Zum Round 4 Algorithmus

Diplomarbeit
von
Georg Baier

Angefertigt am Fachbereich Mathematik
der Technischen Universität Berlin
Berlin 1996

Inhaltsverzeichnis

Einleitung

Die schnell fortschreitende Entwicklung der Rechentechnik ermöglicht es, viele Fragestellungen, welche bisher nur vom Existenzstandpunkt aus behandelt wurden, nun auch konstruktiven Untersuchungen zu unterziehen. Der algebraischen Zahlentheorie kommt dabei eine wichtige Rolle zu, da sich die Menschen schon vor mehreren Tausend Jahren mit der algorithmischen Lösung von algebraischen Gleichungen beschäftigt haben. In diesem Jahrhundert hat sich die konstruktive Zahlentheorie endgültig zu einem eigenständigen Forschungsgebiet herausgebildet.

Eine der grundlegenden Aussagen der algebraischen Zahlentheorie ist die Existenz einer Ganzheitsbasis. Ihre Kenntnis ist für viele weiterführende Konstruktionsprobleme von Bedeutung, um praktisch rechnen zu können. Für die Bestimmung von Ganzheitsbasen stehen verschiedene Verfahren zur Verfügung, einige davon sind nur in speziellen Körpern anwendbar. Thema dieser Arbeit ist die Beschreibung und Implementierung eines von D. Ford [Fo87] und H. Zassenhaus entwickelten Algorithmus, welcher die Ganzheitsbasis von beliebigen algebraischen Zahlkörpern berechnet. Er ist unter der Bezeichnung Round 4 bekannt geworden.

Vor der Entwicklung des Round 4 existierten schon andere Verfahren zur Lösung der gleichen Aufgabenstellung. Von diesen hat vor allem der Round 2 größere Verbreitung gefunden. Die Idee des Round 2 besteht in dem schrittweisen Aufsteigen von einer Startordnung zur Maximalordnung. Ordnungen sind immer durch $\mathbb{Z}$-Basen gegeben. Dabei wird ständig der Index der aktuellen Ordnung in der Maximalordnung verringert. Hat die Startordnung nun einen sehr großen Index in der Maximalordnung, so kann es zu großen Rechenzeiten kommen. Damit war das Ziel weiterer Forschungen gegeben. Es mußte eine andere Aufteilung der Konstruktion in weniger Teilprobleme gefunden werden.

Grundlage des Round 4 ist eine Arbeit von H. Zassenhaus [Za], welche die Verlagerung der Berechnungen von großen Strukturen in mehrere kleinere Strukturen im nicht primären Fall ermöglicht. Als problematisch erwies sich die Einschränkung, daß die Zerlegung des Problems nur bei Vorliegen einer Gleichungsordnung möglich ist. Es ist somit nicht möglich, diese Zerlegung in den Round 2 – mit Ausnahme der Startordnung – einzubinden und so eine gemischte Berechnung durchzuführen. D. Ford hat in seiner Arbeit [Fo87] einen Weg angegeben, auf welchem es möglich ist, bis zum Erreichen der Maximalordnung die Berechnungen immer wieder in kleinere Teile zu zerlegen. Seit der ersten Implementation durch D. Ford wurden zahlreiche Verbesserungen von R. Böffgen, D. Ford, R. Land und H. Zassenhaus in den Algorithmus eingebracht.

Wir werden in dieser Arbeit zuerst den Algorithmus schrittweise entwickeln und anschließend Probleme der Implementation diskutieren. Die recht komplexe Natur des Algorithmus ließ diese Trennung von Korrektheits- und Effizienzüberlegungen ratsam erscheinen. In den ersten beiden Kapiteln werden wir die theoretischen Grundlagen für den Algorithmus zusammenstellen. Das zweite Kapitel enthält im Gegensatz zum ersten schon erste für den Algorithmus verallgemeinerte, spezielle Aussagen. Den kompletten, in drei Teilprobleme zerlegten Algorithmus stellen wir im dritten Kapitel vor. Im vierten Kapitel fassen wir dann unsere Teilergebnisse zusammen, was vor allem auf dem Hasseschen „Lokal – Global“ Prinzip basiert. Anschließend werden wir im fünften Kapitel die Probleme bei der Implemetation und Modifikationen zur Laufzeitverbesserung diskutieren. Die dargelegten Erfahrungen wurden bei der Einbindung des Round 4 in das Programmpaket KANT gesammelt. Beispiele mit einem Laufzeitvergleich des Round 4 zum Round 2 und statistischen Werten zum Verhalten des Round 4 im Kernalgorithmus listen wir im sechsten Kapitel auf. Abschließend zeigen wir, daß sich die Idee des Round 4 auch für eine andere Problemstellung als Lösungsansatz anbietet. Unter Beibehaltung der Kerngedanken des Algorithmus werden wir zeigen, daß es möglich ist, separable Polynome über $\mathbb{Q}_p$ zu faktorisieren.

An dieser Stelle möchte ich mich bei Herrn Professor Dr. M. E. Pohst und den Mitarbeitern des KANT Projektes bedanken. Für viele fruchtbare Diskussionen und die TEXnische Unterstützung bin ich Florian Heß und Claus Fieker dankbar.

Schließlich gilt mein besonderer Dank meinen Eltern, die mir das Studium ermöglicht haben, und Maren.

Kapitel 1

Grundlagen

In diesem Kapitel werden wir die grundlegenden Begriffe der algebraischen Zahlentheorie mit Ausnahme der Bewertungstheorie einführen. Wir beschränken uns auf Aussagen, welche später noch benötigt werden. Eine umfassende Einführung in die Theorie der algebraischen Zahlkörper wird in den Werken [Ar, Ri, We] gegeben.

1.1 Algebraische Zahlkörper

Dieses Gebiet ist in vielen Lehrbüchern der Zahlentheorie ausführlich beschrieben, so daß hier auf Beweise vollständig verzichtet werden soll.

Eine endliche Erweiterung $\mathcal{F}$ ($\subset \mathbb{C}$) des Körpers der rationalen Zahlen $\mathbb{Q}$ heißt **algebraischer Zahlkörper**. $\mathcal{F}$ ist als endliche Erweiterung eines vollkommenen Körpers einfach, es existiert also ein $\xi \in \mathcal{F}$ mit

$$\mathcal{F} = \mathbb{Q}(\xi).$$

Sei $f \in \mathbb{Z}[t]$ normiert und irreduzibel mit $f(\xi) = 0$, so gilt

$$\mathcal{F} \cong \mathbb{Q}[t]/f(t)\mathbb{Q}[t] = \mathbb{Q}(\rho)$$

mit $\rho := t + f(t)\mathbb{Q}[t]$ und $[\mathcal{F} : \mathbb{Q}] = \mathrm{Grad}(f) = n$. Zu $\alpha \in \mathcal{F}$ heißt das normierte Polynom $\mu_\alpha \in \mathbb{Z}[t]$ minimalen Grades mit $\mu_\alpha(\alpha) = 0$ das **Minimalpolynom** von α. Für ρ gilt somit $\mu_\rho = f$. Über $\mathbb{C}$ zerfällt μ_ρ in Linearfaktoren

$$\mu_\rho(t) = \prod_{i=1}^{n}(t - \rho^{(i)}).$$

Man bezeichnet $\rho^{(i)}$ als die i-te **Konjugierte** von ρ und $\mathcal{F}^{(i)} := \mathbb{Q}(\rho^{(i)})$ als den i-ten **Konjugiertenkörper** von $\mathcal{F}$. Vermöge der $\mathbb{Q}$-linearen Fortsetzung der Abbildung

$$\sigma_i : \rho \longmapsto \rho^{(i)}$$

für $i \in \{1, \ldots, n\}$ erhält man $\mathbb{Q}$-Isomorphismen zwischen $\mathcal{F}$ und seinen Konjugiertenkörpern, welche $\mathbb{Q}$ elementweise festhalten. Für ein beliebiges $\alpha \in \mathcal{F}$ bezeichnet man $\alpha^{(i)} := \sigma_i(\alpha)$ als die i-te **Konjugierte** zu α. Im Gegensatz zu $\rho^{(1)}, \ldots, \rho^{(n)}$ sind die Konjugierten $\alpha^{(1)}, \ldots, \alpha^{(n)}$ von α im allgemeinen nicht paarweise verschieden.

Wir können $\mathcal{F}$ auch als $\mathbb{Q}$-Vektorraum betrachten und entsprechend der linearen Algebra für ein Element α aus $\mathcal{F}$ das charakteristische Polynom definieren. Sei $l_\alpha : \mathcal{F} \longrightarrow \mathcal{F}$ die $\mathbb{Q}$-lineare Abbildung $x \mapsto \alpha x$ und M_α die darstellende Matrix von l_α für eine beliebige $\mathbb{Q}$-Basis $\omega_1, \ldots, \omega_n$ von $\mathcal{F}$, so ist das **charakteristische Polynom** von α definiert durch

$$\chi_\alpha(t) := \det(tE_n - M_\alpha).$$

χ_α liegt in $\mathbb{Q}[t]$ und ist von der Wahl der $\mathbb{Q}$-Basis von $\mathcal{F}$ unabhängig. Weiterhin definiert man mit M_α die **Norm** und die **Spur** von α

$$\begin{aligned} \mathrm{N}(\alpha) &:= \det(M_\alpha) \\ \mathrm{Tr}(\alpha) &:= \mathrm{Tr}(M_\alpha). \end{aligned}$$

Da $-\mathrm{Tr}(M_\alpha)$ dem Koeffizienten der zweithöchsten t-Potenz und $(-1)^n \det(M_\alpha)$ dem konstanten Term des charakteristischen Polynoms von α entsprechen, sind auch sie von der Basis unabhängig. Die Norm und die Spur lassen sich auch mit Hilfe der Konjugierten von α beschreiben. Es gilt $\mathrm{N}(\alpha) = \prod_{i=1}^n \sigma_i(\alpha)$ und $\mathrm{Tr}(\alpha) = \sum_{i=1}^n \sigma_i(\alpha)$.

Jeder $\mathbb{Q}$-Basis $\omega_1, \ldots, \omega_n$ von $\mathcal{F}$ kann man durch

$$\mathrm{d}(\omega_1, \ldots, \omega_n) := \det(\mathrm{Tr}(\omega_i \omega_j))$$

eine Zahl zuordnen, die als **Diskriminante** von $\omega_1, \ldots, \omega_n$ bezeichnet wird. Sei $\omega_1', \ldots, \omega_n'$ eine weitere Basis von $\mathcal{F}$ und T die Übergangsmatrix

$$(\omega_1', \ldots, \omega_n') = (\omega_1, \ldots, \omega_n)T,$$

so gilt

$$\mathrm{d}(\omega_1', \ldots, \omega_n') = (\det T)^2 \mathrm{d}(\omega_1, \ldots, \omega_n).$$

Kommen wir jetzt zu dem wichtigsten Begriff für diese Arbeit.

Ganze Elemente und Ordnungen

Existiert zu einem Element α aus $\mathcal{F}$ ein normiertes Polynom $g \in \mathbb{Z}[t]$ mit $g(\alpha) = 0$, so heißt α **ganzalgebraisch**. Die Menge aller ganzalgebraischen Elemente aus $\mathcal{F}$ werde mit $\mathfrak{o}_{\mathcal{F}}$ beziehungsweise $\mathfrak{o}_f$ bezeichnet ($\mathcal{F} \cong \mathbb{Q}[t]/f(t)\mathbb{Q}[t]$). $\mathfrak{o}_{\mathcal{F}}$ bildet mit der Addition und der Multiplikation aus $\mathcal{F}$ einen Ring, für den der folgende wichtige Satz gilt.

Satz 1.1.1 *Der Ring $\mathfrak{o}_{\mathcal{F}}$ ist ein freier $\mathbb{Z}$-Modul vom Rang $n = [\mathcal{F} : \mathbb{Q}] = \mathrm{Grad}(f)$.*

Beweis: Ein Beweis findet sich in [Ri].

$\mathfrak{o}_{\mathcal{F}}$ besitzt also eine $\mathbb{Z}$-Basis $\omega_1, \ldots, \omega_n$, die als **Ganzheitsbasis** von $\mathcal{F}$ bezeichnet wird.

Einen unitären Teilring von $\mathcal{F}$, der ein freier $\mathbb{Z}$-Modul vom Rang $n = [\mathcal{F} : \mathbb{Q}]$ ist, bezeichnet man als **Ordnung** von $\mathcal{F}$. Der Ring $\mathfrak{o}_{\mathcal{F}}$ ist also eine Ordnung. $\mathfrak{o}_{\mathcal{F}}$ spielt eine besondere Rolle unter den Ordnungen von $\mathcal{F}$. Denn ist $\mathcal{R}$ eine beliebige Ordnung von $\mathcal{F}$, so gilt $\mathcal{R} \subseteq \mathfrak{o}_{\mathcal{F}}$. Sei dazu α aus $\mathcal{R}$ beliebig. Wir müssen zeigen, daß α einer Polynomgleichung $\alpha^n + a_1\alpha^{n-1} + \ldots + a_n = 0$ mit $a_i \in \mathbb{Z}$ genügt. Sei $M_\alpha \in \mathbb{Q}^{n\times n}$ die Darstellungsmatrix von α bezüglich der $\mathbb{Z}$-Basis $\omega_1, \ldots, \omega_n$ von $\mathcal{R}$, d.h.

$$\alpha(\omega_1, \ldots, \omega_n) = (\omega_1, \ldots, \omega_n)M_\alpha.$$

Da für alle $i \in \{1, \ldots, n\}$ mit α auch $\alpha\omega_i$ in $\mathcal{R}$ liegt, ist M_α aus $\mathbb{Z}^{n\times n}$. Sei $g(t) = \det(tE_n - M_\alpha)$ das charakteristische Polynom von α, so ist g ein normiertes Polynom mit ganzrationalen Koeffizienten und α eine Nullstelle von g. Denn nach der Wahl von M_α gilt $(\omega_1, \ldots, \omega_n)(\alpha E_n - M_\alpha) = (0, \ldots, 0)$. Nach der Cramerschen Regel muß damit für alle $i \in \{1, \ldots, n\}$ gelten $\det(\alpha E_n - M_\alpha)\omega_i = 0$, was nur für $0 = \det(\alpha E_n - M_\alpha) = g(\alpha)$ möglich ist. Deshalb heißt $\mathfrak{o}_{\mathcal{F}}$ **Maximalordnung** von $\mathcal{F}$. Wir haben dabei sogar zusätzlich gezeigt, daß ein Element α genau dann ganzalgebraisch ist, wenn sein charakteristisches Polynom Koeffizienten aus $\mathbb{Z}$ hat.

Die Diskriminante einer Ganzheitsbasis ist nicht von der Basis abhängig, denn die Übergangsmatrizen zwischen Ganzheitsbasen sind unimodular. Die Diskriminante verändert sich aber um das Quadrat der Determinante der Übergangsmatrix und ist somit invariant. Die Diskriminante einer Ganzheitsbasis bildet eine Invariante des Körpers. Man nennt sie daher **Körperdiskriminante** von $\mathcal{F}$. Nach einem Resultat von Minkowski ist die Körperdiskriminante für algebraische Zahlkörper, ungleich dem Körper der rationalen Zahlen, immer von Eins verschieden.

Die Maximalordnung eines algebraischen Zahlkörpers hat eine weitere sehr wichtige Eigenschaft. Dazu führen wir zunächst den Begriff des Dedekindringes ein. Ein Integritätsring R heißt **Dedekindring**, wenn sich jedes Ideal von R, ungleich dem Nullideal, als eindeutiges Produkt von Primidealen darstellen läßt.

Satz 1.1.2 *Die Maximalordnung eines algebraischen Zahlkörpers ist ein Dedekindring.*

Beweis: Zum Beweis siehe [Ri].

Die Kenntnis der Maximalordnung ist also für das Verständnis der Strukturen in einem algebraischen Zahlkörpers von besonderem Interesse. Dazu ist es notwendig, eine Ganzheitsbasis konstruktiv erzeugen zu können. Die Beschreibung eines solchen Algorithmus ist das Ziel dieser Arbeit. Dabei handelt es sich um den unter dem Namen Round 4 bekannten Algorithmus von D. Ford. Im Gegensatz zum Round 2, der nur im Körper $\mathcal{F}$ und der Maximalordnung $\mathfrak{o}_{\mathcal{F}}$ rechnet, ist der Round 4 gezwungen, auch in allgemeineren Strukturen – Algebren – zu rechnen. Das führt häufig zu einer schnelleren Reduktion der Problemstellung und somit zu kürzeren Rechenzeiten. Die mit der Ausweitung der algebraischen Strukturen einhergehenden notwendigen Verallgemeinerungen der benötigten Begriffe, wie „ganzes Element“, sollen in diesem und dem nächsten Kapitel kurz dargelegt werden.

1.2 Quotientenringe

Sei R ein kommutativer Ring mit Eins. Da wir nur kommutative Ringe betrachten werden, soll im *ganzen Text* mit Ring immer ein kommutativer Ring mit Eins gemeint sein. Hat man eine multiplikative Teilmenge S von R ohne Nullteiler und Null, so kann man den **Quotientenring** $S^{-1}R$ von R nach S definieren durch

$$S^{-1}R := \left\{ \frac{r}{s} \mid r \in R, s \in S \right\},$$

wobei $\frac{r}{s}$ die Äquivalenzklasse von (r, s) zu der Äquivalenzrelation $(r, s) \sim (\tilde{r}, \tilde{s}) \Leftrightarrow r\tilde{s} = \tilde{r}s$ auf dem direkten Produkt $R \times S$ von R und S ist. Man kann nun R vermöge der Abbildung $r \mapsto (rs, s)$ — für ein beliebiges festes Element s aus S — als Teilmenge von $S^{-1}R$ betrachten. Ist R ein Integritätsring, so kann für S die Menge $R\backslash\{0\}$ gewählt werden. Man erhält mit $S^{-1}R$ dann den Quotientenkörper $\mathcal{Q}(R)$ von R. Für einen Ring R mit Nullteilern ist die Menge S aller Nichtnullteiler ungleich Null eine zulässige multiplikative Teilmenge von R. Der

Quotientenring $S^{-1}R$ heißt **totaler Quotientenring** von R. Wir bezeichnen ihn ebenfalls mit $\mathcal{Q}(R)$, da wir für Integritätsringe als totalen Quotientenring gerade den Quotientenkörper erhalten.

Für einen Integritätsring R und ein Primideal $\mathfrak{p}$ von R ist $S := R \backslash \mathfrak{p}$ eine multiplikative Teilmenge mit Eins von R. Der Quotientenring R' von R nach S wird **$\mathfrak{p}$-Lokalisierung** von R genannt. Im weiteren wird die $\mathfrak{p}$-Lokalisierung von Ringen eine wichtige Rolle spielen. Interessant wird sie durch die Beziehung zwischen den Idealen im Ring R und denen in der $\mathfrak{p}$-Lokalisierung R'.

Satz 1.2.1 *Seien R ein Integritätsring und R' der Quotientenring von R nach S. Dann gilt*

- *Für jedes Ideal $\mathfrak{a}'$ von R' gilt $R'(\mathfrak{a}' \cap R) = \mathfrak{a}'$.*
  Die Abbildung $\mathfrak{a}' \longmapsto \mathfrak{a}' \cap R$ ist also injektiv und inklusionserhaltend.
  Insbesondere gilt $(\mathfrak{a}' \cap R) \cap S = \emptyset$ für alle Ideale $\mathfrak{a}' \neq R'$ von R'.

- *Die Abbildung $\mathfrak{p}' \longmapsto \mathfrak{p}' \cap R$ bildet die Primideale $\mathfrak{p}'$ von R' surjektiv auf die zu S disjunkten Primideale von R ab.*

- *Für das Mengenkomplement $S = R \backslash \mathfrak{p}$ eines Primideales $\mathfrak{p}$ von R ergibt sich, daß die $\mathfrak{p}$-Lokalisierung R' von R nur noch ein maximales Ideal $R'\mathfrak{p}$ hat.*
  Durch die Abbildung $\mathfrak{p}' \longmapsto \mathfrak{p}' \cap R$ werden alle Primideale von R , die in $\mathfrak{p}$ liegen, erreicht.

Beweis: Siehe [Ri].

Grob gesagt, besteht also die $\mathfrak{p}$-Lokalisierung in der Vernachlässigung aller Primideale von R, die nicht in $\mathfrak{p}$ liegen. Bei Dedekindringen erhält man also, daß die $\mathfrak{p}$-Lokalisierung von R nur noch genau ein Primideal hat und alle anderen Ideale davon Potenzen sind.

Eine detaillierte Beschreibung der Eigenschaften von Quotientenringen findet sich in [Ri].

1.3 Algebren

Sei $\mathcal{K}$ ein Körper und $\mathcal{A}$ ein $\mathcal{K}$-Vektorraum. Besitzt $\mathcal{A}$ eine weitere innere binäre Verknüpfung $\cdot : \mathcal{A} \times \mathcal{A} \longrightarrow \mathcal{A}$, die Multiplikation, bezüglich der $\mathcal{A}$ ein unitärer Ring ist und für welche die Assoziativität $\lambda(a \cdot b) = (\lambda a) \cdot b = a \cdot (\lambda b)$ für beliebiges

λ aus $\mathcal{K}$ und a, b aus $\mathcal{A}$ gilt, so heißt $\mathcal{A}$ eine **$\mathcal{K}$-Algebra**. Ist die Multiplikation kommutativ, so heißt $\mathcal{A}$ eine kommutative $\mathcal{K}$-Algebra. Unter dem Rang einer Algebra versteht man die Dimension des $\mathcal{K}$-Vektorraumes $\mathcal{A}$. Wir werden uns nur mit speziellen kommutativen $\mathbb{Q}$-Algebren beschäftigen.

Falls nicht anders erwähnt, so soll unter einer Algebra immer eine der im folgenden beschriebenen Art gemeint sein. Sei f ein normiertes separables Polynom mit Koeffizienten aus dem unitären $R \subset \mathbb{Q}$, das heißt, f hat keine mehrfachen Nullstellen, so bildet der Faktorring

$$\mathcal{A}_f := \mathbb{Q}[t]/f(t)\mathbb{Q}[t]$$

zusammen mit der Polynommultiplikation eine Algebra über $\mathbb{Q}$ vom Rang $n = \mathrm{Grad}(f)$. Ist f nicht irreduzibel über R, so gilt nach dem chinesischen Restsatz die Isomorphie

$$\mathcal{A}_f \cong \bigoplus_{i=1}^{r} \mathcal{A}_{f_i},$$

wobei $f = \prod_{i=1}^{r} f_i$ die Zerlegung von f in normierte, irreduzible Faktoren über $\mathbb{Q}$ sei. Die f_i sind paarweise koprim, da f separabel ist, und der chinesische Restsatz ist anwendbar. Nach der Wahl von R ist der Quotientenkörper von R gleich $\mathbb{Q}$ und somit nach dem Lemma von Gauß jede Zerlegung von f über $\mathbb{Q}$ eine Zerlegung über R. Für f_i irreduzibel ist $\mathcal{A}_{f_i}$ aber ein Körper. Wir können also alle unsere Algebren $\mathcal{A}_f$ als direkte Summe von Körpern schreiben. Damit setzen sich auch alle Rechnungen in $\mathcal{A}_f$ aus den gewohnten Rechnungen in Körpern zusammen. $\mathcal{A}_f$ enthält möglicherweise Nullteiler, aber da es eine Summe von Körpern ist, keine nilpotenten Elemente ungleich Null. Es gilt sogar die umgekehrte Aussage, ist $\mathcal{A}$ eine endliche $\mathbb{Q}$-Algebra mit dem einzigen nilpotenten Element Null, so ist $\mathcal{A}$ die direkte Summe von Körpern.

Ganze Elemente und Ordnungen

Analog zu algebraischen Zahlkörpern wollen wir ganzalgebraische Elemente auszeichnen. Die neue Definition muß natürlich mit der aus Abschnitt 1.1 auf Algebren, die Körper sind, übereinstimmen.

Im Hinblick auf unsere Konstruktionsaufgabe wollen wir jedoch unsere Definition noch weiter fassen. Wir können ganz allgemein für eine unitäre Ringerweiterung $\mathcal{S}/\mathcal{R}$ definieren, daß ein Element α aus $\mathcal{S}$ **ganzalgebraisch über $\mathcal{R}$** heißen soll, wenn es ein normiertes Polynom g aus $\mathcal{R}[t]$ mit $g(\alpha) = 0$ gibt. Analog zu Abschnitt 1.1 können wir die über $\mathcal{R}$ ganzalgebraischen Elemente von $\mathcal{S}$ charakterisieren.

Satz 1.3.1 *Sei $\mathcal{S}/\mathcal{R}$ eine unitäre Ringerweiterung. Ein Element α aus $\mathcal{S}$ ist genau dann ganzalgebraisch über $\mathcal{R}$, wenn $\mathcal{R}[\alpha]$ ein endlich erzeugter $\mathcal{R}$-Modul ist.*

Beweis: Sei g aus $\mathcal{R}[t]$ ein normiertes Polynom mit $g(\alpha) = 0$, dann ist offensichtlich, daß $1, \alpha, \ldots, \alpha^{\mathrm{Grad}(g)-1}$ ein endliches $\mathcal{R}$-Erzeugendensystem von $\mathcal{R}[\alpha]$ ist.

Seien umgekehrt $\mathcal{R}[\alpha]$ ein endlich erzeugter $\mathcal{R}$-Modul und $\omega_1, \ldots, \omega_k$ ein $\mathcal{R}$-Erzeugendensystem des Moduls. Für jedes $i \in \{1, \ldots, k\}$ liegt $\alpha\omega_i$ in $\mathcal{R}[\alpha]$. Die $k \times k$-Matrix $M_\alpha^{\mathcal{R}}$ mit $\alpha(\omega_1, \ldots, \omega_k) = (\omega_1, \ldots, \omega_k)M_\alpha^{\mathcal{R}}$ ist somit aus $\mathcal{R}^{k\times k}$. Sei $g(t)$ das normierte Polynom $\det(E_k t - M_\alpha^{\mathcal{R}})$ vom Grad k. Nach der Cramerschen Regel gilt $\det(E_k\alpha - M_\alpha^{\mathcal{R}})\omega_i = 0$ für alle $i \in \{1, \ldots, k\}$. Da $\mathcal{R}$ die Eins enthält, existieren $b_1, \ldots, b_k$ aus $\mathcal{R}$ mit $\sum_{i=1}^k b_i\omega_i = 1$. Für $g(\alpha)$ gilt damit $1 \cdot g(\alpha) = \sum_{i=1}^k b_i(\det(E_k\alpha - M_\alpha^{\mathcal{R}})\omega_i) = 0$. □

Die ganzalgebraischen Elemente eines Zahlkörpers $\mathcal{F}$ sind also genau die über $\mathbb{Z}$ ganzalgebraischen Elemente von $\mathcal{F}$. Wir wollen nun die Situation fixieren, daß $\mathcal{S}$ gleich unserer $\mathbb{Q}$-Algebra $\mathcal{A}_f$ ist und $\mathcal{R}$ gleich dem faktoriellen Ring R, über welchem unser Polynom gegeben ist. Das im Beweis von Satz 1.3.1 konstruierte Polynom g ist in diesem Fall also das charakteristische Polynom χ_α von α. Unter dem charakteristischen Polynom eines Elements der $\mathbb{Q}$-Algebra $\mathcal{A}_f$ verstehen wir das in dem unterliegenden $\mathbb{Q}$-Vektorraum gegebene charakteristische Polynom. Für unsere Situation haben wir also folgenden Satz gezeigt.

Satz 1.3.2 *Ein Element α aus $\mathcal{A}_f$ ist genau dann über dem faktoriellen Ring R ganz, wenn das charakteristische Polynom von α Koeffizienten aus R hat.*

Aus Satz 1.3.1 erhalten wir weiterhin, daß die Menge aller über R ganzalgebraischen Elemente von $\mathcal{A}_f$ ein Ring ist, denn mit $R[\alpha]$ und $R[\beta]$ ist auch $R[\alpha, \beta]$ ein endlich erzeugter R-Modul. Die Menge aller über $\mathbb{Z}$ ganzalgebraischen Elemente aus $\mathcal{A}_f$ bezeichnen wir wie in Abschnitt 1.1 ebenfalls mit $\mathfrak{o}_{\mathcal{A}_f}$ oder einfach mit $\mathfrak{o}_f$. Für $\mathfrak{o}_f$ gilt in Analogie zum Zahlkörperfall der folgende Satz.

Satz 1.3.3 *Der Ring $\mathfrak{o}_{\mathcal{A}_f}$ ist ein freier $\mathbb{Z}$-Modul vom Rang n.*

Beweis: Auf den Beweis soll an dieser Stelle verzichtet werden, da wir die Aussage später aus Satz 1.3.8 leicht folgern können.

Analog zu dem Abschnitt 1.1 bezeichnen wir einen unitärer Teilring von $\mathcal{A}_f$, der ein freier R-Modul vom Rang $n = \mathrm{Grad}(f)$ ist, mit R-**Ordnung** von $\mathcal{A}_f$.

Ist R der Ring der ganzrationalen Zahlen oder aus dem Kontext ersichtlich, um welchen Ring R es sich handelt, so wollen wir kürzer nur von einer Ordnung von $\mathcal{A}_f$ sprechen.

Wenden wir uns nun einigen konstruktiven Problemen in Algebren zu. Ist $\mathcal{A}_f$ kein Körper, so haben wir bereits gesehen, daß die Algebra isomorph zur direkten Summe $\bigoplus_{i=1}^r \mathcal{A}_{f_i}$ von Körpern ist. Wollen wir in der Summe, statt in $\mathcal{A}_f$ rechnen, so müssen wir explizit einen $\mathbb{Q}$-Isomorphismus zwischen den Algebren $\mathcal{A}_f$ und $\bigoplus_{i=1}^r \mathcal{A}_{f_i}$ angeben, welcher R-Ordnungen auf R-Ordnungen abbildet. Zunächst zeigen wir, daß wir orthogonale Idempotente in $\mathcal{A}_f$ konstruieren können, so daß die damit erhaltene Zerlegung der Algebra $\mathcal{A}_f$ in eine innere direkte Summe genau der schon erwähnten äußeren Summe entspricht.

Lemma 1.3.4 *Sei $f = f_1 f_2$ eine Zerlegung von f über R in normierte, koprime Faktoren. Dann existieren orthogonale Idempotente e_1 und e_2 von $\mathcal{A}_f$ und ein $\mathbb{Q}$-Isomorphismus φ von $\mathcal{A}_f$ nach $\mathcal{A}_{f_1} \oplus \mathcal{A}_{f_2}$ mit*

$$\begin{aligned} \varphi(e_1\mathcal{A}_f) &= \mathcal{A}_{f_1} \oplus \{0\} \\ \varphi(e_2\mathcal{A}_f) &= \{0\} \oplus \mathcal{A}_{f_2}. \end{aligned}$$

Beweis: Durch

$$\begin{aligned} \varphi \,:\, \mathcal{A}_f &\longrightarrow \mathcal{A}_{f_1} \oplus \mathcal{A}_{f_2} \\ g(t) + f(t)\mathbb{Q}[t] &\longmapsto (g(t) + f_1(t)\mathbb{Q}[t]) \oplus (g(t) + f_2(t)\mathbb{Q}[t]) \end{aligned}$$

wird ein $\mathbb{Q}$-Modulisomorphismus definiert. Seien $r_1, r_2 \in \mathbb{Q}[t]$ mit $r_1 f_1 + r_2 f_2 = 1$. Setze $\tilde{e}_2 = r_1 f_1$ und $\tilde{e}_1 = r_2 f_2$. Dann sind

$$\begin{aligned} e_1 &= \tilde{e}_1(t) + f(t)\mathbb{Q}[t] \\ e_2 &= \tilde{e}_2(t) + f(t)\mathbb{Q}[t] \end{aligned}$$

orthogonale Idempotenten in $\mathcal{A}_f$ mit

$$\begin{aligned} \varphi(e_1\mathcal{A}_f) &= \mathcal{A}_{f_1} \oplus \{0\} \\ \varphi(e_2\mathcal{A}_f) &= \{0\} \oplus \mathcal{A}_{f_2}. \end{aligned}$$

Denn $e_1 + e_2 = 1$ nach Wahl von r_1, r_2 und $e_1 e_2 = r_1 r_2 f_1 f_2 + f(t)\mathbb{Q}[t] = 0$. Damit gilt auch $e_i = e_i e_1 + e_i e_2 = {e_i}^2$ für $i \in \{1, 2\}$, und die Eigenschaften von zwei orthogonale Idempotenten sind gezeigt. Daß $\varphi(e_1\mathcal{A}_f) = \mathcal{A}_{f_1} \oplus \{0\}$ und $\varphi(e_2\mathcal{A}_f) = \{0\} \oplus \mathcal{A}_{f_2}$ gilt, ist offensichtlich nach der Wahl von φ und der Definition von e_1, e_2. $\square$

Durch die konstruktive Angabe der orthogonalen Idempotenten e_1 und e_2 im Beweis des Lemmas 1.3.4 — die Existenz ist schon im Voraus klar gewesen — erhalten wir eine explizite Darstellung von φ^{-1}.

Bemerkung 1.3.5 *Das Inverse, des in Lemma 1.3.4 konstruierten $\mathbb{Q}$-Isomorphismus φ, ist gegeben durch*

$$\begin{array}{rcl} \varphi^{-1} \ : \ \mathcal{A}_{f_1} \oplus \mathcal{A}_{f_2} & \longrightarrow & \mathcal{A}_f \\ g_1(\xi_1) \oplus g_2(\xi_2) & \longmapsto & e_1 g_1(\xi) + e_2 g_2(\xi), \end{array}$$

mit $\xi_i := t + f_i(t)\mathbb{Q}[t]$ für $i \in \{1, 2\}$ und $\xi := t + f(t)\mathbb{Q}[t]$.

Aus Lemma 1.3.4 erhalten wir induktiv das Korollar.

Korollar 1.3.6 *Sei $f = \prod_{i=1}^r f_i$ die Zerlegung von f in normierte, koprime Faktoren über R, so existieren orthogonale Idempotente $e_1, \ldots, e_r$ in $\mathcal{A}_f$ und ein R-Isomorphismus φ von $\mathcal{A}_f$ nach $\bigoplus_{i=1}^r \mathcal{A}_{f_i}$ mit*

$$\varphi(e_i \mathcal{A}_f) = \bigoplus_{j=1}^{r} \delta_{i,j} \mathcal{A}_{f_i}$$

für alle $i \in \{1, \ldots, r\}$.

Wir gehen noch kurz auf die Beziehung zwischen dem charakteristischen Polynom eines Elements α aus $\mathcal{A}_f$ und denen seiner Bilder unter φ in den Körpern $\mathcal{A}_{f_i}$ ein. Bezeichnen wir $e_i \mathcal{A}_f$ mit $\mathcal{A}_i$ und die Projektion $e_i \alpha$ von α auf $\mathcal{A}_i$ mit α_i, so ist klar, daß das charakteristische Polynom von α_i gleich dem charakteristischen Polynom von $\varphi(\alpha_i)$ ist.

Satz 1.3.7 *Seien $e_1, \ldots, e_r$ orthogonale Idempotenten von $\mathcal{A}_f$ und $\mathcal{A}_i := e_i \mathcal{A}_f$, so ist das charakteristische Polynom von α aus $\mathcal{A}_f$ gleich dem Produkt der charakteristischen Polynome der Projektionen von α in $\mathcal{A}_i$.*

Beweis: Für jedes $i \in \{1, \ldots, r\}$ sei $\omega_{i1} e_i, \ldots, \omega_{ij_i} e_i$ eine $\mathbb{Q}$-Basis von $\mathcal{A}_i$. Dann ist $\omega_{11} e_1, \ldots, \omega_{1j_1} e_1, \ldots, \omega_{r1} e_r, \ldots, \omega_{rj_r} e_r$ eine $\mathbb{Q}$-Basis von $\mathcal{A}_f$. Betrachten wir die Darstellungsmatrix M_α von α bezüglich dieser Basis. Auf Grund der Eigenschaften von Idempotenten gilt

$$\begin{array}{rl} & (\omega_{11} e_1, \ldots, \omega_{1j_1} e_1, \ \ldots, \ \omega_{r1} e_r, \ldots, \omega_{rj_r} e_r) M_\alpha \\ = & \alpha(\omega_{11} e_1, \ldots, \omega_{1j_1} e_1, \ \ldots, \ \omega_{r1} e_r, \ldots, \omega_{rj_r} e_r) \\ = & \left(\sum_{i=1}^r \alpha e_i \right) (\omega_{11} e_1, \ldots, \omega_{1j_1} e_1, \ \ldots, \ \omega_{r1} e_r, \ldots, \omega_{rj_r} e_r) \\ = & (\alpha e_1 \omega_{11} e_1, \ldots, \alpha e_1 \omega_{1j_1} e_1, \ \ldots, \ \alpha e_r \omega_{r1} e_r, \ldots, \alpha e_r \omega_{rj_r} e_r) \\ = & (\alpha_1 \omega_{11} e_1, \ldots, \alpha_1 \omega_{1j_1} e_1, \ \ldots, \ \alpha_r \omega_{r1} e_r, \ldots, \alpha_r \omega_{rj_r} e_r). \end{array}$$

M_α hat also die Gestalt

$$M_\alpha = \begin{pmatrix} M_{\alpha_1} & & \\ & \ddots & \\ & & M_{\alpha_r} \end{pmatrix},$$

wobei die Matrizen M_{α_i} die Darstellungsmatrizen der α_i in $\mathcal{A}_i$ bezüglich der Basen $\omega_{i1}e_i, \ldots, \omega_{ij_i}e_i$ sind. Für das charakteristische Polynom von α folgt

$$\begin{aligned} \chi_\alpha(t) &= \det(E_n t - M_\alpha) \\ &= \prod_{i=1}^{r} \det(E_{j_i} t - M_{\alpha_i}) \\ &= \prod_{i=1}^{r} \chi_{\alpha_i}(t). \end{aligned}$$

□

Die charakteristischen Polynome von über R ganzalgebraischen Elementen sind nach Konstruktion und Satz 1.3.2 normiert und aus $R[t]$. Da R ein faktorieller Ring ist, ist das Produkt von normierten Polynomen über $\mathcal{Q}(R) = \mathbb{Q}$ nach dem Lemma von Gauß genau dann aus $R[t]$, wenn alle Faktoren aus $R[t]$ sind. Damit haben wir auch folgenden Satz gezeigt.

Satz 1.3.8 *Sei $f = \prod_{i=1}^{r} f_i$ die Zerlegung von f in normierte, koprime Faktoren über $\mathbb{Q}$, so gilt für die Maximalordnung von $\mathcal{A}_f$*

$$\mathfrak{o}_f \cong \bigoplus_{i=1}^{r} \mathfrak{o}_{f_i}$$

unter dem $\mathbb{Q}$-Isomorphismus φ aus Korollar 1.3.4.

Aus Satz 1.3.8 folgt sofort mit Satz 1.1.1 die Aussage von Satz 1.3.3.

Zum Schluß wollen wir noch eine spezielle Ordnung, welche häufiger benötigt wird, bezeichnen. $\mathcal{R}_f := \mathbb{Z}[\xi]$ mit $\xi = t + f(t)\mathbb{Q}[t]$ ist eine Ordnung von $\mathcal{A}_f$, die sogenannte **Gleichungsordnung** von ξ.

Im Kapitel 2 werden wir eine für unsere Ringe äquivalente Charakterisierung von ganzalgebraischen Elementen zeigen, die besser auf die Entwicklung des Algorithmus zugeschnitten ist.

1.4 p-adische Körper

Für Effizienzuntersuchungen und die Beschreibung einer weiteren Anwendungsmöglichkeit der Grundidee des Algorithmus benötigen wir eine andere Metrik auf dem Körper $\mathbb{Q}$ der rationalen Zahlen, als die durch den Absolutbetrag gegebene. Desweiteren suchen wir einen vollständigen metrischen Oberkörper von $\mathbb{Q}$, in welchem $\mathbb{Q}$ dicht liegt und dessen Metrik eine Fortsetzung von der auf $\mathbb{Q}$ ist. In Kapitel 2 werden wir sehen, daß die benötigte Metrik von einer nichtarchimedischen Bewertung induziert wird.

Definieren wir zunächst die Metrik. Seien p eine beliebige rationale Primzahl und $v_p : \mathbb{Q} \longrightarrow \mathbb{Z}$ folgende Abbildung. Für eine ganze rationale Zahl n ungleich Null sei $v_p(n)$ der Exponent von p in der eindeutigen Zerlegung von n in Primfaktoren. $v_p(0)$ definieren wir als plus unendlich. Für eine rationale Zahl $\frac{n}{m}$ sei $v_p(\frac{n}{m}) := v_p(n) - v_p(m)$. Diese Definition ist von der Wahl des Repräsentanten $\frac{n}{m}$ für die rationale Zahl unabhängig. Durch $\mathrm{d}_p(r,q) := p^{-v_p(r-q)}$ wird auf $\mathbb{Q}$ eine Metrik definiert. Dabei soll $p^{-\infty}$ als Null interpretiert werden. Sie heißt die p-adische Metrik. Somit existiert ein bis auf Isomorphie eindeutiger vollständiger Körper $\mathbb{Q}_p$, in welchem $\mathbb{Q}$ dicht liegt, und dessen Metrik auf $\mathbb{Q}$ mit d_p übereinstimmt. $\mathbb{Q}_p$ heißt der Körper der **p-adischen Zahlen**. Wir können die Struktur von $\mathbb{Q}_p$ noch genauer angeben. Es gilt

$$\mathbb{Q}_p = \left\{ \sum_{i=r}^{\infty} a_i\, p^i \mid a_i \in \{0, \ldots, p-1\}, r \in \mathbb{Z}, a_r \neq 0 \right\},$$

dabei ist die Summendarstellung für die Elemente aus $\mathbb{Q}_p$ eindeutig. An dieser Darstellung läßt sich leicht der Abstand eines Elements von $\mathbb{Q}_p$ zur Null ablesen $\mathrm{d}_p(0, \sum_{i=r}^{\infty} a_i\, p^i) = p^{-r}$. Die Elemente mit $r \geq 0$ bilden einen Ring. Sie heißen die **ganzen** p-adischen Zahlen

$$\mathbb{Z}_p = \left\{ \sum_{i=r}^{\infty} a_i\, p^i \mid a_i \in \{0, \ldots, p-1\}, r \in \mathbb{Z}^{\geq 0}, a_r \neq 0 \right\}.$$

Zum Schluß wollen wir noch eine Abbildung angeben, welche $\mathbb{Q}_p$ auf $\mathbb{Q}$ abbildet. Sei $m \in \mathbb{Z}$, so können wir $b = \sum_{i=r}^{\infty} a_i\, p^i$ abbilden auf $\bar{b} = \sum_{i=r}^{m-1} a_i\, p^i$. Die Abbildung „$^-$“ ist additiv und auf $\mathbb{Z}_p$ multiplikativ. Zwischen dem Argument und dem Bild besteht weiterhin folgender Zusammenhang

$$\begin{aligned} a &\equiv \bar{a} \mod p^m \mathbb{Q}_p \\ b &\equiv \bar{b} \mod p^m \mathbb{Z}_p \end{aligned}$$

beziehungsweise

$$\begin{aligned} \mathrm{d}_p(a,\bar{a}) &\leq p^{-m} \\ \mathrm{d}_p(b,\bar{b}) &\leq p^{-m} \end{aligned}$$

für $a \in \mathbb{Q}_p$ und $b \in \mathbb{Z}_p$, $\bar{b}$ ist dabei aus $\mathbb{Z}$.

Die aufgeführten Aussagen und eine weitergehende Beschreibung der engen Beziehung zur Bewertungstheorie sowie weitere tiefliegende Eigenschaften der p-adischen Zahlen und ihrer Verallgemeinerung auf beliebige algebraische Zahlkörper wird in [Ar, Na, We] gegeben. Die topologischen Aussagen sind [Qe] entnommen.

Kapitel 2

Bewertungstheorie

Zahlreiche Werke analysieren das Gebiet der algebraische Zahlentheorie aus bewertungstheoretischer Sicht. Wir werden uns deshalb hier auf die sehr spezielle Sicht zur Lösung unserer Konstruktionsaufgabe beschränken. Eine allgemeine Beschreibung der Bewertungstheorie kann man zum Beispiel in [Ar, Na, Po/Za, We] nachlesen.

Wir wollen die Situation in Algebren $\mathcal{A}_f$ der in Abschnitt 1.3 beschriebenen Form untersuchen. Dazu fixieren wir die Situation, daß R, S und $\mathcal{A}$ kommutative, unitäre Ringe, möglicherweise mit Nullteilern, sind. R ist wieder ein faktorieller Teilring von $\mathbb{Q}$ und $\mathcal{A}$ eine von einem normierten, separablen Polynom f aus $R[t]$ erzeugte $\mathbb{Q}$-Algebra $\mathcal{A}_f$, das heißt, $\mathcal{A}$ ist die innere direkte Summe von Körpern. Das Radikal von $\mathcal{A}$ ist somit das Nullideal. $\mathcal{A}/S/R$ seien unitäre Ringerweiterungen. Ist $\mathcal{A}$ ein Körper, so wollen wir statt dessen das Symbol $\mathcal{F}$ benutzen.

Die übersprungenen Beweise finden sich, soweit nicht anders angeben, in [Ar, Po/Za, We].

2.1 Bewertungen und verallgemeinerte Bewertungen

Ausgehend von dem Absolutbetrag auf dem Körper der komplexen Zahlen erhält man durch Reduktion auf das Wesentliche den Begriff der **Bewertung** als einer Abbildung φ von einem Körper in die reellen Zahlen mit den Eigenschaften

(i) $\varphi(\alpha) \geq 0$

(ii) $\varphi(\alpha) = 0 \Leftrightarrow \alpha = 0$

(iii) $\varphi(\alpha + \beta) \leq \varphi(\alpha) + \varphi(\beta)$

(iv) $\varphi(\alpha\beta) = \varphi(\alpha)\varphi(\beta)$.

Es ist unmittelbar einsichtig, daß diese Definition nicht auf Ringe mit Nullteilern übertragen werden kann. Zwei Möglichkeiten stehen zur Verfügung, um eine angepaßte Definition für Ringe zu erhalten. Da wir nicht auf die Verträglichkeit von φ mit der Multiplikation verzichten wollen, werden wir die Bedingung $\varphi(\alpha) = 0 \Leftrightarrow \alpha = 0$ aufgeben.

Definition 2.1.1 *Sei R ein Ring mit Eins. Eine* **verallgemeinerte Bewertung** *auf R ist eine Abbildung $\varphi : R \longrightarrow \mathbb{R}$ mit den Eigenschaften:*

(i) $\varphi(\alpha) \geq 0$

(ii) $\varphi(\alpha + \beta) \leq \varphi(\alpha) + \varphi(\beta)$

(iii) $\varphi(\alpha\beta) = \varphi(\alpha)\varphi(\beta)$

(iv) $\varphi(\pm 1) = 1, \quad \varphi(0) = 0$

für $\alpha, \beta \in R$ beliebig.

Der Punkt (iv) ist wichtig, um die trivialen Fälle $\varphi \equiv 0$ und $\varphi \equiv 1$ zu verhindern.

Beispiel 2.1.2 *(i) Der Absolutbetrag auf $\mathbb{R}$ ist eine verallgemeinerte Bewertung von $\mathbb{R}$.*

(ii) Seien $R = \mathbb{Z}$ und p eine beliebige Primzahl. Für α aus $\mathbb{Z}$ sei $\lambda(\alpha)$ die größte Zahl aus $\mathbb{Z}^{\geq 0}$ mit $p^{\lambda(\alpha)}|\alpha$. Dann wird durch

$$\varphi(\alpha) := c^{\lambda(\alpha)} \qquad c \in (0,1)$$

eine verallgemeinerte Bewertung auf $\mathbb{Z}$ definiert.

(iii) Seien $\mathcal{F}$ ein algebraischer Zahlkörper und $R = \mathfrak{o}_{\mathcal{F}}$ der Ring der ganzalgebraischen Elemente von $\mathcal{F}$. Weiter sei $\mathfrak{p}$ ein beliebiges Primideal von $\mathfrak{o}_{\mathcal{F}}$. Die Maximalordnung $\mathfrak{o}_{\mathcal{F}}$ ist ein Dedekindring. Jedem Element α von $\mathcal{F}$ läßt sich also eindeutig der Exponent $\lambda(\alpha)$ von $\mathfrak{p}$ in der Zerlegung des Hauptideals $\alpha\mathfrak{o}_{\mathcal{F}}$ zuordnen. Dann wird analog zu (ii) durch

$$\varphi(\alpha) := c^{\lambda(\alpha)} \qquad c \in (0,1)$$

eine verallgemeinerte Bewertung auf $\mathfrak{o}_{\mathcal{F}}$ erklärt.

(iv) *Seien $S = R_1 \oplus R_2$ und φ_1 eine verallgemeinerte Bewertung auf R_1, so ist*

$$\varphi(r_1 \oplus r_2) := \varphi_1(r_1)$$

eine verallgemeinerte Bewertung von S.

Eine verallgemeinerte Bewertung heißt **nichtarchimedisch**, falls sie statt der Dreiecksungleichung (ii) die schärfere Ungleichung

$$\varphi(\alpha + \beta) \leq \max\{\varphi(\alpha), \varphi(\beta)\}$$

erfüllt. Sind die Bewertungen von α und β verschieden, so erhalten wir als Bewertung von $\alpha + \beta$ genau das Maximum der Bewertungen von α und β.

Beispiel 2.1.3 *In Beispiel 2.1.2 (ii) und (iii) handelt es sich um nichtarchimedische Bewertungen.*

Definiert man für nichtarchimedische verallgemeinerte Bewertungen φ

$$I(\varphi, x) := \{\alpha \in R \mid \varphi(\alpha) \leq x\},$$

so ist $I(\varphi, x)$ ein $\mathbb{Z}$-Modul für alle $x \in \mathbb{R}^{\geq 0}$. Für $I(\varphi, x)$ gilt

- $I(\varphi, x) \subseteq I(\varphi, y)$ für $0 \leq x \leq y$
- $I(\varphi, x)I(\varphi, y) \subseteq I(\varphi, xy)$ für $x, y \in \mathbb{R}^{\geq 0}$
- $I(\varphi, 0)$ ist ein Primideal von R.

Damit ergibt sich auch die Verbindung zwischen Bewertungen und verallgemeinerten Bewertungen. Geht man über zu dem nullteilerfreien Faktorring

$$\bar{R} = R/I(\varphi, 0)$$

und definiert

$$\begin{array}{rcl} \bar{\varphi} : \bar{R} & \longrightarrow & R \\ a + I(\varphi, 0) & \longmapsto & \varphi(a), \end{array}$$

so erhält man mit $\bar{\varphi}$ eine Bewertung auf $\bar{R}$.

Desweiteren besitzt $I(\varphi, 1)$ eine Sonderstellung, denn offensichtlich führt hier die Multiplikation nicht aus der Menge. $I(\varphi, 1)$ ist ein Ring, der als **verallgemeinerter Bewertungsring** von φ bezeichnet wird. Er besitzt das maximale

Ideal $\{\alpha \in R \mid \varphi(\alpha) < 1\}$, welches **verallgemeinertes Bewertungsideal** von φ heißt. Ist φ auf einem Körper definiert, so ist der Bewertungsring ein lokaler Ring und das Bewertungsideal das zugehörige eindeutige maximale Ideal.

Sei $Q \subseteq R$ eine zu $I(\varphi, 0)$ disjunkte, multiplikative Teilmenge von R. Q ist wegen 2.1.1 (iv) nullteilerfrei, und somit läßt sich φ vermittels

$$\tilde{\varphi}\left(\frac{r}{q}\right) := \frac{\varphi(r)}{\varphi(q)}$$

mit $r \in R, q \in Q$ auf den Quotientenring von R nach Q fortsetzen.

Beispiel 2.1.4 *Sei φ die Bewertung aus Beispiel 2.1.2.(ii). Es gilt*

- *Der Bewertungsring von φ ist $\mathbb{Z}$ und $p\mathbb{Z}$ das Bewertungsideal.*
- *Sei $\tilde{\varphi}(\frac{r}{q}) = \frac{\varphi(r)}{\varphi(q)}$ die Fortsetzung von φ auf $\mathbb{Q}$. So ist der Bewertungsring von $\tilde{\varphi}$ die p-Lokalisierung $\mathbb{Z}'$ von $\mathbb{Z}$ und $p\mathbb{Z}'$ das Bewertungsideal.*

2.2 Exponentialbewertungen

Nun wollen wir die nichtarchimedischen Bewertungen noch einmal von einer anderen Seite betrachten. Jede Bewertung φ auf R macht R zu einem metrischen Raum (R, d) durch $\mathrm{d}(\alpha, \beta) := \varphi(\alpha - \beta)$. Auf Grund der Tatsache, daß für eine nichtarchimedische Bewertung φ auch φ^2 eine nichtarchimedische Bewertung ist, welche dieselbe Topologie auf R induziert, ergibt sich die Idee zwei Bewertungen mit dieser Eigenschaft **äquivalent** zu nennen. Die Äquivalenzklassen nennt man **Primteiler** von R.

Satz 2.2.1 *Sei P ein Primteiler von $\mathcal{F}$, so gilt*

$$P = \{\varphi^c \mid c \in \mathbb{R}^{>0}\}$$

für $\varphi \in P$ beliebig.

Beweis: Ein Beweis findet sich in [Ar].

Jede Bewertung $\varphi \in P$ läßt sich also schreiben als $\varphi(\alpha) = e^{-c_\varphi v(\alpha)}$, wobei c_φ eine positive reelle Konstante und $e^{-v(\alpha)}$ eine beliebige Bewertung aus P ist. Da $e^{-v(\alpha)}$ nichtarchimedisch ist, ist die Definition der Bewertung äquivalent zu

(i) $v(\alpha) \in \mathbb{R} \cup \{\infty\}$

(ii) $v(\alpha) = \infty \Leftrightarrow \alpha = 0$

(iii) $v(\alpha + \beta) \geq \min\{v(\alpha), v(\beta)\}$

(iv) $v(\alpha\beta) = v(\alpha) + v(\beta)$.

Auch hier gilt bei der Dreiecksungleichung (iii) wieder Gleichheit, wenn $v(\alpha)$ ungleich $v(\beta)$ ist. Bei verallgemeinerten Bewertungen entfällt entsprechend Punkt (ii), und zur Verhinderung der trivialen Fälle kommen die Bedingungen $v(\pm 1) = 0$ und $v(0) = \infty$ hinzu. v heißt (verallgemeinerte) **Exponentialbewertung** von R.

Beispiel 2.2.2 *Die in den Beispielen 2.1.2 (ii) und (iii) jeweils definierte Funktion λ ist eine Exponentialbewertung von $\mathbb{Z}$ beziehungsweise $\mathfrak{o}_{\mathcal{F}}$. Man nennt sie entsprechend die p-adische oder $\mathfrak{p}$-adische Bewertung und bezeichnet sie gewöhnlich mit v_p oder $v_{\mathfrak{p}}$.*

Aus Satz 2.2.1 folgt, daß zwei Exponentialbewertungen äquivalent sind, wenn sie sich nur um einen positiven, konstanten Faktor unterscheiden. Ein Primteiler, in Exponentialbewertungen notiert, ist also die Menge $\tilde{P} = \{cv \mid c \in \mathbb{R}^{>0}\}$. Da aus dem Kontext und der Schreibweise zu erkennen ist, ob wir es mit Bewertungen oder Exponentialbewertungen zu tun haben, bezeichnen wir wieder den Primteiler mit P statt mit $\tilde{P}$.

Gilt für ein $v \in P$, daß $v(R \backslash \{\alpha \in R \mid v(\alpha) \neq \infty\})$ eine diskrete Menge ist, so heißt P **diskreter Primteiler** von R. Für diskrete Primteiler läßt sich eine kanonische Exponentialbewertung $v \in P$ auswählen. Gilt $v(R \backslash \{\alpha \in R \mid v(\alpha) \neq \infty\}) = \mathbb{Z}$, so heißt v **normalisierte** Exponentialbewertung von P.

Weitere Aussagen und Beweise werden in [Ar, Na, Po/Za, We] gegeben.

2.3 Fortsetzungen von Bewertungen

Eine der zentralen Fragestellungen der Bewertungstheorie ist die Fortsetzung von Bewertungen auf einen Oberring. Seien ψ und φ Bewertungen auf S beziehungsweise R. ψ heißt eine Fortsetzung von φ auf S, falls

$$\psi|_R = \varphi$$

gilt. Betrachten wir wieder Klassen von äquivalenten nichtarchimedischen Bewertungen, so ist klar, was unter der Fortsetzung eines Primteilers zu verstehen ist.

Die Lösung des allgemeinen Problems der Fortsetzbarkeit einer nichtarchimedischen Bewertung von R auf S leistet für uns folgender Satz aus [Po/Za] Seite 245.

Satz 2.3.1 *Jede verallgemeinerte, nichtarchimedische Bewertung φ von R läßt sich auf den unitären Oberring S fortsetzen, falls*

$$I(\varphi, 0)S \cap R = I(\varphi, 0)$$

gilt.

Wir können also insbesondere jede Bewertung von R auf S fortsetzen, denn für Bewertungen ist $I(\varphi, 0) = \{0\}$. Die Möglichkeiten der Fortsetzung einer Bewertung eines algebraischen Zahlkörpers auf eine endliche Erweiterung wollen wir noch genauer beschreiben.

Fortsetzung von Bewertungen in algebraischen Zahlkörpern

Satz 2.3.2 *Sei $\mathcal{F}$ ein algebraischer Zahlkörper, dann ist jede nicht triviale Bewertung von $\mathcal{F}$ entweder diskret oder archimedisch.*

Falls die Bewertung φ archimedisch ist, so existiert ein $\mathbb{Q}$-Isomorphismus σ von $\mathcal{F}$ in $\mathbb{C}$ mit $\varphi(\alpha) = |\sigma(\alpha)|$ wobei $|\cdot|$ der absolute Betrag auf $\mathbb{C}$ ist.

Beweis: Siehe [Na].

Die nichtarchimedischen Bewertungen eines algebraischen Zahlkörpers sind also diskret. Alle diskreten Bewertungen werden durch den folgenden Satz charakterisiert.

Satz 2.3.3 *Sei $\mathcal{F}$ ein algebraischer Zahlkörper und P ein diskreter Primteiler. Dann existiert ein Primideal $\mathfrak{p}$ von $\mathfrak{o}_{\mathcal{F}}$ mit*

$$v_{\mathfrak{p}} \in P.$$

Beweis: Siehe [Na].

Damit haben wir also alle Bewertungen auf einem algebraischen Zahlkörper beschrieben.

Wie schon erwähnt, ist die Maximalordnung $\mathfrak{o}_{\mathcal{F}}$ von $\mathcal{F}$ ein Dedekindring. Jedes Primideal $\mathfrak{p}$ von $\mathfrak{o}_{\mathcal{F}}$ enthält genau eine Primzahl p. Damit kann die $\mathfrak{p}$-adische Bewertung von $\mathcal{F}$ nur eine Fortsetzung der p-adischen Bewertung von $\mathbb{Q}$ sein. Sei $\mathfrak{p}_1^{e_1} \cdot \ldots \cdot \mathfrak{p}_r^{e_r}$ die eindeutige Zerlegung des Hauptideals $p\mathfrak{o}_{\mathcal{F}}$ in Primideale. Dann hat die p-adische Bewertung von $\mathbb{Q}$ genau die r nicht äquivalenten Bewertungsfortsetzungen $v_{\mathfrak{p}_1}, \ldots, v_{\mathfrak{p}_r}$ auf $\mathcal{F}$.

Beispiel 2.3.4 *Sei $\mathcal{F} = \mathbb{Q}(\rho)$ mit $\rho^2 - 13 = 0$, so ist $\mathfrak{o}_{\mathcal{F}} = \mathbb{Z} + \frac{1+\rho}{2}\mathbb{Z}$. Wie zerlegt sich nun das Hauptideal $3\mathfrak{o}_f$? 3 teilt nicht 13, das heißt, 3 ist nicht verzweigt in $\mathcal{F}$. Wegen $1^2 \equiv 13 \mod 3$ ist 13 ein Quadrat modulo 3 und somit zerlegt in $\mathcal{F}$. Über 3 liegen also zwei Primideale $\mathfrak{p}_1 \neq \mathfrak{p}_2$ von $\mathfrak{o}_{\mathcal{F}}$. Entsprechend Satz 2.3.3 gibt es genau die zwei nichtäquivalenten Fortsetzungen $v_{\mathfrak{p}_1}$ und $v_{\mathfrak{p}_2}$ der 3-adischen Bewertung von $\mathbb{Q}$ auf $\mathcal{F}$.*

Der Durchschnitt aller Primideale einer Ordnung $\mathfrak{o}$ von $\mathcal{A}_f$ über p wird später noch von Bedeutung sein, er heißt das p-**Radikal** von $\mathfrak{o}$, geschrieben $\mathcal{J}_p(\mathfrak{o})$. Für das p-Radikal der Maximalordnung wollen wir statt $\mathcal{J}_p(\mathfrak{o}_f)$ auch das Symbol $\mathcal{J}_p(\mathcal{A}_f)$ oder kürzer $\mathcal{J}_p$ benutzen, sofern aus dem Kontext zu erkennen ist, welche Algebra gemeint ist. Auf Grund der Maximalitätseigenschaft von $\mathfrak{o}_f$ erhalten wir für eine beliebige Ordnung $\mathfrak{o}$ von $\mathcal{A}_f$ die Beziehung $\mathcal{J}_p(\mathfrak{o}) = \mathcal{J}_p \cap \mathfrak{o}$.

2.4 Der Ganze Abschluß

Wir haben jetzt alle Voraussetzungen, um die angekündigte Beschreibung „ganzer Elemente“ einer Algebra $\mathcal{A}_f$ aus bewertungstheoretischer Sicht zu entwickeln. Als erstes werden wir definieren, was bewertungstheoretisch ein über einem Ring R ganzes Element ist. Danach zeigen wir, daß die über R ganzen Elemente der Algebra $\mathcal{A}_f$ genau die über R ganzalgebraischen Elemente von $\mathcal{A}_f$ sind. Diese neue Charakterisierung von ganzen Elementen liegt der Idee der „Suche“ nach einer Ganzheitsbasis zu Grunde, die von dem zu beschreibenden Algorithmus ausgeführt wird.

Definition 2.4.1 *Sei S/R eine unitäre Ringerweiterung. Den Durchschnitt aller verallgemeinerten Bewertungsringe von S, die R enthalten, bezeichnet man als*

den **ganzen Abschluß** *von R in S geschrieben $Cl(R,S)$.*
Die Elemente aus $Cl(R,S)$ heißen **ganz über** *R.*

Der ganze Abschluß besitzt damit die folgenden, schon vom Namen her erwarteten, Eigenschaften

- $Cl(Cl(R,S),S) = Cl(R,S)$
- $Cl(R_1,S) \subseteq Cl(R_2,S)$ für $R_1 \subseteq R_2 \subseteq S$
- $Cl(R,S_1) \subseteq Cl(R,S_2)$ für $R \subseteq S_1 \subseteq S_2$.

Beispiel 2.4.2 *Sei S der Körper $\mathbb{Q}$ der rationalen Zahlen und $R = \mathbb{Z}'$ die p-Lokalisierung von $\mathbb{Z}$ für eine beliebige Primzahl p. Die p-adische Bewertung von $\mathbb{Q}$ ist eine Bewertung, deren Bewertungsring gleich $\mathbb{Z}'$ ist. Damit ist der ganze Abschluß von $\mathbb{Z}'$ in $\mathbb{Q}$ gleich $\mathbb{Z}'$.*

Satz 2.4.3 *Seien S_1/R_1 und S_2/R_2 unitäre Ringerweiterungen, so gilt für den ganzen Abschluß der direkten Summe*

$$Cl(R_1 \oplus R_2, S_1 \oplus S_2) = Cl(R_1,S_1) \oplus Cl(R_2,S_2).$$

Beweis: Wir zeigen zunächst die Inklusion „$\subseteq$“.
Sei $\alpha_1 \oplus \alpha_2 \in Cl(R_1 \oplus R_2, S_1 \oplus S_2)$. Nehmen wir an, daß α_1 nicht in $Cl(R_1,S_1)$ liegt, so muß es eine verallgemeinerte Bewertung φ_1 von S_1 geben, deren Bewertungsring R_1 enthält, mit

$$\varphi_1(\alpha_1) > 1.$$

Setzen wir nun $\varphi(x_1 \oplus x_2) := \varphi_1(x_1)$, so ist φ eine verallgemeinerte Bewertung von $S_1 \oplus S_2$, deren Bewertungsring $R_1 \oplus R_2$ enthält. Für $\alpha_1 \oplus \alpha_2$ gilt damit

$$\varphi(\alpha_1 \oplus \alpha_2) = \varphi_1(\alpha_1) > 1,$$

was der Voraussetzung $\alpha_1 \oplus \alpha_2 \in Cl(R_1 \oplus R_2, S_1 \oplus S_2)$ widerspricht. Unsere Annahme ist also falsch, α_1 muß in $Cl(R_1,S_1)$ liegen. Analog folgt, daß α_2 in $Cl(R_2,S_2)$ liegt, womit die Inklusion gezeigt ist.

Für die umgekehrte Inklusion nehmen wir an, daß α_i in $Cl(R_i,S_i)$ für $i \in \{1,2\}$ und $\alpha_1 \oplus \alpha_2$ nicht in $Cl(R_1 \oplus R_2, S_1 \oplus S_2)$ liegt. Es existiert wieder eine verallgemeinerte Bewertung φ, diesmal von $S_1 \oplus S_2$ mit

$$\varphi(\alpha_1 \oplus \alpha_2) > 1.$$

Dann liegt $\alpha_1 \oplus 0$ oder $0 \oplus \alpha_2$ nicht in $Cl(R_1 \oplus R_2, S_1 \oplus S_2)$. Ohne Einschränkung liege $\alpha_1 \oplus 0$ nicht in $Cl(R_1 \oplus R_2, S_1 \oplus S_2)$. Setzen wir nun $\varphi_1(x) := \varphi(x \oplus 0)$, so ist φ_1 eine verallgemeinerte Bewertung von S_1, deren Bewertungsring R_1 enthält. Denn der Bewertungsring von φ enthält $R_1 \oplus \{0\}$. Für α_1 gilt damit

$$\varphi_1(\alpha_1) = \varphi(\alpha_1 \oplus 0) > 1,$$

was der Voraussetzung $\alpha_1 \in Cl(R_1, S_1)$ widerspricht. Unsere Annahme ist also falsch, und $\alpha_1 \oplus \alpha_2$ muß in $Cl(R_1 \oplus R_2, S_1 \oplus S_2)$ liegen. □

Beispiel 2.4.4 *Seien S_1 und S_2 gleich dem Körper der rationalen Zahlen und R_1 beziehungsweise R_2 die Lokalisierungen von $\mathbb{Z}$ nach p und q. Dabei seien p und q zwei beliebige Primzahlen. So ist der ganze Abschluß von $R_1 \oplus R_2$ in $S_1 \oplus S_2$ nach Beispiel 2.4.2 gleich $R_1 \oplus R_2$.*

Satz 2.4.5 *Seien S_1/R und S_2/R unitäre Ringerweiterungen, so gilt für den ganzen Abschluß der Einbettung $D = \{r \oplus r \mid r \in R\}$ von R in die direkte Summe von S_1 und S_2*

$$Cl(D, S_1 \oplus S_2) = Cl(R, S_1) \oplus Cl(R, S_2).$$

Beweis: Auf Grund der Eigenschaften des ganzen Abschlusses und der Aussage von Satz 2.4.3 genügt es zu zeigen, daß der Bewertungsring jeder verallgemeinerten Bewertung φ von $S_1 \oplus S_2$ mit D auch die direkte Summe $R \oplus R$ enthält. Dazu müssen wir nur zeigen, daß die Elemente $1 \oplus 0$ und $0 \oplus 1$ im Bewertungsring von φ liegen, sie also durch φ auf einen Wert kleiner gleich Eins abgebildet werden.

Zunächst stellen wir fest, daß wegen $0 = \varphi(0 \oplus 0) = \varphi(1 \oplus 0)\varphi(0 \oplus 1)$ eines der Elemente $1 \oplus 0$ beziehungsweise $0 \oplus 1$ durch φ auf Null abgebildet wird. Betrachten wir die Ungleichungen $0 \leq \varphi(1 \oplus 1) = \varphi(1 \oplus 0 \, + \, 0 \oplus 1) \leq \max\{\varphi(1 \oplus 0), \varphi(0 \oplus 1)\}$. Wir wissen, daß einer der beiden Terme, von denen das Maximum bestimmt wird, gleich Null ist. Weiterhin ist auf Grund der Eigenschaften von verallgemeinerten nichtarchimedischen Bewertungen $\varphi(1 \oplus 0 \; + \; 0 \oplus 1)$ gleich dem Maximum der Bewertungen der Summanden, wenn diese verschieden sind. Der Fall, daß die Bewertungen gleich sind, ist trivial, da dann beide die Bewertung Null haben und somit im Bewertungsring von φ liegen. Nehmen wir also an, die Bewertungen von $1 \oplus 0$ und $0 \oplus 1$ sind verschieden. Dann erhalten wir wegen der Voraussetzung $\varphi(1 \oplus 0 \, + \, 0 \oplus 1) = \varphi(1 \oplus 1) \leq 1$, daß wiederum beide Summanden eine Bewertung kleiner oder gleich Eins haben und damit im Bewertungsring von φ liegen. □

Wir wollen statt $Cl(D, S_1 \oplus S_2)$ die etwas ungenaue, aber verständlichere Notation $Cl(R, S_1 \oplus S_2)$ verwenden.

Definition 2.4.6 *Ein Integritätsring R heißt* **ganz abgeschlossen**, *wenn in dem Quotientenkörper $\mathcal{Q}(R)$ gilt: $R = Cl(R, \mathcal{Q}(R))$.*

Beispiel 2.4.7 *$\mathbb{Z}$ und $\mathbb{Z}'$ sind in $\mathbb{Q}$ ganz abgeschlossen.*

Wir haben nun den bewertungstheoretisch motivierten Begriff des über R ganzen Elements für unitäre Ringerweiterungen eingeführt. Uns interessieren die Beziehungen zwischen den „bewertungstheoretisch-“ und den „algebraisch-“ganzen Elementen.

Satz 2.4.8 *Sei S/R eine unitäre Ringerweiterung. Dann liegt jedes über R ganzalgebraische Element in dem ganzen Abschluß $Cl(R, S)$ von R in S.*

Beweis: Sei $\alpha \in S$ mit $\alpha^n + \sum_{i=1}^n a_i\alpha^{n-i} = 0$, wobei $a_i \in R$, also α ganzalgebraisch über R ist. $\varphi : S \longrightarrow \mathbb{R}$ sei eine beliebige verallgemeinerte Bewertung deren Bewertungsring R enthält. So gilt

$$\begin{aligned}
\varphi(\alpha)^n &= \varphi(\alpha^n) = \varphi(-\sum_{i=1}^n a_i\alpha^{n-i}) \\
&\leq \max_{i\in\{1,\dots,n\}} \varphi(-a_i\alpha^{n-i}) \\
&= \max_{i\in\{1,\dots,n\}} \varphi(-a_i)\varphi(\alpha^{n-i}) \\
&\leq \max_{i\in\{1,\dots,n\}} \varphi(\alpha)^{n-i},
\end{aligned}$$

da $a_i \in R \subseteq I(\varphi, 1)$. Für alle $i \in \{1, \dots, n\}$ gilt somit die Ungleichung $\varphi(\alpha)^n \leq \varphi(\alpha)^{n-i}$, was nur für $\varphi(\alpha) \leq 1$ gelten kann. α liegt also im Bewertungsring von φ. □

Satz 2.4.9 *Sei S ein Integritätsring, dann ist jedes Element aus $Cl(R, S)$ ganzalgebraisch über R.*

Beweis: Zunächst wollen wir den Quotientenkörper von S mit $\mathcal{F}$ bezeichnen. Sei $\alpha \in Cl(R, S)\backslash\{0\}$ beliebig. Dann gilt für jede verallgemeinerte Bewertung $\varphi : S \longrightarrow \mathbb{R}$, deren Bewertungsring R enthält, $\varphi(\alpha) \leq 1$. Betrachten wir nun den unitären Teilring $R[\alpha^{-1}]$ von $\mathcal{F}$. Sei $\mathfrak{a} := \alpha^{-1}R[\alpha^{-1}] = \sum_{i=1}^\infty R\alpha^{-i}$ das von α^{-1} erzeugte Hauptideal in $R[\alpha^{-1}]$. Für den Fall, daß die Eins in $\mathfrak{a}$ liegt, ist wegen

$$\begin{aligned}
1 &= \sum_{i=1}^m a_i\alpha^{-i} \\
\alpha^m &= \sum_{i=1}^m a_i\alpha^{m-i} \\
0 &= \alpha^m + \sum_{i=1}^m -a_i\alpha^{m-i}
\end{aligned}$$

α Nullstelle eines normierten Polynoms aus $R[t]$ und damit ganz über R.

Wir werden nun zeigen, daß die Eins immer in $\mathfrak{a}$ liegen muß und somit α ganzalgebraisch über R ist. Nehmen wir an, daß die Eins nicht im Ideal $\mathfrak{a}$ liegt, so ist $\mathfrak{a}$ ein echtes Ideal von $R[\alpha^{-1}]$ und somit in einem maximalen Ideal $\mathfrak{M}$ von $R[\alpha^{-1}]$ enthalten. Die Idee ist, zu zeigen, daß es eine Bewertung $\tilde{\varphi}$ von $\mathcal{F}$ gibt, deren Bewertungsring R und ein Ideal $\tilde{\mathfrak{P}}$ mit

$$\mathfrak{M} = \tilde{\mathfrak{P}} \cap R[\alpha^{-1}]$$

enthält. Dann erhalten wir, daß α^{-1} in $\mathfrak{M}$ liegt und wegen obiger Gleichheit auch im Bewertungsideal von $\tilde{\varphi}$. Da der Bewertungsring von $\tilde{\varphi}$ eine Obermenge des Ringes R ist, muß er auch das über R ganze Element α enthalten. Wir stoßen damit auf den Widerspruch, daß einerseits $\tilde{\varphi}(\alpha)$ kleiner gleich Eins sein muß und andererseits wegen $\alpha^{-1} \in \tilde{\mathfrak{P}} \Rightarrow \tilde{\varphi}(\alpha)^{-1} = \tilde{\varphi}(\alpha^{-1}) < 1$ auch echt größer als Eins sein muß. Die Annahme, daß die Eins nicht im Ideal $\mathfrak{a}$ liegt, ist somit falsch. Daß diese Idee realisierbar ist, werden wir in Lemma 2.4.11 zeigen. $\square$

Um den Beweis des Lemmas 2.4.11 zu vereinfachen, zeigen wir, daß es genügt, lokale Ringe zu betrachten.

Lemma 2.4.10 *$\mathcal{F}/R$ sei eine unitäre Ringerweiterung, wobei $\mathcal{F}$ einen Körper bezeichne. $\mathfrak{p}$ sei ein beliebiges Primideal von R und R' die Lokalisierung von R nach $\mathfrak{p}$. $\tilde{\varphi}$ sei eine Bewertung auf $\mathcal{F}$, für deren Bewertungsideal $\tilde{\mathfrak{P}}$ gilt*

$$\tilde{\mathfrak{P}} \cap R' = \frac{\mathfrak{p}}{R \backslash \mathfrak{p}}.$$

Dann schneidet das Bewertungsideal $\tilde{\mathfrak{P}}$ von $\tilde{\varphi}$ den Ring R in $\mathfrak{p}$

$$\tilde{\mathfrak{P}} \cap R = \mathfrak{p}.$$

Beweis: Wir zeigen zunächst die Inklusion „$\supseteq$“. Sei α aus $\mathfrak{p}$ beliebig. Dann liegt α insbesondere in dem von $\mathfrak{p}$ in der $\mathfrak{p}$-Lokalisierung von R erzeugten Primideal. Nach der Voraussetzung an das Bewertungsideal von $\tilde{\varphi}$ ist α somit aus $\tilde{\mathfrak{P}} \cap R'$. Daraus folgt die gewünschte Inklusion wegen $\mathfrak{p} \subset R$.

Für die umgekehrte Inklusion sei α aus $\tilde{\mathfrak{P}} \cap R$ beliebig. Dann liegt α insbesondere in $\tilde{\mathfrak{P}} \cap R' \cap R$ und damit wegen der Voraussetzung an $\tilde{\mathfrak{P}}$ in $\frac{\mathfrak{p}}{R \backslash \mathfrak{p}} \cap R$. Nach Satz 1.2.1 gilt $\frac{\mathfrak{p}}{R \backslash \mathfrak{p}} \cap R = \mathfrak{p}$, da $\mathfrak{p}$ ein Primideal von R ist. Somit liegt α auch in $\mathfrak{p}$. $\square$

Lemma 2.4.11 *$\mathcal{F}/R$ sei eine unitäre Ringerweiterung und $\mathcal{F}$ wieder ein Körper. $\mathfrak{M}$ sei ein maximales Ideal von R. Dann existiert eine Bewertung $\tilde{\varphi}$ von $\mathcal{F}$, deren Bewertungsring R enthält, so daß für das Bewertungsideal $\tilde{\mathfrak{P}}$ von $\tilde{\varphi}$ gilt*

$$\tilde{\mathfrak{P}} \cap R = \mathfrak{M}.$$

Beweis: Sei zunächst R ein lokaler Ring. Betrachten wir die unitären Ringe $\tilde{I}$ über R in $\mathcal{F}$ mit der Eigenschaft $1 \notin \mathfrak{M}\tilde{I}$. Sie bilden bezüglich der Inklusion eine induktiv geordnete Menge, denn die Vereinigung aller Ringe einer Kette ist ein Ring $\hat{I}$, wobei die Eins nicht in $\mathfrak{M}\hat{I}$ liegt. $\hat{I}$ ist somit eine obere Schranke. Nach dem Lemma von Zorn existiert also ein maximales Element I.

Für I gilt dann, $\mathfrak{M}I$ enthält nicht die Eins und ist somit in einem maximalen Ideal $\mathfrak{p}$ von I enthalten. $\mathfrak{p}$ enthält ebenfalls nicht die Eins, und es gilt nach Satz 1.2.1

$$\mathfrak{p} = I \cap \frac{\mathfrak{p}}{I\backslash\mathfrak{p}} \supseteq I \cap \mathfrak{M}\frac{I}{I\backslash\mathfrak{p}}.$$

Das heißt, $\mathfrak{M}\frac{I}{I\backslash\mathfrak{p}}$ enthält nicht die Eins, denn I ist ein unitärer Ring, die Eins würde im Durchschnitt und damit auch in $\mathfrak{p}$ liegen. Auf Grund der Maximalitätseigenschaft von I muß somit I mit seiner $\mathfrak{p}$-Lokalisierung $\frac{I}{I\backslash\mathfrak{p}}$ übereinstimmen. I ist also ein lokaler Ring, und $\mathfrak{p}$ ist sein eindeutiges maximales Ideal. Sei $\tilde{\varphi}$ eine Fortsetzung der $\mathfrak{p}$-adischen Bewertung von I auf $\mathcal{F}$. Dann enthält der Bewertungsring von $\tilde{\varphi}$ den Ring R, und für das Bewertungsideal $\tilde{\mathfrak{P}}$ von $\tilde{\varphi}$ gilt

$$\tilde{\mathfrak{P}} \cap R = \mathfrak{p} \cap R = \mathfrak{M},$$

da der Durchschnitt von $\mathfrak{p}$ und R nicht die Eins enthält. $\mathfrak{p} \cap R$ ist somit ein echtes Ideal von R, welches in dem maximalen Ideal $\mathfrak{M}$ von R liegt. Andererseits ist wegen $\mathfrak{M}I \subseteq \mathfrak{p} \subseteq \tilde{\mathfrak{P}}$ auch $\mathfrak{M}$ Teilmenge von $\tilde{\mathfrak{P}}$. Für lokale Ringe haben wir das Lemma also gezeigt.

Betrachten wir nun den Fall eines beliebigen unitären Ringes R. Sei R' die Lokalisierung von R nach $\mathfrak{M}$. Dann existiert nach dem eben Gezeigten eine Bewertung $\tilde{\varphi}$ von $\mathcal{F}$, für deren Bewertungsideal $\tilde{\mathfrak{P}}$ gilt

$$\tilde{\mathfrak{P}} \cap R' = \frac{\mathfrak{M}}{R\backslash\mathfrak{M}}.$$

Nach Lemma 2.4.10 schneidet dann $\tilde{\mathfrak{P}}$ den Ring R in $\mathfrak{M}$. $\square$

Die verbliebene Lücke im Beweis von Satz 2.4.9 ist damit geschlossen.

Wir haben also die Äquivalenz der „bewertungstheoretisch“ und der „algebraisch“ motivierten Definition eines über einem Ring R ganzen Elements aus

S, für den Fall, daß S ein Integritätsring ist, gezeigt. Als letztes bleibt uns die Äquivalenz für den allgemeinen Fall, daß S eine Algebra $\mathcal{A}_f$ ist, zu zeigen. Die Schlüssel dazu sind die Sätze 2.4.5 und 1.3.8. Denn wie schon in Abschnitt 1.3 erwähnt, ist unsere Algebra $\mathcal{A}_f$ nach dem chinesischen Restsatz isomorph zur direkten Summe $\bigoplus_{i=1}^r \mathcal{A}_{f_i}$ von Körpern $\mathcal{A}_{f_i}$. Nach Satz 2.4.5 gilt für die direkte Summe: $Cl(R, \bigoplus_{i=1}^r \mathcal{A}_{f_i}) = \bigoplus_{i=1}^r Cl(R, \mathcal{A}_{f_i})$. Für die Summanden haben wir aber schon die Äquivalenz gezeigt, das heißt, es gilt $Cl(R, \mathcal{A}_{f_i}) = \{\alpha \in \mathcal{A}_{f_i} \mid \alpha \text{ ist ganzalgebraisch über } R\}$. Analog Satz 1.3.8 ist α genau dann ganzalgebraisch über R, wenn die α_i ganzalgebraisch über R sind, wobei α_i das Bild von α in $\mathcal{A}_{f_i}$ unter dem $\mathbb{Q}$-Isomorphismus von $\mathcal{A}_f$ nach $\bigoplus_{i=1}^r \mathcal{A}_{f_i}$ aus Lemma 1.3.4 ist. Wir haben also folgenden Satz gezeigt.

Satz 2.4.12 *Sei $\mathcal{A}_f/R$ eine unitäre Ringerweiterung und R ein faktorieller Teilring von $\mathbb{Q}$. Dann sind die über R ganzalgebraischen Elemente von $\mathcal{A}_f$ genau die über R ganzen Elemente.*

2.5 Die v_p^*-Bewertung

Am Ende dieses Kapitels soll noch eine spezielle Funktion betrachtet werden.

Definition 2.5.1 *Sei $f \in \mathbb{Z}[t]$ ein normiertes, separables Polynom. Für $\alpha \in \mathcal{A}_f$ definiere*

$$v_p^*(\alpha) := \min_{i \in \{1,\dots,r\}} v_p^{(i)}(\alpha),$$

wobei $v_p^{(i)}$ die nicht äquivalenten Bewertungsfortsetzungen der p-adischen Bewertung v_p von $\mathbb{Q}$ auf $\mathcal{A}_f$ seien.

Aus der Definition und den Eigenschaften von verallgemeinerten Bewertungen ergibt sich für v_p^*

- $v_p^*(\alpha + \beta) \geq \min\{v_p^*(\alpha), v_p^*(\beta)\}$
- $v_p^*(\alpha + \beta) = \min\{v_p^*(\alpha), v_p^*(\beta)\}$ für $v_p^*(\alpha) \neq v_p^*(\beta)$
- $v_p^*(\alpha\beta) \geq v_p^*(\alpha) + v_p^*(\beta)$
- $v_p^*(\alpha^n) = n v_p^*(\alpha)$ für $n \in \mathbb{N}$.

Die v_p^*-Bewertung wird für uns interessant, da sie mit Hilfe des charakteristischen Polynoms von α berechnet werden kann und einige wichtige Eigenschaften des Elements durch sie beschrieben werden.

Satz 2.5.2 *Sei $\alpha \in \mathfrak{o}_f \backslash \{0\}$. Das charakteristische Polynom von α habe die Darstellung $\chi_\alpha(x) = x^n + c_1 x^{n-1} + \ldots + c_n$. Dann gilt*

$$v_p^*(\alpha) = \min_{i \in \{1,\ldots,n\}} \frac{v_p(c_i)}{i}.$$

Beweis: Ein Beweis findet sich in [We] beziehungsweise anderen Werken über algebraische Zahlentheorie unter dem Stichwort „Newton Polygon“.

Mit Hilfe der v_p^*-Bewertung läßt sich auch das p-Radikal von $\mathfrak{o}_f$ leicht beschreiben:

$$\mathcal{J}_p = \{\alpha \in \mathcal{A}_f \mid v_p^*(\alpha) > 0\}.$$

Kapitel 3

Lokalisierung

Der erste Schritt, die komplexe Aufgabenstellung zu reduzieren, basiert auf folgender Beobachtung. Sei $\mathcal{R} \subseteq \mathfrak{o}_f$ eine Ordnung, so gilt

$$\mathrm{d}(\mathcal{R}) = [\mathfrak{o}_f : \mathcal{R}]^2 \mathrm{d}(\mathfrak{o}_f).$$

Teilt eine Primzahl p den Index von $\mathcal{R}$ in der Maximalordnung, so muß p^2 die Diskriminante von $\mathcal{R}$ teilen. Es liegt also nahe, eine Ordnung $\mathcal{R} \subseteq \mathfrak{o}_f$ **p-maximal** zu nennen, wenn p nicht den Index von $\mathcal{R}$ in $\mathfrak{o}_f$ teilt. $\mathcal{R}$ ist somit gleich der Maximalordnung, wenn $\mathcal{R}$ p-maximal für alle Primzahlen p ist, welche quadratisch in der Diskriminante von $\mathcal{R}$ aufgehen — bezüglich der verbliebenen Primzahlen p ist $\mathcal{R}$ in jedem Fall p-maximal — Zu einer beliebigen Ordnung $\mathcal{R} \subseteq \mathfrak{o}_f$ bezeichnen wir mit $\mathcal{R}^p$ die Ordnung mit den Eigenschaften

- $\mathcal{R} \subseteq \mathcal{R}^p \subseteq \mathfrak{o}_f$
- $[\mathcal{R}^p : \mathcal{R}] = p$-Potenz
- $p \not| [\mathfrak{o}_f : \mathcal{R}^p]$.

$\mathcal{R}^p$ heißt **p-Maximalordnung** über $\mathcal{R}$. Für $\mathcal{R}^p$ gilt

$$\mathcal{R}^p = \{a \in \mathfrak{o}_f \mid \exists k \in \mathbb{N} : p^k a \in \mathcal{R}\}.$$

Per Definition einer Ordnung von $\mathcal{A}_f$ sind $\mathfrak{o}_f$ und $\mathcal{R}$ $\mathbb{Z}$-Moduln vom Rang n. Der Faktor $\mathfrak{o}_f/\mathcal{R}$ ist also ein endlicher $\mathbb{Z}$-Modul und somit ein Torsionsmodul. Nach dem Struktursatz über Torsionsmoduln ist $\mathfrak{o}_f/\mathcal{R}$ die direkte Summe seiner p-Komponenten

$$\mathfrak{o}_f/\mathcal{R} = \bigoplus_{p \mid [\mathfrak{o}_f : \mathcal{R}]} M_p,$$

dabei sind die p-Komponenten M_p von $\mathfrak{o}_f/\mathcal{R}$ definiert als

$$M_p = \{a \in \mathfrak{o}_f/\mathcal{R} \mid \exists k \in \mathbb{N} : p^k a = 0\}.$$

Die p-Komponenten von $\mathfrak{o}_f/\mathcal{R}$ sind also die Faktoren $\mathcal{R}^p/\mathcal{R}$. Die Maximalordnung von $\mathcal{A}_f$ ist somit gleich der Summe der p-Maximalordnungen von $\mathcal{R}$

$$\mathfrak{o}_f = \sum_{p \in \mathbb{P}_{\mathcal{R}}} \mathcal{R}^p$$

mit $\mathbb{P}_{\mathcal{R}} := \{p \in \mathbb{P} \mid p^2 | \mathrm{d}(\mathcal{R})\}$. Daher genügt es, die p-Maximalordnungen für alle $p \in \mathbb{P}_{\mathcal{R}}$ zu berechnen. $\mathfrak{o}_f$ als Modulsumme läßt sich daraus leicht unter Verwendung der Hermiteschen Normalform erzeugen. Dazu verwende man den modularen Algorithmus mit der in Abschnitt 3.2 entwickelten reduzierten Diskriminante von $\mathcal{R}$ als Modulerzeuger. Zur algorithmischen Repräsentation von endlich erzeugten Moduln siehe [Co].

Betrachten wir den ganzen Abschluß der p-Lokalisierung $\mathbb{Z}'$ von $\mathbb{Z}$, so erhalten wir die Beziehung

$$Cl(\mathbb{Z}', \mathcal{A}_f) = \mathbb{Z}'\mathcal{R}^p = \mathbb{Z}'\mathfrak{o}_f = \mathfrak{o}'_f$$

für eine beliebige Ordnung $\mathcal{R}$ von $\mathcal{A}_f$, wobei $\mathfrak{o}'_f$ den Quotientenring von $\mathfrak{o}_f$ nach $\mathbb{Z}'\backslash p\mathbb{Z}$ bezeichne. $\mathcal{R}^p$ ergibt sich somit als der Durchschnitt von $Cl(\mathbb{Z}', \mathcal{A}_f)$ und $\frac{1}{p^\kappa}\mathcal{R}$, wobei wegen $[\mathfrak{o}'_f : \mathcal{R}] \mid \mathrm{d}(\mathcal{R})$ zum Beispiel $\kappa = v_p(\mathrm{d}(\mathcal{R}))$ gewählt werden kann. Wir können also aus einer $\mathbb{Z}'$-Basis von $Cl(\mathbb{Z}', \mathcal{A}_f)$ eine $\mathbb{Z}$-Basis von $\mathcal{R}^p$ durch Multiplikation mit Einheiten aus $\mathbb{Z}'$ gewinnen. Es genügt damit einen Algorithmus für den lokalen Fall zu beschreiben.

Im folgenden sei p eine fest gewählte Primzahl, die quadratisch in der Diskriminante von f aufgeht. Im ganzen Kapitel wird die Quotientenringbildung nach der multiplikativen Gruppe $\mathbb{Z}\backslash p\mathbb{Z}$ durch den Index „ $'$ “ gekennzeichnet. Unter einer Ordnung werden wir im weiteren eine $\mathbb{Z}'$-Ordnung verstehen. Wir beschreiben jetzt in drei Schritten einen Algorithmus, welcher eine $\mathbb{Z}'$-Basis des ganzen Abschlusses von $\mathbb{Z}'$ in $\mathcal{A}_f$ berechnet.

3.1 Die Geichungsordnung ist maximal

Zuerst soll der Fall, daß die Gleichungsordnung maximal ist, behandelt werden. Dazu gibt es ein einfaches Kriterium, das sogenannte Dedekind Kriterium.

3.1.1 Der Dedekind Test

Um den Notationsaufwand im Satz so gering wie möglich zu halten, wollen wir im voraus eine Konvention vereinbaren. Seien g und h zwei Polynome aus $\mathbb{Z}'[t]$ und $\bar{g}, \bar{h}$ die Bilder unter dem kanonischen Homomorphismus von $\mathbb{Z}'[t]$ nach $\mathbb{Z}'/p\mathbb{Z}'[t] = \mathbb{F}_p[t]$. Unter dem größten gemeinsamen Teiler $\mathrm{ggT}_p(g, h)$ von g und h modulo p wollen wir ein Lifting gleichen Grades des größten gemeinsamen Teilers der Polynome $\bar{g}$ und $\bar{h}$ von $\mathbb{F}_p[t]$ nach $\mathbb{Z}'[t]$ verstehen.

Satz 3.1.1 (Dedekind) *Seien f ein normiertes, separables Polynom aus $\mathbb{Z}'[t]$ und*

$$f \equiv gh \mod p\mathbb{Z}'[t]$$

eine Zerlegung von f in normierte Polynome g und h aus $\mathbb{Z}'[t]$, wobei g der quadratfreie Teiler maximalen Grades von f modulo p ist. Setze $\varphi := t + f(t)\mathbb{Q}[t]$ und

$$k := \mathrm{ggT}_p\left(\frac{f - gh}{p},\ g,\ h\right),$$

so ist die Gleichungsordnung $\mathbb{Z}'[\varphi]$ von φ genau dann maximal, wenn k eine Konstante ist.

Der Multiplikatorring $\mathfrak{o}' := [\mathcal{J}_p'(\mathbb{Z}'[\varphi])/\mathcal{J}_p'(\mathbb{Z}'[\varphi])]$ des p-Radikals der Gleichungsordnung von φ ist gleich $\mathbb{Z}'[\varphi] + \frac{l(\varphi)}{p}\mathbb{Z}'[\varphi]$, wobei $l(t)$ ein normiertes Polynom aus $\mathbb{Z}'[t]$ mit $lk \equiv f \mod p\mathbb{Z}'[t]$ ist. Der Index von $\mathbb{Z}'[\varphi]$ in dem Multiplikatorring $\mathfrak{o}'$ ist gleich p^m mit $m := \mathrm{Grad}(k)$ und somit $\mathrm{d}(\mathfrak{o}') = \frac{\mathrm{d}(f)}{p^{2m}}$.

Beweis: Satz und Beweis sind in dem Buch [Co] für $\mathbb{Z}$-Ordnungen algebraischer Zahlkörper aufgeführt. Eine genaue Analyse des Beweises ergibt jedoch, daß die Irreduzibilität von f an keiner Stelle in dem Beweis benötigt wird. Die Aussagen für den ganzen Abschluß der p-Lokalisierung von $\mathbb{Z}$ sind ein Spezialfall, da sich die Ergebnisse nur um Einheiten aus $\mathbb{Z}'$ unterscheiden.

Aus dem zweiten Teil des Satzes erhalten wir für spezielle Fälle eine Testmöglichkeit, mit der ermittelt werden kann, ob die Ordnung $\mathfrak{o}'$ maximal ist. Stellt sich heraus, daß in der Diskriminante von $\mathfrak{o}'$ unsere Primzahl p nicht mehr quadratisch aufgeht, das heißt, $v_p(\mathrm{d}(f)) - 1$ ist kleiner gleich $2m$, so muß der Multiplikatorring $\mathfrak{o}'$ maximal sein. Für diesen Fall müssen wir also nur noch eine $\mathbb{Z}'$-Basis der Modulsumme $\mathbb{Z}'[\varphi] + \frac{l(\varphi)}{p}\mathbb{Z}'[\varphi]$ bestimmen. Dazu muß keine Hermite Normalform einer $n \times 2n$ Matrix bestimmt werden, denn durch

$$1, \varphi, \ldots, \varphi^{n-(m+1)}, \frac{l(\varphi)}{p}, \frac{l(\varphi)}{p}\varphi, \ldots, \frac{l(\varphi)}{p}\varphi^{m-1}$$

ist uns eine $\mathbb{Z}'$-Basis des Multiplikatorringes $\mathfrak{o}'$ explizit gegeben. Sei $\mathcal{R}$ der durch das angegebene $\mathbb{Z}'$-Erzeugendensystem definierte $\mathbb{Z}'$-Modul. $\mathcal{R}$ ist sicherlich in der Modulsumme von $\mathbb{Z}'[\varphi]$ und $\frac{l(\varphi)}{p}\mathbb{Z}'[\varphi]$ enthalten. Wir werden zeigen, daß umgekehrt $\mathcal{R}$ die Moduln $\mathbb{Z}'[\varphi]$ und $\frac{l(\varphi)}{p}\mathbb{Z}'[\varphi]$ enthält. Sei i aus $\{0,\dots,m-1\}$ beliebig, so ist zu zeigen, daß φ^{n-m+i} in $\mathcal{R}$ liegt. Nach Konstruktion ist l ein normiertes Polynom über $\mathbb{Z}'$ vom Grad $n-m$, somit ist $p\,\frac{l(t)t^i}{p} - t^{n-m+i}$ ein Polynom über $\mathbb{Z}'$ vom Grad kleiner als $n-m+i$. Spezialisieren wir $t \mapsto \varphi$, so erhalten wir, daß φ^{n-m+i} in $\mathcal{R}$ liegt, wenn $1, \varphi, \dots, \varphi^{n-m+i-1}, \frac{l(\varphi)}{p}, \frac{l(\varphi)}{p}\varphi, \dots, \frac{l(\varphi)}{p}\varphi^{m-1}$ in $\mathcal{R}$ liegen. Für i gleich Null ist die Bedingung erfüllt, und wir erhalten induktiv die Behauptung, daß $\mathbb{Z}'[\varphi]$ in $\mathcal{R}$ enthalten ist. Analog zeigen wir, daß $\frac{l(\varphi)}{p}\varphi^{m+i}$ für i aus $\{0,\dots,n-(m+1)\}$ in dem Modul $\mathcal{R}$ liegt. Nach Konstruktion der normierten Polynome k und l gilt $f = kl + pr$ für ein Polynom r aus $\mathbb{Z}'[t]$. Daraus erhalten wir die Beziehung

$$\frac{l(t)t^{m+i} - f(t)}{p} \quad = \quad \frac{l(t)(t^{m+i} - k(t))}{p} + r(t).$$

Spezialisieren wir $t \mapsto \varphi$, so erhalten wir wegen $f(\varphi) = 0$, daß $\frac{l(\varphi)}{p}\varphi^{m+i}$ in $\mathcal{R}$ liegt, wenn $1, \varphi, \dots, \varphi^{n-1}, \frac{l(\varphi)}{p}\varphi, \dots, \frac{l(\varphi)}{p}\varphi^{m+i-1}$ in $\mathcal{R}$ liegen. Es folgt wieder induktiv die Behauptung und somit die Gleichheit $\mathcal{R} = \mathbb{Z}'[\varphi] + \frac{l(\varphi)}{p}\mathbb{Z}'[\varphi]$.

Um die Koeffizienten der Basiselemente für weitere Rechnungen zu reduzieren, berechnen wir eine modulare Hermite Normalform von der Koeffizientenmatrix der Elemente $p^\kappa(1, \varphi, \dots, \varphi^{n-(m+1)}, \frac{l(\varphi)}{p}, \frac{l(\varphi)}{p}\varphi, \dots, \frac{l(\varphi)}{p}\varphi^{m-1})$ bezüglich des Moduls $p^\kappa\mathbb{Z}'$. Für κ muß dabei gelten $p^\kappa\mathfrak{o}'_f \subseteq \mathbb{Z}'[\varphi]$, das ist zum Beispiel für $\kappa = v_p(\mathrm{d}(f))$ erfüllt. Vorgreifend auf den Abschnitt 3.2.2 wollen wir schon den Wert $v_p(\mathrm{d}_r(f))$ für κ im Algorithmus verwenden — $\mathrm{d}_r(f)$ ist die reduzierte Diskriminante von f —

Dieser Test ist besonders einfach algorithmisch zu realisieren und somit für unsere Zwecke gut geeignet.

3.1.2 Der Dedekindalgorithmus

Wir werden den Dedekindtest nur in einer speziellen Situation anwenden. Das Polynom f wird modulo p immer nur genau einen irreduziblen Faktor ν besitzen. Das heißt, wir wissen sofort, daß g gleich ν ist und h demzufolge ein normiertes Lifting von $\bar{f}/\bar{\nu}$, wobei $\bar{f}, \bar{\nu}$ die Bilder von f und ν unter dem kanonischen Homomorphismus von $\mathbb{Z}'[t]$ nach $\mathbb{Z}'/p\mathbb{Z}'[t]$ sind.

Algorithmus 3.1.2 *Dedekind Test*

Eingabe:

Es wird ein normiertes, separables Polynom f aus $\mathbb{Z}'[t]$ erwartet, welches modulo p genau einen irreduziblen Faktor g besitzt.

Ausgabe:

Es wird „wahr“ zurückgegeben, wenn die Gleichungsordnung $\mathcal{R}'_f$ oder wenn der Multiplikatorring des p-Radikals der Gleichungsordnung $\mathcal{R}'_f$ maximal ist. Im letzteren Fall wird außerdem das Polynom l aus dem Satz 3.1.1 für den Algorithmus 3.1.3 bereitgestellt.

In den anderen Fällen wird „falsch“ zurückgegeben.

1. Schritt: (Quotient)

Bestimme ein normiertes Polynom h aus $\mathbb{Z}'[t]$ mit $f \equiv gh \mod p\mathbb{Z}'[t]$.

2. Schritt: (ggT_p)

Setze

$$k \leftarrow \mathrm{ggT}_p(\frac{f-gh}{p},\ g,\ h).$$

3. Schritt: (Gleichungsordnung maximal?)

Wenn k eine Konstante ist, so terminiere mit „wahr“.

4. Schritt: (Multiplikatorring maximal?)

Wenn $v_p(\mathrm{d}(f)) \leq 2\,\mathrm{Grad}(k)-1$, so bestimme ein normiertes Polynom l mit $f \equiv lk \mod p\mathbb{Z}'[t]$ und terminiere mit „wahr“.

5. Schritt:

Terminiere mit „falsch“.

Algorithmus 3.1.3 *Dedekindbasis*

Eingabe:

Es wird ein normiertes, separables Polynom f aus $\mathbb{Z}'[t]$ und ein Element φ aus $\mathfrak{o}'_f$ mit $\mathbb{Q}(\varphi) = \mathcal{A}_f$ erwartet. Dabei ist entweder die Gleichungsordnung von φ oder der Multiplikatorring der Gleichungsordnung von φ maximal. Im letzteren Fall wird außerdem das Polynom l aus Algorithmus 3.1.2 benötigt — Das heißt, l ist das Polynom gleichen Namens aus Satz 3.1.1, wobei dort statt f das Minimalpolynom von φ verwendet wird —

Ausgabe:

Es wird eine Ganzheitsbasis von $\mathfrak{o}'_f$ zurückgegeben.

1. Schritt: (Gleichungsordnung ist maximal)

Falls l nicht übergeben wurde, so setze

$$(\beta_1, \dots, \beta_n) \leftarrow (1, \varphi, \dots, \varphi^{n-1})$$

mit $n := \mathrm{Grad}(f)$ *und gehe zu Schritt 3.*

2. Schritt: (Multiplikatorring ist maximal)

Setze

$$(\beta_1, \dots, \beta_n) \leftarrow (1, \varphi, \dots, \varphi^{n-(m+1)}, \frac{l(\varphi)}{p}, \frac{l(\varphi)}{p}\varphi, \dots, \frac{l(\varphi)}{p}\varphi^{m-1})$$

mit $m := \mathrm{Grad}(f) - \mathrm{Grad}(l)$.

3. Schritt: (Hermite Reduktion)

Sei A die $n \times n$ Matrix über $\mathbb{Z}'$, welche als i-te Spalte die Koeffizienten von $p^{v_p(d_r(f))}\beta_i$ bezüglich der Basis $1, \xi, \dots, \xi^{n-1}$ mit $\xi := t + f(t)\mathbb{Q}[t]$ hat. $B = (b_{ij})$ sei die auf Hermite Normalform transformierte Matrix A. Setze

$$\tilde{\omega}_j \leftarrow \frac{1}{p^{v_p(d_r(f))}} \sum_{i=1}^{n} b_{ij}\xi^{i-1}$$

für $j \in \{1, \dots, n\}$. *Terminiere mit*

$$(\tilde{\omega}_1, \dots, \tilde{\omega}_n).$$

3.2 Die Algebra ist zerlegbar

Als zweites soll der Fall, daß f modulo p in zwei verschiedene, teilerfremde Polynome zerlegbar ist, betrachtet werden. Sei

$$f \equiv f_1 f_2 \mod p\mathbb{Z}'[t]$$

eine Zerlegung von f in zwei, modulo p teilerfremde normierte Polynome. Mittels Hensels Lemma lassen sich zu beliebigem $\kappa \in \mathbb{N}$ normierte, modulo p teilerfremde Polynome $\tilde{f}_1, \tilde{f}_2 \in \mathbb{Z}'[t]$ mit

$$\begin{aligned} f &\equiv \tilde{f}_1 \tilde{f}_2 \mod p^\kappa \mathbb{Z}'[t] \\ f_1 &\equiv \tilde{f}_1 \mod p^\kappa \mathbb{Z}'[t] \\ f_2 &\equiv \tilde{f}_2 \mod p^\kappa \mathbb{Z}'[t] \end{aligned}$$

berechnen. Siehe dazu [Co, Po/Za]. Ziel ist die Herstellung einer Isomorphie zwischen den Strukturen $\mathfrak{o}'_f$ und $\mathfrak{o}'_{\tilde{f}_1} \oplus \mathfrak{o}'_{\tilde{f}_2}$ für ein hinreichend großes κ. Grundlage dafür ist eine Arbeit von Zassenhaus [Za], welche die Isomorphie von $\mathfrak{o}'_f$ und $\mathfrak{o}'_{\tilde{f}}$ garantiert, wenn nur f und $\tilde{f}$ p-adisch nahe beieinander liegen. Zunächst wollen wir erst einmal die Beziehung zwischen $\mathfrak{o}'_{\tilde{f}}$ und $\mathfrak{o}'_{\tilde{f}_1}, \mathfrak{o}'_{\tilde{f}_2}$ für $\tilde{f} = \tilde{f}_1 \tilde{f}_2$ untersuchen.

3.2.1 Reduktion durch Zerlegung

Sei $\tilde{f} = \tilde{f}_1 \tilde{f}_2$ mit $\tilde{f}_1, \tilde{f}_2$ zwei normierte, teilerfremde Polynome über $\mathbb{Z}'$, die beide keine Konstanten modulo p sind. Nach dem chinesischen Restsatz gilt

$$\mathcal{A}_{\tilde{f}} \cong \mathcal{A}_{\tilde{f}_1} \oplus \mathcal{A}_{\tilde{f}_2}.$$

Wegen $\mathrm{Grad}(\tilde{f}) > \mathrm{Grad}(\tilde{f}_1), \mathrm{Grad}(\tilde{f}_2)$ reduzieren wir das Problem, wenn die Berechnung von $\mathfrak{o}'_{\tilde{f}}$ auf die Berechnung von $\mathfrak{o}'_{\tilde{f}_1}$ und $\mathfrak{o}'_{\tilde{f}_2}$ zurückgeführt werden kann. In Satz 2.4.5 haben wir gezeigt, daß $Cl(\mathbb{Z}', \mathcal{A}_{\tilde{f}_1} \oplus \mathcal{A}_{\tilde{f}_2}) = Cl(\mathbb{Z}', \mathcal{A}_{\tilde{f}_1}) \oplus Cl(\mathbb{Z}', \mathcal{A}_{\tilde{f}_2})$ ist. In Lemma 1.3.4 haben wir einen speziellen $\mathbb{Z}'$-Isomorphismus $\varphi : \mathcal{A}_{\tilde{f}} \longrightarrow \mathcal{A}_{\tilde{f}_1} \oplus \mathcal{A}_{\tilde{f}_2}$ gefunden, welcher dem chinesischen Restsatz genügt und zwei orthogonale Idempotente e_1, e_2 von $\mathcal{A}_{\tilde{f}}$ konstruiert mit den Eigenschaften $\varphi(e_i \mathcal{A}_{\tilde{f}}) = \delta_{1,i} \mathcal{A}_{\tilde{f}_1} \oplus \delta_{2,i} \mathcal{A}_{\tilde{f}_2}$ für $i \in \{1,2\}$. Aus Satz 1.3.7 können wir weiter folgern, daß $\varphi(Cl(e_i \mathbb{Z}', e_i \mathcal{A}_{\tilde{f}})) = \delta_{1,i} Cl(\mathbb{Z}', \mathcal{A}_{\tilde{f}_1}) \oplus \delta_{2,i} Cl(\mathbb{Z}', \mathcal{A}_{\tilde{f}_2})$ für $i \in \{1,2\}$ ist. Damit sind wir in der Lage, aus $\mathbb{Z}'$-Basen von $Cl(\mathbb{Z}', \mathcal{A}_{\tilde{f}_1})$ und $Cl(\mathbb{Z}', \mathcal{A}_{\tilde{f}_2})$ zwei $\mathbb{Z}'$-Basen für $Cl(e_1 \mathbb{Z}', e_1 \mathcal{A}_{\tilde{f}})$ und $Cl(e_2 \mathbb{Z}', e_2 \mathcal{A}_{\tilde{f}})$ zu berechnen und diese zu einer $\mathbb{Z}'$-Basis von $Cl(\mathbb{Z}', \mathcal{A}_{\tilde{f}})$ zusammenzusetzen.

Satz 3.2.1 *Seien $\omega_{11}, \dots, \omega_{1j_1}$ und $\omega_{21}, \dots, \omega_{2j_2}$ $\mathbb{Z}'$-Basen von $Cl(\mathbb{Z}', \mathcal{A}_{\tilde{f}_1})$ beziehungsweise $Cl(\mathbb{Z}', \mathcal{A}_{\tilde{f}_2})$. Definieren wir*

$$\begin{aligned} \tilde{\omega}_{1j} &:= \varphi^{-1}(\omega_{1j} \oplus 0) \quad j \in \{1, \dots, j_1\} \\ \tilde{\omega}_{2j} &:= \varphi^{-1}(0 \oplus \omega_{2j}) \quad j \in \{1, \dots, j_2\}, \end{aligned}$$

so bildet $\tilde{\omega}_{11}, \dots, \tilde{\omega}_{1j_1}, \tilde{\omega}_{21}, \dots, \tilde{\omega}_{2j_2}$ eine $\mathbb{Z}'$-Basis von $Cl(\mathbb{Z}', \mathcal{A}_{\tilde{f}}) = \mathfrak{o}'_{\tilde{f}}$.

Nach Bemerkung 1.3.5 ist uns φ^{-1} konstruktiv gegeben, so daß wir $\tilde{\omega}_{ij}$ wirklich bestimmen können.

Das Berechnen einer Basis für $\mathfrak{o}'_{\tilde{f}}$ kann also auf die Berechnung der Basen von $\mathfrak{o}'_{\tilde{f}_1}$ und $\mathfrak{o}'_{\tilde{f}_2}$ zurückgeführt werden, da diese mittels orthogonaler Idempotenter und des Isomorphismus φ zu Basen von $\mathfrak{o}'_{\tilde{f}}$ zusammengesetzt werden können.

Vom algorithmischen Standpunkt aus betrachtet ist die Konstruktion von φ^{-1} entsprechend Bemerkung 1.3.5 sehr aufwendig, da wir einen erweiterten größten gemeinsamen Teiler bestimmen müssen. Setzen wir die zusätzliche Annahme, daß $\tilde{f}_1$ und $\tilde{f}_2$ modulo p teilerfremd sind, voraus, so können wir, statt der in Bemerkung 1.3.5 benutzten $\tilde{e}_1$ und $\tilde{e}_2$, einfach die Polynome $\tilde{f}_2$ und $\tilde{f}_1$ verwenden und erhalten bei Anwendung der dadurch definierten Abbildung ψ an Stelle von φ^{-1} ebenfalls eine $\mathbb{Z}'$-Basis von $\mathfrak{o}'_{\tilde{f}}$.

Satz 3.2.2 *Seien $\tilde{f}_1$ und $\tilde{f}_2$ zusätzlich koprim modulo p, und $\psi : \mathcal{A}_{\tilde{f}_1} \oplus \mathcal{A}_{\tilde{f}_2} \longrightarrow \mathcal{A}_{\tilde{f}}$ definiert durch $\psi(g_1(\xi_1) \oplus g_2(\xi_2)) := g_1(\xi)\tilde{f}_2(\xi) + g_2(\xi)\tilde{f}_1(\xi)$ mit $\xi := t + \tilde{f}(t)\mathbb{Q}[t]$ und $\xi_i := t + \tilde{f}_i(t)\mathbb{Q}[t]$ für $i \in \{1, 2\}$. So ist $\psi(\omega_{11}), \dots, \psi(\omega_{1j_1}), \psi(\omega_{2,1}), \dots, \psi(\omega_{2j_2})$ eine $\mathbb{Z}'$-Basis von $\mathfrak{o}'_{\tilde{f}}$.*

Beweis: Zunächst bezeichnen wir der Übersicht halber die im Satz definierte Basis mit $\tilde{\omega}_{11}, \dots, \tilde{\omega}_{1j_1}, \tilde{\omega}_{21}, \dots, \tilde{\omega}_{2j_2}$. Wir zeigen, daß es $\mathbb{Z}'$-Basen $\hat{\omega}_{i1}, \dots \hat{\omega}_{ij_i}$ von $\mathfrak{o}'_{f_i}$ für $i \in \{1, 2\}$ gibt, so daß $\tilde{\omega}_{1j} = \varphi^{-1}(\hat{\omega}_{1j} \oplus 0)$ beziehungsweise $\tilde{\omega}_{2j} = \varphi^{-1}(0 \oplus \hat{\omega}_{2j})$ für alle $j \in \{1, \dots, j_i\}$ und $i \in \{1, 2\}$ gilt. Nach Satz 3.2.1 ist dann $\tilde{\omega}_{11}, \dots, \tilde{\omega}_{2j_2}$ eine $\mathbb{Z}'$-Basis von $\mathfrak{o}'_{\tilde{f}}$. Wir benutzen die Bezeichnungen aus dem Beweis von Lemma 1.3.4. Dabei sind nur f, f_1 und f_2 durch $\tilde{f}, \tilde{f}_1$ und $\tilde{f}_2$ zu ersetzen.

Ohne Einschränkung sei i gleich Eins. Seien $a := \tilde{f}_2(\xi_1)$ aus $\mathbb{Z}'[\xi_1]$ und g_j aus $\mathbb{Q}[t]$ mit $g_j(\xi_1) = \omega_{1j}$ für $j \in \{1, \dots, j_1\}$. Für $a\omega_{1j} \oplus 0$ erhalten wir unter φ^{-1} das Bild $\varphi^{-1}(a\omega_{1j} \oplus 0) = e_1\tilde{f}_2(\xi)g_j(\xi) = \tilde{e}_1(\xi)\tilde{f}_2(\xi)g_j(\xi) = r_2(\xi)\tilde{f}_2^2(\xi)g_j(\xi) = \tilde{f}_2(\xi)(1 - r_1(\xi)\tilde{f}_1(\xi))g_j(\xi) = \tilde{f}_2(\xi)g_j(\xi) = \psi(g_j(\xi_1) \oplus 0) = \psi(\omega_{1j} \oplus 0)$ für alle j aus $\{1, \dots, j_1\}$. Wir müssen also nur noch zeigen, daß a eine Einheit aus $\mathfrak{o}'_{\tilde{f}_1}$ ist.

a ist eine Einheit in $\mathfrak{o}'_{\tilde{f}_1}$ genau dann, wenn a bezüglich jeder Fortsetzung der p-adischen Bewertung von $\mathbb{Z}'$ auf $\mathfrak{o}'_{\tilde{f}_1}$ den Wert Null hat. Das geht auf Grund der Eigenschaft (iv) von Exponentialbewertungen und der Minimabildung bei der v_p^*-Bewertung nur für $v_p^*(a) = v_p^*(a^{-1}) = 0$. Da a nach Konstruktion in $\mathbb{Z}'[\xi_1]$ liegt, muß die v_p^*-Bewertung von a größer gleich Null sein. Wir müssen also zeigen, daß a in keinem Primideal $\mathfrak{p}$ von $\mathbb{Z}'[\xi_1]$ liegt. Greifen wir auf den Satz 3.3.4 vor. Die Primideale von $\mathbb{Z}'[\xi_1]$ haben danach die Gestalt $\mathfrak{p} = \mu(\xi_1)\mathbb{Z}'[\xi_1] + p\mathbb{Z}'[\xi_1]$, wobei μ aus $\mathbb{Z}'[t]$ ein normierter, irreduzibler Teiler von $\tilde{f}_1$ modulo p ist. Da $\tilde{f}_1$ und $\tilde{f}_2$ modulo p teilerfremd und normiert sind, kann $\tilde{f}_2(\xi_1) = a$ nicht in einem Primideal von $\mathbb{Z}'[\xi_1]$ liegen und hat somit die v_p^*-Bewertung Null. □

Die zusätzliche Voraussetzung der Teilerfremdheit von $\tilde{f}_1$ und $\tilde{f}_2$ modulo p ist keine echte Einschränkung, da wir $\tilde{f}$ gerade als das Produkt zweier Polynome mit dieser Eigenschaft konstruiert haben.

3.2.2 Structural Stability

Damit kommen wir zum Kerngedanken des Algorithmus. Wir müssen aus einer $\mathbb{Z}'$-Basis von $\mathfrak{o}'_{\tilde{f}}$ eine $\mathbb{Z}'$-Basis von $\mathfrak{o}'_f$ bestimmen. H. Zassenhaus hat in seiner Arbeit [Za] gezeigt, daß die isomorphen $\mathbb{Q}$-Moduln $\mathcal{A}_f$ und $\mathcal{A}_{\tilde{f}}$ für p-adisch nahe beieinanderliegende Polynome f und $\tilde{f}$ auch „strukturell ähnliche“ Ordnungen besitzen. Wir zeigen den folgenden spezielleren Satz, welcher für unsere Bedürfnisse genügt.

Satz 3.2.3 (Structural Stability) *Seien $f, \tilde{f} \in \mathbb{Z}'[t]$ normiert und $d \in \mathbb{N}$ mit*

$$\begin{aligned} p^d \mathfrak{o}'_f &\subseteq \mathcal{R}'_f \\ p^d \mathfrak{o}'_{\tilde{f}} &\subseteq \mathcal{R}'_{\tilde{f}} \\ f &\equiv \tilde{f} \mod p^{2d}\mathbb{Z}'[t], \end{aligned}$$

so gilt für den $\mathbb{Q}$-Modulisomorphismus

$$\begin{aligned} \sigma : \mathcal{A}_f &\longrightarrow \mathcal{A}_{\tilde{f}} \\ t^i + f(t)\mathbb{Q}[t] &\longmapsto t^i + \tilde{f}(t)\mathbb{Q}[t] \end{aligned}$$

mit $i \in \{0, \dots, \mathrm{Grad}(f) - 1\}$

$$\sigma(\alpha\beta) \equiv \sigma(\alpha)\sigma(\beta) \mod p^{2d}\mathcal{R}'_{\tilde{f}}$$

für α und β aus $\mathcal{R}'_f$ beliebig.

Beweis: Seien $\xi := t + f(t)\mathbb{Q}[t]$ und $\tilde{\xi} = t + \tilde{f}(t)\mathbb{Q}[t]$, so gilt für die Algebren $\mathcal{A}_f = \mathbb{Q}(\xi)$ und $\mathcal{A}_{\tilde{f}} = \mathbb{Q}(\tilde{\xi})$. Die Polynome f und $\tilde{f}$ haben die Gestalt $f(t) = t^n + a_{n-1}t^{n-1} + \ldots + a_0$ und $\tilde{f}(t) = t^n + \tilde{a}_{n-1}t^{n-1} + \ldots + \tilde{a}_0$ mit $a_i, \tilde{a}_i \in \mathbb{Z}'$. Für die n-ten Potenzen von ξ beziehungsweise $\tilde{\xi}$ ergeben sich die Darstellungen $\xi^n = -\sum_{j=0}^{n-1} a_j\xi^j$ und $\tilde{\xi}^n = -\sum_{j=0}^{n-1} \tilde{a}_j\tilde{\xi}^j$. Auf Grund der $\mathbb{Q}$-Linearität von σ genügt es, die Behauptung für beliebige ξ Potenzen anstelle von α und β zu zeigen.

Im Fall $i \in \mathbb{N}$ mit $i < n = \mathrm{Grad}(f)$ ist nichts zu zeigen, da nach Definition von σ gilt $\sigma(\xi^i) = \tilde{\xi}^i = \sigma(\xi)^i$. Den Fall $i \geq n$ werden wir durch Induktion über $k = i - n$ zeigen.

Induktionsanfang: $k = 0$, das heißt $i = n$.
Betrachten wir die Differenz $\sigma(\xi^n) - \sigma(\xi)^n$.

$$\begin{aligned}
\sigma(\xi^n) - \sigma(\xi)^n &= \sigma(-\sum_{j=0}^{n-1} a_j\xi^j) - \tilde{\xi}^n \\
&= -\sum_{j=0}^{n-1} a_j\tilde{\xi}^j + \sum_{j=0}^{n-1} \tilde{a}_j\tilde{\xi}^j \\
&= \sum_{j=0}^{n-1}(\tilde{a}_j - a_j)\tilde{\xi}^j
\end{aligned}$$

$\tilde{a}_j - a_j$ liegt in $p^{2d}\mathbb{Z}'$, da nach Voraussetzung $f \cong \tilde{f} \mod p^{2d}\mathbb{Z}'[t]$. Das heißt, die Differenz $\sigma(\xi^n) - \sigma(\xi)^n$ liegt in $p^{2d}\mathbb{Z}'[\tilde{\xi}]$.

Induktionsschritt: $k \to k + 1$.
Es sei schon gezeigt, daß $\sigma(\xi^{n+k}) - \sigma(\xi)^{n+k} = p^{2d}\sum_{j=0}^{n-1} h_j\tilde{\xi}^j \in p^{2d}\mathcal{R}'_{\tilde{f}}$ gilt. Seien $\xi^{n+k} = \sum_{j=0}^{n-1} m_j\xi^j$ und $\tilde{\xi}^{n+k} = \sum_{j=0}^{n-1} \tilde{m}_j\tilde{\xi}^j$ mit $m_j - \tilde{m}_j = p^{2d}h_j$, so gilt

$$\begin{aligned}
&\sigma(\xi^{n+k+1}) - \sigma(\xi)^{n+k+1} \\
&= \sigma(\xi^{n+k}\xi) - \tilde{\xi}^{n+k}\tilde{\xi} \\
&= \sigma\left(\sum_{j=0}^{n-1} m_j\xi^{j+1}\right) - \sum_{j=0}^{n-1} \tilde{m}_j\tilde{\xi}^{j+1} \\
&= \sigma\left(\sum_{j=0}^{n-2} m_j\xi^{j+1} - m_{n-1}\sum_{j=0}^{n-1} a_j\xi^j\right) - \sum_{j=0}^{n-2} \tilde{m}_j\tilde{\xi}^{j+1} + \tilde{m}_{n-1}\sum_{j=0}^{n-1} \tilde{a}_j\tilde{\xi}^j \\
&= \sum_{j=0}^{n-2} m_j\tilde{\xi}^{j+1} - \sum_{j=0}^{n-2} \tilde{m}_j\tilde{\xi}^{j+1} - m_{n-1}\sum_{j=0}^{n-1} a_j\tilde{\xi}^j + \tilde{m}_{n-1}\sum_{j=0}^{n-1} \tilde{a}_j\tilde{\xi}^j \\
&= \sum_{j=0}^{n-2}(m_j - \tilde{m}_j)\tilde{\xi}^{j+1} - (m_{n-1} - \tilde{m}_{n-1})\sum_{j=0}^{n-1} a_j\tilde{\xi}^j - \tilde{m}_{n-1}\sum_{j=0}^{n-1}(a_j - \tilde{a}_j)\tilde{\xi}^j \\
&\in p^{2d}\mathbb{Z}'[\tilde{\xi}],
\end{aligned}$$

da die Differenzen $m_j - \tilde{m}_j$ und $a_j - \tilde{a}_j$ für alle j aus $\{0, \ldots, n-1\}$ in $p^{2d}\mathbb{Z}'$ liegen. $\square$

Korollar 3.2.4 *Mit den Voraussetzungen aus Satz 3.2.3 ist* $\tilde{R} := \sigma(\mathfrak{o}'_f)$ *eine Ordnung.*

Beweis: $\tilde{R} = \sigma(\mathfrak{o}'_f)$ ist als Bild eines $\mathbb{Z}'$-Moduls unter einem $\mathbb{Q}$-Modulisomorphismus ebenfalls ein $\mathbb{Z}'$-Modul gleichen Ranges. Zum Nachweis, daß $\tilde{R}$ eine Ordnung ist, bleibt noch zu zeigen, daß $\tilde{R}$ bezüglich der Multiplikation abgeschlossen ist. Seien $\tilde{\alpha}$ und $\tilde{\beta}$ aus $\tilde{R}$ und $\alpha, \beta \in \mathfrak{o}'_f$, so daß $\tilde{\alpha} = \sigma(\alpha)$ und $\tilde{\beta} = \sigma(\tilde{\beta})$ gilt. Aus Satz 3.2.3 erhalten wir wegen $p^d\alpha, p^d\beta \in \mathcal{R}'_f$ für $\tilde{\alpha}$ und $\tilde{\beta}$ die Darstellung

$$\begin{aligned}
\tilde{\alpha}\tilde{\beta} &= \sigma(\alpha)\sigma(\beta) \\
&= p^{-2d}\sigma(p^d\alpha)\sigma(p^d\beta) \\
&= p^{-2d}(\sigma(p^{2d}\alpha\beta) + p^{2d}\gamma) \\
&= \sigma(\alpha\beta) + \gamma
\end{aligned}$$

mit $\gamma \in \mathcal{R}'_{\tilde{f}}$. Nach der Konstruktion von σ ist $\mathcal{R}'_{\tilde{f}}$ eine Teilmenge von $\tilde{R}$, und somit liegt auch $\tilde{\alpha}\tilde{\beta} = \sigma(\alpha\beta) + \gamma$ in $\tilde{R}$. $\square$

Uns liegt also die Situation, daß $\sigma(\mathfrak{o}'_f) \subseteq \mathcal{A}_{\tilde{f}}$ und $\sigma^{-1}(\mathfrak{o}'_{\tilde{f}}) \subseteq \mathcal{A}_f$ Ordnungen sind, vor. Für $\mathfrak{o}'_f$ müssen somit die Inklusionen

$$\mathfrak{o}'_f = \sigma^{-1}(\sigma(\mathfrak{o}'_f)) \subseteq \sigma^{-1}(\mathfrak{o}'_{\tilde{f}}) \subseteq \mathfrak{o}'_f$$

gelten. Das heißt, in σ haben wir einen $\mathbb{Q}$-Modulisomorphismus zwischen $\mathfrak{o}'_f$ und $\mathfrak{o}'_{\tilde{f}}$ gefunden. Wurde eine Ganzheitsbasis für $\mathfrak{o}'_{\tilde{f}}$ berechnet, so können wir auf Grund der $\mathbb{Q}$-Linearität von σ sofort eine Ganzheitsbasis für $\mathfrak{o}'_f$ vermittels σ^{-1} angeben. Die Umkehrabbildung von σ hat die einfache Gestalt $\sigma^{-1} : t^i + \tilde{f}(t)\mathbb{Q}[t] \mapsto t^i + f(t)\mathbb{Q}[t]$.

Satz 3.2.5 *Mit den Voraussetzungen aus Satz 3.2.3 gilt, der ganze Abschluß* $\mathfrak{o}'_f$ *von* $\mathbb{Z}'$ *in* $\mathcal{A}_f$ *ist isomorph dem ganzen Abschluß* $\mathfrak{o}'_{\tilde{f}}$ *von* $\mathbb{Z}'$ *in* $\mathcal{A}_{\tilde{f}}$. *Die Funktion* σ *bildet* $\mathfrak{o}'_f$ $\mathbb{Q}$*-invariant und isomorph auf* $\mathfrak{o}'_{\tilde{f}}$ *ab. Insbesondere werden* $\mathbb{Z}'$*-Basen durch* σ *auf* $\mathbb{Z}'$*-Basen abgebildet.*

Offen geblieben ist damit noch die Bestimmung von $d \in \mathbb{N}$, das in der Voraussetzung von Satz 3.2.3 steht. Auf das Problem, einen $\mathbb{Q}$-Isomorphismus zwischen zwei Algebren zu konstruieren, der auch ein $\mathbb{Q}$-Isomorphismus zwischen den Maximalordnungen ist, sind wir gekommen durch die Existenz einer Zerlegung von f modulo p in zwei verschiedene, teilerfremde, normierte Faktoren

$$f \equiv f_1 f_2 \mod p\mathbb{Z}'[t]$$

und der Möglichkeit, mittels des Henselschen Lemmas eine analoge Zerlegung modulo einer beliebigen p-Potenz berechnen zu können. Das heißt, wir haben zur Berechnung von d zwei Probleme zu lösen.

(i) Bestimmung eines $\kappa \in \mathbb{N}$ mit $p^\kappa \mathfrak{o}'_f \subseteq \mathcal{R}'_f$

(ii) Bestimmung eines $\lambda \in \mathbb{N}$ mit

$$f \equiv \tilde{f} \mod p^{2\lambda}\mathbb{Z}'[t] \Rightarrow \tilde{f} \text{ ist separabel und } p^\lambda \mathfrak{o}'_{\tilde{f}} \subseteq \mathcal{R}'_{\tilde{f}}.$$

Das Maximum beider Zahlen ist dann als das gewünschte d wählbar.

Bestimmung von κ

Das kleinste $p^\kappa \in \mathbb{N}$ mit $p^\kappa \mathfrak{o}'_f \subseteq \mathcal{R}'_f$ ist der Exponent der Gruppe $\mathfrak{o}'_f/\mathcal{R}'_f$. Gesucht ist also eine Abschätzung des Exponenten nach oben. Diese ist gefunden, wenn wir aus $\mathcal{R}'_f$ einen $\mathbb{Z}'$-Modul M konstruieren, der $\mathfrak{o}'_f$ enthält und wir den Exponenten von $M/\mathcal{R}'_f$ berechnen können. Dazu bedienen wir uns einiger Hilfsmittel der linearen Algebra.

Mit Hilfe der Spur auf $\mathcal{A}_f$ kann eine symmetrische, nicht entartete Bilinearform auf $\mathcal{A}_f$ durch

$$\begin{aligned} B : \mathcal{A}_f \times \mathcal{A}_f &\longrightarrow \mathbb{Q} \\ (\alpha, \beta) &\longmapsto \mathrm{Tr}(\alpha\beta) \end{aligned}$$

definiert werden. Sei R eine Ordnung in $\mathcal{A}_f$ mit der $\mathbb{Z}'$-Basis $\omega_1, \ldots, \omega_n$, so ist der Dualraum $R^\#$ zu R definiert durch

$$R^\# := \mathbb{Z}'\omega_1^\# + \ldots + \mathbb{Z}'\omega_n^\#,$$

wobei

$$\omega_i^\# \in \mathcal{A}_f \text{ mit } B(\omega_i^\#, \omega_j) = \delta_{i,j} \quad \forall i, j \in \{1, \ldots, n\}$$

die duale Basis zu $\omega_1, \ldots, \omega_n$ bezüglich B ist. Den Dualraum von R können wir auch wie folgt charakterisieren.

Lemma 3.2.6 $R^\# = \{\alpha \in \mathcal{A}_f | \forall \beta \in R : \mathrm{Tr}(\alpha\beta) \in \mathbb{Z}'\}$

Aus dem Lemma erhalten wir sofort unsere Forderung $\mathfrak{o}'_f \subseteq R^\#$. Der Exponent von $R^\#/R$ ist also eine obere Schranke des Exponenten von $\mathfrak{o}'_f/R$. Beweisen wir zunächst das Lemma.

Beweis: Sei α ein beliebiges Element aus dem Dualraum, dann hat α die Darstellung

$$\alpha = \sum_{i=1}^{n} \alpha_i \omega_i^{\#} \in R^{\#}$$

mit $\alpha_i \in \mathbb{Z}'$. Auf Grund der Linearität der Spur erhalten wir für $\beta = \sum_{i=1}^{n} \beta_i \omega_i$ aus R beliebig

$$\mathrm{Tr}(\alpha\beta) = \mathrm{Tr}(\alpha \sum_{i=1}^{n} \beta_i \omega_i) = \sum_{i=1}^{n} \beta_i \,\mathrm{Tr}(\alpha\omega_i).$$

Für unsere Bedingung „$\forall \beta \in R : \mathrm{Tr}(\alpha\beta) \in \mathbb{Z}'$“ ergibt sich somit die äquivalente Aussage „$\forall i \in \{1, \ldots, n\} : \mathrm{Tr}(\alpha\omega_i) \in \mathbb{Z}'$“. Betrachten wir für $k \in \{1, \ldots, n\}$ die Spur von $\alpha\omega_k$

$$\begin{aligned}
\mathrm{Tr}(\alpha\omega_k) &= \mathrm{Tr}(\sum_{i=1}^{n} \alpha_i \omega_i^{\#} \omega_k) \\
&= \sum_{i=1}^{n} \alpha_i \,\mathrm{Tr}(\omega_i^{\#} \omega_k) \\
&= \alpha_k.
\end{aligned}$$

Nach der Definition von $R^{\#}$ folgt damit die Behauptung. □

Zu einer beliebigen Ordnung R von $\mathcal{A}_f$ ist der Dualraum von R ein $\mathbb{Z}'$-Modul, welcher $\mathfrak{o}'_f$ enthält. Wir müssen den Exponenten der Faktorgruppe $R^{\#}/R$ bestimmen. Seien $\omega_1, \ldots, \omega_n$ eine $\mathbb{Z}'$-Basis von R und $T^{\#}$ die Übergangsmatrix von $\omega_1^{\#}, \ldots, \omega_n^{\#}$ nach $\omega_1, \ldots, \omega_n$. Der Exponent der Gruppe $R^{\#}/R$ ist gleich dem Betrag des maximalen Elementarteilers von $T^{\#}$. Welche Gestalt hat die Übergangsmatrix $T^{\#}$? Aus der Linearität der Spur erhalten wir

$$\begin{aligned}
\mathrm{Tr}(\omega_i\omega_j) &= \mathrm{Tr}((\omega_i\omega_1^{\#}, \ldots, \omega_i\omega_n^{\#})T_j^{\#}) \\
&= (\mathrm{Tr}(\omega_i\omega_1^{\#}), \ldots, \mathrm{Tr}(\omega_i\omega_n^{\#}))T_j^{\#} \\
&= (\delta_{i,1}, \ldots, \delta_{i,n})T_j^{\#} \\
&= t_{ij}^{\#},
\end{aligned}$$

wobei $(t_{ij}^{\#})_{i,j=1,\ldots,n} = (T_1^{\#} \ldots T_n^{\#}) = T^{\#}$ die Elemente beziehungsweise Spalten der Übergangsmatrix sind. Die Übergangsmatrix $T^{\#}$ zwischen den $\mathbb{Z}'$-Moduln R und $R^{\#}$ bezüglich der Basen $\omega_1, \ldots, \omega_n$ und $\omega_1^{\#}, \ldots, \omega_n^{\#}$ ist also die Spurenmatrix $(\mathrm{Tr}(\omega_i\omega_j))_{i,j=1,\ldots,n}$. Sei $\mathrm{Diag}(d_1, \ldots, d_n) = V^{-1}T^{\#}U$ die Smith Normalform von $T^{\#}$. Die Matrix $\mathrm{Diag}(d_1, \ldots, d_n) = (\delta_{ij}d_i)_{i,j=1,\ldots,n}$ sei dabei die $n \times n$-Diagonalmatrix mit den Einträgen $d_1, \ldots, d_n$ auf der Diagonalen. Dann sind $(\omega_1, \ldots, \omega_n)U$ und $(\omega_1^{\#}, \ldots, \omega_n^{\#})V$ $\mathbb{Z}'$-Basen von R beziehungsweise $R^{\#}$, und

$\mathrm{Diag}(d_1, \ldots, d_n)$ ist die Übergangsmatrix zwischen diesen Basen. Auf Grund der Teilbarkeitsbedingung $d_i | d_{i+1}$ für die Diagonaleneinträge in der Smith Normalform gilt

$$(\omega_1^{\#}, \ldots, \omega_n^{\#})\, V \begin{pmatrix} d_n & & \\ & \ddots & \\ & & d_n \end{pmatrix} \in R \times \ldots \times R,$$

womit $|d_n|$ der Exponent von $R^{\#}/R$ ist. $|d_n|$ heißt die **reduzierte Diskriminante** von R und wird mit $\mathrm{d}_r(R)$ bezeichnet. Ist R gleich der Gleichungsordnung $\mathcal{R}_f$ und $\omega_1, \ldots, \omega_n$ eine $\mathbb{Z}$-Basis, so bezeichnet man $|d_n|$ mit $\mathrm{d}_r(f)$.

Wählen wir als κ den Exponenten von p in $\mathrm{d}_r(\mathcal{R}'_f)$, so haben wir das erste Problem gelöst.

Bestimmung von λ

Wenn es möglich ist zu zeigen, daß für $\lambda := v_p(\mathrm{d}_r(\mathcal{R}'_f))$ gilt

$$f \equiv \tilde{f} \mod p^{2\lambda}\mathbb{Z}'[t] \Longrightarrow \tilde{f} \text{ ist separabel und } \ v_p(\mathrm{d}_r(\mathcal{R}'_{\tilde{f}})) = \lambda,$$

so haben wir auch das zweite Problem gelöst. Dazu müssen wir zuerst eine andere Charakterisierung der reduzierten Diskriminante für den Fall, daß $R = \mathcal{R}'_f$ eine Gleichungsordnung ist, herleiten.

Satz 3.2.7 *Für eine Gleichungsordnung $\mathcal{R}'_f$ gilt*

$$\mathcal{R}'^{\#}_f = \frac{1}{f'(\rho)}\mathcal{R}'_f$$

mit ρ Nullstelle von f.

Beweis: In einem Zerfällungskörper von f haben f und $\tilde{f}$ die Faktorisierung

$$\begin{aligned} f(t) &= \prod_{i=1}^{n}(t - \rho^{(i)}) \\ f'(t) &= \sum_{j=1}^{n} \prod_{i=1, i\neq j}^{n} (t - \rho^{(i)}), \end{aligned}$$

wobei $\rho = \rho^{(1)}, \ldots, \rho^{(n)}$ die Konjugierten von ρ sind. Wir werden zunächst Polynome g_j konstruieren mit $g_j(\rho^{(i)}) = \rho^{(i)j-1}$ für alle $i, j \in \{1, \ldots, n\}$. Für $f'(\rho^{(i)})$ gilt

$$f'(\rho^{(i)}) = \prod_{j=1, j\neq i}^{n} (\rho^{(i)} - \rho^{(j)}).$$

Daher leistet

$$h_i(t) := \frac{1}{f'(\rho^{(i)})}\frac{f(t)}{t-\rho^{(i)}}$$

dann

$$h_i(\rho^{(j)}) = \delta_{i,j}.$$

Definieren wir nun für $j \in \{1, \ldots, n\}$ das Polynom g_j durch

$$g_j(t) := \sum_{i=1}^{n} h_i(t)\rho^{(i)j-1},$$

so hat g_j ausgewertet an der Stelle $\rho^{(i)}$ den Wert $\rho^{(i)j-1}$. Die g_j für $j \in \{1, \ldots, n\}$ sind also Polynome der gewünschten Art. Da der Grad von g_j höchstens gleich $n-1$ ist und $g_j(t) - t^{j-1}$ aber die n Nullstellen $\rho = \rho^{(1)}, \ldots, \rho^{(n)}$ hat, muß

$$\begin{aligned} t^{j-1} &= g_j(t) \\ &= \sum_{i=1}^{n} h_i(t)\rho^{(i)j-1} \end{aligned} \tag{3.1}$$

gelten. In h_i tritt für $i = 1$ der behauptete Nenner $\frac{1}{f'(\rho)}$ auf, und mit der Summe $\sum_{i=1}^{n} \frac{1}{f'(\rho^{(i)})} = Tr(\frac{1}{f'(\rho)})$ erhalten wir die Spur. Wir müssen nun eine andere Darstellung von t^{j-1} aus den g_j entwickeln, so daß wir durch einen Koeffizientenvergleich die Bedingung an die duale Basis $Tr(\omega_i \omega_j^{\#}) = \delta_{ij}$ für einen Ausdruck mit dem Nenner $f'(\rho)$ bezüglich einer $\mathbb{Z}'$-Basis von $\mathcal{R}'_f$ erhalten. Die Polynomdivision liefere für f

$$\frac{f}{t-\rho^{(i)}} = \sum_{j=1}^{n} \gamma_j^{(i)} t^{j-1}.$$

Betrachten wir

$$\theta_j^{(i)} := \frac{\gamma_j^{(i)}}{f'(\rho^{(i)})}$$

für $j = 1, \ldots, n$ und setzen in Gleichung (3.1) die Definition von h_i ein, so erhalten wir

$$\begin{aligned} t^{j-1} &= \sum_{i=1}^{n} h_i(t)\rho^{(i)j-1} \\ &= \sum_{i=1}^{n} \frac{1}{f'(\rho^{(i)})}\frac{f(t)}{t-\rho^{(i)}}\rho^{(i)j-1} \\ &= \sum_{i=1}^{n} \frac{1}{f'(\rho^{(i)})}\sum_{k=1}^{n} \gamma_k^{(i)} t^{k-1}\rho^{(i)j-1} \\ &= \sum_{k=1}^{n} t^{k-1}\sum_{i=1}^{n} \frac{\gamma_k^{(i)}}{f'(\rho^{(i)})}\rho^{(i)j-1} \\ &= \sum_{k=1}^{n} t^{k-1}\sum_{i=1}^{n} \theta_k^{(i)}\rho^{(i)j-1}. \end{aligned}$$

Ein Koeffizientenvergleich für die t-Potenzen liefert nun

$$\delta_{j-1,k} = \sum_{i=1}^{n} \theta_k^{(i)} \rho^{(i)j-1} = Tr(\theta_k^{(1)} \rho^{j-1})$$

und damit die duale Basis zu $1, \rho, \ldots, \rho^{n-1}$:

$$\omega_k^{\#} = \theta_k^{(1)}.$$

Es bleibt also wegen

$$\omega_k^{\#} = \frac{\gamma_k^{(1)}}{f'(\rho)}$$

nur noch zu zeigen, daß $\gamma_1^{(1)}, \ldots, \gamma_n^{(1)}$ eine $\mathbb{Z}'$-Basis von $\mathcal{R}'_f$ bildet. Der Übersicht halber definieren wir $\gamma_i := \gamma_i^{(1)}$ für $i \in \{1, \ldots, n\}$. Sei $A \in \mathbb{Q}^{n \times n}$ eine Übergangsmatrix von $1, \rho, \ldots, \rho^{n-1}$ nach $\gamma_1, \ldots, \gamma_n$. Zu zeigen ist, daß A unimodular ist. Sei $f = t^n + c_1 t^{n-1} + \ldots + c_n$. Dann gilt

$$\begin{aligned} \gamma_n t^{n-1} &+ \gamma_{n-1} t^{n-2} + \ldots + \gamma_1 \\ &= \frac{t^n + c_1 t^{n-1} + \ldots + c_n}{t - \rho} \\ &= t^{n-1} + (c_1 + \rho) t^{n-2} + (c_2 + c_1\rho + \rho^2) t^{n-3} + \\ &\quad\ \vdots \\ &\quad +(c_{n-1} + c_{n-2}\rho + \ldots + c_1 \rho^{n-2} + \rho^{n-1}). \end{aligned}$$

Ein weiterer Koeffizientenvergleich für die t-Potenzen liefert

$$\begin{aligned} \gamma_n &= 1 \\ \gamma_{n-1} &= c_1 + \rho \\ \gamma_{n-2} &= c_2 + c_1\rho + \rho^2 \\ &\ \vdots \\ \gamma_1 &= c_{n-1} + c_{n-2}\rho + \ldots + c_1\rho^{n-2} + \rho^{n-1}. \end{aligned}$$

Die Übergangsmatrix A hat also die Gestalt

$$A = \begin{pmatrix} 1 & 0 & & & \cdots & 0 \\ c_1 & 1 & 0 & & \cdots & 0 \\ c_2 & c_1 & 1 & 0 & \cdots & 0 \\ \multicolumn{6}{c}{\dotfill} \\ c_{n-1} & & \cdots & & c_1 & 1 \end{pmatrix}$$

und ist somit unimodular. □

Jetzt können wir leicht die erwähnte andere Charakterisierung der reduzierten Diskriminante für Gleichungsordnungen zeigen.

Satz 3.2.8 *Für eine Gleichungsordnung $\mathcal{R}'_f$ gilt*

$$\mathrm{d}_r(\mathcal{R}'_f)\mathbb{Z}' = (f(t)\mathbb{Z}'[t] + f'(t)\mathbb{Z}'[t]) \cap \mathbb{Z}'.$$

Beweis: Sei $x = u(t)f(t) + v(t)f'(t) \in (f(t)\mathbb{Z}'[t] + f'(t)\mathbb{Z}'[t]) \cap \mathbb{Z}'$ beliebig, dann gilt insbesondere für die Spezialisierung $t \mapsto \rho$

$$x = u(\rho)f(\rho) + v(\rho)f'(\rho) = v(\rho)f'(\rho),$$

also $\frac{1}{f'(\rho)}x = v(\rho) \in \mathcal{R}'_f$. Damit muß der Exponent von $\mathcal{R}'^{\#}_f/\mathcal{R}'_f$ wegen $\mathcal{R}'^{\#}_f = \frac{1}{f'(\rho)}\mathcal{R}'_f$ aber x teilen, und x liegt in $\mathrm{d}_r(\mathcal{R}'_f)\mathbb{Z}'$.

Andererseits gilt für $\mathrm{d}_r(\mathcal{R}'_f)$

$$\frac{\mathrm{d}_r(\mathcal{R}'_f)}{f'(\rho)}\mathcal{R}'_f = \mathrm{d}_r(\mathcal{R}'_f)\mathcal{R}'^{\#}_f \subseteq \mathcal{R}'_f,$$

es gibt also ein $g \in \mathbb{Z}'[t]$ mit einem Grad kleiner $n = \mathrm{Grad}(f)$ und $\mathrm{d}_r(\mathcal{R}'_f) = g(\rho)f'(\rho)$. Dann liegt aber $\mathrm{d}_r(\mathcal{R}'_f)$ in $(f(t)\mathbb{Z}'[t] + f'(t)\mathbb{Z}'[t]) \cap \mathbb{Z}'$. □

Mit dieser Charakterisierung der reduzierten Diskriminante einer Gleichungsordnung sind wir in der Lage, folgenden Satz, der unser zweites Problem vollständig löst, zu zeigen.

Satz 3.2.9 *Sei $\tilde{f}$ ein normiertes Polynom aus $\mathbb{Z}'[t]$ mit $f \equiv \tilde{f} \mod p^\lambda\mathbb{Z}'[t]$ mit $\lambda \geq v_p(\mathrm{d}_r(\mathcal{R}'_f)) + 1$, dann gilt*

(i) $\tilde{f}$ ist separabel

(ii) $v_p(\mathrm{d}_r(\mathcal{R}'_f)) = v_p(\mathrm{d}_r(\mathcal{R}'_{\tilde{f}}))$.

Beweis: Für die Separabilität von $\tilde{f}$ müssen wir zeigen, daß $\tilde{f}$ und $\tilde{f}'$ teilerfremd sind. Sei $f = \tilde{f} + p^\lambda h$ mit h aus $\mathbb{Z}'[t]$ und $\mathrm{Grad}(h) < n = \mathrm{Grad}(f)$. Es gilt $f' = \tilde{f}' + p^\lambda h'$. Seien $u, v \in \mathbb{Z}'[t]$ mit $\mathrm{d}_r(\mathcal{R}'_f) = uf + vf'$ entsprechend Satz 3.2.8. Dann gilt

$$\begin{aligned} u\tilde{f} + v\tilde{f}' &= uf - p^\lambda uh + vf' - p^\lambda vh' \\ &= \mathrm{d}_r(\mathcal{R}'_f) - p^\lambda(uh + vh'). \end{aligned}$$

Falls $\tilde{f}$ nun nicht separabel ist, so gibt es einen nicht trivialen Teiler g von $\tilde{f}$ und $\tilde{f}'$. g ist normiert, da $\tilde{f}$ normiert ist. Modulo $p^\lambda\mathbb{Z}'[t]$ erhalten wir damit, daß $\mathrm{d}_r(\mathcal{R}'_f)$ das Produkt zweier nicht trivialer Polynome ist, von denen eines normiert ist. Das ist wegen $\mathrm{d}_r(\mathcal{R}'_f) \in \mathbb{Z}'$ nur für $\mathrm{d}_r(\mathcal{R}'_f) \equiv 0 \mod p^\lambda\mathbb{Z}'$ möglich.

Das steht im Widerspruch zur Wahl von λ, für welches $\mathrm{d}_r(\mathcal{R}'_f)$ nicht kongruent Null modulo $p^\lambda\mathbb{Z}'$ ist. $\tilde{f}$ ist somit separabel.

Kommen wir zur Gleichheit der p-adischen Bewertungen von den reduzierten Diskriminanten der Ordnungen $\mathcal{R}'_f$ und $\mathcal{R}'_{\tilde{f}}$. Da $\lambda \geq v_p(\mathrm{d}_r(\mathcal{R}'_f)) + 1$ und $f \equiv \tilde{f} \mod p^\lambda\mathbb{Z}'[t]$ ist, gilt nach Satz 3.2.8 $0 \not\equiv d_r(\mathcal{R}'_f) \equiv c\,\mathrm{d}_r(\mathcal{R}'_{\tilde{f}}) \mod p^\lambda\mathbb{Z}'$ mit $c \in \mathbb{Z}'$, das heißt, es muß $v_p(\mathrm{d}_r(\mathcal{R}'_{\tilde{f}})) \leq v_p(\mathrm{d}_r(\mathcal{R}'_f))$ gelten. Wegen der schon gezeigten Separabilität von $\tilde{f}$ können wir die Rollen von f und $\tilde{f}$ vertauschen und erhalten die umgekehrte Ungleichung. $\square$

3.2.3 Der Zerlegungsalgorithmus

Auf Grund seiner klaren und übersichtlichen Struktur wollen wir den Algorithmus zunächst entsprechend der bisher entwickelten Theorie, ohne Effizienzüberlegungen, aufschreiben. Im Anschluß werden wir eine erste Verbesserung angeben und uns, nachdem wir alle Teilprobleme vom theoretischen Standpunkt aus gelöst haben, nochmals gesondert in Kapitel 5 mit der Effizienzproblematik bei der Implementierung beschäftigen.

Algorithmus 3.2.10 *Zerlegungsalgorithmus*

Eingabe:

Es wird ein normiertes, separables Polynom f aus $\mathbb{Z}'[t]$ erwartet, welches modulo p in mindestens zwei koprime Faktoren zerfällt.

Ausgabe:

Es wird eine Ganzheitsbasis von $\mathfrak{o}'_f$ zurückgegeben.

1. Schritt: (Faktorisierung)

Faktorisiere f modulo p

$$f \equiv f_1 \dots f_s \mod p\mathbb{Z}'[t]$$

mit f_i normiert und paarweise koprim modulo p.

2. Schritt: (Liften der Faktorisierung)

Lifte mittels Hensels Lemma die Faktorisierung zu

$$f \equiv \tilde{f}_1 \dots \tilde{f}_s \mod p^{2\kappa}\mathbb{Z}'[t],$$

wobei $\kappa \geq v_p(\mathrm{d}_r(f))$ *ist.*

3. Schritt: (Bestimmung „orthogonaler Idempotenter")

Seien $\hat{f}_i$ *die Auslassungsprodukte* $\prod_{j=1,j\neq i}^{s} \tilde{f}_j$ *für alle* $i \in \{1, \dots, s\}$ *und* $r_1, \dots, r_s \in \mathbb{Q}[t]$ *mit* $1 = r_1\hat{f}_1 + \dots + r_s\hat{f}_s$. *Setze*

$$e_i \leftarrow r_i(\xi)\hat{f}_i(\xi)$$

für $i \in \{1, \dots, s\}$ *und* $\xi := t + f(t)\mathbb{Q}[t]$.

Wir haben jetzt erreicht, daß für $\tilde{f} := \tilde{f}_1 \dots \tilde{f}_s$ gilt

$$\begin{aligned} Cl(\mathbb{Z}', \mathcal{A}_f) &\cong Cl(\mathbb{Z}', \mathcal{A}_{\tilde{f}}) \quad \text{nach Satz 3.2.5} \\ &\cong Cl(\mathbb{Z}', \mathcal{A}_{\tilde{f}_1}) \oplus \dots \oplus Cl(\mathbb{Z}', \mathcal{A}_{\tilde{f}_s}) \quad \text{nach Satz 2.4.5} \end{aligned}$$

und für $\tilde{e}_i := r_i(\tilde{\xi})\hat{f}_i(\tilde{\xi})$, $\tilde{\xi} := t + \tilde{f}(t)\mathbb{Q}[t]$

$$\mathcal{A}_{\tilde{f}_i} \cong \tilde{e}_i \mathcal{A}_{\tilde{f}}.$$

4. Schritt: (Ganzheitsbasen der Summanden)

Bestimme die Ganzheitsbasen von $Cl(\mathbb{Z}', \mathcal{A}_{\tilde{f}_1}), \dots, Cl(\mathbb{Z}', \mathcal{A}_{\tilde{f}_s})$.
Seien $(\omega_{11}(\xi_1), \dots, \omega_{1n_1}(\xi_1)), \dots, (\omega_{s1}(\xi_s), \dots, \omega_{sn_s}(\xi_s))$ *mit* $\xi_i := t + \tilde{f}_i(t)\mathbb{Q}[t]$ *die berechneten Ganzheitsbasen.*

5. Schritt: (Addition)

Zusammensetzen der einzelnen Basen zu einer Ganzheitsbasis von $Cl(\mathbb{Z}', \mathcal{A}_f)$. *Setze*

$$(\omega_1, \dots, \omega_n) \leftarrow (e_1\omega_{11}(\xi), \dots, e_1\omega_{1n_1}(\xi), \dots, e_s\omega_{s1}(\xi), \dots, e_s\omega_{sn_s}(\xi)).$$

6. Schritt: (Hermite Reduktion)

Sei A die $n \times n$ Matrix über $\mathbb{Z}'$, welche als i-te Spalte die Koeffizienten von $p^{v_p(\mathrm{d}_r(f))}\omega_i$ bezüglich der Basis $1, \xi, \ldots, \xi^{n-1}$ hat. $B = (b_{ij})$ sei die auf Hermite Normalform transformierte Matrix A. Setze

$$\tilde{\omega}_j \leftarrow \frac{1}{p^{v_p(\mathrm{d}_r(f))}} \sum_{i=1}^{n} b_{ij}\xi^{i-1}$$

für $j \in \{1, \ldots, n\}$. Terminiere mit

$$(\tilde{\omega}_1, \ldots, \tilde{\omega}_n).$$

Wir können natürlich statt Schritt 3 den folgenden veränderten Schritt benutzen.

$3'$. Schritt: (Bestimmung „orthogonaler Elemente“)

Setze

$$e_i \leftarrow \prod_{j=1, j\neq i}^{s} f_j(\xi)$$

für $i \in \{1, \ldots, s\}$ und $\xi := t + f(t)\mathbb{Q}[t]$.

Nun haben wir nicht mehr eine so klare Aufteilung der Algebra wie durch „orthogonale Idempotenten“, aber nach Satz 3.2.2 wird in Schritt 5 mit den neuen Elementen e_i ebenfalls eine Ganzheitsbasis von $\mathfrak{o}'_f$ konstruiert.

3.3 Primärer Fall

Als letztes bleibt die Situation, daß die Gleichungsordnung weder maximal noch zerlegbar ist, zu lösen.

Wir haben es also mit einem normierten, separablen Polynom f aus $\mathbb{Z}'[t]$ zu tun, welches modulo p nur einen nicht trivialen Teiler besitzt. Um diesen komplexen Fall beschreiben zu können, ist es von Vorteil, einige Definitionen und einfache Aussagen voranzustellen.

3.3.1 Definitionen und Sätze

Ein Element $\alpha \in \mathfrak{o}'_f$ heißt **primär**, wenn sein charakteristisches Polynom beziehungsweise sein Minimalpolynom modulo p genau einen irreduziblen Faktor hat, das heißt

$$\chi_\alpha \equiv \nu_\alpha^{E_\alpha} \mod p\mathbb{Z}'[t].$$

ν_α heißt das p-**Minimalpolynom** von α. D_α sei der Grad von ν_α. $\mathrm{Grad}(f) = n = D_\alpha E_\alpha$.

Wir wollen während des Algorithmus ganze Elemente abändern, ohne daß sich bestimmte Eigenschaften ändern. Zunächst zeigen wir, daß das charakteristische Polynom eines ganzen Elements α sich nicht wesentlich ändert, wenn man zu α Elemente aus dem p-Radikal der Maximalordnung addiert.

Satz 3.3.1 *Seien $\alpha, \beta \in \mathfrak{o}'_f$ mit $\alpha \equiv \beta \mod \mathcal{J}'_p$, so gilt*

$$\chi_\alpha \equiv \chi_\beta \mod p\mathbb{Z}'[t].$$

Beweis: $\mathcal{A}_f$ ist eine innere direkte Summe $+_{i=1}^{s}\mathcal{A}_i$ von Körpern. Für das p-Radikal eines Körpers $\mathcal{A}_i$ gilt offensichtlich $\mathcal{J}'_p(\mathcal{A}_i) = \mathcal{J}'_p \cap \mathcal{A}_i$. Damit ist das p-Radikal von $\mathcal{A}_f$ gleich der inneren direkten Summe der p-Radikale der $\mathcal{A}_i$. Nach Satz 1.3.7 ist das charakteristische Polynom eines Elements aus $\mathcal{A}_f$ gleich dem Produkt der charakteristischen Polynome der Projektionen des Elements in die Körper $\mathcal{A}_i$ für alle $i \in \{1, \ldots, s\}$. Wir müssen also die Behauptung nur noch für den Fall zeigen, daß f irreduzibel ist.

Seien $\mathcal{A}_f$ ein Körper und $\sigma_1, \ldots, \sigma_n$ die verschiedenen $\mathbb{Q}$-Homomorphismen von $\mathcal{A}_f$ in einen algebraischen Abschluß $\mathcal{L}$ von $\mathcal{A}_f$. π sei die Differenz von β und α, das heißt, π liegt in $\mathcal{J}'_p$. Für die charakteristischen Polynome von α und β gilt

$$\begin{aligned}
\chi_\alpha(t) &= \prod_{i=1}^{n}(t - \sigma_i(\alpha)) \\
\chi_\beta(t) &= \prod_{i=1}^{n}(t - \sigma_i(\beta)) \\
&= \prod_{i=1}^{n}(t - \sigma_i(\alpha) - \sigma_i(\pi)).
\end{aligned}$$

Sei $\mathcal{J}'_p(\mathfrak{o}'_\mathcal{L})$ das p-Radikal von $\mathfrak{o}'_\mathcal{L}$, wenn wir zeigen, daß alle Konjugierten von π

in dem p-Radikal von $\mathfrak{o}'_{\mathcal{L}}$ liegen, so erhalten wir

$$\begin{aligned} \chi_\beta(t) &= \prod_{i=1}^{n}(t - \sigma_i(\alpha) - \sigma_i(\pi)) \\ &\equiv \prod_{i=1}^{n}(t - \sigma_i(\alpha)) \\ &= \chi_\alpha(t) \mod \mathcal{J}'_p(\mathfrak{o}'_{\mathcal{L}})[t] \end{aligned}$$

und daraus, wegen $\mathbb{Z}' \cap \mathcal{J}'_p(\mathfrak{o}'_{\mathcal{L}}) = p\mathbb{Z}'$, die gewünschte Kongruenz der charakteristischen Polynome von α und β.

π liegt im p-Radikal der Maximalordnung des Körpers $\mathcal{A}_f$. Sei $\mathfrak{P}$ ein beliebiges Primideal von $\mathfrak{o}'_{\mathcal{L}}$, so ist der Schnitt von $\mathfrak{P}$ mit $\mathfrak{o}'_f$ ein Primideal $\mathfrak{p}$ von $\mathfrak{o}'_f$. Damit liegt π in allen Primidealen von $\mathfrak{o}'_{\mathcal{L}}$ also im p-Radikal von $\mathfrak{o}'_{\mathcal{L}}$. Das p-Radikal von $\mathfrak{o}'_{\mathcal{L}}$ ist unter Körperautomorphismen invariant, da diese Primideale in Primideale überführen. Das heißt, mit π liegen auch alle Konjugierten von π im p-Radikal von $\mathfrak{o}'_{\mathcal{L}}$. □

Damit ändert sich bei der Addition von Elementen aus $\mathcal{J}'_p$ insbesondere nicht die Eigenschaft eines Elements, primär zu sein. Diesen wichtigen Fall wollen wir als Korollar nocheinmal gesondert festhalten.

Korollar 3.3.2 *Seien $\alpha, \beta \in \mathfrak{o}'_f$, α primär und $\alpha \equiv \beta \mod \mathcal{J}'_p$, so ist β primär und*

$$\nu_\alpha \equiv \nu_\beta \mod p\mathbb{Z}'[t].$$

Die p-Minimalpolynome von α und β sind also bei der Wahl eines geeigneten Liftings gleich.

Als nächstes werden wir den Restklassenring der Gleichungsordnung eines Elements α nach dem von p erzeugten Hauptideal untersuchen.

Lemma 3.3.3 *Sei $\alpha \in \mathfrak{o}'_f$, so gilt die Isomorphie*

$$\mathbb{Z}'[\alpha]/p\mathbb{Z}'[\alpha] \cong \mathbb{F}_p[t]/\bar{\mu}_\alpha(t)\mathbb{F}_p[t].$$

Beweis: Wir betrachten die folgenden beiden Verkettungen von Epimorphismen.

$$\begin{aligned} \mathbb{Z}'[t] &\longrightarrow \mathbb{Z}'[\alpha] \longrightarrow \mathbb{Z}'[\alpha]/p\mathbb{Z}'[\alpha] \\ \mathbb{Z}'[t] &\longrightarrow \mathbb{F}_p[t] \longrightarrow \mathbb{F}_p[t]/\bar{\mu}_\alpha\mathbb{F}_p[t] \end{aligned}$$

Der Kern beider Verkettungen ist offensichtlich $p\mathbb{Z}'[t] + \mu_\alpha(t)\mathbb{Z}'[t]$. Daraus folgt nach dem Isomorphiesatz für Ringe sofort die Behauptung. □

Nachdem wir den Restklassenring $\mathbb{Z}'[\alpha]/p\mathbb{Z}'[\alpha]$ als Faktor von Polynomringen beschrieben haben, können wir jetzt die Struktur der p enthaltenden Ideale der Gleichungsordnung von α untersuchen.

Satz 3.3.4 *Sei $\alpha \in \mathfrak{o}'_f$ und $\mu_\alpha \equiv \mu_1^{e_1} \cdot \ldots \cdot \mu_r^{e_r} \mod p\mathbb{Z}'[t]$ die Zerlegung von f in paarweise irreduzible, normierte Faktoren modulo p, so gilt*

$$p\mathbb{Z}'[\alpha] = \mathfrak{p}_1^{e_1} \cdot \ldots \cdot \mathfrak{p}_r^{e_r}$$

mit

$$\mathfrak{p}_i = \mu_i(\alpha)\mathbb{Z}'[\alpha] + p\mathbb{Z}'[\alpha]$$

für $i \in \{1, \ldots, r\}$ die verschiedenen Primideale von $\mathbb{Z}'[\alpha]$ über p.

Beweis: Auf Grund der Isomorphie aus Lemma 3.3.3 genügt es, die nicht trivialen Primideale von $\mathbb{F}_p[t]/\bar{\mu}_\alpha(t)\mathbb{F}_p[t]$ zu bestimmen.

Die Primideale über $\bar{\mu}_\alpha(t)\mathbb{F}_p[t]$ des Hauptidealrings $\mathbb{F}_p[t]$ werden durch die irreduziblen Teiler von $\bar{\mu}_\alpha$ in $\mathbb{F}_p[t]$ erzeugt. Die einzigen irreduziblen Teiler von $\bar{\mu}_\alpha$ sind $\bar{\mu}_1, \ldots, \bar{\mu}_r$. Das heißt, $\bar{\mu}_1(t)\mathbb{F}_p[t], \ldots, \bar{\mu}_r(t)\mathbb{F}_p[t]$ sind alle Primideale von $\mathbb{F}_p[t]$ über $\bar{\mu}_\alpha(t)\mathbb{F}_p[t]$. Alle nicht trivialen Primideale von $\mathbb{F}_p[t]/\bar{\mu}_\alpha(t)\mathbb{F}_p[t]$ sind somit $\bar{\mu}_1(t) + \bar{\mu}_\alpha(t)\mathbb{F}_p[t], \ldots, \bar{\mu}_r(t) + \bar{\mu}_\alpha(t)\mathbb{F}_p[t]$. Wir erhalten daraus alle Primideale von $\mathbb{Z}'[\alpha]$ über $p\mathbb{Z}'[\alpha]$

$$\mathfrak{p}_i = \mu_i(\alpha)\mathbb{Z}'[\alpha] + p\mathbb{Z}'[\alpha].$$

Die Beziehung $p\mathbb{Z}'[\alpha] = \mathfrak{p}_1^{e_1} \cdot \ldots \cdot \mathfrak{p}_r^{e_r}$ ergibt sich aus der Zerlegung $\bar{\mu}_\alpha = \bar{\mu}_1^{e_1} \cdot \ldots \cdot \bar{\mu}_r^{e_r}$ in $\mathbb{F}_p[t]$ und dem daraus folgenden Produkt $0 + \bar{\mu}_\alpha\mathbb{F}_p[t] = (\bar{\mu}_1(t) + \bar{\mu}_\alpha(t)\mathbb{F}_p[t])^{e_1} \cdot \ldots \cdot (\bar{\mu}_r(t) + \bar{\mu}_\alpha(t)\mathbb{F}_p[t])^{e_r}$ in $\mathbb{F}_p[t]/\bar{\mu}_\alpha(t)\mathbb{F}_p[t]$. $\square$

Für primäre Elemente stellt sich die Primidealstruktur in der Gleichungsordnung besonders einfach dar.

Korollar 3.3.5 *Sei $\alpha \in \mathfrak{o}'_f$ primär mit $\mathcal{A}_f = \mathbb{Q}(\alpha)$. Dann gilt*

$$p\mathbb{Z}'[\alpha] = \mathfrak{p}^{E_\alpha}$$

mit

$$\mathfrak{p} = \nu_\alpha(\alpha)\mathbb{Z}'[\alpha] + p\mathbb{Z}'[\alpha] = \mathcal{J}'_p \cap \mathbb{Z}'[\alpha]$$

dem einzigen Primideal in $\mathbb{Z}'[\alpha]$.

Bemerkung 3.3.6 *Wir erhalten damit für primäre α die Isomorphie*

$$\mathbb{Z}'[\alpha]/(\mathcal{J}'_p \cap \mathbb{Z}'[\alpha]) \cong \mathbb{F}_p[t]/\bar{\nu}_\alpha(t)\mathbb{F}_p[t].$$

Nach Satz 2.3.3 über die Fortsetzungen diskreter Bewertungen stimmen somit alle nicht trivialen Bewertungen, deren Bewertungsring p enthält, auf der Gleichungsordnung von α überein.

$$v_p^{(1)}|_{\mathbb{Z}'[\alpha]} = \ldots = v_p^{(r)}|_{\mathbb{Z}'[\alpha]} \tag{3.2}$$

Für die v_p^*-Bewertung erhalten wir die Gleichheit

$$v_p^*|_{\mathbb{Z}'[\alpha]} = v_p^{(i)}|_{\mathbb{Z}'[\alpha]}$$

für alle $i \in \{1, \ldots, r\}$. Damit hat die v_p^*-Bewertung auf der Gleichungsordnung eines primären Elements die Eigenschaften einer nichtarchimedischen Bewertung. Ist α ein primitives primäres Element der Algebra $\mathcal{A}_f$, so erhalten wir für alle Elemente β aus der Gleichungsordnung von α, welche zusätzlich noch im p-Radikal liegen die Abschätzung

$$v_p^*(\beta) \geq \frac{1}{E_\alpha}$$

der v_p^*-Bewertung von β nach unten. Für ein primäres α seien L_α und M_α definiert durch $v_p^*(\nu_\alpha(\alpha)) = \frac{L_\alpha}{M_\alpha}$ mit $\mathrm{ggT}(L_\alpha, M_\alpha) = 1$ und $M_\alpha > 0$. Die Größe M_α wird für die Termination des Algorithmus von Bedeutung sein. Da $\nu_\alpha(\alpha)$ nach Korollar 3.3.5 in $\mathcal{J}'_p \cap \mathbb{Z}'[\alpha]$ liegt, bekommen wir für den Nenner M_α die Abschätzung

$$v_p^*(\nu_\alpha(\alpha)) = \frac{L_\alpha}{M_\alpha} \geq \frac{1}{E_\alpha} \quad \Longrightarrow \quad M_\alpha \leq E_\alpha L_\alpha. \tag{3.3}$$

Später können wir zeigen, daß M_α schon durch E_α beschränkt ist.

Durch D_α und M_α werden wir jetzt zwei Elemente charakterisieren, deren Gleichungsordnung maximal ist.

Definition und Satz 3.3.7 *Sei $\alpha \in \mathfrak{o}'_f$ primär mit*

(i) $\mathrm{Grad}(\mu_\alpha) = n$

(ii) $v_p^*(\nu_\alpha(\alpha)) = \frac{1}{E_\alpha} \neq 1$,

dann heißt α **Eisenstein Element** *zu p.*
Für ein Eisenstein Element ist die Gleichungsordnung maximal.

Beweis: Die Anwendung des Dedekind Kriteriums liefert die Behauptung, falls der

$$\mathrm{ggT}_p\left(\frac{\mu_\alpha(t)-\nu_\alpha(t)^{E_\alpha}}{p}, \nu_\alpha(t)^{E_\alpha-1}\right)$$

eine Konstante ist. Sei $h(t) := \frac{\mu_\alpha(t)-\nu_\alpha^{E_\alpha}(t)}{p}$. Das Polynom h hat Koeffizienten aus $\mathbb{Z}'$, da nach (i) $\mu_\alpha = \chi_\alpha$ und χ_α kongruent $\nu_\alpha^{E_\alpha}$ modulo $p\mathbb{Z}'[t]$ ist. Der größte gemeinsame Teiler von h und $\nu_\alpha^{E_\alpha-1}$ über $\mathbb{F}_p$ ist auf Grund der Irreduzibilität von ν_α genau dann keine Konstante, wenn ν_α ein Teiler von h ist. Nach Bemerkung 3.3.6 gilt

$$\mathbb{Z}'[\alpha]/(\mathcal{J}_p' \cap \mathbb{Z}'[\alpha]) \cong \mathbb{F}_p[t]/\bar{\nu}_\alpha[t].$$

Das heißt, das Element $h(\alpha)$ liegt in dem p-Radikal von $\mathbb{Z}'[\alpha]$, wenn der größte gemeinsame Teiler von h und $\nu_\alpha^{E_\alpha-1}$ über $\mathbb{F}_p$ keine Konstante ist. Insbesondere muß die v_p^*-Bewertung von $h(\alpha)$ dann echt größer als Null sein. Bestimmen wir also die v_p^*-Bewertung von $h(\alpha)$.

$$\begin{aligned}
v_p^*(h(\alpha)) &= v_p^*(\mu_\alpha(\alpha)-\nu_\alpha(\alpha)^{E_\alpha})-1\\
&= E_\alpha v_p^*(\nu_\alpha(\alpha))-1\\
&= E_\alpha\frac{1}{E_\alpha}-1 \quad \text{wegen (ii)}\\
&= 0
\end{aligned}$$

$h(\alpha)$ liegt also nicht in dem p-Radikal von $\mathbb{Z}'[\alpha]$, und der größte gemeinsame Teiler von h und $\nu_\alpha^{E_\alpha-1}$ über $\mathbb{F}_p$ kann nur eine Konstante sein. □

Definition und Satz 3.3.8 *Sei $\alpha \in \mathfrak{o}_f'$ primär mit*

(i) $\mathrm{Grad}(\mu_\alpha) = n$

(ii) $D_\alpha = \mathrm{Grad}(\nu_\alpha) = n$,

dann heißt α ein **Berwick Element** *zu p.*
Für ein Berwick Element ist die Gleichungsordnung maximal.

Beweis: Als Beweisansatz soll wiederum das Dedekind Kriterium herangezogen werden. Aus (i) folgt wieder $\mu_\alpha = \chi_\alpha$ und somit gilt mit (ii)

$$\mu_\alpha \equiv \nu_\alpha \cdot 1 \mod p\mathbb{Z}'[t].$$

Das heißt, es ist der

$$\mathrm{ggT}_p\left(\frac{\mu_\alpha(t)-\nu_\alpha(t)}{p}, 1\right)$$

zu bestimmen. Die Behauptung folgt sofort. □

Wie sich in den letzten beiden Sätzen zeigte, spielen die primären, $\mathcal{A}_f$ erzeugenden, ganzen Elemente α mit $v_p^*(\nu_\alpha(\alpha)) = \frac{1}{E_\alpha}$ beziehungsweise $\mathrm{Grad}(\nu_\alpha) = \mathrm{Grad}(\mu_\alpha)$ eine besondere Rolle.

In der Tat bildet die Suche nach einem Berwick oder Eisenstein Element die Grundlage des Kernalgorithmus. Die Suche erfolgt dabei im wesentlichen in zwei geschachtelten Transformationen. Immer vorausgesetzt, wir stoßen nicht auf ein nicht primäres Element, so wird im ersten Schritt aus dem aktuellen Element ein $\mathcal{A}_f$ erzeugendes Element α mit $v_p^*(\nu_\alpha(\alpha)) = \frac{1}{M_\alpha}$ konstruiert. Im zweiten Schritt wird mit α ein neues Element gesucht, welches einem Eisenstein beziehungsweise Berwick Element näher kommt.

Stoßen wir auf kein nicht primäres Element, so erhalten wir nach endlich vielen Transformationen ein Eisenstein oder Berwick Element. Leider handelt es sich bei der Suche nicht um ein gezieltes Vorgehen. Der Algorithmus konstruiert eine Folge von ganzen Elementen, von der sichergestellt ist, daß nach endlich vielen Schritten ein Eisenstein, Berwick oder nicht primäres Element auftritt.

Die benötigten Sätze und Konstruktionen sollen im folgenden entwickelt werden.

Normierung von α

Ein primäres Element $\alpha \in \mathfrak{o}'_f$ heißt **normiert**, wenn für die v_p^*-Bewertung von $\nu_\alpha(\alpha)$ gilt
$$v_p^*(\nu_\alpha(\alpha)) = \frac{1}{M_\alpha}.$$
Wir wollen zeigen, daß zu einem beliebigen primären $\alpha \in \mathfrak{o}'_f$ ein normiertes $\tilde{\alpha}$ existiert mit
$$\alpha \equiv \tilde{\alpha} \mod \mathcal{J}'_p.$$
Nach Korollar 3.3.2 gilt damit insbesondere, daß als p-Minimalpolynom von $\tilde{\alpha}$ das Polynom ν_α gewählt werden kann.

Satz 3.3.9 *Sei α aus $\mathcal{A}_f$ primär und $\eta_\alpha := \frac{\nu_\alpha(\alpha)^k}{p^l}$ mit $k, l \in \mathbb{N}$, $kL_\alpha - lM_\alpha = 1$, so liegt η_α in $\mathcal{J}'_p$, und $\tilde{\alpha} := \alpha + \eta_\alpha$ ist normiert mit $M_{\tilde{\alpha}} = M_\alpha$.*

Beweis:

Behauptung 1: $\eta_\alpha \in \mathcal{J}'_p$

Wir zeigen, daß $v_p^*(\eta_\alpha)$ größer als Null ist.

$$\begin{aligned}
v_p^*(\eta_\alpha) &= \min_{i\in\{1,\dots,r\}} v_p^{(i)}\left(\frac{\nu_\alpha(\alpha)^k}{p^l}\right)\\
&= \min_{i\in\{1,\dots,r\}} \{k v_p^{(i)}(\nu_\alpha(\alpha)) - l v_p^{(i)}(p)\}\\
&= \min_{i\in\{1,\dots,r\}} k v_p^{(i)}(\nu_\alpha(\alpha)) - l\\
&= k\frac{L_\alpha}{M_\alpha} - l\\
&= \frac{kL_\alpha - lM_\alpha}{M_\alpha}\\
&= \frac{1}{M_\alpha}\\
&> 0
\end{aligned}$$

Behauptung 2: $v_p^*(\nu_{\tilde\alpha}(\tilde\alpha)) = \frac{1}{M_\alpha}$

Nach Korollar 3.3.2 und Behauptung 1 ist $\nu_{\tilde\alpha} = \nu_\alpha$ wählbar. Betrachten wir für

$$\nu_{\tilde\alpha}(\tilde\alpha) = \nu_\alpha(\tilde\alpha) = \nu_\alpha(\alpha + \eta_\alpha)$$

die formale Taylorentwicklung

$$\nu_\alpha(\alpha + \eta_\alpha) = \nu_\alpha(\alpha) + \eta_\alpha \nu'_\alpha(\alpha) + \eta_\alpha^2 h(\alpha, \eta_\alpha)$$

mit $h(x,y) \in \mathbb{Z}'[x,y]$. Wir können summandenweise auswerten und erhalten als $v_p^*(\nu_{\tilde\alpha}(\tilde\alpha))$ das Minimum der v_p^*-Bewertungen der Summanden, falls es nicht von zwei Summanden gleichzeitig angenommen wird.

$$\begin{aligned}
v_p^*(\nu_\alpha(\alpha)) &= \frac{L_\alpha}{M_\alpha} > \frac{1}{M_\alpha}\\
v_p^*(\eta_\alpha \nu'_\alpha(\alpha)) &= \min_{i\in\{1,\dots,r\}} \{v_p^{(i)}(\eta_\alpha) + v_p^{(i)}(\nu'_\alpha(\alpha))\}\\
&= \min_{i\in\{1,\dots,r\}} v_p^{(i)}(\eta_\alpha)\\
&= v_p^*(\eta_\alpha)\\
&= \frac{1}{M_\alpha} \qquad \text{nach Behauptung 1}
\end{aligned}$$

Die zweite Gleichheit für $v_p^*(\eta_\alpha \nu'_\alpha(\alpha))$ gilt, da nach Satz 3.3.5 $\mathbb{Z}'[\alpha] \cap \mathcal{J}'_p = \nu_\alpha(\alpha)\mathbb{Z}'[\alpha] + p\mathbb{Z}'[\alpha]$ ist, also $\nu'_\alpha(\alpha)$ nicht in $\mathbb{Z}'[\alpha] \cap \mathcal{J}'_p$ liegen kann. Damit folgt $v_p^{(i)}(\nu'_\alpha(\alpha)) = 0$ für alle $i \in \{1,\dots,r\}$, denn nach Satz 3.3.5 ist $\mathbb{Z}'[\alpha] \cap \mathcal{J}'_p$ das einzige nicht triviale Primideal von $\mathbb{Z}'[\alpha]$.

$$\begin{aligned} v_p^*(\eta_\alpha^2 h(\alpha,\eta_\alpha)) &\geq v_p^*(\eta_\alpha^2) + v_p^*(h(\alpha,\eta_\alpha)) \\ &= \frac{2}{M_\alpha} + v_p^*(h(\alpha,\eta_\alpha)) \\ &\geq \frac{2}{M_\alpha} \end{aligned}$$

Das Minimum der Bewertungen wird nur von dem zweiten Summanden angenommen, für die v_p^*-Bewertung von $\nu_{\tilde{\alpha}}(\tilde{\alpha})$ erhalten wir somit $\frac{1}{M_\alpha}$. □

Aus dem Satz können wir sofort die schon erwähnte Verschärfung der Abschätzung (3.3) von M_α ableiten. Nach Korollar 3.3.1 ist wegen $\tilde{\alpha} \equiv \alpha \mod \mathcal{J}_p'$ insbesondere $E_{\tilde{\alpha}} = E_\alpha$. Für M_α erhalten wir damit aus $M_\alpha = M_{\tilde{\alpha}} \leq E_{\tilde{\alpha}} L_{\tilde{\alpha}} = E_{\tilde{\alpha}}$ die Abschätzung

$$M_\alpha \leq E_\alpha. \tag{3.4}$$

Annäherung an die Eisenstein Element Schranke

Als zweites soll gezeigt werden, wie man aus zwei normierten, primären Elementen ein neues ganzes Element gewinnen kann, welches näher an der Eisenstein Element Schranke 3.3.7 (ii) liegt, ohne sich von der Berwick Element Schranke 3.3.8 (ii) entfernt zu haben.

Satz 3.3.10 *Seien α, β primäre, normierte Elemente von $\mathcal{A}_f$ mit $M_\beta \nmid M_\alpha$. Setze $\psi := \frac{\eta_\alpha^k \eta_\beta^l}{p^m}$ mit η_α, η_β wie in Satz 3.3.9 definiert und $k, l, m \in \mathbb{Z}^{\geq 0}$ so, daß $\mathrm{ggT}(M_\alpha, M_\beta) = lM_\alpha + kM_\beta - mM_\alpha M_\beta$ ist. Dann liegt ψ in $\mathcal{J}_p'$, und $\tilde{\alpha} := \alpha + \psi$ ist primär und normiert mit $M_{\tilde{\alpha}} = \mathrm{kgV}(M_\alpha, M_\beta)$.*

Beweis:

BEHAUPTUNG 1: $\psi \in \mathcal{J}_p'$

Wir zeigen, daß $v_p^*(\psi)$ größer als Null ist. α und β sind primär. Nach (3.2) gelten somit die Gleichungen $v_p^{(1)}(\nu_\alpha(\alpha)) = \ldots = v_p^{(r)}(\nu_\alpha(\alpha)) = v_p^*(\nu_\alpha(\alpha))$ und $v_p^{(1)}(\nu_\beta(\beta)) = \ldots = v_p^{(r)}(\nu_\beta(\beta)) = v_p^*(\nu_\beta(\beta))$. Entsprechend der Konstruktion von η_α beziehungsweise η_β ist dann ebenfalls $v_p^{(i)}(\eta_\alpha) = v_p^*(\eta_\alpha)$ und $v_p^{(i)}(\eta_\beta) = v_p^*(\eta_\beta)$

für alle $i \in \{1, \ldots, r\}$ erfüllt und wir erhalten für $v_p^*(\psi)$.

$$\begin{aligned}
v_p^*(\psi) &= v_p^*\left(\frac{\eta_\alpha^k \eta_\beta^l}{p^m}\right) \\
&= \min_{i \in \{1,\ldots,r\}} \{k v_p^{(i)}(\eta_\alpha) + l v_p^{(i)}(\eta_\beta) - m v_p^{(i)}(p)\} \\
&= k v_p^*(\eta_\alpha) + l v_p^*(\eta_\beta) - m v_p^*(p) \\
&= \frac{l M_\alpha + k M_\beta - m M_\alpha M_\beta}{M_\alpha M_\beta} \\
&= \frac{\mathrm{ggT}(M_\alpha, M_\beta)}{M_\alpha M_\beta} \\
&= \frac{1}{\mathrm{kgV}(M_\alpha, M_\beta)} \\
&> 0
\end{aligned}$$

α ist somit kongruent $\tilde{\alpha} := \alpha + \psi$ modulo dem p-Radikal von $\mathfrak{o}'_f$. Nach Korollar 3.3.2 kann als p-Minimalpolynom von $\tilde{\alpha}$ das p-Minimalpolynom von α gewählt werden.

Behauptung 2: $v_p^*(\nu_{\tilde{\alpha}}(\tilde{\alpha})) = \frac{1}{\mathrm{kgV}(M_\alpha, M_\beta)}$
Der Beweis erfolgt analog zu Behauptung 2 von Satz 3.3.9 über die formale Taylorreihe von $\nu_\alpha(\alpha + \psi)$. Sei

$$\nu_\alpha(\alpha + \psi) = \nu_\alpha(\alpha) + \psi \nu'_\alpha(\alpha) + \psi^2 h(\alpha, \psi)$$

mit $h(x, y) \in \mathbb{Z}'[x, y]$ die formale Taylorentwicklung von $\nu_\alpha(\alpha + \psi)$. Betrachten wir wieder die v_p^*-Bewertung der Summanden.

$$\begin{aligned}
v_p^*(\nu_\alpha(\alpha)) &= \frac{1}{M_\alpha} > \frac{1}{\mathrm{kgV}(M_\alpha, M_\beta)} \\
v_p^*(\psi \nu'_\alpha(\alpha)) &= \min_{i \in \{1,\ldots,r\}} \{v_p^{(i)}(\psi) + v_p^{(i)}(\nu'_\alpha(\alpha))\} \\
&= v_p^*(\psi) \\
&= \frac{1}{\mathrm{kgV}(M_\alpha, M_\beta)}.
\end{aligned}$$

Die zweite Gleichheit erhalten wir aus Satz 3.3.5. Danach ist wieder $\mathbb{Z}'[\alpha] \cap \mathcal{J}'_p = \nu_\alpha(\alpha)\mathbb{Z}'[\alpha] + p\mathbb{Z}'[\alpha]$, das heißt, $\nu'_\alpha(\alpha)$ liegt nicht in $\mathbb{Z}'[\alpha] \cap \mathcal{J}'_p$. Für alle $i \in \{1, \ldots, r\}$ gilt somit $v_p^{(i)}(\nu'_\alpha(\alpha)) = 0$.

$$\begin{aligned}
v_p^*(\psi^2 h(\alpha, \psi)) &\geq 2 v_p^*(\psi) + v_p^*(h(\alpha, \psi)) \\
&\geq \frac{2}{M_\alpha}
\end{aligned}$$

Das Minimum der Bewertungen wird nur von dem zweiten Summanden angenommen, und wir erhalten

$$v_p^*(\tilde{\alpha}) = \frac{1}{\mathrm{kgV}(M_\alpha, M_\beta)}.$$

□

Wichtig für die Termination des Algorithmus ist, daß aus der Kongruenz $\tilde{\alpha} \equiv \alpha \mod \mathcal{J}'_p$ nach Korollar 3.3.2 die Gleichheit $D_{\tilde{\alpha}} = D_\alpha$ folgt. Wir können also näher an die Eisenstein Element Schranke rücken, ohne uns von der Berwick Element Schranke zu entfernen.

Annäherung an die Berwick Element Schranke

Analog zur Eisenstein Element Schranke wollen wir eine Methode entwickeln, mit der man aus zwei primären Elementen ein neues ganzes Element konstruieren kann, welches näher an der Berwick Element Schranke 3.3.8 (ii) liegt.

Satz 3.3.11 *Seien $\alpha, \beta \in \mathfrak{o}'_f \backslash \mathcal{J}'_p$ normiert, primär und $D_\beta \nmid D_\alpha$. Dann existieren Polynome $P_1, P_2 \in \mathbb{Z}'[t]$ mit $\mathrm{Grad}(P_1) < D_\alpha, \mathrm{Grad}(P_2) < D_\beta$, und die Koeffizienten von P_1, P_2 sind reduziert modulo p, so daß für*

$$\tilde{\alpha} := P_1(\alpha) + P_2(\beta)$$

eine der folgenden Aussagen gilt

- *$\tilde{\alpha}$ ist primär und $\mathrm{Grad}(\nu_{\tilde{\alpha}}) > \mathrm{Grad}(\nu_\alpha)$*
- *$\tilde{\alpha}$ ist nicht primär.*

Beweis: Wir unterscheiden zwei Fälle.

1. Fall: $\mathcal{L} := \mathbb{Z}'[\alpha, \beta]/(\mathbb{Z}'[\alpha, \beta] \cap \mathcal{J}'_p)$ ist ein Körper.

Sei $\mathfrak{P}$ das maximale Ideal $\mathbb{Z}'[\alpha, \beta] \cap \mathcal{J}'_p$ von $\mathbb{Z}'[\alpha, \beta]$. Nach Voraussetzung sind α und β primär, das heißt, $\mathfrak{p}_\alpha := \mathbb{Z}'[\alpha] \cap \mathcal{J}'_p$ und $\mathfrak{p}_\beta := \mathbb{Z}'[\beta] \cap \mathcal{J}'_p$ sind maximale Ideale von $\mathbb{Z}'[\alpha]$ beziehungsweise $\mathbb{Z}'[\beta]$, somit sind $\mathcal{K}_\alpha := \mathbb{Z}'[\alpha]/\mathfrak{p}_\alpha$ sowie $\mathcal{K}_\beta := \mathbb{Z}'[\beta]/\mathfrak{p}_\beta$ Körper. Die Abbildungen $\varphi_i : \mathcal{K}_i \longrightarrow \mathcal{L}; \; x + \mathfrak{p}_i \mapsto x + \mathfrak{P}$ sind Injektionen von $\mathcal{K}_i$ in $\mathcal{L}$ für $i \in \{\alpha, \beta\}$. Denn wegen $\mathfrak{p}_i \subseteq \mathfrak{P}$ ist φ_i wohldefiniert. Der Schnitt von $\mathfrak{P}$ mit der Gleichungsordnung von α ist $\mathfrak{P} \cap \mathbb{Z}'[\alpha] = \mathcal{J}'_p \cap \mathbb{Z}'[\alpha] = \mathfrak{p}_\alpha$ das Primideal $\mathfrak{p}_\alpha$, das heißt $\varphi_\alpha(a) = \varphi_\alpha(b)$ genau dann, wenn $a = b$ für beliebige a, b aus $\mathcal{K}_\alpha$. φ_α ist also injektiv. Analog folgt, daß φ_β injektiv ist. Wir können $\mathcal{K}_\alpha$ und $\mathcal{K}_\beta$ als Teilkörper von $\mathcal{L}$ auffassen.

$\mathcal{K}_\alpha$ und $\mathcal{K}_\beta$ sind nach Lemma 3.3.3 endliche Körper mit p^{D_α} beziehungsweise p^{D_β} Elementen. Der Körper $\mathcal{L}$ muß somit auch den endlichen Körper mit $p^{\mathrm{kgV}(D_\alpha,D_\beta)}$ Elementen enthalten. Da endliche Körper einfach sind, existiert ein Element $\tilde{\alpha}+\mathfrak{P}$, welches über dem Primkörper $\mathbb{F}_p$ einen $p^{\mathrm{kgV}(D_\alpha,D_\beta)}$–elementigen Teilkörper von $\mathcal{L}$ erzeugt. Der Repräsentant $\tilde{\alpha}$ von $\tilde{\alpha}+\mathfrak{P}$ ist in der Form $P_1(\alpha)+P_2(\beta)$ mit Polynomen P_1, P_2 der geforderten Art wählbar. Ist $\tilde{\alpha}$ primär, so muß wegen der Voraussetzung $D_\beta \nmid D_\alpha$ der Wert $D_{\tilde{\alpha}} = \mathrm{kgV}(D_\alpha, D_\beta)$ größer als D_α sein.

2. Fall: $\mathbb{Z}'[\alpha,\beta]/(\mathbb{Z}'[\alpha,\beta]\cap\mathcal{J}_p')$ ist kein Körper.
Sei $\mathfrak{A}$ das nicht maximale Ideal $\mathbb{Z}'[\alpha,\beta]\cap\mathcal{J}_p'$. Wir betrachten wieder die Abbildung $\varphi : \mathbb{Z}'[\alpha]/\mathfrak{p} \longrightarrow \mathbb{Z}'[\alpha,\beta]/\mathfrak{A}$, wobei $\mathfrak{p}$ das maximale Ideal $\mathcal{J}_p' \cap \mathbb{Z}'[\alpha]$ von $\mathbb{Z}'[\alpha]$ sei. φ ist wie im ersten Fall φ_α wohldefiniert und injektiv. $\mathbb{Z}'[\alpha,\beta]/\mathfrak{A}$ enthält somit den Körper $\varphi(\mathbb{Z}'[\alpha]/\mathfrak{p})$ und ist selbst kein Körper. Es existiert also in $\mathbb{Z}'[\alpha,\beta]/\mathfrak{A}$ ein Element $\tilde{\alpha}+\mathfrak{P}$, dessen charakteristisches Polynom in nicht triviale, koprime Faktoren zerfällt. $\tilde{\alpha}$ kann wieder, wie im ersten Fall, in der Form $P_1(\alpha)+P_2(\beta)$ gewählt werden. □

D. Ford hat in seiner Dissertation [Fo78] für $\tilde{\alpha}$ die Summe $\alpha+\beta$ gewählt. Zu dieser Aussage jedoch keinen vollständigen Beweis angegeben. In seinem Artikel [Fo87] ist er von dieser Wahl wieder abgerückt. Für den speziellen Fall, daß D_α und D_β teilerfremd sind, kann $\tilde{\alpha}=\alpha+\beta$ gesetzt werden. Heuristisch findet sich für $\tilde{\alpha}$ immer ein Kandidat der Gestalt $\alpha+P_2(\beta)$. In den meisten Fällen ist schon $\alpha+\beta$ ein passender Kandidat. Die Effizienz des Algorithmus ist an dieser Stelle nicht auf die theoretische Endlichkeit der Suche zurückzuführen, sondern auf das günstige Verhalten des Algorithmus. Bei größeren Primzahlen würde schon ein notwendiges vollständiges Auszählen der $p^{D_\beta-2}$ vielen Möglichkeiten für die Wahl von $\tilde{\alpha}$ in der Gestalt $\alpha+P_2(\beta)$ zu unbrauchbar langen Rechenzeiten führen.

Die angegebene Konstruktion von $\tilde{\alpha}$ hat leider noch einen weiteren Nachteil, sie erhält uns nicht den Abstand zur Eisenstein Element Schranke. Wir können uns jedoch nach Satz 3.3.10 wieder dorthin vorarbeiten, ohne D_α zu verändern. In Kapitel 5 werden dieses Problem noch einmal aufgreifen.

Finden neuer erzeugender Elemente

Die erste Bedingung an ein Berwick beziehungsweise Eisenstein Element ist, daß das Minimalpolynom maximalen Grad hat. Das heißt, es erzeugt über $\mathbb{Q}$ die ganze Algebra $\mathcal{A}_f$. Wir haben bis jetzt drei Konstruktionen entwickelt, bei denen unser konstruiertes Element immer modulo $\mathcal{J}_p'$ kongruent zum Ausgangselement geblieben ist. Die einzelnen Konstruktionen beeinflussen sich zwar gegenseitig, jedoch nicht zyklisch. Eine analoge Konstruktion fehlt uns jetzt noch, um aus einem beliebigen ganzen Element ein modulo $\mathcal{J}_p'$ kongruentes, den ganzen Körper über $\mathbb{Q}$ erzeugendes Element zu berechnen. Die vier Konstruktionen zusammen dürfen ebenfalls nicht die bisher erreichten Eigenschaften des betrachteten Elements so verändern, daß es zu einem Konstruktions – Zerstörungs Zyklus kommt. Zunächst müssen wir wieder die Kongruenz modulo $\mathcal{J}_p'$ erhalten, um den Abstand zur Berwick Element Schranke nicht zu verlieren. Desweiteren sollte unser neues Element normiert sein, um nicht in einen Zyklus mit der Normierung zu gelangen.

Satz 3.3.12 *Seien $\xi \in \mathfrak{o}_f'$ mit $\mathcal{A}_f = \mathbb{Q}(\xi)$ und $\alpha \in \mathfrak{o}_f'$ sowie $\kappa \in \{1, 2\}$ beliebig. Dann existiert ein $k \in \mathbb{Z}$, so daß für $q := p^\kappa$ gilt*

$$\tilde{\alpha} := \alpha + qk\xi$$

erzeugt über $\mathbb{Q}$ die ganze Algebra $\mathcal{A}_f$.

Beweis: Wir werden zeigen, daß es nur endlich viele $k \in \mathbb{Z}^{\geq 0}$ gibt, für die $\tilde{\alpha}$ kein primitives Element der Algebra ist.

1. FALL: Sei f irreduzibel. Die Algebra $\mathcal{A}_f$ ist also ein Körper. Wir zeigen, daß für ein beliebiges Element α aus $\mathbb{Q}(\xi)$ nur für endlich viele $k \in \mathbb{Z}^{\geq 0}$ das Element $\alpha + qk\xi$ über $\mathbb{Q}$ nicht den ganzen Körper erzeugt. Seien $\sigma_1, \ldots, \sigma_n$ die verschiedenen $\mathbb{Q}$-Isomorphismen von $\mathbb{Q}(\xi)$ in einen algebraischen Abschluß von $\mathbb{Q}(\xi)$. Wir müssen zeigen, daß es nur für endlich viele $k \in \mathbb{Z}$ Indizes $i \neq j$ aus $\{1, \ldots, n\}$ mit $\sigma_i(\alpha + kq\xi) = \sigma_j(\alpha + kq\xi)$ geben kann. Dazu konstruieren wir ein Polynom, welches genau dann in qk eine Nullstelle hat, wenn es Indizes mit obiger Eigenschaft gibt. Definieren wir das Hilfspolynom

$$h(t) := \prod_{i \neq j} (\, \sigma_i(\alpha) - t\sigma_i(\xi) - [\sigma_j(\alpha) - t\sigma_j(\xi)]\,),$$

so ist h nicht das Nullpolynom. Nehmen wir nun an, ein Faktor für $i \neq j$ wäre identisch Null

$$0 = t(\sigma_j(\xi) - \sigma_i(\xi)) + \sigma_i(\alpha) - \sigma_j(\alpha),$$

so muß insbesondere

$$\sigma_i(\xi) = \sigma_j(\xi)$$

gelten, was nur für $i = j$ möglich ist. Das steht im Widerspruch zur Voraussetzung $i \neq j$. Sei $N := \{l \in \mathbb{N} \,|\, h(lq) = 0\}$ die Menge der Nullstellen von h der Form lq. N ist, als Teilmenge der Nullstellenmenge eines Polynoms ungleich Null, endlich. Sei $k \in \mathbb{Z} \backslash N$ beliebig. Dann ist $h(kq)$ ungleich Null, das heißt, alle Faktoren von

h sind von Null verschieden. Wir erhalten also für alle $i \neq j \in \{1, \ldots, n\}$ die Ungleichungen

$$\begin{aligned} \sigma_i(\alpha) - kq\sigma_i(\xi) &\neq \sigma_j(\alpha) - kq\sigma_j(\xi) \\ \sigma_i(\alpha - kq\xi) &\neq \sigma_j(\alpha - kq\xi). \end{aligned}$$

Die Konjugierten von $\tilde{\alpha} := \alpha - kq\xi \in \mathbb{Q}(\xi)$ sind alle verschieden, das heißt, der durch $\tilde{\alpha}$ erzeugte Teilkörper von $\mathbb{Q}(\xi)$ hat den gleichen Grad über $\mathbb{Q}$ wie $\mathbb{Q}(\xi)$. Die Körper $\mathbb{Q}(\xi)$ und $\mathbb{Q}(\tilde{\alpha})$ müssen also gleich sein.

2. FALL: Sei f nicht irreduzibel. Die Algebra $\mathcal{A}_f$ ist somit die innere direkte Summe $+_{i=1}^{s}\mathcal{A}_i$ von Körpern. Wir müssen zeigen, daß nur für endlich viele $k \in \mathbb{Z}^{\geq 0}$ das Element $\alpha(k) := \alpha + qk\xi$ über $\mathbb{Q}$ nicht die ganze Algebra $\mathcal{A}_f$ erzeugt. Zu einem beliebigen Element β aus $\mathcal{A}_f$ sei β_i die Projektion von β auf $\mathcal{A}_i$. Das charakteristische Polynom χ_β ist nach Satz 1.3.7 das Produkt der charakteristischen Polynome χ_{β_i} der β_i in $\mathcal{A}_i$. Seien $N_1, \ldots, N_s$ die endlichen Teilmengen von $\mathbb{Z}^{\geq 0}$ entsprechend FALL 1 für die das Element $\alpha_i(k) = \alpha_i + qk\xi_i$ nicht den Körper $\mathcal{A}_i$ erzeugt. Dann ist für ein beliebiges k aus $\mathbb{Z}^{\geq 0} \setminus \bigcup_{i=1}^{s} N_i$ das Minimalpolynom von $\alpha(k)$ gleich dem kleinsten gemeinsamen Vielfachen der Polynome $\chi_{\alpha_1(k)}, \ldots, \chi_{\alpha_s(k)}$. Wir müssen also zeigen, daß nochmals höchstens für endlich viele k aus $\mathbb{Z}^{\geq 0} \setminus \bigcup_{i=1}^{s} N_i$ der größte gemeinsame Teiler der Polynome $\chi_{\alpha_1(k)}, \ldots, \chi_{\alpha_s(k)}$ keine Konstante ist.

Betrachten wir den Körper $\mathbb{Q}(\xi_1, \ldots, \xi_s)$, wobei ξ_i eine Nullstelle des irreduziblen Faktors f_i ist. Für die Diskriminante des Polynoms $g := \chi_{\alpha_1(k)} \cdot \ldots \cdot \chi_{\alpha_s(k)}$ erhalten wir bis auf das Vorzeichen das Produkt

$$\prod_{i \neq j} \prod_{\substack{1 \leq l \leq n_i \\ 1 \leq m \leq n_j}} \left(\alpha_i^{(l)}(k) - \alpha_j^{(m)}(k)\right) \prod_{1 \leq i \leq s} \prod_{\substack{l \neq m \\ 1 \leq l, m \leq n_i}} \left(\alpha_i^{(l)}(k) - \alpha_i^{(m)}(k)\right),$$

wobei n_i der Grad des charakteristischen Polynoms von $\alpha_i(k)$ ist. Das zweite Doppelprodukt ist ungleich Null, da k in keiner der endlichen Ausnahmemengen N_i liegt. Die Polynomdiskriminante ist somit genau dann gleich Null, wenn das erste Produkt gleich Null ist. Sei

$$\begin{aligned} h(k) &:= \prod_{i \neq j} \prod_{\substack{1 \leq l \leq n_i \\ 1 \leq m \leq n_j}} \left(\alpha_i^{(l)}(k) - \alpha_j^{(m)}(k)\right) \\ &= \prod_{i \neq j} \prod_{\substack{1 \leq l \leq n_i \\ 1 \leq m \leq n_j}} \left(\alpha_i^{(l)} - \alpha_j^{(m)} + kq(\xi_i^{(l)} - \xi_j^{(m)})\right). \end{aligned}$$

Auf Grund der Separabilität unseres Polynoms f ist keiner der Koeffizienten von k im letzten Produkt gleich Null. $h(k)$ ist also ein nicht konstantes Polynom in k und hat somit nur endlich viele Nullstellen. $\chi_{\alpha(k)}$ ist also nur für endlich viele $k \in \mathbb{Z}^{\geq 0} \setminus \bigcup_{i=1}^{s} N_i$ nicht separabel. Sei nun $k \in \mathbb{Z}^{\geq 0} \setminus \bigcup_{i=1}^{s} N_i$ so gewählt, daß $\chi_{\alpha(k)}$ separabel ist. Dann ist das kleinste gemeinsame Vielfache der Polynome $\chi_{\alpha_1(k)}, \ldots, \chi_{\alpha_s(k)}$ gleich dem Produkt dieser Polynome. Das Minimalpolynom von $\tilde{\alpha} := \alpha(k)$ hat also den gleichen Grad wie f und $\tilde{\alpha}$ muß ein primitives Element der Algebra sein. □

In Satz 3.3.12 haben wir uns die Möglichkeiten, α modulo $p\mathbb{Z}'[\xi]$ oder modulo $p^2\mathbb{Z}'[\xi]$ abzuändern, offen gehalten. Wofür benötigen wir diese Wahlfreiheit? Im voraus hatten wir uns überlegt, daß unser neues erzeugendes Element $\tilde{\alpha}$ normiert sein soll, wenn α normiert ist. Bestimmen wir also $L_{\tilde{\alpha}}$ und $M_{\tilde{\alpha}}$. Analog zum Beweis von Satz 3.3.9 betrachten wir dazu die formale Taylorentwicklung $\nu_\alpha(\alpha) + qk\xi\nu'_\alpha(\alpha) + (qk\xi)^2 h(\alpha, qk\xi)$ von $\nu_{\alpha+qk\xi}(\alpha + qk\xi) = \nu_\alpha(\alpha + qk\xi)$ mit $h(x,y) \in \mathbb{Z}'[x,y]$. Unser Ausgangselement α soll normiert sein, das heißt $v_p^*(\nu_\alpha(\alpha)) = \frac{1}{M_\alpha}$. Wenn nun $\tilde{\alpha}$ ebenfalls normiert sein soll mit $M_\alpha = M_{\tilde{\alpha}}$, so müssen der zweite und der dritte Summand der Taylorentwicklung eine v_p^*-Bewertung echt größer als $\frac{1}{M_\alpha}$ haben. Das heißt, $v_p^*(qk\xi\nu'_\alpha(\alpha)) = v_p^*(qk\xi)$ muß größer als $\frac{1}{M_\alpha}$ sein. — Da α primär ist, liegt $\nu'_\alpha(\alpha)$ nicht in $\nu_\alpha(\alpha)\mathbb{Z}'[\alpha] + p\mathbb{Z}'[\alpha] = \mathcal{J}'_p(\mathbb{Z}'[\alpha])$, dem einzigen Primideal von $\mathbb{Z}'[\alpha]$. Für alle i gilt $v_p^{(i)}(\nu'_\alpha(\alpha)) = 0$, und wir erhalten für die v_p^*-Bewertung die Gleichheit $v_p^*(qk\xi\nu'_\alpha(\alpha)) = v_p^*(qk\xi)$. — Für $M_\alpha > 1$ ist das für $q = p$ garantiert, für $M_\alpha = 1$ benötigen wir jedoch $q = p^2$. An dieser Stelle ist die Fordsche Dissertation nicht korrekt.

Technische Hilfssätze

Wir haben jetzt alle wichtigen Konstruktionen für den Algorithmus zusammengestellt. Ausgehend von einem primären, die Algebra erzeugenden Element ξ von $\mathcal{A}_f$ wollen wir eine Folge (φ_i) von primitiven, primären Elementen konstruieren, für deren Folgenglieder entweder $D_{\varphi_i} = D_{\varphi_{i+1}}$ und $M_{\varphi_i} < M_{\varphi_{i+1}}$ oder $D_{\varphi_i} < D_{\varphi_{i+1}}$ gilt. Auf Grund der Diskretheit von $\mathbb{N}$ und der Beschränktheit von D_ξ und E_ξ muß diese Folge nach endlich vielen Schritten ein Berwick, Eisenstein oder nicht primäres Element enthalten, womit wir unser Ziel erreicht hätten. Problematisch ist dabei jedoch, daß in den Sätzen 3.3.10 und 3.3.11 ein weiteres primäres Element mit speziellen Eigenschaften benötigt wird. Das heißt, wir müssen zu jedem φ_i weiterhin eine Folge $(\beta_j^{(i)})$ von ganzen primären Elementen konstruieren, von der wir wissen, daß nach endlich vielen Schritten ein nicht primäres oder ein den Voraussetzungen von Satz 3.3.10 oder 3.3.11 entsprechendes Element erzeugt wird. Der Lösung dieses Problems, welches nicht unmittelbar mit der Strategie des Algorithmus, eine Ganzheitsbasis zu finden, zusammenhängt, wollen wir uns jetzt im letzten Abschnitt zuwenden.

Gegeben ist uns ein primitives, normiertes, primäres Element φ der Algebra $\mathcal{A}_f$. Um näher an die Berwick oder Eisenstein Element Schranke zu kommen, benötigen wir ein weiteres Element. Wie bereits angesprochen wird der Algorithmus eine Folge $(\beta_j^{(i)})$ von ganzen Elementen außerhalb der Gleichnungsordnung von φ mit streng wachsender v_p^*-Bewertung erzeugen. Wir werden zeigen, daß die Elemente außerhalb der Gleichungsordnung von φ eine nach oben beschränkte v_p^*-Bewertung haben. Da wir nach Satz 3.3.9 jedes primäre Element normieren können, die normierten Elemente jedoch eine nach unten durch $\frac{1}{E_\xi}$ beschränkte v_p^*-Bewertung haben, können wir nach endlich vielen Schritten die Folge der $(\beta_j^{(i)})$ nicht fortsetzen. Das heißt, wir müssen an einer der Terminationsstellen nach endlich vielen konstruierten Folgengliedern $\beta_j^{(i)}$ ein passendes Element gefunden haben.

Zunächst benötigen wir ein Startelement, das ein ganzes Element außerhalb der Gleichungsordnung von φ sein muß.

Satz 3.3.13 *Sei φ ein normiertes, primäres Element von $\mathcal{A}_f$ mit $M_\varphi < E_\varphi$ und $\mathbb{Q}(\varphi) = \mathcal{A}_f$. Dann ist*

$$\beta := \frac{\nu_\varphi(\varphi)^{M_\varphi}}{p}$$

ganz über $\mathbb{Z}'$ und liegt nicht in der Gleichungsordnung von φ.

Beweis: Für die v_p^*-Bewertung von β gilt

$$\begin{aligned} v_p^*(\beta) &= v_p^*(\frac{\nu_\varphi(\varphi)^{M_\varphi}}{p}) \\ &= M_\varphi v_p^*(\nu_\varphi(\varphi)) - 1 \\ &= \frac{M_\varphi}{M_\varphi} - 1 = 0. \end{aligned}$$

β ist also ganz über $\mathbb{Z}'$. Es bleibt noch zu zeigen, daß β nicht in der Gleichungsordnung von φ liegt. β liegt in $\mathbb{Z}'[\varphi]$ genau dann, wenn $p\beta = \nu_\varphi(\varphi)^{M_\varphi}$ in $p\mathbb{Z}'[\varphi]$ liegt. Nach der Voraussetzung gilt jedoch $M_\varphi < E_\varphi$, das heißt $\nu_\varphi(t)^{M_\varphi} \not\equiv \chi_\varphi(t) \mod p\mathbb{Z}'[t]$. Damit ist auch $\nu_\varphi(\varphi)^{M_\varphi} \not\equiv 0 \mod p\mathbb{Z}'[\varphi]$, da χ_φ wegen $\mathbb{Q}(\varphi) = \mathcal{A}_f$ minimalen Grad hat. □

Für die Termination des Algorithmus benötigen wir die Beschränktheit der v_p^*-Bewertung der ganzen Elemente außerhalb der Gleichungsordnung von φ nach oben.

Satz 3.3.14 *Sei φ primär und α aus $\mathfrak{o}'_f \backslash \mathbb{Z}'[\varphi]$, so ist die v_p^*-Bewertung von α durch die p-adische Bewertung der reduzierten Diskriminante der Gleichungsordnung von φ nach oben beschränkt.*

Beweis: Sei $d_\varphi = v_p(\mathrm{d}_r(\mathbb{Z}'[\varphi]))$. Nehmen wir an $v_p^*(\alpha) \geq d_\varphi$. Dann ist $\frac{1}{p^{d_\varphi}}\alpha$ ganz, und $\alpha = p^{d_\varphi}(\frac{1}{p^{d_\varphi}}\alpha)$ liegt wegen $p^{d_\varphi}\mathfrak{o}'_f \subseteq \mathbb{Z}'[\varphi]$ in $\mathbb{Z}'[\varphi]$, was im Widerspruch zur Voraussetzung steht. □

Für die Konstruktion des nächsten Folgengliedes $\beta_j^{(i)}$ benötigen wir ein $r \in \mathbb{Z}$ mit der Eigenschaft

$$\theta \in \mathbb{Z}'[\varphi] + \mathcal{J}'_p \Longrightarrow \theta^{p^{rD_\varphi}} \in \mathbb{Z}'[\varphi].$$

Sei dazu $\theta = \alpha + \beta$ mit $\alpha \in \mathbb{Z}'[\varphi]$ und $\beta \in \mathcal{J}'_p$ beliebig. Für die v_p^*-Bewertung von β gilt

$$v_p^*(\beta) \geq \frac{1}{n},$$

wobei n der Grad von f ist. Denn sei $\prod_{i=1}^r \mathfrak{p}_i^{e_i}$ die eindeutige Zerlegung von $p\mathfrak{o}_f$ in Primideale, so gilt $\sum_{i=1}^r e_i \leq n$. Damit liegt aber β^n in $p\mathfrak{o}_f$. Für jede Fortsetzung $v_p^{(i)}$ der p-adischen Bewertung von $\mathbb{Q}$ auf $\mathcal{A}_f$ gilt somit $v_p^{(i)}(\beta^n) \geq 1$. Auf Grund der Homogenität der Bewertungen folgt damit sofort die Behauptung $v_p^*(\beta) \geq \frac{1}{n}$. Für die p-adische Bewertung $d_\varphi := v_p(\mathrm{d}_r(\mathbb{Z}'[\varphi]))$ der reduzierten Diskriminante von $\mathbb{Z}'[\varphi]$ gilt $p^{d_\varphi}\mathfrak{o}'_f \subseteq \mathbb{Z}'[\varphi]$. Wir wollen jetzt zeigen, daß für $k \geq nd_\varphi$ die Potenz β^k in $\mathbb{Z}'[\varphi]$ liegt. Dazu benutzen wir die Charakterisierung von über $\mathbb{Z}'$ ganzen Elementen durch die v_p^*-Bewertung, um zu zeigen, daß $\frac{1}{p^{d_\varphi}}\beta^k$ ganz ist. Dann liegt β^k wegen $\beta^k = p^{d_\varphi}(\frac{1}{p^{d_\varphi}}\beta^k) \in p^{d_\varphi}\mathfrak{o}'_f \subseteq \mathbb{Z}'[\varphi]$ in $\mathbb{Z}'[\varphi]$. Für die v_p^*-Bewertung von $\frac{1}{p^{d_\varphi}}\beta^k$ gilt

$$\begin{aligned} v_p^*(\frac{1}{p^{d_\varphi}}\beta^k) &= kv_p^*(\beta) - d_\varphi \\ &\geq nd_\varphi\frac{1}{n} - d_\varphi \\ &= 0, \end{aligned}$$

das heißt, $\frac{1}{p^{d_\varphi}}\beta^k$ ist ganz über $\mathbb{Z}'$. Betrachten wir nun $\theta^{p^{rD_\varphi}}$. Der Übersicht halber sei $s = rD_\varphi$. Nach dem binomischen Lehrsatz erhalten wir die Summe

$$\theta^{p^s} = (\alpha+\beta)^{p^s} = \sum_{i=0}^{p^s} \binom{p^s}{i} \beta^i \alpha^{p^s - i}$$

für θ^{p^s}. Der erste Summand ($i = 0$) und die letzten $p^s - nd_\varphi + 1$ Summanden ($nd_\varphi \leq i \leq p^s$) liegen in $\mathbb{Z}'[\varphi]$. Es bleibt also ein r zu finden, so daß die verbliebenen Summanden ($0 < i < nd_\varphi$) ebenfalls in $\mathbb{Z}'[\varphi]$ liegen. Dazu werden wir zeigen, daß sich r so wählen läßt, daß $v_p^*\left(\binom{p^s}{i}\right) \geq v_p^*(\mathrm{d}_r(\mathbb{Z}'[\varphi])) = d_\varphi$ ist und somit $\binom{p^s}{i}\beta^i\alpha^{p^s-i}$ in $\mathbb{Z}'[\varphi]$ liegt.

$$\begin{aligned} v_p^*\left(\binom{p^s}{i}\right) &= v_p\left(\frac{(p^s)!}{(p^s-i)!}\frac{1}{i!}\right) \\ &= v_p(p^s) + v_p\left(\frac{(p^s-1)!}{(p^s-i)!}\right) - v_p(i!) \\ &\geq s - v_p(i!) \end{aligned}$$

Wir müssen also $v_p(i!)$ noch nach oben abschätzen. Sei $l \in \mathbb{N}$ mit $i-(p-1) < p^l \leq i$:

$$\begin{aligned} v_p(i!) &= v_p((p^l)!) \\ &= p^{l-1} + p^{l-2} + \ldots + 1 \\ &= \frac{p^l - 1}{p-1} \\ &\leq \frac{i-1}{p-1}. \end{aligned}$$

Wählen wir s so groß, daß

$$d_\varphi \leq s - \frac{nd_\varphi - 1}{p-1}$$

ist, so liegt $\binom{p^s}{i}\beta^i$ in $\mathbb{Z}'[\varphi]$ für $0 < i < nd_\varphi$. Für

$$r := \left\lceil \frac{d_\varphi + \frac{nd_\varphi - 1}{p-1}}{D_\varphi} \right\rceil = \left\lceil \frac{d_\varphi(p-1+n)-1}{D_\varphi(p-1)} \right\rceil$$

ist das sicher erfüllt. Somit haben wir folgenden Satz gezeigt.

Satz 3.3.15 *Sei φ ein über $\mathbb{Z}'$ ganzes Element von $\mathcal{A}_f$ und $r = \left\lceil \frac{d_\varphi(p-1+n)-1}{D_\varphi(p-1)} \right\rceil$ mit $d_\varphi := v_p(\mathrm{d}_r(\mathbb{Z}'[\varphi]))$, so liegt für beliebiges θ aus $\mathbb{Z}'[\varphi] + \mathcal{J}_p'$ die Potenz $\theta^{p^{rD_\varphi}}$ in $\mathbb{Z}'[\varphi]$.*

Mit Hilfe des eben berechneten r können wir eine Situation kennzeichnen, in der es möglich ist, nach einer endlichen Anzahl von Versuchen ein nicht primäres Element zu finden.

Satz 3.3.16 *Seien φ und γ primär mit $D_\gamma | D_\varphi$ und $\gamma^{p^{rD_\varphi}} \notin \mathbb{Z}'[\varphi]$, wobei r entsprechend Satz 3.3.15 gewählt wird. Dann existieren Polynome P_1, P_2 mit reduzierten Koeffizienten modulo p und* $\mathrm{Grad}(P_1) < D_\gamma, \mathrm{Grad}(P_2) < D_\varphi$*, so daß $\tilde{\varphi} := P_1(\gamma) + P_2(\varphi)$ nicht primär ist.*

Beweis: Zum Nachweis der Existenz von P_1 und P_2 müssen wir analog zum Beweis von Satz 3.3.11 Fall 2 nur zeigen, daß

$$\mathbb{Z}'[\varphi, \gamma] / (\mathbb{Z}'[\varphi, \gamma] \cap \mathcal{J}_p')$$

kein Körper ist. Nehmen wir an, $\mathcal{K} := \mathbb{Z}'[\varphi, \gamma] / (\mathbb{Z}'[\varphi, \gamma] \cap \mathcal{J}_p')$ ist ein Körper, und $\mathcal{K}_\varphi$ und $\mathcal{K}_\gamma$ sind die von $\varphi + (\mathbb{Z}'[\varphi, \gamma] \cap \mathcal{J}_p')$ beziehungsweise $\gamma + (\mathbb{Z}'[\varphi, \gamma] \cap \mathcal{J}_p')$ über dem Primkörper erzeugten Teilkörper von $\mathcal{K}$. Dann muß wegen $D_\gamma | D_\varphi$ die Elementanzahl von $\mathcal{K}_\varphi$ ein Vielfaches der von $\mathcal{K}_\gamma$ sein. Da in endlichen Körpern aber die Teilkörper durch ihre Kardinalität eindeutig bestimmt sind, muß $\mathcal{K}_\gamma$ ein Teilkörper von $\mathcal{K}_\varphi$ sein. Das heißt aber, daß γ in $\mathbb{Z}'[\varphi] + \mathcal{J}_p'$ liegt, was der Wahl von r widerspricht. $\mathcal{K}$ kann also kein Körper sein. □

Wir haben jetzt alle Voraussetzungen für den letzten Teil des Algorithmus zusammengetragen.

3.3.2 Der Kernalgorithmus

Im wesentlichen versucht der Algorithmus eine Folge von ganzen Elementen zu erzeugen, wobei jeweils eine Annäherung an eine der Bedingungen 3.3.7 (ii) oder 3.3.8 (ii) für ein Eisenstein beziehungsweise Berwick Element erreicht werden soll. Er terminiert bei Auffinden eines Berwick, Eisenstein oder nicht primären Elements. Wir erhalten also entweder ein Element, dessen Gleichungsordnung maximal ist, oder ein nicht primäres Element, womit sich eine Reduzierung unseres Problems entsprechend den Ausführungen in Abschnitt 3.2 ergibt.

Zunächst wollen wir eine Grobstruktur des Algorithmus angeben, um danach den Algorithmus mit detaillierten Beschreibungen angeben zu können, ohne den Überblick zu verlieren.

Algorithmus 3.3.17 *Struktur des Kernalgorithmus*

E: Ein normiertes, separables Polynom aus $\mathbb{Z}'[t]$ vom Grad n mit einem primären $\xi := t + f(t)\mathbb{Q}[t]$.

A: Eine $\mathbb{Z}'$-Basis von $Cl(\mathbb{Z}', \mathcal{A}_f)$.

1. $\varphi \longleftarrow \xi$
2. *Stelle sicher, daß $\mathbb{Q}(\varphi)$ gleich der Algebra $\mathcal{A}_f$ ist.*
3. *Teste, ob $\mathbb{Z}'[\varphi]$ gleich $\mathfrak{o}'_f$ ist. Terminiere gegebenenfalls mit $1, \varphi, \ldots, \varphi^{n-1}$.*
4. *Teste, ob φ nicht primär ist. Terminiere mit der vom Zerlegungsalgorithmus 3.2.10 berechneten Basis.*
5. *Stelle sicher, daß φ nicht in $\mathcal{J}'_p$ liegt.*
6. *Falls φ nicht normiert ist, so normiere φ und gehe zu Schritt 2.*
7. *Suche ein neues φ mit Hilfe des Algorithmus 3.3.18.*
8. *Gehe zu Schritt 2.*

Algorithmus 3.3.18 *Suche neues φ*

E: Ein primäres, normiertes Element φ aus $\mathfrak{o}'_f$ mit $\mathbb{Q}(\varphi) = \mathcal{A}_f$.

A: Ein neues Element $\tilde{\varphi}$ aus $\mathfrak{o}'_f$, welches nicht primär ist oder eine der folgenden Bedingungen erfüllt

- $D_\varphi = D_{\tilde{\varphi}}$ *und* $M_\varphi < M_{\tilde{\varphi}}$
- $D_\varphi < D_{\tilde{\varphi}}$.

1. *Finde ein β_0 aus $\mathfrak{o}'_f \backslash \mathbb{Z}'[\varphi]$.*
   Setze $i \leftarrow 0$.
2.
   - *Teste, ob β_i nicht primär ist. Terminiere mit $\tilde{\varphi} \leftarrow \beta_i$.*
   - *Teste, ob mit Hilfe von β_i eine Annäherung an ein Berwick oder Eisenstein Element möglich ist. Berechne gegebenenfalls $\tilde{\varphi}$ entsprechend dem Satz 3.3.11 oder 3.3.10 und terminiere mit $\tilde{\varphi}$.*
3. *Finde ein neues Element β_{i+1} aus $\mathfrak{o}'_f \backslash \mathbb{Z}'[\varphi]$ mit $v_p^*(\beta_{i+1}) > v_p^*(\beta_i)$ oder β_{i+1} nicht primär. Setze $i \leftarrow i + 1$ und gehe zu Schritt 2.*

Nachdem wir nun einen groben Überblick von dem Kernalgorithmus gewonnen haben, werden wir ihn detailliert beschreiben. Der Algorithmus 3.3.18 „Suche neues φ“ wird im folgenden der Schleife Schritte 7 - 12 entsprechen.

Algorithmus 3.3.19 *Kernalgorithmus*

Eingabe:

Für den Kernalgorithmus wird ein normiertes, separables Polynom f aus $\mathbb{Z}'[t]$ mit $\xi := t + f(t)\mathbb{Q}[t]$ primär erwartet.

Ausgabe:

Es wird eine Ganzheitsbasis von $Cl(\mathbb{Z}', \mathcal{A}_f)$ zurückgegeben.

Im ersten Teil testen wir, ob wir bereits fertig sind, beziehungsweise stellen den Ausgangszustand, für die Suche nach einem neuen primären Element, welches näher an der Berwick oder Eisenstein Element Schranke liegt, her. — Entspricht den Schritten 1 - 6 im Algorithmus 3.3.17 —

1. Schritt: (Initialisierung)

Setze

$$\begin{aligned} \varphi &\leftarrow \xi \\ q &\leftarrow p \end{aligned}$$

2. Schritt: (Suche erzeugendes Element)

Teste, ob φ die ganze Algebra über $\mathbb{Q}$ erzeugt. Falls nicht, so finde ein $k \in \mathbb{Z}$ so, daß

$$\tilde{\varphi} = \varphi + qk\xi$$

die ganze Algebra über $\mathbb{Q}$ erzeugt. Setze

$$\varphi \longleftarrow \tilde{\varphi}.$$

In Satz 3.3.12 haben wir gezeigt, daß nach endlich vielen Versuchen ein solches k auftreten muß. Entsprechend Satz 3.3.1 ist wegen $\tilde{\varphi} \equiv \varphi \mod q\mathfrak{o}'_f$ das

Minimalpolynom von $\tilde{\varphi}$ kongruent μ_φ modulo $p\mathbb{Z}'[t]$. Der Abstand zur Berwick Element Schranke bleibt also gleich. Weiterhin ist bei richtiger Wahl von q, den Erläuterungen zu Satz 3.3.12 folgend, das neue Element $\tilde{\varphi}$ normiert, wenn φ normiert ist.

3. Schritt: (Dedekind Test)

> *Führe mit μ_φ einen erweiterten Dedekindtest mit dem Algorithmus 3.1.2 durch und terminiere mit der von Algorithmus 3.1.3 berechneten Basis, wenn die Gleichungsordnung oder der Multiplikatorring des p-Radikals der Gleichungsordnung maximal ist.*

4. Schritt:

> *Teste, ob φ in $\mathcal{J}_p'$ liegt. Ist das der Fall, so setze*
>
> $$\varphi \longleftarrow \varphi + 1.$$

Wir stellen fest, daß mit φ auch $\varphi + 1$ die ganze Algebra über $\mathbb{Q}$ erzeugt. Weiterhin gilt für das charakteristische Polynom von $\varphi + 1$

$$\chi_{\varphi+1}(t) = \chi_\varphi(t-1).$$

Auf Grund der Äquivalenz $v_p^*(\varphi) > 0 \Longleftrightarrow \nu_\varphi(t) = t$ ergibt sich das p-Minimalpolynom von $\varphi + 1$ zu

$$\nu_{\varphi+1}(t) = \nu_\varphi(t-1) = t - 1$$

und somit $v_p^*(\varphi + 1) = 0$. $\varphi + 1$ liegt also nicht in $\mathcal{J}_p'$. Im primären Fall gilt insbesondere

$$v_p^*(\nu_{\varphi+1}(\varphi + 1)) = v_p^*(\nu_\varphi(\varphi + 1 - 1)) = \frac{L_\varphi}{M_\varphi},$$

weshalb der Nenner M_φ, der für der Termination wichtig ist, nicht verkleinert wird.

5. Schritt: (Normierung)

Teste, ob φ normiert ist, ist das nicht der Fall, so berechne entsprechend Satz 3.3.9 ein normiertes $\tilde{\varphi}$, setze

$$\varphi \longleftarrow \tilde{\varphi}.$$

Falls M_φ gleich Eins ist, so setze $q \longleftarrow p^2$ sonst $q \longleftarrow p$ und gehe zu Schritt 2.

Nun sind die Grundvoraussetzungen für unsere zweite Konstruktionsstufe — entspricht Algorithmus 3.3.18 „Suche neues φ“ — erfüllt. Dabei wurde der Wert M_φ nicht verändert.

6. Schritt: (Initialisierung der Schleife)

Initialisiere

$$\beta \longleftarrow \frac{\nu_\varphi(\varphi)^{M_\varphi}}{p}.$$

β ist nach Satz 3.3.13 ganz über $\mathbb{Z}'$ und liegt nicht in $\mathbb{Z}'[\varphi]$.

Die folgenden Schritte 7 bis 12 bilden eine Schleife, in der bei jedem Durchlauf ein neues $\beta \in \mathfrak{o}'_f \backslash \mathbb{Z}'[\varphi]$ mit einer größeren v_p^*-Bewertung konstruiert wird. Diese ist jedoch für ganze Elemente außerhalb von $\mathbb{Z}'[\varphi]$ nach Satz 3.3.14 beschränkt. Es muß also zu einer Termination durch das Finden eines Berwick, Eisenstein oder nicht primären Elementes beziehungsweise durch eine Annäherung an die Berwick oder die Eisenstein Element Schranke kommen.

7. Schritt: (Termination der Schleife?)

- *Teste, ob β primär ist.*
  Wenn nicht, so finde, falls notwendig, entsprechend Schritt 2 mit $q = p$ ein $\tilde{\beta}$, welches die ganze Algebra über $\mathbb{Q}$ erzeugt. Nach Satz 3.3.1 ist $\tilde{\beta}$ nicht primär. Berechne mit Hilfe des Zerlegungsalgorithmus 3.2.10 eine Ganzheitsbasis von $Cl(\mathbb{Z}', \mathbb{Q}(\tilde{\beta}))$ und terminiere.
- *Teste, ob mit β die Annäherung an ein Berwick Element möglich ist — $D_\beta \nmid D_\varphi$ —*
  Berechne gegebenenfalls entsprechend Satz 3.3.11 $\tilde{\varphi}$, setze

$$\begin{array}{ccc} \varphi & \longleftarrow & \tilde{\varphi} \\ q & \longleftarrow & p \end{array}$$

  und gehe zu Schritt 2.
- *Teste, ob mit β eine Annäherung an ein Eisenstein Element möglich ist — $M_\beta \nmid M_\varphi$ —*
  Berechne gegebenenfalls entsprechend Satz 3.3.10 $\tilde{\varphi}$, setze

$$\begin{array}{ccc} \varphi & \longleftarrow & \tilde{\varphi} \\ q & \longleftarrow & p \end{array}$$

  und gehe zu Schritt 2.

Zur Wahl von q ist zu bemerken, daß im Fall der Vergrößerung von D_φ uns in der Konstruktion entsprechend Satz 3.3.11 nicht der Erhalt des Abstandes zur Eisenstein Element Schranke garantiert wird. Wir können also nichts durch die Wahl von $q = p$ verlieren. Im zweiten Fall, der Vergrößerung von M_φ, ist M_φ für das neue φ größer als Eins, denn Eins ist die untere Schranke. In Schritt 2 genügt uns somit die Bedingung $v_p^*(qk\xi) \geq 1$.

Hat keiner der Tests zu einem Rücksprung beziehungsweise zum Verlassen des Kernalgorithmus geführt, so gilt für β:

- β ist primär
- $D_\beta | D_\varphi$
- $M_\beta | M_\varphi$

8. Schritt:

Setze

$$k \longleftarrow M_\varphi v_p^*(\beta).$$

k liegt in $\mathbb{Z}$, denn entweder ist $v_p^*(\beta) = 0$ oder $v_p^*(\beta) = v_p^*(\nu_\beta(\beta)) = \frac{L_\beta}{M_\beta}$, und da nach obiger Bemerkung $M_\beta | M_\varphi$ gilt, liegt $M_\varphi v_p^*(\beta)$ in $\mathbb{Z}$. Daß die Gleichheit $v_p^*(\beta) = v_p^*(\nu_\beta(\beta))$ gilt, sieht man folgendermaßen. β ist ganz über $\mathbb{Z}'$ und $v_p^*(\beta) \neq 0$ genau dann, wenn $v_p^*(\beta) > 0$. Nach Satz 2.5.2 muß damit $\nu_\beta(t)$ gleich dem Monom t sein, das heißt $\nu_\beta(\beta) = \beta$.

9. Schritt: (Hilfselemente)

Setze

$$\begin{aligned} \gamma &\longleftarrow \frac{\beta}{\nu_\varphi(\varphi)^k} \\ \delta &\longleftarrow \gamma^{p^{rD_\varphi}} \end{aligned}$$

mit $r \in \mathbb{Z}$ entsprechend Satz 3.3.15, so daß

$$\theta \in \mathbb{Z}'[\varphi] + \mathcal{J}_p' \Longrightarrow \theta^{p^{rD_\varphi}} \in \mathbb{Z}'[\varphi]$$

gilt.

Die konstruierten Elemente sind aus $\mathfrak{o}'_f$, denn wegen

$$\begin{aligned} v_p^*\left(\frac{\beta}{\nu_\varphi(\varphi)^k}\right) &\geq v_p^*(\beta) - k v_p^*(\nu_\varphi(\varphi)) \\ &= v_p^*(\beta) - k M_\varphi \\ &= v_p^*(\beta) - v_p^*(\beta) \\ &= 0 \end{aligned}$$

ist γ und damit auch δ ganz über $\mathbb{Z}'$.

Zuerst testen wir jetzt natürlich, ob wir zufällig ein nicht primäres Element gefunden haben oder eines, daß die Anwendung von Satz 3.3.11 oder Satz 3.3.10 ermöglicht.

10. Schritt: (Termination der Schleife?)

- *Führe Schritt 7 für γ an Stelle von β aus*
- *Führe Schritt 7 für δ an Stelle von β aus*

Analog der Bermerkung nach Schritt 7 gilt also

- γ, δ sind primär
- $M_\gamma | M_\varphi$ und $M_\delta | M_\varphi$
- $D_\gamma | D_\varphi$ und $D_\delta | D_\varphi$.

Der Rücksprung von Schritt 7 oder Schritt 10 zu Schritt 2 kann nicht beliebig oft erfolgen. Denn D_φ ist durch $n = \mathrm{Grad}(f)$, und M_φ ist nach der verschärften Abschätzung (3.4) durch E_ξ nach oben beschränkt.

In den folgenden beiden letzten Schritten konstruieren wir entweder ein neues Glied in der Folge der β mit größerem v_p^*-Wert, oder wir finden ein nicht primäres Element.

11. Schritt: (Nächstes Element in der Folge – neuer Schleifendurchlauf)

Falls $\delta \in \mathbb{Z}'[\varphi]$, so setze

$$\beta \longleftarrow \beta - \nu_\varphi(\varphi)^k \delta$$

und gehe zu Schritt 7.

12. Schritt: (Suche nicht primäres Element)

δ liegt also nicht in $\mathbb{Z}'[\varphi]$, nach Satz 3.3.16 finden wir ein nicht primäres $\tilde{\varphi}$. Falls erforderlich, so ändere $\tilde{\varphi}$ entsprechend Schritt 2 mit $q = p$ so ab, daß $\tilde{\varphi}$ ein primitives Element der Algebra ist. Berechne mit Hilfe des Zerlegungsalgorithmus 3.2.10 eine Ganzheitsbasis von $Cl(\mathbb{Z}', \mathbb{Q}(\tilde{\varphi}))$ und terminiere.

Für die Termination müssen wir zeigen, daß das in Schritt 11 neu konstruierte β nicht in $\mathbb{Z}'[\varphi]$ liegt und sich die v_p^*-Bewertung vergrößert hat. Nach Voraussetzung liegt δ in $\mathbb{Z}'[\varphi]$ und somit auch $\nu_\varphi(\varphi)^k\delta$. β hingegen liegt nicht in $\mathbb{Z}'[\varphi]$ und damit auch nicht $\beta - \nu_\varphi(\varphi)^k\delta$. Um die Vergrößerung der v_p^*-Bewertung des neuen β zu zeigen, benutzen wir die Definition von γ

$$\beta - \nu_\varphi(\varphi)^k\delta = \nu_\varphi(\varphi)^k(\gamma - \delta).$$

Wir erhalten also für die v_p^*-Bewertung des neuen β

$$\begin{aligned} v_p^*(\beta - \nu_\varphi(\varphi)^k\delta) &= v_p^*(\nu_\varphi(\varphi)^k(\gamma - \delta)) \\ &\geq k v_p^*(\nu_\varphi(\varphi)) + v_p^*(\gamma - \delta) \\ &= v_p^*(\beta) + v_p^*(\gamma - \delta) \end{aligned}$$

wegen φ normiert und $k = M_\varphi v_p^*(\beta) = \frac{v_p^*(\beta)}{v_p^*(\nu_\varphi(\varphi))}$. Wir müssen also zeigen, daß $v_p^*(\gamma - \delta) > 0$ ist, welches äquivalent zu $\gamma - \delta \in \mathcal{J}_p'$ ist.

γ ist nach Schritt 10 primär. $\mathcal{K} := \mathbb{Z}'[\gamma]/(\mathbb{Z}'[\gamma] \cap \mathcal{J}_p')$ ist damit nach Bemerkung 3.3.6 der endliche Körper mit p^{D_γ} Elementen. In $\mathcal{K}$ gilt nach dem Kleinen Fermatschen Satz

$$(\gamma + (\mathbb{Z}'[\gamma] \cap \mathcal{J}_p'))^{p^{rD_\varphi}} - (\gamma + (\mathbb{Z}'[\gamma] \cap \mathcal{J}_p')) = 0 + (\mathbb{Z}'[\gamma] \cap \mathcal{J}_p'),$$

da D_γ nach Schritt 10 D_φ teilt. Das heißt, $\delta - \gamma = \gamma^{p^{rD_\varphi}} - \gamma$ liegt in $\mathbb{Z}'[\gamma] \cap \mathcal{J}_p'$, also insbesondere in $\mathcal{J}_p'$.

Der Algorithmus muß somit terminieren. Dies kann nur in den Schritten 3, 7, 10 oder 12 erfolgen. Dabei können wir entweder unser Problem auf Algebren kleineren Grades reduzieren, oder wir finden eine Ganzheitsbasis entsprechend unserem erweiterten Dedkindkriterium 3.1.1.

Kapitel 4

Globalisierung

Nachdem wir nun in Kapitel 3 vollständig das Problem der Berechnung einer lokalen Maximalordnung gelöst haben, müssen wir uns überlegen, wie wir zum globalen Fall zurückfinden. In Kapitel 3 hatten wir schon festgestellt, daß die Maximalordnung von $\mathcal{A}_f$ die Summe $\mathfrak{o}_f = \sum_{p \in \mathbb{P}_f} \mathcal{R}^p$ der p-Maximalordnungen ist. Wir müssen also eine Modulsumme bilden. Dazu benutzen wir die modulare Hermite Normalform von ganzzahligen Matrizen. Siehe auch [Co, Po/Za].

Wir sind nunmehr in der Lage den vollständigen Algorithmus zur Berechnung einer Ganzheitsbasis eines algebraischen Zahlkörpers beziehungsweise allgemeiner einer separablen Algebra anzugeben.

4.1 Der Round 4 Algorithmus

Algorithmus 4.1.1 *Round 4*

Eingabe:

Es wird ein normiertes, separables Polynom f aus $\mathbb{Z}[t]$ erwartet.

Ausgabe:

Es wird eine Ganzheitsbasis von $\mathcal{A}_f$ zurückgegeben.

1. Schritt:

Bestimme die reduzierte Diskriminante sowie die Polynomdiskriminante von f.

2. Schritt: (quadratische Diskriminantenteiler)

Faktorisiere die reduzierte Diskriminante von f. Bestimme aus der Faktorisierung der reduzierten Diskriminante die Faktorisierung der Polynomdiskriminante von f. Setze

$$\begin{aligned} \mathbb{P}_f &\leftarrow \{p \in \mathbb{P} \mid v_p(\mathrm{d}(f)) \geq 2\} \\ \mathcal{B} &\leftarrow \{1, \xi, \ldots, \xi^{n-1}\} \end{aligned}$$

Die folgenden Schritte 3 bis 8 bilden eine Schleife.

3. Schritt: (Schleifentermination)

Falls $\mathbb{P}_f = \emptyset$ gehe zu Schritt 9.

4. Schritt: (Wähle p für Lokalisierung)

Wähle p aus $\mathbb{P}_f$ beliebig.
Setze $\mathbb{P}_f \leftarrow \mathbb{P}_f \backslash \{p\}$.

5. Schritt: (Dedekind Test)

Untersuche mit dem Dedekind Test Algorithmus 3.1.2, ob die lokale Gleichungsordnung von f oder der Multiplikatorring des p-Radikals der Gleichungsordnung von f maximal sind. Bestimme gegebenenfalls mit dem Dedekindbasis Algorithmus 3.1.3 eine Ganzheitsbasis $\omega_1, \ldots, \omega_n$ des ganzen Abschlusses der p-Lokalisierung von $\mathbb{Z}$ in $\mathcal{A}_f$. Gehe zu Schritt 8.

6. Schritt: (Lokale Ganzheitsbasis mit Zerlegungsalgorithmus)

Falls f modulo p in verschiedene koprime Faktoren zerfällt, so bestimme eine Ganzheitsbasis $\omega_1, \ldots, \omega_n$ des ganzen Abschlusses der p-Lokalisierung von $\mathbb{Z}$ in $\mathcal{A}_f$ mit Hilfe des Zerlegungsalgorithmus 3.2.10. Gehe zu Schritt 8.

7. Schritt: (Lokale Ganzheitsbasis mit Kernalgorithmus)

Bestimme eine Ganzheitsbasis $\omega_1, \ldots, \omega_n$ von $Cl(\mathbb{Z}', \mathcal{A}_f)$ mit Hilfe des Kernalgorithmus 3.3.19.

8. Schritt:

Für alle i aus $\{1, \ldots, n\}$ multipliziere ω_i mit einer passenden Einheit aus $\mathbb{Z}'$, so daß ω_i in $\mathcal{R}_f^p$ liegt. Setze

$$\mathcal{B} \leftarrow \mathcal{B} \cup \{\omega_1, \ldots, \omega_n\},$$

gehe zu Schritt 3.

9. Schritt: (Summieren der lokalen Basen)

Sei A die $n \times m$ Matrix ($m = |\mathcal{B}|$) über $\mathbb{Q}$, die zu jedem Element β aus $\mathcal{B}$ eine Spalte mit den Koeffizienten der Darstellung von $d_r(f)\beta$ bezüglich der Basis $1, \xi, \ldots, \xi^{n-1}$ enthält. $B = (b_{ij})$ sei die auf Hermite Normalform transformierte Matrix A. Es sind nun nur noch die ersten n Spalten ungleich Null. Setze

$$\tilde{\omega}_j \leftarrow \frac{1}{d_r(f)} \sum_{i=1}^{n} b_{ij} \xi^{i-1}$$

für $j \in \{1, \ldots, n\}$. Terminiere mit

$$(\tilde{\omega}_1, \ldots, \tilde{\omega}_n).$$

Kapitel 5

Implementierung

5.1 Implementierung des Kernalgorithmus

Die Schritte 1 – 5 des Algorithmus 3.3.19 lassen sich direkt, bei Vorhandensein eines Computeralgebra Systems wie zum Beispiel KANT, implementieren. Hingegen ist eine solche Herangehensweise für die Schleife, Schritte 7 – 12, nicht möglich, da schon bei sehr kleinen Beispielen große Rechenzeiten auftreten. Das liegt am starken Anwachsen der Koeffizienten der konstruierten Elemente β, γ, δ bezüglich der $\mathbb{Q}$-Basis $1, \varphi, \ldots, \varphi^{n-1}$ von $\mathcal{A}_f$. Wir werden jetzt untersuchen, wie durch Reduktionen die Koeffizientenexplosion der zu berechnenden algebraischen Zahlen verhindert werden kann. Zunächst stellen wir nochmals fest, daß die Termination des Algorithmus im wesentlichen durch die Beschränkung der v_p^*-Bewertung der berechneten Elemente garantiert wird. Somit müssen wir mindestens die Invarianz der v_p^*-Bewertung der algebraischen Elemente unter den Reduktionen sicherstellen. Wir werden jetzt nacheinander die Reduktionsmöglichkeiten für die einzelnen Schritte des Algorithmus 3.3.19, in denen ein starkes Koeffizientenwachstum auftreten kann, untersuchen.

Schritt 5: (Normierung)
Unser aktuelles φ ist nicht normiert, das heißt, L_φ ist ungleich Eins. Entsprechend Satz 3.3.9 berechnen wir ein $\tilde{\varphi} = \varphi + \eta_\varphi$ mit $\eta_\varphi \in \mathcal{J}_p'$, $\tilde{\varphi}$ normiert und $M_{\tilde{\varphi}} = M_\varphi$. Gesucht ist ein $\kappa \in \mathbb{Z}^{>0}$, so daß für $\delta \in p^\kappa \mathbb{Z}'[\xi]$ beliebig das Element $\tilde{\varphi} + \delta$ vom algorithmischen Standpunkt aus — Termination — die gleichen Eigenschaften wie $\tilde{\varphi}$ hat, das heißt, $\tilde{\varphi} + \delta$ ist normiert, $M_{\tilde{\varphi}+\delta} = M_{\tilde{\varphi}} = M_\varphi$ und $D_{\tilde{\varphi}+\delta} = D_{\tilde{\varphi}} = D_\varphi$. Offensichtlich ist, daß κ größer gleich Eins sein muß, damit entsprechend Korollar 3.3.2 das p-Minimalpolynom von $\tilde{\varphi} + \delta$ gleich dem von $\tilde{\varphi}$ gewählt werden kann. Analog zu dem Beweis von Satz 3.3.9 bestimmen wir die v_p^*-Bewertung von

$\nu_{\tilde{\varphi}+\delta}(\tilde{\varphi}+\delta) = \nu_\varphi(\tilde{\varphi}+\delta)$. Sei

$$\begin{aligned}\nu_\varphi(\tilde{\varphi}+\delta) &= \nu_\varphi(\varphi+(\eta_\varphi+\delta)) \\ &= \nu_\varphi(\varphi)+(\eta_\varphi+\delta)\nu'_\varphi(\varphi)+(\eta_\varphi+\delta)^2 h(\varphi,\eta_\varphi+\delta)\end{aligned}$$

mit $h(x,y) \in \mathbb{Z}[x,y]$ die formale Taylorentwicklung von $\nu_\varphi(\tilde{\varphi}+\delta)$. Für die v_p^*-Bewertung der Summanden erhalten wir entsprechend dem Beweis von Satz 3.3.9

$$\begin{aligned}v_p^*(\nu_\varphi(\varphi)) &= \frac{L_\varphi}{M_\varphi} > \frac{1}{M_\varphi} \\ v_p^*((\eta_\varphi+\delta)\nu_\varphi(\varphi)) &= v_p^*(\eta_\varphi+\delta) \\ v_p^*((\eta_\varphi+\delta)^2 h(\varphi,\eta_\varphi+\delta)) &\geq 2v_p^*(\eta_\varphi+\delta).\end{aligned}$$

κ ist also so zu wählen, daß $v_p^*(\eta_\varphi+\delta) = v_p^*(\eta_\varphi)$ gilt und damit $v_p^*(\,\nu_\varphi(\varphi+(\eta_\varphi+\delta))\,) = v_p^*(\eta_\varphi) = \frac{1}{M_\varphi}$ die gewünschte Invarianz der v_p^*-Bewertung unter der Reduktion gegeben ist.

Da $\nu_\varphi(\varphi)$ in der Gleichungsordnung des primären Elemets φ liegt, gilt für $v_p^*(\eta_\varphi)$

$$\begin{aligned}v_p^*(\eta_\varphi) &= \min_{i\in\{1,\dots,r\}} v_p^{(i)}\left(\frac{\nu_\varphi^k(\varphi)}{p^l}\right) \\ &= \min_{i\in\{1,\dots,r\}} kv_p^{(i)}(\nu_\varphi(\varphi)) - l \\ &= \min_{i\in\{1,\dots,r\}} kv_p^{(j)}(\nu_\varphi(\varphi)) - l \\ &= v_p^{(j)}(\eta_\varphi)\end{aligned}$$

für alle $j \in \{1,\dots,r\}$. Die Gleichheit $v_p^*(\eta_\varphi+\delta) = v_p^*(\eta_\varphi)$ ist demzufolge sicherlich für $v_p^*(\eta_\varphi) < v_p^*(\delta)$ erfüllt. Wir erhalten die beiden Fälle $M_\varphi > 1$ und $M_\varphi = 1$. Im ersten Fall können wir $\kappa = 1$ wählen und im zweiten Fall $\kappa = 2$, das entspricht genau unserer Wahl von q. Wir können also modulo $q\mathbb{Z}'[\xi]$ reduzieren.

Schritt 8: (Initialisierung der Schleife)
Wir benötigen als Startelement für die Schleife ein über $\mathbb{Z}'$ ganzes Element, welches nicht in der Gleichungsordnung von φ liegt. Sei $b := \nu_\varphi(\varphi)^{M_\varphi}$, so ist β definiert als $\frac{b}{p}$. Zum Nachweis, daß β über $\mathbb{Z}'$ ganz ist und nicht in der Gleichungsordnung von φ liegt, hatten wir in Satz 3.3.13 gezeigt, daß b nicht in $p\mathbb{Z}'[\varphi]$ liegt und die v_p^*-Bewertung von b gleich Eins ist. Ändern wir b um ein Element δ aus $p^2\mathbb{Z}'[\varphi]$ ab, so liegt $b+\delta$ ebenfalls nicht in $p\mathbb{Z}'[\varphi]$ und $v_p^*(b+\delta) = v_p^*(b) = 1$. Bei der Berechnung der Initialisierung von β können wir also $\nu_\varphi(\varphi)^{M_\varphi}$ modulo $p^2\mathbb{Z}'[\varphi]$ reduzieren.

Schritt 9: (Hilfselemente) **&**

Schritt 11: (Nächstes Element in der Folge – neuer Schleifendurchlauf)
Wir befinden uns in der Schleife Schritte 7 – 12. Ziel der Schleife ist die Annäherung an ein Berwick beziehungsweise Eisenstein Element. Dazu erzeugen wir Elemente β in $\mathfrak{o}'_f \backslash \mathbb{Z}'[\varphi]$ mit streng steigenden M_β Werten. Nach Satz 3.3.14 ist deren v_p^*-Bewertung nach oben durch $d_\varphi := v_p(\mathrm{d}_r(\mathbb{Z}'[\varphi]))$ beschränkt. Wir können also modulo $p^{d_\varphi}\mathbb{Z}'[\varphi]$ reduzieren, ohne die v_p^*-Bewertung der Elemente zu verändern. Dabei ist es sinnvoll die Berechnung der Elemente modular durchzuführen. Bei der Potenzierung von γ haben wir es im allgemeinen mit sehr großen Exponenten zu tun. Eine exakte Berechnung mit einer anschließenden Reduktion wäre zu zeitaufwändig.

Schritte 7 & 10: (Termination der Schleife?)
Stellen wir in einem der beiden Schritte fest, daß wir näher an ein Berwick oder Eisenstein Element rücken können, so ist eine Reduktion von $\tilde{\varphi}$ möglich, wenn wir nicht $D_{\tilde{\varphi}}$ beziehungsweise $M_{\tilde{\varphi}}$ verändern. Im ersten Fall genügt die Bedingung, daß wir um δ aus $\mathcal{J}'_p$, also zum Beispiel modulo $p\mathbb{Z}'[\varphi]$, reduzieren. Im zweiten Fall dürfen wir ebenfalls modulo $p\mathbb{Z}'[\varphi]$ reduzieren, da $\tilde{\varphi}$ nach Satz 3.3.10 normiert und $M_{\tilde{\varphi}}$ größer als Eins ist, also die Situation aus Schritt 5 vorliegt.

Den Fall, daß wir ein nicht primäres Element gefunden haben, werden wir bei der Untersuchung des Zerlegungsalgorithmus betrachten.

Jetzt wollen wir noch einmal das Problem, der Annäherung an ein Berwick Element, betrachten. Wie schon in Abschnitt 3.3.1 erwähnt, erhält die Konstruktion des neuen $\tilde{\varphi}$ nach Satz 3.3.11 nicht den Wert M_φ. Vielmehr muß sich der Algorithmus durch Anwendung von Satz 3.3.10 wieder vorarbeiten. Dazu benötigen wir ein primäres Element β mit $M_\beta \nmid M_{\tilde{\varphi}}$. Wir könnten also im günstigsten Fall $M_{\tilde{\varphi}}$ sofort vergrößern, wenn wir uns dasjenige Element β mit dem größten M_β Wert, welches während des Kernalgorithmus auftrat, gemerkt hätten. Diesen kleinen Test, ob M_β nicht M_φ teilt, können wir sofort an die Änderung von φ nach Satz 3.3.11 — Schritte 7 und 10 — anschließen. Überlegen wir uns zuerst, welches das Element mit dem größten bisher aufgetretenen „M-Wert“ ist. Während des Kernalgorithmus 3.3.19 kommt es nur bei Benutzung der Konstruktion nach Satz 3.3.11 in den Schritten 7 und 10 zu einer möglichen Verkleinerung von M_φ. Sei $\tilde{\varphi}$ das nach Satz 3.3.11 konstruierte Element mit $D_{\tilde{\varphi}} > D_\varphi$. Wenn M_φ nicht $M_{\tilde{\varphi}}$ teilt, so können wir mit Hilfe von Satz 3.3.10 $M_{\tilde{\varphi}}$ vergrößern. Teilt jedoch M_φ das neue $M_{\tilde{\varphi}}$, so ist $M_{\tilde{\varphi}}$ größer oder gleich M_φ. Schließen wir an die Veränderung von φ mit dem Ziel der Vergrößerung von D_φ immer den Test $M_\varphi \nmid M_{\tilde{\varphi}}$ mit der gegebenenfalls möglichen Vergrößerung von $M_{\tilde{\varphi}}$ an, so ist φ immer dasjenige Element mit dem größten bisher im Kernalgorithmus aufgetretenen „M-Wert“ bis zur Konstruktion von $\tilde{\varphi}$. Zur Durchführung des Test müssen wir zunächst $M_{\tilde{\varphi}}$ berechnen. Dazu benötigen wir das charakteristische Polynom von $\nu_{\tilde{\varphi}}(\tilde{\varphi})$, welches zu berechnen einen erheblichen Zeitaufwand bedeutet. Leider können wir bei einem fehlgeschlagenen Test die berechneten Werte nicht zu einem späteren Zeitpunkt verwenden. Es kommt also in manchen Beispielen zu einer größeren Laufzeit des Algorithmus. Im allgemeinen wird während des Kernalgorithmus nur sehr selten näher an ein Berwick Element gerückt. Zudem ist der Test meist nur für den speziellen Fall, daß M_{φ} gleich Eins ist, nicht erfolgreich. Dieser triviale Fall läßt sich gesondert, ohne die Berechnung von $M_{\tilde{\varphi}}$ abfangen. Trotz dieses Nachteils erweist sich der Test als sinnvoll, da er die Anzahl der Schleifendurchläufe im Kernalgorithmus und damit die Anzahl der zu berechnenden charakteristischen Polynome stark reduzieren kann.

5.2 Implementierung des Zerlegungsalgorithmus

Laufzeituntersuchungen zeigen, daß vor allem nach einer Zerlegung entsprechend dem Zerlegungsalgorithmus 3.2.10 die Teilprobleme eine lange Rechenzeit erfordern. Das liegt vor allem daran, daß auch bei einem Startpolynom mit kleinen Koeffizienten die im Kernalgorithmus berechneten charakteristischen Polynome sehr große Koeffizienten haben. Mit einem solchen Polynom zerlegen wir danach unsere Maximalordnung. Es stellt sich somit die Frage, ob es möglich ist, eine Zerlegung unseres Startpolynoms in koprime Faktoren modulo einer geeigneten p-Potenz zu konstruieren, statt mit dem neuen schlechteren erzeugenden Polynom weiterzurechnen.

Zunächst rekapitulieren wir noch einmal das bisherige Vorgehen nach der Konstruktion eines nicht primären Elements im Kernalgorithmus. Gegeben ist ein normiertes, separables Polynom f über $\mathbb{Z}'$ und ein über $\mathbb{Z}'$ ganzes, nicht primäres Element φ. Unter Berufung auf Satz 3.3.12 finden wir nach endlich vielen Versuchen ein $k \in \mathbb{Z}^{\geq 0}$ so, daß $\tilde{\varphi} := \varphi + pk\xi$ mit $\xi = t + f(t)\mathbb{Q}[t]$ nicht primär ist und die ganze Algebra $\mathcal{A}_f$ über $\mathbb{Q}$ erzeugt. Statt des Polynoms f haben wir unsere Algebra nun durch das Minimalpolynom von $\tilde{\varphi}$ erzeugt. Jetzt konnten wir mit Hilfe des Henselschen Lemmas eine Zerlegung $f_1 f_2$ des Minimalpolynoms von $\tilde{\varphi}$ modulo $d^{2v_p(\mathrm{d}_r(\mathbb{Z}'[\tilde{\varphi}]))}\mathbb{Z}'[t]$ bestimmen und die Berechnung von $\mathfrak{o}'_f$ auf die Berechnung von $\mathfrak{o}'_{f_1}$ und $\mathfrak{o}'_{f_2}$ zurückführen.

5.2.1 Approximation orthogonaler Idempotenter

Auf Grund unserer bisherigen Überlegungen wissen wir also, daß es eine Algebra $\mathcal{A}_{\tilde{f}}$ mit einer zu $\mathfrak{o}'_f$ isomorphen p-Maximalordnung gibt, welche zwei orthogonale Idempotente besitzt. Die Algebra $\mathcal{A}_{\tilde{f}}$ ist als $\mathbb{Q}$-Modul jedoch zu unserer Ausgangsalgebra $\mathcal{A}_f$ isomorph. Es ist auch möglich zuerst die Urbilder der Idempotenten unter dem Isomorphismus σ aus dem Structural Stability Satz 3.2.3 in $\mathcal{A}_f$ zu bestimmen, um daraus ein $\tilde{f}$ mit kleineren Koeffizienten, welches zu f modulo einer geeigneten p-Potenz kongruent ist, zu erhalten. Diese Urbilder der Idempotenten werden wir p-adisch approximieren, denn σ ist bis auf einen bekannten p-adischen Fehler multiplikativ.

Seien $b_1 b_2$ die Zerlegung des charakteristischen Polynoms von φ in zwei normierte, teilerfremde Faktoren modulo $p\mathbb{Z}'[t]$ und r_1, r_2 aus $\mathbb{Z}'[t]$ so gewählt, daß $r_1 b_1 + r_2 b_2 \equiv 1 \mod p\mathbb{Z}'[t]$. Setzen wir $e \leftarrow (r_1 b_1)(\varphi)$, so liegt e in $\mathbb{Z}'[\varphi]$, und es gilt

$$\begin{aligned} e &\equiv e(e + (r_2 b_2)(\varphi)) \\ &\equiv e^2 + (r_1 r_2)(\varphi)(b_1 b_2)(\varphi) \\ &\equiv e^2 \mod p\mathbb{Z}'[\varphi], \end{aligned}$$

da $(b_1 b_2)(\varphi)$ kongruent Null modulo $p\mathbb{Z}'[\varphi]$ ist. e und $1 - e$ bilden somit modulo $p^k \mathfrak{o}'_f$ für $k = 1$ zwei orthogonale Idempotente. Diese Eigenschaft ist eine Schleifeninvariante des folgenden Iterationsverfahrens

$$\begin{aligned} e &\longleftarrow 3e^2 - 2e^3 \\ k &\longleftarrow 2k. \end{aligned}$$

Wir können also zwei orthogonale Idempotente beliebig genau p-adisch approximieren. Beweisen wir zunächst einmal, daß $e^2 \equiv e \mod p^k \mathfrak{o}'_f$ eine Schleifeninvariante ist. Sei $\tilde{e} := 3e^2 - 2e^3$, so müssen wir zeigen, daß $\tilde{e}^2 \equiv \tilde{e} \mod p^{2k} \mathfrak{o}'_f$. Nach Voraussetzung ist $e^2 = e + \delta$ mit $\delta \in p^k \mathfrak{o}'_f$. Wir stellen $\tilde{e}$ und $\tilde{e}^2$ in e und δ dar

$$\begin{aligned} \tilde{e} &= 3e^2 - 2e^3 \\ &= 3e^2 - 2e(e + \delta) \\ &= e^2 - 2e\delta \\ &= e + \delta - 2e\delta \\ &= e + (1 - 2e)\delta. \end{aligned}$$

Damit erhalten wir für $\tilde{e}^2$ die Darstellung

$$\begin{aligned}
\tilde{e}^2 &= (e + (1-2e)\delta)^2 \\
&= e^2 + 2(e - 2e^2)\delta + (1-2e)^2\delta^2 \\
&= e + \delta + 2(e - 2e - 2\delta)\delta + (1-2e)^2\delta^2 \\
&= e + \delta - 2e\delta + ((1-2e)^2 - 2)\delta^2 \\
&= \tilde{e} + ((1-2e)^2 - 2)\delta^2
\end{aligned}$$

und die gewünschte Kongruenz $\tilde{e}^2 \equiv \tilde{e} \mod p^{2k}\mathfrak{o}'_f$. Benutzen wir die Eigenschaft der reduzierten Diskriminante, daß $\mathrm{d}_r(\mathbb{Z}'[\xi])\mathfrak{o}'_f \subseteq \mathbb{Z}'[\xi]$, so gilt für $k > v_p(\mathrm{d}_r(\mathbb{Z}'[\xi]))$

$$e^2 \equiv e \mod p^{k - v_p(\mathrm{d}_r(\mathbb{Z}'[\xi]))}\mathbb{Z}'[\xi].$$

Wir können also orthogonale Idempotente sogar modulo $p^k\mathbb{Z}'[\xi]$ beliebig genau approximieren und erhalten somit eine Folge von Polynomen $\hat{e}_i$ aus $\mathbb{Q}[t]$ vom Grad kleiner $n = \mathrm{Grad}(f)$ mit $\hat{e}_i^2 \equiv \hat{e}_i \mod p^i f(t)\mathbb{Q}[t]$ und $\hat{e}_{i+1} \equiv \hat{e}_i \mod p^i f(t)\mathbb{Q}[t]$. Es existiert also ein Polynom $\hat{e}$ vom Grad kleiner n mit Koeffizitenten aus $\mathbb{Q}_p$ und $\hat{e}^2 \equiv \hat{e} \mod f(t)\mathbb{Q}_p[t]$, das heißt, f teilt $\hat{e}(1-\hat{e})$ in $\mathbb{Q}_p[t]$. Sei $d > 0$ so gewählt, daß $p^d\hat{e}$ in $\mathbb{Z}_p[t]$ liegt. Wir definieren in $\mathbb{Z}_p[t]$

$$\begin{aligned}
\hat{f}_1 &:= \mathrm{ggT}(f, p^d\hat{e}) \\
\hat{f}_2 &:= \mathrm{ggT}(f, p^d(1-\hat{e})).
\end{aligned}$$

$\hat{f}_1$ und $\hat{f}_2$ sind mit f normiert, und wegen der Teilerfremdheit von $\hat{e}$ und $1-\hat{e}$ sowie der Teilbarkeit von $\hat{e}(1-\hat{e})$ durch f ist $\hat{f}_1\hat{f}_2$ eine Faktorisierung von f in zwei koprime Faktoren über $\mathbb{Z}_p$.

Wir müssen nun aus einer p-adischen Approximation e_i an $\hat{e}$ eine Approximation an den größten gemeinsamen Teiler $\hat{f}_1$ von f und $p^d\hat{e}$ aus $\mathbb{Z}'$ bestimmen.

Approximation des p-adischen ggT

Seien $\hat{e} \in \mathbb{Z}_p[t]$ und $e \in \mathbb{Z}'[t]$ zwei Polynome vom Grad kleiner n mit

$$\begin{aligned}
\hat{e}^2 &\equiv \hat{e} \mod f(t)\mathbb{Z}_p[t] \\
\hat{e} &\equiv e \mod p^m\mathbb{Z}_p[t]
\end{aligned}$$

und $\tilde{f}_1$ ein Polynom minimalen Grades aus $(f\mathbb{Z}'[t] + e\mathbb{Z}'[t] + p^m\mathbb{Z}'[t]) \backslash p^m\mathbb{Z}'$ gegeben. Für $G := \mathrm{ggT}(f, p^d\hat{e})$ gilt in $\mathbb{Z}_p[t]$

$$p^s G = c_1 f + c_2\, p^d \hat{e}$$

mit $c_1, c_2 \in \mathbb{Z}_p[t]$ und s so, daß $p^s\mathbb{Z}_p = (\frac{f}{G}\mathbb{Z}_p[t] + \frac{p^d\hat{e}}{G}\mathbb{Z}_p[t]) \cap \mathbb{Z}_p$ gilt. Weiterhin ist G wieder mit f normiert. Sei $^-\colon \mathbb{Z}_p[t] \longrightarrow \mathbb{Z}[t]$ der in Abschnitt 1.4 eingeführte Homomorphismus, welcher in der Laurent-Entwicklung bezüglich p die Terme mit einer p-Potenz größer als $m-1$ abschneidet. Ist m größer als s, so gilt

$$\begin{aligned} \bar{\hat{e}} &\equiv e \mod p^m\mathbb{Z}'[t] \\ 0 \not\equiv p^s\bar{G} &\equiv \bar{c}_1 f + \bar{c}_2\, p^d e \mod p^m\mathbb{Z}'[t], \end{aligned}$$

und $\bar{G}$ teilt modulo $p^m\mathbb{Z}'[t]$ die Polynome f und e. Somit muß $p^s\bar{G}$ auch $\tilde{f}_1$ modulo p^m teilen. Wegen der Bedingung an den Grad von $\tilde{f}_1$ muß dieser mit dem von $\bar{G}$ übereinstimmen und $\tilde{f}_1$ durch p^s teilbar sein. Da $\bar{G}$ normiert ist, gilt

$$\bar{G} \equiv f_1 := \frac{\tilde{f}_1}{l} \mod p^{m-s}\mathbb{Z}'[t],$$

wobei l der Leitkoeffizient von $\tilde{f}_1$ ist.

Wir haben also in f_1 eine p-adische Approximation aus $\mathbb{Z}'[t]$ an den größten gemeinsamen Teiler von f und $p^d\hat{e}$ modulo $p^{m-s}\mathbb{Z}_p[t]$ gefunden. Es bleibt somit nur noch $\tilde{f}_1$ zu bestimmen und eine Abschätzung für s herzuleiten.

$\tilde{f}_1$ kann wie folgt bestimmt werden. Für e gilt, $p^{\mathrm{d}_r(f)}\, e(\xi)$ liegt in der Gleichungsordnung $\mathbb{Z}'[\xi]$ von ξ, das heißt, $p^{\mathrm{d}_r(f)}\, e$ hat Koeffizienten aus $\mathbb{Z}'$. Seien S die Sylvestermatrix von f und $p^{\mathrm{d}_r(f)}\, e$ und $H = (h_{ij})_{i,j=1,\ldots N}$ die zeilenreduzierte Hermite Normalform der Matrix

$$\begin{pmatrix} S \\ p^m E_N \end{pmatrix}$$

über $\mathbb{Z}'$ mit $N := \mathrm{Grad}(f) + \mathrm{Grad}(e)$. Das Polynom

$$\tilde{f}_1 := \sum_{j=i}^{N} h_{ij}\, t^{N-j}$$

für $i := \max\{k \mid h_{kk} \neq 0\}$ hat die gewünschte Eigenschaft.

Wir wollen jetzt zeigen, daß $r := v_p(\mathrm{d}_r(f))$ eine obere Abschätzung von s ist. Entsprechend der Konstruktion der Polynome $\hat{e}_i$ gilt $\hat{e}_i(\xi)$ ist ganz über $\mathbb{Z}'$. Das Produkt $p^r\hat{e}_i$ hat also Koeffizienten aus $\mathbb{Z}'$. Damit liegt aber das Polynom $p^r\hat{e}$ in $\mathbb{Z}_p$. Seien $e_1 := p^r\,\hat{e}$, $e_2 := p^r(1-\hat{e})$, $G_i := \mathrm{ggT}(f, e_i)$ und $p^{s_i}\mathbb{Z}_p = \left(\frac{f}{G_i}\mathbb{Z}_p[t] + \frac{e_i}{G_i}\mathbb{Z}_p[t]\right) \cap \mathbb{Z}_p$ für $i = 1, 2$. Auf Grund der Teilerfremdheit von e_1 und e_2 gilt $f = G_1G_2$, das heißt $\frac{f}{G_i} = G_{3-i}$ für $i = 1, 2$. Damit liegt $G_1\frac{e_1}{G_1} + G_2\frac{e_2}{G_2} = p^r$ sowohl in $p^{s_1}\mathbb{Z}_p$ als auch in $p^{s_2}\mathbb{Z}_p$, und r muß insbesondere größer oder gleich s_1 und s_2 sein.

Fassen wir unsere Ergebnisse zum Schluß zusammen. Wir wollen eine Zerlegung $f \equiv f_1 f_2 \mod p^\kappa \mathbb{Z}'[t]$ von f in zwei modulo $p^\kappa \mathbb{Z}'[t]$ koprime, normierte Polynome f_1 und f_2 für $\kappa \in \mathbb{Z}^{>0}$ bestimmen. Dazu berechnen wir zunächst mit unserem Iterationsverfahren orthogonale Idempotente e und $1-e$ modulo $p^{\kappa+2\mathrm{d}_r(f)}\mathfrak{o}'_f$. Dann sind e und $1-e$ auch orthogonale Idempotente modulo $p^{\kappa+\mathrm{d}_r(f)}\mathbb{Z}'[\xi]$. Sei $\tilde{e}$ ein Polynom aus $\mathbb{Q}[t]$ vom Grad kleiner n mit $\tilde{e}(\xi) = e$. $\tilde{e}$ ist modulo $p^{\kappa+\mathrm{d}_r(f)}\mathbb{Q}_p[t]$ kongruent zu einem Polynom $\hat{e}$ aus $\mathbb{Q}_p[t]$ mit $\hat{e} \equiv \hat{e}^2 \mod f(t)\mathbb{Q}_p[t]$. Als nächstes berechnen wir entsprechend den obigen Ausführungen eine Approximation f_1 aus $\mathbb{Z}'[t]$ an den p-adischen größten gemeinsamen Teiler von f und $p^{\mathrm{d}_r(f)}\,\hat{e}$

$$f_1 \equiv \mathrm{ggT}(f,\, p^{\mathrm{d}_r(f)}\,\hat{e}) \mod p^{\kappa+\mathrm{d}_r(f)-s}\mathbb{Z}_p[t].$$

Analog berechnen wir

$$f_2 \equiv \mathrm{ggT}(f,\, p^{\mathrm{d}_r(f)}(1-\hat{e})) \mod p^{\kappa+\mathrm{d}_r(f)-s}\mathbb{Z}_p[t].$$

Wir haben gezeigt, daß s kleiner oder gleich $\mathrm{d}_r(f)$ ist. Damit gilt

$$f \equiv f_1 f_2 \mod p^\kappa \mathbb{Z}_p[t].$$

Da f_1 und f_2 aus $\mathbb{Z}'[t]$ sind, haben wir die gesuchte Zerlegung berechnet.

5.2.2 Der Zerlegungsalgorithmus II

Algorithmus 5.2.1 *Zerlegungsalgorithmus mit approximierten Idempotenten*

Eingabe:

Es werden ein normiertes, separables Polynom f aus $\mathbb{Z}'[t]$, ein algebraisches Element φ aus $\mathcal{A}_f$ und eine Zerlegung $b_1 b_2 = \chi_\varphi$ des charakteristischen Polynoms von φ in zwei normierte koprime Faktoren modulo $p\mathbb{Z}'[t]$ erwartet.

Ausgabe:

Es wird eine Ganzheitsbasis von $Cl(\mathbb{Z}', \mathcal{A}_f)$ zurückgegeben.

1. Schritt: (reduzierte Diskriminante)

Bestimme die reduzierte Diskriminante von f und setze

$$\kappa \longleftarrow v_p(\mathrm{d}_r(f)).$$

2. Schritt: (Idempotente modulo $p\mathbb{Z}'[\varphi]$)

Bestimme r_1 *und* r_2 *aus* $\mathbb{Z}'[t]$, *so daß* $r_1 b_1 + r_2 b_2 \equiv 1 \mod p\mathbb{Z}'[t]$ *und initialisiere* e, k *mit*

$$\begin{aligned} e &\longleftarrow r_1(\varphi) b_1(\varphi) \\ k &\longleftarrow 1. \end{aligned}$$

3. Schritt:

Wiederhole

$$\begin{aligned} e &\longleftarrow 3e^2 - 2e^3 \\ k &\longleftarrow 2k \end{aligned}$$

solange, bis $k > 3\kappa + 1$. *Die Berechnung von* e *kann jeweils modulo* $p^{2k}\mathbb{Z}'[\xi]$, $\xi := t + f(t)\mathbb{Q}[t]$, *mit dem aktuellen* k *erfolgen.*

4. Schritt: (Approximation des p-adischen ggT)

Sei g *ein Polynom aus* $\mathbb{Q}[t]$ *von kleinerem Grad als* f *mit* $g(\xi) = e$. *Dann hat* $p^\kappa g$ *Koeffizienten aus* $\mathbb{Z}'$. *Sei* H *die modulare zeilenreduzierte Hermite Normalform der Sylvestermatrix von* f *und* $p^\kappa g$, *bezüglich des Moduls* $p^{3\kappa+1}\mathbb{Z}'$. *Für* $i := \max\{k \mid h_{kk} \neq 0\}$ *und* $N := \mathrm{Grad}(f) + \mathrm{Grad}(g)$ *setze*

$$\tilde{f}_1 \longleftarrow \frac{1}{h_{ii}} \sum_{j=i}^{N} h_{ij} t^{N-j}.$$

Reduziere $\tilde{f}_1$ *modulo* $p^{2\kappa+1}\mathbb{Z}'[t]$.

5. Schritt: (Approximation einer p-adischen Faktorisierung)

Bestimme $\tilde{f}_2$ *aus* $\mathbb{Z}'[t]$ *mit*

$$\tilde{f}_1 \tilde{f}_2 \equiv f \mod p^{2\kappa+1}\mathbb{Z}'[t].$$

6. Schritt: (Ganzheitsbasen der Faktoren)

Bestimme die Ganzheitsbasen von $Cl(\mathbb{Z}', \mathcal{A}_{\tilde{f}_1})$ *und* $Cl(\mathbb{Z}', \mathcal{A}_{\tilde{f}_2})$.
Seien $(\omega_{i1}(\xi_i), \ldots, \omega_{in_i}(\xi_i))$ *mit* $\xi_i := t + \tilde{f}_i\mathbb{Q}[t]$ *und* $n_i = \mathrm{Grad}(\tilde{f}_i)$ *für* $i \in \{1, 2\}$ *die berechneten Ganzheitsbasen von* $\mathcal{A}_{\tilde{f}_1}$ *und* $\mathcal{A}_{\tilde{f}_2}$.

7. Schritt: (Addition)

Zusammensetzen der einzelnen Basen zu einer Ganzheitsbasis von $Cl(\mathbb{Z}', \mathcal{A}_f)$. *Setze*

$$(\omega_1, \ldots, \omega_n) \leftarrow (e\omega_{11}(\xi), \ldots, e\omega_{1n_1}(\xi), (1-e)\omega_{21}(\xi), \ldots, (1-e)\omega_{2n_2}(\xi)).$$

6. Schritt: (Hermite Reduktion)

Sei A *die* $n \times n$ *Matrix über* $\mathbb{Z}'$, *welche als* i*-te Spalte die Koeffizienten von* $p^\kappa\omega_i$ *bezüglich der Basis* $1, \xi, \ldots, \xi^{n-1}$ *hat.* $B = (b_{ij})$ *sei die auf Hermite Normalform transformierte Matrix* A. *Setze*

$$\tilde{\omega}_j \leftarrow \frac{1}{p^\kappa} \sum_{i=1}^{n} b_{ij}\xi^{i-1}$$

für $j \in \{1, \ldots, n\}$. *Terminiere mit*

$$(\tilde{\omega}_1, \ldots, \tilde{\omega}_n).$$

Kapitel 6

Beispiele

Zur Untersuchung des Verhaltens des Algorithmus wollen wir noch einige Beispiele angeben. Die Berechnungen wurden auf einer Hewlett Packard HP 9000 Series 735/100 mit 160 MB RAM und maximal 60 MB für einen Prozess unter HP-UX 9.05 durchgeführt. Die Polynome sind zum Teil den im Literaturverzeichnis aufgeführten Werken über den Round 4 entnommen. Sie sind so gewählt, daß der Round 4 nach Möglichkeit nicht sofort mit dem Dedekind Kriterium die p-Maximalität der Gleichungsordnung feststellt.

In der ersten Tabelle geben wir zum Vergleich die benötigten Rechenzeiten von Round 2 und Round 4 an. Beim Round 2 handelt es sich um eine erweiterte Version, welche analog dem Round 4 zuerst versucht, die Startgleichungsordnung entsprechend dem Zerlegungsalgorithmus zu zerlegen.

Die folgenden Tabellen enthalten detailliertere Angaben zum Laufzeitverhalten des Round 4. Für jeden Körper wird das erzeugende Polynom f, die Faktorisierung der Diskriminante und der reduzierten Diskriminante von f sowie die Zeit zur Faktorisierung der Diskriminante aufgeführt. Zur Faktorisierung wird zuerst die reduzierte Diskriminate berechnet und faktorisiert, um von den erhaltenen Faktoren die korrekten Exponenten in der Zerlegung der Diskriminante zu bestimmen. Darauf folgend werden für alle Primzahlen p, die quadratisch in der Diskriminante von f aufgehen, und für die die Gleichungsordnung nicht p-maximal ist, einige statistische Größen angegeben. Das ist zunächst der Index der lokalen Maximalordnung in der lokalen Gleichungsordnung, die Laufzeit, die zur Berechnung der p-Maximalordnung benötigt wurde, und die Zeit, die dabei zur Berechnung charakteristischer Polynome aufgewandt wurde. Weiterhin ist die Häufigkeit, mit der die Schleife Schritte 2 – 8 im Algorithmus 3.3.17 „Struktur des Kernalgorithmus“ durchlaufen wird — dabei wird jeder zusätzliche Test in

Schritt 2 als ein Durchlauf gezählt — und die Häufigkeit, mit der die Schleife Schritte 2 und 3 im Algorithmus 3.3.18 „Suche neues φ“ durchlaufen wird, angegeben. Zum Algorithmus 3.3.18 „Suche neues φ“ ist ebenfalls die Anzahl der in Schritt 2 durchgeführten Tests aufgeführt. Diese sind aufgeschlüsselt in die Tests A, B und C, welche wie folgt zugeordnet wurden.

A: Test, ob das Element primär nicht ist.

B: Test, ob die Annäherung an ein Berwick Element möglich ist.

C: Test, ob die Annäherung an ein Eisenstein Element möglich ist.

In den Tabellen sind zu jedem Test zwei Werte aufgeführt. Der erste Wert gibt an, wie oft der entsprechende Test zur Termination des Algorithmus 3.3.18 „Suche neues φ“ geführt hat, der zweite Wert in Klammern gibt an, wie häufig der Test insgesamt durchgeführt wurde. Dabei werden die Ergebnisse aller Kernalgorithmusaufrufe zur Berechnung einer p-Maximalordnung aufsummiert.

Aus den Beobachtungen kann entnommen werden, daß eine lange Laufzeit in den meisten Fällen durch die Berechnung der charakteristischen Polynome der im Kernalgorithmus erzeugten algebraischen Elemente hervorgerufen wird. Durch die Reduktion der Koeffizienten der berechneten Elemente, entsprechend den Ausführungen in Kapitel 5, wurde diese erheblich verringert. Desweiteren ist zu bemerken, daß der zusätzliche Test auf p-Maximalität des Multiplikatorringes entsprechend den Ausführungen zu Satz 3.1.1 besonders bei größeren Primzahlen oft zur sofortigen Termination des Kernalgorithmus führt. Das ist daran zu erkennen, daß es zu keinem Schleifendurchlauf im Algorithmus 3.3.18 „Suche neues φ“ kommt. Der Round 4 hat vor allem dann eine erheblich kürzere Laufzeit als der Round 2, wenn er den Grad durch Zerlegung reduzieren kann und die lokale Gleichungsordnung einen großen Index in den lokalen Maximalordnungen hat. Das ist an den Beispielpolynomen größeren Grades zu erkennen, siehe die Polynome vom Grad 30 oder 40. Wie das zweite Beispiel vom Grad 16 zeigt, kann es auch sehr effizient sein, nach einem Berwick beziehungsweise Eisenstein Element zu suchen, wenn die zu bestimmenden charakteristischen Polynome schnell berechenbar sind.

Rechenzeiten und Verhältnis von Round 4 zu Round 2			
Polynom	Zeit in sec		Verhältnis
	Round 4	Round 2	
$t^5 + 20t - 16$	0.07	0.11	0.63
$t^7 - 56t + 48$	0.08	0.37	0.21
$t^8 - 8t^7 + 6588344$	0.31	1.59	0.19
$t^8 + 2t^7 - 327617t^6 + 4967336t^5 - 30273556t^4 + 94618928t^3 - 159301148t^2 + 136438758t - 46443931$	2.19	2.83	0.77
$t^{10} - 10t^9 - 3874204890$	2.87	9.09	0.31
$t^{11} - 5082t^9 - 181016t^8 + 820908t^7 + 826455168t^6 + 28828948896t^5 + 557148848256t^4 + 6517138725504t^3 + 46090291534848t^2 + 182206040924160t + 310338030993408$	20.71	36.25	0.57
$t^{11} - 132t + 120$	0.91	3.90	0.23
$t^{12} + t^9 + 3t^6 + 12t^4 + 8$	0.21	0.47	0.44
$t^{12} - t^{11} + t^6 - 3t^4 - 10t^2 - 4$	0.38	0.28	1.35
$t^{14} + 2t^{12} - 2t^{11} - t^{10} - 2t^7 - t^4 - 1$	0.21	0.37	0.56
$t^{15} - 240t + 224$	12.89	15.44	0.83
$t^{16} + 132t^{14} + 6868t^{12} + 179570t^{10} + 2494972t^8 + 18111820t^6 + 65000173t^4 + 102234000t^2 + 46240000$	2.87	5.91	0.48
$t^{16} - 16t^{15} + 7006302246093750000$	35.82	205.82	0.17
$t^{20} - 4t^{12} - 1$	0.56	4.28	0.13
$t^{20} + t^{15} + 2t^{10} - t^5 + 1$	0.08	0.38	0.21
$t^{21} + 420t - 400$	20.23	107.34	0.18
$t^{22} - 22t^{21} - 1285369144044916154703847372 62$	323.00	1668.15	0.19
$t^{25} + 600t - 576$	437.34	279.85	1.56
$t^{27} - 756t + 728$	105.17	509.61	0.20
$t^{29} + 812t - 784$	74.43	504.17	0.14
$t^{30} + 234t^{20} - 5678t^{10} + 670097641028$	15.82	196.00	0.08
$t^{40} + 5t^{30} + 26t^{20} - 5t^{10} + 1$	2.23	10.66	0.20
$t^{40} - t^{30} + 2t^{20} + t^{10} + 1$	1.60	6.34	0.25

Laufverhalten des Round 4

$f(t) = t^5 + 20t - 16$		
$\mathrm{d}(f) = 2^{16}5^6$	$\mathrm{d}_r(f) = 2^4 5^2$	
Gesamtzeit: 0.08 sec	Faktorisierung von $\mathrm{d}_r(f)$: 0.00 sec	
2–Maximalordnung	Index: 2^5	
Zeit: 0.05 sec	Zeit char. Polynom: 0.04 sec	
Schleifendurchläufe		
Kernalogrithmus: 3	Suche neues φ: 3	
Tests		
A: 1(6)	B: 0(5)	C: 1(5)

$f(t) = t^7 - 56t + 48$		
$\mathrm{d}(f) = 2^{24}3^6 7^8$	$\mathrm{d}_r(f) = 2^4 3^1 7^2$	
Gesamtzeit: 0.08 sec	Faktorisierung von $\mathrm{d}_r(f)$: 0.00 sec	
2–Maximalordnung	Index: 2^9	
Zeit: 0.04 sec	Zeit char. Polynom: 0.00 sec	
Schleifendurchläufe		
Kernalogrithmus: 4	Suche neues φ: 3	
Tests		
A: 2(3)	B: 1(1)	C: 0(0)

$f(t) = t^8 - 8t^7 + 6588344$		
$\mathrm{d}(f) = 2^{42}7^{50}$	$\mathrm{d}_r(f) = 2^6 7^{14}$	
Gesamtzeit: 0.32 sec	Faktorisierung von $\mathrm{d}_r(f)$: 0.01 sec	
2–Maximalordnung	Index: 2^7	
Zeit: 0.02 sec	Zeit char. Polynom: 0.01 sec	
Schleifendurchläufe		
Kernalogrithmus: 2	Suche neues φ: 0	
Tests		
A: 0(0)	B: 0(0)	C: 0(0)
7–Maximalordnung	Index: 7^{21}	
Zeit: 0.27 sec	Zeit char. Polynom: 0.00 sec	
Schleifendurchläufe		
Kernalogrithmus: 2	Suche neues φ: 1	
Tests		
A: 0(1)	B: 0(1)	C: 1(1)

$f(t) = t^8 + 2t^7 - 327617t^6 + 4967336t^5 - 30273556t^4 + 94618928t^3$ $-159301148t^2 + 136438758t - 46443931$	
$\mathrm{d}(f) = 2^8 5^2 41^2 47^4 401^3 12253^2$ $11031067^2 17856506257631^2$	$\mathrm{d}_r(f) = 2^1 5^2 41^2 47^1 401^1 12253^2$ $11031067^2 17856506257631^2$
Gesamtzeit: 3.23 sec	Faktorisierung von $\mathrm{d}_r(f)$: 1.82 sec

5–Maximalordnung	Index: 5^1	
Zeit: 0.01 sec	Zeit char. Polynom: 0.00 sec	
Schleifendurchläufe		
Kernalogrithmus: 0	Suche neues φ: 0	
Tests		
A: 0(0)	B: 0(0)	C: 0(0)

41–Maximalordnung	Index: 41^1	
Zeit: 0.02 sec	Zeit char. Polynom: 0.00 sec	
Schleifendurchläufe		
Kernalogrithmus: 0	Suche neues φ: 0	
Tests		
A: 0(0)	B: 0(0)	C: 0(0)

12253–Maximalordnung	Index: 12253^1	
Zeit: 0.02 sec	Zeit char. Polynom: 0.00 sec	
Schleifendurchläufe		
Kernalogrithmus: 0	Suche neues φ: 0	
Tests		
A: 0(0)	B: 0(0)	C: 0(0)

11031067–Maximalordnung	Index: 11031067^1	
Zeit: 0.03 sec	Zeit char. Polynom: 0.00 sec	
Schleifendurchläufe		
Kernalogrithmus: 0	Suche neues φ: 0	
Tests		
A: 0(0)	B: 0(0)	C: 0(0)

17856506257631–Maximalordnung	Index: 17856506257631^1	
Zeit: 0.63 sec	Zeit char. Polynom: 0.00 sec	
Schleifendurchläufe		
Kernalogrithmus: 0	Suche neues φ: 0	
Tests		
A: 0(0)	B: 0(0)	C: 0(0)

$f(t) = t^{10} - 10t^9 - 3874204890$	
$\mathrm{d}(f) = 2^{18}3^{162}5^{18}11^1$	$\mathrm{d}_r(f) = 2^2 3^{34} 5^2 11^1$
Gesamtzeit: 2.99 sec	Faktorisierung von $\mathrm{d}_r(f)$: 0.02 sec

3–Maximalordnung	Index: 3^{75}	
Zeit: 2.92 sec	Zeit char. Polynom: 0.33 sec	
Schleifendurchläufe		
Kernalogrithmus: 6	Suche neues φ: 4	
Tests		
A: 1(4)	B: 0(3)	C: 3(3)

$f(t) = t^{11} - 5082t^9 - 181016t^8 + 820908t^7 + 826455168t^6$ $+28828948896t^5 + 557148848256t^4 + 6517138725504t^3$ $+46090291534848t^2 + 182206040924160t + 310338030993408$	
$\mathrm{d}(f) = 2^{118}3^{39}11^{52}191^1 6037^1$ $32183^1 69899^2 502121046523^1$ 43477717621421^1 3763521724294384699^1	$\mathrm{d}_r(f) = 2^{35}3^{12}11^{12}191^1 6037^1$ $32183^1 69899^1 502121046523^1$ 43477717621421^1 3763521724294384699^1
Gesamtzeit: 24.13 sec	Faktorisierung von $\mathrm{d}_r(f)$: 14.45 sec

2–Maximalordnung	Index: 2^{52}	
Zeit: 1.30 sec	Zeit char. Polynom: 0.11 sec	
Schleifendurchläufe		
Kernalogrithmus: 10	Suche neues φ: 11	
Tests		
A: 4(21)	B: 1(17)	C: 2(16)

3–Maximalordnung	Index: 3^{15}	
Zeit: 0.59 sec	Zeit char. Polynom: 0.03 sec	
Schleifendurchläufe		
Kernalogrithmus: 6	Suche neues φ: 4	
Tests		
A: 1(7)	B: 1(6)	C: 1(5)

11–Maximalordnung	Index: 11^{22}	
Zeit: 7.56 sec	Zeit char. Polynom: 1.62 sec	
Schleifendurchläufe		
Kernalogrithmus: 5	Suche neues φ: 2	
Tests		
A: 2(2)	B: 0(0)	C: 0(0)

$f(t) = t^{11} - 132t + 120$	
$\mathrm{d}(f) = 2^{30}3^{10}5^{10}11^{12}$	$\mathrm{d}_r(f) = 2^3 3^1 5^1 11^2$
Gesamtzeit: 0.91 sec	Faktorisierung von $\mathrm{d}_r(f)$: 0.01 sec

2–Maximalordnung	Index: 2^{11}	
Zeit: 0.86 sec	Zeit char. Polynom: 0.55 sec	
Schleifendurchläufe Kernalogrithmus: 2	Suche neues φ: 5	
Tests A: 2(12)	B: 0(10)	C: 0(10)

$f(t) = t^{12} + t^9 + 3t^6 + 12t^4 + 8$	
$\mathrm{d}(f) = 2^{21}3^{12}5^3 23^4 43^1 38629^1$	$\mathrm{d}_r(f) = 2^5 3^1 5^2 23^1 43^1 38629^1$
Gesamtzeit: 0.24 sec	Faktorisierung von $\mathrm{d}_r(f)$: 0.03 sec

2–Maximalordnung	Index: 2^6	
Zeit: 0.13 sec	Zeit char. Polynom: 0.02 sec	
Schleifendurchläufe Kernalogrithmus: 4	Suche neues φ: 3	
Tests A: 1(3)	B: 1(2)	C: 1(1)
5–Maximalordnung	Index: 5^1	
Zeit: 0.03 sec	Zeit char. Polynom: 0.00 sec	
Schleifendurchläufe Kernalogrithmus: 0	Suche neues φ: 0	
Tests A: 0(0)	B: 0(0)	C: 0(0)

$f(t) = t^{12} - t^{11} + t^6 - 3t^4 - 10t^2 - 4$	
$\mathrm{d}(f) = 2^{10}1279^1$ 9282895166777041^1	$\mathrm{d}_r(f) = 2^4 1279^1$ 9282895166777041^1
Gesamtzeit: 0.37 sec	Faktorisierung von $\mathrm{d}_r(f)$: 0.18 sec

2–Maximalordnung	Index: 2^2	
Zeit: 0.19 sec	Zeit char. Polynom: 0.03 sec	
Schleifendurchläufe Kernalogrithmus: 3	Suche neues φ: 4	
Tests A: 0(9)	B: 1(9)	C: 1(8)

$f(t) = t^{14} + 2t^{12} - 2t^{11} - t^{10} - 2t^7 - t^4 - 1$	
$\mathrm{d}(f) = 2^{20} 271^1 719^1 811^1 3127693^1$	$\mathrm{d}_r(f) = 2^3 271^1 719^1 811^1 3127693^1$
Gesamtzeit: 0.23 sec	Faktorisierung von $\mathrm{d}_r(f)$: 0.05 sec

2–Maximalordnung	Index: 2^4	
Zeit: 0.18 sec	Zeit char. Polynom: 0.06 sec	
Schleifendurchläufe		
Kernalogrithmus: 3	Suche neues φ: 2	
Tests		
A: 0(5)	B: 1(5)	C: 0(4)

$f(t) = t^{15} - 240t + 224$	
$\mathrm{d}(f) = 2^{70} 3^{16} 5^{16} 7^{14}$	$\mathrm{d}_r(f) = 2^5 3^2 5^2 7^1$
Gesamtzeit: 12.91 sec	Faktorisierung von $\mathrm{d}_r(f)$: 0.01 sec

2–Maximalordnung	Index: 2^{26}	
Zeit: 12.88 sec	Zeit char. Polynom: 11.40 sec	
Schleifendurchläufe		
Kernalogrithmus: 5	Suche neues φ: 4	
Tests		
A: 1(9)	B: 0(8)	C: 1(8)

$f(t) = t^{16} + 132t^{14} + 6868t^{12} + 179570t^{10} + 2494972t^8 + 18111820t^6$ $+65000173t^4 + 102234000t^2 + 46240000$	
$\mathrm{d}(f) = 2^{72} 3^8 5^{20} 7^8 13^{12} 17^6 53^{12}$ $7901^4 3665437^4$	$\mathrm{d}_r(f) = 2^{13} 3^2 5^5 7^2 13^1 17^2 53^1$ $7901^2 3665437^2$
Gesamtzeit: 3.06 sec	Faktorisierung von $\mathrm{d}_r(f)$: 0.17 sec

2–Maximalordnung	Index: 2^{36}	
Zeit: 0.59 sec	Zeit char. Polynom: 0.08 sec	
Schleifendurchläufe		
Kernalogrithmus: 7	Suche neues φ: 6	
Tests		
A: 1(9)	B: 4(8)	C: 0(4)

3–Maximalordnung	Index: 3^4	
Zeit: 0.04 sec	Zeit char. Polynom: 0.00 sec	
Schleifendurchläufe		
Kernalogrithmus: 0	Suche neues φ: 0	
Tests		
A: 0(0)	B: 0(0)	C: 0(0)

5–Maximalordnung	Index: 5^{10}
Zeit: 0.35 sec	Zeit char. Polynom: 0.00 sec
Schleifendurchläufe Kernalogrithmus: 2	 Suche neues φ: 1
Tests A: 0(1) B: 1(1)	 C: 0(0)

7–Maximalordnung	Index: 7^4
Zeit: 0.04 sec	Zeit char. Polynom: 0.00 sec
Schleifendurchläufe Kernalogrithmus: 0	 Suche neues φ: 0
Tests A: 0(0) B: 0(0)	 C: 0(0)

17–Maximalordnung	Index: 17^3
Zeit: 0.05 sec	Zeit char. Polynom: 0.00 sec
Schleifendurchläufe Kernalogrithmus: 0	 Suche neues φ: 0
Tests A: 0(0) B: 0(0)	 C: 0(0)

7901–Maximalordnung	Index: 7901^2
Zeit: 0.07 sec	Zeit char. Polynom: 0.00 sec
Schleifendurchläufe Kernalogrithmus: 0	 Suche neues φ: 0
Tests A: 0(0) B: 0(0)	 C: 0(0)

3665437–Maximalordnung	Index: 3665437^2
Zeit: 0.16 sec	Zeit char. Polynom: 0.00 sec
Schleifendurchläufe Kernalogrithmus: 0	 Suche neues φ: 0
Tests A: 0(0) B: 0(0)	 C: 0(0)

$f(t) = t^{16} - 16t^{15} + 7006302246093750000$	
$\mathrm{d}(f) = 2^{120}3^{226}5^{226}$	$\mathrm{d}_r(f) = 2^{8}3^{30}5^{30}$
Gesamtzeit: 36.29 sec	Faktorisierung von $\mathrm{d}_r(f)$: 0.15 sec

2–Maximalordnung	Index: 2^{41}	
Zeit: 3.81 sec	Zeit char. Polynom: 2.85 sec	
Schleifendurchläufe		
Kernalogrithmus: 4	Suche neues φ: 6	
Tests		
A: 2(15)	B: 0(13)	C: 1(13)

3–Maximalordnung	Index: 3^{105}	
Zeit: 11.29 sec	Zeit char. Polynom: 0.05 sec	
Schleifendurchläufe		
Kernalogrithmus: 5	Suche neues φ: 2	
Tests		
A: 1(2)	B: 1(1)	C: 0(0)

5–Maximalordnung	Index: 5^{105}	
Zeit: 20.56 sec	Zeit char. Polynom: 0.04 sec	
Schleifendurchläufe		
Kernalogrithmus: 5	Suche neues φ: 3	
Tests		
A: 1(3)	B: 1(2)	C: 1(1)

$f(t) = t^{20} - 4t^{12} - 1$	
$\mathrm{d}(f) = 2^{40}107467^{4}$	$\mathrm{d}_r(f) = 2^{2}107467^{1}$
Gesamtzeit: 0.67 sec	Faktorisierung von $\mathrm{d}_r(f)$: 0.03 sec

2–Maximalordnung	Index: 2^{10}	
Zeit: 0.54 sec	Zeit char. Polynom: 0.30 sec	
Schleifendurchläufe		
Kernalogrithmus: 4	Suche neues φ: 2	
Tests		
A: 0(2)	B: 2(2)	C: 0(0)

$f(t) = t^{20} + t^{15} + 2t^{10} - t^5 + 1$		
$\mathrm{d}(f) = 2^{10}3^{10}5^{30}$	$\mathrm{d}_r(f) = 2^1 3^1 5^2$	
Gesamtzeit: 0.09 sec	Faktorisierung von $\mathrm{d}_r(f)$: 0.02 sec	
2–Maximalordnung	Index: 2^5	
Zeit: 0.06 sec	Zeit char. Polynom: 0.00 sec	
Schleifendurchläufe		
Kernalogrithmus: 0	Suche neues φ: 0	
Tests		
A: 0(0)	B: 0(0)	C: 0(0)

$f(t) = t^{21} + 420t - 400$		
$\mathrm{d}(f) = 2^{80}3^{22}5^{40}7^{22}$	$\mathrm{d}_r(f) = 2^4 3^2 5^2 7^2$	
Gesamtzeit: 19.00 sec	Faktorisierung von $\mathrm{d}_r(f)$: 0.03 sec	
2–Maximalordnung	Index: 2^{21}	
Zeit: 15.55 sec	Zeit char. Polynom: 13.89 sec	
Schleifendurchläufe		
Kernalogrithmus: 3	Suche neues φ: 3	
Tests		
A: 1(6)	B: 0(5)	C: 1(5)
5–Maximalordnung	Index: 5^1	
Zeit: 2.87 sec	Zeit char. Polynom: 2.30 sec	
Schleifendurchläufe		
Kernalogrithmus: 1	Suche neues φ: 1	
Tests		
A: 1(1)	B: 0(0)	C: 0(0)
7–Maximalordnung	Index: 7^1	
Zeit: 0.45 sec	Zeit char. Polynom: 0.01 sec	
Schleifendurchläufe		
Kernalogrithmus: 1	Suche neues φ: 1	
Tests		
A: 1(1)	B: 0(0)	C: 0(0)

$f(t) = t^{22} - 22t^{21} - 1285369144044916154703847372 62$	
$\mathrm{d}(f) = 2^{42}3^{441}7^{441}11^{42}23^{1}$	$\mathrm{d}_r(f) = 2^{2}3^{41}7^{41}11^{2}23^{1}$
Gesamtzeit: 325.54 sec	Faktorisierung von $\mathrm{d}_r(f)$: 0.98 sec

3–Maximalordnung	Index: 3^{210}	
Zeit: 86.52 sec	Zeit char. Polynom: 0.09 sec	
Schleifendurchläufe		
Kernalogrithmus: 5	Suche neues φ: 2	
Tests		
A: 1(2)	B: 1(1)	C: 0(0)

7–Maximalordnung	Index: 7^{210}	
Zeit: 237.10 sec	Zeit char. Polynom: 0.08 sec	
Schleifendurchläufe		
Kernalogrithmus: 8	Suche neues φ: 5	
Tests		
A: 2(5)	B: 0(3)	C: 3(3)

$f(t) = t^{25} + 600t - 576$	
$\mathrm{d}(f) = 2^{144}3^{48}5^{52}$	$\mathrm{d}_r(f) = 2^{6}3^{2}5^{4}$
Gesamtzeit: 446.65 sec	Faktorisierung von $\mathrm{d}_r(f)$: 0.04 sec

2–Maximalordnung	Index: 2^{27}	
Zeit: 435.55 sec	Zeit char. Polynom: 392.08 sec	
Schleifendurchläufe		
Kernalogrithmus: 5	Suche neues φ: 5	
Tests		
A: 2(8)	B: 1(6)	C: 1(5)

3–Maximalordnung	Index: 3^{1}	
Zeit: 7.44 sec	Zeit char. Polynom: 6.49 sec	
Schleifendurchläufe		
Kernalogrithmus: 1	Suche neues φ: 1	
Tests		
A: 1(1)	B: 0(0)	C: 0(0)

5–Maximalordnung	Index: 5^{5}	
Zeit: 3.49 sec	Zeit char. Polynom: 2.09 sec	
Schleifendurchläufe		
Kernalogrithmus: 1	Suche neues φ: 1	
Tests		
A: 1(1)	B: 0(0)	C: 0(0)

$f(t) = t^{27} - 756t + 728$	
$\mathrm{d}(f) = 2^{78}3^{84}7^{26}13^{26}$	$\mathrm{d}_r(f) = 2^3 3^6 7^1 13^1$
Gesamtzeit: 101.71 sec	Faktorisierung von $\mathrm{d}_r(f)$: 0.06 sec

2–Maximalordnung	Index: 2^{24}	
Zeit: 99.02 sec	Zeit char. Polynom: 93.03 sec	
Schleifendurchläufe		
Kernalogrithmus: 3	Suche neues φ: 4	
Tests		
A: 1(9)	B: 0(8)	C: 1(8)

3–Maximalordnung	Index: 3^{12}	
Zeit: 2.48 sec	Zeit char. Polynom: 1.26 sec	
Schleifendurchläufe		
Kernalogrithmus: 2	Suche neues φ: 2	
Tests		
A: 2(2)	B: 0(0)	C: 0(0)

$f(t) = t^{29} + 812t - 784$	
$\mathrm{d}(f) = 2^{112}7^{56}29^{30}$	$\mathrm{d}_r(f) = 2^4 7^2 29^2$
Gesamtzeit: 74.95 sec	Faktorisierung von $\mathrm{d}_r(f)$: 0.07 sec

2–Maximalordnung	Index: 2^{29}	
Zeit: 50.37 sec	Zeit char. Polynom: 45.85 sec	
Schleifendurchläufe		
Kernalogrithmus: 3	Suche neues φ: 2	
Tests		
A: 1(2)	B: 0(1)	C: 1(1)

7–Maximalordnung	Index: 7^1	
Zeit: 24.39 sec	Zeit char. Polynom: 22.32 sec	
Schleifendurchläufe		
Kernalogrithmus: 1	Suche neues φ: 1	
Tests		
A: 1(1)	B: 0(0)	C: 0(0)

$f(t) = t^{30} + 234t^{20} - 5678t^{10} + 670097641028$	
$\mathrm{d}(f) = 2^{98}5^{30}13^{10}2311^{10}114269^{9}$ $131497^{10}1466053^{9}$ 95903095582571^{10}	$\mathrm{d}_r(f) = 2^{4}5^{1}13^{1}2311^{1}114269^{1}$ $131497^{1}1466053^{1}$ 95903095582571^{1}
Gesamtzeit: 15.88 sec	Faktorisierung von $\mathrm{d}_r(f)$: 1.08 sec

2–Maximalordnung	Index: 2^{10}	
Zeit: 14.47 sec	Zeit char. Polynom: 13.19 sec	
Schleifendurchläufe		
Kernalogrithmus: 1	Suche neues φ: 1	
Tests		
A: 1(1)	B: 0(0)	C: 0(0)

$f(t) = t^{40} + 5t^{30} + 26t^{20} - 5t^{10} + 1$	
$\mathrm{d}(f) = 2^{60}3^{20}5^{40}13^{20}29^{20}$	$\mathrm{d}_r(f) = 2^{2}3^{1}5^{1}13^{2}29^{1}$
Gesamtzeit: 2.85 sec	Faktorisierung von $\mathrm{d}_r(f)$: 0.15 sec

2–Maximalordnung	Index: 2^{10}	
Zeit: 1.91 sec	Zeit char. Polynom: 0.14 sec	
Schleifendurchläufe		
Kernalogrithmus: 3	Suche neues φ: 2	
Tests		
A: 1(2)	B: 1(1)	C: 0(0)
13–Maximalordnung	Index: 13^{10}	
Zeit: 0.47 sec	Zeit char. Polynom: 0.00 sec	
Schleifendurchläufe		
Kernalogrithmus: 0	Suche neues φ: 0	
Tests		
A: 0(0)	B: 0(0)	C: 0(0)

$f(t) = t^{40} - t^{30} + 2t^{20} + t^{10} + 1$	
$\mathrm{d}(f) = 2^{60}3^{20}5^{60}$	$\mathrm{d}_r(f) = 2^2 3^1 5^2$
Gesamtzeit: 1.85 sec	Faktorisierung von $\mathrm{d}_r(f)$: 0.10 sec

2–Maximalordnung	Index: 2^{10}	
Zeit: 1.71 sec	Zeit char. Polynom: 0.13 sec	
Schleifendurchläufe		
Kernalogrithmus: 3	Suche neues φ: 2	
Tests		
A: 1(2)	B: 1(1)	C: 0(0)

Kapitel 7

Faktorisierung von separablen Polynomen über $\mathbb{Q}_p$

In diesem Kapitel wollen wir zeigen, daß sich der Grundgedanke des lokalen Round 4 Algorithmus auch für die Faktorisierung von separablen Polynomen über dem Körper der p–adischen Zahlen $\mathbb{Q}_p$ verwenden läßt. Wir suchen nicht mehr nach einer $\mathbb{Z}'$–Basis des ganzen Abschlußes von $\mathbb{Z}'$ in $\mathcal{A}_f$, sondern nach einer p–adischen Approximation an die Zerlegung von f in irreduzible Faktoren über $\mathbb{Q}_p$ beziehungsweise den Nachweis der Irreduzibilität von f über $\mathbb{Q}_p$. Dabei fixieren wir wieder eine rationale Primzahl p und kennzeichnen die Quotientenringbildung nach der multiplikativen Gruppe $\mathbb{Z}\backslash p\mathbb{Z}$ durch den Index „ $'$ “.

Analog zur Darstellung von reellen Zahlen im Rechner können wir p–adische Zahlen nur mit einer begrenzten Genauigkeit repräsentieren. Das Henselsche Lemma garantiert uns jedoch, daß sich eine gegebene Zerlegung von f in koprime Faktoren modulo p^κ beliebig genau an eine Faktorisierung in $\mathbb{Q}_p[t]$ mit der gleichen Anzahl von koprimen Faktoren liften läßt. Damit ist klar, daß die Faktorisierung von f über $\mathbb{Q}_p$ nur so genau zu approximieren ist, daß die Anzahl der koprimen Faktoren von f modulo p^κ mit der in $\mathbb{Q}_p[t]$ übereinstimmt.

Fassen wir zunächst zusammen, welche Zerteilung der lokale Round 4 Algorithmus uns in Polynomen beschrieben liefert. Dabei gehen wir davon aus, daß wir den Zerlegungsalgorithmus 5.2.1 mit approximierten Idempotenten, jedoch nicht den erweiterten Dedekindtest, verwenden. Unter diesen Bedingungen berechnet der lokale Round 4

- eine Zerlegung von f in koprime, normierte Polynome $f_1, \dots, f_s$ modulo $p^\kappa\mathbb{Z}'[t]$ so, daß die ganzen Abschlüsse von $\mathbb{Z}'$ in $\mathcal{A}_f$ und $\mathcal{A}_{f_1 \cdot \ldots \cdot f_s}$ isomorph sind und

- der ganze Abschluß von $\mathbb{Z}'$ in $\mathcal{A}_{f_i}$ gleich der Gleichungsordnung eines primitiven, primären Elements der Algebra $\mathcal{A}_{f_i}$ ist.

Der lokale Round 4 zerlegt also entweder die Konstruktionsaufgabe oder findet ein erzeugendes primäres Element, dessen Gleichungsordnung maximal ist. Die einzige Terminationsmöglichkeit besteht somit in dem letzten Fall. Wir verändern die Rückgabewerte des lokalen Round 4 wie folgt. Falls mit dem Dedekindkriterium festgestellt wird, daß die Gleichungsordnung eines Elemets maximal ist, so soll die einelementige Liste mit dem aktuellen erzeugenden Polynom der Algebra statt der Potenzganzheitsbasis zurückgegeben werden. Statt der Bestimmung einer Basis der Modulsumme soll die Vereinigung der Listen zurückgegeben werden. Wir erhalten mit unserem so veränderten lokalen Round 4 das oben angegebene Produkt $f_1, \ldots, f_s$ von Polynomen. Es stellt sich die Frage, ob die erhaltene Faktorisierung von f modulo $p^\kappa\mathbb{Z}'[t]$ schon die anfangs geforderten Eigenschaften einer Approximation an die Zerlegung von f über $\mathbb{Q}_p$ erfüllt. Können wir zeigen, daß die Faktoren f_i über $\mathbb{Q}_p$ irreduzibel sind, so kann keiner der Faktoren beim Liften zu einer Faktorisierung von f in $\mathbb{Q}_p$ mehr zerfallen. Das heißt, statt des Dedekind Tests benötigen wir einen Irreduzibilitätstest für Polynome über $\mathbb{Q}_p$. Leider erfüllen die f_i diese Bedingungen noch nicht. Der lokale Round 4 garantiert uns nur, daß die Algebra $\mathcal{A}_{f_i}$ die direkte Summe von Körpern ist, wobei in jedem Körper ein primitives Element existiert, dessen Gleichungsordnung maximal ist. Wir werden jetzt zeigen, daß die irreduziblen Faktoren von f_i über $\mathbb{Q}$ auch in $\mathbb{Q}_p$ irreduzibel sind. Damit reduziert der lokale Round 4 die Faktorisierung über $\mathbb{Q}_p$ auf eine Faktorisierung über $\mathbb{Q}$. Sei also g ein irreduzibler Teiler von f_i aus $\mathbb{Q}[t]$, so liegt die folgende Situation vor. $\mathcal{F} := \mathcal{A}_g$ ist ein Körper, g hat modulo $p\mathbb{Z}'[t]$ genau einen irreduziblen Faktor, und in $\mathfrak{o}'_\mathcal{F}$ liegt ein Element α mit

- α ist primär
- α erzeugt $\mathcal{F}$ über $\mathbb{Q}$
- $\mathbb{Z}'[\alpha] = \mathfrak{o}'_\mathcal{F}$.

Seien $v_{\mathfrak{P}_1}, \ldots, v_{\mathfrak{P}_r}$ die r nicht äquivalenten Bewertungsfortsetzungen der p–adischen Bewertung von $\mathbb{Q}$ auf $\mathcal{F}$ und $\mathcal{F}_{\mathfrak{P}_i}$ die Vervollständigung von $\mathcal{F}$ bezüglich der durch die Bewertung $v_{\mathfrak{P}_i}$ induzierten Topologie auf $\mathcal{F}$ für alle i aus $\{1, \ldots, r\}$. Da $\mathcal{F}/\mathbb{Q}$ separabel ist, erhalten wir für den Grad der Erweiterung

$$\mathrm{Grad}(g) = [\mathcal{F} : \mathbb{Q}] = \sum_{i=1}^{r} [\mathcal{F}_{\mathfrak{P}_i} : \mathbb{Q}_p].$$

Für einen Beweis verweisen wir auf [We]. Wenn wir zeigen, daß $r = 1$ ist, so gibt es nur genau ein Primideal $\mathfrak{P}$ über p in $\mathcal{F}$, und es gilt $[\mathcal{F}_{\mathfrak{P}} : \mathbb{Q}_p] = \mathrm{Grad}(g)$. Damit ist aber, wie behauptet, g über $\mathbb{Q}_p$ irreduzibel.

Für unseren speziellen Fall hat Kummer einen Satz über die Struktur der über p liegenden Primideale von $\mathfrak{o}_{\mathcal{F}}$ angegeben. Wir werden hier nur die für uns notwendige Aussage zitieren.

Satz 7.0.2 (Kummer) *Sei $\mathcal{F}/\mathbb{Q}$ eine separable Zahlkörpererweiterung und α ein Element aus $\mathfrak{o}'_{\mathcal{F}}$ mit $\mathcal{F} = \mathbb{Q}(\alpha)$ und $\mathfrak{o}'_{\mathcal{F}} = \mathbb{Z}'[\alpha]$. Ist*

$$\bar{\mu}_\alpha = \prod_{i=1}^{r} \bar{g}_i^{e_i}$$

die Zerlegung des Minimalpolynoms von α in irreduzible, koprime Faktoren in $\mathbb{F}_p[t] = \mathbb{Z}'/p\mathbb{Z}'[t]$, so liegen über p die r verschiedenen Primideale

$$\mathfrak{P}_i = p\mathfrak{o}'_{\mathcal{F}} + g_i(\alpha)\mathfrak{o}'_{\mathcal{F}}$$

und $p\mathfrak{o}'_{\mathcal{F}} = \prod_{i=1}^{r} \mathfrak{P}_i^{e_i}$.

Beweis: Den vollständigen Satz von Kummer einschließlich eines Beweises findet man in [We].

Auf Grund des Zerlegungsverhalten von μ_α modulo p — α ist primär — kann nach dem Satz von Kummer also nur genau ein Primideal über p in $\mathcal{F}$ liegen. Unser Polynom g ist entsprechend den obigen Überlegungen irreduzibel über $\mathbb{Q}_p$.

In dem Artikel [Fo/Le] wird zusätzlich behauptet, daß die Polynome f_i über $\mathbb{Q}_p$ irreduzibel sind. Das ist im allgemeinen nicht so, wie folgendes Beispiel zeigt. Seien $l_1(t) = t^3 - t^2 - 1$, $l_2(t) = t^3 + t^2 + 4t - 1$ und $f = l_1 l_2$. f ist separabel, jedoch nicht irreduzibel. Wollen wir die Faktorisierung von f in $\mathbb{Q}_2[t]$ bestimmen, so terminiert unser veränderter lokaler Round 4 mit der einelementigen Liste $[f]$. In der Tat sind l_1 und l_2 in $\mathbb{Q}_2$ irreduzibel. Der Dedekind Test ist jedoch schon für f erfolgreich. Da l_1 kongruent l_2 modulo $2\mathbb{Z}'[t]$ ist, kann der lokale Round 4 auch f nicht zerlegen.

Notation

p	Primzahl
f	normiertes, separables Polynom aus $\mathbb{Z}[t]$
n	$\mathrm{Grad}(f)$
$\mathrm{d}(f)$	Polynomdiskriminante von f
$\mathrm{d}_r(f)$	reduzierte Diskriminante von f
$\mathrm{d}_r(R)$	reduzierte Diskriminante der Ordnung R
δ_{ij}	Kronecker Symbol
E_n	$n \times n$ Einheitsmatrix
$\mathrm{Diag}(d_1, \ldots, d_n)$	Diagonalmatrix mit den Elementen $d_1, \ldots, d_n$ auf der Diagonalen
$\mathbb{F}_p$	endlicher Körper mit p Elementen
$\mathbb{F}_{p^k}$	endlicher Körper mit p^k Elementen
$\mathcal{A}_f$	$\mathbb{Q}[t]/f(t)\mathbb{Q}[t]$
$\mathcal{R}_f$	Gleichungsordnung von $\xi = t + f(t)\mathbb{Q}[t]$
$Cl(\mathbb{Z}, \mathcal{A}_f)$	ganze Abschluß von $\mathbb{Z}$ in $\mathcal{A}_f$
$\mathfrak{o}_f$	Maximalordnung von $\mathcal{A}_f$
$\mathfrak{p}_i$	$i = 1, \ldots, r$ Primideale in $\mathfrak{o}_f$ über p
$\mathcal{J}_p$	$\bigcap_{i=1}^r \mathfrak{p}_i$ das p-Radikal von $\mathfrak{o}_f$
$\mathbb{Z}'$	p-Lokalisierung von $\mathbb{Z}$
$\mathfrak{o}'_f$	Quotientenring von $\mathfrak{o}_f$ nach $\mathbb{Z}'$
$\mathcal{J}'_p$	Quotientenring von $\mathcal{J}_p$ nach $\mathbb{Z}'$

Für $\alpha \in \mathcal{A}_f$ wird definiert:

χ_α	charakteristisches Polynom von α
μ_α	Minimalpolynom von α

Für $\theta \in \mathcal{A}_f$ primär werden definiert:

ν_θ	eindeutiger irreduzibler Faktor von χ_θ modulo p
D_θ	Grad von ν_θ
E_θ	$\mathrm{Grad}(f)/\mathrm{Grad}(\nu_\theta)$
$\frac{L_\theta}{M_\theta}$	$v^*(\nu_\theta(\theta))$ mit $L_\theta, M_\theta \geq 0, ggT(L_\theta, M_\theta) = 1$
η_θ	$\nu_\theta(\theta)^{r_\theta}/p^{s_\theta}$ mit $r_\theta L_\theta - s_\theta M_\theta = 1$ $(r_\theta, s_\theta \in \mathbb{N})$

Literaturverzeichnis

[Ar] Artin, E.
Theory of Algebraic Numbers,
Göttingen 1959

[Bö85] Böffgen, R.
Der Algorithmus von Ford/Zassenhaus zur Berechnung von Ganzheitsbasen in Polynomalgebren,
Diplomarbeit Saarbrücken 1985

[Bö87] Böffgen, R.
Der Algorithmus von Ford/Zassenhaus zur Berechnung von Ganzheitsbasen in Polynomalgebren,
Annales Universitatis Saraviensis Series Mathematicae Vol. 1 No. 3 1987

[Co] Cohen, H.
A Course in Computational Algebraic Number Theory,
Springer-Verlag 1993

[Fo78] Ford, D.
On the Construction of the Maximal Order in a Dedekind Domain,
Ph.D. Dissertation, Ohio State Universaty 1978

[Fo87] Ford, D.
The Construction of Maximal Orders over a Dedekind Domain,
Journal Symbolic Computation 1987

[Fo/Le] Ford, D. und Letard, P.
Implementing the Round Four Maximal Order Algorithm,
Journal de Théorie des Nombres de Bordeaux 1993

[Ha] Hasse, H.
Zahlentheorie
Akademie – Verlag Berlin 1963

[Ja] Jacobson, N.
Basic Algebra I,
W. H. Freeman and Company 1974

[Na] Narkiewicz, W.
Elementary and Analytic Theory of Algebraic Number,
Springer Verlag Berlin Heidelberg New York 1990
PWN –Polish Scienific Publishers– Warzawa 1990

[Po/Za] Pohst, M. und Zassenhaus, H.
Algorithmic algebraic number theory,
Cambridge Universaty Press 1993

[Qe] Qerenburg, B.
Mengentheoretische Topologie,
Springer Verlag Berlin Heidelberg New York 1979

[Ri] Ribenboim, P.
Algebraic Number Theory,
PURE AND APPLIED MATHEMATICS VOLUM XXVII

[We] Weiss, E.
Algebraic Number Theory,
McGraw-Hill 1963

[Za] Zassenhaus, H.
On Structural Stability,
Communications in algebra, 8(19), 1980