Lecture 23: Further Examples of Galois Theory

E1 We've studied $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ over $\mathbb{Q}$ and I've argued that $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2}+\sqrt{3})$. Let's see what Galois Theory brings to the discussion.

(1.) $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = K$ is splitting field of $(x^2-2)(x^2-3)$ over $\mathbb{Q}$ thus $K/\mathbb{Q}$ is Galois Extension hence

$$[K, \mathbb{Q}] = |\mathrm{Aut}(K/\mathbb{Q})|$$

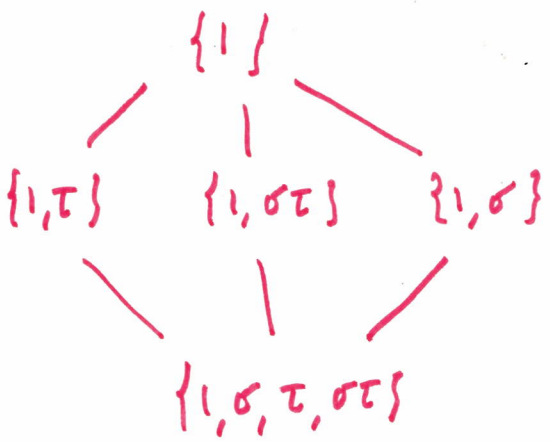
Of course Automorphisms fix the prime subfield $\mathbb{Q}$ since they map 1 to 1 etc.

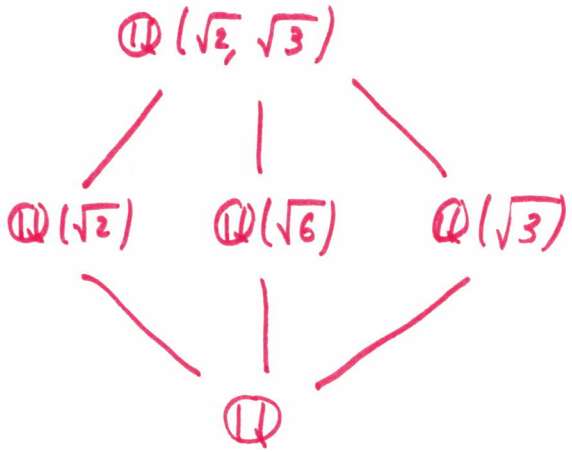
(2.) automorphisms are defined by what they do to $\sqrt{2}$ and $\sqrt{3}$ for K and as we discussed,

$$\sigma(\sqrt{2}) = \sqrt{2} \;\&\; \sigma(\sqrt{3}) = -\sqrt{3} \Rightarrow \sigma(\sqrt{6}) = -\sqrt{6}$$
$$\tau(\sqrt{3}) = \sqrt{3} \;\&\; \tau(\sqrt{2}) = -\sqrt{2} \Rightarrow \tau(\sqrt{6}) = -\sqrt{6}$$
$$\sigma\tau(\sqrt{3}) = -\sqrt{3} \;\&\; \sigma\tau(\sqrt{2}) = -\sqrt{2} \Rightarrow \sigma\tau(\sqrt{6}) = \sqrt{6}$$

Thus $\mathrm{Aut}(K) = \{1, \sigma, \tau, \sigma\tau\}$ $\therefore$ $\underline{|\mathrm{Aut}(K/\mathbb{Q})| = 4}$.

There is a correspondence between fixed fields and subgroups of $\mathrm{Aut}(K/\mathbb{Q})$. For $\mathrm{Aut}(K) = \mathrm{Gal}(\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}) = \{1, \sigma, \tau, \sigma\tau\}$ we have subgroups $\{1\}$, $\{\sigma, 1\}$, $\{\sigma\tau, 1\}$, $\{\tau, 1\}$ and $\{1, \sigma, \tau, \sigma\tau\}$





What is the subgroup whose fixed field is $\mathbb{Q}(\sqrt{2}+\sqrt{3})$?

What subgroup of $Gal(K/\mathbb{Q}) = \{1, \sigma, \tau, \sigma\tau\}$ has fixed field $\mathbb{Q}(\sqrt{2}+\sqrt{3})$? Consider,

$$\sigma(\sqrt{2}+\sqrt{3}) = \sigma(\sqrt{2}) + \sigma(\sqrt{3}) = \sqrt{2} - \sqrt{3} \neq \sqrt{2}+\sqrt{3}$$

$$\tau(\sqrt{2}+\sqrt{3}) = \tau(\sqrt{2}) + \tau(\sqrt{3}) = -\sqrt{2} + \sqrt{3} \neq \sqrt{2}+\sqrt{3}$$

$$\sigma\tau(\sqrt{2}+\sqrt{3}) = \sigma\tau(\sqrt{2}) + \sigma\tau(\sqrt{3}) = -\sqrt{2} - \sqrt{3} \neq \sqrt{2}+\sqrt{3}$$

$$1(\sqrt{2}+\sqrt{3}) = \sqrt{2}+\sqrt{3}$$

Thus the trivial subgroup $\{1\}$ has fixed field $\mathbb{Q}(\sqrt{2}+\sqrt{3})$

Recall $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ has $K^{\{1\}} = \mathbb{Q}(\sqrt{2}, \sqrt{3})$

$$K^H = \{\alpha \in K \mid \sigma(\alpha) = \alpha \quad \forall \sigma \in H\}$$

Thus $\mathbb{Q}(\sqrt{2}+\sqrt{3})$ is fixed field of $\{1\}$ just like $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ is fixed field of $\{1\}$. Thus, by correspondence, the Galois correspondence,

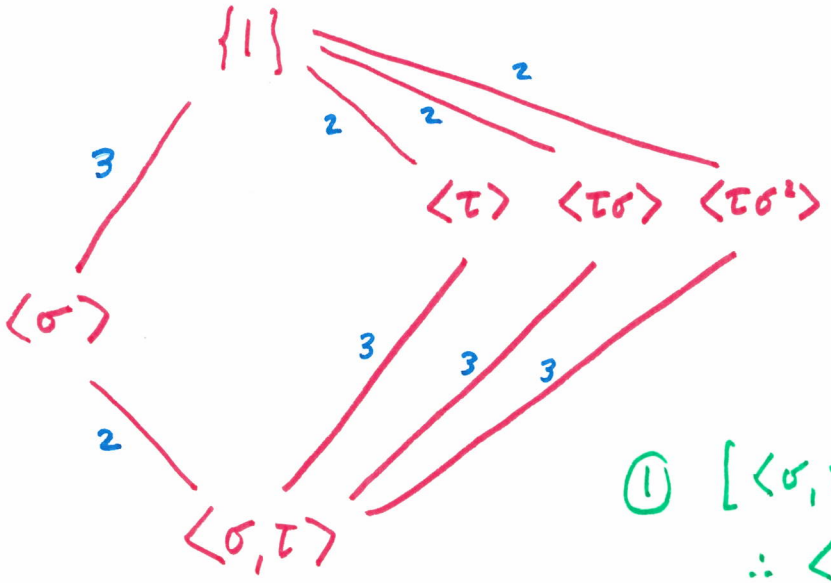
$$\boxed{\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2}+\sqrt{3})}$$

Observations: Let $G = Gal(K/\mathbb{Q})$

every subgroup $\{1, \sigma\}$, $\{1, \tau\}$, $\{1, \sigma\tau\}$ is normal in G hence every fixed subfield corresponding these, namely $\mathbb{Q}(\sqrt{3})$, $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{6})$ is galois over $\mathbb{Q}$. Indeed these are respectively the splitting field of x^2-3, x^2-2 and x^2-6.

E2 $\mathbb{Q}(\sqrt[3]{2}, \rho)$ where $\rho = e^{\frac{2\pi i}{3}} = \frac{-1+i\sqrt{3}}{2}$ over $\mathbb{Q}$

had $G = Gal(K/\mathbb{Q}) = \langle \sigma, \tau \rangle \cong S_3$ where $|\sigma| = 3$, $|\tau| = 2$



$\rho^2 + \rho = -1$

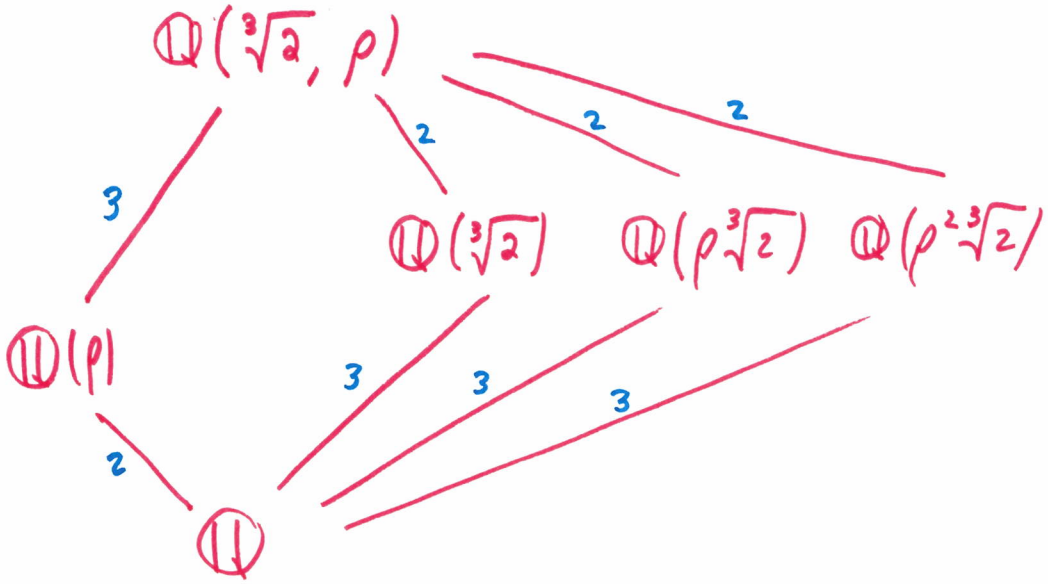
$\rho^2 + \rho + 1 = 0$

$m_{\rho, \mathbb{Q}}(x) = x^2 + x + 1 = \Phi_3(x)$

① $[\langle \sigma, \tau \rangle : \langle \sigma \rangle] = 2$

$\therefore \langle \sigma \rangle \trianglelefteq \langle \sigma, \tau \rangle$

$\Rightarrow \mathbb{Q}(\rho)$ is Galois over $\mathbb{Q}$.



② $\langle \tau \rangle$, $\langle \tau\sigma \rangle$, $\langle \tau\sigma^2 \rangle$ are not normal subgroups of $\langle \sigma, \tau \rangle$ and likewise $\mathbb{Q}(\sqrt[3]{2})$, $\mathbb{Q}(\rho\sqrt[3]{2})$, $\mathbb{Q}(\rho^2\sqrt[3]{2})$ are not splitting fields over $\mathbb{Q}$, they're not Galois extensions of $\mathbb{Q}$.

SPLITTING FIELD OF $X^8 - 2$ OVER $\mathbb{Q}$

E3

$$\zeta_8 = \exp\left(\frac{2\pi i}{8}\right) = \exp\left(\frac{\pi i}{4}\right) = \cos(\pi/4) + i\sin(\pi/4) = \frac{1+i}{\sqrt{2}}$$

Then sol^{n}s of $X^8 = 2$ are given by $X_k = \Theta \zeta_8^k$ for $k = 0, 1, 2, \ldots, 7$ for $\Theta = \sqrt[8]{2}$ then

$$x^8 - 2 = (x - X_1)(x - X_2)\cdots(x - X_7)(x - \Theta)$$

$K = \mathbb{Q}(\Theta, \zeta_8)$ but notice $\zeta_8 \sqrt{2} = 1 + i$

thus $\mathbb{Q}(\zeta_8) = \mathbb{Q}(i, \sqrt{2})$ and as $(\sqrt[4]{2})^2 = \sqrt{2}$

we deduce $\boxed{K = \mathbb{Q}(\sqrt[8]{2}, i)}$

Remark: $[\mathbb{Q}(\sqrt[8]{2}) : \mathbb{Q}] = 8$ and $[\mathbb{Q}(i) : \mathbb{Q}] = 2$

since $\mathbb{Q}(i) \not\subseteq \mathbb{Q}(\sqrt[8]{2}) \subseteq \mathbb{R}$ we find

$[\mathbb{Q}(\sqrt[8]{2}, i) : \mathbb{Q}] = 16.$

GALOIS GROUP: $\mathrm{Aut}(K/\mathbb{Q}) = \mathrm{Aut}(K)$

$$\begin{cases} \Theta \longmapsto \zeta^a \Theta \\ i \longmapsto \pm i \end{cases}$$

16 possibilities, and since K is splitting field we deduce these are all automorphisms.

continuing splitting field of x^8-2

After much calculation (see p. 578) if we define

$$\sigma: \begin{cases} \theta \longmapsto \zeta\theta \\ i \longmapsto i \\ \zeta \longmapsto \zeta^5 = -\zeta \end{cases} \qquad \tau: \begin{cases} \theta \longmapsto \theta \\ i \longmapsto -i \\ \zeta \longmapsto \zeta^7 \end{cases}$$

It turns out,

$$\boxed{\mathrm{Gal}(\mathbb{Q}(\sqrt[8]{2}, i)/\mathbb{Q}) = \langle \sigma, \tau \mid \sigma^8 = \tau^2 = 1, \sigma\tau = \tau\sigma^3 \rangle}$$

this is the quasidihedral group, interestingly,

$$\langle \sigma^2, \tau \rangle \cong D_8 \,, \quad \langle \sigma \rangle \cong \mathbb{Z}_8 \,, \quad \langle \sigma^2, \tau\sigma^3 \rangle \cong Q_8$$

with fixed fields,

$$\mathbb{Q}(\sqrt{2}) \,, \quad \mathbb{Q}(i) \,, \quad \mathbb{Q}(\sqrt{-2})$$

Look at pg. 580 – 581 for the group / field diagrams for this beast of an example.

We have shown $[\mathbb{Q}(\zeta_n):\mathbb{Q}] = \varphi(n)$. Notice any automorphism of $\mathbb{Q}(\zeta_n)$ is fixed by its action on ζ_n which must map to $(\zeta_n)^k$ where $\gcd(k,n) = 1$; $\sigma(\zeta_n) = \zeta_n^k$ where $k \in U(n)$ there are $|U(n)| = \varphi(n)$ choices for k thus each such σ is an automorphism.

Thm (26) The Galois group of the cyclotomic field $\mathbb{Q}(\zeta_n)$ is isomorphic to $\mathbb{Z}_n^\times = U(n)$ and the isomorphism is given by

$$\sigma_a(\zeta_n) = \zeta_n^a$$

in the sense $a \longmapsto \sigma_a$ for $a \in U(n)$.

Proof: $(\sigma_a\sigma_b)(\zeta_n) = \sigma_a(\zeta_n^b)$

$$= (\zeta_n^b)^a$$
$$= \zeta_n^{ba}$$
$$= \zeta_n^{ab}$$
$$= \sigma_{ab}(\zeta_n) \quad \therefore \underline{\sigma_a\sigma_b = \sigma_{ab}}.$$

It follows $\psi(a) = \sigma_a$ defines homomorphism of $U(n)$ and $\mathrm{Aut}(\mathbb{Q}(\zeta_n))$ and it is clearly a bijection $\therefore \psi$ is group isomorphism. //

E4 $\mathbb{Q}(\zeta_5)$ is Galois over $\mathbb{Q}$ with

$G = Gal(\mathbb{Q}(\zeta_5)/\mathbb{Q}) \cong \mathbb{Z}_5^\times \cong \mathbb{Z}_4$

$G = \{1, \sigma_2, \sigma_3, \sigma_4\}$

$\sigma_2(\zeta_5) = \zeta_5^2$

$\sigma_2\sigma_2(\zeta_5) = \zeta_5^4$

$\sigma_2\sigma_2\sigma_2(\zeta_5) = (\zeta_5^4)^2 = \zeta_5^8 = \zeta_5^3$

$\sigma_2\sigma_2\sigma_2\sigma_2(\zeta_5) = \sigma_2(\zeta_5^3) = (\zeta_5^2)^3 = \zeta_5^6 = \zeta_5$

Remark: $1 + \zeta_5 + \zeta_5^2 + \zeta_5^3 + \zeta_5^4 = 0$

Consider fixed subfield of $\{1, \sigma_4\}$

we can show that $K^{\{1,\sigma_4\}} = \mathbb{Q}(\zeta_5 + \zeta_5^{-1}) = \mathbb{Q}(\sqrt{5})$.

$\{1\}$	$\mathbb{Q}$
2	2
$\{1, \sigma_4\}$	$\mathbb{Q}(\sqrt{5})$
2	2
$\{1, \sigma_2, \sigma_3, \sigma_4\}$	$\mathbb{Q}(\zeta_5)$

Fun with Galois Conjugates!