3/18

Monday, March 18, 2019 11:30

Char $F \neq 2$, $[K:F]=2 \Rightarrow K = F(\sqrt{D})$, $D \in F$.

Char $F=2 \Rightarrow$? then this is not true:

Φ $\alpha \longrightarrow \alpha^2$ is a hom-sm

$$(\alpha+\beta)^2 = \alpha^2 + 2\alpha\beta + \beta^2 = \alpha^2+\beta^2.$$

If K is finite then Φ is an automorphism of K.

$\operatorname{Ker} \Phi = 0$ always.

If $\alpha \in K \setminus F$ then $\Phi(\alpha) \notin F$ so $\alpha^2 \neq D$.

HW Problem: $f(g(\alpha))$.

K/F , $\alpha \in K$ is algebraic over F, then $m_{\alpha,F}$ is irred. in $F[x]$.

Let $f \in F[x]$ be irred.

is there K/F & $\alpha \in K$ s.t. $f(\alpha)=0$?

Yes. put $K = F[x]/(f)$. Put $\alpha = \bar{x} = x \bmod f$.

then K is a field since (f) is max'l ideal.

$\forall g \in F[x]$, $g(\alpha) = g(\bar{x}) = g(x) \mod (f)$

in particular, $f(\alpha) = f \mod (f) = 0$.

So α is a root of f & $f = m_{\alpha, F}$.

$F \longmapsto F(\alpha)$ s.t. $f(\alpha) = 0$ is called adjoining a root of f.

it's always possible

$\sqrt{2}$, i. $\sqrt{2} = \alpha \in \mathbb{R}$ s.t. $\alpha^2 = 2$.

i is <u>defined</u> as root of x^2+1.

<u>Theorem</u> if $f \in F[x]$ is irr.ble, K_1/F, K_2/F are extensions,

$\alpha_1 \in K_1$, $\alpha_2 \in K_2$ are s.t. $f(\alpha_1) = f(\alpha_2) = 0$, then $F(\alpha_1) \underset{\varphi}{\cong} F(\alpha_2)$ s.t. $\varphi|_F = \mathrm{Id}_F$, $\varphi(\alpha_1) = \alpha_2$.

$$\begin{tikzcd} F(\alpha_1) \arrow[r, "\varphi"] & F(\alpha_2) \\ F \arrow[u, "\cup"] \arrow[r, "\mathrm{id}"'] & F \arrow[u, "\cup"'] \end{tikzcd}$$

<u>Proof</u> both $F(\alpha_i) \cong F[x]/(f)$ with $\alpha_i \longleftrightarrow x$.

$$F(\alpha_1) \cong F[x]/(f) \cong F(\alpha_2)$$

$$\alpha_1 \longleftrightarrow x \bmod f \longleftrightarrow \alpha_2 .$$

<u>B.1.1)</u> $f(x) = x^3 + 9x + 6 \in \mathbb{Q}[x]$. α is a root of F.

irr-le.

Find $(1+\alpha)^{-1}$ in $\mathbb{Q}(\alpha)$. $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$

basis is $\{1, \alpha, \alpha^2\}$.

want $(1+\alpha)^{-1} = a + b\alpha + c\alpha^2$.

$(a + b\alpha + c\alpha^2)(1+\alpha) = 1 \rightsquigarrow$ solve.

<u>OR</u>: $\cdot\alpha$ is a lin. transf. of $\mathbb{Q}(\alpha)$. find its matrix & invert it.

13.2.1) $|F| < \infty \Rightarrow \operatorname{char} F = p.$

Then $|F| = p^n$, $n \in \mathbb{N}$.

Pf $\mathbb{F}_p \subset F$, let $n = \dim_{\mathbb{F}_p} F = [F : \mathbb{F}_p]$.

then $F \cong \mathbb{F}_p^{\,n}$ as V. spaces.

2 $g(x) = x^2 + x - 1$, $h(x) = x^3 - x + 1 \in \mathbb{Z}_2[x]$.

construct fields of order 8.

0, 1 are not roots, so g, h are irred.

So $\mathbb{F}_2[x]/(g)$ & $\mathbb{F}_2[x]/(h)$ are fields

$\{ax+b : a, b \in \mathbb{F}_2\}$ 4 elts 8 elts.

g & h are also irred. in $\mathbb{Z}_3$, so we

can make fields of size 9 & 27

3 $m_{\alpha, \mathbb{Q}}$ for $\alpha = 1 + i$. $\alpha \in \mathbb{Q}(i)$.

$$(\alpha-1)^2 = -1 \quad \Rightarrow \quad \alpha^2 - 2\alpha + 2 = 0$$

$$\text{So } m_{\alpha,\mathbb{Q}} = x^2 - 2x + 2.$$

(5) $F = \mathbb{Q}(i)$.

Prove: $x^3 - 2$ is irr.-le over F.

If it weren't, then it has a linear factor $(x-c)$, so it has a root c. but x^3-2 is irr.-le over $\mathbb{Q}$, so $\deg_{\mathbb{Q}} c = 3$.

So $c \notin \mathbb{Q}(i)$.

So no roots in $\mathbb{Q}(i)$ so it's irr.-le over $\mathbb{Q}(i)$.

(10) $\alpha = \sqrt{3 + 2\sqrt{2}}$. $\deg_{\mathbb{Q}}(\alpha) = ?$

$$\begin{array}{c} \mathbb{Q}(\alpha) \\ \big| \; 2 \text{ or } 1 \\ \mathbb{Q}(\sqrt{2}) \\ \big| \\ \mathbb{Q}. \end{array}$$

$\exists\, a, b \in \mathbb{Q}$ s.t. $(a + b\sqrt{2})^2 = 3 + 2\sqrt{2}$?

Yes, $1+\sqrt{2}$ works. So $\alpha = 1 + \sqrt{2}$, $\deg_{\mathbb{Q}}(\alpha) = 2$.

(14) if $\deg_F \alpha$ is odd then $F(\alpha^2) = F(\alpha)$.

$$\begin{tikzcd} F(\alpha) \arrow[d, dash, "1 \text{ or } 2"'] \\ F(\alpha^2) \arrow[d, dash] \\ F \end{tikzcd} \quad \text{odd}$$

So it must be 1.

(19) $[K : F] = n$. $\forall \alpha \in K$, $\varphi_\alpha \in End_F K$ (as a v.s.)

$$\varphi_\alpha(\beta) = \alpha\beta.$$

$$K \longrightarrow Mat_{n \times n} F$$

hom-sm of rings.

This is embedding

So $Mat_{n \times n} F$ contains a copy of K.