# Apr 26: Splitting fields

Last 2 lectures: diversion to ruler & compass constructions

Today: Splitting fields

- definition
- properties (uniqueness!)

## §1. Definitions

Let $K \subset L$ be a field extension

We say a polynomial $f \in K[x]$ **splits over L** if $f(x)$ factors as

$$f(x) = a_n(x-\alpha_1)\cdots(x-\alpha_n)$$

where $\alpha_i \in L$

Ex: . $f(x) = x^2 - 1 \in \mathbb{Q}[x]$ splits over $\mathbb{Q}$
$= (x-1)(x+1)$

. $f(x) = x^2+1 \in \mathbb{R}[x]$
does not split / $\mathbb{R}$
does split / $\mathbb{C}$ $\quad x^2+1 = (x+i)(x-i)$

**Fund thm of algebra**
Every polynomial $f \in \mathbb{C}[x]$ splits over $\mathbb{C}$. ($\mathbb{C}$ is alg. closed)

**Defn** $K$ is alg. closed if every polynomial $f \in K[x]$ splits.

**Defn** Let $K \subset L$ be a field ext
Let $f(x) \in K[x]$
We say $L$ is **splitting field for $f(x)$** if

1. $f(x)$ splits over $L$
   i.e. $f(x) = a_n(x-\alpha_1)\cdots(x-\alpha_n)$
2. $L = K(\alpha_1, \ldots, \alpha_n)$

Ques: Does it exist?
Is it unique?

Explicitly for $f(x) \in \mathbb{Q}[x]$
Then splitting field for $f(x)$ is the smallest subfield $L \subset \mathbb{C}$ s.t. $L$ contains all roots.

- This requires fund thm of algebra
- Uses a fixed ext. $\mathbb{Q} \subset \mathbb{C}$

ex: $\mathbb{C} = \mathbb{R}(i) = \{a+ib \mid a,b \in \mathbb{R}\}$
$= \mathbb{R}[x]/(x^2+1)$

$\mathbb{C} = \mathbb{R}(-i)$

## Examples

① $x^2+1 \in \mathbb{R}[x] \rightsquigarrow$ splitting field is $\mathbb{C}$

($x^2+1 \in \mathbb{Q}[x] \rightsquigarrow$ splitting field $\mathbb{Q}(i)$)

② $x^3-1 \in \mathbb{Q}[x] \rightsquigarrow$ roots $= 1, \frac{-1\pm\sqrt{-3}}{2}$

$\quad\;\, \shortparallel$

$(x-1)(x^2+x+1)$

splitting field $K = \mathbb{Q}\left(1, \frac{-1+\sqrt{-3}}{2}, \frac{-1-\sqrt{-3}}{2}\right)$

$= \mathbb{Q}(\sqrt{-3})$

③ $x^4-5x^2+6 \in \mathbb{Q}[x]$

$= (x^2-3)(x^2-2)$

Splitting field $\mathbb{Q}(\pm\sqrt{3}, \pm\sqrt{2})$

$= \mathbb{Q}(\sqrt{3}, \sqrt{2})$

$f(x)$ irred

④ $f(x) = x^3-2 \in \mathbb{Q}[x]$

roots $\sqrt[3]{2}, \sqrt[3]{2}\rho, \sqrt[3]{2}\rho^2$

prim $3^{rd}$ root

$\rho = e^{2\pi i/3} = \frac{1}{2} + \frac{\sqrt{3}}{2}i$

$K = \mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}\rho, \sqrt[3]{2}\rho^2)$

$= \mathbb{Q}(\sqrt[3]{2}, \sqrt{-3})$

$\sqrt{-3} = \sqrt{3}i$

Rmk: For $x^2-2$, just ~~to~~ need to adjoin one root $\sqrt{2}$, then get other $-\sqrt{2}$.

But here just adjoining one root $\sqrt[3]{2}$ ~~one~~ is not enough.

$\mathbb{Q} \longrightarrow \mathbb{Q}[x]/(f(x)) = K$ field

**Thm** (Existence) Let $K$ be a field. Let $f(x) \in K[x]$ poly of deg $n$. Then $\exists$ splitting field $K < L$ for $f(x)$. Moreover $|L:K| \le n!$

**Proof** Construct $L$ inductively

Write $f(x) = f_1(x) \cdots f_s(x)$ where each $f_i(x)$ is irred

Suffices to assume $f(x)$ irred.

$$\big( K < L_1 < L_2 < \cdots \quad L_s = L \big)$$

$L_1$: splitting field for $f_1$; $L_2$: splitting for $f_2 \in L_1[x]$ irred

Therefore, can construct

$$K < F_1 = K[x]/(f)$$

Let $K[x] \twoheadrightarrow K[x]/(f) = F_1$

$$x \longmapsto \alpha_1 = \bar{x}$$

$|F_1 : K| \le n$

$\big( |F_2 : F_1| \le n-1$ & tower law to get $|L:K| \le n! \big)$

So $\alpha_1$ is a root of $f(x)$

$\Rightarrow f(x) = (x - \alpha_1) g_1(x)$

Since $\deg g_1 < n$, the inductive hypothesis implies there exists a splitting field $F_1 \hookrightarrow L$ of $g_1(x) \in F_1[x]$

Then $L$ is splitting field of $f(x) \in K[x]$.

---

$$K[x] \longrightarrow K[x]/(f(x))$$

$$x \longmapsto \alpha_1 = \text{coset } x + (f)$$

$$f = a_0 + a_1 x + \cdots + a_n x^n \longmapsto 0$$

Since ring hom,

$$f(\alpha_1) = \boxed{a_0 + a_1 \alpha + \cdots + a_n \alpha^n = 0}$$

## ⇝ Uniqueness

**Lemma:** Let $K \subset L$ be the splitting field for $f(x) \in K[x]$.
Let $\sigma : K \to L'$ be another field ext such that $f(x)$ splits$/L'$.
Then there exist $\bar{\sigma} : L \to L'$ such that $\forall x \in K$ $\sigma(x) = \bar{\sigma}(x)$

In other words,

splitting field of $f(x)$

$$\begin{tikzcd} L \arrow[rr, dashed, "\bar{\sigma}"] & & L' \\ K \arrow[u, phantom, "\cup"] \arrow[urr, "\sigma"'] & & \end{tikzcd}$$

$x \in L$, $x \mapsto \bar{\sigma}(x)$; $x \in K$, $x \mapsto \sigma(x)$

$f(x)$ splits

such that diagram commutes.

**Pf:** By induction on $|L:K|$

Factor $f(x) = a_n(x-\alpha_1)\cdots(x-\alpha_n)$
$\alpha_i \in L$

- Base case: $|L:K| = 1$
  $\implies K = L$. Take $\bar{\sigma} = \sigma$.
- In general, if $|L:K| > 1$,
  then $K \neq L$.
  Choose $\alpha \in L$ not in $K$.
  Let $\underline{g(x)} \in K[x]$ min poly of $\alpha$
  irred.

$$\begin{tikzcd} L & & \\ K(\alpha) \cong K[x]/(g) \arrow[u, phantom, "\cup"] \arrow[rr, dashed, "\sigma_1"] & & L' \\ K \arrow[u, phantom, "\cup"] \arrow[urr, "\sigma"'] & & \end{tikzcd}$$

## ⇝ Uniqueness

**Lemma:** Let $K \subset L$ be the splitting field for $f(x) \in K[x]$.
Let $\sigma : K \to L'$ be another field ext such that $f(x)$ splits$/L'$.
Then there exist $\bar{\sigma} : L \to L'$ such that $\forall x \in K$ $\sigma(x) = \bar{\sigma}(x)$

---

**Pf:** By induction on $|L:K|$

- If $K \neq L$, choose a root $\alpha \in L$ of $f(x)$ not in $K$.

---

Goal

$$
\begin{tikzcd}
L \arrow[dr, dashed, "\bar{\sigma}"] & \\
K(\alpha) \cong K[x]/(g) \arrow[u, phantom, "\cup"] \arrow[r, dashed, "\sigma_1"] & L' \\
K \arrow[u, phantom, "\cup"] \arrow[ur, "\sigma"'] &
\end{tikzcd}
$$

$\alpha \in K(\alpha)$

Let $g(x)$ be min poly of $\alpha$

Since $f(x)$ splits in $L'$, can also choose a root $\beta \in L'$

Let's define $\sigma_1$

Define $K[x] \longrightarrow L'$
$x \longmapsto \beta$.

Check $f(x)$ is in kernel.

Continue on Wed.