Field Permutation and Automorphism of Roots

Dr. Rajiva Dixit

Department of Mathematics,

B. S. N. V. P. G. College, Lucknow, U. P., India

Email: dixit.rajiva@gmail.com

Abstract

The purpose of this research paper is to illustrate the theoretical concept of Galois Theory in the form of numerical illustration of field permutation and automorphism under composition By looking at the effect of a Galois group on field generators we can interpret Galois group as permutations, which makes it a subgroup of a symmetric group . This makes Galois groups into relatively concrete and numerical and is particularly effective when the Galois group turns out to be a symmetric or alternative group .

FIELDS AUTOMORPHISM WITH RESPECT TO ROOTS

The Galois group of a polynomial f (X) ε K [X] is defined to be the Galois group of a splitting field for f (X) over K. We do not need f (X) to be irreducible in K (X).

Example : 2.1 The polynomial $X^4 - 2$ has splitting field $Q(\sqrt[4]{2}, i)$ over Q .

So the Galois group of $X^4 - 2$ over Q is isomorphic to D_4.

The splitting field of $X^4 - 2$ over R is C, so the Galois group of $X^4 - 2$ over R is

$Gal(C/R) = \{ z \to z, \ z \to \bar{z} \}$, which is cyclic of order 2 .

Example 2 .2 Consider the polynomial $f(X) = X^4 - 2$ over Q We will construct

Its Galois group. f (x) has four roots

$\sqrt[4]{2}$, $i\sqrt[4]{2}$, $-\sqrt[4]{2}$, $-i\sqrt[4]{2}$.

Splitting field is $Q(\sqrt[4]{2}, i)$. Its degree is 4. The mappings of $\sqrt[4]{2}$ and i are:

$\sqrt[4]{2} \to \pm\sqrt[4]{2}$

and $i \to \pm i$

$\sqrt[4]{2} \to \pm i\sqrt[4]{2}$

Now we construct their permutations, as under

$$i = \begin{pmatrix} \sqrt[4]{2} & i \\ \sqrt[4]{2} & i \end{pmatrix} \qquad D = \begin{pmatrix} \sqrt[4]{2} & i \\ \sqrt[4]{2} & -i \end{pmatrix}$$

$$A = \begin{pmatrix} \sqrt[4]{2} & i \\ -\sqrt[4]{2} & i \end{pmatrix} \qquad E = \begin{pmatrix} \sqrt[4]{2} & i \\ i\sqrt[4]{2} & -i \end{pmatrix}$$

$$B = \begin{pmatrix} \sqrt[4]{2} & i \\ i\sqrt[4]{2} & i \end{pmatrix} \qquad F = \begin{pmatrix} \sqrt[4]{2} & i \\ -\sqrt[4]{2} & -i \end{pmatrix}$$

$$C = \begin{pmatrix} \sqrt[4]{2} & i \\ -i\sqrt[4]{2} & i \end{pmatrix} \qquad G = \begin{pmatrix} \sqrt[4]{2} & i \\ -i\sqrt[4]{2} & -i \end{pmatrix}$$

Second approach of writing the above permutation is

Automorphism	i	A	B	C	D	E	F	G
Value on $\sqrt[4]{2}$	$\sqrt[4]{2}$	$i\sqrt[4]{2}$	$-\sqrt[4]{2}$	$-i\sqrt[4]{2}$	$\sqrt[4]{2}$	$i\sqrt[4]{2}$	$-\sqrt[4]{2}$	$-i\sqrt[4]{2}$
Value on i	i	i	i	i	$-i$	$-i$	$-i$	$-i$

Table 1

The effect of mapping (m) on the roots of $f(x) = x^4 - 2$ is
$m(\sqrt[4]{2}) = i\sqrt[4]{2}$, $m(i\sqrt[4]{2}) = -\sqrt[4]{2}$, $m(-\sqrt[4]{2}) = -i\sqrt[4]{2}$)

$m(-i\sqrt[4]{2}) = \sqrt[4]{2}$. It is a 4 – cycle. The effect of the mapping (n) on the roots of $f(x) = x^4 - 2$ is,

$n(\sqrt[4]{2}) = \sqrt[4]{2}$, $n(i\sqrt[4]{2}) = -i\sqrt[4]{2}$, $n(-i\sqrt[4]{2}) = i\sqrt[4]{2}$

$n(-\sqrt[4]{2}) = -\sqrt[4]{2}$. This map (n) swaps $i\sqrt[4]{2}$ and $-i\sqrt[4]{2}$, while fixing $\sqrt[4]{2}$ and $-\sqrt[4]{2}$. So n is a 2 – cycle on roots.
Renaming the roots of $f(x) = x^4 - 2$ as:

2.1 $r_1 = \sqrt[4]{2}$, $r_2 = i\sqrt[4]{2}$, $r_3 = -\sqrt[4]{2}$, $r_4 = -i\sqrt[4]{2}$

The mapping / automorphism (m) acts on the roots like (1234) and the automorphism (n) Acts on the roots like (12) . With the indexing (renaming) of the roots , the Galois group of $f(x) = x^4 - 2$ over Q becomes the group of permutations in S_4 in the following table , It is isomorphic to S_4.

Automorphism	1	r	r^2	r^3	s	r s	r^2s	r^3s
Permutation	(1)	(1234)	(13)(24)	(1432)	(24)	(12)(34)	(13)	(14)(23)

Table 2

Example 2.4. Consider the polynomial $f(x) = (x^2 - 2)(x^3 - 3)$
Its roots / zeros are
$r_1 = \sqrt{2}$, $r_2 = -\sqrt{2}$, $r_3 = \sqrt{3}$, $r_4 = -\sqrt{3}$.

Then the Galois group of $(x^2 - 2)(x^3 - 3)$ over Q becomes the following subgroups of S_4.

(2.2) (1), (12), (34) , (12)(34) .

Renaming the roots of f (x) in different ways can identify the Galois group with different subgroups of S_n.

Example 2.5 Renaming $\sqrt[4]{n}$, $i\sqrt[4]{2}$, $-\sqrt[4]{n}$, $-i\sqrt[4]{n}$
In this order such as r_2, r_4, r_3, r_1 identifies the Galois group of $x^4 - 2$ Over Q with the subgroup of S_4 in the following table 3 , which is not the same subgroup of S_4 in the above problem .

Automorphism	1	r	r^2	r^3	s	rs	r^2s	r^3s
Permutation	(1)	(1243)	(14)(23)	(1342)	(14)	(13)(24)	(23)	(12)(34)

Table 3

Example 2. 6: If we label $\sqrt{2}$, $-\sqrt{2}$, $\sqrt{3}$, $-\sqrt{3}$ in this order such as r_2, r_4, r_1, r_3 then the Galois group of $(x^2 - 2)(x^2 - 3)$ over Q comes into the following subgroup of S_4.

(2,3) (1), (13), (24) , (13)(24) .

This is not the same subgroup as (2.2)

General Technique:

(1) In general , associating to each mapping (r) in the Galois group of f (X) over K its permutation on the roots of f (X) , viewed as a permutation of the subscripts of the roots when we list them as r_1, r_2, r_3, …….r_n is a homomorphism from the Galois group to S_n. This homomorphism is injective since its kernel is trivial an element of the Galois group that fixes every r_I is the identity on the splitting field.

This technique about the Galois group of a polynomial with degree n as a subgroup of S_n is the original viewpoint of Galois [1] (The description of Galois theory in terms of field automorphisms is due to Dedkind [2] , with more abstraction , Artin [3].

2. Two different choices for labeling the roots of f (X) can lead to different Subgroups of S_n. , but they will be conjugate subgroups. For instance, the subgroups

in tables 2 and 3 are conjugate by the permutation $\begin{pmatrix} 1234 \\ 2431 \end{pmatrix} = (124)$

Which is the permutation turning one indexing of the roots into the other, and the subgroups (2.2) and (2.3) are conjugate by $\begin{pmatrix} 1234 \\ 2413 \end{pmatrix} = (1243)$

We can speak about Galois groups of irreducible or reducible polynomials , like $X^4 - 2$ or $(x^2 - 2)(x^2 - 3)$ over Q Galois group of irreducible polynomials has a special property , called " transitivity property " . It is when Galois group is subgroup of S_p. (p is prime) A subgroup; $G < S_n$ is called transitive when, for any $i \neq j$.
In { 1 , 2 , 3 , ……..n } , there is permutation in G sending i to j .

Example 2.7 The subgroups of S_4 in table 2 and 3 are transitive. This corresponds to the fact that for any two roots of $T^4 - 2$ there is an element of its Galois group over Q taking the first root for the second .

Example 2.8 : The subgroup of S_4 in $(x^2 - 2)(x^2 - 3)$ is not transitive since no element of the subgroup takes 1 to 3 . This corresponds to the fact that an element of $G(\sqrt{2}, \sqrt{3})$ cannot send $\sqrt{2}$ to $\sqrt{3}$.

Being transitive is not a property of an abstract group. It is property of S_n. A conjugate subgroup of a transitive subgroup of S_n is also transitive since conjugation on S_n. Amounts to listing the numbers from1to n in a different order.

Now we illustrate the following theorem by giving numerical examples with their solutions.

Theorem:

Let $f(T) \in K[T]$ be a separable polynomial of degree n

(a) If f (T) is irreducible in K [T] then its Galois group over K has order divisible by n.

(b) The polynomial f (T) is irreducible in K [T] if and only if its Galois group over K is a transitive subgroup .

Example (a) : Let $f(x) = x^4 - 3x^2 - 10 = (x^2 - 5)(x^2 + 2)$

Its zeros are $x = \pm\sqrt{5}$, $\pm i\sqrt{2}$

Extension field = $Q[\sqrt{5}, i\sqrt{2}]$

Degree = 4

Possible automorphisms are $\sqrt{5} \to \sqrt{5}$

$\to -\sqrt{5}$

$i\sqrt{2} \to i\sqrt{2}$

$\to -i\sqrt{2}$

In detail all permutations /automorphisms are:

$e = \begin{pmatrix} \sqrt{5} & i\sqrt{2} \\ \sqrt{5} & i\sqrt{2} \end{pmatrix}$ Order = 1

$A = \begin{pmatrix} \sqrt{5} & i\sqrt{2} \\ \sqrt{5} & -i\sqrt{2} \end{pmatrix}$ Order = 2

$B = \begin{pmatrix} \sqrt{5} & i\sqrt{2} \\ -\sqrt{5} & i\sqrt{2} \end{pmatrix}$ Order = 2

$AB = \begin{pmatrix} \sqrt{5} & i\sqrt{2} \\ -\sqrt{5} & -i\sqrt{2} \end{pmatrix}$ Order = 2

Galois Group = $\langle I, A, B, AB \rangle$ order of Galois group =4

The subgroups are I, $\langle A \rangle$, $\langle B \rangle$, $\langle AB \rangle$. The corresponding subgroups and subfields along with their orders are in the following table

SUBGROUPS	NORMAL	ORDER	SUBFIELDS	POLYNOMIALS	DEGREE
G	√	4	Q	Q	1
$\langle A \rangle$	√	2	$Q[\sqrt{5}]$	$Q[x^2 - 5]$	2
$\langle B \rangle$	√	2	$Q[i\sqrt{2}]$	$Q[x^2 + 2]$	2
$\langle AB \rangle$	√	2	$Q[i\sqrt{10}]$	$Q[x^2 + 10]$	2
I	√	1	$Q[x^4 - 3x - 10]$	$Q[x^4 - 3x - 10]$	4

Order of each subgroup divides the order of order of Galois group i.e., 4/2 = 2

(b) The Galois group of the above polynomial is transitive , therefore the given polynomial is irreducible .

Example. (a) Consider the symmetric group S_3 . Its order is $|S_3| = 3.2.1 = 6$

Its permutations are

$e = I = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$ **C** $= \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$

$A = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ $D = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$

$$B = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \qquad E = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

Subgroups of S_3 are { I } its order is 1. It divides the order of S_3

(E, C) Its order is 2. It divides the order of S_3. i. e., 6/2 = 3

(e, D) Its order is 2, It divides the order of S_3. i. e., 6 / 2 = 3

(e, E) Its order is 2. It divides the order of S_3. i. e., 6 / 2 = 3.

Example 2 Consider the4 symmetric group S_4. Its order is = 4.3.2. 1 = 24

Its some few subgroups are:

{ e , (123) , (132) } . Its order is 3. It divides the order of S_4 .i.e. 24/3 = 8

{ e , (124) , (132) } . Its order is 3. It divides the order of S_4 i.e. 24 / 3 = 8

{E, (134), (143)} Its order is 3. It divides the order of S_4. i.e. 24 / 3 = 8

Other subgroups of S_4 are of orders 2 , 4 , 6 , 8 . All these orders divide the order of S_4 .

References

1. Ian Stewart : " Galois Theory " , Chapman and Hall , London , 1979.
2. Dedikind .J. W. R " Field of Rational Numbers and Real numbers ".
3. Artin E , " Galois Theory " Notre Dame . 1948.
4. Kaplansky , " Fields and Rings " , 2nd ed. Uny . of Chicago Press , Chicago .
5. P . Morandi . " Field and Galois Theory " Springer – Verlag, New York , 1996
6. https://kconrad.math.uconn.edu/blurbs/galoistheory/galoisapp.pdf
7. https://www.chegg.com/homework-help/questions-and-answers/show-irreducible-polynomial-x4-2-q-roots-b-c-splitting-field-fields-q-b-q-c-isomorphic-q-h-q36690561
8. https://sciencedocbox.com/Physics/68920290-Galois-groups-as-permutation-groups.html