Technische Universität Berlin
Fakultät II – Institut für Mathematik
Fachgebiet Algebra und Zahlentheorie

Ein polynomialer Algorithmus zur Bestimmung der Auflösbarkeit eines Polynoms durch Radikale

Bachelorarbeit

im Studiengang Mathematik

Vorgelegt von
Rico Raber
Berlin, März 2015

Betreuer: Prof. Dr. Peter Bürgisser

Inhaltsverzeichnis

1 Einleitung **1**

2 Grundlagen der Galoistheorie **3**
2.1 Algebraische Körpererweiterungen 3
2.2 Separable und normale Körpererweiterungen 4
2.3 Der Hauptsatz der Galoistheorie 5
2.4 Auflösbarkeit durch Radikale 7

3 Permutationsgruppen und Blöcke **9**
3.1 Eigenschaften von Blöcken 9
3.2 Berechnung von minimalen nichttrivialen Blöcken 12

4 Funktionsweise des Algorithmus **15**

5 Zwischenkörper **17**
5.1 Zusammenhang zwischen Blöcken und Zwischenkörpern . . . 17
5.2 Divide et impera 18
5.3 Polynome mit primitiver Galoisgruppe 22

6 Faktorisierung von Polynomen über Zahlkörpern **25**

7 Berechnung von Galoisgruppen **30**
7.1 Algorithmus: GALOIS 30
7.2 Korrektheit des Algorithmus 33
7.3 Abbruchkriterium 34

8 Minimale nichttriviale Blöcke von Galoisgruppen **36**
8.1 Die Faktorisierung von f enthält mehrere Linearfaktoren . . . 36
8.2 Die Faktorisierung von f enthält nur einen Linearfaktor . . . 38
8.2.1 Berechnung der Menge B_β 38
8.2.2 Finden von gemeinsamen Nullstellen 40
8.3 Algorithmus: BLOCKS 43

9 Kette von Zwischenkörpern **45**
9.1 Algorithmus: FIELDS 45
9.2 Bemerkungen zur Implementierung 47

10 Auflösbarkeit eines Polynoms durch Radikale **49**
10.1 Zusammenfügen der Algorithmen 49
10.2 Algorithmus: SOLVABILITY 49

11 Fazit und Ausblick **50**

Eidesstattliche Erklärung **51**

Literaturverzeichnis **52**

1 Einleitung

Bereits früh in der Schule lernt man die Formel zur Berechnung der Lösung der allgemeinen quadratischen Gleichung

$$X^2 + aX + b = 0.$$

Die Lösungen sind gegeben durch

$$X_1 = -\frac{a}{2} + \sqrt{\left(\frac{a}{2}\right)^2 - b}, \qquad X_2 = -\frac{a}{2} - \sqrt{\left(\frac{a}{2}\right)^2 - b}.$$

Tatsächlich wurden diese bereits 2000 v. Chr. von den Babylonien entdeckt. Auch für die allgemeinen Gleichungen vom Grad 3 und 4 gibt es solche Lösungsformeln, wenn auch deutlich kompliziertere. Dabei wird verlangt, dass sich die Nullstellen mithilfe einer endlichen Kombination der vier Grundrechenarten sowie Wurzelziehen angewendet auf die Koeffizienten des Polynoms darstellen lassen. Man könnte vermuten, dass sich dies so fortsetzt und Formeln zur Bestimmung von Nullstellen von allgemeinen Polynomen beliebigen Grades existieren. Wie sich jedoch Anfang des 19. Jahrhunderts herausstellte, ist man mit Grad 4 bereits an die obere Grenze gestoßen. Es zeigt sich, dass es für Polynomgleichungen vom Typ

$$X^n + a_1 X^{n-1} + \cdots + a_n = 0$$

für $n \geqslant 5$ keine allgemeine Lösungsformel, die die genannten Kriterien erfüllt, existiert. Dennoch ist es für einige konkrete Polynome mit rationalen Koeffizienten möglich, deren Nullstellen durch die beschriebene Weise auszudrücken. Man sagt dann, das Polynom sei *durch Radikale auflösbar*. Wie aber stellt man fest, ob ein gegebenes Polynom durch Radikale auflösbar ist? Diese Frage wurde Anfang des 19. Jahrhunderts beantwortet von Évariste Galois, dem französischen Mathematiker und Begründer der nach ihm benannten Galoistheorie, der bereits im Alter von 20 Jahren in einem Duell starb. Jedoch waren bis in den 1980er Jahren sämtliche Algorithmen, die für ein gegebenes Polynom mit rationalen Koeffizienten entscheiden sollten, ob dieses durch Radikale auflösbar ist, ineffizient: sie haben exponentielle Laufzeit. Erst 1983 ist es Landau und Miller [3, 4] gelungen, einen Algorithmus zu entwickeln, der diese Frage in polynomialer Zeit beantwortet.

Ziel dieser Arbeit ist die Beschreibung und Analyse des von Landau und Miller vorgestellten Algorithmus zur Bestimmung der Auflösbarkeit eines gegebenen normierten und irreduziblen Polynoms $f \in \mathbb{Z}[X]$ durch Radikale. Dabei soll hier der Fokus mehr auf dem Beweis der Korrektheit des Algorithmus und der Erläuterung der einzelnen Schritte, sowie der Nähe zur Implementation liegen als auf der Laufzeitanalyse.

Die Idee des Algorithmus ist die Folgende: Sei α eine Nullstelle von f. Wir konstruieren eine spezielle Kette von Körpern

$$\mathbb{Q} = \mathbb{Q}(\rho_r) \subset \mathbb{Q}(\rho_{r-1}) \subset \cdots \subset \mathbb{Q}(\rho_1) \subset \mathbb{Q}(\rho_0) = \mathbb{Q}(\alpha)$$

und irreduzible Polynome $g_1 \in \mathbb{Q}(\rho_1)[X], \ldots, g_r \in \mathbb{Q}(\rho_r)[X]$, sodass gilt:

$$\mathbb{Q}(\rho_{i-1}) \simeq \mathbb{Q}(\rho_i)[X]/g_i, \quad i = 1, \ldots, r.$$

Diese Kette wird eine besondere Eigenschaft aufweisen: Für alle $i = 1, \ldots, r$ wirkt die Galoisgruppe G_i von g_i *primitiv* auf den Nullstellen von g_i, eine spezielle Eigenschaft von Permutationsgruppen, die wir in Kapitel 3 näher erläutern werden.

Wir werden außerdem in Kapitel 5 zeigen, dass f genau dann über $\mathbb{Q}$ durch Radikale auflösbar ist, wenn für alle $i = 1, \ldots, r$ das Polynom g_i über $\mathbb{Q}(\rho_i)$ durch Radikale auflösbar ist, was wiederum genau dann der Fall ist, wenn die Galoisgruppe G_i von g_i auflösbar ist.

Wie können wir diese Konstruktion nun verwenden, um die Auflösbarkeit von f in polynomialer Zeit festzustellen? Wie eben erklärt, lässt sich die Auflösbarkeit von f auf die Auflösbarkeit der Galoisgruppen $G_1, \ldots, G_r$ reduzieren. Unsere Konstruktion wird zudem sicherstellen, dass die Bestimmung der Auflösbarkeit dieser Galoisgruppen in polynomialer Zeit möglich ist: Pálfy zeigte [5], dass die Kardinalität auflösbarer Gruppen, die transitiv und primitiv auf einer n-elementigen Menge wirken, kleiner ist als $\lambda \coloneqq 24^{-1/3} n^{3,25}$ $(*)$. Wir werden also versuchen, die Galoisgruppe G_i innerhalb eines dieser Kardinalität entsprechenden Zeitlimits zu berechnen. Erhalten wir eine Ausgabe, so können wir aufgrund der dann durch λ beschränkten Kardinalität von G_i in polynomialer Zeit entscheiden, ob G_i auflösbar ist. Erhalten wir keine Ausgabe, so ist die Kardinalität von G_i größer als λ und G_i kann wegen $(*)$ nicht auflösbar sein.

Die Arbeit ist folgendermaßen strukturiert. In Kapitel 2 werden zunächst die wichtigsten Grundlagen der Galoistheorie wiederholt. Anschließend wird in Kapitel 3 die Struktur von Permutationsgruppen untersucht und die für diese Arbeit sehr wichtigen Begriffe des *Blocks* und der *primitiven* Wirkung einer Permutationsgruppe auf einer endlichen Menge näher beleuchtet. Nachdem diese Begriffe eingeführt wurden, kann in Kapitel 4 die Funktionsweise des vorgestellten Algorithmus detailliert erläutert werden. Hiernach werden einige Vorbereitungen getroffen, die für den Algorithmus von zentraler Bedeutung sind: In Kapitel 5 beschreiben wir die Struktur von Zwischenkörpern zwischen $\mathbb{Q}$ und $\mathbb{Q}(\alpha)$ und in Kapitel 6 wird ein Verfahren vorgestellt, mit welchem sich Polynome über diesen Zwischenkörpern faktorisieren lassen. Kapitel 7 nutzt dieses Verfahren, um einen Algorithmus zu beschreiben, der Galoisgruppen von Polynomen explizit berechnen kann. Das Herz dieser Arbeit bildet Kapitel 8. Darin wird dargestellt, wie man Polynome konstruieren kann, deren Galoisgruppe primitiv auf den Nullstellen des Polynoms wirkt. Diese Erkenntnisse werden in Kapitel 9 genutzt, um die oben beschriebene Körperkette zwischen $\mathbb{Q}$ und $\mathbb{Q}(\alpha)$ zu konstruieren. Schließlich werden in Kapitel 10 die einzelnen Bausteine zu einem Algorithmus zusammengefügt, welcher in polynomialer Zeit die Frage nach der Auflösbarkeit eines Polynoms beantwortet.

2 Grundlagen der Galoistheorie

Dieser Abschnitt dient der Wiederholung der für diese Arbeit wichtigsten Begriffe und Sätze der Galoistheorie. Sämtliche Beweise können in [1] nachgeschlagen werden.

2.1 Algebraische Körpererweiterungen

Sei $\mathbb{L}/\mathbb{K}$ eine Körpererweiterung von $\mathbb{K}$. Dann können wir $\mathbb{L}$ als $\mathbb{K}$-Vektorraum auffassen. Der *Grad* der Körpererweiterung $\mathbb{L}/\mathbb{K}$ ist die Dimension von $\mathbb{L}$ über $\mathbb{K}$ und wird mit $[\mathbb{L} : \mathbb{K}]$ bezeichnet. Wir nennen $\mathbb{L}$ eine *endliche* Körpererweiterung von $\mathbb{K}$, falls $[\mathbb{L} : \mathbb{K}] < \infty$.

Satz 2.1 (Gradsatz). *Es seien $\mathbb{E}/\mathbb{K}$ und $\mathbb{L}/\mathbb{E}$ endliche Körpererweiterungen. Dann ist $\mathbb{L}/\mathbb{K}$ eine endliche Körpererweiterung und es gilt*

$$[\mathbb{L} : \mathbb{K}] = [\mathbb{L} : \mathbb{E}][\mathbb{E} : \mathbb{K}].$$

Es sei $\mathbb{L}/\mathbb{K}$ eine Körpererweiterung und $a_1, \ldots, a_n \in \mathbb{L}$. Dann bezeichnen wir mit $\mathbb{K}(a_1, \ldots, a_n)$ den kleinsten Unterkörper von $\mathbb{L}$, welcher $\mathbb{K}$ und $\{a_1, \ldots, a_n\}$ enthält: der von $a_1, \ldots, a_n$ über $\mathbb{K}$ erzeugte Unterkörper. Für $a \in \mathbb{L}$ nennen wir $\mathbb{K}(a)/\mathbb{K}$ *einfache Körperweiterung.*
Sei $\varphi_a : \mathbb{K}[X] \to \mathbb{L},\ f \mapsto f(a)$ der Einsetzungshomomorphismus. Das Element a heißt *algebraisch über* $\mathbb{K}$, falls $\ker(\varphi_a) \neq \{0\}$.

Satz 2.2. *Es sei a algebraisch über $\mathbb{K}$ und habe das Minimalpolynom $m_a \in \mathbb{K}[X]$. Dann ist m_a irreduzibel und $\mathbb{K}(a)$ ist isomorph zu $\mathbb{K}[X]/m_a$, wobei der Isomorphismus durch*

$$\mathbb{K}[X]/m_a \to \mathbb{K}(a),\ \overline{X} \mapsto a$$

gegeben ist. Außerdem gilt

$$\mathbb{K}(a) = \left\{ \sum_{i=0}^{n-1} \lambda_i a^i \mid \lambda_i \in \mathbb{K} \right\}$$

mit $n \coloneqq \deg(m_a) \geqslant 1$ sowie $[\mathbb{K}(a) : \mathbb{K}] = \deg(m_a)$.

Eine Körpererweiterung $\mathbb{L}/\mathbb{K}$ heißt *algebraisch*, falls jedes Element von $\mathbb{L}$ algebraisch über $\mathbb{K}$ ist. Ein *(algebraischer) Zahlkörper* ist eine endliche algebraische Körpererweiterung der rationalen Zahlen.

Satz 2.3. *Ist $\mathbb{L}/\mathbb{K}$ eine Körpererweiterung, so sind die folgenden Aussagen äquivalent:*

(1) Die Körpererweiterung $\mathbb{L}$ ist endlich.

(2) Die Körpererweiterung $\mathbb{L}$ wird von endlich vielen algebraischen Elementen erzeugt.

(3) $\mathbb{L}$ ist eine endlich erzeugte algebraische Körpererweiterung.

Es sei $f \in \mathbb{K}[X]$ von Null verschieden. Ein *Zerfällungskörper* von f über $\mathbb{K}$ ist ein Erweiterungskörper $\mathbb{L}/\mathbb{K}$, so dass es $a_1, \ldots, a_n \in \mathbb{L}$ und $\lambda \in \mathbb{K}\backslash\{0\}$ gibt mit

$$f = \lambda(X - a_1) \ldots (X - a_n)$$

und $\mathbb{L} = \mathbb{K}(a_1, \ldots, a_n)$. Ein Körper $\mathbb{K}$ heißt *algebraisch abgeschlossen*, falls jedes nichtkonstante Polynom über $\mathbb{K}$ mindestens eine Nullstelle hat.
Ein *algebraischer Abschluss* eines Körpers $\mathbb{K}$ ist ein algebraisch abgeschlossener Oberkörper $\overline{\mathbb{K}}$ von $\mathbb{K}$, so dass die Körpererweiterung $\overline{\mathbb{K}}/\mathbb{K}$ algebraisch ist.

Satz 2.4. *Jeder Körper $\mathbb{K}$ hat einen algebraischen Abschluss. Sind $\overline{\mathbb{K}}_1$ und $\overline{\mathbb{K}}_2$ algebraische Abschlüsse von $\mathbb{K}$, so existiert ein Isomorphismus $\overline{\mathbb{K}}_1 \to \overline{\mathbb{K}}_2$, welcher auf $\mathbb{K}$ die Identität ist.*

2.2 Separable und normale Körpererweiterungen

Sei $\mathbb{L}/\mathbb{K}$ eine algebraische Körpererweiterung. Ein Polynom $f \in \mathbb{K}[X]$ heißt *separabel*, wenn es keine mehrfachen Nullstellen in $\overline{\mathbb{K}}$ hat. Ein Element $a \in \mathbb{L}$ heißt *separabel über* $\mathbb{K}$, wenn das Minimalpolynom von a über $\mathbb{K}$ separabel ist. Die Erweiterung $\mathbb{L}/\mathbb{K}$ heißt *separabel*, falls jedes $a \in \mathbb{L}$ separabel über $\mathbb{K}$ ist.

Satz 2.5 (Satz vom primitiven Element). *Sei $\mathbb{L} = \mathbb{K}(a_1, \ldots, a_k)$ eine endliche separable Körpererweiterung von $\mathbb{K}$ und $|\mathbb{K}| = \infty$. Dann existiert ein $\rho \in \mathbb{L}$ mit $\mathbb{L} = \mathbb{K}(\rho)$. Das Element ρ kann in der Form $\rho = \lambda_1 a_1 + \cdots + \lambda_k a_k$, $\lambda_1, \ldots, \lambda_k \in \mathbb{K}$ gewählt werden.*

Ein Körper $\mathbb{K}$ heißt *perfekt*, falls jede algebraische Erweiterung von $\mathbb{K}$ separabel ist. Zum Beispiel ist $\mathbb{Q}$ ein perfekter Körper.

Satz 2.6. *Sei $\mathbb{K}$ ein perfekter Körper und $f \in \mathbb{K}[X]$. Dann ist f genau dann separabel, wenn f quadratfrei ist. Ist f irreduzibel, so ist f separabel.*

Eine *normale* Körpererweiterung $\mathbb{L}/\mathbb{K}$ ist eine algebraische Erweiterung mit der Eigenschaft, dass jedes irreduzible $f \in \mathbb{K}[X]$, das eine Nullstelle in $\mathbb{L}$ hat, über $\mathbb{L}$ in Linearfaktoren zerfällt.

Satz 2.7. *Sei $\mathbb{L}/\mathbb{K}$ eine endliche Körpererweiterung. Die Erweiterung ist genau dann normal, wenn $\mathbb{L}$ der Zerfällungskörper eines Polynoms $f \in \mathbb{K}[X]\backslash\mathbb{K}$ ist.*

Satz 2.8. *Seien $\mathbb{L}/\mathbb{E}$ und $\mathbb{E}/\mathbb{K}$ endliche Körpererweiterungen und sei die Erweiterung $\mathbb{L}/\mathbb{K}$ normal. Dann ist auch die Erweiterung $\mathbb{L}/\mathbb{E}$ normal.*

2.3 Der Hauptsatz der Galoistheorie

Für eine algebraische Körpererweiterung $\mathbb{L}/\mathbb{K}$ bezeichne $\mathrm{Hom}_{\mathbb{K}}(\mathbb{L}, \overline{\mathbb{K}})$ die Menge der Homomorphismen $\mathbb{L} \to \overline{\mathbb{K}}$, welche die Elemente von $\mathbb{K}$ fixieren ($\mathbb{K}$-Homomorphismen). Entsprechend bezeichne $\mathrm{Aut}_{\mathbb{K}}(\mathbb{L})$ die Menge der Automorphismen $\mathbb{L} \to \mathbb{L}$, welche die Elemente von $\mathbb{K}$ fixieren.

Satz 2.9. *Die Körpererweiterung $\mathbb{L}/\mathbb{K}$ ist genau dann normal, wenn für alle $\sigma \in \mathrm{Hom}_{\mathbb{K}}(\mathbb{L}, \overline{\mathbb{K}})$ gilt, dass $\sigma(\mathbb{L}) = \mathbb{L}$, das heißt $\sigma \in \mathrm{Aut}_{\mathbb{K}}(\mathbb{L})$.*

Eine algebraische Körpererweiterung $\mathbb{L}/\mathbb{K}$ heißt *galoisch*, wenn sie normal und separabel ist. Man nennt $\mathrm{Gal}(\mathbb{L}/\mathbb{K}) \coloneqq \mathrm{Aut}_{\mathbb{K}}(\mathbb{L})$ die *Galoisgruppe* der Erweiterung $\mathbb{L}/\mathbb{K}$.

Satz 2.10. *Sei $\mathbb{L}/\mathbb{K}$ eine endliche Galois-Erweiterung. Dann folgt $|\mathrm{Gal}(\mathbb{L}/\mathbb{K})| = [\mathbb{L} : \mathbb{K}]$.*

Sei $\mathbb{L}$ ein Körper und G eine Untergruppe von $\mathrm{Aut}(\mathbb{L})$. Dann ist der *Fixkörper* von G definiert als $\mathbb{L}^G \coloneqq \{a \in \mathbb{L} \mid \sigma(a) = a \text{ für alle } \sigma \in G\}$.

Satz 2.11. *Ist G eine endliche Untergruppe von* $\mathrm{Aut}(\mathbb{L})$*, so ist* $\mathbb{L}/\mathbb{L}^G$ *eine Galois-Erweiterung mit Galoisgruppe* $\mathrm{Gal}(\mathbb{L}/\mathbb{L}^G) = G$*.*

Satz 2.12 (Hauptsatz der Galois-Theorie). *Sei $\mathbb{L}/\mathbb{K}$ eine endliche Galois-Erweiterung mit $G = \mathrm{Gal}(\mathbb{L}/\mathbb{K})$. Dann sind die Zuordnungen*

$$\{\textit{Untergruppen von } G\} \longleftrightarrow \{\textit{Zwischenkörper von } \mathbb{L}/\mathbb{K}\}$$

$$H \longrightarrow \mathbb{L}^H$$

$$\mathrm{Gal}(\mathbb{L}/\mathbb{E}) \longleftarrow \mathbb{E}$$

bijektiv und invers zueinander. Weiterhin gilt:

(1) $H_1 \leqslant H_2 \Leftrightarrow \mathbb{L}^{H_1} \supseteq \mathbb{L}^{H_2}$

(2) $\mathbb{E}_1 \subseteq \mathbb{E}_2 \Leftrightarrow \mathrm{Gal}(\mathbb{L}/\mathbb{E}_1) \geqslant \mathrm{Gal}(\mathbb{L}/\mathbb{E}_2)$*.*

Satz 2.13. *Sei $\mathbb{L}/\mathbb{K}$ eine Galois-Erweiterung und $\mathbb{K} \subseteq \mathbb{E} \subseteq \mathbb{L}$ ein Zwischenkörper. Dann ist die Erweiterung $\mathbb{L}/\mathbb{E}$ galoisch. Seien weiter $G \coloneqq \mathrm{Gal}(\mathbb{L}/\mathbb{K})$ und $H \coloneqq \mathrm{Gal}(\mathbb{L}/\mathbb{E})$. Dann gilt: H ist genau dann Normalteiler von G, wenn die Erweiterung $\mathbb{E}/\mathbb{K}$ normal ist. Ist dies der Fall, so folgt* $\mathrm{Gal}(\mathbb{E}/\mathbb{K}) \simeq G/H$*.*

Sei $f \in \mathbb{K}[X]$ ein nichtkonstantes, separables Polynom und $\mathbb{L}$ der Zerfällungskörper von f. Dann ist $\mathbb{L}/\mathbb{K}$ eine endliche Galois-Erweiterung. Man nennt $\mathrm{Gal}(f) \coloneqq \mathrm{Gal}(\mathbb{L}/\mathbb{K})$ die *Galoisgruppe des Polynoms f*.

Satz 2.14. *Sei $f \in \mathbb{K}[X]$ separabel, $m = \deg(f) \geqslant 1$ und $\mathbb{L}$ der Zerfällungskörper von f.*

(1) Sind $\alpha_1, \ldots, \alpha_m$ die Nullstellen von f, so definiert

$$\begin{aligned} \varphi : \mathrm{Gal}(\mathbb{L}/\mathbb{K}) &\to \mathcal{S}_{\{\alpha_1,\ldots,\alpha_m\}} \simeq \mathcal{S}_m \\ \sigma &\mapsto \sigma|_{\{\alpha_1,\ldots,\alpha_m\}} \end{aligned}$$

einen injektiven Gruppen-Homomorphismus. Insofern können die Elemente von $\mathrm{Gal}(\mathbb{L}/\mathbb{K})$ *als Permutation der Nullstellen von f aufgefasst werden.*

(2) *f ist genau dann irreduzibel, wenn* $\mathrm{Gal}(\mathbb{L}/\mathbb{K})$ *transitiv auf* $\{\alpha_1, \ldots, \alpha_m\}$ *wirkt.*

(3) *Ist f irreduzibel und α eine Nullstelle von f, so sind die Nullstellen von f gegeben durch* $\{\sigma(\alpha) \mid \sigma \in \mathrm{Hom}_{\mathbb{K}}(\mathbb{K}(\alpha), \overline{\mathbb{K}})\}$.

2.4 Auflösbarkeit durch Radikale

Es sei G eine Gruppe. Eine Kette

$$G = G_0 \geqslant G_1 \geqslant \cdots \geqslant G_r = \{e\}$$

heißt *Normalreihe* von G, falls G_{i+1} stets Normalteiler von G_i ist, $i = 0, \ldots, r-1$. Eine Gruppe G_i/G_{i+1} heißt *Faktor* der Normalreihe.
G heißt *auflösbar*, falls sie eine Normalreihe mit abelschen Faktoren besitzt.

Satz 2.15. *Sei G eine endliche Gruppe. Dann gelten folgende Aussagen:*

(1) *Ist G auflösbar und H eine Untergruppe von G, dann ist auch H auflösbar.*

(2) *Sei H ein Normalteiler von G. Dann ist G genau dann auflösbar, wenn H und G/H auflösbar sind.*

(3) *Gilt $G = H \times K$, so ist G genau dann auflösbar, wenn H und K auflösbar sind.*

(4) *G ist genau dann auflösbar, wenn G eine Normalreihe besitzt, deren Faktoren zyklisch von Primzahlordnung sind.*

Eine endliche Körpererweiterung $\mathbb{L}/\mathbb{K}$ heißt *durch Radikale auflösbar*, wenn es einen Erweiterungskörper $\mathbb{E} \supseteq \mathbb{L}$ und eine Körperkette $\mathbb{K} = \mathbb{E}_0 \subseteq \mathbb{E}_1 \subseteq \cdots \subseteq \mathbb{E}_t = \mathbb{E}$ gibt, so dass $\mathbb{E}_i = \mathbb{E}_{i-1}(\alpha_i)$ für eine Nullstelle α_i von $X^{n_i} - a_i \in \mathbb{E}_{i-1}[X]$ für $i = 1, 2, \ldots, t$.

Die Erweiterung $\mathbb{L}/\mathbb{K}$ heißt *auflösbar*, wenn es eine Erweiterung $\mathbb{E}/\mathbb{L}$ gibt, so dass $\mathbb{E}/\mathbb{K}$ eine endliche Galois-Erweiterung mit auflösbarer Galoisgruppe $\mathrm{Gal}(\mathbb{E}/\mathbb{K})$ ist.

Sei $f \in \mathbb{K}[X]$ ein separables Polynom und $\mathbb{L}$ der Zerfällungskörper von f. Das Polynom f heißt *durch Radikale auflösbar*, wenn die Erweiterung $\mathbb{L}/\mathbb{K}$ durch Radikale auflösbar ist.

Satz 2.16. *Ein Polynom ist genau dann durch Radikale auflösbar, wenn seine Galoisgruppe auflösbar ist.*

Seien $a_1, \ldots, a_n$ Unbestimmte über dem Körper $\mathbb{K}$. Man nennt

$$f = X^n + a_1 X^{n-1} + \cdots + a_n \in \mathbb{K}(a_1, \ldots, a_n)[X]$$

das *allgemeine Polynom* vom Grad n.

Satz 2.17. *Die Galoisgruppe des allgemeinen Polynoms vom Grad n ist isomorph zur symmetrischen Gruppe $\mathcal{S}_n$. $\mathcal{S}_n$ ist auflösbar für $n \leqslant 4$ und nicht auflösbar für $n \geqslant 5$. Folglich ist das allgemeine Polynom vom Grad n für $n \leqslant 4$ durch Radikale auflösbar und für $n \geqslant 5$ nicht durch Radikale auflösbar.*

3 Permutationsgruppen und Blöcke

Um Aussagen über die Auflösbarkeit eines Polynoms treffen zu können, müssen wir uns genauer mit der Wirkung der Galoisgruppe des Polynoms auf dessen Nullstellen auseinandersetzen. Hierfür ist es notwendig, die Struktur von Permutationsgruppen, die auf einer endlichen Menge Ω wirken, zu verstehen. Für dieses Kapitel gelte folgende Generalvoraussetzung.

Generalvoraussetzung 3.1. Im Folgenden sei G stets eine endliche Permutationsgruppe, die auf einer endlichen Menge Ω wirke.

Definition 3.2. Wir sagen, G wirkt *transitiv* auf Ω, wenn für je zwei $\alpha, \beta \in \Omega$ eine Abbildung $\sigma \in G$ existiert mit $\sigma(\alpha) = \beta$. Für $\alpha \in \Omega$ nennen wir $G(\alpha) \coloneqq \{\sigma(\alpha) \mid \sigma \in G\}$ die *Bahn* von α. Sei H eine Teilmenge von G sowie B eine Teilmenge Ω. Wir verwenden die Notation $H(B) \coloneqq \{\sigma(B) \mid \sigma \in H\}$ sowie $H(\alpha) \coloneqq H(\{\alpha\})$ für $\alpha \in \Omega$.

3.1 Eigenschaften von Blöcken

Die Menge Ω lässt sich bezüglich der Wirkung der Permutationsgruppe in sogenannte *Blöcke* aufteilen, die im Folgenden eine zentrale Rolle spielen werden und daher nun näher beleuchtet werden sollen. Die Darstellung orientiert sich dabei größtenteils an [4, S. 32–35].

Definition 3.3. Eine Teilmenge $B \subseteq \Omega$ heißt *Block* von G, falls für alle $\sigma \in G$ gilt, dass $\sigma(B) = B$ oder $\sigma(B) \cap B = \varnothing$. Die Blöcke $B = \{x\}$, $x \in \Omega$ heißen *triviale Blöcke*. Besitzt G nur triviale Blöcke und den Block $B = \Omega$, so nennt man die Wirkung von G auf Ω *primitiv* (kurz: G ist primitiv).

Beispiel 3.4. (i) Es sei

$$G = \{\mathrm{id}, (12)(34), (13)(24), (14)(23)\} =: \{\sigma_1, \sigma_2, \sigma_3, \sigma_4\} \subset \mathcal{S}_4$$

die Kleinsche Vierergruppe und $\Omega = \{1, 2, 3, 4\}$. Dann bildet $B = \{1, 2\}$ einen Block von G, da $\sigma_1(B) = \sigma_2(B) = B$ und

$$\sigma_3(B) \cap B = \sigma_4(B) \cap B = \{3, 4\} \cap \{1, 2\} = \varnothing.$$

(ii) Die symmetrische Gruppe $\mathcal{S}_n$ ist für alle $n \in \mathbb{N}$ primitiv. △

Haben wir einen Block B der Permutationsgruppe G gefunden, so können wir G aufteilen in diejenigen Abbildungen, die B mengenweise festhalten und diejenigen, die B auf eine zu B disjunkte Menge abbilden. Hierfür führen wir folgenden Begriff ein:

Definition 3.5. Sei B eine Teilmenge von Ω. Wir nennen

$$G_B \coloneqq \{\sigma \in G \mid \sigma(B) = B\}$$

den *Stabilisator* von B. Für ein Element $\alpha \in \Omega$ schreiben wir $G_\alpha \coloneqq G_{\{\alpha\}}$.

Beispiel 3.6. Sei $G = \{\mathrm{id}, (12)(34), (13)(24), (14)(23)\}$ die Kleinsche Vierergruppe, die auf der Menge $\Omega = \{1, 2, 3, 4\}$ wirke und $B = \{1, 2\}$. Dann ist $G_B = \{\mathrm{id}, (12)(34)\}$. △

Satz 3.7. *Sei $B \subseteq \Omega$ ein Block von G und $\alpha \in B$. Dann gilt $G_\alpha \subseteq G_B$.*

Beweis. Sei $\sigma \in G_\alpha$, d.h. $\sigma(\alpha) = \alpha$. Dann folgt $\sigma(B) \cap B \neq \varnothing$ und da B ein Block ist, gilt $\sigma(B) = B$, also $\sigma \in G_B$. □

Durch die Kenntnis eines Blocks $B \subseteq \Omega$ von G erhalten wir durch Anwenden von G gleich mehrere Blöcke. Wir können sogar, vorausgesetzt G wirkt transitiv auf Ω, ganz Ω in Blöcke partitionieren:

Satz 3.8. *Sei B ein Block von G und $\sigma \in G$. Dann ist auch $\sigma(B)$ ein Block von G. Wirkt G transitiv auf Ω, so existieren $\sigma_1, \ldots, \sigma_l \in G$, so dass $\sigma_1(B), \ldots, \sigma_l(B)$ eine Partition von Ω bilden.*

Beweis. Sei $\sigma \in G$. Wir wollen zunächst zeigen, dass $\sigma(B)$ ein Block ist, d.h. dass $\tau\sigma(B) \cap \sigma(B) \in \{\varnothing, \sigma(B)\}$ für alle $\tau \in G$. Angenommen, es gibt ein $\tau \in G$ mit $\tau\sigma(B) \cap \sigma(B) \neq \varnothing$ und sei $\beta \in \tau\sigma(B) \cap \sigma(B)$. Es existieren also $\alpha, \gamma \in B$ mit $\sigma(\alpha) = \beta = \tau\sigma(\gamma)$. Daraus folgt $\alpha = \sigma^{-1}\tau\sigma(\gamma)$, d.h. $\alpha \in B \cap \sigma^{-1}\tau\sigma(B)$. Da B ein Block ist, folgt $\sigma^{-1}\tau\sigma(B) = B$ und damit $\sigma(B) = \tau\sigma(B)$. Also ist $\sigma(B)$ ein Block.

Wirkt G transitiv auf Ω, so existieren $\sigma_1, \ldots, \sigma_l$ mit $\Omega = \sigma_1(B) \cup \cdots \cup \sigma_l(B)$. Gilt $\sigma_i(B) \cap \sigma_j(B) \neq \varnothing$, so folgt $B \cap \sigma_i^{-1}\sigma_j(B) \neq \varnothing$ und daher $B = \sigma_i^{-1}\sigma_j(B)$, also $\sigma_i(B) = \sigma_j(B)$. Folglich existieren $\sigma_1, \ldots, \sigma_l$, so dass $\sigma_1(B), \ldots, \sigma_l(B)$ eine Partition von Ω bilden. □

Definition 3.9. Man nennt die Partition $\sigma_1(B), \ldots, \sigma_l(B)$ aus Satz 3.8 ein *vollständiges Blocksystem* von G.

Beispiel 3.10. Betrachte die Diedergruppe $D_6 \coloneqq \langle (123456), (26)(35) \rangle$, d.h. die von den Permutationen $r \coloneqq (123456)$ und $s \coloneqq (26)(35)$ erzeugte 12-elementige Untergruppe von $\mathcal{S}_6$ und sei $B \coloneqq \{1, 4\}$. Es gilt $r^2 = (135)(246)$, $r^3 = (14)(25)(36)$, $r^4 = (153)(264)$, $r^5 = (165432)$. Man prüft leicht nach, dass B einen Block von D_6 bildet. Außerdem ist $\mathrm{id}(B) = \{1, 4\}$, $r(B) = \{2, 5\}$, $r^2(B) = \{3, 6\}$ ein vollständiges Blocksystem von D_6. △

Sei nun B ein Block von G. Offensichtlich ist G_B eine Untergruppe von G. Wir können also G_B als eine Permutationsgruppe auffassen, die auf der Menge B wirkt:

Definition 3.11. Sei B ein Block von G. Wir setzen $G^B \coloneqq \{\sigma|_B \mid \sigma \in G_B\}$ und nennen die Wirkung von G^B auf B die *induzierte Wirkung* von G auf B.

Wir wollen später Erkenntnisse über Blöcke von G^B ausnutzen, um Blöcke der ursprünglichen Gruppe G zu finden. Die Grundlage hierfür liefert der folgende Satz.

Satz 3.12. *Sei B ein Block von G. Dann bildet jeder Block von G^B auch einen Block von G.*

Beweis. Sei $B' \subseteq B$ ein Block von G^B und $\sigma \in G_B$. Folglich ist $\sigma|_B \in G^B$ und es gilt $\sigma(B') \cap B' = \sigma|_B(B') \cap B' \in \{\varnothing, B'\}$. Sei nun $\sigma \in G \backslash G_B$. Dann folgt $\sigma(B) \cap B = \varnothing$ und daher $\sigma(B') \cap B' = \varnothing$. Insgesamt gilt also für alle $\sigma \in G$, dass $\sigma(B') \cap B' \in \{\varnothing, B'\}$, d.h. B' ist ein Block von G. □

Ein weitere nützliche Aussage betrifft die Kardinalität der Menge G_B:

Satz 3.13. *G wirke transitiv auf Ω. Sei $B \subseteq \Omega$ ein Block von G. Dann gilt $|G_B| = |G_\alpha| \cdot |B|$ für alle $\alpha \in B$.*

Beweis. Sei $B = \{\alpha_1, \ldots, \alpha_k\}$ und $\alpha \in B$. Aufgrund der Transitivität der Wirkung von G auf Ω gibt es $\sigma_i \in G$ mit $\sigma_i(\alpha) = \alpha_i$, $i = 1, \ldots, k$. Wir behaupten, dass $G_B = \sigma_1 G_\alpha \dot\cup \ldots \dot\cup \sigma_k G_\alpha =: H$. Zunächst gilt

$$\sigma_i G_\alpha(\alpha) = \sigma_i(\{\alpha\}) = \{\alpha_i\}$$

für alle $i = 1, \ldots, k$. Daraus folgt die Disjunktheit der Mengen $\sigma_1 G_\alpha, \ldots, \sigma_k G_\alpha$.

Wir zeigen jetzt $G_B = H$. Sei dazu $\sigma \in H$, etwa $\sigma = \sigma_i \tau$ mit $\tau \in G_\alpha$. Dann folgt $\sigma(\alpha) = \alpha_i \in B$. Es gilt also $\sigma(B) \cap B \neq \varnothing$ und daher, da B ein Block ist, $\sigma(B) = B$, also $\sigma \in G_B$. Sei umgekehrt $\sigma \in G_B$. Dann gilt $\sigma(\alpha) = \alpha_i$ für ein $i \in \{1, \ldots, k\}$. Folglich ist $\sigma_i^{-1}\sigma(\alpha) = \alpha$, also $\sigma_i^{-1}\sigma \in G_\alpha$ und damit $\sigma \in \sigma_i G_\alpha \subseteq H$. Insgesamt folgt $|G_B| = k \cdot |G_\alpha|$. □

Für uns werden im Laufe der Arbeit vor allem spezielle minimale Blöcke von besonderer Bedeutung sein. Genauer interessieren wir uns für Blöcke mit der folgenden Eigenschaft:

Definition 3.14. Ein *minimaler nichttrivialer Block* B von G ist ein Block mit mehr als einem Element für den gilt:

$$\big(B' \subseteq B,\ |B'| > 1,\ B' \text{ ist Block von } G\big) \ \Rightarrow\ B' = B.$$

3.2 Berechnung von minimalen nichttrivialen Blöcken

Nachdem wir den Begriff des minimalen nichttrivialen Blocks definiert haben, ist es natürlich wünschenswert Aussagen darüber treffen zu können, wie man einen solchen berechnen kann. Genauer interessieren wir uns für die Berechnung minimaler nichttrivialer Blöcke, die ein bestimmtes vorgegebenes Element enthalten sollen.

Im besten Fall kennen wir die Gruppe G sowie ihre Wirkung auf der Menge Ω explizit. Dann können wir einen minimalen nichttrivialen Block von G mit folgendem Algorithmus direkt berechnen:

Algorithmus: MINBLOCK

Eingabe: Gruppe $G = \{\sigma_1, \ldots, \sigma_n\}$, die auf der Menge $\Omega = \{\alpha_1, \ldots, \alpha_m\}$, $m \geqslant 2$, wirkt

Ausgabe: Minimaler nichttrivialer Block von G, welcher α_1 enthält

1 $\mathcal{B} \leftarrow \varnothing$
2 Für $i = 2, \ldots, m$ führe aus:
3 $\quad C \leftarrow \{\alpha_1, \alpha_i\}$
4 $\quad$ Solange es ein $\sigma \in G$ gibt, mit $\sigma(C) \neq C$ und $\sigma(C) \cap C \neq \varnothing$:
5 $\quad\quad C \leftarrow C \cup \sigma(C)$
6 $\quad \mathcal{B} \leftarrow \mathcal{B} \cup \{C\}$
7 Gib ein C aus $\mathcal{B}$ mit minimaler Kardinalität aus.

Satz 3.15. *Der Algorithmus* MINBLOCK *arbeitet korrekt.*

Beweis. Damit eine Teilmenge $C \subseteq \Omega$ ein Block von G ist, muss für alle $\sigma \in G$ gelten, dass $\sigma(C) = C$ oder $\sigma(C) \cap C = \varnothing$. Wir stellen also zunächst fest, dass die Schleife in den Zeilen 4 und 5 erst verlassen wird, wenn C ein Block ist. Da die Kardinalität von C in Zeile 5 stets vergrößert wird, aber durch m beschränkt ist, wird die Schleife nach höchstens m Schritten verlassen. Folglich terminiert der Algorithmus und alle Mengen aus $\mathcal{B}$ sind Blöcke von G. Außerdem haben alle Blöcke in $\mathcal{B}$ mindestens zwei Elemente, da in Zeile 3 jeder potentielle Block bereits mit zwei Elementen initialisiert wird.

Sei nun B ein minimaler nichttrivialer Block von G, welcher α_1 enthält. Wir wollen zeigen, dass B in $\mathcal{B}$ enthalten ist. Da B per Definition mehr als ein Element hat, gilt $B' \coloneqq \{\alpha_1, \alpha_i\} \subseteq B$ für ein $i \in \{2, \ldots, m\}$. Wir beginnen also Zeile 4 mit einer Menge $B' \subseteq B$. Falls für alle $\sigma \in G$ gilt, dass $\sigma(B') = B'$ oder $\sigma(B') \cap B' = \varnothing$, so ist B' ein Block. Da aber $B' \subseteq B$ und B ein minimaler nichttrivialer Block ist, folgt $B' = B$. Die Schleife wird verlassen und B zu $\mathcal{B}$ hinzugefügt. Existiert hingegen ein $\sigma \in G$ mit

$\sigma(B') \neq B$ und $\sigma(B') \cap B' \neq \varnothing$, so gilt wegen $B' \subseteq B$ auch $\sigma(B) \cap B \neq \varnothing$ und daher (da B ein Block ist) $\sigma(B) = B$. Daraus folgt $\sigma(B') \subseteq \sigma(B) = B$, insgesamt also $B' \cup \sigma(B') \subseteq B$. In Schritt 5 wird dann die Zuweisung $B' \leftarrow B' \cup \sigma(B')$ durchgeführt. Somit wurde B' vergrößert, aber es gilt weiterhin $B' \subseteq B$ und wir springen wieder zu Schritt 4. Dieses Vorgehen wird so lange wiederholt, bis $B' = B$ gilt und B zu $\mathcal{B}$ hinzugefügt wird. Dies zeigt also, dass jeder minimale nichttriviale Block, welcher α_1 enthält, nach Beendigung des Algorithmus in $\mathcal{B}$ enthalten ist. Da in Zeile 7 eine kardinalitätsminimale Menge von $\mathcal{B}$ ausgegeben wird, erhalten wir folglich als Rückgabe einen minimalen nichttrivialen Block von G, welcher α_1 enthält, was zu zeigen war. □

Es ist jedoch häufig der Fall, dass man die Gruppe G sowie ihre Wirkung auf Ω nicht explizit bzw. nicht vollständig kennt. Aber auch in diesem Fall gibt es unter bestimmten Voraussetzungen eine Möglichkeit, einen minimalen nichttrivialen Block, welcher ein vorgegebenes Element enthält, zu berechnen. Diese wird im Folgenden beschrieben. Zunächst aber noch eine Bemerkung zur Notation:

Notation 3.16. Seien H, K Untergruppen von G. Dann bezeichne $\langle H, K \rangle$ die von H und K erzeugte Untergruppe von G.

Ein besonderer Fall, welcher im weiteren Verlauf eine wichtige Rolle spielen wird, tritt ein, wenn der Stabilisator eines Elements $\alpha \in \Omega$ keinen Fixpunkt außer α hat, d.h. wenn $G_\alpha(\beta) \neq \{\beta\}$ für alle $\beta \in \Omega$ mit $\beta \neq \alpha$ gilt. Ist dies der Fall, so genügt uns zur Berechnung eines minimalen nichttrivialen Blocks $B \subseteq \Omega$, welcher α enthält, die Stabilisatoren der Elemente aus Ω zu kennen:

Satz 3.17. *Die Permutationsgruppe G wirke transitiv auf der Menge Ω. Angenommen G_α hat keinen Fixpunkt außer α. Für alle $\beta \in \Omega$ bildet $\langle G_\alpha, G_\beta \rangle(\alpha)$ einen Block von G. Sei B ein minimaler nichttrivialer Block, welcher α enthält. Dann gilt für alle $\beta \in B$ mit $\beta \neq \alpha$:*

$$B = \langle G_\alpha, G_\beta \rangle(\alpha).$$

Lemma 3.18. *Die Permutationsgruppe G wirke transitiv auf der Menge Ω. Seien $\beta_1, \beta_2 \in \Omega$. Dann hat G_{β_1} genau dann keinen Fixpunkt außer β_1, wenn G_{β_2} keinen Fixpunkt außer β_2 hat.*

Beweis. G_{β_1} habe keinen Fixpunkt außer β_1. Da G transitiv auf Ω wirkt, gibt es ein $\sigma \in G$ mit $\sigma(\beta_2) = \beta_1$. Dann hat $\sigma^{-1} G_{\beta_1} \sigma$ keinen Fixpunkt außer β_2. Dies sieht man so: Sei $\beta \in \Omega$ mit $\beta \neq \beta_2$. Dann folgt aufgrund der Injektivität von σ, dass $\beta' \coloneqq \sigma(\beta) \neq \beta_1$. Da G_{β_1} keinen Fixpunkt außer

β_1 hat, folgt also $G_{\beta_1}\sigma(\beta) = G_{\beta_1}(\beta') \neq \{\beta'\}$. Mit der Injektivität von σ^{-1} ergibt sich dann $\sigma^{-1}G_{\beta_1}\sigma(\beta) \neq \{\beta\}$.

Da $\sigma^{-1}G_{\beta_1}\sigma \subseteq G_{\beta_2}$, hat auch G_{β_2} keinen Fixpunkt außer β_2. Der Beweis der Rückrichtung verläuft analog. □

Beweis von Satz 3.17. Sei $\beta \in \Omega$. Wir zeigen zunächst, dass $C \coloneqq \langle G_\alpha, G_\beta\rangle(\alpha)$ ein Block von G ist. Angenommen, $C \cap \tau(C) \neq \varnothing$ für ein $\tau \in G$. Wir müssen $\tau(C) = C$ zeigen. Sei dazu $\gamma \in C \cap \tau(C)$. Dann existieren $\sigma_1, \sigma_2 \in \langle G_\alpha, G_\beta\rangle$ mit $\sigma_1(\alpha) = \gamma = \tau\sigma_2(\alpha)$, also $\sigma_1^{-1}\tau\sigma_2(\alpha) = \alpha$. Dies impliziert $\sigma_1^{-1}\tau\sigma_2 \in G_\alpha \subseteq \langle G_\alpha, G_\beta\rangle$ und damit $\tau \in \langle G_\alpha, G_\beta\rangle$. Folglich ist $\tau(C) = \tau\langle G_\alpha, G_\beta\rangle(\alpha) = \langle G_\alpha, G_\beta\rangle(\alpha) = C$, also ist C ein Block.

Sei nun B ein minimaler nichttrivialer Block, welcher α enthält und sei $\beta \in B$, $\beta \neq \alpha$. Wir setzen wieder $C \coloneqq \langle G_\alpha, G_\beta\rangle(\alpha)$ und wollen $B = C$ zeigen. Da B ein Block ist, gilt nach Satz 3.7, dass $G_\alpha, G_\beta \subseteq G_B$. Da außerdem G_B eine Untergruppe von G ist, folgt $\langle G_\alpha, G_\beta\rangle \subseteq G_B$ und damit $C = \langle G_\alpha, G_\beta\rangle(\alpha) \subseteq G_B(\alpha) = B$. Die letzte Gleichheit folgt aus der Transitivität von G.

Nach Voraussetzung hat G_α keinen Fixpunkt außer α. Nach Lemma 3.18 hat auch G_β keinen Fixpunkt außer β. Folglich gilt $G_\beta(\alpha) \neq \{\alpha\}$ und damit $|C| \geqslant 2$. Die Menge C ist also ein Block mit mehr als einem Element und da B ein minimaler nichttrivialer Block und $C \subseteq B$ gilt, folgt $C = B$, was zu zeigen war. □

4 Funktionsweise des Algorithmus

Die folgende Darstellung ist [4] entnommen. Sei $f \in \mathbb{Z}[X]$ normiert, irreduzibel und vom Grad $m \geqslant 2$ und sei α eine Nullstelle von f. Unser Ziel ist es, zu bestimmen, ob f durch Radikale auflösbar ist. Das einfachste Verfahren, dies zu überprüfen, wäre, die Galoisgruppe G von f explizit zu berechnen und deren Auflösbarkeit zu bestimmen. Jedoch ist die Kardinalität von G möglicherweise exponentiell im Grad von f und somit könnte G nicht in polynomialer Zeit berechnet werden. Daher ist es sinnvoll, das Problem auf kleinere Teilprobleme zu reduzieren: Wir konstruieren eine Körperkette

$$\mathbb{Q} = \mathbb{Q}(\rho_r) \subset \mathbb{Q}(\rho_{r-1}) \subset \cdots \subset \mathbb{Q}(\rho_1) \subset \mathbb{Q}(\rho_0) = \mathbb{Q}(\alpha)$$

und irreduzible Polynome $g_1 \in \mathbb{Q}(\rho_1)[X], \ldots, g_r \in \mathbb{Q}(\rho_r)[X]$, sodass für $i = 1, \ldots, r$ gilt, dass

$$\mathbb{Q}(\rho_{i-1}) \simeq \mathbb{Q}(\rho_i)[X]/g_i.$$

Wir werden in Kapitel 5 zeigen, dass f genau dann durch Radikale auflösbar ist, wenn jedes der Polynome $g_1, \ldots, g_r$ durch Radikale auflösbar ist. Um die Auflösbarkeit der g_i zu überprüfen, müssen wir wiederum die Galoisgruppe G_i von g_i berechnen und deren Auflösbarkeit bestimmen. Wie können wir hieraus einen Vorteil hinsichtlich der Laufzeit erreichen? Wir konstruieren die Körperkette derart, dass G_i primitiv auf den Nullstellen von g_i wirkt und nutzen folgenden Satz von Pálfy [5] aus:

Satz 4.1. *Sei G eine auflösbare Gruppe, die transitiv und primitiv auf einer n-elementigen Menge wirkt. Dann ist die Kardinalität von G kleiner als $\lambda(n) \coloneqq 24^{-1/3} n^{3{,}25}$.*

Wir versuchen nun G_i mittels des in Kapitel 7 beschriebenen Algorithmus GALOIS zu berechnen. Ist $|G_i|$ kleiner als $\lambda(\deg(g_i))$, so gelingt uns die Berechnung von G_i in polynomialer Zeit. Mithilfe eines geeignetes Algorithmus (siehe z.B. [6] oder den von David Joyner in SAGE implementierten Algorithmus `is_solvable`) können wir dann überprüfen, ob G_i auflösbar ist oder nicht. Andernfalls brechen wir GALOIS ab, sobald wir feststellen, dass $|G_i|$ größer als $\lambda(\deg(g_i))$ ist. Ist dies der Fall, so kann G_i wegen Satz 4.1 nicht auflösbar sein und wir sind fertig.

Es verbleibt also die Aufgabe, die oben beschriebene Körperkette mit der Eigenschaft, dass G_i primitiv auf den Nullstellen von g_i wirkt, zu berechnen. Seien $\alpha = \alpha_1, \ldots, \alpha_m$ die Nullstellen von f und $\Omega \coloneqq \{\alpha_1, \ldots, \alpha_m\}$. Sei weiter G die Galoisgruppe von f und $B = \{\alpha_1, \ldots, \alpha_k\}$ ein minimaler nichttrivialer Block von G, welcher α enthält. In Kapitel 8 wird beschrieben, wie sich ein

solcher Block berechnen lässt. Definieren wir

$$g_1 \coloneqq \prod_{i=1}^{k}(X - \alpha_i) = X^k + a_1 X^{k-1} + \cdots + a_k \in \mathbb{Q}(a_1, \ldots, a_k)[X],$$

dann wirkt, wie wir später zeigen werden, die Galoisgruppe von g_1 primitiv auf den Nullstellen von g_1 und es gilt $\mathbb{Q}(a_1, \ldots, a_k) \subset \mathbb{Q}(\alpha)$. Als nächstes finden wir ein primitives Element ρ_1 von $\mathbb{Q}(a_1, \ldots, a_k)$ (dann gilt also $\mathbb{Q}(\rho_1) = \mathbb{Q}(a_1, \ldots, a_k)$) und das Minimalpolynom h_1 von ρ_1 über $\mathbb{Q}$. Nun spielt h_1 die Rolle, die zuvor f eingenommen hat. Sei also Ω_1 die Nullstellenmenge von h_1, auf welcher die Galoisgruppe H_1 von h_1 wirkt und sei $B_1 = \{\beta_1, \ldots, \beta_l\}$ ein minimaler nichttrivialer Block von H_1. Wir setzen

$$g_2 \coloneqq \prod_{i=1}^{l}(X - \beta_i) = X^l + b_1 X^{l-1} + \cdots + b_l \in \mathbb{Q}(b_1, \ldots, b_l)[X].$$

Wiederum wirkt die Galoisgruppe von g_2 primitiv auf den Nullstellen von g_2 und es gilt $\mathbb{Q}(b_1, \ldots, b_l) \subset \mathbb{Q}(\rho_1) \subset \mathbb{Q}(\alpha)$. Wir berechnen ein primitives Element ρ_2 von $\mathbb{Q}(b_1, \ldots, b_l)$ und das Minimalpolynom h_2 von ρ_2 über $\mathbb{Q}$. Wir fahren so fort, bis $g_r \in \mathbb{Q}[X]$ gilt. Dies liefert uns die Körperkette mit den gewünschten Eigenschaften.

5 Zwischenkörper

Generalvoraussetzung 5.1. Sei $f \in \mathbb{Z}[X]$ irreduzibel, normiert und vom Grad $m \geqslant 2$ und $\alpha = \alpha_1, \ldots, \alpha_m$ die Nullstellen von f. Sei weiter $\Omega = \{\alpha_1, \ldots, \alpha_m\}$ und G die Galoisgruppe von f, welche auf der Menge Ω wirke.

5.1 Zusammenhang zwischen Blöcken und Zwischenkörpern

Um die Frage nach der Auflösbarkeit von f durch Radikale beantworten zu können, benötigen wir mehr Kenntnisse über die Struktur von Zwischenkörpern zwischen $\mathbb{Q}$ und $\mathbb{Q}(\alpha)$. Es stellt sich heraus [4, S. 43–47], dass diese Zwischenkörper eng verbunden sind mit den Blöcken von G, welche α enthalten:

Satz 5.2. *Seien $f \in \mathbb{Z}[X]$ irreduzibel und normiert, $\alpha = \alpha_1, \ldots, \alpha_m$ die Nullstellen von f, $\mathbb{L} \coloneqq \mathbb{Q}(\alpha_1, \ldots, \alpha_m)$ und $G = \mathrm{Gal}(f)$. Sei außerdem ein Zwischenkörper $\mathbb{Q} \subseteq \mathbb{E} \subseteq \mathbb{Q}(\alpha)$ gegeben. Dann gibt es einen Block B von G, welcher α enthält und für den $\mathbb{E} = \mathbb{L}^{G_B}$ gilt.*

Sei umgekehrt B ein Block von G, welcher α enthält. Dann existiert ein Zwischenkörper $\mathbb{Q} \subseteq \mathbb{E} \subseteq \mathbb{Q}(\alpha)$ mit $\mathbb{E} = \mathbb{L}^{G_B}$.

Beweis. Ist B ein Block von G, welcher α enthält dann gilt nach Satz 3.7, dass $G_\alpha \leqslant G_B \leqslant G$. Mit dem Hauptsatz der Galoistheorie folgt dann $\mathbb{Q} \subseteq \mathbb{E} \coloneqq \mathbb{L}^{G_B} \subseteq \mathbb{L}^{G_\alpha} = \mathbb{Q}(\alpha)$.

Sei nun umgekehrt ein Zwischenkörper $\mathbb{Q} \subseteq \mathbb{E} \subseteq \mathbb{Q}(\alpha)$ gegeben. Wir wollen zeigen, dass es einen Block B von G gibt, welcher α enthält und für den $\mathbb{E} = \mathbb{L}^{G_B}$ gilt. Sei $k \coloneqq [\mathbb{Q}(\alpha) : \mathbb{E}]$ und $g = X^k + a_1 X^{k-1} + \cdots + a_k \in \mathbb{E}[X]$ das Minimalpolynom von α über $\mathbb{E}$ und sei $\mathbb{L} \coloneqq \mathbb{Q}(\alpha_1, \ldots, \alpha_m)$. Die Nullstellen von g sind nach Satz 2.14 gegeben durch

$$\begin{aligned} B' &\coloneqq \mathrm{Hom}_{\mathbb{E}}(\mathbb{E}(\alpha), \overline{\mathbb{E}})(\alpha) = \left\{\sigma(\alpha) \mid \sigma \in \mathrm{Hom}_{\mathbb{E}}(\mathbb{E}(\alpha), \overline{\mathbb{E}})\right\} \\ &= \mathrm{Hom}_{\mathbb{E}}(\mathbb{Q}(\alpha), \overline{\mathbb{Q}})(\alpha) \subseteq \mathrm{Hom}_{\mathbb{Q}}(\mathbb{Q}(\alpha), \overline{\mathbb{Q}})(\alpha) = \Omega = \{\alpha_1, \ldots, \alpha_m\}, \end{aligned}$$

etwa $B' = \{\alpha_1, \ldots, \alpha_k\}$. Folglich gilt

$$g = (X - \alpha_1) \ldots (X - \alpha_k) = X^k + a_1 X^{k-1} + \cdots + a_k \in \mathbb{E}[X]$$

und daher $a_i = \pm\sigma_i(\alpha_1, \ldots, \alpha_k)$, wobei σ_i das i-te elementarsymmetrische Polynom in k Variablen sei, $i = 1, \ldots, k$. Wir setzen $\mathbb{F} \coloneqq \mathbb{Q}(a_1, \ldots, a_k)$ und wollen $\mathbb{E} = \mathbb{F}$ zeigen. Da $a_1, \ldots, a_k \in \mathbb{E}$, folgt $\mathbb{F} \subseteq \mathbb{E}$ und da $g \in \mathbb{E}[X]$ das Minimalpolynom von α ist, gilt nach Satz 2.2, dass $[\mathbb{Q}(\alpha) : \mathbb{E}] = \deg(g)$. Die Koeffizienten $a_1, \ldots, a_k$ von g sind in $\mathbb{F}$ enthalten, also können wir g auch als ein Polynom in $\mathbb{F}[X]$ auffassen, welches α als Nullstelle besitzt. Sei m_α das Minimalpolynom von α über $\mathbb{F}$. Folglich gilt

$$[\mathbb{Q}(\alpha) : \mathbb{F}] = \deg(m_\alpha) \leqslant \deg(g) = [\mathbb{Q}(\alpha) : \mathbb{E}].$$

Zusammen mit $\mathbb{F} \subseteq \mathbb{E}$ ergibt sich $\mathbb{E} = \mathbb{F}$.

Sei $H \coloneqq \mathrm{Gal}(\mathbb{L}/\mathbb{E}) = \mathrm{Gal}(\mathbb{L}/\mathbb{Q}(a_1, \ldots, a_k))$. Wir wollen $H = G_{B'}$ zeigen. Es gilt

$$G_{B'} = \{\sigma \in G \mid \sigma(B') = B'\} = \left\{\sigma \in \mathrm{Gal}(\mathbb{L}/\mathbb{Q}) \mid \sigma(B') = B'\right\}.$$

Sei zunächst $\sigma \in G_{B'}$. Folglich hält σ die Menge $B' = \{\alpha_1, \ldots, \alpha_k\}$ fest. Da außerdem $a_1, \ldots, a_k$ (bis auf Vorzeichen) die elementarsymmetrischen Polynome in k Variablen ausgewertet bei $\alpha_1, \ldots, \alpha_k$ sind, werden $a_1, \ldots, a_k$ und damit auch $\mathbb{E} = \mathbb{Q}(a_1, \ldots, a_k)$ elementweise von σ festgehalten, d.h. $\sigma \in \mathrm{Gal}(\mathbb{L}/\mathbb{E}) = H$, also $G_{B'} \subseteq H$.

Sei nun $\tau \in H$, d.h. τ ist ein $\mathbb{E}$-Homomorphismus von $\mathbb{L}$ nach $\mathbb{L}$. Damit gilt $\tau(a_i) = a_i$ für $i = 1, \ldots, k$. Da $a_i = \pm\sigma_i(\alpha_1, \ldots, \alpha_k)$ und $\sigma_i(\alpha_1, \ldots, \alpha_k)$ nur aus Summen und Produkten der Elemente $\alpha_1, \ldots, \alpha_k$ besteht, folgt aus der Homomorphismus-Eigenschaft von τ, dass

$$\tau(\sigma_i(\alpha_1, \ldots, \alpha_k)) = \sigma_i(\tau(\alpha_1), \ldots, \tau(\alpha_k)),$$

also zusammen

$$\sigma_i(\tau(\alpha_1), \ldots, \tau(\alpha_k)) = \tau(\sigma_i(\alpha_1, \ldots, \alpha_k)) = \sigma_i(\alpha_1, \ldots, \alpha_k)$$

für $i = 1, \ldots, k$. Aus dem Hauptsatz über symmetrische Polynome (siehe z.B. [1]) folgt dann $\{\tau(\alpha_1), \ldots, \tau(\alpha_k)\} = \{\alpha_1, \ldots, \alpha_k\}$, also $\tau(B') = B'$ und daher $\tau \in G_{B'}$, insgesamt also $H = G_{B'}$.

Des Weiteren ist $B \coloneqq G_{B'}(\alpha)$ ein Block von G, welcher α enthält und es gilt $G_{B'} = G_B$. Dies sieht man so: Offensichtlich ist $\mathrm{id} \in G_{B'}$ und damit $\alpha \in B$. Wir zeigen nun, dass B ein Block von G ist. Angenommen, es existiert ein $\tau \in G$ mit $B \cap \tau(B) \neq \varnothing$ und sei $\beta \in B \cap \tau(B)$. Da $B = G_{B'}(\alpha)$ gilt, gibt es $\sigma_1, \sigma_2 \in G_{B'}$ mit $\sigma_1(\alpha) = \beta = \tau\sigma_2(\alpha)$, also $\alpha = \sigma_1^{-1}\tau\sigma_2(\alpha)$. Folglich ist $\sigma_1^{-1}\tau\sigma_2 \in G_\alpha \subseteq G_{B'}$ und damit $\tau \in G_{B'}$. Daraus folgt $\tau(B) = \tau(G_{B'}(\alpha)) = G_{B'}(\alpha) = B$. Dies zeigt, dass B ein Block ist. Wir zeigen schließlich noch $G_B = G_{B'}$. Sei dazu $\tau \in G_B$, d.h. $\tau(B) = B$ und folglich $\tau(B) \cap B \neq \varnothing$. Die eben geführte Argumentation zeigt, dass dann $\tau \in G_{B'}$ gilt, also $G_B \subseteq G_{B'}$. Sei umgekehrt $\tau \in G_{B'}$. Da $G_{B'}$ eine Untergruppe von G ist, folgt $\tau G_{B'} = G_{B'}$. Damit ist

$$\tau(B) = \tau(G_{B'}(\alpha)) = \tau G_{B'}(\alpha) = G_{B'}(\alpha) = B.$$

Insgesamt folgt also $G_B = G_{B'}$. Damit haben wir $\mathbb{E} = \mathbb{L}^{G_B}$ für einen Block B, welcher α enthält, gezeigt. □

5.2 Divide et impera

Um die Auflösbarkeit des Polynoms f zu bestimmen, könnten wir nach Satz 2.16 einfach die Galoisgruppe G von f berechnen und überprüfen, ob diese auflösbar ist. Das Problem hierbei ist, dass die Kardinalität von G exponentiell im Grad von f sein kann und daher die Berechnung von

G nicht in polynomialer Zeit durchführbar wäre. Um dieses Problem zu umgehen, unterteilen wir die Körpererweiterung $\mathbb{Q}(\alpha)/\mathbb{Q}$ in eine Kette von Zwischenkörpern $\mathbb{Q} = \mathbb{Q}(\rho_r) \subset \mathbb{Q}(\rho_{r-1}) \subset \cdots \subset \mathbb{Q}(\rho_1) \subset \mathbb{Q}(\rho_0) = \mathbb{Q}(\alpha)$. Sei hierbei $g_i \in \mathbb{Q}(\rho_i)[X]$ das Minimalpolynom von ρ_{i-1} über $\mathbb{Q}(\rho_i)$, d.h. $\mathbb{Q}(\rho_{i-1}) \simeq \mathbb{Q}(\rho_i)[X]/g_i$ für $i = 1, \ldots, r$. Statt die Galoisgruppe G direkt zu berechnen, können wir nun für $i = 1, \ldots, r$ die Galoisgruppe G_i von g_i berechnen und deren Auflösbarkeit bestimmen. Der folgende Satz garantiert uns, dass f tatsächlich genau dann durch Radikale auflösbar ist, wenn die Polynome $g_1, \ldots, g_r$ durch Radikale auflösbar sind. Man beachte, dass hierbei nicht vorausgesetzt werden muss, dass G_i primitiv auf den Nullstellen von g_i wirkt.

Satz 5.3. *Sei $f \in \mathbb{Z}[X]$ irreduzibel und normiert mit $\deg(f) \geqslant 2$ und α eine Nullstelle von f. Seien weiter eine Kette von Körpern*

$$\mathbb{Q} = \mathbb{Q}(\rho_r) \subset \mathbb{Q}(\rho_{r-1}) \subset \cdots \subset \mathbb{Q}(\rho_1) \subset \mathbb{Q}(\rho_0) = \mathbb{Q}(\alpha)$$

und irreduzible Polynome $g_1 \in \mathbb{Q}(\rho_1)[X], \ldots, g_r \in \mathbb{Q}(\rho_r)[X]$ gegeben, sodass g_i das Minimalpolynom von ρ_{i-1} über $\mathbb{Q}(\rho_i)$ ist, für $i = 1, \ldots, r$. Dann ist f genau dann durch Radikale auflösbar, wenn für alle $i = 1, \ldots, r$ das Polynom g_i durch Radikale auflösbar ist.

Beweis. Wir zeigen die Aussage zunächst für $r = 2$. Seien also die Kette $\mathbb{Q} \subset \mathbb{Q}(\rho) \subset \mathbb{Q}(\alpha)$, sowie Polynome $h \in \mathbb{Q}[X]$ und $g \in \mathbb{Q}(\rho)[X]$ mit $\mathbb{Q}[X]/h \simeq \mathbb{Q}(\rho)$ und $\mathbb{Q}(\rho)[X]/g \simeq \mathbb{Q}(\alpha)$ gegeben. Nach Voraussetzung ist ρ eine Nullstelle von h und α eine Nullstelle von g. Wir zeigen, dass f genau dann durch Radikale auflösbar ist, wenn g und h durch Radikale auflösbar sind.

Seien $\alpha = \alpha_1, \ldots, \alpha_m$ die Nullstellen von f, sowie $\Omega \coloneqq \{\alpha_1, \ldots, \alpha_m\}$ und $\mathbb{L} \coloneqq \mathbb{Q}(\alpha_1, \ldots, \alpha_m)$ der Zerfällungskörper von f. Sei weiter $\mathbb{H} \subset \mathbb{L}$ der Zerfällungskörper von h (in Abb. 5.2 sind die in diesem Beweis eingeführten Körpererweiterungen schematisch dargestellt). Dann ist $H \coloneqq \mathrm{Gal}(h) = \mathrm{Gal}(\mathbb{H}/\mathbb{Q})$. Da $\mathbb{H}/\mathbb{Q}$ eine normale Körpererweiterung ist, ist nach Satz 2.13 die Gruppe $F \coloneqq \mathrm{Gal}(\mathbb{L}/\mathbb{H})$ ein Normalteiler von $G \coloneqq \mathrm{Gal}(f) = \mathrm{Gal}(\mathbb{L}/\mathbb{Q})$. Zudem folgt aus Satz 2.13, dass $G/F \simeq H$ gilt. Nach Satz 2.15 ist also $G = \mathrm{Gal}(f)$ genau dann auflösbar, wenn F und $H = \mathrm{Gal}(h)$ auflösbar sind.

Seien nun zunächst $H = \mathrm{Gal}(h)$ und $K \coloneqq \mathrm{Gal}(g)$ auflösbar. Wir wollen zeigen, dass dann auch F auflösbar ist und folglich auch G. Nach Satz 5.2 ist $\mathbb{Q}(\rho) = \mathbb{L}^{G_B}$ für einen Block $B = \{\alpha_1, \ldots, \alpha_k\} \subset \Omega$ von G, welcher α enthält und aus Satz 2.11 folgt

$$\mathrm{Gal}(\mathbb{L}/\mathbb{Q}(\rho)) = \mathrm{Gal}(\mathbb{L}/\mathbb{L}^{G_B}) = G_B \tag{1}$$

sowie

$$\mathrm{Gal}(\mathbb{L}/\mathbb{Q}(\alpha)) = \mathrm{Gal}(\mathbb{L}/\mathbb{L}^{G_\alpha}) = G_\alpha. \tag{2}$$

Sei $B = B_1 \coloneqq \sigma_1(B),\ B_2 \coloneqq \sigma_2(B),\ \ldots,\ B_l \coloneqq \sigma_l(B),\ \mathrm{id} = \sigma_1, \ldots, \sigma_l \in G$ ein vollständiges Blocksystem von G, das heißt

$$\Omega = \sigma_1(B) \dot\cup \ldots \dot\cup \sigma_l(B). \tag{3}$$

Behauptung 1. Es sind $\rho_1 \coloneqq \sigma_1(\rho), \ldots, \rho_l \coloneqq \sigma_l(\rho)$ die Nullstellen von h und $\alpha_1, \ldots, \alpha_k$ die Nullstellen von g.

Beweis der Behauptung 1. Die Nullstellen von h sind nach Satz 2.14 gegeben durch

$$\begin{aligned}\mathrm{Hom}_{\mathbb{Q}}(\mathbb{Q}(\rho), \overline{\mathbb{Q}})(\rho) &= \{\sigma(\rho) \mid \sigma \in \mathrm{Hom}_{\mathbb{Q}}(\mathbb{Q}(\rho), \overline{\mathbb{Q}})\} \\ &= \mathrm{Hom}_{\mathbb{Q}}(\mathbb{L}, \overline{\mathbb{Q}})(\rho) = G(\rho) \supseteq \{\sigma_1(\rho), \ldots, \sigma_l(\rho)\}.\end{aligned}$$

Zudem gilt $\deg(h) = l$, denn nach den Sätzen 2.1 und 2.2 sowie Satz 2.10 ist

$$\deg(h) = [\mathbb{Q}(\rho) : \mathbb{Q}] = \frac{[\mathbb{Q}(\alpha) : \mathbb{Q}]}{[\mathbb{Q}(\alpha) : \mathbb{Q}(\rho)]} = \frac{\deg(f)}{\deg(g)} = \frac{|\Omega|}{\deg(g)} \overset{(3)}{=} \frac{l \cdot |B|}{\deg(g)}$$

und

$$\begin{aligned}\deg(g) &= [\mathbb{Q}(\alpha) : \mathbb{Q}(\rho)] \\ &= \frac{[\mathbb{L} : \mathbb{Q}(\rho)]}{[\mathbb{L} : \mathbb{Q}(\alpha)]} = \frac{|\operatorname{Gal}(\mathbb{L}/\mathbb{Q}(\rho))|}{|\operatorname{Gal}(\mathbb{L}/\mathbb{Q}(\alpha))|} \overset{(1,2)}{=} \frac{|G_B|}{|G_\alpha|} = |B|,\end{aligned} \tag{4}$$

wobei die letzte Gleichheit aus Satz 3.13 folgt. Folglich sind die Nullstellen von h gegeben durch $\sigma_1(\rho), \ldots, \sigma_l(\rho)$.

Die Nullstellenmenge von g ist

$$\mathrm{Hom}_{\mathbb{Q}(\rho)}(\mathbb{Q}(\alpha), \overline{\mathbb{Q}})(\alpha) = \mathrm{Hom}_{\mathbb{Q}(\rho)}(\mathbb{L}, \overline{\mathbb{Q}})(\alpha) = \mathrm{Gal}(\mathbb{L}/\mathbb{Q}(\rho))(\alpha) \overset{(1)}{=} G_B(\alpha).$$

Da G transitiv auf Ω wirkt, $\alpha \in B$ gilt und $B \subset \Omega$ ein Block von G ist, folgt $G_B(\alpha) = B$. Außerdem gilt $\deg(g) = |B|$ (siehe (4)), also sind die Nullstellen von g durch $B = \{\alpha_1, \ldots, \alpha_k\}$ gegeben. △

Der Zerfällungskörper von h ist also $\mathbb{H} = \mathbb{Q}(\rho_1, \ldots, \rho_l)$.

Behauptung 2. Es gilt $\mathbb{Q}(\rho_i) = \mathbb{L}^{G_{B_i}}$.

Beweis der Behauptung 2. Es gilt

$$\mathbb{Q}(\rho_i) = \mathbb{Q}(\sigma_i(\rho)) = \sigma_i(\mathbb{Q}(\rho)) = \sigma_i\left(\mathbb{L}^{G_B}\right).$$

Zudem ist $\sigma_i\left(\mathbb{L}^{G_B}\right) = \mathbb{L}^{\sigma_i G_B \sigma_i^{-1}}$. Dies sieht man so: Sei $a \in \sigma_i\left(\mathbb{L}^{G_B}\right)$, d.h. es existiert ein $b \in \mathbb{L}^{G_B}$ mit $a = \sigma_i(b)$. Dann gilt für alle $\tau \in G_B$, dass

$$\sigma_i \tau \sigma_i^{-1}(a) = \sigma_i \tau(b) = \sigma_i(b) = a,$$

also $a \in \mathbb{L}^{\sigma_i G_B \sigma_i^{-1}}$. Sei umgekehrt $a \in \mathbb{L}^{\sigma_i G_B \sigma_i^{-1}}$ und setze $b \coloneqq \sigma_i^{-1}(a)$. Dann folgt für alle $\tau \in G_B$, dass

$$\sigma_i \tau(b) = \sigma_i \tau \sigma_i^{-1}(a) = a,$$

also $\tau(b) = \sigma_i^{-1}(a) = b$ und somit $b \in \mathbb{L}^{G_B}$. Demnach ist $a = \sigma_i(b) \in \sigma_i\left(\mathbb{L}^{G_B}\right)$, insgesamt also $\sigma_i\left(\mathbb{L}^{G_B}\right) = \mathbb{L}^{\sigma_i G_B \sigma_i^{-1}}$. Zuletzt gilt

$$\sigma_i G_B \sigma_i^{-1} = G_{B_i}, \tag{5}$$

denn sei $\sigma \in \sigma_i G_B \sigma_i^{-1}$. Dann gibt es ein $\tau \in G_B$ mit $\sigma = \sigma_i \tau \sigma_i^{-1}$. Folglich ist $\sigma(B_i) = \sigma_i \tau \sigma_i^{-1} \sigma_i(B) = \sigma_i \tau(B) = \sigma_i(B) = B_i$. Dies zeigt $\sigma_i G_B \sigma_i^{-1} \subseteq G_{B_i}$. Sei umgekehrt $\sigma \in G_{B_i}$ und setze $\tau \coloneqq \sigma_i^{-1} \sigma \sigma_i$. Dann folgt $\tau(B) = \sigma_i^{-1} \sigma \sigma_i(B) = \sigma_i^{-1} \sigma(B_i) = \sigma_i^{-1}(B_i) = B$, also $\tau \in G_B$ und damit $\sigma \in \sigma_i G_B \sigma_i^{-1}$. △

Mit Behauptung 2 folgt also $\mathrm{Gal}(\mathbb{L}/\mathbb{Q}(\rho_i)) = G_{B_i}$ für $i = 1, \ldots, l$. Wir erinnern daran, dass wir zeigen wollen, dass aus der Auflösbarkeit von $K = \mathrm{Gal}(g)$ die Auflösbarkeit von $F = \mathrm{Gal}(\mathbb{L}/\mathbb{H})$ folgt. Setze $\mathbb{L}_i \coloneqq \mathbb{Q}(\sigma_i(\alpha_1), \ldots, \sigma_i(\alpha_k))$ und $K_i \coloneqq \mathrm{Gal}(\mathbb{L}_i/\mathbb{Q}(\rho_i))$ für $i = 1, \ldots, l$ (vgl. Abbildung 5.2). Die Gruppe K_i ist also $G_{B_i} = \mathrm{Gal}(\mathbb{L}/\mathbb{Q}(\rho_i))$, eingeschränkt auf $\mathbb{L}_i$. Folglich gilt $K_i = (\sigma_i|_{\mathbb{L}_i}) K (\sigma_i^{-1}|_{\mathbb{L}_i})$ (vgl. (5)) und die Körper $K_1, \ldots, K_l$ sind isomorph. Außerdem gilt

$$K_1 = \mathrm{Gal}(\mathbb{L}_1/\mathbb{Q}(\rho_1)) = \mathrm{Gal}(\mathbb{Q}(\alpha_1, \ldots, \alpha_k)/\mathbb{Q}(\rho)) = \mathrm{Gal}(g) = K.$$

Die Idee ist nun die Folgende: Wir wollen zunächst zeigen, dass F isomorph zu einer Untergruppe von $K_1 \times \cdots \times K_l$ ist. Nach Satz 2.15 ist F auflösbar, wenn die Gruppen $K_1, \ldots, K_l$ auflösbar sind. Aufgrund der Isomorphie von $K_1, \ldots, K_l$ ist dies genau dann der Fall, wenn die Gruppe K auflösbar ist. Damit haben wir dann gezeigt, dass aus der Auflösbarkeit von K die Auflösbarkeit von F folgt. Wir führen hierfür folgende Abbildung ein:

$$\begin{aligned} \varphi : F &\to K_1 \times \cdots \times K_l \\ \tau &\mapsto (\tau|_{\mathbb{L}_1}, \ldots, \tau|_{\mathbb{L}_l}). \end{aligned}$$

Es sei an die Definition $K_i \coloneqq \mathrm{Gal}(\mathbb{L}_i/\mathbb{Q}(\rho_i))$ erinnert. Da $F = \mathrm{Gal}(\mathbb{L}/\mathbb{H}) = \mathrm{Gal}(\mathbb{L}/\mathbb{Q}(\rho_1, \ldots, \rho_l))$ gilt, hält jedes Element aus F die Mengen $\mathbb{Q}(\rho_1), \ldots, \mathbb{Q}(\rho_l)$ fest. Folglich ist die Abbildung wohldefiniert. Außerdem gilt für $\tau_1, \tau_2 \in F$, dass

$$\begin{aligned} \varphi(\tau_1 \circ \tau_2) &= \left((\tau_1 \circ \tau_2)|_{\mathbb{L}_1}, \ldots, (\tau_1 \circ \tau_2)|_{\mathbb{L}_l}\right) = \left(\tau_1|_{\mathbb{L}_1} \circ \tau_2|_{\mathbb{L}_1}, \ldots, \tau_1|_{\mathbb{L}_l} \circ \tau_2|_{\mathbb{L}_l}\right) \\ &= (\tau_1|_{\mathbb{L}_1}, \ldots, \tau_1|_{\mathbb{L}_l}) \circ (\tau_2|_{\mathbb{L}_1}, \ldots, \tau_2|_{\mathbb{L}_l}) = \varphi(\tau_1) \circ \varphi(\tau_2), \end{aligned}$$

also ist φ ein Homomorphismus. Sei weiter $\varphi(\tau_1) = \varphi(\tau_2)$. Daraus folgt $\tau_1|_{\mathbb{L}_i} = \tau_2|_{\mathbb{L}_i}$ für alle $i = 1, \ldots, l$ und da die Wirkung von τ_1 und τ_2 auf $\mathbb{L}$ eindeutig durch deren Wirkung auf $\mathbb{L}_1, \ldots, \mathbb{L}_l$ festgelegt sind, folgt $\tau_1 = \tau_2$,

also ist φ injektiv. Folglich ist $F \simeq \varphi(F) \leqslant K_1 \times \cdots \times K_l$. Insgesamt folgt aus der Auflösbarkeit von g und h die Auflösbarkeit von f.

Sei nun umgekehrt $G = \mathrm{Gal}(f)$ auflösbar. Nach Satz 2.15 ist dann auch $G/F \simeq H$ auflösbar und somit auch $H = \mathrm{Gal}(h)$. Die Gruppe $G_B = \mathrm{Gal}(\mathbb{L}/\mathbb{Q}(\rho))$ ist eine Untergruppe von $G = \mathrm{Gal}(\mathbb{L}/\mathbb{Q})$, also nach Satz 2.15 auflösbar. Sei weiter $U \coloneqq \mathrm{Gal}(\mathbb{L}/\mathbb{L}_1) \leqslant G_B$. Da $\mathbb{L}_1 = \mathbb{Q}(\alpha_1, \ldots, \alpha_k)$ der Zerfällungskörper von g ist, ist die Erweiterung $\mathbb{L}_1/\mathbb{Q}(\rho)$ normal. Daher ist nach Satz 2.13 die Gruppe U ein Normalteiler G_B. Nach Satz 2.15 ist also G_B/U auflösbar. Außerdem folgt aus Satz 2.13, dass $G_B/U \simeq \mathrm{Gal}(\mathbb{L}_1/\mathbb{Q}(\rho)) = K = \mathrm{Gal}(g)$. Also ist auch K auflösbar. Insgesamt folgt aus der Auflösbarkeit von f also auch die Auflösbarkeit von g und h.

Wir beweisen nun die allgemeine Aussage per Induktion über r. Den Induktionsanfang haben wir soeben gezeigt. Sei also die Kette $\mathbb{Q} \subset \mathbb{Q}(\rho_{r-1}) \subset \mathbb{Q}(\rho_{r-2}) \subset \cdots \subset \mathbb{Q}(\rho_1) \subset \mathbb{Q}(\alpha)$ sowie die Polynome $g_1, \ldots, g_r$ mit den Voraussetzungen aus dem Satz gegeben und sei h das Minimalpolynom von ρ_{r-2} über $\mathbb{Q}$. Dann ist f nach Induktionsvoraussetzung genau dann durch Radikale auflösbar, wenn $h, g_{r-2}, \ldots, g_1$ durch Radikale auflösbar sind. Der Beweis des Induktionsanfangs zeigt, dass h genau dann durch Radikale auflösbar, wenn g_r und g_{r-1} durch Radikale auflösbar sind. Daraus folgt die Behauptung. □

5.3 Polynome mit primitiver Galoisgruppe

Zunächst ist nicht sofort klar, wie wir die Reduktion der Auflösbarkeit von f auf die Auflösbarkeit der Polynome $g_1, \ldots, g_r$ nutzen können, um einen Vorteil bzgl. der Laufzeit zu erhalten. Statt der einen Galoisgruppe $G = \mathrm{Gal}(f)$ müssen wir nun die r Galoisgruppen $G_1 = \mathrm{Gal}(g_1), \ldots, G_r = \mathrm{Gal}(g_r)$ berechnen. Wäre die Körperkette

$$\mathbb{Q} = \mathbb{Q}(\rho_r) \subset \mathbb{Q}(\rho_{r-1}) \subset \cdots \subset \mathbb{Q}(\rho_1) \subset \mathbb{Q}(\rho_0) = \mathbb{Q}(\alpha)$$

beliebig gewählt, so kann weiterhin eine der Galoisgruppen G_i exponentiell groß sein. Die Körperkette und damit die Galoisgruppen G_i sollen also eine ganz spezielle Struktur haben: Wir wollen erreichen, dass die Galoisgruppe G_i primitiv auf den Nullstellen von g_i wirkt. Ist dies der Fall, so können wir, wie in Kapitel 4 beschrieben, tatsächlich die Auflösbarkeit der G_i und damit auch die Auflösbarkeit von G in polynomialer Zeit bestimmen.

Wir werden also im Folgenden an ganz speziellen Zwischenkörpern interessiert sein: Sei $\mathbb{Q} \subset \mathbb{E} \subset \mathbb{Q}(\alpha)$ ein Zwischenkörper und g das Minimalpolynom von α über $\mathbb{E}$. Der Zwischenkörper soll die Eigenschaft besitzen, dass die Galoisgruppe von g primitiv auf den Nullstellen von g wirkt. Folgender Satz gibt Aufschluss darüber, wie ein solcher Zwischenkörper gefunden werden kann. Die Darstellung orientiert sich dabei an [4, S. 43–47].

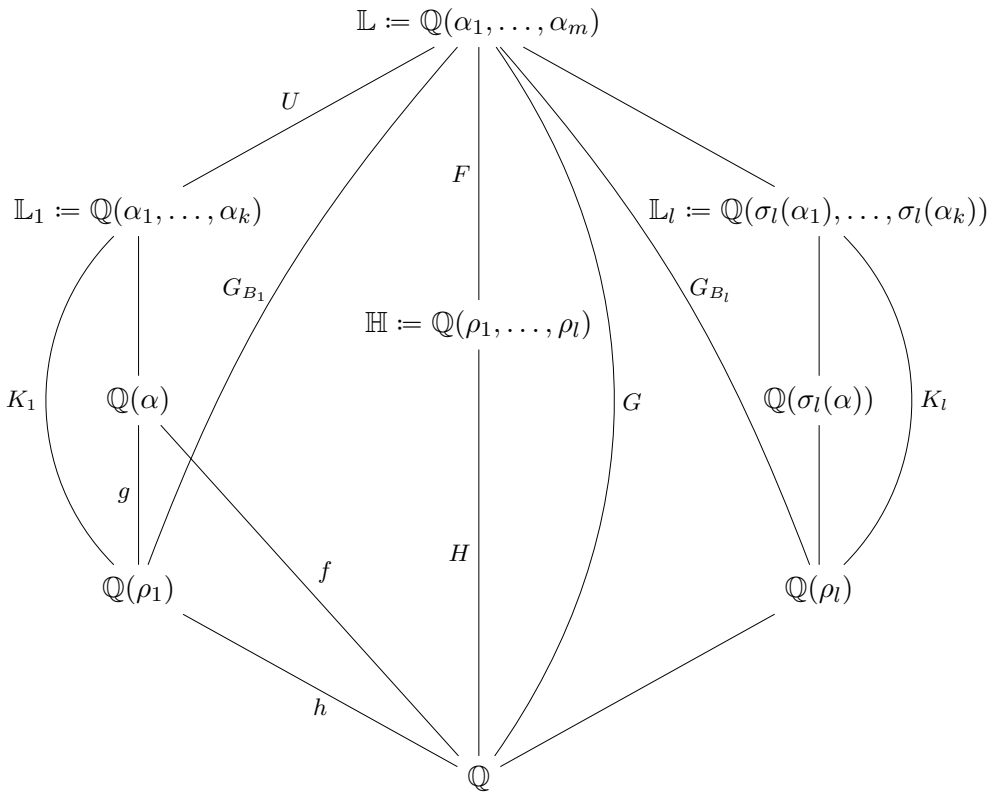

Abbildung 1: Schematische Darstellung der Körpererweiterungen im Beweis von Satz 5.3

Satz 5.4. *Sei $f \in \mathbb{Z}[X]$ ein irreduzibles und normiertes Polynom mit Nullstellen $\alpha = \alpha_1, \ldots, \alpha_m$ und Galoisgruppe G. Sei weiter $\Omega \coloneqq \{\alpha_1, \ldots, \alpha_m\}$ und $B \coloneqq \{\alpha_1, \ldots, \alpha_k\} \subseteq \Omega$ ein minimaler nichttrivialer Block von G. Setze*

$$g \coloneqq \prod_{i=1}^{k} X - \alpha_i =: X^k + a_1 X^{k-1} + \cdots + a_k \in \mathbb{Q}(a_1, \ldots, a_k)[X].$$

Dann gilt $\mathbb{Q} \subseteq \mathbb{Q}(a_1, \ldots, a_k) \subset \mathbb{Q}(\alpha)$ und die Galoisgruppe von g wirkt primitiv auf den Nullstellen von g.

Beweis. Sei $B \coloneqq \{\alpha_1, \ldots, \alpha_k\}$ ein minimaler nichttrivialer Block von G und

$$g \coloneqq (X - \alpha_1) \ldots (X - \alpha_k) =: X^k + a_1 X^{k-1} + \cdots + a_k \in \mathbb{Q}(a_1, \ldots, a_k)[X].$$

Wir zeigen zunächst die Aussage $\mathbb{Q}(a_1, \ldots, a_k) \subset \mathbb{Q}(\alpha)$. Die Zahlen $a_1, \ldots, a_k$ sind (bis auf Vorzeichen) die elementarsymmetrischen Polynome in k Variablen ausgewertet bei $\alpha_1, \ldots, \alpha_k$. Demnach gilt für alle $\sigma \in G_B = \{\sigma \in$

$G \mid \sigma(B) = B\}$, dass $\sigma(a_i) = a_i$ für $i = 1, \ldots, k$, also auch $\sigma(a) = a$ für alle $a \in \mathbb{Q}(a_1, \ldots, a_k)$ $(*)$. Dies impliziert $\mathbb{Q}(a_1, \ldots, a_k) \subseteq \mathbb{L}^{G_B}$ für $\mathbb{L} \coloneqq \mathbb{Q}(\alpha_1, \ldots, \alpha_m)$. Aus Satz 5.2 folgt aber, dass $\mathbb{L}^{G_B} \subset \mathbb{Q}(\alpha)$. Damit gilt auch $\mathbb{Q}(a_1, \ldots, a_k) \subset \mathbb{Q}(\alpha)$.

Sei $\mathbb{E} \coloneqq \mathbb{Q}(a_1, \ldots, a_k)$. Da die Nullstellen von $g \in \mathbb{E}[X]$ durch $\alpha_1, \ldots, \alpha_k$ gegeben sind, ist $\mathbb{E}(\alpha_1, \ldots, \alpha_k)$ der Zerfällungskörper von g und demnach

$$\begin{aligned} H \coloneqq \mathrm{Gal}(g) &= \mathrm{Gal}(\mathbb{E}(\alpha_1, \ldots, \alpha_k)/\mathbb{E}) = \mathrm{Gal}(\mathbb{Q}(\alpha_1, \ldots, \alpha_k)/\mathbb{E}) \\ &= \mathrm{Aut}_{\mathbb{E}}(\mathbb{Q}(\alpha_1, \ldots, \alpha_k)) \end{aligned}$$

die Galoisgruppe von g. Wir zeigen, dass $H = \mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\alpha_1, \ldots, \alpha_k)) =: H'$ gilt. Offensichtlich gilt $H \subseteq H'$. Da außerdem für $\sigma \in H'$ gilt, dass $\sigma(B) = B$ folgt $\sigma(a_i) = a_i$ für $i = 1, \ldots, k$ (siehe $(*)$) und damit $H' \subseteq H$. Die Galoisgruppe H eingeschränkt auf die Nullstellen $B = \{\alpha_1, \ldots, \alpha_k\}$ ist also gleich der Menge $G^B = \{\sigma|_B \mid \sigma \in G\}$.

Zuletzt zeigen wir, dass die Galoisgruppe H primitiv auf den Nullstellen B von g wirkt. Angenommen, es gibt einen Block $B' \subsetneq B$, $|B'| > 1$ von H, also auch von G^B. Dann ist nach Satz 3.12 die Menge B' aber auch ein Block von G, im Widerspruch zur Minimalität von B. Folglich wirkt $H = \mathrm{Gal}(g)$ primitiv auf den Nullstellen von g. $\square$

6 Faktorisierung von Polynomen über Zahlkörpern

Generalvoraussetzung 6.1. In diesem Kapitel sei stets $f \in \mathbb{Z}[X]$ ein irreduzibles, normiertes Polynom vom Grad $m \geqslant 2$ und $\alpha = \alpha_1, \ldots, \alpha_m$ die Nullstellen von f. Des Weiteren sei $\Omega = \{\alpha_1, \ldots, \alpha_m\}$ und $G = \mathrm{Gal}(f)$ die Galoisgruppe von f, welche auf der Nullstellenmenge Ω wirke.

Wie in Kapitel 4 erläutert, wollen wir eine Körperkette

$$\mathbb{Q} = \mathbb{Q}(\rho_r) \subset \mathbb{Q}(\rho_{r-1}) \subset \cdots \subset \mathbb{Q}(\rho_1) \subset \mathbb{Q}(\rho_0) = \mathbb{Q}(\alpha)$$

und irreduzible Polynome $g_1 \in \mathbb{Q}(\rho_1)[X], \ldots, g_r \in \mathbb{Q}(\rho_r)[X]$ konstruieren, sodass für $i = 1, \ldots, r$ gilt, dass

$$\mathbb{Q}(\rho_{i-1}) \simeq \mathbb{Q}(\rho_i)[X]/g_i$$

und die Galoisgruppe von g_i primitiv auf den Nullstellen von g_i wirkt. Hierfür müssen wir zunächst einen minimalen nichttrivialen Block B von G berechnen, welcher die Nullstelle α enthält. Satz 3.17 wird sich dabei als sehr nützlich erweisen: Wir erhalten B indem wir für eine geeignete Nullstelle $\beta \in \Omega \backslash \{\alpha\}$ die Menge $\langle G_\alpha, G_\beta \rangle(\alpha)$ berechnen. Die Untergruppen G_α und G_β der Galoisgruppe G korrespondieren nach dem Hauptsatz der Galoistheorie mit den Körpererweiterungen $\mathbb{Q}(\alpha)$ bzw. $\mathbb{Q}(\beta)$. In Kapitel 8.2 stellen wir ein Verfahren vor, wie man die Bahn von α bzgl. der Stabilisatoren G_α und G_β berechnen kann, ohne die Mengen G_α und G_β explizit zu kennen. Hierfür wird es notwendig sein, das Polynom f über $\mathbb{Q}(\alpha)$ bzw. $\mathbb{Q}(\beta)$ faktorisieren zu können.

Allgemeiner aufgefasst ist also das Ziel dieses Abschnitts die Faktorisierung eines gegebenen Polynoms $g \in \mathbb{Q}(\alpha)[X]$ in irreduzible Faktoren. Die erlangten Resultate wie auch deren Beweise sind dabei größtenteils [4] entnommen. Es ist bekannt (siehe z.B. [2]), wie man Polynome über $\mathbb{Q}$ effizient faktorisieren kann. Diese Kenntnis nutzen wir aus, indem wir folgende Reduktion vornehmen. Wir führen zunächst die *Norm* eines Polynoms ein, überführen dann g mithilfe der Norm in ein Polynom $r \in \mathbb{Q}[X]$, faktorisieren r in $\mathbb{Q}[X]$ und verwenden dies, um die Faktorisierung von g in $\mathbb{Q}(\alpha)[X]$ zu berechnen.

Definition 6.2. Sei $g \in \mathbb{Q}(\alpha)[X]$ und seien für $i = 1, \ldots, m$

$$\begin{aligned} \sigma_i : \mathbb{Q}(\alpha)[X] &\longrightarrow \mathbb{Q}(\alpha_i)[X] \\ \alpha &\longmapsto \alpha_i \\ X &\longmapsto X \end{aligned}$$

die kanonischen $\mathbb{Q}$-Isomorphismen. Die *Norm* von g ist definiert als

$$N_{\mathbb{Q}(\alpha)/\mathbb{Q}}(g) \coloneqq \prod_{i=1}^{m} \sigma_i(g) \in \mathbb{Q}[X].$$

Wenn klar ist, welche Körpererweiterung gemeint ist, schreiben wir einfach $N(g)$ anstelle von $N_{\mathbb{Q}(\alpha)/\mathbb{Q}}(g)$.

Beispiel 6.3. Sei $f \coloneqq X^2 + 1 \in \mathbb{Q}[X]$ mit Nullstellen $\alpha_1 = i$ und $\alpha_2 = -i$ und sei $g \coloneqq X^2 + 2iX \in \mathbb{Q}(i)[X]$. Dann ist

$$N(g) = (X^2 + 2iX)(X^2 - 2iX) = X^4 + 4X^2 \in \mathbb{Q}[X]. \qquad \triangle$$

Lemma 6.4. *Die Norm ist multiplikativ. Gilt also $g = g_1 g_2 \in \mathbb{Q}(\alpha)[X]$, so folgt $N(g) = N(g_1)N(g_2)$.*

Beweis. Dies folgt unmittelbar aus der Homomorphismen-Eigenschaft der σ_i:

$$N(g_1 g_2) = \prod_{i=1}^{m} \sigma_i(g_1 g_2) = \prod_{i=1}^{m} \sigma_i(g_1)\sigma_i(g_2) = N(g_1)N(g_2). \qquad \square$$

Möglicherweise kennen wir nur eine Nullstelle α von f, während uns die anderen Nullstellen $\alpha_2, \ldots, \alpha_m$ unbekannt sind. Auch in diesem Fall möchten wir die Norm eines Polynoms $g \in \mathbb{Q}(\alpha)[X]$ effizient berechnen können. Hierfür können wir uns die Resultante zu Nutze machen. Dafür ist es notwendig, jedes Vorkommen der algebraischen Zahl α in den Koeffizienten von g durch eine Unbestimmte T zu ersetzen. Dies erreichen wir wie folgt:

Definition 6.5. Sei $g = b_n X^n + b_{n-1} X^{n-1} + \cdots + b_0 \in \mathbb{Q}(\alpha)[X]$. Da α eine algebraische Zahl vom Grad m über $\mathbb{Q}$ ist, hat jeder Koeffizient b_i von g eine eindeutige Darstellung als $b_i = \sum_{j=0}^{m-1} b_{ij}\alpha^j$ mit $b_{ij} \in \mathbb{Q}$ für $i = 0, \ldots, n$, $j = 0, \ldots, m-1$. Wir bezeichnen mit

$$\Phi : \mathbb{Q}(\alpha)[X] \to \mathbb{Q}[T, X]$$

diejenige Abbildung, die bezüglich dieser Darstellung von Polynomen in $\mathbb{Q}(\alpha)[X]$ jedes Vorkommen von α durch die Unbestimmte T ersetzt, d.h.

$$\Phi\left(\sum_{i=0}^{n}\sum_{j=0}^{m-1} b_{ij}\alpha^j X^i\right) = \sum_{i=0}^{n}\sum_{j=0}^{m-1} b_{ij} T^j X^i \in \mathbb{Q}[T, X].$$

Beispiel 6.6. Sei die algebraische Zahl α vom Grad $m = 3$ über $\mathbb{Q}$ und $g = X^3 + 2\alpha^2 X - \alpha \in \mathbb{Q}(\alpha)[X]$. Dann ist

$$\Phi(g) = X^3 + 2T^2 X - T \in \mathbb{Q}[T, X]. \qquad \triangle$$

Mithilfe dieser Substitution können wir die Resultante verwenden, um die Norm eines Polynoms $g \in \mathbb{Q}(\alpha)[X]$ zu berechnen:

Satz 6.7. *Sei $g \in \mathbb{Q}(\alpha)[X]$ und Φ wie in Definition 6.5. Dann ist*

$$N(g) = \mathrm{Res}_T(f(T), \Phi(g)) \in \mathbb{Q}[X].$$

Beweis. Siehe [4, S. 18–20]. □

Nun, da wir die Norm von $g \in \mathbb{Q}(\alpha)[X]$ effizient berechnen können, kommen wir wieder zur eigentlichen Aufgabe zurück, der Faktorisierung von g in irreduzible Faktoren. Betrachten wir zunächst den Spezialfall, dass $N(g)$ quadratfrei ist. Dann lässt sich die Faktorisierung von g wie folgt berechnen.

Satz 6.8. *Sei $g \in \mathbb{Q}(\alpha)[X]$ ein normiertes Polynom für welches $r \coloneqq N(g)$ quadratfrei ist und sei $r = \prod_i r_i$ die Faktorisierung von r in irreduzible Polynome in $\mathbb{Q}[X]$. Dann ist*

$$g = \prod_i \mathrm{ggT}(g, r_i)$$

die Faktorisierung von g in irreduzible Faktoren in $\mathbb{Q}(\alpha)[X]$.

Lemma 6.9. *Sei $g \in \mathbb{Q}(\alpha)[X]$ irreduzibel. Dann ist $N(g)$ eine Potenz eines irreduziblen Polynoms in $\mathbb{Q}[X]$.*

Beweis. Angenommen $N(g) = \prod_{i=1}^{m} \sigma_i(g) = r_1 r_2$ mit $r_1, r_2 \in \mathbb{Q}[X]$ und $\mathrm{ggT}(r_1, r_2) = 1$. Dann gilt o.B.d.A. $g = \sigma_1(g) \mid r_1$, da g irreduzibel ist, d.h. es existiert ein $h \in \mathbb{Q}(\alpha)[X]$ mit $gh = r_1$. Dann folgt für alle $i = 1, \ldots, m$, dass $\sigma_i(g)\sigma_i(h) = \sigma_i(gh) = \sigma_i(r_1) = r_1$, also $\sigma_i(g) \mid r_1$ und da r_1 und r_2 teilerfremd sind, gilt $\sigma_i(g) \nmid r_2$. Damit folgt $N(g) \mid r_1$ und $r_2 = 1$. □

Beweis von Satz 6.8. Sei $g = \prod_{i=1}^{k_1} g_i$ die Faktorisierung von g in irreduzible Faktoren in $\mathbb{Q}(\alpha)[X]$. Dann folgt mit der Multiplikativität der Norm, dass

$$\prod_{i=1}^{k_2} r_i = r = N(g) = \prod_{i=1}^{k_1} N(g_i).$$

Das Polynom g_i ist für alle $i = 1, \ldots, k_1$ irreduzibel, also ist $N(g_i)$ nach Lemma 6.9 eine Potenz eines irreduziblen Polynoms in $\mathbb{Q}[X]$. Da aber r quadratfrei ist, folgt, dass $N(g_i)$ irreduzibel ist. Dies impliziert $k_1 = k_2 \eqqcolon k$ und o.B.d.A. $r_i = N(g_i)$. Aus der Quadratfreiheit von r folgt außerdem, dass g quadratfrei ist und nach Satz 2.6, dass r separabel ist. Damit ist

$$\mathrm{ggT}(g, r_i) = \mathrm{ggT}(g, N(g_i)) = \mathrm{ggT}\left(\prod_{j=1}^{k} g_j \,,\, \prod_{l=1}^{m} \sigma_l(g_i)\right) \eqqcolon \tilde{g}.$$

Zunächst gilt $g_i = \sigma_1(g_i) \mid \tilde{g}$ und $g_i^2 \nmid \tilde{g}$, da g quadratfrei ist. Angenommen, es existiert ein $j \in \{1, \ldots, k\} \backslash \{i\}$ und ein $l \in \{1, \ldots, m\}$ mit $g_j \mid \tilde{g}$, d.h. $\sigma_l(g_i) = g_j$. Damit folgt $g_j^2 = g_j \sigma_l(g_i) \mid N(g_j)N(g_i) = r_j r_i \mid r$. Dies ist jedoch ein Widerspruch zur Separabilität von r. Insgesamt ergibt sich also $\mathrm{ggT}(g, r_i) = g_i$. □

Beispiel 6.10. Wir wollen im Folgenden die Faktorisierung des Polynoms

$$g \coloneqq X^3 - 8iX^2 - 19X + 12i \in \mathbb{Q}(i)[X]$$

mithilfe von Satz 6.8 berechnen. Zunächst gilt

$$\begin{aligned} r \coloneqq N(g) &= (X^3 - 8iX^2 - 19X + 12i)(X^3 + 8iX^2 - 19X - 12i) \\ &= X^6 + 26X^4 + 169X^2 + 144 \in \mathbb{Q}[X]. \end{aligned}$$

Die Faktorisierung von r ist gegeben durch $r = r_1 r_2 r_3$ mit $r_1 \coloneqq X^2 + 16$, $r_2 \coloneqq X^2 + 9$ und $r_3 \coloneqq X^2 + 1$. Das Polynom r ist also quadratfrei, d.h. die Voraussetzungen von Satz 6.8 sind erfüllt. Es gilt $\mathrm{ggT}(g, r_1) = X - 4i$, $\mathrm{ggT}(g, r_2) = X - 3i$ und $\mathrm{ggT}(g, r_3) = X - i$. Folglich ist die Faktorisierung von g über $\mathbb{Q}(i)$ gegeben durch

$$g = X^3 - 8iX^2 - 19X + 12i = (X - 4i)(X - 3i)(X - i). \qquad \triangle$$

Wir wissen nun also, wie man die Faktorisierung eines Polynoms $g \in \mathbb{Q}(\alpha)[X]$ berechnen kann für den Fall, dass $N(g)$ quadratfrei ist. Ist $N(g)$ hingegen nicht quadratfrei, so können wir g zu einem Polynom $g(X - c\alpha)$, $c \in \mathbb{Z}$, modifizieren, so dass $N(g(X - c\alpha))$ quadratfrei ist. Dies wird in Satz 6.11 beschrieben. Anschließend können wir Satz 6.8 verwenden, um $g(X - c\alpha)$ über $\mathbb{Q}(\alpha)$ zu faktorisieren. Schließlich erhalten wir aus der Faktorisierung von $g(X - c\alpha)$ die Faktorisierung von g.

Satz 6.11. *Sei $g \in \mathbb{Q}(\alpha)[X]$ ein quadratfreies Polynom vom Grad n. Dann gibt es höchstens $(nm)^2$ ganze Zahlen c, so dass $N(g(X - c\alpha))$ nicht quadratfrei ist.*

Beweis. Wir zeigen, dass es nicht mehr als $(nm)^2$ ganze Zahlen c gibt, so dass $N(g(X - c\alpha))$ mehrfache Nullstellen hat. Es gilt

$$N(g(X - c\alpha)) = \prod_{i=1}^{m} \sigma_i(g(X - c\alpha)) = \prod_{i=1}^{m} \sigma_i(g)(X - c\alpha_i).$$

Seien $\beta_1^i, \ldots, \beta_n^i$ die Nullstellen von $\sigma_i(g)$. Folglich sind die Nullstellen von $N(g(X - c\alpha))$ gegeben durch $\beta_j^i + c\alpha_i$, $i = 1, \ldots, m$, $j = 1, \ldots, n$. Das Polynom $N(g(X - c\alpha))$ hat genau dann mehrfache Nullstellen, wenn es i, j, k, l gibt mit $(i, j) \neq (k, l)$, so dass $\beta_j^i + c\alpha_i = \beta_l^k + c\alpha_k$ gilt. Es gibt offenbar weniger als $(mn)^2$ ganze Zahlen c, die dies erfüllen. $\square$

Mit Satz 6.8 können wir jetzt also die Faktorisierung von $g(X - c\alpha)$ in $\mathbb{Q}(\alpha)[X]$ berechnen. Daraus erhalten wir dann die Faktorisierung von g:

Korollar 6.12. *Sei $c \in \mathbb{Z}$ so gewählt, dass $r \coloneqq N(g(X - c\alpha)) \in \mathbb{Q}[X]$ quadratfrei ist und sei $r = \prod_i r_i$ die Faktorisierung von r in irreduzible Faktoren. Dann ist*

$$g = \prod_i \mathrm{ggT}(g, r_i(X + c\alpha))$$

die Faktorisierung von g in irreduzible Faktoren in $\mathbb{Q}(\alpha)[X]$.

Beweis. Nach Satz 6.8 ist $g(X - c\alpha) = \prod_i \mathrm{ggT}(g(X - c\alpha), r_i)$ und daher ist $g = \prod_i \mathrm{ggT}(g, r_i(X + c\alpha))$ die Faktorisierung von g in irreduzible Faktoren in $\mathbb{Q}(\alpha)[X]$. □

Beispiel 6.13. Betrachte das Polynom

$$g \coloneqq X^3 + iX^2 + 2X \in \mathbb{Q}(i)[X].$$

Für dieses gilt

$$\begin{aligned} N(g) &= (X^3 + iX^2 + 2X)(X^3 - iX^2 + 2X) = X^6 + 5X^4 + 4X^2 \\ &= (X^2 + 4)(X^2 + 1)X^2 \in \mathbb{Q}[X]. \end{aligned}$$

Die Norm von g ist also nicht quadratfrei. Betrachte nun

$$g(X - 3i) = X^3 - 8iX^2 - 19X + 12i.$$

Aus Beispiel 6.10 kennen wir bereits die Faktorisierung von $g(X - 3i)$:

$$g(X - 3i) = (X - i)(X - 3i)(X - 4i).$$

Folglich ist Faktorisierung von g gegeben durch

$$g = X^3 + iX^2 + 2X = (X + 2i)X(X - i).$$ △

7 Berechnung von Galoisgruppen

Es sei wieder $f \in \mathbb{Z}[X]$ ein irreduzibles und normiertes Polynom vom Grad $m \geqslant 2$ und $\alpha = \alpha_1, \ldots, \alpha_m$ die Nullstellen von f. Weiter seien $\Omega = \{\alpha_1, \ldots, \alpha_m\}$ und G die Galoisgruppe von f, welche auf der Menge Ω wirke.

Wie in Kapitel 4 beschrieben, wollen wir eine Körperkette

$$\mathbb{Q} = \mathbb{Q}(\rho_r) \subset \cdots \subset \mathbb{Q}(\rho_1) \subset \mathbb{Q}(\rho_0) = \mathbb{Q}(\alpha)$$

sowie Polynome $g_1 \in \mathbb{Q}(\rho_1)[X], \ldots, g_r \in \mathbb{Q}(\rho_r)$ berechnen mit $\mathbb{Q}(\rho_i)/g_i \simeq \mathbb{Q}(\rho_{i-1})$ für $i = 1, \ldots, r$ und die Frage nach der Auflösbarkeit der Galoisgruppe G von f auf die Frage nach der Auflösbarkeit der Galoisgruppen G_i von g_i, $i = 1, \ldots, r$ zurückführen. Um diese zu beantworten, müssen wir die Galoisgruppen G_i explizit berechnen.

In diesem Kapitel beschäftigen wir uns also mit der Aufgabe, die Galoisgruppe H eines beliebigen irreduzibles Polynoms $g \in \mathbb{K}[X]$ zu berechnen, wobei $\mathbb{K}$ ein algebraischer Zahlkörper sei. Die folgende Darstellung orientiert sich an [4, S. 55–58]. Die Idee zur Berechnung von H ist die Folgende. Seien $\beta_1, \ldots, \beta_m$ die Nullstellen von g. Wir wollen mithilfe der Ergebnisse aus Kapitel 6 ein Polynom $h \in \mathbb{K}[X]$ konstruieren, so dass $\mathbb{K}[X]/h$ isomorph zum Zerfällungskörper $\mathbb{K}(\beta_1, \ldots, \beta_m)$ von g ist. Wir konstruieren das Polynom h derart, dass h über $\mathbb{K}(\beta_1, \ldots, \beta_m)$ in Linearfaktoren zerfällt. Seien dann $\tau = \tau_1, \ldots, \tau_n$ die Nullstellen von h. Da h über $\mathbb{K}(\beta_1, \ldots, \beta_m)$ in Linearfaktoren zerfällt, gilt also

$$\mathbb{K}(\beta_1, \ldots, \beta_m) \simeq \mathbb{K}[X]/h \simeq \mathbb{K}(\tau) = \mathbb{K}(\tau_1, \ldots, \tau_n).$$

Nach den Sätzen 2.2 und 2.10 ist $|H| = \deg(h) = n$. Es wirkt also die n-elementige Gruppe H transitiv auf der ebenfalls n-elementigen Menge $\{\tau_1, \ldots, \tau_n\}$. Folglich gibt es Abbildungen $\sigma_1, \ldots, \sigma_n$ mit $H = \{\sigma_1, \ldots, \sigma_n\}$ und $\sigma_i(\tau) = \tau_i$ für $i = 1, \ldots, n$. Da außerdem $\mathbb{K}(\beta_1, \ldots, \beta_m) = \mathbb{K}(\tau)$ gilt, gibt es Polynome $q_1, \ldots, q_m \in \mathbb{K}[T]$ mit $q_1(\tau) = \beta_1, \ldots, q_m(\tau) = \beta_m$. Da g über $\mathbb{Q}(\tau)$ in Linearfaktoren zerfällt, können wir anhand der Faktorisierung von g über $\mathbb{Q}(\tau)$ die Polynome $q_1, \ldots, q_m$ direkt ablesen. Damit lässt sich die Wirkung von H auf den Nullstellen $\beta_1, \ldots, \beta_m$ einfach bestimmen: Für $i = 1, \ldots, n$ und $j = 1, \ldots, m$ gilt $\sigma_i(\beta_j) = \sigma_i(q_j(\tau)) = q_j(\sigma_i(\tau)) = q_j(\tau_i)$.

7.1 Algorithmus: GALOIS

Eingabe: $g \in \mathbb{K}[X]$, ein irreduzibles Polynom vom Grad m, wobei $\mathbb{K}$ ein algebraischer Zahlkörper sei

Ausgabe: $H = \{\sigma_1, \ldots, \sigma_n\}$, die Galoisgruppe von g über $\mathbb{K}$. Die Gruppe H wird hierbei als zweidimensionale Liste kodiert sein. Gilt dann $H[i][j] = k$, so bedeutet dies $\sigma_i(\beta_j) = \beta_k$, wobei $\beta_1, \ldots, \beta_m$ die Nullstellen von g seien.

Schritt 1: $h \leftarrow g$

Schritt 2: Finde ein $c \in \mathbb{N}$, so dass

$r \coloneqq \mathrm{Res}_T(h(T), g(X - cT)) \in \mathbb{K}[X]$

quadratfrei ist

[Dann ist $r = N_{\mathbb{K}(\tau)/\mathbb{K}}(g(X - c\tau)) \in \mathbb{K}[X]$ für eine Nullstelle τ von h, vgl. Satz 6.7 und Satz 6.11]

Schritt 3: Faktorisiere $r = \prod_{i=1}^{k} r_i$ in $\mathbb{K}[X]$

[siehe Kapitel 6]

Schritt 4: Falls es ein r_i gibt mit $\deg(r_i) > \deg(h)$, dann

$h \leftarrow r_i$ und gehe zu Schritt 2

Sonst $n \leftarrow \deg(h)$

[Dann ist $\mathbb{K}[X]/h$ isomorph zum Zerfällungskörper von g, vgl. Beweis von Satz 7.2]

Schritt 5: Für $i = 1, \ldots, m$ führe aus:

$\tau \leftarrow$ Restklasse von Z in $\mathbb{K}[Z]/h$

[Fasse im Folgenden $\mathbb{K}[Z]/h$ als Körpererweiterung $\mathbb{K}(\tau)$ auf]

$X - \beta_i \leftarrow \mathrm{ggT}\left(r_i(X + c\tau), g(X)\right) \in \mathbb{K}(\tau)[X]$

[Dann ist $g = \prod_{i=1}^{m}(X - \beta_i)$ die Faktorisierung von g in Linearfaktoren über $\mathbb{K}(\tau)$, vgl. Korollar 6.12]

Schritt 6: Faktorisiere $h = \prod_{i=1}^{n}(X - \tau_i)$ in $\mathbb{K}(\tau)[X]$

[Dass h über $\mathbb{K}(\tau)$ tatsächlich in Linearfaktoren zerfällt, wird im Beweis von Satz 7.2 gezeigt.]

Schritt 7: $\Phi \leftarrow$ Abbildung $\mathbb{K}(\tau) \to \mathbb{K}[T]$ mit

$\tau \mapsto T,\ k \mapsto k$ für alle $k \in \mathbb{K}$

[τ wird durch die Unbestimmte T ersetzt, vgl. Definition 6.5]

Für $j = 1, \ldots, m$ führe aus:

$q_j \leftarrow \Phi(\beta_j)$

[q_j sind dann die Polynome aus $\mathbb{K}[T]$ mit $q_j(\tau) = \beta_j$]

Für $i = 1, \ldots, n$ führe aus:

Für $l = 1, \ldots, m$ führe aus:

Falls $q_j(\tau_i) = \beta_l$, dann $H[i][j] \leftarrow l$

Schritt 8: Gib H aus.

Beispiel 7.1. Sei $g = X^3 - 7X + 7 \in \mathbb{Q}[X]$. Wir wollen mithilfe des Algorithmus GALOIS die Galoisgruppe von g berechnen. Wir setzen in Schritt 1 zunächst $h \leftarrow g$ und stellen in Schritt 2 fest, dass für $c = 2$ das Polynom

$$\begin{aligned} r &\coloneqq \operatorname{Res}_T(h(T), g(X - cT)) \\ &= X^9 - 105X^7 + 189X^6 + 3087X^5 \\ &\qquad - 7938X^4 - 27832X^3 + 83349X^2 + 3087X - 9261 \in \mathbb{Q}[X] \end{aligned}$$

quadratfrei ist. Die Faktorisierung von r ist gegeben durch

$$r = (X^3 - 63X + 189)(X^3 - 21X - 7)(X^3 - 21X + 7).$$

Da kein irreduzibler Faktor von r einen größeren Grad als h hat, ist $\mathbb{Q}[X]/h = \mathbb{Q}[X]/g$ isomorph zum Zerfällungskörper von g (siehe Beweis von Satz 7.2) und wir gehen zu Schritt 5.

Wir setzen nun $\tau \leftarrow Z + (h) \in \mathbb{Q}[Z]/h$ und fassen $\mathbb{Q}[Z]/h$ als Körpererweiterung $\mathbb{Q}(\tau)$ auf. Als nächstes faktorisieren wir $h = g$ über $\mathbb{Q}(\tau)$:

$$g = \big(X - \tau\big)\big(X - (3\tau^2 + 4\tau - 14)\big)\big(X - (-3\tau^2 - 5\tau + 14)\big).$$

Die Nullstellen von g und h sind also gegeben durch

$$\begin{aligned} \beta_1 = \tau_1 &\coloneqq \tau, \\ \beta_2 = \tau_2 &\coloneqq 3\tau^2 + 4\tau - 14, \\ \beta_3 = \tau_3 &\coloneqq -3\tau^2 - 5\tau + 14. \end{aligned}$$

In Schritt 7 werden die Polynome $q_j \in \mathbb{Q}[X]$ bestimmt, für die $q_j(\tau) = \beta_j$ gilt. Diese können direkt anhand der Faktorisierung von g abgelesen werden:

$$q_1 = X, \quad q_2 = 3X^2 + 4X - 14, \quad q_3 = -3X^2 - 5X + 14.$$

Da nun z.B.

$$\begin{aligned} q_3(\tau_2) &= -27\tau^4 - 72\tau^3 + 189\tau^2 + 316\tau - 504 \\ &= (-27\tau - 72)(\tau^3 - 7\tau + 7) + \tau \\ &= (-27\tau - 72)h(\tau) + \tau = \tau = \beta_1 \end{aligned}$$

gilt, wird $H[2][3] \leftarrow 1$ zugewiesen. Analog ergeben sich die anderen Werte von H. Insgesamt ergibt sich dann

$$H = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{bmatrix}$$

das heißt die Galoisgruppe H von g ist durch die alternierende Gruppe $\mathcal{A}_3$ gegeben. △

7.2 Korrektheit des Algorithmus

Satz 7.2. *Der Algorithmus* GALOIS *arbeitet korrekt.*

Beweis. Behauptung 1. Die Schritte 1 – 4 berechnen ein Polynom $h \in \mathbb{K}[X]$, so dass $\mathbb{K}[X]/h$ isomorph zum Zerfällungskörper von g ist.

Beweis der Behauptung 1. Die Nullstellen $\beta_1, \ldots, \beta_m$ von g seien o.B.d.A. so geordnet, dass $\beta_{i+1} \notin \mathbb{K}(\beta_1, \ldots, \beta_i)$ für $i < t$ und $\beta_{i+1} \in \mathbb{K}(\beta_1, \ldots, \beta_i)$ für $i \geqslant t$ für ein $t \in \mathbb{N}$.

Wir zeigen per Induktion, dass für jedes $i \leqslant t$ gilt: Vor dem i-ten Durchlauf von Schritt 2 ist

$$\mathbb{K}[X]/h \simeq \mathbb{K}(\lambda_i) = \mathbb{K}(\beta_1, \ldots, \beta_i)$$

mit $\lambda_i \coloneqq \beta_i + c_{i-1}\beta_{i-1} + c_{i-1}c_{i-2}\beta_{i-2} + \cdots + c_{i-1}c_{i-2}\ldots c_1\beta_1$, wobei c_j das im j-ten Durchlauf von Schritt 2 berechnete c sei.

Für $i = 1$ gilt $h = g$ und daher $\mathbb{K}[X]/h \simeq \mathbb{K}(\beta_1)$. Es gelte nun

$$\mathbb{K}[X]/h \simeq \mathbb{K}(\lambda_i) = \mathbb{K}(\beta_1, \ldots, \beta_i)$$

vor dem i-ten Durchlauf von Schritt 2 für ein beliebiges aber festes $i \leqslant t$. Es sei $g = \prod_{j=1}^{k} g_j$ die Faktorisierung von g in irreduzible Faktoren über $\mathbb{K}(\lambda_i)$ und

$$r \coloneqq N_{\mathbb{K}(\lambda_i)/\mathbb{K}}(g(X - c_i\lambda_i)) = \prod_{j=1}^{k} N_{\mathbb{K}(\lambda_i)/\mathbb{K}}(g_j(X - c_i\lambda_i)) =: \prod_{j=1}^{k} r_j \in \mathbb{K}[X].$$

Ist g_j vom Grad l, so ist $r_j = N_{\mathbb{K}(\lambda_i)/\mathbb{K}}(g_j(X - c\lambda_i))$ ein Polynom vom Grad $l \cdot [\mathbb{K}(\lambda_i) : \mathbb{K}] = l \cdot \deg(h)$. Ist $\mathbb{K}(\lambda_i)$ der Zerfällungskörper von g, so gilt $k = m$ und $\deg(g_j) = 1$, also $\deg(r_j) = \deg(h)$ für $j = 1, \ldots, m$. Es gilt also $i = t$ und es wird kein weiteres Mal zu Schritt 2 gesprungen. Andernfalls hat g über $\mathbb{K}(\lambda_i)$ einen irreduziblen Faktor g_j mit $\deg(g_j) \geqslant 2$ und Nullstelle β_{i+1} und es folgt $\deg(r_j) = \deg(N(g_j(X - c\lambda_i))) > \deg(h)$. Da β_{i+1} Nullstelle von g_j ist, ist $\lambda_{i+1} = \beta_{i+1} + c_i\lambda_i$ Nullstelle von $r_j = N(g_j(X - c_i\lambda_i))$. Somit gilt

$$\mathbb{K}[X]/r_j \simeq \mathbb{K}(\beta_{i+1} + c_i\lambda_i).$$

Da außerdem nach den Sätzen 2.1 und 2.2 gilt, dass

$$\begin{aligned}[\mathbb{K}(\beta_{i+1} + c_i\lambda_i) : \mathbb{K}] &= \deg(r_j) = \deg(g_j)\deg(h) \\ &= [\mathbb{K}(\beta_{i+1}, \lambda_i) : \mathbb{K}(\lambda_i)][\mathbb{K}(\lambda_i) : \mathbb{K}] = [\mathbb{K}(\beta_{i+1}, \lambda_i) : \mathbb{K}],\end{aligned}$$

folgt mit der Induktionsvoraussetzung, dass

$$\mathbb{K}[X]/r_j \simeq \mathbb{K}(\beta_{i+1} + c_i\lambda_i) = \mathbb{K}(\beta_{i+1}, \lambda_i) = \mathbb{K}(\beta_1, \ldots, \beta_{i+1}).$$

In Schritt 4 wird schließlich h auf r_j gesetzt. △

Behauptung 2. Sei τ eine Nullstelle von h. Das Polynom h zerfällt über $\mathbb{K}(\tau) \simeq \mathbb{K}[X]/h$ in Linearfaktoren.

Beweis der Behauptung 2. Es bezeichne h_i das im i-ten Durchlauf von Schritt 4 berechnete h und $h_0 \coloneqq g$. Wir zeigen per Induktion über i, dass die Nullstellen von h_i in $\mathbb{L} \coloneqq \mathbb{K}(\beta_1, \ldots, \beta_m)$ enthalten sind.

Für $i = 0$ gilt $h_i = g$ und die Aussage ist trivial. Betrachte nun den $i+1$-ten Durchgang. Sei λ_i wie im Beweis von Behauptung 1, also $\mathbb{K}[X]/h_i \simeq \mathbb{K}(\lambda_i)$ und $r = N_{\mathbb{K}(\lambda_i)/\mathbb{K}}(g(X - c_i\lambda_i))$. Seien weiter $\lambda_i = \gamma_1, \ldots, \gamma_k$ die Nullstellen von h_i. Nach Induktionsvoraussetzung sind diese $\mathbb{L}$ enthalten. Seien $\sigma_j : \mathbb{K}(\gamma_1)[X] \to \mathbb{K}(\gamma_j)[X],\ j = 1, \ldots, k$ die kanonischen $\mathbb{K}$-Homomorphismen (vgl. Definition 6.2). Dann gilt

$$r = N_{\mathbb{K}(\gamma_1)/\mathbb{K}}(g(X - c_i\gamma_1)) = \prod_j \sigma_j(g(X - c_i\gamma_1)) = \prod_j g(X - c_i\gamma_j).$$

Da $\beta_1, \ldots, \beta_m$ die Nullstellen von g sind, sind

$$\{\beta_j + c_i\gamma_l \mid i = 1, \ldots, m,\ l = 1, \ldots, k\} \subset \mathbb{L}$$

die Nullstellen von r. Sei nun r' der in Schritt 4 gefundene Faktor von r mit $\deg(r') > \deg(h_i)$. Dann folgt $h_{i+1} = r'$ und die Nullstellen von h_{i+1} sind in denen von r und damit in $\mathbb{L}$ enthalten. △

Es gilt also $\mathbb{K}(\beta_1, \ldots, \beta_m) = \mathbb{K}(\tau) = \mathbb{K}(\tau_1, \ldots, \tau_n) \simeq \mathbb{K}[X]/h$, wobei $\tau = \tau_1, \ldots, \tau_n$ die Nullstellen von h seien. Die Wirkung von $H = \mathrm{Gal}(g)$ auf den Nullstellen von g kann nun wie folgt bestimmt werden: Da $\mathbb{K}(\tau) = \mathbb{K}(\beta_1, \ldots, \beta_m)$, gibt es Polynome $q_1, \ldots, q_m \in \mathbb{K}[X]$ mit $q_j(\tau) = \beta_j$. Diese können anhand der Faktorisierung von g in Linearfaktoren über $\mathbb{K}(\tau)$ direkt abgelesen werden. Nach den Sätzen 2.2 und 2.10 ist $|H| = \deg(h) = n$. Aufgrund der transitiven Wirkung der n-elementigen Gruppe H auf der n-elementigen Menge $\{\tau_1, \ldots, \tau_n\}$ gibt es Abbildungen $\sigma_1, \ldots, \sigma_n$ mit $H = \{\sigma_1, \ldots, \sigma_n\}$ und $\sigma_i(\tau) = \tau_i$. Es folgt

$$\sigma_i(\beta_j) = \sigma_i(q_j(\tau)) = q_j(\sigma_i(\tau)) = q_j(\tau_i) = \beta_l,$$

für ein $l \in \{1, \ldots, m\}$. Damit ist die Wirkung von H auf den Nullstellen von g bestimmt. □

7.3 Abbruchkriterium

Es sei wieder $f \in \mathbb{Z}[X]$ ein irreduzibles und normiertes Polynom mit $\deg(f) \geqslant 2$ und α eine Nullstelle von f. Um die Auflösbarkeit von f zu bestimmen, wollen wir, wie bereits beschrieben, eine Körperkette

$$\mathbb{Q} = \mathbb{Q}(\rho_r) \subset \cdots \subset \mathbb{Q}(\rho_1) \subset \mathbb{Q}(\alpha)$$

und irreduzible Polynome $g_i \in \mathbb{Q}(\rho_i)[X]$ konstruieren, so dass $\mathbb{Q}(\rho_i)[X]/g_i \simeq \mathbb{Q}(\rho_{i-1})$ und die Galoisgruppe G_i von g_i primitiv auf den Nullstellen von g_i

wirkt. Anschließend führen wir die Auflösbarkeit von f auf die Auflösbarkeit der Galoisgruppen $G_1, \ldots, G_r$ zurück. Wie in Kapitel 4 beschrieben, wollen wir die Galoisgruppen G_i mittels des Algorithmus GALOIS nur dann vollständig berechnen, wenn die Kardinalität von G_i unterhalb einer gewissen Schranke λ ist. Andernfalls soll der Algorithmus abgebrochen und das Überschreiten der Grenze festgestellt werden.

Sei nun $\mathbb{K}$ ein algebraischer Zahlkörper und $g \in \mathbb{K}[X]$ ein beliebiges irreduzibles Polynom, sowie H die Galoisgruppe von g. Die Frage ist also, wie in GALOIS festgestellt werden kann, dass die Kardinalität der Galoisgruppe H eine Grenze λ überschreitet. Hierfür gibt es ein einfaches Verfahren: In den Schritten 1–4 wird iterativ eine Folge von Polynomen $g = h_0, h_1, \ldots, h_k =: h$ aus $\mathbb{K}[X]$ berechnet, sodass $\deg(h_0) < \deg(h_1) < \cdots < \deg(h_k)$ und $\mathbb{K}[X]/h$ isomorph zum Zerfällungskörper von g ist. Aus den Sätzen 2.2 und 2.10 folgt, dass $|H| = \deg(h)$. Sobald wir also feststellen, dass der Grad eines der Polynome h_i größer als λ ist, folgt $|H| > \lambda$ und wir können den Algorithmus abbrechen.

8 Minimale nichttriviale Blöcke von Galoisgruppen

In diesem Kapitel gelte folgende Generalvoraussetzung:

Generalvoraussetzung 8.1. Es sei stets $f \in \mathbb{Z}[X]$ ein irreduzibles, normiertes Polynom vom Grad $m \geqslant 2$ und $\alpha = \alpha_1, \ldots, \alpha_m$ die Nullstellen von f. Weiterhin sei $\Omega = \{\alpha_1, \ldots, \alpha_m\}$ und $G = \mathrm{Gal}(f)$ die Galoisgruppe von f, welche auf der Nullstellenmenge Ω wirke.

Wie in Kapitel 4 beschrieben, wollen wir eine Körperkette

$$\mathbb{Q} = \mathbb{Q}(\rho_r) \subset \mathbb{Q}(\rho_{r-1}) \subset \cdots \subset \mathbb{Q}(\rho_1) \subset \mathbb{Q}(\rho_0) = \mathbb{Q}(\alpha)$$

und irreduzible Polynome $g_1 \in \mathbb{Q}(\rho_1)[X], \ldots, g_r \in \mathbb{Q}(\rho_r)[X]$ berechnen, sodass

$$\mathbb{Q}(\rho_{i-1}) \simeq \mathbb{Q}(\rho_i)[X]/g_i$$

und die Galoisgruppe von g_i primitiv auf den Nullstellen von g_i wirkt.

Der erste Schritt auf dem Weg dorthin besteht aus der Konstruktion eines Zwischenkörpers $\mathbb{Q} \subseteq \mathbb{E} \subset \mathbb{Q}(\alpha)$ und eines irreduziblen Polynoms $g \in \mathbb{E}[X]$, so dass die Galoisgruppe von g primitiv auf den Nullstellen von g wirkt. Mit Satz 5.2 wissen wir bereits, wie wir g konstruieren können: Wir müssen einen minimalen nichttrivialen Block $B \subseteq \Omega$ von G finden, welcher α enthält, und setzen anschließend $g \coloneqq \prod_{\beta \in B} X - \beta$. Die Aufgabe dieses Kapitels besteht nun also darin, einen minimalen nichttrivialen Block $B \ni \alpha$ der Galoisgruppe G von f zu finden. Die Ergebnisse basieren hierbei größtenteils auf [4, S. 32–40].

8.1 Die Faktorisierung von f enthält mehrere Linearfaktoren

Enthält die Faktorisierung von f in $\mathbb{Q}(\alpha)[X]$ mehr als einen Linearfaktor, ist es leicht einen minimalen nichttrivialen Block von G zu finden, wie der folgende Satz zeigt. Es sei zuvor an die Definition $G^B \coloneqq \{\sigma|_B \mid \sigma \in G_B\}$ erinnert.

Satz 8.2. *Sei $f = \prod_i f_i$ die Faktorisierung von f in irreduzible Polynome in $\mathbb{Q}(\alpha)[X]$ und seien $f_1 = (X - \alpha_1), \ldots, f_k = (X - \alpha_k)$ mit $\alpha_1, \ldots, \alpha_k \in \mathbb{Q}(\alpha)$ die Linearfaktoren von f. Seien weiter $p_i \in \mathbb{Q}[X]$ Polynome mit $p_i(\alpha) = \alpha_i$, $i = 1, \ldots, k$. Dann bildet die Menge $B \coloneqq \{\alpha_1, \ldots, \alpha_k\}$ einen Block von G und es existieren Abbildungen $\sigma_1, \ldots, \sigma_k \in G$, so dass $G^B = \{\sigma_1, \ldots, \sigma_k\}$ und $\sigma_i(\alpha) = \alpha_i$. Ferner gilt $\sigma_i(\alpha_j) = p_j(\alpha_i)$ für $i, j = 1, \ldots, k$.*

Beispiel 8.3. Sei $f \coloneqq X^3 - 7X + 7 \in \mathbb{Q}[X]$ und α eine Nullstelle von f. Dann ist die Faktorisierung von f über $\mathbb{Q}(\alpha)$ gegeben durch $f = (X - \alpha_1)(X - \alpha_2)(X - \alpha_3)$ mit

$$\alpha_1 \coloneqq \alpha, \quad \alpha_2 \coloneqq 3\alpha^2 + 4\alpha - 14, \quad \alpha_3 \coloneqq -3\alpha^2 - 5\alpha + 14,$$

(vgl. Beispiel 7.1). Folglich gilt für die Polynome

$$p_1 \coloneqq X, \quad p_2 \coloneqq 3X^2 + 4X - 14, \quad p_3 \coloneqq -3X^2 - 5X + 14,$$

dass $p_i(\alpha) = \alpha_i,\ i = 1, 2, 3$. Es sei G die Galoisgruppe von f, die auf der Menge $\Omega = \{\alpha_1, \alpha_2, \alpha_3\}$ wirke. Offensichtlich ist $B \coloneqq \{\alpha_1, \alpha_2, \alpha_3\} = \Omega$ ein Block von G und es gilt $G^B = G$. Da $\mathbb{Q}[X]/f$ isomorph zum Zerfällungskörper von f ist, gilt nach den Sätzen 2.2 und 2.10, dass $|G| = \deg(f) = 3$. Da G außerdem transitiv auf Ω wirkt, gibt es Abbildungen $\sigma_1, \sigma_2, \sigma_3$ mit $G^B = G = \{\sigma_1, \sigma_2, \sigma_3\}$ und $\sigma_i(\alpha) = \alpha_i$ für $i = 1, 2, 3$. Damit lässt sich nun die Wirkung von G^B auf B bestimmen. Beispielsweise gilt $\sigma_2(\alpha_3) = p_3(\alpha_2) = \alpha_1$ (vgl. Beispiel 7.1). △

Bemerkung 8.4. Mit Satz 8.2 lässt sich die Wirkung von G^B auf B explizit berechnen. Daraus kann anschließend mittels des Algorithmus MINBLOCK ein minimaler nichttrivialer Block B von G^B berechnet werden. Aus Satz 3.12 folgt, dass dann B auch ein minimaler nichttrivialer Block von G ist und wir sind fertig.

Lemma 8.5. *Sei $\beta \in \Omega$ eine Nullstelle von f mit $G_\alpha(\beta) = \{\beta\}$. Dann folgt $G_\alpha = G_\beta$.*

Beweis. Sei $\sigma \in G_\alpha$. Dann gilt nach Voraussetzung $\sigma(\beta) = \beta$, also $\sigma \in G_\beta$. Dies zeigt $G_\alpha \subseteq G_\beta$. Sei $\mathbb{L} \coloneqq \mathbb{Q}(\alpha_1, \ldots, \alpha_m)$. Aus dem Hauptsatz der Galoistheorie sowie den Sätzen 2.1 und 2.2 folgt dann

$$|G_\alpha| = [\mathbb{L} : \mathbb{Q}(\alpha)] = \frac{[\mathbb{L} : \mathbb{Q}]}{[\mathbb{Q}(\alpha) : \mathbb{Q}]} = \frac{[\mathbb{L} : \mathbb{Q}]}{\deg(f)} = \frac{[\mathbb{L} : \mathbb{Q}]}{[\mathbb{Q}(\beta) : \mathbb{Q}]} = |G_\beta|.$$

Folglich ist $G_\alpha = G_\beta$. □

Beweis von Satz 8.2. Nach dem Hauptsatz der Galoistheorie ist $\mathbb{Q}(\alpha) = \mathbb{Q}(\alpha_1, \ldots, \alpha_m)^{G_\alpha}$. Da $B = \{\alpha_1, \ldots, \alpha_k\}$ in $\mathbb{Q}(\alpha)$ enthalten ist, wird also jedes Element aus B von G_α fixiert. Da zudem außer B keine weiteren Nullstellen von f in $\mathbb{Q}(\alpha)$ enthalten sind, folgt $B = \{\beta \in \Omega \mid \forall \sigma \in G_\alpha : \sigma(\beta) = \beta\}$. Lemma 8.5 impliziert $G_\alpha = G_\beta$ für alle $\beta \in B$.

Wir wollen nun zeigen, dass $B = \{\alpha_1, \ldots, \alpha_k\}$ einen Block von G bildet, das heißt, dass $\sigma(B) \cap B \in \{\varnothing, B\}$ für alle $\sigma \in G$. Angenommen, es existiert ein $\sigma \in G$ mit $\sigma(B) \cap B \neq \varnothing$ und sei $\beta \in \sigma(B) \cap B$. Dann existiert ein $\gamma \in B$ mit $\beta = \sigma(\gamma)$. Folglich gilt für alle $\tau \in G_\alpha = G_\gamma$, dass $\sigma\tau\sigma^{-1}(\beta) = \sigma\tau(\gamma) = \sigma(\gamma) = \beta$ und daher $\sigma\tau\sigma^{-1} \in G_\beta = G_\alpha$. Wir wollen nun $B \subseteq \sigma(B)$ zeigen. Sei dazu $\delta \in B$. Dann folgt $\sigma\tau\sigma^{-1}(\delta) = \delta$ und damit $\tau\sigma^{-1}(\delta) = \sigma^{-1}(\delta)$ für alle $\tau \in G_\alpha$. Also gilt $\sigma^{-1}(\delta) \in B$ bzw. $\delta \in \sigma(B)$. Da δ beliebig aus B gewählt wurde, ergibt sich $B \subseteq \sigma(B)$ und mit der Bijektivität von σ und der Endlichkeit von B schließlich $B = \sigma(B)$.

Zuletzt bestimmen wir G^B. Wir können G^B wie folgt partitionieren: $G^B = G_1 \dot\cup \ldots \dot\cup G_k$, wobei $G_i \coloneqq \{\sigma \in G^B \mid \sigma(\alpha) = \alpha_i\}$. Es gilt für alle $i =$

$1, \ldots, k$, dass $|G_i| \geqslant 1$, da G und damit auch G^B transitiv auf B wirkt. Seien $\sigma, \tau \in G_i$ und $\alpha_j \in B$. Dann folgt

$$\sigma(\alpha_j) = \sigma(p_j(\alpha)) = p_j(\sigma(\alpha)) = p_j(\alpha_i) = p_j(\tau(\alpha)) = \tau(\alpha_j).$$

Folglich ist $\sigma = \tau$ und daher $|G_i| = 1$ für $i = 1, \ldots, k$. Das heißt, es existieren $\sigma_1, \ldots, \sigma_k$ mit $G^B = \{\sigma_1, \ldots, \sigma_k\}$ und $\sigma_i(\alpha) = \alpha_i$ und es gilt $\sigma_i(\alpha_j) = \sigma_i(p_j(\alpha)) = p_j(\sigma_i(\alpha)) = p_j(\alpha_i)$ für $i, j = 1, \ldots, k$, was zu zeigen war. □

8.2 Die Faktorisierung von f enthält nur einen Linearfaktor

Es sei daran erinnert, dass $f \in \mathbb{Z}[X]$ ein irreduzibles, normiertes Polynom vom Grad $m \geqslant 2$ und $\alpha = \alpha_1, \ldots, \alpha_m$ die Nullstellen von f sind, sowie $\Omega = \{\alpha_1, \ldots, \alpha_m\}$ und G die Galoisgruppe von f ist, welche auf der Menge Ω wirke.

Die Hauptaufgabe besteht in der Behandlung des Falls, dass die Faktorisierung von f über $\mathbb{Q}(\alpha)$ nur einen Linearfaktor enthält. Ist dies der Fall, so enthält $\mathbb{Q}(\alpha) = \mathbb{Q}(\alpha_1, \ldots, \alpha_m)^{G_\alpha}$ keine Nullstelle von f außer α. Folglich hat G_α keinen Fixpunkt aus Ω außer α. Damit sind die Voraussetzungen von Satz 3.17 erfüllt, welcher der Schlüssel zur Berechnung eines minimalen nichttrivialen Blocks von G ist.

Wir halten hierzu α fest und berechnen für alle Nullstellen $\beta \in \Omega \backslash \{\alpha\}$ die Menge $B_\beta \coloneqq \langle G_\alpha, G_\beta \rangle(\alpha)$. Diese Menge B_β ist nach Satz 3.17 für alle β stets ein Block mit mehr als einem Element. Dasjenige B_β minimaler Kardinalität ist folglich ein minimaler nichttrivialer Block von G.

8.2.1 Berechnung der Menge B_β

Wie also lässt sich die Menge $B_\beta = \langle G_\alpha, G_\beta \rangle(\alpha)$ berechnen? Die Idee ist die Folgende. Wir wissen bereits, wie wir f über $\mathbb{Q}(\alpha)$ faktorisieren können (siehe Kapitel 6), etwa $f = \prod_i f_i^\alpha$ mit $f_1^\alpha = X - \alpha$. Da für jede Nullstelle $\beta \in \Omega \backslash \{\alpha\}$ gilt, dass $\mathbb{Q}(\alpha) \simeq \mathbb{Q}[X]/f \simeq \mathbb{Q}(\beta)$, erhalten wir außerdem die Faktorisierung von f über $\mathbb{Q}(\beta)$, indem wir in jedem Faktor f_i^α das Element α durch β ersetzen, sagen wir $f = \prod_j f_j^\beta$. Wir fassen nun die Indizes (α, i), (β, j) der Faktoren f_i^α bzw. f_j^β von f als Knoten eines ungerichteten Graphen Γ auf und fügen zwischen (α, i) und (β, j) eine Kante ein, falls f_i^α und f_j^β eine gemeinsame Nullstelle besitzen. Folglich ist der Graph bipartit. Wir berechnen nun die Menge Y, welche aus allen Zahlen i besteht, für die (α, i) mit $(\alpha, 1)$ verbunden ist, d.h. für die ein Weg zwischen (α, i) und $(\alpha, 1)$ existiert (da Γ bipartit ist, treten bei einem solchen Weg stets Knoten (β, j) als innere Knoten auf). Schließlich setzen wir

$$g \coloneqq \prod_{i \in Y} f_i^\alpha.$$

Wie wir gleich sehen werden, ist die Nullstellenmenge von g gerade gegeben durch $B_\beta = \langle G_\alpha, G_\beta \rangle(\alpha)$.

Lemma 8.6. *Sei $h \in \mathbb{Q}(\alpha)[X]$ ein irreduzibler Faktor von f in $\mathbb{Q}(\alpha)[X]$ und sei $\gamma \in \Omega$ eine Nullstelle von h. Dann sind die Nullstellen von h gegeben durch $G_\alpha(\gamma)$.*

Beweis. Seien $\gamma = \gamma_1, \ldots, \gamma_k$ die Nullstellen von h und sei $\mathbb{F} \coloneqq \mathbb{Q}(\alpha)(\gamma_1, \ldots, \gamma_k)$ der Zerfällungskörper von h. Dann ist $H = \mathrm{Gal}(h) = \mathrm{Gal}(\mathbb{F}/\mathbb{Q}(\alpha)) = \mathrm{Aut}_{\mathbb{Q}(\alpha)}(\mathbb{F})$ die Galoisgruppe von h. Diese wirkt transitiv auf den Nullstellen von h, da h irreduzibel in $\mathbb{Q}(\alpha)[X]$ ist. Damit folgt $H(\gamma) = \{\gamma_1, \ldots, \gamma_k\}$. Sei $\mathbb{L} \coloneqq \mathbb{Q}(\alpha_1, \ldots, \alpha_m)$ der Zerfällungskörper von f. Damit folgt

$$G_\alpha = \{\sigma \in G \mid \sigma(\alpha) = \alpha\} = \{\sigma \in \mathrm{Aut}_{\mathbb{Q}}(\mathbb{L}) \mid \sigma(\alpha) = \alpha\} = \mathrm{Aut}_{\mathbb{Q}(\alpha)}(\mathbb{L}).$$

Hieraus ergibt sich $H = G_\alpha|_{\mathbb{F}}$, was schließlich $G_\alpha(\gamma) = H(\gamma) = \{\gamma_1, \ldots, \gamma_k\}$ zeigt. □

Satz 8.7. *Sei $\beta \in \Omega \backslash \{\alpha\}$ eine Nullstelle von f und seien $f = \prod_i f_i^\alpha = \prod_j f_j^\beta$ die Faktorisierungen von f über $\mathbb{Q}(\alpha)$ bzw. $\mathbb{Q}(\beta)$. Sei weiter $f_1^\alpha \coloneqq X - \alpha$. Definiere den bipartiten Graphen $\Gamma_\beta \coloneqq (V, E)$ mit*

$$V \coloneqq \bigcup_i \{(\alpha, i)\} \;\dot\cup\; \bigcup_j \{(\beta, j)\} \qquad \textit{und}$$

$$E \coloneqq \left\{ [(\alpha, i), (\beta, j)] \mid f_i^\alpha \textit{ und } f_j^\beta \textit{ haben gemeinsame Nullstelle} \right\}.$$

Sei $Y \coloneqq \{i \mid$ es existiert ein Weg zwischen (α, i) und $(\alpha, 1)\}$ und setze $g_\beta \coloneqq \prod_{i \in Y} f_i^\alpha$. Dann sind die Nullstellen von g_β gegeben durch $\langle G_\alpha, G_\beta \rangle(\alpha)$.

Beweis. Seien α_i und α_j Nullstellen von f_i^α bzw. f_j^β. Nach Lemma 8.6 sind die Nullstellen von f_i^α und f_j^β durch $G_\alpha(\alpha_i)$ bzw. $G_\beta(\alpha_j)$ gegeben. Folglich ist $[(\alpha, i), (\beta, j)]$ genau dann in E enthalten ist, wenn $G_\alpha(\alpha_i) \cap G_\beta(\alpha_j) \neq \varnothing$.

Sei (α, i) mit $(\alpha, 1)$ verbunden, d.h. es existiere ein Weg zwischen (α, i) und $(\alpha, 1)$. Wir zeigen per Induktion über die Länge l des Weges zwischen (α, i) und $(\alpha, 1)$, dass die Nullstellen von f_i^α in $\langle G_\alpha, G_\beta \rangle(\alpha)$ enthalten sind. Sei dazu γ eine Nullstelle von f_i^α. Für $l = 0$ gilt $f_i^\alpha = f_1^\alpha = X - \alpha$, also $\gamma = \alpha$ und α ist in $\langle G_\alpha, G_\beta \rangle(\alpha)$ enthalten. Die Aussage gelte nun für alle f_i^α, die durch einen Weg der Länge kleiner oder gleich $l - 2$ mit f_1^α verbunden sind. Sei jetzt

$$[(\alpha, 1), (\beta, i_1), (\alpha, i_2), (\beta, i_3), \ldots, (\alpha, i_{l-2}), (\beta, i_{l-1}), (\alpha, i_l) = (\alpha, i)]$$

ein Weg der Länge l zwischen $(\alpha, 1)$ und (α, i). Sei γ_1 eine gemeinsame Nullstelle von $f_{i_{l-2}}^\alpha$ und $f_{i_{l-1}}^\beta$ und γ_2 eine gemeinsame Nullstelle von $f_{i_{l-1}}^\beta$ und $f_{i_l}^\alpha = f_i^\alpha$. Die Elemente γ_1 und γ_2 sind also beide Nullstellen von $f_{i_{l-1}}^\beta$ und

die Elemente γ und γ_2 sind beide Nullstellen von f_i^α. Mit Lemma 8.6 folgt $\gamma_2 \in G_\beta(\gamma_1)$ und $\gamma \in G_\alpha(\gamma_2) \subseteq G_\alpha(G_\beta(\gamma_1))$. Nach Induktionsvoraussetzung ist $\gamma_1 \in \langle G_\alpha, G_\beta\rangle(\alpha)$ und damit $\gamma \in G_\alpha(G_\beta(\langle G_\alpha, G_\beta\rangle(\alpha))) = \langle G_\alpha, G_\beta\rangle(\alpha)$.

Sei nun umgekehrt $\gamma \in \langle G_\alpha, G_\beta\rangle(\alpha)$, das heißt es existieren $\sigma_1, \ldots, \sigma_l$ jeweils aus G_α oder G_β mit $\gamma = \sigma_1 \ldots \sigma_l(\alpha)$. Wir zeigen per Induktion über l, dass γ eine Nullstelle eines Polynoms f_i^α ist, dessen Index (α, i) im Graph Γ_β mit $(\alpha, 1)$ verbunden ist. Für $l = 0$ folgt $\gamma = \alpha$ und die Aussage ist klar. Die Aussage gelte nun für $l - 1$, d.h. $\gamma' \coloneqq \sigma_2 \ldots \sigma_l(\alpha)$ ist Nullstelle eines Polynoms f_i^α dessen Index (α, i) mit $(\alpha, 1)$ verbunden ist. Gilt $\sigma_1 \in G_\alpha$, so ist nach Lemma 8.6 auch $\gamma = \sigma_1(\gamma') \in G_\alpha(\gamma')$ Nullstelle von f_i^α und wir sind fertig. Sei also $\sigma_1 \in G_\beta$. Da γ' als Nullstelle von f_i^α insbesondere auch Nullstelle von f ist, ist γ' auch Nullstelle eines Faktors f_j^β. Es existiert also eine Kante zwischen den Indizes (α, i) und (β, j). Nach Lemma 8.6 ist $\gamma = \sigma_1(\gamma') \in G_\beta(\gamma')$ auch Nullstelle von f_j^β, also auch von einem Faktor f_k^α, d.h. es existiert wiederum eine Kante zwischen den Indizes (β, j) und (α, k). Der Knoten (α, k) ist somit über (β, j) mit (α, i) verbunden und da (α, i) nach Voraussetzung mit $(\alpha, 1)$ verbunden ist, ist auch (α, k) mit $(\alpha, 1)$ verbunden. Das Element γ ist also Nullstelle eines Polynoms f_k^α, dessen Index (α, k) mit $(\alpha, 1)$ verbunden ist. Dies zeigt die Behauptung. □

Um einen minimalen nichttrivialen Block von G, welcher α enthält, zu berechnen, gehen wir also folgendermaßen vor: Wir berechnen für jede Nullstelle $\beta \in \Omega\backslash\{\alpha\}$ den Graphen Γ_β sowie das Polynom g_β aus Satz 8.7. Die Nullstellen von g_β sind durch den Block $B_\beta = \langle G_\alpha, G_\beta\rangle(\alpha)$ gegeben. Wir wählen dann aus der Menge $\{g_\beta \mid \beta \in \Omega\backslash\{\alpha\}\}$ ein Polynom g mit minimalen Grad aus, d.h. welches $\deg(g) = \min\{\deg(g_\beta) \mid \beta \in \Omega\backslash\{\alpha\}\}$ erfüllt. Die Nullstellen von g bilden dann einen minimalen nichttrivialen Block von G, welcher α enthält.

8.2.2 Finden von gemeinsamen Nullstellen

Sei wie zuvor $f = \prod_i f_i^\alpha = \prod_j f_j^\beta$ die Faktorisierung von f in $\mathbb{Q}(\alpha)[X]$ bzw. $\mathbb{Q}(\beta)[X]$. Die Berechnung des Graphen aus Satz 8.7 erfordert die Kenntnis darüber, wie man feststellen kann, ob zwei Faktoren f_i^α und f_j^β von f gemeinsame Nullstellen haben. Dieses Problem lässt sich auf folgende Weise lösen. Die Polynome $f_i^\alpha \in \mathbb{Q}(\alpha)[X]$ und $f_j^\beta \in \mathbb{Q}(\beta)[X]$ sind über unterschiedlichen Körpern $\mathbb{Q}(\alpha)$ und $\mathbb{Q}(\beta)$ definiert. Unser Ziel ist die Konstruktion einer Körpererweiterung $\mathbb{Q}(\gamma)$ mit einem primitiven Element γ, so dass $\mathbb{Q}(\gamma) = \mathbb{Q}(\alpha, \beta)$ gilt. Dann können wir die Polynome f_i^α und f_j^β als Polynome in $\mathbb{Q}(\gamma)$ ausdrücken. Dazu ist es erforderlich die Elemente α und β als Polynome in γ auszudrücken. Satz 8.8 beschreibt, wie dies umgesetzt werden kann. Ist es schließlich gelungen f_i^α und f_j^β als Polynome in $\mathbb{Q}(\gamma)[X]$ auszudrücken, so können wir einfach feststellen, ob sie eine gemeinsame Nullstelle haben: Wir bilden den größten gemeinsamen Teiler der beiden Polynome in $\mathbb{Q}(\gamma)[X]$. Ist er 1, so haben f_i^α und f_j^β keine gemeinsame Nullstelle, andernfalls haben sie eine gemeinsame Nullstelle.

Wie finden wir also ein primitives Element γ von $\mathbb{Q}(\alpha,\beta)$ und wie lassen sich α und β als Polynome in γ ausdrücken? Hierzu können wir unsere Erkenntnisse aus Kapitel 6 über die Faktorisierung von f über $\mathbb{Q}(\alpha)$ verwenden: Wir haben dort für eine geeignete Wahl einer ganzen Zahl c die Norm $r \coloneqq N(f(X-c\alpha)) \in \mathbb{Q}[X]$ gebildet und $r = \prod_i r_i$ über $\mathbb{Q}$ faktorisiert. Die Faktorisierung von f über $\mathbb{Q}(\alpha)$ ergab sich dann als $f = \prod_i f_i = \prod_i \operatorname{ggT}(f, r_i(X+c\alpha))$. Das Element β ist Nullstelle einer der irreduziblen Faktoren von f, sagen wir f_i, folglich ist $\mathbb{Q}(\alpha,\beta) \simeq \mathbb{Q}(\alpha)[X]/f_i$. Wie wir gleich sehen werden, stellt sich heraus, dass $\gamma \coloneqq \beta + c\alpha$ ein primitives Element von $\mathbb{Q}(\alpha,\beta)$ und Nullstelle von r_i ist, und dass $\mathbb{Q}(\alpha,\beta) \simeq \mathbb{Q}[X]/r_i$. Der folgende Satz fasst diese Ergebnisse zusammen und beschreibt, wie sich α und β als Polynome in γ ausdrücken lassen.

Satz 8.8. *Sei $f = \prod_i f_i = \prod_i \operatorname{ggT}(f, r_i(X+c\alpha))$ mit $r_i = N(f_i(X-c\alpha))$ die Faktorisierung von f über $\mathbb{Q}(\alpha)$ wie in Korollar 6.12 und sei β eine Nullstelle von f_i. Dann ist $\gamma \coloneqq \beta + c\alpha$ eine Nullstelle von r_i und es gilt*

$$\mathbb{Q}(\alpha)[X]/f_i \simeq \mathbb{Q}(\alpha,\beta) = \mathbb{Q}(\gamma) \simeq \mathbb{Q}[X]/r_i.$$

Sei $\Phi : \mathbb{Q}(\alpha)[X] \to \mathbb{Q}[T,X]$ die Abbildung aus Definition 6.5. Dann gilt

$$X - \alpha = \operatorname{ggT}\big(\Phi(f_i)(X, \gamma - cX), f\big) \in \mathbb{Q}(\gamma)[X].$$

Beispiel 8.9. Sei $f \coloneqq X^3 + 2 \in \mathbb{Q}[X]$ und α eine Nullstelle von f. Für $c = 2$ ist

$$N(f(X-c\alpha)) = (X^3+54)(X^6+108) =: r_1 r_2 \in \mathbb{Q}[X]$$

quadratfrei. Mithilfe von Satz 6.12 berechnen wir damit die Faktorisierung von f:

$$f = f_1 f_2 \coloneqq (X-\alpha)(X^2+\alpha X+\alpha^2).$$

Sei nun β eine Nullstelle von f_2. Nach Satz 8.8 ist dann

$$\mathbb{Q}(\alpha,\beta) = \mathbb{Q}(\beta+2\alpha) \simeq \mathbb{Q}[X]/r_2$$

und $\gamma \coloneqq \beta + 2\alpha$ ist eine Nullstelle von r_2. Wir zeigen nun wie man das Polynom $\Phi(f_2)(X, \gamma-2X)$ berechnet. Zunächst gilt $\Phi(f_2) = X^2+TX+T^2 \in \mathbb{Q}[T,X]$. Folglich ist

$$\Phi(f_2)(X, \gamma-2X) = (\gamma-2X)^2 + X(\gamma-2X) + X^2 = 3X^2 - 3\gamma X + \gamma^2.$$

Wir wollen nun noch α und β als Polynome in γ ausdrücken. Es gilt

$$\operatorname{ggT}\big(\Phi(f_2)(X,\gamma-2X),\, f\big) = \operatorname{ggT}(3X^2-3\gamma X+\gamma^2,\, X^3+2) = X - \left(\frac{1}{36}\gamma^4 + \frac{1}{2}\gamma\right).$$

Mit Satz 8.8 folgt also $\alpha = \frac{1}{36}\gamma^4 + \frac{1}{2}\gamma$ und $\beta = \gamma - 2\alpha = -\frac{1}{18}\gamma^4$. △

Beweis von Satz 8.8. Da β Nullstelle von $f_i = \mathrm{ggT}(f, r_i(X + c\alpha))$ ist, ist $\beta + c\alpha$ Nullstelle des irreduziblen Polynoms r_i. Folglich gilt

$$\mathbb{Q}[X]/r_i \simeq \mathbb{Q}(\beta + c\alpha) \subseteq \mathbb{Q}(\alpha, \beta) \simeq \mathbb{Q}(\alpha)[X]/f_i.$$

Zudem ist $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}] = \deg(f)\deg(f_i)$ und $[\mathbb{Q}(\beta + c\alpha) : \mathbb{K}] = \deg(r_i)$. Mit

$$r_i = N(f_i(X - c\alpha)) = \prod_{j=1}^{m} \sigma_j(f_i(X - c\alpha))$$

folgt $\deg(r_i) = m \cdot \deg(f_i) = \deg(f)\deg(f_i)$, also insgesamt $\mathbb{Q}(\alpha, \beta) = \mathbb{Q}(\beta + c\alpha)$.

Kommen wir nun zur zweiten Aussage des Satzes. Wir wollen zunächst zeigen, dass $\mathrm{ggT}\left(\Phi(f_i)(X, \gamma - cX), f\right) \in \mathbb{Q}(\gamma)[X]$ von $X - \alpha$ geteilt wird, d.h. das α gemeinsame Nullstelle von $\Phi(f_i)(X, \gamma - cX)$ und f ist. Das Polynom $\Phi(f_i) \in \mathbb{Q}[T, X]$ wurde aus $f_i \in \mathbb{Q}(\alpha)[X]$ erhalten, indem jedes Vorkommen von α in den Koeffizienten von f_i durch die Unbestimmte T ersetzt wurde (siehe Definition 6.5). Ersetzen wir in $\Phi(f_i) \in \mathbb{Q}[T, X]$ die Unbestimmte T durch α, erhalten wir also wieder f_i. Damit folgt

$$\Phi(f_i)(\alpha, \gamma - c\alpha) = f_i(\gamma - c\alpha) = f_i(\beta) = 0 = f(\alpha).$$

Daher wird $\mathrm{ggT}\left(\Phi(f_i)(X, \gamma - cX), f\right)$ von $X - \alpha$ geteilt.

Angenommen, es gibt eine weitere Nullstelle $\alpha_l \neq \alpha = \alpha_1$ von f, die auch Nullstelle von $\Phi(f_i)(X, \gamma - cX)$ ist, das heißt

$$0 = \Phi(f_i)(\alpha_l, \gamma - c\alpha_l) = \Phi(f_i)(\alpha_l, X)|_{X=\gamma - c\alpha_l}.$$

Betrachte die Abbildung $\Phi(f_i)(\alpha_l, X) \in \mathbb{Q}(\alpha_l)[X]$. Diese geht aus f_i hervor, indem jedes Vorkommen von α durch α_l ersetzt wird. Wie zuvor bezeichnen wir mit $\sigma_l : \mathbb{Q}(\alpha)[X] \to \mathbb{Q}(\alpha_l)[X]$ den kanonischen $\mathbb{Q}$-Isomorphismus. Dann ist also $\Phi(f_i)(\alpha_l, X) = \sigma_l(f_i) \in \mathbb{Q}(\alpha_l)[X]$. Folglich gilt

$$0 = \Phi(f_i)(\alpha_l, \gamma - c\alpha_l) = \sigma_l(f_i)(\gamma - c\alpha_l) = \sigma_l(f_i(X - c\alpha))(\gamma).$$

Dann ist γ gemeinsame Nullstelle von $\sigma_l(f_i(X - c\alpha))$ und $f_i(X - c\alpha) = \sigma_1(f_i(X - c\alpha))$. Dies ist ein Widerspruch, da das Polynom

$$r_i = N(f_i(X - c\alpha)) = \prod_{j=1}^{m} \sigma_j(f_i(X - c\alpha))$$

separabel ist. □

Wir erinnern nochmals an das eigentliche Ziel dieses Kapitels. Gegeben ist ein irreduzibles und normiertes Polynom $f \in \mathbb{Z}[X]$ vom Grad $m \geqslant 2$ und $\alpha = \alpha_1, \ldots, \alpha_m$ die Nullstellen von f. Weiterhin sind $\Omega = \{\alpha_1, \ldots, \alpha_m\}$ und G die Galoisgruppe von f, welche auf der Menge Ω wirkt. Um die in Kapitel 4 beschriebene Körperkette zwischen $\mathbb{Q}$ und $\mathbb{Q}(\alpha)$ zu konstruieren, wollen wir zunächst ein Polynom $g \in \mathbb{E}[X]$ berechnen für einen Zwischenkörper $\mathbb{Q} \subseteq \mathbb{E} \subset \mathbb{Q}(\alpha)$, so dass die Galoisgruppe von g primitiv auf den Nullstellen von g wirkt. Der folgende Algorithmus BLOCKS verwendet unsere erzielten Ergebnisse und berechnet das Polynom g.

8.3 Algorithmus: BLOCKS

Eingabe: $f \in \mathbb{Z}[X]$, irreduzibel, normiert, $\deg(f) = m \geqslant 2$

Ausgabe: Ein Polynom $g \in \mathbb{E}[X] \subset \mathbb{Q}(\alpha)[X]$, dessen Galoisgruppe primitiv auf den Nullstellen von g wirkt, wobei α eine Nullstelle von f und $\mathbb{Q} \subseteq \mathbb{E} \subset \mathbb{Q}(\alpha)$ ein Zwischenkörper sei

Schritt 1: Finde ein $c \in \mathbb{N}$, so dass

$$r \coloneqq \mathrm{Res}_T\big(f(T), f(X - cT)\big) \in \mathbb{Q}[X]$$

quadratfrei ist

[Vgl. Satz 6.7 und Satz 6.11. Es gilt dann $r = N(f(X - c\alpha))$ für eine Nullstelle α von f. Nach Satz 6.11 kann c kleiner als m^4 gewählt werden.]

und faktorisiere r in $\mathbb{Q}[X]$:

$$r = \textstyle\prod_{i=1}^{l} r_i$$

[Nutze hierzu z.B. einen passenden Algorithmus aus [2]]

Schritt 2: $\alpha \leftarrow$ Restklasse von Z in $\mathbb{Q}[Z]/f$

[Folglich ist α eine Nullstelle von f. Fasse im Folgenden $\mathbb{Q}[Z]/f$ als Körpererweiterung $\mathbb{Q}(\alpha)$ auf.]

Für $i = 1, \ldots, l$ führe aus:

$$f_i \leftarrow \mathrm{ggT}(f, r_i(X + c\alpha)) \text{ in } \mathbb{Q}(\alpha)[X]$$

[Dann ist $f = \prod f_i$ eine vollständige Faktorisierung von f in $\mathbb{Q}(\alpha)[X]$, vgl. Korollar 6.12. Wir nehmen im Folgenden an, dass die Faktoren so numeriert sind, dass $f_1 = X - \alpha$ gilt.]

Schritt 3: Falls f mehr als einen Linearfaktor in $\mathbb{Q}(\alpha)[X]$ hat, berechne mithilfe von Satz 8.2 die induzierte Wirkung der Galoisgruppe auf diese Nullstellen und finde mit MINBLOCK einen minimalen nichttrivialen Block B, welcher α enthält.

$$g \leftarrow \textstyle\prod_{\alpha_i \in B}(X - \alpha_i)$$

Gib g aus. STOP

Schritt 4: Für alle Faktoren $f_j \neq f_1$ von f führe Schritte 5–9 aus:

Schritt 5: $\gamma \leftarrow$ Restklasse von Z in $\mathbb{Q}[Z]/r_j$

[Dann ist γ eine Nullstelle von r_j. Fasse im Folgenden $\mathbb{Q}[Z]/r_j$ als Körpererweiterung $\mathbb{Q}(\gamma)$ auf.]

$$X - \alpha \leftarrow \mathrm{ggT}\left(\Phi(f_j)(X, \gamma - cX), f\right) \in \mathbb{Q}(\gamma)[X]$$

$\beta \leftarrow \gamma - c\alpha$

[Vgl. Satz 8.8. Dies drückt α und β als Polynome in γ aus. Das Element β ist hierbei eine Nullstelle des Faktors f_j.]

Schritt 6: Für $i = 1, .., l$ führe aus:

$\tilde{f}_i \leftarrow \Phi(f_i) \in \mathbb{Q}[T, X]$

[Φ ist hierbei die Funktion aus Definition 6.5, die jedes Vorkommen von α in f_i durch die Unbestimmte T ersetzt]

$f_i^{\alpha} \leftarrow \tilde{f}_i(\alpha, X)$
$f_i^{\beta} \leftarrow \tilde{f}_i(\beta, X)$

[Dann sind $f = \prod_i f_i^{\alpha}$ und $f = \prod_k f_k^{\beta}$ die Faktorisierungen von f über $\mathbb{Q}(\alpha)$ bzw. $\mathbb{Q}(\beta)$, wobei die Faktoren f_i^{α} und f_k^{β} nun als Polynome in $\mathbb{Q}(\gamma)[X]$ ausgedrückt sind. Damit ist es möglich festzustellen, ob diese Faktoren gemeinsame Nullstellen haben, vgl. Abschnitt 8.2.2.]

Schritt 7: Berechne den Graphen $\Gamma = (V, E)$ mit Knoten V und Kanten E gegeben durch:

$V = \bigcup_{i=1}^{l} \{(\alpha, i)\} \dot{\cup} \bigcup_{k=1}^{l} \{(\beta, k)\}$

$E = \left\{ [(\alpha, i), (\beta, k)] \mid \mathrm{ggT}(f_i^{\alpha}, f_k^{\beta}) \neq 1 \right\}$

[vgl. Satz 8.7]

Schritt 8: $Y \leftarrow \left\{ i \mid \text{es existiert ein Weg zwischen } (\alpha, i) \text{ und } (\alpha, 1) \right\}$

[Hierbei ist $(\alpha, 1)$ der Index des Faktors $f_1^{\alpha} = X - \alpha$]

Schritt 9: $g_j \leftarrow \prod_{i \in Y} f_i^{\alpha}$

[Folglich sind die Nullstellen von g_j durch den Block $B_{\beta} = \langle G_{\alpha}, G_{\beta} \rangle(\alpha)$ gegeben, vgl. Satz 8.7]

Schritt 10: $g \leftarrow g_i$ minimalen Grades
Gib g aus.

[Dann bilden die Nullstellen von g einen minimalen nichttrivialen Block $B \ni \alpha$ der Galoisgruppe G von f und die Galoisgruppe von g wirkt primitiv auf den Nullstellen von g.]

9 Kette von Zwischenkörpern

Die folgende Darstellung orientiert sich an [4, S. 43–53]. Es sei wieder $f \in \mathbb{Z}[X]$ ein irreduzibles und normiertes Polynom vom Grad $m \geqslant 2$ und $\alpha = \alpha_1, \ldots, \alpha_m$ die Nullstellen von f.

Mithilfe des Algorithmus BLOCKS lässt sich nun die Kette von Zwischenkörpern zwischen $\mathbb{Q}$ und $\mathbb{Q}(\alpha)$ konstruieren. Wir setzen zunächst $h_0 \coloneqq f$ und berechnen

$$g_1 \coloneqq X^k + a_1 X^{k-1} + \cdots + a_k \coloneqq \text{BLOCKS}(h_0) \in \mathbb{Q}(a_1, \ldots, a_k)[X].$$

Dann gilt nach Konstruktion $\mathbb{Q} \subseteq \mathbb{Q}(a_1, \ldots, a_k) \subset \mathbb{Q}(\alpha)$ und die Galoisgruppe von g_1 wirkt primitiv auf den Nullstellen von g_1. Wir berechnen ein primitives Element ρ_1, so dass $\mathbb{Q}(\rho_1) = \mathbb{Q}(a_1, \ldots, a_k)$ und drücken g_1 als Polynom in $\mathbb{Q}(\rho_1)[X]$ aus. Dazu finden wir Polynome $\tilde{a}_1, \ldots, \tilde{a}_k \in \mathbb{Q}[X]$ mit $\tilde{a}_1(\rho_1) = a_1, \ldots, \tilde{a}_k(\rho_1) = a_k$ und setzen

$$g_1 \coloneqq X^k + \tilde{a}_1(\rho_1) X^{k-1} + \cdots + \tilde{a}_k(\rho_1) \in \mathbb{Q}(\rho_1)[X].$$

Anschließend finden wir das Minimalpolynom $h_1 \in \mathbb{Q}[X]$ von ρ_1 und berechnen

$$g_2 \coloneqq X^l + b_1 X^{l-1} + \cdots + b_l \coloneqq \text{BLOCKS}(h_1) \in \mathbb{Q}(b_1, \ldots, b_l)[X].$$

Wieder gilt nach Konstruktion $\mathbb{Q} \subseteq \mathbb{Q}(b_1, \ldots, b_l) \subset \mathbb{Q}(\rho_1) \subset \mathbb{Q}(\alpha)$ und die Galoisgruppe von g_2 wirkt primitiv auf den Nullstellen von g_2. Wir berechnen ein primitives Element ρ_2, so dass $\mathbb{Q}(\rho_2) = \mathbb{Q}(b_1, \ldots, b_l)$, drücken g_2 als Polynom in $\mathbb{Q}(\rho_2)[X]$ aus, finden das Minimalpolynom $h_2 \in \mathbb{Q}[X]$ von ρ_2 und berechnen $g_3 \coloneqq \text{BLOCKS}(h_2)$. Wir fahren so fort, bis $g_r \in \mathbb{Q}[X]$ ist. Dies liefert uns die Kette von Zwischenkörpern

$$\mathbb{Q} = \mathbb{Q}(\rho_r) \subset \mathbb{Q}(\rho_{r-1}) \subset \cdots \subset \mathbb{Q}(\rho_1) \subset \mathbb{Q}(\rho_0) = \mathbb{Q}(\alpha)$$

mit den gewünschten Eigenschaften.

9.1 Algorithmus: FIELDS

Eingabe: $f \in \mathbb{Z}[X]$, normiert und irreduzibel, $\deg(f) = m \geqslant 2$

Ausgabe: Polynome $g_1, \ldots, g_r$ und algebraische Zahlen $\rho_1, \ldots, \rho_r$ mit den folgenden Eigenschaften:

(1) $\mathbb{Q} = \mathbb{Q}(\rho_r) \subset \cdots \subset \mathbb{Q}(\rho_1) \subset \mathbb{Q}(\rho_0) = \mathbb{Q}(\alpha)$

(2) $g_i \in \mathbb{Q}(\rho_i)[X]$ irreduzibel

(3) $\mathbb{Q}(\rho_i)/g_i \simeq \mathbb{Q}(\rho_{i-1})$

(4) Die Galoisgruppe von g_i über $\mathbb{Q}(\rho_i)$ wirkt primitiv auf den Nullstellen von g_i.

Hierbei sei α eine Nullstelle von f.

Schritt 1: $i \leftarrow 1,\ h \leftarrow f$

Schritt 2: $X^k + a_1X^{k-1} + \cdots + a_k \leftarrow \text{BLOCKS}(h) \in \mathbb{Q}(a_1, \ldots, a_k)[X]$
$g_i \leftarrow X^k + a_1X^{k-1} + \cdots + a_k$

Schritt 3: Falls $g_i \in \mathbb{Q}[X]$:
$r \leftarrow i, \quad \rho_r \leftarrow 1$
Gib $g_1, \ldots, g_r$ und $\rho_1, \ldots, \rho_r$ aus. STOP

Schritt 4: $\rho \leftarrow a_1$
Für $j = 2, \ldots, k$ führe aus:
Solange $a_j \notin \text{span}_{\mathbb{Q}}\big(\{1, \rho, \ldots, \rho^{m-1}\}\big)$: $\rho \leftarrow \rho + a_j$
[Dies berechnet ein primitives Element $\rho = a_1 + c_2a_2 + \cdots + c_ka_k$ mit $c_2, \ldots, c_k \in \mathbb{N}$, sodass $\mathbb{Q}(a_1, \ldots, a_k) = \mathbb{Q}(\rho)$, vgl. Satz 2.5]

Schritt 5: $l \leftarrow 1$
Solange $\{1, \rho, \ldots, \rho^l\}$ linear unabhängig über $\mathbb{Q}$ ist: $l \leftarrow l + 1$

Schritt 6: Finde $d_1, \ldots, d_l \in \mathbb{Q}$ mit $\rho^l + d_1\rho^{l-1} + \cdots + d_l = 0$
$h \leftarrow X^l + d_1X^{l-1} + \cdots + d_l \in \mathbb{Q}[X]$
[Dann ist h das Minimalpolynom von ρ über $\mathbb{Q}$]

Schritt 7: Für $j = 1, \ldots, k$ führe aus:
Finde Polynom $\tilde{a}_j \in \mathbb{Q}[X]$ mit $\tilde{a}_j(\rho) = a_j$

Schritt 8: $\rho_i \leftarrow$ Restklasse von T in $\mathbb{Q}[T]/h$
[Fasse $\mathbb{Q}[T]/h$ im Folgenden als Körpererweiterung $\mathbb{Q}(\rho_i)$ auf]
$g_i \leftarrow X^k + \tilde{a}_1(\rho_i)X^{k-1} + \cdots + \tilde{a}_k(\rho_i) \in \mathbb{Q}(\rho_i)[X]$

Schritt 9: $i \leftarrow i + 1$
Gehe zu Schritt 2.

Beispiel 9.1. Sei $f \coloneqq X^6 + 4X^4 + 2X^2 + 1 \in \mathbb{Z}[X]$ und α eine Nullstelle von f. In Schritt 2 wird zunächst

$$g_1 \coloneqq \text{BLOCKS}(f) = X^2 - \alpha^2 \in \mathbb{Q}(-\alpha^2)[X]$$

berechnet. Offensichtlich ist $-\alpha^2$ ein primitives Element von $\mathbb{Q}(-\alpha^2)$, also wird $\rho \leftarrow -\alpha^2$ in Schritt 4 zugewiesen.

In den Schritten 5 und 6 wird das Minimalpolynom von ρ berechnet: Zunächst stellen wir fest, dass die Elemente $1, \rho = -\alpha^2$ und $\rho^2 = \alpha^4$ linear

unabhängig über $\mathbb{Q}$ sind, da α Nullstelle des irreduzibles Polynoms f und $\deg(f) = 6$ ist. Jedoch sind 1, ρ, ρ^2, ρ^3 linear abhängig, denn

$$\begin{aligned}\rho^3 &= -\alpha^6 = -\alpha^6 - 4\alpha^4 - 2\alpha^2 - 1 + 4\alpha^4 + 2\alpha^2 + 1 \\ &= f(\alpha) + 4\alpha^4 + 2\alpha^2 + 1 = 4\alpha^4 + 2\alpha^2 + 1 = 4\rho^2 - 2\rho + 1.\end{aligned}$$

Das Minimalpolynom von ρ ist also vom Grad 3. Da außerdem

$$(-\alpha^2)^3 - 4(-\alpha^2)^2 + 2(-\alpha^2) - 1 = -f(\alpha) = 0$$

gilt, ist $h \coloneqq X^3 - 4X^2 + 2X - 1 \in \mathbb{Q}[X]$ das Minimalpolynom von ρ.

In Schritt 7 wird ein Polynom $\tilde{a}_1 \in \mathbb{Q}[X]$ berechnet, für welches $\tilde{a}_1(\rho) = -\alpha^2$ gilt. Offensichtlich ist dieses durch $\tilde{a}_1 = X$ gegeben. In Schritt 8 setzen wir $\rho_1 \leftarrow T + (h) \in \mathbb{Q}[T]/h$ und fassen $\mathbb{Q}[T]/h$ als Körpererweiterung $\mathbb{Q}(\rho_1)$ auf. Zuletzt drücken wir g_1 als Polynom in $\mathbb{Q}(\rho_1)[X]$ aus:

$$g_1 = X^2 + \tilde{a}_1(\rho_1) = X^2 + \rho_1.$$

Der erste Durchlauf der Schritte 2–9 ist damit beendet. Wir springen wieder zu Schritt 2 zurück und berechnen

$$g_2 \coloneqq \textsc{blocks}(h) = h \in \mathbb{Q}[X].$$

Da nun $g_2 \in \mathbb{Q}[X]$ gilt, sind wir fertig und geben $g_1 = X^2 + \rho_1 \in \mathbb{Q}(\rho_1)[X]$, $g_2 = X^3 - 4X^2 + 2X - 1 \in \mathbb{Q}(\rho_2)[X] = \mathbb{Q}[X]$ sowie $\rho_1 = T \mod (T^3 - 4T^2 + 2T - 1)$ und $\rho_2 = 1$ aus. △

9.2 Bemerkungen zur Implementierung

In Schritt 2 wird

$$g \coloneqq X^k + a_1 X^{k-1} + \cdots + a_k \coloneqq \textsc{blocks}(h)$$

berechnet. Es bezeichne τ die Restklasse von T in $\mathbb{Q}[T]/h$ und wir fassen $\mathbb{Q}(\tau) \simeq \mathbb{Q}[T]/h$ als Körpererweiterung auf. Dann ist $g \in \mathbb{Q}(a_1, \ldots, a_k)[X] \subset \mathbb{Q}(\tau)[X]$, wobei die Koeffizienten $a_1, \ldots, a_k$ als Polynome in τ dargestellt werden. Der Körper $\mathbb{Q}(\tau)$ kann als $\mathbb{Q}$-Vektorraum mit Basis $B \coloneqq \{1, \tau, \ldots, \tau^{n-1}\}$ aufgefasst werden, mit $n \coloneqq \deg(h)$.

Da die Koeffizienten $a_1, \ldots, a_k$ als Polynome in τ dargestellt werden, wird das in Schritt 3 berechnete primitive Element ρ von $\mathbb{Q}(a_1, \ldots, a_k)$ ebenfalls als Polynom in τ dargestellt. Damit lässt sich in Schritt 4 die lineare Unabhängigkeit von $\{1, \rho, \ldots, \rho^l\}$ über $\mathbb{Q}$ einfach überprüfen: Man berechnet $1, \rho, \ldots, \rho^l$, wobei diese wiederum Polynome in τ sind, und liest anhand der Koeffizienten dieser Polynome die Koordinaten von $1, \rho, \ldots, \rho^l$ bezüglich der Basis B ab. Schließlich überprüft man, z.B. mithilfe der Gauß-Elimination, ob sich $\varphi(\rho^l)$ als Linearkombination von $\varphi(1), \varphi(\rho), \ldots, \varphi(\rho^{l-1})$ darstellen lässt, wobei $\varphi : \mathbb{Q}(\tau) \to \mathbb{Q}^n$ die Koordinatenabbildung bzgl. B bezeichne.

Das gleiche Verfahren kann man für Schritt 5 und 6 verwenden. In Schritt 5 ist nach Koeffizienten $d_1, \ldots, d_l$ gesucht, so dass $\rho^l + d_1\rho^{l-1} + \cdots + d_l = 0$ gilt. Hierfür berechnet man den Kern der Matrix $\left[\varphi(\rho^l), \ldots, \varphi(\rho), \varphi(1)\right] \in \mathbb{Q}^{n,l+1}$ und wählt sich aus diesem einen Vektor $d = (d_0, d_1, \ldots, d_l) \in \mathbb{Q}^{l+1}$, dessen erste Komponente d_0 auf 1 normiert ist. Dann ist $h \coloneqq X^l + d_1X^{l-1} + \cdots + d_l$ das Minimalpolynom von ρ über $\mathbb{Q}$.

In Schritt 6 ist nach Polynomen $\tilde{a}_1, \ldots, \tilde{a}_k \in \mathbb{Q}[X]$ gesucht mit $\tilde{a}_1(\rho) = a_1, \ldots, \tilde{a}_k(\rho) = a_k$. Hierfür löst man für $j = 1, \ldots, k$ das lineare Gleichungssystem $\left[\varphi(\rho^{l-1}), \ldots, \varphi(\rho), \varphi(1)\right] = \varphi(a_j)$. Sei $(b_{l-1}, \ldots, b_1, b_0) \in \mathbb{Q}^l$ ein Lösungsvektor. Setzen wir $\tilde{a}_j \coloneqq b_{l-1}X^{l-1} + \cdots + b_1X + b_0$, so folgt $\tilde{a}_j(\rho) = a_j$.

10 Auflösbarkeit eines Polynoms durch Radikale

10.1 Zusammenfügen der Algorithmen

Wir haben nun die nötige Vorarbeit geleistet, um in polynomialer Zeit die Frage zu beantworten, ob ein gegebenes normiertes, irreduzibles Polynom $f \in \mathbb{Z}[X]$ durch Radikale auflösbar ist. Die Basis der folgenden Darstellung bildet [4, S. 59 f.]. Wir gehen wie folgt vor. Wir berechnen mithilfe des Algorithmus FIELDS eine Kette von Körpern $\mathbb{Q} = \mathbb{Q}(\rho_r) \subset \cdots \subset \mathbb{Q}(\rho_1) \subset \mathbb{Q}(\rho_0) = \mathbb{Q}(\alpha)$ und irreduzible Polynome $g_i \in \mathbb{Q}(\rho_i)[X]$, so dass $\mathbb{Q}(\rho_i)[X]/g_i \simeq \mathbb{Q}(\rho_{i-1})$ und die Galoisgruppe G_i von g_i primitiv auf den Nullstellen von g_i wirkt. Das Polynom f ist nach Satz 5.3 genau dann durch Radikale auflösbar, wenn jede der Gruppen $G_1, \ldots, G_r$ auflösbar ist. Pálfy [5] zeigte, dass die Kardinalität auflösbarer Gruppen, die transitiv und primitiv auf einer n-elementige Menge wirken, kleiner als $\lambda(n) \coloneqq 24^{-1/3} n^{3,25}$ ist (siehe Satz 4.1). Wir versuchen also die Galoisgruppe G_i mithilfe des Algorithmus GALOIS zu berechnen. Ist die Kardinalität von G_i kleiner als $\lambda(\deg(g_i))$, so gelingt uns die Berechnung von G_i in polynomialer Zeit. Da die Kardinalität von G_i dann durch ein Polynom in $\deg(g_i)$ beschränkt ist, können wir mittels eines geeigneten Algorithmus (siehe z.B. [6] oder den von David Joyner in SAGE implementierten Algorithmus `is_solvable`) in polynomialer Zeit bestimmen, ob G_i auflösbar ist. Andernfalls brechen wir die Berechnung von G_i mittels GALOIS ab, sobald wir feststellen, dass die Kardinalität von G_i größer als $\lambda(\deg(g_i))$ ist (siehe dazu Abschnitt 7.3). Obwohl wir G_i dann nicht berechnet haben, können wir trotzdem eine Aussage über die Auflösbarkeit von G_i treffen: Wir wissen, dass G_i nach Konstruktion primitiv auf eine $\deg(g_i)$-elementige Menge wirkt. Da aber $|G_i|$ größer als $\lambda(\deg(g_i))$ ist, kann G_i nach Satz 4.1 nicht auflösbar sein.

10.2 Algorithmus: SOLVABILITY

Eingabe: $f \in \mathbb{Z}[X]$, normiert, irreduzibel, $\deg(f) = m \geqslant 2$

Ausgabe: `True`, falls f durch Radikale auflösbar ist,
`False`, sonst

Schritt 1: $\{g_i \in \mathbb{Q}(\rho_i)[X] \mid i = 1, \ldots, r\} \leftarrow \text{FIELDS}(f)$

Schritt 2: Für $i = 1, \ldots, r$ führe aus:

Schritt 3: Rufe $G_i \leftarrow \text{GALOIS}(g_i)$ auf
Falls $|G_i|$ während der Berechnung den Wert $24^{-1/3} \deg(g_i)^{3,25}$ übersteigt:
Brich die Berechnung ab und gib `False` aus. STOP
Falls G_i nicht auflösbar ist:
Gib `False` aus. STOP

Schritt 4: Gib `True` aus.

11 Fazit und Ausblick

In dieser Arbeit wurde ein polynomialer Algorithmus beschrieben, der die Frage beantwortet, ob ein gegebenes normiertes und irreduzibles Polynom $f \in \mathbb{Z}[X]$ durch Radikale auflösbar ist. Die Darstellung wurde dabei so gewählt, dass sich die einzelnen Schritte leicht mit einem Computeralgebraprogramm wie beispielsweise SAGE implementieren lassen. Der Fokus lag stets darauf, die Funktionsweise der Bestandteile des Algorithmus verständlich zu machen sowie deren Korrektheit zu verifizieren. Eine ausführliche Laufzeitanalyse hätte den Rahmen dieser Arbeit gesprengt. Es sei hierzu auf [4] verwiesen.

Trotz der im Vergleich zur exponentiellen Laufzeit „theoretisch guten“ polynomialen Laufzeit, ist es fraglich, ob dieser Algorithmus in der Praxis tatsächlich vernünftig einsetzbar ist. Für den Programmierer wird es unter allen Umständen viel Spielraum geben, die einzelnen Schritte zu optimieren, um sie effizient implementieren zu können.

Nachdem die Auflösbarkeit eines Polynoms festgestellt wurde, ist es natürlich wünschenswert, die Nullstellen des Polynoms auch tatsächlich durch Radikale auszudrücken. Hinweise auf eine mögliche Umsetzung dieser Aufgabe in polynomialer Zeit werden in [3] gegeben.

Trotz aller Bemühungen zur Laufzeitverbesserung bleibt der immense Laufzeitunterschied zwischen Algorithmen, die die Nullstellen eines Polynoms exakt und solchen, die jene numerisch bis zu einer beliebigen Genauigkeit berechnen, weiter bestehen.

Eidesstattliche Erklärung zur Bachelorarbeit

Hiermit erkläre ich, dass ich die vorliegende Arbeit selbstständig und eigenhändig sowie ohne unerlaubte fremde Hilfe und ausschließlich unter Verwendung der aufgeführten Quellen und Hilfsmittel angefertigt habe.

Die selbstständige und eigenständige Anfertigung versichert an Eides statt.

Berlin, den 22. Mai 2015

Rico Raber

Literatur

[1] Bosch, Siegfried: *Algebra*. Springer Berlin Heidelberg, 2009

[2] Gathen, Joachim Von Z. ; Gerhard, Jürgen: *Modern Computer Algebra*. Cambridge University Press, 2003

[3] Landau, Susan E. ; Miller, Gary L.: Solvability by radicals is in polynomial time. In: *Journal of computer and system sciences* 30 (1985), April, Nr. 2, S. 179–208

[4] Landau, Susan E.: *On computing Galois groups and its application to solvability by radicals*, Massachusetts Institute of Technology, Diss., 1983

[5] Pálfy, P. P.: A polynomial bound for the orders of primitive solvable groups. In: *Journal of algebra* 77 (1982), S. 127–137

[6] Seress, Á.: *Permutation Group Algorithms*. Cambridge University Press, 2003 (Cambridge Tracts in Mathematics)