Lecture 11.1

Last time:

- For a field extension K/F, there is a correspondence

$$\left\{\begin{array}{l}\text{subfields} \\ F \subseteq E \subseteq K\end{array}\right\} \rightleftarrows \left\{\begin{array}{l}\text{subgroups} \\ H \subseteq \mathrm{Aut}(K/F)\end{array}\right\}$$

$$E \longmapsto \mathrm{Aut}(K/E)$$

$$K^H \longmapsfrom H$$

- This is not always a bijection, but in some cases it is, e.g. $K = \mathbb{Q}(\zeta_5)$.

Splitting Fields

Ex 1 Let $K = \mathbb{Q}(\zeta)$ where $\zeta = \zeta_3 = e^{2\pi i/3}$.

We know $x^3-1 = (x-1)(x^2+x+1)$ and x^2+x+1

is the minimal polynomial of y over $\mathbb{Q}$.

This means x^2+x+1 factors over K, and so does x^3-1:

$$x^3-1 = (x-1)(x-y)(x-y^2) \in K[x].$$

On the other hand, x^6-1 does not split into linear factors over K:

$$x^6-1 = (x^3-1)(x^3+1)$$

$$= (x-1)(x-y)(x-y^2)(x+1)\underbrace{(x^2-x+1)}_{\text{irreducible over } K}.$$

Def Let F be a field and $f(x) \in F[x]$.

A **splitting field** for f is any field extension K/F such that f splits into linear factors in $K[x]$, but f does not split in any proper

subfield $F \subseteq E \subsetneq K$.

Ex ② For any $f(x) = ax^2 + bx + c \in \mathbb{Q}[x]$, the extension $K = \mathbb{Q}(\sqrt{b^2-4ac})$ is a splitting field for f. Notice that when b^2-4ac is a square in $\mathbb{Q}$, $K = \mathbb{Q}$ and f has two rational roots.

③ $\mathbb{C}$ is a splitting field for $x^2+1 \in \mathbb{R}[x]$, but not for $x^2+1 \in \mathbb{Q}[x]$ since x^2+1 splits in the proper subfield $\mathbb{Q}(i) \subsetneq \mathbb{C}$.

By ②, $\mathbb{Q}(i)$ is a splitting field for x^2+1 over $\mathbb{Q}$.

Theorem Let $f(x) \in F[x]$, with $\deg f = n$.

(1) A splitting field exists for f and it is

unique up to F-isomorphism.

(2) If K_f is a splitting field for f over F, then $[K_f : F] \leq n!$.

Pf: (1) If $F \subseteq \mathbb{C}$ then we can take

$$K_f = F(\alpha_1, \ldots, \alpha_n)$$

where $\alpha_1, \ldots, \alpha_n \in \mathbb{C}$ are the complex roots of f, which exist by the fundamental theorem of algebra.

In general, we can prove this for any F by induction on n, with $n = 1$ easy: $K_f = F$.

Suppose a splitting field exists for every polynomial of degree $\leq n-1$.

If $f(x) = (x - \alpha)h(x)$ then h has a splitting

field by induction, and f has the same splitting field.

Otherwise, write $f(x) = g(x)h(x)$ with g irreducible (it could be that $h(x) = 1$).

Consider the field extension

$$K = F[x]/(g) \geq F.$$

We know $\alpha = x + (g)$ is a root of g in K, so f can be written as

$$f(x) = (x - \alpha)j(x) \in K[x],$$

reducing to the previous case.

Notice that once we have a splitting field Kf/F for f, it must necessarily be

$$Kf = F(\alpha_1, \ldots, \alpha_n)$$

where $\alpha_1, \ldots, \alpha_n$ are the roots of f in K_f.

This proves uniqueness.

(2) Induct again:

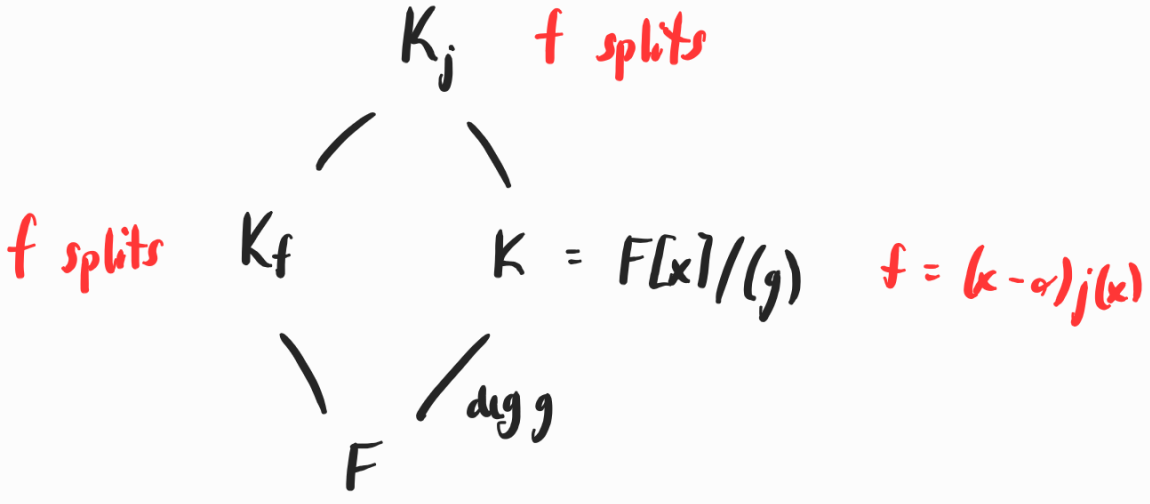
- $n = 1 \Rightarrow f(x) = x - \alpha$ for $\alpha \in F$

  $\Rightarrow K_f = F$

- $n = 2 \Rightarrow K_f = F(\sqrt{d})$ for some $d \in F$

  $\Rightarrow [K_f : F] \leq 2 = 2!$

- if $f(x) = g(x)h(x)$ with g irreducible over F, then by the above,



and by induction, $[K_j : K] \leq (n-1)!$.

By the tower law,

$$[K_f : F] \leq [K_j : F]$$

$$= [K_j : K][K : F]$$

$$\leq (n-1)! \deg g$$

$$\leq (n-1)! \deg f = n! \quad \square$$

Ex (4) Different polynomials may have the same splitting, e.g.

- $f(x) = x^3 - 1$ and $g(x) = x^2 + x + 1$ both have $K = \mathbb{Q}(\zeta_3)$ as their splitting field over $\mathbb{Q}$.

- (same degree) $f(x) = (x^2-3)(x^2-x+1)$ and

$g(x) = (x+1)(x^2-2x-2)$ both have

$K = \mathbb{Q}(\sqrt{3}, i)$ as their splitting field over $\mathbb{Q}$.

- (same degree and irreducible) $f(x) = x^2 - 3$ and $g(x) = x^2 - 2x - 2$ have splitting field $K = \mathbb{Q}(\sqrt{3})$.

Exercise 1: Verify these statements.

Def An extension K/F is normal if K is a splitting field for every minimal polynomial $p_\alpha(x) \in F[x]$ of $\alpha \in K$.

Ex ⑤ Every quadratic extension $F(\sqrt{d})/F$ is normal. (Why?)

⑥ $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is not normal since $\sqrt[3]{2}$ has

minimal polynomial $x^3 - 2$ over $\mathbb{Q}$, which does not split completely in $\mathbb{Q}(\sqrt[3]{2})$.

Theorem For a finite extension K/F, the following are equivalent:

(1) K/F is normal.

(2) Every irreducible polynomial $f(x) \in F[x]$ that has a root in K splits completely over K.

(3) $K = K_f$ for some $f(x) \in F[x]$.

Pf: (1) $\Rightarrow$ (2) If $f(x) \in F[x]$, we may divide out by the leading coefficient to make it monic.

By previous work, f is the minimal polynomial

By previous theory, α is the minimal polynomial

for some $\alpha \in K$, so it splits by (1).

(2) $\Rightarrow$ (3) Since K/F is finite, it is of the

form $K = F(\alpha_1, \ldots, \alpha_n)$ for some $\alpha_j \in K$.

Let $f(x) = p_{\alpha_1}(x) \cdots p_{\alpha_n}(x) \in F[x]$.

Since each p_{α_j} has a root in K, namely α_j,

they all split completely and therefore so

does f.

If f split in a smaller extension, so would

each of the p_{α_j}, but by definition

$F(\alpha_1, \ldots, \alpha_n)$ is the smallest extension containing

the α_j. So this must be a splitting field

for F.

(3) $\Rightarrow$ (1) Suppose $K = K_0$

(3) $\Rightarrow$ (1) Suppose $K = K_f$ and let $\alpha \in K$ with minimal polynomial $p_\alpha(x) \in F[x]$.

Let $g(x) = p_\alpha(x) f(x)$, which has splitting field K_g/F, with $K \subseteq K_g$ by definition.

We claim $K = K_g$, which will imply that $K = K_{p_\alpha}$ and thus K/F is normal.

Since p_α splits in K_g, it has all of its roots in K_g, including α.

Let α' be any other root of p_α in K_g.

Then $p_\alpha = p_{\alpha'}$ since minimal polynomials are unique, so $F(\alpha) \cong F(\alpha')$.

By the tower law,

$$[K(\alpha) : K][K : F] = [K(\alpha) : F] = [K(\alpha) : F(\alpha)][F(\alpha) : F]$$

and

$$[K(\alpha'):K][K:F] = [K(\alpha'):F] = [K(\alpha'):F(\alpha')][F(\alpha'):F].$$

Also, $K(\alpha) = F(\alpha)_g \cong F(\alpha')_g = K(\alpha')$ over F,

so $[K(\alpha):F] = [K(\alpha'):F]$, which then implies

$$[K(\alpha):K] = [K(\alpha'):K].$$

But we chose $\alpha \in K$, so $K(\alpha) = K$ and

therefore $K(\alpha') = K$ as well, showing $\alpha' \in K$.

Repeat with the other roots. □

Ex (7) For any $n \geq 2$, $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is a splitting field for the minimal polynomial $\Phi_n(x)$ of ζ_n and is therefore a normal extension. Without knowing $\Phi_n(x)$ — see

HW 7 — it's still easy to conclude that $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is normal: it's a splitting field for $x^n - 1$.

For $n = p > 3$ a prime, we know

$$[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p - 1 < (p-1)!$$

which is an example where the inequality $[K_f : F] \leq (\deg f)!$ is strict.

Next time: Galois extensions.