8. Einfache und auflösbare Gruppen

Wir haben am Ende des letzten Kapitels in Bemerkung 7.37 gesehen, dass es praktisch aussichtslos ist, alle endlichen Gruppen klassifizieren zu wollen. Wenn wir ein übersichtlicheres Resultat haben möchten, müssen wir uns also weiter einschränken und nur bestimmte endliche Gruppen untersuchen. Natürlich sollten wir diese Einschränkung aber so vornehmen, dass das Ergebnis hinterher trotzdem noch möglichst vielseitig anwendbar ist.

Die Idee hierfür ist die folgende. Angenommen, wir haben eine endliche Gruppe G, die wir klassifizieren bzw. untersuchen wollen. Wenn G nun einen nicht-trivialen Normalteiler U besitzt, können wir statt G auch erst einmal die kleineren Gruppen U und G/U untersuchen. Da G dann ja die disjunkte Vereinigung aller Nebenklassen von U ist und die Gruppe dieser Nebenklassen gerade G/U ist, können wir in diesem Sinne sagen, dass sich G aus den Gruppen U und G/U „zusammensetzt". Es ist zwar nicht richtig, dass man aus U und G/U die Gruppe G wieder bis auf Isomorphie zurück gewinnen kann, aber dennoch kann man so natürlich viele Informationen über G erhalten, wenn man U und G/U genau kennt.

Diese Strategie lässt sich nun rekursiv fortsetzen: wenn U oder G/U selbst wieder nicht-triviale Normalteiler besitzen, kann man diese wie oben dazu benutzen, um sich auch U oder G/U als aus kleineren Bestandteilen zusammengesetzt vorzustellen. Das Verfahren endet erst bei Gruppen, die keine nicht-trivialen Normalteiler mehr besitzen und die sich daher nicht mehr weiter auf diese Art aufspalten lassen. Gruppen dieser Art bezeichnet man als *einfach* (auch wenn wir in Bemerkung 8.5 noch sehen werden, dass auch diese einfachen Gruppen durchaus sehr kompliziert sein können). In obigem Sinne kann man dann also sagen, dass sich jede endliche Gruppe in einfache Bestandteile zerlegen lässt und es daher für viele Anwendungen ausreicht, die einfachen Gruppen zu klassifizieren.

Wir wollen daher nun kurz diese einfachen Gruppen untersuchen — zumal sie auch eng mit den auflösbaren Gruppen zusammenhängen, die wir später noch für die Untersuchung der Auflösbarkeit von Polynomen aus Problem 0.2 benötigen.

Definition 8.1 (Einfache Gruppen)**.** Eine Gruppe G heißt **einfach**, wenn G keinen nicht-trivialen Normalteiler besitzt, also wenn es kein $U \trianglelefteq G$ gibt mit $U \neq \{e\}$ und $U \neq G$.

Beispiel 8.2. Es sei G eine endliche Gruppe.

(a) Ist $|G| = p$ eine Primzahl, also $G \cong \mathbb{Z}_p$ [G, Satz 6.21 (b)], so besitzt G nach dem Satz von Lagrange [G, Satz 5.10] nicht einmal eine nicht-triviale Untergruppe. Also ist G dann natürlich einfach.

(b) Ist $|G| = q\,p^k$ für ein $k \in \mathbb{N}_{>0}$ und zwei verschiedene Primzahlen p und q mit $q \neq 1 \mod p$, so besitzt G nach Folgerung 7.32 einen Normalteiler der Ordnung p^k und ist somit nicht einfach.

(c) Ist $|G| = 36$, so ist G nicht einfach: nach dem 3. Satz von Sylow aus Satz 7.30 gilt für die Anzahl s_3 der 3-Sylowgruppen von G, dass $s_3 = 1 \mod 3$ und $s_3 \,|\, 4$, also $s_3 = 1$ oder $s_3 = 4$. Wir unterscheiden nun diese beiden Fälle:

- Ist $s_3 = 1$, so ist die einzige 3-Sylowgruppe von G nach [G, Aufgabe 6.9 (b)] ein Normalteiler in G.
- Ist $s_3 = 4$, so operiert G durch Konjugation auf der Menge $\mathrm{Syl}_3(G)$ der 3-Sylowgruppen von G und definiert damit nach Bemerkung 7.12 einen Gruppenhomomorphismus $f : G \to S(\mathrm{Syl}_3(G)) = S_4$. Wegen $|G| = 36 > 24 = |S_4|$ kann dieser natürlich nicht injektiv sein, d. h. es ist $\mathrm{Ker}\, f \neq \{e\}$. Es ist aber auch $\mathrm{Ker}\, f \neq G$, denn andernfalls wäre die Konjugationsoperation trivial, also $aUa^{-1} = U$ für alle $a \in G$ und jede

3-Sylowgruppe U — im Widerspruch zum 2. Satz von Sylow aus Satz 7.29 (b). Da Kerne von Gruppenhomomorphismen immer Normalteiler sind [G, Lemma 6.7], ist $\operatorname{Ker} f$ also ein nicht-trivialer Normalteiler in G.

Aufgabe 8.3. Zeige, dass Gruppen der folgenden Ordnungen nicht einfach sein können:

(a) 42;

(b) 30;

(c) 27.

Wer besonders fleißig ist, kann sogar für jede Zahl $n < 60$, die keine Primzahl ist, zeigen, dass eine Gruppe der Ordnung n nicht einfach sein kann. Hierfür werden keine anderen Methoden benötigt als die in den Fällen (a), (b), (c) oben sowie die aus Beispiel 8.2.

Wie wir jetzt sehen werden, ist damit die kleinste einfache Gruppe, deren Ordnung keine Primzahl ist, die alternierende Gruppe A_5 mit 60 Elementen [G, Beispiel 6.19 (a)].

Satz 8.4. *Die alternierende Gruppe A_5 ist einfach.*

Beweis. Angenommen, es gäbe einen nicht-trivialen Normalteiler $U \trianglelefteq A_5$. Wir unterscheiden drei Fälle:

(a) $|U|$ ist ein Vielfaches von 5. Dann enthält U nach dem 1. Satz von Sylow aus Satz 7.22 eine Untergruppe V der Ordnung 5, also eine 5-Sylowgruppe von A_5. Ist nun $\sigma = (a\ b\ c\ d\ e) \in A_5$ ein 5-Zykel (beachte, dass dieser nach [G, Aufgabe 4.6] auch wirklich Signum 1 hat und damit in A_5 liegt), so ist $\langle \sigma \rangle$ ebenfalls eine 5-Sylowgruppe von A_5 und damit nach Satz 7.29 (b) von der Form $\tau V \tau^{-1}$ für ein $\tau \in A_5$. Damit folgt aber

$$\sigma \in \langle \sigma \rangle = \tau V \tau^{-1} \leq \tau U \tau^{-1} = U,$$

d. h. U enthält sämtliche 5-Zykel. Da man 5-Zykel immer in der Form $(a\ b\ c\ d\ e)$ mit $a = 1$ schreiben kann und jede Permutation der anderen vier Elemente dann einen anderen Zykel liefert, gibt es genau $4! = 24$ solche 5-Zykel. Also enthält U mit der Identität und den 5-Zykeln schon einmal mindestens 25 Elemente.

Da $|U|$ nach dem Satz von Lagrange aber auch ein Teiler von $|A_5| = 60$ sein muss, kommt nur noch $|U| = 30$ in Frage. Damit ist auch 3 ein Teiler von $|U|$, und wir können das obige Argument für die 5-Sylowgruppen wörtlich genauso auch für die 3-Sylowgruppen anwenden, um zu sehen, dass U auch alle 3-Zykel $(a\ b\ c)$ enthalten muss. Die Anzahl solcher 3-Zykel ist $2 \cdot \binom{5}{3} = 20$, da es $\binom{5}{3}$ Möglichkeiten gibt, die Zahlen a, b, c aus der Menge $\{1, \ldots, 5\}$ auszuwählen und es für jede solche Wahl dann genau zwei verschiedene 3-Zykel $(a\ b\ c)$ und $(a\ c\ b)$ gibt. Insgesamt hat U nun also mit der Identität, den 5-Zykeln und den 3-Zykeln schon mindestens $1 + 24 + 20 = 45$ Elemente, im Widerspruch zu $|U| = 30$. Also ist dieser erste Fall, in dem $|U|$ ein Vielfaches von 5 ist, unmöglich.

(b) $|U|$ ist ein Vielfaches von 3. Dies führt man genauso zum Widerspruch wie in Fall (a), nur dass man hier zuerst die 3-Sylowgruppen und danach die 5-Sylowgruppen betrachtet.

(c) $|U|$ ist weder ein Vielfaches von 5 noch von 3. Als Teiler von $|A_5| = 60$ kommen für $|U|$ dann nur noch 2 und 4 in Frage. In jedem Fall enthält U wiederum nach dem 1. Satz von Sylow eine Untergruppe und damit auch ein Element der Ordnung 2. Da die Elemente der Ordnung 2 in A_5 genau die Doppeltranspositionen $(a\ b)(c\ d)$ sind, können wir ohne Einschränkung annehmen, dass $(1\ 2)(3\ 4) \in U$. Dann liegen aber auch die hierzu in A_5 konjugierten Elemente in U, also z. B.

$$(1\ 2\ 5)(1\ 2)(3\ 4)(1\ 2\ 5)^{-1} = (5\ 2)(3\ 4),$$
$$(2\ 1\ 5)(1\ 2)(3\ 4)(2\ 1\ 5)^{-1} = (1\ 5)(3\ 4),$$
$$(3\ 4\ 5)(1\ 2)(3\ 4)(3\ 4\ 5)^{-1} = (1\ 2)(5\ 4).$$

Zusammen mit der Identität muss U also mindestens 5 Elemente enthalten, im Widerspruch zu $|U| \leq 4$.

Insgesamt erhalten wir also in jedem Fall einen Widerspruch. Damit kann A_5 keinen nicht-trivialen Normalteiler besitzen. □

Bemerkung 8.5 (Klassifikation einfacher Gruppen)**.** Wir hatten in Bemerkung 7.37 gesehen, dass die Klassifikation aller endlichen Gruppen modulo Isomorphie praktisch ein aussichtsloses Unterfangen ist. Beschränkt man sich nun mit dem Hintergrund der Einleitung zu diesem Kapitel auf einfache Gruppen, so wird die Situation sofort deutlich überschaubarer: so haben wir z. B. in Beispiel 8.2 und Aufgabe 8.3 gesehen, dass die einfachen Gruppen mit weniger als 60 Elementen genau die zyklischen Gruppen $\mathbb{Z}_p$ von Primzahlordnung sind — während die Tabelle in Bemerkung 7.37 ja zeigt, dass es ohne die Einschränkung der Einfachheit auch für diese kleinen Gruppenordnungen bereits sehr viel mehr verschiedene Gruppen gibt.

In der Tat ist die Klassifikation der einfachen endlichen Gruppen inzwischen ein gelöstes Problem. Wann genau das Problem endgültig gelöst wurde, lässt sich allerdings gar nicht so genau sagen, da sich das gesamte Resultat über unzählige Forschungsarbeiten aus der 2. Hälfte des 20. Jahrhunderts erstreckt, in denen in den ersten Jahren nach der Veröffentlichung immer mal wieder kleine Fehler entdeckt wurden, die dann nachträglich noch korrigiert werden mussten. Auch das Ergebnis der Klassifikation ist so kompliziert, dass wir es hier gar nicht vollständig angeben, sondern nur kurz skizzieren können:

(a) Die zyklischen Gruppen $\mathbb{Z}_p$ für eine Primzahl p sind einfach (siehe Beispiel 8.2 (a)). Man sagt, dass sie eine *Serie* einfacher Gruppen bilden.

(b) Die kleinste einfache Gruppe, die nicht von dieser Form ist, ist die alternierende Gruppe A_5 mit 60 Elementen (siehe Aufgabe 8.3 und Satz 8.4). In der Tat kann man zeigen, dass alle alternierenden Gruppen A_n für $n \geq 5$ einfach sind und damit eine weitere Serie einfacher Gruppen bilden.

(c) Die kleinste einfache Gruppe, die nicht von der Form (a) oder (b) ist, hat Ordnung 168. Es handelt sich hierbei um die multiplikative Gruppe

$$\{A \in \mathrm{Mat}(2 \times 2, \mathbb{Z}_7) : \det A = 1\}/\{E, -E\}$$

aller invertierbaren 2×2-Matrizen mit Determinante 1 über dem Körper $\mathbb{Z}_7$, modulo dem von der negativen Einheitsmatrix erzeugten Normalteiler. Auch dieses Beispiel führt gleich zu einer ganzen Serie einfacher Gruppen, wenn man die Größe der quadratischen Matrizen variiert oder den Grundkörper $\mathbb{Z}_7$ durch einen anderen endlichen Körper ersetzt. Man kann sogar noch auf geeignete Art die Bedingungen an die Matrizen durch andere ersetzen (z. B. $\det A = 1$ durch $A^T \cdot A = E$, so dass man also nur orthogonale Matrizen betrachtet) und erhält so nicht nur eine, sondern insgesamt 16 solcher Serien von einfachen „Matrixgruppen“.

(d) Die kleinste einfache Gruppe, die nicht von der Form (a), (b) oder (c) ist, hat Ordnung 7920. Man wird nun wohl befürchten (und hat dies sicher auch getan, solange man die Klassifikation der einfachen Gruppen noch nicht vollständig gefunden hatte), dass dieses Prinzip immer so weiter geht: immer neue und komplizierter werdende Serien, und immer wieder die nächste Ausnahme. Dem ist allerdings nicht so: das erstaunliche Resultat ist nun, dass es nur noch genau 26 einfache Gruppen gibt, die nicht in die Serien (a), (b) oder (c) passen. Diese Gruppen werden *sporadische Gruppen* genannt. Die größte von ihnen hat übrigens die Ordnung

$$808017424794512875886459904961710757005754368000000000$$

und wird als *Monstergruppe* bezeichnet, während die zweitgrößte mit der Ordnung

$$4154781481226426191177580544000000$$

das *Baby-Monster* genannt wird.

Nach den einfachen Gruppen kommen wir nun zum eng verwandten Konzept der auflösbaren Gruppen. Wie bereits erwähnt wird dies dann letztlich genau der Begriff sein, der in der Gruppentheorie der Auflösbarkeit von Polynomen entspricht.

Definition 8.6 (Auflösbare Gruppen)**.** Eine endliche Gruppe G heißt **auflösbar**, wenn es eine Kette

$$\{e\} = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_n = G$$

von Untergruppen von G gibt, so dass G_{i-1} für alle $i = 1, \ldots, n$ ein Normalteiler in G_i ist und die zugehörigen Faktorgruppen G_i/G_{i-1} abelsch sind.

Bemerkung 8.7.

(a) Beachte bei der Schreibweise von Definition 8.6, dass die Normalteilereigenschaft im Allgemeinen nicht transitiv ist! Die Gruppen in der Kette müssen also z. B. keine Normalteiler in G, sondern lediglich in der jeweils nächsten Gruppe der Kette sein.

(b) Im Sinne der Einleitung zu diesem Kapitel kann man auch bei einer auflösbaren Gruppe sagen, dass sie sich mit der Notation aus Definition 8.6 aus den einzelnen Bestandteilen G_i/G_{i-1} „zusammensetzt“. Man kann sich eine auflösbare Gruppe daher als eine Gruppe vorstellen, die sich in abelsche Anteile aufspalten lässt. Da wir die abelschen Gruppen ja im Hauptsatz über endlich erzeugte abelsche Gruppen aus Folgerung 7.4 vollständig klassifiziert haben, ist diese Aufspaltung hier also besonders einfach.

Beispiel 8.8.

(a) Natürlich ist jede abelsche Gruppe G auflösbar, da wir hier ja die triviale Kette $\{e\} \trianglelefteq G$ nehmen können.

(b) Die symmetrische Gruppe S_3 ist auflösbar, denn in der Kette

$$\{\mathrm{id}\} \trianglelefteq A_3 \trianglelefteq S_3$$

sind A_3 (mit 3 Elementen) und S_3/A_3 (mit 2 Elementen) als Gruppen von Primzahlordnung beide zyklisch [G, Satz 6.21 (b)] und damit insbesondere abelsch.

(c) Ist G einfach und nicht abelsch, so kann G nicht auflösbar sein: die triviale Kette wie in (a) ist dann ja nicht zulässig, und andere kann es nicht geben, da G überhaupt keine nicht-trivialen Normalteiler besitzt. Insbesondere folgt aus Satz 8.4 also, dass die alternierende Gruppe A_5 nicht auflösbar ist.

Um weitere Beispiele auflösbarer und nicht auflösbarer Gruppen einfacher angeben zu können, brauchen wir zunächst ein paar einfache Eigenschaften auflösbarer Gruppen.

Aufgabe 8.9 (Eigenschaften auflösbarer Gruppen)**.** Es sei G eine endliche Gruppe. Man zeige:

(a) G ist genau dann auflösbar, wenn es eine Kette

$$\{e\} = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_n = G$$

gibt, so dass $|G_i/G_{i-1}|$ für alle i eine Primzahl ist.

(Hinweis: Zeige mit Hilfe von Folgerung 7.7, dass sich eine Kette mit abelschen Quotienten wie in Definition 8.6 stets zu einer Kette verfeinern lässt, in der die Quotienten Primzahlordnung haben.)

(b) Ist G auflösbar und $U \leq G$, so ist auch U auflösbar.

(c) Ist $U \trianglelefteq G$, so ist G genau dann auflösbar, wenn U und G/U auflösbar sind.

Folgerung 8.10.

(a) *Jede Gruppe mit weniger als* 60 *Elementen ist auflösbar.*

(b) *Die symmetrischen und alternierenden Gruppen S_n und A_n sind genau für $n \leq 4$ auflösbar.*

Beweis.

(a) Es sei G eine Gruppe mit $|G| = n < 60$. Wir zeigen mit Induktion über n, dass G auflösbar ist; der Induktionsanfang für $n = 1$ ist natürlich trivial.

Ist n eine Primzahl, so ist $G \cong \mathbb{Z}_n$ [G, Satz 6.21 (b)], also insbesondere abelsch und damit auch auflösbar. Andernfalls ist G nach Aufgabe 8.3 nicht einfach und besitzt daher einen nicht-trivialen Normalteiler U. Nach Induktionsvoraussetzung sind U und G/U dann auflösbar, mit Aufgabe 8.9 (c) also auch G.

(b) Der Fall $n \leq 4$ wird durch (a) abgedeckt. Für $n \geq 5$ hingegen enthalten sowohl S_n als auch A_n die alternierende Gruppe A_5 als Untergruppe. Da A_5 nach Beispiel 8.8 (c) nicht auflösbar ist, können nach Aufgabe 8.9 (b) also auch S_n und A_n für $n \geq 5$ nicht auflösbar sein. □

Wir wollen nun unsere Ergebnisse zu auflösbaren Gruppen anwenden, um Aussagen über die Auflösbarkeit von Polynomen zu beweisen. Es sei dazu $f = t^n + a_{n-1}t^{n-1} + \cdots + a_1 t + a_0 \in \mathbb{C}[t]$ ein komplexes Polynom und $K = \mathbb{Q}(a_0, \ldots, a_{n-1})$. Wir erinnern uns daran, dass wir f in Definition 1.20 auflösbar genannt haben, wenn sich alle Nullstellen von f aus K mit Hilfe der Körperoperationen und komplexem Wurzelziehen exakt berechnen lassen, also wenn es eine Radikalerweiterung

$$K = K_0 \leq K_1 \leq \cdots \leq K_n = L$$

von K in $\mathbb{C}$ gibt, so dass L alle Nullstellen und damit den Zerfällungskörper von f über K enthält.

Formal sieht dieses Kriterium fast genauso aus wie das der Konstruierbarkeit mit Zirkel und Lineal in Beispiel 1.23. Allerdings besteht ein wesentlicher Unterschied darin, dass wir im Fall der Konstruktionen mit Zirkel und Lineal nur 2-Radikalerweiterungen zugelassen haben, was zu der einfachen numerischen Bedingung geführt hat, dass der Grad von L (und damit auch von allen Elementen von L) über K eine Zweierpotenz sein musste (siehe Folgerung 2.22 und Beispiel 2.23). Im nun vorliegenden Fall der Auflösbarkeit haben wir dagegen keine solche Gradbeschränkung und können daher auch kein analoges einfaches numerisches Kriterium für die Auflösbarkeit von f erwarten.

Die entscheidende Beobachtung zur Lösung dieses Problems ist nun, dass eine einfache m-Radikalerweiterung nach Aufgabe 5.20 stets eine *abelsche* Galoisgruppe besitzt (zumindest unter der technischen Zusatzvoraussetzung, dass der Grundkörper bereits die m-ten Einheitswurzeln enthält — wir werden gleich aber sehen, dass diese Voraussetzung kein größeres Problem darstellt). Wir wollen nun zeigen, dass die obige Kette von Zwischenkörpern auf diese Art mit Hilfe der Galoistheorie einer Kette von Gruppen entspricht, von denen jeweils der Quotient von zwei aufeinander folgenden eine abelsche Gruppe ist — was also genau zum Konzept von auflösbaren Gruppen führt.

Lemma 8.11. *Es seien $K \leq L \leq \mathbb{C}$ Körper, so dass L/K eine Radikalerweiterung ist. Ferner sei Z ein Zwischenkörper von L/K, der galoissch über K ist. Dann ist die Galoisgruppe* $\mathrm{Gal}(Z/K)$ *auflösbar.*

Beweis. Nach Definition 1.18 einer Radikalerweiterung gibt es eine Kette

$$K = K_0 \leq K_1 \leq \cdots \leq K_n = L, \qquad (*)$$

so dass jedes K_j/K_{j-1} eine einfache Radikalerweiterung ist.

Als ersten Reduktionsschritt wollen wir zunächst zeigen, dass wir annehmen dürfen, dass jede Körpererweiterung K_j/K_{j-1} in dieser Kette zusätzlich galoissch mit abelscher Galoisgruppe ist. Es sei dazu K_j/K_{j-1} eine einfache m_j-Radikalerweiterung. Mit $m := m_1 \cdot \cdots \cdot m_n$ und $z := e^{\frac{2\pi i}{m}}$ betrachten wir nun statt $(*)$ die Kette

$$K = K_0 \leq K_0(z) \leq K_1(z) \leq \cdots \leq K_n(z) = L(z),$$

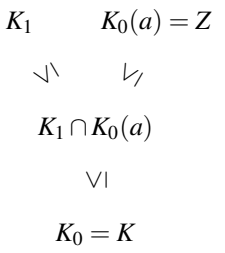
in der wir als Erstes die m-te Einheitswurzel adjungieren. Natürlich sind hier weiterhin alle Körpererweiterungen einfache Radikalerweiterungen (die erste, neue Erweiterung $K_0(z)/K_0$ ist offensichtlich eine einfache m-Radikalerweiterung), und Z ist immer noch ein Zwischenkörper von $L(z)/K$. Weiterhin ist nun jede Körpererweiterung in dieser Kette galoissch mit abelscher Galoisgruppe:

- für die erste Erweiterung $K_0(z)/K_0$ folgt dies aus dem Translationssatz aus Aufgabe 5.21, da $\mathbb{Q}(z)/\mathbb{Q}$ nach Beispiel 5.3 (c) galoissch mit abelscher Galoisgruppe $\mathbb{Z}_m^*$ ist;

- für alle anderen Erweiterungen der Kette ergibt sich dies aus Aufgabe 5.20, die besagt, dass $K_j(z)/K_{j-1}(z)$ galoissch mit abelscher Galoisgruppe (nämlich einer Untergruppe von $\mathbb{Z}_{m_j}$) ist, da $K_{j-1}(z)$ mit $e^{\frac{2\pi i}{m}}$ insbesondere auch die m_j-te Einheitswurzel enthält.

Wir können der Einfachheit halber also annehmen, dass die ursprüngliche Kette $(*)$ bereits so gewählt war, dass jede Körpererweiterung galoissch mit abelscher Galoisgruppe ist. Darüber hinaus können wir nach dem Satz 4.28 vom primitiven Element annehmen, dass $Z = K(a)$ für ein $a \in Z$.

Wir zeigen die Behauptung des Lemmas nun mit Induktion über n; der Induktionsanfang für $n = 0$ ist trivial. Es sei also $n > 0$. Wir betrachten wie im Bild rechts dargestellt den Körper $K_1 \cap K_0(a)$ als Zwischenkörper der beiden Erweiterungen K_1/K_0 und Z/K.



Wir beginnen mit der linken Erweiterung K_1/K_0, die nach unserem Reduktionsschritt galoissch mit abelscher Galoisgruppe ist. Die in der Galois-Korrespondenz zum Zwischenkörper $K_1 \cap K_0(a)$ gehörige Untergruppe von $\mathrm{Gal}(K_1/K_0)$ ist damit natürlich automatisch ein Normalteiler. Nach Satz 6.14 ist die im Bild untere Körpererweiterung $K_1 \cap K_0(a)/K_0$ damit ebenfalls galoissch, und ihre Galoisgruppe ist als Faktorgruppe der abelschen Gruppe $\mathrm{Gal}(K_1/K_0)$ ebenfalls abelsch.

Wir gehen nun zur rechten Körpererweiterung Z/K über, die ja nach Voraussetzung des Lemmas galoissch ist. Da wir die untere Körpererweiterung $K_1 \cap K_0(a)/K_0$ gerade als galoissch erkannt haben, können wir wiederum mit Satz 6.14 schließen, dass die zum Zwischenkörper $K_1 \cap K_0(a)$ gehörige Untergruppe $\mathrm{Gal}(Z/K_1 \cap K_0(a))$ von $\mathrm{Gal}(Z/K)$ ein Normalteiler ist, und dass

$$\mathrm{Gal}(K_1 \cap K_0(a)/K_0) \;=\; \mathrm{Gal}(Z/K) \;/\; \mathrm{Gal}(Z/K_1 \cap K_0(a)).$$

Um die Auflösbarkeit von $\mathrm{Gal}(Z/K)$ zu beweisen, genügt es nach Aufgabe 8.9 (c) also, die Auflösbarkeit der beiden Gruppen $\mathrm{Gal}(K_1 \cap K_0(a)/K_0)$ und $\mathrm{Gal}(Z/K_1 \cap K_0(a))$ zu zeigen:

- $\mathrm{Gal}(K_1 \cap K_0(a)/K_0)$ ist nach Beispiel 8.8 (a) auflösbar, denn von dieser Gruppe haben wir oben ja bereits gesehen, dass sie abelsch ist.
- $\mathrm{Gal}(Z/K_1 \cap K_0(a)) = \mathrm{Gal}(K_0(a)/K_1 \cap K_0(a))$ ist nach dem Translationssatz aus Aufgabe 5.21 isomorph zu $\mathrm{Gal}(K_1(a)/K_1)$. Diese Gruppe ist nun aber nach Induktionsvoraussetzung auflösbar, denn $K_1(a)$ ist einerseits nach Aufgabe 5.21 galoissch über K_1, und andererseits ein Zwischenkörper der $(n-1)$-stufigen Radikalerweiterung $K_1 \leq \cdots \leq K_n = L$.

Damit ist $\mathrm{Gal}(Z/K)$ auflösbar. □

Folgerung 8.12 (Auflösbarkeit von Polynomen und Gruppen)**.** *Es seien $f = t^n + a_{n-1}t^{n-1} + \cdots + a_1 t + a_0 \in \mathbb{C}[t]$ ein komplexes Polynom und $K = \mathbb{Q}(a_0, \ldots, a_{n-1})$. Ist f dann auflösbar im Sinne von Definition 1.20, so ist die Galoisgruppe des Zerfällungskörpers von f über K auflösbar im Sinne von Definition 8.6.*

Beweis. Es sei $Z \leq \mathbb{C}$ der Zerfällungskörper von f über K. Weil f auflösbar ist, ist Z nach Definition 1.20 in einer Radikalerweiterung L von K enthalten. Da Z als Zerfällungskörper außerdem nach Satz 5.8 galoissch über K ist, folgt die Behauptung nun sofort aus Lemma 8.11. □

Beispiel 8.13. Es sei $f \in \mathbb{Q}[t]$ ein rationales Polynom vom Grad $n \geq 5$. Nach Lemma 5.11 (a) ist die Galoisgruppe $\mathrm{Gal}(f)$ dann eine Untergruppe von S_n. Ist sogar $\mathrm{Gal}(f) = S_n$, so ist $\mathrm{Gal}(f)$ damit nach Folgerung 8.10 (b) nicht auflösbar, d. h. nach Folgerung 8.12 ist dann auch f nicht auflösbar. In der Tat ist dies für die meisten Polynome vom Grad $n \geq 5$ der Fall. Die folgende Aufgabe gibt ein konkretes Beispiel dafür.

Aufgabe 8.14 (Beispiel für ein nicht-auflösbares Polynom)**.** Für das Polynom $f = t^5 - 80t + 2 \in \mathbb{Q}[t]$ zeige man:

(a) f ist irreduzibel und hat genau drei reelle Nullstellen.

(b) $\mathrm{Gal}(f)$ ist isomorph zu einer Untergruppe $U \leq S_5$ mit $(1\ 2\ 3\ 4\ 5) \in U$ und $(1\ 2) \in U$.

(c) $\mathrm{Gal}(f) \cong S_5$.

Nach Beispiel 8.13 ist f damit also nicht auflösbar.

Bemerkung 8.15. Man kann zeigen, dass in Folgerung 8.12 auch die Umkehrung gilt, dass ein Polynom also genau dann auflösbar ist, wenn sein Zerfällungskörper eine auflösbare Galoisgruppe besitzt [B, Kapitel 6.1]. Da Untergruppen von S_n für $n \leq 4$ nach Folgerung 8.10 (a) stets auflösbar sind, bedeutet dies also, dass Polynome vom Grad höchstens 4 immer auflösbar sind — was man aber natürlich auch schon ohne die Hilfe der Galoistheorie wusste, da in diesen Fällen nach Problem 0.2 ja konkrete Lösungsformeln existieren.

14