Syllabus + icebreaker

H/W #1 will be posted by Wednesday (due Tues 1/17)

Today: Overview of course

Important perspective shift: don't ask "what", ask "where" for sol'ns to polynomial eqn.

Two (very) classical problems:

1) Constructability via straightedge & compass:

e.g Given a cube, can we make a cube w/ 2x the volume?

i.e. Given a line segment of length 1, can we construct a line segment of length $\sqrt[3]{2}$?

2) Solvability by radicals:

Quadratic formula: $ax^2+bx+c=0$ has sol'ns

$$x = \frac{-b \pm \sqrt{b^2-4ac}}{2a}$$

Cubic formula (Cardano & others, '45 ... 1545):

$x^3+px+q=0$ has sol'ns

$$x = \sqrt[3]{-\frac{q}{2}+\sqrt{\frac{q^2}{4}+\frac{p^3}{27}}} + \sqrt[3]{-\frac{q}{2}-\sqrt{\frac{q^2}{4}+\frac{p^3}{27}}}$$

for compatible choices of the cube roots

Quartic formula (Ferrari, 1540)

relies on cubic formula

What about the quintic equation?

$$x^5 + ax^4 + bx^3 + cx^2 + dx + e = 0$$

Thm (Ruffini 1799, Abel 1824): There is no (general) "quintic formula" by radicals.

Galois (1830): New proof of Abel-Ruffini
- Provides specific polynomials that are not solvable by radicals

Method: connect field extensions to subgroups of "Galois group"

Def: A field extension E/F is a pair of fields $F \subseteq E$

$F(\alpha)$ means the smallest field containing F and α

e.g. $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is a field ext'n

Fact: E is a vector space over F with $\underbrace{[E:F]}_{\text{degree of ext'n}} := \dim_F E$

e.g. $\mathbb{Q}(\sqrt[3]{2}) = \{a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2 \mid a,b,c \in \mathbb{Q}\}$,

So $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$

Def: The splitting field of a polynomial p w/ coeffs. in F is $F(\text{roots of } p)$

e.g. $p(x) = x^3 - 2$ has roots $\sqrt[3]{2}$, $\omega\sqrt[3]{2}$, $\omega^2\sqrt[3]{2}$, ω: cube root of 1

So the splitting field of p is

$$\mathbb{Q}(\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2}) = \mathbb{Q}(\sqrt[3]{2}, \omega)$$

What is $[\mathbb{Q}(\sqrt[3]{2}, \omega) : \mathbb{Q}]$?

Tower law: If $F \subseteq K \subseteq E$, then

$$[E:F] = [E:K][K:F],$$

so $$[\mathbb{Q}(\sqrt[3]{2}, \omega) : \mathbb{Q}] = \underbrace{[\mathbb{Q}(\sqrt[3]{2}, \omega) : \mathbb{Q}(\sqrt[3]{2})]}_{2} \underbrace{[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}]}_{3} = 6$$

Constructability problems:

If we can construct a, b, we can construct: $a+b$, $a-b$, ab, a/b, $\sqrt{a}$

Start with $\mathbb{Q}$. Each "move" gives an extension with degree 1 or 2.

Tower law $\Rightarrow$ $[E:\mathbb{Q}]$ is power of 2

Doubling a cube: need to construct $2^{1/3}$, so

$$[E:\mathbb{Q}] = [E:\mathbb{Q}(2^{1/3})][\mathbb{Q}(2^{1/3}):\mathbb{Q}] \text{ is divisible by } 3$$

Impossible!

Now let E be the splitting field for p over F

The Galois group $\mathrm{Gal}(E/F)$ is the set of automorphisms of E that fix F; elements of $\mathrm{Gal}(E/F)$ permute the roots of p.

Fundemental Theorem of Galois Theory: In this setting, $\exists$ bijection

$$\left\{\begin{array}{l}\text{subfields} \\ k \text{ of } E \qquad F \subseteq k \subseteq E \\ \text{containing } F\end{array}\right\} \longleftrightarrow \left\{\begin{array}{c}\text{subgroups of} \\ \mathrm{Gal}(E/F)\end{array}\right\}$$

e.g.

$$\begin{tikzcd}[column sep=small]
& & \mathbb{Q}(\sqrt[3]{2}, \omega) \arrow[dll, dash] \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
\mathbb{Q}(\omega) \arrow[drr, dash] & \mathbb{Q}(\sqrt[3]{2}) \arrow[dr, dash] & \mathbb{Q}(\omega\sqrt[3]{2}) \arrow[d, dash] & \mathbb{Q}(\omega^2\sqrt[3]{2}) \arrow[dl, dash] \\
& & \mathbb{Q} &
\end{tikzcd}
\qquad
\begin{tikzcd}[column sep=small]
& & \{1\} \arrow[dll, dash] \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
\langle (123) \rangle \arrow[drr, dash] & \langle (12) \rangle \arrow[dr, dash] & \langle (13) \rangle \arrow[d, dash] & \langle (23) \rangle \arrow[dl, dash] \\
& & S_3 &
\end{tikzcd}$$

Galois' proof of Abel-Ruffini:

- p is solvable by radicals $\Leftrightarrow$ the Galois group of p is solvable
- There exist (many) polynomials with Galois group S_n
- S_n is not solvable for $n \geq 5$

Next time: start over from the beginning