Vertiefung der Algebra

Wintersemester 2011/2012

Universität Bayreuth

Michael Stoll

Inhaltsverzeichnis

25. Einführung

Diese Vorlesung setzt die Vorlesung „Einführung in die Algebra“ fort. Die Nummerierung der Abschnitte in diesem Skript führt deshalb die Nummerierung aus dem Skript für die „Einführung in die Algebra“ weiter.

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 kann. 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.

Während eines großen Teils unserer Zeit werden wir uns mit der sogenannten *Galois-Theorie* beschäftigen. 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.

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

25.1. **Beispiel.** Wir setzen $k = \mathbb{Q}$ und betrachten das Polynom $f = X^4 - 17 \in \mathbb{Q}[X]$. Das Eisenstein-Kriterium 12.10 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, i, $i^2 = -1$ und $i^3 = -i$. Wir erhalten also

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

(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 $\zeta_n = e^{2\pi i/n}$ eine primitive $n$te Einheitswurzel ist.) Wegen $\alpha_3 = -\alpha_1$ und $\alpha_4 = -\alpha_2$ ist

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

Die letzte Gleichheit folgt aus

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

und

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

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:

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

Den zweiten Faktor können wir leicht bestimmen: Für *einfache* algebraische Körpererweiterungen $k \subset k(a)$ gilt $[k(a) : k] = \deg(m)$, wenn $m \in k[X]$ das Minimalpolynom von a über k ist (vgl. 21.3–5). 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

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

zu bestimmen. Dies ist ebenfalls eine einfache Körpererweiterung, denn wir adjungieren i zu $\mathbb{Q}(\sqrt[4]{17})$. Da i Nullstelle von X^2+1 ist, ist der Grad dieser Erweiterung höchstens $\deg(X^2 + 1) = 2$. Da 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 $\mathbb{Q} \subset K$. Diese sind die Elemente der Untergruppe

$$\mathrm{Aut}(K/\mathbb{Q}) = \{\sigma \in \mathrm{Aut}(K) \mid \forall x \in \mathbb{Q} : \sigma(x) = x\} \leq \mathrm{Aut}(K)$$

der Automorphismengruppe von K. Allgemein ist ein Automorphismus einer Körpererweiterung $k \subset K$ ein Automorphismus von K (also ein bijektiver Ringhomomorphismus $\sigma : K \to K$ — man erinnere sich daran, dass ein Ringhomomorphismus von einem Körper in einen nichttrivialen Ring stets injektiv ist; das Entscheidende ist also die Surjektivität), der k „elementweise fest lässt“; es muss also $\sigma(x) = x$ gelten für alle $x \in k$. Für $k = \mathbb{Q}$ ist das automatisch der Fall, da die Elemente von $\mathbb{Q}$ aus 0 und 1 (die beide fest bleiben) durch die vier Grundrechenarten gebildet werden können.

Ist $k \subset K$ eine *endliche* Körpererweiterung, dann ist jeder Ringhomomorphismus $\sigma : K \to K$, der k elementweise fest lässt, bereits ein Automorphismus der Körpererweiterung. Es folgt nämlich, dass σ ein Endomorphismus des endlichdimensionalen k-Vektorraums K ist (Beweis als Übung); außerdem ist σ injektiv und damit auch bijektiv.

Wie können wir die Elemente von $\mathrm{Aut}(K/\mathbb{Q})$ beschreiben? Offenbar genügt es, die Bilder der Erzeuger $\sqrt[4]{17}$ und 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 i? Dazu ein Lemma:

25.2. **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.*

Beweis. Sei $f = a_n X^n + a_{n-1}X^{n-1} + \ldots + a_1 X + a_0$. 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

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

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

25.3. **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 $\sigma(\alpha) = \beta$.*

Beweis. Das ist ein Spezialfall von Satz 22.2. □

Wir können das hier wie folgt anwenden:

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

Die erste Aussage folgt daraus, dass f auch über $\mathbb{Q}(i)$ irreduzibel ist (denn es gilt $[\mathbb{Q}(i, \sqrt[4]{17}) : \mathbb{Q}(i)] = 4 = \deg(f)$), 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

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

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	$i\alpha$	$-\alpha$	$-i\alpha$	α	α	α	$i\alpha$	$-\alpha$	$-i\alpha$	$-i\alpha$
i	i	i	i	i	$-i$	i	$-i$	$-i$	$-i$	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	$i\alpha$	$-\alpha$	$-i\alpha$	α	$i\alpha$	$-\alpha$	$-i\alpha$
$i\alpha$	$i\alpha$	$-\alpha$	$-i\alpha$	α	$-i\alpha$	α	$i\alpha$	$-\alpha$
$-\alpha$	$-\alpha$	$-i\alpha$	α	$i\alpha$	$-\alpha$	$-i\alpha$	α	$i\alpha$
$-i\alpha$	$-i\alpha$	α	$i\alpha$	$-\alpha$	$i\alpha$	$-\alpha$	$-i\alpha$	α

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

25.4. **Lemma.** *Sei $k \subset K$ eine Körpererweiterung, $\sigma \in \mathrm{Aut}(K/k)$ und $f \in k[X]$ normiert. Sei $N_f = \{\alpha \in K \mid f(\alpha) = 0\}$ 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.*

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 25.2 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 können also einem Polynom $f \in \mathbb{Q}[X]$ eine Gruppe zuordnen.

25.5. **Satz und Definition.** *Sei $f \in \mathbb{Q}[X]$ ein nicht-konstantes Polynom und $K \subset \mathbb{C}$ der Zerfällungskörper von f in $\mathbb{C}$. Dann gilt $\#\,\mathrm{Aut}(K/\mathbb{Q}) = [K : \mathbb{Q}]$, und $\mathrm{Aut}(K/\mathbb{Q})$ 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 ist.*

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

Beweis. Die Aussage „$\#\,\mathrm{Aut}(K/\mathbb{Q}) = [K : \mathbb{Q}]$“ wurde in Bemerkung 22.6 gezeigt. Die zweite Aussage wurde in Lemma 25.4 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 $\mathrm{Gal}(f/\mathbb{Q}) = D_4$.

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

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

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

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

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

Dieser Körper $Z(U)$ heißt auch der *Fixkörper* von U, weil er aus den Elementen 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

$$a + b\alpha + c\alpha^2 + d\alpha^3 + ei + fi\alpha + gi\alpha^2 + hi\alpha^3$$

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

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

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

- $Z(\langle\sigma^2\tau\rangle) = \mathbb{Q}(i\sqrt[4]{17})$.
  Es gilt $b = d = e = g = 0$; die verbleibenden Terme sind Potenzen von $i\alpha$.
- $Z(\langle\sigma^3\tau\rangle) = \mathbb{Q}((1-i)\sqrt[4]{17})$.
  Das ist analog zu $\langle\sigma\tau\rangle$.
- $Z(\langle\sigma\rangle) = \mathbb{Q}(i)$,
  denn $\sigma(x) = x \iff b = c = d = f = g = h = 0$.
- $Z(\langle\sigma^2, \tau\rangle) = \mathbb{Q}(\sqrt{17})$.
  Fixpunkt von σ^2 und τ zu sein bedeutet $b = d = e = f = g = h = 0$, also haben die Elemente die Form $a + c\alpha^2 = a + c\sqrt{17}$.
- $Z(\langle\sigma^2, \sigma\tau\rangle) = \mathbb{Q}(i\sqrt{17})$.
  Ähnlich wie eben findet man die Bedingung $b = c = d = e = f = h = 0$; die Elemente haben die Form $a + gi\alpha^2 = a + gi\sqrt{17}$.
- $Z(D_4) = \mathbb{Q}$.
  Wenn ein Element sowohl unter σ als auch unter τ fest bleibt, folgt $b = c = d = e = f = g = h = 0$.

26. 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 werden wir separable Elemente und Erweiterungen einführen und untersuchen und insbesondere auch diesen „Satz vom primitiven Element“ beweisen. Wir orientieren uns hier an [KM, Kap. 24].

26.1. **Definition.** Sei K ein Körper, $0 \neq f \in K[x]$ 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.

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.

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

Beweis. Wir können ohne Einschränkung annehmen, dass f normiert ist. Sei $K \subset L$ ein Zerfällungskörper von f. Ist f nicht separabel, dann hat f eine mehrfache Nullstelle α in L. Damit ist α eine Nullstelle von $f' \in K[x]$ (denn $f = (x-\alpha)^2 g$ impliziert $f' = (x-\alpha)(2g + (x-\alpha)g')$), also muss das Minimalpolynom f von α über K ein Teiler von f' sein. Auf der anderen Seite ist $\deg(f') < \deg(f)$, daher bleibt nur die Möglichkeit, dass $f' = 0$ ist. Damit ist „$\Leftarrow$“ gezeigt.

Ist umgekehrt f separabel, dann sei $\alpha \in L$ eine einfache Nullstelle von f; wir schreiben $f = (x-\alpha)g$ in $L[x]$. Dann gilt

$$f' = g + (x-\alpha)g', \qquad \text{also} \qquad f'(\alpha) = g(\alpha) \neq 0,$$

denn α ist eine einfache Nullstelle von f. Das zeigt $f' \neq 0$. □

Aus dem Beweis ergibt sich auch, dass entweder *alle* Nullstellen von f in L einfach sind oder *keine*.

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

Beweis. In Charakteristik 0 gilt für f nicht konstant, dass $\deg(f') = \deg(f) - 1$ ist (Lemma 12.13, (4)); es folgt $f' \neq 0$, also ist f nach Lemma 26.2 separabel. □

26.4. **Beispiel.** Nicht separable Polynome sind also nicht so einfach zu finden. Das Standardbeispiel sieht so aus: Sei $K = \mathbb{F}_p(y)$ der Quotientenkörper der Polynomringe $\mathbb{F}_p[y]$ 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.

Das lässt sich verallgemeinern:

26.5. **Lemma.** *Sei K ein Körper der Charakteristik $p > 0$ und $f \in K[x]$ irreduzibel. Dann ist f genau dann nicht separabel, wenn es ein Polynom $g \in K[x]$ gibt mit $f = g(x^p)$.*

Beweis. Nach Lemma 26.2 genügt es zu zeigen, dass $f' = 0$ ist genau dann, wenn $f = g(x^p)$ ist für ein $g \in K[x]$. Gilt $f = g(x^p)$, dann ist $f' = px^{p-1}g'(x^p) = 0$. Für die Gegenrichtung sei $f = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$. Dann ist

$$f' = na_n x^{n-1} + (n-1)a_{n-1}x^{n-2} + \ldots + a_1\,.$$

Ist $f' = 0$, dann folgt $ma_m = 0$ für alle $0 \leq m \leq n$. Ist m kein Vielfaches von p, dann ist $m \neq 0$ in K und es folgt $a_m = 0$. Also hat f die Form

$$a_{pn'}x^{pn'} + a_{p(n'-1)}x^{p(n'-1)} + \ldots + a_p x^p + a_0 = g(x^p)$$

mit

$$g = a_{pn'}x^{n'} + a_{p(n'-1)}x^{n'-1} + \ldots + a_p x + a_0\,. \qquad \square$$

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

26.6. **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*.

26.7. **Proposition.** *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 separabel über k genau dann, wenn $k(a^p) = k(a)$ ist.*
(3) *a ist separabel über k genau dann, wenn die Körpererweiterung $k \subset k(a)$ separabel ist.*

Beweis. Der Fall von Charakteristik 0 folgt aus Folgerung 26.3.

Sei also $\mathrm{char}(k) = p > 0$. Wir haben den Zwischenkörper $k \subset k(a^p) \subset k(a)$. Ist a separabel über k, dann ist a auch separabel über $k(a^p)$ (denn das Minimalpolynom von a über $k(a^p)$ teilt das Minimalpolynom von a über k). Sei f das Minimalpolynom von a über $k(a^p)$, dann ist f ein Teiler von $x^p - a^p \in k(a^p)[x]$, denn a ist eine Nullstelle dieses Polynoms. Auf der anderen Seite gilt in $k(a)[x]$, dass $x^p - a^p = (x-a)^p$ ist. Da f keine mehrfachen Nullstellen hat, folgt $f = x - a$, also $a \in k(a^p)$ und damit $k(a) = k(a^p)$. Ist a nicht separabel über k, dann hat das Minimalpolynom h von a über k die Form $h = g(x^p)$ nach Lemma 26.5. Da h irreduzibel ist, muss auch g irreduzibel sein (eine Faktorisierung von g würde sich auf h übertragen), und da $g(a^p) = h(a) = 0$ ist, ist g das Minimalpolynom von a^p über k. Es folgt

$$[k(a) : k(a^p)] = \frac{[k(a) : k]}{[k(a^p) : k]} = \frac{\deg(h)}{\deg(g)} = p\,,$$

also gilt hier $k(a^p) \subsetneq k(a)$.

In der dritten Aussage gilt „$\Leftarrow$“ nach Definition. Für die Gegenrichtung ist nur im Fall $\mathrm{char}(k) = p > 0$ etwas zu zeigen. Sei $b \in k(a)$ und sei $f \in k(b)[x]$ das Minimalpolynom von a über $k(b)$. Wir schreiben $\phi : K \to K$ für den Frobenius-Endomorphismus $\lambda \mapsto \lambda^p$ und $f^\phi \in k(b^p)[x]$ für das Polynom, das man erhält, wenn man ϕ auf die Koeffizienten von f anwendet. Dann gilt

$$f^\phi(a^p) = f^\phi(\phi(a)) = \phi(f(a)) = \phi(0) = 0\,,$$

also hat f^ϕ die Nullstelle a^p. Damit gilt

$$[k(a^p) : k(b^p)] \leq \deg(f^\phi) = \deg(f) = [k(a) : k(b)]\,,$$

also folgt unter Verwendung von $k(a) = k(a^p)$:

$$[k(b) : k(b^p)] = \frac{[k(a) : k(b^p)]}{[k(a) : k(b)]} = \frac{[k(a^p) : k(b^p)]}{[k(a) : k(b)]} \leq 1\,.$$

Das heißt aber $k(b) = k(b^p)$, also ist b separabel über k. □

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

26.8. **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.

26.9. **Satz (Steinitz).** *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 $\phi : K \to K$, $a \mapsto a^p$, surjektiv ist.*
(3) *Ist K endlich, dann ist K vollkommen.*

Beweis. Der Fall von Charakteristik 0 folgt wieder aus Folgerung 26.3.

Wir betrachten den Fall $\mathrm{char}(K) = p > 0$. Wir nehmen zunächst an, dass ϕ nicht surjektiv ist. Dann gibt es $a \in K$ mit $a \neq b^p$ für alle $b \in K$. Wir betrachten eine Körpererweiterung L von K, in der $x^p - a$ eine Nullstelle α hat. Es gilt dann $\alpha \notin K$, aber $\alpha^p = a \in K$, also ist $K(\alpha^p) = K \subsetneq K(\alpha)$ und damit ist α nicht

separabel über K nach Proposition 26.7. Jetzt nehmen wir an, dass φ surjektiv ist. Sei $f \in K[x]$ ein irreduzibles Polynom. Wenn f nicht separabel wäre, dann gäbe es $g \in K[x]$ mit $f = g(x^p)$. Wir schreiben $g = a_n x^n + \ldots + a_1 x + a_0$, dann ist $f = a_n x^{pn} + \ldots + a_1 x^p + a_0$. Da φ surjektiv ist, gibt es $b_0, b_1, \ldots, b_n \in K$ mit $b_j^p = a_j$ für $0 \leq j \leq n$. Dann ist

$$f = b_n^p x^{np} + b_{n-1}^p x^{(n-1)p} + \ldots + b_1^p x^p + b_0^p = (b_n x^n + b_{n-1} x^{n-1} + \ldots + b_1 x + b_0)^p \,,$$

also kann f nicht irreduzibel sein, ein Widerspruch. Also muss f separabel sein, und K ist vollkommen.

Ist K endlich, dann gilt $\mathrm{char}(K) = p$ für eine Primzahl p. Der Frobenius-Endomorphismus φ ist ein Körperhomomorphismus und als solcher injektiv. Weil K endlich ist, ist ϕ dann auch surjektiv, also ist K nach Teil (2) vollkommen. □

26.10. **Beispiel.** Ein unvollkommener Körper ist also nicht so leicht zu finden. Wie Beispiel 26.4 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.

26.11. **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. Damit ist die multiplikative Gruppe zyklisch (siehe Folgerung 15.5), also $k(a,b)^\times = \langle c \rangle$ für ein $c \in k(a,b)$. Dann gilt natürlich auch $k(c) = k(a,b)$. 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 zu zeigen, dass $a, b \in k(c)$. 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 $b \in k(c)$. □

26.12. **Beispiel.** Wir kommen zurück zu unserem Beispiel $\mathbb{Q} \subset K = \mathbb{Q}(\sqrt[4]{17}, i)$. Mit $\lambda = 1$ sehen wir, dass alle Elemente $i^m \sqrt[4]{17} \pm i$ (mit $0 \leq m \leq 3$) paarweise verschieden sind. Da wir uns in Charakteristik 0 befinden, sind alle Elemente separabel. Es folgt $K = \mathbb{Q}(\sqrt[4]{17} + i)$.

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

Insbesondere hat jede endliche separable Körpererweiterung $k \subset K$ ein ***primitives Element*** *c (d.h. mit $K = k(c)$) und ist damit einfach.*

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 $c' \in k(a, b_1, \dots, b_{n-1})$ mit $k(a, b_1, \dots, b_{n-1}) = k(c')$; insbesondere ist c' algebraisch über k. Dann haben wir

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

Nach Lemma 26.11 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:

26.14. **Satz (Transitivität der Separabilität).** *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 und sind die Erweiterungen $k \subset K$ und $K \subset L$ separabel, dann ist auch $k \subset L$ separabel.*

Beweis. Es ist nur im Fall positiver Charakteristik p etwas zu zeigen. Zum Beweis der ersten Aussage benutzen wir Proposition 26.7. Nach Voraussetzung gilt $k(a^p) = k(a)$ und $k(a)(b^p) = k(a)(b)$. Es folgt $k(a^p, b^p) = k(a, b^p) = k(a, b)$. Ähnlich wie beim Beweis von Teil (3) von Proposition 26.7 haben wir $[k(a^p, b^p) : k(b^p)] \leq [k(a, b) : k(b)]$, und wie dort folgt $k(b^p) = k(b)$, also ist b separabel über k.

Zum Beweis der zweiten Aussage sei $b \in L$; wir müssen zeigen, dass b separabel über k ist. Sei dazu f das Minimalpolynom von b über K und K' der von den Koeffizienten von f über k erzeugte Zwischenkörper. Dann ist K' eine von endlich vielen separablen Elementen erzeugte Erweiterung von k; nach dem Satz vom primitiven Element 26.13 ist also $K' = k(a)$ mit einem $a \in K' \subset K$; a ist separabel über k, da die Körpererweiterung $k \subset K$ separabel ist. Nach Teil (1) folgt, dass auch b separabel über k ist. □

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

26.15. **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.*

Beweis. Nach dem Satz vom primitiven Element 26.13 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“ $\phi : K \to L$ 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. Nach Satz 22.2 (vergleiche auch Lemma 25.3) gibt es zu jeder dieser Nullstellen einen eindeutig bestimmten k-Homomorphismus $\phi : K \to L$. □

Wir beweisen noch ein allgemeines Lemma.

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

(1) $$k = \mathcal{F}(G) = \{a \in K \mid \gamma(a) = a \text{ für alle } \gamma \in G\}$$
ist ein Unterkörper 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 $[K : k] = \#G$.*

$\mathcal{F}(G)$ heißt der *Fixkörper* von G. Die Schreibweise variiert in der Literatur; wir verwenden hier die von [KM].

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 26.13 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 26.15 $\#G \leq [K : k]$, also muss Gleichheit gelten. □

26.17. **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.*

Beweis. Die Aussage „$\#\operatorname{Aut}(K/k) \leq [K : k]$“ ist als Spezialfall $L = K$ in Satz 26.15 enthalten. Hat K die angegebene Eigenschaft, dann ist im Beweis von Satz 26.15 $L = K$ 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 26.16, (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 26.16 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. □

26.18. **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*.

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

26.19. **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 also $\deg(f) = 2$ annehmen, also $f = x^2 + ax + b$ mit $a, b \in K$. Dann ist aber $f = (x - \alpha)(x + a + \alpha)$ in $K[x]$, also zerfällt f in $K[x]$ in Linearfaktoren.

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.

26.20. **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.

27. Galois-Erweiterungen

27.1. **Definition.** Eine Körpererweiterung $k \subset K$ heißt *galoissch* oder *Galois-Erweiterung*, wenn gilt $k = \mathcal{F}(\mathrm{Aut}(K/k))$. 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“!

Wir können endliche Galois-Erweiterungen charakterisieren:

27.2. **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 26.16 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 26.16 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 26.17 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 26.13 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 26.15. □

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]).

27.3. **Beispiel.** Ist $\mathrm{char}(k) \neq 2$ 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 $\mathrm{Aut}(K/k) = \{\mathrm{id}_K, \tau\}$ für einen Automorphismus $\tau \neq \mathrm{id}_K$. Wegen $\mathrm{char}(k) \neq 2$ 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: $\tau(a + bi) = a - bi$.

27.4. **Beispiel.** Zu Beginn dieses Semesters haben wir ausführlich die Körpererweiterung $\mathbb{Q} \subset K = \mathbb{Q}(\sqrt[4]{17}, i)$ studiert. Da K der Zerfällungskörper von $x^4 - 17$ ist, ist diese Körpererweiterung galoissch; für die Galoisgruppe hatten wir $\mathrm{Aut}(K/\mathbb{Q}) \cong D_4$ erhalten.

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.

27.5. **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 $\phi : K \to K$, $x \mapsto x^q$ 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 $\phi \in \mathrm{Aut}(K/k)$, und es gilt $\mathcal{F}(\mathrm{Aut}(K/k)) \subset \mathcal{F}(\langle\phi\rangle) = k$. Damit ist $k \subset K$ jedenfalls galoissch und es folgt zusätzlich, dass $\mathrm{Aut}(K/k) = \langle\phi\rangle$ ist, denn

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

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

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

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

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.

27.7. **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. Wir können f durch seinen quadratfreien Anteil f_0 (also das Produkt der verschiedenen irreduziblen Faktoren von f ohne Vielfachheit) ersetzen. Da f separabel ist, hat f_0 nur einfache Nullstellen. Wir hatten in Bemerkung 22.6 gesehen, dass in diesem Fall $\#\operatorname{Aut}(K/k) = [K : k]$ 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?

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

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

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 $\operatorname{Aut}(K/k)/\operatorname{Aut}(K/L)$.

Beweis. Wir zeigen erst einmal, dass $L \subset K$ galoissch ist. Nach Satz 27.2 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 27.7 ist also $L \subset K$ galoissch.

Da $k \subset K$ nach Satz 27.2 separabel ist, gilt das auch für $k \subset L$. Wiederum nach Satz 27.2 ist $k \subset L$ also genau dann galoissch, wenn $k \subset L$ normal ist. Wir zeigen, dass das äquivalent ist zu $\forall \gamma \in \operatorname{Aut}(K/k) : \gamma(L) = L$.

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 $\gamma \in \operatorname{Aut}(K/k)$. 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 26.16 folgt, dass $\operatorname{Aut}(K/k)$ auf den Nullstellen von f in K transitiv operiert. Da $\gamma(L) = L$ ist für alle $\gamma \in \operatorname{Aut}(K/k)$ 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 $\gamma \in \operatorname{Aut}(K/k)$ folgt aus $\gamma(L) = L$, dass die Einschränkung $\gamma|_L \in \operatorname{Aut}(L/k)$ ist; die Abbildung Φ ist also wohldefiniert, und es ist klar, dass Φ ein Gruppenhomomorphismus ist. Die Definition von $\operatorname{Aut}(K/L)$ liefert $\ker(\Phi) = \operatorname{Aut}(K/L)$, also ist $\operatorname{Aut}(K/L)$ ein Normalteiler von $\operatorname{Aut}(K/k)$. Es bleibt die Surjektivität von Φ zu zeigen. Nach dem Homomorphiesatz für Gruppen ist das Bild von Φ isomorph zu $\operatorname{Aut}(K/k)/\operatorname{Aut}(K/L)$. Es gilt dann

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

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

27.9. **Bemerkung und Definition.** Ist $k \subset K$ eine endliche separable Körpererweiterung, dann ist $K = k(\alpha)$ eine einfache Körpererweiterung nach dem Satz vom primitiven Element 26.13. 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:

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

Es gibt auch eine Abbildung in der anderen Richtung, nämlich

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

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

27.10. **Satz über die Galois-Korrespondenz.** *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 Proposition 27.8 ist $L \subset K$ für jedes L galoissch, also ist nach Satz 27.2 $\#\mathcal{U}(L) = [K : L]$. Nach Lemma 26.16 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 Proposition 27.8 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

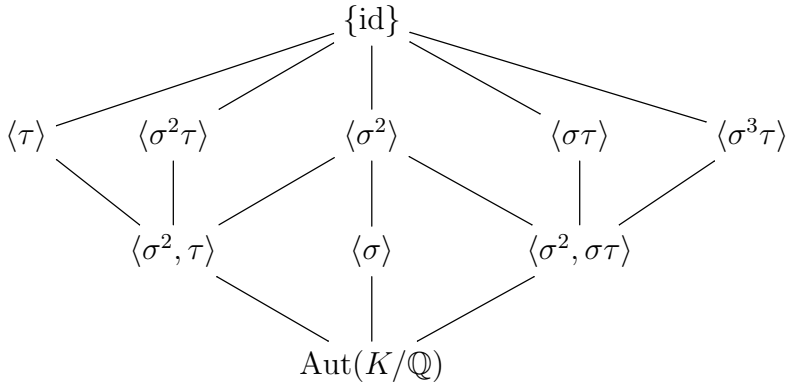
Implikation überlegen wir Folgendes. Seien $\gamma, \phi \in \mathrm{Aut}(K/k)$. Dann gilt

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

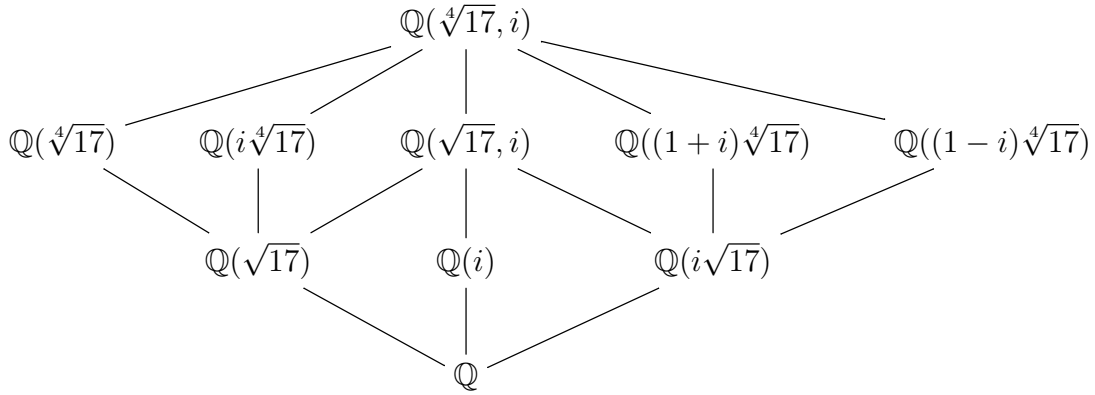
Das bedeutet $\mathrm{Aut}(K/\gamma(L)) = \gamma\,\mathrm{Aut}(K/L)\gamma^{-1} = \mathrm{Aut}(K/L)$, wobei wir benutzen, dass $\mathrm{Aut}(K/L)$ ein Normalteiler ist. Es folgt $\mathcal{U}(L) = \mathcal{U}(\gamma(L))$, nach dem ersten Teil des Satzes also $L = \gamma(L)$ (für alle $\gamma \in \mathrm{Aut}(K/k)$). Nach Proposition 27.8 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.

27.11. **Beispiel.** Für die Galois-Erweiterung $\mathbb{Q} \subset K = \mathbb{Q}(\sqrt[4]{17}, i)$ hatten wir bereits die Untergruppen der Galoisgruppe $\mathrm{Aut}(K/\mathbb{Q}) \cong D_4$ klassifiziert und die zugehörigen Fixkörper bestimmt. Satz 27.10 sagt uns nun, dass es keine weiteren Zwischenkörper gibt. Dem „Untergruppenverband“



der Diedergruppe D_4 (den wir hier „auf dem Kopf stehend“ wiedergegeben haben, also mit den kleineren Gruppen oberhalb der größeren) entspricht genau der „Zwischenkörperverband“



von $\mathbb{Q} \subset K$.

28. 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:

28.1. **Satz.** *Sei 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:

28.2. **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 28.1 lässt sich verallgemeinern. Dazu definieren wir die Diskriminante für ein beliebiges normiertes Polynom.

28.3. **Definition.** Sei 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

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

Dann ist die *Diskriminante* von f definiert als

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

28.4. **Lemma.** *Sei k ein Körper und $f \in k[x]$ ein normiertes Polynom vom Grad n.*

(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 $\operatorname{disc}(f) \in \mathcal{F}(\operatorname{Aut}(K/k)) = k$. □

28.5. **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 28.1 lautet jetzt wie folgt.

28.6. **Satz.** *Sei k ein Körper 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 28.4 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 $\varepsilon(\sigma) = 1$, 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 $\operatorname{char}(k) \neq 2$):

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

29. Lösungsformeln für Gleichungen vom Grad 3 und 4

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

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

wobei K der Zerfällungskörper von f ist; die Körpererweiterung $L \subset K$ ist galoissch mit Galoisgruppe $A_3 \cong \mathbb{Z}_3$. 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 $\sigma \in \operatorname{Aut}(K/L)$ ein Erzeuger. Dann ist $\sigma : K \to K$ 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 $\operatorname{char}(k) \neq 3$) 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 $\sigma(\alpha^3) = (\omega\alpha)^3 = \omega^3\alpha^3 = \alpha^3$ 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 $\sqrt{\operatorname{disc}(f)}$ 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 $\operatorname{disc}(f)$. 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

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

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

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

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:

29.1. **Satz („Cardanosche" Lösungsformel für kubische Gleichungen).** *Sei k ein Körper mit $\operatorname{char}(k) \neq 2,3$ 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

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

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. Man rechnet 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:

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

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.

29.2. **Beispiel.** Sei $k = \mathbb{Q}$, $K = \mathbb{C}$ und $f = x^3 - 3x + 1 \in \mathbb{Q}[x]$. Wir haben also $p = -3$ und $q = 1$. Mit $\omega = e^{2\pi i/3} = (-1+\sqrt{-3})/2$ ergibt das $d = (p/3)^3+(q/2)^2 = -1+1/4 = -3/4$, also $\delta = \sqrt{-3}/2$. Für α haben wir $\alpha = \sqrt[3]{-1/2 + \sqrt{-3}/2} = \sqrt[3]{\omega}$, 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.

29.3. **Satz.** *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.*

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 komplexe 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 $-4(\operatorname{Im}\beta)^2 < 0$. □

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:

29.4. **Satz (Lösungsformeln für Gleichungen vom Grad 4).** *Sei k ein Körper mit $\operatorname{char}(k) \neq 2, 3$ 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 29.1 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 29.1. □

29.5. **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

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

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:

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

Beweis. Sei K ein Zerfällungskörper von f über k. Dann ist $\mathrm{Gal}(f/k) = \mathrm{Aut}(K/k)$. Wenn diese Gruppe transitiv auf den Nullstellen von f operiert, dann ist f nach Lemma 26.16 irreduzibel. Ist die Operation nicht transitiv, dann führt jede Bahn wiederum nach Lemma 26.16 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 $\sigma \in \mathrm{Gal}(f/k) \subset S_4$ 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 $\mathrm{Gal}(f/K) \subset D_4$. (Beachte, dass die kubische Resolvente g keine mehrfachen Nullstellen hat, denn $\mathrm{disc}(g) = \mathrm{disc}(f) \neq 0$.) Sind alle drei Nullstellen von g in k, dann folgt entsprechend $\mathrm{Gal}(f/k) \subset V_4$.

29.7. **Satz.** *Sei k ein Körper und $f \in k[x]$ irreduzibel vom Grad 4 mit $d = \mathrm{disc}(f) \neq 0$. Sei weiter g die kubische Resolvente von f und n die Anzahl der Nullstellen von g in k. Dann ergibt sich die Galoisgruppe* $\mathrm{Gal}(f/k)$ *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.

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

(1) $f = x^4 + x + 1$. Dann ist $g = x^3 - 4x + 1$ mit $\mathrm{disc}(f) = \mathrm{disc}(g) = -4(-4)^3 - 27 \cdot 1^2 = 256 - 27 = 229$. g ist irreduzibel (da ohne rationale Nullstelle; nur ± 1 kommen in Frage) und $\mathrm{disc}(f)$ ist kein Quadrat, also ist $\mathrm{Gal}(f/\mathbb{Q}) = S_4$.

(2) $f = x^4+3x^2-7x+4$. Dann ist $g = x^3-6x^2-7x+49$. Zur Berechnung der Diskriminante betrachten wir $g(x+2) = x^3 - 19x + 19$, also ist $\operatorname{disc}(f) = \operatorname{disc}(g) = -4(-19)^3 - 27 \cdot 19^2 = 17689 = 133^2$. Außerdem ist $g(x+2)$ irreduzibel nach Eisenstein mit $p = 19$, also ist $\operatorname{Gal}(f/\mathbb{Q}) = A_4$.

(3) $f = x^4 - 2$. Dann ist $g = x^3 + 8x$; g zerfällt in die irreduziblen Faktoren x und $x^2 + 8$, 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 $\operatorname{Gal}(f/\mathbb{Q})$, das genau zwei Nullstellen vertauscht, damit kann $\operatorname{Gal}(f/\mathbb{Q})$ nicht C_4 sein, also ist $\operatorname{Gal}(f/\mathbb{Q}) = D_4$.

(4) $f = x^4 + 1$. Dann ist $g = X^3 - 4x = x(x-2)(x+2)$ und hat drei rationale 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 $\#\operatorname{Gal}(f/\mathbb{Q}) = \#[K:\mathbb{Q}] = \deg(f) = 4$. 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 $\operatorname{Gal}(f/\mathbb{Q})$ transitiv auf den Nullstellen. Es gibt also ein Element $\sigma \in \operatorname{Gal}(f/\mathbb{Q})$, 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 $\#\operatorname{Gal}(f/\mathbb{Q}) = 4$, also ist $\operatorname{Gal}(f/\mathbb{Q}) = C_4$.

30. 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.

30.1. **Definition.** Sei 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.

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 $m \perp n$.

30.2. **Proposition.** *Sei k ein Körper,* $\mathrm{char}(k) \nmid n$ *und 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*

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

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 $\mathrm{Aut}(K_n/k)$ 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 $\gamma \in \mathrm{Aut}(K_n/k)$. 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 $\mathrm{Aut}(K_n/k)$, 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 $\Phi(\gamma' \circ \gamma) = \Phi(\gamma')\Phi(\gamma)$. Also ist Φ ein Gruppenhomomorphismus. Φ ist injektiv, denn $\ker(\Phi) = \{\mathrm{id}_{K_n}\}$: Gilt $\Phi(\gamma) = 1$, dann wir ζ von γ festgelassen; wegen $K_n = k(\zeta)$ muss dann $\gamma = \mathrm{id}_{K_n}$ sein.

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

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

Eine natürliche Frage, die sich jetzt stellt, ist, 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.

30.3. **Definition und Satz.** Das Polynom

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

heißt das n-te Kreisteilungspolynom.

Es hat folgende Eigenschaften:

(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. □

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

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

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 $m \geq 1$:

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

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 $n = 105$.

30.5. **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.

30.6. **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. □

30.7. **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 30.6 ist dann für jede Primzahl $p \nmid n$ auch ζ^p eine Nullstelle von f. Durch nochmalige Anwendung des Lemmas sieht man, dass 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 $0 \le m < n$ und $m \perp n$ und m als Produkt solcher Primzahlen 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 30.3 und Lemma 30.5. □

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

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

30.8. **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 $m \ge 0$. Das bedeutet konkret, dass n die Form $n = 2^k p_1 p_2 \cdots p_l$ hat mit $k \ge 0$ und paarweise verschiedenen Fermatschen Primzahlen $p_1, p_2, \ldots, p_l$.*

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 schon für $n = 5$ falsch, wie Euler zeigte. Es ist unbekannt, ob es weitere Fermatsche Primzahlen gibt.

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 27.10 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. □

31. Radikalerweiterungen und auflösbare Gruppen

31.1. **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 29 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:

31.2. **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?

31.3. **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 G_{j-1} ein Normalteiler von G_j mit abelscher Faktorgruppe G_j/G_{j-1} ist, für alle $j \in \{1, 2, \ldots, n\}$.

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

31.4. **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 31.3. 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 $\phi_j : U_j = U \cap G_j \to G_j \to G_j/G_{j-1}$. 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. □

31.5. **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.*

Beweis. "⇒": Sei G auflösbar. Nach Lemma 31.4 ist dann auch N auflösbar. Um zu zeigen, dass G/N auflösbar ist, sei $\phi : G \to G/N$ der kanonische Epimorphismus, und

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

eine Kette von Untergruppen wie in Definition 31.3. 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 31.3. 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 $\phi : G \to G/N$ 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. □

31.6. **Bemerkung.** *Ist G endlich, dann kann man in Definition 31.3 sogar annehmen, dass die Quotienten G_j/G_{j-1} zyklisch (und von Primzahlordnung) sind.*

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 31.3; 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 31.5 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:

31.7. **Proposition.** *Sei $n \in \mathbb{Z}_{>0}$. Die symmetrische Gruppe S_n ist auflösbar genau dann, 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 (Beweis evtl. später in der Vorlesung). 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. □

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

Aus Proposition 31.7 und Satz 31.2 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 31.2 wird durch das folgende Lemma geleistet.

31.8. **Lemma.** *Sei k ein Körper, $n \in \mathbb{Z}_{>0}$ mit $\operatorname{char}(k) \nmid n$; 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 $j \in \{0, 1, \dots, n-1\}$. Wegen $\zeta \in k$ ist $K = k(\alpha)$. Ein Automorphismus $\gamma \in \operatorname{Aut}(K/k)$ ist dann durch $\gamma(\alpha)$ festgelegt. Wir definieren $\Phi : \operatorname{Aut}(K/k) \to \mathbb{Z}/n\mathbb{Z}$, $\gamma \mapsto j + n\mathbb{Z}$, wobei $\gamma(\alpha) = \zeta^j \alpha$ ist. Nach den eben Gesagten ist Φ wohldefiniert und injektiv; außerdem ist Φ ein Gruppenhomomorphismus: Seien $\gamma, \gamma' \in \operatorname{Aut}(K/k)$ 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 $\operatorname{Aut}(K/k)$ zu einer Untergruppe von $Z/n\mathbb{Z}$ isomorph ist; das sind aber (bis auf Isomorphie) genau die zyklischen Gruppen mit n teilender Ordnung.
(2) Sei $\gamma \in \operatorname{Aut}(K/k)$ ein Erzeuger (also $\operatorname{ord}(\gamma) = n$). $\gamma : K \to K$ ist k-linear, die Eigenwerte müssen n-te Einheitswurzeln sein. Als k-linearer Automorphismus endlicher Ordnung (die nicht durch $\operatorname{char}(k)$ teilbar ist) ist γ diagonalisierbar; seien $\alpha_1, \dots, \alpha_n \in K$ k-linear unabhängige Eigenvektoren zu den Eigenwerten $\zeta^{m_1}, \dots, \zeta^{m_n}$. Da $\operatorname{ord}(\gamma) = n$ ist und kein echter Teiler davon, gilt $\langle \zeta^{m_1}, \dots, \zeta^{m_n} \rangle = \langle \zeta \rangle$. Es gibt also ganze Zahlen $l_1, \dots, l_n$ 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 $1, \alpha, \alpha^2, \dots, \alpha^{n-1}$ Eigenvektoren zu den Eigenwerten $1, \zeta, \zeta^2, \dots, \zeta^{n-1}$ sind. Damit sind $1, \alpha, \alpha^2, \dots, \alpha^{n-1}$ 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.

31.9. **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 $\operatorname{Aut}(L_1L_2/k) \to \operatorname{Aut}(L_1/k) \times \operatorname{Aut}(L_2/k)$, $\gamma \mapsto (\gamma|_{L_1}, \gamma|_{L_2})$, ist ein injektiver Gruppenhomomorphismus.*

Beweis. Nach Satz 27.2 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 27.7 ist L_1L_2 über k galoissch.

Dass die angegebene Abbildung ein Gruppenhomomorphismus ist, ist klar. Ist $\gamma \in \operatorname{Aut}(L_1L_2/k)$ 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. □

31.10. **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 27.2 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 27.7 L_1L_2 galoissch über L_2.

Dass die angegebene Abbildung ein Gruppenhomomorphismus ist, ist klar. 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 31.2 beweisen:

31.11. **Lemma.** *Sei $\mathrm{char}(k) = 0$ und $k \subset K$ galoissch mit auflösbarer Galoisgruppe. Dann ist $k \subset K$ eine 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 31.3. Nach Bemerkung 31.6 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 31.10 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 27.10 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 31.8, 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.

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

Beweis. Sei $k = K_0 \subset K_1 \subset K_2 \subset \ldots \subset K_m$ ein Körperturm wie in Definition 31.1 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 31.9 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 wesentlichen Schritt im Beweis von Satz 31.2:

31.13. **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 31.1 mit $K \subset K_m$. Nach Lemma 31.12 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 31.5 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 $X^n - a \in k[X]$ 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 31.5 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 30.2 ist $k \subset k'$ galoissch mit abelscher Galoisgruppe, und nach Lemma 31.8 ist $k' \subset K_1$ mit abelscher (sogar zyklischer) Galoisgruppe; insgesamt folgt (wieder mit Lemma 31.5), dass $\mathrm{Aut}(K_1/k)$ auflösbar ist. □

Der Beweis von Satz 31.2 geht dann so:

Beweis. „⇒“: Sei $k \subset K$ eine Radikalerweiterung. Nach Lemma 31.12 gibt es eine galoissche Radikalerweiterung $k \subset L$ mit $K \subset L$. Nach Lemma 31.13 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 31.11 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:

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

31.15. **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. □

31.16. **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 ist $\mathrm{Gal}(f/\mathbb{Q}) = S_p$.*
(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 $\{1, 2, \ldots, p\}$ operiert; es gibt also ein Element der Ordnung p in G, das 1 auf 2 abbildet. Wiederum nach eventueller Änderung der Nummerierung der Elemente $3, 4, \ldots, p$ können wir annehmen, dass der p-Zykel $\sigma = (1\ 2\ 3\ \ldots\ p)$ in G ist. Für $1 \leq m \leq p-2$ ist $\sigma^m \circ \tau \circ \sigma^{-m} = (m+1\ \ m+2)$, also enthält G alle Transpositionen $(1\ 2)$, $(2\ 3)$, $\ldots$, $(p-1\ p)$. 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:

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

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 $1 \leq 2m+1 \leq p-2$, 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 $\geq 2p^2$ hat. Da h nur einfache Nullstellen hat, und zwar an den Stellen $-\sqrt{p-3}, \ldots, -\sqrt{4}, -\sqrt{2}, 0, \sqrt{2}, \ldots, \sqrt{p-3}$, müssen die Vorzeichen an den $p-1$ Stellen

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

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).

31.17. **Bemerkung.** Man kann für jedes n (nicht nur 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 27.10 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:

31.18. **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 $p = 2$):

31.19. **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

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

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.

31.20. **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 mit $\#N = p$.*

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 31.19. Induktion über n. Im Fall $n = 0$ ist G trivial, und es ist nichts zu zeigen. Sei also $n > 0$. Nach Lemma 31.20 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 $\phi : G \to G'$ 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 $G_1/G_0 \cong G_1 \cong \mathbb{Z}/p\mathbb{Z}$. □

32. Semidirekte Produkte von Gruppen

Wir erinnern uns an folgende Aussage (Proposition 19.8) aus der *Einführung in die Algebra*:

Sind $p < q$ Primzahlen mit $p \nmid q-1$, dann ist jede Gruppe G mit $\#G = pq$ zyklisch.

Wir wollen jetzt untersuchen, was passiert, wenn p ein Teiler von $q-1$ ist. Dazu erinnern wir uns an den Beweis der obigen Aussage: Wenn s_p und s_q die Anzahl der p- bzw. q-Sylowgruppen von G bezeichnet, dann gelten nach den Sätzen von Sylow die Aussagen

$$s_p \mid q, \quad s_p \equiv 1 \bmod p \quad \text{und} \quad s_q \mid p, \quad s_q \equiv 1 \bmod q\,.$$

Wegen $q > p$ folgt daraus $s_q = 1$. Die Voraussetzung $p \nmid q-1$ diente dann dazu, die Möglichkeit $s_p = q$ auszuschließen, sodass dann $s_p = 1$ sein musste. Dann sind sowohl p- als auch q-Sylowgruppe Normalteiler und die Behauptung folgt.

Wenn nun p ein Teiler von $q-1$ ist, dann ist der Fall $s_p = q$ durch die Sylowschen Sätze nicht ausgeschlossen. Die Frage ist, ob er tatsächlich vorkommt und wie dann die Gruppe aussieht.

Wir haben in jedem Fall $s_q = 1$; es gibt also genau eine q-Sylowgruppe S_q in G und S_q ist ein Normalteiler von G. Sei S_p eine p-Sylowgruppe von G. Dann gilt $S_q \cap S_p = \{1\}$ und $S_q S_p = \{xy \mid x \in S_q, y \in S_p\} = G$: Die erste Aussage folgt daraus, dass die Ordnung der Untergruppe $S_q \cap S_p$ von S_q und S_p sowohl q als auch p teilen muss. Die zweite folgt daraus, denn die Abbildung $S_q \times S_p \to G$, $(x, y) \mapsto xy$, ist injektiv: Aus $xy = x'y'$ folgt $x'^{-1}x = y'y^{-1} \in S_q \cap S_p = \{1\}$, also $x = x'$ und $y = y'$. Da beide Seiten die gleiche Anzahl pq von Elementen haben, ist die Abbildung auch surjektiv.

Wenn wir die Elemente von G in der Form xy schreiben mit $x \in S_q$ und $y \in S_p$, dann können wir G als Menge mit $S_q \times S_p$ identifizieren. Wie sieht die Verknüpfung dann aus? Es ist

$$(x_1y_1)(x_2y_2) = (x_1(y_1x_2y_1^{-1}))(y_1y_2)$$

und $y_1x_2y_1^{-1} \in S_q$, da S_q ein Normalteiler ist. Wir müssen also wissen, wie S_p auf S_q durch Konjugation operiert. Allgemeiner haben wir folgende Konstruktion.

32.1. **Lemma und Definition.** *Seien N und H zwei Gruppen, und sei $\phi : H \to \mathrm{Aut}(N)$ ein Gruppenhomomorphismus. Wir schreiben $h{*}n$ für $\phi(h)(n)$; das ist eine Operation von H auf N durch Gruppenautomorphismen. Dann wird $G = N \times H$ zu einer Gruppe, wenn wir die Verknüpfung wie folgt definieren:*

$$(n_1, h_1) \cdot (n_2, h_2) = (n_1(h_1 * n_2), h_1h_2)\,.$$

Die Projektion $\mathrm{pr}_2 : G = N \times H \to H$ ist ein surjektiver Gruppenhomomorphismus mit Kern $N \times \{1_H\} \cong N$.

G heißt das *semidirekte Produkt* von N und H bezüglich ϕ und wird $G = N \rtimes_\phi H$ (oder auch $N \rtimes H$, wenn ϕ aus dem Kontext klar ist) geschrieben.

Beweis. Wir müssen zeigen, dass G eine Gruppe ist. Dabei verwenden wir die Rechenregeln

$$h * (n_1n_2) = (h * n_1)(h * n_2) \quad \text{und} \quad (h_1h_2) * n = h_1 * (h_2 * n)\,,$$
$$\text{sowie} \qquad 1_H * n = n \quad \text{und} \quad h * 1_N = 1_N\,.$$

- Assoziativität:

$$\begin{aligned}\big((n_1, h_1) \cdot (n_2, h_2)\big) \cdot (n_3, h_3) &= (n_1(h_1 * n_2), h_1h_2) \cdot (n_3, h_3)\\ &= \big(n_1(h_1 * n_2)((h_1h_2) * n_3), h_1h_2h_3\big)\\ &= \big(n_1(h_1 * n_2)(h_1 * (h_2 * n_3)), h_1h_2h_3\big)\\ &= \big(n_1(h_1 * (n_2(h_2 * n_3))), h_1h_2h_3\big)\\ &= (n_1, h_1) \cdot (n_2(h_2 * n_3), h_2h_3)\\ &= (n_1, h_1) \cdot \big((n_2, h_2) \cdot (n_3, h_3)\big)\end{aligned}$$

- Neutrales Element ist $(1_N, 1_H)$:

$$(n, h) \cdot (1_N, 1_H) = (n(h * 1_N), h1_H) = (n1_N, h) = (n, h)$$
$$(1_N, 1_H) \cdot (n, h) = (1_N(1_H * n), h1_H) = (1_Nn, h) = (n, h)$$

- Das Inverse von (n,h) ist $(h^{-1}*n^{-1},h^{-1})$:

$$\begin{aligned}(n,h)\cdot(h^{-1}*n^{-1},h^{-1}) &= \big(n(h*(h^{-1}*n^{-1})),hh^{-1}\big)\\ &= \big(n((hh^{-1})*n^{-1}),1_H\big) = (nn^{-1},1_H) = (1_N,1_H)\\ (h^{-1}*n^{-1},h^{-1})\cdot(n,h) &= \big((h^{-1}*n^{-1})(h^{-1}*n),h^{-1}h\big)\\ &= \big(h^{-1}*(n^{-1}n),1_H\big) = (h^{-1}*1_N,1_H) = (1_N,1_H)\end{aligned}$$

Dass pr_2 ein Gruppenhomomorphismus ist, folgt daraus, dass in der zweiten Komponente die Elemente von H einfach wie in H verknüpft werden. Die Abbildung ist surjektiv: Z.B. ist $(1_N,h)\mapsto h$. Der Kern ist offensichtlich $N\times\{1_H\}$, der Isomorphismus $(n,1_H)\mapsto n$ ist klar wegen

$$(n_1,1_H)\cdot(n_2,1_H) = (n_1(1_H*n_2),1_H) = (n_1n_2,1_H)\,. \qquad \square$$

Ist ϕ trivial, also $h*n=n$ für alle $h\in H$, $n\in N$, dann ist $N\rtimes_\phi H\cong N\times H$ ein direktes Produkt.

Im Hinblick auf unser Klassifikationsproblem ist folgende Aussage wichtig.

32.2. **Proposition.** *Sei G eine Gruppe mit einem Normalteiler $N\lhd G$ und einer Untergruppe $H\le G$, sodass $N\cap H=\{1\}$ und $NH=G$. Sei $\phi: H\to\mathrm{Aut}(N)$, $h\mapsto(n\mapsto hnh^{-1})$, der Homomorphismus, der die Operation von H auf N durch Konjugation beschreibt. Dann ist*

$$N\rtimes_\phi H\longrightarrow G,\quad (n,h)\mapsto nh$$

ein Gruppenisomorphismus.

Beweis. Die Abbildung ist bijektiv (injektiv wegen $N\cap H=\{1\}$ und surjektiv wegen $NH=G$). Dass sie ein Gruppenhomomorphismus ist, folgt aus der Relation $(n_1h_1)(n_2h_2)=(n_1(h_1n_2h_1^{-1}))(h_1h_2)$. $\square$

Man beachte, dass $N\rtimes H$ nicht abelsch zu sein braucht, selbst wenn N und H beide abelsch sind.

32.3. **Beispiel.** Sei $n\in\mathbb{Z}_{>0}$, $N=\mathbb{Z}/n\mathbb{Z}$ (additiv), $H=\{\pm1\}$ (multiplikativ) und $\phi: H\to\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})\cong(\mathbb{Z}/n\mathbb{Z})^\times$ die Abbildung $h\mapsto h+n\mathbb{Z}$. Dann ist $(\pm1)*n=\pm n$, und $G=N\rtimes H$ ist isomorph zur Diedergruppe D_n: Die Elemente von $N\times\{1\}$ entsprechen den Drehungen, die von $N\times\{-1\}$ den Spiegelungen (mit $\sigma=(1,1)$ und $\tau=(0,-1)$ prüft man die Relationen (multiplikativ geschrieben) $\sigma^n=\mathrm{id}$, $\tau^2=\mathrm{id}$, $\tau\sigma\tau=\sigma^{-1}$ nach).

Damit können wir die Klassifikation der Gruppen der Ordnung pq abschließen.

32.4. **Satz.** *Seien $p<q$ Primzahlen und G eine Gruppe mit $\#G=pq$. Dann ist G entweder zyklisch, oder $q\equiv1 \bmod p$ und $G\cong\mathbb{Z}/q\mathbb{Z}\rtimes_\phi\mathbb{Z}/p\mathbb{Z}$, wobei $\phi:\mathbb{Z}/p\mathbb{Z}\to\mathrm{Aut}(\mathbb{Z}/q\mathbb{Z})\cong\mathbb{F}_q^\times$ injektiv ist. ϕ ist bis auf Komposition mit einem Automorphismus von $\mathbb{Z}/p\mathbb{Z}$ eindeutig bestimmt; daher sind alle semidirekten Produkte der Form $\mathbb{Z}/q\mathbb{Z}\rtimes_\phi\mathbb{Z}/p\mathbb{Z}$ zueinander isomorph.*

Beweis. Im Fall $q\not\equiv1 \bmod p$ muss G nach dem bekannten Ergebnis zyklisch sein. Ist G nicht zyklisch, dann auch nicht abelsch. Die Operation von S_p auf dem Normalteiler S_q von G durch Konjugation ist also nichttrivial. $\mathrm{Aut}(S_q)\cong\mathbb{F}_q^\times\cong\mathbb{Z}/(q-1)\mathbb{Z}$ hat genau eine Untergruppe der Ordnung p; der Homomorphismus $\phi: S_p\to\mathrm{Aut}(S_q)$, der die Operation durch Konjugation beschreibt, muss also ein

Isomorphismus auf diese Untergruppe sein. Als solcher ist ϕ bis auf Komposition mit einem Isomorphismus von S_p eindeutig bestimmt. Proposition 32.2 liefert dann die Behauptung. $\square$

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.