Insolvability of the quinctic

Ex. Roots of x^2+x+1 are $\frac{-1\pm\sqrt{-3}}{2} = \frac{-1\pm i\sqrt{3}}{2} = \omega^{\pm 1}$

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{-3}) \leftarrow \text{splitting field of } x^2+x-1.$$

- Roots of x^3-6x+2

$$x = -\frac{1\pm i\sqrt{3}}{\sqrt[3]{-1+i\sqrt{7}}} - \frac{1}{2}(1\pm i\sqrt{3})\sqrt[3]{-1+i\sqrt{7}} \quad ,$$

$$x = \frac{2}{\sqrt[3]{-1+i\sqrt{7}}} + \sqrt[3]{-1+i\sqrt{7}}$$

So to get all the roots we do the following

$$\begin{array}{ccccccc}
\mathbb{Q} & \subseteq & \mathbb{Q}(i\sqrt{7}) & \subseteq & K_1(\sqrt[3]{-1+i\sqrt{7}}) & \subseteq & K_2(i\sqrt{3}) \\
\| & & \| & & \| & & \| \\
K_0 & & K_1 & & K_2 & & K_3
\end{array}$$

root of x^2+7 root of $x^3+1-i\sqrt{7}$ root of x^2+3

So in K_3 we factored x^3-6x+2. To get there we successively added "roots" i.e. we adjoined by α where α is a root of x^n-a irreducible in $K_i[x]$.

This is what it means to solve by radicals

Defn Let $f \in \mathbb{Q}[x]$, we say f is solvable by radicals if there's a chain of subfields $\mathbb{Q} = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_m \subseteq \mathbb{C}$ s.t.

1. K_m contains the splitting field of f (call it K_f)
2. $K_{i+1} = K_i(\alpha_i)$ where α_i is the root of a polynomial of the form $x^{n_i} - b_i \in K_i[x]$ $\forall\ 1 \leq i < m$.

- $K_i \subseteq K_{i+1}$ is called a radical extension
- Note, we may assume n_i is prime by splitting the extensions up: $\sqrt[10]{6} = \sqrt[5]{\sqrt{6}}$.

Thm Let L be the splitting field of $x^m - 1$ over $\mathbb{Q}$. Then $\mathrm{Gal}(L/\mathbb{Q}) \cong (\mathbb{Z}/m\mathbb{Z})^*$ and $L = \mathbb{Q}(\zeta_m)$ where $\zeta_m = e^{\frac{2\pi i}{m}}$.

Thm Let $f = x^m - a$, for $a \in \mathbb{Q}$. Then the splitting field L of f contains $\zeta_m = e^{\frac{2\pi i}{m}}$ and $\mathrm{Gal}(L/\mathbb{Q}(\zeta_m))$ is cyclic. If f is irreducible $\mathrm{Gal}(L/\mathbb{Q}(\zeta_m)) \cong \mathbb{Z}/m\mathbb{Z}$

We can replace $\mathbb{R}$ by $\mathbb{Q}$ in the previous example.

Ex. $\overset{=K_0}{\mathbb{Q}} \subseteq \overset{=K_1}{\mathbb{Q}(\zeta_3)} \subseteq \overset{=K_2}{\mathbb{Q}(\zeta_3, \sqrt[3]{2})}$

$\mathrm{Gal}(\,/\,) \cong \mathbb{Z}/2\mathbb{Z}$ $\qquad$ $\mathrm{Gal}(\,/\,) \cong \mathbb{Z}/3\mathbb{Z}$

$$\{e\} = \mathrm{Gal}(K_2/K_2) \trianglelefteq \mathrm{Gal}(K_2/K_1) \trianglelefteq \mathrm{Gal}(K_2/K_0)$$

(Fundamental thm + showing K_1 is galois over $\mathbb{Q}$)

$$\underset{G_0}{\{e\}} \subseteq \underset{G_1}{\langle (123) \rangle} \subseteq \underset{G_2}{S_3} = \mathrm{Gal}(K_2/\mathbb{Q})$$

$G_1/G_0 \cong \mathrm{Gal}(K_2/K_1) \cong \mathbb{Z}/3\mathbb{Z}$

$G_2/G_1 \cong \mathrm{Gal}(K_1/K_0) \cong \mathbb{Z}/2\mathbb{Z}$

Thus $S_3 = \mathrm{Gal}(K_2/\mathbb{Q})$ is solvable

<u>Thm</u>) f solvable by radicals $\iff \mathrm{Gal}(K_f/\mathbb{Q})$ is a solvable group.

Recall S_5 is not solvable as A_5 is simple (Hwk 4)

$\{1\} \subseteq A_5 \subseteq S_5$ and A_5 is not cyclic (or abelian).

Ex. S_2, S_3, S_4 are solvable

$(\{e\} \subseteq \langle (12)(34)\rangle \subseteq (\mathbb{Z}/2\mathbb{Z})^2 \subseteq A_4 \subseteq S_4)$

Also any subgroup of a solvable group is solvable.

Note $\mathrm{Gal}(K_f/\mathbb{Q}) \hookrightarrow S_{\deg f}$. Thus deg 2, 3, 4 polynomials are solvable by radicals.

Thm Let $f \in \mathbb{Q}[x]$ be irreducible, and suppose f has exactly two non-real roots. Then $\mathrm{Gal}(K_f/\mathbb{Q}) \cong S_5$.

Pf ① S_n is generated by a 2-cycle and an n-cycle

i.e. $S_n = \langle (12)(123\ldots n)\rangle$

② f has two non real roots, they are conjugate.

But $\varphi: \mathbb{C} \to \mathbb{C}$ by $a+bi \mapsto a-bi$ is an automorphism of $\mathbb{C}$!

Moreover φ fixes all the other roots of f

i.e. $\varphi: K_f \to K_f$ is well defined and gives a transposition.

③ Let α be a root of f,

$\mathbb{Q} \subseteq \mathbb{Q}(\alpha) \subseteq K_f$

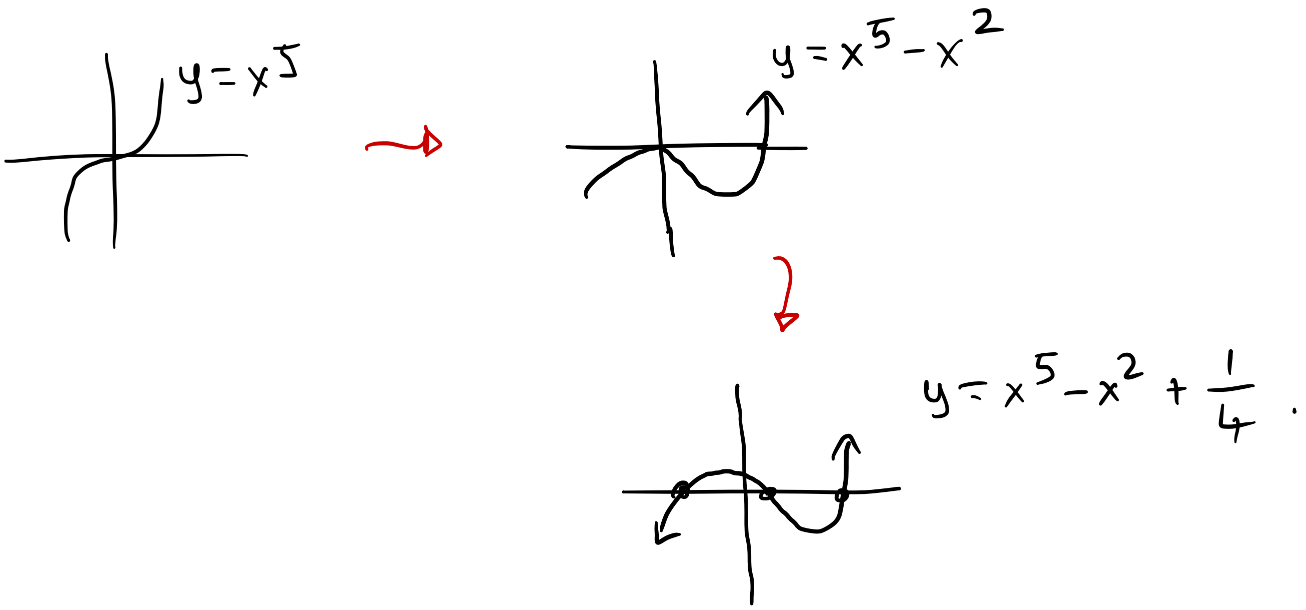
Then $[\mathbb{Q}(\alpha):\mathbb{Q}]=5$ and by fundamental theorem, $|\mathrm{Gal}(K_f/\mathbb{Q})| = [K_f:\mathbb{Q}]$

Since $[\mathbb{Q}(\alpha):\mathbb{Q}] \mid [K_f:\mathbb{Q}] \Rightarrow 5 \mid \mathrm{Gal}(K_f/\mathbb{Q})$.

Since $\mathrm{Gal}(K_f/\mathbb{Q})$ "$\subseteq$" S_5, any order 5 element is a 5-cycle $\Rightarrow$ $\mathrm{Gal}(K_f/\mathbb{Q})$ has a 5 cycle.

Thus $\mathrm{Gal}(K_f/\mathbb{Q}) \cong S_5$.

How to find such a polynomial



Check $x^5-x^2+\frac{1}{3}$ is irreducible.

I promised x^5-x-1. That also works for different reasons.