Central Department of Mathematics, TU

Applications of Galois Theory

Presenter:

Mr. Sandesh Thakuri

Roll no: 43

Supervisor:

Asoc. Prof. Tulasi Prasad Nepal

2080-12-24

Outlines

Background

Let F be a field extension of a field K.

1. K-automorphism

A field-automorphism $\sigma \in AutF$ which is also K-homomorphism is called K-automorphism. In other words, a field-automorphism $\sigma \in AutF$ that fixes K element-wise is called K-automorphism [3].

2. Galois Group

The group of all K-automorphisms of F is called the Galois group of F over K and it is denoted by Aut_K^F [3].

3. Galois Extension

Let F be an extension field of K such that the fixed field of the Galois group Aut_K^F is K itself. Then F is said to be a Galois extension of K or Galois over K [3].

Fixed Field

Let E be an intermediate field and H be a subgroup of Aut_K^F, then:

i) $H' = \{v \in F \mid \sigma(v) = v, \text{ for all } \sigma \in H\}$ is an intermediate field of the extension field F of K;

ii) $E' = \{\sigma \in Aut_K^F \mid \sigma(u) = u, \text{ for all } u \in E\} = Aut_E^F$ is a subgroup of Aut_K^F.

The field H' is called the fixed field of the subgroup H in F [3].

4. Fundamental Theorem of Galois Theory

If F is a finite dimensional Galois extension of K, then there is a one-to-one correspondence between the set of all intermediate fields of F over K and the set of subgroups of the Galois group Aut_K^F such that:

i) *the relative dimension of two intermediate fields is equal to the relative index of the corresponding subgroups. In particular Aut_K^F has order $[F : K]$;*

ii) *F is Galois over every intermediate field E, but E is Galois over K if and only if the corresponding subgroup $E' = Aut_E^F$ is normal in $G = Aut_K^F$.In this case G/E' is isomorphic to the Galois group Aut_K^E of E over K [3].*

Illustration of The Fundamental Theorem

Let F be an Galois extension of a field K. Let the towers of the intermediate fields of F over K be as follows:

$$K \subset E \subset F$$

Let G be the Galois group of F over K. Then its subsets are

$$\{e\} \subset H \subset G$$

Then the one-to-one correspondence is as shown:

Galois-correspondence

$$\begin{tikzcd}
F \arrow[r, leftrightarrow] \arrow[d] & \{e\} \\
E \arrow[r, leftrightarrow] \arrow[d] & H \arrow[u] \\
K \arrow[r, leftrightarrow] & G \arrow[u]
\end{tikzcd}$$

5. Remark

The intermediate fields are getting larger as we go from top to bottom as the fields are getting extended. But the subgroups are getting smaller.

Proof

We already have a correspondence between the intermediate fields and the subgroup of Galois group.
That is to each intermediate field E, there is a subgroup Aut_E^F and to each subgroup H there is a fixed field H'. But this correspondence is one-to-one if and only if for each intermediate field E, it satisfies $E'' = E$ and for each subgroup H, it satisfies $H'' = H$.

6. Closed Field or Closed Subgroup

Let X be an intermediate field or subgroup of the Galois group. X will be called **closed** provided $X = X''$ [3].

7. Galois Lemma

i) *If F is an extension field of K, then there is one-to-one correspondence between the closed intermediate fields of the extension and the closed subgroups of the Galois group, given by $E \to E' = Aut_E^F$ [3].*

ii) *If F is a finite dimensional Galois extension of K, then all intermediate fields and all subgroups of the Galois group are closed and Aut_K^F has order $[F : K]$ [3].*

Question

Galois extension F of K is a field for which the fixed field of the Galois group Aut_K^F is K itself.

Questions:

1. But for what extension field F of K the Galois group keeps the base field K fixed?
2. What is the structure of Galois field and how do we construct (obtain) a Galois field?

Since, for $F = K(u)$, any $\sigma \in Aut_K^F$ is completely determined by its action on u. Any algebraic Galois extension of K is generated by all roots u of a polynomial $f \in K[x]$.

Such a minimal field F where a polynomial $f \in K[x]$ splits into linear factors and thus contains all roots of $f(x)$ is called a splitting field of f over K [3].

Thus, an algebraic Galois extension is going to be characterized by a splitting field of a polynomial over the base field.

Example

The extension field $\mathbb{Q}(\sqrt{3})$ over the field $\mathbb{Q}$ is a Galois extension and it is also a splitting field of the polynomial $f(x) = x^2 - 3 \in \mathbb{Q}[x]$.

As, the roots of f are $\sqrt{3}$ and $-\sqrt{3}$ which are the generators of the field $\mathbb{Q}(\sqrt{3})$.

8. Galois Group

The Galois group of a polynomial $f \in K[x]$ is the group Aut_K^F, where F is a splitting field of f over K [3].

9. Characterization of Galois Groups

Let G be a Galois group of a polynomial $f \in K[x]$.

i) *G is isomorphic to a subgroup of some symmetric group S_n[3].*

ii) *If f is separable of degree n, the n divides $|G|$ and G isomorphic to a transitive subgroup of S_n [3].*

10. Corollary

i) *If the degree of f is 2 then its Galois group $G \cong \mathbb{Z}_2$.*

ii) *If the degree of f is 3 then its Galois group G is either S_3 or A_3 [3].*

11. Discriminant of a Polynomial

Let $f \in K[x]$ a polynomial of degree n with n distinct roots $u_1, u_2, ..., u_n$ in some splitting field F of f over K. Let $\Delta = \prod_{i<j}(u_i - u_j) = (u_1 - u_2)(u_1 - u_3)...(u_{n-1} - u_n) \in F$.
The discriminant of f is the element $D = \Delta^2$. [3].

12. Theorem

If f is a separable polynomial of degree 3, then the Galois group of f is A_3 if and only if the discriminant of f is the square of an element of K [3].

13. Resolvant Cubic of a Quartic

Let $u_1, u_2, ..., u_4$ be the roots of a quartic $f \in K[x]$ and
$\alpha = u_1u_2 + u_3u_4$, $\beta = u_1u_3 + u_2u_4$, $\gamma = u_1u_4 + u_2u_3$.

The polynomial $(x - \alpha)(x - \beta)(x - \gamma)$ is called the resolvant cubic of f. The resolvant cubic is actually a polynomial over K[3].

An Application of Fundamental Theorem

Now under "the Galois correspondence the subfield $K(\alpha, \beta, \gamma)$ corresponds to the normal subgroup $V \cap G$" [3] because $K(\alpha, \beta, \gamma)$ is a splitting field of the resolvant cubic whose Galois group is a subgroup of S_3 and only normal subgroup of N of S_4 with $|N| \leq 6$ is V, where
$V = \{(1), (12)(34), (13)(24), (14)(23)\}$.
Hence $K(\alpha, \beta, \gamma)$ is Galois over K and $Aut_K^{K(\alpha,\beta,\gamma)} = G/(G \cap V)$[3].

14. Theorem

Let K be a field and $f \in K[x]$ a separable quartic with Galois Group G. Let α, β, γ be the roots of the resolvant cubic of f and let $m = [K(\alpha, \beta, \gamma) : K]$ then,

i) $m = 6 \iff G = S_4$;

ii) $m = 3 \iff G = A_4$;

iii) $m = 1 \iff G = V$;

iv) $m = 2 \iff G = D_4$ or $G = \mathbb{Z}_4$; in this case $G = \mathbb{Z}_4$ if f is irreducible over $K(\alpha, \beta, \gamma)$ and $G = \mathbb{Z}_4$ otherwise[3].

15. Theorem

If p is a prime and f is an irreducible polynomial of degree p over $\mathbb{Q}$ which has precisely two nonreal roots, then the Galois group of f is S_p[3].

The polynomial is $f(x) = x^5 - 10x + 5 \in \mathbb{Q}[x]$. Its graph is shown below.

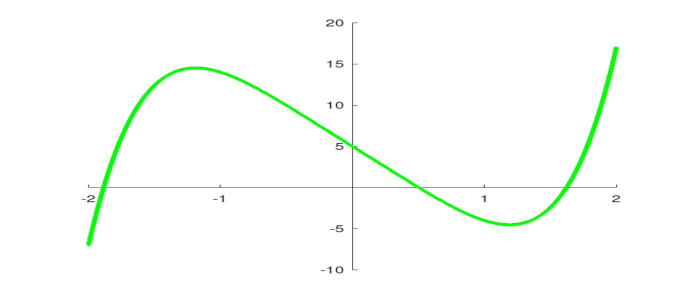

Figure: Plotted by the "GNU-Octave"

From its graph this polynomial has only three real roots. This polynomial is "irreducible over $\mathbb{Q}$ by the Eisenstein's criterion" [3] so by Theorem-15 its Galois group is S_5 which contains $5! = 120$ elements.

Galois Group of a seventh degree polynomial

The polynomial is $f(x) = x^7 - 2x^5 - 4x^3 + 2x^2 + 4x - 2$ which is "irreducible over $\mathbb{Q}$ by the Eisenstein's criterion" [3]. Its graph is shown below.

Figure: Plotted by the "Geogebra"

The Graph shows this polynomial has exactly five real roots. So exactly two of its roots are complex. Hence by the Theorem-15 its Galois Group is S_7 which contains $7! = 5040$ elements.

Galois Group of Multi-variable Polynomials

The Galois group of a polynomial in single variable can be generalized to the Galois group of a multi-variable polynomial.

If the polynomial is $f(x, y) = x + y \in \mathbb{Q}[x, y]$. Now the roots of f over all the complex numbers. Hence its Galois group is $\mathbb{C}$.

Example

The polynomials in $\mathbb{Q}[x, y]$ are:

$$y = x^2 + 1 \tag{1}$$

$$y = 1 - x \tag{2}$$

. The roots of these simultaneous polynomials are ω, ω^2. Then the splitting field of this system is $\mathbb{Q}(\omega)$. Here the automorphisms of $\mathbb{Q}(\omega)$ are:
$\omega \longmapsto \omega$ and $\omega \longmapsto \omega^2$.
Hence the Galois group of this system is $\{(1), (1, 2)\} \cong \mathbb{Z}_2$.

References

[1] J. P. Escofier. *Galois Theory*. Springer, New York:219-225,2000.

[2] G. R. Holdman. *Error Correcting Codes Over Galois Rings*. Graduate Dissertation, Department of Mathematics, Whitman college, 345 Boyer Ave. Walla Walla, Washington, U.S.A, 2019.

[3] T. W. Hungerford. *Algebra*. Springer (India), New Dheli, 2012.

[4] A. Lenstra, H. Lenstra, and L. Lovasz. Factoring polynomials with rational coefficients. *Mathematische Annalen*,261,12,1982.

[5] A. Neubaer and J. Freudenberger and V. Kuhn. *Coding Theory, Algorithms, Architectures, and Applications*. John Wiley and Sons Ltd, Chichester, West Sussex, England:1-93,2007.

[6] D. Sarma. Implementation of Galois Field for Application in Wireless Communication Channels. *MATEC Web of Conferences*,2010:03012,2018.

[7] National Institute of Standards and Technology. Advanced Encryption Standard (AES). *(Department of Commerce, Washington, D.C.), Federal Information Processing Standards Publication (FIPS) NIST FIPS*. 197-upd1, 2001. updated May 9, 2023. doi:10.6028/NIST.FIPS.197-upd1.