5. Galoisgruppen

Nach dem Studium von Zerfällungskörpern im letzten Kapitel wollen wir nun wieder zu unseren Problemen aus der Einleitung zurückkehren. Dazu erinnern wir uns zunächst noch einmal kurz daran, was wir z. B. über die Konstruktion des regelmäßigen n-Ecks mit Zirkel und Lineal bereits wissen: nach Beispiel 1.23 (C) ist das n-Eck genau dann konstruierbar, wenn $z = e^{\frac{2\pi i}{n}}$ in einer 2-Radikalerweiterung von $\mathbb{Q}$ liegt, d. h. wenn es eine Kette

$$\mathbb{Q} = K_0 \leq K_1 \leq \cdots \leq K_m = L$$

von Unterkörpern von $\mathbb{C}$ gibt, so dass $z \in L$ und jedes K_i/K_{i-1} für $i = 1, \ldots, m$ eine einfache 2-Radikalerweiterung ist (bzw. nach Aufgabe 2.21 (b) einfach Grad 2 hat).

Wir haben in Folgerung 2.22 (a) gezeigt, dass eine *notwendige* Bedingung hierfür ist, dass der Grad $[z : \mathbb{Q}]$ eine Zweierpotenz ist. Diesen Grad haben wir in Satz 3.29 dann auch konkret berechnet — er ist gerade der Wert $\varphi(n)$ der Eulerschen φ-Funktion.

Wir wollen nun sehen, ob wir auch *hinreichende* Kriterien für die Konstruierbarkeit angeben können, die sich ähnlich leicht nachprüfen lassen. Nach Satz 3.29 ist für $n = 17$ z. B. $\varphi(n) = 16 = 2^4$ eine Zweierpotenz; unser notwendiges Kriterium ist damit in diesem Fall erfüllt. Wir müssen jetzt also herausfinden, ob wir eine Kette

$$\mathbb{Q} = K_0 \leq K_1 \leq K_2 \leq K_3 \leq K_4 = \mathbb{Q}\left(e^{\frac{2\pi i}{17}}\right)$$

von Körpern mit $[K_i : K_{i-1}] = 2$ für $i = 1, \ldots, 4$ finden können. Dies ist jedoch nicht so einfach. Wir benötigen dazu offensichtlich genauere Informationen über die Zwischenkörper von $\mathbb{Q}(z)/\mathbb{Q}$, also über die Körper Z mit $\mathbb{Q} \leq Z \leq \mathbb{Q}(z)$.

Die Idee der Galoistheorie ist nun, die Frage nach *Zwischenkörpern einer gegebenen Körpererweiterung* auf die Frage nach *Untergruppen einer gegebenen Gruppe* zurückzuführen. Die Anzahl der Elemente der Gruppen entsprechen dabei den Graden der Körpererweiterung. Im Fall des 17-Ecks werden wir also eine gewisse Gruppe G mit 16 Elementen haben und untersuchen müssen, ob es eine Kette von Untergruppen

$$G = U_0 \geq U_1 \geq U_2 \geq U_3 \geq U_4 = \{e\}$$

gibt, deren Anzahl Elemente genau 16, 8, 4, 2 bzw. 1 ist. Da endliche Gruppen viel einfacher zu behandeln sind als Körpererweiterungen, werden wir unser Problem schließlich auf diese Art lösen können. In der Tat werden wir in Aufgabe 5.4 sehen, dass die Gruppe G im Fall des 17-Ecks einfach $\mathbb{Z}_{16}$ ist. Von dieser Gruppe können wir natürlich alle Untergruppen leicht angeben [G, Aufgabe 6.28 (a)] und insbesondere sehen, dass dort eine Untergruppenkette

$$\mathbb{Z}_{16} = \langle \overline{1} \rangle \geq \langle \overline{2} \rangle \geq \langle \overline{4} \rangle \geq \langle \overline{8} \rangle \geq \{\overline{0}\}$$

wie oben existiert — woraus wir dann mit Hilfe der Galoistheorie schließen können, dass auch die oben erwähnte Kette von Zwischenkörpern von $\mathbb{Q}(z)/\mathbb{Q}$ existiert und das 17-Eck damit konstruierbar ist.

Wir wollen diesen Zusammenhang zwischen Untergruppen und Zwischenkörpern nun in diesem und dem folgenden Kapitel konkret konstruieren. Da unsere Anwendungen der Galoistheorie letztlich bei Körpererweiterungen von $\mathbb{Q}$ liegen, werden wir uns dabei auf den Fall von (endlichen) Körpererweiterungen in Charakteristik 0 beschränken. Galoistheorie funktioniert zwar auch in positiver Charakteristik, jedoch ist sie dort komplizierter, da dort einige Sätze nicht gelten, die uns im Folgenden das Leben einfacher machen werden (wie z. B. der Satz 4.28 vom primitiven Element oder die Äquivalenz von galoisschen und normalen Körpererweiterungen in Satz 5.8). Wir vereinbaren also:

In Kapitel 5 und 6 seien alle Körpererweiterungen endlich und von Charakteristik 0.

Um mit unserem Programm zu beginnen, werden wir nun als Erstes angeben, wie wir überhaupt einem Körper bzw. einer Körpererweiterung eine Gruppe zuordnen wollen.

Definition 5.1 (Automorphismengruppe und Galoisgruppe)**.** Es sei L/K eine Körpererweiterung.

(a) Wir bezeichnen mit $\mathrm{Aut}(L)$ die Menge aller Körperisomorphismen $\sigma : L \to L$. Der Name kommt daher, dass man Isomorphismen mit gleichem Start- und Zielraum auch als **Automorphismen** bezeichnet. Offensichtlich ist $\mathrm{Aut}(L)$ mit der Verkettung von Abbildungen eine Gruppe. Man nennt sie die **Automorphismengruppe** von L.

(b) Wichtiger für uns ist die entsprechende relative Version: die Menge

$$\mathrm{Gal}(L/K) := \mathrm{Aut}(L/K) := \{\sigma : L \to L \text{ Körperisomorphismus mit } \sigma|_K = \mathrm{id}\}$$

der Automorphismen von L, die alle Elemente von K fest lassen (also die Menge aller K-Automorphismen in der Sprechweise von Bemerkung 4.9). Auch dies ist zusammen mit der Verkettung von Abbildungen offensichtlich eine Gruppe. Man nennt sie die **Galoisgruppe** bzw. Automorphismengruppe von L/K (in der Literatur sind beide Bezeichnungen üblich).

Das Ziel dieses Kapitels ist es, diese Galoisgruppen von Körpererweiterungen zu studieren. Dazu werden wir natürlich gleich auch einige Beispiele von Galoisgruppen sehen. Um diese einfacher berechnen zu können, benötigen wir jedoch zunächst ein Lemma.

Lemma 5.2 (Eigenschaften von Galoisgruppen)**.** *Es sei L/K eine Körpererweiterung (gemäß unserer Konvention endlich und von Charakteristik 0). Dann gilt:*

(a) *Es sei $f \in K[t]$ und $a \in L$ mit $f(a) = 0$. Für jedes Element der Galoisgruppe $\sigma \in \mathrm{Gal}(L/K)$ gilt dann auch $f(\sigma(a)) = 0$. (Man sagt: die Elemente der Galoisgruppe bilden Nullstellen auf Nullstellen ab.)*

(b) *Ist $L = K(a)$ und f das Minimalpolynom von a, so gibt es eine Bijektion*

$$\begin{aligned} \{\textit{Nullstellen von } f \textit{ in } L\} &\overset{1:1}{\longleftrightarrow} \mathrm{Gal}(L/K) \\ b &\longmapsto \textit{der eindeutig bestimmte Isomorphismus } \sigma : L \to L \\ &\qquad \textit{mit } \sigma|_K = \mathrm{id} \textit{ und } \sigma(a) = b \\ \sigma(a) &\longmapsfrom \sigma. \end{aligned}$$

(c) $|\mathrm{Gal}(L/K)| \leq [L : K]$. *(Insbesondere sind Galoisgruppen also stets endliche Gruppen.)*

Beweis.

(a) Es sei $f = c_n t^n + \cdots + c_1 t + c_0$ mit $c_0, \ldots, c_n \in K$. Dann gilt

$$\begin{aligned} f(\sigma(a)) &= c_n \sigma(a)^n + \cdots + c_1 \sigma(a) + c_0 \\ &= \sigma(c_n)\,\sigma(a)^n + \cdots + \sigma(c_1)\sigma(a) + \sigma(c_0) && (\sigma|_K = \mathrm{id}) \\ &= \sigma(c_n a^n + \cdots + c_1 a + c_0) && (\sigma \text{ Körperhomomorphismus}) \\ &= \sigma(f(a)) = \sigma(0) = 0. \end{aligned}$$

(b) Wir müssen zeigen, dass die beiden angegebenen Abbildungen existieren.

Für die Abbildung „$\longmapsto$“ betrachten wir eine Nullstelle b von f in L. Dann ist $K(b) \leq L$ nach Bemerkung 4.2 (a) ein Stammkörper von f, nach Bemerkung 4.2 (c) ist demzufolge $[K(b) : K] = \deg f = [K(a) : K] = [L : K]$. Mit der Gradformel aus Satz 2.17, angewendet auf $K \leq K(b) \leq L$, bedeutet dies $[L : K(b)] = 1$ und damit $K(b) = L$.

Die Eindeutigkeit von Stammkörpern aus Lemma 4.8 besagt daher nun, dass es genau einen Isomorphismus σ von $K(a) = L$ nach $K(b) = L$ mit $\sigma|_K = \mathrm{id}$ und $\sigma(a) = b$ gibt. Also existiert die im Lemma angegebene Abbildung „$\longmapsto$“.

Die Abbildung „$\longmapsfrom$“ existiert, da jedes $\sigma \in \mathrm{Gal}(L/K)$ die Nullstelle a von f nach (a) wieder auf eine Nullstelle von f abbildet.

Nach Konstruktion ist klar, dass die beiden Abbildungen invers zueinander sind.

(c) Nach dem Satz 4.28 vom primitiven Element können wir annehmen, dass $L = K(a)$ eine einfache Körpererweiterung ist. Ist f das Minimalpolynom von a, so ist $\mathrm{Gal}(L/K)$ nach (b) bijektiv zur Menge der Nullstellen von f in L. Also hat $\mathrm{Gal}(L/K)$ höchstens $\deg f$ Elemente. Da nach Bemerkung 4.2 (c) ferner $\deg f = [L:K]$ gilt, folgt die Behauptung. □

Beispiel 5.3. Wir wollen nun mit Hilfe von Lemma 5.2 (b) einige Galoisgruppen konkret berechnen. Dazu müssen wir offensichtlich die gegebene Körpererweiterung L/K als einfache Körpererweiterung $K(a)/K$ schreiben, das Minimalpolynom f von a bestimmen, und untersuchen, welche bzw. wie viele Nullstellen f in L besitzt.

(a) Es sei $L/K = \mathbb{C}/\mathbb{R} = \mathbb{R}(i)/\mathbb{R}$ (vgl. Beispiel 4.10 (a)). Das Minimalpolynom von i ist natürlich $f = t^2+1$, und dieses Polynom hat in L zwei Nullstellen, nämlich i und $-i$. Also hat die Galoisgruppe $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$ nach Lemma 5.2 (b) zwei Elemente $\sigma_0, \sigma_1 : \mathbb{C} \to \mathbb{C}$, die eindeutig bestimmt sind durch

$$\begin{aligned} & \sigma_0|_{\mathbb{R}} = \mathrm{id} \quad \text{und} \quad \sigma_0(i) = i \\ \text{bzw.} \quad & \sigma_1|_{\mathbb{R}} = \mathrm{id} \quad \text{und} \quad \sigma_1(i) = -i. \end{aligned}$$

In der Tat kann man hier einfach sehen, dass diese Angaben σ_0 und σ_1 eindeutig bestimmen: für jedes $z = x+iy \in \mathbb{C}$ mit $x, y \in \mathbb{R}$ ist ja

$$\begin{aligned} & \sigma_0(x+iy) = \sigma_0(x) + \sigma_0(i)\,\sigma_0(y) = x+iy \\ \text{und} \quad & \sigma_1(x+iy) = \sigma_1(x) + \sigma_1(i)\,\sigma_1(y) = x-iy, \end{aligned}$$

also ist σ_0 die Identität und σ_1 die komplexe Konjugation. Als Gruppe gilt offensichtlich $\mathrm{Gal}(\mathbb{C}/\mathbb{R}) = \{\sigma_0, \sigma_1\} \cong \mathbb{Z}_2$, wobei die Identität σ_0 das neutrale Element ist. Insbesondere gilt hier in Lemma 5.2 (c) also die Gleichheit $|\mathrm{Gal}(\mathbb{C}/\mathbb{R})| = 2 = [\mathbb{C}:\mathbb{R}]$, da das quadratische Polynom f in $\mathbb{C}$ wirklich zwei (verschiedene) Nullstellen besitzt.

(b) Es sei $L/K = \mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$. Hier hat das Minimalpolynom $f = t^3 - 2$ von $\sqrt[3]{2}$ nur die Nullstelle $\sqrt[3]{2}$ in L, da die anderen beiden (komplexen) Nullstellen $\sqrt[3]{2}\,e^{\frac{2\pi i}{3}}$ und $\sqrt[3]{2}\,e^{\frac{4\pi i}{3}}$ nicht reell sind und somit nicht im Körper $\mathbb{Q}(\sqrt[3]{2}) \leq \mathbb{R}$ liegen können. Also ist das einzige Element in der Galoisgruppe nach Lemma 5.2 (b) die Identität auf L, d. h. $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$ ist die triviale Gruppe mit nur einem Element. Insbesondere gilt nun in Lemma 5.2 (c) eine echte Ungleichung $|\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})| = 1 < 3 = [\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}]$, da das kubische Minimalpolynom $t^3 - 2$ keine drei Nullstellen in $\mathbb{Q}(\sqrt[3]{2})$ besitzt.

(c) Es sei $L/K = \mathbb{Q}(e^{\frac{2\pi i}{n}})/\mathbb{Q}$ für ein $n \in \mathbb{N}_{>0}$. Nach Satz 3.27 (b) ist das Minimalpolynom f von $e^{\frac{2\pi i}{n}}$ gerade das n-te Kreisteilungspolynom Φ_n aus Definition 3.16. Die Nullstellen dieses Polynoms sind nach Konstruktion genau die primitiven n-ten Einheitswurzeln E_n', also nach Bemerkung 3.15 (b) die komplexen Zahlen $e^{\frac{2\pi ik}{n}}$ für alle k mit $\mathrm{ggt}(k,n) = 1$ bzw. $\overline{k} \in \mathbb{Z}_n^*$. Diese liegen natürlich alle im Körper L, denn L ist ja multiplikativ abgeschlossen und $e^{\frac{2\pi ik}{n}}$ gerade die k-te Potenz von $e^{\frac{2\pi i}{n}}$.

Also ist $\mathrm{Gal}(L/K)$ nach Lemma 5.2 (b) bijektiv zur Menge E_n' der primitiven n-ten Einheitswurzeln bzw. zu $\mathbb{Z}_n^*$: zu jedem k mit $\mathrm{ggt}(k,n) = 1$ gehört ein Element σ_k von $\mathrm{Gal}(L/K)$, das durch

$$\sigma_k|_{\mathbb{Q}} = \mathrm{id} \quad \text{und} \quad \sigma_k(e^{\frac{2\pi i}{n}}) = e^{\frac{2\pi ik}{n}} \qquad (*)$$

eindeutig bestimmt ist. Insbesondere gilt hier in Lemma 5.2 (c) also wieder die Gleichheit: es ist $|\mathrm{Gal}(L/K)| = |E_n'| = \varphi(n) = [L:K]$ nach Satz 3.29.

Um auch noch die Gruppenstruktur der Galoisgruppe zu verstehen, müssen wir schließlich noch die Verknüpfungstabelle der σ_k berechnen. Dies ist sehr einfach: haben wir k, l mit $\mathrm{ggt}(k,n) = \mathrm{ggt}(l,n) = 1$, so gilt nach $(*)$

$$(\sigma_k \circ \sigma_l)(e^{\frac{2\pi i}{n}}) = \sigma_k(e^{\frac{2\pi il}{n}}) = \sigma_k(e^{\frac{2\pi i}{n}})^l = (e^{\frac{2\pi ik}{n}})^l = e^{\frac{2\pi ikl}{n}}$$

und damit $\sigma_k \circ \sigma_l = \sigma_{k \cdot l}$. Diese Gleichung bedeutet aber genau, dass die Abbildung

$$\mathbb{Z}_n^* \to \mathrm{Gal}(L/K), \quad \bar{k} \mapsto \sigma_k$$

ein Gruppenhomomorphismus ist. Da wir diese Abbildung oben schon als bijektiv erkannt haben, ist sie also sogar ein Isomorphismus, und wir erhalten als Resultat, dass

$$\mathrm{Gal}\left(\mathbb{Q}(e^{\frac{2\pi i}{n}})/\mathbb{Q}\right) \cong \mathbb{Z}_n^*.$$

Aufgabe 5.4. Zeige, dass die Gruppen $\mathbb{Z}_{17}^*$ und $\mathbb{Z}_{16}$ isomorph sind, und dass mit Beispiel 5.3 (c) demnach

$$\mathrm{Gal}\left(\mathbb{Q}(e^{\frac{2\pi i}{17}})/\mathbb{Q}\right) \cong \mathbb{Z}_{16}$$

gilt. (Wenn ihr die Vorlesung „Elementare Zahlentheorie“ bereits gehört habt, werdet ihr dies bereits wissen, da ihr dort dann allgemein bewiesen habt, dass die Gruppe $\mathbb{Z}_p^*$ für jede Primzahl p zyklisch mit $p-1$ Elementen und somit isomorph zu $\mathbb{Z}_{p-1}$ ist.)

Aufgabe 5.5. Es sei L/K eine algebraische, aber nicht notwendig endliche Körpererweiterung. Beweise, dass jeder K-Homomorphismus $\varphi : L \to L$ (also jeder Körperhomomorphismus $\varphi : L \to L$ mit $\varphi|_K = \mathrm{id}$) bereits ein K-Isomorphismus ist.

08

Wir hatten in der Einleitung zu diesem Kapitel ja schon erwähnt, dass in unserer Galois-Korrespondenz zwischen Untergruppen und Zwischenkörpern letztlich die Ordnungen der Gruppen den Graden der Körpererweiterungen entsprechen sollen. Daher werden für uns in Zukunft besonders die Körpererweiterungen L/K interessant sein, bei denen in der Beziehung $|\mathrm{Gal}(L/K)| \leq [L:K]$ aus Lemma 5.2 (c) die Gleichheit gilt. Wir geben diesen Erweiterungen zunächst einen besonderen Namen.

Definition 5.6 (Galoissche Körpererweiterung)**.** Eine Körpererweiterung L/K heißt **galoissch**, wenn $|\mathrm{Gal}(L/K)| = [L:K]$.

Beispiel 5.7. Wie wir in Beispiel 5.3 gesehen haben, sind die Körpererweiterungen $\mathbb{C}/\mathbb{R}$ und $\mathbb{Q}(e^{\frac{2\pi i}{n}})/\mathbb{Q}$ für $n \in \mathbb{N}_{>0}$ galoissch, $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ jedoch nicht.

Zur Eigenschaft „galoissch“ einer Körpererweiterung gibt es einige äquivalente Bedingungen. Die wichtigsten von ihnen, die auch in der Praxis häufig verwendet werden, sind die folgenden.

Satz 5.8 (Äquivalente Bedingungen zu „galoissch“)**.** *Es sei L/K eine Körpererweiterung (wie üblich endlich und von Charakteristik 0). Dann sind die folgenden Eigenschaften äquivalent:*

(a) *L/K ist galoissch.*

(b) *L ist der Zerfällungskörper eines Polynoms über K.*

(c) *Ist $g \in K[t]$ ein irreduzibles Polynom, das eine Nullstelle in L besitzt, so zerfällt g in L bereits in Linearfaktoren. (Körpererweiterungen mit dieser Eigenschaft werden in der Literatur oft als **normal** bezeichnet.)*

Beweis. Nach dem Satz 4.28 vom primitiven Element können wir annehmen, dass $L = K(a)$ eine einfache Körpererweiterung ist. Es sei $f \in K[t]$ das Minimalpolynom von a, so dass L also der Stammkörper von f ist. Wir zeigen die Äquivalenz der angegebenen Aussagen durch einen Ringschluss.

„(a) $\Rightarrow$ (b)“: Die Anzahl der Nullstellen von f in L ist gleich

$$\begin{aligned} & |\mathrm{Gal}(L/K)| && \text{(Lemma 5.2 (b))} \\ = {} & [L:K] && \text{(Voraussetzung)} \\ = {} & \deg f && \text{(Bemerkung 4.2 (c)).} \end{aligned}$$

Insbesondere muss f damit über L in Linearfaktoren zerfallen. Da a eine Nullstelle von f ist, ist L also der Zerfällungskörper von f.

„(b) $\Rightarrow$ (c)“: Dies ist genau die Aussage von Aufgabe 4.19 (b).

„(c) $\Rightarrow$ (a)“: Das irreduzible Polynom f hat natürlich die Nullstelle a in L und zerfällt nach Voraussetzung damit über L in Linearfaktoren. Diese Linearfaktoren sind nach Folgerung 4.30 auch alle verschieden. Also hat f genau $\deg f$ Nullstellen in L. Nach Lemma 5.2 (b) und Bemerkung 4.2 (c) gilt damit $|\mathrm{Gal}(L/K)| = \deg f = [L:K]$, d. h. L/K ist galoissch. □

Bemerkung 5.9.

(a) Der Beweis der Richtung „(a) $\Rightarrow$ (b)“ in Satz 5.8 zeigt zusätzlich, dass es eine weitere äquivalente Bedingung für eine galoissche Körpererweiterung L/K ist, dass L der Zerfällungskörper eines *irreduziblen* Polynoms über K ist.

(b) In positiver Charakteristik ist die Aussage von Satz 5.8 falsch. Man kann z. B. zeigen, dass die Begriffe „galoissch“ und „normal“ dort in der Regel verschieden sind — was auch erklärt, warum es hierfür zwei verschiedene Namen gibt.

Da die für uns später besonders wichtigen galoisschen Körpererweiterungen nach Satz 5.8 genau die Zerfällungskörper von Polynomen sind, führen wir nun eine weitere Notation ein, die einem Polynom direkt die Galoisgruppe seines Zerfällungskörpers zuordnet. Gleichzeitig gibt uns dies im folgenden Lemma auch eine gute Möglichkeit, wie wir uns solche Galoisgruppen anschaulich vorstellen können.

Definition 5.10 (Galoisgruppe eines Polynoms)**.** Es sei $f \in K[t]$ ein Polynom über einem Körper K mit $f \neq 0$. Ist L der Zerfällungskörper von f (der nach Satz 5.8 galoissch über K ist), so definieren wir die **Galoisgruppe** von f als $\mathrm{Gal}(f) := \mathrm{Gal}(L/K)$.

Lemma 5.11 (Galoisgruppen als Untergruppen von S_n)**.** *Es sei $f \in K[t]$ ein Polynom über einem Körper K mit $n := \deg f \in \mathbb{N}_{>0}$. Dann gilt:*

(a) *Jedes Element von $\mathrm{Gal}(f)$ permutiert die Nullstellen von f in seinem Zerfällungskörper. Auf diese Art ist $\mathrm{Gal}(f)$ isomorph zu einer Untergruppe der symmetrischen Gruppe S_n.*

(b) *Ist f irreduzibel, so ist die Ordnung $|\mathrm{Gal}(f)|$ der Galoisgruppe von f ein Vielfaches von n.*

Beweis. Es seien L der Zerfällungskörper von f und $a_1, \dots, a_m$ mit $m \leq n$ die verschiedenen Nullstellen von f in L, so dass also $L = K(a_1, \dots, a_m)$.

(a) Beachte, dass jedes Element $\sigma \in \mathrm{Gal}(f)$ als Körperisomorphismus $\sigma : L \to L$ bijektiv ist und Nullstellen von f nach Lemma 5.2 (a) wieder auf Nullstellen von f abbildet. Also induziert ein solches σ eine Permutation der Nullstellen von f, d. h. wir erhalten eine Abbildung

$$\begin{aligned} \mathrm{Gal}(f) &\to S_m \\ \sigma &\mapsto \text{die Permutation } \tau \in S_m \text{ mit } \sigma(a_i) = a_{\tau(i)} \text{ für } i = 1, \dots, m. \end{aligned}$$

Diese Abbildung ist ein Gruppenhomomorphismus, denn wird unter ihr σ auf τ und σ' auf τ' abgebildet, so ist

$$(\sigma \circ \sigma')(a_i) = \sigma(a_{\tau'(i)}) = a_{(\tau \circ \tau')(i)},$$

d. h. $\sigma \circ \sigma'$ wird auf $\tau \circ \tau'$ abgebildet. Außerdem ist sie injektiv, denn ist $\sigma \in \mathrm{Gal}(f)$ mit $\sigma(a_i) = a_i$ für alle $i = 1, \dots, m$, so ist σ die Identität auf K und allen a_i und damit auch auf dem davon erzeugten Körper $K(a_1, \dots, a_m) = L$.

Nach dem Homomorphiesatz [G, Satz 6.17] ist $\mathrm{Gal}(f)$ also isomorph zu einer Untergruppe von S_m, und wegen $S_m \leq S_n$ damit auch zu einer Untergruppe von S_n.

(b) Nach Lemma 2.18 ist $[a_1 : K]$ ein Teiler von $[L : K]$. Nun ist aber einerseits $[a_1 : K] = \deg f = n$, da f irreduzibel und damit bis auf Normierung das Minimalpolynom von a_1 ist, und andererseits $[L : K] = |\mathrm{Gal}(L/K)| = |\mathrm{Gal}(f)|$, da L/K als Zerfällungskörper nach Satz 5.8 galoissch ist. Also ist n wie behauptet ein Teiler von $|\mathrm{Gal}(f)|$. □

Beispiel 5.12. Das Polynom $f = t^3 - 2$ hat offensichtlich die drei Nullstellen

$$a_1 = \sqrt[3]{2}, \quad a_2 = \sqrt[3]{2}e^{\frac{2\pi i}{3}}, \quad a_3 = \sqrt[3]{2}e^{\frac{4\pi i}{3}}$$

in $\mathbb{C}$. Sein Zerfällungskörper ist also nach Aufgabe 4.18 (a)

$$L = \mathbb{Q}(a_1, a_2, a_3) = \mathbb{Q}\left(\sqrt[3]{2}, e^{\frac{2\pi i}{3}}\right)$$

und hat Grad $[L : \mathbb{Q}] = 6$ über $\mathbb{Q}$. Da diese Körpererweiterung nach Satz 5.8 galoissch ist, ist also $|\mathrm{Gal}(f)| = |\mathrm{Gal}(L/\mathbb{Q})| = [L : \mathbb{Q}] = 6$. Mit der Interpretation aus Lemma 5.11 (a) bedeutet dies genau, dass $\mathrm{Gal}(f) \cong S_3$ gelten muss, also dass man jede Permutation der drei Nullstellen von f durch einen $\mathbb{Q}$-Automorphismus von L erzeugen kann. Die Permutation $(2\ 3) \in S_3$ erhält man z. B. genau durch die komplexe Konjugation $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$, $\sigma(z) = \overline{z}$, denn es ist ja $\sigma(a_1) = \overline{a_1} = a_1$, $\sigma(a_2) = \overline{a_2} = a_3$ und $\sigma(a_3) = \overline{a_3} = a_2$.

Allgemein besagt Lemma 5.11 für ein irreduzibles Polynom f vom Grad 3, dass $\mathrm{Gal}(f)$ isomorph zu einer Untergruppe von S_3 ist, deren Ordnung ein Vielfaches von 3 ist. Nach [G, Beispiel 5.16] sind die einzigen solchen Untergruppen die symmetrische Gruppe S_3 selbst sowie die alternierende Gruppe $A_3 = \{\mathrm{id}, (1\ 2\ 3), (1\ 3\ 2)\}$. Wiederum nach der Interpretation aus Lemma 5.11 (a) liegt der Unterschied dieser beiden Fälle darin, dass sich im Fall $\mathrm{Gal}(f) \cong A_3$ nicht jede Permutation der Nullstellen von f durch einen $\mathbb{Q}$-Automorphismus von L realisieren lässt. Wie aber kann man in der Praxis für ein gegebenes Polynom feststellen, ob dies der Fall ist? Die Antwort auf diese Frage gibt der folgende Satz. Er ist zwar einerseits sehr konkret, andererseits aber auch überraschend komplex, und soll hier vor allem als Beispiel dafür dienen, welche Art von Überlegungen man anstellen muss, um Galoisgruppen explizit zu berechnen.

Satz 5.13 (Galoisgruppen irreduzibler Polynome vom Grad 3)**.** *Es sei $f = t^3 + \lambda_2 t^2 + \lambda_1 t + \lambda_0 \in \mathbb{Q}[t]$ ein normiertes irreduzibles Polynom vom Grad 3. Wir definieren die **Diskriminante** von f als*

$$\Delta := \lambda_1^2\lambda_2^2 - 4\lambda_1^3 - 4\lambda_0\lambda_2^3 + 18\lambda_0\lambda_1\lambda_2 - 27\lambda_0^2 \quad \in \mathbb{Q}.$$

Dann ist $\Delta \neq 0$, und es gilt:

(a) *Ist Δ ein Quadrat in $\mathbb{Q}$, also $\Delta = z^2$ für ein $z \in \mathbb{Q}$, so ist $\mathrm{Gal}(f) \cong A_3$.*

(b) *Ist Δ kein Quadrat in $\mathbb{Q}$, so ist $\mathrm{Gal}(f) \cong S_3$.*

Beweis. Da f irreduzibel ist, hat f nach Folgerung 4.30 drei verschiedene komplexe Nullstellen a_1, a_2, a_3. Offensichtlich gilt dann

$$t^3 + \lambda_2 t^2 + \lambda_1 t + \lambda_0 = (t - a_1)(t - a_2)(t - a_3),$$

woraus man durch Ausmultiplizieren und Koeffizientenvergleich die drei Gleichungen

$$\begin{aligned} \lambda_2 &= -a_1 - a_2 - a_3, \\ \lambda_1 &= a_1a_2 + a_2a_3 + a_3a_1, \\ \lambda_0 &= -a_1a_2a_3 \end{aligned}$$

erhält. Einsetzen dieser Ausdrücke in die Diskriminante von f zeigt nach einer elementaren, aber sehr langen Rechnung, dass

$$\Delta = (a_1 - a_2)^2(a_2 - a_3)^2(a_3 - a_1)^2.$$

Für ein geeignetes $z \in \mathbb{C}$ mit $z^2 = \Delta$ gilt also

$$z = (a_1 - a_2)(a_2 - a_3)(a_3 - a_1). \qquad (*)$$

Da die drei Nullstellen von f verschieden sind, ist ferner $\Delta \neq 0$ und damit auch $z \neq 0$.

(a) Es sei nun $z \in \mathbb{Q}$. Angenommen, die Transposition $(1\ 2)$ wäre in der Galoisgruppe von f, d. h. es gäbe einen $\mathbb{Q}$-Automorphismus σ des Zerfällungskörpers $\mathbb{Q}(a_1, a_2, a_3)$ mit $\sigma(a_1) = a_2$, $\sigma(a_2) = a_1$ und $\sigma(a_3) = a_3$. Wenden wir σ auf die Gleichung $(*)$ an, erhalten wir dann

$$\sigma(z) = (\sigma(a_1) - \sigma(a_2))(\sigma(a_2) - \sigma(a_3))(\sigma(a_3) - \sigma(a_1))$$

und damit

$$z = (a_2 - a_1)(a_1 - a_3)(a_3 - a_2),$$

durch Vergleich mit $(*)$ also $z = -z$, was wegen $z \neq 0$ ein Widerspruch ist. Also ist $(1\ 2) \notin \mathrm{Gal}(f)$, d. h. $\mathrm{Gal}(f)$ ist nicht die gesamte Gruppe S_3 und muss nach Beispiel 5.12 damit isomorph zu A_3 sein.

(b) Ist dagegen $z \notin \mathbb{Q}$, so folgt $[z : \mathbb{Q}] = 2$ wegen $z^2 = \Delta \in \mathbb{Q}$. Aber z liegt wegen der Gleichung $(*)$ offensichtlich im Zerfällungskörper $\mathbb{Q}(a_1, a_2, a_3)$ von f. Damit muss der Grad des Zerfällungskörpers nach Folgerung 2.18 durch 2 teilbar sein. Dies schließt $\mathrm{Gal}(f) \cong A_3$ aus, und nach Beispiel 5.12 bleibt nur noch die Möglichkeit $\mathrm{Gal}(f) \cong S_3$. □

Beispiel 5.14.

(a) Irreduzible kubische Polynome der Form $t^3 - a \in \mathbb{Q}[t]$ haben nach Satz 5.13 stets die Galoisgruppe S_3, denn ihre Diskriminante $\Delta = -27a^2$ ist negativ und damit nie ein Quadrat in $\mathbb{Q}$. In der Tat funktioniert für solche Polynome auch stets das Argument aus Beispiel 5.12, um zu sehen, dass ihre Galoisgruppe S_3 ist.

(b) Im Gegensatz dazu hat das rationale Polynom $f = t^3 - 3t + 1$ die Diskriminante

$$\Delta = -4 \cdot (-3)^3 - 27 \cdot 1^2 = 81 = 9^2,$$

die ein Quadrat in $\mathbb{Q}$ ist. Da f außerdem keine Nullstellen in $\mathbb{Q}$ hat und damit nach Aufgabe 2.7 (a) irreduzibel ist, ist also $\mathrm{Gal}(f) \cong A_3$ nach Satz 5.13.

Wir sehen hier also schon, dass es eine besondere Bedingung ist, dass $\mathrm{Gal}(f) \cong A_3$ gilt. Für die „meisten“ irreduziblen kubischen Polynome über $\mathbb{Q}$ wird die Diskriminante kein Quadrat und die Galoisgruppe daher S_3 sein.

Bemerkung 5.15 (Diskriminanten)**.** Diskriminanten wie in Satz 5.13 kann man nicht nur für kubische Polynome konstruieren. Ist etwa $f = t^n + \lambda_{n-1}t^{n-1} + \cdots + \lambda_1 t + \lambda_0 \in \mathbb{Q}[t]$ ein normiertes Polynom vom Grad n mit (nicht notwendig verschiedenen) Nullstellen $a_1, \ldots, a_n \in \mathbb{C}$, so setzt man

$$\Delta := \prod_{1 \leq i < j \leq n} (a_i - a_j)^2.$$

Offensichtlich ist Δ genau dann gleich Null, wenn f mehrfache Nullstellen in $\mathbb{C}$ besitzt. Die Quadrate in der obigen Formel bewirken, dass Δ unabhängig von der Nummerierung der Nullstellen ist und damit nur von f abhängt. In der Tat kann man zeigen, dass Δ stets ein Polynom in den Koeffizienten $\lambda_0, \ldots, \lambda_{n-1}$ von f und damit insbesondere eine rationale Zahl ist (siehe Aufgabe 6.13 (a)). Für $n = 2$ ist z. B.

$$t^2 + \lambda_1 t + \lambda_0 = (t - a_1)(t - a_2),$$

also

$$\lambda_1 = -a_1 - a_2 \quad \text{und} \quad \lambda_0 = a_1 a_2,$$

und damit

$$\Delta = (a_1 - a_2)^2 = a_1^2 - 2a_1a_2 + a_2^2 = \lambda_1^2 - 4\lambda_0.$$

Dies ist natürlich genau der aus der Lösungsformel für quadratische Gleichungen bekannte Term, der entscheidet, ob es eine oder zwei Lösungen gibt bzw. ob diese Lösungen reell oder komplex sind.

Mit ähnlichen Methoden wie im Beweis von Satz 5.13 kann man nun zeigen, dass die Galoisgruppe $\mathrm{Gal}(f)$ eines irreduziblen Polynoms vom Grad n genau dann eine Untergruppe der alternierenden Gruppe A_n ist, wenn seine Diskriminante Δ ein Quadrat in $\mathbb{Q}$ ist — in Aufgabe 6.13 (a) werden wir zumindest eine Richtung dieser Äquivalenz zeigen.

Bemerkung 5.16. Wie man aus Satz 5.13 schon erahnen kann, ist es im Allgemeinen nicht einfach, die Galoisgruppe eines gegebenen Polynoms zu berechnen — in der Tat wird man für die konkrete Berechnung von Galoisgruppen in der Regel Computeralgebrasysteme einsetzen. Die umgekehrte Frage, wie man zu einer gegebenen Untergruppe $G \leq S_n$ ein Beispiel eines rationalen Polynoms f vom Grad n mit Galoisgruppe G finden kann, und ob ein solches überhaupt für alle G existiert,

ist sogar ein bis heute noch ungelöstes Problem! Es wird im Rahmen der sogenannten *inversen Galoistheorie* untersucht.

Zum Abschluss dieses Kapitels wollen wir nun noch ein paar wichtige Eigenschaften galoisscher Körpererweiterungen angeben.

Lemma 5.17 (Eigenschaften galoisscher Körpererweiterungen)**.**

(a) *Jede Körpererweiterung vom Grad* 2 *ist galoissch.*

(b) *Sind* $K \leq Z \leq L$ *Körper und ist* L/K *galoissch, so auch* L/Z*.*

Beweis.

(a) Nach dem Satz 4.28 vom primitiven Element ist $L = K(a)$ für ein a mit $[a : K] = 2$. Ist f das Minimalpolynom von a, so spaltet f in L natürlich die Nullstelle a ab und zerfällt damit bereits in Linearfaktoren, da es ja ein quadratisches Polynom ist. Also ist L der Zerfällungskörper von f. Damit ist L/K nach Satz 5.8 galoissch.

(b) Ist L/K galoissch, so ist L nach Satz 5.8 der Zerfällungskörper eines Polynoms über K. Dann ist L aber natürlich auch der Zerfällungskörper desselben Polynoms über Z. Wiederum nach Satz 5.8 ist damit auch L/Z galoissch. □

Beachte, dass sich die Eigenschaft „galoissch“ bei verketten Körpererweiterungen also zunächst etwas ungewohnt verhält: sind $K \leq Z \leq L$ Körper und ist die große Körpererweiterung L/K galoissch, so ist es nach Lemma 5.17 (b) auch die „obere“ L/Z. Unter welchen Bedingungen dann auch die „untere“ Erweiterung Z/K galoissch ist, werden wir in Satz 6.14 noch sehen. Definitiv nicht gilt jedoch die Eigenschaft, die man vielleicht als Erstes vermutet hätte, nämlich die Transitivität:

Bemerkung 5.18 (Nicht-Transitivität der Eigenschaft „galoissch“)**.** Sind $K \leq Z \leq L$ Körper und Z/K und L/Z galoissch, so muss deswegen nicht notwendig auch L/K galoissch sein. Dies zeigt das Beispiel $\mathbb{Q} \leq \mathbb{Q}(\sqrt{2}) \leq \mathbb{Q}(\sqrt[4]{2})$: nach Beispiel 3.10 ist $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ und $[\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = 4$, mit der Gradformel aus Satz 2.14 also $[\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}(\sqrt{2})] = 2$. Also sind zunächst einmal die beiden Körpererweiterungen $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ und $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})$ nach Lemma 5.17 (a) galoissch. Aber die zusammengesetzte Körpererweiterung $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ ist nach Satz 5.8 nicht galoissch, denn das Polynom $t^4 - 2 \in \mathbb{Q}[t]$ hat in $\mathbb{Q}(\sqrt[4]{2})$ zwar die Nullstelle $\sqrt[4]{2}$, zerfällt dort aber nicht in Linearfaktoren, da z. B. die komplexe Nullstelle $\sqrt[4]{2}\,i$ nicht im reellen Körper $\mathbb{Q}(\sqrt[4]{2})$ liegt.

Aufgabe 5.19.

(a) Zeige, dass die Körpererweiterung $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$ galoissch mit Galoisgruppe $\mathbb{Z}_2 \times \mathbb{Z}_2$ ist.

(b) Gib ein Beispiel für einen Erweiterungskörper L von $\mathbb{Q}$ an, so dass $L/\mathbb{Q}$ galoissch mit Galoisgruppe $\mathbb{Z}_4$ ist.

(c) Gib ein Beispiel für einen Erweiterungskörper L von $\mathbb{Q}$ an, so dass $L/\mathbb{Q}$ Galoisgruppe $\mathbb{Z}_2 \times \mathbb{Z}_2$ hat, aber *nicht* galoissch ist.

Aufgabe 5.20. Es seien $n \in \mathbb{N}_{>0}$ und $K \leq \mathbb{C}$ ein Körper mit $e^{\frac{2\pi i}{n}} \in K$.

Man zeige: Ist L/K eine einfache n-Radikalerweiterung, so ist L/K galoissch, und die Galoisgruppe $\mathrm{Gal}(L/K)$ ist isomorph zu einer Untergruppe von $\mathbb{Z}_n$.

Aufgabe 5.21 (Translationssatz)**.** Es seien $K \leq L \leq Z$ Körper und $a \in Z$. Man zeige:

Ist die Körpererweiterung $K(a)/K$ galoissch, so ist auch $L(a)/L$ galoissch, und es gilt

$$\mathrm{Gal}(L(a)/L) \cong \mathrm{Gal}(K(a)/(K(a) \cap L)) \leq \mathrm{Gal}(K(a)/K).$$

(Hinweis: Es ist nützlich zu zeigen, dass a über L und $K(a) \cap L$ dasselbe Minimalpolynom hat.)

09