Galois Theory (M.Sc. Sem-IV)

By : Shailendra Pandit

Guest Assistant Prof. of Mathematics

P.G. Dept. Patna University, Patna

Email : sksuman1575@gmail.com
Call : 9430974625

Introduction :– Let $p(x) \in F[x]$ be a polynomial over the field F in x then Galois group is nothing but the group of permutations of the roots of $p(x)$.

Before playing Galois group we should aware with splitting field of field F there after we define Galois group as the group automorphism over splitting field and the so many result will come into light as relationship between subgroups of Galois group and subfields of splitting field. Now we shall put our concentration first on splitting field & automorphism.

Splitting field : Let $p(x) \in F[x]$ be apolynomial in x on F then splitting field of $p(x)$ is nothing but the field K such that $p(x)$ can be factored linearly in K and $F \subseteq K$.

e.g.,

$x^2 - 3 \in Q(x)$: Q is set of rationals

$x^2 - 3$ can be factored linearly as $\left(x-\sqrt{3}\right)\left(x+\sqrt{3}\right]$ into $Q\left(\sqrt{3}\right)$

thus $Q\left(\sqrt{3}\right)$ is a splitting field of Q

where $Q\left(\sqrt{3}\right) = \left\{a + b\sqrt{3} : a, b \in Q\right\}$

Automorphism :– Let K be a field then an automophism ϕ on K means an isomorphism from K to K.

or $\phi(a+b) = \phi(a) + \phi(b)$ and $\phi(ab) = \phi(a)\phi(b)$

* $a, b \in K$

two automprhisms ϕ and ψ as different

iff $\phi(a) = \psi(a)$ for some $a \in K$.

Definition :

Fixed field :– If G is a group of automorphisms of K, then the fixed field of G is the set of all elements $\in K$ such that $\phi(a) = a \ \forall \ \phi \in G$

Note : $G(K, F) =$ Group of automorphisms of K leaving every element of F fixes.

Theorem (1.1) :

The fixed field of G is a subfield of K.

Proof :

Let $a,$ & $b \in F$ where F is fixed field of G

thus

$\phi(a) = a \ \forall \ \phi \in G$

$\phi(b) = b \ \forall \ \phi \in G$

But $\phi(a \pm b) = \phi(a) \pm \phi(b) = a \pm b$

$\Rightarrow \ a \pm b \in F$

& $\phi(ab) = \phi(a)\phi(b) = ab$

$\Rightarrow \quad ab \in F$

Again

$$\phi\left(a^{-1}\right)=\left[\phi(a)\right]^{-1}=a^{-1} \ \forall \ a \neq 0$$

$\Rightarrow \quad a^{-1} \in F$

$\Rightarrow \quad F$ is subfield of K.

Theorem (1.2)

$G(K, F)$ is a subroup of the group of all automorphisms of K.

Proof : As we know

$G(K, F)=$ Group of automorphism of K.

Relative to F and fixes the elements of F and let G be the group of all automorphisms of K.

Let ϕ & $\psi \in G(K, F)$

$\Rightarrow \quad \phi(a)=a; \ \psi(a)=a \ \forall \ a \in F$

Now,

if $\quad a \in F$

$$(\phi\psi)(a)=\phi\left[\psi(0)\right]=\phi(a)=a$$

$\Rightarrow \quad \phi\psi \in G(K, F)$

and $\phi=\phi^{-1} \in G(K, F)$

$\Rightarrow \quad G(K, F)$ is subgroup of G.

Example (1.1) :

Let K be the field of complex numbers and R be field of real.

Compute $G(K, R):-$

Solution :- If ϕ is a automorphism of K

then $\phi\left(i^2\right)=\phi(-1)=-1=\left[\phi(i)\right]^2$

$\Rightarrow \quad \phi(i)=i$ or -1

If ϕ leaves every element of R fixed.

then,

$$\begin{aligned}\phi(a+ib)&=\phi(a)+\phi(i)\phi(b)\\&=a+\phi(i)b\\&=(a+ib) \text{ or } (a-ib)\end{aligned}$$

$\Rightarrow$ there are only two automorphisms are possible.

$\phi_0(a+ib)=a+ib \quad (\text{Identity})$

& $\quad \phi(a+ib)=a-ib \ (\text{conjugate})$

which fixes the real numbers.

$G(K, R)=\{\phi_0, \phi\}$

fixed field of $G(K, R)=R$.

Example (1.2)

Let Q be the field of rationals and $K = Q\left(\sqrt[3]{2}\right)$ where $\sqrt[3]{2}$ is real cube root of 2.

with $K = \left\{a + b\sqrt[3]{2} + c\left(\sqrt[3]{2}\right)^2 : a,\ b,\ \&\ c \in Q\right\}$

then find $G(K, Q)$

Solution :- Let ϕ be an automorphism of K.

$\Rightarrow \quad \phi\left(\sqrt[3]{2}\right)^3 = Q(2) = 2$

$\phi\left(\sqrt[3]{2}\right) =$ cube root of $2 \in K$.

$\phi\left(\sqrt[3]{3}\right) =$ real cube root of 2 $\{\because K \subset \mathbb{R}\}$

$\phi\left(\sqrt[3]{2}\right) = \sqrt[3]{2}$

Hence,

$$\phi\left(a + b\sqrt[3]{2} + c\left(\sqrt[3]{2}\right)^2\right) = \phi(a) + \phi(b)\phi\left(\sqrt[3]{2}\right) + \phi(c)\phi\left(\sqrt[3]{2}\right)^2$$

$$= a + b\sqrt[3]{2} + c\left(\sqrt[3]{2}\right)^2$$

$\Rightarrow \quad \phi$ is identify automorphism (only possible).

Hence, $G(K, Q) = \{\phi_0\}$

<u>fixed field of *G*(*k*, *Q*)</u>

Since ϕ_0 is identity automorphis thus fixed field of $G(K, Q)$ is not Q but all of K.

<u>Exercises :</u>

(i) Find $G\left(\mathbb{R}, Q\left(\sqrt{2}\right)\right)$

(ii) Find $G(Q(w), Q)$: where w is non-real cube root of unity.

(iii) Compute $G(Q(w), Q)$: where w is non-real fifth root of unity.

Results :-

(*) Each of $G(K, F)$ computed above is cyclic.

(**) A highly important result is that in general $G(K, F)$ need not be abelian.