Splitting Fields §50

Recall isomorphism extensions.

Def 49.9 E finite extension of F

The index of E over F is:

identity map

$\{E:F\}$ = # of extensions of $id: F \to F$ to $\tau: E \to \tau[E]$ isomorphism where $\tau[E] \leq \overline{F}$

Thm $|G(E/F)| \leq \{E:F\} \leq [E:F]$.

$\Uparrow$ $\Uparrow$

Proof all automorphisms are isomorphisms. exercise 49.13

Example

$$
\begin{array}{ccc}
 & & \overline{\mathbb{Q}} \\
\mathbb{Q}(2^{1/3}, i) & \longrightarrow & ? \\
| & & \\
\mathbb{Q}(2^{1/3}) & \rightrightarrows & \mathbb{Q}(2^{1/3}),\ \mathbb{Q}(e^{2\pi i/3}2^{1/3}),\ \mathbb{Q}(e^{4\pi i/3}2^{1/3}) \\
| & & | \\
\mathrm{id} : \mathbb{Q} & \longrightarrow & \mathbb{Q}
\end{array}
$$

$$\{a_0 + a_1 2^{1/3} + a_2 2^{2/3}\} = \mathbb{Q}(2^{1/3}) \qquad a_0, a_1, a_2 \in \mathbb{Q}$$

$$\{\mathbb{Q}(2^{1/3}) : \mathbb{Q}\} = 3$$

$$\| \qquad \text{Notice}$$

$$[\mathbb{Q}(2^{1/3}) : \mathbb{Q}]$$

Exercise

$$\{\mathbb{Q}(2^{1/3}, i) : \mathbb{Q}(2^{1/3})\}$$

$$\{\mathbb{Q}(2^{1/3}, i) : \mathbb{Q}\}$$

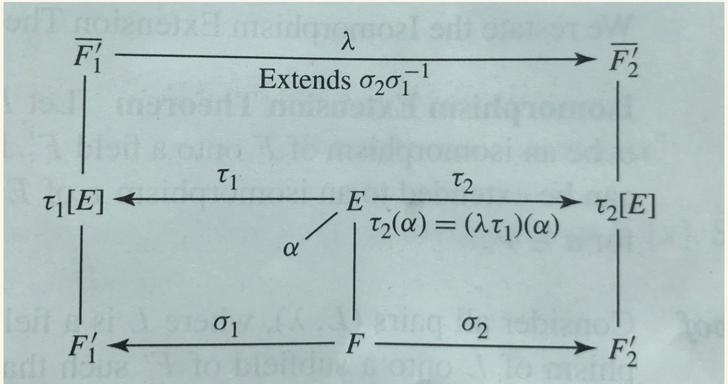
$$\begin{tikzcd} K = \mathbb{Q}(2^{1/3}, e^{2\pi i/3} 2^{1/3}, e^{4\pi i/3} 2^{1/3}) \arrow[r] \arrow[d, dash] & ? \\ \mathrm{id} : \mathbb{Q} \arrow[r] & \mathbb{Q} \end{tikzcd}$$

Thm 49.7 Let E be a finite ext of F and $\sigma : F \to F'$ an isomorphism. The # of extensions of σ to $E \xrightarrow[\simeq]{} E'$ for some $E' \leq \overline{F'}$ is finite and independent of F', $\overline{F'}$, and σ.

Proof start with F_1', F_2' and $\sigma_1 : F \to F_1'$, $\sigma_2 : F \to F_2'$

want to make a bijection:

$$\underbrace{\{\tau_1 : E \to \tau_1[E]\}}_{\text{ext'n of } \sigma_1} \longrightarrow \underbrace{\{\tau_2 : E \to \tau_2[E]\}}_{\text{ext'n of } \sigma_2}$$



49.8 Figure

To see that the # of extensions is finite see text or exercise 49.13 which proves $\{E:F\} \leq [E:F] = n$.

Corollary 49.10 If $F \leq E \leq K$ where K is a finite extension field of F then $\{K:F\} = \{K:E\}\{E:F\}$.

We will soon establish that $\{E:F\} = [E:F]$ for finite fields or fields of char $= 0$

Def 50.1 Let $\mathcal{F} = \{ f_i(x) \mid i \in I \}$ be a collection of polynomials in $F[x]$. The splitting field of $\mathcal{F}$ over F is the smallest field $E \leq \overline{F}$ s.t. $F \leq E$ and E contains all zeros of polynomials in $\mathcal{F}$.

"splitting" $\Rightarrow \forall f_i \in \mathcal{F}$, $f_i(x)$ "splits" into linear factors over E.

Say K is a splitting field over F if $\exists$ a collection of polynomials $\mathcal{F} \subset F[x]$

Example 50.8

$\mathbb{Q}(\sqrt{2}, \sqrt{3})$ is the splitting field of $\{x^2-2, x^2-3\}$ and $\{x^4-5x^2+6\}$.

$\{\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}\} = 4$

all extensions of $id : \mathbb{Q} \to \mathbb{Q}$ are automorphisms

$G(E/F) =$
$\{id, \sigma_1, \sigma_2, \sigma_3\}$

$$\begin{tikzcd}
\mathbb{Q}(\sqrt{2}, \sqrt{3}) \arrow[rr] \arrow[d, dash] & & \mathbb{Q}(\sqrt{2}, \sqrt{3}) \arrow[d, dash] \\
\mathbb{Q}(\sqrt{2}) \arrow[rr, shift left, "\sqrt{2} \mapsto \sqrt{2}"] \arrow[rr, shift right, "\sqrt{2} \mapsto -\sqrt{2}"'] \arrow[dr, dash] & & \mathbb{Q}(\sqrt{2}) \arrow[dl, dash] \\
& \mathbb{Q} &
\end{tikzcd}$$

Klein 4-group!

How to think about the splitting field:

Suppose E is a splitting field of $\mathcal{F} \subset F[x]$

let $Z = \{ \alpha_j \mid \alpha_j \text{ zero of some } f \in \mathcal{F} \} \subset \overline{F}$

- If $|Z| = k < \infty$ then $E = F(\alpha_1, \alpha_2, \ldots, \alpha_k)$.
- If $|Z| = \infty$ then E consists of all <u>finite</u> sums and <u>finite</u> products of elements in Z and F. (see beginning of proof 50.3).

An isomorphism of E fixing F is determined by where it sends Z.

Thm 50.3 A field E where $F \leq E \leq \overline{F}$ is a splitting field over F if and only if every isomorphism of $\overline{F}$ leaving F fixed restricts to an automorphism of E.

Proof Let E be a splitting field and $\sigma : \overline{F} \to \overline{F}$ an automorphism with $\sigma(a) = a \ \forall a \in F$.

For $\alpha_j \in \mathcal{Z}$ $\sigma(\alpha_j)$ must be a conjugate of α_j hence $\operatorname{irr}(\alpha_j, F) = \operatorname{irr}(\sigma(\alpha_j), F)$ and $\sigma(\alpha_j)$ is a zero of some $f \in \mathcal{F}$ $\Rightarrow$ $\sigma(\alpha_j) \in E$.

So $\sigma(E) \subset E$ and is in fact an automorphism.

Suppose every $\sigma: \overline{F} \to \overline{F}$ fixing F restricts to an automorphism of E.

let $\mathcal{F} = \{ g(x) \in F[x] \mid$ irreducible $g(x)$ has a zero in $E \}$.

<u>claim</u> E is splitting field of $\mathcal{F}$. (see text)

<u>idea</u>: if $\alpha \in E$ $\alpha \notin F$ it is the zero of some $g \in \mathcal{F}$. If β is conjugate consider $\psi_{\alpha,\beta}: F(\alpha) \to F(\beta)$ and its extension to $\overline{F} \to \overline{F}$. This must restrict to an automorphism of E hence $\beta \in E$.

Corollary 50.6 If $E \leq \overline{F}$ is a splitting field over F then every irreducible polynomial in $F[x]$ with a zero in E splits over E.

Corollary 50.7 If $E \leq \overline{F}$ is a splitting field over F of finite degree then

$$\{E : F\} = |G(E/F)|.$$

Exercise 50.10 Let α be a zero of x^3+x^2+1 over $\mathbb{Z}_2$. Show that it splits in $\mathbb{Z}_2(\alpha)$. What are the other zeros?

$$\alpha, \ \alpha^2, \ \alpha^4 = \alpha(\alpha^3) = \alpha(\alpha^2+1) = \alpha^3+\alpha.$$

$$(x+\alpha)(x+\alpha^2)(x+\alpha^3+\alpha) = x^3+x^2+1.$$