Vertiefung der Algebra

Wintersemester 2013/2014

Universität Bayreuth

Michael Stoll

Inhaltsverzeichnis

Druckversion vom 21. Januar 2014, 17:52 Uhr.

1. Einführung

Diese Vorlesung setzt die Vorlesung „Einführung in die Algebra“ fort. Zweck der Vorlesung ist es, Ihnen den Stoff aus dem Bereich der Algebra nahe zu bringen, den Sie für die Staatsexamensklausur brauchen, der aber in den ersten beiden Algebra-Vorlesungen („Einführung in die Zahlentheorie und algebraische Strukturen“ und „Einführung in die Algebra“) nicht untergebracht werden konnte. Natürlich kann die „Vertiefung der Algebra“ auch für Fach-Studierende interessant sein, die sich im Bereich der Algebra spezialisieren wollen; Leistungspunkte gibt es allerdings nur für die Lehramts-Studierenden.

Dieser noch fehlende Stoff umfasst im Wesentlichen die sogenannte *Galoistheorie*. Kurz gesagt, handelt es sich um das Studium der Struktur von Zerfällungskörpern; insbesondere um die Beschreibung der Zwischenkörper zwischen dem Grundkörper k und dem Zerfällungskörper K eines Polynoms $f \in k[X]$. Eine entscheidende Rolle spielt dabei die *Automorphismengruppe* der Körpererweiterung $k \subset K$. Dies ist eine endliche Gruppe der Ordnung $[K : k]$, deren Elemente man mit gewissen Permutationen der Nullstellen von f in K identifizieren kann. Daran können Sie schon sehen, dass Sie sich noch einmal die Theorie der algebraischen Körpererweiterungen und die Theorie der endlichen Gruppen aus der „Einführung in die Algebra“ gut ansehen sollten.


É. Galois
(1811–1832)

Die Bezeichnung „Galoistheorie“ verweist auf Évariste Galois, der die grundlegenden Zusammenhänge Anfang der 1830er Jahre erkannte und kurz darauf nach einem Duell im Alter von 20 Jahren starb.

Um diese Zusammenhänge zu verdeutlichen, beginnen wir mit einem Beispiel, das so oder ähnlich immer mal wieder als Aufgabe im Staatsexamen auftaucht.

Beispiel. Wir setzen $k = \mathbb{Q}$ und betrachten das Polynom $f = X^4 - 17 \in \mathbb{Q}[X]$. Das Eisenstein-Kriterium mit $p = 17$ sagt uns, dass f in $\mathbb{Z}[X]$ und damit auch in $\mathbb{Q}[X]$ irreduzibel ist.

Wir wollen einen Zerfällungskörper K von f konstruieren. Da $\mathbb{Q}$ in den algebraisch abgeschlossenen Körper $\mathbb{C}$ eingebettet ist, erhalten wir K als $\mathbb{Q}(\alpha_1, \ldots, \alpha_4) \subset \mathbb{C}$, wobei $\alpha_1, \ldots, \alpha_4 \in \mathbb{C}$ die vier Nullstellen von f sind. Wir müssen also die komplexen Nullstellen von f finden. Eine davon ist sicherlich $\alpha_1 = \sqrt[4]{17}$. Für jede weitere Nullstelle α gilt dann $(\alpha/\alpha_1)^4 = \alpha^4/\alpha_1^4 = 17/17 = 1$, also ist α/α_1 eine vierte Einheitswurzel. Davon gibt es vier Stück, nämlich 1, $\boldsymbol{i}$, $\boldsymbol{i}^2 = -1$ und $\boldsymbol{i}^3 = -\boldsymbol{i}$. Wir erhalten also

$$\alpha_1 = \sqrt[4]{17}\,, \qquad \alpha_2 = \boldsymbol{i}\sqrt[4]{17}\,, \qquad \alpha_3 = -\sqrt[4]{17} \qquad \text{und} \qquad \alpha_4 = -\boldsymbol{i}\sqrt[4]{17}\,.$$

(Allgemein gilt analog, dass die Nullstellen in $\mathbb{C}$ von $X^n - a$ genau die Zahlen $\zeta_n^j \sqrt[n]{a}$ sind für $j = 0, 1, \ldots, n-1$, wobei $\zeta_n = e^{2\pi \boldsymbol{i}/n}$ eine primitive $n$te Einheitswurzel ist.) Wegen $\alpha_3 = -\alpha_1$ und $\alpha_4 = -\alpha_2$ ist

$$K = \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3, \alpha_4) = \mathbb{Q}(\alpha_1, \alpha_2) = \mathbb{Q}(\sqrt[4]{17}, \boldsymbol{i}\sqrt[4]{17}) = \mathbb{Q}(\sqrt[4]{17}, \boldsymbol{i})\,.$$

Die letzte Gleichheit folgt aus

$$\boldsymbol{i}\sqrt[4]{17} = \boldsymbol{i} \cdot \sqrt[4]{17} \in \mathbb{Q}(\sqrt[4]{17}, \boldsymbol{i})$$

und

$$\boldsymbol{i} = \frac{\boldsymbol{i}\sqrt[4]{17}}{\sqrt[4]{17}} \in \mathbb{Q}(\sqrt[4]{17}, \boldsymbol{i}\sqrt[4]{17})\,.$$

Hier verwenden wir, dass der Körper $k(\alpha, \beta, \gamma, \ldots)$ genau aus allen rationalen Ausdrücken in $\alpha, \beta, \gamma, \ldots$ über k besteht, also Quotienten von Polynomen in $\alpha, \beta, \gamma, \ldots$ mit Koeffizienten in k (wobei der Nenner natürlich nicht verschwinden darf).

Was ist der Grad der Körpererweiterung $\mathbb{Q} \subset K$? Um ihn zu bestimmen, zerlegt man die Körpererweiterung am besten in zwei Schritte und verwendet den Gradsatz:

$$[K : \mathbb{Q}] = [K : \mathbb{Q}(\sqrt[4]{17})] \cdot [\mathbb{Q}(\sqrt[4]{17}) : \mathbb{Q}] \,.$$

Den zweiten Faktor können wir leicht bestimmen. Zur Erinnerung:

LEMMA Grad für einfache KE

1.1. **Lemma.** *Sei $k \subset k(a)$ eine einfache algebraische Körpererweiterung. Sei weiter $m \in k[X]$ das Minimalpolynom von a. Dann ist*

$$[k(a) : k] = \deg(m) \,.$$

Allgemeiner gilt: Ist $p \in k[X]$ ein normiertes Polynom mit $p(a) = 0$, dann ist

$$[k(a) : k] \leq \deg(p) \,.$$

Hier wissen wir, dass $\sqrt[4]{17}$ eine Nullstelle des normierten irreduziblen Polynoms f ist, also ist f das Minimalpolynom von $\sqrt[4]{17}$, und es folgt

$$[\mathbb{Q}(\sqrt[4]{17}) : \mathbb{Q}] = \deg(f) = 4 \,.$$

Es bleibt der Faktor

$$[K : \mathbb{Q}(\sqrt[4]{17})] = [\mathbb{Q}(\sqrt[4]{17}, \boldsymbol{i}) : \mathbb{Q}(\sqrt[4]{17})]$$

zu bestimmen. Dies ist ebenfalls eine einfache Körpererweiterung, denn wir adjungieren $\boldsymbol{i}$ zu $\mathbb{Q}(\sqrt[4]{17})$. Da $\boldsymbol{i}$ Nullstelle von X^2+1 ist, ist der Grad dieser Erweiterung höchstens $\deg(X^2 + 1) = 2$. Da $\boldsymbol{i}$ nicht reell ist, aber wegen $\sqrt[4]{17} \in \mathbb{R}$ der Körper $\mathbb{Q}(\sqrt[4]{17})$ in $\mathbb{R}$ enthalten ist, ist $X^2 + 1$ auch in $\mathbb{Q}(\sqrt[4]{17})[X]$ irreduzibel (da ohne Nullstelle), und es folgt

$$[K : \mathbb{Q}(\sqrt[4]{17})] = 2 \,, \qquad \text{also} \qquad [K : \mathbb{Q}] = 2 \cdot 4 = 8 \,.$$

Wir betrachten jetzt die Automorphismen der Körpererweiterung $\mathbb{Q} \subset K$.

DEF Automorphismus einer KE

1.2. **Definition.** Sei $k \subset K$ eine Körpererweiterung. Ein *Automorphismus* dieser Körpererweiterung ist ein Automorphismus σ von K mit $\sigma|_k = \mathrm{id}_k$ (also $\sigma(a) = a$ für alle $a \in k$).

Wie üblich bildet die Menge aller Automorphismen eine Gruppe, die *Automorphismengruppe* der Körpererweiterung, geschrieben $\mathrm{Aut}(K/k)$. Sie ist eine Untergruppe der Automorphismengruppe $\mathrm{Aut}(K)$ von K. ♢

Ein Automorphismus eines Körpers K ist ein bijektiver Ringhomomorphismus $\sigma\colon K \to K$. Wir erinnern uns:

LEMMA Ringhom. von Körpern sind injektiv

1.3. **Lemma.** *Seien K ein Körper und $R \neq \{0\}$ ein Ring. Dann ist jeder Ringhomomorphismus $\phi\colon K \to R$ injektiv.*

Beweis. ϕ ist genau dann injektiv, wenn $\ker(\phi) = \{0\}$ ist. Nun ist $\ker(\phi)$ ein Ideal von K, aber als Körper hat K nur die beiden Ideale $\{0\}$ und K. $\ker(\phi) = K$ kommt wegen $\phi(1) = 1 \neq 0$ nicht infrage, also muss $\ker(\phi) = \{0\}$ sein. ❑

Auch die Surjektivität müssen wir normalerweise nicht nachweisen, denn es gilt Folgendes.

1.4. **Lemma.** *Sei $k \subset K$ eine endliche Körpererweiterung und sei $\sigma\colon K \to K$ ein Ringhomomorphismus mit $\sigma|_k = \mathrm{id}_k$. Dann ist $\sigma \in \mathrm{Aut}(K/k)$.*

LEMMA Surjektivität automatisch

Beweis. Wir erinnern uns daran, dass K ein k-Vektorraum ist. Weil σ ein Ringhomomorphismus ist und $\sigma(\lambda) = \lambda$ gilt für $\lambda \in k$, ist σ eine k-lineare Abbildung $K \to K$. Da die Körpererweiterung endlich ist, ist K als k-Vektorraum endlichdimensional. Nach Lemma 1.3 ist σ injektiv. Ein injektiver Endomorphismus eines endlich-dimensionalen Vektorraums ist aber schon bijektiv. ❑

Ist $k = \mathbb{Q}$, dann ist die Bedingung „$\sigma|_k = \mathrm{id}_k$“ automatisch erfüllt, denn alle rationalen Zahlen lassen sich aus 0 und 1 erzeugen, die beide unter jedem Automorphismus von K fest bleiben. Es gilt hier also einfach

$$\mathrm{Aut}(K/\mathbb{Q}) = \mathrm{Aut}(K) = \{\sigma\colon K \to K \mid \sigma \text{ Ringhomomorphismus}\}\,.$$

Wie können wir die Elemente von $\mathrm{Aut}(K/\mathbb{Q})$ beschreiben? Offenbar genügt es, die Bilder der Erzeuger $\sqrt[4]{17}$ und $\boldsymbol{i}$ zu kennen, denn dann weiß man auch, wie jeder $\mathbb{Q}$-rationale Ausdruck in diesen Erzeugern abgebildet wird, also kennt man die Abbildung auf ganz K. Was sind nun die möglichen Bilder von $\sqrt[4]{17}$ und von $\boldsymbol{i}$? Dazu ein Lemma:

1.5. **Lemma.** *Sei $k \subset K$ eine Körpererweiterung, $\alpha \in K$ und $f \in k[X]$ ein Polynom mit $f(\alpha) = 0$. Ist $\sigma \in \mathrm{Aut}(K/k)$, dann ist $\sigma(\alpha)$ eine Nullstelle von f in K.*

LEMMA Nullstellen bleiben Nullstellen

Beweis. Sei $f = a_nX^n + a_{n-1}X^{n-1} + \ldots + a_1X + a_0$. Dann ist

$$\begin{aligned} f(\sigma(\alpha)) &= a_n\sigma(\alpha)^n + a_{n-1}\sigma(\alpha)^{n-1} + \ldots + a_1\sigma(\alpha) + a_0 \\ &= \sigma(a_n)\sigma(\alpha^n) + \sigma(a_{n-1})\sigma(\alpha^{n-1}) + \ldots + \sigma(a_1)\sigma(\alpha) + \sigma(a_0) \\ &= \sigma(a_n\alpha^n + a_{n-1}\alpha^{n-1} + \ldots + a_1\alpha + a_0) \\ &= \sigma(f(\alpha)) = \sigma(0) = 0\,. \end{aligned}$$

Hierbei haben wir verwendet, dass σ ein Ringhomomorphismus ist, und dass $\sigma(a) = a$ gilt für alle $a \in k$, also insbesondere für die Koeffizienten von f. ❑

Damit sehen wir, dass für $\sigma \in \mathrm{Aut}(K/\mathbb{Q})$ gelten muss

$$\sigma(\sqrt[4]{17}) \in \{\sqrt[4]{17}, \boldsymbol{i}\sqrt[4]{17}, -\sqrt[4]{17}, -\boldsymbol{i}\sqrt[4]{17}\} \qquad \text{und} \qquad \sigma(\boldsymbol{i}) \in \{\boldsymbol{i}, -\boldsymbol{i}\}\,.$$

Um zu sehen, welche dieser (insgesamt acht) Möglichkeiten tatsächlich zu einem Automorphismus führen, brauchen wir ein weiteres Lemma.

1.6. **Lemma.** *Sei $k \subset K = k(\alpha)$ eine einfache Körpererweiterung, sei f das Minimalpolynom von α über k, und sei $\beta \in K$ eine Nullstelle von f. Dann gibt es einen eindeutig bestimmten Automorphismus $\sigma \in \mathrm{Aut}(K/k)$ mit $\sigma(\alpha) = \beta$.*

LEMMA Existenz von Automorphismen

Beweis. Wir erinnern uns daran, dass die durch $X \mapsto \alpha$ (Auswertungshomomorphismus) gegebene Abbildung $k[X] \to K$ einen k-linearen Isomorphismus $\phi_\alpha\colon k[X]/\langle f\rangle \to K$ induziert. (Denn der Kern ist gerade $\langle f\rangle$: Die Polynome mit Nullstelle α sind genau die Vielfachen des Minimalpolynoms. Das Bild ist $k(\alpha) = K$.) Da f auch das Minimalpolynom von β ist, erhalten wir ebenso einen k-linearen Isomorphismus $\phi_\beta\colon k[X]/\langle f\rangle \to K$. Die Komposition $\phi_\beta \circ \phi_\alpha^{-1}$ leistet das Gewünschte. ❑

Wir können das hier wie folgt anwenden:

(1) Es gibt ein eindeutig bestimmtes $\sigma \in \mathrm{Aut}(K/\mathbb{Q}(\boldsymbol{i})) \leq \mathrm{Aut}(K/\mathbb{Q})$ mit $\sigma(\sqrt[4]{17}) = \boldsymbol{i}\sqrt[4]{17}$.
(2) Es gibt ein eindeutig bestimmtes $\tau \in \mathrm{Aut}(K/\mathbb{Q}(\sqrt[4]{17})) \leq \mathrm{Aut}(K/\mathbb{Q})$ mit $\tau(\boldsymbol{i}) = -\boldsymbol{i}$.

Die erste Aussage folgt daraus, dass f auch über $\mathbb{Q}(\boldsymbol{i})$ irreduzibel ist (denn es gilt $[\mathbb{Q}(\boldsymbol{i}, \sqrt[4]{17}) : \mathbb{Q}(\boldsymbol{i})] = 4 = \deg(f)$), die zweite daraus, dass $X^2 + 1$ über $\mathbb{Q}(\sqrt[4]{17})$ irreduzibel ist (das haben wir bereits bei der Bestimmung von $[K : \mathbb{Q}]$ benutzt). Für $\sigma, \tau \in \mathrm{Aut}(K/\mathbb{Q})$ gilt also

$$\sigma(\sqrt[4]{17}) = \boldsymbol{i}\sqrt[4]{17}\,, \quad \sigma(i) = \boldsymbol{i} \qquad \text{und} \qquad \tau(\sqrt[4]{17}) = \sqrt[4]{17}\,, \quad \tau(\boldsymbol{i}) = -\boldsymbol{i}\,.$$

Dass $X^4 - 17$ über $\mathbb{Q}(\boldsymbol{i})$ irreduzibel bleibt, kann man auch mit dem Eisenstein-Kriterium sehen: Der Ring $\mathbb{Z}[\boldsymbol{i}]$ der ganzen gaußschen Zahlen, dessen Quotientenkörper $\mathbb{Q}(\boldsymbol{i})$ ist, ist euklidisch und damit ein Hauptidealring. Die Primzahl 17 zerlegt sich in $\mathbb{Z}[\boldsymbol{i}]$ in ein Produkt von zwei nicht-assoziierten Primelementen: $17 = (4 + \boldsymbol{i})(4 - \boldsymbol{i})$. Mit (z.B.) $\pi = 4 + \boldsymbol{i}$ gilt dann, dass π alle Koeffizienten von $X^4 - 17$ bis auf den Leitkoeffizienten teilt, aber π^2 den konstanten Term 17 nicht teilt. Damit ist $X^4 - 17$ irreduzibel über $\mathbb{Z}[\boldsymbol{i}]$ und also auch über $\mathbb{Q}(\boldsymbol{i})$.

Daraus folgt $\sigma^4 = \tau^2 = \mathrm{id}_K$ und $\tau\sigma\tau = \sigma^{-1}$, wie folgende Tabellen zeigen. Wir schreiben $\alpha = \sqrt[4]{17}$. (Beachte: $\sigma\tau = \sigma \circ \tau$; τ wird zuerst ausgeführt.)

	σ	σ^2	σ^3	σ^4	τ	τ^2	$\sigma\tau$	$\sigma^2\tau$	$\sigma^3\tau$	$\tau\sigma\tau$
α	$\boldsymbol{i}\alpha$	$-\alpha$	$-\boldsymbol{i}\alpha$	α	α	α	$\boldsymbol{i}\alpha$	$-\alpha$	$-\boldsymbol{i}\alpha$	$-\boldsymbol{i}\alpha$
$\boldsymbol{i}$	$\boldsymbol{i}$	$\boldsymbol{i}$	$\boldsymbol{i}$	$\boldsymbol{i}$	$-\boldsymbol{i}$	$\boldsymbol{i}$	$-\boldsymbol{i}$	$-\boldsymbol{i}$	$-\boldsymbol{i}$	$\boldsymbol{i}$

Wir erhalten insgesamt acht verschiedene Automorphismen, nämlich

$$\mathrm{id}_K,\ \sigma,\ \sigma^2,\ \sigma^3,\ \tau,\ \sigma\tau,\ \sigma^2\tau,\ \sigma^3\tau\,,$$

und die Relationen $\sigma^4 = \tau^2 = \mathrm{id}_K$, $\tau\sigma\tau = \sigma^{-1}$ zeigen, dass die Gruppe $\mathrm{Aut}(K/\mathbb{Q})$ isomorph zur Diedergruppe D_4 ist, wobei σ der Drehung um $\pi/2$ und τ einer Spiegelung entspricht.

Wenn man die vier Nullstellen von f betrachtet, dann ergibt sich folgende Wirkung der acht Automorphismen (die natürlich auch dadurch festgelegt sind, was sie mit diesen Nullstellen machen, denn die Nullstellen von f erzeugen K).

	id_K	σ	σ^2	σ^3	τ	$\sigma\tau$	$\sigma^2\tau$	$\sigma^3\tau$
α	α	$\boldsymbol{i}\alpha$	$-\alpha$	$-\boldsymbol{i}\alpha$	α	$\boldsymbol{i}\alpha$	$-\alpha$	$-\boldsymbol{i}\alpha$
$\boldsymbol{i}\alpha$	$\boldsymbol{i}\alpha$	$-\alpha$	$-\boldsymbol{i}\alpha$	α	$-\boldsymbol{i}\alpha$	α	$\boldsymbol{i}\alpha$	$-\alpha$
$-\alpha$	$-\alpha$	$-\boldsymbol{i}\alpha$	α	$\boldsymbol{i}\alpha$	$-\alpha$	$-\boldsymbol{i}\alpha$	α	$\boldsymbol{i}\alpha$
$-\boldsymbol{i}\alpha$	$-\boldsymbol{i}\alpha$	α	$\boldsymbol{i}\alpha$	$-\alpha$	$\boldsymbol{i}\alpha$	$-\alpha$	$-\boldsymbol{i}\alpha$	α

Wir sehen, dass die vier Nullstellen jeweils permutiert werden. Das gilt allgemein:

1.7. **Lemma.** *Seien $k \subset K$ eine Körpererweiterung, $\sigma \in \mathrm{Aut}(K/k)$ und $f \in k[X]$ normiert. Sei weiter $N_f = \{\alpha \in K \mid f(\alpha) = 0\}$ die Menge der Nullstellen von f in K. Dann permutiert σ die Elemente von N_f, und wir erhalten einen Gruppenhomomorphismus $\mathrm{Aut}(K/k) \to S(N_f)$, $\sigma \mapsto \sigma|_{N_f}$. Ist K ein Zerfällungskörper von f, dann ist dieser Gruppenhomomorphismus injektiv.*

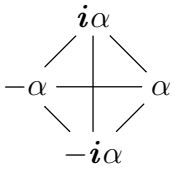
LEMMA Automorphismen permutieren Nullstellen

Dabei bezeichnet $S(X)$ die symmetrische Gruppe (Gruppe der Permutationen) einer Menge X. Wir können die Gruppe $\mathrm{Aut}(K/k)$ also als eine Untergruppe von $S(N_f)$ betrachten.

Beweis. Nach Lemma 1.5 bildet σ die Menge N_f in sich ab. Da σ bijektiv ist, ist $\sigma|_{N_f}$ jedenfalls injektiv. Weil N_f endlich ist, muss $\sigma|_{N_f}$ dann auch bijektiv sein, also ist $\sigma|_{N_f} \in S(N_f)$. Dass die Abbildung $\sigma \mapsto \sigma|_{N_f}$ ein Gruppenhomomorphismus ist, ist klar.

Ist K Zerfällungskörper von f, dann gilt $K = k(N_f)$, und σ ist durch $\sigma|_{N_f}$ eindeutig bestimmt. Also ist die Abbildung $\mathrm{Aut}(K/k) \to S(N_f)$, $\sigma \mapsto \sigma|_{N_f}$ in diesem Fall injektiv. ❑

In unserem Beispiel können wir die Diedergruppe D_4 sogar „sehen“: Die Gruppe $\mathrm{Aut}(K/\mathbb{Q})$ entspricht nämlich genau der Symmetriegruppe des Quadrats in der Ebene $\mathbb{C}$, dessen Ecken die vier Nullstellen von f sind. (Es gilt aber *nicht*, dass die Wirkung etwa von σ auf jedes Element von K einer Drehung um $\pi/2$ entspricht, denn zum Beispiel ist $\sigma(1) = 1$. Diese Entsprechung gilt *nur* für die Menge der Nullstellen von f; sie kommt aus der speziellen Form des Polynoms und lässt sich nicht unbedingt auf andere Polynome übertragen.)



Wir haben also unserem Polynom $f \in \mathbb{Q}[X]$ eine Gruppe zugeordnet. Wir überlegen uns jetzt, dass das ganz allgemein funktioniert.

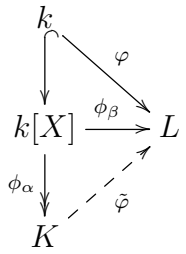
Dazu verallgemeinern wir zunächst Lemma 1.6:

1.8. **Lemma.** *Sei $k \subset K = k(\alpha)$ eine einfache Körpererweiterung und sei f das Minimalpolynom von α über k. Seien L ein weiterer Körper und $\varphi\colon k \to L$ ein Homomorphismus. Wir schreiben f^φ für das Polynom in $L[X]$, das aus f entsteht, indem man φ auf die Koeffizienten anwendet. Ist $\beta \in L$ eine Nullstelle von f^φ, dann gibt es einen eindeutig bestimmten Homomorphismus $\tilde\varphi\colon K \to L$ mit $\tilde\varphi(\alpha) = \beta$ und $\tilde\varphi|_k = \varphi$.*

LEMMA
Fortsetzung von Automorphismen

Insbesondere gibt es genau $\#\{\beta \in L \mid f^\varphi(\beta) = 0\}$ verschiedene Homomorphismen $\tilde\varphi\colon K \to L$ mit $\tilde\varphi|_k = \varphi$.

Beweis. Der durch $X \mapsto \alpha \in K$ gegebene Einsetzungshomomorphismus ϕ_α ist surjektiv. Wir betrachten folgendes Diagramm:



Nach der universellen Eigenschaft des Polynomrings gibt es genau einen Ringhomomorphismus $\phi_\beta\colon k[X] \to L$ mit $\phi_\beta|_k = \varphi$ und $\phi_\beta(X) = \beta$. Da $\phi_\beta(f) = f^\varphi(\beta) = 0$ ist, gilt $\ker(\phi_\beta) \supset \langle f\rangle_{k[X]}$. Also induziert ϕ_β einen eindeutig bestimmten Homomorphismus $\tilde\varphi$ mit den gewünschten Eigenschaften.

Für jedes solche $\tilde\varphi$ muss gelten $f^\varphi\big(\tilde\varphi(\alpha)\big) = \tilde\varphi\big(f(\alpha)\big) = \tilde\varphi(0) = 0$, α muss also auf eine Nullstelle von f^φ in L abgebildet werden. Nach dem bereits Bewiesenen gibt es zu jeder solchen Nullstelle genau ein passendes $\tilde\varphi$. ❑

1.9. **Satz.** *Sei $f \in \mathbb{Q}[X]$ ein normiertes irreduzibles Polynom und $K \subset \mathbb{C}$ der Zerfällungskörper von f in $\mathbb{C}$. Dann gilt $\#\operatorname{Aut}(K/\mathbb{Q}) = [K : \mathbb{Q}]$, und $\operatorname{Aut}(K/\mathbb{Q})$ ist in natürlicher Weise eine Untergruppe von $S(N_f)$, wobei*

$$N_f = \{\alpha \in \mathbb{C} \mid f(\alpha) = 0\}$$

die Menge der Nullstellen von f in $\mathbb{C}$ ist.

SATZ $\#\operatorname{Aut}(K/\mathbb{Q}) = [K : \mathbb{Q}]$

1.10. **Definition.** Diese Untergruppe von $S(N_f)$ heißt die *Galoisgruppe* von f (über $\mathbb{Q}$), $\operatorname{Gal}(f/\mathbb{Q})$. ♢

DEF Galoisgruppe $\operatorname{Gal}(f/\mathbb{Q})$

Beweis. Wir zeigen durch Induktion über $[K : L]$ für jeden Zwischenkörper $\mathbb{Q} \subset L \subset K$, dass sich jeder Homomorphismus $\varphi\colon L \to K$ auf genau $[K : L]$ verschiedene Weisen zu einem Automorphismus von K fortsetzen lässt. Die Aussage „$\#\operatorname{Aut}(K/\mathbb{Q}) = [K : \mathbb{Q}]$“ folgt dann mit $L = \mathbb{Q}$ (mit dem eindeutig bestimmten $\varphi\colon \mathbb{Q} \hookrightarrow K$).

Im Induktionsanfang ist $L = K$ und $[K : L] = 1$; in diesem Fall ist die Aussage trivial. Sei nun $\mathbb{Q} \subset L \subsetneq K$ ein Zwischenkörper. Dann gibt es eine Nullstelle $\alpha \in K$ von f mit $\alpha \notin L$ (denn K wird von allen Nullstellen erzeugt; wären sie bereits alle in L, dann folgte $L = K$). Sei $L' = L(\alpha) \subset K$ und sei $\varphi\colon L \to K$ ein Homomorphismus. Sei weiter f_L das Minimalpolynom von α über L; dann sind f_L und f_L^φ Teiler von f in $K[X]$, und weil f in K keine mehrfachen Nullstellen hat, hat f_L^φ in K genau $\deg(f_L^\varphi) = \deg(f_L) = [L'\colon L]$ verschiedene Nullstellen. Nach Lemma 1.8 gibt es also $[L'\colon L]$ verschiedene Fortsetzungen von φ zu Homomorphismen $\varphi'\colon L' \to K$. Nach Induktionsvoraussetzung (beachte $[K : L'] < [K : L]$ wegen $L \subsetneq L'$) lässt sich jedes solche φ' auf genau $[K : L']$ verschiedene Weisen zu einem Automorphismus von K fortsetzen. Insgesamt sehen wir, dass es genau $[K : L'] \cdot [L' : L] = [K : L]$ verschiedene Fortsetzungen von φ zu einem Automorphismus von K gibt, wie behauptet.

Die zweite Aussage im Satz wurde bereits in Lemma 1.7 bewiesen. ❑

Wenn $\#N_f = n$ ist und man die Nullstellen irgendwie nummeriert, dann kann man $S(N_f)$ mit der symmetrischen Gruppe S_n identifizieren. Die Galoisgruppe von f ist dann eine Untergruppe von S_n; sie ist bis auf Konjugation in S_n eindeutig bestimmt. (Konjugation in S_n entspricht einem Wechsel der Nummerierung — Übung!) In unserem Beispiel können wir also schreiben $\operatorname{Gal}(f/\mathbb{Q}) = D_4$.

Wir werden das bald auf beliebige Körper (an Stelle von $\mathbb{Q}$) verallgemeinern.

1.11. **Beispiel.** Damit Sie sehen, dass die Gleichung $\#\operatorname{Aut}(K/\mathbb{Q}) = [K : \mathbb{Q}]$ nicht immer gelten muss, betrachten wir jetzt noch den Körper $L = \mathbb{Q}(\sqrt[4]{17})$. Die Nullstellen von f in L sind $\sqrt[4]{17}$ und $-\sqrt[4]{17}$. Damit gibt es nur die beiden Automorphismen id_L und $\sigma^2|_L$, also ist

BSP $\#\operatorname{Aut}(K/\mathbb{Q}) \neq [K : \mathbb{Q}]$

$$4 = [L : \mathbb{Q}] \neq \#\operatorname{Aut}(L/\mathbb{Q}) = 2\,.$$

Die Voraussetzung, dass K Zerfällungskörper eines Polynoms ist, ist also wesentlich. ♣

Wir können nun jeder *Untergruppe* $U \leq \operatorname{Gal}(f/\mathbb{Q}) = \operatorname{Aut}(K/\mathbb{Q})$ einen *Zwischenkörper* der Körpererweiterung $\mathbb{Q} \subset K$ zuordnen durch

$$\mathcal{F}(U) = \{a \in K \mid \sigma(a) = a \text{ für alle } \sigma \in U\}\,.$$

Dieser Körper $\mathcal{F}(U)$ heißt auch der *Fixkörper* von U, weil er aus den Elementen

DEF Fixkörper

besteht, die von U fest gelassen werden, die also Fixpunkte von allen $\sigma \in U$ sind. Wie sieht das im Beispiel aus? Dazu beachten wir, dass sich jedes Element von K eindeutig in der Form

$$a + b\alpha + c\alpha^2 + d\alpha^3 + e\boldsymbol{i} + f\boldsymbol{i}\alpha + g\boldsymbol{i}\alpha^2 + h\boldsymbol{i}\alpha^3$$

mit $a, b, c, d, e, f, g, h \in \mathbb{Q}$ schreiben lässt. Wenn wir dafür kurz (a, b, c, d, e, f, g, h) schreiben, dann operieren die Elemente von $\mathrm{Gal}(f/\mathbb{Q})$ wie folgt:

id	$(a, \ b, \ c, \ d, \ e, \ f, \ g, \ h)$
σ	$(a, -f, -c, \ h, \ e, \ b, -g, -d)$
σ^2	$(a, -b, \ c, -d, \ e, -f, \ g, -h)$
σ^3	$(a, \ f, -c, -h, \ e, -b, -g, \ d)$
τ	$(a, \ b, \ c, \ d, -e, -f, -g, -h)$
$\sigma\tau$	$(a, \ f, -c, -h, -e, \ b, \ g, -d)$
$\sigma^2\tau$	$(a, -b, \ c, -d, -e, \ f, -g, \ h)$
$\sigma^3\tau$	$(a, -f, -c, \ h, -e, -b, \ g, \ d)$

Welche Untergruppen hat die Diedergruppe D_4? Außer der trivialen Gruppe und D_4 selbst kann es noch Untergruppen der Ordnung 2 und 4 geben. Eine Untergruppe der Ordnung 2 besteht aus id und einem Element der Ordnung 2; es gibt also die fünf Untergruppen

$$\langle\sigma^2\rangle, \quad \langle\tau\rangle, \quad \langle\sigma\tau\rangle, \quad \langle\sigma^2\tau\rangle, \quad \langle\sigma^3\tau\rangle\,.$$

Untergruppen der Ordnung 4 sind entweder zyklisch, also von einem Element der Ordnung 4 erzeugt — das liefert eine Untergruppe $\langle\sigma\rangle$ — oder von zwei miteinander kommutierenden Elementen der Ordnung 2 erzeugt. Das liefert noch zwei Untergruppen

$$\langle\sigma^2, \tau\rangle \qquad \text{und} \qquad \langle\sigma^2, \sigma\tau\rangle\,.$$

Wir bestimmen jetzt die zugehörigen Zwischenkörper.

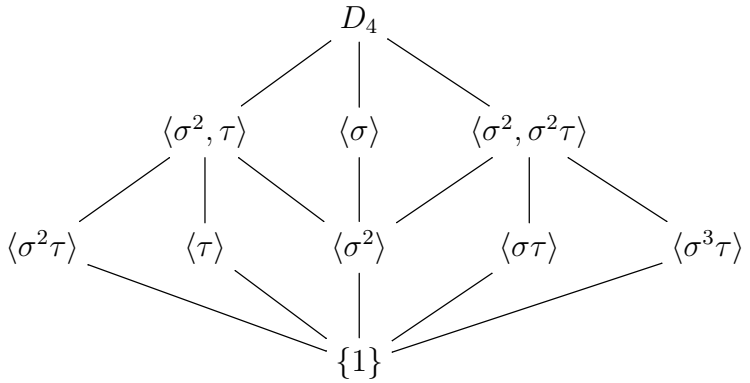
- $\mathcal{F}(\{\mathrm{id}\}) = K$,
  denn alle Elemente sind Fixpunkte der Identität.
- $\mathcal{F}(\langle\sigma^2\rangle) = \mathbb{Q}(\sqrt{17}, \boldsymbol{i})$,
  denn aus der obigen Tabelle findet man für $x \in K$ in der Basisdarstellung: $\sigma^2(x) = x \iff b = d = f = h = 0$.
- $\mathcal{F}(\langle\tau\rangle) = \mathbb{Q}(\sqrt[4]{17})$.
  Hier muss $e = f = g = h = 0$ sein.
- $\mathcal{F}(\langle\sigma\tau\rangle) = \mathbb{Q}((1+\boldsymbol{i})\sqrt[4]{17})$.
  Hier gilt $c = e = 0$, $b = f$, $d = -h$; die Elemente haben die Form

$$a + b(1+\boldsymbol{i})\alpha + g\boldsymbol{i}\alpha^2 + d(1-\boldsymbol{i})\alpha^3 = a + b(1+\boldsymbol{i})\alpha + \frac{g}{2}\big((1+\boldsymbol{i})\alpha\big)^2 - \frac{d}{2}\big((1+\boldsymbol{i})\alpha\big)^3.$$

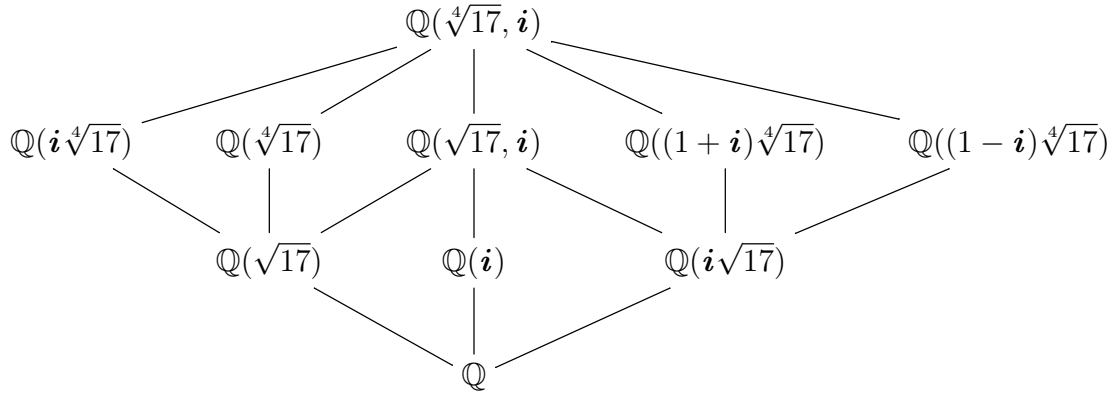
- $\mathcal{F}(\langle\sigma^2\tau\rangle) = \mathbb{Q}(\boldsymbol{i}\sqrt[4]{17})$.
  Es gilt $b = d = e = g = 0$; die verbleibenden Terme sind Potenzen von $\boldsymbol{i}\alpha$.
- $\mathcal{F}(\langle\sigma^3\tau\rangle) = \mathbb{Q}((1-\boldsymbol{i})\sqrt[4]{17})$.
  Das ist analog zu $\langle\sigma\tau\rangle$.
- $\mathcal{F}(\langle\sigma\rangle) = \mathbb{Q}(\boldsymbol{i})$,
  denn $\sigma(x) = x \iff b = c = d = f = g = h = 0$.
- $\mathcal{F}(\langle\sigma^2, \tau\rangle) = \mathbb{Q}(\sqrt{17})$.
  Fixpunkt von σ^2 und τ zu sein bedeutet $b = d = e = f = g = h = 0$, also haben die Elemente die Form $a + c\alpha^2 = a + c\sqrt{17}$.

- $\mathcal{F}(\langle\sigma^2, \sigma\tau\rangle) = \mathbb{Q}(\boldsymbol{i}\sqrt{17})$.
  Ähnlich wie eben findet man die Bedingung $b = c = d = e = f = h = 0$; die Elemente haben die Form $a + g\boldsymbol{i}\alpha^2 = a + g\boldsymbol{i}\sqrt{17}$.
- $\mathcal{F}(D_4) = \mathbb{Q}$.
  Wenn ein Element sowohl unter σ als auch unter τ fest bleibt, folgt $b = c = d = e = f = g = h = 0$.

Da offenbar zu einer größeren Untergruppe ein kleinerer Fixkörper gehört, wird aus dem „Untergruppenverband“



durch Spiegelung an einer horizontalen Achse ein „Zwischenkörperverband“:



Wir werden später sehen, dass das tatsächlich *alle* Zwischenkörper sind.

2. Wiederholung: Separable Körpererweiterungen

Eine wichtige Eigenschaft der Galois-Erweiterungen (die wir in dieser Vorlesung genauer studieren wollen) ist, dass sie *separabel* sind. Endliche separable Körpererweiterungen haben außerdem die schöne Eigenschaft, dass sie einfach sind. In diesem Abschnitt wiederholen wir die relevanten Begriffe und Resultate (vgl. §13 im Skript „Einführung in die Algebra“ vom Sommersemester 2013, wo Sie auch alle Beweise finden).

2.1. **Definition.** Seien K ein Körper und $0 \neq f \in K[X]$ ein Polynom. f heißt *separabel*, wenn für jeden irreduziblen normierten Teiler h von f gilt, dass h in einem Zerfällungskörper von h (oder f) nur einfache Nullstellen hat. ♢

DEF separables Polynom

Häufig wird einfach gefordert, dass f selbst in seinem Zerfällungskörper nur einfache Nullstellen hat, was eine stärkere Einschränkung ist. Für irreduzible Polynome stimmen beide Versionen überein, und wir werden den Begriff „separabel“ fast ausschließlich im Zusammenhang mit irreduziblen Polynomen verwenden. In diesem Fall können wir Separabilität auf einfache Weise charakterisieren.

2.2. **Lemma.** *Seien K ein Körper und $f \in K[X]$ irreduzibel. Dann ist f genau dann separabel, wenn die Ableitung $f' \neq 0$ ist.*

LEMMA Kriterium für separabel

2.3. **Folgerung.** *Ist K ein Körper der Charakteristik 0, dann ist jedes irreduzible Polynom über K separabel.*

FOLG Char. 0

Beweis. In Charakteristik 0 gilt für f nicht konstant, dass $\deg(f') = \deg(f) - 1$ ist; es folgt $f' \neq 0$, also ist f nach Lemma 2.2 separabel. ❑

2.4. **Beispiel.** Nicht separable (irreduzible) Polynome sind also nicht so einfach zu finden. Das Standardbeispiel sieht so aus: Sei $K = \mathbb{F}_p(y)$ der Quotientenkörper des Polynomrings $\mathbb{F}_p[y]$ und sei $f = X^p - y \in K[X]$. Nach dem Eisenstein-Kriterium (mit dem Primelement $y \in \mathbb{F}_p[y]$) ist f irreduzibel. Auf der anderen Seite ist $f' = pX^{p-1} = 0$, da K Charakteristik p hat. Also ist f nicht separabel. Sei L ein Zerfällungskörper von f über K und sei $\alpha \in L$ eine Nullstelle von f. Dann ist $\alpha^p = y$ und es gilt

$$(X - \alpha)^p = X^p - \alpha^p = X^p - y = f\,,$$

also hat f die p-fache Nullstelle α in L. ♣

BSP nicht separabel

Wir erweitern den Begriff „separabel“ auf Elemente und Körpererweiterungen.

2.5. **Definition.** Sei $k \subset K$ eine Körpererweiterung. Ein Element $a \in K$ heißt *separabel über k*, wenn es algebraisch über k ist und sein Minimalpolynom über k separabel ist. Die Körpererweiterung $k \subset K$ heißt *separabel*, wenn jedes Element $a \in K$ separabel über k ist. Anderenfalls heißt sie *inseparabel*. ♢

DEF separable Körpererweiterung

LEMMA Charakterisierung separabler Erweiterungen

2.6. **Lemma.** *Sei $k \subset K$ eine Körpererweiterung und $a \in K$ algebraisch über k.*

(1) *Ist* $\mathrm{char}(k) = 0$*, dann ist a separabel über k.*

(2) *Ist* $\mathrm{char}(k) = p > 0$*, dann ist a genau dann separabel über k, wenn $k(a^p) = k(a)$ ist.*

(3) *a ist separabel über k genau dann, wenn die Körpererweiterung $k \subset k(a)$ separabel ist.*

Körper mit der Eigenschaft, dass jede algebraische Erweiterung separabel ist, haben einen besonderen Namen.

DEF vollkommen perfekt

2.7. **Definition.** Ein Körper K heißt *vollkommen* oder *perfekt*, wenn jedes irreduzible Polynom in $K[X]$ separabel ist. Dann ist auch jede algebraische Körpererweiterung von K separabel. ♢

SATZ Satz von Steinitz

2.8. **Satz.** *Sei K ein Körper.*

(1) *Gilt* $\mathrm{char}(K) = 0$*, dann ist K vollkommen.*

(2) *Gilt* $\mathrm{char}(K) = p > 0$*, dann ist K genau dann vollkommen, wenn $\{a^p \mid a \in K\} = K$ gilt, wenn also der Frobenius-Endomorphismus $\phi\colon K \to K$, $a \mapsto a^p$, surjektiv ist.*

(3) *Ist K endlich, dann ist K vollkommen.*

BSP unvollkommener Körper

2.9. **Beispiel.** Ein unvollkommener Körper ist also nicht so leicht zu finden. Wie Beispiel 2.4 zeigt, ist $\mathbb{F}_p(y)$ ein solcher. In jedem Fall muss es ein unendlicher Körper von Primzahlcharakteristik sein. ♣

Wir kommen zum Satz vom primitiven Element. Wir behandeln den wesentlichen Schritt als Lemma vorneweg.

LEMMA $k(a,b) = k(c)$

2.10. **Lemma.** *Sei $k \subset K$ eine Körpererweiterung und seien $a, b \in K$ algebraisch über k mit b separabel über k. Dann gibt es $c \in k(a,b)$ mit $k(c) = k(a,b)$.*

Beweis. $k(a,b)$ ist eine endliche Erweiterung von k. Ist k ein endlicher Körper, dann ist auch $k(a,b)$ endlich. Dann ist die Erweiterung $k \subset k(a,b)$ einfach. Wir können ab jetzt also annehmen, dass k unendlich ist.

Seien f das Minimalpolynom von a und g das Minimalpolynom von b über k und sei $k(a,b) \subset L$ ein Zerfällungskörper von fg über k. Wir bezeichnen die verschiedenen Nullstellen von f in L mit $a = a_1, a_2, \ldots, a_m$ und die verschiedenen Nullstellen von g in L mit $b = b_1, b_2, \ldots, b_n$. Die Menge der $\lambda \in k$, für die es ein Paar $(i,j) \neq (1,1)$ gibt mit

$$a + \lambda b = a_i + \lambda b_j$$

ist endlich (jedes Paar (i,j) schließt höchstens ein λ aus). Da k unendlich ist, gibt es also ein $\lambda \in k$ mit $c := a + \lambda b \neq a_i + \lambda b_j$ für alle $(i,j) \neq (1,1)$. Wir wollen jetzt $k(c) = k(a,b)$ zeigen. Die Inklusion „$\subset$“ ist klar; es bleibt also $a, b \in k(c)$ zu zeigen. Wir zeigen $b \in k(c)$, dann folgt $a = c - \lambda b \in k(c)$. Dazu betrachten wir $h = \mathrm{ggT}(g, f(c - \lambda X))$ in $k(c)[X]$. Da b eine gemeinsame Nullstelle von g und $f(c - \lambda X)$ ist, muss $X - b$ ein Teiler von h sein (in $k(a,b)[X]$). Wäre b_j mit $j > 1$ eine Nullstelle von h, dann wäre b_j auch eine Nullstelle von $f(c - \lambda X)$, also wäre $c - \lambda b_j = a_i$ für ein $1 \leq i \leq m$, im Widerspruch zur Wahl von λ. Da h ein

Teiler von g sein muss und da g nur einfache Nullstellen hat (denn b ist separabel über k — hier wird diese wichtige Voraussetzung verwendet!), folgt $h = X - b$. Da der ggT aber durch den Euklidischen Algorithmus in $k(c)[X]$ berechnet werden kann, folgt $b \in k(c)$. ❑

2.11. **Beispiel.** Wir betrachten unser Standardbeispiel $\mathbb{Q} \subset K = \mathbb{Q}(\sqrt[4]{17}, \boldsymbol{i})$, den Zerfällungskörper von $X^4 - 17$ über $\mathbb{Q}$. Mit $\lambda = 1$ sehen wir, dass alle Elemente $\boldsymbol{i}^m \sqrt[4]{17} \pm \boldsymbol{i}$ (mit $0 \leq m \leq 3$) paarweise verschieden sind. Da wir uns in Charakteristik 0 befinden, sind alle Elemente separabel. Es folgt $K = \mathbb{Q}(\sqrt[4]{17} + \boldsymbol{i})$. ♣

BSP primitives Element

2.12. **Satz.** *Sei $k \subset K$ eine Körpererweiterung und seien $a, b_1, \ldots, b_n \in K$ algebraisch über k mit $b_1, \ldots, b_n$ separabel über k. Dann gibt es $c \in k(a, b_1, \ldots, b_n)$ mit $k(c) = k(a, b_1, \ldots, b_n)$.*

Insbesondere ist jede endliche separable Körpererweiterung $k \subset K$ einfach, hat also ein primitives Element c (mit $K = k(c)$).

SATZ Satz vom primitiven Element

Beweis. Wir beweisen die Aussage durch Induktion nach n. Für $n = 0$ gilt die Behauptung trivialerweise mit $c = a$. Sei also $n \geq 1$. Nach Induktionsvoraussetzung gibt es $c' \in k(a, b_1, \ldots, b_{n-1})$ mit $k(a, b_1, \ldots, b_{n-1}) = k(c')$; insbesondere ist c' algebraisch über k. Dann haben wir

$$k(a, b_1, \ldots, b_{n-1}, b_n) = k(a, b_1, \ldots, b_{n-1})(b_n) = k(c')(b_n) = k(c', b_n)\,.$$

Nach Lemma 2.10 gibt es $c \in k(c', b_n)$ mit $k(c', b_n) = k(c)$.

Ist $k \subset K$ endlich und separabel, dann wird K von endlich vielen separablen Elementen über k erzeugt; damit ist der erste Teil des Satzes anwendbar. ❑

Wie Algebraizität ist auch Separabilität transitiv:

2.13. **Satz.** *Sei $k \subset K$ eine Körpererweiterung.*

(1) *Sind $a, b \in K$, sodass a separabel ist über k und b separabel ist über $k(a)$, dann ist b auch separabel über k.*

(2) *Ist $K \subset L$ eine weitere Körpererweiterung, dann ist $k \subset L$ genau dann separabel, wenn die Erweiterungen $k \subset K$ und $K \subset L$ beide separabel sind.*

SATZ Transitivität der Separabilität

(Hier endet die „Wiederholung“; die folgenden Resultate wurden nicht in der „Einführung in die Algebra“ besprochen.)

Endliche separable Körpererweiterungen haben auch gute Eigenschaften hinsichtlich der Existenz von Körperhomomorphismen.

2.14. **Satz.** *Sei $k \subset K$ eine endliche separable Körpererweiterung und sei $K \subset L$ eine weitere Körpererweiterung. Dann gibt es höchstens $[K : k]$ Körperhomomorphismen $K \to L$, die auf k die Identität induzieren. Für geeignete („hinreichend große“) Körpererweiterungen L (z.B. wenn L algebraisch abgeschlossen ist) gibt es genau $[K : k]$ solcher Homomorphismen.*

SATZ

Beweis. Nach dem Satz vom primitiven Element 2.12 gibt es ein Element $\alpha \in K$, sodass $K = k(\alpha)$. Sei f das Minimalpolynom von α über k; dann haben wir $\deg(f) = [K : k]$; wir bezeichnen diese Zahl mit n. Wir hatten bereits gesehen, dass jeder „k-Homomorphismus“ $\phi\colon K \to L$ das primitive Element α auf eine Nullstelle von f in L abbilden muss; außerdem ist ϕ durch $\phi(\alpha)$ eindeutig bestimmt. Es folgt, dass es höchstens so viele Möglichkeiten für ϕ gibt, wie f Nullstellen in L hat, und das sind höchstens n.

Nun nehmen wir an, dass L einen Zerfällungskörper von f über k enthält. Da $k \subset K$ separabel ist, ist α separabel, was bedeutet, dass f in L nur einfache Nullstellen hat. Da f in $L[x]$ nach Annahme in Linearfaktoren zerfällt, hat f in L *genau* n Nullstellen. Wie im Beweis von Lemma 1.6 gibt es zu jeder dieser Nullstellen einen eindeutig bestimmten k-Homomorphismus $\phi\colon K \to L$. ❑

Wir beweisen noch ein allgemeines Lemma. Die erste Aussage hatten wir bereits am Beispiel $\mathbb{Q} \subset \mathbb{Q}(\sqrt[4]{17}, \boldsymbol{i})$ gesehen.

2.15. **Lemma.** *Sei K ein Körper und sei $G \subset \mathrm{Aut}(K)$ eine endliche Untergruppe der Automorphismengruppe von K. Dann operiert G auf K.*

LEMMA
Fixkörper einer Untergruppe von $\mathrm{Aut}(K)$

(1) $$k = \mathcal{F}(G) = \{a \in K \mid \gamma(a) = a \text{ für alle } \gamma \in G\}$$
ist ein Teilkörper von K.

(2) *Sei $\alpha \in K$ und seien $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_m$ die verschiedenen Elemente der Bahn von α unter G. Dann ist*
$$f = (x - \alpha_1)(x - \alpha_2)\cdots(x - \alpha_m) \in k[x]$$
ein normiertes irreduzibles Polynom. Insbesondere ist α algebraisch über k mit Minimalpolynom f.

(3) *$k \subset K$ ist separabel und $[K : k] = \#G$.*

2.16. **Definition.** $\mathcal{F}(G)$ heißt der *Fixkörper* von G. ♢

DEF
Fixkörper

Die Schreibweise variiert in der Literatur.

Beweis.

(1) Es ist zu zeigen, dass k unter Addition, Negation, Multiplikation und Kehrwertbildung abgeschlossen ist und 0 und 1 enthält. Das folgt daraus, dass alle $\gamma \in G$ Körperautomorphismen sind.

(2) Es ist zunächst zu zeigen, dass f Koeffizienten in k hat. Wir können die Automorphismen von K zu Automorphismen des Polynomrings $K[x]$ fortsetzen, indem wir sie auf die Koeffizienten der Polynome anwenden. Für $\gamma \in G$ gilt dann $\gamma(f) = f$, denn γ permutiert die Elemente der Bahn von α und damit die Faktoren in der Produktdarstellung von f. Das bedeutet, dass alle Koeffizienten Fixpunkte der Operation von G sind; nach Definition des Fixkörpers sind sie also in $k = \mathcal{F}(G)$. Dass f normiert ist, ist klar. Als Nullstelle eines normierten Polynoms in $k[x]$ ist α dann algebraisch über k. Es bleibt zu zeigen, dass f irreduzibel ist. Das liegt daran, dass G auf der Bahn von α (wie auf jeder Bahn) transitiv operiert: Haben wir eine Faktorisierung $f = f_1 f_2$ in $k[x]$, wobei wir annehmen können, dass $f_1(\alpha) = 0$ ist, dann muss jeder Automorphismus von K α auf eine Nullstelle von f_1 abbilden. Also hat f_1 schon alle Elemente der Bahn von α

als Nullstellen; damit muss f_2 konstant sein. Da $f \in k[x]$ irreduzibel und normiert ist und α als Nullstelle hat, muss f das Minimalpolynom von α über k sein.

(3) Sei $\alpha \in K$ und f wie in Teil (2) das Minimalpolynom von α über k. Da f offensichtlich über K in Linearfaktoren zerfällt, hat f nur einfache Nullstellen, also ist α separabel über k. Da $\alpha \in K$ beliebig war, folgt, dass die Körpererweiterung $k \subset K$ separabel ist. Wir zeigen, dass die Körpererweiterung auch endlich ist: Nach Teil (2) gilt für jedes $\alpha \in K$

$$[k(\alpha) : k] = \deg(f) = \#(G \cdot \alpha) \leq \#G\,.$$

Nach dem Satz vom primitiven Element 2.12 folgt, dass jeder Zwischenkörper $k \subset L \subset K$, der über k endlich ist, Grad $\leq \#G$ hat. Sei L ein Zwischenkörper mit $[L : k]$ endlich und maximal. Gäbe es $\beta \in K \setminus L$, dann wäre $L \subsetneq L(\beta) \subset K$ und damit $[L : k] < [L(\beta) : k] < \infty$, im Widerspruch zur Wahl von L. Es folgt $K = L$, also ist $k \subset K$ endlich, und $[K : k] \leq \#G$. Auf der anderen Seite gilt nach Satz 2.14 $\#G \leq [K : k]$, also muss Gleichheit gelten. ❑

2.17. **Folgerung.** *Sei $k \subset K$ eine endliche separable Körpererweiterung. Dann gilt $\#\operatorname{Aut}(K/k) \leq [K : k]$ mit Gleichheit genau dann, wenn jedes normierte irreduzible Polynom $f \in k[x]$, das in K eine Nullstelle hat, in $K[x]$ bereits in Linearfaktoren zerfällt.*

FOLG $\#\operatorname{Aut}(K/k) \leq [K : k]$

Beweis. Die Aussage „$\#\operatorname{Aut}(K/k) \leq [K : k]$“ ist als Spezialfall $L = K$ in Satz 2.14 enthalten. Hat K die angegebene Eigenschaft, dann ist im Beweis von Satz 2.14 $L = K$ ein Zerfällungskörper von f, und es folgt Gleichheit. Jetzt nehmen wir umgekehrt an, dass $\#\operatorname{Aut}(K/k) = [K : k]$ gilt. Dann ist $k = \mathcal{F}(\operatorname{Aut}(K/k))$, denn

$$k \subset \mathcal{F}(\operatorname{Aut}(K/k)) \qquad \text{und} \qquad [K : k] = \#\operatorname{Aut}(K/k) = [K : \mathcal{F}(\operatorname{Aut}(K/k))]$$

nach Lemma 2.15, (3). Sei $f \in k[x]$ normiert und irreduzibel und $\beta \in K$ mit $f(\beta) = 0$. Wir betrachten die Bahn $\{\phi(\beta) \mid \phi \in \operatorname{Aut}(K/k)\}$ von β unter der Automorphismengruppe von $k \subset K$; ihre Elemente seien $\beta = \beta_1, \beta_2, \ldots, \beta_m$. Nach Lemma 2.15 ist dann $\tilde{f} = \prod_{j=1}^{m}(x - \beta_j) \in k[x]$ das Minimalpolynom von β, also ist $f = \tilde{f}$, und f zerfällt in $K[x]$ in Linearfaktoren. ❑

2.18. **Definition.** Eine Körpererweiterung $k \subset K$ mit der Eigenschaft, dass jedes normierte irreduzible Polynom $f \in k[x]$, das in K eine Nullstelle hat, in $K[x]$ in Linearfaktoren zerfällt, heißt *normal*. ♢

DEF normale KE

(Das ist eine ziemlich dämliche Bezeichnung, weil „normal“ alles Mögliche heißen kann, aber sie hat sich nun einmal durchgesetzt.)

2.19. **Beispiele.** Sei $k \subset K$ eine Körpererweiterung vom Grad $[K : k] = 2$. Dann ist $k \subset K$ normal. Denn sei $f \in k[x]$ ein normiertes irreduzibles Polynom, das in K eine Nullstelle α hat. Dann folgt $\deg(f) \leq 2$. Jedes Polynom vom Grad 1 „zerfällt“ trivialerweise in Linearfaktoren. Wir können demnach $\deg(f) = 2$ annehmen, also $f = x^2 + ax + b$ mit $a, b \in K$. Dann ist aber $f = (x - \alpha)(x + a + \alpha)$ in $K[x]$; damit zerfällt f in $K[x]$ in Linearfaktoren.

BSP (nicht) normale KE

Eine Körpererweiterung vom Grad 3 braucht dagegen nicht normal zu sein. Zum Beispiel hat $f = x^3 - 2$ in $K = \mathbb{Q}(\sqrt[3]{2})$ eine Nullstelle, zerfällt aber über K nicht in Linearfaktoren, da die anderen beiden Nullstellen nicht in K liegen. Also ist $\mathbb{Q} \subset K$ nicht normal.

Ist K algebraisch abgeschlossen, dann ist $k \subset K$ normal, weil *jedes* Polynom in $K[x]$ in Linearfaktoren zerfällt. ♣

2.20. **Beispiel.** Im Gegensatz zu Algebraizität und Separabilität ist Normalität *nicht* transitiv. Zum Beispiel ist $\mathbb{Q} \subset \mathbb{Q}(\sqrt[4]{17})$ nicht normal, denn $L = \mathbb{Q}(\sqrt[4]{17})$ enthält nur zwei der vier Nullstellen von $x^4 - 17$. Auf der anderen Seite sind aber die beiden Körpererweiterungen $\mathbb{Q} \subset \mathbb{Q}(\sqrt{17})$ und $\mathbb{Q}(\sqrt{17}) \subset \mathbb{Q}(\sqrt[4]{17})$ normal, da sie Grad 2 haben. ♣

BSP Normalität nicht transitiv

3. Galois-Erweiterungen

DEF Galois-Erweiterung

Galoisgruppe

3.1. **Definition.** Eine Körpererweiterung $k \subset K$ heißt *galoissch* oder *Galois-Erweiterung*, wenn $k = \mathcal{F}(\mathrm{Aut}(K/k))$ ist. In diesem Fall heißt $\mathrm{Aut}(K/k)$ die *Galoisgruppe* der Körpererweiterung $k \subset K$; sie wird häufig $\mathrm{Gal}(K/k)$ geschrieben. ♢

Beachte: $k \subset \mathcal{F}(\mathrm{Aut}(K/k))$ gilt immer nach Definition von $\mathrm{Aut}(K/k)$. Die Bedingung ist also, dass jedes unter $\mathrm{Aut}(K/k)$ festgehaltene Element von K bereits in k liegt.

Man beachte auch die zwei „s“ in „galoissch“!

BSP keine Galois-Erweiterung

3.2. **Beispiel.** Die Körpererweiterung $\mathbb{Q} \subset K = \mathbb{Q}(\sqrt[3]{17})$ ist nicht galoissch, denn K hat keine nichttrivialen Automorphismen (jeder Automorphismus muss $\sqrt[3]{17}$ auf eine Nullstelle von $X^3 - 17$ abbilden; in K gibt es aber keine andere Nullstelle); damit ist $\mathcal{F}(\mathrm{Aut}(K/\mathbb{Q})) = K \neq \mathbb{Q}$. ♣

Wir können endliche Galois-Erweiterungen charakterisieren:

SATZ Galois-Erweiterungen

3.3. **Satz.** *Sei $k \subset K$ eine endliche Körpererweiterung. Dann sind die folgenden Aussagen äquivalent:*

(1) *$k \subset K$ ist galoissch.*

(2) *$k \subset K$ ist separabel und normal.*

(3) *$\#\,\mathrm{Aut}(K/k) = [K : k]$.*

(4) *K ist Zerfällungskörper eines normierten separablen irreduziblen Polynoms $f \in k[x]$.*

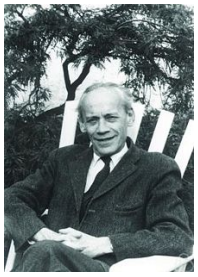
Beweis. „(1) $\Rightarrow$ (3)“: Wir wenden Lemma 2.15 an auf $G = \mathrm{Aut}(K/k)$. Nach Voraussetzung ist $k = \mathcal{F}(G)$, also ist $[K : k] = \#G$ (und $k \subset K$ ist separabel).

„(3) $\Rightarrow$ (1)“: Sei wieder $G = \mathrm{Aut}(K/k)$; es gelte $[K : k] = \#G$. Dann haben wir $k \subset \mathcal{F}(G) \subset K$ und nach Lemma 2.15 gilt $[K : \mathcal{F}(G)] = \#G = [K : k]$. Daraus folgt $k = \mathcal{F}(G)$.

„(1) $\Rightarrow$ (2)“: Wir haben schon gesehen, dass aus (1) die Separabilität folgt. Außerdem folgt (3); nach Folgerung 2.17 bedeutet die Gleichheit $[K : k] = \#\,\mathrm{Aut}(K/k)$ gerade, dass $k \subset K$ normal ist.

„(2) $\Rightarrow$ (4)“: Da $k \subset K$ endlich und separabel ist, gibt es nach dem Satz vom primitiven Element 2.12 ein $\alpha \in K$ mit $K = k(\alpha)$. Sei f das Minimalpolynom von α über k. Da $k \subset K$ normal ist und f die Nullstelle α in K hat, zerfällt f in $K[x]$ in Linearfaktoren. Damit ist K ein Zerfällungskörper von f; f ist separabel, da α separabel über k ist (denn $k \subset K$ ist separabel).

„(4) $\Rightarrow$ (3)“: Das folgt aus dem Beweis von Satz 2.14. ❑



E. Artin
(1898–1962)

Da Normalität nicht transitiv in Körpererweiterungen ist, gilt das analog für die Eigenschaft galoissch zu sein (wie dasselbe Beispiel zeigt).

Die Äquivalenz von (1) und (2) gilt auch noch für unendliche algebraische Körpererweiterungen (Satz von Artin, siehe z.B. [KM, Satz 26.7]).

BSP quadratische Erweiterung

3.4. **Beispiel.** Ist $\operatorname{char}(k) \neq 2$ und $k \subset K$ eine quadratische Körpererweiterung (also mit $[K : k] = 2$), dann ist $k \subset K$ galoissch, denn eine quadratische Erweiterung ist stets normal, und sie kann nur dann inseparabel sein, wenn die Charakteristik den Grad teilt. Es gilt dann $\operatorname{Aut}(K/k) = \{\mathrm{id}_K, \tau\}$ für einen Automorphismus $\tau \neq \mathrm{id}_K$. Wegen $\operatorname{char}(k) \neq 2$ können wir die übliche quadratische Ergänzung durchführen. Das zeigt, dass $K = k(\sqrt{a})$ ist für ein $a \in k$ (sodass a kein Quadrat in k ist). Das Minimalpolynom von $\sqrt{a}$ ist $x^2 - a$ und hat $-\sqrt{a}$ als einzige weitere Nullstelle, also muss $\tau(\sqrt{a}) = -\sqrt{a}$ sein.

Als konkretes Beispiel haben wir $\mathbb{R} \subset \mathbb{C} = \mathbb{R}(i)$; in diesem Fall ist τ die komplexe Konjugation: $\tau(a + bi) = a - bi$. ♣

BSP $\mathbb{Q}(\sqrt[4]{17}, \mathbf{i})$

3.5. **Beispiel.** Zu Beginn dieser Vorlesung haben wir ausführlich die Körpererweiterung $\mathbb{Q} \subset K = \mathbb{Q}(\sqrt[4]{17}, \boldsymbol{i})$ studiert. Da K der Zerfällungskörper von $x^4 - 17$ ist, ist diese Körpererweiterung galoissch; wir hatten gesehen, dass die Galoisgruppe $\operatorname{Aut}(K/\mathbb{Q}) \cong D_4$ ist.

Demgegenüber ist $\mathbb{Q} \subset \mathbb{Q}(\sqrt[4]{17})$ nicht galoissch, denn die Erweiterung ist nicht normal. Daran sieht man, dass Zwischenkörper einer Galois-Erweiterung nicht galoissch über dem Grundkörper sein müssen. ♣

BSP endliche Körper

3.6. **Beispiel.** Ist $k \subset K$ eine Erweiterung von *endlichen* Körpern, so ist sie galoissch.

Sei $q = \#k$ (dann ist $q = p^f$ eine Primzahlpotenz und p ist die Charakteristik von k), dann ist $\phi\colon K \to K, x \mapsto x^q$ ein Automorphismus von K, der die Elemente von k (und nur diese, denn die Fixpunkte sind genau die q Nullstellen von $x^q - x$) fest lässt, also ist $\phi \in \operatorname{Aut}(K/k)$, und es gilt $\mathcal{F}(\operatorname{Aut}(K/k)) \subset \mathcal{F}(\langle\phi\rangle) = k$. Damit ist $k \subset K$ jedenfalls galoissch und es folgt zusätzlich, dass $\operatorname{Aut}(K/k) = \langle\phi\rangle$ ist, denn

$$\#\operatorname{Aut}(K/k) = [K : k] = [K : \mathcal{F}(\langle\phi\rangle)] = \#\langle\phi\rangle\,.$$

Die Galoisgruppe $\operatorname{Aut}(K/k)$ ist also zyklisch und wird von ϕ erzeugt. ♣

BSP $\mathbb{R}$ ist keine Galois-Erweiterung

3.7. **Beispiel.** Die Automorphismengruppe von $\mathbb{R}$ ist trivial: $\operatorname{Aut}(\mathbb{R}) = \{\mathrm{id}_{\mathbb{R}}\}$. Sei dazu $\sigma \in \operatorname{Aut}(\mathbb{R})$. Dann gilt für $x \in \mathbb{R}$:

$$x \geq 0 \iff \exists y \in \mathbb{R}\colon x = y^2 \iff \exists z \in \mathbb{R}\colon \sigma(x) = z^2 \iff \sigma(x) \geq 0\,.$$

Damit folgt auch für $x, y \in \mathbb{R}$:

$$x \geq y \iff x - y \geq 0 \iff \sigma(x - y) \geq 0 \iff \sigma(x) \geq \sigma(y)\,;$$

σ erhält also die Anordnung von $\mathbb{R}$. Als Körperautomorphismus ist σ die Identität auf dem Primkörper $\mathbb{Q} \subset \mathbb{R}$. Da eine reelle Zahl x durch $L(x) = \{a \in \mathbb{Q} \mid a \leq x\}$ eindeutig bestimmt ist (als $x = \sup L(x)$), und weil $\sigma(L(x)) = L(x)$ gilt, folgt

$$\sigma(x) = \sigma(\sup L(x)) = \sup \sigma(L(x)) = \sup L(x) = x\,.$$

Als Konsequenz ergibt sich, dass es *keine* Galois-Erweiterung $k \subset \mathbb{R}$ mit $k \neq \mathbb{R}$ geben kann. ♣

LEMMA Zerfällungskörper sind galoissch

3.8. **Lemma.** *Ist K der Zerfällungskörper über k eines (nicht notwendig irreduziblen) normierten separablen Polynoms $f \in k[x]$, dann ist $k \subset K$ galoissch.*

Beweis. Seien $f_1, f_2, \ldots, f_m$ die verschiedenen normierten irreduziblen Faktoren von f. Da f separabel ist, sind auch alle f_j separabel. Dann können wir statt f auch $f_0 = f_1 f_2 \cdots f_m$ betrachten; f_0 hat nur einfache Nullstellen in K. Wir zeigen, dass $\#\operatorname{Aut}(K/k) = [K : k]$ ist. Sei dazu $k \subset L \subset K$ ein Zwischenkörper. Wir schreiben $\operatorname{Hom}_k(L, K)$ für die Menge der Homomorphismen $L \to K$, die auf k die Identität induzieren. Wir nehmen als Induktionsvoraussetzung an, dass

$$\#\operatorname{Hom}_k(L, K) = [L : k]$$

ist (das ist im Induktionsanfang mit $L = k$ erfüllt). Ist $L = K$, dann sind wir fertig, denn $\operatorname{Hom}_k(K, K) = \operatorname{Aut}(K/k)$. Anderenfalls gibt es eine Nullstelle $\alpha \in K$ von f_0 mit $\alpha \notin L$. Sei $L' = L(\alpha) \subset K$, dann ist $L \subset L'$ eine nichttriviale einfache Körpererweiterung. Sei f_α das Minimalpolynom von α über L; dann hat f_α genau $\deg f_\alpha = [L' : L]$ verschiedene Nullstellen in K, und dasselbe gilt für f_α^ϕ für jeden Homomorphismus $\phi \in \operatorname{Hom}_k(L, K)$ (denn f_α und f_α^ϕ sind Teiler von f_0 in $K[x]$). Nach Lemma 1.8 lässt sich jedes $\phi \in \operatorname{Hom}_k(L, K)$ also auf genau $[L' : L]$ verschiedene Arten zu einem Homomorphismus $L' \to K$ fortsetzen. Insgesamt erhalten wir dann

$$\#\operatorname{Hom}_k(L', K) = [L' : L] \cdot \#\operatorname{Hom}_k(L, K) = [L' : L] \cdot [L : k] = [L' : k]$$

wie gewünscht. (Ähnlich hatten wir bereits im Beweis von Satz 1.9 argumentiert.) Aus $\#\operatorname{Aut}(K/k) = [K : k]$ folgt mit Satz 3.3, dass $k \subset K$ galoissch ist. ❑

Wir betrachten jetzt eine Galois-Erweiterung $k \subset K$ mit einem Zwischenkörper L. Wann sind die beiden Körpererweiterungen $k \subset L$ und $L \subset K$ wieder galoissch?

SATZ galoissch für Zwischenkörper

3.9. **Satz.** *Sei $k \subset K$ eine endliche Galois-Erweiterung und sei $k \subset L \subset K$ ein Zwischenkörper. Dann ist $L \subset K$ galoissch. Die Erweiterung $k \subset L$ ist genau dann galoissch, wenn $\gamma(L) = L$ ist für alle $\gamma \in \operatorname{Aut}(K/k)$. In diesem Fall ist*

$$\Phi\colon \operatorname{Aut}(K/k) \longrightarrow \operatorname{Aut}(L/k), \quad \gamma \longmapsto \gamma|_L$$

ein surjektiver Gruppenhomomorphismus mit Kern $\operatorname{Aut}(K/L)$*. Insbesondere ist* $\operatorname{Aut}(K/L)$ *ein Normalteiler von* $\operatorname{Aut}(K/k)$ *und* $\operatorname{Aut}(L/k)$ *ist isomorph zur Faktorgruppe* $\operatorname{Aut}(K/k)/\operatorname{Aut}(K/L)$*.*

Die letzte Aussage liefert eine Erklärung für die Bezeichnung „normal“ bei Körpererweiterungen.

Beweis. Wir zeigen erst einmal, dass $L \subset K$ galoissch ist. Nach Satz 3.3 ist K Zerfällungskörper über k eines normierten (sogar irreduziblen) separablen Polynoms $f \in k[x]$. Dann ist K auch Zerfällungskörper von f über L. Nach Lemma 3.8 ist also $L \subset K$ galoissch.

Da $k \subset K$ nach Satz 3.3 separabel ist, gilt das auch für $k \subset L$. Wiederum nach Satz 3.3 ist $k \subset L$ also genau dann galoissch, wenn $k \subset L$ normal ist. Wir zeigen, dass das äquivalent ist zu $\forall \gamma \in \operatorname{Aut}(K/k)\colon \gamma(L) = L$.

Sei jetzt zunächst $k \subset L$ als normal angenommen; sei $a \in L$ und $\gamma \in \operatorname{Aut}(L/k)$. Wir müssen zeigen, dass $\gamma(a) \in L$ ist. Sei dazu $f \in k[x]$ das Minimalpolynom von a, dann sind alle Nullstellen von f in K bereits in L (denn $k \subset L$ ist normal). Auf der anderen Seite muss $\gamma(a)$ aber eine Nullstelle von f sein, also ist $\gamma(a) \in L$.

Jetzt nehmen wir an, dass $\gamma(L) = L$ ist für alle $\gamma \in \mathrm{Aut}(K/k)$. Wir wollen zeigen, dass dann $k \subset L$ normal ist. Sei also $f \in k[x]$ irreduzibel und normiert und $a \in L$ eine Nullstelle von f. Da $k \subset K$ normal ist, zerfällt f in $K[x]$ in Linearfaktoren. Aus Lemma 2.15 folgt, dass $\mathrm{Aut}(K/k)$ auf den Nullstellen von f in K transitiv operiert. Da $\gamma(L) = L$ ist für alle $\gamma \in \mathrm{Aut}(K/k)$ und eine Nullstelle (nämlich a) in L ist, sind alle Nullstellen in L, also zerfällt f auch schon in $L[x]$ in Linearfaktoren. Wir sehen also, dass jedes irreduzible normierte Polynom $f \in k[x]$, das in L eine Nullstelle hat, in $L[x]$ in Linearfaktoren zerfällt. Damit ist $k \subset L$ normal.

Sei jetzt $k \subset L$ galoissch. Für $\gamma \in \mathrm{Aut}(K/k)$ folgt aus $\gamma(L) = L$, dass die Einschränkung $\gamma|_L \in \mathrm{Aut}(L/k)$ ist; die Abbildung Φ ist also wohldefiniert, und es ist klar, dass Φ ein Gruppenhomomorphismus ist. Die Definition von $\mathrm{Aut}(K/L)$ liefert $\ker(\Phi) = \mathrm{Aut}(K/L)$, also ist $\mathrm{Aut}(K/L)$ ein Normalteiler von $\mathrm{Aut}(K/k)$. Es bleibt die Surjektivität von Φ zu zeigen. Nach dem Homomorphiesatz für Gruppen ist das Bild von Φ isomorph zu $\mathrm{Aut}(K/k)/\mathrm{Aut}(K/L)$. Es gilt dann

$$[L:k] = \#\,\mathrm{Aut}(L/k) \geq \#\frac{\mathrm{Aut}(K/k)}{\mathrm{Aut}(K/L)} = \frac{\#\,\mathrm{Aut}(K/k)}{\#\,\mathrm{Aut}(K/L)} = \frac{[K:k]}{[K:L]} = [L:k]\,,$$

also folgt Gleichheit. Damit ist Φ surjektiv; die letzte Behauptung folgt dann auch. ❑

DEF Galois-Abschluss

3.10. **Definition.** Ist $k \subset K$ eine endliche separable Körpererweiterung, dann ist $K = k(\alpha)$ eine einfache Körpererweiterung nach dem Satz vom primitiven Element 2.12. Sei $f \in k[x]$ das Minimalpolynom von α über k. Sei L ein Zerfällungskörper von f über K. Dann ist L auch Zerfällungskörper von f über k, also ist $k \subset L$ eine Galois-Erweiterung. Auf der anderen Seite muss jede Galois-Erweiterung von k, die K enthält, einen Zerfällungskörper von f enthalten. Damit ist L (bis auf Isomorphie) die kleinste K enthaltende Galois-Erweiterung von k. Die Erweiterung $k \subset L$ heißt der *Galois-Abschluss* oder die *galoissche Hülle* von $k \subset K$. ♢

Wir kommen jetzt zu einem wichtigen Aspekt der Galoistheorie, nämlich zur Beschreibung aller Zwischenkörper durch die Untergruppen der Galoisgruppe. Sei $k \subset K$ galoissch. Wir erinnern uns an die Konstruktion des Fixkörpers einer Untergruppe der Automorphismengruppe:

$$\begin{aligned}\mathcal{F}\colon \{U \subset \mathrm{Aut}(K/k) \mid U \text{ Untergruppe}\} &\longrightarrow \{L \mid L \text{ Zwischenkörper von } k \subset K\}\\ U &\longmapsto \mathcal{F}(U) = \{a \in K \mid \forall \gamma \in U\colon \gamma(a) = a\}\end{aligned}$$

Es gibt auch eine Abbildung in der anderen Richtung, nämlich

$$\begin{aligned}\mathcal{U}\colon \{L \mid L \text{ Zwischenkörper von } k \subset K\} &\longrightarrow \{U \subset \mathrm{Aut}(K/k) \mid U \text{ Untergruppe}\}\\ L &\longmapsto \mathcal{U}(L) = \mathrm{Aut}(K/L)\,.\end{aligned}$$

Die wesentliche Aussage des nun folgenden Satzes ist, dass diese beiden Abbildungen zueinander invers sind.

SATZ Galois-Korrespondenz

3.11. **Satz.** *Sei $k \subset K$ eine endliche Galois-Erweiterung. Dann sind die oben definierten Abbildungen $\mathcal{F}$ und $\mathcal{U}$ inklusionsumkehrend und zueinander invers.*

Für einen Zwischenkörper L von $k \subset K$ gilt, dass $k \subset L$ genau dann galoissch ist, wenn $\mathcal{U}(L)$ Normalteiler in $\mathrm{Aut}(K/k)$ ist.

Inklusionsumkehrend heißt dabei, dass aus $U_1 \subset U_2$ die die umgekehrte Inklusion $\mathcal{F}(U_1) \supset \mathcal{F}(U_2)$ folgt; entsprechend für $\mathcal{U}$.

Beweis. Dass $\mathcal{F}$ und $\mathcal{U}$ inklusionsumkehrend sind, folgt direkt aus den Definitionen. Wir zeigen, dass die Abbildungen zueinander invers sind. Für Untergruppen U und Zwischenkörper L gilt

$$U \subset \mathcal{U}(\mathcal{F}(U)) \qquad \text{und} \qquad L \subset \mathcal{F}(\mathcal{U}(L))$$

(denn jedes Element von U lässt $\mathcal{F}(U)$ elementweise fest und jedes Element von L wird von allen Elementen von $\mathcal{U}(L)$ festgelassen). Nach Satz 3.9 ist $L \subset K$ für jedes L galoissch, also ist nach Satz 3.3 $\#\mathcal{U}(L) = [K : L]$. Nach Lemma 2.15 gilt $[K : \mathcal{F}(U)] = \#U$. Beides zusammen bedeutet

$$\#U = \#\mathcal{U}(\mathcal{F}(U)) \qquad \text{und} \qquad [K : L] = [K : \mathcal{F}(\mathcal{U}(L))]\,.$$

Zusammen mit der bereits bewiesenen Inklusion folgt

$$U = \mathcal{U}(\mathcal{F}(U)) \qquad \text{und} \qquad L = \mathcal{F}(\mathcal{U}(L))\,,$$

was zu zeigen war.

In Satz 3.9 hatten wir schon gesehen, dass aus „$k \subset L$ galoissch“ folgt, dass $\mathcal{U}(L) = \mathrm{Aut}(K/L)$ ein Normalteiler von $\mathrm{Aut}(K/k)$ ist. Für die umgekehrte Implikation überlegen wir Folgendes. Seien $\gamma, \phi \in \mathrm{Aut}(K/k)$. Dann gilt

$$\begin{aligned}
\phi \in \mathrm{Aut}(K/L) &\iff \forall a \in L\colon \phi(a) = a \\
&\iff \forall a \in L\colon \gamma(\phi(a)) = \gamma(a) \\
&\iff \forall a \in L\colon (\gamma\phi\gamma^{-1})(\gamma(a)) = \gamma(a) \\
&\iff \forall b \in \gamma(L)\colon (\gamma\phi\gamma^{-1})(b) = b \\
&\iff \gamma\phi\gamma^{-1} \in \mathrm{Aut}(K/\gamma(L))\,.
\end{aligned}$$

Das bedeutet $\mathrm{Aut}(K/\gamma(L)) = \gamma\,\mathrm{Aut}(K/L)\gamma^{-1} = \mathrm{Aut}(K/L)$, wobei wir benutzen, dass $\mathrm{Aut}(K/L)$ ein Normalteiler ist. Es folgt $\mathcal{U}(L) = \mathcal{U}(\gamma(L))$, nach dem ersten Teil des Satzes also $L = \gamma(L)$ (für alle $\gamma \in \mathrm{Aut}(K/k)$). Nach Satz 3.9 bedeutet das, dass $k \subset L$ galoissch ist. ❑

Da es relativ einfach ist, sich einen Überblick über die Untergruppen einer endlichen Gruppe zu verschaffen, erlaubt es uns dieser Satz, auch alle Zwischenkörper einer endlichen Galois-Erweiterung zu beschreiben.

3.12. **Beispiel.** Für die Galois-Erweiterung $\mathbb{Q} \subset K = \mathbb{Q}(\sqrt[4]{17}, \boldsymbol{i})$ hatten wir bereits die Untergruppen der Galoisgruppe $\mathrm{Aut}(K/\mathbb{Q}) \cong D_4$ klassifiziert und die zugehörigen Fixkörper bestimmt. Satz 3.11 sagt uns nun, dass es keine weiteren Zwischenkörper gibt. **BSP** $\mathbb{Q}(\sqrt[4]{17}, \mathbf{i})$

Die nichttrivialen Normalteiler von $D_4 = \langle \sigma, \tau \rangle$ sind die Untergruppen $\langle \sigma \rangle$, $\langle \sigma^2, \tau \rangle$ und $\langle \sigma^2, \sigma\tau \rangle$ vom Index 2 und das Zentrum $\langle \sigma^2 \rangle$. Die einzigen (nichttrivialen) Zwischenkörper, die über $\mathbb{Q}$ galoissch sind, sind also $\mathbb{Q}(\boldsymbol{i})$, $\mathbb{Q}(\sqrt{17})$, $\mathbb{Q}(\boldsymbol{i}\sqrt{17})$ und $\mathbb{Q}(\sqrt{17}, \boldsymbol{i})$. ♣

4. Die Diskriminante

Sie kennen alle die Lösungsformel für quadratische Gleichungen:

$$x^2 + px + q = 0 \quad \Longrightarrow \quad x = \frac{-p \pm \sqrt{p^2 - 4q}}{2}\,.$$

Lässt sich eine Formel dieser Art auch für Gleichungen höheren Grades finden? Dabei soll „dieser Art“ bedeuten, dass außer den vier Grundrechenarten auch noch n-te Wurzeln vorkommen dürfen. Die Galois-Theorie wird uns darauf eine Antwort liefern.

Wir betrachten zunächst ein Polynom vom Grad 3:

$$f(x) = x^3 + ax^2 + bx + c\,.$$

Ähnlich wie man ein Polynom vom Grad 2 durch „quadratisches Ergänzen“ vereinfachen kann, können wir hier durch „kubisches Ergänzen“ den Koeffizienten von x^2 zum Verschwinden bringen:

$$f\big(x - \tfrac{1}{3}a\big) = (x^3 - ax^2 + \ldots) + ax^2 + \ldots = x^3 + px + q$$

mit Koeffizienten p und q, die gewisse Ausdrücke in a, b und c sind. Wir nehmen daher an, dass unser Polynom diese Form hat. Außerdem nehmen wir an, dass das Polynom irreduzibel ist, denn sonst könnten wir es faktorisieren, und dann hätten wir es mit Polynomen kleineren Grades zu tun. Sei also

$$f(x) = x^3 + px + q \in k[x]$$

irreduzibel; dabei sei k ein Körper mit $\mathrm{char}(k) \neq 2, 3$. Sei K der Zerfällungskörper von f über k; dann ist $k \subset K$ eine Galois-Erweiterung, und die Galoisgruppe von f ist

$$\mathrm{Gal}(f/k) = \mathrm{Aut}(K/k)\,.$$

Wir hatten bereits gesehen, dass man $\mathrm{Gal}(f/k)$ mit einer Gruppe von Permutationen der Nullstellen von f in k identifizieren kann. Wenn wir die Nullstellen als $\alpha_1, \alpha_2, \alpha_3$ nummerieren, dann können wir also $\mathrm{Gal}(f/k)$ als Untergruppe von S_3 betrachten. Da $k(\alpha_1) \subset K$ und $[k(\alpha_1) : k] = \deg(f) = 3$ ist, folgt

$$\#\,\mathrm{Gal}(f) = [K : k] \in \{3, 6\}\,.$$

Es gibt also die beiden Möglichkeiten $\mathrm{Gal}(f/k) = S_3$ oder $\mathrm{Gal}(f/k) = A_3$ (denn die alternierende Gruppe A_3 ist die einzige Untergruppe von S_3 der Ordnung 3). Wie können wir entscheiden, welche der beiden Möglichkeiten zutrifft?

Im Fall $\mathrm{Gal}(f/k) = S_3$ muss es einen Zwischenkörper $k \subset L \subset K$ geben, der quadratisch über k ist, nämlich $L = \mathcal{F}(A_3)$. Dann ist $L = k(\sqrt{d})$ für ein $d \in k$, das kein Quadrat ist. Da A_3 ein Normalteiler von S_3 ist, ist $k \subset L$ galoissch (das wissen wir schon, da jede quadratische Körpererweiterung in Charakteristik $\neq 2$ galoissch ist) mit Galoisgruppe S_3/A_3. Das heißt konkret, dass für $\sigma \in S_3 = \mathrm{Gal}(f/k)$ gilt

$$\sigma \in A_3 \Rightarrow \sigma(\sqrt{d}) = \sqrt{d} \qquad \text{und} \qquad \sigma \in S_3 \setminus A_3 \Rightarrow \sigma(\sqrt{d}) = -\sqrt{d}\,.$$

(Im zweiten Fall wird $\sqrt{d}$ nicht festgelassen, muss also auf die andere Nullstelle von $x^2 - d$ abgebildet werden.) Man kann das als

$$\sigma(\sqrt{d}) = \varepsilon(\sigma)\sqrt{d}$$

zusammenfassen; dabei ist $\varepsilon(\sigma)$ das Signum der Permutation σ.

Umgekehrt gilt: Ist $\delta \in K$ mit $\sigma(\delta) = \varepsilon(\sigma)\delta$ für alle $\sigma \in S_3$, dann ist $\delta^2 \in k$ und $L = k(\delta)$. Denn $\sigma(\delta^2) = \sigma(\delta)^2 = \varepsilon(\sigma)^2\delta^2 = \delta^2$ für alle $\sigma \in S_3$, also ist

$\delta^2 \in \mathcal{F}(S_3) = k$. Da δ von allen $\sigma \in A_3$ festgelassen wird, gilt entsprechend $\delta \in \mathcal{F}(A_3) = L$. Aus $\delta \in L \setminus k$ folgt $L = k(\delta)$.

Wir werden jetzt ein solches Element δ aus den Nullstellen von f zusammenbauen:

$$\delta = (\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)(\alpha_2 - \alpha_3)\,.$$

Eine Permutation σ der drei Nullstellen vertauscht die drei Faktoren und ändert möglicherweise bei einigen von ihnen das Vorzeichen:

$$\frac{\sigma(\delta)}{\delta} = (-1)^{\#\{(i,j)|1\le i<j\le 3,\sigma(i)>\sigma(j)\}} = \varepsilon(\sigma)\,,$$

also hat δ die gewünschte Eigenschaft.

$$\operatorname{disc}(f) = d = \delta^2 = \prod_{i<j}(\alpha_i - \alpha_j)^2 \in k^\times$$

heißt die *Diskriminante* von f. Wir haben dann das folgende Ergebnis:

SATZ A_3 oder S_3

4.1. **Satz.** *Seien k ein Körper mit $\operatorname{char}(k) \neq 2, 3$ und $f = x^3 + px + q \in k[x]$ irreduzibel. Ist $\operatorname{disc}(f) \in k^\times$ ein Quadrat in k, dann ist $\operatorname{Gal}(f/k) = A_3$, anderenfalls ist $\operatorname{Gal}(f/k) = S_3$.*

Beweis. Ist $\operatorname{disc}(f) = \delta^2$ kein Quadrat in k, dann ist $\delta \notin k$, also gibt es den quadratischen Zwischenkörper $L = k(\delta)$ und es folgt $2 = [L : k] \mid [K : k] = \#\operatorname{Gal}(f/k)$, also muss $\operatorname{Gal}(f/k) = S_3$ sein.

Sei jetzt $\operatorname{disc}(f)$ ein Quadrat, also $\delta \in k$. Sei $\sigma \in \operatorname{Gal}(f/k) \subset S_3$. Nach dem oben Gesagten gilt einerseits $\sigma(\delta) = \varepsilon(\sigma)\delta$, andererseits wegen $\delta \in k$ aber auch $\sigma(\delta) = \delta$. Beides zusammen impliziert $\varepsilon(\sigma) = 1$, also $\sigma \in A_3$. Es folgt $A_3 \subset \operatorname{Gal}(f/k) \subset A_3$, also $\operatorname{Gal}(f/k) = A_3$. ❑

Aus der Tatsache, dass $\operatorname{disc}(f)$ in jedem Körper enthalten ist, der die Koeffizienten von f enthält, folgt, dass $\operatorname{disc}(f)$ durch diese ausgedrückt werden kann. Konkret gilt:

LEMMA Diskriminante für Grad 3

4.2. **Lemma.** *Für $f = x^3 + px + q$ gilt*

$$\operatorname{disc}(f) = -4p^3 - 27q^2\,.$$

Beweis. Aus $f = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)$ folgt

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

Die behauptete Gleichheit folgt dann durch eine einfache, aber umständliche Rechnung. ❑

Die Aussage von Satz 4.1 lässt sich verallgemeinern. Dazu definieren wir die Diskriminante für ein beliebiges normiertes Polynom.

4.3. **Definition.** Seien k ein Körper und $f \in k[x]$ ein normiertes Polynom vom Grad $n \geq 1$. Sei K ein Zerfällungskörper von f über k, sodass **DEF** Diskriminante

$$f = \prod_{j=1}^{n}(x - \alpha_j) \in K[x]\,.$$

Dann ist die *Diskriminante* von f definiert als

$$\operatorname{disc}(f) = \prod_{i<j}(\alpha_i - \alpha_j)^2\,. \qquad \diamondsuit$$

4.4. **Lemma.** *Seien k ein Körper und $f \in k[x]$ ein normiertes Polynom vom Grad n.* **LEMMA** Diskriminante und mehrfache Nullstellen

(1) $\operatorname{disc}(f) \in k$.

(2) $\operatorname{disc}(f) \neq 0$ *genau dann, wenn f nur einfache Nullstellen hat; insbesondere ist f dann separabel.*

Beweis. Der zweite Teil folgt direkt aus der Definition der Diskriminante. Wenn $\operatorname{disc}(f) = 0$ ist, dann ist $\operatorname{disc}(f) \in k$. Sei also jetzt $\operatorname{disc}(f) \neq 0$. Dann ist f separabel, also ist $k \subset K$ eine Galois-Erweiterung, wobei K ein Zerfällungskörper von f über k ist. Die Elemente von $\operatorname{Gal}(f/k) = \operatorname{Aut}(K/k)$ permutieren die Nullstellen α_j von f und damit die Faktoren in der Definition von $\operatorname{disc}(f)$. Es folgt $\operatorname{disc}(f) \in \mathcal{F}(\operatorname{Aut}(K/k)) = k$. ❑

4.5. **Bemerkung.** Man kann sogar zeigen, dass die Diskriminante ein Polynom mit ganzzahligen Koeffizienten in den Koeffizienten $a_0, a_1, \ldots, a_{n-1}$ von

$$f = x^n + a_{n-1}x^{n-1} + \ldots + a_2x^2 + a_1x + a_0$$

ist. Genauer gilt

$$\operatorname{disc}(f) = (-1)^{\binom{n}{2}} \begin{vmatrix} 1 & a_{n-1} & a_{n-2} & \cdots & a_0 & 0 & \cdots & 0 \\ 0 & 1 & a_{n-1} & \cdots & a_1 & a_0 & \cdots & 0 \\ \vdots & & \ddots & \ddots & & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 & a_{n-1} & \cdots & a_1 & a_0 \\ n & (n-1)a_{n-1} & (n-2)a_{n-2} & \cdots & a_1 & 0 & \cdots & 0 \\ 0 & n & (n-1)a_{n-1} & \cdots & 2a_2 & a_1 & \cdots & 0 \\ \vdots & & \ddots & \ddots & & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & n & (n-1)a_{n-1} & \cdots & 2a_2 & a_1 \end{vmatrix}.$$

Das ist eine $(2n-1)$-reihige Determinante, in deren ersten $n-1$ Zeilen die Koeffizienten von f stehen (in jeder Zeile gegenüber der vorigen um einen Platz nach rechts verschoben) und in deren letzten n Zeilen die Koeffizienten der Ableitung f' stehen. Zum Beispiel erhalten wir für $f = x^3 + px + q$:

$$\begin{aligned} \operatorname{disc}(f) &= -\begin{vmatrix} 1 & 0 & p & q & 0 \\ 0 & 1 & 0 & p & q \\ 3 & 0 & p & 0 & 0 \\ 0 & 3 & 0 & p & 0 \\ 0 & 0 & 3 & 0 & p \end{vmatrix} = -\begin{vmatrix} 1 & 0 & p & q & 0 \\ 0 & 1 & 0 & p & q \\ 0 & 0 & -2p & -3q & 0 \\ 0 & 0 & 0 & -2p & -3q \\ 0 & 0 & 3 & 0 & p \end{vmatrix} \\ &= -\big((-2p)(-2p)p + (-3q)(-3q)q\big) = -4p^3 - 27q^2\,. \end{aligned}$$

Für $f = x^2 + px + q$ erhalten wir die bekannte Formel

$$\operatorname{disc}(f) = -\begin{vmatrix} 1 & p & q \\ 2 & p & 0 \\ 0 & 2 & p \end{vmatrix} = p^2 - 4q\,.$$

Die Verallgemeinerung unseres Satzes 4.1 lautet jetzt wie folgt.

SATZ Gal $\subset A_n$

4.6. **Satz.** *Sei k ein Körper mit $\operatorname{char}(k) \neq 2$ und sei $f \in k[x]$ ein normiertes Polynom vom Grad $n \geq 1$ mit $\operatorname{disc}(f) \neq 0$. Dann ist f separabel und es gilt für die Galoisgruppe $\operatorname{Gal}(f/k) \subset S_n$:*

$$\operatorname{Gal}(f/k) \subset A_n \iff \operatorname{disc}(f) \text{ ist ein Quadrat in } k.$$

Beweis. Dass aus $\operatorname{disc}(f) \neq 0$ folgt, dass f separabel ist, hatten wir bereits in Lemma 4.4 gesehen. Sei K ein Zerfällungskörper von f über k und sei $\delta \in K$ mit $\delta^2 = \operatorname{disc}(f)$, also etwa

$$\delta = \prod_{i<j} (\alpha_i - \alpha_j)\,,$$

wenn $\alpha_1, \ldots, \alpha_n \in K$ die Nullstellen von f sind. Für $\sigma \in \operatorname{Gal}(f/k) \subset S_n$ gilt dann wie vorher $\sigma(\delta) = \varepsilon(\sigma)\delta$. Ist $\operatorname{disc}(f)$ ein Quadrat in k, dann ist $\delta \in k$, also $\sigma(\delta) = \delta$, und es folgt $\varepsilon(\sigma) = 1$ (man beachte $1 \neq -1$ wegen $\operatorname{char}(k) \neq 2$), also $\sigma \in A_n$. Ist $\delta \notin k$, dann ist $L = k(\delta)$ ein Zwischenkörper vom Grad 2 in $k \subset K$ und es gilt $L = \mathcal{F}(\operatorname{Gal}(f/k) \cap A_n)$, denn

$$\sigma|_L = \mathrm{id}_L \iff \sigma(\delta) = \delta \iff \varepsilon(\sigma) = 1\,.$$

Dann muss $\operatorname{Gal}(f/k) \cap A_n$ eine echte Untergruppe von $\operatorname{Gal}(f/k)$ sein, also folgt $\operatorname{Gal}(f/k) \not\subset A_n$. ❑

Für Polynome $f = x^2 + px + q$ vom Grad 2 bedeutet das gerade (falls $\operatorname{char}(k) \neq 2$):

$$f \text{ zerfällt über } k \iff p^2 - 4q \text{ ist ein Quadrat in } k.$$

5. Lösungsformeln für Gleichungen vom Grad 3 und 4

Für ein irreduzibles Polynom $f = x^3 + px + q \in k[x]$ (mit $\mathrm{char}(k) \neq 2, 3$) vom Grad 3 haben wir den Körperturm

$$k \subset L = k(\sqrt{\mathrm{disc}(f)}) \subset K\,,$$

wobei K der Zerfällungskörper von f ist; die Körpererweiterung $L \subset K$ ist galoissch mit Galoisgruppe $A_3 \cong \mathbb{Z}/3\mathbb{Z}$. Können wir die Elemente von K (also insbesondere die Nullstellen von f) durch geeignete dritte Wurzeln von Elementen von L ausdrücken? Dazu nehmen wir erst einmal an, dass k eine primitive dritte Einheitswurzel enthält, also ein Element ω mit $\omega^3 = 1$, aber $\omega \neq 1$ (d.h., ω erfüllt die Gleichung $\omega^2+\omega+1 = 0$). Sei $\sigma \in \mathrm{Aut}(K/L)$ ein Erzeuger. Dann ist $\sigma\colon K \to K$ ein L-linearer Endomorphismus des L-Vektorraums K, und σ hat Ordnung 3. Das Minimalpolynom von σ als L-linearer Endomorphismus teilt x^3-1, also ist σ diagonalisierbar (hier brauchen wir $\mathrm{char}(k) \neq 3$) und die Eigenwerte sind unter $1, \omega, \omega^2$ zu finden. Der Eigenwert 1 tritt mit Vielfachheit 1 auf; der zugehörige Eigenraum ist L. Es tritt also ω oder ω^2 als Eigenwert auf; tatsächlich sogar beide (sei etwa $\alpha \in K$ Eigenvektor zum Eigenwert ω, dann ist $\sigma(\alpha^2) = (\sigma(\alpha))^2 = (\omega\alpha)^2 = \omega^2\alpha^2$, also ist α^2 ein Eigenvektor zum Eigenwert ω^2). Sei $\alpha \in K$ Eigenvektor zum Eigenwert ω^2, also $\sigma(\alpha) = \omega^2\alpha$. Dann ist $a = \alpha^3 \in L$, denn $\sigma(\alpha^3) = (\omega^2\alpha)^3 = \omega^6\alpha^3 = \alpha^3$ und es folgt $K = L(\sqrt[3]{a})$ (denn $\alpha \in K \setminus L$).

Wenn k keine primitive dritte Einheitswurzel enthält, dann adjungieren wir eine, ersetzen k also durch $k(\omega) = k(\sqrt{-3})$. Um eine explizite Formel zu bekommen, müssen wir noch herausfinden, wie wir das Element a durch die Koeffizienten von f und $\sqrt{\mathrm{disc}(f)}$ ausdrücken können. Seien dazu $\alpha_1, \alpha_2, \alpha_3$ die Nullstellen von f in K. Wir können die Nummerierung so wählen, dass $\sigma(\alpha_1) = \alpha_2$, $\sigma(\alpha_2) = \alpha_3$ und $\sigma(\alpha_3) = \alpha_1$ ist. Dann gilt für $\alpha = \alpha_1 + \omega\alpha_2 + \omega^2\alpha_3$:

$$\sigma(\alpha) = \alpha_2 + \omega\alpha_3 + \omega^2\alpha_1 = \omega^2(\omega\alpha_2 + \omega^2\alpha_3 + \alpha_1) = \omega^2\alpha\,,$$

also liegt α im richtigen Eigenraum. Wir machen noch ein paar vorbereitende Rechnungen. Sei dazu

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

eine Quadratwurzel aus $\mathrm{disc}(f)$. Aus einem Koeffizientenvergleich

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

folgt

$$\alpha_1 + \alpha_2 + \alpha_3 = 0, \qquad \alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3 = p \quad \text{und} \quad \alpha_1\alpha_2\alpha_3 = -q$$

und damit

$$\begin{aligned}(\alpha_1^2\alpha_2 + \alpha_2^2\alpha_3 + \alpha_3^2\alpha_1) + (\alpha_1\alpha_2^2 + \alpha_2\alpha_3^2 + \alpha_3\alpha_1^2)&\\ = (\alpha_1 + \alpha_2 + \alpha_3)(\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3) - 3\alpha_1\alpha_2\alpha_3&\\ = 3q&\end{aligned}$$

und

$$\begin{aligned}&\alpha_1^3 + \alpha_2^3 + \alpha_3^3\\ &\quad = (\alpha_1 + \alpha_2 + \alpha_3)^3 - 3(\alpha_1 + \alpha_2 + \alpha_3)(\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3) + 3\alpha_1\alpha_2\alpha_3\\ &\quad = -3q\,.\end{aligned}$$

Außerdem ist $\omega = -\frac{1}{2} + \frac{1}{2}\sqrt{-3}$. Wir haben dann

$$\begin{aligned} a = \alpha^3 &= (\alpha_1 + \omega\alpha_2 + \omega^2\alpha_3)^3 \\ &= \alpha_1^3 + \alpha_2^3 + \alpha_3^3 + 6\alpha_1\alpha_2\alpha_3 \\ &\quad + 3\omega(\alpha_1^2\alpha_2 + \alpha_1\alpha_3^2 + \alpha_2^2\alpha_3) + 3\omega^2(\alpha_1\alpha_2^2 + \alpha_1^2\alpha_3 + \alpha_2\alpha_3^2) \\ &= -3q - 6q + \frac{3}{2}\omega(3q+\delta) + \frac{3}{2}\omega^2(3q-\delta) \\ &= -\frac{27}{2}q + \frac{3\sqrt{-3}}{2}\delta \\ &= 27\Big(-\frac{q}{2} + \sqrt{\Big(\frac{p}{3}\Big)^3 + \Big(\frac{q}{2}\Big)^2}\Big) \end{aligned}$$

Mit $\bar\alpha = \alpha_1 + \omega^2\alpha_2 + \omega\alpha_3$ und $\bar a = \bar\alpha^3$ erhalten wir analog

$$\bar a = 27\Big(-\frac{q}{2} - \sqrt{\Big(\frac{p}{3}\Big)^3 + \Big(\frac{q}{2}\Big)^2}\Big)\,.$$

Dabei gilt

$$\begin{aligned} \alpha\bar\alpha &= \alpha_1^2 + \alpha_2^2 + \alpha_3^2 - \alpha_1\alpha_2 - \alpha_1\alpha_3 - \alpha_2\alpha_3 \\ &= (\alpha_1 + \alpha_2 + \alpha_3)^2 - 3(\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3) \\ &= -3p\,. \end{aligned}$$

N. Tartaglia
(1499?–1557)

Wegen

$$\alpha_1 = \frac{1}{3}\big((\alpha_1 + \alpha_2 + \alpha_3) + \alpha + \bar\alpha\big) = \frac{1}{3}(\alpha + \bar\alpha)$$

ist

$$\alpha_1 = \sqrt[3]{-\frac{q}{2} + \sqrt{\Big(\frac{p}{3}\Big)^3 + \Big(\frac{q}{2}\Big)^2}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\Big(\frac{p}{3}\Big)^3 + \Big(\frac{q}{2}\Big)^2}}\,;$$

dabei sind die dritten Wurzeln so zu wählen, dass ihr Produkt $-p/3$ ist. Wir halten fest:

SATZ
Lösungsformel für kubische Gleichungen

5.1. **Satz.** *Sei k ein Körper mit $\mathrm{char}(k) \neq 2, 3$ und $f = x^3 + px + q \in k[x]$. Sei $k \subset K$ eine Körpererweiterung, die eine primitive dritte Einheitswurzel ω und die Nullstellen von f enthält.*

Sei weiter $d = (p/3)^3 + (q/2)^2 = -\operatorname{disc}(f)/(4\cdot 27)$ und $\delta = \sqrt{d} \in K$ eine Quadratwurzel von d. Seien $\alpha = \sqrt[3]{-q/2 + \delta}, \bar\alpha = \sqrt[3]{-q/2 - \delta} \in K$ dritte Wurzeln mit $\alpha\bar\alpha = -p/3$. Dann sind die Nullstellen von f in K gegeben durch

$$\alpha_1 = \alpha + \bar\alpha, \qquad \alpha_2 = \omega\alpha + \omega^2\bar\alpha \qquad \text{und} \qquad \alpha_3 = \omega^2\alpha + \omega\bar\alpha\,.$$

G. Cardano
(1501–1576)

Diese Formeln gehen auf Tartaglia und del Ferro (ca. 1515) zurück. Cardano veröffentlichte sie als Erster (1545), nachdem er unveröffentlichte Notizen von del Ferro dazu gesehen hatte, obwohl Tartaglia ihm die Formeln nur unter der Bedingung verraten hatte, dass er sie geheim hält.

Beweis. Dass $\delta, \alpha, \bar\alpha \in K$ sind, folgt aus den vorhergehenden Überlegungen (und in jedem Fall könnte man K geeignet wählen). Man rechnet nun nach:

$$(\alpha\bar\alpha)^3 = \alpha^3\bar\alpha^3 = \Big(-\frac{q}{2} + \delta\Big)\Big(-\frac{q}{2} - \delta\Big) = \Big(\frac{q}{2}\Big)^2 - \Big(\Big(\frac{p}{3}\Big)^3 + \Big(\frac{q}{2}\Big)^2\Big) = \Big(-\frac{p}{3}\Big)^3,$$

also können α und $\bar\alpha$ wie angegeben gewählt werden. Es gilt dann:

$$\begin{aligned}\alpha_1+\alpha_2+\alpha_3 &= (1+\omega+\omega^2)\alpha+(1+\omega^2+\omega)\bar\alpha = 0\,,\\ \alpha_1\alpha_2+\alpha_1\alpha_3+\alpha_2\alpha_3 &= (\omega+\omega^2+1)\alpha^2+(\omega^2+\omega+1)\bar\alpha^2\\ &\quad +(\omega^2+\omega+\omega+\omega^2+\omega^2+\omega)\alpha\bar\alpha\\ &= -3\alpha\bar\alpha = p\,,\\ \alpha_1\alpha_2\alpha_3 &= \alpha^3+\bar\alpha^3+(\omega^2+\omega+1)\alpha^2\bar\alpha+(1+\omega^2+\omega)\alpha\bar\alpha^2\\ &= \alpha^3+\bar\alpha^3 = -\frac{q}{2}+\delta-\frac{q}{2}-\delta = -q\,.\end{aligned}$$

Die Behauptung folgt durch Koeffizientenvergleich in

$$f = x^3+px+q = (x-\alpha_1)(x-\alpha_2)(x-\alpha_3)\,. \qquad \square$$

Für diesen Beweis haben wir die Galois-Theorie nicht gebraucht, wohl aber dafür, die Formel herzuleiten.

5.2. **Beispiel.** Sei $k=\mathbb{Q}$, $K=\mathbb{C}$ und $f=x^3-3x+1\in\mathbb{Q}[x]$. Wir haben also $p=-3$ und $q=1$. Das ergibt **BSP** x^3-3x+1

$$d = (p/3)^3+(q/2)^2 = -1+1/4 = -3/4\,,$$

also $\delta=\sqrt{-3}/2$. Für α haben wir $\alpha=\sqrt[3]{-1/2+\sqrt{-3}/2}=\sqrt[3]{\omega}$ (mit $\omega=e^{2\pi i/3}=(-1+\sqrt{-3})/2$ wie oben), also können wir $\alpha=\zeta_9=e^{2\pi i/9}$ nehmen; das ergibt dann $\bar\alpha=1/\alpha=\zeta_9^{-1}$. Die Nullstellen von f sind demnach

$$\begin{aligned}\zeta_9+\zeta_9^{-1} &= 2\cos\frac{2\pi}{9}\,,\\ \omega\zeta_9+\omega^2\zeta_9^{-1} &= \zeta_9^4+\zeta_9^{-4} = 2\cos\frac{8\pi}{9} \qquad \text{und}\\ \omega^2\zeta_9+\omega\zeta_9^{-1} &= \zeta_9^{-2}+\zeta_9^2 = 2\cos\frac{4\pi}{9}\,.\end{aligned}$$ ♣

In diesem Beispiel mussten wir mit echt komplexen Zahlen rechnen (δ ist rein imaginär), obwohl die Nullstellen alle reell sind. Das ist kein Zufall.

5.3. **Lemma.** *Sei $f\in\mathbb{R}[x]$ normiert mit $\deg(f)=3$. Dann hat f entweder genau eine oder genau drei reelle Nullstellen (mit Vielfachheit gerechnet). Der erste Fall tritt ein, wenn $\operatorname{disc}(f)<0$ ist, der zweite Fall, wenn $\operatorname{disc}(f)\geq 0$ ist.* **LEMMA** kubische Polynome über $\mathbb{R}$

Beweis. Seien $\alpha_1,\alpha_2,\alpha_3\in\mathbb{C}$ die Nullstellen von f. Es ist

$$\operatorname{disc}(f) = (\alpha_1-\alpha_2)^2(\alpha_1-\alpha_3)^2(\alpha_2-\alpha_3)^2\,.$$

Sind die Nullstellen reell, dann ist $\operatorname{disc}(f)$ Quadrat einer reellen Zahl, also ≥ 0. Sind nicht alle Nullstellen reell, dann gibt es eine reelle Nullstelle α und ein Paar zueinander konjugierter komplexer Nullstellen β und $\bar\beta$. Dann ist

$$\operatorname{disc}(f) = \big((\alpha-\beta)(\alpha-\bar\beta)\big)^2(\beta-\bar\beta)^2<0\,,$$

denn der erste Faktor ist das Quadrat der von null verschiedenen reellen Zahl $\alpha^2-2\alpha\operatorname{Re}\beta+|\beta|^2$ und der zweite Faktor ist $-4(\operatorname{Im}\beta)^2<0$. $\square$

Da wir für die Lösungsformel die Quadratwurzel aus $-\operatorname{disc}(f)/108$ brauchen, ist diese rein imaginär genau dann, wenn die Nullstellen von f alle reell sind. Diese Beobachtung ('casus irreducibilis' genannt) hat übrigens in der historischen Entwicklung letztendlich zur Anerkennung der komplexen Zahlen geführt, nicht etwa der Wunsch, einer Gleichung wie $x^2+1=0$ eine Lösung zu verschaffen. Denn man konnte ja akzeptieren, dass so eine Gleichung keine (reelle) Lösung hat, während im kubischen Fall drei reelle Lösungen existieren konnten, zu deren Berechnung man aber die komplexen Zahlen benötigte.

Für die Lösung einer Gleichung vom Grad 4 gehen wir erst einmal davon aus, dass das zugehörige Polynom Galoisgruppe S_4 hat. In der S_4 gibt es als Normalteiler die *Kleinsche Vierergruppe* $V_4 = \{\mathrm{id}, (12)(34), (13)(24), (14)(23)\}$. Es ist $S_4/V_4 \cong S_3$ (S_4 operiert auf den drei nichttrivialen Elementen von V_4 durch Konjugation, das liefert einen Homomorphismus in die S_3 mit Kern V_4). Der entsprechende Zwischenkörper ist dann galoissch über dem Grundkörper mit Galoisgruppe S_3, man sollte ihn also durch Lösen einer geeigneten kubischen Gleichung erhalten können. Die verbleibende Erweiterung bis zum Zerfällungskörper hat dann Galoisgruppe $V_4 \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ und ist durch Quadratwurzeln erzeugbar. Die Nullstellen der kubischen Gleichung sollten also gerade den Fixkörper von V_4 erzeugen. Wie bei quadratischen und kubischen Gleichungen können wir durch geeignete Verschiebung erreichen, dass das Polynom vierten Grades, dessen Nullstellen wir berechnen wollen, die Form $f = x^4 + px^2 + qx + r$ hat. Wir bezeichnen die Nullstellen von f mit $\alpha_1, \alpha_2, \alpha_3, \alpha_4$. Dann sind die Elemente

$$\beta = (\alpha_1+\alpha_2)(\alpha_3+\alpha_4), \quad \beta' = (\alpha_1+\alpha_3)(\alpha_2+\alpha_4) \quad \text{und} \quad \beta'' = (\alpha_1+\alpha_4)(\alpha_2+\alpha_3)$$

in $\mathcal{F}(V_4)$, denn sie sind unter den Permutationen in V_4 invariant. Wegen $\alpha_1+\alpha_2+\alpha_3+\alpha_4 = 0$ ist

$$(\alpha_1+\alpha_2)^2 = -\beta, \qquad (\alpha_1+\alpha_3)^2 = -\beta' \qquad \text{und} \qquad (\alpha_1+\alpha_4)^2 = -\beta'',$$

sodass mit geeigneten Quadratwurzeln gilt

$$\alpha_1 = \frac{1}{2}\big((\alpha_1+\alpha_2)+(\alpha_1+\alpha_3)+(\alpha_1+\alpha_4)\big) = \frac{1}{2}(\sqrt{-\beta}+\sqrt{-\beta'}+\sqrt{-\beta''}).$$

Man kann folgende Beziehung nachrechnen:

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

Außerdem ist $(\alpha_1+\alpha_2)(\alpha_1+\alpha_3)(\alpha_1+\alpha_4) = -q$. Wir fassen zusammen:

SATZ Lösungsformel für Gleichungen vom Grad 4

5.4. **Satz.** *Sei k ein Körper mit $\mathrm{char}(k) \neq 2, 3$ und $f = x^4+px^2+qx+r \in k[x]$. Sei $k \subset K$ eine Körpererweiterung, die eine primitive dritte Einheitswurzel ω und die Nullstellen von f enthält.*

Sei $g = x^3 - 2px^2 + (p^2-4r)x + q^2$. Dann zerfällt g über K in Linearfaktoren. Seien $\beta, \beta', \beta'' \in K$ die Nullstellen von g (die man mit Satz 5.1 bestimmen kann). Seien weiter $\gamma = \sqrt{-\beta} \in K$, $\gamma' = \sqrt{-\beta'}, \gamma'' = \sqrt{-\beta''} \in K$ Quadratwurzeln, sodass $\gamma\gamma'\gamma'' = -q$. Dann sind die Nullstellen von f gegeben durch

$$\begin{aligned}
\alpha_1 &= \tfrac{1}{2}(\gamma+\gamma'+\gamma''),\\
\alpha_2 &= \tfrac{1}{2}(\gamma-\gamma'-\gamma''),\\
\alpha_3 &= \tfrac{1}{2}(-\gamma+\gamma'-\gamma'') \qquad \textit{und}\\
\alpha_4 &= \tfrac{1}{2}(-\gamma-\gamma'+\gamma'').
\end{aligned}$$

Die Formeln gehen auf Ferrari (ca. 1545) zurück.

Das Polynom g heißt die *kubische Resolvente* von f. Es gilt $\operatorname{disc}(g) = \operatorname{disc}(f)$, denn (z.B.) $\beta - \beta' = (\alpha_1 - \alpha_4)(\alpha_3 - \alpha_2)$.

Beweis. Man rechnet die relevanten Beziehungen nach, analog zum Beweis von Satz 5.1. ❑

5.5. **Beispiel.** Wir betrachten wieder $k = \mathbb{Q}$, $K = \mathbb{C}$ und $f = x^4 - 10x^2 + 1$. Die kubische Resolvente ist $g = x^3 + 20x^2 + 96x = x(x+8)(x+12)$. Ihre Nullstellen sind $\beta = 0$, $\beta' = -8$, $\beta'' = -12$. Wir können also $\gamma = 0$, $\gamma' = 2\sqrt{2}$, $\gamma'' = 2\sqrt{3}$ wählen und erhalten die Nullstellen

BSP $x^4 - 10x^2 + 1$

$$\sqrt{2} + \sqrt{3}, \quad -\sqrt{2} - \sqrt{3}, \quad \sqrt{2} - \sqrt{3} \quad \text{und} \quad -\sqrt{2} + \sqrt{3}\,.$$

In diesem Fall könnte man die Lösungen auch durch sukzessives Lösen zweier quadratischer Gleichungen finden: $x^2 = 5 \pm 2\sqrt{6}$, also sind die Lösungen $\pm\sqrt{5 \pm 2\sqrt{6}}$. Tatsächlich ist $(\sqrt{2} \pm \sqrt{3})^2 = 5 \pm 2\sqrt{6}$; der Satz liefert die einfachere Form direkt. ♣

Die kubische Resolvente erlaubt es uns auch, zwischen den verschiedenen Möglichkeiten für die Galoisgruppe eines irreduziblen Polynoms vom Grad 4 zu unterscheiden. Grundsätzlich gilt folgende Aussage:

5.6. **Lemma.** *Sei k ein Körper und $f \in k[x]$ ein normiertes Polynom ohne mehrfache Nullstellen in seinem Zerfällungskörper. Dann ist f genau dann irreduzibel, wenn die Galoisgruppe* $\operatorname{Gal}(f/k)$ *auf den Nullstellen von f transitiv operiert.*

LEMMA Kriterium für irreduzibel

Beweis. Sei K ein Zerfällungskörper von f über k. Dann ist $\operatorname{Gal}(f/k) = \operatorname{Aut}(K/k)$. Wenn diese Gruppe transitiv auf den Nullstellen von f operiert, dann ist f nach Lemma 2.15 irreduzibel. Ist die Operation nicht transitiv, dann führt jede Bahn wiederum nach Lemma 2.15 zu einem nichttrivialen Teiler von f in $k[x]$, also ist in diesem Fall f nicht irreduzibel. ❑

Die transitiv operierenden Untergruppen der S_4 sind (bis auf Konjugation)

(1) die zyklische Gruppe $C_4 = \langle (1234) \rangle$,

(2) die Kleinsche Vierergruppe V_4,

(3) die Diedergruppe $D_4 = \langle (1234), (13) \rangle$,

(4) die alternierende Gruppe A_4 und

(5) die symmetrische Gruppe S_4 selbst.

Davon sind die V_4 und die A_4 in der A_4 enthalten, die übrigen Gruppen nicht (denn ein Viererzykel ist eine ungerade Permutation). Da wir über die Diskriminante feststellen können, ob die Galoisgruppe in der A_4 enthalten ist, müssen wir noch zwischen V_4 und A_4 bzw. zwischen C_4, D_4 und S_4 unterscheiden. Dazu betrachten wir die Anzahl der Nullstellen der kubischen Resolvente in k. Wenn eine Nullstelle, zum Beispiel $\beta' = (\alpha_1 + \alpha_3)(\alpha_2 + \alpha_4)$ in k liegt, dann muss jedes Element $\sigma \in \operatorname{Gal}(f/k) \subset S_4$ dieses Element fest lassen, was damit äquivalent ist, dass σ die Partition $\{\{1,3\},\{2,4\}\}$ von $\{1,2,3,4\}$ fest lässt. Das bedeutet $\operatorname{Gal}(f/K) \subset D_4$. (Beachte, dass die kubische Resolvente g keine mehrfachen Nullstellen hat, denn $\operatorname{disc}(g) = \operatorname{disc}(f) \neq 0$.) Sind alle drei Nullstellen von g in k, dann folgt entsprechend $\operatorname{Gal}(f/k) \subset V_4$.

SATZ Galoisgruppen Grad 4

5.7. **Satz.** *Sei k ein Körper und sei $f \in k[x]$ irreduzibel vom Grad 4 mit $d = \operatorname{disc}(f) \neq 0$. Sei weiter g die kubische Resolvente von f und n die Anzahl der Nullstellen von g in k. Dann ergibt sich die Galoisgruppe $\operatorname{Gal}(f/k)$ aus folgender Tabelle (dabei heißt „$d = \square$“, dass d ein Quadrat in k ist):*

	$n=0$	$n=1$	$n=3$
$d = \square$	A_4	$-$	V_4
$d \neq \square$	S_4	C_4, D_4	$-$

Die Unterscheidung zwischen C_4 und D_4 ist etwas schwieriger; wir werden das hier nicht ausführen. Man kann aber im Fall „C_4 oder D_4“ geeignete Ausdrücke D in den Koeffizienten von f und der Nullstelle von g in k konstruieren, sodass (wenn $D \neq 0$ ist, anderenfalls muss man einen anderen Ausdruck verwenden) man genau dann im Fall C_4 ist, wenn D ein Quadrat in k ist. In den Beispielen unten werden wir statt dessen ad-hoc-Argumente verwenden.

Ist $b \in k$ die einzige Nullstelle von g in k und hat f die Form $f = x^4 + px^2 + qx + r$, dann ist die Galoisgruppe genau dann C_4, wenn $2b^2p - 3bp^2 - 4br - 3q^2$ ein Quadrat in k ist. Dieser Ausdruck ergibt sich (mit $b = \beta'$) aus

$$\left((\alpha_1^2\alpha_2 + \alpha_2^2\alpha_3 + \alpha_3^2\alpha_4 + \alpha_4^2\alpha_1) - (\alpha_1\alpha_2^2 + \alpha_2\alpha_3^2 + \alpha_3\alpha_4^2 + \alpha_4\alpha_1^2)\right)^2 .$$

Die Elemente der C_4 lassen beide Terme in der Differenz fest, während die zusätzlichen Elemente der D_4 die beiden Terme vertauschen. Die Galoisgruppe ist die C_4 also genau dann, wenn die Differenz in k ist, jedenfalls dann, wenn diese Differenz nicht null ist.

Bevor wir uns Beispiele anschauen, überlegen wir noch Folgendes:

Sei $f \in k[x]$ vom Grad 4 mit kubsicher Resolvente g. Ist g irreduzibel, dann operiert $G = \operatorname{Gal}(f/k)$ transitiv auf den Nullstellen von g. Damit ist das Bild von G unter $G \hookrightarrow S_4 \to S_3$ mindestens die A_3. Ist f nicht irreduzibel, dann muss f eine Nullstelle in k haben, denn im verbleibenden Fall, dass f Produkt zweier irreduzibler Faktoren vom Grad 2 ist, ist $G \subset \langle (1\ 2), (3\ 4) \rangle$ (wobei wir die Nullstellen so nummeriert haben, dass die ersten beiden zu einem der irreduziblen Faktoren gehören) und damit $\#G$ ein Teiler von 4, sodass das Bild von G in S_3 nicht durch 3 teilbare Ordnung haben kann. Also:

Ist g irreduzibel und hat f keine Nullstelle in k, dann ist auch f irreduzibel.

BSP Grad 4: Galois-gruppen

5.8. **Beispiele.** Wie üblich sei $k = \mathbb{Q}$.

(1) $f = x^4 + x + 1$. Dann ist f irreduzibel nach dem Reduktionskriterium mit $p = 2$ (denn $x^4 + x + 1$ ist irreduzibel in $\mathbb{F}_2[x]$) und $g = x^3 - 4x + 1$ mit

$$\operatorname{disc}(f) = \operatorname{disc}(g) = -4(-4)^3 - 27 \cdot 1^2 = 256 - 27 = 229 .$$

g ist irreduzibel (da ohne rationale Nullstelle; nur ± 1 kommen in Frage) und $\operatorname{disc}(f)$ ist kein Quadrat, also ist $\operatorname{Gal}(f/\mathbb{Q}) = S_4$.

(2) $f = x^4 + 3x^2 - 7x + 4$. Dann ist $g = x^3 - 6x^2 - 7x + 49$. Zur Berechnung der Diskriminante betrachten wir $g(x + 2) = x^3 - 19x + 19$; es ergibt sich

$$\operatorname{disc}(f) = \operatorname{disc}(g) = -4(-19)^3 - 27 \cdot 19^2 = 17689 = 133^2 .$$

Außerdem ist $g(x + 2)$ irreduzibel nach Eisenstein mit $p = 19$. f hat keine rationale Nullstelle (nur ± 1, ± 2 kommen infrage), also ist f irreduzibel und $\operatorname{Gal}(f/\mathbb{Q}) = A_4$.

(3) $f = x^4 - 2$; f ist irreduzibel nach Eisenstein mit $p = 2$. Die kubische Resolvente ist $g = x^3 + 8x = x(x^2 + 8)$; der zweite Faktor ist irreduzibel, also ist die Galoisgruppe C_4 oder D_4. Wir wissen, dass f zwei reelle und ein Paar konjugiert komplexe Nullstellen hat. Die komplexe Konjugation liefert ein Element von $\mathrm{Gal}(f/\mathbb{Q})$, das genau zwei Nullstellen vertauscht. Damit kann $\mathrm{Gal}(f/\mathbb{Q})$ nicht C_4 sein, also ist $\mathrm{Gal}(f/\mathbb{Q}) = D_4$.

(4) $f = x^4 + 1$. Es ist $f(x + 1) = x^4 + 4x^3 + 6x^2 + 4 + 2$; dieses Polynom ist irreduzibel nach Eisenstein mit $p = 2$. Es ist $g = x^3 - 4x = x(x - 2)(x + 2)$ mit drei rationalen Nullstellen, also ist die Galoisgruppe V_4.

(5) $f = x^4 + x^3 + x^2 + x + 1$. Die Nullstellen von f sind gerade die fünften Einheitswurzeln außer 1, also $\zeta, \zeta^2, \zeta^3, \zeta^4$ mit $\zeta = e^{2\pi i/5}$. Wenn $K \subset \mathbb{C}$ der Zerfällungskörper von f ist, dann ist $K = \mathbb{Q}(\zeta)$ (da sich die anderen Nullstellen durch ζ ausdrücken lassen), also ist $\#\,\mathrm{Gal}(f/\mathbb{Q}) = \#[K : \mathbb{Q}] = \deg(f) = 4$. Die Galoisgruppe ist also C_4 oder V_4. Da f irreduzibel ist ($f(x + 1) = x^4 + 5x^3 + 10x^2 + 10x + 5$ ist irreduzibel nach Eisenstein), operiert $\mathrm{Gal}(f/\mathbb{Q})$ transitiv auf den Nullstellen. Es gibt also ein Element $\sigma \in \mathrm{Gal}(f/\mathbb{Q})$, das ζ auf ζ^2 abbildet. Dann ist $\sigma(\zeta^2) = (\zeta^2)^2 = \zeta^4$, $\sigma(\zeta^4) = (\zeta^2)^4 = \zeta^8 = \zeta^3$ und $\sigma(\zeta^3) = (\zeta^2)^3 = \zeta^6 = \zeta$; σ operiert also als Zykel der Länge 4 auf den Nullstellen. Damit muss die Galoisgruppe isomorph zur C_4 sein.

Alternativ könnte man die kubische Resolvente bestimmen:

$$f(x - \tfrac{1}{4}) = x^4 + \frac{5}{8}x^2 + \frac{5}{8}x + \frac{205}{256}\,,$$

damit ist

$$g = x^3 - \frac{5}{4}x^2 - \frac{45}{16}x + \frac{25}{64}\,.$$

Mögliche rationale Nullstellen von g erfüllen $64x^3 - 80x^2 - 180x + 25 = 0$, der Zähler muss also ein Teiler von 25 und der Nenner ein Teiler von 64 sein. Man findet die Nullstelle $-5/4$ und damit

$$g = \Big(x + \frac{5}{4}\Big)\Big(x^2 - \frac{5}{2}x + \frac{5}{16}\Big)\,.$$

Die Diskriminante des zweiten Faktors ist $(-5/2)^2 - 4 \cdot 5/16 = 5$, also kein Quadrat, damit hat g genau eine Nullstelle, und die Galoisgruppe von f muss C_4 oder D_4 sein. Da sich alle Nullstellen von f durch eine ausdrücken lassen, ist $\#\,\mathrm{Gal}(f/\mathbb{Q}) = 4$, also ist $\mathrm{Gal}(f/\mathbb{Q}) = C_4$. ♣

6. Kreisteilungskörper und Kreisteilungspolynome

Bevor wir uns der Frage zuwenden können, welche Polynomgleichungen durch „Radikale“ (also Ausdrücke, die n-te Wurzeln enthalten können) gelöst werden können, müssen wir uns noch genauer mit dem einfachsten Fall einer „Radikalerweiterung“ beschäftigen, nämlich mit der Adjunktion von Einheitswurzeln.

DEF Kreisteilungskörper

6.1. **Definition.** Seien k ein Körper und $n \in \mathbb{Z}_{>0}$, sodass $\operatorname{char}(k) \nmid n$. Dann ist $X^n - 1 \in k[X]$ separabel. Der Zerfällungskörper K_n von $X^n - 1$ über k heißt der *n-te Kreisteilungskörper über k.* ♢

Man adjungiert also gerade die n-ten Einheitswurzeln zu k. Der Name „Kreisteilungskörper“ kommt daher, dass die n-ten Einheitswurzeln in $\mathbb{C}$ gerade die Ecken eines regelmäßigen, dem Einheitskreis einbeschriebenen, n-Ecks sind; sie teilen also den Einheitskreis in n gleiche Teile.

$X^n - 1$ ist separabel, weil die Ableitung nX^{n-1} nur bei null verschwindet (denn $n \neq 0$ in k), was aber keine Nullstelle von $X^n - 1$ ist. Also hat $X^n - 1$ nur einfache Nullstellen.

DEF primitive n-te Einheitswurzel

Wir erinnern uns daran, dass eine *primitive n-te Einheitswurzel* ein Element ζ der Ordnung n in der multiplikativen Gruppe ist; es gilt also $\zeta^n = 1$, aber $\zeta^m \neq 1$ für $1 \leq m < n$. Dann ist ζ ein Erzeuger der Gruppe der n-ten Einheitswurzeln. Alle primitiven n-ten Einheitswurzeln sind gegeben durch ζ^m mit $0 \leq m < n$ und $m \perp n$.

SATZ Kreisteilungskörper

6.2. **Satz.** *Sei k ein Körper mit $\operatorname{char}(k) \nmid n$ und sei K_n der n-te Kreisteilungskörper über k. Dann ist $k \subset K_n$ eine Galois-Erweiterung. Sei $\zeta \in K_n$ eine primitive n-te Einheitswurzel. Dann ist $K_n = k(\zeta)$ und*

$$\Phi\colon \operatorname{Aut}(K_n/k) \longrightarrow (\mathbb{Z}/n\mathbb{Z})^\times, \qquad \gamma \longmapsto \log_\zeta \gamma(\zeta)$$

ist ein injektiver Gruppenhomomorphismus. Für $m \in \mathbb{Z}$ sei dabei

$$\log_\zeta \zeta^m = m + n\mathbb{Z}\,.$$

Insbesondere ist $[K_n : k]$ ein Teiler von $\phi(n)$ (Eulersche ϕ-Funktion) und die Galoisgruppe $\operatorname{Aut}(K_n/k)$ ist abelsch.

Beweis. Der Zerfällungskörper eines separablen Polynoms ist eine Galois-Erweiterung. Da alle Nullstellen von $X^n - 1$ Potenzen von ζ sind, gilt $K_n = k(\zeta)$. Sei $\gamma \in \operatorname{Aut}(K_n/k)$. Dann ist $\gamma(\zeta)$ wieder eine primitive n-te Einheitswurzel, also ist $\gamma(\zeta) = \zeta^m$ mit $m \perp n$. Damit ist $\log_\zeta \gamma(\zeta) = m + n\mathbb{Z} \in (\mathbb{Z}/n\mathbb{Z})^\times$, also ist Φ als Abbildung wohldefiniert. Ist γ' ein weiteres Element von $\operatorname{Aut}(K_n/k)$, dann gilt $\gamma'(\zeta) = \zeta^{m'}$ für geeignetes m', und es folgt $(\gamma' \circ \gamma)(\zeta) = \gamma'(\zeta^m) = \gamma'(\zeta)^m = \zeta^{m'm}$, also gilt $\Phi(\gamma' \circ \gamma) = \Phi(\gamma')\Phi(\gamma)$. Damit ist Φ ein Gruppenhomomorphismus. Φ ist injektiv, denn $\ker(\Phi) = \{\mathrm{id}_{K_n}\}$: Gilt $\Phi(\gamma) = 1$, dann wird ζ von γ festgelassen; wegen $K_n = k(\zeta)$ muss dann $\gamma = \mathrm{id}_{K_n}$ sein.

Es folgt, dass $\operatorname{Aut}(K_n/k)$ zu einer Untergruppe von $(\mathbb{Z}/n\mathbb{Z})^\times$ isomorph und damit abelsch ist. Nach dem Satz von Lagrange haben wir dann

$$[K_n : k] = \#\operatorname{Aut}(K_n/k) \mid \#(\mathbb{Z}/n\mathbb{Z})^\times = \phi(n)\,. \qquad ❑$$

Es stellt sich jetzt die Frage, ob Φ surjektiv sein kann, d.h., ob $[K_n : k] = \phi(n)$ möglich ist. Im Rest dieses Abschnitts werden wir zeigen, dass das für $k = \mathbb{Q}$ der Fall ist.

Zuerst definieren wir ein Polynom Φ_n kleineren Grades als n, sodass K_n auch Zerfällungskörper von Φ_n ist.

6.3. **Definition.** Das Polynom

DEF Kreisteilungspolynom

$$\Phi_n = \prod_{\substack{\zeta\in\mathbb{C} \\ \text{pr. } n\text{-te EW}}} (X-\zeta) = \prod_{0\le m<n, m\perp n} (X - e^{2\pi i m/n}) \in \mathbb{C}[X]$$

heißt das n-te Kreisteilungspolynom. ♢

6.4. **Lemma.** *Das Kreisteilungspolynom hat folgende Eigenschaften:*

LEMMA Eigensch. Kreisteilungspolynom

(1) $\prod_{d|n} \Phi_d = X^n - 1$ *(d durchläuft die positiven Teiler von n).*
(2) $\Phi_n \in \mathbb{Z}[X]$, *und* Φ_n *ist normiert.*

Beweis.

(1) Jede n-te Einheitswurzel $\zeta \in \mathbb{C}$ ist eine primitive d-te Einheitswurzel für genau einen Teiler d von n (nämlich $d = \#\langle\zeta\rangle$). Die Nullstellen von $X^n - 1$ sind also gerade die Nullstellen aller Polynome Φ_d mit $d \mid n$ zusammen. Daraus, und weil alle vorkommenden Polynome normiert sind, folgt die Produktformel.
(2) Dass Φ_n normiert ist, ist klar. Wir zeigen $\Phi_n \in \mathbb{Z}[X]$ durch Induktion. Für $n = 1$ ist $\Phi_1 = X - 1 \in \mathbb{Z}[X]$. Sei also $n > 1$. Nach Teil (1) gilt dann
$$\Phi_n = \frac{X^n - 1}{\prod_{d|n, d<n} \Phi_d};$$
nach Induktionsvoraussetzung ist der Nenner ein normiertes Polynom mit ganzzahligen Koeffizienten. Polynomdivision zeigt, dass der Quotient auch ganzzahlige Koeffizienten hat. ❑

6.5. **Beispiele.** Die ersten paar Kreisteilungspolynome ergeben sich wie folgt:

BSP Kreisteilungspolynome

$$\begin{aligned}
\Phi_1 &= X - 1 \\
\Phi_2 &= X + 1 \\
\Phi_3 &= X^2 + X + 1 \\
\Phi_4 &= X^2 + 1 \\
\Phi_5 &= X^4 + X^3 + X^2 + X + 1 \\
\Phi_6 &= X^2 - X + 1
\end{aligned}$$

Allgemein gilt für Primzahlen p:

$$\Phi_p = \frac{X^p - 1}{X - 1} = X^{p-1} + X^{p-2} + \ldots + X + 1$$

und für Zweierpotenzen 2^m mit $m \ge 1$:

$$\Phi_{2^m} = X^{2^{m-1}} + 1\,.$$

Diese Beispiele lassen vermuten, dass die Koeffizienten von Φ_n immer nur -1, 0 oder 1 sind. Das ist aber falsch: Die Koeffizienten werden sogar beliebig groß. Das kleinste n, für das ein Koeffizient vom Betrag > 1 auftritt, ist $n = 105$. ♣

LEMMA

6.6. **Lemma.** *Sei k ein Körper und $\mathrm{char}(k) \nmid n$. Sei $\Phi_{n,k} \in k[X]$ das n-te Kreisteilungspolynom, als Polynom über k betrachtet. Dann ist der n-te Kreisteilungskörper K_n über k der Zerfällungskörper von $\Phi_{n,k}$, und $[K_n : k] = \phi(n)$ gilt genau dann, wenn $\Phi_{n,k}$ irreduzibel ist.*

Beweis. Sei ζ eine Nullstelle von $\Phi_{n,k}$. Dann ist ζ eine primitive n-te Einheitswurzel, also gilt $K_n = k(\zeta)$, und Letzterer ist der Zerfällungskörper von $\Phi_{n,k}$. Das Minimalpolynom f von ζ über k ist ein Teiler von $\Phi_{n,k}$; es gilt

$$[K_n : k] = \deg(f) \leq \deg(\Phi_{n,k}) = \phi(n)$$

mit Gleichheit genau dann, wenn $f = \Phi_{n,k}$ ist, also wenn $\Phi_{n,k}$ irreduzibel ist. ❑

Es bleibt zu zeigen, dass Φ_n über $\mathbb{Q}$ irreduzibel ist. Der entscheidende Beweisschritt wird im folgenden Lemma getan.

LEMMA

6.7. **Lemma.** *Sei $n \in \mathbb{Z}_{>0}$, sei $\zeta \in \mathbb{C}$ eine primitive n-te Einheitswurzel und sei $f \in \mathbb{Q}[X]$ das Minimalpolynom von ζ. Sei weiter p eine Primzahl mit $p \nmid n$. Dann ist $f(\zeta^p) = 0$.*

Beweis. Wir nehmen an, die Behauptung sei falsch. Da ζ^p eine Nullstelle von Φ_n ist, können wir $\Phi_n = fg$ schreiben mit normierten Polynomen f und g, sodass $g(\zeta^p) = 0$ ist. Da ζ eine Nullstelle von $g(X^p)$ ist, gilt $f \mid g(X^p)$. Aus dem Lemma von Gauß folgt, dass f und g ganzzahlige Koeffizienten haben. Wir können also die Gleichung $\Phi_n = fg$ modulo p betrachten: $\Phi_{n,\mathbb{F}_p} = \bar{f}\bar{g}$ in $\mathbb{F}_p[X]$, und $\bar{f}$ teilt $\bar{g}(X^p) = \bar{g}^p$ (hier verwenden wir $a^p = a$ für $a \in \mathbb{F}_p$ und $(x + y)^p = x^p + y^p$ in Charakteristik p). Auf der anderen Seite sind $\bar{f}$ und $\bar{g}$ teilerfremd, da $X^n - 1$ auch über $\mathbb{F}_p$ nur einfache Nullstellen hat. Das ist der gewünschte Widerspruch. ❑

SATZ
Kreisteilungspolynom irreduzibel

6.8. **Satz.** *Sei $n \in \mathbb{Z}_{>0}$. Dann ist $\Phi_n \in \mathbb{Q}[X]$ irreduzibel. Für den n-ten Kreisteilungskörper K_n über $\mathbb{Q}$ gilt $[K_n : \mathbb{Q}] = \phi(n)$, und $\mathrm{Aut}(K_n/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$.*

Beweis. Sei f ein irreduzibler Faktor von Φ_n. Sei $\zeta \in \mathbb{C}$ eine Nullstelle von f; dann ist ζ eine primitive n-te Einheitswurzel mit Minimalpolynom f. Nach Lemma 6.7 ist dann für jede Primzahl $p \nmid n$ auch ζ^p eine Nullstelle von f. Durch nochmalige Anwendung des Lemmas sieht man, dass dann auch ζ^{pq} für beliebige Primzahlen $p, q \nmid n$ eine Nullstelle von f ist; das kann dann auf beliebige Produkte von n nicht teilenden Primzahlen ausgedehnt werden. Da jede primitive n-te Einheitswurzel die Form ζ^m hat mit $0 \leq m < n$ und $m \perp n$ und da jedes solche m als Produkt von Primzahlen $p \nmid n$ geschrieben werden kann, sind *alle* primitiven n-ten Einheitswurzeln Nullstellen von f. Dann muss aber $f = \Phi_n$ sein; insbesondere ist Φ_n selbst irreduzibel.

Die restlichen Aussagen folgen aus Satz 6.3 und Lemma 6.6. ❑

C.F. Gauß
(1777–1855)

Anwendung:
Konstruierbarkeit des regulären n-Ecks mit Zirkel und Lineal.

Wir können das Erarbeitete verwenden, um folgenden Satz von Gauß zu beweisen:

SATZ Konstruierbarkeit des regulären n-Ecks

6.9. **Satz.** *Sei $n \in \mathbb{Z}_{>0}$. Das reguläre n-Eck ist genau dann mit Zirkel und Lineal konstruierbar, wenn $\phi(n) = 2^m$ ist für ein $m \geq 0$. Das bedeutet konkret, dass n die Form $n = 2^k p_1 p_2 \cdots p_l$ hat mit $k \geq 0$ und paarweise verschiedenen Fermatschen Primzahlen $p_1, p_2, \ldots, p_l$.*

DEF Fermatsche Primzahl

Zur Erinnerung: Eine *Fermatsche Primzahl* ist eine Primzahl der Form 2^m+1. Dabei muss m selbst eine Potenz von 2 sein. Die folgenden Fermatschen Primzahlen sind bekannt:

$$F_0 = 2^{2^0} + 1 = 3, \quad F_1 = 2^{2^1} + 1 = 5, \quad F_2 = 2^{2^2} + 1 = 17,$$
$$F_3 = 2^{2^3} + 1 = 257, \quad F_4 = 2^{2^4} + 1 = 65\,537\,.$$

Fermat hatte vermutet, dass $F_n = 2^{2^n} + 1$ immer eine Primzahl ist; das ist jedoch bereits für $n = 5$ falsch, wie schon Euler zeigte. Es ist unbekannt, ob es weitere Fermatsche Primzahlen gibt. Man weiß, dass $F_5, F_6, \ldots, F_{32}$ (und viele weitere F_n) keine Primzahlen sind.

P. de Fermat (1607–1665)

L. Euler (1707–1783)

Beweis. Wir hatten im letzten Semester gesehen, dass eine Zahl $\alpha \in \mathbb{C}$ genau dann konstruierbar ist, wenn $\mathbb{Q}(\alpha)$ aus $\mathbb{Q}$ durch sukzessive quadratische Erweiterungen erhalten werden kann. Eine notwendige Bedingung ist, dass $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ eine Potenz von 2 ist. Das reguläre n-Eck zu konstruieren bedeutet, den Winkel $2\pi/n$ zu konstruieren, und das ist dazu äquivalent, die primitive n-te Einheitswurzel $\zeta_n = e^{2\pi i/n}$ zu konstruieren. Nun haben wir gelernt, dass $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \phi(n)$ ist, also ist die angegebene Bedingung jedenfalls notwendig für die Konstruierbarkeit. Es bleibt zu zeigen, dass die Bedingung auch hinreichend ist. Sei also $\phi(n) = 2^m$. Die Gruppe $\Gamma = \mathrm{Aut}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$ ist abelsch von der Ordnung 2^m. Man findet dann (etwa mit Hilfe des Klassifikationssatzes für endliche abelsche Gruppen) leicht eine Folge

$$\{\mathrm{id}\} = G_0 \leq G_1 \leq G_2 \leq \ldots \leq G_m = \Gamma$$

von Untergruppen mit $(G_k : G_{k-1}) = 2$ für alle $k = 1, 2, \ldots, m$. Nach dem Satz 3.11 über die Galois-Korrespondenz gehört dazu eine Kette von Körpererweiterungen

$$\mathbb{Q} = L_m \subset L_{m-1} \subset \ldots \subset L_1 \subset L_0 = \mathbb{Q}(\zeta_n)$$

(mit $L_k = \mathcal{F}(G_k)$), sodass $[L_{k-1} : L_k] = 2$ ist. Das zeigt, dass ζ_n konstruierbar ist.

Die Charakterisierung der n mit $\phi(n) = 2^m$ ergibt sich so: Sei $n = 2^r p_1^{e_1} p_2^{e_2} \cdots p_l^{e_l}$ die Primfaktorzerlegung von n (mit $r \geq 0$, paarweise verschiedenen ungeraden Primzahlen p_j und $e_j \geq 1$). Dann ist

$$\begin{aligned}\phi(n) &= \phi(2^r)\phi(p_1^{e_1})\phi(p_2^{e_2}) \cdots \phi(p_l^{e_l}) \\ &= 2^{\max\{0,r-1\}} p_1^{e_1-1}(p_1-1) p_2^{e_2-1}(p_2-1) \cdots p_l^{e_l-1}(p_l-1)\,.\end{aligned}$$

Das ist genau dann einer Zweierpotenz, wenn das auf jeden Faktor zutrifft. Das bedeutet gerade $e_j = 1$ für alle j und $p_j = 2^{m_j} + 1$, also dass die p_j Fermatsche Primzahlen sind. ❑

7. Radikalerweiterungen und auflösbare Gruppen

DEF Radikalerweiterung

7.1. **Definition.** Sei k ein Körper. Eine *Radikalerweiterung* von k ist eine Körpererweiterung $k \subset K$, sodass es einen Turm von Körpererweiterungen

$$k = K_0 \subset K_1 \subset K_2 \subset \ldots \subset K_m$$

gibt mit $K \subset K_m$ und der Eigenschaft, dass es für jedes $j \in \{1, 2, \ldots, m\}$ ein Element $a_j \in K_{j-1}$ und eine Zahl $n_j \in \mathbb{Z}_{>0}$ mit $\mathrm{char}(k) \nmid n_j$ gibt, sodass K_j der Zerfällungskörper von $X^{n_j} - a_j$ über K_{j-1} ist. ♢

Man erhält also K_j aus K_{j-1} durch Adjunktion aller n_j-ter Wurzeln aus a_j. Das bedeutet, dass sich alle Elemente von K durch einen *Radikalausdruck* über k darstellen lassen, also eine Formel, die Elemente von k, die vier Grundrechenarten und n-te Wurzeln verwendet.

Die Ergebnisse aus Abschnitt 5 lassen sich dann so interpretieren, dass die Nullstellen eines Polynoms vom Grad höchstens 4 über k in einer Radikalerweiterung von k enthalten sind.

Unser Ziel in diesem Abschnitt wird es sein, das folgende Ergebnis zu beweisen:

SATZ Charakterisierung von Radikalerweiterungen

7.2. **Satz.** *Sei $k \subset K$ eine endliche Körpererweiterung und* $\mathrm{char}(k) = 0$. *Dann ist K eine Radikalerweiterung von k genau dann, wenn es eine endliche Galois-Erweiterung $k \subset L$ gibt, deren Galoisgruppe auflösbar ist, und sodass $K \subset L$ ist.*

Was ist eine auflösbare Gruppe?

DEF auflösbare Gruppe

7.3. **Definition.** Eine Gruppe G heißt *auflösbar*, wenn es eine Kette von Untergruppen

$$\{1\} = G_0 \leq G_1 \leq \ldots \leq G_n = G$$

in G gibt, sodass für alle $j \in \{1, 2, \ldots, n\}$ die Untergruppe G_{j-1} ein Normalteiler von G_j mit abelscher Faktorgruppe G_j/G_{j-1} ist. ♢

Es ist nicht schwer zu sehen, dass Untergruppen und Faktorgruppen von auflösbaren Gruppen wieder auflösbar sind.

LEMMA Untergruppe auflösbar

7.4. **Lemma.** *Sei G eine auflösbare Gruppe und $U \leq G$ eine Untergruppe. Dann ist U ebenfalls auflösbar.*

Beweis. Sei

$$\{1\} = G_0 \leq G_1 \leq \ldots \leq G_n = G$$

eine Kette von Untergruppen wie in Definition 7.3. Für $j \in \{0, 1, \ldots, n\}$ sei $U_j = U \cap G_j$. Dann ist

$$\{1\} = U_0 \leq U_1 \leq \ldots \leq U_n = U$$

eine Kette von Untergruppen von U. Für gegebenes $j \geq 1$ betrachten wir den Gruppenhomomorphismus $\phi_j \colon U_j = U \cap G_j \to G_j \to G_j/G_{j-1}$. Sein Kern ist $U_j \cap G_{j-1} = U \cap G_{j-1} = U_{j-1}$, also ist $U_{j-1} \triangleleft U_j$ und wir bekommen nach dem Homomorphiesatz für Gruppen einen *injektiven* Gruppenhomomorphismus $U_j/U_{j-1} \to G_j/G_{j-1}$. Da G_j/G_{j-1} nach Voraussetzung abelsch ist, gilt das auch für U_j/U_{j-1}, denn diese Gruppe ist zu einer Untergruppe von G_j/G_{j-1} isomorph. Damit ist U auflösbar. ❑

7.5. **Lemma.** *Sei G eine Gruppe und $N \triangleleft G$ ein Normalteiler. Dann ist G genau dann auflösbar, wenn sowohl N als auch die Faktorgruppe G/N auflösbar sind.*

LEMMA Faktorgruppe auflösbar

Beweis. "⇒": Sei G auflösbar. Nach Lemma 7.4 ist dann auch N auflösbar. Um zu zeigen, dass G/N auflösbar ist, sei $\phi\colon G \to G/N$ der kanonische Epimorphismus, und

$$\{1\} = G_0 \leq G_1 \leq \ldots \leq G_n = G$$

eine Kette von Untergruppen wie in Definition 7.3. Wir setzen $Q_j = \phi(G_j) \leq G/N$, dann ist

$$\{1_{G/N}\} = Q_0 \leq Q_1 \leq \ldots \leq Q_n = G/N$$

eine Kette von Untergruppen von G/N mit $Q_{j-1} \triangleleft Q_j$ für alle $j \in \{1, 2, \ldots, n\}$. Der Kern von $G_j \xrightarrow{\phi} Q_j \to Q_j/Q_{j-1}$ enthält G_{j-1}, also erhalten wir einen surjektiven Gruppenhomomorphismus $G_j/G_{j-1} \to Q_j/Q_{j-1}$. Damit ist Q_j/Q_{j-1} (als Quotient einer abelschen Gruppe) abelsch, und G/N ist auflösbar.

"⇐": Seien N und G/N auflösbar, und seien

$$\{1\} = N_0 \leq N_1 \leq \ldots \leq N_m = N \quad \text{und} \quad \{1_{G/N}\} = Q_0 \leq Q_1 \leq \ldots \leq Q_n = G/N$$

Ketten von Untergruppen wie in Definition 7.3. Für $j \in \{0, 1, \ldots, m\}$ sei $G_j = N_j$ und für $k \in \{0, 1, \ldots, n\}$ sei $G_{m+k} = \phi^{-1}(Q_k)$, wobei $\phi\colon G \to G/N$ der kanonische Epimorphismus ist (beide Definitionen von $G_m = N$ stimmen überein). Dann ist

$$\{1\} = G_0 \leq G_1 \leq \ldots \leq G_{m-1} \leq G_m = N \leq G_{m+1} \leq \ldots \leq G_{m+n} = G$$

eine Kette von Untergruppen von G mit $G_{j-1} \triangleleft G_j$ für alle $j \geq 1$, und es gilt $G_j/G_{j-1} = N_j/N_{j-1}$ für $j \leq m$ und $G_j/G_{j-1} \cong Q_{j-m}/Q_{j-m-1}$ für $j > m$; alle Quotienten sind nach Voraussetzung abelsch, also ist G auflösbar. ❑

7.6. **Lemma.** *Ist G endlich, dann kann man in Definition 7.3 sogar verlangen, dass die Quotienten G_j/G_{j-1} zyklisch (und von Primzahlordnung) sind.*

LEMMA zyklische Quotienten

Beweis. Durch Induktion über $\#G$. Klar für $\#G = 1$. Sei G also nichttrivial und auflösbar und sei $G_{n-1} \triangleleft G_n = G$ der letzte Schritt in der Kette von Untergruppen aus Definition 7.3; dabei sei ohne Einschränkung $G_{n-1} \neq G$. Nach Induktionsvoraussetzung können wir annehmen, dass die Quotienten G_j/G_{j-1} zyklisch von Primzahlordnung sind für $j < n$. Wenn G/G_{n-1} ebenfalls zyklisch ist, dann sind wir fertig. Anderenfalls gibt es eine echte Untergruppe $Q \subset G/G_{n-1}$ von Primzahlordnung (nach dem Satz von Cauchy oder dem Klassifikationssatz für endliche abelsche Gruppen). Da G/G_{n-1} abelsch ist, ist Q Normalteiler. Nach Induktionsvoraussetzung ($\#(G/G_{n-1})/Q < \#G/G_{n-1} \leq \#G$) gibt es eine Kette

$$\{1_{(G/G_{n-1})/Q}\} \leq Q'_1 \leq \ldots \leq Q'_m = (G/G_{n-1})/Q$$

mit Quotienten, die zyklisch von Primzahlordnung sind. Wie im Beweis von Lemma 7.5 können wir die Ketten zu einer Kette für G mit den gewünschten Eigenschaften zusammensetzen. ❑

Die Existenz der Lösungsformeln für Gleichungen von Grad ≤ 4 hängt mit folgender Tatsache zusammen:

SATZ Auflösbarkeit von S_n

7.7. **Satz.** *Sei $n \in \mathbb{Z}_{>0}$. Die symmetrische Gruppe S_n ist genau dann auflösbar, wenn $n \leq 4$ ist.*

Beweis. Die Gruppen S_1 und S_2 sind abelsch und daher trivialerweise auflösbar. Die Gruppe S_3 enthält den abelschen Normalteiler A_3 mit abelscher Faktorgruppe $S_3/A_3 \cong \mathbb{Z}/2\mathbb{Z}$, ist also ebenfalls auflösbar. In der S_4 haben wir die Kette $\{\mathrm{id}\} \leq V_4 \leq A_4 \leq S_4$ mit abelschen Faktorgruppen $S_4/A_4 \cong \mathbb{Z}/2\mathbb{Z}$, $A_4/V_4 \cong \mathbb{Z}/3\mathbb{Z}$ und $V_4 \cong (\mathbb{Z}/2\mathbb{Z}) \oplus (\mathbb{Z}/2\mathbb{Z})$.

Sei jetzt $n \geq 5$. Dann ist die Untergruppe $A_n \leq S_n$ eine nicht-abelsche einfache Gruppe. Wäre S_n auflösbar, dann müsste auch A_n auflösbar sein. Eine einfache Gruppe hat aber (definitionsgemäß) keine nicht-trivialen Normalteiler, also könnte die Länge der Untergruppen-Kette nur 1 sein. Die Faktorgruppe $A_n/\{\mathrm{id}\} \cong A_n$ ist aber nicht abelsch, also kann die Bedingung für Auflösbarkeit nicht erfüllt werden. ❑

N.H. Abel 1802–1829

Tatsächlich haben wir die im Beweis für $n = 3$ und $n = 4$ angegebenen Ketten von Untergruppen für die Konstruktion der Lösungsformeln benutzt.

Aus Satz 7.7 und Satz 7.2 folgt, dass die Nullstellen eines irreduziblen Polynoms vom Grad $n \geq 5$, dessen Galoisgruppe S_n (oder A_n) ist, nicht durch einen Radikalausdruck gegeben werden können. Dieses Resultat (Satz von Abel-Ruffini) wurde sehr viel später erhalten als die expliziten Formeln für niedrigere Grade, die ja aus dem 16. Jahrhundert stammen. Wie in vielen anderen ähnlichen Fällen liegt das daran, dass ein Unmöglichkeitsbeweis oft sehr viel schwieriger zu führen ist als der Nachweis, dass ein Objekt mit gewissen Eigenschaften (wie die expliziten Lösungsformeln) existiert: Auf die Lösungsformeln kann man mit genügend Intuition und Hartnäckigkeit kommen (und ihre Gültigkeit kann man dann ohne allzu große Schwierigkeiten beweisen), während man für den Beweis ihrer Nicht-Existenz erst einmal die Theorie der Radikalerweiterungen (und dafür wiederum die Galois-Theorie) aufbauen muss.

Ein wesentlicher Schritt im Beweis von Satz 7.2 wird durch das folgende Lemma geleistet.

LEMMA zyklische Galoisgruppe

7.8. **Lemma.** *Sei k ein Körper, $n \in \mathbb{Z}_{>0}$ mit $\mathrm{char}(k) \nmid n$; k enthalte eine primitive n-te Einheitswurzel ζ.*

(1) *Sei $a \in k$ und K der Zerfällungskörper von $X^n - a$ über k. Dann ist $k \subset K$ galoissch mit zyklischer Galoisgruppe, deren Ordnung ein Teiler von n ist.*

(2) *Sei $k \subset K$ eine galoissche Körpererweiterung mit zyklischer Galoisgruppe der Ordnung n. Dann gibt es $a \in k$, sodass K der Zerfällungskörper von $X^n - a$ über k ist.*

Beweis.

(1) Sei $\alpha \in K$ mit $\alpha^n = a$ eine Nullstelle von $X^n - a$. Dann sind alle Nullstellen von der Form $\zeta^j\alpha$ mit $j \in \{0, 1, \ldots, n-1\}$. Wegen $\zeta \in k$ ist $K = k(\alpha)$. Ein Automorphismus $\gamma \in \mathrm{Aut}(K/k)$ ist dann durch $\gamma(\alpha)$ festgelegt. Wir definieren $\Phi\colon \mathrm{Aut}(K/k) \to \mathbb{Z}/n\mathbb{Z}$, $\gamma \mapsto j + n\mathbb{Z}$, wobei $\gamma(\alpha) = \zeta^j\alpha$ ist. Nach den eben Gesagten ist Φ wohldefiniert und injektiv; außerdem ist Φ

ein Gruppenhomomorphismus: Seien $\gamma, \gamma' \in \mathrm{Aut}(K/k)$ mit $\Phi(\gamma) = j + n\mathbb{Z}$, $\Phi(\gamma') = j' + n\mathbb{Z}$. Dann ist

$$(\gamma \circ \gamma')(\alpha) = \gamma(\gamma'(\alpha)) = \gamma(\zeta^{j'}\alpha) = \zeta^{j'}\gamma(\alpha) = \zeta^{j'}\zeta^{j}\alpha = \zeta^{j+j'}\alpha\,,$$

also ist $\Phi(\gamma \circ \gamma') = (j + j') + n\mathbb{Z} = \Phi(\gamma) + \Phi(\gamma')$. Es folgt, dass $\mathrm{Aut}(K/k)$ zu einer Untergruppe von $\mathbb{Z}/n\mathbb{Z}$ isomorph ist; das sind aber (bis auf Isomorphie) genau die zyklischen Gruppen mit n teilender Ordnung.

(2) Sei $\gamma \in \mathrm{Aut}(K/k)$ ein Erzeuger (also $\mathrm{ord}(\gamma) = n$). $\gamma\colon K \to K$ ist k-linear, die Eigenwerte müssen n-te Einheitswurzeln sein. Als k-linearer Automorphismus endlicher Ordnung (die nicht durch $\mathrm{char}(k)$ teilbar ist) ist γ diagonalisierbar; seien $\alpha_1, \ldots, \alpha_n \in K$ k-linear unabhängige Eigenvektoren zu den Eigenwerten $\zeta^{m_1}, \ldots, \zeta^{m_n}$. Da $\mathrm{ord}(\gamma) = n$ ist und kein echter Teiler davon, gilt $\langle \zeta^{m_1}, \ldots, \zeta^{m_n} \rangle = \langle \zeta \rangle$. Es gibt also ganze Zahlen $l_1, \ldots, l_n$ mit $\zeta = (\zeta^{m_1})^{l_1} \cdots (\zeta^{m_n})^{l_n}$. Sei $\alpha = \alpha_1^{l_1} \cdots \alpha_n^{l_n}$. Dann ist

$$\begin{aligned}\gamma(\alpha) &= \gamma(\alpha_1^{l_1}) \cdots \gamma(\alpha_n^{l_n}) = \gamma(\alpha_1)^{l_1} \cdots \gamma(\alpha_n)^{l_n} \\ &= (\zeta^{m_1}\alpha_1)^{l_1} \cdots (\zeta^{m_n}\alpha_n)^{l_n} = (\zeta^{m_1})^{l_1} \cdots (\zeta^{m_n})^{l_n} \cdot \alpha_1^{l_1} \cdots \alpha_n^{l_n} = \zeta\alpha\,.\end{aligned}$$

Genauso sieht man, dass $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ Eigenvektoren zu den Eigenwerten $1, \zeta, \zeta^2, \ldots, \zeta^{n-1}$ sind. Damit sind $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ eine k-Basis von K; insbesondere ist $K = k(\alpha)$. Außerdem gilt für $a = \alpha^n$, dass $\gamma(a) = \gamma(\alpha^n) = \gamma(\alpha)^n = (\zeta\alpha)^n = \alpha^n = a$ ist; es folgt $a \in k$. Das zeigt, dass K der Zerfällungskörper von $X^n - a$ über k ist. ❑

Um das auf unser Problem anwenden zu können, müssen wir sicherstellen, dass k „genügend viele“ Einheitswurzeln enthält. Damit das funktioniert, brauchen wir noch etwas mehr Information aus der Galoistheorie.

SATZ Kompositum von Galois-Erweiterungen

7.9. **Satz.** *Sei $k \subset K$ eine Körpererweiterung und seien L_1 und L_2 Zwischenkörper, die endlich und galoissch über k sind. Dann ist auch das Kompositum L_1L_2 über k galoissch, und $\mathrm{Aut}(L_1L_2/k) \to \mathrm{Aut}(L_1/k) \times \mathrm{Aut}(L_2/k)$, $\gamma \mapsto (\gamma|_{L_1}, \gamma|_{L_2})$, ist ein injektiver Gruppenhomomorphismus.*

Beweis. Nach Satz 3.3 gibt es separable (irreduzible) Polynome $f_1, f_2 \in k[X]$, sodass L_1 und L_2 die Zerfällungskörper von f_1 und f_2 über k sind. Dann ist L_1L_2 der Zerfällungskörper von f_1f_2, und nach Lemma 3.8 ist L_1L_2 über k galoissch.

Die angegebene Abbildung ist wohldefiniert, da L_1 und L_2 galoissch über k sind, siehe Satz 3.9. Dass die Abbildung ein Gruppenhomomorphismus ist, ist klar. Ist $\gamma \in \mathrm{Aut}(L_1L_2/k)$ im Kern, dann folgt $\gamma|_{L_1} = \mathrm{id}_{L_1}$ und $\gamma|_{L_2} = \mathrm{id}_{L_2}$. Weil sich die Elemente von L_1L_2 rational über k durch die Elemente von L_1 und L_2 ausdrücken lassen, folgt $\gamma = \mathrm{id}_{L_1L_2}$. Der Kern ist also trivial. ❑

SATZ Translation von Galois-Erweiterungen

7.10. **Satz.** *Sei $k \subset K$ eine Körpererweiterung und seien L_1 und L_2 Zwischenkörper, sodass L_1 endlich und galoissch über k ist. Dann ist L_1L_2 galoissch über L_2, und $\mathrm{Aut}(L_1L_2/L_2) \to \mathrm{Aut}(L_1/k)$, $\gamma \mapsto \gamma|_{L_1}$, ist ein injektiver Gruppenhomomorphismus. Insbesondere ist $\mathrm{Aut}(L_1L_2/L_2)$ isomorph zu einer Untergruppe von $\mathrm{Aut}(L_1/k)$.*

Beweis. Nach Satz 3.3 gibt es ein separables (irreduzibles) Polynom $f \in k[X]$, sodass L_1 der Zerfällungskörper von f über k ist. Dann ist L_1L_2 der Zerfällungskörper von f über L_2, also ist nach Lemma 3.8 L_1L_2 galoissch über L_2.

Dass die angegebene Abbildung wohldefiniert und ein Gruppenhomomorphismus ist, sieht man wie im Beweis von Satz 7.9. Ist $\gamma \in \mathrm{Aut}(L_1L_2/L_2)$ im Kern, dann folgt $\gamma|_{L_1} = \mathrm{id}_{L_1}$; außerdem ist $\gamma|_{L_2} = \mathrm{id}_{L_2}$ nach Definition von $\mathrm{Aut}(L_1L_2/L_2)$. Wie oben folgt $\gamma = \mathrm{id}_{L_1L_2}$; der Kern ist also trivial. ❑

Damit können wir schon einmal eine Richtung von Satz 7.2 beweisen:

7.11. **Lemma.** *Sei* $\mathrm{char}(k) = 0$ *und* $k \subset K$ *galoissch mit auflösbarer Galoisgruppe. Dann ist* $k \subset K$ *eine Radikalerweiterung.*

LEMMA auflösbare Erweiterung ist Radikalerweiterung

Beweis. Sei $G = \mathrm{Aut}(K/k)$ und sei $\{1\} = G_0 \leq G_1 \leq \ldots \leq G_n = G$ eine Kette von Untergruppen wie in Definition 7.3. Nach Bemerkung 7.6 können wir annehmen, dass die Quotienten G_j/G_{j-1} alle zyklisch sind. Sei N das kleinste gemeinsame Vielfache aller ihrer Ordnungen. Sei L der N-te Kreisteilungskörper (hier brauchen wir $\mathrm{char}(k) = 0$ oder wenigstens $\mathrm{char}(k) \nmid N$), dann ist nach Satz 7.10 KL galoissch über L und die Galoisgruppe G' ist als Untergruppe von $\mathrm{Aut}(K/k)$ ebenfalls auflösbar. Sei $\{1\} = G'_0 \leq G'_1 \leq \ldots \leq G'_m = G'$ eine Kette von Untergruppen mit zyklischen Quotienten von N teilender Ordnung und seien $L = L_m \subset L_{m-1} \subset \ldots \subset L_1 \subset L_0 = KL$ die zugehörigen Fixkörper. Nach Satz 3.11 ist L_{j-1} galoissch über L_j mit zyklischer Galoisgruppe G'_j/G'_{j-1} der Ordnung $n_j \mid N$. Da die N-ten Einheitswurzeln in L vorhanden sind, folgt nach Lemma 7.8, dass es $a_j \in L_j$ gibt, sodass L_{j-1} der Zerfällungskörper von $X^{n_j} - a_j$ über L_j ist. Außerdem ist L der Zerfällungskörper von $X^N - 1$ über k. Wegen $K \subset KL$ ist K eine Radikalerweiterung. ❑

Für die andere Richtung müssen wir noch ein wenig mehr arbeiten.

7.12. **Lemma.** *Ist* $k \subset K$ *eine Radikalerweiterung, dann gibt es eine Radikalerweiterung* $k \subset L$ *mit* $K \subset L$*, die galoissch ist.*

LEMMA Radikalerweiterung in Galois-Erweiterung

Beweis. Sei $k = K_0 \subset K_1 \subset K_2 \subset \ldots \subset K_m$ ein Körperturm wie in Definition 7.1 mit $K \subset K_m$. Wir führen den Beweis durch Induktion über m. Im Fall $m = 0$ ist nichts zu zeigen (denn $K = k$). Sei also $m > 0$. Wir können die Induktionsvoraussetzung auf K_{m-1} anwenden: Es gibt eine galoissche Körpererweiterung $k \subset L'$ mit $K_{m-1} \subset L'$, die eine Radikalerweiterung ist. Sei K_m der Zerfällungskörper von $X^n - a$ über K_{m-1} (mit $a \in K_{m-1}$). Dann ist $a \in L'$; sei $\{a_1 = a, a_2, a_3, \ldots, a_l\}$ die Bahn von a unter $\mathrm{Aut}(L'/k)$. Dann ist $f = (X^n - a_1)(X^n - a_2)\cdots(X^n - a_l) \in k[X]$, denn die Koeffizienten von f sind unter $\mathrm{Aut}(L'/k)$ invariant, da die Faktoren nur permutiert werden. Sei L'' der Zerfällungskörper von f über k, dann ist $k \subset L''$ galoissch. Sei schließlich $L = L'L''$ das Kompositum von L' und L''. Nach Satz 7.9 ist $k \subset L$ galoissch. Außerdem ist L auch der Zerfällungskörper von f über L', enthält also K_m als Zerfällungskörper von $X^n - a_1$ über $K_{m-1} \subset L'$. Es bleibt zu zeigen, dass $k \subset L$ eine Radikalerweiterung ist. Das ergibt sich daraus, dass wir einen Körperturm

$$L' = L_0 \subset L_1 \subset L_2 \subset \ldots \subset L_l = L$$

haben, wo L_j der Zerfällungskörper von $X^n - a_j$ über L_{j-1} ist, zusammen mit der Aussage, dass $k \subset L'$ eine Radikalerweiterung ist. ❑

Das folgende Lemma ergibt den letzten fehlenden Schritt im Beweis von Satz 7.2:

LEMMA Radikalerweiterung auflösbar

7.13. **Lemma.** *Ist $k \subset K$ eine galoissche Radikalerweiterung, dann ist* $\mathrm{Aut}(K/k)$ *auflösbar.*

Beweis. Sei $k = K_0 \subset K_1 \subset K_2 \subset \ldots \subset K_m$ ein Körperturm wie in Definition 7.1 mit $K \subset K_m$. Nach Lemma 7.12 können wir annehmen, dass $k \subset K_m$ ebenfalls galoissch ist. Es genügt dann zu zeigen, dass $\mathrm{Aut}(K_m/k)$ auflösbar ist, denn $\mathrm{Aut}(K/k)$ ist eine Faktorgruppe von $\mathrm{Aut}(K_m/k)$, also nach Lemma 7.5 ebenfalls auflösbar.

Der Beweis geht durch Induktion über m. Der Fall $m = 0$ ist klar (die triviale Gruppe ist auflösbar). Sei also $m > 0$. Dann ist K_1 der Zerfällungskörper eines Polynoms $X^n - a \in k[X]$ (mit $\mathrm{char}(k) \nmid n$) und damit eine Galois-Erweiterung von k. Nach Induktionsvoraussetzung, angewandt auf die galoissche Radikalerweiterung $K_1 \subset K_m$, ist die Untergruppe $\mathrm{Aut}(K_m/K_1)$ von $\mathrm{Aut}(K_m/k)$ auflösbar. Nach Lemma 7.5 genügt es also zu zeigen, dass auch die Faktorgruppe $\mathrm{Aut}(K_1/k)$ auflösbar ist. Dazu beachten wir, dass K_1 den n-ten Kreisteilungskörper k' über k enthält (denn eine primitive n-te Einheitswurzel ergibt sich als Quotient geeigneter Nullstellen von $X^n - a$). Wir haben also den Turm $k \subset k' \subset K_1$. Nach Proposition 6.2 ist $k \subset k'$ galoissch mit abelscher Galoisgruppe, und nach Lemma 7.8 ist $k' \subset K_1$ mit abelscher (sogar zyklischer) Galoisgruppe; insgesamt folgt (wieder mit Lemma 7.5), dass $\mathrm{Aut}(K_1/k)$ auflösbar ist. ❑

Der Beweis von Satz 7.2 geht dann so:

Beweis. „⇒“: Sei $k \subset K$ eine Radikalerweiterung. Nach Lemma 7.12 gibt es eine galoissche Radikalerweiterung $k \subset L$ mit $K \subset L$. Nach Lemma 7.13 ist die Galoisgruppe von $k \subset L$ auflösbar.

„⇐“: Sei $\mathrm{char}(k) = 0$ und $k \subset L$ endlich und galoissch mit auflösbarer Galoisgruppe, sodass $K \subset L$. Nach Lemma 7.11 ist $k \subset L$ eine Radikalerweiterung. Dann ist aber $k \subset K$ ebenfalls eine Radikalerweiterung (man kann denselben Körperturm verwenden wie für $k \subset L$). ❑

Daraus ergibt sich unmittelbar:

FOLG Auflösung durch Radikale

7.14. **Folgerung.** *Sei k ein Körper mit* $\mathrm{char}(k) = 0$ *und $f \in k[X]$. Dann lassen sich die Nullstellen von f genau dann durch Radikalausdrücke über k darstellen, wenn die Galoisgruppe* $\mathrm{Gal}(f/k)$ *auflösbar ist.*

FOLG nicht auflösbare Polynome

7.15. **Folgerung.** *Für jedes $n \geq 5$ gibt es Polynome $f \in \mathbb{Q}[X]$, deren Nullstellen nicht durch Radikalausdrücke darstellbar sind.*

Beweis. Wir konstruieren ein Polynom f mit $\mathrm{Gal}(f/\mathbb{Q}) = S_5$. Da S_5 nicht auflösbar ist, sind die Nullstellen von f nicht durch Radikalausdrücke darstellbar. Für beliebiges $n \geq 5$ betrachten wir ein Polynom der Form fg mit $g \in \mathbb{Q}[X]$ normiert vom Grad $n - 5$. Die Konstruktion von f wird durch das folgende Lemma erledigt. ❑

LEMMA $\mathrm{Gal}(f/\mathbb{Q}) = S_p$

7.16. **Lemma.** *Sei p eine ungerade Primzahl.*

(1) *Ist G eine Untergruppe von S_p, sodass G ein Element der Ordnung p und eine Transposition enthält, dann ist $G = S_p$.*

(2) *Ist $f \in \mathbb{Q}[X]$ normiert vom Grad p und irreduzibel, sodass f genau $p-2$ reelle und ein Paar konjugiert komplexer Nullstellen hat, dann hat f Galoisgruppe $\mathrm{Gal}(f/\mathbb{Q}) = S_p$.*

(3) *Polynome wie in Teil (2) existieren.*

Beweis.

(1) Nach eventueller Änderung der Nummerierung können wir annehmen, dass die Transposition $\tau = (1\ 2)$ in G ist. Das Element der Ordnung p erzeugt eine Untergruppe, die transitiv auf $\{1, 2, \dots, p\}$ operiert; es gibt also ein Element der Ordnung p in G, das 1 auf 2 abbildet. Wiederum nach eventueller Änderung der Nummerierung der Elemente $3, 4, \dots, p$ können wir annehmen, dass der p-Zykel $\sigma = (1\ 2\ 3\ \dots\ p)$ in G ist. Für $1 \le m \le p-2$ ist $\sigma^m \circ \tau \circ \sigma^{-m} = (m+1\ \ m+2)$, also enthält G alle Transpositionen $(1\ 2)$, $(2\ 3)$, $\dots$, $(p-1\ p)$. Diese Transpositionen erzeugen S_p; es folgt, dass $G = S_p$ ist.

(2) Sei $G = \mathrm{Gal}(f/\mathbb{Q})$. Da f irreduzibel ist, ist p ein Teiler von $\#G$, also enthält G ein Element der Ordnung p (Satz von Cauchy oder Sylow). Sei $\mathbb{Q} \subset K \subset \mathbb{C}$ der Zerfällungskörper von f. Die komplexe Konjugation induziert durch Einschränkung auf K ein Element von G, das die beiden konjugiert komplexen Nullstellen von f vertauscht und die übrigen Nullstellen fest lässt; dieses Element entspricht also einer Transposition. Nach Teil (1) folgt $G = S_p$.

(3) Wir betrachten zunächst das folgende Polynom vom Grad p:

$$\begin{aligned} h &= X(X^2-2)(X^2-4)\cdots(X^2-(p-3))(X^2+2p^2) \\ &= X(X^2+2p^2)\prod_{j=1}^{(p-3)/2}(X^2-2j) \\ &= X^p + \Big(2p^2 - \frac{(p-1)(p-2)}{4}\Big)X^{p-2} + \dots \in \mathbb{Q}[X]\,. \end{aligned}$$

Es hat offensichtlich genau $p-2$ reelle Nullstellen. Seine $(p-2)$-te Ableitung ist

$$h^{(p-2)} = \frac{p!}{2}X^2 + (p-2)!\Big(2p^2 - \frac{(p-1)(p-3)}{4}\Big)$$

und damit ohne reelle Nullstelle. Außerdem gilt für ungerade Zahlen $1 \le 2m+1 \le p-2$, dass

$$h(\pm\sqrt{2m+1}) = \pm\sqrt{2m+1}(2m+1+2p^2)\prod_{j=1}^{(p-3)/2}(2(m-j)+1)$$

Betrag $\ge 2p^2$ hat. Da h nur einfache Nullstellen hat, und zwar an den Stellen $-\sqrt{p-3}, \dots, -\sqrt{4}, -\sqrt{2}, 0, \sqrt{2}, \dots, \sqrt{p-3}$, müssen die Vorzeichen an den $p-1$ Stellen

$$-\sqrt{p-2}, \dots, -\sqrt{3}, -1, 1, \sqrt{3}, \dots, \sqrt{p-2}$$

alternieren. Wir setzen jetzt $f = h + 2$. Das Polynom h ist ungerade und $h \equiv X^p \bmod 2$. Es folgt $f \equiv X^p \bmod 2$ und $f(0) = 2$; damit ist f irreduzibel nach dem Eisenstein-Kriterium. Da $2 < 2p^2$ ist, hat f an den $p-1$ oben angegebenen Stellen dasselbe Vorzeichen wie h; nach dem Zwischenwertsatz hat f also mindestens $p-2$ reelle Nullstellen. Auf der anderen Seite kann f nicht mehr als $p-2$ reelle Nullstellen haben, denn sonst hätte die $(p-2)$-te Ableitung von f zwei reelle Nullstellen (Induktion mit dem Satz von Rolle), was wegen $f^{(p-2)} = h^{(p-2)}$ nicht stimmt. ❑

Für $p = 5$ kann man z.B. auch $f = X^5 - 6X + 1$ nehmen (denn f ist irreduzibel mod 5 und hat genau drei reelle Nullstellen: ≥ 3 mit Zwischenwertsatz, ≤ 3, da $f' = 5X^4 - 6$ nur zwei reelle Nullstellen hat).

7.17. **Bemerkung.** Man kann für jedes n (nicht nur für Primzahlen) Polynome über $\mathbb{Q}$ konstruieren, deren Galoisgruppe S_n (oder auch A_n) ist. Die weitergehende Frage, ob *jede* endliche Gruppe (bis auf Isomorphie) als Galoisgruppe eines Polynoms über $\mathbb{Q}$ auftritt, das sogenannte *Umkehrproblem der Galoistheorie*, ist jedoch offen.

Auf der anderen Seite ist leicht einzusehen, dass jede endliche Gruppe als Galoisgruppe irgendeiner Galois-Erweiterung auftritt: Sei G eine endliche Gruppe mit $\#G = n$, dann ist G isomorph zu einer Untergruppe der S_n (betrachte die Operation von G auf sich selbst durch Translation). Ist $p > n$ eine Primzahl, dann ist S_n isomorph zu einer Untergruppe von S_p (die aus den Permutationen besteht, die gewisse $p - n$ Elemente fest lassen). Sei $\mathbb{Q} \subset K$ eine Galois-Erweiterung mit $\mathrm{Aut}(K/\mathbb{Q}) \cong S_p$ und sei $k = \mathcal{F}(G)$ der Fixkörper von G (als Untergruppe von S_p betrachtet). Dann ist nach dem Satz 3.11 über die Galois-Korrespondenz $k \subset K$ galoissch mit $\mathrm{Aut}(K/k) \cong G$.

Wenn man sich bei der Definition von Radikalerweiterungen auf die Adjunktion von *Quadratwurzeln* (statt beliebiger n-ter Wurzeln) beschränkt, dann erhält man genau die (mit Zirkel und Lineal) *konstruierbaren* Elemente, vgl. die „Einführung in die Algebra“. Mit im Wesentlichen dem gleichen Beweis (sogar einfacher, weil die zweiten Einheitswurzeln ± 1 in jedem Körper der Charakteristik 0 schon vorhanden sind) erhält man dafür die folgende Aussage:

SATZ Charakterisierung von Konstruierbarkeit

7.18. **Satz.** *Sei $k \subset \mathbb{C}$ ein Teilkörper und sei $\alpha \in \mathbb{C}$. Dann sind äquivalent:*

(1) *α ist ausgehend von den Elementen von k mit Zirkel und Linear konstruierbar.*

(2) *Es gibt eine Galois-Erweiterung $k \subset K$ mit $K \subset \mathbb{C}$ und $\alpha \in K$, sodass $\#\,\mathrm{Aut}(K/k) = 2^n$ ist für ein $n \in \mathbb{Z}_{\geq 0}$.*

(3) *α ist algebraisch über k und für das Minimalpolynom $f \in k[X]$ von α über k gilt $\#\,\mathrm{Gal}(f/k) = 2^n$ für ein $n \in \mathbb{Z}_{\geq 0}$.*

Der Beweis liefert zunächst, dass die Galoisgruppe auflösbar sein muss (mit sukzessiven Quotienten $\cong \mathbb{Z}/2\mathbb{Z}$, was bedeutet, dass die Gruppenordnung eine Potenz von 2 sein muss). Der Schritt, der im Beweis noch fehlt, ist folgende Aussage (für $p = 2$):

SATZ *p*-Gruppen sind auflösbar

7.19. **Satz.** *Sei p eine Primzahl und G eine endliche p-Gruppe, d.h., $\#G = p^n$ für ein $n \in \mathbb{Z}_{\geq 0}$. Dann ist G auflösbar. Genauer: Es gibt eine Kette $\{1\} = G_0 \leq G_1 \leq \ldots \leq G_n = G$ von Untergruppen mit $G_{j-1} \triangleleft G_j$ und $G_j/G_{j-1} \cong \mathbb{Z}/p\mathbb{Z}$ für alle $1 \leq j \leq n$.*

Wir zeigen zuerst ein Lemma. Das *Zentrum* einer Gruppe G war definiert als

$$Z(G) = \{g \in G \mid \forall g' \in G \colon gg' = g'g\}\,.$$

Man beachte die folgenden beiden Eigenschaften:

- Die Elemente von $Z(G)$ sind gerade die Fixpunkte der Operation von G auf sich selbst durch Konjugation (denn $gh = hg \iff hgh^{-1} = g$).
- Jede Untergruppe von $Z(G)$ ist ein Normalteiler von G.

LEMMA *p*-Gruppe hat nicht-triviales Zentrum

7.20. **Lemma.** *Sei p eine Primzahl und G eine nicht-triviale endliche p-Gruppe. Dann ist $Z(G)$ nicht-trivial. Insbesondere hat G einen Normalteiler N der Ordnung $\#N = p$.*

Jede Gruppe der Ordnung p ist zyklisch, also gilt dann $N \cong \mathbb{Z}/p\mathbb{Z}$.

Beweis. Wir betrachten die Operation von G auf sich selbst durch Konjugation: $g * h = ghg^{-1}$. Die Bahnen dieser Operation haben Längen, die Teiler von $\#G$ sind; die Längen sind also Potenzen von p. Es folgt, dass die Anzahl der Fixpunkte durch p teilbar ist. Da das neutrale Element ein Fixpunkt ist, gibt es mindestens p Fixpunkte. Die Fixpunkte sind aber gerade die Elemente des Zentrums, also ist $Z(G)$ nicht-trivial. Da $p \mid \#Z(G)$, hat $Z(G)$ eine Untergruppe der Ordnung p; jede Untergruppe von $Z(G)$ ist ein Normalteiler von G. ❑

Beweis von Satz 7.19. Induktion über n. Im Fall $n = 0$ ist G trivial, und es ist nichts zu zeigen. Sei also $n > 0$. Nach Lemma 7.20 hat G einen Normalteiler G_1 mit $\#G_1 = p$. Sei $G' = G/G_1$, dann ist $\#G' = p^{n-1}$; nach Induktionsvoraussetzung gibt es also eine Kette

$$\{1_{G'}\} = G'_0 \leq G'_1 \leq \ldots \leq G'_{n-1} = G'$$

von Untergruppen von G' mit $G'_{j-1} \triangleleft G'_j$ und $G'_j/G'_{j-1} \cong \mathbb{Z}/p\mathbb{Z}$ für $1 \leq j \leq n-1$. Sei $\phi \colon G \to G'$ der kanonische Epimorphismus. Wir setzen $G_j = \phi^{-1}(G'_{j-1})$ für $1 \leq j \leq n$ (für $j = 1$ erhalten wir dieselbe Gruppe G_1 wie oben) und $G_0 = \{1_G\}$, dann gilt $G_j/G_{j-1} \cong G'_{j-1}/G'_{j-2} \cong \mathbb{Z}/p\mathbb{Z}$ für $2 \leq j \leq n$ und $G_1/G_0 \cong G_1 \cong \mathbb{Z}/p\mathbb{Z}$. ❑

Sei $\alpha \in \mathbb{C}$ algebraisch mit Minimalpolynom f über $\mathbb{Q}$ vom Grad n. Die Bedingung „n ist Zweierpotenz“ ist *notwendig* für die Konstruierbarkeit von α (denn da f irreduzibel ist, gilt $n \mid \#\operatorname{Gal}(f/\mathbb{Q})$ — das haben wir in der „Einführung in die Algebra“ für verschiedene Unmöglichkeitsbeweise benutzt — aber *nicht hinreichend*. Wir haben gesehen, dass es irreduzible Polynome f vom Grad 4 über $\mathbb{Q}$ gibt mit $\operatorname{Gal}(f/\mathbb{Q}) \cong S_4$ oder A_4, aber $\#S_4 = 24$ und $\#A_4 = 12$ sind keine Zweierpotenzen.

Literatur

[Fi] Gerd Fischer: *Lehrbuch der Algebra,* Vieweg, 2008. Signatur 80/SK 200 F529 L5. Online-Zugriff unter http://dx.doi.org/10.1007/978-3-8348-9455-7

[KM] Christian Karpfinger und Kurt Meyberg: *Algebra. Gruppen - Ringe - Körper,* Spektrum Akademischer Verlag, 2010. Online-Zugriff unter http://dx.doi.org/10.1007/978-3-8274-2601-7.