

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

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

$\Phi: \alpha \rightarrow \alpha^2$ is a non-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 .

$\text{Ker } \Phi = 0$ 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 $\alpha = \bar{x} = x \text{ mod } f$.

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

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

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

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

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

it's always possible

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

i is defined as root of $x^2 + 1.$

Theorem if $f \in F[x]$ is irr. $K_1/F, K_2/F$ are extensions,
 $\alpha_1 \in K_1, \alpha_2 \in K_2$ are s.t. $f(\alpha_1) = f(\alpha_2) = 0,$

then $F(\alpha_1) \cong_{\varphi} F(\alpha_2)$ st. $\varphi|_F = \text{Id}_F$, $\varphi(\alpha_1) = \alpha_2$.

$$\begin{array}{ccc} F(\alpha_1) & \xrightarrow{\varphi} & F(\alpha_2) \\ \uparrow \nu & & \uparrow \nu \\ F & \xrightarrow{\text{id}} & F \end{array}$$

Proof both $F(\alpha_i) \cong F[x]/(f)$ with $\alpha_i \leftrightarrow x$.

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

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

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

irr-le.

Find $(1+\alpha)^{-1}$ in $\mathbb{Q}(\alpha)$.

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$$

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

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

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

OR! $-\alpha$ is a lin. trans. of $\mathbb{Q}(\alpha)$. find its matrix & invert it.

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

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

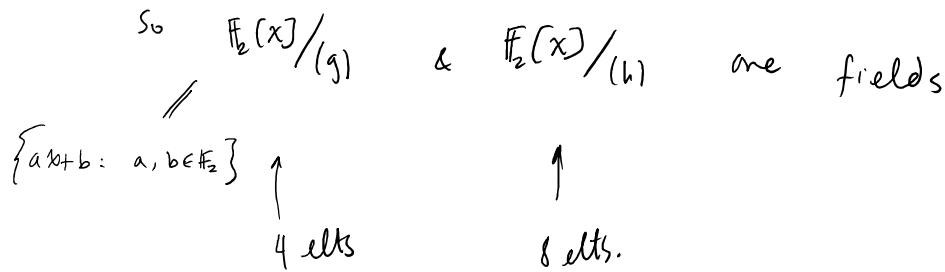
$\mathbb{F}_p \subset F$, let $n = \dim_{\mathbb{F}_p} F = [F : \mathbb{F}_p].$

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.



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

can make fields of size 9 & 27

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

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

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

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 $\deg_{\mathbb{Q}} c = 3.$

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

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

⑩

$$\alpha = \sqrt{3 + 2\sqrt{2}}.$$

$$\deg_{\mathbb{Q}}(\alpha) = ?$$

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

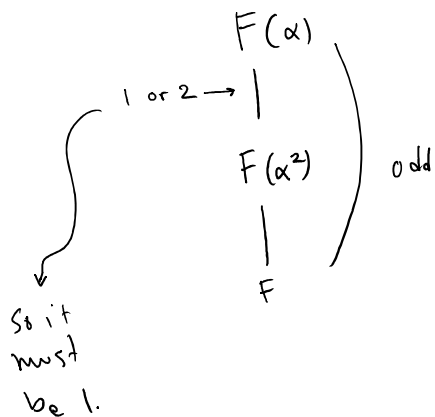
$$\begin{array}{c} \mathbb{Q}(\sqrt{2}) \\ | \end{array}$$

$$\mathbb{Q}.$$

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

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

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



(19) $[K : F] = n$. $\forall \alpha \in K$, $\varphi_\alpha \in \text{End}_F K$ (as a v.s.)

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

$$K \longrightarrow \text{Mat}_{n \times n} F$$

hom-om of rings.

This is embedding

So $\text{Mat}_{n \times n} F$ contains a copy of K .