Galois Group of polynomials

Miliyon T.

1 Introduction

All fields are assumed to be subfields of $\mathbb{C}$. If F is a subfield of K we call K an extension of F and we can regard it as a vector space over F whose dimension, called the degree of the extension, is written $[K : F]$.

The **Galois group** of the extension, $G(K/F)$,is the group of all field automorphisms (1-1 maps from the field to itself which preserve sums and products)which fix the elements of F, with multiplication of maps as the operation. The fixed field of a subgroup of $G(K/F)$ is the set of all elements of K which are fixed by every automorphism in the subgroup. If σ_1, ... $\sigma_n \in$ C, $\mathbf{F[\sigma_1,\ ...\ \sigma_n]}$ denotes the smallest subfield which contains F and the a_i. If $a_1, ..., a_n$, are the zeros of $f(x) \in F[x]$ this field is written as $\mathbf{F[f(x) = 0]}$ and such an extension is called a **polynomial extension**.

The minimum polynomial of $\sigma \in \mathbb{C}$ over F is the monic polynomial $p(x) \in F[x]$ of smallest degree for which $p(\sigma) = 0$. It is a prime polynomial and its degree, n, is the dimension of $F[\sigma]$ over F. In fact $1, \sigma, \sigma^2, ..., \sigma^{n-1}$ is a basis. Numbers with the same minimum polynomial over F are said to be **algebraic conjugates**, over F. Under an automorphism in $G(K/F)$ every element of K must be mapped to one of its algebraic conjugates. The Galois group of an extension of a field by a polynomial of degree n is isomorphic to a subgroup of S_n. The degree of the extension itself equals the order of the Galois group over F and there is a 1-1 order-reversing correspondence between the subfields and the subgroups with the index of a subgroup being the degree, over F, of its fixed field and with normal subgroups corresponding to polynomial extensions.

If $C \supset B \supset A$ are fields, $[C : A] = [C : B][B : A]$. If X, Y are bases for C over B and B over A then a basis for C over A is $\beta\ \gamma \mid \beta\ ,\gamma \in$ Y. B and C are polynomial extensions of A, then $G(C/A)/G(C/B) \cong G(B/A)$.

A **radical extension** is one of the form $F[x^n = a]$, for $a \in F$. Radical extensions have abelian Galois groups and so a field which can be reached from F by a sequence of radical extensions has a soluble Galois group over F. A polynomial is solvable by radicals over F if and only if its Galois group is solvable.

2 Field Extensions

Definition 2.1. Let E be an extension field of F. An automorphism of E is a ring isomorphism from E onto E. An $F - automorphism$ of E is an automorphism $\phi \quad of \quad E$ such that $\phi x = x \forall x \in F$.

Definition 2.2. The automorphism group $Aut(E:F)$ of $E:F$ fixing F is the set of all all $F-automorphisms$ of E.

Theorem 2.3. *The automorphism group $Aut(E:F)$ is a group under composition.*

Proof. First, note that the composition operation $\circ$ is always associative. Let $\phi, \psi \in G(E:F)$.Then $(\phi o\psi)(a) = \phi(\psi(a)) = \phi(a) = a, \forall a \in F$, and hence $\phi o\psi \in$ Aut(E : F). Moreover, for any $a \in F, \phi^{-1}(a) = b$, where $\phi(b) = a$. But ϕ is an F-automorphism, so $\phi(b) = b \Rightarrow b = a$. Hence,$\phi^{-1}(a)(a) = a, \forall a \in F \Rightarrow \phi^{-1} \in Aut(E:F)$. As such, $(\phi o\phi^{-1} = id \in Aut(E:F)$, and therefore Aut(E:F) is a group. □

Example 2.4. Consider $G(\mathbb{C}:\mathbb{R})$: Suppose α is an $R-automorphism$ of $\mathbb{C}$, and let $j = \alpha(i)$, where i^2=-1. Then we have that $j^2 = \alpha(-1) = -1 \Rightarrow j = \pm i$, Therefore, $\alpha(x+iy) = \alpha(x) + \alpha(i)\alpha(y) = x + jy = x \pm iy$. Hence, we have two possible $\mathbb{R} - automorphismsof\mathbb{C}$:

$$\alpha_1(x+iy)\text{=x+iy}$$

and

$$\alpha_2(x+iy)\text{=x-iy}$$

The identity is obviously an R-automorphism.

To check the latter,

$$\begin{aligned}\alpha_2((x+iy)+(u+iv)) &= \alpha_2((x+u)+i(y+v))\\ &= (x+u)-i(y+v)\\ &= x-iy+u-iv\\ &= \alpha_2(x+iy)+\alpha_2(u+iv)\end{aligned}$$

$$\begin{aligned}\alpha_2((x+iy)(u+iv)) &= \alpha_2((xu-yv+i(xv+yu))\\ &= xu-yv-i(xv+yu)\\ &= (x-iy)(u-iv)\\ &= \alpha_2(x+iy)\alpha_2(u+iv)\end{aligned}$$

Hence, α_2 is an R-automorphism. Clearly, ${\alpha_2}^2 = \text{id}$, and we can see that G(C : R) = id,α_2 α_2g is a cyclic group of order 2.

Example 2.5. Consider the prototypical example of $\mathbb{Q}[\sqrt{2}]$ as an extension of $\mathbb{Q}$. We already know that $\mathbb{Q}[\sqrt{2}] = a + b\sqrt{2}, a, \in \mathbb{Q}$. Therefore, if ϕ is a $\mathbb{Q}$-automorphism, then for all $\alpha \in \mathbb{Q}[\sqrt{2}]$, $\phi\ \alpha = \phi a + \phi(b)\phi\sqrt{2} = a + b\phi\sqrt{2}$.

Therefore, $\phi : \mathbb{Q}[\sqrt{2}] \to \mathbb{Q}[\sqrt{2}]$ is completely determined by the value of $\phi\sqrt{2}$. Now, because

$$\begin{aligned}2 = \phi(2) &= \phi(\sqrt{2})\\ &= \phi\sqrt{2}\phi\sqrt{2}\\ &= (\phi\sqrt{2})^2\end{aligned}$$

$\Rightarrow \phi\sqrt{2} = \pm\sqrt{2}$

we see that, as before, there are two possible automorphisms and hence $|G(Q[\sqrt{2}] : Q| = 2$.

Definition 2.6. Let H be a finite subgroup of the group of automorphisms of a field E: The fixed field of H E_H is given by E_H ={x∈ E/ ϕ(x)=x,∀ ϕ ∈H }.

Notice the importance of the previous definition, We have just associated a field E_H with the group of automorphisms of a field extension E : F. We can now make the following proposition:

Proposition 2.7. *The association of groups to fields and fields to group defined above is inclusion reversing. That is,*

1. *if E is an extension of F_1 and F_2, with $F_1 \subseteq F_2 \subseteq E$; then Aut(E : F_1)⊇(E : F_2), and*
2. *if $H_1 \subseteq H_2 \subseteq$ Aut(E); then $E_{H_1} \supseteq E_{H_2}$.*

Example 2.8. Consider our previous example of $\mathbb{Q}[\sqrt{2}]$ as an extension of $\mathbb{Q}$: We showed that $|Aut(\mathbb{Q}[\sqrt{2}]) : \mathbb{Q}| = 2 \Rightarrow Aut(\mathbb{Q}[\sqrt{2}]) : \mathbb{Q} = 1, \sigma = A$. The identity fixes everything, so the fixed field $\mathbb{Q}[\sqrt{2}]_A$ is the set of elements in $\mathbb{Q}[\sqrt{2}]$ that are fixed by σ. That is, $\mathbb{Q}[\sqrt{2}]_A = \{x \in A | \sigma x = x\}$. But,
$\sigma(a + b\sqrt{2}) = a + b\sqrt{2}$
$\Rightarrow a - b\sqrt{2} = a + b\sqrt{2}$
$\Rightarrow b = 0$.
Therefore,$\mathbb{Q}[\sqrt{2}]_A = \mathbb{Q}$ is the the only fixed field of $Aut(\mathbb{Q}[\sqrt{2}]$.

The Galois group of a polynomial extension can be computed readily if the zeros of the polynomial are known and can sometimes be obtained indirectly when they are not.

Example 2.9. **f(x) = x^4 - x^2 - 2**

1. Factors: x^4 - x^2 - 2 = (x^2 - 2)(x^2 + 1).
2. Zeros: $\pm\sqrt{2}, \pm i$
3. Splitting field = F = $\mathbb{Q}[\sqrt{2}, -\sqrt{2}, i, -i] = \mathbb{Q}[\sqrt{2}, i] = \mathbb{Q}[i][\sqrt{2}]$.
4. $|F : \mathbb{Q}| = 4[= |F : \mathbb{Q}[\sqrt{2}]| \times |\mathbb{Q}[\sqrt{2}] : \mathbb{Q}| = 2 \times 2]$
5. The Galois group has order 4.
6. Possible automorphisms: i→ ±i and $\sqrt{2} \to \pm\sqrt{2}$, giving four combinations.
7. All 4 combinations arise. [since $|F : \mathbb{Q}| = 4$]

8. In this group every subgroup is normal, so every subfield must be a polynomial extension. Indeed they are since:
   * $K = \mathbb{Q}[x^4 - x^2 - 2 = 0]$;
   * $\mathbb{Q}[i] = \mathbb{Q}[x^2 + 1 = 0]$;
   * $Q[\sqrt{2}] = \mathbb{Q}[x^2 - 2 = 0]$;
   * $\mathbb{Q}[\sqrt{2}] = \mathbb{Q}[x^2 + 2 = 0]$.
9. The subfields are: $K, \mathbb{Q}[i], \mathbb{Q}[\sqrt{2}], \mathbb{Q}[\sqrt{2}], \mathbb{Q}$

3 Galois Theory

Definition 3.1 (Automorphism)**.** A bijective mapping of the elements of a set onto itself. So, the domain and range of the function are the same.

Let E be an extension field of the field F. An automorphism of E is a ring isomorphism from E onto E. The Galois group of E over F, $Gal(E/F)$ is the set of all automorphisms of E that take every element of F to itself.

Definition 3.2. If H is a subgroup of $Gal(E/F)$ is the set $E_H = \{x \in E/\phi(x) = x \forall \phi \in H\}$ is called the fixed field of H.

The set of automorphisms of E forms a group under composition. The automorphism group of E fixing F is a subgroup of the automorphism group of E and for any subgroup H of $Gal(E/F)$,the fixed field E_H of H is a subfield of E. The group $Gal(E/F)$ is called Galois group of E over F.

Theorem 3.3. ***(Fundamental Theorem of Galois Theory)***
Let $E : F$ be a Galois extension. Then there exists a bijection between subfields Mi of E containing F and subgroups H_i of G(E : F) given by $\phi : M_i \to G(E : M_i)$ and $\varphi : H_i \to E_H$; which are mutual inverses. Moreover,

1 *If M_i;M_j correspond to H_i;H_j ; respectively, then $M_i \subseteq M_j$ if and only if $H_i \supseteq H_j$,$\forall$ $i \neq j$.*

2 *[E : M_i] = | H_i | and [M_i : F] = |G(E:F) : H_i |, $\forall$ i.*

3 E : M_i is always Galois, with G(E : M_i) = H_i; $\forall$i.

4 M_i : F is Galois if and only if H_i is a normal subgroup of G(E : F): If this is the case, then G(M_i : F)$\cong$ G(E : F)/ H_i.

5 The lattice of subfields of E containing F and the lattice of subgroups of G(E : F) are dual.

Example 3.4. Consider the polynomial $f(x) = x^4 - 2$ over $\mathbb{Q}$, Then a splitting field for f is $\mathbb{Q}[\sqrt[4]{2}, i]$; where $f(x) = (x + \xi)(x - \xi)(x + \xi i)(x - \xi i)$, and $\xi = \sqrt[4]{2}$. We can immediately conclude that $\mathbb{Q}[\sqrt[4]{2}, i]$ is normal and separable. To compute the degree of $\mathbb{Q}[\sqrt[4]{2}, i]$ over $\mathbb{Q}$, simply consider the form of any element: For any $\gamma \in \mathbb{Q}[\sqrt[4]{2}, i]$, γ=a_1 + a_2 ξ +a_3 ξ^2 + a_4 ξ^3 + a_5i + a_6 ξi + $a_7\xi^2$i + $a_8\xi^3$i. Therefore, we know that $[\mathbb{Q}[\sqrt[4]{2}, i] : \mathbb{Q}] = 8$ Therefore, $\mathbb{Q}[\sqrt[4]{2}, i] : \mathbb{Q}$ is a Galois extension.

4 Solvability of Polynomials by Radicals

Galois' entire purpose for investigating this structure in the first place was to find solutions of polynomials by radicals. To see how this is achieved, we need the following definitions.

Definition 4.1. A polynomial, f (x) ∈ K[x], is said to be solvable by radicals if its splitting field is contained in a radical extension of K.

Definition 4.2. A group G is solvable if it has a finite sequence of subgroups id = $H_0 \subset H_1 \subset H_2 \subset ... \subset H_k$ = G;where for each 0 ≤ i ≤ k; H_i is normal in H_{i+1} and H_{i+1} / H_i is Abelian.

The use of the Galois group in understanding polynomials is that a given polynomial is solvable by radicals if and only if its corresponding Galois group is solvable.

This allows us to easily answer the question of the solvability of the quintic (and higher) polynomial equation. It is a theorem that for all n ≥ 5; the Galois group of the general polynomial of degree n is isomorphic to $S_[n]$; and, therefore, not solvable. This is not to say that there may exist radical solutions to some n degree polynomials whose coefficients are related in some special way. It is very important to realize that, although Galois theory is a powerful tool inasmuch as it can tell us whether or not a given polynomial is solvable by radicals, it does not say anything about how to solve a polynomial by radicals.Given the specific polynomial $x^2 + 3x + 4$ over the field of rational numbers Q, from the quadratic formula for its roots we know that its roots are $(-3 \pm \sqrt{-7})/2$ thus the field Q($\sqrt{-7}$)i is the splitting field of $x^2 + 3x + 4$ over Q . Consequently there is an element y = $\sqrt{-7}$ in Q such that the extension field Q(ω) where ω^2 = y is such that it contains all the roots of $x^2 + 3x + 4$.

From a slightly different point of view, given the general quadratic polynomial p(x) = $x^2 - 3x + 4$ over F, we can consider it as a particular polynomial over the field F(a_1, a_2)of rational functions in the two variables a_1,a_2 over F ; in the extension obtained by adjoining ω to F(a_1, a_2).Here ω^2=a_1^2-4a_2 ∈F(a_1,a_2), We find all roots of p(x).There is a formula which expresses the roots of p(x) in terms of a_1,a_2 square roots of rational functions of these.
For cubic equation p(x) = x^3-a_1x^2+a_2x+a_3 a an explicit formula can be given, involving combinations of square roots and cube roots of rational functions in a_1, a_2, a_3 .

They are explicitly given by Cardan's formulas: Let $p = a_2 - ((a_1^2)/3)$ and $q = \frac{2a_1^3}{27} - \frac{a_1a_2}{3} + a_3$.

$$p = \sqrt[3]{\frac{-q}{2} + \sqrt{\frac{p^3}{27} + \frac{q^2}{4}}}$$

and let

$$q = \sqrt[3]{\frac{-q}{2} + \sqrt{\frac{p^3}{27}+}} - \frac{q^2}{4}$$

Then the roots are P+Q$-(a_1/3)$,ωP+ω^2Q-$a_1/3$ and ω^2p+ωQ - $a_1/3$, where $\omega \neq 1$ ω is a cube root of 1.

The above formulas only serve to illustrate for us that by adjoining a certain square root and then a cube root to F(a_1, a_2, a_3),we reach a field in which p(x) has its roots.
For fourth-degree polynomials, which we shall not give explicitly, by using rational operations and square roots, we can reduce the problem to that of solving a certain cubic, so here too a formula can be given expressing the roots in terms of combinations of radicals of rational functions of the coefficients.
For polynomials of degree five and higher, no such universal radical formula can be given, for we shall prove that it is impossible to express their roots, in general, in this way.

Example 4.3. $f(x) = x^3 - 2$

1. Zeros: $2^{1/3}, 2^{1/3}\omega, 2^{1/3}\omega^2$.
2. Splitting field = F = $Q[2^{1/3}, 2^{1/3}\omega, 2^{1/3}\omega^2] = Q[2^{1/3}, \omega]$.
3. The minimum polynomial of $2^{1/3}$ is $x^3 - 2$. Thus $|Q[2^{1/3}] : Q| = 3$.
4. The minimum polynomial for w over Q is $x^2 + x + 1$ and over $Q[2^{1/3}]$ it is the same.
5. $|F : Q| = 6[= |F : Q[2^{1/3}]||Q[2^{1/3}] : Q| = 2 \times 3]$
6. The Galois group has order 6.
7. Possible automorphisms:

$$2^{1/3} \to 2^{1/3}, 2^{1/3}\omega, 2^{1/3}\omega^2 and$$
$$w \to \omega or \omega^2,$$

   giving six combinations.

8. All 6 combinations arise. [since $|F : Q| = 6$]