Berechnung von Maximalordnungen über Dedekindringen

vorgelegt von
Diplom-Mathematiker

Carsten Friedrichs

aus Detmold

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

Berlin 2000
D83

Promotionsausschuß

Vorsitzender:	Professor Dr. K.-H. Förster
Berichter:	Professor Dr. M. E. Pohst
Berichter:	Professor Dr. F. Leprévost (Grenoble)

Tag der wissenschaftlichen Aussprache: 19. Dezember 2000.

Inhaltsverzeichnis

Einleitung

Even the method of algebra with its equations, from which the correct answer, together with its proof, is deduced by reduction, is not indeed geometrical in nature, but is still constructive in a way characteristic of the science [Kant, S. 590].

Die Computeralgebra schenkt dem konstruktiven Gesichtspunkt der Mathematik besondere Beachtung. Man interessiert sich nicht alleine für Existenzaussagen wie Korollar 1.3 „In jeder separablen Algebra existiert eine Maximalordnung“, sondern ist auf der Suche nach Verfahren, mit deren Hilfe die entsprechenden Strukturen berechnet werden können, wie zum Beispiel Algorithmus 3.20.

Ausgangspunkt der vorliegenden Arbeit war die Entwicklung von generischen Algorithmen für globale Körper. Nachdem schon eine Reihe bekannter Verfahren von algebraischen Zahlkörpern auf globale Funktionenkörper übertragen worden sind (Reduktion von Ganzheitsbasen und Berechnung der Einheitengruppe [Sch96], Bestimmung der (Divisor-)Klassengruppe [Heß99]) stellte sich die Frage, ob man nicht beide Fälle gemeinsam behandeln und allgemeingültige (generische) Algorithmen formulieren könne.

Eines der zentralen Probleme ist die Berechnung des ganzen Abschluß (Maximalordnung) in globalen Körpern. Hierzu wird in dem Computeralgebra-System KASH [DFK+97] in beiden Fällen der *Round 2 Algorithmus* [Fri97] verwendet. Während der Arbeit stellte sich sehr bald heraus, daß dieses Verfahren nicht nur auf globale Körper angewendet werden kann, sondern sich allgemeiner auf ganze kommutative separable Erweiterungen von Dedekindringen übertragen läßt.

In dieser Arbeit wird ein Verfahren vorgestellt, daß in noch allgemeinerem Rahmen die Berechnung von Maximalordnungen ermöglicht: Ausgangspunkt ist eine separable F-Algebra A über dem Quotientenkörper F eines Dedekindringes R. Zu einer gegebenen R-Ordnung Λ kann dann mit Hilfe von Algorithmus 3.18, Algorithmus 3.20 oder Algorithmus 4.16 eine maximale R-Ordnung $\Lambda^{\max} \supseteq \Lambda$ berechnet werden.

Aufbau der Arbeit Im ersten Kapitel werden die Grundlagen für die Entwicklung der Algorithmen aufgeführt. Ein wesentlicher Unterschied zu globalen Körpern oder allgemeiner zum kommutativen Fall ist, daß die Ma-

ximalordnung in der Regel nicht eindeutig bestimmt ist. Angaben über die Anzahl der verschiedenen Maximalordnungen, die eine gegebene Ordnung enthalten, machen zum Beispiel [Bru83, Cor. 2.2] und [Rog70, Chpt. IX,§2, Thm. 2.15].

Mit der Arithmetik von Elementen und Idealen in allgemeinen Ordnungen beschäftigt sich das zweite Kapitel. Hier werden insbesondere polynomielle Verfahren für die Multiplikation (Algorithmus 2.24), Invertierung (Algorithmus 2.30 bzw. Algorithmus 2.42) und Quotientenbildung (Bemerkung 2.23) von beliebigen Idealen entwickelt. Weiterhin wird mit einer Verallgemeinerung der Aussagen aus [Zas67] (Zassenhaus hatte Ordnungen über den ganzen Zahlen betrachtet) eine wesentliche Vorarbeit für den Algorithmus zur Faktorisierung von zweiseitigen Idealen in beliebigen Ordnungen (Algorithmus 5.27) und das Maximalitätskriterium (Theorem 3.11) geleistet.

Das erste Verfahren zur Berechnung von Maximalordnungen, der *Round 1 Algorithmus*, wird im dritten Kapitel von der ursprünglichen Fassung [Zas67] (über den ganzen Zahlen) auf Ordnungen über Dedekindringen übertragen (Algorithmus 3.18 und Algorithmus 3.20). Die Hauptaussage dieses Kapitels ist das Maximalitätskriterium Theorem 3.11. Anschließend folgen einige Bemerkungen zur konstruktiven Verwendung der Lokalisierung.

Das vierte Kapitel widmet sich der Berechnung hereditärer Ordnungen und damit dem *Round 2 Algorithmus* (Algorithmus 4.16) und deren Verwendung bei der Berechnung von Maximalordnungen. Im letzten Abschnitt wird gezeigt, daß mit Algorithmus 4.16 im kommutativen Fall schon die eindeutig bestimmte Maximalordnung erzeugt werden kann und somit die Erklärung für die Namensgebung des bekannten *Round 2 Algorithmus* zur Berechnung von Maximalordnungen in globalen Körpern gegeben.

Die Berechnung des $\mathfrak{p}$-Radikals und der Primideale einer Ordnung spielen eine entscheidende Rolle im *Round 1* und *Round 2 Algorithmus*. Verfahren dazu werden in Kapitel 5 angegeben. Für die Berechnung der Primideale (Algorithmus 5.23) in beliebigen Ordnungen wird der Zusammenhang zur Faktorisierung von Indexteilern algebraischer Zahlkörper nach dem Verfahren von Buchmann-Cohen-Lenstra hergestellt. Schließlich wird als Anwendung die Faktorisierung von zweiseitigen Idealen in beliebigen Ordnungen (Algorithmus 5.27) demonstriert. Algorithmus 5.27 stellt einen konstruktiven Beweis von Theorem 2.28 „Die Menge der zweiseitigen Ideale einer Maximalordnung ist eine freie abelsche Gruppe, die von den Primidealen erzeugt wird“ dar.

Erweiterungen und Verbesserungen des *Round 2 Algorithmus* werden im sechsten Kapitel beschrieben. Hierzu zählen die Verallgemeinerung der Verfahren von Buchmann und Lenstra [BL, BL94] und die Verwendung von Potenzen des $\mathfrak{p}$-Radikals nach Trager und Bradford [Bra88, Sect. 7.4, S. 7.8]. Die Verallgemeinerung der Verfahren von Buchmann und Lenstra ist erst durch

die Entwicklung eines neuen Verfahrens zur Berechnung des $\mathfrak{m}$-Radikals (Algorithmus 6.16) allgemein möglich geworden. Mit den in der vorliegenden Arbeit beschriebenen Verfahren ist auch die Komplexität zur Berechnung der Links-Ordnung (Multiplikatorring) des $\mathfrak{m}$-Radikals von $O(n^5)$ auf $O(n^4)$ verbessert worden, vgl. Proposition 6.17, Proposition 2.18 und [BL, Thm. 3.4].

Die Arbeit wir durch Bemerkungen zur Implementierung der beschriebenen Verfahren in dem Computeralgebra-System KASH und einige Beispiele abgeschlossen.

In der gesamten Arbeit wurde größter Wert auf eine möglichst allgemeingültige Darstellung der Algorithmen gelegt. Dies erlaubt es, sich bei der Untersuchung auf die wesentlichen Teile bzw. Probleme zu konzentrieren und so eine tiefere Einsicht in die Arithmetik allgemeiner R-Ordnungen zu erhalten: Mit der Faktorisierung von ganzen zweiseitigen Idealen in beliebigen Ordnungen (Algorithmus 5.27) kristallisiert sich zum Beispiel eine weitere arithmetische Eigenschaft der Indexteiler (Bemerkung 3.15) heraus. Damit liefert diese Arbeit nicht nur einen Beitrag zur konstruktiven Algebra bzw. Zahlentheorie, sondern auch zur rein theoretischen Betrachtung. Des weiteren sind — wenn möglich — Laufzeitabschätzungen für die Algorithmen angegeben worden.

Historische Anmerkungen Schon im inzwischen vorletzten Jahrhundert beschäftigte man sich mit der Analogie zwischen Zahl- und Funktionenkörpern, wobei die betrachteten Funktionenkörper damals aus den rationalen Funktionen einer Unbestimmten mit komplexen Koeffizienten bestanden. Diese Analogie wurde erstmals 1919 von Emmy Noether in [Noe19] veröffentlicht. Der Begriff *Dedekindring* tauchte schließlich 1958 in [ZS58] auf. Siehe hierzu [Ull99, S. 130, 132].

Erste Verfahren und Ideen zur Berechnung der Maximalordnung und der Faktorisierung von Indexteilern algebraischer Zahlkörper findet man zu Beginn des letzten Jahrhundert von Berwick [Ber27] und in den zahlreichen Arbeiten von Ore [Ore23, Ore25b, Ore25a, Ore26a, Ore26b, Ore27a, Ore27b, Ore28].

Darauf aufbauend ist der *Round 4 Algorithmus* zur Berechnung der Maximalordnung in algebraischen Zahlkörpern entwickelt worden [For78, Lan78, Bö85, For87, BR87, Bra88, MN92, FL93, Mon99] und in den folgenden Jahren auf Erweiterungen lokaler Ringe übertragen worden [Hal98, Hal00]. Parallel dazu hat Pohst in [Poh91] die Ideen von Ore direkt aufgegriffen, um die Faktorisierung von Indexteilern algebraischer Zahlkörper zu bestimmen. Die neusten Entwicklungen beschreiben den *Round 4 Algorithmus* als p-adische Faktorisierung des erzeugenden Polynoms [FPR00, CG00, Pau00], wobei die

letzten beiden sogar eine Laufzeitabschätzung entwickelt haben.

Trotz der in einigen Fällen deutlich besseren Laufzeit des *Round 4 Algorithmus* (getestet für algebraische Zahlkörper) haben sowohl der *Round 1* als auch der *Round 2 Algorithmus* wesentliche Vorteile, da sie beide in einem viel allgemeineren Rahmen eingesetzt werden können: Der *Round 4 Algorithmus* ist immer an ein primitives Element bzw. erzeugendes Polynom gebunden.

Grenzen des Verfahrens Die Verfahren, die in der algebraischen Geometrie verwendet werden, um ganze Abschlüsse zu berechnen, sind dem *Round 1* bzw. *Round 2 Algorithmus* sehr ähnlich, vgl. [Vas91, dJ98, DdJGP99]. Dort wird auch eine Art Multiplikatorring von entsprechenden Idealen berechnet, um einen entsprechenden größeren Ring zu erhalten. Dies Verfahren ist in der algebraischen Geometrie unter dem Namen *Grauert-Remmert-Algorithmus* bekannt, siehe [DdJGP99, Prop. 9.1] oder den aktuellen Übersichtsartikel [Gre00, Crit. S. 266]. Im wesentlichen Unterschied zu Ordnungen über Dedekindringen sind die von Null verschiedenen Primideale nicht notwendig maximal, vgl. Theorem 2.27 und [Vas76].

Auch die Übertragung der hier beschriebenen Verfahren auf nicht notwendig kommutative Grundringe bereitet große Probleme. Ausgangspunkt für entsprechende zukünftige Untersuchungen könnten zum Beispiel [Rob68] für eine Theorie nicht-kommutativer Dedekindringe oder [vG81] für eine Bewertungstheorie nicht-kommutativer Ringe sein.

Ich möchte an dieser Stelle Herrn Prof. Dr. M. E. Pohst ganz herzlich für die Betreuung und Unterstützung während der Anfertigung dieser Arbeit danken.

Ferner danke ich Herrn Prof. Dr. F. Leprévost für die Übernahme des Koreferats, Dr. Claus Fieker und Dr. Jürgen Klüners für die Durchsicht einer vorläufigen Fassung dieser Arbeit und viele anregende Diskussionen.

Darüber hinaus bedanke ich mich für die Förderung durch ein Stipendium nach dem Nachwuchs-Förderungs-Gesetz des Landes Berlin bei den dafür zuständigen Personen.

Mein Dank gilt schließlich meinen Eltern, die mir das Studium ermöglicht haben.

Ich widme diese Arbeit meiner Freundin Susanne, die mir immer zur Seite stand, unendliches Verständnis für mich und meine Arbeit aufgebracht hat und mir Mut gemacht hat, wenn ich kein Licht mehr sah.
— Vielen Dank. —

Kapitel 1
Grundlagen

Die meisten Definitionen und Aussagen dieses Abschnitts lassen sich auch allgemeiner formulieren: Die Ergebnisse über Ordnungen und Maximalordnungen über noetherschen ganz abgeschlossenen Ringen werden zum Beispiel in [Rei75, Chpt. 2] erklärt. Die Struktursätze für halbeinfache Algebren gelten allgemeiner für nicht notwendig endlich dimensionale artinsche Algebren [Lor90, §§28,29].

Da die Darstellung von endlich erzeugten Moduln wesentlich für die algorithmische Betrachtung ist, und endlich erzeugte Moduln über Dedekindringen eine besonders einfache Form haben (vgl. Abschnitt 1.8), wird im folgenden der Grundring immer ein Dedekindring sein.

Es sei R ein Dedekindring mit Quotientenkörper $F = Q(R)$, speziell sind R und F immer kommutativ. Eine F-Algebra A heißt *endlich dimensional*, wenn sie als F-Vektorraum endlich dimensional ist. Die *Dimension* $[A : F]$ der F-Algebra A ist die Dimension des F-Vektorraums A.

Das *Zentrum* der F-Algebra A besteht aus allen Elementen der Algebra A, die mit allen anderen Elementen von A kommutieren, $\mathrm{Z}(A) = \{a \in A | ax = xa \text{ für alle } x \in A\}$. Das Zentrum ist eine F-Teilalgebra von A. F soll immer im Zentrum der Algebra A enthalten sein.

1.1 Halbeinfache und separable Algebren

Eine F-Algebra A heißt *halbeinfach*, wenn das *Jacobson-Radikal* $J(A)$ von A, also der Durchschnitt über alle maximalen Linksideale (oder Rechtsideale), trivial ist.

Eine halbeinfache F-Algebra A kann in ihre (bis auf die Reihenfolge eindeutigen) *einfachen Bestandteile* $A_i \subseteq A$ $(1 \leq i \leq v)$ zerlegt werden [Lor90, §29, Satz 1]. Für diese einfachen Bestandteile gilt $A = \bigoplus_{i=1}^{v} A_i$ mit zugehörigen *zentralen Idempotenten* $1 = \bigoplus_{i=1}^{v} e_i, e_i \in A_i$ $(1 \leq i \leq v)$ mit $e_i e_j = 0$ $(i \neq j)$ und $A_i = Ae_i$ $(1 \leq i \leq v)$. Die einfachen Bestandteile sind gerade die minimalen (zweiseitigen) Ideale der F-Algebra A. (Zum Vergleich: Ein Ring heißt *einfach*, wenn er keine nicht-trivialen zweiseitigen Ideale besitzt.)

Die Zentren $K_i = \mathrm{Z}(A_i)$ $(1 \leq i \leq v)$ der einfachen Bestandteile sind

Körper [Lor90, §29, F 59], genauer gilt: $\mathrm{Z}(A) = \bigoplus_{i=1}^{v} K_i$. Man nennt die endlich dimensionale halbeinfache F-Algebra A *separabel*, wenn die Zentren K_i $(1 \leq i \leq v)$ der einfachen Bestandteile separable Körpererweiterungen von F sind.

(1.1) **Proposition** *Eine endlich dimensionale halbeinfache Algebra A über einem vollkommenen Körper F ist separabel.*

Beweis: Die Zentren $K_i = Z(A_i)$ der einfachen Bestandteile A_i $(1 \leq i \leq v)$ der F-Algebra A sind als Unterräume des endlich erzeugten F-Vektorraums A endlich erzeugt und damit algebraische Körpererweiterungen von F, also separabel. □

1.2 Reduzierte Spur

In einer separablen F-Algebra A erhält man analog zum Zahlkörperfall eine symmetrische nicht-degenerierte Bilinearform (induziert durch die reduzierte Spur), vgl. [Bou58, Chpt. VII, §12 no. 3]:

Es seien zunächst K ein Körper und A eine endlich dimensionale *zentraleinfache* K-Algebra, also eine einfache K-Algebra, deren Zentrum gerade K entspricht. Der *Satz von Wedderburn* [Lor90, §29, Satz 5] sagt aus, daß $A \cong D^{k\times k}$ ist, mit einem Schiefkörper D/K. Weiterhin gilt $[A : K] = m^2$ für eine natürliche Zahl m [Lor90, §29, F 16].

Ein Körper L/K heißt *Zerfällungskörper* von A, wenn $L \otimes_K A \cong L^{m\times m}$ gilt [Lor90, §29, Def. 8] oder [Rei75, S. 96, 97]. Nach [Lor90, §29, Satz 17] oder [Rei75, S. 97-99] existiert zu jeder zentraleinfachen K-Algebra A ein Zerfällungskörper L/K.

Ist L ein Zerfällungskörper von A, dann heißt das charakteristische Polynom $\mathrm{P}_{L^{m\times m}/L}(1 \otimes_K x)$ *reduziertes charakteristisches Polynom* $\mathrm{Pr}_{A/K}(x)$ von $x \in A$. Es ist unabhängig von der Wahl des Zerfällungskörpers [Lor90, §29, F 23] oder [Rei75, Thm. 9.3]. Die Spur $\mathrm{T}_{L^{m\times m}/L}(1 \otimes_K x)$ ist dann die *reduzierte Spur* $\mathrm{Tr}_{A/K}(x)$ von $x \in A$.

Zu dem charakteristischen Polynom und der Spur von $x \in A$ gilt der Zusammenhang [Lor90, §29, F 23], [Rei75, Thm. 9.5] $\mathrm{P}_{A/K}(x) = \mathrm{Pr}_{A/K}(x)^m$ und daher $\mathrm{T}_{A/K}(x) = m\,\mathrm{Tr}_{A/K}(x)$.

Für eine halbeinfache K-Algebra A sei $A = \bigoplus_{i=1}^{v} A_i$ die Zerlegung von A in die einfachen Bestandteile, vgl. Abschnitt 1.1, mit dem Zentrum $\mathrm{Z}(A) = \bigoplus_{i=1}^{v} K_i$ und den Idempotenten $1 = \bigoplus_{i=1}^{v} e_i, e_i \in A_i$. A_i ist dann eine zentraleinfache K_i-Algebra. Das *reduzierte charakteristische Polynom* von $x \in A$ wird dann definiert durch $\mathrm{Pr}_{A/K}(x) := \prod_{i=1}^{v} \mathrm{N}_{K_i/K}(\mathrm{Pr}_{A_i/K_i}(xe_i))$, wobei $\mathrm{N}_{K_i/K}$ die Norm von K_i über K ist, vgl. [Rei75, Def. 9.13, (9.20)]. Für

die *reduzierte Spur* erhält man analog $\mathrm{Tr}_{A/K}(x) := \sum_{i=1}^{v} \mathrm{T}_{K_i/K}(\mathrm{Tr}_{A_i/K_i}(xe_i))$ [Rei75, (9.15), (9.22)].

Für eine separable F-Algebra A erhält man dann aus [Rei75, Thm. 9.26], daß die reduzierte Spur $\mathrm{Tr}_{A/F}$ eine symmetrische nicht-degenerierte Bilinearform auf $A \times A$ induziert.

1.3 Ordnungen, Maximalordnungen und der ganze Abschluß

Der Begriff der Ordnung in einer endlich dimensionalen Algebra ist einer der fundamentalen Begriffe in der Darstellungstheorie [CR62, CR81, CR87] und [RR79, RHD70, Rog70, Rog81, RR85]. Erstmals wurde der Begriff Ordnung von Dedekind im Jahre 1871 in [Ded71] eingeführt (vgl. [Gus81, S. 1]).

Unter einer *R-Ordnung in A* versteht man einen Teilring Λ von A, so daß R im Zentrum von Λ enthalten ist, Λ als R-Modul endlich erzeugt ist und Λ eine F-Basis von A enthält, also $F\Lambda = A$ gilt. Jedes Element einer R-Ordnung Λ in A ist ganz über R [Rei75, Thm. 8.6].

$\mathbb{Z}[t]/f\mathbb{Z}[t]$ ist zum Beispiel eine $\mathbb{Z}$-Ordnung in der $\mathbb{Q}$-Algebra $\mathbb{Q}[t]/f\mathbb{Q}[t]$, wobei f ein separables normiertes Polynom aus $\mathbb{Z}[t]$ sei. Ist G eine endliche Gruppe, dann ist die *Gruppen-Ordnung* $RG := \{\sum_{x\in G} \alpha_x x | \alpha_x \in R\}$ (formale Summe) eine R-Ordnung in der *Gruppen-Algebra* $FG := \{\sum_{x\in G} \alpha_x x | \alpha_x \in F\}$ [CR81, S. 524].

Eine R-Ordnung $\Lambda^{(\max)}$ in A heißt *maximale R-Ordnung in A* oder *R-Maximalordnung in A*, wenn sie nicht echt in einer weiteren R-Ordnung in A enthalten ist. Ist der ganze Abschluß $\mathrm{Cl}(R, A)$ eine R-Ordnung in A, so ist $\mathrm{Cl}(R, A)$ trivialerweise die einzige R-Maximalordnung in A.

Hinreichend für die Ringeigenschaft von $\mathrm{Cl}(R, A)$ ist die Kommutativität der F-Algebra A, aber selbst dann muß $\mathrm{Cl}(R, A)$ noch nicht notwendig eine R-Ordnung in A sein, ein Beispiel hierzu ist [Art50] oder [PZ89, Chpt. 4.5, Ex. 3]: Es seien p eine Primzahl, $\mathbb{F}_p$ der endliche Körper mit p Elementen und $F = \mathbb{F}_p(t, x)$ der von t und $x := \sum_{i=0}^{\infty} t^{pi^2}$ erzeugte Teilkörper von $\mathbb{F}_p((t))$. $R := \mathbb{F}_p((t)) \cap F$ ist ein Dedekindring mit Quotientenkörper F und $E := F(y)$, mit $y^p = x$, ist Teilkörper von $\mathbb{F}_p((t))$. Der ganze Abschluß $\mathrm{Cl}(R, E)$ ist über R nicht endlich erzeugt, also auch keine R-Ordnung.

Eine Antwort auf die Frage, wann $\mathrm{Cl}(R, A)$ eine R-Ordnung und damit die einzige R-Maximalordnung in A ist, gibt Proposition 1.7.

Mit der reduzierten Spur, vgl. Abschnitt 1.2, läßt sich die Diskriminante für R-Ordnungen in A definieren [Rei75, Thm. 10.1], siehe auch Seite 27. Die Separabilität ist dann eine hinreichende Voraussetzung für die Existenz von

R-Maximalordnungen:

(1.2) **Theorem** [Rei75, Thm. 10.3] *Ist $\Lambda \supseteq R$ ein Teilring der separablen F-Algebra A, so daß $F\Lambda = A$ und jedes Element von Λ ganz über R ist, dann ist Λ eine R-Ordnung in A. Umgekehrt hat jede R-Ordnung in A diese Eigenschaften.*

(1.3) **Korollar** [Rei75, Cor. 10.4] *Jede R-Ordnung in der separablen F-Algebra A ist in einer maximalen R-Ordnung enthalten. Es existiert also mindestens eine R-Maximalordnung in A.*

Auf der anderen Seite ist die Separabilität aber keine notwendige Voraussetzung, wie man an dem folgenden Beispiel [CR81, S. 563] sieht: Es seien $F = \mathbb{F}_p(t)$ der Funktionenkörper in einer Variablen über dem endlichen Körper mit p Elementen und $R = \mathbb{F}_p[t]$. Dann ist $A := F(y)$ mit $y^p = t$ eine inseparable Erweiterung von F, aber $\Lambda := R[y] = \mathbb{F}_p[t, y] = \mathbb{F}_p[y]$ ist ein Hauptidealring und damit ganz abgeschlossen in seinem Quotientenkörper A. Wegen $\Lambda = \mathrm{Cl}(R, A)$ ist also Λ die einzige Maximalordnung in der inseparablen Erweiterung A/F.

Betrachtet man die einfachen Bestandteile der F-Algebra A, so lassen sich die Aussagen von Theorem 1.2 und Korollar 1.3 noch verfeinern:

(1.4) **Theorem** [Rei75, Thm. 10.5] *Für die separable F-Algebra A seien $R_i = \mathrm{Cl}(R, \mathrm{Z}(A_i))$ $(1 \leq i \leq v)$ die ganzen Abschlüsse von R in den Zentren der einfachen Bestandteile. Dann gelten:*

(1) Für jede maximale R-Ordnung Λ in A gilt $\Lambda = \bigoplus_{i=1}^{v} \Lambda e_i$, wobei Λe_i maximale R-Ordnungen in A_i $(1 \leq i \leq v)$ sind.

(2) Sind Λ_i $(1 \leq i \leq v)$ maximale R-Ordnungen in A_i, dann ist $\bigoplus_{i=1}^{v} \Lambda_i$ eine maximale R-Ordnung in A.

(3) Eine R-Ordnung Λ_i in A_i ist genau dann eine maximale R-Ordnung, wenn sie eine maximale R_i-Ordnung in A_i ist.

Ein Beispiel für die Nicht-Existenz von Maximalordnungen liefert

(1.5) **Proposition** [RHD70, Chpt. IV, Lem. 4.7] *Ist A eine endlich dimensionale F-Algebra, deren Jacobson-Radikal nicht trivial ist (A also nicht halbeinfach ist), dann existiert keine maximale R-Ordnung in A.*

Zur Illustration dieser Aussage zieht man ein Beispiel aus [Rei75, S. 128] heran: In der Situation von Proposition 1.5 sei Λ eine beliebige R-Ordnung in A, weiterhin sei $r \in R \setminus R^\times$ und $L_k := \Lambda \cap J(A)^k$ $(k \geq 1)$. Da das Jacobson-Radikal (einer artinschen Algebra) nilpotent ist [Lor90, §28, Satz 4], existiert $n \geq 1, J(A)^n \neq 0, J(A)^{n+1} = 0$. Dann sind $\Lambda_k := \Lambda + r^{-k}L_1 + r^{-2k}L_2 + \cdots + r^{-nk}L_n, (k \geq 0)$ alles R-Ordnungen in A und es gilt: $\Lambda = \Lambda_0 \subset \Lambda_1 \subset \ldots$.

Aus Theorem 1.2 leitet man die folgenden Aussagen leicht ab:

(1.6) **Korollar** [CR81, Cor. 26.9] *Ist Λ ein Teilring der separablen F-Algebra A, der R enthält, und als R-Modul endlich erzeugt ist, dann ist Λ in einer R-Maximalordnung enthalten.*

(1.7) **Proposition** [PZ89, Chpt. 4, Thm. 5.19], [CR81, Prop. 26.10] *Es sei A eine kommutative separable F-Algebra, dann existiert eine eindeutig bestimmte R-Maximalordnung, diese ist gleich dem ganzen Abschluß $\mathrm{Cl}(R, A)$.*

Für einen Zahlkörper F und den Ring $R = \mathrm{Cl}(\mathbb{Z}, F)$ der ganzen Zahlen von F ist nach Proposition 1.1 jede endlich dimensionale halbeinfache Algebra A separabel und jede R-Ordnung in A ist in einer Maximalordnung enthalten.

1.4 Existenz und Erzeugung von Ordnungen

Es sei V ein endlich dimensionaler F-Vektorraum. Ein *R-Gitter* in V ist ein endlich erzeugter torsionsfreier R-Modul, der in V enthalten ist. Ein *volles R-Gitter* in V ist ein R-Gitter $\Lambda \subseteq V$, das eine F-Basis von V enthält [Bou72, Chpt. VII,§4.1]. Für $V = F$ sind die vollen R-Gitter in F genau die gebrochenen Ideale von R.

(1.8) **Korollar** *$\Lambda \subset A$ ist genau dann eine R-Ordnung, wenn Λ sowohl ein Ring ist, der R enthält, als auch ein volles R-Gitter in A ist.*

Für ein volles R-Gitter Λ in A definiert man die *Links-* beziehungsweise *Rechts-Ordnung* von Λ als $\mathcal{O}_l(\Lambda) := \{a \in A | a\Lambda \subseteq \Lambda\}$ beziehungsweise $\mathcal{O}_r(\Lambda) := \{a \in A | \Lambda a \subseteq \Lambda\}$, diese heißen auch *linker* beziehungsweise *rechter Multiplikatorring* von Λ.

Ein volles R-Gitter Λ kann man leicht erzeugen: Es sei $\omega_1, \ldots, \omega_n \in A$ eine F-Basis von A. Dann ist $\Lambda := \bigoplus_{i=1}^n R\omega_i$ ein volles R-Gitter in A. Mit der nächsten Aussage erhält man dann die Existenz von R-Ordnungen in endlich dimensionalen F-Algebren.

(1.9) **Proposition** [RHD70, Chpt. IV,Lem. 1.3] *Ist Λ ein volles R-Gitter in der endlich dimensionalen F-Algebra A, dann sind sowohl die Links- als auch die Rechts-Ordnung von Λ R-Ordnungen in A.*

(1.10) **Bemerkung** *Zusammen mit Korollar 2.17 erhält man dadurch nicht nur die Existenz von R-Ordnungen in beliebigen endlich dimensionalen F-Algebren, sondern auch ein Verfahren, mit dem man immer eine R-Ordnung in A ausrechnen kann.*

Dies erlaubt unter anderem auch die Berechnung einer Ordnung in einer F-Algebra, die von einem nicht normierten Polynom aus $F[t]$ erzeugt wird.

1.5 Endliche Erweiterungen von Dedekindringen

In diesem Abschnitt soll das folgende Problem betrachtet werden: Gegeben sei eine (als R-Modul) endlich erzeugte torsionsfreie R-Algebra Λ, für die R im Zentrum von Λ liegt. Gibt es eine F-Algebra A, so daß Λ eine R-Ordnung in A ist?

Aus der Definition folgt sofort, daß die Elemente von Λ ganz über R sind [Lor96, §16, F1]. Um die Eigenschaft des vollen Gitters zu erhalten, setzt man $A := F \otimes_R \Lambda$, wobei man $F \otimes_R \Lambda$ wegen der fehlenden Torsion auch mit $K\Lambda = \{\alpha x | \alpha \in K, x \in \Lambda\}$ identifizieren kann [CR81, S. 523]. A ist eine endlich dimensionale F-Algebra und Λ eine R-Ordnung in A.

Um mit dieser Konstruktion eine halbeinfache F-Algebra zu erhalten, muß man voraussetzten, daß in Λ keine nilpotenten Ideale außer $\{0\}$ existieren [Zas72, Prop. 2.3, S. 398].

Für den Rest dieser Arbeit sei, wenn nichts anderes angegeben wird, A eine (nicht notwendig kommutative) separable F-Algebra der Dimension n.

1.6 Gebrochene Ideale in Dedekindringen

Über gebrochene Ideale in kommutativen Ringen und ganzen Erweiterungen von kommutativen Ringen kann man in [Gil72], [LM71] oder [Nor63] lesen. Hier soll nur kurz auf die gebrochenen Ideale in dem Dedekindring R eingegangen werden. Die allgemeineren (gebrochenen) Ideale in Ordnungen werden in Abschnitt 2.4 behandelt.

Um die Schreibweise zu vereinfachen wird in natürlicher Weise das Nullideal $\{0\}$ im folgenden immer ausgeschlossen, wenn von Idealen von R die

Rede ist. Ein *gebrochenes Ideal* von R ist ein volles R-Gitter in F, vgl. Abschnitt 1.4. Die *ganzen Ideale* von R sind die gebrochenen Ideale $\mathfrak{a}$ mit $\mathfrak{a} \subseteq R$.

Ein gebrochenes Ideal $\mathfrak{a}$ eines beliebigen Ringes S heißt *regulär*, wenn es mindestens ein von Null verschiedenes Element enthält, das kein Nullteiler ist. Die gebrochenen Ideale eines Dedekindringes sind damit trivialerweise regulär. Weiterhin lassen sich die gebrochenen Ideale $\mathfrak{a}$ von R bis auf die Reihenfolge eindeutig als Produkt von Primidealen schreiben: $\mathfrak{a} = \prod_{i=1}^{r} \mathfrak{p}_i^{e_i}, e_i \neq 0\ (1 \leq i \leq r)$.

Die Primideale von R sind gerade die maximalen Ideale von R. Anders ausgedrückt sind Dedekindringe noethersche Ringe mit Dimension 1 [AM69, Chpt. 9].

(1.11) **Proposition** [AM69, Chpt. 9, Ex. 7] *Für ein beliebiges ganzes Ideal $\mathfrak{a}$ von R ist $R/\mathfrak{a}$ ein Ring, in dem jedes Ideal von einem Element erzeugt wird.*

Da $R/\mathfrak{a}$ in Proposition 1.11 im allgemeinen nicht nullteilerfrei ist, ist $R/\mathfrak{a}$ kein Hauptidealring (Principal Ideal Domain, PID) sondern nur ein *Principal Ideal Ring (PIR)*.

(1.12) **Korollar 2-Element Darstellung** [Nar89, Chpt. 1, §1, Cor. 5, S. 10], [OMe63, 22:5a] *Jedes gebrochene Ideal $\mathfrak{a}$ von R läßt sich durch zwei Elemente $a, b \in F$ darstellen: $\mathfrak{a} = aR + bR$.*

1.7 Komplexitätsanalyse

Bei der Betrachtung von Algorithmen spielt die Abschätzung der Laufzeit in der Größe der Eingabedaten eine entscheidende Rolle, sie wird auch *Komplexitätsanalyse* genannt. Zentraler Bestandteil der Komplexitätsanalyse ist die Funktion O (*groß-O Notation)*. Sie wurde 1892 von Bachmann in [Bac92] eingeführt, vgl. [Knu77, Sect. 1.2.11.1, S. 104].

Für die Funktionen $f, g : \mathbb{N} \to \mathbb{N}$ gilt $g(n) = O(f(n))$ genau dann, wenn zwei Konstanten $c, N > 0$ existieren, mit $g(n) \leq cf(n)$ für alle $n \geq N$. Diese Definition findet man auch in [BS96, Def. 2.4.1] und [AHU74].

In dieser Arbeit werden Algebren und Ordnungen über dem Grundkörper F bzw. dem Dedekindring R betrachtet. Unter *Elementaroperationen* in F versteht man die Arithmetik mit Elementen von F (Addition, Subtraktion, Multiplikation, Division), wie auch Arithmetik mit gebrochenen Idealen von R (Addition, Multiplikation, Division). Betrachtet man die Darstellung von gebrochenen Idealen mit zwei Elementen (Korollar 1.12) oder auch die sogenannte *P-Normal Darstellung* und die daraus resultierende Arithmetik,

vgl. [PZ89, S. 400-405] oder [Poh93, S. 65,66], so sieht man, daß die Idealoperationen durchaus zu den Elementaroperationen gezählt werden können.

Die Komplexität wird immer in Elementaroperationen des Grundkörpers F angegeben. Da im allgemeinen keine Abschätzungen für die Arithmetik im Grundkörper F gegeben sind, wird die *Bit-Komplexität*, also die Anzahl der Binäroperationen, hier nicht betrachtet.

Bei der Arithmetik mit Matrizen über F „genügen“ die trivialen einfachen Verfahren, Multiplikation von zwei $n \times n$-Matrizen in $O(n^3)$ Elementaroperationen, Invertierung einer $n \times n$-Matrix in $O(n^3)$ Elementaroperationen, vgl. [Coh96a, Alg. 2.2.2] und Berechnung des Kerns einer $n \times m$-Matrix in $O(nm^2)$ Elementaroperationen, vgl. [Coh96a, Alg. 2.3.1].

Schnellere Verfahren, wie zum Beispiel die *Strassen-Multiplikation*, die zwei $n \times n$-Matrizen in $O(n^{\log(7)})$ Elementaroperationen multipliziert [AHU74, Thm. 6.1], sind nicht notwendig. Für die Analyse der Algorithmen, die in dieser Arbeit entwickelt werden, sind nur obere Abschätzungen notwendig. Die anderen Teile der Algorithmen werden immer eine mindestens genauso große Komplexität haben, vgl. auch Bemerkung 2.4.

1.8 Darstellung von Moduln und Gittern über Dedekindringen

Voraussetzung für die algorithmische Betrachtung von R-Ordnungen und R-Gittern ist eine vernünftige Darstellung. Es sei $\mathcal{M}$ ein volles R-Gitter in dem F-Vektorraum V der Dimension m.

(1.13) **Proposition** [OMe63, 81:3] *$\mathcal{M}$ läßt sich darstellen als $\mathcal{M} = \bigoplus_{i=1}^{m} \mathfrak{a}_i x_i$, mit gebrochenen Idealen $\mathfrak{a}_i$ $(1 \leq i \leq m)$ von R und einer F-Basis $x_1, \ldots, x_m$ von V.*

Ist ein R-Gitter $\mathcal{M} = \sum_{i=1}^{k} \mathfrak{a}_i x_i \subseteq V$ durch ein Erzeugendensystem gegeben, so entspricht dies der folgenden Schreibweise $\mathcal{M} = \begin{bmatrix} \mathfrak{a}_1 & \cdots & \mathfrak{a}_k \\ & M & \end{bmatrix}$, wobei $M \in F^{m \times k}$ die Matrix mit den Spalten $x_1, \ldots, x_k$ ist.

(1.14) **Korollar Pseudo-Basis** *Ein R-Gitter Λ in A läßt sich wie folgt darstellen: $\Lambda = \bigoplus_{i=1}^{m} \mathfrak{a}_i \omega_i$, wobei $\mathfrak{a}_i$ $(1 \leq i \leq m)$ gebrochene Ideale von R sind und $\omega_1, \ldots, \omega_m$ eine F-Basis des Vektorraums $F\Lambda \subseteq A$ ist.*

Ist Λ ein volles R-Gitter oder eine R-Ordnung, so gilt $m = n$ und $\omega_1, \ldots, \omega_n$ ist eine F-Basis von A.

1.8 Darstellung von Moduln und Gittern über Dedekindringen

Eine Darstellung wie in Proposition 1.13 oder Korollar 1.14 heißt *Pseudo-Basis*. Das erste konstruktive Verfahren zur Berechnung einer solchen Pseudo-Basis über Maximalordnungen in algebraischen Zahlkörpern, haben Bosma und Pohst [BP91, Alg. 2.5] aus [OMe63, 81:3] abgeleitet. Danach gab es entsprechende Weiterentwicklungen von Cohen [Coh96b, Alg. 2.6], [Coh00, Alg. 1.4.7] und Hoppe [Hop98], aber auch nur für den Fall von Maximalordnungen in algebraischen Zahlkörpern. Fieker [Fie00] liefert nicht nur die Aussage für allgemeine Dedekindringe sondern gleichzeitig eine Komplexitätsanalyse.

(1.15) **Theorem Hermite-Normal-Form** *Eine Hermite-Normal-Form eines R-Gitters $\mathcal{M}$ in V, das durch k Erzeuger gegeben ist, kann in $O(km^2)$ Elementaroperationen in F berechnet werden.*

Daraus leiten sich eine Reihe von Algorithmen für R-Gitter ab.

(1.16) **Korollar** *Für die Summe von zwei R-Gittern $\mathcal{M}_1, \mathcal{M}_2 \subseteq V$ mit k_1 bzw. k_2 Erzeugern kann in $O((k_1 + k_2)m^2)$ Elementaroperationen in F eine Hermite-Normal-Form berechnet werden.*

(1.17) **Korollar** *Für zwei volle R-Gitter $\mathcal{M}_1, \mathcal{M}_2 \subseteq V$ kann in $O(m^3)$ Elementaroperationen in F eine Hermite-Normal-Form von $\mathcal{M}_1 \cap \mathcal{M}_2$ berechnet werden.*

Beweis: Es seien $\mathcal{M}_1 = \begin{bmatrix} \mathfrak{a}_{1,1} & \cdots & \mathfrak{a}_{1,m} \\ & M_1 & \end{bmatrix}$ und $\mathcal{M}_2 = \begin{bmatrix} \mathfrak{a}_{2,1} & \cdots & \mathfrak{a}_{2,m} \\ & M_2 & \end{bmatrix}$, dann sei $\begin{bmatrix} \mathfrak{b}_1 & \cdots & \mathfrak{b}_m \\ & \tilde{M} & \end{bmatrix}$ eine Hermite-Normal-Form von $\begin{bmatrix} \mathfrak{a}_{1,1}^{-1} & \cdots & \mathfrak{a}_{1,m}^{-1} \\ & (M_1^{tr})^{-1} & \end{bmatrix} + \begin{bmatrix} \mathfrak{a}_{2,1}^{-1} & \cdots & \mathfrak{a}_{2,m}^{-1} \\ & (M_2^{tr})^{-1} & \end{bmatrix}$. Durch $\begin{bmatrix} \mathfrak{b}_1^{-1} & \cdots & \mathfrak{b}_m^{-1} \\ & (\tilde{M}^{tr})^{-1} & \end{bmatrix}$ erhält man eine Hermite-Normal-Form von $\mathcal{M}_1 \cap \mathcal{M}_2$, vgl. [OMe63, S. 231] oder [Hop98, Prop. 4.10.3].

Für die Invertierung der Matrizen sind je $O(m^3)$ für die Invertierung der Ideale $O(m)$ Elementaroperationen nötig. Korollar 1.16 liefert $O(m^3)$ Operationen für die Berechnung der Summe. Anschließend muß man noch einmal die Ideale ($O(m)$) und die Matrix ($O(m^3)$) invertieren. □

(1.18) **Theorem Smith-Normal-Form** [OMe63, Thm. 81:11], [CR81, Thm. 4.14] *Es seien $\mathcal{M}_2 \subseteq \mathcal{M}_1$ zwei volle R-Gitter in V. Dann existieren Darstellungen der Form $\mathcal{M}_1 = \bigoplus_{i=1}^m \mathfrak{a}_i x_i$ und $\mathcal{M}_2 = \bigoplus_{i=1}^m \mathfrak{b}_i \mathfrak{a}_i x_i$, mit gebrochenen Idealen $\mathfrak{a}_i$ $(1 \leq i \leq m)$ von R, einer F-Basis $x_1, \ldots, x_m$ von V und ganzen Idealen $\mathfrak{b}_m \subseteq \ldots \subseteq \mathfrak{b}_1$ von R.*

Die Ideale $\mathfrak{b}_1, \ldots, \mathfrak{b}_m$ aus Theorem 1.18 heißen *Elementarteiler-Ideale*. Einen Algorithmus zur Berechnung dieser Darstellung für Gitter über Maximalordnungen in algebraischen Zahlkörpern liefert [Coh96b, Alg. 4.4], [Coh00, Alg. 1.7.3].

Es sei $x \in F\mathcal{M}$ ein beliebiger Vektor, und $\mathcal{M} = \bigoplus_{i=1}^{k} \mathfrak{a}_i x_i$ eine Pseudo-Basis des R-Gitters $\mathcal{M}$. In [OMe63, §81B, S. 210] wird gezeigt, daß das *Koeffizientenideal* $\mathfrak{a}_x = \{\alpha \in F | \alpha x \in \mathcal{M}\}$ ein gebrochenes Ideal von R ist. Ist weiterhin $x = \sum_{i=1}^{k} \alpha_i x_i$ die Darstellung von x so kann nach [OMe63, Ex. 81:4] das Koeffizientenideal wie folgt berechnet werden:

$$\mathfrak{a}_x = \bigcap_{i=1, \alpha_i \neq 0}^{k} \mathfrak{a}_i \alpha_i^{-1}. \tag{1.19}$$

(1.20) **Proposition** *Für eine volles R-Gitter $\mathfrak{b} \subseteq A$ gilt $R \cap \mathfrak{b} \neq \{0\}$.*

Beweis: Es sei $\mathfrak{b} = \bigoplus_{i=1}^{n} \mathfrak{b}_i \eta_i$ eine Pseudo-Basis von $\mathfrak{b}$. Dann gilt $F\mathfrak{b} = A \ni 1 = \sum_{i=1}^{n} \beta_i \eta_i$. Mit (1.19) kann das Koeffizientenideal $\mathfrak{a}_1$ von 1 berechnet werden. Es gilt $F \cap \mathfrak{b} = \mathfrak{a}_1$ und weiterhin $R \cap \mathfrak{b} = R \cap \mathfrak{a}_1$. Da $\mathfrak{a}_1$ ein gebrochenes Ideal von R ist, gilt $0 \neq R \cap \mathfrak{b}$. □

Kapitel 2
Arithmetik in Ordnungen

Auf den folgenden Seiten soll die Arithmetik in nicht notwendig kommutativen Ordnungen über Dedekindringen in separablen Algebren beschrieben werden. Ein wesentlicher Teil ist dabei die Betrachtung von Idealen und deren Invertierbarkeit, da sie eine entscheidende Rolle für den *Round 1 Algorithmus* spielt.

Ein weiterer Schwerpunkt liegt auf den konstruktiven Verfahren und deren Komplexität (polynomielle Algorithmen), die es ermöglichen, Arithmetik sowohl mit Elementen als auch mit Idealen in diesen Ordnungen zu machen.

2.1 Multiplikationstabelle und Darstellungsmatrizen

Für eine feste F-Basis $\omega_1, \ldots, \omega_n$ von A bezeichnet man mit dem Begriff *Multiplikationstabelle* die n Matrizen $M(i) \in F^{n\times n}$ $(1 \leq i \leq n)$, die die Multiplikation der Basiselemente beschreiben: $\omega_i\omega_j = \sum_{k=1}^{n} M(i)_{k,j}\omega_k = (\omega_1, \ldots, \omega_n)M(i)_{(\cdot,j)}$.

Mit der Multiplikationstabelle, auch *structure constants* genannt, wird die F-Algebra A dargestellt. Diese Darstellung kann man allgemeiner für assoziative endlich dimensionale Algebren verwenden, vgl. [Pie82, Sect. 1.5 (1), S. 10].

Anders als im kommutativen Fall gibt es im allgemeinen zwei verschiedene Darstellungsmatrizen, eine für die Links-Multiplikation und eine für die Rechts-Multiplikation. Für $\gamma \in A$ heißt die Matrix $R_r(\gamma) \in F^{n\times n}$, die die Rechts-Multiplikation mit γ darstellt, *Rechts-Darstellungsmatrix*.

Für $\gamma = \sum_{i=1}^{n} \gamma_i\omega_i$ erhält man mit Hilfe der Multiplikationstabelle $\omega_j\gamma = (\omega_1, \ldots, \omega_n)M(j)(\gamma_1, \ldots, \gamma_n)^{tr}$, also

$$R_r(\gamma) = \left(M(1)(\gamma_1, \ldots, \gamma_n)^{tr}, \ldots, M(n)(\gamma_1, \ldots, \gamma_n)^{tr}\right). \tag{2.1}$$

Für die Links-Multiplikation mit γ erhält man die *Links-Darstellungsmatrix* $R_l(\gamma) \in F^{n\times n}$ ganz analog

$$R_l(\gamma) = \sum_{i=1}^{n} \gamma_i M(i). \tag{2.2}$$

Man erhält die Beziehung $M(i) = R_l(\omega_i)$ $(1 \leq i \leq n)$.

(2.3) **Proposition** *Die Komplexität für die Berechnung der Links- bzw. Rechts-Darstellungsmatrix ist $O(n^3)$, gemessen in Elementaroperationen in dem Körper F.*

Beweis: An (2.1) sieht man, daß n Matrix-Vektor-Multiplikationen zu je $O(n^2)$ Elementaroperationen nötig sind. Zur Berechnung der Links-Darstellungsmatrix sind nach (2.2) n Multiplikationen eines Koeffizienten mit einer Matrix ($O(n^2)$) und anschließend $n-1$ Additionen von $n \times n$-Matrizen ($O(n^2)$) erforderlich. □

2.2 Arithmetik mit Elementen

Da die Komplexität der Arithmetik mit Elementen einer R-Ordnung Λ in der Algebra A später gebraucht wird, soll hier kurz auf die Verfahren und ihre Komplexität eingegangen werden.

Im folgenden sei die Pseudo-Basis $\Lambda = \bigoplus_{i=1}^{n} \mathfrak{a}_i \omega_i$ von Λ fest. Elemente $x = \sum_{i=1}^{n} x_i \omega_i \in \Lambda$ werden im allgemeinen durch den *zugehörigen Koeffizientenvektor* $\vec{x} = (x_1, \ldots, x_n)^{tr} \in F^n$ dargestellt.

(2.4) **Bemerkung** *Aus praktischer Sicht sollten in einem Computeralgebra-System aber neben der Darstellung durch den Koeffizientenvektor noch andere Darstellungen für die Elemente möglich sein, zum Beispiel die sogenannte Polynomdarstellung und Produktdarstellung.*

In Spezialfällen verringern andere Darstellungen die Komplexität der Arithmetik (Division mit Polynomdarstellung vgl. [Poh93, S. 31,32] oder Multiplikation und Faktorisierung mit Produktdarstellung) entscheidend.

Allerdings sind im allgemeinen nicht alle Darstellungen möglich. Die Polynomdarstellung kann man zum Beispiel nicht im nicht-kommutativen Fall verwenden. Für die meisten Verfahren in dieser Arbeit ist der Koeffizientenvektor sogar explizit erforderlich.

In den Komplexitätsuntersuchungen der weiteren Algorithmen spielt die Arithmetik mit Elementen nicht die entscheidende Rolle, die Operationen mit R-Moduln (Hermite-Normal-Form, Theorem 1.15) haben immer eine mindestens genauso große Komplexität. Daher reichen die hier beschriebenen einfachen Verfahren für die Arithmetik mit Elementen aus. Durch schnellere Verfahren zur Addition, Subtraktion, Multiplikation oder Invertierung von Elementen kann man die Komplexität der weiteren Algorithmen nicht verringern.

(2.5) **Proposition** *Die Addition und die Subtraktion von zwei Elementen der Ordnung Λ werden komponentenweise auf den Koeffizientenvektoren durchgeführt und haben somit eine Komplexität von $O(n)$, gemessen in Elementaroperationen des Grundkörpers F.*

(2.6) **Proposition** *Der Koeffizientenvektor des Produktes zweier Elemente $x, y \in \Lambda$ ist durch $\sum_{i=1}^{n} x_i M(i)(y_1, \ldots, y_n)^{tr}$ gegeben und läßt sich in $O(n^3)$ Elementaroperationen des Grundkörpers F berechnen.*

Beweis: Aus Abschnitt 2.1 erhält man $\omega_i\omega_j = \sum_{k=1}^{n} M(i)_{k,j}\omega_k$ $(1 \leq i, j \leq n)$, also $\sum_{i=1}^{n} x_i\omega_i \cdot \sum_{i=1}^{n} y_i\omega_i = (\omega_1, \ldots, \omega_n) \sum_{i=1}^{n} x_i M(i)(y_1, \ldots, y_n)^{tr}$. Die wesentlichen Operationen sind n Matrix-Vektor-Multiplikationen zu je $O(n^2)$ Elementaroperationen. □

(2.7) **Bemerkung** *Sobald man mehr als eine Multiplikation mit dem selben $x \in \Lambda$ (von der selben Seite) durchführt, bietet es sich an, die entsprechende Darstellungsmatrix zu berechnen und zu speichern. Ist zum Beispiel die Links-Darstellungsmatrix $R_l(x)$ bekannt, erhält man den Koeffizientenvektor von $x \cdot y$ durch $R_l(x)(y_1, \ldots, y_n)^{tr}$, mit $O(n^2)$ Elementaroperationen.*

Muß man zum Beispiel n mal mit dem selben Element von rechts multiplizieren, so erhält man eine Komplexität von $O(n^3)$ an Stelle von $O(n^4)$.

(2.8) **Proposition** *Das Inverse $z = x^{-1} \in A$ von $x \in \Lambda$ erhält man, wenn es existiert, durch Lösen des linearen Gleichungs-Systems $R_l(x)(z_1, \ldots, z_n)^{tr} = (e_1, \ldots, e_n)^{tr}$ in $O(n^3)$ Schritten, wobei $1 = \sum_{i=1}^{n} e_i\omega_i$ sei.*

Beweis: Wenn $z \in A$ existiert, dann gilt $(\omega_1, \ldots, \omega_n)R_l(x)(z_1, \ldots, z_n)^{tr} = xz = 1 = (\omega_1, \ldots, \omega_n)(e_1, \ldots, e_n)^{tr}$. Sowohl die Berechnung von $R_l(x)$ als auch die Lösung des linearen Gleichungs-Systems benötigt $O(n^3)$ Operationen. □

2.3 Links- und Rechtsordnungen

Die Berechnung der Links- bzw. Rechtsordnung ist eine Verallgemeinerung der in [Zas67, S. 98] und [Fri97, Anhang A] beschriebenen Verfahren. An Stelle der Links- bzw. Rechtsordnung sollen hier die *Quotienten* $(\mathfrak{a}/\mathfrak{b}) := \{x \in A | x\mathfrak{b} \subseteq \mathfrak{a}\}$ bzw. $(\mathfrak{b}\backslash\mathfrak{a}) := \{x \in A | \mathfrak{b}x \subseteq \mathfrak{a}\}$ berechnet werden, denn es gelten: $\mathcal{O}_l(\Lambda) = (\Lambda/\Lambda)$ und $\mathcal{O}_r(\Lambda) = (\Lambda\backslash\Lambda)$, wobei $\mathfrak{a}, \mathfrak{b}$ und Λ volle R-Gitter in der Algebra A sind.

(2.9) **Proposition** *Sind $\mathfrak{a}$ und $\mathfrak{b}$ volle R-Gitter in der Algebra A, so sind auch die Quotienten $(\mathfrak{a}/\mathfrak{b})$ und $(\mathfrak{b}\backslash\mathfrak{a})$ volle R-Gitter.*

Beweis: Die Gitter Eigenschaft ist unmittelbar klar, deshalb wird hier nur die Existenz einer F-Basis von A in dem Quotienten $(\mathfrak{a}/\mathfrak{b})$ gezeigt.

Es sei $y \in A$ beliebig, dann ist sicherlich $y\mathfrak{b}$ ein R-Gitter. Für jedes Element $x \in y\mathfrak{b}$ existiert ein $r \in R$ mit $rx \in \mathfrak{a}$, da $\mathfrak{a}$ ein volles R-Gitter ist. Da mit $\mathfrak{b}$ auch $y\mathfrak{b}$ endlich erzeugt ist, existiert auch ein $\bar{r} \in R$ mit $\bar{r}y\mathfrak{b} \subseteq \mathfrak{a}$, also liegt $\bar{r}y$ in $(\mathfrak{a}/\mathfrak{b})$ und damit auch eine F-Basis von A. □

(2.10) **Bemerkung** *Im Beweis der vorangegangenen Proposition ist die Existenz einer Pseudo-Basis der Gitter $\mathfrak{a}$ und $\mathfrak{b}$ nicht verwendet worden. Die Aussage gilt also allgemeiner auch für noethersche Ringe R.*

Es seien $\mathfrak{a} = \bigoplus_{i=1}^{n} \mathfrak{a}_i\alpha_i$ und $\mathfrak{b} = \bigoplus_{i=1}^{n} \mathfrak{b}_i\beta_i$ Pseudo-Basen des vollen Gitters $\mathfrak{a}$ bzw. des Gitters $\mathfrak{b}$. Weiterhin wird eine F-Basis $\omega_1, \ldots, \omega_n$ von A fixiert. Im folgenden wird der Algorithmus zur Berechnung des Quotienten $(\mathfrak{a}/\mathfrak{b})$ beschrieben, die Berechnung von $(\mathfrak{b}\backslash\mathfrak{a})$ erfolgt analog.

Für ein beliebiges Element $\gamma \in A$ sei $R_r(\gamma)$ die Rechts-Darstellungsmatrix bezüglich der F-Basis $\omega_1, \ldots, \omega_n$. Des weiteren sei $S \in F^{n\times n}$ die Matrix, die die F-Basis $\omega_1, \ldots, \omega_n$ in die F-Basis $\alpha_1, \ldots, \alpha_n$ überführt, also $(\omega_1, \ldots, \omega_n)S = (\alpha_1, \ldots, \alpha_n)$.

Zu einem beliebigen $x = \sum_{i=1}^{n} x_i\omega_i \in A$ sei $\vec{x}$ der Koeffizientenvektor. In dieser Darstellung gilt dann

$$x\beta_i = \sum_{j=1}^{n} x_j\omega_j\beta_i = \sum_{j=1}^{n} x_j(\omega_1, \ldots, \omega_n)R_r(\beta_i)_{\cdot,j} \tag{2.11}$$

$$= \sum_{j=1}^{n} x_j(\alpha_1, \ldots, \alpha_n)S^{-1}R_r(\beta_i)_{\cdot,j} = \sum_{k=1}^{n} \alpha_k(S^{-1}R_r(\beta_i))_{k,\cdot}\vec{x}, \tag{2.12}$$

wobei $R_r(\beta_i)_{\cdot,j}$ die j-te Spalte von $R_r(\beta_i)$ und $(S^{-1}R_r(\beta_i))_{k,\cdot}$ die k-te Zeile von $S^{-1}R_r(\beta_i)$ bezeichnen. Hieraus erhält man $x\mathfrak{b} = \bigoplus_{i=1}^{n} x\mathfrak{b}_i\beta_i = \bigoplus_{i=1}^{n} \mathfrak{b}_i \sum_{k=1}^{n} \alpha_k(S^{-1}R_r(\beta_i))_{k,\cdot}\vec{x}$ und damit $x\mathfrak{b} \subseteq \mathfrak{a}$ genau dann, wenn

$$(1 \le i, k \le n)\ \mathfrak{b}_i(S^{-1}R_r(\beta_i))_{k,\cdot}\vec{x} \subseteq \mathfrak{a}_k \tag{2.13}$$

genau dann, wenn

$$(1 \le i, k \le n)\ \mathfrak{b}_i/\mathfrak{a}_k(S^{-1}R_r(\beta_i))_{k,\cdot}\vec{x} \subseteq R. \tag{2.14}$$

Mit der Matrix

$$M_r := \begin{pmatrix} S^{-1}R_r(\beta_1) \\ \hline \vdots \\ \hline S^{-1}R_r(\beta_n) \end{pmatrix} \tag{2.15}$$

erhält man dann die Äquivalenz zu: Für jedes Element y des R-Gitters $\mathcal{M}_r := \begin{bmatrix} (\mathfrak{b}_1/\mathfrak{a}_1) & \cdots & (\mathfrak{b}_1/\mathfrak{a}_n) & (\mathfrak{b}_2/\mathfrak{a}_1) & \cdots & (\mathfrak{b}_n/\mathfrak{a}_n) \\ & & M_r^{tr} & & & \end{bmatrix}$ gilt $\vec{x}^{tr} \cdot y \in R$. Diese Äquivalenz bleibt natürlich durch Anwendung der Hermite-Normal-Form für Moduln über Dedekindringen (Theorem 1.15) unverändert, so daß $x \in (\mathfrak{a}/\mathfrak{b})$ genau dann gilt, wenn für jedes Element y des R-Gitters $\begin{bmatrix} \mathfrak{c}_1 & \cdots & \mathfrak{c}_n \\ & \tilde{M}_r & \end{bmatrix} := \mathrm{HNF}(\mathcal{M}_r)$ die Bedingung $\vec{x}^{tr} \cdot y \in R$ erfüllt ist, also genau dann, wenn $\vec{x} \in \begin{bmatrix} 1/\mathfrak{c}_1 & \cdots & 1/\mathfrak{c}_n \\ & \left(\tilde{M}_r^{tr}\right)^{-1} & \end{bmatrix}$ gilt. Abschließend erhält man $(\mathfrak{a}/\mathfrak{b}) = \bigoplus_{i=1}^{n}(1/\mathfrak{c}_i)\gamma_i$, wobei $(\gamma_1, \ldots, \gamma_n) := (\omega_1, \ldots, \omega_n)\left(\tilde{M}_r^{tr}\right)^{-1}$.

Zur Berechnung des Quotienten $(\mathfrak{b}\backslash\mathfrak{a})$ verwendet man bei der Definition der Matrix M_l wie in (2.15) die Links-Darstellungsmatrizen $R_l(\beta_i)$ $(1 \le i \le n)$.

(2.16) **Algorithmus Quotient von R-Gittern**
Input: *Zwei volle R-Gitter $\mathfrak{a} = \bigoplus_{i=1}^{n} \mathfrak{a}_i\alpha_1$ und $\mathfrak{b} = \bigoplus_{i=1}^{n} \mathfrak{b}_i\beta_1$ und eine F-Basis $\omega_1, \ldots, \omega_n$ von A.*
Output: *Den Quotienten $(\mathfrak{a}/\mathfrak{b})$ bzw. $(\mathfrak{b}\backslash\mathfrak{a})$.*

(1) *Berechne $M = M_r$ wie in (2.15) bzw. $M = M_l$.*
(2) *Modul zusammensetzen:* $\mathcal{M} = \begin{bmatrix} (\mathfrak{b}_1/\mathfrak{a}_1) & \cdots & (\mathfrak{b}_n/\mathfrak{a}_n) \\ & M^{tr} & \end{bmatrix}$.
(3) *Hermite-Normal-Form:* $\begin{bmatrix} \mathfrak{c}_1 & \cdots & \mathfrak{c}_n \\ & \tilde{M} & \end{bmatrix} = \mathrm{HNF}(\mathcal{M})$.
(4) *Quotienten zusammensetzen:* $(\mathfrak{a}/\mathfrak{b}) = \bigoplus_{i=1}^{n}(1/\mathfrak{c}_i)\gamma_i$, *mit* $(\gamma_1, \ldots, \gamma_n) := (\omega_1, \ldots, \omega_n)\left(\tilde{M}_r^{tr}\right)^{-1}$.

An Stelle einer dritten F-Basis $\omega_1, \ldots, \omega_n$ von A kann man auch die F-Basis aus der Darstellung des vollen R-Gitters $\mathfrak{a}$ verwenden. Bei Verwendung der F-Basis $\alpha_1, \ldots, \alpha_n$ kann man sich sowohl die Berechnung der Matrizen S, S^{-1}, als auch die Multiplikationen in (2.15) sparen.

(2.17) **Korollar** *Mit dem Algorithmus 2.16 kann man sowohl die Links- als auch die Rechtsordnung eines vollen R-Gitter Λ berechnen.*

(2.18) **Proposition** *Die Komplexität für die Berechnung der Quotienten $(\mathfrak{a}/\mathfrak{b})$, $(\mathfrak{b}\backslash\mathfrak{a})$ von vollen R-Gitter $\mathfrak{a}$ und $\mathfrak{b}$ beträgt $O(n^4)$.*

Die Berechnung der Links- bzw. Rechtsordnung hat eine Komplexität von $O(n^4)$, gemessen in Elementaroperationen des Grundkörpers F.

Beweis: In Algorithmus 2.16 werden die folgenden Operationen durchgeführt: Invertierung der Matrix S ($O(n^3)$), Berechnung von n Darstellungsmatrizen (je $O(n^3)$, vgl. Proposition 2.3 also $O(n^4)$), n Multiplikationen von $n \times n$ Matrizen (je $O(n^3)$ also $O(n^4)$), n^2 Ideal-Divisionen ($O(n^2)$), Berechnung der Hermite-Normal-Form ($O(n^4)$, vgl. Theorem 1.15), Invertierung der Matrix $\hat{M}^{tr}$ ($O(n^3)$) und n Ideal-Invertierungen ($O(n)$). Insgesamt erhält man also $O(n^4)$ Elementaroperationen. □

2.4 Idealtheorie in Ordnungen

In diesem Abschnitt soll die Theorie der einseitigen und zweiseitigen Ideale in nicht notwendig kommutativen, nicht notwendig maximalen Ordnungen beschrieben werden. Ein besonderes Augenmerk liegt dabei auf den konstruktiven Verfahren zur Arithmetik dieser Ideale, also Addition, Multiplikation, Invertierung (wenn möglich). Im Fall von nicht-maximalen Ordnungen in Zahlkörpern sind Division bzw. Invertierung von beliebigen Idealen z.B. in [San91, Sect. II, S. 48-50] dargestellt.

Zu diesem Zweck sei Λ stets eine R-Ordnung in der Algebra A. Es wird sich herausstellen, daß sich die Ideale von Λ durch eine Pseudo-Basis darstellen lassen, so wie das von Ordnungen in globalen Körpern her bekannt ist. Des weiteren werden noch andere Analogien zu Ordnungen in globalen Körpern aufgezeigt.

2.4.1 Gebrochene Ideale

Eine Teilmenge $\mathfrak{a}$ von A heißt *gebrochenes Rechts- (Links-, zweiseitiges) Ideal* von Λ, wenn $\mathfrak{a}$ ein rechts- (links-, zwei-) seitiger Λ-Modul mit $\mathfrak{a} \cap R \neq \{0\}$ ist, und es ein Element $0 \neq r \in R$ gibt, so daß $r\mathfrak{a} \subseteq \Lambda$ gilt, vgl. [Deu68, S. 69]. Ebenso wie in Dedekindringen (vgl. Abschnitt 1.6) wird auch hier das Nullideal $\{0\}$ in natürlicher Weise ausgeschlossen.

(2.19) **Proposition** *Ist $\mathfrak{a}$ ein reguläres Rechts- (Links-, zweiseitiges) Ideal der Ordnung Λ, also ein Ideal, das mindestens ein von Null verschiedenes*

Element enthält, das kein Nullteiler ist, so ist $\mathfrak{a}$ *auch ein gebrochenes Rechts- (Links, zweiseitiges) Ideal.*

Beweis: Die erste und die dritte Bedingung sind trivialerweise erfüllt, zum Nachweis der zweiten Bedingung wählt man ein $x \in \mathfrak{a} \subseteq \Lambda$, das kein Nullteiler ist. Da x ganz über R ist, genügt es einer Gleichung $x^r + a_{r-1}x^{r-1} + \cdots + a_1x + a_0 = 0$ mit Elementen $a_i \in R, 0 \leq i < r$. Ohne Einschränkung kann man annehmen, daß $a_0 \neq 0$ und damit das gesuchte Element ist. Sonst geht man zu der Gleichung $x^{r-1} + a_{r-1}x^{r-2} + \cdots + a_1 = 0$ über. □

Zur besseren Unterscheidung von den gebrochenen Idealen nennt man die üblichen (regulären) Ideale *ganze Rechts- (Links-, zweiseitige) Ideale* von Λ. Wenn im folgenden von Idealen der Ordnung Λ die Rede ist, sind immer gebrochene und einseitige Ideale gemeint, wobei die Spezifikation Rechts-, Links- oder zweiseitiges Ideal nur angegeben wird, wenn dies nötig ist. *Maximale Ideale* sind natürlich wie üblich maximale ganze Ideale der Ordnung Λ.

(2.20) **Proposition** *Ein gebrochenes Rechts- (Links-, zweiseitiges) Ideal* $\mathfrak{a}$ *der Ordnung* Λ *ist ein volles* R*-Gitter in* A*.*

Umgekehrt ist jedes volle R*-Gitter* $\mathfrak{a}$ *Rechts- bzw. Links-Ideal in einer* R*-Ordnung* Λ*, die in* $\mathcal{O}_r(\mathfrak{a})$ *bzw.* $\mathcal{O}_l(\mathfrak{a})$ *enthalten ist.*

Beweis: $\mathfrak{a}$ ist ein torsionsfreier R-Modul. Da R noethersch ist, ist mit Λ auch jeder R-Teilmodul endlich erzeugt und $\mathfrak{a}$ damit ein R-Gitter. Sei $0 \neq r \in \mathfrak{a} \cap R$ und $\omega_1, \ldots, \omega_n \in \Lambda$ eine F Basis von A, dann ist $r\omega_1, \ldots, r\omega_n$ (man beachte hierbei $R \subseteq \mathrm{Z}(A)$) eine F-Basis von A, die in $\mathfrak{a}$ enthalten ist.

$\mathcal{O}_r(\mathfrak{a})$ ist nach Abschnitt 1.4 eine R-Ordnung und damit das volle R-Gitter $\mathfrak{a}$ ein rechts-seitiger $\mathcal{O}_r(\mathfrak{a})$-Modul und ebenso ein rechts-seitiger Λ-Modul für eine R-Ordnung $\Lambda \subseteq \mathcal{O}_r(\mathfrak{a})$. Die Existenz eines nicht-trivialen Elementes in $R \cap \mathfrak{a}$ folgt direkt aus Proposition 1.20. Schließlich existiert für jedes Element $x \in \mathfrak{a} \subseteq A$ ein $r \in R$ mit $rx \in \Lambda$, denn Λ enthält eine F-Basis von A. Da $\mathfrak{a}$ über R endlich erzeugt ist, existiert auch ein $\bar{r} \in R$, so daß $\bar{r}\mathfrak{a} \subseteq \Lambda$. □

Ist $\mathfrak{a}$ ein gebrochenes Rechts- bzw. Links-Ideal von Λ, so ist $\mathfrak{a}$ also auch ein gebrochenes Rechts- bzw. Links-Ideal in jeder Ordnung, die in der Rechts- bzw. Links-Ordnung ($\mathcal{O}_r(\mathfrak{a})$ bzw. $\mathcal{O}_l(\mathfrak{a})$) enthalten ist.

(2.21) **Bemerkung** *Da die (gebrochenen) Ideale* $\mathfrak{a}$ *einer* R*-Ordnung* Λ *nach Proposition 2.20 stets volle* R*-Gitter sind, lassen sie sich genauso wie Ideale in Ordnungen globaler Körper auch durch Pseudo-Basen darstellen:* $\mathfrak{a} = \bigoplus_{i=1}^{n} \mathfrak{a}_i\omega_i$*, wobei* n *der Dimension der Algebra* A *über* F *entspricht,* $\mathfrak{a}_i$ $(1 \leq i \leq n)$ *(gebrochene) Ideale von* R *sind, und* $\omega_1, \ldots, \omega_n$ *eine* F*-Basis von* A *ist, vgl. Proposition 1.13.*

(2.22) **Proposition** *Es seien $\mathfrak{a}$ und $\mathfrak{b}$ zwei volle R-Gitter, dann ist $(\mathfrak{a}/\mathfrak{b})$ ein gebrochenes Rechts-Ideal in allen Ordnungen, die in $\mathcal{O}_l(\mathfrak{b})$ enthalten sind und ein gebrochenes Links-Ideal in allen Ordnungen, die in $\mathcal{O}_l(\mathfrak{a})$ enthalten sind, mit anderen Worten: $\mathcal{O}_l(\mathfrak{b}) \subseteq \mathcal{O}_r(\mathfrak{a}/\mathfrak{b})$ und $\mathcal{O}_l(\mathfrak{a}) \subseteq \mathcal{O}_l(\mathfrak{a}/\mathfrak{b})$.*

Ebenso ist $(\mathfrak{b}\backslash\mathfrak{a})$ ein gebrochenes Rechts- bzw. Links-Ideal in allen Ordnungen, die in $\mathcal{O}_r(\mathfrak{a})$ bzw. $\mathcal{O}_r(\mathfrak{b})$ enthalten sind, also $\mathcal{O}_r(\mathfrak{a}) \subseteq \mathcal{O}_r(\mathfrak{b}\backslash\mathfrak{a})$ und $\mathcal{O}_r(\mathfrak{b}) \subseteq \mathcal{O}_l(\mathfrak{b}\backslash\mathfrak{a})$.

Insbesondere ist der Quotient von zweiseitigen Idealen einer Ordnung Λ wieder ein zweiseitiges Ideal in Λ.

Beweis: Nach Proposition 2.9 sind $(\mathfrak{a}/\mathfrak{b})$ und $(\mathfrak{b}\backslash\mathfrak{a})$ volle R-Gitter in A. Für jedes $y \in \mathcal{O}_l(\mathfrak{b})$ und jedes $x \in (\mathfrak{a}/\mathfrak{b})$ gilt $xy\mathfrak{b} \subseteq x\mathfrak{b} \subseteq \mathfrak{a}$, also $xy \in (\mathfrak{a}/\mathfrak{b})$ und damit $\mathcal{O}_l(\mathfrak{b}) \subseteq \mathcal{O}_r(\mathfrak{a}/\mathfrak{b})$. $(\mathfrak{a}/\mathfrak{b})$ ist wegen Proposition 2.20 ein gebrochenes Rechts-Ideal für alle Ordnungen, die in $\mathcal{O}_l(\mathfrak{b})$ enthalten sind. Die Behauptung für Links-Ideale und die anderen beiden Teile zeigt man analog. □

Ist $\mathfrak{a} \subseteq \mathcal{O}_r(\mathfrak{a})$ so gilt wegen $\mathfrak{a}\mathfrak{a} \subseteq \mathfrak{a}$ auch $\mathfrak{a} \subseteq \mathcal{O}_l(\mathfrak{a})$ und umgekehrt, vgl. [Deu68, S. 69]. Folglich ist $\mathfrak{a}$ genau dann in seiner Rechts-Ordnung enthalten, wenn es in seiner Links-Ordnung enthalten ist.

(2.23) **Bemerkung** *Aus der Darstellung der (gebrochenen) Ideale einer Ordnung Λ ergeben sich konstruktive Verfahren für die Arithmetik dieser Ideale:*

(1) Die Summe zweier Rechts-, Links- bzw. gleichseitiger Ideale $\mathfrak{a}, \mathfrak{b}$ läßt sich durch die Addition der beiden R-Gitter mit einer Komplexität von $O(n^3)$ realisieren (Korollar 1.16).

(2) Der Schnitt zweier Rechts-, Links- bzw. gleichseitiger Ideale $\mathfrak{a}, \mathfrak{b}$ läßt sich durch den Schnitt der beiden R-Gitter mit einer Komplexität von $O(n^3)$ realisieren (Korollar 1.17).

(3) Das Produkt $\mathfrak{a} \cdot \mathfrak{b}$ eines Links-Ideals $\mathfrak{a}$ mit einem beliebigen Ideal $\mathfrak{b}$ von Λ ist ein Links-Ideal von Λ, ebenso ist das Produkt $\mathfrak{a} \cdot \mathfrak{b}$ eines beliebigen Ideals $\mathfrak{a}$ mit einem Rechts-Ideal $\mathfrak{b}$ ein Rechts-Ideal. Ein konstruktives Verfahren zur Berechnung des Produktes $\mathfrak{a} \cdot \mathfrak{b}$ liefert Algorithmus 2.24.

(4) Sind $\mathfrak{a}$ ein Links-Ideal und $\mathfrak{b}$ ein beliebiges Ideal von Λ, so ist der Quotient $(\mathfrak{a}/\mathfrak{b})$ ein Links-Ideal von Λ. Für ein Rechts-Ideal $\mathfrak{a}$ und ein beliebiges Ideal $\mathfrak{b}$ von Λ ist der Quotient $(\mathfrak{b}\backslash\mathfrak{a})$ ein Rechts-Ideal von Λ, vgl. Proposition 2.22.

Beide Quotienten $(\mathfrak{a}/\mathfrak{b}), (\mathfrak{b}\backslash\mathfrak{a})$ können mit Hilfe von Algorithmus 2.16 mit $O(n^4)$ Elementaroperationen in F berechnet werden. Die Quotienten sind im allgemeinen nicht identisch, siehe hierzu auch Bemerkung 2.50.

(2.24) **Algorithmus Multiplikation von Idealen**
Input: *Zwei Ideale* $\mathfrak{a} = \bigoplus_{i=1}^{n} \mathfrak{a}_i\alpha_i, \mathfrak{b} = \bigoplus_{i=1}^{n} \mathfrak{b}_i\beta_i$ *von* Λ.
Output: *Das Produkt* $\mathfrak{a} \cdot \mathfrak{b}$.

(1) *Bilde sämtliche Produkte von Basiselementen* $\alpha_i\beta_j$ $(1 \leq i, j \leq n)$ *und Koeffizientenidealen* $\mathfrak{a}_i\mathfrak{b}_j$ $(1 \leq i, j \leq n)$.

(2) *Berechne mit Theorem 1.15*

$$\mathfrak{a} \cdot \mathfrak{b} = \mathrm{HNF}\left(\begin{bmatrix} \mathfrak{a}_1\mathfrak{b}_1 & \cdots & \mathfrak{a}_i\mathfrak{b}_j & \cdots & \mathfrak{a}_n\mathfrak{b}_n \\ \vec{\alpha_1\beta_1} & \cdots & \vec{\alpha_i\beta_j} & \cdots & \vec{\alpha_n\beta_n} \end{bmatrix}\right).$$

(2.25) **Proposition** *Mit Algorithmus 2.24 wird das Produkt der Ideale* $\mathfrak{a}$ *und* $\mathfrak{b}$ *in* $O(n^4)$ *Elementaroperationen des Grundkörpers* F *berechnet.*

Beweis: Der Algorithmus zur Multiplikation von Idealen in Relativerweiterungen von Zahlkörpern ist in [Hop98, S. 97] beschrieben. Da das Produkt zweier Ideale unabhängig von der Kommutativität des Ringes Λ definiert ist, und sich das Verfahren direkt an die Definition und die Gitter-Eigenschaft hält, läßt es sich auch auf allgemeine nicht notwendig kommutative Ordnungen über Dedekindringen übertragen.

Die wesentlichen Operationen sind die Multiplikation der Basiselemente, die nach Bemerkung 2.7 $O(n^4)$ Elementaroperationen benötigen und die Hermite-Normal-Form auf das R-Gitter mit n^2 Erzeugern, hierfür werden ebenfalls $O(n^4)$ Elementaroperationen benötigt, vgl. Theorem 1.15. □

2.4.2 Primideale

Ein zweiseitiges ganzes Ideal $\{0\} \subset \mathfrak{P} \subset \Lambda$ heißt *Primideal* von Λ, wenn für zwei beliebige zweiseitige Ideale $\mathfrak{a}, \mathfrak{b}$ von Λ mit $\mathfrak{ab} \subseteq \mathfrak{P}$ schon $\mathfrak{a} \subseteq \mathfrak{P}$ oder $\mathfrak{b} \subseteq \mathfrak{P}$ gilt, vgl. [Deu68, Chpt. VI, §2, Def. 3, S. 73], [LM71, Def. A.1], [Rei75, S. 190] und [CR81, Def. 26.13].

(2.26) **Proposition** [LM71, Prop. A.2] *Das zweiseitige Ideal* $\{0\} \subset \mathfrak{P} \subset \Lambda$ *ist genau dann ein Primideal, wenn für zwei Elemente* $a, b \in \Lambda$ *aus* $a\Lambda b \subseteq \mathfrak{P}$ *entweder* $a \in \mathfrak{P}$ *oder* $b \in \mathfrak{P}$ *folgt.*

Eine wichtige Charakterisierung der Primideale in Ordnungen, die die Analogie zu den Primidealen in Ordnungen globaler Körper aufzeigt, liefert

(2.27) **Theorem** [Rei75, Thm. 22.3] *Die Primideale der Ordnung* Λ *stimmen mit den maximalen zweiseitigen Idealen von* Λ *überein. Ist* $\mathfrak{P}$ *ein Primideal von* Λ*, so ist* $\mathfrak{p} := \mathfrak{P} \cap R$ *ein von Null verschiedenes Primideal von* R*. Weiterhin ist* $\bar{\Lambda} := \Lambda/\mathfrak{P}$ *eine endlich dimensionale einfache Algebra über dem Körper* $R/\mathfrak{p}$.

Nicht nur in Ordnungen in globalen Körpern, sondern allgemein in ganzen Erweiterungen von Dedekindringen sind alle von Null verschiedenen Primideale stets maximal [Gil72, Prop. 11.8].

Den Primidealen in maximalen Ordnungen Λ kommt eine ähnliche Bedeutung zu, wie den Primidealen in Dedekindringen, weshalb die Maximalordnungen manchmal auch als *Dedekind ähnliche Ringe (Dedekind-like rings)* bezeichnet werden [MR87, Chpt. 5].

(2.28) **Theorem** [Deu68, Chpt. VI, §2, Satz 7], [CR81, Thm. 26.14] *Die Menge der (gebrochenen) zweiseitigen Ideale einer Maximalordnung Λ ist eine freie abelsche Gruppe, die von den Primidealen von Λ erzeugt wird.*

2.4.3 Zerlegung der Primideale

Es sei $\mathfrak{p}$ ein maximales Ideal von R. Hier soll kurz auf das durch Theorem 2.28 motivierte Zerlegungsverhalten von $\mathfrak{p}$ in der Maximalordnung Λ eingegangen werden.

Wie in Abschnitt 1.1 sei $A = \bigoplus_{i=1}^{v} A_i$ die Zerlegung der Algebra A in ihre einfachen Bestandteile A_i mit den Idempotenten $1 = \bigoplus_{i=1}^{v} e_i, e_i \in A_i$ $(1 \leq i \leq t)$. Die Zentren $K_i = \mathrm{Z}(A_i)$ $(1 \leq i \leq v)$ der einfachen Bestandteile sind endliche separable Körpererweiterungen von F, so daß die ganzen Abschlüsse $R_i = \mathrm{Cl}(R, K_i)$ $(1 \leq i \leq v)$ von R in K_i wieder Dedekindringe sind, vgl. [PZ89, Chpt. 4, Thm. 5.9] oder [LM71, Prop. 6.22].

Zuerst betrachtet man die Zerlegung von $\mathfrak{p}R_i$ in dem Dedekindring R_i. Die Bewertungstheorie, z.B. [Wei63, Thm. 2-4-6], oder die Idealtheorie, z.B. [Rei75, (4.27) und Thm. 4.30], liefern $\mathfrak{p}R_i = \prod_{j=1}^{r_i} \mathfrak{P}_{i,j}^{e_{i,j}}$. Zusammen mit den Restklassengraden $f_{i,j} = [R_i/\mathfrak{P}_{i,j} : R/\mathfrak{p}]$ $(1 \leq j \leq r_i)$ erhält man $\sum_{j=1}^{r_i} e_{i,j} f_{i,j} = [K_i : F]$.

Theorem 1.4 erlaubt die Zerlegung der Maximalordnung Λ in Maximalordnungen der einfachen Bestandteile $\Lambda_i := \Lambda e_i$. Jedes A_i ist eine *zentraleinfache* K_i-Algebra, also eine einfache K_i-Algebra, deren Zentrum gerade K_i entspricht. Es sei jetzt $\mathfrak{P}$ ein maximales Ideal von R_i, dann zerlegt sich $\mathfrak{P}\Lambda_i$ nach [Rei75, Thm. 22.14] in $\mathfrak{P}\Lambda_i = \mathfrak{Q}^m$.

Die maximalen zweiseitigen Ideale der Maximalordnung Λ sind gerade von der Form $\mathfrak{Q}_{i,j} := \Lambda_1 \oplus \cdots \Lambda_{i-1} \oplus \tilde{\mathfrak{Q}}_{i,j} \oplus \Lambda_{i+1} \oplus \cdots \oplus \Lambda_v$ für ein maximales zweiseitiges Ideal $\tilde{\mathfrak{Q}}_{i,j}$ von Λ_i, vgl. [Rei75, (22.13)]. Damit erhält man insgesamt das folgende Zerlegungsverhalten.

(2.29) **Theorem** *Das maximale Ideal $\mathfrak{p}$ von R zerlegt sich in der Maximalordnung Λ wie folgt: $\mathfrak{p}\Lambda = \prod_{i=1}^{v} \prod_{j=1}^{r_i} \mathfrak{Q}_{i,j}^{e_{i,j} m_{i,j}}$. Die Anzahl der Primideale*

$\mathfrak{Q}_{i,j}$ ist durch die Dimension der F-Algebra A nach oben beschränkt. Außerdem ist die Anzahl der Primideale $\mathfrak{Q}_{i,j}$ unabhängig von der Wahl der Maximalordnung Λ, also für alle Maximalordnungen gleich.

Ein Zusammenhang zu den Primidealen in beliebigen (nicht notwendig maximalen) Ordnungen läßt sich hier nicht herstellen. Die Situation ist sehr viel komplizierter als im kommutativen Fall. Im kommutativen Fall kann man die sogenannten *Going-Up* und *Going-Down* Theoreme [LM71, Cor. 4.7, Thm. 4.9] verwenden. Abschnitt 5.2 wird Auskunft über die Primideale in beliebigen Ordnungen geben.

2.4.4 Inverse Gitter

Wesentlich für die Gruppeneigenschaft der zweiseitigen Ideale ist natürlich die Existenz eines inversen Ideals. Das Inverse läßt sich aber allgemeiner nicht nur für einseitige Ideale beliebiger Ordnungen, sondern sogar für volle R-Gitter definieren.

Es sei im folgenden $\mathfrak{a}$ ein volles R-Gitter. Das *Inverse Gitter* von $\mathfrak{a}$ wird definiert als $\mathfrak{a}^{-1} := \{x \in A | \mathfrak{a}x\mathfrak{a} \subseteq \mathfrak{a}\}$ [Deu68, Chpt. VI, §2, Def. 2, S. 73], [CR81, (26.15)], [Rei75, (22.5)]. Man sieht sofort, daß auch $\mathfrak{a}^{-1} = (\mathfrak{a}\backslash(\mathfrak{a}/\mathfrak{a})) = ((\mathfrak{a}\backslash\mathfrak{a})/\mathfrak{a})$ gelten. Daraus leitet man sofort ein konstruktives Verfahren zur Berechnung des inversen Gitter ab.

(2.30) **Algorithmus Invertierung von R-Gittern**
Input: *Ein volles R-Gitter $\mathfrak{a} = \bigoplus_{i=1}^{n} \mathfrak{a}_i\alpha_i$.*
Output: *Das inverse Gitter $\mathfrak{a}^{-1}$.*
(1) *Berechne mit Algorithmus 2.16 den Quotienten $\mathfrak{b} = (\mathfrak{a}/\mathfrak{a})$.*
(2) *Berechne mit Algorithmus 2.16 den Quotienten $\mathfrak{a}^{-1} = (\mathfrak{a}\backslash\mathfrak{b})$.*

(2.31) **Proposition** *Die Komplexität für die Berechnung des inversen Gitters $\mathfrak{a}^{-1}$ ist $O(n^4)$, gemessen in Elementaroperationen des Grundkörpers F.*

Beweis: Zur Berechnung des inversen Gitters wird zweimal der Algorithmus 2.16 angewendet, der nach Proposition 2.18 je $O(n^4)$ Elementaroperationen benötigt. □

(2.32) **Proposition** [CR81, (26.16)] *Für ein volles R-Gitter $\mathfrak{a}$ in A gelten $\mathcal{O}_l(\mathfrak{a}) \subseteq \mathcal{O}_r(\mathfrak{a}^{-1})$ und $\mathcal{O}_r(\mathfrak{a}) \subseteq \mathcal{O}_l(\mathfrak{a}^{-1})$.*

Ist Λ eine Maximalordnung und $\mathfrak{a}$ ein zweiseitiges Ideal von Λ, dann gelten trivialerweise $\mathcal{O}_l(\mathfrak{a}) = \mathcal{O}_r(\mathfrak{a}^{-1}) = \Lambda$ und $\mathcal{O}_r(\mathfrak{a}) = \mathcal{O}_l(\mathfrak{a}^{-1}) = \Lambda$.

(2.33) **Proposition** *Es sei $\mathfrak{a}$ ein volles R-Gitter in A, dann gelten $\mathfrak{a}\mathfrak{a}^{-1} \subseteq \mathcal{O}_l(\mathfrak{a})$ und $\mathfrak{a}^{-1}\mathfrak{a} \subseteq \mathcal{O}_r(\mathfrak{a})$. Ist $\mathcal{O}_l(\mathfrak{a})$ bzw. $\mathcal{O}_r(\mathfrak{a})$ maximal, so gilt sogar $\mathfrak{a}\mathfrak{a}^{-1} = \mathcal{O}_l(\mathfrak{a})$ bzw. $\mathfrak{a}^{-1}\mathfrak{a} = \mathcal{O}_r(\mathfrak{a})$.*

Beweis: Aus $\mathfrak{a}^{-1} = \{x \in A | \mathfrak{a}x\mathfrak{a} \subseteq \mathfrak{a}\} = \{x \in A | \mathfrak{a}x \subseteq \mathcal{O}_l(\mathfrak{a})\}$ folgt leicht die Inklusion $\mathfrak{a}\mathfrak{a}^{-1} \subseteq \mathcal{O}_l(\mathfrak{a})$. Analog folgt auch die entsprechende Aussage für die Rechts-Ordnung.

Den zweiten Teil der Aussage entnimmt man [CR81, (26.17)]. □

(2.34) **Proposition** [Deu68, Chpt. VI, §2, Satz 12] *Die Links-Ordnung $\mathcal{O}_l(\mathfrak{a})$ eines vollen R-Gitters $\mathfrak{a}$ ist genau dann maximal, wenn die Rechts-Ordnung $\mathcal{O}_r(\mathfrak{a})$ von $\mathfrak{a}$ maximal ist.*

(2.35) **Proposition** *Ist $\mathfrak{a}$ ein volles R-Gitter in A, so gilt $\mathfrak{a} \subseteq (\mathfrak{a}^{-1})^{-1}$.*

Beweis: Es sei $x \in \mathfrak{a}$, aus Proposition 2.33 und Proposition 2.32 folgen $\mathfrak{a}^{-1}x \subseteq \mathcal{O}_r(\mathfrak{a}) \subseteq \mathcal{O}_l(\mathfrak{a}^{-1})$, also $(\mathfrak{a}^{-1}x)\mathfrak{a}^{-1} \subseteq \mathfrak{a}^{-1}$. □

(2.36) **Proposition** [Rei75, Thm. 22.7] *Wenn die Links-Ordnung $\mathcal{O}_l(\mathfrak{a})$ eines vollen R-Gitters $\mathfrak{a}$ maximal ist, dann gilt $\mathfrak{a} = (\mathfrak{a}^{-1})^{-1}$.*

(2.37) **Bemerkung** *Das Inverse eines Rechts- bzw. Links-Ideals einer maximalen Ordnung Λ ist ein Links- bzw. Rechts-Ideal von Λ. Insbesondere handelt es sich entsprechend um ein Links- bzw. Rechts-Inverses bezüglich der Ideal-Multiplikation.*

Ist die Ordnung Λ nicht maximal, so ist zwar nach wie vor das inverse Gitter des Rechts- bzw. Links-Ideals von Λ ein Links- bzw. Rechts-Ideal von Λ, aber nicht mehr notwendig das inverse Element bezüglich der Ideal-Multiplikation.

Da die gebrochenen Ideale einer beliebigen R-Ordnung Λ volle R-Gitter in A sind, läßt sich das Verfahren zur Berechnung des inversen Gitters (Algorithmus 2.30) auf gebrochene Ideale anwenden. Für die Invertierung von zweiseitigen Idealen bietet sich aber ein einfacheres Verfahren an, siehe hierzu Algorithmus 2.42.

2.4.5 Zweiseitige Ideale

Dieser Teil der Arbeit bezieht sich ausschließlich auf die zweiseitigen Ideale der Ordnung Λ. Trivialerweise gilt

(2.38) **Proposition** *Es seien $\Lambda \subseteq \Lambda'$ zwei Ordnungen und $\mathfrak{a}$ ein zweiseitiges Ideal von Λ. Dann ist $\mathfrak{a}' := \Lambda'\mathfrak{a}\Lambda'$ ein zweiseitiges Ideal von Λ', das $\mathfrak{a}$ enthält.*

2.4 Idealtheorie in Ordnungen

Die Menge der zweiseitigen (gebrochenen) Ideale bildet zusammen mit Λ als Einselement einen Monoid bezüglich der Multiplikation. Durch die übliche Definition „Ein zweiseitiges Ideal $\mathfrak{a}$ der Ordnung Λ heißt *invertierbar in der Ordnung* Λ, wenn ein zweiseitiges Ideal $\mathfrak{b}$ existiert mit $\mathfrak{ab} = \Lambda = \mathfrak{ba}$.“ ist das Inverse dann, falls es existiert, bereits eindeutig bestimmt. Der Zusammenhang zu den inversen Gittern wird in Theorem 2.40 gezeigt.

(2.39) **Proposition** *Ist das zweiseitige Ideal $\mathfrak{a}$ der Ordnung Λ invertierbar in Λ, so ist Λ gleich der Links- und der Rechts-Ordnung von $\mathfrak{a}$.*

Beweis: Λ ist trivialerweise in $\mathcal{O}_l(\mathfrak{a}) = (\mathfrak{a}/\mathfrak{a})$ enthalten. Sei $x \in \mathcal{O}_l(\mathfrak{a})$ und $\mathfrak{b}$ das inverse Ideal von $\mathfrak{a}$, dann gelten $x\mathfrak{a} \subseteq \mathfrak{a}$ und $x\Lambda = x\mathfrak{ab} \subseteq \mathfrak{ab} = \Lambda$, also auch $x \in \Lambda$. $\Lambda = \mathcal{O}_r(\mathfrak{a})$ folgt auf die gleiche Weise. □

Damit ist $\mathcal{O}_l(\mathfrak{a}) = \Lambda = \mathcal{O}_r(\mathfrak{a})$ eine notwendige Voraussetzung für die Invertierbarkeit eines beliebigen zweiseitigen Ideals $\mathfrak{a}$. Wie Zassenhaus in einem Beispiel in [Zas67, S. 99] zeigt, ist dies aber keine hinreichende Voraussetzung, nicht einmal für maximale zweiseitige Ideale.

(2.40) **Theorem** *Für ein zweiseitiges Ideal $\mathfrak{a}$ der Ordnung Λ sind die folgenden Aussagen äquivalent:*

(1) $\mathfrak{a}$ *ist invertierbar in* Λ.

(2) $(\Lambda/\mathfrak{a})$ *ist das Inverse zu* $\mathfrak{a}$.

(3) $(\mathfrak{a}\backslash\Lambda)$ *ist das Inverse zu* $\mathfrak{a}$.

Wenn $\mathfrak{a}$ invertierbar ist, so stimmt das Inverse von $\mathfrak{a}$ mit dem inversen Gitter von $\mathfrak{a}$ überein.

Beweis: Die Schritte (2)⇒(1) und (3)⇒(1) sind trivial. Es sei $\mathfrak{b}$ das Inverse zu $\mathfrak{a}$, für $x \in \mathfrak{b}$ gilt dann $x\mathfrak{a} \subseteq \Lambda$, also $x \in (\Lambda/\mathfrak{a})$. Aus der Definition des Quotienten folgt $(\Lambda/\mathfrak{a})\mathfrak{a} \subseteq \Lambda$ und aus der Existenz des Inversen sogar $(\Lambda/\mathfrak{a})\mathfrak{a} = \Lambda$. Damit ist wegen der Eindeutigkeit des Inversen (1)⇒(2) gezeigt, für (1)⇒(3) verfährt man analog.

Sei jetzt $\mathfrak{a}$ invertierbar. Dann ist $(\Lambda/\mathfrak{a})$ das Inverse zu $\mathfrak{a}$. Für jedes $x \in (\Lambda/\mathfrak{a})$ gilt $\mathfrak{a}(x\mathfrak{a}) \subseteq \mathfrak{a}\Lambda \subseteq \mathfrak{a}$, daher $x \in \mathfrak{a}^{-1}$, wobei mit $\mathfrak{a}^{-1}$ das inverse Gitter von $\mathfrak{a}$ bezeichnet wird. Auf der anderen Seite gilt nach Proposition 2.33 $\mathfrak{a}^{-1}\mathfrak{a} \subseteq \mathcal{O}_r(\mathfrak{a}) = \Lambda$, also $\mathfrak{a}^{-1} \subseteq (\Lambda/\mathfrak{a})$. □

Damit ist der Zusammenhang zu den inversen Gittern aus dem vorangegangenen Abschnitt geschaffen und die Verwendung der Notation $\mathfrak{a}^{-1}$ sowohl für das inverse Ideal von $\mathfrak{a}$, falls es existiert, als auch für das inverse Gitter ohne weiteres möglich.

(2.41) **Bemerkung** *Aus Theorem 2.40 ergibt sich ein einfacheres Verfahren als Algorithmus 2.30 zur Berechnung des inversen Ideals zu einem zweiseitigen Ideal einer beliebigen Ordnung, falls das Inverse existiert (Algorithmus 2.42).*

Die Komplexität gemessen in Elementaroperationen des Grundkörpers bleibt zwar $O(n^4)$, es muß aber nur ein Quotient berechnet werden, an Stelle von zweien. Die absolute Laufzeit wird sich demnach halbieren. Dieses Verfahren sollte also insbesondere für die Arithmetik von zweiseitigen Idealen in Maximalordnungen verwendet werden.

(2.42) **Algorithmus Invertierung von zweiseitigen Idealen**
Input: *Ein invertierbares zweiseitiges Ideal $\mathfrak{a} = \bigoplus_{i=1}^{n} \mathfrak{a}_i\alpha_i$ der Ordnung Λ.*
Output: *Das inverse Ideal $\mathfrak{a}^{-1}$ in Λ.*

(1) *Berechne mit Algorithmus 2.16 den Quotienten $\mathfrak{a}^{-1} = (\Lambda/\mathfrak{a})$.*

Zusätzlich zu Theorem 2.40 gibt es für maximale zweiseitige Ideale noch:

(2.43) **Proposition** *Es sei $\mathfrak{a}$ ein zweiseitiges maximales Ideal in Λ. $\mathfrak{a}$ ist genau dann in Λ invertierbar, wenn $\mathcal{O}_l(\mathfrak{a}) = \Lambda \subset (\Lambda/\mathfrak{a})$ oder $\mathcal{O}_r(\mathfrak{a}) = \Lambda \subset (\mathfrak{a}\backslash\Lambda)$ gilt.*

Beweis: Es sei zunächst $\mathfrak{a}$ invertierbar mit dem Inversen $(\Lambda/\mathfrak{a})$, vgl. Theorem 2.40. Die erste Bedingung $\mathcal{O}_l(\mathfrak{a}) = \Lambda$ folgt aus Proposition 2.39. Angenommen $\Lambda = (\Lambda/\mathfrak{a})$, so ist dies wegen $(\Lambda/\mathfrak{a})\mathfrak{a} = \Lambda\mathfrak{a} \subseteq \mathfrak{a} \subset \Lambda$ ein Widerspruch.

Jetzt gelte $\mathcal{O}_l(\mathfrak{a}) = \Lambda \subset (\Lambda/\mathfrak{a})$. Für diesen Teil des Beweises siehe auch [Zas67, S. 99]. $\mathfrak{b} = (\Lambda/\mathfrak{a})\mathfrak{a}$ ist ein zweiseitiges Ideal von Λ (Proposition 2.22). Es gilt $\mathfrak{a} \subseteq \mathfrak{b} \subseteq \Lambda$, so daß wegen der Maximalität von $\mathfrak{a}$ entweder $\mathfrak{a} = \mathfrak{b}$ oder $\mathfrak{b} = \Lambda$ gelten muß. Aus $\mathfrak{a} = \mathfrak{b}$ folgt aber sofort $(\Lambda/\mathfrak{a}) \subseteq (\mathfrak{a}/\mathfrak{a}) = \Lambda$ ein Widerspruch zur Voraussetzung. Es gilt also $(\Lambda/\mathfrak{a})\mathfrak{a} = \Lambda$.

$\mathfrak{c} = \mathfrak{a}(\Lambda/\mathfrak{a})$ ist auch ein zweiseitiges Ideal von Λ, für das $\mathfrak{a} \subseteq \mathfrak{c} \subseteq (\mathfrak{a}/\mathfrak{a}) = \Lambda$ gilt, so daß aus der Maximalität von $\mathfrak{a}$ entweder $\mathfrak{a} = \mathfrak{c}$ oder $\mathfrak{c} = \Lambda$ folgt. Mit $\mathfrak{a} = \mathfrak{c}$ erhält man aber wegen $\Lambda = \mathfrak{b}\mathfrak{a} = \mathfrak{b}\mathfrak{c} = \mathfrak{b}\mathfrak{a}(\Lambda/\mathfrak{a}) = \Lambda(\Lambda/\mathfrak{a}) = (\Lambda/\mathfrak{a})$ einen Widerspruch zur Voraussetzung, so daß $\mathfrak{a}(\Lambda/\mathfrak{a}) = \Lambda$ gelten muß. Somit ist $\mathfrak{a}$ in Λ invertierbar mit dem inversen Ideal $(\Lambda/\mathfrak{a})$.

Die anderen beiden Teile zeigt man analog. □

(2.44) **Bemerkung** *Da für ein (zweiseitiges) Ideal $\mathfrak{a}$ von Λ $\mathcal{O}_l(\mathfrak{a}) = \Lambda = \mathcal{O}_r(\mathfrak{a})$ notwendige Voraussetzung für die Invertierbarkeit von $\mathfrak{a}$ ist, kann man auf der Suche nach einer Maximalordnung immer Λ durch die Rechts- oder Links-Ordnung von $\mathfrak{a}$ ersetzen, wenn diese nicht mit Λ übereinstimmen. Ist eine der beiden Ordnungen echt größer als Λ, so war Λ nicht maximal.*

Wenn $\mathfrak{a}$ nur ein Rechts- bzw. Links-Ideal von Λ ist, dann darf man entsprechend nur die Rechts- bzw. Links-Ordnung von $\mathfrak{a}$ betrachten.

Wenn man aber schon von einer ganzen Reihe von Idealen von Λ die Rechts- bzw. Links-Ordnungen berechnet hat, und keine echt größere Ordnung als Λ gefunden hat, ist dann Λ maximal? Eine Antwort auf diese Frage liefern das Verfahren von Zassenhaus [Zas67] für den Fall $R = \mathbb{Z}$, das im nächsten Kapitel auf beliebige Dedekindringe R übertragen wird.

Die folgenden Aussagen über invertierbare maximale Ideale der Ordnung Λ sind auch eine Verallgemeinerung von [Zas67]. Die Beweise verlaufen im wesentlichen analog, sind aber aus Gründen der Vollständigkeit hier aufgeführt.

(2.45) **Proposition** [Zas67, Hilfssatz 1, S. 99] *Ein invertierbares zweiseitiges Ideal $\mathfrak{a}$ der Ordnung Λ kommutiert mit allen zweiseitigen (ganzen) Idealen $\mathfrak{b}$, für die $\mathfrak{a} + \mathfrak{b} = \Lambda$ gilt.*

Beweis: Es gelten $\mathfrak{b} = \mathfrak{a}^{-1}(\mathfrak{a}\mathfrak{b}) \subseteq \mathfrak{a}^{-1}(\mathfrak{a} \cap \mathfrak{b}) \subseteq (\mathfrak{a}^{-1}\mathfrak{a}) \cap (\mathfrak{a}^{-1}\mathfrak{b}) \subseteq \Lambda \cap (\mathfrak{a}^{-1}\mathfrak{b})$, also

$$\mathfrak{b} \subseteq \Lambda \cap (\mathfrak{a}^{-1}\mathfrak{b}), \tag{2.46}$$

sowie die trivialen Inklusionen

$$\mathfrak{a}(\Lambda \cap (\mathfrak{a}^{-1}\mathfrak{b})) \subseteq \mathfrak{a}\mathfrak{a}^{-1}\mathfrak{b} = \mathfrak{b} \quad \text{und} \quad \mathfrak{b}(\Lambda \cap (\mathfrak{a}^{-1}\mathfrak{b})) \subseteq \mathfrak{b}\Lambda = \mathfrak{b}. \tag{2.47}$$

Weiterhin erhält man $\Lambda \cap (\mathfrak{a}^{-1}\mathfrak{b}) = \Lambda(\Lambda \cap (\mathfrak{a}^{-1}\mathfrak{b})) = (\mathfrak{a} + \mathfrak{b})(\Lambda \cap (\mathfrak{a}^{-1}\mathfrak{b})) \subseteq \mathfrak{a}(\Lambda \cap (\mathfrak{a}^{-1}\mathfrak{b})) + \mathfrak{b}(\Lambda \cap (\mathfrak{a}^{-1}\mathfrak{b})) \subseteq \mathfrak{b}$, wobei bei der letzten Inklusion (2.47) ausgenutzt wurde. In Verbindung mit (2.46) folgt

$$\Lambda \cap (\mathfrak{a}^{-1}\mathfrak{b}) = \mathfrak{b}. \tag{2.48}$$

Mit (2.48) folgt nun $\mathfrak{a}^{-1}(\mathfrak{a} \cap \mathfrak{b}) \subseteq (\mathfrak{a}^{-1}\mathfrak{a}) \cap (\mathfrak{a}^{-1}\mathfrak{b}) = \Lambda \cap (\mathfrak{a}^{-1}\mathfrak{b}) = \mathfrak{b}$, also $\mathfrak{a} \cap \mathfrak{b} \subseteq \mathfrak{a}\mathfrak{b}$. Es gilt also $\mathfrak{a} \cap \mathfrak{b} = \mathfrak{a}\mathfrak{b}$.

Analog zeigt man $\mathfrak{a} \cap \mathfrak{b} = \mathfrak{b}\mathfrak{a}$, und damit $\mathfrak{a}\mathfrak{b} = \mathfrak{b}\mathfrak{a}$. □

(2.49) **Proposition** [Zas67, Hilfssatz 2, S. 99] *Ein invertierbares maximales zweiseitiges Ideal $\mathfrak{a}$ der Ordnung Λ kommutiert mit jedem (gebrochenen) zweiseitigen Ideal $\mathfrak{b}$ von Λ.*

Beweis: Ist $\mathfrak{b}$ ein ganzes Ideal, das nicht in $\mathfrak{a}$ enthalten ist, so ist wegen Proposition 2.45 nichts weiter zu zeigen. Wenn $\Lambda \subset \mathfrak{b}$, $\mathfrak{b}$ also kein ganzes Ideal ist, dann existiert ein $r \in R$, so daß $r\mathfrak{b}$ ein ganzes Ideal von Λ ist. An dieser Stelle kann man ohne Einschränkung annehmen, daß $\{0\} \neq \mathfrak{b}$ ein ganzes in $\mathfrak{a}$ enthaltenes Ideal ist.

Es gilt stets $\mathfrak{a}^{j+1} \subset \mathfrak{a}^j, j \geq 0$, sonst erhält man mit $\Lambda = \mathfrak{a}^j(\mathfrak{a}^{-1})^j = \mathfrak{a}\mathfrak{a}^j(\mathfrak{a}^{-1})^j = \mathfrak{a}$ einen Widerspruch. Daher muß ein Exponent $\nu > 0$ existieren

mit $\mathfrak{b} \subseteq \mathfrak{a}^\nu$ aber $\mathfrak{b} \not\subseteq \mathfrak{a}^{\nu+1}$. Hierzu genügt es, den Index von $\mathfrak{a}^j$ in $\mathfrak{b}$ und die eindeutige Primideal-Faktorisierung in R zu betrachten.

Für $\mathfrak{c} := \mathfrak{a}^{-\nu}\mathfrak{b} \subseteq \Lambda$ gelten $\mathfrak{c} \not\subseteq \mathfrak{a}$ und $\mathfrak{c} + \mathfrak{a} = \Lambda$. Nach Proposition 2.45 gilt $\mathfrak{ca} = \mathfrak{ac}$, also auch $\mathfrak{ab} = \mathfrak{aa}^\nu\mathfrak{c} = \mathfrak{a}^\nu\mathfrak{ca} = \mathfrak{ba}$. □

(2.50) **Bemerkung** *Es seien $\mathfrak{a}, \mathfrak{b}$ zweiseitige Ideale von Λ, $\mathfrak{a}$ sei invertierbar und $\mathfrak{a}$ kommutiere mit $\mathfrak{b}$. (Dies erhält man zum Beispiel, wenn $\mathfrak{a}$ maximal und invertierbar ist, vgl. Proposition 2.49.)*

Dann gilt auch $\mathfrak{a}^{-1}\mathfrak{b} = \mathfrak{a}^{-1}\mathfrak{b}(\mathfrak{a}\mathfrak{a}^{-1}) = \mathfrak{a}^{-1}\mathfrak{a}\mathfrak{b}\mathfrak{a}^{-1} = \mathfrak{b}\mathfrak{a}^{-1}$. Weiterhin gilt $(\mathfrak{b}/\mathfrak{a}) = \mathfrak{b}\mathfrak{a}^{-1} = \mathfrak{a}^{-1}\mathfrak{b} = (\mathfrak{a}\backslash\mathfrak{b})$. Man kann also von einer eindeutigen Division von $\mathfrak{b}$ durch $\mathfrak{a}$ sprechen.

(2.51) **Korollar** [Zas67, Korollar 1 und 3, S. 100, 101] *Jedes ganze zweiseitige Ideal $\mathfrak{a}$ der Ordnung Λ läßt sich als Produkt von invertierbaren maximalen zweiseitigen Idealen von Λ und einem zweiseitigen Ideal von Λ, das in keinem invertierbaren maximalen zweiseitigen Ideal von Λ enthalten ist, schreiben.*

Beweis: Ist $\mathfrak{a}$ in keinem invertierbaren maximalen zweiseitigen Ideal von Λ enthalten, so ist man fertig. Es gelte also $\mathfrak{a} \subseteq \mathfrak{b}$, wobei $\mathfrak{b}$ ein invertierbares maximales zweiseitiges Ideal von Λ ist. Wie im Beweis zu Proposition 2.49 erhält man einen Exponenten $\nu > 0$ mit $\mathfrak{a} \subseteq \mathfrak{b}^\nu$ $\mathfrak{a} \not\subseteq \mathfrak{b}^{\nu+1}$. Für $\mathfrak{a}' := \mathfrak{b}^{-\nu}\mathfrak{a}$ gilt dann $\mathfrak{a}' \not\subseteq \mathfrak{b}$ und man kann mit dem ganzen zweiseitigen Ideal $\mathfrak{a}'$ fortfahren. Die Betrachtung des Index und die Endlichkeit der Primideal-Faktorisierung des Index in R liefern, daß diese Rekursion nach endlich vielen Schritten abbrechen muß. □

(2.52) **Bemerkung** *Die Faktorisierung aus Korollar 2.51 läßt sich auch auf gebrochene zweiseitige Ideale der Ordnung Λ übertragen: Der mögliche Nenner $r \in R$ faktorisiert dann ebenso in ein Produkt von invertierbaren maximalen zweiseitigen Idealen von Λ und ein zweiseitiges Ideal $\mathfrak{m} \subseteq \Lambda$, das in keinem invertierbaren maximalen zweiseitigen Ideal von Λ enthalten ist. Da $r\Lambda$ in Λ invertierbar ist, ist auch das Ideal $\mathfrak{m}$ in Λ invertierbar, so daß man die Faktorisierung zusammensetzten kann.*

Ein Verfahren zur Berechnung dieser Faktorisierung ist Algorithmus 5.27. In Proposition 5.29 wird außerdem die Eindeutigkeit der Faktorisierung aus Korollar 2.51 gezeigt.

Aus Korollar 2.51 läßt sich eine weitere Charakterisierung der Indexteiler ableiten, siehe Bemerkung 3.15.

Kapitel 3
Der Round 1 Algorithmus

In diesem Kapitel wird der *Round 1 Algorithmus* von Zassenhaus [Zas67] zur Berechnung von Maximalordnungen beschrieben und verallgemeinert. Zassenhaus hatte das Verfahren für Ordnungen Λ über $\mathbb{Z}$ erklärt [Zas67, S. 90].

Die Halbeinfachheit der $\mathbb{Q}$-Algebra $A := \mathbb{Q} \otimes_{\mathbb{Z}} \Lambda$ erhält er durch die Bedingung $\left|(\mathrm{Tr}(\omega_i\omega_j))_{(1\le i,j\le n)}\right| \neq 0$, wobei $\omega_1, \ldots, \omega_n$ eine $\mathbb{Z}$-Basis von Λ sei. Die Separabilität einer endlich dimensionalen halbeinfachen Algebra A über $\mathbb{Q}$ erhält man trivialerweise, vgl. Proposition 1.1.

Hier wird dieses Verfahren verallgemeinert, so daß es zur Berechnung von Maximalordnungen von Ordnungen Λ über Dedekindringen R angewendet werden kann, wobei Λ eine Ordnung in der separablen F-Algebra A der Dimension n und F der Quotientenkörper von R ist.

3.1 Diskriminante und Index von R-Gittern

Die aus der Theorie von Ordnungen in globalen Körpern wohlbekannte Diskriminante von Ordnungen und der Index einer Ordnung in einer anderen Ordnung werden hier allgemeiner für volle R-Gitter in A definiert.

Es seien $\Lambda \subseteq \Lambda'$ stets zwei volle R-Gitter in A. Weiterhin seien die Pseudo-Basen beider Gitter nach Theorem 1.18 wie folgt gegeben: $\Lambda' = \bigoplus_{i=1}^{n} \mathfrak{a}_i\omega_i$ und $\Lambda = \bigoplus_{i=1}^{n} \mathfrak{b}_i\mathfrak{a}_i\omega_i$.

Mit $\mathrm{Tr} : A \to F$ wird im folgenden die reduzierte Spur von A bezeichnet, vgl. Seite 2. Die reduzierte Spur induziert eine symmetrische nichtdegenerierte Bilinearform $\Gamma : A \times A \to F : (x, y) \mapsto \mathrm{Tr}(xy)$ [Rei75, Thm. 9.26].

Die *Diskriminante* $\mathrm{disc}(\Lambda)$des R-Gitters Λ ist definiert als das (gebrochene) Ideal von R, das von allen Elementen $\left|(\mathrm{Tr}(x_ix_j))_{(1\le i,j\le n)}\right|$ erzeugt wird, wobei $x_1, \ldots, x_n \in \Lambda$, vgl. [CR81, (4.25)] oder [PZ89, Chpt. 4.5, 5.50]. Aus der Pseudo-Basis von Λ' erhält man $\mathrm{disc}(\Lambda') = \prod_{i=1}^{n} \mathfrak{a}_i^2 \left|(\mathrm{Tr}(\omega_i\omega_j))_{(1\le i,j\le n)}\right|$. Der Beweis hiervon verläuft analog zu dem für Relativerweiterungen von Zahlkörpern [Fri97, Satz II.49].

Für einen R-Torsionsmodul Λ^{tor} seien $\mathfrak{n}_1 \supseteq \mathfrak{n}_2 \supseteq \cdots \supseteq \mathfrak{n}_r$ die *Elementarteiler-Ideale* [PZ89, Chpt. 4.5, Def. 5.25]. Bei dem R-

Torsionsmodul $\Lambda^{\mathrm{tor}} = \Lambda'/\Lambda$ entsprechen die Elementarteiler-Ideale gerade den Elementarteiler-Idealen aus Theorem 1.18 $\mathfrak{n}_i = \mathfrak{b}_i$ $(1 \leq i \leq n)$.

Das *Ordnungsideal* des R-Torsionsmoduls Λ^{tor} ist definiert als $\mathrm{ord}(\Lambda^{\mathrm{tor}}) = \prod_{i=1}^{r} \mathfrak{n}_i$ [PZ89, Chpt. 4.5, Def. 5.30], [Rei75, (4.16)]. In [Rei75, (4.16)] wird das Ordnungsideal auch für beliebige R-Moduln (nicht notwendig Torsionsmodule) erklärt. In diesem Rahmen genügt aber die Einschränkung auf Torsionsmodule. Aus dem Ordnungsideal leitet man den *Index* von Λ' in Λ wie folgt ab: $(\Lambda' : \Lambda) = \mathrm{ord}(\Lambda'/\Lambda)$ [PZ89, Chpt. 4.5, Lemma 5.35].

(3.1) **Korollar** *Für die vollen R-Gitter $\Lambda \subseteq \Lambda'$ gilt* $\mathrm{disc}(\Lambda) = (\Lambda' : \Lambda)^2 \mathrm{disc}(\Lambda')$.

Mit Hilfe des *dualen Gitters* $\Lambda^{\perp} = \{x \in A | \mathrm{Tr}(x\Lambda) \in R\}$ von Λ [OMe63, §82F] kann man die *reduzierte Diskriminante* $\mathrm{disc}_r(\Lambda)$ von Λ definieren als das größte Elementarteiler-Ideal von $\Lambda^{\perp}/\Lambda$ [PZ89, Chpt. 4.5, Def. 5.46], weiterhin erhält man

(3.2) **Proposition** [PZ89, Chpt. 4.5, Lemma 5.49], [Rei75, S. 218] *Für das R-Gitter Λ gilt* $\mathrm{disc}(\Lambda) = (\Lambda^{\perp} : \Lambda)$.

3.2 $\mathfrak{p}$-Maximalität

Die Begriffe Diskriminante und Index werden aus dem vorangegangenen Abschnitt in natürlicher Weise auf R-Ordnungen übertragen, vgl. [Deu68, Chpt. VI, §6, Def. 1, S. 87], [Rei75, S. 126].

(3.3) **Theorem** [Deu68, S. 88], [Rei75, Thm. 25.3] *Zwei Maximalordnungen in A haben dieselbe Diskriminante.*

Damit kann man ähnlich wie bei globalen Körpern die Diskriminante einer Maximalordnung auch auf die ganze Algebra A übertragen. Außerdem ist der folgende Begriff wohldefiniert.

Es sei $\mathfrak{p}$ ein maximales Ideal von R. Dann heißt die R-Ordnung Λ $\mathfrak{p}$-*maximal*, wenn der Index einer beliebigen über Λ liegenden Maximalordnung $\Lambda^{(\max)}$ in Λ nicht von $\mathfrak{p}$ geteilt wird. Nach Theorem 3.3 und Korollar 3.1 ist $(\Lambda^{(\max)} : \Lambda) = (\Lambda_2 : \Lambda)$ für jede über Λ liegende Maximalordnung Λ_2.

Der Begriff der $\mathfrak{p}$-*maximalen Oberordnung*, der aus der Betrachtung von Ordnungen in globalen Körpern bekannt ist, muß im nicht-kommutativen Fall angepaßt werden, da hier keine eindeutige Maximalordnung existiert. Zu einer gegebenen Maximalordnung $\Lambda^{(\max)}$ und einer darin enthaltenen Ordnung Λ heißt die Menge $\Lambda^{(\mathfrak{p})} := \{x \in \Lambda^{(\max)} | \mathfrak{p}^{\nu} x \subseteq \Lambda, \text{ für ein } \nu \geq 0\}$ $\mathfrak{p}$-*maximale Zwischenordnung* zu Λ und $\Lambda^{(\max)}$. Die Eigenschaften von $\Lambda^{(\mathfrak{p})}$ sind aber dieselben wie im Fall globaler Körper, vgl. [Fri97, Lemma III.3]:

(3.4) **Proposition** *$\Lambda^{(\mathfrak{p})}$ ist eine $\mathfrak{p}$-maximale Ordnung und es existiert ein $\nu \geq 0$ mit $\mathfrak{p}^\nu \Lambda^{(\mathfrak{p})} \subseteq \Lambda$. Hierfür gilt $(\Lambda^{(\mathfrak{p})} : \Lambda) \mid \mathfrak{p}^{\nu n}$.*

Beweis: Die R-Modul-Eigenschaft von $\Lambda^{(\mathfrak{p})}$ ist unmittelbar klar. Da $\Lambda^{(\mathfrak{p})}$ nach Definition auch ein Teilmodul von $\Lambda^{(\max)}$ ist, ist $\Lambda^{(\mathfrak{p})}$ auch endlich erzeugt, also ein R-Gitter. Aus $\Lambda \subseteq \Lambda^{(\mathfrak{p})}$ folgt dann, daß $\Lambda^{(\mathfrak{p})}$ sogar ein volles R-Gitter ist.

Für $x, y \in \Lambda^{(\mathfrak{p})}$ mit $\mathfrak{p}^{\nu_1} x, \mathfrak{p}^{\nu_2} y \subseteq \Lambda$ gilt $\mathfrak{p}^{\nu_1+\nu_2}(xy) = \mathfrak{p}^{\nu_1} x \cdot \mathfrak{p}^{\nu_2} y \subseteq \Lambda$. Nach Korollar 1.8 ist $\Lambda^{(\mathfrak{p})}$ also eine Ordnung.

Da $\Lambda^{(\mathfrak{p})}$ über R endlich erzeugt ist, und für jeden Erzeuger y ein entsprechender Exponent $\mu \geq 0$ existiert mit $\mathfrak{p}^\mu y \subseteq \Lambda$, existiert auch ein $\nu \geq 0$ mit $\mathfrak{p}^\nu \Lambda^{(\mathfrak{p})} \subseteq \Lambda$. $(\Lambda^{(\mathfrak{p})} : \Lambda) \mid \mathfrak{p}^{\nu n}$ folgt dann aus der Betrachtung der n Elementarteiler, die alle $\mathfrak{p}^\nu$ teilen müssen.

Angenommen $\Lambda^{(\mathfrak{p})}$ ist nicht $\mathfrak{p}$-maximal, dann liefert Theorem 1.18 die Darstellungen $\Lambda^{(\max)} = \bigoplus_{i=1}^r \mathfrak{a}_i \omega_i$ und $\Lambda^{(\mathfrak{p})} = \bigoplus_{i=1}^r \mathfrak{b}_i \mathfrak{a}_i \omega_i$, wobei ein $1 \leq j \leq n$ existiert mit $\mathfrak{p}^\mu \mathfrak{c} = \mathfrak{b}_j, \mathfrak{c} \not\subseteq \mathfrak{p}$. Mit $x := \gamma \omega_j, \gamma \in \mathfrak{c}\mathfrak{a}_j \setminus \mathfrak{b}_j \mathfrak{a}_j$ erhält man $x \in \Lambda^{(\max)}$ und $x \notin \Lambda^{(\mathfrak{p})}$, aber $\mathfrak{p}^\mu x \in \mathfrak{b}_j \mathfrak{a}_j \omega_j \subseteq \Lambda^{(\mathfrak{p})}$, also auch $\mathfrak{p}^{\nu\mu} x \in \Lambda$, einen Widerspruch zur Annahme. □

(3.5) **Korollar** *Λ ist genau dann $\mathfrak{p}$-maximal, wenn $\Lambda = \Lambda^{(\mathfrak{p})}$ gilt.*

3.3 Das $\mathfrak{p}$-Radikal

Die folgende Aussage wird häufiger gebraucht werden, deshalb taucht sie hier in einer allgemeinen Formulierung auf.

(3.6) **Proposition** *Es seien S ein nicht notwendig kommutativer Ring mit Eins und I ein beliebiges zweiseitiges Ideal von S. Der kanonische Homomorphismus $\varphi : S \to S/I : x \mapsto x + I$ induziert eine Bijektion zwischen den ganzen (maximalen) Rechts-, Links- bzw. zweiseitigen Idealen von S, die I enthalten und den ganzen (maximalen) Rechts-, Links- bzw. zweiseitigen Idealen von S/I.*

Beweis: Für zweiseitige Ideale ist diese Aussage wohlbekannt, z.B. [Mey75, Satz 3.1.11 und Satz 3.1.17]. Eine Analyse der Beweise zeigt, daß man die Aussage auch auf Rechts- bzw. Links-Ideale übertragen kann. Die Bijektion zwischen den maximalen Idealen ist dann eine Folgerung aus der Bijektion zwischen allen entsprechenden Idealen. □

Es seien $\mathfrak{p}$ ein maximales Ideal von R und Λ eine Ordnung. Weiterhin werden $\bar{\Lambda} := \Lambda/\mathfrak{p}\Lambda$ und das Jacobson-Radikal $J := J(\bar{\Lambda})$ von $\bar{\Lambda}$ definiert. J

ist der Schnitt über alle maximalen Links-Ideale von $\bar{\Lambda}$ und ein zweiseitiges Ideal von $\bar{\Lambda}$ [Lor90, §28, Bemerkung (b) nach Def. 10].

Es sei $\varphi : \Lambda \to \bar{\Lambda} : x \mapsto x + \mathfrak{p}\Lambda$ der kanonische Homomorphismus. An dieser Stelle möchte ich Gabriele Nebe für den Hinweis [Neb00] danken, der den Beweis der folgenden Aussage geliefert hat.

(3.7) **Proposition** *J ist der Durchschnitt aller maximalen zweiseitigen Ideale von $\bar{\Lambda}$.*

Beweis: Aus Λ endlich erzeugt über R folgert man, daß $\bar{\Lambda}$ auch endlich erzeugt über dem Körper $\bar{R} := R/\mathfrak{p}$ ist. Damit ist aber $\bar{\Lambda}$ nach [Lor90, §28, F24] eine artinsche Algebra. Man sieht mit [Lor90, §28, Bem. (f) und (i) nach Def. 10], daß $\bar{\Lambda}/J$ eine halbeinfache artinsche Algebra ist, sich also wegen [Lor90, §29, Satz 1] in seine einfachen Bestandteile zerlegen läßt: $\bar{\Lambda}/J = \bigoplus_{i=1}^{k} L_i$. $\psi : \bar{\Lambda} \to \bar{\Lambda}/J$ sei der kanonische Homomorphismus.

Die maximalen zweiseitigen Ideale von $\bar{\Lambda}/J$ sind dann gerade von der Form $\mathfrak{m}_i = L_1 \oplus \cdots \oplus L_{i-1} \oplus \{0\} \oplus L_{i+1} \oplus \cdots \oplus L_k$ $(1 \leq i \leq k)$ und insbesondere gilt $\bigcap_{i=1}^{k} \mathfrak{m}_i = \{0\}$.

Nach Proposition 3.6 sind $\psi^{-1}(\mathfrak{m}_i)$ gerade die maximalen zweiseitigen Ideale von $\bar{\Lambda}$, die J enthalten und man folgert $J \supseteq \bigcap_{i=1}^{k} \psi^{-1}(\mathfrak{m}_i)$. Da J außerdem in jedem maximalen zweiseitigen Ideal von $\bar{\Lambda}$ enthalten ist [Rei75, Cor. 6.13], erhält man die Behauptung. □

Der Schnitt $\sqrt{\mathfrak{p}\Lambda}$ über alle maximalen zweiseitigen Ideale von Λ, die $\mathfrak{p}$ enthalten, heißt das $\mathfrak{p}$-*Radikal* von Λ. Korollar 5.22 wird zeigen, daß es nur endlich viele maximale zweiseitige Ideale in Λ gibt, die $\mathfrak{p}$ enthalten. $\sqrt{\mathfrak{p}\Lambda}$ ist ein zweiseitiges Ideal in Λ, das $\mathfrak{p}$ enthält. Man erhält den folgenden Zusammenhang zum Jacobson-Radikal von $\bar{\Lambda}$.

(3.8) **Korollar** *Es gilt $\varphi^{-1}(J) = \sqrt{\mathfrak{p}\Lambda}$.*

Beweis: Mit Proposition 3.6 erhält man $\varphi^{-1}(J) = \varphi^{-1}(\bigcap \bar{\mathfrak{m}})$, wobei nach Proposition 3.7 der Schnitt über alle maximalen zweiseitigen Ideale $\bar{\mathfrak{m}}$ von $\bar{\Lambda}$ genommen wird. Daraus folgt $\varphi^{-1}(J) = \bigcap \mathfrak{m} = \sqrt{\mathfrak{p}\Lambda}$. Diesmal wird der Schnitt aller maximalen zweiseitigen Ideale von Λ betrachtet, die $\mathfrak{p}$ enthalten. □

(3.9) **Proposition** *Es existiert ein $\nu > 0$ mit $J^\nu = \{0\}$ und ebenso $\sqrt{\mathfrak{p}\Lambda}^\nu \subseteq \mathfrak{p}\Lambda$.*

Beweis: $\bar{\Lambda}$ ist eine endlich dimensionale artinsche Algebra über $R/\mathfrak{p}$, vgl. Beweis zu Proposition 3.7. Weiterhin ist das Jacobson-Radikal einer artinschen Algebra stets nilpotent [Lor90, §28, Satz 4]. □

Die folgende Aussage ist eine Verallgemeinerung von [Zas67, Satz 2] und eines der wesentlichen Hilfsmittel für das Maximalitätskriterium Theorem 3.11.

(3.10) **Proposition** [Zas67, Satz 2] *Entweder gibt es ein maximales zweiseitiges Ideal $\mathfrak{P}$ von Λ, das $\mathfrak{p}$ enthält und dessen Links-Ordnung echt größer ist als Λ, also $\Lambda \subset \mathcal{O}_l(\mathfrak{P}) = (\mathfrak{P}/\mathfrak{P})$, oder alle maximalen zweiseitigen Ideale, die $\mathfrak{p}$ enthalten, sind invertierbar.*

Beweis: $\{\mathfrak{P}_1, \ldots, \mathfrak{P}_s\}$ sei die Menge der maximalen zweiseitigen Ideale von Λ, die $\mathfrak{p}$ enthalten. Gilt $\Lambda \subset \mathcal{O}_l(\mathfrak{P}_j)$ für ein $\mathfrak{P}_j$, so kann wegen Proposition 2.39 $\mathfrak{P}_j$ nicht invertierbar sein. Es gelte also $\Lambda = \mathcal{O}_l(\mathfrak{P}_j)$ $(1 \leq j \leq s)$.

Wegen $\left(\prod_{j=1}^{s} \mathfrak{P}_j\right)^{\nu} \subseteq \sqrt{\mathfrak{p}\Lambda}^{\nu} \subseteq \mathfrak{p}\Lambda$ gibt es Produkte $Q_i = \prod_{j=1}^{s_i} \mathfrak{Q}_{i,j} \subseteq \mathfrak{p}\Lambda$ $(i \in \mathcal{I})$, wobei $\mathfrak{Q}_{i,j} \in \{\mathfrak{P}_1, \ldots, \mathfrak{P}_s\}$ $(i \in \mathcal{I}, 1 \leq j \leq s_i)$. Sei Q_i $(i \in \mathcal{I})$ eines dieser Produkte, dann gilt $Q_i \subseteq \mathfrak{p}\Lambda \subseteq \mathfrak{P}_j$ $(1 \leq j \leq s)$, und aus der Primideal-Eigenschaft der $\mathfrak{P}_j$, vgl. Theorem 2.27, folgt, daß für jedes $1 \leq j \leq s$ ein $1 \leq k_j \leq s_i$ existieren muß mit $\mathfrak{Q}_{i,k_j} \subseteq \mathfrak{P}_j$, also wegen der Maximalität auch $\mathfrak{Q}_{i,k_j} = \mathfrak{P}_j$. Die Produkte Q_i $(i \in \mathcal{I})$ haben alle mindestens s Faktoren und jedes der $\mathfrak{P}_j$ kommt darin vor.

Jetzt wählt man ein Produkt Q_i $(i \in \mathcal{I})$ mit der kleinsten Anzahl von Faktoren. Man erhält $Q_i = \prod_{j=1}^{s_i} \mathfrak{Q}_{i,j} \subseteq \mathfrak{p}\Lambda$ und $\prod_{j=1}^{s_i-1} \mathfrak{Q}_{i,j} \not\subseteq \mathfrak{p}\Lambda$. Hieraus ergibt sich $\Lambda \subset \mathfrak{p}^{-1} \prod_{j=1}^{s_i-1} \mathfrak{Q}_{i,j} \subseteq (\Lambda/\mathfrak{Q}_{i,s_i})$. Aus Proposition 2.43 folgt, daß $\mathfrak{Q}_{i,s_i}$ invertierbar ist, und wegen Proposition 2.49 mit den Idealen $\mathfrak{Q}_{i,j}$ $(1 \leq j < s_i)$ kommutiert.

Die Umstellung des Produktes Q_i liefert $\mathfrak{Q}_{i,s_i} \prod_{j=1}^{s_i-1} \mathfrak{Q}_{i,j} = Q_i \subseteq \mathfrak{p}\Lambda$, und wegen der minimalen Anzahl der Faktoren muß $\mathfrak{Q}_{i,s_i} \prod_{j=1}^{s_i-2} \mathfrak{Q}_{i,j} \not\subseteq \mathfrak{p}\Lambda$ gelten. Wie oben folgert man, daß das Ideal $\mathfrak{Q}_{i,s_i-1}$ invertierbar ist. Führt man diesen Schritt mehrfach durch, so gelangt man zu dem Ergebnis, daß alle Ideale $\mathfrak{Q}_{i,1}, \ldots, \mathfrak{Q}_{i,s_i}$ und damit auch alle Ideale $\mathfrak{P}_1, \ldots, \mathfrak{P}_s$ invertierbar sind. □

3.4 Das $\mathfrak{p}$-Maximalitätskriterium

Mit den Vorarbeiten der letzten Abschnitte läßt sich jetzt die Hauptaussage [Zas67, Satz 3] formulieren und auf R-Ordnungen über Dedekindringen übertragen. Dazu sei wieder $\mathfrak{p}$ ein maximales Ideal von R.

(3.11) **Theorem Maximalitätskriterium** [Zas67, Satz 3] *Die R-Ordnung Λ ist genau dann $\mathfrak{p}$-maximal, wenn jedes maximale zweiseitige Ideal von Λ, das $\mathfrak{p}$ enthält, in Λ invertierbar ist.*

Beweis: Λ' sei eine Λ enthaltende Maximalordnung. Zuerst sei Λ $\mathfrak{p}$-maximal und $\mathfrak{P}$ sei ein maximales Ideal von Λ, das $\mathfrak{p}$ enthält. Dann ist $\mathfrak{P}' := \Lambda'\mathfrak{P}\Lambda'$ ein zweiseitiges Ideal von Λ', vgl. Proposition 2.38, das invertierbar ist. Man erhält damit $(\Lambda' : \Lambda)\mathfrak{P}'^{-1}\mathfrak{P} \subseteq (\Lambda' : \Lambda)\mathfrak{P}'^{-1}\mathfrak{P}' = (\Lambda' : \Lambda)\Lambda' \subseteq \Lambda$, also

$$(\Lambda' : \Lambda)\mathfrak{P}'^{-1} \subseteq (\Lambda/\mathfrak{P}). \tag{3.12}$$

Aus $(\Lambda' : \Lambda)^2\mathfrak{P}' = ((\Lambda' : \Lambda)\Lambda')\mathfrak{P}((\Lambda' : \Lambda)\Lambda') \subseteq \Lambda\mathfrak{P}\Lambda \subseteq \mathfrak{P}$ folgert man $((\Lambda' : \Lambda)\mathfrak{P}'^{-1})\mathfrak{P} \supseteq ((\Lambda' : \Lambda)\mathfrak{P}'^{-1})(\Lambda' : \Lambda)^2\mathfrak{P}' \supseteq (\Lambda' : \Lambda)^3\Lambda' \supseteq (\Lambda' : \Lambda)^3\Lambda$, und damit

$$(\Lambda' : \Lambda)^3\Lambda \subseteq ((\Lambda' : \Lambda)\mathfrak{P}'^{-1})\mathfrak{P}. \tag{3.13}$$

Setzt man (3.12) ein, so liefert dies $(\Lambda/\mathfrak{P})\mathfrak{P} \supseteq ((\Lambda' : \Lambda)\mathfrak{P}'^{-1})\mathfrak{P} \supseteq (\Lambda' : \Lambda)^3\Lambda$, wobei für die letzte Inklusion (3.13) verwendet wurde. $\mathfrak{p}\Lambda$ ist trivialerweise in $(\Lambda/\mathfrak{P})\mathfrak{P}$ enthalten, so daß $(\Lambda/\mathfrak{P})\mathfrak{P} \supseteq (\Lambda' : \Lambda)^3\Lambda + \mathfrak{p}\Lambda \supseteq ((\Lambda' : \Lambda)^3 + \mathfrak{p})\Lambda = \Lambda$ folgt.

Mit der triviale Inklusion $\Lambda \supseteq (\Lambda/\mathfrak{P})\mathfrak{P}$ sieht man $\Lambda = (\Lambda/\mathfrak{P})\mathfrak{P}$. Auf die gleiche Weise zeigt man, daß auch $\Lambda = \mathfrak{P}(\Lambda/\mathfrak{P})$ gilt, $\mathfrak{P}$ demnach invertierbar ist.

Jetzt seien alle maximalen zweiseitigen Ideale von Λ, die $\mathfrak{p}$ enthalten, invertierbar. Korollar 3.5 zeigt, daß Λ genau dann $\mathfrak{p}$-maximal ist, wenn Λ mit der $\mathfrak{p}$-maximalen Zwischenordnung $\Lambda^{(\mathfrak{p})}$ zu Λ' übereinstimmt. Nach Proposition 3.4 existiert ein $\nu > 0$ und es gilt $\mathfrak{a} := \mathfrak{p}^\nu\Lambda^{(\mathfrak{p})} \subseteq \Lambda$. $\mathfrak{a}$ ist daher ein (ganzes) zweiseitiges Ideal von Λ, das $\mathfrak{p}^\nu$ enthält.

Nun läßt sich $\mathfrak{a}$ aber nach Korollar 2.51 als Produkt der maximalen zweiseitigen Ideale von Λ, die $\mathfrak{p}$ enthalten, schreiben, und ist folglich invertierbar. Mit $\mathfrak{a}$ läßt sich dann auch das (gebrochene) zweiseitige Ideal $\Lambda^{(\mathfrak{p})}$ in Λ invertieren. Es muß nach Proposition 2.39 $\mathcal{O}_l(\Lambda^{(\mathfrak{p})}) = \Lambda$, also $\Lambda = \Lambda^{(\mathfrak{p})}$ gelten. □

Die Verwendung von Proposition 3.10 liefert dann

(3.14) **Korollar** *Die R-Ordnung Λ ist genau dann $\mathfrak{p}$-maximal, wenn für alle maximalen zweiseitigen Ideale $\mathfrak{P}$ von Λ, die $\mathfrak{p}$ enthalten, $\mathcal{O}_l(\mathfrak{P}) = \Lambda$ gilt.*

Man muß demnach für jedes der maximal n Primideale $\mathfrak{P}$ der Ordnung Λ, die $\mathfrak{p}$ enthalten, testen, ob $\mathcal{O}_l(\mathfrak{P}) = \Lambda$ gilt, wobei n die Dimension der F-Algebra A ist, vgl. Korollar 5.22.

(3.15) **Bemerkung** *Korollar 2.51 und Theorem 3.11 zeigen, daß die maximalen Ideale $\mathfrak{p}$ von R, für die die Ordnung Λ nicht $\mathfrak{p}$-maximal ist, sich in der Ordnung Λ nicht vollständig faktorisieren lassen.*

3.5 Berechnung von Maximalordnungen

In diesem Abschnitt werden die theoretischen Ergebnisse (besonders Korollar 3.14) nun zu entsprechenden Algorithmen ausgebaut, die es erlauben zu einer gegeben Ordnung Λ und einem maximalen Ideal $\mathfrak{p}$ von R erst eine $\mathfrak{p}$-maximale Ordnung $\Lambda^{(\mathfrak{p})}$ zu berechnen (Algorithmus 3.16), die Λ enthält, und anschließend dann eine Maximalordnung $\Lambda^{(\max)} \supseteq \Lambda$ (Algorithmus 3.18, Algorithmus 3.20).

(3.16) **Algorithmus $\mathfrak{p}$-maximale Ordnung (Round 1)**
Input: *Eine Ordnung Λ und ein maximales Ideal $\mathfrak{p}$ von R.*
Output: *Eine $\mathfrak{p}$-maximale Ordnung $\Lambda^{(\mathfrak{p})} \supseteq \Lambda$.*

(1) *Initialisiere $\Lambda^{(\mathfrak{p})} := \Lambda$.*
(2) *Berechne alle maximalen Ideale $\mathfrak{P}_1, \ldots, \mathfrak{P}_s$ von $\Lambda^{(\mathfrak{p})}$, die $\mathfrak{p}$ enthalten.*
(3) *Für $(1 \leq i \leq s)$ liefert Korollar 2.17 $\mathcal{O}_l(\mathfrak{P}_i)$.*
(4) *Gilt $\Lambda^{(\mathfrak{p})} \subset \mathcal{O}_l(\mathfrak{P}_i)$, dann ersetze $\Lambda^{(\mathfrak{p})} := \mathcal{O}_l(\mathfrak{P}_i)$ und gehe zu Schritt (2).*
(5) *Gilt $\Lambda^{(\mathfrak{p})} = \mathcal{O}_l(\mathfrak{P}_i)$ für $(1 \leq i \leq s)$, dann terminiere.*

Verfahren zur Berechnung der maximalen Ideale, die $\mathfrak{p}$ enthalten, findet man in Abschnitt 5.2.2.

(3.17) **Proposition** *Es sei $\operatorname{disc}(\Lambda) = \mathfrak{p}^{2\mu}\mathfrak{q}$ mit $\mathfrak{q} \not\subseteq \mathfrak{p}^2$. Die Komplexität von Algorithmus 3.16 beträgt $O(\mu(n^5+g(n)))$, wobei $g(n)$ die Komplexität für die Berechnung der $\mathfrak{p}$ enthaltenden Primideale einer beliebigen Ordnung ist.*

Beweis: Ist $\Lambda^{(\mathfrak{p})}$ in Schritt (4) nicht $\mathfrak{p}$-maximal, dann liefert $\mathcal{O}_l(\mathfrak{P})$ für ein $\mathfrak{p} \subseteq \mathfrak{P}$ eine größere Ordnung. Für $x \in \mathcal{O}_l(\mathfrak{P})$ gilt $\mathfrak{p}x = x\mathfrak{p} \subseteq x\mathfrak{P} \subseteq \mathfrak{P} \subseteq \Lambda^{(\mathfrak{p})}$, also $\mathfrak{p}\mathcal{O}_l(\mathfrak{P}) \subseteq \Lambda^{(\mathfrak{p})}$. Es gilt demnach $(\mathcal{O}_l(\mathfrak{P}) : \Lambda^{(\mathfrak{p})}) \mid \mathfrak{p}^n$.

Nach maximal μ solchen Aufstiegen ist man an einer $\mathfrak{p}$-maximalen Ordnung angelangt. Unter Umständen muß man aber in jedem dieser (maximal) μ Schritte alle $\mathfrak{p}$ enthaltenden Primideale konstruieren $(g(n))$ und anschließend für jedes der maximal n Primideale (Korollar 5.22) die Links-Ordnung berechnen $(O(n^4))$.

Den Test $\Lambda_{\mathfrak{p}} = \mathcal{O}_l(\mathfrak{P}_i)$ bekommt man durch eine geeignete Modifikation von Algorithmus 2.16: „=“ gilt genau dann, wenn die Diskriminanten gleich sind. Es genügt daher, das Produkt der Koeffizientenideale aus der Darstellung von $\Lambda^{(\mathfrak{p})}$ mit dem Produkt $\prod_{j=1}^{n} \mathfrak{c}_j |\tilde{M}|$ der Koeffizientenideale und der Determinante der Matrix der Hermite-Normal-Form aus Algorithmus 2.16 Schritt (3) zu vergleichen. Da $\tilde{M}$ in Dreiecksform ist, hat dieser Test eine Komplexität von $O(n)$. □

(3.18) **Algorithmus Maximalordnung (iterativ)**
Input: *Eine Ordnung* Λ.
Output: *Eine Maximalordnung* $\Lambda^{(max)} \supseteq \Lambda$.
(1) *Faktorisiere die Diskriminante* $\mathrm{disc}(\Lambda) = \prod_{j=1}^{r} \mathfrak{p}_j^{e_j}$.
(2) *Initialisiere* $\Lambda^{(max)} := \Lambda$.
(3) *Für* $(1 \leq j \leq r, e_j > 1)$ *wiederhole*
(4) *Algorithmus 3.16 liefert eine* $\mathfrak{p}_j$*-maximale Ordnung* $\Lambda' \supseteq \Lambda^{(max)}$.
(5) *Setze* $\Lambda^{(max)} := \Lambda'$.

(3.19) **Proposition** *Für die maximalen Ideale* $\mathfrak{p}, \mathfrak{q}$ *von* R *seien die Ordnungen* $\Lambda^{(\mathfrak{p})}, \Lambda^{(\mathfrak{q})} \supseteq \Lambda$ $\mathfrak{p}$*-maximal bzw.* $\mathfrak{q}$*-maximal. Dann ist die Ordnung* $\Lambda' := \Lambda^{(\mathfrak{p})} + \Lambda^{(\mathfrak{q})}$ *sowohl* $\mathfrak{p}$*-maximal als auch* $\mathfrak{q}$*-maximal.*

Beweis: Ohne Einschränkung gelte $\mathfrak{p} \neq \mathfrak{q}$. Die Summe zweier voller R-Gitter ist trivialerweise wieder ein volles R-Gitter. Es existieren $\mu, \nu > 0$ mit $\mathfrak{p}^{\mu}\Lambda^{(\mathfrak{p})} \subseteq \Lambda$ und $\mathfrak{q}^{\nu}\Lambda^{(\mathfrak{q})} \subseteq \Lambda$. Weiterhin seien $\alpha \in \mathfrak{p}^{\mu}$ und $\beta \in \mathfrak{q}^{\nu}$ mit $\alpha + \beta = 1$. Für $x \in \Lambda^{(\mathfrak{p})}, y \in \Lambda^{(\mathfrak{q})}$ erhält man dann $xy = \alpha xy + \beta xy = (\alpha x)y + x(\beta y) \subseteq \Lambda\Lambda_{\mathfrak{q}} + \Lambda^{(\mathfrak{p})}\Lambda = \Lambda^{(\mathfrak{q})} + \Lambda_{\mathfrak{p}}$. Damit ist Λ' eine Ordnung, vgl. Korollar 1.8.

Angenommen Λ' ist nicht $\mathfrak{p}$-maximal, dann liefert $\mathfrak{p} \mid (\Lambda^{(\max)} : \Lambda') \mid (\Lambda^{(\max)} : \Lambda^{(\mathfrak{p})})$ einen Widerspruch. □

Hiermit kann man den Algorithmus zur Berechnung der Maximalordnung auch parallelisieren. Dies bietet sich zum Beispiel in einem Computeralgebra-System wie KASH [DFK+97] an, das mit dem PVM System (Parallel Virtual Machine) [GBD+94] ausgestattet ist. Damit können die einzelnen $\mathfrak{p}$-maximalen Ordnungen in einem heterogenen Netzwerk auf unterschiedlichen Computern berechnet werden und anschließend wieder zu einer Maximalordnung zusammengesetzt werden:

(3.20) **Algorithmus Maximalordnung (parallel)**
Input: *Eine Ordnung* Λ.
Output: *Eine Maximalordnung* $\Lambda^{(max)} \supseteq \Lambda$.
(1) *Faktorisiere die Diskriminante* $\mathrm{disc}(\Lambda) = \prod_{j=1}^{r} \mathfrak{p}_j^{e_j}$.
(2) *Für* $(1 \leq j \leq r, e_j > 1)$ *wiederhole*
(3) *Algorithmus 3.16 liefert eine* $\mathfrak{p}_j$*-maximale Ordnung* $\Lambda_j \supseteq \Lambda$.
(4) *Setze* $\Lambda^{(max)} := \sum_{j=1}^{r} \Lambda_j$.

(3.21) **Bemerkung** *Die Komplexität von Algorithmus 3.18 sowie Algorithmus 3.20 wird im wesentlichen von der Faktorisierung der Diskriminante beeinflußt.*

Die Erfahrung im Bereich algebraischer Zahlkörper zeigt, daß der „kritische“ Teil bei Konstruktion der Maximalordnung die Faktorisierung der

Diskriminante ist. Die Polynomdiskriminante von $f(t) = t^n - a \in \mathbb{Z}[t]$ *ist* $(-1)^{\binom{n}{2}} n^n a^{n-1}$*, vgl. [Ber27, S. 63]. Die Diskriminante ist unter Umständen also exponentiell im Grad der Erweiterung.*

(3.22) **Bemerkung** *Die neue Diskriminante läßt sich in Algorithmus 3.16 leicht durch Betrachtung der Koeffizientenideale und der Determinante der Matrix der Hermite-Normal-Form aus Algorithmus 2.16 Schritt (3) berechnen.*

Damit ist es möglich, nach jedem Aufstieg zu testen, ob $\mathfrak{p}$ *weiterhin ein quadratischer Teiler der Diskriminante ist. Aus Gründen der Übersichtlichkeit wurde darauf verzichtet, diese Verbesserungen in die Algorithmen direkt einzubauen.*

3.6 Lokalisierung

Nicht nur im theoretischen Teil ist die Verwendung von Lokalisierungen sinnvoll, sie läßt sich unter Umständen auch praktisch gewinnbringend einsetzen, d.h. wenn die Lokalisierung von dem Computeralgebra-System unterstützt wird.

Für ein maximales Ideal $\mathfrak{p}$ von R ist die Lokalisierung $R_\mathfrak{p} = S^{-1}R$ von R an $\mathfrak{p}$, mit $S = R \setminus \mathfrak{p}$, ein diskreter Bewertungsring. Die *Lokalisierung* des R-Gitters Λ ist definiert als $\Lambda_\mathfrak{p} := R_\mathfrak{p} \otimes_R \Lambda$. Da Λ torsionsfrei ist, kann $R_\mathfrak{p} \otimes_R \Lambda$ mit $S^{-1}\Lambda$ identifiziert werden. Ist Λ ein volles R-Gitter in A, so ist $\Lambda_\mathfrak{p}$ ein volles $R_\mathfrak{p}$-Gitter in A, vgl. [Rei75, Chpt. 1, Sect. 3b] oder [OMe63, §81E].

Nicht nur die R-Gitter $\Lambda \subseteq \Lambda'$ in A, sondern auch die dazugehörigen Größen Diskriminante, Ordnungsideal und Index lassen sich lokalisieren. Es gilt $\operatorname{disc}(\Lambda_\mathfrak{p}) = (\operatorname{disc}(\Lambda))_\mathfrak{p}$ [PZ89, Chpt. 4, (5.47)], $\operatorname{ord}(\Lambda'_\mathfrak{p}/\Lambda_\mathfrak{p}) = \operatorname{ord}((\Lambda'/\Lambda)_\mathfrak{p}) = (\operatorname{ord}(\Lambda'/\Lambda))_\mathfrak{p}$ [Rei75, Thm. 4.20]. Daraus leitet sich dann die Lokalisierung des Index $(\Lambda'_\mathfrak{p} : \Lambda_\mathfrak{p}) = (\Lambda' : \Lambda)_\mathfrak{p}$ und ebenso die Lokalisierung der reduzierten Diskriminante $\operatorname{disc}_r(\Lambda_\mathfrak{p}) = (\operatorname{disc}_r(\Lambda))_\mathfrak{p}$ ab, siehe auch [PZ89, Chpt. 4, (5.47)].

Weiterhin gilt $\Lambda = \bigcap_\mathfrak{p} \Lambda_\mathfrak{p}$, wobei $\mathfrak{p}$ alle maximalen Ideale von R durchläuft [Rei75, Thm. 4.21]. Ist für jedes maximale Ideal $\mathfrak{p}$ von R ein volles $R_\mathfrak{p}$-Gitter $X(\mathfrak{p})$ in A gegeben, so ist $\Lambda = \bigcap_\mathfrak{p} X(\mathfrak{p})$ ein volles R-Gitter in A und es gilt $\Lambda_\mathfrak{p} = X(\mathfrak{p})$ [Rei75, Thm. 4.22].

Übertragen auf R-Ordnungen ist die Lokalisierung $\Lambda_\mathfrak{p}$ einer R-Ordnung Λ eine $R_\mathfrak{p}$-Ordnung in A.

(3.23) **Proposition** [Rei75, Cor. 11.2], [CR81, Thm 26.21] *Die Ordnung* Λ *ist genau dann maximal, wenn für jedes maximale Ideal* $\mathfrak{p}$ *von* R *die Lokalisierung* $\Lambda_\mathfrak{p}$ *maximal ist.*

(3.24) **Proposition** *Für ein maximales Ideal $\mathfrak{p}$ ist die R-Ordnung Λ genau dann $\mathfrak{p}$-maximal, wenn die $R_\mathfrak{p}$-Ordnung $\Lambda_\mathfrak{p}$ maximal ist.*

Beweis: Λ ist $\mathfrak{p}$-maximal $\Leftrightarrow$ $\mathfrak{p}$ teilt nicht $(\Lambda^{(\max)} : \Lambda) \Leftrightarrow ((\Lambda^{(\max)})_\mathfrak{p} : \Lambda_\mathfrak{p}) = (\Lambda^{(\max)} : \Lambda)_\mathfrak{p} = R_\mathfrak{p} \Leftrightarrow \Lambda_\mathfrak{p} = \Lambda_\mathfrak{p}^{(\max)} \Leftrightarrow \Lambda_\mathfrak{p}$ ist maximal. □

Man kann also zu einer gegebenen Ordnung Λ und gegebenem maximalem Ideal $\mathfrak{p}$ von R in der Lokalisierung eine Maximalordnung mit Algorithmus 3.16 ausrechnen. Dies hat den Vorteil, daß man über einem diskreten Bewertungsring $R_\mathfrak{p}$ arbeitet und nicht über dem Dedekindring R. Die Hermite-Normal-Form muß also nur über einem Hauptidealring berechnet werden, und man kann sich die Operationen mit den Koeffizientenidealen sparen.

Hat man eine maximale $R_\mathfrak{p}$ Ordnung $\Lambda_\mathfrak{p}^{(\max)}$ berechnet, so kommt man wie folgt zu einer $\mathfrak{p}$-maximalen R-Ordnung zurück. Man setzt $X(\mathfrak{p}) := \Lambda_\mathfrak{p}^{(\max)}$ und $X(\mathfrak{q}) := \Lambda_\mathfrak{q}$, für $\mathfrak{q} \neq \mathfrak{p}$. Dann ist $\Lambda' := \bigcap_\mathfrak{p} X(\mathfrak{p})$ eine R-Ordnung in A, die $\mathfrak{p}$-maximal ist, vgl. Proposition 3.24. Ist $(\Lambda_\mathfrak{p}^{(\max)} : \Lambda_\mathfrak{p}) = \mathfrak{p}^\nu R_\mathfrak{p}$, so erhält man Λ' auch einfach durch den Schnitt der zwei Gitter $\Lambda_\mathfrak{p}^{(\max)} \cap \mathfrak{p}^{-\nu}\Lambda$.

Es folgen noch einige Zusammenhänge zwischen Idealen von Λ und deren Lokalisierungen in $\Lambda_\mathfrak{p}$. Jedes zweiseitige Ideal $\mathfrak{m}$ von Λ erzeugt durch $R_\mathfrak{p}\mathfrak{m}$ ein zweiseitiges Ideal von $\Lambda_\mathfrak{p}$ und umgekehrt erhält man aus einem zweiseitigen Ideal $\mathfrak{m}_\mathfrak{p}$ von $\Lambda_\mathfrak{p}$ durch $\mathfrak{m}_\mathfrak{p} \cap \Lambda$ ein zweiseitiges Ideal von Λ. Die erste Aussage ist eine Verallgemeinerung von [Gil72, Thm. 4.4(2)].

(3.25) **Proposition** *Es sei $\mathfrak{m}_\mathfrak{p}$ ein beliebiges zweiseitiges Ideal von $\Lambda_\mathfrak{p}$, dann gilt $R_\mathfrak{p}(\Lambda \cap \mathfrak{m}_\mathfrak{p}) = \mathfrak{m}_\mathfrak{p}$.*

Beweis: Trivialerweise gilt wegen $\Lambda \cap \mathfrak{m}_\mathfrak{p} \subseteq \mathfrak{m}_\mathfrak{p}$ auch $R_\mathfrak{p}(\Lambda \cap \mathfrak{m}_\mathfrak{p}) \subseteq \mathfrak{m}_\mathfrak{p}$. Sei $x \in \mathfrak{m}_\mathfrak{p}$, dann existieren $y \in \mathfrak{m}, s \in R \setminus \mathfrak{p}$ mit $\frac{1}{s}y = x$. Es gilt aber auch $y \in \Lambda \cap \mathfrak{m}_\mathfrak{p}$, also $x \in R_\mathfrak{p}(\Lambda \cap \mathfrak{m}_\mathfrak{p})$. □

Natürlich gilt auch $\mathfrak{m} \subseteq (R_\mathfrak{p}\mathfrak{m}) \cap \Lambda$ für jedes beliebige zweiseitige Ideal $\mathfrak{m}$ von Λ.

(3.26) **Proposition** *Für ein Primideal $\mathfrak{P} \subseteq \Lambda$, das $\mathfrak{p}$ enthält, gilt sogar $\mathfrak{P} = (R_\mathfrak{p}\mathfrak{P}) \cap \Lambda$.*

Beweis: Sei $x = \frac{1}{s}y \in (R_\mathfrak{p}\mathfrak{P}) \cap \Lambda$ mit $y \in \mathfrak{P}$ und $s \in R \setminus \mathfrak{P}$. Wegen $s\frac{1}{s}y \in \mathfrak{P}$ folgt auch $s\Lambda\frac{1}{s}y = \Lambda s\frac{1}{s}y \subseteq \mathfrak{P}$ und mit Proposition 2.26 $\frac{1}{s}y \in \mathfrak{P}$. □

(3.27) **Proposition** *Ist $\mathfrak{P}$ ein Primideal von Λ, das $\mathfrak{p}$ enthält, dann ist $\mathfrak{P}_\mathfrak{p} = R_\mathfrak{p}\mathfrak{P}$ ein Primideal von $\Lambda_\mathfrak{p}$. Ist umgekehrt $\mathfrak{P}_\mathfrak{p}$ ein Primideal von $\Lambda_\mathfrak{p}$, so ist $\mathfrak{P} = \mathfrak{P}_\mathfrak{p} \cap \Lambda$ ein Primideal von Λ.*

Beweis: Sei $\mathfrak{P} \supseteq \mathfrak{p}$ ein Primideal von Λ. Angenommen für das zweiseitige Ideal $\mathfrak{P}_\mathfrak{p} := R_\mathfrak{p}\mathfrak{P}$ würde gelten $\mathfrak{P}_\mathfrak{p} \subset \mathfrak{m}_\mathfrak{p} \subset \Lambda_\mathfrak{p}$, dann folgt auch $\mathfrak{m} := \mathfrak{m}_\mathfrak{p} \cap \Lambda \subset \Lambda$ (liegt $1 \in \mathfrak{m}$, so liegt auch $1 \in R_\mathfrak{p}\mathfrak{m} \subseteq \mathfrak{m}_\mathfrak{p}$). Aus $\mathfrak{P} = \mathfrak{P}_\mathfrak{p} \cap \Lambda \subseteq \mathfrak{m}_\mathfrak{p} \cap \Lambda = \mathfrak{m}$ folgert man mit Proposition 3.25 sofort den Widerspruch $\mathfrak{P}_\mathfrak{p} = \mathfrak{m}_\mathfrak{p}$. $\mathfrak{P}_\mathfrak{p}$ ist daher ein Primideal in der $R_\mathfrak{p}$-Ordnung $\Lambda_\mathfrak{p}$.

Sei jetzt $\mathfrak{P}_\mathfrak{p}$ ein Primideal von $\Lambda_\mathfrak{p}$. Angenommen für $\mathfrak{P} := \mathfrak{P}_\mathfrak{p} \cap \Lambda$ würde $\mathfrak{P} \subset \mathfrak{m}$ mit einem Primideal $\mathfrak{m}$ gelten, dann folgt aus dem ersten Teil der Aussage und aus Proposition 3.25 $R_\mathfrak{p}\mathfrak{m} = \mathfrak{P}_\mathfrak{p}$. Es folgt $\mathfrak{m} \subseteq (R_\mathfrak{p}\mathfrak{m}) \cap \Lambda = \mathfrak{P}$, also ein Widerspruch. □

(3.28) **Proposition** *Sind $\mathfrak{P}_1, \mathfrak{P}_2$ zwei Primideale von Λ, so gilt $R_\mathfrak{p}(\mathfrak{P}_1 \cap \mathfrak{P}_2) = R_\mathfrak{p}\mathfrak{P}_1 \cap R_\mathfrak{p}\mathfrak{P}_2$.*

Beweis: Der Beweis gliedert sich in drei Teile. Zuerst sei $\mathfrak{p} \subseteq \mathfrak{P}_1, \mathfrak{P}_2$. Aus Proposition 3.27 folgt $(R_\mathfrak{p}\mathfrak{P}_1 \cap R_\mathfrak{p}\mathfrak{P}_2) \cap \Lambda = (R_\mathfrak{p}\mathfrak{P}_1 \cap \Lambda) \cap (R_\mathfrak{p}\mathfrak{P}_2 \cap \Lambda) = \mathfrak{P}_1 \cap \mathfrak{P}_2$. Auf der anderen Seite gilt $R_\mathfrak{p}\mathfrak{P}_1 \cap R_\mathfrak{p}\mathfrak{P}_2 = R_\mathfrak{p}((R_\mathfrak{p}\mathfrak{P}_1 \cap R_\mathfrak{p}\mathfrak{P}_2) \cap \Lambda) = R_\mathfrak{p}(\mathfrak{P}_1 \cap \mathfrak{P}_2)$, vgl. Proposition 3.25.

Jetzt gelte ohne Einschränkung $\mathfrak{p} \neq \mathfrak{q} \subseteq \mathfrak{P}_1$ und $\mathfrak{p} \subseteq \mathfrak{P}_2$ mit dem Primideal $\mathfrak{q}$ von R. Es gilt $(R_\mathfrak{p}\mathfrak{P}_1 \cap R_\mathfrak{p}\mathfrak{P}_2) \cap \Lambda = (R_\mathfrak{p}\mathfrak{P}_1 \cap \Lambda) \cap (R_\mathfrak{p}\mathfrak{P}_2 \cap \Lambda) = \Lambda \cap (R_\mathfrak{p}\mathfrak{P}_2 \cap \Lambda) = \Lambda \cap \mathfrak{P}_2 = \mathfrak{P}_2$ nach Proposition 3.27. Aus Proposition 3.25 folgt dann $R_\mathfrak{p}\mathfrak{P}_1 \cap R_\mathfrak{p}\mathfrak{P}_2 = R_\mathfrak{p}((R_\mathfrak{p}\mathfrak{P}_1 \cap R_\mathfrak{p}\mathfrak{P}_2) \cap \Lambda) = R_\mathfrak{p}\mathfrak{P}_2$. Trivialerweise gilt $R_\mathfrak{p}(\mathfrak{P}_1 \cap \mathfrak{P}_2) \subseteq R_\mathfrak{p}\mathfrak{P}_2$, außerdem folgt aus $\mathfrak{P}_1\mathfrak{P}_2 \subseteq \mathfrak{P}_1 \cap \mathfrak{P}_2$ auch $R_\mathfrak{p}\mathfrak{P}_2 = \Lambda_\mathfrak{p}\mathfrak{P}_2 = (R_\mathfrak{p}\mathfrak{P}_1)\mathfrak{P}_2 = R_\mathfrak{p}(\mathfrak{P}_1\mathfrak{P}_2) \subseteq R_\mathfrak{p}(\mathfrak{P}_1 \cap \mathfrak{P}_2) \subseteq R_\mathfrak{p}\mathfrak{P}_2$. Man erhält $R_\mathfrak{p}(\mathfrak{P}_1 \cap \mathfrak{P}_2) = R_\mathfrak{p}\mathfrak{P}_2 = R_\mathfrak{p}\mathfrak{P}_1 \cap R_\mathfrak{p}\mathfrak{P}_2$.

Zum Abschluß seien $\mathfrak{q}_1 \subseteq \mathfrak{P}_1$ und $\mathfrak{q}_2 \subseteq \mathfrak{P}_2$ mit den Primidealen $\mathfrak{p} \neq \mathfrak{q}_1, \mathfrak{q}_2$ von R. $R_\mathfrak{p}\mathfrak{P}_1 \cap R_\mathfrak{p}\mathfrak{P}_2 = \Lambda_\mathfrak{p} \cap \Lambda_\mathfrak{p} = \Lambda_\mathfrak{p}$. Es existiert ein $s \notin \mathfrak{p}, s \in \mathfrak{q}_1\mathfrak{q}_2 \subseteq \mathfrak{q}_1 \cap \mathfrak{q}_2 \subseteq \mathfrak{P}_1 \cap \mathfrak{P}_2$, woraus sofort $1 = \frac{s}{s} \in R_\mathfrak{p}(\mathfrak{P}_1 \cap \mathfrak{P}_2)$ und damit $R_\mathfrak{p}(\mathfrak{P}_1 \cap \mathfrak{P}_2) = \Lambda_\mathfrak{p} = R_\mathfrak{p}\mathfrak{P}_1 \cap R_\mathfrak{p}\mathfrak{P}_2$ folgt. □

Kapitel 4
Der Round 2 Algorithmus

Im „Second Round of the Maximal Order Program“ [Zas72] hat Zassenhaus nicht nur eine Verbesserung des bisherigen Verfahrens eingebracht, sondern gleichzeitig den Namen *Round 2 Algorithmus* für das Verfahren geliefert, das heute in fast allen Computeralgebra-Systemen zur Berechnung der Maximalordnungen in globalen Körpern verwendet wird.

4.1 Hereditäre Ordnungen

Eine R-Ordnung $\Lambda^{(\mathrm{her})}$ heißt *hereditär* oder *erblich*, wenn jedes Links-Ideal von Λ ein *projektiver* Λ-Modul, also direkter Summand eines freien Moduls, ist. Λ ist genau dann hereditär, wenn jedes Rechts-Ideal von Λ projektiv ist [Rei75, Thm. 40.1].

Dem *Round 2 Algorithmus* liegt die Idee zugrunde, die gegebene Ordnung Λ zuerst in eine hereditäre Ordnung $\Lambda^{(\mathrm{her})} \supseteq \Lambda$ und anschließend die hereditäre Ordnung in eine maximale Ordnung $\Lambda^{(\max)} \supseteq \Lambda^{(\mathrm{her})}$ einzubetten. Da jede Maximalordnung $\Lambda^{(\max)}$ hereditär ist [AG60, Thm. 2.3], [Rei75, Thm. 21.4] oder [CR81, Thm. 26.12(i)], und mit der hereditären Ordnung Λ auch jede Ordnung $\Lambda' \supseteq \Lambda$ hereditär ist [Rei75, Thm. 40.4], scheint diese Vorgehensweise sinnvoll.

Ebenso wie die Maximalität läßt sich auch die Eigenschaft hereditär sowohl über die einfachen Bestandteile der Algebra A charakterisieren (Theorem 1.4) als auch lokalisieren (Proposition 3.23).

(4.1) **Proposition** [Rei75, Thm. 40.7], [CR81, Thm. 26.20a] *Für die separable F-Algebra A seien $R_i = \mathrm{Cl}(R, \mathrm{Z}(A_i))$ $(1 \le i \le v)$ die ganzen Abschlüsse von R in den Zentren der einfachen Bestandteile. Dann gelten:*

(1) Für jede hereditäre R-Ordnung Λ in A gilt $\Lambda = \bigoplus_{i=1}^{v} \Lambda e_i$, wobei Λe_i hereditäre R-Ordnungen in A_i $(1 \le i \le v)$ sind.

(2) Sind Λ_i $(1 \le i \le v)$ hereditäre R-Ordnungen in A_i, dann ist $\bigoplus_{i=1}^{v} \Lambda_i$ eine hereditäre R-Ordnung in A.

(4.2) **Proposition** [Rei75, Cor. 3.24], [CR81, Thm 26.21a] *Die Ordnung Λ ist genau dann hereditär, wenn für jedes maximale Ideal $\mathfrak{p}$ von R die Lokalisierung $\Lambda_{\mathfrak{p}}$ hereditär ist.*

4.2 Vervollständigungen

Im folgenden sei $R_\mathfrak{p}$ die Lokalisierung des Dedekindringes R an dem maximalen Ideal $\mathfrak{p}$ von R. Das Primideal $\mathfrak{p}$ erzeugt die $\mathfrak{p}$-*adische exponentielle Bewertung* $\nu_\mathfrak{p} : F \to \mathbb{Z} \cup \{\infty\}$ z.B. [Rei75, (4.19a)], wobei $R_\mathfrak{p}$ gerade der Bewertungsring von $\nu_\mathfrak{p}$ ist. Die *Vervollständigung* von F bezüglich $\nu_\mathfrak{p}$ wird mit $\hat{F}_\mathfrak{p}$ bezeichnet. Die $\mathfrak{p}$-adische Bewertung von $\hat{F}_\mathfrak{p}$ sei $\hat{\nu}_\mathfrak{p}$ und der Bewertungsring von $\hat{\nu}_\mathfrak{p}$ sei $\hat{R}_\mathfrak{p}$. Ebenso wird auch die separable F-Algebra vervollständigt $\hat{A}_\mathfrak{p} := \hat{F}_\mathfrak{p} \otimes_F A$. $\hat{A}_\mathfrak{p}$ ist eine separable $\hat{F}_\mathfrak{p}$-Algebra [Rei75, Ex. 7.13].

Ein R-Gitter Λ kann analog zur Lokalisierung auch vervollständigt werden $\hat{\Lambda}_\mathfrak{p} := \hat{R}_\mathfrak{p} \otimes_R \Lambda \cong \hat{R}_\mathfrak{p} \otimes_{R_\mathfrak{p}} \Lambda_\mathfrak{p}$. Wie in Abschnitt 3.6 (Lokalisierung) kann $\hat{\Lambda}_\mathfrak{p}$ bzw. $\hat{A}_\mathfrak{p}$ wegen der Torsionsfreiheit mit $\hat{R}_\mathfrak{p}\Lambda$ bzw. $\hat{F}_\mathfrak{p}A$ identifiziert werden.

(4.3) **Proposition** [Rei75, Thm. 5.2] *Für ein volles $R_\mathfrak{p}$-Gitter $\Lambda_\mathfrak{p}$ in A ist $\hat{\Lambda}_\mathfrak{p} = \hat{R}_\mathfrak{p}\Lambda_\mathfrak{p}$ ein volles $\hat{R}_\mathfrak{p}$-Gitter in $\hat{A}_\mathfrak{p}$. Umgekehrt ist für ein volles $\hat{R}_\mathfrak{p}$-Gitter $\hat{\Lambda}_\mathfrak{p}$ in $\hat{A}_\mathfrak{p}$ die Menge $\Lambda_\mathfrak{p} := \hat{\Lambda}_\mathfrak{p} \cap A$ ein volles $R_\mathfrak{p}$-Gitter in A.*

Dies liefert eine bijektive Abbildung zwischen den vollen $R_\mathfrak{p}$-Gittern in A und den vollen $\hat{R}_\mathfrak{p}$-Gitter in $\hat{A}_\mathfrak{p}$, die die Inklusion erhält.

(4.4) **Proposition** [Rei75, Thm. 40.5] *Die R-Ordnung Λ ist genau dann hereditär, wenn für jedes maximale Ideal $\mathfrak{p}$ von R die $\hat{R}_\mathfrak{p}$-Ordnung $\hat{\Lambda}_\mathfrak{p}$ hereditär ist.*

(4.5) **Korollar** *Die $R_\mathfrak{p}$-Ordnung $\Lambda_\mathfrak{p}$ ist genau dann hereditär, wenn die $\hat{R}_\mathfrak{p}$-Ordnung $\hat{\Lambda}_\mathfrak{p}$ hereditär ist.*

Es seien $\hat{\Lambda}_\mathfrak{p} \subseteq \hat{\Lambda}'_\mathfrak{p}$ zwei $\hat{R}_\mathfrak{p}$-Ordnungen. $J(\hat{\Lambda}_\mathfrak{p})$, bzw. $J(\hat{\Lambda}'_\mathfrak{p})$ bezeichne im folgenden das Jacobson-Radikal von $\hat{\Lambda}_\mathfrak{p}$, bzw. $\hat{\Lambda}'_\mathfrak{p}$. Man sagt die Ordnung $\hat{\Lambda}'_\mathfrak{p}$ *deckt* die Ordnung $\hat{\Lambda}_\mathfrak{p}$, vgl. [Rei75, S. 356] oder [Neb99, Def. 4.1.1(v)], wenn $J(\hat{\Lambda}_\mathfrak{p}) \subseteq J(\hat{\Lambda}'_\mathfrak{p})$ gilt. $\hat{\Lambda}_\mathfrak{p}$ heißt *extremal*, wenn sie in keiner weiteren deckenden Ordnung echt enthalten ist, vgl. [Rei75, S. 356] oder [Neb99, Def. 4.1.1(v)].

(4.6) **Bemerkung** *Ist der Dedekindring R nicht semilokal, dann ist das Jacobson-Radikal einer R-Ordnung Λ immer $J(\Lambda) = \{0\}$. Jede R-Ordnung $\Lambda' \supseteq \Lambda$ ist damit eine deckende Ordnung und der Begriff extremal fällt mit maximal zusammen.*

Im folgenden sei J bzw. $\hat{J}$ das Jacobson-Radikal der $R_\mathfrak{p}$-Ordnung $\Lambda_\mathfrak{p}$ bzw. der $\hat{R}_\mathfrak{p}$-Ordnung $\hat{\Lambda}_\mathfrak{p}$. Die Menge $Id(J) = \mathcal{O}_l(J) \cap \mathcal{O}_r(J)$ nennt man *Idealisator* von J, vgl. [Zas72, S. 409] oder [Neb99, Def. 4.1.4]. Entsprechend

ist $Id(\hat{J})$ der Idealisator von $\hat{J}$. In der Literatur gibt es auch andere Definitionen des Begriffs Idealisator, so zum Beispiel in [Gol72, S. 161].

Da sowohl $R_\mathfrak{p}$ als auch $\hat{R}_\mathfrak{p}$ lokal sind, fällt das Jacobson-Radikal der Ordnung mit dem $\mathfrak{p}$-Radikal zusammen, J und $\hat{J}$ sind also beides zweiseitige Ideale, gerade der Schnitt über alle maximalen zweiseitigen Ideale, die $\mathfrak{p}$ enthalten.

Als Erweiterung der Aussagen von Auslander und Goldmann [AG60, Cor. S. 5] erhält man

(4.7) **Proposition** *Für die $\hat{R}_\mathfrak{p}$-Ordnung $\hat{\Lambda}_\mathfrak{p}$ sind die folgenden Aussagen äquivalent:*

(1) $\hat{\Lambda}_\mathfrak{p}$ *ist hereditär,*

(2) $\hat{\Lambda}_\mathfrak{p}$ *ist extremal,*

(3) $\mathcal{O}_l(\hat{J}) = \hat{\Lambda}_\mathfrak{p}$,

(4) $\mathcal{O}_r(\hat{J}) = \hat{\Lambda}_\mathfrak{p}$,

(5) $Id(\hat{J}) = \hat{\Lambda}_\mathfrak{p}$.

Beweis: Die Äquivalenzen (1) $\Leftrightarrow$ (2) kann man [Jac71, Thm. 1 und Prop. 1] oder [Rei75, Thm. 39.14(i)], (2) $\Leftrightarrow$ (3) [Rei75, Thm. 39.11] entnehmen. Der Beweis zu (2) $\Leftrightarrow$ (4) verläuft analog zu (2) $\Leftrightarrow$ (3), ebenso wie (2) $\Leftrightarrow$ (5). Ein Beweis zu (1) $\Leftrightarrow$ (5) steht auch in [Neb99, Satz 4.1.5], wobei dort nur Ordnungen über Maximalordnungen in p-adischen Zahlkörpern betrachtet werden. An den Beweisen ändert sich allerdings nichts, so daß sie hier nicht aufgeführt werden. □

(4.8) **Proposition** *Es gilt $\mathcal{O}_l(\hat{J}) = \hat{\Lambda}_\mathfrak{p} \Leftrightarrow \mathcal{O}_l(J) = \Lambda_\mathfrak{p}$, $\mathcal{O}_r(\hat{J}) = \hat{\Lambda}_\mathfrak{p} \Leftrightarrow \mathcal{O}_r(J) = \Lambda_\mathfrak{p}$ und $Id(\hat{J}) = \hat{\Lambda}_\mathfrak{p} \Leftrightarrow Id(J) = \Lambda_\mathfrak{p}$.*

Beweis: Mit Proposition 4.3 erhält man $J = \hat{J} \cap A$ und $\hat{J} = \hat{R}_\mathfrak{p} J$. Ist $x \in \mathcal{O}_l(J)$, so folgt $x\hat{J} = x\hat{R}_\mathfrak{p} J = \hat{R}_\mathfrak{p} x J \subseteq \hat{R}_\mathfrak{p} J = \hat{J}$, also $\hat{R}_\mathfrak{p}\mathcal{O}_l(J) \subseteq \mathcal{O}_l(\hat{J})$. Für $x = A \cap \mathcal{O}_l(\hat{J})$ gilt $x J \subseteq x\hat{J} \subseteq \hat{J} \cap A = J$, also $\mathcal{O}_l(\hat{J}) \cap A \subseteq \mathcal{O}_l(J)$. Man folgert $\mathcal{O}_l(\hat{J}) = \hat{R}_\mathfrak{p}(\mathcal{O}_l(\hat{J}) \cap A) \subseteq \hat{R}_\mathfrak{p}\mathcal{O}_l(J)$, und damit $\hat{R}_\mathfrak{p}\mathcal{O}_l(J) = \mathcal{O}_l(\hat{J})$ und $\mathcal{O}_l(\hat{J}) \cap A = \mathcal{O}_l(J)$.

Ebenso erhält man auch $\hat{R}_\mathfrak{p}\mathcal{O}_r(J) = \mathcal{O}_r(\hat{J})$, und $\mathcal{O}_r(\hat{J}) \cap A = \mathcal{O}_r(J)$. Woraus man dann das folgende ableiten kann $Id(\hat{J}) \cap A = \mathcal{O}_l(\hat{J}) \cap A \cap \mathcal{O}_r(\hat{J}) = \mathcal{O}_l(J) \cap \mathcal{O}_r(J) = Id(J)$ und damit $\hat{R}_\mathfrak{p}\, Id(J) = \hat{R}_\mathfrak{p}(Id(\hat{J}) \cap A) = Id(\hat{J})$.

Damit ergeben sich dann $\mathcal{O}_l(J) = \Lambda_p \Leftrightarrow \mathcal{O}_l(\hat{J}) = \hat{R}_\mathfrak{p}\mathcal{O}_l(J) = \hat{R}_\mathfrak{p}\Lambda_\mathfrak{p} = \hat{\Lambda}_\mathfrak{p}$ und analog die anderen Äquivalenzen. □

(4.9) **Theorem** [Zas72, Thm. 4.2] *Für die $R_\mathfrak{p}$-Ordnung $\Lambda_\mathfrak{p}$ gilt $Id(J(\Lambda_\mathfrak{p})) = \Lambda_\mathfrak{p}$ genau dann, wenn $J(\Lambda_\mathfrak{p})$ in $\Lambda_\mathfrak{p}$ invertierbar ist.*

Dies ist die zentrale Aussage in [Zas72]. In Verbindung mit Theorem 3.11 sieht man dann noch einmal, daß die maximale $R_\mathfrak{p}$-Ordnung $\Lambda_\mathfrak{p}^{(\max)}$ hereditär ist. Da sämtliche Primideale von $\Lambda_\mathfrak{p}^{(\max)}$ invertierbar sind, ist das Jacobson-Radikal J invertierbar, vgl. Korollar 2.51.

4.3 Berechnung von hereditären Ordnungen

Analog zur $\mathfrak{p}$-Maximalität wird jetzt der Begriff $\mathfrak{p}$-hereditär eingeführt. Eine R-Ordnung $\Lambda^{(\mathfrak{p}\text{-her})}$ heißt $\mathfrak{p}$-*hereditär*, wenn ihre $\mathfrak{p}$-Lokalisierung $\Lambda_\mathfrak{p}$ hereditär ist. Wie man Proposition 4.4 entnimmt, ist dies äquivalent dazu, daß die Vervollständigung $\hat{\Lambda}_\mathfrak{p}$ hereditär ist.

(4.10) **Proposition** *Die R-Ordnung Λ ist genau dann $\mathfrak{p}$-hereditär, wenn das $\mathfrak{p}$-Radikal $\sqrt{\mathfrak{p}\Lambda}$ in Λ invertierbar ist.*

Beweis: Ist $\sqrt{\mathfrak{p}\Lambda}$ invertierbar, so existiert $\mathfrak{b}$ mit $\mathfrak{b}\sqrt{\mathfrak{p}\Lambda} = \Lambda$ und $\sqrt{\mathfrak{p}\Lambda}\mathfrak{b} = \Lambda$. Für das Jacobson-Radikal J von $\Lambda_\mathfrak{p}$ gilt nach Proposition 3.28 $J = \left(\sqrt{\mathfrak{p}\Lambda}\right)_\mathfrak{p} = R_\mathfrak{p}\sqrt{\mathfrak{p}\Lambda}$, also $J\,\mathfrak{b}_\mathfrak{p} = R_\mathfrak{p}\sqrt{\mathfrak{p}\Lambda}R_\mathfrak{p}\mathfrak{b} = R_\mathfrak{p}R_\mathfrak{p}\sqrt{\mathfrak{p}\Lambda}\mathfrak{b} = R_\mathfrak{p}\Lambda = \Lambda_\mathfrak{p}$. Ebenso gilt $\mathfrak{b}_\mathfrak{p}\,J = \Lambda_\mathfrak{p}$. Mit Theorem 4.9 und Proposition 4.7 erhält man, daß Λ $\mathfrak{p}$-hereditär ist.

Ist auf der anderen Seite Λ $\mathfrak{p}$-hereditär, also J invertierbar in $\Lambda_\mathfrak{p}$, so setzt man $\mathfrak{a}_\mathfrak{p} := J^{-1}$ und $\mathfrak{a}_\mathfrak{q} := \Lambda_\mathfrak{q}$ für $\mathfrak{q} \neq \mathfrak{p}$. Dann ist $\mathfrak{a} := \bigcap_\mathfrak{q} \mathfrak{a}_\mathfrak{q}$ nach [Rei75, Thm. 4.22] ein zweiseitiges Ideal in Λ. Wegen $\mathfrak{p} \subseteq \sqrt{\mathfrak{p}\Lambda}$ ist $(\sqrt{\mathfrak{p}\Lambda})_\mathfrak{q} = \Lambda_\mathfrak{q}$, also $((\sqrt{\mathfrak{p}\Lambda})_\mathfrak{q})^{-1} = \Lambda_\mathfrak{q}$ für $\mathfrak{q} \neq \mathfrak{p}$. Für jedes $\mathfrak{q}$ gilt demnach $(\sqrt{\mathfrak{p}\Lambda})_\mathfrak{q}\mathfrak{a}_\mathfrak{q} = \Lambda_\mathfrak{q}$. Daraus folgt $\sqrt{\mathfrak{p}\Lambda}\mathfrak{a} = \bigcap_\mathfrak{q}(\sqrt{\mathfrak{p}\Lambda}\mathfrak{a})_\mathfrak{q} = \bigcap_\mathfrak{q}(\sqrt{\mathfrak{p}\Lambda})_\mathfrak{q}\mathfrak{a}_\mathfrak{q} = \bigcap_\mathfrak{q}\Lambda_\mathfrak{q} = \Lambda$, vgl. [Rei75, Thm. 4.21]. □

(4.11) **Korollar** *Für die R-Ordnung Λ sind die folgenden Aussagen äquivalent:*

(1) Λ *ist $\mathfrak{p}$-hereditär,*

(2) $\mathcal{O}_l(\sqrt{\mathfrak{p}\Lambda}) = \Lambda$,

(3) $\mathcal{O}_r(\sqrt{\mathfrak{p}\Lambda}) = \Lambda$,

(4) $Id(\sqrt{\mathfrak{p}\Lambda}) = \Lambda$.

Beweis: Es genügt hier, die erste Äquivalenz zu zeigen, die anderen folgen analog. Ist Λ $\mathfrak{p}$-hereditär, so erhält man mit Proposition 4.10 und Proposition 2.39 $\mathcal{O}_l(\sqrt{\mathfrak{p}\Lambda}) = \Lambda$. Für die andere Richtung genügt es wegen Proposition 4.8 und Proposition 4.7 $\mathcal{O}_l(J) \subseteq \Lambda_\mathfrak{p}$ zu zeigen, wobei $J = R_\mathfrak{p}\sqrt{\mathfrak{p}\Lambda}$ das Jacobson-Radikal von $\Lambda_\mathfrak{p}$ ist.

Es sei $x \in \mathcal{O}_l(J)$, dann gilt $x\sqrt{\mathfrak{p}\Lambda} \subseteq R_\mathfrak{p}\sqrt{\mathfrak{p}\Lambda}$. Da $x\sqrt{\mathfrak{p}\Lambda}$ über R endlich erzeugt ist, existiert ein $s \in R \setminus \mathfrak{p}$ mit $x\sqrt{\mathfrak{p}\Lambda} \subseteq \frac{1}{s}\sqrt{\mathfrak{p}\Lambda}$ und daher $sx \in \mathcal{O}_l(\sqrt{\mathfrak{p}\Lambda})$. Man folgert $x = \frac{1}{s}sx \in R_\mathfrak{p}\Lambda = \Lambda_\mathfrak{p}$. □

(4.12) **Algorithmus $\mathfrak{p}$-hereditäre Ordnung**
Input: *Eine Ordnung Λ und ein maximales Ideal $\mathfrak{p}$ von R.*
Output: *Eine $\mathfrak{p}$-hereditäre Ordnung $\Lambda^{(\mathfrak{p}\text{-}her)} \supseteq \Lambda$.*

(1) *Initialisiere $\Lambda^{(\mathfrak{p}\text{-}her)} := \Lambda$.*
(2) *Berechne das $\mathfrak{p}$-Radikal $\sqrt{\mathfrak{p}\Lambda^{(\mathfrak{p}\text{-}her)}}$ von $\Lambda^{(\mathfrak{p}\text{-}her)}$.*
(3) *Gilt $\Lambda^{(\mathfrak{p}\text{-}her)} \subset \mathcal{O}_l\left(\sqrt{\mathfrak{p}\Lambda^{(\mathfrak{p}\text{-}her)}}\right)$, dann ersetze $\Lambda^{(\mathfrak{p}\text{-}her)} := \mathcal{O}_l\left(\sqrt{\mathfrak{p}\Lambda^{(\mathfrak{p}\text{-}her)}}\right)$ und gehe zu Schritt (2).*
(4) *Gilt $\Lambda^{(\mathfrak{p}\text{-}her)} = \mathcal{O}_l\left(\sqrt{\mathfrak{p}\Lambda^{(\mathfrak{p}\text{-}her)}}\right)$, dann terminiere.*

Ein Verfahren zur Berechnung des $\mathfrak{p}$-Radikals liefert Algorithmus 5.1 in Abschnitt 5.1.

(4.13) **Proposition** *Es sei* $\mathrm{disc}(\Lambda) = \mathfrak{p}^{2\mu}\mathfrak{q}$ *mit* $\mathfrak{q} \not\subseteq \mathfrak{p}^2$. *Die Komplexität von Algorithmus 4.12 beträgt $O(\mu(n^4+g(n)))$, wobei $g(n)$ die Komplexität für die Berechnung des $\mathfrak{p}$-Radikals ist.*

Beweis: Ist $\Lambda^{(\mathfrak{p}\text{-her})}$ in Schritt (3) nicht $\mathfrak{p}$-hereditär, dann liefert $\mathcal{O}_l\left(\sqrt{\mathfrak{p}\Lambda^{(\mathfrak{p}\text{-her})}}\right)$ eine deckende Ordnung. Für $x \in \mathcal{O}_l\left(\sqrt{\mathfrak{p}\Lambda^{(\mathfrak{p}\text{-her})}}\right)$ gilt $\mathfrak{p}x = x\mathfrak{p} \subseteq x\sqrt{\mathfrak{p}\Lambda^{(\mathfrak{p}\text{-her})}} \subseteq \sqrt{\mathfrak{p}\Lambda^{(\mathfrak{p}\text{-her})}} \subseteq \Lambda^{(\mathfrak{p}\text{-her})}$. So erhält man aus $\mathfrak{p}\mathcal{O}_l\left(\sqrt{\mathfrak{p}\Lambda^{(\mathfrak{p}\text{-her})}}\right) \subseteq \Lambda^{(\mathfrak{p}\text{-her})}$ den Index $\left(\mathcal{O}_l\left(\sqrt{\mathfrak{p}\Lambda^{(\mathfrak{p}\text{-her})}}\right) : \Lambda^{(\mathfrak{p}\text{-her})}\right) \mid \mathfrak{p}^n$.

Nach maximal μ solchen Aufstiegen ist man an einer $\mathfrak{p}$-hereditären Ordnung angelangt, vgl. Proposition 3.17. In jedem dieser (maximal) μ Schritte muß das $\mathfrak{p}$-Radikal konstruiert werden ($g(n)$) und anschließend die Links-Ordnung berechnen werden ($O(n^4)$).

Für den Test $\Lambda^{(\mathfrak{p}\text{-her})} = \mathcal{O}_l\left(\sqrt{\mathfrak{p}\Lambda^{(\mathfrak{p}\text{-her})}}\right)$ siehe auch Proposition 3.17. □

Wie bei der Berechnung einer Maximalordnung bieten sich auch bei der Berechnung einer hereditären Ordnung die Möglichkeiten iterativ oder parallel zu verfahren an, vgl. Algorithmus 3.18 und Algorithmus 3.20. Hier wird nun nur der parallele Algorithmus aufgeführt.

(4.14) **Proposition** *Für die maximalen Ideale $\mathfrak{p}, \mathfrak{q}$ von R seien die Ordnungen $\Lambda^{(\mathfrak{p}\text{-}her)}, \Lambda^{(\mathfrak{q}\text{-}her)} \supseteq \Lambda$ $\mathfrak{p}$-hereditär bzw. $\mathfrak{q}$-hereditär. Dann ist die Ordnung $\Lambda' := \Lambda^{(\mathfrak{p}\text{-}her)} + \Lambda^{(\mathfrak{q}\text{-}her)}$ sowohl $\mathfrak{p}$-hereditär als auch $\mathfrak{q}$-hereditär.*

Beweis: Analog zu Proposition 3.19 wird gezeigt, daß Λ' eine Ordnung ist. Wegen $\Lambda_{\mathfrak{p}}^{(\mathfrak{p}\text{-her})} \subseteq \Lambda'_{\mathfrak{p}}$ ist mit $\Lambda_{\mathfrak{p}}^{(\mathfrak{p}\text{-her})}$ auch die $R_{\mathfrak{p}}$-Ordnung $\Lambda'_{\mathfrak{p}}$ hereditär, vgl. [Rei75, Thm. 40.4]. Damit ist aber Λ' $\mathfrak{p}$-hereditär. □

(4.15) **Korollar** *Die Ordnung Λ ist genau dann hereditär, wenn Λ für jedes maximale Ideal $\mathfrak{p}$ von R, das die Diskriminante* $\operatorname{disc}(\Lambda)$ *mindestens quadratisch teilt, $\mathfrak{p}$-hereditär ist.*

Beweis: Teilt das maximale Ideale $\mathfrak{p}$ von R die Diskriminante nicht quadratisch, so ist Λ $\mathfrak{p}$-maximal und damit die $R_{\mathfrak{p}}$-Ordnung $\Lambda_{\mathfrak{p}}$ maximal, also auch hereditär [Rei75, Thm. 21.4]. Nach Proposition 4.2 ist Λ folglich hereditär. □

(4.16) **Algorithmus hereditäre Ordnung (parallel)**
Input: *Eine Ordnung Λ.*
Output: *Eine hereditäre Ordnung $\Lambda^{(her)} \supseteq \Lambda$.*
(1) *Faktorisiere die Diskriminante* $\operatorname{disc}(\Lambda) = \prod_{j=1}^{r} \mathfrak{p}_j^{e_j}$.
(2) *Für $(1 \leq j \leq r, e_j > 1)$ wiederhole*
(3) *Algorithmus 4.12 liefert eine $\mathfrak{p}_j$-hereditäre Ordnung $\Lambda_j \supseteq \Lambda$.*
(4) *Setze $\Lambda^{(her)} := \sum_{j=1}^{r} \Lambda_j$.*

Auch hier müssen nach Korollar 4.15 nur die quadratischen Diskriminantenteiler $\mathfrak{p}_j$ überprüft werden. Eine Aussage über die Komplexität von Algorithmus 4.16 zu machen, ist ebenso schwierig wie für Algorithmus 3.18 oder Algorithmus 3.20, vgl. Bemerkung 3.21. In Verbindung mit Algorithmus 3.16 ergibt sich

(4.17) **Algorithmus $\mathfrak{p}$-maximale Ordnung (Round 2)**
Input: *Eine Ordnung Λ und ein maximales Ideal $\mathfrak{p}$ von R.*
Output: *Eine $\mathfrak{p}$-maximale Ordnung $\Lambda^{(\mathfrak{p})} \supseteq \Lambda$.*
(1) *Berechne mit Algorithmus 4.12 $\Lambda^{(\mathfrak{p}\text{-}her)} \supseteq \Lambda$ eine $\mathfrak{p}$-hereditäre Ordnung.*
(2) *Berechne mit Algorithmus 3.16 $\Lambda^{(\mathfrak{p})} \supseteq \Lambda^{(\mathfrak{p}\text{-}her)}$ eine $\mathfrak{p}$-maximale Ordnung.*

(4.18) **Bemerkung** *Obwohl sich die Komplexitätsanalyse von Algorithmus 4.17 im Vergleich zu Proposition 3.17 im allgemeinen nicht verbessern läßt, wird der Algorithmus in der Praxis überlegen sein, da für jeden Aufstieg, den*

man bis zur $\mathfrak{p}$-hereditären Ordnung macht, die Komplexität nur $O(n^4+g(n))$ an Stelle von $O(n^5+f(n))$ beträgt, $g(n)$ sei die Komplexität für die Berechnung des $\mathfrak{p}$-Radikals, $f(n)$ die Komplexität zur Konstruktion der maximalen Ideale, die $\mathfrak{p}$ enthalten, vgl. Proposition 3.17 und Proposition 4.13.

(4.19) **Bemerkung** *Ebenso wie die Lokalisierung in Abschnitt 3.6 zur Berechnung von $\mathfrak{p}$-maximalen Ordnungen ausgenutzt wurde, kann die Lokalisierung ganz analog zur Berechnung von $\mathfrak{p}$-hereditären Ordnungen eingesetzt werden.*

4.4 Kommutative Ordnungen

In der Darstellung von A durch einfache Bestandteile $A = \bigoplus_{i=1}^{v} A_i$ und des Zentrums $\mathrm{Z}(A) = \bigoplus_{i=1}^{v} K_i$, wie in Abschnitt 1.1, seien $R_i = \mathrm{Cl}(R, K_i)$ $(1 \leq i \leq v)$ die ganzen Abschlüsse von R in den Zentren der einfachen Bestandteile.

(4.20) **Proposition** [Rei75, Thm. 40.7(iii)] *Eine R-Ordnung Λ_i in A_i ist genau dann eine hereditäre R-Ordnung, wenn sie schon eine hereditäre R_i-Ordnung ist.*

In Verbindung mit Proposition 4.1 sieht man, daß jede hereditäre R-Ordnung Λ den ganzen Abschluß von R in $\mathrm{Z}(A)$ enthält.

(4.21) **Korollar** *In kommutativen separablen Algebren A sind die hereditären Ordnungen bereits maximal. Insbesondere gibt es eine eindeutig bestimmte hereditäre bzw. maximale Ordnung.*

Im Kommutativen erhält man den Aufstieg zur maximalen oder $\mathfrak{p}$-maximalen Ordnung alleine durch Berechnung der Links-Ordnung des $\mathfrak{p}$-Radikals ($\mathcal{O}_l(\sqrt{\mathfrak{p}\Lambda}) = \mathcal{O}_r(\sqrt{\mathfrak{p}\Lambda})$). Die Berechnung der Primideale, die $\mathfrak{p}$ enthalten kann man sich hier sparen. Algorithmus 4.12 liefert damit im Falle einer kommutativen Algebra A die eindeutig bestimmte $\mathfrak{p}$-maximale Oberordnung und Algorithmus 4.16 die eindeutig bestimmte Maximalordnung.

Algorithmus 4.16 ist dann der aus der Theorie der globalen Körper bekannte *Round 2 Algorithmus* zur Berechnung der Maximalordnung in globalen Körpern, z.B. [PZ89, Chpt. 4, Lem. 5.53], [Fri97, Alg. III.14]. Allerdings ist das Verfahren hier in einem sehr viel allgemeineren Rahmen (kommutative separable Algebren über Quotientenkörpern von Dedekindringen) beschrieben.

Kapitel 5
Berechnung des $\mathfrak{p}$-Radikals und der Primideale

Es sei Λ eine R-Ordnung in A und $\mathfrak{p}$ ein maximales Ideal von R. Ziel dieses Abschnitts ist es, Verfahren zur Berechnung des $\mathfrak{p}$-Radikals $\sqrt{\mathfrak{p}\Lambda}$ und der Primideale von Λ, die $\mathfrak{p}$ enthalten, sowie Anwendungen davon anzugeben.

Weiterhin seien $\bar{\Lambda} := \Lambda/\mathfrak{p}\Lambda$ die artinsche Algebra über dem Körper $\bar{R} := R/\mathfrak{p}$ und $\varphi : \Lambda \to \bar{\Lambda}$ der kanonische Homomorphismus.

5.1 Das $\mathfrak{p}$-Radikal

Die Berechnung des $\mathfrak{p}$-Radikals wird auf die Berechnung des Jacobson-Radikals J der artinschen Algebra $\bar{\Lambda}$ über dem Körper $\bar{R}$ zurückgeführt.

(5.1) **Algorithmus $\mathfrak{p}$-Radikal**
Input: *Eine Ordnung Λ und ein maximales Ideal $\mathfrak{p}$ von R.*
Output: *Das $\mathfrak{p}$-Radikal $\sqrt{\mathfrak{p}\Lambda}$ von Λ.*
(1) *Berechne das Jacobson-Radikal $J = \bigoplus_{i=1}^{m} \bar{R}\eta_i$ von $\bar{\Lambda}$.*
(2) *Hermite-Normal-Form:* $\sqrt{\mathfrak{p}\Lambda} = \mathrm{HNF}\,(\sum_{i=1}^{m} R\varphi^{-1}(\eta_i) + \mathfrak{p}\Lambda)$.

(5.2) **Proposition** *Algorithmus 5.1 berechnet aus einer $\bar{R}$-Basis von J eine Pseudo-Basis von $\sqrt{\mathfrak{p}\Lambda}$ in $O(n^3)$ Elementaroperationen in F.*

Beweis: Das R-Gitter $\sum_{i=1}^{m} R\varphi^{-1}(\eta_i) + \mathfrak{p}\Lambda$ entspricht gerade $\varphi^{-1}(J)$, die Hermite-Normal-Form wird auf $m + n$ Erzeuger in einem Vektorraum der Dimension n angewendet, wobei $m \leq n$. □

Die Verfahren zur Berechnung des Jacobson-Radikals von $\bar{\Lambda}$ hängen wesentlich von dem Körper $\bar{R}$ ab.

5.1.1 Spur-Radikal

Die Charakteristik von $\bar{R}$ sei Null oder größer als die Dimension n der F-Algebra A (und damit auch der $\bar{R}$-Algebra $\bar{\Lambda}$). Das Verfahren, das in diesem Fall angewandt wird, geht auf Dickson [Dic60, §§64, 65] zurück und ist für Zahlkörper A in [Fri97, Alg. VI.8] oder im Fall von Charakteristik Null in

[Ebe89, Sect. 2.3.1, S. 61] beschrieben. Hier wird das Verfahren für beide Fälle zusammengefaßt und allgemein bewiesen.

Ein Element $a \in \bar{\Lambda}$ heißt *stark-nilpotent*, wenn für jedes $x \in \bar{\Lambda}$ auch xa nilpotent ist. Wegen $(ax)^{k+1} = a(xa)^k x = 0$ ist xa genau dann nilpotent, wenn ax nilpotent ist.

(5.3) **Proposition** *Das Jacobson-Radikal J von $\bar{\Lambda}$ besteht genau aus den stark-nilpotenten Elementen von $\bar{\Lambda}$.*

Beweis: Da $\bar{\Lambda}$ artinsch ist, ist J nilpotent [Lor90, §28, Satz 4]. Daher ist für $a \in J, x \in \bar{\Lambda}$ auch $xa \in J$ und damit xa nilpotent. Ist auf der anderen Seite $a \in \bar{\Lambda}$ stark-nilpotent, dann ist $\bar{\Lambda}a$ ein Links-Ideal von $\bar{\Lambda}$, das nur aus nilpotenten Elementen besteht, und in J enthalten ist [Lor90, §28, F 37]. □

(5.4) **Proposition** [Dic60, §64, Cor.] *Ein Element $a \in \bar{\Lambda}$ ist genau dann nilpotent, wenn sämtliche Nullstellen (in einem Zerfällungskörper von $\bar{R}$) des charakteristischen Polynoms von a Null sind.*

Die folgende Aussage ist eine Verallgemeinerung von [Dic60, §65, Thm.]. Ursprünglich war die Aussage nur für Charakteristik 0 formuliert.

(5.5) **Proposition** *Ein Element $a \in \bar{\Lambda}$ ist genau dann stark-nilpotent, wenn für jedes $x \in \bar{\Lambda}$ die Spur $\mathrm{T}_{\bar{\Lambda}/\bar{R}}(xa) = 0$ ist.*

Beweis: Ist $a \in \bar{\Lambda}$ stark-nilpotent, so ist xa nilpotent für jedes $x \in \bar{\Lambda}$. Aus Proposition 5.4 folgt, daß sämtliche Nullstellen von $\mathrm{P}(xa) \in \bar{R}[t]$ Null sind, daher ist auch $\mathrm{T}(xa) = 0$.

Sei $a \in \bar{\Lambda}$ ein Element mit $\mathrm{T}(xa) = 0$ für alle $x \in \bar{\Lambda}$. Für beliebiges $i > 0$ gilt $(xa)^i = x(ax)^{i-1}a$, also $\mathrm{T}((xa)^i) = 0$. $\mathrm{P}(xa) = \prod_{i=1}^{n}(t - \xi_i)$ sei die Faktorisierung des charakteristischen Polynoms in einem entsprechenden Zerfällungskörper von $\bar{R}$.

Mit den *elementar symmetrischen Funktionen* $\sigma_i := \sigma_i(\xi_1, \ldots, \xi_n) := \sum_{1 \le j_1 < \ldots < j_i \le n} \xi_{j_1} \cdot \xi_{j_2} \cdot \ldots \cdot \xi_{j_i}$ $(1 \le i \le n)$ erhält man $\mathrm{P}(xa) = t^n - \sigma_1 t^{n-1} + \sigma_2 t^{n-2} + \cdots + (-1)^n \sigma_n$, vgl. [PZ89, Chpt. 2.3]. Die *Newton-Relationen* [PZ89, Chpt. 2, Thm. 3.12] liefern die elementar symmetrischen Funktionen $\sigma_1, \ldots, \sigma_n$ als Linearkombination der *k-ten Potenzsummen* $S_k := \sum_{i=1}^{n} \xi_i^k$ $(k \ge 0)$, wenn die Elemente $1, \ldots, n \in \bar{R}$ invertierbar sind. Da die Charakteristik von $\bar{R}$ Null oder größer als n ist, ist dies aber der Fall.

Da $S_k = \mathrm{T}((xa)^k) = 0$ $(1 \le k \le n)$, folgert man $\sigma_i = 0$ $(1 \le i \le n)$ und damit $\mathrm{P}(xa) = t^n$. Nach Proposition 5.4 ist xa nilpotent. □

Ist $\omega_1, \ldots, \omega_n$ eine $\bar{R}$-Basis von $\bar{\Lambda}$, so ist $\mathrm{T}(xa) = 0$ genau dann, wenn $\mathrm{T}(\omega_i a) = 0$ $(1 \le i \le n)$. Die $\bar{R}$-lineare Abbildung $\psi : \bar{\Lambda} \to (\bar{R})^n : a \mapsto (\mathrm{T}(\omega_i a))_{(1 \le i \le n)}$ wird (bzgl. der Basis $\omega_1, \ldots, \omega_n$) durch die Matrix $M := (\mathrm{T}(\omega_i \omega_j))_{(1 \le i,j \le n)}$ beschrieben.

(5.6) **Korollar** *Das Jacobson-Radikal J von $\bar{\Lambda}$ entspricht der Menge $\{a \in \bar{\Lambda} | \, \mathrm{T}(xa) = 0$ für alle $x \in \bar{\Lambda}\}$ und damit dem Kern der Abbildung ψ.*

Eine $\bar{R}$-Basis von J erhält man, wenn man den Kern der Matrix M berechnet.

(5.7) **Proposition** *Die Komplexität zur Berechnung des Jacobson-Radikals über den Kern der linearen Abbildung ψ beträgt $O(n^4)$ gemessen in Elementaroperationen des Grundkörpers F.*

Beweis: Zur Vereinfachung kann man davon ausgehen, daß die Operationen in dem Restklassenkörper $\bar{R}$ durch entsprechende Operationen in F beschränkt sind. In der Tat ist die Arithmetik in $\bar{R}$ auch häufig durch Arithmetik in F (über kanonische Repräsentanten und anschließendes Reduzieren) implementiert.

Der wesentliche Teil ist die Berechnung der Matrix $M := (\mathrm{T}(\omega_i\omega_j))_{(1\le i,j\le n)}$, die die Abbildung ψ darstellt. Es seien $\eta_1, \ldots, \eta_n$ kanonische Repräsentanten von $\omega_1, \ldots, \omega_n$. In der Regel wird $\eta_1, \ldots, \eta_n$ gerade die zugrundeliegende F-Basis von A sein, so daß man die Links-Darstellungsmatrizen von $\eta_1, \ldots, \eta_n$ nicht berechnen muß ($R_l(\eta_i) = M(i)$, die Multiplikationstabelle, vgl. Abschnitt 2.1). Sonst kann man alle n Links-Darstellungsmatrizen in $O(n^4)$ Elementaroperationen berechnen (Proposition 2.3).

Die Spur von $\omega_i\omega_j$ erhält man aus der Spur von $\eta_i\eta_j$, diese wiederum über die Links-Darstellungsmatrix $R_l(\eta_i\eta_j) = R_l(\eta_j)R_l(\eta_i)$. Da man nur die Einträge auf der Hauptdiagonalen benötigt, muß man keine vollständige Multiplikation durchführen. Die Einträge auf der Hauptdiagonalen von $R_l(\eta_i\eta_j)$ bekommt man in $O(n^2)$ Elementaroperationen. Die Spur von $\eta_i\eta_j$ zu berechnen kostet dann noch einmal $O(n)$ Elementaroperationen. Zusammen benötigt man zur Berechnung aller Spuren folglich $O(n^4)$ Elementaroperationen.

Da die Spur eine symmetrische Bilinearform erzeugt, muß man nicht alle Einträge gesondert berechnen, sondern kann die Symmetrie von M ausnutzen. Dies ändert allerdings nichts an der Komplexität. Für die Berechnung des Kerns von M sind dann noch einmal $O(n^3)$ Elementaroperationen erforderlich. □

Die Menge $I_{\mathfrak{p},\Lambda}^{(\mathrm{Spur})} := \{a \in \Lambda | \, \mathrm{T}(xa) \in \mathfrak{p}$ für alle $x \in \Lambda\}$ heißt $\mathfrak{p}$-*Spur-Radikal*.

(5.8) **Korollar** *Ist die Charakteristik von $\bar{R}$ Null oder größer als n, so gilt $\sqrt{\mathfrak{p}\Lambda} = I_{\mathfrak{p},\Lambda}^{(Spur)}$.*

Direkt aus dem Beweis zu Proposition 5.5 liest man die folgende Aussage ab.

(5.9) **Korollar** *Ist die positive Charakteristik von $\bar{R}$ nicht größer als n, so gilt trotzdem $J \subseteq \{a \in \bar{\Lambda} | \, \mathrm{T}(xa) = 0$ für alle $x \in \bar{\Lambda}\}$ und entsprechend $\sqrt{\mathfrak{p}\Lambda} \subseteq I_{\mathfrak{p},\Lambda}^{(Spur)}$.*

(5.10) **Korollar** *Das $\mathfrak{p}$-Spur-Radikal $I_{\mathfrak{p},\Lambda}^{(Spur)}$ kann mit Algorithmus 5.1 in $O(n^4)$ Elementaroperationen konstruiert werden.*

Ein weiteres Verfahren zur Berechnung des $\mathfrak{p}$-Spur-Radikals liefert Algorithmus 6.16.

5.1.2 Frobenius-Homomorphismus

In Proposition 3.9 wurde gezeigt, daß ein $\nu > 0$ existiert mit $\sqrt{\mathfrak{p}\Lambda}^{\nu} \subseteq \mathfrak{p}\Lambda$. Diese Aussage soll im folgenden präzisiert werden, siehe auch [Fri97, Lemma III.6(4)] oder [Coh96a, Lem. 6.1.6].

(5.11) **Proposition** *Für das $\mathfrak{p}$-Radikal von Λ gilt $\sqrt{\mathfrak{p}\Lambda}^{n} \subseteq \mathfrak{p}\Lambda$.*

Beweis: Man definiert die Ideale $\mathfrak{a}_i := \sqrt{\mathfrak{p}\Lambda}^{i} + \mathfrak{p}\Lambda$ $(i > 0)$. Es gilt $\Lambda \supset \mathfrak{a}_1 \supseteq \cdots \supseteq \mathfrak{a}_n \supseteq \cdots \supseteq \mathfrak{a}_\nu \supseteq \cdots \supseteq \mathfrak{p}\Lambda$. Wegen $(\Lambda : \mathfrak{p}\Lambda) = \mathfrak{p}^n$ kann $\Lambda \supset \mathfrak{a}_1 \supset \mathfrak{a}_2 \supset \cdots \supset \mathfrak{a}_n \supset \mathfrak{a}_{n+1}$ nicht gelten. Es existiert ein $1 \leq k \leq n$ mit $\mathfrak{a}_k = \mathfrak{a}_{k+1}$.

Per Induktion über $j \geq k$ erhält man $\mathfrak{a}_j = \mathfrak{a}_{j+1}$: Sei $j \geq k$. $\mathfrak{a}_{j+1} = \sqrt{\mathfrak{p}\Lambda}^{j+1} + \mathfrak{p}\Lambda \subseteq \left(\sqrt{\mathfrak{p}\Lambda}^{j+1} + \mathfrak{p}\Lambda\right)\sqrt{\mathfrak{p}\Lambda} + \mathfrak{p}\Lambda \subseteq \sqrt{\mathfrak{p}\Lambda}^{j+2} + \mathfrak{p}\Lambda + \mathfrak{p}\Lambda = \mathfrak{a}_{j+2}$. Man erhält $\sqrt{\mathfrak{p}\Lambda}^{n} \subseteq \mathfrak{a}_n = \mathfrak{a}_\nu = \sqrt{\mathfrak{p}\Lambda}^{\nu} + \mathfrak{p}\Lambda \subseteq \mathfrak{p}\Lambda$. □

(5.12) **Korollar** *Für das Jacobson-Radikal von $\bar{\Lambda}$ gilt $J^n = \{0\}$.*

Ist $\bar{R} = \mathbb{F}_q$, mit $q = p^r$, ein endlicher Körper und $\bar{\Lambda}$ kommutativ, so kann der Frobenius-Homomorphismus angewendet werden. Dazu sei $\omega_1, \ldots, \omega_n$ eine $\bar{R}$-Basis von $\bar{\Lambda}$. $\kappa > 0$ sei so gewählt, daß $q^{\kappa-1} < n \leq q^\kappa$. Die Abbildung $\psi : \bar{\Lambda} \to \bar{\Lambda} : x \mapsto x^{q^\kappa}$ ist $\bar{R}$-linear: $\psi(\alpha x) = \alpha^{q^\kappa} x^{q^\kappa} = \alpha x^{q^\kappa} = \alpha\psi(x)$ für $\alpha \in \bar{R}, x \in \bar{\Lambda}$. Da $p | \binom{q^\kappa}{i}$ für $1 \leq i < q^\kappa$, gilt $\psi(x+y) = (x+y)^{q^\kappa} = \sum_{i=0}^{q^\kappa} \binom{q^\kappa}{i} x^i y^{q^\kappa - i} = x^{q^\kappa} + y^{q^\kappa} = \psi(x) + \psi(y)$ für $x, y \in \bar{\Lambda}$. Man beachte, daß die Binomische Formel nur im kommutativen Fall angewendet werden kann.

(5.13) **Korollar** *Das Jacobson-Radikal entspricht dem Kern der Abbildung ψ.*

Die Elemente $\alpha_{i,j} \in \bar{R}$ seien durch $\omega_i^{q^\kappa} = \sum_{j=1}^n \alpha_{j,i}\omega_j$ bestimmt, dann wird die Abbildung ψ (bzgl. der Basis $\omega_1, \ldots, \omega_n$) durch die Matrix $M := (\alpha_{i,j})_{(1\le i,j\le n)}$ beschrieben. Eine $\bar{R}$-Basis von J erhält man durch Berechnung des Kerns von M.

(5.14) **Proposition** *Das Jacobson-Radikal kann in $O(\max(n^2, q)n^3)$ Elementaroperationen über den Kern der Abbildung ψ berechnet werden. Damit beträgt die Komplexität zur Berechnung des $\mathfrak{p}$-Radikals mit Algorithmus 5.1 $O(\max(n^2, q)n^3)$.*

Beweis: Ähnlich wie in Proposition 5.7 seien auch hier wieder $\eta_1, \ldots, \eta_n$ kanonische Repräsentanten von $\omega_1, \ldots, \omega_n$. Für die Matrix M muß man die Potenzen $\omega_1^{q^\kappa}, \ldots, \omega_n^{q^\kappa}$ bzw. $\eta_1^{q^\kappa}, \ldots, \eta_n^{q^\kappa}$ berechnen. Man überlegt sich, daß q^κ in jedem Fall durch $\tau := \max(n^2, q)$ beschränkt ist.

Nachdem man die Links-Darstellungsmatrix von η_i berechnet hat ($O(n^3)$, Proposition 2.3; unter Umständen ist auch $R_l(\eta_i) = M(i)$ die Multiplikationstabelle, vgl. Proposition 5.7), kann man die maximal $\tau - 1$ Multiplikationen mit η_i in jeweils $O(n^2)$ Operationen durchführen, vgl. Bemerkung 2.7. Zusammen kommt man daher auf $O(\tau n^2)$ Operationen, um $\eta_i^{q^\kappa}$ zu berechnen. Die Matrix M ist demnach nach $O(\tau n^3)$ Operationen konstruiert. Die Berechnung des Kerns von M kostet wiederum $O(n^3)$ Operationen. □

Ist $\bar{\Lambda}$ nicht kommutativ, so wird in [Ebe89, Sect. 2.3.2, Thm. 2.3.17 und S. 71] ein Verfahren zur Berechnung des Radikals angegeben, das wegen seiner Komplexität hier nicht wiederholt wird.

5.1.3 Der fehlende Fall

Für den Fall, daß $\bar{R}$ positive Charakteristik hat, die kleiner oder gleich n ist, und $\bar{R}$ kein endlicher Körper ist, ist derzeit kein Verfahren bekannt, das im allgemeinen das Jacobson-Radikal von $\bar{\Lambda}$ berechnet.

Ein Beispiel hierfür ist ein globaler Funktionenkörper $\bar{R} = \mathbb{F}_q(t_1)$. Dieser Fall tritt ein, wenn man endliche Erweiterungen von Funktionenkörpern in zwei Variablen über endlichen Körpern untersucht: $F = \mathbb{F}_q(t_1, t_2), R = \mathbb{F}_q(t_1)[t_2]$ und zum Beispiel $A = F[t_3]/fF[t_3]$ mit einem separablen Polynom $f \in R[t_3]$.

Die folgenden Anmerkungen zeigen, was in diesem Fall trotzdem möglich ist.

(5.15) **Bemerkung** *Ist die Ordnung Λ_f eine* Gleichungsordnung*, also durch ein normiertes (separables) Polynom $f \in R[t]$ erzeugt, $\Lambda_f = R[t]/fR[t]$, so kann man das $\mathfrak{p}$-Radikal von Λ wie im* Dedekindtest *berechnen, vgl. [Zas75, Thm. 1] oder [PZ89, Chpt. 4, (5.55b)]:*

Es sei $f \equiv \prod_{i=1}^{k} g_i^i \mod \mathfrak{p}R[t]$ mit normierten separablen und paarweise teilerfremden $g_1, \ldots, g_k \in R[t]$. Dann gilt $\sqrt{\mathfrak{p}\Lambda_f} = \mathfrak{p}\Lambda_f + \prod_{i=1}^{k} g_i(\zeta)\Lambda_f$ mit $\zeta = t + fR[t] \in \Lambda_f$.

(5.16) **Bemerkung** *Das $\mathfrak{p}$-Radikal der Ordnung Λ erzeugt in einer erweiterten Ordnung Λ', beim Aufstieg zu einer $\mathfrak{p}$-maximalen Ordnung, ein zweiseitiges Ideal $\mathfrak{Q} := \Lambda'\sqrt{\mathfrak{p}\Lambda}\Lambda'$, das $\mathfrak{p}\Lambda'$ enthält. Deckt die R-Ordnung Λ' die R-Ordnung Λ, so ist $\mathfrak{Q}$ im $\mathfrak{p}$-Radikal von Λ' enthalten. Dies ist also insbesondere im kommutativen Fall erfüllt.*

Es besteht die berechtigte Hoffnung, daß man mit $\mathcal{O}_l(\mathfrak{Q})$ ebenfalls einen weiteren Aufstieg in Richtung $\mathfrak{p}$-maximaler bzw. $\mathfrak{p}$-hereditärer Ordnung erreicht. Im Falle $\mathcal{O}_l(\mathfrak{Q}) = \Lambda'$ hat man aber keine Garantie, daß Λ' bereits $\mathfrak{p}$-maximal bzw. $\mathfrak{p}$-hereditär ist.

(5.17) **Bemerkung** *Nach Korollar 5.9 gilt in jedem Fall $\sqrt{\mathfrak{p}\Lambda} \subseteq I_{\mathfrak{p},\Lambda}^{(Spur)}$, so daß sich wie in Bemerkung 5.16 anbietet, das Ideal $I_{\mathfrak{p},\Lambda}^{(Spur)}$ zu verwenden, um eine größere Ordnung zu konstruieren.*

Ein Beispiel für $\sqrt{\mathfrak{p}\Lambda} \neq I_{\mathfrak{p},\Lambda}^{(Spur)}$ liefert [Ebe89, Ex. 2.3.7]. Dort werden obere 2×2-Dreiecksmatrizen über $\mathbb{F}_2$ betrachtet.

(5.18) **Bemerkung** *$\mathfrak{a} \subseteq \Lambda$ sei ein zweiseitiges Ideal von Λ. Hierfür bieten sich zum Beispiel die Ideale aus Bemerkung 5.16, Bemerkung 5.17 oder auch einfach $\mathfrak{p}\Lambda$ an.*

Im kommutativen Fall liefern die Ideale der Form $[\mathfrak{a} : x] := \{y \in \Lambda | yx \in \mathfrak{a}\} = (\mathfrak{a}/x\Lambda) \cap \Lambda$ für $x \in \Lambda$ eine Reihe von Idealen, die unter Umständen die Konstruktion einer größeren Ordnung $\mathcal{O}_l([\mathfrak{a} : x])$ ermöglichen, da [AM69, Prop. 7.17] zeigt, daß alle Primideale von Λ, die $\mathfrak{a}$ enthalten unter den Idealen der Form $[\mathfrak{a} : x]$ vorkommen.

$[\mathfrak{a} : x]$ ist in $O(n^4)$ Elementaroperationen berechenbar: Zuerst bildet man den Quotienten der R-Gitter $\mathfrak{a}$ und $x\Lambda$ und anschließend schneidet man diesen Quotienten mit dem R-Gitter Λ.

(5.19) **Bemerkung** *Ähnlich ist auch die Methode, die in nicht-maximalen Ordnungen in Zahlkörpern verwendet wird, um Primideale zu bestimmen, vgl. [PZ89, Chpt. 6, Prop. 3.29]. Durch systematisches Durchprobieren kanonischer Repräsentanten x des Restsystems $\Lambda/\mathfrak{a}$ erhält man mit $\mathfrak{a} + x\Lambda$ alle maximalen Ideale von Λ, die $\mathfrak{a}$ enthalten. In der Praxis ($\Lambda/\mathfrak{a}$ ist nicht immer endlich) bietet sich zur Berechnung der Primideale allerdings Algorithmus 5.23 an.*

Mit den Idealen aus den obigen Bemerkungen kann man unter Umständen eine gegebene Ordnung in eine $\mathfrak{p}$-maximale bzw. $\mathfrak{p}$-hereditäre Ordnung einbetten. Ist die Diskriminante einer Maximalordnung vorher bekannt (z.B. in

der Klassenkörpertheorie), so kann man dann sogar die erhaltene Ordnung als $\mathfrak{p}$-maximal verifizieren.

5.2 Die Primideale

Die maximalen zweiseitigen Ideale stehen in folgenden Zusammenhang zu einfachen Faktoralgebren:

(5.20) **Proposition** *Es sei S ein beliebiger Ring und $\mathfrak{m} \subseteq S$ ein zweiseitiges Ideal. $\mathfrak{m}$ ist genau dann ein maximales zweiseitiges Ideal, wenn $S/\mathfrak{m}$ einfach ist.*

Beweis: Proposition 3.6 liefert eine Bijektion zwischen den zweiseitigen Idealen von S, die $\mathfrak{m}$ enthalten, und den zweiseitigen Idealen von $S/\mathfrak{m}$, die die Inklusion erhält. Der Ring $S \neq \{0\}$ ist genau dann einfach, wenn $\{0\}$ und S die einzigen zweiseitigen Ideale sind. □

(5.21) **Korollar** *Sei $\mathfrak{p} \subseteq \mathfrak{P} \subseteq \Lambda$ ein zweiseitiges Ideal. $\mathfrak{P}$ ist genau dann ein Primideal, wenn $\Lambda/\mathfrak{P}$ einfach ist.*

5.2.1 Berechnung einfacher Bestandteile

Für diesen Abschnitt sei $\hat{\Lambda}$ eine endlich dimensionale halbeinfache Algebra über dem Körper $\bar{R}$. Die Berechnung der einfachen Bestandteile von $\hat{\Lambda}$ ist zum Beispiel in [Ebe89, Chpt. 2.4, S. 82ff.] beschrieben. Seine Arbeit ist eine Verallgemeinerung der Arbeiten von Friedl und Ronyai [FR85]:

Die einfachen Bestandteile des Zentrums $\mathrm{Z}(\hat{\Lambda}) = \bigoplus_{i=1}^{k} B_i$ liefern die einfachen Bestandteile von $\hat{\Lambda} = \bigoplus_{i=1}^{k} \hat{\Lambda}_i$ durch $\hat{\Lambda}_i = \hat{\Lambda}B_i = \{\alpha\beta | \alpha \in \hat{\Lambda}, \beta \in B_i\}$, vgl. [Ebe89, Prop. 2.4.2(ii)].

Die einfachen Bestandteile des Zentrums von $\hat{\Lambda}$ bekommt man durch die Berechnung von zentralen Idempotenten. Ist der Körper $\bar{R}$ endlich, algebraisch abgeschlossen oder hat er Charakteristik Null, so liefert [Ebe89, Algorithmus auf S. 101] ein Verfahren zur Berechnung der einfachen Bestandteile von $\hat{\Lambda}$ [Ebe89, Thm. 2.4.16].

Das Verfahren ist probabilistisch, da ein wesentlicher Teil aus der Berechnung primitiver Elemente und der Faktorisierung entsprechender charakteristischer Polynome besteht. Auch hier fehlt, ebenso wie zur Berechnung des Radikals, ein allgemeingültiges Verfahren für den Fall eines unendlichen Körpers $\bar{R}$ positiver Charakteristik. Ein weiteres Verfahren zur Berechnung der einfachen Bestandteile einer Algebra beschreibt Parker in [Par84].

5.2.2 Berechnung der Primideale

$\mathfrak{P}_1, \ldots, \mathfrak{P}_s$ seien die Primideale von Λ, die $\mathfrak{p}$ enthalten, und $\sqrt{\mathfrak{p}\Lambda} = \bigcap_{i=1}^{s} \mathfrak{P}_i$ sei das $\mathfrak{p}$-Radikal von Λ, das mit Algorithmus 5.1 berechnet werden kann. Weiterhin sei $\hat{\Lambda} := \Lambda/\sqrt{\mathfrak{p}\Lambda}$. Es gilt $\Lambda/\sqrt{\mathfrak{p}\Lambda} \cong (\Lambda/\mathfrak{p}\Lambda) \,/\, \left(\sqrt{\mathfrak{p}\Lambda}/\mathfrak{p}\Lambda\right) = \bar{\Lambda}/\,J$. Wie im Beweis zu Proposition 3.7 folgert man, daß $\hat{\Lambda}$ eine halbeinfache artinsche $\bar{R}$-Algebra ist.

Die Zerlegung in einfache Bestandteile, die nach [Lor90, §29 Satz 1] existiert, kann mit [Ebe89, Algorithmus, S. 101] wie oben berechnet werden: $\hat{\Lambda} = \bigoplus_{i=1}^{k} \hat{\Lambda}_i$. $\hat{\Lambda}$ ist wie Λ auch endlich erzeugt und hat insbesondere eine Dimension (über $\bar{R}$) $\leq n$. Damit erhält man $k \leq n$.

Die maximalen zweiseitigen Ideale von $\hat{\Lambda}$ sind damit von der Form $\hat{\mathfrak{m}}_i = \hat{\Lambda}_1 \oplus \cdots \oplus \hat{\Lambda}_{i-1} \oplus \{0\} \oplus \hat{\Lambda}_{i+1} \oplus \cdots \oplus \hat{\Lambda}_k$ $(1 \leq i \leq k)$. Unter Verwendung des kanonischen Homomorphismus $\hat{\varphi} : \Lambda \to \Lambda/\sqrt{\mathfrak{p}\lambda}$ erhält man die Primideale von Λ, die $\mathfrak{p}$ enthalten, durch $\hat{\varphi}^{-1}(\hat{\mathfrak{m}}_i)$. Es gilt gerade $s = k \leq n$ und damit eine Verallgemeinerung der Aussage für Maximalordnungen $\Lambda^{(\max)}$, Theorem 2.29:

(5.22) **Korollar** *Die Anzahl der Primideale $\mathfrak{P}$ einer beliebigen Ordnung Λ, die $\mathfrak{p}$ enthalten, ist durch n, die Dimension der F-Algebra A, nach oben beschränkt, und damit insbesondere endlich.*

Wenn man sowohl das $\mathfrak{p}$-Radikal der Ordnung Λ als auch die einfachen Bestandteile der $\bar{R}$-Algebra $\Lambda/\sqrt{\mathfrak{p}\Lambda}$ ausrechnen kann, erhält man die Primideale von Λ, die $\mathfrak{p}$ enthalten, durch Anwendung von

(5.23) **Algorithmus Primideale über $\mathfrak{p}$**
Input: *Eine Ordnung Λ und ein maximales Ideal $\mathfrak{p}$ von R.*
Output: *Die Primideale $\mathfrak{P}_1, \ldots, \mathfrak{P}_s$ von Λ, die $\mathfrak{p}$ enthalten.*

(1) *Berechne das $\mathfrak{p}$-Radikal $\sqrt{\mathfrak{p}\Lambda}$ mit Algorithmus 5.1.*
(2) *[Ebe89, Algorithmus, S. 101] liefert die einfachen Bestandteile $\Lambda/\sqrt{\mathfrak{p}\Lambda} = \bigoplus_{i=1}^{s} \hat{\Lambda}_i$.*
(3) *$\hat{\mathfrak{m}}_i = \hat{\Lambda}_1 \oplus \cdots \oplus \hat{\Lambda}_{i-1} \oplus \{0\} \oplus \hat{\Lambda}_{i+1} \oplus \cdots \oplus \hat{\Lambda}_s$ $(1 \leq i \leq s)$, sind die maximalen zweiseitigen Ideale von $\Lambda/\sqrt{\mathfrak{p}\Lambda}$.*
(4) *Der kanonische Homomorphismus liefert $\mathfrak{P}_i = \hat{\varphi}^{-1}(\hat{\mathfrak{m}}_i)$ $(1 \leq i \leq s)$.*

Algorithmus 5.23 ist eine Verallgemeinerung des Verfahrens von Buchmann, Cohen und Lenstra, das zur Faktorisierung von Indexteilern in Maximalordnungen in algebraischen Zahlkörpern verwendet wird. $\mathfrak{p}$ ist ein *Indexteiler*, wenn $\mathfrak{p} \mid (\Lambda^{(\max)} : \Lambda_f)$, wobei $f \in \mathbb{Z}[t]$ ein normiertes irreduzibles Polynom sei, das den Zahlkörper K über $\mathbb{Q}$ erzeugt. Das Verfahren ist in [BL, Sect. 4.5], [Coh96a, Sect. 6.2.2, Alg. 6.2.9] oder [Ogn94, Alg. 6.5] für absolute

Erweiterungen und [Coh00, Sect. 2.4.3, Alg. 2.4.13] für Relativerweiterungen von algebraischen Zahlkörpern beschrieben.

Das hier beschriebene Verfahren ist allgemeiner gültig und nicht nur in Maximalordnungen anwendbar. Damit ist das Verfahren zur Berechnung einer Maximalordnung $\Lambda^{(\max)}$ mit dem *Round 1* bzw. *Round 2 Algorithmus* vollständig beschrieben.

(5.24) **Bemerkung** *Die Komplexität zur Berechnung der Primideale mit Algorithmus 5.23 hängt nicht nur von der Berechnung des $\mathfrak{p}$-Radikals ab, für das mit Korollar 5.10 und Proposition 5.14 Abschätzungen angegeben sind. Ein großer Teil geht in die Berechnung der einfachen Bestandteile der Algebra $\hat{\Lambda}$ mit Hilfe des probabilistischen Verfahrens [Ebe89, Algorithmus, S. 101]. Deshalb ist hier keine Abschätzung für die gesamte Komplexität angegeben.*

5.3 Faktorisierung in beliebigen Ordnungen

Es sei $\mathfrak{a} \subseteq \Lambda$ ein beliebiges zweiseitiges ganzes Ideal. Hier soll ein Verfahren entwickelt werden, das die von Korollar 2.51 motivierte Faktorisierung von $\mathfrak{a}$ in der Form

$$\mathfrak{a} = \mathfrak{b} \prod_{i=1}^{r} \mathfrak{P}_i^{e_i} \tag{5.25}$$

in das Produkt von invertierbaren Primidealen $\mathfrak{P}_i$ und einem zweiseitigen Ideal $\mathfrak{b}$, das in keinem maximalen zweiseitigen invertierbaren Ideal von Λ enthalten ist, berechnet. Dem Algorithmus liegt dieselbe Idee zugrunde wie dem Algorithmus zur Faktorisierung von Idealen in Maximalordnungen von Zahlkörpern [Coh00, Alg. 2.3.22].

Die *Norm* eines ganzen zweiseitigen Ideals $\mathfrak{c}$ von Λ ist $\mathrm{N}(\mathfrak{c}) := \mathrm{ord}(\Lambda/\mathfrak{c})$. Sie ist ein ganzes Ideal von R. Ist $\mathfrak{d}$ ein weiteres ganzes zweiseitiges Ideal von Λ, so folgt aus $\mathfrak{d} \subseteq \mathfrak{c} \subseteq \Lambda$ sofort $\mathrm{ord}(\Lambda/\mathfrak{d}) = \mathrm{ord}(\Lambda/\mathfrak{c}) \cdot \mathrm{ord}(\mathfrak{c}/\mathfrak{d})$ [PZ89, Chpt. 4, Lem. 5.35] oder [Rei75, Thm. 4.17]. Daraus leitet man dann $\mathrm{N}(\mathfrak{c}) | \mathrm{N}(\mathfrak{d})$ (in dem Dedekindring R) ab.

Enthält das Primideal $\mathfrak{P}$ von Λ das Primideal $\mathfrak{p}$ von R, so erhält man aus $\mathfrak{p}\Lambda \subseteq \mathfrak{P} \subseteq \Lambda$ und $\mathrm{N}(\mathfrak{p}\Lambda) = \mathrm{ord}(\Lambda/\mathfrak{p}\Lambda) = \mathfrak{p}^n$ die Norm von $\mathfrak{P}$ als $\mathrm{N}(\mathfrak{P}) = \mathfrak{p}^k$ mit $k \leq n$.

Im folgenden sei $\mathrm{N}(\mathfrak{a}) = \prod_{i=1}^{\bar{r}} \mathfrak{p}_i^{\bar{e}_i}$ die Faktorisierung der Norm in Primideale von R. Ist dann $\mathfrak{P}$ ein invertierbares Primideal, das $\mathfrak{a}$ enthält, so muß $\mathfrak{P}$ automatisch eines der Primideale $\mathfrak{p}_j$ $(1 \leq j \leq \bar{r})$ enthalten und es gilt $\mathrm{N}(\mathfrak{P}) = \mathfrak{p}_j^k$ mit $k \leq \min(n, \bar{e}_j)$.

Die invertierbaren Primideale, die $\mathfrak{a}$ enthalten, liegen demnach in der Menge der Primideale von Λ, die eines der Primideale $\mathfrak{p}_j$ $(1 \leq j \leq \bar{r})$ enthalten. Ist $\mathfrak{P}$ ein solches Primideal von Λ, dann muß es zuerst auf seine Invertierbarkeit hin überprüft werden. Dies ist nach Proposition 2.43 genau dann der Fall, wenn $\mathcal{O}_l(\mathfrak{P}) = \Lambda \subset (\Lambda/\mathfrak{P})$ gilt.

(5.26) **Algorithmus Test auf Invertierbarkeit**
Input: *Ein zweiseitiges maximales Ideal $\mathfrak{P}$ der Ordnung Λ.*
Output: *Das inverse Ideal $\mathfrak{P}^{-1}$ in Λ falls $\mathfrak{P}$ invertierbar ist, FALSE sonst.*
(1) *Berechne die Links-Ordnung $\mathcal{O}_l(\mathfrak{P})$ mit Algorithmus 2.16.*
(2) *Gilt $\mathcal{O}_l(\mathfrak{P}) \supset \Lambda$, so terminiere mit FALSE.*
(3) *Berechne mit Algorithmus 2.16 den Quotienten $(\Lambda/\mathfrak{P})$.*
(4) *Gilt $(\Lambda/\mathfrak{P}) = \Lambda$, so terminiere mit FALSE.*
(5) *$\mathfrak{P}$ ist invertierbar, $\mathfrak{P}^{-1} = (\Lambda/\mathfrak{P})$.*

$\mathfrak{P}$ taucht genau dann in der Faktorisierung (5.25) von $\mathfrak{a}$ auf, wenn $\mathfrak{P}^{-1}\mathfrak{a} \subseteq \Lambda$ gilt. Damit erhält man den folgenden

(5.27) **Algorithmus Faktorisierung von Idealen**
Input: *Ein ganzes zweiseitiges Ideal $\mathfrak{a}$ der Ordnung Λ.*
Output: *Die Faktorisierung von $\mathfrak{a}$ in der Form von (5.25).*
(1) *Faktorisiere die Norm $\mathrm{N}(\mathfrak{a}) = \prod_{i=1}^{\bar{r}} \mathfrak{p}_i^{\bar{e}_i}$.*
(2) *Initialisiere $\mathfrak{b} := \mathfrak{a}$.*
(3) *Für $(1 \leq i \leq \bar{r})$ wiederhole*
(4) *Algorithmus 5.23 liefert die Primideale $\mathfrak{P}_{i,1}, \ldots, \mathfrak{P}_{i,s_i}$ über $\mathfrak{p}_i$.*
(5) *Für $(1 \leq j \leq s_i)$ wiederhole*
(6) *Initialisiere $e_{i,j} := 0$.*
(7) *Ist $\mathfrak{P}_{i,j}$ invertierbar (Algorithmus 5.26)?*
(8) *Wenn ja, dann initialisiere $\bar{\mathfrak{b}} := \mathfrak{P}_{i,j}^{-1}\mathfrak{b}$.*
(9) *Wiederhole bis $\bar{\mathfrak{b}} \not\subseteq \Lambda$*
(10) *$\mathfrak{b} := \bar{\mathfrak{b}}, e_{i,j} := e_{i,j} + 1$ und setze $\bar{\mathfrak{b}} := \mathfrak{P}_{i,j}^{-1}\mathfrak{b}$.*
(11) $\mathfrak{a} = \mathfrak{b} \prod_{i=1}^{\bar{r}} \prod_{j=1}^{s_i} \mathfrak{P}_{i,j}^{e_{i,j}}$.

(5.28) **Bemerkung** *Wie in Bemerkung 5.24 ist auch die Komplexität von Algorithmus 5.23 nicht angegeben, da sie wesentlich an der Berechnung der Primideale und damit auch an der Konstruktion der einfachen Bestandteile [Ebe89, Algorithmus, S. 101] hängt.*

(5.29) **Proposition** *Die Faktorisierung eines ganzen zweiseitigen Ideals $\mathfrak{a}$ der Ordnung Λ in der Form von (5.25), die von Algorithmus 5.27 berechnet wird, ist eindeutig.*

Beweis: Es seien $\mathfrak{P}_1, \mathfrak{P}_2$ zwei verschiedene invertierbare Primideale von Λ. Weiterhin gelte $\mathfrak{a} \subseteq \mathfrak{P}_1$ und $\mathfrak{b} = \mathfrak{a}\mathfrak{P}_2^{-1} \subseteq \Lambda$. Angenommen $\mathfrak{b} \not\subseteq \mathfrak{P}_1$, dann folgt aus der Primideal-Eigenschaft von $\mathfrak{P}_1$ wegen $\mathfrak{b}\mathfrak{P}_2 = \mathfrak{a} \subseteq \mathfrak{P}_1$ sofort der Widerspruch $\mathfrak{P}_2 \subseteq \mathfrak{P}_1$.

Außerdem kommutieren die Ideale $\mathfrak{P}_1, \mathfrak{P}_1^{-1}, \mathfrak{P}_2, \mathfrak{P}_2^{-1}$ mit allen anderen zweiseitigen Idealen von Λ, vgl. Bemerkung 2.50. Es spielt also keine Rolle, in welcher Reihenfolge man die invertierbaren Primideale abspaltet. □

(5.30) **Bemerkung** *Das oben beschriebene Verfahren läßt sich ebenso auch auf gebrochene zweiseitige Ideale $\mathfrak{b}$ von Λ anwenden, da ein $r \in R$ existiert mit $r\mathfrak{b} = \mathfrak{a}$ ist ein ganzes zweiseitiges Ideal von Λ, siehe auch Bemerkung 2.52.*

In Maximalordnungen bekommt man mit Algorithmus 5.27 die vollständige Faktorisierung beliebiger zweiseitiger Ideal in Primideale. Das Verfahren ist ein konstruktiver Beweis von Theorem 2.28.

Kapitel 6
Erweiterungen

In diesem Kapitel werden einige Erweiterungen und Verbesserungen der Verfahren zur Berechnung von Maximalordnungen in separablen Algebren entwickelt. Insbesondere gehen die Abschnitte 6.3.1 und 6.3.2 auf die Anwendung dieser Erweiterungen zur Berechnung der Maximalordnung in algebraischen Zahlkörpern bzw. algebraischen Funktionenkörpern ein.

6.1 $\mathfrak{m}$-maximal und $\mathfrak{m}$-hereditär

$\{0\} \neq \mathfrak{m} \neq R$ sei ein beliebiges Ideal des Dedekindringes R. Man nennt die R-Ordnung Λ $\mathfrak{m}$-*maximal*, wenn $\gcd\left((\Lambda^{(\max)}) : \Lambda, \mathfrak{m}\right) = R$ für eine (und damit jede) Maximalordnung $\Lambda^{(\max)} \supseteq \Lambda$ gilt, vgl. [PZ89, Chpt. 4, Def. 5.83].

(6.1) **Korollar** *Die Ordnung Λ ist genau dann $\mathfrak{m}$-maximal, wenn Λ für jedes Primideal $\mathfrak{p} \supseteq \mathfrak{m}$ von R $\mathfrak{p}$-maximal ist.*

(6.2) **Korollar** *Die Ordnung Λ ist genau dann maximal, wenn sie* $\mathrm{disc}(\Lambda)$*-maximal ist.*

Analog zur $\mathfrak{m}$-Maximalität heißt eine R-Ordnung Λ $\mathfrak{m}$-hereditär, wenn Λ für jedes Primideal $\mathfrak{p} \supseteq \mathfrak{m}$ von R $\mathfrak{p}$-hereditär ist.

(6.3) **Korollar** *Die Ordnung Λ ist genau dann hereditär, wenn sie* $\mathrm{disc}(\Lambda)$*-hereditär ist.*

Wie in Abschnitt 3.3 bekommt der Schnitt $\sqrt{\mathfrak{m}\Lambda}$ über alle maximalen zweiseitigen Ideale von Λ, die das Ideal $\mathfrak{m}$ enthalten, den Namen $\mathfrak{m}$-*Radikal*.

(6.4) **Proposition** *Ist $\mathfrak{p}$ ein Primideal von R, das $\mathfrak{m}$ enthält, so gilt für die Lokalisierung des $\mathfrak{m}$-Radikals $\left(\sqrt{\mathfrak{m}\Lambda}\right)_{\mathfrak{p}} = J(\Lambda_{\mathfrak{p}})$, mit dem Jacobson-Radikal $J(\Lambda_{\mathfrak{p}})$ von $\Lambda_{\mathfrak{p}}$.*

Wenn $\mathfrak{m}$ nicht in dem Primideal $\mathfrak{p}$ von R enthalten ist, so erhält man für die Lokalisierung des $\mathfrak{m}$-Radikals $\left(\sqrt{\mathfrak{m}\Lambda}\right)_{\mathfrak{p}} = \Lambda_{\mathfrak{p}}$.

Beweis: Mit Proposition 3.28 erhält man $\left(\sqrt{\mathfrak{m}\Lambda}\right)_\mathfrak{p} = \left(\bigcap_{\mathfrak{m}\subseteq\mathfrak{P}} \mathfrak{P}\right)_\mathfrak{p} = \bigcap_{\mathfrak{m}\subseteq\mathfrak{P}} \mathfrak{P}_\mathfrak{p}$, wobei jeweils die Ideale $\mathfrak{P}$ Primideale von Λ seien. Gilt $\mathfrak{m} \subseteq \mathfrak{p}$, so tauchen unter den Idealen $\mathfrak{P}_\mathfrak{p}$ mit $\mathfrak{m} \subseteq \mathfrak{P}$ gerade alle Primideale von $\Lambda_\mathfrak{p}$ auf. Man erhält die erste Aussage.

Ist $\mathfrak{m}$ nicht in $\mathfrak{p}$ enthalten, so enthält jedes Primideal $\mathfrak{P} \supseteq \mathfrak{m}$ von Λ ein zu $\mathfrak{p}$ teilerfremdes Primideal von R. Es folgt $\mathfrak{P}_\mathfrak{p} = \Lambda_\mathfrak{p}$ und damit die zweite Aussage. □

(6.5) **Proposition** *Für ein Primideal $\mathfrak{p} \supseteq \mathfrak{m}$ von R gelten $\mathcal{O}_l(J(\Lambda_\mathfrak{p})) = \left(\mathcal{O}_l(\sqrt{\mathfrak{m}\Lambda})\right)_\mathfrak{p}$, $\mathcal{O}_r(J(\Lambda_\mathfrak{p})) = \left(\mathcal{O}_r(\sqrt{\mathfrak{m}\Lambda})\right)_\mathfrak{p}$ und $Id(J(\Lambda_\mathfrak{p})) = \left(Id(\sqrt{\mathfrak{m}\Lambda})\right)_\mathfrak{p}$.*

Beweis: Für $x \in \mathcal{O}_l(\sqrt{\mathfrak{m}\Lambda})$ gilt $x\sqrt{\mathfrak{m}\Lambda} \subseteq \sqrt{\mathfrak{m}\Lambda}$, also $xR_\mathfrak{p}\sqrt{\mathfrak{m}\Lambda} \subseteq R_\mathfrak{p}\sqrt{\mathfrak{m}\Lambda}$ und damit $x\,J(\Lambda_\mathfrak{p}) \subseteq J(\Lambda_\mathfrak{p})$. Es gilt daher $R_\mathfrak{p}\mathcal{O}_l(\sqrt{\mathfrak{m}\Lambda}) \subseteq \mathcal{O}_l(J(\Lambda_\mathfrak{p}))$.

Auf der anderen Seite sei $x \in \mathcal{O}_l(J(\Lambda_\mathfrak{p}))$, dann gilt $x\sqrt{\mathfrak{m}\Lambda} \subseteq xR_\mathfrak{p}\sqrt{\mathfrak{m}\Lambda} = x\,J(\Lambda_\mathfrak{p}) \subseteq J(\Lambda_\mathfrak{p}) = R_\mathfrak{p}\sqrt{\mathfrak{m}\Lambda}$. Da $x\sqrt{\mathfrak{m}\Lambda}$ ein endlich erzeugter R-Modul ist, existiert ein $s \in R \setminus \mathfrak{p}$ mit $x\sqrt{\mathfrak{m}\Lambda} \subseteq \frac{1}{s}\sqrt{\mathfrak{m}\Lambda}$, also $sx \in \mathcal{O}_l(\sqrt{\mathfrak{m}\Lambda})$ und damit $x = \frac{1}{s}sx \in R_\mathfrak{p}\mathcal{O}_l(\sqrt{\mathfrak{m}\Lambda})$.

Die anderen Aussagen folgen analog. □

Die Anwendungen folgen direkt aus der Hauptaussage dieses Kapitels.

(6.6) **Theorem** *Für die R-Ordnung Λ sind die folgenden Aussagen äquivalent:*

(1) Λ ist $\mathfrak{m}$-hereditär,

(2) das $\mathfrak{m}$-Radikal $\sqrt{\mathfrak{m}\Lambda}$ ist in Λ invertierbar,

(3) $\mathcal{O}_l(\sqrt{\mathfrak{m}\Lambda}) = \Lambda$,

(4) $\mathcal{O}_r(\sqrt{\mathfrak{m}\Lambda}) = \Lambda$,

(5) $Id(\sqrt{\mathfrak{m}\Lambda}) = \Lambda$.

Beweis: Ist Λ $\mathfrak{m}$-hereditär, so ist für jedes Primideal $\mathfrak{p} \supseteq \mathfrak{m}$ von R das Jacobson-Radikal $J_\mathfrak{p}$ der Lokalisierung $\Lambda_\mathfrak{p}$ invertierbar, da $\Lambda_\mathfrak{p}$ hereditär ist, vgl. Theorem 4.9. Wie im Beweis zu Proposition 4.10 setzt man aus $\mathfrak{a}_\mathfrak{p} := (J_\mathfrak{p})^{-1}$ für $\mathfrak{m} \subseteq \mathfrak{p}$ und $\mathfrak{a}_\mathfrak{p} := \Lambda_\mathfrak{p}$ für $\mathfrak{m} \not\subseteq \mathfrak{p}$ das zweiseitige Ideal $\mathfrak{a} := \bigcap_\mathfrak{p} \mathfrak{a}_\mathfrak{p}$ zusammen, für das $\sqrt{\mathfrak{m}\Lambda}\mathfrak{a} = \bigcap_\mathfrak{p} \left(\sqrt{\mathfrak{m}\Lambda}\right)_\mathfrak{p} \mathfrak{a}_\mathfrak{p} = \bigcap_\mathfrak{p} \Lambda_\mathfrak{p} = \Lambda$ und ebenso $\mathfrak{a}\sqrt{\mathfrak{m}\Lambda} = \Lambda$ gilt.

Andersherum sei $\mathfrak{p} \supseteq \mathfrak{m}$ ein Primideal von R, dann ist mit $\sqrt{\mathfrak{m}\Lambda}$ nach Proposition 6.4 auch $J(\Lambda_\mathfrak{p}) = \left(\sqrt{\mathfrak{m}\Lambda}\right)_\mathfrak{p}$ invertierbar mit $\left(\left(\sqrt{\mathfrak{m}\Lambda}\right)^{-1}\right)_\mathfrak{p}$. Die Ordnung Λ ist $\mathfrak{p}$-hereditär (Theorem 4.9).

Die Äquivalenz (1) $\Leftrightarrow$ (2) ist damit gezeigt. Als nächste folgt beispielhaft die Äquivalenz (1) $\Leftrightarrow$ (3), die anderen kann man ganz analog beweisen.

Ist die Ordnung Λ $\mathfrak{m}$-hereditär, so ist $\sqrt{\mathfrak{m}\Lambda}$ invertierbar (siehe oben) und deshalb nach Proposition 2.39 $\mathcal{O}_l(\sqrt{\mathfrak{m}\Lambda}) = \Lambda$. Aus Proposition 6.5 erhält man im Falle $\mathcal{O}_l(\sqrt{\mathfrak{m}\Lambda}) = \Lambda$ für jede Lokalisierung $O_l(J(\Lambda_\mathfrak{p})) = R_\mathfrak{p}\mathcal{O}_l(\sqrt{\mathfrak{m}\Lambda}) = R_\mathfrak{p}\Lambda = \Lambda_\mathfrak{p}$ für jedes Primideal $\mathfrak{p} \supseteq \mathfrak{m}$ von R. Damit ist Λ nach Proposition 4.7 und Proposition 4.8 $\mathfrak{p}$-hereditär. □

(6.7) **Korollar** *Die Ordnung Λ ist genau dann hereditär, wenn $\Lambda = \mathcal{O}_l(\sqrt{\mathrm{disc}(\Lambda)\Lambda})$ gilt. Dies ist genau dann erfüllt, wenn $\Lambda = \mathcal{O}_r(\sqrt{\mathrm{disc}(\Lambda)\Lambda})$ oder $\Lambda = Id(\sqrt{\mathrm{disc}(\Lambda)\Lambda})$ gilt.*

(6.8) **Proposition** *Das R Ideal $\mathfrak{m}$ habe die Faktorisierung $\mathfrak{m} = \prod_{i=1}^{k} \mathfrak{p}_i^{e_i}$ in R. Ist die R-Ordnung Λ nicht $\mathfrak{p}_j$-hereditär, für ein $1 \leq j \leq k$, so gilt $\mathfrak{p}_j \mid \left(\mathcal{O}_l(\sqrt{\mathfrak{m}\Lambda}) : \Lambda\right)$.*

Für jedes $1 \leq j \leq k$ sei $\mathrm{disc}(\Lambda) = \mathfrak{p}_j^{2\mu_j}\mathfrak{q}_j$ mit $\mathfrak{q}_j \not\subseteq \mathfrak{p}_j^2$. Dann ist die Komplexität zur Berechnung einer $\mathfrak{m}$-hereditären Ordnung mit Hilfe des $\mathfrak{m}$-Radikals $O(\mu(n^4 + g(n)))$, mit $\mu = max_{i=1}^{k}\mu_i$ und $g(n)$ sie die Komplexität für die Berechnung des $\mathfrak{m}$-Radikals.

Beweis: Sei $1 \leq j \leq k$ beliebig und gelte $\mathfrak{p}_j$ teilt nicht $\left(\mathcal{O}_l(\sqrt{\mathfrak{m}\Lambda}) : \Lambda\right)$, so erhält man nach Proposition 6.5 $R_{\mathfrak{p}_j}\mathfrak{p}_j$ teilt nicht $\left(\mathcal{O}_l(J(\Lambda_{\mathfrak{p}_j})) : \Lambda_{\mathfrak{p}_j}\right)$. $\Lambda_{\mathfrak{p}_j}$ ist demnach hereditär, Λ also $\mathfrak{p}_j$-hereditär.

Die Komplexität erhält man analog zu Proposition 4.13. □

Für kommutative Algebren erhält man ähnlich wie in Korollar 4.21 die folgende Aussage, die man allerdings auch auf direktem Wege beweisen kann.

(6.9) **Korollar** [PZ89, Chpt. 4, Lem. 5.53] *Die R-Ordnung Λ in der kommutativen F-Algebra A ist genau dann $\mathfrak{m}$-maximal, wenn das $\mathfrak{m}$-Radikal invertierbar ist. Dies ist genau dann der Fall, wenn $\mathcal{O}_l(\sqrt{\mathfrak{m}\Lambda}) = \Lambda$.*

Insbesondere ist Λ genau dann maximal, wenn $\mathcal{O}_l\left(\sqrt{\mathrm{disc}(\Lambda)\Lambda}\right) = \Lambda$ gilt.

(6.10) **Bemerkung** *Der erste Teil von Proposition 6.8 zeigt, daß es genügt, bei der Berechnung einer $\mathfrak{m}$-hereditären Ordnung, nach dem ersten Schritt ($\mathcal{O}_l(\sqrt{\mathfrak{m}\Lambda})$) das Ideal $\mathfrak{m}$ durch den Index $\left(\mathcal{O}_l(\sqrt{\mathfrak{m}\Lambda}) : \Lambda\right)$ zu ersetzen.*

(6.11) **Bemerkung** *An Stelle der Diskriminante* $\mathrm{disc}(\Lambda)$ *kann in Korollar 6.7 oder Korollar 6.9 natürlich auch die reduzierte Diskriminante* $\mathrm{disc}_r(\Lambda)$ *verwendet werden. Sie enthält ebenfalls alle Primideale von* R*, die auch in* $\mathrm{disc}(\Lambda)$ *aufgehen.*

Die Verwendung der reduzierten Diskriminante wurde erstmals von Rudolf Land zur Berechnung von Maximalordnungen in algebraischen Zahlkörpern verwendet, vgl. [PZ89, Chpt. 4, S. 296].

6.2 Berechnung des $\mathfrak{m}$-Radikals

Hier wird gezeigt, unter welchen Voraussetzungen an das Ideal $\mathfrak{m}$ das $\mathfrak{m}$-Radikal $\sqrt{\mathfrak{m}\Lambda}$ berechnet werden kann. Man kann damit also eine hereditäre Ordnung oder im kommutativen Fall eine maximale Ordnung berechnen, ohne die Diskriminante vollständig zu faktorisieren.

Die Berechnung des $\mathfrak{m}$-Radikals hängt wieder wesentlich von den Eigenschaften der Restklassenkörper $\bar{R} = R/\mathfrak{p}$ für alle Primideale $\mathfrak{p} \supseteq \mathfrak{m}$ ab.

6.2.1 Frobenius-Homomorphismus

$\varphi : \Lambda \to \hat{\Lambda} := \Lambda/\mathfrak{m}\Lambda$ sei der kanonische Homomorphismus. Eine direkte Folgerung aus Proposition 5.11 ist

(6.12) **Proposition** *Für das* $\mathfrak{m}$*-Radikal von* Λ *gilt* $\sqrt{\mathfrak{m}\Lambda}^n \subseteq \left(\prod_{\mathfrak{m}\subseteq\mathfrak{p}} \mathfrak{p}\right)\Lambda$*, wobei* $\mathfrak{p}$ *Primideale von* R *seien.*

Beweis: Es gilt $\sqrt{\mathfrak{m}\Lambda}^n = \left(\bigcap_{\mathfrak{m}\subseteq\mathfrak{p}} \sqrt{\mathfrak{p}\Lambda}\right)^n \subseteq \bigcap_{\mathfrak{m}\subseteq\mathfrak{p}} \left(\sqrt{\mathfrak{p}\Lambda}\right)^n \subseteq \bigcap_{\mathfrak{m}\subseteq\mathfrak{p}} \mathfrak{p}\Lambda = \left(\prod_{\mathfrak{m}\subseteq\mathfrak{p}} \mathfrak{p}\right)\Lambda$. □

Für das Jacobson-Radikal $J = J(\hat{\Lambda}) = \varphi(\sqrt{\mathfrak{m}\Lambda})$ gilt dann $J^n = \{0\}$. Für den Rest dieses Abschnitts wird als Voraussetzung benötigt, daß eine Primzahl p existiert, so daß für alle Primideale $\mathfrak{p} \supseteq \mathfrak{m}$ von R der Restklassenkörper $R/\mathfrak{p}$ endlich ist und Charakteristik p hat. Außerdem sei die Faktoralgebra $\hat{\Lambda}$ kommutativ. In diesem Fall kann dann ebenfalls der Frobenius-Homomorphismus zur Berechnung des $\mathfrak{m}$-Radikals verwendet werden.

Das Ideal $\mathfrak{m}$ hat in dem Dedekindring R die Faktorisierung $\mathfrak{m} = \prod_{i=1}^{k} \mathfrak{p}_i^{e_i}$, dann gilt nach dem chinesischen Restsatz $R/\mathfrak{m} \cong \bigoplus_{i=1}^{k} R/\mathfrak{p}_i^{e_i}$. Jeder Faktorring $R/\mathfrak{p}_i^{e_i}$ ist eine endlich dimensionale Algebra über $\mathbb{F}_p$. Folglich ist auch $R/\mathfrak{m}$ in diesem Fall eine endlich dimensionale $\mathbb{F}_p$-Algebra mit $q = p^f$ Elementen. Außerdem ist $R/\mathfrak{m}$ nach Proposition 1.11 ein Ring, in dem jedes Ideal Hauptideal ist. Folglich ist $\hat{\Lambda}$ eine endlich dimensionale Algebra über $\mathbb{F}_p$.

Es sei $\kappa > 0$ so gewählt, daß $p^{\kappa-1} < n \leq p^{\kappa}$. Die Abbildung $\psi : \hat{\Lambda} \to \hat{\Lambda} : x \mapsto x^{q^{\kappa}}$ ist $\mathbb{F}_p$-linear, vgl. Abschnitt 5.1.2, und der Kern von ψ entspricht gerade J. Da $\hat{R} = R/\mathfrak{m}$ im allgemeinen nicht nullteilerfrei ist, vgl. Abschnitt 1.6, gilt in $\hat{R} \setminus \{0\}$ der kleine Fermat'sche Satz [Mey75, Kapitel 1.7, Kor. 3, S. 48] nicht mehr, so daß ψ nicht $\hat{R}$-linear ist.

(6.13) **Bemerkung** *Das $\mathfrak{m}$-Radikal kann in diesem Fall durch den Kern der linearen Abbildung ψ und Anwendung eines analogen Verfahrens zu Algorithmus 5.1 berechnet werden.*

Ebenso wie in Proposition 5.14 ist auch hier $\tau := \max(n^2, p)$ eine obere Abschätzung für den Exponenten κ. Man muß dann sowohl die n $R/\mathfrak{m}$-Basiselemente $\omega_1, \ldots, \omega_n$ von $\hat{\Lambda}$, als auch die f $\mathbb{F}_p$-Basiselemente $\eta_1, \ldots, \eta_f$ von $R/\mathfrak{m}$ potenzieren. Dies wird dann zu einer Darstellung der linearen Abbildung ψ über $\mathbb{F}_p$ zusammengesetzt. ψ wird durch eine $fn \times fn$-Matrix über $\mathbb{F}_p$ dargestellt.

Die Komplexität kann also in diesem Fall nicht über $R/\mathfrak{m}$ bzw. F angegeben werden, sondern über $\mathbb{F}_p$. Im allgemeinen ist aber die Dimension f der $\mathbb{F}_p$-Algebra $R/\mathfrak{m}$ vorher nicht bekannt.

6.2.2 Spur-Radikal

Hier wird das Verfahren aus [BL, BL94] zur Berechnung des $\mathfrak{m}$-Radikals von Ordnungen in endlichen Erweiterungen von $\mathbb{Q}$ verallgemeinert. Für alle Primideale $\mathfrak{p} \supseteq \mathfrak{m}$ von R sei jetzt die Charakteristik von $R/\mathfrak{p}$ Null oder größer als n.

Ähnlich wie in Abschnitt 5.1.1 ist für ein beliebiges Ideal $\mathfrak{n}$ von R das $\mathfrak{n}$-*Spur-Radikal* $I_{\mathfrak{n},\Lambda}^{(\mathrm{Spur})} := \{a \in \Lambda | \, \mathrm{T}(xa) \in \mathfrak{n} \text{ für alle } x \in \Lambda\}$.

(6.14) **Proposition** *Es sei $\mathfrak{m} = \prod_{i=1}^{k} \mathfrak{p}_i^{e_i}$ die Faktorisierung von $\mathfrak{m}$ in R. Dann gilt für das $\mathfrak{m}$-Radikal von Λ $\sqrt{\mathfrak{m}\Lambda} = I_{\mathfrak{n},\Lambda}^{(Spur)}$, mit $\mathfrak{n} = \prod_{i=1}^{k} \mathfrak{p}_i$.*

Ist das Ideal $\mathfrak{m}$ quadratfrei, also alle $e_i = 1$, so gilt $\sqrt{\mathfrak{m}\Lambda} = I_{\mathfrak{m},\Lambda}^{(Spur)}$.

Beweis: Es gilt $\sqrt{\mathfrak{m}\Lambda} = \bigcap_{i=1}^{k} \sqrt{\mathfrak{p}_i\Lambda}$, also $x \in \sqrt{\mathfrak{m}\Lambda} \Leftrightarrow x \in \sqrt{\mathfrak{p}_i\Lambda}$ $(1 \leq i \leq k) \Leftrightarrow \mathrm{T}(yx) \in \mathfrak{p}_i$ $(1 \leq i \leq k) \Leftrightarrow \mathrm{T}(yx) \in \bigcap_{i=1}^{k} \mathfrak{p}_i = \prod_{i=1}^{k} \mathfrak{p}_i$, vgl. Korollar 5.8. □

Zur Berechnung des $\mathfrak{m}$-Spur-Radikals wird hier ein anderes Verfahren als [BL, Sect. 3.7] oder [BL94, Alg. 6.3] herangezogen. Im Falle $R = \mathbb{Z}, \mathfrak{m} = mZ$ wird dort zur Berechnung des $\mathfrak{m}$-Spur-Radikals das zu Korollar 5.6 analoge Verfahren verwendet. Dazu wird Arithmetik in $R/\mathfrak{m}$ und zur Berechnung des Kerns der linearen Abbildung insbesondere eine Hermite-Normal-Form über $R/\mathfrak{m}$ benötigt.

Da $R/\mathfrak{m}$ im allgemeinen nicht nullteilerfrei ist, sind die Algorithmen dort wie folgt formuliert: „Der Algorithmus liefert das gewünschte Ergebnis oder einen nicht trivialen Teiler von m.“ Diese Probleme mit der modularen Arithmetik und der Berechnung des Kerns sind inzwischen für den Fall $R = \mathbb{Z}$ gelöst [Nei98, Sect. 3 und Alg. 2]. In [BN98, Sect. 2, S. 3] wird das Verfahren zur Berechnung des größten gemeinsamen Teilers in $R/\mathfrak{m}$ beschrieben, das zur Berechnung einer Hermite-Normal-Form erforderlich ist. Es wird von einer erweiterten ggT-Berechnung in R abgeleitet, so daß sich das Verfahren zwar auf Hauptidealringe R ausdehnen läßt, aber in allgemeinen Dedekindringen nicht anwendbar ist.

Die Idee für den Algorithmus, der hier vorgestellt wird, liefert [OMe63, §82I]: Es gilt $I_{\mathfrak{m},\Lambda}^{(\mathrm{Spur})} = \mathfrak{m}\Lambda^{\perp} \cap \Lambda$. Dies Verfahren läßt sich in dem üblichen allgemeinen Rahmen (R Dedekindring) anwenden. Im folgenden wird dies Verfahren erläutert.

Die Ordnung Λ sei durch eine Pseudo-Basis $\Lambda = \bigoplus_{i=1}^{n} \mathfrak{a}_i\omega_i$ gegeben. Damit können beliebige Elemente $x, y \in A$ durch ihre Koeffizientenvektoren $\vec{x}, \vec{y}$ bezüglich $\omega_1, \ldots, \omega_n$ dargestellt werden.

Für ein beliebiges $x \in A$ gilt $x \in I_{\mathfrak{m},\Lambda}^{(\mathrm{Spur})}$ genau dann, wenn $\mathrm{T}(yx) = \sum_{i=1}^{n}\sum_{j=1}^{n}(y_i x_j \,\mathrm{T}(\omega_i\omega_j)) \in \mathfrak{m}$ für jedes $y \in \Lambda$ und $(1 \le i \le n)$ $x_i \in \mathfrak{a}_i$ erfüllt ist. Dies trifft genau dann zu, wenn $(1 \le i \le n)$ $\mathfrak{a}_i \left(\mathrm{T}(\omega_i\omega_j)\right)_{(i,\cdot)} \vec{x} \in \mathfrak{m}$ und $x_i \in \mathfrak{a}_i$. Was wiederum äquivalent ist zu $(1 \le i \le n)$ $\mathfrak{a}_i/\mathfrak{m} \left(\mathrm{T}(\omega_i\omega_j)\right)_{(i,\cdot)} \vec{x} \in R$ und $(1/\mathfrak{a}_i)x_i \in R$.

Daraus folgt die Äquivalenz zu: Für jedes Element z des R-Gitters

$$\mathcal{M} := \begin{bmatrix} (\mathfrak{a}_1/\mathfrak{m}) & \cdots & (\mathfrak{a}_n/\mathfrak{m}) & (1/\mathfrak{a}_1) & \cdots & (1/\mathfrak{a}_n) \\ & & & 1 & \cdots & 0 \\ & \left(\mathrm{T}(\omega_i\omega_j)\right)_{(1\le i,j\le n)} & & \vdots & \ddots & \vdots \\ & & & 0 & \cdots & 1 \end{bmatrix} \tag{6.15}$$

gilt $\vec{x}^{tr} \cdot z \in R$. Die Anwendung der Hermite-Normal-Form (Theorem 1.15) auf $\mathcal{M}$ verändert die letzte Äquivalenz nicht, so daß $x \in I_{\mathfrak{m},\Lambda}^{(\mathrm{Spur})}$ dann und nur dann, wenn für jedes Element z des R-Gitters $\begin{bmatrix} \mathfrak{b}_1 & \cdots & \mathfrak{b}_n \\ & M & \end{bmatrix} := \mathrm{HNF}(\mathcal{M})$ wieder $\vec{x}^{tr} \cdot z \in R$ erfüllt ist. Schließlich erhält man $I_{\mathfrak{m},\Lambda}^{(\mathrm{Spur})} := \bigoplus_{i=1}^{n}(1/\mathfrak{b}_i)\gamma_i$, wobei $(\gamma_1, \ldots, \gamma_n) := (\omega_1, \ldots, \omega_n) \cdot (M^{tr})^{-1}$ gilt.

(6.16) **Algorithmus $\mathfrak{m}$-Spur-Radikal**
Input: *Eine Ordnung $\Lambda = \bigoplus_{i=1}^{n} \mathfrak{a}_i\omega_i$ und ein Ideal $\mathfrak{m} \subset R$.*
Output: *Das $\mathfrak{m}$-Spur-Radikal von Λ.*

(1) *Initialisiere das Gitter $\mathcal{M}$ wie in (6.15).*

(2) *Hermite-Normal-Form:* $\begin{bmatrix} \mathfrak{b}_1 & \cdots & \mathfrak{b}_n \\ & M & \end{bmatrix} = \mathrm{HNF}(\mathcal{M})$.

(3) $\mathfrak{m}$*-Spur-Radikal zusammensetzen:* $I_{\mathfrak{m},\Lambda}^{(Spur)} := \bigoplus_{i=1}^{n}(1/\mathfrak{b}_i)\gamma_i$, *mit* $(\gamma_1,\ldots,\gamma_n) := (\omega_1,\ldots,\omega_n)\cdot(M^{tr})^{-1}$.

(6.17) **Proposition** *Die Komplexität von Algorithmus 6.16 ist $O(n^4)$ gemessen in Elementaroperationen des Grundkörpers F.*

Beweis: Für die Komplexität der Berechnung von $(\mathrm{T}(\omega_i\omega_j))_{(1\le i,j\le n)}$ erhält man wie im Beweis zu Proposition 5.7 $O(n^4)$. Bei den restlichen Abschätzungen verfährt man so wie im Beweis zu Proposition 2.18: Die Konstruktion von $\mathfrak{a}_1/\mathfrak{m},\ldots,\mathfrak{a}_n/\mathfrak{m},1/\mathfrak{a}_1,\ldots,1/\mathfrak{a}_n$ benötigt $O(n)$ Elementaroperationen. Demnach kostet der erste Schritt $O(n^4)$ Elementaroperationen. Die Anwendung der Hermite-Normal-Form auf einen Modul mit $2n$ Erzeugern hat eine Komplexität von $O(n^3)$, vgl. Theorem 1.15.

Für die Erzeugung der Basiselemente $\gamma_1,\ldots,\gamma_n$ werden $O(n^2)$ und zur Invertierung der Koeffizientenideale $\mathfrak{b}_i$ $O(n)$ Schritte benötigt. □

(6.18) **Bemerkung** $\mathfrak{p}$ *sei ein Primideal von R. Algorithmus 6.16 läßt sich natürlich auch verwenden, um das* $\mathfrak{p}$*-Spur-Radikal und damit in den entsprechenden Fällen auch das* $\mathfrak{p}$*-Radikal der Ordnung Λ zu berechnen.*

Die Komplexität von Algorithmus 6.16 ist die gleiche wie die von Korollar 5.10. In der Praxis hat sich allerdings herausgestellt, daß die Berechnung des $\mathfrak{p}$*-Radikals mit Hilfe des Verfahrens aus Abschnitt 5.1.1 durch die Arithmetik über dem Restklassenkörper schneller ist.*

6.2.3 $\mathfrak{m}$ nicht quadratfrei

Aus Proposition 6.14 leitet man für beliebige Ideale $\mathfrak{m}$ von R sofort die folgende Aussage ab.

(6.19) **Korollar** *Für jedes Ideal $\{0\}\subset\mathfrak{m}\subset R$ von R, so das für alle Primideale $\mathfrak{p}\supseteq\mathfrak{m}$ von R die Charakteristik des Restklassenkörpers $R/\mathfrak{p}$ Null oder größer als n ist, gilt $I_{\mathfrak{m},\Lambda}^{(Spur)}\subseteq\sqrt{\mathfrak{m}\Lambda}$.*

Sollte $\mathfrak{p}$ ein Primideal von R sein, für das die positive Charakteristik des Restklassenkörpers $R/\mathfrak{p}$ kleiner oder gleich n ist, so erhält man nach Korollar 5.9 nur $\sqrt{\mathfrak{p}\Lambda}\subseteq I_{\mathfrak{p},\Lambda}^{(\mathrm{Spur})}$.

(6.20) **Korollar** *Für ein beliebiges Ideal $\mathfrak{m}=\prod_{i=1}^{k}\mathfrak{p}_i^{e_i}$ von R gilt demnach $\sqrt{\mathfrak{m}\Lambda}\subseteq I_{\mathfrak{n},\Lambda}^{(Spur)}$, mit $\mathfrak{n}=\prod_{i=1}^{k}\mathfrak{p}_i$.*

Ähnlich wie in Abschnitt 5.1.3 bleibt neben der Verwendung der Ideale aus Korollar 6.19 und Korollar 6.20 noch die Möglichkeit, mit Hilfe von Bemerkung 5.17, Bemerkung 5.18 oder Bemerkung 5.19 einen Aufstieg zu einer größeren Ordnung zu erhalten.

6.3 Anwendungen

Das $\mathfrak{m}$-Radikal läßt sich natürlich verwenden, um nicht für jeden Teiler $\mathfrak{p}$ der Diskriminante $\mathrm{disc}(\Lambda)$, $\mathfrak{p} \supseteq \mathrm{disc}(\Lambda)$ Primideal von R, einzeln (lokal) eine $\mathfrak{p}$-hereditäre Ordnung $\Lambda^{(\mathfrak{p}\text{-her})} \supseteq \Lambda$ zu berechnen, und das Ergebnis anschließend wieder zusammenzusetzen (Proposition 4.14, Algorithmus 4.16). Man kann das $\mathrm{disc}(\Lambda)$-Radikal verwenden, um eine $\mathrm{disc}(\Lambda)$-hereditäre Ordnung (und damit eine hereditäre Ordnung) direkt zu berechnen, vgl. Theorem 6.6. Die Komplexität wird dadurch kleiner, da weniger „Links-Ordnungs-Schritte“ gemacht werden müssen, siehe Proposition 6.8.

Zur Berechnung des $\mathrm{disc}(\Lambda)$-Radikals bietet sich entweder eine der Möglichkeiten aus dem vorangegangenen Abschnitt an, oder wenn die Faktorisierung von $\mathrm{disc}(\Lambda)$ bekannt ist, kann man auch mit Algorithmus 5.1 für jeden Teiler $\mathfrak{p}$ von $\mathrm{disc}(\Lambda)$ das $\mathfrak{p}$-Radikal einzeln berechnen, und das $\mathrm{disc}(\Lambda)$-Radikal mittels $\sqrt{\mathrm{disc}(\Lambda)\Lambda} = \bigcap_{\mathfrak{p} \supseteq \mathrm{disc}(\Lambda)} \sqrt{\mathfrak{p}\Lambda}$ zusammensetzen.

Wie in Bemerkung 6.11 kann an Stelle von $\mathrm{disc}(\Lambda)$ oben auch $\mathrm{disc}_r(\Lambda)$ verwendet werden. Im Fall kommutativer Algebren gelten die Ausführungen auch für „maximal“ an Stelle von „hereditär“.

6.3.1 Algebraische Zahlkörper

Zu den bisher in Computeralgebra-Systemen implementierten Fällen gehören die algebraischen Zahlkörper A, also $R = \mathbb{Z}$ und $F = \mathbb{Q}$ oder für Relativerweiterungen $R = \mathrm{Cl}(\mathbb{Z}, F)$ mit einem algebraischen Zahlkörper $F \subseteq A$. Bei der Berechnung der Maximalordnung in A hat sich gezeigt, daß die Faktorisierung der Diskriminante einer der aufwendigsten Teile ist.

In einigen Fällen ist die Diskriminante der Maximalordnung allerdings im voraus bekannt, so daß man schon den nötigen Index kennt. Die Primideale, deren Restklassenkörper eine Charakteristik haben, die kleiner oder gleich n ist, können gesondert behandelt werden.

Man behält ein Ideal $\mathfrak{m}$ (ein Teiler des Index) übrig, das nur noch die Primideale enthält, deren Restklassenkörper eine Charakteristik haben, die größer als n ist. Berechnet man dann die Links-Ordnung des $\mathfrak{m}$-Spur-Radikals, so erreicht man häufig einen Aufstieg. Da der nötige Index bekannt ist, kann man überprüfen, ob die erhaltene Ordnung maximal ist, oder nicht.

Erhält man keinen Aufstieg und ist die Ordnung noch nicht maximal, so versucht man, die Wurzel aus dem Ideal $\mathfrak{m}$ zu ziehen und arbeitet damit weiter. Beispiele, die dieses Verhalten demonstrieren, sind in Abschnitt 7.2.1 aufgeführt. Bei den Beispielen die [GP97] entnommen sind genügt sogar die Berechnung einer einzigen Links-Ordnung des $\mathfrak{m}$-Spur-Radikals, wenn $\mathfrak{m}$ der Index ist.

6.3.2 Algebraische Funktionenkörper

Für Funktionenkörper $R = K[t], F = K(t)$ und $A = F[y]/fF[y]$, wobei $f \in R[y]$ ein normiertes irreduzibles Polynom und K ein endlicher Körper (globaler Funktionenkörper), $\mathbb{Q}$ oder ein Zahlkörper ist, wird die Diskriminante $\mathrm{disc}(\Lambda) = gK[t]$ einer Ordnung Λ von einem Polynom g aus $K[t]$ erzeugt. Man kann also besonders einfach eine quadratfreie-Faktorisierung der Diskriminante berechnen $g = \prod_{i=1}^{k} g_i^i$ mit paarweise teilerfremden quadratfreien Polynomen $g_i \in K[t]$, vgl. [Zip93, Chpt. 18, S. 293].

Außerdem kann man die relevanten Eigenschaften des Restklassenkörpers $R/\mathfrak{p}$ schon an K ablesen. Sie sind unabhängig von den Primidealen $\mathfrak{p}$ von R. Im Falle von Funktionenkörpern über $\mathbb{Q}$ oder über Zahlkörpern, oder wenn im Falle globaler Funktionenkörper die Charakteristik des endlichen Körpers K größer ist als der Grad der Erweiterung $n = [A : F]$, läßt sich auf $\mathfrak{m} = \prod_{i=1}^{k} g_i K[t]$ immer Algorithmus 6.16 anwenden.

Ist A ein globaler Funktionenkörper, so kann man auch ohne quadratfreie Faktorisierung der Diskriminante mit Hilfe des in Abschnitt 6.2.1 entwickelten Verfahrens das $\mathrm{disc}(\Lambda)$-Radikal berechnen. Beispiele zur Berechnung von Maximalordnungen in Funktionenkörpern findet man in Abschnitt 7.2.2.

6.4 Trager/Bradford

Nach [Bra88, Sect. 7.4, S. 7.8] schlägt Trager vor, an Stelle des $\mathfrak{p}$-Radikals bei der Berechnung von $\mathfrak{p}$-maximalen Ordnungen in algebraischen Zahlkörpern Potenzen des $\mathfrak{p}$-Radikals zu verwenden. Es werden in [Bra88, Sect. 7.4, S. 7.8] auch einige Beispiele angegeben, in denen der Index $\left(\mathcal{O}_l\left(\sqrt{\mathfrak{p}\Lambda}^k\right) : \Lambda\right)$ größer ist als der Index $\left(\mathcal{O}_l\left(\sqrt{\mathfrak{p}\Lambda}\right) : \Lambda\right)$. Diese Idee läßt sich auf die Berechnung von $\mathfrak{m}$-hereditären Ordnungen übertragen. Es sei $\{0\} \subset \mathfrak{m} \subset R$ ein Ideal und Λ eine R-Ordnung.

(6.21) **Proposition** *Es seien $\mathfrak{a}, \mathfrak{b}$ zwei zweiseitige Ideale der Ordnung Λ, dann gelten $\mathcal{O}_l(\mathfrak{b}) \subseteq \mathcal{O}_l(\mathfrak{b}\mathfrak{a})$ und $\mathcal{O}_r(\mathfrak{b}) \subseteq \mathcal{O}_r(\mathfrak{a}\mathfrak{b})$.*

Beweis: Es gilt $x \in \mathcal{O}_l(\mathfrak{b}) \Leftrightarrow x\mathfrak{b} \subseteq \mathfrak{b} \Rightarrow x\mathfrak{b}\mathfrak{a} \subseteq \mathfrak{b}\mathfrak{a} \Leftrightarrow x \in \mathcal{O}_l(\mathfrak{b}\mathfrak{a})$. Ebenso zeigt man auch die zweite Aussage. □

(6.22) **Korollar** *Für $k > 0$ gilt sowohl $\mathcal{O}_l(\sqrt{\mathfrak{m}\Lambda}) \subseteq \mathcal{O}_l\left(\sqrt{\mathfrak{m}\Lambda}^k\right)$ als auch $\mathcal{O}_r(\sqrt{\mathfrak{m}\Lambda}) \subseteq \mathcal{O}_r\left(\sqrt{\mathfrak{m}\Lambda}^k\right)$.*

Man kann also zur Berechnung einer $\mathfrak{m}$-hereditären Ordnung an Stelle von $\sqrt{\mathfrak{m}\Lambda}$ auch jede Potenz $\sqrt{\mathfrak{m}\Lambda}^k$ verwenden und die resultierende Links- bzw. Rechts-Ordnung ist auf jeden Fall nicht kleiner. Ein größerer Index ist aber auch nicht garantiert, wie die Beispiele für algebraische Zahlkörper in [Bra88, Sect. 7.4, S. 7.8] belegen.

Es sei $\mathfrak{p}$ ein Primideal von R, und $\mathfrak{P}_1, \ldots, \mathfrak{P}_s$ seien die Primideale von Λ, die $\mathfrak{p}$ enthalten. Ist die Algebra A kommutativ, so sieht man sofort, daß $\mathfrak{P}_1, \ldots, \mathfrak{P}_s$ invertierbar sind, genau dann, wenn auch $\left(\prod_{i=1}^{k} \mathfrak{P}_i\right)^k$ invertierbar ist.

(6.23) **Bemerkung** *Obwohl $\sqrt{\mathfrak{m}\Lambda}^n \subseteq \left(\prod_{\mathfrak{m}\subseteq\mathfrak{p}} \mathfrak{p}\right)\Lambda$, wobei $\mathfrak{p}$ Primideale von R seien, vgl. Proposition 6.12, muß man durch $\mathcal{O}_l\left(\left(\prod_{\mathfrak{m}\subseteq\mathfrak{p}} \mathfrak{p}\right)\Lambda\right)$ keine größere Ordnung erhalten als Λ, auch wenn Λ nicht $\mathfrak{m}$-hereditär ist.*

Im allgemeinen gilt $\sqrt{\mathfrak{m}\Lambda}^n \subset \left(\prod_{\mathfrak{m}\subseteq\mathfrak{p}} \mathfrak{p}\right)\Lambda$ und $\left(\prod_{\mathfrak{m}\subseteq\mathfrak{p}} \mathfrak{p}\right)\Lambda$ läßt sich nicht in Primideale von Λ faktorisieren, vgl. Korollar 2.51 und Bemerkung 3.15. Sollte doch „=“ gelten, so kann man natürlich auch mit $\left(\prod_{\mathfrak{m}\subseteq\mathfrak{p}} \mathfrak{p}\right)\Lambda$ an Stelle des $\mathfrak{m}$-Radikals rechnen, und sich damit viel Arbeit ersparen.

Kapitel 7
Praxis und Beispiele

Zum Abschluß werden in diesem Kapitel noch ein paar Bemerkung zu der Implementierung der Verfahren aus dieser Arbeit und illustrative Beispiele für die beschriebenen Algorithmen gegeben.

7.1 Implementierung in KASH

Der in den Abschnitten 6.3.1 und 6.3.2 beschriebene Algorithmus zur Berechnung der $\mathfrak{m}$-Spur-Radikale bzw. der $\mathfrak{m}$-Radikale in algebraischen Zahlkörpern und Funktionenkörpern und die damit verbundenen Verfahren zur Berechnung von Maximalordnungen, sind in dem Computeralgebra-System KASH [DFK+97] implementiert.

Besonders die Verfahren für die algebraischen Zahlkörper werden häufig benutzt, wenn man die Körperdiskriminante vorher schon kennt. Die Beispiele in Abschnitt 7.2.1 belegen das günstige Verhalten. An dieser Stelle möchte ich Claus Fieker und Jürgen Klüners meinen Dank aussprechen für die Hilfe bei der Implementierung dieser Verfahren und die Beispiele, die sie mir zur Verfügung gestellt haben.

Im Bereich der kommutativen Erweiterungen von Dedekindringen sind auch schon einige Teile in KASH programmiert. Da derzeit noch keine entsprechende Generik für allgemeine Dedekindringe existiert (siehe weiter unten) beschränken sich die implementierten Algorithmen auf die Lokalisierungen, vgl. Abschnitt 3.6 und Bemerkung 4.19. Die Arbeiten in Lokalisierungen ermöglichen es, herkömmliche Hermite-Normal-Formen über Hauptidealringen an Stelle von Dedekindringen zu verwenden. Außerdem ist auch die Idealarithmetik um ein Vielfaches einfacher.

Da an Dedekindringen bisher nur die Ringe $\mathbb{Z}, \mathrm{Cl}(\mathbb{Z}, K), \mathbb{F}_q[t], \mathbb{Q}[t]$ und $K[t]$, für Zahlkörper K, in KASH zur Verfügung stehen, werden damit keine neuen Gebiete erschlossen. Im Prinzip ist es aber möglich, ganz allgemein eine Ordnung über einem lokalisierten Dedekindring (mit entsprechender Information: Multiplikations-, Invertierungs-Funktion) in KASH anzulegen, und dann die maximale Ordnung zu berechnen.

Um den ganz allgemeinen Fall zu implementieren, also über einem allgemeinen Dedekindring zu arbeiten, muß neben der Struktur für nicht-

kommutative Algebren vor allem die Generik für die Dedekindringe verallgemeinert und implementiert werden. Dieser Teil von KASH ist dem Computeralgebra-System Magma [BCP97] entnommen, mit dem seit vielen Jahren eine Kooperation besteht. Die Generik erlaubt den Zugriff auf die Arithmetik-Funktionen sowohl für Elemente des Dedekindringes als auch für gebrochene Ideale des Dedekindringes.

Bisher ist in KASH bzw. Magma nur eines von beiden möglich, entweder Arithmetik mit Elementen oder Arithmetik mit gebrochenen Idealen. Insbesondere die Implementierung einer allgemeinen Hermite-Normal-Form (Theorem 1.15) über Dedekindringen erfordert aber, daß sowohl Arithmetik mit Elementen als auch mit gebrochenen Idealen (Koeffizientenidealen) zur gleichen Zeit zur Verfügung stehen. Daneben werden auch noch spezielle Funktionen benötigt, die sowohl mit Elementen als auch mit Idealen arbeiten, zum Beispiel eine Funktion, die testet, ob eine Element in einem Ideal enthalten ist.

Diese fehlende Generik soll aber in den nächsten Jahren entwickelt und implementiert werden, so daß danach mit der Programmierung der in dieser Arbeit beschriebenen allgemeinen Verfahren zur Berechnung von Maximalordnungen bzw. hereditären Ordnungen über Dedekindringen begonnen werden kann.

7.2 Beispiele

Alle Beispiele wurden auf einem Intel Pentium III (600MHz, 512MB RAM) unter Linux 2.2.13-SMP mit KASH Version 2.2 gerechnet.

7.2.1 Algebraische Zahlkörper

Absolute Erweiterungen 1

Die folgenden Polynome sind [KM00a] und [KM00b] entnommen. Durch sie werden spezielle vorgegebene Galois-Gruppen erreicht. Die Konstruktion des Polynoms erlaubt es auch gleich die Körperdiskriminante des Zahlkörpers mit anzugeben, der von dem Polynom erzeugt wird, so daß sie sich für die Anwendung der Ideen aus Abschnitt 6.3.1 gut eignen. Zur Demonstration sind die folgenden Polynome von Grad 14 und 15 mit den Galois-Gruppen 14T22 (die 22. Gruppe vom Grad 14), 14T23, 15T65 und 15T66 ausgewählt worden:

$f_1 := t^{14} - 63t^{12} - 9555t^{11} + 118671t^{10} - 708246t^9 - 17922660t^8 + 859373823t^7 + 2085856500t^6 - 117366985106t^5 - 335941176396t^4 + 4638317668005t^3 + 17926524826973t^2 + 74298465684445t + 91264986397629,$

$f_2 = t^{14} - 129864t^{12} - 517832t^{11} + 6567239322t^{10} + 33352434192t^9 - 166594899026864t^8 - 7529153154813 12t^7 + 22758917364590849 40t^6 + 77430780946040887 68t^5 - 16633213695413438344032t^4 - 39871919309692447523616t^3 + 60126791399546070679893112t^2 + 7784411853385272869875104 0t - 831734981995068547514587013 76,$

$f_3 = t^{14} + 7t^{13} - 140t^{12} - 931t^{11} + 7497t^{10} + 46186t^9 - 196273t^8 - 1074901t^7 + 2525502t^6 + 11656897t^5 - 12004657t^4 - 46585868t^3 - 17319029t^2 + 16247105t + 7630855,$

$f_4 = t^{14} - 266t^{12} + 27797t^{10} - 1440390t^8 + 27797t^7 + 38314374t^6 - 3697001t^5 - 48531540 4t^4 + 140486038t^3 + 2305248169t^2 - 1334617361t + 74413291,$

$f_5 = t^{14} - 14t^{12} + 77t^{10} - 210t^8 - 11t^7 + 294t^6 + 77t^5 - 196t^4 - 154t^3 + 49t^2 + 77t + 29,$

$f_6 = t^{14} - 56t^{12} + 245t^{11} + 2534t^{10} - 1372t^9 - 24528t^8 - 257782t^7 - 1470049t^6 + 1229802 t^5 + 12092913t^4 + 48481531t^3 + 478963261t^2 + 704643912t - 1494810659,$

$f_7 = t^{15} - 9358616t^{14} - 981801545363928t^{13} + 6132613307938894691999t^{12} + 2349656477641 2829419153938603 2t^{11} - 4872912333823537560361809995122043 96t^{10} - 1982121381294782068461392707625900354341008t^9 + 5093680464578715428636642615068984463691553718512t^8 - 1796382251442182084973410359337073117751008892067511360t^7 - 1624342531639838367959606954894776448845155527408053206753216t^6 + 5989557566959352268372244461433751019778863015041480859373423623 68t^5 + 1274556126756596685106567257384705051526981243567705247857922373407308 80t^4 - 5046130692638762567367572997781832935016185675384203103729306611900753065472 0t^3 - 1397964991904452724705356908128360083374719570322775353180279503186688568438657024t^2 + 9615259643343417540585286536609803298594495184709472097945339505129830079477624101191 68t - 1151455379287134460926605218857093250907196705907461675315578536501224426900715073792217 4976,$

$f_8 = t^{15} - 763627t^{14} - 7918503214887t^{13} - 1581904663932204363 5t^{12} - 134119227043006044 31206763t^{11} - 1984466180821028674417984036359t^{10} + 6985833031084493124518306103325292349t^9 + 7618002696501418814499247584924820359873665t^8 + 5358075653529910566901629262583658515856250754339t^7 + 2211671727427977558077897328424183557093938830835814495t^6 + 3034134508529149334322901385469158837311598110010080209547 63t^5 - 8627403092409100975136520515144936254604050842799615280111224738 5t^4 - 1356508258664056793590955617031769401263452525480356859394201412943858 5t^3 + 1547659401597267916564915173147304849198163743060134868979310156219644930515t^2 + 2845251922177398728125423160962475356458379581283768257940462018573091853193142 3t - 1034065306596988705801174192973952219371728777104203323360249438767943798293198985333,$

$f_9 = t^{15} - 9t^{14} - 777124356t^{13} - 1133827391276t^{12} + 2486674914459716 40t^{11} + 1982470037108913200760t^{10} - 2025167492138674323308966 4t^9 - 4775820969076609505231170148 16t^8 - 3308886107335264486810139708481072t^7 + 7821964130713177696750855493860013 92t^6 + 1367713846547631259756286359449137871626 88t^5 + 4953057527153646148002049060206164940625342 08t^4 - 2654636123517266162930575109745213496431971332096t^3 - 2669084947908663894975022618997030481566144542047283 2t^2 - 8476288755275455192793686564658325924269703449220811161 6t - 1024871671448323058965788498735385810803135249473163217674 24,$

$f_{10} = t^{15} - 3t^{14} - 687858797t^{13} - 2293640100713t^{12} + 113089731329026272t^{11} + 107773$
$7915724143112520t^{10} + 4942821089093099455184 0t^{9} - 1089000551515278031049516387 04$
$t^{8} - 1112508997817381234277823383171904t^{7} - 3424789921144574753049302371033829 31$
$2t^{6} + 3426104731698449005713692551235426486963 2t^{5} + 4697795186001728662998212940$
$669900884858032 64t^{4} + 2857336113050234752843481877396574445745460390912t^{3} + 9643$
$894366398012083167128665485160407030639351820288t^{2} + 1615592857741185517006433 1$
$707805843364634285522479439872t + 9745261198924540463184999279016505232539165 28$
$7580656586752,$
$f_{11} = t^{15} + 14t^{14} - 490102048t^{13} - 1443619696925t^{12} + 73076305015275276t^{11} + 4242972$
$85981352343828t^{10} - 6885611391117763548878208t^{9} - 1358172348361970327660547927 04$
$t^{8} - 1303133741618662827446853858425536t^{7} - 7853564823768301122889431429746549 95$
$2t^{6} - 2585649065201829351280521898820830968422 4t^{5} - 1366829824723969519237021739$
$00348413433579 52t^{4} + 2385728381875214528139975054345792075654999726 08t^{3} + 105220$
$176794285210009338877451600486826617409532006 4t^{2} + 2247229991592507744775455354$
$460577271500596394764492800t + 2214207762197676928867617302556145208714561573 82$
$7407908864,$
$f_{12} = t^{15} + 4t^{14} - 490102100t^{13} - 2271033227529t^{12} + 76744427566459970t^{11} + 6957085$
$38380570693696t^{10} - 5762533832169356285480188t^{9} - 1562367358389791878664739314 22$
$t^{8} - 1513319384516363752951684915149615t^{7} - 8626371994702576396082306373427394 82$
$4t^{6} - 2644380260897189507096728070029626530312 8t^{5} + 4957564389432783841054501927$
$3243800519586 07t^{4} + 4425569488457103626487259086529732643868467924 68t^{3} + 1673268$
$885383135576744422820876384207378556166859276t^{2} + 2524020170959396645044119777 3$
$577104166900083689568587 52t + 1364156404098579750286880766110742909935409399055$
473111056 und
$f_{13} = t^{15} - 114t^{14} + 282185319t^{13} + 1247857228852t^{12} - 35114805704965233t^{11} - 141524$
$337796433387826t^{10} + 2604584980442264028744009t^{9} + 1415394893213291827298415038 4$
$t^{8} - 1782730772483533699413276284795 52t^{7} - 1142953506821390914419260564494304768$
$t^{6} + 1597506914221127696313459949501499063961 6t^{5} + 3351668443830308801821730825 3$
$251277376159744t^{4} - 6175897771082037162323963724536193095544712560 64t^{3} - 3975614$
$124450669195454617623548846315018061748633 60t^{2} + 2266657182908547570648245464 21$
$519235780204710162818662 4t - 1302222456532760256406916223259306960560 5616574287778$
$14196224.$

In Tabelle 7.1 sind die Polynome, die Körperdiskriminante, die Dezimalstellen der Körperdiskriminante, die Zeit (t_1) zur Berechnung der Maximalordnung mit dem in Abschnitt 6.3.1 beschriebenen Verfahren, die Galois-Gruppe des Polynoms, die Dezimalstellen der Polynomdiskriminante, die Zeit (t_2) zur Faktorisierung der Polynomdiskriminante und die Zeit (t_3) zur Berechnung der Maximalordnung mit dem herkömmlichen Algorithmus (in diesem Fall der Round 4 Algorithmus, vgl. [Bai96]). Dabei wurden die folgenden Primzahlen verwendet:
$p_1 = 99896563575189398407775205343 7471,$

Tabelle 7.1: Algebraische Zahlkörper 1

f	$\mathrm{disc}(\mathbb{Q}[t]/f\mathbb{Q}[t])$	$\log_{10}(\mathrm{disc}(\mathbb{Q}[t]/f\mathbb{Q}[t]))$	t_1
$\mathrm{Gal}(f)$	$\log_{10}(\mathrm{disc}(f))$	t_2	t_3
f_1	$2^8 3^{16} 5^{10} 7^{24} 59^6$	47.94	2 sec
14T22	216.87	16 sec	18 sec
f_2	$2^{36} 3^{16} 7^{18} 4145023^6$	73.39	4 sec
14T22	376.25	> 60 min	> 60 min
f_3	$2^{12} 3^6 5^{10} 7^{14} 11^6$	31.54	2.20 sec
14T23	108.99	0.02 sec	0.35 sec
f_4	$3^6 5^{10} 7^{20} 19^{12}$	42.10	2.18 sec
14T23	129.64	0.02 sec	0.75 sec
f_5	$5^{10} 7^{14} 11^6$	25.07	2.26 sec
14T23	25.07	0.00 sec	0.02 sec
f_6	$7^{24} 13^{12}$	33.65	1.23 sec
14T23	139.28	17.00 sec	17.00 sec
f_7	$17^4 19^7 103^7 16857391^4 p_1^4$	188.87	69 sec
15T65	1388.40	> 60 min	> 60 min
f_8	$2^{10} 13^8 37^{11} 7951^4 p_2^4$	162.35	27 sec
15T65	1251.63	> 60 min	> 60 min
f_9	$-2^{32} 3^{20} 31^4 p_3^4$	122.48	11 sec
15T65	855.83	> 60 min	> 60 min
f_{10}	$19^5 103^5 p_4^4$	118.01	12 sec
15T66	843.72	> 60 min	> 60 min
f_{11}	$-3^4 331^5 p_5^4 p_6^4 p_7^4$	118.26	11 sec
15T66	826.38	> 60 min	> 60 min
f_{12}	$-3^4 331^5 p_5^4 p_6^4 p_7^4$	118.26	12 sec
15T66	836.35	> 60 min	> 60 min
f_{13}	$-2^{32} 3^{20} p_8^4 p_9^4$	120.82	9.63 sec
15T66	846.59	> 60 min	> 60 min

$p_2 = 24764267354322727267344323198011$,
$p_3 = 21559057393020528603666631$, $p_4 = 24423540709476440647407001$,
$p_5 = 2791121$, $p_6 = 36793741$, $p_7 = 843230867441$,
$p_8 = 3377890562461$, $p_9 = 7623585272461$.

Absolute Erweiterungen 2

Jetzt werden, wie schon in Abschnitt 6.3.1 angedeutet, die Polynome aus [GP97] verwendet, um algebraische Zahlkörper zu erzeugen. Es sei $f_n = t^5 + n^2t^4 - (2n^3 + 6n^2 + 10n + 10)t^3 + (n^4 + 5n^3 + 11n^2 + 15n + 5)t^2 + (n^3 + 4n^2 + 10n + 10)t + 1$ für jedes $n \in \mathbb{Z}$. Die Zahlkörper $K_n = \mathbb{Q}[t]/f_n\mathbb{Q}[t]$ haben nur für $n = -1, -2$ Potenzganzheitsbasen.

Weiterhin seien $m_n := n^4+5n^3+15n^2+25n+25$ und $d_n := n^3+5n^2+10n+7$. Nach [GP97, Lem. 2] ist die Diskriminante von K_n im Falle von $p^2 \not| m_n$ für jede Primzahl $p \neq 5$ gerade m_n^4 und d_n der Index $(\mathrm{Cl}(\mathbb{Z}, K_n) : \mathbb{Z}[t]/f_n\mathbb{Z}[t])$.

$d_n^{>5}$ sei der Teil des Index d_n, in dem die Primfaktoren $2, 3, 5$ gestrichen sind, für $d_n = 2^{\hat{e}_2}3^{\hat{e}_3}5^{\hat{e}_5}\prod_{i=1}^{k} p_i^{e_i}$ mit den Primzahlen $p_i > 5$ ist $d_n^{>5} = \prod_{i=1}^{k} p_i^{e_i}$. Für $-10000 \leq n \leq 10000$ ist mit KASH jeweils $\mathcal{O}_l\left(\sqrt{d_n^{>5}(\mathbb{Z}[t]/f_n\mathbb{Z}[t])}\right)$ berechnet worden. Die Primzahlen $2, 3, 5 \leq [K_n : \mathbb{Q}]$ werden separat behandelt.

Man stellt fest, daß $\mathcal{O}_l\left(\sqrt{d_n^{>5}(\mathbb{Z}[t]/f_n\mathbb{Z}[t])}\right)$ für alle Werte von n bereits $d_n^{>5}$-maximal ist. Es genügt also ein einziger „Spur-Radikal-Links-Ordnungs-Schritt“ zur Berechnung der $d_n^{>5}$-Maximalordnung, obwohl die Gleichungsordnung in allen Fällen (bis auf $n = -1, -2$, vgl. [GP97, Rem. S. 1696]) nicht maximal ist und der Index $d_n^{>5}$ in etwa 4% der Fälle nicht quadratfrei ist. Die Voraussetzung von [GP97, Lem. 2] ist in 4% der Fälle nicht erfüllt.

Die Schranken könnten auch noch sehr viel weiter nach unten beziehungsweise nach oben verlegt werden, die Berechnung eines „Spur-Radikal-Links-Ordnungs-Schritts“ dauerte im Schnitt eine halbe Sekunde.

7.2.2 Algebraische Funktionenkörper

Für algebraische Funktionenkörper kann eine quadratfreie Faktorisierung der Diskriminante sehr effizient berechnet werden [Zip93, Chpt. 18, S. 293]. Allerdings bereitet die Arithmetik mit Matrizen über $K[t]$ für $K = \mathbb{F}_q, K = \mathbb{Q}$ oder algebraische Zahlkörper K noch erhebliche Probleme. Die kritischen Funktionen sind hier die Hermite-Normal-Form und das Invertieren von Matrizen. Ist $g \in K[t]$ ein Erzeuger des Ideals $\mathfrak{m}$, dann wächst die Laufzeit des Algorithmus zur Berechnung eine $\mathfrak{m}$-maximalen Ordnung mit dem Grad des Polynoms g.

Die folgenden Beispiele demonstrieren aber, daß das Verfahren aus Abschnitt 6.3.2 bei kleinen Graden durchaus anwendbar ist. Für große Grade muß die Arithmetik mit Matrizen über $K[t]$ in dem Computeralgebra-System KASH bzw. Magma noch verbessert werden.

Globale Funktionenkörper

In Tabelle 7.2 werden durchschnittliche Laufzeiten für zufällige Beispiele angegeben. Als Grundkörper ist $K = \mathbb{F}_q$ vorgegeben, das erzeugende Polynom ist jeweils von der Form $f = y^d - \alpha^3\beta^3$, wobei $\alpha, \beta \in K[t]$ zufällig gewählt sind mit $\deg(\alpha) = \deg(\beta) = 3$. Das Polynom $f \in K(t)[y]$ erzeugt dann den globalen Funktionenkörper $A = F[y]/fF[y]$ über dem Körper $F = \mathbb{F}_q(t)$. Durch diese spezielle Wahl der Polynome f erhält man mehrere kubische Diskriminantenteiler.

Es wurden jeweils 100 Beispiele gerechnet. t_1 gibt die durchschnittliche Zeit für den herkömmlichen *Round 2 Algorithmus* (vollständige Faktorisierung der Diskriminante) und t_2 die durchschnittliche Zeit für den *Round 2 Algorithmus*, der nur die quadratfreie Faktorisierung der Diskriminante nutzt, an.

An Tabelle 7.2 sieht man, daß bei kleinen Beispielen ($d = 2$) die Verwendung der nur quadratfrei faktorisierten Diskriminante trotz der noch nicht verbesserten Arithmetik für Matrizen über $\mathbb{F}_q[t]$ immer schneller ist. Dies begründet die Hoffnung, daß durch eine Verbesserung der Matrix-Arithmetik auch für die größeren Beispiele das Verfahren aus Abschnitt 6.3.2 Anwendung finden wird.

Funktionenkörper über algebraischen Zahlkörpern

Die Beispiele für Funktionenkörper über algebraischen Zahlkörpern orientieren sich an denen für globale Funktionenkörper. Allerdings muß die Diskriminante (Grad des Polynoms, das die Diskriminante erzeugt) hier noch einmal deutlich kleiner sein.

In Tabelle 7.3 findet man die folgenden Daten: Der Zahlkörper ist $K = \mathbb{Q}(\sqrt[r]{s})$, die Funktionenkörper werden erzeugt von dem Polynom $f = y^2 - \alpha^3\beta^3$, wobei $\alpha, \beta \in K[t]$ zufällig gewählte lineare Polynome sind. Das Polynom $f \in K(t)[y]$ erzeugt dann den algebraischen Funktionenkörper $A = F[y]/fF[y]$ über dem Körper $F = K(t)$. Wie oben ist t_1 die durchschnittliche Zeit für den herkömmlichen *Round 2 Algorithmus* und t_2 die durchschnittliche Zeit für den *Round 2 Algorithmus*, der nur die quadratfrei faktorisierte Diskriminante nutzt. Es wurden jeweils 100 zufällige Beispiele gerechnet.

Tabelle 7.2: Globale Funktionenkörper

q	d	t_1	t_2	d	t_1	t_2
11^2	2	8.9 msec	2.9 msec	4	36.3 msec	59.2 msec
11^2	6	131.6 msec	713.2 msec	8	279.1 msec	4665.6 msec
13^2	2	8.7 msec	3.6 msec	4	38.7 msec	44.5 msec
13^2	6	133.3 msec	653.4 msec	8	284.5 msec	5578.4 msec
17^2	2	9.1 msec	2.6 msec	4	36.4 msec	76.6 msec
17^2	6	128.6 msec	965.1 msec	8	275.7 msec	6127.7 msec
19^2	2	8.2 msec	3.9 msec	4	37.4 msec	65.7 msec
19^2	6	140.8 msec	957.3 msec	8	283.7 msec	2592.4 msec
23^2	2	8.0 msec	3.8 msec	4	36.7 msec	76.2 msec
23^2	6	136.6 msec	962.7 msec	8	288.0 msec	6175.0 msec
29^2	2	9.7 msec	3.1 msec	4	38.2 msec	77.0 msec
29^2	6	138.4 msec	880.4 msec	8	298.8 msec	5876.2 msec
31^2	2	9.2 msec	3.6 msec	4	40.3 msec	77.5 msec
31^2	6	183.9 msec	663.6 msec	8	319.2 msec	6464.4 msec
37^2	2	10.0 msec	3.3 msec	4	38.4 msec	66.7 msec
37^2	6	148.5 msec	1078.2 msec	8	303.1 msec	6692.9 msec
41^2	2	9.8 msec	2.8 msec	4	39.0 msec	76.3 msec
41^2	6	145.9 msec	1061.1 msec	8	298.3 msec	6746.7 msec

Tabelle 7.3: Funktionenkörper über Zahlkörpern

r	s	t_1	t_2	s	t_1	t_2
2	2	34.0 msec	742.2 msec	-2	33.5 msec	951.3 msec
3	2	43.6 msec	3377.7 msec	-2	43.5 msec	3347.4 msec
2	5	38.4 msec	822.7 msec	-5	33.7 msec	1113.2 msec
3	5	44.8 msec	4209.2 msec	-5	46.3 msec	3952.1 msec
2	7	34.7 msec	1097.9 msec	-7	39.2 msec	887.9 msec
3	7	45.8 msec	4448.6 msec	-7	46.6 msec	4512.1 msec
2	11	38.5 msec	1227.9 msec	-11	38.8 msec	1150.4 msec
3	11	78.1 msec	4941.4 msec	-11	46.9 msec	5196.7 msec
2	13	38.4 msec	937.8 msec	-13	36.5 msec	1428.0 msec
3	13	46.9 msec	5130.9 msec	-13	48.8 msec	5265.7 msec

Um die großen Probleme mit der Arithmetik über $K[t]$ für $K = \mathbb{Q}$ oder Zahlkörper K zu dokumentieren, wird hier noch ein besonders großes Beispiel angeführt. Das Polynom

$f := y^{10}+(-20t^4+20t^3-20t^2+20t-20)y^8+(70t^8-140t^7+310t^6-480t^5+600t^4-530t^3+460t^2-290t+120)y^6+(-100t^{12}+300t^{11}-600t^{10}+1000t^9-1625t^8+2675t^7-4150t^6+4800t^5-4625t^4+4000t^3-2850t^2+1175t-225)y^4+(65t^{16}-260t^{15}+350t^{14}-100t^{13}-525t^{12}+2470t^{11}-4930t^{10}+3950t^9+1550t^8-7800t^7+12745t^6-15830t^5+14850t^4-9600t^3+3975t^2-910t+90)y^2-16t^{20}+80t^{19}-40t^{18}-440t^{17}+895t^{16}+101t^{15}-2285t^{14}+2605t^{13}+55t^{12}-2590t^{11}+3124t^{10}-3060t^9+2080t^8+1180t^7-4115t^6+3631t^5-1320t^4+60t^3+60t^2-5t-1$

erzeugt den Funktionenkörper $A = \mathbb{Q}(t)[y]/f\mathbb{Q}(t)[y]$. In der quadratfreien Faktorisierung der Diskriminante taucht ein Faktor von Grad 26 auf. Die Berechnung des zugehörigen $\mathfrak{m}$-Radikals benötigt 694 Sekunden und bei der Berechnung der Links-Ordnung des $\mathfrak{m}$-Radikals, genauer bei der Invertierung einer Matrix über $\mathbb{Q}[t]$, stürzt das System ab, da der Arbeitsspeicher (512 MB) nicht ausreicht.

Notation

In der vorliegenden Arbeit werden die folgenden Symbole und Notationen verwendet, in der rechten Spalte steht die Seite des ersten Auftretens.

$M \subseteq N$	$x \in M \Rightarrow x \in N$, für beliebige Mengen M, N	
$M \subset N$	$M \subseteq N$ und $M \neq N$	
$\mathbb{F}_q$	endlicher Körper mit q Elementen	3
R	ein Dedekindring	1
F	Quotientenkörper von R	1
K, L	Körper L/K	2
$[L : K]$	Grad der Körpererweiterung L/K	
A	eine separable F-Algebra der Dimension n	6
$[A : F]$	Dimension der F-Algebra A	1
n	Dimension der F-Algebra A	6
$J(A), J(S)$	das Jacobson-Radikal von A bzw. S für einen beliebigen Ring S.	1
$\mathrm{Cl}(R, A)$	ganzer Abschluß von R in A	3
$\vec{x}$	Koeffizientenvektor von $x \in A$	12
$M_{\cdot,j}, M_{k,\cdot}$	j-te Spalte bzw. k-te Zeile der Matrix M	14
$\mathrm{P}_{A/K}(x), \mathrm{P}(x)$	charakteristisches Polynom von $x \in A$	2
$\mathrm{T}_{A/K}(x), \mathrm{T}(x)$	Spur von $x \in A$	2
$\mathrm{Pr}_{A/K}(x), \mathrm{Pr}(x)$	reduziertes charakteristisches Polynom von $x \in A$	2
$\mathrm{Tr}_{A/K}(x), \mathrm{Tr}(x)$	reduzierte Spur von $x \in A$	2
$\mathfrak{a}, \mathfrak{b}$, usw.	Ideale oder R-Gitter	5
V	ein F-Vektorraum	5, 8
$[V : F]$	Dimension des F-Vektorraums V	
$\mathcal{M}$	R-Gitter in dem F-Vektorraum V	8
$\mathfrak{a}_x$	Koeffizientenideal zu $x \in F\mathcal{M}$ und dem R-Gitter $\mathcal{M}$, $\{\alpha \in F \mid \alpha x \in \mathcal{M}\}$	10
Λ	R-Gitter oder R-Ordnungen in A	3, 5

Notation

$(\mathfrak{a}/\mathfrak{b})$	Quotient von zwei R-Gittern oder Idealen, $\{x \in A \mid x\mathfrak{b} \subseteq \mathfrak{a}\}$	13
$(\mathfrak{b}\backslash\mathfrak{a})$	wie oben, aber $\{x \in A \mid \mathfrak{b}x \subseteq \mathfrak{a}\}$	13
$\mathcal{O}_l(\mathfrak{a})$	Links-Ordnung des R-Gitters oder Ideals $\mathfrak{a}$, $(\mathfrak{a}/\mathfrak{a})$	5
$\mathcal{O}_r(\mathfrak{a})$	Rechts-Ordnung des R-Gitters oder Ideals $\mathfrak{a}$, $(\mathfrak{a}\backslash\mathfrak{a})$	5
$Id(\mathfrak{a})$	Idealisator des zweiseitigen Ideals $\mathfrak{a}$, $\mathcal{O}_l(\mathfrak{a}) \cap \mathcal{O}_r(\mathfrak{a})$	39
$\mathfrak{a}^{-1}$	Inverses R-Gitter von $\mathfrak{a}$, $\{x \in A \mid \mathfrak{a}x\mathfrak{a} \subseteq \mathfrak{a}\}$	21
$[\mathfrak{a} : x]$	$\{y \in \Lambda \mid yx \in \mathfrak{a}\}$	50
$\mathrm{disc}(\Lambda)$	Diskriminante des vollen R-Gitters oder der R-Ordnung Λ	27
$\mathrm{disc}_r(\Lambda)$	reduzierte Diskriminante des vollen R-Gitters oder der R-Ordnung Λ	28
$\mathrm{ord}(\Lambda^{\mathrm{tor}})$	Ordnungsideal des R-Torsionsmoduls Λ^{tor}	28
$(\Lambda' : \Lambda)$	Index von R-Gittern oder R-Ordnungen	28
$\mathrm{N}(\mathfrak{a})$	Norm des Ideals $\mathfrak{a}$ von Λ, $\mathrm{ord}(\Lambda/\mathfrak{a})$	53
$\Lambda^{\perp}$	duales R-Gitter zu Λ	28
$\Lambda^{(\max)}$	maximale Ordnung	3
$\Lambda^{(\mathfrak{p})}$	$\mathfrak{p}$-maximale Zwischenordnung $\{x \in \Lambda^{(\max)} \mid \mathfrak{p}^{\nu}x \subseteq \Lambda,\ \text{für ein } \nu \geq 0\}$ zu Λ und $\Lambda^{(\max)}$	28
$\Lambda^{(\mathrm{her})}$	hereditäre Ordnung	38
$\Lambda^{(\mathfrak{p}\text{-her})}$	$\mathfrak{p}$-hereditäre Ordnung	41
$\sqrt{\mathfrak{p}\Lambda}, \sqrt{\mathfrak{m}\Lambda}$	$\mathfrak{p}$-Radikal bzw. $\mathfrak{m}$-Radikal der Ordnung Λ	30, 56
$I^{(\mathrm{Spur})}_{\mathfrak{p},\Lambda}, I^{(\mathrm{Spur})}_{\mathfrak{n},\Lambda}$	$\mathfrak{p}$-Spur-Radikal, bzw. $\mathfrak{n}$-Spur-Radikal der Ordnung Λ, $\{a \in \Lambda \mid \mathrm{T}(xa) \in \mathfrak{n} \text{ für alle } x \in \Lambda\}$	47, 60
$R_{\mathfrak{p}}$	Lokalisierung von R an $\mathfrak{p}$	35
$\Lambda_{\mathfrak{p}}$	Lokalisierung der R-Ordnung oder des R-Gitters Λ an $\mathfrak{p}$	35
$\nu_{\mathfrak{p}}$	$\mathfrak{p}$-adische exponentielle Bewertung	39
$\hat{F}_{\mathfrak{p}}$	Vervollständigung von F bezüglich $\nu_{\mathfrak{p}}$	39
$\hat{R}_{\mathfrak{p}}$	Bewertungsring von $\hat{\nu}_{\mathfrak{p}}$	39
$\hat{A}_{\mathfrak{p}}$	Vervollständigung von A, $\hat{F}_{\mathfrak{p}} \otimes_F A$	39
$\hat{\Lambda}_{\mathfrak{p}}$	Vervollständigung von Λ, $\hat{R}_{\mathfrak{p}} \otimes_R \Lambda$	39

Literaturverzeichnis

[AG60] Maurice Auslander und Oscar Goldman. Maximal orders. *Transactions of the American Mathematical Society*, **97** (1960), 1–24.

[AHU74] Alfred V. Aho, John E. Hopcroft und Jeffrey D. Ullman. *The Design and Analysis of Computer Algorithms*. Addison-Wesley, Reading, Massachusetts, 1974.

[AM69] M. F. Atiyah und I. G. Macdonald. *Introduction to Commutative Algebra*. Addison-Wesley Series in Mathematics. Addison-Wesley Publishing Co., 1969.

[Art50] Emil Artin. Questions de base minimale dans la théorie des nombres algébriques. *Colloque international du CNRS*, (1950), 19–20. In [LT65], 229–231.

[Bac92] Paul Bachmann. *Analytische Zahlentheorie*. 1892.

[Bai96] Georg Baier. Zum Round-4-Algorithmus. Diplomarbeit, Technische Universität Berlin, 1996.

[BCP97] Wieb Bosma, John J. Cannon und Cathrine Playoust. The Magma algebra system I: The user language. *Journal of Symbolic Computation*, **24** (1997), 235–265.

[Ber27] William Edward Hodgson Berwick. *Integral Bases*, Band 22 aus *Cambridge Tracts in Mathematics and Mathematical Physics*. Cambridge University Press, 1927.

[BL] Johannes A. Buchmann und Hendrik W. Lenstra. Computing maximal orders and factoring over Zp. Preprint, published as [BL94].

[BL94] Johannes A. Buchmann und Hendrik W. Lenstra. Approximating rings of integers in number fields. *Journal de Theorie des Nombres de Bordeaux*, **6** (1994), 221–260.

[BN98] Johannes Buchmann und Stefan Neiss. Algorithms for linear algebra problems over principal ideal rings. Submitted to SIAM Journal of Computation, 1998.

Literaturverzeichnis

[Bö85] Rudolf Böffgen. Der Algorithmus von Ford/Zassenhaus zur Berechnung von Ganzheitsbasen in Polynomalgebren. Diplomarbeit, Universität des Saarlandes, Saarbrücken, 1985.

[Bou58] Nicolas Bourbaki. *Algèbre*, Band 2 aus *Éléments de Mathématique*. Hermann, Paris, 1958.

[Bou72] Nicolas Bourbaki. *Commutative Algebra*. Elements of Mathematics. Addison-Wesley, Reading, Massachusetts, 1972.

[BP91] Wieb Bosma und Michael E. Pohst. Computations with finitely generated modules over Dedekind domains. In Stephen M. Watt, Herausgeber, *Proceedings ISSAC'91*, Seiten 151–156, 1991.

[BR87] R. Böffgen und 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** (1987), 3–10.

[Bra88] Russel John Bradford. *On the Computation of Integral Bases*. Dissertation, University of Bath, 1988.

[Bru83] Lieven Le Bruyen. A note on maximal orders over Krull domains. *Journal of Pure and Applied Algebra*, **28** (1983), 241–248.

[BS96] Eric Bach und Jeffrey Shallit. *Efficient Algorithms*, Band 1 aus *Algorithmic Number Theory*. MIT Press, Camebridge–Massachusetts, 1996.

[CG00] David G. Cantor und Daniel M. Gordon. Factoring polymials over p-adic fields. In W. Bosma, Herausgeber, *Algorithmic Number Theory, ANTS IV*, Band 1838 aus *Lecture Notes in Computer Science*, Seiten 185–208 Springer-Verlag, 2000.

[Coh96a] Henri Cohen. *A Course in Computational Algebraic Number Theory*, Band 138 aus *Graduate Texts in Mathematics*. Springer-Verlag, Berlin–Heidelberg–New York, 3. Auflage, 1996.

[Coh96b] Henri Cohen. Hermite and Smith normal form algorithms over Dedekind domains. *Mathematics of Computation*, **65** (1996), 1681–1699.

[Coh00] Henri Cohen. *Advanced Topics in Computational Number Theory*, Band 193 aus *Graduate Texts in Mathematics*. Springer-Verlag, Berlin–Heidelberg–New York, 2000.

[CR62] Charles W. Curtis und Irving Reiner. *Representation Theory of Finite Groups and Associative Algebras*, Band 11 aus *Pure and Applied Mathematics*. Wiley (Interscience), New York–London, 1962.

[CR81] Charles W. Curtis und Irving Reiner. *Methods of Representation Theory with Applications to Finite Groups and Orders, Volume 1*. Wiley, New York, 1981.

[CR87] Charles W. Curtis und Irving Reiner. *Methods of Representation Theory with Applications to Finite Groups and Orders, Volume 2*. Wiley, New York, 1987.

[DdJGP99] Wolfram Decker, Theo de Jong, Gert-Martin Greuel und Gerhard Pfister. The normalization: A new algorithm, implementation and comparisons. In P. Dräxler, G. O. Michler und C. M. Ringel, Herausgeber, *Computational Methods for Representation of Groups and Algebras, Proceedings of the Euroconference in Essen, Germany, April 1–5 1997*, Band 173 aus *Progress in Mathematics*, Seiten 177–185, Basel–Boston–Berlin, 1999. Birkhäuser.

[Ded71] Richard Dedekind. *Über die Compositon der binären quadratischen Formen. Supplement X zu Peter Gustav Lejeune Dirichlet, Vorlesungen über Zahlentheorie*. Friedrich Vieweg und Sohn, Braunschweig, 2. Auflage, 1871.

[Deu68] Max Deuring. *Algebra*, Band 41 aus *Ergebnisse der Mathematik und ihrer Grenzgebiete*. Springer-Verlag, Berlin–Heidelberg–New York, 2. Auflage, 1968.

[DFK+97] Mario Daberkow, Claus Fieker, Jürgen Klüners, Michael E. Pohst, Katherine Roegner, Martin Schörnig und Klaus Wildanger. KANT V4. *Journal of Symbolic Computation*, **24** (1997), 267–283.

[Dic60] Leonard Eugene Dickson. *Algebras and their Arithmetic*. Dover Publications, New York, 1960.

[dJ98] Theo de Jong. An algorithm for computing the integral closure. *Journal of Symbolic Computation*, **26** (1998), 273–277.

[Ebe89] Wayne Eberly. *Computations for Algebras and Group Representations*. Dissertation, University of Toronto, 1989.

[Fie00] Claus Fieker. On the computation of HNF and SNF over Dedekind domains. Preprint, July 2000.

[FL93] David Ford und Pascal Letard. Implementing the round four maximal order algorithm. *Journal de Theorie des Nombres de Bordeaux*, **6** (1993), 39–80.

[For78] David Ford. *On the Construction of the Maximal Order in a Dedekind Domain.* Dissertation, Ohio State University, 1978.

[For87] David Ford. The construction of maximal orders over a Dedekind domain. *Journal of Symbolic Computation*, **4** (1987), 69–75.

[FPR00] David Ford, Sebastian Pauli und Xavier F. Roblot. A guide to polynomial factorization over Qp. CICMA Reports, March 2000.

[FR85] Katalin Friedl und Lajos Rónyai. Polynomial time solutions for some problems in computational algebra. In *Proceedings of the seventeenth annual ACM Symposium on Theory of Computing, 1985*, Seiten 153–162. ACM Press, 1985.

[Fri97] Carsten Friedrichs. Bestimmung relativer Ganzheitsbasen mit dem Round-2-Algorithmus. Diplomarbeit, Technische Universität Berlin, 1997.

[GBD+94] Al Geist, Adam Beguelin, Jack Dongarra, Weicheng Jiang, Robert Manchek und Viady Sunderam. *PVM: Parallel Virtual Machine, A Users' Guide and Tutorial for Networked Parallel Computing.* MIT Press, 1994. `http://www.epm.ornl.gov/pvm/pvm`.

[Gil72] Robert Gilmer. *Multiplicative Ideal Theory*, Band 12 aus *Pure and Applied Mathematics, A Series of Monographs and Textbooks.* Marcel Dekker, INC., 1972.

[Gol72] A. W. Goldie. Properties of the idealizer. In Robert Gordon, Herausgeber, *Proceedings of a Conference on Ring Theory, Park City, Utah, March 2–6 1971*, Seiten 161–169, New York–London, 1972. Academic Press.

[GP97] Istvan Gaál und Michael E. Pohst. Power integral bases in a parametric family of totally real cyclic quintics. *Mathematics of Computation*, **66** (1997), 1689–1696.

[Gre00] Gert Martin Greuel. Computer algebra and algebraic geometrie — Achievements and perspectives. *Journal of Symbolic Computation*, **30** (2000), 253–289.

[Gus81] William H. Gustafson. Remarks on the history and applications of integral representations. In *Integral Representations and Applications [Rog81]*, Seiten 1–36, 1981.

[Hal98] Emmanuel Hallouin. *Calcul de fermeture intégrale en dimension 1 et factorisation*. Dissertation, Université de Poitiers, 1998.

[Hal00] Emmanuel Hallouin. Computing local integral closures. Preprint, Submitted to Journal of Symbolic Computation, Mai 2000.

[Heß99] Florian Heß. *Zur Divisorenklassengruppenberechnung in globalen Funktionenkörpern*. Dissertation, Technische Universität Berlin, 1999.

[Hop98] Andreas Hoppe. *Normal forms over Dedekind domains, efficient implementation in the computer algebra system KANT*. Dissertation, Technische Universität Berlin, 1998.

[Jac71] Heinz Jacobinski. Two remarks about hereditary orders. *Proceedings of the American Mathematical Society*, **28** (1971), 1–8.

[Kant] Imanuel Kant. *Critique of pure reason*. Macmillan, London, 1929. Translation by Norman Kemp Smith. e-text by Stephen Palmquist (1985): `http://www.hkbu.edu.hk/~ppp/cpr/toc.html`.

[KM00a] Jürgen Klüners und Gunter Malle. A database for field extensions of the rationals. Preprint, 2000.

[KM00b] Jürgen Klüners und Gunter Malle. Explicit Galois realization of transitive groups of degree up to 15. To appear in Journal of Symbolic Computation, 2000.

[Knu77] Donald E. Knuth. *Fundamental Algorithms*, Band 1 aus *The Art of Computer Programming*. Addison-Wesley, Reading, Massachusetts, 1977.

[Lan78] Rudolf Land. Konstruktive Methoden zur Bestimmung von Maximalordnungen und Kroneckerklassen. Diplomarbeit, Universität zu Köln, 1978.

Literaturverzeichnis

[LM71] Max D. Larsen und Paul J. McCarthy. *Multiplicative Theory of Ideals*, Band 43 aus *Pure and Applied Mathematics, A Series of Monographs and Textbooks*. Academic Press, New York–London, 1971.

[Lor90] Falko Lorenz. *Einführung in die Algebra, Teil 2*. BI Wissenschaftsverlag, Mannheim–Wien–Zürich, 1990.

[Lor96] Falko Lorenz. *Einführung in die Algebra I*. Spektrum Akademischer Verlag, Heidelberg–Berlin–Oxford, 3. Auflage, 1996.

[LT65] Serge Lang und John T. Tate, Herausgeber. *The collected papers of Emil Artin*. Addison-Wesley, Reading, Massachusetts, 1965.

[Mey75] Kurt Meyberg. *Algebra Teil 1*. Carl Hanser Verlag, München–Wien, 1975.

[MN92] Jesús Montes und Enric Nart. On a theorem of Ore. *Journal of Algebra*, **146** (1992), 318–334.

[Mon99] Jesús Montes. *Polígonos de Newton de orden superior y aplicaciones aritméticas*. Dissertation, Universitat de Bercelona, 1999.

[MR87] J. C. McConnell und J. C. Robson. *Noncommutative Noetherian Rings*. Pure and Applied Mathematics. Wiley (Interscience), New York–London, 1987.

[Nar89] Wladislaw Narkiewicz. *Elementary and Analytic Theory of Algebraic Numbers*. Springer-Verlag, Berlin–Heidelberg–New York, 2. Auflage, 1989.

[Neb99] Gabriele Nebe. *Orthogonale Darstellungen endlicher Gruppen und Gruppenringe*. Habilitationsschrift, Rheinisch-Westfälische Technische Hochschule Aachen, 1999. Aachener Beiträge zur Mathematik 26, Verlag Mainz, Aachen.

[Neb00] Gabriele Nebe. eMail vom 14. August, 2000.

[Nei98] Stefan Neiss. Reducing ideal arithmetic to linear algebra problems. In J. P. Buhler, Herausgeber, *Algorithmic Number Theory, ANTS III*, Band 1423 aus *Lecture Notes in Computer Science*, Seiten 299–310. Springer-Verlag, 1998.

[Noe19] Emmy Noether. Die arithmetische Theorie der algebraischen Funktionen einer Veränderlichen, in ihrer Beziehung zu den übrigen Theorien und zu der Zahlkörpertheorie. *Jahresbericht der Deutschen Mathematiker-Vereinigung*, **28** (1919), 299–310.

[Nor63] D. G. Northcott. *Ideal Theory*, Band 42 aus *Cambridge Tracts in Mathematics and Mathematical Physics*. Cambridge University Press, 1963.

[Ogn94] Claudia Ognibeni. Zur Berechnung der Zerlegung von Indexteilern. Diplomarbeit, Heinrich-Heine-Universität Düsseldorf, 1994.

[OMe63] O.T. O'Meara. *Introduction to Quadratic Forms*, Band 117 aus *Die Grundlehren der Mathematischen Wissenschaften*. Springer-Verlag, Berlin–Göttingen–Heidelberg, 1963.

[Ore23] Öystein Ore. Zur Theorie der algebraischen Körper. *Acta Mathematica*, **44** (1923), 219–314.

[Ore25a] Öystein Ore. Bestimmung der Diskriminante algebraischer Körper. *Acta Mathematica*, **45** (1925), 303–344.

[Ore25b] Öystein Ore. Weitere Untersuchungen zur Theorie der algebraischen Körper. *Acta Mathematica*, **45** (1925), 145–160.

[Ore26a] Öystein Ore. Bemerkungen zur Theorie der Differente. *Mathematische Zeitschrift*, **25** (1926), 1–8.

[Ore26b] Öystein Ore. Existenzbeweise für algebraische Körper mit vorgeschriebenen Eigenschaften. *Mathematische Zeitschrift*, **25** (1926), 474–488.

[Ore27a] Öystein Ore. Über den Zusammenhang zwischen den definierenden Gleichungen und der Idealtheorie in algebraischen Körpern. (erste Mitteilung). *Mathematische Analen*, **96** (1927), 313–352.

[Ore27b] Öystein Ore. Über den Zusammenhang zwischen den definierenden Gleichungen und der Idealtheorie in algebraischen Körpern. (zweite Mitteilung). *Mathematische Analen*, **97** (1927), 569–598.

[Ore28] Öystein Ore. Newtonsche Polygone in der Theorie der algebraischen Körper. *Mathematische Analen*, **99** (1928), 84–117.

Literaturverzeichnis

[Par84] Richard A. Parker. The computer calculation of modular characters. (The meat-axe). In M. D. Atkinson, Herausgeber, *Computational group theory. Proceedings of the London Mathematical Society Symposium on Computational Group Theory (Durham, July 30 – August 9, 1982)*, Seiten 267–274. Academic Press, 1984.

[Pau00] Sebastian Pauli. Polynomial factorization over Qp. Preprint, Submitted to Journal of Symbolic Computation, October 2000.

[Pie82] Richard S. Pierce. *Associative Algebra*, Band 88 aus *Graduate Texts in Mathematics*. Springer-Verlag, Berlin–Heidelberg–New York, 1982.

[Poh91] Michael E. Pohst. A note on index divisors. In Attila Pethö, Michael E. Pohst, Hugh C. Williams und Horst G. Zimmer, Herausgeber, *Computational Number Theory, Proceedings of the Colloquium on Computational Number Theory, Kossuth Lajos University Debrecen, Hungary, September 4–9 1989*, Seiten 173–182, Berlin–New York, 1991. Walter de Gruyter.

[Poh93] Michael E. Pohst. *Computational Algebraic Number Theory*. Deutsche Mathematiker-Vereinigung: DMV-Seminar. Birkhäuser, Basel–Boston–Berlin, 1993.

[PZ89] Michael E. Pohst und Hans Zassenhaus. *Algorithmic Algebraic Number Theory*. Encyclopaedia of Mathematics and its Applications. Cambridge University Press, Cambridge, 1989. Extended Paperback Edition 1997.

[Rei75] Irving Reiner. *Maximal Orders*, Band 5 aus *London Mathematical Society Monographs*. Academic Press, London, 1975.

[RHD70] Klaus W. Roggenkamp und Verena Huber-Dyson. *Lattices over Orders I*, Band 115 aus *Lecture Notes in Mathematics*. Springer-Verlag, Berlin–Heidelberg–New York, 1970.

[Rob68] J. C. Robson. Non-commutative Dedekindrings. *Journal of Algebra*, **9** (1968), 249–265.

[Rog70] Klaus W. Roggenkamp. *Lattices over Orders II*, Band 142 aus *Lecture Notes in Mathematics*. Springer-Verlag, Berlin–Heidelberg–New York, 1970.

[Rog81] Klaus W. Roggenkamp, Herausgeber. *Integral Representations and Applications, Proceedings of a Conference, Oberwolfach, Germany, June 22–28, 1980*, Band 882 aus *Lecture Notes in Mathematics*, Berlin–Heidelberg–New York, 1981. Springer-Verlag.

[RR79] Irving Reiner und Klaus W. Roggenkamp. *Integral Representations*, Band 744 aus *Lecture Notes in Mathematics*. Springer-Verlag, Berlin–Heidelberg–New York, 1979.

[RR85] Irving Reiner und Klaus W. Roggenkamp, Herausgeber. *Orders and their Applications, Proceedings of a Conference, Oberwolfach, Germany, June 3–9, 1984*, Band 1142 aus *Lecture Notes in Mathematics*, Berlin–Heidelberg–New York, 1985. Springer-Verlag.

[San91] Jonathan W. Sands. Generalization of a theorem of Siegel. *Acta Arithmetica*, **58** (1991), 47–57.

[Sch96] Martin Schörnig. *Untersuchungen konstruktiver Probleme in globalen Körpern*. Dissertation, Technische Universität Berlin, 1996.

[Ull99] P. Ullrich. Die Entdeckung der Analogie zwischen Zahl- und Funktionenkörpern: der Ursprung der Dedekind-Ringe. *Jahresbericht der Deutschen Mathematiker-Vereinigung*, **101** (1999), 116–134.

[Vas76] Wolmer V. Vasconcelos. *The rings of dimension two*, Band 22 aus *Lecture Notes in Pure and Applied Mathematics*. Marcel Dekker, New York–Basel, 1976.

[Vas91] Wolmer V. Vasconcelos. Computing the integral closure of an affine domain. *Proceedings of the AMS*, **113** (1991), 633–638.

[vG81] Jan van Geel. *Places and Valuations in noncommutative Ring Theory*, Band 71 aus *Lecture Notes in Pure and Applied Mathematics*. Marcel Dekker, New York–Basel, 1981.

[Wei63] Edwin Weiss. *Algebraic Number Theory*. Chelsea Publishing, New York, 2. Auflage, 1963.

[Zas67] Hans Zassenhaus. Ein Algorithmus zur Berechnung einer Minimalbasis über gegebener Ordnung. In L. Collatz, G. Meinardus und H. Unger, Herausgeber, *Funktionalanalysis, Approximationstheorie, Numerische Mathematik, Oberwolfach, Germany, 1965*, Seiten 90–103, Basel, 1967. Birkhäuser.

[Zas72] Hans Zassenhaus. On the second round of the maximal order program. In S.K. Zaremba, Herausgeber, *Applications of Number Theory to Numerical Analysis, Proceedings of a Symposium in Montreal 1971*, Seiten 389–431, New York, 1972. Academic Press.

[Zas75] Hans Zassenhaus. On Hensel factorization II. In *Symposia Mathematica XV, Instituto di Alta Mathematica, 1973*, Seiten 499–513. Academic Press, 1975.

[Zip93] Richard Zippel. *Effective Polynomial Computation*. Kluwer Academic Publishers, Boston–Dordrecht–London, 1993.

[ZS58] Oscar Zariski und Pierre Samuel. *Commutative Algebra Volume 1*, Band 28 aus *Graduate Texts in Mathematics*. Springer-Verlag, New York–Heidelberg–Berlin, 1958.

Index

Zusammenfassung

R sei ein beliebiger Dedekindring mit Quotientenkörper $F = Q(R)$. In dieser Arbeit werden R-Ordnungen Λ in endlich dimensionalen separablen F-Algebren A betrachtet, wobei A nicht notwendig kommutativ ist.

Es werden (in der Dimension der F-Algebra A) polynomielle Verfahren zur Arithmetik (Summe, Schnitt, Produkt, Quotienten und Inverses) von Rechts-, Links- und zweiseitigen Idealen von Λ entwickelt. Nebenbei werden Analogien zu Ordnungen in globalen Körpern aufgezeigt, die auch zum Verständnis der arithmetischen Eigenschaften der Ideale in Ordnungen algebraischer Zahlkörpern beitragen.

Ähnlich wie in globalen Körpern interessiert man sich für die Berechnung einer Maximalordnung. Im Gegensatz zum kommutativen Fall, ist die Maximalordnung im allgemeinen nicht eindeutig. Zur Berechnung von Maximalordnungen in separablen Algebren wird der *Round 1 Algorithmus* von Zassenhaus verallgemeinert.

Der *Round 2 Algorithmus* von Zassenhaus nutzt aus, daß jede Maximalordnung *hereditär* ist, und berechnet erst eine hereditäre Ordnung $\Lambda^{(\mathrm{her})} \supseteq \Lambda$ und dann eine Maximalordnung $\Lambda^{(\max)} \supseteq \Lambda^{(\mathrm{her})}$. Wenn die Algebra kommutativ ist, so fällt die hereditäre Ordnung mit der Maximalordnung und mit dem ganzen Abschluß zusammen, so daß man den in globalen Körpern bekannten *Round 2 Algorithmus* erhält.

Ein Teilproblem des *Round 1* bzw. *Round 2 Algorithmus* ist, zu vorgegebenem Primideal $\mathfrak{p}$ von R, das sogenannte $\mathfrak{p}$-Radikal bzw. die maximalen Ideale von Λ zu konstruieren, die $\mathfrak{p}$ enthalten. Hierzu werden allgemeine Verfahren angegeben. Insbesondere wird die Verbindung zu dem Algorithmus von Buchmann-Cohen-Lenstra zur Faktorisierung von Indexteilern in algebraischen Zahlkörpern hergestellt. Als Anwendung wird gezeigt, wie man in (nicht notwendig maximalen) Ordnungen beliebige zweiseitige Ideale faktorisiert, wobei man im allgemeinen keine vollständige Faktorisierung in Primideale erhält.

Zum Abschluß werden noch einige Verbesserungen betrachtet. Die Verwendung des $\mathfrak{m}$-Radikals zur Berechnung hereditärer Ordnungen erlaubt zum Beispiel die Verwendung der nicht vollständig faktorisierten Diskriminante. Die Ausführungen zum $\mathfrak{m}$-Radikal stellen eine entscheidende Verallgemeinerung der Verfahren von Buchmann und Lenstra dar.

Illustrative Beispiele, die vor allem die Vorteile der Verwendung des $\mathfrak{m}$-Radikals demonstrieren, und einige Bemerkungen zur Implementierung der beschriebenen Algorithmen runden diese Arbeit ab.

Lebenslauf

Perönliche Daten:	Carsten Friedrichs Schustehrusstraße 48 10585 Berlin geboren am 27.8.1973 in Detmold ledig
Schulausbildung:	4.6.1992 Abitur am Gymnasium Leopoldinum in Detmold.
Studium:	10/1992 - 9/1994 Grundstudium der Mathematik (Diplom) mit Nebenfach Informatik an der Universität-Gesamthochschule Paderborn. 10/1994 - 4/1997 Hauptstudium der Mathematik an der TU Berlin. 24.4.1997 Diplom in Mathematik (Titel der Diplomarbeit: „Berechnung relativer Ganzheitsbasen mit dem Round-2-Algorithmus“). 4/1998 - 10/2000 Anfertigung der Dissertation an der TU Berlin. 19.12.2000 Tag der wissenschaftlichen Aussprache.
Stipendium:	1.7.1998 - 31.3.2000 gefördert durch ein Stipendium nach dem Nachwuchs-Förderungs-Gesetz des Landes Berlin.
Tätigkeiten:	1.10.1995 - 30.4.1997 Studentische Hilfskraft von Prof. Pohst am Fachbereich 3 Mathematik der TU Berlin im Rahmen eines DFG-Projektes. 1.1.1998 - 31.8.1999 Wissenschaftlicher Mitarbeiter von Prof. Pohst am Fachbereich 3 Mathematik der TU Berlin im Rahmen eines DFG-Projektes. 1.4.2000 - 31.3.2001 Wissenschaftlicher Mitarbeiter am Fachbereich 3 Mathematik der TU Berlin (Lehrtätigkeiten).
Wehrdienst:	1.5.1997 - 28.2.1998 Panzergrenadierbataillon 421 in Brandenburg an der Havel.