Applications of Galois Theory

Sandesh Thakuri

January 11, 2024

Contents

Part I

Galois Theory

Chapter 1

Field Extension

1.1 Structure of Field Extension

Let $F = K(u)$ be a field extension of the field K. Then F is a vector space over K generated by 'u'. So F consists of all linear combinations of 'u' and their quotients. A linear combinations of 'u'; $a_n u^n + a_{n-1}u^{n-1} + ... + a_1 u + a_0$ is given by the polynomial $f(u)$,where $f(x) = a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0$.

So the structure of the extension field $F = K(u)$ is:
$F = \{\frac{f(u)}{g(u)} | f, g \in K[x], g(u) \neq 0\}$.

1.1.1 Existence of Extension field

If K is a field and $f \in K[x]$ is a polynomial of degree n,then there exists a simple extension field $F = K(u)$ of K such that:

i) $u \in F$ is a root of f;

ii) $[K(u) : K] \leq n$, with equality holding if and only if f is irreducible in K[x];

iii) if f is irreducible in K[x], then K(u) is unique up to isomorphism which is the identity on K.

1.2 Algebraic and Transcendental element

From previous section we can deduce that $K[x]$ and $K[u]$ are homomorphic.

1. If u is transcendental over K then $K[u]$ is not a field and $K[x] = K[u]$.

2. If u is algebraic over K then, $K[x] \neq K[u]$ because $Ker\phi$ is not trival and we have,

   i) $K(u) = K[u]$;

   ii) $K(u) = K[x]/(f)$, where $f \in K[x]$ is an 'irreducible monic polynomial of degree $n \geq 1$;

   iii) $[K(u) : K] = n$ and $\{1_k, u, u^2, ..., u^{n-1}\}$ is a basis of the vector space $K(u)overK$.

1.3 Isomorphism of Extension fields

Let K be a field. Then 'u' and 'v' are roots of the same irreducible polynomial $f \in K[x]$ if and only if there is an isomorphism of fields $K[u] = Kp[v]$ which sends u onto v and is the identity on K.

Chapter 2

Galois Theory

2.1 Galois Group

Let F be a field. The set $AutF$ of all field-automorphisms $F \to F$ forms a group under the function composition.

Let E and F be extension fields of a field K. If nonzero field-homomorphism $\sigma : E \to F$ is a K-module homomorphism then
$\sigma(k) = \sigma(k1_E) = k\sigma(1_E) = k1_F = k$.
i.e, σ fixes K elementwise.

Conversely, if field homomorphism $\sigma : E \to F$ fixes K elementwise, then σ is a nonzero and for any $u \in E$,
$\sigma(ku) = \sigma(k)\sigma(u) = k\sigma(u)$ i.e σ is a K-module homomorphism.

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 elementwise is called K-automorphism.

The group of all K-automorphisms of F is called the Galois group of $FoverK$ and is denoted by Aut_K^F.

2.2 Galois extension

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

i) $H' = \{v \in F | \sigma(v) = v, forall\sigma \in H\}$ is an intermediate field of the extension field F of K.

ii) $E' = \{\sigma \in Aut_K^F | \sigma(u) = u, forallu \in E\} = Aut_E^F$ is a subgroup of Aut_K^F.

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

2.2.1 Fixed Field

We have,
$H' \to fixedfield \qquad E' \to Aut_E^F$
Let $Aut_K^F = G$ then the field fixed by it is G'.
It is not necessary that the field fixed by G is K i.e, $G' = K$.

Example
For $f(x) = x^3 - 2 \in Q[x]$. Let $u \in F$ such that $f(u) = 0$ and $F = Q[u]$.Then $G = Aut_Q^{Q(u)} = 1$ so, $G' = F \neq K$.

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 to be Galois over K.

2.3 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 the extension 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.

We already have a correspondence between the intermediate fields and the subgroup of Galois group given by the fixed fields and the corresponding subgroups of the intermediate field E, Aut_E^F. i.e, 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 $E'' = E$ and so on.

2.3.1 Closed Field and Subgroup

We have,

i) $F' = 1$ and $K' = G$;

ii) $1' = F$;

If F is Galois over K then by definition, $G' = K$. Since $K' = G$ we have $K = K''$ if and only if F is Galois over K.

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

Theorem. 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 $E \to E' = Aut_E^F$.

Lemma. Let F be an extension field of K, L and M intermediate fields with $L \subset M$, and H, J subgroups of Galois group Aut_K^F with $H < J$.

i) If L is closed and $[M : L]$ finite, then M is closed and $[L' : M'] = [M : L]$;

ii) if H is closed and $[J : H]$ finite, then J is closed and $[H' : J'] = [J : H]$;

iii) 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 $[F : K]$.

2.3.2 Stable Intermediate

Lemma. Let F be an extension field of K.

i) If E is a stable intermediate field of the extension, then $E' = Aut_E^F$ is a normal subgroup of the Galois group Aut_K^F;

ii) if H is a normal subgroup of Aut_K^F, then the fixed field H' of H is a stable intermediate field of the extension.

2.3.3 Proof of the Fundamental Theorem

From the above section there is one-to-one correspondence between closed intermediate fields of the extension and closed subgroups of the Galois group. But in this case all intermediate fields and all subgroups are closed. Thus follows Statement(i) of the theorem.

F is Galois over E since E is closed. E is finite dimensional over K since F is and hence algebraic over K. Consequently, if E is Galois over K, then E is stable. $E' = Aut_E^F$ is normal in Aut_K^F. Conversely if E' is normal in Aut_K^F, then E'' is

stable intermediate field. But $E = E''$ since all intermediate fields are closed and hence E is Galois over K.

Suppose E is an intermediate field that is Galois over K. Since E and E' are closed and $G' = K$(F is Galois over K), we have $|G/E'| = [G : E'] = [E'' = G'] = [E : K]$. So, $G/E' = Aut_K^F/Aut_E^F$ is isomorphic to a subgroup of Aut_K^F. But by first part of the theorem, $|Aut_K^E| = [E : F]$(since E is Galois over K). This implies $G/E' = Aut_K^E$.

Chapter 3

Structure of Galois Extension

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

3.1 Splitting Field

Since, for $F = K(u)$, any $\sigma \in Aut_K^F$ is completely determined by its action on u. So, the algebraic Galois extension is generated of all roots $u$of a polynomial. 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 a splitting field of f over K. And the algebraic Galois extension is to be characterized by the splitting field.

Existence of a Splitting field If K is a field and $f \in K[x]$ has degree $n \geq 1$, then there exists a splitting field F of f with $[F : K] \leq n!$.

3.1.1 Algebraic Closure of a Field

A field F is said to be algebraically closed in every nonconstant polynomial $f \in F[x]$ has a root in F. For,example the field of complex number C is algebraically closed.

An extension field F of a field K is said to be algebraic closure of K if,

i) F is algebraically closed and,

ii) F is algebraic over K.

So, C is algebraically closed field but is not an algebraic closure of Q because C is not algebraic over Q. But C is an algebraic closure of R.

This shows algebraic closure is an special case of a splitting field.

3.2 Separable Extension

An irreducible polynomial $f \in K[x]$ is said to be separable if in some splitting field of f over K every root of f is a simple root.

An algebraic element $u \in F$ is said to be separable over K provided its irreducible polynomial is separable. If ever element of F is separable over K, then F is said to be a separable extension of K.

Characteristic of a Separable extension
Every algebraic extension field of a field of characteristic 0 is separable.

It is clear that a separable polynomial $f \in K[x]$ has no multiple roots in any splitting field of f over K. This shows that an irreducible polynomial in $K[x]$ is separable if and only if its derivative is nonzero. Hence every irreducible polynomial is separable if $charK = 0$.

3.3 Galois extension

F is algebraic and Galois over K if and only if F is separable over K and F is a splitting field over K of a set S of polynomials in $K[x]$.

This proves the *Generalized Fundamental Theorem of Galois Theory*,
which sates the *Fundamental Theorem of Galois Theory* still holds if the extension field F is not finite dimensional as-well i.e, if F is algebraic and Galois over K.

Part II

Applications

Chapter 4

Galois Group of a Polynomial

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.

Theorem 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..

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

So, the Galois group of polynomial is identified with the subgroup of S_n.

Corollary

i) If the degree of f is 2 then the Galois group $G = Z_2$.

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

4.1 Galois group of cubic polynomials

Discriminant of f

hspace3mm Let K be a field with $charK \neq 2$ and $f \in K[x]$ 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 $D = \Delta^2$.

Theorem

i) The discriminant Δ^2 of f actually lies in K.

ii) For each $\sigma \in Aut_K^F < S_n, \sigma$ is an even[resp. odd] if and only if $\sigma(\Delta) = \Delta$[resp. $\sigma(\Delta) = -\Delta$].

Because the $\Delta^2 \in K$ and $\Delta \in F$, in the Galois correspondence the subfield $K(\Delta)$ corresponds to the subgroup $G \cap A_n$. In particular, G consists of even permutations if and only if $\Delta \in K$.

Corollary 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.

Theorem Let K be a field of $charK \neq 2, 3$. If $f(x) = x^3 + bx^2 + cx + d \in K[x]$ has three distinct roots in some splitting field, then the polynomial $g(x) = f(x - b/3) \in K[x]$ has the form $x^3 + p^2 + q$ and the discriminant of f is $-4p^3 - 27q^2$.

Theorem Let $K, f, F, u_i, V, andG = Aut_K^F < S_4$ be as in the preceding paragraph.
If $\alpha = u_1u_2 + u_3 + u_4, \beta = u_1u_3 + u_2 + u_4, \gamma = u_1u_4 + u_2 + u_3$, then under the Galois correspondence the subfield $K(\alpha, \beta, \gamma)$ corresponds to the normal subgroup $V \cap G$. Hence $K(\alpha, \beta, \gamma)$is Galois over K and $Aut_K^{K(\alpha,\beta,\gamma)} = G/(G \cap V$.

4.1.1 Resolvant Cubic of Quartic

The elements α, β, γ play a crucial role in determining the Galois Groups of arbitrary quartics. The polynomial
$(x - \alpha)(x - \beta)(x - \gamma)$ is called the resolvant cubic of f.
The resolvant cubic is actually a polynomial over K.

Theorem If K is a field and $f = x^4 + bx^3 + cx^2 + dx + e \in K[x]$, then the resolvant cubic of f is the polynomial $x^3 - cx^2 + (bd - 4e)x - b^2e + 4ce - d^2 \in K[x]$.

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) $m = 6 \Longleftrightarrow G = S_4$;

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

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

iv) $m = 2 \iff G = D_4$ or $G = Z_4$; in this case $G = Z_4$ if f is irreducible over $K(\alpha, \beta, \gamma)$ and $G = Z_4$ otherwise.