HISTORY OF GALOIS THEORY

Part I : BEFORE GALOIS

(1) Babylonians (2000 BC)
Greeks (Euclid 300 BC)
Arabs (Omar Khayam 1000 AD) $\Big\}$ $x^2+bx+c=0$

$$(x+\tfrac{b}{2})^2 = \frac{b^2}{4}-c \qquad \text{rad equ of deg 2}$$

$$\begin{cases} x = y - \frac{b}{2} \\ y^2 = \frac{b^2}{4} - c \end{cases}$$

$$x = \frac{-b \pm \sqrt{\Delta}}{2}, \quad \Delta = b^2 - 4\cdot c$$

(2) Plato 300's BC interpreting a problem of Delos oracle : can one construct $\sqrt[3]{2}$ w/ straightedge & compass
(equivalently : can one solve $x^3-2=0$ using only sq roots.
(similarly : can one construct reg poly's, trisect angles, etc $\sqrt{\ }$?.

(3) del Ferro 1500's
Tartaglia (won contest)
Cardano (disclosed)

$$\underset{(*)}{x^3+px+q=0} \Leftarrow \begin{cases} x = u+v \\ \underbrace{(u+v)^3}_{u^3+v^3+3uv(u+v)}+p(u+v)+q=0 \end{cases} \Leftarrow \begin{cases} x=u+v \\ u^3+v^3=-q \\ 3uv=-p \end{cases}$$

$$\Leftarrow \begin{cases} x=u+v \\ u^3+v^3=-q \\ u^3v^3=-p^3/27 \end{cases} \Leftarrow \begin{cases} x=u+v \\ u^3=z_1 \\ v^3=z_2 \\ z_i^2+qz_i-\frac{p^3}{27}=0 \end{cases} \Leftarrow \begin{cases} x=\sqrt[3]{z_1}+\sqrt[3]{z_2} \\ z_{1,2} = \frac{-q\pm\sqrt{\Delta}}{2} \end{cases}$$

* Solved by "rad equs" of deg 2 & 3

Ferrari same for $x^4+ax^3+bx^2+cx+d=0$

comment : birth of $\mathbb{C}$ (b/c can happen $\Delta<0$ & $x\in\mathbb{R}$)

(4) Gauss 1800's

Th (FTA) Any $f\in\mathbb{C}[X]$ is a prod of lin factors (so has a root in $\mathbb{C}$).

Th $x^n-1=0$ is "solvable by radicals (of deg $< n$)"

Th $x^p-1=0$ * is "sol by rad's of deg 2 (square roots)" iff $p=2^{2^m}+1$ for some m (a Fermat prime)
(equivalently "a reg polyg w/ p sides is constructible iff p is Fermat").

Th (indep: Wantzel) $\sqrt[3]{2}$, $\cos 20^\circ$ not constructible (Plato's pblm)

(5) Abel 1800's

Th $x^5+ax^4+bx^3+\cdots+e=0$ (where $a,b,\dots,e$ indet) not "sol by rad's". ♡

* Solved by rad's of deg 2, 3

---

* p prime.

♡ For some values of $a,b,\dots$ it is, eg $x^5-c=0$ is

PART II GALOIS & AFTER.

Galois 1800's

Th Let $f \in \mathbb{Q}[x]$ irr (coeff #'s not letters!) & $\alpha_1,\dots,\alpha_n \in \mathbb{C}$ its roots.

Let K be the smallest subf of $\mathbb{C}$ s.t. $\alpha_1,\dots,\alpha_n \in K$. (note $K = \left\{ \frac{F(\alpha_1 \dots \alpha_n)}{G(\quad)} \right\}$ / ...)

Let $G = G(K/\mathbb{Q}) = \{\sigma : K \to K \mid \sigma \text{ field aut}\}$ (finite gr)

Then $f=0$ "sol by rad's" $\Leftrightarrow$ G solvable

((Cor: Gauss, Abel, Same for $\mathbb{Q}$ replaced by any subfield L of $\mathbb{C}$)

(Pblm 1: how to compute G from f w/o knowing α_i?

2: what G's can occur? (Inverse Gal. problem) $\Big\}$ OPEN in general)

Kronnecker 1800's

Th Let f as above be s.t. G abelian. Then its roots α_i are all $\mathbb{Q}$-lin combinations of (roots of $x^n-1=0$ (i.e. of) #'s of the form $\zeta_n^i := \cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n}$) ~~[illegible]~~

(note $\zeta_n^i = f(\frac{k}{n})$, $f(z) = e^{2\pi i z}$)

K's jugendtraum Prove smth similar w/ $\mathbb{Q}$ replaced by other subf of $\mathbb{C}$

Hilbert: some of K's jug... "abelian class field th." program (xpln! define $G(K/k)$ etc) $f(z)=e^{2\pi i z}$ repl by other hol fcns

Artin 1930's finished "abelian class field th". Given k find all K w/ $G(K/k)$ ab.

Also W/ f as above he attached to each prime $p \in \mathbb{Z}$ an elt $\sigma_p \in G$, he embedded $G \subset GL_N(\mathbb{C})$, he set $a_p = tr(\sigma_p)$ & constructed holo fcn $L(z)$ from a_p's.

He introduced the philosophy that L should have (magic properties like a fcnal eqn.) (hidden symmetry).

Shafarevich ≥ 1950

Th Any solvable group appears (as G) for some $f \in \mathbb{Q}[x]$.

Langlands ~1970, ..., Wiles 1995

Cases when Artin's L has the beautiful prop's.

& alg. geo. analogues Non-ab. class field th ????