Die allgemeine Gleichung

Definition (24.7)

Sei K ein Körper und $K[s_0, ..., s_{n-1}]$ ein Polynomring über K, dessen n Variablen mit $s_0, ..., s_{n-1}$ bezeichnet sind. Es sei $F = K(s_0, ..., s_{n-1})$ der Quotientenkörper dieses Polynomrings. Dann bezeichnet man

$$f \quad = \quad x^n + s_{n-1}x^{n-1} + ... + s_1x + s_0 \quad \in F[x]$$

als allgemeines Polynom und die Gleichung $f = 0$ als allgemeine Gleichung n-ten Grades über dem Körper K.

Die Galoisgruppe der allgemeinen Gleichung

Satz (24.8)

Sei E ein Zerfällungskörper des allgemeinen Polynoms f über F. Dann ist $E|F$ eine Galois-Erweiterung, mit $\mathrm{Gal}(E|F) \cong S_n$.

Beweis von Satz 24.8 (Fortsetzung)

geg: $F = K(s_0, \dots, s_{n-1})$, E Zerf.-Körp von f über F

zzg: $E|F$ galoissch, $\mathrm{Gal}(E|F) \leq S_n$

Die Erweiterung ist galoissch, weil E Zerfällungskörper eines Polynoms über f ist und (wie wir sehen werden) die Nullstellen von f in E paarweise verschieden sind

Sei $K[x_1, \dots, x_n]$ ein weiterer Polynomring über K, $\tilde{E} = K(x_1, \dots, x_n)$ sein Quotientenkörper. Die Gruppe S_n operiert auf $\tilde{E}$ durch $\sigma(x_k) = x_{\sigma(k)}$ $\forall \sigma \in S_n$ und $k \in \{1, \dots, n\}$.

operiert auf $\tilde{E}$ durch $\sigma(x_k) = x_{\sigma(k)}$ $\forall \sigma \in S_n$

bereits gezeigt: $\tilde{E}^{S_n} = \tilde{F}$, wobei $\tilde{F} = K(\varepsilon_1, \dots, \varepsilon_n)$

Prop. 21.3, Folgerung 21.6 $\Rightarrow$ $\tilde{E} | \tilde{F}$ ist galoissch, und für die Galoisgruppe gilt $Gal(\tilde{E}|\tilde{F}) = S_n$

Sei $\Phi : K[s_0, \dots, s_{n-1}] \to K[\varepsilon_1, \dots, \varepsilon_n]$ der Auswertungshom. gegeben durch $\Phi(s_k) = (-1)^{n-k} \varepsilon_{n-k}$ für $0 \le k \le n-1$. Dieser kann fortgesetzt werden zu einem Hom. von Körpern $K(s_0, \dots, s_{n-1}) \to K(\varepsilon_1, \dots, \varepsilon_n)$ gegeben durch $\Phi\left(\frac{u}{v}\right) = \frac{\Phi(u)}{\Phi(v)}$ für $u, v \in K[s_0, \dots, s_{n-1}]$, $v \neq 0$. Satz 24.4 $\Rightarrow$ Φ ist surjektiv $\Rightarrow$ erhalte einen Isomorphismus $F \xrightarrow{\sim} \tilde{F}$ von Körpern. Sei $\Psi : \tilde{F} \to F$ die Umkehrabb. dieses Isomorphismus.

Seien $x_1, \dots, x_n \in E$ die Nullstellen von f

Sei $\tilde{f} = (x - x_1) \cdot \dots \cdot (x - x_n) \in \tilde{E}[x]$

Dann gilt $\Phi(f) = x^n + \sum_{k=0}^{n-1} \Phi(s_k) x^k$

$= x^n + \sum_{k=0}^{n-1} (-1)^{n-k} \varepsilon_{n-k} x^k = (x - x_1) \cdots (x - x_n)$

$= \tilde{f}$.

Für $0 \le j \le n$ definiere $\tilde{E}_j = \tilde{F}(x_1, \dots, x_j)$

$\tilde{r}_j = (x - x_1) \cdots (x - x_j)$, $\tilde{g}_j = (x - x_{j+1}) \cdots (x - x_n)$

$(\Rightarrow \tilde{f} = \tilde{r}_j \tilde{g}_j)$ x_{j+1} Nullstelle von $\tilde{g}_j \Rightarrow \mu_{x_{j+1}, \tilde{E}_j} \mid \tilde{g}_j$

Gradformel $\Rightarrow [\tilde{E} : \tilde{F}] =$

$$\prod_{i=0}^{n-1} [\tilde{E}_{i+1} : \tilde{E}_i] = \prod_{i=0}^{n-1} [\tilde{E}_i(x_{i+1}) : \tilde{E}_i]$$

$$= \prod_{i=0}^{n-1} \operatorname{grad}(\mu_{x_{i+1}, \tilde{E}_i}) \leq \prod_{i=0}^{n-1} \operatorname{grad}(\tilde{q}_i)$$

$$= \prod_{i=0}^{n-1} (n-i) = n! = |S_n| = [\tilde{E} : \tilde{F}]$$

$\Rightarrow \mu_{x_{i+1}, \tilde{E}_i} = \tilde{q}_i$ für $0 \leq i \leq n-1$, d.h.
die Polynome $\tilde{q}_i$ sind irreduzibel
$\Rightarrow$ Fortsetzungssatz anwendbar
Die n-fache Anwendung des Fortsetzungssatzes

liftet die Fortsetzung $\hat{\Psi}: \tilde{E} \to E$ von Ψ
mit $\hat{\Psi}(x_{j+1}) = \alpha_{j+1}$ für $0 \le j \le n-1$.
Die Injektivität von $\hat{\Psi}$ zeigt, dass $\alpha_1, \dots, \alpha_n \in E$
verschieden sind. $\Rightarrow$ erhalte einen Gruppenhom.
$\mathrm{Gal}(\tilde{E}|\tilde{F}) \to \mathrm{Gal}(E|F)$ durch $\sigma \mapsto \hat{\Psi} \circ \sigma \circ \Psi^{-1}$
$\to \mathrm{Gal}(E|F) \le \mathrm{Gal}(\tilde{E}|\tilde{F}) = S_n$. □

Anmerkung: Jedes Polynom n-ten Grades

$f = x^n + a_{n-1}x^{n-1} + \dots + a_1 x + a_0$

kann durch Substitution $x \mapsto x - \frac{1}{n} a_{n-1}$

in ein Polynom $g(x) = f(x - \frac{1}{n} a_{n-1})$ ohne

x^{n-1} - Term transformiert werden. Sind

$x_1, \dots, x_n$ die Nullstellen von f (evtl. mit Viel-

fachheit), dann sind $x_j + \frac{1}{n} a_{n-1}$ $(1 \leq j \leq n)$ die

Nullstellen von g.

Grundvoraussetzungen an K:

$\mathrm{char}(K) = 0$, $\tilde{L} \supseteq K$ algebraisch abg. Erweiterungskörper mit einer Quadrat- und einer Kubikwurzelfkt. $\sqrt{\cdot} : \tilde{L} \to \tilde{L}$ bzw. $\sqrt[3]{\cdot} : \tilde{L} \to \tilde{L}$.

Annahmen
- K enthält die primitive dritte Einheitswurzel $\zeta = -\frac{1}{2} + \frac{1}{2}\sqrt{-3}$
- Das Polynom $f = x^3 + px + q \in K[x]$ erfüllt $\mathrm{Gal}(f|K) \cong S_3$.

Seien $\alpha_1, \alpha_2, \alpha_3 \in \tilde{L}$ die Nullstellen von f in $\tilde{L}$ (evtl. mit

Vielfachheiten, d.h. $f = (x-\alpha_1)(x-\alpha_2)(x-\alpha_3)$

$\rightarrow \alpha_1+\alpha_2+\alpha_3 = 0$, $\alpha_1\alpha_2+\alpha_1\alpha_3+\alpha_2\alpha_3 = p$, $\alpha_1\alpha_2\alpha_3 = -q$

Betrachte zur Untergruppenkette $\mathrm{id} \subseteq A_3 \subseteq S_3$ die Körperkette $L_0 = K = L^{S_3} \subseteq L_1 = L^{A_3} \subseteq L_2 = L^{\mathrm{id}} = L$

wobei $L = K(\alpha_1, \alpha_2, \alpha_3)$ der Zerfällungskörper von f über K ist.

$\mathrm{Gal}(L|L^{A_3}) \cong A_3 \cong \mathbb{Z}/3\mathbb{Z}$ (zyklisch)

Bilde die Lagrange-Resolventen $\beta_1 = \alpha_1 + \zeta\alpha_2 + \zeta^2\alpha_3$

und $\beta_2 = \alpha_1 + \zeta^2\alpha_2 + \zeta\alpha_3$ [allgem.: $\alpha + \zeta\sigma(\alpha) + \ldots + \zeta^{n-1}\sigma^{n-1}(\alpha)$

wende dies auf $\sigma = (123)$ an] $\Rightarrow \alpha_1 = \frac{1}{3}\beta_1 + \frac{1}{3}\beta_2$,

$\alpha_2 = \frac{1}{3}\zeta^2\beta_1 + \frac{1}{3}\zeta\beta_2$, $\alpha_3 = \frac{1}{3}\zeta\beta_1 + \frac{1}{3}\zeta^2\beta_2$

Ziel: Stelle β_1, β_2 durch die Koeff. p, q von f dar.

Definiere $\beta = \frac{1}{3}\beta_1$, $\gamma = \frac{1}{3}\gamma_2$

Betrachte das Polynom $h = (x-\beta^3)(x-\gamma^3)$

Beob.: Die Koeff. von h, also $-(\beta^3+\gamma^3)$ und $\beta^3\gamma^3$ bleiben unter der Op. der Galoisgruppe unverändert, d.h. sie liegen im Grundkörper. Darüber hinaus sind $\beta^3+\gamma^3$ und $\beta^3\gamma^3$ (sogar $\beta\gamma$) symmetrisch in den Nullstellen $\alpha_1, \alpha_2, \alpha_3$

$\Rightarrow$ qG $(x_1+\zeta x_2+\zeta^2 x_3)(x_1+\zeta^2 x_2+\zeta x_3)$

$= x_1^2+x_2^2+x_3^2-x_1x_2-x_1x_3-x_2x_3$

$= \varepsilon_1^2-3\varepsilon_2$ Einsetzen von $\alpha_1, \alpha_2, \alpha_3$ $\Rightarrow$

$$\beta_1\beta_2 = 0^2 - 3p = -3p \Rightarrow \beta\gamma = \frac{1}{9}(-3p) = -\frac{1}{3}p$$
$$\Rightarrow \beta_1^3\beta_2^3 = -\frac{1}{27}p^3$$

$$(x_1 + \delta x_2 + \delta^2 x_3)^3 + (x_1 + \delta^2 x_2 + \delta x_3)^3 =$$
$$x_1^3 + x_2^3 + x_3^3 - 3x_1^2x_2 - 3x_1^2x_3 - 3x_2^2x_3$$
$$- 3x_1x_2^2 - 3x_1x_3^2 - 3x_2x_3^2 + 12x_1x_2x_3$$
$$= 2\varepsilon_1^3 - 9\varepsilon_1\varepsilon_2 + 27\varepsilon_3$$

Einsetzen von $\alpha_1, \alpha_2, \alpha_3 \Rightarrow \beta_1^3 + \beta_2^3 = 2\cdot 0^3$
$$- 9\cdot 0\cdot p + 27(-q) = -27q \Rightarrow \beta^3 + \gamma^3 =$$
$$3^{-3}\beta_1^3 + 3^{-3}\beta_2^3 = -q$$

einsetzen in das Polynom $h \Rightarrow$

$$h = x^2 + qx - \frac{1}{27}p^3$$

$\Rightarrow$ Nullstellen von h: $-\frac{1}{2}q \pm \frac{1}{2}\sqrt{\Delta}$,

mit $\Delta = q^2 + \frac{4}{27}p^3$

Nach evtl. Vertauschung von α_2, α_3 (⇝ Vertauschung von β und γ) gilt $\beta^3 = -\frac{1}{2}q + \frac{1}{2}\sqrt{\Delta}$ und $\gamma^3 = -\frac{1}{2} - \frac{1}{2}\sqrt{\Delta}$. Annahme: $\beta = \sqrt[3]{-\frac{1}{2}q + \frac{1}{2}\sqrt{\Delta}}$

Dann haben wir β, γ und damit auch β_1, β_2 und $\alpha_1, \alpha_2, \alpha_3$ durch p und q ausgedrückt

□

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.

geg. $f = x^4 + px^2 + qx + r$

$= (x-\alpha_1)(x-\alpha_2)(x-\alpha_3)(x-\alpha_4)$

$\Rightarrow \alpha_1 + \alpha_2 + \alpha_3 + \alpha_4 = 0$, $p = \varepsilon_2(\alpha_1, \dots, \alpha_4)$,

$q = -\varepsilon_3(\alpha_1, \dots, \alpha_4)$, $r = \varepsilon_4(\alpha_1, \dots, \alpha_4) = \alpha_1\alpha_2\alpha_3\alpha_4$

Setze $L = K(\alpha_1, \dots, \alpha_4)$, $G = \mathrm{Gal}(L|K)$

$= \mathrm{Gal}(f|K)$. Annahme: $G \leq S_4$

Betrachte die Körpertafel

$K = L^{S_4} \subseteq L^{A_4} \subseteq L^{V_4} \subseteq L^{\mathrm{id}} = L$

$\alpha_1 + \dots + \alpha_4 = 0 \quad \Rightarrow$ erhalte

$$\alpha_1 = \tfrac{1}{2}(\alpha_1+\alpha_2) + \tfrac{1}{2}(\alpha_1+\alpha_3) + \tfrac{1}{2}(\alpha_1+\alpha_4)$$
$$\alpha_2 = \tfrac{1}{2}(\alpha_1+\alpha_2) - \tfrac{1}{2}(\alpha_1+\alpha_3) - \tfrac{1}{2}(\alpha_1+\alpha_4)$$
$$\alpha_3 = -\tfrac{1}{2}(\alpha_1+\alpha_2) + \tfrac{1}{2}(\alpha_1+\alpha_3) - \tfrac{1}{2}(\alpha_1+\alpha_4)$$
$$\alpha_4 = -\tfrac{1}{2}(\alpha_1+\alpha_2) - \tfrac{1}{2}(\alpha_1+\alpha_3) + \tfrac{1}{2}(\alpha_1+\alpha_4)$$

Definiere
$$\theta_1 = -(\alpha_1+\alpha_2)^2 = (\alpha_1+\alpha_2)(\alpha_3+\alpha_4) \in L^{V_4}$$
$$\theta_2 = -(\alpha_1+\alpha_3)^2 = (\alpha_1+\alpha_3)(\alpha_2+\alpha_4) \in L^{V_4}$$
$$\theta_3 = -(\alpha_1+\alpha_4)^2 = (\alpha_1+\alpha_4)(\alpha_2+\alpha_3) \in L^{V_4}$$

Bilde das Polynom $g = (x-\theta_1)(x-\theta_2)(x-\theta_3)$.

Beob.: Dieses Polynom, und somit auch seine Koeff., ...

Bleiben unter der Operation von S_4 unverändert.
Daraus Ausdrücke sind die Koeff. symmetrisch in $x_1, \dots, x_4$.

$$(x_1+x_2)(x_3+x_4) + (x_1+x_3)(x_2+x_4) + (x_1+x_4)(x_2+x_3) = 2\varepsilon_2$$

$$(x_1+x_2)(x_3+x_4)\cdot(x_1+x_3)(x_3+x_4) + (x_1+x_3)(x_3+x_4)\cdot(x_1+x_4)(x_2+x_3)$$
$$+ (x_1+x_3)(x_2+x_4)\cdot(x_1+x_4)(x_2+x_3) = \varepsilon_2^2 + \varepsilon_1\varepsilon_3 - 4\varepsilon_4$$

$$(x_1+x_2)(x_3+x_4)\cdot(x_1+x_3)(x_2+x_4)\cdot(x_1+x_4)(x_2+x_3) = \varepsilon_1\varepsilon_2\varepsilon_3 - \varepsilon_1^2\varepsilon_4 - \varepsilon_3^2$$

einsetzen von $x_1, \dots, x_4 \Rightarrow \theta_1+\theta_2+\theta_3 = 2p,$

$$\theta_1\theta_2+\theta_1\theta_3+\theta_2\theta_3 = p^2 + 0\cdot(-q) - 4r = p^2 - 4r$$

$$\theta_1\theta_2\theta_3 = 0\cdot p\cdot(-q) - 0^2 r - (-q)^2 = -q^2$$

$$\Longrightarrow g = x^3 - 2px^2 + (p^2-4r)x + q^2$$ kubische Resolvente

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.