Automorphism Groups:-

Let E be an extension of a field F $\left(\begin{smallmatrix}E\\|\\F\end{smallmatrix}\right)$ then the group of F- automorphisms of E denoted as $G(E/F)$ and which is the group of all automorphisms $\sigma: E \rightarrow E$ which leave each element of F fixed.

Results:- If E is a finite extension of a field F then $|G(E/F)| \leq [E:F]$

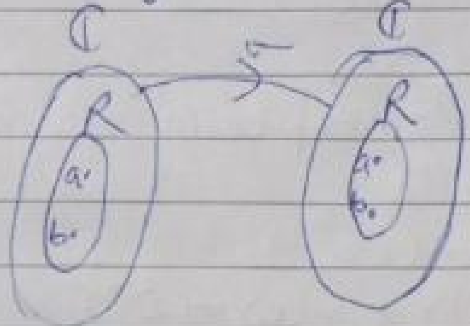
In general $o[G(E/F)] \le$ degree of extension $[E:F]$

Ex: Find (i) $G(\mathbb{C}/\mathbb{R})$

(ii) $|G(\mathbb{C}/\mathbb{R})|$

(iii) verify that $|G(\mathbb{C}/\mathbb{R})| \le [\mathbb{C}:\mathbb{R}]$

Solⁿ:



$\sigma : \mathbb{C} \to \mathbb{C}$

$\sigma(a+ib) = a+ib$

$\sigma(\cancel{z}) = \cancel{z}$

Let $a+ib \in \mathbb{C}$

$$\sigma(a+ib) = \sigma(a) + \sigma(ib) \qquad a,b \in R$$
$$= \sigma(a) + \sigma(i)\,\sigma(b)$$
$$= a + \sigma(i)\,b$$

Find $\sigma(i) = i, -i$

Trick $(i)^2 = -1$

$\sigma(i^2) = \sigma(i)\sigma(i) = \sigma(-1)$

$\sigma(i)\,\sigma(i) = -1$

$[\sigma(i)]^2 + 1 = 0$

$\sigma(i) = i, -i$

$\therefore \sigma(a+ib) = a+ib$

or $\sigma(a+ib) = a-ib$

$\therefore$ there are two automorphisms from $\mathbb{C} \to \mathbb{C}$

$\therefore$ (i) $G(\mathbb{C}/R) \cong \mathbb{Z}_2$

$G(\mathbb{C}/R) = \{\sigma_1, \sigma_2,\ \sigma_1(z) = z$

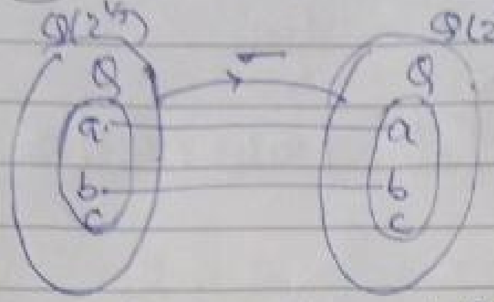
$\sigma_2(z) = \bar{z}\}$

(ii) $|G(\mathbb{C}/R)| = 2$

(iii) $|G(\mathbb{C}/R)| \le [\mathbb{C}:R]$

Q Consider the polynomial $x^3-2 \in \mathbb{Q}[x]$
find (i) $G[\mathbb{Q}(2^{1/3})/\mathbb{Q}]$

(ii) $|G[\mathbb{Q}(2^{1/3})/\mathbb{Q}]|$



$\mathbb{Q}(2^{1/3})$
| basis $\{1, 2^{1/3}, 2^{2/3}\}$
$\mathbb{Q} \to \mathbb{Q}[x] \supseteq (x^3-2)$ irreducible

$x = 2^{1/3} = a$
$a^0, a^1, a^2, \dots a^{n-1}$

Let σ be automorphism i.e $\sigma : \mathbb{Q}(2^{1/3}) \to \mathbb{Q}(2^{1/3})$

s.t. $\sigma(x+y) = \sigma(x)+\sigma(y)$
$\sigma(xy) = \sigma(x)\sigma(y)$

$\sigma(a+b2^{1/3}+c2^{2/3})$
$= \sigma(a)+\sigma(b2^{1/3})+\sigma(c2^{2/3})$
$= a+\sigma(b)\sigma(2^{1/3})+\sigma(c)\sigma(2^{2/3})$
$= a+b\,\sigma(2^{1/3})+c\,\sigma(2^{2/3})$ — ①
$= a+b(2^{1/3})+c2^{2/3}$

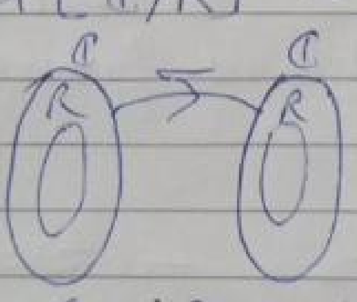
$\therefore$

$\sigma(x) = x$

$\therefore G[\mathbb{Q}(2^{1/3})/\mathbb{Q}] = \{\sigma : \mathbb{Q}(2^{1/3}) \to \mathbb{Q}(2^{1/3})$ s.t. $\sigma(x)=x\}$

$\because (2^{1/3})^3 = 2$
$\sigma(2^{1/3})^3 = \sigma(2)$
$[\sigma(2^{1/3})]^3 = 2$
$\sigma(2^{1/3}) = 2^{1/3}\cdot(1)^{1/3}$
$2^{1/3},\ 2^{1/3}\omega,\ 2^{1/3}\omega^2$
but over $\mathbb{Q}(2^{1/3})$
only one root.

Q $G[\mathbb{C}/\mathbb{R}] \cong \mathbb{Z}_2$



$a+ib = a(1)+b(i)$
$\forall a,b \in \mathbb{R}$

$\sigma(a+ib) = \sigma(1)a+\sigma(i)b$
$= a+b\,\sigma(i) \quad \forall a,b\in\mathbb{R}$

T.F. $\therefore$ $\sigma(i)$ decides the no of σ

$\sigma(i) = i$
$\sigma(i) = -i$

$\because i^2 = -1$
$\sigma(i^2) = [\sigma(i)]^2 = \sigma(-1)$
$\sigma(i)\sigma(i) = -1$
$\Rightarrow \sigma(i) = (-1)^{1/2}$
$(-1)i,\ (-1)(-i)$

$\therefore$ $\sigma(a+ib) = a+ib$
$\sigma(a+ib) = a-ib$
] two automorphisms $\therefore G[\mathbb{C}/\mathbb{R}] \cong \mathbb{Z}_2$

DATE : /

Fixed Field:

Let G be a group of automorphism of a field K then

$F_0 = \{ x \in K ; \sigma(x) = x \ \forall \sigma \in G \}$ is a subfield of K. F_0 is a fixed field under G.

Galois Extension

A finite extension K/F is said to be Galois extension of F if F is the fixed subfield of K under the group $G(K,F)$ of all F-automorphisms of K.

i.e

K/F is Galois Extension if $K_{G(K,F)} = F$

Results: