Day 26 July 15, 2024

Recall: A polynomial $p(x) \in F[x]$ **splits** if we can write
$$p(x) = c(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n).$$
If $p(x)$ splits over $E = F(\alpha_1, \dots, \alpha_n)$, then we call E a **splitting field** for $p(x)$.

Thm: Splitting fields exist.

<u>Lemma</u>: Suppose we have

1. an isomorphism of fields $\phi: E \to F$;
2. extension fields $K \supset E$ and $L \supset F$;
3. an alg. elt. $\alpha \in K$ with minimal polynomial $p(x) \in E[x]$;
4. a root $\beta \in L$ of $\phi(p(x)) \in F[x]$.

Then there exists a unique extension of ϕ to an isomorphism $\Phi: E(\alpha) \to F(\beta)$ s.t. the following diagram commutes:

$$\begin{tikzcd}
K \arrow[d] & L \arrow[d] \\
E(\alpha) \arrow[r, dashed, "\Phi"] \arrow[d, "\substack{\alpha \\ \downarrow \\ 0}"'] & F(\beta) \arrow[d, "\substack{\beta \\ \downarrow \\ 0}"] \\
E \arrow[r, "\phi"] & F
\end{tikzcd}$$

$$\Phi(c_0 + c_1\alpha + \cdots + c_{n-1}\alpha^{n-1})$$
$$\parallel$$
$$\phi(c_0) + d_1\beta + \cdots + d_{n-1}\beta^{n-1}$$

(Proof ingredients) $E(\alpha) \cong E[x]/\langle p(x) \rangle$ & $F(\beta) \cong F[x]/\langle \phi(p(x)) \rangle$ + linear algebra.

Thm Suppose we have
1. an isomorphism of fields $\phi : E \to F$;
2. a nonconstant polynomial $p(x) \in E[x]$;
3. a splitting field $K \supset E$ of $p(x)$ and a splitting field $L \supset F$ of $\phi(p(x))$.

Then ϕ extends to an isomorphism $\psi : K \to L$.

Cor. Splitting fields are unique, up to isomorphism.

(Proof.) If $K, L \supset E$ are splitting fields for $p(x) \in E[x]$, apply the previous theorem to the isomorphism $id : E \to E$:

$$\begin{tikzcd} K \arrow[r, dashed, "\psi"] & L \\ E \arrow[u] \arrow[r, "id"] & E \arrow[u] \end{tikzcd}$$

$\blacksquare$

(Proof of theorem.)

We apply induction on $n = \deg p(x)$.

Base: $n = 1$. Then $K = E$ and $L = F$, so we can let $\psi = \phi$.

Inductive hypotesis: Assume the the theorem holds for polynomials of degree $1 \le k < n$. Assume also that $p(x)$ is irreducible.

Now pick a root $\alpha \in K$ of $p(x)$ and a root $\beta \in L$ of $\phi(p(x))$. From previous lemma, $\exists$ isomorphism $\overline{\Phi} : E(\alpha) \to F(\beta)$:

$$\begin{tikzcd} E(\alpha) \arrow[r, "\overline{\Phi}"] \arrow[d] & F(\beta) \arrow[d] \\ E \arrow[r, "\phi"] & F \end{tikzcd}.$$

In $E(\alpha)[x]$ we can write

$$p(x) = (x-\alpha) f(x),$$

for some $f(x) \in E(\alpha)[x]$. Similarly,

$$\phi(p(x)) = (x-\beta)\, g(x),$$

for some $g(x) \in F(\beta)[x]$.

Moreover, $\Phi(f(x)) = g(x)$, and $K \supset E(\alpha)$ & $L \supset F(\beta)$ are splitting fields for $f(x)$ & $g(x)$, respectively. Since $\deg f(x) = \deg g(x) < \deg p(x)$, I.H. gives an isomorphism ψ s.t.

$$\begin{tikzcd} K \arrow[r, "\psi"] \arrow[d] & L \arrow[d] \\ E(\alpha) \arrow[r, "\overline{\Phi}"] & F(\beta) \end{tikzcd}$$

commutes. ∎

Galois groups

Given any field, let $\mathrm{Aut}(F)$ denote the set of field automorphisms of F.

Prop. For any field F, $\mathrm{Aut}(F)$ is a group under composition.

Prop. Let $E \supset F$ be a field extension. Then

$$G(E/F) := \{\sigma \in \mathrm{Aut}(E) \mid \sigma(\alpha) = \alpha,\ \forall\, \alpha \in F\} \subseteq \mathrm{Aut}(E)$$

is a subgroup of $\mathrm{Aut}(E)$.

(Proof.) • $\mathrm{id} \in G(E/F)$.

• $\sigma, \tau \in G(E/F) \Rightarrow$

$$\begin{aligned}(\sigma \circ \tau^{-1})(\alpha) &= \sigma(\tau^{-1}(\alpha)) \\ &= \sigma(\alpha) \\ \text{b/c } \tau(\alpha)=\alpha \qquad &= \alpha\end{aligned}$$

$\therefore\ \sigma \circ \tau^{-1} \in G(E/F)$. ∎

Def. For any field extension $E \supset F$, $G(E/F)$ is called the **Galois group of E over F.** If $f(x) \in F[x]$ has splitting field E over F, then the **Galois group of $f(x)$ over F** is $G(E/F)$.

Ex. Consider $\mathbb{Q}(\sqrt{3}, \sqrt{5}) \supset \mathbb{Q}$.

Any elt. of $\mathbb{Q}(\sqrt{3}, \sqrt{5})$ can be written $a + b\sqrt{3}$, with $a, b \in \mathbb{Q}(\sqrt{5})$. Define

$$\sigma(a + b\sqrt{3}) := a - b\sqrt{3},$$

an automorphism of $\mathbb{Q}(\sqrt{3}, \sqrt{5})$. Similarly, elts. can be written $c + d\sqrt{5}$, with $c, d \in \mathbb{Q}(\sqrt{3})$. Define

$$\tau(c + d\sqrt{5}) := c - d\sqrt{5}.$$

Later we'll see that

$$G(\mathbb{Q}(\sqrt{3}, \sqrt{5})/\mathbb{Q}) = \{\mathrm{id}, \sigma, \tau, \sigma\tau\} \cong \mathbb{Z}_2 \times \mathbb{Z}_2.$$

Prop. Let $E \supset F$ be a field extension, $f(x) \in F[x]$. Then any element of $G(E/F)$ permutes the roots of $f(x)$ which lie in E.

(Proof.) Pick a root $\alpha \in E$ of $f(x)$ and an automorphism $\sigma \in G(E/F)$. We NTS that $\sigma(\alpha)$ is a root of $f(x)$.

Write $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in F[x]$.

Then $0 = a_0 + a_1 \alpha + \cdots + a_n \alpha^n$.

Now apply σ:

$$\begin{aligned}
\sigma(0) &= \sigma(a_0 + a_1 \alpha + \cdots + a_n \alpha^n) \\
0 &= \sigma(a_0) + \sigma(a_1)\sigma(\alpha) + \cdots + \sigma(a_n)\sigma(\alpha)^n \\
0 &= a_0 + a_1 \sigma(\alpha) + \cdots + a_n \sigma(\alpha)^n \\
0 &= f(\sigma(\alpha)).
\end{aligned}$$

So $\sigma(\alpha)$ is a root of $f(x)$. ∎