## 10.5 Die Auflösbarkeit algebraischer Gleichungen

Gleichungen der Form $x^2 + ax + b = 0$, $a, b \in \mathbb{R}$, also algebraische Gleichungen zweiten Grades, besitzen bekanntlich die Wurzeln

$$x_{1,2} = \frac{-a}{2} \pm \sqrt[2]{\frac{a^2}{4} - b},$$

sie sind also durch Wurzelziehen bei arithmetischen Ausdrücken in den Koeffizienten lösbar. Das gilt auch für die Gleichungen $x^3 + a_1x^2 + a_2x + a_3 = 0$, $a_i \in \mathbb{R}$. Setzt man

$$p := a_2 - \frac{a_1^2}{2},\ q := \frac{2a_1^3}{27} - \frac{a_1a_2}{3} + a_3,\ r := \frac{p^3}{27} + \frac{q^2}{4},$$

sowie

$$P := \sqrt[3]{\frac{-q}{2} + r},\ Q := \sqrt[3]{\frac{-q}{2} - r},\ \zeta := \exp(\frac{2\pi i}{3}),$$

dann ergeben sich die Wurzeln zu

$$x_1 = P + Q - \frac{a_1}{3}, x_2 = \zeta P + \zeta^2 Q - \frac{a_1}{3}, x_3 = \zeta^2 P + \zeta Q - \frac{a_1}{3},\ \text{(Cardano)}$$

Ähnliches gilt für Gleichungen vierten Grades, wie man schon im 16. Jahrhundert festgestellt hat. 1826 hat dann N. H. Abel bewiesen, daß Gleichungen fünften Grades nicht immer auf diese Weise durch Wurzelziehen lösbar sind, und E. Galois fand dann eine notwendige und hinreichende Bedingung für die Existenz solcher Lösungen. Diese Bedingung soll jetzt hergeleitet werden.

**10.5.1 Definition (Radikalerweiterung)** $\mathbb{L} : \mathbb{K}$ heißt *Radikalerweiterung,* wenn $\mathbb{L}$ von $\mathbb{K}$ aus in endlich vielen Schritten durch sukzessives Adjungieren von Wurzeln reiner Polynome erzeugbar ist, d.h. es gilt $\mathbb{L} = \mathbb{K}$ oder es gibt eine endliche Kette

$$\mathbb{K} = \mathbb{K}_0 < \cdots < \mathbb{K}_m = \mathbb{L}$$

von Zwischenkörpern $\mathbb{K}_i$ mit $\mathbb{K}_{i+1} = \mathbb{K}_i(\lambda_i)$, und $\lambda_i^{n_i} \in \mathbb{K}_i$, $n_i$ geeignet. •

**10.5.2 Hilfssatz** *Ist* $\mathbb{L} : \mathbb{K}$ *eine Radikalerweiterung und* $\mathrm{Char}(\mathbb{K}) = 0$, *dann gibt es Erweiterungen* $\mathbb{M} : \mathbb{L}$, *so daß* $\mathbb{M} : \mathbb{K}$ *Galoiserweiterung und Radikalerweiterung von* $\mathbb{K}$ *ist.*

Beweis: Durch Induktion nach $[\mathbb{L} : \mathbb{K}]$.

I $[\mathbb{L} : \mathbb{K}] = 1 : \mathbb{K} = \mathbb{L}$, hier gilt also die Behauptung.

II $[\mathbb{L} : \mathbb{K}] > 1$ : Sei $\mathbb{K} = \mathbb{K}_0 < \cdots < \mathbb{K}_m = \mathbb{L}$. Wir unterscheiden zwei Fälle:

a) $m = 1$ : Sei $\mathbb{L} = \mathbb{K}(\lambda)$ und $\lambda^n \in \mathbb{K}$. Wir adjungieren, falls notwendig, noch eine primitive $n$-te Einheitswurzel $\zeta$ und setzen $\mathbb{M} := \mathbb{L}(\zeta)$. $\mathbb{M}$ enthält mit $\lambda$ und $\zeta$ alle Wurzeln von $x^n - \kappa$, wenn $\kappa := \lambda^n$. $\mathbb{M}$ ist also Zerfällungskörper dieses reinen Polynoms. Demnach ist $\mathbb{M} : \mathbb{K}$ eine Radikalerweiterung mit der Kette von Zwischenkörpern

$$\mathbb{K} = \mathbb{K}_0 \subset \mathbb{K}_1 = \mathbb{L} \subseteq \mathbb{K}_2 = \mathbb{M}.$$

Außerdem ist $\mathbb{M} : \mathbb{K}$ eine Galoiserweiterung, denn $\mathbb{M}$ ist ja Zerfällungskörper eines über $\mathbb{K}$ separablen Polynoms.

b) $m > 1$ : Ohne Einschränkung können wir $\mathbb{K}_{m-1} \subset \mathbb{L}$ und damit, wegen der Endlichkeit von $[\mathbb{L} : \mathbb{K}]$, die Ungleichung $[\mathbb{K}_{m-1} : \mathbb{K}] < [\mathbb{L} : \mathbb{K}]$ voraussetzen, so daß die Induktionsannahme die Existenz eines Erweiterungskörpers $\mathbb{M}'$ (oberhalb von $\mathbb{K}_{m-1}$) liefert, der Galoiserweiterung und Radikalerweiterung von $\mathbb{K}$ ist.

Mit Hilfe von dessen Galoisgruppe definieren wir das Polynom

$$f := \prod_{\sigma \in \mathrm{Gal}(\mathbb{M}' : \mathbb{K})} (x^n - \sigma(\kappa^n)),$$

wobei $\kappa$ und $n$ durch $\mathbb{L} = \mathbb{K}_{m-1}(\kappa)$ und $\kappa^n \in \mathbb{K}_{m-1}$ definiert seien (für irgendein $\kappa$, das durch Adjunktion $\mathbb{L}$ ergibt). Wegen $\tau f = f$, für alle $\tau \in \mathrm{Gal}(\mathbb{M}' : \mathbb{K})$ folgt $f \in \mathbb{K}[x]$.

Jetzt sei $\mathbb{M}$ definiert als Zerfällungskörper von $f$ über $\mathbb{M}'$. Er entsteht durch Adjunktion der $n$-ten Wurzeln der $\sigma(\kappa^n)$ an $\mathbb{M}'$, also ist $\mathbb{M} : \mathbb{M}'$ eine Radikalerweiterung. Da auch $\mathbb{M}' : \mathbb{K}$ Radikalerweiterung ist, erweist sich insgesamt auch $\mathbb{M} : \mathbb{K}$ als Radikalerweiterung.

Es bleibt zu zeigen, daß $\mathbb{M} : \mathbb{K}$ Galoiserweiterung ist. $\mathbb{M}'$ ist Zerfällungskörper eines $g \in \mathbb{K}[x]$, $\mathbb{M}$ ist Zerfällungskörper von $f$ über $\mathbb{M}'$. Insgesamt ist also $\mathbb{M}$ Zerfällungskörper von $gf$ über $\mathbb{K}$, also eine Galoiserweiterung von $\mathbb{K}$, denn $gf$ ist, wegen $\mathrm{Char}(\mathbb{K}) = 0$, separabel.

□

**10.5.3 Satz** *Ist* $\mathrm{Char}(\mathbb{K}) = 0$ *und* $\mathbb{L} : \mathbb{K}$ *sowohl Galoiserweiterung als auch Radikalerweiterung, dann besitzt die Galoisgruppe* $\mathrm{Gal}(\mathbb{L} : \mathbb{K})$ *eine Normalreihe mit zyklischen Faktoren.*

Beweis: Der Fall $\mathbb{L} = \mathbb{K}$ ist trivial. Sei deshalb

$$\mathbb{K} = \mathbb{K}_0 < \cdots < \mathbb{K}_m = \mathbb{L}$$

mit $\mathbb{K}_{i+1} = \mathbb{K}_i(\lambda_i)$ und $\lambda_i^{n_i} \in \mathbb{K}_i$. Wir setzen

$$n := n_0 \cdots n_{m-1},$$

bezeichnen mit $\zeta$ eine primitive $n$-te Einheitswurzel und betrachten die Erweiterungen $\mathbb{K}'_i := \mathbb{K}_i(\zeta)$. Sie bilden die Kette

$$\mathbb{K} \leq \mathbb{K}'_0 \leq \mathbb{K}'_1 \leq \cdots \leq \mathbb{K}'_m = \mathbb{L}' = \mathbb{L}(\zeta).$$

In dieser Kette bilden benachbarte Zwischenkörper Galoiserweiterungen $\mathbb{K}'_{i+1} : \mathbb{K}'_i$, denn $\mathbb{K}'_i$ enthält ja die primitive $n_i$-te Einheitswurzel $\zeta^{n/n_i}$, das Polynom $x^{n/n_i} - \lambda_i^{n_i}$ ist also separabel über $\mathbb{K}'_i$. Außerdem ist die Galoisgruppe dieser Erweiterung, $G_i := \mathrm{Gal}(\mathbb{K}'_{i+1} : \mathbb{K}'_i)$, zyklisch, nach 10.4.10.
Die Erweiterung $\mathbb{L} : \mathbb{K}$ ist Galoiserweiterung, also Zerfällungskörper, etwa von $g \in \mathbb{K}[x]$. $\mathbb{L}(\zeta)$ ist dann Zerfällungskörper von $g(x^n - 1)$, $\mathbb{L}(\zeta) : \mathbb{K}$ ist also Galoiserweiterung, und auch $\mathbb{L}(\zeta) : \mathbb{K}(\zeta)$.
Der Kette

$$\mathbb{K} \leq \mathbb{K}'_0 \leq \mathbb{K}'_1 \leq \ldots \leq \mathbb{K}'_m = \mathbb{L}' = \mathbb{L}(\zeta).$$

entspricht deshalb, nach dem Hauptsatz der Galoistheorie, die Normalkette der entsprechenden Galoisgruppen (durch Anwendung von $\Gamma$):

$$\mathrm{Gal}(\mathbb{L}' : \mathbb{K}) \trianglerighteq \mathrm{Gal}(\mathbb{L}' : \mathbb{K}'_0) \trianglerighteq \ldots \trianglerighteq \mathrm{Gal}(\mathbb{L}' : \mathbb{K}'_m) = \{1\}.$$

Weiter gilt nach dem Hauptsatz, daß deren Faktoren

$$\mathrm{Gal}(\mathbb{L}' : \mathbb{K}'_i)/\mathrm{Gal}(\mathbb{L}' : \mathbb{K}'_{i+1}) \simeq \mathrm{Gal}(\mathbb{K}'_{i+1} : \mathbb{K}'_i)$$

zyklisch sind. Daraus folgt, weil mit $\mathbb{L}' : \mathbb{K}$ auch $\mathbb{L} : \mathbb{K}$ Galoiserweiterung ist, nach dem Hauptsatz:

$$\mathrm{Gal}(\mathbb{L} : \mathbb{K}) \simeq \mathrm{Gal}(\mathbb{L}' : \mathbb{K})/\mathrm{Gal}(\mathbb{L}' : \mathbb{L}).$$

Demnach besitzt auch $\mathrm{Gal}(\mathbb{L} : \mathbb{K})$ eine Normalreihe mit zyklischen Faktoren.
□

**10.5.4 Satz** *Ist* $\mathbb{L} : \mathbb{K}$ *eine endliche Galoiserweiterung,* $\mathrm{Char}(\mathbb{K}) = 0$ *und besitzt* $\mathrm{Gal}(\mathbb{L} : \mathbb{K})$ *eine Kompositionsreihe mit zyklischen Faktoren, dann gibt es eine Einheitswurzel* $\zeta$*, so daß* $\mathbb{L}(\zeta) : \mathbb{K}$ *eine Radikalerweiterung ist.*

Beweis: Eine aus dieser Normalreihe durch Verfeinerung hervorgegangene Kompositionsreihe sei

$$\mathrm{Gal}(\mathbb{L} : \mathbb{K}) = G_0 \rhd G_1 \rhd \cdots \rhd G_m = \{1\},$$

mit den (zyklischen!) Faktoren $G_i/G_{i+1}$. Die Abbildung $\Phi$ aus der Galoisverbindung ergibt die entsprechende Kette von Fixkörpern

$$\mathbb{K} = \mathbb{L}_{G_0} < \mathbb{L}_{G_1} < \cdots < \mathbb{L}_{G_m} = \mathbb{L}.$$

Hierfür gilt nach dem Hauptsatz, wenn $\mathbb{K}_i := \mathbb{L}_{G_i}$,

a) $G_i = \mathrm{Gal}(\mathbb{L} : \mathbb{K}_i) \trianglelefteq \mathrm{Gal}(\mathbb{L} : \mathbb{K})$,

b) $\mathbb{K}_{i+1} : \mathbb{K}_i$ ist endliche Galoiserweiterung,

c) $\mathrm{Gal}(\mathbb{K}_{i+1} : \mathbb{K}_i) \simeq \mathrm{Gal}(\mathbb{L} : \mathbb{K}_i)/\mathrm{Gal}(\mathbb{L} : \mathbb{K}_{i+1})$,

und aus der letzten Isomorphie folgt noch, daß $\mathrm{Gal}(\mathbb{K}_{i+1} : \mathbb{K}_i)$ zyklisch ist.

Sei jetzt $n := |\mathrm{Gal}(\mathbb{L} : \mathbb{K})|$, $\zeta$ eine primitive $n-$te Einheitswurzel. Wir wollen zeigen, daß $\mathbb{L}(\zeta) : \mathbb{K}$ die Behauptung erfüllt.

$\mathbb{K}_{i+1} : \mathbb{K}_i$ ist Galoiserweiterung, also auch $\mathbb{K}_{i+1}(\zeta) : \mathbb{K}_i$ und $\mathbb{K}_{i+1} : \mathbb{K}_i(\zeta)$. Die Einschränkung $\psi$ der Automorphismen auf $\mathbb{K}_{i+1}$ ist ein Homomorphismus

$$\psi\colon \mathrm{Gal}(\mathbb{K}_{i+1}(\zeta) : \mathbb{K}_i) \to \mathrm{Gal}(\mathbb{K}_{i+1} : \mathbb{K}_i), \sigma \mapsto \sigma \downarrow \mathbb{K}_{i+1}.$$

Dessen Einschränkung auf die Untergruppe $\mathrm{Gal}(\mathbb{K}_{i+1}(\zeta) : \mathbb{K}_i(\zeta))$ ist dann ein Homomorphismus

$$\psi \downarrow \mathrm{Gal}(\mathbb{K}_{i+1}(\zeta) : \mathbb{K}_i(\zeta))\colon \mathrm{Gal}(\mathbb{K}_{i+1}(\zeta) : \mathbb{K}_i(\zeta)) \to \mathrm{Gal}(\mathbb{K}_{i+1} : \mathbb{K}_i), \sigma \mapsto \sigma \downarrow \mathbb{K}_{i+1}.$$

Dieser erweist sich als injektiv: Liegt $\sigma$ im Kern, dann ist $\sigma(\kappa) = \kappa$, für alle $\kappa \in \mathbb{K}_{i+1} \cup \mathbb{K}_i(\zeta) = \mathbb{K}_{i+1}(\zeta)$, und damit die identische Abbildung.
Wir können also darauf schließen, daß $\mathrm{Gal}(\mathbb{K}_{i+1}(\zeta) : \mathbb{K}_i(\zeta))$ isomorph zu einer Untergruppe von $\mathrm{Gal}(\mathbb{K}_{i+1} : \mathbb{K}_i)$ und damit ebenfalls zyklisch ist, ihre Ordnung $n_i$ teilt $n$. Also enthält $\mathbb{K}_i(\zeta)$ eine primitive $n_i-$te Einheitswurzel: $\zeta^{n/n_i}$. $\mathbb{K}_{i+1}(\zeta)$ entsteht demnach aus $\mathbb{K}_i(\zeta)$ durch Adjunktion einer $n_i-$ten Wurzel. Demnach ist $\mathbb{L}(\zeta) : \mathbb{K}$ eine Radikalerweiterung, wie behauptet.

□