Galois理论

根式可解 $\Leftrightarrow$ Galois群可解

---

§1.1. 集合, 映射

$X. Y. Z$

映射 $f: X \to Y$

$\mathrm{Id}: X \to X$

$x \mapsto x$

$S \subseteq X$

$\mathrm{inc}: S \to X$

$x \mapsto x$

定义: $f: X \to Y$ $f': X' \to Y'$

若 $X = X'$ $Y = Y'$ $f(x) = f(x')$, $\forall x$.

$f = f'$

复合： $\begin{tikzcd} X \arrow[r, "f"] \arrow[rr, bend right] & Y \arrow[r, "g"] & Z \end{tikzcd}$

$f \circ g$.

① 结合律 $(f\circ g)\circ h = f\circ(g\circ h)$

② 有单位 (Id)

所有集合 / 所有映射 → category

单射、满射、双射.

$X \xhookrightarrow{f} Y \quad X \xrightarrow{f} \!\!\!\rightarrow Y \quad X \xrightarrow{f} Y$

$\mathrm{Im}(f) = \{ f(x) \mid x \in X \} \subset Y$

Ex. 单、满的内蕴刻画

(1) $f: X \mapsto Y$

证: f 单 $\Leftrightarrow$ $\forall g, g': Z \mapsto X$

$f \circ g = f \circ g'$

$\Rightarrow g = g'$ (左消去律)

(2) $f: X \mapsto Y$

证: f 满 $\Leftrightarrow$ $\forall g, g'$ $Y \mapsto W$

$g \circ f = g' \circ f$

$\Rightarrow g = g'$ (右消去律)

(3) $f: X \mapsto Y$ 双

$\Leftrightarrow$ $\exists g: Y \mapsto X$ s.t.

$f \circ g = Id_Y$

$g \circ f = Id_X$

集合的构造

(1) 不交并 $\sqcup$

(2) $X \times Y$

☆(3) $Map(X, Y) = \{ f \mid f: X \mapsto Y \}$ $\quad Y^X$

(4) $P(X) = \{X$ 全体子集$\}$

$Map(X, \{0,1\}) \xrightarrow{\sim} P(X)$.

逆映射: $C \mapsto \chi_C$

$$\chi_C(x) = \begin{cases} 1 & x \in C \\ 0 & x \notin C \end{cases}$$

(1) $\mathrm{Map}(X \sqcup Y, Z) \xrightarrow{\sim} \mathrm{Map}(X, Z) \times \mathrm{Map}(Y, Z)$

(2) $\mathrm{Map}(X, Y \times Z) \xrightarrow{\sim} \mathrm{Map}(X, Y) \times \mathrm{Map}(X, Z)$

(3) $\mathrm{Map}(X \times Y, Z) \xrightarrow{\sim} \mathrm{Map}(X, \mathrm{Map}(Y, Z))$

$f \mapsto (X \mapsto \phi_{f,x})$.

其中 $\phi_{f,x}: Y \mapsto Z$.

$y \mapsto f(x, y)$

等价关系

定义 X 上的关系 $R \subseteq X \times X$

① $\forall x \in X, (x, x) \in R$

$R \quad (\ldots) \in R$

② $\forall (x,y) \in R \Rightarrow (y,x) \in R$

③ $\forall (x,y) \in R, (y,z) \in R \Rightarrow (x,z) \in R$

记作 $x \overset{R}{\sim} y$

---

① $R = \{(x,x) \mid x \in X\}$

② 同余

根据等价关系分类

$[a] = \{x \in X \mid x \overset{R}{\sim} a\}$

① $b \in [a] \Leftrightarrow [b] = [a]$

② $[a] = [a'] \Leftrightarrow [a] \cap [a'] \neq \emptyset$

商集 关系

商集 为

$X/R = \{\text{所有等价类}\} \subseteq \mathcal{P}(X)$

$\pi_R: x \mapsto [x]$ 商映射.

定义. 完全代表元系. (依赖 Axiom of choice)

$S \subseteq X$. $\boxed{\forall x, \text{有且仅有一个 } s, \text{ s.t. } s \in [x].}$

Ex.

设 $\overset{R}{\sim}$ 是 X 上等价关系.

证: S 是完全代表元系

$\iff$ 复合映射

$$S \xhookrightarrow{inc} X \xrightarrow{\pi_R} X/R$$

为双射

$X = \bigsqcup [s].$

$X = \bigsqcup_{s\in S}$

定义X上的一个分拆为 $R = \{X_i \mid i\in I\} \subset \mathcal{P}(X)$

满足: ① $X_i \neq \emptyset$

② $X_i \cap X_j = \emptyset, \forall i \neq j.$

③ $X = \bigsqcup_{i\in I} X_i$

Fact: 等价关系和分拆可互相诱导.

Ex. $x \overset{I}{\sim} y \iff \exists i \in I.$ s.t. $x, y \in X_i$

· $\overset{I}{\sim}$ 为等价关系.

· $X/\overset{I}{\sim} = R$

$f: X \to Y$

Ex: 由f诱导等价关系: $\overset{f}{\sim}$

$[x] = f^{-1}(f(x))$

$[x] = \{y \mid f(y) = f(x)\}$

$y \in [x] \iff f(y) = f(x) \iff [y] = [x]$

$[y] \cap [x] \neq \emptyset \iff \exists z,\ f(y) = f(z), f(x) = f(z)$

$\iff f(x) = f(y) \iff [y] = [x]$

定理. 映射基本定理

$f: X \to Y$

由 f 诱导双射:

$X/\sim_f \xrightarrow{\sim} \mathrm{Im}(f)$

$[x] \longmapsto f(x)$

· well defined.

若 $[x] = [y]$ 则 $x \overset{f}{\sim} y$ $f(x) = f(y)$ ✓

若 $[x]=[y]$, ...

· 双:

单: 若 $f(x)=f(y)$

$\Rightarrow x \sim_f y$

$\Rightarrow [x]=[y]$

满: $\forall y \in \mathrm{Im} f$

$\exists x$, s.t. $f(x)=y$

则 $[x] \mapsto f(x)=y$

注:

$$\begin{tikzcd} X \arrow[r, "f"] \arrow[d] & Y \\ X/f \arrow[r, "\tilde{f}"] & \mathrm{Im}(f) \arrow[u, "inc"'] \end{tikzcd}$$

$f=$ 单 · 双 · 满

Ex. : $X^2 \to X$ 满足结合律

...

对 $((x\cdot y)\cdot z)\cdot w = x\cdot(y\cdot(z\cdot w))$,

左 $= (x\cdot y)\cdot(z\cdot w) = x\cdot(y\cdot(z\cdot w)) =$ 右.

环 $(R, +, \cdot)$.

定义 ① + 法 Abel group.

② × 法 结合律

③ 分配律

环的基本性质.

① 求和号

$a_1 + \cdots + a_n = \sum_{i=1}^{n} a_i$ (注意顺序)

② $-(-a) = a$ ✓

③ 数乘: $a \in R$ $n \in \mathbb{Z}$ (R作为 $\mathbb{Z}$-module).

$$na = \begin{cases} \sum_{i=1}^{n} a & n > 0 \\ 0 & n = 0 \end{cases}$$

$$\begin{cases} 0 & n=0 \\ -\sum_{i=1}^{-n} a & n<0 \end{cases}$$

Ex. $\forall a\in\mathbb{R}$, $n,m\in\mathbb{Z}$

① $(n+m)a = na+ma$

$nm=0$ 时显然

$n,m>0$ 时

$$(n+m)a=\sum_{i=1}^{n+m} a=\sum_{i=1}^{n} a+\sum_{i=1}^{m} a=na+ma$$

$nm<0$ 时. 不妨 $n>0>m$

$n+m\geq 0$ 时, $(n+m)a=\sum_{i=1}^{n+m} a=\sum_{i=1}^{n} a-\sum_{i=1}^{-m} a=na+ma$

$n+m<0$ 时, $(n+m)a=-(-n-m)a=-(-n)a-(-m)a$
$=na+ma$

$n,m<0$ 时, $(n+m)a=-(-n-m)a=-(-n)a-(-m)a$
$=na+ma$

② $na=(n1_R)a$ ($n=0$ 时特殊).

$n=0$ 时, 左 $=0a=(0+0)a=0a+0a$

$\Rightarrow 0a=0$

左 $= (0\mathbb{1}_R)a = ((0+0)\mathbb{1}_R)a = (0\mathbb{1}_R)a + (0\mathbb{1}_R)a$

$\Rightarrow (0\mathbb{1}_R)a = 0 \Rightarrow$ 左 $=$ 右

$n>0$ 时

$n=1$ 时成立

设 $n=k$ 时成立，则 $n=k+1$ 时

$(k+1)a = ka + a = k\mathbb{1}_R a + \mathbb{1}_R a = ((k+1)\mathbb{1}_R)a$，成立

$n<0$ 时

$na = -(-n)a = -((-n)\mathbb{1}_R)a = (n\mathbb{1}_R)a$

③ 广义分配律

$$\left(\sum_{i=1}^{n} a_i\right)\left(\sum_{j=1}^{m} b_j\right) = \sum_{i=1}^{n}\sum_{j=1}^{m} a_i b_j$$

Lemma. $\forall b, a_i \in R$, $n \in \mathbb{N}^*$

$$b\sum_{i=1}^{n} a_i = \sum_{i=1}^{n} ba_i \quad ①$$

$$\left(\sum_{i=1}^{n} a_i\right)b = \sum_{i=1}^{n} a_i b \quad ②$$

对 n 归纳，$n=1$ 时显然成立

设 $n=k$ 时成立，$n=k+1$ 时

①: $b\sum_{i=1}^{k+1}a_i = b\left(\sum_{i=1}^{k}a_i + a_{k+1}\right)$

$$= b\sum_{i=1}^{k}a_i + ba_{k+1}$$

$$= \sum_{i=1}^{k}ba_i + ba_{k+1} = \sum_{i=1}^{k+1}ba_i$$

②: 同理

$$\Rightarrow \sum_{i=1}^{n}\sum_{j=1}^{m}a_ib_j = \sum_{i=1}^{n}a_i\sum_{j=1}^{m}b_j$$

$$= \left(\sum_{i=1}^{n}a_i\right)\left(\sum_{j=1}^{m}b_j\right)$$

$n\in\mathbb{Z}$ $a.b\in R$

Ex. $(na)b = n(ab) = a(nb)$

Fact. 设R为环

以下等价:

① $0 = 1_R$

$\begin{cases} ① \ 0_R = 1_R \\ ② \ R = \{0_R\} \\ ③ \ R \text{ 一元} \end{cases}$

找本质！ 同构 → 本质一样.

以下，我们总假设 R 为含幺交换环.

$n \in \mathbb{N}$. $\quad a^0 = 1_R$

$$a^n = \underbrace{a \cdots a}_{n\text{个}}$$

Fact. $\forall n, m \in \mathbb{N}$

$$a^n \cdot a^m = a^{m+n}.$$

2项式定理（需交换）

$$(a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^i b^{n-i}$$

Ex. 证明 二项式定理. 归纳

定义. $a \in R$ 乘法可逆元 (单位 unit)

若 $\exists b$ s.t. $ab = 1_R$

记 $b = a^{-1}$

逆唯一: 若 $ab' = 1_R$

$$b' = b' \cdot 1_R = b'ab = b$$

Ex. $(1_R)^{-1} = 1_R$

非零环, 0_R 不可逆.

除法: a 可逆

$$c \div a = ca^{-1}$$

Fact. a 可逆，若

$ab=ac$

$\Rightarrow b=c$

对 $n<0$，定义 $a^n=(a^{-1})^{-n}$

Ex.

$a^n \cdot a^m = a^{n+m} \quad \forall n,m \in \mathbb{Z}$.

R 环

$U(R)=\{a\in R \mid a \text{ 可逆}\}$ 对乘法成群

$U(\mathbb{Z})=\{-1,1\}$

$U(\mathbb{Q})=\mathbb{Q}\setminus\{0\}$

$|U(\mathbb{Z}_n)| = \varphi(n)$.

例 $U(\mathbb{Z}_8) = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}$

$\cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

例. $U(\mathbb{Z}[\sqrt{-1}]) = \{\pm 1, \pm i\} \cong \mathbb{Z}_4$

$\mathbb{Z}[\sqrt{-1}] = \{m+ni \mid m, n \in \mathbb{Z}\}$.

证明: 取模长

称环 R 为整环 (integral domain).

$ab = 0_R \Rightarrow a = 0_R$ 或 $b = 0_R$

Fact. 消去律. $a \neq 0_R$

$ab = ac$

$\Rightarrow a(b-c) = 0 \Rightarrow b = c$

定义. 环R称域(field)，若

$U(R) = R \setminus \{0_R\}$

域为整环. 有限整环为域.

$n \geq 2$，以下等价.

① $\mathbb{Z}_n$ 整环

② n 素

③ $\mathbb{Z}_n$ 域

证明：显然

有限域：p^n 阶 $n \geq 1$.

同阶域唯一.

Ex. R有限整环

求证: R为域

定义 R环

子环 $S \subseteq R$, 若　　subring.

① $1_R \in S$.

② S对 $+$, $\times$ 封闭

S自然成环.

定义. 设K为域

子环S称子域, 若 $\forall a \neq 0_K \in S$.

$a^{-1} \in S$.

Ex. 例子.

$$\cdots = \left\{ \frac{m}{a} \;\middle|\; \begin{array}{l} a \geq 0 \\ \cdots \in \mathbb{Z} \end{array} \right\} \subseteq \mathbb{Q}$$

$R[p] \quad \{ p \ldots \mid m \in \ldots$

为子环.

Ex. $\mathbb{Q}(\sqrt{-1}) = \{a+b\sqrt{-1} \mid a, b \in \mathbb{Q}\} \subseteq \mathbb{C}$

为子域

Ex. $S \subseteq \mathbb{Q}(\sqrt{-1})$ 为子域

$\Rightarrow S = \mathbb{Q}$ 或 $S = \mathbb{Q}(\sqrt{-1})$.

§1.3. 理想, 商环.

设 $(R, +, \cdot)$, $(S, +, \cdot)$ 为环

定义: $\theta: R \to S$ 称环同态, 若

(1) $\theta(a+b)=\theta(a)+\theta(b)$

$\theta(ab)=\theta(a)\theta(b)$

☆(2) $\theta(1_R)=1_S$ （不同于参考教材）.

ring homomorphism

若θ双射，称环同构

ring isomorphism

Fact. θ homomorphism.

(1) $\theta(0_R)=0_S$.

(2) $\theta(na)=n\theta(a)$

注. 若θ同态.

保有一定性质.

例1 … 环同态

例. $\mathbb{Q}$ 到 $\mathbb{Z}_8$ 无环同态.

思维

Ex. $\nexists\ \mathbb{Z}_8 \xrightarrow{\theta} \mathbb{Q}$ 同态.

例 $S \subseteq R$ 子环

(1) inc $S \hookrightarrow R$ 单同态

(2) $\mathbb{Z} \to \mathbb{Z}_n$

$a \to \bar{a}$ 满同态

Lemma. $a \in U(R)$

$\Rightarrow \theta(a) \in U(S)$.

即: $\theta|_{U_R}$ 为 $U(R)$ 到 $U(S)$ 群同态.

$\theta: R \to S$ 为环同构

$\Rightarrow \theta^{-1}$ 为环同构.

证明: 显然...

定义. R 环.

$\mathrm{Aut}(R) = \{ R \xrightarrow{\sigma} R \mid \sigma \text{ 为同构} \}$.

$\mathrm{id} \in \mathrm{Aut}(R)$. Automorphism.

环 R 的自同构群. 极难研究.

例. $\mathbb{Z}$, $\mathrm{Aut}(\mathbb{Z})$.

$1 \to 1 \quad 2 \to 2 \quad -1 \to -1 \quad \cdots\cdots$

$\Rightarrow \mathrm{Aut}(\mathbb{Z}) = \{\mathrm{Id}\}$

例 $\mathbb{Z}[\sqrt{-1}]$ $\mathrm{Aut}(\mathbb{Z}[\sqrt{-1}])$

$\sigma: \mathbb{Z}[\sqrt{-1}] \to \mathbb{Z}[\sqrt{-1}]$

$m+ni \to m-ni$ 为自同构

$\sigma^2 = \mathrm{Id}$

断言：θ 为自同构 $\Rightarrow \theta = \mathrm{Id}, \sigma$

$\theta|_{\mathbb{Z}} = \mathrm{Id}_{\mathbb{Z}}$

$\theta^2(\sqrt{-1}) = \theta(-1) = -1$

$\Rightarrow \theta(\sqrt{-1}) = \pm i$

$\theta(\sqrt{-1}) = i$ 时 $\theta = \mathrm{Id}$

$= -i$ 时 $\theta = \sigma$

Ex. $\mathrm{Aut}(\mathbb{Q}) = \{\mathrm{Id}_{\mathbb{Q}}\}$

$\mathrm{Aut}(\mathbb{Q}[\sqrt{-1}]) = \{\mathrm{Id}_{\mathbb{Q}[\sqrt{-1}]}, \sigma\}$.

例 R 环

$\theta: \mathbb{Z} \to R$ 为环同态

$\Rightarrow$ θ 唯一

原因：保幺元

Fact $\theta: R \xrightarrow{\sim} S$ 同构

① $a \in U(R) \Leftrightarrow \theta(a) \in U(S)$

② $U(R) \xrightarrow{\sim} U(S)$ 群同构

☆ ③ $\varphi: \mathrm{Aut}(R) \xrightarrow{\sim} \mathrm{Aut}(S)$ 群同构

$\varphi(\gamma) = \theta \circ \gamma \circ \theta^{-1}$ $\quad S \xrightarrow{\theta^{-1}} R \xrightarrow{\gamma} R \xrightarrow{\theta} S$

④ R 域 $\Leftrightarrow$ S 域

Recall：映射基本定理.

$X \xrightarrow{f} Y$. $\quad \sim_f : x \sim_f y \Leftrightarrow f(x) = f(y)$

$\Rightarrow X/\underset{f}{\sim} \xrightarrow{\sim} \mathrm{Im}(f)$

$\theta: R \to S$ 为环同态

$\mathrm{Im}(\theta) \subseteq S$ 为子环

等价关系 $\sim_\theta$: $a \sim_\theta b \Leftrightarrow \theta(a)=\theta(b)$

$\Leftrightarrow \theta(a-b)=0$

定义. θ的核(kernel)为

$$\mathrm{Ker}(\theta)=\{a \mid \theta(a)=0_S\} \subseteq R$$

$\Leftrightarrow a-b \in \mathrm{Ker}\,\theta$

定义 $[a]=a+\mathrm{Ker}(\theta)=\{a+b \mid b\in \mathrm{Ker}(\theta)\}$

$\mathrm{Ker}(\theta)$ 对 $\pm\times$ 封闭 乘法

$\forall a \in R,\ r \in \mathrm{Ker}\,\theta.$

$ar \in \mathrm{Ker}\,\theta.$ → 对倍元封闭

定义. R为环, $I \subseteq R$ 称为理想 (Ideal)

若满足: ① $a,b \in I$, 则 $a \pm b \in I$

② $a \in I, b \in R, ab \in I$

记 $I \lhd R$

注: ① $I=R \iff 1_R \in I$

② 平凡理想: $\{0\}$, R.

③ $\forall a\in R$ 由a生成理想称主理想

$(a)=aR=\{ar \mid r\in R\}$

$(0)=\{0_R\}$

$R=(1_R)$

(4) $\ker\theta$为理想

Lemma. R为域 $\iff$ R仅平凡理想

证: R为域, 对任意$I\neq\{0\}$

取$a\in I$, $a\neq 0$ $\Rightarrow 1\in I \Rightarrow R=I$

Ex. 若R仅平凡理想, $\forall a\neq 0$

$(a)=aR=R$

$\Rightarrow \exists r\in R$, $ar=1$, 即可逆

例: $\mathbb{Z}$的理想

对 $I\neq\{0\}$

取 a 为 I 中最小正数

断言：$I = a\mathbb{Z}$

$a\mathbb{Z} \subseteq I$

$\forall r \in I$, $r = ap + q$ $0 \le q < a$

$q \in I \Rightarrow q = 0 \Rightarrow I \subseteq a\mathbb{Z}$

$\Rightarrow I = a\mathbb{Z}$

显然 $\forall a$, $a\mathbb{Z}$ 为理想，故 $a\mathbb{Z}$, $a \in \mathbb{Z}$ 为全部理想

定义 $I \triangleleft R$ 商环 R/I

$\boxed{\text{step 1}}$ $a, b \in R$

$a \equiv b \bmod I \Leftrightarrow a - b \in I$

Ex. $\equiv (\bmod I)$ 为 R 上等价关系

对 $\bar{a} = \{a + r \mid r \in I\} = a + I$ 为等价类

step 2. 定义运算

$\bar{a} + \bar{b} = \overline{a+b}$ (良定？) ✓

$\bar{a} \cdot \bar{b} = \overline{a \cdot b}$ (〃)

$\bar{a} = \bar{a'}$ $\bar{b} = \bar{b'}$

$\overline{ab} - \overline{a'b'} = \overline{(a-a')b + a'(b-b')} = \bar{0}$ ✓

$\Rightarrow R/I$ 为含幺交换环，零 0_R 幺 I_R

典范同态（canonical，商）

$\theta: R \to R/I$

$r \overset{\theta}{\to} \bar{r}$ 　　易证同态

$\boxed{\ker(\theta) = I.}$

例：$\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$

环同态基本定理 $\theta: R \to S.$

$R/\ker\theta \xrightarrow{\sim} \mathrm{Im}\,\theta$

$\bar{\theta}: R/\ker\theta \xrightarrow{\sim} \mathrm{Im}\,\theta$

只需：良定，保 $+\times$，双射

应用

① $\theta: R \hookrightarrow S$ 同态

θ 单 $\Leftrightarrow \ker\theta = \{0_R\}$

此时 $R \cong \mathrm{Im} R$

R 本质上为 S 子环

② $\theta: R \twoheadrightarrow S$ 满

$\Rightarrow R/\ker\theta \xrightarrow{\sim} S$ 同构

S本质为商环

例. 环 R

特征同态 $\mathbb{Z} \xrightarrow{\phi} R$

$n \to n1_R$

$\ker\phi = \{n \in \mathbb{Z} \mid n1_R = 0\}$ 为子理想

$\Rightarrow \exists n \geq 0 \quad \ker\phi = n\mathbb{Z}$

称 $n = char(R)$ (特征, character)

$\begin{cases} char(R) = 0, & \phi \text{单} \\ char(R) = n > 0 \ (n \geq 2) & \end{cases}$

$\Rightarrow Im(\phi) = \mathbb{Z}_n$

若 R 为整环，$\mathrm{char}(R)=0, p$，p 素数

否则 $\mathrm{char}(R)=n$ 合数

$\mathbb{Z}_n \subseteq R$（本质嵌入），有零因子

若 R 为域，$\mathrm{char}(R)=p$

$\mathbb{F}_p \subseteq R$ 为子域

若 $\mathrm{char}(R)=0$，$\mathbb{Q} \hookrightarrow R$

对 ϕ 延拓，$\tilde{\phi}(m/n)=\phi(m)\phi(n)^{-1}$

需验证良定性 ✓

Ex. $\tilde{\phi}$ 同态且 $\tilde{\phi}$ 单

命题: ($I \lhd R$, $can_I: R \to R/I$)

设 $R \xrightarrow{\theta} S$ 同态

对 $I \subset \ker\theta$

$\Leftrightarrow$ $\exists!$ 环同态 $R/I \xrightarrow{\theta'} S$ s.t. $\theta = \theta' \circ can$

$$\begin{tikzcd} R \arrow[r, "\theta"] \arrow[d, "can"'] & S \\ R/I \arrow[ur, "\theta'"'] & \end{tikzcd}$$

$\Leftarrow$: 显然

$\Rightarrow$: 唯一性:

$\theta = \theta' \circ can = \theta'' \circ can$

can 满射，有右消去律 $\Rightarrow \theta = \theta'$

存在性：

$\theta' : R/I \to S$

$\bar{a} \to \theta(a)$

well-defined: ✓

例. $I \subseteq J \subseteq R$, $I, J \trianglelefteq R$

$R/I \twoheadrightarrow R/J$

$a+I \longrightarrow a+J$

良定，满同态

核: $\{j+I \mid j \in J\} = J/I$

Abelian group 作商

$$(R/I)/(J/I) \xrightarrow{\sim} R/J$$

$$(a+I)+J/I \to a+J$$

Fact. $I \lhd R$

$$\{J \lhd R \mid J \supseteq I\} \xrightarrow[\phi]{\text{bijective}} \{R/I \text{ 的理想}\}$$

$$J \overset{\phi}{\mapsto} J/I$$

$$f(\bar{J}) = \{a \mid a+I \in \bar{J}\} \longleftarrow \bar{J} \lhd R/I$$

Ex. 1. $\psi(\bar{J}) \trianglelefteq R$

2. $\psi(\bar{J})/I = \bar{J}$

3. $\psi(J/I) = J$

注：由此得：$I \trianglelefteq R$
I为极大理想 $\Leftrightarrow$
R/I为域

例. $\mathbb{Z}_n$的理想

$$\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$$

$$\left\{\bar{J} \,\middle|\, \begin{array}{l} \bar{J} \trianglelefteq \mathbb{Z}_n \\ \bar{J} \subseteq n\mathbb{Z} \end{array}\right\} \Leftrightarrow \left\{J \,\middle|\, \begin{array}{l} J \trianglelefteq \mathbb{Z} \\ J \supseteq n\mathbb{Z} \end{array}\right\}$$

$$\Leftrightarrow \{d\mathbb{Z} \mid d \mid n\}$$

$$d \longmapsto d\mathbb{Z}/n\mathbb{Z}$$

Ex. $I \trianglelefteq R$

$\{S \subseteq R \mid S \supseteq I\} \longrightarrow \{R/I \text{ 的子环}\}$

$$S \mapsto S/I \subseteq R/I$$

注：双射.

---

§1.4 分式域. 商域

(1) 分式域 $\left\{\begin{array}{l} \mathbb{Z} \hookrightarrow \mathbb{Q} \\ n \mapsto n/1 \end{array}\right.$

R. 整环

$R^\times = R \setminus \{0_R\}$

$R \times R^\times = \{(a,x) \mid a \in R, x \in R^\times\}$

$(a,x)\sim(b,y) \Leftrightarrow ay=bx$ in R

Ex. 证明"$\sim$"为等价关系.

定义. 分式

$$\frac{a}{x} = \{(b,y) \mid (b,y)\sim(a,x)\}$$

$$\mathrm{Frac}(R) = R\times R^{\times}/\sim$$

定义. 运算

$$\frac{a}{x}+\frac{b}{y} = \frac{ay+bx}{xy} \qquad (xy\neq 0_R)$$

若 $\frac{a}{x}=\frac{a'}{x'}$, $\frac{b}{y}=\frac{b'}{y'}$

$x'y'(ay+bx)$

$\Rightarrow xy(a'y'+b'x') - x'y'(ay+bx)$

$= yy'(xa'-x'a) + xx'(yb'-y'b) = 0_R$

$$\frac{a}{x}\cdot\frac{b}{y} = \frac{ab}{xy}$$

$\Rightarrow (\mathrm{Frac}(R), +, \cdot)$ 为交换环

Fact. $(\mathrm{Frac}(R), +, \cdot)$ 为域（R的分式域）

$a \neq 0$.

$$\frac{a}{x}\cdot\frac{x}{a} = 1$$

R可嵌入$\mathrm{Frac}(R)$

$R \hookrightarrow \mathrm{Frac}(R)$

$r \mapsto r$

1_R

易证单射，

满射 $\iff$ R为域

命题（$can_R: R \to Frac(R)$）

R整环，K域，单同态 $\phi: R \hookrightarrow K$

则 $\exists!$ 同态 $Frac(R) \xrightarrow{\tilde{\phi}} K$，$\phi = \tilde{\phi} \circ can_R$

$$\begin{tikzcd} R \arrow[r, "\phi"] \arrow[d, "can_R"'] & K \\ Frac(R) \arrow[ur, "\tilde{\phi}"'] & \end{tikzcd}$$

（即 $Frac(R)$ 是包含R的最小子域）

证：唯一性：

x^{-1}

$$\tilde{\phi}\left(\frac{a}{x}\right) = \tilde{\phi}\left(\frac{a}{1_R}\right)\tilde{\phi}\left(\frac{x}{1_R}\right)^{-1}$$

$$= \tilde{\phi}(\mathrm{can}_R(a))\,\tilde{\phi}(\mathrm{can}_R(x))^{-1}$$

$$= \phi(a)\phi(x)^{-1}$$

存在性:

令 $\tilde{\phi}(a/x) = \phi(a)\underline{\phi(x)}^{-1}$ (单同态)

well-defined ✓

$\tilde{\phi}$ 单

Ex. K, L 域

$\theta: K \to L$ 同态

$\Rightarrow$ θ 单

例.

(1) $\mathrm{Frac}(\mathbb{Z}) = \mathbb{Q}$

(2) $\mathrm{Frac}(\mathbb{Z}[\sqrt{-1}])$

Ex. $\widetilde{\mathrm{inc}} : \mathrm{Frac}(\mathbb{Z}[\sqrt{-1}]) \xrightarrow{\sim} \mathbb{Q}(\sqrt{-1})$

注：分式域缺点：若 R 非 UFD，无法定义"既约"，不好找完全代表元系.

定义. 真理想 $\mathfrak{p} \neq R$ 称素理想

$\Leftrightarrow ab \in \mathfrak{p} \Rightarrow a \in \mathfrak{p} / b \in \mathfrak{p}$

Fact.

① $\{0\}$ 为素理想 $\Leftrightarrow$ R 整环

② $\mathfrak{p} \neq R$

$\mathfrak{p}$素 $\Leftrightarrow$ $R/\mathfrak{p}$ 整环

$\Rightarrow$: $\bar{a}\cdot\bar{b}=\bar{0} \Rightarrow \bar{a}=0 / \bar{b}=0$

即 $ab\in\mathfrak{p} \Rightarrow a\in\mathfrak{p} / b\in\mathfrak{p}$

$\Leftarrow$: 同理.

例. $R=\mathbb{Z}$

(0) 素

$n\geq 2$ $\quad n\mathbb{Z}$ 素 $\Leftrightarrow$ n 素数.

R 为环

$\mathrm{Spec}(R)=\{\mathfrak{p}\triangleleft R \mid \mathfrak{p}$ 素理想$\}$

素谱 (spectral)

注：Spec(R)上

Zariski拓扑

sheaf结构

真理想 $M \lhd R$ 称极大理想，若

$M \subseteq I \lhd R$，则 $I = R$ maximal ideal

命题. $M \lhd R$

M 极大

$\Leftrightarrow$ R/M 域 由此得极大理想为素理想

R/M 的理想 $\longleftrightarrow \{ I \mid M \subseteq I \lhd R \}$

M 极大

$\Leftrightarrow R/M$ 仅平凡理想

$\Leftrightarrow R/M$ 为域　　剩余域

另：$\forall a \in R$，$\bar{a} \in R/M$，$a \notin M$

$\Rightarrow$：$a \in Ra+M \neq M$

$\Rightarrow Ra+M=R$

$1_R = \underset{\text{为逆}}{r}a+m$

$\mathrm{Max}(R) = \{I \trianglelefteq R \mid I$ 极大理想$\}$

极大谱

Fact. (Hilbert)

$\mathrm{Max}(\mathbb{C}[x_1, \cdots, x_n]) \longleftrightarrow \mathbb{C}^n$

对于 $(a_1,\cdots,a_n)\in\mathbb{C}$

由 $x_1-a_1, x_2-a_2,\cdots,x_n-a_n$ 生成的理想

与几何相关。

以下 R 为整环

$a\neq 0_R$

$a\mid b \Leftrightarrow \exists c\in R,\ b=ac$

$\Leftrightarrow b\in(a)=aR$

设 $0_R\neq a\in R$，a 素元 $\Leftrightarrow (a)$ 素理想

$\Rightarrow a\notin U(R)$

$\Leftrightarrow xy\in(a) \Rightarrow x\in(a)$ 或 $y\in(a)$

$a\mid xy \Leftrightarrow a\mid x$ 或 $a\mid y$

定义. $0_R \neq a \in R$, a 不可约 $\Leftrightarrow$

$$\begin{cases} a \notin U(R) \\ a = bc,\ 则\ b \in U(R)\ 或\ c \in U(R) \end{cases}$$

Fact. 素元必为不可约元.

a 素 $a = bc \Rightarrow a \mid b$ 或 $a \mid c$, 不妨 $a \mid b$

设 $b = at$

$\Rightarrow a = atc \Rightarrow tc = 1 \Rightarrow c \in U(R)$

例. $\mathbb{Z}[\sqrt{-3}]$

断言: 2 不可约 证明: 取模

$2 \mid (1+\sqrt{-3})(1-\sqrt{-3}) = 4$ 2 非素元.

例- $\mathbb{Z}[\omega] = \{m+n\omega \mid m,n\in\mathbb{Z}\}$ 为 $\mathbb{C}$ 子环

Eisenstein 整环

claim: 2 in $\mathbb{Z}[\omega]$ 为素元

设 $2 \mid (m_1+n_1\omega)(m_2+n_2\omega)$

$$= m_1m_2-n_1n_2+(m_1n_2+n_1m_2-n_1n_2)\omega$$

$2 \mid m_1m_2-n_1n_2 \qquad 2 \mid m_1n_2+n_1m_2-n_1n_2$

§1.5 一元多项式环

R 环 x 字母

$$R[x] = \left\{\sum_{i=0}^{n} a_i x^i \;\middle|\; a_i \in R\right\}$$

定义 $f=g \Leftrightarrow$ 各项系数相等

$$f(x) = \sum^{n} a_i x^i$$

$i=0$

$a_n \neq 0$，称首项系数

若 $a_n = 1$，称首一多项式

定义 $f(x) = \sum_{i=0}^{n} a_i x^i$，$a_n \neq 0_R$，$f \neq 0_R$

记 $\deg f = n$

Fact. $F[x]$ 自然为环（含幺交换）

(1) + 系数相加

(2) 乘法.

$$\left(\sum_{i=0}^{n} a_i x^i\right)\left(\sum_{i=0}^{m} b_i x^i\right) = \sum_{i=0}^{n+m} \sum_{j=0}^{i} a_j b_{i-j} x^i$$

注：$R \hookrightarrow R[x]$

$a \longrightarrow a$ 常值多项式

命题，R 整环 $\Rightarrow R[x]$ 整环

证明：取最高次项 $\deg gf = \deg g + \deg f$

Ex. R

$R'[x] = \{(a_0, a_1, \cdots, a_n) \mid a_i \in R$，有限项非 $0\}$

$R[x]$ 与 $R'[x]$ 同构

命题：$R \hookrightarrow R[x]$ 的泛性质

$\forall \varphi: R \to S$ 同态　$s \in S$

对 $\exists!$ 环同态 $R[x] \xrightarrow{\tilde{\varphi}} S$

s.t. $\tilde{\varphi}|_R = \varphi$，$\tilde{\varphi}(x) = s$

代数一性：

$$\tilde{\varphi}(x^n)=s^n$$

$$\tilde{\varphi}(a_n x^n)=\varphi(a_n)s^n \quad 唯一$$

$$\tilde{\varphi}(\sum a_i x^i) = \sum \varphi(a_i) s^i$$

Ex. 证明存在性

$$\tilde{\varphi}(\sum_{i=0}^{n} a_i x^i) = \sum_{i=0}^{n} \varphi(a_i) s^i$$

例. $a \in R$ fix a.

$$f(x)=\sum_{i=0}^{n} a_i x^i$$

$$ev_a : R[x] \to R$$

$ev_a(\sum_{i=0}^{n} a_i x^i) = \sum_{i=0}^{n} a_i a^i$ 为环同态

注：多项式 $\Longleftrightarrow$ 多项式函数

定义. $f(x) \in R[x]$ $\quad a \in R$

$$f(a) = \sum_{i=0}^{n} a_i a^i$$ 赋值运算

fix $a \in R$

$$ev_a : R[x] \to R$$

$$ev_a\left(\sum_{i=0}^{n} a_i x^i\right) = \sum_{i=0}^{n} a_i a^i$$

fix $f(x) \in R[x]$

$$f : R \to R \qquad f \in Map(R, R)$$

$Map(R, R)$ 自然成环，称函数环

乘，加

Fact.

$$ev: \mathbb{R}[x] \longrightarrow Map(\mathbb{R}, \mathbb{R})$$

$$f(x) \to f \text{ 多项式函数}$$

Ex. ev为同态

以下设 k 是域.

$k[x]$

首一化

带余除法 $f, g \in k[x]$, 则 $\exists!\, q(x)$, s.t.

$$f = gq + r, \quad \deg r < \deg g$$

余数定理. $\exists!\, q(x)$ s.t.

$$f(x) = q(x)(x-a) + f(a)$$

证明: $f(x) = q(x)(x-a) + r$

用 ev_a 作用

$\Rightarrow f(a) = r$ ✓

$\square$

$$\mathrm{Root}_k(f(x)) = \{a \in k \mid f(a) = 0_k\}$$

$\Updownarrow$

"一次因式"

定义. 整环的 PID (Principal ideal domain)

主理想整环

若所有理想为主理想

证: (1) $I \lhd k[x]$

设 $h \in I$ 为 I 中 $\deg \geq 1$ 的次数最小元

$I = h(x)k(x)$.

$(2)\ \mathbb{Z}$

PID的基本性质

(1) R整环

最大公因子 (great common divisor)

$0 \neq d = \gcd(a,b)$，满足：

$$\begin{cases} d \mid a,\ d \mid b \\ 若 d' \mid a, d\ ,\ 则\ d' \mid d \end{cases}$$

注：不一定存在

在相差一个可逆元的情况下唯一.

$\Leftrightarrow\ (d \mid e,\ e \mid d) \Leftrightarrow (e) = (d)$

注：$d \mid a, b \Leftrightarrow (a), (b) \subset (d)$

Ex. $d = \gcd(a,b)$

$\Longleftrightarrow (d) \supseteq (a)+(b)$

为包含 $(a)+(b)$ 的最小主理想 in R 整环.

Fact. R PID 则 $\gcd$ $\exists$

证: $a, b \in R$

取 $(d) = (a)+(b) \Rightarrow d = \gcd(a,b)$

注: R PID 时有 Bezout 等式 $\exists u, v \in R$

$\gcd(a,b) = ua + vb$

取 $(a)+(b)$ 中"极小"元素即 $\gcd$

Ex. $R = \mathbb{Z}[\sqrt{-3}]$

$\gcd(4, (1-\sqrt{-3})^2) \nexists$

$4 = (1-\sqrt{-3})(1+\sqrt{-3})$, 设 $d = \gcd$

$d = (1-\sqrt{-3})d'$, $d' \mid 1-\sqrt{3}$ $d' \mid 1+\sqrt{3}$

$\Rightarrow d' \mid 2$, $d' = 1$, $d = (1-\sqrt{3})$

$2 \mid 4$, $2 \mid (1-\sqrt{-3})^2$, $2 \nmid d$, 矛盾.

(2) 不可约元为素元

证: a 不可约

$a \mid bc$, $a \nmid b$

$\Rightarrow \gcd(a,b) = 1_R$

$ua + vb = 1_R$

$\Rightarrow c = (ua+vb)c$

$= uc \cdot \underline{a} + v \cdot (\underline{bc})$ $a \mid c$

(3) R PID, $0 \neq P \in \mathrm{Spec}(R)$

(3) R 为 PID, $0 \neq \mathfrak{p}$ …

则 $\mathfrak{p} \in \mathrm{Max}(R)$

即 $\mathrm{Spec}(R) = \{0\} \cup \mathrm{Max}(R)$

证: 设 $\mathfrak{p} \in \mathrm{Spec}(R)$, $\mathfrak{p} \neq \{0\}$

$\Rightarrow \mathfrak{p} = (p)$, p 素元.

若 $\mathfrak{p} \lhd I \lhd R$, $\mathfrak{p} \subsetneq I \subsetneq R$

设 $I = (b)$

$\Rightarrow b \mid p \Rightarrow b \in U(R)$, 矛盾.

$f(x), g(x) \in k[x]$

$\gcd(f, g) = h$

h monic

· $h|f$, $h|g$

· 若 $a|f$, $a|g$, 则 $a|h$

$\Rightarrow h\ \exists!$

$k[x]$ 中不可约元，称不可约元。

$$\mathrm{Max}(k[x]) \xleftrightarrow{1:1} k\text{上首一不可约多项式}$$

R 整环，称 a,b 相伴，若 $a=ub$, $u\in U(R)$

$\Leftrightarrow a|b$, $b|a$

$\Leftrightarrow (a)=(b)$

整除时 a,b 等价.

Kronecker 添根构造

$f(x)\in k[x]$ 首一不可约

$$k[x]\Big/\overset{\text{Max}}{(f(x))} = K \text{ 为域}$$

$$k \overset{\theta}{\hookrightarrow} K$$

$$x \longrightarrow \bar{x} \quad \text{同余类}$$

$$k \overset{inc}{\hookrightarrow} k[x] \xrightarrow{can} K \qquad \theta = can \circ inc$$

Ex. $a \in k$

$x - a \in k[x]$ 首1不可约

$$k \overset{\theta}{\hookrightarrow} k[x]\big/(x-a) \text{ 为同构.}$$

记 $u = x + (f(x)) \in K$ (即记为 $\bar{x}$)

$$k \overset{1:1}{\longrightarrow} k^{\deg f}$$

例 $\mathbb{F}_2=\{0,1\}$ $\quad x^2+x+1$ 不可约

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

$$=\begin{Bmatrix} \theta(\bar{0}) & u \\ \theta(\bar{1}) & u+\theta(\bar{1}) \end{Bmatrix}$$

$$\sum_{i=0}^{n} c_i x^i \xrightarrow{\theta} \sum_{i=0}^{n} \theta(c_i) u^i \quad (系数对应)$$

Ex. K, L 域

$\theta: K \hookrightarrow L$ 单同态

对 L 自然成 K 线性空间

$\lambda \in k \quad a \in L$

$\lambda a = \theta(\lambda) a$ (视其倍数 θ).

$\sum_{i=0}^{n} c_i x^i \xrightarrow{\theta} \sum_{i=0}^{n} \theta(c_i) u^i$ (系数对应)

为 k-线性空间之

$\{1_K, u, \dots, u^{\deg f - 1}\}$ 构成一组基.

维数 $\deg f$

$\theta(\lambda) = \bar{\lambda} = \lambda 1_K$

故以下省略 θ (用线性空间数乘代替)

$$F_f = \begin{pmatrix} \bar{0} & u \\ & \\ \bar{1} & u+1 \end{pmatrix}$$

$x^2+x+1=(x-u)(x-u-1)$

Ex. $f\in k[x]$, $\deg f\le 3$

f 不可约 $\Leftrightarrow \mathrm{Root}_k(f)=\emptyset$

Fact. $|\mathrm{Root}_k(f)|\le \deg f$

$k\subseteq K$ $\quad f(x)\in k[x]$

$\Rightarrow \mathrm{Root}_k(f)\subseteq \mathrm{Root}_K(f)$

☆ $f,g\in k[x]$，则

$\gcd_k(f,g)=\gcd_K(f,g)$

证法1：辗转相除

证法2：$d_1=\gcd_k$ $\qquad d_2=\gcd_K$

$d_1 \mid d_2$

$d_1=af+bg \Rightarrow d_2\mid d_1$

思考：$k\xhookrightarrow{\theta}K$ 单同态

$k\cong \mathrm{Im}(k)\subseteq K$

$$k[x] \overset{\theta}{\hookrightarrow} K[x]$$ 此处由系数对应同态

$$\sum a_i x^i \to \sum \theta(a_i) x^i$$

于是

$$\theta(\mathrm{Root}_k(f)) \subseteq \mathrm{Root}_K(f)$$

Ex. 证明上式

$f(x), g(x) \in k[x]$, 则

$$\theta(\gcd_k(f(x), g(x))) = \gcd_K(f, g)$$

Ex. 证明上式

添根构造

$f(x) \in k[x]$, 首一不可约

$$\mathrm{Root}_k(f) = \emptyset$$

$K = k[x]/(f(x))$

$u = x + (f(x))$

$k \overset{\theta}{\hookrightarrow} K[x]$

$\lambda \longrightarrow \lambda + (f(x))$ θ单同态

$\forall \lambda \in k$, $\theta(\lambda)$ 记为 λ

$f(x) \in k[x] \xrightarrow{\theta} K[x]$

Key Claim.

$u \in \mathrm{Root}_K(f(x))$

即 $\sum_{i=0}^{n} u^i a_i = \sum_{i=0}^{n} \bar{x}^i \theta(a_i)$

$$= \sum_{i=0}^{n} \theta(a_i) x^i =$$

$$\mathbb{R}[x]/(x^2+1) \xrightarrow{\sim} \mathbb{C}$$

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

Ex. 不存在 $\mathbb{F}_4$ 到 $\mathbb{Z}_4$ 同态

存在唯一 $\mathbb{Z}_4$ 到 $\mathbb{F}_4$ 同态

$$x^2+x+\bar{1} = (x+u)(x+u+\bar{1})$$

泛性质.

$$\theta: k \hookrightarrow k[x]/(f(x))$$

$\delta: k \hookrightarrow F$

$\alpha \in \mathrm{Root}_F(\delta(f))$ $\delta(f)$为系数对应

对 $\exists!\ K \xhookrightarrow{\tilde{\delta}} F$

s.t. $\begin{cases} \tilde{\delta}\circ\theta = \delta \ (\text{延拓}) \\ \tilde{\delta}(u) = \alpha \end{cases}$

唯一性：确定 $\tilde{\delta}(u)$，$\delta\circ\theta$ 即可确定 $\forall\ \delta(\alpha)$

存在性：

$K \xhookrightarrow{\delta} F$

Recall: P50 泛性质

$\tilde{\delta}: K = k[x]/(f(x)) \to F$

$$\overline{g(x)} \longmapsto \sigma'(g(x))$$

$$u=\bar{x} \longrightarrow \alpha$$

注：依赖 α 为根原因：$\operatorname{Ker}\sigma' = (f(x))$

Ex. $\mathbb{F}_3=\{\bar{0},\bar{1},\bar{2}\}$

$x^2+\bar{1}$ 不可约

$$\mathbb{F}_9 = \mathbb{F}_3[x]\big/(x^2+\bar{1})$$

算 $\mathbb{F}_9$ 乘法表

Ex. $K=\mathbb{R}[x]\big/(x^2+2)$

$$K \xrightarrow{\sim} \mathbb{C}$$

§1.6 欧氏整环 (Euclidean Domain)

定义. R 称为 ED

$\Leftrightarrow \exists \varphi: R^* = R \setminus \{0_R\} \to N$

$a \mapsto \varphi(a)$ size function

s.t. $\forall a, b \in R^*$, $\exists q, r \in R$

$b = qa + r$

$r = 0_R$ 或 $\varphi(r) < \varphi(a)$

$15 = 2 \times 6 + 3$

$= 3 \times 6 + (-3)$ q, r 不唯一

定理: ED $\to$ PID

取任意非零理想 I.

取 $p \in I$, s.t. $\varphi(p)$ 最小.

$\Rightarrow \forall a \in I,\ p \mid a$

故 $(p) = I$

例. Gauss 整数环

$$\mathbb{Z}[\sqrt{-1}] = \{a + b\sqrt{-1} \mid a, b \in \mathbb{Z}\}$$

$$\mathbb{Z}[\sqrt{-1}] \subseteq \mathbb{Q}[\sqrt{-1}]$$

norm map.

$$N : \mathbb{Q}(\sqrt{-1})^* \to \mathbb{Q}^+$$

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

$$N(zw) = N(z)N(w).$$

$$N : \mathbb{Z}[\sqrt{-1}] \to \mathbb{Z}^+$$

$\forall\ x, y \in \mathbb{Z}[\sqrt{-1}]$

$\frac{x}{y} = \alpha + \beta i \in \mathbb{Q}[\sqrt{-1}]$

$\exists\ m, n \in \mathbb{Z},\ |\alpha - m| \le \frac{1}{2},\ |\beta - n| \le \frac{1}{2}$

$\Rightarrow \frac{x}{y} = \underbrace{m + n\sqrt{-1}}_{q} + \underbrace{(\alpha - m) + (\beta - n)\sqrt{-1}}_{}$

$x = yq + \underbrace{((\alpha - m) + (\beta - n)\sqrt{-1})\,y}_{r}$

$\varphi(r) = \varphi((\alpha - m) + (\beta - n)\sqrt{-1})\,\varphi(y)$

$\le \frac{1}{2}\varphi(y) < \varphi(y)$

例. $\mathbb{Z}[\sqrt{-1}]$

$\gcd(4+7i, 3+4i)$ $\quad \frac{4+7i}{3+4i} = \frac{8}{5} + \frac{1}{5}i$

$= \gcd(2+i, 3+4i)$ $\qquad \frac{3+4i}{2+i} = 2+i$

$= \gcd(2+i, (2+i)^2)$

$= 2+i$

Ex. $a = qb + r$

$\Rightarrow \gcd(a,b) = \gcd(r,b)$

例. $\mathbb{Z}[\sqrt{-2}]$

$\mathbb{Z}[\sqrt{-2}] \subseteq \mathbb{Q}(\sqrt{-2})$

claim. $\mathbb{Z}[\sqrt{-2}]$ 为 ED.

$\left(\frac{1}{2}\right)^2 + \left(\frac{\sqrt{2}}{2}\right)^2 < 1$

Ex. $U(\mathbb{Z}[\sqrt{-2}]) = \{\pm 1\}$

Recall $\mathbb{Z}[\sqrt{-3}]$ 非 PID

Recall: $\mathbb{Z}[\sqrt{-3}]$ 非 PID

$\omega = -\frac{1}{2} + \frac{\sqrt{3}}{2} i$

$\mathbb{Z}[\omega] \subseteq \mathbb{Q}[\sqrt{-3}]$ Eisenstein 整数环

定理. $\mathbb{Z}[\omega]$ 为 ED

$$N(a+\omega b) = (a+b\omega)(a+b\bar{\omega})$$

$$= a^2+b^2+ab$$

$$\frac{x}{y} = a+b\omega$$

取 m, n, $|m-a|, |n-b| \le \frac{1}{2}$

$$N(r) = N(|m-a|+|n-b| i) N(y)$$

$$\le \frac{3}{4} N(y)$$

Ex.

$U(\mathbb{Z}[\omega])=\{\pm1,\pm\omega,\pm\omega^2\}$

$\mathbb{Z}\subseteq\mathbb{Q}\to F$, $[F:\mathbb{Q}]<+\infty$

$\alpha\in F$，称 Algebraic integer，若

∃首一整系数多项式 p. s.t.

$$p(\alpha)=0$$

$O_F=\{\alpha\mid\alpha$ 为 Algebraic integer$\}$

为 F 子环，且 $\mathrm{Frac}(O_F)=F$

Fact. $\mathbb{Z}\subseteq R$, $F=\mathrm{frac}(R)$，且 $R\subseteq O_F$

则 R 是 PID (or UFD)

$\Rightarrow R=O_F$ O_F 为 PID?

例. $\mathbb{Z}[\sqrt{2}] \subseteq \mathbb{Q}(\sqrt{2})$

$\mathbb{Z}[\sqrt{2}]$ 为ED

$N(a+b\sqrt{2}) = |a^2 - 2b^2|$

Ex. $\sigma: \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{2})$

$a+b\sqrt{2} \to a-b\sqrt{2}$

证明: ① σ 为自同构

② $\mathrm{Aut}(\mathbb{Q}(\sqrt{2})) = \{Id, \sigma\}$

③ $\nexists\ \delta \in \mathrm{Aut}(\mathbb{R})$, s.t. $\delta|_{\mathbb{Q}(\sqrt{2})} = \sigma$

Ex. $\mathbb{Z}[\sqrt{2}]$ 为ED.

Ex $U(\mathbb{Z}[\sqrt{2}])$ 为无限群

Ex. ... $\mathbb{Z}[\sqrt{2}]$ 为ED

Fact. (1) $\mathbb{Z}[\sqrt{3}]$ 为 ED

(2) $\mathbb{Z}[\sqrt{5}]$ 不为 ED

$\frac{1+\sqrt{5}}{2}$ 为 AI $\Rightarrow$ $\mathbb{Z}[\frac{1+\sqrt{5}}{2}]$ 为 ED.

---

§1.7 Gauss 整数.

关于 $\mathbb{Z}[\sqrt{-1}]$ 中素元

$\mathrm{Max}(R) \longleftrightarrow \{a \in R \text{ 素元}\}/\text{相伴}$

$\mathbb{Z}[\sqrt{-1}]$ 中

$m+n\sqrt{-1} \sim -m-n\sqrt{-1},\ -n+m\sqrt{-1},\ n-m\sqrt{-1}$

Ex. $1+i \in \mathbb{Z}[\sqrt{-1}]$ 为素元

Ex. $\mathbb{Z}[\sqrt{-1}]/(1+i) \xrightarrow{\sim} \mathbb{F}_2$

Ex. $\mathbb{Z}[\sqrt{-1}]/(2) \xrightarrow{\sim} R$

$\{0, 1, i, 1+i\}$

(1) R 几个元素

(2) 是否同构于 $\mathbb{Z}_4$?

关于 $\mathcal{O}_F$ 形成环的证明

设 $\alpha, \beta \in \mathcal{O}_F$，只需证 $\mathbb{Z}[\alpha, \beta] \in \mathcal{O}_F$

设 $\gamma = p(\alpha, \beta)$

$$= (p_1 \cdots p_{mn}) \begin{pmatrix} 1 \\ \vdots \\ \alpha^n \\ \alpha^n \beta \\ \vdots \\ \alpha^n \beta^m \end{pmatrix}$$

由于 α, β 可被首一多项式化零，故

$$\gamma\begin{pmatrix}\vdots\\ \alpha^n\\ \vdots\\ \alpha^n\beta^m\end{pmatrix}=(s_{ij})_{1\le i,j\le mn}\begin{pmatrix}\alpha\\ \vdots\\ \alpha^n\\ \vdots\\ \alpha^n\beta^m\end{pmatrix}$$

$s_{ij}\in\mathbb{Z}$

设 $\varphi(x)=|xI-(s_{ij})|$

$$\Rightarrow\quad \varphi(\gamma)\begin{pmatrix}1\\ \vdots\\ \alpha^n\\ \vdots\\ \alpha^n\beta^m\end{pmatrix}=\varphi((s_{ij}))\begin{pmatrix}1\\ \vdots\\ \alpha^n\\ \vdots\\ \alpha^n\beta^m\end{pmatrix}=0$$

$\varphi(\gamma)=0$

引理. $z\in\mathbb{Z}[i]$, $N(z)$为素数

$\Rightarrow$ z为Gauss素数.

证明: z不可约

引理: $p=4k+3$ 素数

$\Rightarrow$ p 为 Gauss 素数.

证明: 否则 p 可约

$p = a^2 + b^2$, $p > a, b > 0$

矛盾.

设 $p = 4k+1$ 奇素, 则 $p = a^2 + b^2$, a.b. 唯一

证明: 在 $\mathbb{F}_p$ 中, $x^2 = -1$ 有解

$\mathbb{F}_p^*$ $p-1$ 阶循环群

$\Rightarrow$ 必有四阶元

Claim: $\mathbb{Z}[i]/(p) \cong \mathbb{F}_p[x]/(x^2+1)$ 非整环

$\Rightarrow p$ 不是 Gauss 素数

$\Rightarrow p$ 可约，$p = x \cdot y$

$\Rightarrow N(x) = N(y) = p$. ✓.

$p = a^2 + b^2$.

$a.b.$ 惟一性：$x.y$ 不可约，分解惟一，

$\Rightarrow a, b.$ 惟一

Claim 的证明.

Step 1. $\mathbb{Z}[i] \cong \mathbb{Z}[x]/(x^2+1)$.

$\mathbb{Z} \xhookrightarrow{\text{inc}} \mathbb{Z}[i]$.

由泛性质，

$$\mathbb{Z}[x] \xrightarrow{\phi} \mathbb{Z}[i]$$

$$x \longrightarrow i$$ 满射.

Ex. $\ker\phi = (x^2+1)$.

step 2.

$$\mathbb{Z}[x]/(x^2+1) \xrightarrow{\tilde{\phi}} \mathbb{Z}[i]$$

$$(p, x^2+1)/(x^2+1) \xrightarrow{\Phi} (p)$$

Ex. $\theta: R \xrightarrow{\sim} S$

$I \lhd R$, 则 $\theta(I)$ 理想

$$R/I \xrightarrow{\sim} S/\theta(I)$$

$$\mathbb{Z}[x]/(x^2+1) \Big/ (x^2+1, p)/(x^2+1) \xrightarrow{\sim} \mathbb{Z}[x]/(x^2+1, p)$$

$$\xrightarrow{\sim} \mathbb{Z}[i]/(p)$$

step 3. $\mathbb{Z}[x]/(p) \xrightarrow[\sim]{\varphi} \mathbb{F}_p[x]$

考虑 $\mathbb{Z}[x] \longrightarrow \mathbb{F}_p[x]$

$$\sum a_i x^i \mapsto \sum \bar{a}_i x^i$$

$$\varphi\left((x^2+1,p)/(p) \right) = (x^2+\bar{1})$$

$$\mathbb{Z}[x]/(p) \Big/ (x^2+1,p)/(p) \xrightarrow{\bar{\varphi}} \mathbb{F}_p[x]/(x^2+\bar{1})$$

$$\big\downarrow\wr$$

$$\mathbb{Z}[x]/(x^2+1,p)$$

$$\big\downarrow\wr$$

$$\mathbb{Z}[x]/(x^2+1) \Big/ (x^2+1,p)/(x^2+1)$$

$$\big\downarrow\wr$$

$\Downarrow$

$$\mathbb{Z}[i]/(p)$$

$$\overline{m+ni} \longmapsto \overline{(\bar{m}+\bar{n}x)}$$

定理. Gauss素数分类（不区分相伴）.

(1) $1+i$

(2) $p=4k+3$，奇素.

(3) $a\pm bi$，$a^2+b^2=p$，$a<b$

证明：(1)(2)(3) 均为 Gauss素数.

· 互不相伴.

· 不遗漏：

设 $z \in \mathbb{Z}[i]$ Gauss素数.

$z \mid N(z) = \prod p_i^{\alpha_i}$，$p_i$ 素.

$\nu(z) \sim \prod z_i$, $z_i \in (1), (2), (3)$

$\Rightarrow z \sim z_i$

二平方和定理.

$N = 2^l \prod p_i^{\alpha_i}$

对$\forall p_i \equiv 3 \bmod 4$, α_i偶

$\Leftrightarrow N = a^2 + b^2$

$\Leftarrow$ 平凡

$\Rightarrow$: 拆分.

例: $z = 29 - 2i$

$N(z) = 5 \times 13^2$

$5 = 2^2 + 1^2 \quad 13 = 2^2 + 3^2$

$2-3i \mid z$ 或 $2+3i \mid z$

$z / (2+3i) = (52 - 91i)/13 = 4 - 7i$

$4 - 7i / 2+3i = -13 - 26i / 13 = -1 - 2i$

问: $\operatorname{Spec} \mathbb{Z}[i] = ?$

$= \{(0)\} \cup \operatorname{Max}(\mathbb{Z}[i])$

$= \{0\} \cup \{(1+i)\} \cup \{(p) \mid p = 4k+3\}$

$\cup \{(a+bi) \mid a^2+b^2 = 4k+1\}$

Ex. $R \overset{inc}{\hookrightarrow} S$ 子环

$$\begin{aligned} \operatorname{Spec} S &\longrightarrow \operatorname{Spec} R \\ \mathfrak{q} &\longmapsto R \cap \mathfrak{q} \end{aligned}$$

$R \cap \mathfrak{q} \in \operatorname{Spec} R$

且 $R/(\mathfrak{q} \cap R) \hookrightarrow S/\mathfrak{q}$

Recall: $\mathbb{Z} \hookrightarrow \mathbb{Z}[i]$

$\operatorname{Spec} \mathbb{Z}[i] \to \operatorname{Spec} \mathbb{Z}$

Ex. $(1+i) \cap \mathbb{Z} = 2\mathbb{Z}$

$(p) \cap \mathbb{Z} = p\mathbb{Z} \quad p = 4k+3$

$(a+bi) \cap \mathbb{Z} = p\mathbb{Z} \quad p = a^2+b^2$

(1) $p = 4k+3$

$\mathbb{Z}[i]/(p) \xrightarrow{\sim} \mathbb{F}_p[x]/(x^2+1). \quad \mathbb{F}_{p^2}$

(2) $p=a^2+b^2$

$\mathbb{Z}[i]/(a+bi) \xrightarrow{\sim} \mathbb{F}_p$

Ex. 证明 (2)

---

§1.8 UFD (uniquely factorial domain).

定义. R 整环. 称 UFD, 若

(1) ∃ 不可约分解.

(2) 唯一:

$a=c_1\cdots c_n$

$=c_1'\cdots c_m'$

本质上唯一:

① $n=m$

② 相差一个置换意义下 $c_i = c_i'$

Fact. (1) 不可约 $\Leftrightarrow$ 素元.

设 a 不可约 $a \mid bc$

$a \cdot d = b \cdot c$.

$a \cdot d_1 \cdots d_s = b_1 \cdots b_r \cdot c_1 \cdots c_t$

$\Rightarrow a$ 与 $\{b_i\} \cup \{c_i\}$ 中某个元素相伴

(2) 有标准分解.（本质：相伴作为等价关系，选取完全代表元系）.

$\forall a \in R$

$a = u \prod_{i=1}^{n} p_i^{r_i} \quad u \in U(R)$

且 $\{p_i\}$ 两两...

相伴意义下相等的

a有 $\prod_{i=1}^{n}(r_i+1)$ 个因子

(3) $\exists \gcd$.

引理. (1) $\gcd\left(\frac{a}{\gcd(a,b)}, \frac{b}{\gcd(a,b)}\right)=1$

(2) $\gcd(a,b)=1 \quad a \mid bc$

$\Rightarrow a \mid c$

(4) $K=\mathrm{Frac}(R)$.

既约表达: $\frac{a'}{b'}\in K$, $\gcd(a',b')=1$

Ex. $\frac{a}{b} = \frac{c}{d}$ in K

$\gcd(a,b) \sim 1 \sim \gcd(c,d)$

$\Rightarrow a \sim c,\ b \sim d$

不可约分解.唯一性:

Noether环: $\forall I \trianglelefteq R$ 为有限生成

Hilbert基定理:

R Noether环

$\Rightarrow R[x_1, \cdots, x_n]$ 及其商环均 Noether.

定理. R 为 Noetherian integral domain $\Rightarrow$ R 上有不可约分解.

$a = a_1 a_2$ $\quad$ a_1 无分解

$a_1 = a_{11} a_{12}$ $\quad$ $a_{11} \cdots$

$(a_1) \subsetneq (a_{11}) \subsetneq (a_{111}) \cdots$

Ex. R 为 Noether 环

$\Rightarrow$ R 中无理想严格升链:

$I_1 \subsetneq I_2 \subsetneq \cdots$

Ex. $R[x]/(c) \xrightarrow{\sim} (R/Rc)[x]$

Gauss 引理 R UFD $\Rightarrow$ $R[x]$ UFD

本原·本原 = 本原

例 x, y 变量.

$$k[x,y] = \sum a_{ij} x^i y^j$$

$$\shortparallel$$

$$(k[x])[y] \Rightarrow \text{为 UFD}$$

Claim. $y^3 - x^2$ 在 $k[x,y]$ 中不可约

$\shortparallel$

本原 $\quad (k[x])[y]$

$$y^3-x^2=(y-a(x))(y+a(x))$$

claim y^3-x^2 在 $(k(x))[y]$ 不可约

令 $A=k[x,y]/(y^3-x^2)$ integral.

Ex. (1) 找 A 线性基

(2) A UFD?

(3) $S=\{a_0+a_2t^2+\cdots\}_{一次项为0} \subseteq k[x]$ 子环

证明: $S\cong A$

Eisenstein 判别法.

R UFD.

$$a(x)=\sum_{i=0}^{n} a_i x^i$$

$\exists\, p$ R中素元

$p \nmid c_n$, $p \mid c_i$, $n > i \geq 0$, $p^2 \nmid c_0$

$\Rightarrow a(x)$不可约

证明：考虑 $R[x]/(p)$

例. x^n-2 不可约 in $\mathbb{Q}[x]$

$\Rightarrow$ 极小多项式

Claim.

$\mathbb{R}$中 $\{1, \sqrt[n]{2}, \dots, \sqrt[n]{2^{n-1}}\}$ $\mathbb{Q}$ 线性无关

---

p 素.

$u(x)=x^{p-1}+\cdots+x+1$ 在 $\mathbb{Q}$ 不可约

$$= \frac{x^n-1}{x-1}$$

$f(x)\in\mathbb{Z}[x]$, $f(x+1)$: 将 x 换为 $x+1$, 关于 x 展开.

Fact: f 不可约 $\Longleftrightarrow$ $f(x+1)$ 不可约

P102. 1, 4, 7, 12

$\mathbb{Z}[x] \to \mathbb{Z}[x]$

$f(x) \overset{\theta}{\mapsto} f(x+1)$ 为环同构

$$u(x+1) = \frac{(x+1)^p - 1}{x} = \sum_{i=0}^{p-1} C_p^{i+1} x^i$$

可用 Eisenstein 判别法

补充：R, S 环

$R \times S = \{(r,s) \mid r \in R, s \in S\}$

direct product (较和，区别于 Tensor)

按分量运算。

Ex. $R \times S \xrightarrow{\text{project}} S$ 满同态

$R\times S \big/ R\times\{0_S\} \longrightarrow S$

中国剩余定理.

$I_1,\dots,I_n \lhd R$, R环

$I_i+I_j=R$ (Bezout定理,互素)

对同态

$$R \xrightarrow{\theta} \prod_{j=1}^{n} R/I_j$$

$$x \longrightarrow (x+I_1,\dots,x+I_n)$$

诱导同构:

$$R/\ \ \xrightarrow{\sim} \prod^{n} R/I$$

$$R/\bigcap_{i=1}^{n} I_j \longrightarrow \prod_{j=1}^{n} R/I_j$$

且 $\bigcap_{i=1}^{n} I_j = I_1 I_2 \cdots\cdots I_n$

证: $x \in \ker\theta$

$\Leftrightarrow \forall j,\ x + I_j = 0 + I_j$

$\Leftrightarrow \forall j,\ x \in I_j$

$\Leftrightarrow x \in \bigcap_{j=1}^{n} I_j$

仅需证此为满射

$\Leftrightarrow \forall (a_1 + I_1, a_2 + I_2, \cdots, a_n + I_n)$

$\exists b,\quad b \equiv a_j \mod I_j$

先解 $\begin{cases} b \equiv 1 \mod I_1 \end{cases}$

$$\begin{cases} b \equiv 0 \mod I_2 \\ \vdots \\ b \equiv 0 \mod I_n \end{cases}$$

Claim. $I_1 + I_2 \cdots I_n = R$

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

$\Rightarrow \quad R = I_1 + I_2 I_3$ $\qquad \underline{\underline{a+b=1}}$.

归纳得

$R = I_1 + I_2 \cdots I_n$

Ex. 若 $I + J = R$

则 $I \cap J = IJ$

添根构造

$f \in k[x]$ 不可约 d次

$\mathrm{Root}_k(f) = \emptyset$

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

$\bar{x} = u \in K$

① K 为 k 一线性空间

一组基 $\{\bar{1}, u, \dots, u^{d-1}\}$

② $f(u) = 0$

证: $f(u) = u^d + a_{d-1}u^{d-1} + \dots + a_0$

$= \overline{x^d + a_{d-1}x^{d-1} + \dots + a_0} = 0_K$

$f(X) = (X - u)\,g(X)$ in $K[X]$

欲使f分裂需添根构造扩张。

§2. 域扩张与单扩张.

定义.
域扩张 $k \overset{\theta}{\hookrightarrow} K$
(非平凡同态自动单)

记 K/k

有理函数域 $k(x) = \mathrm{Frac}(k[x])$

$k \hookrightarrow k(x)$

Fact. $k \overset{\theta}{\hookrightarrow} K$

对 K 自然成 k 线性空间

定义. $\theta: k \hookrightarrow K$

$\theta': k \hookrightarrow K'$

称 θ, θ' 同构, 若 $\exists$ 域同构

$\varphi: K \to K'$

且 $\varphi \circ \theta = \theta'$

Ex.

$$\begin{tikzcd}
K \arrow[rr, "\varphi"] & & K' \\
& k \arrow[ul, "\theta"] \arrow[ur, "\theta'"'] &
\end{tikzcd}$$

φ 域扩张同构

则 φ 为 k 线性空间同构

[illegible]

定义：θ 的自同构 φ

$$\begin{tikzcd} k \arrow[r, "\theta"] \arrow[dr, "\theta"'] & K \arrow[d, "\varphi"] \\ & K \end{tikzcd}$$

$$\varphi \circ \theta = \theta$$

即 $\theta \in \mathrm{Aut}(K)$ 且保持 k

记作 $\mathrm{Aut}(K/k) \le \mathrm{Aut}(K)$

记号.　$R \subseteq S$

$R[x] =$ S中包含 R, x 的最小子环

$= \{ \sum a_i x^i \mid a_i \in R \}$

$= \left\{ \sum r_i x^i \,\middle|\, r_i \in R \right\}$

注：为何最小子环，子域总存在？

子环，子域的任意交均为子环，子域！

$k(\alpha)$ = K 中包含 k, α 的最小子域.

$$= \left\{ \sum a_i\alpha^i \Big/ \sum b_i\alpha^i \,\middle|\, \begin{array}{l} a_i, b_i \in k \\ \sum b_i\alpha^i \neq 0 \end{array} \right\}$$

Fact. $R[x_1, x_2] = (R[x_1])[x_2]$

$$k(\alpha,\beta) = \left\{ \frac{\sum a_{ij}\alpha^i\beta^j}{\sum b_{ij}\alpha^i\beta^j} \,\middle|\, \sum b_{ij}\alpha^i\beta^j \neq 0 \right\}$$

Fact: $k(\alpha_1, \alpha_2) = (k(\alpha_1))(\alpha_2)$

定义. K/k 是扩张

定义. K/k 单扩张

$\Leftrightarrow \exists \alpha \in K$ s.t. $K = k(\alpha)$

称根构造为单扩张

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

定义 K/k, $\alpha \in K$

α 为 k 上代数元, 若

$\exists f \in k[x]$, $f \neq 0$, $f(\alpha) = 0$

否则 α 为超越元

i.e. π, e 在 $\mathbb{Q}$ 上超越

$k \hookrightarrow K$

α 在 k 上超越

定理 α 在 k 上代数 $\Rightarrow \exists!$ 首一不可约的多项式 f，① $f(\alpha)=0$ ② $\forall g, g(\alpha)=0$，则 $f \mid g$

称 f 为极小多项式

证：$ev_\alpha : k[x] \to K$

$$\ker(ev_\alpha) = (f)$$

$$k[x]/(f) \xrightarrow{\sim} k[\alpha] \text{ 整环}$$

$\Rightarrow (f) \in \operatorname{Spec}(k[x])$

f 不可约

$k[\alpha]$为域

例 $\mathbb{C}/\mathbb{R}$

i 极小 x^2+1

Ex. $\theta: k \hookrightarrow K$

$\theta': k \hookrightarrow K'$

$\phi: K \to K'$ 域扩张同构

$\Rightarrow$ (1) α在k上代数

$\Leftrightarrow \phi(\alpha)$ 代数

(2) $\alpha, \phi(\alpha)$ 同极小多项式

极...

域扩张结构定理

(1) α 在 k 上代数，极小多项式 d 次 $\to f$

$$\Rightarrow \dim_k k(\alpha)=d$$

基 $\{1,\alpha,\cdots,\alpha^{d-1}\}$

且同构于 $f \hookrightarrow k[x]/(f)$

(2) α 超越，则

(1) $\dim_k k(\alpha)=\infty$

(2) $k[\alpha]\subsetneq k(\alpha)$

(3) $k\hookrightarrow k(\alpha)$

$k\hookrightarrow k(x)$ 同构

$k \hookrightarrow K$

$\sqrt[3]{2}\omega$ $\qquad \dim_{\mathbb{Q}} \mathbb{Q}(\sqrt[3]{2}\omega)=3$

$\underline{x^3-2}$

$$\begin{tikzcd}
\mathbb{Q}(\sqrt[3]{2}\omega) & \mathbb{Q}[x]/(x^3-2) \arrow[l, "\sim"'] \\
& \mathbb{Q}(\sqrt[3]{2}) \arrow[u, "\wr"]
\end{tikzcd}$$

$\sqrt[3]{2} \to x \to \sqrt[3]{2}\omega$

域的代数扩张

K/k 称代数扩张，若 $\forall \alpha \in K$，α 代数

引理：

引理

若 $\dim_k K < +\infty$

则 K 为代数扩张.

证: 一步步可取 $\dim_{k[\alpha_1,\cdots,\alpha_n]} K = 1$

$\Rightarrow K = k[\alpha_1,\cdots,\alpha_m]$

<u>维数公式</u>. 非平凡, 考试要求证明!

$k \subseteq E \subseteq K$ $\quad K/E$, E/k 有限维

$\Rightarrow \dim_k K = \dim_E K \cdot \dim_k E$

由 Galois 对应

此定理对应 Galois 定理(陪集个数)

$k \subseteq K = k(\alpha_1, \alpha_2)$

记号: $\dim_k K = [K : k]$

$[K : k(\alpha_1)] = \deg$ α_2 在 $k(\alpha_1)$ 上极小多项式

$$[K : k] = [K : k(\alpha_1)][k(\alpha_1) : k]$$

维度公式 证明. $k \subseteq E \subseteq K$ Tower

$$\begin{array}{c} K \\ | \\ E \\ | \\ k \end{array}$$

$$[K : k] = [K : E][E : k]$$

E/k k-basis $\{u_1, \dots, u_n\}$

K/E E-basis $\{v_1, \dots, v_m\}$

Claim. K/k k-basis $\{u_i v_j\}_{\substack{n \geq i \geq 1 \\ m \geq j \geq 1}}$

seep 1. 可生成 K. ✓.

seep 2. 线性无关. ✓

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

$$\mathbb{Q} \xrightarrow{3} \mathbb{Q}(\sqrt[3]{2}) \xrightarrow{2} \mathbb{Q}(\sqrt[3]{2})(\omega)$$

$$\omega \notin \mathbb{Q}(\sqrt[3]{2}) \Rightarrow [\mathbb{Q}(\sqrt[3]{2})(\omega) : \mathbb{Q}(\sqrt[3]{2})] \leq 2$$

$$\Rightarrow \quad = 2.$$

Ex: $\mathbb{Q} \subseteq \mathbb{Q}(\omega) \subseteq K$

求 $\sqrt[3]{2}$ 在 $\mathbb{Q}(\omega)$ 上极小多项式.

Ex: K/k 有限维, $\alpha \in K$

α 在 k 上极小多项式 f

$\Rightarrow \deg f \mid [K:k]$

定理：K/k

K/k 有限维 $\Leftrightarrow$ 有限生成代数扩张

命题：

$k \subseteq E \subseteq K$

K/k 代数 $\Leftrightarrow$ K/E，E/k 代数

$\Rightarrow$：显然

$\Leftarrow$：找代零多项式，维数有限

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

$\Rightarrow E$ 子域

证明：

包含在某个有限维扩张

Ex. $f(x)$ 为 α 极小多项式 $\deg f = n$

$\Rightarrow f(\frac{1}{x})x^n$ 为 $\frac{1}{\alpha}$ 极小多项式

如何构造 $\alpha+\beta$, $\alpha\beta$ 等极小多项式?

将 $x \in k(\alpha,\beta)$ 看作线性映射

$l_x : k(\alpha,\beta) \to k(\alpha,\beta)$

$y \mapsto xy$

随后 Cayley-hamilton 构造

$\{ \quad k \mid x$ 在 k 上代数$\} \subseteq K$

Ex. $k \subseteq E = \{x \in K \mid x$ 在 k 上代数$\} \subsetneq K$
$\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad \ni u$

取 $u \notin E$, $u \in K$

$\Rightarrow$ u 在 E 上超越

此时称 E 为 k 在 K 中代数闭包.

定义. 域 K 代数封闭

$\Rightarrow$ $\forall$ 代数扩张 E/K

$\dim_K E = 1$

Ex. K 代数闭 $\Rightarrow$ $|K| = +\infty$

(考虑 $\prod_{\lambda \in K} (x - \lambda) + 1$).

代数基本定理

代数基本定理

$\mathbb{C}$ 为代数封闭域

即 $\forall \mathbb{C}[x]$ 在 $\mathbb{C}$ 上分裂

证明：$\mathbb{R} \subseteq \mathbb{C} \subseteq K$

$K/\mathbb{C}$ 代数扩张

$\Rightarrow K/\mathbb{R}$ 为代数扩张

$\mathbb{R}$ 上奇次多项式有根：$[K:\mathbb{R}]$ 偶

$\mathbb{C}$ 上二次 有根：$[K:\mathbb{C}] \neq 2$

$[K:\mathbb{R}] = 2[K:\mathbb{C}]$

随后作 $Gal(K/\mathbb{R})$，用 Sylow 定理，Galois 对应

Ex. $\mathbb{Q} \subseteq \mathbb{C}$

$\overline{\mathbb{Q}} = \{\alpha \in \mathbb{C} \mid \alpha$ 在 $\mathbb{Q}$ 代数$\}$

则 $\overline{\mathbb{Q}}$ 代数封闭

Fact. $\forall k$, $\exists\, \overline{k}/k$ 代数扩张

$\overline{k}$ 代数封闭

why?

$$\overline{\mathbb{F}_p} = \bigcup_{n=1}^{\infty} \mathbb{F}_{p^n}$$

延拓问题.

$$\begin{tikzcd} E \arrow[r, dashed, "\delta"] & E' \\ k \arrow[u, hook, "\alpha"] \arrow[r, "\sigma"] & k' \arrow[u, hook] \end{tikzcd}$$

σ 同构

[illegible]

能否延拓?

α 极小多项式 $f \in k[x]$.

$\sigma(f)$ 为按系数对应

(1) 若 $\beta \in \mathrm{Root}_{E'}(\sigma(f))$

则 $\exists!\ \tilde{\sigma}$, s.t.

$\tilde{\sigma}(\alpha) = \beta$

$\tilde{\sigma}\big|_{k} = \sigma$

(2) 这样的延拓恰有 $|\mathrm{Root}_{E'}(\sigma(f))|$ 个

$$\begin{tikzcd}
E \\
k(\alpha) \arrow[u, hook] \arrow[r, "\tilde{\sigma}"] & k(\beta) \\
f \arrow[u, dash] & \sigma(f) \arrow[u, dash]
\end{tikzcd}$$

$$k \xrightarrow[\sigma]{\sim} k'$$

∃!性:

$$\begin{tikzcd}
k(\alpha) & k[x]/(f) \arrow[l, "\sim"'] \arrow[d, "\wr"] & k \arrow[l, hook'] \arrow[d, "\wr\,\sigma"] \\
k'(\beta) & k'[x]/(f') \arrow[l, "\sim"'] & k' \arrow[l, hook']
\end{tikzcd}$$

借助添根构造同构

那么我们有 $\overline{\mathbb{F}_p}=\bigcup_{n=1}^{\infty}\mathbb{F}_{p^n}$.

命题 2.3.4 (E. Artin). 任何域 F 都存在一个代数闭域 E 作为其扩张.

证明: 我们首先构造一个 F 的一个域扩张 E_1 使得任意次数大于等于 1 的 $f\in F[x]$ 在 E_1 中都有根: 考虑集合 $\mathfrak{X}=\{x_f\mid f\in F[x],\deg(f)\geq 1\}$, 以及以集合 $\mathfrak{X}$ 为未定元的多项式环 $F[\mathfrak{X}]$. 令 $I=(f(x_f))$, 我们断言 I 是 $F[\mathfrak{X}]$ 的一个真理想. 假设 $I=F[\mathfrak{X}]$, 则有

$$\sum_{i=1}^{n}g_if_i(x_{f_i})=1$$

由于只有有限多个 f_i, 那么根据分裂域存在性的证明过程不难构造 F 的一个域扩张 F' 使得每一个 f_i 在 F' 中都有根 u_i. 考虑 $F[\mathfrak{X}]\to F'$, 定义为 $x_{f_i}\mapsto u_i$, 其余的 x_f 被映成零, 则考虑上述等式在这个映射下的结果, 我们有 $0=1$, 矛盾. 因此 I 是真理想, 我们取 $\mathfrak{m}$ 是包含 I 的一个极大理想, 令 $E_1=F[\mathfrak{X}]/\mathfrak{m}$, 则

$$F\hookrightarrow F[\mathfrak{X}]\to F[\mathfrak{X}]/\mathfrak{m}=E_1$$

我们用 $\overline{x}_f$ 记 x_f 在 E_1 中的像, 可以发现其为 $f(x)$ 的一个根. 不断进行如上操作则有

$$F=E_0\subseteq E_1\subseteq E_2\subseteq\dots$$

令 $E=\bigcup_{i=0}^{\infty}E_i$, 我们证明 E 是代数闭的. 任取多项式 $f\in E[x]$, 那么其系数总会落在某一个 E_n 中, 则它在 E_{n+1} 中有根, 即在 E_{n+1} 中有分解

$$f=(x-u_1)f_1$$

其中 $f_1\in E_{n+1}[x]$, 继续对 f_1 使用如上操作即可. □

命题 2.3.5. F 是域, E 是代数闭域, 并且有嵌入 $\tau\colon F\hookrightarrow E$. 如果 K/F 是代数扩张, 则 τ 可以延拓成 $\tau'\colon K\to E$. 特别地, 如果 K 是代数闭域, 那么 $\tau'\colon K\to E$ 是同构.

证明: 任取 $u\in K$, α 在 F 上的极小多项式记作 $P_{\alpha,F}$, 由于 E 是代数闭域, 那么 $\tau(P_{\alpha,F})$ 在 E 中存在根 β, 那么根据引理1.2.4可知 σ 可以延拓到 $F(\alpha)\to E$. 用 M 记所有的 (K',τ'), 其中 K' 是 K 的包含 F 的子域, τ' 是 τ 的延拓. 并且定义偏序关系 $(K_1',\tau_1')\leq(K_2',\tau_2')$ 为 $K_1'\subseteq K_2'$ 并且 $\tau_2'|_{K_1'}=\tau_1'$. 我们已经知道 M 非空, 从而根据祖恩引理存在极大元 K', 并且再次利用引理1.2.4可知 K' 就是 K. □

定理 2.3.6. 域 F 的代数闭包 $\bar{F}$ 存在且唯一 *(在同构意义下)*.

证明: 存在性: 根据命题2.3.4, 存在代数闭域 E 使得其是 F 的扩张, 定义

$$\bar{F}:=\{\alpha\in E\mid\alpha\text{ 在 }F\text{ 上代数}\}$$

那么有 $\bar{F}$ 是 F 的代数扩张. 并且 $\bar{F}$ 是代数闭域, 因为任取 $f(x)=a_nx^n+\cdots+a_0\in\bar{F}[x]$, 根据韦达定理可知其根在 $F(a_0,\dots,a_n)$ 上面代数, 从而在 F 上代数, 进而属于 $\bar{F}$.

唯一性: 根据命题2.3.5即可. □

§2.3. 分裂域

定义. $f(x) \in k[x]$ 的分裂域 E, 若

(1) $f(x)$ split over E.

$$f(x) = \prod_{i=1}^{n} (x-\alpha_i), \ \alpha_i \in E$$

(2) $E = k(\alpha_1, \cdots, \alpha_n)$

问题: 存在性, 唯一性.

∃: 不断作添根构造

定义. $\mathrm{Gal}(f(x)) = \mathrm{Aut}(E/k)$

$$= \{\sigma \in \mathrm{Aut}(E) \mid \sigma|_k = \mathrm{Id}\}$$

Fact. $\forall \alpha \in \mathrm{Root}_E(f)$

$\forall \sigma \in \mathrm{Gal}(f(x))$

$\Rightarrow \sigma(\alpha) \in \mathrm{Root}_E(f)$

分裂域的唯一性.

$\sigma: k \to k'$ 域同构

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

取 $k \hookrightarrow E$ f分裂域

$k' \hookrightarrow E'$ $\sigma(f)$分裂域

则σ可延拓为δ

$E \xrightarrow{\delta} E'$ 域同构

这样的 σ 至多有 $\dim_k E$ 个

推论. (1) 分裂域的唯一性

取 σ 为 Id.

(2) $|\mathrm{Gal}(f)| \le \dim_k E$

证明: 对 $\dim_k E$ 归纳

若 $\dim_k E = 1$ ✓

$\dim_k E > 1$

$$f = \prod_{i=1}^{n} (x-\alpha_i)$$

$\alpha_1 \notin K$

α_1在K上极小多项式 g

$\Rightarrow g \mid f,\ \sigma(g) \mid \sigma(f)$

$$\begin{tikzcd}
E & E' \\
K(\alpha_1) \arrow[u, hook] \arrow[r, "\sim"] & K'(\sigma(\alpha_1)) \arrow[u, hook] \\
K \arrow[u, hook] \arrow[r, "\sim", "\sigma"'] & K' \arrow[u, hook]
\end{tikzcd}$$

关键引理

$\mathrm{Root}_{E'}(\sigma(g)) \neq \emptyset$

$\ni$

β_1

构造 $K(\alpha_1) \xrightarrow[\sigma_1]{\sim} K(\beta_1)$

Claim. E为$k(\alpha_1)$上关于$f(x)$的分裂域

$$\dim_{k(\alpha_1)} E < \dim_k E$$

由归纳假设.

$$\left| \sigma\text{的个数} \right| \le \underset{\le \deg g}{\mathrm{Root}_E(g)} \cdot \dim_{k(\alpha_1)} E$$

$$\le \dim_k k(\alpha_1) \dim_{k(\alpha_1)} E$$

$$= \dim_k E$$

取等：f可分

不可约因子无重根

例

求 $\mathbb{Q}$ 上 $\mathrm{Gal}(x^3-2)$

$\mathbb{Q}(\sqrt[3]{2})$

$\sqrt[3]{2} \to \sqrt[3]{2},\ \omega\sqrt[3]{2},\ \omega^2\sqrt[3]{2}$

$\sigma_1 : \mathbb{Q}(\sqrt[3]{2}) \to \mathbb{Q}(\beta_j)$

$\beta_0 \quad \beta_1 \quad \beta_2$

$\sqrt[3]{2},\ \omega\sqrt[3]{2},\ \omega^2\sqrt[3]{2} \qquad 3$

$\mathrm{Root}_E(x^2+x+1) = \{\omega, \omega^2\}$

$\sigma_2 : \mathbb{Q}(\sqrt[3]{2}) \to \mathbb{Q}_1(\beta_2)$

$\alpha_1 \quad \alpha_2$

$\omega,\ \omega^2 \qquad 2$

$\mathrm{Aut}(E/\mathbb{Q}) = \left\{ \delta_{ij} \;\middle|\; \begin{array}{l} \delta_{ij}(\sqrt[3]{2}) = \omega^i\sqrt[3]{2} \\ \delta_{ij}(\omega) = \omega^j \end{array} \right\}$

$2 \geq i \geq 0$

$2 \geq j \geq 1$

Ex. 算其乘法表

例 $\mathbb{F}_2 \hookrightarrow \mathbb{F}_4 = \mathbb{F}_2[x] / (x^2+x+1)$

$$x^2+x+1 = (x-u)(x-u-1)$$

$\delta_0: \quad u \to u$

$\delta_1: \quad u \to u+1$

二阶群

Ex. $\forall a \in \mathbb{F}_4$

$\delta_1(a) = a^2$ (Frobenius automorphism)

定义. $f(x) \in F[x]$

有重根，若 $\exists$ 扩 $E \supset F$, $a \in E$

s.t. $(x-a)^2 \mid f(x)$

例如: $(x^2+1)^2$

问: 如何不作扩域, 判定是否重根

形式微商

$$f(x) = \sum_{i=0}^{n} a_i x^i$$

$$f'(x) = \sum_{i=1}^{n} \underline{i a_i} x^{i-1}$$ 此为 $\mathbb{Z}$ module 数乘.

Claim $(fg)' = f'g + fg'$

Claim:

证. 若 $n1 \neq 0$

$\deg f' = \deg f - 1$

若 char $\bar{F} = p$

$(x^p - x)' = -1$

Fact. f 有重根 $\Leftrightarrow$

$(f', f) \neq 1$ ✓

有重根 $\Rightarrow$

$(f', f) \neq$

定义. f 可分 (separable)

若其不可约因子无重根

都是不可约的

引理 若 $\mathrm{char}\,k=0$

$\Rightarrow$ 所有多项式可分

定理 f 可分 $\Leftrightarrow |\mathrm{Gal}_k(f)| = \dim_k E$

证: $\Rightarrow$ ✓

$\Leftarrow$ ✓

Ex. $f\in k[x]$ $k\subseteq K$

f 在 k 上可分 $\Leftrightarrow$ f 在 K 上可分

(3) f 可分 $\Leftrightarrow |\mathrm{Gal}_k(f)| = \dim_k E$

其中 E 为 f 在 k 上分裂域

定义:

$f \in k[x]$

E/k f 分裂域.

记 $\mathrm{Gal}_k(f) = \mathrm{Aut}(E/k)$

有限　　　　无限

§2.4. 有限域.

有限域 $|E| < +\infty$

① $\mathrm{char}\, E = p > 0$

② $\mathbb{F}_p \hookrightarrow E$

$1 \longrightarrow 1_E$ (可以认为包含).

$E/\mathbb{F}_p$ 域扩张

③ E 可看作 $\mathbb{F}_p$ 线性空间

④ $\dim_{\mathbb{F}_p} E = n$

线性空间同构：$E \cong \mathbb{F}_p^n$

定义.
$$E \xrightarrow{\sigma} E$$
$$a \longrightarrow a^p$$

Claim. $\sigma \in \mathrm{Aut}(E)$

Frobenius 自同构

$$\sigma(a+b) = (a+b)^p = \sigma(a) + \sigma(b)$$

$$\sigma(ab) = a^p b^p = \sigma(a)\sigma(b)$$

域同态 $\Rightarrow$ 单射 $\Rightarrow$ 满射.

Fermat $\Rightarrow$ $\sigma|_{\mathbb{F}_p} = \mathrm{Id}$.

$|E| = p^n$.

$E^\times = E \setminus \{0_E\}$. 单位群.

也为分循环群

证明: Abelian group 结构

$a^{(p^n-1)} = 1$, $a \in E^\times$

$\Rightarrow \forall b \in E$

$b^{p^n} = b$.

定理 $\forall n \geq 1$

$\exists!$ p^n阶有限域.

证明:

唯一性 $|E| = p^n$

$\Rightarrow$ E为$\mathbb{F}_p$上, $x^{p^n} - x$分裂域.

存在性.

设$K/\mathbb{F}_p$为$x^{p^n} - x$分裂域

只要$|K| = p^n$

取$E = \{a \in K \mid a^{p^n} - a = 0\}$

claim. E为K子域

$a^{p^n} = a \quad b^{p^n} = b$

$\Rightarrow a+b, ab, a^{-1} \in E$

$E = Root(x^{p^n} - x)$，E

$x^{p^n} - x$ 无重根

$\Rightarrow E$ 为 $x^{p^n} - x$

命题.

$$x^{p^n} - x = \prod_{d \mid x} \prod_{\substack{f\ d次 \\ 不可约}} f(x)$$

Ex.

$\mathbb{F}_2[x]$ 分解 $x^{16} - x$

Ex. $\mathbb{F}_3[x]$上，分解

$x^q - x$

证明.

$\forall g(x)$. $\deg g = d \mid n$ 不可约

$$\mathbb{F}_p \subseteq K = \mathbb{F}_p[x]/(g)$$

$$\dim_{\mathbb{F}_p} K = d.$$

$$\Rightarrow g \mid x^{p^d} - x \mid x^{p^n} - x$$

若 g 不可约 $g \mid x^{p^n} - x$.

取 $a \in E$

$\Rightarrow g(a) = 0$

$\Rightarrow g($

$\Rightarrow \deg g = \dim_{\mathbb{F}_p} g \mid n.$

$x^{p^n} - x$ 无重根.

$$\begin{tikzcd}[column sep=small, row sep=small]
 & K_1 \arrow[dr, phantom, "\subsetneq"] & \\
\mathbb{F}_2 \arrow[ur, phantom, "\subsetneq"] \arrow[dr, phantom, "\subsetneq"] & & E = \mathbb{F}_{2^6}. \\
 & K_2 \arrow[ur, phantom, "\subsetneq"] &
\end{tikzcd}$$

$|K_1| = 2^2 \quad |K_2| = 2^3$

Ex.

① $K_1 \cap K_2 = \mathbb{F}_2$

② $|\{u \in E \mid \mathbb{F}_2(u) = E\}| = ?$

hint: 考虑 $u \notin K_1, K_2.$

$|E| = p^n$.

$\mathbb{F}_p \subseteq K \subseteq E$.

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

$\Rightarrow [K:\mathbb{F}_p] \mid n$.

$\forall d \mid n$. $\exists!$ 子域 $K \subseteq E$ $|K| = p^d$.

(非同构意义惟一，真正惟一).

$\mathcal{L}(n) = \{d \mid 1 \le d \mid n\} \xleftrightarrow{1:1} \{E 子域\}$

$|K_d| = p^d$ $\mathbb{F}_p$, E 中间域.

$K_d = \mathrm{Root}_E(x - x)$

Ex. $K_d \subseteq K_{d'} \Leftrightarrow d \mid d'$

$$K_d \cap K_{d'} = K_{\gcd(d,d')}$$

偏序关系：$\subseteq$

找极大真子域

$$n = \prod_{i=1}^{s} q_i^{m_i}$$

极大真子域形如 $K_{\frac{n}{q_i}}$

Claim. $\displaystyle\bigcup_{i=1}^{s} K_{\frac{n}{q_i}} \subsetneq E$

计算元素个数

$$|LHS| < \sum_{i=1}^{s} p^{\frac{n}{q_i}} \leq s\, p^{\frac{n}{2}} < p^n.$$

$\exists\, u \in E,\ u \notin \bigcup_{i=1}^{s} K_{\frac{n}{s_i}}$

$\Rightarrow E = \mathbb{F}_p(u).$

u的个数可算.

Fix $u \in E$.

s.t. $\mathbb{F}_p(u) = E$.

Claim. $\{u, \sigma(u), \cdots, \sigma^{n-1}(u)\}$

两两不同.

否则 $\sigma^m(u)=u.\quad \sigma^n(u)=u$

$d=\gcd(m,n)$

$\Rightarrow\ \sigma^d(u)=u \quad d<n \quad d\mid n.$

$u^{p^d}=u$

$\Rightarrow\ u\in k_d$ 矛盾.

(非平凡! 区别于其他域).

极小多项式为:

$$f(x)=\prod_{i=0}^{n-1}(x-\sigma^i(u))\in F_p[x].$$

$\Leftrightarrow\ \mathrm{Root}(f)=\{u,\sigma(u),\cdots,\sigma^{n-1}(u)\}.$

Galois Group 的例化很集上.

定理.

$|E| = p^n.$

$Aut(E/\mathbb{F}_p) = Aut(E)$

$= \{Id, \sigma, \sigma^2, \cdots, \sigma^{n-1}\}$

证明. $|Aut(E/\mathbb{F}_p)| \le n.$

$\{Id, \sigma, \cdots, \sigma^{n-1}\} \subseteq Aut(E/\mathbb{F}_p).$

$\Rightarrow$ $Aut(E/\mathbb{F}_p) = \{Id, \cdots, \sigma^{n-1}\}$

$\Rightarrow$ $x^{p^n} - x$ 为可分多项式.

定理 有限域的 Galois 对应

成立：有限 ...

$$\{H \le \mathrm{Aut}(E) \text{ 子群}\} \xleftrightarrow{1:1} \{k \text{ 子域}\}$$

$$\langle \alpha^d \rangle = H_d \longleftrightarrow k_d = \mathbb{F}_{p^d}$$

---

§. 2.5 分圆域

k 域，$\omega \in k$

ω 单位根，若 $\exists d$ s.t. $\omega^d = 1$

ω 的阶为最小正整数 d s.t.

$\omega^d = 1$. $\quad \mathrm{ord}(\omega) = d$.

注. char $k = p$.

$\mathrm{ord}(u) = d$

$\Rightarrow p \nmid d$

否则 $d = pk$ $\quad u^{pk} - 1 = 0$

$(u^k - 1)^p = 0$

$\mathrm{ord}(u) = d$，称 u 为 p 次本原单位根.

Fact. $u \in k^*$ $\mathrm{ord}(u) = d$.

- $1, u, \cdots, u^{d-1}$ 两两不同
- 以上为 $x^d - 1$ 全部根

定理. k域.

$H \le k^\times = k \setminus \{0_k\}$ d阶子群

$\Rightarrow$ 有d阶本原单位根 ω

$H = \{1, \omega, \cdots, \omega^{d-1}\}$

重要性: $k^\times$ 的有限子群均为循环群.

证明: 有限 Abelian Group 结构.

例. $\mathbb{F}_3[x]/(x^2+1)$

$$\begin{array}{ccc} \cancel{0} & \cancel{1} & \cancel{2} \\ \cancel{u} & u+1 & u+2 \\ \cancel{2u} & 2u+1 & 2u+2 \end{array}$$

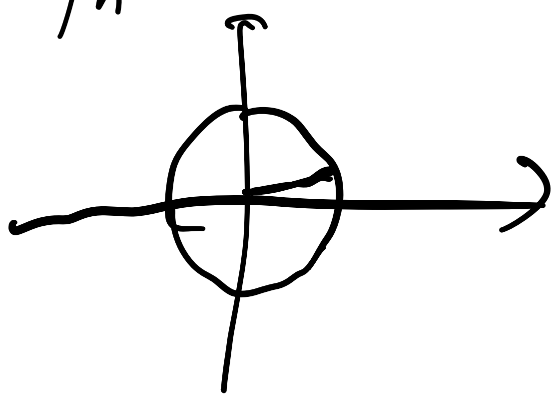
找其c为本原单位根

找关于次单元本征值.

4个, $n+1$, $n+2$, $2n+1$, $2n+2$.

$\mathbb{C}$中.

$\zeta_n = e^{\frac{2\pi i}{n}}$ 本原单位根.



$\mathbb{C}^\times$ n阶子群唯一.

Fact.

$$\operatorname{ord}(\zeta_n^m) = \frac{n}{\gcd(m,n)}$$

定义. $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ 为 x^n-1 分裂域

例 分圆域:

$$\Phi_n(x) = \prod_{\zeta_n^i \text{ n次本原}} (x - \zeta_n^i)$$

分圆多项式.

$$x^n - 1 = \prod_{d \mid n} \Phi_d(x)$$

归纳知

$\Phi_n \in \mathbb{Z}[x]$.

Φ_n 不可约.

恰有 $\varphi(n)$ 个 n 次本原单位根.

$$x^n-1=\prod_{d\mid n}\prod_{\mathrm{ord}(\omega)=d}(x-\omega)$$

$$=\prod_{d\mid n}\Phi_d.$$

定理 (Kronecker, 1854).

$\Phi_n(x)$ 在 $\mathbb{Z}[x]$ 中不可约

$\mathbb{Q}\subseteq\mathbb{Q}(\zeta_n)$.

取 $f(x)\in\mathbb{Q}[x]$ 为 ζ_n 极小多项式

$f(x)\mid\Phi_n(x)$ $f(x)$ 首一, $\in\mathbb{Z}[x]$.

Claim: $p\mid n$, 若

$f(x)=0 \Rightarrow f(x^p)=0$.

$$\mathrm{Aut}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \xrightarrow{\sim} U(\mathbb{Z}_n)$$

乘法群.

Fact.

$\sigma \in \mathrm{Aut}(\mathbb{Q}(\zeta))$

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

要用极小多项式.

$\sigma_m \in \mathrm{Aut}(\mathbb{Q}(\zeta))$

$\sigma_m(\zeta) = \zeta^m.$

$\phi(\sigma_m) = m.$

$\phi(\sigma_m \sigma_n) = mn$

中环同构.

Ex. $E = k(u_1, \dots, u_n)$

$\sigma, \tau \in \mathrm{Aut}(E/k)$

则 $\sigma = \tau \iff \sigma(u_i) = \tau(u_i)$

定理:

$$|\mathrm{Aut}(E/k)| \le \dim_k E.$$

取等 $(=)$ E/k 为某个可分多项式分裂域

$\Rightarrow$: $k(u_1) \xrightarrow{\sigma_1} k(\beta_1)$

$\uparrow \qquad \uparrow$ g_1 为 u_1 极小多项式

$k \longrightarrow k$

σ_1 个数 $= |\mathrm{Root}_E(g_1)|$

$\leq \deg g_1$.

$\Rightarrow g_1$ 在 E 上分裂且可分

E/k 域扩张.

$H \leq \mathrm{Gal}(E/k)$

① 考虑 $E^H = \{x \in E \mid \sigma(x) = x, \forall \sigma \in H\}$

H-不变子域 (H-invariant subfield)

② 中间域 $k \subseteq K \subseteq E$.

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

以：中间域与子群如何对应

此为 Galois 对应.

$$\left\{\begin{array}{c}\mathrm{Aut}(E/k)\\ \text{的子群}\end{array}\right\} \overset{\text{1:1 correspondence.}}{\rightleftarrows} \left\{\begin{array}{c}E/k\ \text{的}\\ \text{中间域}\end{array}\right\}$$

$$H \longmapsto E^H$$

$$\mathrm{Aut}(E/K) \longleftarrow\!\!\shortmid\ K$$

需求：E/k 为 Galois Extension

即 E 为可分多项式的分裂域

则有上述对应

Galois's fundamental theorem.

§3.1 群的定义.

$(G, \cdot)$.

$\cdot : G \times G \to G.$

$(g, h) \to gh$

满足:

① $(gh)k = g(hk)$

② $\exists 1, \text{ s.t. } \forall g,\ 1g = g1$

③ $\forall g, \exists g^{-1}$

③ $\forall g, \exists g^{-1}, \ gg^{-1} = g^{-1}g = 1$

Ex. 证幺元惟一

设 e_1, e_2 幺

$e_1 = e_1 e_2 = e_2$

Ex. 证逆元惟一.

设 g_1, g_2 均为 g 的逆

$g_1 g = g_2 g = 1$

右乘 g_1

$\Rightarrow g_1 = g_2$

Remark.

通常无交换律.

Ex.

(1) 消去律

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

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

(4) $\forall n, m \in \mathbb{Z}$

$$a^n a^m = a^{n+m}$$

定义. $H \subseteq G$ H群 (关于运算).

$\Rightarrow$ 称 $H \leq G$ 子群.

例.

$GL_n(F)$ general linear group.

子群 $SL_n(F) = \{A \in GL_n(F) \mid \det A = 1\}$

O_n, SO_n, U, SU

例.

R 含幺交换环.

① 加法 Abelian group.

② 乘法. 含幺半群, 交换性.

③ 结合律

terms R 具单位群.

$U(R) = \{x \in R \mid x \text{ 可逆}\}$ Abelian group.

③. 自同构群.

$\mathrm{Aut}(R)$.

例

$R = \mathbb{Z}$

$U(R) = \{\pm 1\}$.

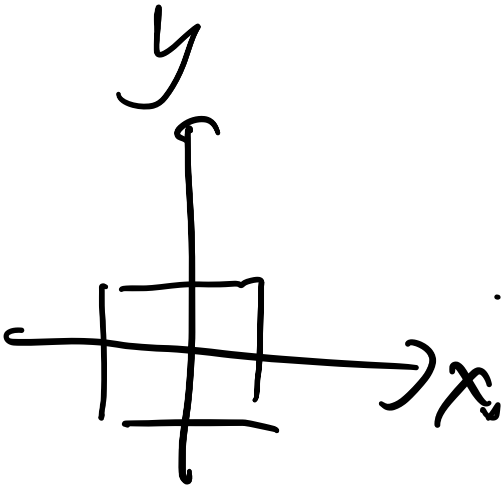
$\mathrm{Aut}(R) = \{\mathrm{Id}\}$.

$U(\mathbb{Z}[\sqrt{-1}]) = \{\pm 1, \pm i\}$

$\mathrm{Aut}(\mathbb{Z}[\sqrt{-1}]) = \{\mathrm{Id}, \widetilde{\mathrm{Id}}\}$.

对称群

$g \in \Sigma(P)$, $g(P) = P$.



$$\Sigma(\square) \leq O_2$$

Ex. 写出 $\Sigma(\square)$ 矩阵.(8个)

例. X的对称群.

置换: $\sigma(X) = X$, $X \xrightarrow{1:1} X$.

Id_X, σ^{-1}, 复合

$+nx$, 0, 变号.

$\mathrm{Aut}(\mathbb{R}) \leq S(\mathbb{R})$.

Lagrange 定理.

G 群 $|G| < +\infty$.

$H \leq G$

$\Rightarrow |H| \,\big|\, |G|$

证明: 定义等价关系.

$a \sim b$ if $\exists h \in H$, $a = bh$.

易验证为等价关系.

$$G = \bigcup_{i\in I} Ha_i$$

$$|Ha_i| = |H|.$$

$$\Rightarrow |H| \mid |G|$$

注: ① 陪集个数记为指数, $[G:H]$

$$|G| = |H||G:H|$$

② 左陪集.

$$aH = \{ah \mid h\in H\}$$

$$a\sim b \Leftrightarrow b^{-1}a\in H$$

Ex. 证此为等价关系.

③. Ex.

$$G = \bigsqcup_{i \in I} H a_i$$

$$\Rightarrow G = \bigsqcup_{i \in I} a_i^{-1} H$$

例. $G = GL_2(\mathbb{F}_2)$. 3.

$$H = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\} \leq G.$$

$$a = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

$$aH \neq Ha$$

定义 a 的阶 $\operatorname{ord}(a) =$ 最小 k s.t.

定义. a的阶 ord(a) = 最小的 k s.t.

$$a^k = 1$$

推论. $|G| < +\infty$

$\Rightarrow$ $\mathrm{ord}(a) < +\infty$, $\mathrm{ord}(a) \mid |G|$

考虑 $\langle a \rangle$.

例子. $\mathbb{F}_p^{\times}$.

阶表. $U(\mathbb{Z}_8) \not\cong U(\mathbb{Z}[i])$.

定义. G 群.

$f: G \to G'$ 同态.

(=) $f(g_1 g_2) = f(g_1) f(g_2), \ \forall g_1, g_2$

① $f(1_G) = 1_{G'}$

② $f(a^{-1}) = f(a)^{-1}$

若 f 双射，称其为群同构.

Ex. $f: G \to G'$ 同态

$a \in G$

$\Rightarrow \operatorname{ord}(f(a)) \mid \operatorname{ord}(a)$

Ex. f 同构，则

$\operatorname{ord}(f(a)) = \operatorname{ord}(a)$.

双射 + 群同态 $\to$ 群同构

双射

例:

(1) $\det: GL_n(F) \to F$

$A \to \det A$ 同志.

(2) $\mu_n = \{w \mid w^n = 1\} \leq \mathbb{C}^\times$

$\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$

Clam:

$\mu_n \xrightarrow{\sim} \mathbb{Z}_n$

群的直积

$$G \times H = \{(g, h)\}.$$

$$(g_1, h_1)\cdot(g_2, h_2) = (g_1 g_2, h_1 h_2).$$

平凡.

(1) $G \hookrightarrow G \times H \twoheadrightarrow G$

Ex. $\mathrm{ord}((g,h)) = \mathrm{lcm}(\mathrm{ord}(g), \mathrm{ord}(h))$

例. Klein 四元群

$$V_4 = \mathbb{Z}_2 \times \mathbb{Z}_2$$

$$= \{(\pm 1, \pm 1)\} \quad (\text{乘法}).$$

Ex. $V_4 \xrightarrow{\sim} U(\mathbb{Z}_8)$

22.8

记号.

$X\subseteq G$, (X) 为包含 X 的最小子群

i.e. 所有包含 X 的子群的交.

Fact.

$(X)=\{x_1\cdots x_n \mid x_i\in X$ 或 $x_i^{-1}\in X\}$.

若 $(X)=G$

称 X 为 G 的生成集

§3.2 循环群.

定义. G 称循环群, iff $\exists a\in G$, s.t.

$(a)=G$

$(\Leftrightarrow)$ $G=\{a^n \mid n\in\mathbb{Z}\}$

Ex. 若 $G\cong H$, G 循环 $\Rightarrow$ H 循环.

Ex: 若 G … , G 循环 … 循环

例: $(\mathbb{Z}, +)$

生成元: ± 1

例: $\mathbb{Z}_n$, U_n

命题.

如果 G 循环群, 则

$G \cong (\mathbb{Z}, +)$ 或 $\cong (\mathbb{Z}_n, +)$

命题. $G = (a)$ 为循环群

(1) $|G| = +\infty$ 时, 则

· G 生成元为 a, a^{-1}

· G 子群形如

$k \in \mathbb{N}^*$

$d \in N$

$\{1_G\}, \{a^d\}$

且 $(a^d) \xrightarrow{\sim} (a)$

(2) $|G| = n < +\infty$

$\Rightarrow$ · G 有 $\varphi(n)$ 个生成元 $\rightarrow$ 唯一性不平凡

· 若 $d \mid n$，$\exists !$ d 阶子群 $H_d = (a^{n/d})$

注：此处蕴含 $\sum_{d \mid n} \varphi(d) = \varphi(n)$

每个元素必生成一子群

Fact. $|G| = n < +\infty$

$|G|$ 循环群 $\Leftrightarrow \exists\, a \in G,\ \mathrm{ord}(a) = n$

推论.

p 素 $\Rightarrow$ 若 $|G| = p$，$G \xrightarrow{\sim} \mathbb{Z}_p$

定理. $|G| = n < +\infty$

G 循环 $\Longleftrightarrow \forall d \mid n$, 至多存在唯一一个 d 阶子群

$\Rightarrow$: 显然

$\Leftarrow$: $\forall d \mid n$.

$$S_d = \{ g \in G \mid \mathrm{ord}(g) = d \}$$

$\Rightarrow |S_d| \leq \varphi(d)$ (取等: d阶子群存在且唯一)

$$G = \dot{\bigcup_{d \mid n}} S_n$$

$$\Rightarrow |G| = \sum_{d \mid n} |S_n| \leq \sum_{d \mid n} \varphi(d) = |G|$$

定理. K 域

$G \leq K^*$ 有限子群

$G \le K^{\times}$ 有限子群

$\Rightarrow$ G 循环群.

推论：· E 有限域 $\Rightarrow$ $E^{\times}$ 循环

· $G \le \mathbb{C}^{\times}$, $|G| = n \Rightarrow G = \mu_n$

Ex. $\mathbb{C}^{\times}$ 不是循环群

证明：

$|G| = n$

$\forall d \mid n$, 设 $|H| = d$, $H \le G$

$\forall h \in H$, $\underline{h^d = 1}$

至多 d 个解

$\Rightarrow H = \mathrm{Root}_K(h^d - 1)$ 唯一.

§3.3. 正规子群

G, H 群

$G \xrightarrow{f} H$ 同态

$\Rightarrow \mathrm{Im} f \leq H$

定义 $\ker f := \{ x \mid f(x) = 1_H \} \leq G$

$f(a) = f(b)$

$\Leftrightarrow ab^{-1} \in \ker f$

$\Leftrightarrow b^{-1}a \in \ker f.$

Claim. 令 $N=\ker f$

则 N 满足: $\forall a\in G$

$$aN=Na$$

证: $\forall b\in aN$

$\Leftrightarrow b=an \Leftrightarrow ba^{-1}\in N$

$\Leftrightarrow a^{-1}b\in N \Leftrightarrow b\in aN$

本质: 运算的可交换性.

定义.

$N\leq G$ 称正规子群 (Normal subgroup)

记 $N\trianglelefteq G$, 若:

$\forall a \in G, \quad aN = Na$

例.

① G Abelian group $\Rightarrow$ every subgroup is normal.

② G 的中心

$Z(G) = \{ g \mid ag = ga, \ \forall a \in G \}$

Ex. $Z(G) \lhd G$

设 $H \leq G, a \in G$

H 的共轭

$aHa^{-1} = \{ aha^{-1} \mid h \in H \}$

Ex.

- $aHa^{-1} \leq G$
- $G \xrightarrow{\sim} aHa^{-1}$

Fact.

$H \triangleleft G$

$\Leftrightarrow H = aHa^{-1}, \forall a$

例

$SL_n(\mathbb{C}) = \ker(\det) \triangleleft GL_n(\mathbb{C})$

例: $H \leq G \quad [G:H]=2$

$\Rightarrow H \triangleleft G \qquad G = H \cup (G \setminus H)$

$GL_2(\mathbb{F}_2)$

$H = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\} \ntriangleleft GL_2(\mathbb{F}_2)$

$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^{-1} \notin H$

$N = \left\{ \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \right\} \triangleleft GL_2(\mathbb{F}_2).$

设 $N \lhd G$

商群： $G/N = \{ \underset{\bar{a}}{\underset{\shortparallel}{aN}} \mid a \in G \}$

$\bar{a} = \bar{b} \iff aN = bN \iff Na = Nb$

$\bar{a} \cdot \bar{b} = \overline{ab}$

well-defined ?

$\bar{a} = \bar{a'} \quad \bar{b} = \bar{b'}$

$\Rightarrow a^{-1}a' \in N, \; b^{-1}b' \in N$

$$(ab)^{-1}a'b' = b^{-1}\underset{}{\overset{n_1 \in N}{\overset{\shortparallel}{(a^{-1}a')}}}b'$$

$$= b^{-1}(n_1 b')$$

$$= (b^{-1}b')n_2 \in N$$

canonical map :

$$\mathrm{can}: G \to G/N$$

$$a \to \bar{a}$$

$\ker(\mathrm{can}) = N \Rightarrow$ 正规子群可作为核

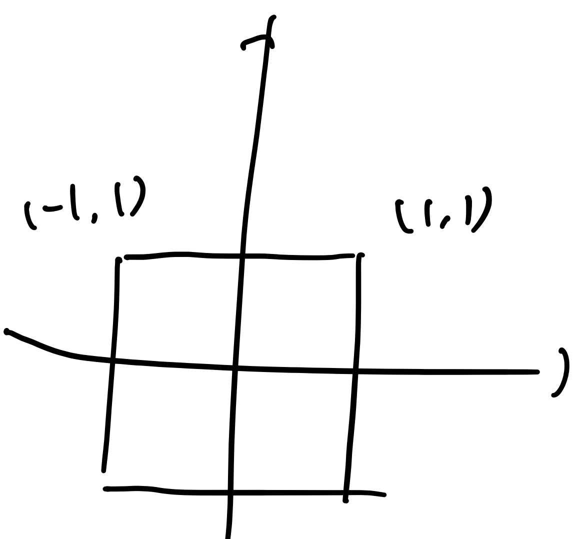
群同态基本定理.

$$f: G \to H$$

inducing a unique isomorphic map:

$$G/\ker(f) \to \mathrm{Im}\, f$$

例.



$$\Sigma = \{ g \in O(2) \mid g(\square) = \square \}$$

8元.

$V = \{$四个顶点$\}$ $\forall g \in \Sigma$ $g|_V \in S(V)$

24元.

$\Sigma(\square) \to S(V)$

$g \longrightarrow g|_V$

claim: φ 单 √. Sylow-8 group.

例: $x^3 - 2 \in \mathbb{Q}[x]$

$E = \mathbb{Q}(\sqrt[3]{2}, \omega) \subseteq \mathbb{C}$

$X = \{\sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2\}$

$\forall \sigma \in \mathrm{Aut}(E/\mathbb{Q})$

$\sigma|_X \in S(X)$

$\varphi : \mathrm{Aut}(E/\mathbb{Q}) \to S(X)$

$$\sigma \longrightarrow \sigma|_X$$

Ex. check ϕ 同态.

$$(\sigma_1 \circ \sigma_2)|_X = \sigma_1 \circ (\sigma_2|_X) = (\sigma_1|_X) \circ (\sigma_2|_X)$$

· 单 ✓. · 满 ✓.

Ex. $S(X) \xrightarrow{\sim} GL_2(\mathbb{F}_2)$

Fact. $N \leq K \leq G$. $N \trianglelefteq G$

$$K/N \leq G/N$$

对应定理: $N \trianglelefteq G$.

则 $\{\forall K$ 中间群, $N \trianglelefteq K \leq G\} \xleftrightarrow{\text{1:1 correspondence}} \{G/N$ 子群$\}$.

$$K \longrightarrow K/N$$

$$\mathrm{can}^{-1}(\bar{K}) \longleftarrow \bar{K}$$

Fact.

$N \trianglelefteq G$, $N \leq K \leq G$

$K \trianglelefteq G \Longleftrightarrow (K/N) \trianglelefteq (G/N)$

且若 $K \trianglelefteq G$， $G/K \xrightarrow{\sim} (G/N)/(K/N)$

证： 设 $K \trianglelefteq G$

$\varphi: G/N \xrightarrow{\varphi} G/K$

$aN \longrightarrow aK$

$aN = bN \Rightarrow aK = bK$ 良定.

$\Leftrightarrow a^{-1}b \in N$

$\ker\varphi = \{aN \mid aK = 1K\} = K/N \trianglelefteq G/N$

且 $(G/N)/(K/N) \xrightarrow{\sim} G/N$

Ex. 若 $K/N \trianglelefteq G/N$，则 $K \trianglelefteq G$

证明：

$\psi: G \longrightarrow (G/N)/(K/N)$

$g \to (gN)\cdot K/N$ 满同态.

$\ker\varphi = \{g \mid (gN)\cdot K/N = N\cdot K/N\}$

$= \{g \mid gN \in K/N\}$

$= K$

设 $N \trianglelefteq G$ $H \leq G$

(1) $NH = HN$ $N \leq NH \leq G$

(2) $(N\cap H) \trianglelefteq H$, 有同构

$$H/(N\cap H) \xrightarrow{\sim} NH/N$$

证: $H \to NH/N$

$h \to hN$ 满同态.

核 $= \{h\in H \mid hN = 1N\}$

$= N\cap H$

§ 2.4 对称群.

X 集 $S(X) = \{\sigma : X \xrightarrow{\sim} X\}$

$S(X)$ the symmetry group of X.

Fact. 若 $\exists X \underset{\delta}{\xrightarrow{\sim}} Y$

则 $S(X) \xrightarrow{\sim} S(Y)$

$\sigma \longrightarrow \delta \sigma \delta^{-1}$ 同构.

$S_n = S(\{1, \dots, n\})$

Fact. 若 $|X| = n$, $S(X) \xrightarrow{\sim} S_n$.

$|S_n| = n!$

例. $S_1 = \{Id\}$

$S_2 = \{Id, \sigma\}$ $\sigma^2 = Id$.

记号. $\sigma \in S_n$ $\quad \sigma(i)$.

$$\sigma = \begin{pmatrix} 1 & \cdots & n \\ \sigma(1) & \cdots & \sigma(n) \end{pmatrix}$$

例. $|S_3| = 6$.

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \qquad \tau = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

$$H = \{Id, \sigma\} \qquad K = \{Id, \tau\}$$

$$|HK| = 4 \qquad HK \nleq S_3$$

$$\sigma\tau \neq \tau\sigma$$

Fact.

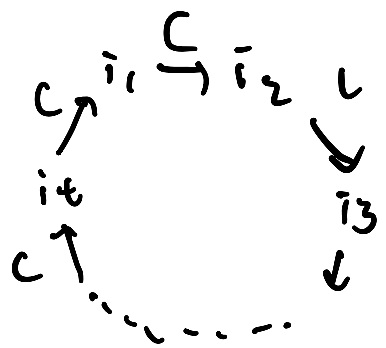
$\forall n$.

$$S_n \hookrightarrow S_{n+1}$$

$$\sigma \longrightarrow \tilde{\sigma} \qquad \tilde{\sigma}(i) = \begin{cases} \sigma(i) & i \leq n \\ n+1 & i = n+1. \end{cases}$$

t-轮换(cycle).

$c=(i_1,\cdots,i_t)\in S_n$ 表示:



$c^{-1}=(i_t\ i_{t-1}\cdots i_1)$

$\mathrm{ord}(c)=t$

on S_3

引理: 若 σ,τ 轮换, 不相交

$\Rightarrow.\ \sigma\tau=\tau\sigma$

证明: ✓.

命题: $\sigma\in S_n$

$\exists\ \sigma = c_1 \cdots c_n \quad c_1, \cdots, c_n$ 为轮换，两两不交。

证明：考虑 1 在 $\langle\sigma\rangle$ 下的轨道

$$1 \to \sigma(1) \to \cdots \to 1$$

轮换的共轭。

$$\sigma \circ (i_1 \cdots i_k) \sigma^{-1}$$

$$= (\sigma(i_1) \cdots \sigma(i_k))$$

Fact. 共轭为等价关系。

a 所在共轭类记为 C_a

$$|C_a| = 1 \iff a \in Z(G).$$

$\sigma \in S_n$.

$\sigma = c_1 \cdots c_r$ 不交轮换.

λ_i：长度为 i 的轮换个数.

σ 的型 $= 1^{\lambda_1} 2^{\lambda_2} \cdots n^{\lambda_n}$.

$$\sum_{i=1}^{n} i\lambda_i = n.$$

定理.

S_n 中两个置换共轭

$\Leftrightarrow$ 具有相同的型.

证："$\Rightarrow$" $\sigma = c_1 \cdots c_r$

$$\tau\sigma\tau^{-1} = (\tau c_1 \tau^{-1}) \cdots (\tau c_r \tau^{-1}).$$

"$\Leftarrow$" 构造一个 τ.

例. S_3. 1^3 $1^1 2^1$ 3^1.

1^3	$1^1 2^1$	3^1
(1)	$(1\ 2)$	$(1\ 2\ 3)$
	$(1\ 3)$	$(1\ 3\ 2)$
	$(2\ 3)$	

S_4	1^4	$1^2 2^1$	2^2	$1^1 3^1$	4^1
	(1)	(12)	$(12)(34)$	(123)	(1234)
		(13)	$(13)(24)$	(132)	(1432)
		(14)	$(14)(23)$	(124)	(1243)
		(23)		(142)	(1342)
		(24)		(134)	(1423)
		(34)		(143)	(1324)
				(234)	
				(243)	

Remark.

以上整合 S_3, S_4 中心平凡.

$S_3 \hookrightarrow S_4$ 对共轭不封闭

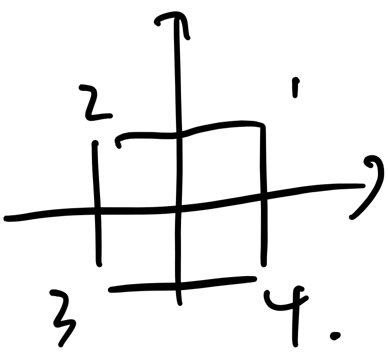
$\Rightarrow$ $S_3 \ntrianglelefteq S_4$.

② $H = \{Id, (1234), (13)(24), (1432)\}$

$H \leq S_4$.

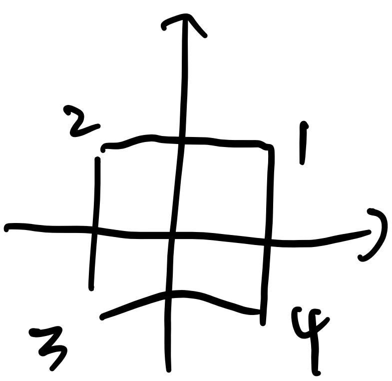
Fact. ① $H \ntrianglelefteq S_4$.

② $H = ((1234), (13))$



$\Sigma(\square) \hookrightarrow S_4$.

Ex. 算



$\Sigma(D) \hookrightarrow S_4$ 像 H.

Fact.

$\forall \sigma$ 可写为对换之积.

$$(i_1 \cdots i_k) = \underbrace{(i_1\ i_k) \cdots\cdots (i_1\ i_3)(i_1\ i_2)}_{k-1\text{个}}$$

引理.

S_n 可由 $((1\ 2), (2\ 3), \ldots, (n-1\ n))$ 生成.

$$(i\ j) = (i+1\ j)(i\ i+1)(i+1\ j)^{-1}$$

对 i, j 归纳.

Remark.

$$s_i = (i\ i+1)$$

$$s_i s_{i+1} s_i = s_{i+1} s_i s_{i+1}$$

$$|i-j| \geq 2 \quad s_i s_j = s_j s_i$$

$$s_i^2 = \mathrm{Id}.$$

$$\mathbb{R}^n = \bigoplus_{i=1}^{n} \mathbb{R}e_i$$

$\sigma \in S_n$ $\quad P_\sigma : \mathbb{R}^n \to \mathbb{R}^n.$

$$e_i \to e_{\sigma(i)}$$

故 $S_n \hookrightarrow GL_n(\mathbb{R})$ 群同态

$$\sigma \mapsto P_\sigma$$

$$\begin{array}{ccccc} S_n & \hookrightarrow & GL_n(\mathbb{R}) & \xrightarrow{\det} & \mathbb{R}^\times \\ \sigma & \longrightarrow & P_\sigma & \longrightarrow & \det P_\sigma. \end{array}$$

sign: $\sigma \twoheadrightarrow \{\pm 1\}^\times.$

$\sigma \in S_n$ $\quad\sigma$偶，若 $\operatorname{sign}\sigma = 1$，偶个对换之积

$$A_n = \{\sigma \mid \operatorname{sign}\sigma = 1\} \lhd S_n$$

$$[S_n : A_n] = 2$$

alternative group 交错群.

分类 S_3 子群.

$\{(1)\}$, S_3

$\langle(12)\rangle$ $\langle(13)\rangle$ $\langle(23)\rangle$

$A_3=\{(1),(123),(132)\}$

S_3 子群格.

Fact.

正规子群可以写成几个共轭类的并.

S_4 的正规子群

$\{1\} \le K_4 \le A_4 \le S_4$

$K_4 = \{Id, (12)(34), (13)(24),$

$(14)(23)\}$

定义. G 称单群，若 G 无非平凡正规子群 (Simple group).

Ex. G Abelian group

G 单 $\Leftrightarrow$ $G = \mathbb{Z}_p$

定理 $n \geq 5$ 时

A_5 单群

推论: $n\geq 5$

A_n为S_n惟一非平凡正规子群.

证明. $N \trianglelefteq S_n \Rightarrow (N\cap A_n) \trianglelefteq A_n$.

① $N\cap A_n = A_n$

$\Rightarrow A_n = N$

② $N\cap A_n = \{Id\}$

(1) $A_n = \{Id\}$

(2) $N \neq \{Id\}$

$\Rightarrow |N| = 2 \Rightarrow N \ntrianglelefteq S_n$.

A_n 单的证明 ($n \geq 5$).

① A_n 可由所有 3-cycle 生成.

$$(i\ j)(r\ s) = \begin{cases} (s\ i\ r) & j = r,\ i \neq s \\ (r\ i\ s)(i\ j\ r), & \{i, j\} \cap \{r, s\} = \emptyset \end{cases}$$

② 所有 3-cycle 在 A_n 中共轭

☆ ③ $N \trianglelefteq A_n$, $N \neq \{Id\}$

$\exists$ N 含有某 3-cycle.

(此步需要 $n \geq 5$).

例. A_4.

$$\frac{\mathrm{Id}.}{(12)(34) \quad (13)(24) \quad (14)(23)}$$

Ex. 解方程

$$\sigma(12)(34)\sigma^{-1} = (13)(24).$$

claim. (123) 与 (132) 在 A_4 中不共轭.

否对.

$\sigma(123)\sigma^{-1} = (132)$

① $\sigma(1) = 1$

$\sigma(2) = 3$

$\sigma(3) = 2$ X

② $\sigma(1) = 3$

$\sigma(2) = 2$ X

$\sigma(3) = 1$

③ $\sigma(1) = 2$

$\sigma(2) = 1$ X

$\sigma(3) = 3.$

Ex: 算 A_4 中 (123) 的共轭类.

§1.7 群作用

群 G 左作用于集合 X, 记 $G \curvearrowright X$

$$G \times X \to X$$
$$gx.$$

满足: · $1x = x, \quad \forall x \in X$

· $h(gx) = (hg)x$

例: $S(X) \curvearrowright X$. $\quad S_n \curvearrowright [n]$

$$\sigma x := \sigma(x)$$

例: $GL_n(\mathbb{R}) \curvearrowright \mathbb{R}^n$.

例 K/k 为 $f(x)$ 分裂域

$$\mathrm{Aut}(K/k) \curvearrowright \mathrm{Root}_K(f)$$

$$\sigma a := \sigma(a)$$

Fact. $G \curvearrowright X$

$G \xrightarrow{f} S(X)$. 同态.

证明: $f(G): X \to X$

$f(g)(x) = gx$.

fix g.

$X \xrightarrow{f(g)} X$

$x \to gx$ $\quad$ g 可逆 $\Rightarrow$ 双射

$f(g) \in S(X)$.

$f(g)\circ f(h) = f(gh) \Rightarrow$ 同态.

Fact. G 群

$f: G \to S(Y)$ 同态.

诱导群作用

$G \curvearrowright Y :=\quad gy = f(g)(y).$

$h\cdot(gy) = f(h)(f(g)(y))$

$= (f(h)f(g))(y)$

$= f(hg)(y)$

$= (hg)y.$

$$\mathrm{Aut}(K/k) \xrightarrow{f} S(\mathrm{Root}_K(f))$$

Ex. f 单.

注:

右作用、op (opposite) 反群

$$f: G \to S(X)^{op} \quad \text{反群}$$

$$f(g): X \to X$$

$$x \mapsto x.g$$

如何转化为左作用?

$$G \longrightarrow G^{op}$$

$$g \to g^{-1} \quad \text{同构.}$$

$$G \curvearrowright X \qquad gx := xg^{-1}$$

$G \curvearrowright G$ 左正则作用

gx

$G \to S(G)$

$g \to t_g \quad t_g(x) = gx$

Ex. 单.

称 G 忠实，若 $\forall g \neq 1_G$, $\exists x$, s.t.

$gx \neq x$.

$\Leftrightarrow$ t 为单同态.

例. 左正则作用忠实.

$G \curvearrowright X$

(1) $x \in X$ x的G-轨道(orbit)-

$O_x = \{gx \mid g \in G\}$

X上等价关系.

$x \sim y \Leftrightarrow \exists g$, s.t. $x = gy$

此为等价关系.

$\Rightarrow$ O_x为x所在等价类.

(3) X有G轨道分解.

$X = \bigsqcup_{x \in I} O_x$.

(4) $G \curvearrowright \Theta_x$.

定义. $G \curvearrowright X$ 可迁 (transitive), 若仅有一条轨道.

例. $f(x) \in k[x]$, 无重根.

K/k 分裂域.

$\mathrm{Aut}(K/k) \curvearrowright \mathrm{Root}_K(f(x))$ 忠实

Claim: $\curvearrowright$ 可迁

$\Leftrightarrow$ $f(x)$ 不可约.

$\Leftarrow$: $f(x)$ 不可约

$u_1, u_2 \in \mathrm{Root}_K(f)$.

$$\begin{tikzcd}
K \arrow[r, dashed] & K \\
k(u_1) \arrow[u, hook] \arrow[r, dashed] & k(u_2) \arrow[u, hook] \\
k \arrow[u, hook] \arrow[r, "id"] & k \arrow[u, hook]
\end{tikzcd}$$

$\Rightarrow$: 需要无重根.

定义. $G \curvearrowright X$ $x \in X$.

x的稳定化子 $G_x = \{g \in G \mid gx = x\}$

stabilizer.

引理：

$x = hy$

则 $G_x = h G_y h^{-1}$

证：若 $g \in G_y$

$hgh^{-1}x = hy = x$.

定理：fixed x.

存在双射

$G/G_x \to O_x$

$gG_x \to gx$

$\Rightarrow |G| = |G_x||O_x|$

例.

$H \leq G$

$H \curvearrowright G$.

例 $G \curvearrowright X$.

$X^G = \{x \mid gx = x\ \forall g \in G\}$.

共轭作用.

G 为 Abelian group

$\Leftrightarrow$ 该作用平凡

$g(x) := g x g^{-1}$

$Z(x) = \{ g \mid gx = xg \}$

$|G| = |C_x| \, |Z(x)|$

例. A_4 中 $(1\,2\,3)$ 共轭类.

$|Z((1\,2\,3))| = 3$

$\Rightarrow$ 4 个.

Ex.

$C_x = \{x\}$

$(\Leftarrow)\quad x \in Z(x)$

$(\Leftarrow)\quad Z(x) = G.$

类等式. (class equation).

$$|G| = |Z(G)| + \sum_{|C_x|>1} |C_x|$$

定义. G称 p-subgroup, 若 $|G| = p^n$.

例: $G = \mathbb{Z}_p$

命题.

p群有非平凡中心.

$$p^n = |G| = |Z(G)| + \sum_{|C_x|>1} |C_x|.$$

p的倍数

$$\Rightarrow p \,\big|\, |Z(G)|$$

注：由此导出 p 群必可解.

命题. $|G| = p^2$

$\Rightarrow G$ Abelian group

$G \cong \mathbb{Z}_{p^2}$ 或 $\mathbb{Z}_p \times \mathbb{Z}_p$.

证: $1 \neq g \in G(Z)$.

(1) $\operatorname{ord}(g) = p^2 \Rightarrow G \xrightarrow{\sim} \mathbb{Z}_{p^2}$

(2) $\mathrm{ord}(g)=p$

$H=(g)\subseteq G(Z)$.

取 $g'\notin H$ s.t.

$\mathrm{ord}(g')=p$. (否则 $\mathrm{ord}(g')=p^2$).

$K=(g')$.

K, H 中元素两两可交换

Ex. $f: H\times K\to G$

$f: (h,k)\to hk$ 同构

例 $H \leq G$

$X_H = \{H' \leq G \mid H' 与 H 共轭\}$

$G \curvearrowright X_H$.

$gH' := gH'g^{-1}$ transitive

$N_G(H) = \{g \in G \mid gHg^{-1} = H\}$

Normalizer. 正规化子.

$|X_H| \, |N_G(H)| = |G|$

例. 共轭作用.

$G \curvearrowright C_x$. $x \in G$.

共轭作用.

$S_4 \curvearrowright C = \{(12)(34), (13)(24), (14)(23)\}$

$$S_4 \xrightarrow{f} S(C) = S_3.$$

Ex. · f 满

· $\ker f = K_4$.

例. A_4 无6阶子群.

A_5 无30阶子群.

定义. $|G| = p^r m \quad p \nmid m$

子群 $P \leq G$ 称 Sylow-p 子群.

若 $|P| = p^r$.

定理. Sylow (1872)

$|G| = p^r m \quad p \nmid m$

(1) 总存在 Sylow-p 子群.

(2). Sylow-p 子群互相共轭

(3) Sylow-p 子群的个数 n.

$\Rightarrow n \mid |G|$ 且 $n \equiv 1 \mod p$

(4) 任意一个 p 子群(阶为 p 的幂) A

必存在一个 Sylow-p 子群 B

s.t. $A \le B$

Remark.

Sylow p 子群正规

$\Leftrightarrow$ 仅有1个.

例. S_4. $|S_4| = 2^3 \times 3$.

Sylow-3 子群. $\{(1), (123), (132)\}$

$\{(1), (124), (142)\}$

$\{(1), (1\,2\,4), (1\,4\,2)\}$

$\{(1), (1\,3\,4), (1\,4\,3)\}$

$\{(1), (2\,3\,4), (2\,4\,3)\}$

Sylow-2 子群

个数：1 或 3.

非正规子群 $\Rightarrow$ 3个，H_1, H_2, H_3

Claim. $K_4 \le H_i$, $\forall i$

$\exists$ Sylow-2 子群 s.t. $K_4 \le H_i$

K_4 正规 $\Rightarrow K_4 \leq H_i, \forall i$

$$H_1 = (K_4, (12)) = \left\{\begin{array}{l}(1), (12)(34), (13)(24), \\ (14)(23), (12), (34), \\ (1423), (1324)\end{array}\right\}$$

$H_2 = (K_4, (13))$

$H_3 = (K_4, (14))$

例 A_4.

Sylow-2 子群.

$K_4 \lhd A_4 \Rightarrow$ 仅1个.

例. 35阶群 $\simeq \mathbb{Z}_{35}$.

$|G| = 5 \times 7$

$\exists$ 5阶子群 P. 个数$|7$, $\equiv 1 \bmod 5$

$\Rightarrow P \triangleleft G$.

同理 $\exists$ 7阶子群 Q

$Q \triangleleft G$.

$P \cap Q = \{1\}$ $\quad P = (p)$ $Q = (q)$

$pq = qp^n = p^n q^m \Rightarrow p^n = p$
$q^m = q$

$\Rightarrow pq = qp$

Ex. $P \times Q \xrightarrow{\sim} G$

$(g,h) \longrightarrow gh.$

$G \xrightarrow{\sim} \mathbb{Z}_5 \times \mathbb{Z}_7 \xrightarrow{\sim} \mathbb{Z}_{35}.$

例. 108阶群非单

$|G| = 2^2 \cdot 3^3$

$\exists P \leq G \quad |P| = 27$

$G \curvearrowright G/P = \{gP \mid g \in G\}.$

$f: G \to S(G/P)$

$\ker f \neq G$

因 $|G| = 108 > 24 = S(G/P)$

$\ker f \neq \{1\}$

$\Rightarrow \ker f$ 非平凡

Fact. G Abelian group.

$|G| = p_1^{s_1} \cdots p_r^{s_r}$.

$\Rightarrow \exists!$ Sylow p_i 子群 P_i

同态：

$$P_1\times\cdots\times P_r \xrightarrow{\varphi} G$$

$$(g_1,\cdots,g_r)\to g_1\cdots g_r$$

Ex. φ 满.

定理.（Cauchy 1845.）

$p\mid |G|$

$\Rightarrow \exists\ p$ 阶元.

Proof of Sylow's theorem.

$|G|=n=p^r m \quad p\nmid m.$

$$X = \{ U \subseteq G \mid |U| = p^r \}$$

$$G \curvearrowright X.$$

$$g \cdot V := gV$$

$$|X| = \binom{p^r m}{p^r}$$

claim.

$$p \nmid |X|.$$ (显然).

轨道分解:

$$X = \dot{\bigcup_V} O_V \Rightarrow \exists V,\ p \nmid V$$

$$G_V = \{g \mid g^V = g\}$$

$$|O_V|\,|G_V| = p^r m$$

$$\Rightarrow \quad p^r \mid |G_V|$$

$$G_V \curvearrowright V.$$

$g \cdot v := gv$ 自由作用.

$$\Rightarrow \quad |G_V| \mid |V|$$

$$\Rightarrow \quad |G_V| = p^r$$

Another proof using linear algebra.

$|G| = p^r m = n.$

- $G \hookrightarrow S(G) \hookrightarrow GL_n(\mathbb{F}_p).$

$$\sigma \longmapsto P_\sigma$$

- $\underline{GL_n(\mathbb{F}_p)}$ 有 Sylow-p 子群.

$$\prod_{i=0}^{n-1}(p^n - p^i) = p^{n(n-1)/2} \cdot \square.$$

$$H = \left\{ \begin{pmatrix} 1 & \square & \cdots & \square \\ & \ddots & & \vdots \\ & & \ddots & \square \\ 0 & & & 1 \end{pmatrix} \right\} \quad p^{n(n-1)/2} \text{ 阶群}$$

Fact. $H\le K$ $\underbrace{P\le K}_{\text{sylow-}p\text{ 子群}}$.

则 $\exists g\in K$ s.t.

$H\cap gPg^{-1}$ 为 H 的 sylow-p 子群

Ex. 证明上述 Fact.

hint: 考虑 $H\curvearrowright (K/P)$

群的表示 (presentation).

目标: 将任一群同构于自由群商群.

自由群

$X \neq \phi$.

形式逆：$X^{-1} = \{x^{-1} \mid x \in X\}$.

$X \sqcup X^{-1}$ 字母.（alphabet）

① 字（word）.

$w = x_1 x_2 \cdots x_n$.

$n=0$ 空字.

② 字 w 既约

若 $\exists i$, s.t. $x_i = x_{i+1}^{-1}$

Fact. 任意字可惟一约化成既约字.

定义 X 上的自由群

$F(X) = \{$以 $X \sqcup X^{-1}$ 为字母的既约字$\}$

乘法：连接+约化

幺元：空字

逆元：$(x_1 \cdots x_n)^{-1} = x_n^{-1} \cdots x_1^{-1}$

若 X 有限，称有限生自由群.

例. $X=\{a\}$

$$F(X) \xrightarrow{\sim} \mathbb{Z}$$

命题. G 群. 映射 $f: X \to G$

X 集.

则唯一延拓群同态, s.t.

$$F(X) \xrightarrow{\bar f} G, \quad \bar f|_X = f$$

$$\begin{tikzcd} X \arrow[r] \arrow[d, hook] & G \\ F(X) \arrow[ur, dashed, "\exists!\, \bar f"'] & \end{tikzcd}$$

Fact. G 群

$\Rightarrow \exists N \trianglelefteq F(G)$ s.t.

$$G = F(G)/N$$

生成元关系

$$G = \langle \underset{\substack{\uparrow \\ \text{字}}}{x_1, \ldots, x_n} \mid \underset{\substack{\uparrow \\ \text{关系}}}{r_1, \ldots, r_m} \rangle$$

$$= F(x_1, \ldots, x_n) / N(r_1, \ldots, r_m)$$

$\underline{N(r_1, \ldots, r_m)}$ 为包含 $r_1 \sim r_m$ 的

最小正规子群.

Fact.

N 为由 $\{ w^{-1} r_i w \mid w \in F \}$ 生成子群.

例

$G = \langle a, b \mid a^2, b^2, (ab)^3 \rangle$

Claim:

$\bar{a} = \bar{a} N$

$\bar{a}^2 = 1 \quad \bar{b}^2 = 1 \quad (\overline{ab})^3 = 1$

如何找 G 的表现?

① $X \subseteq G$, $\langle X \rangle = G$

② 找 X 满足关系. $F(X) \overset{\varphi}{\twoheadrightarrow} G$.

找 $r_1, \cdots, r_n \in \ker \varphi$

③ $\ker \varphi = N(r_1, \cdots, r_n)$.

证 $\subseteq$ 较为困难.

例. $G = \langle a, b \mid a^2, b^2, (ab)^3 \rangle$

Fact. 泛性质.

$G=\langle x_1,\cdots,x_n \mid r_1,\cdots,r_m\rangle$

$\forall$ 群 H, $\forall$ 映射.

$X=\{x_1,\cdots,x_n\}\xrightarrow{f} H.$

则 f 可唯一延拓为群同态.

$\varphi: G\to H$

$\Leftrightarrow \tilde{\varphi}(r_i)=1, \forall i.$

$\tilde{\varphi}$ 为 $F(X)\to H$ 的同态.

例. $G=\langle a,b \mid a^2, b^2, (ab)^3 \rangle$

$\{a,b\} \xrightarrow{f} S_3$

$a \to (1\ 2)$

$b \to (2\ 3)$

$f(a)^2 = f(b)^2 = (f(a)f(b))^3 = (1)$.

G中, a,b 满足

$a^2=b^2=(ab)^3=1$

G中元素可写成 $a^{n_1}b^{m_1}\cdots a^{n_k}b^{n_k}$

$a=a^{-1} \quad b=b^{-1}$

$\Rightarrow$ 可写成 $abab\cdots ab$. 或 b 开头

$(ab)^3=1$

$\boxed{aba=bab}$.

$a \qquad b$

$ab \qquad ba$.

$aba = bab$

G 不超过 6 个元素!

Ex. in $F(a,b)$

$$N(a^2, b^2, (ab)^3) = N(a^2, b^2, abab^{-1}a^{-1}b^{-1})$$

例. $n \geq 3$.

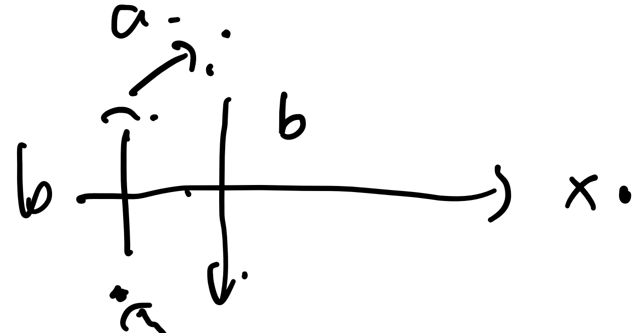
正n边形

$D_n = \{ g \in O_2 \mid g(⬡) = ⬡ \}$

n个旋转 $1, a, \cdots, a^{n-1}$. a 顺 $\frac{2\pi}{n}$

n个镜像对称 b. 关于 x 轴对称.

$(ab)^2 = 1$



a

令 $G = \langle x, y \mid x^n, y^2, (xy)^2 \rangle$

$G \to D_n$.

$x \to a$

$y \to b$. $\Rightarrow G \twoheadrightarrow D_n$

Claim: $|G| \le 2n$.

任意元素形如

$x^i y^j$ 至多 $2n$.

Ex $D_n \xrightarrow{\sim} \langle s, t \mid s^2, t^2, (st)^n \rangle$

hint: $s \to ab$ $t \to b$.

Ex.

$$G = \{x, y \mid x^4, x^2y^2, yxy^{-1}x\}.$$

则 $G \xrightarrow{\sim} Q_8$

$x \to i$

$y \to j$

有限生成 Abel 群.

A abelian group

运算记为 $+$

直积记为直和 $\oplus$

Abelian group 自然构成 $\mathbb{Z}$ module.

free Abelian group 称为 free-$\mathbb{Z}$ module.

A,B 加法群

外直和

$$A \oplus B \xrightarrow{\sim} A \times B.$$

内直和

$A,B \le U$

若 $A+B=U$

$A\cap B=\{0\}$

$A\oplus B \xrightarrow{\sim} U$

记 $U=A\oplus B$.

$$\mathbb{Z}^n=\bigoplus_{i=1}^{n}\mathbb{Z}$$

rank n 自由 Abelian group.

Fact. $\mathbb{Z}^n$ 泛性质.

$\forall$ 加法群 A, $v_1,\dots,v_n\in A$.

$\exists!$ 群同态 $\mathbb{Z}^n \xrightarrow{\varphi} A$

s.t. $\varphi(e_i) = v_i$

Ex. 证明 Fact.

Ex. $\mathbb{Z}_n \xrightarrow{\sim} \langle x_1, \cdots, x_n \mid x_i x_j x_i^{-1} x_j^{-1} \rangle$

Fact. A finited generated $\mathbb{Z}$-module.

$\Rightarrow A \xrightarrow{\sim} \mathbb{Z}^n / K$

Fact. $K \leq \mathbb{Z}^n$

本质: $\mathbb{Z}$ noetherian ring.

$$K/(K\cap \mathbb{Z}\vec{e}_1) = (K+\mathbb{Z}\vec{e}_1)/\mathbb{Z}\vec{e}_1$$

Ex.

$$\le \mathbb{Z}^2/\mathbb{Z}\vec{e}_1$$

$$\simeq \mathbb{Z}\vec{e}_2$$

Ex. $N \trianglelefteq G$

N f.g. G/N f.g.

$\Rightarrow G$ f.g.

群同态.

$$\mathbb{Z}^m_{col} \longrightarrow \mathbb{Z}^n_{col}.$$ column 列向量.

$$m\ \begin{bmatrix} x \\ \\ \end{bmatrix} \longrightarrow \begin{bmatrix} n\times m. \\ \underline{\mathbb{Z}\text{ matrix}} \end{bmatrix} \begin{bmatrix} x \\ \\ \end{bmatrix}$$

$$\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}^m, \mathbb{Z}^n) \xrightarrow{\sim} M_{n\times m}(\mathbb{Z}).$$

定义.

$$\mathbb{Z}^m \xrightarrow{\phi_A} \mathbb{Z}^n.$$

$$\mathrm{cok}(\phi_A) = \mathbb{Z}^n / \mathrm{Im}(\phi_A)$$

Key Fact. $\forall$ f.g. Abelian group G.

$\exists\ \phi_A$, s.t.

$$G \xrightarrow{\sim} \mathrm{cok}(\phi_A)$$

证: $G \xrightarrow{\sim} \mathbb{Z}^n/K$

$K = \mathbb{Z}v_1 + \cdots + \mathbb{Z}v_m$.

定义. $A, B \in M_{n\times m}(\mathbb{Z})$

A, B 相抵

$\Leftrightarrow \exists\ P \in GL_{n\times n}(\mathbb{Z}),\ Q \in GL_{m\times m}(\mathbb{Z})$

s.t. $PAQ = B$.

Smith 标准型

化 A 为 Smith 标准型

Ex. G_1, G_2 群.

$N_1 \trianglelefteq G_1,\ N_2 \trianglelefteq G_2$

$\Rightarrow$ · $N_1 \times N_2 \trianglelefteq G_1 \times G_2$

· $(G_1 \times G_2) / (N_1 \times N_2) \xrightarrow{\sim} G_1/N_1 \times G_2/N_2$

f.g Abelian group

结构定理.

G f.g. Abelian group

$\Rightarrow G \xrightarrow{\sim} (\mathbb{Z}_{d_1} \oplus \cdots \oplus \mathbb{Z}_{d_r}) \oplus \mathbb{Z}^s$

$d_1 \mid d_2 \mid d_3 \mid \cdots \mid d_r$.

若 $|G| < +\infty$, $s = 0$.

证明: $G \xrightarrow{\sim} \operatorname{cok}(\phi_A) \xrightarrow{\sim} \operatorname{cok}(\phi_B)$

$$B = \begin{pmatrix} d_1 & & & & & \\ & \ddots & & & & \\ & & d_r & & & \\ & & & 0 & & \\ & & & & \ddots & \\ & & & & & 0 \end{pmatrix}$$

$\operatorname{Im} \phi_B = d_1 \mathbb{Z} \oplus \cdots \oplus d_r \mathbb{Z} \oplus \{0\} \oplus \cdots$

$($

Fact. (1) $A \in M_n(\mathbb{Z})$

$\det A \neq 0$

$\Rightarrow |\operatorname{cok}(\varphi_A)| = |\det A|$

Fact. $K \leq \mathbb{Z}^n$, $\exists$ $\mathbb{Z}^n$的基 $e_1 \sim e_n$ s.t.

$\exists$ $d_1 | \cdots | d_r$

s.t. K 以 $d_1e_1, \cdots d_re_r$ 为基

推广: R is PID, if M is a torsion-free f.g. R module, then M is R-free.

证： $\exists v_1 \sim v_m$

$$\text{s.t. } K = \mathbb{Z} v_1 + \cdots + \mathbb{Z} v_m.$$

$$\phi_A : \mathbb{Z}^m \to \mathbb{Z}^n \qquad \operatorname{Im}\phi_A = K$$

$$e_i \to v_i.$$

$$B = P^{-1} A Q.$$

$$\begin{tikzcd}
\mathbb{Z}^m \arrow[r, "\phi_A"] & \mathbb{Z}^n \\
\mathbb{Z}^m \arrow[u, "\phi_Q"] \arrow[r, "\phi_B"'] & \mathbb{Z}^n \arrow[u, "\phi_P"']
\end{tikzcd}$$

$$\phi_P(\operatorname{Im}\phi_B) = \operatorname{Im}\phi_A$$

$\mathrm{Im}\,\varphi_A \xrightarrow{\sim} \mathrm{Im}\,\varphi_B \xrightarrow{\sim} \ldots$

定义. G Abelian 群

$t(G) = \{ g \in G \mid g \text{ 有限阶} \}$.

torsion subgroup.

定理: G f.g. Ab. grp

$\exists$ 内直和

$G = t(G) \oplus F$

F free.

回归域论.

定理. $G \leq \mathrm{Aut}(K)$ 有限, 则

高度不平凡

① $[K:K^G] = |G| < +\infty$

② $G = \mathrm{Gal}(K/K^G)$

证: 令 $k = K^G$, $n = |G|$

Claim: $\dim_k K \leq n$

若 claim 成立,

$$n = |G| \leq |\mathrm{Gal}(K/k)| \leq \dim_k K \leq n.$$

Proof of claim.

否则 $\exists \{e_1,\cdots,e_{n+1}\}\subseteq K$，故一线性无关

$G \curvearrowright K$

得到

$$A=(\sigma_i(e_j))_{n\times(n+1)}\in M_{n\times(n+1)}(K).$$

$$V=\{v\in K^{n+1} \mid Av=0\}\neq\{0\}\ (\text{由 rank 得}).$$

$G \curvearrowright V$

$$\sigma\cdot\begin{pmatrix} v_1\\ \vdots\\ v_{n+1}\end{pmatrix}=\begin{pmatrix}\sigma(v_1)\\ \vdots\\ \sigma(v_{n+1})\end{pmatrix}\in V$$

取 $0\neq \nu\in V$ s.t. ν 中非 0 分量最少.

- ν 中至少两个分量非零，否则 $\lambda_i e_i=0$.
- $\nu=(\lambda_1,\lambda_2,\cdots\cdots)$

不妨设 $\lambda_1=1$, $\lambda_2\neq 0$.

Fact. v 中分量不全在 k 中 (因为 $\{e_i\}$ k 线性无关)

不妨 $\lambda_2\notin k$

$\Rightarrow \exists\, \tau\in G$, s.t. $\tau(\lambda_2)\neq\lambda_2$.

考虑 $u=v-\tau v\in V$

$=(0,\square,\cdots,\lambda_i-\tau(\lambda_i),\cdots)\neq 0$

u 中分量 0 的个数比 v 更多! 矛盾.

有限维域扩张 K/k

$G=\mathrm{Gal}(K/k)$ $\quad |G|\leq \dim(K/k)<+\infty$

$k\leq K^G$

定理：TFSAE

① $k = K^G$

② $|G| = \dim_k K$

③ $\forall \alpha \in K$，α在k上极小多项式可分且在K上分裂

④ K/k为某可分多项式分裂域.

若满足以上，称为 Galois 扩张

证：① $\Leftrightarrow$ ②

$$\dim_k K = \dim_k K^G \cdot \dim_{K^G} K$$

$$= \dim_k K^G \cdot |G|$$

② $\Rightarrow$ ③ 思路：抓取等条件

设 $|G| = \dim_k K$, fix $\alpha \in K$

$$\begin{tikzcd} K & K \\ k(\alpha) \arrow[u, hook] \arrow[r, "\sigma_\beta\ \sim", "\alpha\mapsto\beta"'] & k(\beta) \arrow[u, hook] \\ k \arrow[u, hook] \arrow[r, "\sim"] & k \arrow[u, hook] \end{tikzcd}$$

$|\mathrm{Root}_k(g(x))|$ 个 β

给定 σ_β，延拓个数 $\leq \dim_{k(\alpha)} K$

$$|G| \leq |\mathrm{Root}_k\, g(x)| \cdot \dim_{k(\alpha)} K$$

$$\leq \dim_k k(\alpha) \cdot \dim_{k(\alpha)} K$$

$$= G$$

③ $\Rightarrow$ ④ $\Rightarrow$ ① ✓.

Ex. 给定 K/k, K'/k' s.t.

$$\dim_k K = \dim_{k'} K' = n.$$

给定同构 $k \xrightarrow{\delta} k'$

则 $\left|\{\sigma : K \xrightarrow{\sim} K' \mid \sigma|_k = \delta\}\right| \le n$

命题. $\forall$ 域 K, $\exists$ 双射

$$\left\{\begin{matrix}\text{有限子群}\\ G \le \mathrm{Aut}(K)\end{matrix}\right\} \xleftrightarrow{1:1} \left\{\begin{matrix}\text{子域}\\ k \le K\end{matrix} \;\middle|\; \begin{matrix}K/k \text{ Galois}\\ \text{扩张}\end{matrix}\right\}$$

$$G \longrightarrow K^G$$

$$\mathrm{Gal}(G/k) \longleftarrow k$$

注：此称为绝对 Galois 对应

命题：relative Galois correspondence.

设 K/k 有限 Galois 扩张

则 ∃ 双射

$$\left\{ \begin{array}{c} Gal(K/k) \text{ 的} \\ \text{子群} \end{array} \right\} \xleftrightarrow{1:1} \left\{ k/K \text{ 中间域 } E \right\}$$

$$H \le Gal(K/k) \longrightarrow K^H$$

$$Gal(K/E) \longleftarrow E$$

Fact: K/E Galois 扩张！

E/k 可分.

$$Gal(K/K^H) = H$$

$$K^{Gal(K/E)} = E.$$

例.

$$\begin{tikzcd}
\mathbb{Q} \arrow[r, hook] \arrow[r, bend left, "\text{非Galois}"] \arrow[rr, bend right=60, "\text{Galois}"'] & \mathbb{Q}(\sqrt[3]{2}) \arrow[r, hook] \arrow[r, bend right, "\text{Galois}"'] & \mathbb{Q}(\omega, \sqrt[3]{2})
\end{tikzcd}$$

Why?: 子群 vs. 正规子群.

扩张 vs. 正规扩张.

命题: 有限 Galois K/k E 中间域

则 E/k Galois $\Longleftrightarrow$ $\forall \sigma \in Gal(K/k)$

$\sigma(E) = E.$

$\Rightarrow$: 设 E/k 为 f 分裂域

$$E = k(\beta_1, \dots, \beta_s)$$

$$\sigma(E) = k(\sigma(\beta_1), \dots, \sigma(\beta_s)) = E.$$

$\Leftarrow$:

$\forall\, b \in E$ 极小多项式 $g \in k[x]$.

$$g = \prod_{i=1}^{s} (x - \beta_i)$$

Claim: $\beta_i \in E \quad \forall i$.

$$\begin{tikzcd}
K & K \\
k(x) \arrow[u, hook] \arrow[r, "\sigma"] & k(\beta_i) \arrow[u, hook] \\
k \arrow[u, hook] \arrow[r, "\sim"] & k
\end{tikzcd}
\qquad \Rightarrow \beta_i \in E.$$

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

$\dim_{\mathbb{Q}}(K)=6$

$a=\sqrt[3]{2}\quad b=\sqrt[3]{2}\,\omega\quad c=\sqrt[3]{2}\,\omega^2$

$\sigma_1: K \xrightarrow{\sim} K$

$\sqrt[3]{2} \to \sqrt[3]{2}\,\omega$

$\sqrt[3]{2}\,\omega \to \sqrt[3]{2}$

$\sqrt[3]{2}\,\omega^2 \to \sqrt[3]{2}\,\omega^2$

$H=(\sigma_1)$

$K^H=\,?$

维数 $\Rightarrow K^H \cong \mathbb{Q}(\sqrt[3]{2}\,\omega^2)$

Ex. 对 G 所有子群计算固定子域

（此为期末考试风格，算+证明）

例: $|K|<+\infty$ $K/\mathbb{F}_p$ $\dim_{\mathbb{F}_p} K = n.$

$x^{p^n} \to$ 分裂域

$$\mathrm{Gal}(K/\mathbb{F}_p) = \{\mathrm{Id}, \sigma, \dots, \sigma^{n-1}\}$$

$\sigma: x \mapsto x^p$ Frobenius automorphism.

例. 任何有限群 G 可看作某Galois群

$G \leq S_n \curvearrowright k(t_1, \dots, t_n)$ n元有理函数域

$$\begin{matrix} k(t_1,\dots,t_n) \\ \parallel \\ K \end{matrix}$$

取 $E = K^G$

$\Rightarrow G = \mathrm{Gal}(K/E).$ //

偏序集 partially ordered set

例. $\mathbb{N}^+ = \{1, \cdots\}$

① $\leq$

② $\preceq$: $a \preceq b \Leftrightarrow a \mid b$.

例. G

$\mathrm{Sub}(G) = \{H \mid H \leq G\}$ $(\mathrm{Sub}(G), \subseteq)$

例

$\mathrm{Lat}(K/k) = \{E \mid E$ 中间域$\}$ Lattice

$(\mathrm{Lat}(K/k), \subseteq)$

例: $(L, \leq)$ 偏序集

反偏序集 $(L, \leq^{op})$

$$a \leq^{op} b \iff b \leq a$$

定义：给定 $(L, \leq)$

· $a, b \in L$ 定义 $a \quad b \in L$，为 a, b 最小上界，若

$$\begin{cases} a \leq a \vee b, \ b \leq a \vee b \\ \forall c, \ a \leq c, \ b \leq c \Rightarrow a \vee b \leq c \end{cases}$$

若∃，则唯一.

· $a, b \in L$ 定义 $a \wedge b \in L$，为 a, b 最大下界，若

$$\begin{cases} a \wedge b \leq a, \ a \wedge b \leq b \\ \forall c, \ c \leq a, \ c \leq b \Rightarrow c \leq a \wedge b \end{cases}$$

若∃，则唯一.

定义. 偏序集称格(Lattice), 若 $\forall a,b$

$a\vee b$. $a\wedge b$ 存在

例. 群 G $\quad$ $\mathrm{Sub}(G)$ 是格. (子群格).

$$H\wedge K = H\cap K$$

$$H\vee K = \langle H\cup K\rangle$$

例. K/k $\quad$ $\mathrm{Lat}(K/k)$.

$$E\wedge F = E\cap F$$

$$E\vee F = EF = \left\{(\textstyle\sum e_i f_i)(\sum e_i' f_i')^{-1}\right\}$$

L 为格 $\Leftrightarrow$ L^{op} 为格.

L, L' 偏序集

$f: L \to L'$ 同态 $\forall a \le b$

$f(a) \le f(b)$

$f: L \to L'$ 同构：f 双射，

f, f^{-1} 同态

Ex、$f: L \to L'$ 同构

$\Rightarrow f(a \wedge b) = f(a) \wedge f(b)$

Galois 理论的基本定理 K/k 有限 Galois 扩张

$G = \mathrm{Gal}(K/k)$

$$\mathrm{Sub}(G) \xrightarrow{\sim} \mathrm{Lat}(K/k)^{op}$$

$$H \longrightarrow K^H$$

$$\mathrm{Gal}(K/E) \longmapsfrom E$$

$H_1 \le H_2 \iff K^{H_1} \le K^{H_2}$

格同构.

Lagrange.

$|G| = |H||G:H|$

$\dim_k K = \dim_k k' \dim_{k'} K.$

$\dim_k K^H = [G:H]$

$G \curvearrowright \mathrm{Sub}(G)$ 共轭作用

$\sigma \cdot H = \sigma H \sigma^{-1}$

$H \in \mathrm{Sub}(G)^G \iff H \trianglelefteq G$

$G \curvearrowright \mathrm{Lat}(K/k)$

$\sigma \cdot E = \sigma(E)$

$E \in \mathrm{Lat}(K/k)^G \iff E/k$ Galois

命题. 格同构

$\mathrm{Sub}(G) \xrightarrow{\sim} \mathrm{Lat}(K/k)^{op}$

保持 G-作用

$\iff K^{\sigma H \sigma^{-1}} = \sigma(K^H)$

证: $v \in K^{\sigma H \sigma^{-1}}$

$\iff \sigma h \sigma^{-1}(v) = v, \forall h.$

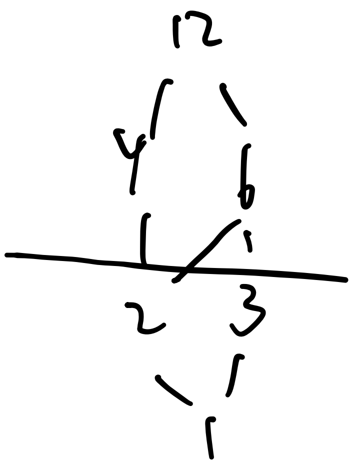
$\iff \sigma^{-1}(v) \in K^H$

$\iff v \in \sigma(K^H)$

定理. K/k Galois 扩张 $k \subseteq E \subseteq K$

E/k Galois $\iff \mathrm{Gal}(K/E) \trianglelefteq \mathrm{Gal}(K/k)$

$\mathcal{L}_{12} = \{1, 2, 3, 4, 6, 12\}$



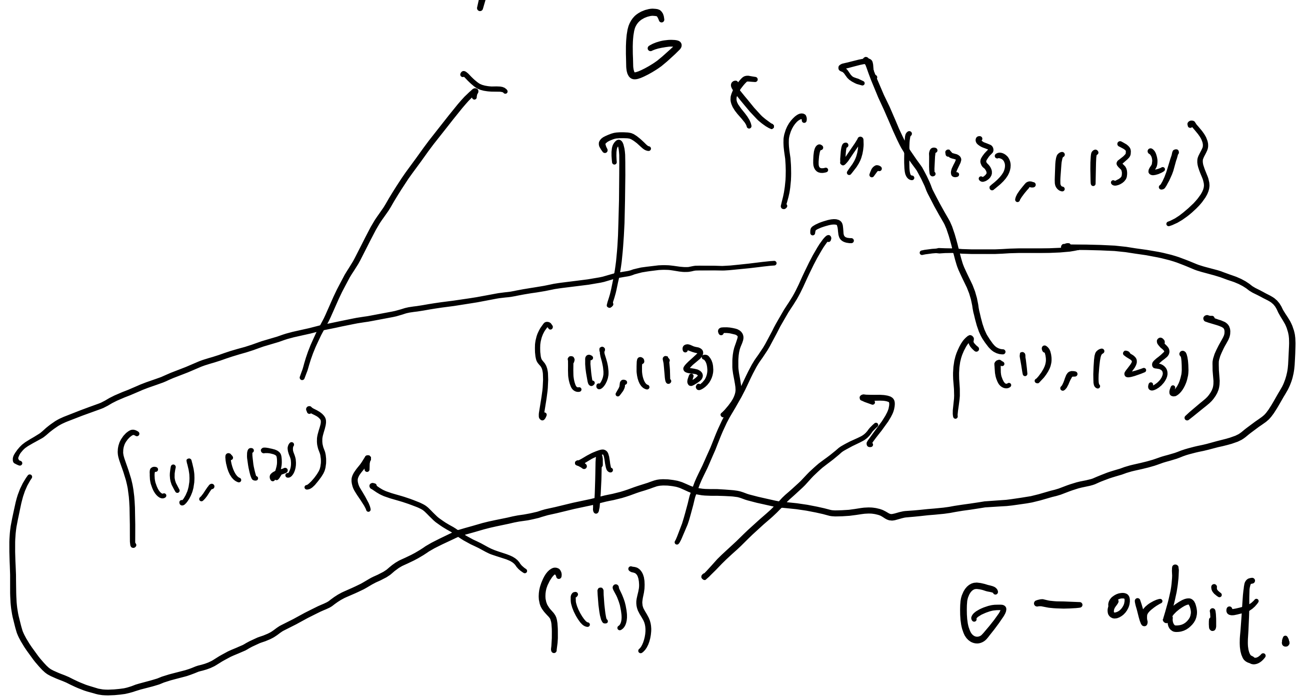
对称

序同: $\mathcal{L}_{12} \to \mathcal{L}_{12}^{op}$

$d \to 12/d$

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

$G = \mathrm{Aut}(K/\mathbb{Q}) \xrightarrow{\sim} S(X) \xrightarrow{\sim} S_3$



$(a\ b\ c)$ $\quad K \to K$

$$\sqrt[3]{2} \to \omega\sqrt[3]{2}$$

$$\omega\sqrt[3]{2} \to \omega^2\sqrt[3]{2}$$

$$\omega^2\sqrt[3]{2} \to \sqrt[3]{2}$$

$$\mathbb{Q}(\omega) \subseteq K^{\langle (abc) \rangle}$$

$$\dim_{\mathbb{Q}} K^{\langle (abc) \rangle} = 6/3 = 2.$$

应用.

Steinitz 1910. K/k 有限扩张.

例 K/k 单扩张 $\Leftrightarrow$ K/k 有限中间域

证: "$\Rightarrow$" $K = k(\alpha)$ α 在 k 上最小多项式 $f(x)$

$k \subseteq E \subseteq K$ $\quad \alpha$ 在 E 上极小多项式 $g(x)$

$g(x) \mid f(x)$ in $K[x]$

$g(x) = x^m + c_1 x^{m-1} + \dots + c_m$

$B = k(c_1, \dots, c_m)$

$B \subseteq E$

x在B上极小多项式也为$g(x)$

$\Rightarrow [K:B] = \deg g = [K:E]$

$\Rightarrow E = B$

$\Rightarrow$ 有限中间域(考虑B的构造)

$\Leftarrow$: $|k| = +\infty$ 时

$K = k(\alpha_1, \dots, \alpha_t)$

$k \subseteq \underset{E}{\underset{\shortparallel}{k(\alpha_1, \alpha_2)}} \subseteq K$

$\forall \lambda \in K \quad E_\lambda = k(\alpha_1 + \lambda\alpha_2)$

$\exists \lambda_1 \neq \lambda_2, \quad E_{\lambda_1} = E_{\lambda_2} \Rightarrow \alpha_1, \alpha_2 \in E_{\lambda_1}, E_{\lambda_2}.$

归纳即可

本原元定理. 设 K/k 有限可分扩张

$\Rightarrow K/k$ 单扩张

证明 $K = k(\alpha_1, \cdots, \alpha_k)$

作 E 为 $\alpha_1, \cdots, \alpha_k$ 极小多项式分裂域

E/k 有限中间域

4.4 根式扩张

定义：根式扩张

E/k 根式扩张，若

$\exists \alpha$, s.t. $E = k(\alpha)$ 且 $\exists m \in \mathbb{N}^*$, $\alpha^m \in k$

根式扩张塔.

定义. $f(x)$ 根式可解，若 $\exists$ 根式扩张塔

$k \subseteq k_1 \subseteq \cdots \subseteq k_n \subseteq E$

s.t. f 在 E 上分裂

Galois 大定理.

定义. E/k 根式扩张，若 $E = k(\alpha)$, $\exists n \geq 1$, s.t.

$\alpha^n \in k$, 记 n 为 E/k 的 type.

定义. 根式扩张塔

$k \subseteq E_1 \subseteq E_2 \subseteq \cdots \subseteq E_k$

相邻两域扩张为根式扩张.

Remark. E/F 根式扩张 of type m.

若 F 包含 m 次本原单位根, E/F 为 Galois 扩张.

$$x^m - a = \prod_{i=0}^{m-1} (x - \omega^i \alpha)$$

此时考虑 $\mathrm{Gal}(E/F) \hookrightarrow (\mathbb{Z}_m, +)$

$$\sigma(\alpha) = \omega^i \alpha \longmapsto i$$

对 E'/F $x^m - 1$ 分裂域.

$$\underline{\mathrm{Root}_{E'}(x^m - 1) \subseteq F^\times \text{ 子群}}$$

Recall 域乘法群的有限子群均循环

对 char E = 0 E' 中有本原单位根.

$$k \subsetneq E \subsetneq E' = E(w) = k'(\alpha)$$

$$k \subseteq k' \subsetneq E', \quad k' = k(w)$$

k'/k, E/k' 均为Galois 扩张.

$$\mathrm{Gal}(E/k) \hookrightarrow (\mathbb{Z}_m, +)$$

$$\mathrm{Gal}(k'/k) \hookrightarrow (\mathbb{Z}_m^{\times}, \times)$$

$$\sigma(w) = w^i \longmapsto \bar{i}$$

E/k 也为 Galois 扩张 $x^m - a$ 分裂域

$$\mathrm{Gal}(E'/k') \hookrightarrow \mathrm{Gal}(E'/k) \twoheadrightarrow \mathrm{Gal}(k'/k).$$

exact sequence.

$\mathrm{Gal}(E'/k) \supseteq \{\sigma \mid \sigma(E)=E\} \longrightarrow \mathrm{Gal}(E/k)$.

定义. $f \in k[x]$ 根式可解.

若∃根式扩张塔

$k \subseteq E_1 \subseteq E_2 \subseteq \cdots \subseteq E_n$

s.t. f 在 E_n 分裂.

Fact. $\mathrm{char}\, k = 0$.

任意根式扩张塔

$k \subseteq E_1 \subseteq \cdots \subseteq E_s$

可以扩成另一塔

$k \subseteq E_1 \subseteq \cdots \subseteq E_t$.

s.t. E_t/k Galois

在中间添加单位根.

若 $k = E_0 \subseteq E_1 \subseteq \cdots \subseteq E_n$ 塔.

E_n/k Galois, E_{i+1}/E_i Galois

$Gal(E_n/E_0) \triangleright Gal(E_n/E_1) \triangleright Gal(E_n/E_2)$.

设 f 在 k 上分裂域为 K

E_n/K Galois

$k \subseteq K \subseteq E_n$.

$Gal(E_n/k) \twoheadrightarrow Gal(K/k)$.

---

in general.

$k = E_0 \subseteq \cdots \subseteq E_n$ 塔.

k' 为 M 次分裂域, M 为 G 所有 Type 的倍数

$$
\begin{tikzcd}
 & E_n \arrow[dr, hook] & \\
k \arrow[ur, hook] \arrow[r, hook] & k' \arrow[r, hook] & E_n'
\end{tikzcd}
$$

将塔的每个域都添加单位根.

$$
\begin{tikzcd}
\mathrm{Gal}(E_n'/k') \arrow[r, hook] & \mathrm{Gal}(E_n'/k) \arrow[r, two heads] \arrow[d] & \mathrm{Gal}(k'/k) \\
 & \mathrm{Gal}_k(f) &
\end{tikzcd}
$$

正规子群. Abelian.

正合列.

定义. Given a finite group G, 称其可解 (solvable), 若 $\exists$ 子群链.

$$G = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_n = \{1\}.$$

- $G_{i+1} \trianglelefteq G_i$

· G_i / G_{i+1} 为 Abelian group.

例：

$S_3 \rhd A_3 \rhd \{1\}$.

例. ① Abel 群

☆ ② p-群可解.

p 群有非平凡的中心

归纳即得.

$P/Z(P)$ 可解.

$Z(P) \hookrightarrow P \twoheadrightarrow P/Z(P)$. 用①.

易证：p^n 阶群，p^{n-1} 阶子群必正规.

(仅有一个).

③ S_4, S_3 可解.

④ $H \leq G$ $\quad G$ 可解 $\Rightarrow$ H 可解
交一下即可.

⑤ A_5 不可解.

⑥. $N \trianglelefteq G$

G 可解 $\Leftrightarrow$ N 可解, G/N 可解.

$\Rightarrow$) : $\quad G_0 \geq G_1 \cdots\cdots$

$G_0/N \geq G_1N/N \geq G_2N/N \geq \cdots$

$\Leftarrow$

Galois 大定理.

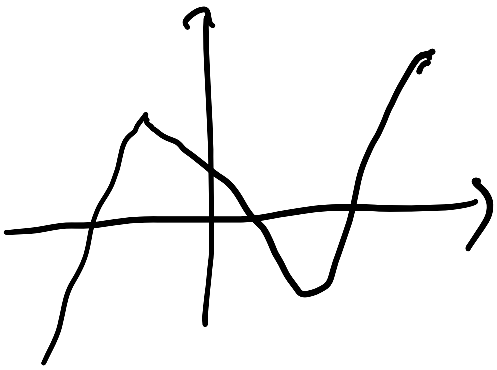
$\operatorname{char} k = 0.$ $\quad f \in k[x].$

· f 根式可解 $\Leftrightarrow$ $\mathrm{Gal}_k(f)$ 可解.

$\Rightarrow$: ✓.

$\Leftarrow$: ✓.

例. $f(x) = x^5 - 4x + 2$



Eisenstein

$\Rightarrow$ irreducible.

$$\mathrm{Root}_{\mathbb{C}}(f) = \{\alpha_1, \alpha_2, \alpha_3, \underbrace{\alpha_4, \alpha_5}_{\text{实}}\}$$

$5 \mid |\mathrm{Gal}_{\mathbb{Q}}(f)| \Rightarrow \mathrm{Gal}_{\mathbb{Q}}(f)$ has 5-cycle

共轭 $\Rightarrow (1\ 2) \in \mathrm{Gal}_{\mathbb{Q}}(f)$

$\Rightarrow \mathrm{Gal}_{\mathbb{Q}}(f) = S_5.$

Fact. $H \leq S_5$

$(1\ 2) \in H$, 5-cycle $\in H$

$\Rightarrow H = S_5$

例. $F = k(t_1, \cdots t_n)$.

n元有理函数域.

$f(x) = x^n - t_1 x^{n-1} + t_2 x^{n-2} - \cdots + (-1)^n t_n$.

称一般方程.

$y_1 \sim y_n$ 为 f 根.

Fact. $\mathrm{Gal}_F(f(x)) \xrightarrow{\sim} S_n$

$S_n \curvearrowright k[y_1, \cdots, y_n]$.

$\sigma.\ g(y_1, \cdots, y_n) \xrightarrow{\sim} g(y_{\sigma(1)}, \cdots, y_{\sigma(n)})$.

对称多项式基本定理：

$k[t_1, \cdots, t_n] \longrightarrow k[y_1, \cdots, y_n]^{S_n}$.（对称多项式）

$$t_i \longrightarrow \sum_{k_1 < \cdots < k_i} y_{k_1} \cdots y_{k_i}$$

$$\mathrm{Gal}_F(f) = \mathrm{Gal}\left(k(y_1, \cdots, y_n) / k(t_1, \cdots, t_n)\right)$$

$$= \mathrm{Gal}\left(k(y_1, \cdots, y_n) / k(y_1, \cdots, y_n)^{S_n}\right)$$

$$= S_n$$

注：若将 $k(t_1, \cdots, t_n)$ 视为 $k(y_1, \cdots, y_n)$ 子域

则 $k(y_1, \cdots, y_n)^{S_n} = k(t_1, \cdots, t_n)$.