Fact let F be a field, E alg. ext. of F $E \leq \overline{F}$

$\alpha, \beta \in E$ are conjugate

$\psi_{\alpha,\beta} : F(\alpha) \to F(\beta)$.

If all isomorphic maps from $E \to E' \leq \overline{F}$ fixing F are actually automorphisms of E, then E contains all conjugates of α.

Recall the splitting field of a set $\{f_j(x)\}$ of polynomials over F is the smallest subfield of $\overline{F}$ containing all the roots of all $f_j(x)$.

Thm If F is a field, $E \leq \overline{F}$ is an alg. extension of F. Then E is a splitting field $\iff$ Every automorphism of $\overline{F}$ fixing F maps $E \to E$.

Cor. If $E \leq \overline{F}$ is a splitting field over F, every irred polynomial in $F[x]$ having one zero in E splits in E.

Cor. If $E \leq \overline{F}$ is a splitting field over F, then every isomorphic mapping of E onto a subfield of $\overline{F}$ fixing F is actually an automorphism of E.

Thus. If E is a finite normal extension of F, then $\{E:F\} = |G(E/F)|$

$\{E:F\}$: # of isom of E onto a subfield of $\overline{F}$ fixing F

$|G(E/F)|$: # automorphisms of E fixing F.

Separability of fields & elements of Extension fields.

Thm If f is irred over $\mathbb{F}[x]$ for some field $\mathbb{F}$, all of the zeros of f have the same multiplicity.

Pf- Suppose α, β are two different zeros of $f(x)$ in $\overline{F}$.

Then $\psi_{\alpha,\beta}: F(\alpha) \to F(\beta)$ and can be extended to

$$\overline{\psi_{\alpha\beta}} : \overline{F} \to \overline{F}.$$

Then $\overline{\psi_{\alpha\beta}}\left((x-\alpha)^{\mu}\right) = (x-\beta)^{\mu}$

map on polynomials as on the coefficients.

β-multiplicity $\geq \alpha$-mult. Then reverse argument α-mult $\geq \beta$-mult.

If $(x-\alpha)^{\mu}$ is a factor of the irreducible poly $f(x)$, then $\overline{\psi_{\alpha\beta}}$ has to map this polynomial to itself (coefficients of $f(x)$ are in F).

We just saw then that $(x-\beta)^{\mu}$ must also be a factor of $f(x)$.

$\therefore$ Mult of α in $f(x)$ = mult of β in $f(x)$

True for any roots α, β of $f(x)$. ☒

Example of an inseparable algebraic extension.

Let $E = \mathbb{Z}_p(y)$ = rational fns in y with coeff in $\mathbb{Z}_p$.

$F = \mathbb{Z}_p(\underbrace{y^p}_{t})$ = rat. fns. in y^p w/ coeff in $\mathbb{Z}_p$.

Then E is algebraic over F, because y is a root of $x^p - t \in F[x]$

$F \neq E \Rightarrow \mathrm{irr}(y, F)$ has deg ≥ 2. [In fact, $x^p - t$ is irred over F.]

But $x^p - t = x^p - y^p = (x-y)^p$ ← y has multiplicity p.

Thm: If E is a finite extension of F, then $\{E:F\} \mid [E:F]$.

Proof: $E = F(\alpha_1, \alpha_2, \dots, \alpha_k)$

$irr(\alpha_1, F)$ — has n_1 distinct zeros of mult. μ_1

$$\{F(\alpha_1) : F\} = n_1$$

$$[F(\alpha_1) : F] = \deg irr(\alpha_1, F) = n_1 \mu_1$$

$irr(\alpha_2, F(\alpha_1))$ — has n_2 dist. zeros of mult μ_2

$$\{F(\alpha_1, \alpha_2) : F(\alpha_1)\} = n_2$$

$$[F(\alpha_1, \alpha_2) : F(\alpha_1)] = n_2 \mu_2$$

$\vdots$

keep going.

$$\{E : F\} = \prod n_j$$

$$[E : F] = \prod n_j \mu_j \quad \boxtimes$$

Defn. Let E be an algebraic extension field of F.

$\alpha \in E$ is called separable over F if All zeros of $irr(\alpha, F)$ have multiplicity 1.

E is a separable extension of F if $\forall \alpha \in E$, all zeros of $irr(\alpha, F)$ have mult. 1.

$\Longleftrightarrow \{E:F\} = [E:F]$

Facts: ① If $F \leq E \leq K$ then

K is a sep. extension of F

$\Longleftrightarrow$ Both E is a sep. ext. of F and K is a sep. ext. of E.

Pf: $\{K:F\} = \{K:E\}\{E:F\}$

$$[K:F] = [K:E][E:F].$$

Next time:

- Every finite algebraic extension is separable. $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$, $[\mathbb{F}_{p^n} : \mathbb{Z}_p]$ split. field of $x^{p^n} - x$.
- Every alg. extension of a field of char. 0 is separable. eg $\mathbb{C}/\mathbb{Q}(\sqrt{2})$ $\mathbb{Q}(2^{1/4})/\mathbb{Q}$