Die Cardanische Formeln

Satz (24.9)

Sei $f = x^3 + px + q \in K[x]$, außerdem $\Delta = q^2 + \frac{4}{27}p^3$,

$$\beta = \sqrt[3]{-\tfrac{1}{2}q + \tfrac{1}{2}\sqrt{\Delta}} \quad , \quad \gamma = \sqrt[3]{-\tfrac{1}{2}q - \tfrac{1}{2}\sqrt{\Delta}}$$

und $k \in \{0, 1, 2\}$ so gewählt, dass $-3\beta(\zeta^k\gamma) = p$ gilt. Dann sind $\alpha_1 = \beta + \zeta^k\gamma$, $\alpha_2 = \zeta^2\beta + \zeta^{k+1}\gamma$ und $\alpha_3 = \zeta\beta + \zeta^{k+2}\gamma$ die Nullstellen von f in L, eventuell mit Vielfachheiten.

Anmerkung zu den Cardanischen Formeln

Auf die Wahl des „richtigen“ Wertes für $k \in \{0, 1, 2\}$ kann verzichtet werden, indem man γ statt dessen durch die Fallunterscheidung

$$\gamma \quad = \quad \begin{cases} -\frac{1}{3} p \beta^{-1} & \text{falls } p \neq 0 \\ \sqrt[3]{-\frac{1}{2} q - \frac{1}{2} \sqrt{\Delta}} & \text{falls } p = 0 \end{cases}$$

definiert.

Lösungsformel für Polynome vom Grad 4

geg. Polynom $f = x^4 + px^2 + qx + r \in K[x]$, $\operatorname{char}(K) = 0$

$\tilde{L} \supseteq K$ alg. abg. Erweiterungskörper mit einer Quadrat- und einer Kubikwurzelfkt. $\sqrt{\ }: \tilde{L} \to \tilde{L}$ bzw. $\sqrt[3]{\ }: \tilde{L} \to \tilde{L}$

$\alpha_1, \dots, \alpha_4$ Nullst. von f evtl. mit Vielfachheiten

$(\Rightarrow \alpha_1 + \alpha_2 + \alpha_3 + \alpha_4 = 0)$

$\theta_1 = (\alpha_1 + \alpha_2)(\alpha_3 + \alpha_4) = -(\alpha_1 + \alpha_2)^2$

$\theta_2 = (\alpha_1 + \alpha_3)(\alpha_2 + \alpha_4) = -(\alpha_1 + \alpha_3)^2$

$\theta_3 = (\alpha_1 + \alpha_4)(\alpha_2 + \alpha_3) = -(\alpha_1 + \alpha_4)^2$

Ann. $\sqrt{-\theta_1} = \alpha_1 + \alpha_2$, $\sqrt{-\theta_2} = \alpha_1 + \alpha_3$

Ann. $\sqrt{-\theta_1} = \alpha_1 + \alpha_2$, $\sqrt{-\theta_2} = \alpha_1 + \alpha_3$

Wähle $\varepsilon \in \{\pm 1\}$ so, dass $\alpha_1 + \alpha_4 = \varepsilon\sqrt{-\theta_3}$.

$$\Rightarrow \alpha_1 = \tfrac{1}{2}\sqrt{-\theta_1} + \tfrac{1}{2}\sqrt{-\theta_2} + \tfrac{1}{2}\varepsilon\sqrt{-\theta_3}$$
$$\alpha_2 = \tfrac{1}{2}\sqrt{-\theta_1} - \tfrac{1}{2}\sqrt{-\theta_2} - \tfrac{1}{2}\varepsilon\sqrt{-\theta_3}$$
$$\alpha_3 = -\tfrac{1}{2}\sqrt{-\theta_1} + \tfrac{1}{2}\sqrt{-\theta_2} - \tfrac{1}{2}\varepsilon\sqrt{-\theta_3}$$
$$\alpha_4 = -\tfrac{1}{2}\sqrt{-\theta_1} - \tfrac{1}{2}\sqrt{-\theta_2} + \tfrac{1}{2}\varepsilon\sqrt{-\theta_3}$$

$\left[\tfrac{1}{2}\cdot\left((\alpha_1+\alpha_2) - (\alpha_1+\alpha_3) - (\alpha_1+\alpha_4)\right)\right.$
$= \tfrac{1}{2}(-\alpha_1 + \alpha_2 - \alpha_3 - \alpha_4)$
$= \tfrac{1}{2}(\alpha_2 + \alpha_2) = \alpha_2 \left.\right]$
$\uparrow \alpha_2 = -\alpha_1 - \alpha_3 - \alpha_4$

Das Polynom $g = (x-\theta_1)(x-\theta_2)(x-\theta_3)$ hat Koeff., die symm. Fkt. in den Nullst. $\alpha_1, \dots, \alpha_4$ sind. $\Rightarrow g \in K[x]$ Eine Rechnung mit elementarsymm. Fkt. ergibt $g = x^3 - 2px^2 + (p^2 - 4r) + q^2$ (kubische Resolvente von f) Stelle $\theta_1, \theta_2, \theta_3$ mit den Cardanischen Formeln als Wurzel dar, setze dies oben ein. $\Rightarrow$ erhalte $\alpha_1, \dots, \alpha_4$ als Wurzelausdrücke.

Lösungsformel für Polynome vierten Grades

Satz (24.10)

Sei $f = x^4 + px^2 + qx + r \in K[x]$, und sei $g \in K[x]$ die kubische Resolvente von f. Es seien $\theta_1, \theta_2, \theta_3 \in \tilde{L}$ die Nullstellen von g, eventuell mit Vielfachheiten, und es sei $\varepsilon \in \{\pm 1\}$ so gewählt, dass die Gleichung $\sqrt{-\theta_1}\sqrt{-\theta_2}(\varepsilon\sqrt{-\theta_3}) = -q$ erfüllt ist. Dann sind die Nullstellen von f, ebenfalls mit Vielfachheiten, gegeben durch

$$\begin{aligned}
\alpha_1 &= \tfrac{1}{2}\sqrt{-\theta_1} + \tfrac{1}{2}\sqrt{-\theta_2} + \tfrac{1}{2}\varepsilon\sqrt{-\theta_3} \\
\alpha_2 &= \tfrac{1}{2}\sqrt{-\theta_1} - \tfrac{1}{2}\sqrt{-\theta_2} - \tfrac{1}{2}\varepsilon\sqrt{-\theta_3} \\
\alpha_3 &= -\tfrac{1}{2}\sqrt{-\theta_1} + \tfrac{1}{2}\sqrt{-\theta_2} - \tfrac{1}{2}\varepsilon\sqrt{-\theta_3} \\
\alpha_4 &= -\tfrac{1}{2}\sqrt{-\theta_1} - \tfrac{1}{2}\sqrt{-\theta_2} + \tfrac{1}{2}\varepsilon\sqrt{-\theta_3}.
\end{aligned}$$

Anmerkung zur Lösungsformel

Ähnlich wie bei den Cardanischen Formeln kann auf die Wahl des „richtigen“ Vorzeichens ε verzichtet werden, in dem man an Stelle von $\varepsilon\sqrt{-\theta_3}$ den Ausdruck γ gegeben durch die Fallunterscheidung

$$\gamma \quad = \quad \begin{cases} -q(\theta_1\theta_2)^{-1/2} & \text{falls } q \neq 0 \\ \sqrt{-\theta_3} & \text{falls } q = 0 \end{cases}$$

in die Formel einsetzt.

Anwendungsbeispiel zu den Cardanischen Fml

$$f = x^3 - x^2 - 8x + 3$$

$$f\left(x + \tfrac{1}{3}\right) = x^3 - \frac{25}{3}x + \frac{7}{27} \quad \left(p = -\frac{25}{3},\ q = \frac{7}{27}\right)$$

$$\Rightarrow -\tfrac{1}{2}q = -\frac{7}{54},\quad q^2 + \frac{4}{27}p^3 = -\frac{257}{3}$$

$$\xi = -\tfrac{1}{2} + \tfrac{1}{2}\sqrt{-3},\quad \beta = \sqrt[3]{-\tfrac{7}{54} + \tfrac{1}{2}\sqrt{-\frac{257}{3}}}$$

$$\gamma = \sqrt[3]{-\tfrac{7}{57} - \tfrac{1}{2}\sqrt{-\frac{257}{3}}}$$

Cardano $\Rightarrow$

f hat die Nullst. $\alpha_1 = \frac{1}{3} + \beta + \gamma$.

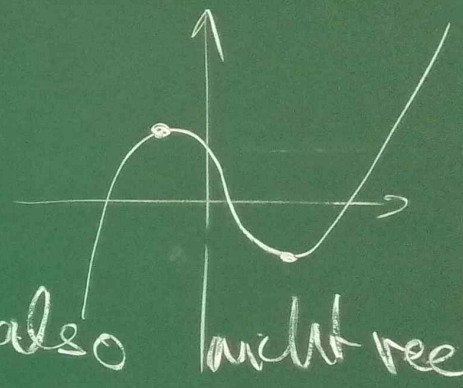
$\alpha_2 = \frac{1}{3} + \xi\beta + \xi^2\gamma$, $\alpha_3 = \frac{1}{3} + \xi^2\beta + \xi\gamma$

(Die Gleichung $-3\beta\gamma = p$ ist erfüllt.)

näherungsweise $x_1 \approx 3{,}204$, $x_2 \approx -2{,}569$, $x_3 \approx 0{,}364$

Kurvendiskussion zeigt, dass die drei Nullstellen tatsächlich reell sind,

obwohl für die Darstellung negative Quadratwurzeln, also nicht reelle Zahlen, benötigt wurden!



Ziel: Es gibt eine Möglichkeit, die Nullstellen von f durch verschachtelte reelle Wurzeln darzustellen.

Definition der reellen Radikalerweiterungen

Definition (24.11)

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.

Irreduzibilität reiner Gleichungen

Proposition (24.12)

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.

Beweis von Prop. 24.12

geg. $f = x^p - a \in K[x]$, p Primzahl

Beh.: f irreduzibel in $K[x] \Leftrightarrow f$ hat in K keine Nullstelle

O.B.d.A. $a \neq 0$. „$\Rightarrow$" klar, da $p = \text{grad}(f) \geq 2$

„$\Leftarrow$" Ang. f hat in K keine Nullstelle, ist aber dennoch reduzibel. Sei α eine Nullstelle von f in einem (alg. abg.) Erw.-Kp. $L \supseteq K$ und $f = gh$ eine Zerlegung von g in nicht-konstante Polynome. Sei $\gamma \in L$ eine weitere Nullst. von f. $\rightarrow$ $\gamma^p = a = \alpha^p \Rightarrow \gamma = \zeta \alpha$ für eine p-te Einheits-

von f in einem Erw.-Körper $L \supseteq K$ und $f = gh$ eine Zerlegung von g in nicht-konstante Polynome

$\approx 0{,}364$

Nullstellen

reelle

die

reelle

Wurzel $\beta \in L \Rightarrow$ Die Nullstellen von f sind gegeben durch $\beta^k \alpha$ mit $0 \le k < p$. Betrachte nun den konstanten Term $b \in K$ von g. $\Rightarrow$ b hat (als Produkt von Nullst. des Polynoms f) bis auf Vorzeichen die Form $\beta^l \alpha^m$ mit $l \in \mathbb{N}_0$, $m = \mathrm{grad}(g)$

p Primzahl, $m \in \{1, \dots, p-1\} \Rightarrow \mathrm{ggT}(m, p) = 1 \Rightarrow$ Bézout

$\exists u, v \in \mathbb{Z}$ mit $um + vp = 1$

$b^u = (\beta^l \alpha^m)^u = \beta^{lu} \alpha^{um} = \beta^{lu} \alpha^{um+vp} \alpha^{-vp}$

$= \beta^{lu} \alpha^1 a^{-v} \Rightarrow \beta^{lu} \alpha = a^v b^u \in K \Rightarrow$

$\exists \alpha^p = a$

f hat in K eine Nullstelle $\lightning$ zu Vor. $\square$

Zwei Hilfsaussagen

Proposition (24.13)

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 $[K(\gamma) : K] = q$.

Proposition (24.14)

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. 24.13

geg. K Teilkörper von R, q Primzahl, $\gamma \in R \setminus K$ mit $\gamma^q \in K$, $f = x^q - \gamma^q$

Beh.: f ist irreduzibel, $[K(\gamma) : K] = q$

Ist f irred. dann folgt $f = \mu_{\gamma, K}$ und $[K(\gamma) : K] = \operatorname{grad}(f) = q$. gemäß nach Prop 24.12 f hat in K keine Nullstelle Ang. $\beta \in K$ ist Nullstelle von $f \Rightarrow$ $\beta^q = \gamma^q \rightarrow \gamma = \zeta\beta$ für ein q-te Einheitswurzel ζ $\gamma \in R$, $\beta \in K \subseteq R \rightarrow \zeta \in R$ Die einzigen Einheitswurzeln in R sind ± 1. $\Rightarrow \gamma \in \{\pm\beta\} \Rightarrow \gamma \in K$ ↯ □

Beweis von Prop. 24.14

geg. L/K Galois-Erw. von Grad p, wobei p ungerade Primzahl und $L \subseteq R$ q-elementare Primzahl. $\gamma \in R$ mit $\gamma \notin K$, $\gamma^q \in K$

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

Prop. 24.13 $\Rightarrow$ $[K(\gamma) : K] = q$ Annahme: $\gamma \in L$

$\Rightarrow$ $K(\gamma)$ Zwischenkp. von L/K Gradformel $\Rightarrow$ $p =$

$[L : K] = [L : K(\gamma)] \cdot [K(\gamma) : K]$ $\gamma \notin K \Rightarrow [K(\gamma) : K] > 1$

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

$f = x^p - \gamma^p \in K[x]$ hat γ als Nullstelle, $[K(\gamma) : K] = p = \text{grad}(f)$

$\Rightarrow$ f ist Min.-pol. von γ über K, insb. irred. Da f in L eine Nullstelle hat und L/K normal ist, zerfällt f über L in Linearfaktoren.

$\Rightarrow$ Alle komplexen Nullst. von f liegen bereits in L, insb $e^{2\pi i/p} \cdot \gamma \quad \gamma \cdot e^{2\pi i/p} \cdot \gamma \in L$

$\Rightarrow e^{2\pi i/p} = \cos\left(\frac{2\pi}{p}\right) + i\sin\left(\frac{2\pi}{p}\right) \in L \subseteq \mathbb{R}$

$\lightning$ da $p > 2$. $\sin\left(\frac{2\pi}{p}\right) \neq 0$

Also war die Annahme falsch, und es gilt $\gamma \notin L$.

s.o. $\Rightarrow \gamma^q \in K \rightarrow \gamma^q \in L$ Prop. 24.13

$\Rightarrow [L(\gamma) : L] = q \Rightarrow$

$q \cdot p = [L(\gamma) : L] \cdot [L : K] \overset{\text{Gradformel}}{=} [L(\gamma) : K]$

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

$\Rightarrow [L(\gamma) : K(\gamma)] = p = [L : K]$ $\square$

Zwei weitere Hilfsaussagen

Proposition (24.15)

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.

Lemma (24.16)

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.

Beweis von Prop. 24.15

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

Angenommen, L liegt in einer reellen Radikalerweiterung $M|K$. $\Rightarrow$ Es gibt einen Körperturm

$K = M_0 \subseteq M_1 \subseteq \dots \subseteq M_r = M \subseteq \mathbb{R}$

$\gamma_1, \dots, \gamma_r \in M_r$, Primzahlen $q_1, \dots, q_r$, so dass

$M_i = M_{i-1}(\gamma_i)$ und $\gamma_i^{q_i} \in M_{i-1}$ für $1 \leq i \leq r$.

Es gilt jeweils $M_i = K(\gamma_1, \dots, \gamma_i)$ und

$LM_i = L(\gamma_1, \dots, \gamma_i)$. Durch wiederholte Anwendung von Kor 24.14 erhalten wir

$[L \cdot M_i : M_i] = p$ für $1 \leq i \leq r$

insb. $[L \cdot M : M] = p$ aber: Ist L in M enthalten, dann gilt $L \cdot M \subseteq M \Rightarrow [L \cdot M : M]$

$= [M : M] = 1$ ↯ □

Notwendiges Kriterium für reelle Radikalerweiterungen

Satz (24.17)

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.

Folgerung (24.18)

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.

Beweis von Satz 24.17

geg: K Teilkörper von $\mathbb{R}$, $f \in K[x]$ irreduzibel mit Zerfällungskörper $L \subseteq \mathbb{R}$.
Ang. eine Nullstelle α von f ist ein reelles Radikal. Beh.: Dann ist $[L:K]$ eine Zweierpotenz.

Ang. $[L:K]$ ist keine Zweierpotenz. Dann besitzt $[L:K]$ einen ungeraden Primteiler p.
p teilt die Ordnung von $|G|$, wobei $G = \mathrm{Gal}(L|K) = \mathrm{Gal}(f|K)$. zeige unten: Es gibt ein $\sigma \in G$ mit $\mathrm{ord}(\sigma) = p$ und $\sigma(\alpha) \neq \alpha$

Sei $M = L^{\langle\sigma\rangle}$ Galoistheorie $\Rightarrow [L:M] = |\langle\sigma\rangle| = p$

Prop 24.15 $\Rightarrow$ $L|M$ ist in keiner reellen Radikalerweiterung von M enthalten

andererseits: $\sigma(\alpha) \neq \alpha \Rightarrow \alpha \in L \setminus M$ Gradformel $\Rightarrow$

$p = [L:M(\alpha)]\,[M(\alpha):M]$ $\alpha \notin M \Rightarrow [M(\alpha):M] = p$

und $L = M(\alpha)$ Vor. $\Rightarrow$ α ist reelles Radikal $\Rightarrow$

α liegt in einer reellen Radikalerw. $\tilde{L}|K$ $\Rightarrow$

$L = M(\alpha) \subseteq M \cdot \tilde{L}$ Lemma 24.16 $\Rightarrow$ $M \cdot \tilde{L}|M$ ist reelle Radikalerw. $\Rightarrow$ $L|M$ liegt in einer reellen Radikalerw.

↯ zu Aussage von oben

Noch z.zg.: $\exists \sigma \in G$ mit $\operatorname{ord}(\sigma) = p$ und $\sigma(\alpha) \neq \alpha$

Seien $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_n$ die versch. Nullst. von f in L

p Primteiler von $|G| \overset{\text{Lemma v. Cauchy}}{\Longrightarrow} \exists \tau \in G$ mit $\operatorname{ord}(\tau) = p$

$\tau \neq \mathrm{id} \Rightarrow \exists j \in \{1, \ldots, n\}$ mit $\tau(\alpha_1) \neq \alpha_j$ f irred. Fortsetzungssatz $\Rightarrow \exists \sigma_j \in G$ mit $\sigma_j(\alpha) = \alpha_j$. Definiere $\sigma := \sigma_j^{-1} \circ \tau \circ \sigma_j$

Dann gilt $\operatorname{ord}(\sigma) = \operatorname{ord}(\tau) = p$, da Konjugation in G ein Automorphismus ist und die Ordn. von τ somit nicht ändert. Ang. $\sigma(\alpha) = \alpha$.

$\tau = \sigma_j \circ \sigma \circ \sigma_j^{-1} \Rightarrow \tau(\alpha_j) = (\sigma_j \circ \sigma \circ \sigma_j^{-1})(\alpha_j) = (\sigma_j \circ \sigma)(\alpha) =$

$\sigma_j(\alpha) = \alpha_j$ ↯ zu $\tau(\alpha_j) \neq \alpha_j$. □