

Last lecture

- (Theorem 30.3) Splitting fields are unique up to isomorphism. More precisely, if $\theta : F \rightarrow K$ is an isomorphism of fields, Σ is a splitting field for $f(x) \in F[x]$, and L is a splitting field for $\theta(f)$ then θ extends to an isomorphism $\Sigma \rightarrow L$.
- An extension $E:F$ is **normal** if every irreducible polynomial $f(x) \in E[x]$ which has at least one root in F splits over F .
- (Theorem 30.6) An extension $E:F$ is normal and finite if and only if E is the splitting field for some polynomial over F .

This lecture

Separable polynomials and Galois extensions.

Two easy lemmas for polynomials over splitting fields

Lemma 31.1

Suppose that Σ is a splitting field for an irreducible polynomial $f(x) \in F[x]$. Then $[\Sigma:F] \leq (\deg f)!$.

Proof We argue by induction on $d = \deg f$.

If $d = 1$ then $F = \Sigma$ and the result holds since $[F:F] = 1$.

If $d > 1$ then let α be a root of $f(x)$ and set $E = F(\alpha)$.

Then $[E:F] = d$ and $f(x) = (x - \alpha)g(x)$, for some $g(x) \in E(\alpha)[x]$.

$\implies [\Sigma:E] \leq (d-1)!$ since Σ is a splitting field for $g(x)$.

Therefore, $[\Sigma:F] = [\Sigma:E][E:F] \leq (d-1)!d = d!$ by Proposition 24.4 \square

Lemma 31.2

Let Σ be a splitting field for $f(x) \in F[x]$ and suppose that $\alpha \in \Sigma$ is a root of $f(x)$. Then $\theta(\alpha)$ is a root of $f(x)$, for all $\theta \in \text{Gal}(\Sigma:F)$.

Proof As $0 = f(\alpha) = \theta(f(\alpha)) = f(\theta(\alpha))$, $\theta(\alpha)$ is a root of $f(x)$. \square

Finite normal extensions

Theorem 30.6

An extension $E:F$ is normal and finite if and only if E is a splitting field for some polynomial over F .

Proof (\implies) Suppose that $E:F$ is normal and finite

$\implies E = F(\alpha_1, \dots, \alpha_d)$ is an algebraic extension by Corollary 25.5.

Let $m_i(x) \in F[x]$ be the minimum polynomial of α_i over F

and set $f(x) = m_{\alpha_1}(x) \dots m_{\alpha_d}(x)$ in $F[x]$.

By definition, each $m_i(x)$ is irreducible in $F[x]$ and has at least one root in E , so each $m_i(x)$ splits over E since E is normal.

$\implies f(x)$ splits over E

$\implies E$ is the splitting field of $f(x)$ over F since no subfield of E contains all of the roots of $f(x)$.

Therefore, E is the splitting field of some polynomial over F as claimed.

(\impliedby) Suppose that E is the splitting field of $f(x) \in F[x]$.

$\implies [E:F]$ is finite by Lemma 31.1.

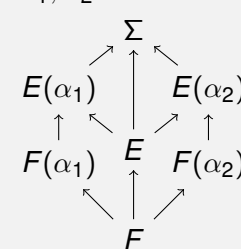
The proof that splitting fields are normal.../2

To show that $E:F$ is normal fix an irreducible polynomial $a(x) \in F[x]$.

Let Σ be a splitting field of a over E

$\implies \Sigma$ is a splitting field for af over F .

Let $\alpha_1, \alpha_2 \in \Sigma$ be two roots of $a(x)$ and consider $F(\alpha_i)$ and $E(\alpha_i)$.



By Theorem 25.2 the identity map on F extends to an isomorphism

$\theta : F(\alpha_1) \rightarrow F(\alpha_2)$

which is determined by $\theta(\alpha_1) = \alpha_2$.

Now, $E(\alpha_i)$ is a splitting field for f over $F(\alpha_i)$

$\implies \theta$ extends to an isomorphism

$E(\alpha_1) \xrightarrow{\sim} E(\alpha_2)$ by Theorem 30.3

$\implies \theta$ extends to an isomorphism $\Sigma \xrightarrow{\sim} \Sigma$ by Theorem 30.3

The map $\theta : \Sigma \rightarrow \Sigma$ fixes the set of the roots of $f(x)$ by Lemma 31.2

$\implies \theta$ restricts to a map $E \xrightarrow{\sim} E$

$\implies \alpha_1 \in E$ if and only if $\alpha_2 = \theta(\alpha_1) \in E$

Therefore, E contains one root of a if and only if it contains all roots.

Thus, $E:F$ is a normal extension of F as claimed. \square

Separable extensions

Definition 31.3

- An irreducible polynomial $f(x) \in F[x]$ is **separable** over F if f has distinct roots in its splitting field; otherwise, f is **inseparable**.
- If $E:F$ is an algebraic extension then $\alpha \in E$ is **separable** over F if its minimum polynomial over F is separable.
- An algebraic extension $E:F$ is **separable** if every element of E is separable over F .

Examples

- Any polynomial is separable over \mathbb{Q} by Theorem 30.1.
- The extension $\mathbb{C}:\mathbb{Q}$ is separable.
- Let $F = \mathbb{F}_p[t]$, for $p > 0$ prime, and let $f(x) = x^p - t \in F[x]$. Let Σ be a splitting field for $f(x)$ and let $\alpha \in \Sigma$ be a root of f .
 $\implies \alpha^p = t \implies (x - \alpha)^p = x^p - \alpha^p = x^p - t = f(x)$
 That is, $f(x) = x^p - t = (x - \alpha)^p$, so that the multiplicity of the root α is $f(x)$ is $p \implies f(x)$ is **not** separable over F .

Inseparable extensions

Proposition 31.4

Suppose that F is a field of characteristic $p \geq 0$ and that f is an irreducible polynomial over F .
 Then f is inseparable over F if and only if $p > 0$ and $f(x) \in F[x^p]$.

Sketch of proof Let Σ be the splitting field of f over F .

Define the **formal derivative** on $F[x]$ to be the F -linear map

$$D: F[x] \longrightarrow F[x] \text{ determined by } D(x^n) = nx^{n-1}, \text{ for } n \geq 0.$$

It is easy to check that $D(ab) = D(a)b + aD(b)$, for $a, b \in F[x]$.

Now, f is inseparable $\iff f$ has a repeated root

$$\iff \gcd(f, Df) \neq 1 \text{ (Check!)}$$

$$\iff Df = 0 \text{ since } f \text{ is irreducible and } \deg Df < \deg f$$

$$\iff p > 0 \text{ and } f(x) = f_0 + f_1 x^p + \dots + f_d x^{pd}, \text{ for } f_i \in F. \quad \square$$

Counting isomorphisms for separable extensions

Theorem 31.5

Suppose that $E:F$ and $K:L$ are separable extensions, and that $\theta: F \longrightarrow L$ is an isomorphism such that E is a splitting field for f over F and K is a splitting field for $\theta(f)$. Then the number of isomorphisms $E \xrightarrow{\cong} K$ which extend θ is $[E:F]$.

Proof As in Theorem 25.2, if $\alpha \in E$ (where $\alpha \notin F$) then θ extends to an isomorphism $F(\alpha) \xrightarrow{\cong} L(\beta)$ such that $\theta(\alpha) = \beta$, where β is any root of $\theta(m_\alpha)$. Now, $F(\alpha):F$ is separable because $E:F$ is separable

$$\implies L(\beta):L \text{ is separable as } L(\beta) \cong F(\alpha)$$

$$\implies \text{there are exactly } [F(\alpha):F] = [L(\beta):L] \text{ choices for } \beta, \text{ each of which gives a different isomorphism extending } \theta.$$

The assumptions of the Theorem still hold for $E:F(\alpha)$ and $K:L(\beta)$

$$\implies \text{by induction there are } [E:F(\alpha)] = [K:L(\beta)] \text{ extensions of each such isomorphism } F(\alpha) \xrightarrow{\cong} L(\beta), \text{ for each } \beta$$

Thus, there are $[E:F] = [E:F(\alpha)][F(\alpha):F]$ isomorphisms $E \xrightarrow{\cong} K$ which extend the map θ . \square

Counting isomorphisms for separable extensions.../2

Corollary 31.6

Suppose that E is a splitting field for $f(x) \in F[x]$ and that $E:F$ is a separable extension. Then $|\mathcal{Gal}(E:F)| = [E:F]$.

Proof An element of $\mathcal{Gal}(E:F)$ is an isomorphism $\theta: E \longrightarrow E$ such that $\theta(f) = f$, for all $f \in F$.

Every such map is an extension of the identity map $\text{id}_F: F \longrightarrow F$.

$$\implies \text{the Corollary is the special case of Theorem 31.5 given by taking } L = F, K = E \text{ and } \theta = \text{id}_F \quad \square$$

Definition 31.7

A **Galois extension** is an extension $E:F$ which is finite, separable and normal.

- Corollary 31.6 can be rephrased as saying that if $E:F$ is Galois then $|\mathcal{Gal}(E:F)| = [E:F]$.
- In characteristic zero, an extension $E:F$ is Galois if and only if E is the splitting field by Theorem 30.6 and Proposition 31.4.