Lösung einer Gleichung durch verschachtelte Wurzeln

gegeben: Körper K , Polynom $f \in K[x] \setminus K$, L Zerfällungskörper von f über K , $G = \text{Gal}(L|K)$ **auflösbare** Galoisgruppe der Erweiterung, $n = [L : K] = |G|$

Der Körper K enthalten für jeden Primteiler p von n eine **primitive p -te Einheitswurzel**, d.h. ein Element ζ_p mit $\text{ord}(\zeta_p) = p$ in $K^\times$.

Die Auflösbarkeit von G liefert in Verbindung mit dem Hauptsatz der Galoistheorie eine **Körperkette**

$$K = L^G = L^{U_0} \subseteq L^{U_1} \subseteq \dots \subseteq L^{U_{r-1}} \subseteq L^{U_r} = L^{\text{id}} = L$$

wobei $p_{j+1} = (U_j : U_{j+1}) = [L_{j+1} : L_j]$ für $0 \leq j < r$ jeweils eine **Primzahl** ist und die Erweiterung $L_{j+1}|L_j$ durch Adjunktion einer **p_{j+1} -ten Wurzel** zu Stande kommt.

Lösung einer Gleichung durch verschachtelte Wurzeln

Allgemeine Vorgehensweise:

- Zu Beginn sei $j = r - 1$. Gegeben seien Elemente $\alpha_1, \dots, \alpha_m$ mit der Eigenschaft $L_{j+1} = L_j(\alpha_i)$ für $1 \leq i \leq m$. Im Fall $j = r - 1$ sind dies die Nullstellen des Polynoms f .
- Bestimme ein System von Elementen $\beta_1, \dots, \beta_\ell$ mit $L_{j+1} = L_j(\beta_i)$ für $1 \leq i \leq \ell$, wobei β_i jeweils eine p_{j+1} -te **Wurzel** eines Elements aus L_j ist. Dies bedeutet, dass die Elemente $\gamma_i = \beta_i^{p_{j+1}}$ in L_j liegen.
- Bestimme Darstellungen von $\alpha_1, \dots, \alpha_m$ als **Polynomausdrücke** in den Elementen $\beta_1, \dots, \beta_\ell$. (In der Regel arbeitet man hierbei mit sog. **Lagrange-Resolventen**, siehe § 23.)
- Im Fall $j = 1$ liegen $\gamma_1, \dots, \gamma_\ell$ im Grundkörper K , und das Verfahren ist abgeschlossen.
- Ansonsten setze das Verfahren für $j - 1$ mit den Elementen $\gamma_1, \dots, \gamma_\ell$ an Stelle von $\alpha_1, \dots, \alpha_m$ fort.

Allgemeine Gleichung dritten Grades

Ausgangssituation:

$$f = (x - \alpha_1) \cdot (x - \alpha_2) \cdot (x - \alpha_3) = x^3 + px + q$$

In diesem Fall hat unsere Körperkette die Form

$$K = L^{S_3} \subseteq L^{A_3} \subseteq L^{\text{id}} = L.$$

- Betrachte zunächst die Teilerweiterung $L|L^{A_3}$ vom Grad 3.
- Setze $\beta_1 = \alpha_1 + \zeta\alpha_2 + \zeta^2\alpha_3$ und $\beta_2 = \alpha_1 + \zeta\alpha_3 + \zeta^2\alpha_2$.
Diese Gleichungen können umgestellt werden zu

$$\alpha_1 = \beta_1 + \beta_2 \quad , \quad \alpha_2 = \frac{1}{3}\zeta^2\beta_1 + \frac{1}{3}\zeta\beta_2 \quad \text{und} \quad \alpha_3 = \frac{1}{3}\zeta\beta_1 + \frac{1}{3}\zeta^2\beta_2.$$

- Überprüfe: Für $\sigma = (1\ 2\ 3) \in A_3$ und eine primitive dritte Einheitswurzel ζ gilt $\sigma(\beta_1) = \zeta^2\beta_1$ und $\sigma(\beta_2) = \zeta\beta_2$. Daraus folgt, dass $L = L^{A_3}(\beta_1) = L^{A_3}(\beta_2)$ gilt und dass die Elemente $\gamma_1 = \beta_1^3$ und $\gamma_2 = \beta_2^3$ in L^{A_3} liegen.

Allgemeine Gleichung dritten Grades (Forts.)

- Die Menge $\{\frac{1}{27}\gamma_1, \frac{1}{27}\gamma_2\}$ bleibt unter der Operation von $S_3 = \langle (1\ 2\ 3), (1\ 2) \rangle$ unverändert. Also gilt dasselbe für die Koeffizienten des Polynoms

$$h = (x - \frac{1}{27}\gamma_1)(x - \frac{1}{27}\gamma_2) = x^2 - \frac{1}{27}(\gamma_1 + \gamma_2)x + (\frac{1}{27})^2\gamma_1\gamma_2.$$

Daraus folgt, dass die Koeffizienten im Grundkörper K enthalten sind.

- Durch Rechnung findet man die Gleichungen

$$\beta_1\beta_2 = -3p \quad \text{und} \quad \beta_1^3 + \beta_2^3 = -27q.$$

Daraus folgt $h = x^2 + qx - \frac{1}{27}p^3$ und $\gamma_1, \gamma_2 = -\frac{27}{2}q \pm \frac{27}{2}\sqrt{\Delta}$ mit $\Delta = \frac{1}{4}q^2 + \frac{1}{27}p^3$.

- Insgesamt erhält man so für $\alpha_1, \alpha_2, \alpha_3$ die Ausdrücke aus den Cardanischen Formeln.

Allgemeine Gleichung vierten Grades

Ausgangssituation:

$$f = (x - \alpha_1) \cdot (x - \alpha_2) \cdot (x - \alpha_3) \cdot (x - \alpha_4) = x^4 + px^2 + qx + r$$

Die Subnormalreihe $S_4 \supseteq A_4 \supseteq V_4 \supseteq C_2 \supseteq \text{id}$ mit der zweielementigen Gruppe $C_2 = \langle \sigma \rangle$ erzeugt durch $\sigma = (1\ 2)(3\ 4)$ liefert die Körperkette

$$K = L^{S_4} \subseteq L^{A_4} \subseteq L^{V_4} \subseteq L^{C_2} \subseteq L^{\text{id}} = L.$$

- Zunächst betrachten wir die Teilerweiterung $L|L^{C_2}$. Es gilt $\sigma(\alpha_1 + \alpha_3) \neq \alpha_1 + \alpha_3$ und somit $L = L^{C_2}(\alpha_1 + \alpha_3)$. Das Element $\theta_2 = -(\alpha_1 + \alpha_3)^2 = (\alpha_1 + \alpha_3)(\alpha_2 + \alpha_4)$ ist in L^{C_2} enthalten.

Allgemeine Gleichung vierten Grades (Forts.)

- Nun betrachten wir die Teilerweiterung $L^{C_2}|L^{V_4}$. Sei $\tau = (1\ 3)(2\ 4)$. Es gilt $\tau(\alpha_1 + \alpha_2) \neq \alpha_1 + \alpha_2$ und somit $L^{C_2} = L^{V_4}(\alpha_1 + \alpha_2)$. Das Element $\theta_1 = -(\alpha_1 + \alpha_2)^2 = (\alpha_1 + \alpha_2)(\alpha_3 + \alpha_4)$ ist in L^{V_4} enthalten.
- Insgesamt kommen die Erweiterungen $L|L^{C_2}$ und $L^{C_2}|L^{V_4}$ also durch Adjunktion der **Quadratwurzeln** $\sqrt{-\theta_1} = \alpha_1 + \alpha_2$ und $\sqrt{-\theta_2} = \alpha_1 + \alpha_3$ zu Stande. Setzt $\theta_3 = (\alpha_1 + \alpha_4)^2$, dann gilt außerdem $\sqrt{-\theta_3} = \alpha_1 + \alpha_4$. Offenbar können die Nullstellen α_j des Polynoms durch die Summe von je zwei dieser Quadratwurzeln darstellen.

Allgemeine Gleichung vierten Grades (Forts.)

- Nun betrachten wir die Teilerweiterung $L^{V_4}|K$. Die Menge $\{\theta_1, \theta_2, \theta_3\}$ bleibt unter V_4 und $\rho = \langle(1\ 2\ 3)\rangle$ unverändert, wegen $\langle V_4 \cup \{\rho\} \rangle = S_4$ also unter der **gesamten Gruppe S_4** .
- Daraus folgt, dass die Koeffizienten des Polynoms

$$g = (x - \theta_1) \cdot (x - \theta_2) \cdot (x - \theta_3)$$

im **Grundkörper** $K = L^{S_4}$ enthalten sind.

- Durch Rechnung findet man

$$g = x^3 - 2px^2 + (p^2 - 4r)x + q^2.$$

Dies ist eine **kubische Gleichung**, die mit den Cardanischen Formeln gelöst werden kann. Wir erhalten eine Darstellung von $\theta_1, \theta_2, \theta_3$ durch verschachtelte Wurzel­ausdrücke, und damit auch eine solche Darstellung für $\alpha_1, \alpha_2, \alpha_3, \alpha_4$.

Definition

Eine Körpererweiterung $L|K$ wird **Galois-Erweiterung** genannt, wenn sie normal **und** separabel ist. Die Gruppe

$$\text{Gal}(L|K) = \text{Aut}_K(L)$$

heißt dann die **Galoisgruppe** der Erweiterung $L|K$.

Ist M ein **Zwischenkörper** einer galois'schen Erweiterung $L|K$, dann ist auch $L|M$ galois'sch.

Satz (19.14)

Eine endliche Körpererweiterung $L|K$ ist genau dann galois'sch, wenn $[L : K] = |\text{Aut}_K(L)|$ gilt. Insbesondere ist für jede Galois-Erweiterung $L|K$ also die Gleichung $|\text{Gal}(L|K)| = [L : K]$ erfüllt.

§ 22. Der Hauptsatz der Galoistheorie

- Sei $L|K$ eine Galois-Erweiterung und M ein Zwischenkörper.
- bereits bekannt: Dann ist auch $L|M$ eine **Galois-Erweiterung**.
- Seien $G = \text{Gal}(L|K)$ und $U = \text{Gal}(L|M)$ die zugehörigen Galoisgruppen.
- leicht zu überprüfen:
Dann ist U eine **Untergruppe** von G .

Definition (22.1)

Sei L ein Körper und G eine Untergruppe von $\text{Aut}(L)$. Dann nennt man $L^G = \{\alpha \in L \mid \sigma(\alpha) = \alpha \ \forall \sigma \in G\}$ den **Fixkörper** von G .

- Wie man leicht überprüft, handelt es sich bei L^G tatsächlich um einen **Teilkörper** von L .
- Ist insbesondere $L|K$ eine Galois-Erweiterung und U eine Untergruppe von $G = \text{Gal}(L|K)$, dann ist L^U ein Teilkörper von L , darüber hinaus ein **Zwischenkörper** von $L|K$.

Die Definition der Galois-Korrespondenz

Sei $L|K$ eine Galois-Erweiterung und $G = \text{Gal}(L|K)$.

Unsere bisherigen Überlegungen zeigen

- Die Zuordnung $M \mapsto \text{Gal}(L|M)$ ist eine Abbildung von der Menge $\mathcal{Z}$ der Zwischenkörper von $L|K$ in die Menge $\mathcal{U}$ der Untergruppen von G .
- Die Zuordnung $U \mapsto L^U$ ist eine Abbildung von $\mathcal{U}$ nach $\mathcal{Z}$.

Unser **Hauptziel** in diesem Kapitel ist der Nachweis, dass im Fall einer **endlichen** Galois-Erweiterung $L|K$ diese Abbildungen **bijektiv** und zueinander invers sind.

Proposition (22.2)

Sei L ein Körper, $G \leq \text{Aut}(L)$ eine endliche Untergruppe und $K = L^G$ der zugehörige Fixkörper.

- (i) Sei $\alpha \in L$ und $G(\alpha) = \{\sigma(\alpha) \mid \sigma \in G\}$. Sind $\alpha_1, \dots, \alpha_r$ die verschiedenen Elemente der Menge $G(\alpha)$, dann ist das Polynom $f = \prod_{i=1}^r (x - \alpha_i)$ das **Minimalpolynom** $\mu_{\alpha, K}$ von α über K .
- (ii) Die Erweiterung $L|K$ ist galoissch.
- (iii) Die Erweiterung $L|K$ ist endlich.
- (iv) Es gilt $G = \text{Gal}(L|K)$.

Beweis von Prop. 22.2

L Körper, $G \subseteq \text{Aut}(L)$, $K = L^G$ (Fixkörper)

zu ii) Sei $\alpha \in L$, $G(\alpha) = \{\sigma(\alpha) \mid \sigma \in G\} = \alpha_1, \dots, \alpha_r$
wobei $r = |G(\alpha)|$. Sei $f = \prod_{j=1}^r (x - \alpha_j)$. Beh. $f = M_{\alpha, K}$

Sei $g = M_{\alpha, K}$. Es ist $f(\alpha) = 0$ wg. $\alpha \in G(\alpha)$.

Da jedes $\sigma \in G$ die Nullstellen von f permutiert, gilt

$\sigma(f) = f \quad \forall \sigma \in G \Rightarrow$ Die Koeff. von f liegen in $L^G = K$.

$\Rightarrow f \in K[x] \xrightarrow{f(\alpha)=0} g \mid f$

außerdem: $g(\alpha) = 0, \sigma \in G, \sigma(g) = g \xrightarrow{\text{„Nullstellen auf Nullstellen“}}$

$g(\alpha) = 0 \quad \forall \alpha \in G \Rightarrow g(\alpha_j) = 0 \text{ für } 1 \leq j \leq r$
 $\Rightarrow (x - \alpha_j) \mid g \text{ für } 1 \leq j \leq r \Rightarrow f = (x - \alpha_1) \cdots (x - \alpha_r)$
 ist Teiler von g $g \mid f$ und $f \mid g$, f und g sind beide
 normiert $\Rightarrow f = g$

ii) Beh. $L|K$ (mit $K = L^G$) ist eine Galois-Erweiterung

$L|K$ ist normal, denn. Sei $f \in K[x]$ irreduzibel, o.B.d.A. normiert
 mit einer Nullstelle $\alpha \in L$. z.zg. f zerfällt in $L[x]$ in Linearfaktoren.

Nach Def. ist $f = m_{\alpha, K}$. Teil i) $\Rightarrow f = \prod_{j=1}^r (x - \alpha_j)$ mit

$G(\alpha) = \{\alpha_1, \dots, \alpha_r\}$, wobei $r = |G(\alpha)| \Rightarrow f$ zerfällt in $L[x]$.

$L|K$ ist separabel, denn. Ist $\alpha \in L$ bel., dann sieht man an
 der Darstellung $f = \prod_{j=1}^r (x - \alpha_j)$, dass f in L nur verschiedene Nullstellen

hat, falls $f = M_{K, K}$ $\Rightarrow K$ ist
separabel über $K \Rightarrow L|K$ ist separabel

Beweis von Prop 22.2 (Forts.)

L Körper, $G \leq \text{Aut}(L)$, $K = L^G$ (Fixkörper)

zu (ii) z.zg. L/K ist endliche Erweiterung

Sei $d = |G|$ und $\alpha \in L$ zunächst beliebig. Für $f = \prod_{\sigma \in G} (x - \sigma(\alpha))$ folgt aus Teil (i), dass $\text{grad}(f) = |G(\alpha)|$ gilt $\Rightarrow$

$$[K(\alpha) : K] = |G(\alpha)| \leq |G| = d \quad \forall \alpha \in L$$

Sei nun $\alpha \in L$ so gewählt, dass $[K(\alpha) : K]$ maximal ist

Beh. $K(\alpha) = L$ Sei $\beta \in L$. Da α, β separabel über K sind, ist $K(\alpha, \beta) : K$ eine endliche separable Erweiterung.

Satz vom primitiven Element $\Rightarrow \exists \gamma \in L$ mit $K(\alpha, \beta) = K(\gamma)$

Sei nun $\alpha \in L$ so gewählt, dass $[K(\alpha):K]$ maximal ist.

Bl. $[K(\alpha):K] = 1$. Sei $\beta \in L$. Da α, β separabel über K

Maximalität $\Rightarrow [K(\beta):K] \leq [K(\alpha):K]$, andererseits $K(\alpha) \subseteq K(\alpha, \beta) = K(\beta) \Rightarrow [K(\alpha):K] \leq [K(\beta):K]$ insgesamt $[K(\alpha):K] = [K(\beta):K] \Rightarrow [K(\alpha):K] = [K(\beta):K] \Rightarrow K(\alpha) = K(\beta) = K(\alpha, \beta) \Rightarrow \beta \in K(\alpha)$ ($\rightarrow$ Beh.) Also ist $[L:K] = [K(\alpha):K]$, und somit tatsächlich eine endl. Erweiterung, mit $[L:K] \leq d$.

zu (iv) z.zg. $G = \text{Gal}(L|K)$, wobei $\text{Gal}(L|K) = \text{Aut}_K(L)$ nach Def.

klar: $G \subseteq \text{Aut}_K(L)$ (denn: Jedes $\sigma \in G$ ist ein Automorphismus von L , und jedes α aus $K = L^G$ erfüllt $\sigma(\alpha) = \alpha \Rightarrow \sigma$ ist ein K -Automorphismus.) außerdem: $d = |G| \leq |\text{Aut}_K(L)| \stackrel{13.14}{=} [L:K]_{\text{dall}K \text{ gal.}} \leq d \Rightarrow |G| = |\text{Aut}_K(L)| \Rightarrow G = \text{Aut}_K(L)$. $\square$

L^G ist Zwischenkörper von $L|K$

$$\text{Gradformel} \Rightarrow [L:K] = [L:L^G] \cdot [L^G:K]$$

$$\text{Es gilt } |G| = [L:L^G] \leq [L:K] \stackrel{13.14}{=} |\text{Aut}_K(L)|$$

$$= |G| \quad \begin{matrix} \uparrow \text{Prop. 22.2} \\ \Rightarrow [L:L^G] = [L:K] \end{matrix} \stackrel{K \subseteq L^G}{\Rightarrow} K = L^G$$

□

Folgerung (22.3)

Sei $L|K$ eine **endliche** Körpererweiterung und $G = \text{Aut}_K(L)$.
Genau dann ist $L|K$ galois'sch, wenn $L^G = K$ erfüllt ist.

Beweis von Folgerung 22.3

geg.: endl. Erw. $L|K$, $G = \text{Aut}_K(L)$

Beh.: $L|K$ galois'sch $\Leftrightarrow L^G = K$

" $\Leftarrow$ " bereits bekannt: G ist eine
endliche Gruppe (mit $|G| \leq [L:K]_{\text{sep}} \leq [L:K]$), also exist. eine endliche
Untergruppe von $\text{Aut}(L)$ $\xrightarrow{\text{Prop. 22.2}}$

$L|L^G$ ist galois'sch $\xrightarrow{\text{vor}}$ $L|K$ ist gal.

" $\Rightarrow$ " offensichtlich: $K \subseteq L^G$, d. h.

Satz (22.4)

Sei $L|K$ eine endliche Galois-Erweiterung mit Galois-Gruppe $G = \text{Gal}(L|K)$, $\mathcal{U}$ die Menge der Untergruppe von G und $\mathcal{Z}$ die Menge der Zwischenkörper von $L|K$. Dann sind durch die Zuordnungen

$$\phi : \mathcal{U} \rightarrow \mathcal{Z}, U \mapsto L^U \quad \text{und} \quad \psi : \mathcal{Z} \rightarrow \mathcal{U}, M \mapsto \text{Gal}(L|M)$$

zueinander inverse Bijektionen zwischen $\mathcal{U}$ und $\mathcal{Z}$ gegeben.

Beweis von Satz 19.4:

z.zg. $\phi: \mathcal{U} \rightarrow \mathcal{Z}$, $U \mapsto L^U$ und

$\psi: \mathcal{Z} \rightarrow \mathcal{U}$, $M \mapsto \text{Gal}(L|M)$ sind zueinander invers

d.h. zu überprüfen: $\psi \circ \phi = \text{id}_{\mathcal{U}}$, $\phi \circ \psi = \text{id}_{\mathcal{Z}}$,

ausdrücklich (i) $(\psi \circ \phi)(U) = U \quad \forall U \in \mathcal{U}$

(ii) $(\phi \circ \psi)(M) = M \quad \forall M \in \mathcal{Z}$

z.z.i) Sei $U \in \mathcal{U}$, z.zg.: $\text{Gal}(L|L^U) = U$

Dies folgt durch Anwendung von Prop. 22.2 auf die endliche Gruppe $U \leq \text{Aut}(L)$.

z.z.ii) Sei $M \in \mathcal{Z}$, z.zg.: $L^{\text{Gal}(L|M)} = M$. Das folgt aus Folg. 22.3, da $L|M$ endl. Galois-Erweiterung ist. $\square$

Satz (22.5)

- (i) Sind $U_1, U_2 \in \mathcal{U}$ mit $U_1 \subseteq U_2$, dann folgt $L^{U_1} \supseteq L^{U_2}$.
- (ii) Sind umgekehrt $M_1, M_2 \in \mathcal{Z}$ mit $M_1 \subseteq M_2$, dann ist $\text{Gal}(L|M_1) \supseteq \text{Gal}(L|M_2)$.
- (iii) Es gilt $L^{\{\text{id}_L\}} = L$, $L^G = K$ und $\text{Gal}(L|L) = \{\text{id}_L\}$,
 $\text{Gal}(L|K) = G$.
- (iv) Ist M ein Zwischenkörper und $U = \text{Gal}(L|M)$ die zugehörige Untergruppe, dann gilt $[L : M] = |U|$ und $[M : K] = (G : U)$.

Beweis von Satz 22.5, Teil (iv)

$[L:M] = |U|$ ist erfüllt nach Prop. 19.14,
da L/M galois'sch ist

Gradformel $\rightarrow [L:K] = [L:M] \cdot [M:K]$

Satz v. Lagrange $\rightarrow |G| = (G:U) \cdot |U|$

$$\rightarrow [M:K] = \frac{[L:K]}{[L:M]} = \frac{|G|}{|U|} = (G:U).$$

Proposition (22.6)

Sei M ein Zwischenkörper von $L|K$ und $U = \text{Gal}(L|M)$ die zugehörige Untergruppe von $G = \text{Gal}(L|K)$. Dann sind folgende Aussagen äquivalent:

- (i) Die Erweiterung $M|K$ ist normal.
- (ii) Die Untergruppe U ist Normalteiler von G .

In diesem Fall erhalten wir durch $\sigma \mapsto \sigma|_M$ eine Abbildung $G \rightarrow \text{Gal}(M|K)$, und diese induziert einen natürlichen Isomorphismus $G/U \cong \text{Gal}(M|K)$.