READING THE LATTICE DIAGRAM AND ITS MEANING

Group H_1 ———— Group H_2
(Line joining H_1 and H_2 signifies *index of H_1* in H_2)

Field K_1 ———— Field K_2
(Line joining K_1 and K_2 signifies *degree of K_2* over K_1)

DEFINITIONS

Let:

1. F = Field
2. E = extension field of F
3. $\varphi: E \to E$

If φ is an *isomorphism* then:

1. **φ** = *Automorphism of E*
2. **Gal(E/F)** = set of *all* automorphism of E *that* takes *every element* of F *to* itself
3. **E_H** = *fixed field of H*, where H is a subgroup of Gal(E/F)
   $= \{x \in E \mid \phi(x) = x, \ \forall \phi \in H\}$

- Set of automorphism of E forms a *group* under *composition!*
- Gal(E/F) group *is a* subgroup *of the* "automorphism group of E"
- E_H of H *is a* subfield of E

EXAMPLE 1

Suppose: F = Q, E = extension field of F = Q(√2)

Then:

- Any automorphism of a field containing Q must act as an identity on Q
- Any automorphism ϕ of E is completely determined by ϕ(√2)

$\therefore \quad 2 = \phi(2) = \phi(\sqrt{2}\sqrt{2}) = (\phi(\sqrt{2}))^2$

$\Rightarrow \quad \phi(\sqrt{2}) = \pm\sqrt{2}$

$\Rightarrow$ Gal(Q(√2)/Q) has two elements:

1. identity mapping
2. mapping that takes $(a + b\sqrt{2})$ to $(a - b\sqrt{2})$

EXAMPLE 2

Suppose: F = Q, E = extension field of F = $Q(\sqrt[3]{2})$

Then: Any automorphism ϕ of E is completely determined by $\phi(\sqrt[3]{2})$

Since $2 = \phi(2) = \phi(\sqrt[3]{2}\sqrt[3]{2}\sqrt[3]{2}) = (\phi(\sqrt[3]{2}))^3$

and $Q(\sqrt[3]{2}) \subset R$

$\therefore$ $\sqrt[3]{2}$ is the only *real cube root* of 2

$\Rightarrow \quad \phi(\sqrt[3]{2}) = \sqrt[3]{2}$ (identity automorphism)

$\Rightarrow$ Gal(E/F) has only one element

$\Rightarrow$ Fixed field of Gal(E/F) = $Q(\sqrt[3]{2})$

<u>EXAMPLE 3</u>

Suppose: $F = Q(i)$, E = extension field of $F = Q(\sqrt[4]{2}, i)$

Then: Any *automorphism* ϕ fixing $Q(i)$ is completely determined by $\phi(\sqrt[4]{2})$

Since $2 = \phi(2) = \phi((\sqrt[4]{2})^4) = (\phi(\sqrt[4]{2}))^4$

$\Rightarrow$ $\phi(\sqrt[4]{2}) = \sqrt[4]{2}$

$\Rightarrow$ *At most* 4 possible automorphisms of $Q(\sqrt[4]{2}, i)$ <u>fixing $Q(i)$</u>

<u>Let:</u> α be an *automormphism* such that:

$\alpha(i) = i$ *and*

$\alpha(\sqrt[4]{2}) = i\sqrt[4]{2}$

<u>Then:</u>

1. $\alpha \in Gal(E/F)$ *and*
2. order of $\alpha = 4$

$\Rightarrow$ $Gal(E/F)$ is a *cyclic group of order 4*

Fixed field of $\{e, \alpha^2\} = Q(\sqrt{2}, i)$

Lattice Diagram of Gal(E/F):

lattice of subgroups of Gal(E/F)		lattice of subfield of E containing F	
$\{e, \alpha, \alpha^2, \alpha^3\}$		E	
|	Index of a subgroup in the group above it = 2	|	Degree of E over the field below it = 2
$\{e, \alpha^2\}$		$Q(\sqrt{2}, i)$	
|	2	|	2
$\{e\}$		F	

lattice of subgroups of Gal(E/F) *lattice of subfield of E containing F*

<u>EXAMPLE 4</u>

Suppose $F = Q$, $E = Q(\sqrt{3}, \sqrt{5})$

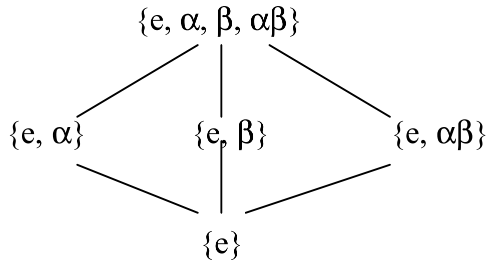
Since $Q(\sqrt{3}, \sqrt{5}) = \{a + b\sqrt{3} + c\sqrt{5} + d\sqrt{3}\sqrt{5} : a, b, c, d \in Q\}$

$\therefore$ Any *automorphism* ϕ is completely determined by: $\phi(\sqrt{3})$ *and* $\phi(\sqrt{5})$

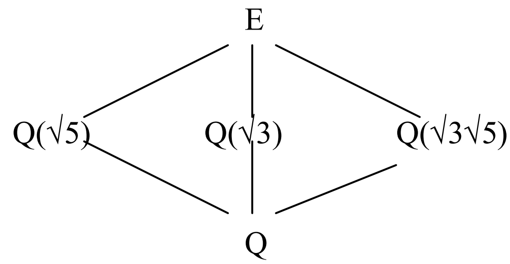
e	α	β	$\alpha\beta$
$\sqrt{3} \to \sqrt{3}$	$\sqrt{3} \to -\sqrt{3}$	$\sqrt{3} \to \sqrt{3}$	$\sqrt{3} \to -\sqrt{3}$
$\sqrt{5} \to \sqrt{5}$	$\sqrt{5} \to \sqrt{5}$	$\sqrt{5} \to -\sqrt{5}$	$\sqrt{5} \to -\sqrt{5}$

- $Gal(E/F) \approx Z_2 \oplus Z_2$
- Fixed Field of: (**)
  1. $\{e, \alpha\} = Q(\sqrt{5})$
  2. $\{e, \beta\} = Q(\sqrt{3})$
  3. $\{e, \alpha\beta\} = Q(\sqrt{3}\sqrt{5})$

*Lattice Diagram of Ex 4: (use result of ** on previous page)*



Lattice subgroups of Gal(E/F)



Lattice Subfields of E containing F

EXAMPLE 5: **SEE CLASS NOTES**

THEOREM 32.1 **Fundamental Theorem of Galois Theory** *(See Class Notes)*

EXAMPLE 6

Suppose $w = \cos(2\pi/7) + i\sin(2\pi/7) \Rightarrow w^7 = 1$ (*)

Let $F = Q(w)$

Then F = splitting field of $x^7 - 1$ *over* Q

∴ We can apply *Fundamental Theorem of Galois Theory*

By Calculation If: ϕ is an *automorphism*, s.t. $\phi(w) = w^3$

Then: $|\phi| = 6$ (**)

- $[F:Q] = |Gal(F/Q)|$ *By Thm 32.1*
  ≥ 6 *By (**)*

- $(x^7 - 1) = (x - 1)(x^6 + x^5 + x^4 + x^3 + x^2 + x + 1)$
  (*) $\Rightarrow$ w *is a* zero *of* $x^7 - 1$

  So: $|Gal(F/Q)| = [F:Q]$ *By Thm 32.1*
  ≤ 6

$\Rightarrow$ Gal(F/Q) = *Cyclic Group of Order 6*

$\Rightarrow$ Lattice Subgroup of Gal(F/Q) is trivial to compute

Then Q(w) contains *2 proper* extensions of Q:

1. Extension of degree 3 with fixed field = $\langle\phi^3\rangle$
2. Extension of degree 2 with fixed field = $\langle\phi^2\rangle$

➢ Fixed Field of $\langle\phi^3\rangle$ = Member in Q(w) *that is* not in Q *that is* fixed by ϕ^3

i.e. $(w + w^{-1})$ *is fixed* by ϕ^3 *and* $Q \subset Q(w + w^{-1}) \subseteq Q(w)_{\langle\phi 3\rangle}$

And Since: $[Q(w)_{\langle\phi 3\rangle} : Q] = 3$ and $[Q(w + w^{-1})_{\langle\phi 3\rangle} : Q]$ *divides* $[Q(w)_{\langle\phi 3\rangle} : Q]$

$\Rightarrow$ $Q(w + w^{-1}) = Q(w)_{\langle\phi 3\rangle}$

➢ Fixed Field of $\langle\phi^2\rangle = (w^3 + w^5 + w^6)$ *by similar argument as above*

➢ See Text Book for Lattice Diagram of this example **//end of page 553//**