Splitting fields: Definitions and Examples

Jiang-Hua Lu

The University of Hong Kong

MATH4302 Algebra II

Thursday April 3, 2025

In this file:

1. §3.2.1: Definition of splitting fields.
2. §3.2.2: Examples of splitting fields.

Main issue: Roots of polynomials in fields.

Definition: Let K be a field and $f(x) \in K[x]$ non-constant.

- An element $\alpha \in K$ is called a root of $f(x)$ in K if $f(\alpha) = 0$.
- If $K \subset L$ is a field extension, regard $f(x) \in L[x]$.
- If $\alpha \in L$ is such that $f(\alpha) = 0$, call α a root of $f(x)$ in L.

Central question: If $f(x) \in K[x]$ is non-constant, is there a field extension $K \subset L$ such that $f(x)$ has a root in L?

Example: $f(x) = x^2 + 1$ has no root in $\mathbb{R}$ but has roots in $\mathbb{C}$.

"mental construction":

$K[x]/\langle x^2+1 \rangle$

Answer to the central question: Yes:

- Let $f \in K[x]$ be non-constant.
- f must have an irreducible factor $p(x)$.
- Take $L = K[x]/\langle p(x) \rangle$ and let $\alpha = \overline{x} \in L$.
- Then α is a root of f in L.

Note $[L : K] \leq \deg p \leq$

Now set up some more precise definitions on roots.

Multiplicities of roots of polynomials. Let K be any field.

Let $f(x) \in K[x]$ be monic, and let $\alpha \in K$ be a root of f.

其实你们用 Taylor's thm 就可以

- By Euclidean algorithm, there exists $g_1(x) \in K[x]$ such that

$$f(x) = (x - \alpha)g_1(x) \in K[x].$$

- If $g_1(\alpha) = 0$, continue to get $g_2(x) \in K[x]$ such that

$$f(x) = (x - \alpha)^2 g_2(x) \in K(x).$$

- Continue to get $g(x) \in K[x]$ such that $g(\alpha) \neq 0$ and

$$f(x) = (x - \alpha)^m g(x) \in K[x].$$

- $m \geq 1$ is called the multiplicity of α as a root of f.
- Call α a repeated root if $m \geq 2$.

multiplicity of α : The largest m s.t. $(x-\alpha)^m \mid f(x)$

Derivative test for repeated roots.

Let $f = a_0 + a_1 x + \cdots + a_n x^n \in K[x]$, with $n \geq 1$ and $a_n \neq 0$.

check: $(f(x)g(x))' = f'(x)g(x) + f(x)g'(x)$

- Define $f'(x) \in K[x]$, the derivative of f, by

$$f'(x) = a_1 + 2a_2 x + \cdots + n a_n x^{n-1} \in K[x].$$

- Use sum and product rules in Calculus when computing $f'(x)$.

Warnings:

- If $\mathrm{Char}(K) = 0$, and $n = \deg f(x) \geq 1$, then $n a_n \neq 0$, so

$$f'(x) \neq 0 \quad \text{and} \quad \deg(f'(x)) = n - 1.$$

- If $\mathrm{Char}(K) > 0$, possible that $f(x)$ non-constant but $f'(x) = 0$.
- For example, $f(x) = x^p - 1 \in \mathbb{F}_p[x]$ has $f'(x) = 0$.

$\boxed{\text{Derivative test for repeated roots.}}$

α is repeated iff $f(\alpha)=f'(\alpha)=0$

Lemma: Let $f(x) \in K[x]$ with $\deg(f(x)) \geq 2$. An element $\alpha \in K$ is a repeated root of $f(x)$ if and only if

pf: Taylor's thm

$$f(\alpha) = 0 \quad \text{and} \quad f'(\alpha) = 0.$$

Proof. Let α be a root of $f(x)$ in K with multiplicity $m \geq 1$.

- Write $f(x) = (x - \alpha)^m g(x)$, where $g(x) \in K[x]$ and $g(\alpha) \neq 0$.
- By definition, α is a repeated root if and only if $m \geq 2$.
- If α is a repeated root, then
$$f'(x) = m(x - \alpha)^{m-1} g(x) + (x - \alpha)^m g'(x),$$
so $f(\alpha) = f'(\alpha) = 0$.
- If $f(\alpha) = f'(\alpha) = 0$, and if $m = 1$, then $f'(\alpha) = g(\alpha) \neq 0$, a contradiction, so $m \geq 2$.

Q.E.D.

Example:

every student's dream

For a prime number p, what is the multiplicity of $\alpha = 1$ as a root of

$$f(x) = x^p - 1 \in \mathbb{F}_p[x]?$$

(Derivative test says $\alpha = 1$ is a repeated root).

$$f(x) = (x-1)^p \in \mathbb{F}_p[x]$$

so $\alpha = 1$ has multiplicity p.

Actually this holds when $\mathrm{Char}(K) = p$, because $f'(x) = 0 \Rightarrow f(x) = f(x^{\frac{1}{p}})^p$

Roots of irreducible polynomials

Lemma: If $\mathrm{Char}(K) = 0$ and $p(x) \in K[x]$ is irreducible, then there exist $h(x), k(x) \in K[x]$ such that

$$h(x)p(x) + k(x)p'(x) = 1 \in K[x]. \tag{1}$$

identity holds in $L[x]$ for any $K \subset L$.

Proof. Let $n = \deg p(x)$.

- Since $\mathrm{Char}(K) = 0$ and $p(x)$ not a constant, $p'(x) \neq 0$.
- Thus $\deg p'(x) = n - 1$.
- Since $p(x)$ is irreducible, $p(x)$ and $p'(x)$ are co-prime.
- Since $K[x]$ is a PID, (1) holds for some $h(x), k(x) \in K[x]$.

$p(x), p'(x)$ coprime $\not\Rightarrow$ $p(x)$ irr

Q.E.D.

$p(x), p'(x)$ coprime $\Leftrightarrow$ no double factor

Lemma: If $\mathrm{Char}(K) = 0$ and $p(x) \in K[x]$ is irreducible, then $p(x)$ has no repeated roots in any field extension L of K.

Proof: Let $K \subset L$ be an extension and that α is a root of p in L.

- By previous Lemma, there exist $h(x), k(x) \in K[x]$ such that

$$h(x)p(x) + k(x)p'(x) = 1 \in K[x].$$

- Plugging in $x = \alpha$, one gets $p'(\alpha) \neq 0$.
- By the Derivative Test, α is not a repeated root of $p(x)$ in L.

Q.E.D.

Complete splitting of polynomials:

Definition. Let K be a field, and let $f(x) \in K[x]$ with degree $n \geq 1$.

- We say that $f(x)$ splits completely over K (or splits over K) if one of the following three equivalent conditins hold:
  1. $\exists\, c_0 \in L \backslash \{0\}$ and $\alpha_1, \cdots, \alpha_n \in K$ (not necessarily pairwise distinct), such that
  $$f(x) = c_0(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n),$$
  2. all the irreducible factors of $f(x)$ in $K[x]$ are linear;
  3. $f(x)$ has n roots in K counting multiplicity.
- If $K \subset L$ is a field extension, say $f(x)$ splits completely over L if $f(x)$, as an element in $L[x]$, is a product of linear factors.

Examples:

- $f(x) = x^3 - x^2 - x + 1 = x^2(x-1) - (x-1) = (x+1)(x-1)^2$ splits comletely in $\mathbb{Q}[x]$;
- $g(x) = (x-2)(x^2+1)$ does not completely splits in $\mathbb{R}[x]$.

Lemma. If L is an algebraically closed field, then every $f \in L[x]$ splits completely over L.

Proof. Direct consequence of the Euclidean Algorithm.

Taylor's theorem

Definition of splitting fields:

Let K be a field and let $f \in K[x]$ with $n = \deg(f) \geq 1$.

Definition: A splitting field of f over K is a field extension $K \subset L$ s.t.

say w/ roots $\alpha_1, \cdots \alpha_n$.

1. $f(x)$ splits completely over L;

   $K(\alpha_1, \cdots, \alpha_n)$

2. L is generated by K and all the roots of $f(x)$ in L, i.e.,

$$L = K(\alpha_1, \alpha_2, \cdots, \alpha_n),$$

where $\alpha_1, \ldots, \alpha_n$ are the n roots (with multiplicity) of f in L.

Remarks on the definition of splitting fields: Let $f(x) \in K[x]$ with $n = \deg f(x) \geq 1$, and let L be a splitting field of $f(x)$ over K.

1. f splits completely over L;
2. L is a finite extension of K;
3. L depends on both $f(x)$ and K such that $f(x) \in K[x]$.
4. A splitting field of $f(x) = x^2 + 1$ over $\mathbb{Q}$ is $\mathbb{Q}[i]$;
5. A splitting field of $f(x) = x^2 + 1$ over $\mathbb{R}$ is $\mathbb{C}$;
6. If $f(x)$ already completely splits over K, then $L = K$.

Existence and Uniqueness of splitting fields $\boxed{\text{(to be proved later):}}$

Theorem: Let K be a field and $f \in K[x]$ non-constant.

1. splitting fields of f over K exist;
2. if $K \subset L$ and $K \subset L'$ are two splitting fields of f over K, then there exists an isomorphism $\sigma : L \to L'$ such that $\sigma(a) = a$ for all $a \in K$.

we prove the one step extension

lemma

$$L = K(\alpha) \text{ — } K[x]/\langle f(x)\rangle \cong M[x]/\langle g(x)\rangle \text{ — } N = M(\beta)$$

embedding   embedding

$$f(x) \in K[x],\ K \xrightarrow{\text{isom } \sigma} M,\ g(x) \in M[x]$$

Easy case of constructing splitting fields:

Suppose that K is a sub-field of an algebraically closed field L. Let $f \in K[x]$ with $n = \deg(f) \geq 1$, and let $a_1, \ldots, a_n \in L$ be the roots of f in L.

Lemma-Definition. The sub-field $K(a_1, \ldots, a_n)$ of L is a splitting field of f over K, also called the splitting field of f in L over K.

Example. The splitting field of $f(x) = x^n - 1 \in \mathbb{Q}[x]$ over $\mathbb{C}$ is called the nth cyclotomic field. $C_n = \mathbb{Q}(e^{\frac{2\pi i}{n}})$

Example. For any sub-field K of $\mathbb{C}$ and $f = x^2 + bx + c \in K[x]$:

- The roots of f in $\mathbb{C}$ are

$$\alpha = \frac{1}{2}(-b \pm \sqrt{b^2 - 4\cancel{a}c}).$$

- Thus the splitting field of f over K is

$$L = K(\sqrt{b^2 - 4\cancel{a}c}).$$

The case of cubic polynomials:

Assume now that K is a subfield of $\mathbb{C}$, and $f \in K[x]$ is cubic, i.e.,

$$f(x) = x^3 + ax^2 + bx + c \in K[x].$$

Easy fact. Setting $x = z - a/3$, one gets

$$\tilde{f}(z) = f(z - \frac{a}{3}) = z^3 + pz + q \in K[z],$$

where

$$p = -\frac{a^2}{3} + b, \qquad q = \frac{2a^3}{27} - \frac{ab}{3} + c. \tag{2}$$

The following fact already known in the middle of the 16th century.

$x^3 - 3MNx - M^3 - N^3$

Lemma. Let $a, b, c \in \mathbb{C}$, and let p, q be given as in (2). Then the three roots of $f(x) = x^3 + ax^2 + bx + c$ in $\mathbb{C}$ are

$$\alpha_1 = -\frac{a}{3} + \beta_1 + \beta_2, \qquad \alpha_2 = -\frac{a}{3} + \omega\beta_1 + \omega^2\beta_2, \qquad \alpha_3 = -\frac{a}{3} + \omega^2\beta_1 + \omega\beta_2,$$

where $\omega = e^{2\pi i/3}$ and $\beta_1, \beta_2 \in \mathbb{C}$ are any cubic roots

$$\beta_1 = \sqrt[3]{\frac{1}{2}\left(-q + \sqrt{q^2 + \frac{4p^3}{27}}\right)}, \qquad \beta_2 = \sqrt[3]{\frac{1}{2}\left(-q - \sqrt{q^2 + \frac{4p^3}{27}}\right)},$$

satisfying $\beta_1\beta_2 = -p/3$.

Lemma. Let $a, b, c \in \mathbb{C}$, and let p, q be given as in (2). Then the three roots of $f(x) = x^3 + ax^2 + bx + c$ in $\mathbb{C}$ are

$$\alpha_1 = -\frac{a}{3} + \beta_1 + \beta_2, \qquad \alpha_2 = -\frac{\overset{a}{\cancel{b}}}{3} + \omega\beta_1 + \omega^2\beta_2, \qquad \alpha_3 = -\frac{a}{3} + \omega^2\beta_1 + \omega\beta_2,$$

where $\omega = e^{2\pi i/3}$ and $\beta_1, \beta_2 \in \mathbb{C}$ are any cubic roots

$$\beta_1 = \sqrt[3]{\frac{1}{2}\left(-q + \sqrt{q^2 + \frac{4p^3}{27}}\right)}, \qquad \beta_2 = \sqrt[3]{\frac{1}{2}\left(-q - \sqrt{q^2 + \frac{4p^3}{27}}\right)},$$

satisfying $\beta_1\beta_2 = -p/3$. Define

$$\Delta_f = (\alpha_1 - \alpha_2)^2(\alpha_2 - \alpha_3)^2(\alpha_3 - \alpha_1)^2.$$

Then

$$\Delta_f = -4p^3 - 27q^2 = a^2b^2 + 18abc - 4b^3 - 4a^3c - 27c^2 \in K.$$

Proof. Exercise (see lecture notes).

Definition of Discriminants:

1. For a quadratic polynomial $f(x) = x^2 + bx + c \in K[x]$,
$$\Delta_f = b^2 - 4c \in K$$
is called the discriminant of $f(x)$.

2. For a cubic polynomial $f(x) = x^3 + ax^2 + bx + c \in K[x]$,
$$\Delta_f = a^2b^2 + 18abc - 4b^3 - 4a^3c - 27c^2 \in K$$
is called the discriminant of f.

Lemma $f(x)$ has a repeated root iff $\Delta_f = 0$.

Splitting fields of cubic polynomials: Let K be a subfield of $\mathbb{C}$.

Theorem. Let $f(x) \in K[x]$ be cubic and monic, and let $\alpha_1, \alpha_2, \alpha_3$ be its roots in $\mathbb{C}$. Let

$$L_f = K(\alpha_1, \alpha_2, \alpha_3)$$

be the splitting field of f in $\mathbb{C}$ over K.

1. If f is reducible over K. then $[L_f : K] = 2$ or 1, depending on whether only one or all the three of $\alpha_1, \alpha_2, \alpha_3$ are in K;

2. If f is irreducible over K, then

$$[L_f : K] = \begin{cases} 3, & \Delta_f \text{ has a square root in } K, \\ 6, & \text{otherwise} \end{cases}.$$

Proof: In tutorial

Proof. May assume that $f(x) = x^3 + px + q$.

- Let $\alpha_1, \alpha_2, \alpha_3$ be the three roots of f in $\mathbb{C}$, and let
$$\delta = (\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)(\alpha_2 - \alpha_3) \in \mathbb{C}.$$
- By definition $\delta^2 = \Delta_f \in K$, but δ may or may not in K.

  Using $\alpha_1 + \alpha_2 + \alpha_3 = 0$ and definition of δ, one has
$$\alpha_2 = \frac{\delta + 2\alpha_1 p + 3q}{2(3\alpha_1^2 + p)}.$$
- Thus $L = K(\alpha_1, \delta)$.

Proof cont'd:

- Assume $\delta \in K$. Then $L_f = K(\alpha_1)$.
- Since f is the minimal polynomial of α_1, we have $[L_f : K] = 3$.
- Assume $\delta \notin K$. Then
  $$[L_f : K] = [K(\alpha_1)(\delta) : K(\alpha_1)][K(\alpha_1) : K] = 3[K(\alpha_1)(\delta) : K(\alpha_1)].$$
- Thus $[L_f : K]$ is divisible by 3.
- Now $\delta^2 - \Delta_f = 0$, where $\Delta_f = -4p^3 - 27q^2 \in K \subset K(\alpha_1)$.
- So $[L_f : K(\alpha_1)] = 1$ or 2 depending on whether $\delta \in K(\alpha_1)$ or $\delta \notin K(\alpha_1)$. Thus $[L : K] \leq 6$.
- Thus As $\delta \notin K$ but $\delta^2 \in K$, $[K(\delta) : K] = 2$, so
  $$[L_f : K] = [K(\delta)(\alpha_1) : K(\delta)][K(\delta) : K] = 2[K(\delta)(\alpha_1) : K(\delta)],$$
  so $[L_f : K]$ is divisible by 2 as well. Thus $[L_f : K] = 6$.

Q.E.D.

Example:

The polynomial $f(x) = x^3 - 4x + 2 \in \mathbb{Q}[x]$ is irreducible by Eisenstein's criterion. We have

$$\Delta_f = -4(-4)^3 - 27 \times 4 = 4 \times 37,$$

which has no square root in $\mathbb{Q}$. Let L be the splitting field of f over $\mathbb{Q}$ in $\mathbb{C}$. Then $[L : \mathbb{Q}] = 6$.

f