Galois Field
Lecture 3

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

Splitting Fields of $x^n - 1$

- Consider the splitting field of the polynomial $x^n - 1$ over $\mathbb{Q}$. The roots of this polynomial are called the n^{th} roots of unity.
- Every nonzero complex number $a + bi \in \mathbb{C}$ can be written uniquely in term of polar coordinate

$$re^{i\theta} = r(\cos\theta + i\sin\theta), \quad r > 0, 0 \le \theta < 2\pi.$$

- There are n distinct solutions of $x^n = 1$ in $\mathbb{C}$, namely

$$e^{\frac{2\pi ki}{n}} = \cos(\frac{2\pi k}{n}) + i\sin(\frac{2\pi k}{n}), \quad k = 0, 1, \ldots, n-1.$$

Splitting Fields of $x^n - 1$ (Continued)

- In fact these are all n^{th} roots of unity, since

$$(e^{\frac{2\pi ki}{n}})^n = e^{\frac{2\pi ki}{n}n} = e^{2\pi ki} = 1.$$

- Hence $\mathbb{C}$ contains a splitting field for $x^n - 1$.
- The splitting field for $x^n - 1$ over $\mathbb{Q}$ is viewed as the field generated by $e^{\frac{2\pi ki}{n}}$ in $\mathbb{C}$, where $k = 0, 1, \ldots, n-1$.

Remark

In any abstract splitting field $K/\mathbb{Q}$ for $x^n - 1$, the collection of n^{th} roots of unity form a (cyclic) group under multiplication, since if $\alpha^n = 1$, $\beta^n = 1$, then $(\alpha\beta)^n = 1$.

Definition

A generator of the cyclic group of all n^{th} roots of unity is called a primitive n^{th} root.

- Let ξ_n denote a primitive n^{th} roots of unity. The other primitive n^{th} roots of unity are the elements ξ_n^a, where $1 \leq a < n$ is an integer relative prime to n.
- These other primitive n^{th} roots of unity are the other generators for a cyclic group of order n.
- There are precisely $\varphi(n)$ primitive n^{th} roots of unity, $\varphi(n)$ denotes the Euler φ-function.

Example

- Over $\mathbb{C}$, let $\xi_n = e^{2\pi i/n}$ the first n^{th} roots of unity. Then all the other roots of unity are

$$\xi_n^k = e^{2\pi k i/n}$$

- The primitive roots of unity in $\mathbb{C}$ for some small values of n are:

$$\begin{aligned} \xi_1 &= 1; \quad \xi_2 = -1; \\ \xi_3 &= \frac{-1 + i\sqrt{3}}{2}; \quad \xi_4 = i; \end{aligned}$$

The splitting field of $x^n - 1$ over $\mathbb{Q}$ is the field $\mathbb{Q}(\xi_n)$.

Definition

The field $\mathbb{Q}(\xi_n)$ is called the cyclotomic field of n^{th} roots of unity.

- If $n = p$, a prime, then $x^p - 1 = (x-1)(x^{p-1} + x^{p-2} + \cdots + x + 1)$.
- Since $\xi_p \neq 1$, it is a root of polynomial

$$\phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + x + 1,$$

which is irreducible.

Cyclotomic Extensions

- $\phi_p(x)$ the minimal polynomial of ξ_p over $\mathbb{Q}$ and $[\mathbb{Q}(\xi_p) : \mathbb{Q}] = p - 1$.
- In general, $[\mathbb{Q}(\xi_n) : \mathbb{Q}] = \varphi(n)$.
- Later, we will use the property :

$$\begin{aligned} \mathrm{Gal}(\mathbb{Q}(\xi_n) : \mathbb{Q}) &\simeq (\mathbb{Z}/\mathbb{Z}_n)^* \\ \sigma_a &\mapsto a \ mod \ n, \end{aligned}$$

where $\sigma_a(\xi_n) = \xi_n^a$.

- Let μ_n denote the group of n^{th} roots of unity over $\mathbb{Q}$, i.e.

$$\mu_n = \{\xi_0, \xi_1, \ldots, \xi_{n-1}\}.$$

- Then $\mathbb{Z}_n \simeq \mu_n$, by $a \mapsto (\xi_n)^a$ for a fixed primitive n^{th} roots of unity.
- If d is a divisor of n and ξ is a d^{th} root of unity, then ξ is also an n^{th} root of unity since $\xi^n = (\xi^d)^{n/d} = 1$.
- Hence $\mu_d \subseteq \mu_n, \quad \forall d \mid n$.
- Conversely, the order of any element of the group μ_n is a divisor of n so that if ξ is an n^{th} root of unity which is also a d^{th} root of unity for some smaller d, then $d \mid n$.

Automorphism of K

Let K be a field.

Definition

- An isomorphism σ of K is called an automorphism of K.The collection of automorphisms of K is denoted by $\mathrm{Aut}(K)$.
- An automorphism $\sigma \in \mathrm{Aut}(K)$ is said to fix an element $\alpha \in K$ if $\sigma\alpha = \alpha$.
- If F is a subset of K, then an automorphism σ is said to fix F if it fixes all the elements of F, i.e. $\sigma|_F = id_F$.

Definition

Let K/F be an extension of field. We denote $\mathrm{Aut}(K/F)$ as the collection of automorphisms of K which fix F, i.e.

$$\mathrm{Aut}(K/F) = \{\sigma : K \to K \mid \sigma|_F = id_F\}.$$

- Any automorphism σ of a field K fixes its prime subfield, since $\sigma(1) = 1$ and $\sigma(0) = 0$.
- If F is the prime subfield of K, then $\mathrm{Aut}(K) = \mathrm{Aut}(K/F)$, since every automorphism of K automatically fixes F.

Proposition

$\mathrm{Aut}(K)$ is a group under composition and $\mathrm{Aut}(K/F)$ is a subgroup.

Proposition

Let K/F be a field extension and let $\alpha \in K$ be algebraic over F. Then for any $\sigma \in \mathrm{Aut}(K/F)$, $\sigma\alpha$ is a root of the minimal polynomial for α over F.

- $\mathrm{Aut}(K/F)$ permutes the roots of irreducible polynomials.
- Any polynomial with coefficients in F having α as a root also has $\sigma\alpha$ as a root.

Example : Finding $\mathrm{Aut}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$

- Let $K = \mathbb{Q}(\sqrt{2})$. Since $\mathbb{Q}$ is the prime subfield of $\mathbb{Q}(\sqrt{2})$,
$$\mathrm{Aut}(\mathbb{Q}(\sqrt{2})) = \mathrm{Aut}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}),$$
- If $\tau \in \mathrm{Aut}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$, then
$$\tau(\sqrt{2}) = \sqrt{2} \quad \text{or} \quad \tau(\sqrt{2}) = -\sqrt{2},$$
since there are two roots of the minimal polynomial $x^2 - 2$ over $\mathbb{Q}$.
- Since τ fixes $\mathbb{Q}$,
$$\begin{aligned} \tau(a + b\sqrt{2}) &= a + b\sqrt{2}, \text{ or} \\ \tau(a + b\sqrt{2}) &= a - b\sqrt{2}. \end{aligned}$$

Finding $\mathrm{Aut}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$ (continued)

- The map $\iota : \sqrt{2} \mapsto \sqrt{2}$ is the identity automorphism.
- The map $\sigma : \sqrt{2} \mapsto -\sqrt{2}$ is the isomorphism.
- Hence

$$\mathrm{Aut}(\mathbb{Q}(\sqrt{2})) = \mathrm{Aut}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) = \{\iota, \sigma\} \simeq \mathbb{Z}_2,$$

a cyclic group of order 2 generated by σ.

We have associated to each field extension K/F a group $\mathrm{Aut}(K/F)$, the group of automorphisms of K which fix F.

Proposition

Let H be a subgroup of $\mathrm{Aut}(K/F)$. Then the collection F of elements of K fixed by all the elements of H is a subfield of K.

Definition

Let H be a subgroup of automorphisms of K, $\mathrm{Aut}(K)$. The subfield E of K fixed by all elements of H is called the fixed field of H.

- Suppose $K = \mathbb{Q}(\sqrt{2})$ and consider $\mathrm{Aut}(\mathbb{Q}(\sqrt{2})) = \{\iota, \sigma\}$.
- The fixed field of $\mathrm{Aut}(\mathbb{Q}(\sqrt{2}))$ will be the set of elements of $\mathbb{Q}(\sqrt{2})$ with $\sigma(a + b\sqrt{2}) = a + b\sqrt{2}$.
- The equation $a + b\sqrt{2} = a - b\sqrt{2}$ is true for $b = 0$, so the fixed field of $\mathrm{Aut}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$ is just $\mathbb{Q}$.

Proposition

Let E be the splitting field over F of the polynomial $f(x) \in F[x]$. Then $|\mathrm{Aut}(E/F)| \leq [E : F]$. If $f(x)$ is separable over F, then $|\mathrm{Aut}(E/F)| = [E : F]$.

- Consider a simple extension $E = F(\alpha)$, and let $p(x)$ be a polynomial in $F[x]$ having α as a root.
- If α is the only root of $p(x)$ in E, then $|\mathrm{Aut}(E/F)| = [E : F] = 1$.
- For example, $\sqrt[3]{2}$ denote the real cube root of 2, then $|\mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})| = 1$.

Separable extension

Definition

An algebraic extension E/F is separable if the minimum polynomial of every element of E is separable; otherwise it is inseparable.

- An algebraic extension E/F is separable if every irreducible polynomial in $F[x]$ having a root in E is separable.
- Let $p(X)$ be an irreducible polynomial of degree m in $F[x]$. If E/F is separable, then roots of $p(x)$ are distinct.

- Example : The polynomial $x^3 - 2$ has one real root $\sqrt[3]{2}$ and two nonreal roots in $\mathbb{C}$. Therefore the extension $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is separable.

Definition

Let K/F be a finite extension.

- K is said to be Galois over F and K/F is a Galois extension if K is normal, separable and finite over F.
- If K/F is Galois the group $\mathrm{Aut}(K/F)$ is called the Galois group of K/F, denoted by $\mathrm{Gal}(K/F)$.

Corollary

If K is the splitting field over F of a separable polynomial $f(x)$, then K/F is Galois.

Necessary and sufficient conditions for Galois extension

Theorem

For an extension K/F, the following statements are equivalent:

1. K is Galois over F;
2. K is the splitting field of a separable polynomial $p(x) \in F[x]$;
3. The elements of F are fixed by all $\sigma \in \mathrm{Aut}(K)$;
4. $|\mathrm{Aut}(K/F)| = [K : F]$.

Definition

If $f(x)$ is a separable polynomial over F, then the Galois group of $f(x)$ over F is the Galois group of the splitting field of $f(x)$ over F.

- The extension $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ is Galois with Galois group $\mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) = \{\iota, \sigma\} \simeq \mathbb{Z}_2$.
- The extension $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is not Galois since its group automorphisms is only of order 1.

Example : Finding $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3}))$

- The extension $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ is Galois over $\mathbb{Q}$ since it is the splitting field of the polynomial $(x^2 - 2)(x^2 - 3)$.
- The only possibility for automorphisms are maps:

$$
\begin{aligned}
\iota &: \sqrt{2} \mapsto \sqrt{2} \text{ and } \sqrt{3} \mapsto \sqrt{3}; \\
\sigma &: \sqrt{2} \mapsto -\sqrt{2} \text{ and } \sqrt{3} \mapsto \sqrt{3}; \\
\tau &: \sqrt{2} \mapsto \sqrt{2} \text{ and } \sqrt{3} \mapsto -\sqrt{3}; \\
\theta &: \sqrt{2} \mapsto -\sqrt{2} \text{ and } \sqrt{3} \mapsto -\sqrt{3}.
\end{aligned}
$$

Example : Finding $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3}))$ (continued)

- Since the Galois group is of order 4, all these elements are in fact automorphisms of $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ over $\mathbb{Q}$.
- Consider the automorphisms :

$$\begin{aligned} \sigma &: \sqrt{2} \mapsto -\sqrt{2} \;\text{ and } \sqrt{3} \mapsto \sqrt{3} \\ \tau &: \sqrt{2} \mapsto \sqrt{2} \;\text{ and } \sqrt{3} \mapsto -\sqrt{3}. \end{aligned}$$

- Then consider that

$$\sigma(\sqrt{6}) = \sigma(\sqrt{2}\sqrt{3}) = \sigma(\sqrt{2})\sigma(\sqrt{3}) = -\sqrt{2}\sqrt{3} = -\sqrt{6}.$$

Example : Finding $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3}))$ (continued)

- Hence, we have explicitely

$$\begin{aligned} \sigma &: a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \mapsto a - b\sqrt{2} + c\sqrt{3} - d\sqrt{6}; \\ \tau &: a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \mapsto a + b\sqrt{2} - c\sqrt{3} - d\sqrt{6}. \end{aligned}$$

- Then $\sigma^2(\sqrt{2}) = \sqrt{2}$ and $\sigma^2(\sqrt{3}) = \sqrt{3}$, or $\sigma^2 = id$.
- Similarly, $\tau^2 = id$.

Example : Finding $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3}))$ (continued)

- The automorphism $\sigma\tau$ can be computed as:

$$\begin{aligned}
\sigma\tau(\sqrt{2}) &= \sigma(\tau(\sqrt{2})) = \sigma(\sqrt{2}) = -\sqrt{2}; \\
\sigma\tau(\sqrt{3}) &= \sigma(\tau(\sqrt{3})) = \sigma(-\sqrt{3}) = -\sqrt{3}.
\end{aligned}$$

- Hence $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}) = \{1, \sigma, \tau, \sigma\tau\}$.
- It is isomorphic to the Klein 4-group.

Example Subgroup of $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})$

- Each subgroup H in $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})$ corresponds to a subfield K of E.

subgroup	fixed field
$\{1\}$	$\mathbb{Q}(\sqrt{2}, \sqrt{3})$
$\{1, \sigma\}$	$\mathbb{Q}(\sqrt{3})$
$\{1, \tau\}$	$\mathbb{Q}(\sqrt{2}))$
$\{1, \sigma, \tau\}$	$\mathbb{Q}(\sqrt{6})$
$\{1, \sigma, \tau, \sigma\tau\}$	$\mathbb{Q}$

Fundamental Theorem of Galois Theory

Let K/F be a Galois extension and $G = \mathrm{Gal}(K/F)$.
There is a bijection :

$$\begin{aligned} \{E \mid F \subset E \subset K\} &\leftrightarrow \{H \mid H \subset G\} \\ E &\mapsto \{\sigma \in G \mid \sigma|_E = id_E\} \\ \{x \in K \mid \sigma(x) = x, \ \forall \sigma \in H\} &\leftarrow H. \end{aligned}$$

Properties

- If E_1 and E_2 corresponding to H_1 and H_2 respectively, then $E_1 \subseteq E_2$ if and only if $H_1 \geq H_2$.
- $F \subset E \subset K$, E corresponding to H. Then $[K : E] = |H|$ and $[E : F] = |G : H|$.
- K/E is always Galois with Galois group $\mathrm{Gal}(K/E) = H$

Properties (continued)

- E is Galois over F if and only if H is a normal subgroup in G. If this is the case, then the Galois group is isomorphic to the quotien group $\mathrm{Gal}(E/F) \simeq G/H$.
- If E_1 and E_2 corresponding to H_1 and H_2 respectively, then:

  a $E_1 \cap E_2$ corresponding to $< H_1, H_2 >$;

  b $E_1 E_2$ corresponding to $H_1 \cap H_2$.

Example

- Consider the field $\mathbb{Q}(\sqrt{2}+\sqrt{3})$ is a subfield of the Galois extension $\mathbb{Q}(\sqrt{2},\sqrt{3})$.
- The other roots of the minimal polynomial for $\sqrt{2}+\sqrt{3}$ over $\mathbb{Q}$ are the distinct conjugate of $\sqrt{2}+\sqrt{3}$, i.e. $\pm\sqrt{2}\pm\sqrt{3}$.
- The minimal polynomial is therefore:

$$(x-(\sqrt{2}+\sqrt{3}))(x-(\sqrt{2}-\sqrt{3}))(x-(-\sqrt{2}+\sqrt{3}))(x-(-\sqrt{2}-\sqrt{3})),$$

that is the irreducible polynomial x^4-10x^2+1.
- Moreover, $\mathbb{Q}(\sqrt{2},\sqrt{3})=\mathbb{Q}(\sqrt{2}+\sqrt{3})$