Last time |

finite extension + degree.

finite $\iff$ algebraic + fin gen'd

alg elts are a subfield

Char | let F a field

$\exists!$ ring homo $\varphi : \mathbb{Z} \longrightarrow F$ $\rightsquigarrow$ $\mathbb{Z}$ is the init ring.

$1 \longmapsto 1$

$2 \longmapsto 1+1$

2 cases

1) φ is injective $\Rightarrow \mathbb{Z} \subset F$ subring

$\Rightarrow \mathbb{Q} \leq F$ subfield

"F has char 0"

2) $\ker(\varphi) \neq 0$ as $\operatorname{im}\varphi \cong \dfrac{\mathbb{Z}}{\ker \varphi}$ is a domain as subring of F

$\Rightarrow \ker \varphi$ is a prime ideal

$\Rightarrow \ker \varphi = (p)$ for prime $p \in \mathbb{Z}$

φ induces a field homo $\mathbb{F}_p \longrightarrow F$

$\mathbb{F}_p = \mathbb{Z}/(p)$

" F has char p "

Rmk | if $F \to K$ is any field homo $\Rightarrow$ char F = char K

Adjoining Elts |

Suppose E/F is a field extn

& let $a \in E$ be alg $/F$.

$\exists!$ ring homo $\varphi : F[x] \longrightarrow E$ $\quad ev_a$.

$h \longmapsto h(a)$

$\ker \varphi$ is a nonzero prime ideal (as $\operatorname{im}\varphi$ is a domain) as $F[x]$ is a PID, it is gen'd by some prime. → single

i.e. $\ker\varphi = (f(x))$ for some irred $f \in F[x]$

In fact $\exists!$ monic $f(x)$ that gives $\ker\varphi$

Defn This is the minimal poly for a

The min poly of a is irred

If $\exists\, g(x) \in F[x]$ so $g(a) = 0 \Rightarrow f \mid g$

$\left[\text{as } g(a) = 0 \Rightarrow g \in \ker\varphi = (f(x))\right]$

Eg 1) $E = \mathbb{C}$, $F = \mathbb{R}$, $a = i$

Min poly is x^2+1

2) $E = \mathbb{C}$, $F = \mathbb{Q}$, $a = \sqrt{2} + \sqrt{3}$

$f(x) = \deg 4$

3) $E = \mathbb{C}$, $F = \mathbb{Q}(\sqrt{2})$, $a = \sqrt{2} + \sqrt{3}$

$f(x) = (x-\sqrt{2})^2 - 3$

Prop let E/F $a \in E$ as abv.

let $f(x) \in F[x]$ be the min poly for a.

Then, $\dfrac{F[x]}{(f(x))} \cong F(a)$ recall, $\varphi: F[x] \to E$

$h(x) \mapsto h(a)$

$\operatorname{im}\varphi = F[a] = F(a)$

by 1st iso $\dfrac{F[x]}{\ker\varphi} \cong \operatorname{im}\varphi = F(a)$

$\ker\varphi = (f(x))$

Defn let E/F & K/F be field ext. An F-homo (F emb) is a field homo $E \to K$ that is the identity on F.

Carefully E/F is $\alpha: F \to E$, K/F is $\beta: F \to K$

let σ F-homo $\Rightarrow \alpha \circ \sigma = \beta$

$$\begin{tikzcd} E \arrow[r, "\varphi"] & K \\ F \arrow[u, "\alpha"] \arrow[ur, "\beta"'] & \end{tikzcd}$$

E.g.| Let $J: \mathbb{C} \to \mathbb{C}$ be complex conjugation.
Then J is an $\mathbb{R}$ aut of $\mathbb{C}$.
↳ (so)

Def| (Milne) Let F be a field and let $f(x) \in F$ be an irred poly
a stem field for F is a pair
$(E/F$ and $a)$
so $f(a) = 0$ and $E = F(a)$

Note: f is min poly of a (as irred)

Thm| Let $f(x) \in F[x]$ be irred.
a) A stem field for f exists
b) If $(E/F, a)$ and $(E'/F, a')$ are 2 stem fields,
$\exists!$ F isom $\sigma: E \to E'$ so $\sigma(a) = a'$

e.g.| $\alpha = \sqrt[3]{2} \in \mathbb{R}$ let $\beta = e^{2\pi i/3} \sqrt[3]{2} \in \mathbb{C}$
$\mathbb{Q}(a)$, $\mathbb{Q}(b)$ diff subfields of $\mathbb{C}$
but, both stem fields $(\mathbb{Q}(\alpha)/\mathbb{Q}, \alpha)$, $(\mathbb{Q}(b)/\mathbb{Q}, \beta)$
of $f(x) = x^3 - 2$
Thm $\Rightarrow$ $\exists!$ isom $\sigma: \mathbb{Q}(a) \to \mathbb{Q}(b)$ so $\sigma(a) = \beta$
↳ every field iso is a $\mathbb{Q}$-auto
↳ think

Pf| $E = \dfrac{F[x]}{(f(x))}$ This is a field since $f(x)$ is irred
$\exists$ natural homo $F \to E$
so E is an ext of F

let a = img of x in E
$\Rightarrow f(a) = 0$ $\Rightarrow$ $E/F, x$ is a stem field

b) Let $(E/F, a)$ be as in part a
$(E'/F, a')$ be a second stem field.

$\exists!$ Map $\varphi : F[x] \longrightarrow E'$

That is the identity on F & $x \mapsto a'$ (mapping prop poly ring)

so F-aut

φ is surj as $a' \in \operatorname{im}\varphi$ & $E' \cong F(a')$

induces an iso $\sigma : E \longrightarrow E'$

$$E = \frac{F[x]}{\ker\varphi}$$

as $\varphi(x) = a' \implies \sigma(a) = a'$

wts σ is unique.

Suppose $\gamma : E \longrightarrow E'$ is an F auto

s.t. $\gamma(a) = a'$ wts $\gamma = \sigma$

Let $x \in E$. Then $x = \sum_{i=1}^{n} c_i a^i$ $c_i \in F$

$$\left.\begin{aligned} \sigma(x) &= \sum c_i \sigma(a)^i \\ \gamma(x) &= \sum c_i \gamma(a)^i \end{aligned}\right\}$$ but $\sigma(a) = \gamma(a)$.

$\implies \sigma = \gamma$

Rmk | let E/F, K/F 2 exts

& $\sigma : E \to K$ field homo.

σ being F-homo $\iff$ σ is an F linear map.