MATH 403/503 - L40

[Judson §23.1] Field Automorphisms

Recall The symmetric group S_X on a set X is the set of all bijections $\sigma: X \to X$. It is a group under composition.

Lemma Let E/F be a field extension.

Define

$\mathrm{Aut}(E) = \{\sigma: E \to E \mid \sigma$ is a (ring) automorphism$\}$

$\mathrm{Gal}(E/F) = \{\sigma \in \mathrm{Aut}(E) \mid \sigma|_F = \mathrm{Id}_F\}$

Then

$\mathrm{Gal}(E/F) \leq \mathrm{Aut}(E) \leq S_E$

Pf $\emptyset \neq \mathrm{Gal}(E/F) \subseteq \mathrm{Aut}(E)$ so both nonempty.

If $\sigma, \tau \in \mathrm{Aut}(E)$ then

$(\sigma\tau^{-1})(x+y) = \cdots$

$xy = \cdots$

$1 = \cdots$

so $\sigma\tau^{-1} \in \mathrm{Aut}(E)$. If $\sigma, \tau \in \mathrm{Gal}(E/F)$ then $\sigma\tau^{-1}|_F = \mathrm{Id}_F$ too ∎

Def $\mathrm{Gal}(E/F)$ is the Galois group of the extension E/F.

Ex $\sigma : \mathbb{C} \to \mathbb{C}$, $\sigma(z) = \bar{z}$. Then $\sigma \in Gal(\mathbb{C}/\mathbb{R})$.

Ex $\sigma : \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{2})$, $\sigma(a+b\sqrt{2}) = a - b\sqrt{2}$. Then $\sigma \in Gal(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$.

Ex Consider $\mathbb{Q} \subset \mathbb{Q}(\sqrt{3}) \subset \mathbb{Q}(\sqrt{5}, \sqrt{3}) = E$

$x^2 - 5 \in \mathbb{Q}(\sqrt{3})[x]$ is irr

$\pm\sqrt{5} \in \mathbb{Q}(\sqrt{5}, \sqrt{3}) = E$ are two roots.

By section on splitting fields, the identity map $\mathbb{Q}(\sqrt{3}) \to \mathbb{Q}(\sqrt{3})$ can be extended to a map $\sigma : E \to E$ s.t. $\sqrt{5} \mapsto -\sqrt{5}$

$$\begin{array}{ccc} E & \xrightarrow{\sigma} & E \\ | & & | \\ \mathbb{Q}(\sqrt{3}) & \xrightarrow{Id} & \mathbb{Q}(\sqrt{3}) \end{array}$$

Similarly $\exists\, \tau \in Aut(E)$ s.t. $\tau|_{\mathbb{Q}(\sqrt{5})} = Id$ and $\tau(\sqrt{3}) = -\sqrt{3}$

$\langle \sigma, \tau \rangle \cong \mathbb{Z}_2 \times \mathbb{Z}_2$

we will soon show $Gal(E/\mathbb{Q}) = \langle \sigma, \tau \rangle$.

Prop 23.5 Let E/F be an extension of fields and $f(x) \in F[x]$. Then any $\sigma \in Gal(E/F)$ permutes the roots of $f(x)$ lying in E.

Pf $f(x) = c_0 + c_1 x + \cdots + c_n x^n \quad c_i \in F$

Let $\alpha \in E$ be a root. Then

$$f(\sigma(\alpha)) = c_0 + c_1 \sigma(\alpha) + \cdots + c_n \sigma(\alpha)^n =$$

$$= \sigma(c_0) + \sigma(c_1)\sigma(\alpha) + \cdots + \sigma(c_n)\sigma(\alpha)^n =$$

since $\sigma|_F = Id$

$$= \sigma\left(c_0 + c_1\alpha + \cdots + c_n\alpha^n\right) = \sigma\left(\underbrace{f(\alpha)}_{=0}\right) = 0$$

So $\sigma(\alpha)$ is also a root. ∎

Def Call $\alpha, \beta \in E$ conjugate over F if they have the same minimal pol.

Recall from splitting field section:

Prop If $\alpha, \beta \in E$ are conjugate over F, then

~~[illegible]~~

$\exists$ isomorphism $\sigma : F(\alpha) \to F(\beta)$ such that

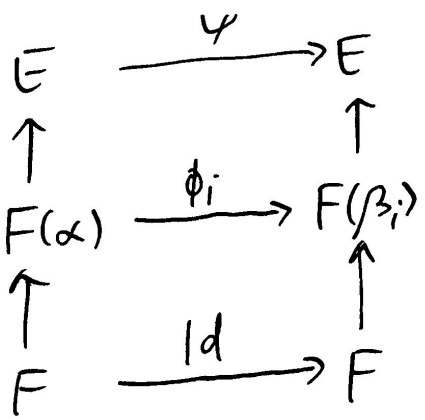
$\sigma|_F = Id_F$, $\sigma(\alpha) = \beta$.

Th 23.7

Let $f(x) \in F[x]$, let E be the splitting field for $f(x)$ over F. If $f(x)$ is separable (= no repeated roots in E) then

$$|Gal(E/F)| = [E:F]$$

Proof Induction on $n = [E:F]$, $n=1$ being trivial. If $n>1$, let $f(x) = p(x)q(x)$ where $p(x)$ is irr of degree $d>1$ (If all irr factor of $f(x)$ have degree 1 then $f(x)$ splits over F so $n=1$). Let $\alpha \in E$ be a root of $p(x)$. If $\phi: F(\alpha) \to E$ is any homomorphism s.t. $\phi|_F = Id_F$ then $\beta := \phi(\alpha)$ is also a root of $p(x)$. Since $f(x)$ has no repeated roots there are exactly d su isomorphisms $\phi_i: F(\alpha) \to F(\beta_i) \subset E$, one for each root $\beta_i \in E$ of $p(x)$. Conside



Since E is a splitting field for $f(x)$ over F, it is so over F and over $F(\beta_i)$. Since $[E:F(\alpha)]$ induction hypothesis implies each ϕ_i has exactly $\frac{n}{d}$ exte to an isomorphism $\psi: E \to E$

Example. $E = \mathbb{Q}(\sqrt{3}, \sqrt{5}) \supset \mathbb{Q}$

we saw $H := \langle \sigma, \tau \rangle \leq \mathrm{Gal}(E/\mathbb{Q})$, $|H| = 4$

Also we now know

$$|\mathrm{Gal}(E/\mathbb{Q})| = [E : \mathbb{Q}] = 4$$

so $\mathrm{Gal}(E/\mathbb{Q}) = \langle \sigma, \tau \rangle$

Example. Let's compute the Galois group of (the splitting field over $\mathbb{Q}$ of)

$f(x) = x^4 + x^3 + x^2 + x + 1 = \frac{x^5 - 1}{x - 1}$

The splitting field is $\mathbb{Q}(\zeta_5)$, where

$\zeta_5 = \exp(2\pi i/5)$ as the roots of

$f(x)$ in $\mathbb{C}$ are $\zeta_5, \zeta_5^2, \zeta_5^3, \zeta_5^4$.

Define $\sigma_i : \mathbb{Q}(\zeta_5) \to \mathbb{Q}(\zeta_5)$ by $i = 1, 2, 3, 4$

$\sigma_i(\zeta_5) = \zeta_5^i$, $\sigma_i|_{\mathbb{Q}} = \mathrm{id}_{\mathbb{Q}}$

Note $\{\sigma_i\}_{i=1}^4 = \{(\sigma_3)^i\}_{i=1}^4$ and $\sigma_1 = \mathrm{id}$

In fact σ_3 has order 4 so

$$\mathbb{Z}_4 \cong \langle \sigma_3 \rangle \leq \mathrm{Gal}(\mathbb{Q}(\zeta_5)/\mathbb{Q})$$

But also, since $f(x)$ is irr/$\mathbb{Q}$,

$$4 = [\mathbb{Q}(\zeta_5) : \mathbb{Q}] = |\mathrm{Gal}(\mathbb{Q}(\zeta_5)/\mathbb{Q})|$$

$$\Rightarrow \mathrm{Gal}(\mathbb{Q}(\zeta_5)/\mathbb{Q}) = \langle \sigma_3 \rangle \cong \mathbb{Z}_4$$