MATH4302, Algebra II

Jiang-Hua Lu

The University of Hong Kong

Monday April 2~~2~~5, 2022

Outline

Today

§3.1.2: Artin's Theorem and Characterizations of Galois extensions.

1. Artin's Theorem;
2. Characterizations of Galois extensions.

Recall

- Definition: For a field extension $K \subset L$,
$$\mathrm{Aut}_K(L) \stackrel{\text{def}}{=} \{\sigma \in \mathrm{Aut}(L) : \ \sigma(k) = k, \forall\, k \in K\}.$$
- Lemma. For any finite extension $K \subset L$, $\mathrm{Aut}_K(L)$ is a finite group.

New for today:

Definition. A finite field extension $K \subset L$ is called a Galois extension if
$$|\mathrm{Aut}_K(L)| = |L : K|.$$

For Galois extensions $K \subset L$, more common to denote $\mathrm{Aut}_K(L)$ by
$$\mathrm{Gal}(L/K) \quad \text{or} \quad \mathrm{Gal}_K(L).$$

What we have proved:

Theorem: If K has characteristic 0 or is a finite field, then every splitting field over K is Galois.

$\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2})$ is not Galois.

Examples: Let G denote the Galois group.

1. $\mathbb{R} \subset \mathbb{C}$ with $G \cong \mathbb{Z}/2\mathbb{Z}$;
2. $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}, \sqrt{3})$ with $G \cong (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$;
3. $\mathbb{Q} \subset \mathbb{Q}\left(e^{\frac{2\pi i}{n}}\right)$ with $G \cong (\mathbb{Z}/n\mathbb{Z})^{\times}$;
4. $\mathbb{F}_p \subset \mathbb{F}_{p^n}$ with $G \cong \mathbb{Z}/n\mathbb{Z}$.
5. $\mathbb{Q}(\sqrt[3]{2})$ is not a Galois extension of $\mathbb{Q}$.

Goal of this section:

- To explain Artin's construction of Galois extensions;
- To give three more equivalent definitions of finite Galois extensions.

Notation-Lemma. For any field L and any subgroup H of $\mathrm{Aut}(L)$,

$$L^H \stackrel{\text{def}}{=} \{a \in L : \sigma(a) = a, \ \forall\, \sigma \in H\} \subset L$$

is a subfield field of L, called the fixed field of H.

Proof: Direct check: If $a, b \in L^H$, then $\forall\, \sigma \in H$

$$\sigma(a+b) = \sigma(a) + \sigma(b) = a+b$$

$$\sigma(ab) = \sigma(a)\sigma(b) = ab$$

When $b \neq 0$ $\quad \sigma(b^{-1}) = \sigma(b)^{-1} = b^{-1}$. //

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

1. L is a (finite) Galois extension of L^H; $|\mathrm{Aut}_{L^H}(L)| = [L : L^H]$
2. $\mathrm{Aut}_{L^H}(L) = H$.

Proof.

$= \{\sigma(\alpha) : \sigma \in H\}$ $\alpha_1 = \alpha$

- Let $\alpha \in L$ be arbitrary, let $H\alpha = \{\alpha_1, \alpha_2, \ldots, \alpha_n\}$, and define

$$f(x) = \prod_{i=1}^{n} (x - \alpha_i) \in L[x].$$

- The coefficients of $f(x)$, expressed as symmetric polynomials of $\alpha_1, \ldots, \alpha_n$, are in L^H.

$n = 3$ $(x-\alpha_1)(x-\alpha_2)(x-\alpha_3)$
$= x^3 - (\alpha_1+\alpha_2+\alpha_3)x^2$
$+ (\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3)x$
$- \alpha_1\alpha_2\alpha_3$

- Thus $f(x) \in L^H[x]$.

$f(\alpha) = 0 \Rightarrow \alpha$ is algebraic over L^H.

Proof of Artin's Theorem continued:

- $f(\alpha) = 0$, so $\alpha \in L$ is algebraic over L^H.
- Let $p \in L^H[x]$ be the minimal polynomial of α in $L^H[x]$. Thus $p|f$.
- Since f has no repeated roots in L, p completely splits over L and has no repeated roots in L. Moreover,

$$|L^H(\alpha) : L^H| = \deg(p) \leq \deg f = n = |H\alpha| \leq |H|.$$

- Since $\alpha \in L$ is arbitrary, we conclude that L is an algebraic extension of L^H that is normal and separable.
- Choose $\alpha \in L$ such that $|L^H(\alpha) : L^H|$ is the largest.

Proof of Artin's Theorem continued:

- We now prove that $L^H(\alpha) = L$, which implies in particular that L is a finite extension of L^H:
  - Suppose that $L^H(\alpha) \neq L$. Choose $\beta \in L \backslash L^H(\alpha)$. Then $L^H(\alpha, \beta)$ is a finite separable extension of L^H.
  - By the Primitive Element Theorem (finite separable extensions are simple), $L^H(\alpha, \beta) = L^H(\gamma)$ for some $\gamma \in L$, contradicting the assumption on α. Thus $L^H(\alpha) = L$.
- By Basic Lemma on automorphism groups of finite simple extensions, we have

$$|\mathrm{Aut}_{L^H}(L)| \leq |L : L^H| \leq |H|.$$

- As $H \subset \mathrm{Aut}_{L^H}(L)$ by definition, one thus has $\mathrm{Aut}_{L^H}(L) = H$ and

$$|\mathrm{Aut}_{L^H}(L)| = |L : L^H|.$$

Q.E.D.

Example: Let K be any field. For any integer $n \geq 1$, let

$$\frac{f(x_1, \cdots, x_n)}{g(x_1, \cdots, x_n)}$$

$$L = K(x_1, \ldots, x_n), \ni$$

the fraction field of the polynomial ring $K[x_1, \ldots, x_n]$. The symmetric group S_n embeds into $\mathrm{Aut}(L)$ as a subgroup via action on L

$$(\sigma \cdot f)(x_1, \ldots, x_n) = f(x_{\sigma(1)}, \ldots, x_{\sigma(n)}), \qquad \sigma \in S_n.$$

Applying Artin's Theorem, we conclude

$$\frac{x_1 + x_2}{x_1 x_2} \in L^{S_2}$$

$$\frac{x_1}{x_1^2 + x_2} \notin L^{S_2}$$

- L is a (finite) Galois extension of L^{S_n} with Galois group S_n.
- For any subgroup $G \subset S_n$, L is a (finite) Galois extension of L^G with Galois group G.

$\subseteq S_{|G|}$

Every finite group is the Galois group of some finite Galois extension!

$G \hookrightarrow \mathrm{Perm}(G)$, $g \mapsto \sigma_g \in \mathrm{Perm}(G)$ hGG

$h \mapsto gh$,

Consequence of Artin's Theorem:

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

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

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

$\subset \mathrm{Aut}(L)$

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

$K \subset L^G$

By the Tower Theorem,

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

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.

Recap.

Definition. A finite field extension $K \subset L$ is called a Galois extension if

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

First characterization of finite Galois extensions:

A finite field extension $K \subset L$ is Galois if and only if $K = L^G$, where $G = \mathrm{Aut}_K(L)$

Always have $K \subset L^G$

We will give:

- two more equivalent characterizations of finite Galois extensions.

Eg: $\underset{K}{\mathbb{Q}} \subset \underset{L}{\mathbb{Q}(\sqrt[3]{2})}$, $G = \{e\}$

$L^G = L$

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.

Next: to prove a third characterization of finite Galois extensions: $G = Aut_K(L)$

- A finite extension is Galois if and only if it is normal and separable.

$|G| = [L:K] \iff K = L^G$

Need to look at minimal polynomials of elements in Galois extensions

1) Consider again $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2})$

$\alpha = \sqrt[3]{2}$, $p(x) = x^3 - 2$

does not split in $L[x]$,

so $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2})$

is not normal

2) $K = \mathbb{F}_2(t)$, $L = K(\sqrt{t})$

$\alpha = \sqrt{t}$, $p(x) = x^2 - t$

$= (x - \sqrt{t})(x + \sqrt{t})$

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

$x^2 + x + t$

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

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

Lemma 0

Then

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

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 $\cancel{q(x)|p(x)}$. Thus $q(x) = p(x)$.

$r \leq \deg p$

$\| \deg q$

$p(x) \mid q(x)$

Q.E.D.

Corollary: A finite Galois extension is normal and separable.

To prove the converse of the above, recall

- A finite extension $K \subset L$ is normal iff L is a splitting field over K.

Construction Lemma of Automorphisms of Splitting Fields

Lemma. Let L be a splitting field over K. If α and β are two roots of an irreducible polynomial $p(x) \in K[x]$, then there exists $\sigma \in \mathrm{Aut}_K(L)$ such that $\cancel{\alpha(\alpha)} = \beta$.
$\sigma(\alpha)$

Proof. We have field isomorphisms

$$K(\alpha) \xrightarrow{\sim} K[x]/\langle p \rangle \xrightarrow{\sim} K(\beta) \subset L.$$

- Note that L is also a splitting field over $K(\alpha)$.
- By Extension Lemma, there exists $\sigma \in \mathrm{Aut}_K(L)$ such that $\sigma(\alpha) = \beta$.

Q.E.D.

$\alpha \in K$, min. poly of α in $K[x]$ is $x - \alpha \in K[x]$

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

Proof. We have proved that Galois $\Rightarrow$ normal and separable.

- Assume finite extension $K \subset L$ is normal and separable.
- Let $G = \mathrm{Aut}_K(L)$. Need to show $L^G \subset K$. $(\Rightarrow L^G = K)$
- Let $\alpha \in L^G$ and $p(x) \in K[x]$ the minimal polynomial of α.
- Let $\beta \in L$ be any root of p. Then $\exists \sigma \in G$ such that $\sigma(\alpha) = \beta$. Since $\alpha \in L^G$, have $\alpha = \beta$. Thus α is the only root of p in L.
- By assumption, p splits completely over L and has no repeated roots in L. So p has only α as a root in L
- So $p \in K[x]$ is linear, and thus $\alpha \in K$.

  $p(x) = x - \alpha$.

Q.E.D.

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. $\Longleftrightarrow$ f has no repeated roots in every extension of K $\Longleftrightarrow$ f and f' are co-prime

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 $c \in K \backslash \{0\}$, 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 finite 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.

Not perfect.

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

$\sqrt[3]{2}, \quad \omega\sqrt[3]{2}, \quad \omega^2\sqrt[3]{2}$

$\omega = e^{2\pi i/3}$

- 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 $\mathrm{Gal}_{\mathbb{Q}}(L) \cong S_3$.

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

- 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 $\mathrm{Gal}_{\mathbb{Q}}(L) \cong S_5$. not solvable