^p = a^p + \binom{p}{1} a^{p-1} b + \dots + \binom{p}{k} a^{p-k} b^k + \dots + b^p$$

$$\text{而对 } 1 \leq k \leq p-1, \quad \binom{p}{k} = \frac{p(p-1)\dots(p-k+1)}{k!} \in \mathbb{Z}$$

且分子与 p 互素. 故 $p \mid \binom{p}{k} \Rightarrow \binom{p}{k} \equiv 0$.

$$\text{从而 } (a+b)^p = a^p + b^p$$

□

Theorem 四元数代数 $A = (\frac{a, b}{F})$ 为体 $\Leftrightarrow c_0^2 = ac_1^2 + bc_2^2$ 在 F 上只有零解 ---(*1)

proof: 定义对合: $\alpha = c_0 + c_1i + c_2j + c_3k$, $\bar{\alpha} = c_0 - c_1i - c_2j - c_3k$.

$$\alpha\bar{\alpha} = c_0^2 - ac_1^2 - bc_2^2 + abc_3^2 \in F, \quad \bar{\alpha} = \alpha.$$

• α 可逆 ($\text{in } A$) $\Leftrightarrow \alpha\bar{\alpha}$ 可逆 ($\text{in } F$) $\Leftrightarrow \alpha \neq 0$ 时 $\alpha\bar{\alpha} \neq 0$

$$\Leftrightarrow c_0^2 - ac_1^2 - bc_2^2 + abc_3^2 = 0 \text{ 只有零解 over } F \quad ---(*2)$$

$$\text{上式可写成 } b(c_2^2 - ac_3^2)^2 = (c_0^2 - ac_1^2)(c_2^2 - ac_3^2)$$

$$= (c_0c_2 + ac_1c_3)^2 - a(c_0c_3 + c_1c_2)^2$$

则显然 $(*2) \Rightarrow (*1)$ ($c_3 = 0$ 时)

$$\text{若 } (*1) \text{ 则 } (c_2^2 - ac_3^2) = 0 \Rightarrow c_2 = c_3 = 0$$

$$\Rightarrow c_0^2 - ac_1^2 = 0 \Rightarrow c_0 = c_1 = 0 \Rightarrow (*2)$$

定义: $C_G(H) = \{x \in G \mid xax^{-1} = a, \forall a \in H\}$

$N_G(H) = \{x \in G \mid xHx^{-1} = H\}$.

$Z(G) = C_G(G)$.

$H \trianglelefteq N_G(H)$. $C_G(H) \trianglelefteq N_G(H)$. $Z(G) \trianglelefteq G$.

$\{Z_0 = Z, Z_1, \dots, Z_k = G\}$ 称为 G 的上中心链

若 $Z_{k+1}(G)/Z_k(G) = Z(G/Z_k(G))$

$$\begin{array}{ccc} G & \xrightarrow{\pi} & G/Z_k(G) \\ & & \downarrow \\ Z_{k+1} & \xleftarrow{\pi^{-1}} & Z(G/Z_k(G)) \end{array}$$

称这样的 G 为幂零群. k 为幂零群的类

Sylow 定理.

定理 1. 设 $n = p^k \cdot m$. 则 $1 \leq l \leq k$. p^l 子群均存在

法 1. 考虑 G 的所有 p^l 元子集构成的集合 S . G 左乘作用到 S .

熟知 $V_p(\binom{p^k \cdot m}{p^l}) = k-l$. 故 $p^{k-l+1} \mid |S|$.

$|S| = \sum |\text{Orb}(A)|$. 故存在 p 元子集 $A \in S$ 使 $p^{k-l+1} \mid |\text{Orb}(A)|$

由 $|\text{Stab}(A)| = \frac{|G|}{|\text{Orb}(A)|}$ 知 $p^l \mid |\text{Stab}(A)|$.

而 $\forall a \in A$. 则 $\{gal \mid g \in \text{Stab}(A)\} \subseteq A$ 且 ga 两两不同.

$\Rightarrow |\text{Stab}(A)| \leq |A| = p^l \Rightarrow |\text{Stab}(A)| = p^l$ 是 p^l 子群.

法2. 对 $|G|$ 归纳.

1°. $|G|=1$ 时显然.

2°. Case 1. $p \nmid |G|$. 显然.

Case 2. $p \mid |Z(G)|$. $R \mid Z(G)$ 是有限生成 Abel 群, 可写为

$$\underbrace{\mathbb{Z}_{p^{r_1}} \times \cdots \times \mathbb{Z}_{p^{r_s}} \times \cdots}_{} = Z(G)$$

记为 $Z(G)_p$.

从而 $Z(G)_p \trianglelefteq G$. 考虑 $G \xrightarrow{\pi} G/Z(G)_p := \bar{G}$.

由归纳假设, 存在 \bar{G} 的 Sylow- p 子群 H .

则 $|\pi^{-1}(H)| = |Z(G)_p| \cdot |H|$ 是 G 的 Sylow- p 子群.

Case 3 $p \mid |Z(G)|$ 但 $p \nmid |G|$.

考虑共轭类方程: $|G| = |Z(G)| + \sum_{i=1}^t |G : C_G(g_i)|$

$\Rightarrow \exists g_i$ 使 $p \nmid |G : C_G(g_i)| \Rightarrow C_G(g_i)$ 是 G 的真子群

且 $v_p(|C_G(g_i)|) = v_p(|G|)$. 在 $C_G(g_i)$ 用归纳假设,

其 Sylow- p 子群 即 G 的 Sylow- p 子群

定理 15 (Cauchy 定理)

设 G 是有限群. 素数 $p \mid \#G$. 则 G 有 p 阶元且 p 阶元个数 n_p

满足 $n_p \equiv -1 \pmod{p}$

定理 16 设 G 是有限群. $p \mid \#G$, 则有

(1) 若 S_p 是 G 的一个 sylow p -子群, P 是 G 的一个 p -子群, 则 $\exists g \in G$

使 $P \subseteq gS_p g^{-1}$

(2) G 的所有 sylow p -子群两两共轭. 因而

$$|G : N_G(S_p)| = N_p \equiv 1 \pmod{p}.$$

pf (1): Ω 是 G 关于 S_p 的全体左陪集的集合. 考察 P 在 Ω 上的左乘作用

$$\text{则 } [G : S_p] = |\Omega| = \sum [P : \text{Stab}(x_i S_p)] \not\equiv 0 \pmod{p}$$

且 $[P : \text{Stab}(x_i S_p)]$ 为 p 的幂 \Rightarrow 存在 x_i 使 $[P : \text{Stab}(x_i S_p)] = 1$

$$\text{即 } P \cdot x_i S_p = x_i S_p \Rightarrow x_i^{-1} P x_i \subseteq S_p \Rightarrow P \subseteq x_i S_p x_i^{-1}$$

(2) G 中元素共轭作用到 $\{G$ 的所有 sylow p -子群 $\} = \Gamma$ 上

由 (1). G 在 Γ 作用只有一条轨道. $N_p = |\Gamma| = [G : \text{Stab}(S_p)]$

$$= [G : N_G(S_p)]$$

引理: P 作用到集合 X 上. $\gcd(|X|, p) = 1$. 则一定有不动元素 $x_0 \in X$.

且 $|X| \equiv$ 不动元素的个数 $(\text{mod } p)$

事实: 设 P 是 G 的 sylow p -子群. 则 P 是 $N_G(P)$ 的唯一 sylow- p 子群

引理: $N_p \equiv 1 \pmod{p}$ 可推出 $[N_G(P) : P] \equiv [G : P] \pmod{p}$

pf: 任 sylow p -子群 P 共轭作用到所有 sylow p -子群上

由于 $N_p = [G : N_G(P)] \not\equiv 0 \pmod{p}$. 且作用下的不同元素只有 P .

(否则有 $Q \neq P$ 也是 $N_G(P)$ 子群, 矛盾!) $\Rightarrow N_p \equiv 1 \pmod{p}$.

定理 17 设 G 是有限群. $p \mid \#G$, S_p 是 G 的一个 sylow- p 子群.

$N_G(S_p) \leq H \leq G$. 则 $N_G(H) = H$.

Pf: $N_G(S_p) \leq H \leq N_G(H) \leq G$

$\nearrow N_H(S_p)$ because

H 中 Sylow- p 子群个数为 $[H : N_G(S_p)]$.

$N_G(S_p) \leq H$

$N_G(H)$ 中 Sylow- p 子群个数为 $[N_G(H) : N_G(S_p)]$.

$\nearrow N_{N_G(H)}(S_p)$ because

$N_G(S_p) \leq N_G(H)$

$N_G(H)$ 中 Sylow- p 子群个数为 $n S_p n^{-1}$, $n \in N_G(H)$

但 $n S_p n^{-1} \leq n H n^{-1} = H$. 故个数相同 $\Rightarrow H = N_G(H)$

$\text{若 } \forall H < G, H < N_G(H)$

\Rightarrow " \Leftarrow " 则 $N_G(\cdot)$ 可使 H "升阶" G .

只须注意到

定理 18 设 G 是有限幂零群. H 是真子群. 则 $H < N_G(H)$ 真子群.

$p \leq H \Rightarrow p \nleq N_G(H)$

Pf: 设 $\{e\} = Z_0(G) \trianglelefteq \dots \trianglelefteq Z_k(G) = G$. $[Z_{i+1}(G), G] = Z_i(G)$

设存在 i 使 $Z_i(G) \leq H$, $Z_{i+1}(G) \not\leq H$. $1 \leq i \leq k-1$

此时 $[Z_{i+1}(G), H] \leq [Z_{i+1}(G), G] \leq Z_i(G) \leq H$

$z^{-1}h^{-1}zh \in H$ 且 $z^{-1}h^{-1}z \in H \Rightarrow Z_{i+1}(G) \leq N_G(H)$

$\Rightarrow N_G(H) \neq H \Rightarrow H < N_G(H)$. $\star Z_i(G) \leq H$

$\Rightarrow Z_{i+1}(G) \leq N_G(H)$

定理 19 设 G 是一个有限幂零群, 素数 p_1, \dots, p_t 为 $\#G$ 所有素因子

则 $G \cong S_{p_1} \oplus S_{p_2} \oplus \dots \oplus S_{p_t}$

Pf: 对于 S_{p_i} , 它一定是 G 正规矩子群. 否则 $N_G(S_{p_i}) < G$

Th18

$\Rightarrow N_G(N_G(S_{p_i})) > N_G(S_{p_i})$. 与 Th17 矛盾!

故 H_i . S_{p_i} 正规且两两互为正规.

$$\Rightarrow S_{p_1} \oplus \dots \oplus S_{p_t} \cong S_{p_1} \dots S_{p_t}$$

$\forall g \in G$, g 可表示为 $g_1 \dots g_t$ 使 $\text{ord}(g_i)$ 为 p_i 方幂

但 $\langle g_i \rangle$ 是 G 的 p_i 子群 $\leq S_{p_i} \Rightarrow g_i \in S_{p_i}$

$$\Rightarrow S_{p_1} \dots S_{p_t} = G \Rightarrow \text{结论成立}$$

定理 20: 设 G 是有限 Abel 群. $\#G = p_1^{e_1} \dots p_t^{e_t}$, 则

$$G \cong \bigoplus_{i=1}^t \bigoplus_{j=1}^{k_i} \mathbb{Z}/p_i^{l_{ij}} \mathbb{Z}, \quad \sum_{j=1}^{k_i} l_{ij} = e_i \text{ for } 1 \leq i \leq t.$$

G 的同构由 $\{l_{ij}\}$ ($p_i^{l_{ij}}$ 称 G 的初等因子) 决定.

定义: 设 G 是交换 p -群, 且 $\max_{g \in G} \{\text{ord}(g)\} = p$. 则称 G 是初等交换 p -群.

引理: \forall 初等交换 p -群 $\cong \bigoplus_{i=1}^t \mathbb{Z}/p \mathbb{Z}$.

Pf: 取 G 最小生成元组. $G = \langle x_1 \rangle + \dots + \langle x_r \rangle$

我们声称和是直积. 否则存在 n_i , $\sum_{i=1}^r n_i x_i = 0$

不妨 $p \mid n_1$. 则 $\exists a, b \in \mathbb{Z}$. $an_1 + bp = 1$

$\Rightarrow x_1 = an_1 x_1 = -a \left(\sum_{i=2}^r x_i \right)$, 与最小性矛盾!

一些观察：① 唯一的 sylow p -子群一定是特征子群.

② 正规子群的特征子群还是正规子群.

③ sylow p -子群正规 \Rightarrow 唯一 \Rightarrow 特征子群

故若 G 是有限群， $\forall H \subset G$ 有 $H \subset N_G(H)$. 设 P 是某 sylow p -子群

则可考虑 $P < N_G(P) < N_G(N_G(P)) < \dots < N_G^{(k)}(P) = G$.

则 $\forall 1 \leq i \leq k-1$. 假设已有 $P \text{ char } N_G^{(i)}(H)$.

则 由 $N_G^{(i)}(P) \triangleleft N_G^{(i+1)}(P)$. $\stackrel{\textcircled{2}}{\Rightarrow} P \trianglelefteq N_G^{(i+1)}(P)$. $\stackrel{\textcircled{3}}{\Rightarrow} P \text{ char } N_G^{(i+1)}(P)$

又由于 $P \text{ char } P$ 作奠基. 知 $P \text{ char } G \Rightarrow P \trianglelefteq G$.

从而 G 的任一个 sylow p 子群均为正规 $\Rightarrow G$ 是幂零群.

因此幂零群 $\Leftrightarrow \forall H \subset G, H \subset N_G(H)$

定义 10 $G = G_0 \trianglerighteq G_1 \trianglerighteq \dots \trianglerighteq G_n = \{e\}$ 称为群 G 的次正规群列

每个 G_i 是 G 的次正规子群.

若 $\forall i, G_{i-1} \ntrianglerighteq G_i$ 且 G_{i-1}/G_i 是单群，则称该群列为

G 的合成群列. G_{i-1}/G_i 为合成因子.

一个群不一定有合成群列： \mathbb{Z} . 但有限群一定有合成群列

定理 21 设 G 是一个有限群. 它的任一个无重复项的次正规群列可以
加细为合成群列.

定理 22 设 G 是有限群，它的所有合成群列长度均相等，且它们的合成因子在不计顺序的意义下对应同构。

证明： 对 G 的合成群列长度的最小值 k 作归纳。

1° $k=1$ 时。平凡

2° 设 $G = G_0 \trianglelefteq G_1 \trianglelefteq \dots \trianglelefteq G_k = \{e\}$ —— (1)

$\overset{\parallel}{H_0} \trianglelefteq H_1 \trianglelefteq \dots \trianglelefteq H_r = \{e\}$ —— (2)

当 $H_1 = G_1$ 时。用归纳假设。平凡

当 $H_1 \neq G_1$ 时。此时 $\underline{G_1 \cdot H_1 = G_1}$. $\rightarrow G_1 \cdot H_1 \trianglelefteq G$ 且 $G_1 \cdot H_1 > G_1$

$$G/G_1 \cong G_1 \cdot H_1 / G_1 \cong H_1 / G_1 \cap H_1 \text{ 单群}$$

$$G/H_1 \cong G_1 \cdot H_1 / H_1 \cong G_1 / G_1 \cap H_1 \text{ 单群}$$

$$\bigwedge K_2 = H_1 \cap G_1. \quad K_2 \trianglelefteq K_3 \trianglelefteq \dots \trianglelefteq K_t = \{e\} \quad --- (3)$$

$$\text{则 } G \trianglelefteq G_1 \triangleright K_2 \trianglelefteq \dots \trianglelefteq K_t = \{e\} \quad --- (4)$$

$$G \trianglelefteq H_1 \trianglelefteq K_2 \trianglelefteq \dots \trianglelefteq K_t = \{e\} \quad --- (5)$$

均为 G 的合成列。

由前述讨论。 G 的合成群列长度 $\leq k-1$ 。用归纳假设 $\Rightarrow t=k$ 。

且 (1) 与 (4) 有相同合成因子。

又由 (5) 知 H_1 最短合成群列长度 $\leq k-1$ 。用归纳假设 $\Rightarrow r=t=k$ 。

且 (2) 与 (5) 有相同合成因子。又 (4) 与 (5) 有相同合成因子。

\Rightarrow (1) 与 (2) 有相同合成因子。 \square

命题4. I, J 是环 R 的两个理想. 则 $I+J, I \cap J$ 也为 R 的理想.

$I+J=R$ 时, 称理想 I 与 J 互素. $\Leftrightarrow 1 \in I+J$

定义4. $IJ = \{ \text{finite sum of } ij \} = \langle ij \mid i \in I, j \in J \rangle$

一般情况下 $IJ \neq JI$ 且 $IJ \subseteq I \cap J$ ($\Rightarrow I+J=R, IJ=JI$)

分配律成立: $I(J+K) = IJ+IK, (J+K)I = JI+KI$.

$I+J=R, IJ=JI$ 则 $1=a+b$ 且 $a \in I, b \in J$.

$r = ra+rb \in JI+IJ = IJ \Rightarrow I \cap J \subseteq IJ \Rightarrow I \cap J = IJ$

命题5 设 I_1, I_2, J 是环 R 的理想. 且 I_1, I_2 与 J 互素 $\Rightarrow I_1I_2$ 与 J 互素.

证明 设 I_1, \dots, I_n 与 J 互素. 则 $I_1 \dots I_n$ 与 J 互素.

定理4 (中国剩余定理)

设 I_1, I_2, \dots, I_n 是环 R 中两两互素的理想. 则

$$R/(I_1 \cap I_2 \cap \dots \cap I_n) \cong R/I_1 \oplus \dots \oplus R/I_n$$

证明: 考虑 $\alpha: R \longrightarrow R/I_1 \oplus \dots \oplus R/I_n$

$$r \longmapsto (r+I_1) + \dots + (r+I_n)$$

α 是环同态. (保 +, \times , 单位元)

$$\ker \alpha = \{ r \mid r \in I_1, r \in I_2, \dots, r \in I_n \} = I_1 \cap \dots \cap I_n$$

故 $\bar{\alpha}: R/(I_1 \cap I_2 \cap \dots \cap I_n) \rightarrow R/I_1 \oplus \dots \oplus R/I_n$ 单射.

下证 $\bar{\alpha}$ 是满的. 设 $1_i \in I_i$, $\forall 1 \leq i \leq n$, $\bar{\alpha} \alpha_i = 0 + \dots + 0 + 1_i + 0 + \dots$

我们让 $\alpha_i \in \text{Im } \bar{\alpha}$.

由于 $I_1 \dots I_{i-1} I_i + I_{i+1} \dots I_n = R$. 故可取 $a_i + b_i = 1_R$.

$R \mid \bar{\alpha}(a_i) = \alpha_i$.

$\forall \bar{u} \in R/I_1 \oplus \dots \oplus R/I_n$.

$$\bar{u} = \bar{u}_1 + \bar{u}_2 + \dots + \bar{u}_n$$

$R \mid \bar{\alpha}(u_1 a_1 + \dots + u_n a_n) = \bar{u}_1 + \dots + \bar{u}_n = \bar{u}$ 故满射.

定义5. P 是 R 的真理想. 若对于 R 的任意理想 I, J , $IJ \subseteq P$ 蕴含 $I \subseteq P$ 或 $J \subseteq P$, 则称 P 为 R 的一个素理想.

若对于 R 的理想 I , $I \neq P$ 蕴含 $I = R$, 则称 P 为 R 的一个极大理想.

定理5 R 是交换环, 则 P 是 R 的素理想 $\Leftrightarrow \forall a, b \in R$,

$ab \in P$ 蕴含 $a \in P$ 或 $b \in P$.

证明: $ab \in P \Leftrightarrow (ab) \subset P \Leftrightarrow (a)(b) \subset P$

$\Leftrightarrow (a) \subset P$ 或 $(b) \subset P \Leftrightarrow a \in P$ 或 $b \in P$

定理8 在交换环 R 中, P 是真理想

(1) P 是素理想 $\Leftrightarrow R/P$ 是整环

(2) P 是极大理想 $\Leftrightarrow R/P$ 是域

证明：(1) P 是素理想 $\Leftrightarrow ab \in P$ 蕴含 $a \in P$ 或 $b \in P$

$\Leftrightarrow \bar{ab} = \bar{0}$ 蕴含 $\bar{a} = \bar{0}$ 或 $\bar{b} = \bar{0}$

$\Leftrightarrow R/P$ 是整环

(2) P 是极大理想 $\Leftrightarrow \forall P \subsetneq I, I$ 理想. $I = R$

$$\left\{ \begin{array}{l} \Leftarrow : \forall a \in I \setminus P, R = (a) + P \subset I \Rightarrow I = R \\ \Rightarrow : P \subsetneq (a) + P. \text{ 故 } (a) + P = R. \\ \Leftrightarrow \forall a \notin P, (a) + P = R \end{array} \right.$$

$\Leftrightarrow \forall \bar{a} \neq \bar{0}. (\bar{a}) = R/P$

$\Leftrightarrow \forall \bar{a} \neq \bar{0}. \exists \bar{b} \in R/P \text{ 使 } \bar{a}\bar{b} = \bar{1}$

$\Leftrightarrow R/P$ 是域

设 R 是交换环, S 是 R 上包含 1 的乘法封闭子集, 在 $R \times S$ 上定义

等价关系 " \sim " : $(a, b) \sim (a', b')$ $\Leftrightarrow \exists t \in S$ 使

$$tab' = ta'b. \quad \text{记 } S^1R := (R \times S)/\sim$$

此时未必有 R 到 S^1R 的嵌入.

$$\alpha : R \longrightarrow S^1R \quad a \mapsto \frac{a}{1}$$

是嵌入 $\Leftrightarrow S$ 中不包含 R 的零因子.

例 1: (1) $S = R \setminus P$. P 是交换环 R 的素理想. P

(2) $S = \{f^n \mid n \in \mathbb{N}\}$. f 是 R 的非零元.

幂零群性质 (12号 Abel)

(1) Two elements having relatively prime orders must commute.

(2) If d divides the order of G , then G has a normal subgroup of order d .

for (2). We only need to prove it when G is a p -group. which means.

(3) If $\#G = p^n$, then for integer k . $1 \leq k \leq n$, G has a normal subgroup with order p^k .

(3) can be proved by induction:

pf of (2) : 我们证明对任意数 p , $n \in \mathbb{N}^*$, p^n 阶群含有 p^k 阶正规子群 ($1 \leq k \leq n$)

对 n 归纳:

1° $n=1$ 平凡

2° $\leq n$ 成立. $n+1$ 时, 知 $Z(G)$ 非平凡. 取 $g \in Z(G)$ 且 $g \neq e$. $\text{ord}(g)=l$

则 $h = g^{l-1}$, 有 $\text{ord}(h)=1$ 且 $h \in Z(G)$. 则 $\langle h \rangle \subset Z(G) \Rightarrow \langle h \rangle \trianglelefteq G$

对 $G/\langle h \rangle$ 用归纳假设. 知 $\forall 1 \leq k \leq n$. 存在 p^k 阶正规子群 Q .

取 $R = \pi^{-1}(Q)$. $\pi: G \rightarrow G/\langle h \rangle$ 则 $\#R = p^{k+1}$ 且 $R \trianglelefteq G$

G 的 p 阶正规子群已由 $\langle h \rangle$ 给出. 证毕.

Q8 是最小的非阿贝尔 p 群.

Feit-Thompson Theorem

奇阶有限群一定可解.

幂零群 " G^k " "2" 定义的等价性

$$1^\circ \quad G^k = [G, G^{k-1}] \quad : \quad G = G^0 \triangleright G^1 \triangleright \cdots \triangleright G^k = \{e\}$$

$$2^\circ \quad G \longrightarrow G/Z_i \quad : \quad G = Z_r \triangleright Z_{r-1} \triangleright \cdots \triangleright Z_0 = \{e\}$$

$$Z_{i+1} \longleftarrow Z(G/Z_i) \quad Z_{i+1}/Z_i = Z(G/Z_i)$$

只需证 $G^k \subseteq Z_{r-k}$. 对 $k < 1$ 为真.

$k=0$ 显.

$$\leq k-1 \text{ 成立: } G^k = [G, G^{k-1}] \subseteq [G, Z_{r+1-k}] \subseteq Z_{r-k}$$

$\downarrow \quad \downarrow$

$$\pi(gzg^{-1}z^{-1}) = \pi(g)\pi(z)\pi(g^{-1})\pi(z^{-1}) \xrightarrow{\text{可交换}} = e$$

$$\Rightarrow [G, Z_{r+1-k}] \subseteq Z_{r-k}$$

意义 右正则表示, 左正则表示: $L(a): G \rightarrow G$

$$g \mapsto ag$$

$$L(G) \leq S(G)$$

指数: 元素阶的最小公倍数

特征子群: (1) $A \trianglelefteq B$ 则 $A \trianglelefteq B$

(2) $A \trianglelefteq B$, $B \trianglelefteq C$ 则 $A \trianglelefteq C$

(3) $A \trianglelefteq B$, $B \trianglelefteq C$ 则 $A \trianglelefteq C$

特别地: $\underline{G^{(n)} \trianglelefteq G}$.

类方程: $|G| = |Z(G)| + \sum_{i=1}^m |G : C_G(g_i)|$

$p \neq q$ 时群分类. $p \leq q$

① $p = q$: $\mathbb{Z}_{p^2}, \mathbb{Z}_p \times \mathbb{Z}_p$

② $p < q$: $n_q | p, n_q \equiv 1 \pmod{q} \Rightarrow n_q = 1$

(i) $n_p = 1, \mathbb{Z}_p \times \mathbb{Z}_q$

(ii) $n_p = q \quad \text{且 } p \mid q-1$

$$G_1 = \mathbb{Z}_q \rtimes_{\phi} \mathbb{Z}_p, \quad \phi: \mathbb{Z}_p \rightarrow \text{Aut}(\mathbb{Z}_q) \cong \mathbb{Z}_{q-1}$$

从而 ϕ 不平凡. ϕ 将 $1_{\mathbb{Z}_p}$ 映射到 \mathbb{Z}_{q-1} 中的一个 p 阶元.

$$G_t = \langle r, s \mid r^p = 1, s^q = 1, rsr^{-1} = s^t \rangle \quad \text{其中 } (t, q) = 1$$

且 $\delta_q(t) = p$ (事实上 G_t 两两同构)

e.g. $(GL_n(\mathbb{R}))^\dagger = SL_n(\mathbb{R})$

且 $SL_n(\mathbb{R}) \subseteq (GL_n(\mathbb{R}))^\dagger$.

设 $\pi: GL_n(\mathbb{R}) \longrightarrow (\mathbb{R}^*, \times)$

$$A \mapsto \det A$$

$$\Rightarrow \ker \pi = SL_n(\mathbb{R}) \quad \Rightarrow \frac{GL_n(\mathbb{R})}{SL_n(\mathbb{R})} = \mathbb{R}^* \quad \underline{\text{Abelian!}}$$

$$\Rightarrow SL_n(\mathbb{R}) \supseteq (GL_n(\mathbb{R}))^\dagger$$

$\#G = p^a \cdot n$, n 不一定与 p 互素. 则 G 中 p^a 阶子群个数 $\equiv 1 \pmod{p}$

pf: 考虑 G 左乘作用到 $M = \{$ 所有 G 的 p^a 阶子群 $\}$. $\#M = \binom{p^a \cdot n}{p^a}$

$\forall M_i \in M$. $P = \text{Stab}(M_i)$, $P M_i = M_i$ 说明 M_i 是 P 若干右陪集的并

$$\Rightarrow \#P \mid \# M_i = p^a$$

且 $\#P = p^a \Leftrightarrow M_i$ 是 P 的右陪集 $\Leftrightarrow \text{Orb}(M_i)$ 中恰有一个子群 $\Omega (= P)$

故类方程: $\binom{p^a \cdot n}{p^a} = n \cdot N(p^a) + \sum_{\text{other}} [G_i : \text{Stab}]$

容易证明 $\frac{1}{n} \binom{p^a \cdot n}{p^a} \equiv 1 \pmod{p}$

$$\Rightarrow 1 \equiv N(p^a) + \sum_{\text{other}} \frac{1}{n} [G_i : \text{Stab}] \pmod{p}$$

$$\equiv N(p^a) \pmod{p}.$$

特别地, p^a 阶子群存在.

§ PID and UFD.

定义7

整除、相伴 (两两整除)

命题6

$a = bc$, 则 a 与 b 相伴 $\Leftrightarrow c$ 是可逆元

定义8

因子、最大公因子 (被所有因子整除) 倍式、最小公倍式 (整除所有公倍式) } 各自内部两两相伴

定义9

Irreducible: $a = bc$ implies b or c has inverse element

Prime: $p \mid ab$ implies $p \mid a$ or $p \mid b$.

命题7

p 是素元 $\Rightarrow (p)$ 是非零素理想. 素元一定不可约.

例1

$$R = \mathbb{Z}[\sqrt{-5}]$$

(i) $3, 2 + \sqrt{-5}, 2 - \sqrt{-5}$ 不可约. 但不是素元.

不可约性化为 $(a^2 + 5b^2)(c^2 + 5d^2) = 9$ 只能为 $9 \times 1 = 9$, 不能是 3×3

$$\text{且 } 9 = 3 \cdot 3 = (2 + \sqrt{-5})(2 - \sqrt{-5})$$

(iii) 9 和 $3(2 + \sqrt{-5})$ 的最大公因子.

否则设为 c . $R \mid 3 \mid c$. $c = 3b$.

由于 $c \mid 3(2 + \sqrt{-5}) \Rightarrow b \mid 2 + \sqrt{-5} \Rightarrow b = \pm 1, \pm (2 + \sqrt{-5})$

$\Rightarrow c = \pm 3, \pm 3(2 + \sqrt{-5})$

$\cancel{2 + \sqrt{-5}} \mid 9, \cancel{2 + \sqrt{-5}} \nmid 3(2 + \sqrt{-5}) \quad \cancel{2 + \sqrt{-5}} \nmid 3,$

$\Rightarrow c = \pm 3(2 + \sqrt{-5})$. 但 $\pm 3(2 + \sqrt{-5}) + 9$. 矛盾!

定义 10

若整环 R 中不存在无穷多元素 a_1, a_2, \dots 使 a_{i+1} 是 a_i 的真因子

$(a_i + a_{i+1}, a_{i+1} \mid a_i)$ 则称 R 满足因子链条件. (e.g. $\mathbb{Z}, F[x]$)

定义 11

① 互素整环 ② R 满足因子链条件且不可约元均为素元

Noether 环: 不存在 R 无限个理想的真升链.

命题 8

PID 是 Noether 环

命题 9

PID 的非零素理想即极大理想. (移为一维的)

命題 10

PID 中 a 不可約 \Leftrightarrow (a) 极大

命題 11

PID 是 UFD

定理 10

ED 是 PID

定理 11

UFD 的多项式环仍为 UFD. (多元也可)

补充:

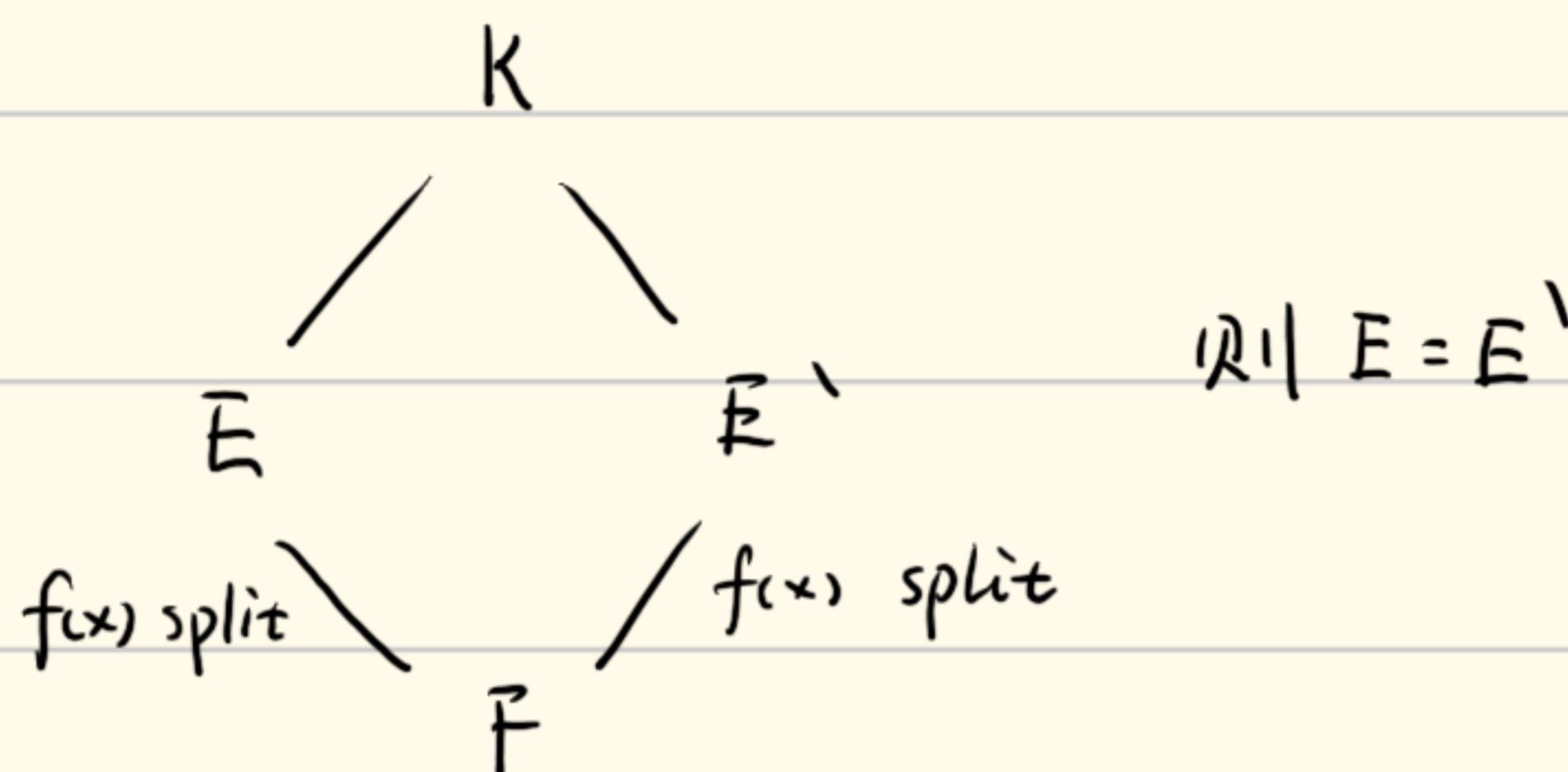
| Integral Domains | 素元 \Rightarrow 不可约元 e.g. $\mathbb{Z}[\sqrt{-5}]$ |
|--|--|
| UFD 唯一分解 素元 \Leftrightarrow 不可约元. e.g. $F[x,y]$ | |
| PID (素元) = 素理想 \Leftrightarrow 极大 理想 = (不可约元) | Dedekind Domain. 素理想 \Leftrightarrow 极大理想 e.g. 所有代数 整数环 $\mathbb{Z}[\sqrt{-5}]$ |
| ED e.g. $\mathbb{Z}[i], F[x]$ | Field. |

域：

引理： E 是 F 的某多项式 $f(x)$ 的分裂域. $K/E/F$ 扩张塔.

则 $\forall \alpha \in \text{Aut}(K)$, 若 $\alpha|_F = \text{id}_F$. 则 $\alpha(E) = E$.

即：



定理：

有限正规扩张 \Leftrightarrow 某个多项式的分裂域.

证：设 $K = F(\alpha_1, \dots, \alpha_r)$, $m_{\alpha_i}(x)$ 是 α_i 的最小多项式.

已经在 K 上有根 α_i . 由正规 $\Rightarrow m_{\alpha_i}(x)$ 在 K 分裂.

$\Rightarrow f(x) = \prod_{i=1}^r m_{\alpha_i}(x)$. K 是 $f(x)$ 在 F 上的分裂域.

取 $p(x)$ 不可约且有一个根 $\alpha \in K$. 以及 β 是 $p(x)$ 另一个根.

$$\begin{array}{ccc} L & \xrightarrow{\cong} & L \\ | & & | \\ \text{splitting field of } p(x) & & \text{splitting field} \\ | & & | \\ K & & \text{of } f(x), p(x) \\ | & & | \\ \text{splitting field of } f(x) & & F(\alpha) \xrightarrow{\cong} F(\beta) \\ | & & | \\ F & & \alpha \mapsto \beta \end{array}$$

由于 $\alpha|_F = \text{id}_F$. 由引理, $\alpha(K) = K$. $F(\beta) = \alpha(F(\alpha))$

$\subset \alpha(K) = K \Rightarrow \beta \in K$. 由 β 任意性知 K 正规.

正规闭包：把 K/F 不完全的根补上，使得全部分裂。

命题： 有限扩张的正规闭包一定存在且唯一。
无限也正确。

存在性： $K = F(\alpha_1, \dots, \alpha_r)$ $f(x) = \prod_{i=1}^r m_{\alpha_i}(x)$.

设 L 是分裂域 of $f(x)$ over F .

唯一性： L 正规 $\Rightarrow f(x)$ 在 L 分裂。这样最小的 L

就是 splitting field of f over F

* $\text{Char}(F)=0$ 或 $\#F < \infty \Rightarrow$ 不可约多项式都是可分离多项式。

当 $\text{Char}(F)=p$ 且 $\#F$ 无穷时的反例：

The splitting field of $x^p - t$ over $\bar{F}_p(t) = \bar{F}_p(t^{1/p})$

$$\text{But } x^p - t = (x - t^{1/p})^p$$

Perfect field: Field with $\text{char}(F)=p$ whose

Frobenius endomorphism is automorphism

Ex. for imperfect field: $\bar{F}_p(t)$. $\Delta(\bar{F}_p(t)) = \bar{F}_p(t^p)$

perfect fields: $\bar{F}_p(t, t^{1/p}, t^{1/p^2}, \dots)$

定理：perfect field 的代数扩张仍是 perfect field.

Remark: $F^{\text{perf}} = \bigcup_n \alpha^{-n}(F)$. defined to be F 's perfection.

F perfect $\Leftrightarrow F = F^{\text{perf}}$.

the perfection of $\overline{F_p}(t)$ is just $\overline{F_p}(t, t^{p}, \dots)$

设 F 是一个域. $f(x) \in F[x]$, α 是 $f(x)$ 的 $k \geq 1$ 重根.

(1) $\text{Char}(F) \nmid k$ 时. α 是 $f'(x)$ 的 $k-1$ 重根.

(2) $\text{Char}(F) \mid k$ 时. α 至少是 $f'(x)$ 的 k 重根.

证明

假设 F 是一个域, $f(x) \in F[x]$ 有重根 $\Leftrightarrow \gcd(f(x), f'(x)) \neq 1$

引理

设 $\text{Char}(F) = p$. $a \in F$. $x^p - a$ 要么不可约. 要么

完全裂为 $(x-b)^p$, $b \in F$

Pf: 记 $b = a^{p^n}$. 考虑 $E = F(b)$,

• 若 $b \in F \Rightarrow$ 分裂

• 若 $b \notin F$, 则 $x^p - a = (x-b)^p \in E[x]$. 反证 $x^p - a$ 可约

即 $f(x)g(x) = x^p - a \Rightarrow \exists 1 \leq m < p. f(x) = (x-b)^m \in F[x]$

$m \leq p \nmid \frac{p}{m} \Rightarrow \exists u, v \in \mathbb{Z}, mu + pv = 1$

$\Rightarrow (x-b) = (x-b)^{mu+pv} = (f(x))^u (x^p - a)^v \in F[x]$

$\Rightarrow b \in F$. 矛盾! $\Rightarrow x^p - a$ 不可约

$$G_1 \subseteq G_2 \Rightarrow \text{Inv}(G_1) \supseteq \text{Inv}(G_2)$$

$$F_1 \subseteq F_2 \Rightarrow \text{Gal}(G/F_1) \supseteq \text{Gal}(G/F_2)$$

例 1 (a) $K = \mathbb{Q}(\sqrt[3]{2})$, 则 $\text{Gal}(K/\mathbb{Q}) = \{\text{id}\}$, $\text{Inv}(\{\text{id}\}) = K$.

(b) $E = \mathbb{Q}(\sqrt[3]{2}, \zeta_3)$. 则 $\text{Gal}(E/\mathbb{Q}) \cong D_3 \cong \langle \sigma, \tau \mid \sigma^3 = 1, \tau^2 = 1 \rangle$

$$\sigma(\sqrt[3]{2}) = \zeta_3 \cdot \sqrt[3]{2}, \quad \sigma(\zeta_3) = \zeta_3$$

$$\tau(\sqrt[3]{2}) = \sqrt[3]{2} \quad \tau(\zeta_3) = \zeta_3^2$$

$$\text{Inv}(\langle \sigma \rangle) = \mathbb{Q}[\zeta_3], \quad \text{Inv}(\langle \tau \rangle) = \mathbb{Q}(\zeta_3)$$

以下命题等价：

(i) K/F 是 Galois 扩张

(ii) K/F 是 可分 正规 扩张

$$(iii) |\text{Gal}(K/F)| = [K:F]$$

定理 16 (Artin 定理)

设 H 是 E 的有限自同构群, $L = \text{Inv}(H)$. 则 $[E:L] \leq |H|$

pf: 设 $H = \{\sigma_1, \dots, \sigma_n\}$, $u_1, \dots, u_{n+1} \in E$. 我们证明它们在 F 上

是 L -线性相关的. 全 $\cup = (v_1, \dots, v_{n+1}) = \begin{pmatrix} \sigma_1(u_1) & \cdots & \sigma_1(u_{n+1}) \\ \vdots & & \vdots \\ \sigma_n(u_1) & \cdots & \sigma_n(u_{n+1}) \end{pmatrix}$

不妨在 E 上 v_1, \dots, v_r 线性无关. $r \leq n$. $v_{r+1} = a_1v_1 + \cdots + a_r v_r$.

则 $\forall \alpha \in H, \alpha \{a_1, \dots, a_n\} = \{a_1, \dots, a_n\}$

从而 $\alpha(v_i)$ 是各分量的重排， $\Rightarrow v_{r+1} = \alpha(a_1)v_1 + \dots + \alpha(a_r)v_r$

由 v_1, \dots, v_r 线性无关 $\Rightarrow \alpha(a_i) = i, 1 \leq i \leq r$.

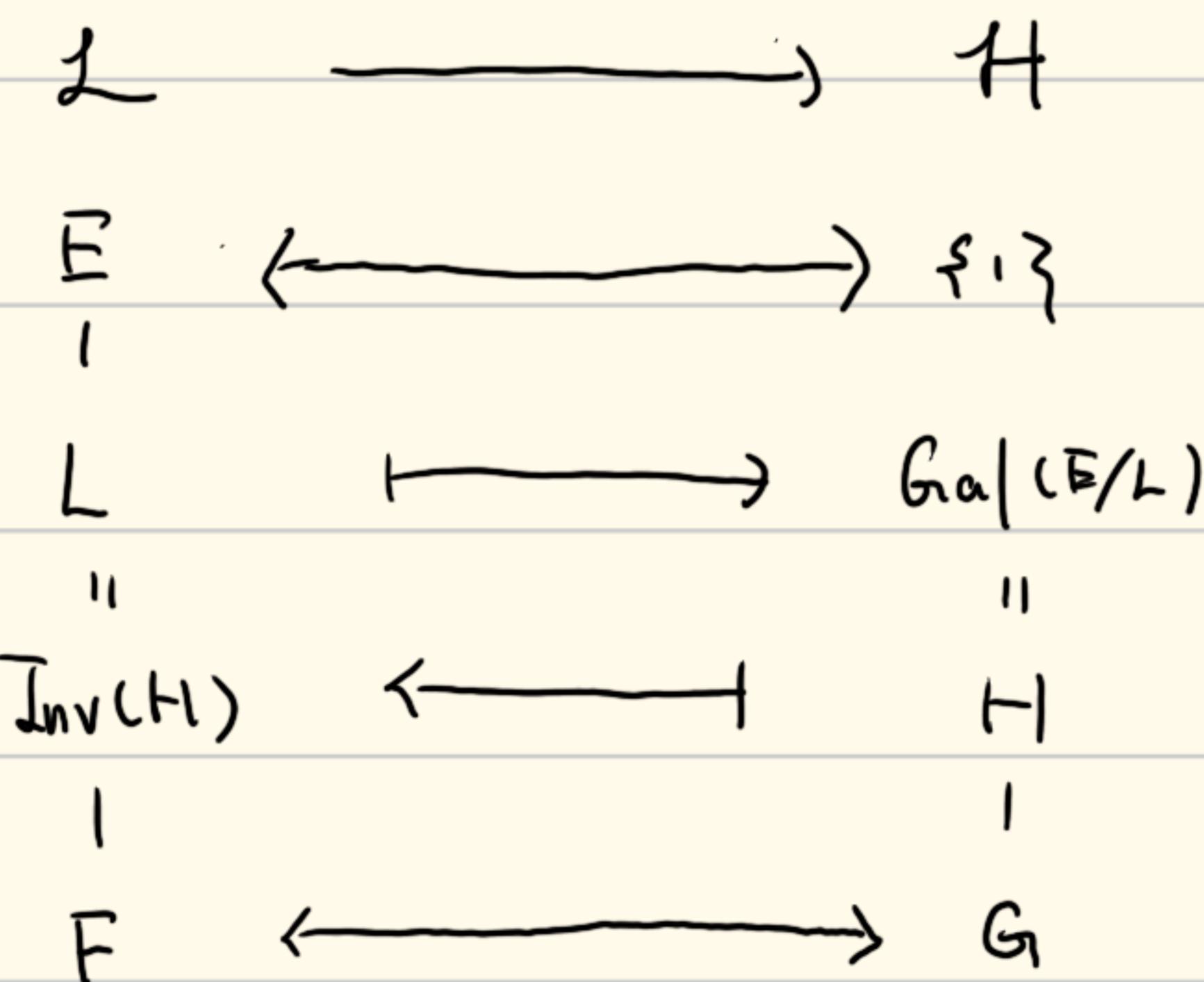
则可证明 $a_i \in L, 1 \leq i \leq n$ 从而 v_1, \dots, v_{n+1} 在 L 上线性相关.

Galois 基本定理 (定理 1)

E/F 是有限 Galois 扩张 (分裂域且可分) $G = \text{Gal}(E/F)$

$$\mathcal{H} = \{\text{G 的子群}\} \quad \mathcal{L} = \{\text{E/F 的中间域}\}$$

(1) $L \mapsto \text{Gal}(E/L), H \mapsto \text{Inv}(H)$ 是双射. E/L Galois



(2) $H_1 \subset H_2 \Leftrightarrow \text{Inv}(H_1) \supset \text{Inv}(H_2)$

(3) $[E:L] = |\text{Gal}(E/L)|, [L:F] = [G:\text{Gal}(E/L)]$

(4) 若 $H \leftrightarrow L$. 则 $\alpha H \alpha^{-1} \leftrightarrow \alpha(L)$

(5) 正规子群 $H \longleftrightarrow F$ 的正规扩张 L . 且 L/F 是 Galois 扩张.

且 $G/H \cong \text{Gal}(L/F)$

\Rightarrow 扩张复合的存在性定理：

设 E/F 正规， K/F 任意，则存在 L/F ，

F -嵌入 $\alpha: E \rightarrow L$.

F -嵌入 $\tau: K \rightarrow L$

使 $L = \alpha(E) \cdot \tau(K)$ 这种合成 L 由 E 与 K 唯一决定.

称为 E 与 K 的复合，记为 EK .

定理 19:

E 是 F 的 Galois 扩张， K 是 F 的任意扩张，则

EK 是 K 的 Galois 扩张且 $\text{Gal}(EK/K) \cong \text{Gal}(E/K \cap E)$

pf: 考虑 $\varphi: \text{Gal}(EK/K) \longrightarrow \text{Gal}(E/K \cap E)$

$$\alpha \longmapsto \alpha|_E$$

由 E/F 正规知 $\alpha(E) = E$. 定义合法,

则 $\ker \varphi = \{\alpha \mid \alpha|_K = \text{id}, \alpha|_E = \text{id}\} = \{\text{id}|_{EK}\}$ 单射

设 $\text{im } \varphi = H$. 考察 $E^H = \{a \in E \mid \alpha(a) = a, \forall \alpha \in H\}$

$$= \{a \in E \mid \alpha(a) = a, \forall \alpha \in \text{Gal}(EK/K)\} = K \cap E.$$

$$\Rightarrow H = \text{Gal}(E/K \cap E)$$

Galois 定理证明:

设 K/F 是 Galois 扩张, $G = \text{Gal}(K/F)$.

(1) 子群与中间域的一一对应.

证: (a) 设 $H \leq G$, 对应到 K^H 是中间域.

有 $K/E/F$, 对应到 $\text{Gal}(K/E) \leq G$

只需证 $H = \text{Gal}(K/E)$

事实上由 K/F Galois 知 K/E Galois. 由

$$[K:E] = \#\text{Gal}(K/E)$$

由 Artin, $|H| \geq [K:E]$, 故 $|H| \geq \#\text{Gal}(K/E)$

而 $\forall \alpha \in H$, $\alpha|_E = \text{id}_E$. $\Rightarrow \alpha \in \text{Gal}(K/E)$

$$\Rightarrow H \subseteq \text{Gal}(K/E) \Rightarrow H = \text{Gal}(K/E)$$

(b) 设中间域 E , 对应到 $\text{Gal}(K/E) := H$

$H \leq G$, 对应到 K^H .

只需证 $E = K^H$

• $\forall \alpha \in E$. $\alpha \in H$, $\alpha(\alpha) = \alpha$, 故 $E \subseteq K^H$

• 由于 K 是 K^H 有限可分扩张 $\Rightarrow \exists \alpha \in K$. $K = K^H(\alpha)$

$$\Rightarrow [K : K^H] = \deg \text{Min}_{\alpha, K^H}(x)$$

而 $\prod_{h \in H} (x - h(\alpha)) := f(x)$ 在 H 作用下不动

$$\Rightarrow f(x) \in K^H[x]. \text{ 且 } f(\alpha) = 0$$

$$\Rightarrow [K : K^H] = \deg \text{Min}_{\alpha, K^H}(x) \leq \deg f = |H|$$

Artin
引理
在可分
情况的
证明

从而 $[K:E] = |\text{Gal}(K/E)|$ 由 K/E 可分

$$|\text{Gal}(K/E)| = |H| \stackrel{(a)}{=} |\text{Gal}(K/K^H)| \Rightarrow K^H = E.$$

重要观察: $[K:F] = |\text{Hom}_F(K,L)| = |\text{Hom}_F(K,K)| = |\text{Gal}(K/F)|$

$$\begin{array}{ccc} \downarrow & \downarrow & \downarrow \\ \text{可分} & \text{正规} & \text{定义} \end{array}$$

定理

设 K/F 是有限扩张. 以下命题等价

- (1) K/F 是 Galois 扩张, 即 K/F 可分且正规
- (2) K 是 $f(x)$ 在 F 的分裂域. 其中 $f(x) \in F[x]$ 是可分离多项式
- (3) $|\text{Gal}(K/F)| \geq [K:F]$
- (4) F 是 H 在 K 上的不动域. 其中 $H \leq \text{Aut}(K)$

定义:

可分多项式在 \mathbb{F} 上的分裂域又称为其 Galois 域

多项式 $x^n - 1$ 在 \mathbb{Q} 上的 Galois 域 称为 n 次单位圆域.

显然 $E = \mathbb{Q}(\zeta)$, ζ 是本原 n 次单位根.

定理 2.0

本原 n 次单位根的极小多项式 (第 n 个分圆多项式)

$$\Phi_n(x) = \prod_{i \in \mathbb{Z}_n^\times} (x - \zeta^i), \quad \zeta = e^{\frac{2\pi i}{n}}$$

pf: 只需证: 设 $f(x)$ 是 ζ 的极小多项式 $(p, n) = 1$. P 整数

我们证 ζ^p 也是 $f(x)$ 的根.

若不然. 设 ζ^p 极小多项式为 $g(x)$, 由 $f \neq g \Rightarrow \exists$ 矛盾.

从而 $f(x) | \Phi_n(x)$, $g(x) | \Phi_n(x) \Rightarrow f(x)g(x) | \Phi_n(x)$

$g(\zeta^p) = 0 \Rightarrow \zeta^p$ 是 $g(x^p)$ 的根. $\Rightarrow f(x) | g(x^p) = f(x)h(x)$

在 \mathbb{F}_p 中考虑: $\bar{g}(x)^p = \bar{g}(x^p) = \bar{f}(x)\bar{h}(x)$

$\Rightarrow \bar{g}(x)$ 与 $\bar{f}(x)$ 不互素 $\Rightarrow x^n - 1$ 在 \mathbb{F}_p 有重根.

但 $(x^n - 1, D(x^n - 1)) = (x^n - 1, n) \stackrel{(p, n)=1}{=} 1$, 矛盾!

定理 2.1

$$\text{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \cong \mathbb{Z}_n^\times$$

推论:

$\text{Char } F = 0$ (以 \mathbb{Q} 为子域), 正是 $x^n - 1$ 在 F 的分裂域.

则 $\text{Gal}(E/F) \leq \mathbb{Z}_n^\times$, 因而 E/F 是阿贝尔扩张

定义:

若 Galois 扩张 E/F 是阿贝尔扩张, 且 for some n ,

$\exp(\text{Gal}(E/F)) \mid n$ 且 F 中包含 n 个 n 次单位根.

则称这种扩张为 Kummer 扩张.

定理 22

设正是 $x^n - a \in F[x]$ 在 F 的分裂域, F 中包含 n 个 n 次单位根

则 $G = \text{Gal}(E/F)$ 是循环群 (称为循环扩张), 且 $|G| \mid n$.

G 是 n 阶循环群 $\Leftrightarrow x^n - a$ 不可约.

推论

设 p 素. F 含 $p+1$ 次单位根. E 是 $x^p - a \in F[x]$ 在 F 的分裂域

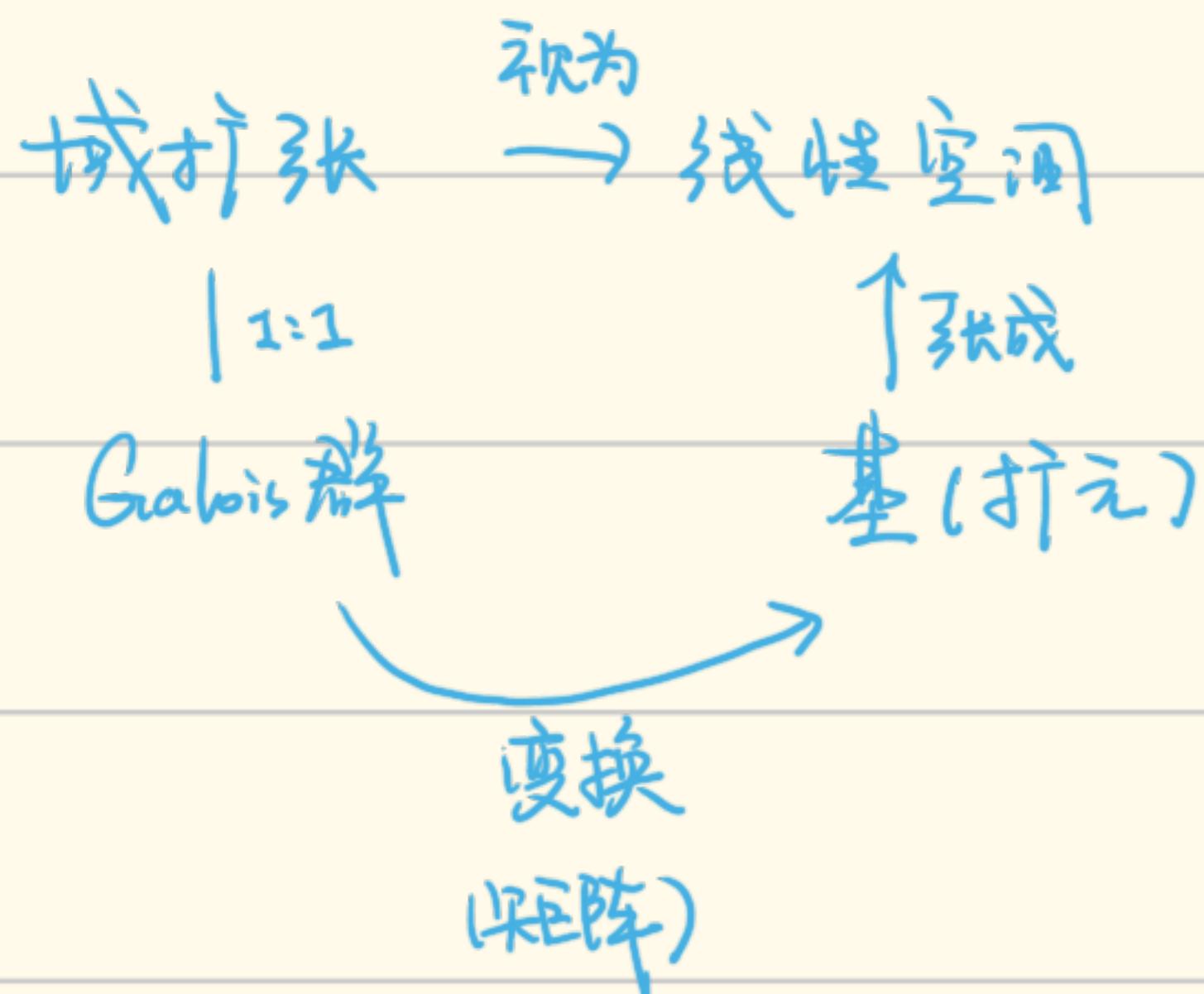
则 $x^p - a$ 在 F 上要么不可约, 要么完全分裂. ($G = \mathbb{Z}/p\mathbb{Z}$ on \mathbb{Z}_p)

定理 23

$\text{char}(F) \neq p$
保证特征为质数分裂!

设 p 是素数, F 中包含 p 个 p 次单位根. E/F 是某个 p 次 Galois

扩张. 则 E 是 $x^p - a \in F[x]$ 在 F 上的分裂域 for some a .



pf: 视 α 为 E/F 的线性空间的线性变换, α 特征值 λ 均为

$x^p - 1$ 的根, 若特征值均为 1 $\Rightarrow \text{Char } \alpha = (x-1)^p = 0$.

又 $\text{Min}_\alpha | x^p - 1 \Rightarrow \text{Min}_\alpha = (x-1) \text{ id. 矛盾!}$

故存在 α 某特征值 $\lambda \neq 1$. 再设 α 是 λ 对应的特征向量

则 $\alpha(\alpha) = \lambda \alpha$. 令 $a = \alpha^p$. 则 $\alpha(a) = a$.

从而 $a \in F$. $E = F[\alpha]$

定义:

若存在域的扩张系列:

$$F = F_0 \subset F_1 \subset \dots \subset F_r = K$$

$$F_i = F_{i-1}[\alpha_i], \quad \alpha_i^{n_i} = \alpha_{i-1} \in F_{i-1}, \quad i=1, 2, \dots, r,$$

则称 K/F 是一个 根扩张, 若 $f(x) \in F[x]$ 在 F 上的分

裂域包含于 F 的某个根扩张中, 则称 $f(x)$ 是 根式

可解的.

定理 24 (Galois 定理)

设 $\text{Char}(F) = 0$, $f(x) \in F[x]$, E 是 $f(x)$ 在 F 上的分
裂域. 则 $f(x) = 0$ 根式可解 $\Leftrightarrow \text{Gal}(E/F)$ 是可解群.

3|理 1

设 $\text{Char}(F) = 0$. $f(x) \in F[x]$, E 是 $f(x)$ 在 F 的分裂域,

对 $|\text{Gal}(E/F)|$ 的每个素因子 p , F 中包含 p 个 p 次单位根.

$\text{Gal}(E/F)$ 可解 则 $f(x) = 0$ 是根式可解的.

pf: 对可解群 $H = \text{Gal}(E/F)$, 我们有合成群列:

$$H = H_0 \triangleleft H_1 \triangleleft \dots \triangleleft H_r = \{1\}$$

假设对应的不动域的扩张序列为:

$$F = F_0 \subseteq F_1 \subseteq \dots \subseteq F_r = E$$

则 F_i/F_{i-1} 是素数次扩张, 满足定理 23 条件.

从而 $F_i = F_{i-1}[\alpha_i]$ 且 $\alpha_i^{n_i} = \alpha_{i-1} \in F_{i-1}$, $i=1, 2, \dots, r$

故 $f(x)$ 是根式可解的.

3|理 2

设 $\text{Char}(F) = 0$, 从 F 到 F_r 有以下扩张序列

$$F = F_0 \subset F_1 \subset F_2 \subset \dots \subset F_r$$

$F_i = F_{i-1}[\alpha_i]$ 且 $\alpha_i^{n_i} = \alpha_{i-1} \in F_{i-1}$, $i=1, 2, \dots, r$

设 K 是 F/F 的正规闭包， p_1, \dots, p_s 是 n_1, \dots, n_r 中全部素因子。 F 包含 p_1, \dots, p_s 次的本原单位根： ζ_1, \dots, ζ_s ，则 $Gal(K/F)$ 可解。

Theorem (Kronecker-Weber)

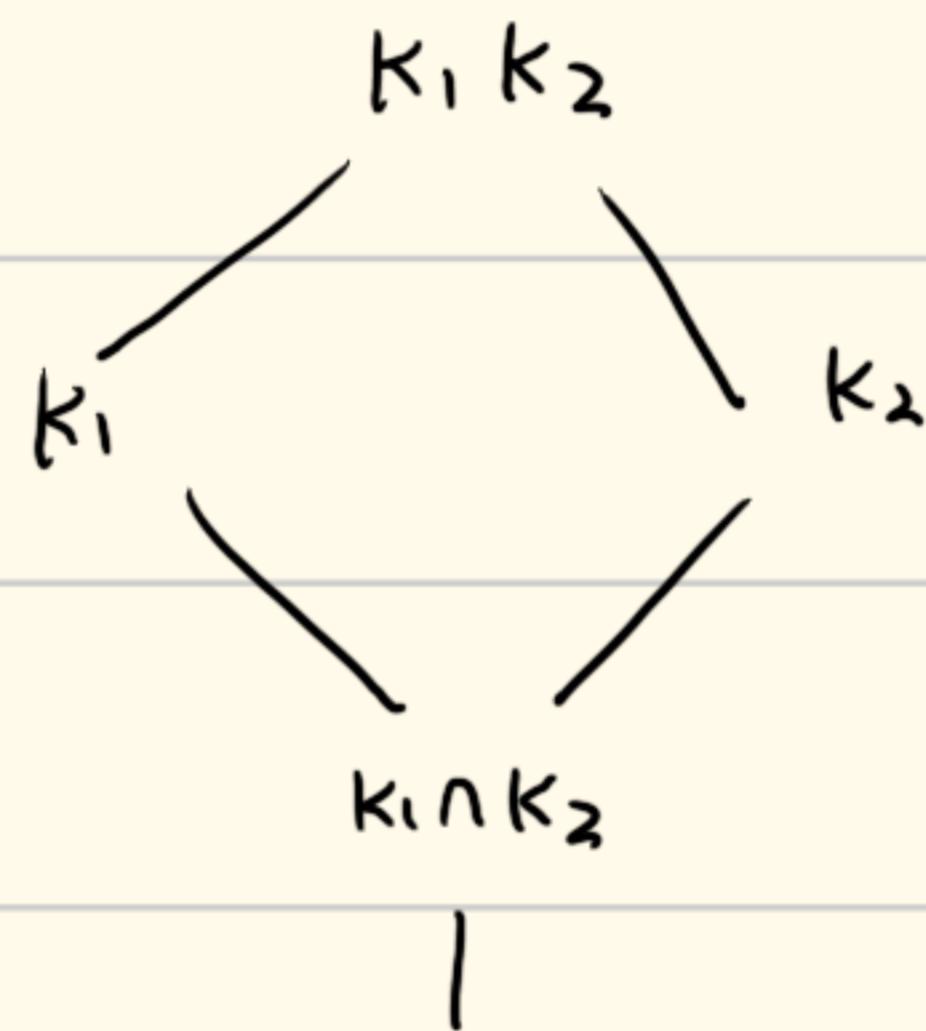
Every finite abelian extension K of \mathbb{Q} is contained in some $\mathbb{Q}(\zeta_n)$

Proposition

suppose that we have

(K_1 and K_2 are Galois over F)

Then we have:



(i) $K_1 \cap K_2$ is Galois over F

F

(ii) $K_1 K_2$ is Galois over F and

$$Gal(K_1 K_2 / F) = \{(g_1, g_2) \in Gal(K_1 / F) \times Gal(K_2 / F) \mid g_1|_{K_1 \cap K_2} = g_2|_{K_1 \cap K_2}\}$$

In particular, if $K_1 \cap K_2 = F$, we have

$$Gal(K_1 K_2 / F) = Gal(K_1 / F) \times Gal(K_2 / F)$$

- 有限可分扩张必为单扩张。而 $Char=0$ 的域上的不可约多项式均为可分多项式 \Rightarrow $Char=0$ 的域的有限扩张必为单扩张。
(或有限域)

命題

(1) $\text{Char}(F) = 0$. 則 F 上不可約多項式 $f(x)$ 一定可分.

(2) F 有限. 則 F 上不可約多項式 $f(x)$ 一定可分.

Pf of (1): 因 $f(x)$ 不可約 $\Rightarrow \deg f > 1 \Rightarrow f'(x) \neq 0$.

又 $\deg f' < \deg f$. $\Rightarrow (f, f') = 1 \Rightarrow$ 无重根.

Pf of (2): 若 f 不可分 $\Rightarrow (f, f') > 1$. $\Rightarrow f' = 0$.

$\Rightarrow \exists g \in F[x]$ 使 $g(x^p) = f(x)$, 設 $g(x) = \sum_{m \geq 0} a_m x^m$

設 $F = G_F(p^n)$. 則 F 中元素均為 $x^{p^n} - x = 0$ 的根.

$$\begin{aligned} \text{設 } f(x) &= \sum_{m \geq 0} a_m x^{mp} = \sum_{m \geq 0} a_m^{p^n} x^{mp} \\ &= \left(\sum_{m \geq 0} a_m^{p^{n-1}} x^m \right)^p \quad \text{可約. 矛盾! 故 } f \text{ 不可分} \end{aligned}$$

命題: K/F 是有限扩张. M 是包含 K 的 F 的正规扩张

則 $\#\text{Hom}_F(K, M) \leq [K:F]$. 等號成立當且僅當 K/F 正規

單扩张時: $\#\text{Hom}_F(F(\alpha), M) \leq [F(\alpha):F] = \deg f$.

若 f 不可分. 則 $\text{Char} F = p$. 且 $\exists e$ 使 $f(x) = g(x^{p^e})$

且 g 可分, 此時 $\#\text{Hom}_F(F(\alpha), M) = \underbrace{\deg g}_{\frac{1}{p^e}} = \frac{1}{p^e} \deg f$

具體給出了 $\text{Hom}_F(K, M)$ 所有情況.

不动域 $\text{Inv}(G)$ 至少包含素域