Definition of Galois Extensions and Examples

Jiang-Hua Lu

The University of Hong Kong

MATH4302, Algebra II

Recall definitions and notation

- For a field L,

$$\mathrm{Aut}(L) = \text{the set of all field isomorphisms } L \longrightarrow L.$$

- For a field extension $K \subset L$, denote

$$\mathrm{Aut}_K(L) = \{\sigma \in \mathrm{Aut}(L) : \ \sigma(k) = k, \ \forall\, k \in K\}.$$

Today:

- Definition of Galois extensions and Examples

Recall Basic lemma on automorphism groups of finite simple extensions:
Assume that $L = K(\alpha)$ for $\alpha \in L$ algebraic over K, and let $p(x) \in K[x]$ be the minimal polynomial of α over K.

$K(\alpha) \to K[x]/\langle p \rangle \leftarrow K(\beta)$

$\sigma \mapsto \sigma(\alpha)$

1. Have bijection $\mathrm{Aut}_K(L) \leftrightarrow R_p$ (set of roots of p in L); Thus

$\beta \in R_p$

$$|\mathrm{Aut}_K(L)| = |R_p| \leq \deg(p) = |L : K|.$$

2. If p completely splits over L with no repeated roots in L, then

$$|\mathrm{Aut}_K(L)| (= |R_p| = \deg(p)) = |L : K|.$$

Fact For any finite ext $K \subset L$, have $|\mathrm{Aut}_K(L)| < \infty$

Definition. A finite extension $K \subset L$ is said to be Galois if

$$|\mathrm{Aut}_K(L)| = |L : K|.$$

For a Galois extension, we also write $\mathrm{Aut}_K(L) = \mathrm{Gal}(L/K)$.

Example. $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$ and

$$p(x) = x^4 - 10x^2 + 1.$$

$R_p = \{\pm(\sqrt{2} \pm \sqrt{3})\}$, so $|\mathrm{Aut}_K(L)| = 4$, thus $\mathrm{Aut}_{\mathbb{Q}}(L) \cong \mathbb{Z}_4$ or $\mathbb{Z}_2 \times \mathbb{Z}_2$.

- Let $\sigma \in \mathrm{Aut}_{\mathbb{Q}}(L)$ and consider $\sigma(\sqrt{2})$ and $\sigma(\sqrt{3})$.
- Must have
$$\sigma(\sqrt{2}) = \pm\sqrt{2}, \qquad \sigma(\sqrt{3}) = \pm\sqrt{3}$$
- Thus $\sigma^2(\sqrt{2}) = \sqrt{2}$ and $\sigma^2(\sqrt{3}) = \sqrt{3}$.
- Thus $\sigma^2 = 1$.
- Thus $\mathrm{Aut}_{\mathbb{Q}}(L) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

Example, the cyclotomic extensions: For $n \geq 1$,

$$C_n = \text{splitting field of } x^n - 1 = \mathbb{Q}(e^{2\pi i/n}).$$

Irreducible polynomial of $\omega_n = e^{2\pi i/n}$ in $\mathbb{Q}[x]$ is

$$\Phi_n = \prod_{1 \leq k \leq n, (k,n)=1} (x - \omega_n^k).$$

So Φ_n completely splits over C_n and has no repeated roots. Thus

$$|\mathrm{Aut}_{\mathbb{Q}}(C_n)| = \deg(\Phi_n) = \phi_n = |\{k \in [1, n] : (k, n) = 1\}|.$$

Each $k \in [1, n]$ with $(k, n) = 1$ defines

$$\sigma_k \in \mathrm{Aut}_{\mathbb{Q}}(C_n) : \quad \sigma_k(\omega_n) = \omega_n^k.$$

$\sigma_k \sigma_{k'} : \omega_n \to (\omega_n^k)^{k'} = \omega_n^{kk'}$

$= \sigma_{k''}$ if $kk' \equiv k'' \mod n$

Let $(\mathbb{Z}/n\mathbb{Z})^\times$ be the group of units of the ring $\mathbb{Z}/n\mathbb{Z}$, i.e.,

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{\bar{k} : 1 \leq k \leq n, \ (k, n) = 1\}.$$

Then we have the group isomorphism

$$(\mathbb{Z}/n\mathbb{Z})^\times \longrightarrow \mathrm{Aut}_{\mathbb{Q}}(C_n) : \quad \bar{k} \longmapsto \sigma_k.$$

The cyclotomic extensions continued:

Let $n = p_1^{k_1} p_2^{k_2} \cdots p_m^{k_m}$ be the prime factorization of n. Then

$$\mathbb{Z}/n\mathbb{Z} \cong (\mathbb{Z}/p_1^{k_1}\mathbb{Z}) \times (\mathbb{Z}/p_2^{k_2}\mathbb{Z}) \times \cdots \times (\mathbb{Z}/p_m^{k_m}\mathbb{Z}),$$

so

$$(\mathbb{Z}/n\mathbb{Z})^\times \cong (\mathbb{Z}/p_1^{k_1}\mathbb{Z})^\times \times (\mathbb{Z}/p_2^{k_2}\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/p_m^{k_m}\mathbb{Z})^\times.$$

Known: For any prime p and integer $k \geq 0$,

- $(\mathbb{Z}/p^k\mathbb{Z})^\times$ is an abelian group of size $p^k - p^{k-1}$ (easy to see);
- $(\mathbb{Z}/p^k\mathbb{Z})^\times \cong \mathbb{Z}/(p^k - p^{k-1})\mathbb{Z}$ is cyclic when $p \neq 2$;
- $(\mathbb{Z}/2^k\mathbb{Z})^\times$ is cyclic iff $k = 0, 1, 2$.
- For example, $(\mathbb{Z}/8\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

$\mathbb{F}_q \subset \mathbb{F}_{q^n}$ for $q = p^k$

Example: $\mathbb{F}_p \subset \mathbb{F}_{p^n}$ for prime number p and $n \geq 1$. We have proved

- $\mathbb{F}_{p^n}$ is a splitting field of $x^{p^n} - x$ over $\mathbb{F}_p$;
- the extension $\mathbb{F}_p \subset \mathbb{F}_{p^n}$ is simple:
$$\mathbb{F}_{p^n} = \mathbb{F}_p(\alpha),$$
where $\alpha \in \mathbb{F}_{p^n} \backslash \{0\}$ is any generator of $\mathbb{F}_{p^n} \backslash \{0\}$ as a cyclic group.
- The irreducible polynomial $q \in \mathbb{F}_p[x]$ of $\alpha \in \mathbb{F}_{p^n} \backslash \{0\}$ splits completely in $\mathbb{F}_{p^n}[x]$.

Thus $|\mathrm{Aut}_{\mathbb{F}_p}(\mathbb{F}_{p^n})| = n$. Which one?

$= \langle \sigma \rangle$

Claim: $\mathrm{Aut}_{\mathbb{F}_p}(\mathbb{F}_{p^n})$ is the cyclic group generated by the Frobenius isomorphism σ.

Proof. Let $G = \mathrm{Aut}_{\mathbb{F}_p}(\mathbb{F}_{p^n})$.

- We already know that $\langle \sigma \rangle \subset G$.
- Also know that $|G| = |\mathbb{F}_{p^n} : \mathbb{F}_p|$, and $\sigma^n = \mathrm{Id}$;
- Need to show $\mathrm{order}(\sigma) = n$.
- If $\sigma^k = \mathrm{Id}$ for $k < n$, then $a^{p^k} = a$ for all $a \in \mathbb{F}_{p^n}$, but

$$f(x) = x^{p^k} - x$$

can not have p^n elements, contradiction.

Q.E.D.