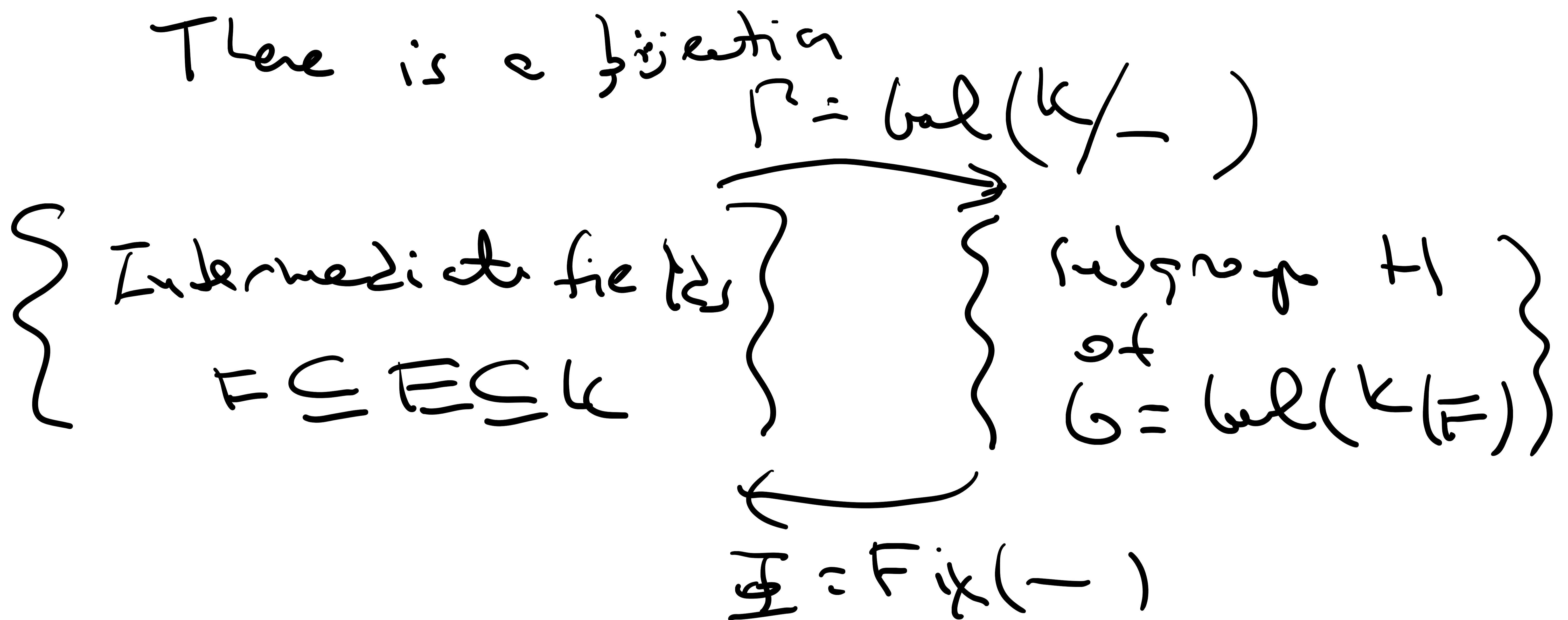


Lec 22 March 3, 2021

Last time:

Thm. - $[K:F] < \infty$ K/F Galois

There is a bijection



which reverses inclusions

i.e. if $F_1 \subseteq F_2$ then

$$\text{Gal}(K/F_2) \subseteq \text{Gal}(K/F_1)$$

if $H_1 \subseteq H_2$ then

$$\text{Fix}(H_2) \subseteq \text{Fix}(H_1).$$

$$|\text{Gal}(K/F)| = [K:F]$$

Also E/F is normal iff
 $\text{Gal}(K/F) \cong \text{Gal}(K^s/F)$.

Ex. $K =$ Splitting field of $x^4 - 2 = f$
over \mathbb{Q} . Let $\alpha = \sqrt[4]{2}$ $i = \sqrt{-1}$

The roots of f in \mathbb{C} are
 $\{\alpha, \alpha i, -\alpha, -\alpha i\}$

So $K = \mathbb{Q}(\alpha, i)$

f is irr. by Eisenstein, so

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4 = \deg f$$

$i \notin \mathbb{Q}(\alpha) \subseteq \mathbb{R}$, i is a root of $x^2 + 1$

$$\text{So } [\mathbb{Q}(\alpha, i) : \mathbb{Q}(\alpha)] = 2$$

$$[\mathbb{Q}(\alpha, i) : \mathbb{Q}] = 8.$$

K/\mathbb{Q} is a splitting field for f so is

Galois. So $|\text{Gal}(K/\mathbb{Q})| = 8$.

Now if $\sigma \in G = \text{Gal}(K/\mathbb{F})$ then

$\sigma(\alpha)$ is a root of f

$\sigma(i)$ is a root of $x^2 + 1$.

8 choices total, and σ is determined by where it sends α and i . So all occur.

Let $\sigma: \alpha \mapsto i\alpha$ $\tau: \alpha \mapsto \alpha$
 $i \mapsto i$ $i \mapsto -i$

$$|\sigma| = 4. \quad |\tau| = 2.$$

$$|\langle \sigma \rangle \langle \tau \rangle| = 8 \quad \langle \sigma \rangle \cap \langle \tau \rangle = 1$$

$$\text{So } G = \{1, \sigma, \sigma^2, \sigma^3, \tau, \sigma\tau, \sigma^2\tau, \sigma^3\tau\}$$

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

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

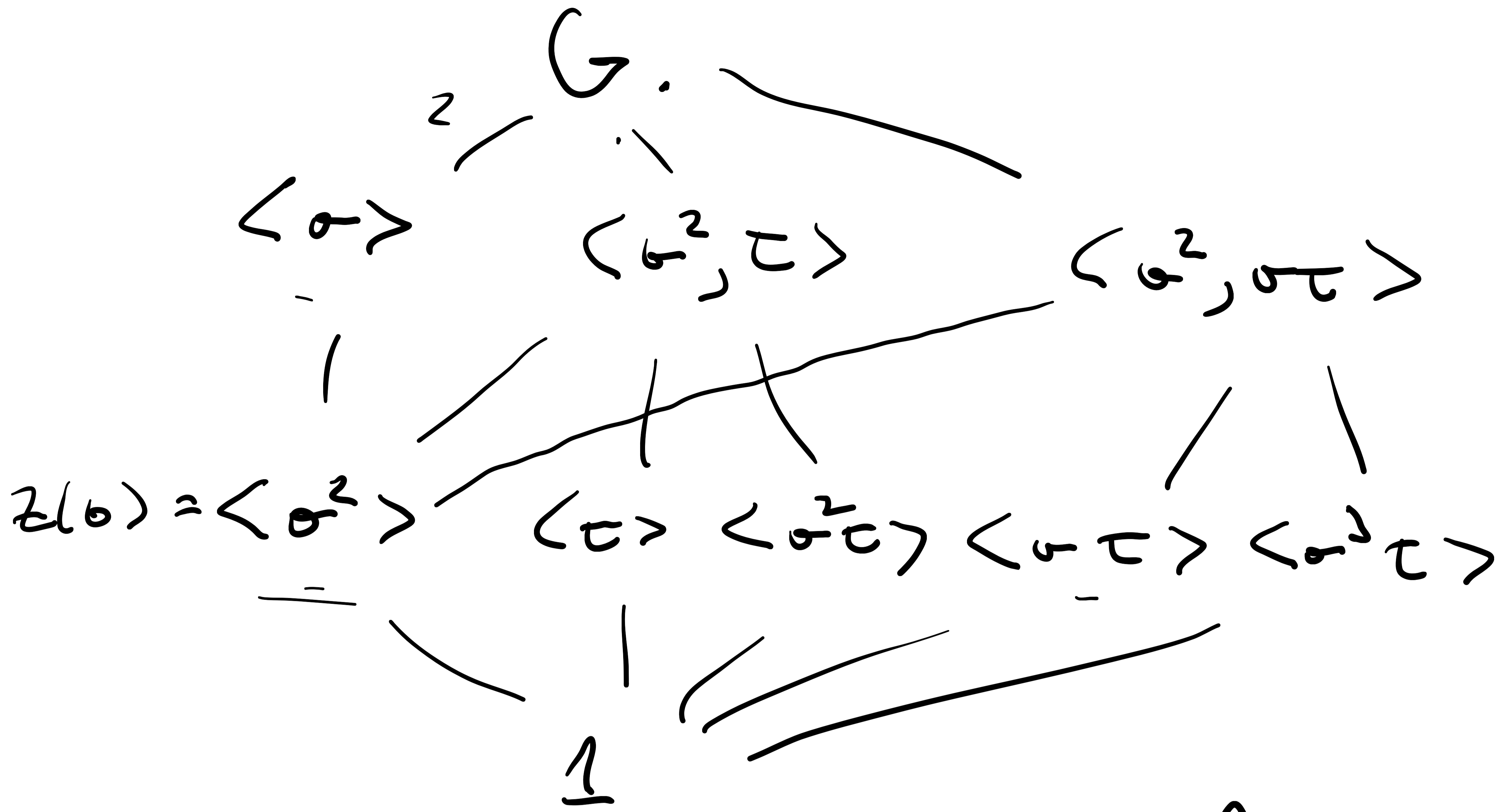
$$\sigma^3\tau(\alpha) = \sigma^3(\alpha) = -i\alpha$$

$$\sigma^3\tau(i) = -i$$

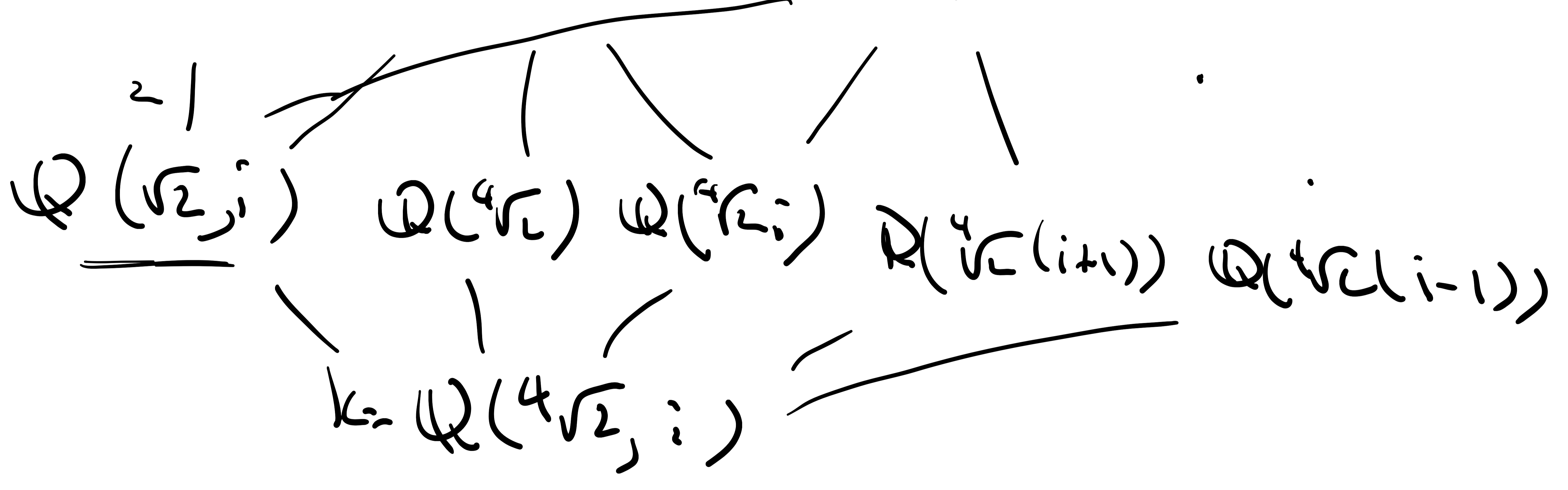
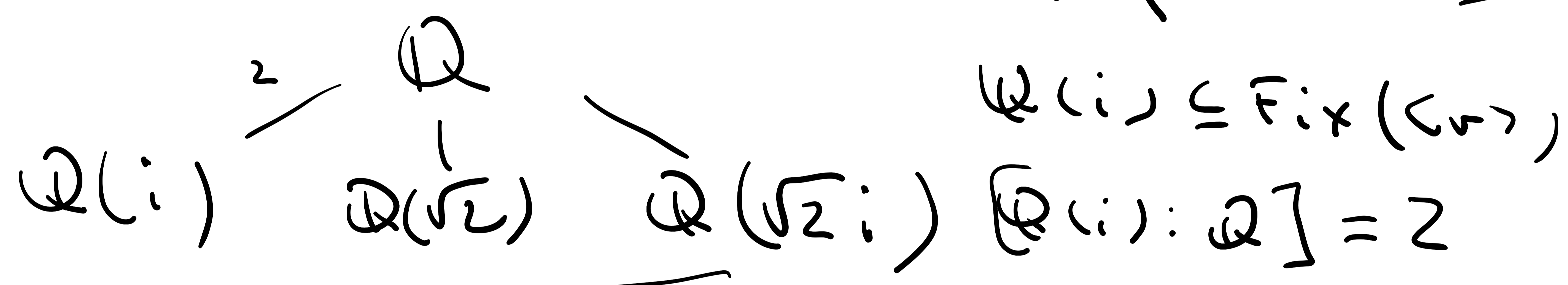
$$\text{So } \tau\sigma = \sigma^3\tau = \sigma^{-1}\tau.$$

$$\text{So } G \cong D_8.$$

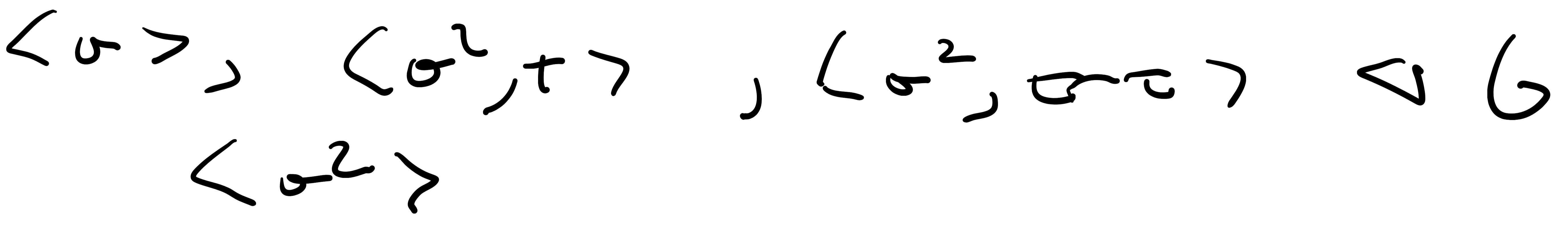
Let's find all subgroups of $G = D_8 = \langle \sigma, \tau \rangle$



Apply $\text{Fix}(-)$



What about normality?



The others are not normal.

So all fields are normal (and Galois) over \mathbb{Q} except.

$$\mathbb{Q}(\sqrt[4]{2}), \mathbb{Q}(\sqrt[4]{2}i), \mathbb{Q}(\sqrt[4]{2}(1+i)), \\ \mathbb{Q}(\sqrt[4]{2}(1-i))$$

e.g. $\sqrt[4]{2}$ is a root of $x^4 - 2$ but $x^4 - 2$ does not split over $\mathbb{Q}(\sqrt[4]{2})$.

$\sqrt[4]{2}(1+i)$ is a root of $x^4 + 8$ which does not split over $\mathbb{Q}(\sqrt[4]{2}(1+i))$.

$$\text{Also } \langle \sigma^2 \rangle = \text{Gal}(K / \mathbb{Q}(\sqrt{2}, i))$$

Fund. Theorem says

$$G / \langle \sigma^2 \rangle \cong \text{Gal}(\mathbb{Q}(\sqrt{2}, i) / \mathbb{Q}).$$

both are \cong to $\mathbb{Z}_2 \times \mathbb{Z}_2$.

Another example.

$$\underline{\text{Ex.}} \quad K = \mathbb{Q}(\sqrt{2+\sqrt{2}}) \quad \alpha = \sqrt{2+\sqrt{2}}$$

$$\text{minpoly}_{\mathbb{Q}}(\alpha) = x^4 - 4x^2 + 2$$

$$\text{roots are } \pm \alpha, \pm \beta \quad \beta = \sqrt{2-\sqrt{2}}$$

check $K =$ splitting field of $x^4 - 4x^2 + 2$
since $\alpha\beta = \sqrt{2+\sqrt{2}}\sqrt{2-\sqrt{2}}$
 $= \sqrt{4-2} = \sqrt{2} \in K.$

$$(\alpha^2 - 2 = \sqrt{2} \in K)$$

$[K:\mathbb{Q}] = 4$, K/\mathbb{Q} is Galois.

What is $\text{Gal}(K/\mathbb{Q})$? Group of size 4.

Any $\sigma \in G = \text{Gal}(K/\mathbb{Q})$ is determined by where it sends α , which is in $\{\pm\alpha, \pm\beta\}$.

Choose $\sigma(\alpha) = \beta$.

$$\text{then } \sigma(-\alpha) = -\beta.$$

$$\text{Since } \alpha\beta = \sqrt{2}$$

$$\sigma(\alpha\beta) = \sigma(\alpha)\sigma(\beta) = \sigma(\sqrt{2})$$

$$\text{Since } \alpha^2 - 2 = \sqrt{2}, \quad \sigma(\sqrt{2}) = \sigma(\alpha^2) - 2 \\ = \sigma(\beta^2) - 2$$

$$\sigma(2 + \sqrt{2}) - 2 = \sigma(2 - \sqrt{2}) - 2$$

$$\sigma(2 + \sqrt{2}) = \sigma(2 - \sqrt{2})$$

$$\sigma(\sqrt{2}) = -\sqrt{2}$$

this forces $\sigma(\beta) = -\alpha$.

$$\sigma: \begin{aligned} \alpha &\rightarrow \beta \\ \beta &\rightarrow -\alpha \\ -\alpha &\rightarrow -\beta \\ -\beta &\rightarrow \alpha \end{aligned} \quad |G| = 4 \quad \text{and } G \cong Q_4.$$

$$\begin{array}{ccc} G = \langle \sigma \rangle & \xrightarrow{\text{Fix}(-)} & \mathbb{Q} \\ | & & | \\ \langle \sigma^2 \rangle & & \mathbb{Q}(\sqrt{2}) \\ | & & | \\ & & \mathbb{K} \end{array}$$

Next time: Cyclotomic polynomials
 Galois group of splitting field
 of $x^n - 1$ over \mathbb{Q} .