MATH 416, Modern Algebra II

Volodymyr Nekrashevych

2020, April 14

Main Theorem of Galois Theory

Theorem 1

Let $F \subseteq K$ be a finite **normal** *extension. Then we have a bijection $E \mapsto G(K/E)$ between the set of intermediate fields $\{E : F \subseteq E \subseteq K\}$ and the set of subgroups of $G(K/F)$. The inverse of this bijection is the map $H \mapsto K_H = \{x \in K : \sigma(x) = x, \forall \sigma \in H\}$. We call these bijection the* **Galois correspondence**. *It has the following properties.*

1. *The described maps are inverse to each other, i.e., $E = K_{G(K/E)}$ for every intermediate field E, and $H = G(K/K_H)$ for every subgroup $H \leq G(K/F)$.*
2. $[K : E] = |G(K/E)|$ *and* $[E : F] = [G(K/F) : G(K/E)]$.
3. *E is a normal extension of F if and only if $G(K/E)$ is a normal subgroup of $G(K/F)$. If it is so, then $G(E/F) \cong G(K/F)/G(K/E)$.*
4. *The Galois correspondence is order-inverting: If $E_1 \subset E_2$, then $G(K/E_1) > G(K/E_2)$.*

Proof

It remains to show that if $F \subseteq E$ is normal, then $G(E/F) \cong G(K/F)/G(K/E)$. Consider the *restriction map* $\sigma \mapsto \sigma|_E$. It is a map from $G(K/F)$ to $G(E/F)$, since $\sigma(E) = E$ for every $\sigma \in G(K/F)$. It is surjective by the Isomorphism Extension Theorem and the fact that $F \subseteq K$ is normal. It is obviously a homomorphism. Its kernel is the set of automorphisms $\sigma \in G(K/F)$ inducing the identity automorphism on E, i.e., it is $G(K/E)$.

Illustrations of the theory

Let F be a field, and consider the field of rational functions $F(y_1, y_2, \ldots, y_n)$, where y_i are independent variables. The symmetric group S_n acts on this field by permuting the variables. For example, the permutations $(1, 2)$ transforms $\frac{y_1^2+y_2-y_3}{y_1+2y_2+y_3^3}$ to $\frac{y_2^2+y_1-y_3}{y_2+2y_1+y_3^3}$.
A function is called *symmetric* if it is fixed under every permutation $\sigma \in S_n$. For example $y_1 + y_2 + \cdots + y_n$, $y_1^2 + y_2^2 + \cdots + y_n^2$, $y_1 y_2 \ldots y_n$ are symmetric, $y_1 - y_2$ and y_1 are not (if $n > 1$). The set of symmetric functions is the fixed field of the described group of automorphisms of the field $F(y_1, y_2, \ldots, y_n)$.

Consider the polynomial
$f(x) = (x - y_1)(x - y_2) \dots (x - y_n) \in F(y_1, y_2, \dots, y_n)[x]$. It is fixed under the action of S_n, hence its coefficients are symmetric functions. We have

$$f(x) = x^n - (y_1 + y_2 + \cdots + y_n)x^{n-1} + (y_1 y_2 + y_1 y_3 + \cdots)x^{n-2} - \cdots + (-1)^n y_1 y_2 \dots$$

The coefficients (up to the sign) are called *elementary symmetric functions* $s_k(y_1, y_2, \dots, y_n)$ equal to the sum of all products of length k.

Consider the field $F(s_1, s_2, \dots, s_n)$. Since $s_i \in F(y_1, y_2, \dots, y_n)$, we have $F(s_1, s_2, \dots, s_n) \subset F(y_1, y_2, \dots, y_n)$. In fact, since each s_i is symmetric, the field $F(s_1, s_2, \dots, s_n)$ is contained in the field of symmetric functions. Note that y_i are the roots of the polynomial $f(x) = (x - y_1)(x - y_2)\cdots(x - y_n)$, so $F(y_1, y_2, \dots, y_n)$ is a splitting extension of $F(s_1, s_2, \dots, s_n)$, namely the splitting field of $f(x)$. It follows that $F(s_1, s_2, \dots, s_n) \subset F(y_1, y_2, \dots, y_n)$ is a normal extension. Every element of the Galois group of this extension is uniquely determined by its action on the roots of $f(x)$. Moreover, since the coefficients are fixed under the action of the Galois group, it has to permute the roots. It follows that the Galois group is a subgroup of the symmetric group on the roots (this is true for every splitting field of a polynomial). But we know that the full S_n acts by automorphisms of the extension. It shows that the Galois group is S_n.

We have shown that the Galois group of the extension $F(s_1, s_2, \dots, s_n) \subset F(y_1, y_2, \dots, y_n)$ is the symmetric group acting by permutations of the variables y_i. Since the extension is normal, the fixed field of the Galois group is $F(s_1, s_2, \dots, s_n)$. But the fixed field is, by definition, the field of symmetric functions. We proved the following fact (known long before Galois Theory)

Theorem 2

Every symmetric function is a function of elementary symmetric functions.

For example $y_1^2 + y_2^2 + \cdots + y_n^2 = s_1^2 - 2s_2$.
$y_1^3 + y_2^3 + \cdots + y_n^3 = s_1^3 - 3s_1s_2 + 3s_3$. The recurrent formulas relating $p_k = y_1^k + y_2^k + \cdots + y_n^k$ and s_i are called *Newton's identities*:

$$ks_k = \sum_{i=k-n}^{n} (-1)^{i-1} s_{k-i} p_i,$$

where s_k is defined as 0 for $k > n$. In order to express a symmetric polynomial $g(y_1, y_2, \ldots, y_n) \in F[y_1, y_2, \ldots, y_n]$ as a function of s_i, one can use the following algorithm: find the lexicographically highest degree monomial $c_{k_1,k_1,\ldots,k_n} y_1^{k_1} y_2^{k_2} \ldots y_n^{k_n}$ (find the highest power of y_1, among them the highest power of y_2, etc.) Note that then $k_1 \geq k_2 \geq \ldots \geq k_n$. Kill it by passing to $g - c_{k_1,k_2,\ldots,k_n} s_n^{k_1-k_2} s_{n-1}^{k_2-k_3} \cdots s_1^{k_n}$. The new polynomial has lower degree of the highest degree monomial. Proceed until you get 0.

An important symmetric polynomial is the *discriminant* $\prod_{i \neq j}(y_i - y_j)$ equal to the product of squares of pairwise differences. For example, for $n = 2$ it is $(y_1 - y_2)^2 = y_1^2 - 2y_1y_2 + y_2^2 = (y_1 + y_2)^2 - 4y_1y_2 = s_1^2 - 4s_2$. Note that this is exactly the discriminant of the polynomial $f(x) = (x - y_1)(x - y_2) = x^2 - (y_1 + y_2)x + y_1y_2 = x^2 - s_1x + s_2$. We will see later that discriminants play important role in solving polynomial equations.

An example

Consider the splitting field over $\mathbb{Q}$ of $x^4 - 2$. The four roots are $\pm\sqrt[4]{2}$, $\pm i\sqrt[4]{2}$. The splitting field is $\mathbb{Q}(\sqrt[4]{2}, i)$. We have a tower of extensions $\mathbb{Q} \subset \mathbb{Q}(\sqrt[4]{2}) \subset \mathbb{Q}(\sqrt[4]{2}, i)$. Note that since $x^4 - 2$ is irreducible over $\mathbb{Q}$, we have $[\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = 4$. Since $i \notin \mathbb{Q}(\sqrt[4]{2})$, and i is a root of a quadratic polynomial over $\mathbb{Q}$, we have $[\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}] = 2$. Consequently, the degree of the splitting field over $\mathbb{Q}$ is $8 = 4 \times 2$. A basis of the extension over $\mathbb{Q}$ is $\{1, \alpha, \alpha^2, \alpha^3, i, i\alpha, i\alpha^2, i\alpha^3\}$, where $\alpha = \sqrt[4]{2}$.

An example

Since the degree is 8 and it is a normal extension, the Galois group consists of 8 elements. These elements permute the roots $\{\alpha, i\alpha, -\alpha, -i\alpha\}$ of $x^4 - 2$ and are uniquely determined by their action on the roots. It follows that the Galois group is an order 8 subgroup of S_4. Let us find all of elements of the Galois group. Since $x^4 - 2$ is irreducible, the Galois group acts transitively on the roots (in fact, a polynomial is irreducible over a field F if and only if the Galois group of its splitting field over F is transitive on the roots). Note that the Galois group of the extension $\mathbb{Q}(\sqrt[4]{2}) \subset \mathbb{Q}(\sqrt[4]{2}, i)$ must be of order 2 (note that any degree 2 separable extension is normal). We know one non-trivial element of this Galois group: complex conjugation.

An example

Every element of the Galois group is determined by its action on the basis $\{1, \alpha, \alpha^2, \alpha^3, i, i\alpha, i\alpha^2, i\alpha^3\}$. If σ is an element of the Galois group, then $\sigma(\alpha) \in \{\alpha, i\alpha, -\alpha, -i\alpha\}$ and $\sigma(i) \in \{i, -i\}$. This gives 8 possibilities. Therefore, all of them must be realized. Let us list them in a table and give them names

	ϵ	ρ_1	ρ_2	ρ_3	μ_1	δ_1	μ_2	δ_2
$\alpha \mapsto$	α	$i\alpha$	$-\alpha$	$-i\alpha$	α	$i\alpha$	$-\alpha$	$-i\alpha$
$i \mapsto$	i	i	i	i	$-i$	$-i$	$-i$	$-i$

	ϵ	ρ_1	ρ_2	ρ_3	μ_1	δ_1	μ_2	δ_2
$\alpha \mapsto$	α	$i\alpha$	$-\alpha$	$-i\alpha$	α	$i\alpha$	$-\alpha$	$-i\alpha$
$i \mapsto$	i	i	i	i	$-i$	$-i$	$-i$	$-i$

Let us see how they permute the roots.

$$\rho_1 : \alpha \mapsto i\alpha \mapsto i \cdot i\alpha = -\alpha \mapsto -i\alpha \mapsto -i(i\alpha) = \alpha$$
$$\rho_2 : \alpha \leftrightarrow -\alpha, \quad i\alpha \leftrightarrow -i\alpha$$
$$\rho_3 : \alpha \mapsto -i\alpha \mapsto -\alpha \mapsto i\alpha \mapsto \alpha$$
$$\mu_1 : \alpha \mapsto \alpha, -\alpha \mapsto -\alpha, i\alpha \leftrightarrow -i\alpha$$
$$\delta_1 : \alpha \mapsto i\alpha \mapsto (-i)(i\alpha) = \alpha, \quad -\alpha \leftrightarrow -i\alpha$$
$$\mu_2 : \alpha \leftrightarrow -\alpha, i\alpha \mapsto (-i)(-\alpha) = i\alpha, -i\alpha \mapsto -(-i)(-\alpha) = -i\alpha$$
$$\delta_2 : \alpha \mapsto -i\alpha, i\alpha \mapsto -i(-i\alpha) = -\alpha, -\alpha \mapsto i\alpha, -i\alpha \mapsto -(-i)(-i\alpha) = -\alpha$$

We see that it acts as D_4 on the square of roots of $x^4 - 2$.

The group D_4 has one cyclic subgroup of order 4: $\{\epsilon, \rho_1, \rho_2, \rho_3\}$ two subgroups isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$ (generated reflections with respect to the two diagonals and generated by reflections with respect to two lines parallel to the sides): $\{\epsilon, \mu_1, \mu_2, \rho_2\}$ and $\{\epsilon, \delta_1, \delta_2, \rho_2\}$. Each of the elements of order 2 $\{\rho_2, \mu_1, \mu_2, \delta_1, \delta_2\}$ generates a subgroup of order 2. And then there is the trivial subgroup and the whole group.

Let us find the fixed fields of the subgroups. The field corresponding to groups of order 4 must be a quadratic extension of $\mathbb{Q}$, since the index of the subgroup is 2. We have i, $\sqrt{2}$, and $i\sqrt{2}$ in the field. Note that $\rho_1(i) = i$, so i belongs to the fixed field of the cyclic group generated by ρ_1. It follows that the fixed field of the cyclic group is $\mathbb{Q}(i)$. We have $\mu_1(\sqrt{2}) = \mu_1(\alpha^2) = \alpha^2$ and $\mu_2(\sqrt{2}) = \mu_2(\alpha^2) = (-\alpha)^2 = \alpha^2$, hence $\mathbb{Q}(\sqrt{2})$ is in the fixed field of $\{\epsilon, \mu_1, \mu_2, \rho_2\}$. Similarly, $\delta_1(i\sqrt{2}) = \delta_1(i\alpha^2) = -i(i\alpha)^2 = i\alpha^2$ and $\delta_2(i\sqrt{2}) = -i(-i\alpha)^2 = i\alpha^2$, hence the fixed field of $\{\epsilon, \delta_1, \delta_2, \rho_2\}$ is $\mathbb{Q}(i\sqrt{2})$.

It remains to find the fixed fields of groups of order two. They must be degree 4 extensions of $\mathbb{Q}$. ρ_2 fixes i and $\alpha^2 = \sqrt{2}$, which gives the degree 4 extension $\mathbb{Q}(i, \sqrt{2})$. μ_1 fixes $\sqrt[4]{2}$, which $\mathbb{Q}(\sqrt[4]{2})$. μ_2 fixes $i\sqrt[4]{2}$, so it gives $\mathbb{Q}(i\sqrt[4]{2})$. δ_1 switches α with $i\alpha$, so it leaves $\alpha + i\alpha$ fixed, so it gives $\mathbb{Q}(\sqrt[4]{2} + i\sqrt[4]{2})$. δ_2 switches α and $-i\alpha$, and we get $\mathbb{Q}(\sqrt[4]{2} - i\sqrt[4]{2})$.

Cyclotomic extensions

The splitting field of $x^n - 1$ over F is the *nth cyclotomic extension of F*. If α is a root of $x^n - 1$, then using long division, we get $g(x) = \frac{x^n - 1}{x - \alpha} = x^{n-1} + \alpha x^{n-2} + \alpha^2 x^{n-3} + \cdots + \alpha^{n-1} x + 1$, hence $g(\alpha) = n\alpha^{n-1} = n\alpha^{-1}$. This is not equal to zero if and only if n is not divisible by the characteristic of F. Consequently, if n is not divisible by the characteristic, then all roots of $x^n - 1$ are simple, and the cyclotomic extension is separable.