Hinreichendes Kriterium für die Auflösbarkeit

Satz (24.5)

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

„Radikalerweiterung $\Rightarrow$ auflösbare Gruppe“

Proposition (24.8)

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

Satz (24.9)

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

Auflösbarkeit der Polynome vom Grad ≤ 4

Satz (24.10)

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

Erzeugendensysteme von S_5

Proposition (25.1)

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.

Nicht-Auflösbarkeit von Polynomen fünften Grades

Satz (25.2)

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 (25.3)

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

Beispiel aus §21:

$$f = x^3 - x^2 - 8x + 3 \in \mathbb{Q}[x]$$

gezeigt: Die Nullstellen von f sind

$$\alpha_1 = \tfrac{1}{3} + \beta + \gamma \approx 3{,}204$$

$$\alpha_2 = \tfrac{1}{3} + \delta\beta + \delta^2\gamma \approx -2{,}569$$

$$\alpha_3 = \tfrac{1}{3} + \delta^2\beta + \delta\gamma \approx 0{,}364$$

mit $\beta = \sqrt[3]{-\frac{7}{54} + \sqrt{-\frac{257}{12}}}$, $\gamma = \frac{25}{9}\beta^{-1}$, $\delta = -\frac{1}{2} + \frac{1}{2}\sqrt{-3}$.

Definition reeller Radikalerweiterungen

Definition (25.4)

Sei K ein Teilkörper von $\mathbb{R}$.

- Wir bezeichnen eine Radikalerweiterung $L|K$ als reelle Radikalerweiterung, wenn $L \subseteq \mathbb{R}$ gilt.
- Die Elemente einer solchen Erweiterungen werde reelle Radikale genannt.
- Man sagt, ein Polynom $f \in K[x]$ sei durch reelle Radikale auflösbar, wenn es über einer reellen Radikalerweiterung von K in Linearfaktoren zerfällt.

Eine Eigenschaft reiner Gleichungen

Proposition (25.5)

Sei K ein Körper, p eine Primzahl, $a \in K$ und $f = x^p - a \in K[x]$. Genau dann ist f in $K[x]$ irreduzibel, wenn f in K keine Nullstelle besitzt.

$\alpha_1 = \frac{1}{3} + \beta + \gamma \approx 3{,}204$

$\alpha_2 = \frac{1}{3} + \beta\beta + \beta^2\gamma \approx -2{,}569$

Beweis von Proposition 25.5

geg: Primzahl p, Körper K, $a \in K$, $f = x^p - a$

Beh: f ist irred in $K[x] \Longleftrightarrow f$ hat keine Nullstelle in K

O.B.d.A. sei $a \in K^\times$ „$\Rightarrow$" ist trg. grad$(f) > 1$ klar

„$\Leftarrow$" Ang., f ist reduzibel, hat aber keine Nullstelle in K

Dann gibt es $g, h \in K[x]$, normiert, mit $f = gh$ und

$2 \leq$ grad(g), grad$(h) \leq p-2$

Sei $L \supseteq K$ ein Zerf.körp. von f über K und $\alpha \in L$ eine Nullstelle von f. Sei $\beta \in L$ eine bel weitere Nullst. $\Rightarrow \beta^p - a = 0 \Rightarrow$

$\beta^p = a = \alpha^p \Rightarrow (\beta\alpha^{-1})^p = 1 \Rightarrow \beta\alpha^{-1}$ ist eine p-te Einheitswurzel

Daraus folgt: Es gibt eine p-te Einheitswurzel $\zeta \in L$, so dass die Nullstellen von f durch $\zeta^j \alpha$ mit $0 \leq j \leq p-1$ gegeben sind.
Daraus folgt, dass der konstante Term von g bis auf Vorzeichen die Form $b = \zeta^u \alpha^m$ hat, mit $u \in \mathbb{N}_0$ und $m = \operatorname{grad}(g)$. Wegen $g \in K[x]$ liegt $b \in K$.

$\operatorname{ggT}(m, p) = 1 \overset{\text{Lemma von Bézout}}{\Longrightarrow} \exists\, r, s \in \mathbb{N}$ mit $rm + sp = 1 \Rightarrow b^r = (\zeta^u \alpha^m)^r$

$= \zeta^{ur} \alpha^{rm} = \zeta^{ur} \alpha^{rm+sp} \alpha^{-sp} =$

$= f^{ur} \alpha^{rm} = f^{ur} \alpha^{rm+s} \cdot \alpha^{-s} =$

$f^{ur} \alpha^1 \cdot (\alpha^r)^{-s} = f^{ur} \alpha \cdot a^{-s} \Rightarrow$

$f^{ur} \alpha = a^s \cdot b^r \in K$ Wegen $f(f^{ur} \alpha) = 0$ besitzt f also eine Nullstelle in K. ein Widerspruch zur Voraussetzung. $\square$

Irreduzibilität reiner Polynome im Reellen

Proposition (25.6)

Sei K ein Teilkörper von $\mathbb{R}$, q eine Primzahl und $\gamma \in \mathbb{R} \setminus K$ mit $\gamma^q \in K$. Dann ist das Polynom $f = x^q - \gamma^q \in K[x]$ irreduzibel, und es gilt $[K(\gamma) : K] = q$.

Beweis von Prop. 25.6:

geg: Teilkörper K von $\mathbb{R}$, $\gamma \in \mathbb{R} \setminus K$, q Primzahl mit $\gamma^q \in K$, $f = x^q - \gamma^q$

z.zg: f ist irred. in $K[x]$, $[K(\gamma) : K] = q$

Aus der ersten Aussage folgt durch die zweite, weil dann $f = \mu_{\gamma, K}$ gilt. Für die erste Aussage reicht es nach Prop. 25.5 zu zeigen, dass f in K keine Nullstelle hat.

Ang. $\beta \in K$ ist eine Nullstelle von f.

Dann gilt $\beta^q - \gamma^q = 0 \Rightarrow \beta^q = \gamma^q$

$\Rightarrow (\beta\gamma^{-1})^q = 1$, d.h. $\beta\gamma^{-1}$ ist eine q-te Einheitswurzel, außerdem $\beta\gamma^{-1} \in R$

Daraus folgt $\beta\gamma^{-1} \in \{\pm 1\}$ und somit $\gamma \in \{\pm\beta\}$.

also: $\beta \in K \Rightarrow \gamma \in K$ ↯ zur Vor. □

Erweiterungen nach Adjunktion reeller Wurzeln

Proposition (25.7)

Sei p eine ungerade Primzahl und $L|K$ eine Galois-Erweiterung vom Grad p, wobei $L \subseteq \mathbb{R}$ ist. Sei q eine weitere Primzahl und $\gamma \in \mathbb{R}$ ein Element mit $\gamma \notin K$ und $\gamma^q \in K$. Dann gilt $[L(\gamma) : K(\gamma)] = [L : K] = p$.

Beweis von Prop. 25.7

gegeben: Primzahlen p, q; $L|K$ Galoiserw. vom Grad p (p ungerade) mit $L \subseteq \mathbb{R}$, $\gamma \in \mathbb{R} \setminus K$ mit $\gamma^q \in K$

Beh. $[L(\gamma) : K(\gamma)] = [L : K] = p$

1. Fall: $\gamma \in L$ Betrachte $f = x^q - \gamma^q \in K[x]$

Prop. 25.6 $\Rightarrow$ f ist über K irreduzibel

$f(\gamma) = 0$ also: f ist irred. Polynom über K, das in L eine Nullst. besitzt, $L|K$ ist normal $\Rightarrow$ f zerfällt über L in Linearfaktoren $\Rightarrow$ $\delta\gamma \in L$, wobei $\delta \in \mathbb{C}^\times$

$f(\gamma) = 0$ also: f ist irred. Polynom über K, das in L eine Nullst. besitzt, $L|K$ ist normal $\Rightarrow$ f zerfällt

primitive q-te Einheitswurzel (da $f(\zeta_q \gamma) = 0$ und f über L zerfällt) $\rightarrow$ $\zeta = (\zeta_q)\, \gamma^{-1} \in L \overset{L \subseteq R}{\Longrightarrow} \zeta \in \mathbb{R}$ Dies ist nur möglich, wenn $q = 2$ ist

$\gamma \in L \rightarrow K(\gamma)$ ist Zwischenkörper von $L|K$ $\overset{\text{Gradformel}}{\rightarrow}$

$p = [L : K] = [L : K(\gamma)] \cdot [K(\gamma) : K] \overset{\text{Prop. 25.6}}{\leq} 1 \cdot q$
$\uparrow \gamma \in L$

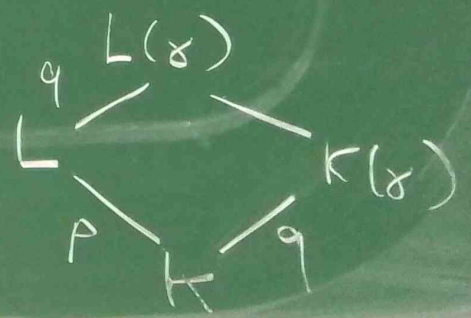
p ungerade $\rightarrow$ q ungerade $\not\downarrow$ es sei $q = 2$

2 Fall: $\gamma \notin L$ Dann gilt $\gamma \in \mathbb{R} \setminus L$, $\gamma^q \in K \subseteq L$

Prop. 25.6 $\rightarrow$ $[L(\gamma) : L] = q$

Auf Grund der Gradformel gilt

$q \cdot p = [L(\gamma) : L] \cdot [L : K] = [L(\gamma) : K] =$
$[L(\gamma) : K(\gamma)] \cdot [K(\gamma) : K] = [L(\gamma) : K(\gamma)] \cdot q$



Durch Kürzen erhalten wir $[L(\gamma) : K(\gamma)] = p$ □

Galois-Erweiterungen in reellen Radikalerweiterungen

Proposition (25.8)

Sei p eine ungerade Primzahl und $L|K$ eine Galois-Erweiterung vom Grad p mit $L \subseteq \mathbb{R}$. Dann ist L in keiner reellen Radikalerweiterung von K enthalten.

Beweis von Prop. 25.8:

geg.: p ungerade Primzahl, $L|K$ Galoiserw. vom Grad p, $L \subseteq \mathbb{R}$

Beh.: L liegt in keiner reellen Radikalerw. von K

Ang. $\tilde{L}|K$ ist eine reelle Radikalerw. mit $\tilde{L} \supseteq L$

$\Rightarrow$ Es gibt Körpertürme $K = L_0 \subseteq L_1 \subseteq \dots \subseteq L_r = \tilde{L}$ und Elemente $\gamma_1, \dots, \gamma_r \in \tilde{L}$, $m_1, \dots, m_r$ Primzahlen mit $L_j = L_{j-1}(\gamma_j)$, $\gamma_j^{m_j} \in L_{j-1}$ für $1 \leq j \leq r$.

Nach Konstruktion gilt jeweils $L_j = K(\gamma_1, \dots, \gamma_j)$

P

für $1 \leq j \leq r$ Satzgemäße Anwendung von Prop. 25.7 zeigt, dass aus $[L : K]_{L(\gamma_1) \; K(\gamma_1)} = p$ nacheinander die Gleichungen $[L_1'' : L : L_1] = p$, $[L_2'' : L : L_2] = p$, ..., $[L_r : L : L_r] = p$ folgen, da $L_j = K(\gamma_1, \ldots, \gamma_j)$, $L \cdot L_j = L \cdot K(\gamma_1, \ldots, \gamma_j) = L(\gamma_1, \ldots, \gamma_j)$. Daraus folgt also $\boxed{[\tilde{L} : L : \tilde{L}] = p}$

aber: $L \subseteq \tilde{L} \Rightarrow \tilde{L} \cdot L = \tilde{L} \Rightarrow$

$[\tilde{L} \cdot L : \tilde{L}] = 1$ ↯

□

Reelle Radikalerw. nach Erweiterung des Grundkörpers

Lemma (25.9)

Sei K ein Teilkörper von $\mathbb{R}$ und $\tilde{L}|K$ eine reelle Radikalerweiterung. Ist M ein Erweiterungskörper von K mit $M \subseteq \mathbb{R}$, dann ist $\tilde{L} \cdot M|M$ ebenfalls eine reelle Radikalerweiterung.

Hauptsatz über reelle Radikalerweiterungen

Satz (25.10)

Sei K ein Teilkörper von $\mathbb{R}$ und $f \in K[x]$ irreduzibel mit einem Zerfällungskörper $L \subseteq \mathbb{R}$. Ist eine Nullstelle von f ein reelles Radikal, dann ist $[L : K]$ eine Zweierpotenz.

Beweis von Satz 25.10:

geg. Teilkörper K von $\mathbb{R}$

$f \in K[x]$ irreduzibel mit einem Zerfällungskörper $L \subseteq \mathbb{R}$ über K

$\alpha \in L$ Nullstelle von f, die in einer reellen Radikalerweiterung $\tilde{L}$ von K liegt

Beh.: $[L:K]$ ist eine Zweierpotenz

Ang., dies ist nicht der Fall $\Rightarrow [L:K]$ hat einen ungeraden Primteiler p

zeige unten (*): Es gibt ein σ in $G = \mathrm{Gal}(L|K)$ $= \mathrm{Gal}(f|K)$ mit $\mathrm{ord}(\sigma) = p$ und $\sigma(\alpha) \neq \alpha$

dann: Setze $M = L^{\langle \sigma \rangle}$ Dann gilt $[L:M] = |\langle \sigma \rangle| = p$

$\sigma(\alpha) \neq \alpha \Rightarrow \alpha \notin M$ Gradformel $\Rightarrow p = [L:M]$

$= [L:M(\alpha)] \cdot [M(\alpha):M]$ $[M(\alpha):M] > 1 \Rightarrow$

$[M(\alpha):M] = p$. $[L:M(\alpha)] = 1 \Rightarrow L = M(\alpha)$.

Vor. $\Rightarrow \alpha$ liegt in eines reellen Radikalturm $\tilde{L}$ von K

$\Rightarrow \tilde{L} \cdot M$ enthält L (wegen $L = M(\alpha)$, $\alpha \in \tilde{L}$)

$\Rightarrow L$ ist in eines reellen Radikalturm von M enthalten

Prop. 25.9 (nämlich in $\tilde{L} \cdot M$) $\lightning$ zu Prop 25.8

Prop. 25.9 (nämlich in $L:M$) ⇵ zu Prop. 25.8

Beweis von (*): p teilt $|G| = [L:K]$

Satz von Cauchy $\Rightarrow \exists\, \tau \in G$ mit $\operatorname{ord}(\tau) = p$

$\tau \neq \mathrm{id}_L$ — $\exists$ Nullst. α_j von f mit $\tau(\alpha_j) \neq \alpha_j$

Fortsetzungssatz, Irred von f $\Rightarrow \exists\, \sigma_j \in G$ mit $\sigma_j(\alpha) = \alpha_j$.

Setze $\sigma = \sigma_j^{-1} \tau \sigma_j$. $\Rightarrow \sigma(\alpha) = (\sigma_j^{-1} \tau \sigma_j)(\alpha) =$

$(\sigma^{-1}\tau)(\alpha_j) \neq \sigma^{-1}(\alpha_j) = \alpha$. Da σ aus τ durch Konjugation entsteht, gilt $\operatorname{ord}(\sigma) = \operatorname{ord}(\tau) = p$. □

Nicht-Auflösbarkeit durch reelle Radikale

Folgerung (25.11)

Ist K ein Teilkörper von $\mathbb{R}$ und $f \in K[x]$ ein irreduzibles Polynom mit ausschließlich reellen Nullstellen, dessen Grad keine Zweierpotenz ist. Dann ist keine Nullstelle von f ein reelles Radikal.