Lecture 17 2/19/2021

Splitting fields

Let F be a field, $f \in F[x]$ irreducible over F. If $\deg f \geq 2$, then f has no roots in F. (otherwise $f = (x-\alpha)g$ where α is the root)

But there is always an extension $F \subseteq K$ where f has a root in K.

Take $K = F[x]/(f)$ and $F \subseteq K$

Then $\alpha = x + (f)$ is a root of f in K since if $f = \sum_{i=0}^{n} a_i x^i$ $a_i \in F$

$$f(\alpha) = \sum_{i=0}^{n} a_i (x + (f))^i$$

$$= \left(\sum_{i=0}^{n} a_i x^i\right) + (f) = 0 + (f).$$

Def. Let $F \subseteq K$ be a field extension and let $f \in F[x]$. Then K is a splitting field for f over F if

(i) f splits over K, i.e. $f = c(x-\alpha_1)\cdots(x-\alpha_n)$ in $K[x]$.

(ii) $K = F(\alpha_1, \dots, \alpha_n)$.

Ex. Let $f = x^n - 1 \in \mathbb{Q}[x]$.

over $\mathbb{C}$, $f = (x-\zeta)(x-\zeta^2)\cdots(x-\zeta^n)$,

$\zeta = e^{2\pi i/n}$ is primitive nth root of 1

So $K = \mathbb{Q}(\zeta, \zeta^2, \dots, \zeta^n)$ is a splitting field for f over $\mathbb{Q}$.

Actually $K = \mathbb{Q}(\zeta)$.

$[K:\mathbb{Q}] = \deg \operatorname{minpoly}_{\mathbb{Q}}(\zeta) = \varphi(n)$

(later)

If $n = p$ is prime,

$$x^p - 1 = (x-1)(x^{p-1} + \cdots + x + 1)$$

irr. over $\mathbb{Q}$

So if $\zeta = e^{2\pi i/p}$, $\operatorname{minpoly}_{\mathbb{Q}}(\zeta) = x^{p-1} + \cdots + x + 1$

So $[\mathbb{Q}(\zeta):\mathbb{Q}] = p-1$.

Lemma. Let F be a field, $f \in F[x]$. Then there exists a splitting field K for f over F.

Pf. First we prove there is $F \subseteq L$ where f splits over L.

Induction on degree of f.

If $\deg f = 0$ or 1 take $K = F$.

Also if f splits over F, $K = F$.

Assume f has an irreducible factor of degree ≥ 2 in $F[x]$, g.

There is an extension $F \subseteq L'$ where g has a root in $L'[x]$, α.

So $f(\alpha) = 0$. Then $f = (x-\alpha) f_1$ in $L'[x]$, $\deg f_1 < \deg f$. By induction there is $L' \subseteq L$ s.t. f_1 splits in $L[x]$.

Now f splits in $L[x]$.

Take $K = F(\alpha_1, \dots, \alpha_n)$ as the splitting field, where $f = c(x-\alpha_1)\cdots(x-\alpha_n)$ in $L[x]$.

<u>Ex.</u> $f = x^p - q$ p, q primes.

Splitting field of f over $\mathbb{Q}$.

Let $\alpha = \sqrt[p]{q} \in \mathbb{R}$.

Let $\zeta = e^{2\pi i/p}$.

Then $\alpha, \alpha\zeta, \alpha\zeta^2, \ldots, \alpha\zeta^{p-1}$ are roots of f in $\mathbb{C}$.

$K = \mathbb{Q}(\underline{\alpha}, \underline{\alpha\zeta}, \ldots, \alpha\zeta^{p-1}) \subseteq \mathbb{C}$.

$= \mathbb{Q}(\alpha, \zeta)$ is the splitting field.

$\text{minpoly}_{\mathbb{Q}}(\zeta) = x^{p-1} + \cdots + x + 1$

$\text{minpoly}_{\mathbb{Q}}(\alpha) = f = x^p - q$ (Eisenstein)

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

$[\mathbb{Q}(\zeta) : \mathbb{Q}] = p-1$

So $[\mathbb{Q}(\alpha, \zeta) : \mathbb{Q}] = p(p-1)$ (last time)

Lemma. Let $\phi: F \to F'$ be an isomorphism of fields. Then $\phi: F[x] \to F'[x]$ be the induced $\cong$.

Let $f \in F[x]$ be irreducible and $f' \in F'[x]$ where $f' = \phi(f)$.

Let $F \subseteq K$ where $\alpha \in K$ is a root of f

Let $F' \subseteq K'$ " $\alpha' \in K$ " " f'.

Then considering $F \subseteq F(\alpha) \subseteq K$

$F' \subseteq F'(\alpha') \subseteq K'$,

there is an isomorphism $\theta: F(\alpha) \to F'(\alpha')$ s.t. $\theta(\alpha) = \alpha'$ and $\theta|_F = \phi$.

Cor. If $\alpha, \alpha' \in K$ are roots of irreducible $f \in F[x]$ and $F \subseteq K$ then $F(\alpha) \cong F(\alpha')$.

in fact there is an iso

$\theta : F(\alpha) \to F(\alpha')$ s.t.

$\theta(\alpha) = \alpha'$, $\theta|_F = 1_F$.

Pf. Take $\phi : F \to F$ as 1_F

take $K = K'$.

Pf of lemma.

$f = \text{minpoly}_F(\alpha)$ $f' = \text{minpoly}_{F'}(\alpha')$

Now there are isos

$$F(\alpha) \xrightarrow{\sigma_1} F[x]/(f) \xrightarrow{\sigma_2} F'[x]/(f') \xrightarrow{\sigma_3} F'(\alpha')$$

take $\theta = \sigma_3 \sigma_2 \sigma_1$

σ_1, σ_3 come from thm on simple extensions. σ_2 is induced by ϕ.

Note $\theta(\alpha) =$

$$\alpha \overset{\sigma_1}{\longmapsto} x+(f) \xrightarrow{\sigma_2} x+(f') \xrightarrow{\sigma_3} \alpha'.$$

$\theta|_F = \phi$ is easy.

<u>Thm.</u> Let $\phi: F \to F'$ be an iso inducing $\phi: F[x] \to F'[x]$.

Let $f \in F[x]$, $f' = \phi(f)$.

Let K be a splitting field for f over F

Let K' " " " f' over F'.

Then there is an iso $\sigma: K \to K'$ s.t. $\sigma|_F = \phi$.

<u>Cor.</u> if K, K' are splitting fields for $f \in F[x]$, then $K \cong K'$

<u>Pf.</u> Take $\phi: F \to F$ $\phi = 1_F$.

<u>Pf</u> of thm:

Induct on $\deg f$. If f splits already in F, then $K = F$, f' splits, so $K' = F'$. Take $\sigma = \phi$. So done if $\deg f = 0$ or 1.

Now assume f has an irreducible factor g of degree ≥ 2. g splits in K, let $\alpha \in K$ be any root. Let $g' = \phi(g) \in F'[x]$, which is irreducible over F'. Let $\alpha' \in K'$ be a root of g'.

$$\begin{tikzcd} K \arrow[r, "\sigma"] \arrow[d, dash] & K' \arrow[d, dash] \\ F(\alpha) \arrow[r, "\theta"] \arrow[d, dash] & F'(\alpha') \arrow[d, dash] \\ F \arrow[r, "\phi"] & F' \end{tikzcd}$$

By the lemma, there is an iso $\theta : F(\alpha) \longrightarrow F'(\alpha')$. $\theta|_F = \phi$, $\theta(\alpha) = \alpha'$.

Now if $f = (x - \alpha) f_1$

so $f' = (x - \alpha')\, \theta(f_1)$

By induction since $\deg f_1 < \deg f$ there is an iso $\sigma : K \longrightarrow K'$ s.t. $\sigma|_{F(\alpha)} = \theta$.

Because K is the splitting field of f_1 over $F(\alpha)$
K' " " $\theta(f_1)$ " $F'(\alpha')$

Then $\sigma|_F = \theta|_F = \phi$.

<u>Cor.</u> Let $f \in F[x]$ and let K be a splitting field of f over F. If g is an irreducible factor of f in $F[x]$, and α, α' roots of g in K. Then there is an automorphism $\sigma : K \longrightarrow K$ s.t. $\sigma(\alpha) = \alpha'$ and $\sigma|_F = 1_F$.

<u>Ex.</u> We proved along the way in the theorem.