Galois Field
Lecture 2

Indah Emilia Wijayanti

Department of Mathematics Universitas Gadjah Mada, Yogyakarta, Indonesia

CIMPA Research School on
Group Actions in Arithmetic and Geometry
Universitas Gadjah Mada, Yogyakarta 17-28 February 2020

Outline

1. Algebraic Extensions

2. Splitting Fields

Preliminaries

- If K is a field containing the field F, then K is said to be an extension field of F.
- We denote it as K/F.
- If K/F is any extension of fields, then K is a vector space of F.
- The degree of a field extension K/F is the dimension of K as a vektor space over F, denoted by $[K : F] = \dim_F(K)$.

Algebraic extension

Let F be a field and K an extension of F, $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in F[x]$. For any $\gamma \in K$, if it satisfies

$$f(\gamma) := a_0 + a_1 \gamma + \cdots + a_n \gamma^n = 0,$$

we call it root of $f(x)$.

Proposition

Let F be a field and let $p(x) \in F[x]$ be an irreducible polynomial. Then there exists a field K containing an isomorphic copy of F in which $p(x)$ has a root

Definition

The element α of K is said to be algebraic over F if α is a root of some nonzero polynomial $f(x) \in F[x]$. The extension K/F is said to be algebraic if every element of K is algebraic over F.

- If α is algebraic over a field F, then it is algebraic over any extension field L of F.
- Example : $f(x) = x^2 + 1 \in \mathbb{Q}[x]$. $i = \sqrt{-1} \in \mathbb{C}$ is a root of $f(x)$, so it is algebraic over $\mathbb{Q}$.

Minimal polynomial (1)

Proposition

Let α be algebraic over F.

1. There is a unique monic irreducible polynomial $m_{\alpha,F}(x) \in F[x]$ which has α as a root.
2. A polynomial $f(x) \in F[x]$ has α as a root if and only if $m_{\alpha,F}(x)$ devides $f(x)$ in $F[x]$.

Minimal polynomial (2)

Definition

The polynomial $m_{\alpha,F}(x)$ or $m_\alpha(x)$ is called the minimal polynomial for α over F. The degree of $m_\alpha(x)$ is called the degree of α.

- The minimal polynomial for $\sqrt{2}$ over $\mathbb{Q}$ is $x^2 - 2$ and $\sqrt{2}$ is of degree 2 over $\mathbb{Q}$, $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$.
- The minimal polynomial for $\sqrt[3]{2}$ over $\mathbb{Q}$ is $x^3 - 2$ and $\sqrt[3]{2}$ is of degree 3 over $\mathbb{Q}$, $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$.

Proposition

Let α be algebraic over F and $F(\alpha)$ the field generated by α over F. Then

$$F(\alpha) \simeq F[x]/ < m_\alpha(x) >$$

and in particular $[F(\alpha) : F] = \deg(m_\alpha(x)) = \deg\, \alpha$.

Proposition

The element α is algebraic over F if and only if $F(\alpha)/F$ is finite. Moreover, if the extension K/F is finite, then it is algebraic.

Proposition

Let $F \subseteq K \subseteq L$ be fields. Then $[L : F] = [L : K][K : F]$.

Corollary

Suppose L/F is a finite extension and let K be any subfield of L containing F, $F \subseteq K \subseteq L$. Then $[K : F]$ is divides $[L : F]$.

Example

- Consider $\sqrt[6]{2}$ and $[\mathbb{Q}(\sqrt[6]{2}) : \mathbb{Q}] = 6$.
- Since $(\sqrt[6]{2})^3 = \sqrt{2}$, we get the minimal polynomial for $\sqrt[6]{2}$ in $\mathbb{Q}(\sqrt{2})$ is $f(x) = x^3 - \sqrt{2} \in \mathbb{Q}(\sqrt{2})[x]$.
- Hence $\mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt[6]{2})$ and $[\mathbb{Q}(\sqrt[6]{2}) : \mathbb{Q}(\sqrt{2})] = 3$.
- Together we have

$$\overbrace{\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt[6]{2})}^{6}$$

and

$$\underbrace{\mathbb{Q} \subset \mathbb{Q}(\sqrt{2})}_{2}, \quad \underbrace{\mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt[6]{2})}_{3}.$$

Example

- Consider the field $\mathbb{Q}(\sqrt{2}, \sqrt{3})$, which is generated by $\sqrt{2}$ and $\sqrt{3}$ over $\mathbb{Q}$.
- Since $x^2 - 3$ is irreducible in $\mathbb{Q}(\sqrt{2})$, $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})] = 2$.
- Hence $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$.

The composite field

Definition

Let K_1 and K_2 be subfields of a field K. The composite field of K_1 and K_2, denoted by K_1K_2, is the smallest subfield K containing both K_1 and K_2.

- Find composite of the two fields $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt[3]{2})$.
- Consider that $\sqrt[6]{2}$ has the polynomial minimal both in $\mathbb{Q}(\sqrt{2})[x]$ and $\mathbb{Q}(\sqrt[3]{2})[x]$.
- Conversely, any field containing $\sqrt{2}$ and $\sqrt[3]{2}$ contains $\sqrt[6]{2}$ too.
- Hence $\mathbb{Q}(\sqrt{2})\mathbb{Q}(\sqrt[3]{2}) = \mathbb{Q}(\sqrt[6]{2})$.

Splitting fields

Definition

The extension field K of F is called a splitting field for the polynomial $f(x) \in F[x]$ if $f(x)$ factors completely into linear factors in $K[x]$ and $f(x)$ does not factor completely into linear factors over any proper subfield of K containing F.

- If $f(x)$ is of degree n, then $f(x)$ has at most n roots in F.
- If $f(x)$ is of degree n, it has precisely n roots in F if and only if $f(x)$ splits completely in $F[x]$.

Existence of splitting field

Theorem

1. For any field F, if $f(x) \in F[x]$, then there exists an extension K of F which is a splitting field for $f(x)$.
2. Any two splitting fields for $f(x) \in F[x]$ over F are isomorphic.

- The splitting field for $x^2 - 2$ over $\mathbb{Q}$ is just $\mathbb{Q}(\sqrt{2})$, since two roots are $\sqrt{2}$ and $-\sqrt{2}$ in $\mathbb{Q}(\sqrt{2})$.
- The splitting field for $(x^2 - 2)(x^2 - 3)$ over $\mathbb{Q}$ is $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ generated by $\sqrt{2}$ and $\sqrt{3}$, since four roots are $\sqrt{2}, -\sqrt{2}, \sqrt{3}, -\sqrt{3}$. Moreover, we know that

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt{2}, \sqrt{3}),$$

- Let F be a field and $f(x) \in F[x]$ be a polynomial with leading cofficient a_n.
- Over a splitting field for $f(x)$ we have the factorization :

$$f(x) = a_n(x - \alpha_1)^{n_1}(x - \alpha_2)^{n_2} \cdots (x - \alpha_k)^{n_k}$$

  where $\alpha_1, \alpha_2, \ldots, \alpha_k$ are distinct elements of the splitting field and $n_i \geq 1$ for all i.
- Recall that α_i is called a multiple root if $n_i > 1$ and is called a simple root if $n_i = 1$.
- The integer n_i is called the multiplicity of α_i.

Separable

Definition

A polynomial over F is called separable if it has no multiple roots. A polynomial which is not separable is called inseparable.

- Polynomial $x^2 - 2$ is separable over $\mathbb{Q}$ since its two roots $\sqrt{2}$ and $-\sqrt{2}$ are distinct.
- Polynomial $(x^2 - 2)^3$ is inseparable over $\mathbb{Q}$ since its roots $\sqrt{2}$ and $-\sqrt{2}$ has multiplicity 3.

Proposition

A polynomial $f(x)$ has a multiple root α if and only if α is also a root of $D_x f(x)$. In particular, $f(x)$ is separable if and only if $(f(x), D_x f(x)) = 1$.

- The polynomial $x^{p^n} - x$ over F_p has derivatif $p^n x^{p^n - 1} - 1 = -1$, since the field has characteristic p. The derivative has no roots, so the polynomial has no multiple roots, hence it is separable.
- For example $x^4 - x$ over F_3 is separable.

- The polynomial $x^n - 1$ has derivatif nx^{n-1}. Over any field of characteristic not dividing n this polynomial has only the root 0, which is not a root of $x^n - 1$. Hence $x^n - 1$ is separable and there are n distinct n^{th} root of unity.

Proposition

Every irreducible polynomial over a field of characteristic 0 is separable. A polynomial over such a field is separable if and only if it is the product of distinct irreducible polynomials.

Proposition

Every irreducible polynomial over a finite field F is separable. A polynomial in $F[x]$ is separable if and only if it is the product of distinct irreducible polynomials in $F[x]$.