13.4 Splitting fields.

Recall. $x^3 - 2$ has a root in $\mathbb{Q}(\sqrt[3]{2})$ but does not split into linear factors. (other roots are complex).
$\cong \mathbb{Q}[x]/(x^3-2)$

Definition. $f(x) \in F[x]$ *splits* over an extension K of F if $f(x)$ is a product of linear factors in $K[x]$.

The *splitting field of $f(x)$* $\in F[x]$ is the unique (up to isomorphism) extension K/F such that

(1) f splits over K and
(2) if $F \subseteq L \subseteq K$ and f splits over L, then $L = K$.

(Uniqueness will be proved below)

Theorem. *Every $f(x) \in F[x]$ has some splitting field K/F.*

Proof. Induct on $\deg f =: n$.
If $f(x)$ splits over F, then $K = F$.
Let $p(x) \in F[x]$ be irreducible with $p(x) \mid f(x)$ and $\deg p(x) > 1$.
In $E := F[x]/(p(x))$, $p(x)$ has a root α.
In $E[x]$

$$f(x) = (x - \alpha)\, g(x)$$

By the induction assumption $g(x)$ splits over some L/E.
Hence L contains all roots of $f(x)$.

$$K := \bigcap \{ F \leq L' \leq L \mid L' \text{ contains all roots of } f(x) \}$$

is the splitting field of $f(x)$ over F. □

Corollary. *A splitting field K of $f(x) \in F[x]$ with $\deg f = n$ has degree $[K : F] \leq n!$*

Proof. In the proof above $[E:F] \leq n$. By induction $[L:E] \leq (n-1)!$ □

Note. A field isomorphism $\varphi\colon F \to F'$ induces a ring isomorphism

$$\varphi\colon F[x] \to F'[x],\ \sum a_i x^i \mapsto \sum \varphi(a_i) x^i.$$

Uniqueness of splitting fields follows from the next theorem for $F = F', \varphi = \mathrm{id}_F$.

Theorem. *Let $\varphi\colon F \to F'$ be a field isomorphism, let E be a splitting field for $f \in F[x]$, let E' be a splitting field for $\varphi(f) \in F'[x]$.*

Then there exists an isomorphism $\bar\varphi\colon E \to E'$ with $\bar\varphi|_F = \varphi$.

$$\begin{tikzcd} E \arrow[r, "\bar\varphi"] & E' \\ F \arrow[u, hook] \arrow[r, "\varphi"] & F' \arrow[u, hook] \end{tikzcd}$$

Proof. Induction on $\deg f$.

If f splits over F, then $F = E$, $F' = E'$, $\bar\varphi = \varphi$.

Let $p(x) \in F[x]$ be an irreducible factor of $f(x)$, $\deg p > 1$.

Let $\alpha \in E$, $\beta \in E'$ such that $p(\alpha) = 0$, $\varphi(p)(\beta) = 0$.

Then $\psi\colon F(\alpha) \to F'(\beta)$ with $\psi(\alpha) = \beta$, $\psi|_F = \varphi$

$g(\alpha) \mapsto \varphi(g)(\beta)$

is a field iso.

Since E is a splitting field of $f(x)$ over F, E is a splitting field of $f_1(x) := f(x)/(x-\alpha)$ over $F(\alpha)$.

By induction assumption on $f_1(x)$ over $F(\alpha)$ and $\psi\colon F(\alpha) \to F'(\beta)$ we obtain $\bar\psi = \bar\varphi\colon E \to E'$. $\square$

Example. The splitting field K of $x^3 - 2$ over $\mathbb{Q}$ contains

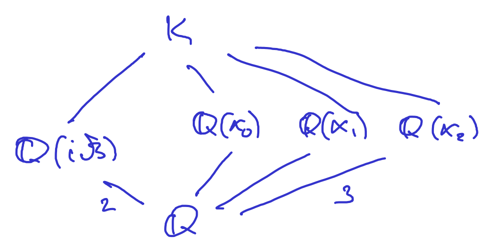
$\alpha_0 = \sqrt[3]{2}$ $\quad \alpha_1 = \sqrt[3]{2}\,\underbrace{e^{\frac{2\pi i}{3}}}_{\frac{-1+i\sqrt{3}}{2}}$ $\quad \alpha_2 = \sqrt[3]{2}\,\underbrace{e^{\frac{4\pi i}{3}}}_{\frac{-1-i\sqrt{3}}{2}}$

$\alpha_0, \alpha_1, \alpha_2 \in K \Rightarrow i\sqrt{3} = \dfrac{\alpha_1 - \alpha_2}{\alpha_0} \in K$

So $K = \mathbb{Q}(\alpha_0, \alpha_1, \alpha_2) = \mathbb{Q}(\sqrt[3]{2}, i\sqrt{3})$

$[K : \mathbb{Q}(\sqrt[3]{2})] \leq 2$ because $i\sqrt{3}$ is a root of $x^2 + 3$.

$[K : \mathbb{Q}] = 6$



Splitting field of $x^n - 1$ over $\mathbb{Q}$: cyclotomic fields.

$$x^n - 1 = \prod_{k=0}^{n-1}(x - e^{k\frac{2\pi i}{n}}) \in \mathbb{C}[x]$$

has splitting field $\mathbb{Q}(1, e^{\frac{2\pi i}{n}}, \ldots, e^{(n-1)\frac{2\pi i}{n}}) = \mathbb{Q}(e^{\frac{2\pi i}{n}})$, the *cyclotomic field of the n-th roots of unity.*

Question. What is $[\mathbb{Q}(e^{\frac{2\pi i}{n}}) \colon \mathbb{Q}]$?

Example. For $n=4$, the 4th roots of unity

$1, i, -1, -i$

$[\mathbb{Q}(i) : \mathbb{Q}] = 2 < 4$

In general $x^n - 1 = (x-1)(x^{n-1} + \cdots + x + 1)$ yields

$[\mathbb{Q}(e^{2\pi i/n}) : \mathbb{Q}] \leq n-1$ ..

Outlook: $= \phi(n)$ Euler's ϕ-function

Algebraic closure.

Definition. A field F is *algebraically closed* if every $f \in F[x]$ splits over F.

Fundamental Theorem of Algebra. $\mathbb{C}$ is algebraically closed.

Proof later using Galois theory.

Lemma. *F is algebraically closed iff every nonconstant $f \in F[x]$ has a root in F.*

Proof. $\Leftarrow$ Assume $f \in F[x]$ has a root $\alpha \in F$.

$f(x) = (x - \alpha)\, f_1(x)$ for $f_1(x) \in F[x]$

$f_1(x) = (x - \alpha_1)\, f_2(x)$

$\vdots$

$\square$

Definition. $\bar{F}$ is an *algebraic closure* of F if $\bar{F}/F$ is algebraic and every $f(x) \in F[x]$ splits over $\bar{F}$.

Proposition. Any algebraic closure $\bar{F}$ of F is algebraically closed.

Proof. Let $f \in \bar{F}[x]$ with root α. Show $\alpha \in \bar{F}$.

Then $\bar{F}(\alpha)/\bar{F}$ is algebraic. By previous Thm "algebraic/algebraic = algebraic", we have $\bar{F}(\alpha)/F$ is algebraic.

Hence α is a root of some $p(x) \in F[x]$ and $\alpha \in \bar{F}$. $\square$

Theorem. *Any field F is contained in an algebraically closed field K.*

Proof. Artin: For any $f(x) \in F[x]$ nonconstant, add a root to F.

Let x_f be a variable.

$Z := \{ x_f \mid f \in F[x], \deg f \geq 1 \}$ infinite

In $F[Z]$ consider the ideal I generated by

$\{ f(x_f) \mid f \in F[x], \deg f \geq 1 \}$ $\qquad f(x_f) = 0 \mod I$

Suppose $I = F[Z]$. Then $1 \in I$ and

$1 = g_1 f_1(x_{f_1}) + \dots + g_n f_n(x_{f_n})$

for some $g_i, f_i \in F[Z]$.

Let α_i be a root of f_i. Plug in α_i for x_{f_i} above.

$1 = 0$ $\lightning$

By Zorn's Lemma I is contained in a max ideal M of $F[Z]$.

Then

$K_1 := F[Z]/M$

is a field in which every $f \in F[x]$ has a root $x_f + M$.

Repeat

$F \subseteq K_1 \subseteq K_2 \subseteq \dots$

Let $K := \bigcup_{i \in \mathbb{N}} K_i$. Then K is alg closed. □

Theorem. *Every field F has an algebraic closure $\bar{F}$, and this is unique (up to isomorphism).*

Proof. Existence: $F \leq K$ for K alg closed by previous Thm.

$\bar{F} := \{ \alpha \in K \mid \alpha \text{ is algebraic over } F \}$ is an alg closure of F.

Uniqueness: similar to the proof for splitting fields using Zorn's Lemma. □

Bernard Banaschewski

Algebraic closure without Choice

- Existence is provable for $\mathbb{Q}$ and finite fields without AC.
- Uniqueness requires AC.
  (Uncountable algebraic closure of $\mathbb{Q}$ is consistent with ZF.)