Über die Berechnung von Automorphismen und Teilkörpern algebraischer Zahlkörper

vorgelegt von
Diplom-Mathematiker
Jürgen Klüners
aus Meerbusch

Vom Fachbereich 3 Mathematik
der Technischen Universität Berlin
zur Erlangung des akademischen Grades eines
Doktors der Naturwissenschaften
genehmigte Dissertation.

Berlin 1997
D83

Promotionsausschuß

Vorsitzender:	Professor Dr. R. Wüst
Berichter:	Professor Dr. M. E. Pohst
Berichter:	Dr. habil. F. Leprévost

Tag der wissenschaftlichen Aussprache: 21. Mai 1997

Inhaltsverzeichnis

KAPITEL I

Einleitung

Rund 1700 Jahre vor Christi Geburt war in Mesopotamien eine algebraische Methode bekannt, um Gleichungen der Form $x^2+px+q=0$ zu lösen [12, 28]. Danach dauerte es mehr als 3000 Jahre, ehe Gleichungen vom Grad 3 und 4 geschlossen, d.h. durch Addition, Subtraktion, Multiplikation, Division und Wurzelziehen, gelöst werden konnten. Lange Zeit war offen, ob Gleichungen vom Grad größer als 4 mit ähnlichen Methoden behandelt werden können. Zu Beginn des 19. Jahrhunderts zeigten zuerst Abel und wenig später auch Galois, daß dies bereits für Grad 5 unmöglich ist. Galois gab zusätzlich eine vollständige Charakterisierung dieses Problems, indem er zeigte, daß eine Gleichung genau dann auflösbar ist, wenn die zugehörige Galoisgruppe auflösbar ist.

Die Galoistheorie bildet auch heute noch eine Grundlage der algebraischen Zahlentheorie. Mit ihrer Hilfe lassen sich z.B. die Automorphismen oder Teilkörper eines algebraischen Zahlkörpers charakterisieren. Die Berechnung der Galoisgruppe erweist sich allerdings als ein sehr schwieriges Problem. Die zur Zeit effizientesten Algorithmen zur Galoisgruppenberechnung greifen auf berechnete Tabellen zurück, die unter anderem alle transitiven Untergruppen der symmetrischen Gruppe $\mathfrak{S}_n$ enthalten. Damit sind diese Methoden auf Polynome kleinen Grades beschränkt. Eine andere Methode, die Galoisgruppe zu berechnen, besteht darin, zuerst den Zerfällungskörper des gegebenen algebraischen Zahlkörpers zu bestimmen, um hiernach in diesem Körper die Automorphismen zu berechnen. Diese Methode erweist sich aber bei gradmäßig großen Zerfällungskörpern als unpraktikabel.

Wir werden bei unserer Algorithmenentwicklung auf Ergebnisse der Galoistheorie zurückgreifen, vermeiden aber die explizite Berechnung der Galoisgruppe. Viele unserer Probleme können durch Faktorisierung von Polynomen über Zahlkörpern gelöst werden. So können die Automorphismen eines normalen Zahlkörpers $\mathbb{Q}(\alpha)$

z.B. dadurch berechnet werden, daß das Minimalpolynom von α über dem Zahlkörper $\mathbb{Q}(\alpha)$ faktorisiert wird. Es zeigt sich, daß diese Methoden bereits bei sehr kleinen Graden (10-15) wenig effizient sind.

In unserer Arbeit werden wir Verfahren für die Berechnung von Teilkörpern und Automorphismen algebraischer Zahlkörper entwickeln. Als Anwendung hiervon führen wir eine neue Dekomposition von Polynomen ein, die einen wichtigen Schritt in Richtung Auflösbarkeit durch Radikalerweiterungen bedeutet.

Zur Berechnung von Teilkörpern gibt es eine Reihe bekannter Algorithmen [15, 21, 24], die auf der Faktorisierung von Polynomen über Zahlkörpern oder Polynomen über $\mathbb{Z}$ von sehr großem Grad basieren. Dabei benötigt die erste Faktorisierung jeweils schon mehr Rechenzeit als die komplette Ausführung unseres Algorithmus. Die in [3] vorgestellte Methode arbeitet mit komplexen Approximationen und Gitterreduktionstechniken. Sie ist bei größeren Beispielen ebenfalls zu aufwendig. Unser Algorithmus ist eine Weiterentwicklung der in [16, 18] vorgestellten Methoden, die ihrerseits auf [11] basieren.

Bei der Berechnung eines Teilkörpers $L = \mathbb{Q}(\beta)$ eines gegebenen Zahlkörpers $E = \mathbb{Q}(\alpha)$ werden sowohl das Minimalpolynom g von β als auch eine Einbettung $\omega \in \mathbb{Q}[t]$ mit $\omega(\alpha) = \beta$ berechnet. Die Idee des Teilkörperalgorithmus in [16, 18] besteht darin, daß es eine Bijektion zwischen den Blocksystemen der Galoisgruppe und den Teilkörpern gibt. Wir berechnen mit dem van der Waerden-Kriterium zyklische Untergruppen der Galoisgruppe und leiten Eigenschaften für die Blocksysteme her, die wir zu deren Bestimmung einsetzen. Daraufhin können wir mit dem Hensel-Lifting in unverzweigten p-adischen Erweiterungen aus einem Blocksystem das Minimalpolynom g berechnen. Die Einbettung ω wird dann mit Hilfe des Newton-Liftings bestimmt.

Die Hauptidee wird in dieser Arbeit beibehalten, wobei wir die zeitkritischen Teile wesentlich effizienter gestalten werden. So haben wir neue Methoden zum Hensel-Lifting in unverzweigten p-adischen Erweiterungen sowie zur Berechnung des Newton-Liftings entwickelt. Weiterhin ist es uns gelungen, die Anzahl der zu betrachtenden Kandidaten für Blocksysteme deutlich zu senken. Als Ergebnis erhalten wir einen Algorithmus, der dem in [16, 18] um Größenordnungen überlegen ist.

Als Anwendung für die Teilkörper haben wir ein neues Konzept für die Dekomposition von Polynomen f und einen effizienten Algorithmus zur Berechnung dieser entwickelt, welches die bisher bekannten verallgemeinert. Ziel dieser Dekompositionen ist es, die Nullstellen von Polynomen dadurch zu erhalten, daß wir sukzessive die Nullstellen von Polynomen kleineren Grades bestimmen. Wir beweisen eine Korrespondenz zwischen den Teilkörpern des von einer Nullstelle von f erzeugten Zahlkörpers und den Dekompositionen. Diese Dekompositionen bilden einen wichtigen Schritt in Richtung eines effizienten Algorithmus zur Auflösbarkeit durch Radikalerweiterungen. Nach Berechnung der Dekompositionen muß „nur noch" ein effizienter Algorithmus für primitive Erweiterungen gefunden werden.

Die Dekompositionen finden für die Konstruktion qualitativ neuer Robotertypen sowie bei der zeitkritischen Steuerung allgemeiner Mechanismen (z.B. Fahrwerksabstimmung von Autos) praktische Anwendung [33]. So ist es von entscheidender Bedeutung, daß die kinematischen Gleichungssysteme in Echtzeit gelöst werden können. Falls eine Dekomposition existiert, können die entstehenden Polynomgleichungen erheblich vereinfacht bzw. symbolisch gelöst werden. Dadurch entfallen die sonst erforderlichen für die Praxis viel zu langsamen numerischen Rechnungen.

Wir stellen in dieser Arbeit erstmalig Algorithmen zur Bestimmung von Automorphismen algebraischer Zahlkörper vor, die nicht auf der Faktorisierung von Polynomen über Zahlkörpern beruhen. Dabei entwickeln wir spezielle Verfahren für über $\mathbb{Q}$ abelsche und normale sowie wie für relativ-abelsche Erweiterungen. Allen Methoden ist gemeinsam, daß sie solange Frobeniusautomorphismen berechnen, bis die gesamte Automorphismengruppe von diesen erzeugt werden kann. Die Frobeniusautomorphismen werden zuerst modulo p und dann mit Hilfe des Newton-Liftings ausgerechnet.

Die vorliegende Arbeit gliedert sich wie folgt:

In Kapitel II werden Grundlagen, wie das van der Waerden-Kriterium, die Rekonstruktion von Zahlen aus einer Approximation sowie wichtige Abschätzungen behandelt. Die grundlegenden p-adischen Algorithmen wie das Hensel- und Newton-Lifting werden in Kapitel III vorgestellt. In Kapitel IV, V und VI beschäftigen wir uns mit Teilkörpern, Dekompositionen und Automorphismen.

Wir geben in Kapitel VII eine große Anzahl von Beispielen an, die die Leistungsfähigkeit unserer Algorithmen unterstreichen.

Abschließend weisen wir auf unsere Bezeichnungen und das Literaturverzeichnis am Ende unserer Arbeit hin.

Ich danke Herrn Prof. Dr. M. Pohst herzlich für seine Unterstützung während der Anfertigung der Arbeit und die gute Zusammenarbeit.
Ferner danke ich Herrn Dr. habil. F. Leprévost für die Übernahme des Koreferats sowie allen Mitgliedern der Kant-Gruppe, durch deren Hilfe die Implementierung der Algorithmen erst ermöglicht wurde.
Mein besonderer Dank gilt jedoch meinen Eltern, die mich während meines ganzen Studiums unterstützt haben. Ihnen ist diese Arbeit gewidmet.

KAPITEL II

Grundlagen

1. Algebraische Zahlkörper und Vervollständigungen

Es seien F ein algebraischer Zahlkörper und $\mathfrak{o}_F$ die Maximalordnung von F. Weiterhin seien $f \in \mathfrak{o}_F[t]$ ein normiertes und irreduzibles Polynom vom Grad n und α eine Nullstelle von f. α erzeugt dann einen algebraischen Zahlkörper $E = F(\alpha)$ vom Grad n. Sei nun $p \in \mathbb{P}$ (Menge der Primzahlen), $\mathfrak{p}$ ein Primideal in $\mathfrak{o}_F$ und $\mathfrak{P}$ ein Primideal in $\mathfrak{o}_E$, wobei zusätzlich $p \in \mathfrak{p} \subseteq \mathfrak{P}$ gelten soll. In diesem Fall sagen wir $\mathfrak{P}$ liegt über $\mathfrak{p}$ bzw. $\mathfrak{p}$ liegt unter $\mathfrak{P}$. Dann sind sowohl $\mathfrak{o}_F/\mathfrak{p}$ als auch $\mathfrak{o}_E/\mathfrak{P}$ endliche Körper, wobei $\mathfrak{o}_F/\mathfrak{p}$ ein Teilkörper von $\mathfrak{o}_E/\mathfrak{P}$ ist.

Definition 2.1. *Der Grad des endlichen Körpers $\mathfrak{o}_F/\mathfrak{p}$ über $\mathbb{F}_p$ wird als Trägheitsgrad $f_\mathfrak{p}$ (über $\mathbb{Q}$) des Primideals $\mathfrak{p}$ bezeichnet. Analog ist der Grad der Körpererweiterung $(\mathfrak{o}_E/\mathfrak{P})/(\mathfrak{o}_F/\mathfrak{p})$ der (relative) Trägheitsgrad $f_{\mathfrak{P}/\mathfrak{p}}$ des Primideals $\mathfrak{P}$.*

Alle in dieser Arbeit auftretenden Primideale sind über $\mathbb{Q}$ unverzweigt, d.h., daß $p \notin \mathfrak{P}^2$ gilt. Somit ist p stets ein Primelement von $\mathfrak{p}$ bzw. $\mathfrak{P}$.

Seien nun $\mathcal{E} = E_\mathfrak{P}$ und $\mathcal{F} = F_\mathfrak{p}$ die Vervollständigungen von E und F an den Primidealen $\mathfrak{P}$ und $\mathfrak{p}$. $\mathcal{E}$ und $\mathcal{F}$ sind unverzweigte p-adische Erweiterungen von $\mathbb{Q}_p$, wobei $\mathcal{F}$ in $\mathcal{E}$ enthalten ist. Wir bezeichnen mit $\bar{\mathcal{E}}$ bzw. $\bar{\mathcal{F}}$ ein minimales Restsystem von $\mathfrak{o}_E/\mathfrak{P}$ bzw. $\mathfrak{o}_F/\mathfrak{p}$. Da p Primelement von $\mathfrak{P}$ und $\mathfrak{p}$ ist, können $\mathcal{E}$ und $\mathcal{F}$ auf folgende Weise dargestellt werden:

$$\mathcal{E} = \{\sum_{i=m}^{\infty} a_i p^i \mid a_i \in \bar{\mathcal{E}},\ m \in \mathbb{Z},\ a_m \neq 0\},$$

$$\mathcal{F} = \{\sum_{i=m}^{\infty} a_i p^i \mid a_i \in \bar{\mathcal{F}},\ m \in \mathbb{Z},\ a_m \neq 0\}.$$

BEZEICHNUNG 2.2. *Wir bezeichnen mit* $\operatorname{disc}(f) \in \mathfrak{o}_{\mathcal{F}}$ *die Polynomdiskriminante von* f *und mit* $\mathfrak{d}(f)$ *das von* $\operatorname{disc}(f)$ *erzeugte Hauptideal in* $\mathfrak{o}_{\mathcal{F}}$.

In unseren Verfahren wollen wir an vielen Stellen vermeiden, die Maximalordnung $\mathfrak{o}_E$ explizit auszurechnen. Stattdessen werden wir in der Gleichungsordnung $\mathfrak{o}_F[\alpha]$ arbeiten. Der Beweis des folgenden Satzes kann in [31, section 6.2] nachgelesen werden.

SATZ 2.3. *Sei* $\mathfrak{p}$ *ein Primideal von* $\mathfrak{o}_F$ *mit* $\mathfrak{p} \nmid \mathfrak{d}(f)$ *und* $\mathfrak{P}$ *ein Primideal von* $\mathfrak{o}_E$, *welches über* $\mathfrak{p}$ *liegt. Weiterhin seien* $\tilde{\mathfrak{P}} = \mathfrak{P} \cap \mathfrak{o}_F[\alpha]$ *und* $f \equiv f_1 \cdots f_r \bmod \mathfrak{p}$. *Dann folgt:*

(i) $\tilde{\mathfrak{P}}$ *ist maximales Ideal von* $\mathfrak{o}_F[\alpha]$.
(ii) $\mathfrak{o}_E/\mathfrak{P} \cong \mathfrak{o}_F[\alpha]/\tilde{\mathfrak{P}}$.
(iii) $\mathfrak{p}\mathfrak{o}_E = \mathfrak{P}_1 \cdots \mathfrak{P}_r$ *mit* $\mathfrak{P}_i = (\mathfrak{p}, f_i(\alpha)) := \mathfrak{p}\mathfrak{o}_E + f_i(\alpha)\mathfrak{o}_E$ $(1 \leq i \leq r)$.
(iv) $\mathfrak{p}\mathfrak{o}_F[\alpha] = \tilde{\mathfrak{P}}_1 \cdots \tilde{\mathfrak{P}}_r$ *mit* $\tilde{\mathfrak{P}}_i = (\mathfrak{p}, f_i(\alpha)) := \mathfrak{p}\mathfrak{o}_F[\alpha] + f_i(\alpha)\mathfrak{o}_F[\alpha]$ $(1 \leq i \leq r)$.

2. Identifikation der Nullstellen

Ein wesentliches Problem dieser Arbeit ist eine günstige Identifizierung der Nullstellen von f, d.h. die Bestimmung der Nullstellen in einem geeigneten Erweiterungskörper von E. Wir können ohne größere Probleme die Nullstellen $\alpha_i \in \mathbb{C}$ $(1 \leq i \leq n)$ ausrechnen. Meistens sind wir aber an einer Darstellung der Nullstellen in einer geeigneten unverzweigten p-adischen Erweiterung interessiert. Seien hierzu N die normale Hülle von E/F, $\mathfrak{P}$ ein Primideal von $\mathfrak{o}_E$ und $\hat{\mathfrak{P}}$ ein Primideal von $\mathfrak{o}_N$, welches über $\mathfrak{P}$ liegt. Dann sei $\mathcal{N} = N_{\hat{\mathfrak{P}}}$ die p-adische Vervollständigung von N an $\hat{\mathfrak{P}}$. Wenn wir nun f auf kanonische Weise in $\mathcal{N}$ einbetten, so zerfällt f in Linearfaktoren, und wir können auf diese Weise die Nullstellen $\tilde{\alpha}_1, \ldots, \tilde{\alpha}_n$ von f in $\mathcal{N}$ bestimmen. Wir merken an, daß die Reihenfolge der α_i im allgemeinen nichts mit der Reihenfolge der $\tilde{\alpha}_i$ zu tun hat. Wir müssen uns daher entscheiden, bezüglich welcher Vervollständigung wir die Nullstellen sortieren wollen.

DEFINITION 2.4. *Unter der Identifizierung der Nullstellen von* f *bzgl.* $\mathfrak{P}$ *bzw. in* $\mathbb{C}$ *verstehen wir die Reihenfolge der Nullstellen, wie wir sie explizit in einer* p*-adischen Vervollständigung bzw. in* $\mathbb{C}$ *ausgerechnet (bzw. fixiert) haben.*

Bei der Berechnung der Nullstellen von f in einer p-adischen Vervollständigung gehen wir folgendermaßen vor:

(1) Faktorisiere $f = f_1 \cdots f_r$ in $\mathcal{E}[t]$.
(2) Erzeuge normale Hülle $\mathcal{N}$ von $\mathcal{E}/\mathcal{F}$.
(3) Berechne die Nullstellen von f_i $(1 \leq i \leq r)$.

Auf diese Weise erhalten wir alle Nullstellen von f. Bei der Erzeugung von $\mathcal{N}$ haben wir natürlich gewisse Freiheiten. Deswegen müssen wir uns hier auf eine Möglichkeit fixieren. In diesem Sinne hängt die Reihenfolge der Nullstellen nur von $\mathfrak{P}$ ab.

Wenn wir die Nullstellen von f in verschiedenen Vervollständigungen ausrechnen, so können wir nur in einer Vervollständigung eine Reihenfolge ausnutzen. Wir werden uns in dieser Arbeit stets für eine p-adische Vervollständigung entscheiden, in der wir aufgrund der Reihenfolge der Nullstellen zusätzliche Informationen gewinnen. Weiterhin betrachten wir die Nullstellen von f in $\mathbb{C}$, um Schranken für den Absolutbetrag der Nullstellen zu erhalten. Diese Schranken sind dann aber von einer Reihenfolge der Nullstellen unabhängig.

Da alle Primideale in dieser Arbeit sowohl unverzweigt als auch keine Indexteiler sind, hat die Faktorisierung

$$f \equiv f_1 \cdots f_r \bmod \mathfrak{P}$$

keine doppelten Faktoren. Daher ist die Reihenfolge der Nullstellen von f in einer p-adischen Vervollständigung bereits durch die Reihenfolge der Nullstellen im zugehörigen Restklassenkörper eindeutig bestimmt.

3. Galoistheorie

Die Galoistheorie ist ein wichtiges Hilfsmittel für die Berechnung von Automorphismen und Teilkörpern. Leider ist es zu kompliziert, zuerst die Galoisgruppe zu bestimmen, um mit deren Hilfe die Teilkörper bzw. Automorphismen zu berechnen. Trotzdem bildet die Galoistheorie eine wesentliche Grundlage für die in den späteren Kapiteln zu entwickelnden Algorithmen. Deswegen werden wir hier die wichtigsten Aussagen der Galoistheorie auflisten. Für weitere Aussagen und die Beweise verweisen wir auf verschiedene Standardwerke über Algebra, z.B. [32, 22].

Definition 2.5. *Wir bezeichnen mit* $\mathrm{Aut}(E/F)$ *die Automorphismengruppe von* E*, die* F *invariant läßt. Die Körpererweiterung* E/F *heißt galoissch, falls* E/F *normal und separabel ist. In diesem Fall ist* $G(E/F)$ *die zugehörige Galoisgruppe. Für* $g \in F[t]$*, welches nicht notwendigerweise irreduzibel ist, bezeichnet* $\mathrm{Gal}(g)$ *die Galoisgruppe von* $F(\beta_1, \ldots, \beta_m)/F$*, wenn* $\beta_1, \ldots, \beta_m$ *die Nullstellen von* g *sind.*

Satz 2.6. *(Hauptsatz der Galoistheorie)*

Sei E/F endliche Galoiserweiterung. Dann besteht eine Bijektion zwischen den Teilkörpern $F \subseteq L \subseteq E$ und den Untergruppen von $G(E/F)$ mittels L wird abgebildet auf $G(E/L)$ und umgekehrt. Dabei ist L/F genau dann galoissch, wenn $G(E/L)$ Normalteiler von $G(E/F)$ ist. In diesem Falle ist $G(L/F)$ isomorph zu $G(E/F)/G(E/L)$.

Der Hauptsatz der Galoistheorie ist für beliebige Körpererweiterungen anwendbar. Noch stärkere Aussagen lassen sich aber treffen, wenn wir endliche Erweiterungen von endlichen Körpern betrachten.

Satz 2.7. *Es sei $p \in \mathbb{P}$ und $\mathbb{F}_q$ eine endliche Erweiterung von $\mathbb{F}_p$ vom Grad n, d.h. $q = p^n$. Dann ist $\mathbb{F}_q/\mathbb{F}_p$ galoissch mit $G(\mathbb{F}_q/\mathbb{F}_p) = \langle\sigma\rangle$, wobei σ der Frobenius-Automorphismus ($x \mapsto x^p$) ist. Ist $\mathbb{F}_{\tilde{q}}$ eine Erweiterung von $\mathbb{F}_q$ vom Grad m, so ist auch $\mathbb{F}_{\tilde{q}}/\mathbb{F}_q$ galoissch mit Galoisgruppe $G(\mathbb{F}_{\tilde{q}}/\mathbb{F}_q) = \langle\tau\rangle$ mit $\tau : x \mapsto x^{p^n}$ ($x \in \mathbb{F}_{\tilde{q}}$).*

4. Das van der Waerden-Kriterium

In diesem Abschnitt stellen wir eine Methode zur Verfügung, die für unser Verfahren der Teilkörperberechnung von zentraler Bedeutung ist. Mit dem folgenden Satz können wir mit Hilfe von Faktorisierungen modulo eines Primideals Elemente der Galoisgruppe eines erzeugenden Polynoms eines Körpers bestimmen. Da die Algorithmen zum Faktorisieren von Polynomen über endlichen Körpern sehr schnell sind, können wir innerhalb kürzester Zeit verschiedene Elemente der Galoisgruppe bestimmen. Die Kenntnis möglichst vieler Elemente der Galoisgruppe ist Grundlage des Algorithmus zur Teilkörperberechnung, den wir in Kapitel IV vorstellen werden.

Satz 2.8. *(van der Waerden-Kriterium)*

Es seien R ein ZPE-Ring, $\mathfrak{p}$ ein Primideal in R, $\overline{R} = R/\mathfrak{p}$ der zugehörige Restklassenring, E und $\overline{E}$ die Quotientenkörper von R und $\overline{R}$, g ein Polynom aus $R[t]$ und $\overline{g}$ das g mittels des kanonischen Epimorphismus $R \longrightarrow \overline{R}$ zugeordnete Polynom, die beide als doppelwurzelfrei vorausgesetzt werden. Dann ist $\overline{G} = \mathrm{Gal}(\overline{g})$ (als Permutationsgruppe der passend angeordneten Wurzeln) eine Untergruppe der Gruppe $G = \mathrm{Gal}(g)$.

Der Beweis dieses Satzes kann Kapitel 25 von [32] entnommen werden. Wir merken an, daß eine allgemeinere Form dieses Satzes in [31] bewiesen wird. Hier wird die

Voraussetzung für R auf einen kommutativen Ring mit 1 abgeschwächt. Für unser Verfahren benötigen wir eine spezielle Form dieses Satzes.

Satz 2.9. *Es sei $g \in \mathbb{Z}[t]$ ein normiertes und irreduzibles Polynom. Ferner sei ein $p \in \mathbb{P}$ mit $p \nmid \operatorname{disc}(g)$ gegeben und es gelte $g(t) \equiv g_1(t) \cdots g_r(t) \bmod p\mathbb{Z}[t]$. Dann enthält $\operatorname{Gal}(g)$ eine zyklische Untergruppe U, die von einer Permutation π erzeugt wird. Wenn wir π in elementfremde Zykel zerlegen, so entspricht die Anzahl der Nullstellen, die in diesen Zykeln permutiert werden, den Graden der Polynome $g_i\,(1 \leq i \leq r)$. Weiterhin permutiert π gerade die Nullstellen eines irreduziblen Faktors g_i untereinander.*

Definition 2.10. *Sei $\Omega = \{\alpha_1, \ldots, \alpha_n\}$ eine Menge mit n Elementen. Eine bijektive Abbildung von Ω auf sich selbst heißt Permutation. Eine Permutation τ heißt Zykel der Länge r, wenn es eine r-elementige Teilmenge $\{\alpha_{i_1}, \ldots, \alpha_{i_r}\}$ von Ω gibt, so daß*

$$\tau(\alpha_{i_j}) = \alpha_{i_{j+1}} \text{ für } 1 \leq j < r,\ \tau(\alpha_{i_r}) = \alpha_{i_1} \text{ und } \tau(\alpha) = \alpha \text{ für } \alpha \notin \{\alpha_{i_1}, \ldots, \alpha_{i_r}\}$$

gilt. Wir bezeichnen einen solchen Zykel mit $(\alpha_{i_1}, \ldots, \alpha_{i_r})$. Ein Zykel τ enthält ein Element $\alpha \in \Omega$, falls $\alpha \in \{\alpha_{i_1}, \ldots, \alpha_{i_r}\}$ gilt.

Jede Permutation läßt sich bis auf Reihenfolge eindeutig als Produkt von elementfremden Zykeln schreiben. Zur Verdeutlichung von Satz 2.9 betrachten wir im folgenden ein Beispiel. Zur kürzeren Schreibweise schreiben wir nur $g \bmod p$ und meinen damit $g \bmod p\mathbb{Z}[t]$.

Beispiel 2.11. *Es seien $g(t) = t^4+2$ und $G = \operatorname{Gal}(g)$. Die Nullstellen von g seien mit $\alpha_1, \ldots, \alpha_4$ bezeichnet. Wir bestimmen im folgenden die Faktorisierungen von $g \bmod 3, 5, 7$ und erhalten:*

(i) $g(t) \equiv (t+2)(t+1)(t^2+1) \bmod 3,$
(ii) $g(t) \equiv t^4 + 2 \bmod 5,$
(iii) $g(t) \equiv (t^2+6t+4)(t^2+t+4) \bmod 7.$

Wir haben g nicht modulo 2 faktorisiert, da 2 ein Diskriminantenteiler von g ist. Mit Hilfe der Faktorisierung modulo 3 erhalten wir, daß G eine Permutation π enthält, deren Zerlegung in elementfremde Zykel bei passender Numerierung der Nullstellen gerade so aussieht:

$$\pi = (\alpha_1)(\alpha_2)(\alpha_3\alpha_4).$$

Auch die beiden folgenden Faktorisierungen erfüllen die Voraussetzung unseres Satzes. Wir können also zwei weitere Elemente von G bestimmen:

$$\tilde{\pi} = (\alpha_{i_1}\alpha_{i_2}\alpha_{i_3}\alpha_{i_4}) \text{ und } \hat{\pi} = (\alpha_{j_1}\alpha_{j_2})(\alpha_{j_3}\alpha_{j_4}).$$

Das Problem dieses Satzes ist, daß wir die verschiedenen Reihenfolgen der Nullstellen, die wir so erhalten, nicht umrechnen können. Deswegen können wir auf diese Weise nur eine ungefähre Vorstellung von den Elementen der Galoisgruppe bekommen.

5. Rekonstruktion von rationalen Zahlen

In diesem Abschnitt lösen wir das Problem, eine rationale Zahl aus einer modulo M–Approximation zu berechnen. Als wichtige Anwendung hiervon werden wir dieses Verfahren auf algebraische Zahlen verallgemeinern.

DEFINITION 2.12. *Für $a, b, s \in \mathbb{Z}$ und $M \in \mathbb{N}^{>1}$ mit $\operatorname{ggT}(b, M) = 1$ sei $\frac{a}{b} \equiv s \bmod M$, falls $a \equiv sb \bmod M$ gilt.*

Wir bezeichnen mit $\mathbb{Q}_{(M)}$ die Menge der rationalen Zahlen, bei denen der Nenner teilerfremd zu M ist. Dann wird durch

$$\Psi : \mathbb{Q}_{(M)} \to \mathbb{Z}/M\mathbb{Z} : \frac{a}{b} \mapsto s \text{ mit } \frac{a}{b} \equiv s \bmod M$$

eine Abbildung definiert, die nicht injektiv ist. Der folgende Satz liefert uns ein eindeutiges Urbild, wenn wir zusätzliche Bedingungen an die Größe von Zähler und Nenner stellen.

SATZ 2.13. *Seien $s, M \in \mathbb{N}$ mit $M > 1$ fixiert. Weiterhin existieren $a \in \mathbb{Z}, b \in \mathbb{N}$ mit*

$$(a, b) = 1 \textit{ sowie } |a|, b \leq \lambda\sqrt{M} \textit{ und } \frac{a}{b} \equiv s \bmod M,$$

wobei $\lambda = \frac{-1+\sqrt{5}}{2}$ ist. Dann sind a, b eindeutig bestimmt und können effizient berechnet werden.

Der Beweis dieses Satzes, der auf der Theorie der Kettenbrüche basiert, kann z.B. [10, 16] entnommen werden. Wir geben an dieser Stelle nur den Algorithmus an, der ungefähr dem Euklidischen Algorithmus entspricht.

ALGORITHMUS 2.14. (Rekonstruktion einer rationalen Zahl)

Input: *Ganze Zahlen* $s \geq 0$ *und* $M > 1$.

Output: *Ganze Zahlen* a *und* $b > 0$ *(falls existent) für die* $\frac{a}{b} \equiv s \bmod M$ *und* $|a|, b < \lambda\sqrt{M}$ *gilt.*

Schritt 1: *Setze* $u_{-1} := M$, $u_0 := s$, $v_{-1} := 0$, $v_0 := 1$ *und* $i := 0$.

Schritt 2: *Falls* $u_i < \sqrt{M}$ *gilt, gib* $(-1)^i \frac{u_i}{v_i}$ *aus und terminiere.*

Schritt 3: *Setze* $q_i := \lfloor \frac{u_{i-1}}{u_i} \rfloor$.

Schritt 4: *Setze* $u_{i+1} := u_{i-1} - q_i u_i$ *und* $v_{i+1} := v_{i-1} + q_i v_i$.

Schritt 5: *Setze* $i := i + 1$ *und gehe zu Schritt 2.*

Falls die Zahlen a und b mit den geforderten Bedingungen nicht existieren, so gibt der Algorithmus 0 aus. Falls 0 tatsächlich die gesuchte Lösung ist, so erkennen wir das daran, daß $s \equiv 0 \bmod M$ gilt. In [6] wird eine wesentlich effizientere Variante dieses Algorithmus angegeben, die auch in unseren Beispielen deutlich schneller ist. Da aber dieses Verfahren nur einen Bruchteil der Gesamtlaufzeit der späteren Algorithmen ausmacht, verzichten wir an dieser Stelle darauf, den verbesserten Algorithmus zu präsentieren.

Seien nun $E = \mathbb{Q}(\alpha)$ $(F = \mathbb{Q})$ ein algebraischer Zahlkörper und $\bar{\gamma} = \sum_{i=0}^{n-1} \bar{c}_i \alpha^i$ mit $\bar{c}_i \in \mathbb{Z}$ $(0 \leq i \leq n-1)$. Gesucht ist $\gamma = \sum_{i=0}^{n-1} c_i \alpha^i$ $(c_i \in \mathbb{Q})$ mit $\gamma \equiv \bar{\gamma} \bmod M\mathbb{Z}[\alpha]$, d.h. $\bar{c_i} \equiv c_i \bmod M$ $(0 \leq i \leq n-1)$. Es ist möglich γ aus $\bar{\gamma}$ dadurch zu erhalten, daß wir jeden einzelnen Koeffizienten rekonstruieren. Wir fassen dies in dem folgenden Lemma zusammen.

LEMMA 2.15. *Seien*

$$\gamma = \sum_{i=0}^{n-1} c_i \alpha^i \text{ und } \bar{\gamma} = \sum_{i=0}^{n-1} \bar{c}_i \alpha^i$$

mit $\gamma \equiv \bar{\gamma} \bmod M\mathbb{Z}[\alpha]$ *gegeben. Wenn die Zähler und Nenner von* $c_0, \ldots, c_{n-1}$ *betraglich kleiner als* B *sind und* $B < \lambda\sqrt{M}$ *gilt, so ist* γ *durch* $\bar{\gamma}$ *eindeutig bestimmt und rekonstruierbar.*

Wir merken an, daß Lemma 2.15 auch in Relativerweiterungen E/F $(F \neq \mathbb{Q})$ gilt. Allerdings müssen wir dann voraussetzen, daß die algebraische Zahl modulo $M\mathfrak{o}_E$ (bzw. $M\mathfrak{o}_F[\alpha]$) bekannt ist, um jeden Koeffizienten einzeln zu rekonstruieren.

6. Obere Abschätzungen für Koeffizienten von algebraischen Zahlen

In diesem Abschnitt werden wir einige wichtige obere Abschätzungen für die Koeffizienten von algebraischen Zahlen herleiten. Wir werden diese Abschätzungen einerseits bei der Berechnung von Einbettungen von Teilkörpern und andererseits bei der Berechnung von Automorphismen benötigen. Die folgenden Ergebnisse basieren auf [11, 20, 34]. Wir betrachten zuerst absolute Erweiterungen. Es gelten daher $F = \mathbb{Q}$ und $E = \mathbb{Q}(\alpha)$, wobei α Nullstelle eines normierten und irreduziblen Polynoms $f \in \mathbb{Z}[t]$ sei. Wir bezeichnen mit $\alpha = \alpha_1, \dots, \alpha_n$ alle Nullstellen von f in $\mathbb{C}$. Im folgenden seien

$$\gamma := \frac{1}{d}\sum_{i=0}^{n-1} c_i\alpha^i \in E \text{ mit } c_i \in \mathbb{Z},\ d \in \mathbb{N} \tag{2-1}$$

und

$$\gamma_j := \frac{1}{d}\sum_{i=0}^{n-1} c_i\alpha_j^i \ (1 \le j \le n). \tag{2-2}$$

Definition 2.16. *Für $\gamma \in E$ bezeichnen wir mit $|\gamma|_\infty := \max_{1\le i\le n}(|\gamma_i|)$ die Maximumsnorm einer algebraischen Zahl.*

Das folgende Lemma ist die Grundlage für die meisten Abschätzungen, die wir benötigen.

Lemma 2.17. *Für $\gamma \in E$ in der Form von (2-1) gilt:*

$$|c_i| \le d|\gamma|_\infty n(n-1)^{(n-1)/2}|\alpha|_\infty^{n(n-1)/2}|\operatorname{disc}(f)|^{-1/2}.$$

Beweis: Wir definieren dazu die folgende $n \times n$ Matrix:

$$A := \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1^1 & \alpha_2^1 & \cdots & \alpha_n^1 \\ \alpha_1^2 & \alpha_2^2 & \cdots & \alpha_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{n-1} & \alpha_1^{n-1} & \cdots & \alpha_n^{n-1} \end{pmatrix} \tag{2-3}$$

Es gilt dann $\operatorname{disc}(f) = (\det(A))^2$. Wir können also die c_i $(0 \le i \le n-1)$ bestimmen, indem wir das folgende Gleichungssystem lösen:

$$(c_0, \dots, c_{n-1}) = d(\gamma_1, \dots, \gamma_n)A^{-1}. \tag{2-4}$$

Wir erhalten:

$$dA^{-1} = \epsilon |\operatorname{disc}(f)|^{-\frac{1}{2}} \operatorname{Adj}(A), \text{ wobei } |\epsilon| = 1 \text{ gilt.} \tag{2-5}$$

Wir wollen nun die Einträge der Matrix $\operatorname{Adj}(A)$ abschätzen. Jedes Element dieser Matrix entspricht bis auf das Vorzeichen einer $(n-1) \times (n-1)$ Determinante, die dadurch entsteht, daß wir jeweils eine Zeile und Spalte von A streichen. Wir schätzen nun alle α_i durch $|\alpha|_\infty \geq 1$ ab und streichen die erste Zeile. Mit Hilfe der Hadamardschen Ungleichung auf den Zeilen erhalten wir für jeden Eintrag a von $\operatorname{Adj}(A)$:

$$a \leq \prod_{j=1}^{n-1} \sqrt{\sum_{i=1}^{n-1} |\alpha|_\infty^{2j}} = \prod_{j=1}^{n-1} \sqrt{n-1}\, |\alpha|_\infty^j = (n-1)^{(n-1)/2}\, |\alpha|_\infty^{n(n-1)/2}. \tag{2-6}$$

Wenn wir nun die Gleichungen (2-4), (2-5) und (2-6) zusammensetzen, so erhalten wir die Behauptung. □

Das folgende Korollar ist sehr nützlich, wenn wir Automorphismen in absoluten Erweiterungen ausrechnen wollen.

Korollar 2.18. *Sei γ eine weitere Nullstelle von f, die in E liegt. Dann gilt:*

$$|c_i| \leq d|\alpha|_\infty n(n-1)^{(n-1)/2} |\alpha|_\infty^{n(n-1)/2} |\operatorname{disc}(f)|^{-1/2}.$$

Beweis: Der Beweis folgt mit $|\alpha|_\infty = |\gamma|_\infty$ aus Lemma 2.17 □

Als nächstes werden wir eine Abschätzung für die Koeffizienten von gewissen algebraischen Zahlen in Relativerweiterungen angeben. Sei hierzu $F = \mathbb{Q}(\rho)$ und $m_\rho \in \mathbb{Z}[t]$ das normierte Minimalpolynom von ρ. Der Zahlkörper $E = F(\alpha)$ vom Grad n sei nun durch ein normiertes irreduzibles Polynom $f \in \mathbb{Z}[\rho][t]$ erzeugt, wobei α eine Nullstelle von f ist. Wir bezeichnen mit $\rho_1, \ldots, \rho_m$ die Nullstellen von m_ρ und mit $f_1, \ldots, f_m$ die Bilder von f unter der kanonischen Abbildung von $\mathbb{Q}(\rho)[t]$ nach $\mathbb{Q}(\rho_i)[t]$. Weiterhin sei $|f_i|_{\max}$ der Betrag der größten Nullstelle von f_i.

Lemma 2.19. *Sei*

$$\gamma = \frac{1}{d} \sum_{i=0}^{n-1} c_i \alpha^i \text{ mit } c_i \in \mathbb{Z}[\rho]$$

eine weitere Nullstelle von f, die in E liegt. Weiterhin sei

$$c_i = \sum_{j=0}^{m-1} c_{i,j} \rho^j \quad (0 \leq i \leq n-1).$$

Dann gilt:

$$|c_{i,j}| \leq d \max_{1 \leq j \leq m} (B_j) m(m-1)^{(m-1)/2} |\rho|_{\infty}^{m(m-1)/2} |\operatorname{disc}(m_\rho)|^{-1/2},$$

wobei

$$B_j \leq |f_j|_{max} n(n-1)^{(n-1)/2} |f_j|_{max}^{n(n-1)/2} |\operatorname{disc}(f_j)|^{-1/2}.$$

Beweis: Lemma 2.17 kann analog für den relativen Fall bewiesen werden. Hiernach folgt die Behauptung durch iterative Anwendung □

Die vorangegangenen Lemmata liefern a priori-Abschätzungen, die im allgemeinen nicht scharf sind. Außerdem sind sie auf den Fall von Gleichungsordnungen beschränkt. Falls wir bessere Abschätzungen benötigen, können wir die komplexe Basis ausrechnen und die Matrix A aus (2-3) über $\mathbb{C}$ invertieren.

KAPITEL III

Unverzweigte p-adische Erweiterungen

Wir werden in den folgenden Kapiteln Algorithmen entwickeln, die auf p-adischen Verfahren beruhen. Hierzu entwickeln wir Methoden, um in unverzweigten p-adischen Erweiterungen zu rechnen.

1. Grundlagen

Bevor wir zur Erzeugung von unverzweigten p-adischen Erweiterungen kommen, fassen wir noch einmal grundlegende Eigenschaften zusammen. Die Beweise der folgenden Aussagen können z.B. in [27, 4] nachgelesen werden. Im folgenden seien $\mathcal{F}$ und $\mathcal{E}$ unverzweigte Erweiterungen von $\mathbb{Q}_p$ mit Maximalordnungen $\mathfrak{o}_{\mathcal{F}}$ bzw. $\mathfrak{o}_{\mathcal{E}}$ und Primidealen $\mathfrak{p}$ bzw. $\mathfrak{P}$. Wir bezeichnen die zugehörigen Restklassenkörper mit $\bar{\mathcal{F}}$ und $\bar{\mathcal{E}}$.

Lemma 3.1. *Zu jeder endlichen Erweiterung $\mathbb{F}_q/\bar{\mathcal{F}}$ existiert genau eine unverzweigte Erweiterung $\mathcal{E}/\mathcal{F}$ derart, daß $\bar{\mathcal{E}}$ und $\mathbb{F}_q$ isomorph sind. Diese Erweiterung ist zyklisch und die Galoisgruppe ist isomorph zu* $\mathrm{Gal}(\bar{\mathcal{E}}/\bar{\mathcal{F}})$.

Lemma 3.2. *Es sei $\mathcal{E}/\mathcal{F}$ eine unverzweigte p-adische Erweiterung vom Grad s. Wenn $\rho_1, \dots, \rho_s$ die Vertreter für eine Basis von $(\mathfrak{o}_{\mathcal{E}}/\mathfrak{P})/(\mathfrak{o}_{\mathcal{F}}/\mathfrak{p})$ sind, so bilden sie eine $\mathfrak{o}_{\mathcal{F}}$–Basis von $\mathfrak{o}_{\mathcal{E}}$.*

Das vorangegangene Lemma gibt uns auf sehr einfache Weise die Möglichkeit, eine Basis für eine unverzweigte p-adische Erweiterung anzugeben, die gleichzeitig Basis für die Maximalordnung ist. Sei hierzu die unverzweigte Erweiterung $\mathcal{F}$ bereits gegeben. Wir wollen nun eine Basis für die Maximalordnung einer unverzweigten Erweiterung von $\mathcal{F}$ vom Grad s berechnen. Sei hierzu $\bar{w} \in \bar{\mathcal{F}}[t]$ ein normiertes, irreduzibles Polynom vom Grad s und $w \in \mathcal{F}[t]$ mit $w \equiv \bar{w} \bmod \mathfrak{p}$ gegeben. Dann ist die Gleichungsordnung $\mathfrak{o}_{\mathcal{F}}[\rho] = \mathfrak{o}_{\mathcal{F}} + \mathfrak{o}_{\mathcal{F}}\rho + \cdots + \mathfrak{o}_{\mathcal{F}}\rho^{s-1}$ bereits die Maximalordnung der unverzweigten Erweiterung $\mathcal{E}/\mathcal{F}$ vom Grad s, wobei ρ eine Nullstelle von w in $\mathcal{E}$ ist.

Mit Hilfe des folgenden Lemmas erhalten wir eine Methode, Elemente von $\mathfrak{o}_{\mathcal{E}}$ modulo $\mathfrak{P}^k$ zu reduzieren.

LEMMA 3.3. *Sei $\mathcal{E}/\mathcal{F}$ eine unverzweigte p-adische Erweiterung mit Ganzheitsbasis $1, \rho, \dots, \rho^{s-1}$. Sei nun $x = \sum_{i=0}^{s-1} x_i\rho^i \in \mathfrak{o}_{\mathcal{E}}$ ($x_i \in \mathfrak{o}_{\mathcal{F}}$) und $k \in \mathbb{N}$. Dann gilt $x \in \mathfrak{P}^k$ genau dann, wenn $x_i \in \mathfrak{p}^k$ ($0 \leq i < s$) gilt.*

Beweis: Wegen $\mathfrak{P} = \mathfrak{p}\mathfrak{o}_{\mathcal{E}}$ folgt $\mathfrak{P}^k = \mathfrak{p}^k\mathfrak{o}_{\mathcal{E}}$ und damit die Behauptung. □

2. Arithmetik in unverzweigten p-adischen Erweiterungen

Mit Hilfe der Lemmata 3.2 und 3.3 können wir unverzweigte p-adische Erweiterungen erzeugen, deren Gleichungsordnung bereits maximal ist. Wir werden dies im folgenden Beispiel verdeutlichen.

BEISPIEL 3.4. *Sei $p = 3$ und $v(t) = t^2 + t - 1 \in \mathbb{Z}_p[t]$. Da $v \bmod p\mathbb{Z}_p$ irreduzibel ist ($t^2 + t + 2$ ist irreduzibel in $\mathbb{F}_3[t]$), ist v auch in $\mathbb{Z}_p[t]$ irreduzibel und erzeugt somit eine unverzweigte Erweiterung $\mathcal{F}/\mathbb{Q}_p$ vom Grad 2. Für eine Nullstelle τ von v ist $1, \tau$ eine Ganzheitsbasis von $\mathfrak{o}_{\mathcal{F}}$. Nun ist $w(t) = t^2 + \tau t + 1 \in \mathfrak{o}_{\mathcal{F}}[t]$ irreduzibel, da $w \bmod \mathfrak{p}$ irreduzibel ist. Damit erzeugt w eine Erweiterung $\mathcal{E}/\mathcal{F}$ vom Grad 2. Sei nun ρ eine Nullstelle von w in $\mathcal{E}$. Dann ist $1, \rho$ eine Ganzheitsbasis von $\mathfrak{o}_{\mathcal{E}}/\mathfrak{o}_{\mathcal{F}}$.*

Wir werden nun erklären, wie wir in unverzweigten p-adischen Erweiterungen addieren und multiplizieren können. Dies geht analog zu den entsprechenden Arithmetikroutinen im Zahlkörperfall [30]. Da wir hier unsere Maximalordnungen stets als Gleichungsordnungen konstruieren können, werden wir uns auf diesen Fall beschränken. Im folgenden seien $x = \sum_{i=0}^{s-1} x_i\rho^i$ und $y = \sum_{i=0}^{s-1} y_i\rho^i$ Elemente von $\mathfrak{o}_{\mathcal{E}}$ ($x_i, y_i \in \mathfrak{o}_{\mathcal{F}}$ $(0 \leq i < s)$). Dann gilt:

$$x + y = \sum_{i=0}^{s-1}(x_i + y_i)\rho^i. \tag{3-1}$$

Die Multiplikation von x und y läßt sich am einfachsten mit Hilfe von Polynomoperationen beschreiben. Seien hierzu $P_x(t) := \sum_{i=0}^{s-1} x_i t^i \in \mathfrak{o}_{\mathcal{F}}[t]$ und $P_y(t) := \sum_{i=0}^{s-1} y_i t^i \in \mathfrak{o}_{\mathcal{F}}[t]$. Nun gilt trivialerweise $xy = P_x(\rho)P_y(\rho)$. Wir müssen jetzt nur noch das Problem lösen, eine Basisdarstellung für xy zu finden. Sei nun $P_{xy} := P_x P_y \bmod w$. Wegen $w(\rho) = 0$ folgt $P_{xy}(\rho) = xy$ und $\deg(P_{xy}) < s$. Mit

$$P_{xy}(t) = \sum_{i=0}^{s-1} z_i t^i \quad \text{erhalten wir} \quad xy = \sum_{i=0}^{s-1} z_i \rho^i. \tag{3-2}$$

Wir können also das Produkt von zwei p-adischen Zahlen dadurch bestimmen, daß wir das Produkt von zwei Polynomen vom Grad kleiner s über dem Koeffizientenring $\mathfrak{o}_\mathcal{F}$ bilden und anschließend das Produkt modulo w reduzieren. Wir merken an, daß wir bei dieser Reduktion keine Divisionen benötigen, da w normiert ist. Die Multiplikation von P_x und P_y kann mit s^2 Multiplikationen und Additionen in $\mathfrak{o}_\mathcal{F}$ durchgeführt werden. Weiterhin können wir die Polynomdivision in $s(s-1)$ Multiplikationen und Additionen in $\mathfrak{o}_\mathcal{F}$ berechnen. Wir benötigen also insgesamt $2s^2 - s$ Multiplikationen und Additionen in $\mathfrak{o}_\mathcal{F}$, um das Produkt xy zu berechnen. Diese Überlegungen führen zu dem folgenden Lemma.

Lemma 3.5. *Die Summe von zwei Zahlen $x, y \in \mathfrak{o}_\mathcal{E}$ kann mit s Additionen in $\mathfrak{o}_\mathcal{F}$ berechnet werden. Das Produkt zweier Zahlen $x, y \in \mathfrak{o}_\mathcal{E}$ kann mit $2s^2 - s$ Multiplikationen und Additionen in $\mathfrak{o}_\mathcal{F}$ berechnet werden.*

Die Division zweier Zahlen $x, y \in \mathfrak{o}_\mathcal{E}$ kann ebenfalls analog zum Zahlkörperfall durchgeführt werden. Da wir aber keine Divisionen benötigen, verzichten wir an dieser Stelle auf das Verfahren.

Zum Abschluß erklären wir, wie eine Zahl $x \in \mathbb{Z}_p$ modulo p^k reduziert werden soll. Im folgenden können wir davon ausgehen, daß p eine ungerade Primzahl und $k \in \mathbb{N}$ ist. Sei nun

$$x = \sum_{i=0}^{\infty} x_i p^i \in \mathbb{Z}_p \text{ mit } x_i \in \{\frac{1-p}{2}, \dots, \frac{p-1}{2}\}.$$

Dann ist $x \bmod p^k$ definiert als $\sum_{i=0}^{k-1} x_i p^i$, welches als ganze Zahl aus $\{\frac{1-p^k}{2}, \dots, \frac{p^k-1}{2}\}$ interpretiert werden kann. Wir haben das symmetrische Restsystem gewählt, um modulo p^k möglichst kleine Zahlen zu erhalten. Mit Hilfe dieser Reduktion in $\mathbb{Z}_p$ und Lemma 3.3 können wir nun beliebige p-adische Zahlen modulo Primidealpotenzen reduzieren. Wir sehen nun an dem folgenden Beispiel, wie dies in der Praxis aussieht.

Beispiel 3.6. *Seien $\mathcal{E}$ und $\mathcal{F}$ wie in Beispiel 3.4 definiert. Wir vereinbaren folgende Kurzschreibweise für Zahlen in $\mathfrak{o}_\mathcal{F}$ bzw. $\mathfrak{o}_\mathcal{E}$: $[[a_1, a_2], [a_3, a_4]] := a_1 + a_2\tau + a_3\rho + a_4\tau\rho \in \mathfrak{o}_\mathcal{E}$. Analog ist $[b_1, b_2] := b_1 + b_2\tau \in \mathfrak{o}_\mathcal{F}$. Sei nun $x = [[3, -3], [4, -4]]$ und $y = [[1, 2], [3, 4]]$. Wir berechnen nun das Produkt gemäß Formel (3-2) und erhalten $xy = [[1, -11], [-27, 51]]$. Wir wollen nun dieses Resultat modulo 3^2*

reduzieren. Dies ist äquivalent dazu, daß wir jeden der Koeffizienten modulo 9 *reduzieren. Wir erhalten damit* $xy \bmod 9 \equiv [[1, -2], [0, -3]]$.

3. Hensel–Lifting

Gegeben sei ein irreduzibles Polynom $f \in \mathbb{Z}[t]$ und eine Primzahl $p \nmid \operatorname{disc}(f)$. Sei nun $\tilde{f}$ die kanonische Einbettung von f nach $\mathbb{Z}_p[t]$. Wir wollen $\tilde{f}$ in einer unverzweigten Erweiterung $\mathcal{F}/\mathbb{Q}_p$ vollständig faktorisieren. Da $f \mod p$ keine doppelten Faktoren hat, hat $\tilde{f}$ auch keine doppelten Faktoren in $\mathcal{F}[t]$. Wir werden den folgenden Satz als sehr wichtiges Hilfsmittel benötigen.

Satz 3.7. *Hensel–Lemma*

Seien R ein kommutativer Ring mit 1 und $\mathfrak{b}$ ein Ideal von R. Ferner seien $f, f_{1,0}$ und $f_{2,0} \in R[t]$ normierte, nicht konstante Polynome, für die folgendes gilt:

(1) $f \equiv f_{1,0} f_{2,0} \mod \mathfrak{b}[t]$
(2) *Es existieren* $a_{i,0} \in R[t], i = 1, 2,\ a_{0,0} \in \mathfrak{b}[t]$ *mit* $a_{1,0} f_{1,0} + a_{2,0} f_{2,0} = 1 + a_{0,0}$.

Dann existieren für jedes $k \in \mathbb{N}$ Polynome $f_{1,k}, f_{2,k}, a_{1,k}, a_{2,k}$ und $a_{0,k} \in R[t]$, mit $f_{i,k}$ normiert und nicht konstant, sowie $\deg(a_{i,k}) < \deg(f_{3-i,k})$ $(i = 1, 2)$ *und* $a_{0,k} \in \mathfrak{b}^{2^k}[t]$*, so daß folgende Bedingungen erfüllt sind:*

(1) $f \equiv f_{1,k} f_{2,k} \mod \mathfrak{b}^{2^k}[t]$
(2) $f_{i,k} \equiv f_{i,0} \mod \mathfrak{b}[t]$
(3) $a_{1,k} f_{1,k} + a_{2,k} f_{2,k} = 1 + a_{0,k}$.

Der Beweis dieses Satzes kann z.B. [31] entnommen werden. Wir bezeichnen die $a_{1,0}$ und die $a_{2,0}$ aus dem obigen Satz als Kofaktoren. In unseren Beispielen ist $\mathfrak{b}$ stets ein Primideal und $R/\mathfrak{b}$ ein endlicher Körper. Deswegen können wir die $a_{i,0}$ sehr einfach mit Hilfe des erweiterten Euklidischen Algorithmus für Polynome über endlichen Körpern bestimmen. Wir geben an dieser Stelle noch einmal den Algorithmus [31] zum Hensel–Lifting zweier Faktoren an.

Algorithmus 3.8. (Hensel-Lifting)

Input: $R, \mathfrak{b}, k, f, f_{1,0}, f_{2,0}, a_{1,0}, a_{2,0}, a_{0,0}$ *wie im Satz* 3.7.

Output: *Polynome* $f_{1,k}, f_{2,k}$ *wie im Satz* 3.7.

Schritt 1: *Setze* $i := 0$.

Schritt 2: *Falls* $i = k$ *ist, gib* $f_{1,k}$ *und* $f_{2,k}$ *aus und terminiere.*

Schritt 3: *Setze* $d_i := f - f_{1,i}f_{2,i}$, $d_{1,i}^* := a_{2,i}d_i$ *und* $d_{2,i}^* := a_{1,i}d_i$.

Schritt 4: *Setze* $d_{j,i} := d_{j,i}^* \bmod f_{j,i}$ *(Division mit Rest) für* $(j = 1, 2)$.

Schritt 5: *Setze* $f_{j,i+1} := f_{j,i} + d_{j,i}$ *für* $(j = 1, 2)$.

Schritt 6: *Setze* $b_{j,i} := -a_{j,i}(a_{0,i} + a_{1,i}d_{1,i} + a_{2,i}d_{2,i})$ *für* $(j = 1, 2)$.

Schritt 7: *Setze* $a_{j,i+1} := a_{j,i} + b_{j,i}$ *für* $(j = 1, 2)$.

Schritt 8: *Setze* $a_{j,i+1} := a_{j,i+1} \bmod f_{3-j,i+1}$ *(Division mit Rest) für* $(j = 1, 2)$.

Schritt 9: *Setze* $a_{0,i+1} := a_{1,i}f_{1,i} + a_{2,i}f_{2,i} - 1$.

Schritt 10: *Setze* $i := i + 1$ *und gehe zu Schritt 2.*

Der Algorithmus ist nur für zwei Faktoren formuliert. Er kann aber auch auf mehrere Faktoren verallgemeinert werden. Dies wird dadurch realisiert, daß wir mehrere Faktoren zu einem zusammenfassen und sukzessive den obigen Algorithmus anwenden. Wir verdeutlichen dies am folgenden Beispiel.

BEISPIEL 3.9. *Sei* $f \equiv f_1f_2f_3 \bmod p$. *Setze* $f_{1,2} := f_1f_2$ *und bestimme mit Hilfe von Algorithmus* 3.8 *die folgende Faktorisierung:* $f \equiv \tilde{f}_{1,2}\tilde{f}_3 \bmod p^k$. *Anschließend berechne mit Hilfe von Algorithmus* 3.8 *die Faktorisierung* $\tilde{f}_{1,2} \equiv \tilde{f}_1\tilde{f}_2 \bmod p^k$. *Beide Ergebnisse liefern die gewünschte Faktorisierung* $f \equiv \tilde{f}_1\tilde{f}_2\tilde{f}_3 \bmod p^k$.

Wir sind nun in der Lage, ein Verfahren zur Faktorisierung eines Polynoms $f \in \mathbb{Z}_p[t]$ über einer Erweiterung $\mathcal{F}$ modulo $\mathfrak{p}^k$ anzugeben:

(1) Faktorisiere $f \equiv f_1 \cdots f_r \bmod \mathfrak{p}$.
(2) Bestimme sukzessive $f \equiv \tilde{f}_1 \cdots \tilde{f}_r \bmod \mathfrak{p}^k$ mit Hilfe des Hensel-Liftings.

Der Nachteil dieses Ansatzes ist, daß wir alle Berechnungen in $\mathcal{F}$ durchführen müssen, die bei großem Grad sehr aufwendig werden können. Wenn z.B. der Grad von $\mathcal{F}/\mathbb{Q}_p$ 10 ist, so müssen wir für eine Multiplikation in $\mathcal{F}$ 190 Multiplikationen in $\mathbb{Z}_p$ durchführen. Wir wollen nun die Idee verfolgen, einzelne Faktorisierungen in kleineren Körpern durchzuführen. Dazu betrachten wir das folgende Verfahren:

(1) Faktorisiere $f \equiv f_1 \cdots f_s \bmod p$.
(2) Berechne sukzessive $f \equiv \tilde{f}_1 \cdots \tilde{f}_s \bmod p^k$ mit Hilfe des Hensel-Liftings.
(3) Für $i = 1, \ldots, s$ tue folgendes:
    (a) Faktorisiere $\tilde{f}_i \equiv f_{i,1} \cdots f_{i,r_i} \bmod \mathfrak{p}$.
    (b) Bestimme sukzessive $\tilde{f}_i \equiv \tilde{f}_{i,1} \cdots \tilde{f}_{i,r_i} \bmod \mathfrak{p}^k$ mit Hilfe des Hensel-Liftings.

(4) Füge die Faktorisierung zusammen: $f \equiv \tilde{f}_{1,1} \cdots \tilde{f}_{s,r_s} \bmod \mathfrak{p}^k$.

Wir verdeutlichen dies an dem folgenden Beispiel.

BEISPIEL 3.10. *Sei* $f(t) = t^{12} + t^{11} - 28t^{10} - 40t^9 + 180t^8 + 426t^7 + 89t^6 - 444t^5 - 390t^4 - 75t^3 + 27t^2 + 11t + 1$. *Wir wollen* f *nun über einer Erweiterung* $\mathcal{F}/\mathbb{Q}_3$ *vom Grad 3 modulo* $\mathfrak{p}^2$ *faktorisieren. In einem ersten Schritt bestimmen wir die Faktorisierung modulo 9 und erhalten:*

$$f \equiv (t^3 + 2t - 2)(t^3 + t^2 - 3t + 2)(t^3 + 4t^2 - 4t - 2)(t^3 - 4t^2 + 2t - 1) \bmod 3^2.$$

In einem zweiten Schritt berechnen wir nun das Hensel–Lifting von jedem der Faktoren in $\mathcal{F}[t]$ *modulo* $\mathfrak{p}^2$*, wobei* $\mathcal{F}$ *von einer Nullstelle von* $v(t) = t^3 - t + 1$ *erzeugt wird:*

$$\begin{aligned}
t^3 + 2t - 2 &\equiv (t + [3, -4, 0])(t + [-2, 2, 3])(t + [-1, 2, -3]) && \bmod \mathfrak{p}^2,\\
t^3 + t^2 - 3t + 2 &\equiv (t + [3, -2, -4])(t + [3, -1, -4])(t + [4, 3, -1]) && \bmod \mathfrak{p}^2,\\
t^3 + 4t^2 - 4t - 2 &\equiv (t + [2, -3, -1])(t + [4, 1, -4])(t + [-2, 2, -4]) && \bmod \mathfrak{p}^2,\\
t^3 - 4t^2 + 2t - 1 &\equiv (t + [-4, 2, 4])(t + [-4, 1, 4])(t + [4, -3, 1]) && \bmod \mathfrak{p}^2.
\end{aligned}$$

Obwohl wir ein Polynom vom Grad 12 faktorisiert haben, brauchten wir das Hensel–Lifting über $\mathcal{F}$ nur auf Polynome vom Grad 3 anwenden. Die anderen Faktorisierungen konnten über $\mathbb{Z}_p$ durchgeführt werden. Bei diesem Beispiel war es sehr wichtig, daß wir $\mathbb{Z}_p$ auf sehr einfache Weise in $\mathfrak{o}_\mathcal{F}$ einbetten konnten. Wir wollen diese Idee nun weiterverfolgen. Nehmen wir an, daß wir ein irreduzibles Polynom f vom Grad 4 in $\mathbb{Z}_p$ haben, welches wir über einer Erweiterung $\mathcal{E}$ vom Grad 4 über $\mathbb{Z}_p$ faktorisieren wollen. Da es (bis auf Isomorphie) nur eine unverzweigte Erweiterung vom Grad 4 über $\mathbb{Z}_p$ gibt, welche zyklisch ist, zerfällt f über $\mathcal{E}$ in Linearfaktoren. Wir wollen nun ausnutzen, daß $\mathcal{E}$ einen Teilkörper $\mathcal{F}$ vom Grad 2 enthält. Da alle Erweiterungen zyklisch sind, zerfällt f in $\mathfrak{o}_\mathcal{F}[t]$ in zwei Faktoren vom Grad 2. Eine natürliche Idee ist es also, zuerst f in $\mathfrak{o}_\mathcal{F}[t]$ zu faktorisieren, um anschließend die zwei quadratischen Faktoren in $\mathfrak{o}_\mathcal{E}[t]$ zu faktorisieren. Hierbei müssen wir allerdings das Problem lösen, wie wir auf einfache Weise Elemente von $\mathfrak{o}_\mathcal{F}$ nach $\mathfrak{o}_\mathcal{E}$ einbetten können. Zu diesem Zweck ist es hinreichend, für jedes Basiselement der Basis von $\mathfrak{o}_\mathcal{F}/\mathbb{Z}_p$ ein entsprechendes Bild in $\mathfrak{o}_\mathcal{E}$ anzugeben. Ein solches Bild kann stets mittels Newton–Lifting 3.14 berechnet werden, welches aber sehr aufwendig sein kann. Wir werden daher die p-adischen Erweiterungen relativ erzeugen, was zur Folge hat, daß unsere gesuchten Einbettungen trivial sind. Dies können wir sehr gut an Beispiel 3.6 sehen. Hier ist $1, \tau$ eine Ganzheitsbasis von $\mathfrak{o}_\mathcal{F}$ über $\mathbb{Z}_p$, während $\mathfrak{o}_\mathcal{E}$ über $\mathbb{Z}_p$ als Ganzheitsbasis $1, \tau, \rho, \rho\tau$ hat. So ist es für uns sehr leicht möglich, Elemente von $\mathfrak{o}_\mathcal{F}$ nach $\mathfrak{o}_\mathcal{E}$ einzubetten. Wir fassen diese

Überlegungen in dem folgenden Lemma zusammen. Zuvor benötigen wir aber noch eine Definition.

DEFINITION 3.11. *Seien $p \in \mathbb{P}$, $n = p_1 \cdots p_r$ mit $p_i \in \mathbb{P}$ und $p_1 \leq p_2 \leq \ldots \leq p_r$. Wir nennen eine Erweiterung $\mathcal{F} = \mathcal{F}_r$ über $\mathbb{Q}_p = \mathcal{F}_0$ sukzessiv erzeugt, wenn $\mathcal{F}_i = \mathcal{F}_{i-1}(\tau_i)$ gilt, wobei τ_i Nullstelle eines irreduziblen und normierten Polynoms $v_i \in \mathfrak{o}_{\mathcal{F}_{i-1}}$ vom Grad p_i ist ($1 \leq i \leq r$). Wir bezeichnen die Primideale in $\mathfrak{o}_{\mathcal{F}_i}$ mit $\mathfrak{p}_i$.*

Der Beweis des folgenden Lemmas folgt direkt.

LEMMA 3.12. *Sei $p \in \mathbb{P}$ und $\mathcal{F}_r/\mathbb{Q}_p$ vom Grad n sukzessiv erzeugt. Dann lassen sich die Elemente von $\mathfrak{o}_{\mathcal{F}_{i-1}}$ kanonisch nach $\mathfrak{o}_{\mathcal{F}_i}$ einbetten ($1 \leq i \leq r$).*

Wir fassen unseren Hensel-Lifting Algorithmus noch einmal zusammen.

ALGORITHMUS 3.13. (Hensel–Lifting)

<u>Input</u>: $p \in \mathbb{P}, k \in \mathbb{N}$, $f \in \mathbb{Z}_p[t]$, $\mathcal{F}_r/\mathbb{Q}_p$ *sukzessiv erzeugt.*

<u>Output</u>: *Faktorisierung von f in $\mathfrak{o}_{\mathcal{F}_r}[t]$ modulo $\mathfrak{p}_r^k$.*

<u>Schritt 1</u>: *Berechne die Faktorisierung von $f \equiv f_{0,1} \cdots f_{0,s_0} \mod p^k$.*

<u>Schritt 2</u>: *Für $i = 1, \ldots, r$ tue folgendes*
1. *Berechne die Faktorisierungen von $f_{i-1,j}$ in $\mathfrak{o}_{\mathcal{F}_i} \bmod \mathfrak{p}_i^k$ ($1 \leq j \leq s_{i-1}$).*
2. *Füge die Faktorisierung zusammen: $f \equiv f_{i,1} \cdots f_{i,s_i} \mod \mathfrak{p}_i^k$.*

<u>Schritt 3</u>: *Gib die Faktorisierung $f \equiv f_{r,1} \cdots f_{r,s_r} \bmod \mathfrak{p}_r^k$ aus.*

4. Das verallgemeinerte Newton–Lifting

Sei F ein algebraischer Zahlkörper und R eine Ordnung in F. Der Spezialfall $F = \mathbb{Q}$ und $R = \mathbb{Z}$ ist dabei natürlich auch möglich. Gegeben seien über F irreduzible Polynome $f, g \in R[t]$ vom Grad n bzw. m, wobei eine Nullstelle α von f einen Zahlkörper $E = F(\alpha)$ erzeuge. Weiterhin sei eine modulo p–Approximation $\beta_0 \in R$ einer Nullstelle von g bekannt, d.h.

$$\beta_0 = \sum_{i=0}^{n-1} b_{0,i}\alpha^i \text{ mit } g(\beta_0) \equiv 0 \bmod pR.$$

Wir schreiben im folgenden $\bmod p^k$ und meinen damit $\bmod p^kR$. Da wir weiterhin $\mathrm{ggT}(pR, \mathfrak{d}(f)\mathfrak{d}(g)) = R$ voraussetzen, können wir mit Hilfe des erweiterten Euklidischen Algorithmus für Polynome über endlichen Körpern ein Element $\omega_0 \in E$ berechnen mit $\omega_o g'(\beta_0) \equiv 1 \bmod p$.

Wir werden im folgenden Elemente β_k, ω_k mit den folgenden Eigenschaften konstruieren:

$$\beta_{k+1} \equiv \beta_k \bmod p^{2^k} \tag{3-3}$$

$$\omega_{k+1} \equiv \omega_k \bmod p^{2^k} \tag{3-4}$$

$$g(\beta_k) \equiv 0 \bmod p^{2^k} \tag{3-5}$$

$$\omega_k g'(\beta_k) \equiv 1 \bmod p^{2^k}. \tag{3-6}$$

Dazu werden wir die folgende doppelte Iteration anwenden:

$$\beta_{k+1} \equiv \beta_k - \omega_k g(\beta_k) \bmod p^{2^{k+1}} \tag{3-7}$$

$$\omega_{k+1} \equiv \omega_k[2 - \omega_k g'(\beta_{k+1})] \bmod p^{2^{k+1}}. \tag{3-8}$$

Die Korrektheit dieser doppelten Iteration kann durch einfaches Nachrechnen bewiesen werden [16]. Wir können dieses Problem auch durch die folgende einfache Iteration lösen:

$$\beta_{k+1} \equiv \beta_k - \frac{g(\beta_k)}{g'(\beta_k)} \bmod p^{2^{k+1}}.$$

Der Nachteil dieses Ansatzes ist die Division, die wir durchführen müssen. Diese Division wird in unserem Ansatz durch drei Multiplikationen ersetzt, die wesentlich schneller berechnet werden können. Wir machen uns nun Gedanken, wie wir die doppelte Iteration geschickt auswerten können. In jedem Schritt ist es am aufwendigsten, $g(\beta_k)$ bzw. $g'(\beta_{k+1})$ zu berechnen. Als erster Ansatz ist es möglich, diese Evaluierungen mit dem Hornerschema zu berechnen. Da $\deg(g) = m$ ist, können wir diese mit $(m-1) + (m-2) = 2m-3$ Multiplikationen von algebraischen Zahlen vom Grad n berechnen. Wir berechnen die Multiplikation von zwei algebraischen Zahlen vom Grad n mit $2n^2 - n$ Multiplikationen in R. Insgesamt erhalten wir also $(2m-3)(2n^2-n)$ Multiplikationen in R.

Wir werden nun einen anderen Ansatz zur Berechnung der Evaluierungen angeben. Wir berechnen zuerst die Werte $1, \beta, \ldots, \beta^m$, wofür wir wir $m-1$ Multiplikationen von algebraischen Zahlen vom Grad n benötigen. Hiernach nutzen wir diese Information, um die Polynome g bzw. g' auszuwerten. Da die Koeffizienten aus R sind, benötigen wir hierzu $m + (m-1)$ Skalarmultiplikationen von Elementen in R

und algebraischen Zahlen vom Grad n. Dies führt zu $n(2m-1)$ Multiplikationen in R. Wir erhalten also insgesamt $(m-1)(2n^2-n)+n(2m-1) = (2m-2)n^2+mn$ Multiplikationen in R. Im Vergleich zum Hornerschema ($(4m-6)n^2-(2m-3)n$ Multiplikationen in R) sparen wir knapp die Hälfte der Multiplikationen ein. Bei dieser Betrachtung wurde die Größe der einzelnen Faktoren vernachlässigt. Praktische Erfahrungen zeigen, daß unser Ansatz ca. 50% schneller ist. Es ist klar, daß alle Berechnungen modulo $p^{2^{k+1}}$ durchgeführt werden. Zum Abschluß geben wir einen Algorithmus zum Newton–Lifting an.

Algorithmus 3.14. (Newton–Lifting)

Input: $p \in \mathbb{P}, k \in \mathbb{N},\ f, g \in R[t],\ \beta_0 \in E$ *mit* $g(\beta_0) \equiv 0 \bmod p$.

Output: $\beta_k \in E$ *mit* $g(\beta_k) \equiv 0 \bmod p^{2^k}$ *und* $\beta_k \equiv \beta_0 \bmod p$.

Schritt 1: *Berechne* $\omega_0 \in E$ *mit* $\omega_0 g'(\beta_0) \equiv 1 \bmod p$.

Schritt 2: $\beta_1 \equiv \beta_0 - \omega_0 g(\beta_0) \bmod p^2$.

Schritt 3: *Für* $i = 1, \ldots, k-1$ *tue folgendes:*
(1) *Berechne* $1, \beta_i, \ldots, \beta_i^m \bmod p^{2^{i+1}}$.
(2) $\omega_i \equiv \omega_{i-1}[2 - \omega_{i-1} g'(\beta_i)] \bmod p^{2^i}$.
(3) $\beta_{i+1} \equiv \beta_i - \omega_i g(\beta_i) \bmod p^{2^{i+1}}$.

Schritt 4: *Gib* β_k *aus und terminiere.*

Wir werden im folgenden noch eine Variante des Newton-Liftings angeben, die für praktische Anwendungen sehr wichtig ist. Dabei werden wir sogenannte „Pseudo-Tests“ durchführen. Unter einem Pseudo-Test verstehen wir eine notwendige Bedingung, die einerseits sehr einfach zu testen ist und andererseits eine hohe Wahrscheinlichkeit hat, daß sie hinreichend ist.

Das Ziel dieses Verfahrens ist es, ein Element $\beta \in E$ zu finden, für welches $g(\beta) = 0$ gilt. Aufgrund von Abschätzungen wissen wir, daß wir dieses Element von β_k mit Hilfe von Lemma 2.15 erhalten können. In der Praxis zeigt sich, daß die Abschätzungen für k, die wir a priori bestimmen können, wesentlich zu groß sind. Es wäre also möglich, β mit Hilfe eines wesentlich kleineren k's zu bestimmen. Mit Hilfe der Evaluierung von g an der Stelle β könnten wir dann beweisen, daß unser Ergebnis korrekt ist. Leider erweist sich eine Evaluierung von g mit einem „falschen“ β als sehr aufwendig. Es wäre also nützlich, einen guten Pseudo-Test zu finden. Ein solcher Test wird in dem folgenden Algorithmus verwendet.

Algorithmus 3.15. (Newton-Lifting)

Input: $p \in \mathbb{P}, k \in \mathbb{N},\ f, g \in R[t],\ \beta_0 \in E$ *mit* $g(\beta_0) \equiv 0 \bmod p$.

Output: *$\beta \in E$ mit $g(\beta) = 0$ oder „falsch“.*

Schritt 1: *Berechne $\omega_0 \in E$ mit $\omega_0 g'(\beta_0) \equiv 1 \bmod p$.*

Schritt 2: $\beta_1 \equiv \beta_0 - \omega_0 g(\beta_0) \bmod p^2$.

Schritt 3: *Setze $\beta_{alt} := 0$.*

Schritt 4: *Für $i = 1, \dots, k-1$ tue folgendes:*

(1) *Berechne $1, \beta_i, \dots, \beta_i^m \bmod p^{2^{i+1}}$.*
(2) $\omega_i \equiv \omega_{i-1}[2 - \omega_{i-1} g'(\beta_i)] \bmod p^{2^i}$.
(3) $\beta_{i+1} \equiv \beta_i - \omega_i g(\beta_i) \bmod p^{2^{i+1}}$.
(4) *Setze β_{neu} auf das Ergebnis der Rekonstruktion von β_{i+1} und $p^{2^{i+1}}$ mit Hilfe von Lemma 2.15.*
(5) *Falls $\beta_{alt} = \beta_{neu}$ gilt, berechne $g(\beta_{neu})$. Falls diese Evaluierung 0 ergibt, terminiere und gebe β_{neu} aus.*
(6) *Setze $\beta_{alt} := \beta_{neu}$.*

Schritt 5: *Berechne (falls noch nicht geschehen) $g(\beta_{neu})$. Falls das Ergebnis 0 ist, gebe β_{neu} aus und terminiere.*

Schritt 6: *Terminiere mit der Meldung: „falsch“.*

KAPITEL IV

Zur Berechnung von Teilkörpern

In diesem Kapitel werden wir einen Algorithmus zur Berechnung von Teilkörpern entwickeln. Die hier vorgestellten Verfahren sind eine Weiterentwicklung der Verfahren aus [16]. Die bisher bekannten Methoden konnten an mehreren Stellen um Größenordnungen verbessert werden. Der hier vorgestellte Algorithmus teilt sich grob in die folgenden drei Schritte ein:

(1) Berechnung von möglichen Blocksystemen
(2) Berechnung von erzeugenden Polynomen für die Teilkörper
(3) Berechnung der Einbettungen.

1. Grundlagen

Wir betrachten in diesem Kapitel nur absolute Erweiterungen, d.h., daß $F = \mathbb{Q}$ gilt. Es sei $E = \mathbb{Q}(\alpha)$ ein algebraischer Zahlkörper vom Grad n, wobei α eine Nullstelle eines irreduziblen und normierten Polynoms $f \in \mathbb{Z}[t]$ ist. Wir wollen nun alle nicht trivialen Teilkörper $L = \mathbb{Q}(\beta)$ von E vom Grad m berechnen. Hierbei ist $g \in \mathbb{Z}[t]$ das normierte Minimalpolynom von β. Wir nennen g ein erzeugendes Polynom für den Teilkörper L.

Wir beschränken uns in diesem Kapitel auf Zahlkörper, die von normierten Polynomen f erzeugt werden. Die hier vorgestellten Algorithmen lassen sich recht einfach auf den nicht normierten Fall verallgemeinern. Die Darstellung dieser Methoden ist aber recht technisch, weswegen wir hier darauf verzichten. Bei der Implementierung für den nicht normierten Fall sollte auf die drei folgenden Dinge geachtet werden:

(1) Die Primzahl p sollte zusätzlich so gewählt sein, daß p nicht den Leitkoef-

fizienten von f teilt.

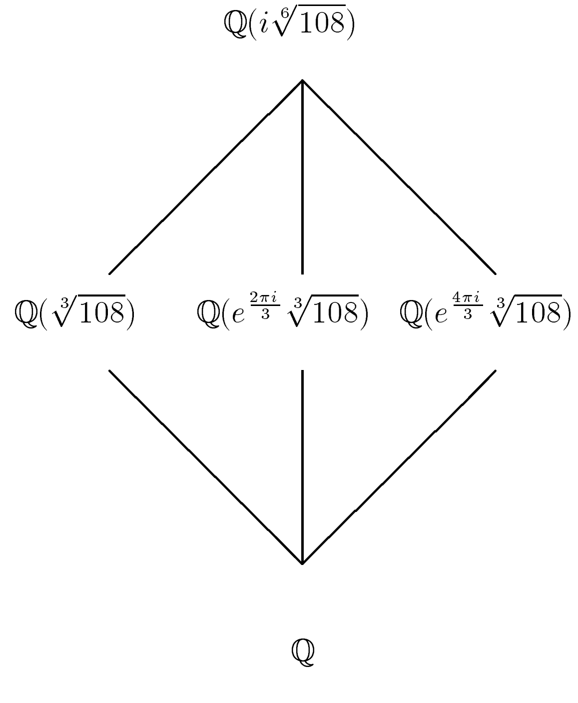
(2) Das Hensel-Lifting sollte für den nicht normierten Fall angepaßt werden. Hierzu verweisen wir auf [14, Seite 240–250].

(3) Es wird eine Arithmetik für Gleichungsordnungen benötigt, die von nicht normierten Polynomen erzeugt werden.

Wie wir an dem folgenden Beispiel sehen werden, reicht die Angabe eines erzeugenden Polynoms g nicht aus, um den Teilkörper L eindeutig zu identifizieren. Hierzu ist es notwendig, ein Einbettungspolynom $\omega \in \mathbb{Q}[t]$ mit $\omega(\alpha) = \beta$ zu bestimmen.

Beispiel 4.1. *Wir betrachten $f(t) = t^6 + 108$. Dieses Polynom erzeugt einen Körper vom Grad 6 über $\mathbb{Q}$. Dieser Körper besitzt 3 Teilkörper vom Grad 3, die alle durch das Minimalpolynom $g(t) = t^3 - 108$ erzeugt werden. Die Nullstellen von g sind $\beta_1 = \sqrt[3]{108}$, $\beta_2 = e^{\frac{2\pi i}{3}}\sqrt[3]{108}$ und $\beta_3 = e^{\frac{4\pi i}{3}}\sqrt[3]{108}$. Durch diese Nullstellen werden jeweils paarweise verschiedene Zahlkörper erzeugt, die aber alle isomorph sind. Wir können diese Körper aber durch ihre Einbettung in $\mathbb{Q}(\alpha)$ unterscheiden. Mit $\alpha = i\sqrt[6]{108}$ gilt dann:*

(i) $\beta_1 = -\alpha^2$ *und damit* $\omega(t) = -t^2$,
(ii) $\beta_2 = \frac{1}{2}\alpha^2 + \frac{1}{12}\alpha^5$ *und damit* $\omega(t) = \frac{1}{2}t^2 + \frac{1}{12}t^5$,
(iii) $\beta_3 = \frac{1}{2}\alpha^2 - \frac{1}{12}\alpha^5$ *und damit* $\omega(t) = \frac{1}{2}t^2 - \frac{1}{12}t^5$.



Wir sehen an dem vorangegangenen Beispiel, daß die Koeffizienten des Einbettungspolynoms nicht notwendigerweise in $\mathbb{Z}$ sind. Dies liegt daran, daß die Gleichungsordnung $\mathbb{Z}[\alpha]$ im allgemeinen nicht die Maximalordnung ist.

Wir können also im folgenden jeden Teilkörper L durch ein Paar (g, ω) darstellen, welches die Eigenschaft $g(\omega(\alpha)) = 0$ besitzt. Umgekehrt entspricht jedes solche Paar einem Teilkörper.

2. Imprimitivitätsgebiete und Blöcke

In diesem Abschnitt werden wir einige Eigenschaften über Imprimitivitätsgebiete von transitiven Permutationsgruppen herleiten. Hierzu sei $G = \mathrm{Gal}(f)$ die Galoisgruppe des von f erzeugten Zerfällungskörpers. Diese operiert auf den Nullstellen $\Omega := \{\alpha = \alpha_1, \ldots, \alpha_n\}$ von f transitiv, da f irreduzibel ist.

Definition 4.2. *(Definition von Imprimitivitätsgebieten bzw. Blöcken)*

(i) $\emptyset \neq \Delta \subseteq \Omega$ *heißt Block (Imprimitivitätsgebiet), falls* $\Delta^\tau \cap \Delta \in \{\emptyset, \Delta\}$ *für alle* $\tau \in G$ *gilt. Hierbei ist* $\Delta^\tau := \{\tau(\alpha) \mid \alpha \in \Delta\}$.

(ii) $\Delta = \{\alpha_i\}$ $(1 \leq i \leq n)$ *und* $\Delta = \Omega$ *sind triviale Blöcke.* G *heißt imprimitiv, falls* G *einen nicht trivialen Block besitzt, ansonsten heißt* G *primitiv.*

(iii) Blöcke $\Delta_1, \ldots, \Delta_m$ *mit* $\Delta_i \neq \Delta_j$ $(1 \leq i < j \leq m)$ *heißen (echtes) Blocksystem, falls die Menge* $\{\Delta_1, \ldots, \Delta_m\}$ *unter* G *invariant bleibt.*

Da mit Δ auch stets Δ^τ ein Block ist, folgt, daß jeder Block Teil eines Blocksystems ist. Die Anzahl der Elemente in einem Block, bzw. die Anzahl der Elemente in jedem Block eines Blocksystems heißt die Größe des Blocks bzw. des Blocksystems. Wir bezeichnen $G_\Delta := \{g \in G \mid \Delta^g = \Delta\}$ als den Stabilisator von Δ.

Der Beweis des folgenden Satzes kann z.B. in [35, Theorem 2.3] gefunden werden. Zusammen mit dem Hauptsatz der Galoistheorie 2.6 erhalten wir den Zusammenhang zwischen Teilkörpern und Blöcken.

Satz 4.3. *Es existiert eine Bijektion zwischen den Untergruppen* $G_\alpha < H < G$ *und den Blöcken, welche* α *enthalten.*

Das folgende Diagramm illustriert unsere Situation:

$$\begin{array}{ccc}
\mathbb{Q}(\alpha_1,\dots,\alpha_n) & \{id\} & \\
\Big| & \Big| & \\
\mathbb{Q}(\alpha_1) & G_{\alpha_1} & \{\alpha_1\} \\
\Big|\; d & \Big| & \Big| \\
\mathbb{Q}(\beta) & H & H\alpha_1 = \{\alpha_{i_1},\dots,\alpha_{i_d}\} = \Delta_1 \\
\Big|\; m = \frac{n}{d} & \Big| & \Big| \\
\mathbb{Q} & G & \{\alpha_1,\dots,\alpha_n\}
\end{array}$$

Wir erhalten also eine Bijektion zwischen den Teilkörpern L von E und den Blöcken Δ, die α enthalten. In diesem Fall sagen wir, daß L zu Δ korrespondiert.

LEMMA 4.4. *Seien B_1 und B_2 zwei Blöcke, die α enthalten, mit korrespondierenden Teilkörpern L_1 und L_2 von E. Dann ist $B = B_1 \cap B_2$ wieder ein Block, der α enthält. Er korrespondiert zu einem Teilkörper $L = L_1L_2$ von E. Weiterhin ist L_1 ein Teilkörper von L_2 genau dann, wenn $B_2 \subseteq B_1$ gilt.*

Beweis: Seien H_1, H_2 die aufgrund der Bijektion aus Satz 4.3 zugeordneten Untergruppen von G zu B_1, B_2. In [35] wird bewiesen, daß $H_1 \cap H_2$ durch die Bijektion auf $B_1 \cap B_2$ abgebildet wird. Weiterhin gilt $H_2 \subseteq H_1$ genau dann, wenn $B_2 \subseteq B_1$ gilt. Die Behauptung folgt mit Hilfe der Galoistheorie. □

Dieses Lemma wird für die Konstruktion von Teilkörpern von großer Bedeutung sein. Dadurch werden wir in der Lage sein, Informationen von bereits berechneten Teilkörpern für weitere zu berechnende Teilkörper auszunutzen.

Nehmen wir nun einmal an, daß wir einen Block Δ_1, der α enthält und damit auch ein komplettes Blocksystem $\Delta_1, \dots, \Delta_m$ kennen, welches zu L korrespondiert. Mit $H = G_{\Delta_1}$ erhalten wir $L = \mathrm{Fix}(H)$. Sei nun

$$\delta_i := \prod_{\gamma \in \Delta_i} \gamma \; (1 \leq i \leq m). \tag{4-1}$$

Damit erhalten wir $\delta_1 \in \mathrm{Fix}(H) = L$, weiterhin sind die δ_i $(1 \leq i \leq m)$ alle Konjugierten von δ_1. Hieraus folgt, daß das Polynom

$$g(t) = \prod_{i=1}^{m}(t - \delta_i) \in \mathbb{Z}[t] \tag{4-2}$$

das charakteristische Polynom von $\delta_1 \in L$ über $\mathbb{Q}$ und damit von der Form $g(t) = \hat{g}^j$ mit $j \in \mathbb{N}$ und einem irreduziblen Polynom $\hat{g}$ ist. Falls das Polynom g selber irreduzibel ist, haben wir bereits ein erzeugendes Polynom für den Teilkörper L gefunden, anderenfalls bedeutet dies, daß das Polynom g doppelte Nullstellen hat. Da dies äquivalent zu $\mathrm{ggT}(g, g') \neq 1$ ist, können wir diese Fälle einfach unterscheiden. In diesem Fall wenden wir eine lineare Transformation $f(t) \leftarrow f(t-a)$ mit $a \in \mathbb{Z}$ auf f an. Wir werden später beweisen, daß maximal n solcher Substitutionen wiederum zu doppelten Nullstellen bei g führen.

Wir haben nun das Problem der Teilkörperberechnung darauf reduziert, daß wir Blocksysteme der Galoisgruppe G berechnen müssen. Diese Reduzierung ist allerdings nur theoretischer Natur, da die Galoisgruppenberechnung für größere Grade ein sehr schwieriges Problem ist. Außerdem würden wir neben dem Gruppennamen die Aktion der Galoisgruppe auf den Nullstellen brauchen.

Wir werden die Nullstellen in geeigneten p-adischen Körpern identifizieren, wobei wir die Kenntnis von zyklischen Untergruppen von G ausnutzen werden, die wir mit van der Waerdens Kriterium 2.9 bestimmen können. Mit diesem Kriterium sind wir in der Lage, zyklische Untergruppen der Galoisgruppe G zu bestimmen, indem wir das Polynom f modulo geeigneter Primzahlen p faktorisieren. Zusätzlich können wir die Nullstellen bestimmen, die in einem Zykel permutiert werden. Im folgenden operieren Permutationen und Zykel auf der Menge $\Omega = \{\alpha_1, \ldots, \alpha_n\}$ (vgl. Def 2.10).

Sei nun $\pi \in G$ beliebig fixiert und $\pi = \pi_1 \cdots \pi_u$ die Zerlegung von π in elementfremde Zykel der Längen $|\pi_i| = n_i$ $(1 \leq i \leq u)$.

Definition 4.5. *Eine d-elementige Teilmenge A von Ω heißt möglicher Block der Größe d, falls $A^{\pi^j} \cap A \in \{\emptyset, A\}$ für $1 \leq j \leq |\langle\pi\rangle|$ gilt. Ein System $A_1, \ldots, A_m$ von möglichen Blöcken der Größe d heißt mögliches Blocksystem der Größe d, falls*

(i) $\Omega = \bigcup_{1 \leq i \leq m} A_i$,
(ii) $A_i \cap A_j = \emptyset$ $(i \neq j)$,
(iii) $A_i^{\pi^j} \in \{A_1, \ldots, A_m\}$ $(1 \leq i \leq m, 1 \leq j \leq |\langle\pi\rangle|)$

gilt.

BEMERKUNG 4.6. *Die Definitionen „möglicher Block“ und „mögliches Blocksystem“ sind natürlich abhängig von der Wahl von π. Weiterhin ist jeder Block ein möglicher Block und jedes Blocksystem ein mögliches Blocksystem für jedes π.*

Wir verfolgen nun das Ziel, alle möglichen Blocksysteme zu einer Permutation π zu bestimmen. Dafür werden wir im folgenden weitere Eigenschaften von möglichen Blöcken und Blocksystemen herleiten.

SATZ 4.7. *Es sei A ein möglicher Block zu π und k die kleinste natürliche Zahl mit $A^{\pi^k} = A$. Falls ein Zykel π_l der Länge n_l ein Element von A enthält, dann wird n_l von k geteilt und π_l enthält exakt $\frac{n_l}{k}$ Elemente von A.*

Beweis: Da A ein möglicher Block ist, folgt die Existenz einer natürlichen Zahl k mit

$$A^{\pi^j} \cap A = \emptyset \text{ für } 1 \leq j < k \text{ und } A^{\pi^k} = A.$$

Sei nun α sowohl in A als auch in π_l enthalten. Dann folgt, daß genau die Elemente der Form $\alpha^{\pi^{ck}}$ $(c \in \mathbb{N})$ in A und π_l enthalten sind. Wegen $\alpha^{\pi^{n_l}} = \alpha$ folgt dann, daß n_l von k geteilt wird und π_l exakt $\frac{n_l}{k}$ Elemente von A enthält. □

DEFINITION 4.8. *Wir bezeichnen die Zahl k aus Satz 4.7 als Trägheitsgrad des möglichen Blocks A.*

SATZ 4.9. *Sei $A_1, \ldots, A_m$ ein mögliches Blocksystem zu π mit Trägheitsgraden $k_1, \ldots, k_m$. Falls A_i und A_j ein Element aus demselben Zykel enthalten, so folgt $k_i = k_j$. In diesem Fall enthält A_i ein Element eines Zykels π_l $(1 \leq l \leq u)$ genau dann, wenn A_j ebenfalls ein Element dieses Zykels enthält.*

Beweis: Nach Voraussetzung existiert eine minimale natürliche Zahl c mit $A_i^{\pi^c} \cap A_j \neq \emptyset$. Aufgrund der Definition eines möglichen Blocksystems folgt dann $A_i^{\pi^c} = A_j$. Hieraus folgt die Behauptung. □

DEFINITION 4.10. *Sei $A_1, \ldots, A_m$ ein (mögliches) Blocksystem mit Trägheitsgraden $k_1, \ldots, k_m$. Für $i \in \{1, \ldots, m\}$ bezeichnen wir $A_i, A_i^{\pi}, \ldots, A_i^{\pi^{k_i-1}}$ als (möglichen) Blockverbund mit Trägheitsgrad k_i.*

Aufgrund von Satz 4.9 ist unmittelbar klar, daß alle (möglichen) Blöcke eines (möglichen) Blockverbunds denselben Trägheitsgrad haben.

Die Aussagen der beiden vorangegangenen Sätze sind sehr wichtig für die Konstruktion von möglichen Blocksystemen. Wir werden für $d \in \mathbb{N}$ Systeme von Teilmengen $A_1, \ldots, A_m \subseteq \Omega$ und zugehörige Trägheitsgrade $k_1, \ldots, k_m$ mit den folgenden Eigenschaften konstruieren:

(1) $|A_i| = d$ für $1 \leq i \leq m$.
(2) Enthält A_i Elemente eines Zykels π_l, so enthält A_i exakt $\frac{n_l}{k_i}$ Elemente dieses Zykels.
(3) $\bigcup_{1 \leq i \leq m} A_i = \Omega$.
(4) $A_i \cap A_j = \emptyset$ $(i \neq j)$.
(5) Mit A_i sind auch alle anderen möglichen Blöcke desselben möglichen Blockverbunds in $A_1, \ldots, A_m$ enthalten, d.h. $A_i^{\pi^j} \in \{A_1, \ldots, A_m\}$ $(0 \leq j < k_i)$.

Eine System von Mengen $A_1, \ldots, A_m$ ist genau dann ein mögliches Blocksystem der Größe d, wenn es die obigen Eigenschaften hat. Diese Eigenschaften genügen, um einen effizienten Algorithmus anzugeben, der die möglichen Blocksysteme erzeugt.

Um mögliche erzeugende Polynome g zu bestimmen, benötigen wir noch eine Verfahren, die Nullstellen zu bestimmen, die in einem möglichen Block liegen. Sei hierzu $p \in \mathbb{P}$ mit $p \nmid \operatorname{disc}(f)$ und $\bar{f} \in \mathbb{F}_p[t]$ das f mittels des kanonischen Epimorphismus von $\mathbb{Z} \longrightarrow \mathbb{F}_p$ zugeordnete Polynom. Wir bezeichnen die Nullstellen von $\bar{f}$ in einem geeigneten Erweiterungskörper $\mathbb{F}_q$ mit $\bar{\alpha}_1, \ldots, \bar{\alpha}_n$. Weiterhin sei $\bar{f} = \bar{f}_1 \cdots \bar{f}_u$ eine Faktorisierung in irreduzible Faktoren in $\mathbb{F}_p[t]$. Wir nehmen an, daß $\pi = \pi_1 \cdots \pi_u$ der mit dem van der Waerden Kriterium 2.9 berechnete Erzeuger der zyklischen Untergruppe $\operatorname{Gal}(\bar{f})$ von G ist, wobei die π_i gerade die Nullstellen von $\bar{f}_i$ permutieren.

Sei nun $A_1, \ldots, A_k$ ein möglicher Blockverbund mit Trägheitsgrad k, der o.B.d.A. genau von den Zykeln $\pi_1, \ldots, \pi_v$ permutiert wird, d.h. aus den Nullstellen der Polynome $\bar{f}_1, \ldots, \bar{f}_v$ besteht. Sei nun

$$\bar{f}_i = \bar{f}_{i,1} \cdots \bar{f}_{i,k} \text{ in } \mathbb{F}_{p^k}[t] \text{ und } \pi_i^k = \pi_{i,1} \cdots \pi_{i,k} \ (1 \leq i \leq v).$$

Dann permutiert $\pi_{i,j}$ gerade die Nullstellen von $\bar{f}_{i,j}(1 \leq j \leq k,\ 1 \leq i \leq v)$, daher liegen diese Nullstellen in einem möglichen Block. Da wir wegen (4-1) nur an dem Produkt der Nullstellen der $\bar{f}_{i,j}$ interessiert sind und dieses gleich $(-1)^{\deg(\bar{f}_{i,j})}\bar{f}_{i,j}(0)$ ist, müssen wir f nicht in einem größeren endlichen Körper faktorisieren.

Definition 4.11. *(Polynomdarstellung von Blöcken bzw. Blocksystemen)*

Sei A eine Menge von Polynomen. Wir sagen, daß A ein möglicher Block in Polynomdarstellung ist, falls die Menge der Nullstellen der Polynome von A einen möglichen Block bildet. Wir sagen, daß ein mögliches Blocksystem $A_1, \ldots, A_m$ in Polynomdarstellung gegeben ist, falls alle A_i in Polynomdarstellung gegeben sind. Analog ist ein Blockverbund in Polynomdarstellung gegeben, wenn alle seine Blöcke in Polynomdarstellung gegeben sind.

Die Polynome einer Polynomdarstellung müssen nicht notwendigerweise linear sein. Mit Hilfe der Polynomdarstellung ist es oftmals möglich, Blocksysteme in wesentlich kleineren endlichen Körpern darzustellen.

ALGORITHMUS 4.12. (Berechnung von möglichen Blocksystemen)

Input: *Erzeugendes Polynom f von E, die Blockgröße d und eine Primzahl $p \nmid \operatorname{disc}(f)$.*

Output: *Eine Liste von allen möglichen Blocksystemen der Größe d in Polynomdarstellung.*

Schritt 1: *Berechne die Faktorisierung $f(t) \equiv \bar{f}_1(t) \cdots \bar{f}_u(t) \bmod p\mathbb{Z}[t]$.*

Schritt 2: *Setze $Z := \{\bar{f}_1, \ldots, \bar{f}_u\}$ und rufe BerechneBlockVerbund($Z, d, \emptyset$) auf.*

ALGORITHMUS 4.13. (BerechneBlockVerbund)

Input: *Eine Menge Z bestehend aus r irreduziblen Polynomen $\bar{f}_i$ in $\mathbb{F}_p[t]$, eine Blockgröße $d \in \mathbb{N}$ und eine Menge Y bestehend aus bereits berechneten Blockverbunden in Polynomdarstellung.*

Output: *Eine Liste von möglichen Blocksystemen der Größe d in Polynomdarstellung.*

Schritt 1: *Setze $k := 1$ und $n_i := \deg(\bar{f}_i)$ $(1 \leq i \leq r)$.*

Schritt 2: *Bestimme alle $B \subseteq \{2, \ldots, r\}$ (einschließlich $\emptyset$), für die $dk - n_1 = \sum_{b \in B} n_b$ und $k \mid n_b$ für alle $b \in B$ gilt.*

Schritt 3: *Für jedes dieser B tue folgendes:*
(1) *Setze $Z' := \{\bar{f}_b \mid b \in B \cup \{1\}\}$.*
(2) *Setze $Y := Y \cup \{Z'\}$.*
(3) *Falls $Z = Z'$ gilt, rufe GebeBlockSystemAus(Y', d) auf; ansonsten rufe BerechneBlockVerbund($Z \setminus Z', d, Y$) auf.*
(4) *Setze $Y := Y \setminus \{Z'\}$.*

Schritt 4: *Terminiere, falls $k = n_1$. Ansonsten setze $k := \min\{l \in \mathbb{N} \mid l > k$ und $l \mid n_1\}$ und gehe zu Schritt 2.*

ALGORITHMUS 4.14. (GebeBlockSystemAus)

Input: *Eine Menge Y bestehend aus r Mengen Y_i von Blockverbunden in Polynomdarstellung und eine Blockgröße d.*

Output: *Eine Liste von allen möglichen Blocksystemen in Polynomdarstellung, die zu Y korrespondieren.*

<u>Schritt 1</u>: *Setze* $A := \emptyset$.

<u>Schritt 2</u>: *Für* $i = 1, \ldots, r$ *tue folgendes*

(1) *Setze* $s_i := |Y_i|$. *Bezeichne mit* $f_{i,1}, \ldots, f_{i,s_i}$ *die Elemente von* Y_i.
(2) *Setze* $k_i := \frac{1}{d} \sum_{j=1}^{s_i} \deg(f_{i,j}) \in \mathbb{N}$.
(3) *Faktorisiere* $f_{i,j} = f_{i,j,1} \cdots f_{i,j,k_i}$ *in* $\mathbb{F}_{p^{k_i}}[t]$ $(1 \leq j \leq s_i)$.
(4) *Sei* σ *der Frobeniusautomorphismus von* $\mathbb{F}_{p^{k_i}}/\mathbb{F}_p$. *Sortiere die* $f_{i,j,l}$, *so daß* $f_{i,j,l} = \sigma(f_{i,j,l-1})$ $(1 \leq j \leq s_i, 2 \leq l \leq k_i)$ *gilt.*
(5) *Setze* $A_l := \{f_{i,1,l}, \ldots, f_{i,s_i,l}\}$ $(1 \leq l \leq k_i)$.
(6) *Füge* $A_1, \ldots, A_{k_i}$ *zu* A *hinzu.*

<u>Schritt 3</u>: *Setze* $\pi_{i,j}(f_{i,j,l}) := f_{i,j,l+1}$ $(f_{i,j,k_i+1} := f_{i,j,1})$ *und* $\pi_{i,j}(f_{i',j',l}) := f_{i',j',l}$ *für* $(i,j) \neq (i',j')$ $(1 \leq i \leq r, 1 \leq j \leq s_i, 1 \leq l \leq k_i)$.

<u>Schritt 4</u>: *Setze* $M := \{\prod_{i=1}^{r} \prod_{j=2}^{s_i} \pi_{i,j}^{e_{i,j}} \mid 1 \leq i \leq r,\ 2 \leq j \leq s_i,\ 0 \leq e_{i,j} < k_i\}$.

<u>Schritt 5</u>: *Für jedes* $\tau \in M$ *gebe das mögliche Blocksystem* $A^\tau := \{A_1^\tau, \ldots, A_m^\tau\}$ *aus.*

Der obige Algorithmus gibt alle möglichen Blocksysteme $A_1, \ldots, A_m$ aus. Jedes dieser A_i enthält irreduzible Polynome $f_{i,j,l}$, die über einem Erweiterungskörper von $\mathbb{F}_p$ gegeben sind. Die Nullstellen dieser Polynome bilden den Block. Wie wir bereits oben bemerkt haben, sind wir nur an dem Produkt der Nullstellen interessiert und brauchen deswegen die Nullstellen dieser Polynome nicht explizit auszurechnen. Es ist möglich, daß die Polynome in verschiedenen Blöcken über verschiedenen Erweiterungen von $\mathbb{F}_p$ gegeben sind. Allerdings sind in einem Blockverbund alle Polynome über derselben Erweiterung von $\mathbb{F}_p$ gegeben. Sei nun $A_1, \ldots, A_k$ ein möglicher Blockverbund. Dann gilt (vgl. (4-2)):

$$\prod_{i=1}^{k} (t - \delta_i) \in \mathbb{F}_p[t] \text{ mit } \delta_i = \prod_{\gamma \in A_i} \gamma \ (1 \leq i \leq k).$$

3. Zum Schneiden von Blocksystemen

Bisher haben wir bei der Bestimmung von möglichen Blocksystemen nur ausgenutzt, daß wir ein $\pi \in G$ kennen. Wenn wir kein „geeignetes“ π finden, müssen wir sehr viele mögliche Blocksysteme untersuchen, die keine Blocksysteme sind.

Wir haben in Lemma 4.4 bereits gesehen, daß der Schnitt von zwei Blöcken wieder ein Block ist. Wir werden dies auf zweierlei Art ausnutzen. Erstens werden wir aus bereits berechneten Blocksystemen weitere bestimmen und zweitens werden wir die Anzahl der zu betrachtenden möglichen Blocksysteme deutlich reduzieren, d.h. von vornherein mögliche Blocksysteme ausschließen, die keine Blocksysteme sind.

Definition 4.15. *Unter dem Schnitt von zwei Blocksystemen* $\Delta_1, \ldots, \Delta_m$ *und* $\tilde{\Delta}_1, \ldots, \tilde{\Delta}_{\tilde{m}}$ *verstehen wir die Blöcke, die in der Menge* $\{\Delta_i \cap \tilde{\Delta}_j \mid 1 \leq i \leq m,\ 1 \leq j \leq \tilde{m}\} \setminus \{\emptyset\}$ *enthalten sind.*

Lemma 4.16. *Der Schnitt von zwei Blocksystemen* $\Delta_1, \ldots, \Delta_m$ *und* $\tilde{\Delta}_1, \ldots, \tilde{\Delta}_{\tilde{m}}$ *ist wieder ein Blocksystem der Größe* $c \in \mathbb{N}$. *Der Schnitt von zwei Blöcken* Δ_i *und* $\tilde{\Delta}_j$ *ist entweder leer oder hat* c *Elemente* $(1 \leq i \leq m, 1 \leq j \leq \tilde{m})$.

Beweis: Da ein Block eindeutig zu einem Blocksystem gehört, folgt direkt, daß auch der Schnitt von zwei Blocksystemen wieder ein Blocksystem ist. Alle Blöcke in diesem Blocksystem haben dieselbe Größe. □

Im folgenden seien $\Delta_1, \ldots, \Delta_m$ ein Blocksystem und $A_1, \ldots, A_r$ ein mögliches Blocksystem. Weiterhin sei o.B.d.A. $\alpha \in \Delta_1 \cap A_1$ und $c = |\Delta_1 \cap A_1|$. Wir wollen nun ein Kriterium entwickeln, das entscheidet, ob $A_1, \ldots, A_r$ ein Blocksystem sein kann. Der Beweis folgt direkt aus dem vorigen Lemma.

Lemma 4.17. *Sei* $M = \{\Delta_i \cap A_j \mid 1 \leq i \leq m, 1 \leq j \leq r\}$. *Enthält* M *neben der leeren Menge Elemente verschiedener Größe, d.h. eine nichtleere Menge mit von* c *verschiedener Größe, so ist* $A_1, \ldots, A_r$ *kein Blocksystem.*

Dieses Lemma liefert uns einen guten Pseudo-Test. Wir betrachten nun den Schnitt $\bar{\Delta}_1, \ldots, \bar{\Delta}_{\bar{m}}$ von zwei Blocksystemen $\Delta_1, \ldots, \Delta_m$ und $\tilde{\Delta}_1, \ldots, \tilde{\Delta}_{\tilde{m}}$. Nach Lemma 4.16 wissen wir, daß dieser Schnitt wieder ein Blocksystem ist. Sei nun $A_1, \ldots, A_r$ ein mögliches Blocksystem. Wir wollen nun mit Hilfe dieser 3 Blocksysteme und Lemma 4.17 testen, ob $A_1, \ldots, A_r$ ein Blocksystem sein kann. Dabei stellen wir uns die Frage, ob wir $A_1, \ldots, A_r$ mit allen 3 Blocksystemen schneiden müssen, um maximale Information zu erhalten. Leider gibt es Beispiele, bei denen wir erst nach dem Schnitt von allen 3 Blocksystemen zeigen können, daß $A_1, \ldots, A_r$ kein Blocksystem ist.

Beispiel 4.18. *Zur Vereinfachung betrachten wir hier nur die Indizes der Nullstellen. Seien* $\Omega = \{1, \ldots, 12\}$ *und zwei Blocksysteme* $\{1, 2, 7, 8\}$, $\{3, 4, 9, 10\}$, $\{5, 6, 11, 12\}$ *und* $\{1, 2, 3, 4, 5, 6\}$, $\{7, 8, 9, 10, 11, 12\}$ *gegeben. Der Schnitt dieser Blocksysteme ist* $\{1, 2, \}, \{3, 4\}, \{5, 6\}, \{7, 8\}, \{9, 10\}, \{11, 12\}$. *Wir betrachten das mögliche Blocksystem* $\{1, 2, 3, 10, 11, 12\}, \{4, 5, 6, 7, 8, 9\}$. *Wenn wir den Schnitt mit den ersten beiden Blocksystemen bilden, können wir keinen Widerspruch herleiten.*

Aber wir erhalten $\{1, 2, 3, 10, 11, 12\} \cap \{1, 2\} = \{1, 2\}$ *und* $\{1, 2, 3, 10, 11, 12\} \cap \{3, 4\} = \{3\}$ *und damit einen Widerspruch.*

Dieses Beispiel zeigt, daß es sinnvoll ist, alle Blocksysteme zum Schneiden heranzuziehen. In der Praxis zeigt sich, daß das Schneiden mit den vorhandenen Blocksystemen erheblich preiswerter als jeder andere Pseudo-Test ist, der uns zur Verfügung steht. Bis zu dieser Stelle haben wir das folgende Verfahren entwickelt. Hierbei seien $L_1, \ldots, L_w$ die bekannten Teilkörper und B sei eine Menge von zu testenden möglichen Blocksystemen.

(1) Berechne die Menge S der zu $L_1, \ldots, L_w$ gehörenden Blocksysteme.
(2) Bilde den Schnitt von allen Blocksystemen in S und füge die nicht trivialen zu S hinzu.
(3) Setze $T := \emptyset$ und für jedes mögliche Blocksystem $A_1, \ldots, A_m$ aus B tue folgendes:
    (a) Schneide $A_1, \ldots, A_m$ mit jedem Blocksystem aus S und wende Lemma 4.17 an.
    (b) Falls $A_1, \ldots, A_m$ noch ein Blocksystem sein kann, so füge es zu T hinzu.
(4) Gebe T aus.

Die Blocksysteme, die in den beiden ersten Schritten berechnet werden, sind in der Praxis meistens schon bekannt und müssen nicht neu berechnet werden. Wir geben im folgenden eine Methode an, mit der wir für einen Teilkörper und eine gewählte Identifizierung von Nullstellen das zugehörige Blocksystem erhalten. Das folgende Lemma ist z.B. dann sinnvoll, wenn wir die Primzahl wechseln wollen oder wenn bereits vorher Teilkörper samt Einbettung ω bekannt waren. Der Beweis folgt direkt.

LEMMA 4.19. *Seien* $\alpha_1, \ldots, \alpha_n$ *die Nullstellen von* f *und* $\beta_1, \ldots \beta_m$ *die Nullstellen von* g *über derselben Vervollständigung identifiziert. Falls die* β_i *paarweise verschieden sind, so bildet* $\Delta_1, \ldots, \Delta_m$ *mit*

$$\Delta_i := \{\alpha_j \mid \omega(\alpha_j) = \beta_i,\ 1 \leq j \leq n\} \ \ (1 \leq i \leq m)$$

das zugehörige Blocksystem.

Wir verfolgen nun die Idee, daß wir bereits durch einen Schnitt ganze „Klassen“ von möglichen Blocksystemen ausschließen können. Dies können wir dadurch erreichen, daß unsere möglichen Blocksysteme keine zufällige Reihenfolge haben. Hierzu untersuchen wir noch einmal Algorithmus 4.14. Dort werden mögliche

Blocksysteme konstruiert, die alle aus r Blockverbunden bestehen. Die Trägheitsgrade dieser Blockverbunde sind mit $k_1, \ldots, k_r$ bezeichnet. Eine weitere wichtige Größe für jeden Blockverbund sind die Zahlen $s_1, \ldots, s_r$, die die Anzahlen der modulo p-Faktoren von f bezeichnen, aus deren Nullstellen der Blockverbund konstruiert wird. Das Ziel dieser Funktion ist es, für $1 \leq i \leq r$ alle möglichen Blockverbunde mit den Nullstellen von diesen s_i Faktoren und Trägheitsgrad k_i zu konstruieren. Enthalte nun V_i die Menge der konstruierten Blockverbunde $(1 \leq i \leq r)$, dann werden im letzten Schritt alle möglichen Blocksysteme auf die folgende Art konstruiert:

$$\{v_1, \ldots, v_r \mid v_i \in V_i,\ 1 \leq i \leq r\}.$$

Dabei ist v_i eine kürzere Schreibweise für einen Blockverbund $A_{i,1}, \ldots, A_{i,k_i}$ $(1 \leq i \leq r)$. Die Mächtigkeit der Mengen V_i ist nur von k_i und s_i abhängig. Wir erhalten:

$$|V_i| = k_i^{s_i - 1}.$$

Der Algorithmus erzeugt also $|V_1| \cdots |V_r|$ verschiedene mögliche Blocksysteme. Nehmen wir nun an, daß wir zeigen können, daß ein möglicher Blockverbund $v_1 \in V_1$ in keinem Blocksystem enthalten sein kann, so haben wir die Anzahl der möglichen Blocksysteme auf diese Weise um $|V_2| \cdots |V_r|$ reduziert. Weiterhin brauchen wir nur solche Blockverbunde miteinander zu kombinieren, die dasselbe Schnittverhalten bezüglich aller bekannter Blocksysteme haben. Dabei verstehen wir unter dem Schnittverhalten die Zahl c aus Lemma 4.17. Falls dieses Lemma liefert, daß das mögliche Blocksystem kein Blocksystem ist, so definieren wir das Schnittverhalten als 0. Wir definieren das Schnittverhalten analog für Blockverbunde. Unter dem Schnittverhalten eines möglichen Blockverbunds mit $\tilde{w}$ Blocksystemen verstehen wir einen Vektor $(c_1, \ldots, c_{\tilde{w}})^t$, wobei c_i das Schnittverhalten mit dem i-ten Blocksystem ist $(1 \leq i \leq \tilde{w})$. Wir können nun den folgenden Algorithmus formulieren.

Algorithmus 4.20. (Pseudo-Test durch Schneiden von Blocksystemen)

<u>Input</u>: *$V_i = \{v_{i,1}, \ldots, v_{i,|V_i|}\}$ $(1 \leq i \leq r)$, $k_1, \ldots, k_r$, $s_1, \ldots, s_r$ wie im vorangegangenen Text definiert. $\tilde{w}$ verschiedene Blocksysteme.*

<u>Output</u>: *Menge von möglichen Blocksystemen, deren Schnitt mit allen bekannten Blocksystemen keinen Widerspruch liefert.*

<u>Schritt 1</u>: *Für $i = 1, \ldots, r$ tue folgendes:*
- (1) *Für $j = 1, \ldots, |V_i|$ tue folgendes:*
  - (a) *Setze $W_{i,j}$ auf das Schnittverhalten von $v_{i,j}$ mit den bekannten Blocksystemen.*

(b) *Falls eine Komponente von* $W_{i,j}$ 0 *ist, so setze* $V_i := V_i \setminus \{v_{i,j}\}$.

<u>Schritt 2</u>: *Berechne alle möglichen Blocksysteme* $v_{1,j_1}, \ldots, v_{r,j_r}$ *mit* $W_{1,j_1} = \cdots = W_{r,j_r}$ *und* $v_{i,j_i} \in V_i$ $(1 \leq i \leq r)$ *und gebe sie aus.*

<u>Schritt 3</u>: *Terminiere den Algorithmus.*

4. Zur Berechnung von erzeugenden Polynomen

Wir werden nun eine Methode herleiten, wie wir aus den bestimmten möglichen Blocksystemen erzeugende Polynome für Teilkörper berechnen können. Weiter werden wir Pseudo–Tests angeben, mit deren Hilfe wir feststellen können, ob ein mögliches Blocksystem kein Blocksystem ist. Diese Tests sind sehr schnell und decken nahezu alle möglichen Fälle ab. Trotzdem kann es passieren, daß wir ein mögliches (falsches) Blocksystem in diesem Stadium nicht als solches erkennen. Solche Kandidaten werden dann vom Einbettungsalgorithmus erkannt, der neben der Einbettung auch einen Beweis liefert, daß die berechneten Teilkörper auch tatsächlich Teilkörper sind.

Sei nun $\Delta_1, \ldots, \Delta_m$ ein Blocksystem, wobei die Nullstellen aus Δ_i im Zerfällungskörper N von E liegen. Weiterhin seien $\mathfrak{P}$ ein beliebiges Primideal von $\mathfrak{o}_N$, welches über p liegt und $\mathcal{E} = N_{\mathfrak{P}}$ die p-adische Vervollständigung. Wir bezeichnen mit ϕ die kanonische Abbildung von N nach $\mathcal{E}$.

Seien nun $\tilde{f} = \phi(f)$ und $\{\tilde{\alpha}_1, \ldots, \tilde{\alpha}_n\}$ die Nullstellen in $\mathcal{E}$, wobei $\phi(\alpha_i) = \tilde{\alpha}_i$ gilt. Mit $\tilde{\Delta}_i = \phi(\Delta_i)$ $(1 \leq i \leq m)$ definieren wir:

$$\tilde{g}(t) := \prod_{i=1}^{k}(t - \tilde{\delta}_i) \in \mathbb{Z}_p[t] \text{ mit } \tilde{\delta}_i := \prod_{\tilde{\gamma} \in \tilde{\Delta}_i} \tilde{\gamma} \; (1 \leq i \leq k). \tag{4-3}$$

$$g(t) := \prod_{i=1}^{k}(t - \delta_i) \in \mathbb{Z}[t] \text{ mit } \delta_i := \prod_{\gamma \in \Delta_i} \gamma \; (1 \leq i \leq k). \tag{4-4}$$

Damit erhalten wir:

Satz 4.21. *Seien* $\Delta_1, \ldots, \Delta_m$ *ein Blocksystem und* g *und* $\tilde{g}$ *wie in* (4-3) *und* (4-4). *Dann gilt* $\phi(g) = \tilde{g}$.

Auch falls $\Delta_1, \ldots, \Delta_m$ nur ein mögliches Blocksystem ist, erhalten wir ein Polynom $\tilde{g} \in \mathbb{Z}_p[t]$. Wir merken an, daß wir nicht in der Lage sind, die Abbildung ϕ konstruktiv zu bestimmen. Wir wissen, daß zu jeder Erweiterung $\mathbb{F}_q/\mathbb{F}_p$ genau eine unverzweigte p-adische Erweiterung $\mathcal{E}/\mathbb{Q}_p$ existiert, deren Restklassenkörper gerade $\mathbb{F}_q$ ist. Im vorigen Abschnitt haben wir einen Algorithmus entwickelt, der mögliche Blocksysteme $A_1, \ldots, A_m$ berechnet. Hierbei wurden die Nullstellen bzw. die δ_i in einem passenden endlichen Körper identifiziert. Es ist nun möglich, diese Nullstellen auch im zugehörigen p-adischen Körper $\mathcal{E}$ zu identifizieren. Dazu haben wir in Kapitel III Methoden entwickelt, diese Nullstellen modulo $\mathfrak{p}^k$ zu berechnen.

Der Beweis des folgenden Lemmas folgt direkt aus den bisherigen Überlegungen.

Lemma 4.22. *Seien $g, \tilde{g}$ und $\tilde{\delta}_i \in \mathcal{E}$ $(1 \le i \le m)$ wie in* (4-3) *und* (4-4) *gegeben. Seien weiterhin $k \in \mathbb{N}$ und $\mathfrak{p}$ das maximale Ideal von $\mathcal{E}$. Zusätzlich gelte $\bar{\delta}_i \equiv \tilde{\delta} \bmod \mathfrak{p}^k$ $(1 \le i \le m)$ und $\bar{g}(t) = \prod_{i=1}^{m}(t - \bar{\delta}_i)$. Dann folgt $\bar{g} \equiv \tilde{g} \bmod p^k$ und damit $\bar{g} \equiv g \bmod p^k$.*

Wenn wir also eine Schranke M für die Koeffizienten von g kennen und $p^k > 2M$ gilt, so folgt $\bar{g} = g$, wenn wir für die Koeffizienten von $\bar{g}$ das symmetrische Restsystem $\{\frac{-(p^k-1)}{2}, \ldots, \frac{p^k-1}{2}\}$ wählen. Das folgende Lemma liefert uns eine solche Schranke M. Es ist eine direkte Folgerung von [5, Lemma 3.5.2].

Lemma 4.23. *Sei $g(t) = \sum_{i=0}^{m} b_i t^i$ und g gemäß* (4-3) *gegeben. Wir erhalten:*

$$|b_i| \le \binom{m-1}{i-1} B + \binom{m-1}{i} \quad (1 \le i < m) \text{ mit } B = \prod_{j=1}^{n} \max(1, |\alpha_j|).$$

Aufgrund der Konstruktion von g gilt $b_m = 1$ und $b_0 = \pm f(0)$. Unter der Voraussetzung, daß wir B bestimmen können, liefert uns dieses Lemma eine sehr einfache Möglichkeit, eine Schranke für die Koeffizienten von g zu bestimmen. Zur Bestimmung einer oberen Schranke von B können wir einerseits die Nullstellen von f in $\mathbb{C}$ ausrechnen und das Produkt der Beträge der Nullstellen bilden, die größer als 1 sind. Natürlich ist es möglich, diese Abschätzung noch zu verbessern, wenn einzelne Nullstellen von f einen Betrag kleiner als 1 haben. Das ist aber für uns von nicht zu großer Bedeutung. Wir werden eine Abschätzung von Mignotte [26, Theorem 1] benutzen, mit deren Hilfe wir eine obere Abschätzung für B ohne die Berechnung der Nullstellen in $\mathbb{C}$ erhalten.

Lemma 4.24. *Sei $f(t) = \sum_{i=0}^{n} a_i t^i \in \mathbb{C}[t]$ mit Nullstellen $\alpha_1, \ldots, \alpha_n \in \mathbb{C}$. Dann gilt:*

$$\prod_{i=1}^{n} \max(1, |\alpha_i|) \le \sqrt{\sum_{i=0}^{n} |a_i|^2}.$$

An dieser Stelle müssen wir noch die Frage beantworten, was passiert, wenn unser konstruiertes charakteristisches Polynom g nicht irreduzibel ist, d.h. doppelte Nullstellen besitzt. Wir hatten schon erwähnt, daß wir in diesem Fall eine lineare Transformation $f(t) \leftarrow f(t+a)$ durchführen werden. Das folgende Lemma zeigt, daß maximal n solcher Substitutionen wieder zu doppelten Nullstellen führen können.

LEMMA 4.25. *Falls die δ_i $(1 \leq i \leq m)$ in (4-4) nicht paarweise verschieden sind, so gibt es höchstens n verschiedene lineare Substitutionen von f, die wiederum nicht paarweise verschiedene Nullstellen liefern.*

Beweis: Für $1 \leq i \leq m$ definieren wir

$$\Phi_i(x) := \prod_{\gamma \in \Delta_i} (x + \gamma).$$

Diese Polynome sind alle verschieden, da sie verschiedene Nullstellen haben. Weiterhin haben alle Polynome Grad d, so daß jeweils höchstens d Funktionswerte übereinstimmen können. Falls die δ_i nicht paarweise verschieden sind, so ist jede Nullstelle doppelte Nullstelle, da g ein charakteristisches Polynom ist. Daher gibt es höchstens $d(m-1) = n - d$ Werte k, so daß $\Phi_1(k) = \Phi_i(k)$ für $2 \leq i \leq m$ gilt. Jedes andere k hat die Eigenschaft, daß die hiernach berechneten δ_i paarweise verschieden sind. $\square$

Lemma 4.25 bleibt auch dann gültig, wenn wir die Nullstellen über einem endlichen Körper identifizieren. Allerdings brauchen wir hier die zusätzliche Voraussetzung, daß der endliche Körper genügend Elemente enthält, da sonst zwei Polynome vom Grad n verschieden sein können, obwohl sie an $n+1$ Funktionswerten übereinstimmen. Der Beweis des folgenden Lemmas folgt direkt.

LEMMA 4.26. *Sei $p > n$ und gelte $p \nmid \mathrm{disc}(f)$. Dann gibt es höchstens n lineare Substitutionen für f, so daß $p \mid \mathrm{disc}(g)$ gilt.*

Für unseren Einbettungsalgorithmus wird es wichtig sein, daß p nicht die Diskriminante von unserem berechneten Teilkörperpolynom g teilt. Dieses Lemma ist der Grund dafür, daß wir mit der Auswahl unserer Primzahlen p erst bei n starten sollten.

Wir sind nun in der Lage, einen Algorithmus zur Berechnung eines erzeugenden Polynoms anzugeben. Die Erzeugung der p-adischen Körper und die Berechnung der Faktorisierung von f über p-adischen Erweiterungen haben wir ausführlich in Kapitel III erläutert.

ALGORITHMUS 4.27. (Berechnung eines erzeugenden Polynoms)

<u>Input</u>: *Ein erzeugendes Polynom f eines Zahlkörpers E. Eine Primzahl $p > n$ und ein mögliches Blocksystem $\Delta_1, \dots, \Delta_m$ in Polynomdarstellung.*

<u>Output</u>: *Ein erzeugendes Polynom g eines möglichen Teilkörpers L, oder die Meldung, daß $\Delta_1, \dots, \Delta_m$ kein Blocksystem ist.*

<u>Schritt 1</u>: *Bestimme die Trägheitsgrade k_i $(1 \le i \le m)$ der Blöcke $\Delta_1, \dots, \Delta_m$.*

<u>Schritt 2</u>: *Setze $l := \mathrm{kgV}(k_1, \dots, k_m)$.*

<u>Schritt 3</u>: *Bestimme mit Lemma 4.23 eine geeignete Schranke M für die Koeffizienten von g.*

<u>Schritt 4</u>: *Bestimme die Faktorisierung von $f \equiv f_1 \cdots f_r \bmod \mathfrak{p}^k$ über einer p-adischen Erweiterung vom Grad l von $\mathbb{Q}_p$, wobei $p^k > 2M$ ist.*

<u>Schritt 5</u>: *Setze $\tilde{\Delta}_j := \{f_i \mid 1 \le i \le r$, es existiert ein $\bar{f} \in \Delta_j$ mit $(f_i \bmod \mathfrak{p}) \mid \bar{f}\}$ $(1 \le j \le m)$.*

<u>Schritt 6</u>: *Für $i = 1, \dots, m$ berechne das Produkt δ_i der Nullstellen, die im Block Δ_i liegen.*

<u>Schritt 7</u>: *Berechne $\sum_{i=1}^m \delta_i$ (modulo p^k). Falls diese Summe betraglich größer als M ist, gehe zu Schritt 12.*

<u>Schritt 8</u>: *Berechne das Polynom $g(t) := \prod_{i=1}^m (t - \delta_i)$ (modulo p^k).*

<u>Schritt 9</u>: *Falls einer der Koeffizienten von g betraglich größer als M ist, gehe zu Schritt 12.*

<u>Schritt 10</u>: *Falls g modulo p doppelte Faktoren hat, setze $f(t) := f(t+1)$ und gehe zu Schritt 3.*

<u>Schritt 11</u>: *Berechne $\tilde{f}(t) := f(t+1)$, $\tilde{\delta}_i := \prod_{\gamma \in \Delta_i} (\gamma - 1)$, $\tilde{g}(t) := \prod_{i=1}^m (t - \tilde{\delta}_i)$ und eine Schranke $\tilde{M}$ für die Koeffizienten von $\tilde{g}$. Teste nun, ob die Koeffizienten von $\tilde{g}$ betraglich kleiner als $\tilde{M}$ sind. In diesem Fall gebe das mögliche erzeugende Polynom g aus und terminiere.*

<u>Schritt 12</u>: *Gebe aus, daß $\Delta_1, \dots, \Delta_m$ kein Blocksystem ist und terminiere.*

Die Korrektheit des obigen Algorithmus folgt aus den vorherigen Überlegungen. Mehrere zu berechnende Größen des obigen Algorithmus sind bereits vorher bestimmt worden und brauchen daher nicht neu berechnet zu werden. So werden die Trägheitsgrade k_i bereits bei der Berechnung der Δ_i mitbestimmt. Die Schranke M in Schritt 3 hängt nur von f und dem Grad des Teilkörpers ab und kann daher auch abgespeichert werden.

Der zeitkritische Teil des Verfahrens ist die Faktorisierung von f über der unverzweigten p-adischen Erweiterung vom Grad l. Diese wird für jeden Grad l nur einmal bestimmt und kann danach abgespeichert werden. Sehr wichtig in diesem Verfahren ist die Wahl von k. Da wir für unser Verfahren das quadratische Hensel-Lifting verwenden, bietet es sich an, k als $2^{\tilde{k}}$ zu wählen. Dabei sollte k auf jeden Fall so gewählt werden, daß $p^k > 2M$ gilt. Praktische Erfahrungen haben gezeigt, daß es wesentlich günstiger ist, k so zu wählen, daß $p^k \approx M^4$ gilt. In diesem Fall haben wir eine wesentliche größere Chance, daß wir in Schritt 7 bzw. 9 feststellen, daß $\Delta_1, \ldots, \Delta_m$ kein Blocksystem ist. Dieser Pseudo-Test ist im Gegensatz zur Berechnung einer Einbettung sehr preiswert. Die Summe in Schritt 7 entspricht der Spur von δ_i. Sie ist wesentlich einfacher als das Polynom zu berechnen und zeigt in vielen Fällen schon an, daß $\Delta_1, \ldots, \Delta_m$ kein Blocksystem ist. In Schritt 11 haben wir einen zweiten Pseudo-Test angegeben, der ebenfalls sehr einfach durchzuführen ist. In unseren praktischen Berechnungen haben wir mehrere Beispiele gefunden, die den ersten Pseudo-Test passieren, aber dennoch zu keinem Blocksystem korrespondieren. Bisher sind keine „falschen“ möglichen Blocksysteme bekannt, die auch noch den zweiten Pseudotest passieren. Diese Pseudotests sind nur dafür da, die Berechnungen zu beschleunigen. Sie haben nichts mit dem Beweis des Verfahrens zu tun.

5. Zur Einbettung von berechneten Teilkörpern

In diesem Abschnitt stellen wir ein Verfahren vor, mit dem wir unsere berechneten Teilkörper in den gegebenen Körper E einbetten können. Hierzu werden wir das zugehörige mögliche Blocksystem $\Delta_1, \ldots, \Delta_m$ benutzen. Die Einbettung ist einerseits wichtig für Anwendungen, die mit Teilkörpern arbeiten, andererseits benötigen wir sie, um zu beweisen, daß unser berechnetes Polynom g tatsächlich einen Teilkörper erzeugt. Unser Ziel ist es, ein Polynom $\omega \in \mathbb{Q}[t]$ vom Grad kleiner n zu bestimmen, so daß $\omega(\alpha) = \beta$ gilt. Wir haben schon an anderer Stelle angemerkt, daß die Koeffizienten von ω nicht notwendigerweise in $\mathbb{Z}$ liegen, da die Gleichungsordnung im allgemeinen keine Maximalordnung ist.

O.B.d.A. gehen wir nun davon aus, daß wir das Polynom g ohne Substitution berechnet haben. Dann gilt für die Nullstellen $\beta_1, \ldots, \beta_m$ von g der folgende Zusammenhang:

$$\beta_j = \prod_{\gamma \in \Delta_j} \gamma \ (1 \leq j \leq m).$$

Damit hat unser gesuchtes Polynom ω die folgende Eigenschaft:

$$\omega(\alpha_i) = \beta_j \text{ für } \alpha_i \in \Delta_j.$$

Wir kennen somit n Funktionswerte von einem Polynom vom Grad kleiner als n, welches dadurch eindeutig bestimmt ist. Da wir das Blocksystem nur in den zugehörigen p-adischen Körpern identifizieren können, werden wir ω in einem ersten Schritt modulo p ausrechnen. Seien im folgenden $\bar{f} \equiv f \bmod p$ und $\{\bar{\alpha}_1, \dots, \bar{\alpha}_n\}$ die Nullstellen von $\bar{f}$ in $\mathbb{F}_{\tilde{q}}$. Hierzu können wir ein Gleichungssystem lösen oder die Formel von Lagrange verwenden. Für beide Verfahren müssen wir zuerst die Nullstellen α_i in einem geeigneten endlichen Körper $\mathbb{F}_{\tilde{q}}/\mathbb{F}_p$ bestimmen. Falls der Grad von $\mathbb{F}_{\tilde{q}}/\mathbb{F}_p$ sehr groß ist, kann die Berechnung der Nullstellen sehr aufwendig werden, da wir in den bisherigen Schritten das Polynom $\bar{f}$ nicht notwendigerweise vollständig faktorisiert haben. So wurden Faktorisierungen lediglich in einer Erweiterung $\mathbb{F}_q/\mathbb{F}_p$ vom Grad $l = \mathrm{kgV}(k_i)$ durchgeführt. Wir werden nun ein Verfahren angeben, welches nur die Faktorisierung von $\bar{f}$ in $\mathbb{F}_q$ benötigt. Wie in den vorherigen Abschnitten sei $\Delta_1, \dots, \Delta_m$ in Polynomdarstellung gegeben. Dies bedeutet, daß alle Nullstellen eines Polynoms in demselben Block liegen. Wir können daher die folgenden Blockpolynome in $\mathbb{F}_q[t]$ berechnen:

$$a_j(t) := \prod_{\bar{\alpha} \in \Delta_j} (t - \bar{\alpha}) \in \mathbb{F}_q[t] \text{ und } b_j(t) := \prod_{\substack{1 \le i \le m \\ i \neq j}} a_i(t) \in \mathbb{F}_q[t] \ (1 \le j \le m).$$

Wir bezeichnen mit $\bar{\beta}_j \in \mathbb{F}_q$ die Nullstellen von $\bar{g} \equiv g \bmod p$. Nun können wir mit Hilfe des erweiterten Euklidischen Algorithmus für Polynome über endlichen Körpern $c_j,\ d_j \in \mathbb{F}_q[t]$ mit

$$a_j c_j + b_j d_j = 1 \ (1 \le j \le m)$$

bestimmen. Mit Hilfe dieser Polynome sind wir nun in der Lage, eine modulo p-Approximation unseres Einbettungspolynoms anzugeben. Wir definieren:

$$\omega_0(t) := \sum_{j=1}^{m} b_j(t) d_j(t) \bar{\beta}_j. \tag{4-5}$$

Für $\bar{\alpha}_i \in \Delta_j$ und jedes $\tilde{j} \neq j$ gilt: $b_{\tilde{j}}(\bar{\alpha}_i) d_{\tilde{j}}(\bar{\alpha}_i) \bar{\beta}_j = 0$. Somit erhalten wir: $\omega_0(\bar{\alpha}_i) = b_j(\bar{\alpha}_i) d_j(\bar{\alpha}_i) \bar{\beta}_j = (1 - a_j(\bar{\alpha}_i) c_j(\bar{\alpha}_i)) \bar{\beta}_j = \bar{\beta}_j$, wegen $a_j(\bar{\alpha}_i) = 0$. Wir sind nun in der Lage, einen Algorithmus zur Einbettung des gefundenen Teilkörpers anzugeben. Vorher geben wir in dem folgenden Lemma eine obere Schranke für die Koeffizienten von ω an.

LEMMA 4.28. *Die Zähler der Koeffizienten von ω sind stets kleiner als M mit*

$$M := |\beta|_\infty n(n-1)^{(n-1)/2} |\alpha|_\infty^{n(n-1)/2}.$$

Beweis: Der Beweis folgt direkt mit Lemma 2.17 und der Abschätzung $\sqrt{|\operatorname{disc}(f)|}$ für den größten Nenner. $\square$

ALGORITHMUS 4.29. (Berechnung der Einbettung eines Teilkörpers)

Input: *Erzeugendes Polynom f eines Körpers E. Polynom g eines Teilkörpers L aus Algorithmus* 4.27. *Zugehöriges Blocksystem $\Delta_1, \ldots, \Delta_m$ in Polynomdarstellung und $p \in \mathbb{P}$ mit $p \nmid \operatorname{disc}(f)\operatorname{disc}(g)$.*

Output: *Einbettungspolynom $\omega \in \mathbb{Q}[t]$, falls L Teilkörper von E ist, „falsch“ sonst.*

Schritt 1: *Bestimme ω_0 mit Formel* (4-5).

Schritt 2: *Setze $\beta_0 \equiv h_0(\alpha) \bmod p$.*

Schritt 3: *Bestimme M mit Lemma* 4.28 *und ein $k \in \mathbb{N}$ derart, daß $p^{2^k} > 2M$ gilt.*

Schritt 4: *Bestimme mit Hilfe des Newton-Liftings* 3.15 *ein Element β mit $g(\beta) = 0$. Falls β nicht berechenbar war, so folgt, daß $\Delta_1, \ldots, \Delta_m$ kein Blocksystem ist.*

Schritt 5: *Berechne $\omega \in \mathbb{Q}[t]$ mit $\omega(\alpha) = \beta$ und gib ω aus.*

6. Zusammenhänge zwischen Blöcken und Primidealen

In diesem Abschnitt werden wir einen Zusammenhang zwischen Blöcken und Primidealen herleiten. Dieser Zusammenhang wird zwar im Teilkörperalgorithmus nicht ausgenutzt, er wird aber nützlich werden, wenn wir spezielle Teilkörper berechnen wollen. Wir werden dies beim Berechnen von Automorphismen in normalen Zahlkörpern ausnutzen.

Seien ein Blocksystem $\Delta_1, \ldots, \Delta_m$ von $G = \operatorname{Gal}(f)$ und eine Primzahl $p \nmid \operatorname{disc}(f)$ gegeben. Wie bisher sei $\pi = \pi_1 \cdots \pi_u$ der zu p korrespondierende Zykel. Das Blocksystem ist unabhängig von der Wahl von π, während die Blockverbunde des Blocksystems von der Wahl von p abhängig sind. Wir erinnern uns, daß in einem Blockverbund alle Blöcke denselben Trägheitsgrad haben. Im nächsten Satz wird die Bezeichnung Trägheitsgrad klar werden.

SATZ 4.30. *Es gilt $p\mathfrak{o}_L = \mathfrak{p}_1 \cdots \mathfrak{p}_r$, wobei r die Anzahl der Blockverbunde ist. Die Trägheitsgrade der $\mathfrak{p}_i$ $(1 \leq i \leq r)$ entsprechen den Trägheitsgraden der Blockverbunde.*

Beweis: Sei $\tilde{g} = \prod_{i=1}^{m}(t - \tilde{\delta}_i))$ mit $\tilde{\delta}_i = \prod_{\gamma \in \tilde{\Delta}_i} \gamma$ wie in (4-3). Die Anzahl und die Grade der Faktoren von $\tilde{g}$ in $\mathbb{Z}_p[t]$ entsprechen gerade der Anzahl und den Trägheitsgraden der Primideale von $\mathfrak{o}_L$ über p. Sei nun (durch Umsortierung) $\tilde{\Delta}_1, \ldots, \tilde{\Delta}_s$ ein beliebiger Blockverbund des Blocksystems vom Trägheitsgrad k. Wir müssen zeigen, daß $\tilde{g}_1 = \prod_{i=1}^{s}(t - \tilde{\delta}_i) \in \mathbb{Z}_p[t]$ irreduzibel ist. Nach Voraussetzung wissen wir, daß die $\tilde{\delta}_i$ paarweise verschieden sind. Sei nun σ der Frobeniusautomorphismus einer unverzweigten Erweiterung vom Grad k von $\mathbb{Q}_p$. Dann erhalten wir nach entsprechender Umsortierung der Nullstellen, daß $\tilde{\delta}_i = \sigma^{i-1}(\tilde{\delta}_1)$ für $1 \leq i \leq s$ gilt. Dies beweist, daß $\tilde{g}_1 \in \mathbb{Z}_p[t]$ irreduzibel ist und damit das korrespondierende Primideal Trägheitsgrad k hat. $\square$

KAPITEL V

Dekompositionen

In diesem Kapitel führen wir die Normdekomposition von einem irreduziblen und normierten Polynom $f \in \mathbb{Q}[t]$ ein. Diese ermöglicht es uns, die Nullstellen durch sukzessives Lösen von Gleichungen kleineren Grades zu erhalten. Die Normdekomposition wird die funktionale [19] und homogene bivariate Dekomposition [33] verallgemeinern. Wir werden zeigen, daß zu imprimitiven Polynomen f stets Normdekompositionen existieren, während dies für funktionale bzw. homogene bivariate Dekompositionen nicht der Fall ist.

1. Grundlagen

In diesem Kapitel sei $f \in \mathbb{Q}[t]$ ein normiertes und irreduzibles Polynom und $E = \mathbb{Q}(\alpha)$, wobei α eine Nullstelle von f ist.

Definition 5.1. *Sei $g \in \mathbb{Q}[t]$ ein normiertes und irreduzibles Polynom mit Nullstellen $\beta_1, \ldots, \beta_m \in \mathbb{C}$ und $L = \mathbb{Q}(\beta_1)$. Wir definieren*

$$(\cdot)^{(i)} : L \to \mathbb{Q}(\beta_i) : \sum_{j=0}^{m-1} b_j \beta_1^j \mapsto \sum_{j=0}^{m-1} b_j \beta_i^j \ (b_j \in \mathbb{Q}).$$

Wir erweitern diese Definition auf den Polynomring mittels

$$(\cdot)^{(i)} : L[t] \to \mathbb{Q}(\beta_i)[t] : h(t) = \sum_{j=0}^{k} c_j t^j \mapsto h^{(i)}(t) = \sum_{j=0}^{k} c_j^{(i)} t^j \ (c_j^{(i)} \in \mathbb{Q}(\beta_i)).$$

Für $h \in L[t]$ definieren wir die Polynomnorm wie folgt:

$$N_g(h) := N_L(h) := \prod_{i=1}^{m} h^{(i)} \in \mathbb{Q}[t].$$

Die Konjugierten einer Zahl aus L sind natürlich nur von L und nicht von g abhängig.

Definition 5.2. *Dekompositionen*

(i) *Wir nennen* $f = g(h)$ *mit* $g, h \in \mathbb{Q}[t]$ *und* $1 < \deg(g) < \deg(f)$ *eine funktionale Dekomposition.*
(ii) *Wir nennen* $f = \hat{g}(h_1, h_2)$ *mit homogenen* $\hat{g} \in \mathbb{Q}[t, u]$ *und* $h_1, h_2 \in \mathbb{Q}[t]$, *wobei* $1 < \deg(\hat{g}) = m < \deg(f)$ *und* $\deg(h_i) \leq \frac{n}{m}$ $(i = 1, 2)$ *gilt, eine homogene bivariate Dekomposition.*
(iii) *Wir nennen* $f = N_g(h)$ *eine Normdekomposition, falls* $g \in \mathbb{Q}[t]$ *irreduzibel mit* $1 < \deg(g) < \deg(f)$ *ist und* $h \in L[t]$ *gilt, wobei* L *der von einer Nullstelle von* g *erzeugte Zahlkörper ist.*

Für $h_2 = 1$ kann die funktionale Dekomposition als Spezialfall der homogenen bivariaten Dekomposition angesehen werden.

Satz 5.3. *Falls* f *eine funktionale oder eine homogene bivariate Dekomposition besitzt, so hat* f *auch eine Normdekomposition.*

Beweis: Sei $f = g(h)$ mit $g, h \in \mathbb{Q}[t]$ und β eine Nullstelle von g. Dann gilt

$$f = g(h) = \prod_{i=1}^{m} (h - \beta^{(i)}) = N_g(h - \beta).$$

Aus $g = g_1 g_2$ folgt $f = g_1(h) g_2(h)$, welches wegen der Irreduziblität von f zu einem Widerspruch führt.

Sei nun $f = \hat{g}(h_1, h_2)$ eine homogene bivariate Dekomposition. f und h_2 haben keine gemeinsame Nullstelle, da $\deg(h_2) < \deg(f)$ gilt. Mit $g(t) = \hat{g}(t, 1)$ erhalten wir:

$$f = h_2^m \cdot g\left(\frac{h_1}{h_2}\right) \text{ und damit } g\left(\frac{h_1(\alpha)}{h_2(\alpha)}\right) = 0.$$

Somit existiert eine Nullstelle $\beta = \frac{h_1(\alpha)}{h_2(\alpha)}$ von g mit $h_1(\alpha) - \beta h_2(\alpha) = 0$. Sei nun $\tilde{g}$ das Minimalpolynom von β (ein Teiler von g) und $\tilde{h} = h_1 - \beta h_2$. Damit erhalten wir $f = N_{\tilde{g}}(\tilde{h})$. Aus Gradgründen folgt nun $\tilde{g} = g$ und damit die Irreduziblität von g. □

Im folgenden Beispiel werden wir sehen, daß die Normdekomposition eine echte Verallgemeinerung der funktionalen und der homogenen bivariaten Dekomposition ist. Wir werden außerdem im weiteren Verlauf sehen, daß Normdekompositionen von Polynomen vom Grad 4 stets zu homogenen bivariaten Dekompositionen korrespondieren.

BEISPIEL 5.4. *Sei* $f(t) = t^6 - 12t^5 + 54t^4 - 134t^3 + 153t^2 - 162t + 81$. *Wir erhalten die Normdekomposition* $f = N_g(h)$, *wobei* $g(t) = t^3 - 18t^2 + 81t - 81$, $h(t) = t^2 + \frac{36-30\beta+2\beta^2}{9}t + \beta$ *und* β *eine Nullstelle von* g *ist. Mit Hilfe der Lemmata* 5.12 *und* 5.13 *sehen wir, daß weder eine homogene bivariate noch eine funktionale Dekomposition von* f *existiert.*

Ein wesentliches Ziel der Dekompositionen ist das Bestimmen von Nullstellen. Hierbei sollen diese durch sukzessives Lösen von Gleichungen kleineren Grades bestimmt werden. Dieses Ziel kann mit allen drei Typen von Dekompositionen erreicht werden.

KOROLLAR 5.5. *Seien* $f = g(h)$ *mit* $g, h \in \mathbb{Q}[t]$ *eine funktionale Dekomposition und seien* $\beta_1, \ldots, \beta_m$ *die Nullstellen von* g. *Dann sind die Nullstellen von* f *gerade die Nullstellen von* $h - \beta_i$ $(1 \leq i \leq m)$.

Beweis: Die Behauptung folgt aus

$$f = g(h) = \prod_{i=1}^{m}(h - \beta_i).$$

$\square$

KOROLLAR 5.6. *Seien* $f = \hat{g}(h_1, h_2)$ *eine homogene bivariate Dekomposition und* $\beta_1, \ldots, \beta_m$ *die Nullstellen von* $g = \hat{g}(t, 1) \in \mathbb{Q}[t]$. *Dann sind die Nullstellen von* f *gerade die Nullstellen von* $h_1 - \beta_i h_2$ $(1 \leq i \leq m)$.

Beweis: Wegen $f = h_2^m g(\frac{h_1}{h_2})$ und $\deg(h_2) < \deg(f)$ erhalten wir, daß $f(t) = 0$ äquivalent zu $g(\frac{h_1}{h_2}) = 0$ ist. Hieraus folgt dann für ein $1 \leq i \leq m$: $\frac{h_1}{h_2} = \beta_i$ und damit $h_1 - \beta_i h_2 = 0$. $\square$

KOROLLAR 5.7. *Seien* $f = N_g(h)$ *eine Normdekomposition und* $\beta_1, \ldots, \beta_m$ *die Nullstellen von* g. *Dann erhalten wir die Nullstellen von* f *als Nullstellen von* $h^{(i)}$ $(1 \leq i \leq m)$.

Beweis: Die Behauptung folgt aus

$$f = N_g(h) = \prod_{i=1}^{m} h^{(i)}.$$

$\square$

2. Zusammenhänge zwischen Teilkörpern und Dekompositionen

In diesem Abschnitt werden wir eine Korrespondenz zwischen Teilkörpern und Normdekompositionen herleiten. Wir werden sehen, daß zu jedem Teilkörper eine Normdekomposition und zu jeder Normdekomposition ein Teilkörper existiert. Weiterhin werden wir ein Verfahren angeben, welches eine zu einem Teilkörper gehörende Normdekomposition berechnet. Im folgenden sei $g \in \mathbb{Q}[t]$ normiert und irreduzibel, und eine Nullstelle β von g erzeuge den Zahlkörper $L = \mathbb{Q}(\beta)$.

Lemma 5.8. *Gilt $f = N_g(h)$, dann ist L ein Teilkörper von E und h ist das Minimalpolynom von α über L.*

Beweis: Wegen $h(\alpha) = 0$ und g irreduzibel, ist L Teilkörper von E und h irreduzibel über L. $\square$

Lemma 5.9. *Sei L ein Teilkörper von E. Dann existiert ein $h \in L[t]$ mit $f = N_g(h)$.*

Beweis: Sei h das Minimalpolynom von α über L. Damit folgt $f = N_g(h)$. $\square$

In den beiden vorangegangenen Lemmata haben wir gesehen, daß zu jedem Teilkörper eine Dekomposition und zu jeder Dekomposition ein Teilkörper korrespondieren.

Definition 5.10. *Wir nennen zwei Dekompositionen äquivalent, falls sie zu demselben Teilkörper korrespondieren.*

Wir geben nun ein Verfahren an, welches eine zugehörige Normdekomposition aus einem bereits berechneten Teilkörper bestimmt. Im folgenden sei L ein Teilkörper von E mit Einbettungspolynom $\omega \in \mathbb{Q}[t]$, d.h. $\omega(\alpha) = \beta$.

Satz 5.11. *Für*

$$h := \mathrm{ggT}(f, \omega - \beta) \text{ in } L[t],$$

ist $N_g(h)$ eine Normdekomposition von f.

Beweis: Sei $\Delta_1, \dots, \Delta_m$ das zugehörige Blocksystem zum Teilkörper L von E, wobei $\alpha \in \Delta_1$ gilt. Dann gilt für alle $\gamma \in \Delta_1 : \ \omega(\gamma) = \beta$. Für ein $\gamma \in \Delta_i$ mit $2 \leq i \leq m$ folgt aber $\omega(\gamma) \neq \beta$. Damit entspricht der Grad von h dem Grad von E/L, woraus die Irreduziblität von h und die Behauptung folgen. $\square$

Wir berechnen den ggT von Polynomen über Zahlkörpern mittels eines modularen Algorithmus aus [13]. Der vorangegangene Satz ermöglicht es uns, auf sehr effiziente Weise eine Normdekomposition aus einem bereits berechneten Teilkörper zu bestimmen. Weiterhin ist es interessant, daß wir in der Lage sind, eine funktionale bzw. homogene bivariate Dekomposition zu bestimmen, falls eine solche existiert. Der Beweis des folgenden Lemmas ist eine direkte Konsequenz von Theorem 8 aus [19].

LEMMA 5.12. *Sei $f = N_g(h)$ eine Normdekomposition. Dann existiert eine äquivalente funktionale Dekomposition von f genau dann, wenn $\tilde{h}(t) = h(t) - h(0) \in \mathbb{Q}[t]$ gilt. In diesem Fall erhalten wir die funktionale Dekomposition $f = \tilde{g}(\tilde{h})$, wobei $\tilde{g}$ das Minimalpolynom von $h(0)$ über $\mathbb{Q}$ ist.*

LEMMA 5.13. *Sei $f = N_g(h)$ eine Normdekomposition. Dann existiert eine äquivalente homogene bivariate Dekomposition genau dann, wenn $h = h_1 - \tilde{\beta} h_2$ mit $h_i \in \mathbb{Q}[t]$ $(1 = 1, 2)$ und $\tilde{\beta} \in L$ gilt. In diesem Fall sei $\tilde{g}$ das Minimalpolynom von $\tilde{\beta}$. Wir erhalten $f = \hat{g}(h_1, h_2)$ mit $\hat{g} \in \mathbb{Q}[t, u]$ homogen und $\hat{g}(t, 1) = \tilde{g}(t)$.*

Beweis: Falls f eine äquivalente homogene bivariate Dekomposition besitzt, folgt aus dem Beweis von Satz 5.3, daß $h = h_1 - \tilde{\beta} h_2$ gilt. Sei nun $h = h_1 - \tilde{\beta} h_2$ und $\tilde{g}$ das Minimalpolynom von $\tilde{\beta}$. Analog zum Beweis von Satz 5.3 erhalten wir, daß $f = \hat{g}(h_1, h_2)$ eine homogene bivariate Dekomposition ist. □

In unserem Teilkörperalgorithmus werden die erzeugenden Polynome g so konstruiert, daß in den Lemmata 5.12 und 5.13 $g = \tilde{g}$ gewählt werden kann. Wir können also eine funktionale oder homogene bivariate Dekomposition an dem Polynom h ablesen.

Um „schönere“ Dekompositionen, d.h. kürzere Darstellungen, zu erhalten, ist es möglich, die OrderShort–Funktion von KASH [7] zu benutzen. Diese liefert im allgemeinen „kürzere“ Polynome g für die Teilkörper, welche in den meisten Fällen auch zu kürzeren Polynomen h führen. Der Algorithmus zur Berechnung der kürzeren Polynomen basiert auf dem LLL–Algorithmus [25] und ist eine leichte Modifikation des in [5, section 4.4.2] beschriebenen Algorithmus.

3. Türme von Zahlkörpern

In diesem Abschnitt entwickeln wir ein Verfahren für Normdekompositionen, falls wir einen ganzen Turm von Teilkörpern kennen. Wir benutzen in diesem Abschnitt die folgenden Bezeichnungen: Seien $E = \mathbb{Q}(\alpha)$ ein Zahlkörper, der von einem normierten Polynom $f \in \mathbb{Q}[t]$ erzeugt wird. Weiterhin seien $L_1 = \mathbb{Q}(\beta_1)$ ein

Teilkörper von E erzeugt durch normiertes $g_1 \in \mathbb{Q}[t]$ und $L_2 = \mathbb{Q}(\beta_2)$ ein Teilkörper von L_1 erzeugt durch normiertes $g_2 \in \mathbb{Q}[t]$. Im für uns günstigsten Fall kennen wir die Einbettungspolynome $\omega_1, \omega_2 \in \mathbb{Q}[t]$ mit $\omega_1(\alpha) = \beta_1$ und $\omega_2(\beta_1) = \beta_2$. Damit erhalten wir die folgende Normdekomposition von f.

LEMMA 5.14. *Seien* $h_1 := \mathrm{ggT}(f, \omega_1 - \beta_1) \in L_1[t]$ *und* $h_2 := \mathrm{ggT}(g_1, \omega_2 - \beta_2) \in L_2[t]$. *Dann erhalten wir:*

$$f = N_{g_1}(h_1) = N_{N_{g_2}(h_2)}(h_1).$$

Beweis: Mit Hilfe von Satz 5.11 erhalten wir $f = N_{g_1}(h_1)$ und $g_1 = N_{g_2}(h_2)$, woraus die Behauptung folgt. □

Im allgemeinen liefert der Teilkörperalgorithmus keine Einbettung von L_2 in L_1, sondern lediglich Einbettungen von L_2 nach E und L_1 nach E. Sei nun $\tau \in \mathbb{Q}[t]$ mit $\tau(\alpha) = \beta_2$ gegeben. Wir wollen nun mit Hilfe von ω_1 und τ das Einbettungspolynom ω_2 berechnen.

LEMMA 5.15. *Seien* $\beta_2 = \sum\limits_{i=0}^{n-1} c_i \alpha^i$ *und* $\beta_1^j = \sum\limits_{i=0}^{n-1} b_{i,j} \alpha^i$ $(0 \le j \le m-1)$. *Seien* $B = (b_{i,j})_{\substack{0 \le i \le n-1 \\ 0 \le j \le m-1}}$, $\underline{c} = (c_0, \ldots, c_{n-1})^t$, *und* $\underline{x} = (x_0, \ldots, x_{m-1})^t$ *mit* $B\underline{x} = \underline{c}$ *gegeben. Dann gilt* $\beta_2 = \sum_{j=0}^{m-1} x_j \beta_1^j$.

Beweis: Das lineare Gleichungssystem hat genau eine Lösung, da $\beta_2 \in \mathbb{Q}(\beta_1)$ gilt. □

Nachdem wir die Dekomposition $f = N_{N_{g_2}(h_2)}(h_1)$ ausgerechnet haben, können wir die Koeffizienten von h_2 auf zwei Arten darstellen. Wir können einerseits die Basis $\{1, \beta_1, \ldots, \beta_1^{m-1}\}$ und andererseits die Basis $\{\beta_2^i \beta_1^j \mid 0 \le i \le l-1, 0 \le j \le \frac{m}{l} - 1\}$ wählen, hierbei ist l der Grad des Teilkörpers L_2. Wir nennen die erste Darstellung absolut und die zweite relativ. In den meisten Fällen führt die relative Darstellung zu kürzeren Koeffizienten.

KAPITEL VI

Automorphismen

In diesem Kapitel werden wir mehrere Verfahren zur Berechnung von Automorphismen algebraischer Zahlkörper entwickeln. Wir werden verschiedene Methoden vorstellen, um Automorphismen in absolut- und relativ-abelschen Erweiterungen zu berechnen. Weiterhin werden wir den Fall eines über $\mathbb{Q}$ normalen Zahlkörpers betrachten. Die Methode zur Berechnung von Automorphismen von über $\mathbb{Q}$ abelschen Zahlkörpern wurden bereits in [1] veröffentlicht.

Zur Bestimmung der Automorphismen eines Zahlkörpers genügt es, alle Nullstellen eines erzeugenden Polynoms zu bestimmen, d.h. das erzeugende Polynom über dem Zahlkörper zu faktorisieren. Die Faktorisierungsalgorithmen für Polynome über Zahlkörpern sind im allgemeinen für dieses Problem aber nicht effizient genug. Wir verfolgen in diesem Kapitel das Ziel, effizientere Lösungen für dieses Problem zu finden.

1. Grundlagen

Es seien F und $E = F(\alpha)$ algebraische Zahlkörper, wobei α Nullstelle von einem irreduziblen und normierten $f \in \mathfrak{o}_F[t]$ ist. Wir bezeichnen mit n den Grad von E/F, wobei zusätzlich E/F normal sein soll.

Nehmen wir nun an, daß wir alle Nullstellen $\alpha := \alpha_1, \dots, \alpha_n$ von f in der folgenden Form darstellen können:

$$\alpha_i = \frac{1}{d}\sum_{j=0}^{n-1} a_{i,j}\alpha^j \text{ mit } d \in \mathbb{N},\ a_{i,j} \in \mathfrak{o}_F\ (1 \le i \le n).$$

Dies ist genau dann möglich, wenn E/F normal ist. Mit Hilfe der Nullstellen können wir nun die Automorphismen σ_i definieren. Dabei soll α von σ_i auf α_i abgebildet werden. Wir können also σ_i in der folgenden Form schreiben:

$$\sigma_i(\alpha) = \frac{1}{d} \sum_{j=0}^{n-1} a_{i,j} \alpha^j \ (1 \leq i \leq n).$$

Es besteht also eine sehr einfache Beziehung zwischen den Nullstellen von f und den Automorphismen von E/F. Wir werden in unseren Algorithmen die Nullstellen von f berechnen und können damit die Automorphismen sofort darstellen.

Sei nun $\gamma := \sum_{j=0}^{n-1} c_j \alpha^j \in E$ mit $c_j \in F$ $(0 \leq j \leq n-1)$ gegeben. Dann gilt:

$$\sigma_i(\gamma) = \sum_{j=0}^{n-1} c_j \sigma_i(\alpha)^j. \tag{6-1}$$

Wir können diesen Ausdruck mittels des Horner-Schemas berechnen. Dieser Ansatz benötigt $n-2$ Multiplikationen von Elementen in E und eine Multiplikation von einem Element in E mit einem von F.

Bei zwei- oder mehrfacher Anwendung des Automorphismus σ_i erweist sich die folgende Berechnungsmethode als günstiger:

(1) Initialisierung: Berechne $1, \sigma_i(\alpha), \ldots, \sigma_i(\alpha)^{n-1}$ und speichere diese Werte ab.
(2) Benutze die $\sigma_i(\alpha)^j$ $(0 \leq j \leq n-1)$ zur Berechnung von $\sigma_i(\gamma)$.

Der Inititialisierungs-Schritt muß nur einmal durchgeführt werden und benötigt $n-2$ Multiplikationen von Elementen in E. Der eigentliche Anwendungsschritt benötigt $n-1$ Multiplikationen von Elementen von E mit Elementen von F.

Die Multiplikation von zwei Elementen in E kann mittels $2n^2 - n$ Multiplikationen von zwei Elementen in F berechnet werden (vgl. Lemma 3.5). Für die Multiplikation von einem Element in E mit einem Element in F benötigen wir n Multiplikationen von zwei Elementen in F. Hieraus ergeben sich für den Horner-Schemaansatz $(n-2)(2n^2-n)+n = 2n^3-5n^2+3n$ Multiplikationen von Elementen in F. Wir benötigen $(n-2)(2n^2-n) = 2n^3-5n^2+2n$ Multiplikationen von Elementen in F für den Inititialisierungsschritt und $(n-1)n = n^2-n$ Multiplikationen von Elementen in F für die eigentliche Anwendung des Automorphismus. Wir fassen dieses Ergebnis in dem folgenden Lemma zusammen.

Lemma 6.1. *Zur Initialisierung eines Automorphismus σ_i benötigen wir $2n^3 - 5n^2 + 2n$ Multiplikationen von Elementen in F. Wir können dann einen Automorphismus mit $n^2 - n$ Multiplikationen in F auf ein Element in E anwenden.*

Wir wollen zur Berechnung der Automorphismen von E/F ohne die Kenntnis der Maximalordnung von E auskommen. Dies bedeutet, daß wir in der Gleichungsordnung $\mathfrak{o}_F[\alpha]$ arbeiten werden. In dieser Ordnung können ganze algebraische Zahlen γ im allgemeinen nur mit Nennern dargestellt werden:

$$\gamma = \frac{1}{d}\sum_{i=0}^{n-1} c_i\alpha^i \text{ mit } c_i \in \mathfrak{o}_F \text{ und } d \in \mathbb{N}.$$

Wir sind nun an einer Abschätzung des Nenners, d.h. an einem Vielfachen von d interessiert. Diese liefert uns das folgende Lemma.

Lemma 6.2. *Sei $\mathfrak{d}(f) = \mathfrak{a}^2\mathfrak{b}$, mit $\mathfrak{b}$ quadratfrei. Dann ist die kleinste positive ganze Zahl in $\mathfrak{a}$ ein Vielfaches von d.*

Beweis: Für ein beliebiges $\gamma \in \mathfrak{o}_E$ gilt: $\gamma\mathfrak{a} \subseteq \mathfrak{o}_F[\alpha]$. Damit gilt insbesondere für die kleinste positive ganze Zahl c in $\mathfrak{a}$: $c\gamma \in \mathfrak{o}_F[\alpha]$. □

Wir klären nun, wie wir diesen Nenner d bei Kongruenzen berücksichtigen. Im folgenden sei $\mathfrak{p}$ stets ein Primideal von $\mathfrak{o}_F$ mit $\mathfrak{p} \nmid \mathfrak{d}(f)$.

Bezeichnung 6.3. *Sei $\mathfrak{P}$ ein Primideal in $\mathfrak{o}_F[\alpha]$, welches über $\mathfrak{p}$ liegt. Wir schreiben für $\gamma, \delta \in \frac{1}{d}\mathfrak{o}_F[\alpha]$:*

$$\gamma \equiv \delta \bmod \mathfrak{P}^k, \textit{ falls } d\gamma \equiv d\delta \bmod \mathfrak{P}^k$$

gilt.

Bei der Berechnung des Frobeniusautomorphismus σ zu $\mathfrak{P}$ werden wir als ersten Schritt ein $\bar{\sigma}$ mit $\bar{\sigma}(\alpha) \equiv \sigma(\alpha) \bmod \mathfrak{P}$ bestimmen.

Lemma 6.4. *Seien $\sigma, \tau \in \mathrm{Aut}(E/F)$. Dann gilt $\sigma = \tau$ genau dann, wenn $\sigma(\alpha) \equiv \tau(\alpha) \bmod \mathfrak{P}$ für ein Primideal $\mathfrak{P}$ über $\mathfrak{p}$ in $\mathfrak{o}_F[\alpha]$ gilt.*

Beweis: Aus $\sigma = \tau$ folgt $\sigma(\alpha) \equiv \tau(\alpha) \bmod \mathfrak{P}$. Da $\mathfrak{p} \nmid \mathfrak{d}(f)$ gilt, wissen wir, daß

$$f(t) \equiv \prod_{i=1}^{n}(t - \bar{\alpha}_i) \bmod \mathfrak{P} \text{ mit } \bar{\alpha}_i \neq \bar{\alpha}_j \text{ für } i \neq j$$

gilt. Damit folgt für $\sigma \neq \tau \in \mathrm{Aut}(E/F)$, daß $\bar{\sigma} \neq \bar{\tau}$ gilt, woraus die Behauptung folgt. □

Dieses Lemma zeigt, daß ein Automorphismus σ, der modulo $\mathfrak{P}$ bekannt ist, dadurch eindeutig bestimmt ist. Wir können nun das folgende Lemma zeigen.

LEMMA 6.5. *Sei $T \subseteq \mathrm{Aut}(E/F)$ und $\sigma \in \mathrm{Aut}(E/F)$. Dann ist $\sigma \in T$ genau dann, wenn ein $\tau \in T$ existiert mit $\tau(\alpha) \equiv \sigma(\alpha) \bmod \mathfrak{P}$ für ein Primideal $\mathfrak{P}$ über $\mathfrak{p}$ in $\mathfrak{o}_F[\alpha]$.*

Beweis: Die Behauptung ist eine direkte Konsequenz von Lemma 6.4. □

Da mit $\sigma, \tilde{\sigma}$ auch $\sigma\tilde{\sigma}$ wieder ein Automorphismus ist, sind wir daran interessiert, alle Elemente von $\langle\sigma, \tilde{\sigma}\rangle$ zu bestimmen. Im folgenden sei stets $G = \mathrm{Gal}(f)$. Zuerst behandeln wir den Fall G abelsch.

LEMMA 6.6. *Seien G abelsch, H Untergruppe von G und $\sigma \in G$. Für die kleinste natürliche Zahl s mit $\sigma^s \in H$ gilt nun:*

$$\langle H, \sigma\rangle = \{h\sigma^i \mid h \in H,\ 0 \leq i < s\}.$$

Weiterhin gilt $h_1\sigma^i = h_2\sigma^j$ mit $0 \leq i, j < s$ nur für $h_1 = h_2$ und $i = j$.

Im nicht abelschen Fall ist die rechte Menge im allgemeinen nur eine Teilmenge des gesuchten Erzeugnisses. Ein Algorithmus (Diminos Algorithmus) für den allgemeinen Fall wird in [2, Seite 14–23] präsentiert. Eine Idee dabei ist, daß wir mit einem neuen Element immer gleich die ganze Nebenklasse der bisher bekannten Untergruppe H zu G hinzufügen kann. Eine andere Idee ist, daß wir nur die Erzeuger von H für die Abgeschlossenheit betrachten müssen. Wir geben an dieser Stelle nur den Algorithmus an und verweisen für einen Beweis auf [2].

ALGORITHMUS 6.7. (Diminos Algorithmus zur Berechnung aller Elemente einer Permutationsgruppe $\langle\sigma_1, \ldots, \sigma_r\rangle \subseteq G$)

Input: $\{\sigma_1, \ldots, \sigma_r\}$, $H = \langle\sigma_1, \ldots, \sigma_{r-1}\rangle$, *sowie alle Elemente von H.*

Output: *Alle Elemente von $\langle\sigma_1, \ldots, \sigma_r\rangle$.*

Schritt 1: *Setze* `klassen` $:= \{$`id`$\}$ *und T auf die Menge der Elemente von H.*

Schritt 2: *Wiederhole*
  (1) *Wähle ein $\tau \in$* `klassen` *und setze* `klassen` $:=$ `klassen` $\setminus\{\tau\}$.
  (2) *Für alle $\sigma \in \{\sigma_1, \ldots, \sigma_r\}$ tue folgendes:*
    (a) *Setze $\omega := \tau\sigma$.*
    (b) *Falls ω nicht in T enthalten ist, so füge ω zu* `klasssen` *und alle Elemente der Nebenklasse $H\omega$ zu T hinzu.*

Schritt 3: *Solange* `klassen` $\neq \emptyset$ *gilt.*

Schritt 4: *Gebe T aus und terminiere.*

2. Abelsche Erweiterungen

Wir werden nun einige Eigenschaften von abelschen Erweiterungen herleiten, die wir zur Berechnung der Automorphismen benötigen. Hierzu sei E/F eine abelsche Erweiterung, wobei der Fall $F = \mathbb{Q}$ ausdrücklich erlaubt ist.

Sei $\mathfrak{p}$ ein Primideal in $\mathfrak{o}_F$, welches nicht $\mathfrak{d}(f)$ teilt. Weiterhin sei die folgende Faktorisierung gegeben:

$$f \equiv f_1 \cdots f_r \bmod \mathfrak{p}.$$

Da E/F normal ist, gilt $\deg(f_i) = \deg(f_j)$ $(1 \leq i, j \leq r)$. Wir erhalten

$$\mathfrak{p}\mathfrak{o}_F[\alpha] = \mathfrak{P}_1 \cdots \mathfrak{P}_r,$$

wobei die $\mathfrak{P}_i$ Primideale in $\mathfrak{o}_F[\alpha]$ sind. Diese Primideale haben alle über $\mathfrak{p}$ denselben Trägheitsgrad $\deg(f_1)$. Wir bezeichnen mit σ_i den Frobeniusautomorphismus von $\mathfrak{P}_i/\mathfrak{p}$, für welchen $\sigma_i(\alpha) \equiv \alpha^{p^{f_\mathfrak{p}}} \bmod \mathfrak{P}_i$ gilt. Wir wissen, daß die Frobeniusautomorphismen $\sigma_1, \ldots, \sigma_r$ zueinander konjugiert sind. Da die Erweiterung E/F abelsch ist, folgt sogar $\sigma_1 = \cdots = \sigma_r$. Wir bezeichnen diesen Automorphismus mit σ und erhalten:

$$\sigma(\alpha) \equiv \alpha^{p^{f_\mathfrak{p}}} \bmod \mathfrak{p}\mathfrak{o}_F[\alpha].$$

Seien nun

$$\sigma(\alpha) = \frac{1}{d} \sum_{i=0}^{n-1} a_i \alpha^i \text{ mit } d \in \mathbb{N},\ a_i \in \mathfrak{o}_F \ (0 \leq i \leq n-1)$$

und

$$\bar{\sigma}(\alpha) = \sum_{i=0}^{n-1} \bar{a}_i \alpha^i \text{ mit } \bar{a}_i \in \mathfrak{o}_F \ (0 \leq i \leq n-1)$$

gegeben mit $\sigma(\alpha) \equiv \bar{\sigma}(\alpha) \bmod \mathfrak{p}^k\mathfrak{o}_F[\alpha]$ für ein $k \in \mathbb{N}$. Dann folgt: $a_i \equiv d\bar{a}_i \bmod \mathfrak{p}^k$.

Da wir $\bar{\sigma}$ konstruktiv berechnen können, wollen wir für jedes $\bar{a}_i$ das Problem lösen, einen geeigneten Vertreter a_i in derselben Restklasse modulo $\mathfrak{p}^k$ zu finden. Im Fall $F = \mathbb{Q}$ ist dies sehr einfach, da wir $\bar{a}_i$ einfach in das symmetrische Restsystem zu 0 bringen können. Eine rationale Zahl können wir dann mit Hilfe von Algorithmus 2.14 ermitteln. Der Fall $F \neq \mathbb{Q}$ ist wesentlich komplizierter zu behandeln. Wir werden darauf später genauer eingehen.

3. Absolut-abelsche Erweiterungen

Im absolut-abelschen Fall sind wir in der Lage, einen sehr effizienten Algorithmus zur Berechnung der Automorphismen anzugeben. Die wesentlichen Ideen wurden bereits in den vorherigen Abschnitten hergeleitet. Da wir im absolut-abelschen Fall sind, bedeutet dies für uns, daß $F = \mathbb{Q}$ und $f \in \mathbb{Z}[t]$ normiert und irreduzibel gelten. Im folgenden Algorithmus werden die Nullstellen von f in E berechnet, d.h. die Automorphismen werden durch algebraische Zahlen dargestellt.

Algorithmus 6.8. (Automorphismen in absolut-abelschen Zahlkörpern)

Input: *$E = \mathbb{Q}(\alpha)/\mathbb{Q}$ abelsch und Minimalpolynom $f \in \mathbb{Z}[t]$ von α.*

Output: *Die Automorphismen von $E/\mathbb{Q}$.*

Schritt 1: *Setze $T := \{\alpha\}$ und $p := 2$.*

Schritt 2: *Berechne mit Korollar 2.18 eine obere Schranke B für d und a_i.*

Schritt 3: *Wiederhole*
- (1) *Wiederhole*
  - (a) *Setze p auf die nächste Primzahl mit $p \nmid \operatorname{disc}(f)$.*
  - (b) *Berechne modulo p den Frobeniusautomorphismus $\bar{\sigma}$ von p.*
- (2) *Solange bis $\sigma \notin T$ gilt (Test mit Lemma 6.5 ohne σ auszurechnen).*
- (3) *Berechne (modulo p) ein minimales a mit $\sigma^a \in T$.*
- (4) *Berechne minimales k mit $p^{2^k} > 2B^2$.*
- (5) *Berechne mit Algorithmus 3.15 den Frobeniusautomorphismus σ.*
- (6) *Berechne $\sigma^2, \dots, \sigma^{a-1}$.*
- (7) *Setze $N := \emptyset$.*
- (8) *Für alle $\gamma \in T$ tue folgendes (vgl. Lemma 6.6)*
  - (a) *Füge die Elemente $\sigma(\gamma), \dots, \sigma^{a-1}(\gamma)$ zu N hinzu.*
- (9) *Setze $T := T \cup N$.*

Schritt 4: *Solange bis $|T| = n$ gilt.*

Schritt 5: *Gebe T aus und terminiere.*

4. Hilbertsche Verzweigungstheorie und Zerlegungskörper

Zur Berechnung der Automorphismen eines normalen Zahlkörpers können wir Ergebnisse aus der Hilbertschen Verzweigungstheorie verwenden. Sei also im folgenden E/F eine normale Erweiterung mit Galoisgruppe $G = \operatorname{Gal}(f)$. Sei weiterhin ein Primideal $\mathfrak{p}$ von $\mathfrak{o}_F$ gegeben, welches unverzweigt in E ist, d.h. $\mathfrak{p}$ teilt nicht die Relativdiskriminante von E/F. Dann zerlegt sich $\mathfrak{p}$ in $\mathfrak{o}_E$ wie folgt:

$$\mathfrak{p}\mathfrak{o}_E = \mathfrak{P}_1 \cdots \mathfrak{P}_r$$

mit paarweise verschiedenen $\mathfrak{P}_i$. Da die Erweiterung normal ist, haben alle Primideale denselben Trägheitsgrad. Die folgenden Resultate gelten nur für den unverzweigten Fall. Für Aussagen im verzweigten Fall verweisen wir auf [27, 23].

DEFINITION 6.9. *Sei $\mathfrak{P}$ ein Primideal von $\mathfrak{o}_E$, welches über $\mathfrak{p}$ liegt. Dann heißt $G_{Z_\mathfrak{P}} := \{g \in G \mid g(\mathfrak{P}) = \mathfrak{P}\}$ die Zerlegungsgruppe von $\mathfrak{P}$. Der zu dieser Gruppe zugehörige Fixkörper $Z_\mathfrak{P}$ heißt Zerlegungskörper.*

LEMMA 6.10. *Die Zerlegungsgruppe $G_{Z_\mathfrak{P}}$ ist zyklisch vom Grad $f_{\mathfrak{P}/\mathfrak{p}}$ und wird vom Frobeniusautomorphismus σ mit $\sigma(\alpha) \equiv \alpha^{p^{f_\mathfrak{p}}} \bmod \mathfrak{P}$ erzeugt.*

Beweis: Der Beweis kann in [27, 23] nachgelesen werden. □

SATZ 6.11. *Seien $K = F(\rho)$ ein algebraischer Zahlkörper, m_ρ das Minimalpolynom von ρ, N die normale Hülle von K/F und $\mathfrak{p}$ unverzweigt in K (und damit auch in N). Für $\mathfrak{p}\mathfrak{o}_K = \mathfrak{P}_1 \cdots \mathfrak{P}_r$ und $\hat{\mathfrak{P}}$ ein beliebiges Primideal von N über $\mathfrak{p}$ gilt dann: $f_{\hat{\mathfrak{P}}/\mathfrak{p}} = \mathrm{kgV}(f_{\mathfrak{P}_1/\mathfrak{p}}, \dots, f_{\mathfrak{P}_r/\mathfrak{p}})$.*

Beweis: Sei $\tilde{m}_\rho = \phi(m_\rho)$ das Bild unter der kanonischen Einbettung von $F[t]$ nach $F_\mathfrak{p}[t]$. Dann faktorisiert $\tilde{m}_\rho$ in r Faktoren, wobei die Grade der Faktoren gerade den Trägheitsgraden der zugehörigen Primideale entsprechen. Hieraus folgt, daß der Grad des Zerfällungskörpers von $\tilde{m}_\rho$ gleich $\mathrm{kgV}(f_{\mathfrak{P}_1/\mathfrak{p}}, \dots, f_{\mathfrak{P}_r/\mathfrak{p}})$ ist. □

SATZ 6.12. *Seien $\mathfrak{p}\mathfrak{o}_{Z_\mathfrak{P}} = \wp_1 \cdots \wp_s$ die Zerlegung von $\mathfrak{p}$ im Zerlegungskörper und N die normale Hülle von $Z_\mathfrak{P}/F$. Dann gilt $[N : Z_\mathfrak{P}] = \mathrm{kgV}(f_{\wp_1}, \dots, f_{\wp_s})$.*

Beweis: Da E normal ist, liegt N zwischen $Z_\mathfrak{P}$ und E. Sei $\tilde{\mathfrak{P}}$ das eindeutige Primideal von $\mathfrak{o}_N$, welches über $\wp$ bzw. unter $\mathfrak{P}$ liegt. Da N die normale Hülle ist, haben alle Primideale in $\mathfrak{o}_N$ nach Satz 6.11 über $\mathfrak{p}$ denselben Trägheitsgrad l. Damit hat insbesondere das einzige Primideal über $\wp$ in $\mathfrak{o}_N$ den Grad l und damit folgt $[N : Z_\mathfrak{P}] = l$. □

KOROLLAR 6.13. *Der Zerlegungskörper $Z_\mathfrak{P}$ ist genau dann normal, wenn $\mathfrak{p}$ in $\mathfrak{o}_{Z_\mathfrak{P}}$ voll zerlegt ist.*

In den vorangegangenen Sätzen haben wir einige Eigenschaften von Zerlegungskörpern kennengelernt, die wir zu deren Berechnung nutzen werden. In Satz 4.30 haben wir einen Zusammenhang zwischen der Primidealzerlegung und dem Blocksystem eines Teilkörpers hergeleitet. Diesen Zusammenhang können wir auf sehr effiziente Weise dazu nutzen, die normale Hülle des Zerlegungskörpers auszurechnen. Da in der normalen Hülle genausoviele Primideale über $\mathfrak{p}$ wie in $\mathfrak{o}_E$ liegen, erhalten wir folgenden Algorithmus zur Berechnung der normalen Hülle des Zerlegungskörpers zu einem Primideal $\mathfrak{P}$, ohne den Zerlegungskörper explizit zu kennen.

ALGORITHMUS 6.14. (Berechnung der normalen Hülle eines Zerlegungskörpers)

Input: *Ein erzeugendes Polynom $f \in \mathfrak{o}_F[t]$ vom Grad n für den Zahlkörper E, ein Primideal $\mathfrak{p}$ von $\mathfrak{o}_F$ mit $\mathfrak{p} \nmid \mathfrak{d}(f)$ und ein Primideal $\mathfrak{P}$ von $\mathfrak{o}_E$, welches über $\mathfrak{p}$ liegt.*

Output: *Die normale Hülle N des Zerlegungskörpers $Z_{\mathfrak{P}}$.*

Schritt 1: *Setze $l := 1$ und berechne $\bar{f} \in \mathbb{F}_q[t]$ mit $f \equiv \bar{f} \bmod \mathfrak{p}$ ($\mathbb{F}_q \cong \mathfrak{o}_F/\mathfrak{p}$).*

Schritt 2: *Faktorisiere $\bar{f} = f_1 \cdots f_r$ in $\mathbb{F}_q[t]$.*

Schritt 3: *Faktorisiere $f_i = f_{i,1} \cdots f_{i,l}$ in $\mathbb{F}_{q^l}[t]$ $(1 \leq i \leq r)$.*

Schritt 4: *Setze $\Delta_{(i-1)l+j} := \{f_{i,j}\}$ $(1 \leq i \leq r, 1 \leq j \leq l)$.*

Schritt 5: *Teste mit den Algorithmen 4.27 bzw. 4.29, ob $\Delta_1, \ldots, \Delta_{rl}$ ein Blocksystem ist.*

Schritt 6: *Falls ja, so gebe den zugehörigen Teilkörper aus und terminiere. Ansonsten setze $l := \min\{\mu \in \mathbb{N} \mid \mu > l \text{ und } \mu \mid n\}$.*

Schritt 7: *Falls $l = n$ gilt, gebe E aus und terminiere. Ansonsten gehe zu Schritt 3.*

Wir merken an, daß die Algorithmen 4.27 und 4.29 nur in dem Fall $F = \mathbb{Q}$ anwendbar sind. Daher ist unsere Implementierung von Algorithmus 6.14 auch auf diesen Fall beschränkt. Zur eigentlichen Berechnung des Zerlegungskörpers können wir uns nun im folgenden auf mögliche Blocksysteme beschränken, die einerseits das Blocksystem von N enthalten und andererseits zu einer Primidealfaktorisierung korrespondieren, die der kgV-Bedingung aus Satz 6.11 genügt.

Wir haben prinzipiell zwei Möglichkeiten, den Zerlegungskörper zu einem Primideal zu bestimmen. Die erste Möglichkeit besteht darin, die normale Hülle N des Zerlegungskörpers mit Algorithmus 6.14 zu berechnen, um anschließend den

Zerlegungskörper als Teilkörper von N zu erhalten. Die andere Möglichkeit besteht darin, alle Teilkörper zu berechnen. Hiernach ist es sehr einfach, anhand der Primidealzerlegung den richtigen Körper zu finden. In der Praxis zeigt sich, daß es für beide Verfahren Beispiele gibt, in denen sie effizienter als das jeweilige andere Verfahren sind. Auf den ersten Blick ist es überraschend, daß das zweite Verfahren, welches alle Teilkörper berechnet, dem ersten Verfahren überlegen sein soll, welches gezielt einen Teilkörper berechnet. Hierfür gibt es aber eine logische Erklärung: Beim ersten Verfahren sind wir gezwungen, die Primzahl für die Teilkörperberechnung zu nehmen, die zum Zerlegungskörper korrespondiert. Diese Primzahl kann für unseren Algorithmus sehr schlechte Eigenschaften haben und sich damit sehr ungünstig auf die Laufzeit auswirken. Allerdings können wir bei der Auswahl auch das Glück haben, daß unser p eine Primzahl ist, die wir auch zur Teilkörperberechnung gewählt hätten. In diesem Fall müssen wir mit dem ersten Verfahren deutlich weniger Teilkörper berechnen.

Wir sind nun daran interessiert, den Frobeniusautomorphismus σ zu $Z_{\mathfrak{P}}$ explizit auszurechnen. Daher werden wir nun einige Eigenschaften herleiten. Dazu sei im folgenden

$$\sigma(\alpha) = \frac{1}{d}\sum_{i=0}^{n-1} a_i\alpha^i \ (d \in \mathbb{N},\ a_i \in \mathfrak{o}_F).$$

Wir bezeichnen mit $\Delta_1, \dots, \Delta_m$ das zu $Z_{\mathfrak{P}}$ gehörige Blocksystem ($m = f_{\mathfrak{P}/\mathfrak{p}}$).

Definition 6.15. *Das Polynom $F_\sigma(t) = \frac{1}{d}\sum_{i=0}^{n-1} a_i t^i \in F[t]$ heißt Polynomdarstellung von σ (bzgl. α).*

Aufgrund der Definition von F_σ ist klar, daß wir mit F_σ auch σ kennen und $F_\sigma(\alpha) = \sigma(\alpha)$ gilt. Wir sind nun im folgenden daran interessiert, wie F_σ auf den Nullstellen $\alpha = \alpha_1, \dots, \alpha_n$ von f operiert.

Da die Koeffizienten von F_σ von allen $\pi \in \mathrm{Aut}(E/F)$ invariant gelassen werden, gilt für $\gamma \in E : \pi(F_\sigma(\gamma)) = F_\sigma(\pi(\gamma))$. Wir erhalten die folgenden Lemmata.

Lemma 6.16. *Durch F_σ wird eine bijektive Abbildung von $\Omega = \{\alpha_1, \dots, \alpha_n\}$ auf sich selbst definiert.*

Beweis: Sei $i \in \{1, \dots, n\}$ beliebig fixiert und $\pi \in \mathrm{Aut}(E/F)$ mit $\pi(\alpha) = \alpha_i$. Weiterhin gelte $\alpha_i \in \Delta_j$. Dann wird Δ_j gerade von $\sigma_j = \pi\sigma\pi^{-1}$ gefixt. Es gilt:

$$\begin{aligned} F_\sigma(\alpha_i) &= F_\sigma(\pi(\alpha)) = \pi(F_\sigma(\alpha)) = \pi\sigma(\alpha) \text{ (und wegen } \sigma = \pi^{-1}\sigma_j\pi) && (6\text{-}2)\\ &= \pi\pi^{-1}\sigma_j\pi(\alpha) = \sigma_j(\alpha_i) && (6\text{-}3) \end{aligned}$$

Da es für jedes i genau ein $\pi \in \mathrm{Aut}(E/F)$ mit $\pi(\alpha) = \alpha_i$ gibt, folgt aus $F_\sigma(\alpha_i) = \pi\sigma(\alpha)$ die Bijektivität. $\square$

LEMMA 6.17. *$F_\sigma(F_\sigma(\alpha)) = \sigma\sigma(\alpha)$, d.h. F_σ operiert auf den Nullstellen von Δ_1 genauso wie σ.*

Beweis: $F_\sigma(F_\sigma(\alpha)) = F_\sigma(\sigma(\alpha)) = \sigma(F_\sigma(\alpha)) = \sigma\sigma(\alpha)$. $\square$

Die für unser Verfahren wichtigste Eigenschaft von F_σ wird im nächsten Satz gezeigt.

SATZ 6.18. *Für alle $1 \leq j \leq m$ gilt: $F_\sigma(\Delta_j) = \Delta_j$.*

Beweis: Sei $\alpha_i = \pi(\alpha) \in \Delta_j$. Hieraus folgt mit (6-3): $F_\sigma(\alpha_i) = \sigma_j(\alpha_i)$, wobei $\sigma_j(\Delta_j) = \Delta_j$ gilt. Hieraus folgt die Behauptung. $\square$

Der vorangegangene Satz gibt bereits eine gute Charakterisierung der Operation von F_σ auf Ω. Wir wissen, daß F_σ gerade die Nullstellen der Δ_i permutiert. Da die Blockgröße von Δ_i gerade $f_{\mathfrak{P}/\mathfrak{p}}$ ist, haben wir die Anzahl der Möglichkeiten für die Operation von F_σ auf Δ_i auf $(f_{\mathfrak{P}/\mathfrak{p}} - 1)!$ eingeschränkt. Für den Fall, daß $f_{\mathfrak{P}/\mathfrak{p}}$ keine Primzahl ist, erhalten wir mit Hilfe des nächsten Lemmas eine weitere Einschränkung der zu betrachtenden Möglichkeiten.

LEMMA 6.19. *Sei l ein Teiler von $f_{\mathfrak{P}/\mathfrak{p}}$ und $Z_\mathfrak{P} \subseteq K \subseteq E$ der eindeutige Zwischenkörper vom Grad l über $Z_\mathfrak{P}$. Sei $\Gamma_1, \ldots, \Gamma_{lf_{\mathfrak{P}/\mathfrak{p}}}$ das zu K gehörige Blocksystem der Größe $\frac{f_{\mathfrak{P}/\mathfrak{p}}}{l}$. Dann gilt ${F_\sigma}^l(\Gamma_i) = \Gamma_i$ $(1 \leq i \leq lf_{\mathfrak{P}/\mathfrak{p}})$. Hierbei ist ${F_\sigma}^l$ die l-fache Hintereinanderausführung von F_σ.*

Beweis: Sei Γ_i $(1 \leq i \leq lf_{\mathfrak{P}/\mathfrak{p}})$ eine Teilmenge des Blocks Δ_j. Sei σ_j die Konjugierte von σ, welche Δ_j invariant läßt. Da K der Fixkörper zu $\langle\sigma^l\rangle$ ist, wird somit Γ_i von σ_j^l gefixt. Sei nun α_k eine Nullstelle aus Γ_i. Wegen $\sigma_j(\alpha_k) = F_\sigma(\alpha_k)$ erhalten wir $\sigma_j^l(\alpha_k) = {F_\sigma}^l(\alpha_k)$ und damit die Behauptung. $\square$

Die Einschränkung der Anzahl der Möglichkeiten, die wir mit Hilfe dieses Lemmas erhalten, ist bereits für kleine Blockgrößen immens. So müssen wir im Fall $f_{\mathfrak{P}/\mathfrak{p}} = 4$ bzw. $f_{\mathfrak{P}/\mathfrak{p}} = 6$ jeweils nur noch 2 statt 6 bzw. 120 Möglichkeiten betrachten.

Bisher haben wir nur die Operation von F_σ auf einem Block untersucht. Im folgenden werden wir Beziehungen zwischen den Aktionen von F_σ auf verschiedenen Blöcken herleiten. Solche Beziehungen können wir erhalten, wenn zwei Blöcke in demselben Blockverbund liegen, d.h. es existiert ein k mit $\sigma^k(\Delta_i) = \Delta_j$.

LEMMA 6.20. *Sei $\alpha_i \in \Delta_i$ und $\alpha_j \in \Delta_j$ mit $\sigma^k(\alpha_i) = \alpha_j$. Dann gilt $F_\sigma(\alpha_j) = \sigma^k(F_\sigma(\alpha_i))$.*

Beweis: $F_\sigma(\alpha_j) = F_\sigma(\sigma^k(\alpha_i)) = \sigma^k(F_\sigma(\alpha_i))$. □

Wir erinnern uns, daß die Operation von σ auf Ω durch die modulo $\mathfrak{p}$-Faktorisierung des erzeugenden Polynoms gegeben ist. Wir werden die Ergebnisse, die wir in diesem Abschnitt hergeleitet haben, zur Berechnung von Automorphismen in normalen Erweiterungen über $\mathbb{Q}$ benutzen.

5. Absolut-normale Erweiterungen

Wir wollen nun ein Verfahren zur Berechnung von Automorphismen in absolut-normalen Zahlkörpern herleiten. Hierzu sei wieder $F = \mathbb{Q}$. Im Abschnitt über abelsche Erweiterungen haben wir gesehen, daß der Frobeniusautomorphismus zu einem Primideal $\mathfrak{p}$ in $\mathfrak{o}_E$ nur von der Primzahl $p \in \mathfrak{p}$ abhängt. Dadurch waren wir in der Lage, den gesuchten Automorphismus modulo $p\mathfrak{o}_E$ und damit mittels Newton-Lifting auch modulo $p^k\mathfrak{o}_E$ zu bestimmen. Seien

$$\sigma(\alpha) = \frac{1}{d}\sum_{i=0}^{n-1} a_i\alpha^i \text{ mit } a_i \in \mathbb{Z}$$

der gesuchte Frobeniusautomorphismus und

$$\bar{\sigma}(\alpha) = \sum_{i=0}^{n-1} \bar{a}_i\alpha^i \text{ mit } \bar{a}_i \in \mathbb{Z},$$

wobei $\sigma(\alpha) \equiv \bar{\sigma}(\alpha) \bmod p^k\mathfrak{o}_E$ gilt. Wir haben gesehen, daß dies äquivalent zu $\frac{a_i}{d} \equiv \bar{a}_i \bmod p^k$ ist. Falls k groß genug ist, können wir auf sehr einfache Weise $\frac{a_i}{d}$ aus $\bar{a}_i$ rekonstruieren. Diese sehr einfache Rekonstruktion ist für unseren Algorithmus von großer Bedeutung. Im nicht abelschen Fall haben wir das Problem, daß wir den Frobeniusautomorphismus zu einem Primideal $\mathfrak{p}$ in $\mathfrak{o}_E$ nur modulo $\mathfrak{p}^k$ bestimmen können. Hierbei kann k wieder geeignet groß gewählt werden.

Wir bezeichnen mit Z den Zerlegungskörper zu $\mathfrak{p}$ und gehen im folgenden davon aus, daß wir Z und alle Zwischenkörper $Z \subseteq K \subseteq E$ mit ihren Blocksystemen kennen. Das Blocksystem zu Z bezeichnen wir mit $\Delta_1, \dots, \Delta_m$ ($m = n/f_\mathfrak{p}$). Wir leiten nun einige Eigenschaften für die Polynomdarstellung F_σ her, die wir zu deren Berechnung ausnutzen werden.

LEMMA 6.21. *Die Polynomdarstellung F_σ von σ genügt den folgenden Bedingungen. Hierbei sei Φ eine Permutation auf $\{1, \dots, n\}$ für die $F_\sigma(\alpha_i) = \alpha_{\Phi(i)}$ gilt.*

(1) $F_\sigma(\alpha_i) = \sigma(\alpha_i) = \alpha_{\Phi(i)}$ *für alle* $\alpha_i \in \Delta_1$.
(2) $F_\sigma(\alpha_i) = \alpha_{\Phi(i)} \in \Delta_j$ *für alle* $\alpha_i \in \Delta_j$.
(3) *Für* $\sigma(\Delta_i) = \Delta_j$ *und* $\alpha_i \in \Delta_i,\ \alpha_j \in \Delta_j$ *mit* $\sigma(\alpha_i) = \alpha_j$ *gilt:*
$\alpha_{\Phi(j)} = F_\sigma(\alpha_j) = \sigma(F_\sigma(\alpha_i)) = \sigma(\alpha_{\Phi(i)})$.
(4) *Für* K/Z *vom Grad* l *und zugehörigen Blocksystem* $\Gamma_1, \ldots, \Gamma_{lm}$ *gilt:*
${F_\sigma}^l(\alpha_i) = \alpha_{\Phi^l(i)} \in \Gamma_j$ *für* $\alpha_i \in \Gamma_j$.

Beweis: Der Beweis folgt aus den Ergebnissen von Abschnitt 4. □

Wir wissen, daß F_σ auf Ω wie eine Permutation wirkt. Zur Berechnung von F_σ werden wir alle Permutationen durchtesten, die den Bedingungen 1–4 genügen. Die erste Bedingung besagt, daß F_σ auf dem ersten Block wie σ operiert, d.h., daß hier $F_\sigma(\alpha) \equiv \alpha^p \bmod \mathfrak{p}$ gilt. Damit ist die Aktion von F_σ auf dem ersten Block eindeutig bestimmt. Die zweite Bedingung drückt aus, daß $F_\sigma(\Delta_i) = \Delta_i$ $(1 \leq i \leq m)$ gilt. Durch die dritte Bedingung erreichen wir, daß die Aktion von F_σ auf einem Blockverbund durch die Aktion von F_σ auf einem Block des Blockverbunds bestimmt ist. Mit Hilfe der vierten Bedingung können wir die Anzahl der Möglichkeiten, wie F_σ auf einem Block operiert, dadurch einschränken, daß wir wissen, daß ${F_\sigma}^l$ die Blöcke eines Blocksystems von K invariant läßt. Wenn wir Φ kennen, können wir das zugehörige F_σ wie folgt bestimmen:

$$F_\sigma(t) = \sum_{i=1}^{n} \alpha_{\Phi(i)} \frac{\prod\limits_{\substack{j=1\\ j\neq i}}^{n} (t - \alpha_j)}{\prod\limits_{\substack{j=1\\ j\neq i}}^{n} (\alpha_i - \alpha_j)}. \tag{6-4}$$

Unser Verfahren sieht folgendermaßen aus:

(1) Berechne mit Korollar 2.18 eine obere Schranke B für die Zähler und Nenner der a_i und ein minimales $k \in \mathbb{N}$ mit $p^{2^k} > 2B^2$.
(2) Bestimme alle Φ, so daß die zugehörigen F_σ den Bedingungen 1–4 von Lemma 6.21 genügen.
(3) Für jedes dieser Φ tue folgendes:
 (a) Berechne $F_\sigma \in \mathbb{F}_q[t]$ mittels (6-4). (Identifizierung der Nullstellen in $\mathbb{F}_q$).
 (b) Rufe Algorithmus 3.15 (Newton-Lifting) auf.
 (c) Falls ein Ergebnis berechnet wurde, so gebe dies aus und terminiere.

Wir merken ohne Beweis an, daß stets $F_\sigma \in \mathbb{F}_p[t]$ gilt, wenn F_σ bzw. Φ die Eigenschaften 1–4 erfüllen. Die Laufzeit des obigen Verfahrens ist stark davon abhängig, wieviele Möglichkeiten wir testen müssen, bzw. nach wievielen Möglichkeiten wir erfolgreich sind. Bisher können wir ein Φ nur dann ausschließen, wenn wir das zugehörige F_σ modulo p^{2^k} bestimmt haben. Dabei kann p^{2^k} eine sehr große Zahl sein, die wir als nötige Präzision bezeichnen. Wir werden im folgenden einen Pseudo-Test angeben, der es uns ermöglicht, Φ's durch Rechnungen mit deutlich geringerer Präzision auszuschließen.

Der folgende Satz ist eine leichte Variation von Proposition 4.5.1 in [5].

Satz 6.22. *Sei Φ eine Permutation auf $\{1, \ldots, n\}$ und $F_\Phi \in \mathbb{C}[t]$ mit $F_\Phi(\alpha_i) = \alpha_{\Phi(i)}$ $(1 \leq i \leq n)$. F_Φ ist die Polynomdarstellung von einem $\sigma \in \mathrm{Aut}(E)$ genau dann, wenn für $1 \leq j < n$*

$$s_j = \sum_{i=1}^{n} \alpha_{\Phi(i)} \alpha_i^j \in \mathbb{Z}$$

gilt. In diesem Falle gilt $F_\Phi \in \mathbb{Q}[t]$ und $\sigma(\alpha) = F_\Phi(\alpha)$.

Beweis: Sei F_Φ die Polynomdarstellung von einem $\sigma \in \mathrm{Aut}(E)$. Damit folgt dann $F_\Phi \in \mathbb{Q}[t]$. Weiterhin gilt für $1 \leq j < n$:

$$s_j = \sum_{i=1}^{n} \alpha_{\Phi(i)} \alpha_i^j = \sum_{i=1}^{n} F_\Phi(\alpha_i) \alpha_i^j = \mathrm{Tr}(F_\Phi(\alpha)\alpha^j) \in \mathbb{Z}, \tag{6-5}$$

da α ganz ist. Für den Beweis der Rückrichtung, die wir für unser Verfahren nicht benötigen, verweisen wir auf [5]. □

Wir wollen diesen Satz als Pseudo-Test verwenden. Für ein Φ wollen wir feststellen, ob mit j geeignet $s_j \in \mathbb{Z}$ gilt. Um dies zu tun, benötigen wir eine Abschätzung für die Größe der s_j. Diese liefert uns das folgende Lemma.

Lemma 6.23. *Sei $\sigma \in \mathrm{Aut}(E/\mathbb{Q})$ mit korrespondierendem F_Φ. Dann gelten für die s_j aus Satz 6.22 $(1 \leq j < n)$:*

$$|s_j| < n|\alpha|_\infty^{j+1}.$$

Beweis:

$$|s_j| = |\sum_{i=1}^{n} \alpha_{\Phi(i)} \alpha_i^j| \leq \sum_{i=1}^{n} |\alpha|_\infty |\alpha|_\infty^j = n|\alpha|_\infty^{j+1}.$$

□

Diese Abschätzungen sind deutlich kleiner als die Abschätzungen, die wir für die a_i bekommen. Wenn wir den Nenner d durch $\sqrt{|\operatorname{disc}(f)|}$ abschätzen, erhalten wir mit Korollar 2.18 die folgende Abschätzung für die a_i:

$$|a_i| \leq |\alpha|_\infty n(n-1)^{(n-1)/2} |\alpha|_\infty^{n(n-1)/2} := B.$$

Da wir in unserem Verfahren rationale Zahlen rekonstruieren, müssen wir im schlimmsten Fall bis $2B^2$ liften, um zu beweisen, daß F_Φ zu keinem Automorphismus korrespondiert. Wir wollen Satz 6.22 dazu verwenden, um für kleine j (≤ 4) zu testen, ob $s_j \in \mathbb{Z}$ gilt.

ALGORITHMUS 6.24. (Pseudotest(Φ, j))

Input: *Permutation Φ und $j \in \mathbb{N}$.*

Output: *„nicht möglich", falls Φ nicht zu einem Automorphismus korrespondieren kann, ansonsten „möglich".*

Schritt 1: *Berechne $B := n|\alpha|_\infty^{j+1}$ und k mit $p^{2^k} > B^2$.*

Schritt 2: *Approximiere die Nullstellen α_i modulo p^{2^k} mit dem Hensel-Lifting.*

Schritt 3: *Berechne s_j modulo p^{2^k} mit (6-4) und (6-5) ($s_j \in \mathbb{Z}_p$).*

Schritt 4: *Sei nun s_j im symmetrischen Restsystem. Falls $|s_j| < B$ gilt, so gebe „möglich" aus, ansonsten gebe „nicht möglich" aus.*

Schritt 5: *Terminiere.*

Wir können nun einen Algorithmus zur Berechnung des Frobeniusautomorphismus zu einem Primideal $\mathfrak{p}$ angeben.

ALGORITHMUS 6.25. (Berechnung des Frobeniusautomorphismus zu $\mathfrak{p}$)

Input: *Erzeugendes Polynom f einer über $\mathbb{Q}$ normalen Erweiterung $E = \mathbb{Q}(\alpha)$ und ein Ideal $\mathfrak{p}$ von $\mathbb{Z}[\alpha]$ ($p \nmid \operatorname{disc}(f)$).*

Output: *Frobeniusautomorphismus σ.*

Schritt 1: *Berechne mit Korollar 2.18 eine obere Schranke B für d und die Koeffizienten a_i ($0 \leq i \leq n-1$) und ein minimales $k \in \mathbb{N}$ mit $p^{2^k} > 2B^2$.*

Schritt 2: *Bestimme alle Φ, so daß die zugehörigen F_Φ den Bedingungen 1–4 von Lemma 6.21 genügen.*

Schritt 3: *Für jedes dieser Φ tue folgendes:*

(1) *Teste für* $1 \leq j \leq \min(4, n-1)$*, ob Algorithmus* 6.22 *„möglich'" liefert. In diesem Fall führe die nächsten Schritte aus. Ansonsten wähle nächstes* Φ.
(2) *Berechne* $\bar{F}_\Phi \in \mathbb{F}_p[t]$ *mittels* (6-4).
(3) *Berechne mit Algorithmus* 3.15 *(Newton-Lifting)* $F_\Phi(\alpha)$*, wobei* $F_\Phi \in \mathbb{Q}[t]$ *mit* $F_\Phi \equiv \bar{F}_\Phi \bmod p$ *gelte.*
(4) *Falls ein Ergebnis berechnet wurde, so gebe dies aus und terminiere.*

Wir fassen nun die bisherigen Überlegungen und Algorithmen zu einem Algorithmus zusammen. Wir wollen sukzessiv Frobeniusautomorphismen berechnen, um anschließend die von ihnen erzeugte Gruppe zu berechnen. Hierzu müssen wir Primzahlen auswählen, die unverzweigt bleiben und deren Frobeniusautomorphismus noch nicht im bisherigen Erzeugnis enthalten ist. Letzteres testen wir mit Lemma 6.5. Weiterhin können wir das Erzeugnis $\langle H, \sigma \rangle$ mit Hilfe von Algorithmus 6.7 ausrechnen. Wir müssen uns nur noch überlegen, wie wir die Primzahlen p geschickt wählen. Dabei wollen wir versuchen, solche Primzahlen zu wählen, die zu möglichst hohem Trägheitsgrad führen. Diese Wahl hat zwei Vorteile. Einerseits hat damit der Frobeniusautomorphismus einen höheren Grad, und wir erhalten so gleich mehrere Automorphismen in einem Schritt. Der andere Vorteil ist, daß höhere Grade im allgemeinen zu weniger Möglichkeiten bei den möglichen Blocksystemen der Teilkörper und damit auch der Zerlegungskörper führen. Wir hoffen also, daß diese Wahl es uns ermöglicht, die Zerlegungskörper sehr schnell zu berechnen.

Algorithmus 6.26. (Automorphismen von $E = \mathbb{Q}(\alpha)/\mathbb{Q}$ normal)

Input: *Minimalpolynom* $f \in \mathbb{Z}[t]$ *von* α.

Output: *Liste der Automorphismen.*

Schritt 1: *Setze* $T := \{\alpha\}$.

Schritt 2: *Wähle 10 Primzahlen* $p > n$ *mit* $p \nmid \operatorname{disc}(f)$ *und berechne die Trägheitsgrade der zugehörigen Primideale in* $\mathbb{Z}[\alpha]$*. Sortiere diese Primzahlen absteigend bezüglich der berechneten Trägheitsgrade und setze* $P := \{p_1, \dots, p_{10}\}$.

Schritt 3: *Wähle* $p \in P$ *mit größtem Trägheitsgrad und setze* $P := P \setminus \{p\}$*. Falls bereits alle* $p \in P$ *gewählt waren, so wähle zufälliges* $p \in \mathbb{P}$ *mit* $p \nmid \operatorname{disc}(f)$ *und* $p > n$.

Schritt 4: *Setze* `anz` *auf die Anzahl der Primideale, die über* p *liegen.*

Schritt 5: *Für $i = 1, \dots, \texttt{anz}$ tue folgendes:*
(1) *Berechne den Frobeniusautomorphismus $\bar{\sigma}$ von $\mathfrak{p}_i$ modulo $\mathfrak{p}_i$.*
(2) *Teste mit Hilfe von Lemma 6.5, ob $\sigma \in T$ gilt.*
(3) *Berechne mit Algorithmus 6.25 den Frobeniusautomorphismus σ zu $\mathfrak{p}$.*
(4) *Setze $T := \langle T, \sigma \rangle$ mit Algorithmus 6.7.*
(5) *Falls $|T| = \deg(f)$ gilt, so gebe T aus und terminiere.*

Schritt 6: *Gehe zu Schritt 3.*

6. Relativ-abelsche Erweiterungen

In diesem Abschnitt werden wir ein Verfahren zur Berechnung von Automorphismen in relativ-abelschen Erweiterungen herleiten. Die Betrachtung von relativ-abelschen Erweiterungen spielt besonders in der Klassenkörpertheorie eine große Rolle. Wie in den absoluten Fällen werden wir Frobeniusautomorphismen zu geeigneten Primidealen berechnen. Genauso wie im absolut-abelschen Fall haben wir den Vorteil, daß der Frobeniusautomorphismus nur von dem Primideal in dem Grundkörper abhängt. Wenn wir analog zu unseren bisherigen Methoden vorgehen, haben wir ähnlich zum absolut-normalen Fall das Problem, daß wir den Frobeniusautomorphismus σ nicht modulo p^k, sondern nur modulo $\mathfrak{p}^k$ bestimmen können, wobei $\mathfrak{p}$ ein Primideal in $\mathfrak{o}_F$ ist. Wir werden im folgenden einige Eigenschaften von der Operation von σ modulo $\mathfrak{p}_i^k$ herleiten, wenn $\mathfrak{p}_i$ $(1 \leq i \leq r)$ die Primideale in $\mathfrak{o}_F$ sind, die über p liegen. Falls wir σ modulo $\mathfrak{p}_i^k$ für alle $1 \leq i \leq r$ bestimmen können, so erhalten wir mit dem chinesischen Restsatz eine modulo p^k–Approximation von σ. In der Praxis versuchen wir σ modulo $\mathfrak{p}_i$ $(1 \leq i \leq r)$ zu bestimmen, um hiernach mit dem chinesischen Restsatz eine modulo p–Approximation zu erhalten. Diese können wir dann mit dem Newton-Lifting zu einer modulo p^k–Approximation anheben.

Seien im folgenden $F = \mathbb{Q}(\beta)$, $g \in \mathbb{Z}[t]$ vom Grad m das Minimalpolynom von β, sowie $\mathfrak{p}$ ein Primideal von $\mathfrak{o}_F$, welches nicht $\mathfrak{d}(f)$ teilt, und $p \in \mathbb{P} \cap \mathfrak{p}$. Mit der zusätzlichen Forderung, daß $p \nmid \operatorname{disc}(g)$ gelten soll, erhalten wir die folgenden Faktorisierungen:

$$p\mathfrak{o}_F = \mathfrak{p}_1 \cdots \mathfrak{p}_r \text{ mit } \mathfrak{p} := \mathfrak{p}_1,$$
$$\mathfrak{p}_i\mathfrak{o}_F[\alpha] = \mathfrak{P}_{i,1} \cdots \mathfrak{P}_{i,r_i} \text{ für } 1 \leq i \leq r.$$

Wir setzen $\mathfrak{P}_i := \mathfrak{P}_{i,1}$ $(1 \leq i \leq r)$, $\mathfrak{P} := \mathfrak{P}_1$ und bezeichnen mit σ_i $(1 \leq i \leq r)$ den Frobeniusautomorphismus zu $\mathfrak{P}_i/\mathfrak{p}_i$, der nur von $\mathfrak{p}_i$ abhängt. Die Ordnung von σ_i ist dann $f_{\mathfrak{P}_i/\mathfrak{p}_i}$. Wir werden nun untersuchen, wie $\sigma = \sigma_1$ modulo $\mathfrak{p}_i$

$(1 \leq i \leq r)$ operiert. Als ersten Schritt wollen wir die Nullstellen von f modulo $\mathfrak{P}_i$ identifizieren. Dazu müssen wir eine Einbettung von $\mathfrak{o}_F/\mathfrak{p}_i$ in den isomorphen endlichen Körper $\mathbb{F}_q$ finden. Wir haben hierbei die Freiheit, den endlichen Körper $\mathbb{F}_q$ mit einem beliebigen Polynom aus $\mathbb{F}_p[t]$ zu erzeugen. Wir werden im folgenden einen Isomorphismus zwischen $\mathbb{Z}[\beta]/\tilde{\mathfrak{p}}_i$ konstruieren, wobei $\tilde{\mathfrak{p}}_i = \mathbb{Z}[\beta] \cap \tilde{\mathfrak{p}}_i$ gilt. Da $p \nmid \operatorname{disc}(g)$ gilt, kann ein solcher Isomorphismus dann einfach auf $\mathfrak{o}_F/\mathfrak{p}_i$ fortgesetzt werden.

Sei nun $g \equiv g_1 \cdots g_r \bmod p$ und $\tilde{\mathfrak{p}}_i = (p, g_i(\beta))$ für $1 \leq i \leq r$. Falls $f_{\mathfrak{p}_i} > 1$ gilt, erzeugen wir $\mathbb{F}_q/\mathbb{F}_p$ mit einer Nullstelle $\bar{\beta}$ von $\bar{g}_i$, wobei $\bar{g}_i \equiv g_i \bmod p$ gilt.

Satz 6.27. *Die Abbildung $\Phi : (\mathbb{Z}[\beta]/\tilde{\mathfrak{p}}_i) \to \mathbb{F}_q : \beta \mapsto \bar{\beta}$ ist ein Isomorphismus.*

Beweis: Aus $\bar{g}_i(\bar{\beta}) = 0$ folgt $\bar{g}(\beta) = 0$. Daher sehen wir durch Nachrechnen, daß $\bar{\Phi} : \mathbb{Z}[\beta] \to \mathbb{F}_q : \beta \mapsto \bar{\beta}$ ein Homomorphismus ist. Wegen $\bar{\Phi}(p) = 0$ und $\bar{\Phi}(g_i(\beta)) = \bar{g}_i(\bar{\beta}) = 0$ liegen die Elemente von $\tilde{\mathfrak{p}}_i$ im Kern von $\bar{\Phi}$. Sei nun $\bar{\gamma} = \sum_{i=0}^{f_{\mathfrak{p}_i}-1} \bar{c}_i \bar{\beta}^i$ ein Erzeuger der multiplikativen Gruppe von $\mathbb{F}_q$. Dann ist $\gamma = \sum_{i=0}^{f_{\mathfrak{p}_i}-1} c_i \beta^i$ mit $c_i \equiv \bar{c}_i \bmod p$ ein Urbild von $\bar{\gamma}$ und $\bar{\Phi}$ surjektiv. Da $\mathbb{Z}[\beta]/\tilde{\mathfrak{p}}_i$ die Ordnung $p^{f_{\mathfrak{p}_i}}$ hat, folgt damit, daß Φ ein Isomorphismus ist. □

Die Abbildung $\beta \mapsto \bar{\beta}$ ist sehr einfach zu realisieren. Obwohl dieser Satz auch für Primideale ersten Grades gilt, können wir hier einfacher vorgehen.

Lemma 6.28. *Sei $\tilde{\mathfrak{p}}_i = (p, \beta + a)$ ein Primideal ersten Grades. Dann wird durch $\Phi : (\mathbb{Z}[\beta]/\tilde{\mathfrak{p}}_i) \to \mathbb{F}_p : \beta \mapsto -\bar{a}$ ein Isomorphismus definiert.*

Beweis: Nach Satz 6.27 ist $\tilde{\Phi} : (\mathbb{Z}[\beta]/\tilde{\mathfrak{p}}_i) \to \mathbb{F}_p : \beta \mapsto \bar{\beta}$ mit $\bar{\beta}$ Nullstelle von $t + \bar{a}$ ein Isomorphismus. Es folgt $\Phi = \tilde{\Phi}$. □

Wir sind nun in der Lage, die Primidealzerlegung von $\mathfrak{p}_i$ in $\mathfrak{o}_F[\alpha]$ explizit auszurechnen. Da $\mathfrak{p}_i$ kein Diskriminanten- und damit auch kein Indexteiler ist, folgt aus $f \equiv f_1 \cdots f_{r_i} \bmod \mathfrak{p}_i$, daß $\mathfrak{p}_i \mathfrak{o}_F[\alpha] = \mathfrak{P}_{i,1} \cdots \mathfrak{P}_{i,r_i}$ mit $\mathfrak{P}_{i,j} = (\mathfrak{p}_i, f_j(\alpha))$ $(1 \leq j \leq r_i)$ gilt. Dabei permutiert σ_i gerade die Nullstellen von f_i in einem Zykel der Ordnung $f_{\mathfrak{P}_i/\mathfrak{p}_i}$. Da wir nur an der Operation von σ_i auf den Nullstellen interessiert sind, spielt die explizite Darstellung der Primideale $\mathfrak{P}_{i,j}$ für uns keine Rolle. Zur Berechnung dieser Zerlegung benötigen wir nur, daß wir $\mathfrak{o}_F/\mathfrak{p}_i$ in den zugehörigen Restklassenkörper einbetten können. Hierzu liefern uns Satz 6.27 und das nachfolgende Lemma ein Verfahren. Wir können die Nullstellen von f modulo $\mathfrak{p}_i$ identifizieren und kennen die Aktion von σ_i modulo $\mathfrak{p}_i$ auf diesen Nullstellen.

Nach diesen Vorüberlegungen werden wir nun Zusammenhänge zwischen σ und σ_i herleiten. Wir merken an, daß σ und σ_i im allgemeinen nicht zueinander konjugiert sind. Als erstes treffen wir Aussagen über $\langle\sigma\rangle \cap \langle\sigma_i\rangle$.

Lemma 6.29. *Sei* $s = \mathrm{ggT}(f_{\mathfrak{P}/\mathfrak{p}}, r_i)$ *und* $S = \{a \in \mathbb{N} \mid a \mid s \text{ und } f_{\mathfrak{P}/\mathfrak{p}} \mid (af_{\mathfrak{P}_i/\mathfrak{p}_i})\}$. *Dann gibt es ein* $\tilde{s} \in S$ *mit* $\langle\sigma^{\tilde{s}}\rangle \subseteq \langle\sigma_i\rangle$. *Das minimale* $\hat{s}$ *mit* $\langle\sigma^{\hat{s}}\rangle \subseteq \langle\sigma_i\rangle$ *ist in* S *enthalten.*

Beweis: Da σ ein Automorphismus ist, permutiert er die $\mathfrak{P}_{i,j}$, die über $\mathfrak{p}_i$ liegen. Die mögliche Ordnung $\hat{s}$ von σ auf den Primidealen ist sowohl ein Teiler von $f_{\mathfrak{P}/\mathfrak{p}}$ als auch ein Teiler von r_i und damit ein Teiler von s. Weiterhin ist $f_{\mathfrak{P}/\mathfrak{p}}$ die Ordnung von σ, welche somit $(\hat{s}f_{\mathfrak{P}_i/\mathfrak{p}_i})$ teilen muß. Sei nun $\hat{s}$ die tatsächliche Ordnung. Dann gilt $\sigma^{\hat{s}}(\mathfrak{P}_{i,j}) = \mathfrak{P}_{i,j}$ $(1 \leq j \leq r_i)$ und da E/F abelsch ist und $\langle\sigma_i\rangle$ gerade die Automorphismen sind, die $\mathfrak{P}_{i,j}$ invariant lassen, folgt $\langle\sigma^{\hat{s}}\rangle \subseteq \langle\sigma_i\rangle$. Weiterhin ist $\hat{s}$ die kleinste Zahl mit dieser Eigenschaft. □

Wir sind an dem minimalen s mit $\sigma^s \in \langle\sigma_i\rangle$ interessiert. Zur weiteren Betrachtung sortieren wir die Nullstellen von f in der folgenden Weise:

$$\{\alpha_{j,l} \mid 1 \leq j \leq r_i,\ 1 \leq l \leq f_{\mathfrak{P}_i/\mathfrak{p}_i} \text{ und } \sigma_i(\alpha_{j,l}) = \alpha_{j,l+1}\}, \tag{6-6}$$

wobei wir aus Vereinfachungsgründen $\alpha_{j,f_{\mathfrak{P}_i/\mathfrak{p}_i}+1} = \alpha_{j,1}$ setzen.

Für $1 \leq j \leq r_i$ sei $\Delta_j = \{\alpha_{j,l} \mid 1 \leq l \leq f_{\mathfrak{P}_i/\mathfrak{p}_i}\}$. Da E/F abelsch ist, bilden $\Delta_1, \ldots, \Delta_{r_i}$ ein komplettes Blocksystem.

Lemma 6.30. *σ operiert auf den Blöcken Δ_j. Die Ordnung von σ auf den Δ_j entspricht dem minimalen $s \in \mathbb{N}$ von Lemma 6.29, d.h. s ist minimal mit $\sigma^s(\Delta_j) = \Delta_j$ für alle $1 \leq j \leq r_i$.*

Beweis: Da $\Delta_1, \ldots, \Delta_{r_i}$ ein komplettes Blocksystem bilden, operiert jedes $\tau \in G$ auf den Δ_j $(1 \leq j \leq r_i)$. Sei σ_i der Frobeniusautomorphismus zu $\mathfrak{P}_i/\mathfrak{p}_i$. Da E/F abelsch ist, wird jeder Block genau von $\langle\sigma_i\rangle$ gefixt. Da s die kleinste Zahl mit $\sigma^s \in \langle\sigma_i\rangle$ ist, folgt die Behauptung. □

Die beiden vorangegangenen Lemmata liefern uns Einschränkungen für die Operation von möglichen σ auf $\Delta_1, \ldots, \Delta_{r_i}$. Der erste Teil unseres Verfahrens wird darin bestehen, diese Möglichkeiten durchzutesten. Wenn wir die Operation von σ auf den Δ_j kennen, sind wir danach an der genauen Operation von σ auf den Nullstellen interessiert. Wir gehen also im folgenden davon aus, daß die Operation von σ auf den Blöcken bereits bestimmt wurde. Weiter werden wir ausnutzen, daß die Operation von σ_i auf den modulo $\mathfrak{P}_i$ identifizierten Nullstellen ebenfalls bekannt ist.

LEMMA 6.31. *Sei s die kleinste Zahl mit $\sigma^s(\Delta_j) = \Delta_j$. Dann existiert für alle $1 \leq l \leq f_{\mathfrak{P}_i/\mathfrak{p}_i}$ ein ν, so daß für alle $1 \leq j \leq r_i$ gilt: $\sigma^s(\alpha_{j,l}) = \alpha_{j,\nu}$.*

Beweis: Da $\sigma^s \in \langle\sigma_i\rangle$ gilt, existiert ein s_0 mit $\sigma^s = \sigma_i^{s_0}$. Sei ein $l \in \{1, \dots, f_{\mathfrak{P}_i/\mathfrak{p}_i}\}$ beliebig fixiert. Dann existiert wegen (6-6) ein ν, sodaß für alle $1 \leq j \leq r_i$ folgendes gilt: $\sigma^s(\alpha_{j,l}) = \sigma_i^{s_0}(\alpha_{j,l}) = \alpha_{j,\nu}$. □

Da σ der Frobeniusautomorphismus zu $\mathfrak{P}/\mathfrak{p}$ ist, hat er Ordnung $f_{\mathfrak{P}/\mathfrak{p}}$. Um die Operation von σ modulo $\mathfrak{p}_i$ zu bestimmen, ist es notwendig, die Operation von σ auf den modulo $\mathfrak{p}_i$ bestimmten Nullstellen von f zu bestimmen. Zur Konstruktion ist noch das folgende Lemma sehr nützlich.

LEMMA 6.32. *Sei F_σ die Polynomdarstellung zu σ. Dann gilt für eine beliebige Nullstelle α_i von f: $F_\sigma(\alpha_i) = \sigma(\alpha_i)$.*

Beweis: Nach (6-3) gilt $F_\sigma(\alpha_i) = \sigma_j(\alpha_i)$ für ein zu σ konjugiertes σ_j. Da E/F abelsch ist, folgt $\sigma = \sigma_j$ und damit die Behauptung. □

Wenn wir also modulo $\mathfrak{p}_i$ das Bild der Nullstellen kennen, können wir analog zum vorherigen Abschnitt die Polynomdarstellung F_σ von σ modulo $\mathfrak{p}_i$ bestimmen. Diese können wir für alle $1 \leq i \leq r$ berechnen und mit dem chinesischen Restsatz zusammensetzen. Wir erhalten so alle „modulo p Kandidaten“ für unseren Automorphismus σ. Um die Anzahl der Möglichkeiten weiter zu reduzieren, wollen wir analog zu Satz 6.22 einen Pseudo-Test entwickeln.

SATZ 6.33. *Sei Φ eine Permutation auf $\{1, \dots, n\}$ und $F_\Phi \in \mathbb{C}[t]$ mit $F_\Phi(\alpha_i) = \alpha_{\Phi(i)}$ $(1 \leq i \leq n)$. Dann ist F_Φ die Polynomdarstellung von einem $\sigma \in \mathrm{Aut}(E/F)$ genau dann, wenn für $1 \leq j < n$*

$$s_j = \sum_{i=1}^{n} \alpha_{\Phi(i)}\alpha_i^j \in \mathfrak{o}_F$$

gilt. In diesem Falle gilt $F_\Phi \in F[t]$ und $\sigma(\alpha) = F_\Phi(\alpha)$.

Beweis: Der Beweis verläuft analog zu dem von Satz 6.22. □

In dieser Form ist dieser Satz nicht so nützlich wie in der absoluten Form, da wir modulo p^k nicht entscheiden können, ob $s_j \in \mathfrak{o}_F$ gilt. Daher werden wir die Spur der s_j betrachten und erhalten die folgende Abschätzung. Wir bezeichen mit $\cdot^{(\nu)}$ $(1 \leq \nu \leq m)$ die ν-te Konjugation von F und setzen die Konjugation auf $F[t]$ fort.

Lemma 6.34. *Seien die* $s_j \in \mathfrak{o}_F$ $(1 \leq j < n)$ *wie in Satz* 6.33 *definiert. Dann gelten* $\mathrm{Tr}(s_j) \in \mathbb{Z}$ $(1 \leq j < n)$ *und*

$$|\,\mathrm{Tr}(s_j)| \leq \sum_{\nu=1}^{m} n|f^{(\nu)}|_\infty^{j+1} \leq mn|f|_\infty^{j+1},$$

wobei $|f^{(\nu)}|_\infty$ *der Betrag der größten Nullstelle von* $f^{(\nu)}$ *und* $|f|_\infty = \max\limits_{1\leq\nu\leq m} |f^{(\nu)}|_\infty$ *ist.*

Beweis:

$$|\,\mathrm{Tr}(s_j)| \leq \sum_{\nu=1}^{m} |s_j^{(\nu)}| \leq \sum_{\nu=1}^{m} n|f^{(\nu)}|_\infty^{j+1} \leq mn|f|_\infty^{j+1}.$$

□

Zur Anwendung dieses Lemmas benötigen wir eine Methode, $\mathrm{Tr}(s_j) \bmod p^k$ zu berechnen.

Lemma 6.35. *Für* $\gamma, \delta \in \mathfrak{o}_F$ *mit* $\gamma \equiv \delta \bmod p^k$ *gilt* $\mathrm{Tr}(\gamma) \equiv \mathrm{Tr}(\delta) \bmod p^k$.

Beweis: Es gilt $\gamma \equiv \delta \bmod p^k$ genau dann, wenn $\gamma - \delta \equiv 0 \bmod p^k$ gilt. Mit $\omega = \gamma - \delta$ reicht es zu zeigen, daß $\mathrm{Tr}(\omega) \equiv 0 \bmod p^k$ gilt. Wegen $\omega \equiv 0 \bmod p^k$ folgt $\tilde{\omega} = \frac{\omega}{p^k} \in \mathfrak{o}_F$, daher erhalten wir $\mathrm{Tr}(\omega) = p^k\,\mathrm{Tr}(\tilde{\omega}) \equiv 0 \bmod p^k$. □

Wir können nun unseren Algorithmus formulieren. Ähnlich zum absolut-normalen Fall werden wir ihn in mehrere Teile aufteilen.

Algorithmus 6.36. (Pseudotest(γ, j))

Input: $\gamma \in \mathfrak{o}_F[\alpha]$ *(mit* $f(\gamma) \equiv 0 \bmod p$*)*, $j \in \mathbb{N}$

Output: *„nicht möglich“, falls* γ *modulo* p *nicht das Bild von* σ *sein kann, ansonsten „möglich“*

Schritt 1: *Berechne mit Lemma* 6.34 *eine obere Schranke* B *für* s_j *und ein* k *mit* $p^{2^k} > B^2$.

Schritt 2: *Berechne mit dem Newton-Lifting* 3.14 *ein* γ_k *mit* $f(\gamma_k) \equiv 0 \bmod p^{2^k}$.

Schritt 3: *Berechne* $s_j \equiv \mathrm{Tr}_{E/\mathbb{Q}}(\alpha^j \gamma_k) \bmod p^{2^k}$.

Schritt 4: *Sei nun* s_j *im symmetrischen Restsystem. Falls* $|s_j| < B$ *gilt, so gebe „möglich“ aus, ansonsten gebe „nicht möglich“ aus.*

Schritt 5: *Terminiere.*

In Schritt 3 berechnen wir s_j von Lemma 6.33 mit Hilfe der Spur, welches aufgrund des Beweises des Lemmas äquivalent ist. Weiterhin gilt $\mathrm{Tr}_{F/\mathbb{Q}}(\mathrm{Tr}_{E/F}(\alpha^j\gamma_k)) = \mathrm{Tr}_{E/\mathbb{Q}}(\alpha^j\gamma_k)$. Aus $x \equiv \alpha^j\gamma_k$ modulo p^{2^k} folgt $\mathrm{Tr}_{E/\mathbb{Q}}(x) \equiv \mathrm{Tr}_{E/\mathbb{Q}}(\alpha^j\gamma_k) \bmod p^{2^k}$.

ALGORITHMUS 6.37. (Berechnung aller möglichen Bilder von $\sigma(\alpha) \bmod \mathfrak{p}_i$.)

Input: *$E = F[\alpha]/F$ abelsch, Minimalpolynom $f \in \mathfrak{o}_F[t]$ von α und $\mathfrak{p}, \mathfrak{p}_i$ Primideale in $\mathfrak{o}_F$ über demselben $p \in \mathbb{P}$.*

Output: *Eine Menge S_i, welche alle möglichen Bilder von $\sigma(\alpha) \bmod \mathfrak{p}_i$ enthält.*

Schritt 1: *Berechne mit Satz 6.27 sowohl den Restklassenkörper $\mathbb{F}_q$ zu $\mathfrak{o}_F[\alpha]/\mathfrak{p}_i$ als auch den Isomorphismus zwischen $\mathfrak{o}_F[\alpha]/\mathfrak{p}_i$ und $\mathbb{F}_q$.*

Schritt 2: *Faktorisiere $f \equiv f_1 \cdots f_{r_i} \bmod \mathfrak{p}_i$ in über $\mathbb{F}_q[t]$ irreduzible Polynome vom Grad $f_{\mathfrak{P}_i/\mathfrak{p}_i}$.*

Schritt 3: *Für $1 \le j \le r_i$ setze $\Delta_j := \{\alpha_{j,1}, \dots, \alpha_{j,r_i}\}$, die Menge der Nullstellen von f_j in einer passenden Erweiterung $\mathbb{F}_{\tilde{q}}/\mathbb{F}_q$, sortiert mit dem zugehörigen Frobeniusautomorphismus σ_i (vgl. (6-6)).*

Schritt 4: *Berechne $s := \mathrm{ggT}(f_{\mathfrak{P}/\mathfrak{p}}, r_i)$ und $S := \{a \in \mathbb{N} \mid a \mid s \text{ und } f_{\mathfrak{P}/\mathfrak{p}} \mid (a f_{\mathfrak{P}_i/\mathfrak{p}_i})\}$.*

Schritt 5: *Setze $T := \emptyset$ und für $s \in S$ tue folgendes:*
- (1) *Berechne alle Permutationen Φ auf $\{\Delta_1, \dots, \Delta_{r_i}\}$ mit der Eigenschaft, daß Φ^s die Identität ist und für alle $1 \le a < s$, $1 \le j \le r_i$ stets $\Phi^a(\Delta_j) \ne \Delta_j$ gilt.*
- (2) *Für jedes dieser Φ tue folgendes:*
  - (a) *Bestimme alle Permutationen τ mit:*
    $\tau(\Delta_j) = \Phi(\Delta_j)$ $(1 \le j \le r_i)$,
    $\tau^s(\alpha_{j,l}) = \alpha_{j,\nu}$ (Lemma 6.31).
  - (b) *Füge jedes τ zu T hinzu.*

Schritt 6: *Für jedes $\tau \in T$ tue folgendes:*
- (1) *Berechne mittels (6-4) ein Polynom $\bar{F_\sigma}(t) \in \mathbb{F}_{\tilde{q}}[t]$ mit $\bar{F_\sigma}(\alpha_{j,l}) = \tau(\alpha_{j,l})$ $(1 \le j \le r_i, 1 \le l \le f_{\mathfrak{P}_i/\mathfrak{p}_i})$.*
- (2) *Falls $\bar{F_\sigma} \in \mathbb{F}_q[t]$ gilt, so berechne $F_\sigma \in \mathfrak{o}_F[t]$ mit $F_\sigma \equiv \bar{F_\sigma} \bmod \mathfrak{p}_i$ und setze $S_i = S_i \cup \{F(\alpha)\}$.*

ALGORITHMUS 6.38. (Berechnung des Frobeniusautomorphismus zu $\mathfrak{P}/\mathfrak{p}$)

Input: *Relativ-abelsche Erweiterung $E = F(\alpha)/F$ gegeben durch das Minimalpolynom $f \in \mathfrak{o}_F[t]$, Primideal $\mathfrak{p}$ von $\mathfrak{o}_F$ mit $\mathfrak{p} \nmid \mathfrak{d}(f)$.*

Output: *Der Frobeniusautomorphismus zu* $\mathfrak{P}/\mathfrak{p}$

Schritt 1: *Berechne eine obere Schranke* B *für die Koeffizienten der Polynomdarstellung von* σ *und ein minimales* $k \in \mathbb{N}$ *mit* $p^{2^k} > 2B^2$.

Schritt 2: *Bestimme die konjugierten Primideale* $\mathfrak{p}_2, \dots, \mathfrak{p}_r$ *von* $\mathfrak{p}$ *in* $\mathfrak{o}_F$.

Schritt 3: *Setze* $S_1 := \{\alpha^{p^{f_\mathfrak{p}}} \bmod \mathfrak{p}\}$ *und berechne mit Algorithmus* 6.37 *für* $2 \leq i \leq r$ *alle möglichen Bilder von* $\sigma(\alpha) \bmod \mathfrak{p}_i$ *und speichere sie in* S_i.

Schritt 4: *Setze* $M := \{(s_1, \dots, s_r) \mid s_i \in S_i \ (1 \leq i \leq r)\}$.

Schritt 5: *Für jedes* $s = (s_1, \dots, s_r) \in M$ *tue folgendes:*

(1) *Berechne mit dem chinesischem Restsatz* $\gamma \in \mathfrak{o}_F[\alpha]$ *mit* $\gamma \equiv s_i \bmod \mathfrak{p}_i\mathfrak{o}_F[\alpha] \ (1 \leq i \leq r)$.

(2) *Teste für* $1 \leq j \leq \min(4, n-1)$, *ob Algorithmus* 6.36 *„möglich“ liefert. In diesem Fall führe die nächsten Schritte aus, ansonsten wähle nächstes* $s \in M$.

(3) *Berechne mit dem Newton-Lifting (Algorithmus* 3.15*) den möglichen Frobeniusautomorphismus. Falls er berechnet wurde, so gebe ihn aus und terminiere.*

Nun können wir den Hauptalgorithmus formulieren.

Algorithmus 6.39. (Automorphismen von $E = F(\alpha)/F$ abelsch)

Input: *Minimalpolynom* $f \in \mathfrak{o}_F[t]$ *von* α.

Output: *Liste der Automorphismen.*

Schritt 1: *Setze* $T := \{\alpha\}$.

Schritt 2: *Wähle nächstes* $\mathfrak{p} \in \mathbb{P}_F$ *mit* $\mathfrak{p} \nmid \mathfrak{d}(f)$ *und* p *teilt nicht die Diskriminante des erzeugenden Polynoms für* F.

Schritt 3: *Berechne den Frobeniusautomorphismus* $\bar{\sigma}$ *von* $\mathfrak{P}/\mathfrak{p}$ *modulo* $\mathfrak{p}$.

Schritt 4: *Teste mit Hilfe von Lemma* 6.5, *ob* $\sigma \in T$ *gilt.*

Schritt 5: *Berechne mit Algorithmus* 6.38 *den Frobeniusautomorphismus* σ *zu* $\mathfrak{P}/\mathfrak{p}$.

Schritt 6: *Setze* $T := \langle T, \sigma \rangle$ *mit Algorithmus* 6.7.

Schritt 7: *Falls* $|T| = \deg(f)$ *gilt, so gebe* T *aus und terminiere.*

Schritt 8: *Gehe zu Schritt 2.*

Im Schritt 6 von Algorithmus 6.39 können wir ausnutzen, daß E/F abelsch ist. Ein für die Laufzeit nicht unerhebliches Problem ist die geeignete Wahl des Primideals $\mathfrak{p}$ in Schritt 2. Eine optimale Wahl wäre ein Primideal $\mathfrak{p}$, welches träge über p ist und $\mathfrak{P}/\mathfrak{p}$ möglichst hohen Trägheitsgrad hat. Die erste Bedingung führt dazu, daß es nur eine Möglichkeit für den Frobeniusautomorphismus gibt. Durch den hohen Trägheitsgrad erreichen wir, daß wir mit der Berechnung eines Frobeniusautomorphismus eine möglichst große Untergruppe bestimmen können. Oft wird es aber so sein, daß wir keine trägen Primideale in $\mathfrak{o}_F$ finden können, bzw. alle trägen Primideale zur Berechnung der Identität führen. Hier müssen wir dann probieren, Primideale mit möglichst wenigen Konjugierten zu finden.

KAPITEL VII

Beispiele

In diesem Kapitel präsentieren wir Beispiele, die die Leistungsfähigkeit unserer Algorithmen unterstreichen. Die Algorithmen wurden in dem Computeralgebrasystem KASH [7] implementiert. Die gemessenen Laufzeiten wurden auf einer HP 9000/735 unter HP-UX 9.05 ermittelt.

1. Teilkörper

Wir starten mit unserem Teilkörperalgorithmus und vergleichen die Laufzeiten mit denen in [16, 18]. Diese unterstreichen auch die Entwicklung, die der Teilkörperalgorithmus genommen hat. Andere Verfahren [15, 3, 24] wurden bereits in [18] bzw. [15] verglichen. Dabei stellte sich heraus, daß die Methoden in [18] deutlich überlegen waren.

r_1	Anzahl Körper	Anzahl Teilkörper	Gesamtlaufzeit		Durchschnittslaufzeit	
			alt	neu	alt	neu
1	485	486	36:43 min	120 sek	4,5 sek	0,25 sek
3	423	446	31:25 min	88 sek	4,5 sek	0,21 sek
5	154	154	9:38 min	31 sek	3,8 sek	0,20 sek
7	23	23	1:30 min	5,7 sek	3,9 sek	0,25 sek
9	27	31	1:39 min	7,2 sek	3,7 sek	0,27 sek

Als erstes vergleichen wir unseren Algorithmus mit dem in der Diplomarbeit des Autors [16] entwickelten Verfahren. Dort wurden die Teilkörper von 1112 imprimitiven Körpern 9. Grades berechnet. Diese Körper sind einer Tabelle von [9] entnommen worden. Explizite Beispiele sind in [16] angegeben worden. Wir listen hier nur die Laufzeiten auf. Hierbei bezeichnet r_1 die Anzahl der reellen

Nullstellen.

Als „größeres" Beispiel wurden in [16] die Teilkörper von einem Körper E mit $\mathrm{Gal}(E/\mathbb{Q}) = \mathfrak{A}_4$ berechnet. Dieser Körper wird von einer Nullstelle von

$$t^{12}+t^{11}-28t^{10}-40t^9+180t^8+426t^7+89t^6-444t^5-390t^4-75t^3+27t^2+11t+1$$

erzeugt. Der Körper besitzt 8 nicht triviale Teilkörper und die Laufzeit wurde von 6:46 min auf 2,5 sek verbessert. Dieses Beispiel wurde auch in [18] verwendet. Hier betrug die Laufzeit 11 sek.

Die folgende Beispieltabelle wurde von A. Hulpke in [15] zusammengestellt. Hier werden die Laufzeiten von verschiedenen Teilkörperalgorithmen verglichen. Wir vergleichen hier nur die Laufzeiten von [18] (alt) mit denen in dieser Arbeit präsentierten Methoden (neu). Wie bereits oben gesagt wurde, sind die Laufzeiten anderer Teilkörperalgorithmen deutlich schlechter als die des in [18] dargestellen Verfahrens. Hierbei bildet Beispiel 6 eine Ausnahme, da hier 3 sek zur Erzeugung des endlichen Körpers mit 13^5 Elementen benötigt werden. Dabei werden Tabellen erstellt, um schnell zwischen additiven und multiplikativen Darstellungen umrechnen zu können. Bei einer anderen Wahl der Primzahl würde diese Laufzeit deutlich niedriger sein.

Nr	Polynom	Zeit alt	Zeit neu
1	t^6+108	1,1 sek	0,2 sek
2	$t^8-12t^6+23t^4-12t^2+1$	4,0 sek	0,6 sek
3	t^8-10t^4+1	1,5 sek	0,4 sek
4	$t^8+4t^6+10t^4+12t^2+7$	1,8 sek	0,4 sek
5	$t^9-18t^8+117t^7-348t^6+396t^5+288t^4+3012t^3+576t^2+576t-512$	3,3 sek	0,7 sek
6	$t^{10}+38t^9-99t^8+1334t^7-4272t^6+9244t^5-8297t^4+1222t^3+1023t^2-74t+1$	3,4 sek	3,5 sek
7	$t^{10}-20t^9+80t^8+200t^7-3770t^6+872t^5+29080t^4+36280t^3-456615t^2+541260t-517448$	3,9 sek	1,9 sek
8	$t^{10}-10t^8+20t^7+235t^6+606t^5+800t^4+600t^3+270t^2+70t+16$	3,2 sek	0,7 sek
9	$t^{12}+6t^9+4t^8+8t^6-4t^5-12t^4+8t^3-8t+8$	7,4 sek	0,8 sek
10	$t^{12}+9t^{11}+3t^{10}-73t^9-177t^8-267t^7-315t^6-267t^5-177t^4-73t^3+3t^2+9t+1$	14 sek	9,7 sek
11	siehe unten	98 sek	15 sek
12	$t^{15}+20t^{12}+125t^{11}+503t^{10}+1650t^9+3430t^8+4690t^7+4335t^6+2904t^5+1400t^4+485t^3+100t^2+15t+1$	10 sek	8,6 sek

Das 11. Polynom in der obigen Tabelle hat die folgende Form:

$$t^{12} - 34734t^{11} + 401000259t^{10} - 14566274928 85t^9 - 2537142937228035t^8 + 18762072755679375516t^7 - 812368636358864062944t^6 - 70132863629758257512231931t^5 + 25834472514893102332821062085t^4 + 766232806103524502472479395847 45t^3 - 4508088501542266213251576349975845 0t^2 - 207049955224081221428831698107181 8900t - 550505759097778545485364826246753544$$

Wir merken an, daß dieses Polynom genauso wie

$$t^{12} + t^{11} - 28t^{10} - 40t^9 + 180t^8 + 426t^7 + 89t^6 - 444t^5 - 390t^4 - 75t^3 + 27t^2 + 11t + 1$$

Galoisgruppe $\mathfrak{A}_4$ hat. Der Laufzeitunterschied ergibt sich daher nur aus der Größe der Koeffizienten.

Ein weiteres Beispiel, welches in [18] berechnet wurde, ist ein Körper $E/\mathbb{Q}$ vom Grad 24 mit Galoisgruppe $\mathfrak{S}_4$. Der Körper wird von einer Nullstelle des folgenden Polynoms erzeugt:

$f(t) = t^{24} + 8t^{23} - 32t^{22} - 298t^{21} + 624t^{20} + 4592t^{19} - 8845t^{18} - 31488t^{17} + 76813t^{16} + 65924t^{15} - 265616t^{14} + 48348t^{13} + 385639t^{12} - 394984t^{11} - 20946t^{10} + 369102t^9 - 362877t^8 + 183396t^7 + 434501t^6 - 194418t^5 + 450637t^4 + 125800t^3 - 16401t^2 - 45880t + 115151.$

Eine Liste der erzeugenden Polynome für die Teilkörper findet sich in [18]. Die Laufzeit betrug dort 3641 sek. Wir sind nun in der Lage, alle Teilkörper in 105 sek zu berechnen. Wir merken an, daß dieses Beispiel bereits mit den Methoden von [16] getestet wurde und damals 3 Tage Rechenzeit benötigte.

Als nächstes betrachten wir ein Beispiel, welches den Teilkörperalgorithmus vor große kombinatorische Probleme stellt. Der folgende Körper E vom Grad 60 wurde als Zerfällungskörper eines Körpers vom Grad 5 mit Galoisgruppe $\mathfrak{A}_5$ berechnet. Das Problem liegt hierbei weniger in Grad und Größe der Koeffizienten, sondern in den Zykeltypen, die bei der modulo p-Faktorisierung auftreten. So treten nur folgende Faktorisierungen auf:

(1) 60 Faktoren vom Grad 1,
(2) 30 Faktoren vom Grad 2,
(3) 20 Faktoren vom Grad 3,
(4) 12 Faktoren vom Grad 5.

Es gibt keine Teilkörper vom Grad 2,3 und 4, welches relativ schnell festgestellt werden kann. Wenn wir eine Primzahl wählen, die zu 12 Faktoren vom Grad 5 korrespondiert, so müssen wir 5^{11} mögliche Blocksysteme betrachten, um die

Teilkörper vom Grad 5 zu berechnen. Dies ist wahrscheinlich innerhalb eines halben Jahres Rechenzeit nicht zu bewältigen. Wir können dieses Beispiel aber trotzdem rechnen, wenn wir die Teilkörper abspeichern, die wir während der Zerfällungskörperberechnung erhalten. Die so erhaltenen Blocksysteme können wir dann zum Schneiden (vgl. Algorithmus 4.20) benutzen, was die Anzahl der Möglichkeiten drastisch reduziert. Der Zerfällungskörper wurde auf die folgende Weise berechnet: Wir sind mit dem Körper gestartet, der von einer Nullstelle von $t^5 + t^4 - 2t^3 + t^2 + t + 1$ erzeugt wird. Als nächstes haben wir dieses Polynom über dem von ihm erzeugten Zahlkörper faktorisiert und einen Faktor vom Grad 4 erhalten, mit dem wir eine Körpererweiterung vom Gesamtgrad 20 erzeugt haben. Für dieses Polynom haben wir dann mit der OrderShort–Funktion in KASH [7] eine kürzere Darstellung gefunden:

$$t^{20} + 8t^{19} + 13t^{18} - 47t^{17} - 136t^{16} - 23t^{15} + 451t^{14} + 761t^{13} + 640t^{12} - 9t^{11} - 390t^{10} - 648t^9 - 396t^8 - 684t^7 + 36t^6 + 162t^5 + 270t^4 - 243t^3 + 405t^2 - 81t + 81.$$

Das Polynom vom Grad 4 hat dann im Zahlkörper vom Grad 20 einen irreduziblen Faktor vom Grad 3, mit dem wir schließlich die Erweiterung vom Grad 60 erhalten haben. Da es bei den oben beschriebenen Verfahren möglich ist, die Einbettungen mitzuberechnen, können wir die Kenntnis der beiden Teilkörper vom Grad 5 bzw. Grad 20 ausnutzen. Unser Körper E wird von einer Nullstelle des folgenden Polynoms erzeugt:

$$t^{60} + 36t^{59} + 579t^{58} + 5379t^{57} + 30720t^{56} + 100695t^{55} + 98167t^{54} - 611235t^{53} - 2499942t^{52} - 1083381t^{51} + 15524106t^{50} + 36302361t^{49} - 22772747t^{48} - 205016994t^{47} - 194408478t^{46} + 417482280t^{45} + 954044226t^{44} + 281620485t^{43} - 366211766t^{42} - 1033459767t^{41} - 8746987110t^{40} - 15534020046t^{39} + 23906439759t^{38} + 104232578583t^{37} + 31342660390t^{36} - 364771340802t^{35} - 547716092637t^{34} + 583582152900t^{33} + 2306558029146t^{32} + 998482693677t^{31} - 3932078004617t^{30} - 5195646620046t^{29} + 2421428069304t^{28} + 10559164336236t^{27} + 3475972372302t^{26} - 22874708335419t^{25} - 33428241525914t^{24} + 21431451023271t^{23} + 90595197659892t^{22} + 50882107959528t^{21} - 67090205528313t^{20} - 117796269461541t^{19} - 74369954660792t^{18} + 25377774560496t^{17} + 126851217660123t^{16} + 104232393296166t^{15} - 29072256729168t^{14} - 83163550972215t^{13} - 24296640395870t^{12} + 14633584964262t^{11} + 8865283658688t^{10} + 5364852154893t^9 - 1565702171883t^8 - 7601782249737t^7 - 2106132289551t^6 + 3369356619543t^5 + 3717661159674t^4 + 1754791133184t^3 + 573470363592t^2 + 74954438640t + 3285118944$$

Aus Platzgründen verzichten wir darauf, die erzeugenden Polynome und die Einbettungen für die Teilkörper anzugeben. Wir geben aber in der folgenden Tabelle eine Statistik über die Laufzeit und die Anzahl der Teilkörper an.

Die Laufzeit für die Teilkörper wächst im allgemeinen mit dem Grad der Teilkörper, da hier das Berechnen der Einbettungen aufwendiger wird. Der Grad 5 bildet eine Ausnahme, da hier erst wenige Teilkörper bekannt waren und dementsprechend erheblich mehr Möglichkeiten für die Blocksysteme durchgetestet werden mußten. Die Berechnung des Körpers E selber hat ungefähr eine Stunde benötigt.

Grad	Anzahl Teilkörper	Laufzeit Gesamt	Laufzeit Einbettung
2	0	21 sek	
3	0	61 sek	
4	0	142 sek	
5	5	2339 sek	610 sek
6	6	1415 sek	859 sek
10	10	2476 sek	2383 sek
12	6	4211 sek	1696 sek
15	5	2459 sek	1790 sek
20	10	6831 sek	4743 sek
30	15	12516 sek	10827 sek
Gesamt	67	$\approx$ 9 h	$\approx$ 6 h 22 min

2. Dekompositionen

Wir betrachten das Beispiel $f(t) = t^{12}+9t^{11}+3t^{10}-73t^9-177t^8-267t^7-315t^6-267t^5-177t^4-73t^3+3t^2+9t+1$ aus [24]. Wir berechnen drei inäquivalente Normdekompositionen ohne irgendwelche zusätzlichen Informationen auszunutzen.

Nach 16 Sekunden erhalten wir die folgenden drei Normdekompositionen der Form $N_{N_g(h_1)}(h_2)$ in einer absoluten Darstellung (bzw. einer relativen Darstellung).

g	t^3+4t^2+3t-1
h_1	$t^2+(-1-3\beta-\beta^2)t+\beta$
h_2	$t^2+(-4\gamma+7\gamma^2+5\gamma^3-2\gamma^4-\gamma^5)t+1$
h_2	$t^2+((-1-\beta)+(5+2\beta)\gamma)t+1$
g	t^2-5t+1
h_1	$t^3+(-3+\beta)t^2+(2-\beta)t-\beta$
h_2	$t^2+(-4\gamma+7\gamma^2+5\gamma^3-2\gamma^4-\gamma^5)t+1$
h_2	$t^2+((-2+3\beta)+(7-\beta)\gamma-3\gamma^2)t+1$
g	t^2-3t-3
h_1	$t^2+(-2+\beta)t+1$
h_2	$t^3+(6+5\gamma-\gamma^2-\gamma^3)t^2+(1+\gamma-2\gamma^2)t-1$
h_2	$t^3+((9-\beta)+(-3+2\beta)\gamma)t^2+(3+(-3+2\beta)\gamma)t-1$

Sei $f(t) = t^8 - 8t^7 + 1448t^6 - 8576t^5 - 203394t^4 + 870600t^3 + 3596804t^2 - 8957592t + 4818366$. Wir benötigten 6,3 sek für die folgenden fünf inäquivalenten Normdekompositionen.

g	$t^2 - 2$
h_1	$t^2 + \beta$
h_2	$t^2 + (-2 - 19\gamma + 10\gamma^3)t + (-24 + 19\gamma - 22\gamma^2 - 10\gamma^3)$
h_2	$t^2 + (-2 + (-19 - 10\beta)\gamma)t + ((-24 + 22\beta) + (19 + 10\beta)\gamma)$
g	$t^2 - 2$
h_1	$t^2 + 11\beta$
h_2	$t^2 + (\frac{1}{11}(-22 + 33\gamma - 5\gamma^3))t + (\frac{1}{11}(286 - 33\gamma + 22\gamma^2 + 5\gamma^3))$
h_2	$t^2 + (-2 + (3 + 5\beta)\gamma)t + ((26 - 22\beta) + (-3 - 5\beta)\gamma)$
g	$t^2 + 8t + 14$
h_1	$t^2 + (4 + \beta)t - 5$
h_2	$t^2 - 2t + (\frac{1}{5}(-1970 + 783\gamma + 625\gamma^2 - 224\gamma^3))$
h_2	$t^2 - 2t + ((1127 + 224\beta) + (-657 - 125\beta)\gamma)$
g	$t^2 + 12t + 25$
h_1	$t^2 + \beta$
h_2	$t^2 - 2t + (\frac{1}{5}(-1970 + 783\gamma + 625\gamma^2 - 224\gamma^3))$
h_2	$t^2 - 2t + (\frac{1}{5}((-1970 - 625\beta) + (783 + 224\beta)\gamma))$
g	$t^2 - 12t + 14$
h_1	$t^2 + (-6 + \beta)t + 5$
h_2	$t^2 - 2t + (\frac{1}{5}(-1970 + 783\gamma + 625\gamma^2 - 224\gamma^3))$
h_2	$t^2 - 2t + ((325 - 224\beta) + (145 - 125\beta)\gamma)$

Nun ist es einfach, f mittels Radikalerweiterungen aufzulösen. Wir benutzen die letzte Dekomposition und erhalten:

$$\beta_{1,2} = 6 + \epsilon_1\sqrt{22} \text{ mit } \epsilon_1 = \pm 1.$$

$$\gamma_{j_1,j_2} = 3 - \frac{\beta - \epsilon_2\sqrt{2}}{2} \text{ mit } \epsilon_2 = \pm 1, \text{ also}$$

$$\gamma_{1,2,3,4} = \frac{-\epsilon_1\sqrt{22} + \epsilon_2\sqrt{2}}{2}$$

$$\text{mit } \epsilon_1 = \pm 1, \epsilon_2 = \pm 1.$$

$$\alpha_{k_1,k_2} = 1 + \epsilon_3\sqrt{-324 + 224\beta - 145\gamma + 125\beta\gamma} \text{ mit } \epsilon_3 = \pm 1, \text{ also}$$

$$\alpha_{1,2,3,4,5,6,7,8} =$$

$$1 + \epsilon_3\sqrt{-324+224(6+\epsilon_1\sqrt{22})-145(\tfrac{-\epsilon_1\sqrt{22}+\epsilon_2\sqrt{2}}{2})+125(6+\epsilon_1\sqrt{22})(\tfrac{-\epsilon_1\sqrt{22}+\epsilon_2\sqrt{2}}{2})}$$

$$\text{mit } \epsilon_1 = \pm 1, \epsilon_2 = \pm 1, \epsilon_3 = \pm 1.$$

3. Absolut-abelsche Automorphismen

Wir können im folgenden keine Laufzeitvergleiche mehr angeben, da keine anderen effizienten Verfahren bekannt sind.

Sei $E = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{7})$ der abelsche Zahlkörper der von einer Nullstelle von $f(t) = t^{16} - 112t^{14} + 4532t^{12} - 83472t^{10} + 730358t^8 - 2962896t^6 + 4936148t^4 - 2507824t^2 + 28561$ erzeugt wird. Die Galoisgruppe ist isomorph zu $C_2 \times C_2 \times C_2 \times C_2$. Wir haben die Bilder von α unter allen Automorphismen in 2,7 sek berechnet:

(1) α

(2) $\frac{1}{398331648}(5717975171\alpha - 8761428723\alpha^3 + 4664561653\alpha^5 - 1085705117\alpha^7 + 120821105\alpha^9 - 6477169\alpha^{11} + 159039\alpha^{13} - 1415\alpha^{15})$

(3) $\frac{1}{165905131392}(1460330046379\alpha - 3045184412874\alpha^3 + 1986742065521\alpha^5 - 506400762490\alpha^7 + 58437366385\alpha^9 - 3179647862\alpha^{11} + 78588459\alpha^{13} - 701446\alpha^{15})$

(4) $\frac{1}{1189284096}(26350979023\alpha - 47987953233\alpha^3 + 28168688129\alpha^5 - 6871662679\alpha^7 + 779636965\alpha^9 - 42131819\alpha^{11} + 1038195\alpha^{13} - 9253\alpha^{15})$

(5) $\frac{1}{1755609856}(-90225319091\alpha + 208977060841\alpha^3 - 137389813037\alpha^5 + 35451218887\alpha^7 - 4150002705\alpha^9 + 228199043\alpha^{11} - 5679447\alpha^{13} + 50917\alpha^{15})$

(6) $\frac{1}{23700733056}(-1534560597347\alpha + 3342495330372\alpha^3 - 2132303894353\alpha^5 + 543190909436\alpha^7 - 63213892265\alpha^9 + 3466078636\alpha^{11} - 86135355\alpha^{13} + 771572\alpha^{15})$

(7) $\frac{1}{30164569344}(1254555904787\alpha - 3036935970291\alpha^3 + 1999380957541\alpha^5 - 517043531333\alpha^7 + 60679616225\alpha^9 - 3342756673\alpha^{11} + 83294415\alpha^{13} - 747311\alpha^{15})$

(8) $\frac{1}{18433903488}(520491772111\alpha - 1450445863719\alpha^3 + 1005978370889\alpha^5 - 265727026789\alpha^7 + 31490655445\alpha^9 - 1743046757\alpha^{11} + 43542171\alpha^{13} - 391207\alpha^{15})$

(9) $\frac{1}{30164569344}(-1254555904787\alpha + 3036935970291\alpha^3 - 1999380957541\alpha^5 + 517043531333\alpha^7 - 60679616225\alpha^9 + 3342756673\alpha^{11} - 83294415\alpha^{13} + 747311\alpha^{15})$

(10) $\frac{1}{18433903488}(-520491772111\alpha + 1450445863719\alpha^3 - 1005978370889\alpha^5 + 265727026789\alpha^7 - 31490655445\alpha^9 + 1743046757\alpha^{11} - 43542171\alpha^{13} + 391207\alpha^{15})$

(11) $\frac{1}{1755609856}(90225319091\alpha - 208977060841\alpha^3 + 137389813037\alpha^5 - 35451218887\alpha^7 + 4150002705\alpha^9 - 228199043\alpha^{11} + 5679447\alpha^{13} - 50917\alpha^{15})$

(12) $\frac{1}{23700733056}(1534560597347\alpha - 3342495330372\alpha^3 + 2132303894353\alpha^5 - 543190909436\alpha^7 + 63213892265\alpha^9 - 3466078636\alpha^{11} + 86135355\alpha^{13} - 771572\alpha^{15})$

(13) $\frac{1}{165905131392}(-1460330046379\alpha + 3045184412874\alpha^3 - 1986742065521\alpha^5 + 506400762490\alpha^7 - 58437366385\alpha^9 + 3179647862\alpha^{11} - 78588459\alpha^{13} + 701446\alpha^{15})$

(14) $\frac{1}{1189284096}(-26350979023\alpha + 47987953233\alpha^3 - 28168688129\alpha^5 + 6871662679\alpha^7 - 779636965\alpha^9 + 42131819\alpha^{11} - 1038195\alpha^{13} + 9253\alpha^{15})$

(15) $-\alpha$

(16) $\frac{1}{398331648}(-5717975171\alpha + 8761428723\alpha^3 - 4664561653\alpha^5 + 1085705117\alpha^7 - 120821105\alpha^9 + 6477169\alpha^{11} - 159039\alpha^{13} + 1415\alpha^{15})$

Wir betrachten nun eine Serie von Beispielen, die wir von [29] erhalten haben. Dort werden Beispiele, die in der lokalen Theorie eine große Rolle spielen, auf globale Eigenschaften untersucht. Seien

$$f(t) := t^{p-1} - pa \text{ und } g(t) := t^p - pat \text{ mit } p \in \mathbb{P}, a \in \mathbb{Z} \text{ und } p \nmid a.$$

Dann definieren wir

$$f_n(t) := g(f^{n-1}(t)),$$

wobei f^{n-1} die $(n-1)$-fache Hintereinanderausführung bezeichnet. Eine wichtige Frage hierbei ist, für welche p, a die Galoisgruppe $\mathrm{Gal}(f_n)$ für alle $n \in \mathbb{N}$ abelsch ist. Für $p = 2, a = -1$ erhalten wir so die 2^n-ten Kreisteilungskörper. Wir haben für $p = 2, a = 1$ sowie für $p = 3, a = 1$ Tabellen gerechnet und dabei festgestellt, daß diese Körper abelsch sind.

p	a	n	Grad	Zeit
2	1	2	2	0,2 sek
2	1	3	4	0,4 sek
2	1	4	8	0,3 sek
2	1	5	16	0,8 sek
2	1	6	32	12,8 sek
2	1	7	64	103 sek
2	1	8	128	1224 sek
2	1	9	256	55685 sek

p	a	n	Grad	Zeit
3	1	1	2	0,2 sek
3	1	2	6	0,2 sek
3	1	3	18	0,4 sek
3	1	4	54	14,1 sek
3	1	5	168	536 sek

Aus Platzgründen haben wir auf die Ausgabe der Automorphismen verzichtet. Die etwas kürzeren Laufzeiten für $p = 3$ erklären sich dadurch, daß diese Körper alle zyklisch sind. Im anderen Beispiel war die Galoisgruppe jeweils $C_2 \times C_{2^{n-2}}$.

4. Absolut-normale Automorphismen

Als nächstes betrachten wir einen über $\mathbb{Q}$ normalen Zahlkörper $E = \mathbb{Q}(\alpha)$, der von einer Nullstelle von

$$f(t) := t^{24}+8t^{23}-32t^{22}-298t^{21}+624t^{20}+4592t^{19}-8845t^{18}-31488t^{17}+76813t^{16}+65924t^{15}-265616t^{14}+48348t^{13}+385639t^{12}-394984t^{11}-20946t^{10}+369102t^{9}-362877t^{8}+183396t^{7}+434501t^{6}-194418t^{5}+450637t^{4}+125800t^{3}-16401t^{2}-45880t+115151$$

erzeugt wird. Dieses Beispiel hatten wir schon im Kapitel über Teilkörper betrachtet. Die Laufzeit zur Berechnung der Automorphismen beträgt 60 sek. Dabei waren die Teilkörper vorher nicht bekannt. Die Automorphismen aufzulisten, würde hier den Rahmen sprengen. Um eine Vorstellung von der Größe der Automorphismen zu bekommen, geben wir im folgenden einen an:

$$\frac{1}{1217906956047137258612934958316973401140826764362401347 20}($$

$$\begin{aligned}
&3293454631029323215922747586430862228755190227384470239 3 - \\
&17474933482955457034052531525149257149466166697054664039 7\alpha - \\
&97079047491279824596936741124757490427446988127007123545\alpha^2 + \\
&33939757069969955443220478843345158521275499025652061533 2\alpha^3 - \\
&29770409920463467507776501130501342253004051728522286370 7\alpha^4 + \\
&63789575092877728274424804618909257413749453358430714095\alpha^5 + \\
&38690711838343400644724022895768071540328201845933937820\alpha^6 - \\
&27395320565142950094763879123928839478932108080816716385 9\alpha^7 +
\end{aligned}$$

$367099377439826778579905734034639946338586046309671037418\alpha^8 -$
$360474426145338237881295129461910236283454791635553460\alpha^9 -$
$310748970203086795118164563533905032086973514176031153701\alpha^{10} +$
$157289832239033400871411435522664560127814264975430157465\alpha^{11} +$
$93744229532071753823642907447434098440342994849814651330\alpha^{12} -$
$92145511216209339830480572114457189001926051707271524384\alpha^{13} -$
$5129518563112831408384569951465858000373289660873081990\alpha^{14} +$
$23101968351144973023926252560618812727922601207631148846\alpha^{15} -$
$3107199925394220252192276503869960843898218700061846049\alpha^{16} -$
$2653352350601664212505495820584232671785323621109542067\alpha^{17} +$
$531996660608059394625133848180284288240364126837515109\alpha^{18} +$
$170329382980382984047569907068113415435578248108167186\alpha^{19} -$
$33588643071717835592330088810816815223970101924337678\alpha^{20} -$
$6528912705767084056683254134625330150194404912468452\alpha^{21} +$
$811648456889473914168077641425854763804851680794223\alpha^{22} +$
$132307197840902131935518657051862180047940693809459\alpha^{23})$

Wir haben auch die Automorphismen des Körpers E vom Grad 60 mit $\mathfrak{A}_5$ als Galoisgruppe berechnet, den wir bereits als Beispiel für die Teilkörperberechnung hatten. Als Input haben wir E sowie die Teilkörper vom Grad 5 und 20 gewählt, die wir bei der Zerfällungskörperberechnung erhalten haben. Die Laufzeit für die Berechnung der Automorphismen betrug 7 h 22 min, wobei 2 Frobeniusautomorphismen berechnet wurden. Die übrigen Automorphismen konnten dann mit Diminos Algorithmus bestimmt werden. Für das Newton-Lifting der zwei Frobeniusautomorphismen wurde insgesamt 1 h Rechenzeit benötigt. Diminos Algorithmus zur Bestimmung aller Automorphismen verbrauchte 43 min Rechenzeit. Aus Platzgründen verzichten wir hier auf die expliziten Ergebnisse.

5. Relativ-abelsche Automorphismen

Die folgenden zwei Beispiele sind dadurch entstanden, daß wir aus einer über $\mathbb{Q}$ normalen Erweiterung E, eine relativ-abelsche Erweiterung erzeugt haben. Hierzu haben wir zu einem unverzweigten Primideal $\mathfrak{p}$ aus $\mathfrak{o}_E$ den Zerlegungskörper $Z_\mathfrak{p}$ berechnet und die Relativerweiterung $E/Z_\mathfrak{p}$ betrachtet, die dann sogar zyklisch ist.

Wir betrachten nun das folgende Beispiel:

Der Grundkörper F wird von einer Nullstelle β von $g(t) = t^2 - t + 1$ erzeugt. Die Gleichungsordnung ist maximal und wir betrachten die Erweiterung E/F erzeugt von einer Nullstelle α von $f(t) = t^3 - (1+\beta)t^2 - (2-\beta)t + 1$. Die Erweiterung E/F ist abelsch und wir berechnen die folgenden Bilder von α unter den Automorphismen:

(1) α,
(2) $-((1-\beta) + (1+\beta)\alpha - \alpha^2)$,
(3) $(2 + \beta\alpha - \alpha^2)$.

Die Laufzeit für dieses Beispiel betrug 0,6 sek.

Sei nun $\beta^6 - 17\beta^5 - 430\beta^4 - 2746\beta^3 + 460\beta^2 - 13\beta + 1 = 0$ und die Maximalordnung $\mathfrak{o}_F$ durch folgende Basis gegeben:

$\mu_1 = 1, \mu_2 = \beta, \mu_3 = \beta^2, \mu_4 = \beta^3$,
$\mu_5 = \frac{1}{3}(1 + 2\beta^3 + \beta^4)$,
$\mu_6 = \frac{1}{76222962}(10015273 + 12049708\beta + 66388506\beta^2 + 74483408\beta^3 + 16371270\beta^4 + \beta^5)$.

Nun sei α Nullstelle von

$f(t) := t^4 - (52025\mu_1 - 98634\mu_2 - 543426\mu_3 - 341660\mu_4 - 402006\mu_5 + 623899\mu_6)t^2 - (183326\mu_1 - 347542\mu_2 - 1914917\mu_3 - 1203939\mu_4 - 1416586\mu_5 + 2198491\mu_6)t + \mu_2$.

Hierdurch wird eine relativ-abelsche Erweiterung vom Grad 4 definiert. Der entstehende Körper vom Grad 24 ist isomorph zu dem Körper vom Grad 24, der sowohl bei der Teilkörper- als auch der Automorphismenberechnung (absolut-normal) betrachtet wurde. Wir erhalten in 18 sek die Bilder von α unter allen Automorphismen:

(1) α
(2) $-\frac{1}{47616411}((17788885313976\mu_1 - 33723310215049\mu_2 - 185812700824741\mu_3 - 116823437087859\mu_4 - 137457501989313\mu_5 + 213329145270432\mu_6) + (26662845436938\mu_1 - 50547263581817\mu_2 - 278504955140271\mu_3 - 175100443559950\mu_4 - 206027736661449\mu_5 + 319747708179492\mu_6)\alpha - (11659641404962\mu_1 - 22103806636482\mu_2 - 121789886523127\mu_3 - 76571257978464\mu_4 - 90095738054535\mu_5 + 139825375306320\mu_6)\alpha^2 - (14417595421918\mu_1 - 27330841890389\mu_2 - 150597312341668\mu_3 - 94683065495200\mu_4 - 111406574388648\mu_5 + 172899031849107\mu_6)\alpha^3)$
(3) $\frac{1}{15872137}((2803286763826\mu_1 - 5314259958967\mu_2 - 29281666326573\mu_3 - 18409864051290\mu_4 - 21661526910066\mu_5 + 33617917769563\mu_6) + (1212207337637\mu_1 - 2298187884300\mu_2 - 12661947910546\mu_3 -$

$7960755769480\mu_4 - 9366831340718\mu_5 + 14536988756902\mu_6)\alpha - (3373947419148\mu_1 - 6396042212950\mu_2 - 35242305578450\mu_3 - 22157415637244\mu_4 - 26070993993026\mu_5 + 40461253533974\mu_6)\alpha^2 - (12484983546296\mu_1 - 23667990569836\mu_2 - 130411215702872\mu_3 - 81991673710772\mu_4 - 96473545246988\mu_5 + 149723503947420\mu_6)\alpha^3)$

(4) $\frac{1}{47616411}((9379025022498\mu_1 - 17780530338148\mu_2 - 97967701845022\mu_3 - 61593844933989\mu_4 - 72472921259115\mu_5 + 112475391961743\mu_6) + (23026175807616\mu_1 - 43652699928917\mu_2 - 240519111408633\mu_3 - 151218176251510\mu_4 - 177927242639295\mu_5 + 276136741908786\mu_6)\alpha - (1537799147518\mu_1 - 2915679997632\mu_2 - 16062969787777\mu_3 - 10099011066732\mu_4 - 11882756075457\mu_5 + 18441614704398\mu_6)\alpha^2 + (23037355216970\mu_1 - 43673129819119\mu_2 - 240636334766948\mu_3 - 151291955637116\mu_4 - 178014061352316\mu_5 + 276271479993153\mu_6)\alpha^3)$.

Nun erzeugen wir eine relativ-abelsche Erweiterung dadurch, daß wir Hilbertsche Klassenkörper berechnen [8].

Der Körper F werde nun von einer Nullstelle ρ von $g(t) = t^3 + t^2 - 13t + 36$ erzeugt. Die Gleichungsordnung ist maximal und wir betrachten den von einer Nullstelle α von f erzeugten Hilbertschen Klassenkörper mit

$f(t) = t^{12} - (108 - 270\rho - 24\rho^2)t^{10} - (14624 + 24744\rho + 4372\rho^2)t^9 - (631344 + 421176\rho + 48369\rho^2)t^8 - (174101760 + 3142080\rho - 6298560\rho^2)t^7 - (1051170392 - 732746246\rho - 186322312\rho^2)t^6 - (85808920416 - 10746990552\rho - 5544877344\rho^2)t^5 + (4717709430588 + 2145887127201\rho + 240342270672\rho^2)t^4 + (160143514883280 + 14458229480636\rho - 3476213893676\rho^2)t^3 + (10741252484644056 - 1619403263824086\rho - 749027789533920\rho^2)t^2 - (62344580730746400 + 18875348023315080\rho + 1285873363213020\rho^2)t - (179237747831041548 - 81710865349088363\rho - 23394835280694410\rho^2)$.

Die 12 Automorphismen wurden in 145 sek berechnet. Wir verzichten hier aus Platzgründen auf die expliziten Ergebnisse.

Literaturverzeichnis

[1] V. Acciaro und J. Klüners. Computing automorphisms of abelian number fields. submitted to Math. Comput., 1997.

[2] G. Butler. *Fundamental Algorithms for Permutation Groups.* LNCS 559. Springer, 1991.

[3] D. Casperson, D. Ford, und J. McKay. Ideal decompositions and subfields, *J. Symb. Comput.* **21** (1996), 133–137.

[4] J. Cassels. *Local Fields.* Cambridge University Press, 1986.

[5] H. Cohen. *A Course in Computational Algebraic Number Theory.* Springer, 1993.

[6] G. Collins und M. Encarnación. Efficient rational number reconstruction, *J.Symb.Comput* **20** (1995), 287–297.

[7] M. Daberkow, C. Fieker, J. Klüners, M. Pohst, K. Roegner, und K. Wildanger. KANT V4. to appear in J. Symb. Comput., 1997.

[8] M. Daberkow und M. Pohst. On the computation of Hilbert class fields. Preprint, 1997.

[9] F. Diaz y Diaz und M. Olivier. Imprimitive ninth-degree number fields with small discriminants, *Math. Comput.* **64** (1995), 305–321.

[10] J. Dixon. Exact solution of linear equations using p-adic expansions, *Numer.Math.* **40** (1982), 147–141.

[11] J. Dixon. Computing subfields in algebraic number fields, *J. Austral. Math. Soc. (Series A)* **49** (1990), 434–448.

[12] H. Edwards. *Galois Theory.* Springer, New York - Berlin - Heidelberg - Tokyo, 1984.

[13] M. Encarnación. Computing GCDs of polynomials over algebraic number fields, *J. Symb. Comput.* **20** (1995), 299–313.

[14] K. Geddes, S. Czapor, und G. Labahn. *Algorithms for Computer Algebra.* Kluwer Academic Publishers, Boston - Dordrecht - London, 1992.

[15] A. Hulpke. Block systems of a Galois group, *Exp. Math.* **4** (1995), 1–9.

[16] J. Klüners. Über die Berechnung von Teilkörpern algebraischer Zahlkörper. Diplomarbeit, Technische Universität Berlin, 1995.

[17] J. Klüners. On polynomial decompositions. Preprint, 1997.

[18] J. Klüners und M. Pohst. On computing subfields. to appear in J. Symb. Comput., 1997.

[19] D. Kozen und S. Landau. Polynomial decomposition algorithms, *J. Symb. Comput.* **7** (1989), 445–456.

[20] S. Landau. Factoring polynomials over algebraic number fields, *SIAM J.Comput.* **14** (1985), 184–195.

[21] S. Landau und G. Miller. Solvability by radicals is in polynomial time, *J. of Computer and System Sciences* **30** (1985), 179–208.
[22] S. Lang. *Algebra*. Addison–Wesley, 1974.
[23] S. Lang. *Algebraic Number Theory*, Band 110 aus *Graduate Texts in Mathematics*. Springer, 1994.
[24] D. Lazard und A. Valibouze. Computing subfields: Reverse of the primitive element problem. In A. G. F. Eyssete, Hrsg., *MEGA-92, Computational algebraic geometry*, Band 109, Seiten 163–176. Birkhäuser, Boston, 1993.
[25] A. K. Lenstra, H. W. Lenstra Jr., und L. Lovász. Factoring polynomials with rational coefficients, *Math.Ann.* **261** (1982), 515–534.
[26] M. Mignotte. An inequality about factors of polynomials, *Math. Comput.* **28** (1974), 1153–1157.
[27] W. Narkiewicz. *Elementary and Analytic Theory of Algebraic Numbers*. Springer, zweite Auflage, 1989.
[28] O. Neugebauer. *The Exact Sciences in Antiquity*. Princeton Univ. Press, Princeton, 1952.
[29] F. Nicolae. Private Mitteilung, 1997.
[30] M. Pohst. *Computational Algebraic Number Theory*. DMV Seminar Band 21. Birkhäuser, Basel - Boston - Berlin, 1993.
[31] M. E. Pohst und H. Zassenhaus. *Algorithmic Algebraic Number Theory*. Encyclopaedia of mathematics and its applications. Cambridge University Press, 1989.
[32] B. van der Waerden. *Algebra I*. Springer–Verlag, Berlin–Heidelberg–New York, 1971.
[33] J. von zur Gathen und J. Weiss. Homogeneous bivariate decompositions, *J. Symb. Comput.* **19** (1995), 409–434.
[34] P. Weinberger und L. Rothschild. Factoring polynomials over algebraic number fields, *J. Assoc. Comput. Mach* **2** (1976), 335–350.
[35] H. Wielandt. *Finite Permutation Groups*. Academic Press, New York and London, 1964.

Bezeichnungen

Wir vereinbaren die folgenden Bezeichnungen, falls sie nicht im Zusammenhang erklärt werden.

$\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$	Menge der natürlichen, ganzen, rationalen, reellen und komplexen Zahlen
$\mathbb{P}$	Menge der Primzahlen
$\mathfrak{S}_n$	symmetrische Gruppe mit $n!$ Elementen
$\mathfrak{A}_n$	alternierende Gruppe mit $\frac{n!}{2}$ Elementen
$\mathrm{Gal}(f)$	Galoisgruppe des von f erzeugten Zerfällungskörpers, Definition 2.5
$\mathrm{Aut}(E/F)$	Automorphismengruppe von E/F, Definition 2.5
$\mathrm{Fix}(H)$	der zu H gehörige Fixkörper
$H < G$	H Untergruppe von G
$\mathrm{disc}(f)$	Polynomdiskriminante von f, Bezeichnung 2.2
$\mathfrak{d}(f)$	das von $\mathrm{disc}(f)$ erzeugte Hauptideal, Bezeichnung 2.2
$\deg(f)$	Grad des Polynoms f
$\lvert\beta\rvert_\infty$	Maximumsnorm einer algebraischen Zahl, Definition 2.16
$\mathbb{F}_p,\ \mathbb{F}_q$	endliche Körper mit p bzw. q Elementen
$\mathfrak{p},\ \mathfrak{P}$	Primideale
$f_\mathfrak{p},\ f_{\mathfrak{P}/\mathfrak{p}}$	Trägheitsgrade der Primideale, Definition 2.1
$\mathbb{Q}_p$	Körper der p-adischen Zahlen
$\mathbb{Z}_p$	Ring der ganzen p-adischen Zahlen
$F_\mathfrak{p}$	$\mathfrak{p}$-adische Vervollständigung des Zahlkörpers F
$G_{Z,}\ Z_\mathfrak{p}$	Zerlegungsgruppe, Zerlegungskörper zu $\mathfrak{p}$
E/F	der gegebene algebraische Zahlkörper
$\mathfrak{o}_E, \mathfrak{o}_F$	Ring der ganz algebraischen Zahlen von E bzw. F
$\mathbb{P}_F$	Menge der Primideale in $\mathfrak{o}_F$
Δ	ein Block einer Permutationsgruppe G
$\pi = \pi_1 \cdots \pi_u$	ein Element von G, zerlegt in elementfremde Zykel
$\mathcal{F}, \mathcal{E}$	unverzweigte p-adische Erweiterungen
$\mathfrak{o}_\mathcal{F}, \mathfrak{o}_\mathcal{E}$	Ring der ganz algebraischen Zahlen in $\mathcal{F}$ bzw. $\mathcal{E}$
$\bar{\mathbb{Q}}$	algebraische Zahlen über $\mathbb{Q}$
$\bar{\mathbb{Q}}_p$	algebraische Zahlen über $\mathbb{Q}_p$
$(\cdot)^{(i)}$	i-te Konjugierte, Definition 5.1
$\lfloor a \rfloor$	größte ganze Zahl kleiner gleich a.

Zusammenfassung

In dieser Arbeit werden effiziente Algorithmen zur Berechnung von Teilkörpern und Automorphismen algebraischer Zahlkörper entwickelt. Ein weiterer Teil beschäftigt sich mit einem Verfahren zur Dekomposition von Polynomen, welches einen wesentlichen Schritt in Richtung Auflösbarkeit durch Radikalerweiterungen bedeutet.

Da alle Verfahren Methoden des Hensel- und Newton-Liftings in unverzweigten p-adischen Erweiterungen von $\mathbb{Q}_p$ benutzen, werden geeignete Darstellungen dieser Körper für einen Computer sowie die zugehörigen Algorithmen erarbeitet.

Angewendet werden diese Methoden zur Berechnung aller Teilkörper eines algebraischen Zahlkörpers E. Zur Berechnung eines Teilkörpers L von E gehört einerseits die Berechnung des Minimalpolynoms eines primitiven Elements β von L sowie die Bestimmung der Darstellung von β in E. Hierzu werden Methoden, die der Autor in seiner Diplomarbeit entwickelt hat, an mehreren Punkten verfeinert bzw. deutlich verbessert.

Als Anwendung hiervon wird eine neue Dekomposition von irreduziblen Polynomen $f \in \mathbb{Q}[t]$ definiert, welche die bisher bekannten verallgemeinert. Es wird eine Beziehung zwischen den Teilkörpern des von einer Nullstelle von f definierten Zahlkörpers und den Dekompositionen hergeleitet. Dies liefert einerseits einen sehr effizienten Algorithmus zur Berechnung dieser Dekompositionen, andererseits zeigt dies, daß die so definierten Dekompositionen in diesem Sinne das maximal Erreichbare darstellen.

Als weiterer Schwerpunkt werden Algorithmen für die Bestimmung von Automorphismen von über $\mathbb{Q}$ normalen und abelschen Zahlkörpern sowie für relativ-abelsche Erweiterungen von Zahlkörpern entwickelt. Hierzu werden Ergebnisse aus der Hilbertschen Verzweigungstheorie verwendet. Allen Verfahren ist gemeinsam, daß sukzessiv Frobeniusautomorphismen zu unverzweigten Primidealen berechnet werden.

Alle Algorithmen wurden vom Autor im Computeralgebrasystem KASH implementiert. Zu jedem Verfahren werden illustrative Beispiele angegeben, die die Leistungsfähigkeit zeigen.

Lebenslauf

Persönliche Daten

	Jürgen Klüners geb. am 1.8.1970 in Meerbusch ledig

Schulausbildung

1977 – 1981	Martinus-Grundschule in Meerbusch-Strümp
1981 – 1990	Meerbusch-Gymnasium in Meerbusch-Strümp
29.05.1990	Abitur

Studium

Okt. 1990 – März 1993	Studium der Mathematik an der Heinrich–Heine–Universität Düsseldorf
26.10.1992	Vordiplom in Mathematik
April 1993 – Feb. 1995	Studium der Mathematik an der Technischen Universität Berlin
28.02.1995	Diplom in Mathematik
März 1995 – März 1997	Anfertigung der Dissertation an der Technischen Universität Berlin
Juli 1995 – Juni 1996	Stipendiat, gefördert durch das Nachwuchsförderungsgesetz des Landes Berlin
seit Juli 1996	Wissenschaftlicher Mitarbeiter von Prof. Dr. M. E. Pohst am Fachbereich 3 Mathematik der Technischen Universität Berlin
21.05.1997	Tag der wissenschaftlichen Aussprache