Characterizations of finite Galois extensions

Jiang-Hua Lu

The University of Hong Kong

MATH4302, Algebra II

Monday, April 28, 2025

Outline

In this file:

4.1.4: Characterizations of finite Galois extensions

1. Characterizations of finite Galois extensions.

If $K \subset L$, $\sigma \in \mathrm{Aut}(L) \Rightarrow$
$\sigma(K)$ is also a subfield

Recall:

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

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

Artin's Theorem: For any field L and any finite sub group H of $\mathrm{Aut}(L)$,

1. L is a Galois extension of L^H; $\stackrel{\text{def}}{=} \{a \in L : \sigma(a) = a \ \forall \sigma \in H\}$
2. $\mathrm{Aut}_{L^H}(L) = H$. $\quad (\Rightarrow |L : L^H| = |H|)$

Consequence of Artin's Theorem:

$K \subset L^G$

Corollary. Let $K \subset L$ be a finite field extension and let $G = \mathrm{Aut}_K(L)$. $\subset \mathrm{Aut}(L)$

1. $|G|$ divides $[L : K]$; In particular, $|G| \leq \cancel{[K : L]}$; $[L : K]$
2. $K \subset L$ is Galois if and only if $K = L^G$.

Proof. Applying Artin's Theorem to $G = \mathrm{Aut}_K(L)$, we see that

$$|G| = [L : L^G].$$

By the Tower Theorem,

1

$$[L : K] = [L : L^G][L^G : K] = |G|[L^G : K],$$

so $|G|$ divides $[L : K]$. In particular, $|G| \leq [L : K]$, and $|G| = [L : K]$ if and only if $[L^G : K] = 1$ which is the same as $L^G = K$.

Q.E.D.

Thus

A finite field extension $K \subset L$ is Galois iff one of the two holds:
1) $|\mathrm{Aut}_K(L)| = |L : K|$;
2) $K = L^G$.

We will give:

- two more equivalent characterizations of finite Galois extensions.

Lemma on minimal polynomials of elements in finite Galois extensions:

Lemma. Let $K \subset L$ be a finite Galois extension and $G = \mathrm{Aut}_K(L)$. Let $\alpha \in L$ and $p(x)$ the minimal polynomial of α in $K[x]$. Let

$$G\alpha = \{\sigma(\alpha) : \sigma \in G\} = \{\alpha, \alpha_2, \ldots, \alpha_r\}.$$

$\alpha_1 = \alpha$

Then

1. $G\alpha = \{$all roots of p in $L\}$, and $p(x) = (x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_r)$.
2. In particular, $p(x)$ $\underbrace{\text{splits completely in } L[x] \text{ with no repeated roots}}_{r = \deg p}$;

Proof. Let $q(x) = (x-\alpha)(x-\alpha_2)\cdots(x-\alpha_r) \in L[x]$.

- All coefficients of $q(x)$ are in $L^G = K$, so $q(x) \in K[x]$.
- By Lemma 0, every element in $G\alpha$ is a root of p.
- Thus $\deg(q) \leq \deg(p)$.
- Since $q(\alpha) = 0$, must have $p(x)|q(x)$. Thus $q(x) = p(x)$.

Eg: $\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2})$ $\cancel{L}$ $\quad \alpha = \sqrt[3]{2}. \quad p(x) = x^3 - 2$

$G = \{e\}$

Q.E.D.

Recall definitions: Let $K \subset L$ be an algebraic extension.

- $K \subset L$ is said to be normal if the minimal polynomial of every $\alpha \in L$ over K completely splits in $L[x]$;
- $K \subset L$ is said to be separable if the minimal polynomial of every $\alpha \in L$ over K has no repeated roots in its splitting field over K.
- Thus $K \subset L$ is both normal and separable iff the minimal polynomial of every $\alpha \in L$ over K completely splits in $L[x]$ and has no repeated roots in L.

Cor: If $K \subset L$ is Galois, then $K \subset L$ is normal & separable.

Theorem: A finite extension $K \subset L$ is Galois iff it is normal and separable.

Proof. By Lemma on minimal polynomials of elements in finite Galois extensions, a finite Galois extension is normal and separable.

- Assume a finite extension $K \subset L$ is normal and separable.
- By Primitive Element Theorem, L is a simple extension of K;
- Let $L = K(\alpha)$ for $\alpha \in L$ and let $p(x) \in K[x]$ be the minimal polynomial of α over K.
- Then $p(x)$ splits completely over L and has no repeated roots in L;
- By the Basic lemma on automorphism groups of finite simple extensions, L is Galois over K.

Q.E.D.

Basic Lemma on automorphism group of finite simple extensions:

Suppose $K \subset L = K(\alpha)$, α algebra. Let $p(x) \in K[x]$ be the mini. poly. of α.

Let R_p be the set of roots of p in L.

We have a map $Aut_K(L) \longrightarrow R_p$, $\sigma \mapsto \sigma(\alpha)$ is bijective.

$\Rightarrow$ ① $|Aut_K(L)| = |R_p| \leq \deg p = |L:K|$

② $|Aut_K(L)| = |L:K| \Longleftrightarrow p$ completely splits in $L[x]$ & w/ no repeat roots

Lemma 0: For $\forall\ K \subset L$ and $\forall\ f(x) \in K[x]$, if $\alpha \in L$ is a root of f in L, so is $\sigma(\alpha)$ for every $\sigma \in Aut_K(L)$.

Recap:

Let $K \subset L$ be a finite extension and let $G = \mathrm{Aut}_K(L)$. The following three statements are equivalent:

1. $|G| = [L : K]$ (Definition of $K \subset L$ being Galois);
2. $L^G = K$;
3. L is a normal and separable extension of K.

For a fourth characterization, recall

- $f(x) \in K[x]$ is said to be separable if f has no repeated roots in its splitting field.

Theorem: A finite extension L of K is a normal and separable if and only if L is the splitting field of a separable polynomial over K.

Proof. Assume first that $K \subset L$ is a normal and separable.

- Then L is the splitting field of some $f(x) \in K[x]$ over K.
- Let $f = cp_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}$, where $c \in K \setminus \{0\}$, and $p_1, \ldots, p_k \in K[x]$ are monic irreducible and pairwise distinct.
- Let $\tilde{f} = p_1 p_2 \cdots p_k \in K[x]$. Then $\tilde{f}$ and f have same roots in L.
- Each p_j splits completely in $L[x]$ with no repeated roots.
- Two different p_i and p_j have no common roots.
- Thus $\tilde{f} \in K[x]$ is separable and L is a splitting field of $\tilde{f}$.

Proof Continued:

Assume L is the splitting field of a separable $f(x) \in K[x]$ over K. We prove $|G| = [L : K]$ by induction on $[L : K]$.

- If $[L : K] = 1$, nothing to prove.
- Assume that $[L : K] \geq 2$.
- Let $p(x) \in K[x]$ be an irreducible factor of f in $K[x]$.
- Then p and f share a common root $\alpha \in L$. Let R_p be the set of all the roots of p in L.
- Since f completely splits in L with no repeated roots, the same holds for $p(x)$.
- Thus $|R_p| = \deg(p) = [K(\alpha) : K]$.

Proof Continued:

- By Construction Lemma of Automorphisms of Splitting Fields, G acts on R_p transitively.
- $\mathrm{Aut}_{K(\alpha)}(L)$ is the stabilizer subgroup at $\alpha \in R_p$.
- Thus $G/\mathrm{Aut}_{K(\alpha)}(L) \cong R_p$.
- Hence $|G| = |\mathrm{Aut}_{K(\alpha)}(L)||R_p| = |\mathrm{Aut}_{K(\alpha)}(L)|[K(\alpha) : K]$.
- Applying induction assumption to L being splitting field of f over $K(\alpha)$ and f separable over $K(\alpha)$, have $|\mathrm{Aut}_{K(\alpha)}(L)| = [L : K(\alpha)]$.
- By the Tower Theorem, $|G| = [L : K(\alpha)]\,[K(\alpha) : K] = [L : K]$.

Q.E.D.

Summary: Four characterizations of Galois extensions:

Theorem

For a finite extension $K \subset L$ with $G = \mathrm{Aut}_K(L)$, the following are equivalent:

1. $K \subset L$ *is Galois, i.e.,* $|G| = [L : K]$;
2. $K = L^G$;
3. *The extension* $K \subset L$ *is normal and separable;*
4. L *is a splitting field over* K *of some separable polynomial in* $K[x]$.

Corollary: For a perfect field K, (for example, K has characteristic 0 or is a finite field,) a finite extension $K \subset L$ is Galois if and only if L is a splitting field over K.

A non-example: Let $K = \mathbb{F}_2(t)$ and let $L = K(\sqrt{t})$, a splitting field of

$$f(x) = x^2 = t.$$

The extension is not separable:

$$f(x) = (x - \sqrt{t})^2.$$

Thus the extension $K \subset L$ is normal but not Galois.

Example. $\mathbb{Q} \subset L = \mathbb{Q}(\sqrt[3]{2}, e^{2\pi i/3})$:

$\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2}) \subset \underbrace{\mathbb{Q}(\sqrt[3]{2}, e^{2\pi i/3})}_{L}$

- Splitting field of $f(x) = x^3 - 2$, thus Galois.
- $\mathrm{Gal}_{\mathbb{Q}}(L)$ is isomorphic to a subgroup of S_3 because f has three roots.
- Know $|L : \mathbb{Q}| = 6$, so $|\mathrm{Gal}_{\mathbb{Q}}(L)| = 6$.
- Thus $\mathrm{Gal}_{\mathbb{Q}}(L) \cong S_3$.

$L \subset \mathbb{C}$

Example. Let L be the splitting field of $f(x) = x^5 - 4x + 2 \in \mathbb{Q}[x]$.

$\mathrm{Gal}_{\mathbb{Q}}(L) \longrightarrow S_5$

- L is a Galois extension of $\mathbb{Q}$.
- As f is irreducible over $\mathbb{Q}$ by Eisenstein's criterion, f has no repeated roots L. Thus $\mathrm{Gal}_{\mathbb{Q}}(L)$ is isomorphic to a subgroup of S_5.
- Calculus shows that f has three real roots and two complex roots.
- The complex conjugation $z \to \overline{z}$ is one element of order 2 in $\mathrm{Gal}_{\mathbb{Q}}(L)$.
- A ~~root~~ real root r of f gives $L_1 = \mathbb{Q}(r)$ with $[L_1 : \mathbb{Q}] = 5$. Thus $|\mathrm{Gal}_{\mathbb{Q}}(L)| = |L : Q|$ is divisible by 5.
- Cauchy's theorem implies that $\mathrm{Gal}_{\mathbb{Q}}(L)$ has an element of order 5.
- Conclude that $\mathrm{Gal}_{\mathbb{Q}}(L) \cong S_5$.