Primidealzerlegung in Komposita von Zahlkörpern

Diplomarbeit von
Siegfried Pohl

Angefertigt am Institut für Mathematik der
Technischen Universität Berlin
2002

Inhaltsverzeichnis

Erklärung **v**

Bezeichnungen **vii**

Einleitung **ix**

1 Grundlagen **1**
1.1 Von Algebraischen Zahlen zu Indexteilern 1
1.2 Dedekindringe 5
1.3 Primidealzerlegung in Erweiterungen 8
1.4 Der Algorithmus von Buchmann-Lenstra 12

2 Der Algorithmus von Fieker **21**
2.1 Primitivitätsnachweis in Zahlkörpern 22
2.2 Bestimmung primitiver Elemente in Komposita von Zahlkörpern 27
2.3 Vermeidung von Indexteilern durch Wechsel des primitiven Elementes 34

3 Primidealfaktorisierung durch Primärdekomposition **43**
3.1 Primärdekomposition in noetherschen Ringen 44
3.2 Primärdekomposition über endlichen Körpern 47
3.3 Der verallgemeinerte Kummersche Zerlegungssatz 53
3.4 Primidealfaktorisierung in der Gleichungsordnung 60
3.5 Indexteilerbestimmung in Komposita 63
3.6 Primidealzerlegung in Komposita Teil 1 69
3.7 Primidealzerlegung in Komposita Teil 2 73

A Repräsentation im Computer **77**
A.1 Darstellung von algebraischen Zahlen 77
A.2 Darstellung von Idealen 79

B Beispiele und Berechnungen am Computer **81**
B.1 Schnelle Regularitätsbestimmung 81
B.2 Beispiele für die $\mathfrak{S}$-Schranke 85
B.3 Leistung des OrderShort Algorithmus 88
B.4 Primidealfaktorisierung in „großen“ Komposita 89

Literaturverzeichnis **94**

Index **97**

Erklärung

Die selbstständige und eigenhändige
Anfertigung versichere ich an Eides statt.

Berlin, den 20. November 2002

(Siegfried Pohl)

Bezeichnungen

In dieser Arbeit gelten folgende Bezeichnungen:

$\mathbb{N}_n$	$\{1, 2, \ldots, n\}$
$\mathbb{N}_{n,m}$	$\{n, n+1, \ldots, m\}$
$\mathbb{N}^0$	$\mathbb{N} \cup \{0\}$
$\mathbb{P}$	Primzahlen
R, S, Λ	Integritätsringe
$\mathfrak{Q}(R)$	Quotientenkörper von R
$\mathrm{Cl}(R, S)$	Ganzer Abschluss von R in S
$\mathcal{U}(R)$	Einheitengruppe von R
$\mathfrak{a}, \mathfrak{b}, \mathfrak{c}$	Ideale eines Ringes
$\mathfrak{p}, \mathfrak{p}_1, \mathfrak{p}_2, \ldots$	Primideale eines Ringes
$\mathcal{I}_R$	Menge der Ideale des Ringes R
$\mathbb{P}_R$	Menge der Primideale des Ringes R
$\mathcal{MI}_R$	Menge der maximalen Ideale des Ringes R
$\mathcal{I}_R^\times$	$\mathcal{I}_R \setminus \{0\}$
$\mathbb{P}_R^\times$	$\mathbb{P}_R \setminus \{0\}$
$\mathcal{MI}_R^\times$	$\mathcal{MI}_R \setminus \{0\}$
$\langle r \rangle_R$	das von $r \in R$ in R erzeugte Hauptideal
$\langle A \rangle_R$	das von $A \subseteq R$ in R erzeugte Ideal
$\mathcal{F}, \mathcal{F}_1, \mathcal{F}_2, \ldots$	algebraische Zahlkörper
$\mathcal{K}$	Zahlkörperkompositum
$\vartheta, \vartheta_1, \vartheta_2, \ldots$	primitive Elemente
σ_i	i-te $\mathbb{Q}$-Einbettung eines Zahlkörpers in $\mathbb{C}$
$\vartheta^{(i)}$	i-te Konjugierte von ϑ
$i(\vartheta)$	Index von ϑ
M_ϑ	Darstellungsmatrix von ϑ
$\mathcal{O}$	Ordnung eines Zahlkörpers
$\mathfrak{o}_\mathcal{F}$	Maximalordnung des Zahlkörpers $\mathcal{F}$
$\tilde{e}(\mathfrak{p}\|\langle p \rangle)$	Verzweigungsindex in der Gleichungsordnung

Bezeichnungen (Fortsetzung):

$\tilde{f}(\mathfrak{p}\|\langle p\rangle)$	Trägheitsgrad in der Gleichungsordnung
$\mathrm{Rad}(\mathfrak{a})$	Radikal von $\mathfrak{a}$
$\mathrm{ass}(\mathfrak{a})$	das zu $\mathfrak{a}$ assoziierte Primideal
$I_p(\mathcal{O})$	p-Radikal der Ordnung $\mathcal{O}$
$\mathrm{C}_\alpha(t)$	charakteristisches Polynom von α
$\overline{M}^p$	Matrix M reduziert modulo p
$\overline{f}^p(t)$	Polynom f reduziert modulo p
ξ_α	Einsetzungshomomorphismus $f(t) \mapsto f(\alpha)$
π	kanonische Projektion
sgn	Signumabbildung
$HT(f)$	Führungsterm des Polynoms f
Id_A	Identität auf der Menge A
O_R	die Null des Ringes R
1_R	die Eins des Ringes R
$\mathcal{S}_n$	Permutationsgruppe

Einleitung

„Indexteiler? Das sind doch die Dinger, ohne die das Leben so langweilig wäre.“
(Dr. Carsten Friedrichs)

Die Maximalordnung eines algebraischen Zahlkörpers ist als Dedekindring auch dadurch gekennzeichnet, dass jedes echte Ideal eine bis auf die Reihenfolge der Faktoren eindeutige Darstellung als Produkt von Primidealen besitzt. Die Möglichkeit, diese Zerlegung effektiv zu berechnen, ist nicht nur für sich allein genommen interessant, sondern findet auch in anderen Bereichen der algorithmischen algebraischen Zahlentheorie Anwendung, zum Beispiel beim Ermitteln der Klassengruppe.

Diese Arbeit beschäftigt sich mit der Berechnung der Primidealfaktorisierung in Zahlkörpern, welche als Komposita gegeben sind. Zahlkörperkomposita treten zum Beispiel in kanonischer Weise beim Ermitteln von Klassenkörpern auf. Besondere Aufmerksamkeit wurde auf den konstruktiven Aspekt gelegt, d. h. die Arbeit ist unter der Fragestellung entstanden, wie man etwas konkret berechnen kann, anstatt zum Beispiel nach theoretischen Existenzaussagen zu suchen.

Ist ein Zahlkörper als Kompositum von mehreren Zahlkörpern gegeben, bedeutet das, dass die bekannten Verfahren zur Primidealfaktorisierung nur noch eingeschränkt angewendet werden können. Im Rahmen dieser Arbeit wurden daher zwei Verfahren entwickelt, welche es in dieser Form noch nicht gibt. Auch wurde die Theorie weiter vorangetrieben, so es zur mathematischen Fundierung der entwickelten Algorithmen notwendig war.

Kapitel 1 ist das Grundlagenkapitel. Besprochen wird die bekannte Theorie der Primidealfaktorisierung in Zahlkörpern, welche nicht als Kompositum gegeben sind. Insbesondere werden immer ein primitives Element und die Maximalordnung des Zahlkörpers als bekannt vorausgesetzt. Schwerpunkt des Kapitels sind der Zerlegungssatz von Kummer und der Algorithmus von Buchmann-Lenstra.

In Kapitel 2 wird ein Verfahren vorgestellt, mit dem es möglich ist, effizient in einem Kompositum ein primitives Element zu bestimmen, um dann

den Zerlegungssatz anwenden zu können. Anschließend wird untersucht, in wieweit es möglich ist, in einem Zahlkörper ein primitives Element zu suchen, welches für eine gegebene Primzahl kein Indexteiler ist. Der momentan aktuelle Stand der Forschung wird eingehend diskutiert und erklärt.

Im dritten Kapitel wird untersucht, in wieweit Primärdekomposition zur Primidealfaktorisierung in Komposita eingesetzt werden kann. Zuerst wird die Technik der Primärdekomposition im Detail diskutiert. Dann wird im theoretischen Teil des dritten Kapitels der verallgemeinerte Kummersche Zerlegungssatz für Komposita bewiesen, und es wird erläutert, warum die Primärdekomposition für beliebige Komposita nicht einsetzbar ist. Anschließend wird die bereitgestellte Technik und Theorie in Algorithmen umgesetzt. Es werden einerseits Komposita betrachtet, für die die Maximalordnung als bekannt vorausgesetzt wird. Andererseits wird diese Voraussetzung fallen gelassen und überprüft, welche Aussagen man auf diesen Fall retten kann.

Das zweite und dritte Kapitel sind im Prinzip voneinander unabhängig, jedoch vereinfachen sich die Algorithmen des dritten Kapitels teilweise durch Benutzung von Ergebnissen des zweiten. Wo es Querverbindungen gibt, sind diese aufgeführt.

Der Anhang ist zweigeteilt: Zuerst werden die computerinternen Repräsentationen der in dieser Arbeit betrachteten zahlentheoretischen Strukturen erklärt. Dieser Teil ist kurz gehalten, es werden nur die Begriffe erläutert, die tatsächlich in dieser Arbeit benutzt werden. Der zweite Teil des Anhangs besteht aus Beispielen, welche am Computer berechnet wurden.

Abgeschlossen wird die vorliegende Arbeit durch ein Literaturverzeichnis und einen Index der wichtigsten Begriffe.

Ich möchte mich an dieser Stelle bei Herrn Prof. Dr. M. E. Pohst herzlich für sein väterliches Geleit durch das Erstellen dieser Arbeit bedanken.

Ich danke Dr. Claus Fieker und Dipl.-Math. Janis Meyer für die Durchsicht einer vorläufigen Fassung dieser Arbeit. Darüber hinaus gilt mein Dank Dr. Jürgen Klüners, Dr. Florian Heß und Markus Wagner für viele anregende Diskussionen und Tipps. Sebastian Freundt schulde ich Dank für seine LaTeX-Ratschläge.

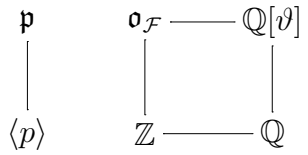
Persönlich möchte ich mich an dieser Stelle bei Mathias, Carsten, Claus und Max bedanken.

Zum Schluss bedanke ich mich beim Bundesministerium für Verteidigung bei den zuständigen Stellen, die mir das Studium finanziert haben.

Ich widme diese Arbeit Major Gerald Heuer †, stellvertretend für alle, die es gut mit mir meinen.

Kapitel 1

Grundlagen



Dieses Kapitel bespricht die Theorie der Primidealzerlegung in algebraischen Zahlkörpern, welche nicht als Kompositum dargestellt werden. Insbesondere ist also ein primitives Element bekannt. Hauptgegenstand ist der Zerlegungssatz von Kummer[1], der die komplette Zerlegung einer Primzahl in einem algebraischen Zahlkörper beschreibt, welche kein Indexteiler ist. Abgeschlossen wird das Kapitel durch den Algorithmus von Buchmann[2]-Lenstra[3], der für den Indexteilerfall entwickelt wurde.

Die in diesem Kapitel aufgeführten Definitionen und Sätze findet man in vielen klassischen Werken zur algebraischen Zahlentheorie, etwa [Poh93, PZ97, Coh93, Nar89, Neu92].

1.1 Von Algebraischen Zahlen zu Indexteilern

Zuerst wird der Begriff der algebraischen Zahl und der ganzen algebraischen Zahl eingeführt:

Definition 1.1. *Eine komplexe Zahl $\alpha \in \mathbb{C}$ heißt **algebraische Zahl**, falls es ein $f(t) \in \mathbb{Q}[t]$ gibt, so dass $f(\alpha) = 0$ gilt. Ist $f(t)$ normiert mit Koeffizienten aus $\mathbb{Z}$, nennt man α **ganze algebraische Zahl**.*

[1] Ernst Eduard Kummer, 1810 – 1893
[2] Johannes Buchmann, $\star$1953
[3] Hendrik Willem Lenstra, $\star$1949

Das Wort „algebraisch“ kommt aus dem Arabischen (9. Jahrhundert n. Chr.) und bedeutet in etwa „Rechnen mit Gleichungen“ [Bos96]. Alle komplexen Zahlen, welche nicht algebraisch sind, nennt man **transzendente Zahlen**. Eine wichtige zahlentheoretische Struktur, ist die des algebraischen Zahlkörpers:

Definition 1.2. *Ein Teilkörper $\mathcal{F}$ von $\mathbb{C}$ heißt **algebraischer Zahlkörper**, falls die Erweiterung $\mathcal{F}/\mathbb{Q}$ endlich ist. $\mathcal{F}$ hat dann als $\mathbb{Q}$-Vektorraum betrachtet endliche Dimension $\dim_{\mathbb{Q}}(\mathcal{F})$, welche man den **Grad des Zahlkörpers** $\deg(\mathcal{F})$ nennt.*

Statt des Begriffes „algebraischer Zahlkörper“, sagt man oft auch nur **Zahlkörper**. Man kann in jedem Zahlkörper die Teilmenge betrachten, die nur aus den ganzen algebraischen Zahlen besteht:

Definition 1.3. *Sei $\mathcal{F}$ algebraischer Zahlkörper. Dann nennt man die Menge*

$$\mathfrak{o}_{\mathcal{F}} := \{\alpha \in \mathcal{F} \mid \alpha \textit{ ist ganze algebraische Zahl }\}$$

*die **Maximalordnung $\mathfrak{o}_{\mathcal{F}}$ von $\mathcal{F}$**.*

Die Maximalordnung $\mathfrak{o}_{\mathcal{F}}$ eines Zahlkörpers $\mathcal{F}$ bildet einen Unterring, dessen additive Struktur eine freie abelsche Gruppe vom Rang $\mathrm{Rg}(\mathfrak{o}_{\mathcal{F}}) = n$ ist. Man kann daher die Maximalordnung eines Zahlkörpers als freien $\mathbb{Z}$-Modul vom Rang n ansehen. Auch erfüllen Maximalordnungen die Dedekindringeigenschaften, siehe (1.2). Eine alternative Bezeichnung für die Maximalordnung ist der Begriff des **Ringes der ganzen algebraischen Zahlen**.

$\mathbb{Q}$ ist perfekt, damit ist jede Erweiterung separabel. Ein algebraischer Zahlkörper $\mathcal{F}$ ist per Definition eine endliche Erweiterung von $\mathbb{Q}$. Man kann den Satz vom primitiven Element [Bos96, 3.6, Satz 12] anwenden, und erhält ein primitives Element ϑ von $\mathcal{F}$. Mit diesem ϑ kann man $\mathcal{F}$ als Menge explizit hinschreiben durch

$$\mathcal{F} = \{a_0 + a_1\vartheta + \ldots + a_{\deg(\mathcal{F})-1}\vartheta^{\deg(\mathcal{F})-1} \mid a_i \in \mathbb{Q},\ i \in \mathbb{N}_{\deg(\mathcal{F})-1}\},$$

weshalb man für $\mathcal{F}$ auch die Bezeichnung $\mathbb{Q}[\vartheta]$ verwendet. Die verschiedenen Potenzen $\{1, \vartheta, \ldots, \vartheta^{\deg(\mathcal{F})-1}\}$ nennt man eine **Potenzbasis von $\mathcal{F}$**.

Für jedes $\vartheta \in \mathcal{F}$ existiert ein normiertes Polynom $m_\vartheta(t) \in \mathbb{Q}[t]$ kleinsten Grades, für welches ϑ Nullstelle ist. Dieses Polynom nennt man das **Minimalpolynom $m_\vartheta(t)$ von ϑ**. Minimalpolynome sind eindeutig bestimmt:

Satz 1.4. *Sei ϑ eine ganze algebraische Zahl, $m_\vartheta(t) \in \mathbb{Z}[t]$ ein normiertes Polynom mit kleinstmöglichem Grad und ϑ Nullstelle von $m_\vartheta(t) \in \mathbb{Z}[t]$. Dann ist $m_\vartheta(t)$ irreduzibel über $\mathbb{Q}$.*

[Mar77, Chapter 2, Theorem 1] Für ein $\vartheta \in \mathcal{F}$ nennt man die anderen Nullstellen des Minimalpolynoms $m_\vartheta(t)$ die **Konjugierten von** ϑ. Je zwei Zahlkörper, die konjugierte primitive Elemente haben, sind isomorph. Sie unterscheiden sich nur um die Art der Einbettung in $\mathbb{C}$:

Definition 1.5. *Sei $\mathcal{F} = \mathbb{Q}[\vartheta]$ Zahlkörper, sei $m_\vartheta(t)$ das Minimalpolynom von ϑ mit Nullstellen $\{\vartheta_1 := \vartheta, \ldots, \vartheta_n\}$, dann nennt man die Abbildungen*

$$\begin{aligned} \sigma_\mu \quad : \quad & \mathbb{Q}[t]/\langle m_\vartheta(t)\rangle_{\mathbb{Q}[t]} \quad \to \mathbb{C} \\ & \sum_{i=0}^{j} a_i t^i \mapsto \sum_{i=0}^{j} a_i \vartheta_\mu^i \end{aligned}$$

*für $\mu \in \mathbb{N}_n$ die $\mathbb{Q}$-**Einbettungen von $\mathcal{F}$ in** $\mathbb{C}$.*

Wenn man von einem algebraischen Zahlkörper $\mathcal{F}$ spricht, meint man daher eigentlich die algebraische Struktur $\mathbb{Q}[t]/\langle m_\vartheta(t)\rangle_{\mathbb{Q}[t]}$, zusammen mit einer Einbettung σ_i.

Bemerkung 1.6. *In dieser Arbeit soll ein Zahlkörper $\mathcal{F}$ immer als die algebraische Struktur $\mathbb{Q}[t]/\langle m_\vartheta(t)\rangle_{\mathbb{Q}[t]}$, zusammen mit einer $\mathbb{C}$-Einbettung aufgefasst werden.*

Sei für den Rest dieses Abschnittes $\mathcal{F}$ Zahlkörper mit primitivem Element ϑ. $m_\vartheta(t)$ sei das Minimalpolynom von ϑ und $\deg(m_\vartheta(t)) =: n$.

Betrachtet man bestimmte $\mathbb{Z}$-Untermoduln der Maximalordnung, erhält man den Begriff einer Ordnung:

Definition 1.7. *Ein Teilring $\mathcal{O}$ von $\mathfrak{o}_\mathcal{F}$ heißt **Ordnung** von $\mathcal{F}$, falls $\mathcal{O}$ freier $\mathbb{Z}$-Modul vom Rang n ist und die Eins enthält.*

Die am einfachsten zu konstruierende Ordnung ist die Gleichungsordnung:

Definition 1.8. *Sei $\mathbb{Q}[\vartheta]$ Zahlkörper, dann ist der $\mathbb{Z}$-Modul*

$$\mathbb{Z}[\vartheta] := \{a_0 + a_1\vartheta + \ldots + a_{n-1}\vartheta^{n-1} \mid a_i \in \mathbb{Z},\ i \in \mathbb{N}_{n-1}\}$$

*eine Ordnung von $\mathbb{Q}[\vartheta]$, welche man die **Gleichungsordnung** nennt.*

Für zwei gegebene Ordnungen $\mathcal{O}_1 \supseteq \mathcal{O}_2$ eines Zahlkörpers, die per Definition $\mathbb{Z}$-Moduln vom Rang n sind, ist der Faktormodul $\mathcal{O}_1/\mathcal{O}_2$ endlich. Setzt man $\mathcal{O}_1 := \mathfrak{o}_\mathcal{F}$ erhält man den Begriff des Index:

Definition 1.9. *Sei $\mathcal{O}$ Ordnung von $\mathcal{F}$, dann bezeichnet man die Mächtigkeit des Faktormoduls $\mathfrak{o}_\mathcal{F}/\mathcal{O}$ als den **Index von** $\mathcal{O}$.*

Bildet man für einen Zahlkörper den Faktormodul der Maximalordnung nach der Gleichungsordnung, erhält man den Begriff des Index eines primitiven Elementes:

Definition 1.10. *Man nennt die Zahl* $i(\vartheta) := \#\mathfrak{o}_K/\mathbb{Z}[\vartheta]$ *den* ***Index von*** ϑ ***in*** $\mathbb{Q}[\vartheta]$. *Eine Primzahl* $p \in \mathbb{P}_\mathbb{Z}$ *mit* $p \mid i(\vartheta)$ *heißt* ***Indexteiler von*** ϑ.

Die Indexteiler spielen in der Theorie der Primidealzerlegung eine große Rolle.

Eine Methode den Index zu berechnen, benötigt den Begriff der Diskriminante, der wiederum über die Begriffe Norm und Spur definiert ist:

Definition 1.11. *Für eine* $\mathbb{Q}$*-Basis* $\{\omega_1, \ldots, \omega_n\}$ *von* $\mathcal{F}$ *existiert zu jedem* $\alpha \in \mathcal{F}$ *eine Matrix* $M_\alpha = (m_{ij}) \in \mathbb{Q}^{n\times n}$ *mit*

$$\alpha \cdot (\omega_1, \ldots, \omega_n) = (\omega_1, \ldots, \omega_n) \begin{pmatrix} m_{11} & \ldots & m_{1n} \\ \vdots & & \vdots \\ m_{n1} & \ldots & m_{nn} \end{pmatrix}$$

M_α *nennt man die* ***Darstellungsmatrix von*** α *in der Basis* $\omega_1, \ldots, \omega_n$.

Der Linearen Algebra folgend, definiert man die Begriffe charakteristisches Polynom, Norm und Spur:

Definition 1.12. *Sei* M_α *die Darstellungsmatrix eines Elementes* $\alpha \in \mathcal{F}$. *Man definiert das* ***charakteristische Polynom*** $\mathrm{C}_\alpha(t)$ ***von*** α *durch*

$$\mathrm{C}_\alpha(t) := \det(t \cdot \mathrm{Id}_n - M_\alpha) \in \mathbb{Q}[t],$$

und die ***Norm*** $\mathrm{N}_{\mathcal{F}|\mathbb{Q}}$ ***von*** α *und* ***Spur*** $\mathrm{Tr}_{\mathcal{F}|\mathbb{Q}}$ ***von*** α *durch die Abbildungen*

$$\begin{array}{rcl} \mathrm{N}_{\mathcal{F}|\mathbb{Q}} & : & \mathcal{F} \to \mathbb{Q} \\ & & \alpha \mapsto \det(M_\alpha) \end{array} \qquad \begin{array}{rcl} \mathrm{Tr}_{\mathcal{F}|\mathbb{Q}} & : & \mathcal{F} \to \mathbb{Q} \\ & & \alpha \mapsto \mathrm{Tr}(M_\alpha) \end{array}$$

Ist klar, in welchem Zahlkörper man die Norm oder Spur berechnen will, schreibt man statt $\mathrm{N}_{\mathcal{F}|\mathbb{Q}}$ nur N und statt $\mathrm{Tr}_{\mathcal{F}|\mathbb{Q}}$ nur Tr.

Jetzt kann man die Diskriminantenabbildung erklären:

Definition 1.13. *Sei* $\mathcal{F}$ *Zahlkörper vom Grad* n, *dann definiere die* ***Diskriminante eines*** n***-Tupels*** *durch*

$$\begin{array}{rcl} \mathrm{disc} & : & \mathcal{F}^n \to \mathbb{Q} \\ & & (\alpha_1, \ldots, \alpha_n) \mapsto \det\left(\mathrm{Tr}(\alpha_i\alpha_j)\right)_{1\le i,j\le n} \end{array}$$

Gilt $\alpha_i = \vartheta^{i-1}$, *setzt man*

$$\mathrm{disc}(\vartheta) := \mathrm{disc}(1, \vartheta, \ldots, \vartheta^{n-1}).$$

Alternativ kann man die Diskriminante eines n-Tupels über die Konjugierten der Elemente des n-Tupels berechnen:

Lemma 1.14. *Seien $\alpha_1, \ldots, \alpha_n \in \mathcal{F}$ und $\sigma_1, \ldots, \sigma_n$ die $\mathbb{Q}$-Einbettungen von $\mathcal{F}$. Definiere die Matrix $M = (m_{ij}) \in \mathbb{Q}^{n \times n}$ mit $m_{ij} = \sigma_i(\alpha_j)$, dann gilt*

$$\operatorname{disc}(\alpha_1, \ldots, \alpha_n) = \det(M)^2$$

[Mar77, Chapter 2, Theorem 6] Verschiedene $\mathbb{Z}$-Basen der Maximalordnung $\mathfrak{o}_{\mathcal{F}}$ eines Zahlkörpers $\mathcal{F}$ haben gleiche Diskriminanten. Diese Zahl ist daher eine Invariante von $\mathcal{F}$:

Definition 1.15. *Sei $\alpha_1, \ldots, \alpha_n$ $\mathbb{Z}$-Basis von $\mathfrak{o}_{\mathcal{F}}$. Man nennt die Zahl*

$$\operatorname{disc}(\mathcal{F}) := \operatorname{disc}(\mathfrak{o}_{\mathcal{F}}) := \operatorname{disc}(\alpha_1, \ldots, \alpha_n)$$

*die **Diskriminante von $\mathcal{F}$**.*

Eine Anwendung der Diskriminantenabbildung ist, Elemente eines Zahlkörpers auf lineare Unabhängigkeit zu überprüfen:

Lemma 1.16. *Seien $\alpha_1, \ldots, \alpha_n \in \mathcal{F}$. Die α_i, $i \in \mathbb{N}_n$ sind genau dann linear unabhängig in dem $\mathbb{Q}$-Vektorraum $\mathcal{F}$, wenn $\operatorname{disc}(\alpha_1, \ldots, \alpha_n) \neq 0$ ist.*

[Mar77, Chapter 2, Theorem 7] Die Diskriminante von $\mathcal{F}$ und die von einem primitiven Element ϑ erzeugte Gleichungsordnung stehen in folgender Beziehung:

Satz 1.17. *Für die Gleichungsordnung $\mathbb{Z}[\vartheta]$ von $\mathcal{F}$ gilt*

$$\operatorname{disc}(\mathbb{Z}[\vartheta]) = \operatorname{disc}(\mathcal{F}) \cdot [\mathfrak{o}_{\mathcal{F}} : \mathbb{Z}[\vartheta]]^2.$$

[Coh93, Proposition 4.4.4] Der Index der Gleichungsordnung geht also immer in zweiter Potenz in die Diskriminante der Gleichungsordnung ein. Man erhält so eine Möglichkeit zum Überprüfen, ob die Gleichungsordnung bereits die Maximalordnung ist: Ist die Diskriminante der Gleichungsordnung quadratfrei, stimmen Gleichungsordnung und Maximalordnung überein.

1.2 Dedekindringe

Dieser Abschnitt führt ein in den Begriff des Dedekindringes[4]. In einem Dedekindring gilt im Allgemeinen nicht der Satz von der eindeutigen Primfaktorzerlegung, d. h. Dedekindringe sind im Allgemeinen keine ZPE-Ringe. Für Ideale bleibt dieser Satz aber richtig:

[4] Richard Dedekind, 1831 – 1916

Jedes Ideal eines Dedekindringes lässt sich eindeutig als Produkt von Primidealen darstellen.

Dedekindringe erlangen ihre Bedeutung dadurch, dass die Maximalordnung eines Zahlkörpers die Dedekindringeigenschaften erfüllt, und die Erforschung von Maximalordnungen geschieht über diese abstraktere Betrachtungsweise. Eine interessante historische Abhandlung ist [Ull99].

Zur Definition des Dedekindringes, benötigt man die Begriffe ganz-abgeschlossen und noethersch:

Definition 1.18. *Seien $R \subseteq S$ Integritätsringe.*

- *Ein Element $\alpha \in S$ heißt **ganz über** R, wenn α Nullstelle eines normierten Polynoms $f(t) \in R[t]$ ist.*
- *S heißt **ganz über** R, wenn jedes Element $\alpha \in S$ ganz über R ist.*
- *Definiere den **ganzen Abschluss von** R **in** S durch*

$$\mathrm{Cl}(R, S) := \{\alpha \in S \mid \alpha \text{ ist ganz über } R\}.$$

- *Gilt $S = \mathfrak{Q}(R)$ und $\mathrm{Cl}(R, S) = R$, so heißt R **ganz-abgeschlossen in seinem Quotientenkörper** oder einfach nur **ganz-abgeschlossen**.*

Zum Beispiel ist $\mathbb{Z}$ ganz-abgeschlossen, denn jede rationale Zahl, die Nullstelle eines normierten Polynoms $f(t) \in \mathbb{Z}[t]$ ist, ist schon aus $\mathbb{Z}$.

Definition 1.19. *Ein Integritätsring R heißt **noethersch**[5], falls R eine der drei folgenden äquivalenten Eigenschaften erfüllt:*

- *Jedes Ideal ist endlich erzeugt.*
- *Jede aufsteigende Kette von Idealen wird konstant.*
- *Jede nicht-leere Menge von Idealen hat ein (nicht notwendigerweise eindeutiges) maximales Element bzgl. der Inklusion.*

Die Äquivalenz der Aussagen folgt mit [Mar77, Chapter 3, Exercise 1]. Ein Beispiel für einen nicht noetherschen Ring ist der Polynomring über $\mathbb{Z}$ in unendlich vielen Unbestimmten. Jetzt wird der Begriff des Dedekindringes eingeführt:

Definition 1.20. *Ein Integritätsring R heißt **Dedekindring**, falls R noethersch und ganz-abgeschlossen ist, und jedes von Null verschiedene Primideal ist maximal.*

[5] Emmy Amalie Noether, 1882 – 1935

Für den Begriff des Dedekindringes existieren mindestens vier äquivalente Definitionen, die für sich allein genommen schon interessant sind [PZ97, Chapter 4, (5.6)].

Die für diese Arbeit wichtigste Eigenschaft eines Dedekindringes ist die Möglichkeit, jedes Ideal in Primideale zu faktorisieren:

Satz 1.21. *Sei R Integritätsring. R ist genau dann Dedekindring, wenn jedes Ideal $\mathfrak{a} \in \mathcal{I}_R^\times$ eine bis auf die Reihenfolge der Faktoren eindeutige Darstellung als Produkt von Primidealen besitzt.*

[PZ97, Chapter 4, (5.6)] [Mar77, Chapter 3, Theorem 16] (Dieser Satz und die folgenden Aussagen gelten auch für gebrochene Ideale.) Eine Anwendung von (1.21) ist, für zwei Ideale $\mathfrak{a}, \mathfrak{b}$ eines Dedekindringes den Begriff des Teilers zu definieren:

Definition 1.22. *Sei R Dedekindring, seien $\mathfrak{a}, \mathfrak{b} \in \mathcal{I}_R^\times$. Gilt $\mathfrak{a} \subseteq \mathfrak{b}$, sagt man $\mathfrak{b}$ **teilt** $\mathfrak{a}$ und schreibt $\mathfrak{b} \mid \mathfrak{a}$.*

Man kann mit (1.22) zum Beispiel die Definitionen des **größten gemeinsamem Teilers** und des **kleinsten gemeinsamen Vielfachen** auf Ideale übertragen.

Dedekindringe sind im Allgemeinen keine Hauptidealringe. Es stellt sich aber heraus, dass aus der Implikation

$$R \text{ ist Hauptidealring } \Rightarrow \quad R \text{ ist ZPE-Ring}$$

in Dedekindringen eine Äquivalenz wird [Mar77, Chapter 3, Theorem 18].

Satz 1.23. *Sei R Dedekindring, dann ist R genau dann Hauptidealring, wenn R ZPE-Ring ist.*

Ein Gegenbeispiel, in dem ein ZPE-Ring, welcher kein Dedekindring ist, auch kein Hauptidealring ist, ist $\mathbb{Z}[t]$. Die Verbindung zwischen Dedekindringen und Maximalordnungen stellt folgender Satz her:

Satz 1.24. *Die Maximalordnung eines Zahlkörpers ist ein Dedekindring. Eine Ordnung $\mathcal{O}$ eines Zahlkörpers, welche nicht die Maximalordnung ist, ist noethersch und jedes Primideal ist maximal, aber $\mathcal{O}$ ist nicht ganz-abgeschlossen.*

[Mar77, Chapter 3, Theorem 14]

1.3 Primidealzerlegung in Erweiterungen

Sei für diesen Abschnitt $\mathcal{F} = \mathbb{Q}[\vartheta]$ algebraischer Zahlkörper vom Grad n, $\mathfrak{p} \neq \{0\}$ Primideal von $\mathfrak{o}_\mathcal{F}$ und $p \in \mathbb{P}_\mathbb{Z}$ Primzahl.

Definition 1.25. *Die Menge $\langle p \rangle_\mathbb{Z}$ ist in $\mathfrak{o}_\mathcal{F}$ kein Ideal mehr, wohl aber die Menge*

$$\langle p \rangle_{\mathfrak{o}_\mathcal{F}} = \{p \cdot \alpha \mid \alpha \in \mathfrak{o}_\mathcal{F}\}.$$

*$\langle p \rangle_{\mathfrak{o}_\mathcal{F}}$ nennt man die **Hochhebung des Ideals** $\langle p \rangle_\mathbb{Z}$.*

Gemäß dem letzten Abschnitt ist eine Maximalordnung $\mathfrak{o}_\mathcal{F}$ nicht notwendig ein Hauptidealring und zwar genau dann nicht, wenn $\mathfrak{o}_\mathcal{F}$ kein ZPE-Ring ist. Primelemente sind irreduzibel und die Umkehrung gilt nur in Hauptidealringen. Das bedeutet aber, dass es ein irreduzibles Element in $\mathfrak{o}_\mathcal{F}$ geben kann, welches kein Primelement ist, oder idealtheoretisch: Ist $\mathfrak{o}_\mathcal{F}$ kein ZPE-Ring, kann es ein Primideal $\langle p \rangle_\mathbb{Z}$ in $\mathbb{Z}$ geben, dessen Erzeuger p in $\mathfrak{o}_\mathcal{F}$ irreduzibel ist, die Hochhebung von $\langle p \rangle_\mathbb{Z}$ nach $\mathfrak{o}_\mathcal{F}$ ist aber kein Primideal mehr. Diesen Vorgang bezeichnet man als **Zerlegung von $\langle p \rangle_\mathbb{Z}$ in $\mathfrak{o}_\mathcal{F}$**.

Eine (fast) vollständige Antwort auf das Zerlegungsverhalten von Primidealen in Maximalordnungen gibt der Zerlegungssatz von Kummer, und dieser Abschnitt behandelt die Theorie bis hin zu diesem Satz:

Definition 1.26. *Gilt $\langle p \rangle_\mathbb{Z} \subseteq \mathfrak{p}$, sagt man $\mathfrak{p}$ **liegt über** $\langle p \rangle_\mathbb{Z}$ oder $\langle p \rangle_\mathbb{Z}$ **liegt unter** $\mathfrak{p}$.*

Lemma 1.27. *Folgende Aussagen sind äquivalent:*

- *$\mathfrak{p}$ liegt über $\langle p \rangle_\mathbb{Z}$*
- *$\langle p \rangle_{\mathfrak{o}_\mathcal{F}} \subseteq \mathfrak{p}$*
- *$\langle p \rangle_\mathbb{Z} = \mathfrak{p} \cap \mathbb{Q}$*
- *$\langle p \rangle_\mathbb{Z} = \mathfrak{p} \cap \mathbb{Z}$*
- *$\mathfrak{p} \mid \langle p \rangle_{\mathfrak{o}_\mathcal{F}}$.*

[Mar77, Chapter 3, Theorem 19]. Weiterhin gilt:

Lemma 1.28. *Für ein Primideal $\langle p \rangle_\mathbb{Z}$ aus $\mathbb{Z}$ gibt es mindestens ein Primideal $\mathfrak{p}$ in $\mathfrak{o}_\mathcal{F}$, welches über $\langle p \rangle_\mathbb{Z}$ liegt. Für ein Primideal $\mathfrak{p}$ aus $\mathfrak{o}_\mathcal{F}$ gibt es genau ein Primideal $\langle p \rangle_\mathbb{Z}$ aus $\mathbb{Z}$, welches unter $\mathfrak{p}$ liegt.*

[Mar77, Chapter 3, Theorem 20] Wegen (1.21) lässt sich jedes Ideal in einer Maximalordnung eindeutig darstellen als Produkt von Primidealen. Die Primideale $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$ von $\mathfrak{o}_\mathcal{F}$, welche über einem Primideal $\langle p \rangle_\mathbb{Z}$ von $\mathbb{Z}$ liegen, sind genau diejenigen, die in dieser Faktorisierung auftreten. Die Exponenten dieser Faktorisierung und die Grade der Körpererweiterungen $[\mathfrak{o}_\mathcal{F}/\mathfrak{p} : \mathbb{Z}/\langle p \rangle]$ erhalten eigene Bezeichnungen:

Definition 1.29. *Es liege $\mathfrak{p}$ über $\langle p \rangle_\mathbb{Z}$, dann heißt der genaue Exponent e, mit dem $\mathfrak{p}$ in die Primidealfaktorisierung von $\langle p \rangle_{\mathfrak{o}_\mathcal{F}}$ eingeht, der **Verzweigungsindex** $e(\mathfrak{p}|\langle p \rangle)$ **von** $\mathfrak{p}$ **über** $\langle p \rangle_\mathbb{Z}$.*

Eine alternative Formulierung ist, den Verzweigungsindex als den Exponenten der Potenz von $\mathfrak{p}$ zu definieren, mit der das Primideal $\mathfrak{p}$ das hochgehobene Ideal $\langle p \rangle_{\mathfrak{o}_\mathcal{F}}$ gerade noch teilt.

Definition 1.30. *Es liege $\mathfrak{p}$ über $\langle p \rangle_\mathbb{Z}$, dann sind die Faktorringe $\mathfrak{o}_\mathcal{F}/\mathfrak{p}$ und $\mathbb{Z}/\langle p \rangle_\mathbb{Z}$ Körper. Betrachte mit der Einbettung*

$$\begin{aligned} \kappa \quad : \quad & \mathbb{Z}/\langle p \rangle_\mathbb{Z} \to \mathfrak{o}_\mathcal{F}/\mathfrak{p} \\ & a + \langle p \rangle_\mathbb{Z} \mapsto a + \mathfrak{p} \end{aligned}$$

*$\mathfrak{o}_\mathcal{F}/\mathfrak{p}$ als Körpererweiterung von $\mathbb{Z}/\langle p \rangle_Z$. Den Grad dieser Körpererweiterung nennt man den **Trägheitsgrad** $f(\mathfrak{p}|\langle p \rangle)$ **von** $\mathfrak{p}$ **über** $\langle p \rangle_\mathbb{Z}$.*

Für die Zerlegung eines Primideals sind also unter anderem die Anzahl der Faktoren der Zerlegung, die Verzweigungsindices und die Trägheitsgrade interessant. Diese drei Werte stehen in folgendem Zusammenhang:

Satz 1.31. *Sei*

$$\langle p \rangle_{\mathfrak{o}_\mathcal{F}} = \mathfrak{p}_1^{e_1} \cdot \ldots \cdot \mathfrak{p}_k^{e_k}$$

die Primidealfaktorisierung der Hochhebung von $\langle p \rangle_\mathbb{Z}$ in $\mathfrak{o}_\mathcal{F}$. Dann gilt für die Verzweigungsindices $e(\mathfrak{p}_i|\langle p \rangle)$ und die Trägheitsgrade $f(\mathfrak{p}_i|\langle p \rangle)$

$$n = \sum_{i=1}^{k} e(\mathfrak{p}_i|\langle p \rangle) f(\mathfrak{p}_i|\langle p \rangle).$$

[Mar77, Chapter 3, Theorem 21] Besprochen wird jetzt der Kummersche Zerlegungssatz. Dieser gilt nicht für beliebige Primideale $\langle p \rangle_\mathbb{Z}$ aus $\mathbb{Z}$, sondern nur für solche, für die der Erzeuger p nicht den Index $[\mathfrak{o}_\mathcal{F} : \mathbb{Z}[\vartheta]]$ teilt. Diese Voraussetzung kann man allgemeiner mit dem Begriff des Führers einer Ordnung formulieren:

Definition 1.32. *Sei $\mathcal{O}$ Ordnung von $\mathcal{F}$, dann nennt man*

$$\mathfrak{F}(\mathcal{O}) := \{x \in \mathfrak{o}_{\mathcal{F}} \mid x \cdot \mathfrak{o}_{\mathcal{F}} \subseteq \mathcal{O}\}$$

*den **Führer** von $\mathcal{O}$ in $\mathfrak{o}_{\mathcal{F}}$.*

Eine umgangssprachliche Erklärung des Führers gibt folgende Bemerkung:

Bemerkung 1.33. *Der Führer $\mathfrak{F}(\mathcal{O})$ von $\mathcal{O}$ in $\mathfrak{o}_{\mathcal{F}}$ ist ein Ideal in $\mathcal{O}$ und auch ein Ideal in $\mathfrak{o}_{\mathcal{F}}$. $\mathfrak{F}(\mathcal{O})$ ist das größte Ideal der Maximalordnung $\mathfrak{o}_{\mathcal{F}}$, welches noch vollständig in $\mathcal{O}$ enthalten ist.*

Auch gibt der Begriff des Führers eine Antwort auf die Frage, für welche Ideale in einer beliebigen Ordnung $\mathcal{O}$ eine eindeutige Primidealfaktorisierung existiert. Für beliebige Ideale in beliebigen Ordnungen kann es keine eindeutige Primidealfaktorisierung geben, da $\mathcal{O}$ dann Dedekindring wäre, siehe (1.21) und (1.24). Die Primidealfaktorisierung gilt aber für die Ideale $\mathfrak{a}$ von $\mathcal{O}$, welche comaximal zum Führer $\mathfrak{F}(\mathcal{O})$ sind:

Satz 1.34. *Sei $\mathcal{O}$ Ordnung von $\mathcal{F}$, $\mathfrak{a}$ echtes Ideal in $\mathcal{O}$ und es gelte*

$$\mathfrak{a} + \mathfrak{F}(\mathcal{O}) = \mathcal{O}.$$

Dann besitzt $\mathfrak{a}$ in $\mathcal{O}$ eine, bis auf die Reihenfolge der Faktoren, eindeutige Darstellung als Produkt von Primidealen von $\mathcal{O}$.

[PZ97, Chapter 6, (2.26)] Jetzt wird der Zerlegungssatz besprochen:

Satz 1.35. *Zerlegungssatz von Kummer*
Sei $\mathcal{F} = \mathbb{Q}[\vartheta]$ Zahlkörper mit Minimalpolynom $m_\vartheta(t) \in \mathbb{Z}[t]$. Sei $\mathfrak{F}(\mathbb{Z}[\vartheta])$ der Führer von $\mathbb{Z}[\vartheta]$ in $\mathfrak{o}_{\mathcal{F}}$. Sei $\langle p\rangle_{\mathbb{Z}}$ ein Primideal von $\mathbb{Z}$, für welches gilt, dass $\langle p\rangle_{\mathbb{Z}[\vartheta]}$ comaximal zu $\mathfrak{F}(\mathbb{Z}[\vartheta])$ ist.
$\langle p\rangle_{\mathfrak{o}_{\mathcal{F}}}$ hat in $\mathfrak{o}_{\mathcal{F}}$ folgende Primidealfaktorisierung:

- *Sei $\overline{m_\vartheta(t)}$ die Reduktion von $m_\vartheta(t)$ modulo p und*

$$\overline{m_\vartheta(t)} = \prod_{i=1}^{r} \overline{f_i(t)}^{e_i}, \qquad e_1, \ldots, e_r \in \mathbb{N}$$

die Primpolynomzerlegung von $\overline{m_\vartheta(t)}$ in $\mathbb{F}_p[t]$.

- *Seien $f_i(t) \in \mathbb{Z}[t]$ normierte Urbilder von $\overline{f_i(t)}$ bezüglich der Restklassenabbildung*

$$\begin{aligned} \bar{} \; : \; & \mathbb{Z}[t] \to \mathbb{F}_p[t] \\ & \sum_{\mu=1}^{l} \alpha_\mu t^\mu \mapsto \sum_{\mu=1}^{l} \overline{\alpha_\mu} t^\mu \end{aligned}$$

Dann hat $\langle p \rangle_{\mathfrak{o}_\mathcal{F}}$ in $\mathfrak{o}_\mathcal{F}$ die Primidealfaktorisierung

$$\langle p \rangle_{\mathfrak{o}_\mathcal{F}} = \mathfrak{p}_1^{e_1} \cdot \ldots \cdot \mathfrak{p}_r^{e_r}$$

mit $\mathfrak{p}_i := \langle p \rangle_{\mathfrak{o}_\mathcal{F}} + \langle f_i(\vartheta) \rangle_{\mathfrak{o}_\mathcal{F}}$. Es gilt $f(\mathfrak{p}_i | \langle p \rangle) = \deg(f_i)$.

[PZ97, Chapter 6, (2.27)] Die Voraussetzung, dass das zu zerlegende Ideal comaximal zum Führer der betrachteten Ordnung sein muss, lässt sich algorithmisch nur schwer verwenden, oder, wie in [PZ97, Seite 392]: „A direct attack of the problem is not very promising...“, da die Berechnung des Führers zwingend die Kenntnis der Maximalordnung voraussetzt. Man formuliert stattdessen hinreichende Bedingungen für die Comaximalität des zu zerlegenden Ideals zum Führer, welche leichter nachprüfbar sind:

Lemma 1.36. *Seien die Voraussetzungen wie in (1.35). Dann ist $\langle p \rangle_{\mathfrak{o}_\mathcal{F}} + \mathfrak{F}(\mathbb{Z}[\vartheta]) = \mathfrak{o}_\mathcal{F}$ erfüllt, wenn zum Beispiel gilt:*

$$[\mathfrak{o}_\mathcal{F} : \mathbb{Z}[\vartheta]] \notin \langle p \rangle_\mathbb{Z},$$

oder auch, wenn gilt:

$$\operatorname{disc}(m_\vartheta(t)) \notin \langle p \rangle_\mathbb{Z}$$

[PZ97, Chapter 6, (2.29)] Mit (1.35) kann man jetzt einen Algorithmus zur Primidealfaktorisierung formulieren:

Algorithmustabelle 1: AlgKummer

Input: Zahlkörper $\mathcal{F} = \mathbb{Q}[\vartheta]$ gegeben durch Minimalpolynom
$m_\vartheta(t) = \sum_{i=1}^{g} \alpha_i t^i \in \mathbb{Z}[t]$
Primzahl $p \in \mathbb{P}_\mathbb{Z}$ kein Indexteiler
Output: Menge M von Tripeln $\{\mathfrak{p}, e, f\}$
mit $\mathfrak{p} \in \mathbb{P}_{\mathfrak{o}_\mathcal{F}}$, $\mathfrak{p} \mid \langle p \rangle_{\mathfrak{o}_\mathcal{F}}$,
$e = e(\mathfrak{p} | \langle p \rangle)$, $f = f(\mathfrak{p} | \langle p \rangle)$
{Bekannt ist eine Ganzheitsbasis von $\mathcal{F}$}
begin

{Reduziere Minimalpolynom modulo p}
$\overline{m}_\vartheta(t) \leftarrow \sum_{i=1}^{g} \overline{\alpha}_i t^i$
{Faktorisiere reduziertes Minimalpolynom}
Sei $\prod_{j=1}^{h} \overline{f}_j^{e_j}(t)$ die Faktorisierung von $\overline{m}_\vartheta(t)$ in $\mathbb{F}_p[t]$
{Bilde Menge M}
$M \leftarrow \emptyset$
for all $j \in \{1, \ldots, h\}$ **do**
  $M \leftarrow M \cup \{\{p, f_j(\vartheta)\}, e_j, \deg(f_j(t))\}$
end for
return M

Jetzt ist deutlich, warum der Index eines primitiven Elementes in der Theorie der Primidealzerlegung große Bedeutung hat. Kennt man mehrere primitive Elemente, wird man eines wählen, dessen Index möglichst wenig Primteiler hat, denn so kann man für eine größere Anzahl von Primzahlen die Primidealfaktorisierung mit dem Kummerschen Zerlegungssatz berechnen. Im Allgemeinen sind Indexteiler aber unvermeidbar, denn es gibt Zahlkörper $\mathcal{F}$ mit der Eigenschaft, dass für jedes primitive Element ϑ von $\mathcal{F}$ (mindestens) eine Primzahl p existiert, welche den Index teilt, siehe (2.19). Man muss also Methoden für die Primidealfaktorisierung von Indexteilern bereitstellen. Diese Theorie wird im nächsten Abschnitt mit dem Algorithmus von Buchmann-Lenstra behandelt.

1.4 Der Algorithmus von Buchmann-Lenstra

Sei für diesen Abschnitt $\mathcal{O}$ Ordnung eines Zahlkörpers $\mathcal{F}$ und $p \in \mathbb{P}_\mathbb{Z}$ Primzahl.

Dieser Abschnitt beschäftigt sich mit der Frage, wie man die Primidealzerlegung in Zahlkörpern berechnen kann, wenn die zu zerlegende Primzahl p Indexteiler ist. Der Algorithmus AlgKummer ist anwendbar auf den „einfachen“ Fall, also p kein Indexteiler. Der Algorithmus von Buchmann-Lenstra ist eine Berechnungsmethode für den Indexteilerfall. Er besteht im Wesentlichen aus drei Schritten:

(1) Berechne das p-Radikal $I_p(\mathfrak{o}_\mathcal{F})$ der Maximalordnung.

(2) Berechne Idealprodukte $H_1, \ldots, H_g$ aus Primidealen, welche über p identischen Verzweigungsindex haben. (In der englischen Literatur nennt man diesen Vorgang „equal degree factorisation“.)

(3) Zerlege die $H_1, \ldots, H_g$ in Primideale.

Es wird nun der Begriff des p-Radikals eingeführt, welcher aus dem Umfeld des von Zassenhaus[6] vorgestellten Round-2 Algorithmus [Poh93, V, 2], [Coh93, Theorem 6.1.3] entliehen ist:

Definition 1.37. *Definiere das* p***-Radikal*** $I_p(\mathcal{O})$ ***von*** $\mathcal{O}$ *durch*

$$I_p(\mathcal{O}) := \{x \in \mathcal{O} \mid \exists\ m \geq 1,\ \textit{so dass gilt}\ x^m \in p\mathcal{O}\}.$$

Ist klar, welche Ordnung gemeint ist, schreibt man auch $I_p := I_p(\mathcal{O})$.

Wichtig ist der Begriff des p-Radikals aufgrund folgender Proposition:

Proposition 1.38. *Für das* p*-Radikal* $I_p(\mathcal{O})$ *gilt:*

(1) Das p*-Radikal* $I_p(\mathcal{O})$ *ist ein Ideal von* $\mathcal{O}$.

(2) $I_p(\mathcal{O})$ *ist das Produkt der in* $\mathcal{O}$ *über* p *liegenden Primideale.*

(3) Es existiert eine ganze Zahl m *mit* $I_p^m(\mathcal{O}) \subseteq \langle p \rangle_{\mathcal{O}}$.

[Coh93, Proposition 6.1.2] Die Berechnung des p-Radikals einer Ordnung erfolgt zum Beispiel über den Kern einer Potenz des Frobenius-Homomorphismus [Poh93, V, 2], oder über die Spurabbildung [Fri00, Kapitel 5].

Schritt 2 im Algorithmus von Buchmann-Lenstra ist die Berechnung von Idealprodukten $H_1, \ldots, H_r$ in $\mathfrak{o}_{\mathcal{F}}$, wobei ein Produkt H_μ, $\mu \in \mathbb{N}_r$, genau aus den Primidealen besteht, welche in die Primidealfaktorisierung von $\langle p \rangle_{\mathfrak{o}_{\mathcal{F}}}$ mit Verzweigungsindex μ eingehen:

Bemerkung 1.39. ***Berechnung der Idealprodukte*** H_μ

- *Für* $j \geq 0$ *setze* $K_j := I_p(\mathfrak{o}_{\mathcal{F}})^j + \langle p \rangle_{\mathfrak{o}_{\mathcal{F}}}$. *Seien* $\mathfrak{p}_1, \ldots, \mathfrak{p}_g$ *die in* $\mathfrak{o}_{\mathcal{F}}$ *über* p *liegenden Primideale. Dann gilt:*

$$K_j = \prod_{i=1}^{g} \mathfrak{p}_i^{\min(e_i, j)},$$

  da jeder Faktor mit Exponent $\min(e_i, j)$ *in* K_j *eingeht.*

- *Es gilt* $K_{j-1} \supseteq K_j \Rightarrow K_{j-1} \mid K_j$, *definiere damit:*

$$J_j := \frac{K_j}{K_{j-1}}.$$

  Die J_j *sind genau das Produkt der Primideale* $\mathfrak{p}_i$ *aus* $\mathfrak{o}_{\mathcal{F}}$ *für die* $e(\mathfrak{p}_i | \langle p \rangle) \geq j$ *gilt.*

[6] Hans Zassenhaus, 1912 – 1991

- *Mit* $J_{j+1} \supseteq J_j \Rightarrow J_{j+1} \mid J_j$ *setze*

$$H_j := \frac{J_j}{J_{j+1}}.$$

Zur Berechnung der H_j ist man im Rahmen einer Implementation auf Algorithmen zur Multiplikation und Division von Idealen angewiesen, siehe dafür [PZ97, Chapter 6, 3], [Coh93, Proposition 4.7.2].

Man hat jetzt Idealprodukte $H_1, \ldots, H_e$ vorliegen, von denen man weiß, dass sie aus paarweise verschiedenen Primidealen, also maximalen Idealen bestehen:

$$H_j = \prod_{\substack{\langle p\rangle_{\mathfrak{o}_\mathcal{F}} \subseteq \mathfrak{p}_{j,i} \\ e(\mathfrak{p}_{j,i} \mid \langle p\rangle) = j}} \mathfrak{p}_{j,i}$$

Alle $\mathfrak{p}_{j,i}$ treten in diesen Produkten in erster Potenz auf. Man muss zum Finden der Primidealzerlegung von $\langle p\rangle_{\mathfrak{o}_\mathcal{F}}$ nur die H_j in Primideale zerlegen, denn die Verzweigungsindices der $\mathfrak{p}_{j,i}$ über $\langle p\rangle_\mathbb{Z}$ sind bekannt. Es ist möglich, den Restklassenring $\mathfrak{o}_\mathcal{F}/H_j$ für jedes j auch als Vektorraum über $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ zu betrachten, da alle Faktoren der Produkte H_j das Ideal $\langle p\rangle_{\mathfrak{o}_\mathcal{F}}$ teilen. $\mathfrak{o}_\mathcal{F}/H_j$ wird als Ringerweiterung von $\mathbb{Z}/p\mathbb{Z}$ und als $\mathbb{F}_p$-Vektorraum, also als $\mathbb{F}_p$-Algebra interpretiert. Deshalb bezeichnet man den letzten Schritt im Algorithmus von Buchmann-Lenstra als die **Zerlegung der $\mathbb{F}_p$-Algebra** $\mathfrak{o}_\mathcal{F}/H_j$. Die Zerlegung von $\mathfrak{o}_\mathcal{F}/H_j$ basiert auf folgendem Lemma:

Lemma 1.40. *Sei A eine endliche, separable Algebra über dem endlichen Körper $\mathbb{F}_p$. Dann existiert ein effizienter Algorithmus, welcher entweder nachweist, dass A Körper ist, oder ein nicht-triviales idempotentes Element $\varepsilon \in A$ findet, d. h. ein Element $\varepsilon \notin \{0, 1\}$, für welches $\varepsilon^2 = \varepsilon$ gilt.*

Da man den Beweis von (1.40) kennen muss, um den Algorithmus von Buchmann-Lenstra zu verstehen, wird hier eine kurze Skizze des Beweises gegeben:

Beweis. (von (1.40)) A ist als endliche separable Algebra isomorph zu einem endlichen Produkt von Körpern, zum Beispiel

$$A \cong A_1 \times \ldots \times A_k.$$

Betrachte den $\mathbb{F}_p$-Vektorraumendomorphismus

$$\begin{aligned} \varphi \quad : \quad & A \to A \\ & \alpha \mapsto \alpha^p - \alpha. \end{aligned}$$

Es gilt $\mathbb{F}_p \subseteq \ker(\varphi)$, wenn man $\mathbb{F}_p$ mit Hilfe der Abbildung

$$\begin{aligned} \iota \quad : \quad & \mathbb{F}_p \to A \\ & a \mapsto (a \cdot 1_{A_1}, \ldots, a \cdot 1_{A_k}) \end{aligned}$$

in A eingebettet, denn für einen endlichen Körper K mit $\#K = p$ gilt, wegen des kleinen Satzes von Fermat[7] und $\#K^\times = p - 1$:

$$x^{p-1} = 1_K \Leftrightarrow \frac{x^p}{x} = 1_K \Leftrightarrow x^p = x \Leftrightarrow x^p - x = 0.$$

Für $\alpha = (\alpha_1, \ldots, \alpha_k) \in A$ gilt nun $\alpha \in \ker(\varphi)$ dann und nur dann, wenn für alle $i \in \mathbb{N}_k$ α_i in $\mathbb{F}_p$ ist. Das bedeutet $\dim(\ker(\varphi)) = k$, und daher $\dim(\ker(\varphi)) = 1$ genau dann, wenn A Körper ist, denn das kartesische Produkt von zwei Körpern kann kein Körper sein. Es existieren effiziente Algorithmen zum Berechnen des Kerns von Homomorphismen [Knu97b, Chapter 4.6.2, Algorithm N], damit ist der erste Teil des Lemmas bewiesen.

Sei nun $\dim(\ker(\varphi)) > 1$ und $\alpha \in \ker(\varphi) \backslash \mathbb{F}_p$. Ermittle, zum Beispiel durch Berechnung von aufeinander folgenden Potenzen von α, das Minimalpolynom $m_\alpha(t) \in \mathbb{F}_p[t]$ von α über $\mathbb{F}_p$. Es gilt

$$\operatorname{lcm}\{m_{\alpha_1}(t), \ldots, m_{\alpha_k}(t)\} = m_\alpha(t),$$

dabei sind die $m_{\alpha_i}(t)$ die Minimalpolynome der einzelnen Komponenten. Wegen $\alpha \in \ker(\varphi)$ gilt $\deg(m_{\alpha_i}(t)) = 1$ für alle i. Damit ist $m_\alpha(t)$ quadratfrei und ein Produkt von mindestens zwei Linearfaktoren, denn angenommen war $\alpha \notin \mathbb{F}_p$. Sei also $m_\alpha(t) = m_1(t)m_2(t)$ mit $m_1(t), m_2(t) \in \mathbb{F}_p[t]$. Da $m_\alpha(t)$ quadratfrei ist, sind $m_1(t)$ und $m_2(t)$ coprim und mit Euklid[8] kann man zwei Polynome $f_1(t), f_2(t) \in \mathbb{F}_p[t]$ finden, so dass gilt

$$f_1(t)m_1(t) + f_2(t)m_2(t) = 1.$$

Setze $\varepsilon := f_1(\alpha)m_1(\alpha)$, dann ist

$$(f_1(\alpha)m_1(\alpha))^2 = f_1(\alpha)m_1(\alpha),$$

wegen

$$f_1(\alpha)m_1(\alpha) - 1 = f_2(\alpha)m_2(\alpha).$$

Also ist ε idempotent. Mit

$$\gcd(f_1, m_2) = \gcd(f_2, m_1) = 1$$

und

$$\deg(m_1(t)), \deg(m_2(t)) \geq 1$$

gilt $\varepsilon \notin \{0, 1\}$. □

[7] Pierre de Fermat, 1601 – 1665

[8] Euklid, vermutlich 325 v. Chr. – 265 v. Chr.

(1.40) ist auf $\mathfrak{o}_\mathcal{F}/H_j$ anwendbar, da die Erweiterung $(\mathfrak{o}_\mathcal{F}/H_j)/\mathbb{F}_p$ endlich ist. Auch ist $\mathfrak{o}_\mathcal{F}/H_j$ separabel, denn H_j ist als Produkt von verschiedenen maximalen Idealen quadratfrei. Wende nun (1.40) auf die Erweiterung $(\mathfrak{o}_\mathcal{F}/H_j)/\mathbb{F}_p$ an:

Bemerkung 1.41. ***Zerlegung von*** $\mathfrak{o}_\mathcal{F}/H_j$ ***mit (1.40)***

(1) Liefert der Algorithmus aus (1.40), dass $\mathfrak{o}_\mathcal{F}/H_j$ Körper ist, ist man mit H_j fertig, denn H_j ist maximal, damit Primideal und geht in die Faktorisierung von $\langle p\rangle_\mathbb{Z}$ mit Verzweigungsindex j ein.

(2) (Setze $H_j =: H$ für diesen Unterpunkt.) Der Algorithmus aus (1.40) liefert als Ergebnis ein Idempotent $\varepsilon \in \mathfrak{o}_\mathcal{F}/H$. Sei $e \in \mathfrak{o}_\mathcal{F}$ ein Repräsentant von ε. Setze

$$H_1 := H + \langle e\rangle_{\mathfrak{o}_\mathcal{F}} \quad \text{und} \quad H_2 := H + \langle 1-e\rangle_{\mathfrak{o}_\mathcal{F}},$$

dann gilt $H = H_1 \cdot H_2$, denn

$$\begin{aligned} H_1 \cdot H_2 &= (H + e\mathfrak{o}_\mathcal{F}) \cdot (H + (1-e)\mathfrak{o}_\mathcal{F}) \\ &= \underbrace{H \cdot H}_{\subseteq H} + \underbrace{(1-e)H \cdot \mathfrak{o}_\mathcal{F}}_{\substack{=(1-e)H \\ =H-eH\subseteq H}} + \underbrace{e\mathfrak{o}_\mathcal{F}H}_{=eH\subseteq H} + \underbrace{e\mathfrak{o}_\mathcal{F}(1-e)\mathfrak{o}_\mathcal{F}}_{\substack{\subseteq e(1-e)\mathfrak{o}_\mathcal{F} \\ =(e-e^2)\mathfrak{o}_\mathcal{F}}} \\ &\subseteq H \end{aligned}$$

wegen $e(1-e) = e - e^2 \in H$. (Das ist gerade die Idempotenteigenschaft von $e + H = \varepsilon$ in $\mathfrak{o}_\mathcal{F}/H$.) Mit einem analogen Argument zeigt man für $x \in H$ auch $x \in H_1 \cdot H_2$.

(3) Mit (2) ist H_j nicht-trivial in zwei Idealprodukte $H_{j,1}, H_{j,2}$ zerlegt. Wende (1.40) auf $H_{j,1}$ und $H_{j,2}$ rekursiv an. Nach spätestens k Schritten ist man fertig, wenn k die Anzahl der Primfaktoren von H ist.

Jetzt kann man den Algorithmus von Buchmann-Lenstra zusammenhängend formulieren. Zuerst folgen zwei Bemerkungen, die alternative Möglichkeiten zur Zerlegung von $\mathfrak{o}_\mathcal{F}/H_j$ beschreiben:

Bemerkung 1.42. ***Zerlegung von*** $\mathfrak{o}_\mathcal{F}/H_j$ ***mit Hilfe der Primpolynomzerlegung von*** $m_\alpha(t)$

Es gibt effiziente Verfahren zum Berechnen der Primpolynomzerlegung eines Polynoms $f(t) \in \mathbb{F}_p[t]$ über einem endlichen Körper [PZ97, Chapter 2, 3], [Knu97b, Chapter 4.6.2]. Statt nun im Fall, dass $\mathfrak{o}_\mathcal{F}/H_j$ kein Körper ist, H_j in lediglich zwei nicht-triviale Ideale aufzuteilen, faktorisiert man das Minimalpolynom $m_\alpha(t)$ im Beweis von (1.40) in $\mathbb{F}_p[t]$. Man erhält so

die vollständige Zerlegung von H_j. Aufgrund der Effizienz der Verfahren zur Polynomfaktorisierung war diese Variante für lange Zeit in dem Computeralgebrasystem KANT-V4 [DFK+97] implementiert.

Bemerkung 1.43. ***Zerlegung von $\mathfrak{o}_\mathcal{F}/H_j$ mit Hilfe eines primitiven Elementes***
$(\mathfrak{o}_\mathcal{F}/H_j)/\mathbb{F}_p$ ist endlich und separabel. Man erhält ein primitives Element $\alpha_j + H_j \in \mathfrak{o}_\mathcal{F}/H_j$ mit

$$\mathfrak{o}_\mathcal{F}/H_j = \mathbb{F}_p[\alpha_j + H_j] \cong \mathbb{F}_p[t]/\langle m_{\alpha+H_j}(t)\rangle_{\mathbb{F}_p[t]}.$$

Bezeichne $\mathrm{C}_j(t) \in \mathbb{Z}[t]$ ein beliebiges Urbild des charakteristischen Polynoms $\overline{\mathrm{C}}_j(t) \in \mathbb{F}_p[t]$ von $\alpha_j + H_j$. Dann sei

$$\overline{\mathrm{C}_j}(t) = \prod_{i=1}^{g_j} \overline{q}_{j,i}(t)$$

die Primpolynomzerlegung von $\mathrm{C}_j(t)$ modulo p in $\mathbb{F}_p[t]$. Die Ideale

$$\mathfrak{q}_{j,i} = H_j + \langle q_{j,i}(\alpha_j)\rangle_{\mathfrak{o}_\mathcal{F}}$$

sind maximal und das Produkt

$$H_j = \prod_{i=1}^{g_j} \mathfrak{q}_{j,i}$$

ist die gewünschte Zerlegung der H_j in ein Produkt von Primidealen. Der Beweis ist derselbe wie beim Kummerschen Zerlegungssatz.

Der konzeptuell schwierigste Teil, nämlich die Zerlegung der separablen $\mathbb{F}_p$-Algebra $\mathfrak{o}_\mathcal{F}/H_j$ ist erstaunlicherweise der Teil, der am wenigsten Rechenzeit erfordert. Die meiste Zeit im Algorithmus von Buchmann-Lenstra verbringt ein Computer mit der Idealmultiplikation und Idealdivision beim Berechnen der Idealprodukte H_j. Man ist deshalb bestrebt, diesen Rechenschritt so effizient wie möglich zu gestalten. Es stellt sich heraus, dass man eine Vielzahl von Problemen im Zusammenhang mit der Hermite-Normalform von Idealen, wie zum Beispiel die Koeffizientenexplosion, siehe Anhang (A), vermeiden kann, wenn man die Berechnungen für alle verwendeten Ideale modulo $p\mathfrak{o}_\mathcal{F}$ durchführt. Man bedenke, dass man mit Koeffizienten aus einem endlichen Körper rechnet, dessen Kardinalität „sehr klein“ ist, denn für den verwendeten endlichen Körper $\mathbb{F}_p$ ist p Indexteiler (sonst verwendet man natürlich den Kummerschen Zerlegungssatz direkt).

Man wird also alle beteiligten Ideale modulo $p\mathfrak{o}_{\mathcal{F}}$ angeben. Lediglich die Ideale im Ergebnis werden mit Hilfe der 2-Element Darstellung beschreiben, siehe (A.10).

Der vollständige Algorithmus zur Berechnung der Primidealfaktorisierung ist in den Algorithmustabellen 2 und 3 formuliert:

Algorithmustabelle 2: AlgPIDecAbs

Input: Zahlkörper $\mathcal{F} = \mathbb{Q}[\vartheta]$ gegeben durch Minimalpolynom $m_\vartheta(t) \in \mathbb{Z}[t]$, Primzahl $p \in \mathbb{P}_{\mathbb{Z}}$
Output: Eine Menge M von Tripeln $\{\mathfrak{p}, e, f\}$
mit $\mathfrak{p} \in \mathbb{P}_{\mathfrak{o}_{\mathcal{F}}}$ und $\mathfrak{p} \mid \langle p \rangle$,
$e = e(\mathfrak{p}_i|\langle p \rangle)$, $f = f(\mathfrak{p}|\langle p \rangle)$
{Bekannt ist eine Ganzheitsbasis von $\mathcal{F}$}
{Alle Ideale, werden dargestellt modulo $p\mathfrak{o}_{\mathcal{F}}$ durch eine $\mathbb{F}_p$-Basis}
if $p \nmid [\mathfrak{o}_{\mathcal{F}} : \mathbb{Z}[\vartheta]]$ **then**
{Rufe Algorithmus AlgKummer auf}
return call AlgKummer ($m_\vartheta(t)$, p)
end if
Berechne p-Radikal $I_p(\mathfrak{o}_{\mathcal{F}})$
Berechne $\mathbb{F}_p$-Basis $\bar{\beta}_1, \ldots, \bar{\beta}_l$ von $I_p(\mathfrak{o}_{\mathcal{F}})/p\mathfrak{o}_{\mathcal{F}}$
{Berechnung der $\overline{K_i}$}
$\overline{K_1} \leftarrow I_p(\mathfrak{o}_{\mathcal{F}})/p\mathfrak{o}_{\mathcal{F}}$, $i \leftarrow 1$
while $\overline{K_i} \neq \{0\}$ **do**
$i \leftarrow i+1$, $\overline{K_i} \leftarrow \overline{K_1 K_{i-1}}$
end while
{Berechnung der $\overline{J_j}$}
$\overline{J_1} \leftarrow \overline{K_1}$
for $j = 2, \ldots, i$ **do**
$\overline{J_j} \leftarrow \overline{K_j K_{j-1}^{-1}}$
end for
{Berechnung der $\overline{H_j}$}
for $j = 1, \ldots, i-1$ **do**
$\overline{H_j} \leftarrow \overline{J_j J_{j+1}^{-1}}$
end for
$\overline{H_i} \leftarrow \overline{J_i}$
{Initialisierung Idealliste }
$\mathcal{L} \leftarrow \{\overline{H_1}, \ldots, \overline{H_j}\}$
while $\mathcal{L} \neq \emptyset$ **do**
{Zerlegung der Idealprodukte}

Sei $\overline{H}_\mu \in \mathcal{L}$
{Berechne $\mathbb{F}_p$-Basis B der Algebra $A := \mathfrak{o}_\mathcal{F}/H_\mu = (\mathfrak{o}_\mathcal{F}/p\mathfrak{o}_\mathcal{F})/(H_\mu/p\mathfrak{o}_\mathcal{F})$}
Sei $\bar{B} := \bar{\beta}_1, \ldots, \bar{\beta}_r$ $\mathbb{F}_p$-Basis von $\overline{H}_\mu$
ergänze $\bar{B}$ zu einer Basis $\bar{\beta}_1, \ldots, \bar{\beta}_n$ von $\mathfrak{o}_\mathcal{F}/p\mathfrak{o}_\mathcal{F}$
$\bar{\beta}_{r+1}, \ldots, \bar{\beta}_n$ ist $\mathbb{F}_p$-Basis von A
{Rufe Algorithmus ZerlSepA auf}
$\{E_1, E_2\} \leftarrow$ **call** ZerlSepA $(\bar{\beta}_{r+1}, \ldots, \bar{\beta}_n, p)$
if $E_1 =$ True **then**
  return $\{H_\mu, \mu, \dim_{\mathbb{F}_p}(A) = \#\bar{B}\}$
else
  $\mathcal{L} \leftarrow \mathcal{L} \cup E_2$
end if
$\mathcal{L} \leftarrow \mathcal{L} \setminus H_\mu$
end while

Ein Algorithmus AlgZerSepA ist separat angegeben. Es wird das Verfahren aus dem Beweis von (1.40) benutzt:

Algorithmustabelle 3: AlgZerSepA

Input: $\mathbb{F}_p$-Algebra $\mathfrak{o}_\mathcal{F}/H$, gegeben durch Basis $A = \bar{\alpha}_1, \ldots, \bar{\alpha}_r$
  Primzahl $p \in \mathbb{P}_\mathbb{Z}$
Output: {True, $\emptyset$} falls $\mathfrak{o}_\mathcal{F}/H$ Körper ist,
  {False, $\{A_1, A_2\}$} mit $A_1 \mid H$, $A_2 \mid H$ sonst
  {Alle Ideale, werden dargestellt modulo $p\mathfrak{o}_\mathcal{F}$ durch eine $\mathbb{F}_p$-Basis}
  begin: {Berechne Abbildung} Sei M die Matrix der Abbildung
  $\varphi : A \to A$, $x \mapsto x^p - x$ bzgl. der Basis A
  {Berechnung der Matrix des Kerns}
  $M_1 \leftarrow \ker(M)$
  if $\mathrm{Rg}(M_1) > 1$ **then**
    {H ist Primideal}
    return {True, $\emptyset$}
  else
    {Zerlege H_μ}
    Sei e wie in (1.41) (2)
    $H_1 \leftarrow H + e\mathfrak{o}_\mathcal{F}$
    $H2 \leftarrow H + (1-e)\mathfrak{o}_\mathcal{F}$
    return {False, $\{H_1, H_2\}$}

end if

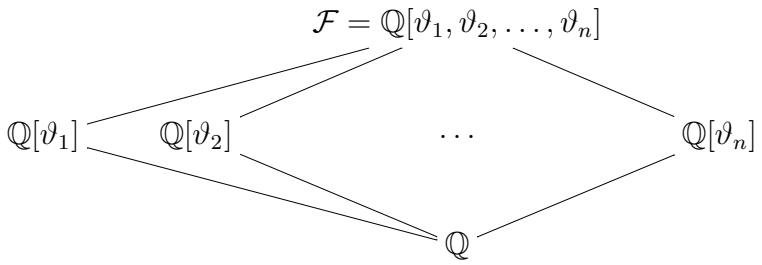
Wie in (1.42) angedeutet, wird die Zerlegung der Algebra $\mathfrak{o}_{\mathcal{F}}/H$ in Algorithmus AlgZerSepA in der Realität meistens ersetzt durch die Polynomfaktorisierung des Minimalpolynoms eines primitiven Elementes der Algebra.

Weitere Verfahren zum Berechnen der Primidealfaktorisierung für den Fall von Indexteilern sind zum Beispiel der Ore[9]-Pohst[10]-Algorithmus [Poh91, Ogn94] und das Newton[11]-Polygon-Verfahren [Coh93, Chapter 6.2.1].

[9] Oystein Ore, 1899 – 1968
[10] Michael Pohst, $\star$ 1945
[11] Sir Isaac Newton, 1643 – 1727

Kapitel 2

Der Algorithmus von Fieker



In diesem Kapitel werden Zahlkörper betrachtet, welche als Kompositum von mehreren Zahlkörpern $\mathbb{Q}[\vartheta_1], \ldots, \mathbb{Q}[\vartheta_n]$ gegeben sind. Die Aufgabe ist, die Primidealfaktorisierung einer Primzahl p in $\mathcal{K} = \mathbb{Q}[\vartheta_1, \ldots, \vartheta_n]$ zu berechnen. Um den Zerlegungssatz (1.35) auf $\mathcal{K}$ anwenden zu können, ist die Kenntnis eines primitiven Elementes ϑ von $\mathcal{K}$ zwingend notwendig. Die Idee liegt nahe, in $\mathcal{K}$ ein primitives Element zu suchen. Genau das macht der Algorithmus von Fieker[1].

Erstaunlicherweise ist dieses Problem alles Andere als trivial: Es ist nicht schwierig für einen Zahlkörper $\mathbb{Q}[\vartheta_1, \ldots, \vartheta_n]$, ein Element hin zuschreiben, welches intuitiv primitiv sein sollte; zum Beispiel $\sum_{i=1}^{n} n_i \vartheta_i$ mit natürlichen Zahlen n_i. Jedoch muss man im Rahmen einer Implementation die Primitivität nachweisen und der Schwerpunkt liegt auf einem schnellen Nachweis. Vielleicht ist es sogar möglich, das neue primitive Element $\vartheta \in \mathcal{K}$ so zu wählen, dass die Primzahl p für ϑ kein Indexteiler ist? Und hat man Verfahren gefunden, primitive Elemente so zu bestimmen, so dass man das Indexteilerproblem los wird, kann man dann diese Verfahren auf den absoluten Fall anwenden, so dass zur Bestimmung der Primidealfaktorisierung der Zerlegungssatz (1.35) ausreicht?

[1] Claus Fieker, $\star$1969

Der erste und zweite Teil dieses Kapitels beschäftigt sich mit dem Finden und dem Nachweis von primitiven Elementen in absoluten Zahlkörpern bzw. in Komposita. Da die Untersuchungen für den Kompositafall auf den Ergebnissen des absoluten Falls aufbauen, wird in (2.1) der absolute, in (2.2) der Kompositafall behandelt.

In (2.3) wird die Frage diskutiert, ob es möglich ist, primitive Elemente so zu bestimmen, dass eine gegebene Primzahl p kein Indexteiler ist.

2.1 Primitivitätsnachweis in Zahlkörpern

In diesem Abschnitt werden Verfahren zum Nachweis der Primitivität eines Elementes $\alpha \in \mathbb{Q}[\vartheta]$ besprochen. Dabei wird besonders Wert auf den algorithmischen Aspekt gelegt, d. h. es wird für jede Darstellungsart einer algebraischen Zahl α aus (A.1) mindestens ein Verfahren angegeben, welches sich für diese Darstellungsart eignet.

Sei für diesen Abschnitt $\mathcal{F} = \mathbb{Q}[\vartheta]$ Zahlkörper vom Grad n. Sei $m_\vartheta(t) \in \mathbb{Z}[t]$ das Minimalpolynom von ϑ.

Primitive Elemente können benutzt werden, um Potenzbasen zu bilden. Insbesondere sind die 0-te bis $(n-1)$-te Potenz eines primitiven Elements linear unabhängig. Man erhält:

Lemma 2.1. *$\alpha \in \mathbb{Q}[\vartheta]$ ist genau dann primitiv, wenn gilt*

$$\operatorname{disc}(1, \alpha, \ldots, \alpha^{n-1}) \neq 0.$$

Beweis. Die n verschiedenen Elemente $\{1, \alpha, \ldots, \alpha^{n-1}\}$ sind genau dann linear unabhängig in dem n-dimensionalen $\mathbb{Q}$-Vektorraum $\mathbb{Q}[\vartheta]$, wenn

$$\operatorname{disc}(1, \alpha, \ldots, \alpha^{n-1}) \neq 0$$

ist, siehe (1.16). □

Wird α in einem Computer in Minimalpolynomdarstellung repräsentiert, siehe (A.1), kann man $\operatorname{disc}(1, \alpha, \ldots, \alpha^{n-1})$ über

$$\operatorname{disc}(1, \alpha, \ldots, \alpha^{n-1}) = \operatorname{disc}(m_\alpha(t)) = (-1)^{\binom{n}{2}} \operatorname{N}(m'_\alpha(\alpha))$$

ermitteln [Mar77, Chapter 3, Theorem 8]. Man spart sich so das Berechnen der Spurmatrix in der Definition der Diskriminante, vergl. (1.13).

Liegt $\alpha \in \mathcal{F}$ in Minimalpolynomdarstellung vor, betrachtet man den Grad des Minimalpolynoms:

Lemma 2.2. *Für $\alpha \in \mathcal{F}$ gilt:*

$$\deg(m_\alpha(t)) = n \Longleftrightarrow \alpha \text{ ist primitiv.}$$

Dieses Verfahren ist für algebraische Zahlen in Minimalpolynomdarstellung das schnellste. Ist α in Matrixdarstellung gespeichert, siehe (A.3), erhält man ein weiteres Kriterium für die Primitivität:

Lemma 2.3. *Sei $M_\alpha \in \mathbb{Q}^{n\times n}$ die Darstellungsmatrix von α und $\mathrm{C}_\alpha(t) \in \mathbb{Q}[t]$ das charakteristische Polynom, siehe (1.12), dann gilt:*

$$\mathrm{C}_\alpha \text{ quadratfrei } \Rightarrow \alpha \text{ ist primitiv.}$$

Beweis. Ist das charakteristische Polynom $\mathrm{C}_\alpha(t)$ quadratfrei, so muss es bereits das Minimalpolynom sein, da das charakteristische Polynom eine Potenz des Minimalpolynoms ist. Aufgrund der Definition von $\mathrm{C}_\alpha(t)$,

$$\mathrm{C}_\alpha(t) := \det(t \cdot \mathrm{Id}_n - M_\alpha) \in \mathbb{Q}[t],$$

gilt

$$\deg(\mathrm{C}_\alpha(t)) = n.$$

Dann ist auch $\deg(m_\alpha(t)) = n$ und mit (2.2) folgt die Behauptung. □

Mit Hilfe der Norm und Spur kann man für ein Element α entscheiden, ob es primitiv ist:

Lemma 2.4. *Sei $\alpha \in \mathcal{F}$. Dann gilt:*

$$\mathrm{N}(\alpha) \text{ ist keine } p\text{-te Potenz für alle } p \text{ mit } p \mid n \Longrightarrow \alpha \text{ ist primitiv.}$$

Beweis. Nehme an, dass α nicht primitiv ist. Dann teilt der Grad von α, also der Grad des Minimalpolynoms $\deg(m_\alpha(t)) =: d$, den Grad der Körpererweiterung $\mathcal{F}/\mathbb{Q}$ und die Darstellungsmatrix $M_\alpha \in \mathbb{Q}^{n\times n}$ hat Kästchengestalt:

$$M_\alpha = \begin{pmatrix} \square & & & \\ & \square & & \\ & & \ddots & \\ & & & \square \end{pmatrix}$$

Jedes einzelne Kästchen entspricht der Darstellungsmatrix von α in dem Zahlkörper $\mathbb{Q}[\alpha]$. Nach dem Gradsatz gilt

$$[\mathcal{F} : \mathbb{Q}[\alpha]] = \frac{n}{d} =: \delta,$$

und δ ist auch die Anzahl der Kästchen in M_α. Die Norm von α ist definiert als die Determinante $\det(M_\alpha)$ der Darstellungsmatrix. Mit dem Determinantenmultiplikationssatz ist

$$\mathrm{N}_{\mathcal{F}|\mathbb{Q}}(\alpha) = \mathrm{N}_{\mathbb{Q}[\alpha]|\mathbb{Q}}(\alpha)^{\frac{n}{d}}$$

eine p-te Potenz, mit $p|n$. □

(2.4) angewandt auf die Spur erhält folgende Form:

Korollar 2.5. *Sei $\alpha \in \mathcal{F}$. Dann gilt:*

$$p \nmid \mathrm{Tr}(\alpha) \ \textit{ für alle } p \mid n \Longrightarrow \alpha \textit{ ist primitiv.}$$

Beweis. Analog zu (2.4). Ersetze die Multiplikativität der Norm bzw. der Determinante durch die Additivität der Spurabbildung. □

Ist für $\alpha \in \mathcal{F}$ eine Repräsentation mit Hilfe der Darstellungsmatrix bekannt, wird man der Methode in (2.5) statt der in (2.4) den Vorzug geben, da statt Multiplikation Addition verwendet wird. Man hat lediglich die Koeffizienten auf der Diagonale zu addieren.

Ist für ein $\alpha \in \mathcal{F}$ das charakteristische Polynom

$$\mathrm{C}_\alpha(t) := t^n + a_1 t^{n-1} + \ldots + a_n \in \mathbb{Q}[t]$$

berechnet, kann man durch Betrachtung des Koeffizienten a_1 sogar auf diese Addition verzichten:

Korollar 2.6. *Sei*

$$\mathrm{C}_\alpha(t) := t^n + a_1 t^{n-1} + \ldots + a_n \in \mathbb{Q}[t]$$

das charakteristische Polynom von $\alpha \in \mathcal{F}$. α ist primitiv, wenn mindestens einer der folgenden Punkte erfüllt ist:

(1)

$$\forall p \in \mathbb{N} \textit{ mit } p \mid n \textit{ gilt } p \nmid a_1.$$

(2)

$$|a_n| \textit{ ist keine } p\textit{-te Potenz für alle } p \textit{ mit } p \mid n.$$

Beweis. Es gilt $(-1)a_1 = \mathrm{Tr}(\alpha)$ und $\mathrm{N}(\alpha) = (-1)^n a_n$. Die Behauptung folgt mit (2.5) und (2.4). □

Normalerweise werden Elemente $\alpha \in \mathcal{F}$ in Standardrepräsentation angegeben, siehe (A.2). Will man auf diese Darstellung zum Beispiel (2.1) anwenden, wird man bestrebt sein, modulare Berechnungen auszuführen. Man verlagert den Bereich der beteiligten Koeffizienten von $\mathbb{Z}$ nach $\mathbb{F}_p$, erhält aber für den Nachweis der Primitivität keine Äquivalenzaussagen mehr, sondern nur noch notwendige Bedingungen:

Lemma 2.7. *Sei $\alpha \in \mathbb{Q}[\vartheta]$ und $p \in \mathbb{P}_\mathbb{Z}$ Primzahl. Seien*

$$\alpha^\mu = \frac{\sum_{j=0}^{n-1} a_{\mu,j}\vartheta^j}{d_\mu}, \quad \mu \in \mathbb{N}_{n-1}^0,\ d \in \mathbb{N}$$

Standardrepräsentationen der Potenzen $\{1, \alpha, \ldots, \alpha^{n-1}\}$. Sei $(m_{i,j}) \in \mathbb{Q}^{n\times n}$ mit $m_{i,j} := a_{\mu+1,j+1}$. Dann ist α primitiv, wenn gilt:

$$\det(\overline{(m_{i,j})}^p) \neq 0.$$

Hier stellt $\overline{(m_{i,j})}^p \in \mathbb{F}_p^{n\times n}$ die Matrix $(m_{i,j})$ modulo p reduziert dar.

Beweis. o. B. d. A. ist $(m_{i,j}) =: M \in \mathbb{Z}^{n\times n}$, denn betrachte statt M die Matrix dM mit $d = \sum_{\nu=0}^{n-1} d_\mu$. Multiplikation von M mit d hat keinen Einfluss auf die lineare (Un)Abhängigkeit der Spalten.

Zeige zuerst die Behauptung für den nicht-modularen Fall: In dem $\mathbb{Q}$-Vektorraum $\mathbb{Q}[\vartheta]$ ist M die Übergangsmatrix von der $\mathbb{Q}$-Basis $\{1, \vartheta, \ldots, \vartheta^{n-1}\}$ zu den Elementen $\{1, \alpha, \ldots, \alpha^{n-1}\}$. Gilt $\det(M) \neq 0$, hat M vollen Rang und $\{1, \alpha, \ldots, \alpha^{n-1}\}$ ist nach dem Basisaustauschsatz eine Basis von $\mathbb{Q}[\vartheta]$. Daher ist α mit (2.1) primitiv.

Zu zeigen bleibt: Existiert eine beliebige Primzahl $p \in \mathbb{P}_\mathbb{Z}$ mit $\det(\overline{M}^p) \neq 0$, so gilt $\det(M) \neq 0$. Beweis durch Widerspruch: Zeige

$$\det(M) = 0 \Longrightarrow \det(\overline{M}^p) = 0 \text{ für alle } p \in \mathbb{P}_\mathbb{Z}.$$

Seien $x, y \in \mathbb{Z}$, $p \in \mathbb{P}_\mathbb{Z}$ eine Primzahl und für ein $a \in \mathbb{Z}$ sei $\overline{a}^p$ die Reduktion modulo p. Da die Restklassenabbildung

$$\begin{aligned} \bar{}\ : \ & \mathbb{Z} \to \mathbb{Z}/p\mathbb{Z} \\ & x \mapsto x + p\mathbb{Z} \end{aligned}$$

homomorph ist, gilt für die Addition

$$\overline{(x+y)}^p = \overline{x}^p + \overline{y}^p,$$

analog für die Multiplikation

$$\overline{(x\cdot y)}^p = \overline{x}^p \cdot \overline{y}^p.$$

An der Berechnung der Determinante einer Matrix $(m_{k,l}) \in \mathbb{Z}^{n\times n}$ sind aber nur Addition und Multiplikation beteiligt:

$$\det((m_{k,l})) = \sum_{\sigma\in\mathcal{S}_n} \operatorname{sgn}(\sigma) \prod_{k=1}^{n} m_{k,\sigma(k)}.$$

Damit gilt $\overline{\det((m_{k,l}))}^p = \det((\overline{m_{k,l}}^p))$. □

In der Praxis wird man so vorgehen, dass man beginnend ab einer kleinen Primzahl, die Matrix M modulo p reduziert, um dann von dieser reduzierten Matrix die Determinante zu berechnen. Man probiert eine Reihe von Primzahlen $p_1, p_2, \ldots$ durch, bis man eine Primzahl p_n gefunden hat, für die $\overline{M}^{p_n} \neq 0$ gilt. Es stellt sich jetzt die Frage, ob es schneller ist, gleich die Determinante der Matrix M zu berechnen, oder M erst zu reduzieren, vielleicht sogar mehrfach für verschiedene Primzahlen, um nach einigen Berechnungen festzustellen, dass tatsächlich $\det(M) = 0$ gilt. Untersuchungen, durchgeführt mit dem Computeralgebrasystem KANT-V4 zeigen, dass es sich prinzipiell lohnt, ab einer Spaltenanzahl größer als 20 die Matrix zu reduzieren und nur noch die Determinante der reduzierten Matrix zu berechnen. Auch zeigt sich, dass es bei einer Reduktion modulo 3 praktisch zu keinen Fehlern mehr kommt. Für Details sei auf Anhang (B.1) verwiesen.

Aus (2.7) folgt des Weiteren:

Lemma 2.8. *Seien die Bezeichnungen wie in (2.7). Dann ist α primitiv, wenn gilt*

$$\operatorname{Rg}(\overline{M}^p) = n.$$

Beweis. Eine Matrix hat genau dann vollen Rang, wenn die Determinante ungleich Null ist. □

Zum Schluss sei noch ein Verfahren zum Nachweis der Primitivität für die Konjugiertenvektordarstellung genannt, siehe (A.4):

Lemma 2.9. *Sei $\alpha \in \mathbb{Q}[\vartheta]$ und seien $\{\alpha =: \alpha^{(1)}, \ldots, \alpha^{(n)}\}$ die Konjugierten von α. Dann gilt*

$$\alpha \text{ ist primitiv} \iff \alpha^{(i)} \neq \alpha^{(j)} \quad \forall i, j \in \mathbb{N}_n, \quad i \neq j.$$

Beweis. Das charakteristische Polynom $\mathrm{C}_\alpha(t) \in \mathbb{Q}^{n\times n}$ von α hat die Form

$$\mathrm{C}_\alpha(t) = \prod_{j=1}^{n} (t - \alpha^{(j)}).$$

$\mathrm{C}_\alpha(t)$ ist genau dann quadratfrei, wenn alle Konjugierten von α verschieden sind. Die Behauptung folgt mit (2.3). □

Welches der genannten Verfahren zum Nachweis der Primitivität man anwenden wird, hängt davon ab, in welcher Form eine algebraische Zahl in einem Computer gespeichert ist. In dem Referenzsystem KANT-V4 wird grundsätzlich eine algebraische Zahl in der Standarddarstellung bzgl. der Potenzbasis eines primitiven Elementes angegeben, so dass man hier (2.7) anwenden wird. Hat man die Wahl zwischen allen vier Darstellungen, d. h. liegt insbesondere das Minimalpolynom vor, wird man (2.2) anwenden.

2.2 Bestimmung primitiver Elemente in Komposita von Zahlkörpern

Dieser Abschnitt beschreibt ein Verfahren zur Bestimmung eines primitiven Elementes in einem Kompositum $\mathcal{K} = \mathbb{Q}[\vartheta_1] \ldots \mathbb{Q}[\vartheta_n]$. Man kann sich auf den Fall beschränken, dass $\mathcal{K}$ als Kompositum von zwei Zahlkörpern gegeben ist, da alle anderen Fälle mit Induktion gelöst werden können. Die Existenz eines primitiven Elementes ist garantiert, da Zahlkörper endlich und separabel sind [Bos96, 3.6, Satz 12].

Sei für diesen Abschnitt $\mathcal{K} = \mathbb{Q}[\vartheta_1, \vartheta_2]$ algebraischer Zahlkörper und $p \in \mathbb{P}_\mathbb{Z}$ eine Primzahl.

Der hier beschriebene Algorithmus beruht auf zwei konstruktiven Beweisen des Satzes vom primitiven Element, angelehnt an [Lan65, VII, §, Theorem 14] und [Mey76, Satz 6.9.17]. Besprochen wird der für den Algorithmus relevante Teil dieser Beweise:

Satz 2.10. ***Satz vom primitiven Element I***
Sei E endliche Erweiterung des Körpers K. E habe o. B. d. A. eine Darstellung der Form $E = K[a, b]$. Dann gilt:

- *Es existieren genau dann nur endlich viele echte Zwischenkörper F von K und E, wenn ein primitives Element $\alpha \in E$ mit $E = K[\alpha]$ existiert.*
- *Ist E/K separabel, so existiert ein solches α.*

Beweis. (nur Teil $\Longrightarrow$ von Punkt 1)
Sei o. B. d. A. $\#K = \infty$. Im Fall $\#K < \infty$ ist $K^\times$ zyklisch, es existiert ein $\alpha \in K^\times$ mit der Eigenschaft $\langle\alpha\rangle = K^\times$. Dann erzeugt α auch E über K.

Seien $\alpha, \beta \in E$ mit $K[\alpha, \beta] = E$. Betrachte Elemente der Form

$$\alpha + c\beta \in E \quad \text{mit } c \in K.$$

Es kann, aufgrund der Annahme, nur eine endliche Anzahl von Körpern des Typs $K[\alpha + c\beta]$ mit

$$K \subsetneqq K[\alpha + c\beta] \subsetneqq K[\alpha, \beta]$$

geben. $K \neq K[\alpha + c\beta]$ gilt wegen $\alpha, \beta \notin K$. $K[\alpha + c\beta] \subseteq K[\alpha, \beta]$ gilt wegen $\alpha, \beta, c \in K[\alpha, \beta]$ und Körper sind abgeschlossen unter Multiplikation und Addition. Aus demselben Grund kann nicht $K[\alpha, \beta] \subsetneqq K[\alpha + c\beta]$ gelten.

Des weiteren kann für $c_1, c_2 \in K$ mit $c_1 \neq c_2$ und $K[\alpha + c_1\beta] \subsetneqq K[\alpha, \beta]$, $K[\alpha + c_2\beta] \subsetneqq K[\alpha, \beta]$ nicht $K[\alpha + c_1\beta] = K[\alpha + c_2\beta]$ gelten, da $\alpha + c_1\beta$ nicht in $K[\alpha + c_2\beta]$ enthalten ist. Wäre $\alpha + c_1\beta \in K[\alpha + c_2\beta]$, wäre auch $\alpha + c_1\beta - (\alpha + c_2\beta) = (c_1 - c_2)\beta \in K[\alpha + c_2\beta]$. Da $c_1 - c_2 \in K$ ist, würde dann $\alpha, \beta \in K[\alpha + c_2\beta]$ gelten. Widerspruch zu $K[\alpha + c_2\beta] \subsetneqq K[\alpha, \beta]$.

Da $\#K = \infty$ vorausgesetzt wurde, existieren in K unendlich viele Elemente c für die gilt $K[\alpha + c\beta] = E$ und jedes dieser $\alpha + c\beta$ ist ein primitives Element von E. □

Um (2.10) anzuwenden, muss man sich noch überlegen, dass für einen algebraischen Zahlkörper $\mathcal{F}$ die Erweiterung $\mathcal{F}/\mathbb{Q}$ nur endlich viele Zwischenkörper hat: $\mathcal{F}/\mathbb{Q}$ ist endlich (nach Definition) und separabel (da $\mathbb{Q}$ perfekt ist), man kann die normale Hülle $N \supseteq \mathcal{F} \supseteq \mathbb{Q}$ betrachten und $N/\mathbb{Q}$ ist galoissch. Nach dem Hauptsatz der Galois-Theorie existieren nur endlich viele Zwischenkörper zwischen N und $\mathbb{Q}$, da die Galois-Gruppe $\mathrm{Gal}(N/\mathbb{Q})$ nur eine endliche Anzahl von Untergruppen hat. Damit hat aber auch $\mathcal{F}/\mathbb{Q}$ nur endlich viele Zwischenkörper.

Überträgt man (2.10) auf die Situation eines Körperkompositums $\mathbb{Q}[\vartheta_1, \vartheta_2]$ folgt, dass es nur endlich viele $q \in \mathbb{Q}$ gibt, für die das Element $\vartheta_1 + q\vartheta_2 \in \mathbb{Q}[\vartheta_1, \vartheta_2]$ nicht primitiv ist. Das ist die Grundidee des zu entwickelnden Algorithmus.

Mit folgendem Satz kann man die Menge dieser „schlechten“ $q \in \mathbb{Q}$ sogar näher bestimmen [Mey76, Satz 6.9.17]:

Satz 2.11. ***Satz vom primitiven Element II***
Sei K Körper. Seien a, b Elemente einer Erweiterung. Es seien a algebraisch und b separabel über K, dann besitzt $K[a, b]$ ein primitives Element c.

Beweis. Da a, b algebraisch sind, ist die Erweiterung $K[a, b]/K$ endlich. Analog zu (2.10) sei $\#K = \infty$.

Betrachte in einem algebraischen Abschluss die paarweise verschiedenen Nullstellen $\{a =: a_1, \ldots, a_r\}$ und $\{b =: b_1, \ldots, b_s\}$ der Minimalpolynome $m_a(t), m_b(t) \in K[t]$ von a und b. Es sei $r := \deg(m_a(t))$ und $s := \deg(m_b(t))$. Definiere für alle $x \in K$ die Menge

$$W(x) := \{a_i x + b_j \mid i \in \mathbb{N}_{2,r},\ j \in \mathbb{N}_{2,s}\}.$$

Wähle ein $y \in K$, welches nicht in der endlichen Menge

$$\mathfrak{S}_{a,b} := \left\{ \frac{b_j - b}{a - a_i} \;\middle|\; i \in \mathbb{N}_{2,r},\ j \in \mathbb{N}_{2,s} \right\}$$

enthalten ist. (Das geht, weil $\#K = \infty$ vorausgesetzt ist.) Dann gilt

$$ay + b \notin W(y),$$

denn wäre $ay + b \in W(y)$, gäbe es $i \in \mathbb{N}_{2,r}$, $j \in \mathbb{N}_{2,s}$ mit

$$ay + b = a_i y + b_j \Longleftrightarrow y = \frac{b_j - b}{a - a_i}.$$

Jetzt ist $c := ay + b$ schon primitives Element von $K[a, b]$: Trivialerweise gilt $K[c] \subseteq K[a, b]$, zeige also $K[a, b] \subseteq K[c]$. Betrachte

$$h(t) := \gcd(m_a(t), m_b(c - yt)) \in K[c][t].$$

Es gilt $m_a(a) = 0$ und

$$m_b(c - ya) = m_b(\underbrace{ay + b}_{=c} - ya) = m_b(b) = 0.$$

Daher ist $t - a$ gemeinsamer Teiler von $m_a(t)$ und $m_b(c - yt)$, also auch von $h(t)$. Jede weitere Nullstelle von $h(t)$ ist auch Nullstelle von $m_a(t)$ und damit aus der Menge $\{a_2, \ldots, a_r\}$. Für alle Elemente dieser Menge gilt

$$m_b(c - ya_i) \neq 0,$$

wegen $c - ya_i \neq b_j$, das besagt gerade die Bedingung $c \notin W(y)$. Also hat $h(t)$ nur die Nullstelle a, das bedeutet aber, dass man $h(t)$ schreiben kann als

$$(t - a)^s = \gcd(m_a(t), m_b(c - yt)).$$

Damit teilt $h(t)$ insbesondere $m_a(t)$. $m_a(t)$ ist separabel (wegen Voraussetzung) und irreduzibel (wegen Minimalpolynomeigenschaft), damit folgt $s = 1$ und $h(t) = t - a$.

Der gcd zweier Polynome aus $K[c][t]$ ist auch aus $K[c][t]$, also $h(t) = t - a \in K[c][t]$, d. h. $a \in K[c]$, damit

$$\underbrace{\underbrace{c}_{\in K[c]} - \underbrace{y}_{\in K} \underbrace{a}_{\in K[c]}}_{\in K[c]} = ay + b - ya = b \Longrightarrow b \in K[c]$$

und daher $K[a, b] \subseteq K[c]$. □

Eine Anwendung des Satzes auf die Situation eines Körperkompositums ergibt:

Korollar 2.12. *Sei $\mathbb{Q}[\vartheta_1, \vartheta_2]$ Körperkompositum der Zahlkörper $\mathbb{Q}[\vartheta_1]$ und $\mathbb{Q}[\vartheta_2]$. Seien $m_{\vartheta_1}(t), m_{\vartheta_2}(t) \in \mathbb{Z}[t]$ die Minimalpolynome von ϑ_1, ϑ_2 in $\mathbb{Q}[\vartheta_1]$ und $\mathbb{Q}[\vartheta_2]$. Sei $\deg(m_{\vartheta_1}(t)) =: m$ und $\deg(m_{\vartheta_2}(t)) =: n$. Sind*

$$\{\vartheta_1 =: \vartheta_1^{(1)}, \ldots, \vartheta_1^{(m)}\} \quad \text{und} \quad \{\vartheta_2 =: \vartheta_2^{(1)}, \ldots, \vartheta_2^{(n)}\}$$

die Konjugierten von ϑ_1 und ϑ_2 in $\mathbb{Q}[\vartheta_1]$ und $\mathbb{Q}[\vartheta_2]$, dann ist jede Zahl $\vartheta_1 q + \vartheta_2 \in \mathbb{Q}[\vartheta_1, \vartheta_2]$, für welches $q \in \mathbb{Q}$ nicht Element der Menge

$$\mathfrak{S}_{\vartheta_1,\vartheta_2} := \left\{ \frac{\vartheta_2^{(j)} - \vartheta_2}{\vartheta_1 - \vartheta_1^{(i)}} \;\middle|\; i \in \mathbb{N}_{2,m},\ j \in \mathbb{N}_{2,n} \right\}$$

ist, primitives Element von $\mathbb{Q}[\vartheta_1, \vartheta_2]$. Die Anzahl der „schlechten" $q \in \mathbb{Q}$ kann man nach oben abschätzen mit:

$$\#\{q \in \mathbb{Q} \mid \vartheta_1 + q\vartheta_2 \text{ ist nicht primitiv } \} \leq (m-1) \cdot (n-1) < [\mathbb{Q}[\vartheta_1, \vartheta_2] : \mathbb{Q}].$$

Die Menge $\mathfrak{S}_{\vartheta_1,\vartheta_2}$ und das Maximum dieser Menge bekommen einen besonderen Namen:

Definition 2.13. *Seien die Voraussetzungen wie in (2.12). Man nennt die Menge $\mathfrak{S}_{\vartheta_1,\vartheta_2}$ die **$\mathfrak{S}$-Menge des Zahlkörpers** $\mathbb{Q}[\vartheta_1, \vartheta_2]$ und die Zahl*

$$\max \mathfrak{S}_{\vartheta_1,\vartheta_2} := \max\{|x| \mid x \in \mathfrak{S}_{\vartheta_1,\vartheta_2}\}$$

*die **$\mathfrak{S}$-Schranke des Zahlkörpers** $\mathbb{Q}[\vartheta_1, \vartheta_2]$.*

Der Begriff „Maximum" in (2.13) bezieht sich auf das Maximum der euklidischen Normen der Elemente der Menge $\mathfrak{S}_{\vartheta_1,\vartheta_2}$ in der Gaußschen Zahlenebene, da die Elemente von $\mathfrak{S}_{\vartheta_1,\vartheta_2}$ im Allgemeinen nicht reell sind.

Mit (2.12) hat man nun einen Ansatzpunkt zur Bestimmung eines primitiven Elementes ϑ in einem Kompositum $\mathbb{Q}[\vartheta_1, \vartheta_2]$. Man erhält sofort mehrere „ad-hoc" Methoden:

- Berechne mit Hilfe von numerischen Methoden die $\mathfrak{S}$-Schranke direkt und wähle $n \in \mathbb{N}$ mit $n := \lceil \max \mathfrak{S}_{\vartheta_1,\vartheta_2} \rceil$; dann ist $\vartheta_1 + n\vartheta_2$ primitiv.

- Berechne die Menge $\mathfrak{S}_{\vartheta_1,\vartheta_2}$ direkt und wähle ein $n \in \mathbb{N}$ mit $n \notin \mathfrak{S}_{\vartheta_1,\vartheta_2}$; dann ist $\vartheta_1 + n\vartheta_2$ primitiv.

Diese beiden Methoden sind sehr zeitaufwendig, besonders in Computeralgebrasystemen, bei denen der Schwerpunkt nicht auf einer geschwindigkeitsoptimierten Gleitkommaarithmetik, sondern auf zahlentheoretischen Aspekten

liegt. Außerdem hat man sich hier mit allen Problemen numerischer Berechnungen zu beschäftigen, zum Beispiel der Auslöschung. Man wird daher bestrebt sein, numerische Berechnungen bzgl. der $\mathfrak{S}$-Menge nach Möglichkeit zu reduzieren, bzw. ganz zu vermeiden.

In der Tat kann man auf die Berechnung der $\mathfrak{S}$-Menge in der Praxis komplett verzichten: Rechnersimulationen, durchgeführt mit dem Computeralgebrasystem KANT-V4 zeigen, dass für zwei zufällig ausgewählte Polynome $f_1(t), f_2(t) \in \mathbb{Z}[t]$ die $\mathfrak{S}$-Schranke zu über 50 % bei einem Wert von unter 1 liegt. Für 90 % der Polynompaare sogar unter 10. Schon über der 1 ist die $\mathfrak{S}$-Schranke sehr wahllos verteilt. Die detaillierten Ergebnisse sind in Anhang (B.2) beschrieben.

Als Idee erhält man:

Bemerkung 2.14. *Seien die Bezeichnungen wie in (2.13).*

(1) Ist der Grad des Kompositums $\mathcal{K} = \mathbb{Q}[\vartheta_1, \vartheta_2]$ bekannt, berechne die Folge

$$\vartheta_1 + q\vartheta_2, \quad q \in \mathbb{N},$$

bis man ein $q \in \mathbb{N}$ erhält, für welches

$$\deg(m_{\vartheta_1+q\vartheta_2}(t)) = \deg(\mathcal{K})$$

gilt. Dieses $\vartheta_1+q\vartheta_2$ ist das gesuchte Element. Den Grad $\deg(m_{\vartheta_1+q\vartheta_2}(t))$ kann man sofort ablesen, da alle Berechnungen in der Minimalpolynomdarstellung durchgeführt werden.

(2) Ist der Grad $\deg(\mathcal{K})$ nicht bekannt, berechne für eine kleine Menge M mit ungerader Mächtigkeit die Werte

$$N := \{\vartheta_1 + q\vartheta_2 \mid q \in M\}.$$

Sei zum Beispiel

$$M := \{10, 20, 30\}.$$

Die Wahrscheinlichkeit, dass N viele primitive Elemente enthält, ist hoch. Haben die Elemente von N unterschiedliche Grade, führe bzgl. dieser Grade eine Mehrheitsentscheidung durch (deshalb soll $\#M$ ungerade sein).

(3) Will man sich nicht auf eine Mehrheitsentscheidung verlassen, berechne solange Elemente der Folge

$$(\vartheta_1 + q\vartheta_2)_{q\in\mathbb{N}},$$

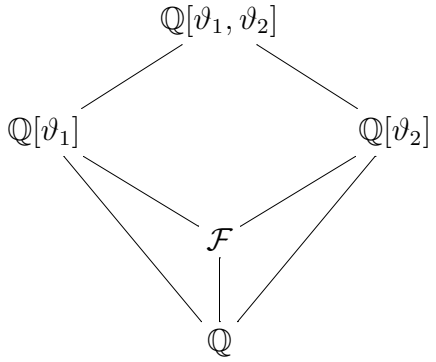
bis man mn Elemente vorliegen hat, welche gleichen Grad haben. Dann ist durch (2.12) garantiert, dass diese Zahl mit $\deg(\mathcal{K})$ übereinstimmt.

In (1) und (2) liegen alle Elemente in Minimalpolynomdarstellung vor, so dass man diese Darstellung sofort für das Minimalpolynom des Kompositums $\mathcal{K}$ benutzen kann. Auch kann man mit den Elementen ϑ_1, ϑ_2 in (2) Arithmetik betreiben, ohne dass diese Zahlen Elemente eines Zahlkörpers sein müssen, siehe (A.1).

Die Bestimmung des Grades eines Kompositums ist nicht trivial:

Bemerkung 2.15. *Seien $\mathbb{Q}[\vartheta_1]$ und $\mathbb{Q}[\vartheta_2]$ Zahlkörper vom Grad m bzw. n. Dann gilt für den Grad des Körperkompositum $\mathbb{Q}[\vartheta_1, \vartheta_2]$ im Allgemeinen nicht $[\mathbb{Q}[\vartheta_1, \vartheta_2] : \mathbb{Q}] = m \cdot n$. Ein Gegenbeispiel ist $\vartheta_1 := \sqrt{2}$, $\vartheta_2 := \sqrt[4]{2}$.*

Betrachte folgendes Diagramm:



Hier haben die Zahlkörper $\mathbb{Q}[\vartheta_1]$ und $\mathbb{Q}[\vartheta_2]$ einen gemeinsamen Teilkörper und es gilt nicht $\deg(\mathbb{Q}[\vartheta_1, \vartheta_2]) = \deg(\mathbb{Q}[\vartheta_1]) \cdot \deg(\mathbb{Q}[\vartheta_2])$.

Es gibt nicht viele hinreichende Kriterien, die sich algorithmisch verwenden lassen, um zu testen, ob der Grad des Körperkompositums $\mathbb{Q}[\vartheta_1, \vartheta_2]$ das Produkt der einzelnen Grade ist. Eine notwendige Bedingung ist der Diskriminantentest:

Lemma 2.16. ***Diskriminantentest***
Seien $\mathbb{Q}[\vartheta_1]$ und $\mathbb{Q}[\vartheta_2]$ Zahlkörper vom Grad m und n, dann gilt

$$\gcd(\mathrm{disc}(\mathbb{Q}[\vartheta_1]), \mathrm{disc}(\mathbb{Q}[\vartheta_2])) = 1 \implies \deg(\mathbb{Q}[\vartheta_1, \vartheta_2]) = m \cdot n$$

[Nar89, 4, §2, Theorem 4.9] Die Idee des Beweises ist, in dem Körperturm

$$\mathbb{Q}[\vartheta_1, \vartheta_2] \supseteq \mathbb{Q}[\vartheta_1] \supseteq \mathbb{Q}$$

die Irreduzibilität des Minimalpolynoms $m_{\vartheta_2}(t) \in \mathfrak{o}_{\mathbb{Q}[\vartheta_1]}[t]$ über $\mathfrak{o}_{\mathbb{Q}[\vartheta_1]}$ zu zeigen, falls $\gcd(\mathrm{disc}(\mathbb{Q}[\vartheta_1]), \mathrm{disc}(\mathbb{Q}[\vartheta_2])) = 1$ gilt. Diese Idee wird in (3.5) wieder aufgegriffen.

Man wird also bei der Berechnung eines primitiven Elementes ϑ in einem Körperkompositum $\mathbb{Q}[\vartheta_1, \vartheta_2]$ mit Hilfe der $\mathfrak{S}$-Menge $\mathfrak{S}_{\vartheta_1,\vartheta_2}$ zuerst den Diskriminantentest durchführen. Ist dieser positiv, wendet man (2.14) (1) an, sonst (2.14) (2).

Jetzt sind alle Bausteine für den Algorithmus von Fieker zusammen. Da sich (2.14) problemlos auf Komposita bestehend aus mehr als zwei Zahlkörpern übertragen lässt, ist der Algorithmus für diesen allgemeinen Fall formuliert:

Algorithmustabelle 4: AlgFieker

Input: n Zahlkörper $\mathbb{Q}[\vartheta_1], \ldots, \mathbb{Q}[\vartheta_n]$ vom Grad $n_1, \ldots, n_n$
gegeben durch Minimalpolynome
$m_{\vartheta_1}(t), \ldots, m_{\vartheta_n}(t) \in \mathbb{Z}[t]$
Output: Primitives Element ϑ von $\mathcal{K} = \mathbb{Q}[\vartheta_1, \ldots, \vartheta_n]$
in Minimalpolynomdarstellung
{Bekannt sind die Diskriminanten der Zahlkörper $\mathbb{Q}[\vartheta_1], \ldots, \mathbb{Q}[\vartheta_n]$}
begin:
{Initialisierung}
$\mathcal{K} \leftarrow \mathbb{Q}[\vartheta_1]$, $x \leftarrow 2$, $M \leftarrow \{10, 20, 30\}$
while $x < n$ **do**
$\tilde{K} \leftarrow \mathbb{Q}[\vartheta_x]$
{Diskriminantentest}
$d \leftarrow \gcd(\mathrm{disc}(\mathcal{K}), \mathrm{disc}(\tilde{\mathcal{K}}))$
if $d = 1$ **then**
$m \leftarrow 0$
repeat
$m \leftarrow m + 10$
until $\deg(m_{\vartheta_1 + m\vartheta_x}(t)) = \deg(m_{\vartheta_1}(t)) \cdot \deg(m_{\vartheta_x}(t))$
else
for all $m_i \in M$ **do**
$\vartheta_{m_i} \leftarrow \vartheta_1 + m_i \vartheta_x$
end for
{Mehrheitsentscheidung}
Bestimme ein $m_i \in M$ mit der Eigenschaft:
$\exists\ m_1, m_2 \in M :\ \deg(m_{\vartheta_{m_1}}(t)) = \deg(m_{\vartheta_{m_2}}(t))$ mit $m_1 \neq m_2$ und $\deg(m_{\vartheta_{m_2}}(t)) = \deg(m_{\vartheta_{m_i}}(t))$
$m \leftarrow m_i$
end if
{Bilde Kompositum}

$\mathcal{K} \leftarrow \mathbb{Q}[\vartheta_1 + m\vartheta_x]$, $\vartheta_1 \leftarrow \vartheta_1 + m\vartheta_x$
$x \leftarrow x + 1$
end while
return $m_{\vartheta_1}(t)$

Bemerkung 2.17. *Modifiziert man den Algorithmus AlgFieker, so dass im else-Zweig der while-Schleife, statt einer Mehrheitsentscheidung die „sichere" Methode aus (2.14) (3) genommen wird, erhält man den Algorithmus* ***AlgFiekerSafe****. Die Richtigkeit dieses Algorithmus beruht nicht auf statistischen Messungen, sondern folgt mit (2.12). Dafür nimmt man aber eine längere Laufzeit in Kauf.*

2.3 Vermeidung von Indexteilern durch Wechsel des primitiven Elementes

Man hat jetzt mit den Algorithmen AlgFieker und AlgFiekerSafe effektive Möglichkeiten, in Komposita von Zahlkörpern die Primidealfaktorisierung zu berechnen, indem man ein primitives Element bestimmt. Vergegenwärtigt man sich dabei die Verfahren aus Kapitel (1), drängt sich die Frage auf, ob es nicht möglich ist, ein primitives Element so zu bestimmen, dass die zu zerlegende Primzahl kein Indexteiler ist. Man könnte diese Verfahren nutzen, um in einem absoluten Zahlkörper $\mathcal{F}$ das primitive Element zu wechseln, oder um den Algorithmus AlgFieker so zu modifizieren, dass man primitive Elemente bestimmt, für welche eine zu zerlegende Primzahl kein Indexteiler ist. Leider erfüllt sich diese Hoffnung nicht, denn es existieren gemeinsame außerwesentliche Diskriminantenteiler:

Definition 2.18. *Sei $\mathcal{F} = \mathbb{Q}[\vartheta]$ Zahlkörper mit Maximalordnung $\mathfrak{o}_\mathcal{F}$, dann nennt man*

$$i(\mathcal{F}) := \gcd\{i(\alpha) \mid \alpha \in \mathfrak{o}_\mathcal{F}\}$$

den ***Index des Zahlkörpers*** *$\mathcal{F}$. Siehe auch (1.10). Eine Primzahl $p \in \mathbb{P}_\mathbb{Z}$, mit $p \mid i(\mathcal{F})$ nennt man* ***gemeinsamen außerwesentlichen Diskriminantenteiler****, im Folgenden CNEDD[2] abgekürzt.*

Die Existenz von CNEDDs zeigt folgendes Beispiel, welches auf Dedekind zurückgeht [Has63, III, §25, 7.1]:

[2]engl. common non-essential discriminant divisor

Beispiel 2.19. *Sei $\mathbb{Q}[\vartheta]$ Zahlkörper mit ϑ Nullstelle des Polynoms $m_\vartheta(t) = t^3 - t^2 - 2t - 8$, dann gilt $2 \mid i(\mathbb{Q}[\vartheta])$.*

Folgender Satz liefert ein Kriterium dafür, wann eine Primzahl CNEDD ist:

Satz 2.20. *Sei $\mathcal{F}$ Zahlkörper und $p \in \mathbb{P}_\mathbb{Z}$ Primzahl. Mit $\langle p \rangle_{\mathfrak{o}_\mathcal{F}} = \mathfrak{p}_1^{e_1} \cdot \ldots \cdot \mathfrak{p}_r^{e_r}$ bezeichne die Primidealfaktorisierung von $\langle p \rangle_{\mathfrak{o}_\mathcal{F}}$ mit Trägheitsgraden $f(\mathfrak{p}_i | \langle p \rangle)$. p ist genau dann kein CNEDD, wenn r verschiedene, irreduzible Polynome $f_1(t), \ldots f_r(t) \in \mathbb{F}_p[t]$ existieren, für deren Grade $f(\mathfrak{p}_i | \langle p \rangle) = \deg(f_i(t))$ für alle $i \in \mathbb{N}_r$ gilt.*

[Nar89, 4, §3, Theorem 4.13]. Um (2.20) anwenden zu können, benötigt man folgende auf Gauß[3] zurückgehende Proposition:

Proposition 2.21. *Sei $r(p, n)$ die Anzahl nicht assoziierter, irreduzibler Polynome vom Grad n über dem endlichen Körper $\mathbb{F}_p$. Für alle Primzahlen $p \in \mathbb{P}_\mathbb{Z}$ und $n \geq 1$ gilt*

$$r(p, n) = \frac{1}{n} \sum_{d|n} \mu(d) p^{n/d}.$$

μ ist die Möbius-Funktion.

[Has63, I, §3, Theorie der endlichen Körper] Mit Hilfe von (2.21) erhält man eine obere Schranke für CNEDDs:

Proposition 2.22. *Sei $\mathcal{F}$ Zahlkörper und $p \in \mathbb{P}_\mathbb{Z}$ Primzahl, dann gilt*

$$p \mid i(\mathcal{F}) \implies p < [\mathcal{F} : \mathbb{Q}].$$

Ist p in $\mathcal{F}$ voll zerlegt, gilt auch die Umkehrung.

[Nar89, 4, §3, Proposition 4.17] [Koc00, Theorem 3.12.13] Um (2.22) algorithmisch verwenden zu können, muss man die Anzahl der Primideale kennen, in die sich ein zu faktorisierendes Ideal zerlegt und die entsprechenden Trägheitsgrade. Gerade das will man aber berechnen. Man kann aber schließen, dass es sich prinzipiell lohnt, für einen Indexteiler p im Falle $p \geq [\mathcal{F} : \mathbb{Q}]$ zu versuchen, das primitive Element zu wechseln.

Mit Verfahren zur Berechnung des Index eines Zahlkörpers $i(\mathcal{F})$ könnte man alle CNEDDs bestimmen. Leider ist auch dieses Problem bis heute nicht befriedigend gelöst. In [Nar89, Unsolved Problems, 6] ist es aufgelistet als

[3] Johann Carl Friedrich Gauß, 1777 – 1855

Nummer 6 der ungelösten Probleme der Zahlentheorie. Es liegen bis heute keine Ergebnisse vor, die sich algorithmisch verwenden lassen. Den aktuellen Stand der Forschung spiegelt zum Beispiel [Nar85] wieder.

Für den Rest dieses Abschnittes werden drei Verfahren diskutiert, um für eine gegebene Primzahl $p \in \mathbb{P}_\mathbb{Z}$, welche Indexteiler in einem Zahlkörper $\mathbb{Q}[\vartheta]$ ist, ein anderes primitives Element $\tilde{\vartheta}$ so zu bestimmen, dass p kein Indexteiler mehr ist.

Sei für den Rest dieses Abschnittes $\mathcal{F} = \mathbb{Q}[\vartheta]$ Zahlkörper vom Grad n. Sei $p \in \mathbb{P}_\mathbb{Z}$ Primzahl mit der Eigenschaft $p \mid i(\vartheta)$.

Zuerst ein ad-hoc Ansatz: Man repräsentiert in Computeralgebrasystemen Elemente eines Zahlkörpers $\mathcal{F}$ bzgl. einer Potenzbasis $\{1, \vartheta, \ldots, \vartheta^{n-1}\}$. ϑ ist ein primitives Element von $\mathcal{F}$, dargestellt durch sein Minimalpolynom $m_\vartheta(t) \in \mathbb{Z}[t]$. Man kann nun versuchen, randomisiert Linearkombinationen

$$\tilde{\alpha} := \sum_{i=0}^{n-1} \alpha_i \vartheta^i, \quad \alpha_i \in \mathbb{N}$$

zu finden, so dass man ein primitives Element $\tilde{\alpha}$ erhält, welches nicht den Index teilt. Leider ist dieser Ansatz nicht erfolgreich:

Satz 2.23. *Die Indexteilereigenschaft von p ist invariant unter Addition und Multiplikation von ϑ mit ganzen Zahlen. Ist eine Potenz ϑ^m mit $m \in \mathbb{N}$ wieder primitiv, so teilt p auch den Index dieser Potenz.*

Beweis. Dass die Summe bzw. das Produkt eines primitiven Elementes mit einer ganzen Zahl wieder primitiv ist, überlegt man sich mit den Verfahren aus (2.1).

Seien $\{\vartheta =: \vartheta^{(1)}, \ldots, \vartheta^{(n)}\}$ die Konjugierten von ϑ und $z \in \mathbb{Z}$. Dann sind $\{\vartheta + z =: \vartheta^{(1)} + z, \ldots, \vartheta^{(n)} + z\}$ die Konjugierten von $\vartheta + z$, und es gilt für die Diskriminante der Gleichungsordnung:

$$\begin{aligned} \operatorname{disc}(\mathbb{Z}[\vartheta]) = \operatorname{disc}(m_\vartheta(t)) &= \prod_{1 \le i < j \le n} (\vartheta^{(i)} - \vartheta^{(j)})^2 \\ &= \prod_{1 \le i < j \le n} (\vartheta^{(i)} + z - (\vartheta^{(j)} + z))^2 \\ &= \operatorname{disc}(m_{\vartheta(t)+z}(t)) = \operatorname{disc}(\mathbb{Z}[\vartheta + z]). \end{aligned}$$

Analog gilt für die Multiplikation:

$$\begin{aligned} \operatorname{disc}(\mathbb{Z}[z\vartheta]) &= \prod_{1 \le i < j \le n} (z\vartheta^{(i)} - z\vartheta^{(j)})^2 \\ &= \prod_{1 \le i < j \le n} z^2 (\vartheta^{(i)} - \vartheta^{(j)})^2 \\ &= z^{2\sum_{\mu=1}^{n-1} \mu} \operatorname{disc}(\mathbb{Z}[\alpha\alpha]). \end{aligned}$$

Für die letzte Behauptung überlege man sich, dass die Gleichungsordnung $\mathbb{Z}[\vartheta^m]$ einer Potenz von ϑ echt in der Gleichungsordnung $\mathbb{Z}[\vartheta]$ enthalten ist, damit teilt der Modulindex $[\mathfrak{o}_\mathcal{F} : \mathbb{Z}[\vartheta]]$ den Modulindex $[\mathfrak{o}_\mathcal{F} : \mathbb{Z}[\vartheta^m]]$. □

Eine weitere Idee um ein primitives Element $\tilde{\vartheta}$, welches für p kein Indexteiler ist, zu berechnen, benutzt den Begriff der p-maximalen Oberordnung. Folgende Schritte skizzieren einen Algorithmus:

(1) Prüfe, dass $p \geq \deg(\mathcal{K})$ gilt.

(2) Berechne die p-maximale Oberordnung $\mathbb{Z}[\vartheta]_p$ der Gleichungsordnung $\mathbb{Z}[\vartheta]$.

(3) Stelle $\mathbb{Z}[\vartheta]_p$ mit Hilfe einer Potenzbasis $\{1, \tilde{\vartheta}, \ldots, \tilde{\vartheta}^{n-1}\}$ dar.

(4) Es gilt $\mathcal{F} \cong \mathbb{Q}[t]/\langle m_{\tilde{\vartheta}}(t)\rangle_{\mathbb{Q}[t]}$ und p teilt nicht den Index $i(\tilde{\vartheta})$.

Der Begriff der p-maximalen Oberordnung ist der Terminologie des Round-2 Algorithmus entliehen:

Definition 2.24. *Sei $\mathcal{O}$ eine Ordnung in $\mathcal{F}$, dann nennt man*

$$\mathcal{O}_p := \{\alpha \in \mathfrak{o}_\mathcal{F} \mid \exists\, m \in \mathbb{N} :\ p^m\alpha \in \mathcal{O}\}$$

*die p-**maximale Oberordnung der Ordnung** $\mathcal{O}$.*

Jede p-maximale Oberordnung $\mathcal{O}_p$ ist eine Ordnung, für welche $p \nmid [\mathfrak{o}_\mathcal{F} : \mathcal{O}_p]$ gilt. Eine genaue Beschreibung der Berechnung von p-maximalen Oberordnungen kann zum Beispiel in [Poh93, V, 2] nachgelesen werden.

Ist $p > \deg(\mathcal{F})$, so weiß man aus (2.20), dass für $\mathcal{O}_p$ eine Potenzbasis existiert; Denn ist p kein CNEDD, muss es ein primitives Element $\tilde{\vartheta}$ geben, für welches p nicht den Index $i(\tilde{\vartheta})$ teilt. Man ist also „nur“ mit dem Problem konfrontiert, für eine gegebene Ordnung $\mathcal{O}$ eine Potenzbasis auszurechnen. Leider ist das alles Andere als trivial. Man wird geführt auf die Theorie der Indexformgleichungen:

Sei $\{1, \alpha_2, \ldots, \alpha_{n-1}\}$ eine Ganzheitsbasis von $\mathcal{F}$. Ein Element $L(\underline{a}) \in \mathcal{F}$ stelle man dar durch

$$L(\underline{a}) = a_1 + a_2\alpha_2 + \ldots + a_{n-1}\alpha_{n-1} \qquad a_i \in \mathbb{Q},\ \forall\, i \in \mathbb{N}_{n-1},$$

dann sind die Konjugierten von $L(\underline{a})$ in $\mathcal{F}$ gegeben durch

$$L(\underline{a})^{(i)} = a_1 + a_2\alpha_2^{(i)} + \ldots + a_{n-1}\alpha_{n-1}^{(i)}$$

für alle $i \in \mathbb{N}_n$. Die Diskriminante der von den $L(\underline{a})^{(i)}$ erzeugten Gleichungsordnungen $\mathbb{Z}[L(\underline{a})^{(i)}]$ berechnet sich zu

$$\operatorname{disc}(\mathbb{Z}[L(\underline{a})^{(i)}]) = \prod_{1 \le i < j \le n} (L(\underline{a})^{(i)} - L(\underline{a})^{(j)})^2.$$

Unter Beachtung von (1.17) definiert man nun:

Definition 2.25. *Seien die Voraussetzungen wie beschrieben. Dann nennt man die Form*

$$I(a_2, \ldots, a_n) := \frac{\prod_{1 \le i < j \le n} (L(\underline{a})^{(i)} - L(\underline{a})^{(j)})^2}{\sqrt{\operatorname{disc}(\mathcal{F})}}$$

die ***Indexform bzgl. der Ganzheitsbasis*** $\{1, \alpha_2, \ldots, \alpha_{n-1}\}$. *Eine Gleichung der Form*

$$I(a_2, \ldots, a_n) = \pm 1$$

nennt man ***die zu*** I ***gehörige Indexformgleichung****.*

Folgendes Lemma beschreibt Indexformen genauer:

Lemma 2.26. *Seien die Voraussetzungen wie in (2.25). Dann ist* $I(a_2, \ldots, a_n)$ *eine homogene Form in* $n-1$ *Variablen vom Grad* $n(n-1)/2$.

[Gaá02, Lemma 1.1.2] Es existieren Algorithmen zum Lösen von Indexformgleichungen für Zahlkörper bis zum Grad 5 einschließlich. Partielle Lösungen existieren bis zum Grad 9, welche aber nicht sehr effektiv sind [Wil97].

Im vorliegenden Fall ist man jedoch an Potenzganzheitsbasen von p-maximalen Oberordnungen interessiert. Sei $\mathcal{O}_p$ eine p-maximale Oberordnung, dann lautet die dazugehörige Indexform

$$I(a_2, \ldots, a_n) := \frac{\prod_{1 \le i < j \le n} (L(\underline{a})^{(i)} - L(\underline{a})^{(j)})^2}{\sqrt{\operatorname{disc}(\mathcal{O}_p)}}.$$

Man ist an einer Lösung der Form $I(a_2, \ldots, a_n) = \pm 1$ interessiert, denn genau diese Lösung generiert ein gesuchtes primitives Element. Oft nennt man diese Gleichungen auch **p-adische Indexformgleichungen**. Leider gibt es bis zum heutigen Stand keine Forschungsergebnisse, welche sich algorithmisch verwenden lassen. Es ist möglich, in kubischen und quartischen Zahlkörpern p-adische Indexformgleichungen zu lösen, jedoch kann man hier die Primidealfaktorisierung sehr schnell mit Hilfe der Algorithmen aus (1.3) und (1.4) ausrechnen.

Der dritte untersuchte Ansatz, in einem Zahlkörper ein „besseres“ primitives Element zu konstruieren, ist die **OrderShort-Methode**:

Beispiel 2.27. *Sei $\mathbb{Q}[\vartheta]$ Zahlkörper mit ϑ Nullstelle des Polynoms $m_\vartheta(t) = t^3+17t^2-2t+9 \in \mathbb{Z}[t]$. Die Transformationsmatrix der Maximalordnung $\mathfrak{o}_\mathcal{F}$ hat die Form*

$$(d, M) := \left(15, \begin{pmatrix} 15 & 0 & 6 \\ 0 & 15 & 13 \\ 0 & 0 & 1 \end{pmatrix} \right).$$

Der Index von ϑ ist $i(\vartheta) = 15$. Das dritte Basiselement der Maximalordnung $\alpha := (6+13\vartheta+15\vartheta^2)/15$ ist primitiv und hat den Index 1! Damit kann man $\mathbb{Q}[\vartheta]$ beschreiben mit Hilfe des Minimalpolynoms $m_\alpha(t) = t^3-6t^2+5t-3$ von α und erhält so eine Darstellung ohne Indexteiler.

Man wird auf folgenden Ansatz geführt:

(1) Betrachte die Maximalordnung des Zahlkörpers $\mathcal{F}$ und führe auf der Basis eine LLL-Reduktion durch [PZ97, Chapter 3, (3.40)]. Die intuitive Idee ist, dass „kurze“ Elemente „kleine“ Indices haben.

(2) Bilde kleine Linearkombinationen $\gamma_1, \gamma_2, \ldots$ von Elementen der LLL-reduzierten Maximalordnung, welche einen Nenner haben. „Elemente mit Nenner“ bedeutet, dass ein Element ω der Maximalordnung nicht dargestellt werden kann durch eine $\mathbb{Z}$-Linearkombinationen mit Elementen der Gleichungsordnung. „Kleine“ Linearkombinationen meint, dass die Koeffizienten Elemente der Menge $\{0, 1\}$ sind. Die Existenz mindestens eines primitiven Elementes in der Menge dieser Linearkombinationen garantiert der Satz von Sonn[4]-Zassenhaus [PZ97, Chapter 2, (12.23)].

(3) Verkleinert sich der Index für ein γ_i, wähle γ_i als neues primitives Element von $\mathcal{F}$ und springe zu (1). Ist für γ_i die zu zerlegende Primzahl $p \in \mathbb{P}_\mathbb{Z}$ kein Indexteiler, terminiere.

Man arbeitet mit drei Zählern: Einem Zähler, A_1, der festlegt, mit wie vielen Koeffizienten ungleich Null man höchstens arbeitet, einem Zähler A_2, welcher festlegt, wie viele Linearkombinationen überprüft werden. Schließlich führt man einen Zähler A_3 ein, die maximale Anzahl der zu testenden Linearkombinationen. Der ausformulierte Algorithmus sieht so aus:

Algorithmustabelle 5: AlgOrderShort

Input: Zahlkörper $\mathcal{F} = \mathbb{Q}[\vartheta]$, Primzahl $p \in \mathbb{P}_\mathbb{Z}$ mit $p \mid i(\vartheta)$

[4] Jack Sonn, $\star$1940

- A_1 Anzahl der zu testenden Linearkombinationen
- A_2 Maximale Anzahl der Koeffizienten ungleich 0

Output: {True, α}, falls ein primitives Element
α gefunden wurde mit $p \nmid i(\alpha)$, sonst {False, 0}
begin:
{Initialisierung}
$a_1 \leftarrow A_1$, $a_2 \leftarrow A_2$, $a_3 \leftarrow 0$
Berechne Maximalordnung $\mathfrak{o}_{\mathcal{F}}$
Führe auf $\mathfrak{o}_{\mathcal{F}}$ LLL-Reduktion durch
erhalte reduzierte $\mathbb{Z}$-Basis $\omega_1, \ldots, \omega_n$ von $\mathfrak{o}_{\mathcal{F}}$
Wähle Elemente $\tilde{\omega}_1, \ldots, \tilde{\omega}_m$ mit Nenner
$a_3 \leftarrow \binom{m}{a_1}$
while $a_1 \neq 0$ **and** $a_3 > 0$ **do**
{Bilde Linearkombination}
$\alpha \leftarrow \sum_{i=1}^{m} a_i \tilde{\omega}_i, \quad a_i \in \{0,1\}, \ \max_{i \in \mathbb{N}_m}\{a_i \mid a_i = 1\} \leq a_2$
$a_3 \leftarrow a_3 - 1$
Berechne $i(\alpha)$
if $p \nmid i(\alpha)$ **then**
return {True, α}
else if $i(\alpha) < i(\vartheta)$ **then**
$\vartheta \leftarrow \alpha$
$a_1 \leftarrow A_1$
else
$a_1 \leftarrow a_1 - 1$
end if
end while
return {False, 0}

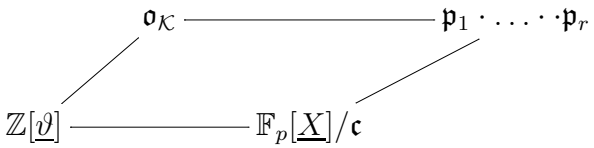
Dieser Algorithmus ist unter dem Namen OrderShort in dem Computeralgebrasystem KANT-V4 implementiert, wurde jedoch im Rahmen dieser Arbeit zur Verwendung für Leistungsmessungen komplett neu geschrieben.

Diese Untersuchungen haben ergeben, dass die Verwendung von OrderShort nicht sinnvoll ist, wenn man diesen Algorithmus nur verwenden möchte, um die Primidealfaktorisierung zu berechnen. Auch garantiert der Algorithmus nicht, dass wirklich ein besseres primitives Element gefunden wird, selbst wenn ein solches existiert, was im Fall $p > \deg(\mathcal{F})$ immer gegeben ist. Hier meint „besser“ ein Element mit kleinerem Index. („Besser“ kann auch meinen, dass der Index eines neuen primitiven Elementes coprim zur zu zer-

legenden Primzahl ist.) Ein weiteres Problem beim OrderShort Algorithmus ist das Anwachsen der Koeffizienten für das neue Minimalpolynom. Hat man ein besseres Minimalpolynom gefunden, so speichert man zusätzlich das ursprüngliche Minimalpolynom ab, damit man bei weiteren Rechnungen darauf zurückgreifen kann und nicht auf die unverhältnismäßig großen Koeffizienten des neuen angewiesen ist. Das Ergebnis dieser Untersuchungen ist in (B.3) zusammengefasst.

Kapitel 3

Primidealfaktorisierung durch Primärdekomposition



Dieses Kapitel untersucht folgenden Ansatz, die Primidealfaktorisierung in einem Kompositum von Zahlkörpern zu bestimmen: Beim Zerlegungssatz (1.35) führt man die Primidealzerlegung zurück auf die Faktorisierung des Minimalpolynoms $m_\vartheta(t) \in \mathbb{Z}[t]$ modulo der Primzahl $p \in \mathbb{P}_\mathbb{Z}$, welche man zerlegen will. Damit bestimmt man die Primideale des Restklassenringes

$$\mathbb{F}_p[t]/\langle \overline{m}_\vartheta(t) \rangle_{\mathbb{F}_p[t]}.$$

Bei einem Körperkompositum $\mathcal{K} := \mathbb{Q}[\vartheta_1, \ldots, \vartheta_n]$ hat man nun nicht ein definierendes Minimalpolynom, sondern mehrere, nämlich die Minimalpolynome $m_{\vartheta_1}(t), \ldots, m_{\vartheta_n}(t) \in \mathbb{Z}[t]$ der an dem Komposition beteiligten Zahlkörper $\mathbb{Q}[\vartheta_1], \ldots, \mathbb{Q}[\vartheta_n]$. Die Idee liegt nahe, die Primideale des Restklassenringes

$$\mathbb{F}_p[X_1, \ldots, X_n]/\langle \overline{m}_{\vartheta_1}(t), \ldots, \overline{m}_{\vartheta_n}(t) \rangle_{\mathbb{F}_p[t]}$$

zu bestimmen, um so Informationen über das Zerlegungsverhalten von p in $\mathcal{K}$ zu erhalten.

Man hat zwei Aufgaben zu lösen: Man betrachtet statt univariaten Polynomringen multivariate, in denen man nicht ein Polynom faktorisiert, sondern mehrere. Diese Aufgabe löst man mit Primärdekomposition, welche detailliert in (3.1) und (3.2) erläutert wird. Die andere Aufgabe ist zu untersuchen,

in wieweit der Zerlegungssatz (1.35) auf Komposita von Zahlkörpern übertragen werden kann. Es wurde im Rahmen dieser Arbeit untersucht, auf welche Komposita sich der Satz übertragen lässt und der Zerlegungssatz wurde in dieser allgemeineren Form bewiesen. Diesem verallgemeinerten Zerlegungssatz ist Unterabschnitt (3.3) gewidmet. Auch wird erläutert, warum die Primärdekomposition nicht zur Primidealfaktorisierung in beliebigen Komposita benutzt werden kann. In den restlichen Unterabschnitten werden die Ergebnisse aus (3.1), (3.2) und (3.3) algorithmisch ausgewertet.

3.1 Primärdekomposition in noetherschen Ringen

Dieser Unterabschnitt führt ein in die Theorie der Primärdekomposition in allgemeinen noetherschen Ringen bis hin zum Satz von Lasker[1]-Noether. Man findet die Theorie der Primärdekomposition zum Beispiel in [BW93, CLO92, Eis95]. Zuerst wird der Sinn und Zweck der Primärdekomposition in einer Bemerkung erläutert.

Seien für diesen Abschnitt alle Ideale ungleich dem Nullideal.

Bemerkung 3.1. *In einem Hauptidealring R kann man ein Ideal $\mathfrak{a}$ in Primideale zerlegen, indem man für den (garantiert existierenden) Erzeuger $a \in R$ dieses Ideals die Primfaktorzerlegung*

$$a = \prod_{i=1}^{n} p_i^{e_i}, \qquad p_i \in \mathbb{P}_R,\ i \in \mathbb{N}_n$$

durchführt. Die einzelnen p_i generieren dann die Primideale $\langle p_i \rangle_R$, welche in der Primidealfaktorisierung von $\mathfrak{a}$ auftreten. Die Idee, welche hinter der Primärdekomposition steht, ist, dieses Vorgehen auf beliebige noethersche Ringe zu übertragen. Man erhält in der Zerlegung keine Primideale mehr, wohl aber Primärideale, das sind Ideale, die sich „so ähnlich" verhalten, wie Primideale.

Definition 3.2. *Sei R ein Ring und sei $\mathfrak{a}$ ein Ideal von R. $\mathfrak{a}$ heißt **Primärideal**, wenn $\mathfrak{a}$ echtes Ideal ist, und für jedes Produkt $ab \in \mathfrak{a}$, mit $a, b \in R$ gilt: aus $a \notin \mathfrak{a}$ folgt $b^n \in \mathfrak{a}$ mit einem $n \in \mathbb{N}$.*

Beispielsweise sind alle Primideale Primärideale. Die Umkehrung gilt nicht, betrachte zum Beispiel $\mathfrak{a} := \langle 4 \rangle_{\mathbb{Z}}$. Zu jedem Primärideal gehört ein eindeutig bestimmtes Primideal:

[1] Emanuel Lasker, 1868 – 1941

Lemma 3.3. *Sei $\mathfrak{a}$ ein Primärideal eines Ringes R. Dann ist das* ***Radikal von*** $\mathfrak{a}$*, also die Menge*

$$\mathrm{Rad}(\mathfrak{a}) := \{a \in R \mid \exists\, n \in \mathbb{N} :\ a^n \in \mathfrak{a}\}$$

ein Primideal von R, welches $\mathfrak{a}$ enthält.

[BW93, Lemma 8.38]

Definition 3.4. *Seien die Bezeichnungen wie in (3.3). Man nennt* $\mathrm{Rad}(\mathfrak{a})$ ***das zu $\mathfrak{a}$ gehörige*** *oder* ***assoziierte Primideal*** $\mathrm{ass}(\mathfrak{a})$*. Statt* $\mathrm{Rad}(\mathfrak{a})$ *ist auch die Bezeichnung $\sqrt{\mathfrak{a}}$ gebräuchlich.*

Bemerkung 3.5. *Das Radikal eines Ideals* $\mathrm{Rad}(\mathfrak{a})$ *und das p-Radikal einer Ordnung $\mathcal{O}$ aus (1.37) sind verschiedene Begriffe.*

Definition 3.6. *Ein Ideal $\mathfrak{a}$ eines Ringes R heißt* ***reduzibel****, falls Ideale $\mathfrak{a}_1, \mathfrak{a}_2 \in R$, $\mathfrak{a}_1 \neq \mathfrak{a} \neq \mathfrak{a}_2$ existieren mit $\mathfrak{a} = \mathfrak{a}_1 \cap \mathfrak{a}_2$, sonst* ***irreduzibel****.*

Den Zusammenhang zwischen irreduziblen und Primäridealen stellt folgendes Lemma her:

Lemma 3.7. *Sei R noetherscher Ring. Dann ist jedes Ideal $\mathfrak{a}$ von R der Schnitt von endlich vielen irreduziblen Idealen*

$$\mathfrak{a} = \bigcap_{i=1}^{r} \mathfrak{q}_i, \quad r \in \mathbb{N},$$

und jedes dieser irreduziblen Ideale ist ein Primärideal.

[BW93, Lemma 8.51, Lemma 8.52] Für die Darstellung eines Ideals als Schnitt von irreduziblen Idealen erhält man, ähnlich der Primidealzerlegung in Dedekindringen, in noetherschen Ringen eine Existenz- und Eindeutigkeitsaussage, welche in der Literatur unter dem Namen „Satz von Lasker-Noether“ bekannt ist:

Satz 3.8. ***Existenz der Primärdekomposition***
Sei R noetherscher Ring und $\mathfrak{a} \in \mathcal{I}_R$ echtes Ideal. Dann existieren Primärideale $\mathfrak{q}_1, \ldots, \mathfrak{q}_r \in \mathcal{I}_R$ mit folgenden Eigenschaften:

- $\mathfrak{a} = \bigcap_{i=1}^{r} \mathfrak{q}_i$.
- *Keines der $\mathfrak{q}_i$ enthält den Schnitt der anderen:*

$$\bigcap_{\substack{i \in \mathbb{N}_r \\ i \neq j}} \mathfrak{q}_i \not\subseteq \mathfrak{q}_j.$$

- *Die zu den* $\mathfrak{q}_1, \ldots, \mathfrak{q}_r$ *assoziierten Primideale* $\operatorname{ass}(\mathfrak{q}_1), \ldots, \operatorname{ass}(\mathfrak{q}_r)$ *sind paarweise verschieden:* $\operatorname{ass}(\mathfrak{q}_i) \neq \operatorname{ass}(\mathfrak{q}_j)$ *für alle* $i, j \in \mathbb{N}_r$ *mit* $i \neq j$.

[BW93, Theorem 8.54] Die $\mathfrak{q}_1, \ldots, \mathfrak{q}_r$ aus (3.8) bekommen einen besonderen Namen:

Definition 3.9. *Seien die Bezeichnungen wie in (3.8). Dann nennt man eine Darstellung von* $\mathfrak{a}$ *der Art* $\mathfrak{a} = \bigcap_{i=1}^{r} \mathfrak{q}_i$ *eine* ***Primärdekomposition des Ideals*** $\mathfrak{a}$ *und die* $\mathfrak{q}_1, \ldots, \mathfrak{q}_r$ *die* ***Primärkomponenten des Ideals*** $\mathfrak{a}$.

Man möchte nun eine Eindeutigkeitsaussage formulieren. Dazu unterscheidet man Primärkomponenten wie folgt:

Definition 3.10. *Eine Primärkomponente* $\mathfrak{q}$ *eines Ideals* $\mathfrak{a}$ *heißt* ***isoliert****, falls das zugehörige Primideal* $\operatorname{ass}(\mathfrak{q})$ *nicht das zugehörige Primideal einer anderen Primärkomponente echt enthält. Sonst heißt* $\mathfrak{q}$ ***eingebettet***.

Die Bezeichnungen „isoliert“ und „eingebettet“ sind auch für die zugehörigen Primideale gebräuchlich. Jetzt kann die Eindeutigkeitsaussage für die Primärdekomposition formuliert werden:

Satz 3.11. ***Eindeutigkeit der Primärdekomposition***
Seien die Bezeichnungen wie in (3.8) und seien

$$\mathfrak{a} = \bigcap_{i=1}^{r_1} \mathfrak{q}_{1,i} = \bigcap_{j=1}^{r_2} \mathfrak{q}_{2,j}$$

zwei Primärdekompositionen von $\mathfrak{a}$. *Dann sind diese im folgendem Sinne eindeutig:*

- $r_1 = r_2$.
- *Die Mengen der zu den Primärkomponenten zugehörigen Primideale sind gleich:*

$$\begin{aligned} & \{\mathfrak{p} \in \mathbb{P}_R \mid \exists\, i \in \mathbb{N}_{r_1} :\ \operatorname{ass}(\mathfrak{q}_{1,i}) = \mathfrak{p}\} \\ = \ & \{\mathfrak{p} \in \mathbb{P}_R \mid \exists\, j \in \mathbb{N}_{r_2} :\ \operatorname{ass}(\mathfrak{q}_{2,j}) = \mathfrak{p}\}. \end{aligned}$$

- *Ist* $\mathfrak{q}$ *isolierte Primärkomponente von* $\mathfrak{a}$, *dann existieren* $i \in \mathbb{N}_{r_1}$ *und* $j \in \mathbb{N}_{r_2}$ *mit* $\mathfrak{q} = \mathfrak{q}_{1,i} = \mathfrak{q}_{2,j}$.

[BW93, Theorem 8.55, Theorem 8.56] [CLO92, 4, §7, Theorem 7, Theorem 9]. Würde man Primärdekompositionen nur in Ringen R betrachten, in denen Primärkomponenten automatisch isoliert sind, erreichte man, ähnlich der Primidealzerlegung in Dedekindringen, Eindeutigkeit der Primärdekomposition bis auf die Reihenfolge der Faktoren:

Korollar 3.12. *Sei R ein noetherscher Ring. Sei jedes Primärideal $\mathfrak{q}$ von R isoliert. Dann hat jedes Ideal $\mathfrak{a}$ von R eine bis auf die Reihenfolge der Faktoren eindeutige Primärdekomposition.*

Dieses Korollar bildet im nächsten Abschnitt die Grundlage, um ein Ideal eines multivariaten Polynomringes über einem endlichen Körper in Primideale zu zerlegen.

3.2 Primärdekomposition über endlichen Körpern

Dieser Unterabschnitt beschreibt die Technik der Primärdekomposition in multivariaten Polynomringen über endlichen Körpern. Sei für diesen Abschnitt $\underline{X} := \{X_1, \ldots, X_n\}$ eine Menge von Unbestimmten und K ein Körper. Sei $K[\underline{X}]$ multivariater Polynomring.

Die Aufgabenstellung für diesen Abschnitt lautet:

Bemerkung 3.13. *Sei $\mathbb{F}_p[\underline{X}]$ multivariater Polynomring über einem endlichen Körper $\mathbb{F}_p$. Sei $\mathfrak{c} = \langle \overline{m}_{\vartheta_1}(X_1), \ldots, \overline{m}_{\vartheta_n}(X_n) \rangle_{\mathbb{F}_p[t]}$ ein Ideal von $\mathbb{F}_p[\underline{X}]$, welches von normierten, irreduziblen Polynomen $\overline{m}_{\vartheta_i}(X_i) \in \mathbb{F}_p[X_i]$, $i \in \mathbb{N}_n$, erzeugt wird. Bestimme alle Primideale des Restklassenringes $\mathbb{F}_p[\underline{X}]/\mathfrak{c}$.*

Man benötigt für das Weitere die Begriffe Dimension von Idealen und radikale Ideale:

Definition 3.14. *Sei $\mathfrak{a} \in \mathcal{I}^{\times}_{K[\underline{X}]}$ echtes Ideal. Sei $\underline{U} := \{U_1, \ldots, U_r\} \subseteq \underline{X}$. Dann heißt die Menge*

$$\mathfrak{a}_{\underline{U}} := \mathfrak{a} \cap K[\underline{U}]$$

*das **Eliminationsideal von $\mathfrak{a}$ bzgl. $\underline{U}$**. $\underline{U}$ heißt **unabhängig modulo $\mathfrak{a}$**, falls $\mathfrak{a}_{\underline{U}} = \{0\}$ ist. $\underline{U}$ heißt **maximal unabhängig**, falls $\underline{U}$ unabhängig modulo $\mathfrak{a}$ ist, und nicht echt in einer modulo $\mathfrak{a}$ unabhängigen Menge enthalten ist.*

$$\dim(\mathfrak{a}) := \max\{\#U \mid \underline{U} \subseteq \underline{X} \text{ ist unabhängig modulo } \mathfrak{a}\}$$

*heißt die **Dimension** $\dim(\mathfrak{a})$ **von** $\mathfrak{a}$.*

Die in diesem Abschnitt betrachteten Ideale sind immer 0-dimensional:

Lemma 3.15. *Sei $\mathfrak{a}$ echtes Ideal von $K[X_1, \ldots, X_n]$. $\mathfrak{a}$ ist genau dann 0-dimensional, falls $\mathfrak{a}$ in jeder Variable X_i, $i \in \mathbb{N}_n$, ein nicht-konstantes, univariates Polynom enthält.*

[BW93, Lemma 6.50] Folgendes Lemma zeigt, dass (3.12) auf das Ideal $\mathfrak{c}$ aus (3.13) angewendet werden kann:

Lemma 3.16. *Sei $\mathfrak{a}$ ein 0-dimensionales Ideal von $K[\underline{X}]$. Dann ist jede Primärkomponente von $\mathfrak{a}$ isoliert.*

[BW93, Lemma 8.60]

Definition 3.17. *Sei $\mathfrak{a}$ ein Ideal eines Ringes R. Ist $\mathfrak{a}$ gleich seinem Radikal* $\mathrm{Rad}(\mathfrak{a})$*, so heißt $\mathfrak{a}$* ***radikales Ideal****.*

Die in diesem Abschnitt betrachteten Ideale sind immer radikal:

Lemma 3.18. *Sei K ein perfekter Körper, dann ist ein 0-dimensionales Ideal $\mathfrak{a}$ von $K[\underline{X}]$ genau dann radikal, wenn $\mathfrak{a}$ in jeder Unbestimmten X_i ein univariates, quadratfreies Polynom enthält.*

[BW93, Lemma 6.50] Insbesondere ist mit (3.18) das betrachtete Ideal $\mathfrak{c}$ aus (3.13) radikal. Für radikale Ideale vereinfacht sich die Primärdekomposition ungemein:

Lemma 3.19. *Sei $\mathfrak{a}$ ein 0-dimensionales Ideal von $K[\underline{X}]$. Dann sind die Primärkomponenten von* $\mathrm{Rad}(\mathfrak{a})$ *genau die zugehörigen Primideale der Primärkomponenten von $\mathfrak{a}$. Ist insbesondere $\mathfrak{a}$ radikal, dann sind die Primärkomponenten von $\mathfrak{a}$ genau die Primideale, welche $\mathfrak{a}$ enthalten.*

[BW93, Lemma 8.60] Man kennt daher die Primärdekomposition von $\mathfrak{c}$ in (3.13), sobald man paarweise verschiedene Primideale $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ gefunden hat, für die gilt:

$$\mathfrak{c} = \mathfrak{p}_1 \cap \ldots \cap \mathfrak{p}_n.$$

Den theoretischen Hintergrund zur Primärdekomposition liefert der Beweis des „Seidenberg[2] Lemma 92“. Diesem Lemma werden zwei Propositionen vorausgeschickt:

Proposition 3.20. *Sei $\mathfrak{a}$ ein Ideal von $K[\underline{X}]$. Seien $f, g_1, \ldots, g_r \in K[X_1]$ mit der Eigenschaft gegeben, dass $f = g_1 \cdot \ldots \cdot g_n$ eine Faktorisierung von f in $K[X_1]$ in paarweise relativ prime Faktoren ist. Dann gilt*

$$\langle \mathfrak{a}, f \rangle_{K[\underline{X}]} = \bigcap_{i=1}^{r} \langle \mathfrak{a}, g_i \rangle_{K[\underline{X}]}.$$

[BW93, Lemma 8.5]

[2] Abraham Seidenberg, 1916 – 1988

Proposition 3.21. *Sei $f : R_1 \to R_2$ ein Ringepimorphismus und $\mathcal{I}_{R_1}^f$ die Menge der Ideale $\mathfrak{a}$ von R_1 mit der Eigenschaft $\ker(f) \subseteq \mathfrak{a}$. Dann ist die Abbildung*

$$\begin{aligned} \chi \quad : \quad & \mathcal{I}_{R_1}^f \to \mathcal{I}_{R_2} \\ & \mathfrak{a} \mapsto f(\mathfrak{a}) \end{aligned}$$

eine Bijektion mit Umkehrabbildung $\chi^{-1}(\mathfrak{a}) = f^{-1}(\mathfrak{a})$. Insbesondere ist χ eine Bijektion zwischen den maximalen Idealen $\mathfrak{m} \in \mathcal{MI}_{R_1}$ mit $\ker(f) \subseteq \mathfrak{m}$ und den maximalen Idealen von R_2.

[BW93, Lemma 1.62]

Lemma 3.22. ***„Seidenbergs Lemma 92“***
Sei $\mathfrak{a}$ ein 0-dimensionales Ideal von $K[\underline{X}]$ mit der Eigenschaft, dass für $i \in \mathbb{N}_n$ ein Polynom $f_i \in K[X_i] \cap \mathfrak{a}$ existiert mit $\gcd(f_i, f_i') = 1$. Dann ist $\mathfrak{a}$ ein Schnitt von endlich vielen maximalen Idealen, insbesondere ist $\mathfrak{a}$ radikal.

Beweis. Wegen $\gcd(f_i, f_i') = 1$ sind die f_i quadratfrei. Der Beweis erfolgt mit Induktion über die Anzahl der Unbestimmten n:

$n = 1$: Sei $f = g_1 \cdot \ldots \cdot g_r$ die Faktorisierung von f in paarweise nicht-assoziierte, irreduzible Polynome aus $K[X_1]$. Dann sind die g_i paarweise relativ prim und es gilt mit (3.20)

$$\mathfrak{a} = \langle f(X_1)\rangle_{K[X_1]} = \bigcap_{i=1}^{r} \langle g_i(X_1)\rangle_{K[X_1]}.$$

Die Ideale $\langle g_i(X_1)\rangle_{K[X_1]}$ sind für alle $i \in \mathbb{N}_r$ maximal, da die Erzeuger $g_i(X_1)$ irreduzibel sind und $K[X_1]$ Hauptidealring ist.

$n > 1$: Wie im Falle $n = 1$ sei $f_1 = g_1 \cdot \ldots \cdot g_r$ eine Faktorisierung von $f_1 \in K[X_1]$ in paarweise nicht-assoziierte, irreduzible Polynome $g_i \in K[X_1]$, $i \in \mathbb{N}_r$. Mit (3.20) gilt

$$\mathfrak{a} = \langle \mathfrak{a}, f_1\rangle_{K[\underline{X}]} = \bigcap_{i=1}^{r} \langle \mathfrak{a}, g_i\rangle_{K[\underline{X}]}.$$

Es reicht zu zeigen, dass die Ideale $\langle \mathfrak{a}, g_i(X_1)\rangle_{K[\underline{X}]}$ für $i \in \mathbb{N}_r$ die Schnitte von endlich vielen maximalen Idealen sind. Nehme also o. B. d. A. an, dass f_1 irreduzibel ist (denn sonst wende (3.20) erneut an).

$K[X_1]/\langle f_1\rangle_{K[X_1]}$ ist ein Restklassenring und Körper. Betrachte dazu die (per Definition surjektive) kanonische Projektion:

$$\begin{aligned} \pi \quad : \quad & K[X_1] \to K[X_1]/\langle f_1\rangle_{K[X_1]} \\ & g(X_1) \mapsto g(X_1) + \langle f_1\rangle_{K[X_1]} \end{aligned}$$

Bildet man über $K[X_1]$ und $K[X_1]/\langle f_1\rangle_{K[X_1]}$ den Polynomring über $n-1$ Unbestimmten, so induziert π einen Ringepimorphismus zwischen diesen Polynomringen:

$$\begin{array}{rcl}\varphi & : & K[X_1][X_2,\ldots,X_n] \to (K[X_1]/\langle f_1\rangle_{K[X_1]})[X_2,\ldots,X_n] \\ & & \sum_{j=1}^{m} g_j(X1)X_2^{\nu_{2,j}}\ldots X_n^{\nu_{n,j}} \mapsto \sum_{j=1}^{m}\left((g_j(X1)+\langle f_1\rangle_{K[X_1]})X_2^{\nu_{2,j}}\ldots X_n^{\nu_{n,j}}\right)\end{array}$$

[BW93, Lemma 2.17, (II)] Das Bild $\varphi(\mathfrak{a}) =: \mathfrak{b}$ ist ein Ideal von

$$(K[X_1]/\langle f_1\rangle_{K[X_1]})[X_2,\ldots,X_n],$$

denn Bilder von Idealen unter Ringepimorphismen sind Ideale.

Die Induktionsvoraussetzung kann auf $\mathfrak{b}$ angewendet werden: Betrachte $K[X_1]/\langle f_1\rangle_{K[X_1]}$ durch die Einbettung

$$\begin{array}{rcl}\iota & : & K \to K[X_1]/\langle f_1\rangle_{K[X_1]} \\ & & a \mapsto a+\langle f_1\rangle_{K[X_1]}\end{array}$$

als Körpererweiterung von K. Es ist $\varphi|_K = \mathrm{Id}_K$ und damit gilt für die Polynome $f_2,\ldots,f_n$ die Voraussetzung $\gcd(f_i, f_i') = 1$ auch über dem Körper $K[X_1]/\langle f_1\rangle_{K[X_1]}$. Denn es ist $\varphi(f_i) = f_i \in \mathfrak{b}$, und der euklidische Algorithmus verläuft in $\iota(K)$ genau so, wie in einer beliebigen Körpererweiterung (hier $K[X_1]/\langle f_1\rangle_{K[X_1]}$) von K.

Nun ist $\mathfrak{b}$ ein Ideal in einem Polynomring in $n-1$ Unbestimmten über einem Körper K und enthält für alle $i \in \mathbb{N}_{2,n}$ ein Polynom $f_i \in K[X_i]$ mit der Eigenschaft $\gcd(f_i, f_i') = 1$. Mit der Induktionsvoraussetzung ist $\mathfrak{b}$ gleich dem Schnitt von endlich vielen maximalen Idealen:

$$\mathfrak{b} = \mathfrak{m}_1 \cap \ldots \cap \mathfrak{m}_s.$$

Betrachte für die Menge $\mathfrak{b}$ die Umkehrabbildung φ^{-1} von φ, dann ist

$$\mathfrak{a} = \varphi^{-1}(\mathfrak{b}) = \varphi^{-1}\left(\bigcap_{i=1}^{s}\mathfrak{m}_i\right) = \bigcap_{i=1}^{s}\varphi^{-1}(\mathfrak{m}_i).$$

Denn aufgrund $\ker(\varphi) = \langle f_1\rangle_{K[\underline{X}]}$ gilt $\ker(\varphi) \subseteq \mathfrak{a}$ und (3.21) ist anwendbar. Wieder wegen (3.21), $\ker(\varphi) \subseteq \mathfrak{a}$ und der Maximalität der $\mathfrak{m}_i$ sind die $\varphi^{-1}(\mathfrak{m}_i)$ maximal. □

Den ersten Schritt in der Primärdekomposition erläutert folgende Bemerkung:

Bemerkung 3.23. ***Primärdekomposition Teil 1***
Seien die Bezeichnungen wie in (3.13). Faktorisiere den normierten Erzeuger $\overline{m}_{\vartheta_1}(X_1) \in \mathbb{F}_p[\underline{X}]$ *des Eliminationsideals* $\mathfrak{c}_{\{X_1\}}$ *in paarweise relativ prime Polynome*

$$\overline{m}_{\vartheta_1}(X_1) = \prod_{i=1}^{s} \overline{g}_i(X_1).$$

Mit (3.20) erhält man eine Faktorisierung

$$\mathfrak{c} = \bigcap_{i=1}^{s} \langle \mathfrak{c}, \overline{g}_i \rangle_{\mathbb{F}_p[\underline{X}]}.$$

Also hat man jedes der (wegen (3.18)) radikalen Ideale $\langle \mathfrak{c}, \overline{g}_i \rangle_{\mathbb{F}_p[\underline{X}]}$ *in Primideale zu zerlegen.*

Mit (3.23) kann man sich auf radikale Ideale beschränken, für die gilt, dass für mindestens ein Eliminationsideal $\mathfrak{c}_{\{X_i\}}$ der Generator $\overline{g}_i(X_i)$ irreduzibel ist. Sei o. B. d. A. $i = 1$ (denn sonst tausche die Unbestimmten). Die Aufgabe ist, für diese Ideale die Primärdekomposition zu berechnen. Zur Lösung dieser Aufgabe benutzt man den Beweis des Seidenberg Lemma (3.22):

Bemerkung 3.24. ***Primärdekomposition Teil 2***
Seien die Bezeichnungen wie in (3.13). Sei o. B. d. A. $\overline{m}_{\vartheta_1}(X_1) =: \overline{g}(X_1)$ *irreduzibel, denn sonst faktorisiere* $\overline{m}_{\vartheta_1}(X_1)$ *in* $\mathbb{F}_p[X_1]$.

Es ist $\mathbb{F}_p[X_1]/\langle \overline{g}(X_1) \rangle_{\mathbb{F}_p[X_1]}$ *ein endlicher Körper, und eine eindeutige Menge von Repräsentanten ist gegeben durch*

$$\{\overline{h}(X_1) \in \mathbb{F}_p[X_1] \mid \deg(\overline{h}(X_1)) < \deg(\overline{g}(X_1))\}.$$

Betrachte das Bild von $\mathfrak{c}$ *unter der Abbildung*

$$\begin{aligned}
&\varphi : \mathbb{F}_p[X_1][X_2, \ldots, X_n] \to (\mathbb{F}_p[X_1]/\langle \overline{g}(X_1) \rangle_{\mathbb{F}_p[X_1]})[X_2, \ldots, X_n] \\
&\sum_{j=1}^{m} \overline{h}_j(X_1) X_2^{\nu_{j2}} \ldots X_n^{\nu_{jn}} \\
&\qquad\qquad \mapsto \sum_{j=1}^{m} \left((\overline{h}_j(X_1) + \langle \overline{g}(X_1) \rangle_{\mathbb{F}_p[X_1]}) X_2^{\nu_{j2}} \ldots X_n^{\nu_{jn}} \right)
\end{aligned}$$

und setze $\mathfrak{d} := \varphi(\mathfrak{c})$. *Das Ideal* $\mathfrak{d}$ *ist ein 0-dimensionales Ideal in dem Polynomring mit* $n-1$ *Unbestimmten über dem endlichen Körper* $\mathbb{F}_p[X_1]/\langle \overline{g}(X_1) \rangle_{\mathbb{F}_p[X_1]}$.

Man ruft diese Prozedur rekursiv auf und endet nach n *Rekursionsschritten bei einem univariaten Polynomring* $\tilde{K}[X_n]$ *über einem endlichen Körper*

$\tilde{K}$. Dieser Ring ist Hauptidealring und man kann die Faktorisierung aus (3.1) anwenden.

Man erhält eine Zerlegung

$$\mathfrak{d} = \mathfrak{m}_1 \cap \ldots \cap \mathfrak{m}_t.$$

Die $\mathfrak{m}_i$, $i \in \mathbb{N}_t$ sind genau die Primideale, welche $\mathfrak{d}$ enthalten, und die Urbilder $\varphi^{-1}(\mathfrak{m}_i)$ sind die gesuchten Primärkomponenten. Die $\mathfrak{m}_i$ sind gegeben durch endliche Basen M_i, $i \in \mathbb{N}_t$ und jedes Element von M_i ist gegeben als Repräsentant in $\mathbb{F}_p[\underline{X}]$ seiner Nebenklasse modulo $\ker(\varphi)$. *Dabei ist* $\ker(\varphi) = \langle \overline{g}(X_1) \rangle_{\mathbb{F}_p[X_1]}$. *Es gilt also $M_i \subseteq \mathbb{F}_p[\underline{X}]$ und eine Basis H_i von $\varphi^{-1}(\mathfrak{m}_i)$ ist gegeben durch*

$$H_i := M_i \cup \{g(X_1)\},$$

wobei $g(X_1)$ ein normiertes Urbild von $\overline{g}(X_1)$ ist.

Anknüpfend an (3.13) erhält man folgende Beschreibung der Primärdekomposition in multivariaten Polynomringen über endlichen Körpern:

Bemerkung 3.25. *Sei $\mathbb{F}_p[\underline{X}]$ mit einem Ideal*

$$\mathfrak{c} := \langle \overline{m}_{\vartheta_1}(X_1), \ldots, \overline{m}_{\vartheta_n}(X_n) \rangle_{\mathbb{F}_p[t]}$$

gegeben. $\mathfrak{c}$ ist 0-dimensional (3.15) und radikal (3.18). Man erhält die ***Primärdekomposition*** *$\mathfrak{c} = \bigcap_{i=1}^{r} \mathfrak{p}_i$ von $\mathfrak{c}$. Die $\mathfrak{p}_i$ sind Primärideale von $\mathbb{F}_p[\underline{X}]$ mit folgenden Eigenschaften:*

- *Jedes $\mathfrak{p}_i$ ist Primideal von $\mathbb{F}_p[\underline{X}]$.*
- *Die $\mathfrak{p}_i$ sind genau die Primideale von $\mathbb{F}_p[\underline{X}]$, welche $\mathfrak{c}$ enthalten.*
- *Es gilt $\mathfrak{c} = \bigcap_{i=1}^{r} \mathfrak{p}_i = \prod_{i=1}^{r} \mathfrak{p}_i$, da Primärkomponenten von 0-dimensionalen Idealen paarweise comaximal sind.*

Eine zusammenfassende Beschreibung der Primärdekomposition sieht so aus:

Algorithmustabelle 6: AlgPrimDec

Input: Endlicher Körper K,
Anzahl der Unbestimmten $n \in \mathbb{N}$ in dem Polynomring $K[X_1, \ldots, X_n]$,
Ideal $\mathfrak{a} = \langle \overline{m}_{\vartheta_1}(X_1), \ldots, \overline{m}_{\vartheta_n}(X_n) \rangle_{K[\underline{X}]}$
alle $\overline{m}_{\vartheta_i}(X_i) \in K[X_i]$ normiert

Output: $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_t\} \subseteq \mathbb{P}_{K[\underline{X}]}$ mit $\mathfrak{a} = \prod_{i=1}^{t} \mathfrak{p}_i$,
jedes $\mathfrak{p}_i$ von der Form $\{p_{i,1}(\underline{X}), \ldots, p_{i,i_n}(\underline{X})\} \subseteq K(\underline{X})$
if n=1 **then**
Faktorisiere $\overline{m}_{\vartheta_1}(X_1)$ in $K[X_1]$: $\overline{m}_{\vartheta_1}(X_1) = \prod_{q=1}^{t} \overline{m}_{\vartheta_1,q}(X_1)$
return $\{\{\overline{m}_{\vartheta_1,1}(X_1)\}, \ldots, \{\overline{m}_{\vartheta_1,t}(X_1)\}\}$
else
Faktorisiere $\overline{m}_{\vartheta_1}(X_1)$ in $K[X_1]$: $\overline{m}_{\vartheta_1}(X_1) = \prod_{q=1}^{t} \overline{m}_{\vartheta_1,q}(X_1)$
for all $q \in \mathbb{N}_t$ **do**
$\mathfrak{c}_q \leftarrow \{\mathfrak{a}\} \cup \{\overline{m}_{\vartheta_1,q}(X_1)\}$
end for
{Sei o.B.d.A. $t = 1$, $\mathfrak{c}_1 =: \mathfrak{c}$ und $\overline{m}_{\vartheta_1,1}(X_1) =: \overline{m}_{\vartheta_1}(X_1)$}
{Konstruiere endlichen Körper}
$\tilde{K} \leftarrow K[X_1]/\langle \overline{m}_{\vartheta_1}(X_1) \rangle_{K[X_1]}$
{Abbildung φ: Reduziere $\mathfrak{c}$ modulo $\overline{m}_{\vartheta_1}(X_1)$}
$\mathfrak{b} \leftarrow \mathfrak{c} \mod \overline{m}_{\vartheta_1}(X_1)$
{Rekursiver Aufruf}
$M \leftarrow$ **call** PrimDec$(\tilde{K}, n-1, \mathfrak{b})$
M ist von der Form: $M = \{\underbrace{\{p_{1,1}, \ldots, p_{1,v_1}\}}_{\mathfrak{p}_1}, \ldots, \underbrace{\{p_{u,1}, \ldots, p_{u,v_u}\}}_{\mathfrak{p}_u}\}$
alle $p_{\mu,\nu} \in \tilde{K}[X_2, \ldots, X_n]$
{Bilde Urbilder der $\mathfrak{p}_k$ unter φ} $\tilde{\mathfrak{p}}_k \leftarrow \mathfrak{p}_k \cup \{m_{\vartheta_1}(X_1)\}$
Return $\{\tilde{\mathfrak{p}}_1, \ldots, \tilde{\mathfrak{p}}_u\}$
end if

Für eine detaillierte Beschreibung der Reduktion eines Ideals $\mathfrak{a}$ modulo einem Polynom siehe [BW93, Chapter 5.1].

3.3 Der verallgemeinerte Kummersche Zerlegungssatz

Nachdem in den ersten beiden Abschnitten dieses Kapitels die Handwerkszeuge für das Berechnen der Primideale in einem Faktorring eines multivariaten Polynomringes über einem endlichen Körper bereitgestellt wurden, wird jetzt die Theorie aufbereitet. Der Kummersche Zerlegungssatz (1.35) wird in Teilen erweitert auf bestimmte Körperkomposita. Der hier gegebene Beweis orientiert sich an [PZ97, Chapter 6, (2.27)].

In diesem Abschnitt wird die verallgemeinerte Gleichungsordnung $\mathbb{Z}[\vartheta_1, \vartheta_2]$ ebenfalls als Gleichungsordnung bezeichnet, obwohl sie eigentlich nicht durch

eine Gleichung definiert ist.

Satz 3.26. *Sei $\mathcal{K} := \mathbb{Q}[\vartheta_1, \vartheta_2]$ ein Kompositum von zwei Zahlkörpern $\mathcal{F}_1 := \mathbb{Q}[\vartheta_1]$, $\mathcal{F}_2 := \mathbb{Q}[\vartheta_2]$, welche gegeben sind durch die Minimalpolynome*

$$m_{\vartheta_1}(X_1) \in \mathbb{Z}[X_1] \quad \text{und} \quad m_{\vartheta_2}(X_2) \in \mathbb{Z}[X_2].$$

Sei $\deg(\mathcal{F}_1) =: n$, $\deg(\mathcal{F}_2) =: m$ und $\deg(\mathcal{K}) = nm$. Die Gleichungsordnung $\mathbb{Z}[\vartheta_1, \vartheta_2]$ von $\mathcal{K}$ hat dann die Form

$$\mathbb{Z}[\vartheta_1, \vartheta_2] = \left\{ \sum_{i=0}^{n-1} \sum_{j=0}^{m-1} a_{i,j} \vartheta_1^i \vartheta_2^j \mid a_{i,j} \in \mathbb{Z} \right\}.$$

Sei $p \in \mathbb{P}_\mathbb{Z}$ eine Primzahl. Seien $\tilde{\mathfrak{p}}_1, \ldots, \tilde{\mathfrak{p}}_r$ die endlich vielen Primideale des Faktorringes

$$\mathbb{F}_p[X_1, X_2] / \underbrace{\langle \overline{m}_{\vartheta_1}(X_1, X_2), \overline{m}_{\vartheta_2}(X_1, X_2) \rangle_{\mathbb{F}_p[X_1, X_2]}}_{=: \mathfrak{c}},$$

gegeben durch ein Repräsentantensystem von Restklassen

$$\tilde{\mathfrak{p}}_i = \langle \overline{h}_{i,1}(X_1, X_2), \ldots, \overline{h}_{i,\mu_i}(X_1, X_2) \rangle_{\mathbb{F}_p[X_1, X_2]}, \quad i \in \mathbb{N}_r$$

mit

$$\overline{h}_{i,j}(X_1, X_2) = h_{i,j}(X_1, X_2) + \mathfrak{c} \in \mathbb{F}_p[X_1, X_2]/\mathfrak{c}, \quad i \in \mathbb{N}_r, j \in \mathbb{N}_{\mu_i}.$$

Dann sind die Primideale, welche in $\mathbb{Z}[\vartheta_1, \vartheta_2]$ über $\langle p \rangle_\mathbb{Z}$ liegen von der Form

$$\mathfrak{p}_i = \langle p \rangle_{\mathbb{Z}[\vartheta_1, \vartheta_2]} + \langle h_{i,1}(\vartheta_1, \vartheta_2), \ldots, h_{i,\mu_i}(\vartheta_1, \vartheta_2) \rangle_{\mathbb{Z}[\vartheta_1, \vartheta_2]}, \quad i \in \mathbb{N}_r.$$

Die $h_{i,j}(X_1, X_2) \in \mathbb{Z}[X_1, X_2]$ sind dabei normierte Urbilder der $\overline{h}_{i,j}(X_1, X_2)$.

Beweis. Bemerkt sei, dass die $m_{\vartheta_i}(X_i) \in \mathbb{Z}[X_i]$ für $i \in \mathbb{N}_2$ auch Elemente von $\mathbb{Z}[X_1, X_2]$ sind.

Die Gleichungsordnung $\mathbb{Z}[\vartheta_1, \vartheta_2]$ hat die angegebene Form, weil $\mathbb{Z}[\vartheta_1, \vartheta_2]$ das Bild von $\mathbb{Z}[X_1, X_2]$ unter dem Einsetzungshomomorphismus

$$\begin{aligned} \xi_{\vartheta_1, \vartheta_2} \quad : \quad & \mathbb{Z}[X_1, X_2] \to \mathbb{C} \\ & \sum_{i=0}^{r} a_i X_1^{\nu_{1,i}} X_2^{\nu_{2,i}} \mapsto \sum_{i=0}^{r} a_i \vartheta_1^{\nu_{1,i}} \vartheta_2^{\nu_{2,i}} \end{aligned}$$

ist. Die zweite Behauptung zeigt man in zwei Schritten:

(1) Zeige, dass es genügt, die Primideale von $\mathbb{Z}[\vartheta_1,\vartheta_2]/\langle p\rangle_{\mathbb{Z}[\vartheta_1,\vartheta_2]}$ zu bestimmen.

(2) Zeige den Isomorphismus

$$\mathbb{Z}[\vartheta_1,\vartheta_2]/\langle p\rangle_{\mathbb{Z}[\vartheta_1,\vartheta_2]} \cong \mathbb{F}_p[X_1,X_2]/\mathfrak{c}.$$

Punkt (1) folgt mit (3.21), wenn man für f die kanonische Projektion

$$\begin{array}{rcl} \pi & : & \mathbb{Z}[\vartheta_1,\vartheta_2] \to \mathbb{Z}[\vartheta_1,\vartheta_2]/\langle p\rangle_{\mathbb{Z}[\vartheta_1,\vartheta_2]} \\ & & \mathfrak{a} \mapsto \mathfrak{a} + \langle p\rangle_{\mathbb{Z}[\vartheta_1,\vartheta_2]} \end{array}$$

einsetzt.

Für den Beweis von (2) betrachte die Abbildung

$$\begin{array}{rcl} \Phi & : & \mathbb{Z}[\vartheta_1,\vartheta_2] \to \mathbb{F}_p[X_1,X_2]/\mathfrak{c} \\ & & h(\vartheta_1,\vartheta_2) \mapsto \overline{h}(X_1,X_2) + \mathfrak{c}. \end{array}$$

Zeigt man, dass Φ ein Ringepimorphismus ist, also wohldefiniert, homomorph und surjektiv, und dass $\ker(\Phi) = p\mathbb{Z}[\vartheta_1,\vartheta_2]$ gilt, folgt die Behauptung (2) mit dem Isomorphiesatz für Ringe [Bos96, 2.3, Korollar 5]. Dann folgt auch, dass $\mathbb{F}_p[X_1,X_2]/\mathfrak{c}$ nur endlich viele Primideale hat, denn $\mathbb{Z}[\vartheta_1,\vartheta_2]/\langle p\rangle_{\mathbb{Z}[\vartheta_1,\vartheta_2]}$ ist als Faktorring einer Ordnung endlich und kann damit nur endlich viele Primideale haben.

Seien $h_1(X_1,X_2), h_2(X_1,X_2) \in \mathbb{Z}[X_1,X_2]$ mit $h_1(\vartheta_1,\vartheta_2) = h_2(\vartheta_1,\vartheta_2)$. Zu zeigen ist $\Phi(h_1(\vartheta_1,\vartheta_2)) = \Phi(h_2(\vartheta_1,\vartheta_2))$, d. h. sind zwei Urbilder gleich, werden diese auf die gleiche Nebenklasse abgebildet. Betrachte das Polynom

$$h_1(X_1,X_2) - h_2(X_1,X_2) =: h(X_1,X_2),$$

und reduziere h mittels verallgemeinerter Polynomdivision zur Normalform modulo

$$\tilde{\mathfrak{c}} := \langle m_{\vartheta_1}(X_1,X_2), m_{\vartheta_2}(X_1,X_2)\rangle_{\mathbb{Z}[X_1,X_2]}$$

[BW93, Proposition 5.22]. Das ist anwendbar, weil man nur Topreduktionen zulässt und $m_{\vartheta_1}(X_1)$, $m_{\vartheta_2}(X_2)$ als Minimalpolynome vorausgesetzt wurden, also insbesondere normiert sind. Man erhält die Normalform $g(X_1,X_2) \in \mathbb{Z}[X_1,X_2]$ von h modulo $\tilde{\mathfrak{c}}$:

$$\begin{array}{rcl} (\star) \quad h(X_1,X_2) & = & q_1(X_1,X_2)m_{\vartheta_1}(X_1,X_2) \\ & + & q_2(X_1,X_2)m_{\vartheta_2}(X_1,X_2) + g(X_1,X_2), \end{array}$$

und es ist

$$\max\{\mathrm{HT}(q_1(X_1,X_2)m_{\vartheta_1}(X_1,X_2)), \mathrm{HT}(q_2(X_1,X_2)m_{\vartheta_2}(X_1,X_2))\} \leq HT(h(X_1,X_2)).$$

Substitution $(X_1, X_2) \mapsto (\vartheta_1, \vartheta_2)$ liefert

$$\underbrace{h_1(\vartheta_1,\vartheta_2) - h_2(\vartheta_1,\vartheta_2)}_{\substack{=0,\text{ gem.}\\ \text{Voraussetzung}}} = \underbrace{q_1(\vartheta_1,\vartheta_2)m_{\vartheta_1}(\vartheta_1,\vartheta_2)}_{\substack{=0,\ m_{\vartheta_1}(X_1,X_2)\\ \text{ist Mipo von } \vartheta_1}} + \underbrace{q_2(\vartheta_1,\vartheta_2)m_{\vartheta_2}(\vartheta_1,\vartheta_2)}_{\substack{=0,\ m_{\vartheta_2}(X_1,X_2)\\ \text{ist Mipo von } \vartheta_2}} + g(\vartheta_1,\vartheta_2).$$

Damit ist $g(\vartheta_1, \vartheta_2) = 0$.

Gezeigt wird jetzt, dass auch $g(X_1, X_2) = 0$ gilt: Wäre $g(X_1, X_2) \neq 0$, würde dies bedeuten, dass es ein Polynom

$$g(X_1, X_2) = \sum_{\mu=1}^{\chi} a_i X_1^{\nu_{1,\mu}} X_2^{\nu_{2,\mu}} \in \mathbb{Z}[X_1, X_2]$$

mit folgenden Eigenschaften gäbe:

$$\begin{aligned} g(X_1, X_2) &\neq 0 & \nu_{1,1} &< \deg(m_{\vartheta_1}(X_1)) \\ g(\vartheta_1, \vartheta_2) &= 0 & \nu_{2,1} &< \deg(m_{\vartheta_2}(X_2)). \end{aligned}$$

Es muss weiterhin

$$g(X_1, X_2) \in \mathbb{Z}[X_1, X_2]$$

gelten mit

$$g(X_1, X_2) \notin \mathbb{Z}[X_1] \quad \text{und} \quad g(X_1, X_2) \notin \mathbb{Z}[X_2],$$

da man sonst einen Widerspruch zur Minimalpolynomeigenschaft von $m_{\vartheta_1}(X_1)$ und $m_{\vartheta_2}(X_2)$ erhielte.

Das Polynom $g(X_1, X_2)$ ist von der Form

$$g(X_1, X_2) = X_1^{\nu_{1,1}} X_2^{\nu_{2,1}} + \ldots$$

mit

$$\nu_{1,1} < n = \deg(m_{\vartheta_1}(X_1) \quad \text{und} \quad \nu_{2,1} < m = \deg(m_{\vartheta_2}(X_2),$$

denn sonst könnte man in $(\star)$ den Term $g(X_1, X_2)$ noch weiter reduzieren. Sei o. B. d. A. $\nu_{1,1} := n-1$, $\nu_{2,1} := m-1$ und jeder Koeffizient von $g(X_1, X_2)$ ungleich Null. Dann hätte man aber $(n-1)(m-1)$ Elemente gefunden, welche in dem freien $\mathbb{Z}$-Modul $\mathbb{Z}[\vartheta_1, \vartheta_2]$ linear abhängig sind. Widerspruch, da $\mathbb{Z}[\vartheta_1, \vartheta_2]$ Rang nm hat, siehe (1.7).

Wende nun die Restklassenabbildung

$$\begin{aligned} {}^{-} \;:\; & \mathbb{Z}[X_1, X_2] \to (\mathbb{Z}/p\mathbb{Z})[X_1, X_2] \\ & \sum_{i=0}^{r} a_i X_1^{\nu_{1,i}} X_2^{\nu_{2,i}} \mapsto \sum_{i=0}^{r} \overline{a}_i X_1^{\nu_{1,i}} X_2^{\nu_{2,i}} \end{aligned}$$

auf $(\star)$ an:

$$\overline{h}(X_1, X_2) = \overline{q}_1(X_1, X_2)\overline{m}_{\vartheta_1}(X_1, X_2) + \overline{q}_2(X_1, X_2)\overline{m}_{\vartheta_2}(X_1, X_2).$$

Dann gilt

$$\overline{h}_1(X_1, X_2) - \overline{h}_2(X_1, X_2) \in \mathfrak{c},$$

also liegen $\overline{h}_1(X_1, X_2)$ und $\overline{h}_2(X_1, X_2)$ bzgl. $\mathfrak{c}$ in derselben Nebenklasse.

Zeige nun $\ker(\Phi) = p\mathbb{Z}[\vartheta_1, \vartheta_2]$. Sei $h(\vartheta_1, \vartheta_2) \in p\mathbb{Z}[\vartheta_1, \vartheta_2]$. Zu zeigen ist $\overline{h}(X_1, X_2) \in \mathfrak{c}$. Es sei

$$h(\vartheta_1, \vartheta_2) = p \sum_{i=0}^{n} \sum_{j=0}^{m} a_{i,j} \vartheta_1^i \vartheta_2^j.$$

Schreibe

$$g(X_1, X_2) := \sum_{i=0}^{n} \sum_{j=0}^{m} p a_{i,j} X_1^i X_2^j.$$

Es gilt aufgrund Distributivität

$$(h(X_1, X_2) - g(X_1, X_2))\,(\vartheta_1, \vartheta_2) = 0.$$

Dann liegen $h(X_1, X_2)$ und $g(X_1, X_2)$ bzgl. $\tilde{\mathfrak{c}}$ in derselben Nebenklasse:

$$h(X_1, X_2) + \tilde{\mathfrak{c}} = g(X_1, X_2) + \tilde{\mathfrak{c}}, \quad \text{in } \mathbb{Z}[X_1, X_2]/\tilde{\mathfrak{c}},$$

da $\mathbb{Z}[\vartheta_1, \vartheta_2]$ genau dann isomorph zu $\mathbb{Z}[X_1, X_2]/\tilde{\mathfrak{c}}$ ist, wenn $\mathbb{Z}[\vartheta_1, \vartheta_2]$ vom Rang mn ist. Also existieren Polynome

$$q_1(X_1, X_2), q_2(X_1, X_2) \in \mathbb{Z}[X_1, X_2]$$

mit

$$\begin{aligned} h(X_1, X_2) - g(X_1, X_2) &= q_1(X_1, X_2) m_{\vartheta_1}(X_1, X_2) \\ &+ q_2(X_1, X_2) m_{\vartheta_2}(X_1, X_2). \end{aligned}$$

(Wegen $h(X_1, X_2) - g(X_1, X_2) \in \tilde{\mathfrak{c}}$.) Reduktion modulo p liefert

$$\begin{aligned} \overline{h}(X_1, X_2) - 0 &= \overline{q}_1(X_1, X_2)\overline{m}_{\vartheta_1}(X_1, X_2) \\ &+ \overline{q}_2(X_1, X_2)\overline{m}_{\vartheta_2}(X_1, X_2). \end{aligned}$$

Also

$$\overline{h}(X_1, X_2) \in \mathfrak{c}.$$

Für die Richtung $\ker(\Phi) \subseteq p\mathbb{Z}[\vartheta_1, \vartheta_2]$ betrachte $h(\vartheta_1, \vartheta_2) \in \mathbb{Z}[\vartheta_1, \vartheta_2]$ mit $\Phi(h(\vartheta_1, \vartheta_2)) = 0$. Zu zeigen ist $h(\vartheta_1, \vartheta_2) \in p\mathbb{Z}[\vartheta_1, \vartheta_2]$.

Es gilt

$$\Phi(h(\vartheta_1, \vartheta_2)) = 0,$$

also

$$\overline{h}(X_1, X_2) \in \mathfrak{c}.$$

Es existieren $\overline{q}_1(X_1, X_2), \overline{q}_2(X_1, X_2) \in \mathbb{F}_p[X_1, X_2]$ mit

$$\overline{h}(X_1, X_2) = \overline{q}_1(X_1, X_2)\overline{m}_{\vartheta_1}(X_1, X_2) + \overline{q}_2(X_1, X_2)\overline{m}_{\vartheta_2}(X_1, X_2).$$

[BW93, Proposition 5.22] garantiert die Existenz eines $r(X_1, X_2) \in p\mathbb{Z}[X_1, X_2]$ mit

$$h(X_1, X_2) = q_1(X_1, X_2)m_{\vartheta_1}(X_1, X_2) + q_2(X_1, X_2)m_{\vartheta_2}(X_1, X_2) + r(X_1, X_2).$$

Substitution $(X_1, X_2) \mapsto (\vartheta_1, \vartheta_2)$ liefert

$$h(\vartheta_1, \vartheta_2) = r(\vartheta_1, \vartheta_2),$$

aufgrund der Minimalpolynomeigenschaft der $m_{\vartheta_1}(X_1, X_2), m_{\vartheta_2}(X_1, X_2)$, also $h(\vartheta_1, \vartheta_2) \in p\mathbb{Z}[\vartheta_1, \vartheta_2]$.

Der Nachweis der Surjektivität von Φ ist trivial. Die Homomorphie von Φ folgt mit der Definition der Addition bzw. Multiplikation in einem Faktorring und der Homomorphie der Restklassenabbildung $\bar{}$. □

Der Beweis von (3.26) lässt sich ohne Probleme auf Komposita erweitern, welche aus mehr als zwei Zahlkörpern bestehen. Das führt auf das Hauptergebnis dieses Abschnittes:

Korollar 3.27. ***Der verallgemeinerte Zerlegungssatz***
Sei $\mathcal{K} := \mathbb{Q}[\underline{\vartheta}] := \mathbb{Q}[\vartheta_1, \ldots, \vartheta_n]$ ein Kompositum von Zahlkörpern $\mathcal{F}_i := \mathbb{Q}[\vartheta_i]$, $i \in \mathbb{N}_n$. Die $\mathcal{F}_i$ seien gegeben durch Minimalpolynome $m_{\vartheta_i}(X_i) \in \mathbb{Z}[X_i]$. Sei

$$\deg(\mathcal{K}) = \prod_{i=1}^{n} \deg(m_{\vartheta_i}(X_i)).$$

Sei $p \in \mathbb{P}_{\mathbb{Z}}$ eine Primzahl. Seien $\tilde{\mathfrak{p}}_1, \ldots, \tilde{\mathfrak{p}}_r$ die Primideale des Faktorringes

$$\mathbb{F}_p[\underline{X}]/\underbrace{\langle \overline{m}_{\vartheta_1}(\underline{X}), \ldots, \overline{m}_{\vartheta_n}(\underline{X})\rangle_{\mathbb{F}_p[\underline{X}]}}_{=:\mathfrak{c}},$$

gegeben durch ein Repräsentantensystem von Restklassen

$$\tilde{\mathfrak{p}}_i = \langle \overline{h}_{i,1}(\underline{X}), \ldots, \overline{h}_{i,\mu_i}(\underline{X}) \rangle_{\mathbb{F}_p[\underline{X}]/\mathfrak{c}}, \quad i \in \mathbb{N}_r$$

mit

$$\overline{h}_{i,j}(\underline{X}) = h_{i,j}(\underline{X}) + \mathfrak{c} \in \mathbb{F}_p[\underline{X}]/\mathfrak{c}, \quad i \in \mathbb{N}_r,\ j \in \mathbb{N}_{\mu_i}.$$

Dann sind die Primideale, welche in $\mathbb{Z}[\underline{\vartheta}]$ über $\langle p \rangle_{\mathbb{Z}}$ liegen, von der Form

$$\mathfrak{p}_i = \langle p \rangle_{\mathbb{Z}[\underline{\vartheta}]} + \langle h_{i,1}(\underline{\vartheta}), \ldots, h_{i,\mu_i}(\underline{\vartheta}) \rangle_{\mathbb{Z}[\underline{\vartheta}]}, \quad i \in \mathbb{N}_r.$$

Die $h_{i,j}(\underline{X}) \in \mathbb{Z}[\underline{X}]$ sind dabei normierte Urbilder der $\overline{h}_{i,j}(\underline{X})$.

Lässt man in (3.26) die Voraussetzung fallen, dass der Grad des Kompositums $\deg(\mathcal{K})$ nicht das Produkt der Grade der Zahlkörper $\mathbb{Q}[\vartheta_1]$ und $\mathbb{Q}[\vartheta_2]$ ist, ist der Satz falsch:

Bemerkung 3.28. *Sei $m_{\vartheta_1}(X_1) = X_1^4 - 2$ und $m_{\vartheta_2}(X_2) = X_2^2 - 2$, dann ist die Abbildung*

$$\begin{array}{rcl} \Phi & : & \mathbb{Z}[\vartheta_1, \vartheta_2] \to \mathbb{F}_2[X_1, X_2]/\mathfrak{c} \\ & & h(\vartheta_1, \vartheta_2) \mapsto \overline{h}(X_1, X_2) + \mathfrak{c} \end{array}$$

nicht wohldefiniert. Es ist

$$\mathfrak{c} = \langle X_1^4, X_2^2 \rangle_{\mathbb{F}_2[X_1, X_2]}.$$

Die Polynome

$$h_1(X_1, X_2) = X_1^2 \quad \textit{und} \quad h_2(X_1, X_2) = X_2$$

haben nach Einsetzung von $(\vartheta_1, \vartheta_2) = (\sqrt[4]{2}, \sqrt{2})$ den Wert

$$h_1(\vartheta_1, \vartheta_2) = \sqrt{2} = h_2(\vartheta_1, \vartheta_2).$$

Es gilt aber

$$\Phi(h_1(X_1, X_2)) = X_1^2 + \mathfrak{c} \quad \textit{und} \quad \Phi(h_2(X_1, X_2)) = X_2 + \mathfrak{c}.$$

Das Urbild $\sqrt{2}$ wird also auf mindestens zwei verschiedene Nebenklassen abgebildet.

Man hat jetzt die Theorie zur Verfügung, um in einem Körperkompositum $\mathcal{K} = \mathbb{Q}[\underline{\vartheta}]$, welches den Voraussetzung aus (3.27) genügt, alle Primideale der Gleichungsordnung zu bestimmen, welche über einer Primzahl p liegen.

Ist das zu zerlegende, hochgehobene Primideal $\langle p \rangle_{\mathbb{Z}[\underline{\vartheta}]}$ comaximal zum Führer von $\mathbb{Z}[\underline{\vartheta}]$, siehe (1.32), kann man auch eine Angabe machen, von welchen Primidealen der Maximalordnung das Ideal $\langle p \rangle_{\mathfrak{o}_\mathcal{K}}$ geteilt wird:

Lemma 3.29. *Sei $\mathcal{K} := \mathbb{Q}[\underline{\vartheta}]$ ein Körperkompositum mit Maximalordnung $\mathfrak{o}_\mathcal{K}$ und Gleichungsordnung $\mathbb{Z}[\underline{\vartheta}]$. Definiere*

$$\begin{aligned} \mathcal{D}_{\mathbb{Z}[\underline{\vartheta}]} &:= \{\mathfrak{a} \in \mathcal{I}_{\mathbb{Z}[\underline{\vartheta}]} \mid \mathfrak{a} + \mathcal{F}(\mathbb{Z}[\underline{\vartheta}]) = \mathbb{Z}[\underline{\vartheta}]\} \\ \mathcal{D}_{\mathfrak{o}_\mathcal{K}} &:= \{\mathfrak{a} \in \mathcal{I}_{\mathfrak{o}_\mathcal{K}} \mid \mathfrak{a} + \mathcal{F}(\mathbb{Z}[\underline{\vartheta}]) = \mathfrak{o}_\mathcal{K}\} \end{aligned}$$

Es gilt

(1) Die Mengen $\mathcal{D}_{\mathbb{Z}[\underline{\vartheta}]}$ und $\mathcal{D}_{\mathfrak{o}_\mathcal{K}}$ sind multiplikative Monoide mit Kürzungsregeln.

(2) Die Abbildung

$$\begin{aligned} \kappa \;:\; & \mathcal{D}_{\mathbb{Z}[\underline{\vartheta}]} \to \mathcal{D}_{\mathfrak{o}_\mathcal{K}} \\ & \mathfrak{a} \mapsto \langle \mathfrak{a} \rangle_{\mathfrak{o}_\mathcal{K}} \end{aligned}$$

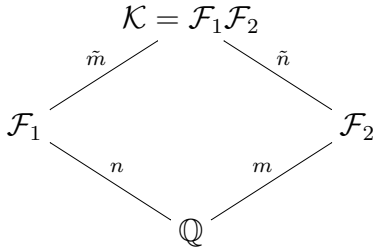
ist ein Idealmonoidisomorphismus mit Umkehrabbildung $\kappa^{-1}(\mathfrak{b}) = \mathfrak{b} \cap \mathbb{Z}[\underline{\vartheta}]$.

(3) Für alle $\mathfrak{a} \in \mathcal{D}_{\mathfrak{o}_\mathcal{K}}$ gilt $\mathfrak{o}_\mathcal{K}/\mathfrak{a} \cong \mathbb{Z}[\underline{\vartheta}]/(\mathfrak{a} \cap \mathbb{Z}[\underline{\vartheta}])$.

Beweis. [PZ97, Chapter 6, (2.24), (2.26)] kann übernommen werden, da die dort betrachteten Ordnungen nicht notwendig monogen sein müssen. □

3.4 Primidealfaktorisierung in der Gleichungsordnung

Bemerkung 3.30. ***Bezeichnungen***
Für den Rest dieses Kapitels gelten folgende Bezeichnungen, es sein denn, es wird ausdrücklich etwas Anderes gesagt: Seien $\mathcal{F}_1 := \mathbb{Q}[\vartheta_1]$, $\mathcal{F}_2 := \mathbb{Q}[\vartheta_2]$ Zahlkörper und $\mathcal{K} := \mathcal{F}_1\mathcal{F}_2$ das Kompositum. Sei $n := \deg(\mathcal{F}_1)$, $m := \deg(\mathcal{F}_2)$ und $s := \deg(\mathcal{K})$. Die Relativgrade seien $\tilde{m} := [\mathcal{K} : \mathcal{F}_1]$ und $\tilde{n} := [\mathcal{K} : \mathcal{F}_2]$.



Sei $p \in \mathbb{P}_\mathbb{Z}$ eine Primzahl und $\mathbb{Z}[\vartheta_1, \vartheta_2]$ die verallgemeinerte Gleichungsordnung. Wird ein Verzweigungsindex mit $\tilde{e}(\mathfrak{p}|\langle p \rangle)$ bezeichnet, so ist $\mathfrak{p}$ ein Primideal der verallgemeinerten Gleichungsordnung und nicht der Maximalordnung, analog für den Trägheitsgrad.

Die Komposita $\mathcal{K}$, auf die (3.26) anwendbar ist, bekommen einen besonderen Namen:

Definition 3.31. *Seien die Bezeichnungen wie in (3.30). Gilt* $\deg(\mathcal{K}) = nm$, *nennt man* $\mathcal{K}$ ***Kompositum vom vollen Grad****. Ein Kompositum, welches nicht notwendig vollen Grad hat, nennt man* ***beliebiges Kompositum****.*

Mit den ersten 3 Abschnitten dieses Kapitels hat man die Technik und Theorie zur Verfügung, um für ein Kompositum vom vollen Grad $\mathcal{K}$ und eine Primzahl $p \in \mathbb{P}_{\mathbb{Z}}$ alle Primideale zu bestimmen, welche in der Gleichungsordnung $\mathbb{Z}[\vartheta_1, \vartheta_2]$ über p liegen. Ist p kein Indexteiler, kann man auch die Primideale der Maximalordnung bestimmen, welche über p liegen. Dieser Abschnitt stellt die Techniken bereit, um die Primidealfaktorisierung in der Gleichungsordnung zu berechnen.

Bemerkung 3.32. *Folgende Informationen werden für die Berechnung der Primidealfaktorisierung in der Gleichungsordnung als bekannt vorausgesetzt:*

- *Ein beliebiges Körperkompositum* $\mathcal{K}$*, gegeben durch zwei Minimalpolynome* $m_{\vartheta_1}(X_1) \in \mathbb{Z}[X_1]$, $m_{\vartheta_2}(X_2) \in \mathbb{Z}[X_2]$.
- *Eine zu zerlegende Primzahl* $p \in \mathbb{P}_{\mathbb{Z}}$.
- *Die Primidealfaktorisierungen von* p *in* $\mathbb{Q}[\vartheta_1]$ *und* $\mathbb{Q}[\vartheta_2]$.
- *Bekannt ist, ob* $\mathcal{F}_1$ *bzw.* $\mathcal{F}_2$ *normal sind.*
- *Die Maximalordnungen* $\mathfrak{o}_{\mathcal{F}_1}$ *und* $\mathfrak{o}_{\mathcal{F}_2}$.

Die Maximalordnung des Kompositums $\mathfrak{o}_{\mathcal{K}}$ *und der Grad sind nicht notwendig bekannt.*

Man hat 3 Aufgaben zu lösen:

(1) Überprüfung, ob $\mathcal{K}$ vom vollen Grad ist, d. h. ob (3.26) anwendbar ist.

(2) Berechnung der Primideale $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$, welche in $\mathbb{Z}[\vartheta_1, \vartheta_2]$ über einer gegebenen Primzahl p liegen.

(3) Berechnung der Verzweigungsindices $\tilde{e}(\mathfrak{p}_i|\langle p\rangle)$ und Trägheitsgrade $\tilde{f}(\mathfrak{p}_i|\langle p\rangle)$.

Ein erster Schritt zur Lösung von (1) ist der **Diskriminantentest** (siehe auch (2.16)):

Satz 3.33. *Seien $\mathcal{F}_1$, $\mathcal{F}_2$ Zahlkörper vom Grad n, m mit teilerfremden Diskriminanten. Sei $\mathcal{K} := \mathcal{F}_1\mathcal{F}_2$ das Kompositum. Dann gilt $[\mathcal{K} : \mathbb{Q}] = nm$ und*

$$\operatorname{disc}(\mathcal{K}) = \operatorname{disc}(\mathcal{F}_1)^m \operatorname{disc}(\mathcal{F}_2)^n.$$

Ist $\{\omega_1, \ldots, \omega_n\}$ eine Ganzheitsbasis von $\mathcal{F}_1$ und $\{\tau_1, \ldots, \tau_m\}$ eine Ganzheitsbasis von $\mathcal{F}_2$, dann ist die Menge

$$\{\omega_i\tau_j \mid i \in \mathbb{N}_n, j \in \mathbb{N}_m\}$$

eine Ganzheitsbasis von $\mathcal{K}$.

[Nar89, 4, §2, Theorem 4.9] Man kennt sogar die Maximalordnung des Kompositums und kann damit Indexteiler leicht bestimmen, siehe (3.5). Liefert der Diskriminantentest gemeinsame Teiler von $\operatorname{disc}(\mathcal{F}_1)$ und $\operatorname{disc}(\mathcal{F}_2)$, können $\mathcal{F}_1$ und $\mathcal{F}_2$ gemeinsame Teilkörper haben:

Bemerkung 3.34. *Im Falle, dass der Diskriminantentest negativ ist, hat man zwei Möglichkeiten den Grad* $\deg(\mathcal{K})$ *zu bestimmen:*

(1) Man faktorisiert das Minimalpolynom $m_{\vartheta_2}(X_2)$ in dem Polynomring $\mathfrak{o}_{\mathcal{F}_1}[X_2]$ über der Maximalordnung von $\mathcal{F}_1$. Man betrachtet also die Relativerweiterung $\mathcal{F}_2/\mathcal{F}_1$ und wählt als Relativgrad $\tilde{m}$ den Grad des Faktors aus, von dem ϑ_2 Nullstelle ist. (Das ist die Idee des Beweises in [Nar89, 4, §2, Theorem 4.9], vergleiche mit (2.16).)

(2) Man wendet (2.14) (2) oder (2.14) (3), bzw. die Algorithmen AlgFieker oder AlgFiekerSafe an.

In der Praxis wird man diese Verfahren weiter verfeinern, zum Beispiel kann man sich den Diskriminantentest sparen, wenn n und m Primzahlen sind, da dann $\mathcal{F}_1$ und $\mathcal{F}_2$ überhaupt keine Teilkörper haben (mit dem Gradsatz).

Ergibt sich aus (3.34) (1) und (2), dass $\mathcal{K}$ vom vollen Grad ist, hat die Gleichungsordnung die Form:

$$\mathbb{Z}[\vartheta_1, \vartheta_2] = \left\{ \sum_{i=0}^{n-1} \sum_{j=0}^{\tilde{m}-1} a_{i,j}\vartheta_1^i\vartheta_2^j \mid a_{i,j} \in \mathbb{Z} \right\},$$

und

$$\left\{\vartheta_1^i\vartheta_2^j \mid i \in \mathbb{N}_{n-1}^0,\ j \in \mathbb{N}_{\tilde{m}-1}^0\right\}$$

ist eine $\mathbb{Q}$-Basis von $\mathcal{K}$. Dann ist (3.26) anwendbar und mit dem Algorithmus AlgPrimDec berechnet man im zweiten Schritt die Primideale $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$ über p in $\mathbb{Z}[\vartheta_1, \vartheta_2]$. Diese haben die Form

$$\mathfrak{p}_i = \langle f_{i,1}(\vartheta_1, \vartheta_2), \ldots, f_{i,m_i}(\vartheta_1, \vartheta_2), p\rangle_{\mathbb{Z}[\vartheta_1,\vartheta_2]}, \quad f_{i,j} \in \mathbb{Z}[X_1, X_2].$$

Das Berechnen der Verzweigungsindices und Trägheitsgrade im univariaten Fall kann nicht ohne Weiteres auf den Kompositafall übertragen werden, da im Beweis zu [PZ97, Chapter 6, (2.27)] die Verzweigungsindices und Trägheitsgrade hergeleitet werden aus den Exponenten und den Graden der Faktoren der Primpolynomzerlegung des Minimalpolynoms modulo der zu zerlegenden Primzahl. Diese Begriffe stehen im multivariaten Fall nicht zur Verfügung. Eine einfache Möglichkeit zum Berechnen der Verzweigungsindices $\tilde{e}(\mathfrak{p}|\langle p\rangle)$ und Trägheitsgrade $\tilde{f}(\mathfrak{p}|\langle p\rangle)$ ist folgende:

(1) Potenziere jedes $\mathfrak{p}_i$ bis gilt $p \notin \mathfrak{p}_i^t$, $t \in \mathbb{N}$, dann ist $\tilde{e}(\mathfrak{p}_i|\langle p\rangle) = t - 1$.

(2) Zur Berechnung der Trägheitsgrade betrachte die Idealnorm eines $\mathfrak{p}_i$ in der Gleichungsordnung

$$\mathrm{N}(\mathfrak{p}_i) = \#\mathbb{Z}[\vartheta_1, \vartheta_2]/\mathfrak{p}_i = p^{f(\mathfrak{p}_i|p)}$$

in Verbindung mit

$$|\det(M)| = \#\mathbb{Z}[\vartheta_1, \vartheta_2]/\mathfrak{p}_i.$$

M ist die Hermite-Normalform einer Transformationsmatrix von $\mathfrak{p}_i$ bzgl. der Basis $\{\vartheta_1^i\vartheta_2^j \mid i \in \mathbb{N}_{n-1}^0,\ j \in \mathbb{N}_{m-1}^0\}$, siehe (A.8). Man erhält:

$$\tilde{f}(\mathfrak{p}_i|\langle p\rangle) = \frac{\ln(|\det(M)|)}{\ln(p)}.$$

Man ist bis jetzt in der Lage, die komplette Primidealfaktorisierung für eine Primzahl p in der Gleichungsordnung für ein Körperkompositum vom vollen Grad anzugeben. Der nächste Schritt ist, zu versuchen, Erkenntnisse über das Zerlegungsverhalten von p in der Maximalordnung $\mathfrak{o}_\mathcal{K}$ zu erlangen. Da der Idealmonoidisomorphismus κ aus (3.29) nicht für beliebige Ideale der Gleichungsordnung definiert ist, muss man die Primzahlen p bestimmen, für die gilt, dass κ auf alle in der Gleichungsordnung über p liegenden Ideale angewandt werden kann. Dieses Problem wird im nächsten Abschnitt behandelt, es werden für Komposita die Indexteiler bestimmt.

3.5 Indexteilerbestimmung in Komposita

Seien für diesen Abschnitt die Bezeichnungen wie in (3.4), $\mathcal{K}$ sei beliebiges Kompositum.

Ist der Diskriminantentest (3.33) positiv, kennt man sofort den Grad von $\mathcal{K}$ und die Maximalordnung. Die Bedingung „teilerfremde Diskriminanten“ ist aber für die Eigenschaft von $\mathcal{K}$, vollen Grad zu haben, nur hinreichend und nicht notwendig. Ein einfaches Gegenbeispiel ist $\mathcal{F}_1 := \mathbb{Q}[\sqrt{5}]$ und

$\mathcal{F}_2 := \mathbb{Q}[\sqrt{15}]$. Es gibt also Komposita $\mathcal{K}$ vom vollen Grad, für die die Diskriminanten $\operatorname{disc}(\mathcal{F}_1)$ und $\operatorname{disc}(\mathcal{F}_2)$ gemeinsame Teiler haben. Dann kann man auch keine genauen Aussagen über die Maximalordnung $\mathfrak{o}_\mathcal{K}$ machen. Will man in $\mathcal{K}$ die Primidealfaktorisierung berechnen, wird man sich daher (leider) mit Komposita beschäftigen müssen, für die die Maximalordnung nicht bekannt ist. Deshalb werden in diesem Kapitel ab jetzt zwei Strategien verfolgt: Zum einen werden Komposita betrachtet, für die die Maximalordnung nicht bekannt ist. Der andere Fall behandelt Komposita, für die die Maximalordnung als bekannt vorausgesetzt wird. Die Verfahren dieses Abschnittes zur Bestimmung von Indexteilern sind unabhängig davon, ob $\mathcal{K}$ vollen Grad hat, deshalb werden alle Verfahren für beliebige Komposita diskutiert. Es wird lediglich unterschieden, ob die Maximalordnung bekannt ist, oder nicht.

Im Falle teilerfremder Diskriminanten ist das Bestimmen der Indexteiler einfach:

Bemerkung 3.35. *Es gelte*

$$\gcd(\operatorname{disc}(\mathcal{F}_1), \operatorname{disc}(F_2)) = 1.$$

Dann kann man mit

$$\operatorname{disc}(\mathcal{K}) = \operatorname{disc}(\mathcal{F}_1)^m \operatorname{disc}(\mathcal{F}_2)^n,$$

siehe (3.33), und

$$\operatorname{disc}(\mathbb{Z}[\vartheta_1, \vartheta_2]) = \operatorname{disc}(\mathbb{Z}[\vartheta_1])^m \operatorname{disc}(\mathbb{Z}[\vartheta_2])^n$$

[Ist01, 3, Gleichung (3)] die Indexteiler einfach bestimmen: Man benutzt

$$[\mathfrak{o}_\mathcal{K} : \mathbb{Z}[\vartheta_1, \vartheta_2] = \sqrt{\frac{\operatorname{disc}(\mathbb{Z}[\vartheta_1, \vartheta_2])}{\operatorname{disc}(\mathfrak{o}_\mathcal{K})}}.$$

Die Maximalordnung ist in diesem Fall mit (3.33) bekannt und $\mathcal{K}$ hat vollen Grad.

Schlägt der Diskriminantentest fehl, hat $\mathcal{K}$ aber trotzdem vollen Grad, kann man nur noch hinreichende Aussagen machen, dass p kein Indexteiler ist, da man die Diskriminante der Maximalordnung nicht kennt. Den ersten Zugang zu diesem Problem liefert folgender Satz:

Satz 3.36. *Seien die Bezeichnungen wie in (3.30). Dann stimmen die Primzahlen, welche* $\operatorname{disc}(\mathcal{K})$ *und* $\operatorname{disc}(\mathcal{F}_1) \cdot \operatorname{disc}(\mathcal{F}_2)$ *teilen, überein.*

[Nar89, 4,§2, Proposition 4.13] Es gilt also nur noch

$$\operatorname{disc}(\mathcal{K}) \leq \operatorname{disc}(\mathcal{F}_1)^m \operatorname{disc}(\mathcal{F}_2)^n,$$

statt Gleichheit. Man kann aber eine genaue Angabe machen, mit welcher Potenz die Primdivisoren von $\operatorname{disc}(\mathcal{F}_1)$ und $\operatorname{disc}(\mathcal{F}_2)$ den Wert $\operatorname{disc}(\mathcal{K})$ teilen:

Satz 3.37. *Seien die Bezeichnungen wie in (3.30), dann gilt*

$$\operatorname{disc}(\mathcal{F}_1)^{\tilde{m}} \mid \operatorname{disc}(\mathcal{K})$$

und

$$\operatorname{disc}(\mathcal{F}_2)^{\tilde{n}} \mid \operatorname{disc}(\mathcal{K}).$$

Also gilt

$$\gcd\left(\operatorname{disc}(\mathcal{F}_1)^{\tilde{m}}, \operatorname{disc}(\mathcal{F}_2)^{\tilde{n}}\right) \mid \operatorname{disc}(\mathcal{K}).$$

[Nar89, 4, §2, Korollar 2 zu Proposition 4.9] Die Gleichung

$$\operatorname{disc}(\mathbb{Z}[\vartheta_1, \vartheta_2]) = \operatorname{disc}(\mathbb{Z}[\vartheta_1])^{\tilde{m}} \operatorname{disc}(\mathbb{Z}[\vartheta_2])^{\tilde{n}},$$

gilt ebenfalls nicht mehr. Betrachte als Gegenbeispiel $\mathcal{F}_1 := \mathcal{F}_2 := \mathbb{Q}[\sqrt{2}]$.

Mit folgendem Verfahren ist man dennoch in der Lage, den genauen Wert der Diskriminante der Ordnung $\mathbb{Z}[\vartheta_1, \vartheta_2]$ zu bestimmen, also den Wert

$$\operatorname{disc}(\{\vartheta_1^{\mu}\vartheta_2^{\nu} \mid \mu \in \mathbb{N}_{n-1}^0,\ \nu \in \mathbb{N}_{\tilde{m}-1}^0\}).$$

Dieses Verfahren ist auch unabhängig davon, ob $\mathcal{K}$ vollen Grad hat oder nicht:

Bemerkung 3.38. ***Berechnung der Diskriminante der Gleichungsordnung für beliebige Komposita***
Für die Diskriminantenabbildung von $\mathcal{K}$ gilt

$$\begin{aligned} \operatorname{disc} \ : \ & \mathcal{K}^s \to \mathbb{Q} \\ & (\alpha_1, \ldots, \alpha_s) \mapsto \det(M), \end{aligned}$$

mit $M := (m_{i,j})_{1 \leq i,j \leq s}$ und $m_{i,j} := \operatorname{Tr}(\alpha_i\alpha_j)$, siehe (1.13). Ist $\beta \in \mathcal{K}$, dann gilt für die Spur von β in $\mathcal{K}$:

$$\operatorname{Tr}_{\mathcal{K}|\mathbb{Q}}(\beta) = \frac{[\mathcal{K} : \mathbb{Q}]}{[\mathbb{Q}[\beta] : \mathbb{Q}]} \left(\operatorname{Tr}_{\mathbb{Q}[\beta]|\mathbb{Q}}(\beta)\right)$$

[Mar77, Chapter 2, Theorem 4']. (Siehe auch den Beweis zu (2.4).) Es ist s durch (3.34) (1) und (2) bekannt.

Man hat daher $\mathrm{Tr}_{\mathbb{Q}[\beta]|\mathbb{Q}}(\beta)$ *zu bestimmen, mit*

$$\beta \in \left\{ \vartheta_1^{\mu}\vartheta_2^{\nu} \mid \mu \in \mathbb{N}_{n-1}^0,\ \nu \in \mathbb{N}_{\tilde{m}-1}^0 \right\}.$$

Die Werte ϑ_1 *und* ϑ_2 *sind ganze algebraische Zahlen, welche man in Minimalpolynomdarstellung beschreiben kann. Diese Darstellung ist unabhängig von dem Zahlkörper, dessen Elemente* ϑ_1 *und* ϑ_2 *sind, siehe (A.1). Man kann mit* ϑ_1 *und* ϑ_2 *Arithmetik betreiben, also insbesondere Multiplikation und Potenzierung. Das führt auf die Minimalpolynomdarstellung von* $\vartheta_1^{\mu}\vartheta_2^{\nu}$ *und damit die Minimalpolynome der Zahlkörper*

$$\left\{ \mathbb{Q}[\vartheta_1^{\mu}\vartheta_2^{\nu}] \mid \mu \in \mathbb{N}_{n-1}^0,\ \nu \in \mathbb{N}_{\tilde{m}-1}^0 \right\}.$$

Es gilt

$$\deg(m_{\vartheta_1^{\mu}\vartheta_2^{\nu}}(X)) \leq \deg(\mathcal{K}), \quad \forall\ \mu, \nu$$

wegen $\vartheta_1^{\mu}\vartheta_2^{\nu} \in \mathcal{K}$.

In $\mathbb{Q}[\vartheta_1^{\mu}\vartheta_2^{\nu}]$ *stimmen das charakteristische und das Minimalpolynom von* $\vartheta_1^{\mu}\vartheta_2^{\nu}$ *überein. Denn das charakteristische Polynom ist eine Potenz des Minimalpolynoms und gelte* $\mathrm{C}_{\vartheta_1^{\mu}\vartheta_2^{\nu}}(X) \neq m_{\vartheta_1^{\mu}\vartheta_2^{\nu}}(X)$, *wäre* $\deg(\mathbb{Q}[\vartheta_1^{\mu}\vartheta_2^{\nu}])$ *echt größer als* $\deg(m_{\vartheta_1^{\mu}\vartheta_2^{\nu}}(X))$ *in* $\mathbb{Q}[\vartheta_1^{\mu}\vartheta_2^{\nu}]$, *was nicht sein kann. An* $\mathrm{C}_{\vartheta_1^{\mu}\vartheta_2^{\nu}}(X)$ *kann man die Spur von* $\vartheta_1^{\mu}\vartheta_2^{\nu}$ *mit (1.12) ablesen.*

Der Wert $[\mathbb{Q}[\vartheta_1^{\mu}\vartheta_2^{\nu}] : \mathbb{Q}]$ *kann ebenfalls über das charakteristische Polynom abgelesen werden.*

Damit hat man alle Werte zur Berechnung von $\mathrm{disc}(\mathbb{Z}[\vartheta_1, \vartheta_2])$ *ermittelt.*

Es liegt bis jetzt der genaue Wert von $\mathrm{disc}(\mathbb{Z}[\vartheta_1, \vartheta_2])$ und eine obere Schranke für $\mathrm{disc}(\mathfrak{o}_{\mathcal{K}})$ vor. Folgende Kriterien sind hinreichend, dass eine Primzahl p kein Indexteiler in $\mathcal{K}$ ist:

Lemma 3.39. *Seien die Voraussetzungen wie in (3.38), setze*

$$\lambda := \gcd\left(\mathrm{disc}(\mathcal{F}_1)^{\tilde{m}}, \mathrm{disc}(\mathcal{F}_2)^{\tilde{n}}\right).$$

Die Zahl p *ist kein Indexteiler, wenn mindestens einer der folgenden Punkte erfüllt ist:*

(1) $p \nmid \mathrm{disc}(\mathbb{Z}[\vartheta_1, \vartheta_2])$.

(2) $p \mid \mathrm{disc}(\mathbb{Z}[\vartheta_1, \vartheta_2])$ *und* $p^2 \nmid \mathrm{disc}(\mathbb{Z}[\vartheta_1, \vartheta_2])$.

(3) $p^2 \mid \mathrm{disc}(\mathbb{Z}[\vartheta_1, \vartheta_2])$, $p^3 \nmid \mathrm{disc}(\mathbb{Z}[\vartheta_1, \vartheta_2])$ *und* $p \mid \lambda$.

(4) $p^q \mid \mathrm{disc}(\mathbb{Z}[\vartheta_1, \vartheta_2])$ *und* $p^q \mid \lambda$, *für ein* $q \in \mathbb{N}$.

Beweis. Das Lemma folgt mit

$$[\mathfrak{o}_\mathcal{K} : \mathbb{Z}[\vartheta_1, \vartheta_2]]^2 = \frac{\operatorname{disc}(\mathbb{Z}[\vartheta_1, \vartheta_2])}{\operatorname{disc}(\mathfrak{o}_\mathcal{K})}$$

und der Tatsache, dass die linke Seite nur Quadrate enthält. □

Probleme bereiten also die Primzahlen p, welche $\operatorname{disc}(\mathbb{Z}[\vartheta_1, \vartheta_2])$ teilen, auf die aber keine der Punkte (2), (3) oder (4) aus (3.39) anwendbar sind. Für Komposita, deren Maximalordnung nicht bekannt ist, muss man diese „problematischen" Primzahlen wie Indexteiler behandeln.

Jetzt wird der Fall betrachtet, dass für ein beliebiges Kompositum die Maximalordnung bekannt ist:

Bemerkung 3.40. *Ist für ein beliebiges Kompositum $\mathcal{K}$ die Maximalordnung bekannt, so ist die Bestimmung der Indexteiler mit Hilfe von*

$$[\mathfrak{o}_\mathcal{K} : \mathbb{Z}[\vartheta_1, \vartheta_2]] = \sqrt{\frac{\operatorname{disc}(\mathbb{Z}[\vartheta_1, \vartheta_2])}{\operatorname{disc}(\mathfrak{o}_\mathcal{K})}}$$

möglich. Den Wert $\operatorname{disc}(\mathbb{Z}[\vartheta_1, \vartheta_2])$ *kennt man mit (3.38). Der Wert* $\operatorname{disc}(\mathfrak{o}_\mathcal{K})$ *ist berechenbar, da die Maximalordnung als bekannt vorausgesetzt wurde.*

Man hat jetzt die Möglichkeit in einem beliebigen Kompositum, welches aus zwei Zahlkörpern konstruiert ist, Indexteiler zu bestimmen. Ist die Maximalordnung des Kompositums bekannt, kann man alle Indexteiler explizit angeben. Ist die Maximalordnung nicht bekannt, existieren mit (3.38) und (3.39) Verfahren, um die potenziellen Indexteiler weitgehend einzuschränken. Das Übertragen der Indexteilerbestimmung auf Komposita, gebildet aus mehr als zwei Zahlkörper, ist nur bedingt möglich und wird in (3.48) und (3.49) diskutiert.

Zum Schluss dieses Abschnittes wird die Möglichkeit betrachtet, den relativen Dedekindtest zu benutzen, um Indexteiler zu bestimmen:

Bemerkung 3.41. *Im Round-2 Algorithmus wird der Dedekindtest benutzt, um für eine Ordnung $\mathcal{O}$ und eine Primzahl p zu entscheiden, ob $\mathcal{O}$ p-maximal ist [PZ97, Chapter 4, (5.55)], [Coh93, Proposition 6.1.2]. Der Dedekindtest existiert auch für Relativerweiterungen [Fri98, Theorem V.4]. Der relative Dedekindtest prüft, ob in der Relativerweiterung $\mathcal{F}_1/\mathcal{F}_2$ die relative Gleichungsordnung $\mathfrak{o}_{\mathcal{F}_1}[t]$ für ein Primideal $\mathfrak{p} \in \mathbb{P}_{\mathfrak{o}_{\mathcal{F}_1}}$ $\mathfrak{p}$-maximal ist. Man interpretiert nun ein Körperkompositum als Relativerweiterung und erhält folgenden Ansatz:*

(1) Gegeben ist ein Kompositum $\mathcal{K}$ und eine „problematische" Primzahl p. Betrachte die Körpertürme $\mathcal{K}/\mathcal{F}_1/\mathbb{Q}$, $\mathcal{K}/\mathcal{F}_2/\mathbb{Q}$.

(2) Berechne die Zerlegung von p in $\mathcal{F}_1$ und $\mathcal{F}_2$. Seien $\mathfrak{p}_{1,1}, \ldots, \mathfrak{p}_{1,\rho}$ die Primideale, welche in $\mathfrak{o}_{\mathcal{F}_1}$ über p liegen, analog $\mathfrak{p}_{2,1}, \ldots, \mathfrak{p}_{2,\eta}$ für $\mathfrak{o}_{\mathcal{F}_2}$.

(3) Überprüfe mit dem relativen Dedekindtest die relative Gleichungsordnung $\mathfrak{o}_{\mathcal{F}_1}[t]$ auf $\mathfrak{p}_{1,\gamma}$-Maximalität für $\gamma \in \mathbb{N}_{1,\rho}$ und die relative Gleichungsordnung $\mathfrak{o}_{\mathcal{F}_2}[t]$ auf $\mathfrak{p}_{2,\delta}$-Maximalität für $\delta \in \mathbb{N}_{2,\eta}$.

(4) Sind alle Dedekindtests positiv, überprüfe die Beziehungen

$$\mathfrak{o}_{\mathcal{F}_1}[\vartheta_1] \supseteq \mathbb{Z}[\vartheta_1, \vartheta_2] \quad \text{und} \quad \mathfrak{o}_{\mathcal{F}_2}[\vartheta_2] \supseteq \mathbb{Z}[\vartheta_1, \vartheta_2].$$

Ist diese Prüfung positiv, ist die Ordnung $\mathbb{Z}[\vartheta_1, \vartheta_2]$ in dem Kompositum $\mathcal{K}$ p-maximal, also p kein Indexteiler.

(5) Schlägt ein Dedekindtest fehl, zum Beispiel für ein Primideal $\mathfrak{p}_{\psi,\omega}$, so berechne die $\mathfrak{p}_{\psi,\omega}$-maximale Oberordnung der Ordnung $\mathfrak{o}_{\mathcal{F}_\psi}[\vartheta_\psi]$, und fahre mit dem Dedekindtest für diese neue Ordnung fort. Man erhält zwei Ordnungen $\tilde{\mathcal{O}}_1$, $\tilde{\mathcal{O}}_2$, welche $\mathfrak{p}_{1,\gamma}$-maximal sind, bzw. $\mathfrak{p}_{2,\delta}$-maximal, für alle γ, δ.

(6) Sind alle Tests negativ, komponiere die Ordnungen $\tilde{\mathcal{O}}_1$, $\tilde{\mathcal{O}}_2$ zu einer Ordnung $\tilde{\mathcal{O}}$ und stelle $\tilde{\mathcal{O}}$ mit zwei neuen primitiven Elementen $\tilde{\vartheta}_1 \in \mathcal{F}_1$ und $\tilde{\vartheta}_2 \in \mathcal{F}_2$ dar. Die Primzahl p ist dann für diese neue Gleichungsordnung $\mathbb{Z}[\tilde{\vartheta}_1, \tilde{\vartheta}_2]$ kein Indexteiler.

Man wird auf folgende Probleme geführt:

- *Die Tests in (4) sind auf jeden Fall negativ, wenn für einen Körper $\mathcal{F}_1$ oder $\mathcal{F}_2$ die Gleichungsordnung nicht maximal ist.*
- *Das Darstellen der Kompositaordnung $\tilde{\mathcal{O}}$ mit zwei primitiven Elementen $\tilde{\vartheta}_1, \tilde{\vartheta}_2$ ist nicht realisierbar.*

Der relative Dedekindtest ist daher nur sinnvoll anwendbar, wenn für die Zahlkörper $\mathcal{F}_1$ und $\mathcal{F}_2$ die Gleichungsordnung maximal ist. Auch liefert der Test nur ein Kriterium, dass eine Primzahl p kein Indexteiler ist. Es ist mit dem heutigen Stand der Forschung nicht möglich, eine neue Gleichungsordnung $\mathbb{Z}[\hat{\vartheta}_1, \hat{\vartheta}_2]$ zu konstruieren, für die p kein Indexteiler ist.

3.6 Primidealzerlegung in Komposita Teil 1

Seien die Bezeichnungen wie in (3.30) und $\mathcal{K}$ vom vollen Grad. Sei zusätzlich $\omega_1, \ldots, \omega_s \in \mathcal{K}$ eine $\mathbb{Z}$-Basis der Maximalordnung von $\mathcal{K}$.

In diesem Abschnitt werden die Ergebnisse aus den vorherigen Abschnitten dieses Kapitels zu Algorithmen zusammengefasst. Auch wird untersucht, in wieweit man Algorithmen aus (1) auf den Kompositafall retten kann. Wie bereits am Anfang von (3.5) besprochen, wird einmal der Fall betrachtet, dass für ein Körperkompositum $\mathcal{K}$ die Maximalordnung bekannt ist. Andererseits wird der Fall betrachtet, dass die Maximalordnung nicht bekannt ist. Der erste Fall wird in diesem Abschnitt behandelt, der zweite in (3.7).

Mit (3.40) kann man sehr leicht feststellen, ob p Indexteiler ist. Ist p kein Indexteiler, hat man alle Werkzeuge zur Verfügung: Man wendet Algorithmus AlgPrimDec an und ermittelt mit den Techniken aus (3.4) die Primidealfaktorisierung in der Gleichungsordnung $\mathbb{Z}[\vartheta_1, \vartheta_2]$. Anschließend wendet man (3.29) an.

Einige Vereinfachungen beschreibt folgende Bemerkung:

Bemerkung 3.42. *Nützliche Hilfsmittel zum Bestimmen der Verzweigungsindices e und Trägheitsgrade f sind:*

- *Ist p total zerlegt in $\mathcal{F}_1$ und in $\mathcal{F}_2$, dann auch in $\mathcal{K}$. Alle Verzweigungsindices und Trägheitsgrade sind* 1 *[Koc00, Proposition 4.9.2].*
- *Die Menge der Primdivisoren von* $\operatorname{disc}(\mathcal{F}_1)\operatorname{disc}(\mathcal{F}_2)$ *ist gleich der Menge der Primdivisoren von* $\operatorname{disc}(\mathcal{K})$ *[Nar89, 4, §2, Proposition 4.13]. Ist also p unverzweigt in $\mathcal{F}_1$ und $\mathcal{F}_2$, so ist p auch unverzweigt in $\mathcal{K}$ und alle Verzweigungsindices sind* 1.
- *Sind sowohl $\mathcal{F}_1$ als auch $\mathcal{F}_2$ normal, muss man nur einen Trägheitsgrad oder einen Verzweigungsindex kennen. [PZ97, Chapter 6, (2.23)]*

Es gilt allerdings nicht: Sei p total verzweigt in $\mathcal{F}_1$ und in $\mathcal{F}_2$, dann ist p auch total verzweigt in $\mathcal{K}$. Ein Gegenbeispiel ist $\mathcal{F}_1 := \mathbb{Q}[\sqrt{3}]$, $\mathcal{F}_2 := \mathbb{Q}[\sqrt{15}]$, $p := 3$.

Man erhält folgenden Algorithmus:

Algorithmustabelle 7: AlgKumBiv

Input: Kompositum $\mathcal{K}$ vom vollen Grad,
gegeben durch zwei Minimalpolynome

$m_{\vartheta_1}(t), m_{\vartheta_2}(t) \in \mathbb{Z}[t]$
$\{\omega_1, \ldots, \omega_s\}$ $\mathbb{Z}$-Basis von $\mathfrak{o}_\mathcal{K}$
Primzahl p, kein Indexteiler
Output: Menge von Tripeln $\{\mathfrak{p}, e, f\}$ mit $\mathfrak{p} \in \mathbb{P}_{\mathfrak{o}_\mathcal{F}}$ und $\mathfrak{p} \mid \langle p \rangle_{\mathfrak{o}_\mathcal{F}}$,
$e = e(\mathfrak{p}|\langle p \rangle)$, $f = f(\mathfrak{p}|\langle p \rangle)$
begin:
{Rufe Algorithmus AlgPrimDec auf}
$M \leftarrow$ **call** AlgPrimDec$(\mathbb{F}_p, 2, \langle m_{\vartheta_1}(X_1, X_2), m_{\vartheta_2}(X_1, X_2) \rangle)$
{M ist von der Form $M = \{M_1, \ldots, M_t\}$
mit $M_i = \{p_{i,1}(X_1, X_2), \ldots, p_{i,i_t}(X_1, X_2)\}$ }
{Erzeuge die Primideale in der Gleichungsordnung}
$N \leftarrow \emptyset$
for all $i \in \mathbb{N}_t$ **do**
  $\mathfrak{p} \leftarrow \langle p, p_{i,1}(\vartheta_1, \vartheta_2), \ldots, p_{i,i_t}(\vartheta_1, \vartheta_2) \rangle$
  $N \leftarrow N \cup \{\mathfrak{p}_i, e_i, f_i\}$
end for
if p ist total zerlegt in $\mathcal{F}_1$ und $\mathcal{F}_2$ **then**
  $e_i \leftarrow 1$, $f_i \leftarrow 1$ für alle $i \in \mathbb{N}_t$
else
  if p unverzweigt in $\mathcal{F}_1$ und $\mathcal{F}_2$ **then**
    $e_i \leftarrow 1$ für alle $i \in \mathbb{N}_t$
    easy1 $\leftarrow$ true
  end if
  if $\mathcal{F}_1, \mathcal{F}_2$ sind normal **then**
    easy2 $\leftarrow$ true
  end if
  {Berechne Verzweigungsindices}
  for all $i \in \mathbb{N}_t$ **do**
    if e_i noch nicht bekannt **then**
      $j \leftarrow 1$, $\tilde{\mathfrak{p}} \leftarrow \mathfrak{p}_i$
      repeat
        $j \leftarrow j + 1$, $\tilde{\mathfrak{p}} \leftarrow \tilde{\mathfrak{p}}^j$
      until $p \notin \tilde{\mathfrak{p}}$
      $e_i \leftarrow i - 1$
    end if
    if easy2 = true **then**
      $e_i \leftarrow i - 1$ für alle noch nicht bekannten e_i
    end if
  end for
  {Berechne Trägheitsgrade}
  if easy2 = true **then**

```
      f_i ← s/e für alle i ∈ N_t
    else
      for all i ∈ N_t do
        if f_i noch nicht bekannt then
          D ← HNF von p
          f_i ← ln(|det(M)|)/ln(p)
        end if
      end for
    end if
  end if
  {Wende (3.29) an}
  for all i ∈ N_t do
    p_i ← ⟨p_i⟩_{o_K}
  end for
  return M
```

Bemerkung 3.43. *Der Algorithmus AlgKumBiv kann mit Hilfe von Induktion einfach auf Komposita vom vollen Grad, bestehend aus mehr als zwei Zahlkörpern übertragen werden. Man erhält den Algorithmus AlgKumMult. Algorithmustabelle 7 kann übernommen werden, lediglich der Aufruf von AlgPrimDec ist im zweiten Parameter zu modifizieren. Es sei aber bemerkt, dass die Maximalordnung des Kompositums bekannt sein muss, da man sonst nur Generatoren der Primideale in der Zerlegung angeben kann, (siehe (3.49)).*

Den Indexteilerfall kann man mit AlgKumBiv nicht lösen, da für diesen Fall der Idealmonoidisomorphismus κ aus (3.29) nicht definiert ist. Man kann lediglich die Primidealfaktorisierung in der Gleichungsordnung berechnen. Überprüft man, welche der Methoden aus (1.4) auf den Kompositafall übertragen werden können, kommt man zu folgendem Ergebnis:

Der Ore-Pohst Algorithmus ist nicht auf den Kompositafall übertragbar, da hier eine sukzessive p-adische Faktorisierung des definierenden Polynoms durchgeführt wird, welche nicht mit den Mitteln der Primärdekomposition emuliert werden kann. Der Algorithmus von Buchmann-Lenstra kann aber auf den Kompositafall übertragen werden:

Bemerkung 3.44. ***Der Algorithmus von Buchmann-Lenstra übertragen auf Komposita***
(Der Algorithmus wurde bereits eingehend in (1.4) beschrieben, deshalb ist die Darstellung knapp gehalten)

- ***Schritt 1: (Berechnen des p-Radikals)***
  In [Coh93, Chapter 6.1.3] wird das p-Radikal $I_p(\mathfrak{o}_\mathcal{K})$ der Maximalordnung als Kern einer q-ten Potenz des Frobenius-Homomorphismus berechnet, mit $p^q \geq [\mathcal{K} : \mathbb{Q}]$. Im Unterschied zu (1.4) ist jetzt die Maximalordnung $\omega_1, \ldots, \omega_s$ nicht als Transformationsmatrix bezüglich einer Potenzbasis von $\mathcal{K}$ gegeben, sondern bezüglich der Basis

  $$\{\vartheta_1^i \vartheta_2^j \mid i \in \mathbb{N}_{n-1}^0,\ j \in \mathbb{N}_{\tilde{m}-1}^0\}.$$

  Das hat auf die Berechnung von $I_p(\mathfrak{o}_\mathcal{K})$ keinen Einfluss. Man erhält die Hermite-Normalform von $I_p(\mathfrak{o}_\mathcal{K})/p\mathfrak{o}_\mathcal{K}$ (, da man alle Berechnungen modulo $p\mathfrak{o}_\mathcal{K}$ durchführt).

- ***Schritt 2: (Berechnen der Idealprodukte H_j)***
  Die Berechnung der H_j kann aus (1.39) wörtlich übernommen werden. Man erhält die H_j als Hermite-Normalformen modulo $p\mathfrak{o}_\mathcal{K}$.

- ***Schritt 3: (Zerlegen der Algebren $\mathfrak{o}_\mathcal{K}/H_j$)***
  Zum Zerlegen der separablen $\mathbb{F}_p$-Algebren $\mathfrak{o}_\mathcal{K}/H_j$ kann Algorithmus AlgZerSepA übernommen werden.

Der Algorithmus von Buchmann-Lenstra kann ohne Weiteres auf beliebige Komposita übertragen werden. Diese brauchen nicht vollen Rang zu haben, allerdings muss die Maximalordnung bekannt sein. Der einzige Unterschied zum bivariaten Fall betrifft die Darstellung der Maximalordnung. Die Transformationsmatrix der Maximalordnung ist nicht bezüglich einer Zahlkörperbasis gegeben, in der nur zwei primitive Elemente erscheinen, sondern beliebig viele:

$$\{\vartheta_1^{i_1} \cdot \ldots \cdot \vartheta_n^{i_n} \mid i_1 \in \mathbb{N}_{[\mathcal{F}_1:\mathbb{Q}]-1}^0,\ \ldots,\ i_n \in \mathbb{N}_{[\mathcal{F}_1 \ldots \mathcal{F}_n : \mathcal{F}_1 \ldots \mathcal{F}_{n-1}]-1}^0\}.$$

Das hat allerdings keinen Einfluss auf die Berechnungen. Man kommt zu folgendem Gesamtergebnis:

Bemerkung 3.45. *Liegt ein Kompositum $\mathcal{K}$ vor, für welches die Maximalordnung bekannt ist, kann man die Primidealfaktorisierung in jedem Fall mit dem Algorithmus von Buchmann-Lenstra berechnen. Primärdekomposition ist nur anwendbar, wenn $\mathcal{K}$ vollen Rang hat und auch dann nur, wenn p kein Indexteiler ist. Sonst ist mit Hilfe von Primärdekomposition lediglich die Berechnung der Primidealfaktorisierung in der Gleichungsordnung möglich.*

3.7 Primidealzerlegung in Komposita Teil 2

Seien die Bezeichnungen wie in (3.30). Sei $\mathcal{K}$ ein Kompositum vom vollen Grad. Die „problematischen“ Primzahlen, für die keine genaue Aussage über die Indexteilereigenschaft mit Hilfe von (3.5) möglich ist, werden ebenfalls als Indexteiler bezeichnet.

In diesem letzten Abschnitt werden Möglichkeiten untersucht, Aussagen zu treffen über das Zerlegungsverhalten einer Primzahl p in einem Kompositum vom vollen Grad, für welches die Maximalordnung nicht bekannt ist. Lediglich die Maximalordnungen der an der Kompositabildung beteiligten Zahlkörper sind bekannt. Interessant sind diese Untersuchungen aus folgendem Grund:

Bemerkung 3.46. *Die Anwendung des Algorithmus von Buchmann-Lenstra setzt zwingend die Kenntnis der Maximalordnung voraus, die Anwendung des Zerlegungssatzes (1.35) zwingend die Kenntnis eines Minimalpolynoms. Die Idee ist, dass man in Komposita die Primidealzerlegung berechnen kann, ohne ein definierendes Minimalpolynom oder die Maximalordnung zu kennen. Man muss lediglich die Maximalordnungen der an der Kompositabildung beteiligten Zahlkörper kennen. Die Berechnung der Maximalordnungen von Zahlkörpern vom Grad 15 und höher sind möglich, also kann man mit den hier vorgestellten Verfahren theoretisch die Primidealzerlegung von Zahlkörpern bis zum Grad 225 und höher berechnen, so sie sich als Komposita vom vollen Grad darstellen lassen. Betrachtet man Komposita, die durch mehr als zwei Zahlkörper gebildet werden, erhöht sich der Grad jeweils um den Faktor 15. Für Beispiele siehe (B.4).*

Es existieren in der Literatur [BR87] bereits Ansätze, lediglich das Zerlegungsverhalten einer Primzahl p zu berechnen und nicht die vollständige Zerlegung.

Zuerst werden „gute“ Primzahlen diskutiert, also Primzahlen, die keine Indexteiler sind:

Bemerkung 3.47. *Mit den Verfahren aus (3.5) ist man in der Lage, die Primidealzerlegung von p in der Gleichungsordnung $\mathbb{Z}[\vartheta_1, \vartheta_2]$ zu bestimmen. Da p kein Indexteiler ist, ist das Zerlegungsverhalten von p mit (3.29) in der Maximalordnung $\mathfrak{o}_\mathcal{K}$ dasselbe, wie in der Gleichungsordnung, d. h. die Generatoren sind dieselben und die Verzweigungsindices und Trägheitsgrade sind gleich. Die Algorithmen AlgKumBiv und AlgKumMult können können wörtlich übernommen werden.*

(3.47) lässt sich ohne die Ergebnisse aus (2.2) nur eingeschränkt auf beliebige Komposita übertragen:

Bemerkung 3.48. *Sei $\mathcal{K}$ ein Kompositum, bestehend aus n Zahlkörpern $\mathcal{K} := \mathcal{F}_1 \dots \mathcal{F}_n$, $n \geq 3$. Es seien nur die Maximalordnungen $\mathfrak{o}_{\mathcal{F}_1}, \dots, \mathfrak{o}_{\mathcal{F}_n}$ bekannt. Dann muss man, um die Algorithmen aus (3.4) anwenden zu können, in dem Körperturm*

$$\mathcal{F}_1 \dots \mathcal{F}_n \supseteq \mathcal{F}_1 \dots \mathcal{F}_{n-1} \supseteq \dots \supseteq \mathcal{F}_1$$

die genauen Grade der Erweiterungen

$$n_n := [\mathcal{F}_1 \dots \mathcal{F}_n : \mathcal{F}_1 \dots \mathcal{F}_{n-1}], \dots, n_2 := [\mathcal{F}_1\mathcal{F}_2 : \mathcal{F}_1]$$

kennen, da sonst die Konstruktion der Gleichungsordnung

$$\mathbb{Z}[\underline{\vartheta}] := \left\{ \sum_{i_1=1}^{n_1} \dots \sum_{i_n=1}^{n_n} a_{i_1,\dots,i_n} \vartheta_1^{i_1} \dots \vartheta_n^{i_n} \mid a_{i_1,\dots,i_n} \in \mathbb{Z} \right\}, \quad n_1 := \deg(\mathcal{F}_1)$$

nicht möglich ist, und man nicht überprüfen kann, ob $\mathcal{K}$ vollen Grad hat. Die Gleichungsordnung muss man auch für die Indexteilerberechnung kennen, siehe (3.38). Haben die Zahlkörper $\mathcal{F}_1, \dots, \mathcal{F}_n$ teilerfremde Diskriminanten, sind die Grade $n_n, \dots, n_1$ bekannt (wende (3.33) induktiv an). Ansonsten muss man, wie in (3.4) bemerkt, das Minimalpolynom $m_{\vartheta_\mu}(t) \in \mathbb{Z}[t]$ für $\mu \in \mathbb{N}_{n-1}$ als Element des Polynomringes $\mathfrak{o}_{\mathcal{F}_1 \dots \mathcal{F}_{\mu-1}}[X_1, \dots, X_{\mu-1}]$ interpretieren, und in diesem faktorisieren. Damit muss man aber die Maximalordnung $\mathfrak{o}_{\mathcal{F}_1 \dots \mathcal{F}_{n-1}}, \dots, \mathfrak{o}_{\mathcal{F}_1\mathcal{F}_2}$ kennen. Man gibt den Vorteil auf, dass man keine Maximalordnung kennen muss, welche durch Kompositumsbildung zustande gekommen ist.

Man kann jedoch die Ergebnisse aus Kapitel 2 heranziehen und erhält:

Satz 3.49. *Seien die Bezeichnungen wie in (3.30) bzw. in (3.48). Die Algorithmen AlgFieker und AlgFiekerSafe geben einem die Möglichkeit, induktiv die Grade der Erweiterungen*

$$n_n := [\mathcal{F}_1 \dots \mathcal{F}_n : \mathcal{F}_1 \dots \mathcal{F}_{n-1}], \dots, n_2 := [\mathcal{F}_1\mathcal{F}_2 : \mathcal{F}_1],$$

zu bestimmen, ohne zusätzlich Maximalordnungen oder Minimalpolynome berechnen zu müssen. Man kann so die Gleichungsordnung

$$\mathbb{Z}[\underline{\vartheta}] := \left\{ \sum_{i_1=1}^{n_1} \dots \sum_{i_n=1}^{n_n} a_{i_1,\dots,i_n} \vartheta_1^{i_1} \dots \vartheta_n^{i_n} \mid a_{i_1,\dots,i_n} \in \mathbb{Z} \right\}, \quad n_1 := \deg(\mathcal{F}_1)$$

generieren, überprüfen, ob (3.27) anwendbar ist und gegebene Primzahlen auf Indexteilereigenschaft mit den Verfahren aus (3.5) untersuchen. Ist die

gegebene Primzahl kein Indexteiler, kann man mit AlgKumMult (3.43) die Primidealfaktorisierung bestimmen. Das Ergebnis sind die Generatoren der Primideale in der Maximalordnung, die zugehörigen Verzweigungsindices und Trägheitsgrade.

Damit ist der Fall, dass eine zu zerlegende Primzahl kein Indexteiler ist, und $\mathcal{K}$ als Kompositum vom vollen Grad von beliebig vielen Zahlkörpern gegeben ist, vollständig gelöst.

Sei nun p Indexteiler im Sinne von (3.5). Der Algorithmus von Buchmann-Lenstra ist nicht anwendbar, weil bei der Konstruktion des p-Radikals, zwingend die Kenntnis der Maximalordnung vorausgesetzt wird, ebenso der Ore-Pohst Algorithmus. Man wird die Primidealzerlegung in der Gleichungsordnung berechnen und hoffen, dass hieraus Aussagen über das Zerlegungsverhalten von p in der Maximalordnung getroffen werden können.

Folgender Satz gibt Auskunft, welche Aussagen des erweiterten Zerlegungssatzes (3.26) auf den Indexteilerfall gerettet werden können:

Satz 3.50. *Seien die Voraussetzungen wie in (3.26). Seien $\tilde{\mathfrak{p}}_1, \ldots, \tilde{\mathfrak{p}}_r$ die Primideale, welche in $\mathbb{Z}[\vartheta_1, \vartheta_2]$ über p liegen. Sei $\mathfrak{a}_i$ das Bild von $\tilde{\mathfrak{p}}_i$ unter der Abbildung κ für $i \in \mathbb{N}_r$, siehe (3.29). Dann gilt*

$$\langle p \rangle_{\mathfrak{o}_\mathcal{K}} = \prod_{i=1}^{r} \mathfrak{a}_i.$$

Die $\mathfrak{a}_i$ sind paarweise coprim.

Beweis. Der Beweis folgt mit (3.26) in Verbindung mit [Coh93, Proposition 6.2.1]. □

Man erhält lediglich ein Produkt von coprimen Idealen, statt einem Produkt von Primidealen. Der Versuch, über das Zerlegungsverhalten von p in der Gleichungsordnung auf das Zerlegungsverhalten in der Maximalordnung zu schließen, ist aber hoffnungslos:

Beispiel 3.51. *Betrachte $\mathbb{Q}[\vartheta]$ mit Minimalpolynom $m_\vartheta(t) := t^3 - 86t^2 - 65t + 326 \in \mathbb{Z}[t]$. Die 2 zerlegt sich in der Gleichungsordnung zu*

$$\langle 2 \rangle_{\mathbb{Z}[\vartheta]} = \langle 2, \vartheta \rangle_{\mathbb{Z}[\vartheta]} \langle 2, 1 + \vartheta \rangle^2_{\mathbb{Z}[\vartheta]},$$

wegen

$$m_\vartheta(t) \equiv t(t+1)^2 \mod \mathbb{F}_2[t].$$

In der Maximalordnung $\mathfrak{o}_{\mathbb{Q}[\vartheta]}$ zerlegt sich die 2 aber zu

$$\langle 2 \rangle_{\mathfrak{o}_{\mathbb{Q}[\vartheta]}} = \langle 2, \vartheta^2 \rangle_{\mathfrak{o}_{\mathbb{Q}[\vartheta]}} \langle 2, \vartheta \rangle_{\mathfrak{o}_{\mathbb{Q}[\vartheta]}} \langle 2, \vartheta + \vartheta^2 \rangle_{\mathfrak{o}_{\mathbb{Q}[\vartheta]}},$$

denn $\langle 2, 1+\vartheta\rangle^2_{\mathbb{Z}[\vartheta]}$ *ist in* $\mathfrak{o}_{\mathbb{Q}[\vartheta]}$ *kein Primideal mehr. Hier gilt*

$$\langle 2, 1+\vartheta\rangle^2_{\mathfrak{o}_{\mathbb{Q}[\vartheta]}} = \langle 2, \vartheta^2\rangle_{\mathfrak{o}_{\mathbb{Q}[\vartheta]}} \langle 2, \vartheta+\vartheta^2\rangle_{\mathfrak{o}_{\mathbb{Q}[\vartheta]}}.$$

Beispiel 3.52. *Betrachte* $\mathbb{Q}[\vartheta]$ *mit* $m_\vartheta(t) := t^2 - 5 \in \mathbb{Z}[t]$. *Die* 2 *zerlegt sich in der Gleichungsordnung zu*

$$\langle 2\rangle_{\mathbb{Z}[\vartheta]} = \langle 2, 1+\vartheta\rangle^2_{\mathbb{Z}[\vartheta]},$$

wegen

$$m_\vartheta(t) \equiv (t+1)^2 \qquad \bmod \mathbb{F}_2[t].$$

In der Maximalordnung $\mathfrak{o}_{\mathbb{Q}[\vartheta]}$ *ist* $\langle 2\rangle_{\mathfrak{o}_{\mathbb{Q}[\vartheta]}}$ *aber ein Primideal. [Mar77, Chapter 3, Theorem 25]*

Man ist also nicht einmal in der Lage, die Anzahl der Primideale anzugeben, in die sich eine Primzahl zerlegt.

Das Gesamtergebnis des Kapitels ist in folgender Bemerkung zusammengefasst:

Bemerkung 3.53. *In diesem Kapitel wurde untersucht, ob man Primärdekomposition einsetzen kann, um die Primidealfaktorisierung in Komposita zu berechnen. Das ist grundsätzlich nicht möglich, sondern nur in Komposita, welche vollen Grad haben (3.31). Dann hat diese Technik aber den Vorteil, dass man weder ein Minimalpolynom noch die Maximalordnung des Kompositums kennen muss. Für diese Situation ist die Primärdekomposition bzgl. der Laufzeit unschlagbar, siehe die Beispiele in (B.4). Des weiteren wurden Verfahren entwickelt, um für eine große Menge von Primzahlen zu entscheiden, ob sie Indexteiler sind, ohne die Maximalordnung zu kennen. Für Indexteiler kann die Primärdekomposition in Komposita von vollem Grad allerdings nur eingesetzt werden, um die Primidealfaktorisierung in der Gleichungsordnung zu berechnen.*

Anhang A

Repräsentation im Computer

Dieses Unterkapitel beschäftigt sich mit der Frage, wie man die in der Theorie der Primidealzerlegung vorkommenden zahlentheoretischen Strukturen im Computer repräsentiert. Die Art und Weise dieser Repräsentation sollte wohl überlegt sein, denn naive Ansätze führen oft zu astronomischer Laufzeit. Als Stichwort sei hier die Koeffizientenexplosion bei der Hermite-Normalform genannt, siehe [Hop94, Kapitel 2].

Referenzsystem für die Implementation ist das Computeralgebrasystem KANT-V4 [DFK+97]. Weiterführende Literatur zu diesem Thema sind [PZ97, Coh93, Coh00] und das Standardwerk [Knu97a, Knu97b, Knu97c].

Zuerst werden Möglichkeiten diskutiert, wie man eine algebraische Zahl in einem Computer speichert. Der zweite Abschnitt behandelt die Speicherung von Idealen.

A.1 Darstellung von algebraischen Zahlen

Im Allgemeinen werden vier Möglichkeiten verwendet, algebraische Zahlen in Computern zu repräsentieren:

Definition A.1. *Sei $\alpha \in \mathbb{C}$ eine algebraische Zahl, nach (1.4) existiert das Minimalpolynom $m_\alpha(t) \in \mathbb{Q}[t]$ und der Grad $\deg(m_\alpha(t))$ entspricht der Anzahl der Konjugierten von α in einem algebraischen Abschluss. Um α von diesen Konjugierten unterscheiden zu können, repräsentiert man α als ein Paar*

$$(m_\alpha(t), x) \in \mathbb{Q}[t] \times \mathbb{C},$$

*wobei $x \in \mathbb{C}$ eine komplexe Approximation ist. Das Paar $(m_\alpha(t), x)$ nennt man die **Minimalpolynomdarstellung von** α.*

Wichtig an der Minimalpolynomdarstellung ist, dass die zu speichernde algebraische Zahl nicht notwendig Element eines Zahlkörpers sein muss. Man hat so die Möglichkeit mit algebraischen Zahlen, unabhängig von dem Zahlkörpern, aus dem sie stammen, Arithmetik zu betreiben.

Sei ab jetzt $\mathcal{F} := \mathbb{Q}[\vartheta]$ algebraischer Zahlkörper vom Grad n und $\alpha \in \mathcal{F}$.

Definition A.2. *Sei $\vartheta_1, \ldots, \vartheta_n$ eine $\mathbb{Q}$-Basis von $\mathcal{F}$, dann kann α eindeutig geschrieben werden als*

$$\alpha = \sum_{j=0}^{n-1} \frac{\tilde{p}_j}{q_j} \vartheta_{j+1}, \quad \frac{\tilde{p}}{q} \in \mathbb{Q},\ \gcd(\tilde{p}, q) = 1.$$

Setzt man $d := \operatorname{lcm}(q_0, \ldots, q_{n-1})$, erhält man eine Darstellung

$$\alpha = \frac{\sum_{j=0}^{n-1} p_j \vartheta_{j+1}}{d}, \quad d > 0,\ p_j \in \mathbb{Z},\ \gcd(p_0, \ldots, p_{n-1}, d) = 1.$$

*Ist die Basis $\{\vartheta_1, \ldots, \vartheta_n\}$ eine Potenzbasis eines primitiven Elementes ϑ, nennt man den $\mathbb{Z}$-Vektor $(p_0, \ldots, p_{n-1}, d) \in \mathbb{Z}^{n+1\times 1}$ die **Standarddarstellung von α bzgl. ϑ.***

Definition A.3. *Betrachte die Darstellungsmatrix M_α von α, siehe (1.11), so kann M_α umgeformt werden zu einer Matrix $\tilde{M}_\alpha = (\tilde{m}_{ij})_{1\le i,j\le n}$ für die gilt:*

$$M_\alpha = \frac{(\tilde{m}_{ij})_{1\le i,j\le n}}{d}, \quad d > 0,\ \tilde{m}_{ij} \in \mathbb{Z},\ \gcd(\{\tilde{m}_{i,j} \mid i, j \in \mathbb{N}_n\}, d) = 1.$$

Man nennt das Paar

$$((\tilde{m}_{ij})_{1\le i,j\le n}, d) \in \mathbb{Z}^{n\times n} \times \mathbb{N}$$

*die **Matrixdarstellung von** α. Die Zahl d nennt man den **Nenner von** α.*

Definition A.4. *Seien $\sigma_1, \ldots, \sigma_n : \mathbb{Q}[t]/\langle m_\vartheta(t)\rangle_{\mathbb{Q}[t]} \to \mathbb{C}$ die $\mathbb{Q}$-Einbettungen von $\mathcal{F}$, siehe (1.5). Seien die σ_i so sortiert, dass gilt*

$$\underbrace{\sigma_1, \ldots, \sigma_{r_1}}_{\substack{\text{reelle}\\ \mathbb{Q}\text{-Einbettungen}}}, \underbrace{\sigma_{r_1+1}, \ldots, \sigma_{r_1+r_2}}_{\substack{\text{komplexe}\\ \mathbb{Q}\text{-Einbettungen}}}, \underbrace{\sigma_{r_1+r_2+1}, \ldots, \sigma_{r_1+r_2+r_2}}_{\substack{\text{zu } \sigma_{r_1+1},\ldots,\sigma_{r_1+r_2}\\ \text{konjugiert komplexe}\\ \mathbb{Q}\text{-Einbettungen}}}.$$

Dann kann α eindeutig dargestellt werden durch den Vektor

$$(\sigma_1(\alpha), \ldots, \sigma_{r_1+r2}(\alpha)) \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2},$$

*welchen man die **Konjugiertenvektordarstellung** von α nennt.*

Gilt $\deg(m_\alpha(t)) \neq \deg(\mathcal{F})$ in der Konjugiertenvektordarstellung einer algebraischen Zahl $\alpha \in \mathcal{F}$, dann wiederholen sich die Komponenten dieser Darstellung $\deg(\mathcal{F})/\deg(m_\alpha(t))$ mal.

Für eine ausführliche Diskussion der Vor- und Nachteile aller vier Darstellungen siehe [Coh93, Chapter 4.2].

A.2 Darstellung von Idealen

Will man Ideale von Ordnungen in Computern repräsentieren, hat man zwei verschiedene Ansätze: Die Hermite-Normalform und die 2-Elementdarstellung.

Sei für diesen Abschnitt $\mathcal{F} := \mathbb{Q}[\vartheta]$ Zahlkörper vom Rang n. Sei $\mathcal{O}$ eine Ordnung von $\mathcal{F}$ und $\mathfrak{a} \in \mathcal{I}_\mathcal{O}^\times$ ein Ideal von $\mathcal{O}$.

Den Zugang zur Hermite-Normalform liefert folgende Proposition:

Proposition A.5. *Es ist $\mathfrak{a}$ freier $\mathbb{Z}$-Modul vom Rang n.*

[Coh93, Proposition 4.6.3] Das Ideal $\mathfrak{a}$ hat daher eine $\mathbb{Z}$-Basis der Mächtigkeit n, zum Beispiel $\omega_1, \ldots, \omega_n \in \mathcal{F}$. Es existiert mindestens eine Zahl $d \in \mathbb{Z}$ für die gilt $d\omega_i \in \mathcal{O}$. Die kleinste positive Zahl d mit dieser Eigenschaft nennt man den **Nenner von $\mathfrak{a}$ bzgl.** $\mathcal{O}$. Man stellt nun $d\omega_1, \ldots, d\omega_n$ mit Hilfe einer Transformationsmatrix $T \in \mathbb{Z}^{n\times n}$ bzgl. $\mathcal{O}$ dar.

Es existieren Transformationsmatrizen, die eine ganz besondere Form haben:

Satz A.6. *Zu jeder Matrix $A \in \mathbb{Z}^{n\times n}$ existiert eines Matrix $U := (u_{i,j}) \in \mathrm{Gl}(n, \mathbb{Z})$, so dass AU untere Dreiecksmatrix ist. Es gilt $u_{i,i} \in \mathbb{N}^0$ und die $u_{i,j}$ mit $j < i$ sind modulo $u_{i,i}$ eindeutig bestimmt für alle $i, j \in \mathbb{N}_n$.*

[PZ97, Chapter 3, (2.6)] Zusammengefasst erhält man:

Satz A.7. *Sei $\alpha_1, \ldots, \alpha_n \in \mathcal{F}$ eine Basis von $\mathcal{O}$, dann existiert eine eindeutig bestimmte $\mathbb{Z}$-Basis $\omega_1, \ldots, \omega_n \in \mathcal{F}$ von $\mathfrak{a}$, so dass, falls man*

$$\omega_i = \frac{\sum_{i=1}^{n} \omega_{i,j}\alpha_i}{d}$$

schreibt, gilt:

- *d ist der Nenner von $\mathfrak{a}$ bzgl. $\mathcal{O}$,*
- *$\omega_{i,j} \in \mathbb{Z}$ für alle $i, j \in \mathbb{N}_n$,*
- *für $i < j$ gilt $\omega_{i,j} = 0$,*

- *für* $i = j$ *gilt* $\omega_{i,j} > 0$,
- *für alle* $i > j$ *gilt* $0 \leq \omega_{i,j} < \omega_{i,i}$.

[Coh93, Theorem 4.7.3]

Definition A.8. *Seien die Bezeichnungen wie in (A.7). Das Paar*

$$(d, (\omega_{i,j})_{1 \leq i,j \leq n}) \in \mathbb{N} \times \mathbb{Z}^{n \times n}$$

nennt man ***Hermite-Normalform*** *oder* ***HNF von*** $\mathfrak{a}$ ***bzgl*** $\mathcal{O}$. *Die Basis* $\{\omega_1, \ldots, \omega_n\}$ *nennt man* ***HNF-Basis von*** $\mathfrak{a}$ ***bzgl.*** $\mathcal{O}$.

Sei ab jetzt $\mathfrak{a} \in \mathcal{I}_{\mathfrak{o}_\mathcal{F}}^\times$. Die Existenz der 2-Elementdarstellung von $\mathfrak{a}$ garantiert folgende Proposition:

Proposition A.9. *Sei* $\alpha \in \mathfrak{a}$, $\alpha \neq 0$ *beliebig. Dann existiert* $\beta \in \mathfrak{a}$, *so dass* $\mathfrak{a} = \langle \alpha, \beta \rangle_{\mathfrak{o}_\mathcal{F}}$ *gilt. Des weiteren ist* $\mathfrak{a} \cap \mathbb{Z} \neq \emptyset$.

[Coh93, Proposition 4.7.7]

Definition A.10. *Sei* α *die kleinste positive Zahl der Menge* $\mathfrak{a} \cap \mathbb{Z}$ *und* $\beta \in \mathfrak{a}$ *wie in (A.9). Dann nennt man das Paar* $(\alpha, \beta) \in \mathbb{N} \times \mathfrak{a}$ *die* ***2-Elementdarstellung von*** $\mathfrak{a}$.

Ein offensichtlicher Vorteil der 2-Elementdarstellung ist der niedrigere Speicherplatz gegenüber der HNF. Ein Nachteil ist, dass man beim Addieren und Multiplizieren von zwei Idealen vier Generatoren erhält und die 2-Elementdarstellung des Ergebnisses neu berechnen muss. Dieses Problem löst die p-Normaldarstellung [PZ97, Chapter 6, (3.14)], [Hop98, Definition 1.2.6].

Für eine weiterführende Diskussion der Darstellung von Idealen sei auf [PZ97, Chapter 6.2] und [Hop98] verwiesen.

Anhang B

Beispiele und Berechnungen am Computer

Dieser Abschnitt beschreibt die Verfahren dieser Arbeit, welche in dem Computeralgebrasystem KANT-V4 implementiert sind bzw. im Rahmen dieser Arbeit implementiert wurden. Alle Berechnungen wurden durchgeführt auf einem Rechner mit AMD Athlon™ XP 1500+ Prozessor mit 512 Megabyte Hauptspeicher und einer Cachegröße von 256 Kilobyte.

B.1 Schnelle Regularitätsbestimmung

In (2.1) ist man darauf angewiesen, schnell für eine Matrix $M \in \mathbb{Z}^{n\times n}$ zu entscheiden, ob die Determinante von M Null ist oder nicht. Die Idee ist, für eine gegebene Matrix M, die man auf Regularität überprüfen will, zuerst M modulo einer Primzahl p zu reduzieren, um dann die Determinante der reduzierten Matrix zu überprüfen, siehe (2.7), (2.8). Hat man eine Primzahl p gefunden, so dass $\det(\overline{M}^p) \neq 0$ ist, ist man fertig.

Folgende Fragen wurden untersucht:

- Ab welcher Spalten- bzw. Zeilenzahl lohnt sich die Reduktion?
- Ab welcher Primzahl kann man davon ausgehen, dass man die Matrix nur einmal reduzieren muss, um ein verlässliches Ergebnis zu haben?
- Ist die modulare Methode schneller, und wenn ja, um welchen Faktor?

Die Ergebnisse sind in folgender Tabelle zusammengefasst, dabei haben die einzelnen Spalten folgende Bedeutung:

- **Spalte 1**: Anzahl der Spalten/Zeilen der untersuchten Matrix.

- **Spalte 2**: Koeffizientenbereich.
- **Spalte 3**: Anzahl der Fehler, d. h. die Determinante der reduzierten Matrix ist Null, obwohl die reale Determinante ungleich Null ist.
- **Spalte 4:** Zeit 1: Durchschnittliche Rechenzeit in Millisekunden für das Ermitteln der realen Determinante.
- **Spalte 5:** Zeit 2: Durchschnittliche Rechenzeit in Millisekunden für das Reduzieren der Matrix und Ermitteln der Determinante.

Betrachtet wurde jeweils eine Reduktion modulo 2, 3 und 5. Es wurden für jede Kombination 20000 Zufallsmatrizen erzeugt.

Tabelle B.1: Regularitätsbestimmung modulo 2

Benutzte Primzahl: 2				
Anzahl Spalten	Koeffizienten-bereich	Anzahl Fehler	Zeit 1	Zeit 2
10	±10k	5838	1.077	0.267
10	±50k	5992	1.112	0.295
10	±100k	5950	1.386	0.281
20	±10k	52	4.132	1.270
20	±50k	39	4.487	1.323
20	±100k	56	5.380	1.337
30	±10k	1	9.865	3.553
30	±50k	0	10.407	3.602
30	±100k	0	12.018	3.544
40	±10k	0	17.157	8.125
40	±50k	0	20.680	8.336
40	±100k	0	21.461	8.358
50	±10k	0	27.339	12.193
50	±50k	0	33.010	12.262
50	±100k	0	33.783	12.307
100	±10k	0	156.740	66.901
100	±50k	0	191.851	66.997
100	±100k	0	197.266	67.011
150	±10k	0	502.541	204.072
150	±50k	0	623.646	204.183
150	±100k	0	639.321	203.845
200	±10k	0	1228.833	428.044
200	±50k	0	1290.573	429.016

Tabelle B.1: (Fortsetzung)

Benutzte Primzahl: 2				
Anzahl Spalten	Koeffizienten-bereich	Anzahl Fehler	Zeit 1	Zeit 2
200	±100k	0	1551.843	428.711
250	±10k	0	2215.004	756.709
250	±50k	0	2747.506	756.810
250	±100k	0	2809.379	757.069

Tabelle B.2: Regularitätsbestimmung modulo 3

Benutzte Primzahl: 3				
Anzahl Spalten	Koeffizienten-bereich	Anzahl Fehler	Zeit 1	Zeit 2
10	±10k	223	1.086	0.429
10	±50k	241	1.121	0.423
10	±100k	250	1.371	0.415
20	±10k	0	4.115	2.163
20	±50k	0	4.366	2.167
20	±100k	0	5.483	2.176
30	±10k	0	9.758	6.341
30	±50k	0	10.300	6.309
30	±100k	0	12.050	6.317
40	±10k	0	17.204	9.832
40	±50k	0	20.560	10.215
40	±100k	0	21.560	9.814
50	±10k	0	27.351	17.463
50	±50k	0	32.992	17.357
50	±100k	0	33.782	17.379
100	±10k	0	156.903	78.621
100	±50k	0	192.093	78.606
100	±100k	0	197.665	78.618
150	±10k	0	508.655	235.747
150	±50k	0	632.132	235.767
150	±100k	0	652.962	236.894
200	±10k	0	1233.566	499.140
200	±50k	0	1287.773	497.910
200	±100k	0	1552.332	497.640

Tabelle B.2: (Fortsetzung)

Benutzte Primzahl: 3				
Anzahl Spalten	Koeffizienten-bereich	Anzahl Fehler	Zeit 1	Zeit 2
250	±10k	0	2216.417	904.574
250	±50k	0	2749.457	904.583
250	±100k	0	2809.536	904.509

Tabelle B.3: Regularitätsbestimmung modulo 5

Benutzte Primzahl: 5				
Anzahl Spalten	Koeffizienten-bereich	Anzahl Fehler	Zeit 1	Zeit 2
10	±10k	5	1.081	0.637
10	±50k	3	1.106	0.630
10	±100k	0	1.366	0.639
20	±10k	0	4.150	3.019
20	±50k	0	4.384	3.020
20	±100k	0	5.326	3.011
30	±10k	0	9.758	6.110
30	±50k	0	10.313	6.080
30	±100k	0	12.061	6.069
40	±10k	0	17.167	12.097
40	±50k	0	20.702	12.141
40	±100k	0	21.532	12.116
50	±10k	0	27.227	18.580
50	±50k	0	32.942	18.622
50	±100k	0	33.739	18.698
100	±10k	0	156.938	89.874
100	±50k	0	192.796	90.173
100	±100k	0	197.626	89.837
150	±10k	0	506.962	264.382
150	±50k	0	630.141	264.278
150	±100k	0	647.115	264.370
200	±10k	0	1228.704	538.494
200	±50k	0	1287.566	538.403
200	±100k	0	1552.429	538.369
250	±10k	0	2218.623	1017.916
250	±50k	0	2753.358	1018.081

Tabelle B.3: (Fortsetzung)

Benutzte Primzahl: 5				
Anzahl Spalten	Koeffizienten-bereich	Anzahl Fehler	Zeit 1	Zeit 2
250	$\pm$100k	0	2813.209	1017.676

Betrachtet man die Tabellen erhält man folgende Ergebnisse:

- Für die Primzahl 2 kommt es ab einer Spalten- bzw. Zeilenanzahl von größer 40 zu keinen Fehlern mehr.
- Für Primzahlen größer als 3 kommt es ab einer Spalten- bzw. Zeilenanzahl von größer 20 zu keinen Fehlern mehr.
- Die modulare Methode ist im Durchschnitt um den Faktor 3 schneller, ab einer Spalten- bzw. Zeilenanzahl größer als 250 um den Faktor 4.
- Die Benutzung der jeweils nächstgrößeren Primzahl verlängert die Rechenzeit der modularen Methode um circa 10 %. Siehe jedoch die nächste Bemerkung.

Bemerkung B.1. *In den Tabellen (B.1), (B.2) und (B.3) wird deutlich, dass die Benutzung einer höheren Primzahl die Rechenzeit der Regularitätsbestimmung erhöht. Es gibt jedoch Prozessoren, deren ALU in der Lage ist, die Multiplikation von zwei Registerinhalten innerhalb eines Prozessortaktes auszuführen. Für solche Hardware kann es sinnvoll sein, als Primzahl p diejenige auszuwählen, die die größte Primzahl ist, welche noch vollständig in einem Register gespeichert werden kann. Dieses Vorgehen erhöht die Wahrscheinlichkeit, dass man die Reduktion der zu überprüfenden Matrix nur ein einziges Mal ausführen muss, um sofort ein zuverlässiges Ergebnis zu produzieren. Auf der anderen Seite verliert man keine Rechengeschwindigkeit. Softwaretechnisch gesehen reduziert eine solche Implementation allerdings die Portabilität auf andere Architekturen.*

B.2 Beispiele für die $\mathfrak{S}$-Schranke

In (2.13) wurde die $\mathfrak{S}$-Menge und $\mathfrak{S}$-Schranke definiert. Im Rahmen dieser Arbeit wurden Untersuchungen durchgeführt, wie für zwei zufällig gewählte Polynome $f_1(t), f_2(t) \in \mathbb{Z}[t]$ die $\mathfrak{S}$-Menge und die $\mathfrak{S}$-Schranke verteilt sind.

In die Untersuchung einbezogen wurden 50000 Paare von Zufallspolynome $(f_1(t), f_2(t)) \in \mathbb{Z}[t] \times \mathbb{Z}[t]$. Alle Polynome waren normiert, irreduzibel und es es galt:

$$2 \leq \deg(f_1(t)), \deg(f_2(t)) \leq 30.$$

Die Koeffizienten hatten Werte zwischen -10000 und 10000, gerechnet wurde mit einer Genauigkeit von 500 Nachkommastellen. Die Ergebnisse sind in (B.4) zusammengefasst. Die einzelnen Spalten haben folgende Bedeutung:

- Spalte 2 gibt die Anzahl der Polynompaare an, die eine $\mathfrak{S}$-Schranke haben, welche kleiner ist als die Zahl in Spalte 1.
- Spalte 3 gibt die Anzahl der Polynompaare aus Spalte 2 in Prozent an.

Tabelle B.4: $\mathfrak{S}$-Schranken von Zufallspolynomen

0.12	2972	5.94
0.25	6156	12.31
0.5	12446	24.89
1	24910	49.82
2	37242	74.48
3	41461	82.92
4	43496	86.99
5	44758	89.51
9	46992	93.98
10	47275	94.55
15	48056	96.11
20	48486	96.97
30	48884	97.76
40	49084	98.16
50	49215	98.43
100	49410	98.82
500	49520	99.04
1000	49553	99.10
5000	49735	99.47
10000	49847	99.69
20000	49932	99.86
1000000	50000	100.00

Auffällig ist, dass bereits 90 % der Paare ein $\mathfrak{S}$-Schranke kleiner als 10 haben. Genau dieser Umstand wird in dem Algorithmus AlgFieker benutzt.

Das Maximum der $\mathfrak{S}$-Schranke betrug 699902 und wurde erzeugt von den Polynomen

$$\begin{aligned} f_1(t) &:= t^{26} - 8969t^{25} + 3738t^{24} - 6258t^{23} + 8211t^{22} + 168t^{21} \\ &\quad -8218t^{20} + 8247t^{19} + 6785t^{18} + 108t^{17} + 1289t^{16} - 7654t^{15} \\ &\quad +2t^{14} + 4941t^{13} - 7057t^{12} + 1889t^{11} + 1139t^{10} - 3982t^9 \\ &\quad -4660t^8 + 7623t^7 - 7146t^6 - 4907t^5 - 10t^4 + 9158t^3 \\ &\quad -9294t^2 + 3504t - 401 \end{aligned}$$

und

$$\begin{aligned} f_2(t) &:= t^{10} + 2396t^9 + 9154t^8 - 6338t^7 - 1591t^6 - 1847t^5 \\ &\quad -7298t^4 - 6792t^3 + 7911t^2 - 819t + 5236. \end{aligned}$$

Als Beispiel, wie wahllos die $\mathfrak{S}$-Schranke verteilt ist, betrachte folgendes Polynompaar, für welches die $\mathfrak{S}$-Schranke besonders klein ist. Die Polynome

$$\begin{aligned} f_1(t) &:= x^{29} - 102t^{28} + 8733t^{27} - 7691t^{26} + 9084t^{25} + 3278t^{24} \\ &\quad +8214t^{23} + 7978t^{22} + 6738t^{21} + 3681t^{20} - 2265t^{19} - 8523t^{18} \\ &\quad +9310t^{17} + 6819t^{16} - 8897t^{15} + 9415t^{14} + 8237t^{13} - 1691t^{12} \\ &\quad -2211t^{11} - 2277t^{10} - 8006t^9 - 7892t^8 + 6265t^7 + 4852t^6 \\ &\quad -3438t^5 + 756t^4 + 8204t^3 + 7242t^2 - 9394 \end{aligned}$$

und

$$\begin{aligned} f_2(t) &:= t^{24} + 2490t^{23} + 1741t^{22} + 8197t^{21} - 1491t^{20} - 3977t^{19} - 4885t^{18} \\ &\quad +5145t^{17} + 4948t^{16} - 9689t^{15} + 6678t^{14} + 9272t^{13} + 1204t^{12} \\ &\quad -1065t^{11} - 6286t^{10} + 2777t^9 + 3789t^8 - 9246t^7 - 31t^6 + 496t^5 \\ &\quad +3542t^4 - 1687t^3 - 304t^2 + 301t + 7393 \end{aligned}$$

haben die $\mathfrak{S}$-Schranke 0.020046720818. Die Polynome

$$\begin{aligned} f_1(t) &:= t^9 - 8951t^8 - 7903t^7 - 6105t^6 + 8673t^5 + 8176t^4 \\ &\quad -6616t^3 - 4470t^2 - 9965t + 2651 \end{aligned}$$

und

$$f_2(t) := t^3 + 1345t^2 - 3491t + 2081$$

haben dagegen die $\mathfrak{S}$-Schranke 12184.

B.3 Leistung des OrderShort Algorithmus

Der OrderShort Algorithmus, wie er in (2.3) beschrieben ist, wurde im Rahmen dieser Arbeit komplett neu implementiert. In der neuen Version kann der Anwender folgende Parameter selbst festlegen:

(1) Soll eine LLL-Reduktion stattfinden oder nicht?

(2) Sollen nur Elemente mit Nenner der (eventuell LLL-reduzierten) Maximalordnung verwendet werden?

(3) Die maximale Anzahl der zu testenden Linearkombinationen in jedem Durchlauf für ein primitives Element.

(4) Soll die Koeffizientenmenge $\{0, 1\}$ der Linearkombinationen um $\{-1\}$ ergänzt werden?

(5) Soll beim Auffinden eines Elementes mit einem kleineren Index sofort gestoppt bzw. in die Rekursion gesprungen werden, oder soll die maximale Anzahl an Linearkombinationen getestet werden?

(6) Die maximale Anzahl rekursiver Aufrufe der Funktion, wenn ein kleinerer Index gefunden wurde.

(7) Die maximale Anzahl von Koeffizienten ungleich Null in einer Linearkombination.

Es wurden für verschiedene Kombinationen jeweils 1000 Zufallspolynome bestimmt, um die Leistung des OrderShort Algorithmus zu testen. Die Zufallspolynome hatten dabei einen vorgegebenen Index. Es kam zu folgenden Ergebnissen:

(1) Die Leistung des Algorithmus mit LLL-Reduktion ist wesentlich besser. Die zusätzliche Rechenzeit für die LLL-Reduktion fällt nicht ins Gewicht.

(2) Es ist sinnvoll, Elemente ohne Nenner in die Bildung der Linearkombinationen mit einzubeziehen.

(3) Die maximale Anzahl der Linearkombinationen sollte möglichst hoch angesetzt werden, und die maximale Anzahl der zu testenden Linearkombinationen über die maximale Anzahl der Koeffizienten ungleich Null gesteuert werden. (Siehe nächsten Punkt)

(4) Die maximale Anzahl von Koeffizienten ungleich Null sollte den Wert 3 nicht überschreiten. In 50 % aller Fälle kommt es schon zu einer Indexreduktion, wenn man nur einen einzigen Koeffizienten ungleich Null zulässt, d. h. wenn man die Elemente der reduzierten Maximalordnung der Reihe nach durchprobiert.

(5) Die maximale Rekursionstiefe der Funktion sollte umgekehrt proportional zur Anzahl der Primdivisoren des Index sein.

(6) Ob man $\{-1\}$ als Koeffizient zulässt, hat keinen Einfluss auf Leistung.

Verwendet man den OrderShort Algorithmus, wenn man die Primidealzerlegung berechnen möchte, reicht die Leistung allerdings nicht an die des Algorithmus von Buchmann-Lenstra heran. Der Algorithmus von Buchmann-Lenstra ist in der in dem System KANT-V4 implementierten Version wesentlich schneller. Der Einsatz von OrderShort bleibt daher auf Gebiete beschränkt, wo man zwingend auf einen kleinen Index angewiesen ist.

B.4 Primidealfaktorisierung in „großen“ Komposita

In diesem Abschnitt werden zwei Beispiele besprochen, die die Leistungsfähigkeit der Primidealzerlegung durch Primärdekomposition in Komposita vom vollen Grad hervorheben. Angewandt wurden die Verfahren aus (3.7). Die an der Kompositabildung beteiligten Zahlkörper wurden der KANT-V4 Datenbank entnommen. Zuerst ein kleines Beispiel:

Beispiel B.2. ***Zahlkörper vom Grad*** 28
Betrachte den Zahlkörper $\mathbb{Q}[\vartheta]$ *mit* ϑ *Nullstelle des Polynoms*

$$\begin{aligned} m_\vartheta(t) \;=\; & t^{28} + 111t^{27} + 5339t^{26} + 144856t^{25} \\ & +2397735t^{24} + 23968904t^{23} + 124050213t^{22} \\ & +39142425t^{21} - 2866083966t^{20} - 7514711113t^{19} \\ & +41365184897t^{18} + 118633909733t^{17} - 569206724921t^{16} \\ & -499467772351t^{15} + 5323168738219t^{14} - 8075616574139t^{13} \\ & -2915603136061t^{12} + 21091176068315t^{11} - 25253551274912t^{10} \\ & +12990181145039t^{9} + 24362931701047t^{8} - 85546892141911t^{7} \\ & +116191002429482t^{6} - 108955850383737t^{5} \\ & +87584279312844t^{4} - 46823283975692t^{3} + \\ & 14271347151002t^{2} - 3350160571911t + 514703916260. \end{aligned}$$

Dieser Zahlkörper $\mathbb{Q}[\vartheta]$ *kann dargestellt werden als Kompositum von* $\mathbb{Q}[\vartheta_1]$ *und* $\mathbb{Q}[\vartheta_2]$*, wobei* ϑ_1 *und* ϑ_2 *Nullstellen der Polynome*

$$m_{\vartheta_1}(t) \;=\; t^4 + 9t^3 - 18t^2 + 7t + 8$$

und

$$m_{\vartheta_2}(t) \;=\; t^7 + 12t^6 - 4t^5 - 12t^4 + 13t^3 + 3t^2 - 13t + 20$$

sind. Die Diskriminanten von $\mathbb{Q}[\vartheta_1]$ *und* $\mathbb{Q}[\vartheta_2]$ *sind teilerfremd, der Diskriminantentest ist also positiv. Es ist:*

$$\begin{aligned}\operatorname{disc}(\mathbb{Q}[\vartheta]) \;=\; & -160586240139546483269465519006950308614793754930849554935897966330204999\\ & 1146319509444916626581026457983975929627924215844202271.\end{aligned}$$

Die Primteiler dieser Diskriminante sind

$$\{29,\ 919019,\ 2021927,\ 1780931668729\}.$$

Der Index $[\mathfrak{o}_{\mathbb{Q}[\vartheta_1,\vartheta_2]} : \mathbb{Z}[\vartheta_1,\vartheta_2]]$ *ist* 1*. Die Primzahl* 13 *ist unverzweigt und zerlegt sich zu*

$$\langle 13\rangle_{\mathfrak{o}_{\mathbb{Q}[\vartheta_1,\vartheta_2]}} = \mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_6,$$

mit

$$\begin{aligned}
\mathfrak{p}_1 &= \langle 13,\ \vartheta_1 + 11,\ \vartheta_2\rangle_{\mathfrak{o}_{\mathbb{Q}[\vartheta_1,\vartheta_2]}}\\
\mathfrak{p}_2 &= \langle 13,\ \vartheta_1,\ \vartheta_2\rangle_{\mathfrak{o}_{\mathbb{Q}[\vartheta_1,\vartheta_2]}}\\
\mathfrak{p}_3 &= \langle 13,\ \vartheta_1^2 + 3\vartheta_1 + 6,\ \vartheta_2\rangle_{\mathfrak{o}_{\mathbb{Q}[\vartheta_1,\vartheta_2]}}\\
\mathfrak{p}_4 &= \langle 13,\ \vartheta_1 + 11,\ \vartheta_2^2 + 7\vartheta_2 + 4\rangle_{\mathfrak{o}_{\mathbb{Q}[\vartheta_1,\vartheta_2]}}\\
\mathfrak{p}_5 &= \langle 13,\ \vartheta_1,\ \vartheta_2^2 + 7\vartheta_2 + 4\rangle_{\mathfrak{o}_{\mathbb{Q}[\vartheta_1,\vartheta_2]}}\\
\mathfrak{p}_6 &= \langle 13,\ \vartheta_1 + 11,\ \vartheta_2^4 + 6\vartheta_2^3 + 6\vartheta_2^2 + 12\vartheta_2 + 10\rangle_{\mathfrak{o}_{\mathbb{Q}[\vartheta_1,\vartheta_2]}}\\
\mathfrak{p}_7 &= \langle 13,\ \vartheta_1,\ \vartheta_2^4 + 6\vartheta_2^3 + 6\vartheta_2^2 + 12\vartheta_2 + 10\rangle_{\mathfrak{o}_{\mathbb{Q}[\vartheta_1,\vartheta_2]}}\\
\mathfrak{p}_8 &= \langle 13,\ \vartheta_1 + 8\vartheta_2^3 + 11\vartheta_2^2 + 3\vartheta_2 + 7,\ \vartheta_2^4 + 6\vartheta_2^3 + 6\vartheta_2^2 + 12\vartheta_2 + 10\rangle_{\mathfrak{o}_{\mathbb{Q}[\vartheta_1,\vartheta_2]}}\\
\mathfrak{p}_9 &= \langle 13,\ \vartheta_1 + 5\vartheta_2^3 + 2\vartheta_2^2 + 10\vartheta_2 + 9,\ \vartheta_2^4 + 6\vartheta_2^3 + 6\vartheta_2^2 + 12\vartheta_2 + 10\rangle_{\mathfrak{o}_{\mathbb{Q}[\vartheta_1,\vartheta_2]}}\\
\mathfrak{p}_{10} &= \langle 13,\ \vartheta_1 + 10\vartheta_2 + 4,\ \vartheta_2^2 + 7\vartheta_2 + 4\rangle_{\mathfrak{o}_{\mathbb{Q}[\vartheta_1,\vartheta_2]}}\\
\mathfrak{p}_{11} &= \langle 13,\ \vartheta_1 + 3\vartheta_2 + 12,\ \vartheta_2^2 + 7\vartheta_2 + 4\rangle_{\mathfrak{o}_{\mathbb{Q}[\vartheta_1,\vartheta_2]}}.
\end{aligned}$$

Für die Trägheitsgrade gilt

$$\begin{array}{lll} f(\mathfrak{p}_1|\langle 13\rangle) = 1 & f(\mathfrak{p}_2|\langle 13\rangle) = 1 & f(\mathfrak{p}_3|\langle 13\rangle) = 2 \\ f(\mathfrak{p}_4|\langle 13\rangle) = 2 & f(\mathfrak{p}_5|\langle 13\rangle) = 2 & f(\mathfrak{p}_6|\langle 13\rangle) = 4 \\ f(\mathfrak{p}_7|\langle 13\rangle) = 4 & f(\mathfrak{p}_8|\langle 13\rangle) = 4 & f(\mathfrak{p}_9|\langle 13\rangle) = 4 \\ f(\mathfrak{p}_{10}|\langle 13\rangle) = 2 & f(\mathfrak{p}_{11}|\langle 13\rangle) = 2. & \end{array}$$

Die Rechenzeit der Berechnung der Maximalordnungen $\mathfrak{o}_{\mathbb{Q}[\vartheta_1]}$, $\mathfrak{o}_{\mathbb{Q}[\vartheta_2]}$ lag unter einer Sekunde. Die Berechnung der Primärdekomposition benötigte 2.849 Sekunden. Das Berechnen des Minimalpolynoms $m_\vartheta(t)$ mit Hilfe der OrderAbs Methode dauerte über 10 Sekunden.

Ein zweites Beispiel betrachtet einen etwas größeren Zahlkörper:

Beispiel B.3. ***Zahlkörper vom Grad*** 100
Betrachte den Zahlkörper $\mathbb{Q}[\vartheta]$ mit ϑ Nullstelle des Polynoms:

$m_\vartheta(t) = t^{100} + 140t^{99} + 8105t^{98} + 239186t^{97} + 3248250t^{96} - 3954574t^{95} - 6$
$81054897t^{94} - 5165679899t^{93} + 55480553506t^{92} + 726870414069t^{91} - 32059$
$05749313t^{90} - 50893981096350t^{89} + 2076278089520 98t^{88} + 188950543163485$
$7t^{87} - 11858457648642766t^{86} - 9649200382884743t^{85} + 265786312513280973$
$t^{84} - 127136715089402 4826t^{83} + 5314941241684072336t^{82} - 201461459973801$
$26059t^{81} + 5888975788220 3936179t^{80} - 1549220572995594 32343t^{79} + 4059671$
$20024620842338t^{78} - 9185081933357528 50686t^{77} + 1920677118201743651812$
$t^{76} - 4007769539415785312041t^{75} + 6932934685661199201995t^{74} - 113480315$
$88667971847002t^{73} + 2100981743300842248 8826t^{72} - 2886700868840259862 2$
$408t^{71} + 2743229449248214160012 0t^{70} - 6540517880657012757025 5t^{69} + 1938$
$6483452570239089385 1t^{68} - 2611381196680301432294 11t^{67} + 2163168356417$
$86063733271t^{66} + 1313250659758780436011 63t^{65} - 2505953589020253766188 7$
$54t^{64} + 5196911165003797201413737t^{63} - 1685685003637604929864280t^{62} - 1$
$92189230691396180007776 5t^{61} - 1108436484110880490196394 8t^{60} + 2524905$
$18062067564594041 85t^{59} - 8088797983994793006513003 5t^{58} + 258000033439$
$55244927591126 8t^{57} - 4281907793132430998162079 17t^{56} + 785770103064464$
$377930986841t^{55} - 1301082994305606518393111067t^{54} + 1322297512868155 8$
$75866927338t^{53} - 1010476301464132015257543761t^{52} + 329366390818426117$
$3273886892t^{51} - 4536725830788255737967593244t^{50} - 2045546441259957999$
$034638544t^{49} + 1757968503741510108487541 9823t^{48} - 3978775147387380290$
$2261978565t^{47} + 7217001164532790177542525 5627t^{46} - 116520183559390447$
$038337889397t^{45} + 1850496597755956081724947 88050t^{44} - 218206583920714$
$194876230097055t^{43} + 1865556738042613093570173 19170t^{42} - 355449258769$
$566780237228807610t^{41} + 8604587222833451618489677742 03t^{40} - 156594343$
$2587525926975688042152t^{39} + 2404901473025399607234437 9187 58t^{38} - 2877$

$$377059253685344480794428473t^{37}+306612650416500716543721431408 0t^{36}-455704757928469987509145194491 1t^{35}+65766258455505587158858418179 79t^{34}-70837884701049104713011643757 64t^{33}+79187090479238408175281740 47447t^{32}-95621664859764026992981296 94288t^{31}+12772765221661524325456209090295t^{30}-17354066070009747610741300882181t^{29}+20578102150452378945769285674977t^{28}-20749522076541550452196740153434t^{27}+2068427921467149940464669825662 3t^{26}-19188297239653832288109462229927t^{25}+163789554116125721685164266439 49t^{24}-13548413678390972330952202101353t^{23}+44010047317235463597221480196 76t^{22}-16727031537752477134360256632 52t^{21}+93922252905206971257587612822t^{20}+2898830910161593868912675578726t^{19}+31813527263057900223515011483 30t^{18}+26375228572410053094326341850 97t^{17}+13112851828096563329527692612 53t^{16}+37986425039644235244112354012 4t^{15}+37810247857555139534538046069 3t^{14}-27588090312399763005602257200 5t^{13}+37925627016400252270612063858 7t^{12}+10436457428590985055583257739 7t^{11}+80556133923588872476341017816t^{10}+438901372336869540713569302 94t^{9}-23204431990425050385798881087t^{8}-8035499645750153711731120422t^{7}-38678684531499817866018344 95t^{6}-1122972802509163797977026423t^{5}+89807693082536571784382336 0t^{4}-11118361687048017190747184 8t^{3}+93769158764957646056303732t^{2}-109248380226222350682601 71t+188304997634436783238017 1.$$

Der Zahlkörper $\mathbb{Q}[\vartheta]$ *kann dargestellt werden als Kompositum von* $\mathbb{Q}[\vartheta_1]$ *und* $\mathbb{Q}[\vartheta_2]$*, wobei* ϑ_1 *und* ϑ_2 *Nullstellen der Polynome*

$$m_{\vartheta_1}(t) = t^{10}+19t^9+11t^8+5t^7-6t^6-18t^5-6t^4+17t^3+18t^2+5t-16$$

und

$$m_{\vartheta_2}(t) = t^{10}-5t^9+3t^8-7t^7+12t^6-3t^5+7t^4+17t^3-6t^2-9t+5$$

sind.

Die Diskriminanten von $\mathbb{Q}[\vartheta_1]$ *und* $\mathbb{Q}[\vartheta_2]$ *sind teilerfremd, und es gilt:*

$$\begin{aligned}\operatorname{disc}(\mathbb{Q}[\vartheta]) = {} & 18263252999987113366928444843979954856697389680051288702746466128775781188277357069621584414176190377960885693304325026070756740006254549110273259794505333678769639196220645400842405080354881916095777232339847187610922279856127691357304549196438769432267372712852650427239397281679335707884898174418291436591904408657350620322432913421048685599336019482309947549304381656938537339361401124213347895661797562684122771060710232817971565522828513432256181372840053956126393314070112985753080896001247883960914855468211972369492189216978586895257600000000000.$$

Die Primteiler dieser Diskriminante sind:

$$\{2,\ 3,\ 5,\ 11,\ 113,\ 433,\ 883,\ 1848550883,\\ 32396271419,\ 36159115591,\ 272610510906919\}.$$

Der Index $[\mathfrak{o}_{\mathbb{Q}[\vartheta_1,\vartheta_2]} : \mathbb{Z}[\vartheta_1,\vartheta_2]]$ *ist* 1. *Die kleinste Primzahl, welche kein Indexteiler ist und nicht verzweigt ist, ist die* 7. *Diese zerlegt sich wie folgt:*

$$\langle 7\rangle_{\mathfrak{o}_{\mathbb{Q}[\vartheta_1,\vartheta_2]}} = \mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_{16}$$

mit

$\mathfrak{p}_1 = \langle 7,\ \vartheta_1 + 3,\ {\vartheta_2}^4 + 3{\vartheta_2}^3 + 2\vartheta_2 + 3\rangle_{\mathfrak{o}_{\mathbb{Q}[\vartheta_1,\vartheta_2]}}$

$\mathfrak{p}_2 = \langle 7,\ \vartheta_1 + 3,\ {\vartheta_2}^6 + 6{\vartheta_2}^5 + 6{\vartheta_2}^4 + {\vartheta_2}^3 + {\vartheta_2}^2 + 6\vartheta_2 + 4\rangle_{\mathfrak{o}_{\mathbb{Q}[\vartheta_1,\vartheta_2]}}$

$\mathfrak{p}_3 = \langle 7,\ {\vartheta_1}^3 + 6{\vartheta_1}^2 + \vartheta_1 + 2,\ {\vartheta_2}^4 + 3{\vartheta_2}^3 + 2\vartheta_2 + 3\rangle_{\mathfrak{o}_{\mathbb{Q}[\vartheta_1,\vartheta_2]}}$

$\mathfrak{p}_4 = \langle 7,\ {\vartheta_1}^2 + 6\vartheta_1{\vartheta_2}^5 + \vartheta_1{\vartheta_2}^4 + \vartheta_1{\vartheta_2}^3 + 4\vartheta_1{\vartheta_2}^2 + \vartheta_1 + {\vartheta_2}^5 + 6{\vartheta_2}^4 + 6{\vartheta_2}^3 + 3{\vartheta_2}^2 + 3,\ {\vartheta_2}^6 + 6{\vartheta_2}^5 + 6{\vartheta_2}^4 + {\vartheta_2}^3 + {\vartheta_2}^2 + 6\vartheta_2 + 4\rangle_{\mathfrak{o}_{\mathbb{Q}[\vartheta_1,\vartheta_2]}}$

$\mathfrak{p}_5 = \langle 7,\ {\vartheta_1}^2 + \vartheta_1{\vartheta_2}^5 + 6\vartheta_1{\vartheta_2}^4 + 6\vartheta_1{\vartheta_2}^3 + 3\vartheta_1{\vartheta_2}^2 + 6{\vartheta_2}^5 + {\vartheta_2}^4 + {\vartheta_2}^3 + 4{\vartheta_2}^2 + 4,\ {\vartheta_2}^6 + 6{\vartheta_2}^5 + 6{\vartheta_2}^4 + {\vartheta_2}^3 + {\vartheta_2}^2 + 6\vartheta_2 + 4\rangle_{\mathfrak{o}_{\mathbb{Q}[\vartheta_1,\vartheta_2]}}$

$\mathfrak{p}_6 = \langle 7,\ \vartheta_1 + 6{\vartheta_2}^5 + 5{\vartheta_2}^4 + 3{\vartheta_2}^3 + 2{\vartheta_2}^2 + 4\vartheta_2 + 2,\ {\vartheta_2}^6 + 6{\vartheta_2}^5 + 6{\vartheta_2}^4 + {\vartheta_2}^3 + {\vartheta_2}^2 + 6\vartheta_2 + 4\rangle_{\mathfrak{o}_{\mathbb{Q}[\vartheta_1,\vartheta_2]}}$

$\mathfrak{p}_7 = \langle 7,\ \vartheta_1 + 6{\vartheta_2}^5 + {\vartheta_2}^4 + {\vartheta_2}^3 + 4{\vartheta_2}^2 + 5,\ {\vartheta_2}^6 + 6{\vartheta_2}^5 + 6{\vartheta_2}^4 + {\vartheta_2}^3 + {\vartheta_2}^2 + 6\vartheta_2 + 4\rangle_{\mathfrak{o}_{\mathbb{Q}[\vartheta_1,\vartheta_2]}}$

$\mathfrak{p}_8 = \langle 7,\ \vartheta_1 + 5{\vartheta_2}^5 + {\vartheta_2}^4 + 2{\vartheta_2}^3 + \vartheta_2 + 2,\ {\vartheta_2}^6 + 6{\vartheta_2}^5 + 6{\vartheta_2}^4 + {\vartheta_2}^3 + {\vartheta_2}^2 + 6\vartheta_2 + 4\rangle_{\mathfrak{o}_{\mathbb{Q}[\vartheta_1,\vartheta_2]}}$

$\mathfrak{p}_9 = \langle 7,\ \vartheta_1 + 3{\vartheta_2}^5 + {\vartheta_2}^4 + 2{\vartheta_2}^3 + 5{\vartheta_2}^2 + 2\vartheta_2 + 2,\ {\vartheta_2}^6 + 6{\vartheta_2}^5 + 6{\vartheta_2}^4 + {\vartheta_2}^3 + {\vartheta_2}^2 + 6\vartheta_2 + 4\rangle_{\mathfrak{o}_{\mathbb{Q}[\vartheta_1,\vartheta_2]}}$

$\mathfrak{p}_{10} = \langle 7,\ \vartheta_1 + {\vartheta_2}^5 + 6{\vartheta_2}^4 + 6{\vartheta_2}^3 + 3{\vartheta_2}^2 + 4,\ {\vartheta_2}^6 + 6{\vartheta_2}^5 + 6{\vartheta_2}^4 + {\vartheta_2}^3 + {\vartheta_2}^2 + 6\vartheta_2 + 4\rangle_{\mathfrak{o}_{\mathbb{Q}[\vartheta_1,\vartheta_2]}}$

$\mathfrak{p}_{11} = \langle 7,\ \vartheta_1 + 4{\vartheta_2}^3 + 3{\vartheta_2}^2 + 5\vartheta_2 + 4,\ {\vartheta_2}^4 + 3{\vartheta_2}^3 + 2\vartheta_2 + 3\rangle_{\mathfrak{o}_{\mathbb{Q}[\vartheta_1,\vartheta_2]}}$

$\mathfrak{p}_{12} = \langle 7,\ \vartheta_1 + 4{\vartheta_2}^3 + 6\vartheta_2,\ {\vartheta_2}^4 + 3{\vartheta_2}^3 + 2\vartheta_2 + 3\rangle_{\mathfrak{o}_{\mathbb{Q}[\vartheta_1,\vartheta_2]}}$

$\mathfrak{p}_{13} = \langle 7,\ \vartheta_1 + 3{\vartheta_2}^3 + 6{\vartheta_2}^2 + 3\vartheta_2 + 5,\ {\vartheta_2}^4 + 3{\vartheta_2}^3 + 2\vartheta_2 + 3\rangle_{\mathfrak{o}_{\mathbb{Q}[\vartheta_1,\vartheta_2]}}$

$\mathfrak{p}_{14} = \langle 7,\ \vartheta_1 + 3{\vartheta_2}^3 + \vartheta_2 + 2,\ {\vartheta_2}^4 + 3{\vartheta_2}^3 + 2\vartheta_2 + 3\rangle_{\mathfrak{o}_{\mathbb{Q}[\vartheta_1,\vartheta_2]}}$

$\mathfrak{p}_{15} = \langle 7,\ \vartheta_1 + 4{\vartheta_2}^2 + \vartheta_2 + 6,\ {\vartheta_2}^4 + 3{\vartheta_2}^3 + 2\vartheta_2 + 3\rangle_{\mathfrak{o}_{\mathbb{Q}[\vartheta_1,\vartheta_2]}}$

$\mathfrak{p}_{16} = \langle 7,\ \vartheta_1 + {\vartheta_2}^2 + 5\vartheta_2,\ {\vartheta_2}^4 + 3{\vartheta_2}^3 + 2\vartheta_2 + 3\rangle_{\mathfrak{o}_{\mathbb{Q}[\vartheta_1,\vartheta_2]}}$.

Für die Trägheitsgrade gilt

$$
\begin{array}{lll}
f(\mathfrak{p}_1|\langle 7\rangle) = 4 & f(\mathfrak{p}_2|\langle 7\rangle) = 6 & f(\mathfrak{p}_3|\langle 7\rangle) = 12 \\
f(\mathfrak{p}_4|\langle 7\rangle) = 12 & f(\mathfrak{p}_5|\langle 7\rangle) = 12 & f(\mathfrak{p}_6|\langle 7\rangle) = 6 \\
f(\mathfrak{p}_7|\langle 7\rangle) = 6 & f(\mathfrak{p}_8|\langle 7\rangle) = 6 & f(\mathfrak{p}_9|\langle 7\rangle) = 6 \\
f(\mathfrak{p}_{10}|\langle 7\rangle) = 6 & f(\mathfrak{p}_{11}|\langle 7\rangle) = 4 & f(\mathfrak{p}_{12}|\langle 7\rangle) = 4 \\
f(\mathfrak{p}_{13}|\langle 7\rangle) = 4 & f(\mathfrak{p}_{14}|\langle 7\rangle) = 4 & f(\mathfrak{p}_{15}|\langle 7\rangle) = 4 \\
f(\mathfrak{p}_{16}|\langle 7\rangle) = 4. & &
\end{array}
$$

Die Rechenzeit der Berechnung der Maximalordnungen $\mathfrak{o}_{\mathbb{Q}[\vartheta_1]}$, $\mathfrak{o}_{\mathbb{Q}[\vartheta_2]}$ betrug 70 bzw. 140 Millisekunden. Die Berechnung der Primärdekomposition benötigte 3.009 Sekunden. Die Berechnung des Minimalpolynoms, um dieses anschließend modulo 7 zu faktorisieren dauerte mehrere Minuten.

Um diese Arbeit nicht mit Zahlenkolonnen zu überfrachten, wurde auf das Anführen von weiteren Beispielen in noch größeren Zahlkörpern verzichtet.

Man erkennt anhand dieser beiden Beispiele die Vorteile, die Primidealfaktorisierung in großen Zahlkörpern zu berechnen, indem man diese Zahlkörper als Komposita darstellt. Weitere Forschung auf diesem Gebiet, vielleicht auch die Berechnung anderer Invarianten von großen Zahlkörpern dargestellt als Komposita, verheißt Aussicht auf Erfolg.

Literaturverzeichnis

[Bos96] Siegfried Bosch. *Algebra 2. Auflage.* Springer, 1996.

[BR87] R. Böffgen and M.A. Reichert. Computing the Decomposition of Primes p and p-adic Absolute Values in Semi-Simple Algebras over Q. *Journal of Symbolic Computation*, 4:3–10, 1987.

[BW93] Thomas Becker and Volker Weispfenning. *Gröbner Bases: A Computational Approach to Commutative Algebra. In cooperation with Heinz Kredel.* Graduate Texts in Mathematics. 141. New York: Springer-Verlag. xxii, 574 p. , 1993.

[CLO92] David Cox, John Little, and Donal O'Shea. *Ideals, Varieties, and Algorithms. An Introduction to Computational Algebraic Geometry and Commutative Algebra.* Undergraduate Texts in Mathematics. New York: Springer-Verlag. xi, 513 p. , 1992.

[Coh93] Henri Cohen. *A Course in Computational Algebraic Number Theory.* Graduate Texts in Mathematics. 138. Springer, 1993.

[Coh00] Henri Cohen. *Advanced Topics in Computational Number Theory.* Graduate Texts in Mathematics. 193. Springer, 2000.

[DFK+97] Mario Daberkow, Claus Fieker, Jürgen Klüners, Michael E. Pohst, Katherine Roegner, Martin Schörnig, and Klaus Wildanger. KANT V4. *Journal of Symbolic Computation*, 24(3):267–283, 1997.

[Eis95] David Eisenbud. *Commutative Algebra. With a View Toward Algebraic Geometry.* Graduate Texts in Mathematics. 150. Berlin: Springer-Verlag. xvi, 785 p., 1995.

[Fri98] Carsten Friedrichs. Berechnung relativer Ganzheitsbasen mit dem Round-2-Algorithmus. Diplomarbeit, überarbeitete Version, Technische Universität Berlin, 1998.

[Fri00] Carsten Friedrichs. *Berechnung von Maximalordnungen über Dedekindringen.* Dissertation, Technische Universität Berlin, 2000.

[Gaá02] István Gaál. *Diophantine Equations and Power Integral Bases.* Birkhäuser, 2002.

[Has63] Helmut Hasse. *Zahlentheorie.* Akademie-Verlag GmbH, Berlin, 1963.

[Hop94] Andreas Hoppe. Effiziente Algorithmen zur Berechnung von Elementarteilern ganzzahliger Matrizen Implementation in GAP. Diplomarbeit, RWTH Aachen, 1994.

[Hop98] Andreas Hoppe. *Normal Forms over Dedekind Domains, Efficient Implementation in the Computer Algebra System KANT.* Dissertation, Technische Universität Berlin, 1998.

[Ist01] Michael E. Pohst István Gaál. Power Integral Bases in Orders of Composite Fields. In *To appear*, 2001.

[Knu97a] Donald E. Knuth. *The Art of Computer Programming. Vol. 1: Fundamental Algorithms. 3rd ed.* Addison-Wesley, 1997.

[Knu97b] Donald E. Knuth. *The Art of Computer Programming. Vol. 2: Seminumerical Algorithms. 3rd ed.* Addison-Wesley, 1997.

[Knu97c] Donald E. Knuth. *The Art of Computer Programming. Vol. 3: Sorting and Searching. 3rd ed.* Addison-Wesley, 1997.

[Koc00] Helmut Koch. *Number Theory. Algebraic Numbers and Functions.* Graduate Studies in Mathematics. 24. Providence, RI: American Mathematical Society (AMS). xviii, 2000.

[Lan65] Serge Lang. *Algebra.* Addison-Wesley, 1965.

[Mar77] Daniel A. Marcus. *Number Fields.* Springer, 1977.

[Mey76] Kurt Meyberg. *Algebra, Teil 2.* Mathematische Grundlagen für Mathematiker, Physiker und Ingnieure. Carl Hanser Verlag, 1976.

[Nar85] Enric Nart. On the Index of a Number Field. *Transactions of the American Mathematical Society, Volume 289, Number 1, May 1985*, 1985.

[Nar89] Władisław Narkiewicz. *Elementary and Analytic Theory of Algebraic Numbers.* Springer, second edition, 1989.

[Neu92] Jürgen Neukirch. *Algebraische Zahlentheorie.* Springer, 1992.

[Ogn94] Claudia Ognibeni. Zur Berechung der Zerlegung von Indexteilern. Diplomarbeit, Heinrich-Heine-Universität Düsseldorf, 1994.

[Poh91] Michael E. Pohst. A Note on Index Divisors. In Attila Pethö, Michael E. Pohst, Hugh C. Williams, and Horst G. Zimmer, editors, *Computational Number Theory, Proceedings of the Colloquium on Computational Number Theory, Kossuth Lajos University Debrecen, Hungary, September 4–9 1989*, pages 173–182, Berlin–New York, 1991. Walter de Gruyter.

[Poh93] Michael E. Pohst. *Computational Algebraic Number Theory.* Deutsche Mathematiker-Vereinigung: DMV-Seminar. Birkhäuser, 1993.

[PZ97] Michael E. Pohst and Hans Zassenhaus. *Algorithmic Algebraic Number Theory, First Paperback Edition.* Encyclopaedia of mathematics and its applications. Cambridge University Press, 1997.

[Ull99] P. Ullrich. Die Entdeckung der Analogie zwischen Zahl- und Funktionenkörpern: der Ursprung der Dedekind-Ringe. *Jahresbericht der Deutschen Mathematiker-Vereinigung*, 101:116–134, 1999.

[Wil97] Klaus Wildanger. *Über das Lösen von Einheiten- und Indexformgleichungen in algebraischen Zahlkörpern mit einer Anwendung auf die Bestimmung aller ganzen Punkte einer Mordellschen Kurve.* Dissertation, Technische Universität Berlin, 1997.

Index

2-Elementdarstellung, 80

Abschluss
  ganzer, 6
Algorithmus
  AlgFieker, 33
  AlgFiekerSafe, 34
  AlgKumBiv, 69
  AlgKummer, 11
  AlgKumMult, 71
  AlgOrderShort, 39
  AlgPIDecAbs, 18
  AlgPrimDec, 52
  AlgZerSepA, 19
  von Buchmann-Lenstra, 12
    für Komposita, 71
  von Ore-Pohst, 20

CNEDD
  siehe Diskriminantenteiler
    gemeinsame außerwesentliche 34

Darstellungsmatrix, 4
Dedekindring, 6
Dimension
  eines Ideals, 47
Diskriminante
  eines Zahlkörpers, 5
Diskriminantenabbildung
  eines n-Tupels, 4
Diskriminantenteiler
  gemeinsame außerwesentliche, 34
Diskriminantentest, 32, 61

Einbettung
  eines Zahlkörpers, 3
Element
  ganzes, 6
  primitives, 2
Eliminationsideal, 47

Führer
  einer Ordnung, 10

ganz-abgeschlossen, 6
  im Quotientenkörper, 6
ganze algebraische Zahl, 1
Gleichungsordnung, 3
Grad
  eines Zahlkörpers, 2

Hauptidealring, 7
Hermite-Normalform, 80
HNF
  siehe Hermite-Normalform 80
HNF-Basis, 80

Ideal
  hochgehobenes, 8
  radikales, 48
  reduzibles, 45
Index
  einer Ordnung, 3
  eines Elementes, 4
  eines Zahlkörpers, 34
Indexform, 38
Indexformgleichung, 38
  p-adische, 38
Indexteiler, 4

Kompositum
beliebiges, 61
vom vollen Grad, 61
Konjugiertenvektordarstellung
einer algebraischen Zahl, 78

Lemma
Seidenbergs Lemma 92, 49
LLL-Reduktion, 39

Matrixdarstellung
einer algebraischen Zahl, 78
Maximalordnung, 2
Minimalpolynom, 2
Minimalpolynomdarstellung
einer algebraischen Zahl, 77
Möbius-Funktion, 35

Nenner
einer algebraischen Zahl, 78
eines Ideals, 79
Norm, 4

Oberordnung
p-maximale, 37
OrderShort-Methode, 38
Ordnung, 3
Ordnungsindex, 3

p-Normaldarstellung, 80
Polynom
charakteristisches, 4
p-Radikal, 13
Primärdekomposition
Eindeutigkeit der, 46
eines Ideals, 46
Existenz der, 45
Primärideal, 44
Primärkomponente
eines Ideals, 46
eingebettete, 46
isolierte, 46

Primideal
assoziiertes, 45
das zu einem Primärideal gehörige, 45
Primidealzerlegung, 8
Primzahlen
„problematische“, 67

Radikal
eines Ideals, 45
Ring
noetherscher, 6

Satz
Kummerscher Zerlegungssatz, 10
verallgemeinerter Zerlegungssatz, 58
vom primitiven Element I, 27
vom primitiven Element II, 28
von Lasker-Noether, 45
$\mathfrak{S}$-Menge, 30
Spur, 4
$\mathfrak{S}$-Schranke, 30
Standarddarstellung
einer algebraischen Zahl, 78

Trägheitsgrad, 9

unabhängig
maximal, 47
modulo einem Ideal, 47

Verzweigungsindex, 9

Zahl
algebraische, 1
ganze algebraische, 1
Zahlen
transzendente, 2
Zahlkörper
algebraischer, 2
ZPE-Ring, 7