Last time:

E/F field ext. defined for $\alpha \in E$ $\min_F \alpha \in F[x]$

$\min_F \alpha$ is the unique monic generator of $\ker(F[x] \to E)$
$x \mapsto \alpha$

in particular, observe
- $[E:F] = \dim_F E = \deg \min_F \alpha$

Def: $\alpha \in E$ is algebraic$/_F$ if it is the root of some poly in $F[x]$

Observation: $\alpha \in E$ is algebraic $\Leftrightarrow$ $[F(\alpha):F] < \infty$

Notation: If E/F field ext. $\alpha \in E$
then $F[\alpha]$ = the subring of E gen. by α & F
= the image of $F[x] \to E$
$x \mapsto \alpha$

$F(\alpha)$ = the subfield of E gen by α & F
$= \mathrm{frac}(F[\alpha])$

"Observed" If α is algebraic then $F[\alpha] = F(\alpha)$

Note: if $\alpha \in E$ not algebraic over F then $F[x] \to E$
$x \mapsto \alpha$

is injective $\Rightarrow$ im $= F[\alpha] \cong F[x]$
we say α is transcendental. $F(\alpha) = F(x)$.

Below: we are going to consider extensions of some given field F

We say F is the "ground field"

<u>Quick consequences:</u>

If $\alpha \in E$ is algebraic over F then so is any element $\beta \in F(\alpha)$.

$F(\beta) \subset F(\alpha)$

$ \uparrow$ f.d. $\Rightarrow F(\beta)$ f.d. $/ F$.

If $F \subset E \subset L$ are extensions w/ $[E:F] = n < \infty$

$[L:E] = m < \infty$

then $[L:F] = mn$ "tower law"

<u>Pf:</u> if $\{e_i\}$ basis for E over F & $\{l_j\}$ basis for L/E

then $e_i l_j$ is a basis for L over F.

<u>Observe:</u> if $\alpha, \beta \in E$ then $\underset{F(\alpha)(\beta) = F(\beta)(\alpha)}{[F(\alpha,\beta) : F(\alpha)]} \leq [F(\beta):F]$

if $F \subset L \subset E$ then $[L(\beta):L] \leq [F(\beta):F]$

$\min_L \beta \mid \min_F \beta$

same poly which β is a root of w/ coeffs in $L \supset F$

$[F(\alpha,\beta):F] = [F(\alpha,\beta):F(\alpha)]\,[F(\alpha):F]$

$\leq [F(\beta):F]\,[F(\alpha):F] < \infty$ if α, β both algebraic.

Cor: if α, β algebraic, then so is $\alpha+\beta$, $\alpha\beta$, etc.

Rem: $\sqrt{2}$, $\sqrt[3]{5}$ alg. over $\mathbb{Q}$. $\sqrt{2}+\sqrt[3]{5}$

x^2-2 x^3-5

$1 \quad \sqrt{2}$

$1 \quad \sqrt[3]{5} \quad (\sqrt[3]{5})^2$

Consequence: if $F \subset E$ the set $\overline{F}^E = \{\alpha \in E \mid \alpha \text{ alg. over } F\}$ is a subfield of E.

$\mathbb{Q} \subset \mathbb{C}$ $\quad$ $\mathbb{Q} \subset \mathbb{R}$

$\overline{\mathbb{Q}}^{\mathbb{C}}$ $\quad$ $\overline{\mathbb{Q}}^{\mathbb{R}}$

A few more observations

Def A simple extension is one of the form $F(\alpha)/F$ & α is called a primitive element for the extension.

Rem. A finite (= finite dim'l $/F$) simple extension is always of the form $\frac{F[x]}{(f)}$ $f = \min_F \alpha$.

Consequence: if $f \in F[x]$ irred, α, β roots of f in E then $F(\alpha) \cong F(\beta)$

Def A poly $f \in F[x]$ splits if it can be written as a product of linear factors. $f = (x-a_1)(x-a_2)\cdots(x-a_n)$

Lemma: given $f \in F[x]$ $\exists E/F$ finite s.t. f splits in $E[x]$.

Pf: induct on largest degree of an irred factor of f. & on # of irred factors of that degree.

If $\prod(\text{lines})$ ✓

let $f = g \cdot h$

g: irred, largest deg.

let $L = \frac{F[x]}{(g)}$ let $\alpha = \bar{x}$ α root of g in L.

in $L[x]$, $g = (x-\alpha)\tilde{g}$ $\tilde{g}$ smaller degree.

E $\underbrace{\text{field ext. of } L \text{ s.t. } \tilde{g}h \text{ splits}}_{\text{exist by induction.}}$, E splits f.

Sublemma: if g has a root α in L then $g = (x-\alpha)\tilde{g}$

Pf

$$\begin{aligned} L[x] &\longrightarrow L \\ x &\longmapsto \alpha \\ g &\longmapsto 0 \end{aligned}$$

ker $L[x]$ pre gen by irred poly

$\underline{x-\alpha}$ in kernel. $\Rightarrow$ generates

$\Rightarrow g \in (x-\alpha)L[x]$

Recall: showed that $L[x]$ is a PID by noting that smallest non-zero deg element in an ideal generates. □

Splitting fields

Given a poly $f \in F[x]$, choose E/F s.t. f splits in E

Can consider the subfield of E gen. by roots of f

$f = (x-\alpha_1) \cdots (x-\alpha_n) \quad \alpha_i \in E, \quad F(\alpha_1, \ldots, \alpha_n)$

Call $F(\alpha_1, \ldots, \alpha_n)$ splitting field for f

Prop: the splitting field, up to iso, doesn't depend on choice of E.

Strategy: adjoin roots one by one, use $L(\beta) = \frac{L[x]}{\min_L \beta} \ldots \square$.

Def: If E/F is a field ext, we say E is an algebraic closure of F if E is alg. over F & if every poly in $F[x]$ splits in E.

Thm: algebraic closures exist.

Pf: Use transfinite induction:

Principle: every set can be well ordered: a total ordering s.t. every nonempty subset has a min'l element.

Given $(S, \leq)$ well ordered and a proposition P on elements of S: P true for all $s \in S$ if $\quad P(s) = P$ true for s.

i) P true for min'l elmt.

ii) if $P(s)$ for all $s < s_0$ then $P(s_0)$.

let choose a well order on $F[x]$.

given $f \in F[x]$ set F_f

F_f if f = min'l elmt $\Rightarrow$ F_f = splitting field for f over F.

given F_g $g < f$ define F_f

Let $F_f' = \bigcup_{g<f} F_g$ set F_f = sp. field for f over F_f'

note $g < f$ then $F_g < F_f$ set $\overline{F} = \bigcup F_f$

<u>Thm</u> (Artin) finite dimensional.

$E|F$ finite " is simple iff $\exists$ finitely many subextensions

$$F \subset L \subset E.$$

<u>Pf</u>: If F is infinite & $\exists$ only finitely many extensions then E simple.

Let $F \subset L \subset E$ w/ L max'l simple. $L = F(\alpha)$

Claim: $L = E$

let $\beta \in E$ consider extensions of form

$$F(\alpha + \lambda\beta) \quad \lambda \in F$$
$$\subset F(\alpha, \beta) \subset E.$$

So $\exists \lambda_1, \lambda_2$ s.t. $F(\alpha + \lambda_1\beta) = F(\alpha + \lambda_2\beta)$

in $F(\alpha+\lambda_1\beta) = F(\alpha+\lambda_2\beta)$ have elements

$$(\alpha+\lambda_1\beta)-(\alpha+\lambda_2\beta) = (\lambda_1-\lambda_2)\beta$$

$$\Rightarrow \beta \in F(\alpha+\lambda_1\beta)$$

$$(\lambda_1-\lambda_2) \in F^* \subset F(\alpha+\lambda_1\beta)$$

then $\alpha+\lambda_1\beta - \lambda_1\beta = \alpha \in F(\alpha+\lambda_1\beta)$

$\Rightarrow \alpha, \beta \in F(\alpha+\lambda_1\beta) \supseteq F(\alpha)$ maxl

$$\Rightarrow \beta \in F(\alpha) \ \square.$$