Über die Berechnung von Teilkörpern algebraischer Zahlkörper

Diplomarbeit
von
Jürgen Klüners
aus Meerbusch

Angefertigt am Fachbereich 3 Mathematik
der Technischen Universität Berlin
Berlin 1994

Inhaltsverzeichnis

KAPITEL 1
Einleitung

Nach den Pionierarbeiten Kummers wurde bis 1871 nichts über die Theorie der algebraischen Zahlen veröffentlicht. Dies war das Jahr, in dem Dedekind seine Arbeit über die Grundlagen der Theorie der algebraischen Zahlen als X. Supplement zur zweiten Auflage der Dirichletschen *Vorlesungen über Zahlentheorie* publizierte [Ded]. In der 1894 veröffentlichten vierten Auflage findet man das X. Supplement, das inzwischen zum XI. Supplement geworden war, in seiner endgültigen Form. Es ist ein Meisterwerk der mathematischen Literatur, in dem Dedekind neben dem Begriff des Körpers auch den Begriff des Moduls einführte, wobei er darunter das verstand, was wir jetzt einen Teilkörper nennen.

Die Kenntnis der Teilkörper eines gegebenen Zahlkörpers erlaubt einen tieferen Einblick in seine Struktur. So bemerkt schon Hilbert [Hil]: „Der Galoissche Körper gestattet ein sehr genaues Studium der Zerlegungsgesetze seiner Zahlen mit Rücksicht auf die in ihm enthaltenen Unterkörper, und die sich hierbei ergebenden Resultate sind vor allem für die Anwendung der allgemeinen Körpertheorie auf besondere Zahlkörper von Wichtigkeit.“

Es besteht also ein großes Interesse, die Teilkörper eines gegebenen algebraischen Zahlkörpers zu bestimmen. Wir könnten versuchen, zuerst die Galoisgruppe der normalen Hülle unseres Körpers zu bestimmen, um hiernach mit deren Hilfe die Teilkörper auszurechnen. Es erweist sich jedoch als zu aufwendig, die Galoisgruppe auszurechnen.

Dixon stellte 1990 in [Dix1] einen Algorithmus zur Bestimmung aller Teilkörper eines algebraischen Zahlkörpers vor. Der hier vorgestellte Algorithmus benutzt Dixons Ideen, verbessert diesen aber entscheidend an verschiedenen Stellen. Unser Verfahren zur Bestimmung der Teilkörper teilt sich in drei Schritte auf.

Im ersten Teil unseres Verfahrens, den wir im 4. Kapitel unserer Arbeit vorstellen, wollen wir mögliche Kandidaten für Teilkörper finden. Wir können beweisen, daß es eine Bijektion zwischen den Teilkörpern und ausgezeichneten Imprimitivitätsgebieten (Blöcken) der Galoisgruppe gibt. Mit Hilfe des van der Waerden-Kriteriums [Wae] können wir zyklische Untergruppen der Galoisgruppe bestimmen und mit Kenntnis dieser können wir auf passende Blöcke zurückschließen. Dazu werden wir Eigenschaften von Blöcken herleiten, die wir zur Berechnung dieser einsetzen werden.

Das 5. Kapitel dieser Arbeit beschäftigt sich mit der Aufgabe, aus den berechneten Blöcken, ein erzeugendes Polynom des gesuchten Teilkörpers zu bestimmen. Hier entwickeln wir ein neues Verfahren, welches nur mit Hilfe von Faktorisierungen von Polynomen über endlichen Körpern und dem Hensel-Lifting über p-adischen Körpern die Teilkörper berechnet.

Der letzte Teil unseres Algorithmus, den wir wir im 6. Kapitel vorstellen werden, beschäftigt sich mit der Einbettung des gefundenen Teilkörpers in den gegebenen Körper. Auch hier können wir die Berechnungen in p-adischen Körpern durchführen. Es werden jedoch auch kompliziertere zahlentheoretische Methoden verwandt.

In dieser Arbeit wird erstmalig ein Algorithmus zur Teilkörperberechnung vorgestellt, der auch auf einem Computer implementiert wurde. Mittels dieses Programms besteht die Möglichkeit effizient Teilkörper auszurechnen. Bisher wurden bei mehr als 1000 Zahlkörper Teilkörper mit ihren Einbettungen bestimmt. Die Kenntnis solcher Teilkörper ist für viele Algorithmen der konstruktiven Zahlentheorie von großer Bedeutung. So können diese Ergebnisse z.B. dazu benutzt werden, Ganzheitsbasen oder Einheiten zu berechnen. Bei der Ganzheitsbasenberechnung kann man versuchen, das Problem zuerst im Teilkörper und hiernach mit relativen Methoden zu lösen. Bei der Einheitenberechnung kann man bereits viele unabhängige Einheiten in den Teilkörpern bestimmen und sie mittels der berechneten Einbettung in den gegebenen Körper liften. Weiterhin besteht die Möglichkeit, dieses Verfahren zur Galoisgruppenberechnung einzusetzen. So stellt der Algorithmus meistens sehr schnell fest, wenn ein Körper primitiv ist, d.h. keine Teilkörper hat. Auch lassen die berechneten Teilkörper Rückschlüsse auf die mögliche Galoisgruppe zu.

Wir werden am Ende der Arbeit mit einer großen Anzahl von Beipielen die Leistungsfähigkeit des Verfahrens unterstreichen.

KAPITEL 2

Grundlagen

1. Algebraische Zahlkörper und deren Teilkörper

In dieser Arbeit betrachten wir endliche Körpererweiterungen des Körpers $\mathbb{Q}$. Hierzu sei ein beliebiges normiertes Polynom $f \in \mathbb{Z}[t]$ gegeben, welches irreduzibel ist. Weiterhin sei α eine Nullstelle des Polynoms f. Durch $K = \mathbb{Q}(\alpha)$ wird eine über $\mathbb{Q}$ algebraische Körpererweiterung vom Grad n definiert, wenn n der Grad des Polynoms f ist. Eine solche Körpererweiterung heißt dann algebraischer Zahlkörper. Falls nun ein Körper L existiert, für den $\mathbb{Q} \subseteq L \subseteq K$ gilt, so wird dieser als Teilkörper von K bezeichnet. Die Angabe eines Algorithmus zur Berechnung aller Teilkörper L eines gegebenen Körpers K ist das Hauptziel dieser Arbeit. Zum besseren Verständnis wollen wir mit einem Beispiel starten.

Beispiel 2.1. *Wir betrachten $f(t) = t^6 + 108$. Dieses Polynom erzeugt eine Körpererweiterung vom Grad 6. Sei α eine Nullstelle von f. Dieser Körper besitzt 3 Teilkörper vom Grad 3. Alle werden durch das Minimalpolynom $g(t) = t^3 - 108$ erzeugt. Die Nullstellen von g sind $\beta_1 = \sqrt[3]{108}$, $\beta_2 = e^{\frac{2\pi i}{3}}\sqrt[3]{108}$ und $\beta_3 = e^{\frac{4\pi i}{3}}\sqrt[3]{108}$. Wie man leicht sieht, werden durch diese Nullstellen 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) $\beta_1 = -\alpha^2$.
(ii) $\beta_2 = \frac{1}{2}\alpha^2 + \frac{1}{12}\alpha^5$.
(iii) $\beta_3 = \frac{1}{2}\alpha^2 - \frac{1}{12}\alpha^5$.

$$\begin{tikzcd} & \mathbb{Q}(i\sqrt[6]{108}) \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\ \mathbb{Q}(\sqrt[3]{108}) \arrow[dr, dash] & \mathbb{Q}(e^{\frac{2\pi i}{3}}\sqrt[3]{108}) \arrow[d, dash] & \mathbb{Q}(e^{\frac{4\pi i}{3}}\sqrt[3]{108}) \arrow[dl, dash] \\ & \mathbb{Q} & \end{tikzcd}$$

Da wir alle Teilkörper L eines gegebenen Körpers K bestimmen wollen, müssen wir isomorphe aber nicht identische Körper unterscheiden. Dies geschieht dadurch, daß wir nicht nur ein Minimalpolynom eines Teilkörpers L, sondern auch seine Einbettung in den Körper K berechnen. Dadurch erhalten isomorphe Teilkörper verschiedene Einbettungen in den Körper K und können somit unterschieden werden. Allerdings kann es auch passieren, daß man in dieser Darstellung auch identische Körper unterscheidet, z.B. $\mathbb{Q}(\sqrt{2})$ und $\mathbb{Q}(-\sqrt{2})$. Der folgende Satz beschreibt, wie die Einbettung aussieht. Vorher wollen wir aber noch zwei Begriffe klären.

Definition 2.2. *Ein Element $\beta \in K$ heißt ganz (algebraisch), falls β einer normierten algebraischen Gleichung*

$$\beta^m + b_1\beta^{m-1} + \ldots + b_m = 0$$

mit Koeffizienten $b_i \in \mathbb{Z}\,(1 \leq i \leq m)$ genügt.

Definition 2.3. *Es sei $f \in \mathbb{Z}[t]$ normiert und irreduzibel. Dann heißt f erzeugendes Polynom für den Zahlkörper K, wenn eine Nullstelle α von f ein primtives Element von K ist.*

Generalvoraussetzung

Für den Rest dieses Kapitel bezeichne f ein erzeugendes Polynom des Zahlkörpers $K = \mathbb{Q}(\alpha)$, α eine Nullstelle und n den Grad von f.

Satz 2.4. *Sei β ein ganzes Element von K, welches einen Teilkörper L erzeugt. Dann existiert ein eindeutig gegebenes Polynom $h \in \mathbb{Q}[t]$ derart, daß $h(\alpha) = \beta$ und der Grad von h echt kleiner als n ist.*

Beweis: Wir stellen β eindeutig in der Potenzbasis $(1, \alpha, \ldots, \alpha^{n-1})$ von K dar, d.h. es gilt: $\beta = b_0 + b_1\alpha + \ldots + b_{n-1}\alpha^{n-1}$ $(b_i \in \mathbb{Q}, 0 \leq i < n)$. Wir definieren nun $h(t) := b_0 + b_1 t + \ldots + b_{n-1}t^{n-1}$. Aufgrund der Konstruktion ist h eindeutig bestimmt und leistet das Gewünschte. □

Die Koeffizenten von h liegen in $\mathbb{Q}$ und nicht notwendigerweise in $\mathbb{Z}$, da β als ganzes Element nicht unbedingt in der Gleichungsordnung $\mathbb{Z}[\alpha]$ liegen muß. Diesen Effekt haben wir schon im obigen Beispiel gesehen.

Also kann jeder Teilkörper L durch ein Paar (h, g) mit $h \in \mathbb{Q}[t]$ und $g \in \mathbb{Z}[t]$ dargestellt werden, für welches gilt:

(1) $L = \mathbb{Q}(h(\alpha))$.
(2) g ist Minimalpolynom zu $h(\alpha)$.

Bevor wir diese Bedingung anders ausdrücken, vereinbaren wir noch eine Schreibweise.

Definition 2.5. *Seien ω, g und $h \in \mathbb{Z}[t]$ oder $\mathbb{Q}[t]$ Polynome. Dann wird folgende Schreibweise definiert:*

$$g \equiv h \bmod \omega \textit{ genau dann, wenn } (g - h) \textit{ in } \mathbb{Q}[t] \textit{ von } \omega \textit{ geteilt wird.}$$

Satz 2.6. *Sei L durch (h, g) mit $h \in \mathbb{Q}[t]$ und $g \in \mathbb{Z}[t]$ beschrieben. Dann sind äquivalent:*

(1) *g ist Minimalpolynom zu $h(\alpha)$.*
(2) *g ist irreduzibel und $g(h) \equiv 0 \bmod f$.*

Beweis: (1)⇒ (2): Da g Minimalpolynom zu $h(\alpha)$ ist, ist g nach Definition irreduzibel. Wir nehmen nun an, daß $g(h) \equiv \omega \bmod f$ mit $\omega \in \mathbb{Q}[t]$ gilt. Wegen $f(\alpha) = g(h(\alpha)) = 0$ folgt $\omega(\alpha) = 0$ und somit wird ω von f geteilt. Also gilt $g(h) \equiv 0 \bmod f$.

(2)⇒ (1): Sei nun umgekehrt $g(h) \equiv 0 \bmod f$. Daraus folgt dann wegen $f(\alpha) = 0$, daß $g(h(\alpha)) = 0$ gilt. Da g zudem irreduzibel ist, folgt die Behauptung. □

Die vorangegangenen Überlegungen zeigen, daß zur Bestimmung der Teilkörper zwei Dinge berechnet werden müssen. Als erstes müssen die Minimalpolynome der Teilkörper und dann die Einbettungen berechnet werden. Dieses wird im 4. bzw. 5. Kapitel dieser Arbeit erläutert werden.

Da die Bedingung $f \mid g(h)$ in $\mathbb{Q}[t]$ sehr häufig getestet werden muß, werden wir hier kurz die Implementierung erläutern. Die Komposition $g(h)$ können wir mit Hilfe des Horner-Schemas ausrechnen. Da der Grad von $g(h)$ sehr groß werden kann und die Arithmetik über den rationalen Zahlen durchgeführt werden muß, erweist es sich als ungünstig, zuerst $g(h)$ auszurechnen und hiernach den Rest von $g(h) \bmod f$ zu bestimmen. Geschickter ist es, wenn wir während der Berechnung von $g(h)$ nach jedem Schritt des Horner-Schemas die Koeffizienten modulo f reduzieren. Dadurch werden die Grade der Polynome klein gehalten.

2. Primideale in der Maximalordnung

Im folgenden werden wir den Begriff der Maximalordnung klären.

Definition 2.7. *Wir definieren $\mathfrak{o}_K := \{\beta \in K \mid \beta \text{ ist ganz}\}$ als die Menge der ganz algebraischen Elemente in K.*

Die Menge der ganz algebraischen Zahlen ist ein Ring. Zusätzlich gilt der folgende Satz:

Satz 2.8. *Der Ring $\mathfrak{o}_K$ ist ein freier $\mathbb{Z}$-Modul vom Rang n. Ist $\omega_1, \dots, \omega_n$ eine $\mathbb{Z}$-Basis von $\mathfrak{o}_K$, so nennen wir sie eine Ganzheitsbasis von K.*

Mit Hilfe dieses Satzes können wir folgendes definieren:

Definition 2.9. *Wir definieren einen unitären Teilring R von $\mathfrak{o}_K$, der ein freier $\mathbb{Z}$-Modul vom Rang n ist, als eine Ordnung des Zahlkörpers K. Weiterhin bezeichnen wir $\mathfrak{o}_K$ als Maximalordnung von K.*

Wir wollen nun auf einige wichtige Eigenschaften der Maximalordnung eingehen. So ist es sehr angenehm für die praktische Arbeit, daß die Maximalordnung ein sogenannter Dedekindring ist. Hiermit beschäftigen sich die nächste Definition und die folgenden Aussagen.

Definition 2.10. *Es sei R ein Integritätsring mit 1 und M sein Quotientenkörper.*

(i) *Eine Teilmenge $\mathfrak{b} \neq \emptyset$ von M heißt gebrochenes Ideal von R, falls $\zeta \in R$ und ein Ideal $\mathfrak{a}$ in R existieren mit $\mathfrak{b} = \frac{1}{\zeta}\mathfrak{a}$.*

(ii) *Falls die gebrochenen Ideale von R eine multiplikative Gruppe bilden, so bezeichnen wir R als Dedekindring.*

SATZ 2.11. *Ist R ein Dedekindring, so gelten*

(i) Jedes Ideal $\mathfrak{a}\,(\mathfrak{a} \notin \{\{0\}, R\})$ hat eine bis auf Reihenfolge eindeutige Zerlegung

$$\mathfrak{a} = \mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_r$$

in Primideale $\mathfrak{p}_i$ von $R\,(1 \leq i \leq r)$.

(ii) Jedes Primideal $\mathfrak{p} \neq \{0\}$ in R ist maximal.

Wir bezeichnen mit I_K die Menge der gebrochenen Ideale in $\mathfrak{o}_K$. Da die Zerlegung eines Ideals in Primideale eindeutig ist, folgt aus der Gruppeneigenschaft der gebrochenen Ideale, daß auch die gebrochenen Ideale Potenzprodukte von Primidealen sind. Deshalb ist die folgende Definition sinnvoll.

DEFINITION 2.12. *Für ein Primideal $\mathfrak{p}$ in $\mathfrak{o}_K$ definieren wir:*

$$\nu_{\mathfrak{p}}(\cdot) : I_K \to \mathbb{Z} : \mathfrak{a} = \mathfrak{p}^k \mathfrak{b} \mapsto k,$$

wobei $\mathfrak{b}$ in ein Potenzprodukt von Primidealen zerlegt werden kann, welches $\mathfrak{p}$ nicht enthält.

Im folgenden werden wir einige Eigenschaften von Primidealen auflisten. Seien hierzu $\mathbb{Q} \subseteq L \subseteq K$ algebraische Zahlkörper. Mit $\mathfrak{o}_K$ und $\mathfrak{o}_L$ seien die zugehörigen Maximalordnungen bezeichnet. Weiterhin sei $\mathfrak{p}$ ein Primideal von $\mathfrak{o}_L$ und $\mathfrak{P}$ ein Primideal von $\mathfrak{o}_K$. Mit diesen Bezeichnungen gilt das folgende Lemma:

LEMMA 2.13. *Die folgenden Aussagen sind äquivalent:*

(i) $\mathfrak{P} \mid \mathfrak{p}\mathfrak{o}_K$
(ii) $\mathfrak{P} \supseteq \mathfrak{p}\mathfrak{o}_K$
(iii) $\mathfrak{P} \supseteq \mathfrak{p}$
(iv) $\mathfrak{P} \cap \mathfrak{o}_L = \mathfrak{p}$
(v) $\mathfrak{P} \cap L = \mathfrak{p}$

Falls in $\mathfrak{o}_K$ die Primidealzerlegung $\mathfrak{p}\mathfrak{o}_K = \mathfrak{P}_1^{e_1} \cdot \ldots \cdot \mathfrak{P}_g^{e_g}$ in paarweise verschiedene Primideale gilt, so sind die Primideale $\{\mathfrak{P}_1, \ldots, \mathfrak{P}_g\}$ gerade die Ideale, die die Bedingungen des Lemmas erfüllen. Daher definieren wir:

DEFINITION 2.14. *Erfüllen $\mathfrak{P}$ und $\mathfrak{p}$ eine der Bedingungen von* 2.13, *so sagen wir, daß $\mathfrak{P}$ über $\mathfrak{p}$ bzw. $\mathfrak{p}$ unter $\mathfrak{P}$ liegt.*

In der Theorie der Primidealzerlegung spielen die beiden folgenden Begriffe eine wesentliche Rolle.

DEFINITION 2.15. *Sei* $\mathfrak{p}$ *ein Primideal in* $\mathfrak{o}_L$. *Wir betrachten die folgende Primidealzerlegung in paarweise verschiedene Primideale in* $\mathfrak{o}_K$:

$$\mathfrak{p}\mathfrak{o}_K = \mathfrak{P}_1^{e_1} \cdot \ldots \cdot \mathfrak{P}_g^{e_g}.$$

Dann definieren wir $e(\mathfrak{P}_i/\mathfrak{p}) := e_i$ *als den Verzweigungsindex von* $\mathfrak{P}_i$ *über* $\mathfrak{p}$. *Gilt* $e(\mathfrak{P}_i/\mathfrak{p}) > 1$ *für ein* i, *so heißt* $\mathfrak{p}$ *verzweigt in* K. *Ansonsten heißt* $\mathfrak{p}$ *unverzweigt.*

Als den Trägheitsgrad von $\mathfrak{P}_i$ *über* $\mathfrak{p}$ *bezeichnen wir mit* $f(\mathfrak{P}_i/\mathfrak{p})$ *den Körpergrad* $[(\mathfrak{o}_K/\mathfrak{P}_i) : (\mathfrak{o}_L/\mathfrak{p})]$.

BEMERKUNG 2.16. *Es sei* $\mathfrak{o}_K$ *die Maximalordnung von* K, $\mathfrak{p} \neq \{0\}$ *ein Primideal in* $\mathfrak{o}_K$, *welches über* $p\mathbb{Z}$ *liegt und* $f = f(\mathfrak{p}/p\mathbb{Z})$. *Dann ist* $\mathfrak{o}_K/\mathfrak{p} \cong \mathbb{F}_q$, *wobei* $\mathbb{F}_q$ *ein endlicher Körper mit* p^f *Elementen ist.*

Falls K galoissch über L ist, so können wir für die Zerlegung eines Primideals $\mathfrak{p}$ eine noch schärfere Aussage treffen.

SATZ 2.17. *Es sei* K *eine normale Erweiterung von* L *und* $\mathfrak{p}$ *ein Primideal in* $\mathfrak{o}_L$. $\mathfrak{P}_1$ *und* $\mathfrak{P}_2$ *seien zwei Primideale in* $\mathfrak{o}_K$, *die über* $\mathfrak{p}$ *liegen. Dann folgt* $e(\mathfrak{P}_1/\mathfrak{p}) = e(\mathfrak{P}_2/\mathfrak{p})$ *und* $f(\mathfrak{P}_1/\mathfrak{p}) = f(\mathfrak{P}_2/\mathfrak{p})$.

Wir wollen an dieser Stelle noch anmerken, daß wir nur an unverzweigten Primidealen interessiert sind. Diese Einschränkung werden wir noch gezielt ausnutzen.

Die folgenden wichtigen Resultate können z.B. in [Mar] entnommen werden.

SATZ 2.18. *Es sei* L *ein algebraischer Zahlkörper und* K *und* M *zwei endliche und algebraische Erweiterungen von* L. *Es sei* $\mathfrak{p}$ *ein Primideal in* $\mathfrak{o}_L$, *welches in* K *und* M *unverzweigt ist. Dann bleibt* $\mathfrak{p}$ *auch in der Komposition* KM *unverzweigt.*

Eine einfache Folgerung aus diesem Satz ist das folgende Korollar.

KOROLLAR 2.19. *Es sei* L *ein algebraischer Zahlkörper und* K *eine endliche, algebraische Erweiterung von* L. *Wieder sei* $\mathfrak{p}$ *ein Primideal von* $\mathfrak{o}_L$. *Falls* $\mathfrak{p}$ *unverzweigt in* K *bleibt, so bleibt* $\mathfrak{p}$ *auch unverzweigt in der normalen Hülle* M *von* K/L.

3. Galoistheorie

Die Galoistheorie ist ein wichtiges Hilfsmittel für die Berechnung der Teilkörper. Leider ist es erheblich zu kompliziert, zuerst die Galoisgruppe zu bestimmen, um mit deren Hilfe die Teilkörper zu berechnen. Trotzdem können Teile der Galoistheorie auch sinnvoll für die Teilkörperberechnung eingesetzt werden. Deswegen werden wir hier die wichtigsten Aussagen der Galoistheorie auflisten. Für weitere Aussagen und die Beweise verweisen wir auf die verschiedenen Standard–Werke der Algebra.

Definition 2.20. *Es sei E/F eine endliche Körpererweiterung. Mit $Aut(E)$ bezeichnen wir die Menge der Körperautomorphismen des Körpers E und sei $G := G(E/F) := \{\sigma \in Aut(E) \mid \sigma(x) = x \text{ für alle } x \in F\}$. Die Körpererweiterung E/F heißt galoissch oder Galoiserweiterung, falls E/F normal und separabel ist. In diesem Fall ist $G(E/F)$ die zugehörige Galoisgruppe.*

Satz 2.21. *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 $G(E/F)/G(E/L)$.

Damit wir die Galoisgruppe einfacher bezeichnen können, wollen wir die folgende Schreibweise vereinbaren.

Definition 2.22. *Es sei F ein Körper und $g \in F[t]$ ein normiertes Polynom, welches nicht notwendigerweise irreduzibel ist. Weiterhin seien $\beta_1, \ldots, \beta_m$ die Nullstellen von g. Dann bezeichnet $Gal(g)$ die Galoisgruppe von $F(\beta_1, \ldots, \beta_m)/F$.*

Der Hauptsatz der Galoistheorie ist für beliebige Körpererweiterungen anwendbar. Noch stärkere Aussagen lassen sich aber treffen, wenn wir endliche Erweiterungen von endlichen Körpern betrachten. Dies soll im folgenden Satz getan werden.

Satz 2.23. *Es sei $p \in \mathbb{P}$ und K eine endliche Erweiterung von $\mathbb{F}_p$ vom Grad n, d.h. $K = \mathbb{F}_q$ mit $q = p^n$. Dann ist $K/\mathbb{F}_p$ galoissch mit $G(K/\mathbb{F}_p) = <\sigma>$, wobei σ der Frobenius-Automorphismus ($x \mapsto x^p$) ist. Ist L eine Erweiterung von K vom Grad m, so ist auch L/K galoissch mit Galoisgruppe $G(L/K) = <\tau>$ mit $\tau : x \mapsto x^{p^n} (x \in L)$.*

4. Hensel-Lifting

Das Hensel-Lifting liefert eine Methode, eine Kongruenzfaktorisierung modulo eines Ideals $\mathfrak{b}$ zu einer Kongruenzfaktorisierung modulo $\mathfrak{b}^k$ für ein beliebiges $k \in \mathbb{N}$ zu liften. Diese Methode wird z.B. bei der Polynomfaktorisierung angewendet. Dabei soll ein Polynom $f \in \mathbb{Z}[t]$ faktorisiert werden. Dies geschieht dadurch, daß dieses Polynom modulo $p\mathbb{Z}[t]$ faktorisiert wird. Falls keine doppelten Faktoren auftreten, wird diese Faktorisierung dann mittels des Hensel-Liftings zu einer Faktorisierung modulo $p^k\mathbb{Z}[t]$ geliftet, wobei k vom gegebenen Polynom f abhängt. Dann wird versucht, aufgrund der gewonnenen Kongruenzfaktorisierung Rückschlüsse auf die Faktorisierung von $f \in \mathbb{Z}[t]$ zu machen. In dieser Arbeit werden wir das Hensel-Lifting auch benutzen, um die sog. Blöcke der Galoisgruppe eines Polynoms f zu berechnen. Hierbei benötigen wir allerdings eine allgemeinere Version des Hensel-Liftings als beim obigen Verfahren. Diese stellen wir im folgenden Satz vor.

Satz 2.24. *Hensel-Lemma*

Sei R ein unitärer kommutativer Ring, $\mathfrak{b}$ ein Ideal von R. Ferner seien f, f_{10} und $f_{20} \in R[t]$ normierte, nicht konstante Polynome, für die folgendes gilt:

(1) $f \equiv f_{10}f_{20} \bmod \mathfrak{b}[t]$
(2) $a_{10}f_{10} + a_{20}f_{20} = 1 + a_{00}\,(a_{i0} \in R[t], 1 \leq i \leq 2, a_{00} \in \mathfrak{b}[t])$

Dann kann man für jedes $k \in \mathbb{N}$ Polynome $f_{1k}, f_{2k}, a_{1k}, a_{2k}$ und a_{0k} bestimmen, so daß folgende Bedingungen erfüllt sind:

(1) $f \equiv f_{1k}f_{2k} \bmod \mathfrak{b}^{2^k}[t]$
(2) $f_{ik} \equiv f_{i0} \bmod \mathfrak{b}[t]\,(f_{ik} \in R[t]$ *normiert, nicht konstant)* $(i = 1, 2)$
(3) $a_{1k}f_{1k} + a_{2k}f_{2k} = 1 + a_{0k}\ (a_{ik} \in R[t],\ \deg(a_{ik}) < \deg(f_{3-i,k}),$
$1 \leq i \leq 2,\ a_{0k} \in \mathfrak{b}^{2^k}[t])$

Der Beweis dieses Satzes kann [PoZa] entnommen werden. Da wir den Algorithmus für einen „komplizierteren“ Ring benutzen wollen, werden wir ihn im folgenden auflisten. In einem späteren Teil dieser Arbeit werden wir uns dann überlegen, wie wir die arithmetischen Operationen, die für diesen Algorithmus benötigt werden, durchführen können. Die Bezeichnungen stimmen mit denen in [PoZa] überein, so daß man die Korrektheit des Algorithmus dort sehr gut nachvollziehen kann.

Algorithmus 2.25. *Hensel-Lifting*

Input: $R, \mathfrak{b}, k, f, f_{10}, f_{20}, a_{10}, a_{20}, a_{00}$ *wie im Satz* 2.24.

Output: *Polynome f_{1k}, f_{2k} wie im Satz 2.24.*

(1) *Setze $i = 0$.*
(2) *Falls $i = k$ ist, gib f_{1k} und f_{2k} aus und terminiere.*
(3) *Setze $d_i = f - f_{1i}f_{2i}$.*
(4) *Setze $d^*_{1i} = a_{2i}d_i$.*
(5) *Setze $d^*_{2i} = a_{1i}d_i$.*
(6) *Setze $d_{ji} = d^*_{ji} \bmod f_{ji}$ (Division mit Rest) für $(j = 1, 2)$.*
(7) *Setze $f_{j(i+1)} = f_{ji} + d_{ji}$ für $(j = 1, 2)$.*
(8) *Setze $b_{ji} = -a_{ji}(a_{0i} + a_{1i}d_{1i} + a_{2i}d_{2i})$ für $(j = 1, 2)$.*
(9) *Setze $a_{j(i+1)} = a_{ji} + b_{ji}$ für $(j = 1, 2)$.*
(10) *Setze $a_{j(i+1)} = a_{j(i+1)} \bmod f_{(3-j)(i+1)}$ (Division mit Rest) für $(j = 1, 2)$.*
(11) *Setze $a_{0(i+1)} = a_{1i}f_{1i} + a_{2i}f_{2i} - 1$.*
(12) *Setze $i = i + 1$ und gehe nach (2).*

Im obigen Satz sind die Kongruenzen nur für zwei Faktoren formuliert. Der Satz kann aber auch sukzessiv auf mehrere Faktoren angewendet werden, da die einzige Voraussetzung an die Faktoren ist, daß deren ggT 1 ist. Das heißt, daß die Faktoren nicht irreduzibel sein müssen. Dies bedeutet, daß man mehrere Faktoren zu einem ausmultiplizieren kann, um danach das Hensel-Lemma auf die verbleibenden zwei Faktoren anzuwenden. Hiernach kann man f durch den einen neu erhaltenen gelifteten Faktor dividieren und das Verfahren auf die verbleibenden Faktoren erneut anwenden.

Zum Abschluß dieses Abschnitts werden wir noch den Begriff einer modulo p^k-Approximation erklären.

Definition 2.26. *Für $p \in \mathbb{P}, k \in \mathbb{N}$ heißt $\tilde{g} \in \mathbb{Z}[t]$ eine modulo p^k-Approximation von $g \in \mathbb{Z}[t]$, wenn $g \equiv \tilde{g} \bmod p^k\mathbb{Z}[t]$ gilt. Wir sagen $\delta \in \mathbb{Z}$ ist eine modulo p^k-Approximation eines primitiven Elements eines Zahlkörpers L, wenn $\tilde{g}(\delta) \equiv 0 \bmod p^k$ für ein erzeugendes Polynom g von L ist.*

5. Das van der Waerden-Kriterium

In diesem Abschnitt wollen wir einen Satz zur Verfügung stellen, der für unser Verfahren der Teilkörperberechnung von zentraler Bedeutung ist. Mit dem folgenden Satz können wir mit Hilfe von Kongruenzfaktorisierungen modulo eines Primideals $p\mathbb{Z}$ Elemente der Galoisgruppe eines erzeugenden Polynoms eines Körpers bestimmen. Da die Algorithmen zum Faktorisieren von Polynomen über endlichen Körpern sehr schnell ist, 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 den folgenden Kapiteln vorstellen.

SATZ 2.27. *van der Waerden-Kriterium*

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

Der Beweis dieses Satzes kann in Kapitel 25 von [Wae] entnommen werden. Dies ist die allgemeine Form dieses Satzes. Weil wir in unserem Verfahren sehr häufig eine spezielle Form dieses Satzes benötigen, stellen wir diese im folgenden Satz vor.

SATZ 2.28. *Es sei $g \in \mathbb{Z}[t]$ ein normiertes und irreduzibles Polynom. Ferner sei ein $p \in \mathbb{P}$ gegeben, welches nicht disc(g) teilt. Es gelte: $g(t) \equiv g_1(t) \cdot \ldots \cdot g_m(t) \bmod p\mathbb{Z}[t]$. Dann enthält Gal($g$) eine zyklische Untergruppe U, die von einer Permutation π erzeugt wird. Wenn man nun π in elementfremde Zykel zerlegt, so entsprechen die Anzahl der Nullstellen, die in diesen Zykeln permutiert werden, gerade den Graden der Polynome g_i $(i = 1, \ldots, m)$. Weiterhin permutiert π gerade die Nullstellen eines irreduziblen Faktors g_i untereinander.*

Damit wir die Anwendung dieses Satzes besser verstehen können, betrachten wir im folgenden einige Beispiele zu 2.28. Zur kürzeren Schreibweise schreiben wir nur $g \bmod p$ und meinen damit $g \bmod p\mathbb{Z}[t]$.

BEISPIEL 2.29. *Es sei $g(t) = t^4 + 2$ und G =Gal(g). Die Nullstellen von g seien mit $\alpha_1, \ldots, \alpha_4$ bezeichnet. Wir bestimmen im folgenden die Faktorisierungen von $g \bmod 2, 3, 5, 7$.*

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

Die erste Faktorisierung ist für uns unbrauchbar, da $g \bmod 2$ doppelte Nullstellen hat und damit 2 ein Diskrimantenteiler von g ist. Wir können den Satz somit nicht anwenden. In der nächsten Faktorisierung tauchen keine doppelten Nullstellen auf. 3 ist somit kein Diskriminantenteiler und der Satz ist anwendbar. Wir erhalten, daß G eine Permutation π enthält, deren Zerlegung in elementfremde Zykel gerade so aussieht:

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

Dabei sollen die Nullstellen passend numeriert sein. Auch die beiden folgenden Faktorisierungen erfüllen die Voraussetzung unseres Satzes. Wir können also zwei weitere Elemente von G bestimmen:

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

Unser Problem bei diesem Satz ist, daß wir die Nullstellen $\alpha_i \in \mathbb{C}$, die in einem Zykel liegen, nicht identifizieren können. Deswegen können wir auf diese Weise nur eine ungefähre Vorstellung von den Elementen der Galoisgruppe bekommen.

Das Element π, welches wir im Satz bestimmen, ist der Erzeuger der zyklischen Galoisgruppe von $\mathbb{F}_q/\mathbb{F}_p$, welche durch das Polynom $\bar{g}$ erzeugt wird. Dabei ist $\bar{g} \in \mathbb{F}_p[t]$ das Polynom, welches aus g dadurch entsteht, daß alle Koeffizienten von g modulo p reduziert werden. Ein Erzeuger dieser Galoisgruppe ist nach 2.23 der Frobeniusautomorphismus τ, der x auf x^p $(x \in \mathbb{F}_q)$ abbildet. Bekanntermaßen kann eine zyklische Gruppe mehrere Erzeuger besitzen. Wenn k die Ordnung und π ein Erzeuger dieser Gruppe ist, so werden alle Erzuger durch π^j mit $1 \leq j < k$ bestimmt, für die $\mathrm{ggT}(j,k) = 1$ gilt. Wir können nun das folgende Lemma beweisen.

Lemma 2.30. *Es gelten die Bezeichnungen dieses Abschnitts. Dann haben alle Erzeuger der zyklischen Galoisgruppe $\bar{G}$ von $\mathbb{F}_q/\mathbb{F}_p$ den selben Zykeltyp, d.h. die Längen der elementfremden Zykel sind gleich.*

Beweis: Es seien π und $\tilde{\pi}$ zwei Erzeuger von $\bar{G}$ und es gelte die Zerlegung $\pi = \pi_1 \cdot \ldots \cdot \pi_u$ in elementfremde Zykel. Dann existiert ein $1 \leq j < k$ mit $\tilde{\pi} = \pi^j$ und $\mathrm{ggT}(j,k) = 1$. Es sei l die Länge eines beliebigen elementfremden Zykels π_i von π. Da die Zykellängen der elementfremden Zykeln die Ordnung k der Gruppe $\bar{G}$ teilen, folgt $\mathrm{ggT}(j,l) = 1$. Hieraus folgt aber, daß π_i^j wieder ein Zykel der Länge l ist. Damit ist die Behauptung gezeigt. □

Wir wollen an dieser Stelle anmerken, daß dieses Lemma auch für den relativen Fall gilt, d.h. für die allgemeine Version 2.27. Da in dem Satz nichts über die Permutation der Nullstellen in einem Zykel ausgesagt wird, können wir für unsere Betrachtung davon ausgehen, daß wir den Frobeniusautomorphismus bestimmt haben. Im nächsten Kapitel über $\mathfrak{p}$-adische Körper werden wir noch einmal auf diese Problematik zurückkommen.

6. Gitter und LLL-Reduktion

In diesem Abschnitt werden wir Gitter und die LLL-Reduktion von A.K. Lenstra, H.W. Lenstra und L. Lovasz einführen. Die LLL-Reduktion ist eine Reduktion der Basisvektoren eines Gitters, die 1982 in [LLL] entwickelt wurde. Sie wurde ursprünglich für die Faktorisierung von Polynomen mit ganzrationalen Koeffizienten eingeführt. Der Algorithmus hat allerdings gerade in vielen anderen Bereichen eine sehr große Bedeutung erlangt. So werden auch wir diesen Algorithmus zur Teilkörperberechnung einsetzen. Das Wesentliche an dieser Gitterreduktion ist einerseits die polynomielle Laufzeit und andererseits die Abschätzungen, die wir für eine LLL-reduzierte Basis angeben können.

Definition 2.31. *Gitter*

(1) *Sei $n \in \mathbb{N}$ und Λ eine Teilmenge eines n-dimensionalen Vektorraums $\mathbb{R}^n$. Λ heißt Gitter, wenn eine Basis $b_1, \dots, b_n$ von $\mathbb{R}^n$ existiert, so daß folgendes gilt:*

$$\Lambda = \sum_{i=1}^{n} \mathbb{Z} b_i = \{\sum_{i=1}^{n} r_i b_i : r_i \in \mathbb{Z}\ (1 \leq i \leq n)\}.$$

In diesem Fall heißt $b_1, \dots, b_n$ Basis und n der Rang oder die Dimension von Λ.

(2) *Die Determinante $d(\Lambda)$ des Gitters Λ ist definiert durch:*

$$d(\Lambda) = |\det(b_1, \dots, b_n)|,$$

wobei die b_i als Spaltenvektoren geschrieben werden. $d(\Lambda)$ ist eine positive reelle Zahl, die nicht von der Wahl der Basis abhängt (vgl. [Cas1]*).*

In der folgenden Definition werden Größen definiert, die beim Gram-Schmidt-Orthogonalisierungsverfahren benötigt werden.

Definition 2.32. *Seien $b_1, \dots, b_n \in \mathbb{R}^n$ linear unabhängig. Die Vektoren b_i^* $(1 \leq i \leq n)$ und die reellen Zahlen μ_{ij} $(1 \leq j < i \leq n)$ werden dann induktiv wie folgt definiert:*

$$b_i^* = b_i - \sum_{j=1}^{i-1} \mu_{ij} b_j^*,$$

$$\mu_{ij} = \frac{(b_i, b_j^*)}{(b_j^*, b_j^*)},$$

wobei $(\cdot, \cdot)$ das kanonische innere Produkt auf dem $\mathbb{R}^n$ bezeichne.

DEFINITION 2.33. *Eine Basis $b_1, \ldots, b_n$ eines Gitters Λ heißt LLL-reduziert, falls die beiden folgenden Bedingungen erfüllt sind:*

$$| \mu_{ij} | \leq \frac{1}{2} \text{ für } 1 \leq j < i \leq n$$

$$| b_i^* + \mu_{ii-1} b_{i-1}^* |^2 \geq \frac{3}{4} | b_{i-1}^* |^2 \text{ für } 1 < i \leq n.$$

Hierbei bezeichne $| \cdot |$ die euklidische Länge.

Im weiteren kann man jetzt mehrere Abschätzungen für eine LLL-reduzierte Basis angeben, welche in [LLL, Poh] nachgelesen werden können. Wir benötigen lediglich das folgende:

SATZ 2.34. *Sei Λ ein Gitter mit LLL-reduzierter Basis $b_1, \ldots, b_n$. Dann gelten die beiden folgenden Abschätzungen.*

$$d(\Lambda) \leq \prod_{i=1}^{n} |b_i| \tag{2-1}$$

$$|b_1|^2 \leq 2^{n-1} |x|^2 \text{für alle } x \in \Lambda, x \neq 0 \tag{2-2}$$

Beweis: (2-1) ist die bekannte Hadamardsche Ungleichung. Die Gleichung (2-2) wird in [LLL] gezeigt. □

Wir haben jetzt einige Eigenschaften einer LLL-reduzierten Basis beschrieben. Bis jetzt ist offen geblieben, wie wir eine solche Basis berechnen können. Dieser Algorithmus wird z.B. in [LLL, Poh, PoZa] aufgeführt. Wir möchten daher an dieser Stelle darauf verzichten, diesen Algorithmus aufzuführen.

7. Kettenbruchentwicklung

In diesem Abschnitt werden wir die grundlegenden Begriffe der Kettenbruchentwicklung definieren. Wir benötigen die Kettenbruchentwicklung, um die Korrektheit unseres Einbettungsalgorithmus zu beweisen. Eine andere Anwendung der Kettenbruchentwicklung ist zum Beispiel das Erkennen von irrationalen Zahlen. So ist eine reelle Zahl genau dann rational, wenn ihre Kettenbruchentwicklung endlich ist. Kommen wir nun zu den wichtigsten Definitionen und Eigenschaften. Die Beweise dieser werden in [Khi] geführt. Dieses Buch sei auch denjenigen empfohlen, die mehr über die Kettenbruchentwicklung erfahren wollen. Anzumerken bleibt noch, daß wir in unserer Arbeit nur endliche Kettenbrüche über den natürlichen Zahlen betrachten. Deswegen werden wir hier auch nur diesen Spezialfall definieren.

Definition 2.35. *Kettenbrüche*

(1) *Einen Ausdruck der Form*

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cdots + \cfrac{1}{a_n}}}$$

bezeichnen wir als n*-gliedrigen Kettenbruch. Dabei soll* $a_0 \in \mathbb{Z}$ *und für* $1 \leq i \leq n$ $a_i \in \mathbb{N}$ *sein.*

(2) *Der einfacheren Schreibweise wegen schreiben wir einen solchen Kettenbruch in der Form:*

$$[a_0; a_1, a_2, \dots, a_n].$$

(3) *Ferner bezeichnen wir für* $0 \leq i \leq n$

$$r_k = [a_k; a_{k+1}, \dots, a_n]$$

als den Rest des endlichen Kettenbruches.

(4) *Einen Kettenbruch* $s_k = [a_0; a_1, \dots, a_k]$ *mit* $k \leq n$ *bezeichnen wir als Abschnitt des endlichen Kettenbruches* $[a_0; a_1, a_2, \dots, a_n]$.

Um besser arbeiten zu können, definieren wir rekursiv eine kanonische Darstellung für unsere Kettenbrüche: Für einen 0-gliedrigen Kettenbruch $[a_0]$ setzen wir die Darstellung $\frac{a_0}{1}$ und für n-gliedrige Kettenbrüche schreiben wir:

$$[a_0; a_1, a_2, \dots, a_n] = [a_0; r_1] = a_0 + \frac{1}{r_1}.$$

Dabei ist r_1 der Rest unseres Kettenbruches. Da r_1 selbst nur $(n-1)$-gliedrig ist, haben wir bereits eine kanonische Darstellung definiert. Es gilt: $r_1 = \frac{p'}{q'}$. Hieraus folgt dann:

$$[a_0; a_1, a_2, \dots, a_n] = a_0 + \frac{q'}{p'} = \frac{a_0 p' + q'}{p'}.$$

Dieser letzte Bruch soll die kanonische Darstellung unseres Kettenbruches sein.

Definition 2.36. *Die kanonischen Darstellungen des Abschnittes*

$$s_k = [a_0; a_1, \dots, a_k] \ (k \leq n)$$

definieren wir als Näherungsbruch der Ordnung k *von* $[a_0; a_1, a_2, \dots, a_n]$ *und bezeichnen ihn in der Form* $\frac{p_k}{q_k}$.

Im folgenden werden wir einige Ergebnisse auflisten, die wir für unsere Beweise in den späteren Kapiteln benötigen werden.

Satz 2.37. *Bildungsgesetz der Näherungsbrüche*

Für ein beliebiges $k \geq 1$ *gilt:*

$$p_k = a_k p_{k-1} + p_{k-2} \text{ und } q_k = a_k q_{k-1} + q_{k-2}.$$

Dabei setzen wir $p_{-1} = 1$ *und* $q_{-1} = 0$*.*

Beweis: Dieser Satz entspricht Satz 1 in [Khi]. □

Satz 2.38. *Für ein beliebiges* $1 \leq k \leq n$ *gilt:*

$$[a_0; a_1, a_2, \dots , a_n] = \frac{p_{k-1} r_k + p_{k-2}}{q_{k-1} r_k + q_{k-2}}.$$

Hierbei gehören die p_i, q_i *und* r_i *zu dem links in der Gleichung stehenden Kettenbruch.*

Beweis: Der Beweis steht in Satz 5 von [Khi]. □

Satz 2.39. *Jeder unkürzbare Bruch* $\frac{a}{b}$*, der der Ungleichung*

$$|\alpha - \frac{a}{b}| < \frac{1}{2b^2}$$

genügt, ist ein Näherungsbruch der Zahl α*. Hierbei ist* $\alpha = [a_0; a_1, a_2, \dots , a_n]$*.*

Beweis: Dieses Ergebnis wird in Satz 19 von [Khi] bewiesen. □

KAPITEL 3

Bewertungstheorie und $\mathfrak{p}$-adische Körper

Für die Durchführung unseres Algorithmus müssen wir Berechnungen in sogenannten p-adischen Vervollständigungen algebraischer Zahlkörper durchführen. Hierzu stellen wir nun die wichtigsten Ergebnisse dieser Theorie vor. Die folgenden Aussagen werden u.a. in [PoZa] und [Nar] bewiesen.

1. Bewertungen

Als erstes werden wir den Begriff einer Bewertung einführen.

DEFINITION 3.1. *Sei K ein Körper und $\psi : K \to \mathbb{R}$ eine Abbildung mit den folgenden Eigenschaften:*

(i) $\psi(1) = 1$
(ii) $\psi(x) \geq 0, \psi(x) = 0 \Leftrightarrow x = 0 \,; \forall x \in K$
(iii) $\psi(x \pm y) \leq \psi(x) + \psi(y) \,; \forall x, y \in K$
(iv) $\psi(x \cdot y) = \psi(x) \cdot \psi(y) \,; \forall x, y \in K$

ψ heißt dann Bewertung des Körpers K. Gilt statt (iii) die stärkere Bedingung

$$\psi(x \pm y) \leq \max(\psi(x), \psi(y)); \forall x, y \in K,$$

so bezeichnen wir ψ als nicht-archimedische Bewertung des Körpers K, oder kurz als Krullbewertung. Andernfalls bezeichnen wir ψ als archimedische Bewertung.

BEMERKUNG 3.2. *Ist ψ eine Bewertung des Körpers K, so wird durch*

$$d(x, y) := \psi(x - y)$$

eine Metrik auf K definiert.

Damit wir den Begriff der Bewertung etwas besser verstehen können, betrachten wir drei Beispiele von Bewertungen. Hierbei ist für uns besonders das 3. Beispiel von besonderer Bedeutung.

Beispiel 3.3. *(Archimedische und nicht-archimedische Bewertungen)*

(i) *Die triviale Abbildung*

$$\psi : K \to \mathbb{R} : x \mapsto \begin{cases} 0 & \textit{falls } x = 0 \\ 1 & \textit{sonst} \end{cases}$$

ist immer eine nicht-archimedische Bewertung.

(ii) *Der gewöhnliche Absolutbetrag ist eine archimedische Bewertung auf* $\mathbb{Q}$.

(iii) *Sei* K *ein algebraischer Zahlkörper und* $\mathfrak{p}$ *ein Primideal in* $\mathfrak{o}_K$. *Sei die Funktion* $\nu_\mathfrak{p}$ *wie in 2.13 definiert. Dann wird durch*

$$|x|_{\mathfrak{p},\gamma} := \begin{cases} \gamma^{\nu_\mathfrak{p}(x)} & \textit{falls } x \neq 0 \\ 0 & \textit{falls } x = 0 \end{cases}$$

mit $\gamma \in]0,1[$ *eine nicht-archimedische Bewertung auf* K *definiert. Wir nennen eine solche Bewertung eine* $\mathfrak{p}$*-adische Bewertung auf* K.

Definition 3.4. *Eigenschaften von Bewertungen*

(i) *Es seien* ψ_1 *und* ψ_2 *zwei Bewertungen auf einem Körper* K. *Dann heißen diese Bewertungen äquivalent, falls*

$$\forall \gamma, \delta \in K \; : \; \psi_1(\gamma) < \psi_1(\delta) \Leftrightarrow \psi_2(\gamma) < \psi_2(\delta)$$

gilt.

(ii) *Ist* ψ *eine Krullbewertung, deren Bild des Definitionsbereiches zyklisch ist, so heißt* ψ *diskret.*

Satz 3.5. *Es sei* ψ *eine Krullbewertung auf einem Körper* K. *Dann ist*

$$R_\psi := \{x \in K \mid \psi(x) \leq 1\}$$

ein lokaler Ring mit dem maximalen Ideal

$$m_\psi := \{x \in K \mid \psi(x) < 1\}.$$

Wir bezeichnen R_ψ als den Bewertungsring und m_ψ als das Bewertungsideal von ψ.

Da wir sehr an Bewertungen auf algebraischen Zahlkörpern interessiert sind, stellt sich uns die Frage, wie diese dort aussehen. Hierauf gibt uns der folgende Satz eine Antwort.

SATZ 3.6. *Es sei K ein algebraischer Zahlkörper über $\mathbb{Q}$. Dann ist jede nicht triviale Bewertung von K entweder diskret oder archimedisch. Ist ψ eine diskrete Bewertung, so existiert ein Primideal $\mathfrak{p}$ von $\mathfrak{o}_K$ und ein $\gamma \in]0,1[$ mit:*

$$\psi(x) = \gamma^{\nu_{\mathfrak{p}}(x)} \qquad \forall x \in K^{\neq 0}$$

Ist ψ aber eine archimedische Bewertung auf K, so gilt

$$\psi(x) = |\Phi(x)| \qquad \forall x \in K,$$

wobei Φ einer der $\mathbb{Q}$-Isomorphismen von K ist.

Um mit den Bewertungen besser arbeiten zu können, ist der folgende Satz von großer Bedeutung.

SATZ 3.7. *Es sei ψ eine beliebige diskrete Bewertung über einem algebraischen Zahlkörper K. Dann hat sie nach dem vorherigen Satz die Form $\psi(x) = \gamma^{\nu_{\mathfrak{p}}(\cdot)}$ für ein $\gamma \in]0,1[$. Eine Bewertung $\tilde{\psi}$ auf K ist genau dann äquivalent zu ψ, wenn ein $\delta \in]0,1[$ existiert, so daß $\tilde{\psi} = \delta^{\nu_{\mathfrak{p}}(\cdot)}$ gilt. Weiterhin besitzen äquivalente Bewertungen den gleichen Bewertungsring und das gleiche Bewertungsideal.*

In 3.3 haben wir die Bewertung $|\cdot|_{\mathfrak{p},\gamma}$ über dem algebraischen Zahlkörper K definiert. Da wir nicht an den eigentlichen Funktionswerten dieser Bewertung, sondern an dem Bewertungsring und dem Bewertungsideal interessiert sind, ist das γ für uns von untergeordneter Bedeutung. Wir sprechen daher für ein beliebiges Primideal von $\mathfrak{o}_K$ von der Bewertung $|\cdot|_{\mathfrak{p}}$ und meinen eine beliebige von $\mathfrak{p}$ erzeugte Bewertung.

2. $\mathfrak{p}$-adische Körper

Eine sehr wichtige Eigenschaft bildet die Vervollständigung algebraischer Zahlkörper bezüglich eine Primideals $\mathfrak{p}$. Dazu betrachten wir den folgenden Satz.

SATZ 3.8. *Es sei K ein algebraischer Zahlkörper und $\mathfrak{p}$ ein Primideal seiner Maximalordnung. Dann existiert ein Körper $K_{\mathfrak{p}} \supseteq K$ mit den f olgenden Eigenschaften:*

(i) *$K_{\mathfrak{p}}$ ist vollständig bzgl. der von der Fortsetzung von $|\cdot|_{\mathfrak{p}}$ auf $K_{\mathfrak{p}}$ erzeugten Metrik. Diese Fortsetzung wird ebenfalls mit $|\cdot|_{\mathfrak{p}}$ bezeichnet.*

(ii) *K liegt dicht in $K_{\mathfrak{p}}$.*

(iii) *Ist $\mathcal{R}$ ein minimales Restsystem von $\mathfrak{o}_K/\mathfrak{p}$ mit $0 \in \mathcal{R}$ und ist $\pi \in \mathfrak{p} \setminus \mathfrak{p}^2$, so gilt:*

$$K_{\mathfrak{p}} = \{\sum_{i=m}^{\infty} \alpha_i \pi^i \mid \alpha_i \in \mathcal{R}, m \in \mathbb{Z}, \alpha_m \neq 0\}.$$

Die Fortsetzung von $|\cdot|_{\mathfrak{p}}$ auf $K_{\mathfrak{p}}$ ist wieder eine diskrete Bewertung. Damit ist

$$R_{\mathfrak{p}} = \{\sum_{i=m}^{\infty} \alpha_i \pi^i \mid \alpha_i \in \mathcal{R}, m \in \mathbb{Z}^{\geq 0}, \alpha_m \neq 0\}$$

der Bewertungsring von $|\cdot|_{\mathfrak{p}}$ in $K_{\mathfrak{p}}$. Er ist ein lokaler Hauptidealring mit dem maximalen Ideal

$$m_{\mathfrak{p}} = \{\sum_{i=m}^{\infty} \alpha_i \pi^i \mid \alpha_i \in \mathcal{R}, m \in \mathbb{Z}^{\geq 1}, \alpha_m \neq 0\}.$$

Weiterhin wollen wir noch anmerken, daß die Restklassenkörper $R_{\mathfrak{p}}/m_{\mathfrak{p}}$ und $\mathfrak{o}_K/\mathfrak{p}$ isomorph zueinander sind.

3. Erweiterungen von $\mathfrak{p}$-adischen Körpern

In diesem Abschnitt werden wir einige Aussagen über $\mathfrak{p}$-adische Erweiterungen treffen.

SATZ 3.9. *Es sei $M/K_{\mathfrak{p}}$ eine endliche Erweiterung vom Grad n. Dann existiert eine bis auf Äquivalenz eindeutige Fortsetzung $|\cdot|$ von $|\cdot|_{\mathfrak{p}}$ auf M mit:*

(i) *M ist vollständig bzgl. $|\cdot|$.*

(ii) *$|x| = |N_{M/K_{\mathfrak{p}}}(x)|_{\mathfrak{p}}^{1/n}\ \forall x \in M$.*

DEFINITION 3.10. *Es sei $M/K_{\mathfrak{p}}$ eine endliche Erweiterung vom Grad n. $\mathfrak{p}$ ist das Primideal des Bewertungrings S von $K_{\mathfrak{p}}$ und $\mathfrak{P}$ das Primideal des Bewertungrings R von M. Die Zahl e mit der Eigenschaft $\mathfrak{p}R = \mathfrak{P}^e$ heißt Verzweigungsindex der Erweiterung $M/K_{\mathfrak{p}}$. Die Zahl $f = [(R/\mathfrak{P}) : (S/\mathfrak{p})]$ heißt Trägheitsgrad der Erweiterung $M/K_{\mathfrak{p}}$. Es gilt bekanntlich $n = ef$. Eine Erweiterung heißt unverzeigt, falls $e = 1$ ist.*

SATZ 3.11. *Es sei K/L eine Relativerweiterung vom Grad n und $|\cdot|_{\mathfrak{p}}$ eine Bewertung auf L. Gilt dann $\mathfrak{p}\mathfrak{o}_K = \mathfrak{P}_1^{e_1} \cdot \ldots \cdot \mathfrak{P}_g^{e_g}$, so sind die Bewertungen $|\cdot|_{\mathfrak{P}_i}$ $(1 \leq i \leq g)$ alle inäquivalenten Fortsetzungen von $|\cdot|_{\mathfrak{p}}$ nach K.*

SATZ 3.12. *Mit den Bezeichnungen des letzten Satzes gilt:*

$$e_i = e(K_{\mathfrak{P}_i}/L_{\mathfrak{p}}) \text{ und } f(\mathfrak{P}_i/\mathfrak{p}) = f(K_{\mathfrak{P}_i}/L_{\mathfrak{p}}).$$

4. Unverzweigte $\mathfrak{p}$-adische Erweiterungen

Wir hatten schon einmal kurz erwähnt, daß wir nur an unverzweigten $\mathfrak{p}$-adischen Erweiterungen interessiert sind. Diese haben einige sehr schöne Eigenschaften, die wir im folgenden auflisten wollen. Sei also $K_{\mathfrak{p}}/\mathbb{Q}_p$ eine $\mathfrak{p}$-adische Erweiterung. Sie heißt unverzweigt genau dann, wenn der Verzweigungsindex e von $\mathfrak{p}$ über $p\mathbb{Z}_p$ gerade 1 ist. Die folgenden Aussagen werden in [Nar] bewiesen. In den folgenden Sätzen sei $K_{\mathfrak{P}}/L_{\mathfrak{p}}$ eine $\mathfrak{p}$-adische Erweiterung. R sei der Bewertungsring von K und S der Bewertungsring von L. $\mathfrak{P}$ und $\mathfrak{p}$ seien die Bewertungsideale von K bzw. L.

SATZ 3.13. *Eine Erweiterung $K_{\mathfrak{P}}/L_{\mathfrak{p}}$ ist unverzweigt genau dann, wenn ein Element $a \in R$ existiert, für das die folgenden Bedingungen erfüllt sind:*

(i) $L = K(a)$, *wobei a Nullstelle eines normierten Polynoms $F \in S[t]$ ist.*
(ii) $a \bmod \mathfrak{P}$ *ist eine einfache Nullstelle von* $F \bmod \mathfrak{p}$.

Aus diesem Satz können wir mehrere einfache Folgerungen ziehen.

KOROLLAR 3.14. *Es sei $K_{\mathfrak{P}}/L_{\mathfrak{p}}$ eine unverzweigte und $M/\mathbb{Q}_p$ eine endliche Erweiterung. Dann ist $K_{\mathfrak{P}}M/L_{\mathfrak{p}}M$ wieder eine unverzweigte Erweiterung.*

KOROLLAR 3.15. *Es seien $K_{\mathfrak{P}}/L_{\mathfrak{p}}$ und $M/L_{\mathfrak{p}}$ unverzweigte Erweiterungen. Dann sind $MK_{\mathfrak{P}}/L_{\mathfrak{p}}$ wieder unverzeigt.*

Im folgenden bezeichnen wir mit $\bar{K}$ und $\bar{L}$ die zugehörigen Restklassenkörper. Der folgende Satz stellt eine wichtige Beziehung zwischen unverzweigten Erweiterungen und den endlichen Körpern auf.

SATZ 3.16. *Es sei $L_{\mathfrak{p}}/\mathbb{Q}_p$ eine $\mathfrak{p}$-adische Erweiterung. Dann existiert zu jeder endlichen Erweiterung $\bar{K}/\bar{L}$ genau eine unverzweigte Erweiterung $K_{\mathfrak{P}}/L_{\mathfrak{p}}$ derart, daß $\bar{K}$ und der Restklassenkörper von $K_{\mathfrak{P}}$ isomorph zueinander sind. Diese Erweiterung ist normal und die Galoisgruppe ist isomorph zu der Galoisgruppe von $\bar{K}/\bar{L}$.*

Aus diesem Satz können wir wieder wichtige Folgerungen ziehen.

KOROLLAR 3.17. *Es existiert genau eine unverzweigte Erweiterung von $\mathbb{Q}_p$ mit fest vorgebenen Grad.*

KOROLLAR 3.18. *Falls $K_{\mathfrak{P}}/L_{\mathfrak{p}}$ unverzweigt ist, so ist die Galoisgruppe zyklisch. Ein Erzeuger dieser zyklischen Gruppe ist der sogenannte Frobeniusautomorphismus. Er induziert den Frobeniusautomorphismus der Galoisgruppe von der Erweiterung der zugehörigen Restklassenkörper.*

Wir haben also festgestellt, daß es nur eine unverzweigte Erweiterung von $\mathbb{Q}_p$ gibt, die einen fest vorgegebenen Grad hat. Diese Erweiterung korrespondiert zu der Erweiterung der zugehörigen Restklassenkörper. So hat sie gleichen Grad und gleiche Galoisgruppe. Beide Galoisgruppen werden vom Frobeniusautomorphismus erzeugt.

Zum Abschluß dieses Abschnitts betrachten wir noch einen wichtigen Satz zur Darstellung des Bewertungsrings bzw. der Maximalordnung eines $\mathfrak{p}$-adischen Körpers, wie er in [Cas2] zu finden ist.

SATZ 3.19. *Es sei $K_{\mathfrak{p}}/\mathbb{Q}_p$ eine unverzweigte Erweiterung vom Grad m. Weiterhin seien $\beta_1, \ldots, \beta_m$ die Vertreter einer Basis von $(\mathfrak{o}_{K_{\mathfrak{p}}}/\mathfrak{p})/(\mathbb{Z}_p/p\mathbb{Z})$. Dann ist $\beta_1, \ldots, \beta_m$ eine Basis für die Maximalordnung $\mathfrak{o}_{K_{\mathfrak{p}}}$.*

Für die Praxis bedeutet dieser Satz, daß wir ein erzeugendes Polynom für die Körpererweiterung unseres Restklassenkörpers kanonisch in $\mathbb{Z}_p[t]$ einbetten. Die von diesem Polynom erzeugte Gleichungsordnung ist dann bereits maximal.

Zum Abschluß dieses Kapitels wollen wir noch eine Anwendung des van der Waerden-Kriteriums 2.28 vorstellen.

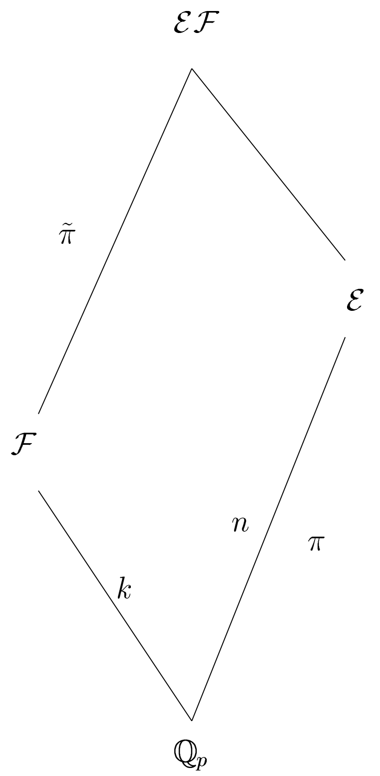
SATZ 3.20. *Sei $f \in \mathbb{Z}[t]$ ein irreduzibles, normiertes Polynom und sei ferner p eine Primzahl für die $f \bmod p$ keine doppelten Nullstellen besitzt. Sei π nun das Element der Galoisgruppe von f, welches durch 2.28 bestimmt wurde. Sei k ein Teiler des Grades der p-adischen Erweiterung $\mathcal{E}/\mathbb{Q}_p$, die durch f erzeugt wird. Dann erhält man durch durch das Faktorisieren von f in einer unverzweigten Erweiterung vom Grad k über $\mathbb{Q}_p$ die Aktion von π^k im Sinne von 2.28.*

BEMERKUNG 3.21. *Damit keine Mißverständnisse auftreten können, wollen wir an dieser Stelle bemerken, wie die Erweiterung $\mathcal{E}/\mathbb{Q}_p$ erzeugt wurde. Sei hierzu $\tilde{f}$ die kanonische Einbettung von f in $\mathbb{Z}_p[t]$. Die Nullstellen von $\tilde{f}$ seien mit $\tilde{\alpha}_1, \ldots, \tilde{\alpha}_n$ bezeichnet. Dann ist $\mathcal{E} = \mathbb{Q}_p(\tilde{\alpha}_1, \ldots, \tilde{\alpha}_n)$.*

Wir kommen nun zum Beweis des Satzes.

Beweis: Die unverzweigte Erweiterung vom Grad k über $\mathbb{Q}_p$ sei mit $\mathcal{F}$ bezeichnet. Sei $\mathfrak{p}$ das maximale Ideal in der Maximalordnung $\mathfrak{o}_{\mathcal{F}}$ von $\mathcal{F}$. Das Faktorisieren von

f in $\mathcal{F}[t]$ entspricht der Faktorisierung von f mod $\mathfrak{p}$. Mittels dieser Faktorisierung wird nach 2.28 der Frobeniusautomorphismus $\tilde{\pi}$ der Erweiterung $\mathcal{E}\mathcal{F}/\mathcal{F}$ ausgerechnet. In der Voraussetzung hatten wir bereits den Frobeniusautomorphismus π der Erweiterung $\mathcal{E}/\mathbb{Q}_p$ bestimmt. Wir zeigen nun, daß für die Frobeniusautomorphismen der Zusammenhang $\pi^k = \tilde{\pi}|_{\mathcal{E}}$ gilt. Hierzu betrachten wir folgende Abbildung:



Wir bezeichnen den Frobeniusautomorphismus von $\mathcal{E}\mathcal{F}/\mathbb{Q}_p$ mit η. Aus der Galoistheorie ist bekannt, daß $\tilde{\pi} = \eta^k$ gilt. Weiterhin ist offensichtlich, daß $\pi = \eta|_{\mathcal{E}}$ gilt. Damit erhalten wir folgende Gleichung:

$$\tilde{\pi}|_{\mathcal{E}} = \eta^k|_{\mathcal{E}} = \pi^k.$$

Da die Nullstellen von f alle in $\mathcal{E}$ liegen und wir an der Aktion von $\tilde{\pi}$ auf diesen Nullstellen interessiert sind, ist damit die gewünschte Behauptung gezeigt. □

KAPITEL 4

Imprimitivitätsgebiete und Blöcke

Als Generalvoraussetzung für dieses Kapitel sei G Untergruppe der symmetrischen Gruppe $\mathfrak{S}_n$. Dabei soll G stets auf $\Omega = \{\alpha_1, \dots, \alpha_n\}$ operieren. Zusätzlich sei $\pi = \pi_1 \cdot \ldots \cdot \pi_u \in G$ stets in elementfremde Zykel zerlegt.

1. Einführung

DEFINITION 4.1. *Eigenschaften von G*

(1) *G heißt transitiv, falls für alle $1 \leq i, j \leq n$ ein $g \in G$ existiert mit $g\alpha_i = \alpha_j$.*
(2) *Sei $\Delta \subseteq \Omega$ und $g \in G$. Dann ist $\Delta^g := \{\alpha \in \Omega \mid \alpha = g\beta \text{ mit } \beta \in \Delta\}$.*
(3) *Sei $\emptyset \neq \Delta \subseteq \Omega$. Dann heißt Δ Block (Imprimitivitätsgebiet), falls für alle $g \in G$ gilt: $\Delta^g \cap \Delta \in \{\emptyset, \Delta\}$.*
(4) *$\Delta = \{\alpha_i\}\,(1 \leq i \leq n)$ und $\Delta = \Omega$ sind die sogenannten trivialen Blöcke, die anderen heißen nicht triviale Blöcke.*
(5) *Sei G transitiv. Falls G einen nicht trivialen Block besitzt, so heißt G imprimitiv, andernfalls heißt G primitiv.*
(6) *Die Anzahl der Elemente eines Blockes wird als Größe bzw. als Blockgröße bezeichnet.*
(7) *Blöcke $\Delta_1, \dots, \Delta_m$ heißen (komplettes) Blocksystem von G, falls folgendes gilt:*
    (a) $\bigcup_{1 \leq i \leq m} \Delta_i = \Omega$.
    (b) $\Delta_i \cap \Delta_j = \emptyset$ *für* $i \neq j$.
    (c) *Alle Blöcke haben die gleiche Blockgröße.*
(8) *Die Blöcke, die in einem Blocksystem liegen, heißen zueinander konjugiert.*

Der folgende Satz beinhaltet die ersten einfachen Folgerungen aus der Definition von Blöcken. Der Beweis kann [Hup] entnommen werden.

SATZ 4.2. *Sei G imprimitiv und sei Δ ein nicht trivialer Block. Sei $H := G_{\{\Delta\}} := \{g \in G \mid \Delta^g = \Delta\}$. Sei weiterhin $G = \bigcup_{r \in R} Hr$ die Nebenklassenzerlegung von G nach H. Dabei sei R ein vollständiges, minimales Restsystem. Dann gelten folgende Behauptungen:*

(1) *Es ist $\Omega = \bigcup_{r \in R} \Delta^r$ mit $\Delta^r \cap \Delta^{r'} = \emptyset$ für $r \neq r'\,(r, r' \in R)$.*
(2) *Mit Δ ist für $g \in G$ auch Δ^g ein Block.*
(3) *Es gilt: $\mid \Omega \mid = \mid \Delta \mid \mid R \mid$.*
(4) *Die Untergruppe H ist transitiv auf Δ.*

Insbesondere bilden die Δ^r, $r \in R$ ein Blocksystem von G.

2. Eigenschaften von Blöcken

In diesem Abschnitt wollen wir Eigenschaften von Blöcken Δ einer Gruppe G herleiten. Grundlage hierfür ist die Kenntnis von einzelnen Elementen der Gruppe G. Die Untersuchung dieses Sachverhalts ist deswegen von besonderer Bedeutung, da wir mit Hilfe des van der Waerden-Kriteriums 2.28 zyklische Untergruppen der Galoisgruppe G und deren Erzeuger π erkennen können.

Wirr können nun die folgenden Begriffe definieren.

DEFINITION 4.3. *Bezeichnungen für Zykel*

(1) *Die Anzahl der Elemente, die in einem Zykel π permutiert werden, bezeichnen wir als Länge eines Zykels.*
(2) *Wir sagen ein Element π ist vom Zykeltyp $[n_1, \ldots, n_u]$, wenn die Länge der π_i gerade den $n_i\,(1 \leq i \leq u)$ entspricht.*

O.E. seien die $\pi_i\,(1 \leq i \leq u)$ gemäß ihrer Länge aufsteigend geordnet. Das folgende Lemma liefert uns eine erste Eigenschaft.

LEMMA 4.4. *Sei G transitiv und Δ ein Block von G. Sei k die kleinste Zahl mit $\Delta^{\pi^k} = \Delta$. Falls ein Zykel π_l der Länge n_l ein Element von einem Block Δ enthält, so wird n_l von k geteilt und π_l enthält exakt $\frac{n_l}{k}$ Elemente von Δ.*

Beweis: Sei Δ ein nicht trivialer Block. Wegen $\Delta \cap \Delta^{\pi} \in \{\emptyset, \Delta\}$ existiert ein $k \geq 1$ mit $\Delta^{\pi^k} = \Delta$ und $\Delta^{\pi^j} \cap \Delta = \emptyset$ für $1 \leq j < k$. Seien o.E. die $\alpha_i\,(1 \leq i \leq n)$ so angeordnet, daß $\pi_l = (\alpha_1 \ldots \alpha_{n_l})$ und $\alpha_1 \in \Delta$ gilt. Wegen $\pi_l^{n_l} = id$ folgt $\Delta^{\pi^{n_l}} \cap \Delta \neq \emptyset$. Da k die kleinste Zahl mit dieser Eigenschaft war, wird n_l von k geteilt. π_l^k zerfällt somit in k Zykel der Länge $\frac{n_l}{k}$ und es gelte, daß α_1 im ersten der so entstandenen Zykel enthalten ist. Wären noch in einem weiteren so entstandenem Zykel Elemente aus Δ enthalten, so müßten alle Elemente dieses Zykels in Δ enthalten sein. Da jeder Zykel von π_l^k genau ein Element von $\{\alpha_1, \ldots, \alpha_k\}$ enthält, müßte ein $\alpha_i\,(2 \leq i \leq k)$ in diesem weiteren Zykel enthalten sein. Dann gilt aber $\pi_l^{i-1}\alpha_1 = \alpha_i$ und somit ist $\alpha_i \in \Delta \cap \Delta^{\pi^{i-1}}$ mit $(i-1) < k$. Dies ist aber ein Widerspruch. $\square$

Das k im Lemma ist von so großer Bedeutung für unsere weiteren Betrachtungen, daß wir dies in einer Definition festhalten wollen.

Definition 4.5. *Sei G transitiv und Δ ein Block von G. Dann ist der k-Wert $k(\Delta, \pi)$ als die kleinste natürliche Zahl definiert, mit $\Delta^{\pi^k} = \Delta$. Wenn klar ist, auf welches π sich der k-Wert bezieht, so wird dies meistens weggelassen. Falls $\Delta_1, \ldots, \Delta_m$ ein komplettes Blocksystem ist, so bezeichnen $k_1, \ldots, k_m$ die k-Werte zu $\Delta_1, \ldots, \Delta_m$ (bezogen auf eine feste Permutation π).*

Generalvoraussetzung:

Im folgenden sei $\Delta_1, \ldots, \Delta_m$ ein komplettes Blocksystem von Blöcken der Größe d einer Gruppe G. Mit $k_1, \ldots, k_m$ werden die k-Werte zu $\Delta_1, \ldots, \Delta_m$ bezeichnet.

In den folgenden Sätzen wird eine noch genauere Aussage über die Verteilung der α_i in den Blöcken Δ_j getroffen.

Satz 4.6. *Wenn zwei Blöcke Δ_r und Δ_s mit $r \neq s$ Elemente eines Zykels π_l enthalten, so folgt $k_r = k_s$.*

Beweis: Offensichtlich gelten $k_r, k_s > 1$. O.E. seien die Elemente aus Ω so angeordnet, daß $\pi_l = (\alpha_1 \ldots \alpha_{n_l})$ und $\alpha_1 \in \Delta_r$ gilt. Dann existiert ein $j \in \mathbb{N}$ minimal mit $\pi_l^j \alpha_1 \in \Delta_s$. Wegen 4.2 (2) wird durch π_l^j jedes Element von $(\alpha_1 \ldots \alpha_{n_l}) \cap \Delta_r$ auf ein Element aus $(\alpha_1 \ldots \alpha_{n_l}) \cap \Delta_s$ abgebildet. Analog existiert ein $\tilde{j}$, so daß durch $\pi_l^{\tilde{j}}$ jedes Element von $(\alpha_1 \ldots \alpha_{n_l}) \cap \Delta_s$ auf ein Element aus $(\alpha_1 \ldots \alpha_{n_l}) \cap \Delta_r$ abgebildet wird. Damit ist gezeigt, daß diese beiden Mengen gleich mächtig sind und es folgt $k_r = k_s$. $\square$

Satz 4.7. *Es enthalte sowohl Δ_r als auch Δ_s Elemente eines Zykels π_l. Für $1 \leq i \leq u$ gilt dann: Falls Δ_r Elemente aus π_i enthält, so auch Δ_s (und umgekehrt).*

Beweis: Nach 4.6 enthalten Δ_r und Δ_s jeweils gleichviele Elemente von π_l. Seien nun α und β Elemente von π_l und gelte $\alpha \in \Delta_r$ und $\beta \in \Delta_s$. Dann existiert ein $j \in \mathbb{N}$ mit $\pi^j\alpha = \beta$. Sei nun γ ein beliebiges anderes Element aus Δ_r, welches nicht in π_l enthalten ist. Falls ein solches Element nicht existiert, ist die Aussage trivial. Nach 4.2 (2) gehört $\pi^j\gamma = \delta$ zum selben Block wie $\pi^j\alpha = \beta$. Weiterhin gehören nach Konstruktion γ und δ dem selben Zykel π_i an. Damit ist die Behauptung gezeigt. □

Korollar 4.8. *Sei Δ ein Block von G. Sei k der zugehörige k-Wert zu Δ. Dann sind durch Δ die $k-1$ konjugierten Blöcke, die Elemente aus den selben Zykeln enthalten wie Δ, eindeutig bestimmt und konstruierbar.*

Beweis: Sei $\pi \in G$ mit dem zugehörigen k-Wert gegeben. Nach den vorangegangenen Sätzen ist es klar, daß es genau $k-1$ konjugierte Blöcke gibt, die Elemente aus den gleichen Zykeln wie Δ entnehmen. Sei Δ aus s Zykeln konstruiert und seien diese Zykel so aufgebaut, daß jeweils das erste Element zu Δ gehört. Analog zu den vorangegangenen Sätzen wird Δ durch π^j $(1 \leq j < k)$ auf die konjugierten Blöcke abgebildet. Dies bedeutet, daß in jedem der s Zykel je eins der ersten k Elemente zu einem konjugierten Block von Δ gehört. □

Die Konstruierbarkeit basiert allerdings auf der Annahme, daß die Aktion von π auf Ω vollständig bekannt ist. Dies ist bei unserer Anwendung i.allg. aber nicht der Fall. Deswegen beschäftigen sich in den nächsten Abschnitten noch weitere Sätze mit diesem Problem.

3. Blöcke der Galoisgruppe von endlichen Erweiterungen von $\mathbb{F}_p$

In diesem Abschnitt sollen die Ergebnisse, die wir bisher über Blöcke erhalten haben, angewendet werden. Bekanntermaßen sind endliche Erweiterungen von endlichen Körpern galoissch mit zyklischer Galoisgruppe G. Die Elemente aus Ω werden ab jetzt auch als Wurzeln bezeichnet. Wir betrachten im weiteren folgende Ausgangsposition als weitere **Generalvoraussetzung** für den Rest dieses Kapitels:

Sei $f \in \mathbb{Z}[t]$ normiert und irreduzibel, und sei ein $p \in \mathbb{P}$ derart gegeben, daß $f(t) \bmod p\mathbb{Z}[t]$ keine doppelten Nullstellen besitzt. Weiterhin gelte:

$$f(t) \equiv f_1(t) \cdot \ldots \cdot f_u(t) \bmod p\mathbb{Z}[t],$$

wobei die f_i $(1 \leq i \leq u)$ in $\mathbb{F}_p[t]$ irreduzibel sind.

Nach dem van der Waerden-Kriterium 2.28 enthält Gal(f) (betrachtet als Erweiterung über $\mathbb{Q}$) eine zyklische Untergruppe H mit Erzeuger π, wobei π vom Zykeltyp $[n_1, \ldots, n_u]$ ist. Die $n_i\,(1 \leq i \leq u)$ entsprechen dabei gerade den Graden der f_i. Ein „Schönheitsfehler" dieser Aussage ist, daß man die Wurzeln nicht richtig unterscheiden kann. Dazu soll der folgende Satz, der auf 4.8 aufbaut, einen Lösungsansatz aufzeigen.

Satz 4.9. *Sei π der Erzeuger einer zyklischen Untergruppe H von G, wobei die $\pi_i\,(1 \leq i \leq u)$ auf den Wurzeln der f_i operieren. Sei nun Δ ein Block von G. Dann können die zu Δ konjugierten Blöcke, die aus den selben Zykeln konstruiert sind, modulo p eindeutig bestimmt werden.*

Bemerkung 4.10. *An dieser Stelle wollen wir die Aussage des letzten Satzes verdeutlichen. Wir haben schon öfters erwähnt, daß wir mit Hilfe des van der Waerden-Kriteriums* 2.28*, die Nullstellen in einem Block nur modulo p, d.h. im zugehörigen endlichen Körper, bestimmen können. Auf diese Art und Weise ist die Konstruierbarkeit zu verstehen.*

Kommen wir nun zum Beweis des Satzes.

Beweis: π ist Erzeuger der zyklischen Galoisgruppe von $\mathbb{F}_q/\mathbb{F}_p$, wobei $\mathbb{F}_q = \mathbb{F}_p(\alpha_1, \ldots, \alpha_n)$ ist. Die $\alpha_1, \ldots, \alpha_n$ sollen hierbei die Nullstellen von f in einer passenden Erweiterung von $\mathbb{F}_p$ sein. Ein Erzeuger dieser Galoisgruppe ist nach 2.23 durch den Frobeniusautomorphismus ϕ mit $\phi(x) = x^p$ gegeben. Seien nun die Zykel, die Elemente von Δ enthalten, so angeordnet, daß jeweils die erste Wurzel zu Δ gehört. Die Elemente des i-ten Zykels seien mit $\alpha_{i_1}, \ldots, \alpha_{i_{n_i}}$ bezeichnet. Dann gilt mit dem Frobeniusautomorphismus: $\alpha_{i_j} = \alpha_{i_1}^{p^{j-1}}$. Damit können die gewünschten konjugierten Blöcke bestimmt werden. □

4. Der Zusammenhang zwischen Blöcken und Teilkörpern

In diesem Abschnitt betrachten wir den Zusammenhang zwischen den Teilkörpern von $K = \mathbb{Q}(\alpha)$ und den Blöcken von $G =$Gal(f), wobei α Nullstelle eines irreduziblen und normierten Polynoms $f \in \mathbb{Z}[t]$ ist. Dabei stellt sich heraus, daß ähnlich zum Hauptsatz der Galoistheorie eine Bijektion zwischen den Teilkörpern von K und den Blöcken von G existiert, die α enthalten. Mit Hilfe dieser Aussage können wir dann die bisherigen Ergebnisse über Blöcke anwenden und diese zur Teilkörperberechnung einsetzen. Das folgende Ergebnis kann [Dix1] entnommen werden.

SATZ 4.11. *Sei $f \in \mathbb{Z}[t]$ normiert und irreduzibel vom Grad n, und sei α eine Nullstelle von f. Sei weiterhin $K = \mathbb{Q}(\alpha)$ ein algebraischer Zahlkörper und $G = Gal(f)$. Dann existiert eine Bijektion zwischen den Teilkörpern von K vom Grad m und den Blöcken der Größe d von G, die α enthalten. Zusätzlich gilt $n = md$.*

Beweis: Sei L ein beliebiger Teilkörper von K. Dann existiert nach dem Hauptsatz der Galoistheorie eine Untergruppe H von G mit $L = \text{Fix}(H)$. Sei $G_\alpha = \{g \in G \mid g\alpha = \alpha\}$ der Stabilisator von α in G. Dann ist $K = \mathbb{Q}(\alpha) = \text{Fix}(G_\alpha)$ und für H gilt die Beziehung $G_\alpha < H < G$. Sei Δ die Bahn (Orbit) von α unter H, d.h. $\Delta = \{h\alpha \mid h \in H\}$. Wir zeigen nun mit Hilfe der Definition 4.1, daß Δ ein Block ist. Sei hierzu ein $g \in G$ beliebig gewählt. Wir unterscheiden im folgenden 2 Fälle:

(1) Sei $g \in H$. Wähle nun $\beta \in \Delta$ beliebig. Dann existiert ein $h \in H$, so daß $h\alpha = \beta$ gilt. Hieraus folgt $g\beta \in \Delta$ wegen $g\beta = gh\alpha = \tilde{h}\alpha$ mit $\tilde{h} \in H$. Damit ist gezeigt, daß $\Delta^g = \Delta$ gilt.

(2) Sei $g \in G \setminus H$. Im folgenden zeigen wir, daß $\Delta^g \cap \Delta = \emptyset$ gilt. Wir nehmen hierzu an, daß ein $\beta \in \Delta$ existiere mit $g\beta \in \Delta$. Nun existiert ein $\tilde{h} \in H$ mit $\tilde{h}\alpha = \beta$. Setze $\tilde{g} = g\tilde{h} \in G \setminus H$. Wegen $\tilde{g}\alpha \in \Delta$ existiert ein $h \in H$ mit $h\tilde{g}\alpha = \alpha$. Damit gilt dann $h\tilde{g} \in G_\alpha$ und somit $h\tilde{g} \in H$. Hieraus folgt aber, daß $\tilde{g} \in H$ ist, was zu einem Widerspruch führt.

Damit haben wir sowohl die Blockeigenschaft von Δ als auch $H = G_{\{\Delta\}}$ gezeigt. Wegen $H = G_{\{\Delta\}}$ ist Δ der eindeutig bestimmte Block zu L, der α enthält.

Sei nun umgekehrt Δ ein Block, der α enthält. Definiere $L := \text{Fix}(G_{\{\Delta\}})$. Wegen $G_\alpha < G_{\{\Delta\}} < G$ ist L nach Galoistheorie ein Teilkörper von K. Damit haben wir die gewünschte Bijektion gezeigt.
Die Gradaussage folgt wegen $\mid \Delta \mid = \mid G_{\{\Delta\}} : G_\alpha \mid = (K : L) = d$. Somit ist $\frac{n}{d} = m$ der Grad von L. □

Im obigen Satz haben wir den Zusammenhang zwischen den Blöcken und den Teilkörpern gezeigt. Mit Hilfe dieser Aussage können wir zwei Korollare zeigen, die uns eine gewisse Einsicht in die Teilkörperproblematik liefern.

KOROLLAR 4.12. *Sei $f \in \mathbb{Z}[t]$ vom Grad n irreduzibel, normiert und sei Gal(f) $= \mathfrak{S}_n$ oder $\mathfrak{A}_n$ (alternierende Gruppe). Dann ist $K = \mathbb{Q}(\alpha)$ mit α Nullstelle von f primitiv, d.h. K besitzt keine echten Teilkörper.*

Beweis: Sei $G = \text{Gal}(f) = \mathfrak{S}_n$. Dann enthält G eine Permutation vom Zykeltyp $[1, n-1]$. O.E. sei α im Zykel der Länge 1 enthalten. Es sei nun Δ ein beliebiger

Block, der α enthält. Wegen $\alpha \in \Delta^\pi \cap \Delta$ folgt $k(\Delta, \pi) = 1$. Damit kann Δ nur die Größe 1 oder n haben, d.h. Δ ist ein trivialer Block. Somit besitzt K nach obigen Satz keine echten Teilkörper.

Sei nun G =Gal$(f) = \mathfrak{A}_n$. Falls n gerade ist, wählen wir ein π wie im ersten Teil des Beweises. Sei also n ungerade. Wir wählen nun ein $\pi \in G$, welches vom Zykeltyp $[1, 1, n-2]$ ist. Analog zum ersten Teil des Beweises können nur Blöcke der Größe $1, 2$ oder n existieren. Da aber n ungerade ist, ist 2 keine gültige Blockgröße. Damit hat G nur die trivialen Blöcke und K ist wiederum primitiv. □

Korollar 4.13. *Sei $f \in \mathbb{Z}[t]$ normiert und irreduzibel vom Grad n und α eine Nullstelle von f. Ferner gelte für ein $p \in \mathbb{P}$ zusätzlich, daß $f(t) \bmod p\mathbb{Z}[t]$ irreduzibel ist. Dann besitzt $K = \mathbb{Q}(\alpha)$ höchstens einen Teilkörper vom Grad m $(m \mid n)$.*

Beweis: Da $f(t) \bmod p\mathbb{Z}[t]$ irreduzibel ist, enthält G =Gal(f) eine Permutation π vom Zykeltyp $[n]$. Sei nun ein m gegeben, so daß n von m geteilt wird. Zu einem Teilkörper vom Grad m muß nach obigen Satz ein Block Δ der Größe $\frac{n}{m}$ existieren, der α enthält. Da π nur aus einem Zykel besteht, kann es höchstens einen solchen Block geben. Damit ist die Behauptung gezeigt. □

Im nächstem Schritt werden wir zeigen, wie man aus einem Block, der α enthält, den zugehörigen Teilkörper berechnen kann.

Satz 4.14. *Sei $f \in \mathbb{Z}[t]$ normiert und irreduzibel vom Grad n, und sei α eine Nullstelle von f. Sei $K = \mathbb{Q}(\alpha)$, $G = Gal(f)$ und Δ ein Block der Größe d, der α enthält. Seien $\Delta_2, \dots, \Delta_m$ die zu $\Delta = \Delta_1$ konjugierten Blöcke $(m = \frac{n}{d})$. Für $i = 1, \dots, m$ setze $\delta_i = \prod_{\beta \in \Delta_i} \beta$. Weiterhin seien die $\delta_i\,(i = 1, \dots, m)$ paarweise verschieden. Dann ist δ_1 primitives Element von $L = \mathrm{Fix}(G_{\{\Delta\}})$ und es gilt: $g(t) = \prod_{i=1}^{m}(t - \delta_i)$ ist ein Minimalpolynom von L.*

Beweis: Da $G_{\{\Delta\}}$ Elemente aus Δ wieder auf Elemente aus Δ überführt, bleibt δ_1 unter $G_{\{\Delta\}}$ fix. Damit ist gezeigt, daß $\delta_1 \in L$ ist.
Aufgrund der Konstruktion ist L ein Teilkörper vom Grad m. Wegen der Blockeigenschaft der Δ_i $(i = 1, \dots, m)$ wird δ_1 durch jedes $g \in G$ auf ein δ_j $(j = 1, \dots, m)$ überführt. Da die $\delta_j\,(j = 1, \dots, m)$ paarweise verschieden sind, besitzt δ_1 somit m verschiedene Konjugierte und hat somit Grad m. Deswegen ist δ_1 primitives Element von L. Aufgrund der Konstruktion erkennen wir, daß die $\delta_i\,(1 \le i \le m)$ die Konjugierten von δ_1 sind. Hieraus folgt die Darstellung von g. □

In der Praxis kann es passieren, daß die $\delta_i\,(i = 1, \dots, m)$ nicht paarweise verschieden sind. Damit der obige Satz angewendet werden kann, muß ein anderes Minimalpolynom des Körpers K gefunden werden, welches die Voraussetzungen des Satzes erfüllt. Hierzu soll der folgende Satz einen Ansatz liefern.

SATZ 4.15. *Falls die $\delta_i\,(i = 1, \dots, m)$ nicht paarweise verschieden sind, substituiere $t := t - k$ in f. Es gibt höchstens $\frac{n^2}{2d}$ solcher Substitutionen, die wiederum nicht paarweise verschiedene $\delta_i\,(i = 1, \dots, m)$ liefern.*

Beweis: Für $i = 1, \dots, m$ definiere $\phi_i(x) := \prod_{\beta \in \Delta_i}(x + \beta)$. Diese Polynome sind alle verschieden, da sie verschiedene Nullstellen haben. Alle Polynome haben Grad d, so daß höchstens d Funktionswerte zweier Polynome übereinstimmen können. Da es maximal $\binom{m}{2}$ Paare von Polynomen gibt, existieren höchstens $\binom{m}{2}d < \frac{1}{2}mn = \frac{n^2}{2d}$ Werte k, für die $\phi_i(k) = \phi_j(k)$ mit $i \neq j$ gilt. Wie man leicht sieht, hat jedes andere $k \in \mathbb{Z}$ die gewünschte Eigenschaft. $\square$

BEMERKUNG 4.16. *Sei $\tilde{f}$ das durch die Substitution $t := t - k$ aus f hervorgegangene Polynom. Dann gilt: disc(f) = disc($\tilde{f}$).*

BEMERKUNG 4.17. *Die im vorangehenden Satz durchgeführte Substitution hat den Nachteil, daß die Koeffizenten des neuen Polynoms sehr groß werden können.*

BEMERKUNG 4.18. *Unter der Annahme, daß die δ_i paarweise verschieden sind, läßt sich ein primitives Element eines Teilkörpers vom Grad m durch das Produkt von $\frac{n}{m}$ geeigneten Nullstellen des Minimalpolynoms von α darstellen. Falls die $\delta_i\,(i = 1, \dots, m)$ nicht paarweise verschieden sind, kann auf diese Art nur ein Teilkörper des gesuchten Körpers dargestellt werden.*

5. Berechnung von möglichen Blöcken

Im bisherigen Teil dieses Kapitels haben wir Eigenschaften von Blöcken einer transitiven (Galois-) Gruppe G angegeben und hergeleitet. Weiterhin haben wir den Zusammenhang zwischen den Blöcken und den Teilkörpern einer algebraischen Erweiterung aufgezeigt. So stellt sich uns nun die Frage, wie wir die Blöcke einer Galoisgruppe G =Gal(f) berechnen können, wenn wir nur das Minimalpolynom f kennen. Wir hatten schon erwähnt, daß es viel zu kompliziert ist, zuerst die Galoisgruppe zu berechnen und hiernach zu versuchen, Teilkörper zu bestimmen. Daher können wir die Definition für Blöcke nicht verifizieren und damit die Blöcke nicht direkt ausrechnen. Deswegen müssen wir einen anderen Weg finden. Wir haben im zweiten Abschnitt dieses Kapitels einige Eigenschaften von Blöcke hergeleitet, die wir nun für unser Verfahren ausnutzen wollen. Wir werden Teilmengen berechnen, die die hergeleiteten Eigenschaften besitzen. Hierzu betrachten wir die folgende Definition.

Definition 4.19. *Mögliche Blöcke und Blocksysteme*

Im folgenden seien $A \subseteq \Omega$, $k \in \mathbb{N}$ und $\pi = \pi_1 \cdot \ldots \cdot \pi_r \in G$, wobei n_i die Länge des Zykels $\pi_i\,(1 \leq i \leq r)$ ist, mit den folgenden Eigenschaften gegeben:

(1) $|A| = d \in \mathbb{N}$.
(2) *Enthält ein Zykel π_i Elemente der Menge A, so wird n_i von k geteilt und π_i enthält exakt $\frac{n_i}{k}$ Elemente der Menge A.*

Eine solche Teilmenge heißt möglicher Block der Größe d mit k-Wert k. Seien weiterhin $A_1, \ldots, A_m$ mögliche Blöcke der Größe d mit k-Werten $k_1, \ldots, k_m$. Dann heißt $A_1, \ldots, A_m$ ein mögliches Blocksystem, falls

(1) $\bigcup\limits_{1 \leq i \leq m} A_i = \Omega$.
(2) $A_i \cap A_j = \emptyset$ *für* $i \neq j$.
(3) *Für jeden möglichen Block A_i ist $A_i^{\pi^j}$ für $1 \leq j < k$ auch ein möglicher Block, der in der Menge $\{A_1, \ldots, A_m\}$ enthalten ist.*

gilt.

Bemerkung 4.20. *Offensichtlich ist jeder Block ein möglicher Block und jedes Blocksystem ein mögliches Blocksystem. Umgekehrt ist nicht jeder mögliche Block ein Block und nicht jedes mögliche Blocksystem ein Blocksystem.*

Bemerkung 4.21. *Die Bezeichnungen möglicher Block bzw. mögliches Blocksystem sind abhängig von der Wahl der Permutation $\pi \in G$.*

Da die Anzahl der möglichen Blöcke stark von der gewählten Permutation π abhängt, sind wir daran interessiert, ein π zu finden, für das es möglichst wenig mögliche Blöcke gibt.

Wir werden also im Algorithmus alle möglichen Blöcke A von Ω berechnen. In den nächsten Kapiteln wird dann bei der Teilkörperberechnung bzw. bei der Einbettung erläutert werden, wie wir „falsche" Blöcke, d.h. mögliche Blöcke, die keine Blöcke sind, erkennen können. Dieser Prozeß ist aber öfters sehr aufwendig, so daß wir daran interessiert sind, möglichst wenig „falsche" Blöcke zu berechnen.

Wir werden den folgenden Blockalgorithmus in zwei Varianten angeben. Im ersten Fall sind wir nur an möglichen Blöcken Δ interessiert, die das primitive Element

α von K enthalten. Da die $\mathbb{Q}(\alpha_i)$ $(i = 1, \ldots, n)$ alle isomorph zueinander sind, können wir o.E. davon ausgehen, daß $\alpha = \alpha_1$ im ersten Zykel enthalten ist. In der zweiten Variante sind wir an allen möglichen Blocksystemen interessiert. Hier können wir im Prinzip den gleichen Algorithmus verwenden, wir müssen nur nach Finden eines möglichen Blocks in den verbliebenen Zykeln nach weiteren möglichen Blöcken suchen.

ALGORITHMUS 4.22. *Berechnung von möglichen Blöcken eines Körpers K.*

Input:	*Erzeugendes Polynom $f \in \mathbb{Z}[t]$ von $K = \mathbb{Q}(\alpha)$ vom Grad n,*
	gesuchte Blockgröße $d \in \mathbb{N}$,
	$p \in \mathbb{P}$, für welches die Berechnung durchgeführt werden soll.
Output:	*Mögliche Blöcke des Körpers K, die α enthalten.*

(1) *Faktorisiere $f \mod p$.*
(2) *Falls die Faktorisierung einen doppelten Faktor enthält, breche mit der Meldung „Algorithmus nicht durchführbar“ ab.*
(3) *Bestimme aus der Faktorisierung den Zykeltyp $[n_1, \ldots, n_u]$ von π.*
(4) *Setze den k-Wert k auf 1 (vgl. 4.4).*
(5) *Bestimme alle Teilmengen A von $\{2, \ldots, u\}$, so daß die folgenden beiden Bedingungen erfüllt sind:*
 (i) *Für alle $a \in A$ gilt: $\frac{n_a}{k} \in \mathbb{N}$.*
 (ii) $dk - n_1 = \sum\{n_a \mid a \in A\}$.
 Gib diese Teilmengen aus.
(6) *Falls $k = d$ ist, terminiere den Algorithmus.*
(7) *Setze k auf den nächstgrößeren Teiler von d.*
(8) *Gehe nach (5).*

BEMERKUNG 4.23. *Der obige Algorithmus geht davon aus, daß das primitive Element des Körpers im ersten Zykel liegt. Dies ist o.E. möglich, da die Körper $\mathbb{Q}(\alpha_i)\,(i = 1, \ldots, n)$ alle isomorph sind. Die α_i sind hierbei die Nullstellen des Minimalpolynoms f.*

SATZ 4.24. *Der Algorithmus 4.22 berechnet alle möglichen Blöcke zu π, die α enthalten.*

Beweis: In den Schritten (1)–(3) wird mit Hilfe des van der Waerden-Kriteriums 2.28 eine zyklische Untergruppe H der Galoisgruppe G bestimmt. Der Satz ist nicht anwendbar, wenn p die Diskriminante von f teilt, also $f \mod p$ doppelte Faktoren enthält. In den Schritten (4)–(8) werden die möglichen Blöcke berechnet. Der Algorithmus terminiert, da es nur endlich viele Teilmengen A gibt, die untersucht werden müssen. □

BEMERKUNG 4.25. *Im obigen Algorithmus ist die Durchführung von Schritt (5) offengeblieben. Dies ist ein kombinatorischer Algorithmus, der auf geschickte Weise alle Möglichkeiten durchprobiert. Ein Problem dieses Algorithmus ist, daß wir nicht wissen, aus wievielen Zykeln ein Block zusammengesetzt ist. In der Praxis hat es sich als vorteilhaft erwiesen, zuerst die großen Zykel auszuprobieren. So stellt man sehr oft fest, daß bereits eine zweielementige Teilmenge zu groß ist, so daß man mehrelementige Mengen, die diese enthalten, erst gar nicht betrachten muß. Weiterhin erweist es sich in diesem Schritt als sehr nützlich, wenn man diesen Schritt vorzeitig abbricht, wenn schon klar ist, daß dieser Zykel unbrauchbar ist. Dies ist z.B. dann der Fall, wenn man weiß, daß es höchstens l Blöcke vom gegebenen Grad geben kann, man aber bereits erheblich mehr ausgerechnet hat. Wir möchten an dieser Stelle allerdings verzichten, eine genaue Implementierung von Schritt (5) anzugeben.*

Zum Abschluß dieses Abschnitts wollen wir noch einen zweiten Algorithmus angeben, der die möglichen Blocksysteme der Galoisgruppe G berechnet. Dadurch, daß wir alle Blöcke eines Blocksystems berechnen, haben wir natürlich noch mehr Möglichkeiten, falsche Blöcke zu berechnen. Wenn zum Beispiel ein Block in mehreren Blocksystemen enthalten ist, so wissen wir, daß nur ein Blocksystem gültig sein kann. Sollten wir in einem späteren Teil des Algorithmus bestätigen können, daß ein mögliches Blocksystem ein Blocksystem war, so brauchen wir die anderen möglichen Blocksysteme, die einen Block aus dem richtigen Blocksystem enthalten, nicht mehr betrachten. Nun wollen wir aber zum Algorithmus kommen.

ALGORITHMUS 4.26. *Berechnung von möglichen Blocksystemen eines Körpers K.*

Input: *Erzeugendes Polynom $f \in \mathbb{Z}[t]$ des Körpers $K = \mathbb{Q}(\alpha_1)$ vom Grad n, gesuchte Blockgröße $d \in \mathbb{N}$, Permutation π samt Zerlegung in elementfremde Zykel $\pi_1, \dots, \pi_u$. $Z = \{\pi_1, \dots, \pi_u\}$.*

Output: *Mögliche Blocksysteme des Körpers K.*

(1) *Setze den k-Wert k auf 1 (vgl. 4.4).*

(2) *Setze l auf die Anzahl der Elemente in Z und bestimme die Zykellängen $n_1, \dots, n_l$ der in Z enthaltenden Zykel.*

(3) *Bestimme alle Teilmengen A von $\{2, \dots, l\}$, so daß die folgenden beiden Bedingungen erfüllt sind:*
   - (i) *Für alle $a \in A$ gilt: $\frac{n_a}{k} \in \mathbb{N}$.*
   - (ii) $dk - n_1 = \sum_{a \in A} n_a$.

(4) *Für jede dieser Teilmengen A tue folgendes:*

(i) *Entferne alle benutzten Zykel aus Z, d.h. setze Z=Z$\setminus$A.*
(ii) *Falls Z die leere Menge ist, gib das mögliche Blocksystem aus.*
(iii) *Ansonsten rufe den Algorithmus erneut mit den verbleibenden Zykeln in Z auf.*

(5) *Falls $k = d$ ist, terminiere den Algorithmus.*
(6) *Setze k auf den nächstgrößeren Teiler von d.*
(7) *Gehe nach (3).*

Beweis: Die Korrektheit dieses Algorithmus folgt unmittelbar aus dem Algorithmus 4.22 und den hergeleiteten Eigenschaften. □

BEMERKUNG 4.27. *Wie wir am 4. Schritt sehen, arbeitet dieser Algorithmus rekursiv. Im Prinzip wird das Verteilen der Zykel auf die möglichen Blöcke sukzessive angewendet, bis keine Zykel mehr da sind. Bei höheren k-Werten brauchen die konjugierten Blöcke, die aus den selben Zykeln bestehen, nicht beachtet werden, da sie eindeutig feststehen. Deswegen kann man an dieser Stelle auch alle benutzten Zykel aus der Liste Z streichen. Bei der Ausgabe des möglichen Blocksystem wird davon ausgegangen, daß dem Algorithmus die vorher berechneten möglichen Blöcke zur Verfügung stehen.*

6. Beispiele

Zum Abschluß wollen wir die Ergebnisse dieses Kapitels an zwei Beispielen demonstrieren. Der kürzeren Schreibweise wegen listen wir ein Blocksystem in der Form $\{\{\dots\},\dots,\{\dots\}\}$ auf.

Zuerst betrachten wir die verschiedenen Zykeltypen eines Körpers vom Grad 4 und bestimmen die Anzahl seiner möglichen Blöcke der Größe 2.

(i) Zykeltyp [4], d.h. $\pi = (\alpha_1, \alpha_2, \alpha_3, \alpha_4)$.
Für $k = 1$ und $k = 4$ können wir keinen Block der Größe 2 bilden. Für $k = 2$ bilden $\{\{\alpha_1, \alpha_3\}, \{\alpha_2, \alpha_4\}\}$ ein Blocksystem.

(ii) Zykeltyp [1,3], d.h. $\pi = (\alpha_1)(\alpha_2, \alpha_3, \alpha_4)$.
Da der erste Faktor Grad 1 hat, muß der zugehörige k-Wert 1 sein. Damit läßt sich aber nur ein Block der Größe 1 oder 4 bilden. Es existiert also kein Block der Größe 2.

(iii) Zykeltyp [2,2], d.h. $\pi = (\alpha_1, \alpha_2)(\alpha_3, \alpha_4)$.
Für k=1 erhalten wir das Blocksystem $\{\{\alpha_1, \alpha_2\}\{\alpha_3, \alpha_4\}\}$. Für k=2 können wir zwei weitere mögliche Blocksysteme bilden, nämlich $\{\{\alpha_1, \alpha_3\}, \{\alpha_2, \alpha_4\}\}$ und $\{\{\alpha_1, \alpha_4\}, \{\alpha_2, \alpha_3\}\}$.

(iv) Zykeltyp [1,1,2], d.h. $\pi = (\alpha_1)(\alpha_2)(\alpha_3\alpha_4)$.
Die Nullstellen α_1 und α_2 müssen zu einem Block mit k-Wert 1 gehören. Sie bilden also einen Block. Damit ergibt sich der zweite Block mit $\{\alpha_3, \alpha_4\}$ automatisch.

(v) Zykeltyp [1,1,1,1], d.h. $\pi = id$.
Die Identität liefert alle Möglichkeiten die Nullstellen in Blöcke der Größe 2 zu gruppieren. Es ergeben sich $\binom{4}{2} = 3$ Möglichkeiten.

Als nächstes werden wir unsere Überlegungen an einem Beispiel vom Grad 6 demonstrieren. Hierzu betrachten wir den Körper K, der vom irreduziblen Polynom $f(t) = t^6 + 108$ erzeugt wird. Wir faktorisieren dieses Polynom modulo mehrerer Primzahlen und erhalten die folgenden Faktorisierungen:

$$\begin{aligned}
f(t) &\equiv t^6 \bmod 2 \\
f(t) &\equiv t^6 \bmod 3 \\
f(t) &\equiv (t^2+2)(t^2+t+2)(t^2+4t+2) \bmod 5 \\
f(t) &\equiv (t^3+2)(t^3+5) \bmod 7 \\
&\vdots \\
f(t) &\equiv (t+3)(t+13)(t+15)(t+16)(t+18)(t+28) \bmod 31
\end{aligned}$$

Die Faktorisierungen modulo 2,3 sind für uns uninteressant, da doppelte Faktoren auftreten. Auf die nächsten drei Faktorisierungen können wir das van der Waerden-Kriterium anwenden und erhalten so Zykeltypen von Elementen der Galoisgruppe von f. Für $p = 5$ erhalten wir so ein Element vom Zykeltyp [2,2,2], d.h. es existiert ein $\pi \in$Gal(f) mit $\pi = (\alpha_1\alpha_2)(\alpha_3\alpha_4)(\alpha_5\alpha_6)$. Hierbei sollen die α_i passend numeriert sein. Analog erhalten wir für $p = 7$ ein Element vom Zykeltyp [3,3] und für $p = 31$ ein Element vom Zykeltyp [1,1,1,1,1,1], welches der Identität entspricht. Die Faktorisierungen modulo der anderen Primzahlen haben keine neuen Zykeltypen ergeben. Wir müssen uns nun überlegen, wieviele Blöcke der Größe 2 und 3 existieren können.

Wir starten mit $p = 5$, dem Zykeltyp [2,2,2] und der Blockgröße 2. Wir setzen $k = 1$, d.h. für jeden Block müssen alle Nullstellen eines Faktors verwendet werden. Wir setzen also $\Delta_1 = \{\alpha_1, \alpha_2\}$. Nun müssen wir die verbleibenden Blöcke bestimmen. Hierzu setzen wir wieder $k = 1$ und erhalten $\Delta_2 = \{\alpha_3, \alpha_4\}$ und damit $\Delta_3 = \{\alpha_5, \alpha_6\}$. Damit haben wir ein erstes mögliches komplettes Blocksystem bestimmt. Für das nächste Blocksystem gilt immer noch $\Delta_1 = \{\alpha_1, \alpha_2\}$ (Wir kommen eine Rekursionsstufe zurück.) Für $k = 1$ können wir keine weiteren

Blöcke bestimmen. Daher setzen wir $k = 2$ und erhalten die beiden Möglichkeiten $\Delta_2 = \{\alpha_3, \alpha_5\}$ und $\Delta_3 = \{\alpha_4, \alpha_6\}$ bzw. $\Delta_2 = \{\alpha_3, \alpha_6\}$ und $\Delta_3 = \{\alpha_4, \alpha_5\}$. Da bei allen 3 Blocksystemen der Block Δ_1 identisch ist, kann nur eins ein gültiges Blocksystem sein. Nun kommen wir zum Block Δ_1 zurück und stellen fest, daß mit $k = 1$ keine weitere Blockbildung möglich ist. Wir setzen also $k = 2$ und erhalten die folgenden Blocksysteme:
$\{\{\alpha_1, \alpha_3\}, \{\alpha_2, \alpha_4\}, \{\alpha_5, \alpha_6\}\}$ $\{\{\alpha_1, \alpha_4\}, \{\alpha_3, \alpha_4\}, \{\alpha_5, \alpha_6\}\}$
$\{\{\alpha_1, \alpha_5\}, \{\alpha_2, \alpha_6\}, \{\alpha_3, \alpha_4\}\}$ $\{\{\alpha_1, \alpha_6\}, \{\alpha_2, \alpha_5\}, \{\alpha_3, \alpha_4\}\}$
Wir müssen also sieben mögliche Blocksysteme untersuchen, von denen aber nur drei gültig sein können.

Für die Blockgröße 3 stellen wir leicht fest, daß alle Blöcke k-Wert 2 haben müssen. Wir erhalten so 4 verschiedene mögliche Blocksysteme.

Wir wechseln nun die Primzahl und betrachten $p = 7$. O.E. gehen wir davon aus, daß die Nullstellen nun so angeordnet sind, daß $\pi = (\alpha_1, \alpha_2, \alpha_3)(\alpha_4, \alpha_5, \alpha_6)$ gilt.

Wir starten mit der Blockgröße 2 und stellen fest, daß Blockbildung nur mit k=3 möglich ist. Dies bedeutet, daß wir jeweils eine Nullstelle des ersten Faktors mit einer Nullstelle des zweiten Faktors kombinieren müssen. Die Anzahl der möglichen Blocksysteme bleibt hier klein, da nach Bildung eines ersten Blocks, die übrigen Blöcke eindeutig mit Hilfe des Frobeniusautomorphismus bestimmt sind. Dieses wird im Kapitel über die Berechnung der Teilkörper noch erläutert werden. Wir erhalten also die drei möglichen Blocksysteme: $\{\{\alpha_1, \alpha_4\}\{\alpha_2, \alpha_5\}\{\alpha_3, \alpha_6\}\}$ $\{\{\alpha_1, \alpha_5\}\{\alpha_2, \alpha_6\}\{\alpha_3, \alpha_4\}\}$ $\{\{\alpha_1, \alpha_6\}\{\alpha_2, \alpha_4\}\{\alpha_3, \alpha_5\}\}$

Für die Blockgröße 3 erhalten wir für $k = 1$ nur einen Blocksystem, wobei die Blöcke aus den Nullstellen der beiden Faktoren bestehen.

Die Identität auszuwerten lohnt sich für uns nicht, da sie $\binom{6}{3}$ Möglichkeiten für Blöcke der Größe 2 und $\binom{6}{2}$ Möglichkeiten für Blöcke der Größe 3 liefert. Wir stellen also fest, daß $p = 7$ für unsere Berechnungen am besten geeignet ist.

KAPITEL 5

Zur Konstruktion von Teilkörpern

1. Einleitung

Im vorherigen Kapitel haben wir Methoden vorgestellt, um aus einem erzeugenden Polynom f eines Körpers K mögliche Blöcke zu berechnen. Im günstigsten Fall haben wir dabei festgestellt, daß es keine Blöcke und damit auch keine Teilkörper geben kann. Falls dieser günstige Fall nicht eintritt, müssen wir hier nun versuchen, aus den möglichen Blöcken erzeugende Polynome von Teilkörpern zu berechnen. Dabei stellt sich uns das Problem, daß wir nicht wissen, ob die möglichen Blöcke auch tatsächlich Blöcke der Galoisgruppe unseres Polynoms sind. Dies zu berücksichtigen wird in den beiden in diesem Kapitel vorgestellten Verfahren noch einige Probleme bereiten.

Ausgangspunkt für beide Verfahren ist, daß wir vom Blockalgorithmus eine „möglichst günstige“ Primzahl p geliefert bekommen. Möglichst günstig heißt hierbei unter anderem, daß sie möglichst wenig Möglichkeiten für verschiedene Blöcke zuläßt. Aber es spielen auch noch andere Punkte eine wichtige Rolle, die in den beiden Verfahren herausgearbeitet werden sollen.

Der erste Algorithmus, den wir im Rahmen dieser Arbeit vorstellen wollen, entspricht im groben dem Verfahren, welches in [Dix1] präsentiert wird. Hier wird dem Algorithmus ein möglicher Block Δ und eine Primzahl p zur Verfügung gestellt. Der Algorithmus ist nur durchführbar, wenn der zugehörige k-Wert 1 ist. Im ersten Schritt wird dann die modulo p-Faktorisierung von f mittels des Hensel-Liftings bis zu einer genügenden p-Potenz geliftet. Hiernach kann ein primitives Element des gesuchten Teilkörpers approximiert werden. Mit Hilfe des LLL-Algorithmus kann dann das Minimalpolynom dieses primitiven Elements ausgerechnet werden. Falls einer dieser Schritte scheitert, bedeutet dies, daß Δ kein Block war.

Der zweite Algorithmus hat den Vorteil, daß er auch mit Primzahlen arbeiten kann, bei denen die zugehörigen k-Werte ungleich 1 sind. Dieses Verfahren benötigt neben der Primzahl p allerdings ein komplettes Blocksystem. Hiernach ist das Minimalpolynom des Teilkörpers lediglich durch das Faktorisieren von Polynomen über endlichen Körpern und durch das Hensel-Lifting berechenbar.

2. Zur Abschätzung der Koeffizienten des gesuchten Minimalpolynoms

In diesem Abschnitt werden wir Schranken für das zu berechnende erzeugende Polynom des Teilkörpers L angeben. Dabei nutzen wir aus, daß das erzeugende Polynom mit Hilfe von 4.14 konstruiert wird. Wir müssen also die folgende Situation betrachten. Gegeben ist ein normiertes und irreduzibles Polynom $f \in \mathbb{Z}[t]$ mit Nullstellen $\alpha_1, \ldots, \alpha_n$. Wir definieren einen algebraischen Zahlkörper durch $K = \mathbb{Q}(\alpha_1)$. Weiterhin nehmen wir an, daß ein Teilkörper L vom Grad m existiert. Nach 4.11 existiert ein Blocksystem $\Delta_1, \ldots, \Delta_m$, welches K/L eindeutig zugeordnet ist. O.E. nehmen wir an, daß die α_i so angeordnet sind, daß für $(j-1)d+1 \leq i \leq jd$ gilt: $\alpha_i \in \Delta_j$. Hierbei ist d die zugehörige Blockgröße; es gilt also $md = n$. Nun wissen wir nach 4.14, daß unser gesuchtes Minimalpolynom g von L die Form

$$g(t) = \prod_{j=1}^{m}(t - \prod_{\alpha \in \Delta_j} \alpha) = \prod_{j=1}^{m}(t - \prod_{i=1}^{d} \alpha_{(j-1)d+i})$$

hat. Weiterhin wissen wir, daß $g \in \mathbb{Z}[t]$ ist.

Bevor wir mit den Abschätzungen beginnen, werden wir erstmal eine Polynomnorm definieren.

Definition 5.1. *Sei $f \in \mathbb{Z}[t]$ mit $f(t) = \sum_{i=0}^{n} c_i t^i$. Dann ist $\|f\|_2 := (\sum_{i=0}^{n} c_i^2)^{\frac{1}{2}}$.*

Das folgende Lemma wird uns zu einer Abschätzung unseres Problems führen.

Satz 5.2. *Sei $f \in \mathbb{Z}[t]$ normiert von der Form $f(t) = \sum_{i=1}^{n} a_i t^i$. Weiterhin seien die Nullstellen $\alpha_1, \ldots, \alpha_n$ so angeordnet, daß für $1 \leq i \leq k$ gilt: $|\alpha_i| \geq 1$. Für $i > k$ soll dann $|\alpha_i| < 1$ gelten. Dann gilt für die Koeffizienten von f folgende Abschätzung:*

$$|a_j| \leq \binom{n-1}{j-1} \prod_{i=1}^{k} |\alpha_i| + \binom{n-1}{j}.$$

Beweis: Wie allgemein bekannt ist, entsprechen die elementarsymmetrischen Funktionen σ_{nj} bis auf das Vorzeichen den Koeffizienten a_j. Wir definieren für

$1 \leq i \leq n : \tilde{\alpha}_i := \max\{|\alpha_i|, 1\}$. Die $\tilde{\sigma}_{n_i}$ sind dann die elementarsymmetrischen Funktionen bezogen auf die $\tilde{\alpha}_i$. Deswegen gilt:

$$|a_j| = |\sigma_{nj}| \leq |\tilde{\sigma}_{nj}| \leq \binom{n-1}{j-1} \prod_{i=1}^{n} \tilde{\alpha}_i + \binom{n-1}{j}.$$

Die letzte Ungleichung folgt nach Lemma 3.5.2 aus [Coh]. Die gesuchte Behauptung folgt, da für $i > k$ stets $\tilde{\alpha}_i = 1$ gilt. □

Mit Hilfe dieses Satzes können wir nun recht einfach Abschätzungen für die Größe der Koeffizienten unseres erzeugenden Polynoms g angeben. Das einzige Problem, was wir lösen müssen, ist die Bestimmung des Produktes der Nullstellen von g, deren Betrag größer gleich 1 ist. Hierzu müssen wir zwei Fälle unterscheiden. Der einfache Fall ist, daß bereits alle Nullstellen von f betraglich größer gleich 1 waren. Dann trifft dies logischerweise auch für die Nullstellen von g zu. Wir können dann für M einfach den Betrag des absoluten Glieds von f wählen. Falls einige Nullstellen von f betraglich kleiner als 1 sind, so können wir für M den Wert wählen, den wir auch für das Polynom f gewählt hätten. Dieser Wert muß zwar nicht optimal sein, reicht aber für unsere Zwecke aus. Wenn man etwas geschickter vorgehen will, so kann man sich überlegen, ob Nullstellen von f, die betraglich kleiner als 1 sind, in einem Block mit Nullstellen liegen, die betraglich größer als 1 sind. Falls man solche Zusammenhänge feststellen kann, kann man die Abschätzung für M verbessern. Diese Überlegungen führen zu folgendem Satz.

Satz 5.3. *Sei f ein erzeugendes Polynom von K. Weiterhin existiere ein Teilkörper L von K, dessen erzeugendes Polynom $g(t) = \sum_{j=0}^{m} b_j t^j$ mittels* 4.14 *konstruiert werden kann. Zusätzlich sei $M = \prod_{i=1}^{k} |\alpha_i|$, wobei $\alpha_1, \ldots, \alpha_k$ gerade die Nullstellen von f sind, deren Betrag größer gleich 1 sind. Dann gilt für die Koeffizienten von g die folgende Abschätzung:*

$$|b_j| \leq \binom{m-1}{j-1} M + \binom{m-1}{j}.$$

Durch diesen Satz können wir nun auch sehr leicht eine Abschätzung für die $\|\cdot\|_2$ des Minimalpolynoms unseres Teilkörpers bestimmen.

3. Konstruktion von Teilkörpern mit Hilfe des LLL-Algorithmus

Gegeben sei ein erzeugendes Polynom f des Zahlkörpers K. G sei die Galoisgruppe von f. Als Ausgangspunkt für diesen Abschnitt sei ein möglicher Block Δ von G der Größe d und eine Primzahl p mit der zugehörigen Permutation π

gegeben, so daß der zugehörige k-Wert 1 ist. Wie im vorigen Kapitel zerlegen wir π in elementfremde Zykel $\pi_1 \cdot \ldots \cdot \pi_u$. Dieser Zerlegung entspricht die Polynomfaktorisierung von f modulo $p\mathbb{Z}[t]$, d.h. der Zykel π_i operiert auf den Nullstellen von $f_i\,(i = 1, \ldots, u)$. Da der k-Wert von Δ bzgl. π 1 ist, besteht Δ nur aus kompletten Zykeln von π. Diese seien mit $\pi_{n_1}, \ldots, \pi_{n_s}$ bezeichnet. Nach Satz 4.14 müssen wir das Produkt der Wurzeln bilden, die in Δ enthalten sind. Dieses Produkt der Wurzeln entspricht bis auf das Vorzeichen gerade dem Produkt der absoluten Glieder der zu $\pi_{n_1}, \ldots, \pi_{n_s}$ gehörigen Polynome. Wenn wir dieses Produkt bilden, erhalten wir eine modulo p-Approximation des gesuchten primitiven Elements. Wenn wir vorher die Kongruenzfaktorisierung mittels des Hensel-Liftings zu einer modulo $p^k\mathbb{Z}[t]$-Faktorisierung liften ($k \in \mathbb{N}$), so erhalten wir für das primitive Element sogar eine modulo p^k-Approximation. Dabei muß das k genügend groß gewählt werden, damit die folgenden Schritte durchgeführt werden können. Diese Überlegungen liefern den folgenden Algorithmus.

Algorithmus 5.4. *Berechnung des Minimalpolynoms eines Teilkörpers L.*

Input:	*Minimalpolynom $f \in \mathbb{Z}[t]$ des Körpers K vom Grad n,* *möglicher Block Δ und Blockgröße d,* *$p \in \mathbb{P}$, Faktorisierung von f modulo $p\mathbb{Z}[t]$.*
Output:	*Mögliches Minimalpolynom g eines Teilkörpers L.*

(1) *Prüfe, ob der zu Δ gehörige k-Wert 1 ist. Falls nicht, breche mit der Fehlermeldung „Algorithmus nicht durchführbar“ ab.*
(2) *Berechne die Zykel $\pi_{n_1}, \ldots, \pi_{n_s}$, deren Wurzeln in Δ enthalten sind.*
(3) *Bestimme ein k, bis zu dem das Hensel-Lifting durchgeführt werden soll.*
(4) *Lifte die Faktorisierung von f mittels des Hensel-Liftings:* $f(t) \equiv \tilde{f}_1(t) \cdot \ldots \cdot \tilde{f}_t(t) \bmod p^k\mathbb{Z}[t]$.
(5) *Berechne das Produkt δ der absoluten Glieder der zu $\pi_{n_1}, \ldots, \pi_{n_s}$ gehörigen Polynome $\tilde{f}_i$ (modulo p^k).*
(6) *Falls d ungerade ist, setze δ auf $-\delta$.*
(7) *Bestimme mit Hilfe des LLL-Algorithmus ein mögliches Minimalpolynom g des Teilkörpers L. Falls der Algorithmus scheitert, war Δ kein Block gewesen.*

Die ersten beiden Schritte des obigen Algorithmus sind selbsterklärend. Im 3. Schritt muß ein k bestimmt werden, bis zu dem das Hensel-Lifting durchgeführt werden soll. Dieses k hängt von dem gegebenen Polynom f ab. Hierbei muß abgeschätzt werden, wie groß die Koeffizienten des gesuchten Minimalpolynoms

von L werden können. Weiterhin muß das k so groß gewählt werden, daß das gesuchte Minimalpolynom vom LLL-Algorithmus gefunden werden kann. Diese Punkte werden in den nächsten Abschnitten beschrieben.
Die Schritte 4 und 5 des Algorithmus sind wiederum selbsterklärend. Im 6. Schritt muß noch auf das Vorzeichen des approximierten Elements geachtet werden. Der 7. Schritt ist der Hauptteil des obigen Verfahrens. Hier muß mit Hilfe des LLL-Algorithmus aus dem approximierten primtiven Element das zugehörige Minimalpolynom berechnet werden. Dies wird in einem der folgenden Abschnitte erläutert werden.

3.1. Bestimmung des Minimalpolynoms eines approximierten primitiven Elements mit Hilfe des LLL-Algorithmus

Als Ausgangspunkt für diesen Abschnitt erhalten wir ein approximiertes primitives Element δ, den Grad m dieses Elements und ein $M = p^k$ bzgl. dem δ approximiert ist. Gesucht wird also ein Minimalpolynom vom Grad m, welches modulo p^k δ als Nullstelle hat. Damit die Eindeutigkeit dieses Polynoms gewährleistet ist, muß weiterhin eine Schranke B für die Koeffizienten vorliegen.
Ein analoges Problem wird in [LLL] gelöst. Im 2. Teil dieser Arbeit soll aus einer modulo p^k-Approximation ein Faktor eines gegebenen Polynoms bestimmt werden. Wir möchten aus einer entsprechenden Approximation ein Minimalpolynom berechnen. Die Eigenschaft, daß in [LLL] ein Faktor ausgerechnet werden soll, wird nur in den Abschätzungen für die Koeffizienten des gesuchten Polynoms verwendet. Diesen Teil müssen wir also getrennt untersuchen. Das eigentliche Verfahren verläuft allerdings völlig analog. Da wir nur mit einer Nullstelle δ, d.h. mit einem linearen Polynom $h(t) = t - \delta$ approximieren, werden einige Formeln sogar einfacher.

In diesem Abschnitt schreiben wir $\mathbb{Z}/p^k\mathbb{Z}$ für den Ring der ganzen Zahlen modulo p^k. Für $f(t) = \sum_{i=0}^n a_i t^i \in \mathbb{Z}[t]$ meinen wir mit $f \bmod p^k$ das Polynom $\sum_{i=0}^n (a_i \bmod p^k) t^i \in \mathbb{Z}/p^k\mathbb{Z}[t]$. Zusätzlich sollen im weiteren die folgenden Voraussetzungen gelten:

(1) $f, g \in \mathbb{Z}[t]$ sind Polynome, wobei f von g geteilt wird.
(2) $h(t) = t - \delta$ mit $\delta \in \mathbb{Z}$ und $h \bmod p^k$ teilt $f \bmod p^k$ in $\mathbb{Z}/p^k\mathbb{Z}[t]$.
(3) $h^2 \bmod p$ teilt nicht $f \bmod p$ in $\mathbb{F}_p[t]$.

Satz 5.5. *Das Polynom f besitze einen irreduziblen Faktor $h_0 \in \mathbb{Z}[t]$, für den $h \bmod p$ teilt $h_0 \bmod p$ gilt. Weiterhin ist dieser Faktor bis auf das Vorzeichen* *eindeutig bestimmt. Wenn nun g teilt f in $\mathbb{Z}[t]$ gilt, sind die drei folgenden Aussagen äquivalent:*

(1) $h \bmod p$ *teilt* $g \bmod p$ *in* $\mathbb{F}_p[t]$.
(2) $h \bmod p^k$ *teilt* $g \bmod p^k$ *in* $\mathbb{Z}/p^k\mathbb{Z}[t]$.
(3) h_0 *teilt* g *in* $\mathbb{Z}[t]$.

Weiterhin gilt dann: $h \bmod p^k$ *teilt* $h_o \bmod p^k\mathbb{Z}[t]$ *in* $\mathbb{Z}/p^k\mathbb{Z}[t]$.

Der Beweis dieses Satzes kann in [LLL] (Proposition (2.5)) entnommen werden.

Damit wir mit den Bezeichnungen von [LLL] konform bleiben, soll f in diesem Abschnitt das gesuchte erzeugende Polynom eines Teilkörpers vom Grad m sein. Wenn dieses existiert, wissen wir aus unseren Vorüberlegungen, daß $f \bmod p^k$ von $h \bmod p^k$ in $\mathbb{Z}/p^k\mathbb{Z}[t]$ geteilt wird. Wir betrachten also im folgenden ein Gitter Λ, welches alle Polynome in $\mathbb{Z}[t]$ enthält, die modulo p^k durch $h \bmod p^k$ teilbar sind. Dies ist eine Teilmenge des $(m+1)$-dimensionalen reellen Vektorraums $\mathbb{R}+\mathbb{R}\cdot t+\ldots+\mathbb{R}\cdot t^m$. Dieser Vektorraum wird auf den $\mathbb{R}^{m+1}$ abgebildet, wenn wir $\sum_{i=0}^m a_i t^i$ auf $(a_0, a_1, \ldots, a_m)$ abbilden. Da h normiert ist, ist Λ ein Gitter vom Grad $m+1$. Die Basis von Λ ist gegeben durch $\{p^k\} \cup \{h(t)t^j : 0 \leq j < m\}$. Aus der Definition der Gitterdiskriminante folgt direkt, daß $d(\Lambda) = p^k$ ist. Im folgenden schreiben wir für $\|\cdot\|_2$ abkürzend $|\cdot|$.

Satz 5.6. *Seien p, f, m, h, h_0 und g wie oben definiert. Nun gelte für ein $b \in \Lambda$: $p^k > |f|^m |b|^m$. Dann ist b in $\mathbb{Z}[t]$ durch f teilbar und damit gilt* $\mathrm{ggT}(f, b) = f \neq 1$.

Beweis: Der Beweis ist ähnlich wie der Beweis von (2.7) in [LLL] Für die Bezeichnungen setze hierzu $h_0 = f, l = 1, n = m, L = \Lambda$.

Sei $b \neq 0$ und setze $g = \mathrm{ggT}(f, b)$. Nach 5.5 ist $h \bmod p$ teilt $g \bmod p$ in $\mathbb{Z}/p\mathbb{Z}[t]$ zu zeigen. Nehmen wir an, daß dies nicht gilt. Dann existieren $\lambda_3, \mu_3, \nu_3 \in \mathbb{Z}[t]$, so daß

$$\lambda_3 h + \mu_3 g = 1 - p\nu_3$$

gilt. Aus dieser Gleichung werden wir einen Widerspruch folgern. Setze $e = \deg(g)$ und $m' = \deg(b)$. Es gilt also $0 \leq e \leq m' \leq m$. Definiere

$$\begin{aligned} M = \{\lambda f + \mu b : \lambda, \mu \in \mathbb{Z}[t], \deg(\lambda) < m' - e, \deg(\mu) < m - e\} \\ \subseteq \mathbb{Z} + \mathbb{Z}t + \ldots + \mathbb{Z}t^{m+m'-e-1}. \end{aligned}$$

Sei M' die Projektion von M auf $\mathbb{Z}t^e + \mathbb{Z}t^{e+1} + \ldots + \mathbb{Z}t^{m+m'-e-1}$. Wenn nun ein $\lambda f + \mu b \in M$ auf 0 in M' projeziert wird, dann gilt: $\deg(\lambda f + \mu b) < e$. Da g aber $\lambda f + \mu g$ teilt, folgt $\lambda f + \mu g = 0$ (in M). Hiermit gilt $\lambda f = -\mu b$, woraus $\lambda \frac{f}{g} = -\mu \frac{b}{g}$

folgt. Wegen $\mathrm{ggT}(\frac{f}{g}, \frac{b}{g}) = 1$, folgt $\frac{f}{g}$ teilt μ. Da aber $\deg(\mu) < m - e = \deg(\frac{f}{g})$ gilt, folgt $\mu = 0$ und damit auch $\lambda = 0$. Damit sind die Projektionen von

$$\{t^i f : 0 \leq i < m' - e\} \cup \{t^j b : 0 \leq j < m - e\}$$

auf M' linear unabhängig. Da diese Projektionen M' aufspannen, ist M' ein Gitter vom Rang $m + m' - 2e$. Wegen Hadamards Ungleichung (2-1) und der Voraussetzung erhalten wir:

$$d(M') \leq |f|^{m'-e}|b|^{m-e} \leq |f|^m|b|^m < p^k.$$

Wir brauchen im weiteren die Aussage des folgenden Lemmata.

Lemma 5.7. *Gelte $\lambda_3 h + \mu_3 g = 1 - p\nu_3$. Dann gilt: $\{\nu \in M : \deg(\nu) \leq e\} \subset p^k\mathbb{Z}[t]$.*

Wähle nun eine Basis $b_e, b_{e+1}, \dots, b_{m+m'-e-1}$ von M' mit der Eigenschaft $\deg(b_j) = j$ (Chapter I, Theorem I.A in [Cas1]). Dann ist der Leitkoeffizent von b_e wegen obigen Lemmas durch p^k teilbar. Man beachte hierbei, daß $e \leq m + m' - e - 1$ wegen g teilt b und $h \bmod p$ teilt $\frac{f}{g} \bmod p$ gilt.
Nun gilt: $d(M') = \prod_{e \leq j \leq m+m'-e-1} \mid l(b_j) \mid$, wobei mit $l(b_j)$ der Leitkoeffizient von b_j bezeichnet werde. Hieraus folgt nun, daß $d(M') \geq p^k$ gilt, was zu einem Widerspruch führt. □

Es bleibt noch das Lemma zu zeigen.

Beweis: Sei $\nu \in M$ mit $\deg(\nu) \leq e$. Dann gilt offensichtlich g teilt ν. Aus der Voraussetzung folgt nun:

$$\lambda_3 h + \mu_3 g \quad = \quad 1 - p\nu_3$$

Diese Gleichung multiplizieren wir mit $\frac{\nu}{g}$ und erhalten:

$$\lambda_3 \nu \frac{h}{g} + \mu_3 \nu \quad = \quad \frac{\nu}{g}(1 - p\nu_3)$$

Durch Erweitern mit $1 + p\nu_3 + p^2\nu_3^2 + \ldots + p^{k-1}\nu_3^{k-1}$ und $(g \mid \nu)$ erhalten wir:

$$\lambda_4 h + \mu_4 \nu \quad = \quad \frac{\nu}{g}(1 - p^k\nu_3^k) \text{ mit } \lambda_4, \mu_4 \in \mathbb{Z}[t]$$

Damit gilt die folgende Kongruenz:

$$\lambda_4 h + \mu_4 \nu \equiv \frac{\nu}{g} \bmod p^k\mathbb{Z}[t]$$

Wegen $\nu \in M$ und $b, f \in \Lambda$ folgt nun:

$$\begin{aligned} h \bmod p^k\mathbb{Z}[t] &\mid \nu \bmod p^k\mathbb{Z}[t] \text{ und damit:} \\ \lambda_5 h &\equiv \frac{\nu}{g} \bmod p^k\mathbb{Z}[t] \text{ und hieraus} \\ h &\mid \frac{\nu}{g} \bmod p^k\mathbb{Z}[t] \end{aligned}$$

Da aber $\deg(h) = 1$ ist und der Grad von $\frac{\nu}{g} \leq e - e = 0$ ist, folgt $\frac{\nu}{g} \equiv 0 \bmod p^k\mathbb{Z}[t]$, also $\nu \equiv 0 \bmod p^k\mathbb{Z}[t]$. □

Mit dem folgenden Satz treffen wir eine Aussage darüber, wann das erste Basiselement einer LLL-reduzierten Basis das gesuchte erzeugende Polynom eines Teilkörpers ist. Der analoge Satz zur Bestimmung von Faktoren eines ganzzahligen Polynoms kann wieder [LLL] entnommen werden. Wie im vorangegangenen Satz soll f wieder das gesuchte erzeugende Polynom eines Teilkörpers sein.

Satz 5.8. *Seien Λ, p, f, k und m wie oben definiert. Weiterhin haben wir eine LLL-reduzierte Basis $b_1, \ldots, b_m$ von Λ ausgerechnet. Zusätzlich wurden p und k so bestimmt, daß $p^k > 2^{\frac{m^2}{2}}|f|^{2m}$ gilt. Dann sind die beiden folgenden Aussagen äquivalent:*

(1) $\deg(f) \leq m$
(2) $|b_1| < (\frac{p^k}{|f|^m})^{\frac{1}{m}}$

Beweis: Es sei nun (2) erfüllt. Dann folgt direkt, daß $p^k > |f|^m |b_1|^m$ gilt. Damit sind die Voraussetzungen von 5.6 erfüllt, wodurch (1) gezeigt ist.

Gelte nun (1). Dies bedeutet, daß $f \in \Lambda$ ist. Aus dem Minimumkriterium der LLL-Abschätzung folgt nun:

$$|b_1| \leq 2^{\frac{m}{2}}|f|$$

Nun potenzieren wir beide Seiten mit m und multiplizieren diese mit $|f|^m$.

$$|b_1|^m|f|^m \;\leq\; 2^{\frac{m^2}{2}}|f|^{2m}$$

Durch Einsetzen der Voraussetzung erhalten wir:

$$|b_1|^m|f|^m \;<\; p^k$$

Hieraus folgt dann (2), womit der Satz gezeigt ist. □

In den vorangegangenen Sätzen sind wir davon ausgegangen, daß das Minimalpolynom des Teilkörpers nur durch ein lineares Polynom h approximiert wurde. Sollten uns mehrere Blöcke eines Blocksystems und damit mehrere approximierte Nullstellen δ_i des Minimalpolynoms bekannt sein, so können wir obige Sätze dahingehend modifizieren, daß wir das Minimalpolynom mit allen bekannten Nullstellen approximieren. Sei hierzu l die Anzahl der bekannten Blöcke. Weiterhin gehen wir davon aus, daß die approximierten Nullstellen $\delta_1, \ldots, \delta_l$ bereits berechnet wurden. Hiernach bilden wir das Polynom h mittels $h(t) = \prod_{1\leq i\leq l}(t-\delta_i)$. Analog zu oben können wir nun ein Gitter Λ vom Rang $m+1$ aufbauen, welches alle Polynome vom Grad kleiner als m enthält, die modulo $p^k\mathbb{Z}[t]$ von h geteilt werden. Eine Basis von Λ hat dann folgende Form:

$$\{p^k t^i : 0 \leq i < l\} \cup \{ht^j : 0 \leq j \leq m-l\}.$$

Mit diesen Bezeichnungen können die beiden folgenden Sätze analog zu 5.6 und 5.8 bewiesen werden.

Satz 5.9. *Seien p, f, m, l, h, h_0 und g wie oben definiert. Nun gelte für ein $b \in \Lambda$: $p^{kl} > |f|^m|b|^m$. Dann ist b in $\mathbb{Z}[t]$ durch f teilbar und damit gilt* $\mathrm{ggT}(f,b) = f \neq 1$.

Satz 5.10. *Seien Λ, p, f, k, l und m wie oben definiert. Weiterhin haben wir eine LLL-reduzierte Basis $b_1, \ldots, b_m$ von Λ ausgerechnet. Zusätzlich wurden p und k so bestimmt, daß $p^{kl} > 2^{\frac{m^2}{2}}|f|^{2m}$ gilt. Dann sind die beiden folgenden Aussagen äquivalent:*

(1) $\deg(f) \leq m$
(2) $|b_1| < (\frac{p^{kl}}{|f|^m})^{\frac{1}{m}}$

Wie wir an diesen beiden Aussagen sehen, ist es für die Bestimmung von k (in Abhängigkeit von p) von großer Bedeutung, wenn $l > 1$ ist. Einerseits muß dann das Hensel-Lifting nicht so weit durchgeführt werden, andererseits kann der LLL-Algorithmus mit wesentlich kleineren Zahlen arbeiten, was in der Laufzeit Größenordnungen ausmacht. Aufgrund dieser Beobachtung ist man geneigt zu versuchen, möglichst viele Blöcke eines Blocksystems zu bestimmen. Dies scheitert jedoch meistens daran, daß nicht alle Blöcke k-Wert 1 haben. Dieses Problem werden wir dann im nächsten Abschnitt lösen, wo wir auch Approximationen von primitiven Elementen von Blöcken bestimmen werden, deren k-Wert größer 1 ist.

4. Ein zweites Verfahren zur Berechnung von Teilkörpern

In diesem Abschnitt untersuchen wir ein zweites Verfahren zur Teilkörperberechnung. Grundlage dieses Verfahrens ist die Kenntnis eines kompletten Blocksystems von Blöcken der Größe d der Galoisgruppe von f. Wie in den vorangegangenen Abschnitten ist f ein erzeugendes Polynom eines Zahlkörpers K vom Grad n. Zur Bestimmung des Blocksystems wurde f modulo einer Primzahl p faktorisiert. Das folgende Verfahren ist auch dann durchführbar, wenn die zugehörigen k-Werte ungleich 1 sind. Falls ein k-Wert größer als 1 ist, so bedeutet dies, daß Elemente aus einem Zykel in k Blöcken enthalten sind. Weiterhin müssen wir das Problem lösen, wie wir das Produkt der Nullstellen berechnen können, die in einem Block liegen. Im vorherigen Verfahren haben wir dieses Produkt derart berechnet, daß wir das Produkt der absoluten Glieder der zugehörigen Faktoren gebildet haben. Hierbei mußten wir allerdings auf das Vorzeichen achten. Diese Möglichkeit haben wir bei einem k-Wert, der größer als 1 ist, nicht mehr. Hier müssen wir uns eine andere Möglichkeit ausdenken. Die Hauptidee des folgenden Verfahrens besteht darin, das Polynom f nicht nur modulo p in $\mathbb{F}_p[t]$, sondern sogar in $\mathbb{F}_q[t]$ mit $q = p^k$ zu faktorisieren. Die zugehörigen Polynome f_i, die Nullstellen von einem Block enthalten, zerfallen dann in k Faktoren gleicher Länge. Hiernach können wir dann wieder das Produkt der Nullstellen als Produkt der absoluten Glieder der zugehörigen Faktoren ausrechnen.

4.1. Berechnung von Teilkörpern im Spezialfall $\mathbf{C_n \subset G}$

Wir wollen unser Verfahren zuerst für einen Spezialfall herleiten, damit die Ideen klarer sind. So werden wir unser Verfahren für den Spezialfall herleiten, daß die zyklische Gruppe C_n Untergruppe der Galoisgruppe von f ist. Dies bedeutet, daß eine Primzahl p existiert, für die f mod p irreduzibel ist. Wir gehen im weiteren davon aus, daß eine solche Primzahl bereits gefunden wurde. Dieser Spezialfall ist für uns sehr vorteilhaft, da nach 4.13 nur ein Teilkörper vom vorgegebenen Grad m existieren kann. Wir werden nun versuchen, einen Teilkörper vom Grad m zu bestimmen bzw. zeigen, daß ein solcher nicht existiert.

Sei nun d die zugehörige Blockgröße ($md = n$). Wir betrachten nun die Körpererweiterung $\mathbb{F}_q/\mathbb{F}_p$, wobei $q = p^m$ gilt. Diese Körpererweiterung kann von einem beliebigen irreduziblen Polynom erzeugt werden. Sei nun f auf kanonische Weise in $\mathbb{F}_q[t]$ eingebettet. Da f in $\mathbb{F}_p[t]$ irreduzibel und m ein Teiler von n ist, faktorisiert f in $\mathbb{F}_q[t]$ in m Faktoren f_i $(1 \leq i \leq m)$ vom Grad d.

$$\begin{tikzcd} \mathbb{F}_{p^n} \arrow[d, dash] & & & \\ \mathbb{F}_q \arrow[d, dash] & \cong & \mathfrak{o}_{\mathcal{E}}/\mathfrak{p}_{\mathcal{E}} \arrow[d, dash] & \mathfrak{o}_{\mathcal{E}} \arrow[d, dash] \\ \mathbb{F}_p & \cong & \mathbb{Z}_p/\mathfrak{p} & \mathbb{Z}_p \end{tikzcd}$$

Seien nun die $\tilde{a}_i \in \mathbb{F}_q$ die absoluten Glieder der Polynome f_i. Wir definieren nun: $a_i := (-1)^d \tilde{a}_i$ $(1 \leq i \leq m)$. Die a_i's sind in gewisser Weise die Approximationen für die Nullstellen eines gesuchten Minimalpolynoms g des Teilkörpers vom Grad m. Wir bilden daher das Polynom g_1 mittels

$$g_1(t) = \prod_{i=1}^{m} (t - a_i).$$

Im folgenden Satz werden wir zeigen, daß $g_1 \in \mathbb{F}_p[t]$ gilt.

SATZ 5.11. *Sei $g_1 \in \mathbb{F}_q[t]$ wie oben definiert. Dann gilt sogar $g_1 \in \mathbb{F}_p[t]$.*

Beweis: Definiere Mengen $\Delta_1, \ldots, \Delta_m$ derart, daß Δ_i die Nullstellen von f_i (dargestellt in $\mathbb{F}_{p^n}$) enthält. Wenn wir zeigen können, daß die Δ_i $(1 \leq i \leq m)$ Blöcke der Galoisgruppe G von $\mathbb{F}_{p^n}/\mathbb{F}_p$ sind, folgt die Behauptung mit 4.14. Sei hierzu ein beliebiges $g \in G$ gegeben. Sei H_1 die Galoisgruppe von $\mathbb{F}_{p^n}/\mathbb{F}_q$ und H_2 die Galoisgruppe von $\mathbb{F}_q/\mathbb{F}_p$. Dann läßt sich g auf eindeutige Weise als Produkt $g = h_1 h_2$ mit $h_1 \in H_1$ und $h_2 \in H_2$ schreiben. O.E. reicht es, wenn wir zeigen, daß Δ_1 ein Block ist. Wir wollen dies mit der Definition 4.1 tun. Die Koeffizienten des Polynoms f_1 liegen alle in $\mathbb{F}_q$. Dies bedeutet, daß sie von allen Elementen aus H_1 und damit auch von h_1 invariant gelassen werden. Damit gilt $\Delta^{h_1} = \Delta$. Da die $f_i \in \mathbb{F}_q[t]$ $(1 \leq i \leq m)$ sind, wird f_1 von h_2 auf ein f_j $(1 \leq j \leq m)$ abgebildet. Damit geht dann Δ_1 auf Δ_j über. Insgesamt gilt also: $\Delta^g \cap \Delta \in \{\emptyset, \Delta\}$. Damit ist die Behauptung gezeigt. □

Das soeben berechnete Polynom g_1 ist eine modulo p-Approximation des gesuchten Minimalpolynoms g. Dies bedeutet, daß

$$g_1(t) \equiv g(t) \bmod p\mathbb{Z}[t]$$

gilt. Diese Aussage ist ein Spezialfall von Satz 5.15, der im folgenden noch bewiesen wird. Wenn man weiß, daß der Betrag der Koeffizienten von g stets kleiner als $\frac{p}{2}$ ist, wäre man an dieser Stelle fertig. I.allg. gilt diese Beziehung nicht. Ziel ist es also, im folgenden zu einer modulo p^k-Approximation zu kommen. Dazu werden wir die zugehörigen p-adischen Körper $\mathbb{Q}_p$ und $\mathcal{E} = K_{\mathfrak{P}}$, wobei $\mathfrak{P}$ das eindeutige Primideal in K ist, welches über $\mathfrak{p} = p\mathbb{Z}$ liegt. Hierbei ist $\mathfrak{P}$ eindeutig bestimmt, da $f \bmod \mathfrak{p}$ irreduzibel ist. Weiterhin bezeichnen wir mit $\mathfrak{o}_{\mathcal{E}}$ die Maximalordnung von $\mathcal{E}$. Da $\mathfrak{p}$ unverzweigt in K ist, können wir eine Gleichungsordnung von $\mathcal{E}$ angeben, die bereits Maximalordnung ist. Sei hierzu $\bar{h} \in \mathbb{F}_p[t]$, welches die Körpererweiterung $(\mathcal{E}/\mathfrak{P})/(\mathbb{Z}/p\mathbb{Z})$ erzeugt. Wähle nun ein $h \in \mathbb{Z}_p[t]$ mit $h \equiv \bar{h} \bmod \mathfrak{p}$. Die von diesem Polynom h erzeugte Gleichungsordnung ist wegen 3.19 bereits die Maximalordnung. Dies vereinfacht das Rechnen in dieser Struktur sehr, wie das folgende Korollar zeigt. Hierzu sei γ eine Nullstelle von h.

KOROLLAR 5.12. *Sei $k \in \mathbb{N}$ und $x \in \mathfrak{o}_{\mathcal{E}}$, d.h. $x = \sum_{i=0}^{m-1} x_i\gamma^i$ $(x_i \in \mathbb{Z}_p)$. Dann gilt $x \in \mathfrak{P}^k$ genau dann, wenn $x_i \in \mathfrak{p}^k$ $(0 \leq i < m)$ gilt.*

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

Wir werden nun erläutern, wie wir zu einer modulo p^k-Approximation unseres gesuchten erzeugenden Polynoms kommen. Hierzu stellen wir zuerst einmal fest, daß die Galoisgruppen von $\mathbb{F}_q/\mathbb{F}_p$ und $\mathcal{E}/\mathbb{Q}_p$ gleich sind (vgl. 3.18). Sei nun

$$f = \hat{f}_1 \cdot \ldots \cdot \hat{f}_m \tag{5-1}$$

die Faktorisierung von f in irreduzible Faktoren $\hat{f}_i$ in $\mathfrak{o}_{\mathcal{E}}[t]$. Diese Faktoren haben alle Grad d. Analog zu oben definieren wir $b_i := (-1)^d\tilde{b}_i$ $(1 \leq i \leq m)$, wobei die $\tilde{b}_i$ die absoluten Glieder der Polynome $\hat{f}_i$ sind. Setzen wir abschließend

$$\tilde{g}(t) := \prod_{i=1}^{m}(t - b_i) \in \mathfrak{o}_{\mathcal{E}}[t],$$

so gilt der folgende Satz.

SATZ 5.13. *Sei $\tilde{g} \in \mathfrak{o}_{\mathcal{E}}[t]$ wie oben definiert. Dann gilt sogar $\tilde{g} \in \mathbb{Z}_p[t]$.*

Beweis: Der Beweis verläuft völlig analog zum Satz 5.11. □

Anhand dieses Satzes sieht man, auf welche Weise man versuchen kann, ein erzeugendes Polynom des gesuchten Teilkörpers zu berechnen. Der Vorteil der p-adischen Körper liegt darin, daß wir mit Hilfe des van der Waerden-Kriteriums 2.28 sogar die Nullstellen identifizieren können, die in den einzelnen Zykeln liegen. Dies konnten wir bei den algebraischen Zahlkörpern nicht.

Das weitere Ziel dieses Abschnitts wird es sein, den folgenden Satz zu beweisen. Er wird schließlich eine direkte Folgerung von Satz 5.15 sein.

SATZ 5.14. *Seien $f, \tilde{g}, m, n, d$ wie oben definiert. Weiterhin nehmen wir an, daß K tatsächlich einen Teilkörper L vom Grad m besitzt. Sei $\Delta_1, \ldots, \Delta_m$ das zugehörige Blocksysten und $\delta_i := \prod_{\alpha_i \in \Delta_i} \alpha_i$ $(1 \leq i \leq m)$. Zusätzlich gelte $g(t) = \prod_{i=1}^{m}(t - \delta_i)$.*

Dann sind die Polynome g und $\tilde{g}$ identisch, wenn man $\mathbb{Z}$ auf kanonische Weise in $\mathbb{Z}_p$ einbettet.

Im folgenden müssen wir zeigen, wie wir das Polynom $\tilde{g}$ hinreichend genau berechnen können. Dazu müssen wir eine Schranke B der Koeffizienten des zu berechnenden Polynoms g kennen. Hierzu habe g die Form $g(t) = \sum_{i=0}^{m} c_i t^i$. Die Schranke soll so gewählt sein, daß für alle Koeffizienten gilt: $|c_i| < B$ $(0 \leq i \leq m)$. Wenn eine solche Schranke bekannt ist, bestimmen wir zum gegebenen p ein minimales $k \in \mathbb{N}$ derart, daß $p^k > 2B$ gilt. Wir wollen nun ein Polynom $g_k \in \mathbb{Z}[t]$ bestimmen, so daß $g_k \equiv g \bmod p^k\mathbb{Z}[t]$ gilt. Wenn wir nun g_k in einem geeigneten Restsystem (symmetrisch zur 0) darstellen, gilt wegen der gefundenen Schranke B: $g = g_k$.

Um dieses Verfahren zu beschreiben, werden wir von der Faktorisierung

$$f(t) = f_1(t) \cdot \ldots \cdot f_m(t) \text{ in } \mathbb{F}_q[t]$$

ausgehen. Da $\mathfrak{P}$ träge ist, ist $\mathfrak{o}_{\mathcal{E}}/\mathfrak{P} \cong \mathbb{F}_q$. Damit ist die Voraussetzung (1) des Hensel-Lemmas 2.24 erfüllt. Die a_{i0} $(0 \leq i \leq 2)$, die in Voraussetzung (2) benötigt werden, können im euklidischen Ring $\mathbb{F}_q[t]$ einfach berechnet werden. Die Konstruktivität dieser Berechnungen wird im nächsten Abschnitt beschrieben. Damit sind alle Voraussetzungen des Hensel-Liftings erfüllt. Wir können also im folgenden eine Kongruenzfaktorisierung der Form

$$f(t) \equiv \tilde{f}_1(t) \cdot \ldots \cdot \tilde{f}_m(t) \bmod \mathfrak{P}^k[t]$$

berechnen. Analog zu oben werden die $\tilde{d}_i$ $(1 \leq i \leq m)$ als die absoluten Glieder der Polynome $\tilde{f}_i$ definiert. Wir setzen weiterhin $d_i := (-1)^d \tilde{d}_i$ $(1 \leq i \leq m)$. Da die $\tilde{f}_i$ modulo $\mathfrak{P}^k[t]$ berechnet worden sind, gilt:

$$b_i \equiv d_i \bmod \mathfrak{P}^k \text{ für } 1 \leq i \leq m.$$

Nun können wir das Polynom g_k durch $g_k(t) = \prod_{i=1}^m (t - d_i)$ definieren. Nach Konstruktion ist es klar, daß

$$g_k(t) \equiv \tilde{g}(t) \bmod \mathfrak{p}^k[t]$$

gilt. Nachdem wir nun beschrieben haben, wie wir das Polynom in der Praxis konstruieren wollen, werden wir im folgenden Satz die Korrektheit des gesamten Verfahrens beweisen. Der Beweis dieses Satz ist allerdings nicht konstruktiv, da man in der Praxis weder im Zerfällungskörper von K noch in den zugehörigen Vervollständigungen rechnet.

Satz 5.15. *Das Polynom g_k ist modulo p^k kongruent zum gesuchten Minimalpolynom g. Dabei soll g_k auf kanonische Weise in $\mathbb{Z}[t]$ eingebettet werden.*

Beweis: Zuerst überlegen wir uns, wie wir das Polynom g in der Theorie berechnen können. Sei hierzu $\Delta_1, \ldots, \Delta_m$ das zugehörige Blocksystem der Körpererweiterung K/L (vgl. 4.11). Nehmen wir nun o.E. an, daß die Nullstellen α_i von f so angeordnet sind, daß für $(j-1)d + 1 \leq i \leq dj$ gilt: $\alpha_i \in \Delta_j$. Dann können wir das Polynom g auf folgende Weise schreiben:

$$g(t) = \prod_{j=1}^{m} (t - \prod_{\alpha \in \Delta_j} \alpha) = \prod_{j=1}^{m} (t - \prod_{i=(j-1)d+1}^{jd} \alpha_i).$$

Da wir alle Nullstellen von f bei der Berechnung von g benutzen, können wir i.allg. die Berechnungen nicht in $K = \mathbb{Q}(\alpha_1)$ durchführen, da K nicht notwendigerweise normal ist. Deswegen führen wir die Berechnungen im Zerfällungskörper $M = \mathbb{Q}(\alpha_1, \ldots, \alpha_n)$ durch. Wir bezeichnen mit $\mathfrak{o}_K$ und $\mathfrak{o}_M$ die Maximalordnungen von K und M. Da $f \bmod p$ irreduzibel ist, existiert in K genau ein Primideal $\mathfrak{p}_K$, welches über $p\mathbb{Z}$ liegt. Dieses ist klarerweise unverzweigt. Damit ist dann nach 2.19 auch jedes Primideal in M unverzweigt, welches über $p\mathbb{Z}$ liegt. Da M zudem eine normale Erweiterung ist, haben alle Primideale in M, welche über p liegen, den selben Trägheitsgrad f. Nehmen wir nun an, daß genau r Primideale $\mathfrak{P}_1, \ldots, \mathfrak{P}_r$ über p liegen. Wenn wir nun die zugehörigen p-adischen Zahlkörper $M_{\mathfrak{P}_i}$ $(i = 1, \ldots, r)$ betrachten, so sind sie alle isomorph, da sie alle unverzweigt sind und den selben Grad über $\mathbb{Q}_p$ haben. Deswegen reicht es aus, nur den p-adischen Zahlkörper $M_{\mathfrak{P}} = M_{\mathfrak{P}_1}$ zu betrachten. Wie wir oben gezeigt haben, können wir in diesem Körper ein Polynom $\tilde{g}$ berechnen, welches sogar in $\mathbb{Z}_p[t]$

liegt. Wenn wir nun M auf kanonische Weise in $M_{\mathfrak{P}}$ einbetten, erhalten wir für jedes $k \in \mathbb{N}$, daß $\tilde{g} \equiv g \bmod p^k$ ist. Damit ist die Behauptung des Satzes gezeigt. $\square$

5. Zum Hensel-Lifting über dem Ring $\mathfrak{o}_{\mathcal{E}}$

Im vorherigen Abschnitt haben wir gezeigt, daß die Voraussetzungen des Hensel-Lemmas 2.24 erfüllt sind und damit das Verfahren durchführbar ist. Wenn wir dieses Problem jedoch aus konstruktiver Sicht betrachten, so ist die Implementierung bis jetzt nicht vollständig erklärt worden. Auf diese Punkte soll in diesem Abschnitt eingegangen werden.

Ein erstes Problem ist die Darstellung des p-adischen Körpers $\mathcal{E}$ bzw. die Darstellung seiner Maximalordnung $\mathfrak{o}_{\mathcal{E}}$. Sei hierzu $\mathfrak{p}_{\mathcal{E}}$ das Primideal und m der Grad von $\mathcal{E}$. Wir sind wir nicht an einer vollständigen Darstellung von $\mathfrak{o}_{\mathcal{E}}$, sondern lediglich an Elementen modulo $\mathfrak{p}_{\mathcal{E}}^k$ interessiert. Sei also $h \in Z[t]$ vom Grad m, welche modulo $p\mathbb{Z}[t]$ irreduzibel ist. Wenn wir h auf kanonische Weise in $\mathbb{Z}_p[t]$ einbetten, ist die von h erzeugte Gleichungsordnung bereits $\mathfrak{o}_{\mathcal{E}}$. Wir erzeugen mit h einen algebraischen Zahlkörper als Körpererweiterung von $\mathbb{Q}$ und betrachten seine Gleichungsordnung O. Da $h \bmod p$ irreduzibel ist, ist das Ideal $p\mathbb{Z}$ träge in O. Wir möchten nun Elemente von $\mathfrak{o}_{\mathcal{E}}$ modulo $\mathfrak{p}_{\mathcal{E}}^k$ darstellen. Nach 5.12 können wir solche Elemente in O darstellen, wobei wir die einzelnen Koeffizienten der Gleichungsordnung modulo p^k bestimmen. Somit können wir alle Berechnungen, die wir benötigen, in O machen. Dies ist eine Ordnung eines algebraischen Zahlkörpers. Die Arithmetik in solchen Ordnungen wird zum Beispiel in [Poh] erläutert und ist ein fester Bestandteil des Programmierpakets KANT (vgl. [Poh]). Ich möchte daher an dieser Stelle nicht mehr weiter darauf eingehen. Wenn wir nun den Algorithmus 2.25 betrachten, stellen wir fest, daß die meisten Schritte nur aus Additionen und Multiplikationen bestehen. Diese Operationen bereiten uns, wie bereits gesagt, keine Probleme. Lediglich in den Schritten 6 und 10 taucht die Division mit Rest auf. Hier müssen wir noch zeigen, daß diese Operation überhaupt durchführbar ist. Die Division mit Rest wird jeweils modulo $f_{ji}\,(i \in \mathbb{N}, j = 1, 2)$ durchgeführt. Diese Polynome haben die folgende Eigenschaft.

Bemerkung 5.16. *Die Polynome $f_{ji}\,(i \in \mathbb{N}, j = 1, 2)$ aus 2.25 sind alle normiert.*

Beweis: Am Anfang sind die Polynome $f_{j0}\,(j = 1, 2)$ normierte Polynome. Die neuen f_{ji} werden jeweils im 7. Schritt durch $f_{j(i+1)} = f_{ji} + d_{ji}$ berechnet. Dabei hat das d_{ji} wegen Schritt 6 stets einen kleineren Grad als f_{ji}. Deswegen ist auch $f_{j(i+1)}$ normiert, wenn f_{ji} normiert war. $\square$

Wenn wir uns nun den Algorithmus der Division mit Rest betrachten, so stellen wir fest, daß im ersten Schritt jeweils ein Monom durch den Leitkoeffizienten von f_{ji} geteilt wird. Da dieser 1 ist, ist dieser Schritt trivial. Hiernach werden nur Additionen bzw. Multiplikationen benötigt, die uns keine Probleme bereiten. Mittels dieser Überlegungen sind wir nun in der Lage, das Hensel-Lifting für unseren Spezialfall auf dem Rechner zu implementieren.

6. Der allgemeine Fall

In diesem Abschnitt werden wir das Verfahren beschreiben, wie wir Teilkörper berechnen können, wenn wir nicht das Glück haben, eine Primzahl p zu finden, für die $f \bmod p$ irreduzibel ist. Wie bisher sei $K = \mathbb{Q}(\alpha_1)$ ein algebraischer Zahlkörper, wobei $\alpha_1, \dots, \alpha_n$ die Nullstellen des irreduziblen, normierten Polynoms $f \in \mathbb{Z}[t]$ sind. Wie bisher gehen wir davon aus, daß ein Teilkörper L vom Grad m existiert. Hierzu sei $\Delta_1, \dots, \Delta_m$ das zugehörige Blocksystem.

Am Anfang des Verfahrens fixieren wir eine Primzahl p, die uns für die Durchführung des Verfahrens günstig erscheint. Welche Kriterien wir dafür ansetzen, wird an anderer Stelle erörtert werden. Wir faktorisieren dann f modulo p und erhalten dann folgende Kongruenzfaktorisierung:

$$f \equiv f_1 \cdot \ldots \cdot f_u \bmod p\mathbb{Z}[t].$$

Aus dieser Faktorisierung können wir dann mittels 2.28 den Zykeltyp $[n_1, \dots, n_u]$ eines Elements π der Galoisgruppe von f bestimmen. Wir gehen an dieser Stelle davon aus, daß bereits die k-Werte $k_1, \dots, k_m$ der Blöcke $\Delta_1, \dots, \Delta_m$ bestimmt worden sind. Wir wissen außerdem, aus welchen Zykeln die einzelnen Blöcke zusammengesetzt sind. Wir müssen im folgenden die Nullstellen identifizieren, die in den einzelnen Blöcken liegen. Falls der k-Wert eines Blocks 1 ist, so bereitet dies keine Probleme, da alle Nullstellen eines Zykels verwendet werden. Was machen wir also, wenn k-Werte einzelner Blöcke größer als 1 sind?

Das Hauptproblem besteht darin, die Nullstellen eines Zykels auf die k verschiedenen Blöcke aufzuteilen. Aufgrund von 2.28 kennen wir die Aktion von einem Element π. Wir kennen hiermit die komplette zyklische Untergruppe, die von π erzeugt wird. Die Nullstellen, auf denen π operiert, können wir aber nur in der zugehörigen p-adischen Vervollständigung bzw. dem zugehörigen endlichen Restklassenkörper identifizieren. An dieser Stelle wollen wir uns noch einmal erinnern, was der k-Wert überhaupt bedeutet. Wenn Δ der zugehörige Block ist, so war k die kleinste natürliche Zahl größer gleich 1, für die $\Delta^{\pi^k} = \Delta$ gilt. Diese Gleichheit bedeutet, daß sich unser gesuchter Block aus kompletten Zykeln von π^k zusammensetzt. Dabei brauchen nur Zykel beachtet werden, die aus einem Zykel von π entstanden sind, dessen Länge durch k teilbar ist. Unser Problem ist es nun, die Aktionen von π^k zu bestimmen. Dazu faktorisieren wir f über der unverzweigten Erweiterung $\mathcal{F}$ vom Grad k über $\mathbb{Q}_p$. Die Faktoren dieser Faktorisierung liefern uns analog zu 2.28 die gewünschte Aktion. Hiernach können wir die Nullstellen in einer passenden Erweiterung von $\mathbb{Z}_p$ bestimmen, die zum gesuchten Block gehören. Dieses Verfahren können wir dann sukzessive für die anderen Blöcke wiederholen. Wichtig ist, daß wir die Nullstellen, die zu den einzelnen Blöcken gehören, identifiziert haben. Im nächsten Schritt bilden wir das kleinste gemeinsame Vielfache der verschiedenen k-Werte und bezeichnen dieses mit l. Wir gehen dann in eine unverzweigte Erweiterung vom Grad l über $\mathbb{Q}_p$ und faktorisieren f über dem zugehörigen endlichen Restklassenkörper. Hiernach können wir das Hensel-Lifting bis zur geforderten Genauigkeit anwenden. Insgesamt führen wir den folgenden Algorithmus durch:

Algorithmus 5.17. *Berechnung eines Teilkörpers im allgemeinen Fall*

Input: *Ein erzeugendes Polynom f eines Zahlkörpers K.*
Eine Primzahl p und ein mögliches Blocksystem $\Delta_1, \dots, \Delta_m$.
Output: *Ein erzeugendes Polynom g eines möglichen Teilkörpers L.*

(1) *Faktorisiere f modulo p und bestimme die k-Werte der Blöcke $\Delta_1, \dots, \Delta_m$.*
(2) *Für $i = 1, \dots, m$ tue folgendes:*
  (a) *Bestimme die Zykel und die zugehörigen Polynome, die Elemente im Block Δ_i haben.*
  (b) *Faktorisiere diese Polynome in einer Erweiterung vom Grad k_i und ermittle dann die Nullstellen, die zum Block Δ_i gehören.*
(3) *Bestimme $l = \mathrm{kgV}(k_1, \dots, k_m)$.*
(4) *Faktorisiere f in einer Erweiterung vom Grad l.*
(5) *Wende auf diese Faktorisierung das Hensel-Lifting bis zu einer genügenden Genauigkeit an.*
(6) *Für $i = 1, \dots, m$ berechne das Produkt δ_i der Nullstellen, die im Block Δ_i liegen.*
(7) *Berechne das Polynom $g(t) = \prod_{i=1}^{m}(t - \delta_i)$.*

Bis auf die angesprochenen Änderungen funktioniert dieser Algorithmus ähnlich zu dem vorher besprochenen. Er sollte daher selbsterklärend sein. Zum Abschluß dieses Abschnitts verbleibt uns die Korrektheit dieses Verfahrens zu zeigen. Diese folgt aus den beiden folgenden Sätzen.

Hierzu sei l das kleinste gemeinsame Vielfache der im Algorithmus berechneten k-Werte. E sei die unverzweigte Erweiterung vom Grad l über $\mathbb{Q}_p$. Weiterhin ist δ_i für $i = 1, \ldots, m$ das Produkt der Nullstellen, die in Δ_i liegen. Dabei können die Nullstellen natürlich in einer passenden Erweiterung von E liegen. Wir definieren dann das Polynom

$$\tilde{g} = \prod_{i=1}^{m} (t - \delta_i).$$

SATZ 5.18. *Sei $\tilde{g} \in \mathfrak{o}_{\mathcal{E}}[t]$ wie oben definiert. Dann gilt sogar $\tilde{g} \in \mathbb{Z}_p[t]$.*

Beweis: Der Beweis verläuft ähnlich zum Beweis des Satzes 5.11. Dort wird die Behauptung gezeigt, wenn $f \bmod p$ irreduzibel ist. Als ersten Schritt faktorisieren wir $f \bmod p$ und erhalten:

$$f \equiv f_1 \cdot \ldots \cdot f_u \bmod p.$$

Jedem dieser Faktoren f_j ist ein k-Wert zugeordnet. Hiermit ist der k-Wert eines Blockes Δ gemeint, der Nullstellen von f_j enthält. Falls dieser k-Wert 1 ist, so ist bereits $\delta_i \in \mathbb{Z}_p$. Interessant ist der Fall, daß der zugehörige k-Wert > 1 ist. Nach 4.7 existieren dann k konjugierte Blöcke, die Nullstellen der selben Polynome enthalten wie Δ. O.E. bezeichnen wir diese Blöcke mit $\Delta_1, \ldots, \Delta_k$.

Wir betrachten nun das folgende Polynom:

$$h(t) = \prod_{i=1}^{k} (t - \delta_i) \in \tilde{E}[t].$$

Hierbei ist $\tilde{E}$ die eindeutige unverzweigte Erweiterung von $\mathbb{Q}_p$ vom Grad k. Wir wollen nun zeigen, daß bereits $h \in \mathbb{Z}_p[t]$ gilt. Damit wäre dann auch $\tilde{g} \in \mathbb{Z}_p[t]$ gezeigt. Seien nun o.E. $f_1, \ldots, f_r$ die Polynome, die Nullstellen von $\Delta_1, \ldots, \Delta_k$ besitzen. Diese Polynome faktorisieren wir dann in $\tilde{E}[t]$ und erhalten:

$$f_j = \prod_{i=1}^{k} f_{i,j} \text{ für } j = 1, \ldots, r.$$

Hierbei sollen die $f_{i,j}$ so angeordnet werden, daß die Nullstellen von $f_{i,j}$ in Δ_i liegen. Das Produkt der Nullstellen eines Polynoms $f_{i,j}$ bezeichnen wir mit $\delta_{i,j}$. Sei σ der Erzeuger der zyklischen Galoisgruppe von $\tilde{E}/\mathbb{Q}_p$ (Frobeniusautomorphismus). Dann können wir o.E. davon ausgehen, daß die Faktoren $f_{i,j}$ von f_j so angordnet sind, daß $f_{i,j} = \sigma^i(f_{1,j})$ gilt. Wir erhalten:

$$\begin{aligned} h(t) &= \prod_{i=1}^{k}(t-\delta_i) \\ &= \prod_{i=1}^{k}(t-\prod_{j=1}^{r}\delta_{i,j}) \end{aligned}$$

Hieraus folgt:

$$\begin{aligned} \sigma(h(t)) &= \prod_{i=1}^{k}(t-\prod_{j=1}^{r}\sigma(\delta_{i,j})) \\ &= \prod_{i=1}^{k}(t-\prod_{j=1}^{r}(\delta_{i+1,j})) \text{ mit } \delta_{k+1,j}=\delta_{1,j} \\ &= \prod_{i=1}^{k}(t-\delta_{i+1}) \text{ mit } \delta_{k+1}=\delta_1 \\ &= \prod_{i=1}^{k}(t-\delta_i) = h(t) \end{aligned}$$

Damit ist gezeigt, daß $h \in \mathbb{Z}_p[t]$ gilt. Hieraus folgt dann die Behauptung des Satzes. □

SATZ 5.19. *Es gelten die Bezeichnungen vom Algorithmus* 5.17. *Wir nehmen an, daß das Hensel-Lifting bis zu einer Genauigkeit modulo p^k durchgeführt wurde. Dann ist das so berechnete Polynom g modulo p^k kongruent zum gesuchten erzeugenden Polynom.*

Beweis: Der Beweis dieses Satzes verläuft vollkommen analog zum Beweis des Satzes 5.15. Wir gehen wieder von K zu einer normalen Hülle N über. Analog erhalten wir, daß das Ideal $p\mathbb{Z}$ in r Ideale vom Trägheitsgrad f zerfällt. Wiederum bleibt $p\mathbb{Z}$ unverzweigt. Somit können wir alle Schritte dieses Beweises analog durchführen. □

7. Beispiele

Zum Abschluß dieses Kapitels wollen wir unsere Methoden an einem Beispiel erläutern. Dazu knüpfen wir an das Beispiel des letzten Kapitels an und wählen wieder den Körper K, der von $f(t) = t^6 + 108$ erzeugt wird. Hierbei sind wir an Teilkörper vom Grad 3 interessiert. Die möglichen Blocksysteme haben wir bereits am Ende des 3. Kapitels ausgerechnet. Wir hatten uns entschlossen, die Berechnungen mit $p = 7$ durchzuführen. Es gilt:

$$f(t) \equiv (t^3 + 2)(t^3 + 5) \bmod 7.$$

Alle möglichen Blöcke wurden mit k-Wert 3 konstruiert. Deswegen müssen wir f in $\mathbb{F}_q[t]$ mit $q = 7^3 = 343$ faktorisieren. Sei nun im folgenden w ein geeigneter Erzeuger von $\mathbb{F}_q^\times$. Damit gilt dann:

$$\begin{aligned} t^3 + 2 &= (t + w^{38})(t + w^{152})(t + w^{266}) \text{ in } \mathbb{F}_q[t]. \\ t^3 + 5 &= (t + w^{95})(t + w^{209})(t + w^{323}) \text{ in } \mathbb{F}_q[t]. \end{aligned}$$

Wir wissen, daß diese Nullstellen in zwei Zykeln der Länge 3 liegen. Momentan wissen wir aber noch nichts über die Reihenfolge. Hier hilft uns der Frobeniusautomorphismus weiter. Wegen $(w^{38})^7 = w^{266}$ und $(w^{95})^7 = w^{323}$ gilt,

$$\pi = (-w^{38} - w^{266} - w^{152})(-w^{95} - w^{323} - w^{209}) = (w^{209} w^{95} w^{323})(w^{266} w^{152} w^{38}).$$

Wir sortieren also die Faktoren entsprechend um und können diese Darstellung dann in dem zugehörigen unverzweigten p-adischen Koerper E liften. Aufgrund unserer Abschätzungen für die Koeffizienten des Minimalpolynoms liften wir diese Darstellung modulo $\mathfrak{p}^4$. Im folgenden erzeugen wir E mit $\omega(t) = t^3 + 6t^2 + 4$. Dabei ist $\mathfrak{p}$ das maximale Ideal in E und γ eine Nullstelle von ω. Im folgenden meinen wir mit $[a, b, c]$ das Element $a + b\gamma + c\gamma^2$. Wir erhalten:

$$\begin{aligned} f(t) \equiv\ & (t + [204, 408, 51])(t + [101, 202, -575]) \\ & (t + [-101, -202, 575])(t + [103, 206, 626]) \\ & (t + [-103, -206, -626])(t + [-204, -408, -51]) \bmod \mathfrak{p}^4. \end{aligned}$$

Die Faktoren sind bereits so angeordnet, daß die jeweils in einer Zeile stehenden zu einem Block gehören. Wir können nun δ_1, δ_2 und δ_3 berechnen und bilden das Polynom $\tilde{g} = \prod_{i=1}^{3}(t - \delta_i) = t^3 - 108$. Dieses Polynom ist aufgrund unserer Überlegungen modulo $7^4 = 2401$ kongruent zum gesuchten erzeugenden Polynoms unseres Teilkörpers. Aufgrund unserer Abschätzung wissen wir, daß die Koeffizienten unseres erzeugenden Polynoms betraglich kleiner als 217 sein müssen. Wenn unser Blocksystem gültig war, so erzeugt $g(t) = \tilde{g}(t) = t^3 - 108$ unseren Teilkörper. Ob unsere Vermutung richtig war, wird sich zeigen, wenn wir die Einbettung ausrechnen.

Für die beiden nächsten Blocksysteme müssen wir das Hensel-Lifting nicht erneut durchführen. Wir ordnen lediglich die bereits gelifteten Faktoren um und erhalten:

$$\begin{aligned} f(t) &\equiv (t+[204,408,51])(t+[103,206,626]) \\ &\quad (t+[-101,-202,575])(t+[-204,-408,-51]) \\ &\quad (t+[-103,-206,-626])(t+[101,202,-575]) \bmod \mathfrak{p}^4. \end{aligned}$$

$$\begin{aligned} f(t) &\equiv (t+[204,408,51])(t+[-204,-408,-51]) \\ &\quad (t+[-101,-202,575])(t+[101,202,-575]) \\ &\quad (t+[-103,-206,-626])(t+[103,206,626]) \bmod \mathfrak{p}^4. \end{aligned}$$

Bei beiden Blocksystemen können wir wieder analog das mögliche Minimalpolynom des zugehörigen Teilkörpers ausrechnen und erhalten jeweils $g(t) = t^3 - 108$. Wir stellen also fest, daß die so berechneten drei Körper isomorph zueinander sind. Bei der Berechnung der Einbettung werden wir feststellen, daß sie verschieden eingebettet werden und somit verschiedene Teilkörper erzeugen. Dazu werden wir im nächsten Kapitel mehr erfahren.

KAPITEL 6

Zur Einbettung von Teilkörpern

1. Einleitung

In diesem Kapitel der Arbeit als Ergebnis ein Verfahren zur Einbettung von einem Teilkörper L in den Körper K. Dieser Einbettungsalgorithmus ist allerdings davon abhängig, daß der Teilkörper mit einem der beiden vorgestellten Verfahren konstruiert worden ist. Allgemeine Einbettungsverfahren beruhen entweder auf dem Faktorisieren von Polynomen über Zahlkörpern oder auf Algorithmen, die den LLL-Algorithmus verwenden. Diese Verfahren können z.B. in [Coh] nachgelesen werden. Sie sind aber in der Praxis für größere Körpergrade (z.B. Einbettung von Grad 10 in 20) erheblich zu langsam.

Wie in den vorherigen Kapiteln sei $f \in \mathbb{Z}[t]$ normiert und irreduzibel vom Grad n. Eine Nullstelle α von f erzeuge den algebraischen Zahlkörper K. Weiterhin seien $\{\alpha = \alpha_1, \alpha_2 \ldots, \alpha_n\}$ die Nullstellen von f. Der berechnete Teilkörper L vom Grad m sei von einem β erzeugt, dessen Minimalpolynom ein $g \in \mathbb{Z}[t]$ ist. Analog seien $\{\beta = \beta_1, \beta_2, \ldots, \beta_m\}$ die Nullstellen von g. Zusätzlich sei d die zugehörige Blockgröße.

Unsere Berechnung beruht darauf, daß wir wissen, daß das erzeugende Polynom des Teilkörpers L mit Hilfe von Satz 4.14 konstruiert worden ist. Dies bedeutet, daß die Nullstellen β_j das Produkt von d passenden Nullstellen α_i sind. Diesen Umstand wollen wir für eine effiziente Berechnung der Einbettung ausnutzen.

Nach Satz 2.4 wollen wir ein Polynom $\omega \in \mathbb{Q}[t]$ derart berechnen, daß g Minimalpolynom zu $\omega(\alpha)$ ist, d.h. $\omega(\alpha) = \beta$ gilt. Aufgrund dieser Anforderung können wir noch weitere Eigenschaften von ω herleiten, wie der folgende Satz zeigt.

Satz 6.1. *Sei $\Delta_1, \ldots, \Delta_m$ das zugehörige Blocksystem zum Teilkörper L von K.*

Weiterhin seien die Nullstellen α_i o.E. so angeordnet, daß die α_i mit $(j-1)d+1 \leq i \leq jd$ in Δ_j liegen. Weiterhin habe $\omega \in \mathbb{Q}[t]$ die Eigenschaft $\omega(\alpha_1) = \beta_1$. Dann gilt für $1 \leq i \leq n$ sogar $\omega(\alpha_i) = \beta_j$, wenn $\alpha_i \in \Delta_j$ ist.

Beweis: Es sei ein i fixiert, so daß $\alpha_i \in \Delta_j$ ist. Nach Voraussetzung ist $\omega(\alpha_1) = \beta_1 = \prod_{k=1}^{d} \alpha_k$. Da $G = Gal(f)$ transitiv auf $\{\alpha_1, \ldots, \alpha_n\}$ operiert, existiert ein $\pi \in G$, welches α_1 auf α_i abbildet. Wegen der Blockeigenschaft bildet dieses π jedes Element von Δ_1 auf ein Element von Δ_j ab. Damit gilt die folgende Gleichung:

$$\omega(\alpha_i) = \omega(\pi(\alpha_1)) = \pi(\omega(\alpha_1)) = \pi(\beta_1) = \pi(\prod_{k=1}^{d} \alpha_k) = \prod_{k=(j-1)d+1}^{jd} \alpha_k = \beta_j$$

□

Mittels dieses Satzes haben wir ein Kriterium gefunden, wie wir das Polynom ω effizient berechnen können. Durch die Gleichung $\omega(\alpha_i) = \beta_j$ $(1 \leq i \leq n, j$ passend) haben wir n Funktionswerte eines Polynoms gegeben, welches höchstens Grad $n-1$ hat. Damit ist dieses Polynom durch die vorgegebenen Funktionswerte eindeutig berechenbar. Um diese Werte berechnen zu können, benötigen wir wie in den vergangenen Kapiteln eine Einteilung der Nullstellen $\alpha_i\,(1 \leq i \leq n)$ in Blöcke. Diese Einteilung kennen wir nur in einer passenden endlichen Erweiterung von $\mathbb{F}_p$. Deswegen werden wir versuchen, dieses Polynom ω erst modulo p zu berechnen, um danach das Ergebnis bis zu einer genügenden Genauigkeit zu liften. Hiernach soll dann aus dieser Approximation das Polynom $\omega \in \mathbb{Q}[t]$ bestimmt werden. Interessant an diesem Teil des Algorithmus ist, daß wir mit modulo p-Approximationen Elemente aus $\mathbb{Q}$ bestimmen können. Auf dieses Phänomen wird in einem der folgenden Abschnitte noch genauer eingegangen werden.

Wir wollen im folgenden den Algorithmus skizzieren.

ALGORITHMUS 6.2. *Berechnung der Einbettung eines Teilkörpers*

Input:	*Erzeugendes Polynom f eines Körpers K.*
	Konstruiertes Erzeugendes Polynom g eines Teilkörpers L.
Output:	*Einbettungspolynom $\omega \in \mathbb{Q}[t]$, falls L Teilkörper von K ist.*

(1) *Fixiere ungerades $p \in \mathbb{P}$ mit $p \not| \operatorname{disc}(f) \operatorname{disc}(g)$.*
(2) *Berechne das zugehörige Blocksystem. Falls dieses nicht eindeutig bestimmbar ist, führe die folgenden Schritte mit allen möglichen Blocksystemen durch.*
(3) *Bestimme aus dem Blocksystem ein $\omega_0 \in \mathbb{F}_p[t]$ mit der Eigenschaft $\omega_0(\alpha_i) \equiv \beta_j \bmod p$ (vgl. 6.1).*

(4) *Bestimme ein $k \in \mathbb{N}$ derart, daß p^{2^k} „groß genug“ ist.*

(5) *Lifte ω_0 mittels des Newton-Liftings zu $\omega_k \in \mathbb{Z}/p^{2^k}\mathbb{Z}[t]$, so daß folgendes gilt:*

(a) $\omega_k \equiv \omega_o \bmod p$.

(b) $g(\omega_k) \equiv 0 \bmod (f, p^{2^k})$.

(6) *Berechne aus ω_k das Polynom $\omega \in \mathbb{Q}[t]$, welches $g(\omega) \equiv 0 \bmod f$ erfüllt. Falls dieser Schritt scheitert, wurde in (2) kein Blocksystem berechnet.*

Wir wollen nun die einzelnen Schritte dieses Algorithmus kurz erläutern. Im ersten Schritt muß eine Primzahl p fixiert werden, bezüglich derer die approximativen Berechnungen durchgeführt werden sollen. Diese Primzahl darf nicht 2 sein, da für $p = 2$ das Newton-Lifting nicht durchführbar ist. Im 2. Schritt soll das zugehörige Blocksystem bestimmt werden. Falls das Minimalpolynom g mit dem 2. Algorithmus berechnet wurde, liegt dieses bereits vor. Ansonsten wurde bisher nur ein Block bestimmt. Falls es nun noch mehrere Möglichkeiten für konjugierte Blöcke gibt, so müssen diese einzeln durchprobiert werden, bis man eine Lösung findet. Im 3. Schritt wird dann das Einbettungspolynom modulo p approximiert. Falls dieser Schritt nicht gelingt, so war in Schritt 2 kein Blocksystem gefunden worden. Im 4. Schritt muß eine Schranke bestimmt werden, bis zu der das Newton-Lifting durchzuführen ist. Auf die Berechnung dieser Schranke wird in den nächsten Abschnitten eingegangen werden. Im 5. Schritt wird das Newton-Lifting angewendet, um ein Polynom ω_k mit den geforderten Eigenschaften zu berechnen. Auf dieses Verfahren wird genauer in einem der nächsten Abschnitte eingegangen. Im letzten Schritt müssen wir probieren aus der modulo p^{2^k}-Approximation ein Polynom $\omega \in \mathbb{Q}[t]$ zu berechnen. Dabei wird in diesem Verfahren für jeden Koeffizienten einzeln das zugehörige Element aus $\mathbb{Q}$ bestimmt. Auch dieses Verfahren wird noch genauer erläutert werden.

2. Zur Abschätzung der Koeffizienten des Einbettungspolynoms

Wie wir in der Einleitung dieses Kapitels bereits erwähnt haben, benötigen wir Abschätzungen für die Koeffizienten des Einbettungspolynoms. Leider liegt das Einbettungspolynom ω i.allg. nicht in $\mathbb{Z}[t]$. Dies liegt daran, daß die Gleichungsordnung O, die von f erzeugt wird, nicht notwendigerweise Maximalordnung ist. So kann es passieren, daß die ganzalgebraische Zahl β, welche primitives Element von L ist, zwar in der Maximalordnung von K, aber nicht in der Gleichungsordnung O liegt. Man könnte zwar probieren, das Problem dadurch zu lösen, daß man die Maximalordnung von K ausrechnet, um dadurch nur ganze Koeffizienten für ω zu erhalten. Diese Möglichkeit ist jedoch nicht praktikabel, da einerseits die Berechnung der Maximalordnung sehr aufwendig ist und andererseits unser Einbettungsverfahren auf einer Potenzbasis von K beruht. So gibt es Körper, für die kein Element existiert, dessen Potenzbasis die Maximalordnung des Körpers erzeugt. Deshalb werden wir uns in diesem Abschnitt mit den Abschätzungen für den Zähler und Nenner der Koeffizienten des zu berechnenden Einbettungspolynoms ω beschäftigen.

Wie in den vorangegangenen Abschnitten seien $f, g \in \mathbb{Z}[t]$ normierte und irreduzible Polynome. Ferner seien $\{\alpha_1, \dots, \alpha_n\}$ die Nullstellen von f und $\{\beta_1, \dots, \beta_m\}$ seien die Nullstellen von g. Weiterhin sei $K = \mathbb{Q}(\alpha_1)$ und $L = \mathbb{Q}(\beta_1)$, wobei gilt, daß L ein Teilkörper von K ist. Zusätzlich bezeichnen wir mit $\Delta_1, \dots, \Delta_m$ das zugehörige Blocksystem.

Zur Lösung unseres Problems betrachten wir zuerst die Diskriminante von f. Es gelte $\mathrm{disc}(f) = D_1^2 D_2$, wobei $D_1, D_2 \in \mathbb{Z}$ und D_2 quadratfrei ist. Dann ist es eine bekannte Tatsache, daß alle ganzalgebraischen Zahlen von K in $D_1^{-1}\mathbb{Z}[\alpha_1]$ liegen. Nehmen wir also an, daß ω das gesuchte Einbettungspolynom mit der Eigenschaft $g(\omega(\alpha_1)) = 0$ ist. Dann ist $D_1\omega \in \mathbb{Z}[t]$ und hat die Form $D_1\omega(t) = u_0 + u_1 t + \dots + u_{n-1}t^{n-1}$. Gemäß Satz 6.1 gilt dann die folgende Gleichung:

$$u_0 + u_1\alpha_i + \dots + u_{n-1}\alpha_i^{n-1} = D_1\beta_{v(i)}\, (i = 1, \dots, n),$$

wobei $\alpha_i \in \Delta_{v(i)}$ ist. Wir definieren nun A durch die folgende $n \times n$ Matrix:

$$\begin{pmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1^1 & \alpha_2^1 & \cdots & \alpha_n^1 \\ \alpha_1^2 & \alpha_2^2 & \cdots & \alpha_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{n-1} & \alpha_1^{n-1} & \cdots & \alpha_n^{n-1} \end{pmatrix}$$

Nach bekannten Formeln gilt dann $\mathrm{disc}(f) = (\det(A))^2 = D_1^2 D_2$. Wir können also die $u_i\, (i = 0, 1, \dots, n-1)$ bestimmen, indem wir das folgende Gleichungssystem lösen:

$$(u_0, u_1, \dots, u_{n-1}) = D_1(\beta_{v(1)}, \beta_{v(2)}, \dots, \beta_{v(n)}A^{-1}).$$

Wir erhalten: $D_1 A^{-1} = \epsilon |D_2|^{-\frac{1}{2}} \mathrm{Adj}(A)$, wobei $|\epsilon| = 1$ gilt. Falls für alle $1 \le i \le n$ eine Schranke c_0 existiert mit $|\alpha_i| \le c_0$, so gibt Hadamards Determinantenungleichung die folgende Abschätzung für die $u_i\, (0 \le i < n)$:

$$|u_i| \le |D_2|^{-\frac{1}{2}} n^{\frac{n-1}{2}} c_0^{\frac{n(n-1)}{2}+d}.$$

Um diese Abschätzung zu beweisen, müssen wir uns zuerst überlegen, wie die Matrix $\mathrm{Adj}(A)$ aussieht. Jedes Element dieser Matrix entspricht bis auf das Vorzeichen dem Wert einer $(n-1) \times (n-1)$ Determinante, die dadurch entsteht, daß wir eine Zeile und eine Spalte von A streichen. Für die Berechnung dieser werden wir die Hadamard'sche Determinantenungleichung benutzen. Allerdings werden wir nicht das Produkt der Spalten, sondern daß Produkt der Zeilen bilden. Zuerst werden wir nun die euklidische Norm einer Zeile berechnen. Dabei ist es unwichtig, welche Spalte gestrichen wird, da wir alle α_i durch c_0 abschätzen. Die Zeilennorm der j-Zeile können wir dann durch $\sqrt{nc_0^{2(j-1)}} = \sqrt{n}c_0^{j-1}$ abschätzen. Den kleinsten Wert erhalten wir hier für $j = 1$, da stets $c_0 \geq 1$ gilt. Wenn wir also jedes Element von $\mathrm{Adj}(A)$ nach oben abschätzen wollen, so können wir stets die 1. Zeile streichen. Wir erhalten also für ein Element b von $\mathrm{Adj}(A)$ die folgende Abschätzung:

$$|b| \leq \prod_{j=1}^{n-1} \sqrt{n}c_0^j = n^{\frac{n-1}{2}} c_0^{\frac{n(n-1)}{2}}.$$

Da wir jedes Element b von $\mathrm{Adj}(A)$ so abschätzen können, erhalten wir so durch einfaches Ausrechnen die gewünschte Formel.

Zum Abschluß wollen wir bemerken, daß diese Schranken den Zähler und Nenner nur ziemlich grob abschätzen. Wir benötigen an dieser Stelle nur die Existenz von solchen Schranken. In der Praxis ist es erheblich schneller, wenn man mehrere Schranken „durchprobiert“, bis man eine Lösung findet.

3. Das verallgemeinerte Newton-Lifting

In diesem Abschnitt werden wir das verallgemeinerte Newton-Lifting untersuchen. Die Verallgemeinerung besteht darin, daß das Newton-Lifting normalerweise über einem Körper durchgeführt wird, wie es zum Beispiel in [Lan] (Seite 308-311) beschrieben wird. John Dixon beschreibt in [Dix1], wie man diese Methode über dem Ring $\mathbb{Z}_p[t]$ durchführen kann. Der entscheidene Unterschied in der Voraussetzung liegt darin, daß wir im Ring keine Division durchführen können. Betrachten wir nun die Iteration, die beim „normalen“ Newton-Lifting durchgeführt wird. Diese wird in [Lan] auf Seite 311 in Proposition 21 beschrieben. Dort wird

$$\alpha_{i+1} = \alpha_i - \frac{f(\alpha_i)}{f'(\alpha_i)}$$

gesetzt. Hierbei sind die α_i Elemente des Körpers. Bei uns entsprechen die α_i dann den Polynomen ω_k aus dem Ring. Wie bereits gesagt können wir die Division, die in diesem Iterationsschritt durchgeführt wird, nicht berechnen. Deswegen müssen wir uns für diesen Teil einen Ersatz ausdenken. Dies wird in dem folgenden Satz deutlich werden. Der Beweis zu diesem Satz ist konstruktiv, so daß wir einen Algorithmus sofort aus diesem herleiten können. Vorher werden wir aus beweistechnischen Gründen noch zwei Lemmata zeigen.

LEMMA 6.3. *Sei $a \in \mathbb{Z}$ und gelte $a \equiv 1 \bmod p^{2^k}$ mit $p \in \mathbb{P}$ und $k \in \mathbb{N}$. Dann gilt:* $2a - a^2 \equiv 1 \bmod p^{2^{k+1}}$.

Beweis: Wegen $a \equiv 1 \bmod p^{2^k}$ gilt $a \equiv 1 + bp^{2^k} \bmod p^{2^{k+1}}$. Damit gilt:

$$\begin{aligned} 2a - a^2 &\equiv 2(1 + bp^{2^k}) - (1 + bp^{2^k})^2 \bmod p^{2^{k+1}} \\ &\equiv 2 + 2bp^{2^k} - 1 - 2bp^{2^k} - (b^2 p^{2^k})^2 \bmod p^{2^{k+1}} \\ &\equiv 1 \bmod p^{2^{k+1}} \end{aligned}$$

□

BEZEICHNUNG 6.4. *Seien $f, g, h \in \mathbb{Z}_p[t], p \in \mathbb{P}$ und $k \in \mathbb{N}$. Dann ist*

$$g \equiv h \bmod (f, p^k) \textit{ eine Schreibweise für } f \mid (g - h) \bmod p^k.$$

LEMMA 6.5. *Seien f, g und $h \in \mathbb{Z}_p[t]$ normiert und es gelte für dieses $p \in \mathbb{P} : p \nmid \operatorname{disc}(f) \operatorname{disc}(g)$. Zusätzlich soll die Bedingung $g(h) \equiv 0 \bmod (f, p)$ erfüllt sein. Dann gilt die folgende Beziehung:* $\operatorname{ggT}(g'(h), f) \equiv 1 \bmod p$.

Beweis: Die Polynome f, g und h seien auf kanonische Weise in $\mathbb{F}_p[t]$ eingebettet. Sei nun $\omega = \operatorname{ggT}(g'(h), f)$ in $\mathbb{F}_p[t]$. Hieraus folgt wegen $f \mid g(h)$, daß $\omega \mid g(h)$ und $\omega \mid g'(h)$ gilt. Nehmen wir nun an, daß $\omega \not\equiv 1$ ist. Dann existiert in einem passenden Erweiterungskörper von $\mathbb{F}_p$ eine Nullstelle γ von ω (ω ist normiert!). Diese ist dann gleichzeitig auch Nullstelle von $g(h)$ und von $g'(h)$. Hiermit ist dann $h(\gamma)$ Nullstelle von g und g' und damit wäre $\operatorname{disc}(g) = 0$ (in $\mathbb{F}_p[t]$). Dies ist aber ein Widerspruch! □

SATZ 6.6. *Sei $p \in \mathbb{P}$ und $f \in \mathbb{Z}_p[t]$. Existiere weiterhin ein $g \in \mathbb{Z}_p[t]$ und ein $\omega_0 \in \mathbb{Z}_p[t]$, so daß folgendes gilt:*

$$\begin{aligned} p &\nmid \operatorname{disc}(f) \operatorname{disc}(g) \\ g(\omega_0) &\equiv 0 \bmod (f, p) \end{aligned}$$

Dann existiert ein $\omega \in \mathbb{Z}_p[t]$, so daß folgendes gilt:

$$\begin{aligned} \omega &\equiv \omega_0 \bmod p \\ g(\omega) &\equiv 0 \bmod f \end{aligned}$$

Weiterhin kann für alle $k \in \mathbb{N}$ ein ω_k bestimmt werden, für welches $\omega_k \equiv \omega \bmod p^{2^k}$ gilt.

Beweis: Nach Lemma 6.5 folgt $\mathrm{ggT}(g'(\omega_0), f) \equiv 1 \bmod p$. Also existiert ein h_0 mit $h_0 g'(\omega_0) \equiv 1 \bmod (f, p)$. Wir konstruieren nun Folgen (ω_k) und (h_k) mit folgenden Eigenschaften ($k \in \mathbb{N}$):

$$\omega_{k+1} \equiv \omega_k \bmod (f, p^{2^k}) \tag{6-1}$$

$$h_{k+1} \equiv h_k \bmod (f, p^{2^k}) \tag{6-2}$$

$$g(\omega_k) \equiv 0 \bmod (f, p^{2^k}) \tag{6-3}$$

$$h_k g'(\omega_k) \equiv 1 \bmod (f, p^{2^k}) \tag{6-4}$$

Dazu führen wir folgende doppelte Iteration durch:

$$\omega_{k+1} \equiv \omega_k - h_k g(\omega_k) \bmod (f, p^{2^{k+1}}) \tag{6-5}$$

$$h_{k+1} \equiv h_k \left[2 - h_k g'(\omega_{k+1})\right] \bmod (f, p^{2^{k+1}}) \tag{6-6}$$

Wir zeigen nun, daß die Eigenschaften durch die Iteration gewahrt bleiben:

zu (6-1):

$$\begin{aligned}
\omega_{k+1} &\overset{(6\text{-}5)}{\equiv} \omega_k - h_k g(\omega_k) \bmod (f, p^{2^{k+1}}) \\
&\equiv \omega_k - h_k \underbrace{g(\omega_k)}_{\equiv 0 \bmod (f, p^{2^k})} \bmod (f, p^{2^k}) \\
&\equiv \omega_k \bmod (f, p^{2^k})
\end{aligned}$$

zu (6-2):

$$\begin{aligned}
h_{k+1} &\overset{(6\text{-}6)}{\equiv} h_k \left[2 - h_k g'(\omega_{k+1})\right] \bmod (f, p^{2^{k+1}}) \\
&\equiv h_k \left[2 - \underbrace{h_k g'(\omega_{k+1})}_{\equiv 1 \bmod (f, p^{2^k})}\right] \bmod (f, p^{2^k}) \\
&\equiv h_k \bmod (f, p^{2^k})
\end{aligned}$$

zu (6-3): Für $k = 0$ gilt die Behauptung nach Voraussetzung.

$$\begin{aligned}
g(\omega_{k+1}) &\overset{(6\text{-}5)}{\equiv} g(\omega_k - h_k g(\omega_k)) \bmod (f, p^{2^{k+1}}) \\
&\overset{\text{Taylor}}{\equiv} g(\omega_k) - h_k g(\omega_k) g'(\omega_k) \bmod (f, p^{2^{k+1}}) \\
&\equiv \underbrace{g(\omega_k)}_{\equiv 0 \bmod (f, p^{2^k})} \left[1 - \underbrace{h_k g'(\omega_k)}_{\equiv 1 \bmod (f, p^{2^k})}\right] \bmod (f, p^{2^{k+1}}) \\
&\equiv 0 \bmod (f, p^{2^{k+1}})
\end{aligned}$$

zu (6-4): Für $k = 0$ gilt die Behauptung nach Konstruktion von h_0.

$$\begin{aligned} h_{k+1}g'(\omega_{k+1}) &\overset{(6\text{-}6)}{\equiv} h_k\,[2 - h_k g'(\omega_{k+1})]g'(\omega_{k+1}) \bmod (f, p^{2^{k+1}}) \\ &\equiv 2(\underbrace{h_k g'(\omega_{k+1})}_{\equiv 1 \bmod (f,p^{2^k})} - (\underbrace{h_k g'(\omega_{k+1}}_{\equiv 1 \bmod (f,p^{2^k})})^2 \bmod (f, p^{2^{k+1}}) \\ &\overset{6.3}{\equiv} 1 \bmod (f, p^{2^{k+1}}) \end{aligned}$$

Damit ist gezeigt, daß (ω_k) eine Cauchyfolge in $\mathbb{Z}_p[t]$ ist. Da $\mathbb{Z}_p$ vollständig ist, konvergiert ω_k gegen ein $\omega \in \mathbb{Z}_p[t]$. Die Eindeutigkeit von ω folgt aus der Tatsache, daß $f \bmod p$ und $g \bmod p$ keine doppelten Nullstellen haben. Nehmen wir an, es existiert ein $\nu \in \mathbb{Z}_p[t]$ höchstens vom Grad $n-1$ mit den geforderten Eigenschaften. Dann gelten für alle α_i $(i = 1, \dots, n)$, die Nullstelle von f sind, daß sowohl $\nu(\alpha_i)$ als auch $\omega(\alpha_i)$ Nullstelle von g ist. Zusätzlich gilt wegen $\nu \equiv \omega_0 \bmod p$ für $1 \le i \le n$: $\nu(\alpha_i) \equiv \omega(\alpha_i) \bmod p$. Da $g \bmod p$ separabel ist, folgt hieraus $\nu(\alpha_i) = \omega(\alpha_i)$ und hiermit $\nu = \omega$. □

Aus dem Beweis dieses Satzes können wir den folgenden Algorithmus zusammenfassen.

Algorithmus 6.7. *Verallgemeinertes Newton-Lifting*

Input: *Polynome* f, g *und* $\omega_0 \in \mathbb{Z}_p[t]$,
$p \in \mathbb{P}$ *mit* $p \nmid \mathrm{disc}(f)\,\mathrm{disc}(g)$,
so daß gilt: $g(\omega_0) \equiv 0 \bmod (f, p)$.
$k \in \mathbb{N}$.

Output: *Ein Polynom* $\omega_k \in \mathbb{Z}_p[t]$,
so daß $g(\omega_k) \equiv 0 \bmod (f, p^{2^k})$ *und*
$\omega_k \equiv \omega_0 \bmod p$ *gilt.*

(1) *Berechne mit dem Euklidischen Algorithmus ein Polynom* $h_0 \in \mathbb{Z}_p[t]$, *für das* $h_0 g'(\omega_0) \equiv 1 \bmod (f, p)$ *gilt.*

(2) *Für* $i = 0, \dots, k-1$ *tue folgendes:*

$$\begin{aligned} \omega_{i+1} &\equiv \omega_i - h_i g(\omega_i) \bmod (f, p^{2^{i+1}}) \\ h_{i+1} &\equiv h_i(2 - h_i g(\omega_{i+1})) \bmod (f, p^{2^{i+1}}) \end{aligned}$$

Die Korrektheit des obigen Algorithmus wird vollständig in 6.6 gezeigt. Zur Implementierung von Schritt (1) wollen wir noch erwähnen, daß der Euklidische Algorithmus in $\mathbb{F}_p[t]$ durchgeführt wird.

4. Bestimmung des Einbettungspolynoms aus der Approximation

Im vorigen Abschnitt haben wir beschrieben, wie wir unser gesuchtes Polynom ω modulo p^{2^k} bestimmen können. Dabei konnten wir das k beliebig groß wählen. Jetzt müssen wir untersuchen, wie wir auf die rationalen Koeffizienten von ω zurückschließen können. Dies werden wir für jeden Koeffizienten einzeln tun. Voraussetzung für dieses Verfahren ist, daß wir Abschätzungen für den Zähler und Nenner jedes einzelnen Koeffizienten besitzen. Wie wir diese erhalten, wurde bereits in einem früheren Abschnitt beschrieben. Der folgende Satz, der in [Dix2] beschrieben ist, ist Grundlage des nachfolgenden Algorithmus.

Satz 6.8. *Seien $s, h \in \mathbb{N}^{>1}$. Weiterhin nehmen wir an, daß $a, b \in \mathbb{Z}$ existieren mit*

$$bs \equiv a \bmod h \text{ und } |a|, |b| \leq \lambda\sqrt{h},$$

wobei $\lambda = 0,618...$ eine Nullstelle von $\lambda^2 + \lambda - 1$ ist. Seien $\frac{w_i}{v_i}$ $(i = 1, 2, \ldots)$ die Näherungsbrüche (convergents) der Kettenbruchentwicklung für $\frac{s}{h}$ und setze $u_i = v_i s - w_i h$. Sei k die kleinste ganze Zahl mit $|u_k| < \sqrt{h}$. Dann gilt: $\frac{a}{b} = \frac{u_k}{v_k}$.

Beweis: Der Beweis dieses Satzes setzt Kenntnisse über die Kettenbruchentwicklung voraus. Diese können [Khi] entnommen werden. So ist bekannt, daß die Folgen (w_i) und (v_j) monoton steigend, während die Folge der (u_i) alternierend und betraglich monoton fallend ist. Setze $a = bs - th$. Dann gilt

$$|\frac{s}{h} - \frac{t}{b}| = |\frac{ab}{hb^2}| \leq \frac{\lambda^2 h}{hb^2} < \frac{1}{2b^2}$$

und so gilt nach 2.39, daß $\frac{t}{b}$ einem Näherungsbruch von $\frac{s}{h}$ entspricht. Dieser sei mit $\frac{w_j}{v_j}$ bezeichnet. Wegen $a = bs - th = v_j s - w_j h = u_j$ gilt $|u_j| = |a| \leq \lambda\sqrt{h} < \sqrt{h}$. Damit gilt nach der Definition von k, daß $j \geq k$ gilt. Andererseits gilt $u_j v_k - u_k v_j \equiv 0 \bmod h$ wegen $u_j = v_j s - w_j h$ und $u_k = v_k s - w_k h$. Da zusätzlich $j \geq k$ gilt, folgt

$$|u_j v_k - u_k v_j| \overset{|v_j|>|v_k|}{\leq} (|u_j| + |u_k|)|v_j| \leq \lambda\sqrt{h}\,\lambda\sqrt{h} < (\lambda+1)\lambda h = h.$$

Diese Ungleichung gilt, da $\frac{t}{b} = \frac{w_j}{v_j}$ gilt. Da beide Brüche zusätzlich gekürzt sind, gilt $|v_j| = |b| \leq \lambda\sqrt{h}$. Wegen $|u_j v_k - u_k v_j| < h$ gilt sogar $u_j v_k = u_k v_j$ und somit $j = k$. Damit ist gezeigt, daß $\frac{a}{b} = \frac{u_k}{v_k}$ gilt. □

Wie wir dem Beweis dieses Satzes entnehmen können, liegt seine Schwierigkeit in der Theorie der Kettenbruchentwicklung. Im folgenden werden wir die Frage beantworten, wie wir die Näherungsbrüche berechnen können. Dies braucht man nicht mit der Definition zu tun, sondern man kann eine Modifikation des Euklidischen Algorithmus anwenden.

ALGORITHMUS 6.9. *Berechnung einer rationalen Zahl aus einer Approximation*

Input: *Ganze Zahlen s und h mit $s, h > 1$.*
Output: *Ganze Zahlen a und b (falls existent) für die $bs \equiv a \bmod h$ und $|a|, |b| < \lambda\sqrt{h}$ gilt.*

(1) *Setze $u_{-1} = h$ und $u_0 = s$.*
(2) *Setze $v_{-1} = 0$ und $v_0 = 1$.*
(3) *Setze $i = 0$.*
(4) *Falls $u_i < \sqrt{h}$ gib $(-1)^i \frac{u_i}{v_i}$ aus und terminiere.*
(5) *Setze $q_i = \frac{u_{i-1}}{u_i}$.*
(6) *Setze $u_{i+1} = u_{i-1} - q_i u_i$.*
(7) *Setze $v_{i+1} = v_{i-1} + q_i v_i$.*
(8) *Setze $i = i + 1$ und gehe nach (4).*

Falls die Zahlen a und b mit den geforderten Bedingungen nicht existieren, so gibt der Algorithmus 0 aus. Falls 0 tatsächlich die gesuchte Lösung war, so erkennt man das daran, daß bereits $s \equiv 0 \bmod h$ war. In dem Algorithmus wird ein Verfahren benutzt, welches auf den ersten Blick nicht viel mit der Berechnung von Näherungsbrüchen zu tun hat. Deswegen werden wir die Korrektheit des Algorithmus beweisen.

Beweis: In 6.8 haben wir die Abhängigkeit der gesuchten Lösung mit dem k-ten Näherungsbruch der Kettenbruchentwicklung von $\frac{s}{h}$ bewiesen. Wenn nun $\frac{w_k}{v_k}$ der k-te Näherungsbruch ist und $u_k = v_k s - w_k$ ist, so ist $\frac{u_k}{v_k} = \frac{a}{b}$. Wir müssen nun zeigen, daß die u_i und v_i, die im Algorithmus berechnet werden, den u_i und v_i aus dem Satz entsprechen. Dabei müssen wir zusätzlich beachten, daß im Algorithmus die u_i nur dem Betrage nach bestimmt werden, d.h. wir müssen die erhaltenen u_i noch mit $(-1)^i$ multiplizieren.

Als ersten Schritt wollen wir zeigen, daß die q_i aus dem Algorithmus gerade den a_{i+1} entsprechen, wenn wir mit $[a_0; a_1, a_2, \ldots, a_n]$ die Kettenbruchentwicklung von $\frac{s}{h}$ bezeichnen. Wir setzen $r_i = [a_i; a_i{+}1, \ldots, a_n]$. Nach 2.38 gilt für alle $0 \leq i < n$:

$$\frac{s}{h} = \frac{w_i r_{i+1} + w_{i-1}}{v_i r_{i+1} + v_{i-1}}.$$

Durch einfache Äquivalenzumformungen erhalten wir:

$$r_{i+1}(v_i s - w_i h) \quad = \quad -(v_{i-1} s - w_{i-1} h)$$

Wegen $u_i = v_i s - w_i h$ gilt:

$$r_{i+1} u_i \quad = \quad -u_{i-1}.$$

Hieraus folgt: (Die u_i sind aus Satz 6.8!)

$$r_{i+1} \quad = \quad -\frac{u_{i-1}}{u_i}.$$

Da die u_i alternierend sind, ist der Bruch stets positiv. Damit folgt:

$$a_{i+1} \quad = \quad q_i.$$

Die letzte Gleichheit gilt, da a_{i+1} stets der größten ganzen Zahl entspricht, die kleiner als r_{i+1} ist. Damit haben wir die Behauptung gezeigt, daß die q_i aus dem Algorithmus den a_{i+1} der Kettenbruchentwicklung entsprechen.

Wenn wir

$$w_i = \frac{v_i s - (-1)^i u_i}{h}$$

setzen, wobei die u_i aus dem Algorithmus kommen, so müssen wir zeigen, daß die so berechneten v_i und w_i denen aus dem Satz entsprechen. Falls uns dieses gelingt, so ist die Korrektheit des Algorithmus bewiesen. Diesen Beweis wollen wir mit vollständiger Induktion führen. Aus $v_0 = 1$ und $u_0 = s$ folgt direkt $w_0 = 0$, womit $\frac{w_0}{v_0} = 0 = a_0$ ist. Aus $v_{-1} = 0$ und $u_{-1} = h$ folgt dann $w_{-1} = 1$. Hiermit ist die Induktionsvoraussetzung für $i = -1$ und $i = 0$ erfüllt, wenn man den -1-ten Näherungsbruch formal mit „$\frac{1}{0}$“ bezeichnet.

Nach Satz 1 von [Khi] gilt für Zähler und Nenner der Näherungsbrüche folgender Zusammenhang: $(1 \leq i \leq n)$

$$w_i = a_i w_{i-1} + w_{i-2} \text{ und } v_i = a_i v_{i-1} + v_{i-2}$$

Der Induktionsschritt für die v_i ist nach dieser Formel trivialerweise erfüllt. Sei also nun $i \geq 1$ und sei der Beweis für alle w_j mit $j < i$ geführt. Dann gilt:

$$\begin{aligned} w_i &= \frac{v_i s - (-1)^i u_i}{h} \\ &= \frac{(v_{i-2} + q_{i-1} v_{i-1}) s - (-1)^i (u_{i-2} - q_{i-1} u_{i-1})}{h} \\ &= \frac{q_{i-1}(v_{i-1} s - (-1)^{i-1} u_{i-1}) + (v_{i-2} s - (-1)^{i-2} u_{i-2})}{h} \\ &= q_{i-1} w_{i-1} + w_{i-2} \\ &= a_i w_{i-1} + w_{i-2} \end{aligned}$$

Damit ist die Behauptung gezeigt. □

5. Beispiele

In diesem Abschnitt wollen wir unser Beispiel aus den vergangenen Kapiteln zu Ende rechnen. Wir hatten einen Körper K durch $f(t) = t^6 + 108$ gegeben. Wir haben bereits drei Teilkörper vom Grad 3 bestimmt, die alle durch $g(t) = t^3 - 108$ erzeugt werden. Zum Abschluß des Algorithmus müssen wir die Einbettung dieser Teilkörper in K bestimmen.

Als erstes bestimmen wir das Einbettungspolynom h modulo p, d.h. es gilt $f \mid g(h) \bmod p$. Hierzu gruppieren wir die Nullstellen von f in das zugehörige und bereits berechnete Blocksystem. In jedem Block Δ_i berechnen wir das Produkt β_i der Nullstellen. Diese Berechnungen werden alle über dem endlichen Körper $\mathbb{F}_7$ durchgeführt. Wir müssen nun ein Polynom h bestimmen, für welches $h(\alpha_i) = \beta_j$ für $\alpha_i \in \Delta_j$ und $1 \leq i \leq n$ gilt. Da h maximal Grad $n - 1 = 5$ hat, wird h durch diese Gleichungen eindeutig bestimmt. Wir erhalten auf diese Weise $h(t) = 4t^5 + 4t^2 \bmod 7$. Aufgrund unserer Abschätzung können wir den Zähler der Koeffizienten des Einbettungspolynoms mit 64134065 und den Nenner mit 15116544 abschätzen. Damit wir auf die Koeffizienten in $\mathbb{Q}$ zurückschließen können, müssen wir unsere Einbettung bis mindestens $7 * 10^{15}$ liften. Wir liften dann unser Einbettungspolynom bis $7^{32} \approx 10^{27}$ und erhalten:

$$\begin{aligned} h(t) \equiv\ & 1012392034723593925779857601 \cdot t^5 \\ &+ 552213837121960323152649601 \cdot t^2 \bmod 7^{32}. \end{aligned}$$

Mit Hilfe von Algorithmus 6.9 können wir dann für jeden Koeffizienten einzeln auf die Koeffizienten aus $\mathbb{Q}$ zurückschließen. Wir erhalten: $h(t) = -\frac{1}{12}t^5 + \frac{1}{2}t^2$.

Zum Abschluß müssen wir testen, ob $f \mid g(h)$ gilt. Wir stellen fest, daß diese Bedingung erfüllt ist und können uns nun sicher sein, daß wir einen Teilkörper samt Einbettung berechnet haben.

Für die beiden anderen Teilkörper erhalten wir auf diese Weise:

$$\begin{aligned} h(t) &\equiv 1012392034723593925779857601 \cdot t^5 \\ &\quad + 552213837121960323152649601 \cdot t^2 \bmod 7^{32}. \end{aligned}$$

Hieraus folgt: $h(t) = \frac{1}{12} \cdot t^5 + \frac{1}{2} \cdot t^2$.

Für den letzten Teilkörper gilt:

$$h(t) \equiv 1104427674243920646305299200 \cdot t^2 \bmod 7^{32}.$$

Hieraus folgt: $h(t) = -t^2$.

Beide erfüllen die Bedingung $f \mid g(h)$, so daß wir insgesamt 3 Teilkörper vom Grad 3 berechnet haben.

KAPITEL 7

Beispiele

Die in dieser Arbeit vorgestellten Algorithmen wurden in dem Computeralgebrasystem KANT (vgl. [Poh]) implementiert. Wir werden nun im folgenden einige der berechneten Beispiele tabellarisch auflisten. Die angegebenen Rechenzeiten wurden auf einer HP 9000/735 ermittelt.

Olivier hat für die Galoisgruppenberechnung Körpertabellen von imprimitiven Körpern 9. Grades aufgestellt. Von diesen Körpern haben wir sämtliche Teilkörper berechnet. Da es sich um insgesamt 1112 Körper handelt, werden wir sie an dieser Stelle nicht alle angeben. Im folgenden sei r_1 die Anzahl der reellen Nullstellen.

r_1	Anzahl Körper	Anzahl Teilkörper	Gesamtlaufzeit	Durchschnittslaufzeit pro Körper
1	485	486	36:43 min	4,5 sek
3	423	446	31:25 min	4,5 sek
5	154	154	9:38 min	3,8 sek
7	23	23	1:30 min	3,9 sek
9	27	31	1:39 min	3,7 sek

Wir geben nun die Ergebnisse der Körper mit $r_1 = 9$ an. In der folgenden Tabelle gibt jeweils die erste Zeile ein erzeugendes Polynom des gegebenen Körpers an. In der zweiten Zeile steht an der ersten Stelle die evtll. durchgeführte Substitution und an der zweiten Stelle das berechnete erzeugende Polynom des Teilkörpers. In der dritten Zeile schließlich steht die ermittelte Einbettung des Teilkörpers bezogen auf das substituierte Polynom. Falls ein Körper mehrere Teilkörper besitzt, so wird das erzeugende Minimalpolynom nicht wiederholt, sondern es werden nur die zweite und dritte Zeile angegeben.

<table>
<tr><td colspan="2">Erzeugendes Polynom des gegebenen Körpers</td></tr>
<tr><td>Durchgeführte Substitution</td><td>Erzeugendes Polynom des Teilkörpers</td></tr>
<tr><td colspan="2">Einbettung des Teilkörpers</td></tr>
<tr><td colspan="2">$x^9 + 2x^8 - 14x^7 - 32x^6 + 16x^5 + 61x^4 + 15x^3 - 18x^2 - 5x + 1$</td></tr>
<tr><td>$x = x$</td><td>$x^3 + 5x^2 - 8x + 1$</td></tr>
<tr><td colspan="2">$-\frac{415}{669}x^8 - \frac{827}{669}x^7 + \frac{1898}{223}x^6 + \frac{4325}{223}x^5 - \frac{5111}{669}x^4 - \frac{7047}{223}x^3 - \frac{7271}{669}x^2 + \frac{695}{669}x + \frac{200}{669}$</td></tr>
<tr><td colspan="2">$x^9 + x^8 - 12x^7 - 10x^6 + 38x^5 + 34x^4 - 23x^3 - 27x^2 - 4x + 1$</td></tr>
<tr><td>$x = x$</td><td>$x^3 + 8x^2 + 6x + 1$</td></tr>
<tr><td colspan="2">$-\frac{2}{101}x^8 - \frac{25}{101}x^7 - \frac{11}{101}x^6 + \frac{247}{101}x^5 + \frac{189}{101}x^4 - \frac{571}{101}x^3 - \frac{511}{101}x^2 - \frac{15}{101}x - \frac{13}{101}$</td></tr>
<tr><td colspan="2">$x^9 + x^8 - 8x^7 - 7x^6 + 21x^5 + 15x^4 - 20x^3 - 10x^2 + 5x + 1$</td></tr>
<tr><td>$x = x$</td><td>$x^3 - 5x^2 + 2x + 1$</td></tr>
<tr><td colspan="2">$x^5 - 4x^3 + x^2 + 2x$</td></tr>
<tr><td colspan="2">$x^9 + 4x^8 - 6x^7 - 36x^6 - 16x^5 + 70x^4 + 99x^3 + 52x^2 + 12x + 1$</td></tr>
<tr><td>$x = x$</td><td>$x^3 - 4x^2 + 3x + 1$</td></tr>
<tr><td colspan="2">$-5x^8 - 20x^7 + 31x^6 + 183x^5 + 71x^4 - 377x^3 - 483x^2 - 199x - 24$</td></tr>
<tr><td>$x = x + 1$</td><td>$x^3 + 22x^2 + 138x + 181$</td></tr>
<tr><td colspan="2">$8x^8 + 95x^7 + 389x^6 + 505x^5 - 637x^4 - 2119x^3 - 827x^2 + 1681x + 1267$</td></tr>
<tr><td colspan="2">$x^9 + x^8 - 13x^7 - 18x^6 + 28x^5 + 48x^4 + 6x^3 - 17x^2 - 8x - 1$</td></tr>
<tr><td>$x = x$</td><td>$x^3 - 5x^2 + 6x - 1$</td></tr>
<tr><td colspan="2">$-\frac{98}{9}x^8 - \frac{37}{9}x^7 + \frac{1294}{9}x^6 + \frac{958}{9}x^5 - \frac{3301}{9}x^4 - \frac{2629}{9}x^3 + \frac{953}{9}x^2 + \frac{343}{3}x + \frac{184}{9}$</td></tr>
<tr><td colspan="2">$x^9 + 3x^8 - 12x^7 - 32x^6 + 51x^5 + 105x^4 - 100x^3 - 114x^2 + 78x + 19$</td></tr>
<tr><td>$x = x$</td><td>$x^3 - 21x^2 + 54x + 19$</td></tr>
<tr><td colspan="2">$\frac{447}{31051}x^8 + \frac{17882}{31051}x^7 + \frac{32343}{31051}x^6 - \frac{188297}{31051}x^5 - \frac{260039}{31051}x^4 + \frac{577033}{31051}x^3 + \frac{507545}{31051}x^2 - \frac{540384}{31051}x - \frac{131841}{31051}$</td></tr>
<tr><td colspan="2">$x^9 - 3x^8 - 11x^7 + 39x^6 + 11x^5 - 86x^4 - 15x^3 + 64x^2 + 28x + 1$</td></tr>
<tr><td>$x = x$</td><td>$x^3 + 12x^2 - 15x + 1$</td></tr>
<tr><td colspan="2">$\frac{42}{83}x^8 - \frac{129}{83}x^7 - \frac{435}{83}x^6 + \frac{1509}{83}x^5 + \frac{123}{83}x^4 - \frac{1860}{83}x^3 - \frac{426}{83}x^2 + \frac{15}{83}x + \frac{7}{83}$</td></tr>
</table>

Erzeugendes Polynom des gegebenen Körpers	
Durchgeführte Substitution	Erzeugendes Polynom des Teilkörpers
Einbettung des Teilkörpers	
$x^9+2x^8-12x^7-22x^6+34x^5+70x^4+x^3-30x^2-4x+1$	
$x=x$	x^3-11x^2-4x+1
$\frac{318}{307}x^8+\frac{269}{307}x^7-\frac{3832}{307}x^6-\frac{1807}{307}x^5+\frac{10956}{307}x^4+\frac{5173}{307}x^3-\frac{4678}{307}x^2-\frac{1411}{307}x+\frac{89}{307}$	
$x^9-9x^7+27x^5-30x^3+9x+1$	
$x=x$	x^3-3x+1
x^3-3x	
$x^9-15x^7-7x^6+66x^5+48x^4-70x^3-30x^2+27x-1$	
$x=x$	$x^3-6x^2-45x-1$
$\frac{640}{647}x^8-\frac{1777}{647}x^7-\frac{6695}{647}x^6+\frac{16227}{647}x^5+\frac{21889}{647}x^4-\frac{39560}{647}x^3-\frac{18867}{647}x^2+\frac{20208}{647}x-\frac{769}{647}$	
$x^9-17x^7-6x^6+87x^5+47x^4-143x^3-69x^2+72x+27$	
$x=x$	$x^3+15x^2+54x+27$
$-\frac{212}{3191}x^8-\frac{683}{3191}x^7+\frac{3556}{3191}x^6+\frac{11464}{3191}x^5-\frac{12999}{3191}x^4-\frac{47824}{3191}x^3-\frac{8160}{3191}x^2+\frac{28678}{3191}x+\frac{7257}{3191}$	
$x^9-15x^7+4x^6+61x^5-19x^4-80x^3+16x^2+34x-1$	
$x=x$	$x^3-10x^2+17x-1$
$-\frac{1383}{2087}x^8+\frac{2476}{2087}x^7+\frac{20204}{2087}x^6-\frac{40294}{2087}x^5-\frac{65783}{2087}x^4+\frac{142626}{2087}x^3+\frac{36511}{2087}x^2-x+\frac{3066}{2087}$	
$x^9-15x^7+2x^6+60x^5-15x^4-83x^3+30x^2+36x-17$	
$x=x$	$x^3+9x^2+15x-17$
$\frac{3410}{613}x^8+\frac{2166}{613}x^7-\frac{49726}{613}x^6-\frac{24864}{613}x^5+\frac{188240}{613}x^4+\frac{69860}{613}x^3-\frac{238030}{613}x^2-\frac{52896}{613}x+\frac{88791}{613}$	
$x^9+2x^8-12x^7-11x^6+44x^5+16x^4-62x^3+28x-7$	
$x=x$	x^3-7x-7
$-\frac{41}{139}x^8+\frac{6}{139}x^7+\frac{591}{139}x^6-\frac{570}{139}x^5-\frac{1618}{139}x^4+\frac{1976}{139}x^3+\frac{952}{139}x^2-\frac{1667}{139}x+\frac{189}{139}$	
$x^9+2x^8-9x^7-10x^6+27x^5+11x^4-25x^3-3x^2+6x-1$	
$x=x$	x^3-3x^2-4x-1
$x^7+2x^6-8x^5-7x^4+22x^3-14x+3$	

Erzeugendes Polynom des gegebenen Körpers	
Durchgeführte Substitution	Erzeugendes Polynom des Teilkörpers
Einbettung des Teilkörpers	
$x^9 - 14x^7 - 2x^6 + 63x^5 + 7x^4 - 106x^3 + 7x^2 + 56x - 13$	
$x = x$	$x^3 - 2x^2 - 15x - 13$
$\frac{168}{701}x^8 - \frac{345}{701}x^7 - \frac{1631}{701}x^6 + \frac{3101}{701}x^5 + \frac{3953}{701}x^4 - \frac{7455}{701}x^3 - \frac{308}{701}x^2 + \frac{2159}{701}x - \frac{1222}{701}$	
$x^9 + 2x^8 - 9x^7 - 15x^6 + 25x^5 + 37x^4 - 20x^3 - 31x^2 - 4x + 1$	
$x = x$	$x^3 - 8x^2 + 5x + 1$
$2x^8 + 5x^7 - 12x^6 - 28x^5 + 14x^4 + 38x^3 + 9x^2 - 3x$	
$x^9 - 11x^7 + 38x^5 - 48x^3 + 7x^2 + 21x - 7$	
$x = x$	$x^3 - 7x - 7$
$2x^8 + 4x^7 - 22x^6 - 39x^5 + 73x^4 + 105x^3 - 71x^2 - 62x + 28$	
$x^9 + x^8 - 15x^7 - 6x^6 + 76x^5 - 24x^4 - 130x^3 + 133x^2 - 38x + 1$	
$x = x$	$x^3 + 13x^2 + 26x + 1$
$\frac{48}{41}x^8 + \frac{99}{41}x^7 - \frac{602}{41}x^6 - 22x^5 + \frac{2541}{41}x^4 + \frac{1371}{41}x^3 - \frac{4381}{41}x^2 + \frac{1783}{41}x - \frac{50}{41}$	
$x^9 + 2x^8 - 13x^7 - 15x^6 + 57x^5 + 27x^4 - 78x^3 - 27x^2 + 32x + 13$	
$x = x$	$x^3 + 2x^2 - 29x + 13$
$-\frac{644}{547}x^8 - \frac{1747}{547}x^7 + \frac{6314}{547}x^6 + \frac{11556}{547}x^5 - \frac{21714}{547}x^4 - \frac{15610}{547}x^3 + \frac{18237}{547}x^2 + \frac{5033}{547}x - \frac{1794}{547}$	
$x^9 - 11x^7 + 3x^6 + 35x^5 - 10x^4 - 42x^3 + 7x^2 + 17x + 1$	
$x = x$	$x^3 + 3x^2 - 13x + 1$
$-3x^8 - 3x^7 + 29x^6 + 20x^5 - 75x^4 - 47x^3 + 54x^2 + 35x + 2$	
$x^9 - 2x^8 - 8x^7 + 18x^6 + 10x^5 - 36x^4 + 10x^3 + 12x^2 - 7x + 1$	
$x = x + 2$	$x^3 + 5x^2 - x - 13$
$-2x^7 - 26x^6 - 126x^5 - 278x^4 - 262x^3 - 50x^2 + 48x + 13$	
$x^9 - 15x^7 - 3x^6 + 68x^5 + 16x^4 - 122x^3 - 26x^2 + 76x + 13$	
$x = x$	$x^3 - 3x^2 - 18x + 13$
$\frac{51}{4}x^8 + \frac{99}{4}x^7 - \frac{345}{2}x^6 - \frac{1455}{4}x^5 + \frac{2145}{4}x^4 + \frac{4929}{4}x^3 - \frac{1473}{4}x^2 - \frac{4623}{4}x - \frac{715}{4}$	

Erzeugendes Polynom des gegebenen Körpers	
Durchgeführte Substitution	Erzeugendes Polynom des Teilkörpers
Einbettung des Teilkörpers	
$x^9 + 4x^8 - 8x^7 - 38x^6 - 2x^5 + 79x^4 + 45x^3 - 20x^2 - 11x - 1$	
$x = x$	$x^3 - 17x^2 + 10x - 1$
$\frac{4281}{4319}x^8 + \frac{10709}{4319}x^7 - \frac{49586}{4319}x^6 - \frac{86523}{4319}x^5 + \frac{114257}{4319}x^4 + \frac{156419}{4319}x^3 - \frac{24015}{4319}x^2 - \frac{34749}{4319}x - \frac{3174}{4319}$	
$x^9 - 2x^8 - 14x^7 + 26x^6 + 31x^5 - 42x^4 - 32x^3 + 10x^2 + 8x + 1$	
$x = x$	$x^3 + 3x^2 - 4x + 1$
$\frac{527}{1471}x^8 - \frac{843}{1471}x^7 - \frac{7562}{1471}x^6 + \frac{10652}{1471}x^5 + \frac{18313}{1471}x^4 - \frac{14626}{1471}x^3 - \frac{17076}{1471}x^2 - \frac{1017}{1471}x + \frac{1319}{1471}$	
$x^9 + 2x^8 - 14x^7 - 10x^6 + 71x^5 - 18x^4 - 117x^3 + 109x^2 - 24x + 1$	
$x = x$	$x^3 + 6x^2 + 5x + 1$
$-16x^8 - 55x^7 + 145x^6 + 368x^5 - 609x^4 - 583x^3 + 1039x^2 - 263x + 11$	
$x^9 - 15x^7 + 4x^6 + 54x^5 - 12x^4 - 38x^3 + 9x^2 + 6x - 1$	
$x = x + 2$	$x^3 + 33x^2 + 279x + 127$
$\frac{3}{2}x^8 + \frac{47}{2}x^7 + 138x^6 + 367x^5 + 376x^4 - 104x^3 - 377x^2 - \frac{131}{2}x + \frac{127}{2}$	
$x = x + 1$	$x^3 + 6x^2 - 51x + 8$
$-\frac{260}{127}x^8 - \frac{2113}{127}x^7 - \frac{3602}{127}x^6 + \frac{7642}{127}x^5 + \frac{22228}{127}x^4 + \frac{1452}{127}x^3 - \frac{25520}{127}x^2 - \frac{15120}{127}x - \frac{2360}{127}$	
$x = x + 1$	$x^3 - 12x^2 + 12x + 8$
$\frac{194}{127}x^8 + \frac{1603}{127}x^7 + \frac{2969}{127}x^6 - \frac{4987}{127}x^5 - \frac{17623}{127}x^4 - \frac{5673}{127}x^3 + \frac{19247}{127}x^2 + \frac{17583}{127}x + \frac{3832}{127}$	
$x = x + 1$	$x^3 - 8x^2 + 12x + 8$
$-\frac{711}{254}x^8 - \frac{5979}{254}x^7 - \frac{11547}{254}x^6 + \frac{17847}{254}x^5 + \frac{67221}{254}x^4 + \frac{22583}{254}x^3 - \frac{71751}{254}x^2 - \frac{31752}{127}x - \frac{6480}{127}$	

Beim Betrachten der Tabelle stellt man fest, daß insgesamt 6 Teilkörper nur nach einer Substitution berechnet werden konnten. Besonders interessant ist hier der letzte Körper, wo alle Teilkörper teils erst nach zweifacher Substitution berechnet werden konnten.

Als nächstes betrachten wir ein Beispiel eines Körpers vom Grad 12, der die $\mathfrak{A}_4$ als Galoisgruppe hat. Ein erzeugendes Polynom für diesen Körper ist:

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

Bekanntermaßen gibt es 3 Teilkörper vom Grad 6, 4 Teilkörper vom Grad 4 und einen vom Grad 3. Diese Körper haben wir mit unserem Verfahren berechnet. Die Berechnungen haben 6:46 min benötigt. In der folgenden Tabelle steht jeweils in der ersten Zeile ein erzeugendes Polynom des Teilkörpers und in der zweiten Zeile seine Einbettung. Beim dritten und siebten Körper mußte das erzeugende Polynom vor der Berechnung mit $x = x + 1$ substituiert werden.

$x^6 - 6x^5 - 2x^4 + 48x^3 - 45x^2 - 22x + 1$
$\frac{197}{196}x^{11} + \frac{215}{196}x^{10} - \frac{1416}{49}x^9 - \frac{8255}{196}x^8 + \frac{9815}{49}x^7 + \frac{21422}{49}x^6 - \frac{1200}{49}x^5 - \frac{102279}{196}x^4 - \frac{52471}{196}x^3 + \frac{1823}{98}x^2 + \frac{4797}{196}x + \frac{279}{98}$
$x^6 - 3x^5 - 11x^4 + 27x^3 - 3x^2 - 11x + 1$
$-\frac{433}{196}x^{11} - \frac{443}{196}x^{10} + \frac{3050}{49}x^9 + \frac{17603}{196}x^8 - \frac{19991}{49}x^7 - \frac{93677}{98}x^6 - \frac{12949}{98}x^5 + \frac{211713}{196}x^4 + \frac{158845}{196}x^3 + \frac{2497}{49}x^2 - \frac{16091}{196}x - \frac{655}{49}$
$x^6 - 24x^5 + 211x^4 - 816x^3 + 1282x^2 - 528x - 241$
$\frac{3473}{196}x^{11} + \frac{20273}{98}x^{10} + \frac{116829}{196}x^9 - \frac{307383}{196}x^8 - \frac{164015}{14}x^7 - \frac{823842}{49}x^6 + \frac{2548557}{98}x^5 + \frac{21948643}{196}x^4 + \frac{1971527}{14}x^3 + \frac{14431917}{196}x^2 + \frac{1621177}{196}x - \frac{164603}{49}$
$x^4 - 24x^3 + 38x^2 + 16x + 1$
$-\frac{83}{14}x^{11} + \frac{29}{14}x^{10} + \frac{2287}{14}x^9 + \frac{229}{14}x^8 - \frac{7652}{7}x^7 - \frac{14599}{14x}^{6} + \frac{12655}{14}x^5 + \frac{9698}{7}x^4 + \frac{2775}{7}x^3 - \frac{444}{7}x^2 - 47x - \frac{81}{14}$
$x^4 - 7x^3 + 5x^2 + 6x + 1$
$-\frac{953}{196}x^{11} - \frac{629}{98}x^{10} + \frac{6771}{49}x^9 + \frac{46419}{196}x^8 - \frac{178833}{196}x^7 - \frac{462883}{196}x^6 - \frac{83043}{196}x^5 + \frac{129868}{49}x^4 + \frac{389689}{196}x^3 + \frac{23745}{196}x^2 - \frac{9657}{49}x - \frac{3163}{98}$
$x^4 - 28x^3 - 15x^2 + 3x + 1$
$\frac{64}{49}x^{11} + \frac{61}{49}x^{10} - \frac{7207}{196}x^9 - \frac{4953}{98}x^8 + \frac{11834}{49}x^7 + \frac{107223}{196}x^6 + \frac{12041}{196}x^5 - \frac{120443}{196}x^4 - \frac{88903}{196}x^3 - \frac{3439}{98}x^2 + \frac{8709}{196}x + \frac{1525}{196}$
$x^4 - 10x^3 - 32x^2 + 410x - 241$
$4x^{11} + 46x^{10} + 128x^9 - 362x^8 - 2560x^7 - 3524x^6 + 5848x^5 + 24142x^4 + 30082x^3 + 15750x^2 + 1804x - 723$
$x^3 + 14x^2 + 11x - 1$
$\frac{335}{98}x^{11} + \frac{165}{196}x^{10} - \frac{4721}{49}x^9 - \frac{3142}{49}x^8 + \frac{130059}{196}x^7 + \frac{187423}{196}x^6 - \frac{81449}{196}x^5 - \frac{236127}{196}x^4 - \frac{21074}{49}x^3 + \frac{11769}{196}x^2 + \frac{8375}{196}x + \frac{443}{98}$

Literaturverzeichnis

[Cas1] J.W.S. Cassels, *An Introduction to the geometry of numbers*, Springer-Verlag, Berlin - Heidelberg - New York, 1971.

[Cas2] J.W.S. Cassels, *Local Fields*, Cambridge University Press, 1986.

[Coh] H. Cohen, *A Course in Computational Algebraic Number Theory*, Springer-Verlag, Berlin - Heidelberg - New York - London - Paris - Tokyo - Hong Kong - Barcelona - Budapest, 1993.

[Ded] R. Dedekind, *Gesammelte mathematische Werke, 3 Bände*, Vieweg, Braunschweig, 1930-1932.

[Dix1] J. Dixon, *Computing Subfields in Algebraic Number Fields*, J. Austral. Math. Soc. (Series A) **49**, (1990), 434–448.

[Dix2] J. Dixon, *Exact Solution of Linear Equations Using p-adic Expansions*, Numer. Math. **40**, (1982), 137–141.

[Hil] D. Hilbert, *Gesammelte Abhandlungen*, Springer-Verlag, Berlin - Heidelberg - New York, 1970.

[Hup] B. Huppert, *Endliche Gruppen I*, Springer-Verlag, Berlin - Heidelberg - New York, 1967.

[Khi] A. Khintchine, *Kettenbrüche*, Teubner Verlagsgesellschaft, Leipzig, 1956.

[Lan] S. Lang, *Algebra*, Addison-Wesley, Amsterdam - London - Manila - Singapore - Sydney - Tokyo, 1974.

[LLL] A.K. Lenstra, H.W. Lenstra und L. Lovász, *Factoring Polynomials with Rational Coefficients*, Math.Ann. **261**, (1982), 515–534.

[Mar] D.A. Marcus, *Number Fields*, Springer Verlag, New York - Heidelberg - Berlin, 1977.

[Nar] W. Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers*, Springer-Verlag, Berlin - Heidelberg - New York - London - Paris - Tokyo - Hong Kong, 1990.

[Poh] M. Pohst, *Computational Algebraic Number Theory*, DMV Seminar Band 21, Birkhäuser-Verlag, Basel - Boston - Berlin, 1993.

[PoZa] M. Pohst und H. Zassenhaus, *Algorithmic Algebraic Number Theory*, Cambridge Univ. Press, New York - Port Chester - Melbourne - Sydney, 1989.

[Wae] B.L. van der Waerden, *Algebra I*, Springer-Verlag, Berlin - Heidelberg - New York, 1971.

Bezeichnungen

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

$\mathbb{Z}$	Menge der ganzen Zahlen
$\mathbb{N}$	Menge der natürlichen Zahlen
$\mathbb{Q}$	Menge der rationalen Zahlen
$\mathbb{R}$	Menge der reellen Zahlen
$\mathbb{C}$	Menge der 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
$\mathrm{Fix}(H)$	der zu H gehörige Fixkörper
$\mathrm{disc}(f)$	Polynomdiskriminante von f
p	Primzahl
$\mathbb{F}_p, \mathbb{F}_q$	endliche Körper mit p bzw. q Elementen

$\mathfrak{p}, \mathfrak{P}$	Primideale
$\nu_{\mathfrak{p}}(\mathfrak{a})$	Exponent von $\mathfrak{p}$ in der Primidealzerlegung von $\mathfrak{a}$
$\mathbb{Q}_p$	Körper der p-adischen Zahlen
$\mathbb{Z}_p$	Ring der ganzen p-adischen Zahlen
$K_{\mathfrak{p}}$	$\mathfrak{p}$-adische Vervollständigung des Zahlkörpers K
K	der gegebene algebraische Zahlkörper
$\mathfrak{o}_K$	Ring der ganz algebraischen Zahlen von K
G	Die Galoisgruppe des Zerfällungskörpers von K.
L	ein Teilkörper von K
Δ	ein Block von G
$f \bmod p$	Ein $\tilde{f}$ mit $f \equiv \tilde{f} \bmod p\mathbb{Z}[t]$
$a \bmod \mathfrak{p}$	Ein $\tilde{a}$ mit $a \equiv \tilde{a} \bmod \mathfrak{p}$
$g \equiv h \bmod \omega$	$(g-h) \mid \omega$ in $\mathbb{Q}[t]$
$\pi = \pi_1 \cdot \ldots \cdot \pi_u$	Element von G, zerlegt in elementfremde Zykel
$[n_1, \ldots, n_u]$	Zykeltyp von π, d.h. die Längen der π_i

Hiermit versichere ich, daß ich die vorliegende Arbeit selbstständig verfaßt und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt habe.

Berlin, den 22.12.94

Ich danke Herrn Professor M. Pohst für die Überlassung dieses interessanten Themas sowie für seine ständige Diskussionsbereitschaft und seine Ratschläge. Weiterhin danke ich allen Mitarbeitern des Softwarepakets KANT, durch das die Implementierung der Algorithmen erst ermöglicht wurde.