Lecture 32: Splitting fields and separable polynomials.

§ 13.4 – 13.5 of [DF].
§ 12–15 of [R3]

Previously:

Thm: $F \subseteq K \subseteq L$ fields. If K/F and L/K are algebraic, so is L/F.

Thm: $F \subseteq K_1, K_2 \subseteq L$ fields. Then

$$[\underbrace{K_1 K_2}_{\text{compositum}} : F] \le [K_1 : F][K_2 : F]$$

$$\begin{tikzcd}[column sep=small] & L \arrow[d, dash] & \\ & K_1K_2 \arrow[dl, dash] \arrow[dr, dash] & \\ K_1 \arrow[dr, dash] & & K_2 \arrow[dl, dash] \\ & F & \end{tikzcd}$$

Def: K/F is a __splitting field__ for $f(x) \in F[x]$ when

(a) $f(x)$ factors into linear terms in $K[x]$. ("splits completely")

(b) $f(x)$ does not split completely in any $F \subseteq L \subsetneq K$.

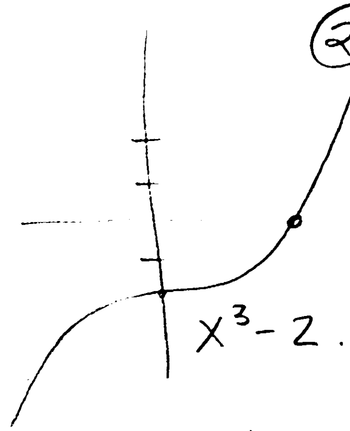
Ex: $\mathbb{Q}(\sqrt{2})$ is the splitting field for $x^2 - 2$ in $\mathbb{Q}[x]$, as $x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2})$. [Note: $\mathbb{R}$ is not a splitting field.]

Q: What is the splitting field of $x^3 - 2 \in \mathbb{Q}[x]$? (inside $\mathbb{C}$).

Note: $\mathbb{Q}(\sqrt[3]{2})$ is not big enough.

$$f(x) = x^3 - 2 = (x - \sqrt[3]{2})\underbrace{(x^2 + \sqrt[3]{2}x + (\sqrt[3]{2})^2)}_{\text{irreducible in } \mathbb{R}[x]}$$

Let $\rho = e^{2\pi i/3}$ so that $\rho^3 = 1$. Then $f(\rho \cdot \sqrt[3]{2}) = f(\rho^2 \cdot \sqrt[3]{2}) = 0$. So over $K = \mathbb{Q}(\sqrt[3]{2}, \rho)$ have



$$X^3 - 2 = (X - \sqrt[3]{2})(X - \rho \cdot \sqrt[3]{2})(X - \rho^2 \cdot \sqrt[3]{2}).$$

In fact, K is a splitting field for f: As $\mathbb{C}[X]$ is a UFD, any field $\leq \mathbb{C}$ where $X^3 - 2$ splits completely must contain $\sqrt[3]{2}$ and $\rho \cdot \sqrt[3]{2}$ and hence ρ.

<u>Thm</u>: Any $f(x) \in F[x]$ has a splitting field K/F. Moreover, if K'/F is another splitting field for f, then $\exists$ an isomorphism $\psi : K \to K'$ with $\psi|_F = id_F$.

<u>Pf</u>: Induct on $\deg f$. Let f_1 be any irreducible factor of f, and set $L := F[x]/(f_1(x)) = F(\theta_1)$ where $\theta_1 = x + (f_1(x))$. Now $f(\theta_1) = 0$, so $f(x) = (x - \theta_1) f_2(x)$ in $L[x]$. By induction, $\exists K/L$ where f_2 splits completely as

$(x-\theta_2)(x-\theta_3)\cdots(x-\theta_n)$

Then $K = F(\theta_1, \ldots, \theta_n)$ is a splitting field for f.

[Again, no smaller field works as $K[x]$ is a UFD.]

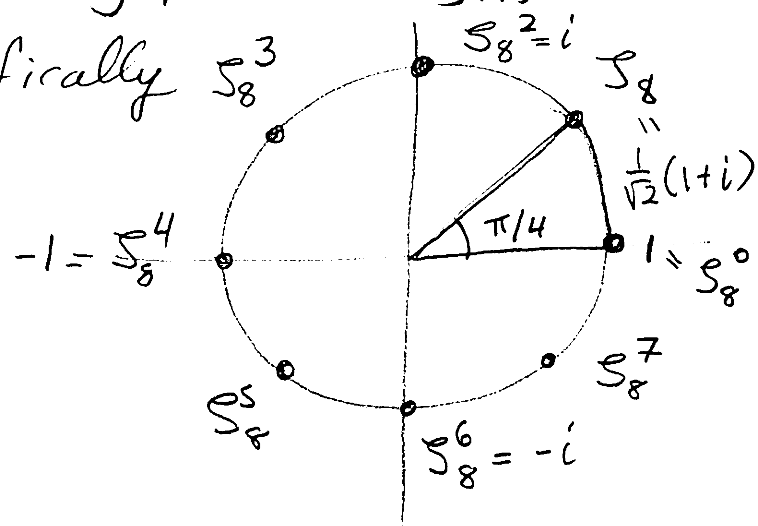
For uniqueness, see §13.4, Thm 27 of [DF].

Think $F(\alpha) \cong F[x]/(m_{\alpha,F}(x))$. ▨

<u>Cor</u>: If K is a splitting field for $f \in F[x]$, then $[K:F] \leq (\deg f)!$

For a random $f \in \mathbb{Z}[x]$, $[K:\mathbb{Q}] = (\deg f)!$ with prob $\to 1$. [Now, here's the opposite behavior.]

<u>Ex</u>: $x^n - 1$ in $\mathbb{Q}[x]$ has splitting field $\mathbb{Q}(\zeta_n) \subseteq \mathbb{C}$ where $\zeta_n := e^{2\pi i/n}$. Specifically



$1, \zeta_n, \zeta_n^2, \ldots, \zeta_n^{n-1}$

are <u>distinct</u> roots of $x^n - 1$,

so $x^n - 1 = \prod_{k=1}^{n-1} (x - \zeta_n^k)$

Thus $\mathbb{Q}(\zeta_n)$ is the splitting field and

$[\mathbb{Q}(\zeta_n):\mathbb{Q}] \leq n-1$. [Will calculate later.]

These cyclotomic fields are central examples in number theory. In the 19th century, F.L.T was "proved" using the (false) "fact" that $\mathbb{Z}[\zeta_n]$ is a UFD. (Actually, $\mathbb{Z}[\zeta_{23}]$ is not a UFD). Lead to introduction of ideals to try to enlarge $\mathbb{Z}[\zeta_n]$ to a UFD (compare $\mathbb{Z}[\sqrt{-3}]$ vs. $\mathbb{Z}[\frac{1}{2}(1+\sqrt{-3})]$).

$f(x) \in F[x]$ monic. Over the splitting field of f, have $f(x) = (x-\alpha_1)^{k_1}(x-\alpha_2)^{k_2} \cdots (x-\alpha_n)^{k_n}$ with α_i distinct. (k_i are the multiplicities)

When $k_i = 1$, α_i is called simple; otherwise α_i is a multiple root.

Def: $f(x)$ is separable when all roots are simple.

Ex: x^2-1, x^2+1 in $\mathbb{Q}[x]$.

Non-Ex:

(1) $x^2+2x+1 = (x+1)^2$ in $\mathbb{Q}[x]$.

(2) $x^2+t \in \underbrace{\mathbb{F}_2(t)}_{\text{field of rat'l fns}}[x]$

(a) Irreducible by Eisenstein with ideal (t).

(b) Let α be a root in the splitting field, so $\alpha^2 = t$. Then $(x-\alpha)^2 = x^2 - 2\alpha x + t$

$$= x^2 + t$$

So α is a mult. root.

Thm: If F has char $= 0$ or F is finite, then every irreducible $f \in F[x]$ is separable.

Pf: §13.5 of [DF].

The broader class of perfect field also has this property (see §13.5 of [DF]).