Section 31 – Algebraic extensions

Instructor: Yifan Yang

Spring 2007

Vector spaces over a field

Definition

Let F be a field. A vector space over F is an additive group V, together with a scalar multiplication by elements of F, satisfying

- $a\alpha \in V$,
- $(ab)\alpha = a(b\alpha)$,
- $(a+b)\alpha = a\alpha + b\alpha$,
- $a(\alpha+\beta) = a\alpha + a\beta$,
- $1\alpha = \alpha$,

for all $a, b \in F$ and all $\alpha, \beta \in V$.

Lemma

Let E be an extension field of a field F. Then E is a vector space over F.

Linear independence and bases

Definition

Let V be a vector space over F. A set $\{\alpha_1, \ldots, \alpha_n\}$ is said to be linearly independent over F if $a_1\alpha_1 + \cdots + a_n\alpha_n = 0$ implies that $a_i = 0$ for all i. If a set of vectors is not linearly independent over F, then it is linearly dependent over F.

Definition

Let V be a vector space over F. A set of vectors $\{\alpha_i : i \in I\}$ is a basis for V over F if it is linearly independent and every vector in V is a finite linear combination of α_i with coefficients in F.

Basis for $F(\alpha)$

Theorem (30.23)

Let $E = F(\alpha)$ be a simple extension of a field F.

- *If α is algebraic over F with $\deg(\alpha, F) = n$, then $E = F(\alpha)$ is a finite-dimensional vector space over n, and a basis is given by $\{1, \alpha, \ldots, \alpha^{n-1}\}$.*
- *If α is not algebraic over F, then $E = F(\alpha)$ is an infinite-dimensional vector space over F.*

Proof.

- If α is algebraic over F, then Theorem 29.18 says that $\{1, \alpha, \ldots, \alpha^{n-1}\}$ is a basis for $F(\alpha)$.
- If α is transcendental over F, then the vectors $1, \alpha, \alpha^2, \ldots$ are linearly independent. Thus, $F(\alpha)$ is not finite-dimensional.

Algebraic extensions and finite extensions

Definition

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

Definition

If an extension field E of a field F is of finite dimension n as a vector space over F, then E is a finite extension of degree n over F. We let $[E : F]$ denote the degree of E over F.

Remark

The finiteness in the definition of a finite extension refers to the degree. It does not mean that the field E is a finite field. For instance, $\mathbb{Q}[i]$ is a finite extension of degree 2 of $\mathbb{Q}$, but it has infinitely many elements.

Finite extension $\Rightarrow$ algebraic extension

Theorem (31.3)

A finite extension E of a field F is an algebraic extension.

Proof.

Let $\alpha \in E$. Assume that $[E : F] = n$. Then the $n + 1$ vectors $1, \alpha, \ldots, \alpha^{n+1}$ are linearly dependent over F. Thus, there are elements a_i, not all zero, such that $a_0 + a_1\alpha + \cdots + a_n\alpha^n = 0$, that is, α is algebraic over F. $\square$

Theorem (31.4)

If E is a finite extension of a field F, and K is a finite extension of E, then K is a finite extension of F and
$[K : F] = [K : E][E : F]$.

Proof of Theorem 31.4. Let $\{\alpha_1, \ldots, \alpha_m\}$ be a basis for E over F, and $\{\beta_1, \ldots, \beta_n\}$ be a basis for K over E. It suffices to prove that

- every element of K is a linear combination of $\alpha_i\beta_j$, $i = 1, \ldots, m$, $j = 1, \ldots, n$, with coefficients in F, and
- $\alpha_i\beta_j$ are linearly independent over F.

Proof of Theorem 31.4, continued

- Let $\gamma \in K$. Then $\gamma = \sum_{i=1}^{m} b_i \alpha_i$ for some $b_i \in E$ since $\{\alpha_i\}$ is a basis for K over E. Each b_i is a linear combination $b_i = \sum_{j=1}^{n} c_{ij} \beta_j$ over F since $\{\beta_j\}$ is a basis for E over F. Then $\gamma = \sum_{i,j} c_{ij} \alpha_i \beta_j$. Thus, every element of K is a linear combination of $\alpha_i \beta_j$ over F.
- Now suppose that c_{ij} are elements in F such that $\sum_{i,j} c_{ij} \alpha_i \beta_j = 0$. Write it in the form

$$\sum_{i=1}^{m} \left(\sum_{j=1}^{n} c_{ij} \beta_j \right) \alpha_i = 0,$$

where $\sum_{j=1}^{n} c_{ij} \beta_j$ are elements of E. Since α_i are linearly independent over E, $\sum_{j=1}^{n} c_{ij} \beta_j = 0$ for each i. Then $c_{ij} = 0$ for all j since β_j are linearly independent over F.

Degrees of field extensions

Corollary (31.6)

If $F_1 \leq F_2 \leq \ldots \leq F_n$ is a series of finite extension of fields, then $[F_n : F_1] = [F_n : F_{n-1}] \ldots [F_2 : F_1]$.

Corollary (31.7)

Assume that E is an extension field of F and $\alpha \in E$ is algebraic over F. If $\beta \in F(\alpha)$, then $\deg(\beta, F)$ divides $\deg(\alpha, F)$.

Example

Using Corollary 31.7, it is easy to see that the field $\mathbb{Q}[\sqrt{2}]$ does not contain $\sqrt[3]{2}$ since $\deg(\sqrt[3]{2}, \mathbb{Q}) = 3$ does not divide $\deg(\sqrt{2}, \mathbb{Q}) = 2$.

Example

Problem. Find the degree and the irreducible polynomial for $\sqrt{2}+\sqrt{3}$ over $\mathbb{Q}[\sqrt{3}]$.

Solution.

- Let $\alpha = \sqrt{2}+\sqrt{3}$. It is clear that α satisfies $(x-\sqrt{3})^2 = 2$, i.e., $x^2 - 2\sqrt{3}x + 1 = 0$.
- Thus, $[\mathbb{Q}(\alpha) : \mathbb{Q}(\sqrt{3})] \leq 2$. Then $[\mathbb{Q}(\alpha) : \mathbb{Q}(\sqrt{3})] = 1$ or 2.
- If $[\mathbb{Q}(\alpha) : \mathbb{Q}(\sqrt{3})] = 1$, then $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{3})$ and $\alpha \in \mathbb{Q}(\sqrt{3})$.
- This implies $\sqrt{2} = a + b\sqrt{3}$ for some $a, b \in \mathbb{Q}$.
- We have $\text{irr}(\sqrt{2}, \mathbb{Q}) = x^2 - 2$ and $\text{irr}(a+b\sqrt{3}, \mathbb{Q}) = x^2 - 2ax + (a^2 - 3b^2)$.
- We find $a = 0$ and $3b^2 = 2$, which is impossible when $b \in \mathbb{Q}$.
- Thus, $[\mathbb{Q}(\alpha) : \mathbb{Q}(\sqrt{3})] = 2$ and $\text{irr}(\alpha, \mathbb{Q}(\sqrt{3})) = x^2 - 2\sqrt{3}x + 1$.

Determining $\mathrm{irr}(\beta, F)$ for $\beta \in F(\alpha)$

Problem. Let $E = F(\alpha)$ be a finite extension of a field F. Given $\beta \in F(\alpha)$, find $\mathrm{irr}(\beta, F)$ (and thus also $\deg(\beta, F)$).

Idea. Assume that $\deg(\alpha, F) = n$.

- Recall that $1, \alpha, \ldots, \alpha^{n-1}$ is a basis for $F(\alpha)$ over F.
- Since $\beta \in F(\alpha)$, this implies that $\beta\alpha^j$ is again a linear combination of α^j.
- In other words, we have

$$\beta \begin{pmatrix} 1 \\ \vdots \\ \alpha^{n-1} \end{pmatrix} = M \begin{pmatrix} 1 \\ \vdots \\ \alpha^{n-1} \end{pmatrix}$$

  for some $n \times n$ matrix over F.
- Thus, β is a zero of the characteristic polynomial of M.
- We then factor the characteristic polynomial to get $\mathrm{irr}(\beta, F)$.

Example

Problem. Find the irreducible polynomial of $\sqrt[3]{2^2} + \sqrt[3]{2} - 1$ over $\mathbb{Q}$.

Solution. Set $\alpha = \sqrt[3]{2}$ and $\beta = \alpha^2 + \alpha - 1$.

- We have $\alpha^3 - 2 = 0$. Thus,

$$\begin{aligned}\beta 1 &= -1 + \alpha + \alpha^2,\\ \beta\alpha &= \alpha^3 + \alpha^2 - \alpha = 2 - \alpha + \alpha^2,\\ \beta\alpha^2 &= \alpha^4 + \alpha^3 - \alpha^2 = 2 + 2\alpha - \alpha^2.\end{aligned}$$

- Thus, β is a zero of the characteristic polynomial of $\begin{pmatrix} -1 & 1 & 1 \\ 2 & -1 & 1 \\ 2 & 2 & -1 \end{pmatrix}$.
- We find β is a zero of $x^3 + 3x^2 - 3x - 11$.

Example

Problem. Let α be a zero of $x^4 - 10x^2 + 1$. Find the irreducible polynomial for $\beta = \alpha^3 - 9\alpha$.

Solution.

- We have

$$\begin{aligned}
\beta 1 &= 0 - 9\alpha + 0\alpha^2 - \alpha^3 \\
\beta\alpha &= \alpha^4 - 9\alpha^2 = (10\alpha^2 - 1) - 9\alpha^2 = -1 + 0\alpha + \alpha^2 + 0\alpha^3 \\
\beta\alpha^2 &= \alpha^5 - 9\alpha^3 = 0 - \alpha + 0\alpha^2 + \alpha^3 \\
\beta\alpha^3 &= -\alpha^2 + \alpha^4 = -1 + 0\alpha + 9\alpha^2 + 0\alpha^3.
\end{aligned}$$

- Thus, β is a zero of the characteristic polynomial of

$$\begin{pmatrix} 0 & -9 & 0 & -1 \\ -1 & 0 & 1 & 0 \\ 0 & -1 & 0 & 1 \\ -1 & 0 & 9 & 0 \end{pmatrix}.$$

Example, continued

- We find β is zero of $x^4 - 18x^2 + 80$.
- This time, $x^4 - 18x^2 + 80 = (x^2 - 8)(x^2 - 10)$ is not irreducible.
- To determine which factor is the irreducible polynomial for β over $\mathbb{Q}$, we compute β^2.
- We find $\beta^2 = (\alpha^3 - 9\alpha)^2 = \alpha^6 - 18\alpha^4 + 81\alpha^2$.
- Using the division algorithm, we find that this is equal to $(\alpha^2 - 8)(\alpha^4 - 10\alpha^2 + 1) + 8 = 8$.
- Therefore, $\mathrm{irr}(\beta, \mathbb{Q}) = x^2 - 8$, i.e., β is either $2\sqrt{2}$ or $-2\sqrt{2}$. (The exact value of β depends on which zero of $x^4 - 10x^2 + 1$ we take as α.)

In-class exercises

Let $\alpha = \sqrt[3]{2}$.

1. Find irr$(\alpha^2 - \alpha, \mathbb{Q})$.
2. Find irr$(\alpha^2 + 1, \mathbb{Q})$.

Let α be a zero of $x^3 + x + 1 \in \mathbb{Z}_2[x]$.

1. Find irr$(\alpha^2 + 1, \mathbb{Z}_2)$.
2. Find irr$(\alpha^2 + \alpha, \mathbb{Z}_2)$.

Algebraic closure

Lemma

Let E be an extension field of a field F. If $\alpha, \beta \neq 0 \in E$ are algebraic over F, then so are $\alpha + \beta$ and α/β.

Proof.

- In view of Theorem 31.3, it suffices to prove that $F(\alpha, \beta) = F(\alpha)(\beta)$ is a finite extension of F.
- Regarding $f(x) = \text{irr}(\beta, F)$ as a polynomial in $F(\alpha)[x]$, we see that β is algebraic over $F(\alpha)$.
- Then $[F(\alpha, \beta) : F] = [F(\alpha)(\beta) : F(\alpha)][F(\alpha) : F] < \infty$.
- Therefore, $F(\alpha, \beta)$ is a finite extension of F. $\square$

Algebraic closure

Corollary (31.12)

Let E be an extension field of F. Then the set

$$\overline{F}_E = \{\alpha \in E : \ \alpha \text{ is algebraic over } F\}$$

is a subfield of E, the algebraic closure of F in E.

Corollary (31.13)

The set $\overline{\mathbb{Q}}$ of all algebraic numbers forms a field.

Algebraically closed

Definition

A field F is algebraically closed if every nonconstant polynomial in $F[x]$ has a zero in F.

Remarks

- An algebraically closed field F can be characterized by the property that every polynomial $f(x)$ in $F[x]$ factors into a product of linear factors over F. (Theorem 31.15.)
- This means that if F is algebraically closed, then we will not get anything new by joining zeros of polynomials in $F[x]$ to F. (Corollary 31.16.)

Algebraic closure of a field

Definition

An algebraic closure $\overline{F}$ of a field F is an algebraic extension of F that is algebraically closed.

Remark

An algebraic closure of a field F can be thought of as the largest field one may obtain by algebraic means.

Example

- The field $\mathbb{C}$ is an algebraic closure of $\mathbb{R}$. (Fundamental theorem of algebra, Theorem 31.18.)
- The set $\overline{\mathbb{Q}}$ of algebraic numbers is an algebraic closure of $\mathbb{Q}$. (Proved in the next page.)

Algebraic closure of $\mathbb{Q}$

Theorem

The set $\overline{\mathbb{Q}}$ of algebraic numbers is an algebraic closure of $\mathbb{Q}$.

Proof.

- We have proved earlier that if α and β are algebraic over $\mathbb{Q}$, then so are $\alpha + \beta$ and α/β. In other words, $\overline{\mathbb{Q}}$ is an algebraic extension of $\mathbb{Q}$.
- It remains to prove that $\overline{\mathbb{Q}}$ is algebraically closed. That is, if α is a zero of $f(x) \in \overline{\mathbb{Q}}[x]$, then α is in $\overline{\mathbb{Q}}$.
- Assume that α is a zero of $a_n x^n + \cdots + a_0$, where a_i are algebraic numbers. We need to show that $[\mathbb{Q}(\alpha) : \mathbb{Q}] < \infty$.

Proof of Theorem, continued

- We have

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] \leq [\mathbb{Q}(\alpha, a_0, \ldots, a_n) : \mathbb{Q}]$$
$$= [\mathbb{Q}(\alpha, a_0, \ldots, a_n) : \mathbb{Q}(a_0, \ldots, a_n)][\mathbb{Q}(a_0, \ldots, a_n) : \mathbb{Q}].$$

- Here $[\mathbb{Q}(\alpha, a_0, \ldots, a_n) : \mathbb{Q}(a_0, \ldots, a_n)] \leq n$.
- Also using the same argument as in the proof of an earlier lemma (with induction), we find $[\mathbb{Q}(a_0, \ldots, a_n) : \mathbb{Q}] < \infty$.
- Therefore, $[\mathbb{Q}(\alpha) : \mathbb{Q}] < \infty$ and α is algebraic over $\mathbb{Q}$. $\square$

Algebraic closure of a field

Theorem (31.17)

Every field has an algebraic closure.

Remark

1. The proof uses Zorn's lemma, which is equivalent to the axiom of choice.
2. A field may have several algebraic closures, but they are all isomorphic.

Homeworks

Problems 8, 10, 12, 24, 26, 28, 29, 30 of Section 31.