Field extensions: definitions and degrees

Jiang-Hua Lu

The University of Hong Kong

MATH4302 Algebra II, HKU

Thursday, March 28, 2025

In this file:

- § 3.1.1: Motivations and definition of field extensions;
- §3.1.2: Degrees of field extensions.

§3.1.1: Motivations and definition of field extensions

- Linear algebra: vector spaces over any field;
- Analysis: $\mathbb{R}$ or $\mathbb{C}$, or p-adic fields;
- Number theory: $\mathbb{Q}$; algebraic number fields, p-adic fields;
- Algebraic and arithmetic geometry: fields of rational functions on geometrical objects;
- Coding theory: finite fields;
- Modern mathematical physics: all the fields above.

Questions on finite fields and answers.

- For any given integer $n \geq 2$, is there a field of size n?
- Is yes, how many up to isomorphisms?

Sub-fields and examples.

Definition. Let L be a field. A subset $K \subset L$ is a sub-field if

- K is a subring;
- K is closed under taking inverses of non-zero elements.

We also call L a field extension of K.

Lemma. If K and L are fields and

$$\phi : K \longrightarrow L$$

is a non-zero ring homomorphism, then ϕ is injective and $\phi(K)$ is a sub-field of L. Also call $\phi : K \to L$ a field extension.

Proof. Exercise.

Observations: Let L be a field.

- The intersection of any family of sub-fields of L is a sub-field of L;

The prime subfield of a field.

Definition. The prime subfield of a field K is the intersection of all subfields of K.

Lemma. Let K be a field.

1. If K has characteristic p, then the prime subfield is isomorphic to $\mathbb{F}_p$, so K is an extension of $\mathbb{F}_p$;
2. If K is has characteristic 0, then the prime subfield of K is isomorphic to $\mathbb{Q}$, so K is an extension of $\mathbb{Q}$.

Thus every field is an extension of either $\mathbb{F}_p$ and $\mathbb{Q}$.

Roots of polynomials: Let $K \subset L$ be a field extension. Let

$$p(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \in K[x].$$

- An element $\alpha \in K$ is called a root of p in K if

$$a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_n\alpha^n = 0 \in K.$$

- An element $\alpha \in L$ is called a root of p in L if

$$a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_n\alpha^n = 0 \in L.$$

Example: $f(x) = x^2 - 2 \in \mathbb{Q}[x]$ has no roots in $\mathbb{Q}$, but $\alpha = \sqrt{2}$ is a root of $f(x)$ in $\mathbb{R}$.

A fundamental example:

Let K be a field and $p(x) \in K[x]$ is irreducible. Let

$$\pi : \quad K[x] \longrightarrow L = K[x]/\langle p(x)\rangle, \quad f(x) \longmapsto f(x) + \langle p(x)\rangle.$$

- For $k \in K$, regard k as a constant polynomial in $K[x]$ and let $\overline{k} = \pi(k) \in L$. Then

$$K \longrightarrow L = K[x]/\langle p(x)\rangle, \quad k \longmapsto \overline{k},$$

  is a field extension.

- We also just write $k = \overline{k} \in L$.

- Define $\alpha = \phi(x) \in L$. Then α is a root of $p(x)$ in L.

Proof. Proved on the board.

Roots of polynomials, cont'd:

Corollary: Let K be any field and let $f(x)$ be any non-constant polynomial in $K[x]$. Then there exists a field extension $K \subset L$ such that $f(x)$ has a root in L.

Proof. Let $p(x)$ be any irreducible factor of $f(x)$, and let

$$L = K[x]/\langle f(x)\rangle.$$

Then L is a field extension of K, and $p(x)$ has a root in L. Thus $f(x)$ has a root in L.

§3.1.2: Degrees of field extensions.

Key idea: If $K \subset L$ is a field extension, then L as a vector space over K.

Definitions.

1. The degree of a field extension $K \subset L$ is the dimension of L as a vector space over K and is denoted as $[L : K]$.
2. If $[L : K] < +\infty$, call L a finite extension of K;
3. If $[L : K] = +\infty$, call L an infinite extension of K.

Example. For a field F,

$$F(x) = \left\{ \frac{f(x)}{g(x)} : \ f, g \in F[x], g \neq 0 \right\}$$

is the field of fractions of $F[x]$, and is an infinite extension of F.

Pf: Check that $\{1, x, x^2, x^3, \ldots\}$ is a linearly independent subset!

The fundamental example again:

Lemma. If $p(x) \in K[x]$ is irreducible and has degree n, the

$$L = K[x]/\langle p(x) \rangle$$

is a field extension of K of degree n.

Pf: Check that $\{\bar{1}, \bar{x}, \cdots, \overline{x^{n-1}}\}$ is a basis of L over K.

(Did this on board)

The Tower Theorem.

The Tower Theorem: If $K \subset L$ and $L \subset M$ are finite extensions, then $K \subset M$ is a finite extension and

$$[M : K] = [M : L][L : K].$$

To continue on Monday March 24, 2025

Orders of finite fields

Theorem. If K is a finite field, then $|K| = p^n$ for some prime number p and some integer n.