

46. 4.2

域扩张 · 同态 $\theta: k \hookrightarrow K$
 记号 K/k 

注. 1) $k \hookrightarrow \theta(k) \subseteq K$
 常等同 $x \in k \xrightarrow{\text{常等同}} \theta(x) \in K$.

(2) K 成为 k -线性空间. 依赖于 θ
 $\lambda, v = \theta(\lambda), v \in K$

$\dim_k K = [K:k]$ "没有"

例 1) $f(x) \in k[x]$ 有一不可约 $\deg f \geq 2$

$(f_m) \in \text{Max}(k[x])$

$k = k[x]/(f_m)$ 

$k \hookrightarrow \bar{k}$ (记为 \bar{x})

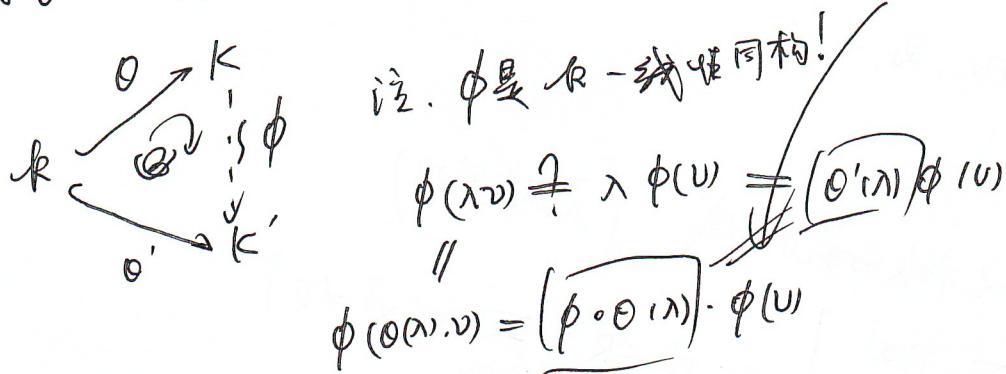
| 已证 $\dim_{\bar{k}} K = d$
 | 有 \bar{k} -基 $\{1, u, \dots, u^{d-1}\}$.
 | 2. 根构造 $u = x + (f_m)$
 | $u \in \text{Root}_k(f_m)$

(2) $k[x]$ $\text{Frac}(k[x]) := k(x)$ 一元有理函数域

$k[x]$ 有理的表达.
 $\cong \text{UFD}$ $\frac{f(x)}{g(x)} : \begin{cases} f(x) \neq 0 \\ g(x) \neq 0 \end{cases}$
 $f, g \in k[x]$.

$k \hookrightarrow k(x)$
 $x \mapsto \frac{1}{x}$ (记为 \bar{x})
 $k(x)$ 无序域 $\left\{ \frac{1}{1}, \frac{x}{1}, \dots \right\}$ k -线性无关

$\theta: k \rightarrow K$
 $\theta': k \hookrightarrow K'$
 指 θ 与 θ' 同构者 且 域同构 $\phi: K \rightarrow K'$ s.t. $\boxed{\phi \circ \theta = \theta'}$



例 (环论3) $K = k(t)$ 是分离 θ

$$\theta_1: K \hookrightarrow K$$

$$\frac{f_1(t)}{g_1(t)} \mapsto \frac{f_1(t^n)}{g_1(t^n)}$$

$$\theta_2: K \hookrightarrow K$$

$$\frac{f_2(t)}{g_2(t)} \mapsto \frac{f_2(t^m)}{g_2(t^m)}$$

[EX] θ_1, θ_2 不同构

定义 $\theta: k \hookrightarrow K$ 的 同构

指 $\varphi: K \hookrightarrow K$ s.t. $\varphi \circ \theta = \theta'$

$\text{Aut}(K)$ K 的 自同构群

$$\text{Aut}(\theta) = \text{Aut}(K/k) = \{ \varphi \in \text{Aut}(K) : \varphi \circ \theta = \theta' \}$$

K/k 的 自同构群 我们要计算的对象!

记号 $R \subseteq S$ 且 R

$\overline{R[x]}$ 包含 R 和 x 的 最小 $\exists R$.

$$\overline{R[x]} = \left\{ \sum_{\text{finite}} r_i x^i \mid r_i \in R \right\}$$

不带多项式项

$$R[x] \longrightarrow \overline{R[x]}$$

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

例 $\mathbb{Z}[x]$

48. 令 $\Omega = R \hookrightarrow S$ 为嵌入
 $R[\alpha] = \Omega(R)[\alpha]$.

类似地, 定义 $R[\alpha_1, \alpha_2, \dots]$

域 $K \subseteq \mathbb{C}$
 $k(\alpha) = \text{包含 } \alpha \text{ 和 } K \text{ 的最小子域} \quad (\text{不加长})$

$$= \left\{ \frac{\sum_{\text{finite}} r_i \alpha^i}{\sum_{\text{finite}} r_j' \alpha^j} \mid r_i, r_j' \in R, \sum_{\text{finite}} r_j' \alpha^j \neq 0 \right\}$$

$k(\alpha)$ 与 $k(x)$ 不完全相等!

(3) $\Omega \subseteq \mathbb{C}$

(a)(i)

$\alpha, \beta \in K$.

$\Omega \hookrightarrow K$

都是代数.

$\Phi, k(\alpha, \beta)$

$k(\alpha)\Phi = \Omega(k)(\alpha)$.

设 K/Ω 为基 焦点 $\exists \alpha \in K$. s.t. $K = k(\alpha)$, α 为生成元

i.e. α 不一意惟一

13. (1) 该根式是单标系

$K = k(u) = \Omega[u]$

(2) $\Omega \hookrightarrow k(x)$ 元素是 x . ($x+1, \dots$ 也对)

$\Omega \hookrightarrow k[x] \not\cong k(x)$.

(3) $\Omega \subsetneqq \Omega^{(1)}$

$\Omega \not\cong \mathbb{C}$

单形论与代数的性质决定

定理 K/k $\alpha \in K$.
 α 为 k 上的代数元. 若 $\exists f(x) \in k[x]$, $\alpha \in \text{Root}_K(f(x))$ /
 $f(\alpha) = 0_K$.

$(f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \in k)$
 $f(\alpha) = 0_K \alpha^n + 0(a_{n-1}) \alpha^{n-1} + \dots + 0(a_0) = 0_K$.

若 $\alpha \in O(k)$ α 为 k 上代数. 取 $f(x) = x - \alpha$

例 $\mathbb{Q} \subseteq \mathbb{C}$

$$x^2 \in \mathbb{Q}[x].$$

否则 α 为 k 上超越元. 例 π, e 是 \mathbb{Q} 上超越元

$$\text{例 } k \hookrightarrow k[x]/(f_m) = k$$

u 为 k 上代数. $u = \bar{x}$

$\forall z \in k. \{z, z^2, \dots, z^d\} \subset k$ - 线性无关.

例 $k \hookrightarrow k[\frac{t}{u}]$
为 k 上超越元 (字母...)

例 $\forall f(\frac{t}{u}) \in k(\frac{t}{u}) \setminus k$ 为 k 上超越

证明. $K/k. \alpha \in K$. k 上代数. 则 $\exists! f - \text{元} \in f(x) \in k[x]$.

即 $f(\alpha) = 0_K$ $f(x)$ 为 α 的最小多项式.

proof $\text{ev}_\alpha: k[x] \longrightarrow K$
 $g(x) \longmapsto g(\alpha)$

$$\text{ker}(\text{ev}_\alpha) = (f(x))$$

α 为
代数

$k[x]/(f(x)) \hookrightarrow K$.

整环

不可约

唯一性

□

例 $\mathbb{Q} \subseteq \mathbb{C}$

$$\sqrt{2} \rightsquigarrow x^2 - 2$$

$$\sqrt{3} \rightsquigarrow x^2 - 3$$

$$\omega \rightsquigarrow \text{min } x^2 + x + 1 = 0$$

$\sqrt{2} + \sqrt{3} \in \mathbb{Q}(\alpha)$
 $\sqrt{2} + \omega \in \mathbb{Q}(\alpha)$

$$\left| \begin{array}{l} \text{min } \alpha = \sqrt{2} + \sqrt{3} \\ (\alpha - \sqrt{2})^2 = 3 \\ \alpha^2 - 1 = 2\sqrt{2}\alpha \end{array} \right.$$

最小多项式要插用. 如 $\sqrt[4]{2}$. 在 $\mathbb{Q}(\sqrt{2})$ 中 $\sqrt[4]{2} \in \mathbb{Q}(\sqrt{2})$ 且 $x^4 - 2$.

单扩张的结构定理.

设 K/k , $\alpha \in K$ s.t. $K = k(\alpha)$

i) α 代数 最少项式 $f(x) \in k[x]$ $\deg f = d \geq 1$

且 $\dim_k K = d$. K 有 k -基 $1, \alpha, \dots, \alpha^{d-1}$.

且 $\underline{k[\alpha]} = K$

扩张: $k \xrightarrow{\alpha} k/(f(x))$

ii) α 超越 $\dim_k K = \infty$

$k[\alpha] \nsubseteq k$

k/α 同构于 $k \hookrightarrow k(x)$

k/α

proof ii) $\alpha: k(x) \rightarrow k$
 $g(x) \mapsto g(\alpha)$
 $x \mapsto \alpha$
 $\lambda \mapsto \alpha(\lambda)$

$(k(x)/f(x)) \xrightarrow{\alpha} K$
 $\text{域 } k(x) \text{ 含 } k, \alpha.$

$\Rightarrow k(x)/f(x) \hookrightarrow K$

$\ker(\alpha) = (f(x))$
 $\frac{k[x]}{(f(x))}$

$u = \bar{x} \xrightarrow{\alpha} \alpha$
 域扩张同构
 $\bar{x} \in \bar{k}$

(2) 超域: env_α is injective

$$\Rightarrow \mathbb{R}[x] \hookrightarrow K$$

so $\mathbb{R}[x] \hookrightarrow K$

$\boxed{\text{Ex}}$ $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ $x^3 - 2$

证: $\mathbb{Q}(\sqrt[3]{2})$ 有 \mathbb{Q} -基 $\{1, \sqrt[3]{2}, \sqrt[3]{4}\}$. (这是易证的)

$\boxed{\text{Ex}}$ w $\sqrt[3]{w}$ 的最小多项式也是 $x^3 - 2$

证 $\mathbb{Q}(\sqrt[3]{w})/\mathbb{Q}$ 同构于 $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ 但作为 \mathbb{Q} -向量空间 (一维-维数不同)

(困难在于不讨论商环...)

代数扩域

$\boxed{\text{定义}}$ K/k 是一个代数扩域, 若 $\forall \alpha \in K$, $\exists \text{在 } k \text{ 上可整除}$

证 $k \xrightarrow{f, d} k(\alpha) \subseteq K$

$\boxed{\text{引理}}$ 若 $\dim_K k < \infty$, 则 K/k 一定代数

prof: $\alpha \in K$ $k \hookrightarrow \frac{k}{k(\alpha)} \subseteq K$
 k -线性子空间 $\subseteq k$
 $\Rightarrow \alpha$ 是代数的. \square

$\boxed{\text{定理}}$ (维数公式) $k \leq E \subseteq K$ $\frac{E}{k}$ 为域

若 $k \hookrightarrow E/E$ & K/E 为有限维

$\Rightarrow K/k$ 也是有限维的. $\dim_K K = \dim_E E \cdot \dim_{E/K} K$
 E -线性

Compare with Lagrange theorem

52. 证. E/\mathbb{Q} 有基底, E 有长基 $\{u_1, \dots, u_{mn}\}$

K/E K 有基 $\{v_1, \dots, v_m\}$

Claim K 的长基是 $\{u_i v_j \mid i=1 \dots n, j=1 \dots m\}$

Ex

例 $\mathbb{Q}(\sqrt{2}, \sqrt{3}) \subseteq \mathbb{C}$

$\dim_{\mathbb{Q}} K = ?$

$$\begin{array}{c} \mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt{2})(\sqrt{3}) \subseteq \mathbb{C} \\ \curvearrowright \quad \curvearrowright \quad \curvearrowright \quad K \\ \text{单} \quad \text{单} \end{array}$$

$$\dim_{\mathbb{Q}} \mathbb{Q}(\sqrt{2}) = 2$$

$$x^2 - 2.$$

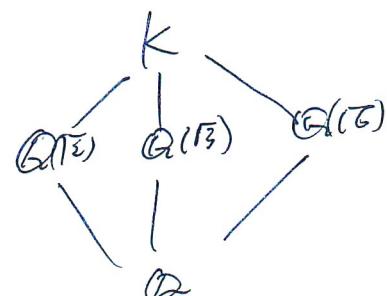
$$\dim_{\mathbb{Q}} \mathbb{Q}(\sqrt{3}) = 2. \Rightarrow \dim_{\mathbb{Q}} K = 4.$$

要 $\sqrt{3}$ 在 $\mathbb{Q}(\sqrt{2})$ 上的最小多项式?

要 $\sqrt{3}$ 在 $\mathbb{Q}(\sqrt{2})$ 上是否不可约?

$$\Leftrightarrow x^2 - \sqrt{3} \text{ 在 } \mathbb{Q}(\sqrt{2}) \text{ 上是否不可约?} \quad \text{假设 } a + b\sqrt{2} = \sqrt{3} \text{ 草稿平方!}$$

$$\Leftrightarrow \pm \sqrt{3} \notin E$$



Rank: 维数被维数公式控制

例. $K = \mathbb{Q}(\sqrt[3]{2}, \omega)$

$$\dim_{\mathbb{Q}} K = ?$$

$$\left\{ \begin{array}{l} \mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{Q}(\sqrt[3]{2})(\omega) \\ \mathbb{Q} \subseteq \mathbb{Q}(\omega) \subseteq \mathbb{Q}(\sqrt[3]{2}, \omega). \end{array} \right. \quad \text{都错}$$

这个错误.

$$\text{记 } E = \mathbb{Q}(\sqrt[3]{2}).$$

E 有 \mathbb{Q} 基 $\{1, \sqrt[3]{2}, \sqrt[3]{4}\}$

E 在 \mathbb{Q} 上的最小多项式?

$$x^3 + x + 1 = 0 \text{ 在 } E \text{ 上可约吗?}$$

$$x^3 + x + 1 = 0 \in E[x]$$

$$= a + b\sqrt[3]{2} + c\sqrt[3]{4} \in \mathbb{Q}[x]$$

$$\Rightarrow x^3 + x + 1 \text{ 不可约!} \Rightarrow \dim_{\mathbb{Q}} K = 6.$$

所以不要过早引入 ω .

在 E 上的最小多项式 $f(x)$

Ex

$$K/\mathbb{Q} \quad f.d. \quad x \in K \quad \text{且在 } E \text{ 上的最小多项式 } f(x)$$

$$\deg f(x) \mid \dim_{\mathbb{Q}} K$$

书 P11 1, 4, 7, 10, 11

圖和 k/k 有很 ~~緊密~~
~~關係~~

$$K = k(\alpha, \dots, \alpha_n)$$

$$k \subseteq k(\alpha_1) \subseteq k(\alpha_1, \alpha_2) \subseteq \dots \subseteq K.$$

Fact k/k f.d. \Leftrightarrow k/k 代數且 k/k 純域

proof (\Rightarrow)

(\Leftarrow) 一步一步做.

Fact $k \subseteq E \subseteq K$
則 k/k 代數 $\Leftrightarrow k/E$ 代數且 E/k 代數

(\Rightarrow) 容易.

(\Leftarrow) α 在 E 上代數 $\frac{\text{fix } \alpha \in E}$

$$\alpha^n + u_{n-1} \alpha^{n-1} + \dots + u_0 = 0 \quad u_i \in E$$

$$\text{取 } E' = k(u_0, \dots, u_{n-1}) \subseteq E$$

$$\Rightarrow k \subseteq E' \subseteq E'(\alpha) \subseteq K$$

$\underbrace{\alpha}_{\text{f.d.}}$ $\underbrace{\text{f.d.}}_{E'(\alpha)}$

$\Rightarrow \alpha$ 在 k 上代數

□

k/k 是一個一般的域形狀

$$E = \{ \alpha \in K \mid \alpha \text{ 在 } k \text{ 上代數} \} \subseteq K.$$

Fact E 是一個域!

$$\text{证. } \underbrace{k}_{\text{f.d.}} \subseteq k(\alpha) \subseteq \underbrace{k(\alpha)(\beta)}_{\text{f.d.}} = k(\alpha, \beta)$$

□

$$\bar{Q} = \{ \alpha \in C \mid \alpha \text{ 在 } Q \text{ 上代數} \}$$

$$\Rightarrow Q \subseteq \underbrace{\bar{Q} \cap C}_{\text{經延}} \text{ 以後}$$

54.

Def 若 R 为一个代数闭域, 若 $\forall f \in R \hookrightarrow E$ 都是单向的, 即 $f = g$.

$\Leftrightarrow \forall$ 不可约 $f(x) \in k[x]$ $f|_R$ 是一次的

$\Leftrightarrow \forall f(x) \in k[x]$ 在 完全分裂 (线性因子之积)

$(k \subseteq k(x))$
其能做.

例 代数基环 ① 代数闭

例 \bar{R} 是代数闭的.

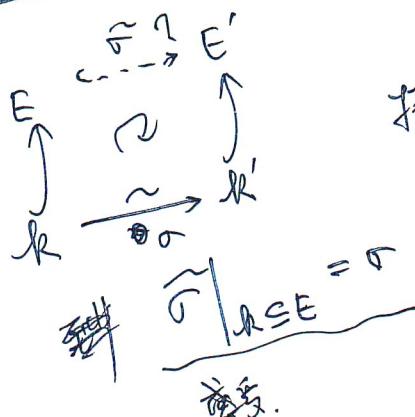
Fact $\forall R \exists! k \hookrightarrow \bar{R}$ 代数闭

可能用到 born 引理. 唯一性是同构意义下的.

默认

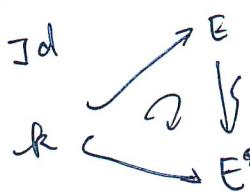
例 $\bar{R} = \bar{k}$

分层域 (Raman)



能合 / 是样 延拓

操作 $\sigma = \text{Id}$

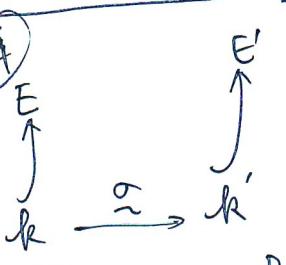


i.e. $\text{Aut}(E/k)$

$\sigma |_{K'} = \sigma$ ($\bar{\sigma}$ 是嵌入时)

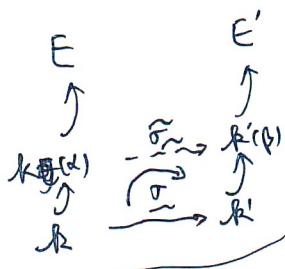
意义.

局部地处理 (key lem)



$\alpha \in k$ 上取最高项项式为 $f(x) = x^n + a_{n-1}x^{n-1} + \dots$ 也是不可约的
 $\text{且 } \sigma(f) = x^n + \sigma(a_{n-1})x^{n-1} + \dots$ 为同构

① 设有 $\beta \in \text{Root}_E(\sigma(f))$, 则 $\exists! \tilde{f} : k(\alpha) \xrightarrow{\sim} k(\beta)$



$\tilde{f} |_{k(\alpha)} = \sigma$

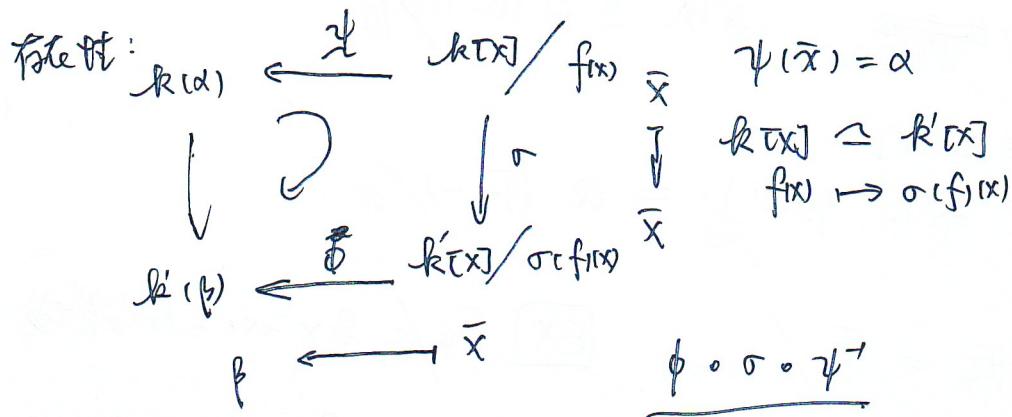
$\Rightarrow \sqrt[n]{\beta} \in \text{Root}_E(\sigma(f))$ 个延拓 $k(\alpha) \xrightarrow{\tilde{f}} E'$

$\tilde{f} |_{k} = \sigma$.

Rank $|\text{Root}_E(\sigma(f))| = \deg f - \deg \tilde{f} = \dim_k k^{(n)}$

证. II) 给定 β 后, 唯一性唯一 $\hat{\sigma}(\lambda) = \sigma(\lambda) \lambda \in K$

$$\begin{aligned}\hat{\sigma}(\alpha) &= \beta \\ \hat{\sigma}(\alpha^n) &= \beta^n \\ \text{又 } K(\alpha) \text{ 有基 } \dots \text{ 所以 } \hat{\sigma} \text{ 已被下述} \end{aligned}$$



(2) $\forall \bar{\alpha} : K(\alpha) \hookrightarrow E'$

$$\bar{\alpha}|_K = \alpha$$

则 claim: $\bar{\alpha}(\alpha) \in \text{Root } (\alpha|f)$.

□

然后爬梯子

[Def] $f(x) \in K[x]$ f 在 K 上的分层域 是 E/K

s.t. \exists , $f(x) \in E \not\subset \text{split}$ (in $E[x]$) $f(x) = (x-a_1) \cdots$

(2) $E = K(a_1, \dots, a_n)$ 即 E 是包含 K, a_1, \dots, a_n 的最小域.

有图, 唯一性(同构)

[Rmk] $\dim_K E < \infty$

存在性不依赖代数闭包.

Fact 1. 分层域总是存在的 $K \hookrightarrow K$. $f.d.$ $f(x)$ split in K

Claim: \exists

Case 1. $f(x)$ 在 K 上分层 \checkmark

$$2. f(x) = f_1(x) \cdots f_s(x)$$

$$\text{取 } K_1 = K[x]/(f(x))$$

内!

该 $E = K(a_1, \dots, a_k)$ 即 \bar{E} .

$f_i(x)$ 不重合

$$f(x) = (x-u) \# h(x)$$

(存在性平凡, 但有多次选择, 看起来很唯一)

56.

$$\text{例 } f(x) \in \mathbb{Q}[x], \quad f(x) = (x-a_1) \cdots (x-a_n)$$

$$a_i \in \overline{\mathbb{Q}}$$

则 $E = \mathbb{Q}(a_1, \dots, a_n) \subseteq \overline{\mathbb{Q}}$ 是 $f(x)$ 的分裂域.

$$\text{例 } (x^2 - 2) \in \mathbb{Q}[x] \text{ 的分裂域是 } \mathbb{Q}(\sqrt{2})/\mathbb{Q}$$

$$\text{例 } x^3 - 2 \in \mathbb{Q}[x]$$

$$\mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2)/\mathbb{Q} = \mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q}$$

$$\text{例 } F_2 \hookrightarrow F_4 = F_2 / (x^2 + x + 1) \text{ 是 } x^2 + x + 1 \text{ 的分裂域}$$

$$F_3 \hookrightarrow F_9 = F_3 / (x^3 + 1) \quad \boxed{\text{EX}} \quad F_9 / F_3 \text{ 是 } x^3 + 1 \text{ 的分裂域}$$

也是 $x^3 + 2x + 1 \in F_3[x]$ 的分裂域

结论: $\sigma: k \xrightarrow{\sim} k'$ 同构 \Leftrightarrow

$$f(x) \in k[x] \Leftrightarrow f(\sigma(x)) \in k'[x]$$

设 E/k 是 $f(x)$ 的分裂域

$$E/k' \text{ 是 } f(x) \text{ 的分裂域}$$

\cong splitting field

不等式

$$\text{则 } \sigma \text{ 可以延拓至 } \tilde{\sigma}: E \xrightarrow{\sim} E'$$

这样而 σ 至少有 $\dim_{k'} E'$

$$\dim_{k'} E' > \infty$$

Cor: 设 $\sigma = \text{Id}$ 是 $f(x)$ 的分裂域在同构意义下唯一.

① $f(x)$ 的分裂域在同构意义下唯一.

$$\text{② } \forall E = E' \Rightarrow |\text{Aut}(E/k)| \leq \dim_k E < \infty.$$

即 E 是 "有限" 的.

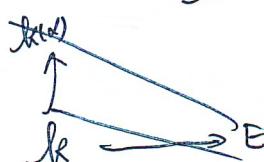
证: 对 $\dim_k E = 1$ 时.

$$\dim_k E = 1 \text{ 时.}$$

$$\dim_k E \geq 1.$$

$$f(x) = (x - \alpha_1) \cdots (x - \alpha_n) \quad \forall E$$

设 $\alpha_1 \notin k$.



$$\begin{array}{c} E \\ \uparrow \\ k(x) \\ \uparrow g \in k[x], \deg g \geq 2 \\ k \xrightarrow{\sim} k' \end{array}$$

$$f(x) = g(x)h(x) \quad \text{if } f = gh \text{ in } k[x]$$

在 E 中能分解
 $\Rightarrow \text{Root}_{E'}(g) \neq \emptyset$

$$\text{if } \beta_1 \in \text{Root}_{E'}(g)$$

$$\begin{array}{ccc} E & \xrightarrow{\exists \delta} & E' \\ \uparrow & \curvearrowright & \uparrow \\ k(x) & \xrightarrow{\tau_1} & k(\beta) \end{array}$$

$$\dim_E E = \frac{\dim_{k(x)} E(x)}{\dim_{k(x)} h} \cdot \dim_{k(x)} E.$$

用 $k(x)$

decide $\left\{ \begin{array}{l} E/\langle k(x) \rangle \\ E'/\langle h \rangle \end{array} \right.$ 是
 fix $k(x)$ 为 $k(\beta)$ 能否达到

维度是 σ_1 且 $\delta \leq \dim_{k(x)} E$
 用维数法 ---

(待续)

例 1 $\text{Aut}(\mathbb{Q}(\sqrt{-1})) = \text{Aut}(\mathbb{Q}(\sqrt{-1})/\mathbb{Q})$.

例 2 $x^3 - 2 \in \mathbb{Q}[x]$. $\rightarrow E = \mathbb{Q}(\sqrt[3]{2}, \omega)$

$$\text{Aut}(E/\mathbb{Q}) = \text{Aut}(E) = ?$$

$$\begin{array}{ccc} \dim_{\mathbb{Q}} E = 6 \\ \mathbb{Q}(\sqrt[3]{2}, \omega) & & \mathbb{Q}(\sqrt[3]{2}, \omega) \\ \uparrow & & \uparrow \\ \mathbb{Q}(\sqrt[3]{2}) & & \mathbb{Q} \\ \uparrow & \xrightarrow{\text{Id}} & \uparrow \\ \mathbb{Q} & & \mathbb{Q} \end{array}$$

$\text{Root}_E(x^3 - 2) = 3$. 17 根 \rightarrow 先打错
 $\{ \sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2 \}$

Int $\mathbb{Q}(\sqrt[3]{2})$ $\begin{array}{c} \tau_1 \\ \mathbb{Q}(\sqrt[3]{2}\omega) \end{array}$ $\begin{array}{c} \sigma_2 \\ \mathbb{Q}(\sqrt[3]{2}\omega^2) \end{array}$

58.

$$\begin{array}{ccc}
 & \xrightarrow{\quad f \quad} & \delta_{11} \\
 E & \xrightarrow{\quad w \quad} & E \\
 \uparrow & & \uparrow \\
 x^2 + x + 1 & & \text{root of } (x^2 + x + 1) = w, w^2
 \end{array}$$

$$\begin{array}{ccc}
 \mathbb{Q}(\sqrt[3]{2}) & \xrightarrow{\sigma_1} & \mathbb{Q}(\sqrt[3]{2}w) \\
 & & \delta_{11}(w) = w \\
 & & \delta_{12}(w) = w^2.
 \end{array}$$

$$\begin{array}{ccc}
 \delta_n & E & \xrightarrow{\sim} E \\
 \sqrt[3]{2} & & \mapsto \sqrt[3]{2}w \\
 w & & \mapsto w
 \end{array}$$

$$\begin{array}{ccc}
 \sigma_1 & \xrightarrow{\sim} & \delta_{11} \\
 & & \delta_{12} \\
 \text{Id} & \xrightarrow{\sim} & \delta_{01} \quad r(w) = w \\
 & & \delta_{02} \quad r(w) = w^2.
 \end{array}$$

$$\text{Aut}(E/\mathbb{Q}) = \{ \delta_{ij} \mid i=0,1,2, \ j=1,2 \}.$$

δ_{ij} 的乘法表.

$$\overline{\delta_{ij}}^{-1} = \delta_{ji}.$$

$\text{Aut}(\mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{3})/\mathbb{Q}) = ?$

$\text{Aut}(\mathbb{F}_4/\mathbb{F}_2)$

What has been proved?

从分裂域看! (同构)

(2) 分裂域 $k \hookrightarrow E$

$$|\text{Aut}(E/\mathbb{Q})| \leq \dim_E k$$

$\text{Aut}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}) \mid \dim_{\mathbb{Q}}(\mathbb{Q}(\sqrt[3]{2}))$

$$\begin{array}{ccc}
 (2) & \mathbb{Q}(\sqrt[3]{2}) & \xrightarrow{\not\exists} \mathbb{Q}(\sqrt[3]{2}) \\
 & \text{U1} & \xrightarrow{\sigma} \text{U1} \\
 & \mathbb{Q}(\sqrt[3]{2}) & \xrightarrow{\sim} \mathbb{Q}(\sqrt[3]{2})
 \end{array}$$

$f(x) \in k[x]$ 有数个重根 者 $\exists E/k \ni \frac{x-a^2}{x-a} \in k[x] / (f(x))$.

$f(x) = (x-a)^2$
 $x^2 - 2ax + a^2 \in k[x], \quad k = (\mathbb{F}_p[x]) \Rightarrow$ 不可以有重根

形式微分

$$f(x) = a_n x^n + \dots + a_0$$

$$f'(x) = \underbrace{n a_n x^{n-1} + \dots}_{\in k[x]}$$

$$\deg f' \leq \deg f - 1$$

↓
可重根的次数，比 $\deg f$ 少 1

有 Leibniz 法則

$$(fg)' = f'g + fg' \quad f, g \in k[x].$$

引理 (內蘊判斷) f 有重根 $\Leftrightarrow \gcd_k(f', f) \neq 1$

若 f 有重根， $\exists a \in E$.

$$f(x) = (x-a)^2 h(x) \quad \text{on } E[x].$$

$$f'(x) = 2(x-a)h(x) + (x-a)^2 h'(x) \in E[x]$$

$$\Rightarrow \gcd_E(f', f) \neq 1$$

↓ 仔擇

ak



$$\gcd_{k[x]}(f', f) = g(x)$$

(\Leftarrow)

取 $g(x)$ 的公因式 $\in K$.

$$\exists a \in k \quad (x-a) \mid \frac{g(x)}{f(x)}$$

$$\left\{ \begin{array}{c|l} (x-a) & f'(x) \\ (x-a) & f(x) \end{array} \right\} \Rightarrow f(x) = \frac{f'(x)(x-a)}{h(x)(x-a)}$$

$$\cancel{f'(x)} = h'(x)(x-a) + h(x) \cancel{(x-a)}$$

$$\Rightarrow (x-a) \mid f'(x).$$

$$\Rightarrow f(x) = (x-a)^2 h(x) \quad \text{in } k[x].$$

无重根 (逆否) : $f(x) \in k[x]$ 无重根 $\Leftrightarrow \forall a \in k$. $(x-a)^2 \nmid f(x)$

$$(x-a)^2 \nmid f(x)$$

$f(x)$ 无重根 $\Leftrightarrow \gcd_{k[x]}(f, f') = 1$.

Lemma. $f(x)$ 在 k 上可分, 若 $f(x)$ 的根不可约, 则无重根.

~~证明~~

反证法: 假设 $f(x)$ 有重根.

Prop: $\deg f = 0$ 则 $f(x) \in k[x]$ 可分.

$$\deg f' = \deg f^{-1}$$

若 f' 为 $f(x)$ 不可约.

$$\Rightarrow \deg f' = \deg f^{-1}$$

$$\gcd_{k[x]}(f' \cdot f) = 1$$

不可约.

反证法: $f(x) \in k[x]$ 有重根 E/k , f 在 k 上可分 $\Rightarrow \dim_E E = 0$

$\dim_E E = 0$.

证: (\Rightarrow) $f(x) = (x - \alpha_1) \cdots (x - \alpha_n) \in E$

$$\begin{array}{c} E \\ \uparrow \\ \alpha_1 \notin k \\ \alpha_1 - \alpha_2 \in k \\ \uparrow \\ q(f) \cdot h = h \end{array}$$

$$\begin{array}{c} \text{不可约} \\ \downarrow \\ \text{Root}_E q^{(n)} = \deg_q q \\ \text{无重根} \end{array}$$

$$q(x) | f(x)$$

$$\sigma_1 = \deg q$$

但 $\dim E/k(\alpha)$ 是 $f(x)$ at α 的分量域

故 σ_1 为 $\dim_{k(\alpha)} E$ 个逆元, 乘起来等于 1.

\Leftrightarrow 若不可约, 有矛盾!

$$f(x) = \underbrace{g(x)}_{\text{不可约}} \underbrace{h(x)}_{\text{无重根}}$$

□

有限域 E

逆元的特征量 $\sigma: \dim E = p > 0$

(1) $\exists! \mathbb{F}_p \hookrightarrow E$

自动有限域扩张 E/\mathbb{F}_p

$$[E : \mathbb{F}_p] = n$$

Frobenius.

自同构

$$\begin{array}{ccc} E & \xrightarrow{\sigma} & E \\ a & \mapsto & a^p \end{array}$$

Fact: $\sigma \in \text{Aut } E$.

$$\sigma(a+b) = \underbrace{\sigma(a)+\sigma(b)}_{\sigma(a+b)}$$

$$\sigma|_{\mathbb{F}_p} = \text{Id.} \quad (\text{Format 小巧})$$

$$\text{B1} \quad \mathbb{F}_4 = \mathbb{F}_2[x]/(x^2 + x + 1)$$

$$\begin{array}{c|cc} & 0 & 1 \\ \hline u & u & u+1 \end{array} \quad \mathbb{F}_2$$

$u \mapsto u^2 \xrightarrow{\sim} u+1$
 $u+1 \mapsto (u+1)^2 = u$

$\mathbb{F}_4/\mathbb{F}_2$ 是 $x^2 + x + 1$ 不可约的

$$\left| \text{Aut} \left(\mathbb{F}_4/\mathbb{F}_2 \right) \right|_2 = \dim_{\mathbb{F}_2} \mathbb{F}_4.$$

↑
 $\{ \text{Id}, \sigma \}$

$$\mathbb{F}_9 = \mathbb{F}_3[x]/(x^2 + 1) = \left\{ \begin{array}{c|ccc} & 0 & 1 & 2 \\ \hline u & u & u+1 & u+2 \\ \downarrow & \downarrow & \downarrow & \downarrow \\ 2u & 2u+1 & 2u+2 \end{array} \right\} \mathbb{F}_3.$$

$$u \mapsto u^2 = \frac{u^2}{u} = -u = 2u$$

$$u+1 \mapsto (u+1)^2 = 2u+1$$

⊗

$$\text{Aut} \left(\mathbb{F}_9/\mathbb{F}_3 \right) = \{ \text{Id}, \sigma \}$$

↑
⊗ [EX]

$$E^x = E \setminus \{0\} \quad \# E^x = p^n - 1$$

B_p 单位群

$$\boxed{a^{\frac{p^n-1}{d}} = 1}.$$

且 d 最小。

$$\exists d. \quad a^d = 1 \quad \Rightarrow \quad \{1, a^d, a^{2d}, \dots, a^{(d-1)d}\} \text{ 两两不同}$$

且 d 最小

由 Lagrange 定理. $d \mid p^n - 1$

□

$$\Rightarrow a^{p^n} = a \Rightarrow \sigma^n(a) = a$$

$\{ \text{Id}, \sigma, \dots, \sigma^{n-1} \} \subseteq \text{Aut } E = \text{Aut} \left(E/\mathbb{F}_p \right)$

还要证单射 (证到这个其实就搞定了)

62

問題 $\forall n \exists! \in \mathbb{F}_{p^n}$ 有理域

Claim 若 E/\mathbb{F}_p 是 $x^{p^n} - x$ 的分域

$$\forall a \in E, x^{p^n} - a = 0.$$

$$\Rightarrow x^{p^n} - x = \prod_{a \in E} (x - a) \text{ on } E \text{ 是其分域}$$

(2) 存在性. 取 E/\mathbb{F}_p 不是 $x^{p^n} - x$ 的分域 f.d

要算 E 的大小

$$\text{取 } K = \text{Root}_E(x^{p^n} - x) = \{a \in E \mid \sigma^k(a) = a\}$$

因 K 是子域 由分域的定理及 f.d. $\#K = p^n$.

故 K 是子域

而 $x^{p^n} - x$ 无重根. $\Rightarrow E$ 是整域. \square

問題 $x^{p^n} - x = \prod_{d|n} (\prod_{\text{deg } f=d} f)$

证. 取 $f(x) | x^{p^n} - x$ claim $\deg f | n$.

取 $\mathbb{F}_{p^n} \Rightarrow f_{\text{irr}}$ split $\exists a \in \mathbb{F}_{p^n}, f(a) = 0$

$f(a)$ 为 a 的最小多项式

$$\mathbb{F}_p \hookrightarrow \mathbb{F}_{p^{(a)}} \hookleftarrow \mathbb{F}_{p^n}$$

$\underbrace{\quad}_{\deg f} \quad \underbrace{n}_{\deg f | n.}$

Claim. $\forall d | n, g(x) \in \mathbb{F}_{p^{(a)}}[x] \Rightarrow g(x) | x^{p^d} - x$.

$$\mathbb{F}_p \hookrightarrow \mathbb{F}_{p^{(a)}} / (g(x)) \quad \dim_{\mathbb{F}_p} K = d \quad \#K = p^d$$

$$\Rightarrow \underbrace{g(x)}_{\text{irr}} \mid \underbrace{x^{p^d} - x}_{\mathbb{F}_{p^{(a)}}} \quad \underbrace{x^{p^n} - x}_{\mathbb{F}_{p^{(a)}}}$$

$\frac{p^d - 1}{p - 1} = p^{d-1}$

$$\text{例 } \frac{x^8 - x}{x^4 - x} = x(x-1)(x^2+x+1)$$

$$x^6 - x = x(x-1) \quad (\text{Ex}) \quad (x^5-1)(x^{10}+x^5+1)$$

$$x^{16} - x = x(x-1) = x(x^15 - 1) = x \cancel{(x-1)(x^{14} + \dots)}$$

$$x^{24} = x(x-1)(x^4 + \dots + 1) (x^{10} + x^5 + 1)$$

$$\begin{array}{r} d/n \\ 1^{24} \\ \hline 360 \\ 180 \\ \hline 72 \\ 36 \\ \hline 12 \\ 6 \\ \hline 4 \\ 2 \\ \hline 1 \end{array}$$

$$x^p$$

□

$$\text{例 } P=3, n=2 \quad x^9 - x = x(x-1)(x+1) \quad (\text{Ex})$$

$\frac{3}{1}, \frac{3}{2}$
 $\frac{3}{2}, \frac{3}{1}$

Galois 代数 分类子域

取至 $|E|=P^n$ ① $K \subseteq E$ 子域 且 $|K|=P^d$ $d|n$

② $\forall a \in E \exists! z \in K \subseteq E, |K|=P^d$.

特征根式

证 ① 令 $a \in K$. $|K|=P^d$ $a^{P^d} - a = 0$.

$K \subseteq \text{Root}_E(x^{P^d} - x)$

只有一解

证 ② 取 $K = \text{Root}_E(x^{P^d} - x)$

$$= \{a \in E \mid a^{P^d} - a = 0\}$$

$$= \{a \in E \mid \sigma^d(a) = a\}$$

i. $|K|=P^d$ $\sqrt{\text{恰一解}}$
 ii. K 子域

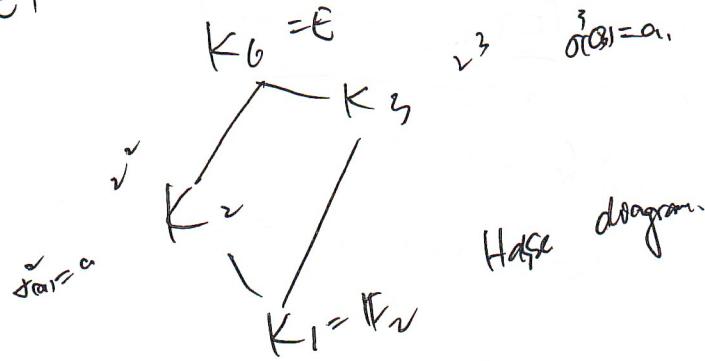
(Ex)

□

~~例 $E = \mathbb{F}_p[x]/(f)$~~

64

$$|E| = 2^6$$



Hasse diagram

$$(3) K_d \subseteq K_{d'} \Leftrightarrow d' | d$$

(4) $\exists n = p_1^{n_1} \cdots p_s^{n_s}$ 使得大寫子域 $K_{\frac{n}{p_i}} \quad 1 \leq i \leq s$.

由 E 有 n 個子域

$$\text{且 } \boxed{\exists} \left| \bigcup_{i=1}^s K_{\frac{n}{p_i}} \right| < |E| \quad \boxed{\exists}$$

(5) 易證 $K_{d_1} \cap K_{d_2} = K_{\gcd(d_1, d_2)}$

(6) $K_{d_1} \vee K_{d_2}$ 之為包含二者的最小子域.

$$\text{由 } K_{d_1} \vee K_{d_2} = K_{\text{lcm}(d_1, d_2)}$$

(7) 取 $u \in E$. $u \notin K_{\frac{n}{p_i}}$ 且

$$\Rightarrow R = \mathbb{F}_p(u) \quad u \text{ 是 } E \text{ 中唯一不可約的元素.}$$

$$(8) \sigma \in \text{Aut}(E) = \text{Aut}\left(\frac{E}{\mathbb{F}_p}\right) \quad \text{and} \quad n \text{ 整除.}$$

$$\overline{\sigma(u)} \quad (1 \leq i \leq n-1)$$

取 $d = n-1$ 使 $\sigma^d(u) = u$ 且 n 整除 d .

$$n = qd+r \quad \text{这个容易} \quad \downarrow \quad u \in K_d \quad \text{但 } \mathbb{F}_p(u) = E$$

$$\text{由 Step 2 } \sigma^i(u) = \sigma^j(u) \quad \text{if } 0 \leq i, j \leq n-1.$$

$$\text{即 } \{u, \sigma(u), \dots, \sigma^{n-1}(u)\} \quad \text{两两不同}$$

$$\Rightarrow \{\text{Id}, \sigma, \dots, \sigma^{n-1}\} \subseteq \text{Aut } E \quad \text{两两不同}$$

$$\text{Recall } \text{Aut}(E/\mathbb{F}_p). \quad |\text{Aut}(E/\mathbb{F}_p)| = \dim_{\mathbb{F}_p} E \Rightarrow \text{Aut } E/\mathbb{F}_p =$$

$$u \in \text{最小子域} \quad f(x) = (x - \sigma u) \cdots (x - \sigma^{n-1}(u))$$

$$f_{\text{res}} = 0. \quad \Rightarrow f(u) = f(\sigma(u)) = 0.$$

$\oplus \quad u, \sigma(u), \dots \in \text{Root}_E(f) \quad \square$

Fact $\forall d | n$

$$H_d = \{ \text{Id}, \sigma^d, \dots, \sigma^{d(\frac{n}{d}-1)} \} \subseteq \text{Aut}(E/F_p).$$

承认这个群论结果. (从循环群看比较自然)

i.e. $\text{Aut}(E/F_p)$ 的 $\frac{n}{d}$ 阶子群恰为 H_d

$$\begin{aligned} \text{定理 (有限域的 Galois 群)} & \text{ 固定 } |E| = p^n \quad E/F_p \\ \Leftrightarrow \text{双射 } \{K \subseteq E \mid K \text{ 是子域}\} & \Leftrightarrow \{\text{Aut}(E) \text{ 为 } \frac{n}{d} \text{ 阶 } H_d\} \\ K_d & \hookrightarrow H_d \end{aligned}$$

$$\begin{aligned} K_d &= \{ \sigma^d(a) = a \} \\ &\stackrel{?}{=} \{ \forall h \in H_d, h(a) = a \} \\ H_d &\stackrel{?}{=} \text{Aut}\left(E/K_d\right) \end{aligned}$$

$\xrightarrow{\text{K_d 为 直接子群}}$

域 ω 次单位根. 若 $\omega^n = 1$

单位根的阶 d s.t. $\omega^d = 1$. 若 $\text{ord}(\omega) = d$ d 次单位根.

Fact $\text{ord}(\omega) = d$ 则 $\omega^n = 1 \Leftrightarrow \text{ord}(n) = d$.

Fact. $\text{ord}(\omega) = d$ $\text{char } k = p > 0$. 则 $p \nmid d$.

Fact. $\text{ord}(\omega) = d$, $\{1, \omega, \dots, \omega^{d-1}\}$ 互不相同. d 阶子群.
 $\text{d 阶子群} \subseteq K^\times$ $\text{Root}_k(X^{d-1}) =$

6. 域 K , $\forall H \leq K$ 则 \exists 与 H 互素的 $H = \{1, \omega, \dots, \omega^{d-1}\}$ 且唯一

pf. 由 - 为 $\text{Root}_K(x^n-1)$

2 级互素

(推论) $|E| = p^n$ 则 E^* 有 p^n-1 个互素元

$\exists \omega \in E^*$, $\text{ord}(\omega) = p^n-1$

$\Rightarrow F_p(\omega) = E$.

分圆域

$\text{Root}_C(x^n-1) = \{1, \omega, \dots, \omega^{n-1}\}$

n 次本原根 $\{\omega^m \mid (m, n) = 1\}$ 有 $\varphi(n)$ 个.

证. $\text{ord}(\omega^m) = \frac{n}{\gcd(m, n)}$.

故. ① 分圆域 ② (ω) $\mathbb{Q}(\omega)/\mathbb{Q}$ 为 ω^n-1 的分圆域.

$$\mathbb{Q}(\omega_1) = \mathbb{Q}$$

$$\mathbb{Q}(\omega_2) = \mathbb{Q}(\sqrt{-3})$$

$$\mathbb{Q}(\omega_3) = \mathbb{Q}(i)$$

$$\mathbb{Q}(\omega_5) \supseteq \mathbb{Q}(\sqrt{5})$$

$$\begin{aligned} \text{定义 } n\text{-th 分圆多项式 } \Phi_n(x) &= \prod_{\substack{m \text{ 为 } n \text{ 本原根} \\ \text{互素}}} (x - \omega^m). \quad \omega \in \mathbb{Z}[i]. \\ &= \prod_{\substack{m \text{ 为 } n \text{ 本原根} \\ \gcd(m, n) = 1}} (x - \omega^m) \end{aligned}$$

$$\deg \Phi_n(x) = \varphi(n)$$

$$\Phi_1(x) = x-1$$

$$\Phi_2(x) = (x+1)$$

$$\boxed{\text{3.23}} \quad x^n - 1 = \prod_{d|n} \Phi_d(x).$$

$$\Phi_n(x) = \frac{x^n - 1}{\prod_{d|n} \Phi_d(x)} \Rightarrow \Phi_d(x) \in \mathbb{Z}[x].$$

类似地, $\Phi_p(x) = \frac{x^p - 1}{x - 1}$

$$\Phi_4 = \frac{x^4 - 1}{x^2 + 1} = x^2 + 1$$

$x^n - 1 = \prod_{0 \leq m \leq n-1} (x - \zeta^{m})$
 和 d 的本原单位根. $\left\{ \zeta^{m' \cdot \frac{n}{d}} \mid 0 \leq m' \leq d, \gcd(m', d) = 1 \right\}$

$$\{1, -\zeta^{n-1}\} = \bigcup_{d|n} \{d\text{ 本原根}\}$$

$$\begin{aligned} x^n - 1 &= \prod_{d|n} \prod_{\substack{0 \leq m \leq n-1 \\ \gcd(m, n)=d}} (x - \zeta^m) \\ &= \prod_{d|n} \Phi_d(x). \end{aligned}$$

□

为什么是这样? 请见.

$$\Phi_d(x) \in \mathbb{Z}[x], \quad d|n, \quad d|n$$

$$\Phi_n(x) = \frac{x^n - 1}{\prod_{d|n, d \neq n} \Phi_d(x)}.$$

$\boxed{\text{Ex}}$ $f, g \in \mathbb{Z}[x]$ 且 $f = gh$, $h \in \mathbb{C}[x]$
 且 $h \in \mathbb{Z}[x]$.

Rank. $\deg f \Rightarrow n = \sum_{d|n} \phi(d)$

$\boxed{\text{证明}}$ (Gauss/Kronecker) $\Phi_n(x) \in \mathbb{Z}[x]$ 不可约

$$\dim_{\mathbb{Q}} \mathbb{Q}[\Phi_n] = \phi(n)$$

proof. $n=p^k$ 且 $\Phi_p = x^{p-1} + \dots + x+1$ 不可约

设 Φ_n 的最小多项式是 $f(x)$

$\Rightarrow f(x) | \Phi_n(x)$

[Claim $x^n - 1 \in p\mathbb{Z}_n[x]$. $f(x) = 0 \Rightarrow f(x^p) = 0$]

$f(x) = 0 \quad \text{gcd}(m, n) = 1 \quad m = p_1 \cdots p_k - p \in \mathbb{Z}_n$

又用 Claim 证得.

~~proof~~ Claim: If $f(x^p) = 0$ x^p 的最小多项式 $g(x) \in \mathbb{Z}_m$ 有

$$\Rightarrow g(x^p) = 0$$

$\Rightarrow x$ 被 $g(\cdot^p)$ 整除

$$\Rightarrow f(\cdot) \mid g(\cdot^p) \quad [f(\cdot) \neq g(\cdot^p)]$$

$$\Rightarrow f(\cdot) \mid x^n - 1 \quad \begin{matrix} \text{?} \\ \uparrow \otimes \end{matrix} \quad \begin{matrix} f(x) \cdot g(x) \cdot (\cdots) \\ \uparrow \otimes \end{matrix} \quad \Rightarrow \text{矛盾}$$

根据定理 $\mathbb{Z} \rightarrow \mathbb{F}_p$

$$\Rightarrow x^n - 1 = f(x) \cdot \bar{g}(x) \cdot \bar{h}(x)$$

$$f(x) \mid g(x^p) \quad \begin{matrix} \uparrow \\ \mathbb{F}_p[x] \end{matrix}$$

$$f(x) \mid g(x^p)$$

$\mathbb{Z}_m[x]$

$$g(x) = b_m x^{mp} + \dots + b_1 x^p + b_0 \quad \text{in } \mathbb{F}_p[x]$$

$$= (b_m x^m + \dots + b_0)^p$$

$f(x)$ 与 $g(x)$ 在 $\mathbb{F}_p[x]$ 上 互素

$f(x)$ 有重根

$\Rightarrow x^n - 1 \in \mathbb{F}_p[x]$ 有重根

$$(1) \quad \text{gcd}(x^n - 1, \frac{n}{p} x^{n-1}) \neq 1 \text{ 无重根!}$$

$$\boxed{\text{证明}} \quad \dim_{\mathbb{Q}} \mathbb{Q}(\zeta_n) = \phi(n) \quad \checkmark$$

(2) 有理数域

$$\mathrm{Aut}(\mathbb{Q}(\zeta)) \xrightarrow{\sim} U(2n) \text{ 单位群}$$

$$\sigma(\zeta) = \zeta^m \quad \gcd(m, n) = 1$$

$$\tau(\zeta) = \zeta^l$$

$$\tau \circ \sigma(\zeta) = \zeta$$

$$\sigma \mapsto m$$

$$\tau \mapsto l$$

$$\text{共轭} \mapsto -1$$

原因:

E/\mathbb{K} f.d. \Rightarrow 纯粹扩张

$$\mathrm{Aut}(E/\mathbb{K}) = \{ \sigma \in \mathrm{Aut}(E) \mid \underbrace{\sigma|_{\mathbb{K}} = \mathrm{Id}_{\mathbb{K}}} \}_{\text{原因.}}$$

$$g(x) \in K[x], \quad u \in \mathrm{Root}_E(g)$$

$$\forall \underbrace{\sigma(u)}_{\text{作用}} \in \mathrm{Root}_E(g)$$

$$(\sigma \text{ 作用 } g(u) = 0_K)$$

$$\dim_{\mathbb{K}} E < \infty \Rightarrow |\mathrm{Aut}(E/\mathbb{K})| \leq \dim_{\mathbb{K}} E < \infty.$$

$$\mathrm{Aut} \frac{E}{\mathbb{K}} \supseteq \mathrm{Root}_E(g).$$

$$\sigma(w) \in \mathrm{Root}_E(g)$$

等价于

(σ 在 K 上的作用在 E 上等于 g).

$$E/\mathbb{K} \text{ f.d. } \mathrm{Aut}(E/\mathbb{K}) \leq \infty.$$

$$\text{① } H \subseteq \mathrm{Aut}(E/\mathbb{K})$$

$$H = \{ \sigma \in E : \sigma(z) = z, \quad \sigma \in H \} \subseteq E \text{ 固定子域}$$

$$\text{② } \mathbb{K} \text{ 为域 } \mathbb{K} \subseteq K \subseteq E$$

$$\mathrm{Aut}(\mathbb{E}/\mathbb{K}) \leq \mathrm{Aut}(E/\mathbb{K})$$

~~Global field. $\mathrm{Aut}(E/\mathbb{K})$ 为有限群.~~

7^o Galois 代數 E/R f.d.

$$\{ \text{Aut}(E/R) \text{ 的子群} \} \xrightarrow{E^H} \{ E/R \text{ 中的域} \}$$

$\text{Aut}(E/K)$

圓塊 若 E/R 可以表示成多個域的分裂域，則以上兩映射互通 (双射)

是新的

群論

$$\boxed{\text{定義}} (G, \cdot) \left\{ \begin{array}{l} \text{結合律} \\ \text{含幺元} \\ \text{可逆} \end{array} \right. \longrightarrow \begin{array}{l} \text{單位元} \\ \text{逆元} \end{array}$$

關係 \rightarrow 集合

Height 2

$$\boxed{\text{TEX}} a^{mn} = a^m \cdot a^n.$$

$$(a^{-1})^{-1} = a$$

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

$$\oplus \quad \text{若 } H \leq G$$

$$\left\{ \begin{array}{l} \text{若 } a, b \in H \Rightarrow a, b \in H \\ a \in H \Rightarrow a^{-1} \in H. \end{array} \right.$$

(公理) $\text{Aut}(E/K)$ 是加法群 $\left\{ \begin{array}{l} \text{结合律} \\ \text{逆元存在} \end{array} \right.$

$$\text{例 } O_n \leq GL_n(\mathbb{R}) \leq GL_n(\mathbb{C})$$

$$\text{Abel 群} \quad GL_1(\mathbb{C}) = \mathbb{C}^\times$$

Point 群 = Abel 群 通常写成 "+" : 逆 \rightarrow 负
逆 \rightarrow 正

加法群 例 离散对称群 \rightarrow 对称群
自同构群 \rightarrow 单值群

三大分支？

自同构群 $\text{Aut}(\mathbb{R}) = \{ \phi : \mathbb{R} \rightarrow \mathbb{R} \mid \phi \text{是双射} \}$
 乘法互结合。
 可能非连续

例 $(\mathbb{Z}_n, +)$ $\cup \mathbb{Z}_n = \{ \bar{m} \mid \gcd(m, n) = 1 \}$

$\text{Aut}(\mathbb{Z}_n) = \{ \text{id} \}$ 除元

例 域扩张 K/k

Aut(k/k) $\leq \text{Aut}(K)$. $\hookrightarrow (\text{Root}_K(F)) = (\text{Root}_{k/F})$
 不在 k 上分解。

例 $P \subseteq \mathbb{R}^n$

P 的(正交)对称群 行群

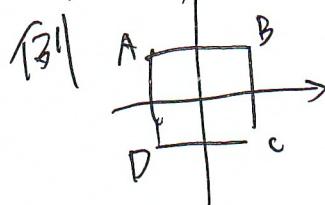
$\Sigma(P) = \{ g \in \text{O}_n \mid g|_P = P \} \leq \text{O}_n$

$\forall v \in P ; \forall v' \in P$

$g(v) \in P ; \exists u \in P \text{ s.t. } g(u) = v'$

$\forall g \in \Sigma(P)$ 通过 P - 一个 (正交) 对称

例 $\Sigma(S^1) = \text{O}_2$



旋转 & 反射

分析 $|g(A)| = P$

$V = \{ A, B, C, D \}$

$g(P) \in V$

EX 写出该群的一个矩阵

(非交换的八阶群)

72 例 | X (抽象群)

X 上置换 $\sigma: X \xrightarrow{\sim} X$

像 X 的 (抽象) 对称群

$$S(X) = \{ \text{对称置换} \}.$$

例 | $\text{Aut}(R) \leq \frac{S(R)}{\text{大R}}$.

Cayley 定理. 任何群同构于 $S(G)$ 的某个子群.

Lagrange 定理. 群 G , $|G| < \infty$. $H \leq G \Rightarrow |H| \mid |G|$.

类比维数公式.

$$H \leq G,$$

右陪集

$$ba \in G. aHa = \{ ba \mid b \in H, a \} \subseteq G.$$

$$Ha = Hb \Leftrightarrow a^{-1}b \in H$$

类比等价关系 $Ha = Hb \Leftrightarrow a \sim b$

$$G \text{ 分解} \sqcup_{i \in I} Ha, \text{ key fact } |Hd| = |H|$$

$$\Rightarrow G = \bigcup Hg = |H| \cdot |I| = |H| \cdot [G:H]$$

例 | 角平分的公因子群

可逆性比较版

$$\{ \bar{0}, \bar{1}, \bar{3} \}$$

(Rank) $|I| = [G:H] = \begin{matrix} \text{右陪集个数} \\ \text{左陪集个数} \end{matrix}$

Ex | $G = \bigcup H + a_i = \bigcup a_i^{-1}H$

例 | $G = GL_2(\mathbb{F}_2) = \{ (v_1, v_2) \mid (v_1, v_2) \in \mathbb{F}_2^2, \det(v_1, v_2) \neq 0 \}$ $|G|=6$.

$$\begin{array}{ccc} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 3 & x & 2 \end{array}$$

$$G = \left\{ \begin{matrix} C & \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} & \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}_b \\ & \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} & \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}_a \\ ab & \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} & \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}_{ac} \end{matrix} \right\} \xrightarrow{A^2 = I}$$

$$H = \{1, a\} \leq G.$$

算子集代表元素 H_b, H_a, H_{ba}

$$\underline{bH \neq Hb} \quad ? \quad ba = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = c$$

$$\text{eg } H \trianglelefteq G = H \cup bH \cup cH \quad \text{from ex}$$

$$\text{且 } G = H \cup b^{-1}H \cup c^{-1}H.$$

因为 H 不正规。

定理. $a \in G$, αa 有阶 (order) - 是最小正整数 $\alpha^d = 1$

若 d 不有限, 则 $d = \infty$. $d = \text{ord}(a)$

推论. $|G| < \infty$. $\text{ord}(a) \mid |G|$

$$(a^{\frac{|G|}{\text{ord}(a)}} = 1).$$

(证明略)

$$\text{例. } F_p^X = \{ \bar{1}, \dots, \bar{p-1} \}.$$

由 Lagrange 定理. $a^{p-1} = 1$.

$$\text{例. } E \text{ 素数域 } |E| = p^n$$

$$|E^X| = p^n - 1 \quad \forall a \in E^X \quad \frac{a^{p^n-1} = 1}{\forall a \in E^X} \Rightarrow \frac{a^{p^n} - a = 0}{\forall a \in E}$$

$$\text{阶素. } Q = U(2^8) = \{1, \bar{3}, \bar{5}, \bar{7}\}$$

$$\begin{array}{cccc} \downarrow & \downarrow & \downarrow & \downarrow \\ \bar{3} & \bar{5} & \bar{7} & \bar{1} \\ \downarrow & \downarrow & \downarrow & \downarrow \\ \bar{1} & \bar{2} & \bar{3} & \bar{4} \end{array}$$

$$\text{例. } Q = (\mathbb{Z}_4, +)$$

$$\begin{array}{cccc} \bar{0} & \bar{1} & \bar{2} & \bar{3} \\ \downarrow & \downarrow & \downarrow & \downarrow \\ \bar{4} & \bar{2} & \bar{0} & \bar{1} \end{array}$$