Lecture 14.1

Last time:

- For a Galois extension K/F,

$$\left\{\begin{matrix}\text{subfields} \\ F \subseteq E \subseteq K\end{matrix}\right\} \longleftrightarrow \left\{\begin{matrix}\text{subgroups} \\ H \subseteq \mathrm{Gal}(K/F)\end{matrix}\right\}$$

$$\cup\!\!\!\!\;\mathsf{I} \qquad\qquad\qquad\qquad \cup\!\!\!\!\;\mathsf{I}$$

$$\left\{\begin{matrix}\text{normal subfields} \\ K^N/F\end{matrix}\right\} \longleftrightarrow \left\{\begin{matrix}\text{normal subgroups} \\ N \trianglelefteq \mathrm{Gal}(K/F)\end{matrix}\right\}$$

- When $N \trianglelefteq \mathrm{Gal}(K/F)$ is normal,

$$\mathrm{Gal}(K^N/F) \cong \mathrm{Gal}(K/F)/N.$$

Ex 1 We saw that for $K = \mathbb{Q}(\sqrt[3]{2})$,

$\mathrm{Aut}(K/\mathbb{Q}) = \{id\}$, so

$$K^{\mathrm{Aut}(K/\mathbb{Q})} = K \neq \mathbb{Q} \Rightarrow K/\mathbb{Q} \text{ is not Galois.}$$

However, a normal closure for $K/\mathbb{Q}$ is

$$L = \mathbb{Q}(\sqrt[3]{2}, \zeta), \quad \zeta = e^{2\pi i/3}.$$

By HW 9, Problem 1, $\mathrm{Gal}(L/\mathbb{Q}) \cong S_3$,

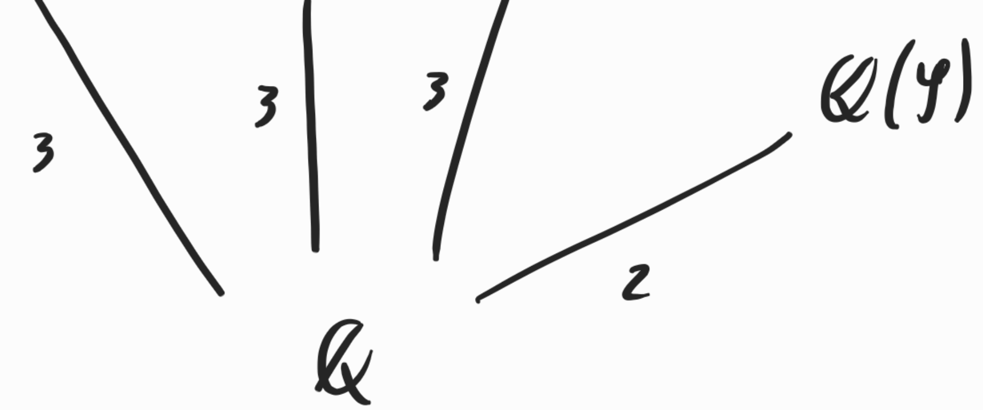
the symmetric group with 6 elements.

Here are the subfield and subgroup

diagrams for $L/\mathbb{Q}$:

$$
\begin{tikzcd}
 & & \{1\} \arrow[dll, dash, "2"'] \arrow[dl, dash, "2"'] \arrow[d, dash, "2"'] \arrow[dr, dash, "3"] & \\
\langle (1\,2) \rangle \arrow[drr, dash, "3"'] & \langle (1\,3) \rangle \arrow[dr, dash, "3"'] & \langle (2\,3) \rangle \arrow[d, dash, "3"'] & \langle (1\,2\,3) \rangle \arrow[dl, dash, "2"] \\
 & & S_3 = \{1, (1\,2), (1\,3), (2\,3), (1\,2\,3), (1\,3\,2)\} &
\end{tikzcd}
$$

$$
\begin{tikzcd}
 & & L = \mathbb{Q}(\sqrt[3]{2}, \zeta) \arrow[dll, dash, "2"'] \arrow[dl, dash, "2"'] \arrow[d, dash, "2"'] \arrow[ddr, dash, "3"] & \\
K = \mathbb{Q}(\sqrt[3]{2}) & \mathbb{Q}(\zeta \sqrt[3]{2}) & \mathbb{Q}(\zeta^2 \sqrt[3]{2}) &
\end{tikzcd}
$$



Exercise 1: Which subfields are normal extensions of $\mathbb{Q}$?

Exercise 2: Let K be a splitting field for $f(x) = x^4 - 2 \in \mathbb{Q}[x]$. Find all subfields of $K/\mathbb{Q}$ and describe which are normal extensions of $\mathbb{Q}$. (See 13.1 in the textbook for a solution.)

$\boxed{\text{Solvability}}$

With Galois theory at our disposal, we can now analyze whether polynomial equations of fixed degree are solvable by radicals.

$\boxed{\text{Def}}$ A polynomial $f(x) \in \mathbb{Q}[x]$ is **solvable** if all of the roots of f can be expressed in terms of the operations $+, -, \times, \div$ and $\sqrt[m]{\ }$ on elements of $\mathbb{Q}$.

$\boxed{\text{Lemma}}$ A polynomial $f(x) \in \mathbb{Q}[x]$ is solvable if and only if there exists a tower of field extensions

$$\mathbb{Q} = K_0 \subseteq K_1 \subseteq \ldots \subseteq K_r$$

such that:

(a) f splits in K_r.

(b) For each $j = 1, \ldots, r$,

$$K_j = K_{j-1}(\sqrt[m]{\beta_j})$$

for some $m \geq 2$ and some $\beta_j \in K_{j-1}$.

$\boxed{\text{Ex}}$ ② The quadratic formula says that every $f(x) = ax^2 + bx + c \in \mathbb{Q}[x]$ is solvable. Here,

$$\mathbb{Q} \subseteq K_1 = \mathbb{Q}(\sqrt{b^2-4ac}).$$

$\boxed{\text{Def}}$ A finite group G is solvable if there is a chain of subgroups

$$\{1\} = G_0 \leq G_1 \leq \cdots \leq G_r = G$$

such that for each $j = 1, \ldots, r,$

$G_{j-1} \trianglelefteq G_j$ and G_j / G_{j-1} is an abelian group.

$\boxed{\text{Theorem (Galois 1832)}}$ A polynomial $f(x) \in \mathbb{Q}[x]$ is solvable if and only if its Galois group

$$\mathrm{Gal}(f) := \mathrm{Gal}(K_f / \mathbb{Q})$$

is a solvable group.

Every subgroup of S_2, S_3 and S_4 is solvable, which is a fancy way of saying that a quadratic, cubic and quartic formula exist!

However, for all $n \geq 5$, S_n has subgroups that are not solvable.

Therefore there can be no quintic, sextic, ... formula in general.

Ex ③ $f(x) = x^5 + 20x + 16$ is an irreducible polynomial over $\mathbb{Q}$ with

$$\mathrm{Gal}(f) \cong A_5$$

which is not solvable. Therefore there is no "algebraic" formula for the roots of $f(x)$.

Exercise 3: Prove both assertions:

(i) $\mathrm{Gal}(K_f/\mathbb{Q}) \cong A_5$.

(ii) A_5 is not solvable.

4 The textbook provides another example:

$f(x) = x^5 - 6x + 3$ is irreducible over $\mathbb{Q}$ with Galois group $\mathrm{Gal}(f) \cong S_5$, which is not solvable.

Pf of Galois' Theorem: Let $f \in \mathbb{Q}[x]$ be solvable and take $K/\mathbb{Q}$ to be a splitting field of f, so that

$$\mathrm{Gal}(f) = \mathrm{Gal}(K/\mathbb{Q}).$$

Since $K/\mathbb{Q}$ is finite, $K = \mathbb{Q}(\alpha_1, \dots, \alpha_n)$ for some $\alpha_j \in \mathbb{C}$, with $\alpha_j^{m_j} \in \mathbb{Q}(\alpha_1, \dots, \alpha_{j-1})$ for some $m_j \geq 2$ by hypothesis.

We induct on n.

If $\alpha_1 \in \mathbb{Q}$ then $K = \mathbb{Q}(\alpha_2, \ldots, \alpha_n)$, so we can assume $\alpha_1 \notin K$.

Let $p_1 = p_{\alpha_1}$ be its minimal polynomial, which has degree ≥ 2 and is separable since we're working over $\mathbb{Q}$.

Then p_1 has another root, say $\beta \neq \alpha_1$, and $\omega = \dfrac{\alpha_1}{\beta}$ satisfies $\omega^{m_1} = 1$, $\omega \neq 1$, so ω is a root of $x^{m_1} - 1 \in \mathbb{Q}[x]$.

As in Lecture 10.2, where we proved

$\mathrm{Gal}(\mathbb{Q}(\zeta_5)/\mathbb{Q}) \cong (\mathbb{Z}/5\mathbb{Z})^\times$, it is possible

to show $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$ for

any $n \geq 2$.

Most importantly, this shows

$$\mathrm{Gal}(x^{m_1}-1) = \mathrm{Gal}(\mathbb{Q}(\zeta_{m_1})/\mathbb{Q}) \cong (\mathbb{Z}/m_1\mathbb{Z})^\times$$

is abelian.

Consider the tower

$$K = E(\alpha_2, \ldots, \alpha_n)$$

| solvable by induction

$$E = \mathbb{Q}(\zeta_{m_1}, \alpha_1)$$

|

$$F = \mathbb{Q}(\varphi_{m_1})$$

$$\Big| \text{ abelian}$$

$$\mathbb{Q}$$

Notice that $E = F(\alpha_1)$ and since $\alpha_1^{m_1} \in E$,

E/F is a splitting field for $x^{m_1} - \alpha_1^{m_1}$.

Exercise 4 below will show that $\mathrm{Gal}(E/F)$ is abelian.

Now $\mathrm{Gal}(K/\mathbb{Q})$ has a chain of subgroups

$$\mathrm{Gal}(K/\mathbb{Q}) \supseteq \mathrm{Gal}(K/F) \supseteq \mathrm{Gal}(K/E) \supseteq \{id\}$$

with:

- $\mathrm{Gal}(K/F) \trianglelefteq \mathrm{Gal}(K/\mathbb{Q})$ since $F = \mathbb{Q}(\varphi_{m_1})$

is a splitting field.

- $\mathrm{Gal}(K/\mathbb{Q}) / \mathrm{Gal}(K/F) \cong \mathrm{Gal}(F/\mathbb{Q})$ by the Fundamental Theorem, and $\mathrm{Gal}(F/\mathbb{Q})$ is abelian.

- $\mathrm{Gal}(K/E) \trianglelefteq \mathrm{Gal}(K/F)$ since E/F is a splitting field.

- $\mathrm{Gal}(K/F) / \mathrm{Gal}(K/E) \cong \mathrm{Gal}(E/F)$ is abelian.

- $\mathrm{Gal}(K/E)$ is solvable by induction.

This proves $\mathrm{Gal}(K/\mathbb{Q})$ is solvable. $\square$

Exercise 4: (a) Prove $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ is isomorphic to $(\mathbb{Z}/n\mathbb{Z})^\times$, which is abelian.

(b) For any $a \in F \subseteq \mathbb{C}$, prove that $\mathrm{Gal}(x^m - a)$ is abelian.

We didn't prove the converse of Galois' Theorem, but see section 18.4 in the textbook.

Next time: constructibility revisited.