

Def: The Galois group of a field extension E over a field F is

$$G(E/F) = \{ \sigma \in \text{Aut}(E) \mid \sigma(\alpha) = \alpha \quad \forall \alpha \in F \}$$

If $f(x) \in F[x]$, E = splitting field of $f(x)$ over F
 define the Galois group of $f(x)$ = $G(E/F)$

Ex] Consider $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{5}) \subseteq \mathbb{Q}(\sqrt{3}, \sqrt{5})$. For
 $a, b \in \mathbb{Q}(\sqrt{5})$

$\sigma(a + b\sqrt{3}) = a - b\sqrt{3}$ is an automorphism
 of $\mathbb{Q}(\sqrt{3}, \sqrt{5})$ leaving $\mathbb{Q}(\sqrt{5})$ fixed

So $\sigma \in (G(\mathbb{Q}(\sqrt{3}, \sqrt{5}) / \mathbb{Q}(\sqrt{5}))$ and

$\tau(a + b\sqrt{3}) = a + b\sqrt{3}$ leaves $\mathbb{Q}(\sqrt{3})$ fixed

$\tau \in G(\mathbb{Q}(\sqrt{3}, \sqrt{5}) / \mathbb{Q}(\sqrt{3}))$

The automorphism $\mu = \sigma \circ \tau$ moves both $\sqrt{5}$ and $\sqrt{3}$
 Can check that $\{\text{id}, \sigma, \tau, \mu\} \cong \mathbb{Z}_2 \times \mathbb{Z}_2$

Note everything fixes \emptyset

$$\therefore \{\text{id}, \sigma, \tau, \mu\} \subseteq G(\mathbb{Q}(\sqrt{3}, \sqrt{5}) / \mathbb{Q})$$

Can show

$$\{\text{id}, \sigma, \tau, \mu\} = G(\mathbb{Q}(\sqrt{3}, \sqrt{5})/\mathbb{Q})$$

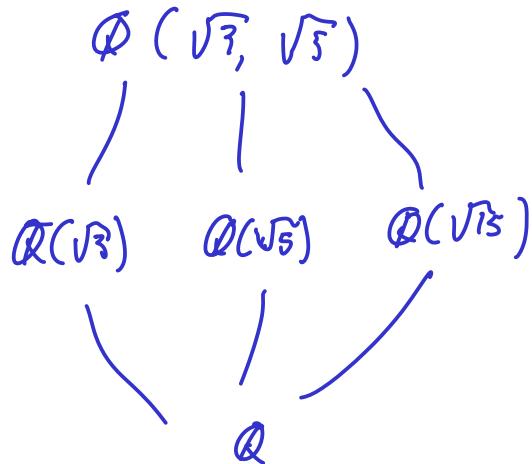
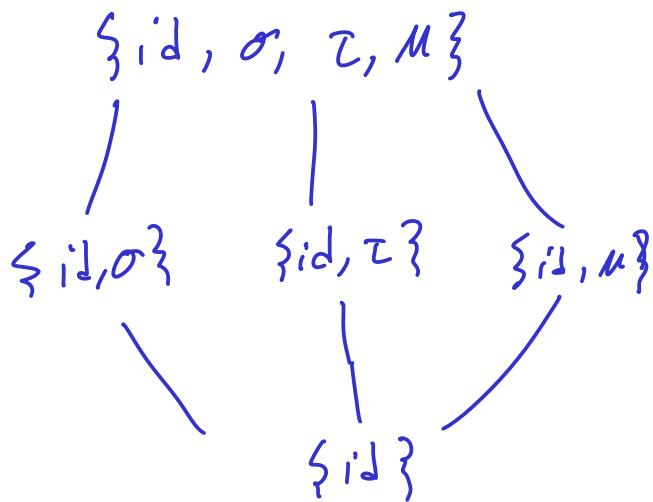
Note

$$|G(\mathbb{Q}(\sqrt{3}, \sqrt{5})/\mathbb{Q})| = 4 = [\mathbb{Q}(\sqrt{3}, \sqrt{5}):\mathbb{Q}]$$

||

$$[G(\mathbb{Q}(\sqrt{3}, \sqrt{5})/\mathbb{Q}) : \{\text{id}\}] = 4$$

$$[G(\mathbb{Q}(\sqrt{3}, \sqrt{5})/\mathbb{Q}) : \{\text{id}, \tau\}] = \frac{[\mathbb{Q}(\sqrt{5})/\mathbb{Q}]}{[\mathbb{Q}(\sqrt{3}, \sqrt{5}):\mathbb{Q}(\sqrt{3})]} = 2$$



Prop)

[E a field ext. of F , $f(x) \in F[x]$]

Then any automorphism in $G(E/F)$ defines a permutation of the roots of $f(x)$ that lie in E .

Mark Break down

$\sim 35-40\%$ fields

$\sim 30-35\%$ rings

$\sim 30\%$ groups

• 8-9 Questions

• All written

Allowed Notes

- Up to 10 single sided pages

- can be Lattered/typed
or hand written

Find an explicit finite field E with 27 elements.

Solution

$$27 = 3^3$$

know that $E \cong GF(3^3)$

we would expect a degree 3 field extension of $\mathbb{Z}/3\mathbb{Z}$

[General Fact : $[GF(p^n) : \mathbb{Z}_p] = n$]

with basis $\{1, \alpha, \alpha^2\}$

Since all finite extensions of finite field are finite and simple
 $\therefore E \cong \mathbb{Z}_3(\alpha)$

Let $p(x) = x^3 - x^2 + x + 1$, $p(x)$ is irreducible

over \mathbb{Z}_3 since $p(0) = 1$, $p(1) = 2$, $p(2) = 1$

[If $p(x)$ factored over \mathbb{Z}_3 it must have at least 1 linear factor]

Let α be a root of $p(x)$

$$\mathbb{Z}_3(\alpha) \cong \mathbb{Z}_3[x]/\langle x^3 - x^2 + x + 1 \rangle$$

This is our field with 27 elements

$$\mathbb{Z}_3(\alpha)^* \cong \mathbb{Z}_{26}^* \cong \langle \alpha \rangle$$

Is $\mathbb{Z}_2[x]/\langle x^3 + x + 1 \rangle \stackrel{p(x)}{\cong} \mathbb{Z}_2[x]/\langle x^3 + x^2 + 1 \rangle \stackrel{g(x)}{\cong} GF(2^8)$

If $p(x), g(x)$ are irreducible then both are $\cong GF(2^8)$

$$p(0) = 1$$

$$g(0) = 1$$

$$p(1) = 1$$

$$g(1) = 1$$

Ex] Let K be a finite extension of F s.t.

$[K:F] = p$ is prime. If $u \in K - F$ show that $K = F(u)$.

Proof:

$$F \subseteq F(u) \subseteq K$$

$$u \notin F \quad \therefore F \neq F(u)$$

$$[F(u):F] > 1$$

[Fact: If $[F(\alpha):F] = 1 \Rightarrow \alpha \in F$
 Since the minimal poly of α over F must be linear, $x - \alpha \in F[x]$]

$$\therefore p = [K:F] = [K:F(u)] \overbrace{[F(u):F]}^{>1}$$

$$\therefore \Rightarrow [K:F(a)] = 1 \text{ and } [F(u):F] = p$$

↓

$$k = F(u) . \quad \blacksquare$$

Example

Let F be a field, K a field extension of F .

Suppose E_1, E_2 are contained in K and that both E_1 and E_2 are field extensions of F . If $p_1 = [E_1 : F]$

$p_2 = [E_2 : F]$ are both prime numbers prove that either

$$E_1 = E_2 \text{ or } E_1 \cap E_2 = F.$$

Proof: First note that $E_1 \cap E_2$ is a field extension of F , since it necessarily contains F (as E_1, E_2 contain F) (and is a field, since the intersection of two fields is a field)

Similarly E_1 and E_2 are extensions of $E_1 \cap E_2$.

$$\therefore F \subseteq E_1 \cap E_2 \subseteq E_2 \text{ and } F \subseteq E_1 \cap E_2 \subseteq E_1$$

$$[E_2 : F] = [E_2 : E_1 \cap E_2] [E_1 \cap E_2 : F]$$

||

p_2 , prime

$$\therefore \text{Either } [E_2 : E_1 \cap E_2] = 1 \text{ OR } [E_1 \cap E_2 : F] = 1$$

↓

$$E_2 = E_1 \cap E_2$$

↓

$$E_1 \cap E_2 = F$$

But by the same argument using $[E_1 : F]$

$$E_1 = E_1 \wedge E_2 \quad \text{or} \quad E_1 \wedge E_2 = F.$$

\therefore All together: either $E_1 \wedge E_2 = F$ or

$$E_1 \wedge E_2 = E_1 = E_2. \quad \blacksquare$$

Example] Let E be an algebraic extension of a field

F , let σ be an automorphism leaving F fixed
(i.e. $\sigma \in G(E/F)$). Let $a \in E$.

Show that σ induces a permutation of the set of all zeros of the minimal polynomial α that are in E .

Proof:

- E is an algebraic extension of F
- $\sigma: E \rightarrow E$ is an automorphism s.t. $\sigma(a) = a$ for $a \in F$.

\therefore exists a unique minimal polynomial $p(x) \in F[x]$, of α over F .

Let $\{\beta_1, \dots, \beta_n\} \subseteq E$ be all roots of $p(x)$ in E , suppose

$$p(x) = x^m + b_{m-1}x^{m-1} + \dots + b_1x + b_0, \quad b_j \in F, \quad m \geq n$$

For all $j = 1, \dots, m$

$0 = p(\beta_j)$, and Since σ is an automorphism $\sigma(0) = 0$

$$\therefore 0 = \sigma(0) = \sigma(p(\beta_j))$$

$$= \sigma(\beta_j^m + b_{m-1}\beta_j^{m-1} + \dots + b_1\beta_j + b_0)$$

$$\begin{aligned}
 &= \sigma(\beta_j)^m + \sigma(b_{m-1})\sigma(\beta_j)^{m-1} + \dots + \sigma(b_1)\sigma(\beta_j) + \sigma(b_0) \\
 &= \sigma(\beta_j)^m + b_{m-1}\sigma(\beta_j)^{m-1} + \dots + b_1\sigma(\beta_j) + b_0 \\
 &= P(\sigma(\beta_j))
 \end{aligned}$$

$\therefore \sigma(\beta_j)$ is a root of $P(x)$, and $\sigma(\beta_j) \in E$

$$\therefore \sigma(\beta_j) \in \{\beta_1, \dots, \beta_n\} \quad \forall j$$

Remember a permutation of $\{\beta_1, \dots, \beta_n\}$ must be 1-1 and onto

Since σ is an automorphism, it is a 1-1 map

$\therefore \sigma$ is a 1-1 map from $\{\beta_1, \dots, \beta_n\}$ to itself

$\therefore \sigma$ is onto $\therefore \sigma$ is a permutation of $\{\beta_1, \dots, \beta_n\}$.

QED