Erinnerung:

7.8.2 Definition: (a) Ein Körperturm $K_m/\ldots/K_0$, bei dem jedes K_i/K_{i-1} eine einfache Radikalerweiterung ist, heisst ein *Radikalturm*.

(b) Ein Polynom $f \in K[X]$ heisst *auflösbar durch Radikale*, wenn es einen Radikalturm $K_m/\ldots/K_0 = K$ gibt, so dass f über K_m in Linearfaktoren zerfällt.

7.8.3 Satz: *(Abel-Ruffini)* Sei L/K endlich galoissch mit $\mathrm{char}(K) = 0$. Dann sind äquivalent:

(a) Es existiert ein Radikalturm $K_m/\ldots/K_0 = K$ mit $L \subset K_m$.

(b) $\mathrm{Gal}(L/K)$ ist auflösbar.

Beweisskizze: (b) $\Rightarrow$ Wähle $1 = \Gamma_0 \lhd \Gamma_1 \lhd \ldots \lhd \Gamma_r = \mathrm{Gal}(L/K)$, Γ_i/Γ_{i-1} zyklisch.

Erster Körper $K(\zeta_n)$ für $n := [L:K]$. $\Rightarrow \mathrm{Gal}(L(\zeta_n)/K(\zeta_n)) < \mathrm{Gal}(L/K)$.

$\Rightarrow$ L über $L(\zeta_n)$ $\quad L = L_0/L_1/\ldots/L_r = K$ entsprechender Zwischenkörper.

$\Rightarrow$ Jede K_{i-1}/K_i ist zyklisch deren Ordnung $|n$; $\zeta_n \in K_i \Rightarrow K_{i-1}/K_i$ einfache Radikalerweiterung.

(a) $\Rightarrow$ Für die normale Hülle $\tilde{K}_m$ von K_m in $\bar{K}$ gilt: $\tilde{K}_m = \prod_{\sigma \in \mathrm{Hom}(K_m, \bar{K})} \sigma(K_m)$.

$\Rightarrow$ existiert ein Radikalturm $\tilde{K}_m/\ldots/K_0 = K$.

$\Rightarrow$ Obda K_m/K galoissch und $\mathrm{Gal}(\tilde{K}_m/K) \twoheadrightarrow \mathrm{Gal}(L/K)$.

Genügt zu zeigen: $\mathrm{Gal}(K_m/K)$ auflösbar.

---

qed.

7.8.4 Satz: Für $n \geqslant 5$ existiert keine Formel in Termen der vier Grundrechenarten und beliebigen Wurzeln, welche für beliebige Wahl der Variablen $b_0, \ldots, b_n$ in einem Körper K der Charakteristik Null eine Nullstelle des Polynoms $\sum_{i=0}^{n} b_i X^i$ produziert.

Man sagt also: *Die allgemeine Gleichung vom Grad $n \geqslant 5$ ist nicht auflösbar durch Radikale.*

Beweis: Sei L/K Zerfällungskörper eines Polynoms vom Grad n mit $\mathrm{Gal}(L/K) = S_n$.

Gleichungen vom Grad $\leqslant 4$ sind aber auflösbar durch Radikale:

7.8.5 Spezialfall: Jedes quadratische Polynom $aX^2 + bX + c$ über einem Körper K der Charakteristik $\neq 2$ hat die Nullstellen

$$\frac{-b \pm \sqrt{b^2 - 4ac}}{2a} \in \overline{K}.$$

7.8.6 Spezialfall: Betrachte ein kubisches Polynom $aX^3 + bX^2 + cX + d$ über einem Körper K der Charakteristik $\neq 2, 3$. Division durch a und die Variablensubstitution $X = Y - \frac{b}{3a}$ transformieren es in die Form $Y^3 + 3pY - 2q$ für gewisse $p, q \in K$. Dieses hat die Nullstellen

$$y_i := \zeta^i \cdot \sqrt[3]{q - \sqrt{p^3 + q^2}} + \zeta^{-i} \cdot \sqrt[3]{q + \sqrt{p^3 + q^2}} \in \overline{K}$$

für $i = 0, 1, 2$ mit $\zeta := \frac{-1+\sqrt{-3}}{2}$ und einer geeigneten Wahl der Wurzeln in $\overline{K}$.

Nullstellen x_1, x_2, x_3

$\mathrm{Disc}\, p = -4 \cdot 27 \cdot (p^3 + q^2) = 2^2 \cdot 3^3 \cdot \sqrt{-3}^2 \cdot (p^3 + q^2)$

$L = K(x_1, x_2, \sqrt{-3})$

$K(\sqrt{-3}, \sqrt{p^3 + q^2})$ } zyklisch Grad 1, 3

$K(\sqrt{-3})$

K

Ansatz: $a := x_1 + \zeta x_2 + \zeta^2 x_3$.

$\Rightarrow a^3 = \ldots = 27q + 3 \cdot \frac{\sqrt{-3}}{2} \cdot \sqrt{D}$

$9 \cdot \sqrt{p^3 + q^2}$

$\left(\frac{a}{3}\right)^3 = q + \sqrt{p^3 + q^2}$

Löse LGS

Analog $a' := \kappa_1 + \zeta^2 \kappa_2 + \zeta \kappa_3$

$\Rightarrow \left(\frac{a'}{3}\right)^3 = q - \sqrt{p^3 + q^2}$

$0 = \kappa_1 + \kappa_2 + \kappa_3$

$\kappa_1 = a + a'$

$\kappa_2 = \zeta a + \zeta^2 a'$

$\kappa_3 = \zeta^2 a + \zeta a'$

$aa' = \ldots = -p.$

7.8.7 Spezialfall: Jedes Polynom $aX^4 + bX^3 + cX^2 + dX + e$ vom Grad 4 über einem Körper der Charakteristik $\neq 2, 3$ ist auflösbar durch Radikale. Explizite Lösungsformeln werden in der Vorlesung und den Übungen entwickelt.

Ansatz: $S_4 \supset H = \langle (12)(34), (13)(24) \rangle \Rightarrow (14)(23)$

$X_1, \dots X_4$ Variable.

$$z_1 := X_1X_2 + X_3X_4 \Rightarrow \mathrm{Stab}_{S_4}(z_1) = D_4$$
$$z_2 := X_1X_3 + X_2X_4$$
$$z_3 := X_1X_4 + X_2X_3$$

$\mathrm{Stab}_{S_4}(z_1) \cap \mathrm{Stab}_{S_4}(z_2) = H$.

$$G(u) := (u - z_1)(u - z_2)(u - z_3) \in L^{S_4}[u].$$
$$= u^3 - s_2u^2 + (s_1s_3 - 4s_4)u - (s_1^2s_4 - 4s_2s_4 + s_3^2)$$

$L = k(X_1, \dots X_4)$

$L^H = L^{S_4}(z_1, z_2, z_3)$

$L^{S_4} = k(s_1, \dots s_4)$

Einsetzen liefert $g \in k[u]$ vom Grad 3.
Beschreibe deren Lösungen durch Radikale.

$t_1 = X_1 + X_2 - X_3 - X_4$
$t_2 = X_1 + X_3 - X_2 - X_4$
$t_3 = X_1 + X_4 - X_2 - X_3$
$t_4 = X_1 + X_2 + X_3 + X_4 = s_1$

$t_1^2 = s_1^2 - 4z_1 - 4z_2 \Rightarrow t_1 = \sqrt{s_1^2 - 4z_1 - 4z_2}$ etc.
$t_2^2 = s_1^2 - 4z_1 - 4z_3$
$t_3^2 = s_1^2 - 4z_2 - 4z_3$.

Löse LGS. $\Rightarrow$ alle $X_1, \dots X_4$.

7.9 Explizite Bestimmung der Galoisgruppe

Betrachte das Polynom in $2n+1$ Variablen

$$G := \prod_{\sigma \in S_n} \Big(Z - \sum_{i=1}^{n} Y_i X_{\sigma i} \Big) \in \mathbb{Z}[Z, Y_1, \ldots, Y_n, X_1, \ldots, X_n].$$

Da es in den Variablen $X_1, \ldots, X_n$ symmetrisch ist, existiert ein eindeutiges Polynom in $1+2n$ Variablen $\overline{G} \in \mathbb{Z}[Z, Y_1, \ldots, Y_n, U_1, \ldots, U_n]$, so dass mit den elementarsymmetrischen Polynomen $S_1, \ldots, S_n \in \mathbb{Z}[X_1, \ldots, X_n]$ gilt

$$G = \overline{G}(Z, Y_1, \ldots, Y_n, S_1, \ldots, S_n).$$

$S_i \mapsto S_i$.

Betrachte nun ein separables Polynom

$$f(X) = \sum_{i=0}^{n} (-1)^i b_i X^{n-i} = X^n - b_1 X^{n-1} + - \ldots + (-1)^n b_n \in K[X].$$

Seien $a_1, \ldots, a_n \in L = K(a_1, \ldots, a_n)$ seine Nullstellen und $\Gamma = \mathrm{Gal}(L/K) < S_n$ seine Galoisgruppe. Betrachte das Hilfspolynom

$$g := \overline{G}(Z, Y_1, \ldots, Y_n, b_1, \ldots, b_n) \in K[Z, Y_1, \ldots, Y_n].$$

7.9.1 Satz: Für jeden irreduziblen Faktor h von g existiert ein $\sigma \in S_n$ mit

$$\big\{ \tau \in S_n \;\big|\; h(Z, Y_{\tau 1}, \ldots, Y_{\tau n}) = h \big\} = {}^{\sigma}\Gamma.$$

7.9.2 Folge: Sei K ein Körper, für den ein Algorithmus existiert, der jedes Polynom in beliebig vielen Variablen über K in irreduzible Faktoren zerlegt. Dann existiert ein Algorithmus zur Bestimmung der Galoisgruppe jedes separablen Polynoms über K.

7.9.3 Spezialfall: (Vgl. §4.7) Insbesondere existiert ein solcher Algorithmus für $K = \mathbb{Q}$.

7.9.4 Satz: Sei zusätzlich $f \in \mathbb{Z}[X]$. Sei p eine Primzahl, welche die Diskriminante von f nicht teilt. Sei $f \bmod (p)$ ein Produkt irreduzibler Polynome in $\mathbb{F}_p[X]$ der Grade $n_1 + \ldots + n_r = n$. Dann enthält Γ eine Permutation, deren zugehörige Partition von n die Form $n_1 + \ldots + n_r = n$ hat.

7.9.5 Beispiel: Die Galoisgruppe von $f(X) := X^4 + 3X^3 - X^2 + 1$ über $\mathbb{Q}$ ist die S_4.

Die Galoisgruppe von $f(X) := X^5 + 2X^2 + 1$ über $\mathbb{Q}$ ist die S_5.

Die Galoisgruppe von $f(X) := X^7 + 3X^2 + 5$ über $\mathbb{Q}$ ist die S_7.

Die Galoisgruppe von $f(X) := X^5 + 20X + 16$ über $\mathbb{Q}$ ist die A_5.

$\equiv X^4+X^3+X^2+1$

$= (X+1)(X^3+X+1) \mod(2) \Rightarrow$ Gal $\ni$ 3-Zykel.
irred.

$\equiv X^4+2X^2+1 = (X^2+1)^2 \mod(3)$

irred. $\mod(p) \Rightarrow$ Gal $\ni$ 4-Zykel.

$\Rightarrow S_4$.

Disc = Quadrat $\Leftrightarrow f$ in $\mathbb{Q}$.

$f \mod(2) = X^7+X^2+1$

$= (X^2+X+1)(X^5+X^4+X^2+X+1)$

irred. irred.

$\Rightarrow$ Gal $\ni (12)(3457)$

$f \mod(3) = (X-1)(X^6+X^5+\ldots+X+1)$

irred.

$\Rightarrow$ Gal $\ni$ 6-Zykel.

$\Rightarrow$ Gal $= S_7$.

Bsp.: $X^3+8X^2-3 = f$

mod(2): $X^3+1 = (X+1)(X^2+X+1)$ $\Rightarrow$ Gal $\ni$ Transp.
(irred.)

mod(3): $X^3-X^2 = (X-1)X^2$

mod(5): X^3-2X^2+2

$\pm 8 - 2\cdot 8 + 2 = \pm 8 + 1 \neq 0$

$\Rightarrow$ irred. $\Rightarrow$ Gal $\ni$ 3-Zykel.

$\Rightarrow$ Gal $= S_3$.