Evariste Galois (1832)

Polynomfunktion (Grad n)

$$p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0 \in \mathbb{C}[x]$$

Fundamentalsatz der Algebra *(Carl Friedrich Gauß)*

$\Rightarrow$ Nullstellen *(Wurzeln)* $\xi_1, \xi_2, \cdots, \xi_n \in \mathbb{C}$ *zeroes (roots)*

$$p(x) = a_n(x-\xi_1)(x-\xi_2)\cdots(x-\xi_n)$$

*(elementar-)*symmetrische Funktionen $a_k/a_0 = s_k(\xi_1, \xi_2, \cdots, \xi_n)$

(invariant gegen Permutation der ξ_k)

Koeffizientenkörper a_k adjungieren

$$K := \mathbb{Q}\{a_{0,}a_1, a_2, \cdots, a_{n-1}\} \subset \mathbb{C} \qquad (a_n = 1)$$

Zerfällungskörper (galoissche) Körpererweiterung (Grad $\leq n$)

$$K \subset N := K(\xi_1, \xi_2, \cdots, \xi_n) \subset \mathbb{C} \qquad \textit{field extension}$$

Automorphismen-Gruppe

$$G := \{\alpha \mid \alpha : N \to N,\ (\forall a \in K)\ \alpha(a) = a\}$$

es gilt: Nullstelle $\mapsto$ Nullstelle

$$\alpha(\xi_i) = \xi_j \qquad (j \text{ passend})$$

daher $\alpha \mapsto \sigma_\alpha$ σ_α Permutation

(Wirkung) $\alpha(\xi_i) = \sigma_\alpha(\xi_i)$ auf $\{\xi_1, \xi_2, \cdots, \xi_n\}$

oder äquivalent $\alpha \mapsto \sigma_\alpha$ σ_α Permutation

$\alpha(\xi_i) = \xi_{\alpha}(i)$ auf $\{1, 2, \cdots, n\}$

also $G \cong \sigma(G) < S_n$ **Galois-Gruppe** von $p(x)$

Untergruppe Zwischenkörper = Fixkörper zu G

„Hauptsatz“ $H < G \quad \leftrightarrow \quad K < F < N$ *(Bijektion)*

Untergruppen von $G \leftrightarrow$ Oberkörper von K

$$K = F_0 < F_1 < \cdots < F_k < F_{k+1} = N \leftrightarrow$$

$$\leftrightarrow \ \{e\} = H_{k+1} < H_k < \cdots < H_1 < H_0 = G$$

Grad der Erweiterung von F_i auf F_{i+1} = Index von H_{i+1} in H_i

---

allgemeine Gleichung n-ten Grades Galoisgruppe S_n

Konstruktionen mit Zirkel und Lineal

Die folgenden klassischen Aufgaben sind

„*mit Zirkel und Lineal*“ nicht lösbar:

Würfelverdoppelung *(Delisches Problem)* $\sqrt[3]{a} \in N \;\Rightarrow\;$ 3 teilt Grad

Quadratur des Kreises:

(Lindemann 1882) π ist transzendent. $\Rightarrow\; \pi, \sqrt{\pi}, 1/\pi, \cdots :$

$\Leftrightarrow\quad (\forall p \in \mathbb{C}[x])\; p(\pi) \neq 0$ Grad nicht endlich

Winkeldreiteilung (Grad von $\sin\varphi/3$ über $\sin\varphi$)

regelmäßiges n-eck *(Gauß 1796)*

konstruierbar $\Leftrightarrow$ $n = 2^k p_1 p_2 \cdots p_m$ $p_i = 2^{s(i)} + 1$

(Fermatsche Primzahlen) $3, 5, 17, 257, 65537$ $p = 2^{2^s} + 1$ *(alle?)*

(Satz von Abel) Niels Henrik Abel (1826)

Die *allgemeine* Gleichung n-ten Grades $(n \geq 5)$
ist nicht durch Radikale lösbar.

Lösung durch Radikale $\sqrt[m]{\cdots \sqrt[n]{\cdots}}$

$\leftrightarrow$ Folge von *reinen* Gleichungen $x^n - a = 0,\; x^m - b = 0,\; \ldots$

Grundkörper $K = \mathbb{Q}(a, \zeta_n)$ ζ_n Einheitswurzel

Galoisgruppe von $K < K(\sqrt[n]{a})$ C_n zyklisch (kommutativ)

$\zeta_n, \zeta_m, a \in K, b \in F_1 := K(\sqrt[n]{a}), F_2 := F_1(\sqrt[m]{b})$ *(zwei Radikale)*

$K = F_0 < F_1 < F_2 \quad\Leftrightarrow\quad G_1 < G_0$ *(über K)*

$(\forall \alpha, \beta \in G_0)$ $\Rightarrow\quad \alpha\beta\alpha^{-1}\beta^{-1} \in G_1$ *(Kommutator)*

daher: Folge von Erweiterungen durch Radikale $\Rightarrow$

$$G_1 < G_2 < \cdots < G_{n-1} < G_n = S_n$$

mit G_1 kommutativ

aber: Der Kommutator der Dreierzyklen enthält alle Dreierzyklen
für S_n $(n \geq 5)$ *(Rekursion)* $\Rightarrow$ G_1 enthält alle Dreierzyklen

$\Rightarrow\quad G_1$ ist nicht kommutativ *Widerspruch!* ∎