

Apr 26: Splitting Fields

Last 2 lectures: diversion to ruler & compass constructions

Today: Splitting fields

- definition
- properties (uniqueness!)

§1. Definition

Let $K \subset L$ be a field extension

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

$$f(x) = a_n(x-d_1) \cdots (x-d_n)$$

where $d_i \in L$

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}

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. $f(x) = a_n(x-d_1) \cdots (x-d_n)$

② $L = K(d_1, \dots, d_n)$

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

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

Examples

① $x^2+1 \in \mathbb{R}[x] \rightarrow$ splitting field
 $(x^2+1 \in \mathbb{Q}[x] \rightarrow$ splitting field $\mathbb{Q}(i))$ is \mathbb{C}

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

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

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

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 3rd root

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

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

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

↑
 $\sqrt{3}i$

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

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

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

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

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.

$(K \subset L_1 \subset L_2 \subset \cdots \subset L_s = L)$
 \uparrow \uparrow
 splitting field for f_1 splitting field for $f_2 \in L_1[x]$
 irred

Therefore, can construct

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

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

$$|F_1:K| \leq n \quad x \mapsto \alpha_1 = \bar{x}$$

($|F_2:F_1| \leq n-1$ & tower law to get $[L:K] \leq n!$)

So α_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 $F_1 \subset L$ of $g_1(x) \in F_1[x]$

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

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

$$x \mapsto \alpha_1 = \text{root } x + (f)$$

$$f = a_0 + a_1x + \cdots + a_nx^n \mapsto 0$$

Since isom hom,

$$f(x) = a_0 + a_1x + \cdots + a_nx^n = 0$$

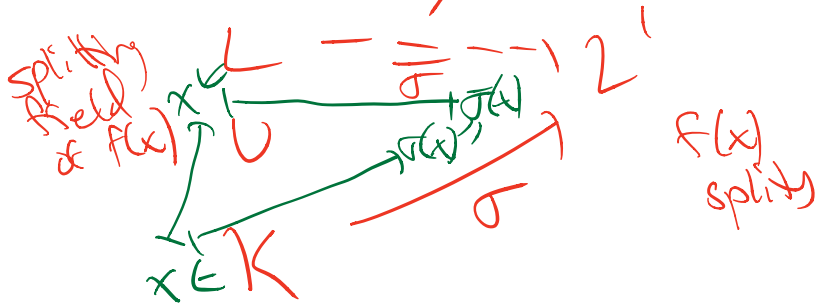
Uniqueness

Lemma: Let $K \subset L$ be the splitting field for $f(x) \in K[x]$.

Let $\sigma: K \rightarrow L'$ be another field ext such that $f(x)$ splits in L' .

Then there exist $\bar{\sigma}: L \rightarrow L'$ such that $\forall x \in K \sigma(x) = \bar{\sigma}(x)$

In other words,



such that diagram commutes.

PF: By induction on $[L:K]$

Factor $f(x) = a_n(x-d_1)\dots(x-d_n)$
 $d_i \in L$

• Base case: $[L:K] = 1$

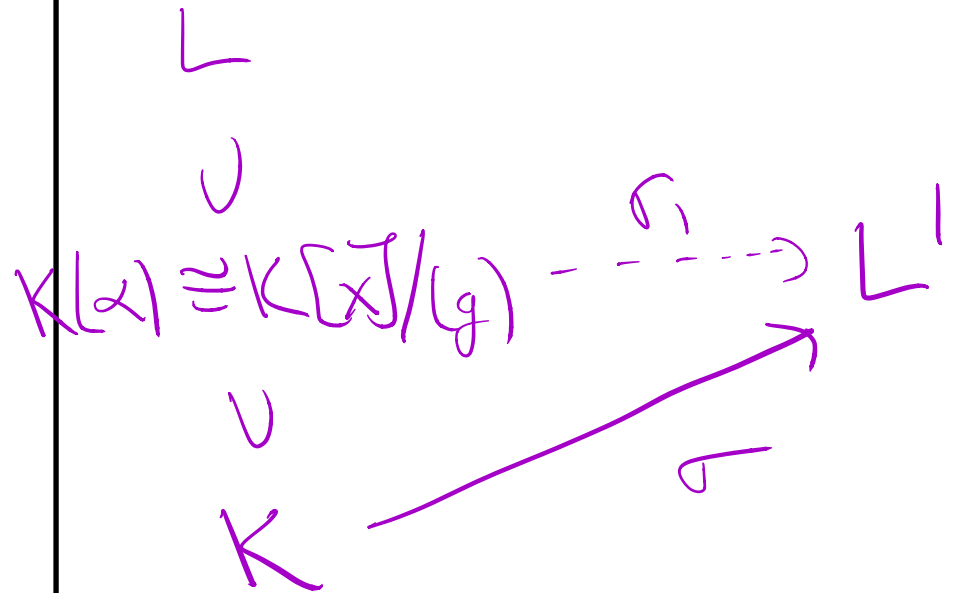
$\Rightarrow K = L$. Take $\bar{\sigma} = \sigma$.

• In general, if $[L:K] > 1$,

then $K \neq L$.

Choose $\alpha \in L$ not in K .

Let $g(x) \in K[x]$ min poly of α
 irred.



Uniqueness

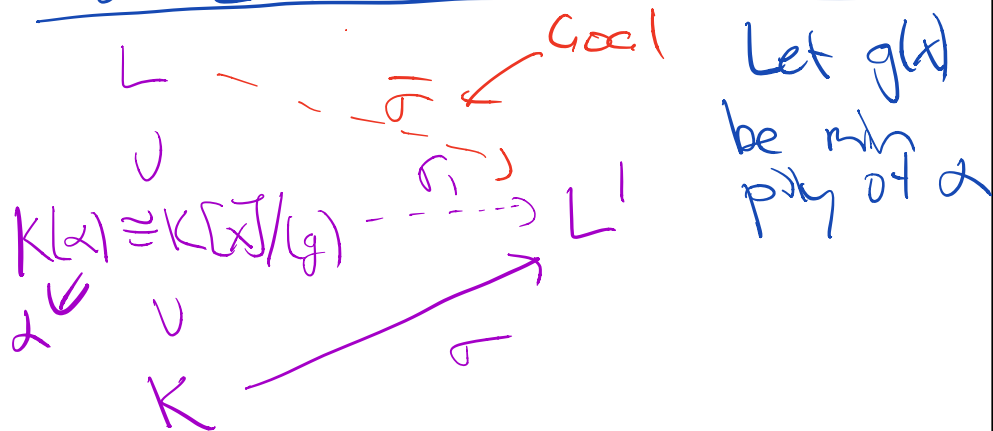
Lemma: Let $K \subset L$ be the splitting field for $f(x) \in K[x]$.

Let $\sigma: K \rightarrow L'$ be another field ext such that $f(x)$ splits in L' .

Then there exist $\bar{\sigma}: L \rightarrow L'$ 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 .



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

Let's define σ_1 .

Define $K[x] \rightarrow L'$
 $x \mapsto \beta$.

Check $f(x)$ is in kernel.

Continue on Wed.