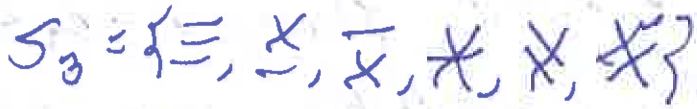
Main point of Galois Theory

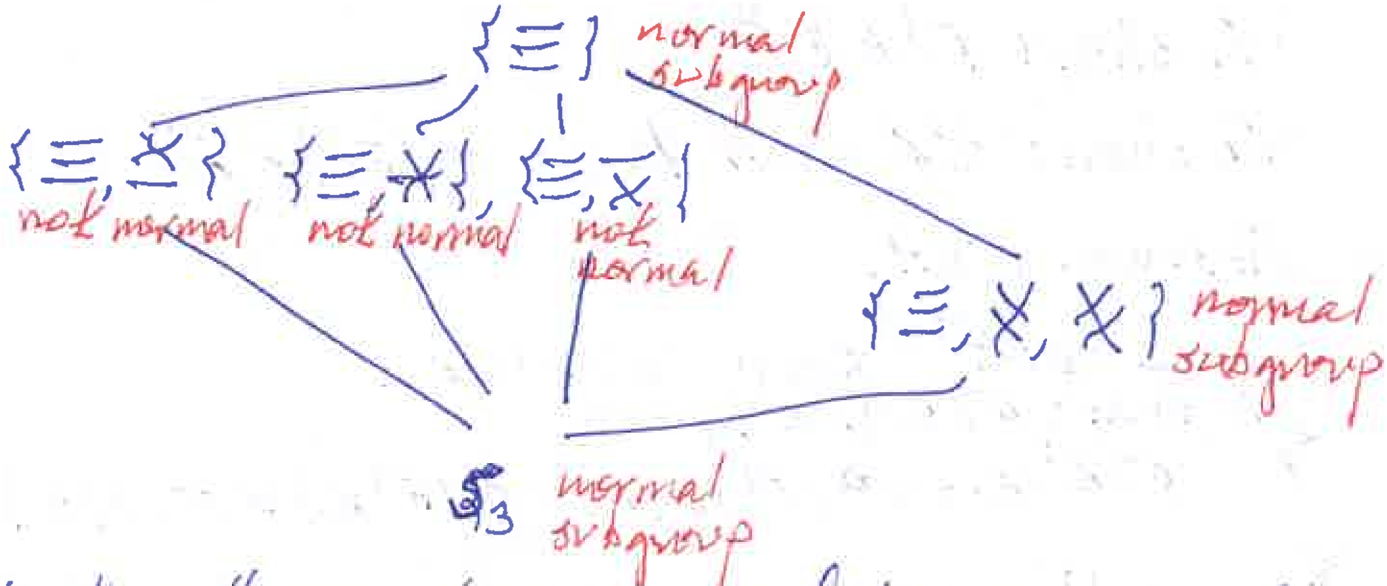
Groups and Fields – the same

The group S_3



Some products

Subgroups $H \leq S_3$

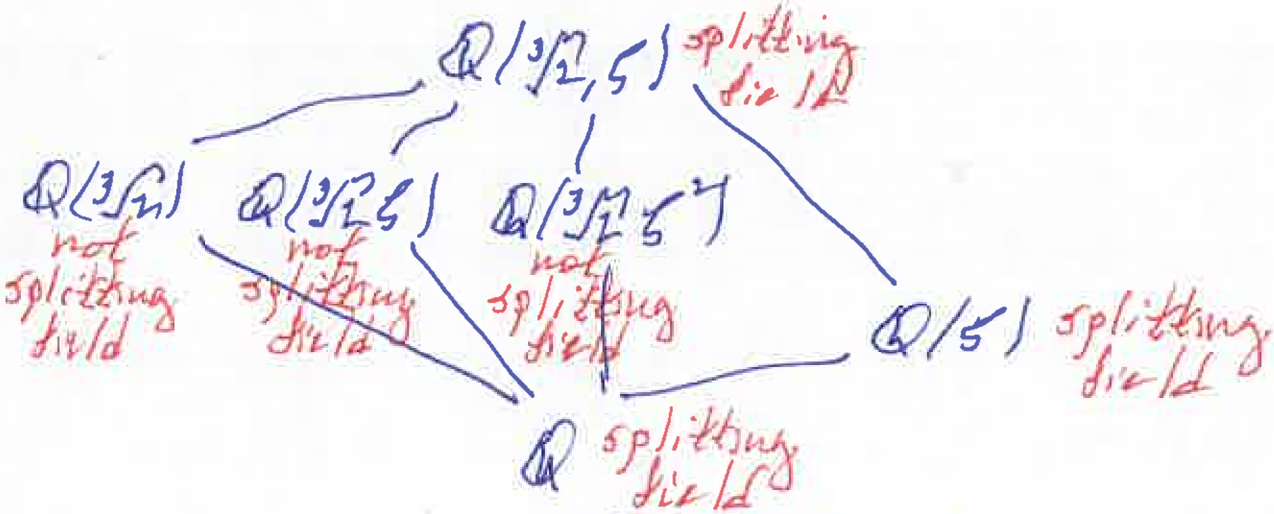


is the Hasse diagram of the poset of subgroups of S_3 partially ordered by inclusion.

<u>Fields</u> Let $\alpha_1, \dots, \alpha_k \in \mathbb{C}$.

The field generated by $\mathbb{Q}$ and $\alpha_1, \dots, \alpha_k$ is the smallest field $\mathbb{Q}(\alpha_1, \dots, \alpha_k)$ of $\mathbb{C}$ containing $\mathbb{Q}$ and $\alpha_1, \dots, \alpha_k$.

Let $\zeta = e^{2\pi i/3}$



are subfields of $\mathbb{Q}(\sqrt[3]{2}, \zeta)$ containing $\mathbb{Q}$.

$\mathbb{Q}(\zeta)$ has $\mathbb{Q}$-basis $\{1, \zeta\}$

$\mathbb{Q}(\sqrt[3]{2})$ has $\mathbb{Q}$-basis $\{1, \sqrt[3]{2}, \sqrt[3]{4}\}$

$\mathbb{Q}(\sqrt[3]{2}\zeta)$ has $\mathbb{Q}$-basis $\{1, \sqrt[3]{2}\zeta, \sqrt[3]{4}\zeta^2\}$

$\mathbb{Q}(\sqrt[3]{2}\zeta^2)$ has $\mathbb{Q}$-basis $\{1, \sqrt[3]{2}\zeta^2, \sqrt[3]{4}\zeta\}$

$\mathbb{Q}(\sqrt[3]{2}, \zeta)$ has $\mathbb{Q}$-basis

$$\{1, \sqrt[3]{2}, \sqrt[3]{4}, \zeta, \sqrt[3]{2}\zeta, \sqrt[3]{4}\zeta\}.$$

Splitting fields

Since

$$x^3-2 = (x-\sqrt[3]{2})(x-\sqrt[3]{2}\zeta)(x-\sqrt[3]{2}\zeta^2)$$

then $\mathbb{Q}(\sqrt[3]{2},\zeta)$ is the splitting field of x^3-2 over $\mathbb{Q}$,

i.e. the smallest field containing $\mathbb{Q}$ and all roots of x^3-2.

Since

$$x^3-1 = (x-1)(x-\zeta)(x-\zeta^2) = (x-1)(x^2+x+1)$$

then $\mathbb{Q}(\zeta)$ is the splitting field of x^3-1 over $\mathbb{Q}$ and $\mathbb{Q}(\zeta)$ is the splitting field of x^2+x+1 over $\mathbb{Q}$

$\mathbb{Q}(\sqrt[3]{2})$ is <u>not</u> the splitting field of x^3-2 over $\mathbb{Q}$

27.02.2024
Algebra Lect 2
A. Ram

Automorphism groups

Let $\sigma \in \mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2}, \zeta))$.

Since $\sqrt[3]{2}$ and ζ generate $\mathbb{Q}(\sqrt[3]{2}, \zeta)$ then

$$\sigma : \mathbb{Q}(\sqrt[3]{2}, \zeta) \to \mathbb{Q}(\sqrt[3]{2}, \zeta)$$

is a $\mathbb{Q}$-linear transformation determined by

$$\sigma(\sqrt[3]{2}) \quad \text{and} \quad \sigma(\zeta).$$

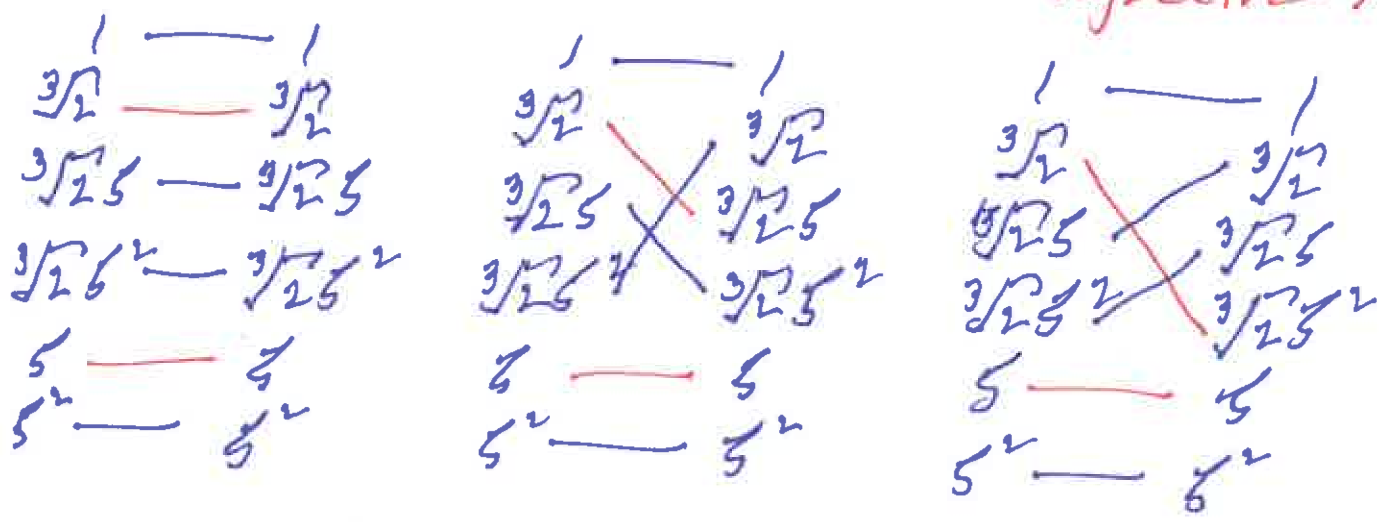
Since σ is an automorphism

$$\sigma(\sqrt[3]{2})^3 = 2 \quad \text{and} \quad \sigma(\zeta)^3 = 1$$

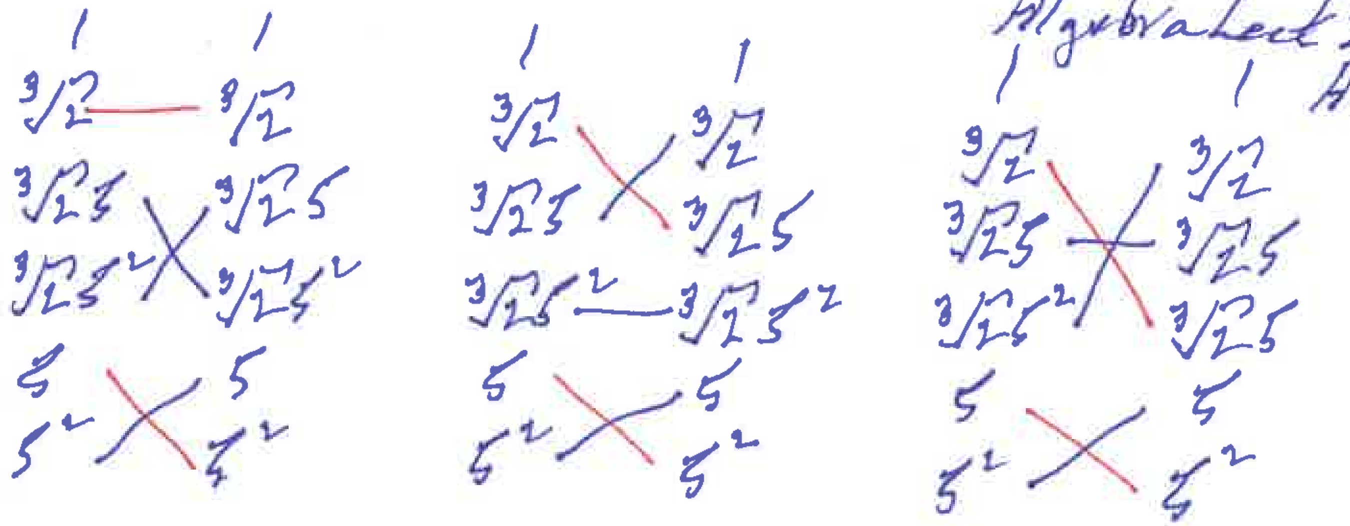
So $\sigma(\sqrt[3]{2}) \in \{\sqrt[3]{2}, \sqrt[3]{2}\zeta, \sqrt[3]{2}\zeta^2\}$

and $\sigma(\zeta) \in \{\zeta, \zeta^2\}$.

($\sigma(\zeta) \neq 1$ since $\sigma(1) = 1$ and σ is injective)



27.02.2024
Algebra Lect 2 (5)
A.Rau



So

$$\mathrm{Aut}_{\mathbb{Q}(\sqrt[3]{2},\zeta)}(\mathbb{Q}(\sqrt[3]{2},\zeta)) = \{\equiv\}$$

$$\mathrm{Aut}_{\mathbb{Q}(\sqrt[3]{2})}(\mathbb{Q}(\sqrt[3]{2},\zeta)) = \{\equiv, \times\} \qquad \mathrm{Aut}_{\mathbb{Q}(\sqrt[3]{2}\zeta)}(\mathbb{K}) = \{\equiv, \ast\} \qquad \mathrm{Aut}_{\mathbb{Q}(\sqrt[3]{2}\zeta^2)}(\mathbb{K}) = \{\equiv, \times\}$$

$$\mathrm{Aut}_{\mathbb{Q}(\zeta)}(\mathbb{K}) = \{\equiv, \times, \times\}$$

$$\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt[3]{2},\zeta)) = S_3$$

<u>Theorem</u> Let $\mathbb{E}$ be a subfield of $\mathbb{K}$. Assume there exists $f \in \mathbb{E}[x]$ such that $\mathbb{K}$ is the splitting field of f. Then

$$\{\text{subgroups } \mathrm{Aut}_{\mathbb{E}}(\mathbb{K}) \supseteq H \supseteq \{1\}\} \longleftrightarrow \{\text{subfields } \mathbb{E} \subseteq \mathbb{F} \subseteq \mathbb{K}\}$$

$$\mathrm{Aut}_{\mathbb{F}}(\mathbb{K}) \longleftarrow\!\shortmid\ \mathbb{F}$$

$$H \longmapsto \mathbb{F}^H$$

is an isomorphism of posets.