A25: Auflösbarkeit durch Radikale

25.1. Einl.: Polynom $f \in K[T]$ sep. auffl'bar durch Radikale $\Leftrightarrow$ Gal S_n auflösbar $\Leftrightarrow n \le 4$

$:\Leftrightarrow \exists$ Radikalerw., die ZK E enthält

$\hookrightarrow \exists$ Radikalturm

$$\begin{array}{l} L = K_n \ldots \\ \quad | \\ \quad K_2 = K_1(x_1),\ x_1^{m_1} \in K_1 \\ E \quad | \\ \quad K_1 = K_0(x_0),\ x_0^{m_0} \in K_0 \\ \quad K = K_0 \end{array}$$

Radikalturm

Def. A8.3: $\exists$ NR aus ab. Faktoren

$\left(N_1 \trianglelefteq N_2 \trianglelefteq \ldots \trianglelefteq G,\ N_{i+1}/N_i \text{ ab. Gr.} \right)$

25.2. Satz: Sei $\operatorname{Char} K = 0$ (f sep.). Dann: $f \in K[T]$ auflösbar durch Radikale $\Leftrightarrow$ Galoisgruppe von $f|K$ auflösbar

Bew.: „$\Rightarrow$": * Sei $\tilde{L}$ Rad.erw. eines ZK L von $f|K$.

Die normale Hülle N von $\tilde{L}|K$ ist ebenso Radikalerw. nach Lemma A24.10.

Sei $K = K_0 \subseteq K_1 \subseteq \ldots \subseteq K_r = N$ ein Rad.turm für $N|K$ vom Typ $(n_1, n_2, \ldots, n_r)$

d.h. $K_i = K_{i-1}(x_i)$, $x_i^{m_i} \in K_{i-1}$.

$$\begin{array}{lll} & N(\zeta) & e \\ & N & \cap\!| \\ & \vdots & \vdots \\ \tilde{L} & & \cap\!| \\ & K_i(\zeta) & G_i \\ & K_i & \cap\!| \\ & K_{i-1}(\zeta) & G_{i-1} \\ & K_{i-1} & \cap\!| \\ & \vdots & \vdots \\ & K_2(\zeta) & G_2 \\ L & K_2 & \cap\!| \\ & K_1(\zeta) & G_1 \\ & K_1 & \cap\!| \\ & K_0(\zeta) & G_0 \\ & K_0 = K & G \end{array}$$

* Sei $n := \operatorname{kgV}(n_1, \ldots, n_r)$, ζ eine primitive n-te EW über N.

Betr. Radikalturm

$K = K_0 \subseteq K_0(\zeta) \subseteq K_1(\zeta) \subseteq \ldots \subseteq K_{i-1}(\zeta) \subseteq K_i(\zeta) \subseteq \ldots \subseteq N(\zeta)$

vom Typ $(n, n_1, \ldots, n_r)$.

Nun ist $N(\zeta)|K$ galois (denn: Ist N ZK von $g \in K[T]$ $\Rightarrow N(\zeta)$ ZK von $g \cdot (T^n - 1) \in K[T]$).

* Sei nun $G := \operatorname{Gal}(N(\zeta)|K)$, und $G_i := \operatorname{Gal}(N(\zeta)|K_i(\zeta))$.

$\forall i$: Es ist $K_i(\zeta)|K_{i-1}(\zeta)$ eine zyklische Galoiserw. nach Satz A24.7(1).

$\hookrightarrow$ d.h. G_i zyklische Gruppe

Nach dem HS der Galoistheorie A 23.10 ist G_i NT in G_{i-1},
und $\underbrace{G_{i-1}/G_i}_{\text{Faktorgruppe!}} \cong Gal(K_i(\zeta)|K_{i-1}(\zeta))$ zyklisch, $1 \le i \le r$.

* Nun $K(\zeta)|K$ ab. Galoiserw. nach Bem. A 22.16.
Somit: $G_0 \subseteq G$ ein NT und G/G_0 abelsch (laut HS),
also $G \supseteq G_0 \supseteq G_1 \supseteq \ldots \supseteq G_r = e$ ist NR für G
mit abelschen Faktoren, d.h. G ist auflösbar.

Nun: $G \longrightarrow Gal(L|K)$
$\sigma \longmapsto \sigma_{\restriction L}$ ist surj. Gruppenhom.
$\Rightarrow Gal(L|K)$ auflösbar. (Bild der NR ist NR, Inklusionen bleiben erhalten)
↳ vgl. Bew. 8.9.

„$\Leftarrow$": Sei $G = Gal(L|K)$ auflösbar, L ein ZK von $f|K$, $n := \# G$,
ζ eine primitive n-te EW in einer Erw. L.
$L(\zeta)|K(\zeta)$ ist galois, und $G' := Gal(L(\zeta)|K(\zeta)) \longrightarrow G$
$\sigma \longmapsto \sigma_{\restriction L}$,
ist injektiver Gruppenhom. ⌈die σ, die El. von $K(\zeta)$ festlassen, lassen El. von K fest.⌋
($\hookrightarrow G' \subseteq G$)
Dann ist $G' = Gal(L(\zeta)|K(\zeta))$ auflösbar (A 8.8: UG von auflösbaren Gr. sind auflösbar)
Sei nun $G' = G_0 \supseteq \ldots \supseteq G_r = e$ eine NR mit zyklischen Faktoren G_{i-1}/G_i
von Primzahlordnung p_i
(Satz A 8.12) ↳ also $p_i | n$.
Sei $K(\zeta) = K_0 \subseteq \ldots \subseteq K_{i-1} \subseteq \underset{\substack{\| \\ Fix(G_i)}}{K_i} \subseteq \ldots \subseteq K_r = L(\zeta)$ der zugeh. Körperturm.

Nach HS der Galoistheorie ist $K_i|K_{i-1}$ galois (da insb. normal)
und $Gal(K_i|K_{i-1}) \cong G_{i-1}/G_i$,
also ist $Gal(K_i|K_{i-1})$ zykl. der Ordnung p_i.
Nach Satz A 24.7(2) ist dann: $K_i = K_{i-1}(x_i)$ für einen $x_i \in K_i$ mit $x_i^{p_i} \in K_{i-1}$.
(denn K_{i-1} enthält alle n-ten EW, also alle p_i-ten EWeln). Also $L(\zeta)|K$ Radikalerw. □

25.3. Satz: Sei $\operatorname{Char} K = 0$. Dann ist jedes $f \in K[T]$ vom Grad ≤ 4 auflösbar durch Radikale.

Bew.: Die Galoisgr. G von f ist isom. einer UG von $\operatorname{Perm}(X)$ wenn X die Menge von Wurzeln von f ist, haben $n = \deg f$ und $\# X = n$, und $\operatorname{Perm}(X) \cong S_n$.

Da S_n auflösbar für $n \leq 4$ nach Kor. A 8.10, ist G auflösbar. $\square$

↳ p-q-Formel für $n=2$

wikipedia / dtv-Atlas zur Mathematik

für $n=3$: Cardano-Formeln / "Cardanische Formeln"

[Cardan / Ferrar → Jahr 1515]

für $n=4$: Ferrari-Formeln / "Quartische Gleichung"

25.4. Def.: Sei $n \geq 1$, $S_1, \dots, S_n$ Unbestimmte über K. Das Polynom

$$g(T) := T^n - S_1 T^{n-1} + S_2 T^{n-2} - \dots + (-1)^n S_n$$

$$\in \underbrace{K(S_1, \dots, S_n)}_{\text{Körper!}}[T]$$

heißt das allgemeine Polynom vom Grad n über K.

25.5. Satz: Für $n \geq 5$ ist das allg. Polynom vom Grad n über K nicht auflösbar über $K(S_1, \dots, S_n) =: K_1$.

Bew.: Sei L der ZK von $g(T)$ über K_1.

$$g(T) = \prod_{i=1}^{n} (T - x_i), \text{ es gilt: } S_1 = \sum_{i=1}^{n} x_i, \quad S_2 = \sum_{i<j} x_i x_j, \dots,$$

$$S_n = x_1 \cdots x_n.$$

Somit: $L = K(x_1, \dots, x_n)$.

Seien $X_1, \dots, X_n$ neue Unbestimmte über K, und

$$f(T) = \prod_{i=1}^{n} (T - X_i) \in K(X_1, \dots, X_n)[T],$$

also $f(T) = T^n - s_1 T^{n-1} + s_2 T^{n-2} - \dots + (-1)^n s_n$

wobei s_i die i-te elementarsymm. Fkt. in $X_1, \dots, X_n$.

Def. $\Phi : K[X_1,\dots,X_n] \to K[x_1,\dots,x_n]$ Ringhom.,

durch $\Phi \restriction K = id_K$, $\Phi(X_i) = x_i$. ⌜Durch Einsetzen der Wurzeln x_i von g⌟

Dann: $f^{\Phi} = \prod_{i=1}^{n} (T - X_i)^{\Phi} = \prod_{i=1}^{n} (T - x_i) = g$.

$\Rightarrow \Phi(s_i) = S_i$

$$\Rightarrow \Phi \restriction K[s_1,\dots,s_n] : K[\underbrace{s_1,\dots,s_n}] \to \overbrace{K[S_1,\dots,S_n]}^{\text{Pol.ring}}$$

ist <u>inj.</u> Ringhom., also Isom.

⌜ $\Phi(\underbrace{h(s_1,\dots,s_n)}) = 0 = h(\underbrace{S_1,\dots,S_n}_{\text{unbest.!}}) \Rightarrow h = 0$ ⌟

Somit:

$$\begin{tikzcd}
K(X_1,\dots,X_n) \arrow[r, dashed, "\tilde{\Phi}", "\cong"'] \arrow[d, dash] & K(x_1,\dots,x_n) = L \arrow[d, dash] \\
K(s_1,\dots,s_n) \arrow[r, dashed, "\tilde{\tilde{\Phi}}", "\cong"'] \arrow[d, dash] & K(S_1,\dots,S_n) = K_1 \arrow[d, dash] \\
K[s_1,\dots,s_n] \arrow[r, "\Phi", "\cong"'] & K[S_1,\dots,S_n]
\end{tikzcd}$$

⌜nach Satz A19.11, da $K(X_i)$ Zk von $K(s_i)$, $K(x_i)$ Zk von $K(S_i)$⌟

⌜Forts. auf Quot.Körper⌟

Also: $\underline{\underline{Gal(L|K_1)}} \cong Gal(\underbrace{K(X_1,\dots,X_n)|K(s_1,\dots,s_n)}) \cong S_n$,

vgl. Ann. A23.5, A23.8.

Also: g aufl'bar durch Radikale

$\overset{25.2}{\Leftrightarrow}$ $Gal(L|K_1)$ aufl'bar

$\Leftrightarrow$ S_n aufl'bar $\Leftrightarrow n \leq 4$.

Nun ist S_n für $n \geq 5$ nicht aufl'bar nach Kor. A8.10,

Somit: Satz 25.2 $\Rightarrow$ Beh. $\square$