MAT205: Abstract Algebra II

Field Extensions and Roots of Polynomials

Ma, Jia-Jun - Xiamen University Malaysia

Part I

Field Extensions

Definition: Field Extension

Let F and E be fields.

A **field extension** is an inclusion of fields

$$F \subseteq E.$$

We write this as

$$E/F.$$

The notation E/F is **not** quotient notation.

Examples: Field Extensions

Extension	Inclusion
$\mathbb{C}/\mathbb{R}$	$\mathbb{R} \subseteq \mathbb{C}$
$\mathbb{R}/\mathbb{Q}$	$\mathbb{Q} \subseteq \mathbb{R}$
$\mathbb{Q}(\sqrt{2})/\mathbb{Q}$	$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2})$
$\mathbb{R}(i)/\mathbb{R}$	$\mathbb{R} \subseteq \mathbb{R}(i) = \mathbb{C}$

Here

$$\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}.$$

Non-Examples

$$\mathbb{Q}/\mathbb{Z}$$

is not a field extension.

Reason:

$$\mathbb{Z}$$

is not a field.

Also,

$$\mathbb{R}/\mathbb{C}$$

is not a field extension by inclusion, because

$$\mathbb{C} \not\subseteq \mathbb{R}.$$

Field Extensions as Vector Spaces

If $F \subseteq E$, then E is a vector space over F.

Scalar multiplication is multiplication in E:

$$\lambda \cdot x = \lambda x, \qquad \lambda \in F, \quad x \in E.$$

The **degree** of E/F is

$$[E : F] = \dim_F E.$$

Examples: Extension Degree

$$[\mathbb{C} : \mathbb{R}] = 2$$

with basis

$$\{1, i\}.$$

$$[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$$

with basis

$$\{1, \sqrt{2}\}.$$

For now, degree is only notation. Its general theory belongs with algebraic extensions.

Part II

Polynomial Equations and Larger Fields

Example: $x^2 - 2$

The equation

$$x^2 - 2 = 0$$

has no solution in $\mathbb{Q}$.

It has solutions in the larger field $\mathbb{Q}(\sqrt{2})$:

$$\sqrt{2}, \qquad -\sqrt{2}.$$

Example: $x^2 + 1$

The equation

$$x^2 + 1 = 0$$

has no solution in $\mathbb{R}$.

It has solutions in the larger field

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

$$i, \qquad -i.$$

Polynomial Roots in Larger Fields

A polynomial over a field F may have no root in F.

It may have a root after passing to a larger field

$$F \subseteq E.$$

The construction will use quotient rings of the form

$$F[x]/(p(x)).$$

Part III

Irreducible Polynomials and Maximal Ideals

Definition: Irreducible Polynomial

Let F be a field.

A polynomial $p(x) \in F[x]$ is **irreducible over F** if:

1. $p(x) \neq 0$;
2. $p(x)$ is nonconstant;
3. if

$$p(x) = a(x)b(x),$$

then $a(x)$ or $b(x)$ is a unit in $F[x]$.

Units in $F[x]$

Since F is a field, the units in $F[x]$ are exactly the nonzero constant polynomials.

Thus $p(x)$ is irreducible if it has no factorization

$$p(x) = a(x)b(x)$$

with

$$\deg a > 0, \qquad \deg b > 0.$$

Examples: Irreducibility

$$x^2 - 2$$

is irreducible over $\mathbb{Q}$.

$$x^2 + 1$$

is irreducible over $\mathbb{R}$.

But $x^2 + 1$ is not irreducible over $\mathbb{C}$, since

$$x^2 + 1 = (x - i)(x + i).$$

$$x^3 - 2$$

is irreducible over $\mathbb{Q}$.

Proposition: Irreducible Implies Maximal

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

Then

$$(p(x))$$

is a maximal ideal of $F[x]$.

Therefore

$$F[x]/(p(x))$$

is a field.

Proof: Maximality

Let I be an ideal such that

$$(p(x)) \subseteq I \subseteq F[x].$$

Since $F[x]$ is a PID, write

$$I = (g(x)).$$

The inclusion $(p(x)) \subseteq (g(x))$ means

$$p(x) = g(x)h(x)$$

for some $h(x) \in F[x]$.

Proof: Maximality

Since $p(x)$ is irreducible,

$$p(x) = g(x)h(x)$$

forces $g(x)$ or $h(x)$ to be a unit.

If $g(x)$ is a unit, then

$$I = (g(x)) = F[x].$$

If $h(x)$ is a unit, then

$$I = (g(x)) = (p(x)).$$

So $(p(x))$ is maximal.

Examples: Quotient Fields

Since $x^2 - 2$ is irreducible over $\mathbb{Q}$,

$$\mathbb{Q}[x]/(x^2 - 2)$$

is a field.

Since $x^2 + 1$ is irreducible over $\mathbb{R}$,

$$\mathbb{R}[x]/(x^2 + 1)$$

is a field.

Part IV

Constructing Roots

Notation in $F[x]/(p(x))$

Let $p(x) \in F[x]$ be irreducible and define

$$E = F[x]/(p(x)).$$

Write

$$\alpha = x + (p(x)).$$

Every element of E can be written as

$$a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1},$$

where $n = \deg p$ and $a_i \in F$.

Constructing a Root

Let $p(x) \in F[x]$ be irreducible and let

$$E = F[x]/(p(x)).$$

The field F embeds into E by sending $a \in F$ to the class of the constant polynomial a.

With this identification,

$$F \subseteq E.$$

So E/F is a field extension.

The Root in the Quotient

Let

$$\alpha = x + (p(x)) \in F[x]/(p(x)).$$

Then

$$p(\alpha) = 0.$$

Indeed, if

$$p(x) = a_0 + a_1 x + \cdots + a_n x^n,$$

then

$$p(\alpha) = p(x) + (p(x)) = 0.$$

Theorem: Existence of a Root

Let F be a field and let $f(x) \in F[x]$ be nonconstant.

Then there exists a field extension E/F and an element $\alpha \in E$ such that

$$f(\alpha) = 0.$$

Proof: Existence of a Root

Choose an irreducible factor $p(x)$ of $f(x)$ in $F[x]$.

Write

$$f(x) = p(x)q(x).$$

Let

$$E = F[x]/(p(x)), \qquad \alpha = x + (p(x)).$$

Then $p(\alpha) = 0$, so

$$f(\alpha) = p(\alpha)q(\alpha) = 0.$$

Part V

Examples

Example: $x^2 - 2$ over $\mathbb{Q}$

Let

$$E = \mathbb{Q}[x]/(x^2 - 2), \qquad \alpha = x + (x^2 - 2).$$

Then

$$\alpha^2 - 2 = 0, \qquad \alpha^2 = 2.$$

Every element of E has the form

$$a + b\alpha, \qquad a, b \in \mathbb{Q}.$$

Example: $\mathbb{Q}[x]/(x^2-2)$

There is an isomorphism

$$\mathbb{Q}[x]/(x^2-2) \longrightarrow \mathbb{Q}(\sqrt{2})$$

given by

$$\alpha \longmapsto \sqrt{2}.$$

The quotient construction is an abstract version of adjoining $\sqrt{2}$.

Example: $x^2 + 1$ over $\mathbb{R}$

Let

$$E = \mathbb{R}[x]/(x^2 + 1), \qquad \alpha = x + (x^2 + 1).$$

Then

$$\alpha^2 + 1 = 0, \qquad \alpha^2 = -1.$$

Every element of E has the form

$$a + b\alpha, \qquad a, b \in \mathbb{R}.$$

Example: $\mathbb{R}[x]/(x^2+1)$

There is an isomorphism

$$\mathbb{R}[x]/(x^2+1) \longrightarrow \mathbb{C}$$

given by

$$\alpha \longmapsto i.$$

So $\mathbb{C}$ can be constructed from $\mathbb{R}$ by adjoining a root of x^2+1.

Example: $x^3 - 2$ over $\mathbb{Q}$

Let

$$E = \mathbb{Q}[x]/(x^3 - 2), \qquad \alpha = x + (x^3 - 2).$$

Then

$$\alpha^3 = 2.$$

Every element of E has the form

$$a + b\alpha + c\alpha^2, \qquad a, b, c \in \mathbb{Q}.$$

This construction gives a field containing one root of $x^3 - 2$.

Definition: Adjoining a Root

The notation

$$F(\alpha)$$

means the smallest subfield containing F and α.

In the construction

$$E = F[x]/(p(x)), \qquad \alpha = x + (p(x)),$$

one has

$$E = F(\alpha).$$

The element α satisfies

$$p(\alpha) = 0.$$

Part VI

Algebraic Elements and Algebraic Extensions

Motivation: Algebraic Extensions from Solving Equations

The construction $F(\alpha) = F[x]/(p(x))$ produced an extension in which the polynomial equation $p(\alpha) = 0$ holds.

Every element of $F(\alpha)$ satisfies *some* polynomial equation over F – closure of F-polynomial expressions in α.

We isolate this property: an extension built from solutions of polynomial equations is an **algebraic extension**.

Definition: Algebraic and Transcendental Elements

Let E/F be a field extension and $\alpha \in E$.

α is **algebraic over** F if there exists nonzero $f \in F[x]$ with $f(\alpha) = 0$.

α is **transcendental over** F otherwise.

Examples: Algebraic and Transcendental

Algebraic over $\mathbb{Q}$:

- $\sqrt{2}$ (root of $x^2 - 2$);
- i (root of $x^2 + 1$);
- $\sqrt[3]{5}$ (root of $x^3 - 5$);
- $\zeta_n = e^{2\pi i/n}$ (root of $x^n - 1$);
- $\frac{1+\sqrt{5}}{2}$ (root of $x^2 - x - 1$).

Transcendental over $\mathbb{Q}$: e (Hermite 1873) and π (Lindemann 1882). Proofs are real-analytic and outside this course.

Definition: Algebraic Extension

Definition. E/F is an **algebraic extension** if every $\alpha \in E$ is algebraic over F.

E/F is a **transcendental extension** if some $\alpha \in E$ is transcendental over F.

Examples.

- $\mathbb{C}/\mathbb{R}$ is algebraic.
- $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ is algebraic.
- $\mathbb{R}/\mathbb{Q}$ is transcendental (since $\pi \in \mathbb{R}$ is transcendental).

Theorem: Finite Implies Algebraic

Theorem. If $[E : F] = n < \infty$, then E/F is algebraic.

Proof. Fix $\alpha \in E$. The $n+1$ powers $1, \alpha, \alpha^2, \ldots, \alpha^n$ lie in an n-dimensional F-vector space.

So they are linearly dependent over F: there exist $c_0, \ldots, c_n \in F$, not all zero, with

$$c_0 + c_1\alpha + \cdots + c_n\alpha^n = 0.$$

The polynomial $\sum c_i x^i \in F[x]$ is nonzero and has α as a root.

Minimal Polynomial and $F(\alpha)$

Let $\alpha \in E$ be algebraic over F. The set

$$I_\alpha = \{f \in F[x] : f(\alpha) = 0\}$$

is a nonzero ideal of $F[x]$.

$F[x]$ is a PID, so $I_\alpha = (m_\alpha)$ for a unique monic generator m_α, the **minimal polynomial** of α over F.

m_α is irreducible (else $F(\alpha)$ would contain zero divisors).

Consequence. $F(\alpha) \cong F[x]/(m_\alpha)$ and $[F(\alpha) : F] = \deg m_\alpha < \infty$.

Tower Law (Statement)

Theorem. Let $F \subseteq K \subseteq E$ be a tower of fields. Then

$$[E : F] = [E : K] \cdot [K : F],$$

with the convention $\infty \cdot n = \infty$.

Theorem: Algebraic Elements Form a Subfield

Let E/F be a field extension. Define

$$F_E^{\text{alg}} = \{\alpha \in E : \alpha \text{ algebraic over } F\}.$$

Theorem. F_E^{alg} is a subfield of E containing F.

Consequence. Sums, products, and inverses of algebraic elements are again algebraic.

Proof: Algebraic Elements Form a Subfield

$F \subseteq F_E^{\text{alg}}$: every $a \in F$ is a root of $x - a \in F[x]$.

Take $\alpha, \beta \in F_E^{\text{alg}}$. Show $\alpha \pm \beta$, $\alpha\beta$, β^{-1} ($\beta \neq 0$) are algebraic.

Step 1. $[F(\alpha) : F] < \infty$ (minimal polynomial slide).

Step 2. β is algebraic over F via $m_\beta \in F[x] \subseteq F(\alpha)[x]$, so also algebraic over $F(\alpha)$. Hence $[F(\alpha)(\beta) : F(\alpha)] < \infty$.

Step 3. Tower law: $[F(\alpha, \beta) : F] = [F(\alpha)(\beta) : F(\alpha)] \cdot [F(\alpha) : F] < \infty$.

Step 4. Finite implies algebraic: every element of $F(\alpha, \beta)$ is algebraic over F. Done.

Corollary: Transitivity of Algebraicity

Corollary. Let $F \subseteq K \subseteq L$ be a tower. If K/F and L/K are both algebraic, then L/F is algebraic.

Proof. Take $\alpha \in L$. There is a nonzero $g(x) \in K[x]$ with $g(\alpha) = 0$; write $g(x) = c_n x^n + \cdots + c_0$ with $c_i \in K$.

Each $c_i \in K$ is algebraic over F, so $K' := F(c_0, \ldots, c_n)$ has $[K' : F] < \infty$ (iterate minimal-polynomial slide + tower law).

α is algebraic over K' (via g), so $[K'(\alpha) : K'] < \infty$.

Tower law: $[K'(\alpha) : F] = [K'(\alpha) : K'] \cdot [K' : F] < \infty$.

Finite implies algebraic: α is algebraic over F.