Chapter 32 Galois Theory

Motivation

There are intimate relation between field extensions and the groups of automorphisms on the extension fields.

Definition Let $\mathbb{E}$ be an extension field of $\mathbb{F}$.
An autormorphism from $\mathbb{E}$ to $\mathbb{E}$ is a ring isomorphism from $\mathbb{E}$ to $\mathbb{E}$.
The Galois group of $\mathbb{E}$ over $\mathbb{F}$ is the group of all automorphisms of $\mathbb{E}$ fixing $\mathbb{F}$, and is denoted by $\mathrm{Gal}(\mathbb{E}/\mathbb{F})$.
If H is a subgroup of $\mathrm{Gal}(\mathbb{E}/\mathbb{F})$, the set

$$E_H = \{x \in \mathbb{E} : \phi(x) = x \text{ for all } \phi \in H\}$$

is the fixed field of H.

Examples

We may consider the following examples and construct the lattice diagrams of the Galois groups and subfields.

Example 1 If $\mathbb{E} = \mathbb{Q}(\sqrt{2})$, then $\mathrm{Gal}(\mathbb{E}/\mathbb{Q}) = \mathbb{Z}_2$.

Example 2 If $\mathbb{E} = \mathbb{Q}(\sqrt[3]{2})$, then $\mathrm{Gal}(\mathbb{E}/\mathbb{Q}) = \{d\}$.

Example 3 If $\mathbb{E} = \mathbb{Q}(\sqrt[4]{2}, i)$ and $\mathbb{F} = \mathbb{Q}(i)$, then $\mathrm{Gal}(\mathbb{E}/\mathbb{F}) = \langle \alpha \rangle \equiv \mathbb{Z}_4$.
Let $H = \{e, \alpha^2\}$. The fixed field will be $\mathbb{Q}(\sqrt{2}, i)$.

Example 4 Let $\mathbb{E} = \mathbb{Q}(\sqrt{3}, \sqrt{5})$. Then $\mathrm{Gal}(\mathbb{E}/\mathbb{Q}) = \mathbb{Z}_2 \oplus \mathbb{Z}_2$.
It has subgroups $\langle (1,0) \rangle$, $\langle (0,1) \rangle$, $\langle (1,1) \rangle$.
The corresponding fixed fields are $\mathbb{Q}(\sqrt{3})$, $\mathbb{Q}(\sqrt{5})$, $\mathbb{Q}(\sqrt{15})$.

Example 5 Let $\mathbb{E} = \mathbb{Q}(w, \sqrt[3]{2})$ with $w = e^{i2\pi/3}$. Then $\mathrm{Gal}(\mathbb{E}/\mathbb{Q}) = S_3$.
It has subgroups $\langle \beta \rangle, \langle \alpha \rangle, \langle \alpha\beta \rangle, \langle \alpha\beta^2 \rangle$.
The corresponding fixed fields are $\mathbb{Q}(w), \mathbb{Q}(\sqrt[3]{2}), \mathbb{Q}(\sqrt[3]{2}w), \mathbb{Q}(\sqrt[2]{2}w^2)$.

Fundamental Theorem of Galois Theory

Theorem 32.1 Let $\mathbb{F}$ be a finite field or a field of characteristic 0.
If $\mathbb{E}$ is the splitting field of $f(x) \in \mathbb{F}[x]$, then there is a one-one correspondence between a subfield $\mathbb{K}$ of $\mathbb{E}$ containing $\mathbb{F}$ a subgroup $\mathrm{Gal}(\mathbb{E}/\mathbb{K})$ of $\mathrm{Gal}(\mathbb{E}/\mathbb{F})$. Furthermore,

- $[\mathbb{E} : \mathbb{K}] = |\mathrm{Gal}(\mathbb{E}/\mathbb{K})|$ and $[\mathbb{K} : \mathbb{F}] = |\mathrm{Gal}(\mathbb{E}/\mathbb{F})|/|\mathrm{Gal}(\mathbb{E}/\mathbb{K})|$.
  The index of $\mathrm{Gal}(\mathbb{E}/\mathbb{K})$ in $\mathrm{Gal}(\mathbb{E}/\mathbb{F})$ equals the degree of $[\mathbb{K} : \mathbb{F}]$.
- If $\mathbb{K}$ is the splitting field of some polynomial in $\mathbb{F}[x]$, then $\mathrm{Gal}(\mathbb{E}/\mathbb{F})$ is a normal subgroup of $\mathrm{Gal}(\mathbb{E}/\mathbb{F})$ and $\mathrm{Gal}(\mathbb{K}/\mathbb{F})$ is isomorphic to $\mathrm{Gal}(\mathbb{E}/\mathbb{F})/\mathrm{Gal}(\mathbb{K}/\mathbb{F})$.
- The fixed field of $H = \mathrm{Gal}(\mathbb{E}/\mathbb{K})$ is $\mathbb{K}$, i.e., $K = E_{\mathrm{Gal}(\mathbb{E}/\mathbb{K})}$.
- If H is a subgroup of $\mathrm{Gal}(\mathbb{E}/\mathbb{F})$, then $H = \mathrm{Gal}(\mathbb{E}/\mathbb{E}_H)$.
  The automorphism group of $\mathbb{E}$ fixing $\mathbb{E}_H$ is H.

Proof. See http://www.math.uiuc.edu/˜r-ash/Algebra/Chapter6.pdf
http://planetmath.org/proofoffundamentaltheoremofgaloistheory

More examples

Example 6 Let $\mathbb{E} = \mathbb{Q}(w)$ with $w = e^{i2\pi/7}$. To determine the number of subfields, not that w is the splitting field of $f(x) = x^7 - 1 \in \mathbb{Q}[x]$.

Note that $\alpha : \mathbb{Q}(w) \to \mathbb{Q}(w)$ sending w to w^3 has order 6.

So, $[\mathbb{Q}(w) : \mathbb{Q}] = |\mathrm{Gal}(\mathbb{Q}(w)/\mathbb{Q})| \geq 6$.

Now, $x^7 - 1 = (x-1)(x^6 + \cdots + x + 1)$ and

$\phi(w)$ can only be a zero of the irreducible polynomial $x^6 + \cdots + 1$.

Thus, $[\mathbb{Q}(w) : \mathbb{Q}] = 6$.

Now, there are two proper subgroups, namely, $\langle \alpha^2 \rangle, \langle \alpha^3 \rangle$.

Example 7 Let $\mathbb{E} = GF(p^n)$ of $\mathbb{F} = GF(p)$.

Then there is a zero b of a degree n irreducible polynomial $f(x) \in \mathbb{F}[x]$

such that $\mathbb{E} = \mathbb{F}(b)$.

Note that $\sigma(a) = a^p$ is a field isomorphism, and $\langle \sigma \rangle$ has order n.

We see that $\mathrm{Gal}(GF(p^n)/GF(p)) \equiv \mathbb{Z}_n$.

Example Solve $ax^2 + bx + c = 0$.

Example The solution of $x^3 + bx + c = 0$ are

$$A + B,\ -(A+B)/2 + (A-B)\sqrt{-3}/2,\ -(A+B)/2 - (A-B)\sqrt{-3}/2,$$

where

$$A = \sqrt[3]{\frac{-c}{2} + \sqrt{\frac{b^3}{27} + \frac{c^2}{4}}} \quad \text{and} \quad B = \sqrt[3]{\frac{-c}{2} + \sqrt{\frac{b^3}{27} - \frac{c^2}{4}}}.$$

Definition Let $\mathbb{F}$ be a field and $f(x) \in \mathbb{F}[x]$. We say that $f(x)$ is solvable by radicals over $\mathbb{F}$ if $f(x)$ splits in some extension $\mathbb{F}(a_1, \ldots, a_n)$ such that $a_1^k \in \mathbb{F}$ and $a_i^{k_i} \in \mathbb{F}(a_1, \ldots, a_{i-1})$ for $i = 2, \ldots, n$.

Example 8 Let $w^{i2\pi/8}$. Then $x^8 - 3 = 0$ is solvable by radicals:

Solutions:

$$\pm\sqrt[8]{3}\sqrt{\pm 1}, \qquad \pm\sqrt[8]{3}\frac{(1 \pm \sqrt{-1})}{\sqrt{2}}.$$

Definition A group G is solvable if there is a sequence of subgroups

$$\{e\} = H_0 < H_1 < \cdots < H_k = G,$$

where H_i is normal in H_{i+1} and H_{i+1}/H_i is Abelian.

Remark If one can express the zeros of a polynomial $f(x)$ in radicals, then the splitting fields of $f(x)$ can be obtained by adjoining n_ith root of unity, so that the Galois group will be a solvable group.

Theorem 32.2 Let $\mathbb{F}$ be a field of characteristic 0. If $\mathbb{E}$ is the splitting field of $x^n - a \in \mathbb{F}[x]$, then $\mathrm{Gal}(\mathbb{E}/\mathbb{F})$ is solvable.

Proof. Let b be a zero of $x^n - a$.

Case 1 Suppose $\mathbb{F}$ contains a root of unit w with $w^n = 1$.

Then the zeros are $b, bw, \ldots, bw^{n-1}$ so that $\mathbb{E} = \mathbb{F}(b)$.

Hence, every $\sigma \in \mathrm{Gal}(\mathbb{E}/\mathbb{F})$ is determined by $\sigma(b) = w^j b$. So,

$$\sigma_1\sigma_2(b) = w^{j+k}b = w^{k+j}b = \sigma_2\sigma_1(b)$$

for any σ_1, σ_2.

Case 2 Suppose $\mathbb{F}$ does not contain a root of unity.

If $b \in \mathbb{E}$ is a zero and w is a primitive root of unity of $w^n = 1$ in some extension field, then $b, wb \in \mathbb{E}$ implies $w \in \mathbb{E}$.

Then $\mathrm{Gal}(\mathbb{F}(w)/\mathbb{F})$ is Abelian because

$$\sigma_i \sigma_j(w) = w^{ij} = w^{ji} \sigma_j \sigma_i(w).$$

Now,

$$\{e\} \leq \mathrm{Gal}(\mathbb{E}/\mathbb{F}(w)) \leq \mathrm{Gal}(\mathbb{E}/\mathbb{F}),$$

and

$$\mathrm{Gal}(\mathbb{E}/\mathbb{F}(w)) \quad \text{and} \quad \mathrm{Gal}(\mathbb{E}/\mathbb{F})/\mathrm{Gal}(E/\mathbb{F}(w)) \equiv \mathrm{Gal}(\mathbb{F}(w)/\mathbb{F})$$

are Abelian by Case 1, and is solvable. Thus, $\mathrm{Gal}(\mathbb{E}/\mathbb{F})$ is solvable. $\square$

Theorem 32.3 A factor group of a solvable group is solvable

Proof. If $\{e\} < H_0 < \cdots < H_k = G$, then

$$\{e\} = H_0N/N < \cdots < H_kN/N = G/N$$

is the corresponding sequence of Abelian factors. □

Theorem 32.4 Suppose N is a normal subgroup of G. If N and G/N are solvable, then so is G.

Proof. Suppose

$$\{e\} = N_0 < \cdots < N_t = N \quad \text{and} \quad N/N = H_0/N < \cdots < H_s/N = G/N$$

are Ableian factors. Then $N_0 < N_1 < \ldots, N_t < H_1 < \cdots < H_s = G$ are the Abelian factors. □

Theorem 32.5 Let $\mathbb{F}$ be a field of characteristic 0, and $f(x) \in \mathbb{F}[x]$ splits in $\mathbb{F}(a_1, \ldots, a_t)$, where $a_1^{n_1} \in \mathbb{F}$ and $a_i^{n_i} \in \mathbb{F}(a_1, \ldots, a_{i-1})$ for $i = 2, \ldots, t$.

If $\mathbb{E}$ is the splitting field of $f(x)$ in $\mathbb{F}(a_1, \ldots, a_t)$, then $\mathrm{Gal}(\mathbb{E}/\mathbb{F})$ is solvable.

Proof. By induction on t. Let $a = a_1^{n_1}$. Suppose $t = 1$. Then $\mathbb{F} \subseteq \mathbb{E} \subseteq \mathbb{F}(a_1)$.

Let $\mathbb{L}$ be the splitting filed of $f(x) = x^{n_1} - a$.

Then $\mathbb{F} \subseteq \mathbb{E} \subseteq \mathbb{L}$, and $\mathrm{Gal}(\mathbb{E}/\mathbb{F}) \equiv \mathrm{Gal}(\mathbb{L}/\mathbb{F})/\mathrm{Gal}(\mathbb{L}/\mathbb{E})$ is solvable.

Suppose $t > 1$. Let $\mathbb{L}$ be the splitting field of $x^{n_1} - a$ over $\mathbb{E}$, and let $\mathbb{K} \subseteq \mathbb{L}$ be the splitting field of $x^{n_1} - a$ over $\mathbb{F}$.

Then $\mathbb{L}$ is a splitting field of $(x^{n_1} - a)f(x)$ over $\mathbb{F}$, and $\mathbb{L}$ is a splitting field of $f(x)$ over $\mathbb{K}$.

Since $\mathbb{F}(a_1) \subseteq K$, it follows that $f(x)$ splits in $K(a_2, \ldots, a_t)$.

By induction assumption. $\mathrm{Gal}(\mathbb{L}/\mathbb{K})$ is solvable. By Theorem 32.2, $\mathrm{Gal}(\mathbb{K}/\mathbb{F})$ is solvable. By Theorem 32.1, $\mathrm{Gal}(\mathbb{L}/\mathbb{F})$ is solvable.

By Theorem 32.1 and Theorem 32.3, $\mathrm{Gal}(\mathbb{E}/\mathbb{F}) \equiv \mathrm{Gal}(\mathbb{L}/\mathbb{F})/\mathrm{Gal}(\mathbb{L}/\mathbb{E})$ is solvable. $\square$

Insolvability of a quintic

Example Let $g(x) = 3x^5 - 15x + 5$. Then $g(x)$ is not solvable by radicals.

Proof. By Eisenstein's Criterion, $g(x)$ is irreducible.

Because $g(-2) < 0$ and $g(-1) > 0$, there is a root in $(-2, -1)$.

One can check that there are zeros in $(0, 1)$ and $(1, 2)$.

Note that $g'(x) = 15x^4 - 15$ so that there are only three real zeros. (Five real roots will generate 4 distinct critical points.)

Now, suppose $a_1, \ldots, a_5$ are the five zeros. Then $\mathbb{K} = \mathbb{Q}(a_1, \ldots, a_5)$ and $\mathrm{Gal}(\mathbb{K}/\mathbb{Q}) \leq S_5$.

Observe that $[\mathbb{Q}(a_1) : \mathbb{Q}] = 5$ and $\mathrm{Gal}(\mathbb{K}/\mathbb{Q})$ contains an element order two element exchanging the two complex zeros.

So, $\mathrm{Gal}(\mathbb{K}/\mathbb{Q}) = S_5$, which is not solvable. $\square$