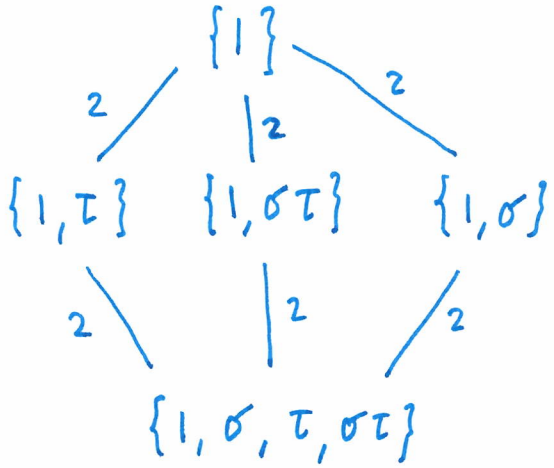
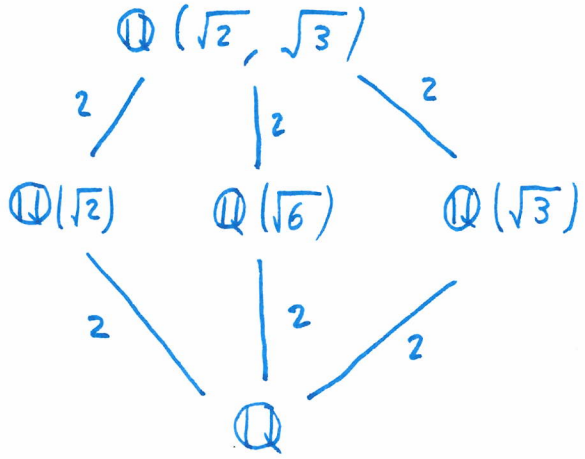
Lecture 22: Fundamental Theorem of Galois Theory

Last lecture we analyzed $\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}$,



subgroups of Galois group $\mathrm{Gal}(\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q})$



subfields of $\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}$

We defined $\sigma(\sqrt{2}) = -\sqrt{2}$ and $\tau(\sqrt{3}) = -\sqrt{3}$ whereas $\sigma\tau(\sqrt{2}) = -\sqrt{2}$ and $\sigma\tau(\sqrt{3}) = -\sqrt{3}$ then the <u>fixed fields</u> for $K = \mathbb{Q}(\sqrt{2},\sqrt{3})$ can be easily seen

$$K^{\{1,\sigma\}} = \{\alpha \in K \mid \sigma(\alpha) = \alpha\} = \mathbb{Q}(\sqrt{3}) \qquad \sigma(\sqrt{3}) = \sqrt{3}$$

$$K^{\{1,\tau\}} = \{\alpha \in K \mid \tau(\alpha) = \alpha\} = \mathbb{Q}(\sqrt{2}) \qquad \tau(\sqrt{2}) = \sqrt{2}$$

$$K^{\{1,\sigma\tau\}} = \{\alpha \in K \mid \sigma\tau(\alpha) = \alpha\} = \mathbb{Q}(\sqrt{6}) \qquad \sigma\tau(\sqrt{6}) = \sqrt{6}.$$

E1 Analyze the splitting field of $X^3 - 2$ over $\mathbb{Q}$

We have roots $\sqrt[3]{2}$, $\rho\sqrt[3]{2}$, $\rho^2\sqrt[3]{2}$ where $\rho = \frac{-1+i\sqrt{3}}{2}$

$K = \mathbb{Q}(\sqrt[3]{2}, \rho\sqrt[3]{2}, \rho^2\sqrt[3]{2})$ $\quad \zeta_3 = e^{\frac{2\pi i}{3}} = \rho$

we can do with less
what is a minimal list?

$$\frac{\rho^2\sqrt[3]{2}}{\rho\sqrt[3]{2}} = \rho \quad \text{and} \quad \frac{\rho\sqrt[3]{2}}{\sqrt[3]{2}} = \rho$$

$\rho, \sqrt[3]{2}$ generate $\sqrt[3]{2}, \rho\sqrt[3]{2}, \rho^2\sqrt[3]{2}$

$\sqrt[3]{2}, \rho\sqrt[3]{2}$ generate $\sqrt[3]{2}, \rho\sqrt[3]{2}, \frac{(\rho\sqrt[3]{2})^2}{\sqrt[3]{2}} = \rho^2\sqrt[3]{2}$.

Let's consider $K = \mathbb{Q}(\sqrt[3]{2}, \rho)$.

- any automorphism of K, say σ, must map $\sqrt[3]{2}$ to $\sqrt[3]{2}$, $\rho\sqrt[3]{2}$ or $\rho^2\sqrt[3]{2}$ (roots of X^3-2) and must map ρ to ρ or ρ^2 (roots of $\Phi_3(x) = x^2+x+1$)
So we face <u>six</u> choices for σ

$$\sigma: \begin{cases} \sqrt[3]{2} \longmapsto \rho\sqrt[3]{2} \\ \rho \longmapsto \rho \end{cases} \qquad \tau: \begin{cases} \sqrt[3]{2} \longmapsto \sqrt[3]{2} \\ \rho \longmapsto \rho^2 = -1-\rho \end{cases}$$

The formulas above serve to define σ and τ on K since $K = \mathbb{Q}(\sqrt[3]{2}, \rho)$ has basis of six elements

$$\{1, \sqrt[3]{2}, (\sqrt[3]{2})^2, \rho, \rho\sqrt[3]{2}, \rho(\sqrt[3]{2})^2\}$$

and the fate of the generators $\sqrt[3]{2}$ and ρ fix the fate of any $\mathbb{Q}$-linear comb. of the above basis.

$$\sigma(\rho\sqrt[3]{2}) = \sigma(\rho)\sigma(\sqrt[3]{2}) = \rho\rho\sqrt[3]{2} = \rho^2\sqrt[3]{2}.$$
$$= -\sqrt[3]{2} - \rho\sqrt[3]{2}.$$

E1 continued

We can work out in lecture,

$$\alpha = a + b\sqrt[3]{2} + c\left(\sqrt[3]{2}\right)^2 + d\rho + e\rho\sqrt[3]{2} + f\rho\sqrt[3]{4}$$

maps to

$$\sigma\alpha = a - e\sqrt[3]{2} + (f-c)\sqrt[3]{4} + d\rho + (b-e)\rho\sqrt[3]{2} - c\rho\sqrt[3]{4}$$

Furthermore, we also have automorphisms given by,

$$1: \begin{cases} \sqrt[3]{2} \longmapsto \sqrt[3]{2} \\ \rho \longmapsto \rho \end{cases}$$

$$\sigma^2: \begin{cases} \sqrt[3]{2} \longmapsto \rho^2\sqrt[3]{2} \\ \rho \longmapsto \rho \end{cases}$$

$$\tau\sigma: \begin{cases} \sqrt[3]{2} \longmapsto \rho^2\sqrt[3]{2} \\ \rho \longmapsto \rho^2 \end{cases}$$

$$\tau\sigma^2: \begin{cases} \sqrt[3]{2} \longmapsto \rho\sqrt[3]{2} \\ \rho \longmapsto \rho^2 \end{cases}$$

Likewise,

$$\sigma\tau: \begin{cases} \sqrt[3]{2} \xmapsto{\tau} \sqrt[3]{2} \xmapsto{\sigma} \rho\sqrt[3]{2} \\ \rho \xmapsto{\tau} \rho^2 \xmapsto{\sigma} \rho^2 \end{cases} \quad \therefore \sigma\tau = \tau\sigma^2$$

In summary, $\sigma^3 = 1$, $\tau^2 = 1$ and $\sigma\tau = \tau\sigma^2 = \tau\sigma^{-1}$

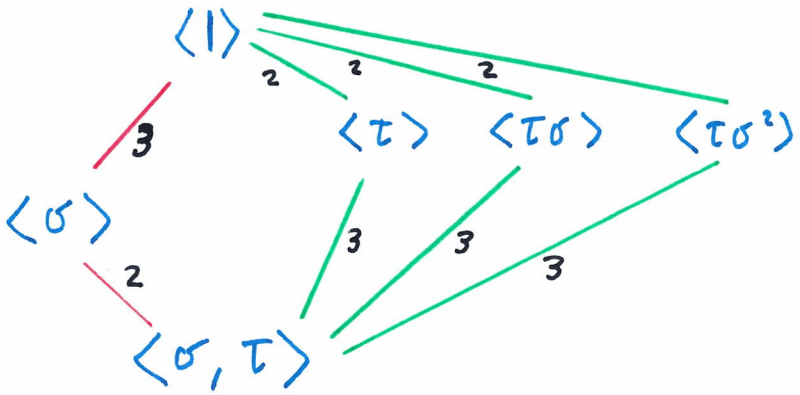
this is the symmetric group on $\{1,2,3\}$ up to isomorphism.

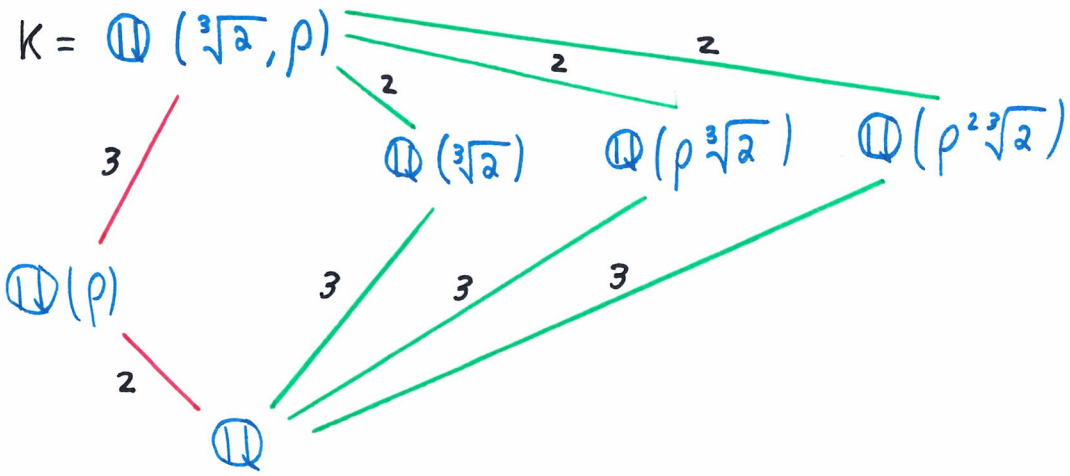
$$\boxed{\mathrm{Gal}\left(\mathbb{Q}(\sqrt[3]{2}, \zeta_3)/\mathbb{Q}\right) = \langle\sigma, \tau\rangle \cong S_3}$$

E| conclusion, fixed field & subgroup diagrams

$|\langle\tau\rangle| = |\{1, \tau\}| = 2$

$|\langle\sigma\rangle| = |\{1, \sigma, \sigma^2\}| = 3$





$K^{\langle\tau\rangle} = \mathbb{Q}(\sqrt[3]{2})$ ← $\tau(\sqrt[3]{2}) = \sqrt[3]{2}$

$K^{\langle\tau\sigma\rangle} = \mathbb{Q}(\rho\sqrt[3]{2})$ ← $\tau\sigma(\rho\sqrt[3]{2}) = \tau(\rho^2\sqrt[3]{2})$
$= \tau(\rho)\tau(\rho)\tau(\sqrt[3]{2})$
$= \rho^2\rho^2\sqrt[3]{2}$
$= \rho\sqrt[3]{2}.$

$K^{\langle\tau\sigma^2\rangle} = \mathbb{Q}(\rho^2\sqrt[3]{2})$

Remark: only the subgroup $\langle\sigma\rangle \trianglelefteq S_3$ since the index of $\langle\sigma\rangle$ is 2 in S_3 and only the subfield $\mathbb{Q}(\rho)$ is Galois over $\mathbb{Q}$.

$\underbrace{\mathbb{Q}(\sqrt[3]{2}), \mathbb{Q}(\rho\sqrt[3]{2}), \mathbb{Q}(\rho^2\sqrt[3]{2})}_{\text{degree 3 over } \mathbb{Q}}$ $\mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2})) = \mathrm{Aut}(\mathbb{Q}(\rho\sqrt[3]{2})) = \mathrm{Aut}(\mathbb{Q}(\rho^2\sqrt[3]{2})) = \{1\}$

In §14.2 of DSF a theory to analyze independence of automorphisms in terms of characters of a group

$$\chi : G \longrightarrow L^{\times}$$

with $\chi(g_1 g_2) = \chi(g_1)\chi(g_2)$ $\forall\, g_1, g_2 \in G$ (a group) and L a field with group of units $L^{\times}$, also $\chi(g) \neq 0$ $\forall g \in G$. They use characters from $K^{\times} \longrightarrow L^{\times}$ where there is some injective homomorphism of the field K into the field L. This machinery is then used with <u>linear algebra</u> to prove the following results,

Cor(8) If $\sigma_1, \sigma_2, \ldots, \sigma_n$ are distinct embeddings of a field K into a field L, then they are LI as functions on K. In particular, distinct automorphisms of a field K are LI as functions on K.

Th^{m}(9) Let $G = \{\sigma_1 = 1, \sigma_2, \ldots, \sigma_n\}$ be subgroup of $\mathrm{Aut}(K)$ and let $F = K^G$ be the fixed field of G. Then

$$[K : F] = [K : K^G] = n = |G|$$

<u>Proof</u>: see pg. 570-571, it's two pages of beautiful, somewhat sneaky linear algebra. One → proof to show $[K : F] \geq n$ followed by another → to show $[K : F] \not< n$ $\therefore$ $[K : F] = n$ follows.

Corollary (10) Let K/F be any finite extension. Then $|\mathrm{Aut}(K/F)| \leq [K : F]$ with equality iff F is the fixed field of $\mathrm{Aut}(K/F)$. That is, K/F is Galois iff $F = K^{\mathrm{Aut}(K/F)}$.

Corollary (11)

Let G be a finite subgroup of $\mathrm{Aut}(K)$ and let $F = K^G$ be the fixed field of G. Then every automorphism of K fixing F is contained in G i.e. $\mathrm{Aut}(K/F) = G$, so that K/F is Galois with $\mathrm{Gal}(K/F) = G$

$$\mathrm{Gal}(K/K^G) = G$$

Corollary (12)

If $G_1 \neq G_2$ are distinct finite subgroups of $\mathrm{Aut}(K)$ then $K^{G_1} \neq K^{G_2}$

Thm (13)

The extension K/F is Galois iff K is the splitting field of some separable polynomial over F. Furthermore, if this is the case then every irred. poly. with coeff in F which has a root in K is separable and has all its roots in K (so, in particular, K/F is separable extension)

Def^n/ Let K/F be a Galois Extension. If $\alpha \in K$ the elements $\sigma\alpha$ for $\sigma \in \mathrm{Gal}(K/F)$ are called the <u>conjugates</u> (or Galois conjugates) of α over F. If E is subfield of K containing F the field $\sigma(E)$ is called the <u>conjugate</u> field of E over F

THEOREM (14) [FUNDAMENTAL THEOREM OF GALOIS THEORY]

Let K/F be a Galois extension and set $G = Gal(K/F)$. Then there is a bijection

$$\left\{ \begin{array}{l} \text{subfields } E \\ \text{of } K \\ \text{containing } F \end{array} \quad \begin{array}{c} K \\ | \\ E \\ | \\ F \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{l} \text{subgroups } H \\ \text{of } G \end{array} \quad \begin{array}{c} 1 \\ | \\ H \\ | \\ G \end{array} \right\}$$

given by the correspondences

$$E \longrightarrow \{ \text{the elements of } G \text{ fixing } E \}$$

$$\{ \text{the fixed field of } H;\ K^H \} \longleftarrow H$$

which are inverse to one another. Under this correspondence,

(1.) (inclusion reversing) $H_2 \leq H_1 \iff K^{H_1} \leq K^{H_2}$

(2.) $[K : E] = [K : K^H] = |H|$ and $[E : F] = [K^H : F] = [G : H]$

$$\begin{array}{cl} K & \\ | & \} \ |H| \\ E & \\ | & \} \ [G : H] \\ F & \end{array}$$

(3.) K/E is always Galois with $Gal(K/E) = H$ which is to say $Gal(K/K^H) = H$.

$$\begin{array}{cl} K & \\ | & H \\ E & \end{array}$$

(4.) E is Galois over $F = K^H$ iff $H \trianglelefteq G$.

In this case

$$Gal(E/F) \cong G/H$$

$$Gal(E/K^H) \cong G/H$$

(5.) If E_1, E_2 I

(5.) If E_1, E_2 correspond to H_1, H_2 respectively then $E_1 \cap E_2$ corresponds to $\langle H_1, H_2 \rangle$ generated by H_1 and H_2 and the composite field $E_1 E_2$ corresponds to $H_1 \cap H_2$. Hence, the lattice of subfields of K containing F and the lattice of subgroups of G are "dual" (upside down to each other as we saw today)