Diplomarbeit

Ein Algorithmus zum Lösen einer Polynomgleichung durch Radikale

Andreas Distler

Betreuerin
Professor Dr. Bettina Eick
Institut Computational Mathematics
Technische Universität Braunschweig
Pockelsstr.14
38106 Braunschweig

Braunschweig, den 10. Mai 2005

Gewidmet meinem Großvater

Selbständigkeitserklärung

Hiermit versichere ich, die vorliegende Arbeit selbständig verfasst und keine anderen als die angegebenen Quellen benutzt zu haben.

Braunschweig, den 10. Mai 2005

Andreas Distler

Inhaltsverzeichnis

Kapitel 1

Einleitung

Jeder Schüler lernt heutzutage, wie man die Nullstellen eines quadratischen Polynoms unter Verwendung eines Wurzelausdrucks bestimmt. So ist etwa

$$x_{1,2} = -\frac{s}{2} \pm \sqrt{\left(\frac{s}{2}\right)^2 - p}$$

die allgemeine Auflösungsformel zu $x^2 + sx + p = 0$, der normierten Form einer quadratischen Gleichung.

In der vorliegenden Arbeit geht es um die Verallgemeinerung dieses Problems. Gegeben sei ein Polynom f aus $\mathbb{Q}[x]$. Es wird ein Algorithmus und dessen Implementation vorgestellt, der die Nullstellen von f mit Hilfe von Wurzelausdrücken angibt, falls dies möglich ist. Wie für quadratische Polynome, erhält man dabei Ausdrücke der Form

$$q_1 + \sqrt[n]{q_2 + q_3 \sqrt[m]{q_4} + \cdots + \sqrt[r]{q_5}},\ q_i \in \mathbb{Q}, n, m, r \in \mathbb{N}.$$

Diese Darstellung durch Radikale gibt an, wie man die Lösungen von $f(x) = 0$ durch Anwenden der vier Grundrechenarten und Wurzelziehen aus den Koeffizienten von f ermittelt. Insbesondere wird untersucht, wie praktikabel die Bestimmung einer Radikaldarstellung mittels Computern zur Zeit ist.

Die Grundidee des Algorithmus geht auf Évariste Galois (1811–1832) zurück [13].

1.1 Zur Geschichte des Auflösens von Polynomgleichungen

Schon die Babylonier lösten um 1700 v. Chr. quadratische Gleichungen durch Anwenden der vier Grundrechenarten und einmaliges Wurzelziehen. Eine ausführliche Darstellung der Rechenmethoden, die auf den Ergebnissen von NEUGEBAUER [25] basiert, findet sich im Buch von EDWARDS [11]. Als damalige Standardform des Problems waren zwei Zahlen zu finden, deren Produkt und Summe man kannte. Dies ist die Frage nach der Lösung des Gleichungssystems $x + y = s$ und $xy = p$, für bekannte Zahlen s und p. Wie man leicht durch Einsetzen verifiziert, sind die gesuchten Zahlen gerade die beiden Lösungen der quadratischen Gleichung $z^2 - sz + p = 0$. Die Babylonier lösten das Problem nach folgendem Schema:

1. Halbiere s.
2. Quadriere das Ergebnis.
3. Subtrahiere davon p.
4. Ziehe die Wurzel aus der Differenz.
5. Addiere die Hälfte von s; dies ist die erste der gesuchten Zahlen und die andere ist s weniger der ersten.

In Formelschreibweise erhält man daraus

$$x = \frac{s}{2} + \sqrt{\left(\frac{s}{2}\right)^2 - p} \quad \text{und} \quad y = s - x,$$

was der einleitend angegebenen Lösungsformel entspricht.

Bis zur Entdeckung von Lösungsformeln für allgemeine Gleichungen dritten und vierten Grades vergingen mehr als 3000 Jahre. Sie wurden im 16. Jahrhundert von europäischen Mathematikern hergeleitet. Laut STROTH [31] entwickelte Scipione del Ferro (1465–1526) als erster Lösungsformeln für kubische Gleichungen. Veröffentlicht wurden solche aber erst von Girolamo Cardano (1501–1576), dessen Ansatz auf Niccolo Tartaglia (1499–1557) zurückgeht, in seinem Werk *Ars Magna*. Für $x^3 + px + q = 0$ erhält man demnach

$$x = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{p^3}{27} + \frac{q^2}{4}}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{p^3}{27} + \frac{q^2}{4}}}.$$

An derselben Stelle wurden auch die von Ludovico Ferrari (1522–1565) erdachten Formeln zum Lösen biquadratischer Gleichungen niedergeschrieben. Aufgrund ihrer komplexen Struktur wird hier nicht näher auf deren Gestalt eingegangen. Eine Angabe der Formeln befindet sich aber im Hauptteil dieser Arbeit als Satz 4.1.3.

Im Jahre 1824 bewies Niels Henrik Abel (1802–1829), dass algebraische Auflösungsformeln, die Wurzelausdrücke in den Koeffizienten sind, für allgemeine Polynome höherer Grade nicht existieren [1]. Unbeantwortet blieb die Frage, welche Polynome durch Wurzeln darstellbare Nullstellen besitzen. Dazu brachten die Ideen von Évariste Galois (1811–1832) den Durchbruch [13]. Er übertrug das Problem der Auflösbarkeit durch Radikale von der Körper- in die Gruppentheorie. Anstatt direkt den Erweiterungskörper, in dem alle Nullstellen des gegebenen Polynoms liegen, zu betrachten, untersuchte Galois die heute nach ihm benannte Automorphismengruppe des Körpers. Das ursprüngliche Problem findet dabei sein Äquivalent in der Frage, ob diese Gruppe auflösbar ist. Galois führte seinen Beweis konstruktiv und zeigte daher gleichzeitig eine Möglichkeit auf, eine Darstellung der Nullstellen durch Wurzelausdrücke zu bestimmen.

Basierend auf den Methoden von Galois wurden seither immer wieder Nullstellen einzelner Polynome ermittelt. So vollendete im Jahre 1894 Johann Gustav Hermes (1846–1912) seine zwölfjährigen Bemühungen eine 65 537-te primitive Einheitswurzel mit Zirkel und Lineal zu konstruieren [15], was einer Darstellung durch Quadratwurzeln gleichkommt. Aufgrund der Komplexität der notwendigen Berechnungen lag jedoch kein praktikabler Lösungsweg für beliebige Polynome vor. Deshalb bemühte man sich, verbesserte Methoden zu entwickeln. Während sich der algorithmische Ansatz seit Galois nicht grundsätzlich geändert hat, gibt es für die anfallenden Berechnungen inzwischen schnellere Vorgehensweisen. Auch Untersuchungen zu Komplexitätsabschätzungen waren erfolgreich. Im Jahre 1985 erbrachten Landau und Miller [22] den Beweis, dass ein Algorithmus mit polynomialer Laufzeit existiert, der die Auflösbarkeit einer Polynomgleichung durch Radikale überprüft. Solche Fortschritte motivierten und ermöglichten die vorliegende Arbeit.

Ein weiterer Aspekt besteht darin, nicht nach irgendeinem Wurzelausdruck für die Nullstelle eines Polynoms zu suchen, sondern nach einem möglichst einfachen. Wege, einen solchen zu ermitteln, beziehungsweise einen gegebenen Ausdruck zu vereinfachen, wurden von Landau in [21] und, darauf aufbauend, von Horng und Huang in [16] untersucht.

Neben der Darstellung durch Radikale wurden andere Möglichkeiten gefunden, die Nullstellen eines Polynoms anzugeben. Allen voran ist die numerische Näherungslösung zu nennen, welche beispielsweise mit dem Newton-Verfahren bestimmt werden kann (siehe z. B. [27]). So werden angenäherte Werte der Nullstellen eines Polynoms auch bei bestimmten Methoden zur Berechnung der Galoisgruppe verwendet (siehe [30]). Des Weiteren ist die Angabe allgemeiner Lösungformeln für Polynome durchaus möglich, wenn man sich nicht auf algebraische Operationen (Addition, Subtraktion, Multiplikation, Division und Wurzelziehen) beschränkt, sondern Funktionen, die mittels Potenzreihen gebildet werden, in die Formeln einbezieht. So gelang es Umemura, die Wurzeln eines beliebigen Polynoms durch Thetafunktionen auszudrücken (vgl. [35]).

1.2 Ein Überblick des Algorithmus

Mittelpunkt dieser Arbeit ist der Algorithmus in Kapitel 5. Dieser wird im Folgenden kurz erläutert. Details und Definitionen der benutzten Begriffe werden in den späteren Kapiteln vorgestellt.

Es wird ein normiertes und irreduzibles Polynom f aus $\mathbb{Q}[x]$ vom Grad n betrachtet. Gesucht ist eine Radikaldarstellung der Wurzeln von f. Es gilt also Elemente $\alpha_1, \ldots, \alpha_n$ zu finden, die $f(x) = (x - \alpha_1) \cdots (x - \alpha_n)$ erfüllen, und diese etwa in der Form

$$q_1 + \sqrt[n]{q_2 + q_3 \sqrt[m]{q_4} + \cdots + \sqrt[r]{q_5}},\ q_i \in \mathbb{Q}, n, m, r \in \mathbb{N}$$

darzustellen. Eine Darstellung der Nullstellen des Polynoms $x^6 + x^4 - x^3 - 2x^2 + x + 1$ ist beispielsweise durch $-\frac{1}{3}\sqrt{-3} + \frac{1}{6}\sqrt[3]{108 + 12\sqrt{-3}}$ gegeben.

Die grundlegende Idee zur algorithmischen Bearbeitung dieser Aufgabe wird durch folgende Anweisungen vermittelt:

Zunächst wird geprüft, ob die Galoisgruppe G_f von f auflösbar ist. Sollte dies nicht der Fall sein, so existiert nach Galois keine Darstellung der Nullstellen mittels Radikale und der Algorithmus bricht hier ab. Anderenfalls wird eine Kompositionsreihe

$$G_f = G_1 \rhd G_2 \rhd \cdots \rhd G_r \rhd G_{r+1} = \{1\}$$

von G_f berechnet. Als nächstes wird der Zerfällungskörper $\mathbb{Q}_f$ von f konstruiert und als einfache Erweiterung $\mathbb{Q}_f = \mathbb{Q}(\gamma)$ dargestellt. Nach dem Hauptsatz der Galoistheorie besteht eine Korrespondenz zwischen den Untergruppen der Galoisgruppe und den Zwischenkörpern des Zerfällungskörpers. Dies wird genutzt, um eine Körperkette

$$\mathbb{Q} = K_1 \subset K_2 \subset \cdots \subset K_r \subset K_{r+1} = \mathbb{Q}_f$$

zu ermitteln, die zur berechneten Kompositionsreihe korrespondiert. Es ist K_i jeweils der Fixkörper $\mathrm{Fix}_{\mathbb{Q}_f}(G_i)$ zu G_i. Da von $\mathbb{Q}_f$ das primitive Element γ bekannt ist, können auch die Glieder der Körperkette als einfache Erweiterungen $K_{i+1} = K_i(\beta_i)$ bestimmt werden. Im Weiteren bezeichnet h das Produkt der Primfaktoren, die in der Ordnung der Galoisgruppe auftauchen. Durch Adjunktion einer primitiven h-ten Einheitswurzel ζ_h werden die Körper $\widetilde{K}_i = K_i(\zeta_h)$ gebildet. Zu jedem Primteiler p der Gruppenordnung liegt somit die p-te Einheitswurzel vor. Dann können die Erweiterungen $\widetilde{K}_{i+1}/\widetilde{K}_i$ vom Grad $\widetilde{p}_i$ durch Adjunktion einer $\widetilde{p}_i$-ten Wurzel erzeugt werden. Es wird also für jedes $i \in \{1, \ldots, r\}$ ein Element $a_i \in \widetilde{K}_i$ mit $\widetilde{K}_{i+1} = \widetilde{K}_i(\sqrt[\widetilde{p}_i]{a_i})$ berechnet. Es ergibt sich für $\mathbb{Q}_f$ die $\mathbb{Q}$-Basis $\{\zeta_h^j \sqrt[p_1]{a_1}^{e_1} \ldots \sqrt[p_r]{a_r}^{e_r} \mid 0 \leq j < \phi(h), 0 \leq e_i < \widetilde{p}_i\}$. Bezüglich dieser Basis gilt es als letzten Schritt, die Darstellung der Nullstellen von f zu finden. Dazu ist für jede Nullstelle ein lineares Gleichungssystem zu lösen.

Die Strukturierung von Kapitel 5 wie auch die Implementation [10] richtet sich daher nach folgendem Schema:

1. Untersuche die Galoisgruppe G_f von f auf Auflösbarkeit.
   - Ist G_f nicht auflösbar $\Rightarrow$ Abbruch
2. Konstruiere den Zerfällungskörper $\mathbb{Q}_f = \mathbb{Q}(\gamma)$ von f.
3. Berechne eine Kompositionsreihe $G_f = G_1 \rhd G_2 \rhd \cdots \rhd G_r \rhd G_{r+1} = \{1\}$.
4. Bestimme eine zur Kompositionsreihe korrespondierende Körperkette $\mathbb{Q} = K_1 \subset K_2 \subset \cdots \subset K_r \subset K_{r+1} = \mathbb{Q}_f$ mit $K_i = \mathrm{Fix}_{\mathbb{Q}_f}(G_i)$.
5. Bilde $\widetilde{K}_i = K_i(\zeta_h)$, wobei h das Produkt der in $|G_f|$ vorkommenden Primfaktoren und ζ_h eine primitive h-te Einheitswurzel sind.
6. Berechne Elemente $a_i \in \widetilde{K}_i$ mit $\widetilde{K}_{i+1} = \widetilde{K}_i(\sqrt[\widetilde{p}_i]{a_i})$ und $\widetilde{p}_i = [\widetilde{K}_{i+1} : \widetilde{K}_i]$.
7. Finde zur $\mathbb{Q}$-Basis $\{\zeta_h^j \sqrt[\widetilde{p}_1]{a_1}^{e_1} \ldots \sqrt[\widetilde{p}_r]{a_r}^{e_r} \mid 0 \leq j < h, 0 \leq e_i < \widetilde{p}_i\}$ von $\mathbb{Q}_f$ die Darstellung der Nullstellen $\alpha_1, \ldots, \alpha_n$ von f.

1.3 Gliederung der Arbeit

Nachdem eine Übersicht des Algorithmus vorliegt, werden die Inhalte der einzelnen Kapitel vorgestellt und deren Relevanz für diese Arbeit, insbesondere die Verknüpfungen mit dem Algorithmus, erläutert.

Kapitel 2 enthält einige Grundlagen der Gruppentheorie. Es werden transitive Permutationsgruppen betrachtet, die als Galoisgruppen der zu untersuchenden Polynome auftreten. Von speziellem Interesse sind dabei die auflösbaren Gruppen.

Kapitel 3 beinhaltet Ergebnisse der Körper- und Galoistheorie. Es wird gezeigt, wie man ein primitives Element einer algebraischen Körpererweiterung finden kann. Weiter werden Eigenschaften der Zerfällungskörper von Polynomen betrachtet. Insbesondere sind solche Körper normal. Jede Galoisgruppe einer endlichen Körpererweiterung lässt sich als Permutationsgruppe auf den Nullstellen eines Polynoms darstellen. Es werden Kriterien für die Zugehörigkeit einer Permutation zur Galoisgruppe gegeben. Galoissche Körpererweiterungen werden auf ihre Struktur untersucht. Der Hauptsatz der Galoistheorie beschreibt eine Korrespondenz zwischen den Zwischenkörpern einer Erweiterung und den Untergruppen der zugehörigen Galoisgruppe.

In Kapitel 4 erfolgt eine eingehende Diskussion des Radikalbegriffs. Zunächst wird definiert, was ein Radikal ist. Radikalerweiterungen lassen sich auf eine Kette von zyklischen Körpererweiterungen zurückführen. Dazu wird die Lagrangesche Resolvente benötigt.

Dabei treten primitive Einheitswurzeln auf, weshalb auch Kreisteilungskörper betrachtet werden. Es wird auf Probleme bei der Deutung einer Radikaldarstellung eingegangen und der Begriff des irreduziblen Radikals eingeführt. Für Einheitswurzeln existieren Darstellungen durch irreduzible Radikale. Für einige kleine Primzahlen wird eine solche angegeben. Eine Radikaldarstellung existiert genau für die Nullstellen von Polynomen mit auflösbarer Galoisgruppe. Für Polynome der Grade 3 und 4 werden Auflösungsformeln angegeben.

Kapitel 5 präsentiert den Ablauf des Algorithmus zur algebraischen Nullstellenberechnung eines rationalen Polynoms im Detail.

In Kapitel 6 wird genauer auf die technischen Details der Implementation des Algorithmus mittels des Programmpakets GAP [32] eingegangen. Es werden die Schwachstellen der Implementation angesprochen und die Laufzeiten von Testläufen kommentiert.

Im Kapitel 7 werden die einzelnen Schritte des Algorithmus an drei ausführlichen Beispielen verdeutlicht.

1.4 Danksagungen

Ich danke meiner Betreuerin Prof. Dr. Bettina Eick. Sie machte mich durch den Hinweis auf [22] mit dem Thema bekannt und unterstützte mich bei meiner Arbeit in allen Belangen mit hilfreichen Kommentaren und großem Verständnis.

Desweiteren danke ich Prof. Dr. Alexander Hulpke für die aufschlussreiche Korrespondenz in der Anfangszeit. Er gab mir entscheidende Hinweise auf grundlegende Probleme sowie auf deren Lösungsmöglichkeiten.

Ich bedanke mich bei Dr Jürgen Klüners für zwei interessante Gespräche und die Übermittlung einer Vorabversion von [4].

Thomas Hennecke danke ich für das intensive Korrekturlesen einer früheren Version der Arbeit und Christian Sievers für seine unschätzbare Hilfe bei meinen zahllosen Computerproblemen.

Immer wieder eine Antwort auf meine Unsicherheiten beim Layout und auf Formulierungsprobleme fanden Björn Aßmann, Heiko Dietrich und Dörte Feichtenschlager, denen ich dafür herzlich Dank sage.

Kapitel 2

Gruppen

Von grundlegender Bedeutung für diese Arbeit sind die Theorien über Gruppen und Körper sowie deren Verknüpfung in der Galoistheorie. Für nachfolgende Kapitel relevantes Wissen aus dem ersten Bereich ist in diesem Kapitel zusammengestellt. Elementare Begriffe und Eigenschaften werden allerdings vorausgesetzt. Für weitere Informationen wird auf die Bücher von HUPPERT [19], ROBINSON [26] und VAN DER WAERDEN [34] verwiesen.

2.1 Transitive Permutationsgruppen

Um dem Leser die verwendete Notation nahe zu bringen, werden grundlegende Begriffe zu Permutationsgruppen definiert. Dies sind Gruppen, die aus bijektiven Abbildungen einer Menge auf sich selbst bestehen. Es bezeichne G in diesem Abschnitt eine endliche Permutationsgruppe.

2.1.1 Definition: Die Gruppe G operiere auf der Menge M. Sei $x \in M$.

1. Es wird $x^G = \{x^g \mid g \in G\}$, die Menge der Bilder von x unter der Operation von G, als *Bahn von x unter G* bezeichnet.
2. Der *Stabilisator von x in G* ist $\mathrm{Stab}_G(x) = \{g \in G \mid x^g = x\}$.

Aus der Definition ist ersichtlich, dass der Stabilisator stets eine Untergruppe von G ist.

2.1.2 Bemerkung: Für eine Teilmenge $X \subseteq M$ setzt man entsprechend obiger Definition $Stab_G(X) = \{g \in G \mid X^g = X\}$, wobei $X^g = \{x^g \mid x \in X\}$ die Menge aller Bilder von Elementen aus X unter der Wirkung von g ist.

2.1.3 Definition: Eine Gruppe G operiert *transitiv* auf einer Menge M, wenn die Bahn jedes Elements ganz M ist.

Es reicht sogar die Existenz eines Elementes mit ganz M als Bahn, damit die Operation transitiv ist. Anders ausgedrückt bedeutet Transitivität, dass zu je zwei Elementen $x, y \in M$ mindestens ein Gruppenelement g existiert, für das $x^g = y$ ist.

2.1.4 Lemma: *Sei U eine Untergruppe von G. Operiert U transitiv auf einer Menge M, so operiert auch G transitiv auf M.*

Beweis: Sei $x \in M$. Nach Voraussetzung ist $x^U = M$. Aus $U \leq G$ folgt $x^U \subseteq x^G$. Also ist $x^G = M$ und G daher transitiv. □

2.1.5 Lemma: *Die Gruppe G operiere auf der Menge M. Sei $x \in M$. Dann gilt $|x^G| = [G : Stab_G(x)]$ und $|x^G| \mid |G|$.*

Beweis: Man betrachte die Abbildung

$$\phi : \mathrm{Stab}_G(x)\backslash G \to x^G,\ \mathrm{Stab}_G(x)g \mapsto x^g.$$

Für $s \in \mathrm{Stab}_G(x)$ gilt $x^{sg} = (x^s)^g = x^g$. Daher ist ϕ wohldefiniert. Nun wird gezeigt, dass ϕ bijektiv ist. Da die Surjektivität offensichtlich ist, bleibt noch die Injektivität zu beweisen. Mit $x^g = x^h$ gilt auch $x^{gh^{-1}} = x$ und somit $gh^{-1} \in \mathrm{Stab}_G(x)$. Also folgt $\mathrm{Stab}_G(x)g = \mathrm{Stab}_G(x)h$ und damit die Injektivität. Aus der Bijektivität von ϕ ergibt sich sofort $|x^G| = [G : \mathrm{Stab}_G(x)]$ und daraus $|x^G| \mid |G|$. □

2.1.6 Beispiel: Zu den kleinsten Untergruppen der symmetrischen Gruppe S_n, die transitiv auf $\{1, \ldots, n\}$ operieren, gehört die zyklische Gruppe $\langle(1 \ldots n)\rangle$. Diese wie auch ihre Konjugierten haben n als Ordnung, was nach Lemma 2.1.5 minimal ist für eine Gruppe, die transitiv auf einer n-elementigen Menge operiert.

Es wird häufiger der Fall auftauchen, dass auf Elementen aus M durch Permutieren der Indizes operiert wird. Man kann die Operation dann ebenso gut als deren Wirkung auf $\{1, \ldots, n\}$ betrachten. Beispielsweise geht a_i^σ über in a_{i^σ}.

2.2 Auflösbare Gruppen

Eine zentrale Rolle in dieser Arbeit spielt die Eigenschaft einer Gruppe auflösbar zu sein. Dies ist eine Struktureigenschaft, die mit den auftretenden Normalteilern zusammenhängt.

Unter anderem wird eine Klassifizierung der auflösbaren, transitiven Permutationsgruppen angestrebt. Es wird auf der Menge $\{1, \ldots, n\}$ operiert, so dass die betrachteten Gruppen stets endlich sind.

Vorweg sei an ein zentrales Lemma der Gruppentheorie erinnert.

2.2.1 Lemma: *Sei $\varphi : G \to H$ ein Homomorphismus zwischen Gruppen. Dann ist $\theta : G/Kern(\varphi) \to Bild(\varphi),\ gKern(\varphi) \mapsto g^{\varphi}$ ein Isomorphismus.*

Beweis: siehe [26, 1.4.3] □

2.2.2 Definition: Eine Gruppe G heißt *einfach*, wenn sie außer sich selbst und der trivialen Gruppe keinen Normalteiler besitzt.

2.2.3 Beispiel:

- Jede Gruppe von Primzahlordnung ist einfach, da die einzige echte Untergruppe die triviale Gruppe ist.
- Die alternierende Gruppe A_n ist einfach für $n \geq 5$. Ein Beweis hierzu findet sich als §55 in [34].

Um beliebige Gruppen auf einfache zurückzuführen, werden ausgewählte Teile des Untergruppenverbandes betrachtet.

2.2.4 Definition: Es sei G eine endliche Gruppe.

1. Eine Reihe von Untergruppen,

$$G = G_0 \geq G_1 \geq \cdots \geq G_r = \{1\},$$

   heißt *Subnormalreihe*, wenn für $i = 1, \ldots, r$ stets G_i Normalteiler in G_{i-1} ist. Dabei wird r als *Länge* der Reihe bezeichnet. Es heißen G_{i-1}/G_i für $i = 1, \ldots, r$ die *Faktoren* der Reihe.

2. Zwei Subnormalreihen von G heißen *isomorph*, wenn alle Faktoren der einen Reihe in irgendeiner Reihenfolge den Faktoren der zweiten Reihe isomorph sind.

2.2.5 Beispiel: In einer zyklischen Gruppe $C_6 \cong \langle g \rangle$ der Ordnung 6 sind die beiden Subnormalreihen $\langle g \rangle > \langle g^2 \rangle > \{1\}$ und $\langle g \rangle > \langle g^3 \rangle > \{1\}$ isomorph, denn es ist jeweils ein Faktor isomorph zur C_2 und einer zur C_3. Um dies zu zeigen wende man Lemma 2.2.1 auf die beiden Endomorphismen $x \mapsto x^2$ und $x \mapsto x^3$ von $\langle g \rangle$ an.

Subnormalreihen lassen sich durch Einfügen weiterer Glieder verfeinern. Hierbei kann dieselbe Untergruppe durchaus wiederholt auftreten. Je feiner eine Subnormalreihe ist, desto mehr Rückschlüsse auf die Gruppenstruktur ermöglicht sie. Wiederholungen bringen natürlich keine neuen Informationen.

2.2.6 Definition: Sei G eine Gruppe. Eine Subnormalreihe $G = G_0 \rhd \cdots \rhd G_r = \{1\}$ von G, deren Faktoren sämtlich einfach sind, heißt *Kompositionsreihe*.

Eine Kompositionsreihe ist also eine Subnormalreihe ohne Wiederholungen, die sich ohne Wiederholungen nicht mehr verfeinern lässt.

2.2.7 Satz: *(Satz von* JORDAN *und* HÖLDER*)*
Je zwei Kompositionsreihen einer Gruppe G sind isomorph.

Beweis: siehe §51 in [34] □

Damit ist der Isomorphietyp einer Kompositionsreihe von G eine Invariante und eignet sich, ähnlich wie die Ordnung, um eine Klassifizierung endlicher Gruppen vorzunehmen. Betrachtet wird im Weiteren aber nur eine weniger detaillierte Unterteilung: Jede Gruppe ist entweder auflösbar oder nicht auflösbar im Sinne der folgenden Definition.

2.2.8 Definition: Eine endliche Gruppe G heißt *auflösbar*, falls eine Kompositionsreihe

$$G = G_0 \rhd G_1 \rhd \cdots \rhd G_r = \{1\},$$

existiert, deren Faktoren G_{i-1}/G_i für $i = 1, \ldots, r$ Primzahlordnung haben.

Es sind viele äquivalente Charakterisierungen der Auflösbarkeit bekannt. Dass die Kommutatorreihe bei der trivialen Gruppe ankommt und dass eine Normalreihe mit abelschen Faktoren existiert, sind zwei der gebräuchlichsten. Innerhalb dieser Arbeit findet jedoch nur Definition 2.2.8 Verwendung. Sie besagt noch nicht, dass man aus einer beliebigen Kompositionsreihe einer Gruppe auf deren Auflösbarkeit schließen kann. Da aber nur der Isomorphietyp der Kompositionsreihe in der Definition eine Rolle spielt, ergibt sich das nächste Lemma.

2.2.9 Lemma: *Sei G eine auflösbare Gruppe. Dann haben alle Faktoren einer beliebigen Kompositionsreihe von G Primzahlordnung.*

Beweis: Nach Voraussetzung besitzt G eine Kompositionsreihe, deren Faktoren sämtlich Primzahlordnung haben. Aus der Isomorphie zweier Kompositionsreihen derselben Gruppe (Satz 2.2.7) folgt die Behauptung. □

2.2.10 Beispiel:

- Jede Gruppe G, die selbst schon Primzahlordnung hat, ist auflösbar mit der Kompositionsreihe $G \rhd \{1\}$.
- Für die S_3 ist die Reihe $S_3 \rhd A_3 \rhd \{1\}$ eine Kompositionsreihe und für die S_4 die Reihe $S_4 \rhd A_4 \rhd V_4 \rhd \{(), (12)(34)\} \rhd \{1\}$.

Mit dem Beispiel als konstruktiven Beweis ergibt sich folgender Satz.

2.2.11 Satz: *Für $n \leq 4$ ist die symmetrische Gruppe S_n auflösbar.*

Es muss nicht jede Gruppe einzeln auf ihre Auflösbarkeit überprüft werden, wie man dem nächsten Lemma entnimmt:

2.2.12 Satz: *Sei G eine auflösbare Gruppe. Dann gelten:*

1. *Jede Untergruppe U von G ist selbst auflösbar.*
2. *Ist N ein Normalteiler von G, so ist die Faktorgruppe G/N auflösbar.*

Beweis: Gegeben sei eine Kompositionsreihe wie in Definition 2.2.8. Durch Schneiden jeder Gruppe der Reihe mit U entsteht

$$U = U_0 \trianglerighteq U_1 \trianglerighteq \cdots \trianglerighteq U_r = \{1\} \tag{2.1}$$

als Reihe von Untergruppen von U. Nun werden die Faktoren in (2.1) untersucht. Wendet man auf den Monomorphismus $\varphi : U_{i-1}/U_i \to G_{i-1}/G_i,\ xU_i \mapsto xG_i$ Lemma 2.2.1 an, ergibt sich, dass der Faktor U_{i-1}/U_i isomorph zu einer Untergruppe von G_{i-1}/G_i ist. Damit ist U_{i-1}/U_i trivial oder zyklisch von Primzahlordnung. Nach Entfernen der Wiederholungen aus (2.1) erhält man daher eine Kompositionsreihe von U, deren Faktoren sämtlich Primzahlordnung besitzen. Somit ist U auflösbar und der erste Teil der Behauptung bewiesen.

Ist N ein Normalteiler von G, kann die Reihe $G \trianglerighteq N \trianglerighteq \{1\}$ zu einer Kompositionsreihe $G = G_0 \triangleright G_1 \triangleright \cdots \triangleright G_r = \{1\}$ verfeinert werden. Es bezeichne k den Index mit $N = G_k$. Dann ist

$$G/N = G_0/N \triangleright G_1/N \triangleright \cdots \triangleright G_k/N = \{1\} \tag{2.2}$$

eine Kompositionsreihe von G/N. Denn für $g_iN \in G_i/N$ sowie $g_{i+1}N \in G_{i+1}/N$ ist $g_{i+1}N^{g_iN} = g_{i+1}^{g_i}N$ ein Element aus G_{i+1}/N. Weiterhin sind die Ordnungen der Faktorgruppen von (2.2) Primzahlen, da

$$|(G_i/N)/(G_{i+1}/N)| = \frac{|G_i/N|}{|G_{i+1}/N|} = \frac{|G_i|/|N|}{|G_{i+1}|/|N|} = \frac{|G_i|}{|G_{i+1}|} = |G_i/G_{i+1}|,$$

gilt. Damit ist die Auflösbarkeit von G/N gezeigt. □

Dieses Lemma erleichtert die Einteilung in auflösbare und nicht auflösbare Gruppen. So lässt sich Satz 2.2.11 um die beiden folgenden Aussagen erweitern.

2.2.13 Folgerung: *Für $n \leq 4$ besteht der Untergruppenverband der S_n aus auflösbaren Gruppen.*

2.2.14 Satz: *Für $n \geq 5$ ist die symmetrische Gruppe S_n nicht auflösbar.*

Beweis: Nach Beispiel 2.2.3 ist die A_n einfach für $n \geq 5$. Sie hat aber keine Primzahlordnung, weshalb sie nicht auflösbar ist. Mit der Kontraposition des ersten Teils von Satz 2.2.12 folgt die Behauptung. □

Eine weitere Möglichkeit eine Gruppe als auflösbar zu identifizieren, besteht, wenn eine stärkere Eigenschaft der Gruppe bereits bekannt ist. Am Rande erwähnt sei, dass jede nilpotente Gruppe auflösbar ist. Hier wird etwas weniger gezeigt und benutzt.

2.2.15 Lemma: *Jede abelsche Gruppe G ist auflösbar.*

Beweis: Es sei $G = G_0 \rhd G_1 \rhd \cdots \rhd G_s = \{1\}$ eine Kompositionsreihe von G. Dann sind die Faktoren G_i/G_{i+1} per Definition einfach. Außerdem sind sie abelsch, weil G nach Voraussetzung abelsch ist. Da jede Untergruppe einer abelschen Gruppe gleichzeitig ein Normalteiler ist, wird eine einfache, abelsche Gruppe von jedem nicht-trivialen Element erzeugt. Die Faktoren G_i/G_{i+1} sind daher zyklische Gruppen von Primzahlordnung. Somit ist G nach Definition 2.2.8 auflösbar. □

2.3 Primitive und imprimitive Gruppen

In diesem Abschnitt wird die Struktur von transitiven Permutationsgruppen genauer untersucht. Daraus gewonnene Erkenntnisse werden für auflösbare, transitive Untergruppen der S_n verwendet.

Es sei G stets eine Gruppe, die transitiv auf der Menge M operiere.

2.3.1 Definition: Sei $\emptyset \neq B \subseteq M$.

1. B heißt *Block* von G, falls $B \cap B^g = B$ oder $B \cap B^g = \emptyset$ für alle $g \in G$ gilt.
2. Einelementige Teilmengen von M sowie M selbst sind *triviale Blöcke* von G.
3. Ist B ein Block von G so wird die Menge $\{B^g \mid g \in G\}$ als *Blocksystem* bezeichnet.

2.3.2 Bemerkung: Jedes Blocksystem von G besteht aus Blöcken gleicher Mächtigkeit und bildet eine Partition von M.

Von den auftretenden Blocksystemen kann man auf Untergruppen von G schließen. So erhält man Informationen zur Struktur der Gruppe.

2.3.3 Satz: *Für jedes $x \in M$ existiert eine Bijektion zwischen den Blöcken von G, in denen x liegt, und der Menge der Untergruppen von G, die $Stab_G(x)$ enthalten. Dabei wird der Block B auf die Untergruppe $Stab_G(B)$ abgebildet und das Urbild der Untergruppe U ist der Block x^U.*

Beweis: Man betrachte die Abbildung

$$\begin{aligned} \phi : \{B \text{ ist Block von } G \mid x \in B\} &\to \{U \leq G \mid Stab_G(x) \leq U\}, \\ B &\mapsto Stab_G(B). \end{aligned}$$

Sei B ein Block mit $x \in B$. Für $g \in \mathrm{Stab}_G(x)$ folgt $B^g \cap B \neq \emptyset$, also $B^g = B$. Mithin gilt $g \in \mathrm{Stab}_G(B)$ und ϕ ist wohldefiniert. Nun wird gezeigt, dass ϕ bijektiv ist. Zunächst sei $B_1^\phi = B_2^\phi$. Für $g \in G$ ist dann $g \in \mathrm{Stab}_G(B_1) = \mathrm{Stab}_G(B_2)$ äquivalent zu $x^g \in B_1, B_2$. Da G transitiv operiert, muss schon $B_1 = B_2$ gelten. Sei nun U eine Untergruppe mit $\mathrm{Stab}_G(x) \leq U$. Dann bildet x^U einen Block von G, der unter ϕ zurück auf U abgebildet wird. Ist nämlich $x^U \cap (x^U)^g \neq \emptyset$ für ein $g \in G$, so folgt $x^{u_1} = (x^{u_2})^g$.

Also ist $u_2 g u_1^{-1} \in \mathrm{Stab}_G(x) \leq U$, was zu $g \in U$ führt und gleichsam $U = \mathrm{Stab}_G(x^U)$ zeigt. □

2.3.4 Definition:

1. Ist jeder Block von G trivial, so heißt G *primitiv*.
2. G heißt *imprimitiv*, wenn G nicht primitiv ist.

2.3.5 Folgerung: *Die Gruppe G ist genau dann primitiv, wenn der Stabilisator $Stab_G(x)$ für jedes $x \in M$ eine maximale Untergruppe von G ist.*

Beweis: Dies folgt aus Satz 2.3.3, nach dem zu jeder Gruppe zwischen $\mathrm{Stab}_G(x)$ und G ein nicht trivialer Block korrespondiert. □

2.3.6 Beispiel: Jede Gruppe G mit Primzahlgrad ist primitiv, da ein nicht-triviales Blocksystem nach Bemerkung 2.3.2 eine Faktorisierung des Grades bedeuten würde.

2.4 Zur Konstruktion maximal auflösbarer Untergruppen der symmetrischen Gruppe

Die transitiven Untergruppen der symmetrischen Gruppen sind bis zum Grad 31 von Hulpke [17] klassifiziert worden. Die Untergruppen werden dabei in Klassen von zueinander konjugierten Gruppen eingeteilt. Hier interessieren vor allem die auflösbaren, transitiven Untergruppen.

2.4.1 Bemerkung: Dass nach Lemma 2.2.15 die abelsche Gruppe $C_n \cong \langle (1 \ldots n) \rangle$ eine auflösbare Untergruppe der S_n ist, stellt für beliebigen Grad die Existenz auflösbarer, transitiver Gruppen sicher.

Zur Konstruktion der maximal auflösbaren Untergruppen der S_n werden primitive und imprimitive Gruppen getrennt betrachtet. Im Folgenden zunächst die primitiven.

2.4.2 Definition: Es sei $G = N \rtimes K$ mit $N \cong \mathbb{F}_p^d$ und $K = GL(d, p)$. Dann ist G die *affine Gruppe* von $\mathbb{F}_p^d$.

Die affine Gruppe operiert auf den p^d Elementen von F_p^d. Das erlaubt es von der affinen Gruppe als Untergruppe der S_{p^d} zu sprechen.

2.4.3 Satz: *Es sei $G \leq S_{p^d}$ eine auflösbare und primitive Gruppe. Dann ist G einer Untergruppe der affinen Gruppe vom Grad p^d ähnlich.*

Beweis: siehe [26, 7.2.7] □

Primitive Gruppen können also nur auflösbar sein, wenn ihr Grad eine Primzahlpotenz ist.

Für eine vollständige Betrachtung müssen als nächstes die imprimitiven Gruppen untersucht werden.

2.4.4 Definition: Seien N und H zwei Gruppen und $\alpha : H \to S_l$ für ein $l \in \mathbb{N}$. Dann ist

$$N \wr H = N^l \rtimes H = \{(n_1, \ldots, n_l; h) \mid n_1, \ldots, n_l \in N, h \in H\}$$

das *Kranzprodukt* von H mit N. Dabei ist die Multiplikation in $N \wr H$ definiert durch

$$(n_1, \ldots, n_l; h)(m_1, \ldots, m_l; g) = (n_1 m_{1^\pi}, \ldots, n_l m_{l^\pi}; hg) \text{ mit } \pi = (h^{-1})^\alpha.$$

2.4.5 Satz: *Es sei $G \leq S_n$ eine maximal imprimitive Gruppe mit dem Blocksystem $\mathfrak{B} = \{B_1, \ldots, B_m\}$ und $|B_1| = \cdots = |B_m| = d$. Dann ist G eindeutig bestimmt und isomorph zu $S_d \wr S_m$.*

Beweis: Auf jeder Menge B_i von $\mathfrak{B}$ operiert die symmetrische Gruppe S_d als Permutationsgruppe. Daher operiert $K = S_d(B_1) \times \cdots \times S_d(B_m)$ dergestalt auf $\{1, \ldots, n\}$, dass jedes B_i als Menge invariant ist. Sicherlich ist K die maximale Gruppe mit dieser Eigenschaft. Weiterhin kann G die Blöcke $B_1, \ldots, B_m$ permutieren. Wenn G mit dieser Eigenschaft wiederum maximal ist, dann operiert G als symmetrische Gruppe S_m auf $\mathfrak{B}$. Also ist G isomorph zum Kranzprodukt $S_d \wr S_m$. □

2.4.6 Satz: *Es sei $G \leq S_n$ eine maximal auflösbare und imprimitive Gruppe mit dem Blocksystem $\mathfrak{B} = \{B_1, \ldots, B_m\}$ und $|B_1| = \cdots = |B_m| = d$. Dann ist G isomorph zu $N \wr H$, wobei $N \leq S_d$ und $H \leq S_m$ sind, so dass N und H maximal auflösbar und transitiv sind.*

Beweis: Nach Satz 2.4.5 existiert eine eindeutig bestimmte maximal imprimitive Gruppe $G_{\max}$ zu dem Blocksystem $\mathfrak{B}$, die man mit $S_d^m \rtimes S_m$ identifizieren kann. Daher ist G eine Untergruppe von $G_{\max}$, und man kann die Projektionen $\phi : G \to S_d^m$ und $\psi : G \to S_m$ betrachten. Es sind $K = G^\phi$ und $H = G^\psi$ auflösbar nach Satz 2.2.12, und sicher ist $G \leq K \rtimes H$. Da $K \rtimes H$ wieder auflösbar und G maximal mit dieser Eigenschaft ist, gilt sogar die Gleichheit. Aus demselben Grund sind auch K und H maximal auflösbar in S_d^m beziehungsweise S_m.

Wegen der Gleichheit $G = K \rtimes H$ gilt insbesondere $K \leq G$. Daher sind in K genau die Elemente aus G, die nur innerhalb der einzelnen Blöcke von $\mathfrak{B}$ permutieren. Also lässt sich jedes Element $g \in K$ eindeutig als $g_1 \cdots g_m$ mit $g_i \in \mathrm{Sym}(B_i) \cong S_d$ schreiben. Somit ist $K \leq N_1 \times \cdots \times N_m$, wobei N_i das Bild der Einschränkung $K \to \mathrm{Sym}(B_i), g \mapsto g_{|B_i}$ ist. Die N_i und auch ihr Produkt sind auflösbar, so dass aus der Maximalität von K schon $K = N_1 \times \cdots \times N_m$ folgt.

Da G transitiv auf $\{1, \ldots, n\}$ operiert, gilt dies auch für die Operation auf $\mathfrak{B}$. Also ist H eine transitive Untergruppe der S_m. Man findet somit zu jedem Paar $i, j \in \{1, \ldots, m\}$ ein $h \in H$ mit $B_i^h = B_j$. Für dieses h folgt $N_i^h \leq N_j$ und ebenso $N_j \leq N_i^{h^{-1}}$. Daher sind

sämtliche $N_i, 1 \leq i \leq m$ in G äquivalent und man kann eine äquivalente Untergruppe $N \leq S_d$ wählen, so dass $K \cong N^m$ ist. Wie oben folgt aus der Maximalität von K, dass auch N maximal auflösbar sein muss.

Es bleibt die Transitivität von N zu zeigen. Da G transitiv ist, existiert zu $i, j \in B_1$ ein $g \in G$ mit $i^g = j$. Schreibt man g als kh mit $k \in K$ und $h \in H$, dann gilt schon $i^k = j$, weil H nur die Blöcke permutiert. Weiter folgt auch für die Einschränkung $k_1 = k_{|B_1}$, dass $i^{k_1} = j$ ist. Das zeigt, dass N_1 und somit N transitiv sind.

Da die gewählten Gruppen N und H die gewünschten Eigenschaften haben und insbesondere $G \cong N \wr H$ gilt, ist die Behauptung gezeigt. □

Die primitiven der maximal auflösbaren, transitiven Gruppen können nach einem Algorithmus von Eick und Höfling [12] berechnet werden. Wesentlich dafür ist Satz 2.4.3. Zusammen mit Satz 2.4.6 erhält man per Induktion über den Grad alle maximal auflösbaren der transitiven Gruppen.

Die folgenden beiden Beispiele sollen einen Eindruck vermitteln, wie sich die auflösbaren in alle transitiven Untergruppen einfügen.

2.4.7 Beispiel: (vgl. Abbildung 2.1)
Die symmetrische Gruppe vom Grad 5 hat 20 transitive Untergruppen, die sich auf 5 Konjugiertenklassen verteilen. Die Gruppen sind zum einen die symmetrische Gruppe $S_5 = \langle (12), (12345) \rangle$ selbst und die alternierende Gruppe $A_5 = \langle (123), (12345) \rangle$, und zum anderen die jeweils 6 Konjugierten der affinen Gruppe $F_{20} = \langle (12), (12345) \rangle \cong \mathrm{Aff}(\mathbb{F}_5)$, der Diedergruppe $D_{10} = \langle (12345), (14)(23) \rangle$ und der zyklischen Gruppe $C_5 = \langle (12345) \rangle$. Nach Beispiel 2.3.6 sind die Gruppen alle primitiv. Die maximal auflösbare ist die F_{20}.

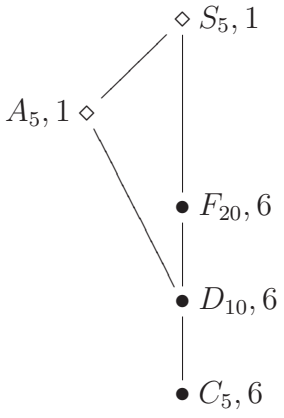

Abbildung 2.1: Transitive ($\diamond$: nicht auflösbare, $\bullet$: auflösbare) Untergruppen der S_5 bis auf Konjugation in S_5; nachgestellt die Mächtigkeit der Konjugiertenklasse

2.4.8 Beispiel: In Abbildung 2.2 ist der Verband transitiver Untergruppen der S_6 dargestellt. Die maximal auflösbaren bestimmt man mit Satz 2.4.6 zu $S_3 \wr C_2$ und $C_2 \wr S_3$.

Die S_6 ist außerdem die kleinste symmetrische Gruppe, in der zueinander isomorphe transitive Untergruppen nicht unbedingt konjugiert sind. Als Stabilisatoren eines Punktes können für zur S_4 isomorphe Gruppen sowohl C_4 wie auch $V_4 = C_2 \times C_2$ auftreten.

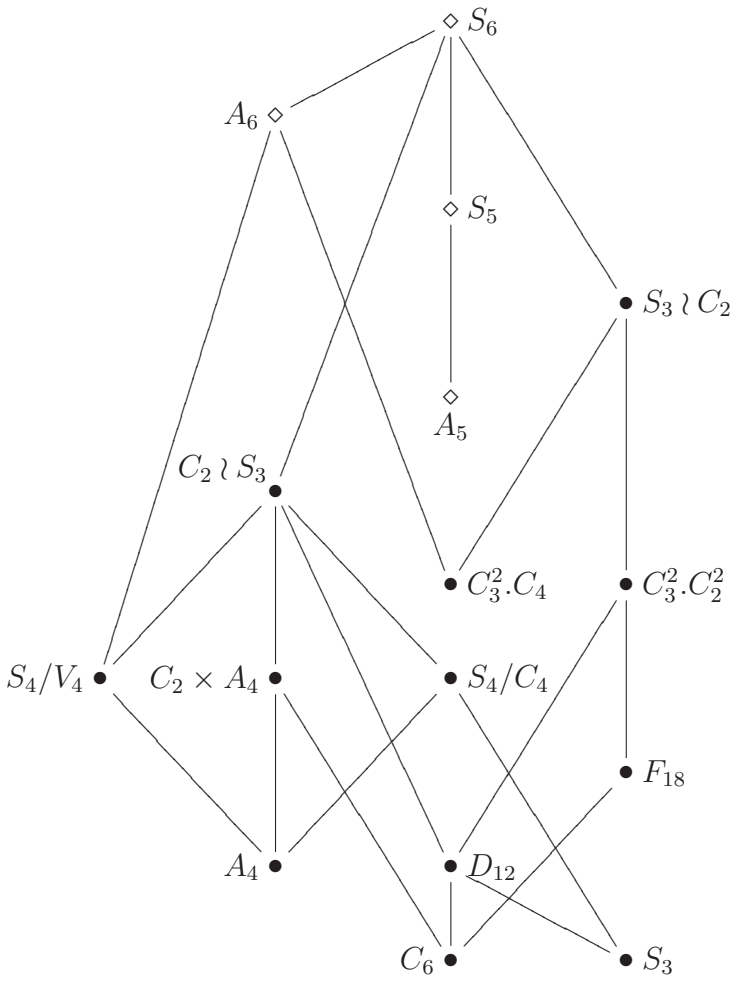

Abbildung 2.2: Transitive ($\diamond$: nicht auflösbare, $\bullet$: auflösbare) Untergruppen der S_6 bis auf Konjugation in S_6. – Der Graph entsteht aus dem Graphen des kompletten Untergruppenverbands, indem konjugierte Gruppen zu einem Knoten zusammengefasst und danach mehrfache Kanten identifiziert werden.

Eine Aufzählung auflösbarer, transitiver Gruppen von kleinem Grad, deren Ordnung für diese Arbeit noch von praktischem Nutzen ist, befindet sich im Abschnitt 6.2. Details zu den Gruppen geben Conway, Hulpke und McKay in [8] an.

Kapitel 3

Körper- und Galoistheorie

Die theoretische Grundlage dieser Arbeit wird von der Galoistheorie gestellt. Sie liefert eine Verbindung zwischen der Permutationsgruppe, die auf den Wurzeln eines Polynoms operiert, und dem Zerfällungskörper desselben. Permutationsgruppen wurden im vorigen Kapitel behandelt. Dieses Kapitel widmet sich in den ersten beiden Abschnitten der Körpertheorie. Es werden allgemeine Aspekte von Körpererweiterungen sowie speziell Zerfällungskörper von Polynomen betrachtet.
Im dritten Abschnitt wird die Galoisgruppe als Automorphismengruppe einer Körpererweiterung eingeführt und der Zusammenhang mit Permutationen der Nullstellen eines Polynoms erläutert. Es folgen im letzten Abschnitt des Kapitels der Hauptsatz der Galoistheorie, und darauf aufbauende Resultate.

Hauptsächlich besteht in dieser Arbeit Interesse an endlichen Körpererweiterungen von $\mathbb{Q}$, denen deshalb besondere Beachtung zu Teil wird.

Grundlegendes Vorwissen aus der Algebra findet man in den Büchern von Bosch [5] und van der Waerden [34].

3.1 Satz vom primitiven Element

In diesem Abschnitt werden einige Grundlagen der Körpertheorie präsentiert. Das Hauptaugenmerk richtet sich dabei auf endliche Körpererweiterungen von $\mathbb{Q}$, sogenannte algebraische Zahlkörper. Es stellt sich heraus, dass diese durch Adjunktion eines einzigen Elements zu erzeugen sind.

Soweit nicht bereits Standard, sind die verwendeten Bezeichnungen an das Buch von Bosch [5] angelehnt. Ist L eine Körpererweiterung von K, wird dies mit L/K notiert.

Entsteht L dabei durch die Adjunktion der Elemente $\alpha_1, \ldots, \alpha_n$, schreibt man $L = K(\alpha_1, \ldots, \alpha_n)$.

3.1.1 Definition: Es sei K ein Körper.

1. Sei L ein Erweiterungskörper von K. Ein Element $\alpha \in L$ heißt *algebraisch über* K, wenn α einer Gleichung $f(\alpha) = 0$ mit $0 \neq f \in K[x]$ genügt. Man nennt L *algebraisch über* K, wenn jedes Element aus L algebraisch über K ist.
2. K heißt *algebraisch abgeschlossen*, wenn jedes nicht-konstante Polynom $f \in K[x]$ eine Nullstelle in K besitzt.
3. Ist $\overline{K}$ ein algebraisch abgeschlossener Oberkörper von K, der algebraisch über K ist, nennt man $\overline{K}$ einen *algebraischen Abschluss* von K.

Wenn α algebraisch über K ist, bedeutet dies, dass der Körpergrad $[K(\alpha) : K]$ endlich ist. Somit ist jeder Erweiterungskörper, der durch Adjunktion algebraischer Elemente entsteht, algebraisch.

3.1.2 Satz: *Zu jedem Körper K existiert ein algebraischer Abschluss $\overline{K}$, der bis auf Isomorphie eindeutig ist.*

Beweis: siehe [5, 3.4] □

Damit gibt es zu K einen Körper, über dem jedes nicht-konstante Polynom $f \in K[x]$ in Linearfaktoren zerfällt. Das erlaubt es von den Nullstellen eines Polynoms zu sprechen und mit diesen zu arbeiten. Insbesondere entspricht die Anzahl der Nullstellen dem Grad des Polynoms, wenn man deren Vielfachheit beachtet.

3.1.3 Beispiel: Die Menge $\mathbb{A} = \{x \in \mathbb{C} \mid x \text{ ist algebraisch über } \mathbb{Q}\}$ ist ein algebraischer Abschluss von $\mathbb{Q}$.

3.1.4 Definition: Es sei L/K eine algebraische Körpererweiterung.

1. Man nennt ein Polynom $f \in K[x]$ *separabel*, wenn es nur einfache Nullstellen besitzt.
2. Ein Element $\alpha \in L$ heißt *separabel* über K, wenn das Minimalpolynom von α separabel ist.
3. Ist jedes Element aus L separabel über K, nennt man auch L *separabel* über K.

3.1.5 Satz: *Seien K ein Körper mit $Char(K) = 0$ und f ein irreduzibles Polynom aus $K[x]$. Dann ist f separabel.*

Beweis: siehe [5, 3.6, Satz 2] □

Somit sind auch alle Polynome, die über Körpererweiterungen von $\mathbb{Q}$ irreduzibel sind, separabel. Das führt zu der nächsten Aussage.

3.1.6 Folgerung: *Seien $K \subseteq L$ zwei algebraische Zahlkörper. Dann ist L/K eine separable Erweiterung.*

Beweis: Jedes Element aus L hat ein irreduzibles Minimalpolynom, das nach Satz 3.1.5 auch separabel ist. Damit ist L per Definition separabel über K. □

Auch wenn die Charakteristik des Körpers nicht Null ist, sind Erweiterungen, die durch Adjunktion separabler Elemente entstehen, separabel.

Nun werden spezielle Körpererweiterungen betrachtet.

3.1.7 Definition:

1. Entsteht ein Oberkörper durch die Adjunktion eines einzigen Elements, so spricht man von einer *einfachen* Körpererweiterung.
2. Sei L eine einfache Körpererweiterung von K. Dann heißt $\alpha \in L$ *primitives Element*, falls $L = K(\alpha)$ gilt.

Eine Besonderheit algebraischer Zahlkörper ist, dass sie sich stets durch Adjunktion eines Elements an $\mathbb{Q}$ erzeugen lassen. Bevor das gezeigt wird, soll an einige wohlbekannte Eigenschaften einfacher Erweiterungen erinnert werden.

3.1.8 Lemma: *Es sei K ein Körper und $\alpha \in \overline{K}$. Die einfache Erweiterung $K(\alpha)$ ist isomorph zu $K[x]/(f)$, wobei f das Minimalpolynom von α ist. Der Grad $[K(\alpha) : K]$ der Körpererweiterung ist gleich dem Grad von f.*

Beweis: siehe [34, §39] □

Über diese Isomorphie kann für einfache Erweiterungen eine definierende Gleichung sowie der Körpergrad bestimmt werden. Ein weiterer Vorteil der Kenntnis eines primitiven Elements, ist die Gestalt einer möglichen Basis, fasst man den Oberkörper als Vektorraum über dem Grundkörper auf.

3.1.9 Lemma: *Es sei $K(\alpha)$ eine Körpererweiterung wie in Lemma 3.1.8 vom Grad n. Dann bildet $1, \alpha, \ldots, \alpha^{n-1}$ eine K-Basis von $K(\alpha)$.*

Beweis: siehe [34, §40] □

3.1.10 Satz: *(Satz vom primitiven Element)*
Sei $L = K(\alpha_1, \ldots, \alpha_n)$ eine endliche Erweiterung von K mit $Char(K) = 0$. Dann ist L eine einfache Erweiterung.

Beweis: Der Beweis erfolgt per Induktion. Für $n = 1$ ist die Voraussetzung gleichzeitig die Behauptung. Sei also $L = K(\beta, \gamma)$. Weiter seien f das Minimalpolynom von β und g das von γ. Beide sind nach Satz 3.1.5 separabel. Es bezeichnen $\beta_1, \ldots, \beta_r$ die paarweise verschiedenen Nullstellen von f aus $\overline{L}$, sowie $\gamma_1, \ldots, \gamma_s$ diejenigen von g. Ohne Einschränkungen seien $\beta_1 = \beta$ und $\gamma_1 = \gamma$.

Für jedes i und jedes $k \neq 1$ hat die Gleichung

$$\beta_i + x\gamma_k = \beta + x\gamma$$

höchstens eine Lösung in K. Wählt man nun $c \in K$ verschieden von jeder der endlich vielen Lösungen dieser linearen Gleichungen und setzt $\vartheta = \beta + c\gamma$, so gilt für jedes i und jedes $k \neq 1$

$$\beta_i + x\gamma_k \neq \vartheta. \tag{3.1}$$

Es liegt ϑ in $K(\beta, \gamma)$, und man findet, dass ϑ sogar schon das gesuchte primitive Element ist:

Das Element γ ist Nullstelle der Polynome $g(x)$ und $f(\vartheta - cx)$, deren Koeffizienten aus $K(\vartheta)$ sind. Für jede weitere Nullstelle $\gamma_k, k \neq 1$, von g gilt nach (3.1) aber $\beta_i \neq \vartheta - c\gamma_k$, $(i = 1, \ldots, r)$, also $f(\vartheta - c\gamma_k) \neq 0$. Demnach haben $g(x)$ und $f(\vartheta - cx)$ nur den Linearfaktor $x - \gamma$ gemein. Die Koeffizienten dieses größten gemeinsamen Teilers müssen schon in $K(\vartheta)$ liegen; also ist $\gamma \in K(\vartheta)$. Aus $\beta = \vartheta - c\gamma$ folgt auch $\beta \in K(\vartheta)$, und somit $K(\beta, \gamma) = K(\vartheta)$.

Damit ist der Satz für $n = 2$ bewiesen. Ist er für $n - 1$ schon bewiesen, so hat man

$$K(\alpha_1, \ldots, \alpha_{n-1}) = K(\eta)$$

als Induktionsvoraussetzung und zeigt mit dem bereits bewiesenen Teil

$$K(\alpha_1, \ldots, \alpha_n) = K(\eta, \alpha_n) = K(\vartheta).$$

Mithin folgt die Aussage des Satzes für n. □

3.1.11 Bemerkung: Der Beweis zu Satz 3.1.10 zeigt eine Möglichkeit auf, für den Körper $L = K(\alpha_1, \ldots, \alpha_n)$ ein primitives Element der Form

$$\alpha_1 + c_2\alpha_2 + \cdots + c_n\alpha_n, \ c_i \in K$$

nach endlich vielen Schritten zu finden. Dies geschieht, indem man sukzessive die Erweiterungen $K(\alpha_1), \ldots, K(\alpha_1, \ldots, \alpha_n)$ als einfache Erweiterungen darstellt. In jedem Schritt liegen zwei Elemente vor, von denen fast alle K-Linearkombinationen ein primitives Element des nächsten Körpers ergeben.

3.2 Zerfällungskörper

Ist f ein irreduzibles Polynom aus $K[x]$, so sind einfache Erweiterungen, die durch Adjunktion einer Nullstelle von f entstehen, nach Lemma 3.1.8 isomorph zueinander. Es ist aber im Allgemeinen nicht möglich, eine Aussage darüber zu treffen, wie viele Nullstellen von f in $K[x]/(f)$ liegen. Dagegen werden in diesem Abschnitt Körper behandelt, die alle Nullstellen eines Polynoms enthalten.

3.2.1 Definition: Seien K ein Körper und f ein nicht konstantes Polynom aus $K[x]$. Dann heißt eine Körpererweiterung L *Zerfällungskörper* von f über K, wenn gilt:

(i) f zerfällt in L vollständig in Linearfaktoren.

(ii) L wird durch Adjunktion der Nullstellen von f an K erzeugt.

Diese Definition wirft die Fragen auf, wann ein Zerfällungskörper existiert und ob er gegebenenfalls eindeutig ist. Während die Existenz recht leicht zu zeigen ist, wird für die Eindeutigkeit noch die Fortsetzbarkeit eines Isomorphismus benötigt. Der wesentliche Satz für die Fortsetzung eines Isomorphismus zwischen algebraischen Erweiterungen lautet:

3.2.2 Satz: *Seien $K(\alpha)$ und $L(\beta)$ Körper und $\sigma : K \to L$ ein Isomorphismus. Weiter existiere das Minimalpolynom f aus $K[x]$ von α. Genau dann gibt es eine Fortsetzung von σ zu einem Isomorphismus $\tau : K(\alpha) \to L(\beta)$ mit $\alpha^\tau = \beta$, wenn $f^\sigma(\beta) = 0$ ist. In diesem Fall ist τ eindeutig bestimmt.*

Beweis: Gibt es eine Fortsetzung τ mit $\alpha^\tau = \beta$, so ist

$$0 = 0^\tau = f(\alpha)^\tau = f^\tau(\alpha^\tau) = f^\sigma(\beta).$$

Sei umgekehrt $f^\sigma(\beta) = 0$. Für ein Element $\sum_i k_i\alpha^i \in K(\alpha)$ wähle man als Bild unter τ das Element $\sum_i k_i^\sigma\beta^i \in K(\beta)$. Dann ist τ eine Fortsetzung von σ, für die $\alpha^\tau = \beta$ gilt. Offensichtlich ist τ in der Tat ein Isomorphismus und eindeutig bestimmt. □

3.2.3 Definition: Es sei K ein Körper. Zwei Elemente aus $\overline{K}$ heißen *konjugiert* bezüglich K, wenn sie Nullstellen desselben irreduziblen Polynoms aus $K[x]$ sind.

Ist $\sigma = id$ in Satz 3.2.2, erhält man die bereits aus Lemma 3.1.8 abgeleitete Aussage, dass zwei einfache Erweiterungen desselben Grundkörpers genau dann isomorph sind, wenn sie durch Adjunktion von zueinander konjugierten Elementen entstehen.

Die Fortsetzbarkeit wird nun auf Zerfällungskörper angewendet.

3.2.4 Satz: *Seien $\sigma : K \to L$ ein Isomorphismus zwischen Körpern und f ein Polynom aus $K[x]$, sowie $g = f^\sigma$ dessen Bild unter σ. Weiter seien K_f und L_g Zerfällungskörper von f über K sowie von g über L. Dann kann man σ zu einem Isomorphismus $\Theta : K_f \mapsto L_g$ fortsetzen.*

Beweis: Der Satz wird per Induktion nach $n = \text{Grad } f$ bewiesen. Sei dazu p ein irreduzibler Teiler von f über K. Es bezeichnen α eine Nullstelle von p in K_f und β eine Nullstelle von p^σ in L_g. Nach Satz 3.2.2 gibt es eine Fortsetzung $\tau : K(\alpha) \to L(\beta)$ von σ mit $\tau(\alpha) = \beta$. Dann sind

$$f = (x - \alpha)\sum_{i=0}^{n-1} c_i x^i \text{ in } K(\alpha)[x]$$

und

$$g = (x - \beta) \sum_{i=0}^{n-1} c_i^\tau x^i \text{ in } L(\beta)[x].$$

Setzt man $h = \sum_{i=0}^{n-1} c_i x^i$, so ist K_f Zerfällungskörper von h über $K(\alpha)$ sowie L_g Zerfällungskörper von h^τ über $L(\beta)$. Es ist Grad $h < n$, so dass sich τ per Induktion zu einem Isomorphismus $\Theta : K_f \to L_g$ fortsetzen lässt. □

3.2.5 Definition: Ein Homomorphismus, der einen Körper K elementweise festlässt, wird als *K-Homomorphismus* bezeichnet.

Damit lässt sich nun auch die Eindeutigkeit des Zerfällungskörpers zeigen.

3.2.6 Satz: *Sei f ein nicht konstantes Polynom aus $K[x]$. Dann existiert ein bis auf Isomorphie eindeutiger Zerfällungskörper von f über K.*

Beweis: Es seien $\alpha_1, \ldots, \alpha_n$ die Nullstellen von f aus einem algebraischen Abschluss $\overline{K}$ von K, der nach Satz 3.1.2 existiert. Dann ist $K(\alpha_1, \ldots, \alpha_n)$ Zerfällungskörper von f.

Setzt man in Satz 3.2.4 für σ die Identität auf K ein, folgt, dass je zwei Zerfällungskörper K-isomorph sind. □

3.2.7 Bemerkung: Aus dem Wissen dieses Satzes heraus ist im Weiteren von dem Zerfällungskörper von f die Rede, der die Bezeichnung K_f erhält.

Ist n der Grad des Polynoms f, gilt der leicht nachzurechnende Zusammenhang, dass $n!$ vom Grad der Erweiterung $[K_f : K]$ geteilt wird. Ist f irreduzibel, so teilt darüberhinaus n den Grad $[K_f : K]$. Allgemein lässt sich bemerken, welch starke strukturelle Eigenschaften daran geknüpft sind, dass ein Körper Zerfällungskörper ist. Dies deutet sich bereits im folgenden Satz an und spielt auch in späteren Abschnitten eine wichtige Rolle.

3.2.8 Definition: Eine Körpererweiterung L von K heißt *normal*, wenn jedes irreduzible Polynom aus $K[x]$, welches in L eine Nullstelle besitzt, über L vollständig in Linearfaktoren zerfällt.

3.2.9 Satz: *Es sei L eine Körpererweiterung von K. Dann sind äquivalent:*

1. *L/K ist normal.*
2. *L ist Zerfällungskörper eines Polynoms f aus $K[x]$.*
3. *Jeder K-Homomorphismus $L \to \overline{L}$ in einen algebraischen Abschluss $\overline{L}$ von L, beschränkt sich zu einem Automorphismus von L.*

Beweis: siehe [5, 3.5, Theorem 4] □

Über einer normalen Erweiterung L/K zerfällt das Minimalpolynom eines primitiven Elements vollständig. Wenn L/K zudem separabel ist, ergibt dies zusammen mit der

Bemerkung 3.1.11 eine Konstruktionsmöglichkeit für ein Polynom aus $K[x]$, dessen Zerfällungskörper gleich L ist. Das Polynom liefert dann zugleich die definierende Gleichung von L über K.

3.2.10 Folgerung: *Sei $f \in K[x]$. Für jeden Zwischenkörper $K \subseteq L \subseteq K_f$ ist die Erweiterung K_f/L normal.*

Beweis: Da $L_f = K_f$ gilt, ergibt sich die Aussage sofort aus Satz 3.2.9. □

Der Begriff der normalen Körpererweiterung verhält sich jedoch *nicht* transitiv. Aus M/L und L/K normal folgt nicht M/K normal, wie man an einem Gegenbeispiel sieht:

3.2.11 Beispiel: Die Kette $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt[4]{2})$ reeller Körper besteht aus zwei normalen Erweiterungen. Dagegen ist $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ nicht normal, da die komplexen Nullstellen des über $\mathbb{Q}$ irreduziblen Polynoms $x^4 - 2$ nicht in $\mathbb{Q}(\sqrt[4]{2})$ liegen.

3.2.12 Lemma: *Sind L/K und M/K zwei normale Körpererweiterungen, dann ist $L \cap M$ ebenfalls normal über K.*

Beweis: Sei $f \in K[x]$ irreduzibel mit einer Nullstelle in $L \cap M$. Also liegt diese Nullstelle sowohl in L wie auch in M. Aus deren Normalität folgt, dass alle Nullstellen von f in L und M und daher in $L \cap M$ liegen. Nach Definition 3.2.8 ist $L \cap M$ damit eine normale Körpererweiterung von K. □

Für Anwendungen ist es oft nützlich von einer Körpererweiterung, die nicht normal ist, zu einem normalen Oberkörper übergehen zu können.

3.2.13 Definition: Sei L/K eine Körpererweiterung. Ein Erweiterungskörper L' von L heißt *normale Hülle* zu L/K, wenn L'/K normal ist und kein echter Teilkörper von L' diese Bedingungen erfüllt.

Tatsächlich ist auch die Existenz einer normalen Hülle stets gewährleistet. Außer im wenig interessanten Fall $L' = L$ ist die Eindeutigkeit aber nur bis auf Isomorphie gegeben.

3.2.14 Satz: *Sei M/K eine normale Körpererweiterung. Zu jedem Zwischenkörper L existiert eine eindeutig bestimmte normale Hülle L' mit $L' \subseteq M$.*

Beweis: siehe [5, 3.5, Satz 7] □

Will man von einer einfachen Körpererweiterung L zu einem normalen Oberkörper übergehen, gibt es die Möglichkeit, den Zerfällungskörper eines Polynoms zu bilden, dessen eine Nullstelle das primitive Element ist. Benutzt man hierzu das Minimalpolynom, bekommt man eine normale Hülle von L.

3.3 Galoisgruppen

Die Idee der Galoistheorie ist es, die Struktur von Erweiterungen durch Betrachtung der Körperautomorphismen zu untersuchen. Ursprünglich lag das Interesse dabei auf den Zerfällungskörpern von Polynomen, wo man jeden Automorphismus eindeutig mit einer Permutation auf den Nullstellen des Polynoms identifizieren kann. Die Gruppe, die von solchen Permutationen gebildet wird, ist Gegenstand dieses Abschnitts.

3.3.1 Definition:

1. Eine Körpererweiterung L/K heißt *galoissch*, wenn L normal und separabel über K ist.
2. Sei L eine galoissche Körpererweiterung von K. Dann besteht die *Galoisgruppe* $\mathrm{Gal}(L/K)$ aus den K-Automorphismen von L.

Wie man sofort einsieht, bilden die Elemente der Galoisgruppe mit der Hintereinanderausführung als Verknüpfung in der Tat eine Gruppe. Strukturaussagen ermöglicht auch die Betrachtung von Automorphismengruppen beliebiger Körpererweiterungen. In ihrer Schärfe gelten die Sätze dieses Abschnitts aber nur für galoissche Erweiterungen.

Die Galoisgruppe eines Zerfällungskörpers K_f besitzt auch eine Darstellung als Permutationsgruppe auf den Nullstellen von f. Als solche wurde sie von Galois eingeführt. Um diese Eigenschaft einzusehen, hat man jeden Körperautomorphismus mit einer Permutation der Nullstellen zu identifizieren.

3.3.2 Satz: *Sei f ein separables Polynom aus $K[x]$ vom Grad $n > 0$. Bezeichnen $\alpha_1, \ldots, \alpha_n$ die Nullstellen von f in K_f, so definiert*

$$\begin{aligned} \varphi : Gal(K_f/K) &\to S(\{\alpha_1, \ldots, \alpha_n\}) \cong S_n, \\ \sigma &\mapsto \sigma_{|\{\alpha_1,\ldots,\alpha_n\}} \end{aligned} \tag{3.2}$$

einen injektiven Gruppenhomomorphismus der Galoisgruppe von K_f über K in die Gruppe der Permutationen von $\alpha_1, \ldots, \alpha_n$, bzw. in die symmetrische Gruppe auf n Elementen.

Beweis: Sei $\sigma \in \mathrm{Gal}(K_f/K)$. Da σ die Koeffizienten von f festlässt, gilt $f(\alpha_i)^\sigma = f(\alpha_i^\sigma)$. Also bildet σ jede Nullstelle von f wieder auf eine Nullstelle von f ab. Da weiter σ injektiv ist, ergibt die Einschränkung auf $\{\alpha_1, \ldots, \alpha_n\}$ eine bijektive Selbstabbildung, eine Permutation. Dies bedeutet, dass die Abbildung φ wohldefiniert ist. Im übrigen ist φ injektiv, denn ein K-Homomorphismus aus $\mathrm{Gal}(K_f/K)$ ist wegen $K_f = K(\alpha_1, \ldots, \alpha_n)$ bereits eindeutig durch seine Werte auf den Elementen $\alpha_1, \ldots, \alpha_n$ bestimmt. □

3.3.3 Bemerkung: Das Bild von $\mathrm{Gal}(K_f/K)$ unter φ aus Satz 3.3.2 wird von nun an mit G_f bezeichnet.

3.3.4 Folgerung: *G_f ist isomorph zu $Gal(K_f/K)$.*

Beweis: Man wende Lemma 2.2.1 auf den Monomorphismus φ aus Satz 3.3.2 an. □

Beim Verwenden der Darstellung G_f der Galoisgruppe als Permutationsgruppe wird von einer festgelegten Reihenfolge der Nullstellen ausgegangen. Ein Element der Galoisgruppe wirkt, indem es die Indizes der Nullstellen permutiert. Ist $\sigma \in G_f$, dann gilt $\alpha_i^\sigma = \alpha_{i^\sigma}$. Ändert man die Reihenfolge der Nullstellen, muss jedes $\sigma \in G_f$ durch eine Permutation mit der gleichen Wirkung auf die Nullstellen ersetzt werden.

3.3.5 Bemerkung: Seien f ein separables Polynom aus $K[x]$ und $\alpha_1, \cdots, \alpha_n$ dessen Nullstellen. Findet vermöge der Permutation τ eine Umnummerierung der Nullstellen statt, so geht G_f über in die konjugierte Gruppe G_f^τ.

3.3.6 Satz: *Die Voraussetzungen seien wie in Satz 3.3.2. Es ist f genau dann irreduzibel, wenn G_f transitiv auf der Menge der Nullstellen $\{\alpha_1, \ldots, \alpha_n\}$ operiert.*

Beweis: Ist f irreduzibel, dann existiert gemäß Satz 3.2.2 zu je zwei Nullstellen α_i und α_j ein K-Isomorphismus $\sigma : K(\alpha_i) \to K(\alpha_j)$ mit $\alpha_i^\sigma = \alpha_j$. Nun soll Satz 3.2.4 benutzt werden, um σ fortzusetzen. Es ist $f^\sigma = f$ sowie $K(\alpha_i)_f = K(\alpha_j)_f = K_f$. Somit ist die Fortsetzung $\tau : K(\alpha_i)_f \to K(\alpha_j)_f$ ein K-Automorphismus von K_f, der α_i in α_j überführt. Die Einschränkung auf $\{\alpha_1, \ldots, \alpha_n\}$ ergibt eine Permutation aus G_f. Da die Nullstellen α_i und α_j beliebig gewählt waren, folgt, dass G_f transitiv ist.

Sei andererseits f reduzibel. Dann existiert eine echte Zerlegung $f = gh$ in $K[x]$. Für jedes $\sigma \in G_f$ folgt wie im Beweis zu Satz 3.3.2, dass σ jede Nullstelle von g wieder auf eine Nullstelle von g abbildet. Nun ist f nach Voraussetzung separabel. Damit sind die Nullstellen von f paarweise verschieden, so dass G_f nicht transitiv operiert. □

Es bedeutet bei einer Reihe von Problemen keine Einschränkung, statt eines Polynoms dessen irreduzible Faktoren einzeln zu behandeln. Dass die Galoisgruppe dann transitiv operiert, macht diese Gruppen (siehe Abschnitt 2.1) zu einem wichtigen Spezialfall.

3.3.7 Folgerung: *Es sei K ein Körper. Zwei Elemente α und β aus $\overline{K}$ sind genau dann konjugiert, wenn sie sich durch einen K-Automorphismus ineinander überführen lassen.*

Beweis: Nach Definition 3.2.3 sind α und β genau dann konjugiert, wenn sie Nullstellen desselben irreduziblen Polynoms aus $K[x]$ sind. Damit folgt die Aussage direkt aus Satz 3.3.6. □

Interessiert man sich für die Galoisgruppe als Permutationsgruppe, möchte man nicht zunächst die Automorphismengruppe eines Zerfällungskörpers bestimmen, um dann die Einschränkungen der Automorphismen auf die Nullstellen zu betrachten. Statt dessen ist man an einem Kriterium interessiert, um jede Permutation auf Zugehörigkeit zu G_f prüfen zu können.

3.3.8 Lemma: *Sei f ein separables Polynom aus $K[x]$ vom Grad $n > 0$ mit den Nullstellen $\alpha_1, \ldots, \alpha_n$. Weiter sei $\sigma \in S(\{\alpha_1, \ldots, \alpha_n\}) \cong S_n$. Es ist σ genau dann aus G_f, wenn für jedes Polynom $\psi \in K[x_1, \ldots, x_n]$ mit $\psi(\alpha_1, \ldots, \alpha_n) = 0$ gilt:*

$$\psi(\alpha_1, \ldots, \alpha_n) = \psi(\alpha_{1^\sigma}, \ldots, \alpha_{n^\sigma}). \tag{3.3}$$

Beweis: Sei zunächst $\sigma \in G_f$. Nach Satz 3.3.2 existiert eine eindeutige Fortsetzung von σ zu einem K-Automorphismus ρ von K_f. Daher gilt:

$$\psi(\alpha_1, \ldots, \alpha_n) = (\psi(\alpha_1, \ldots, \alpha_n))^\rho = \psi(\alpha_1^\rho, \ldots, \alpha_n^\rho) = \psi(\alpha_{1^\sigma}, \ldots, \alpha_{n^\sigma})$$

Umgekehrt ist zu beweisen, dass die Fortsetzung zu einem K-Automorphismus gelingt. Da $K_f = K(\alpha_1, \ldots, \alpha_n)$ ist, gibt es nur eine mögliche homomorphe Fortsetzung. Ein beliebiges Element aus K_f ist von der Form $\psi(\alpha_1, \ldots, \alpha_n)$ und muss auf $\psi(\alpha_{1^\sigma}, \ldots, \alpha_{n^\sigma})$ abgebildet werden. Es bleibt zu zeigen, dass die entstehende Abbildung wohldefiniert ist. Seien ϕ und χ zwei Polynome in n Variablen mit $\phi(\alpha_1, \ldots, \alpha_n) = \chi(\alpha_1, \ldots, \alpha_n)$. Dann gilt für $\phi - \chi$ nach Gleichung (3.3)

$$0 = (\phi - \chi)(\alpha_1, \ldots, \alpha_n) = (\phi - \chi)(\alpha_{1^\sigma}, \ldots, \alpha_{n^\sigma}).$$

Es folgt $\phi(\alpha_{1^\sigma}, \ldots, \alpha_{n^\sigma}) = \chi(\alpha_{1^\sigma}, \ldots, \alpha_{n^\sigma})$, was zu zeigen war. □

Man kann auch sagen, dass eine Permutation der Wurzeln genau dann ein Automorphismus der Galoisgruppe ist, wenn alle polynomialen Ausdrücke in den Wurzeln, so sie im Grundkörper liegen, invariant sind unter Anwendung der Permutation.

Für eine algorithmische Überprüfung eignet sich das angegebene Kriterium allerdings nicht, da die Anzahl der zu prüfenden Ausdrücke nicht endlich ist. Anders ist dies im Falle einer einfachen Erweiterung.

3.3.9 Lemma: *Es seien $K(\alpha)$ eine endliche, galoissche Erweiterung des Körpers K und $\alpha = \alpha_1, \ldots, \alpha_n$ die Nullstellen des Minimalpolynoms f von α über K. Für $i = 1, \ldots, n$ sei dabei $\alpha_i = \psi_i(\alpha)$ mit $\psi_i \in K[x]$. Eine Permutation $\sigma \in S_n$ ist genau dann aus G_f, wenn gilt:*

$$\alpha_i^\sigma = \psi_i(\alpha^\sigma) \text{ für alle } i = 1, \ldots, n. \tag{3.4}$$

Beweis: Sei $\sigma \in G_f$. Es ist $K(\alpha) = K_f$. Somit lässt σ sich zu einem K-Automorphismus aus $\mathrm{Gal}(K(\alpha)/K)$ fortsetzen. Aufgrund der Homomorphie erfüllt σ daher die Gleichungen (3.4).

Sei umgekehrt $\sigma \in S_n$ mit $\alpha_i^\sigma = \psi_i(\alpha^\sigma)$ für alle $i \in \{1, \ldots, n\}$. Da G_f nach Satz 3.3.6 transitiv operiert, existiert zu σ eine Permutation $\tau \in G_f$ mit $\alpha^\tau = \alpha^\sigma$. Dann erfüllt τ nach dem bereits Bewiesenen die Gleichungen (3.4). Also ist $i^\sigma = i^\tau$ für alle $i \in \{1, \ldots, n\}$. Daraus folgt $\sigma = \tau \in G_f$. □

Dieses Lemma ermöglicht es, nach n Überprüfungen zu entscheiden, ob eine Permutation zu G_f gehört. Man kann sogar die Elemente von G_f unter Verwendung der Identitäten aus (3.4) direkt ermitteln, indem man sich die Bilder von α vorgibt.

3.4 Galoiskorrespondenz

Um Rückschlüsse von der Galoisgruppe auf die Körpererweiterung zu erhalten, wird der Hauptsatz der Galoistheorie benötigt. Dieser beschreibt die Korrespondenz zwischen Untergruppen und Zwischenkörpern.

Hierbei richtet sich das Interesse wieder auf algebraische Zahlkörper, und zwar speziell auf solche, die Zerfällungskörper eines Polynoms sind.

3.4.1 Lemma: *Ein algebraischer Zahlkörper ist genau dann galoissch über* $\mathbb{Q}$*, wenn er Zerfällungskörper eines Polynoms aus* $\mathbb{Q}[x]$ *ist.*

Beweis: Nach Korollar 3.1.6 ist jeder algebraische Zahlkörper separabel. Weiterhin ist ein Körper genau dann normal, wenn er Zerfällungskörper eines Polynoms ist (siehe Satz 3.2.9). Damit folgt die Aussage nach Definition. □

Ersetzt man in der Aussage „eines Polynoms“ durch „eines separablen Polynoms“, gilt das Lemma für beliebige endliche Erweiterungen.

Wenn man, wie hier, an endlichen Erweiterungen interessiert ist, bedeutet es daher keine Einschränkung die Galoistheorie für Zerfällungskörper separabler Polynome zu betrachten. Es bezeichne im Weiteren K einen Körper und f ein nicht-konstantes, separables Polynom aus $K[x]$, so dass K_f eine galoissche Erweiterung von K ist.

Eine erste Aussage über Zwischenkörper, die auch in den Hauptsatz eingeht, ergibt sich aus der Definition von galoissch.

3.4.2 Lemma: *Sei* L *ein Zwischenkörper der galoisschen Erweiterung* K_f/K*. Dann ist auch* K_f/L *galoissch und* $Gal(K_f/L) \leq Gal(K_f/K)$*.*

Beweis: Jedes über K separable Element ist auch über L separabel. Also ist K_f/L eine separable Erweiterung. Weiterhin ist K_f/L nach Korollar 3.2.10 normal und damit galoissch. Da jeder L-Automorphismus gleichzeitig ein K-Automorphismus ist, gilt $\mathrm{Gal}(K_f/L) \leq \mathrm{Gal}(K_f/K)$. □

Als nächster Schritt wird die Zugehörigkeit eines Elements zum Grundkörper über die Automorphismen der Galoisgruppe charakterisiert.

3.4.3 Lemma: *Ein Element* $\alpha \in K_f$ *ist genau dann aus* K*, wenn* α *von jedem Element der Galoisgruppe* $Gal(K_f/K)$ *auf sich abgebildet wird.*

Beweis: Für $\alpha \in K$ ist die Aussage trivial, da $\mathrm{Gal}(K_f/K)$ lauter K-Automorphismen enthält. Liegt α nicht in K, dann hat α ein nicht-lineares Minimalpolynom, das natürlich separabel ist. Somit existiert nach Satz 3.2.2 ein K-Isomorphismus auf $K(\alpha)$, der ungleich der Identität ist. Da f von diesem in sich selbst überführt wird, lässt er sich laut Satz 3.2.4 zu einem K-Automorphismus von K_f fortsetzen. Also existiert ein Element aus $\mathrm{Gal}(K_f/K)$, das α nicht festlässt. □

3.4.4 Definition: Für eine Untergruppe H von $\mathrm{Gal}(K_f/K)$ ist der *Fixkörper* von H, in Zeichen

$$\mathrm{Fix}_{K_f}(H) = \{x \in K_f | \forall \sigma \in \mathrm{Gal}(K_f/K) : x^\sigma = x\},$$

die Menge der Elemente aus K_f, die unter jedem K-Automorphismus aus H invariant bleiben.

3.4.5 Theorem: *(Hauptsatz der Galoistheorie)*

1. *Zu jedem Zwischenkörper L von K_f/K gehört eine Untergruppe H von $Gal(K_f/K)$, nämlich die Gesamtheit der L-Automorphismen von K_f.*
2. *Der Körper L wird von H eindeutig bestimmt. In L liegen die Elemente aus K_f, die unter H invariant bleiben.*
3. *Zu jeder Untergruppe H von $Gal(K_f/K)$ kann man einen Körper L finden, für den $H = Gal(K_f/L)$ ist.*
4. *Die Untergruppe H ist genau dann normal in $Gal(K_f/K)$, wenn L/K eine galoissche Erweiterung ist. Dann gilt $Gal(L/K) \cong G/H$.*
5. *Es gelten $|H| = [K_f : L]$ und $[Gal(K_f/K) : H] = [L : K]$.*

Beweis: Punkt 1 entspricht der Aussage von Lemma 3.4.2.

Da $H = \mathrm{Gal}(K_f/L)$ ist, folgt Punkt 2 aus Lemma 3.4.3, indem man L als Grundkörper betrachtet. Es ist somit $\mathrm{Fix}_{K_f}(\mathrm{Gal}(K_f/L)) = L$.

Sei nun $H = \{\sigma_1, \ldots, \sigma_h\}$ eine Untergruppe von $\mathrm{Gal}(K_f/K)$ und $L = \mathrm{Fix}_{K_f}(H)$. Offenbar ist L ein Zwischenkörper von K_f/K. Man betrachte für ein Element $\gamma \in K_f$ mit $K_f = L(\gamma)$, das nach Satz 3.1.10 existiert, das Polynom

$$j(x) = \prod_{i=1}^{h} x - \gamma^{\sigma_i}.$$

Die Koeffizienten von j sind bis auf das Vorzeichen die elementarsymmetrischen Funktionen in $\gamma^{\sigma_1}, \ldots, \gamma^{\sigma_h}$. Diese sind sicherlich in L enthalten, da die Anwendung eines Elementes aus H einer Permutation von $\gamma^{\sigma_1}, \ldots, \gamma^{\sigma_h}$ entspricht. Also wird j von dem Minimalpolynom m_γ von γ über L geteilt. Somit gilt $[K_f : L] = \mathrm{Grad}\ m_\gamma \leq h$. Klar ist weiter, dass H eine Untergruppe von $\mathrm{Gal}(K_f/L)$ ist, also $|H| \leq |\mathrm{Gal}(K_f/L)|$ gilt.

Zusammen hat man:

$$h = |H| \leq |\mathrm{Gal}(K_f/L)| = [K_f : L] \leq h.$$

Es folgt die Behauptung $H = \mathrm{Gal}(K_f/Fix_{K_f}(H))$.

Sei nun H eine Untergruppe von $\mathrm{Gal}(K_f/K)$, so dass $L = Fix_{K_f}(H)$ galoissch über K ist. Man betrachte

$$\varphi : \mathrm{Gal}(K_f/K) \to \mathrm{Gal}(L/K),\ \sigma \mapsto \sigma_{|L}.$$

Die Abbildung ist wohldefiniert, da L nach Voraussetzung normal ist. Denn dadurch liegen alle Konjugierten eines Elements aus L selbst wieder in L. Zudem ist φ surjektiv. Ist nämlich τ ein K-Isomorphismus $L \to L$, so kann man diesen nach Satz 3.2.4 fortsetzen zu einem K-Isomorphismus $L_f \to L_f$. Da $L_f = K_f$ ist, taucht somit τ im Bild von φ auf. Es besteht der Kern von φ aus allen K-Automorphismen von K_f, die L festlassen. Also ist $\mathrm{Kern}(\varphi) = \mathrm{Gal}(K_f/L) = H$. Als Kern eines Gruppenhomomorphismus ist H Normalteiler in G_f und nach Lemma 2.2.1 induziert φ dann einen Isomorphismus $\mathrm{Gal}(K_f/K)/H \to \mathrm{Gal}(L/K)$.

Sei umgekehrt H ein Normalteiler von $\mathrm{Gal}(K_f/K)$. Es wird gezeigt, dass zu jedem Element $\alpha \in L = \mathrm{Fix}_{K_f}(H)$ auch alle seine Konjugierten in L liegen. Diese sind nach Korollar 3.3.7 von der Form α^σ mit $\sigma \in \mathrm{Gal}(K_f/K)$. Für ein beliebiges $\tau \in H$ existiert aufgrund der Normalteilereigenschaft ein Element $\tau' \in H$, so dass $\tau \circ \sigma = \sigma \circ \tau'$ ist. Wegen $\alpha \in L$ gilt damit $(\alpha^\sigma)^\tau = (\alpha^{\tau'})^\sigma = \alpha^\sigma$. Also bleiben die Konjugierten von α invariant unter den Elementen aus H und liegen deshalb selbst in L. Dies zeigt, dass jedes irreduzible Polynom aus $K[x]$ mit einer Nullstelle in L dort ganz zerfällt. Somit ist L normal und als Zwischenkörper von K_f/K auch separabel über K. Damit ist Punkt 4 bewiesen.

Korrespondiert L zu der Untergruppe H, gilt $|H| = [K_f : L]$, wie man sofort am Beweis zu Punkt 3 sieht. Für den zweiten Teil von Punkt 5 wende man den Gradsatz für Körper auf $K \subseteq L \subseteq K_f$ an. Es ist

$$[L : K] = [K_f : K]/[K_f : L] = |\mathrm{Gal}(K_f/K)|/|H| = [\mathrm{Gal}(K_f/K) : H].$$

□

Die ersten drei Punkte des Theorems 3.4.5 drücken aus, dass die beiden Abbildungen

$$\begin{aligned} \{\text{Untergruppen von } \mathrm{Gal}(K_f/K)\} &\longleftrightarrow \{\text{Zwischenkörper von } K_f/K\}, \\ H &\longmapsto \mathrm{Fix}_{K_f}(H), \\ \mathrm{Gal}(K_f/L) &\longmapsfrom L \end{aligned}$$

zueinander inverse Bijektionen sind. Dies wird in Abbildung 3.1 veranschaulicht.

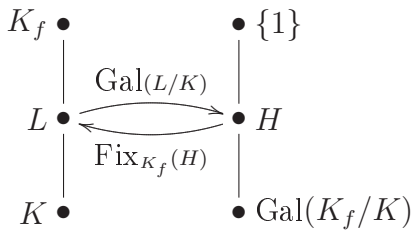

Abbildung 3.1: Die Bildung des Fixkörpers und der Galoisgruppe sind zueinander inverse Bijektionen zwischen der Menge der Untergruppen von $\mathrm{Gal}(K_f/Ks)$ und der Menge der Zwischenkörper von K_f.

3.4.6 Folgerung: *Seien $H_1 \leq H_2$ normale Untergruppen der Galoisgruppe mit den Fixkörpern $L_1 \supseteq L_2$. Dann sind deren Faktorgruppe H_2/H_1 und die zur Körpererweiterung L_1/L_2 gehörende Galoisgruppe isomorph.*

Beweis: Es ist K_f/L_2 eine galoissche Erweiterung mit der Galoisgruppe H_2, auf die sich Punkt 3 des Hauptsatzes 3.4.5 anwenden lässt. Dieser besagt, dass $\mathrm{Gal}(L_1/L_2) \cong H_2/H_1$ ist. □

Will man die Aussagen des Hauptsatzes 3.4.5 nutzen, braucht man eine konkrete Möglichkeit, die Bijektion zwischen den Untergruppen und den Zwischenkörpern auszuführen. Hat man einen Zwischenkörper L als einfache Erweiterung von K vorliegen, so reicht es alle Automorphismen aus $\mathrm{Gal}(K_f/K)$ zu bestimmen, die das primitive Element festlassen. Das umgekehrte Problem ist etwas schwieriger. Der nächste Satz zeigt, wie man zu einer Untergruppe von $\mathrm{Gal}(K_f/K)$ den Fixkörper bestimmt.

3.4.7 Satz: *Es sei $H = \{\sigma_1, \ldots, \sigma_h\}$ eine Untergruppe der Galoisgruppe $Gal(K_f/K)$. Bezeichnet γ ein primitives Element von K_f über K, dann wird der zu H gehörende Fixkörper $Fix_{K_f}(H)$ durch die elementarsymmetrischen Funktionen, ausgewertet bei $\gamma^{\sigma_1}, \ldots, \gamma^{\sigma_h}$, erzeugt.*

Beweis: Man betrachte wie beim Beweis zu Punkt 3 von Theorem 3.4.5 das Polynom

$$j(x) = \prod_{i=1}^{h} x - \gamma^{\sigma_i} \in \mathrm{Fix}_{K_f}(H)[x].$$

Die Koeffizienten von j sind bis aufs Vorzeichen die elementarsymmetrischen Funktionen in $\gamma^{\sigma_1}, \ldots, \gamma^{\sigma_h}$. Diese erzeugen einen Erweiterungskörper L von K. Zur Vervollständigung des Beweises genügt es $[\mathrm{Fix}_{K_f}(H) : L] = 1$ zu zeigen. Das Minimalpolynom von γ über L teilt j, dessen Grad h ist. Also ist $[K_f : L] \leq h$. Nach dem Hauptsatz der Galoistheorie ist $h = |H| = [K_f : \mathrm{Fix}_{K_f}(H)]$. Daraus erhält man mit dem Gradsatz für Körper

$$h \leq h\,[\mathrm{Fix}_{K_f}(H) : L] = [K_f : L] \leq h. \tag{3.5}$$

Somit ist $[K_f : L] = h$, was wieder in (3.5) eingesetzt die Behauptung liefert. □

3.4.8 Lemma: *Es sei $\alpha \in \overline{K}$. Dann ist Gal$(K_f(\alpha)/K(\alpha))$ isomorph zur Untergruppe Gal$(K_f/K(\alpha) \cap K_f)$ von Gal(K_f/K).*

Beweis: Offensichtlich ist

$$\begin{aligned} \psi : \mathrm{Gal}(K_f(\alpha)/K(\alpha)) &\to \mathrm{Gal}(K_f/K) \\ \sigma &\mapsto \sigma_{|K_f} \end{aligned}$$

ein wohldefinierter Homomorphismus. Es ist ψ sogar injektiv, da σ aus dem Kern von ψ ein $K(\alpha)$-Homomorphismus ist, für den zudem $\sigma_{|K_f} = id$ gilt. Somit ist σ die Identität auf $K_f(\alpha)$. Mit dem Homomorphiesatz für Gruppen 2.2.1 folgt

$$\mathrm{Bild}(\psi) \cong \mathrm{Gal}(K_f(\alpha)/K(\alpha))/\mathrm{Kern}(\psi) = \mathrm{Gal}(K_f(\alpha)/K(\alpha)).$$

Es bleibt zu zeigen, dass $\mathrm{Bild}(\psi) = \mathrm{Gal}(K_f/K(\alpha) \cap K_f)$ gilt. Die Inklusion „$\subseteq$“ ist offensichtlich. Umgekehrt kann man jedes Element $\tau \in \mathrm{Gal}(K_f/K(\alpha) \cap K_f)$ durch $\alpha^\tau = \alpha$ zu einem $K(\alpha)$-Automorphismus auf $K_f(\alpha)$ fortsetzen. Da dessen Bild unter ψ wieder τ ergibt, ist die Behauptung gezeigt. □

Die Aussage des Lemmas wird in Abbildung 3.2 verdeutlicht.

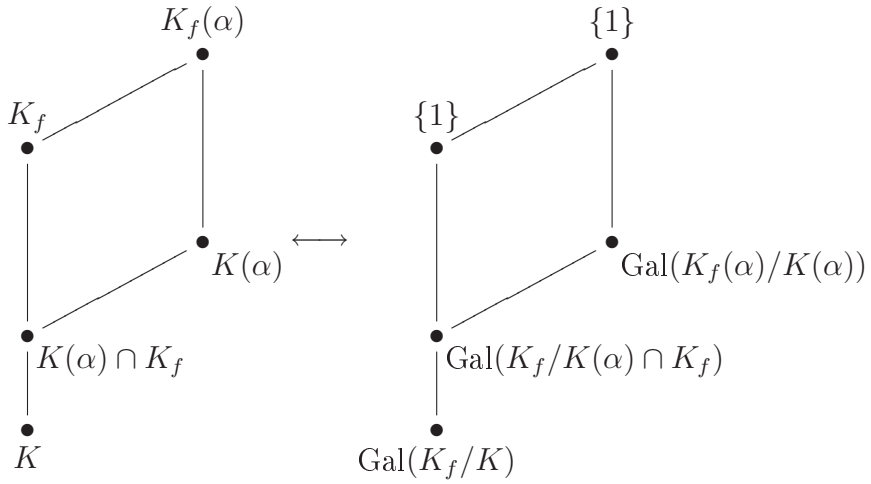

Abbildung 3.2: Bei Adjunktion eines algebraischen Elements α an die Körpererweiterung K_f/K erhält man als Galoisgruppe von $K_f(\alpha)/K(\alpha)$ eine Untergruppe von $\mathrm{Gal}(K_f/K)$

Kapitel 4

Radikale

In diesem Kapitel wird geklärt, welche Polynome Nullstellen besitzen, die sich durch die Grundrechenarten und Wurzelziehen aus den Koeffizienten ermitteln lassen. Darüberhinaus wird die Theorie erläutert, um Nullstellen solcher Polynome durch Wurzelausdrücke darzustellen.

Einleitend werden allgemeine Auflösungsformeln behandelt. Die beiden nachfolgenden Abschnitte widmen sich sogenannten reinen Gleichungen $x^n - c = 0$, deren Lösungen offensichtlich Wurzelausdrücke sind, und ihren Zerfällungskörpern. Darauf aufbauend werden beliebige Körper aus Elementen, die als Wurzelausdrücke darstellbar sind, betrachtet. Dazu erfolgt eine Diskussion des Radikalbegriffs und es wird erläutert, welche Anforderungen eine Radikaldarstellung sinnvollerweise erfüllen sollte.

4.1 Auflösungsformeln

Sei K ein Körper. Um die Nullstellen eines Polynoms aus $K[x]$ als Wurzelausdrücke darzustellen, war auch historisch der erste Ansatz, die allgemeine Gleichung vom Grad n, $x^n + t_{n-1}x^{n-1} + \cdots + t_1 x + t_0 = 0$ über dem Körper $K(t_0, \ldots, t_{n-1})$ algebraisch zu lösen. Dies gelang für $n \leq 4$, woraus sich die Auflösungsformeln für Polynome bis zum Grad 4 ergaben. Deren Angabe erfolgt hier für die Grade 3 und 4 ohne Herleitung. Eine solche findet man in [5, 6.2]. Die Formel für quadratische Polynome kann in der Einleitung nachgelesen werden.

4.1.1 Bemerkung: Durch Normieren ändern sich die Nullstellen eines Polynoms nicht. Ist $f(x) = x^n + \sum_{i=0}^{n-1} a_i x^i \in K[x]$ mit $\mathrm{Char}(K) \nmid n$, erhält man durch eine lineare Substitution das Polynom $g(x) = f(x - n^{-1}a_{n-1})$. Die Nullstellen von f und g unterscheiden sich somit nur um eine Konstante aus K, und der Koeffizient vor x^{n-1} von g ist Null.

Daher bedeutet die Form der Polynome in den beiden folgenden Sätzen keine Einschränkung der Allgemeingültigkeit, sondern trägt lediglich zur Vereinfachung der Formeln bei.

4.1.2 Satz: *(Cardanosche Formeln)*
Es sei K ein Körper mit $Char(K) \neq 2,3$. Für $p,q \in K$ werden die Lösungen der algebraischen Gleichung $x^3+px+q=0$ gegeben durch

$$x_1 = u+v, \qquad x_2 = \zeta^2 u + \zeta v, \qquad x_3 = \zeta u + \zeta^2 v.$$

Dabei ist ζ eine primitive dritte Einheitswurzel, sowie

$$u = \sqrt[3]{-\frac{q}{2} + \sqrt{\left(\frac{p}{3}\right)^3 + \left(\frac{q}{2}\right)^2}}, \; v = \sqrt[3]{-\frac{q}{2} - \sqrt{\left(\frac{p}{3}\right)^3 + \left(\frac{q}{2}\right)^2}},$$

wobei die dritten Wurzeln mit der Nebenbedingung $uv = -\frac{1}{3}p$ zu wählen sind.

Beweis: siehe [5, 6.2] □

4.1.3 Satz:
Es sei K ein Körper mit $Char(K) \neq 2,3$. Für $p,q,r \in K$ werden die Lösungen der algebraischen Gleichung $x^4+px^2+qx+r=0$ gegeben durch

$$\begin{aligned}
x_1 &= \frac{1}{2}(\;\sqrt{-z_1}+\sqrt{-z_2}+\sqrt{-z_3}),\\
x_2 &= \frac{1}{2}(\;\sqrt{-z_1}-\sqrt{-z_2}-\sqrt{-z_3}),\\
x_3 &= \frac{1}{2}(-\sqrt{-z_1}+\sqrt{-z_2}-\sqrt{-z_3}),\\
x_4 &= \frac{1}{2}(-\sqrt{-z_1}-\sqrt{-z_2}+\sqrt{-z_3}).
\end{aligned}$$

Dabei sind z_1, z_2, z_3 die Lösungen der kubischen Resolvente

$$z^3 - 2pz^2 + (p^2-4r)z + q^2 = 0,$$

und es sind die Quadratwurzeln mit der Nebenbedingung

$$\sqrt{-z_1}\sqrt{-z_2}\sqrt{-z_3} = -q$$

zu wählen.

Beweis: siehe [5, 6.2] □

Die Suche nach Auflösungsformeln für Polynome höherer Grade ist vergeblich, was Abel in seiner berühmten Arbeit [1] zeigen konnte.

Dennoch können die Nullstellen eines Polynoms höheren Grades sehr wohl als Wurzelausdrücke darstellbar sein, wie man z. B. an reinen Gleichungen $x^n - c = 0$ sieht.

4.2 Kreisteilungskörper

Schon in der Auflösungsformel für Polynome vom Grad 3 aus $\mathbb{Q}[x]$ kommt man selbst bei drei reellen Nullstellen nicht ohne komplexe Zahlen aus (siehe Satz 4.1.2). Es tritt immer eine primitive dritte Einheitswurzel auf. Es sollen daher Erweiterungskörper von $\mathbb{Q}$ untersucht werden, die durch Adjunktion von Einheitswurzeln entstehen. Für letztere wird folgende Definition verwendet.

4.2.1 Definition:

1. Ein Element $\zeta \in \overline{\mathbb{Q}}$ heißt *h-te Einheitswurzel*, falls es Nullstelle von $x^h - 1$ ist. Weiter ist $U_h = \{\zeta \in \overline{K} \mid \zeta^h - 1 = 0\}$.
2. Eine h-te Einheitswurzel ζ heißt *primitiv*, wenn $\zeta^i \neq 1$ ist für alle $0 < i < h$. Es ist $U_h^{\text{prim}} = \{\zeta \in U_h \mid \zeta \notin U_i \text{ für } 0 < i < h\}$.

Die h-ten Einheitswurzeln sind also gerade die h verschiedenen Nullstellen des Polynoms $x^h - 1$. Die Anzahl der primitiven Einheitswurzeln ist durch die Eulersche Funktion gegeben, an deren Definition hier erinnert werden soll.

4.2.2 Definition: Es bezeichne φ die *Eulersche Funktion*, deren Wert für $h \in \mathbb{N}$ durch $\varphi(h) = |\{1 \leq i \leq h \mid \text{ggT}(i,h) = 1\}|$ definiert ist.

4.2.3 Satz: *Es ist U_h eine zyklische Untergruppe von $\overline{K}^*$ mit $|U_h| = h$. Die Erzeuger von U_h sind gerade die primitiven h-ten Einheitswurzeln.*

Beweis: Es wird gezeigt, dass eine beliebige primitive h-te Einheitswurzel ζ die Gruppe U_h erzeugt. Für $1 \leq i \leq h$ ist ζ^i Nullstelle von $x^h - 1$. Seien $1 \leq i \leq j \leq h$ mit $\zeta^i = \zeta^j$. Dann ist $\zeta^{j-i} = 1$ und somit $i = j$, da ζ nach Voraussetzung primitiv ist. Also ist $\{\zeta^i \mid 1 \leq i \leq h\}$ die Menge der h Nullstellen von $x^h - 1$. Ist andererseits $\zeta \in U_h - U_h^{\text{prim}}$, so existiert ein $i < h$ mit $\zeta \in U_i^{\text{prim}}$. Das Erzeugnis von ζ besteht dann aus weniger als h Elementen und ist damit nicht U_h. □

Daraus kann man folgern, dass der Zerfällungskörper von $x^h - 1$ über $\mathbb{Q}$ durch die Adjunktion einer h-ten Einheitswurzel entsteht, falls sie primitiv ist.

4.2.4 Folgerung: *Für $\zeta \in U_h$ gilt $\mathbb{Q}(\zeta) = \mathbb{Q}_{x^h-1}$ genau dann, wenn ζ primitiv ist.*

Beweis: Es ist $\mathbb{Q}_{x^h-1} = \mathbb{Q}(U_h)$. Nach Satz 4.2.3 gilt $U_h = \langle\zeta\rangle$ genau für $\zeta \in U_h^{\text{prim}}$, was die Behauptung zeigt. □

Im Weiteren wird der Zerfällungskörper von $x^h - 1$ eingehender untersucht. Dabei soll zunächst das definierende Polynom bestimmt werden.

4.2.5 Definition:

1. Der Körper $\mathbb{Q}_{x^h-1}$ heißt *h-ter Kreisteilungskörper* und wird mit $\mathbb{Q}_h$ bezeichnet.

2. Das *h-te Kreisteilungspolynom* ist $\phi_h(x) = \prod_{\zeta \in U_h^{\text{prim}}} (x - \zeta)$.

Eine explizite Formel für die Kreisteilungspolynome existiert nicht. Anders liegt der Fall, wenn h eine Primzahl ist.

4.2.6 Lemma: *Für eine Primzahl $p \in \mathbb{N}$ ist $\phi_p(x) = \sum_{i=0}^{p-1} x^i$.*

Beweis: Es ist U_p nach Satz 4.2.3 eine zyklische Gruppe der Ordnung p. Also sind alle p-ten Einheitswurzeln ungleich 1 Erzeuger von U_p und somit primitiv. Daraus folgt $x^p - 1 = (x-1)\phi_p(x)$, womit die Behauptung durch Einsetzen zu verifizieren ist. □

4.2.7 Satz: *Es ist $\phi_h(x)$ ein irreduzibles Polynom aus $\mathbb{Z}[x]$.*

Beweis: Es sei ζ eine primitive h-te Einheitswurzel und f ihr Minimalpolynom. Dann ist f ein Teiler von $x^h - 1$, weshalb die Konjugierten von ζ aus U_h stammen. Insbesondere ist f als normierter Teiler eines normierten Polynoms aus $\mathbb{Z}[x]$ selber aus $\mathbb{Z}[x]$. Nach Folgerung 3.3.7 ist eine h-te Einheitswurzel ζ' genau dann zu ζ konjugiert, wenn sich ζ durch einen $\mathbb{Q}$-Automorphismus auf ζ' abbilden lässt. Nun ist $\mathbb{Q}(\zeta) = \mathbb{Q}_{x^h-1}$ nach Folgerung 4.2.4. Da ζ von einem $\mathbb{Q}$-Automorphismus wieder auf ein primitives Element von $\mathbb{Q}_{x^h-1}$ abgebildet wird, gilt mit derselben Folgerung $\zeta' \in U_h^{\text{prim}}$. Da $\zeta \in U_h^{\text{prim}}$ beliebig gewählt war, ist ϕ_h gerade das Produkt aller auftretenden Minimalpolynome von primitiven h-ten Einheitswurzeln. Daraus folgt $\phi_h(x) \in \mathbb{Z}[x]$.

Es bleibt zu zeigen, dass $f = \phi_h$ gilt, also jede primitive h-te Einheitswurzel Nullstelle von f ist. Für eine Primzahl p mit $p \nmid h$ ist ζ^p offensichtlich aus U_h^{prim}. Angenommen ζ^p sei keine Nullstelle von f, dann gilt bei der Zerlegung $x^h - 1 = f(x)g(x)$, dass ζ^p Nullstelle von g ist. Im Übrigen ist mit f auch g ein normiertes Polynom aus $\mathbb{Z}[x]$. Aus $g(\zeta^p) = 0$ folgt weiter $f(x) \mid g(x^p)$. Über $\mathbb{F}_p$ gelesen ergibt sich $\bar{f}(x) \mid \bar{g}(x^p) = \bar{g}(x)^p$. Damit haben f und g gemeinsame Nullstellen in $\overline{\mathbb{F}_p}$, was ein Widerspruch zur Separabilität von $x^h - 1$ ist. Also ist ζ^p Nullstelle von f.

Ist $\zeta' \in U_h^{\text{prim}}$ beliebig folgt aus Satz 4.2.3 unmittelbar die Existenz eines $k \in \mathbb{N}$ mit $\text{ggT}(k, i) = 1$ und $\zeta' = \zeta^k$. Ist $k = p_1 \dots p_l$ die Zerlegung von k in Primfaktoren, so folgt aus dem eben Gezeigten, dass ζ^{p_1} und damit induktiv auch $\zeta^{p_1 \cdots p_l} = \zeta'$ Nullstellen von f sind. Also ist $f = \phi_h$ und ϕ_h damit irreduzibel. □

4.2.8 Folgerung: *Es ist $\mathbb{Q}_h \cong \mathbb{Q}[x]/(\phi_h)$ und $[\mathbb{Q}_h : \mathbb{Q}] = \varphi(h)$.*

Beweis: Für eine primitive h-te Einheitswurzel ζ gilt $\mathbb{Q}_h = \mathbb{Q}(\zeta)$ nach Folgerung 4.2.4, und nach dem vorangehenden Satz ist ϕ_h das Minimalpolynom von ζ. Damit folgt die Behauptung aus Lemma 3.1.8. □

Bisher wurde der Kreisteilungskörper für ein festes h betrachtet. Nun sollen verschiedene Kreisteilungskörper zueinander in Beziehung gesetzt werden.

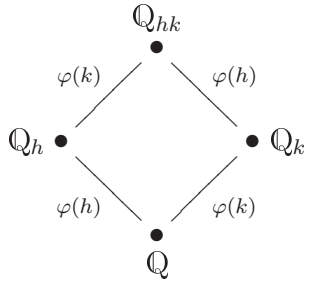

Abbildung 4.1: Schnitt und Erzeugnis der Kreisteilungskörper $\mathbb{Q}_h$ und $\mathbb{Q}_k$ für teilerfremde $h, k \in \mathbb{N}$.

4.2.9 Lemma: *Seien $h, k \in \mathbb{N}$ mit $ggT(h,k) = 1$. Dann gelten*

1. $\mathbb{Q}_h\mathbb{Q}_k = \mathbb{Q}_{hk}$,
2. $\mathbb{Q}_h \cap \mathbb{Q}_k = \mathbb{Q}$.

Beweis: Es seien ζ_h eine primitive h-te sowie ζ_k eine primitive k-te Einheitswurzel. Sicher gilt $\zeta_h, \zeta_k \in \mathbb{Q}_{hk}$, womit die Inklusion $\mathbb{Q}_h\mathbb{Q}_k \subseteq \mathbb{Q}_{hk}$ gezeigt ist. Weiter ist $\zeta_h\zeta_k$ eine (hk)-te Einheitswurzel, deren Ordnung in U_{hk} gerade $\mathrm{kgV}(h,k) = hk$ ist. Also ist $\zeta_h\zeta_k \in U_{hk}^{\mathrm{prim}}$ und damit $\mathbb{Q}_h\mathbb{Q}_k \supseteq \mathbb{Q}_{hk}$, was den Beweis zur ersten Aussage vervollständigt.

Wegen der Teilerfremdheit von h und k gilt für die Eulersche Funktion

$$\varphi(hk) = \varphi(h)\varphi(k). \tag{4.1}$$

Aus dem Gradsatz für Körper erhält man $[\mathbb{Q}_{hk} : \mathbb{Q}] = [\mathbb{Q}_{hk} : \mathbb{Q}_k][\mathbb{Q}_k : \mathbb{Q}]$ und zusammen mit Gleichung (4.1) folgt daraus $[\mathbb{Q}_{hk} : \mathbb{Q}_k] = \varphi(h)$ (vgl. Abbildung 4.1). Setzt man $L = \mathbb{Q}_h \cap \mathbb{Q}_k$, dann ist sicherlich $[\mathbb{Q}_{hk} : \mathbb{Q}_k] \leq [\mathbb{Q}_h : L]$, da beide Erweiterungen durch Adjunktion von ζ_h entstehen und $L \subseteq \mathbb{Q}_k$ gilt. Also ist $[\mathbb{Q}_h : L] = \varphi(h)$ und $L = \mathbb{Q}$. □

Zum Abschluss der Untersuchungen von Kreisteilungskörpern werden ihre Galoisgruppen betrachtet.

4.2.10 Satz: *Der Körper $\mathbb{Q}_h$ ist eine zyklische Galoiserweiterung über $\mathbb{Q}$, deren Galoisgruppe zur Einheitengruppe von $\mathbb{Z}/n\mathbb{Z}$ isomorph ist: $Gal(\mathbb{Q}_h/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^*$.*

Beweis: Nach Definition ist $\mathbb{Q}_h$ Zerfällungskörper über $\mathbb{Q}$ und daher wegen Lemma 3.4.1 galoissch. Ist ζ eine primitive h-te Einheitswurzel, entnimmt man dem Beweis von Satz 4.2.3, dass $U_h^{\mathrm{prim}} = \{\zeta^i \mid 1 \leq i \leq h, \mathrm{ggT}(i,h) = 1\}$ ist. Sei nun $\sigma \in \mathrm{Gal}(\mathbb{Q}_h/\mathbb{Q})$. Dann ist ζ^σ wieder Nullstelle von φ und damit aus U_h^{prim}. Mithin gilt ζ^σ für ein eindeutig bestimmtes $1 \leq i \leq h$ mit $\mathrm{ggT}(i,h) = 1$. Das definiert einen Monomorphismus

$$\psi : \mathrm{Gal}(\mathbb{Q}_h/\mathbb{Q}) \to (\mathbb{Z}/n\mathbb{Z})^*, \sigma \mapsto i + n\mathbb{Z},$$

der unabhängig von der Wahl von ζ ist, da $(\zeta^s)^\sigma = (\zeta^\sigma)^s = (\zeta^i)^s = (\zeta^s)^i$ gilt. Nach dem Homomorphiesatz für Gruppen 2.2.1 ist $\mathrm{Gal}(\mathbb{Q}_h/\mathbb{Q}) \cong \mathrm{Bild}(\psi)$. Da ψ surjektiv ist, wie die Gleichungskette $(\mathbb{Z}/n\mathbb{Z})^* = \varphi(h) = [\mathbb{Q}_h : \mathbb{Q}] = |\mathrm{Gal}(\mathbb{Q}_h/\mathbb{Q})|$ zeigt, folgt die Behauptung $\mathrm{Gal}(\mathbb{Q}_h/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^*$. □

4.3 Zyklische Körper

In diesem Abschnitt bezeichnen K und L endliche Erweiterungen von $\mathbb{Q}$.

Es werden Körpererweiterungen mit zyklischer Galoisgruppe und Zerfällungskörper von sogenannten reinen Gleichung $x^n - a = 0, (a \in K^*)$ betrachtet. Ziel ist es, die Körpererweiterungen zu charakterisieren, die ein primitives Element besitzen, das Wurzel einer reinen Gleichung ist, und für diese Erweiterungen eine entsprechende Darstellung zu finden.

4.3.1 Definition: Eine Körpererweiterung L/K heißt *zyklisch*, wenn ihre Galoisgruppe $\mathrm{Gal}(L/K)$ zyklisch ist.

4.3.2 Satz: *Sei K ein Körper, der die n-ten Einheitswurzeln enthält. Dann ist K_{x^n-a} mit $a \in K^*$ zyklisch.*

Beweis: Ist α eine Wurzel der Gleichung $x^n - a = 0$, so sind $\zeta\alpha, \zeta^2\alpha, \ldots, \zeta^{n-1}\alpha$ die übrigen, wobei ζ eine primitive n-te Einheitswurzel ist. Daher erzeugt α schon den Körper der Wurzeln, und jede Permutation der Galoisgruppe hat die Gestalt $\alpha \mapsto \zeta^i\alpha$. Die Zusammensetzung zweier Permutationen $\alpha \mapsto \zeta^i\alpha$ und $\alpha \mapsto \zeta^k\alpha$ ergibt $\alpha \mapsto \zeta^{i+k}\alpha$. Demnach entspricht jeder Permutation eine bestimmte Einheitswurzel ζ^i und dem Produkt der Permutationen das Produkt der Einheitswurzeln. Also ist die Galoisgruppe isomorph einer Untergruppe der Gruppe der n-ten Einheitswurzeln. Da U_n nach Satz 4.2.3 zyklisch ist, gilt dies auch für jede ihrer Untergruppen und die Galoisgruppe von $x^n - a$ ist ebenfalls zyklisch. □

Ist speziell das Polynom $x^n - a$ irreduzibel, so operiert die Galoisgruppe transitiv auf den Nullstellen und ist damit isomorph der vollen Gruppe der n-ten Einheitswurzeln. Ihre Ordnung ist in diesem Falle n. Eine schärfere Aussage ist für Primzahlen möglich.

4.3.3 Folgerung: *Sei K ein Körper, der die p-ten Einheitswurzeln (p prim) enthält. Dann zerfällt die reine Gleichung $x^p - a, a \in K^*$ entweder in Linearfaktoren oder ist irreduzibel.*

Beweis: Die Galoisgruppe der Gleichung ist entweder die zyklische Gruppe der Ordnung p, oder deren einzige echte Untergruppe, die triviale Gruppe. Im ersten Fall ist die Gruppe transitiv, daher die Gleichung nach Satz 3.3.6 irreduzibel. Im zweiten Fall gehören

die Wurzeln zum Fixkörper der Galoisgruppe; mithin liegen alle Nullstellen schon in K. □

Den Beweisen ist zu entnehmen, dass in $K(\sqrt[n]{a})$ bereits alle n-ten Wurzeln aus a liegen, solange $\mathbb{Q}_n \subseteq K$ gilt. Man kann sogar umgekehrt schließen: Wird für nur ein Polynom der Form $x^n - a$ der Zerfällungskörper K_{x^n-a} bereits durch die Adjunktion einer Wurzel erzeugt, so enthält K die n-ten Einheitswurzeln. Ansonsten ist $K(\sqrt[n]{a})$ nicht einmal galoissch.

Zum Beweis der Umkehrung von Satz 4.3.2, dass sich eine zyklische Erweiterung durch die Adjunktion der Wurzel einer reinen Gleichung erzeugen lässt, wird die Lagrangesche Resolvente benötigt.

4.3.4 Definition: Es L/K eine zyklische Erweiterung vom Grad n. Weiter bezeichnen ζ eine primitive n-te Einheitswurzel und σ ein erzeugendes Element von $\mathrm{Gal}(L/K)$. Dann wird die *Lagrangesche Resolvente* für jedes $\alpha \in L$ gebildet durch die Vorschrift

$$(\zeta, \alpha) = \alpha + \zeta\alpha^{\sigma} + \zeta^2\alpha^{\sigma^2} + \cdots + \zeta^{n-1}\alpha^{\sigma^{n-1}}. \tag{4.2}$$

Der Nutzen der Lagrangeschen Resolvente für diese Arbeit ergibt sich vor allem aus der Konstruktivität des anstehenden Beweises.

4.3.5 Satz: *Sei K ein Körper, der die n-ten Einheitswurzeln enthält, sowie L eine zyklische Erweiterung von K mit $[L : K] = n$. Dann lässt sich L durch die Adjunktion einer n-ten Wurzel erzeugen. Genauer existiert ein $\alpha \in L$ mit $(\zeta, \alpha) \neq 0$ und dafür ist $(\zeta, \alpha)^n \in K^*$ und (ζ, α) ein primitives Element von L.*

Beweis: Die Elemente der Galoisgruppe sind linear unabhängig über K (siehe [34, §54, Unabhängigkeitssatz]). Daher kann man α so wählen, dass $(\zeta, \alpha) \neq 0$ ist. Wendet man σ auf (ζ, α) an, so erhält man unter Verwendung von Gleichung (4.2):

$$\begin{aligned}(\zeta, \alpha)^{\sigma} &= \alpha^{\sigma} + \zeta\alpha^{\sigma^2} + \cdots + \zeta^{n-1}\alpha \\ &= \zeta^{-1}(\zeta\alpha^{\sigma} + \zeta^2\alpha^{\sigma^2} + \cdots + \alpha) \\ &= \zeta^{-1}(\zeta, \alpha).\end{aligned}$$

Bei Anwendung des Automorphismus σ bleibt die n-te Potenz $(\zeta, \alpha)^n$ somit unverändert, d. h. $(\zeta, \alpha)^n \in K^*$.

Durch mehrfaches Anwenden von σ auf Gleichung (4.2) erhält man $(\zeta, \alpha)^{\sigma^k} = \zeta^{-k}(\zeta, \alpha)$. Somit ist das einzige Element der Galoisgruppe, das die Resolvente (ζ, α) invariant lässt, die Identität. Also erzeugt (ζ, α) den ganzen Körper L.

Zusammengefasst ist (ζ, α) ein primitives Element aus L mit dem Minimalpolynom $x^n - (\zeta, \alpha)^n$. □

4.3.6 Bemerkung: Auf der Suche nach einem α, für das $(\zeta, \alpha) \neq 0$ gilt, reicht es offensichtlich eine Basis von L über K zu durchlaufen, da die Lagrangesche Resolvente linear ist.

Was ist zu tun, wenn K keine n-ten Einheitswurzeln enthält? Um mit den obigen Methoden arbeiten zu können, adjungiere man an K eine primitive n-te Einheitswurzel ζ_n . Für eine zyklische Galoiserweiterung L/K vom Grad n ist $L(\zeta_n)/K(\zeta_n)$ nach Lemma 3.4.8 wieder zyklisch (vgl. Abbildung 3.2). Der Grad der Erweiterung $L(\zeta_n)/K(\zeta_n)$ ist dann nicht mehr unbedingt n, aber ein Teiler von n. Die Voraussetzungen, um $L(\zeta_n)/K(\zeta_n)$ durch die Adjunktion der Wurzel einer reinen Gleichung zu erzeugen, sind daher erfüllt.

4.4 Irreduzible Radikale

Wurzeln sind aus der Schule wohlbekannt, und es bereitet sicherlich keine Probleme, die Ausdrücke aus Satz 4.1.2 für die Lösungen kubischer Gleichungen zu verstehen. Die Mehrdeutigkeit beim Wurzelziehen kann aber zu verschiedenen Interpretationen eines Wurzelausdrucks führen. In diesem Abschnitt wird die Darstellung mittels Wurzeln $(\sqrt{}, \sqrt[3]{}, \dots)$ näher beschrieben und eine Möglichkeit diskutiert, Missverständnisse bei der Interpretation zu vermeiden. Ausgangspunkt der Untersuchungen ist die Absicht, Nullstellen eines Polynoms nur durch rationale Operationen und Wurzelziehen aus den Koeffizienten zu ermitteln.

Wieder stehen K und L für endliche Erweiterungen von $\mathbb{Q}$.

Die erste wichtige Einsicht ist, zwischen dem Symbol $\sqrt[p]{a}$ und den Nullstellen von $x^p - a$ zu differenzieren. Dazu wird der Begriff des Radikals eingeführt.

4.4.1 Definition: Ein *Radikal* ist ein Ausdruck der Form $\sqrt[p]{a}$ für eine Wurzel der reinen Gleichung $x^p - a = 0, a \in K, p \geq 2$.

Die algebraische Operation ist also das Wurzelziehen und Radikale sind die Notation dazu. Anders gesagt ist $\sqrt[p]{a}$ die Anweisung, eine Nullstelle von $x^p - a$ zu wählen.

Lässt man neben dem Wurzelziehen auch andere algebraische Operationen $(+, -, \cdot, \div)$ zu, erhält man allgemeinere Ausdrücke als Radikale.

4.4.2 Definition: Eine Darstellung, die aus Elementen eines Körpers K und algebraischen Operationen besteht, wird *Radikalausdruck* oder *Darstellung durch Radikale* (bezüglich K) genannt.

Im konkreten Fall wird zumeist der Koeffizientenkörper eines Polynoms, insbesondere die rationalen Zahlen, Verwendung finden.

Es soll noch einmal auf die Form von Radikalen eingegangen werden. Das Körperelement a aus Definition 4.4.1 kann selbst als Radikalausdruck vorliegen. Anschaulich verbirgt sich hinter einem Radikal also ein Ausdruck der Gestalt

$$\sqrt[p_1]{\cdots \sqrt[p_2]{\cdots} + \sqrt[p_3]{\cdots} + \cdots + \cdots} \tag{4.3}$$

Mit den Elementen, die durch Radikale dargestellt werden, lässt sich exakt arbeiten, wenn man auf das Symbol $\sqrt{\ }$ zunächst verzichtet, und so auch dessen Mehrdeutigkeit meidet. Dazu werden Radikalausdrücke mit der Körpertheorie in Verbindung gebracht.

4.4.3 Definition: Eine Körpererweiterung L/K heißt *Radikalerweiterung*, falls

$$L = K(\beta_1, \ldots, \beta_r) \text{ mit } \beta_i^{p_i} \in K(\beta_1, \ldots, \beta_{i-1})$$

für geeignete $p_i \in \mathbb{N}, i = 1, \ldots, r$ ist.

4.4.4 Satz: *Für ein Element $\alpha \in \overline{K}$ lässt sich genau dann ein Radikalausdruck finden, wenn eine Radikalerweiterung L von K mit $\alpha \in L$ existiert.*

Beweis: Jedes Element einer Radikalerweiterung $L = K(\beta_1, \ldots, \beta_r)$ lässt sich offensichtlich durch einen Radikalausdruck darstellen, da die Adjunktion eines β_i dem Wurzelziehen aus einem bereits bekannten Element entspricht. Alle Elemente des Körpers $K(\beta_1, \ldots, \beta_i)$ erhält man dann durch Anwenden der Verknüpfungen $+$ und $\cdot$.

Liegt andererseits ein Radikalausdruck für ein Element $\alpha \in \overline{K}$ vor, so steht dieser für eine endliche Anzahl von Anweisungen, um α aus Elementen von K zu erhalten. Sei induktiv nach $k-1$ Schritten eine Radikalerweiterung M von K erreicht. Ist als k-te Anweisung eine rationale Operation durchzuführen, verbleibt man in M. Ist dagegen eine Wurzel zu ziehen, erhält man eine Radikalerweiterung L von M. Mit M/K und L/M ist auch L/K wieder eine Radikalerweiterung. □

Damit ist die Möglichkeit, algebraische Elemente durch Radikale darzustellen, auf die Struktur von Körpererweiterungen zurückgeführt.

Möchte man auf das Element zurückschließen, das durch Radikale dargestellt wurde, verbleibt eine Ungenauigkeit. Das Wurzelziehen ist in einem Körper im Allgemeinen eine mehrdeutige Zuordnung, und es fragt sich, welche Wurzel jeweils mit dem Radikal $\sqrt[p]{a}$ gemeint ist.

4.4.5 Beispiel: Wenn man eine primitive sechste Einheitswurzel durch Radikale ausdrückt, indem man sie einfach durch $\sqrt[6]{1}$ oder gar durch $\sqrt[12]{1}$ darstellt, wird man das als eine unbefriedigende Lösung anzusehen haben, während die Lösung $\zeta = \frac{1}{2} \pm \frac{1}{2}\sqrt{-3}$ viel befriedigender ist, weil der Ausdruck $\frac{1}{2} \pm \frac{1}{2}\sqrt{-3}$ bei jeder Wahl des Wertes von $\sqrt{-3}$ (d. h. einer Lösung der Gleichung $x^2 + 3 = 0$) die beiden primitiven sechsten Einheitswurzeln darstellt.

Ein Element durch einen Radikalausdruck eindeutig zu beschreiben, wird daher im Allgemeinen nicht möglich sein. Schon das einfache Radikal $\sqrt[p]{a}$ ist ja stets mehrdeutig.

Sucht man die Nullstellen einer Polynomgleichung, so ist die schärfste Forderung, die man in dieser Hinsicht stellen kann, dass man erstens *alle* Lösungen der fraglichen Gleichung durch Radikalausdrücke darstellen soll und zweitens diese Ausdrücke bei jeder Wahl der in ihnen vorkommenden Radikale Lösungen der Gleichung seien sollen. Dabei ist natürlich, wenn ein Radikal $\sqrt[p]{a}$ im Ausdruck mehrmals vorkommt, ihm stets derselbe Wert zu geben. Möchte man diese Bedingungen erfüllen, darf man keine beliebigen Radikalausdrücke mehr zulassen.

4.4.6 Definition:

1. Es sei $a \in K$ und $p \geq 2$. Dann heißt das Radikal $\sqrt[p]{a}$ *irreduzibel* (bezüglich K), wenn das Polynom $x^p - a \in K[x]$ irreduzibel ist.
2. Gegeben sei ein Radikalausdruck mit Elementen aus dem Körper K. Der Ausdruck wird als *irreduzibel* bezeichnet, wenn jede darin vorkommende Wurzel $\sqrt[p]{a}$ irreduzibel bezüglich $K(a)$ ist.

4.4.7 Bemerkung: Ein Schritt, der manche Überlegungen vereinfacht, ist, dass man die Wurzelexponenten vermöge

$$\sqrt[sr]{a} = \sqrt[s]{\sqrt[r]{a}}$$

stets zu Primzahlen machen kann. Dies soll im Folgenden jeder Wurzelexponent erfüllen.

4.4.8 Lemma: *Aus einem irreduziblen Radikalausdruck (bezüglich des Körpers K) erhält man bei jeder Wahl der Wurzelwerte eine Nullstelle desselben irreduziblen Polynoms (aus $K[x]$).*

Beweis: Es sei ρ ein irreduzibler Radikalausdruck. Es ist nun zu zeigen, dass man bei jeder Wahl der Wurzelwerte in ρ zueinander konjugierte Elemente erhält, welche sich nach Folgerung 3.3.7 gerade durch einen K-Isomorphismus ineinander überführen lassen.

Eine Wahl der Wurzelwerte in ρ führe zur Radikalerweiterung $L = K(\beta_1, \ldots, \beta_r)$ mit $\beta_i^{p_i} = a_i \in K(\beta_1, \ldots, \beta_{i-1})$, wobei $\sqrt[p_i]{a_i}$ genau die in ρ vorkommenden Wurzeln sind. Damit sind alle Elemente in L unter Verwendung der $\sqrt[p_i]{a_i}$ durch irreduzible Radikale darstellbar. Dass die Wahl der Wurzelwerte, der Anwendung eines K-Isomorphismus von L entspricht, wird per Induktion über die Anzahl der adjungierten Elemente bewiesen.

Für $r = 0$ ist $\rho \in K$ und es gibt nichts zu zeigen. Es führe nach Induktionsvoraussetzung jede Wahl der Werte von $\sqrt[p_1]{a_1}, \ldots, \sqrt[p_{r-1}]{a_{r-1}}$ zu einem K-Isomorphismus von $K(\beta_1, \ldots, \beta_{r-1})$. Geht dabei a_r über in $\tilde{a}_r$, so wird $\beta_r = \sqrt[p_r]{a_r}$ in $\sqrt[p_r]{\tilde{a}_r}$ überführt. Letzterer Ausdruck ist bei jeder Wahl Nullstelle von $x^{p_r} - \tilde{a}_r$ und erfüllt damit genau die Bedingung aus Satz 3.2.2, um eine Fortsetzung des Isomorphismus auf L zu liefern.

Es bleibt noch zu zeigen, dass auch die Wahl von $\sqrt[p_r]{a_r}$ der Anwendung eines K-Isomorphismus entspricht. Da $x^{p_r} - a_r$ nach Voraussetzung irreduzibel ist, sind alle Wahlen von $\sqrt[p_r]{a_r}$ konjugiert (auch bezüglich K). Also existiert ein K-Isomorphismus, der β_r in jede Wahl von $\sqrt[p_r]{a_r}$ überführt.

Insgesamt entspricht jede Wahl der Wurzelwerte einem K-Isomorphismus von L. Ein Radikalausdruck wie ρ ergibt daher bei jeder Wahl konjugierte Elemente, die nach Definition 3.2.3 Nullstellen desselben irreduziblen Polynoms aus $K[x]$ sind. □

Mit einem irreduziblen Radikalausdruck stellt man also sicher, bei jeder Auswertung eine Nullstelle des gleichen Polynoms zu erhalten. Genauer kann man mit der Darstellung durch Radikale nicht werden. Dennoch lässt sich die Aussage des Lemmas entscheidend erweitern.

4.4.9 Satz: *Gegeben seien ein irreduzibles Polynom $f \in K[x]$ sowie eine irreduzible Radikaldarstellung ρ einer Nullstelle. Dann bekommt man durch passende Wahl der Wurzelwerte in ρ jede Nullstelle von f.*

Beweis: Man erhält bei der Auswertung von ρ bei (mindestens) einer Wahl der Wurzeln in ρ eine Nullstelle $\gamma \in \overline{K}$ von f. Diese Wahl führe zu der Radikalerweiterung $L = K(\beta_1, \ldots, \beta_r)$ mit $\beta_i^{p_i} \in K(\beta_1, \ldots, \beta_{i-1})$. Jede Nullstelle von f geht aus γ unter einem K-Isomorphismus σ von L hervor. Per Induktion über r wird gezeigt, dass man zu jedem K-Isomorphismus σ eine Wahl der Wurzeln finden kann, die der Anwendung von σ entspricht.

Für $r = 0$ ist $\gamma \in K$ die einzige Nullstelle von f und es nichts zu zeigen. Nach Induktionsvoraussetzung ist jeder K-Isomorphismus von $K(\beta_1, \ldots, \beta_{r-1})$ durch Wahl der Wurzelwerte auszuführen. Für $\beta_r^{p_r} = a$ bleibt zu zeigen, dass man jedes Konjugierte von β_r durch Wahl der Wurzeln in $\sqrt[p_r]{a}$ erhalten kann. Dann gilt dies für alle Elemente aus L und insbesondere für die Darstellung ρ von γ. Es bezeichnen $a = a_1, \ldots, a_m$ die Konjugierten von a. Damit ist $[K(a) : K] = m$ und β_r hat $p_r m$ Konjugierte, da $x^{p_r} - a$ nach Definition 4.4.6 irreduzibel ist. Ist $g(x)$ das Minimalpolynom von a über K und $h(x)$ das von β_r, dann gilt $g(x^{p_r}) = h(x)$. Somit sind die Nullstellen der Polynome $x^{p_r} - a_i, 1 \leq i \leq m$ zu β_r konjugiert. Für $i \neq j$ ist $\sqrt[p_r]{a_i}$ sicher bei jeder Wahl von $\sqrt[p_r]{a_j}$ verschieden. Wählt man für ein festes $i \in \{1, \ldots, m\}$ einen Wert $\tilde{\beta}_r$ für $\sqrt[p_r]{a_i}$, sind die anderen möglichen Wahlen die $p_r - 1$ verschiedenen Werte $\zeta_{p_r}\tilde{\beta}_r$, wobei ζ_{p_r} alle primitiven p_r-ten Einheitswurzeln durchläuft. Da diese genau die p_r Lösungen von $x^{p_r} - a_i = 0$ sind, erhält man durch Wahl der Wurzelwerte also alle $p_r m$ Konjugierten von β_r. □

Ohne eine Wertezuweisung bestimmt eine irreduzible Radikaldarstellung ein Element also nur bis auf Konjugation, während durch geeignete Wahl der Werte jedes der konjugierten Elemente aus der Darstellung ermittelt werden kann. Das bedeutet insbesondere, dass durch Einsetzen aller möglichen Wahlen alle Konjugierten entstehen.

4.4.10 Bemerkung: Bei den Auflösungsformeln für Polynome der Grade 3 und 4 (siehe Sätze 4.1.2 und 4.1.3) ist das Problem mit mehrdeutigen Wurzeln anders gelöst. Dort werden Nebenbedingungen angegeben, die bei der Wahl gewisser Wurzelwerte zu beachten sind.

4.5 Auflösbare Polynome

4.5.1 Definition: Ein Polynom heißt *auflösbar*, falls alle seine Nullstellen mittels algebraischer Operationen aus den Koeffizienten zu ermitteln sind.

Es wird geklärt, von welchen Polynomen die Nullstellen durch irreduzible Radikale darstellbar sind. Bevor eine Antwort für jedes beliebige Polynom möglich ist, müssen die in Abschnitt 4.3 vorgestellten Kreisteilungspolynome untersucht werden. Können deren Nullstellen, die primitiven Einheitswurzeln, durch irreduzible Radikale dargestellt werden? Diese Frage ist mit einem Blick auf die Auflösungsformel für Polynome dritten Grades (siehe Satz 4.1.2) zu motivieren. Nur weil die auftretenden dritten Einheitswurzeln in der Form $-\frac{1}{2}\pm\frac{1}{2}\sqrt{-3}$ angegeben werden können, ist auch der komplette Ausdruck eine irreduzible Radikaldarstellung.

Die Untersuchung kann zudem durch zwei einfache Argumente auf Einheitswurzeln mit Primzahlordnung beschränkt werden. Es bezeichne ζ_i eine primitive i-te Einheitswurzel. Gilt $\mathrm{ggT}(r,s)=1$, so kann ζ_{rs} gleich $\zeta_r\zeta_s$ gewählt werden. Ist dagegen eine Primzahlpotenz $n=p^r$ gegeben, so gilt einfach $\zeta_n = \sqrt[p^{r-1}]{\zeta_p}$. Wie gefordert, ist dabei jede Lösung der Gleichung $x^{p^{r-1}}-\zeta_p=0$ eine primitive n-te Einheitswurzel.

4.5.2 Lemma: *Die p-ten Einheitswurzeln (p prim) sind durch irreduzible Radikale darstellbar.*

Beweis: Da die Behauptung für $p=2$ trivial ist (die zweiten Einheitswurzeln ±1 sind ja im Primkörper der Charakteristik Null enthalten), kann man sie induktiv für alle Primzahlen unterhalb p als bewiesen annehmen. Der Körper der p-ten Einheitswurzeln ist nach Satz 4.2.10 zyklisch und der Körpergrad $\varphi(p)=p-1$. Die Primfaktorzerlegung des Grades sei $q_1^{e_1}\ldots q_r^{e_r}$. Der Kreisteilungskörper kann also durch zyklische Erweiterungen von Primzahlgrad aufgebaut werden. Adjungiert man vorher die q_1-ten, …, q_r-ten Einheitswurzeln, die nach der Induktionsvoraussetzung ja durch Radikale darstellbar sind, so kann auf die zyklischen Erweiterungen der Grade q_i der Satz 4.3.5 angewendet werden. Dieser lehrt die Darstellbarkeit der sukzessiven Körpererweiterungen durch Radikale. Die betreffenden Gleichungen $x^{q_i}-a_i=0$ müssen dabei irreduzibel sein, da sonst die Körpergrade nicht gleich den q_i sein könnten. □

Der Beweis enthält prinzipiell dieselben Argumente wie sie für den zweiten Teil des

folgenden Theorems verwendet werden. Einzig die Existenz einer Radikaldarstellung für beliebige Einheitswurzeln wird dann als Voraussetzung benötigt. Für Primzahlen $p \leq 17$ wurden entsprechende Darstellungen mit dem GAP-Paket RADIROOT [10] erzeugt und in Details manuell angepasst. Die dafür zu lösende Gleichung ist nach Lemma 4.2.6 gerade $x^{p-1} + x^{p-2} + \cdots + x + 1 = 0$. In der Tabelle 4.1 werden die Ergebnisse präsentiert.

4.5.3 Theorem: *Sei f ein irreduzibles Polynom aus $K[x]$.*

1. *Wenn eine Nullstelle der Gleichung $f(x) = 0$ sich durch Radikale darstellen lässt, so ist die Galoisgruppe dieser Gleichung auflösbar.*
2. *Ist umgekehrt die Galoisgruppe der Gleichung auflösbar, so lassen sich alle Nullstellen von f durch irreduzible Radikale darstellen.*

Beweis: Zunächst sei für eine Nullstelle von f ein Ausdruck der Form (4.3) bekannt. Sodann adjungiere man an K alle p_1-ten, p_2-ten, $\ldots, p_r$-ten Einheitswurzeln, wobei $p_1, \ldots, p_r$ die als Wurzelexponenten in der Darstellung auftretenden Primzahlen sind. Dies ist eine Reihe zyklischer, normaler Körpererweiterungen, die man sich noch in Erweiterungen von Primzahlgrad zerlegt denken kann, wie im Beweis von Lemma 4.5.2. Sind diese Einheitswurzeln einmal vorhanden, so ist auch die Adjunktion von $\sqrt[p_i]{a_i}$ nach Folgerung 4.3.3 entweder überhaupt keine Erweiterung oder eine zyklische Erweiterung vom Grad p_i. Adjungiert man mit jedem $\sqrt[p_i]{a_i}$ auch die p_i-ten Wurzeln der zu a_i konjugierten Elemente, sind dies ebenfalls gar keine oder zyklische Erweiterungen von Primzahlgrad. Dadurch bleibt der Erweiterungskörper stets normal in Bezug auf K. So kommt man durch eine Reihe zyklischer Adjunktionen:

$$K = K_0 \subset K_1 \subset K_2 \subset \cdots \subset K_m = L, \tag{4.4}$$

zu einem normalen Körper L, der den Ausdruck (4.3), eine Nullstelle von f enthält. Da L/K eine normale Erweiterung ist, liegen alle Nullstellen von f in L und es gilt $K_f \subseteq L$.

Betrachtet man die Galoisgruppe von L/K dann entspricht der Körperkette (4.4) nach Theorem 3.4.5 eine Reihe von Untergruppen

$$\mathrm{Gal}(L/K) = G_0 > G_1 > \cdots > G_m = \{1\}, \tag{4.5}$$

für die $G_i = \mathrm{Gal}(L/K_i)$ ist. Da jede Körpererweiterung zyklisch war, ist jede Gruppe Normalteiler in der vorangehenden, und die Faktorgruppen sind zyklisch von Primzahlgrad. Das heißt, die Gruppe $\mathrm{Gal}(L/K)$ ist auflösbar und (4.5) eine Kompositionsreihe. Wieder nach dem Hauptsatz der Galoistheorie gilt für den normalen Zwischenkörper K_f, dass $\mathrm{Gal}(K_f/K)$ zur Faktorgruppe $\mathrm{Gal}(L/K)/\mathrm{Gal}(L/K_f)$ isomorph ist. Dass die Faktorgruppe nach Lemma 2.2.12 auflösbar ist, zeigt den ersten Teil der Behauptung.

Es sei nun $\mathrm{Gal}(K_f/K)$ auflösbar und

$$\mathrm{Gal}(L/K) = G_0 > G_1 > \cdots > G_m = \{1\}, \tag{4.6}$$

p	irreduzible Radikaldarstellung der primitiven p-ten Einheitswurzeln
2	-1
3	$\frac{1}{2}(-1+\sqrt{-3})$
5	$\frac{1}{4}(-1+\sqrt{5}+\sqrt{-10-\sqrt{5}})$
7	$\frac{1}{6}\left(-1+\sqrt[3]{\frac{7}{2}-\frac{21}{2}\sqrt{-3}}+(\frac{1}{14}+\frac{3}{14}\sqrt{-3})\sqrt[3]{\frac{7}{2}-\frac{21}{2}\sqrt{-3}}^2+3\sqrt{-\frac{7}{3}-(\frac{1}{6}-\frac{1}{6}\sqrt{-3})\sqrt[3]{\frac{7}{2}-\frac{21}{2}\sqrt{-3}}+(\frac{2}{21}+\frac{1}{21}\sqrt{-3})\sqrt[3]{\frac{7}{2}-\frac{21}{2}\sqrt{-3}}}\right)$
11	$\frac{1}{10}\Bigg(-1+\sqrt[5]{-\frac{1}{4}\left(979+275\sqrt{5}-(165-210\sqrt{5})\sqrt{-10-2\sqrt{5}}\right)}+\frac{1-5\sqrt{5}-\sqrt{5}\sqrt{-10-2\sqrt{5}}}{4}\sqrt[5]{-\frac{1}{4}\left(979+275\sqrt{5}-(165-210\sqrt{5})\sqrt{-10-2\sqrt{5}}\right)}^2$ $-\frac{50+2\sqrt{5}-(7-7\sqrt{5})\sqrt{-10-2\sqrt{5}}}{968}\sqrt[5]{-\frac{1}{4}\left(979+275\sqrt{5}-(165-210\sqrt{5})\sqrt{-10-2\sqrt{5}}\right)}^3$ $-\frac{89-25\sqrt{5}-(15+10\sqrt{5})\sqrt{-10-2\sqrt{5}}}{5324}\sqrt[5]{-\frac{1}{4}\left(979+275\sqrt{5}-(165-210\sqrt{5})\sqrt{-10-2\sqrt{5}}\right)}^4$ $+5\sqrt{-\frac{11}{5}-\frac{2+2\sqrt{5}-(1-\sqrt{5})\sqrt{-10-2\sqrt{5}}\ \omega_1}{40}-\frac{4-4\sqrt{5}+(1+\sqrt{5})\sqrt{-10-2\sqrt{5}}\ \omega_2^2}{220}-\frac{1+19\sqrt{5}-(4-\sqrt{5})\sqrt{-10-2\sqrt{5}}\ \omega_2^3}{2420}-\frac{118-2\sqrt{5}-(21-41\sqrt{5})\sqrt{-10-2\sqrt{5}}\ \omega_2^4}{53240}}\Bigg)$
13	$\frac{1}{12}\Bigg(-1+\sqrt{13}+2\sqrt[3]{13-(\frac{5}{2}+\frac{3}{2}\sqrt{-3})\sqrt{13}}+(\frac{1}{2}+\frac{1}{6}\sqrt{-3}-\frac{3}{78}\sqrt{13}+\frac{7}{78}\sqrt{-3}\sqrt{13})\sqrt[3]{13-(\frac{5}{2}+\frac{3}{2}\sqrt{-3})\sqrt{13}}^2$ $+\sqrt{-78-6\sqrt{13}+(3+\sqrt{-3}+3\sqrt{13}+\sqrt{-3}\sqrt{13})\sqrt[3]{13-(\frac{5}{2}+\frac{3}{2}\sqrt{-3})\sqrt{13}}+(2+2\sqrt{-3}+\frac{14}{13}\sqrt{13}+\frac{2}{13}\sqrt{-3}\sqrt{13})\sqrt[3]{13-(\frac{5}{2}+\frac{3}{2}\sqrt{-3})\sqrt{13}}^2}\Bigg)$
17	$\frac{1}{16}\Bigg(-1+\sqrt{17}+\sqrt{34-2\sqrt{17}}+\sqrt{68+12\sqrt{17}-(12+4\sqrt{17})\sqrt{34-2\sqrt{17}}}$ $+\sqrt{-136+8\sqrt{17}-16\sqrt{34-2\sqrt{17}}-(8-8\sqrt{17}-16\sqrt{34-2\sqrt{17}})\sqrt{68+12\sqrt{17}-(12+4\sqrt{17})\sqrt{34-2\sqrt{17}}}}\Bigg)$

Tabelle 4.1: Radikaldarstellung primitiver p-ter Einheitswurzeln für die Primzahlen p mit $p \leq 17$

eine Kompositionsreihe. Zu den Gruppen gehört eine Kette von Fixkörpern

$$K = K_0 \subset K_1 \subset \cdots \subset K_m = K_f,$$

in der jeder Körper normal und zyklisch in Bezug auf den vorangehenden ist. Sind $q_1, \ldots, q_l$ die in der Reihe vorkommenden Relativgrade, so werden zuerst die q_1-ten, $\ldots$, q_l-ten Einheitswurzeln adjungiert, was nach Lemma 4.5.2 durch irreduzible Radikale geschehen kann. Dann lassen sich nach Satz 4.3.5 die Erzeugenden von $K_1, \ldots, K_r$ durch Radikale ausdrücken, wobei die betreffenden Gleichungen $x^{q_i} - a_i = 0$ jedesmal entweder irreduzibel sind oder in Linearfaktoren zerfallen (siehe Folgerung 4.3.3). Im letzteren Fall ist die Adjunktion der entsprechenden Wurzel überflüssig. Damit ist auch der zweite Teil der Behauptung gezeigt. □

Insbesondere besagt das Theorem, dass eine Nullstelle, die sich durch Radikale darstellen lässt, sich auch durch irreduzible Radikale darstellen lässt. Letzteres ist also keine schärfere Forderung, sondern eine andere – in gewisser Weise genauere – Art, um die Nullstellen anzugeben.

Aus Theorem 4.5.3 kann leicht auf den Satz von Abel geschlossen werden, wobei die Reihenfolge chronologisch umgekehrt war.

4.5.4 Satz: *(Abel)*
Die allgemeine Gleichung n-ten Grades ist für $n > 4$ nicht durch Radikale lösbar.

Beweis: Die Galoisgruppe der allgemeinen Gleichung n-ten Grades ist isomorph zur S_n (siehe [34, §63]). Für $n \geq 5$ ist die symmetrische Gruppe nach Satz 2.2.14 aber nicht auflösbar, und die Nullstellen der allgemeinen Gleichung daher nicht durch Radikale auszudrücken. □

In dieser Arbeit wurde bisher noch nicht gezeigt, dass ein konkretes Polynom aus $\mathbb{Q}[x]$ existiert, dessen Nullstellen nicht durch Radikale darstellbar sind. Gesucht wird also ein Polynom mit einer nicht-auflösbaren Galoisgruppe. Für eine gegebene Permutationsgruppe G ein Polynom f zu finden, so dass G zu G_f konjugiert ist, wird als Umkehrproblem der Galoistheorie bezeichnet. Sucht man Polynome aus $\mathbb{Q}[x]$, ist zur Zeit keine Lösung des Problems für beliebige Gruppen bekannt. Dagegen kann man für die ganze symmetrische Gruppe zu jedem Grad ein entsprechendes Polynom ermitteln. Eine Formel dafür sowie Beispielpolynome für die transitiven Gruppen bis zum Grad 12 kann man im Buch von Malle und Matzat zum Umkehrproblem der Galoistheorie [23] nachschlagen. Für die auflösbaren Gruppen wurden die Polynome in den Abschnitt 6.2 übernommen.

Kapitel 5

Der Algorithmus

Aus den vorigen Kapiteln steht nun das theoretische Wissen zur Verfügung, um einen Algorithmus zu beschreiben, der eine irreduzible Radikaldarstellung für die Nullstellen eines gegebenen Polynoms zurückgibt, falls es auflösbar ist.

Beliebige Polynome können durch Faktorisieren in irreduzible zerlegt werden. Es genügt daher im Algorithmus irreduzible Polynome zu behandeln. Bei diesen besitzt nach Theorem 4.5.3 jede oder keine der Nullstellen eine Radikaldarstellung. Bei einem zusammengesetzten Polynom kann dagegen der Fall eintreten, dass für einige der Nullstellen eine Darstellung durch Wurzelausdrücke existiert und für andere nicht. Die irreduziblen Faktoren eines Polynoms getrennt zu behandeln, vereinfacht eine präzise und unmissverständliche Angabe der Ergebnisse somit deutlich.

Die einzelnen Schritte werden in einem Pseudocode angegeben, der sich an die Befehle des Computeralgebrapaketes GAP [32] anlehnt. Für die nicht explizit ausgeführten Berechnungen werden in der Implementation bereits in GAP vorhandene Funktionen verwendet. Darauf wird an den jeweiligen Stellen nochmals gesondert hingewiesen. Darüberhinaus befindet sich am Ende des Kapitels eine umfassende Liste der benutzten Notation.

5.1 Realisierung der Erweiterungskörper

Die benötigte Theorie über endliche Erweiterungen von $\mathbb{Q}$ wurde in Kapitel 3 abgehandelt. Für die Implementation muss man sich entscheiden, auf welche Weise Elemente aus dem algebraischen Abschluss von $\mathbb{Q}$ dargestellt werden sollen. Hier werden zwei Darstellungen eingesetzt. Zum einen wird eine Erweiterung als Matrixkörper realisiert

und zum anderen als Quotientenkörper des Polynomrings $\mathbb{Q}[x]$. Die beiden Fälle werden nacheinander betrachtet und anschließend zueinander in Beziehung gesetzt.

Es wird jeweils davon ausgegangen, dass ein primitives Element des Körpers bekannt ist. Dies kann für endliche Erweiterungen von $\mathbb{Q}$ nach Satz 3.1.10 und der anschließenden Bemerkung angenommen werden.

5.1.1 Matrixkörper

Es sei $K = \mathbb{Q}[M]$ ein Matrixkörper vom Grad n über $\mathbb{Q}$. Das ist genau dann der Fall, wenn M algebraisch über $\mathbb{Q}$ ist, also eine irreduzible Gleichung vom Grad n erfüllt. Mithin bildet $\mathbb{E}, M, \ldots, M^{n-1}$ eine $\mathbb{Q}$-Basis von K.

Eine rationale Matrix A ist genau dann aus K, wenn das lineare Gleichungssystem

$$q_0\mathbb{E} + q_1 M + \cdots + q_{n-1}M^{n-1} = A,\ q_i \in \mathbb{Q},$$

eine Lösung besitzt. Gerechnet wird in K wie im Matrizenring. Das Inverse von $A \neq 0$ kann durch Lösen des linearen Gleichungssystems $A \cdot A^{-1} = \mathbb{E}$ ermittelt werden.

5.1.1 Definition: Seien $A = (a_{ij}) \in \mathbb{Q}^{n\times n}$ und $B = (b_{ij}) \in \mathbb{Q}^{m\times m}$. Dann ist das *Kroneckerprodukt* $A \otimes B$ gegeben durch die $(nm) \times (nm)$-Matrix

$$\begin{pmatrix} a_{11}B & a_{12}B & \cdots & a_{1n}B \\ a_{21}B & a_{22}B & \cdots & a_{2n}B \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1}B & a_{n2}B & \cdots & a_{nn}B \end{pmatrix}.$$

Mit Hilfe des Kroneckerprodukts lässt sich ein Matrixkörper in einen Matrizenring höherer Dimension einbetten.

5.1.2 Lemma: *Seien K ein Matrixkörper und $\mathbb{E}$ eine Einheitsmatrix beliebiger Dimension. Dann ist $L = \{\mathbb{E} \otimes M \mid M \in K\}$ ein zu K isomorpher Körper.*

Beweis: Offensichtlich ist die Abbildung $K \to L, M \mapsto \mathbb{E} \otimes M$ ein Isomorphismus. □

5.1.2 Quotientenkörper von $\mathbb{Q}[x]$

Bezeichnet f_α das Minimalpolynom von $\alpha \in \overline{\mathbb{Q}}$, so ist $\mathbb{Q}(\alpha) \cong \mathbb{Q}[x]/(f_\alpha)$ nach Lemma 3.1.8. Eine $\mathbb{Q}$-Basis von $\mathbb{Q}[x]/(f_\alpha)$ ist durch $1, x, \ldots, x^{n-1}$ gegeben, wobei n dem Grad von f_α entspricht. Damit kann für jede Äquivalenzklasse ein eindeutig bestimmter Vertreter in der reduzierten Darstellung $\sum_{i=0}^{n-1} q_i x^i$ angegeben werden.

Für jede Nullstelle von f_α ist $K = \mathbb{Q}[x]/(f_\alpha)$ der gleiche Körper. Hat man ein weiteres Element $\beta \in \overline{\mathbb{Q}}$ und fragt sich, ob es in K liegt, ist diese Frage daher nur bis auf Konjugation zu beantworten. Dazu prüfe man, ob das Minimalpolynom von β über $\mathbb{Q}$ eine Nullstelle aus K besitzt, indem man es über K faktorisiert.

Addition, Subtraktion und Multiplikation in K funktionieren wie im Polynomring. Beachtet man bei der Multiplikation stets die Identität $f_\alpha \cong 0$, kann man die reduzierte Darstellung erreichen. Zum Ausführen der Division bestimmt man wie bei Matrizenkörpern das Inverse durch Lösen eines linearen Gleichungssystems. Dieses ergibt sich für $\sum_{i=0}^{n-1} q_i x^i \in K$ durch Koeffizientenvergleich vor den Potenzen von x in

$$\left(\sum_{i=0}^{n-1} q_i x^i\right)\left(\sum_{i=0}^{n-1} c_i x^i\right) = 1.$$

Für die linke Seite ist nach der Multiplikation die reduzierte Darstellung zu wählen, so dass die Eindeutigkeit der Koeffizienten vorausgesetzt werden kann.

5.1.3 Darstellungswechsel

Es sei eine einfache Körpererweiterung als Matrixkörper $H = \mathbb{Q}[M]$ gegeben und man bilde den isomorphen Körper $K = \mathbb{Q}[x]/(f)$, wobei f das Minimalpolynom von M ist. Um zwischen den beiden Realisierungen wechseln zu können, benutze man den kanonischen Isomorphismus. Dafür hat man in der Darstellung eines Elements als $\mathbb{Q}$-Linearkombination einfach M und x auszutauschen.

5.1.4 Faktorisieren

Als grundlegend für die anstehenden Berechnungen erweist es sich, Polynome über algebraischen Erweiterungen von $\mathbb{Q}$ faktorisieren zu können. Schon vor Beginn des Algorithmus ist es notwendig, um reduzible Polynome in ihre irreduziblen Faktoren zu zerlegen. Für die Koeffizienten des gegebenen Polynoms wird zum Faktorisieren die Darstellung als Elemente des Quotientenkörpers gewählt.

Es sei $g \in \mathbb{Q}(\alpha)[x]$ mit einem algebraischen Element α. Das Faktorisieren von g in $\mathbb{Q}(\alpha)[x]$ kann man nach den Ideen von Trager [33] auf eine Faktorisierung der Norm von g über $\mathbb{Q}$ zurückführen. Die Norm ist für Polynome analog zu der für algebraische Elemente definiert. Fasst man g als Polynom über $\mathbb{Q}$ in den beiden Variablen x und α auf, dann ist

$$\mathrm{Norm}(g) = \prod_{\alpha_i \text{ konjugiert zu } \alpha} g(x, \alpha_i).$$

Bezeichnet f das Minimalpolynom von α, dann gilt $\text{Norm}(g) = \text{Res}(f_\alpha(y), g(x,y))$, so dass man die Norm auch ohne Kenntnis der Konjugierten von α berechnen kann. Die einzelnen Faktoren von g sind die größten gemeinsamen Teiler von g und den Faktoren von $\text{Norm}(g)$. Dazu muss $\text{Norm}(g)$ allerdings quadratfrei sein, wofür gegebenenfalls durch eine lineare Substitution von x zu sorgen ist.

Das Faktorisieren der Norm von g über $\mathbb{Q}$ geschieht nach den neuen Methoden, die von Belabas, van Hoeij, Klüners und Steel in [4] präsentiert werden.

5.2 Galoisgruppe und Zerfällungskörper

In Weiteren ist f ein irreduzibles Polynom vom Grad n aus $\mathbb{Q}[x]$. Bezeichnet a_n den Leitkoeffizienten von f, hat $\frac{f}{a_n}$ dieselben Nullstellen wie f. Vermöge dieser Substitution, kann man sich bei den Betrachtungen auf normierte Polynome beschränken.

Das Vorgehen bei der Konstruktion des Zerfällungskörpers und der Galoisgrupppe ist den Anforderungen des Algorithmus in den darauf folgenden Schritten angepasst. Insbesondere wird der Zerfällungskörper als einfache Erweiterung benötigt. Eine alternative Methode stellen Anai, Noro und Yokoyama in [2] vor.

5.2.1 Prüfung der Auflösbarkeit von f

Im ersten Schritt soll untersucht werden, ob die Nullstellen von f eine Radikaldarstellung besitzen. Nach Theorem 4.5.3 ist dies genau dann der Fall, wenn die Galoisgruppe $\text{Gal}(\mathbb{Q}_f/\mathbb{Q})$ auflösbar ist. Man benötigt daher zumindest den Isomorphietyp von $\text{Gal}(\mathbb{Q}_f/\mathbb{Q})$. Dafür wird eine zu $\text{Gal}(\mathbb{Q}_f/\mathbb{Q})$ isomorphe Permutationsgruppe bestimmt. Die Berechnungen hierzu beruhen im Wesentlichen auf den Methoden von McKay und Soicher [24]. Einen Überblick zu verschiedenen Techniken der Galoisgruppenberechnung gibt Hulpke in [18]. Weitere Fortschritte erzielten Geissler und Klueners [14].

Nun wird die Auflösbarkeit der Galoisgruppe geprüft. Auch auf diesen Schritt wird hier nicht genauer eingegangen. Es findet die auf Sims [29] zurückgehende Methode für Permutationsgruppen Verwendung. Sollte die Galoisgruppe nicht auflösbar sein, bricht der Algorithmus an dieser Stelle ab.

5.2.2 Berechnung primitiver Elemente

Auftretende Körper sollen im Weiteren als einfache Erweiterungen von $\mathbb{Q}$ dargestellt werden. Deshalb wird in diesem Abschnitt gezeigt, wie man ein primitives Element von

$K = \mathbb{Q}(\alpha, \beta)$ bestimmen kann. Nach Bemerkung 3.1.11 existiert ein primitives Element der Form $\gamma = \alpha + c\beta$ mit $c \in \mathbb{N}$ von K. Die Suche danach kann mit folgender Funktion geschehen, wofür der Nachweis im Anschluss erbracht wird.

```
INPUT: Zwei über ℚ algebraische Elemente α und β
OUTPUT: Primitives Element von ℚ(α,β)

Primitives_Element(α, β)
  if α in ℚ(β)
    return β
  end if
  c := 0
  while β not in ℚ(α+cβ) do
    c := c+1
  end while
return α+cβ
```

5.2.1 Lemma: *Die Funktion* `Primitives_Element` *liefert ein primitives Element von* $\mathbb{Q}(\alpha, \beta)$. *Dies ist* β *im Falle* $\mathbb{Q}(\alpha, \beta) = \mathbb{Q}(\beta)$ *und ansonsten von der Form* $\alpha + c\beta$ *mit minimalem* $c \in \mathbb{N}_0$.

Beweis: Wie in den vorangehenden Erklärungen gesagt, ist die Existenz eines primitiven Elements der Form $\alpha + c\beta$ mit $c \in \mathbb{N}_0$ gesichert. Nun ist $\mathbb{Q}(\alpha, \beta) = \mathbb{Q}(\beta)$ genau dann, wenn $\alpha \in \mathbb{Q}(\beta)$ gilt, und in diesem Fall gibt die Funktion wie behauptet β zurück. Andernfalls liegt mit β auch α in $\mathbb{Q}(\alpha+c\beta)$, so dass die Funktion in der Tat ein primitives Element liefert. Gilt $\beta \notin \mathbb{Q}(\alpha+c\beta)$, dann ist $\alpha+c\beta$ offensichtlich kein primitives Element, womit gezeigt ist, dass die Funktion bei minimalem c terminiert. □

Die Funktion `Primitives_Element` kann für algebraische Elemente in beliebiger Darstellung angewendet werden, solange man in der Lage ist, die Zugehörigkeit eines Elementes zu einem Körper zu überprüfen. In dieser Arbeit soll sie für Matrixkörper benutzt werden. Wie die Überprüfung dort geschieht, wurde im Abschnitt 5.1.1 geklärt.
Notwendig ist natürlich, dass die Matrizen α und β demselben Körper angehören. Dazu genügt es im Übrigen nicht, dass sie dieselbe Dimension haben. Da im Allgemeinen mehr als $\mathrm{Grad}(f)$ Matrizen ebendieser Dimension existieren, die Nullstellen des irreduziblen Polynoms f sind, können nicht alle im gleichen Körper liegen.

5.2.3 Konstruktion des Zerfällungskörper

Als nächstes wird eine Möglichkeit benötigt, mit den Nullstellen von f zu rechnen. Man erhält den Zerfällungskörper durch sukzessive Adjunktion der Nullstellen von f.

Im ersten Schritt entsteht der Körper $L_1 = \mathbb{Q}(\alpha_1)$, wobei α_1 die definierende Gleichung $f(x) = 0$ erfüllt. Nun kann f als Polynom aus $L_1[x]$ betrachtet und dort in irreduzible Faktoren zerlegt werden. Sei α_2 Nullstelle eines nicht-linearen Faktors, dann wird als nächster Körper $L_2 = L_1(\alpha_2)$ konstruiert. Diese Prozedur wird fortgesetzt, bis der Zerfällungskörper erreicht ist, f beim Faktorisieren im zuletzt entstandenen Polynomring also in Linearfaktoren zerfällt. Da die Anzahl der Nullstellen von f endlich ist und in jedem Schritt eine weitere Nullstelle adjungiert wird, terminiert der Algorithmus.

Die Körper L_i werden bei der Konstruktion als einfache Erweiterungen von $\mathbb{Q}$ dargestellt. In jedem Schritt wird mit der Funktion `Primitives_Element()` ein primitives Element gesucht. Ist $L_i = \mathbb{Q}(\gamma_i)$, so wird also von $L_{i+1} = L_i(\alpha_{i+1})$ das primitive Element $\gamma_{i+1} = \alpha_{i+1} + c\gamma_i$ mit minimalem $c \in \mathbb{N}$ bestimmt.

Es soll erläutert werden, wie die Konstruktion des Zerfällungskörpers mit den gewählten Darstellungen für Erweiterungskörper realisiert wird. Die Vorgehensweise wird induktiv beschrieben. Im ersten Schritt wird ein Körper $L_1 \cong \mathbb{Q}(\alpha_1)$ gesucht, wobei α_1 eine Nullstelle von $f = \sum_{i=0}^{n-1} a_i x^i \in \mathbb{Q}[x]$ bezeichnet. Ist

$$M_f = \begin{pmatrix} 0 & 1 & & & \\ & 0 & \ddots & & \\ & & \ddots & 1 & \\ & & & 0 & 1 \\ -a_0 & & \dots & & -a_{n-1} \end{pmatrix}$$

die Begleitmatrix von f, dann erfüllt der Matrixkörper $\mathbb{Q}[M_f]$ diese Bedingung. Die definierende Gleichung von L_1 ist $f(x) = 0$ vor, so dass man auch im Quotientenkörper rechnen kann. Das primitive Element des Matrixkörpers muss nicht extra bestimmt werden, denn es ist einfach M_f.

Nach Induktionsvoraussetzung sei nun L_i in beiden Darstellungen realisiert. Das bedeutet, γ_i entspricht der Matrix M_i und deren Minimalpolynom g_i ist bekannt, so dass $L_i \cong \mathbb{Q}[M_i] \cong \mathbb{Q}[x]/(g_i)$ gilt. Man faktorisiere f über L_i und wähle einen nicht-linearen Faktor h. Falls keiner existiert, ist die Konstruktion abgeschlossen und $\mathbb{Q}_f = L_i$ der Zerfällungskörper von f. Ansonsten wird durch die Begleitmatrix von h der Körper $L_{i+1} = L_i[M_h]$ erzeugt. Dieser besteht aus Matrizen der Dimension $\mathrm{Grad}(h)$, deren Einträge aus $\mathbb{Q}[x]/(g_i)$ sind. Benutzt man für die Einträge in den Matrizen aus $L_i[M_h]$ ihre Matrixdarstellung aus $\mathbb{Q}[M_i]$, kann man L_{i+1} auch als Matrixkörper über $\mathbb{Q}$ auffassen. Die Dimension der Matrizen ist $\mathrm{Grad}(h)[L_i : \mathbb{Q}] = [L_{i+1} : \mathbb{Q}]$. Die Einbettung von L_i in L_{i+1} geschieht durch Bilden des Kroneckerprodukts $\mathbb{E} \otimes M$ für $M \in L_i$, wobei $\mathbb{E}$ die Einheitsmatrix der Dimension $\mathrm{Grad}(h)$ ist. Für $L_{i+1} = \mathbb{Q}[M_h, \mathbb{E} \otimes M_i]$ wird mittels `Primitives_Element(`$M_h, \mathbb{E} \otimes M_i$`)` eine Matrix M_{i+1} bestimmt, so dass $L_{i+1} = \mathbb{Q}[M_{i+1}]$ gilt. Deren Minimalpolynom g_{i+1} liefert die definierende Gleichung für L_{i+1}.

Im Pseudocode zur beschriebenen Konstruktion des Zerfällungskörpers werden die in der Implementation gewählten Darstellungen algebraischer Elemente benutzt, um einen Eindruck der Umsetzung zu vermitteln.

```
INPUT: Irreduzibles Polynom f ∈ ℚ[x]
OUTPUT: Primitives Element in Matrixdarstellung von ℚ_f über ℚ

Zerfällungskörper(f)
  Setze M_γ = (1)     # Initialisierung ℚ[M_γ] ≅ ℚ
  while f ≠ 1 do
    h := irreduzibler Faktor von f
    M_h := Begleitmatrix von h
    𝔼 := M_h^0      # Einheitsmatrix gleicher Größe wie M_h
    Stelle Einträge in M_h mit Elementen aus ℚ[M_γ] dar
    M_γ := Primitives_Element(M_h, 𝔼 ⊗ M_γ)
    g := Minimalpolynom von M_γ
    Faktorisiere f über ℚ[x]/(g)
    Bezeichne mit f_1, ..., f_k die Linearfaktoren von f
    f := f/(f_1 ··· f_k)
  end while
return M_γ
```

Damit ist $\mathbb{Q}_f$ als einfache Erweiterung $\mathbb{Q}(\gamma)$ konstruiert, deren Grad $m = [\mathbb{Q}_f : \mathbb{Q}]$ ein Teiler von $n!$ ist. Die Anzahl der benötigten Durchläufe bis der Zerfällungskörper erreicht ist wird fortan mit s bezeichnet. Es ist also $L_s = \mathbb{Q}_f$ und γ ist eine $\mathbb{N}$-Linearkombination aus s Nullstellen von f.

5.2.4 Finden der Nullstellen von f

Nach Satz 3.3.2 kann die Galoisgruppe als Permutationsgruppe auf den Wurzeln aufgefasst werden. Um G_f ermitteln zu können, muss den Nullstellen von f eine Reihenfolge zugewiesen werden. Das ist nun möglich, da mit $\mathbb{Q}_f$ ein Körper erreicht ist, in dem alle Wurzeln der Gleichung $f(x) = 0$ liegen. Die einfachste Methode ist, f über $\mathbb{Q}_f$ zu faktorisieren und die Nullstellen aus den Linearfaktoren zu ermitteln. Man bekommt daraus eine willkürliche Reihenfolge der Nullstellen, die nur vom Faktorisierungsalgorithmus abhängt.

Hier sollen die Nullstellen schon während der Konstruktion des Zerfällungskörpers gespeichert werden. Das erleichtert es, den Aufbau des primitiven Elements γ nachzuvollziehen, der später noch benötigt wird. Dabei bekommt jede neu adjungierte Nullstelle

von f den nächsten freien Index, so dass beim Erreichen des Zerfällungskörpers eine Liste mit den Nullstellen $\alpha_1, \ldots, \alpha_s$ vorliegt. Die übrigen Nullstellen $\alpha_{s+1}, \ldots, \alpha_n$ können im Anschluss aus den Linearfaktoren von f über $\mathbb{Q}_f = \mathbb{Q}(\alpha_1, \ldots, \alpha_s)$ ermittelt werden. Bei diesem Vorgehen ist es notwendig die gespeicherten Nullstellen in jede neue Erweiterung zu übertragen. Dies geschieht durch die im Abschnitt 5.2.3 beschriebene Einbettung von L_i in L_{i+1} mit Hilfe des Kroneckerprodukts (vgl. Abschnitt 5.1.1). Als erweiterte Version von `Zerfällungskörper()` erhält man die folgende Funktion.

```
INPUT: Irreduzibles Polynom f ∈ ℚ[x]
OUTPUT: Primitives Element in Matrixdarstellung von ℚ_f über ℚ
        Liste der Nullstellen von f als Matrizen

Zerfällungskörper_und_Nullstellen(f)
  M_γ := (1)     # Initialisierung ℚ[M_γ] ≅ ℚ
  Wurzeln := [ ]     # leere Liste
  while f ≠ 1 do
    h := irreduzibler Faktor von f
    M_h := Begleitmatrix von h
    𝔼 := M_h^0      # Einheitsmatrix gleicher Größe wie M_h
    Stelle Einträge in M_h mit Elementen aus ℚ[M_γ] dar
    M_γ := Primitives_Element(M_h, 𝔼 ⊗ M_γ)
    Ersetze jede Matrix M in Wurzeln durch 𝔼 ⊗ M
    Füge Wurzeln die Matrix M_h hinzu
    g := Minimalpolynom von M_γ
    Faktorisiere f über ℚ[x]/(g)
    Bezeichne mit f_1,...,f_k die Linearfaktoren von f
    f := f/(f_1 ··· f_k)
  end while
  for i in [ 1..n ] do
    α := -(Koeffizient vor x^0 von f_i)
    Stelle α als Matrix M aus ℚ[M_γ] dar
    if M ∉ Wurzeln then
      Füge Wurzeln die Matrix M hinzu
    end if
  end for
return M_γ und Wurzeln
```

Die Funktion gibt zusätzlich zum primitiven Element des Zerfällungskörpers noch die Nullstellen $\alpha_1, \ldots, \alpha_n$ von f in ihrer Matrixdarstellung zurück.

Damit kann die Gestalt des primitiven Elements angegeben werden. Es gilt $\gamma = \sum_{i=1}^{s} c_i \alpha_i$

mit $c_i \in \mathbb{N}$, da in der Funktion `Primitives_Element()` stets $\mathbb{N}$-Linearkombinationen gebildet werden. Die Matrixdarstellungen von γ sowie $\alpha_1, \ldots, \alpha_s$ sind bekannt, so dass die c_i aus $\gamma = \sum_{i=1}^{s} x_i \alpha_i$ zu ermitteln sind. Da die α_i linear unabhängig sind – sie liegen in der gleichen $\mathbb{Q}$-Basis von $\mathbb{Q}_f$ –, ist die Lösung eindeutig.

5.2.5 Bestimmung von G_f

Bezogen auf die gewählte Reihenfolge der Nullstellen kann G_f ermittelt werden. Zuerst wird die Abbildung von Körperelementen unter einem Automorphismus realisiert. Nach Satz 3.3.2 reicht es, von $\sigma \in \mathrm{Gal}(\mathbb{Q}_f/\mathbb{Q})$ dessen Einschränkung auf $\{\alpha_1, \ldots, \alpha_n\}$ zu kennen. Andererseits ist ein Automorphismus von $\mathbb{Q}_f = \mathbb{Q}(\gamma)$ eindeutig durch seine Wirkung auf das primitive Element γ bestimmt. Die zu σ gehörende Permutation aus G_f sei mit τ bezeichnet, so dass $\alpha_i^\sigma = \alpha_{i^\tau}$ ist. Dann gilt für das primitive Element offensichtlich $\gamma^\sigma = \sum_{i=1}^{s} c_i \alpha_{i^\tau}$. Für ein beliebiges Körperelement der Form $\sum_{i=0}^{m-1} a_i \gamma^i$ mit $a_i \in \mathbb{Q}$ ist das Bild wegen der Homomorphie von σ durch $\sum_{i=0}^{m-1} a_i (\gamma^\sigma)^i$ gegeben. Liegt die Permutation $\tau \in G_f$ vor, kann sie daher mit der folgenden Funktion homomorph auf $\mathbb{Q}_f$ fortgesetzt werden.

```
INPUT: α ∈ Q_f, Permutation τ (aus G_f), γ = Σ_{i=1}^{s} c_i α_i
OUTPUT: α^σ, das Bild von α unter der Fortsetzung σ von τ

Bild(α, σ, γ)
  Löse α = a_0 + a_1 γ +...+ a_{m-1} γ^{m-1}      # lineares GlS
  γ̄ := Σ_{i=1}^{s} c_i α_{i^τ}      # γ̄ = γ^σ
  α^σ := a_0 + a_1 γ̄ +...+ a_{m-1} γ̄^{m-1}
return α^σ
```

Damit $\tau \in S_n$ in G_f liegt, muss γ nach Folgerung 3.3.7 auf ein konjugiertes Element abgebildet werden, was bedeutet, dass $\mathtt{Bild}(\gamma, \tau, \gamma)$ Nullstelle des Minimalpolynoms g von γ sein muss. Das soll genutzt werden, um die Permutationen aus G_f zu bestimmen.

5.2.2 Satz: *Sei τ eine Permutation aus S_n, für die $\mathtt{Bild}(\gamma, \tau, \gamma)$ zu γ konjugiert ist. Dann definiert*

$$\alpha_{i^\sigma} = \mathtt{Bild}(\alpha_i, \tau, \gamma) \text{ für } i = 1, \ldots, n \tag{5.1}$$

eine Permutation $\sigma \in G_f$, und es gilt $\mathtt{Bild}(\gamma, \sigma, \gamma) = \mathtt{Bild}(\gamma, \tau, \gamma)$.

Beweis: Ein Automorphismus $\rho \in \mathrm{Gal}(\mathbb{Q}_f/\mathbb{Q})$ ist durch seine Wirkung auf das primitive Element γ eindeutig bestimmt. Nach Folgerung 3.3.7 ist dann γ^ρ zu γ konjugiert. Weiterhin gilt $\mathrm{Grad}(g) = [\mathbb{Q}_f : \mathbb{Q}] = |\mathrm{Gal}(\mathbb{Q}_f/\mathbb{Q})|$, wobei g das Minimalpolynom von γ ist. Daher tritt jedes zu γ konjugierte Element als γ^ρ für ein $\rho \in \mathrm{Gal}(\mathbb{Q}_f/\mathbb{Q})$ auf.

Nun ist $\texttt{Bild}(\gamma, \tau, \gamma)$ zu γ konjugiert, so dass die homomorphe Fortsetzung von τ durch $\texttt{Bild}(\cdot, \tau, \gamma)$ einem Automorphismus $\rho \in \mathrm{Gal}(\mathbb{Q}_f/\mathbb{Q})$ entspricht. Dieser erfüllt nach seiner Definition die Gleichungen $\alpha_i^\rho = \texttt{Bild}(\alpha_i, \tau, \gamma)$ für $i = 1, \ldots, n$. Mit Satz 3.3.2 folgt (5.1) für die Einschränkung $\sigma \in G_f$ von ρ. Da σ auf $\mathbb{Q}_f$ fortgesetzt wieder ρ ergibt, gilt auch $\texttt{Bild}(\gamma, \sigma, \gamma) = \texttt{Bild}(\gamma, \tau, \gamma)$. □

5.2.3 Beispiel: Es sei $\gamma = \alpha_1 + \alpha_2$ und $\tau = (12)$. Dann wird γ auf ein Konjugiertes, nämlich sich selbst abgebildet, weshalb α_1 und α_2 bei der homomorphen Fortsetzung mittels $\texttt{Bild}(\cdot, \tau, \gamma)$ fest bleiben, anstatt wie unter τ zu vertauschen. Wählt man σ so, dass (5.1) erfüllt ist, erhält man die Permutation $\sigma = () \in G_f$.

Sucht man auf diese Weise nach allen Elementen aus G_f, muss man nur dafür sorgen, dass jedes Konjugierte von γ als $\texttt{Bild}(\gamma, \tau, \gamma)$ vorkommt. Dies ist sicher gewährleistet, wenn man eine Transversale von $\mathrm{Stab}_{S_n}(\gamma)$ durchläuft. Um den Stabilisator nicht berechnen zu müssen, werden stattdessen die Untergruppe $\mathrm{Stab}_{S_n}((1, \ldots, s))$ und deren Transversale betrachtet. (Der Stabilisator des Tupels $(1, \ldots, s)$ ist eine Untergruppe von $\mathrm{Stab}_{S_n}(\gamma)$, da $\sum_{i=1}^s c_i\alpha_i$ fest bleibt, wenn schon jedes α_i fest bleibt.) Außerdem muss man nur Erzeuger ermitteln, um G_f zu bestimmen. Dabei kann man abbrechen, wenn die gefundenen Permutationen eine Gruppe der Ordnung m erzeugen, da für die Ordnung der Gruppe $|G_f| = [\mathbb{Q}_f : \mathbb{Q}]$ nach Theorem 3.4.5 gilt.

```
INPUT: Nullstellen α_1,...,α_n eines Polynoms f ∈ Q[x];
       primitives Element γ = Σ_{i=1}^s c_i α_i von Q_f
OUTPUT: Galoisgruppe G_f zu α_1,...,α_n

Galoisgruppe((α_1,...,α_n), γ)
  G_f := ∅
  T := Transversale von Stab_{S_n}(1,...,s)
  Wähle P mit γ^P = γ^T und |P| = |γ^P|     # doppelte Bilder entfernen
  P := {τ ∈ P | Bild(γ,τ,γ) ist zu γ konjugiert}
  repeat
    Wähle τ aus P
    for i in [ 1..n ] do
      ᾱ_i := Bild(α_i,τ,γ)
    end for
    Wähle σ ∈ S_n so, dass (α_{1^σ},...,α_{n^σ}) = (ᾱ_1,...,ᾱ_n) ist
    G_f := ⟨G_f, σ⟩
    P := {τ ∈ P | Bild(γ,τ,γ) ≠ Bild(γ,σ,γ) ∀ σ ∈ G_f}
  until |G_f| = [Q(γ) : Q]
return G_f
```

Die passende Permutation zu einer gefundenen Bijektion ist leicht zu bestimmen. Man muss dazu einfach die Veränderung der Indizes nachvollziehen.

In diesem Unterabschnitt war es wichtig sich zu überlegen, wie die Körperautomorphismen realisiert werden. Da G_f nun konstruiert ist und $\texttt{Bild}(\alpha, \tau, \gamma)$ daher nur noch für $\tau \in G_f$ angewendet wird, kann stattdessen wieder kurz α^σ notiert werden. Mit welcher Funktion das Bild ermittelt wird, hat keine Bedeutung mehr.

5.3 Berechnung einer Körperkette

Für die Radikalerweiterung $\mathbb{Q}_f = \mathbb{Q}(\gamma)$ wird jetzt eine Liste von Elementen $\beta_1, \ldots, \beta_r$ mit der Eigenschaft $\beta_i^{p_i} \in \mathbb{Q}(\beta_1, \ldots, \beta_{i-1})$ benötigt, wie sie in Definition 4.4.3 gefordert ist. Dann läge eine Körperkette vor, deren nächstes Glied stets durch Adjunktion der Wurzel einer reinen Gleichung entsteht. Dies geschieht hier in zwei Schritten. Erst wird mit Hilfe der Galoiskorrespondenz eine Körperkette bestimmt, deren einzelne Erweiterungsschritte zyklisch sind. Im Anschluss wird für jeden Erweiterungsschritt ein spezielles primitives Element ermittelt, das Lösung einer reinen Gleichung ist. Dieses Vorgehen ist genau deshalb möglich, weil die Galoisgruppe auflösbar ist.

5.3.1 Primitive Elemente

Zu der auflösbaren Galoisgruppe G_f wird eine Kompositionsreihe

$$G_f = G_1 \rhd G_2 \rhd \cdots \rhd G_r \rhd G_{r+1} = \{1\} \tag{5.2}$$

berechnet, deren Faktorgruppen G_i/G_{i+1} nach Abschnitt 2.2 Primzahlordnung haben. Für $|G_i/G_{i+1}|$ wird die Bezeichnung p_i gewählt. Es wird dieselbe Theorie wie zur Prüfung der Auflösbarkeit einer Permutationsgruppe verwendet (vgl. Abschnitt 5.2.1). Eine Zusammenstellung algorithmischer Lösungsmethoden für Permutationsgruppen mit Betrachtung existierender Implementationen findet sich bei Seress [28].

Nach dem Hauptsatz der Galoistheorie 3.4.5, korrespondiert jede Untergruppe von G_f zu einem Zwischenkörper von $\mathbb{Q}_f/\mathbb{Q}$. Zu der Kompositionsreihe kann dem entsprechend eine korrespondierende Körperkette bestimmt werden (vgl. Abbildung 5.1).

Um primitive Elemente der einzelnen Körpererweiterungen in der Kette zu finden, wird auf Satz 3.4.7 zurückgegriffen. Demnach erzeugen die Koeffizienten von

$$j_{G_i}(x) = \prod_{\sigma \in G_i} x - \gamma^\sigma \tag{5.3}$$

den zu G_i gehörenden Fixkörper K_i. Die Koeffizienten eines Polynoms sind - bis aufs Vorzeichen - die elementarsymmetrischen Funktionen in dessen Nullstellen. Bezeichnen

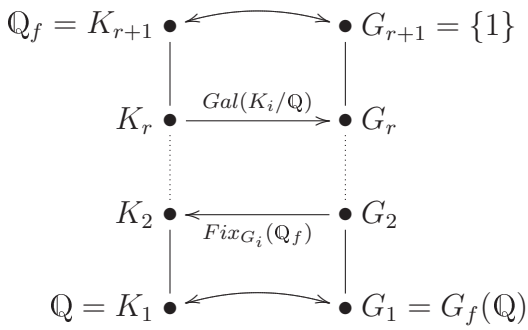

Abbildung 5.1: Korrespondenz zwischen Kompositionsreihe und Körperkette

$\sigma_1, \ldots, \sigma_l$ die Permutationen aus G_i und s_k die k-te elementarsymmetrische Funktion, dann sind $s_1(\gamma^{\sigma_1}, \ldots, \gamma^{\sigma_l}), \ldots, s_l(\gamma^{\sigma_1}, \ldots, \gamma^{\sigma_l})$ die Koeffizienten von j_{G_i}, weshalb $K_i = \mathbb{Q}(s_1(\gamma^{\sigma_1}, \ldots, \gamma^{\sigma_l}), \ldots, s_r(\gamma^{\sigma_1}, \ldots, \gamma^{\sigma_l}))$ folgt.

Aus Folgerung 3.4.6 ist bekannt, dass $\mathrm{Gal}(K_{i+1}/K_i) = G_i/G_{i+1}$ gilt, und der Grad $[K_{i+1} : K_i]$ entspricht nach dem Hauptsatz 3.4.5 der Ordnung der zugehörigen Galoisgruppe und ist somit gleich p_i. Eine Körpererweiterung von Primzahlgrad hat keine echten Zwischenkörper, so dass für jedes $\beta \in K_i - K_{i-1}$ bereits $K_i = K_{i-1}(\beta)$ ist. Lägen alle Koeffizienten von $j_{G_i}(x)$ in K_{i-1}, könnten sie nicht K_i erzeugen. Daher findet sich unter den Koeffizienten mindestens einer, der sich als primitives Element eignet.

Als Funktion zur Bestimmung primitiver Elemente jeder Erweiterung in der Körperkette erhält man daraus:

```
INPUT: Kompositionsreihe G_1,...,G_{r+1} von G_f,
       primitives Element γ von Q_f
OUTPUT: Primitive Elemente von K_i = Fix_{G_i}(Q_f) bezüglich K_{i-1}

Fixkörper(G_1,...,G_{r+1}, γ)
  K := Q
  for i in [1..r] do
    k := 1
    repeat
      c_k := s_k({σγ | σ ∈ G_{i+1}})
      k := k+1
    until c_k ∉ K
    β_i := c_k
    K := K(β_i)      # Fixkörper von G_{i+1}
  end for
return β_1,...,β_r
```

Da das Polynom zur trivialen Gruppe $x-\gamma$ ist, gibt die Funktion als primitives Element von K_{r+1}/K_r wieder γ selbst zurück. Es ist also $K_{i+1} = K_i(\beta_i)$ und speziell $\beta_r = \gamma$.

5.3.2 Zyklische Elemente

Für jede Erweiterung K_{i+1}/K_i liegt mit β_i zwar ein primitives Element vor, aber im Allgemeinen keines, das einer reinen Gleichung genügt. Um ein solches zu ermitteln, muss zusätzliches Wissen aus der Korrespondenz zwischen der Körperkette und der Kompositionsreihe genutzt werden. Aus Folgerung 3.4.6 ist bekannt, dass $\mathrm{Gal}(K_{i+1}/K_i) = G_i/G_{i+1}$ gilt, womit die Erweiterungen in der Körperkette jeweils zyklisch vom Grad p_i sind.

Zyklische Körpererweiterungen vom Grad p können nach Satz 4.3.5 durch Adjunktion einer p-ten Wurzel erzeugt werden. Dazu müssen aber die p-ten Einheitswurzeln im Grundkörper enthalten sein. Damit diese Voraussetzung stets erfüllt ist, soll an alle Glieder der Körperkette eine primitive h-te Einheitswurzel ζ_h adjungiert werden, wobei h das Produkt der in $|G_f|$ vorkommenden Primfaktoren ist. Die Bezeichnungen werden aus Abschnitt 4.2 übernommen. Für den Parameter h sind $\widetilde{\mathbb{Q}} = \mathbb{Q}_h$ und entsprechend $\widetilde{K}_i = K_i(\zeta_h)$.

Um $\widetilde{\mathbb{Q}}_f$ zu erhalten, faktorisiere man das h-te Kreisteilungspolynom ϕ_h über $\mathbb{Q}_f$. Ein irreduzibler Faktor sei mit ϕ bezeichnet. Dann ist $\widetilde{\mathbb{Q}}_f \cong \mathbb{Q}_f[x]/(\phi)$ nach Lemma 3.1.8. Es ist $\mathrm{Grad}(\phi) = [\widetilde{\mathbb{Q}}_f : \mathbb{Q}_f]$ und insbesondere hat jeder irreduzible Faktor von ϕ_h den gleichen Grad, da alle h-ten Einheitswurzeln in $\widetilde{\mathbb{Q}}_f$ liegen.

Jetzt wird betrachtet, was mit den einzelnen Körpererweiterungen in der Körperkette bei Adjunktion von ζ_h geschieht. Nach Lemma 3.4.8 ist $\mathrm{Gal}(\widetilde{K}_{i+1}/\widetilde{K}_i)$ einer Untergruppe von $\mathrm{Gal}(K_{i+1}/K_i)$ isomorph, wofür nur die triviale Gruppe und die Gruppe selbst in Frage kommen. Mithin ist jede der zyklischen Körpererweiterungen nach der Adjunktion entweder noch vom Grade p_i oder gar keine echte Erweiterung mehr. Der neue Grad wird mit $\widetilde{p}_i$ bezeichnet. Er ist genau dann 1, wenn β_i in $\widetilde{K}_i$ liegt. In jedem Falle behalten die Gleichungen $\widetilde{K}_{i+1} = \widetilde{K}_i(\beta_i), i = 1, \ldots, r$ ihre Gültigkeit.

Aus dem konstruktiven Beweis von Satz 4.3.5 wird ein Algorithmus deduziert, der aus jedem der β_i ein erzeugendes Element von $\widetilde{K}_{i+1}$ ermittelt, das einer reinen Gleichung im Körper $\widetilde{K}_i$ genügt. Ein solches liefert die Lagrangesche Resolvente $(\zeta_{p_i}, \cdot)$, wenn ihr Wert ungleich Null ist. Dabei erhält man eine p_i-te Einheitswurzel ζ_{p_i} durch Potenzieren von ζ_h mit $\frac{h}{p_i}$.

Nach Definition ist die Lagrangesche Resolvente eine lineare Abbildung von $\widetilde{K}_{i+1}$ in sich selbst, deren Bild nach Satz 4.3.5 nicht $\{0\}$ ist. Auf Grund der Linearität existiert

in einer beliebigen Basis ein Element, das nicht auf Null abgebildet wird. Betrachtet man die Basis $1, \beta_i, \ldots, \beta_i^{p_i-1}$, können daher nicht alle Potenzen von β_i im Kern der Lagrangeschen Resolvente liegen. Beachtet man noch $(\zeta_{p_i}, 1) = 0$, findet sich ein k mit $1 \leq k \leq p_i - 1$ und $(\zeta_{p_i}, \beta_i^k) \neq 0$. Für ein entsprechendes k ist (ζ_{p_i}, β_i^k) nach Satz 4.3.5 ein primitives Element von $\widetilde{K}_{i+1}/\widetilde{K}_i$, für welches $(\zeta_{p_i}, \beta_i^k)^{p_i} \in K_i^*$ gilt.

```
INPUT: Erzeuger der Galoisgruppe einer zyklischen Erweiterung;
       primitives Element der Erweiterung
OUTPUT: Zyklisches Element der Erweiterung

Lagrangesche_Resolvente(σ, β)
  p := o(σ)     # Ordnung von σ
  k := 0
  repeat
    k := k+1
    (σ, β) := Σ_{i=0}^{l-1} ζ_p^i σ^i(β^k)     # ζ_p: primitive p-te Einheitswurzel
  until (σ, β) ≠ 0
return (σ, β)
```

Bevor `Lagrangesche_Resolvente` auf alle Elemente der Körperkette angewendet wird, benötigt man Erzeuger von $\mathrm{Gal}(\widetilde{K}_{i+1}/\widetilde{K}_i) = G_i/G_{i+1}$ für $i = 1, \ldots, r$. Diese sind besonders einfach zu bestimmen, da jede Faktorgruppe G_i/G_{i+1} Primzahlordnung hat. Somit ist $G_i/G_{i+1} = \langle \sigma G_{i+1} \rangle$ für alle $\sigma \in G_i - G_{i+1}$.

```
INPUT: Kompositionsreihe von G_f;
       primitive Elemente der korrespondierenden Körperkette
OUTPUT: Zyklische Elemente der Körperkette

Zyklische_Elemente([ G_1,...,G_{r+1} ], [ β_1,...,β_r ])
  for i in [ 1..r ] do
    σ := Erzeuger von G_i/G_{i+1}
    ω_i := Lagrangesche_Resolvente(σ, β_i)
  end for
return ω_1,...,ω_r
```

Die reine Gleichung, die ω_i über $\widetilde{K}_i$ erfüllt, sei $x^{\widetilde{p}_i} - a_i = 0$. Nach Folgerung 4.3.3 ist diese in $\widetilde{K}_i[x]$ irreduzibel und zerfällt über $\widetilde{K}_{i+1}$ in Linearfaktoren, da mit ω_i eine der Nullstellen in $\widetilde{K}_{i+1}$ liegt. Somit ist $\widetilde{\mathbb{Q}}(\omega_1, \ldots, \omega_r)$ eine irreduzible Radikalerweiterung über $\widetilde{\mathbb{Q}}$. Gesucht wurde ursprünglich eine Radikalerweiterung über $\mathbb{Q}$. Nun ist ζ_h für jedes $h \in \mathbb{N}$ nach Lemma 4.5.2 durch irreduzible Radikale darstellbar. Indem man den

hier vorgestellten Algorithmus rekursiv benutzt, kann $\mathbb{Q}_h$ durch zyklische Elemente erzeugt werden. Für $k \in \mathbb{N}$ ist $k > \varphi(k) = |G_{\phi_k}|$, so dass im nächsten Rekursionsschritt der Kreisteilungskörper zu einer kleineren natürlichen Zahl durch zyklische Elemente erzeugt werden soll. Die Rekursion endet, wenn $\mathbb{Q}$ selbst der Körper mit den benötigten Einheitswurzeln ist. Insgesamt ist dann $\widetilde{\mathbb{Q}}_f/\mathbb{Q}$ als irreduzible Radikalerweiterung dargestellt.

5.4 Darstellung der Nullstellen

Im letzten Schritt des Algorithmus erfolgt die Angabe einer irreduziblen Radikaldarstellung für die Wurzeln von f. Dazu wird eine $\widetilde{\mathbb{Q}}$-Basis aus den zyklischen Elementen $\omega_1, \ldots, \omega_r$ gebildet. Diese wird einerseits für die Berechnungen als eine Menge von Matrizen aus $\widetilde{\mathbb{Q}}_f$ benötigt und andererseits in Radikaldarstellung für die Ausgabe.

Die Darstellung für ζ_h durch irreduzible Radikale nach Lemma 4.5.2 wird im Folgenden als bekannt vorausgesetzt. Für kleine Primzahlen p sind entsprechende Darstellungen der p-ten Einheitswurzeln in der Tabelle 4.1 zu finden. Diese decken fast alle für die Implementation momentan interessanten Fälle ab. Induktiv lässt sich zu jeder Zahl $h \in \mathbb{N}$ eine Darstellung einer primitiven h-ten Einheitswurzel bestimmen. Dieses Vorgehensweise wurde schon im Beweis zu Lemma 4.5.2 verwendet.

Im Code der Funktion `Basis` wird unterschieden zwischen den Elementen als Matrizen und in der Radikaldarstellung. Letztere wird mit $\widehat{\ }$gekennzeichnet. Mit ihr können keine Berechnungen durchgeführt werden.

5.4.1 Beispiel: Die Situation kann man sich am Rechnen in den komplexen Zahlen verdeutlichen. Die imaginäre Einheit i, oder auch $\sqrt{-1}$, ist ein Symbol, das wir zu interpretieren gelernt haben. Im Computer kann man i zum Beispiel als 2×2-Matrix $\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$ realisieren, denn es gilt $\mathbb{C} \cong \{\left(\begin{smallmatrix} a & b \\ -b & a \end{smallmatrix}\right) \mid a, b \in \mathbb{R}\}$. Für die Ausgabe würde $\left(\begin{smallmatrix} a & b \\ -b & a \end{smallmatrix}\right) = a\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) + b\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$ dann zu $a + bi$.

```
INPUT: Elemente ω_1,...,ω_r, für die ω_i^{p_i} ∈ Q̃(ω_1,...,ω_{i-1}) gilt
OUTPUT: Eine Basis aus dem Input

Basis( ω_1,...,ω_r )
  B := ( 𝟙 )      # das 1-Tupel mit der Eins aus Q̃_f
  for i in [ 1..r ] do
    l := Länge von B
    Wähle c als Lösung zu xB = ω_i^{p_i}      # Koeffizientenvektor aus Q̃^l
    ω̂_i := ∛(c_1 B_1 + ··· + c_l B_l)
    # Erzeugen der neuen Basis:
    for k in [ 1..p_i-1 ] do      # für ω_i bis ω_i^{p_i-1}
      for j in [ 1..l ]      # für alle bisherigen Basiselemente
        B_{j+kl} := B_j ω_i^k
        B̂_{j+kl} := B̂_j ω̂_i^k      # Verknüpfung ist Hintereinanderschreiben
      end for
    end for
  end for
return ( B, B̂ )
```

Die Radikaldarstellung $\widehat{B}_1$ zum Basiselement $\mathbb{1}$ bleibt leer, da nur der Koeffizient vor 1 interessiert. Im obigen Beispiel zu den komplexen Zahlen wird auch nicht $a1 + bi$, sondern nur $a + bi$ ausgegeben.

Die zurückgegebene Basis B lässt sich als $\{\omega^{e_1} \dots \omega^{e_r} \mid 0 \leq e_i < \widetilde{p}_i\}$ schreiben. Ersetzt man eines der ω_i durch eines seiner Konjugierten, gehen auch die Basiselemente in Konjugierte über. Demnach kann man die in $\widehat{B}$ auftretenden Wurzeln als jede beliebige Lösung der entsprechenden reinen Gleichung interpretieren.

Für jede Nullstelle α_i von f kann man nun die Gleichung

$$\alpha_i = c_1^i B_1 + c_2^i B_2 + \cdots + c_{|B|}^i B_{|B|}$$

über $\widetilde{\mathbb{Q}}$ lösen, wobei die B_i die Basiselemente aus B bezeichnen. Sind dazu passend $\widehat{B}_i$ die Symbole der Basis in Radikaldarstellung, so ist

$$c_1^i \widehat{B}_1 + c_2^i \widehat{B}_2 + \cdots + c_{|B|}^i \widehat{B}_{|B|}$$

die angestrebte Radikaldarstellung von α_i. Da f irreduzibel ist, steht nach Satz 4.4.9 jede der Darstellungen für alle Nullstellen von f. Die Anwendung eines Elements der Galoisgruppe G_f entspricht einer Neuwahl der Werte der Wurzeln.

5.5 Notation

f	normiertes, irreduzibles Polynom aus $\mathbb{Q}[x]$
n	Grad von f
α_i	Nullstelle von f
G_f	Galoisgruppe als Permutationsgruppe auf den Wurzeln von f
L_i	$\mathbb{Q}(\alpha_1, \ldots, \alpha_i)$
γ_i	primitives Element von L_i, $L_i = \mathbb{Q}(\gamma_i)$
M_i	Matrixdarstellung von γ_i
g_i	Minimalpolynom von γ_i über $\mathbb{Q}$
$\mathbb{Q}_f$	Zerfällungskörper von f, $\mathbb{Q}_f = \mathbb{Q}(\alpha_1, \ldots, \alpha_n)$
s	$\min\{i \mid L_i = \mathbb{Q}_f\}$
γ	primitives Element von $\mathbb{Q}_f/\mathbb{Q}$, $\gamma = \sum_{i=1}^{s} c_i\alpha_i, c_i \in \mathbb{N}$
m	Grad von $\mathbb{Q}_f$ über $\mathbb{Q}$, $m = [\mathbb{Q}_f : \mathbb{Q}]$
r	Länge einer Kompositionsreihe von G_f
G_i	i-te Gruppe der berechneten Kompositionsreihe
K_i	Fixkörper zu G_i, $K_i = \mathrm{Fix}_{\mathbb{Q}_f}(G_i)$
p_i	Grad der Erweiterung K_{i+1}/K_i, $p_i = [K_{i+1} : K_i]$
β_i	primitives Element von K_{i+1}/K_i, $K_{i+1} = K_i(\beta_i)$
h	Produkt der Primfaktoren von $\lvert G_f \rvert$
ζ_h	primitive h-te Einheitswurzel
$\widetilde{\mathbb{Q}}$	$\mathbb{Q}(\zeta_h)$
$\widetilde{K}_i$	$K_i(\zeta_h)$
$\tilde{p}_i$	Grad der Erweiterung $\widetilde{K}_{i+1}/\widetilde{K}_i$, $\tilde{p}(i) \in \{1, p_i\}$
ω_i	primitives Element von $\widetilde{K}_{i+1}/\widetilde{K}_i$ mit $\omega_i^{\tilde{p}_i} \in \widetilde{K}_i$
a_i	$\omega_i^{\tilde{p}_i}$
B	Basis von $\widetilde{\mathbb{Q}}_f$ aus $\omega_1, \ldots, \omega_r$, $B = \{\omega^{e_1} \ldots \omega^{e_r} \mid 0 \leq e_i < \tilde{p}_i\}$
B_i	Elemente aus B

Kapitel 6

Implementation und Laufzeiten

Nachdem im letzten Kapitel der theoretische Ablauf des Algorithmus präsentiert wurde, wird hier dessen Umsetzung in die Praxis behandelt. Der erste Abschnitt stellt die Implementation in GAP [32] vor, während der zweite Laufzeiten für Polynome mit verschiedenen Galoisgruppen beinhaltet.

6.1 Das GAP-Paket RADIROOT

Wie bereits erwähnt, wurde der Algorithmus aus Kapitel 5 im Computer-Algebra-System GAP implementiert. Die Implementation liegt als Programm-Paket RADIROOT [10] vor, das auch auf der beiliegenden CD gespeichert ist. Hier soll die vom Paket zur Verfügung gestellte Funktionalität erläutert werden.

6.1.1 Funktionalität

In der Hauptfunktion `RootsOfPolynomialAsRadicals()` wurde der Algorithmus aus Kapitel 5 umgesetzt. Zu einem irreduziblen Polynom aus $\mathbb{Q}[x]$ wird eine irreduzible Radikaldarstellung der Nullstellen ausgegeben. Als Zwischenergebnisse der notwendigen Berechnungen werden der Zerfällungskörper und die Galoisgruppe auf den Nullstellen des Polynoms bestimmt.

Es existiert eine weitere Version dieser Funktion, `RootsOfPolynomialAsRadicalsNC()`, die nicht als ersten Schritt die Auflösbarkeit der Galoisgruppe des Polynoms überprüft. Der Grund dafür ist, dass der zur Bestimmung des Isomorphietyps verwendete Befehl `GaloisType()` zur Zeit nur für Polynome funktioniert, deren Grad kleiner oder gleich

15 ist. In `RootsOfPolynomialAsRadicalsNC()` geschieht die Überprüfung erst, nachdem die Galoisgruppe als Permutationsgruppe auf den Wurzeln realisiert wurde. So können auch Polynome höherer Grade, wie z. B. ϕ_{17} (siehe Tabelle 4.1) behandelt werden.

Einzelne Schritte der Berechnungen sind auch als eigenständige Funktionen aufzurufen. So lässt sich mit `SplittingField()` der Zerfällungskörper eines irreduziblen Polynoms aus $\mathbb{Q}[x]$ bestimmen. Zudem gibt `GaloisGroupOnRoots()` eine Liste der Nullstellen $\alpha_1, \ldots, \alpha_n$ des Polynoms als Matrizen, sowie die zur Nummerierung in der Liste passende Galoisgruppe als Permutationsgruppe auf $\{1, \ldots, n\}$ zurück. Für Polynome, deren irreduzible Faktoren höchstens den Grad 15 haben, ermittelt `IsSolvablePolynomial()`, ob alle Nullstellen durch Radikale darstellbar sind.

6.1.2 Umsetzung des Algorithmus

Bei der theoretischen Darstellung des Algorithmus wurde Wert darauf gelegt, die praktische Umsetzung nicht außer Acht zu lassen. So wurde beschrieben, wie für die Elemente der Körpererweiterungen zwei verschiedene Darstellungen eingesetzt werden. Beim Rechnen mit Matrixkörpern kommt dabei das Paket ALNUTH [3] zum Einsatz. Um beim Faktorisieren von Polynomen die im Abschnitt 5.1.4 beschriebene Methode nutzen zu können, wird ALNUTH zudem in seiner Funktion als Interface zu KASH, der Shell des Computeralgebrasystems KANT [9], verwendet. In KANT ist das Verfahren aus [4] bereits integriert.

Ein Trick, der in Spezialfällen das zu behandelnde Problem stark vereinfacht, beruht auf der in Bemerkung 4.1.1 beschriebenen Transformation. Danach kann jedes Polynom $f(x)$ eindeutig in ein Polynom gleichen Grades überführt werden, dessen zweithöchster Koeffizient Null ist. Die Nullstellen der beiden Polynome unterscheiden sich dann nur um eine Konstante. So lässt sich eindeutig feststellen, ob man $f(x)$ als $g((x-a)^k)$ mit einem $k > 1$ schreiben kann. Falls ja, wird der Algorithmus auf g angewendet und dessen Nullstellen $\beta_1, \ldots, \beta_l$ ermittelt. Je k Nullstellen von f sind dann durch $\sqrt[k]{\beta_i + a}$ für $i \in \{1, \ldots, l\}$ gegeben.

Implizit wurde bei der Anwendung von `GaloisType()` Nutzen aus der Klassifikation transitiver Untergruppen der S_n gezogen. Hat man zumindest die maximal auflösbaren dieser Gruppen (siehe Abschnitt 2.4) und damit ihre Ordnungen, kann man z. B. die Konstruktion des Zerfällungskörpers abbrechen, wenn der Grad der Erweiterung keine dieser Ordnungen teilt. Der Vorteil der Funktion `RootsOfPolynomialAsRadicalsNC()` ist dagegen, dass sie ohne jedwede Kenntnis von Untergruppen der S_n auskommt.

Bei der Umsetzung des Kreisteilungskörpers werden je nach vorgegebenem Polynom $f \in \mathbb{Q}[x]$ verschiedene Methoden benutzt. Ist $[\widetilde{\mathbb{Q}}_f : \widetilde{\mathbb{Q}}] = [\mathbb{Q}_f : \mathbb{Q}]$, so wird $\widetilde{\mathbb{Q}}_f$ realisiert, indem eine $\mathbb{Q}$-Basis von $\mathbb{Q}_f$ nun als $\widetilde{\mathbb{Q}}$-Basis betrachtet wird. Dabei findet für $\widetilde{\mathbb{Q}}$ der in

GAP bereits vorhandene Kreisteilungskörper Verwendung. Ist dagegen $\widetilde{\mathbb{Q}}_f = \mathbb{Q}_f$, wird die benötigte Einheitswurzel aus $\mathbb{Q}_f$ bestimmt, und ist damit als Matrix dargestellt. Im letzteren Fall Koeffizienten aus den Kreisteilungskörpern von GAP zuzulassen, würde zu Widersprüchen führen, weil der entstehende Matrizenring nicht mehr nullteilerfrei und daher kein Körper wäre. Da die Situation für die Primteiler von h einzeln betrachtet werden kann, kommt man mit diesen beiden Fällen aus, solange $\mathbb{Q}_h \cap \mathbb{Q}_f$ ein Kreisteilungskörper ist. Zerfällt aber für eine Primzahl p mit $p \mid h$ das Kreisteilungspolynom ϕ_p über $\mathbb{Q}_f$ in nicht-lineare Faktoren, so ist keine der bisher aufgeführten Methoden anwendbar. In diesem Fall startet der Algorithmus neu. Dabei wird als Grundkörper $\widetilde{\mathbb{Q}}$ statt $\mathbb{Q}$ benutzt und als Matrixkörper dargestellt. Über dem Zerfällungskörper $\widetilde{\mathbb{Q}}_f$, der Matrizen der Dimension $[\widetilde{\mathbb{Q}}_f : \mathbb{Q}]$ enthält, zerfallen dann alle Kreisteilungspolynome ϕ_p mit $p \mid h$ in Linearfaktoren. Die benötigte Einheitswurzel liegt damit als Matrix vor. Der Nachteil dieser Methode im Vergleich zu den vorher angeführten ist die höhere Dimension der Matrizen.

6.1.3 Analyse der Laufzeiten und Schwachstellen

Von vorrangigem Interesse bei der Anwendung der Implementation ist deren Praktikabilität. Deshalb werden eine Reihe von Erfahrungswerten aus Testläufen präsentiert, die zeigen, wann eine Nutzung des Paketes RADIROOT sinnvoll ist. Die Laufzeiten für Polynome mit unterschiedlichen Galoisgruppen sind im nächsten Abschnitt als Tabelle aufgelistet.

Theoretisch ist der zeitbestimmende Schritt die Faktorisierung des Eingabepolynoms über dem Zerfällungskörper. Wie komplex diese Faktorisierung genau ist, hängt von der Form des definierenden Polynoms ab. Wünschenswert wäre ein möglichst kleiner Betrag dessen Diskriminante. Das definierende Polynom des Zerfällungskörpers ist gleich dem Minimalpolynom des primitiven Elements, dessen Gestalt durch die Methode in `Primitives_Element()` bestimmt wird. Unter zur Hilfenahme des LLL Algorithmus (siehe [7, 4.4.2]) ließe sich zumeist ein besseres primitives Element aus dem berechneten ermitteln. Bei Tests mit dieser Variante stellte sich aber heraus, dass sie die zeitaufwendigere Alternative ist. Sie beschleunigt zwar das Faktorisieren, braucht aber zu lange, um überhaupt ein geeignetes, definierendes Polynom zu bestimmen.

Da für das Faktorisieren auf KANT zurückgegriffen wird, ist dies in der Implementation selten die am längsten dauernde Berechnung. Am ehesten ist das für Polynome höherer Grade der Fall, wie etwa im Beispiel zur Gruppe T_{49} vom Grad 12 (vgl. Abschnitt 6.2). Die zweite Berechnung, die als zeitintensiver Schritt auftritt, ist die Bestimmung des Minimalpolynoms zum primitiven Element des Zerfällungskörpers. Die Suche danach ist exponentiell in der Ordnung der Galoisgruppe. Wenn dagegen der Grad $[\widetilde{\mathbb{Q}}_f : \mathbb{Q}_f]$ groß ist, braucht zumeist das Ermitteln einer Darstellung der Wurzeln von f bezüglich

einer Radikalbasis von $\widetilde{\mathbb{Q}}_f$ am längsten. Dies tritt auf, falls die Ordnung der Gruppe relativ große Primfaktoren hat, zu denen die Einheitswurzeln nicht schon in $\mathbb{Q}_f$ liegen.

Eine spezielle Schwachstelle wurde bereits in Abschnitt 6.1.2 angesprochen. Ist $\mathbb{Q}_h \cap \mathbb{Q}_f$ kein Kreisteilungskörper, wird der Algorithmus mit $\mathbb{Q}_h$ als Grundkörper neu gestartet. Wie sehr dies die Laufzeiten für Polynome mit ansonsten ähnlichen Voraussetzungen beeinflusst, demonstriert die letzte Tabelle im Abschnitt 6.2.

Letztlich beeinflusst natürlich auch die Größe der Koeffizienten, beziehungsweise der Diskriminante des Polynoms die Laufzeit.

6.2 Laufzeiten für transitive, auflösbare Gruppen

In diesem Abschnitt findet sich eine Liste mit transitiven, auflösbaren Untergruppen der S_n für $n \leq 15$ sowie zu jeder der Gruppen ein Polynom aus $\mathbb{Q}[x]$, das diese Gruppe als Galoisgruppe besitzt. Dabei wird dieselbe Nummerierung für transitive Gruppen wie in GAP [32] verwendet. Nähere Angaben zu den jeweiligen Gruppen entnimmt man der Arbeit von CONWAY, HULPKE und MCKAY [8].

Die ersten Spalten der Tabelle sind ein Auszug der im Anhang des Buchs von MALLE und MATZAT [23] befindlichen Liste mit Beispielpolynomen, ergänzt um die Ordnung der Gruppe und die Anzahl der Adjunktionsschritte bei der Konstruktion des Zerfällungskörpers.

Die Laufzeiten in der letzten Spalte beziehen sich auf die Anwendung der Funktion `RootsOfPolynomialAsRadicalsNC()` auf das Beispielpolynom. Die Berechnungen hierzu wurden unter SUSE 9.1 mit der Version 4.4.4 von GAP auf einem Pentium 4 Prozessor mit 3,2 GHz und 2 GB Arbeitsspeicher durchgeführt und zur Kontrolle auf einem zweiten, gleichartigen Rechner wiederholt. Angegeben ist jeweils der Mittelwert aus den beiden Durchläufen.

Zur Bestimmung der Laufzeiten wurde auf Vereinfachungen aus Zusammenhängen der Form $f(x) = g(x^k)$ (vgl. Abschnitt 6.1.2) verzichtet, um den Algorithmus tatsächlich für die angegebenen Galoisgruppen auszuführen.

	Name	$\lvert T_i \rvert$	s	Beispielpolynom	Laufzeit
Grad 2					
T_1	C_2	2	1	$x^2 + x + 1$	0,019
Grad 3					
T_2	S_3	6	2	$x^3 - x - 1$	0,080

	Name	$\lvert T_i\rvert$	s	Beispielpolynom	Laufzeit
T_1	C_3	3	1	$x^3 - x^2 - 2x + 1$	0,054
Grad 4					
T_5	S_4	24	3	$x^4 - x + 1$	1,704
T_4	A_4	12	2	$x^4 - 2x^3 + 2x^2 + 2$	0,514
T_3	D_4	8	2	$x^4 - x^3 - x^2 + x + 1$	0,168
T_2	V_4	4	1	$x^4 - x^2 + 1$	0,102
T_1	C_4	4	1	$x^4 + x^3 + x^2 + x + 1$	0,077
Grad 5					
T_3	F_{20}	20	2	$x^5 + x^4 + 2x^3 + 4x^2 + x + 1$	7,695
T_2	D_5	10	2	$x^5 - x^3 - 2x^2 - 2x - 1$	0,485
T_1	C_5	5	1	$x^5 + x^4 - 4x^3 - 3x^2 + 3x + 1$	0,332
Grad 6					
T_{13}	$C_3^2.D_4$	72	4	$x^6 + x^5 - x^2 - x + 1$	3:08:00,550
T_{11}	$C_2 \times S_4$	48	3	$x^6 + x^5 + 2x^4 + 2x^3 + 2x^2 + 2x + 1$	4:08,367
T_{10}	$C_3^2.C_4$	36	3	$x^6 + x^5 + x^4 + x^3 - 4x^2 + 5$	2:46,849
T_9	$C_3^2.C_2^2$	36	3	$x^6 - 2x^4 - 4x^3 + 6x^2 + 4x - 1$	2:32,365
T_8	$S_4/4$	24	2	$x^6 + 2x^5 - x^4 - 4x^3 + 7x^2 - 4x + 1$	8,327
T_7	S_4/V_4	24	2	$x^6 - x^2 - 1$	1,683
T_6	$C_2 \times A_4$	24	3	$x^6 + x^5 - 2x^3 + 2x - 1$	3,523
T_5	$C_3 \times S_3$	18	2	$x^6 + x^4 - x^3 - 2x^2 + x + 1$	1,431
T_4	A_4	12	2	$x^6 + x^4 - 2x^2 - 1$	0,475
T_3	D_6	12	2	$x^6 + x^4 - 2x^3 + x^2 - x + 1$	0,481
T_2	S_3	6	1	$x^6 + x^5 + 4x^4 + x^3 + 2x^2 - 2x + 1$	0,183
T_1	C_6	6	1	$x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$	0,107
Grad 7					
T_4	F_{42}	42	2	$x^7 + 2x^6 - 2x^5 - x^4 + 6x^3 - x + 4$	3:36:47,351
T_3	F_{21}	21	2	$x^7 - 8x^5 - 2x^4 + 16x^3 + 6x^2 - 6x - 2$	2:03:506
T_2	D_7	14	2	$x^7 + x^6 + 2x^5 + 4x^3 + 2x + 1$	7,533
T_1	C_7	7	1	$x^7 - x^6 - 12x^5 + 7x^4 + 28x^3 - 14x^2 - 9x - 1$	1,081

Für die bis hierhin angeführten Grade ist die Aufzählung der auflösbaren, transitiven Gruppen vollständig. Die weiteren Angaben beschränken sich auf Gruppen, deren Ordnung kleiner als 100 ist, da die Berechnungen darüberhinaus unpraktikabel beziehungsweise mit den zur Verfügung stehenden Mitteln nicht zu bewältigen sind. Trat dieser Fall

bei einem der angegebenen Beispiele auf, wurde die Laufzeit mit '–' gekennzeichnet. Die Polynome der Grade 13, 14 und 15 wurden aus der Datenbank [20] von KLÜNERS und MALLE entnommen, wobei jeweils das Polynom mit dem kleinsten Betrag seiner Diskriminante gewählt wurde. Zusätzlich wurden einige Polynome der Form $x^{12} + a, a \in \mathbb{Z}$ durch weniger triviale Beispiele aus der Datenbank ersetzt.

	$\lvert T_i\rvert$	s	Beispielpolynom	Laufzeit
Grad 8				
T_{34}	96	3	$x^8 + x^7 + 2x^6 - 3x^5 - x^3 + 10x^2 + 7x + 3$	51:39:34,345
T_{33}	96	3	$x^8 - 4x^7 + 4x^6 + 14x^4 - 28x^3 + 28$	29:11:10,620
T_{32}	96	3	$x^8 + x^6 + 3x^2 + 4$	13:44:50,790
T_{31}	64	3	$x^8 - 3x^6 - 4x^5 + x^4 + 6x^3 + 7x^2 + 4x + 1$	43:39.630
T_{30}	64	3	$x^8 + x^7 + 2x^6 + 5x^5 + x^4 + 5x^3 + 2x^2 + x + 1$	1:42:28,013
T_{29}	64	3	$x^8 - x^6 - x^4 + x^2 + 1$	29:36.450
T_{28}	64	3	$x^8 - x^6 - 6x^4 + 5$	40:27,758
T_{27}	64	3	$x^8 - 3x^6 + 4x^4 - 5x^3 + 3x^2 + 1$	1:10:18,306
T_{26}	64	3	$x^8 + x^7 + 3x^6 - x^4 - x^3 - 7x^2 + 4x - 1$	2:09:01,655
T_{25}	56	2	$x^8 - 4x^7 + 8x^6 - 6x^5 + 2x^4 + 6x^3 - 3x^2 + x + 3$	14:15:13,172
T_{24}	48	3	$x^8 + x^6 - 2x^5 + x^4 - 2x^3 + x^2 + 1$	20:32,450
T_{23}	48	2	$x^8 + x^7 - 2x^6 - 2x^4 + 9x^3 - 3x^2 + 2x + 1$	49:10,578
T_{22}	32	3	$x^8 - x^4 + 4$	12,578
T_{21}	32	3	$x^8 + 2x^4 - 4x^2 + 2$	32,938
T_{20}	32	3	$x^8 - 3x^7 + 12x^5 - 11x^4 - 12x^3 + 20x^2 + 3x + 1$	2:34,539
T_{19}	32	2	$x^8 + 4x^4 - 4x^2 + 1$	1:05,522
T_{18}	32	2	$x^8 - 2x^6 - 3x^4 + 4x^2 + 16$	8,466
T_{17}	32	2	$x^8 - 4x^5 + 2x^4 - 4x^3 + 9x^2 - 4x + 1$	11:01,457
T_{16}	32	3	$x^8 - 3x^7 + 3x^6 - x^5 + 5x^4 - x^3 - 2x^2 + 2x + 1$	2:05,728
T_{15}	32	2	$x^8 - 2x^7 + 3x^6 - 2x^5 - x^4 + 6x^3 + 7x^2 + 4x + 1$	1:12,852
T_{14}	24	2	$x^8 - x^6 - 3x^4 + 4x^2 + 4$	15,012
T_{13}	24	2	$x^8 + 2x^6 + 3x^4 - 3x^2 + 1$	12,011
T_{12}	24	2	$x^8 + 9x^6 + 23x^4 + 14x^2 + 1$	19,403
T_{11}	16	2	$x^8 - x^5 - 2x^4 + 4x^2 + x + 1$	3,607
T_{10}	16	2	$x^8 - 2x^6 - x^4 + 7x^2 - 5x + 1$	3,171
T_9	16	2	$x^8 + 2x^6 - 5x^4 + 2x^2 + 1$	1,187
T_8	16	2	$x^8 - 2x^7 + 2x^6 + x^4 + 5x^3 - 7x^2 - 6x + 1$	3,779
T_7	16	2	$x^8 - 5x^6 + 15x^4 - 15x^3 - 5x^2 + 15x - 5$	3,234
T_6	16	2	$x^8 - 3x^5 - x^4 + 3x^3 + 1$	3,421
T_5	8	1	$x^8 + 12x^6 + 36x^4 + 36x^2 + 9$	0,288
T_4	8	1	$x^8 + x^6 - 3x^4 + x^2 + 1$	0,337
T_3	8	1	$x^8 - x^4 + 1$	0,259
T_2	8	1	$x^8 - x^7 + x^5 - x^4 + x^3 - x + 1$	0,317
T_1	8	1	$x^8 + x^7 - 7x^6 - 6x^5 + 15x^4 + 10x^3 - 10x^2 - 4x + 1$	0,167
Grad 9				
T_{17}	81	3	$x^9 - 4x^8 - 2x^7 + 22x^6 - 14x^5 - 22x^4 + 20x^3 + 2x^2 - 5x + 1$	11:16:50,092
T_{16}	72	3	$x^9 - 2x^7 - 3x^6 + x^5 + x^4 - 3x^3 + x - 1$	19:31:54,390
T_{15}	72	2	$x^9 - 72x^7 + 1464x^5 - 960x^4 - 8928x^3 + 13440x^2 - 2064x - 2560$	9:42:04,287

	$\lvert T_i\rvert$	s	Beispielpolynom	Laufzeit
T_{14}	72	2	$x^9 - 12x^5 + 132x - 128$	2:56:36,155
T_{13}	54	3	$x^9 - x^6 - 2x^3 + 1$	2:43,406
T_{12}	54	2	$x^9 - 2x^8 - 4x^7 + 9x^5 + 17x^4 + 12x^3 - x^2 - 4x - 1$	34:28,519
T_{11}	54	2	$x^9 - 3x^6 + 3x^3 + 8$	1:12,470
T_{10}	54	2	$x^9 - x^7 - 2x^6 + 3x^5 + x^4 + 2x^3 - x^2 + x - 3$	42:48,080
T_9	36	2	$x^9 - 3x^8 + 3x^7 - 15x^6 + 33x^5 - 3x^4 + 24x^3 + 6x^2 - 4$	3:44,542
T_8	36	2	$x^9 - x^8 + 3x^6 + x^5 + x^4 + 3x^3 + 2x^2 + 1$	2:37,351
T_7	27	3	$x^9 - 3x^8 - 15x^7 + 51x^6 + 39x^5 - 219x^4 + 81x^3 + 204x^2 - 132x - 8$	1:45,859
T_6	27	3	$x^9 - 21x^7 - 7x^6 + 126x^5 + 42x^4 - 273x^3 - 63x^2 + 189x + 7$	2:10,973
T_5	18	2	$x^9 - 3x^6 - 3x^3 - 1$	2,397
T_4	18	2	$x^9 - 6x^6 - 16x^3 - 8$	1,760
T_3	18	2	$x^9 + x^8 + 3x^6 + 3x^3 - 3x^2 + 5x - 1$	6,935
T_2	9	1	$x^9 - 15x^7 + 4x^6 + 54x^5 - 12x^4 - 38x^3 + 9x^2 + 6x - 1$	0,968
T_1	9	1	$x^9 + x^8 - 8x^7 - 7x^6 + 21x^5 + 15x^4 - 20x^3 - 10x^2 + 5x + 1$	0,294
Grad 10				
T_8	80	4	$x^{10} - 4x^8 + 2x^6 + 5x^4 - 2x^2 - 1$	8:39:09,839
T_6	50	2	$x^{10} - x^9 + 3x^7 - 3x^6 + x^5 + 5x^4 - x^3 + 2x^2 + 3x + 1$	15:58,994
T_5	40	2	$x^{10} - 2x^8 - x^6 + 5x^4 - 5x^2 + 3$	11:50,339
T_4	20	2	$x^{10} + 22x^5 - 4$	3,623
T_3	20	2	$x^{10} - 2x^9 + 2x^8 - 2x^7 + 2x^6 - x^5 + 3x^4 - 4x^3 + x^2 + 1$	14,775
T_2	10	1	$x^{10} - 2x^8 + 7x^6 + 41x^4 + 103x^2 + 47$	2,108
T_1	10	1	$x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$	0,413
Grad 11				
T_3	55	2	$x^{11} - 33x^9 + 396x^7 - 2079x^5 + 4455x^3 - 2673x - 243$	47:02:40,389
T_2	22	2	$x^{11} - x^{10} + 5x^9 - 4x^8 + 10x^7 - 6x^6 + 11x^5 - 7x^4$ $+9x^3 - 4x^2 + 2x + 1$	7:04,509
T_1	11	1	$x^{11} + x^{10} - 10x^9 - 9x^8 + 36x^7 + 28x^6 - 56x^5 - 35x^4$ $+35x^3 + 15x^2 - 6x - 11$	29,186
Grad 12				
T_{69}	96	4	$x^{12} - 3x^{10} - 2x^8 + 9x^6 - 5x^2 + 1$	51:57:02,780
T_{68}	96	2	$x^{12} + x^{10} + 6x^8 + 3x^6 + 6x^4 + x^2 + 1$	97:53:04,176
T_{67}	96	2	$x^{12} - x^8 - x^6 - x^4 + 1$	6:42:37,892
T_{66}	96	2	$x^{12} + 6x^{10} + 12x^8 + 8x^6 - 3$	63:41:56,339
T_{65}	96	2	$x^{12} - 3x^4 + 4$	81:17:22,602
T_{64}	96	2	$x^{12} - x^8 + 9x^4 - 1$	62:29:53,912
T_{63}	96	2	$x^{12} - 6x^{10} + 104x^6 + 93x^4 + 18x^2 + 4$	78:43:51,349
T_{62}	96	2	$x^{12} + 6x^{10} - 104x^6 + 93x^4 - 18x^2 + 4$	89:12:26,371
T_{61}	96	3	$x^{12} - 3x^4 - 1$	18:49:41,319
T_{60}	96	3	$x^{12} - 14x^8 - 7x^4 + 4$	77:08:26,132
T_{59}	96	3	$x^{12} - 6x^{10} + 6x^8 - 4x^6 - 3x^4 + 3$	32:34:10,772
T_{58}	96	4	$x^{12} - 12x^8 - 14x^6 + 9x^4 + 12x^2 + 1$	53:21:48,697
T_{57}	96	3	$x^{12} - 69x^{10} - 2091x^8 - 7571x^6 + 134691x^4 + 960267x^2 + 1545049$	27:09:45,061
T_{56}	96	3	$x^{12} - 2x^{10} + x^6 - 2x^2 + 1$	43:31:04,459
T_{55}	96	3	$x^{12} - 30x^{10} + 348x^8 - 1960x^6 + 5505x^4 - 7050x^2 + 3025$	38:47:40,447
T_{54}	96	3	$x^{12} - 6x^8 + 9x^4 + 12$	3:08:56,192

	$\lvert T_i\rvert$	s	Beispielpolynom	Laufzeit
T_{53}	96	3	$x^{12}+2x^8-16x^6+4x^4+8$	21:29:19,687
T_{52}	96	4	$x^{12}+12x^4-12$	3:08:00,669
T_{51}	96	4	$x^{12}+6x^8+9x^4+3$	8:12:12,529
T_{50}	96	4	$x^{12}-3x^4+6$	47:34:53,017
T_{49}	96	2	$x^{12}+3x^8-4x^6-3x^4-1$	90:21:39,951
T_{48}	96	3	$x^{12}-x^8+3x^4+1$	3:24:33,654
T_{47}	72	3	$x^{12}-6x^{10}+20x^9-72x^7+128x^6-96x^5+45x^4$ $-8x^3-18x^2+12x-2$	23:44:43,872
T_{46}	72	3	$x^{12}+12x^{10}-19x^9+54x^8-171x^7+169x^6-513x^5$ $+447x^4-573x^3+549x^2-180x+16$	7:55:01,010
T_{45}	72	3	$x^{12}-3x^9-18x^8-24x^6-9x^5+69x^4-x^3+3x-1$	19:53:34,759
T_{44}	72	2	$x^{12}-6x^6-10x^3-6$	20:36,003
T_{43}	72	2	$x^{12}-6x^9+10x^6+4x^3+2$	20:57,049
T_{42}	72	2	$x^{12}-x^6+7$	5:16:13,554
T_{41}	72	3	$x^{12}-x^9-9x^6-x^3+1$	4:46:03,294
T_{40}	72	3	$x^{12}-7x^{10}+24x^8-36x^6+24x^4+13x^2+1$	40:36:38,905
T_{39}	72	3	$x^{12}-5x^3+5$	24:48,984
T_{38}	72	2	$x^{12}+x^6-3$	1:17:39,982
T_{37}	72	3	$x^{12}+x^6+9$	14:52,306
T_{36}	72	2	$x^{12}-x^9-x^6-x^3+1$	14:33,138
T_{35}	72	2	$x^{12}-x^9-x^6-x^3+1$	14:38,622
T_{34}	72	3	$x^{12}+12x^{10}+54x^8+108x^6+81x^4+16$	4:57:41,016
T_{32}	48	2	$x^{12}+7x^{10}-x^8-23x^6-x^4+7x^2+1$	3:33,938
T_{31}	48	2	$x^{12}-30x^{10}+343x^8-1860x^6+4760x^4-4600x^2+225$	54:01,975
T_{30}	48	3	$x^{12}-7x^{10}-14x^8+115x^6-70x^4-175x^2+125$	26:25,400
T_{29}	48	3	$x^{12}-45x^8+50x^6+225x^4-375x^2+125$	10:44,144
T_{28}	48	2	$x^{12}+x^{11}-x^{10}-2x^9-x^8+4x^7+2x^6-7x^5+5x^4$ $+x^3-3x^2+1$	7:36,610
T_{27}	48	2	$x^{12}+12x^{10}+68x^8+220x^6+392x^4+360x^2+148$	1:30:22,678
T_{26}	48	2	$x^{12}-9x^8-8x^6-9x^4+1$	2:43,264
T_{25}	48	3	$x^{12}+5x^8+6x^4+1$	3:12,624
T_{24}	48	2	$x^{12}+4x^{10}+7x^8+4x^6-x^4-2x^2+1$	41:02,399
T_{23}	48	2	$x^{12}-4x^4+4$	1:00,810
T_{22}	48	2	$x^{12}-5x^{10}+7x^8-6x^7-17x^6-6x^5+7x^4-5x^2+1$	27:23,796
T_{21}	48	3	$x^{12}+3x^8-4x^6+3x^4+1$	14:43,692
T_{20}	36	2	$x^{12}-4x^9+72x^8-84x^7+236x^6-144x^5+324x^4$ $-192x^3+72x^2+8$	21:42,525
T_{19}	36	2	$x^{12}-2x^{11}+4x^{10}+x^9+5x^8+8x^7+53x^6+44x^5$ $+59x^4+19x^3+13x^2+5x+1$	11:33,085
T_{18}	36	2	$x^{12}-4x^6+16$	28,297
T_{17}	36	2	$x^{12}+4x^8+4x^6+5x^4+12x^2+2$	7:33,475
T_{16}	36	2	$x^{12}-x^6+4$	30,861
T_{15}	24	2	$x^{12}+5x^{11}+9x^{10}+3x^9-9x^8-6x^7+21x^6+50x^5+57x^4$ $+41x^3+20x^2+6x+1$	58,949
T_{14}	24	2	$x^{12}-9x^6+27$	9,829
T_{13}	24	2	$x^{12}-10x^9-12x^6-4x^3-2$	6,601
T_{12}	24	2	$x^{12}+x^6-27$	8,835
T_{11}	24	2	$x^{12}+10x^6+5$	5,085

	$\lvert T_i\rvert$	s	Beispielpolynom	Laufzeit
T_{10}	24	2	$x^{12} - 4x^{11} + 4x^{10} + 4x^9 - 8x^8 - 4x^7 + 6x^6 + 8x^5 + x^4$ $-8x^3 - 2x^2 + 4x + 2$	44,831
T_9	24	2	$x^{12} + 3x^8 + 4x^6 + 3x^4 + 1$	8,368
T_8	24	2	$x^{12} - 6x^{10} - 8x^9 + 9x^8 + 12x^7 - 20x^6 + 9x^4 - 24x^3 - 4$	2:58,866
T_7	24	2	$x^{12} + 4x^{10} - x^8 - x^4 + 4x^2 + 1$	8,357
T_6	24	2	$x^{12} + 2x^{10} - 6x^8 + 2x^6 - 6x^4 + 2x^2 + 1$	22,183
T_5	12	1	$x^{12} - 80x^{10} + 1820x^8 - 13680x^6 + 29860x^4 - 2720x^2 + 32$	2,798
T_4	12	1	$x^{12} + 6x^8 + 26x^6 - 63x^4 + 162x^2 + 81$	3,779
T_3	12	1	$x^{12} + 36$	0,512
T_2	12	1	$x^{12} - x^6 + 1$	0,515
T_1	12	1	$x^{12} - x^{11} + x^{10} - x^9 + x^8 - x^7 + x^6 - x^5 + x^4 - x^3 + x^2 - x + 1$	0,427
Grad 13				
T_5	78	2	$x^{13} - 3x^{12} + 8x^{11} - 11x^{10} + 17x^9 - 19x^8 + 30x^7 + 3x^6$ $-43x^5 + 95x^4 - 24x^3 - 9x^2 + 38x + 25$	–
T_4	52	2	$x^{13} + 13x^{10} - 26x^8 + 13x^7 + 52x^6 - 39x^4 + 26x^2 + 13x + 2$	–
T_3	39	2	$x^{13} - 39x^{11} + 468x^9 - 1989x^7 - 507x^6 + 2886x^5 + 1443x^4$ $-624x^3 - 234x^2 + 3$	–
T_2	26	2	$x^{13} - 6x^{12} + 10x^{11} - 16x^{10} + 22x^9 - 19x^8 + 11x^7 - 5x^6$ $-x^5 + 5x^4 - 4x^3 + 2x - 1$	51:20,143
T_1	13	1	$x^{13} - x^{12} - 24x^{11} + 19x^{10} + 190x^9 - 116x^8 - 601x^7 + 246x^6$ $+738x^5 - 215x^4 - 291x^3 + 68x^2 + 10x - 1$	13:32,327
Grad 14				
T_8	98	2	$x^{14} + 28x^{11} + 28x^{10} - 28x^9 + 140x^8 + 360x^7 + 147x^6 + 196x^5$ $+336x^4 - 546x^3 - 532x^2 + 896x + 823$	–
T_7	84	2	$x^{14} - x^{13} + 4x^{12} - 5x^{11} + 11x^{10} - 14x^9 + 21x^8 - 33x^7 + 30x^6$ $-29x^5 + 29x^4 - 8x^3 + 13x^2 - x + 1$	–
T_6	56	2	$x^{14} + 13x^{12} + 31x^{10} - 9x^8 - 54x^6 - 3x^4 + 23x^2 - 1$	1:17:29.895
T_5	42	3	$x^{14} - 6x^{13} + 18x^{12} - 18x^{11} + 12x^{10} - 54x^9 + 270x^8 - 202x^7$ $+244x^5 + 390x^4 + 128x^3 + 16x^2 - 8x + 2$	7:55:01,010
T_4	42	3	$x^{14} + 4x^{13} + 4x^{12} + 4x^{11} + 24x^{10} + 33x^9 - 9x^8 - 3x^7 + 67x^6$ $+22x^5 - 72x^4 - 42x^3 + 7x^2 + 10x + 9$	4:34:23,931
T_3	28	2	$x^{14} + 2x^{13} + 5x^{12} + 2x^{10} - 4x^9 + 2x^8 - 4x^7 + 3x^6 - 4x^5 + 3x^4$ $-x^3 + 2x^2 - x + 1$	4:30,533
T_2	14	1	$x^{14} + 8x^{12} + 22x^{10} + 8x^8 - 55x^6 - 48x^4 + 64x^2 + 71$	30,620
T_1	14	1	$x^{14} - x^{13} - 13x^{12} + 12x^{11} + 66x^{10} - 55x^9 - 165x^8 + 120x^7$ $+210x^6 - 126x^5 - 126x^4 + 56x^3 + 28x^2 - 7x - 1$	13,823
Grad 15				
T_9	75	2	$x^{15} - 470x^{13} - 305x^{12} + 71840x^{11} + 85357x^{10} - 4292700x^9 - 3714805x^8$ $+119761820x^7 + 25284495x^6 - 1542190154x^5 + 717324725x^4$ $+7178878600x^3 - 5452953875x^2 - 7998223215x + 4461221029$	98:53:49,110
T_8	60	2	$x^{15} + 6x^{14} + 9x^{13} - 13x^{12} - 52x^{11} - 78x^{10} - 78x^9 - 26x^8$ $+39x^7 + 78x^6 + 91x^5 + 65x^4 + 39x^3 + 16x^2 + 5x + 1$	6:47,859
T_7	60	2	$x^{15} - 2x^{14} + 2x^{13} - 2x^{11} + 6x^{10} + 7x^9 + 2x^8 + x^7 + 5x^6 - 3x^5$ $-3x^4 + 6x^3 + 2x^2 + 1$	15:16,223
T_6	60	2	$x^{15} - 30x^{10} - 3708x^5 - 2$	12:48,723

	$\lvert T_i\rvert$	s	Beispielpolynom	Laufzeit
T_4	30	2	$x^{15}-7x^{14}+19x^{13}-16x^{12}-15x^{11}+10x^{10}+60x^9$ $-102x^8+81x^7-42x^6+12x^5+11x^4-21x^3+14x^2-5x+1$	23:58,598
T_3	30	2	$x^{15}-5x^{13}-8x^{12}-20x^{11}-8x^{10}+9x^9+x^8$ $-4x^7+30x^6-55x^5-4x^4+7x^3+8x^2+4x+1$	19:22,097
T_2	30	2	$x^{15}+x^{14}-10x^{13}+3x^{12}+28x^{11}-39x^{10}+29x^9-42x^8$ $+43x^7+19x^6-39x^5+103x^4-82x^3+40x^2-9x+1$	32:41,354
T_1	15	1	$x^{15}-x^{14}-14x^{13}+13x^{12}+78x^{11}-66x^{10}-220x^9+165x^8$ $+330x^7-210x^6-252x^5+126x^4+84x^3-28x^2-8x+1$	19,046

In den Abschnitten 6.1.2 und 6.1.3 wurde angesprochen, dass die Realisierung des Kreisteilungskörpers im Algorithmus deutliche Auswirkungen auf dessen Laufzeit hat. Die Konsequenzen werden hier für die 281 Polynome vom Grad 5 aus [20] mit der affinen Gruppe F_{20} (vgl. Beispiel 2.4.7) als Galoisgruppe vorgestellt. Die Primfaktoren in der Ordnung der Galoisgruppe $|G_f| = 20$ sind 2 und 5. Entscheidend ist daher, wie sich $\phi_5(x) = x^4+x^3+x^2+x+1$ über dem Zerfällungskörper $\mathbb{Q}_f$ verhält. Dabei treten alle drei wesentlich verschiedenen Umsetzungen des Kreisteilungskörpers auf:

1. Ist ϕ_5 auch über $\mathbb{Q}_f$ irreduzibel, dann wird für die primitive 5-te Einheitswurzel ζ_5 die in GAP vorliegende Darstellung verwendet. In $\widetilde{\mathbb{Q}}_f$ liegen dann (20×20)-Matrizen mit Einträgen aus $\mathbb{Q}_5$.
2. Liefert das Faktorisieren von ϕ_5 über $\mathbb{Q}_f$ zwei quadratische Faktoren, dann startet der Algorithmus mit $\widetilde{\mathbb{Q}} = \mathbb{Q}_5$ als Grundkörper neu. Man erhält $[\widetilde{\mathbb{Q}}_f : \widetilde{\mathbb{Q}}] = 10$, was insgesamt zu Matrizen der Dimension 40 mit Einträgen aus $\mathbb{Q}$ führt.
3. Zerfällt ϕ_5 in Linearfaktoren, so ist $\mathbb{Q}_5 \supset \mathbb{Q}_f$ und ζ_5 ist als Matrix vorhanden. Damit gilt $\widetilde{\mathbb{Q}}_f = \mathbb{Q}_f$, so dass in einem Matrizenkörper der Dimension 20 über $\mathbb{Q}$ gerechnet wird.

# Faktoren von ϕ_5	# Polynome	durchschnittliche Laufzeit
1	81	20,156
2	183	3:50,375
4	17	3,377

6.2.1 Bemerkung: Es sei noch angemerkt, dass der in diesem Beispiel häufigste Fall, der ja gerade der langsamste ist, bei den meisten der weiter oben angeführten transitiven Gruppen gar nicht auftreten kann. Zwei einfache Argumente schränken die möglichen Kandidaten bereits stark ein. Zunächst muss ein Primteiler p von h (dem Produkt der Primfaktoren in $|G_f|$) existieren, der größer als 3 ist, damit ϕ_p in nicht-lineare Faktoren zerfallen kann. Desweiteren muss $\mathrm{ggT}(p-1,h) \neq 1$ gelten, um dies auch über $\mathbb{Q}_f$ zu ermöglichen. Wegen der Grade der Körpererweiterungen gilt ansonsten $\mathbb{Q}_f \cap \mathbb{Q}_p = \mathbb{Q}$.

Kapitel 7

Beispiele

Der Ablauf des Algorithmus soll an drei Beispielen verdeutlicht werden. Auch wenn die Anwendung der Implementation erst für Polynome der Grade 5 und höher zweckmäßig ist, werden hier der Einfachheit halber zunächst zwei Polynome vom Grad 3 angeführt. Es existieren zwei transitive Untergruppen der S_3. Dies führt zu verschiedenen Möglichkeiten für die Galoisgruppe eines kubischen Polynoms. Betrachtet werden zwei Polynome, deren Galoisgruppe über $\mathbb{Q}$ die symmetrische Gruppe S_3 ist. Über dem Erweiterungskörper von $\mathbb{Q}$, der die sechsten Einheitswurzeln enthält, ist die Galoisgruppe dagegen in einem Fall die A_3.

Danach wird das Polynom $f(x) = x^5 - x^3 - 2x^2 - 2x + 1$ untersucht, bei dem die Anwendung des Algorithmus notwendig ist und die Berechnungen noch darstellbar sind.

Es wird die im Abschnitt 5.5 aufgeführte Notation benutzt.

7.1 $f(x) = x^3 + 2x^2 - 5$

Die drei Nullstellen $\alpha_1, \alpha_2, \alpha_3$ von $f(x) = x^3 + 2x^2 - 5$ sollen als Wurzelausdrücke dargestellt werden. Als erstes wird festgestellt, dass f tatsächlich irreduzibel ist.

Da die Diskriminante von f kein Quadrat ist, muss die Galoisgruppe die S_3 sein. Als nächstes stellt der Algorithmus die Auflösbarkeit der Galoisgruppe fest und berechnet die Kompositionsreihe

$$S_3 \rhd A_3 \rhd \{1\}. \tag{7.1}$$

Nun wird der Zerfällungskörper erzeugt. Als erstes entsteht $L_1 \cong \mathbb{Q}[x]/(f)$. Die adjungierte Nullstelle wird mit α_1 bezeichnet. Für das primitive Element gilt $\gamma_1 = \alpha_1$. Über

L_1 zerfällt f folgendermaßen:

$$f(x) = (x - \alpha_1)(x^2 + (2 + \alpha_1)x + (\alpha_1^2 + 2\alpha_1)).$$

Sei g der zweite Faktor, so wird zur Konstruktion von L_2 der Quotientenkörper $L_1[x]/(g)$ gebildet. Es ist $L_2 = L_1(\alpha_2) = \mathbb{Q}(\gamma_2)$, wobei $\gamma_2 = 2\alpha_1 + \alpha_2$ ist. Mit L_2 ist der Zerfällungskörper $\mathbb{Q}_f$ erreicht, da nun die drei Nullstellen α_1, α_2 und $-2 - \alpha_1 - \alpha_2$ in L_2 enthalten sind. Es ist $\mathbb{Q}_f = \mathbb{Q}(\gamma)$ mit $\gamma = \gamma_2$.

Im nächsten Schritt werden primitive Elemente β_i für die Glieder der Körperkette, die zur Kompositionsreihe (7.1) korrespondiert, gesucht. Für $i = 1$ werden die Koeffizienten des Polynoms

$$j_{A_3}(x) = \prod_{\sigma \in A_3} (x - \gamma^\sigma) = x^3 + 6x^2 + 8x - (15 + 8\alpha_1 + 4\alpha_1^2 + 8\alpha_1\alpha_2 + 6\alpha_1^2\alpha_2)$$

betrachtet. Somit ist $\beta_1 = 15 + 8\alpha_1 + 4\alpha_1^2 + 8\alpha_1\alpha_2 + 6\alpha_1^2\alpha_2$. Weiter ist $\beta_2 = \gamma$. An die Körperkette wird nun eine primitive sechste Einheitswurzel ζ_6 adjungiert.

Aus den β_i werden mit Hilfe der Lagrangesche Resolvente zyklische Elemente ermittelt, die über dem direkten Unterkörper eine reine Gleichung erfüllen. Für $i = 1$ ist die benötigte Faktorgruppe $S_3/A_3 = \langle (12)A_3 \rangle$. Damit berechnet sich ω_1 zu

$$\omega_1 = (15 + 8\alpha_1 + 4\alpha_1^2 + 8\alpha_1\alpha_2 + 6\alpha_1^2\alpha_2) + (-1)(15 + 8\alpha_1 + 4\alpha_1^2 + 8\alpha_1\alpha_2 + 6\alpha_1^2\alpha_2)^{(12)}.$$

Das Minimalpolynom von ω_1 ist $x^2 + 515$.

Für $i = 2$ ist die Faktorgruppe $A_3/\{1\} = \langle (123) \rangle$. Somit ergibt sich:

$$\omega_2 = \gamma + \zeta_6^2\gamma^{(132)} + \zeta_6^4\gamma^{(123)}.$$

(Ergäbe diese Rechnung 0, so wäre γ durch γ^2 zu ersetzen.) Das Minimalpolynom von ω_2 ist $x^3 - \frac{27}{2}\beta_1 - \frac{375}{2}(\zeta_3^2 - \zeta_3^4) = x^3 - \frac{27}{2}\beta_1 - \frac{375}{2}\sqrt{-3}$. Die zyklischen Erweiterungen ergeben sich also durch die Elemente

$$\begin{aligned} \omega_1 &= \sqrt{-515} \\ \omega_2 &= \sqrt[3]{\frac{357}{2}\sqrt{-3} + \frac{27}{2}\sqrt{-515}}. \end{aligned}$$

Man beachte, dass hier die irreduzible Radikaldarstellung (siehe Tabelle 4.1) für die primitive dritte Einheitswurzel eingesetzt wurde.

Eine Basis von $\widetilde{\mathbb{Q}}_f/\widetilde{\mathbb{Q}}$ ist durch $\{1, \omega_1, \omega_2, \omega_1\omega_2, \omega_2^2, \omega_1\omega_2^2\}$ gegeben. Drückt man die Nullstellen von f in dieser Basis aus, erhält man drei Darstellungen durch irreduzible Radikale, von denen eine

$$-\frac{2}{3} + \frac{1}{9}\sqrt{-3}\sqrt[3]{\frac{357}{2}\sqrt{-3} + \frac{27}{2}\sqrt{-515}} - \left(\frac{119}{288} + \frac{1}{96}\sqrt{-515}\sqrt{-3}\right)\sqrt[3]{\frac{357}{2}\sqrt{-3} + \frac{27}{2}\sqrt{-515}}^2$$

ist.

7.2 $f(x) = x^3 - 2$

In diesem Beispiel wird das Polynom $f(x) = x^3 - 2$ betrachtet. Dessen Nullstellen sind offenbar $\sqrt[3]{2}, \zeta_3\sqrt[3]{2}$ und $\zeta_3^2\sqrt[3]{2}$. Daraus wird klar, dass die dritten Einheitswurzeln im Zerfällungskörper liegen.

Da die Galoisgruppe von f die S_3 ist, wird nach Feststellung der Irreduziblität, wieder deren einzige Kompositionsreihe, $S_3 \rhd A_3 \rhd \{1\}$, bestimmt.

Über $L_1 = \mathbb{Q}(\alpha_1)$ erhält man durch Faktorisieren

$$f(x) = (x - \alpha_1)(x^2 + \alpha_1 x + \alpha_1^2).$$

Für $\mathbb{Q}_f = L_2$ ist $\gamma = 2\alpha_1 + \alpha_2$ ein primitives Element, und die dritte Nullstelle von f ist $-(\alpha_1 + \alpha_2)$.

Formal weitergeführt bestimmt der Algorithmus nun ein primitives Element für K_1, den Fixkörper zu A_3, aus den Koeffizienten von

$$j_{A_3}(x) = \prod_{\sigma \in A_3} (x - \gamma^\sigma) = x^3 - (6 + 6\alpha_1^2\alpha_2).$$

Es gilt also $K_1 = \mathbb{Q}(6 + 6\alpha_1^2\alpha_2)$. Nach Hinzufügen der 6-ten Einheitswurzeln behält die entsprechende Beziehung $\widetilde{K}_1 = \widetilde{\mathbb{Q}}(6 + 6\alpha_1^2\alpha_2)$ ihre Gültigkeit. Nun ist die Lagrangesche Resolvente zu berechnen, wobei als Repräsentant des Erzeugers der Faktorgruppe S_3/A_3 wieder die Permutation (12) verwendet wird.

$$\begin{aligned}
\omega_1 = (-1, 6 + 6\alpha_1^2\alpha_2) &= 6 + 6\alpha_1^2\alpha_2 - (6 + 6\alpha_1^2\alpha_2)^{(12)} \\
&= 6 + 6\alpha_1^2\alpha_2 - 6 - 6\alpha_2^2\alpha_1 \\
&= 6 + 6\alpha_1^2\alpha_2 - 6 + 6(\alpha_1\alpha_2 + \alpha_1^2)\alpha_1 \\
&= 12\alpha_1^2\alpha_2 + 6\alpha_1^3 \\
&= 12 + 12\alpha_1^2\alpha_2.
\end{aligned}$$

In der Tat wird die quadratische, reine Gleichung $x^2 + 432$ nun von ω_1 erfüllt. Wegen $432 = 3 \cdot 12^2$ kann man als endgültiges ω_1 vereinfachend $1 + \alpha_1^2\alpha_2$ wählen.

Die Mühe, ω_2 mit der Lagrangeschen Resolvente zu berechnen, kann man sich in diesem einfachen Beispiel sparen. Es ist ja schon $j_{A_3}(x) = 0$ eine reine Gleichung aus $\widetilde{K}[x]$ mit γ als Nullstelle. Daher ist $\omega_2 = 2\alpha_1 + \alpha_2$.

Da $\widetilde{K}_1 = \widetilde{\mathbb{Q}}$ gilt, ist $\widetilde{p}_1 = 1$ und eine $\widetilde{\mathbb{Q}}$-Basis von $\widetilde{\mathbb{Q}}_f$ schon durch $1, \gamma, \gamma^2$ gegeben. Als Wurzelausdruck bekommt man auf diesem Wege

$$\frac{1}{3}\sqrt{-3}\sqrt[3]{6\sqrt{-3}}.$$

Dass das Radikal $\sqrt[3]{2}$ dieselben Elemente repräsentiert, verdeutlicht die Bedeutung, die einer Vereinfachung der Radikaldarstellung zukommt.

7.3 $f(x) = x^5 - x^3 - 2x^2 - 2x - 1$

In den beiden vorangegangenen Beispielen wurden zwei kubische Polynome untersucht, so dass die Nullstellen auch mit den Cardanoschen Formeln 4.1.2 durch Radikale ausgedrückt werden konnten. Mit $f(x) = x^5 - x^3 - 2x^2 - 2x - 1$ wird nun ein Polynom behandelt, das als irreduzibles Polynom vom Grad 5 nicht durch allgemeine Formeln auflösbar ist. Das Bestimmen der Nullstellen mit dem vorgestellten Algorithmus verläuft wie folgt:

Der Isomorphietyp der Galoisgruppe G_f ist D_5. Damit gilt $[\mathbb{Q}_f : \mathbb{Q}] = 10$, was schon einen Hinweis darauf gibt, wie die Konstruktion des Zerfällungskörpers abläuft. In der Erweiterung $L_1 \cong \mathbb{Q}[x]/(f) \cong \mathbb{Q}(\alpha_1)$ erhält man die irreduziblen Faktoren

$$\begin{aligned}
&x - \alpha_1,\\
&x^2 + (-2\alpha_1^4 + \alpha_1^3 + 2\alpha_1^2 + 3\alpha_1 + 2)x - \alpha_1^4 + \alpha_1^3 + \alpha_1^2 + \alpha_1,\\
&\text{und}\quad x^2 + (2\alpha_1^4 - \alpha_1^3 - 2\alpha_1^2 - 2\alpha_1 - 2)x - \alpha_1^4 + \alpha_1^3 + 2\alpha_1^2 + 1.
\end{aligned}$$

Durch Adjunktion einer Nullstelle α_2 des letzten Faktors entsteht ein Körper vom Grad 10 über $\mathbb{Q}$, der deshalb der Zerfällungskörper von f ist. Die drei weiteren Nullstellen von f in $\mathbb{Q}_f = \mathbb{Q}(\gamma)$ mit $\gamma = 2\alpha_1 + \alpha_2$ sind

$$\begin{aligned}
\alpha_3 &= -1 - \alpha_1 - \alpha_1^2 - \alpha_1^3 + \alpha_1^4 + \alpha_2 + \alpha_1\alpha_2 - \alpha_1^3\alpha_2,\\
\alpha_4 &= -1 - 2\alpha_1 - \alpha_1^2 + \alpha_1^4 - \alpha_2 - \alpha_1\alpha_2 + \alpha_1^3\alpha_2\\
\text{und}\quad \alpha_5 &= 2 + 2\alpha_1 + 2\alpha_1^2 + \alpha_1^3 - 2\alpha_1^4 - \alpha_2.
\end{aligned}$$

Da mehrere Konjugierte zur Galoisgruppe D_5 in der symmetrischen Gruppe vom Grad 5 existieren, ist es nun nötig, die Permutationsgruppe zur gewählten Nummerierung zu bestimmen. Dazu werden die Nullstellen, die im primitiven Element auftauchen, injektiv auf die Menge aller Nullstellen abgebildet. Wenn sich diese Abbildung in $\mathbb{Q}_f$ homomorph zu einer Bijektion auf den Nullstellen fortsetzen lässt, liegt ein Element der Galoisgruppe vor. Bildet man das Tupel (α_1, α_2) auf (α_2, α_1) ab, lässt sich dazu eine automorphe Fortsetzung in $\mathbb{Q}_f$ finden. Diese entspricht der Permutation $(12)(45)$. Sucht man mit einer gewissen Systematik weiter, ist $(\alpha_1, \alpha_2) \mapsto (\alpha_5, \alpha_1)$ die nächste Abbildung, die sich zu einem Element der Galoisgruppe fortsetzen lässt. Man verifiziert mittels der Gruppenordnung, dass $G_f = \langle (12)(45), (15)(34) \rangle$ ist. Dies kann hier auch sehr einfach ohne

Computerhilfe geschehen. Da die Gruppe, die von den beiden ermittelten Permutationen erzeugt wird, offensichtlich nicht zyklisch ist, kann keine echte Untergruppe der Galoisgruppe vorliegen.

Als eine Kompositionsreihe wird

$$G_f = G_1 \rhd G_2 = \langle (15423) \rangle \rhd G_3 = \{1\}$$

berechnet, wozu eine korrespondierende Körperkette zu bestimmen ist. Da die Fixkörper von G_1 und G_3 schon bekannt sind, bleibt noch $K_2 = \mathrm{Fix}_{\mathbb{Q}_f}(G_2)$ zu ermitteln. Unter den Koeffizienten von

$$j_{G_2}(x) = \prod_{\sigma \in G_2} x - \gamma^\sigma$$

tauchen außer ganzen Zahlen nur Vielfache von

$$\beta_1 = 6 + 2\alpha_1 + \alpha_1^2 + 2\alpha_1^3 - \alpha_1^4 + \alpha_2 + 2\alpha_1\alpha_2 + 5\alpha_1^2\alpha_2 - 2\alpha_1^3\alpha_2$$

auf. Mit $\beta_2 = 2\alpha_1 + \alpha_2$ hat man also die Körperkette

$$\mathbb{Q} = K_1 \subset K_1(\beta_1) = K_2 \subset K_2(\beta_2) = K_3 = \mathbb{Q}_f$$

vorliegen. Nach Adjunktion einer primitiven zehnten Einheitswurzel ist $[\widetilde{\mathbb{Q}}_f : \widetilde{\mathbb{Q}}] = 10$, so dass die Relativgrade in der Körperkette erhalten bleiben.

Um den Zerfällungskörper als Radikalerweiterung darzustellen, wird für jede Erweiterung in der Körperkette ein primitives Element gesucht, das Nullstelle einer reinen Gleichung ist. Dazu werden die Faktoren der Kompositionsreihe benötigt. Es sind $G_1/G_2 = \langle (24)(35)G_2 \rangle$ und $G_2/G_3 = G_2 = \langle (15423) \rangle$. Mit der primitiven fünften Einheitswurzel $\zeta_5 = \zeta_{10}^2$ ergeben sich die beiden Lagrangeschen Resolventen

$$\begin{aligned} (-1, \beta_1) &= \beta_1 - \beta_1^{(24)(35)} = 2\beta_1 \\ (\zeta_5, \beta_2) &= \beta_2 + \zeta_5\beta_2^{(15423)} + \zeta_5^2\beta_2^{(14352)} + \zeta_5^3\beta^{(12534)} + \zeta_5^4\beta^{(13245)} \end{aligned}$$

und deren jeweilige Potenzen

$$\begin{aligned} a_1 &= (-1, \beta_1)^2 = 4\beta_1^2 = -47 \\ a_2 &= (\zeta_5, \beta_2)^5 = \frac{416}{125}\zeta_5 - \frac{377}{250}\zeta_5^2 + \frac{923}{250}\zeta_5^3 + \frac{91}{125}\zeta_5^4 \\ &\quad + (-\frac{339}{625}\zeta_5 - \frac{409}{1250}\zeta_5^2 - \frac{91}{1250}\zeta_5^3 - \frac{486}{625}\zeta_5^4)\sqrt{-47}. \end{aligned}$$

Damit ist $\widetilde{\mathbb{Q}}_f = \mathbb{Q}_f(\zeta_5) = \widetilde{\mathbb{Q}}(\sqrt[2]{a_2}, \sqrt[5]{a_2})$. Dessen $\widetilde{\mathbb{Q}}$-Basis ist gegeben durch

$$\{1, \sqrt[5]{a_2}, \sqrt[5]{a_2}^2, \sqrt[5]{a_2}^3, \sqrt[5]{a_2}^4, \sqrt[2]{a_2}, \sqrt[2]{a_2}\sqrt[5]{a_2}, \sqrt[2]{a_2}\sqrt[5]{a_2}^2, \sqrt[2]{a_2}\sqrt[5]{a_2}^3, \sqrt[2]{a_2}\sqrt[5]{a_2}^4\}.$$

Für jede Nullstelle von f ist zum Abschluss der Berechnungen ein lineares Gleichungssystem zu lösen. Eine Radikaldarstellung für die Nullstellen von f erhält man aus der Lösung für α_1:

$$\begin{aligned}
\alpha_1 \;=\; & (-\frac{4}{11}\zeta_5 - \frac{5}{11}\zeta_5^2 - \frac{8}{11}\zeta_5^3 - \frac{6}{11}\zeta_5^4)\sqrt[5]{a_2} \\
& +(-\frac{4275}{242}\zeta_5 + \frac{445}{242}\zeta_5^2 - \frac{1470}{121}\zeta_5^3 - \frac{2205}{242}\zeta_5^4)\sqrt[5]{a_2}^2 \\
& +(-\frac{321}{242}\zeta_5 - \frac{437}{242}\zeta_5^2 + \frac{31}{121}\zeta_5^3 - \frac{619}{242}\zeta_5^4)\sqrt[2]{a_2}\sqrt[5]{a_2}^2 \\
& +(\frac{100105}{2662}\zeta_5 - \frac{22430}{1331}\zeta_5^2 + \frac{40540}{1331}\zeta_5^3 + \frac{2575}{1331}\zeta_5^4)\sqrt[5]{a_2}^3 \\
& +(\frac{16875}{2662}\zeta_5 + \frac{6525}{1331}\zeta_5^2 + \frac{2300}{1331}\zeta_5^3 + \frac{10800}{1331}\zeta_5^4)\sqrt[2]{a_2}\sqrt[5]{a_2}^3 \\
& +(-\frac{4654000}{14641}\zeta_5 + \frac{15266875}{29282}\zeta_5^2 - \frac{7609875}{14641}\zeta_5^3 + \frac{8935875}{29282}\zeta_5^4)\sqrt[5]{a_2}^4 \\
& +(-\frac{2083550}{14641}\zeta_5 - \frac{1564575}{29282}\zeta_5^2 - \frac{759575}{14641}\zeta_5^3 - \frac{4171925}{29282}\zeta_5^4)\sqrt[2]{a_2}\sqrt[5]{a_2}^4.
\end{aligned}$$

Kapitel 8

Fazit und Ausblick

Mehr als 150 Jahre nach der theoretischen Lösung des Problems der Auflösbarkeit von Polynomgleichungen ist es möglich, diese Lösung praktisch zu nutzen. Darin liegt das Hauptresultat der Arbeit.

Dabei hat sich die Grundidee der untersuchten Methode seit Galois nicht geändert. Damit kommt der ständigen Verbesserung der einzelnen im Algorithmus vorkommenden Schritte eine entscheidende Bedeutung zu. Für viele davon sind die Berechnungsmöglichkeiten so weit fortgeschritten, dass an ihnen die Behandlung weit komplizierterer Beispiele als hier geschehen nicht scheitern würde. Daran trägt die Weiterentwicklung der Computertechnik einen wesentlichen Anteil.

Auch aus dieser Arbeit können neue Erkenntnisse mitgenommen werden. Gerade bei der Bestimmung der Galoisgruppe ergeben sich wegen des erst vor kurzem verbesserten Faktorisierungsalgorithmus neue Möglichkeiten, alte Ansätze zu nutzen. Die Berechnung des Zerfällungskörpers, und darauf aufbauend der Galoisgruppe eines Polynoms, ist für kleine Grade der Erweiterung durchaus effektiv. Dies macht sich gegenüber anderen Methoden zur Berechnung der Galoisgruppe positiv bemerkbar, wenn deren Index in der symmetrischen Gruppe relativ groß ist. Herkömmliche Methoden sind dagegen besonders schnell, wenn der Index klein ist. Dies alles scheint einen Ansatz, der zwei Methoden geschickt kombiniert, sehr vielversprechend zu machen.

Die Vereinfachung der Ausgabe sollte bei weiterer Beschäftigung mit dem Thema am ehesten als nächstes betrachtet werden. Eine weitere Verbesserung des Algorithmus bringt für die Darstellung nicht viel, solange letztere nicht halbwegs überschaubar bleibt. Ansätze dazu finden sich bei Landau [21] sowie Horng und Huang [16]. Eines der auftretenden Probleme bei der Vereinfachung liegt im Rechnen mit Wurzelausdrücken. Auf den ersten Blick wird wohl jeder die Richtigkeit von $\sqrt{2}\sqrt{3}+\sqrt{6}=2\sqrt{6}$ bestätigen. Bei genauerer Überlegung fällt jedoch auf, dass die linke Seite der Gleichung bei ent-

sprechender Wahl der Wurzeln auch den Wert 0 annehmen kann. Daher wird versucht, einen Wurzelausdruck durch andere Vorgehensweisen einfacher darzustellen, ohne die Genauigkeit der Lösungen zu gefährden.

Ansonsten liegen Ansatzpunkte für weitere Verbesserungen bei den Schwachstellen des Algorithmus (siehe Abbschnitt 6.1.3). Statt eine Beschleunigung der Berechnungen anzustreben, könnte man versuchen, alternative Methoden zu verwenden. Ließen sich mit einer anderen Darstellung des Zerfällungskörpers alle weiteren, notwendigen Berechnungen ausführen, könnte man beispielsweise die Bestimmung eines primitiven Elements umgehen.

Literaturverzeichnis

[1] N. H. Abel: *Beweis der Unmöglichkeit, algebraische Gleichungen von höheren Graden als dem vierten allgemein aufzulösen.* J. für die reine und angewandte Math. (Crelle's Journal), 1:65–84, 1826.

[2] H. Anai, M. Noro und K. Yokoyama: *Computation of the splitting fields and the Galois groups of polynomials*. In: *Algorithms in algebraic geometry and applications (Santander, 1994)*, Bd. 143 d. Reihe *Progr. Math.*, S. 29–50. Birkhäuser, Basel, 1996.

[3] B. Assmann, A. Distler und B. Eick: *ALNUTH - ALgebraic NUmber THeory and an interface to the KANT system.* `http://www.icm.tu-bs.de/ag_algebra/software/assmann/Alnuth`, 2003. An accepted GAP 4 package, siehe [32].

[4] K. Belabas, M. van Hoeij, J. Klüners und A. Steel: *Factoring polynomials over global fields.* Submitted, 2004.

[5] S. Bosch: *Algebra.* Springer, Berlin–Heidelberg–New York, 4. Aufl., 2001.

[6] G. Butler: *Fundamental Algorithms for Permutation Groups*, Bd. 559 d. Reihe *Lecture Notes in Computer Science*. Springer, Berlin–Heidelberg–New York, 1991.

[7] H. Cohen: *A course in computational algebraic number theory*, Bd. 138 d. Reihe *Graduate Texts in Mathematics*. Springer, New York–Heidelberg–Berlin, 1993.

[8] J. H. Conway, A. Hulpke und J. McKay: *On transitive permutation groups.* LMS J. Comput. Math., 1:1–8 (electronic), 1998.

[9] M. Daberkow, C. Fieker, J. Klüners, M. Pohst, K. Roegner und K. Wildanger: *Kant V4*. J. Symb. Comput., 24:267 – 283, 1997.

[10] A. Distler: *Radiroot - Roots of a Polynomial as Radicals.* `http://www.icm.tu-bs.de/ag_algebra/software/distler/radiroot`, 2005. A GAP 4 package, siehe [32].

[11] H. M. Edwards: *Galois Theory*, Bd. 101 d. Reihe *Graduate Texts in Mathematics*. Springer, New York–Berlin–Heidelberg–Tokyo, 1984.

[12] B. Eick und B. Höfling: *The solvable primitive permutation groups of degree at most 6560*. LMS J. Comput. Math., 6:29–39 (electronic), 2003.

[13] É. Galois: *Oeuvres Mathématiques d'Évariste Galois*. Gauthier-Villars, Paris, 1897.

[14] K. Geissler und J. Klüners: *Galois group computation for rational polynomials*. J. Symbolic Comput., 30(6):653–674, 2000. Algorithmic methods in Galois theory.

[15] J. Hermes: *Ueber die Teilung des Kreises in 65537 gleiche Teile*. Nachrichten von der Gesellschaft der Wissenschaften zu Göttingen, Mathematisch-Physikalische Klasse, S. 170–186, 1894.

[16] G. Horng und M.-D. Huang: *Solving Polynomials by Radicals with Roots of Unity in Minimum Depth*. Mathematics of Computation, 68(226):881–885, 1999.

[17] A. Hulpke: *Konstruktion transitiver Permutationsgruppen*, Bd. 18 d. Reihe *Aachener Beiträge zur Mathematik*. RWTH Aachen, 1996.

[18] A. Hulpke: *Techniques for the computation of Galois groups*. In: *Algorithmic algebra and number theory (Heidelberg, 1997)*, S. 65–77. Springer, Berlin, 1999.

[19] B. Huppert: *Endliche Gruppen I*, Bd. 134 d. Reihe *Die Grundlehren der mathematischen Wissenschaften*. Springer-Verlag, Berlin–Heidelberg, 1967.

[20] J. Klüners und G. Malle: *A database for field extensions of the rationals*. LMS J. Comput. Math., 4:182–196 (electronic), 2001.

[21] S. Laundau: *Simplification of Nested Radicals*. SIAM J. Comp., 21(1):85–110, 1992.

[22] S. Laundau und G. L. Miller: *Solvability by Radicals Is in Polynomial Time*. J. of Computer and System Sciences, 30:179–208, 1985.

[23] G. Malle und B. H. Matzat: *Inverse Galois Theory*. Springer Monographs in Mathematics. Springer, Berlin–Heidelberg–New York, 1999.

[24] J. McKay und L. H. Soicher: *Computing Galois groups over the rationals*. J. Number Theory, 20:273–281, 1985.

[25] O. Neugebauer: *The Exact Sciences in Antiquity*. Dover Publications, Inc., New York, zweite Aufl., 1969.

[26] D. J. S. Robinson: *A Course in the Theory of Groups*, Bd. 80 d. Reihe *Graduate Texts in Mathematics*. Springer-Verlag, Berlin–Heidelberg–New York, 1982.

[27] H. R. Schwarz: *Numerische Mathematik*. B. G. Teubner, Stuttgart, vierte Aufl., 1997. With a contribution by Jörg Waldvogel.

[28] Á. Seress: *Permutation group algorithms*, Bd. 152 d. Reihe *Cambridge Tracts in Mathematics*. Cambridge University Press, Cambridge, 2003.

[29] C. C. Sims: *Computing the order of a solvable permutation group*. J. Symbolic Comput., 9:699–705, 1990.

[30] R. P. Stauduhar: *The determination of Galois groups*. Math. Comput., 27:981–996, 1973.

[31] G. Stroth: *Algebra: Einführung in die Galoistheorie*. De-Gruyter-Lehrbuch. de Gruyter, New York, 1998.

[32] The GAP Group: *GAP — Groups, Algorithms and Programming,Version 4.4*, 2004. `http://www.gap-system.org`.

[33] B. M. Trager: *Algebraic Factoring and Rational Function Integration*. In: *Proceedings of the 1976 ACM Symposium on Symbolic and Algebraic Computation*, S. 219–226, 1976.

[34] B. L. van der Waerden: *Algebra*, Bd. Erster Teil. Springer, Berlin–Heidelberg–New York, siebte Aufl., 1966.

[35] E. W. Weisstein: *Siegel Theta Function*. MathWorld–A Wolfram Web Resource. `http://mathworld.wolfram.com/SiegelThetaFunction.html`.

[36] H. Wielandt: *Finite Permutation Groups*. Academic Press, 1964.