Lecture 11.2

Last time:

- A **splitting field** for $f \in F[x]$ is an extension K/F such that f splits into linear factors in $K[x]$ but not in $E[x]$ for $E \subsetneq K$.

- A **normal extension** is an extension K/F which is a splitting field for the minimal polynomial $p_\alpha(x) \in F[x]$ of any $\alpha \in K \setminus F$.

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 <u>some</u> $f(x) \in F[x]$.

<u>Pf</u>: (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 for some $\alpha \in K$, so it splits by (1).

(2) $\Rightarrow$ (3) Since K/F is finite, it is of the form $K = F(\alpha_1, \dots, \alpha_n)$ 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 $K = K_f$ 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. $\square$

Ex ① 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

$[K_f : F] \le (\deg f)!$ is strict.

$\boxed{\text{Def}}$ A polynomial $f \in F[x]$ is **separable** if, in its splitting field, it has <u>distinct</u> roots:

$$f(x) = c(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)$$

where $\alpha_j \neq \alpha_k$ for any $j \neq k$.

$\boxed{\text{Ex}}$ ② $x^2+1 = (x-i)(x+i)$ is separable over $\mathbb{Q}$.

③ $(x-1)^2$ is inseparable over $\mathbb{Q}$ but its irreducible factors $x-1$ and $x-1$ are separable.

④ $x^4+x^3+x^2+x+1$ is separable over $\mathbb{Q}$ because its complex roots are $\zeta = \zeta_5, \zeta^2, \zeta^3$ and ζ^4.

⑤ Let t be an indeterminate and consider the field $\mathbb{F}_p(t) = \left\{ \frac{f(t)}{g(t)} : f, g \in \mathbb{F}_p[t], g \neq 0 \right\}$

of rational functions in t. An example of an inseparable polynomial in $\mathbb{F}_p(t)[x]$ is $x^p - t$, which is irreducible over $\mathbb{F}_p(t)$ but factors as

$$x^p - t = (x - t^{1/p})^p$$

over the field extension $\mathbb{F}_p(t^{1/p})$.

Remark: This is basically the only way to get an inseparable irreducible polynomial, so we won't worry much about it.

$\boxed{\text{Prop}}$ A polynomial $f \in F[x]$ is separable if and only if it shares no common factors with its formal derivative f'.

if $f(x) = a_0 + a_1 x + \dots + a_n x^n$

then $f'(x) = a_1 + 2a_2 x + \dots + n a_n x^{n-1}$

Pf: If f has a multiple root, it can be written as

$$f(x) = (x-\alpha)^2 g(x)$$

for some $g \in K_f[x]$. Then

$$f'(x) = 2(x-\alpha)g(x) + (x-\alpha)^2 g'(x)$$

so $x-\alpha$ is a common factor of f and f'.

Conversely, if f and f' share a common factor, it can be assumed to be a linear factor $x-\alpha$ over K_f.

Write $f(x) = (x-\alpha)g(x)$ for some $g \in K_f[x]$

so that $f'(x) = g(x) + (x-\alpha)g'(x)$.

Then $0 = f'(\alpha) = g(\alpha)$, so $g(x) = (x-\alpha)h(x)$

$x-\alpha$ is a factor of $f'(x)$

for some $h \in K_f[x]$, showing f is inseparable:

$$f(x) = (x-\alpha)g(x) = (x-\alpha)^2 h(x). \quad \square$$

$\boxed{\text{Theorem}}$ For $F \subseteq \mathbb{C}$ or F a finite extension of $\mathbb{F}_p$, every irreducible polynomial $f \in F[x]$ is separable.

$\boxed{\text{Def}}$ An extension K/F is **separable** if for every $\alpha \in K$, the minimal polynomial $p_\alpha(x)$ is separable.

$\boxed{\text{Def}}$ An extension K/F is **Galois** if it is finite, separable and normal.

That is,

- $[K:F] < \infty$,
- $p_\alpha(x)$ is separable for all $\alpha \in K$,
- $K = K_{p_\alpha}$ for $p_\alpha(x)$ for any $\alpha \in K \setminus F$.

Next week, we will prove:

$\boxed{\text{Theorem}}$ Let K/F be a field extension and set $G = \mathrm{Aut}(K/F)$. Then the following are equivalent:

(1) K/F is Galois.

(2) K is a splitting field for some separable polynomial $f \in F[x]$.

(3) K/F is finite and $K^G = F$.

These will turn out to be exactly the field extensions for which the subfield - subgroup correspondence is bijective.

(6) Since $f(x) = x^4 + x^3 + x^2 + x + 1$ is irreducible and separable over $\mathbb{Q}$, its splitting field $\mathbb{Q}(\zeta)$, $\zeta = e^{2\pi i/5}$, is a Galois extension of $\mathbb{Q}$.

In Lecture 10.2, we computed

$$G = \mathrm{Aut}(\mathbb{Q}(\zeta)/\mathbb{Q}) = \{\zeta \mapsto \zeta^j \mid 1 \leq j \leq 4\} \cong \mathbb{F}_5^\times$$

which is a cyclic group of order 4 generated by $\sigma : \zeta \mapsto \zeta^2$ $(\longleftrightarrow 2 \in \mathbb{F}_5^\times)$.

Since $\mathbb{Q}(\zeta)/\mathbb{Q}$ is Galois, $\mathbb{Q}(\zeta)^G = \mathbb{Q}$: indeed,

if $\alpha = a + b\zeta + c\zeta^2 + d\zeta^3 \in \mathbb{Q}(\zeta)$ is fixed

by σ, then

$$\alpha = \sigma(\alpha) = a + b\sigma(\zeta) + c\sigma(\zeta)^2 + d\sigma(\zeta)^3$$

$$= a + b\zeta^2 + c\zeta^4 + d\zeta$$

$$= (a-c) + (d-c)\zeta + (b-c)\zeta^2 - c\zeta^3$$

$\Longrightarrow$ $a = a - c \Rightarrow c = 0$

$d = -c \Rightarrow d = 0$

$b = d - c \Rightarrow b = 0.$

So $\alpha \in \mathbb{Q}$, implying $\mathbb{Q}(\zeta)^G = \mathbb{Q}$.

Consider the subgroup $H = \langle \tau : \zeta \mapsto \zeta^4 \rangle \cong \langle 4 \rangle \leq \mathbb{F}_5^\times$.

This is a subgroup of order 2 and τ clearly fixes things outside $\mathbb{Q}$, such as $\zeta + \zeta^4$, $\zeta^2 + \zeta^3$, etc.

Claim: $\mathbb{Q}(\zeta)^H = \mathbb{Q}(\zeta + \zeta^4)$.

Since $H = \langle \tau \rangle = \{id, \tau\}$ fixes $\zeta + \zeta^4$, we get

$$\mathbb{Q}(\zeta + \zeta^4) \subseteq \mathbb{Q}(\zeta)^H.$$

On the other hand, suppose $\alpha = a + b\zeta + c\zeta^2 + d\zeta^3$ is in $\mathbb{Q}(\zeta)^H$.

Then $\alpha = \tau(\alpha) = a + b\tau(\zeta) + c\tau(\zeta)^2 + d\tau(\zeta)^3$

$$= a + b\zeta^4 + c\zeta^3 + d\zeta^2$$

$$= (a-b) - b\zeta + (d-b)\zeta^2 + (c-b)\zeta^3$$

$\Rightarrow$ $a = a - b \Rightarrow b = 0$

$c = d - b \Rightarrow c = d.$

So $\alpha = a + c(\zeta^2 + \zeta^3)$ but remember that

$$\zeta + \zeta^2 + \zeta^3 + \zeta^4 = 0 \implies \zeta^2 + \zeta^3 = -(\zeta + \zeta^4).$$

This shows that $\alpha \in \mathbb{Q}(\zeta + \zeta^4)$, so this is the fixed field of H:

$$\begin{tikzcd}
\mathbb{Q}(\zeta) = \mathbb{Q}(\zeta)^{\{id\}} \arrow[d, dash, "2"'] & & \{id\} \arrow[d, dash, "2"'] \\
\mathbb{Q}(\zeta + \zeta^4) = \mathbb{Q}(\zeta)^H \arrow[d, dash, "2"'] & & H = \langle \tau \rangle = \langle \sigma^2 \rangle \arrow[d, dash, "2"'] \\
\mathbb{Q} = \mathbb{Q}(\zeta)^G & & G = \langle \tau \rangle
\end{tikzcd}$$

Next time: counting field homomorphisms, more Galois theory.