Vorlesung Algebra

SoSe'21, hhu
K. Halupczok

Teil IV: und zurück (GALOISTHEORIE)

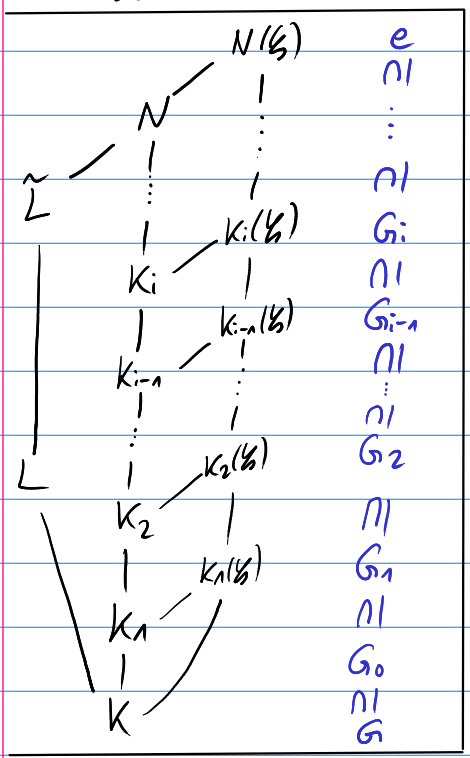
A25: Auflösbarkeit durch Radikale

Stichworte: Polynom vom Grad n auflösbar durch Radikale $\Leftrightarrow$ Galoisgruppe auflösbar $\Leftrightarrow n \leq 4$

25.1. **Einleitung:** Ob ein Polynom auflösbar durch Radikale ist, kann man daran erkennen, ob die Galoisgruppe davon eine auflösbare Gruppe ist. In Charakteristik 0 ist demnach jedes Polynom vom Grad ≤ 4 auflösbar durch Radikale und für höhere Grade nicht, weil die Gruppe S_n ab $n \geq 5$ nicht mehr auflösbar ist.

25.2. **Satz:** Sei $\mathrm{Char}\, K = 0$. 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 $K = K_0 \subseteq \ldots \subseteq K_r = N$ ein Rad.turm für $N|K$ vom Typ $(n_1, \ldots, n_r)$, d.h. $K_i = K_{i-1}(x_i)$ mit $x_i^{n_i} \in K_{i-1}$.
* Sei $n := \mathrm{kgV}(n_1, \ldots, n_r)$, ζ eine primitive n-te EW über N.
Betr. den 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 $G := \mathrm{Gal}(N(\zeta)|K)$
und $G_i := \mathrm{Gal}(N(\zeta)|K_i(\zeta))$.

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

Nach dem Hauptsatz der Galoistheorie A23.10 ist G_i NT in G_{i-1},
und $G_{i-1}/G_i \cong \mathrm{Gal}(K_i(\zeta)|K_{i-1}(\zeta))$ zyklisch, $1 \le i \le r$.

* Nun $K(\zeta)|K$ abelsche Galoiserw. nach Bem. A22.16.

Somit: $G_0 \subseteq G$ ein NT und G/G_0 abelsch (vgl. Hauptsatz),
also $G \supseteq G_0 \supseteq G_1 \supseteq \dots \supseteq G_r = e$ ist NR für G
mit abelschen Faktoren, d.h. G ist auflösbar.

Nun: $G \to \mathrm{Gal}(L|K)$, $\sigma \mapsto \sigma|_L$ ist surj. Gruppenhom.

$\Rightarrow \mathrm{Gal}(L|K)$ auflösbar.

"$\Leftarrow$": Sei $G = \mathrm{Gal}(L|K)$ auflösbar, L ein ZK von $\Omega|K$, $n := \#G$,
ζ eine primitive n-te EW in einer Erw. von L.
$L(\zeta)|K(\zeta)$ ist galois, und $G' := \mathrm{Gal}(L(\zeta)|K(\zeta)) \to G$, $\sigma \mapsto \sigma|_L$
ist injektives Gruppenhom.

Dann ist $\mathrm{Gal}(L(\zeta)|K(\zeta))$ auflösbar,
und $n' := \#G'$ teilt $n = \#G$.

Sei nun $G' = G_0 \supseteq \dots \supseteq G_r = e$ eine NR mit zyklischen Faktoren
G_{i-1}/G_i von Primzahlordnung p_i (Satz A8.12, $p_i | n$).

Sei $K(\zeta) = K_0 \subseteq \dots \subseteq K_{i-1} \subseteq K_i \subseteq \dots \subseteq K_r = L(\zeta)$
der zugehörige Körperturm.

Nach dem Hauptsatz der Galoistheorie A23.10 ist $K_i|K_{i-1}$ galois
und $\mathrm{Gal}(K_i|K_{i-1}) \cong G_{i-1}/G_i$,
also ist $\mathrm{Gal}(K_i|K_{i-1})$ zyklisch der Ordnung p_i.

Nach Satz A24.7(2) ist dann: $K_i = K_{i-1}(x_i)$ für ein $x_i \in K_i$ mit $x_i^{p_i} \in K_{i-1}$
(denn K_{i-1} enthält alle n-ten und damit alle p_i-ten EWeln).

Somit ist $L(\zeta)|K$ eine Radikalerweiterung. □

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

Bew.: Die Galoisgruppe G von f ist isomorph einer UG von $\mathrm{Perm}(X)$, X die Menge der Wurzeln von f. Da S_n auflösbar für $n \leq 4$ nach Kor. A8.10, ist G auflösbar. □

25.4. **Def.:** Sei $n \geq 1$, $S_1, \dots, S_n$ Unbestimmte über K. Das Polynom
$$g(T) := T^n - S_1 T^{n-1} + S_2 T^{n-2} - \dots + (-1)^n S_n \in K(S_1, \dots, S_n)[T]$$
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: $g(T) = \prod_{i=1}^{n} (T - x_i)$.
Es gilt: $S_1 = \sum_{i=1}^{n} x_i$, $S_2 = \sum_{i<j} x_i x_j, \dots, S_n = x_1 \cdots x_n$.
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 elementarsymmetrische Fkt. in $X_1, \dots, X_n$.
Def. $K[X_1, \dots, X_n] \to K[x_1, \dots, x_n]$ Ringhom.
durch $\Phi \restriction K = \mathrm{id}_K$, $\Phi(X_i) = x_i$.

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

$\Rightarrow \Phi(s_i) = S_i \Rightarrow \Phi \restriction K[s_1, \dots, s_n] : K[s_1, \dots, s_n] \to K[S_1, \dots, S_n]$
ist injektiv, also Iso.
$\lceil \Phi(h(s_1, \dots, s_n)) = 0 = h(S_1, \dots, S_n) \Rightarrow h = 0 \rfloor$

Somit:

$$\begin{array}{ccc} K(X_1,\dots,X_n) & \xrightarrow[\cong]{\Phi} & K(x_1,\dots,x_n) = L \\ | & & | \\ K(s_1,\dots,s_n) & \xrightarrow[\cong]{\tilde{\Phi}} & K(S_1,\dots,S_n) = K_1 \\ | & & | \\ K[s_1,\dots,s_n] & \xrightarrow[\cong]{\Phi} & K[S_1,\dots,S_n] \end{array}$$

「vgl. Satz A19.11, da $K(X_i)$ Zk von $K(s_i)$, $K(x_i)$ Zk von $K(S_i)$」

「Fortsetzbarkeit auf Quotientenkörpern」

Also: $\mathrm{Gal}(L \mid K_1) \cong \mathrm{Gal}\left(K(X_1,\dots,X_n) \mid K(s_1,\dots,s_n)\right) \cong S_n$,

vgl. Anwendung A23.5, A23.8.

Nun ist S_n für $n \geq 5$ nicht auflösbar nach Kor. A8.10, Satz 25.2 $\Rightarrow$ Beh. □