§9, Ex3 - Additional Details

- Let E be the splitting field of $F = x^4 - 2 \in \mathbb{Q}[x]$
- We saw in lectures that $G = \mathrm{Aut}(E/\mathbb{Q})$ has order 8 and $G = \langle \sigma, \tau \rangle$ where $\sigma : \begin{array}{l} \alpha \mapsto \alpha i \\ i \mapsto i \end{array}$ and $\tau : \begin{array}{l} \alpha \mapsto \alpha \\ i \mapsto -i \end{array}$

- Let $\mathcal{H}$ be the set of subgroups of G (you won't be expected to calc all these!)

$$\Rightarrow \quad \mathcal{H} = \left\{ \begin{array}{c} \{id\} \\ \langle \sigma \rangle, \ \langle \sigma^2 \rangle, \ \langle \tau \rangle \\ \langle \sigma\tau \rangle, \langle \sigma^2\tau \rangle, \ \langle \sigma^3\tau \rangle \\ \langle \sigma^2, \tau \rangle, \ \langle \sigma^2, \sigma\tau \rangle \\ \langle \sigma, \tau \rangle = G \end{array} \right\}$$

- Lets consider the Galois correspondence
- For $H \in \mathcal{H}$, we know $(\mathrm{Fix}(H) : \mathbb{Q}) = \dfrac{|G|}{|H|}$

- If we can spot elements of E fixed by H then fab!

Lets do some of the cases where we can do this

* We know $\mathrm{Fix}(\{id\}) = E$ and $\mathrm{Fix}(G) = \mathbb{Q}$

* $|\langle \sigma \rangle| = 4 \Rightarrow (\mathrm{Fix}(\langle \sigma \rangle) : \mathbb{Q}) = \dfrac{|G|}{|\langle \sigma \rangle|} = \dfrac{8}{4} = 2$

  σ fixes $i \Rightarrow \mathbb{Q}(i) \subseteq \mathrm{Fix}(\langle \sigma \rangle)$

  $(\mathbb{Q}(i) : \mathbb{Q}) = 2 \Rightarrow \mathbb{Q}(i) = \mathrm{Fix}(\langle \sigma \rangle)$

* $|\langle \tau \rangle| = 2 \Rightarrow (\mathrm{Fix}(\langle \tau \rangle) : \mathbb{Q}) = \dfrac{|G|}{|\langle \tau \rangle|} = \dfrac{8}{2} = 4$

  τ fixes $\alpha \Rightarrow \mathbb{Q}(\alpha) \subseteq \mathrm{Fix}(\langle \tau \rangle)$

  $(\mathbb{Q}(\alpha) : \mathbb{Q}) = 4 \Rightarrow \mathbb{Q}(\alpha) = \mathrm{Fix}(\langle \tau \rangle)$

* $|\langle \sigma^2 \rangle| = 2 \Rightarrow (\mathrm{Fix}(\langle \sigma^2 \rangle) : \mathbb{Q}) = \dfrac{|G|}{\langle \sigma^2 \rangle} = \dfrac{8}{2} = 4$

  σ^2 fixes $i \Rightarrow \mathbb{Q}(i) \subseteq \mathrm{Fix}(\langle \sigma^2 \rangle)$

  $(\mathbb{Q}(i) : \mathbb{Q}) = 2 \Rightarrow \mathbb{Q}(i) \subsetneq \mathrm{Fix}(\langle \sigma^2 \rangle)$

  $\Rightarrow$ we need to search for more fixed els

$$\begin{aligned} \sigma^2(\alpha^2) &= \sigma(\sigma(\alpha)) \cdot \sigma(\sigma(\alpha)) \\ &= \sigma(i\alpha) \cdot \sigma(i\alpha) \\ &= i^2\alpha \cdot i^2\alpha \\ &= \alpha^2 \end{aligned}$$

$\Rightarrow \mathbb{Q}(\alpha^2) \subseteq \mathrm{Fix}(\langle \sigma^2 \rangle)$

$\Rightarrow \mathbb{Q}(\alpha^2, i) \subseteq \mathrm{Fix}(\langle \sigma^2 \rangle)$

[Exercise - show using the tower law $(\mathbb{Q}(\alpha^2, i) : \mathbb{Q}) = 4$]

$\Rightarrow \mathrm{Fix}(\langle \sigma^2 \rangle) = \mathbb{Q}(\alpha^2, i)$

$* \ |\langle \sigma^2, \tau \rangle| = 4 \Rightarrow (\mathrm{Fix}(\langle \sigma^2, \tau\rangle) : \mathbb{Q}) = \frac{|G|}{|\langle \sigma^2, \tau \rangle|} = \frac{8}{4} = 2$

$$\begin{aligned} \sigma^2(\alpha^2) &= \sigma^2(\alpha)\sigma^2(\alpha) \\ &= \sigma(\alpha i)\sigma(\alpha i) \\ &= \alpha i^2 \cdot \alpha i^2 \\ &= \alpha^2 i^4 \\ &= \alpha^2 \end{aligned} \qquad \begin{aligned} \tau(\alpha^2) &= \tau(\alpha)\tau(\alpha) \\ &= \alpha \cdot \alpha \\ &= \alpha^2 \end{aligned}$$

$\Rightarrow \mathbb{Q}(\alpha^2) \subseteq \mathrm{Fix}(\langle \sigma^2, \tau \rangle)$

$(\mathbb{Q}(\alpha^2) : \mathbb{Q}) = 2 \Rightarrow \mathrm{Fix}(\langle \sigma^2, \tau \rangle) = \mathbb{Q}(\alpha^2)$

$* \ |\langle \sigma^2, \sigma\tau \rangle| = 4$

$\Rightarrow (\mathrm{Fix}(\langle \sigma^2, \sigma\tau \rangle) : \mathbb{Q}) = \frac{|G|}{4} = 2$

$\langle \sigma^2 \rangle \leq \langle \sigma^2, \sigma\tau \rangle \Rightarrow \mathrm{Fix}(\langle \sigma^2, \sigma\tau \rangle) \subseteq \mathrm{Fix}(\langle \sigma^2 \rangle) = \mathbb{Q}(\sqrt{2}, i)$

$\sigma\tau(\sqrt{2}) = \sigma\tau(\alpha^2) = \sigma(\alpha^2) = -\alpha^2$

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

$\sigma\tau(\sqrt{2}i) = \sigma\tau(\alpha^2 i) = \sigma(-\alpha^2 i) = \alpha^2 i = \sqrt{2}i$

$\Rightarrow \mathbb{Q}(\sqrt{2}i) \subseteq \mathrm{Fix}(\langle \sigma^2, \sigma\tau \rangle)$

$(\sqrt{2}i)^2 = -2 \Rightarrow \sqrt{2}i$ is a root of x^2+2 which is irr by Eis with $p=2$

$\Rightarrow (\mathbb{Q}(\sqrt{2}i) : \mathbb{Q}) = 2$

$\Rightarrow \mathrm{Fix}(\langle \sigma^2, \sigma\tau \rangle) = \mathbb{Q}(\sqrt{2}i)$

- Now lets do some which are harder to spot

$$\begin{aligned} * \ (\sigma^3\tau)^2 &= \sigma^3\tau\sigma^3\tau \\ &= \sigma^3\sigma \\ &= \sigma^4 \\ &= id \end{aligned}$$

we showed in the lecture $\tau\sigma\tau = \sigma^3$
$\Rightarrow \tau\sigma^3\tau = \sigma$

$\Rightarrow |\langle \sigma^3\tau \rangle| = 2$

$\Rightarrow |\mathrm{Fix}(\langle \sigma^3\tau \rangle)| = \frac{8}{2} = 4$

$(E : \mathbb{Q}) = 8$

$\Rightarrow E$ as a vector space over $\mathbb{Q}$ has a basis of size 8

One basis is $\{1, \alpha, \alpha^2, \alpha^3, i, i\alpha, i\alpha^2, i\alpha^3\}$ where $\alpha = \sqrt[4]{2}$

$\Rightarrow$ an arbitary element $b \in E$ can be expressed as

$b = a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3 + a_4 i + a_5 i\alpha + a_6 i\alpha^2 + a_7 i\alpha^3 \qquad a_i \in \mathbb{Q}$

What does $\sigma^3\tau$ do to b?

$$\begin{aligned} \sigma^3\tau(b) &= \sigma^3\tau(a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3 + a_4 i + a_5 i\alpha + a_6 i\alpha^2 + a_7 i\alpha^3) \\ &= a_0 + a_1(i^3\alpha) + a_2(i^3\alpha)^2 + a_3(i^3\alpha)^3 + a_4(-i) + a_5(-i \cdot i^3\alpha) + a_6(-i(i^3\alpha)^2) + a_7(-i(i^3\alpha)^3) \\ &= a_0 - a_1 i\alpha - a_2\alpha^2 + a_3 i\alpha^3 - a_4 i - a_5\alpha + a_6 i\alpha^2 + a_7\alpha^3 \end{aligned}$$

$\Rightarrow \sigma^3\tau(b) = b \iff -a_1 = a_5 \quad -a_2 = a_2 \quad a_3 = a_7 \quad -a_4 = a_4$

$\iff -a_1 = a_5 \quad a_2 = 0 \quad a_3 = a_7 \quad a_4 = 0$

$\Rightarrow$ Elements of E fixed by $\sigma^3\tau$ can be expressed as

$$a_0 + a_1(\alpha - i\alpha) + a_3(\alpha^3 + i\alpha^3) + a_6 \, i\alpha^2$$

$$= a_0 + a_1 \alpha(1-i) + a_3[\alpha(1-i)]^3 + a_6[\alpha(1-i)]^2$$

$$\Rightarrow \quad \mathbb{Q}(\alpha(1-i)) \subseteq \mathrm{Fix}(\langle\sigma^3\tau\rangle)$$

$[\alpha(1-i)]^4 = -\alpha^4 = -2 \Rightarrow \alpha(1-i)$ is a root of x^4+2 (irr by Eis with $p=2$)

$$\Rightarrow \quad (\mathbb{Q}(\alpha(1-i)) : \mathbb{Q}) = 4$$

$$\Rightarrow \quad \mathbb{Q}(\alpha(1-i)) = \mathrm{Fix}(\langle\sigma^3\tau\rangle)$$

* $\sigma^2\tau\sigma^2\tau = \sigma^2\tau\sigma\tau\tau\sigma\tau$
$= \sigma^2\sigma^3\sigma^3$
$= \sigma^8$
$= 1$

$\Rightarrow |\langle\sigma^2\tau\rangle| = 2$

$\Rightarrow (\mathrm{Fix}(\langle\sigma^2\tau\rangle) : \mathbb{Q}) = \dfrac{|G|}{2} = 4$

$$\sigma^2\tau(a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3 + a_4 i + a_5 i\alpha + a_6 i\alpha^2 + a_7 i\alpha^3)$$
$$= a_0 - a_1\alpha + a_2\alpha^2 - a_3\alpha^3 - a_4 i + a_5 i\alpha - a_6 i\alpha^2 + a_7 i\alpha^3$$

$\Rightarrow \sigma^2\tau$ fixes $a_0 + a_1\alpha + \dots + a_7 i\alpha^3$

$\Leftrightarrow a_1 = -a_1 \quad a_3 = -a_3 \quad a_4 = -a_4 \quad a_6 = -a_6$

$\Leftrightarrow a_1 = a_3 = a_4 = a_6 = 0$

$\Rightarrow \sigma^2\tau$ fixes $a_0 + a_2\alpha^2 + a_5 i\alpha + a_7 i\alpha^3$
$= a_0 - a_2(i\alpha)^2 + a_5 i\alpha - a_7(i\alpha)^3$

$\Rightarrow \sigma^2\tau$ fixes $i\alpha$

$\Rightarrow \mathbb{Q}(i\alpha) \subseteq \mathrm{Fix}(\langle\sigma^2\tau\rangle)$

$i\alpha$ is a root of $f = x^4 - 2$ which is irr

$\Rightarrow (\mathbb{Q}(i\alpha) : \mathbb{Q}) = 4$

$\Rightarrow \mathrm{Fix}(\langle\sigma^2\tau\rangle) = \mathbb{Q}(i\alpha)$

* In the lecture we showed
$\mathrm{Fix}(\langle\sigma\tau\rangle) = \mathbb{Q}(\alpha(1+i))$