

L17 节主要内容是：

- $\left\{ \begin{array}{l} \text{closure 相关概念} \\ \text{straightedge 例子 (设写)} \\ \text{finite field 作为有限乘法群 (1). 剩下在 L19 Galois 之后才会讲} \end{array} \right.$

def: \bar{F} 是 F 的 algebraic closure if; \bar{F} is algebraic over F .

$\left\{ \begin{array}{l} \forall f \in F[x], f \text{ splits completely over } \bar{F}, \text{ 即 } \bar{F} \text{ 中有 } n \text{ 个因子} \\ \text{且 } \bar{F} \Rightarrow \text{所有 } \bar{F} \text{ 中的数都是 } F \text{ 中的数} \end{array} \right.$

obv: $\bar{F} \Rightarrow \bar{F}$ algebraic number over F ; obv $\bar{F} = \bar{F}$

def: K is algebraically closed if: $\forall f \in K[x], \exists \text{ a root in } K, \nexists f \text{ is reducible, except } \deg(f) = 1$

obv: algebraic closure \bar{F} algebraically closed \bar{F}

prop 30: \forall field F , 存在一个 algebraic closed field $K \supseteq F$

{ prop 31: K is algebraically closed, $F \subseteq K$, then \bar{F} is algebraic closure of F .

algebraic closure is unique up to isomorphism, \uparrow \bar{F} 的定义: 在 F 上 alg 的所有元素

coro 32: 代数基本定理, \mathbb{C} is alge-closed;

Q: 请明白 def 和 prop 都很混乱; 为什么 alg-closure 是 ISO 而不是仅有一个.

finite field F :

• $|F| = p^d$ $p \in \text{Prime}$

• $\text{char}(F) = p$, p 定义为 $1+1+\dots+1=0$ 最少个数. $n \cdot 1 = (p \cdot q) \cdot 1 = (p \cdot 1) \cdot (q \cdot 1) = 0$

field 没有 zero-divisor $\therefore p \cdot 1 = 0$ 或 $q \cdot 1 = 0$ 由此下推, 可知 $\text{char}(F) = p$ for $|F| = p^d$.

但 p 不是 zero-divisor: p 除 1 元素外都是不在 F 中的

• $|F| = p^d$, $F_{p^d} \cong F_p \times F_p \times \dots \times F_p$ as group (F_{p^d}, \cdot)

有限 Abel group 定理: $|G| = p^r$, $G = \langle a_1 \rangle \times \langle a_2 \rangle \times \dots \times \langle a_r \rangle$, a_i 是 G 中阶最大的

由 char 定义知: $\forall x \in F_{p^d}, x + \dots + x = x \cdot r = 0$; 无 zero-divisor $\therefore 1 \cdot n = 0$, n 为 p . $\text{P.P}(x) = p \nmid x$

$x \in F_{p^d}$ 中 $x \neq 0$, n 是不["]在 field 中的

• $(F, +) \cong \mathbb{Z}_{p^d}$, F^* 已被 0 指剩下一 $p^d - 1$ 个元素

1. n 是 $1+1+\dots+1$ 产生的, 由 F 中, 1.7 是没有定义的

[设 $m = \text{lcm}(F^* \text{ 中元素的 order})$, 这是 group order 新的定义]

$\nexists F_3$, 1.7 的定义是 $1+1+\dots+1$ 产生的

由下节引理可知 F 是 cyclic (下面)

finite Abel

cyclic

prop: 在 field 中, $\text{lcm}(\text{所有元素的 order}) = \text{lcm}(\text{最大阶元素 } g) = |F|$ field as group

由于域生成的群均满足 "prop 1.5"

某子群 or 加法群均成立

引理：若 G 是有限阿贝尔群， G 是循环的 $\Leftrightarrow \exists g \in G$, $\forall n \in \mathbb{Z}^+$, $x^n = e$ 在 G 中至多有 n 个解

$\Rightarrow G$ 是循环的, $G = \langle g \rangle$ for some $g \in G$; $|G| = |\langle g \rangle| = n$

若 $x^n = e$, $x \in G$, 则 $\exists t \in \mathbb{Z}^+$, $x^n = e$

由于 $\text{gcd}(m, n)$ 用元素线性表示, 即 $\text{gcd}(m, n) = am + bn$ Some $a, b \in \mathbb{Z}$

$$\therefore x^{\text{gcd}(m, n)} = e, g^{t(m, n)} = e \quad \because n \mid t(m, n)$$

$$\therefore \frac{n}{\text{gcd}(m, n)} \mid t$$

$\therefore \langle g^t \rangle \subseteq \langle g^{\frac{n}{\text{gcd}(m, n)}} \rangle$, 则 $x \in \langle g^t \rangle \subseteq \langle g^{\frac{n}{\text{gcd}(m, n)}} \rangle$

即 $\forall x \in G$: $x^n = e$, $x \in \langle g^{\frac{n}{\text{gcd}(m, n)}} \rangle$,

$$|\langle g^{\frac{n}{\text{gcd}(m, n)}} \rangle| = k, g^{\frac{k}{\text{gcd}(m, n)}} = e, \frac{k}{\text{gcd}(m, n)}$$
 是最小公倍数 $= n \Rightarrow k = \text{lcm}(m, n) \leq m$

这样的 x 的个数至多 m 个

counter example: group $\langle a, b : a^2 = b^3 = (ab)^5 = e \rangle$ $x^2 = 1$ $x = a, b^2, ab$

$$n=4$$

• 有限阿贝尔群中, 存在元素 g . $|\langle g \rangle| = \text{lcm}(\text{所有元素的阶})$

• 阿贝尔群中, $a, b \in G$, $\text{d}(a) = m$, $\text{d}(b) = n$; $(m, n) = 1$ then $\text{d}(a, b) = mn$

设 g 是 G 中阶最大的元素, $|\langle g \rangle| = m$;

h 是 G 中任意元素, $|\langle h \rangle| = n$, 并设 $n \mid m$.

若不然: \exists prime p , $p \nmid n$, $p \nmid m$, $s > t$,

设 $n = xps$, $m = ypt$, $(x, p) = (y, p) = 1$

$\therefore |\langle h^x \rangle| = p^s$, $|\langle g^{p^t} \rangle| = y$ $\Rightarrow |\langle h^x \cdot g^{p^t} \rangle| = p^s \times y > p^t \times y = m$ 与阶最大矛盾

即阶最高的元素 g . $|\langle g \rangle| = \text{lcm}(\text{所有元素的阶})$

\Leftarrow 取 G 中阶最大的 g , $|\langle g \rangle| = n$; $|G| = l$ $n \leq l$

$\forall h \in G$, $h^n = 1 \Rightarrow h^n = 1$ 在 G 中有 l 个解 $l \leq n$

$\therefore |\langle h \rangle| \mid |\langle g \rangle|$

* Semidirect ("Exercise" section)

Consider the group action of multiple group on addition group, we can get a semidirect product of two groups such as $Z_p^d : Z_{p^d-1}$, denoted by $\text{AGL}_1(p^d)$.

Let F be a finite field of order p^d , i.e. \mathbb{F}_{p^d} or denoted by $\text{GF}(p^d)$.

Theorem 5. $\phi : F \rightarrow F$ s.t. $x \mapsto x^p$ is an automorphism of F . ★ See it in "Exercise" section

证明. Check: $(xy)^\phi = x^p y^p = x^\phi y^\phi$, $(x+y)^\phi = x^\phi + y^\phi$. This is called Frobenius automorphism. \square

$$x^{p-1}y + x^{p-1}y^p + \dots + xy^{p-1} = 0 \quad \text{因为 } \mathbb{F}_p \text{ 中 } p \neq 0, \mathbb{F}_p = \{0, 1, \dots, p-1\}$$