Lecture 12

Extension Fields (体の拡大)

12.1 Extension Fields (体の拡大)

12.2 Simple Field

12.3 Algebra Closure

12.1 Extension Fields (体の拡大)

12.1 Extension Fields (体の拡大)

It is natural to ask whether or not some field F is contained in a larger field. We think of the rational numbers, which reside inside the real numbers, while in turn, **the real numbers live inside the complex numbers**. We can also study the fields between $\mathbb{Q}$ and $\mathbb{R}$ and inquire as to the nature of these fields.

More specifically if we are given a field F and a polynomial $p(x) \in F[x]$, we can ask whether or not we can find a field E containing F such that $p(x)$ factors into linear factors over $E[x]$. For example, if we consider the polynomial

$$p(x) = x^4 - 5x^2 + 6$$

In $\mathbb{Q}[x]$, then $p(x)$ factors as $(x^2 - 2)(x^2 - 3)$. However, both of these factors are irreducible in $\mathbb{Q}[x]$. If we wish to find a root of $p(x)$, we must go to a larger field. Certainly the field of real numbers will work, since

$$p(x) = \left(x - \sqrt{2}\right)\left(x + \sqrt{2}\right)\left(x - \sqrt{3}\right)\left(x + \sqrt{3}\right)$$

It is possible to find a smaller field in which $p(x)$ has a root, namely

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

We wish to be able to compute and study such fields for arbitrary polynomials over a field F.

12.1 Extension Fields (体の拡大)

Definition 12.1

A **field** E is an **extension field of a field** F if F is a **subfield of** E. We write $F \subseteq E$. The field F is called the **base field**.

For example,

$\mathbb{R}$ is an extension field of $\mathbb{Q}$,

$\mathbb{C}$ is an extension field of both $\mathbb{R}$ and $\mathbb{Q}$,

$\mathbb{Q}(\sqrt{2})$ is an extension field of $\mathbb{Q}$.

12.1 Extension Fields (体の拡大)

Theorem 12.1 (Kronecker's Theorem or Fundamental Theorem of Field Theory)

Let F be a **field and** $f(x)$ is a **polynomial** in $F[x]$ **of degree at least** 1.

Then **there exists an extension field** E **of** F **and** an $\tau \in E$ such that $f(\tau) = 0$.

Proof (See page 356 of the textbook)

12.1 Extension Fields (体の拡大)

Definition 12.2

Let E be **an extension field** of a **field** F. **For** $\tau \in E$, **if** $f(\tau) = 0$ **for some nonzero** $f(x) \in F[x]$, we say τ is **algebraic (代数的) over** F.

Otherwise, τ is **transcendental (超越的) over** F.

An **extension field** E of a field F is an **algebraic extension** of F if **every element in** E **is algebraic over** F.

Example 12.1

(1) Because $\sqrt{2}$ is a **root** of $x^2 - 2 \in \mathbb{Q}[x]$, so $\sqrt{2}$ is **algebraic over** $\mathbb{Q}$.

(2) i is **algebraic over** $\mathbb{Q}$ because i is a **root** of $x^2 + 1 \in \mathbb{Q}[x]$.

Example 12.2

We will show that $\sqrt{1+\sqrt{3}}$ is **algebraic over** $\mathbb{Q}$.

If $\tau = \sqrt{1+\sqrt{3}}$, then $\tau^2 = 1+\sqrt{3}$.

Hence $\tau^2 - 1 = \sqrt{3}$ and $(\tau^2-1)^2 = 3$.

Since $\tau^4 - 2\tau^2 - 2 = 0$, it must be true that τ is a **root** of the polynomial $x^4 - 2x^2 - 2 \in \mathbb{Q}[\mathrm{x}]$.

12.2 Simple Extension (単純拡大)

12.2 Simple Extension (単純拡大)

Definition 12.3

An element of $\mathbb{C}$ that is **algebraic over** $\mathbb{Q}$ is an **algebraic number (代数的数)**.

A **transcendental number (超越数)** is an element of $\mathbb{C}$ that is **transcendental over** $\mathbb{Q}$.

12.2 Simple Extension (単純拡大)

Consider the **extension field** $\mathbb{R}$ of $\mathbb{Q}$. We know that $\sqrt{2}$ is **algebraic over** $\mathbb{Q}$, being a **root** of $x^2 - 2$. We know that $\sqrt{2}$ is also a **root** of $x^3 - 2x$ and of $x^4 - 3x^2 + 2 = (x^2 - 2)(x^2 - 1)$.

Both these other polynomials having $\sqrt{2}$ as a root were multiplies of $x^2 - 2$. The next theorem shows that this is an illustration of a general situation.

12.2 Simple Extension (単純拡大)

Theorem 12.2

Let E be an extension field of F, and let $\tau \in E$, where τ is algebraic over F. Then there is an irreducible polynomial $p(x) \in F[x]$ such that $p(\tau) = 0$. This irreducible polynomial $p(x)$ is uniquely determined up to a constant factor in F and is a polynomial of minimal degree $\deg p(x) \geq 1$ in $F[x]$ having τ as a root. If $f(x) = 0$ for $f(x) \in F[x]$, with $f(x) \neq 0$, then $p(x)$ divides $f(x)$.

By multiplying by a suitable constant in F, we can assume that the coefficient of the highest power of x appearing in $p(x)$ of the Theorem 12.2 is 1. Such a polynomial having 1 as the coefficient of the highest power of x appearing is a **monic polynomial** (モニック多項式).

12.2 Simple Extension (単純拡大)

Definition 12.4

Let E be an extension field of a field F, and let $\tau \in E$ be algebraic over F. The unique **monic polynomial** $p(x)$ having the property described in Theorem 12.2 is the **irreducible polynomial for τ over F** and will be denoted by $\mathrm{irr}(\tau, F)$. The **degree of irreducible polynomial** $\mathrm{irr}(\tau, F)$ is the degree of τ over F, denoted by $\deg(\tau, F)$.

Example 12.3

We know that $\mathrm{irr}(\sqrt{2}, \mathbb{Q}) = x^2 - 2$. Referring to Example 12.2, we see that for $\tau = \sqrt{1+\sqrt{3}}$ in $\mathbb{R}$, τ is a root of $x^4 - 2x^2 - 2$, which is in $\mathbb{Q}[x]$. Since $x^4 - 2x^2 - 2$ is irreducible over $\mathbb{Q}$, we see that

$$\mathrm{irr}\left(\sqrt{1+\sqrt{3}}, \mathbb{Q}\right) = x^4 - 2x^2 - 2$$

Thus $\sqrt{1+\sqrt{3}}$ is algebraic of degree 4 over $\mathbb{Q}$.

12.2 Simple Extension (単純拡大)

Definition 12.5

An **extension field** E of a field F is a **simple extension** of F if $E = F(\tau)$ for some $\tau \in E$.

Theorem 12.3

Let E be a **simple extension** $F(\tau)$ of a field F, and let τ be algebraic over F. Let the degree of $\mathrm{irr}(\tau, F)$ be at least 1. Then every element of β can be uniquely expressed in the form

$$\beta = b_0 + b_1\tau + b_2\tau^2 + \cdots + b_{n-1}\tau^{n-1}$$

where the b_i are in F.

12.2 Simple Extension (単純拡大)

*Theorem 12.4

Let $f(x) \in \mathrm{F}[x]$ and let $f(x)$ be of degree 2 or 3. Then $f(x)$ is **reducible** over F if and only if it has a root in F.

Example 12.4 The polynomial in $p(x) = x^2 + x + 1$ in $\mathbb{Z}_2[x]$ is irreducible over $\mathbb{Z}_2$ by Theorem 12.4, since neither element 0 nor element 1 of $\mathbb{Z}_2$ is a root of $p(x)$. By Theorem 12.1, we know that there is an extension field E of $\mathbb{Z}_2$ containing a root τ of $x^2 + x + 1$. By theorem 12.3, it has as elements $0 + 0\tau$, $1 + 0\tau$, $0 + 1\tau$, and $1 + 1\tau$, that is 0, 1, τ and $1 + \tau$. This gives us *a new finite field of four elements*! The addition and multiplication tables for this field are shown in Table 12.1 and Table 12.2. For example, to compute $(1 + \tau)(1 + \tau)$, we observe that since $p(\tau) = \tau^2 + \tau + 1 = 0$, then

$$\tau^2 = -\tau - 1 =_2 \tau + 1$$

Therefore

$$(1 + \tau)(1 + \tau) = 1 + 2\tau + \tau^2 =_2 1 + \tau^2 = 1 + (\tau + 1) =_2 \tau$$

$+$	0	1	τ	$1+\tau$
0	0	1	τ	$1+\tau$
1	1	0	$1+\tau$	τ
τ	τ	$1+\tau$	0	1
$1+\tau$	$1+\tau$	τ	1	0

Table 12.1

$\cdot$	0	1	τ	$1+\tau$
0	0	0	0	0
1	0	1	τ	$1+\tau$
τ	0	τ	$1+\tau$	1
$1+\tau$	0	$1+\tau$	1	τ

Table 12.2

12.3 Algebra Closure

12.3 Algebra Closure

Theorem 12.5

Let E be an **extension field of** F. **The set of elements in** E that are **algebraic over** F **form a field.**

Proof (See page 361 of the textbook)

Corollary 12.1

The set of all **algebraic numbers forms a field**; that is, **the set of all complex numbers** that are **algebraic over** $\mathbb{Q}$ **makes up a field.**

Definition 12.6

Let E be a field extension of a field F. We define the **algebraic closure (代数的閉包)** of a field F in E **to be the field consisting of all elements in** E that are **algebraic** over F. A field F is **algebraically closed** if **every nonconstant polynomial in** $F[x]$ has a **root** in F.

12.3 Algebra Closure

Theorem 12.6 (Fundamental Theorem of Algebra)

The field of complex numbers is **algebraically closed**.

Review for Lecture 12

- Extension Fields (体の拡大)
- Simple Field
- Algebraic number (代数的数) and Transcendental number (超越数)
- Algebra Closure

Assignment

Please Check https://github.com/uoaworks/Applied-Algebra

References

[1] Thomas W. Judson etc. Abstract Algebra Theory and Applications, 2018
[2] D. S. Malik, John N. Mordeson, M.K. Sen, Introduction to Abstract Algebra, 2007
[3] **(おすすめ)** 松本 眞, 代数系への入門, http://www.math.sci.hiroshima-u.ac.jp/~m-mat/TEACH/daisu-nyumon2014.pdf
[4] Wikipedia
[5] Materials from internet.