Extension fields I

Sergei Silvestrov

Spring term 2011, Lecture 12

Abstract

Contents of the lecture.

Introduction to extension fields.

 Vector spaces.

Extension fields and Kronecker’s theorem

Definition 1. If $E$ is a field containing $F$ as a subfield, then $E$ is called a extension field of $F$.

Theorem 1 (Kronecker). If $F$ is a field and $f(x) \in F[x]$ is a nonconstant polynomial, then there exist an extension field $E$ of $F$ and an $\alpha \in E$ with $f(\alpha) = 0$.

Proof. If the degree of $f$ is 1, then $f(x)$ is linear and we can choose $E = F$. If the degree of $f$ is greater than 1, write $f(x) = p(x)g(x)$, where $p(x)$ is irreducible. The quotient ring $E = F[x]/\langle p(x) \rangle$ is a field. The natural map $\varphi(a) : E \mapsto F$ defined by $\varphi(a) = a + \langle p(x) \rangle$, is an isomorphism from $F$ to the subfield $F' = \{a + \langle p(x) \rangle : a \in F \}$ of $E$.

Put $\alpha = x + \langle p(x) \rangle \in E$. Let $p(x) = a_0 + a_1x + \cdots + a_{d-1}x^{d-1} + x^d$, where $a_i \in F$ for all $i$. In $E = F[x]/\langle p(x) \rangle$, we have

$$p(\alpha) = (a_0 + \langle p(x) \rangle) + (a_1 + \langle p(x) \rangle)\alpha + \cdots + (1 + \langle p(x) \rangle)\alpha^d$$

$$= (a_0 + \langle p(x) \rangle) + (a_1 + \langle p(x) \rangle)(x + \langle p(x) \rangle) + \cdots + (1 + \langle p(x) \rangle)(x + \langle p(x) \rangle)^d$$

$$= (a_0 + \langle p(x) \rangle) + (a_1x + \langle p(x) \rangle) + \cdots + (1x^d + \langle p(x) \rangle)$$

$$= a_0 + a_1x + \cdots + x^d + \langle p(x) \rangle$$

$$= p(x) + \langle p(x) \rangle = \langle p(x) \rangle,$$

because $p(x) \in \langle p(x) \rangle$. But $\langle p(x) \rangle = 0 + \langle p(x) \rangle$ is the zero element of $E = F[x]/\langle p(x) \rangle$, and so $\alpha$ is a root of $p(x)$. □
Example 1. The polynomial \( x^2 + 1 \in \mathbb{R}[x] \) is irreducible, and so \( K = \mathbb{R}[x]/\langle x^2 + 1 \rangle \) is a field extension. If \( \alpha \) is a root of \( x^2 + 1 \), then \( \alpha^2 = -1 \); moreover, every element of \( K \) has a unique expression of the form \( a + b\alpha \), where \( a, b \in \mathbb{R} \). Clearly, this is another construction of \( \mathbb{C} \).

### Algebraic and transcendental elements

**Definition 2.** Let \( E \) be an extension field of \( F \). An element \( \alpha \in E \) is **algebraic** over \( F \) if there is some nonzero polynomial \( f(x) \in F[x] \) having \( \alpha \) as a root; otherwise, \( \alpha \) is **transcendental** over \( F \).

**Example 2.** \( i \in \mathbb{C} \) is algebraic over \( \mathbb{Q} \) and over \( \mathbb{R} \). It is a nontrivial fact that \( \pi, e \in \mathbb{R} \) are transcendental over \( \mathbb{Q} \).

**Theorem 2.** Let \( E \) be an extension field of \( F \). An element \( \alpha \in E \) is transcendental over \( F \) if and only if the evaluation homomorphism \( \varphi_\alpha : F[x] \to E \) is a one-to-one map.

**Proof.**

1. The element \( \alpha \) is transcendental over \( F \) \iff
2. \( f(\alpha) \neq 0 \) for all nonzero \( f(x) \in F[x] \) \iff
3. \( \varphi_\alpha(f(x)) \neq 0 \) for all nonzero \( f(x) \in F[x] \) \iff
4. \( \ker(\varphi_\alpha) = \{0\} \) \iff
5. \( \varphi_\alpha \) is one-to-one.

\[ \square \]

### The irreducible polynomial for \( \alpha \) over \( F \)

**Theorem 3.** Let \( E \) be an extension field of \( F \) and let \( \alpha \in E \) be algebraic over \( F \). There exist a unique irreducible monic polynomial \( f(x) \in F[x] \) such that

1. \( f(\alpha) = 0 \).
2. If \( g(x) \in F[x] \) and \( g(\alpha) = 0 \), then \( f \) divides \( g \).

**Definition 3.** Let \( E \) be an extension field of \( F \) and let \( \alpha \in E \) be algebraic over \( F \). The polynomial described in Theorem 3 is called the **irreducible polynomial for \( \alpha \) over \( F \)** and is denoted by \( \text{irr}(\alpha, F) \). The degree of \( \text{irr}(\alpha, F) \) is the **degree of \( \alpha \) over \( F \)**, denoted by \( \deg(\alpha, F) \).
Example 3. \( \text{irr} (\sqrt{2}, \mathbb{Q}) = x^2 - 2 \) and \( \deg(\sqrt{2}, \mathbb{Q}) = 2 \). Similarly, \( \text{irr} (\sqrt{2}, \mathbb{Q}) = x^n - 2 \) and \( \deg(\sqrt{2}, \mathbb{Q}) = n \) for \( n \geq 2 \). Over \( \mathbb{R} \), the element \( \sqrt{2} \) is of degree 1, with minimal polynomial \( \text{irr}(\sqrt{2}, \mathbb{R}) = x - \sqrt{2} \).

Simple extensions

Definition 4. Let \( E \) be an extension field of \( F \) and let \( \alpha \in E \). The smallest subfield of \( E \) containing both \( F \) and \( \alpha \) is called the simple extension of \( F \) and is denoted by \( F(\alpha) \).

If \( \alpha \) is algebraic over \( F \), then \( F(\alpha) = \varphi_\alpha[F[x]] \). If \( \alpha \) is transcendental over \( F \), then \( F(\alpha) \) is the quotient field of \( \varphi_\alpha[F[x]] \).

Theorem 4. Let \( E \) be an extension field of \( F \) and let \( \alpha \in E \) be algebraic over \( F \). Let \( n = \deg(\alpha, F) \). Then

\[
F(\alpha) = \{ a_0 + \cdots + a_{n-1} \alpha^{n-1} : a_0, \ldots, a_{n-1} \in F \}.
\]

Example 4. Let \( F = \mathbb{Z}_2 \), let \( p(x) = x^2 + x + 1 \). There exist a simple extension field \( \mathbb{Z}_2(\alpha) \) of \( \mathbb{Z}_2 \) containing a zero \( \alpha \) of \( p(x) \). Then

\[
\mathbb{Z}_2(\alpha) = \{ a_0 + a_1 \alpha : a_0, a_1 \in \mathbb{Z}_2 \}
\]

which is a new field containing 4 elements.

Vector spaces

Definition 5. Let \( F \) be a field. A vector space over \( F \) is an additive abelian group \( V \) equipped with a scalar multiplication of each element \( \alpha \in V \) by each element \( a \in F \) on the left, such that for all \( a, b \in F \) and \( \alpha, \beta \in V \) the following is true

\[
\begin{align*}
\gamma_1: \quad & \alpha a \in V. \\
\gamma_2: \quad & a(b\alpha) = (ab)\alpha. \\
\gamma_3: \quad & (a + b)\alpha = a\alpha + b\alpha. \\
\gamma_4: \quad & a(\alpha + \beta) = a\alpha + a\beta. \\
\gamma_5: \quad & 1\alpha = \alpha.
\end{align*}
\]

The elements of \( V \) are vectors and the elements of \( F \) are scalars.
Examples of vector spaces

Example 5. The Cartesian product $F^n$ is a vector space over $F$ with scalar multiplication
\[ a(a_1, \ldots, a_n) = (aa_1, \ldots, aa_n). \]

Example 6. Let $E$ be an extension field of $F$. Then $E$ is a vector space over $F$. In particular, $\mathbb{R}$ is a $\mathbb{Q}$-vector space, $\mathbb{C}$ is a $\mathbb{R}$-vector space, $\mathbb{Q}(\sqrt{2})$ is a $\mathbb{Q}$-vector space.

Linear independence

Definition 6. Let $V$ be a vector space, and let $S \subseteq V$. The vectors of $S$ span or generate $V$ if for any $\beta \in V$ there exist $n \in \mathbb{Z}^+$, scalars $a_i \in F$ and vectors $\alpha_i \in S$ for $1 \leq i \leq n$ such that
\[ \beta = \sum_{i=1}^{n} a_i \alpha_i. \]
In other words, $\beta$ is a linear combination of the $a_i$.

Definition 7. A vector space $V$ is finite-dimensional if there is a finite subset $S \subseteq V$ whose vectors span $V$.

Example 7. The vectors $(1,0,\ldots,0)$, $(0,1,0,\ldots,0)$, \ldots, $(0,0,\ldots,1)$ span the finite-dimensional space $F^n$.

Example 8. Let $E$ be an extension field of $F$ and let $\alpha \in E$ be algebraic over $F$. Let $n = \deg(\alpha, F)$. Then the elements
\[ 1, \alpha, \ldots, \alpha^{n-1} \]
span $F(\alpha)$.

Definition 8. Let $V$ be a vector space, and let $S \subseteq V$. The vectors in $S$ are linearly independent, if for any $n \in \mathbb{Z}^+$, scalars $a_i \in F$ and distinct vectors $\alpha_i \in S$ for $1 \leq i \leq n$ we have
\[ \sum_{i=1}^{n} a_i \alpha_i = 0 \Leftrightarrow a_1 = a_2 = \cdots = a_n = 0. \]

Example 9. The vectors defined in Examples 5 and 6, are linearly independent.
Definition 9. Let $V$ be a vector space over a field $F$, and let $B \subset V$. The vectors in $B$ form a basis for $V$ over $F$ if they span $V$ and are linearly independent.

Example 10. The vectors defined in Examples 5 and 6, form a basis.

**Dimension**

**Theorem 5.** Every finite-dimensional vector space has a basis. Any two bases of a finite-dimensional vector space have the same number of elements.

This theorem remains true without the assumption that the vector space is finite dimensional.

Definition 10. If $V$ is a finite-dimensional vector space over $F$, then the number of elements in a basis is called the dimension of $V$ over $F$.

Example 11. $F^n$ is $n$-dimensional vector space over $F$.

Example 12. Let $E$ be an extension field of $F$ and let $\alpha \in E$ be algebraic over $F$. Then $F(\alpha)$ is $\deg(\alpha, F)$-dimensional space over $F$. 