Algebra. Lec 19. Primitive element theorem, Finite fields.

Thm. 4.6 Primitive element theorem.

E. finite ext $/k$

$\exists\ \alpha \in E$ s.t. $E = k(\alpha)$. $\Longleftrightarrow$ $\exists$ only finite numbers of F.

$k \subset F \subset E$.

pf. if $|k| < \infty$ E: finite ext $/k$ $\therefore |E| < \infty$

$\therefore \exists\ \alpha.$ s.t. $k(\alpha) = E$

generator of $(E - \{0\})$ $\square$

$\therefore$ may assume k. is infinite field.

$\Leftarrow$). Assume $\exists$ only finite numbers of intermediate field F

Let $\alpha. \beta \in E$, consider $k(\alpha + c\beta)$. $c \in k$

$\Rightarrow k(\alpha + c_1\beta) = k(\alpha + c_2\beta)$. for some $c_1, c_2 \in k$. $c_1 \neq c_2$

$\Rightarrow (c_1 - c_2)\beta \in k(\alpha + c_1\beta)$

$\beta \in k(\alpha + c_1\beta)$

$\alpha \in k(\alpha + c_1\beta)$

$\therefore\ k(\alpha,\beta) = k(\alpha + c_1\beta)$ $\quad\quad$ $\therefore\ k(\alpha,\beta) = k(\alpha + c_1\beta)$ for some $c_1 \in k$

Now write $\quad E = k(\alpha_1, \dots, \alpha_n) = k(\alpha_1,\alpha_2)(\alpha_3, \dots, \alpha_n)$

$$= k(\alpha_1 + c_1\alpha_2, \alpha_3, \dots, \alpha_n)$$

$$\vdots$$

$$= k(\alpha_1 + c_1\alpha_2 + c_3\alpha_3 + \dots + c_n\alpha_n)$$

$\Rightarrow]$ $\quad$ Assume $\quad E = k(\alpha)$ $\quad\quad$ α. is alg$/k$

$f(x) = \mathrm{Irr}(\alpha, k, x)$.

Let $k \subset F \subset E$ $\quad\quad$ $g_F(x) = \mathrm{Irr}(\alpha, F, x)$

$$g_F(x) \mid f(x)$$

$F \longrightarrow g_F(x)$

$\quad\quad \shortparallel$ product of $(x - \alpha_i)$ $\quad$ $\alpha_i \in$ splitting field of $f(x)$

$\Rightarrow$ $g_F(x)$ only have finite possibility

$F_0 = k(\text{coff of } g_F(x)) \subset F$

$g_F(x)$. irred in $F[x]$ $\quad$ $\therefore$ also irred in $F_0[x]$

$\downarrow$

$\therefore\ (\text{deg of } \alpha \text{ over } F) = (\text{deg of } \alpha \text{ over } F_0)$

$$\therefore\ F = F_0$$

i.e. the int field F is uniquely determined by $g_F(x)$

i.e. $F \longrightarrow g_F(x)$ (bijective map). $\square$

Rmk E: finite ext $/k$

if E is also sep. $/k$. $\Rightarrow \exists \alpha \in E$. s.t. $E = k(\alpha)$

pf. $E = k(\alpha, \beta)$. α, β sep $/k$ (alg $/k$)

$n = [E:k]_s \leq [E:k] < \infty$

$\{\sigma_1, \dots, \sigma_n\}$ distinct embedding $E = k(\alpha, \beta) \hookrightarrow k^a$

---

let $P(x) = \prod_{i \neq j} (\sigma_i \alpha + X \sigma_i \beta - \sigma_j \alpha - x \sigma_j \beta)$

$P(x)$: not a zero polynomial

if zero $\Rightarrow$ $\begin{cases} \sigma_i \alpha = \sigma_j \alpha \\ \sigma_i \beta = \sigma_j \beta \end{cases} \Rightarrow \sigma_i = \sigma_j$ $\times$

$\therefore \exists c \in k$. st. $P(c) \neq 0$

$\therefore \sigma_i(\alpha + c\beta)$ distinct, $\forall i = 1, \dots, n$.

$n \leq [k(\alpha + c\beta) : k]_s \leq [k(\alpha, \beta) : k]_s = [k(\alpha, \beta) : k] = n$

$\cap$ for $k(\alpha, \beta)$

$\Rightarrow k(\alpha, \beta) = k(\alpha + c\beta) \dots$ $\square$

Finite fields.

F: field. $|F| = q < \infty$.

Construct. $\mathbb{Z} \xrightarrow{\varphi} F$

$1 \longmapsto 1$

$1+1 \longmapsto 1+1$

$1+1+1 \longmapsto 1+1+1.$

$\vdots$

φ: ring hom.

$\ker(\varphi) = \text{ideal of } \mathbb{Z} = k\mathbb{Z}$

$\ker(\varphi) \neq \{0\}$!

Claim: k must be a prime number.

pf. If not, say $k = k_1 k_2$

$k_1 \geq 2.\ k_2 \geq 2$

$\mathbb{Z} \xrightarrow{\varphi} F$

$k_1 k_2 \longmapsto \underbrace{(1+\cdots+1)}_{k_1 \text{ times}}\underbrace{(1+\cdots+1)}_{k_2 \text{ times}} = 0$

say $k_1 \cdot 1 = 0.$

$\Rightarrow \underline{k_1\mathbb{Z} \subseteq \ker(\varphi)} = \underline{(k_1k_2)\mathbb{Z} \subsetneq k_1\mathbb{Z}}$ $\times$

$\therefore \ker\varphi = p\mathbb{Z}$

In this case, we say the characteristic of F is p.

$\mathrm{Char}(F) = p$

$$\mathbb{Z}/p\mathbb{Z} \cong (1) \subseteq F$$

use "+" to generate

subfield.

$\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ called prime field.

Rmk. if $\exists F$: field. $|F|<\infty$

F contains a subfield $\simeq \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$

F : vs $/ \mathbb{F}_p$

$\because |F|<\infty$ $\{w_1, \dots, w_n\}$ basis of F as a vs $/ \mathbb{F}_p$.

$\therefore \{ a_1 w_1 + \dots + a_n w_n \mid a_i \in \mathbb{F}_p \} = F$

$\therefore |F| = p^n = q$

- Consider multiplicative group

$(F^\times = F - \{0\}, \times)$. $|F^\times| = q-1$

$\forall \alpha \in F^\times$, α satisfies $x^{q-1} = 1$.

$\forall \alpha \in F$, α satisfies $x^q - x = 0$

$\therefore f(x) = x^q - x$ has q distinct roots in F

$$= \prod_{\alpha \in F} (x-\alpha)$$

$\therefore F$ is the splitting field of $f(x) = x^q - x \in \mathbb{F}_p[x]$

$\Downarrow$

$\Rightarrow F$ is unique up to iso

Conversely

Given $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ $\quad \mathbb{F}_p^a$: alg closure of $\mathbb{F}_p$

Consider the splitting field of $X^{p^n} - X \in \mathbb{F}_p[x]$ in $\mathbb{F}_p^a$

claim. the splitting field $= \{$ roots of $X^q - X$ in $\mathbb{F}_p^a \}$

pf. $\left[\underline{\{\text{roots form a field}\}} \right.$

α, β : roots of $X^q - X = 0$

$(\alpha+\beta)^q - (\alpha+\beta) = \alpha^q + \beta^q - \alpha - \beta = 0$

$(\alpha\beta)^q - \alpha\beta = 0$

$0, 1 \in \{\text{roots}\}$

β^{-1} : also ...

$-\beta$: also —

$f(x) = X^{p^n} - X$

$Df(x) = p^n X^{p^n - 1} - 1 = -1 \neq 0.$

$\Rightarrow$ are roots are distinct. $\left.\right]$

Thm 5.1 For each prime p $n \geq 1$

$\exists$ a finite field of order p^n

uniquely determined as a subfield of $\overline{\mathbb{F}_p}^a$ (denote as $\mathbb{F}_q$)

It's the splitting field of $x^q - x \in \mathbb{F}_p[x]$ in $\overline{\mathbb{F}_p}^a$

splitting field $=$ { roots }

$\Rightarrow$ Every finite field is isomorphism to one $\mathbb{F}_q = \mathbb{F}_{p^n}$ in $\overline{\mathbb{F}_p}^a$

$\triangle$

Cor 5.2 $\mathbb{F}_q$. finite field.

In a given $\overline{\mathbb{F}_q}^a$, $\exists$ one and only one ext of $\mathbb{F}_q$ of degree n

and the ext is $\mathbb{F}_{q^n}$

① find 1

Pf. $q = p^m$ $q^n = p^{mn}$

$$\mathbb{F}_q \subseteq \mathbb{F}_{q^n} = \mathbb{F}_{p^{mn}} = \left\{ \begin{array}{c} \text{Splitting field of} \\ x^{q^n} - x \end{array} \right\} \subseteq \overline{\mathbb{F}_q}^a$$

$\forall \alpha \in \mathbb{F}_q$ $\alpha^q = \alpha$

$$\therefore \alpha^{q^n} = (\alpha^q)^{q^{n-1}} = \alpha^{q^{n-1}} = \cdots = \alpha^q = \alpha$$

②. uniqueness

any ext of deg n over $\mathbb{F}_q$, has deg mn over $\mathbb{F}_p$.

$\Rightarrow$ it's $\mathbb{F}_{p^{mn}}$ (i.e. $\mathbb{F}_{q^n}$)

Rmk (Thm 5.3)

$|F| < \infty$ ($F^\times = F - \{0\}$, $\times$). cyclic.

Frobenice mapping $\mathrm{char}(\mathbb{F}_q) = p$

$$\varphi : \mathbb{F}_q \longrightarrow \mathbb{F}_q \quad \Rightarrow \text{ field hom (ring)}$$
$$x \longmapsto x^p$$

field's ideal!

$\ker(\varphi)$: ideal of $\mathbb{F}_q$ $\Rightarrow$ $\ker(\varphi) = \{0\}$

$\Rightarrow$ φ : iso.

In general char $(F) = p$ $|F|$ not finite.

$$\varphi : F \to F \quad \text{field hom}$$
$$x \mapsto x^p \quad \& \text{ injective.}$$

Thm 5.4 The group of automorphism $\mathbb{F}_q \xrightarrow{\sim} \mathbb{F}_q$ is cyclic of order n generated by Frobenice φ

pf ① $G = \langle \varphi \rangle$ $\quad \varphi^n : \mathbb{F}_q \to \mathbb{F}_q$

$x \to \cdots = x$ $\quad$ id

let d be order of φ

$\varphi^d = \mathrm{id}$

$$\varphi^d(x) = x^{p^d} = x \quad \forall x \in \mathbb{F}_q$$

i.e. each $x \in \mathbb{F}_q$ is a root of $x^{p^d} - x = 0$. $\Rightarrow d \geq n$.

$\therefore d = n$.

② $\forall$ automorphism σ: fixes $\mathbb{F}_p = (1)$

for $\sigma : \mathbb{F}_q \xrightarrow{\sim} \mathbb{F}_q$, $1 \mapsto 1$, $\sigma(1) = 1$

$$\begin{tikzcd} \mathbb{F}_q \arrow[rr, "\sim"] \arrow[dr, dash] & & \mathbb{F}_q \arrow[dl, dash] \\ & \mathbb{F}_p & \end{tikzcd}$$

already form: $\{1, \varphi, \cdots, \varphi^{n-1}\}$

$$n \leq [\mathbb{F}_q : \mathbb{F}_p]_s \leq [\mathbb{F}_q : \mathbb{F}_p] = n$$

$$\begin{tikzcd} & \mathbb{F}_p^a \arrow[d, dash] \\ \mathbb{F}_q \arrow[ur] & \mathbb{F}_q \arrow[d, dash] \\ & \mathbb{F}_p \end{tikzcd}$$

$\therefore [\mathbb{F}_q : \mathbb{F}_p]_s = n$

HW

Lang chap V 12~17

Thm 5.5