Midterm: Wed. Feb. 8th 7:00 pm - 9:00 pm (room TBD)

---

§13.4: Splitting Fields & Algebraic Closure

Def: K/F field ext'n. The poly. $f(x) \in F[x]$ splits over K if $f(x)$ factors into linear factors in $K[x]$

K is called a <u>splitting field</u> for f if f splits over K, but not over any proper subfield of K.

Thm 25/ Cor 28: A splitting field for f always exists and is unique up to isomorphism.

Pf: Assume f irreducible. Otherwise, treat each irred. factor in turn.

Existance: Induction on $n := \deg f$. If $n = 1$, splitting field is F.

If $n > 1$, let α be a root of (some irred factor of) f. Then $[F(\alpha):F] \leq n$ and in $F(\alpha)$, $f(x) = (x-\alpha) f_1(x)$ for some $f_1 \in F(\alpha)[x]$. f_1 has degree $\leq n-1$, so by inductive hypothesis, $\exists$ ext'n E of $F(\alpha)$ containing all roots of f_1, and F splits $/ E$. The splitting field K of f is the intersection of all subfields of E in which f splits.

(Cor. of this: $[K:F] \leq n!$)

Uniqueness: Use Thm 8: Let $\varphi: F \to F'$ be an isom. of fields, and extend to the map $F[x] \to F'[x]$ by sending $x \mapsto x$. Let $p(x) \in F[x]$ be irred, and let $p'(x) = \varphi(p(x)) \in F'[x]$. Then if α is any root of p and β is any root of p', $\exists$ isom. $\sigma: F(\alpha) \longrightarrow F'(\beta)$ where $\sigma(a) = \varphi(a)$, $a \in F$ and $\sigma(\alpha) = \beta$

$$\begin{tikzcd} \sigma: F(\alpha) \arrow[r, "\sim"] & F'(\beta) \\ \varphi: F \arrow[u, no head] \arrow[r, "\sim"] & F' \arrow[u, no head] \end{tikzcd}$$

Pf: Both $F(\alpha), F'(\beta)$ isom to $F[x]/(p)$

Back to the pf: We'll prove the more general result (Thm 27): Let $\varphi: F \xrightarrow{\sim} F'$ be an isom of fields. Let $f \in F[x]$, and $f' = \varphi(f) \in F'[x]$. If E is a splitting field for f and E' is a splitting field for f', then φ extends to an isom $\sigma: E \xrightarrow{\sim} E'$.

$$\begin{tikzcd} \sigma: E \arrow[r, "\sim"] & E' \\ \varphi: F \arrow[u, no head] \arrow[r, "\sim"] & F' \arrow[u, no head] \end{tikzcd}$$

Pf: Induction on n. Assume result holds for any poly. of degree $< n$ over <u>any</u> field and for any field isom.

Idea: adjoint roots of f and f' to F and F' to reduce to a smaller ext'n

$$\begin{tikzcd}
\sigma : E \arrow[r, "\sim"] \arrow[d, dash] & E' \arrow[d, dash] \\
\sigma' : F(\alpha) \arrow[r, "\sim"] \arrow[d, dash] & F'(\beta) \arrow[d, dash] \\
\varphi : F \arrow[r, "\sim"] & F'
\end{tikzcd}$$

If all roots of f are in F, then $E = F \cong F' = E'$.
So assume that f has an irred. factor $p(x)$ of deg ≥ 2, and let $p' = \varphi(p)$. Let α be a root of p in E and β be a root of p' in E'. Over $F(\alpha)$, $f(x) = (x-\alpha) f_1(x)$, while over $F'(\beta)$, $f'(x) = (x-\beta) f_1'(x)$.
By Thm 8, $\exists$ isom. $\sigma' : F(\alpha) \xrightarrow{\sim} F'(\beta)$ extending φ; can check that σ' maps coeffs of f_1 to coeffs of f_1'.
Therefore, by inductive hypothesis, have map $\sigma : E \to E'$ extending σ', and therefore φ.

Examples: 1) $f(x) = x^2 - 2$, $F = \mathbb{Q}$

roots are $\pm\sqrt{2}$, so splitting field $= \mathbb{Q}(\sqrt{2})$

$$\begin{tikzcd} \mathbb{Q}(\sqrt{2}) \arrow[d, dash, "2"] \\ \mathbb{Q} \end{tikzcd}$$

2) $f(x) = (x^2-2)(x^2-3)$, $F = \mathbb{Q}$

roots are $\pm\sqrt{2}$, $\pm\sqrt{3}$, so s.f. $= \mathbb{Q}(\sqrt{2}, \sqrt{3})$

$$\begin{tikzcd} & \mathbb{Q}(\sqrt{2}, \sqrt{3}) \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\ \mathbb{Q}(\sqrt{2}) \arrow[dr, dash] & \mathbb{Q}(\sqrt{6}) \arrow[d, dash] & \mathbb{Q}(\sqrt{3}) \arrow[dl, dash] \\ & \mathbb{Q} & \end{tikzcd}$$

(like 12.2 Prob 7)

3) $p(x) = x^3 - 2, \quad F = \mathbb{Q}$

roots: $\underbrace{\sqrt[3]{2}}_{\theta_1}, \underbrace{\omega\sqrt[3]{2}}_{\theta_2}, \underbrace{\omega^2\sqrt[3]{2}}_{\theta_3}$ where $\omega = \dfrac{-1+\sqrt{-3}}{2}$

$K = \mathbb{Q}(\theta_1, \theta_2, \theta_3)$: splitting field of f

$\omega = \dfrac{\theta_2}{\theta_1} \in K$, so $\sqrt{-3} \in K$

$\sqrt{-3}$ is deg 2 over $\mathbb{Q}$

θ_1 is deg 3 over $\mathbb{Q}$

So $[K:\mathbb{Q}] \geq [\mathbb{Q}(\theta_1,\omega):\mathbb{Q}] \geq 6$, but also $[K:\mathbb{Q}] \leq 3! = 6$

$$\begin{tikzcd}
 & & K = \mathbb{Q}(\sqrt[3]{2}, \sqrt{-3}) \arrow[dll, dash] \arrow[d, dash] \arrow[dr, dash] \arrow[drr, dash] & & \\
\mathbb{Q}(\sqrt{-3}) \arrow[dr, dash] & & \mathbb{Q}(\theta_1) \arrow[dl, dash] & \mathbb{Q}(\theta_2) \arrow[dll, dash] & \mathbb{Q}(\theta_3) \arrow[dlll, dash] \\
 & \mathbb{Q} & & &
\end{tikzcd}$$

Cyclotomic Fields

$x^n - 1$ has roots $\underbrace{e^{2\pi i/n}}_{\text{form a cyclic gp. } \mu_n} \in \mathbb{C}$, $0 \leq i < n$

Def: A primitive nth root of unity is a generator of μ_n i.e. elt. of μ_n but not an elt of any μ_d, $d < n$.

ζ_n: primitive nth root of 1

other primitive nth roots of 1: ζ_n^a, $\gcd(n,a) = 1$

Def: The field $\mathbb{Q}(\zeta_n)$ is called the cyclotomic field of nth roots of unity.

If p: prime,

$$x^p - 1 = (x-1)\underbrace{(x^{p-1} + \cdots + x + 1)}_{\text{irred.}}$$

$\Phi_p := x^{p-1} + \cdots + x + 1$ is min'l poly for ζ_p over $\mathbb{Q}$, so

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

Algebraic closure

Def: F: field. An alg. ext. $\overline{F}/F$ is an alg. closure of F if every poly. $f \in F[x]$ splits over $\overline{F}$.

This always exists (Prop. 30), and is unique (Prop. 31)

Def: A field F is alg. closed if $\overline{F} = F$.

Prop 29: An alg. closure is alg. closed