Hinreichendes Kriterium für die Auflösbarkeit

Satz (23.5)

Sei $f \in K[x]$ ein nicht-konstantes Polynom mit auflösbarer Galoisgruppe $G = \mathrm{Gal}(f|K)$. Dann ist f durch Radikale auflösbar.

Eigenschaften von Radikalerweiterungen

Proposition (23.7)

(i) Sei $L|K$ eine Radikalerweiterung, $\tilde{K}$ ein algebraischer Abschluss von K und $\sigma : L \to \tilde{K}$ ein K-Homomorphismus. Dann ist auch $\sigma(L)|K$ eine Radikalerweiterung.

(ii) Ein Kompositum zweier Radikalerweiterungen ist eine Radikalerweiterung.

(iii) Ist $L|K$ eine separable Radikalerweiterung, so gibt es einen Erweiterungskörper M von L mit der Eigenschaft, dass $M|K$ eine Galois-Erweiterung und zugleich eine Radikalerweiterung ist.

„Radikalerweiterung $\Rightarrow$ auflösbare Gruppe“

Proposition (23.8)

Ist $L|K$ eine galoissche Radikalerweiterung, dann ist $G = \mathrm{Gal}(L|K)$ eine auflösbare Gruppe.

Beweis von Prop. 23.8

geg: galoissche Radikalerweiterung $L|K$

z.zg: $G = \mathrm{Gal}(L|K)$ ist auflösbar

$L|K$ Radikalerw. $\Rightarrow$ Es gibt eine Körperkette

$K = L_0 \subseteq L_1 \subseteq \dots \subseteq L_r = L$ und $\gamma_i \in L$, $n_i \in \mathbb{N}$,

so dass jeweils $\gamma_i^{n_i} \in L_{i-1}$, $L_i = L_{i-1}(\gamma_i)$, für $1 \le i \le r$.

Sei $n = \mathrm{kgV}(n_1, \dots, n_r)$, $\tilde{K}$ ein alg. Abschluss von L und

$\zeta \in \tilde{K}$ eine primitive n-te Einheitswurzel. Setze nun

$K' = K(\zeta)$, $L' = L(\zeta)$ und $L_i' = L_i(\zeta)$ $(0 \le i \le r)$.

→ erhalte eine neue Körperkette

$$K' = L_0' \subseteq L_1' \subseteq \dots \subseteq L_r' = L'$$

$L'|K$ ist Kompositum der Erw. $K(S)|K$ und $L|K$.
Weil beide Erw. normal sind, gilt dasselbe für $L'|K$.
$\overset{\text{char}(K)=0}{\Rightarrow}$ $L'|K$ ist galoissch, ebenso $L'|K'$.
Nach den Ergänzungen zum Hauptsatz der Galoistheorie erhalten wir durch $U_i = \text{Gal}(L'|L_i')$ eine Untergruppenkette

$$\text{Gal}(L'|K') = U_0 \supseteq U_1 \supseteq \dots \supseteq U_r = \text{Gal}(L'|L') = \{\text{id}_{L'}\}$$

$L_i = L_{i-1}(\alpha_i)$, $\alpha_i^{n_i} \in L_{i-1}$ $\Rightarrow$ $L_i' = L_{i-1}'(\gamma_i)$, und L_{i-1}' enthält mit $\zeta_i = \zeta^{n/n_i}$ eine primitive n_i-te Einheitswurzel $\overset{\S 22}{\Rightarrow}$
$L_i'|L_{i-1}'$ ist galoissch, mit zyklischer Galoisgruppe

$L'|L'_{i-1}$ ist normale Teilerweiterung von $L'|L'_i$

$\xrightarrow{\text{Gal-th}}$ $\mathrm{Gal}(L'|L'_i) \trianglelefteq \mathrm{Gal}(L'|L'_{i-1}) \Rightarrow$

$U_i \trianglelefteq U_{i-1}$, außerdem $U_{i-1}/U_i =$

$\mathrm{Gal}(L'|L'_{i-1})/\mathrm{Gal}(L'|L'_i) \cong \mathrm{Gal}(L'_i|L'_{i-1})$

$\xrightarrow{\text{s.o.}}$ U_{i-1}/U_i ist endliche zyklische Gruppe

Insgesamt ist damit bewiesen, dass

$\mathrm{Gal}(L'|K')$ eine auflösbare Gruppe ist

Damit ist auch $\mathrm{Gal}(L'|K)$ auflösbar, denn

[G Gpp., $N \trianglelefteq G$, dann: G auflösbar $\overset{(*)}{\Leftrightarrow}$ N, G/N auflösbar.]

$K(S)|K$ ist normale Teilerw. von $L'|K$

(da $K(S)|K$ eine Kreisteilungserw. ist)

$\Rightarrow N = \mathrm{Gal}(L'|K(S)) = \mathrm{Gal}(L'|K')$ ist Normalteiler von $\mathrm{Gal}(L'|K)$, außerdem

$\mathrm{Gal}(L'|K)/\mathrm{Gal}(L'|K') \cong \mathrm{Gal}(K'|K) =$

$\mathrm{Gal}(K(S)|K)$ §21 $\rightarrow \mathrm{Gal}(k(S)|k)$ ist abelsch, damit auch auflösbar. Ebenso ist da Normalteiler N auflösbar (s.o.) $\overset{(*)}{\Rightarrow}$ $\mathrm{Gal}(L'|K)$ ist auflösbar. Es ist $L|K$ eine normale Teilerw. von $L'|K$. $\Rightarrow \mathrm{Gal}(L'|L) \trianglelefteq \mathrm{Gal}(L'|K)$, $\mathrm{Gal}(L|K) \cong \mathrm{Gal}(L'|K)/\mathrm{Gal}(L'|L)$

Mit $\mathrm{Gal}(L'|K)$ ist nach (*) auch $\mathrm{Gal}(L|K)$ auflösbar. $\square$

Notwendiges Kriterium für Auflösbarkeit

Satz (23.9)

Sei $f \in K[x]$ ein nicht-konstantes, durch Radikale auflösbares Polynom. Dann ist $\mathrm{Gal}(f|K)$ eine auflösbare Gruppe.

Satz (23.10)

Jedes Polynom über einem Körper der Charakteristik 0 vom Grad ≤ 4 ist durch Radikale auflösbar.

Beweis von Satz 23.9:

geg. $f \in K[x]$, $G = \mathrm{Gal}(f|K)$, f durch Radikale auflösbar $\Rightarrow$ G ist auflösbar

Vor. $\Rightarrow$ Es gibt eine Radikalerw. $L|K$, so dass f über L in Linearfaktoren zerfällt.

Prop. 23.7 (iii) $\Rightarrow$ dürfen voraussetzen, dass $L|K$ galois'sch ist. Seien $\alpha_1, \dots, \alpha_r \in L$ die Nullstellen von f in L, $L_1 = K(\alpha_1, \dots, \alpha_r)$.

$\Rightarrow$ $L_1|K$ ist galois'sch und $G \cong \mathrm{Gal}(L_1|K)$.

Prop. 23.8 $\Rightarrow$ $\mathrm{Gal}(L|K)$ ist auflösbar

Gal. th. $\Rightarrow$ $\mathrm{Gal}(L|L_1) \trianglelefteq \mathrm{Gal}(L|K)$ und

$G \cong \mathrm{Gal}(L_1|K) \leq \mathrm{Gal}(L|K)/\mathrm{Gal}(L|L_1)$.

Mit $\mathrm{Gal}(L|K)$ sind auch $\mathrm{Gal}(L_1|K)$ und G auflösbare Gruppen. $\square$

Existenz nicht-auflösbarer Polynome

Proposition (23.11)

Jede zweielementige Menge $\{\sigma, \tau\}$ bestehend aus dem 5-Zykel $\sigma = (1\ 2\ 3\ 4\ 5)$ und einer beliebigen Transposition τ ist ein Erzeugendensystem von S_5.

Satz (23.12)

Sei $f \in \mathbb{Q}[x]$ ein normiertes, irreduzibles Polynom vom Grad 5 mit genau drei reellen Nullstellen. Dann ist $\mathrm{Gal}(f|\mathbb{Q})$ isomorph zu S_5.

Satz (23.13)

Es gibt Polynome in $\mathbb{Q}[x]$ vom Grad 5, die nicht durch Radikale auflösbar sind.

Bew. von Prop. 23.11:

Sei $\sigma = (1\,2\,3\,4\,5) \in S_5$ und $\tau \in S_5$ eine beliebige Transposition. Zzg: $\langle \sigma, \tau \rangle = S_5$

Sei ν_5 die Anzahl der 5-Sylowgr. von $\langle \sigma, \tau \rangle$, also die Anzahl der Untergr. der Ordnung 5. Beh: $\nu_5 = 6$

$\operatorname{ord}(\sigma) = 5 \Rightarrow \langle \sigma \rangle$ ist eine 5-Sylowgr.

Mit σ ist auch $\tau\sigma\tau^{-1} = (\tau(1)\,\tau(2) \ldots \tau(5))$ (*)

ein 5-Zyklel, und dieser ist nicht in $\langle \sigma \rangle =$

$\{\mathrm{id}, (1\,2\,3\,4\,5), (1\,3\,5\,2\,4), (1\,4\,2\,5\,3), (1\,5\,4\,3\,2)\}$

enthalten. (da in (*) nur zwei der Zahlen 1, ..., 5 ihren Platz tauschen) $\Rightarrow \langle \tau\sigma\tau^{-1} \rangle$ ist 5-Sylowgr. $\neq \langle \sigma \rangle \Rightarrow \nu_5 \geq 2$

3. Sylowsatz $\Rightarrow \nu_5 \mid \frac{|\langle \sigma, \tau \rangle|}{5} \Rightarrow \nu_5 \mid \frac{120}{5} \Rightarrow \nu_5 \mid 24$

$\Rightarrow \nu_5 \in \{1, 2, 4, 8, 3, 6, 12, 24\}$, außerdem $\nu_5 \equiv 1 \bmod 5$

$\Rightarrow \nu_5 = 6$ ($\Rightarrow$ Beh.)

Auch $V = \langle \sigma, \tau\sigma\tau^{-1} \rangle \leq U$ enthält 6 5-Sylowgruppen

$\Rightarrow$ In V gibt es genau $\varphi(5) \cdot \nu_5 = 4 \cdot 6 = 24$ Elemente der Ordnung 5. außerdem: $\operatorname{sgn}(\sigma) = \operatorname{sgn}(\tau\sigma\tau^{-1}) = 1 \Rightarrow$

$\{\sigma, \tau\sigma\tau^{-1}\} \leq A_5 \Rightarrow V \leq A_5 \rightarrow |V|$ ist Teiler von 60

$|V| \geq 24 \Rightarrow |V| \in \{30, 60\}$ Ang. $|V| = 30 \Rightarrow (A_5 : V) = 2$

$\Rightarrow$ V ist nicht trivialer Normalteiler von A_5

$\lightning$ da A_5 einfache Gruppe also:

$|V| = 60 = |A_5| \overset{V \leq A_5}{\Rightarrow} V = A_5$

$\overset{V \leq H}{\Longrightarrow} A_5 \leq \langle \sigma, \tau \rangle$ Wegen $\operatorname{sgn}(\tau) = -1$

gilt darüber hinaus $A_5 \subsetneq \langle \sigma, \tau \rangle \Rightarrow$

$\langle \sigma, \tau \rangle = S_5$. $\square$

Beweis von Satz 23.12:

geg. $f \in \mathbb{Q}[x]$ mit genau drei reellen Nullstellen $\alpha_1, \alpha_2, \alpha_3$ und einem Paar α_4, α_5 nicht-reeller komplex-konj. Nullstellen, außerdem f in $\mathbb{Q}[x]$ irred.

z.zg: $\mathrm{Gal}(f|\mathbb{Q}) \cong S_5$

Sei G_1 das Bild in S_5 bzgl. der Nummerierung der Nullstellen. z.zg.: $G_1 = S_5$

Nach Prop. 23.11 genügt es z.zg., dass G_1 $(12\ldots5)$ und eine Transposition enthält.

Durch Einschränkung der komplexen Konj. auf $L = \mathbb{Q}(\alpha_1, \ldots, \alpha_5)$ erhalten wir ein Element

$\tau \in Gal(L|\mathbb{Q})$ mit $\tau(x_j) = x_j$ für $j = 1, 2, 3$

$\tau(x_4) = \overline{x_4} = x_5$, $\tau(x_5) = \overline{x_5} = x_4$ $\Rightarrow$ τ entspricht

in G_1 dem Element $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 5 & 4 \end{pmatrix} = (4\ 5)$, d.h.

eine Transposition

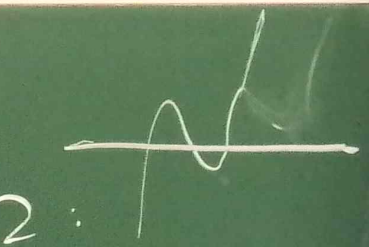
f irred. über $\mathbb{Q}$, $f(x_1) = 0$ $\Rightarrow$ $[\mathbb{Q}(x_1) : \mathbb{Q}] = \text{grad}(f) = 5$

Gradformel $\Rightarrow$ $[L : \mathbb{Q}] = [L : \mathbb{Q}(x_1)] \cdot [\mathbb{Q}(x_1) : \mathbb{Q}]$ $\Rightarrow$

$5 \mid [L : \mathbb{Q}]$ $\Rightarrow$ $5 \mid |Gal(L|\mathbb{Q})|$ $\Rightarrow$ $5 \mid |G_1|$ $\Rightarrow$

G_1 enthält einen 5-Zykel. Nach Umnummerierung der Nullst. stimmt dieser mit $(1\,2\,3\,4\,5)$ überein, und drei Transp. bleibt erhalten. $\square$

Konkretes Beispiel für ein Polynom mit den Eigenschaften aus Satz 23.12:



Sei $g = x(x^2-2)(x^2+2) = x^5 - 4x$.

Das Pol. hat 3 reelle Nullstellen $(0, \pm\sqrt{2})$

$g' = 5x^4 - 4$ hat zwei reelle Nullst. $(\pm\sqrt[4]{5/4})$

$\Rightarrow$ g hat höchstens zwei lokale Extrema

Einsetzen in g'' $\Rightarrow$ g hat lokales Maximum $\approx (-0{,}950,\ 3{,}026)$, lok. Min. bei $\approx (0{,}950, -3{,}026)$

Dies zeigt, dass $f = x^5 - 4x + 2$ ebenfalls genau zwei reelle Nullst. hat. Außerdem ist f lt. Eisenstein-Krit. irred.

$\overset{(23.12)}{\Rightarrow}$ $\mathrm{Gal}(f|\mathbb{Q}) \cong S_5$, f ist nicht durch Radikale auflösbar

Bez. zw. den Koeffizienten und Nullstellen eines Polynoms

$$x^2 + px + q = (x - \alpha_1)(x - \alpha_2)$$

$$\Leftrightarrow x^2 + px + q = x^2 - (\alpha_1 + \alpha_2) + \alpha_1 \alpha_2 \quad \text{also:}$$

$$p = -(\alpha_1 + \alpha_2), \quad q = \alpha_1 \alpha_2$$

$$x^3 + px^2 + qx + r = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)$$

$$\Rightarrow p = -(\alpha_1 + \alpha_2 + \alpha_3), \quad q = \alpha_1 \alpha_2 + \alpha_1 \alpha_3 + \alpha_2 \alpha_3, \quad r = -\alpha_1 \alpha_2 \alpha_3$$

Definition der elementarsymmetrischen Polynome

Definition (24.1)

Sei R ein Ring, $n \in \mathbb{N}$ und $R[x_1, ..., x_n]$ der Polynomring über R in n Variablen. Dann bezeichnet man für $1 \leq k \leq n$ das Polynom

$$\varepsilon_k = \sum_{1 \leq i_1 < ... < i_k \leq n} \prod_{j=1}^{k} x_{i_j}$$

als k-tes elementarsymmetrisches Polynom in $R[x_1, ..., x_n]$.

Beispiel: die elementarsymmetrischen Polynome für $n = 4$

$$\varepsilon_1 = x_1 + x_2 + x_3 + x_4$$

$$\varepsilon_2 = x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 + x_3x_4$$

$$\varepsilon_3 = x_1x_2x_3 + x_1x_2x_4 + x_1x_3x_4 + x_2x_3x_4$$

$$\varepsilon_4 = x_1x_2x_3x_4$$

Bedeutung: Ist $f \in K[x]$ ein normiertes Polynom und sind $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ die Nullstellen von f (evtl. mit Vielfachheiten), dann sind 1 und $(-1)^k \varepsilon_k(\alpha_1, \alpha_2, \alpha_3, \alpha_4)$ $(1 \leq k \leq 4)$ die Koeffizienten von f.