Mathematisches Institut
LUDWIG–MAXIMILIANS–UNIVERSITÄT MÜNCHEN

Masterarbeit

Algorithmische Umsetzung der Idealarithmetik in nicht-maximalen Ordnungen von Zahlkörpern

Thomas Burger

Mathematik Master

Aufgabensteller: Dr. Ralf Gerkmann
Abgabetermin: 5. März 2013

Ich versichere hiermit, dass ich die vorliegende Arbeit selbstständig verfasst und nur die im Literaturverzeichnis angegebenen Quellen verwendet habe.

Ort, Datum	Unterschrift

Inhaltsverzeichnis

1 Einführung **7**

2 Vorbereitung **9**
2.1 Erweiterung und Kontraktion 9
2.2 Faktormoduln und Faktorringe 12
2.3 Lokalisierung 21
2.4 Ring- und Körpererweiterungen 25
2.5 Euklidischer Algorithmus 28
2.6 Chinesischer Restsatz 31
2.7 Spezielle Matrizen 33
2.7.1 Zeilenstufenform 33
2.7.2 Hermite-Normalform 37
2.7.3 Smith-Normalform 40
2.8 Eigenschaften von Moduln/Ringen/Algebren 43
2.8.1 Noethersch und artinsch 44
2.8.2 Endlich erzeugt 47
2.8.3 Jacobson-Radikal und Nilradikal 50
2.8.4 Einfachheit und idempotente Elemente 55
2.9 Norm, Spur und Diskriminante 59

3 Algebraische Zahlentheorie **61**
3.1 Grundbegriffe 61
3.1.1 Moduln 62
3.1.2 Ordnungen 65
3.1.3 Gebrochene und ganzzahlige Ideale 68
3.2 Bewertungen 70
3.2.1 Definitionen 71
3.2.2 Eigenschaften 75
3.3 Primideale und Idealzerlegung 78
3.3.1 Primideale 78
3.3.2 Bewertung an Primidealen 83
3.3.3 Zusammenhang mit Lokalisierung $\mathcal{O}_{\mathfrak{p}}$ 87
3.3.4 Zerlegung von Idealen in Primideale 89

3.3.5 p-Maximalität 95

4 Algorithmen **97**
4.1 Koordinatensysteme in Zahlkörpern 97
4.2 Übersicht über Funktionen 101
4.2.1 Zahlkörper 101
4.2.2 Elemente von Zahlkörpern 102
4.2.3 Moduln 103
4.2.4 Ordnungen 105
4.2.5 Ideale 106
4.3 Beschreibung der Algorithmen 107
4.3.1 Matrixalgorithmen 108
4.3.2 Modulalgorithmen 116
4.3.3 Ordnungsalgorithmen 120
4.3.4 Idealalgorithmen 123
4.3.5 Zahlkörperalgorithmen 125
4.4 Umsetzung der Algorithmen in Sage 126
4.4.1 Vorbemerkungen 127
4.4.2 Zahlkörper 127
4.4.3 Moduln 130
4.4.4 Ideale 134

5 Zusammenfassung **137**

Literaturverzeichnis **138**

Stichwortverzeichnis **139**

Kapitel 1

Einführung

Motivation und Ziele der Arbeit

Ein wichtiger Satz der elementaren Zahlentheorie besagt, dass sich jede ganze Zahl außer 0 eindeutig in ein Produkt von Primzahlen zerlegen lässt. Man nennt diesen Satz auch den Fundamentalsatz der Arithmetik. Ein ähnlicher Satz findet sich auch im Bereich der algebraischen Zahlentheorie, wenn man einen Zahlkörper K und seinen Ganzheitsring $\mathcal{O}_K$ betrachtet. Dort stellt man fest, dass sich jedes Ideal in $\mathcal{O}_K$ eindeutig in ein Produkt von Primidealen zerlegen lässt.

Statt die Ideale in $\mathcal{O}_K$ zu betrachten, kann man allerdings auch Ideale in einer Ordnung von K betrachten, wobei Ordnungen spezielle Unterringe von K sind. Der Ring $\mathcal{O}_K$ ist eine solche Ordnung und wird auch als Maximalordnung bezeichnet. In der Literatur wird häufig nur die vollständige Zerlegbarkeit von Idealen in der Maximalordnung gezeigt. Deswegen soll in dieser Arbeit die Arithmetik und Zerlegbarkeit von Idealen in allgemeinen Ordnungen untersucht werden, insbesondere in nicht-maximalen Ordnungen. Gerade bei komplizierteren Zahlkörpern lässt sich die Idealarithmetik nur sehr schwer per Hand ausführen oder es dauert zumindest sehr lange. Deshalb werden in der Arbeit Algorithmen vorgestellt und implementiert, mit denen man die Berechnungen auch am Computer ausführen kann.

Vorwissen

In dieser Arbeit wird vorausgesetzt, dass man mit grundlegenden Begriffen aus der Algebra vertraut ist (insbesondere Ringe, Ideale und Homomorphismen). Diese können in einführenden Büchern über Algebra nachgelesen werden, beispielsweise in [FS78] oder [Fis11]. An vielen Stellen wird außerdem das Lemma von Zorn benötigt, das ebenfalls in diesen beiden Büchern zu finden ist. Für manche Algorithmen und Beweise werden zudem grundlegende Kenntnisse über Matrizen, Eigenwerte und charakteristische Polynome benötigt, wie man sie in [Fis08] oder anderen Büchern über lineare

Algebra nachlesen kann. Der Begriff „Modul“ ist ebenfalls dort zu finden. Grundlegende Kenntnisse über Körpererweiterungen sind zu empfehlen, allerdings wird an entsprechenden Stellen oft explizit auf Sätze aus [FS78] und [Fis11] verwiesen.

Übersicht über die Arbeit

Kapitel 2 dient vor allem als Nachschlagewerk für Sätze aus der (linearen) Algebra und elementaren Zahlentheorie, die in der Arbeit wichtig für bestimmte Beweise sind, aber nicht als Vorwissen vorausgesetzt werden. Für die meisten Leser mit algebraischen Vorkenntnissen ist es sinnvoll das Kapitel 2 beim ersten Lesen zu überspringen und nur bei Interesse an bestimmten Beweisen darauf zurückzugreifen. In Kapitel 3 werden grundlegende Begriffe der algebraischen Zahlentheorie eingeführt und es wird untersucht, wie man Ideale zerlegen kann. Der Schwerpunkt liegt dabei auf Idealen in nichtmaximalen beziehungsweise allgemeinen Ordnungen, allerdings werden auch einige Sätze speziell für die Maximalordnung gezeigt. In Kapitel 4 wird gezeigt, wie man mit Hilfe von Koordinatensystemen und Matrizen die Idealarithmetik und -zerlegung algorithmisch darstellen kann. Außerdem werden diese Algorithmen mit dem Algebra-System Sage (siehe [S$^+$09]) umgesetzt. Im letzten Kapitel befindet sich eine Zusammenfassung der Ergebnisse der Arbeit und nach dem Literaturverzeichnis ein Stichwortverzeichnis. Am Anfang vieler Abschnitte befindet sich eine kurze Inhaltsbeschreibung für den jeweiligen Abschnitt. Die meisten Sätze und Algorithmen der Arbeit orientieren sich an [Ger09], in manchen Abschnitten wird aber noch zusätzliche Literatur genannt.

Kapitel 2

Vorbereitung

2.1 Erweiterung und Kontraktion

In diesem Abschnitt werden die Erweiterung und die Kontraktion von Idealen eingeführt. Dies sind die Ideale, die von den Bildern und den Urbildern von Idealen unter einem Ringhomomorphismus gebildet werden. Dabei ist jedoch zu beachten, dass zwar das Urbild eines Ideals wieder ein Ideal ist, aber das Bild eines Ideals im Allgemeinen kein Ideal ist (sondern nur eine abelsche Gruppe). Man muss also bei der Erweiterung das Bild noch zu einem Ideal erweitern. Im Allgemeinen sind Erweiterung und Kontraktion nicht invers zueinander. In späteren Abschnitten wird jedoch gezeigt, dass Erweiterung und Kontraktion bei bestimmten Homomorphismen doch eine Bijektion zwischen gewissen Mengen von Idealen definieren. Aber auch für allgemeine Ringhomomorphismen gibt es einige Sätze und Eigenschaften, die in späteren Abschnitten noch sehr nützlich sind und deshalb in diesem Abschnitt bewiesen werden. Meistens sind die betrachteten Ringhomomorphismen einfache Inklusionen und es ergeben sich dadurch noch zusätzliche Eigenschaften für Erweiterung und Kontraktion. Beispiele für in dieser Arbeit betrachtete Ringhomomorphismen sind die kanonischen Homomorphismen in den Faktorring oder in die Lokalisierung. In den Einleitungen zu den Abschnitten 2.2 und 2.3 wird näher erläutert, wofür man diese nutzen kann. Die Begriffe Erweiterung und Kontraktion sind aus [NW10, S.24-27] entnommen.

Definition 2.1.1. Sei $\varphi : A \to B$ ein Ringhomomorphismus, sei $\mathfrak{a}$ ein Ideal in A. Im Allgemeinen ist $\varphi(\mathfrak{a})$ kein Ideal, aber man kann das von der Menge $\varphi(\mathfrak{a})$ erzeugte Ideal

$$B\mathfrak{a} := (\varphi(\mathfrak{a}))_B$$

betrachten. Man bezeichnet $B\mathfrak{a}$ als **Erweiterung** von $\mathfrak{a}$ bezüglich φ. Ist $\mathfrak{b}$ die Erweiterung eines Ideals in A, so nennt man $\mathfrak{b}$ auch **erweitertes Ideal**.

Bemerkung 2.1.2. *Ist $\iota : A \to B$ eine Ringinklusion, so besteht $B\mathfrak{a}$ genau aus den B-Linearkombinationen von Elementen $x_i = \iota(x_i) \in \mathfrak{a} \subset A \subset B$:*

$$B\mathfrak{a} = \left\{ \sum_{i=1}^{k} y_i * \iota(x_i) \mid k \in \mathbb{N},\ \forall\, i \in \{1, \ldots, k\} :\ x_i \in \mathfrak{a},\ y_i \in B \right\}$$

Definition 2.1.3. Sei $\varphi : A \to B$ ein Ringhomomorphismus, sei $\mathfrak{b}$ ein Ideal in B. Dann ist

$$\mathfrak{b}|_A := \varphi^{-1}(\mathfrak{b})$$

ein Ideal in A und wird als **Kontraktion** von $\mathfrak{b}$ bezüglich φ bezeichnet. Ist $\mathfrak{a}$ die Kontraktion eines Ideals in B, so heißt $\mathfrak{a}$ auch **kontrahiertes Ideal**.

Bemerkung 2.1.4. *Ist $\iota : A \to B$ eine Ringinklusion, so gilt:*

$$\mathfrak{a}|_A = \mathfrak{b} \cap A$$

Lemma 2.1.5. *Sei $\varphi : A \to B$ ein Ringhomomorphismus und $\mathfrak{p}$ ein Primideal in B. Dann ist die Kontraktion $\mathfrak{q} := \mathfrak{p}|_A$ ein Primideal in A.*

Beweis. Seien $a, b \in A$ Elemente mit $a*b \in \mathfrak{q}$. Es ist zu zeigen, dass entweder a oder b in $\mathfrak{q}$ liegen muss. Da $a * b$ in $\mathfrak{q}$ liegt, gilt $\varphi(a * b) \in \mathfrak{p}$, also wegen den Homomorphismuseigenschaften auch $\varphi(a) * \varphi(b) = \varphi(a * b) \in \mathfrak{p}$. Da $\mathfrak{p}$ ein Primideal in B ist, muss also entweder $\varphi(a) \in \mathfrak{p}$ gelten oder $\varphi(b) \in \mathfrak{p}$. Damit gilt aber auch $a \in \mathfrak{q}$ oder $b \in \mathfrak{q}$. □

Bemerkung 2.1.6. *(i) Die Kontraktion eines maximalen Ideals ist im Allgemeinen kein maximales Ideal.*

(ii) Die Erweiterung eines Primideals ist im Allgemeinen kein Primideal.

Beweis. Einfache Gegenbeispiele ergeben sich durch die Inklusion

$$\begin{array}{rccc} \varphi : & \mathbb{Z} & \to & \mathbb{Q} \\ & z & \mapsto & z \end{array}$$

Da $\mathbb{Q}$ ein Körper ist, gibt es in $\mathbb{Q}$ nur die beiden Ideale $(1)_{\mathbb{Q}} = \mathbb{Q}$ und $(0)_{\mathbb{Q}}$. Somit ist $(0)_{\mathbb{Q}}$ ein maximales Ideal. Die Kontraktion von $(0)_{\mathbb{Q}}$ auf $\mathbb{Z}$ ist dann das Ideal $(0)_{\mathbb{Z}}$. Dieses Ideal ist jedoch nicht maximal, da beispielsweise $(0)_{\mathbb{Z}} \subsetneq (2)_{\mathbb{Z}} \subsetneq (1)_{\mathbb{Z}}$ gilt. Für den zweiten Teil der Bemerkung kann man das Primideal $(2)_{\mathbb{Z}}$ in $\mathbb{Z}$ betrachten. Die Erweiterung $\mathbb{Q}(2)_{\mathbb{Z}}$ von $(2)_{\mathbb{Z}}$ bezüglich φ enthält auf jeden Fall das Element $\varphi(2_{\mathbb{Z}}) = 2_{\mathbb{Q}} \neq 0_{\mathbb{Q}}$. Da es im Körper $\mathbb{Q}$ nur das Nullideal und das Einheitsideal gibt, muss also die Erweiterung von $(2)_{\mathbb{Z}}$ das Einheitsideal sein. Das Einheitsideal ist aber kein Primideal. □

Proposition 2.1.7. *Sei $\varphi : A \to B$ ein Ringhomomorphismus, $\mathfrak{a}, \mathfrak{a}_1, \mathfrak{a}_2$ Ideale in A und $\mathfrak{b}, \mathfrak{b}_1, \mathfrak{b}_2$ Ideale in B. Dann gilt:*

(i) $\mathfrak{a}_1 \subset \mathfrak{a}_2 \Rightarrow B\mathfrak{a}_1 \subset B\mathfrak{a}_2$

(ii) $\mathfrak{a} \subset (B\mathfrak{a})|_A$

(iii) $B(\mathfrak{b}|_A) \subset \mathfrak{b}$

(iv) $B(\mathfrak{a}_1 \cap \mathfrak{a}_2) \subset B\mathfrak{a}_1 \cap B\mathfrak{a}_2$

(v) $B(\mathfrak{a}_1 + \mathfrak{a}_2) = B\mathfrak{a}_1 + B\mathfrak{a}_2$

(vi) $B(\mathfrak{a}_1 * \mathfrak{a}_2) = B\mathfrak{a}_1 * B\mathfrak{a}_2$

(vii) $\mathfrak{b}_1|_A \cap \mathfrak{b}_2|_A = (\mathfrak{b}_1 \cap \mathfrak{b}_2)|_A$

(viii) $\mathfrak{b}_1|_A + \mathfrak{b}_2|_A \subset (\mathfrak{b}_1 + \mathfrak{b}_2)|_A$

(ix) $\mathfrak{b}_1|_A * \mathfrak{b}_2|_A \subset (\mathfrak{b}_1 * \mathfrak{b}_2)|_A$

Beweis. (i) Sei $b \in B\mathfrak{a}_1$. Dann ist b eine B-Linearkombination von den Bildern der Elemente in $\mathfrak{a}_1$, also wegen $\mathfrak{a}_1 \subset \mathfrak{a}_2$ auch eine B-Linearkombination von den Bildern der Elemente in $\mathfrak{a}_2$. Damit gilt $b \in B\mathfrak{a}_2$.

(ii) Die Erweiterung $B\mathfrak{a}$ enthält zumindest die Elemente $\varphi(\mathfrak{a})$, da diese nach Definition die Erzeuger des erweiterten Ideals sind. Somit enthält auch die Kontraktion von $B\mathfrak{a}$ auf A zumindest die Urbilder der Elemente in $\varphi(\mathfrak{a})$, also insbesondere die Elemente in $\mathfrak{a}$.

(iii) Alle Elemente in $\mathfrak{b}|_A$ sind Urbilder von Elementen in $\mathfrak{b}$. Somit sind die Erzeuger des Ideals $B(\mathfrak{b}|_A)$ in $\mathfrak{b}$ und da $\mathfrak{b}$ ein Ideal in B ist, muss sogar das ganze Ideal $B(\mathfrak{b}|_A)$ in $\mathfrak{b}$ liegen.

(iv) Sei $b \in B(\mathfrak{a}_1 \cap \mathfrak{a}_2)$. Dann ist b eine B-Linearkombination von den Bildern $\varphi(a_i)$ von Elementen $a_i \in \mathfrak{a}_1 \cap \mathfrak{a}_2$. Da jedes a_i sowohl in $\mathfrak{a}_1$ als auch in $\mathfrak{a}_2$ ist, ist also b auch eine B-Linearkombination von den Bildern von Elementen in $\mathfrak{a}_1$ beziehungsweise $\mathfrak{a}_2$. Somit ist b auch in $B\mathfrak{a}_1$ und in $B\mathfrak{a}_2$ und somit auch im Schnitt von beiden.

(v) Sei zunächst $b \in B(\mathfrak{a}_1 + \mathfrak{a}_2)$. Dann ist b eine B-Linearkombination von den Bildern $\varphi(a_i + b_i)$, wobei $a_i \in \mathfrak{a}_1$ und $b_i \in \mathfrak{a}_2$ gilt. Wegen den Homomorphismuseigenschaften gilt aber $\varphi(a_i + b_i) = \varphi(a_i) + \varphi(b_i)$. Somit lässt sich die Linearkombination aufspalten in die Summe von zwei B-Linearkombinationen, so dass in einer der Linearkombinationen nur die Elemente $\varphi(a_i)$ und in der anderen nur die Elemente $\varphi(b_i)$ auftauchen. Also ist b in $B\mathfrak{a}_1 + B\mathfrak{a}_2$. Für die umgekehrte Teilmengenrelation folgt aus $\mathfrak{a}_1 \subset \mathfrak{a}_1 + \mathfrak{a}_2$ und (i) auch $B\mathfrak{a}_1 \subset B(\mathfrak{a}_1 + \mathfrak{a}_2)$ und zusammen mit der analogen Aussage für $\mathfrak{a}_2$ folgt $B\mathfrak{a}_1 + B\mathfrak{a}_2 \subset B(\mathfrak{a}_1 + \mathfrak{a}_2)$, da $B(\mathfrak{a}_1 + \mathfrak{a}_2)$ als Ideal bezüglich Addition abgeschlossen ist.

(vi) Sei zunächst $b \in B(\mathfrak{a}_1 * \mathfrak{a}_2)$. Da jedes Element in $\mathfrak{a}_1 * \mathfrak{a}_2$ eine Summe von Elementen der Form $a_1 * a_2$ mit $a_1 \in \mathfrak{a}_1$ und $a_2 \in \mathfrak{a}_2$ ist und die Übertragung der Summe bereits in (v) gezeigt wurde, genügt es, die Aussage für $b = \bar{b} * \varphi(a_1 * a_2)$ zu zeigen. Wegen den Homomorphismuseigenschaften gilt dann

$$b = \bar{b} * \varphi(a_1) * \varphi(a_2) = \bar{b} * \varphi(a_1) * 1_B * \varphi(a_2) \in B\mathfrak{a}_1 * B\mathfrak{a}_2.$$

Für die umgekehrte Richtung reicht es wegen (v), den Fall

$$b = b_1 * \varphi(a_1) * b_2 * \varphi(a_2) \in B\mathfrak{a}_1 * B\mathfrak{a}_2$$

zu zeigen. Es folgt aber sofort $b = (b_1 * b_2) * \varphi(a_1 * a_2) \in B(\mathfrak{a}_1 * \mathfrak{a}_2)$.

(vii) Sei zunächst $a \in \mathfrak{b}_1|_A \cap \mathfrak{b}_2|_A$. Dann ist $\varphi(a)$ sowohl in $\mathfrak{b}_1$ als auch in $\mathfrak{b}_2$. Somit ist a auch im Urbild von $\mathfrak{b}_1 \cap \mathfrak{b}_2$, also $a \in (\mathfrak{b}_1 \cap \mathfrak{b}_2)|_A$. Sei nun umgekehrt $a \in (\mathfrak{b}_1 \cap \mathfrak{b}_2)|_A$. Dann gilt $\varphi(a) = b \in \mathfrak{b}_1 \cap \mathfrak{b}_2 \subset \mathfrak{b}_i$. Somit ist a auch im Schnitt $\mathfrak{b}_1|_A \cap \mathfrak{b}_2|_A$.

(viii) Sei $a \in \mathfrak{b}_1|_A + \mathfrak{b}_2|_A$. Dann ist $a = a_1 + a_2$ mit $\varphi(a_i) \in \mathfrak{b}_i$. Wegen den Homomorphismuseigenschaften gilt also

$$\varphi(a) = \varphi(a_1 + a_2) = \varphi(a_1) + \varphi(a_2) \in \mathfrak{b}_1 + \mathfrak{b}_2.$$

Somit gilt $a \in (\mathfrak{b}_1 + \mathfrak{b}_2)|_A$.

(ix) Sei $a \in \mathfrak{b}_1|_A * \mathfrak{b}_2|_A$. Dann gilt $a = \sum_{ij} a_i * \bar{a}_j$ mit $\varphi(a_i) \in \mathfrak{b}_1$ und $\varphi(\bar{a}_j) \in \mathfrak{b}_2$. Wegen den Homomorphismuseigenschaften folgt also:

$$\varphi(a) = \varphi(\sum_{ij} a_i * \bar{a}_j) = \sum_{ij} \varphi(a_i) * \varphi(\bar{a}_j) \in \mathfrak{b}_1 * \mathfrak{b}_2$$

Somit ist a auch in $(\mathfrak{b}_1 * \mathfrak{b}_2)|_A$.

□

2.2 Faktormoduln und Faktorringe

In diesem Abschnitt werden Faktormoduln und Faktorringe definiert. Faktormoduln sind Moduln, bei denen ein Untermodul annulliert wird und Faktorringe sind Ringe, bei denen ein Ideal annulliert wird. Da jeder kommutative Ring $\mathcal{R}$ mit Einselement kanonisch ein $\mathcal{R}$-Modul ist, dessen Untermoduln genau seine Ideale sind (siehe die folgende Bemerkung), sind Faktorringe ein Spezialfall von Faktormoduln. Es wird am Anfang der entsprechenden Unterabschnitte näher beschrieben, wofür die Faktormoduln und Faktorringe in dieser Arbeit verwendet werden. Im gesamten Abschnitt sei $\mathcal{R}$ ein kommutativer Ring mit Einselement.

Bemerkung 2.2.1. *Der Ring $\mathcal{R}$ ist kanonisch ein $\mathcal{R}$-Modul, der vom Element $1_\mathcal{R}$ erzeugt wird. Die Addition vom Modul $\mathcal{R}$ ist dabei die Addition vom Ring $\mathcal{R}$ und die Skalarmultiplikation mit $\mathcal{R}$ vom Modul $\mathcal{R}$ ist die Multiplikation von Elementen im Ring $\mathcal{R}$. Die $\mathcal{R}$-Untermoduln vom Modul $\mathcal{R}$ sind dann genau die Ideale vom Ring $\mathcal{R}$. Viele Begriffe im Ring $\mathcal{R}$ mit Idealen sind gleichbedeutend mit Begriffen im $\mathcal{R}$-Modul $\mathcal{R}$ mit Untermoduln (zum Beispiel maximale Ideale/Untermoduln, Faktorringe/Faktormoduln).*

Notation. In der ganzen Arbeit werden Moduln, die von einer Menge X oder einer Folge von Elementen (a_i) erzeugt werden (über einem Ring R), durch $[X]_R$ beziehungsweise $[(a_i)]_R$ notiert.

Faktormoduln

In der Arbeit werden hauptsächlich Faktorringe betrachtet. Da jeder Faktorring aber gleichzeitig ein Faktormodul ist, können manche der benötigten Sätze für Faktorringe bereits für Faktormoduln gezeigt werden. Diese Sätze werden dann im nächsten Abschnitt auf Faktorringe übertragen. Es wird außerdem der Index definiert, der später im Zusammenhang mit der Diskriminante eine wichtige Rolle spielt. Durch Index und Diskriminante kann man die Primideale einschränken, die über einem Ideal liegen (und somit in der Produktzerlegung auftauchen können). Außerdem zeigt der Index $(\mathcal{O}_K : \mathcal{O})$ der Maximalordnung $\mathcal{O}_K$ über einer Ordnung $\mathcal{O}$, über welchen Primzahlen es nicht-invertierbare Primideale gibt.

Definition 2.2.2. Sei M ein $\mathcal{R}$-Modul und $N \subset M$ ein $\mathcal{R}$-Untermodul von M. Dann wird durch $m_1 \sim m_2 :\Leftrightarrow m_1 - m_2 \in N$ eine Äquivalenzrelation für Elemente in M definiert. Man nennt die Faktormenge $M/N := M/\sim$ auch **Faktormodul** von M und N, wobei die Faktormenge die Menge der Äquivalenzklassen von M bezüglich $\sim$ bezeichnet. Die kanonische Abbildung

$$\begin{aligned} \iota : M &\to M/N \\ m &\mapsto [m] \end{aligned}$$

ist ein Homomorphismus von $\mathcal{R}$-Moduln. Die Anzahl der Elemente in M/N wird als **Index** bezeichnet und durch $(M : N)$ notiert. Die Addition und die Skalarmultiplikation des $\mathcal{R}$-Moduls M/N ergeben sich direkt aus der Addition und Skalarmultiplikation von M:

$$\begin{aligned} + : \quad ([a],[b]) &\mapsto [a+b] \\ * : \quad (r,[a]) &\mapsto [r*a] \end{aligned}$$

Proposition 2.2.3 (Homomorphiesatz)**.** *Sei $f : A \to B$ ein Homomorphismus von $\mathcal{R}$-Moduln. Dann gilt $A/\ker f \cong f(A)$.*

Beweis. Da $\ker f$ ein Untermodul von A ist, kann man den Faktormodul $A/\ker f$ bilden. Die Funktion

$$\begin{aligned} \bar{f} : A/\ker f &\to f(A) \\ [a] &\mapsto f(a) \end{aligned}$$

ist wohldefiniert, da für einen anderen Repräsentanten $b \in [a]$ der Äquivalenzklasse nach Definition der Äquivalenzrelation $b - a \in \ker f$ gilt. Somit ist wegen den Homomorphismuseigenschaften von f auch

$$f(b) = f(b - a + a) = f(b - a) + f(a) = 0 + f(a) = f(a).$$

Es gilt außerdem für alle $a, b \in A$, $r \in \mathcal{R}$

$$\begin{aligned} \bar{f}([a] + [b]) &= \bar{f}([a + b]) = f(a + b) = f(a) + f(b) = \bar{f}([a]) + \bar{f}([b]) \\ \bar{f}(r * [a]) &= \bar{f}([r * a]) = f(r * a) = r * f(a) = r * \bar{f}([a]) \end{aligned}$$

also ist $\bar{f}$ sogar ein Homomorphismus von $\mathcal{R}$-Moduln. Ist $b \in f(A)$, so gibt es ein $a \in A$ mit $f(a) = b$. Somit ist auch $\bar{f}([a]) = f(a) = b$, also ist $\bar{f}$ surjektiv. Ist $\bar{f}([a]) = \bar{f}([b])$, so gilt $f(a) = f(b)$ und wegen f Homomorphismus auch $f(b - a) = f(b) - f(a) = 0$. Also ist $b - a \in \ker f$ und somit $[a] = [b]$. Damit ist gezeigt, dass $\bar{f}$ injektiv ist. Somit ist der Ringhomomorphismus bijektiv, also ein Isomorphismus. □

Lemma 2.2.4. *Sei $f : M \to N$ ein Homomorphismus von $\mathcal{R}$-Moduln, $\bar{a} \in N$ und $a \in M$ mit $f(a) = \bar{a}$. Dann ist das Urbild von $\bar{a}$ gegeben durch die Menge*

$$a + \ker f := \{b \in M \mid \exists\, c \in \ker f : b = a + c\}.$$

Beweis. Zunächst gilt für jedes $c \in \ker f$ wegen den Homomorphismuseigenschaften die Gleichung

$$f(a + c) = f(a) + f(c) = f(a) + 0 = f(a).$$

Somit ist $a + \ker f \subset f^{-1}(\bar{a})$. Sei nun $b \in f^{-1}(\bar{a})$. Dann gilt $f(b) = \bar{a}$ und somit wegen den Homomorphismuseigenschaften auch

$$f(b - a) = f(b) - f(a) = \bar{a} - \bar{a} = 0.$$

Somit ist $b - a \in \ker f$, also auch $b = a + b - a \in a + \ker f$. Damit ist auch die umgekehrte Inklusion $a + \ker f \supset f^{-1}(\bar{a})$ gezeigt. □

Lemma 2.2.5. *Sei $f : M \to N$ ein Homomorphismus von $\mathcal{R}$-Moduln. Sei $\bar{M} = [(m_i)_{i \in I}]_{\mathcal{R}}$ ein Untermodul von M. Dann gilt*

$$f(\bar{M}) = [(f(m_i))_{i \in I}]_{\mathcal{R}}$$

und $[(f(m_i))_{i \in I}]_{\mathcal{R}}$ ist ein Untermodul von $f(M)$.

Beweis. Jedes Element $x \in \bar{M}$ ist eine $\mathcal{R}$-Linearkombination vom Erzeugendensystem $(m_i)_{i\in I}$, das heißt $x = \sum_{i\in I} r_i * m_i$ mit $r_i \in \mathcal{R}$ und nur endlich vielen r_i ungleich $0_\mathcal{R}$. Da f ein Homomorphismus ist, gilt also

$$f(x) = f(\sum_{i\in I} r_i * m_i) = \sum_{i\in I} r_i * f(m_i).$$

Somit ist $f(\bar{M}) \subset [(f(m_i))_{i\in I}]_\mathcal{R}$. Umgekehrt ist wegen der gleichen Homomorphismusgleichung auch jedes Element

$$\bar{x} := \sum_{i\in I} \bar{r}_i * f(m_i) \in [(f(m_i))_{i\in I}]_\mathcal{R}$$

das Bild des Elements $x := \sum_{i\in I} \bar{r}_i * m_i$. Also ist $\bar{x}$ in $f(\bar{M}) \subset f(M)$. Insgesamt wurde also gezeigt, dass $f(\bar{M})$ gleich $[(f(m_i))_{i\in I}]_\mathcal{R}$ und ein Untermodul von $f(M)$ ist. □

Lemma 2.2.6. *Sei $f : M \to N$ ein Homomorphismus von $\mathcal{R}$-Moduln. Sei $\bar{N} = [(n_i)_{i\in I}]_\mathcal{R}$ ein Untermodul von $f(M)$ und seien $m_i \in M$ beliebige Urbilder der n_i, das heißt $f(m_i) = n_i$ für jedes $i \in I$. Dann gilt*

$$f^{-1}(\bar{N}) = [(m_i)_{i\in I}]_\mathcal{R} + \ker f.$$

Beweis. Jedes Element $\bar{x} \in \bar{N}$ ist eine $\mathcal{R}$-Linearkombination vom Erzeugendensystem $(n_i)_{i\in I}$, das heißt $\bar{x} = \sum_{i\in I} r_i * n_i$ mit $r_i \in \mathcal{R}$ und nur endlich vielen r_i ungleich $0_\mathcal{R}$. Da f ein Homomorphismus ist, gilt also:

$$f(\sum_{i\in I} r_i * m_i) = \sum_{i\in I} r_i * f(m_i) = \sum_{i\in I} r_i * n_i = \bar{x}$$

Somit ist $\sum_{i\in I} r_i * m_i$ ein Element des Urbilds von $\bar{x}$. Nach Lemma 2.2.4 ist dann das ganze Urbild von $\bar{x}$ gegeben durch $\sum_{i\in I} r_i * m_i + \ker f$. Es folgt, dass das Urbild vom Modul $[(n_i)_{i\in I}]_\mathcal{R}$ durch den Modul $[(m_i)_{i\in I}]_\mathcal{R} + \ker f$ gegeben ist. □

Proposition 2.2.7. *Seien $M \hookrightarrow N \hookrightarrow O$ $\mathcal{R}$-Untermoduln voneinander. Dann gilt:*

$$O/N \cong (O/M)/(N/M)$$

Beweis. Man definiert die folgende Abbildung:

$$\begin{array}{rcl} f : O/M & \to & O/N \\ [x]_M & \mapsto & [x]_N \end{array}$$

Die Abbildung f ist wohldefiniert, da für $x, y \in [x]_M$ auch $x - y \in M \subset N$ gilt und somit $x, y \in [x]_N$. Sie ist außerdem ein Homomorphismus, da für $x, y \in O$, $r \in R$ die folgenden Gleichungen gelten:

$$\begin{array}{rcccl} f([x]_M + [y]_M) & = & f([x+y]_M) = [x+y]_N & = & [x]_N + [y]_N \\ f(r * [x]_M) & = & f([r*x]_M) = [r*x]_N & = & r * [x]_N \end{array}$$

Sei $\iota_{O/M} : O \to O/M$ der kanonische Homomorphismus in den Faktormodul. Sei zunächst $f([x]_M) = 0_{O/N}$. Dann gilt $[x]_N = 0_{O/N}$ und somit $x - 0 \in N$. Also ist $[x]_M \in \iota_{O/M}(N)$. Ist umgekehrt $[x]_M \in \iota_{O/M}(N)$, so ist $x \in N$ und somit $f([x]_M) = [x]_N = 0_{O/N}$. Somit gilt $\ker f = \iota_{O/M}(N)$. Nach der Definition der Faktormoduln ist aber $\iota_{O/M}(N) = N/M$. Also ist der Kern des Homomorphismus f gegeben durch N/M. Das Bild von f ist ganz O/N, da jedes Element $[x]_N$ das Bild von $[x]_M$ unter f ist. Nach Proposition 2.2.3 gilt $(O/M)/\ker f \cong f(O/M)$ und somit $(O/M)/(N/M) \cong O/N$ wie behauptet. □

Proposition 2.2.8. *Seien $M \hookrightarrow N \hookrightarrow O$ $\mathcal{R}$-Untermoduln voneinander mit $(O : N) < \infty$ und $(N : M) < \infty$. Dann gilt*

$$(O : M) = (O : N) * (N : M).$$

Beweis. Sei $\bar{O}$ der Faktormodul O/M und $\bar{N}$ der Faktormodul N/M. Nach Proposition 2.2.7 gilt dann

$$(\bar{O} : \bar{N}) = (O/M : N/M) = |(O/M)/(N/M)| = |O/N| = (O : N)$$

Da der Index $o := (\bar{O} : \bar{N}) = (O : N)$ (und somit die Anzahl der Elemente im Faktorring $\bar{O}/\bar{N}$) nach Voraussetzung endlich ist, bildet der kanonische Homomorphismus $\bar{\iota} : \bar{O} \to \bar{O}/\bar{N}$ die Elemente von $\bar{O}$ auf o verschiedene Aquivalenzklassen beziehungsweise Elemente im Faktormodul ab. Ist $[a]$ eine beliebige Äquivalenzklasse im Faktormodul und $a \in \bar{O}$ ein Urbild von dieser Äquivalenzklasse, so ist $a + \bar{N}$ das gesamte Urbild der Äquivalenzklasse (vergleiche Lemma 2.2.4). Somit ist das Urbild jeder Äquivalenzklasse isomorph zu $\bar{N}$, enthält also nach der Definition des Index $n := |\bar{N}| = (N : M) < \infty$ Elemente. Die Urbilder der Äquivalenzklassen sind zueinander disjunkt und ergeben zusammen den ganzen Faktormodul $\bar{O}$. Also besteht $\bar{O}$ aus $o * n$ Elementen. Gleichzeitig gilt aber auch $|\bar{O}| = (O : M)$. Insgesamt folgt also:

$$(O : M) = |\bar{O}| = o * n = (\bar{O} : \bar{N}) * |\bar{N}| = (O : N) * (N : M)$$

□

Bemerkung 2.2.9. *Man kann auch $(O : M) < \infty$ als Voraussetzung nehmen. Der Faktormodul N/M ist dann ein Untermodul vom endlichen Faktormodul O/M und hat somit ebenfalls eine endliche Zahl an Elementen. Der Faktormodul O/N hat mindestens genauso große Äquivalenzklassen wie O/M, kann also höchstens so viele Äquivalenzklassen wie O/M haben, also eine endliche Zahl. Dadurch sind die Indizes $(O : N)$ und $(N : M)$ ebenfalls endlich.*

Proposition 2.2.10. *Sei $f : M \to N$ ein Homomorphismus von $\mathcal{R}$-Moduln. Dann induziert f eine Bijektion zwischen den Untermoduln von M, die den Kern von f enthalten und den Untermoduln von $f(M)$.*

Beweis. Sei g die Abbildung, die jedem Untermodul $\bar{M} \supset \ker f$ von M das Bild $f(\bar{M}) \subset f(M)$ zuordnet und $\bar{g}$ die Abbildung, die jedem Untermodul $\bar{N}$ von $f(M)$ das Urbild $f^{-1}(\bar{N})$ zuordnet. Um die Behauptung zu zeigen, müssen die folgenden vier Aussagen bewiesen werden:

1. Das Bild $g(\bar{M})$ ist ein Untermodul von $f(M)$.
2. Das Bild $\bar{g}(\bar{N})$ ist ein Untermodul von M, der den Kern von f enthält.
3. Es gilt $\bar{g}(g(\bar{M})) = \bar{M}$ für alle Untermoduln $\bar{M}$ von M, die $\ker f$ enthalten.
4. Es gilt $g(\bar{g}(\bar{N})) = \bar{N}$ für alle Untermoduln $\bar{N}$ von $f(M)$.

Durch diese vier Aussagen ist dann gezeigt, dass die Abbildungen g und $\bar{g}$ zueinander inverse Abbildungen zwischen der Menge der Untermoduln von M die $\ker f$ enthalten und der Menge der Untermoduln von $f(M)$ sind. Damit ist dann g beziehungsweise $\bar{g}$ eine geeignete Bijektion.

1. Nach Lemma 2.2.5 ist das Bild $g(\bar{M}) = f(\bar{M})$ der Untermodul von $f(M)$, der von den Bildern des Erzeugendensystems von $\bar{M}$ erzeugt wird.
2. Nach Lemma 2.2.6 ist das Urbild von $\bar{N} = [(n_i)_{i\in I}]_{\mathcal{R}}$ der Modul $[(m_i)_{i\in I}]_{\mathcal{R}} + \ker f$, wobei jedes m_i ein Element des Urbilds von n_i ist. Man sieht sofort, dass dies ein Untermodul von M ist, der den Kern enthält. Man beachte dabei, dass der Kern eines Homomorphismus ein Untermodul von M ist und die Summe von zwei Untermoduln wieder ein Untermodul ist.
3. Sei $\bar{M} = [(m_i)_{i\in I}]_{\mathcal{R}}$. Nach Lemma 2.2.5 ist dann

   $$g(\bar{M}) = f(\bar{M}) = [(f(m_i))_{i\in I}]_{\mathcal{R}}.$$

   Da jedes m_i ein Element des Urbilds von $f(m_i)$ ist, gilt also nach Lemma 2.2.6 auch

   $$\bar{g}([(f(m_i))_{i\in I}]_{\mathcal{R}}) = f^{-1}([(f(m_i))_{i\in I}]_{\mathcal{R}}) = [(m_i)_{i\in I}]_{\mathcal{R}} + \ker f.$$

   Insgesamt ist also $\bar{g}(g(\bar{M})) = \bar{M} + \ker f$ und da $\bar{M}$ den Untermodul $\ker f$ schon enthält, gilt $\bar{M} + \ker f = \bar{M}$ und somit die Behauptung.
4. Sei $\bar{N} = [(n_i)_{i\in I}]_{\mathcal{R}}$ und sei für jedes $i \in I$ das Element $m_i \in M$ ein Element des Urbilds von n_i (die m_i existieren, da $\bar{N}$ ein Untermodul von $f(M)$ ist). Dann gilt nach Lemma 2.2.6 die Gleichung

   $$\bar{g}(\bar{N}) = f^{-1}(\bar{N}) = [(m_i)_{i\in I}]_{\mathcal{R}} + \ker f.$$

Sei nun $(\bar{m}_i)_{i\in\bar{I}}$ ein $\mathcal{R}$-Erzeugendensystem des Kerns von f (dieser ist ein $\mathcal{R}$-Untermodul von M). Dann gilt

$$\bar{M} := [(m_i)_{i\in I}]_{\mathcal{R}} + \ker f = [(m_i)_{i\in I} \cup (\bar{m}_i)_{i\in\bar{I}}]_{\mathcal{R}}$$

und somit nach Lemma 2.2.5

$$g(\bar{M}) = f([(m_i)_{i\in I} \cup (\bar{m}_i)_{i\in\bar{I}}]_{\mathcal{R}}) = [(f(m_i))_{i\in I} \cup (f(\bar{m}_i))_{i\in\bar{I}}]_{\mathcal{R}}$$

Es gilt aber $f(\bar{m}_i) = 0_N$, da die $\bar{m}_i$ Erzeuger des Kerns von f sind, also gilt

$$[(f(m_i))_{i\in I} \cup (f(\bar{m}_i))_{i\in\bar{I}}]_{\mathcal{R}} = [(f(m_i))_{i\in I}]_{\mathcal{R}} = [(n_i)_{i\in I}]_{\mathcal{R}} = \bar{N},$$

da 0_N in $[(f(m_i))_{i\in I}]_{\mathcal{R}}$ sowieso schon enthalten ist. Insgesamt gilt also die behauptete Gleichung $g(\bar{g}(\bar{N})) = \bar{N}$.

□

Proposition 2.2.11. *Sei M ein $\mathcal{R}$-Modul, N ein Untermodul von M und M/N der Faktormodul von M und N. Dann induziert die kanonische Inklusion $\iota : M \to M/N$ eine Bijektion zwischen den Untermoduln von M, die N enthalten und den Untermoduln von M/N. Dabei werden in beide Richtungen maximale Untermoduln auf maximale Untermoduln abgebildet.*

Beweis. Da ι ein Homomorphismus ist, folgt aus Proposition 2.2.10, dass ι eine Bijektion zwischen den Untermoduln von M, die den Kern von ι enthalten und den Untermoduln von $\iota(M)$ induziert. Durch ι werden aber genau die Elemente auf $0_{M/N}$ abgebildet, die in N sind. Damit ist der Kern von ι gleich N. Außerdem ist ι surjektiv, das heißt $\iota(M) = M/N$. Somit ist die eben erwähnte Bijektion sogar zwischen den Untermoduln von M, die N enthalten und den Untermoduln von M/N, wie behauptet. Die Bijektion ist inklusionserhaltend, das heißt aus $\mathfrak{m} \subsetneq \mathfrak{n} \subsetneq M$ folgt $\iota(\mathfrak{m}) \subsetneq \iota(\mathfrak{n}) \subsetneq M/N$ und ebenso für die Umkehrfunktion (die den Moduln ihre Urbilder bezüglich ι zuordnet). Somit bildet die Bijektion auch maximale Untermoduln auf maximale Untermoduln ab (da in M genau dann Moduln zwischen $\mathfrak{m}$ und M existieren, wenn in M/N Moduln zwischen $\iota(\mathfrak{m})$ und M/N existieren). □

Proposition 2.2.12. *Sei N ein Untermodul von einem $\mathcal{R}$-Modul M. Dann ist M/N genau dann einfach, wenn N maximal ist.*

Beweis. Nach Proposition 2.2.11 induziert die Inklusion $\iota : M \to M/N$ eine Bijektion zwischen der Menge von Moduln $\mathcal{N} := \left\{\bar{N} \mid N \subset \bar{N} \subset M\right\}$ und der Menge von Moduln $\bar{\mathcal{N}} := \left\{\tilde{N} \mid [0]_{M/N} \subset \tilde{N} \subset [1]_{M/N}\right\}$. N ist genau dann maximal, wenn die Menge $\mathcal{N}$ genau zwei Elemente hat (nämlich N und M) und M/N ist genau dann einfach, wenn die Menge $\bar{\mathcal{N}}$ genau zwei Elemente hat (nämlich $[0]_{M/N}$ und $[1]_{M/N}$). Wegen der Bijektion zwischen $\mathcal{N}$ und $\bar{\mathcal{N}}$ ist also N genau dann maximal, wenn M/N einfach ist. □

Faktorringe

In diesem Abschnitt werden vor allem zwei wichtige Verwendungen von Faktorringen beschrieben. In Proposition 2.2.16 wird gezeigt, dass bestimmte Eigenschaften von Faktorringen zu bestimmten Eigenschaften des annullierten Ideals korrespondieren. Dies wird in der Arbeit mehrfach benötigt, um herauszufinden, ob ein Ideal ein Primideal oder sogar ein maximales Ideal ist. Die Bijektion zwischen bestimmten Idealen in $\mathcal{R}$ und Idealen im Faktorring (siehe Proposition 2.2.14 und Proposition 2.2.15) wird später bei der Bestimmung von Primidealen über einer bestimmten Primzahl benötigt.

Definition 2.2.13. Sei $\mathfrak{a} \subset \mathcal{R}$ ein Ideal in $\mathcal{R}$. Durch $a \sim b :\Leftrightarrow a - b \in \mathfrak{a}$ wird eine Äquivalenzrelation definiert. Man kann also die Faktormenge $\bar{\mathcal{R}} := \mathcal{R}/\sim$ bilden. Die Addition und die Multiplikation lassen sich von $\mathcal{R}$ direkt auf $\bar{\mathcal{R}}$ übertragen:

$$\begin{aligned} + : \quad ([a],[b]) &\mapsto \quad [a+b] \\ * : \quad ([a],[b]) &\mapsto \quad [a*b] \end{aligned}$$

Dadurch bekommt $\mathcal{R}/\mathfrak{a}$ eine Ringstruktur. Man nennt $\mathcal{R}/\mathfrak{a}$ den **Faktorring** von $\mathcal{R}$ bezüglich $\mathfrak{a}$. Andere übliche Bezeichnungen für die Faktorringe sind **Restklassenringe** oder **Quotientenringe**.

Proposition 2.2.14. *Sei $\mathcal{R}/\mathfrak{a}$ der Faktorring von $\mathcal{R}$ bezüglich $\mathfrak{a}$. Dann induziert die kanonische Inklusion $\iota : \mathcal{R} \to \mathcal{R}/\mathfrak{a}$ eine Bijektion zwischen den Idealen von $\mathcal{R}$, die $\mathfrak{a}$ enthalten und den Idealen von $\mathcal{R}/\mathfrak{a}$.*

Beweis. Betrachtet man den Ring $\mathcal{R}$ als $\mathcal{R}$-Modul über sich selbst, so sind die Ideale vom Ring $\mathcal{R}$ genau die Untermoduln vom Modul $\mathcal{R}$. Ebenso sind die Ideale vom Ring $\mathcal{R}/\mathfrak{a}$ die Untermoduln vom Modul $\mathcal{R}/\mathfrak{a}$. Außerdem ist der Faktorring vom Ring $\mathcal{R}$ und dem Ideal $\mathfrak{a}$ gleichzeitig der Faktormodul vom Modul $\mathcal{R}$ und dem Untermodul $\mathfrak{a}$. Die Aussage ergibt sich also sofort aus der analogen Aussage für Faktormoduln und Untermoduln (vergleiche Proposition 2.2.11). □

Proposition 2.2.15. *Die Bijektion aus Proposition 2.2.14 bildet Primideale auf Primideale ab (in beide Richtungen) und maximale Ideale auf maximale Ideale (in beide Richtungen).*

Beweis. Da die maximalen Ideale im Ring $\mathcal{R}$ den maximalen Untermoduln im kanonischen Modul $\mathcal{R}$ entsprechen, ergibt sich der zweite Teil der Aussage direkt aus der entsprechenden Aussage über Moduln (vergleiche Proposition 2.2.11). Sei $\iota : \mathcal{R} \to \mathcal{R}/\mathfrak{a}$ der kanonische Ringhomomorphismus, der ein Element auf seine Äquivalenzklasse abbildet. Sei zunächst $\mathfrak{p}$ ein Primideal in $\mathcal{R}$ mit $\mathfrak{a} \subset \mathfrak{p}$ und $\bar{\mathfrak{p}} := \iota(\mathfrak{p})$ das Bild von $\mathfrak{p}$. Seien $\bar{a}, \bar{b} \in \mathcal{R}/\mathfrak{a}$ Elemente mit

$\bar{a} * \bar{b} \in \bar{\mathfrak{p}}$. Seien $a, b \in \mathcal{R}$ mit $\iota(a) = \bar{a}$ und $\iota(b) = \bar{b}$ (diese existieren, da ι surjektiv ist). Dann gilt wegen ι Homomorphismus auch

$$\iota(a * b) = \iota(a) * \iota(b) = \bar{a} * \bar{b} \in \bar{\mathfrak{p}}.$$

Sei nun $c \in \mathfrak{p}$ mit $\iota(c) = \bar{a} * \bar{b}$. Dann gilt

$$\iota(a * b - c) = \iota(a * b) - \iota(c) = 0_{\mathcal{R}/\mathfrak{a}},$$

also $a * b - c \in \mathfrak{a} \subset \mathfrak{p}$. Somit ist auch $a * b = a * b - c + c \in \mathfrak{p}$. Da $\mathfrak{p}$ ein Primideal ist, gilt also $a \in \mathfrak{p}$ oder $b \in \mathfrak{p}$. Also ist $\bar{a} = \iota(a) \in \bar{\mathfrak{p}}$ oder $\bar{b} = \iota(b) \in \bar{\mathfrak{p}}$ und damit $\bar{\mathfrak{p}}$ ein Primideal. Sei nun umgekehrt $\bar{\mathfrak{p}}$ ein Primideal in $\mathcal{R}/\mathfrak{a}$ und $\mathfrak{p} := \iota^{-1}(\bar{\mathfrak{p}})$ das Urbild von $\bar{\mathfrak{p}}$. Seien $a, b \in \mathcal{R}$ mit $a * b \in \mathfrak{p}$. Dann gilt $\iota(a * b) \in \bar{\mathfrak{p}}$ und somit auch $\iota(a) * \iota(b) \in \bar{\mathfrak{p}}$. Da $\bar{\mathfrak{p}}$ ein Primideal ist, gilt also $\iota(a) \in \bar{\mathfrak{p}}$ oder $\iota(b) \in \bar{\mathfrak{p}}$. Somit ist entweder a oder b im Urbild $\mathfrak{p}$ von $\bar{\mathfrak{p}}$. Also ist $\mathfrak{p}$ ein Primideal. □

Proposition 2.2.16. *Sei $\mathfrak{a}$ ein Ideal von $\mathcal{R}$. Dann gilt:*

(i) $\mathfrak{a}$ ist genau dann ein Primideal, wenn $\mathcal{R}/\mathfrak{a}$ ein Integritätsring ist.

(ii) $\mathfrak{a}$ ist genau dann ein maximales Ideal, wenn $\mathcal{R}/\mathfrak{a}$ ein Körper ist.

Beweis. Sei $\iota : \mathcal{R} \to \mathcal{R}/\mathfrak{a}$ der kanonische Homomorphismus vom Ring in den Faktorring, der jedem Element seine Äquivalenzklasse zuordnet.

(i) Seien zunächst $\mathfrak{a}$ ein Primideal, $\bar{m}, \bar{n}$ Elemente in $\mathcal{R}/\mathfrak{a}$ mit $\bar{m} * \bar{n} = 0_{\mathcal{R}/\mathfrak{a}}$. Es ist zu zeigen, dass entweder $\bar{m}$ oder $\bar{n}$ gleich $0_{\mathcal{R}/\mathfrak{a}}$ sein muss. Seien m, n Elemente in $\mathcal{R}$ mit $\iota(m) = \bar{m}$ und $\iota(n) = \bar{n}$ (diese existieren, da ι surjektiv ist). Da ι ein Homomorphismus von Ringen ist, gilt also

$$\iota(m * n) = \iota(m) * \iota(n) = \bar{m} * \bar{n} = 0_{\mathcal{R}/\mathfrak{a}}.$$

Da der Kern von ι genau das Ideal $\mathfrak{a}$ ist, gilt also $m * n \in \mathfrak{a}$, also muss wegen $\mathfrak{a}$ Primideal auch $m \in \mathfrak{a}$ oder $n \in \mathfrak{a}$ gelten. Damit gilt aber auch $\bar{m} = \iota(m) = 0_{\mathcal{R}/\mathfrak{a}}$ oder $\bar{n} = \iota(n) = 0_{\mathcal{R}/\mathfrak{a}}$, also ist $\mathcal{R}/\mathfrak{a}$ ein Integritätsring. Sei nun $\mathcal{R}/\mathfrak{a}$ ein Integritätsring. Seien m, n Elemente in $\mathcal{R}$ mit $m * n \in \mathfrak{a}$. Es ist zu zeigen, dass entweder m oder n in $\mathfrak{a}$ liegt. Da ι ein Homomorphismus ist und $\mathfrak{a}$ der Kern von ι ist, gilt aber $0_{\mathcal{R}/\mathfrak{a}} = f(m * n) = f(m) * f(n)$. Da $\mathcal{R}/\mathfrak{a}$ ein Integritätsring ist, gilt dann entweder $f(m) = 0_{\mathcal{R}/\mathfrak{a}}$ oder $f(n) = 0_{\mathcal{R}/\mathfrak{a}}$. Also ist $m \in \mathfrak{a}$ oder $n \in \mathfrak{a}$ und $\mathfrak{a}$ ist ein Primideal.

(ii) Nach Proposition 2.2.14 gibt es eine Bijektion zwischen der Menge von Idealen $\mathcal{N} := \{\mathfrak{b} \mid \mathfrak{a} \subset \mathfrak{b} \subset \mathcal{R}\}$ in $\mathcal{R}$, die $\mathfrak{a}$ enthalten und der Menge von Idealen $\bar{\mathcal{N}} := \left\{\tilde{\mathfrak{b}} \mid (0)_{\mathcal{R}/\mathfrak{a}} \subset \tilde{\mathfrak{b}} \subset (1)_{\mathcal{R}/\mathfrak{a}}\right\}$ in $\mathcal{R}/\mathfrak{a}$. Das Ideal $\mathfrak{a}$ ist genau dann maximal, wenn $\mathcal{N}$ genau zwei Elemente hat und $\mathcal{R}/\mathfrak{a}$ ist genau dann ein Körper, wenn $\bar{\mathcal{N}}$ genau zwei Elemente hat. Durch die Bijektion zwischen $\mathcal{N}$ und $\bar{\mathcal{N}}$ ist also $\mathfrak{a}$ genau dann ein maximales Ideal, wenn $\mathcal{R}/\mathfrak{a}$ ein Körper ist.

□

2.3 Lokalisierung

Manchmal möchte man aus einem Ring einen neuen Ring konstruieren, in dem mehr Elemente invertierbar sind als im Ursprungsring. Dafür definiert man die sogenannte Lokalisierung. Dabei achtet man darauf, dass die Umwandlung von Elementen im Ursprungsring zu Elementen in der Lokalisierung ein Homomorphismus ist. Dadurch erhält man mit Hilfe von Erweiterung und Kontraktion eine Bijektion zwischen bestimmten Primidealen im Ursprungsring und der Menge aller Primideale in der Lokalisierung. Auch die Multiplikation von Idealen wird in der Lokalisierung erhalten, das heißt man kann entweder zwei Ideale miteinander multiplizieren und dann das Ideal in die Lokalisierung abbilden oder zuerst die beiden Ideale in die Lokalisierung abbilden und dann miteinander multiplizieren. Da die Lokalisierung weniger (Prim-)Ideale hat als der Ursprungsring, erhält man dadurch eine Einschränkung der Idealarithmetik auf bestimmte Ideale und somit in bestimmten Fällen eine Vereinfachung von Berechnungen. Eine der bekanntesten Lokalisierungen ist die Lokalisierung an Primidealen. Es wird später in dieser Arbeit gezeigt, dass man an der Lokalisierung einer Ordnung an einem Primideal erkennen kann, ob ein Primideal in der Ordnung invertierbar ist. Außerdem hängt die Lokalisierung am Primideal mit der Bewertung am Primideal zusammen, die den Exponenten eines invertierbaren Primideals in der Primidealzerlegung eines Ideals angibt. Im gesamten Abschnitt sei $\mathcal{R}$ ein kommutativer Ring mit Einselement.

Definition 2.3.1. Eine Teilmenge $S \subset \mathcal{R} \setminus \{0\}$ heißt **multiplikativ**, wenn folgende Eigenschaften erfüllt sind:

i) $1 \in S$

ii) $\forall a, b \in S : a * b \in S$

Man könnte auch sagen, dass S ein Untermonoid von $(\mathcal{R} \setminus \{0\}, *)$ ist.

Definition 2.3.2. Sei $S \subset \mathcal{R}$ eine multiplikative Teilmenge. Definiere die Menge $S^{-1}\mathcal{R} := (\mathcal{R} \times S)/\sim$, wobei $\sim$ durch folgende Äquivalenzrelation gegeben ist:

$$(a, r) \sim (b, s) :\Leftrightarrow \exists\, t \in S : t(sa - rb) = 0$$

Man nennt $S^{-1}\mathcal{R}$ die **Lokalisierung** von $\mathcal{R}$ bezüglich S. Die Äquivalenzklasse von (a, r) wird mit $\frac{a}{r}$ bezeichnet. Außerdem definiert man zwei Verknüpfungen:

$$+ : \quad (\tfrac{a}{r}, \tfrac{b}{s}) \mapsto \quad \frac{sa + rb}{rs}$$

$$* : \quad (\tfrac{a}{r}, \tfrac{b}{s}) \mapsto \quad \frac{ab}{rs}$$

Dadurch erhält man eine Ringstruktur auf der Lokalisierung.

Beispiel 2.3.3. Da $S := (\mathcal{R} \setminus \{0\}, *)$ multiplikativ ist, lässt sich die Lokalisierung $k := S^{-1}\mathcal{R}$ bilden. In k sind dann alle Elemente außer 0 invertierbar und k ist somit ein Körper. Man nennt k den **Quotientenkörper** von $\mathcal{R}$.

Bemerkung 2.3.4. *Sei $S^{-1}\mathcal{R}$ die Lokalisierung an einer multiplikativen Teilmenge S. Die Abbildung*

$$\begin{array}{rcl} \iota : \mathcal{R} & \to & S^{-1}\mathcal{R} \\ x & \mapsto & \dfrac{x}{1} \end{array}$$

ist ein Ringhomomorphismus. Man kann also Erweiterungen von Idealen in $\mathcal{R}$ und Kontraktionen von Idealen in $S^{-1}\mathcal{R}$ betrachten.

Lemma 2.3.5. *Jedes Ideal $\mathfrak{b}$ in $S^{-1}\mathcal{R}$ ist ein erweitertes Ideal. Genauer gesagt ist $\mathfrak{b}$ die Erweiterung seiner Kontraktion $\mathfrak{a} := \mathfrak{b}|_{\mathcal{R}}$, das heißt es gilt $(S^{-1}\mathcal{R})(\mathfrak{b}|_{\mathcal{R}}) = \mathfrak{b}$.*

Beweis. Nach den Eigenschaften von Kontraktion und Erweiterung (siehe Proposition 2.1.7) gilt $(S^{-1}\mathcal{R})(\mathfrak{b}|_{\mathcal{R}}) \subset \mathfrak{b}$. Sei umgekehrt $\frac{a}{s} \in \mathfrak{b}$ mit $a \in \mathcal{R}$ und $s \in S$. Dann ist $a = \frac{a}{1} = \frac{a}{s} * \frac{s}{1} \in \mathfrak{b} \cap \mathcal{R}$ und $\frac{1}{s} \in S^{-1}\mathcal{R}$. Somit gilt auch $\frac{a}{s} = \frac{1}{s} * \frac{a}{1} \in (S^{-1}\mathcal{R})(\mathfrak{b}|_{\mathcal{R}})$. □

Lemma 2.3.6. *Sei $\mathfrak{p}$ ein Primideal in $\mathcal{R}$ mit $\mathfrak{p} \cap S = \emptyset$. Dann ist seine Erweiterung $\bar{\mathfrak{p}} := (S^{-1}\mathcal{R})\mathfrak{p}$ ein Primideal in $S^{-1}\mathcal{R}$.*

Beweis. Seien $\frac{a}{s}, \frac{b}{t} \in S^{-1}\mathcal{R}$ mit $a, b \in \mathcal{R}$, $s, t \in S$ und $\frac{a}{s} * \frac{b}{t} \in \bar{\mathfrak{p}}$. Dann gilt $\frac{a}{s} * \frac{b}{t} = \frac{c}{u} * p$ für geeignete $c \in \mathcal{R}$, $u \in S$, $p \in \mathfrak{p}$. Somit ist $a * b * u = \tilde{s} * p \in \mathfrak{p}$ für $\tilde{s} = s * t * c \in S$ und wegen $\mathfrak{p}$ Primideal und $\mathfrak{p} \cap S = \emptyset$ gilt $a \in \mathfrak{p}$ oder $b \in \mathfrak{p}$. Also ist $\frac{a}{s} = \frac{1}{s} * \frac{a}{1} \in \bar{\mathfrak{p}}$ oder $\frac{b}{t} = \frac{1}{t} * \frac{b}{1} \in \bar{\mathfrak{p}}$. □

Lemma 2.3.7. *Sei $\mathfrak{p}$ ein Primideal in $\mathcal{R}$ mit $\mathfrak{p} \cap S = \emptyset$. Dann ist $\mathfrak{p}$ ein kontrahiertes Ideal. Genauer gesagt ist $\mathfrak{p}$ die Kontraktion seiner Erweiterung $\bar{\mathfrak{p}} := (S^{-1}\mathcal{R})\mathfrak{p}$, das heißt es gilt $\bar{\mathfrak{p}}|_{\mathcal{R}} = \mathfrak{b}$.*

Beweis. Nach Proposition 2.1.7 gilt $\mathfrak{p} \subset ((S^{-1}\mathcal{R})\mathfrak{p})|_{\mathcal{R}} = \bar{\mathfrak{p}}|_{\mathcal{R}}$. Sei umgekehrt $x \in \bar{\mathfrak{p}}|_{\mathcal{R}}$, das heißt $x \in \mathcal{R}$ und $x = \frac{r}{s} * p$ für geeignete $r \in \mathcal{R}$, $p \in \mathfrak{p}$, $s \in S$. Dann gilt $x * s = \tilde{r} * p \in \mathfrak{p}$ für ein geeignetes $\tilde{r} \in S$. Somit ist $\bar{x} * \bar{s} = 0$ in $\mathcal{R}/\mathfrak{p}$. Da $\mathfrak{p}$ ein Primideal ist, ist nach Proposition 2.2.16 der Ring $\mathcal{R}/\mathfrak{p}$ ein Integritätsring, also folgt $\bar{x} = 0$ oder $\bar{s} = 0$ in $\mathcal{R}/\mathfrak{p}$ und somit $x \in \mathfrak{p}$ oder $s \in \mathfrak{p}$. Letzteres ist aber nicht möglich, da $\mathfrak{p} \cap S = \emptyset$ vorausgesetzt wurde. Also ist $x \in \mathfrak{p}$ und es folgt $\bar{\mathfrak{p}}|_{\mathcal{R}} \subset \mathfrak{p}$. □

Korollar 2.3.8. *Es gibt eine Bijektion zwischen Primidealen $\mathfrak{p}$ in $\mathcal{R}$ mit $\mathfrak{p} \cap S = \emptyset$ und Primidealen in $S^{-1}\mathcal{R}$.*

Beweis. Nach Lemma 2.3.6 ist die Erweiterung eines Primideals $\mathfrak{p}$ in $\mathcal{R}$ mit $\mathfrak{p} \cap S = \emptyset$ ein Primideal. Außerdem ist nach Lemma 2.1.5 die Kontraktion eines Primideals $\bar{\mathfrak{p}}$ in $S^{-1}\mathcal{R}$ ein Primideal. Hätte diese Kontraktion ein gemeinsames Element x mit S, so wäre $\frac{x}{1} \in \bar{\mathfrak{p}}$ eine Einheit und somit $\bar{\mathfrak{p}} = (1)_{S^{-1}\mathcal{R}}$. Dann wäre aber $\bar{\mathfrak{p}}$ kein Primideal. Man hat also durch Kontraktion und Erweiterung zwei wohldefinierte Abbildungen zwischen der Menge der Primideale in $\mathcal{R}$ mit $\mathfrak{p} \cap S = \emptyset$ und der Menge der Primideale in $S^{-1}\mathcal{R}$ gegeben. Diese sind nach Lemma 2.3.5 und Lemma 2.3.7 invers zueinander. □

Beispiel 2.3.9. Sei $\mathfrak{p}$ ein Primideal in $\mathcal{R}$. Nach der Definition eines Primideals kann $x * y$ nur dann in $\mathfrak{p}$ sein, wenn x oder y in $\mathfrak{p}$ ist. Sind $x, y \in \mathcal{R} \setminus \mathfrak{p}$, so ist damit auch $x * y \in \mathcal{R} \setminus \mathfrak{p}$. Die Menge $\mathcal{R} \setminus \mathfrak{p}$ ist also multiplikativ. Man kann also die Lokalisierung $(\mathcal{R} \setminus \mathfrak{p})^{-1}\mathcal{R}$ bilden.

Definition 2.3.10. Man bezeichnet $\mathcal{R}_\mathfrak{p} := (\mathcal{R} \setminus \mathfrak{p})^{-1}\mathcal{R}$ als **Lokalisierung** vom Ring $\mathcal{R}$ am Primideal $\mathfrak{p}$. Ist $\mathfrak{a}$ ein Ideal in $\mathcal{R}$, so wird die Erweiterung $\mathcal{R}_\mathfrak{p}\mathfrak{a}$ im Folgenden auch als $\mathfrak{a}_\mathfrak{p}$ notiert.

Proposition 2.3.11. *Sei $\mathfrak{p}$ ein Primideal. Dann gibt es eine Bijektion zwischen Primidealen $\mathfrak{q}$ in $\mathcal{R}$ mit $\mathfrak{q} \subset \mathfrak{p}$ und Primidealen in $\mathcal{R}_\mathfrak{p}$.*

Beweis. Nach Korollar 2.3.8 gibt es eine Bijektion zwischen Primidealen $\mathfrak{q}$ in $\mathcal{R}$ mit $\mathfrak{q} \cap S = \emptyset$ und Primidealen in $S^{-1}\mathcal{R}$. Hier ist aber $S = \mathcal{R} \setminus \mathfrak{p}$ und somit gilt $\mathfrak{q} \cap S = \emptyset$ genau dann wenn $\mathfrak{q} \subset \mathfrak{p}$ gilt. Damit ist die Behauptung gezeigt. □

Definition 2.3.12. Der Ring $\mathcal{R}$ heißt **lokal**, wenn er genau ein maximales Ideal $\mathfrak{m}$ hat.

Lemma 2.3.13. *Der Ring $\mathcal{R}$ ist genau dann lokal, wenn die Menge der Nicht-Einheiten in $\mathcal{R}$ ein Ideal ist. Dieses Ideal ist dann das maximale Ideal des lokalen Rings.*

Beweis. Zunächst stellt man fest, dass jedes echte Ideal $\mathfrak{a}$ von $\mathcal{R}$ eine Teilmenge der Nicht-Einheiten ist. Wäre nämlich $a \in \mathfrak{a}$ eine Einheit, so wäre $1 = a * a^{-1} \in (a)_\mathcal{R}$ und somit $(1)_\mathcal{R} \subset (a)_\mathcal{R} \subset \mathfrak{a} \subset (1)_\mathcal{R}$. Dann wäre aber $\mathfrak{a} = (1)_\mathcal{R}$ und deshalb $\mathfrak{a}$ kein echtes Ideal. Ist nun $\mathcal{R}$ lokal mit maximalem Ideal $\mathfrak{m}$, $a \in \mathcal{R}$ eine Nicht-Einheit und $\mathfrak{a} := (a)_\mathcal{R} \neq (1)_\mathcal{R}$ das von a erzeugte Hauptideal, so ist das Ideal $\mathfrak{a}$ in einem (dem einzigen) maximalen Ideal $\mathfrak{m}$ enthalten und somit insbesondere auch $a \in \mathfrak{m}$. Damit ist jede Nicht-Einheit in $\mathfrak{m}$ und wie vorher bereits festgestellt jede Einheit nicht in $\mathfrak{m}$. Somit ist das maximale Ideal genau die Menge der Nicht-Einheiten in $\mathcal{R}$ und diese bilden somit ein Ideal. Setzt man umgekehrt voraus, dass die Menge der Nicht-Einheiten ein Ideal in $\mathcal{R}$ ist, so ist das Ideal maximal, da alle größeren Ideale eine Einheit enthalten und somit gleich $(1)_\mathcal{R}$ sind. Außerdem enthält

die Menge der Nicht-Einheiten nach der Vorbemerkung alle echten Ideale, also ist sie auch das einzige maximale Ideal. □

Lemma 2.3.14. *Sei $\mathcal{R}_\mathfrak{p}$ die Lokalisierung von $\mathcal{R}$ am Primideal $\mathfrak{p}$. Sei*

$$\begin{array}{rcl} \iota : \mathcal{R} & \to & \mathcal{R}_\mathfrak{p} \\ r & \mapsto & \frac{r}{1} \end{array}$$

der kanonische Ringhomomorphismus von $\mathcal{R}$ nach $\mathcal{R}_\mathfrak{p}$. Dann gilt:

(i) Ist $\mathcal{R}$ nullteilerfrei, so ist ι injektiv.

(ii) Die Erweiterung $\mathfrak{p}_\mathfrak{p} = \mathcal{R}_\mathfrak{p}\mathfrak{p}$ ist das einzige maximale Ideal in $\mathcal{R}_\mathfrak{p}$. Somit ist $\mathcal{R}_\mathfrak{p}$ ein lokaler Ring.

(iii) Für jedes Ideal $\mathfrak{a}$ mit $\mathfrak{a} \not\subset \mathfrak{p}$ gilt $\mathfrak{a}_\mathfrak{p} = \mathcal{R}_\mathfrak{p}$.

(iv) Für zwei Ideale $\mathfrak{a}$, $\mathfrak{b}$ in $\mathcal{R}$ gilt $(\mathfrak{a} * \mathfrak{b})_\mathfrak{p} = \mathfrak{a}_\mathfrak{p} * \mathfrak{b}_\mathfrak{p}$.

Beweis. (i) Sei $\frac{a}{1} = \iota(a) = \iota(b) = \frac{b}{1}$. Dann gilt nach der Definition der Äquivalenzrelation $t * (1 * a - 1 * b) = 0_\mathcal{R}$ für ein $t \in \mathcal{R} \setminus \mathfrak{p} \subset \mathcal{R} \setminus \{0_\mathcal{R}\}$. Da $\mathcal{R}$ nullteilerfrei ist und $t \neq 0_\mathcal{R}$ ist, gilt also $a - b = 0_\mathcal{R}$ und somit $a = b$.

(ii) Sei $\bar{\mathfrak{q}}$ ein maximales Ideal in $\mathcal{R}_\mathfrak{p}$. Dann ist $\bar{\mathfrak{q}}$ insbesondere ein Primideal. Nach Proposition 2.3.11 ist also $\mathfrak{q} := \bar{\mathfrak{q}}|_\mathcal{R} = \bar{\mathfrak{q}} \cap \mathcal{R}$ ein Primideal in $\mathcal{R}$ mit $\mathfrak{q} \subset \mathfrak{p}$ und es gilt $\mathfrak{q}_\mathfrak{p} = \bar{\mathfrak{q}}$. Da die Erweiterung Teilmengenrelationen erhält, gilt also $\bar{\mathfrak{q}} = \mathfrak{q}_\mathfrak{p} \subset \mathfrak{p}_\mathfrak{p}$ und somit wegen der Maximalität von $\bar{\mathfrak{q}}$ auch $\bar{\mathfrak{q}} = \mathfrak{p}_\mathfrak{p}$. Da es in einem Ring immer ein maximales Ideal gibt und (wie eben festgestellt) jedes maximale Ideal gleich $\mathfrak{p}_\mathfrak{p}$ ist, ist $\mathfrak{p}_\mathfrak{p}$ das einzige maximale Ideal in $\mathcal{R}_\mathfrak{p}$.

(iii) Da $\mathfrak{a} \not\subset \mathfrak{p}$ gilt, gibt es ein $x \in (\mathfrak{a} \setminus \mathfrak{p}) \subset (\mathcal{R} \setminus \mathfrak{p})$. Somit ist $1_{\mathcal{R}_\mathfrak{p}} = \frac{x}{x} \in \mathcal{R}_\mathfrak{p}\mathfrak{a}$ und damit $\mathcal{R}_\mathfrak{p} = (1_{\mathcal{R}_\mathfrak{p}})_{\mathcal{R}_\mathfrak{p}} \subset \mathfrak{a}_\mathfrak{p} \subset \mathcal{R}_\mathfrak{p}$. Also gilt die Behauptung.

(iv) Dies folgt direkt aus den allgemeinen Eigenschaften der Erweiterung (vergleiche Proposition 2.1.7).

□

Lemma 2.3.15. *Seien $R \subset T$ Ringe, $\mathfrak{p}$ ein Primideal in R und $\mathfrak{q}$ ein Primideal in T mit $\mathfrak{p} = \mathfrak{q} \cap R$. Dann gilt $R_\mathfrak{p} \subset T_\mathfrak{q}$.*

Beweis. Sei $\frac{a}{b} \in R_\mathfrak{p}$ mit $a \in R$ und $b \in R \setminus \mathfrak{p}$. Angenommen b wäre in $\mathfrak{q}$. Dann wäre b auch in $\mathfrak{q} \cap R = \mathfrak{p}$, was ein Widerspruch zu $b \in R \setminus \mathfrak{p}$ ist. Somit gilt $a \in R \subset T$, $b \in R \subset T$ und $b \notin \mathfrak{q}$. Also ist $\frac{a}{b} \in T_\mathfrak{q}$. □

2.4 Ring- und Körpererweiterungen

In diesem Abschnitt werden einige Sätze über Ganzheit und Ringerweiterungen gezeigt, die im Verlauf der Arbeit benötigt werden. Darunter befindet sich auch ein Satz, dass jede endliche Erweiterung von $\mathbb{Q}$ (und somit auch jeder Zahlkörper) von einem ganzen Element erzeugt wird. Der Beweis dieses Satzes wird jedoch nur angedeutet und verwendet dabei mehrere Sätze aus der Theorie der Körpererweiterungen, die nicht in dieser Arbeit vorkommen. Es wird dort aber explizit auf die entsprechenden Sätze in [FS78] und [Fis11] verwiesen.

Definition 2.4.1. Sei $T \mid R$ eine Ringerweiterung. Dann heißt $t \in T$ **ganz** über R, wenn es ein normiertes Polynom $p \in R[x]$ gibt, so dass $p(t) = 0$ gilt. Das Polynom p heißt dann **Minimalpolynom** von t. $T \mid R$ heißt **ganz**, wenn alle $t \in T$ ganz über R sind.

Lemma 2.4.2. *Sei $T \mid R$ eine Ringerweiterung. Sei M ein endlich erzeugter R-Modul in T. Gilt $\alpha * M \subset M$ für ein $\alpha \in T$, so ist α ganz über R.*

Beweis. Sei $b_1, \ldots, b_n$ ein R-Erzeugendensystem von M. Wegen $\alpha * M \subset M$ gilt

$$\alpha * b_i = \sum_{j=1}^{n} a_{ij} * b_j$$

mit Elementen $a_{ij} \in R$. Sei $A = (a_{ij})$ die von den a_{ij} erzeugte $n \times n$-Matrix. Dann gilt

$$A * \begin{pmatrix} b_1 \\ \ldots \\ b_n \end{pmatrix} = \begin{pmatrix} \sum_{j=1}^{n} a_{1j} * b_j \\ \ldots \\ \sum_{j=1}^{n} a_{nj} * b_j \end{pmatrix} = \begin{pmatrix} \alpha * b_1 \\ \ldots \\ \alpha * b_n \end{pmatrix} = \alpha * \begin{pmatrix} b_1 \\ \ldots \\ b_n \end{pmatrix}.$$

Damit ist das Element α ein Eigenwert von A und somit eine Nullstelle des charakteristischen Polynoms von A (vergleiche [Fis08, Abschnitt 4.2]). Da A Koeffizienten in R hat, ist das charakteristische Polynom ein normiertes Polynom mit Koeffizienten in R, also ist α ganz über R. □

Lemma 2.4.3. *Sei $T \mid R$ eine endliche Ringerweiterung. Dann ist jedes Element $\alpha \in T$ ganz über R.*

Beweis. Da $T \mid R$ eine endliche Ringerweiterung ist, ist T ein endlich erzeugter R-Modul in T. Außerdem ist T ein Ring, also gilt für jedes $\alpha \in T$ auch $\alpha * T \subset T$. Somit ist nach Lemma 2.4.2 das Element α ganz über R. Da α beliebig gewählt war, ist jedes $\alpha \in T$ ganz über R. □

Lemma 2.4.4. *Sei $T \mid R$ eine Ringerweiterung, $\alpha \in T$. Dann ist α genau dann ganz über R, wenn der R-Modul*

$$R[\alpha] := \left\{ \sum_{i=0}^{m} z_i * \alpha^i \mid m \in \mathbb{N}_0, z_i \in R \right\}$$

endlich erzeugt ist.

Beweis. Sei zunächst α ganz über R. Dann gibt es nach Definition ein normiertes Polynom $f \in R[x]$, das α als Nullstelle hat. Sei also

$$f(\alpha) = \alpha^r + a_{r-1} * \alpha^{r-1} + \ldots + a_1 * \alpha + a_0 = 0$$

mit $a_i \in R$. Die Gleichung lässt sich umformen zu

$$\alpha^r = -(a_{r-1} * \alpha^{r-1} + \ldots + a_1 * \alpha + a_0)$$

Somit lässt sich α^r als R-Linearkombination von $\left\{1, \alpha, \ldots, \alpha^{r-1}\right\}$ darstellen und ebenso auch alle α^{r+i} für $i \in \mathbb{N}$. Damit gilt

$$R[\alpha] = \left\{ \sum_{i=0}^{r-1} z_i * \alpha^i \mid z_i \in R \right\} = [1, \alpha, \ldots, \alpha^{r-1}]_R,$$

also ist $R[\alpha]$ ein endlich erzeugter R-Modul.

Sei umgekehrt der R-Modul $R[\alpha]$ endlich erzeugt. Dann ist $R[\alpha] \mid R$ eine endliche Ringerweiterung. Nach Lemma 2.4.3 ist also jedes Element in $R[\alpha]$ ganz über R, insbesondere α selbst.

□

Lemma 2.4.5. *Sei $T \mid R$ eine Ringerweiterung und R ein Integritätsring. Sei $\alpha \in T \setminus \{0_T\}$ ganz über R. Dann ist der Koeffizient a_0 des Minimalpolynoms $\mu_\alpha(x) = x^r + a_{r-1} * x^{r-1} + \ldots + a_0$ ungleich 0_R.*

Beweis. Angenommen $a_0 = 0_R$. Wäre $r = 1$, so würde $\mu_\alpha = x$ und somit $\alpha = \mu_\alpha(\alpha) = 0_T$ folgen, was ein Widerspruch zur Voraussetzung ist. Sei also $r > 1$. Dann folgt

$$x^r + a_{r-1} * x^{r-1} + \ldots + a_0 = x * (x^{r-1} + a_{r-1} * x^{r-2} + \ldots + a_1) =: x * f(x)$$

Da aber R nullteilerfrei ist, ist auch $R[x]$ nullteilerfrei. Also ist wegen $\alpha \neq 0_T$ und $\alpha * f(\alpha) = \mu_\alpha(\alpha) = 0_T$ auch $f(\alpha) = 0_T$. Somit ist f ein normiertes Polynom mit Koeffizienten in R, das α als Nullstelle hat mit einem kleineren Grad als μ_α. Dies ist aber ein Widerspruch, da μ_α das Minimalpolynom von α über R ist. Somit war die Annahme $a_0 = 0_R$ falsch und es folgt die Behauptung. □

Lemma 2.4.6. *Sei k ein Körper, A eine kommutative, nullteilerfreie, unitäre k-Algebra, in der jedes Element ganz über k ist. Dann ist A ein Körper.*

Beweis. Da A nach den Voraussetzungen bereits ein Ring ist, ist nur noch zu zeigen, dass jedes Element in $A \setminus \{0_A\}$ invertierbar ist. Sei also $a \in A \setminus \{0_A\}$. Da a ganz ist, existiert das Minimalpolynom

$$\mu_a := x^r + a_{r-1} * x^{r-1} + \ldots + a_0$$

von a. Da k als Körper ein Integritätsring ist, folgt nach Lemma 2.4.5, dass $a_0 \neq 0_k$ gilt. Somit ist a_0 in k invertierbar und es folgt

$$\mu_a(a) * a_0^{-1} = a * (a^{r-1} + a_{r-1} * a^{r-2} + \ldots + a_1) * a_0^{-1} + 1 = 0.$$

Löst man die Gleichung nach der 1 auf, ergibt sich

$$a * (a^{r-1} + a_{r-1} * a^{r-2} + \ldots + a_1) * (-a_0^{-1}) = 1.$$

Somit ist $(a^{r-1} + a_{r-1} * a^{r-2} + \ldots + a_1) * (-a_0^{-1}) \in A$ ein Inverses zu a. Da $a \neq 0_A$ beliebig gewählt war, hat A für jedes Element $a \in A \setminus \{0_A\}$ ein Inverses und ist somit ein Körper. □

Definition 2.4.7. Sei $L \mid K$ eine Körpererweiterung. Dann heißt $l \in L$ **algebraisch** über K, wenn es ein Polynom $p \in K[x]$ gibt, so dass $p(l) = 0$ gilt. $L \mid K$ heißt **algebraisch**, wenn alle $l \in L$ algebraisch über K sind. Der **(Erweiterungs-)Grad** $\dim_K(L) := [L : K]$ von $L \mid K$ ist die Dimension von L als K-Vektorraum.

Bemerkung 2.4.8. *Sei $L \mid K$ eine Körpererweiterung und $l \in L$ algebraisch. Dann gibt es genau ein normiertes Polynom minimalen Grades in $K[x]$, das l als Nullstelle hat.*

Beweis. Existenz: Da l algebraisch ist, gibt es mindestens ein $f \in K[x]$ mit $f(l) = 0$, somit gibt es auch ein solches Polynom mit minimalem Grad. Da K ein Körper ist, lässt sich das Polynom normieren, indem man durch den führenden Koeffizienten teilt. Dieses normierte Polynom hat dann immer noch minimalen Grad und l ist von diesem Polynom ebenfalls eine Nullstelle.

Eindeutigkeit: Seien $f, f' \in K[x]$ zwei normierte Polynome minimalen Grades mit $f(l) = 0 = f'(l)$. Dann ist $g = f - f'$ ebenfalls ein Polynom in $K[x]$ mit Nullstelle l. Da f und f' normiert waren, hat g einen kleineren Grad als f und f', muss also wegen der Minimalität das Nullpolynom sein. Somit ist $f = f'$.

□

Definition 2.4.9. Man nennt das eindeutige normierte Polynom aus der Bemerkung auch das **Minimalpolynom** μ_l von l.

Theorem 2.4.10. *Sei K eine endliche Erweiterung von $\mathbb{Q}$. Dann wird K von einem Element erzeugt, das heißt es gibt ein $\alpha \in K$ mit $K = \mathbb{Q}(\alpha)$. Dieses Element ist algebraisch über $\mathbb{Q}$ und es gilt $\mathbb{Q}(\alpha) = \mathbb{Q}[\alpha]$.*

Beweis. Der Beweis dieses Satzes verwendet einige Sätze aus der Theorie der Körpererweiterungen. Diese werden hier nicht bewiesen, aber es wird auf entsprechende Beweise in der Literatur verwiesen. Nach dem Satz vom primitiven Element [Fis11, S.294] hat jede endliche Erweiterung von einem

Körper k mit Charakteristik 0 ein primitives Element, das heißt ein Element α mit $K = k(\alpha)$. Da $\mathbb{Q}$ die Charakteristik 0 hat, gilt also $K = \mathbb{Q}(\alpha)$ für ein geeignetes Element α. Da K eine endliche (und somit algebraische) Erweiterung über $\mathbb{Q}$ ist (siehe [Fis11, S. 259]), ist also insbesondere das Element $\alpha \in K$ algebraisch über $\mathbb{Q}$. Außerdem gilt für jedes algebraische Element α über $\mathbb{Q}$ auch $\mathbb{Q}[\alpha] = \mathbb{Q}(\alpha)$ (siehe [Fis11, S.253]). □

Bemerkung 2.4.11. *In der Literatur wird der Satz vom primitiven Element häufig in einer anderen Version formuliert (vergleiche zum Beispiel* [FS78, Satz 4.2.3.]*). Diese besagt, dass jede endliche separable Körpererweiterung ein primitives Element enthält. Jeder Körper k mit Charakteristik* 0 *ist vollkommen (siehe* [Fis11, S.286] *oder* [FS78, Korollar 3.4.8.]*), das heißt jedes Polynom in* $k[x]$ *ist separabel. Somit ist jede endliche Erweiterung von einem Körper mit Charakteristik* 0 *eine endliche separable Körpererweiterung. Also ist der Satz vom primitiven Element in* [Fis11] *ein Spezialfall des Satzes in* [FS78].

Korollar 2.4.12. *Sei K eine endliche Erweiterung von $\mathbb{Q}$. Dann gibt es ein über $\mathbb{Z}$ ganzes Element $\gamma \in K$ mit $K = \mathbb{Q}[\gamma]$.*

Beweis. Nach Theorem 2.4.10 gibt es ein über $\mathbb{Q}$ algebraisches Element α mit $K = \mathbb{Q}[\alpha]$. Da α algebraisch ist, gibt es also $a_0, \ldots, a_{r-1}, s_0, \ldots, s_{r-1} \in \mathbb{Z}$ mit

$$0 = \alpha^r + \frac{a_{r-1}}{s_{r-1}} * \alpha^{r-1} + \ldots + \frac{a_1}{s_1} * \alpha + \frac{a_0}{s_0}$$

Durch Multiplikation mit der r-ten Potenz des Hauptnenners s von den s_i erhält man

$$0 = s^r * \alpha^r + \frac{a_{r-1}}{s_{r-1}} * s^1 * s^{r-1} * \alpha^{r-1} + \ldots + \frac{a_1}{s_1} * s^{r-1} * s^1 * \alpha^1 + \frac{a_0}{s_0} * s^r.$$

Da s als Hauptnenner der s_i definiert war, sind alle $z_{r-i} := \frac{a_{r-i}}{s_{r-i}} * s^i$ für $i \in \{1, \ldots, r\}$ in $\mathbb{Z}$ und somit liefert

$$0 = (s * \alpha)^r + z_{r-1} * (s * \alpha)^{r-1} + \ldots + z_1 * (s * \alpha)^1 + z_0$$

ein normiertes Polynom mit Koeffizienten in $\mathbb{Z}$ und Nullstelle $s * \alpha$. Somit ist $s * \alpha$ ganz über $\mathbb{Z}$. Außerdem gilt wegen $s \in \mathbb{Z}$ auch $\mathbb{Q}[s * \alpha] = \mathbb{Q}[\alpha] = K$ und damit ist $\gamma := s * \alpha$ ein über $\mathbb{Z}$ ganzes Element, das K erzeugt. □

2.5 Euklidischer Algorithmus

In diesem Abschnitt wird der Euklidische Algorithmus vorgestellt, mit dem man den größten gemeinsamen Teiler von Elementen eines euklidischen Rings berechnen kann. Eine Abwandlung des Euklidischen Algorithmus wird

benötigt, um die Hermite-Normalform beziehungsweise die Smith-Normalform in einem späteren Abschnitt zu berechnen. Da Hermite-Normalform und Smith-Normalform in einigen Algorithmen eine wichtige Rolle spielen, wird der Euklidische Algorithmus in diesem Abschnitt wiederholt, obwohl er vermutlich den meisten Lesern bereits bekannt ist. Im ganzen Abschnitt sei $(\mathcal{R}_\mathrm{e}, N)$ ein euklidischer Ring $\mathcal{R}_\mathrm{e}$ mit Normfunktion $N : \mathcal{R}_\mathrm{e} \setminus \{0_{\mathcal{R}_\mathrm{e}}\} \to \mathbb{N}_0$.

Theorem 2.5.1. *Seien $a, b \in \mathcal{R}_e$. Dann existiert ein größter gemeinsamer Teiler von a und b. Durch den **Euklidischen Algorithmus** kann man einen größten gemeinsamen Teiler von a und b bestimmen:*

1. *Falls $N(a) < N(b)$ gilt, vertausche a und b.*
2. *Setze $x_0 := a$, $y_0 := b$, $i := 0$;*
3. *Berechne die Division x_i/y_i mit Rest r_i, das heißt $x_i = q_i * y_i + r_i$ mit entweder $r_i = 0$ oder $N(r_i) < N(y_i)$.*
4. *Ist $r_i = 0$, so gib y_i zurück. Ansonsten setze zunächst $x_{i+1} := y_i$ und $y_{i+1} := r_i$ und danach $i := i + 1$ und gehe zu Schritt 3).*

Beweis. Sei g ein gemeinsamer Teiler von x_i und y_i in Schritt 3). Dann ist $x_i = g * \bar{x}$ und $y_i = g * \bar{y}$ für geeignete $\bar{x}, \bar{y} \in \mathcal{R}_\mathrm{e}$. Berechnet man nun die Division $x_i = q_i * y_i + r_i$, so ergibt sich $g * \bar{x} = q_i * g * \bar{y} + r_i$, also $r_i = g*(\bar{x} - q_i * \bar{y})$. Somit ist g ein Teiler von r_i. Außerdem ist wegen $y_i = g*\bar{y}$ auch g ein Teiler von y_i. Setzt man nun also x_{i+1} und y_{i+1} auf y_i und r_i, so ist g auch ein gemeinsamer Teiler von x_{i+1} und y_{i+1}. Falls der Algorithmus terminiert, so ergibt sich bei der letzten Division $x_k = q_k * y_k$. Somit ist y_k ein gemeinsamer Teiler von x_k und y_k. Außerdem ist jeder gemeinsame Teiler von a und b nach dem Algorithmus auch ein gemeinsamer Teiler von x_i und y_i für alle $i \in \{0, \ldots, k\}$, also insbesondere ein Teiler von y_k. Damit ist y_k ein größter gemeinsamer Teiler von a und b. Es bleibt zu zeigen, dass der Algorithmus terminiert. Nach Schritt 1 gilt $N(b) < N(a)$ und somit im ersten Schritt $N(y_0) < N(x_0)$. Solange r_i nicht 0 wird, gilt wegen der Eigenschaft der Division mit Rest die Ungleichung $N(r_i) < N(y_i)$ und somit auch im nächsten Schritt $N(y_{i+1}) < N(x_{i+1})$. Wegen $x_{i+1} = y_i$ gilt also

$$N(x_0) > N(y_0) = N(x_1) > \ldots > N(y_{i-1}) = N(x_i) > N(y_i) = N(x_{i+1}) > \ldots$$

Würde der Algorithmus nicht terminieren, so würde man durch die $N(y_i)$ eine unendliche streng monoton absteigende Kette von natürlichen Zahlen bekommen, was nicht möglich ist. Somit muss der Algorithmus terminieren. □

Bemerkung 2.5.2. *Wenn man den größten gemeinsamen Teiler einer endlichen Menge $a_1, \ldots, a_n$ von Ringelementen berechnen will, dann kann man einen ähnlichen Algorithmus verwenden. Die Schritte können dann folgendermaßen beschrieben werden:*

1. *Falls Elemente ungleich* 0 *mit geringerer Norm als* a_1 *in* $a_2, \ldots, a_n$ *vorkommen, wähle eines von ihnen aus und vertausche es mit* a_1.

2. *Berechne die Divisionen mit Rest von beliebig vielen Elementen in* $a_2, \ldots, a_n$ *mit Divisor* a_1 *und ersetze die entsprechenden* a_i *durch die Reste der entsprechenden Divisionen. Dabei muss dafür gesorgt werden, dass sich mindestens ein* a_i *ändert, da ansonsten der Algorithmus nicht unbedingt terminiert.*

3. *Falls alle Elemente* $a_2, \ldots, a_n$ *gleich* 0 *sind, so ist* a_1 *der größte gemeinsame Teiler von den ursprünglichen* a_i.

Beweis. Der Beweis für diesen Algorithmus ist ähnlich zum Beweis des normalen Euklidischen Algorithmus. Die wichtigsten Schritte im Beweis sind, dass größte gemeinsame Teiler von den $a_1, \ldots, a_n$ erhalten bleiben und in jedem Schritt mindestens ein Element mit geringerer Norm als a_1 entsteht. Dieses wird dann im nächsten Schritt mit a_1 ausgetauscht, so dass die Norm von a_1 immer echt kleiner wird. Dadurch muss der Algorithmus terminieren und das letzte Element ungleich 0 muss dann der größte gemeinsame Teiler sein. □

Proposition 2.5.3. *Seien* $a, b \in \mathcal{R}_e$. *Dann gibt es Elemente* $s, t \in \mathcal{R}_e$ *mit* $a * s + b * t = ggT(a, b)$.

Beweis. Berechnet man den größten gemeinsamen Teiler von a und b mit dem Euklidischen Algorithmus, so muss man dabei immer Divisionen der Form $x_i = q_i * y_i + r_i$ ausführen. Dadurch bekommt man in jedem Schritt eine Darstellung $r_i = x_i - q_i * y_i$ des Restes r_i durch Dividend x_i und Divisor y_i. Wegen $x_i = y_{i-1}$ und $y_i = r_{i-1}$ ergibt sich dann

$$\begin{aligned} r_i &= x_i - q_i * y_i = y_{i-1} - q_i * r_{i-1} = y_{i-1} - q_i * (x_{i-1} - q_{i-1} * y_{i-1}) \\ &= q_i * x_{i-1} + (1 - q_i * q_{i-1}) * y_{i-1} = q_i * y_{i-2} + (1 - q_i * q_{i-1}) * r_{i-2} \\ &= \ldots \end{aligned}$$

Auf diese Weise erhält man nach i Schritten eine Darstellung von r_i als $\mathcal{R}_\mathrm{e}$-Linearkombination von $x_0 = a$ und $y_0 = b$. In der letzten Division des Euklidischen Algorithmus gilt $x_k = q_k * y_k = q_k * \mathrm{ggT}(a, b)$ und somit $\mathrm{ggT}(a, b) = y_k = r_{k-1}$. Somit ist der größte gemeinsame Teiler wie alle anderen r_i im Euklidischen Algorithmus eine $\mathcal{R}_\mathrm{e}$-Linearkombination von a und b. □

Definition 2.5.4. Man nennt den Algorithmus zur Bestimmung der Elemente s, t auch **Erweiterter Euklidischer Algorithmus**. Dieser wird hier nicht explizit angegeben, wurde aber im Beweis zu Proposition 2.5.3 angedeutet. Im Fall $\mathcal{R}_\mathrm{e} = \mathbb{Z}$ ist die Proposition 2.5.3 auch als **Lemma von Bézout** bekannt.

2.6 Chinesischer Restsatz

In diesem Abschnitt wird der Chinesische Restsatz bewiesen. Dieser beschreibt einen Isomorphismus, mit dem man in vielen Fällen einen vorgegebenen Faktorring als Produkt von Faktorringen mit einfacherer Struktur beschreiben kann. In dieser Arbeit wird er verwendet, um einen Zusammenhang zwischen dem Index $(\mathcal{O}_K : \mathcal{O})$ der Maximalordnung $\mathcal{O}_K$ über einer Ordnung $\mathcal{O}$ und der Invertierbarkeit von Primidealen über bestimmten Primzahlen herzustellen.

Definition 2.6.1. Sei R ein Ring und $\mathfrak{a}, \mathfrak{b}$ zwei Ideale in R. $\mathfrak{a}$ und $\mathfrak{b}$ heißen **teilerfremd**, falls $\mathfrak{a} + \mathfrak{b} = (1)_R$ gilt. Man sagt in diesem Fall auch $\mathfrak{a}$ ist **teilerfremd zu** $\mathfrak{b}$.

Lemma 2.6.2. *Sei R ein Ring, $\mathfrak{a}_1, \mathfrak{a}_2, \mathfrak{b}$ Ideale in R. Dann gilt:*

(i) $\mathfrak{a}_1$ *teilerfremd zu* $\mathfrak{a}_2 \Rightarrow \mathfrak{a}_1 * \mathfrak{a}_2 = \mathfrak{a}_1 \cap \mathfrak{a}_2$

(ii) $\mathfrak{a}_1$ *und* $\mathfrak{a}_2$ *jeweils teilerfremd zu* $\mathfrak{b} \Rightarrow \mathfrak{a}_1 * \mathfrak{a}_2$ *teilerfremd zu* $\mathfrak{b}$

Beweis. (i) Die Inklusionen $\mathfrak{a}_1 * \mathfrak{a}_2 \subset \mathfrak{a}_i$ sind aus den allgemeinen Idealeigenschaften bekannt. Somit ist auch $\mathfrak{a}_1 * \mathfrak{a}_2 \subset \mathfrak{a}_1 \cap \mathfrak{a}_2$. Sei umgekehrt $x \in \mathfrak{a}_1 \cap \mathfrak{a}_2$. Da $\mathfrak{a}_1$ teilerfremd zu $\mathfrak{a}_2$ ist, gilt $\mathfrak{a}_1 + \mathfrak{a}_2 = (1)_R$. Somit gibt es Elemente $a_1 \in \mathfrak{a}_1, a_2 \in \mathfrak{a}_2$ mit $a_1 + a_2 = 1$. Dann gilt

$$x = 1 * x = (a_1 + a_2) * x = a_1 * x + a_2 * x = a_1 * x + x * a_2$$

Da x sowohl in $\mathfrak{a}_1$ als auch in $\mathfrak{a}_2$ liegt, folgt $a_1 * x, x * a_2 \in \mathfrak{a}_1 * \mathfrak{a}_2$ und somit auch $x \in \mathfrak{a}_1 * \mathfrak{a}_2$. Damit ist die Behauptung gezeigt.

(ii) Sind $\mathfrak{a}_1$ und $\mathfrak{a}_2$ teilerfremd zu $\mathfrak{b}$, so gilt $\mathfrak{a}_i + \mathfrak{b} = (1)_{\mathcal{O}}$. Damit gilt

$$\begin{aligned}(1)_{\mathcal{O}} = (1)_{\mathcal{O}}^2 &= (\mathfrak{a}_1 + \mathfrak{b}) * (\mathfrak{a}_2 + \mathfrak{b}) \\ &= \mathfrak{a}_1 * \mathfrak{a}_2 + \mathfrak{a}_1 * \mathfrak{b} + \mathfrak{b} * \mathfrak{a}_2 + \mathfrak{b} * \mathfrak{b} \\ &= \mathfrak{a}_1 * \mathfrak{a}_2 + \mathfrak{b} * (\mathfrak{a}_1 + \mathfrak{a}_2 + \mathfrak{b}) \\ &\subset \mathfrak{a}_1 * \mathfrak{a}_2 + \mathfrak{b}\end{aligned}$$

Somit muss $(1)_{\mathcal{O}} = \mathfrak{a}_1 * \mathfrak{a}_2 + \mathfrak{b}$ gelten, also ist $\mathfrak{a}_1 * \mathfrak{a}_2$ teilerfremd zu $\mathfrak{b}$. □

Bemerkung 2.6.3. *Die Aussagen lassen sich durch vollständige Induktion direkt verallgemeinern zu:*

(i') $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ *paarweise teilerfremd* $\Rightarrow \prod_{i=1}^n \mathfrak{a}_i = \bigcap_{i=1}^n \mathfrak{a}_i$

(ii') $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ *jeweils teilerfremd zu* $\mathfrak{b} \Rightarrow \prod_{i=1}^n \mathfrak{a}_i$ *teilerfremd zu* $\mathfrak{b}$

Lemma 2.6.4. *Sei R ein Ring, $p \neq q \in \mathbb{Z}$ Primzahlen. Dann ist $(p * 1_R)_R$ teilerfremd zu $(q * 1_R)_R$, wobei $z * r$ mit $z \in \mathbb{Z}$ und $r \in R$ definiert ist durch $z * r = \sum_{i=1}^z r \in R$.*

Beweis. Da p und q Primzahlen sind, ist der größte gemeinsame Teiler von p und q in $\mathbb{Z}$ gleich $1_\mathbb{Z}$. Somit gibt es nach Proposition 2.5.3 Elemente $a, b \in \mathbb{Z}$ mit $a * p + b * q = 1_\mathbb{Z}$. Es gilt dann

$$(a * 1_R) * (p * 1_R) + (b * 1_R) * (q * 1_R) = (a * p + b * q) * 1_R = 1_\mathbb{Z} * 1_R = 1_R.$$

Dabei ist $(a*1_R)*(p*1_R) \in (p*1_R)_R$ und $(b*1_R)*(q*1_R) \in (q*1_R)_R$. Also ist die Einheit 1_R in $(p*1_R)_R+(q*1_R)_R$. Dann muss aber $(p*1_R)_R+(q*1_R)_R$ das Einheitsideal in R sein, also gilt $(p * 1_R)_R + (q * 1_R)_R = (1_R)_R$ und die beiden Ideale sind teilerfremd. □

Theorem 2.6.5 (Chinesischer Restsatz)**.** *Sei R ein Ring, $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ paarweise teilerfremde Ideale in R, $\mathfrak{a} := \prod_{i=1}^n \mathfrak{a}_i$. Dann ist $R/\mathfrak{a}$ isomorph zu $\bigoplus_{i=1}^n R/\mathfrak{a}_i$.*

Beweis. Da n endlich ist, entspricht die direkte Summe $\bigoplus_{i=1}^n R/\mathfrak{a}_i$ dem direkten Produkt $\prod_{i=1}^n R/\mathfrak{a}_i$. Man definiert sich die folgende Abbildung:

$$\begin{aligned} f : R &\to \prod_{i=1}^n R/\mathfrak{a}_i \\ x &\mapsto [x]_{\mathfrak{a}_i} \end{aligned}$$

Da jede der Abbildungen $f_i : R \to R/\mathfrak{a}_i$ ein Homomorphismus ist, ist auch f ein Homomorphismus. Der Kern von jedem f_i ist gegeben durch $\mathfrak{a}_i$, also ist der Kern von f gleich dem Durchschnitt der a_i. Da die a_i paarweise teilerfremd sind, ist wegen Bemerkung 2.6.3 der Durchschnitt der a_i gleich dem Produkt der a_i. Also ist der Kern von f gleich $\mathfrak{a}$. Nach Proposition 2.2.3 ist also $R/\mathfrak{a} = R/\ker f \cong f(R)$. Es ist also nur noch zu zeigen, dass f surjektiv ist. Dies lässt sich durch Induktion über n zeigen. Für $n = 1$ ist die Aussage trivial. Sei nun $n = 2$ und $([x_1]_{\mathfrak{a}_1}, [x_2]_{\mathfrak{a}_2})$ ein beliebiges Element in $R/\mathfrak{a}_1 \times R/\mathfrak{a}_2$. Da $\mathfrak{a}_1$ und $\mathfrak{a}_2$ teilerfremd zueinander sind, gibt es Elemente $a_1 \in \mathfrak{a}_1$ und $a_2 \in \mathfrak{a}_2$ mit $a_1 + a_2 = 1_R$. Setzt man nun $x = x_1 * a_2 + x_2 * a_1$, so ergibt sich

$$[x]_{\mathfrak{a}_1} = [x_1 * a_2 + x_2 * a_1]_{\mathfrak{a}_1} = [x_1 * (1_R - a_1) + x_2 * a_1]_{\mathfrak{a}_1} = [x_1]_{\mathfrak{a}_1}$$

und analog dazu auch $[x]_{\mathfrak{a}_2} = [x_2]_{\mathfrak{a}_2}$. Somit ist $f(x) = ([x_1]_{\mathfrak{a}_1}, [x_2]_{\mathfrak{a}_2})$, also f surjektiv für $n = 2$. Sei nun $n > 2$ und es gelte als Induktionsannahme $\bar{f} : R \to \prod_{j=1}^{n-1} R/\mathfrak{a}_j$ surjektiv. Sei $([x_i]_{\mathfrak{a}_i})_{i\in\{1,\ldots,n\}} \in \prod_{i=1}^n R/\mathfrak{a}_i$. Nach der Induktionsannahme gibt es dann ein $y \in R$ mit $\bar{f}(y) = ([x_j]_{\mathfrak{a}_j})_{j\in\{1,\ldots,n-1\}}$. Wegen Bemerkung 2.6.3 folgt aus $\mathfrak{a}_j$ teilerfremd zu $\mathfrak{a}_n$ für $j \in \{1, \ldots, n-1\}$ auch $\prod_{j=1}^{n-1} \mathfrak{a}_j = \bigcap_{j=1}^{n-1} \mathfrak{a}_j$ teilerfremd zu $\mathfrak{a}_n$. Somit gibt es Elemente $a \in \bigcap_{j=1}^{n-1} \mathfrak{a}_j$ und $b \in \mathfrak{a}_n$ mit $a + b = 1_R$. Setzt man nun $x := y * b + x_n * a$, so ergibt sich für alle $j \in \{1, \ldots, n-1\}$:

$$\begin{aligned} [x]_{\mathfrak{a}_j} &= [y * b + x_n * a]_{\mathfrak{a}_j} = [y * (1_R - a) + x_n * a]_{\mathfrak{a}_j} = [y]_{\mathfrak{a}_j} = [x_j]_{\mathfrak{a}_j} \\ [x]_{\mathfrak{a}_n} &= [y * b + x_n * a]_{\mathfrak{a}_n} = [y * b + x_n * (1_R - b)]_{\mathfrak{a}_n} = [x_n]_{\mathfrak{a}_n} \end{aligned}$$

Somit ist das Bild von x das gewünschte Element und f ist surjektiv. Damit ist die Behauptung gezeigt. □

2.7 Spezielle Matrizen

In diesem Abschnitt werden die Zeilenstufenform, die Hermite-Normalform und die Smith-Normalform von Matrizen vorgestellt. Sowohl die Hermite-Normalform als auch die Smith-Normalform sind spezielle Zeilenstufenformen. Die Hermite-Normalform wird in dieser Arbeit dafür verwendet, um aus einem Erzeugendensystems eines Zahlkörpermoduls eine eindeutige $\mathbb{Z}$-Basis des Moduls zu bestimmen. Dadurch vereinfachen sich viele algorithmische Berechnungen mit Moduln. Mit Hilfe der Smith-Normalform kann man den Index eines Faktormoduls berechnen (vergleiche Abschnitt 2.8.2). Wie bereits in der Einleitung zu Abschnitt 2.2 beschrieben, ist der Index sowohl bei der Idealzerlegung als auch bei der Invertierbarkeit von Primidealen wichtig. Im ganzen Abschnitt sei $(\mathcal{R}_\mathrm{e}, N)$ ein euklidischer Ring $\mathcal{R}_\mathrm{e}$ mit Normfunktion $N : \mathcal{R}_\mathrm{e} \setminus \{0_{\mathcal{R}_\mathrm{e}}\} \to \mathbb{N}_0$. Außerdem sei $\mathrm{Rep}(\mathcal{R}_\mathrm{e})$ ein Repräsentantensystem von $\mathcal{R}_\mathrm{e}$ bezüglich Assoziiertheit und für jedes $a \in \mathcal{R}_\mathrm{e}$ ein Repräsentantensystem $\mathrm{Rep}(\mathcal{R}_\mathrm{e}/(a)_{\mathcal{R}_\mathrm{e}})$ für den Faktorring $\mathcal{R}_\mathrm{e}/(a)_{\mathcal{R}_\mathrm{e}}$ gegeben.

2.7.1 Zeilenstufenform

Definition 2.7.1. Sei $A = (a_{ij})$ eine $m \times n$-Matrix mit Koeffizienten in $\mathcal{R}_\mathrm{e}$. Eine Zeile beziehungsweise Spalte, in der jeder Koeffizient gleich $0_{\mathcal{R}_\mathrm{e}}$ ist, heißt **Nullzeile** beziehungsweise **Nullspalte**. Definiere

$$s_i(A) := \begin{cases} 0 & \text{falls Zeile } i \text{ Nullzeile} \\ \min\{j \in \{1,\dots,n\} \mid a_{ij} \neq 0_{\mathcal{R}_\mathrm{e}}\} & \text{falls Zeile } i \text{ keine Nullzeile} \end{cases}$$

$$t_j(A) := \begin{cases} 0 & \text{falls Spalte } j \text{ Nullspalte} \\ \max\{i \in \{1,\dots,m\} \mid a_{ij} \neq 0_{\mathcal{R}_\mathrm{e}}\} & \text{falls Spalte } j \text{ keine Nullspalte} \end{cases}$$

Dann ist $s_i(A)$ der Spaltenindex des ersten Elements ungleich $0_{\mathcal{R}_\mathrm{e}}$ in der Zeile i und wird deshalb im Folgenden **i-ter Zeilenanfang** genannt. Der Wert $t_j(A)$ ist hingegen der Zeilenindex des letzten Elements ungleich $0_{\mathcal{R}_\mathrm{e}}$ in der Spalte j und wird deshalb als **j-tes Spaltenende** bezeichnet.

Definition 2.7.2. Sei $A = (a_{ij})$ eine $m \times n$-Matrix mit Koeffizienten in $\mathcal{R}_\mathrm{e}$. Dann ist A in **Zeilenstufenform**, wenn es ein $0 \leq r \leq m$ gibt, so dass die Zeilenanfänge bis Zeile r monoton aufsteigend sind und danach nur noch Nullzeilen vorkommen, das heißt es gilt

$$\begin{aligned} &s_1(A) < s_2(A) < \ldots < s_r(A) \\ &s_{r+1}(A) = s_{r+2}(A) = \ldots = s_m(A) = 0 \end{aligned}$$

Die Spalten mit den Indizes $s_1(A), \dots s_r(A)$ werden dann im Folgenden als **Stufenspalten** bezeichnet und die Elemente $a_{is_i(A)} = a_{t_{s_i(A)}(A)s_i(A)}$ als **Stufenelemente**. Jedes Stufenelement ist somit das erste Element ungleich 0 in seiner Zeile und gleichzeitig das letzte Element ungleich 0 in seiner Spalte.

Proposition 2.7.3. *Jede $m \times n$-Matrix A mit Koeffizienten in $\mathcal{R}_e$ kann mit elementaren Zeilenumformungen in Zeilenstufenform gebracht werden.*

Beweis. Zunächst stellt man fest, dass bei allen elementaren Zeilenumformungen die j-te Spalte der neuen Matrix nur von der j-ten Spalte der alten Matrix und von der Zeilenumformung abhängt. Betrachtet man sich also nur eine Spalte der Matrix, so entsprechen die elementaren Zeilenumformungen einfach Vertauschung von zwei Elementen der Spalte, Addition von einem Element der Spalte zu einem anderen Element und Multiplikation eines Elements der Spalte mit einer Einheit. Man kann also eine Variante des Euklidischen Algorithmus (vergleiche Bemerkung 2.5.2) auf eine Spalte (oder einen Teil davon) anwenden, um alle Elemente bis auf eines auf 0 zu bringen. Das letzte Element ungleich 0 ist dann der größte gemeinsame Teiler von den ursprünglichen Elementen in der Spalte (beziehungsweise dem betrachteten Teil der Spalte). Damit die Zeilenanfänge aufsteigend werden, betrachtet man zuerst die erste Spalte i_1, die keine Nullspalte ist. In dieser Spalte wendet man nun den Euklidischen Algorithmus an, um alle Elemente bis auf das Element in der ersten Zeile auf 0 zu bringen. Dabei verwendet man aber anstatt der üblichen Vertauschungen von Elementen und Addition von Elementen die entsprechenden Zeilenumformungen. Die Spalten mit Spaltenindex kleiner als i_1 sind Nullspalten, werden also durch die Operationen nicht verändert. Die erste Zeile ist nun schon in der Form, die für die Zeilenstufenform gebraucht wird. Bei den zukünftigen Operationen sollen somit keine Zeilenumformungen mehr vorkommen, die mit der ersten Zeile zu tun haben. Man betrachtet sich also nur noch die Teilmatrix, bei der die erste Zeile fehlt und wendet den Algorithmus iterativ weiter an. Dabei ist zu beachten, dass in der neuen Matrix alle Spalten mit Spaltenindex kleiner gleich i_1 Nullspalten sind. Für die Spalten kleiner i_1 ist dies klar, da diese auch mit der ersten Zeile Nullspalten sind. In der Spalte i_1 ist nach dem Euklidischen Algorithmus nur noch das erste Element ungleich 0, aber dieses wird ja zusammen mit der ersten Zeilen entfernt. Somit ist klar, dass bei der iterativen Anwendung des obigen Algorithmus auf die Teilmatrizen die Zeilenanfänge streng monoton größer werden. Insgesamt erhält man durch dieses Vorgehen eine Zeilenstufenform. □

Bemerkung 2.7.4. *Da bei der Berechnung der Hermite-Normalform zunächst auch die Zeilenstufenform berechnet wird, ist das Beispiel 4.3.2 für das Berechnen der Hermite-Normalform gleichzeitig auch ein Beispiel für das Berechnen der Zeilenstufenform. Die letzten beiden Matrizen in diesem*

Beispiel sind aber nur für die Hermite-Normalform nötig und gehören somit nicht zum Berechnen der Zeilenstufenform.

Proposition 2.7.5. *Sei U eine invertierbare $n \times n$-Matrix mit Koeffizienten in $\mathcal{R}_e$. Dann ist U ein Produkt von Elementarmatrizen.*

Beweis. Es reicht zu zeigen, dass man U durch elementare Zeilenumformungen zur Einheitsmatrix umwandeln kann, da elementare Zeilenumformungen durch Multiplikation mit einer Elementarmatrix ausgeführt werden und es zu jeder Elementarmatrix eine inverse Elementarmatrix gibt. Zunächst kann man U nach Proposition 2.7.3 mit elementaren Zeilenumformungen in Zeilenstufenform Z bringen und wegen U invertierbar ist dann auch Z invertierbar. Somit hat Z den Zeilenrang n und es gilt $\det Z \in \mathcal{R}_\mathrm{e}{}^*$. Damit ist Z eine obere Dreiecksmatrix mit Einheiten als Diagonalelemente. Durch Multiplikation der Zeilen mit entsprechenden Einheiten kann man die Diagonalelemente auf $1_{\mathcal{R}_\mathrm{e}}$ bringen. Danach kann man alle Elemente z_{in} mit $i < n$ auf $0_{\mathcal{R}_\mathrm{e}}$ bringen, indem man das z_{in}-fache der n-ten Zeile von der i-ten Zeile abzieht. Sobald alle Elemente der letzten Spalte $0_{\mathcal{R}_\mathrm{e}}$ sind (bis auf das Diagonalelement), kann man alle Elemente $z_{i,n-1}$ mit $i < n-1$ auf $0_{\mathcal{R}_\mathrm{e}}$ bringen, indem man das $z_{i,n-1}$-fache der $n-1$-ten Zeile von der i-ten Zeile abzieht. Dabei bleiben die Nullen der letzten Spalte und die Diagonalelemente erhalten. Dieses Verfahren kann man dann schrittweise für immer kleinere Spalten ausführen, bis die Matrix am Ende in Diagonalform ist. Da die Diagonalelemente alle $1_{\mathcal{R}_\mathrm{e}}$ sind, ist die Matrix dann die Einheitsmatrix. Dabei wurden im ganzen Verfahren nur elementare Zeilenumformungen angewendet, also ist U ein Produkt von Elementarmatrizen. □

Definition 2.7.6. Sei A eine $m \times n$-Matrix mit Koeffizienten in $\mathcal{R}_\mathrm{e}$ und $\mathfrak{m}$ der Modul in $\mathcal{R}_\mathrm{e}^n$, der von den Zeilen von A erzeugt wird. Dann wird $\mathfrak{m}$ im Folgenden als **Zeilenmodul** von A bezeichnet.

Proposition 2.7.7. *Elementare Zeilenumformungen ändern den Zeilenmodul einer Matrix nicht.*

Beweis. Sei A die ursprüngliche Matrix mit Zeilen z_i und $\bar{A}$ eine Matrix mit Zeilen $\bar{z}_i$, die aus A durch eine elementare Zeilenumformung entsteht. Es muss für jede elementare Zeilenumformung gezeigt werden, dass der Modul $\mathfrak{m}$ erzeugt von den Zeilen z_i und der Modul $\bar{\mathfrak{m}}$ erzeugt von den Zeilen $\bar{z}_i$ gleich sind. Dafür reicht es zu zeigen, dass jede Zeile von $\bar{\mathfrak{m}}$ eine $\mathcal{R}_\mathrm{e}$-Linearkombination von Zeilen von $\mathfrak{m}$ ist und somit $\bar{\mathfrak{m}} \subset \mathfrak{m}$ gilt. Da jede elementare Zeilenumformung eine inverse Zeilenumformung hat, gilt dann auch die Inklusion in die andere Richtung und somit die Gleichheit der Moduln.

Sei zunächst $\bar{A}$ durch eine Zeilenvertauschung erzeugt. Dann sind die Zeilen $\bar{z}_i$ nur eine Permutation der Zeilen z_i, also ist jede Zeile leicht als Linearkombination der Zeilen des anderen Moduls darstellbar (mit nur einem

Koeffizienten 1 und den anderen Koeffizienten 0). Somit sind die Moduln $\mathfrak{m}$ und $\bar{\mathfrak{m}}$ gleich.

Nun sei $\bar{A}$ durch Multiplikation einer Zeile mit einer Einheit $e \in \mathcal{R}_\mathrm{e}{}^*$ entstanden. Da schon gezeigt wurde, dass Vertauschungen der Zeilen nichts am Modul ändern, kann man ohne Beschränkung der Allgemeinheit annehmen, dass $\bar{z}_1 = e * z_1$ gilt und ansonsten $\bar{z}_i = z_i$ gilt. Damit wurden alle $\bar{z}_i$ als $\mathcal{R}_\mathrm{e}$-Linearkombinationen der z_i dargestellt.

Als letztes sei ohne Beschränkung der Allgemeinheit $\bar{z}_1 = z_1 + r * z_2$, da Zeilenvertauschungen schon gezeigt wurden (und für alle $i \neq 1$ wieder $\bar{z}_i = z_i$). Dann sind auch in diesem Fall alle $\bar{z}_i$ als $\mathcal{R}_\mathrm{e}$-Linearkombinationen der z_i dargestellt.

□

Korollar 2.7.8. *Sei A eine $m \times n$-Matrix und U eine invertierbare $m \times m$-Matrix. Dann erzeugen A und $U * A$ den gleichen Zeilenmodul.*

Beweis. Nach Proposition 2.7.5 ist die invertierbare Matrix U ein Produkt von Elementarmatrizen. Da U von links an A multipliziert wird, entsteht also $U * A$ aus A durch elementare Zeilenumformungen. Nach Proposition 2.7.7 sind also auch der Zeilenmodul von A und der Zeilenmodul von $U * A$ gleich. □

Lemma 2.7.9. *Sei A eine Matrix und B eine Zeilenstufenform von A. Dann sind die Zeilen (ausgenommen Nullzeilen) von B eine $\mathcal{R}_e$-Basis für Zeilenmodul $\mathfrak{m}$ von A. Insbesondere ist der (Zeilen-)Rang von B gleich dem Rang des Moduls $\mathfrak{m}$.*

Beweis. Die Zeilenstufenform entsteht aus A durch elementare Zeilenumformungen. Diese verändern nach Proposition 2.7.7 den Zeilenmodul nicht. Somit erzeugen die Zeilen z_i von B den gleichen Modul wie die Zeilen von A. Es ist noch zu zeigen, dass die Zeilen von B linear unabhängig sind. Sei $\sum_{i=1}^{\mathrm{rg}(B)} a_i * z_i$ eine $\mathcal{R}_\mathrm{e}$-Linearkombination vom Nullvektor. Dann muss zunächst der Koeffizient a_1 gleich 0 sein, da die $s_1(B)$-te Koordinate in der ersten Zeile ungleich 0 ist und in allen weiteren Zeilen diese Koordinate gleich 0 ist (da die Zeilenanfänge streng monoton aufsteigend sind). Somit gilt schon $\sum_{i=2}^{\mathrm{rg}(B)} a_i * z_i = 0_{\mathcal{R}_\mathrm{e}^n}$. Dies lässt sich nun induktiv für jede weitere Zeile fortsetzen, da nun in den verbliebenen Zeilen der Summe der Vektor z_2 als einziger einen Wert ungleich 0 in der $s_2(B)$-ten Koordinate hat. Es werden somit insgesamt alle Koeffizienten gleich 0. Somit gibt es nur die triviale Linearkombination der $0_{\mathcal{R}_\mathrm{e}^n}$, also sind die Zeilen linear unabhängig. Die nicht-Nullzeilen von B sind also eine Basis des Zeilenmoduls von B und somit eine Basis vom Zeilenmodul $\mathfrak{m}$ von A. Die Anzahl der nicht-Nullzeilen von B ist also sowohl die Größe der Basis von B als auch der Rang der Matrix B. □

2.7.2 Hermite-Normalform

Definition 2.7.10. Sei $A = (a_{ij})$ eine $m \times n$-Matrix mit Koeffizienten in $\mathcal{R}_\mathrm{e}$. Dann heißt die j-te Spalte **normiert**, wenn sie entweder eine Nullspalte ist oder eine Stufenspalte, bei der das Stufenelement $a := a_{t_j(A)j}$ in $\mathrm{Rep}(\mathcal{R}_\mathrm{e})$ und alle anderen Elemente der Spalte in $\mathrm{Rep}(\mathcal{R}_\mathrm{e}/(a)_{\mathcal{R}_\mathrm{e}})$ liegt.

Definition 2.7.11. Eine Matrix A mit Koeffizienten in $\mathcal{R}_\mathrm{e}$ ist in **Hermite-Normalform**, wenn die folgenden Eigenschaften erfüllt sind:

(i) A ist in Zeilenstufenform

(ii) Die Stufenspalten sind normiert.

Eine Matrix B ist eine **Hermite-Normalform** einer Matrix A, wenn B in Hermite-Normalform ist und es eine invertierbare Matrix U mit $B = U * A$ gibt.

Theorem 2.7.12. *Sei A eine Matrix. Dann gibt es eine Hermite-Normalform von A.*

Beweis. Zunächst kann man A nach Proposition 2.7.3 durch elementare Zeilenumformungen in Zeilenstufenform bringen. Nun muss man nur noch die Stufenspalten normieren. Dafür multipliziert man die Zeilen mit entsprechenden Einheiten, um die Stufenelemente zu Elementen im Repräsentantensystem von $\mathcal{R}_\mathrm{e}$ umzuwandeln. Dann geht man die Stufenspalten in aufsteigender Reihenfolge durch und addiert zu jeder Zeile das entsprechende Vielfache der Zeile des Stufenelements, damit die entsprechenden Elemente in der Stufenspalte im Repräsentantensystem sind. Dabei werden die Stufenelemente nicht verändert und wegen der Zeilenstufenform auch die Elemente der höheren Stufenspalten nicht verändert. Insgesamt bekommt man auf diese Weise normierte Stufenspalten und die Behauptung ist gezeigt, da nur elementare Zeilenumformungen verwendet wurden und somit jeder Schritt durch Linksmultiplikation von einer (invertierbaren) Elementarmatrix ausgeführt werden kann. Multipliziert man also die Elementarmatrizen der einzelnen Schritte in der richtigen Reihenfolge, so erhält man eine invertierbare Matrix U, so dass $U * A$ eine Hermite-Normalform ist. □

Bemerkung 2.7.13. *Das Verfahren für das Berechnen der Hermite-Normalform wird in Algorithmus 4.3.1 nochmal genauer definiert und dann an einem Beispiel durchgeführt.*

Theorem 2.7.14. *Die Zeilen von zwei verschiedenen Hermite-Normalformen H, $\bar{H}$ erzeugen unterschiedliche $\mathcal{R}_e$-Moduln in $\mathcal{R}_e^n$.*

Beweis. Es werden die folgenden Fälle überprüft:

1. H und $\bar{H}$ haben unterschiedlichen Rang.

2. Rang ist gleich, aber Zeilenanfänge sind verschieden.

3. Zeilenanfänge und Rang sind gleich, aber Stufenelemente sind verschieden.

4. Stufenelemente, Zeilenanfänge und Rang sind gleich, aber ein anderes Element ist verschieden.

Dies deckt alle Fälle ab, in denen H und $\bar{H}$ nicht gleich sind. Es ist jeweils zu zeigen, dass der Zeilenmodul von H nicht gleich dem Zeilenmodul von $\bar{H}$ ist.

1. Da H und $\bar{H}$ in Zeilenstufenform sind, haben die Zeilenmoduln von H und $\bar{H}$ nach Lemma 2.7.9 den gleichen Rang wie die Matrizen H und $\bar{H}$. Somit haben die Zeilenmoduln unterschiedliche Ränge, sind also verschieden.

2. Sei m der Rang von H und $\bar{H}$, $z_1, \ldots, z_m$ die Zeilen von H und $\bar{z}_1, \ldots, \bar{z}_m$ die Zeilen von $\bar{H}$. Es sei $\pi_i : \mathbb{Z}^n \to Z_i := \mathbb{Z}$ die Projektion auf die i-te Koordinate und

$$f := \pi_1 \times \ldots \times \pi_{s_{i_0}(H)} : \mathbb{Z}^n \to \mathbb{Z}^r = Z_1 \times Z_2 \times \ldots \times Z_{s_{i_0}(H)}$$

   die Projektion auf die ersten $s_{i_0}(H)$ Koordinaten, wobei i_0 der erste Zeilenanfang ist, der sich unterscheidet und ohne Beschränkung der Allgemeinheit $s_{i_0}(H) < s_{i_0}(\bar{H})$ gilt. Die Zeilenanfänge sind streng monoton aufsteigend, also gilt für die Bilder der Zeilen z_i von H und die Bilder der Zeilen $\bar{z}_i$ folgendes:

   (a) $B := \{f(z_1), f(z_2), \ldots, f(z_{i_0})\}$ linear unabhängig
   (b) $f(z_{i_0+1}) = f(z_{i_0+2}) = \ldots = f(z_m) = 0$
   (c) $\bar{B} := \{f(\bar{z}_1), f(\bar{z}_2), \ldots, f(\bar{z}_{i_0-1})\}$ linear unabhängig
   (d) $f(\bar{z}_{i_0}) = f(\bar{z}_{i_0+1}) = \ldots = f(\bar{z}_m) = 0$

   Somit bildet f den Zeilenmodul von H auf einen i_0-dimensionalen Modul in $\mathbb{Z}^r$ ab (mit der Basis B), während der Zeilenmodul von $\bar{H}$ unter der gleichen Abbildung f nur auf einen $i_0 - 1$-dimensionalen Modul in $\mathbb{Z}^r$ abgebildet wird (mit der Basis $\bar{B}$). Da f ein Homomorphismus ist, muss schon der Ursprungsmodul unterschiedlich gewesen sein.

3. Sei $a_k := h_{is_k(H)}$ das Stufenelement von $H = (h_{ij})$ in Zeile k und $\bar{a}_k := \bar{h}_{is_k(\bar{H})}$ das entsprechende Stufenelement von $\bar{H}$. Da die Zeilenanfänge gleich sind, befinden sich a_k und $\bar{a}_k$ an den gleichen Positionen. Angenommen die beiden Matrizen würden den gleichen Zeilenmodul erzeugen. Dann ist die k-te Zeile $z_k = (0, \ldots, 0, a_k, *, \ldots, *)$ von H eine $\mathcal{R}_e$ Linearkombination von den Zeilen $\bar{z}_i$ von $\bar{H}$, also

$z_k = \sum_{i=0}^{m} b_i * \bar{z}_i$ für Elemente $b_i \in \mathcal{R}_\mathrm{e}$. Dann müssen zunächst alle b_i mit $i < s_k(H)$ gleich 0 sein, da ansonsten (wegen der Zeilenstufenform) in z_k nicht nur Nullen vor a_k stehen würden. Außerdem verändern die Koeffizienten b_i mit $i > s_k(H)$ nichts an dem Wert a_k. Somit ist der Wert a_k nur abhängig vom Koeffizienten b_k und es muss $a_k = b_k * \bar{a}_k$ gelten. Außerdem ist die k-te Zeile von $\bar{H}$ eine $\mathcal{R}_\mathrm{e}$-Linearkombination von den Zeilen z_i von H und es folgt ganz analog zu vorher, dass es ein $\bar{b}_k \in \mathcal{R}_\mathrm{e}$ gibt mit $\bar{a}_k = \bar{b}_k * a_k$. Es ist also $a_k = b_k * \bar{b}_k * a_k$, also wegen $\mathcal{R}_\mathrm{e}$ Integritätsring auch $b_k \in \mathcal{R}_\mathrm{e}{}^*$. Dann ist aber a_k assoziiert zu $\bar{a}_k$. In der Hermite-Normalform sind aber alle Stufenelemente im Repräsentantensystem bezüglich Assoziiertheit, also gilt sogar $a_k = \bar{a}_k$. Somit sind alle Stufenelemente gleich, falls der gleiche Zeilenmodul erzeugt wird. Dies bedeutet aber umgekehrt auch, dass nicht der gleiche Zeilenmodul erzeugt wird, falls ein Stufenelement verschieden ist, also ist dieser Fall auch gezeigt.

4. Sei j der Index der ersten Spalte, in der sich die Matrizen unterscheiden und i minimal, so dass $h_{ij} \neq \bar{h}_{ij}$ gilt. Angenommen die Zeile z_i ist eine Linearkombination $\sum_{k=1}^{m} b_k * \bar{z}_k$. Dann müssen zunächst die Koeffizienten b_k für $k < i$ gleich 0 sein, da die Werte vor dem Zeilenanfang in z_i gleich 0 sein müssen. Der Koeffizient b_i muss gleich 1 sein, damit der Zeilenanfang von z_i richtig ist. Außerdem müssen alle Koeffizienten b_k mit $s_k(H) < j$ gleich 0 sein, damit die Elemente links von h_{ij} stimmen (in diesen Spalten sind die Werte von H und $\bar{H}$ noch gleich). Nun gibt es zwei Fälle: Entweder es gibt einen Zeilenanfang $s_{k_0}(H) = j$ oder der nächste Zeilenanfang ist schon größer als j. Im zweiten Fall ist h_{ij} allein durch $\bar{h}_{ij}$, da alle weiteren Elemente der Spalte den Wert 0 oder Koeffizienten 0 haben und es gilt $h_{ij} = b_i * \bar{h}_{ij} = \bar{h}_{ij}$. Dies ist ein Widerspruch dazu, dass $h_{ij} \neq \bar{h}_{ij}$ ist. Im anderen Fall ist unter h_{ij} noch ein Zeilenanfang, der einen unbekannten Koeffizienten b_{k_0} haben kann. Es gilt dann aber $h_{ij} = b_i * \bar{h}_{ij} + b_{k_0} * \bar{h}_{k_0 j}$. Somit sind h_{ij} und $\bar{h}_{ij}$ nur um ein Vielfaches ihres Stufenelements verschieden und somit in der gleichen Äquivalenzklasse modulo ihres Stufenelements. Wegen den Eigenschaften der Hermite-Normalform muss aber sowohl h_{ij} als auch $\bar{h}_{ij}$ im entsprechenden Repräsentantensystem modulo der Äquivalenzklasse ihres Stufenelements sein, also gilt insbesondere $h_{ij} = \bar{h}_{ij}$. Dies ist wieder ein Widerspruch zur Annahme $h_{ij} \neq \bar{h}_{ij}$. Somit kann es nur dann unterschiedliche Elemente geben, wenn mindestens eine Zeile von H keine Linearkombination der Zeilen von $\bar{H}$ ist. Und dies kann nur der Fall sein, wenn die Zeilenmoduln von H und $\bar{H}$ unterschiedlich sind.

□

Korollar 2.7.15. *Zwei $m \times n$-Matrizen A, $\bar{A}$ erzeugen genau dann den gleichen Zeilenmodul, wenn für jede Hermite-Normalform H von A und jede Hermite-Normalform $\bar{H}$ von $\bar{A}$ auch $H = \bar{H}$ gilt. Insbesondere ist die Hermite-Normalform einer Matrix eindeutig.*

Beweis. Da die Hermite-Normalform durch elementare Zeilenumformungen entsteht, erzeugt die Hermite-Normalform H nach Proposition 2.7.7 den gleichen Zeilenmodul wie die Matrix A. Ebenso erzeugen $\bar{A}$ und $\bar{H}$ den gleichen Zeilenmodul. Nach Theorem 2.7.14 werden außerdem von verschiedenen Hermite-Normalformen auch verschiedene Zeilenmoduln erzeugt (und von gleichen Hermite-Normalformen natürlich auch gleiche Zeilenmoduln). Somit sind die Zeilenmoduln von A und $\bar{A}$ genau dann gleich, wenn die Hermite-Normalformen H und $\bar{H}$ gleich sind. □

2.7.3 Smith-Normalform

Definition 2.7.16. Eine Matrix A ist in **Smith-Normalform**, wenn sie in Hauptdiagonalform ist und jedes Hauptdiagonalelement a_{ii} das darauffolgende Hauptdiagonalelement $a_{i+1,i+1}$ teilt. Außerdem soll jedes Hauptdiagonalelement im Repräsentantensystem liegen. Eine Matrix S heißt **Smith-Normalform** einer Matrix B, wenn S in Smith-Normalform ist und es invertierbare Matrizen U, V gibt mit $S = U * B * V$.

Theorem 2.7.17. *Jede Matrix A hat eine Smith-Normalform und kann durch elementare Zeilen- und Spaltenumformungen in diese gebracht werden.*

Beweis. Ähnlich wie im Beweis zur Existenz der Zeilenstufenform stellt man fest, dass bei elementaren Spaltenumformungen (Zeilenumformungen) die i-te Zeile (j-te Spalte) nur von der i-ten Zeile (j-ten Spalte) der alten Matrix und von der Spaltenumformung (Zeilenumformung) abhängt. Man kann also wieder entsprechende Varianten des Euklidischen Algorithmus anwenden. Dabei ist jedoch zu beachten, dass sich Zeilenumformungen und Spaltenumformungen gegenseitig beeinflussen. Bringt man also zunächst eine Zeile in die Form mit nur einem Element ungleich 0 und danach eine Spalte in die Form mit nur einem Element ungleich 0, so hat man dabei vermutlich wieder die vorher fertige Zeile verändert. Wendet man jedoch die Algorithmen abwechselnd auf eine Zeile und eine Spalte mit dem gleichen Index s an, so wird sowohl beim Euklidischen Algorithmus der Zeile als auch beim Euklidischen Algorithmus der Spalte das Element a_{ss} durch ein Element mit geringerer Norm ersetzt. Somit müssen irgendwann sowohl der Zeilenalgorithmus als auch der Spaltenalgorithmus terminieren, das heißt das Element a_{ss} ist dann sowohl in der Zeile s als auch in der Spalte s das einzige Element ungleich 0. Mit diesem Verfahren bekommt man schonmal eine Matrix in Hauptdiagonalform, wenn man mit $s = 1$ beginnt und danach s immer um 1 erhöht.

Da aber für die Smith-Normalform zusätzlich gefordert ist, dass die Hauptdiagonalelemente jeweils das folgende Hauptdiagonalelement teilen, muss man vor der Erhöhung von s noch dafür sorgen, dass $a_{s-1,s-1}$ das Element a_{ss} teilt. Ist dies nicht der Fall, so addiert man einfach die s-te Zeile zur $(s-1)$-ten Zeile und wendet wieder das Euklidische Verfahren für die Zeile und Spalte $s-1$ an. Da $a_{s-1,s-1}$ das Element a_{ss} nicht geteilt hat, bekommt man dadurch wieder ein neues Element $a_{s-1,s-1}$ mit kleinerer Norm. Da sich $a_{s-1,s-1}$ nun verändert hat, muss man nun auch wieder prüfen, ob $a_{s-2,s-2}$ das Element $a_{s-1,s-1}$ teilt und das Verfahren entsprechend fortsetzen. Irgendwann müssen jedoch alle $a_{i-1,i-1}$ die folgenden Elemente a_{ii} teilen für alle $i <= s$, da man ansonsten wegen der Verringerung der Norm eines der $a_{i-1,i-1}$ in jedem Schritt wieder eine unendliche streng monoton absteigende Folge von natürlichen Zahlen bilden könnte, was nicht möglich ist. Sobald die Teilbarkeitsbedingung für alle $i <= s$ erfüllt ist, kann man s wieder um 1 erhöhen. Irgendwann erreicht s einen der Ränder der Matrix und man muss nur noch jede Zeile mit entsprechenden Einheiten multiplizieren, um die Hauptdiagonalelemente ins Repräsentantensystem zu bringen. Dann ist die Matrix in der gewünschten Form. Insgesamt werden im Algorithmus nur elementare Zeilen- und Spaltenumformungen durchgeführt, also ergibt sich die Matrix durch Multiplikation von invertierbaren Matrizen (von beiden Seiten). □

Bemerkung 2.7.18. *Das Verfahren für das Berechnen der Smith-Normalform wird in Algorithmus 4.3.2 nochmal genauer definiert und dann an einem Beispiel durchgeführt.*

Definition 2.7.19. Sei A eine $m \times n$-Matrix und B eine $k \times k$-Untermatrix von A. Dann nennt man die Determinante von B einen **k-Minor** von A. Im Folgenden sei $M_k(A)$ die Menge aller k-Minoren von A.

Lemma 2.7.20. *Sei A eine $m \times n$-Matrix und U eine invertierbare $m \times m$-Matrix. Dann gilt $ggT(M_k(A)) = ggT(M_k(U * A))$.*

Beweis. Nach Proposition 2.7.5 ist U ein Produkt von Elementarmatrizen. Es reicht also zu zeigen, dass die Aussage für Elementarmatrizen gilt. Multiplikation einer Elementarmatrix von links entspricht einer elementaren Zeilenumformung. Bei Zeilenvertauschungen ist die Aussage klar, da die Menge der $k \times k$-Untermatrizen und somit die Menge der k-Minoren gleich bleibt (die Untermatrizen werden höchstens in einer anderen Reihenfolge aufgeschrieben). Wird eine Zeile mit einer Einheit e multipliziert, so werden einige Minoren mit e multipliziert. Dadurch ändert sich aber der größte gemeinsame Teiler nicht. Sei also nun $A = (z_1, \ldots, z_n)$ und ohne Beschränkung der Allgemeinheit $U * A = (z_1 + z_2, \ldots, z_n)$. Dann werden nur die Untermatrizen verändert, die (einen Teil von) z_1 enthalten. Wegen der Linearität der Determinante in jeder Zeile gilt aber für einen Minor

$$d = \det(\bar{z}_1 + \bar{z}_2, \bar{z}_{i_2}, \ldots, \bar{z}_{i_k}) = \det(\bar{z}_1, \bar{z}_{i_2}, \ldots, \bar{z}_{i_k}) + \det(\bar{z}_2, \bar{z}_{i_2}, \ldots, \bar{z}_{i_k}),$$

wobei $\bar{z}_i$ jeweils die auf bestimmte k Spalten verkürzten Zeilen sind und $1 \neq i_2 \neq i_3 \neq \ldots \neq i_k$ gilt. Falls ein i_j gleich 2 ist, so fällt der zweite Summand weg (da eine Matrix mit zwei gleichen Zeilen die Determinante 0 hat). In beiden Fällen ist aber der k-Minor d der Matrix $U * A$ eine Summe von k-Minoren der Matrix A (dabei hat die Summe entweder einen oder zwei Summanden). Die Summe erhält gemeinsame Teiler, wobei damit gemeint ist, dass jeder gemeinsamer Teiler von einer Menge von Elementen auch ein Teiler von beliebigen Summen dieser Elemente ist. Somit teilt $\mathrm{ggT}(M_k(A))$ jeden Minor in $M_k(U * A)$ und damit auch den größten gemeinsamen Teiler der Minoren in $M_k(U * A)$. Es gilt also bei der Addition von Vielfachen von Zeilen $\mathrm{ggT}(M_k(A)) \mid \mathrm{ggT}(M_k(U * A))$. Da auch U^{-1} eine invertierbare Matrix ist, folgt analog dazu auch

$$\mathrm{ggT}(M_k(U * A)) \mid \mathrm{ggT}(M_k(U^{-1} * U * A)) = \mathrm{ggT}(M_k(A)).$$

Somit bleibt bei allen elementaren Zeilenumformungen der größte gemeinsame Teiler der k-Minoren erhalten und damit auch bei Multiplikation mit einer invertierbaren Matrix von links. □

Bemerkung 2.7.21. *Die Aussage von Lemma 2.7.20 gilt auch bei der Multiplikation einer inversen $n \times n$-Matrix von rechts. Der Beweis ist analog, nur verwendet man dann elementare Spaltenumformungen und die Linearität der Determinanten in jeder Spalte.*

Theorem 2.7.22. *Die Smith-Normalform einer Matrix A ist eindeutig.*

Beweis. Sei S eine Smith-Normalform von A. Dann gilt $S = U * A * V$ für invertierbare Matrizen U, V. Nach Lemma 2.7.20 und der darauffolgenden Bemerkung gilt dann

$$\mathrm{ggT}(M_k(A)) = \mathrm{ggT}(M_k(U * A)) = \mathrm{ggT}(M_k(U * A * V)) = \mathrm{ggT}(M_k(S)).$$

Der größte gemeinsame Teiler der k-Minoren ist also bei A und S gleich. In der Smith-Normalform lassen sich aber die k-Minoren ungleich 0 einfach bestimmen, da sie die Produkte von je k Diagonalelementen sind. Wegen der Teilerbedingung zwischen den Diagonalelementen ist dann der größte gemeinsame Teiler $d_k(S)$ jeweils das Produkt der ersten k Diagonalelemente (bis auf Multiplikation mit Einheiten). Ist also $S = (s_{ij})$, so erhält man die Gleichung

$$d_k(S) = \prod_{i=1}^{k} s_{ii}.$$

Daraus ergibt sich aber (bis auf Multiplikation mit Einheiten)

$$\begin{aligned} s_{11} &= d_1(S) \\ s_{22} &= \frac{d_2(S)}{d_1(S)} \\ &\dots \\ s_{kk} &= \frac{d_k(S)}{d_{k-1}(S)} \end{aligned}$$

Damit sind die Diagonalelemente von S durch die $d_k(S) = d_k(A)$ und somit durch die Matrix A bis auf Einheiten eindeutig bestimmt. Da aber die Diagonalelemente im Repräsentantensystem liegen müssen, sind die Diagonalelemente bei verschiedenen Smith-Normalformen der Matrix A gleich und somit ist die Smith-Normalform sogar eindeutig bestimmt. □

2.8 Eigenschaften von Moduln/Ringen/Algebren

In diesem Abschnitt werden die Eigenschaften „noethersch“, „artinsch“, „einfach“ und „halbeinfach“ und die Begriffe des „Nilradikals“ und des „Jacobson-Radikals“ eingeführt. Viele von den Sätzen dieses Abschnittes werden nur benötigt, um bestimmte Hauptergebnisse zu beweisen, die im weiteren Verlauf der Arbeit eine wichtige Bedeutung haben. Es wird am Anfang der Unterabschnitte jeweils darauf hingewiesen, welche Hauptergebnisse in den entsprechenden Unterabschnitten vorkommen. Der Begriff noethersch ist vor allem deswegen wichtig, weil in einem noetherschen Ring alle Ideale endlich erzeugt sind. Es wird in Proposition 3.1.13 noch gezeigt werden, dass jede Ordnung noethersch ist. Der Begriff „endlich erzeugt“ ist deshalb wichtig, weil Moduln und Ideale in Zahlkörpern als endlich erzeugt vorausgesetzt werden. Außerdem kann man mit endlich erzeugten Moduln einfacher rechnen. Die Eigenschaft „artinsch“ und die Radikale werden vor allem für die Sätze zu den Begriffen „halbeinfach“ und „einfach“ benötigt. Diese Sätze bereiten wiederum einen Algorithmus vor, der eine bestimmte Faktoralgebra einer endlich-dimensionalen $\mathbb{F}_p$-Algebra in eine direkte Summe von Körpern zerlegt. In den weiteren Kapiteln wird dieser Algorithmus näher ausgeführt und gezeigt, dass er wichtig für die Bestimmung von Primidealen in einer Ordnung ist (vergleiche Algorithmus 4.3.7 und Algorithmus 4.3.8).

Definition 2.8.1. Sei M ein R-Modul. Man nennt M:

(i) **noethersch**, falls jede aufsteigende Kette (M_i) von Untermoduln stationär wird.

(ii) **artinsch**, falls jede absteigende Kette (M_i) von Untermoduln stationär wird.

(iii) **einfach**, falls $\{0\}$ und M die einzigen Untermoduln von M sind.

(iv) **halbeinfach**, falls M eine direkte Summe von einfachen Moduln ist.

Bemerkung 2.8.2. *Für eine R-Algebra A benutzt man die obigen Begriffe, wenn die Algebra als R-Modul die Voraussetzungen erfüllt.*

Definition 2.8.3. Ein Ring R heißt **noethersch** beziehungsweise **artinsch**, wenn er als kanonischer R-Modul noethersch beziehungsweise artinsch ist. Es muss also jede aufsteigende beziehungsweise absteigende Kette von Idealen stationär werden.

2.8.1 Noethersch und artinsch

Eines der Hauptergebnisse dieses Abschnittes ist ein Theorem, das besagt, dass die Eigenschaft „noethersch“ dazu äquivalent ist, dass alle Untermoduln von M endlich erzeugt sind. Die weiteren Sätze des Abschnittes sind Vorbereitungen für die Beweise der folgenden Abschnitte und für den Beweis, dass jede Ordnung in einem Zahlkörper noethersch ist. Die Beweise in diesem Abschnitt orientieren sich teilweise an Beweisen in [BBR09, S.1-14] und [NW10, S.74-88].

Theorem 2.8.4. *Sei M ein R-Modul. Dann sind die folgenden Aussagen äquivalent:*

(i) M ist noethersch.

(ii) Jeder Untermodul von M ist endlich erzeugt.

Beweis. Sei zunächst M noethersch und $N \subset M$ ein Untermodul von M. Sei $\mathcal{N}$ die Menge aller endlich erzeugten Untermoduln von N. Dann sind alle Elemente in $\mathcal{N}$ auch Untermoduln von M. Da M noethersch ist, wird also jede aufsteigende Kette von Elementen aus $\mathcal{N}$ stationär, hat also insbesondere eine obere Schranke. Nach dem Lemma von Zorn gibt es also ein maximales Element N_0 in $\mathcal{N}$. Da N_0 in N enthalten und endlich erzeugt ist, ist auch $N_0 + x * R$ in N enthalten und endlich erzeugt für alle $x \in N$. Es ist also auch $N_0 + x * R$ in $\mathcal{N}$ und wegen der Maximalität von N_0 folgt $N_0 = N_0 + x * R$. Damit ist aber auch $N_0 = N_0 + N = N$ und somit ist N endlich erzeugt. Sei nun umgekehrt jeder Untermodul von M endlich erzeugt. Sei $(N_i)_{i\in\mathbb{N}}$ eine aufsteigende Kette von Untermoduln von M. Dann ist auch $N = \bigcup_{i=1}^{\infty} N_i$ ein Untermodul von M und somit nach Voraussetzung endlich erzeugt. Da jeder Erzeuger von N in einem der N_i vorkommt und es nur endlich viele Erzeuger sind, gibt es ein i_0, so dass $N \subset N_{i_0}$ gilt. Dann ist aber $N = N_{i_0}$ und somit auch $N = N_i$ für alle $i >= i_0$. Somit wird die Kette ab i_0 stationär und es folgt, dass M noethersch ist. □

Beispiel 2.8.5. Sei R ein Hauptidealring. Dann ist R noethersch.

Beweis. Die Untermoduln von R entsprechen den Idealen in R. Da R ein Hauptidealring ist, ist jedes Ideal von einem Element erzeugt, also insbesondere endlich erzeugt. Nach Theorem 2.8.4 folgt also, dass R noethersch ist. □

Beispiel 2.8.6. Jeder Körper K ist noethersch und artinsch als kanonischer K-Modul.

Beweis. Da K ein Körper ist, sind die einzigen Ideale von K (und somit die einzigen K-Untermoduln von K) das Nullideal und das Einheitsideal. Es ist klar, dass dann jede monoton absteigende oder aufsteigende Kette von Untermoduln in K stationär wird. □

Definition 2.8.7. Seien $M_1, \ldots, M_k$ R-Moduln und $f_i : M_i \to M_{i+1}$ Homomorphismen für $i \in \{1, \ldots, k-1\}$. Dann heißt die Sequenz

$$M_1 \xrightarrow{f_1} M_2 \xrightarrow{f_2} \ldots \xrightarrow{f_{k-1}} M_k$$

exakt an der Stelle i, falls in M_i die Gleichung $f_{i-1}(M_{i-1}) = \ker f_i$ gilt. Die ganze Sequenz heißt **exakt**, wenn sie an allen Stellen $i \in \{2, \ldots, k-1\}$ exakt ist.

Proposition 2.8.8. *Gegeben sei die exakte Sequenz*

$$0 \longrightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0$$

von R-Moduln. Dann ist M genau dann noethersch beziehungsweise artinsch wenn M' und M'' noethersch beziehungsweise artinsch sind.

Beweis. Die Beweise für artinsch und noethersch sind vollkommen analog. Man muss nur überall den Begriff noethersch durch den Begriff artinsch ersetzen und alle Teilmengenrelationen umkehren (insbesondere müssen aufsteigende Ketten durch absteigende Ketten ersetzt werden). Deswegen wird hier die Aussage nur für noethersch bewiesen. Sei zunächst M noethersch. Sei $(\mathfrak{m}'_i)_{i\in\mathbb{N}}$ eine aufsteigende Kette von Untermoduln von M'. Dann sind die $\mathfrak{m}_i := f(\mathfrak{m}'_i)$ Untermoduln von M, da f ein Homomorphismus ist. Diese bilden eine aufsteigende Kette in M und da M noethersch ist, muss die Kette stationär werden. Es gibt also ein $i_0 \in \mathbb{N}$ mit $\mathfrak{m}_i = \mathfrak{m}_{i_0}$ für alle $i \geq i_0$. Wegen der exakten Sequenz ist f injektiv, also gibt es für jedes Element x in $f(M')$ genau ein Element in M', das auf x abgebildet wird. Somit gilt $f^{-1} \circ f = \mathrm{Id}(M')$, wobei f^{-1} das Urbild von f ist. Daraus folgt aber, dass die Urbilder der $\mathfrak{m}_i$ die $\mathfrak{m}'_i$ sind und somit auch $\mathfrak{m}'_i = \mathfrak{m}'_{i_0}$ für alle $i \geq i_0$. Also ist auch M' noethersch. Sei nun $(\mathfrak{m}''_i)_{i\in\mathbb{N}}$ eine absteigende Kette von Untermoduln von M''. Dann sind die Urbilder $\mathfrak{n}_i := g^{-1}(\mathfrak{m}''_i)$ Untermoduln von M. Diese Kette in M wird stationär, also gibt es ein $i_1 \in \mathbb{N}$ mit $\mathfrak{n}_i = \mathfrak{n}_{i_1}$

für alle $i \geq i_1$. Wegen der exakten Sequenz ist g surjektiv, also gibt es für jedes Element x in M'' ein Element in M, das auf x abgebildet wird. Somit ist das Bild jedes Untermoduls $\mathfrak{n}_i$ wieder der ursprüngliche Modul $\mathfrak{m}_i''$ und es folgt $\mathfrak{m}_i'' = \mathfrak{m}_{i_1}''$ für alle $i \geq i_1$. Also ist auch M'' noethersch. Seien nun umgekehrt M'' und M' noethersch. Sei $(\mathfrak{m}_i)_{i\in\mathbb{N}}$ eine Kette von Untermoduln von M. Dann sind die Urbilder $\mathfrak{m}_i' := f^{-1}(\mathfrak{m}_i)$ und die Bilder $\mathfrak{m}_i'' := g(\mathfrak{m}_i)$ Untermoduln von M' beziehungsweise M''. Da M' und M'' noethersch sind, gibt es also $i_0 \in \mathbb{N}$ und $i_1 \in \mathbb{N}$ mit $\mathfrak{m}_i' = \mathfrak{m}_{i_0}'$ und $\mathfrak{m}_j'' = \mathfrak{m}_{i_1}''$ für alle $i \geq i_0$ und alle $j \geq i_1$. Sei $i_2 := \max(i_0, i_1)$. Es ist zu zeigen, dass $\mathfrak{m}_i = \mathfrak{m}_{i_2}$ für alle $i \geq i_2$ gilt. Die Teilmengenrelation $\mathfrak{m}_{i_2} \subset \mathfrak{m}_i$ ist bereits bekannt, da die $\mathfrak{m}_i$ eine aufsteigende Kette bilden. Sei also nun $x \in \mathfrak{m}_i$ für ein $i \geq i_2$. Dann ist $g(x) \in \mathfrak{m}_i'' = \mathfrak{m}_{i_2}''$. Somit gibt es ein $x_2 \in \mathfrak{m}_{i_2}$ mit $g(x_2) = g(x)$. Dann gilt aber wegen g Homomorphismus auch $g(x - x_2) = g(x) - g(x_2) = 0$, wobei $x - x_2 \in \mathfrak{m}_i$ gilt. Also ist $x - x_2$ im Kern von g, also wegen der Exaktheit auch im Bild von f. Es gibt also ein $x' \in \mathfrak{m}_i' = \mathfrak{m}_{i_2}'$ mit $f(x') = x - x_2$. Also ist $x - x_2 \in \mathfrak{m}_{i_2}$ und somit auch $x = x - x_2 + x_2 \in \mathfrak{m}_{i_2}$. Somit wurde gezeigt, dass auch $\mathfrak{m}_i \subset \mathfrak{m}_{i_2}$ für alle $i \geq i_2$ gilt und damit auch, dass die aufsteigende Kette der $\mathfrak{m}_i$ stationär wird. Also ist M noethersch. □

Korollar 2.8.9. *Sei $h : M \to N$ ein surjektiver Homomorphismus von R-Moduln und M noethersch beziehungsweise artinsch. Dann ist auch N noethersch beziehungsweise artinsch.*

Beweis. Die Sequenz

$$\begin{array}{ccccccccc} 0 & \to & \ker h & \to & M & \to & N & \to & 0 \\ & & m & \mapsto & m & & & & \\ & & & & m & \mapsto & h(m) & & \end{array}$$

ist exakt. Da M noethersch ist, sind somit nach Proposition 2.8.8 auch $\ker h$ und N noethersch. Für den anderen Teil des Beweises vertauscht man einfach noethersch durch artinsch. □

Proposition 2.8.10. *Sei R ein noetherscher beziehungsweise artinscher Ring. Dann ist R^n noethersch beziehungsweise artinsch.*

Beweis. Die Sequenz

$$\begin{array}{ccccccccc} 0 & \to & R & \to & R^n & \to & R^{n-1} & \to & 0 \\ & & r & \mapsto & (0,\ldots,0,r) & & & & \\ & & & & (r_1,\ldots,r_n) & \mapsto & (r_1,\ldots,r_{n-1}) & & \end{array}$$

ist exakt. Sind also R und R^{n-1} noethersch, so ist auch R^n noethersch. Somit folgt durch Induktion aus R noethersch auch R^n noethersch für alle $n \in \mathbb{N}$. Für den anderen Teil des Beweises vertauscht man einfach noethersch durch artinsch. □

Proposition 2.8.11. *Sei R ein noetherscher beziehungsweise artinscher Ring und M ein endlich erzeugter R-Modul. Dann ist M noethersch beziehungsweise artinsch.*

Beweis. Sei $m_1, \ldots, m_r$ ein R-Erzeugendensystem von M und $e_1, \ldots, e_r$ die Standardbasis von R^r. Dann ist

$$\begin{aligned} h : R^r &\to M \\ e_i &\mapsto m_i \end{aligned}$$

ein surjektiver Homomorphismus von R-Moduln. Da R noethersch ist, ist nach Proposition 2.8.10 auch R^r noethersch. Wegen h surjektiv, folgt nach Korollar 2.8.9, dass M noethersch ist. Für den anderen Teil des Beweises vertauscht man einfach noethersch durch artinsch. □

Lemma 2.8.12. *Sei R ein artinscher Ring, $\mathfrak{a}$ ein Ideal in R. Dann ist der Faktorring $R/\mathfrak{a}$ artinsch.*

Beweis. Da $\iota : R \to R/\mathfrak{a}$ ein surjektiver Homomorphismus von R-Moduln ist, folgt aus R artinsch und Korollar 2.8.9 sofort, dass $R/\mathfrak{a}$ artinsch ist. □

Lemma 2.8.13. *Sei R ein artinscher Ring, $\mathfrak{p}$ ein Primideal in R. Dann ist $\mathfrak{p}$ maximal.*

Beweis. Da $\mathfrak{p}$ ein Primideal ist, ist nach Proposition 2.2.16 der Faktorring $R/\mathfrak{p}$ ein Integritätsring. Nach der gleichen Proposition ist dann nur noch zu zeigen, dass $R/\mathfrak{p}$ sogar ein Körper ist, da dann $\mathfrak{p}$ maximal folgt. Sei also $0_{R/\mathfrak{p}} \neq x \in R/\mathfrak{p}$ ein beliebiges Element im Faktorring. Da nach Lemma 2.8.12 aus R artinsch auch $R/\mathfrak{p}$ artinsch folgt, wird jede absteigende Kette von Idealen in $R/\mathfrak{p}$ stationär, also insbesondere die Kette

$$(x)_{R/\mathfrak{p}} \supset (x^2)_{R/\mathfrak{p}} \supset \ldots \supset (x^i)_{R/\mathfrak{p}} \supset \ldots$$

Sei i_0 ein Index, ab dem die Kette stationär ist. Dann gilt die Gleichung $(x^{i_0})_{R/\mathfrak{p}} = (x^{i_0+1})_{R/\mathfrak{p}}$ und somit auch $x^{i_0} \in (x^{i_0+1})_{R/\mathfrak{p}}$. Damit gibt es ein $y \in R/\mathfrak{p}$ mit $x^{i_0} = y * x^{i_0+1}$ und somit $x^{i_0} * (1_{R/\mathfrak{p}} - y * x) = 0_{R/\mathfrak{p}}$. Wegen $x \neq 0_{R/\mathfrak{p}}$ und $R/\mathfrak{p}$ Integritätsring folgt also $1_{R/\mathfrak{p}} - y * x = 0_{R/\mathfrak{p}}$ und somit $y * x = 1_{R/\mathfrak{p}}$. Damit ist x invertierbar und es folgt die Behauptung. □

2.8.2 Endlich erzeugt

Dieser Abschnitt beschreibt, wie endlich erzeugte Moduln über einem euklidischen Ring aussehen (bis auf Isomorphie von Moduln) und wie man mit der Smith-Normalform den Index eines Faktormoduls bestimmen kann. In diesem Abschnitt sei $\mathcal{R}_\mathrm{e}$ wieder ein euklidischer Ring.

Theorem 2.8.14. *Sei M ein endlich erzeugter $\mathcal{R}_e$-Modul. Dann gibt es $r, s \in \mathbb{N}_0$ und $d_1, \ldots, d_s \in \mathbb{N}$ mit den folgenden Eigenschaften:*

(i) $M \cong \mathcal{R}_e^r \oplus \bigoplus_{i=1}^{s} \mathcal{R}_e/(d_i)_{\mathcal{R}_e}$

(ii) $d_i \mid d_{i+1}$ *für* $i \in \{1, \ldots, s-1\}$

Beweis. Man betrachte ein Erzeugendensystem $m_1, \ldots, m_t$ von M und den Epimorphismus

$$\begin{aligned} \pi : \mathcal{R}_{\mathrm{e}}^t &\to M \\ e_i &\mapsto m_i \end{aligned}$$

Sei $N := \ker \pi$ der vom Kern erzeugte Untermodul von $\mathcal{R}_{\mathrm{e}}^t$. Da $\mathcal{R}_{\mathrm{e}}$ ein euklidischer Ring ist, ist er insbesondere ein Hauptidealring und somit nach Beispiel 2.8.5 noethersch. Damit ist nach Proposition 2.8.10 auch $\mathcal{R}_{\mathrm{e}}^t$ noethersch und somit N als Untermodul eines noetherschen Rings endlich erzeugt. Es gibt also ein Erzeugendensystem $n_1, \ldots, n_u \in \mathcal{R}_{\mathrm{e}}^t$. Seien $a_{ij} \in \mathcal{R}_{\mathrm{e}}^t$ mit $n_i = \sum_{j=1}^{t} a_{ij} * e_j$. Dann sind die Koordinaten der n_i (bezüglich der Standardbasis von $\mathcal{R}_{\mathrm{e}}^t$) die Zeilen der $u \times t$-Matrix $A := (a_{ij})$. Berechnet man nun die Smith-Normalform B von A, so erhält man invertierbare Matrizen U, V und Elemente $d_1, \ldots, d_s \in \mathcal{R}_{\mathrm{e}}$ mit

$$B = \operatorname{diag}(d_1, \ldots, d_s, 0, \ldots, 0) = V * A * U$$

Da die Zeilen mit Index größer als s in B Nullzeilen sind, wird der Zeilenmodul von B schon von den Zeilen $b_1, \ldots, b_s$ von B erzeugt. Die Matrix U induziert eine Basistransformation in $\mathcal{R}_{\mathrm{e}}^t$, die $\mathcal{R}_{\mathrm{e}}^t$ auf $\mathcal{R}_{\mathrm{e}}^t$ abbildet und die Zeilen $\bar{n}_1, \ldots, \bar{n}_u$ von $V * A$ auf die Zeilen von B. Damit ist der Modul in $\mathcal{R}_{\mathrm{e}}^t$ erzeugt von den Zeilen von $V * A$ isomorph zum Modul in $\mathcal{R}_{\mathrm{e}}^t$ erzeugt von den Zeilen von B. Außerdem gilt nach Korollar 2.7.8, dass der Zeilenmodul von $V * A$ gleich dem Zeilenmodul von A ist. Insgesamt gilt also:

$$\begin{aligned} M &\cong \mathcal{R}_{\mathrm{e}}^t/N = \mathcal{R}_{\mathrm{e}}^t/[n_1, \ldots, n_u]_{\mathcal{R}_{\mathrm{e}}} = \mathcal{R}_{\mathrm{e}}^t/[\bar{n}_1, \ldots, \bar{n}_u]_{\mathcal{R}_{\mathrm{e}}} \\ &\cong \mathcal{R}_{\mathrm{e}}^t/[b_1, \ldots, b_s]_{\mathcal{R}_{\mathrm{e}}} = [e_1, \ldots, e_t]_{\mathcal{R}_{\mathrm{e}}}/[d_1 * e_1, \ldots, d_s * e_s]_{\mathcal{R}_{\mathrm{e}}} \\ &\cong \mathcal{R}_{\mathrm{e}}^{t-s} \oplus \bigoplus_{i=1}^{s} \mathcal{R}_{\mathrm{e}}/(d_i)_{\mathcal{R}_{\mathrm{e}}} \end{aligned}$$

□

Korollar 2.8.15. *Sei M ein endlich erzeugter $\mathcal{R}_e$-Modul. Dann sind die folgenden Aussagen äquivalent:*

(i) *M frei*

(ii) *M torsionsfrei*

(iii) $M \cong \mathcal{R}_e^t$ *für ein geeignetes* $t \in \mathbb{N}_0$

Beweis. (i) $\Rightarrow$ (ii): Sei $m_1, \ldots, m_t$ eine linear unabhängiges Erzeugendensystem von M. Angenommen M wäre nicht torsionsfrei. Dann gäbe es ein $0_{\mathcal{R}_\mathrm{e}} \neq r \in \mathcal{R}_\mathrm{e}$ und ein $0_M \neq m = \sum_{i=1}^{t} r_i * m_i \in M$ mit $r * m = 0_M$. Dann folgt aber $0_M = \sum_{i=1}^{t} r * r_i * m_i$, also wegen m_i linear unabhängig auch $r * r_i = 0_{\mathcal{R}_\mathrm{e}}$ für alle i. Da $\mathcal{R}_\mathrm{e}$ ein Integritätsring ist, muss dann aber entweder $r = 0$ oder $r_i = 0$ für alle i gelten. Dies ist ein Widerspruch zur Wahl von r und $m = \sum_{i=1}^{t} r_i * m_i$. Also ist M torsionsfrei.

(ii) $\Rightarrow$ (iii): Da M endlich erzeugt über einem euklidischen Ring ist, ist M nach Theorem 2.8.14 isomorph zu $N := \mathcal{R}_\mathrm{e}^k \oplus \bigoplus_{i=1}^{s} \mathcal{R}_\mathrm{e}/(d_i)_{\mathcal{R}_\mathrm{e}}$. Wäre $s > 0$, so wäre $e_{k+1} := (0_{\mathcal{R}_\mathrm{e}^k}, 1_{\mathcal{R}_\mathrm{e}/(d_1)_{\mathcal{R}_\mathrm{e}}}, 0_{\bigoplus_{i=2}^{s} \mathcal{R}_\mathrm{e}/(d_i)_{\mathcal{R}_\mathrm{e}}})$ ein Torsionselement in N, da $(d_1 * 1_{\mathcal{R}_\mathrm{e}}) * e_{k+1} = 0_N$ gilt. Somit wäre das Urbild von e_{k+1} unter dem Isomorphismus $M \cong N$ ein Torsionselement ungleich 0_M in M, was ein Widerspruch zu M torsionsfrei ist. Also muss $s = 0$ gelten und somit $M \cong \mathcal{R}_\mathrm{e}^k$.

(iii) $\Rightarrow$ (i): In $\mathcal{R}_\mathrm{e}^t$ ist die Standardbasis $e_1, \ldots, e_t$ eine linear unabhängige Menge, die $\mathcal{R}_\mathrm{e}^t$ erzeugt. Somit ist $\mathcal{R}_\mathrm{e}^t$ frei und damit auch M, da M isomorph zu $\mathcal{R}_\mathrm{e}^t$ ist.

□

Definition 2.8.16. Ist ein $\mathcal{R}_\mathrm{e}$-Modul M isomorph zu $\mathcal{R}_\mathrm{e}^t$ für ein $t \in \mathbb{N}_0$, so nennt man $\mathrm{rg}(M) := t$ den **Rang** des Moduls M.

Lemma 2.8.17. *Sei M ein freier, endlich erzeugter $\mathcal{R}_e$-Modul und $N \subset M$ ein freier Untermodul. Gilt $rg(M) = rg(N)$, so ist der Index endlich und es gilt $(M : N) = |\det(S)|$, wobei S die Smith-Normalform der Transformationsmatrix von einem Koordinatensystem von N zu einem Koordinatensystem von M ist. Ansonsten gilt $(M : N) = \infty$.*

Beweis. Dieser Beweis ist ähnlich zum Beweis von Theorem 2.8.14. Sei t der Rang von M und $s <= t$ der Rang von N. Sei $m_1, \ldots, m_t$ eine Basis des freien Moduls M. Sei

$$\begin{array}{rccccc} \phi : \mathcal{R}_\mathrm{e}^t & \to & M & \to & M/N \\ e_i & \mapsto & m_i & \mapsto & [m_i] \end{array}$$

die Abbildung vom Koordinatensystem von M in den Faktorring M/N. Dann ist der Kern von ϕ genau der Modul im Koordinatensystem von M, der dem freien Modul N in M entspricht, ist also insbesondere von s linear unabhängigen Elementen erzeugt. Sei $n_1, \ldots, n_s \in \mathcal{R}_\mathrm{e}^t$ eine Basis des Kerns von ϕ. Dann kann man durch $n_i = \sum_{j=1}^{t} a_{ij} * e_j$ eine Matrix $A := (a_{ij})$ definieren. Falls $t = s$ ist, so ist dies genau die Transformationsmatrix vom Koordinatensystem von N bezüglich $\phi_B^{-1}(n_1), \ldots, \phi_B^{-1}(n_s)$ zum Koordinatensystem von M bezüglich $m_1, \ldots, m_t$, wobei ϕ_B die Koordinatenabbildung

bezüglich $m_1, \ldots, m_t$ ist. Sei $S = \operatorname{diag}(d_1, \ldots, d_s, 0, \ldots, 0)$ die Smith-Normalform von A. Dann folgt wie im Beweis von Theorem 2.8.14:

$$\begin{aligned} M/N &= \mathcal{R}_{\mathrm{e}}^t/[n_1, \ldots, n_s]_{\mathcal{R}_{\mathrm{e}}} \cong [e_1, \ldots, e_t]_{\mathcal{R}_{\mathrm{e}}}/[d_1 * e_1, \ldots, d_s * e_s]_{\mathcal{R}_{\mathrm{e}}} \\ &\cong \mathcal{R}_{\mathrm{e}}^{t-s} \oplus \bigoplus_{i=1}^{s} \mathcal{R}_{\mathrm{e}}/(d_i)_{\mathcal{R}_{\mathrm{e}}} \end{aligned}$$

Somit hat der Faktormodul für $s < t$ unendlich viele Elemente und für $s = t$ genau $\prod_{i=1}^{s} |d_i| = |\det S|$ Elemente. □

2.8.3 Jacobson-Radikal und Nilradikal

Die Sätze in diesem Abschnitt werden vor allem für die Zerlegung einer halbeinfachen Algebra in eine direkte Summe von Körpern benötigt. Außerdem wird das Lemma von Nakayama bewiesen, das bei der Zerlegung von Idealen eine Rolle spielen wird. Die Beweise in diesem Abschnitt orientieren sich vor allem an [Ger09, S.69, 119-128] und [NW10, S.19-20, 84-85].

Definition 2.8.18. Sei R ein Ring, $\mathfrak{a}$ ein Ideal in R. Dann heißt

$$\sqrt{\mathfrak{a}} := \{x \in R \mid \ \exists\, n \in \mathbb{N} : x^n \in \mathfrak{a}\}$$

das **Radikal** von $\mathfrak{a}$. Das Radikal ist ein Ideal in R. Im Spezialfall des Nullideals nennt man $\mathcal{N}_R := \sqrt{(0_R)_R}$ das **Nilradikal** von R. Die Elemente des Nilradikals nennt man auch **nilpotente** Elemente, da es für jedes dieser Elemente einen Exponenten gibt, so dass die Potenz 0_R ist.

Definition 2.8.19. Sei R ein Ring, M ein R-Modul. Man nennt den Schnitt aller maximalen Untermoduln von M das **Jacobson-Radikal** $\operatorname{Jac}(M)$ von M. Das **Jacobson-Radikal** $\operatorname{Jac}(R)$ von R ist das Jacobson-Radikal des kanonischen R-Moduls R, also der Durchschnitt über alle maximalen Ideale von R.

Proposition 2.8.20. *Sei R ein Ring. Dann ist das Nilradikal von R gleich dem Schnitt über die Primideale von R.*

Beweis. Sei zunächst $x \in \mathcal{N}_R$. Sei $n \in \mathbb{N}$ mit $x^n = 0_R$. Dann gilt für jedes Primideal $\mathfrak{p}$ auch $x^n = 0_R \in \mathfrak{p}$. Aus den Primidealeigenschaften folgt dann (durch Induktion), dass $x \in \mathfrak{p}$ gilt. Somit ist x in jedem Primideal enthalten, also auch im Schnitt über die Primideale. Sei nun $x \notin \mathcal{N}_R$. Es ist zu zeigen, dass dann x nicht im Schnitt über die Primideale enthalten ist. Sei $\mathcal{J}$ die Menge der Ideale in R, die keines der x^n enthalten. Wegen x nicht nilpotent ist $(0)_R \in \mathcal{J}$ und somit $\mathcal{J}$ nicht leer. Betrachtet man nun eine aufsteigende Kette von Idealen in $\mathcal{J}$, so sieht man, dass die Vereinigung der Elemente der Kette ebenfalls ein Ideal in $\mathcal{J}$ ist und alle Elemente der Kette in diesem Ideal enthalten sind. Somit hat jede aufsteigende Kette von Idealen in $\mathcal{J}$ eine obere Schranke in $\mathcal{J}$ und es folgt nach dem Lemma von Zorn, dass $\mathcal{J}$ mindestens ein maximales Element hat. Sei $\mathfrak{p}$ ein maximales Element in $\mathcal{J}$. Ist $\mathfrak{p}$ ein

Primideal, dann folgt aus $x^1 \notin \mathfrak{p}$, dass x nicht im Schnitt aller Primideale enthalten ist. Seien also $a_1, a_2 \in R$ mit $a_1 * a_2 \in \mathfrak{p}$. Angenommen es ist weder a_1 noch a_2 in $\mathfrak{p}$. Dann sind die $\mathfrak{p} + (a_i)_R \supsetneq \mathfrak{p}$ wegen der Maximalität von $\mathfrak{p}$ keine Ideale in $\mathcal{J}$. Es gibt also $n_1, n_2 \in \mathbb{N}$ mit $x^{n_i} \in \mathfrak{p} + (a_i)_R$. Dann gibt es aber $p_1, p_2 \in \mathfrak{p}$, und $r_1, r_2 \in R$ mit $x^{n_i} = p_i + r_i * a_i$ und es folgt wegen $a_1 * a_2 \in \mathfrak{p}$ auch

$$\begin{aligned} x^{n_1+n_2} &= x^{n_1} * x^{n_2} = (p_1 + r_1 * a_1)(p_2 + r_2 * a_2) \\ &= p_1 * p_2 + p_1 * r_2 * a_2 + p_2 * r_1 * a_1 + r_1 * r_2 * a_1 * a_2 \in \mathfrak{p} \end{aligned}$$

Dies ist aber ein Widerspruch zu $\mathfrak{p} \in \mathcal{J}$. Somit muss a_1 oder a_2 in $\mathfrak{p}$ sein und $\mathfrak{p}$ ist ein Primideal mit $x \notin \mathfrak{p}$. Also ist x nicht im Schnitt der Primideale und die Behauptung ist gezeigt. □

Lemma 2.8.21. *Sei R ein Ring. Dann gilt*

$$Jac(R) = \{x \in R \mid \ \forall\ y \in R : 1 - x * y \in R^*\}.$$

Beweis. Sei zunächst $a \in \mathrm{Jac}(R)$. Angenommen es gibt ein $y \in R$ mit $1 - a * y \notin R^*$. Da $1 - a * y$ keine Einheit ist, muss $1 - a * y$ in einem maximalen Ideal $\mathfrak{m}$ liegen, da das Hauptideal erzeugt von $1 - a * y$ in einem maximalen Ideal liegen muss. Es gilt aber auch $a \in \mathrm{Jac}(R) \subset \mathfrak{m}$ und somit $a * y \in \mathfrak{m}$. Damit folgt aber auch

$$1 = (1 - a * y) + a * y \in \mathfrak{m} + \mathfrak{m} = \mathfrak{m},$$

was ein Widerspruch zu $\mathfrak{m}$ maximales Ideal ist. Also muss $1 - a * y \in R^*$ für alle $y \in R$ gelten. Sei nun umgekehrt $a \in \{x \in R \mid \ \forall\ y \in R : 1 - x * y \in R^*\}$. Angenommen a wäre nicht in $\mathrm{Jac}(R)$. Dann gibt es ein maximales Ideal $\mathfrak{m}$ mit $a \notin \mathfrak{m}$. Somit muss das Ideal $\mathfrak{m} + (a)_R$ das Einheitsideal sein. Es gilt also $m + r * a = 1$ für geeignete $m \in \mathfrak{m}$ und $r \in R$ und somit auch $1 - r * a = m \in \mathfrak{m}$. Da $\mathfrak{m}$ keine Einheiten enthält, ist dann aber $1 - r * a \notin R^*$, was ein Widerspruch zu $a \in \{x \in R \mid \ \forall\ y \in R : 1 - x * y \in R^*\}$ ist. Somit muss a in $\mathrm{Jac}(R)$ sein. □

Lemma 2.8.22 (Nakayama)**.** *Sei R ein Ring, M ein endlich erzeugter R-Modul. Sei $\mathfrak{a}$ ein Ideal von R mit $\mathfrak{a} \subset Jac(M)$. Dann gilt:*

$$\mathfrak{a} * M = M \Rightarrow M = \{0_M\}$$

Beweis. Angenommen M ist nicht gleich $\{0_M\}$. Dann gibt es ein minimales Erzeugendensystem $m_1, \ldots, m_n$ mit $n > 0$ und $m_n \neq 0$. Dann folgt aber aus $M = \mathfrak{a} * M$ auch $m_n = \sum_{i=1}^{n} a_i * m_i$ für geeignete Elemente $a_i \in \mathfrak{a}$. Es gilt also

$$\sum_{i=1}^{n-1} a_i * m_i = m_n - a_n * m_n = (1_R - a_n) * m_n.$$

Nach Lemma 2.8.21 besteht das Jacobsonradikal genau aus den Elementen $x \in R$, so dass $1_R - x * y \in R^*$ für alle $y \in R$ gilt. Da a_n wegen $\mathfrak{a} \subset \mathrm{Jac}(M)$ im Jacobson-Radikal enthalten ist, gilt also

$$(1_R - a_n) = (1_R - a_n * 1_R) \in R^*.$$

Somit folgt $m_n = (1_R - a_n)^{-1} * \sum_{i=1}^{n-1} a_i * m_i$. Damit wurde aber m_n als R-Linearkombination von den Elementen $m_1, \ldots, m_{n-1}$ dargestellt, was ein Widerspruch dazu ist, dass das Erzeugendensystem $m_1, \ldots, m_n$ minimal gewählt wurde. Also ist die Annahme $M \neq \{0_M\}$ falsch und es muss die Gleichung $M = \{0_M\}$ gelten. □

Lemma 2.8.23. *Sei R ein artinscher Ring, $\mathcal{N}_R$ das Nilradikal von R. Dann ist $\mathcal{N}_R$ nilpotent, das heißt es gibt ein $k \in \mathbb{N}$ mit $\mathcal{N}_R^k = (0)_R$.*

Beweis. Da R artinsch ist, muss die absteigende Kette von Idealen

$$\mathcal{N}_R \supset \mathcal{N}_R^2 \supset \ldots \supset \mathcal{N}_R^i \supset \ldots$$

stationär werden. Sei k ein Index, ab dem die Kette stationär ist. Dann gilt $\mathcal{N}_R^k = \mathcal{N}_R^i$ für alle $i \geq k$. Es ist nur zu zeigen, dass dann $\mathcal{N}_R^k = (0)_R$ gelten muss. Sei $\mathcal{J}$ die Menge aller Ideale $\mathfrak{b}$ mit $\mathcal{N}_R^k * \mathfrak{b} \neq (0)_R$. Angenommen es gilt $\mathcal{N}_R^k \neq (0)_R$. Dann ist die Menge $\mathcal{J}$ nichtleer, da

$$\mathcal{N}_R^k * \mathcal{N}_R = \mathcal{N}_R^{k+1} = \mathcal{N}_R^k \neq (0)_R$$

gilt und somit $\mathcal{N}_R$ in $\mathcal{J}$ enthalten ist. Da jede absteigende Kette von Idealen aus $\mathcal{J}$ ein minimales Element und somit eine untere Schranke bezüglich Inklusion enthält, folgt nach dem Lemma von Zorn, dass $\mathcal{J}$ ein minimales Element hat (wobei für die Anwendung des Zornsche Lemma die Halbordnung $\supset$ betrachtet wird und ein maximales Element bezüglich $\supset$ einem minimalen Element bezüglich $\subset$ entspricht). Sei nun $\mathfrak{a}$ ein minimales Element in $\mathcal{J}$. Dann gilt $\mathcal{N}_R^k * \mathfrak{a} \neq (0)_R$, also gibt es auch ein $a \in \mathfrak{a}$ mit $\mathcal{N}_R^k * a \neq (0)_R$. Dann ist $\mathcal{N}_R^k * (a)_R \neq (0)_R$ und somit $(a)_R \in \mathcal{J}$. Wegen $(a)_R \subset \mathfrak{a}$ und der Minimalität von $\mathfrak{a}$ in $\mathcal{J}$ folgt also $\mathfrak{a} = (a)_R$. Analog dazu gilt auch

$$\mathcal{N}_R^k * (\mathcal{N}_R * (a)_R) = \mathcal{N}_R^{k+1} * (a)_R = \mathcal{N}_R^k * (a)_R \neq (0)_R$$

und somit $\mathcal{N}_R * (a)_R \in \mathcal{J}$. Wegen der Minimalität von $\mathfrak{a}$ in $\mathcal{J}$ folgt also auch $(a)_R = \mathfrak{a} = \mathcal{N}_R * (a)_R$. Also gibt es ein $y \in \mathcal{N}_R$ mit $a = y * a$. Da y im Nilradikal liegt, gilt $y^n = 0$ für ein $n \in \mathbb{N}$ und somit

$$a = y * a = \ldots = y^n * a = 0.$$

Dies ist aber ein Widerspruch dazu, dass $\mathcal{N}_R^k * (a)_R = \mathcal{N}_R^k * \mathfrak{a} \neq (0)_R$ gilt, also muss die Annahme $\mathcal{N}_R^k \neq (0)_R$ falsch sein. Somit ist die Behauptung gezeigt. □

Lemma 2.8.24. *Sei A eine endlich-dimensionale $\mathbb{F}_p$-Algebra mit Dimension $n := (A : \mathbb{F}_p) < \infty$. Sei $k \in \mathbb{N}$ mit $p^{k-1} < n \leq p^k$. Dann ist das Nilradikal von A gleich dem Kern der Abbildung ϕ^k, wobei ϕ die folgende Abbildung ist:*

$$\begin{array}{rcl} \phi : A & \to & A \\ x & \mapsto & x^p \end{array}$$

Die Abbildung ϕ ist ein Homomorphismus von $\mathbb{F}_p$-Algebren und wird auch ***Frobenius-Homomorphismus*** *Frob(p) genannt.*

Beweis. Der Frobenius-Homomorphismus (bezüglich der Primzahl p) ist ein Ringhomomorphismus, wenn die Definitionsmenge ein Ring mit Charakteristik p ist (dies kann man mit Hilfe des binomischen Lehrsatzes nachrechnen). Die Charakteristik vom $\mathbb{F}_p$-Modul A ist p. Die Verträglichkeit mit der Skalarmultiplikation folgt aus $\lambda^p = \lambda$ für $\lambda \in \mathbb{F}_p$. Somit ist ϕ ein Homomorphismus von $\mathbb{F}_p$-Algebren. Nach Beispiel 2.8.6 ist der Körper $\mathbb{F}_p$ artinsch. Also ist nach Proposition 2.8.11 auch der endlich erzeugte $\mathbb{F}_p$-Modul A artinsch. Nach Lemma 2.8.23 ist $\mathcal{N}_A$ nilpotent, es gibt also ein $k \in \mathbb{N}$ mit $\mathcal{N}_A^k = (0)_A$. Man betrachte nun die folgende absteigende Kette:

$$A \supset \mathcal{N}_A \supset \mathcal{N}_A^2 \supset \ldots \supset \mathcal{N}_A^i \supset \ldots$$

Jedes $\mathcal{N}_A^i$ ist ein $\mathbb{F}_p$-Untervektorraum von A. Da die Dimension von A gleich n ist, können also höchstens die ersten n Teilmengenrelationen echt sein. Sobald eine Gleichheit auftritt, müssen auch alle folgenden Teilmengenrelationen Gleichheiten sein. Somit kann das kleinste k mit $\mathcal{N}_A^k = (0)_A$ höchstens n sein und es gilt auf jeden Fall $\mathcal{N}_A^n = \mathcal{N}_A^{n+i} = (0)_A$ für alle $i \in \mathbb{N}$. Wegen $n \leq p^k$ gilt also für $x \in \mathcal{N}_A$ auch

$$\phi^k(x) = \phi^{k-1}(x^p) = \ldots = x^{p^k} = x^{n+i} = x^n * x^i \in \mathcal{N}_A^n = (0)_A$$

und somit $\mathcal{N}_A \subset \ker \phi^k$. Sei umgekehrt $x \in \ker \phi^k$. Dann folgt daraus sofort $x^{p^k} = \phi^k(x) = 0$, also ist x nilpotent und somit im Nilradikal. Damit gilt auch $\ker \phi^k \subset \mathcal{N}_A$. □

Lemma 2.8.25. *Sei R ein Ring und $f : M \to N$ ein Homomorphismus von R-Moduln. Dann gilt:*

$$f(Jac(M)) \subset Jac(N)$$

Beweis. Sei $\mathfrak{n}$ ein maximaler Untermodul von N, $S := N/\mathfrak{n}$ und

$$\bar{f} := \iota \circ f : M \to N \to S.$$

Da $\mathfrak{n}$ maximal ist, ist nach Proposition 2.2.12 der Modul S einfach. Somit ist das Bild von $\bar{f}$ entweder $\{0\}$ oder S. Da $\bar{f}$ ein Modulhomomorphismus ist,

gilt nach dem Homomorphiesatz (Proposition 2.2.3), dass $M/\ker \bar{f}$ isomorph zum Bild von $\bar{f}$ ist. Außerdem ist $\ker \bar{f} = f^{-1}\mathfrak{n} =: \mathfrak{m}$. Es gilt also entweder $M/\mathfrak{m} = \{0\}$ oder $M/\mathfrak{m} \cong S$. Falls $M/\mathfrak{m} = \{0\}$ ist, so gilt $\mathfrak{m} = M$ und somit für einen beliebigen maximalen Untermodul $\mathfrak{m}'$ die Gleichung

$$f(\mathfrak{m}') \subset f(M) = f(\mathfrak{m}) \subset \mathfrak{n}.$$

Falls $M/\mathfrak{m} \cong S$ ist, so ist $M/\mathfrak{m}$ einfach, also nach Proposition 2.2.12 auch $\mathfrak{m}$ maximal. Außerdem gilt wieder

$$f(\mathfrak{m}) \subset \mathfrak{n}.$$

In beiden Fällen gibt es einen maximalen Untermodul in M, dessen Bild unter f eine Teilmenge von $\mathfrak{n}$ ist. Somit ist $f(\mathrm{Jac}(M)) \subset \mathfrak{n}$. Da dies für jeden maximalen Untermodul $\mathfrak{n}$ von N gilt, ist also $f(\mathrm{Jac}(M)) \subset \mathrm{Jac}(N)$. □

Proposition 2.8.26. *Sei R ein Ring, M, N R-Moduln. Dann gilt:*

$$Jac(M \oplus N) = Jac(M) \oplus Jac(N)$$

Beweis. Betrachtet man die Inklusionshomomorphismen $\iota_M : M \to M \oplus N$ und $\iota_N : N \to M \oplus N$, so erhält man wegen Lemma 2.8.25 die Teilmengenrelationen $\mathrm{Jac}(M) \subset \mathrm{Jac}(M \oplus N)$ und $\mathrm{Jac}(N) \subset \mathrm{Jac}(M \oplus N)$. Somit erhält man $\mathrm{Jac}(M) \oplus \mathrm{Jac}(N) \subset \mathrm{Jac}(M \oplus N)$. Analog erhält man aus den Projektionen $\pi_M : M \oplus N \to M$ und $\pi_N : M \oplus N \to N$ durch das gleiche Lemma $\mathrm{Jac}(M \oplus N) \subset \mathrm{Jac}(M) \oplus \mathrm{Jac}(N)$. Somit ergibt sich die behauptete Gleichheit. □

Lemma 2.8.27. *Sei R ein Ring, M ein R-Modul. Dann gilt:*

$$Jac(M/Jac(M)) = \left\{0_{M/Jac(M)}\right\}$$

Beweis. Nach Proposition 2.2.11 gibt es eine Bijektion zwischen den maximalen Untermoduln von $M/\mathrm{Jac}(M)$ und den maximalen Untermoduln von M, die $\mathrm{Jac}(M)$ enthalten. Da aber $\mathrm{Jac}(M)$ das Produkt aller maximalen Untermoduln von M ist, enthält jedes maximale Untermodul von M auch $\mathrm{Jac}(M)$. Somit sind die maximalen Untermoduln von $M/\mathrm{Jac}(M)$ genau die Inklusionen der maximalen Untermoduln von M. Ist $\bar{x}$ in $\mathrm{Jac}(M/\mathrm{Jac}(M))$, so ist $\bar{x}$ in allen maximalen Untermoduln von $M/\mathrm{Jac}(M)$ enthalten. Dann ist jedes Urbild x von $\bar{x}$ in M in jedem maximalen Untermodul von M enthalten, also auch in $\mathrm{Jac}(M)$. Somit ist $\bar{x} = x + \mathrm{Jac}(M) = 0_M + \mathrm{Jac}(M)$. Da $x \in \mathrm{Jac}(M/\mathrm{Jac}(M))$ beliebig gewählt war, ist also $\mathrm{Jac}(M/\mathrm{Jac}(M))$ eine Teilmenge von $\left\{0_{M/\mathrm{Jac}(M)}\right\}$ und somit sogar gleich $\left\{0_{M/\mathrm{Jac}(M)}\right\}$, da das neutrale Element der Addition in jedem Untermodul enthalten ist. □

2.8.4 Einfachheit und idempotente Elemente

In diesem Abschnitt wird gezeigt, dass der Faktorring $A/\mathcal{N}_A$ einer endlichdimensionalen $\mathbb{F}_p$-Algebra halbeinfach ist und wie man mit Hilfe von idempotenten Elementen eine halbeinfache Algebra in Körper zerlegen kann. Wie in Algorithmus 4.3.8 noch gezeigt wird, bekommt man dadurch eine Möglichkeit, um Primideale in einer Ordnung zu bestimmen.

Definition 2.8.28. Seien K ein Körper, A eine assoziative, kommutative K-Algebra mit Einselement und $\epsilon \in A$. ϵ heißt **idempotent** beziehungsweise **idempotentes Element**, falls $\epsilon^2 = \epsilon$ gilt. Die idempotenten Elemente 0 und 1 heißen **triviale** idempotente Elemente, alle anderen heißen **nicht-triviale** idempotente Elemente.

Proposition 2.8.29. *Seien K ein Körper, A eine assoziative, kommutative K-Algebra mit Einselement und $\epsilon \in A$ ein nicht-triviales idempotentes Element. Dann sind die Mengen $A_1 := \epsilon * A$ und $A_2 := (1-\epsilon) * A$ Unteralgebren mit Einselementen ϵ und $(1-\epsilon)$. Außerdem gilt $A_1 \oplus A_2 = A$.*

Beweis. Zunächst ist zusammen mit ϵ auch $(1-\epsilon)$ ein nicht-triviales idempotentes Element, da $(1-\epsilon)^2 = 1^2 - 2*\epsilon + \epsilon^2 = 1 - 2*\epsilon + \epsilon = 1 - \epsilon$ gilt und aus $(1-\epsilon)$ gleich 0 oder 1 sofort ϵ gleich 1 oder 0 folgen würde. Die Menge $x * A = \{a \in A \mid \exists\, y \in A : a = x * y\}$ ist für jedes beliebige $x \in A$ eine Unteralgebra von A, also insbesondere für $x = \epsilon$ und $x = (1-\epsilon)$. Dabei ist ϵ ein Einselement in $\epsilon * A$, da für jedes $a = \epsilon * a_1 \in \epsilon * A$ wegen ϵ idempotent auch $\epsilon * a = \epsilon * (\epsilon * a_1) = \epsilon * a_1 = a$ gilt. Für $(1-\epsilon)$ ist es ganz analog. Es bleibt noch zu zeigen, dass A die direkte Summe von A_1 und A_2 ist. Ist $a \in A$, so kann man a auch schreiben als

$$a = a - a*\epsilon + a*\epsilon = (1-\epsilon)*a + \epsilon * a \in (1-\epsilon)*A + \epsilon * A$$

Somit ist A die Summe von A_1 und A_2. Sei nun ein Element $a \in A$ sowohl in A_1 als auch in A_2. Da ϵ ein Einselement in A_1 ist und $(1-\epsilon)$ ein Einselement in A_2 ist, gilt also

$$a = a * (1-\epsilon) = a - a*\epsilon = a - a = 0.$$

Somit ist der Schnitt von A_1 und A_2 gleich $\{0\}$, also ist A sogar eine direkte Summe von A_1 und A_2. □

Lemma 2.8.30. *Sei K ein Körper mit Charakteristik p. Dann gilt*

$$\{x \in K \mid \mathit{Frob}(x) = x\} = \mathbb{F}_p * 1_K.$$

Beweis. Zunächst ist klar, dass $\mathbb{F}_p * 1_K \subset \{x \in K \mid \mathrm{Frob}(x) = x\}$ gilt, da für jedes $a \in \mathbb{F}_p$ nach dem kleinen fermatschen Satz die Gleichung $a^p = a$ gilt und somit wegen Charakteristik p auch $(a * 1_K)^p = a^p * 1_K^p = a * 1_K$ gilt.

Da das Polynom $\phi(x) = x^p - x$ den Grad $p > 0$ hat, kann ϕ nur maximal p Nullstellen in K haben. Somit sind $\mathbb{F}_p * 1_K$ schon alle p Nullstellen von ϕ und es gilt

$$\{x \in K \mid \mathrm{Frob}(x) = x\} = \{x \in K \mid \phi(x) = 0_K\} = \mathbb{F}_p * 1_K.$$

□

Lemma 2.8.31. *Sei A eine einfache kommutative assoziative R-Algebra mit Einselement. Dann ist A ein Körper.*

Beweis. Die Algebra A ist mit den Voraussetzungen ein kommutativer Ring mit Einselement und ein R-Modul und enthält wegen der Einfachheit als R-Modul nur die zwei trivialen Untermoduln. Somit enthält sie als Ring auch nur die zwei trivialen Ideale und ist somit ein Körper. □

Lemma 2.8.32. *Sei K ein Körper, p eine Primzahl, $A = \bigoplus_{i=1}^{r} A_i$ die Zerlegung einer endlich-dimensionalen halbeinfachen $\mathbb{F}_p$-Algebra in einfache Algebren $A_1, \ldots, A_r$ und*

$$\begin{aligned} \psi : A &\to A \\ x &\mapsto x^p - x \end{aligned}$$

Dann gilt:

(i) $\dim \ker \psi = r$

(ii) Falls $\dim \ker \psi = 1$*, so ist A einfach und es gilt* $\ker \psi = \mathbb{F}_p * 1_A$

(iii) Falls $\dim \ker \psi > 1$*, so gibt es für jedes $\alpha \in \ker \psi \setminus (\mathbb{F}_p * 1_A)$ Polynome $u, v, m_1, m_2 \in \mathbb{F}_p[x]$ mit:*

- *m_1, m_2 nicht konstant*
- *$\mu_\alpha(\alpha) = m_1(\alpha) * m_2(\alpha)$*
- *$u * m_1 + v * m_2 = 1_{\mathbb{F}_p[x]}$ (das heißt insbesondere m_1 und m_2 teilerfremd)*

(iv) Seien α, u, v, m_1, m_2 wie in (iii) , $\epsilon := (u * m_1)(alpha)$. Dann ist ϵ ein nicht-triviales idempotentes Element von A.

Beweis. (i) Jede einfache Algebra ist nach Lemma 2.8.31 ein Körper, also sind die A_i Erweiterungskörper von $\mathbb{F}_p$ mit Charakteristik p. Nach Lemma 2.8.30 ist dann

$$\mathbb{F}_p * 1_{A_i} = \{x \in A_i \mid \mathrm{Frob}(p)(x) = x\} = \{x \in A_i \mid \psi(x) = 0\}.$$

Da A die direkte Summe der A_i ist, ist also der Kern von $\psi \restriction_{A_i}$ gleich $\mathbb{F}_p * 1_{A_i}$ und der Kern von ψ gleich $\bigoplus_{i=1}^{r} \mathbb{F}_p * 1_{A_i}$. Also ist $\dim \ker \psi = r$.

(ii) Wenn $\dim \ker \psi = 1$ ist, gilt nach (i) auch $r = 1$, also $A = A_1$ für eine einfache Algebra A_1. Wie in (i) gilt dann $\mathbb{F}_p * 1_{A_1} = \ker \psi \restriction_{A_1}$. Wegen $A = A_1$ ist also $\mathbb{F}_p * 1_A = \ker \psi$.

(iii) Sei $\alpha = (\alpha_1, \ldots, \alpha_r) \in \bigoplus_{i=1}^{r} A_i \setminus \mathbb{F}_p * 1_A$ ein Element mit $\psi(\alpha) = 0$. Dann gilt wie im Beweis von (i) auch $\alpha_i \subset \mathbb{F}_p * 1_{A_i}$. Somit sind die Minimalpolynome $\mu_{\alpha_i} \in \mathbb{F}_p[x]$ vom Grad 1. Sowohl die Addition als auch die Multiplikation mit $\mathbb{F}_p$ in A übertragen sich wegen der direkten Summe auf die einzelnen Summanden A_i. Somit muss ein Polynom mit Koeffizienten in $\mathbb{F}_p$, das α als Nullstelle hat, auch jedes α_i als Nullstelle haben. Hat ein Polynom umgekehrt alle α_i als Nullstellen, so ist auch α eine Nullstelle des Polynoms. Also ist das Minimalpolynom von α das kleinste gemeinsame Vielfache der Minimalpolynome μ_{α_i}. Wäre μ_α nicht zerlegbar in zwei teilerfremde nicht-konstante Polynome, so müsste es eine Potenz von einem irreduziblen Polynom sein. Da das Minimalpolynom allerdings das kleinste gemeinsame Vielfache von Polynomen vom Grad 1 ist, müsste der Exponent gleich 1 sein und somit μ_α ein Polynom vom Grad 1. Dann wäre aber $\alpha \in \mathbb{F}_p * 1_A$, was bei der Wahl von α ausgeschlossen wurde. Somit ist μ_α zerlegbar in zwei teilerfremde nicht-konstante Polynome. Mit dem erweiterten euklidischen Algorithmus findet man dann wegen der Teilerfremdheit auch Polynome u, v mit $u * m_1 + v * m_2 = 1_{\mathbb{F}_p[x]}$.

(iv) Es gilt

$$\begin{aligned} \epsilon &= (u * m_1)(\alpha) = (u * m_1 * 1_{\mathbb{F}_p[x]})(\alpha) \\ &= (u * m_1 * (u * m_1 + v * m_2))(\alpha) \\ &= ((u * m_1)^2 + \mu_\alpha)(\alpha) \\ &= ((u * m_1)(\alpha))^2 + \mu_\alpha(\alpha) = \epsilon^2 + 0_A \quad = \quad \epsilon^2 \end{aligned}$$

Somit ist ϵ ein idempotentes Element. Es bleibt zu zeigen, dass ϵ nicht trivial ist. Angenommen $\epsilon = 0$. Dann ist $u * m_1$ ein Polynom mit Nullstelle α. Da μ_α das Minimalpolynom von α ist, gilt dann $\mu_\alpha \mid u * m_1$. Gleichzeitig ist aber $\mu_\alpha = m_1 * m_2$, also folgt $m_1 * m_2 \mid u * m_1$ und somit $m_2 \mid u$. Dann ist aber

$$1_{\mathbb{F}_p[x]} = u * m_1 + v * m_2 = \bar{u} * m_2 * m_1 + v * m_2 = m_2 * (\bar{u} * m_1 + v),$$

woraus folgt, dass m_2 konstant ist. Dies ist aber ein Widerspruch zu (iii). Angenommen $\epsilon = 1$. Dann ist $v * m_2 = 1_{\mathbb{F}_p[x]} - u * m_1$ ein Polynom mit Nullstelle α. Somit gilt $\mu_\alpha \mid v * m_2$ und somit $m_1 \mid v$. Dies führt ganz analog zum Widerspruch, dass m_1 konstant ist. Also ist ϵ nicht-trivial. □

Theorem 2.8.33. *Sei R ein Ring, M ein artinscher R-Modul. Dann ist M genau dann halbeinfach, wenn das Jacobson-Radikal $Jac(M)$ gleich $\{0_M\}$ ist.*

Beweis. Sei zunächst M halbeinfach. Dann gilt $M = \bigoplus_{i=1}^{r} M_i$ für einfache R-Moduln $M_1, \ldots, M_r$. Da M_i einfach ist, ist $\{0_{M_i}\} = \{0_M\}$ der einzige echte Untermodul von M_i und somit $\mathrm{Jac}(M_i) = \{0_M\}$. Nach Proposition 2.8.26 gilt dann

$$\mathrm{Jac}(M) = \mathrm{Jac}(\bigoplus_{i=1}^{r} M_i) = \bigoplus_{i=1}^{r} \mathrm{Jac}(M_i) = \bigoplus_{i=1}^{r} \{0_M\} = \{0_M\}.$$

Sei umgekehrt $\mathrm{Jac}(M) = \{0_M\}$. Falls M einfach ist, ist die Behauptung gezeigt. Sei also M nicht einfach. Jeder nicht einfache Modul hat echte Untermoduln, die nicht $\{0_M\}$ sind. Sei $M_1, \ldots, M_{r+1}$ eine streng monoton absteigende Kette von Untermoduln M_i von M. Da M artinsch ist, muss die Kette endlich sein, das heißt es gilt $r < \infty$. Sei nun ohne Beschränkung der Allgemeinheit die Kette maximal gewählt, das heißt es gebe keine Moduln zwischen M_i und M_{i+1} und es sei $M_{r+1} = \{0_M\}$. Dann muss M_r einfach sein, da es ansonsten einen echten Untermodul N von M_r gäbe und dieser wäre zwischen M_r und $M_{r+1} = \{0_M\}$, was der Maximalität der Kette widerspräche. Wegen der Einfachheit von M_r gilt für jeden maximalen Untermodul $\mathfrak{m}$ von M entweder $M_r \cap \mathfrak{m} = \{0\}$ oder $M_r \cap \mathfrak{m} = M_r$. Würde für jeden maximalen Untermodul $\mathfrak{m}$ die Gleichung $M_r \cap \mathfrak{m} = M_r$ gelten, so wäre M_r auch im Durchschnitt der maximalen Untermoduln (also im Jacobson-Radikal) enthalten. Dann wäre aber $M_r \subset \mathrm{Jac}(M) = \{0_M\}$ und somit $M_r = \{0\} = M_{r+1}$, was ein Widerspruch dazu ist, dass die Kette der M_i streng monoton absteigend ist. Also muss es einen maximalen Untermodul $\mathfrak{m}_1$ von M mit $M_r \cap \mathfrak{m}_1 = \{0_M\}$ geben. Da $\mathfrak{m}_1$ maximal ist und M_r wegen $M_r \cap \mathfrak{m}_1 = \{0_M\} \neq M_r$ nicht in $\mathfrak{m}_1$ enthalten ist, muss der Modul $M_r + \mathfrak{m}_1$ schon ganz M sein. Somit gilt wegen $M_r \cap \mathfrak{m}_1 = \{0_M\}$ sogar $M = M_r \oplus \mathfrak{m}_1$. Nach Proposition 2.8.26 gilt dann $\{0_M\} = \mathrm{Jac}(M) = \mathrm{Jac}(M_r) \oplus \mathrm{Jac}(\mathfrak{m}_1)$ und somit auch $\mathrm{Jac}(\mathfrak{m}_1) = \{0_M\}$. Man kann also induktiv $\mathfrak{m}_1$ weiter zerlegen und erhält so eine streng monoton absteigende Kette von Untermoduln $M =: \mathfrak{m}_0 \supset \mathfrak{m}_1 \supset \ldots \supset \mathfrak{m}_s$ und einfache Moduln N_i mit $\mathfrak{m}_i = N_i \oplus \mathfrak{m}_{i+1}$ (wobei $N_0 = M_r$ ist und N_i immer ein einfacher Untermodul von $\mathfrak{m}_i$ ist). Da M artinsch ist, muss diese Kette endlich sein, also muss ohne Beschränkung der Allgemeinheit $\mathfrak{m}_s$ einfach sein und sich somit nicht weiter zerlegen lassen. Es gilt dann

$$M = N_0 \oplus \mathfrak{m}_1 = N_0 \oplus N_1 \oplus \mathfrak{m}_2 = \ldots = \bigoplus_{i=0}^{s-1} N_i \oplus \mathfrak{m}_s,$$

also ist M eine direkte Summe von einfachen Moduln und somit halbeinfach. □

Theorem 2.8.34. *Sei A eine assoziative, kommutative K-Algebra mit Einselement und $(A : K) < \infty$. Sei $\mathcal{N}_A$ das Nilradikal von A. Dann ist $A/\mathcal{N}_A$ eine halbeinfache K-Algebra.*

Beweis. Da K ein Körper ist, ist K nach Beispiel 2.8.6 ein artinscher Ring. Die Algebra A ist somit endlich erzeugt über einem artinschen Ring, also nach Proposition 2.8.11 ebenfalls artinsch. Somit ist A ein artinscher Ring (mit der Algebra-Multiplikation als Ringmultiplikation). Nach Lemma 2.8.13 sind dann alle Primideale maximal, also ist das Nilradikal $\mathcal{N}_A$ gleich dem Jacobson-Radikal $\mathrm{Jac}(A)$. Da $\mathrm{Jac}(A)$ ein Ideal ist, kann man die Faktoralgebra $\bar{A} := A/\mathrm{Jac}(A) = A/\mathcal{N}_A$ bilden. Nach Lemma 2.8.12 ist $\bar{A}$ wegen A artinsch ebenfalls artinsch (da jede Algebra ein Ring ist, das Nilradikal ein Ideal ist und die Faktoralgebra dem Faktorring entspricht). Außerdem gilt nach Lemma 2.8.27 die Gleichung $\mathrm{Jac}(A/\mathrm{Jac}(A)) = 0$. Es ist also $\bar{A}$ artinsch und $\mathrm{Jac}(\bar{A}) = 0$, somit folgt nach Theorem 2.8.33, dass $\bar{A}$ halbeinfach ist. □

2.9 Norm, Spur und Diskriminante

In diesem Abschnitt werden die Begriffe Spur, Norm, Spurform und Diskriminante einer Algebra bezüglich einer Basis eingeführt.

Definition 2.9.1. Sei $L \mid K$ eine endliche Körpererweiterung, $\alpha \in L$. Dann definiert man:

$$\begin{aligned} \mathrm{N}_{L \mid K}(\alpha) &:= \det m(\alpha) \quad \textbf{Norm} \text{ von } \alpha \text{ bezüglich } L \mid K \\ \mathrm{Tr}_{L \mid K}(\alpha) &:= \mathrm{tr}\ m(\alpha) \quad \textbf{Spur} \text{ von } \alpha \text{ bezüglich } L \mid K \end{aligned}$$

Bemerkung 2.9.2. *Die Norm ist multiplikativ und die Spur ist additiv.*

Definition 2.9.3. Sei k ein Körper und A eine assoziative k-Algebra mit Dimension n. Die **Spurform** auf A ist die folgende Abbildung:

$$\begin{aligned} <\cdot,\cdot>_A \colon A \times A &\to k \\ (v, w) &\mapsto <v, w>_A := \mathrm{tr}\ m(v * w) \end{aligned}$$

Definition 2.9.4. Sei k ein Körper, A eine assoziative k-Algebra mit Basis $a_1, \ldots, a_n$ und

$$<\cdot,\cdot>_A \colon A \times A \to k$$

die Spurform auf A. Dann nennt man die Matrix

$$M := \begin{pmatrix} <a_1, a_1>_A & \ldots & <a_1, a_n>_A \\ \ldots & & \ldots \\ <a_n, a_1>_A & \ldots & <a_n, a_n>_A \end{pmatrix}$$

die **Darstellungsmatrix** der Spurform auf A bezüglich der Basis $a_1, \ldots, a_n$.

Definition 2.9.5. Sei k Körper, A eine assoziative k-Algebra, B eine k-Basis von A und M_B die Darstellungsmatrix von $< \cdot, \cdot >_A$ bezüglich B. Dann heißt

$$d_B(A) := \det(M_B)$$

die **Diskriminante** von A bezüglich B.

Kapitel 3

Algebraische Zahlentheorie

In diesem Kapitel wird untersucht, inwieweit man Ideale in bestimmten Unterringen von Zahlkörpern (sogenannten Ordnungen) in Primideale zerlegen kann. Dafür werden im Abschnitt 3.1 zunächst die Begriffe Zahlkörper, Moduln (in Zahlkörpern), Ordnungen (von Zahlkörpern) und (gebrochene) Ideale (von Ordnungen) erläutert und einige Eigenschaften dieser Objekte bewiesen. Mit Hilfe des Begriffs der Bewertung, der im Abschnitt 3.2 eingeführt wird, kann in Abschnitt 3.3 eine spezielle Bewertung eingeführt werden (die Bewertung an invertierbaren Primidealen). Im Verlauf von Abschnitt 3.3 wird erläutert, wie man mit Hilfe dieser Bewertung (gebrochene) Ideale von Ordnungen teilweise in Primidealpotenzen zerlegen kann. Es können dabei jedoch nur invertierbare Primideale aus Idealen herausfaktorisiert werden. Deshalb werden in diesem Abschnitt auch einige Äquivalenzen bewiesen, mit denen man bestimmen kann, ob ein Primideal invertierbar ist. Zusätzlich wird noch gezeigt, dass in der Maximalordnung eines Zahlkörpers alle Primideale invertierbar sind und somit Ideale in der Maximalordnung vollständig zerlegt werden können. Es wird sogar bewiesen, dass diese Zerlegung eindeutig ist. Auch wenn in diesem Kapitel schon einige Algorithmen vorbereitet werden, folgt die genaue Beschreibung und Umsetzung der Algorithmen erst im nächsten Kapitel. Viele Beweise des Kapitels orientieren sich an Beweisen in [Ger09], wobei in [Ger09] teilweise allgemeinere Aussagen gezeigt werden.

3.1 Grundbegriffe

Definition 3.1.1. Ein **(algebraischer) Zahlkörper** K ist eine endliche Erweiterung von $\mathbb{Q}$.

Bemerkung 3.1.2. *Da jede endliche Körpererweiterung algebraisch ist, ist auch jeder Zahlkörper algebraisch über* $\mathbb{Q}$ *(vergleiche* [Fis11, S.259]*).*

Notation. Im gesamten Kapitel über Algebraische Zahlentheorie sei K ein beliebiger Zahlkörper, sofern nicht anders definiert.

3.1.1 Moduln

In diesem Abschnitt werden Moduln in Zahlkörpern definiert und es wird gezeigt, dass Moduln in Zahlkörpern frei sind. Außerdem wird der Quotient von Moduln eingeführt, der benutzt wird, um Ordnungen von Moduln zu erzeugen und Inverse von (gebrochenen) Idealen zu bestimmen (vergleiche die folgenden Abschnitte über Ordnungen und gebrochene Ideale). Schließlich wird noch die Diskriminante von Moduln eingeführt und mit der Diskriminanten-Index-Formel ein Zusammenhang zwischen dem Index von ineinander enthaltenen Moduln und Diskriminanten hergestellt. Die Diskriminante liefert ein Indiz dafür, welche Primideale über einem gegebenen Ideal liegen können (vergleiche Abschnitt 3.3.1).

Definition 3.1.3. Ein **Modul** $\mathfrak{m}$ in K ist ein endlich erzeugter $\mathbb{Z}$-Untermodul von K. Der Modul $\mathfrak{m}$ heißt **vollständig**, wenn er eine $\mathbb{Q}$-Basis von K enthält.

Proposition 3.1.4. *Sei $n := [K : \mathbb{Q}]$ und $\mathfrak{m}$ ein Modul in K. Dann gilt:*

i) $\mathfrak{m}$ ist ein freier Modul.

ii) $rg(\mathfrak{m}) \leq n$, wobei Gleichheit genau dann gilt, wenn $\mathfrak{m}$ vollständig ist.

Beweis. (i) Sei $m \in \mathfrak{m}$ ein Torsionselement, das heißt $r * m = 0$ für ein $r \in \mathbb{Z} \setminus \{0\}$. Dann gilt:

$$m = (r^{-1} * r) * m = r^{-1} * (r * m) = r^{-1} * 0 = 0$$

Somit ist 0 das einzige Torsionselement in $\mathfrak{m}$, also ist $\mathfrak{m}$ torsionsfrei. Da aber $\mathfrak{m}$ endlich erzeugt ist, folgt nach Korollar 2.8.15 daraus, dass der Modul frei ist.

(ii) Nach (i) ist der Modul $\mathfrak{m}$ frei. Somit ist der Rang von $\mathfrak{m}$ wohldefiniert und es gilt $\mathfrak{m} \cong \mathbb{Z}^{\mathrm{rg}(\mathfrak{m})}$. Es gibt also $\mathrm{rg}(\mathfrak{m})$ $\mathbb{Z}$-linear unabhängige Elemente in $\mathfrak{m}$, die $\mathfrak{m}$ erzeugen. Diese sind dann aber auch $\mathbb{Q}$-linear unabhängig. Da K jedoch den Grad n über $\mathbb{Q}$ hat, kann es in K nicht mehr als n Elemente geben, die $\mathbb{Q}$-linear unabhängig sind. Somit gilt $\mathrm{rg}(\mathfrak{m}) \leq n$. Ein Modul ist genau dann vollständig, wenn er eine $\mathbb{Q}$-Basis von K enthält, also $n = [K : \mathbb{Q}]$ Elemente, die $\mathbb{Q}$-linear unabhängig sind. Dies ist genau dann der Fall wenn $\mathrm{rg}(\mathfrak{m})$ gleich n ist.

□

Lemma 3.1.5. *Der Schnitt von zwei vollständigen Moduln $\mathfrak{m}_1$, $\mathfrak{m}_2$ ist vollständig.*

Beweis. Da $\mathfrak{m}_1$ und $\mathfrak{m}_2$ vollständig sind, gibt es $\mathbb{Q}$-Basen $b_1, \ldots, b_n \in \mathfrak{m}_1$ und $m_1, \ldots, m_n \in \mathfrak{m}_2$ von K. Für jedes Element b_i gibt es dann Elemente

$q_{i1}, \dots q_{in} \in \mathbb{Q}$, so dass $b_i = \sum_{j=1}^{n} q_{ij} * m_j$ gilt. Sei nun $s \in \mathbb{Z}$ der Hauptnenner aller q_{ij}. Dann gilt $s * b_i = \sum_{j=1}^{n} s * q_{ij} * m_j$. Da s der Hauptnenner der q_{ij} ist, ist also $s * b_i$ eine $\mathbb{Z}$-Linearkombination von den m_j und somit in $\mathfrak{m}_2$ enthalten. Außerdem sind die $s * b_i$ als $\mathbb{Z}$-Vielfache von Elementen in $\mathfrak{m}_1$ auch in $\mathfrak{m}_1$ enthalten. Somit sind die $s * b_i$ in $\mathfrak{m}_1 \cap \mathfrak{m}_2$ enthalten. Da $b_1, \dots, b_n$ eine $\mathbb{Q}$-Basis von K ist und $s \in \mathbb{Z}$ gilt, ist auch $s * b_1, \dots, s * b_n$ eine $\mathbb{Q}$-Basis von K. Also enthält $\mathfrak{m}_1 \cap \mathfrak{m}_2$ eine $\mathbb{Q}$-Basis von K und ist somit vollständig. □

Definition 3.1.6. Seien $\mathfrak{m}_1$ und $\mathfrak{m}_2 \neq [0]_{\mathbb{Z}}$ Moduln in K. Dann heißt

$$\mathfrak{m}_1 \% \mathfrak{m}_2 := \{\alpha \in K \mid \alpha * \mathfrak{m}_2 \subset \mathfrak{m}_1\}$$

der **Quotient** von $\mathfrak{m}_1$ und $\mathfrak{m}_2$.

Proposition 3.1.7. *Seien $\mathfrak{m}_1, \mathfrak{m}_2$ Moduln in K.*

(i) Für jede $\mathbb{Z}$-Basis $m_1, \dots, m_r$ von $\mathfrak{m}_2$ gilt $\mathfrak{m}_1 \% \mathfrak{m}_2 = \bigcap_{i=1}^{r} (m_i^{-1} * \mathfrak{m}_1)$.

(ii) $\mathfrak{m}_1 \% \mathfrak{m}_2$ ist ein Modul in K.

(iii) Ist $\mathfrak{m}_1$ vollständig, so ist auch $\mathfrak{m}_1 \% \mathfrak{m}_2$ vollständig.

Beweis. (i) Sei zunächst $a \in \mathfrak{m}_1 \% \mathfrak{m}_2$. Dann gilt $a * \mathfrak{m}_2 \subset \mathfrak{m}_1$, also insbesondere $a * m_i \subset \mathfrak{m}_1$ für alle $i \in \{1, \dots, r\}$. Damit ist a in jedem $m_i^{-1} * \mathfrak{m}_1$ enthalten und somit auch in ihrem Schnitt. Sei umgekehrt $a \in \bigcap_{i=1}^{r} (m_i^{-1} * \mathfrak{m}_1)$. Dann gilt $a * m_i \in \mathfrak{m}_1$ für alle i. Da $m_1, \dots, m_r$ eine $\mathbb{Z}$-Basis von $\mathfrak{m}_2$ ist und $\mathfrak{m}_1$ ein $\mathbb{Z}$-Modul ist, gilt also auch $a * \mathfrak{m}_2 \subset \mathfrak{m}_1$ und somit $a \in \mathfrak{m}_1 \% \mathfrak{m}_2$.

(ii) Sei $m_1, \dots, m_r$ eine $\mathbb{Z}$-Basis von $\mathfrak{m}_2$. Nach (i) gilt dann

$$\mathfrak{m}_1 \% \mathfrak{m}_2 = \bigcap_{i=1}^{r} (m_i^{-1} * \mathfrak{m}_1).$$

Somit ist $\mathfrak{m}_1 \% \mathfrak{m}_2$ als Schnitt von endlich vielen $\mathbb{Z}$-Untermoduln von K ebenfalls ein $\mathbb{Z}$-Untermodul von K. Da $\mathfrak{m}_1$ ein endlich erzeugter Modul über $\mathbb{Z}$ ist, ist auch $m_1^{-1} * \mathfrak{m}_1$ ein endlich erzeugter Modul über $\mathbb{Z}$. Somit ist nach Proposition 2.8.11 wegen $\mathbb{Z}$ noethersch auch der endlich erzeugte $\mathbb{Z}$-Modul $m_1^{-1} * \mathfrak{m}_1$ noethersch. Damit ist der Schnitt $\bigcap_{i=1}^{r} (m_i^{-1} * \mathfrak{m}_1)$ als Untermodul von $m_1^{-1} * \mathfrak{m}_1$ ebenfalls endlich erzeugt und somit $\mathfrak{m}_1 \% \mathfrak{m}_2$ ein Modul in K.

(iii) Sei $m_1, \dots, m_r$ eine $\mathbb{Z}$-Basis von $\mathfrak{m}_2$. Ist der Modul $\mathfrak{m}_1$ vollständig, so enthält er eine $\mathbb{Q}$-Basis $b_1, \dots, b_n$ von K. Dann sind aber auch die Elemente $m_i^{-1} * b_1, \dots, m_i^{-1} * b_n$ eine $\mathbb{Q}$-Basis von K und in $m_i^{-1} * \mathfrak{m}_1$ enthalten. Somit sind die $m_i^{-1} * \mathfrak{m}_1$ vollständig. Da nach (i) der Quotient

der Schnitt über die $m_i^{-1} * \mathfrak{m}_1$ ist und nach Lemma 3.1.5 der Schnitt von zwei vollständigen Moduln wieder vollständig ist, zeigt man durch Induktion nach r, dass $\mathfrak{m}_1 \% \mathfrak{m}_2$ vollständig ist.

□

Definition 3.1.8. Sei $\mathfrak{m}$ ein vollständiger Modul in K, B eine Basis von $\mathfrak{m}$. Dann heißt $d(\mathfrak{m}) := d_B(K)$ die **Diskriminante** von $\mathfrak{m}$. Dabei bezeichnet $d_B(K)$ die Diskriminante aus Definition 2.9.5, das heißt die Determinante der Darstellungsmatrix der Spurform auf K bezüglich B.

Bemerkung 3.1.9. *Die Definition ist wohldefiniert, das heißt unabhängig von der Wahl der Modulbasis B.*

Beweis. Seien B, B' zwei $\mathbb{Z}$-Basen von $\mathfrak{m}$. Seien M, M' die Darstellungsmatrizen der Spurform auf K bezüglich der Basen B, B' (vergleiche Definition 2.9.4) und sei $T := T_B^{B'}$ die Transformationsmatrix von B nach B'. Da B und B' $\mathbb{Z}$-Basen des gleichen $\mathbb{Z}$-Moduls sind, muss die Transformationsmatrix Koeffizienten in $\mathbb{Z}$ haben und somit ihre Determinante in $\mathbb{Z}$ sein. Außerdem ist die Transformationsmatrix invertierbar, also ist ihre Determinante sogar eine Einheit in $\mathbb{Z}$, das heißt $\det T = \det T^t = \pm 1$. Wegen $M = T^t * M' * T$ (beziehungsweise $M = T * M' * T^t$, wenn man statt Spalten mit Zeilen rechnet) gilt also

$$d_B(K) = \det M = (\det T)^2 * \det M' = \det M' = d_{B'}(K).$$

□

Theorem 3.1.10 (Diskriminanten-Index-Formel)**.** *Seien $\mathfrak{m}_1, \mathfrak{m}_2$ vollständige Moduln in K mit $\mathfrak{m}_2 \subset \mathfrak{m}_1$. Dann gilt:*

$$d(\mathfrak{m}_2) = (\mathfrak{m}_1 : \mathfrak{m}_2)^2 * d(\mathfrak{m}_1)$$

Beweis. Sei B_1 eine Basis von $\mathfrak{m}_1$ und B_2 eine Basis von $\mathfrak{m}_2$. Sei $T := T_{B_2}^{B_1}$ die Transformationsmatrix von B_2 nach B_1. Seien M_1, M_2 die Darstellungsmatrizen der Spurform bezüglich B_1, B_2. Dann gilt $M_2 = T^t * M_1 * T$ (beim Rechnen mit Spalten). Da die beiden vollständigen Moduln den gleichen Rang haben, gilt nach Lemma 2.8.17, dass der Index von $\mathfrak{m}_1$ über $\mathfrak{m}_2$ endlich und gleich dem Betrag der Determinante der Smith-Normalform S von T ist. Die Smith-Normalform entsteht aber durch Multiplikation mit invertierbaren Matrizen U, V über $\mathbb{Z}$, die Determinante ± 1 haben. Somit folgt:

$$\begin{aligned} d(\mathfrak{m}_2) &= \det M_2 = (\det T)^2 * \det M_1 \\ &= (\det U^t)^2 * (\det S)^2 * (\det V^t)^2 * \det M_1 \\ &= (\det S)^2 * \det M_1 = (\mathfrak{m}_1 : \mathfrak{m}_2)^2 * d(\mathfrak{m}_1) \end{aligned}$$

□

3.1.2 Ordnungen

In diesem Abschnitt werden Ordnungen eingeführt und erläutert, wie man Ordnungen über vollständigen Moduln erzeugt. Außerdem wird gezeigt, dass Ordnungen noethersch sind und es eine Maximalordnung gibt, die alle anderen Ordnungen enthält und dem ganzen Abschluss von $\mathbb{Z}$ in K entspricht. Es wird auch erläutert, warum man durch Multiplikation mit geeigneten Skalaren jeden Modul in beliebige Ordnungen bringen kann. Schließlich wird noch der Begriff des Führers einer Ordnung eingeführt. Es wird in einem späteren Abschnitt noch gezeigt, dass dieser in einem Zusammenhang mit der Invertierbarkeit von Primidealen in Ordnungen steht (siehe Theorem 3.3.28).

Definition 3.1.11. Eine **Ordnung** $\mathcal{O}$ in K ist ein vollständiger Modul, der gleichzeitig ein Unterring von K ist.

Bemerkung 3.1.12. *Im weiteren Verlauf dieses Kapitels sei $\mathcal{O}$ eine beliebige Ordnung in K, sofern nicht anders definiert.*

Proposition 3.1.13. *Jede Ordnung $\mathcal{O}$ in K ist noethersch.*

Beweis. Nach Definition ist $\mathcal{O}$ ein Modul, also ein endlich erzeugter $\mathbb{Z}$-Untermodul von K. Nach Proposition 2.8.11 ist jeder endlich erzeugte Modul über einem noetherschen Ring wieder noethersch. Somit folgt die Behauptung, da $\mathbb{Z}$ ein Hauptidealring und somit nach Beispiel 2.8.5 noethersch ist. □

Bemerkung 3.1.14. *i) Aus einem vollständigen Modul $\mathfrak{m}$ kann man mit dem Quotienten $Ord(\mathfrak{m}) := \mathfrak{m}\%\mathfrak{m} = \{\alpha \in K \mid \alpha * \mathfrak{m} \subset \mathfrak{m}\}$ eine zu $\mathfrak{m}$ gehörige Ordnung konstruieren. Man nennt diese die **Ordnung** von $\mathfrak{m}$.*

ii) Für jede Ordnung $\mathcal{O}$ gilt $Ord(\mathcal{O}) = \mathcal{O}$. Insbesondere ist jede Ordnung die Ordnung von einem vollständigen Modul (nämlich von sich selbst).

Beweis. i) Nach Proposition 3.1.7 (iii) ist $\mathfrak{m}\%\mathfrak{m}$ ein vollständiger Modul, da $\mathfrak{m}$ vollständig ist. Damit dieser ein Unterring von K ist, muss nur noch gezeigt werden, dass das multiplikative neutrale Element 1_K enthalten ist und $\mathfrak{m}\%\mathfrak{m}$ bezüglich $*$ abgeschlossen ist. Man sieht aber sofort, dass $1_K * \mathfrak{m} = \mathfrak{m} \subset \mathfrak{m}$ gilt und aus $\alpha * \mathfrak{m} \subset \mathfrak{m}$ und $\beta * \mathfrak{m} \subset \mathfrak{m}$ folgt

$$(\alpha * \beta) * \mathfrak{m} = \alpha * (\beta * \mathfrak{m}) \subset \alpha * \mathfrak{m} \subset \mathfrak{m}.$$

Damit ist die Behauptung gezeigt.

ii) Sei $\mathcal{O}$ eine Ordnung, also insbesondere ein vollständiger Modul. Da $\mathcal{O}$ ein Ring ist, gilt für alle α in $\mathcal{O}$ die Inklusion $\alpha * \mathcal{O} \subset \mathcal{O}$. Somit ist $\mathcal{O} \subset \mathcal{O}\%\mathcal{O}$. Umgekehrt gilt für alle $\alpha \in \mathcal{O}\%\mathcal{O}$ auch $\alpha * \mathcal{O} \subset \mathcal{O}$, also insbesondere $\alpha = \alpha * 1_K \in \mathcal{O}$. Deshalb ist auch $\mathcal{O}\%\mathcal{O} \subset \mathcal{O}$. Damit wurde gezeigt, dass $\mathrm{Ord}(\mathcal{O}) = \mathcal{O}\%\mathcal{O} = \mathcal{O}$ ist und somit die Behauptung.

□

Lemma 3.1.15. *Seien $\mathcal{O}_1$, $\mathcal{O}_2$ zwei Ordnungen in K. Dann ist das Produkt $\mathcal{O} := \mathcal{O}_1 * \mathcal{O}_2$ ein vollständiger Modul und $\mathcal{O}_1, \mathcal{O}_2$ sind in der Ordnung $Ord(\mathcal{O}_1, \mathcal{O}_2) := Ord(\mathcal{O}_1 * \mathcal{O}_2)$ enthalten.*

Beweis. Als Produkt von $\mathbb{Z}$-Untermoduln von K ist $\mathcal{O}$ ein $\mathbb{Z}$-Untermodul von K. Da $1 \in \mathcal{O}_2$ gilt, ist auch $\mathcal{O}_1 * 1 \subset \mathcal{O}_1 * \mathcal{O}_2$. Somit enthält $\mathcal{O}$ ganz $\mathcal{O}_1$, also insbesondere die $\mathbb{Q}$-Basis von K, die wegen der Vollständigkeit in $\mathcal{O}_1$ enthalten ist. Also ist auch $\mathcal{O}$ vollständig und es kann die Ordnung $\mathrm{Ord}(\mathcal{O})$ gebildet werden. Sei $m_1, \ldots, m_n$ eine $\mathbb{Z}$-Basis von $\mathcal{O}_1$ und $\bar{m}_1, \ldots, \bar{m}_n$ eine $\mathbb{Z}$-Basis von $\mathcal{O}_2$. Dann sind die Elemente $m_{ij} = m_i * \bar{m}_j$ ein $\mathbb{Z}$-Erzeugendensystem von $\mathcal{O}$. Sei $o \in \mathcal{O}_1$. Es ist zu zeigen, dass $o * \mathcal{O} \subset \mathcal{O}$ gilt. Dafür reicht es zu zeigen, dass $o * m_{ij} \subset \mathcal{O}$ gilt für alle m_{ij}. Dies folgt aber direkt aus

$$o * m_{ij} = o * (m_i * \bar{m}_j) = (o * m_i) * \bar{m}_j \subset \mathcal{O}_1 * \mathcal{O}_2$$

Somit ist $o \in \mathrm{Ord}(\mathcal{O})$, also insgesamt $\mathcal{O}_1 \subset \mathrm{Ord}(\mathcal{O})$. Analog dazu kann man auch zeigen, dass $\mathcal{O}_2 \subset \mathrm{Ord}(\mathcal{O})$ gilt. □

Theorem 3.1.16. *Es gibt eine Ordnung $\mathcal{O}_K$ in K, die alle Ordnungen in K enthält. Diese ist somit eindeutig und man nennt sie die **Maximalordnung** von K.*

Beweis. Sei $(\mathcal{O}_i)_{i \in \mathbb{N}}$ eine aufsteigende Kette von Ordnungen bezüglich Inklusion. Nach Lemma 3.1.10 [Diskriminanten-Index-Formel] ist die dazugehörige Diskriminantenfolge $d(\mathcal{O}_i)_{i \in \mathbb{N}}$ eine monoton absteigende Folge von Zahlen in $\mathbb{N}$ oder eine monoton aufsteigende Folge von Zahlen in $-\mathbb{N}$. Somit wird die Diskriminantenfolge stationär und damit auch die Folge der Ordnungen, da nach Lemma 3.1.10 [Diskriminanten-Index-Formel] zwei echt ineinander enthaltene Ordnungen unterschiedliche Diskriminanten haben. Insbesondere ist die Kette der Ordnungen nach oben beschränkt. Nach dem Lemma von Zorn folgt also, dass es ein maximales Element in der Menge der Ordnungen von K gibt. Sei nun ein solches maximales Element $\mathcal{O}_K$ und eine beliebige Ordnung $\mathcal{O}$ gegeben. Dann enthält nach Lemma 3.1.15 die Ordnung $\mathrm{Ord}(\mathcal{O}_K, \mathcal{O})$ sowohl $\mathcal{O}_K$ als auch $\mathcal{O}$. Wegen der Maximalität von $\mathcal{O}_K$ gilt also $\mathcal{O} \subset \mathrm{Ord}(\mathcal{O}_K, \mathcal{O}) = \mathcal{O}_K$ und damit ist die Behauptung gezeigt. □

Proposition 3.1.17. *Sei $\mathcal{O}$ eine Ordnung in K und $\alpha \in \mathcal{O}$. Dann ist α ganz über $\mathbb{Z}$.*

Beweis. Die Ordnung $\mathcal{O}$ ist ein endlich erzeugter $\mathbb{Z}$-Untermodul von K. Somit ist $\mathcal{O} \mid \mathbb{Z}$ eine endliche Ringerweiterung und damit nach Lemma 2.4.3 jedes Element $\alpha \in \mathcal{O}$ ganz über $\mathbb{Z}$. □

Korollar 3.1.18. *Die Ordnung $\mathcal{O}_K$ stimmt mit dem ganzen Abschluss $\bar{\mathbb{Z}}^K$ von $\mathbb{Z}$ in K überein.*

Beweis. Nach Proposition 3.1.17 ist jedes Element in $\mathcal{O}_K$ ganz über $\mathbb{Z}$. Noch zu zeigen ist, dass jede ganze Zahl über $\mathbb{Z}$ in einer Ordnung enthalten ist und somit auch in der Maximalordnung. Sei $\alpha \in K$ ganz über $\mathbb{Z}$ und $\mathcal{O}$ eine beliebige Ordnung von K. Dann ist α auch ganz über $\mathcal{O}$, da $\mathbb{Z} \subset \mathcal{O}$ gilt. Nach Lemma 2.4.4 ist dann $\mathcal{O}[\alpha]$ ein endlich erzeugter $\mathcal{O}$-Modul. Der Modul $\mathcal{O}$ ist aber ein endlich erzeugter $\mathbb{Z}$-Modul, also ist $\mathcal{O}[\alpha]$ auch ein endlich erzeugter $\mathbb{Z}$-Modul und somit wegen $\mathcal{O}[\alpha] \subset K$ ein Modul in K. Da $\mathcal{O}$ eine $\mathbb{Q}$-Basis von K enthält, enthält auch $\mathcal{O}[\alpha]$ eine $\mathbb{Q}$-Basis von K, ist also vollständig. Außerdem ist $\mathcal{O}[\alpha]$ ein Unterring von K und somit sogar eine Ordnung. Es folgt $\alpha \subset \mathcal{O}[\alpha] \subset \mathcal{O}_K$. □

Definition 3.1.19. Wegen Korollar 3.1.18 nennt man $\mathcal{O}_K$ auch den **Ganzheitsring** von K.

Definition 3.1.20. Sei K ein Zahlkörper, $\mathcal{O}$ eine Ordnung in K. Dann ist der Modul $\mathfrak{F}_\mathcal{O} := \mathcal{O}\%\mathcal{O}_K = \{x \in K \mid x * \mathcal{O}_K \subset \mathcal{O}\}$ ein Ideal und heißt der **Führer** von $\mathcal{O}$.

Beweis. Da der Quotient $\mathcal{O}\%\mathcal{O}_K$ ein Modul in K ist, ist er insbesondere eine Untergruppe von $(K, +)$. Er ist außerdem in $\mathcal{O}$ enthalten, da für alle $x \in \mathcal{O}\%\mathcal{O}_K$ die Gleichung $x * \mathcal{O}_K \subset \mathcal{O}$ gilt, also insbesondere $x * 1 \in \mathcal{O}$. Somit ist der Quotient sogar eine Untergruppe von $(\mathcal{O}, +)$. Es bleibt noch zu zeigen, dass der Quotient abgeschlossen bezüglich Multiplikation mit $\mathcal{O}$ ist, aber das ist aufgrund von $\mathcal{O} \subset \mathcal{O}_K$ und $x * \mathcal{O}_K \subset \mathcal{O}$ klar. □

Bemerkung 3.1.21. *Der Führer ist das größte Ideal von $\mathcal{O}_K$, das auch ein Ideal in $\mathcal{O}$ ist. Betrachtet man den Führer von $\mathcal{O}_K$, so erhält man:*

$$\mathfrak{F}_{\mathcal{O}_K} = \mathcal{O}_K\%\mathcal{O}_K = Ord(\mathcal{O}_K) = \mathcal{O}_K = (1)_{\mathcal{O}_K}$$

Proposition 3.1.22. *Sei $\mathcal{O}$ eine Ordnung in K.*

(i) Sei $x \in K$. Dann gibt es ein $z \in \mathbb{Z}$ mit $z * x \in \mathcal{O}$.

(ii) Sei $\mathfrak{m}$ ein Modul in K. Dann gibt es ein $z \in \mathbb{Z}$ mit $z * \mathfrak{m} \subset \mathcal{O}$.

Beweis. (i) Sei $a_1, \ldots, a_n$ eine $\mathbb{Q}$-Basis von K, die in $\mathcal{O}$ enthalten ist. Diese existiert, da $\mathcal{O}$ ein vollständiger Modul ist. Dann lässt sich $x \in K$ als Linearkombination

$$x = q_1 * a_1 + q_2 * a_2 + \ldots + q_n * a_n$$

schreiben mit Elementen $q_1, \ldots, q_n \in \mathbb{Q}$. Sei z der Hauptnenner der q_i. Dann folgt:

$$x = q_1 * a_1 + q_2 * a_2 + \ldots + q_n * a_n = \frac{q_1 * z}{z} * a_1 + \frac{q_2 * z}{z} * a_2 + \ldots + \frac{q_n * z}{z} * a_n$$

Setzt man nun $z_i := q_i * z$, so ergibt sich

$$z * x = z_1 * a_1 + z_2 * a_2 + \ldots + z_n * a_n$$

Da z der Hauptnenner der q_i ist, sind die z_i in $\mathbb{Z}$. Außerdem sind die a_i in $\mathcal{O}$, also ist $z * x$ eine $\mathbb{Z}$-Linearkombination von Elementen in $\mathcal{O}$ und somit in $\mathcal{O}$ enthalten.

(ii) Sei $m_1, \ldots, m_r$ ein $\mathbb{Z}$-Erzeugendensystem von $\mathfrak{m}$. Nach (i) gibt es $z_i \in \mathbb{Z}$ mit $z_i * m_i \in \mathcal{O}$. Sei z das kleinste gemeinsame Vielfache von den z_i. Dann sind die Elemente $z * m_i$ ebenfalls in $\mathcal{O}$. Alle Elemente aus $\mathfrak{m}$ sind $\mathbb{Z}$-Linearkombinationen der m_i, somit sind alle Elemente aus $z * \mathfrak{m}$ auch $\mathbb{Z}$-Linearkombinationen von der Menge der $z * m_i \in \mathcal{O}$. Damit ist $z * \mathfrak{m} \subset \mathcal{O}$.

□

3.1.3 Gebrochene und ganzzahlige Ideale

In diesem Abschnitt werden gebrochene und ganzzahlige Ideale von Ordnungen definiert und der Zusammenhang mit dem üblichen Idealbegriff und mit vollständigen Moduln erläutert. Außerdem wird Invertierbarkeit von gebrochenen Idealen definiert und gezeigt, wie man das Inverse eines gebrochenen Ideals berechnen kann (sofern es existiert).

Definition 3.1.23. Sei $\mathfrak{a}$ ein $\mathcal{O}$-Untermodul von K, der von endlich vielen Elementen $a_1, \ldots, a_n$ erzeugt wird. Dann nennt man $\mathfrak{a}$ ein **gebrochenes Ideal** von $\mathcal{O}$.

Notation. Das gebrochene Ideal $\mathfrak{a}$ aus der obigen Definition wird im folgenden auch als $(a_1, \ldots, a_n)_\mathcal{O}$ oder (falls $\mathcal{O}$ klar ist) auch als $(a_1, \ldots, a_n)$ bezeichnet.

Definition 3.1.24. Sei $\mathfrak{a} = (a_1, \ldots, a_n)_\mathcal{O}$ ein gebrochenes Ideal von $\mathcal{O}$. Sind die Erzeuger $a_1, \ldots, a_n$ in $\mathcal{O}$, so nennt man das Ideal ein **ganzzahliges Ideal** von $\mathcal{O}$. Wird ein gebrochenes/ganzzahliges Ideal von genau einem Element $a \in K$ erzeugt, so nennt man $\mathfrak{a} = (a)_\mathcal{O}$ ein gebrochenes/ganzzahliges **Hauptideal** von $\mathcal{O}$.

Bemerkung 3.1.25. *Die ganzzahligen Ideale der Ordnung $\mathcal{O}$ sind genau die Ring-Ideale im Ring $\mathcal{O}$.*

Beweis. Ist $\mathfrak{a}$ ein ganzzahliges Ideal von $\mathcal{O}$, so ist es ein $\mathcal{O}$-Untermodul von K, der wegen der Ganzzahligkeit in $\mathcal{O}$ enthalten ist. Damit ist $\mathfrak{a}$ ein $\mathcal{O}$-Untermodul von $\mathcal{O}$ und somit ein Ring-Ideal.

Ist $\mathfrak{a}$ ein Ring-Ideal, so ist es ein $\mathcal{O}$-Untermodul von $\mathcal{O}$. Da $\mathcal{O}$ noethersch ist, ist nach Theorem 2.8.4 der Untermodul $\mathfrak{a}$ endlich erzeugt über $\mathcal{O}$ und somit auch endlich erzeugt über $\mathbb{Z}$, da $\mathcal{O}$ ein endlich erzeugter $\mathbb{Z}$-Modul ist. Damit ist $\mathfrak{a}$ ein gebrochenes Ideal. Da die Erzeuger in $\mathcal{O}$ sind, ist es sogar ein ganzzahliges Ideal.

□

Proposition 3.1.26. *(i) Jeder vollständige Modul $\mathfrak{m}$ in K ist ein gebrochenes Ideal von Ord($\mathfrak{m}$).*

(ii) Jedes gebrochene Ideal $\mathfrak{a} \neq (0)_{\mathcal{O}}$ von einer Ordnung $\mathcal{O}$ von K ist ein vollständiger Modul in K.

Beweis. (i) Der Modul $\mathfrak{m}$ ist ein $\mathbb{Z}$-Untermodul von K und somit insbesondere eine Untergruppe von $(K, +)$. Die Ordnung $\mathrm{Ord}(\mathfrak{m})$ von einem vollständigen Modul $\mathfrak{m}$ sind die Elemente in K, die man mit ganz $\mathfrak{m}$ multiplizieren kann, ohne den Modul zu verlassen. Somit ist $\mathfrak{m}$ abgeschlossen bezüglich Multiplikation mit $\mathrm{Ord}(\mathfrak{m})$. Da der Modul $\mathfrak{m}$ schon als $\mathbb{Z}$-Modul endlich erzeugt ist, ist er auch als $\mathrm{Ord}(\mathfrak{m})$-Modul endlich erzeugt. Also ist er ein gebrochenes Ideal von $\mathrm{Ord}(\mathfrak{m})$.

(ii) Das gebrochene Ideal $\mathfrak{a} = (a_1, \ldots, a_r)_{\mathcal{O}}$ entspricht dem Modul-Produkt $[a_1, \ldots, a_r]_{\mathbb{Z}} * \mathcal{O}$, ist also ein Modul in K. Da $\mathcal{O}$ vollständig ist, enthält $\mathcal{O}$ eine $\mathbb{Q}$-Basis $b_1, \ldots, b_n$ von K. Dann ist aber $a_1 * b_1, \ldots, a_1 * b_n$ ebenfalls eine $\mathbb{Q}$-Basis von K und in $\mathfrak{a}$ enthalten (wobei ohne Beschränkung der Allgemeinheit $a_1 \neq 0$ vorausgesetzt wird), da Multiplikation mit einem Zahlkörperelement ungleich 0 die $\mathbb{Q}$-lineare Unabhängigkeit erhält.

□

Korollar 3.1.27. *Sei $\mathfrak{a} = (a_1, \ldots, a_r)_{\mathcal{O}}$ ein gebrochenes Ideal von $\mathcal{O}$. Dann gibt es ein $z \in \mathbb{Z}$, so dass $z * \mathfrak{a}$ ein ganzzahliges Ideal in $\mathcal{O}$ ist.*

Beweis. Da $\mathfrak{a}$ nach Proposition 3.1.26 ein Modul ist, gibt es nach Proposition 3.1.22 ein Element $z \in \mathbb{Z}$, so dass $z * \mathfrak{a} \subset \mathcal{O}$ gilt. Außerdem ist $z * \mathfrak{a}$ ein gebrochenes Ideal, das von $z * a_1, \ldots, z * a_r$ erzeugt wird. Somit ist $z * \mathfrak{a}$ ein ganzzahliges Ideal in $\mathcal{O}$. □

Definition 3.1.28. Sei $\mathfrak{a}$ ein gebrochenes Ideal von $\mathcal{O}$. $\mathfrak{a}$ heißt **invertierbar** (in $\mathcal{O}$), falls es ein gebrochenes Ideal $\mathfrak{b}$ gibt, so dass $\mathfrak{a} * \mathfrak{b} = (1)_{\mathcal{O}} = \mathcal{O}$ gilt.

Proposition 3.1.29. *(i) Sei $\mathfrak{a} = (a)_{\mathcal{O}}$ ein gebrochenes Hauptideal mit $a \neq 0$. Dann ist $\mathfrak{a}$ in $\mathcal{O}$ invertierbar.*

(ii) Sei $\mathfrak{a} = \prod_{i=1}^{r} \mathfrak{a}_i$ ein Produkt von gebrochenen Idealen. Dann ist $\mathfrak{a}$ genau dann invertierbar, wenn alle $\mathfrak{a}_i$ invertierbar sind.

Beweis. (i) Der Erzeuger $a \neq 0$ ist in $(K, *)$ invertierbar und mit dem gebrochenen Hauptideal $(a^{-1})_{\mathcal{O}}$ ergibt sich

$$(a)_{\mathcal{O}} * (a^{-1})_{\mathcal{O}} = (a * a^{-1})_{\mathcal{O}} = (1)_{\mathcal{O}}.$$

Damit ist $\mathfrak{a}$ invertierbar.

(ii) Sei zunächst $\mathfrak{a} = \prod_{i=1}^{r} \mathfrak{a}_i$ invertierbar mit Inversem $\mathfrak{b}$. Dann gilt:

$$\mathfrak{a}_i * (\mathfrak{a}_1 * \ldots * \mathfrak{a}_{i-1} * \mathfrak{a}_{i+1} * \ldots * \mathfrak{a}_r * \mathfrak{b}) = (\mathfrak{a}_1 * \ldots * \mathfrak{a}_r) * \mathfrak{b} = \mathfrak{a} * \mathfrak{b} = (1)_{\mathcal{O}}$$

Somit ist jedes $\mathfrak{a}_i$ invertierbar. Seien nun umgekehrt alle $\mathfrak{a}_i$ invertierbar mit Inversen $\mathfrak{b}_i$. Dann gilt:

$$\mathfrak{a} * (\prod_{i=1}^{r} \mathfrak{b}_i) = (\prod_{i=1}^{r} \mathfrak{a}_i)(\prod_{i=1}^{r} \mathfrak{b}_i) = \prod_{i=1}^{r} (\mathfrak{a}_i * \mathfrak{b}_i) = \prod_{i=1}^{r} (1)_{\mathcal{O}} = (1)_{\mathcal{O}}$$

Somit ist auch $\mathfrak{a}$ invertierbar.

□

Proposition 3.1.30. *Definiere für jedes gebrochene Ideal $\mathfrak{a}$ von $\mathcal{O}$:*

$$\tilde{\mathfrak{a}} := \mathcal{O}\%\mathfrak{a} = \{x \in K \mid x * \mathfrak{a} \subset \mathcal{O}\}$$

Dann ist $\mathfrak{a}$ genau dann invertierbar, wenn $\mathfrak{a} * \tilde{\mathfrak{a}} = (1)_{\mathcal{O}} = \mathcal{O}$ gilt.

Beweis. Sei zunächst $\mathfrak{a}$ invertierbar. Dann gibt es ein gebrochenes Ideal $\mathfrak{b}$ mit $\mathfrak{b} * \mathfrak{a} = (1)_{\mathcal{O}}$. Somit bleibt für jedes $b \in \mathfrak{b}$ das Produkt $b * \mathfrak{a}$ in $\mathcal{O}$. Deshalb gilt $\mathfrak{b} \subset \tilde{\mathfrak{a}}$. Es folgt sofort:

$$(1)_{\mathcal{O}} = \mathfrak{a} * \mathfrak{b} \subset \mathfrak{a} * \tilde{\mathfrak{a}} \subset \mathcal{O} = (1)_{\mathcal{O}}$$

Damit ist $\tilde{\mathfrak{a}}$ ein Inverses (beziehungsweise das Inverse) zu $\mathfrak{a}$. Die Rückrichtung folgt direkt aus der Definition von Invertierbarkeit. □

Notation. Im Folgenden wird $\tilde{\mathfrak{a}}$ auch als $\mathfrak{a}^{-1}$ bezeichnet, wenn bekannt ist, dass das Ideal invertierbar ist.

3.2 Bewertungen

Damit im nächsten Abschnitt die Bewertung über Primideale leichter eingeführt werden kann, werden hier zunächst die allgemeineren Begriffe „Bewertung“ und „diskrete Bewertung“ definiert. Es wird außerdem dargestellt, wie man jeder surjektiven Bewertung einen Bewertungsring zuordnen kann und jedem Bewertungsring eine surjektive Bewertung. Schließlich werden einige Eigenschaften und Sätze der Bewertung bewiesen, die im nächsten Abschnitt benötigt werden. Einige der Beweise orientieren sich dabei an [Kir04].

3.2.1 Definitionen

Definition 3.2.1. Sei k ein Körper, $k^* = (k \setminus \{0\}, *)$ die Einheitengruppe von k. Sei $(G, +, \geq)$ eine total geordnete abelsche Gruppe und $(G_\infty, +, \geq)$ der total geordnete abelsche Monoid, der durch Erweiterung von G mit ∞ entsteht, das heißt:

$$\begin{array}{rcll} G_\infty & := & G \cup \{\infty\} & \\ x + \infty & := & \infty & \forall\ x \in G_\infty \\ \infty & :\geq & x & \forall\ x \in G_\infty \end{array}$$

Dann heißt eine Abbildung $\nu : k \to G_\infty$ **(Exponential-)Bewertung**, wenn sie für alle $x, y \in k$ die folgenden Eigenschaften erfüllt:

a) $\nu(x) = \infty \Leftrightarrow x = 0_k$

b) $\nu(x + y) \geq \min(\nu(x), \nu(y))$

c) $\nu(x * y) = \nu(x) + \nu(y)$

Bemerkung 3.2.2. *Man kann annehmen, dass die Bewertung surjektiv ist, da ansonsten $\bar{G} := \nu(k^*)$ eine geordnete abelsche Untergruppe von G ist. Die Bewertung ist dann surjektiv auf $\bar{G}_\infty$.*

Lemma 3.2.3. *Sei R ein Integritätsring mit Quotientenkörper k, $(G, +, \geq)$ eine total geordnete abelsche Gruppe und $\tilde{\nu} : R \to G_\infty$ eine Abbildung, die für $a, b \in R^* = R \setminus \{0_R\}$ die folgenden Eigenschaften erfüllt:*

(i) $\tilde{\nu}(0_R) = \infty$

(ii) $\tilde{\nu}(R^*) = G^+ := \{x \in G \mid x \geq 0_G\}$

(iii) $\tilde{\nu}(a + b) \geq \min(\tilde{\nu}(a), \tilde{\nu}(b))$

(iv) $\tilde{\nu}(a * b) = \tilde{\nu}(a) + \tilde{\nu}(b)$

Dann ist die Abbildung

$$\begin{array}{rcll} \nu : k & \to & G_\infty & \\ \frac{a}{b} & \mapsto & \tilde{\nu}(a) - \tilde{\nu}(b) & \forall\ a \in R, b \in R \setminus \{0_R\} \end{array}$$

wohldefiniert und eine surjektive Bewertung auf k.

Beweis. Die beiden Eigenschaften (iii) und (iv) von $\tilde{\nu}$ für $a, b \in R \setminus \{0_R\}$ gelten auch für $a, b \in R$, da ohne Beschränkung der Allgemeinheit für $a \in R$, $b = 0_R$ folgendes gilt:

$\tilde{\nu}(a + 0_R) = \tilde{\nu}(a) = \min(\tilde{\nu}(a), \infty) = \min(\tilde{\nu}(a), \tilde{\nu}(0_R))$

$\tilde{\nu}(a * 0_R) = \tilde{\nu}(0_R) = \infty = \tilde{\nu}(a) + \infty = \tilde{\nu}(a) + \tilde{\nu}(0_R)$

Mit diesen Eigenschaften kann man nun die Wohldefiniertheit und die Bewertungseigenschaften für die Abbildung ν zeigen. Für die Wohldefiniertheit betrachte man zwei verschiedene Darstellungen $\frac{a}{b}$, $\frac{c}{d}$ eines Elements $x \in k$, wobei $a, c \in R$ und $b, d \in R \setminus \{0_R\}$ gilt. Da R ein Integritätsring ist, gilt dann die Gleichung $a * d = b * c$. Somit gilt

$$\tilde{\nu}(a) + \tilde{\nu}(d) = \tilde{\nu}(a * d) = \tilde{\nu}(b * c) = \tilde{\nu}(b) + \tilde{\nu}(c).$$

Daraus folgt

$$\nu(\frac{a}{b}) = \tilde{\nu}(a) - \tilde{\nu}(b) = \tilde{\nu}(c) - \tilde{\nu}(d) = \nu(\frac{c}{d})$$

und somit die Wohldefiniertheit. Nun sind noch die Eigenschaften der Bewertung und die Surjektivität zu zeigen.

a) Wegen

$$\tilde{\nu}(1_R) = \tilde{\nu}(1_R * 1_R) = \tilde{\nu}(1_R) + \tilde{\nu}(1_R)$$

gilt $\tilde{\nu}(1_R) = 0_G$. Somit ist

$$\nu(0_k) = \tilde{\nu}(0_R) - \tilde{\nu}(1_R) = \infty - 0_G = \infty.$$

Ist umgekehrt $\nu(\frac{a}{b}) = \infty$ für $a \in R$, $b \in R \setminus \{0_R\}$, so gilt

$$\infty = \infty + \tilde{\nu}(b) = \nu(\frac{a}{b}) + \tilde{\nu}(b) = \tilde{\nu}(a).$$

Nach Voraussetzung ist aber $\tilde{\nu}(a) \in G^+ \not\ni \infty$ für $a \neq 0_R$. Somit gilt $a = 0_R$ und deshalb $\frac{a}{b} = 0_k$.

b) Seien $x = \frac{a}{b}, y = \frac{c}{d} \in k$ mit $a, c \in R$, $b, d \in R \setminus \{0_R\}$. Dann gilt

$$\begin{aligned}
\nu(x+y) &= \nu(\tfrac{a}{b} + \tfrac{c}{d}) = \nu(\tfrac{ad+bc}{bd}) = \tilde{\nu}(ad+bc) - \tilde{\nu}(bd) \\
&\geq \min\{\tilde{\nu}(ad), \tilde{\nu}(bc)\} - \tilde{\nu}(bd) \\
&= \min\{\tilde{\nu}(ad) - \tilde{\nu}(bd), \tilde{\nu}(bc) - \tilde{\nu}(bd)\} \\
&= \min\{\nu(\tfrac{ad}{bd}), \nu(\tfrac{bc}{bd})\} = \min\{\nu(\tfrac{a}{b}), \nu(\tfrac{c}{d})\} \\
&= \min\{\nu(x), \nu(y)\}
\end{aligned}$$

c) Seien $x = \frac{a}{b}, y = \frac{c}{d} \in k$ mit $a, c \in R$, $b, d \in R \setminus \{0_R\}$. Dann gilt

$$\begin{aligned}
\nu(x*y) &= \nu(\tfrac{ac}{bd}) = \tilde{\nu}(ac) - \tilde{\nu}(bd) = (\tilde{\nu}(a) + \tilde{\nu}(c)) - (\tilde{\nu}(b) + \tilde{\nu}(d)) \\
&= \tilde{\nu}(a) - \tilde{\nu}(b) + \tilde{\nu}(c) - \tilde{\nu}(d) = \nu(\tfrac{a}{b}) + \nu(\tfrac{c}{d}) \\
&= \nu(x) + \nu(y)
\end{aligned}$$

Damit sind die Eigenschaften einer Bewertung erfüllt. Sei nun $z \in G \cup \{\infty\}$. Es ist zu zeigen, dass z im Bild von ν ist. Für $z = \infty$ gilt $z = \nu(0_k)$. Gilt $z \in G$ und $z \geq 0_G$, so ist $z = \tilde{\nu}(a) = \nu(\frac{a}{1_R})$ für ein $a \in R^*$ wegen (ii). Ist hingegen $z \in G$ mit $z \leq 0_G$, so ist $-z \geq 0_G$ und somit $-z = \tilde{\nu}(b) = \nu(\frac{b}{1_R})$ für ein $b \in R^*$. Damit ist aber $z = 0_G - \tilde{\nu}(b) = \tilde{\nu}(1_R) - \tilde{\nu}(b) = \nu(\frac{1}{b})$. □

Beispiel 3.2.4. Sei $G = \{0_G\}$. Die Abbildung

$$\begin{array}{rccll} \nu_0 : & k & \to & G_\infty & \\ & x & \mapsto & 0_G & \forall\, x \in k^* \\ & 0_k & \mapsto & \infty & \end{array}$$

definiert offensichtlich eine Bewertung. Man nennt diese die **triviale** Bewertung von k. Hat das Bild einer Bewertung noch andere Werte als 0_G und ∞, so nennt man sie **nicht-trivial**.

Definition 3.2.5. Sei R ein Integritätsring, k sein Quotientenkörper. Dann heißt R **Bewertungsring**, wenn für jedes $x \in k^*$ mindestens eines der Elemente x, x^{-1} in R ist.

Beispiel 3.2.6. Sei $\nu : k \to G_\infty$ eine Bewertung. Dann ist die Menge $R_\nu := \{x \in k \mid \nu(x) \geq 0_G\}$ ein Bewertungsring.

Beweis. Es gilt $\nu(0_k) = \infty \geq 0_G$ und somit $0_k \in R_\nu$. Da ν eine Bewertung ist, gilt außerdem für zwei Elemente $a, b \in R_\nu$

$$\begin{array}{rcl} \nu(a+b) & \geq & \min\{\nu(a), \nu(b)\} \geq 0_G \\ \nu(a*b) & = & \nu(a) + \nu(b) \geq 0_G + 0_G = 0_G. \end{array}$$

Also ist R_ν ein Unterring vom nullteilerfreien kommutativen Ring k und somit ebenfalls nullteilerfrei und kommutativ. Wegen

$$\nu(1_k) = \nu(1_k * 1_k) = \nu(1_k) + \nu(1_k)$$

ist $\nu(1_k) = 0_G$ und somit $1_k \in R_\nu$. Damit ist R_ν ein Integritätsring. Betrachtet man nun ein Element $x \in k^*$, so muss man nur zeigen, dass aus $x \notin R_\nu$ sofort $x^{-1} \in R_\nu$ folgt. Ist $x \notin R_\nu$, so gilt insbesondere $0_G \geq \nu(x)$. Damit folgt

$$\nu(x^{-1}) = 0_G + \nu(x^{-1}) \geq \nu(x) + \nu(x^{-1}) = \nu(x * x^{-1}) = \nu(1) = 0_G$$

und somit $x^{-1} \in R_\nu$. □

Lemma 3.2.7. *Sei R ein Bewertungsring, k sein Quotientenkörper. Sei $(G, \oplus, \geq)$ definiert durch die Faktorgruppe k^*/R^*, das heißt*

$$\begin{array}{rcl} G & := & k^*/R^* \\ [x] & := & x * R^* \in k^*/R^* \\ [x] \oplus [y] & := & (x*y) * R^* = [x*y] \\ [x] \geq [y] & :\Leftrightarrow & \dfrac{x}{y} \in R \subset k \end{array}$$

wobei $x, y \in k^*$ sind. Dann ist $(G, \oplus, \geq)$ eine total geordnete abelsche Gruppe.

Beweis. Zunächst ist $(G, \oplus)$ als Faktorgruppe eine Gruppe. Wegen R kommutativ ist $(k^*, *)$ kommutativ und somit auch die Faktorgruppe G. Man beachte, dass das neutrale Element 0_G durch $[1_k] = 1_k * R^*$ gegeben ist. Es ist noch zu zeigen, dass die Ordnungsrelation total, reflexiv, transitiv und verträglich mit der Gruppenstruktur ist.

a) Totalität: Die Ordnungsrelation ist für alle $[a], [b] \in k^*/R^*$, $a, b \in k^*$ definiert, da wegen R Bewertungsring $\frac{a}{b} \in R$ oder $\frac{b}{a} \in R$ gilt und somit $[a] \geq [b]$ oder $[b] \geq [a]$ gilt.

b) Reflexivität: Für $x \in k^*$ gilt $\frac{x}{x} = 1_k = 1_R \in R$ und somit $[x] \geq [x]$.

c) Transitivität: Für $x, y, z \in k^*$ gilt

$$\begin{array}{rcl} [x] \geq [y] \wedge [y] \geq [z] & \Leftrightarrow & \frac{x}{y} \in R \wedge \frac{y}{z} \in R \\ & \Rightarrow & \frac{x}{z} = \frac{x}{y} * \frac{y}{z} \in R \quad \Leftrightarrow \quad [x] \geq [z] \end{array}$$

d) Verträglichkeit mit Gruppenstruktur: Für $x, y, z \in k^*$ mit $[x] \geq [y]$ gilt $\frac{x}{y} \in R$. Also ist $\frac{x*z}{y*z} = \frac{x}{y} \in R$ und somit auch

$$[x] \oplus [z] = [x * z] \geq [y * z] = [y] \oplus [z].$$

□

Beispiel 3.2.8. Sei R ein Bewertungsring, $k = R \setminus \{0_R\}^{-1} R$ sein Quotientenkörper. Sei $(G, \oplus) := (k^*/R^*, \odot)$ die Faktorgruppe der Einheitengruppen von k und R. Dann ist

$$\begin{array}{rcl} \nu : k & \to & G \cup \infty \\ 0_k & \mapsto & \infty \\ x & \mapsto & [x] := x * R^* \end{array}$$

eine surjektive Bewertung auf dem Quotientenkörper k von R, wobei die Ordnungsrelation auf G durch $[a] \geq [b] \Leftrightarrow \frac{a}{b} \in R$ definiert ist.

Beweis. Nach Lemma 3.2.7 ist $(G, \oplus, \geq)$ eine total geordnete abelsche Gruppe. Da für $x \in R^*$ die Äquivalenz $[x] \geq 0_G = [1_k] \Leftrightarrow x = \frac{x}{1_k} \in R$ gegeben ist, ist die Abbildung

$$\nu \restriction_{R^*} \colon R \setminus \{0_R\} \to G^+ := \{[x] \in G \mid [x] \geq 0_G\} = \{[x] \mid x \in R^*\}$$

eine surjektive Abbildung in die positive Menge der total geordneten abelschen Gruppe G. Es gilt außerdem $\nu(0_R) = \nu(0_k) = \infty$ und die Abbildung $\tilde{\nu} := \nu \restriction_R$ erfüllt für alle $x, y \in R \setminus \{0\}$ die Eigenschaften

(i) $\tilde{\nu}(x + y) \geq \min\{\tilde{\nu}(x), \tilde{\nu}(y)\}$

(ii) $\tilde{\nu}(x * y) = \tilde{\nu}(x) \oplus \tilde{\nu}(y)$,

da folgendes gilt:

(i) Sei ohne Beschränkung der Allgemeinheit $\min\{\tilde{\nu}(x), \tilde{\nu}(y)\} = \tilde{\nu}(y)$, das heißt $\tilde{\nu}(x) \geq \tilde{\nu}(y)$ und somit $\frac{x}{y} \in R$. Dann gilt $\frac{x+y}{y} = \frac{x}{y} + 1_k \in R$ und somit $\tilde{\nu}(x+y) \geq \tilde{\nu}(y) = \min\{\tilde{\nu}(x), \tilde{\nu}(y)\}$

(ii) $\tilde{\nu}(x * y) = (x * y) * R^* = x * R^* \odot y * R^* = \tilde{\nu}(x) \oplus \tilde{\nu}(y)$

Nach Lemma 3.2.3 ist also die Abbildung

$$\begin{array}{rcll} \nu' : k & \to & G \cup \infty & \\ \frac{a}{b} & \mapsto & \tilde{\nu}(a) \ominus \tilde{\nu}(b) & \forall\ a \in R, b \in R \setminus \{0_R\} \end{array}$$

eine surjektive Bewertung auf k. Man sieht leicht, dass ν' mit der Abbildung ν übereinstimmt, da für $a, b \in R^*$

$$\begin{array}{rcl} \nu(\frac{a}{b}) & = & \left[\frac{a}{b}\right] = \frac{a}{b} * R^* = a * R^* \odot (b^{-1}) * R^* \\ & = & a * R^* \odot (b * R^*)^{-1} = \nu(a) \ominus \nu(b) \quad = \quad \tilde{\nu}(a) \ominus \tilde{\nu}(b) \end{array}$$

gilt und wegen der Bewertungseigenschaft von ν' auch $\nu(0_k) = \infty = \nu'(0_k)$ gilt. □

Bemerkung 3.2.9. *Nach Beispiel 3.2.6 und Beispiel 3.2.8 kann man aus jedem Bewertungsring eine surjektive Bewertung bilden und umgekehrt. Dies ergibt eine Bijektion von surjektiven Bewertungen und Bewertungsringen.*

Definition 3.2.10. Sei $\nu : k \to G_\infty$ eine Bewertung und G so gewählt, dass ν surjektiv ist. Dann heißt die Bewertung ν **diskret**, wenn $(G, +, \geq)$ isomorph zu $(\mathbb{Z}, +_\mathbb{Z}, \geq_\mathbb{Z})$ ist. In diesem Fall heißt $R_\nu = \{x \in k \mid \nu(x) \geq 0_G\}$ ein **diskreter Bewertungsring**.

3.2.2 Eigenschaften

Proposition 3.2.11. *Sei R ein Bewertungsring. Dann ist R ganzabgeschlossen in seinem Quotientenkörper k.*

Beweis. Sei $x \in k^*$ ganz über R. Es ist zu zeigen, dass x in R ist. Da R ein Bewertungsring ist, gilt $x \in R$ oder $x^{-1} \in R$. Für den Fall $x^{-1} \in R$ existieren wegen der Ganzheit von x Elemente $a_0, \ldots, a_{r-1} \in R$, so dass

$$0 = x^r + a_{r-1} * x^{r-1} + a_{r-2} * x^{r-2} + \ldots + a_1 * x + a_0.$$

gilt. Daraus folgt dann

$$x = -(a_{r-1} + a_{r-2} * x^{-1} + \ldots + a_1 * x^{-(r-2)} + a_0 * x^{-(r-1)})$$

und somit wegen $a_0, \ldots, a_{r-1}, x^{-1} \in R$ auch $x \in R$. Damit ist die Behauptung gezeigt. □

Lemma 3.2.12. *Sei k ein Körper, $\nu : k \to G_\infty$ eine Bewertung auf k mit Bewertungsring $R_\nu = \{x \in k \mid \nu(x) \geq 0_G\}$, $x \in k \setminus \{0_k\}$. Dann gilt:*

(i) $\nu(1_k) = 0_G$

(ii) $\nu(x^{-1}) = -\nu(x)$

(iii) *x ist eine Einheit in R_ν genau dann wenn $\nu(x) = 0_G$ gilt*

(iv) *R_ν ist ein lokaler Ring mit maximalem Ideal $\mathfrak{m} = \{x \in K \mid \nu(x) > 0_G\}$*

Beweis. (i) Wegen der Definition der Bewertung gilt

$$\nu(1_k) = \nu(1_k * 1_k) = \nu(1_k) + \nu(1_k)$$

und somit auch

$$0_G = \nu(1_k) - \nu(1_k) = \nu(1_k) + \nu(1_k) - \nu(1_k) = \nu(1_k).$$

(ii) Nach (i) und den Eigenschaften der Bewertung gilt

$$0_G = \nu(1_k) = \nu(x * x^{-1}) = \nu(x) + \nu(x^{-1}).$$

und somit auch $\nu(x^{-1}) = -\nu(x)$.

(iii) Sei zunächst $\nu(x) = 0_G$. Dann gilt nach (ii) die Gleichung

$$\nu(x^{-1}) = -\nu(x) = -0_G = 0_G.$$

Somit sind x, x^{-1} beide in R_ν, also x eine Einheit in R_ν. Umgekehrt sei x eine Einheit in R_ν, das heißt $x, x^{-1} \in R_\nu$. Dann gilt $\nu(x) \geq 0_G$ und $\nu(x^{-1}) \geq 0_G$ und damit nach (ii) auch $0_G \leq \nu(x^{-1}) = -\nu(x) \leq 0_G$. Somit muss $\nu(x)$ gleich 0_G sein.

(iv) Nach (iii) ist $\mathfrak{m} = \{x \in K \mid \nu(x) > 0_G\}$ genau die Menge der Nichteinheiten in R_ν. Es gilt für $a, b \in \mathfrak{m}$, $r \in R_\nu$ (nach den Eigenschaften der Bewertung):

a) $\nu(0_k) = \infty > 0_G$, also $0_k \in \mathfrak{m}$.

b) $\nu(a + b) \geq \min(\nu(a), \nu(b)) > 0_G$, also $(\mathfrak{m}, +)$ abgeschlossen

c) $\nu(r*a) = \nu(r)+\nu(a) \geq 0_G+\nu(a) = \nu(a) > 0_G$, also $\mathfrak{m}$ abgeschlossen bezüglich Skalarmultiplikation von R_ν

Somit ist die Menge der Nichteinheiten $\mathfrak{m}$ ein Ideal in R_ν und deshalb nach Lemma 2.3.13 der Ring R_ν lokal.

□

Definition 3.2.13. Sei $\mathcal{R}$ ein kommutativer Ring mit Einselement. Dann heißt $\pi \in \mathcal{R} \setminus \{0_R\}$ ein **Primelement**, wenn π keine Einheit ist und für alle $a, b \in \mathcal{R}$ aus $\pi \mid a * b$ auch $\pi \mid a$ oder $\pi \mid b$ folgt.

Lemma 3.2.14. *Sei k ein Körper, $\nu : k \to \mathbb{Z}_\infty$ eine (surjektive) diskrete Bewertung auf k mit Bewertungsring $R_\nu = \{x \in k \mid \nu(x) \geq 0_\mathbb{Z}\} = \mathbb{N}_0$. Dann gilt für jedes Element $x \in R_\nu$:*

(i) Es ist $\nu(x) = 1_\mathbb{Z}$ genau dann wenn x ein Primelement in R_ν ist.

(ii) Sei π ein Primelement in R_ν. Dann gilt $x = \pi^{\nu(x)} * y$ für eine Einheit y in R_ν.

Beweis. (i) Sei zunächst $\nu(x) = 1_\mathbb{Z}$. Dann ist x nach Lemma 3.2.12 keine Einheit und nach den Eigenschaften der Bewertung auch $x \neq 0$. Es gelte $x \mid a * b$ für Elemente $a, b \in R_\nu$, also $x * s = a * b$ für ein $s \in R_\nu$. Dann gilt

$$1 + \nu(s) = \nu(x) + \nu(s) = \nu(x * s) = \nu(a * b) = \nu(a) + \nu(b).$$

Sei ohne Beschränkung der Allgemeinheit $\nu(a) \geq \nu(b)$. Dann gilt wegen $\nu(a), \nu(b), \nu(s) \geq 0$ und der obigen Gleichung auch $\nu(a) \geq 1$ und somit $\nu(s) = -1 + \nu(a) + \nu(b) \geq \nu(b)$. Also ist $\nu(\frac{s}{b}) = \nu(s) - \nu(b) \geq 0$ und deshalb auch $\frac{s}{b} \in R_\nu$. Es folgt $x * \frac{s}{b} = a$ und somit wegen $\frac{s}{b} \in R_\nu$ auch $x \mid a$. Also ist x ein Primelement. Sei nun umgekehrt $x \in R_\nu$ ein Primelement. Sei π ein Element mit $\nu(\pi) = 1$. Dieses existiert, da ν surjektiv ist. Da x keine Einheit und nicht 0 ist, gilt $\nu(x) \in \mathbb{N}$. Es ist dann

$$\nu\left(\frac{\pi^{\nu(x)}}{x}\right) = \nu(x) * \nu(\pi) - \nu(x) = 0$$

und somit $\frac{\pi^{\nu(x)}}{x}$ nach Lemma 3.2.12 eine Einheit in R_ν. Also gilt wegen

$$x * \frac{\pi^{\nu(x)}}{x} = \pi * \pi^{\nu(x)-1}$$

und x Primelement auch $x \mid \pi$ oder $x \mid \pi^{\nu(x)-1}$. Durch Induktion folgt $x \mid \pi$. Es gibt also ein $s \in R_\nu$ mit $x * s = \pi$. Damit folgt aber

$$\nu(x) + \nu(s) = \nu(\pi) = 1$$

und wegen $\nu(x) \geq 1$ und $\nu(s) \geq 0$ auch $\nu(x) = 1$.

(ii) Analog zum Beweis von (i) gilt

$$\nu\Big(\frac{x}{\pi^{\nu(x)}}\Big) = \nu(x) - \nu(x) * \nu(\pi) = 0,$$

also ist $y := \frac{x}{\pi^{\nu(x)}}$ nach Lemma 3.2.12 eine Einheit in R_ν und es gilt

$$x = \pi^{\nu(x)} * \frac{x}{\pi^{\nu(x)}} = \pi^{\nu(x)} * y$$

wie behauptet.

□

3.3 Primideale und Idealzerlegung

Im Abschnitt 3.3.1 wird die Basisprimzahl eines Primideals definiert und ein Zusammenhang mit der Diskriminante gezeigt. Außerdem wird bewiesen, dass jedes Primideal maximal ist und es wird die Invertierbarkeit von Primidealen untersucht. Danach wird im Abschnitt 3.3.2 die Bewertung an einem invertierbaren Primideal definiert und gezeigt, dass diese Bewertung diskret ist. Als nächstes wird im Abschnitt 3.3.3 untersucht, welche Zusammenhänge es zwischen der Bewertung an einem Primideal und der Lokalisierung an einem Primideal gibt und es werden weitere Äquivalenzen zur Invertierbarkeit von Primidealen beschrieben. Im Abschnitt 3.3.4 wird nun untersucht, in welchen Fällen man (gebrochene) Ideale einer Ordnung in Primideale zerlegen kann und welcher Zusammenhang zwischen der Zerlegung und der Bewertung an Primidealen besteht. Außerdem wird gezeigt, dass in der Maximalordnung jedes gebrochene Ideal invertierbar ist. Schließlich wird im Abschnitt 3.3.5 der Begriff p-maximal eingeführt und es wird der Zusammenhang zwischen p-Maximalität, Invertierbarkeit und Teilerfremdheit zum Führer untersucht.

3.3.1 Primideale

In diesem Abschnitt wird gezeigt, dass jedes Primideal $\mathfrak{p}$ in einer Ordnung $\mathcal{O}$ eine eindeutig bestimmte Primzahl enthält, die sogenannte Basisprimzahl. Ist ein beliebiges Ideal $\mathfrak{a}$ in $\mathfrak{p}$ enthalten, so muss die Basisprimzahl von $\mathfrak{p}$ die Diskriminante des Ideals $\mathfrak{a}$ mindestens quadratisch teilen. Außerdem wird bewiesen, dass jedes Primideal in $\mathcal{O}$ maximal ist und es wird gezeigt, wie man aus bestimmten Teilmengenrelationen auf die Invertierbarkeit von Primidealen schließen kann.

Lemma 3.3.1. *Sei $k \in \mathbb{N}$ eine natürliche Zahl und n der Grad von $K \mid \mathbb{Q}$. Dann gilt:*

$$(\mathcal{O} : (k)_{\mathcal{O}}) = k^n$$

Beweis. Die Moduln $\mathcal{O}$ und $(k)_{\mathcal{O}}$ sind beide vollständig, haben also nach Proposition 3.1.4 den Rang $n = [K : \mathbb{Q}]$. Sei $b_1, \ldots, b_n$ eine Basis von $\mathcal{O}$. Dann ist $k * b_1, \ldots, k * b_n$ eine Basis von $(k)_{\mathcal{O}}$. Nach Lemma 2.8.17 gilt dann $(\mathcal{O} : (k)_{\mathcal{O}}) = |\det S|$, wobei S die Smith-Normalform der Transformationsmatrix von der Basis $\{k * b_1, \ldots, k * b_n\}$ zur Basis $\{b_1, \ldots, b_n\}$ ist. Man sieht jedoch sofort, dass die Transformationsmatrix einfach das k-fache der Einheitsmatrix ist, da jedes Basiselement von $(k)_{\mathcal{O}}$ genau das k-fache des entsprechenden Basiselements von $\mathcal{O}$ ist. Somit ist die Transformationsmatrix schon in Smith-Normalform (bis auf eine mögliche Multiplikation mit -1, je nach Wahl des Repräsentantensystems). Der Betrag der Determinante ist dann (unabhängig vom Repräsentantensystem) k^n, womit die Behauptung bewiesen ist. □

Proposition 3.3.2. *Sei $\mathfrak{p} \neq (0)_{\mathcal{O}}$ ein Primideal in $\mathcal{O}$. Dann gibt es genau eine Primzahl $p \in \mathbb{Z}$ mit $p \in \mathfrak{p}$ und es gilt $(\mathcal{O} : \mathfrak{p}) = p^k$ für ein geeignetes $k \in \mathbb{N}$ mit $1 \leq k \leq [K : \mathbb{Q}]$.*

Beweis. Man betrachte die Ringinklusion $\iota : \mathbb{Z} \to \mathcal{O}$ und die Kontraktion $\mathfrak{q} := \iota^{-1}(\mathfrak{p}) = \mathfrak{p} \cap \mathbb{Z}$. Dann ist nach Lemma 2.1.5 das Ideal $\mathfrak{q}$ als Kontraktion eines Primideals ein Primideal, also entweder $(0)_{\mathbb{Z}}$ oder $(p)_{\mathbb{Z}}$ für eine Primzahl $p \in \mathbb{Z}$. Da $\mathfrak{p} \neq (0)_{\mathcal{O}}$ ist, gibt es ein $0 \neq a \in \mathfrak{p}$. Sei

$$\mu_a(x) = x^r + a_{r-1} * x^{r-1} + \ldots + a_0 \in \mathbb{Z}[x] \setminus \left\{0_{\mathbb{Z}[x]}\right\}$$

das Minimalpolynom von a über $\mathbb{Z}$. Da a ganz ist und $\mathbb{Z}$ ein Integritätsring ist, gilt $a_0 \neq 0$ nach Lemma 2.4.5. Außerdem ist a eine Nullstelle von μ_a und es folgt:

$$a_0 = -(a^n + a_{n-1} * a^{n-1} + \ldots + a * a_1) \in \mathfrak{p}$$

Damit ist $0 \neq a_0 \in \mathfrak{p} \cap \mathbb{Z} = \mathfrak{q}$, also $\mathfrak{q} \neq (0)_{\mathbb{Z}}$ und somit $\mathfrak{q} = (p)_{\mathbb{Z}}$ für eine Primzahl p. Dann ist aber p die einzige Primzahl in $\mathfrak{p}$, da p die einzige Primzahl in $\mathfrak{p} \cap \mathbb{Z} = \mathfrak{q} = (p)_{\mathbb{Z}}$ ist. Es gilt also wegen $(p)_{\mathcal{O}} \subset \mathfrak{p} \subset \mathcal{O}$ nach dem Multiplikationssatz für Indizes (Proposition 2.2.8) die Gleichung

$$(\mathcal{O} : \mathfrak{p}) * (\mathfrak{p} : (p)_{\mathcal{O}}) = (\mathcal{O} : (p)_{\mathcal{O}}).$$

Außerdem wurde in Lemma 3.3.1 gezeigt, dass $(\mathcal{O} : (p)_{\mathcal{O}}) = p^n$ ist, wobei n der Grad von $K \mid \mathbb{Q}$ ist. Somit gilt

$$(\mathcal{O} : \mathfrak{p}) * (\mathfrak{p} : (p)_{\mathcal{O}}) = (\mathcal{O} : (p)_{\mathcal{O}}) = p^n,$$

und es folgt $(\mathcal{O} : \mathfrak{p}) = p^k$ für ein $0 \leq k \leq n$. Wäre $k = 0$, so wäre $(\mathcal{O} : \mathfrak{p}) = 1$ und somit $\mathcal{O} = \mathfrak{p}$, was ein Widerspruch zu $\mathfrak{p}$ Primideal ist. Es gilt also $(\mathcal{O} : \mathfrak{p}) = p^k$ für ein $1 \leq k \leq n$. □

Definition 3.3.3. Sei $\mathfrak{p}$ ein Primideal und $p \in \mathbb{Z}$ die nach Proposition 3.3.2 einzige Primzahl in $\mathfrak{p}$. Dann nennt man $\mathfrak{p}$ ein **Primideal über** p und p die **Basisprimzahl** von $\mathfrak{p}$.

Lemma 3.3.4. *Sei $\mathfrak{p}$ ein Primideal in $\mathcal{O}$ mit Basisprimzahl p. Dann teilt p die Diskriminante von $\mathfrak{p}$ (mindestens) quadratisch.*

Beweis. Wegen $\mathfrak{p} \subset \mathcal{O}$ und Lemma 3.1.10 [Diskriminanten-Index-Formel] gilt die Gleichung

$$d(\mathfrak{p}) = (\mathcal{O} : \mathfrak{p})^2 * d(\mathcal{O}).$$

Da aber wegen Proposition 3.3.2 für ein $1 \leq k \leq n$ die Gleichung $(\mathcal{O} : \mathfrak{p}) = p^k$ gilt, gilt insbesondere $p \mid (\mathcal{O} : \mathfrak{p})$ und somit

$$p^2 \mid (\mathcal{O} : \mathfrak{p})^2 * d(\mathcal{O}) = d(\mathfrak{p}).$$

□

Korollar 3.3.5. *Sei $\mathfrak{a}$ ein Ideal und $\mathfrak{p}$ ein Primideal mit Basisprimzahl p, das $\mathfrak{a}$ enthält. Dann teilt p die Diskriminante von $\mathfrak{a}$ (mindestens) quadratisch.*

Beweis. Nach Lemma 3.3.4 teilt p die Diskriminante von $\mathfrak{p}$ mindestens quadratisch. Da $\mathfrak{a} \subset \mathfrak{p}$ gilt, teilt nach Lemma 3.1.10 [Diskriminanten-Index-Formel] die Diskriminante von $\mathfrak{p}$ die Diskriminante von $\mathfrak{a}$. Somit teilt p auch die Diskriminante von $\mathfrak{a}$ mindestens quadratisch. □

Bemerkung 3.3.6. *Das Korollar 3.3.5 ist eine Möglichkeit, um die Primideale einzuschränken, die ein gegebenes Ideal enthalten können. Berechnet man die Diskriminante von einem Ideal $\mathfrak{a}$, so muss man nur diejenigen Basisprimzahlen heraussuchen, die in der Primidealzerlegung der Diskriminante einen Exponenten größer oder gleich 2 haben. Nur Primideale über diesen Basisprimzahlen können $\mathfrak{a}$ enthalten. Da Primidealfaktoren einer (eventuell unvollständigen) Faktorisierung eines Ideals $\mathfrak{a}$ immer $\mathfrak{a}$ enthalten müssen, kann man so die möglichen Primidealfaktoren einschränken.*

Proposition 3.3.7. *Sei $\mathfrak{p} \neq (0)_{\mathcal{O}}$ ein Primideal in $\mathcal{O}$. Dann ist $\mathfrak{p}$ maximal.*

Beweis. Wie im Beweis von Proposition 3.3.2 ist $\mathbb{Z} \cap \mathfrak{p} = (p)_{\mathbb{Z}}$ für die Basisprimzahl p von $\mathfrak{p}$. Die Einbettung $\iota : \mathbb{Z} \to \mathcal{O}$ induziert dann einen Ringhomomorphismus

$$\bar{\iota} : \mathbb{Z}/p\mathbb{Z} \to \mathcal{O}/\mathfrak{p}.$$

Der Ring $\mathcal{O}/\mathfrak{p}$ ist dann eine $\mathbb{Z}/p\mathbb{Z}$-Algebra und wegen $\mathfrak{p}$ Primideal auch ein Integritätsring (siehe Proposition 2.2.16). Da die Elemente aus $\mathcal{O}$ ganz über $\mathbb{Z}$ sind, sind auch die Elemente aus $\mathcal{O}/\mathfrak{p}$ ganz über $\mathbb{Z}/p\mathbb{Z}$. Nach Lemma 2.4.6 ist damit $\mathcal{O}/\mathfrak{p}$ ein Körper, also $\mathfrak{p}$ nach Proposition 2.2.16 maximal. □

Proposition 3.3.8. *Sei $\mathfrak{a} \neq (0)_{\mathcal{O}}$ ein ganzzahliges Ideal in $\mathcal{O}$. Dann gibt es ein $k \in \mathbb{N}$ und Primideale $\mathfrak{p}_1, \ldots, \mathfrak{p}_k \neq (0)_{\mathcal{O}}$ mit*

$$\prod_{i=1}^{k} \mathfrak{p}_i \subset \mathfrak{a}.$$

Beweis. Sei $\mathcal{J}$ die Menge der Ideale ungleich $(0)_{\mathcal{O}}$ in $\mathcal{O}$, die kein endliches Produkt aus Primidealen ungleich $(0)_{\mathcal{O}}$ enthalten (also die Ideale, für die die Behauptung nicht gilt). Angenommen $\mathcal{J} \neq \emptyset$. Da im noetherschen Ring $\mathcal{O}$ jede aufsteigende Kette von Idealen stationär wird, wird insbesondere jede aufsteigende Kette von Idealen in $\mathcal{J}$ stationär. Nach dem Lemma von Zorn gibt es also ein maximales Element $\mathfrak{b}$ in $\mathcal{J}$. Das Ideal $\mathfrak{b}$ kann kein Primideal $\mathfrak{p}$ sein, da sonst trivialerweise $\mathfrak{p} \subset \mathfrak{b}$ gelten würde und somit $\mathfrak{b}$ nicht in $\mathcal{J}$ wäre. Da $\mathfrak{b}$ kein Primideal ist, gibt es $b_1, b_2 \in \mathcal{O} \setminus \mathfrak{b}$ mit $b_1 * b_2 \in \mathfrak{b}$. Setzt man nun $\mathfrak{b}_i := \mathfrak{b} + (b_i)_{\mathcal{O}}$, so ergibt sich wegen $b_i \notin \mathfrak{b}$ auch $\mathfrak{b} \subsetneq \mathfrak{b}_i$ und da $\mathfrak{b}$ maximal

in $\mathcal{J}$ gewählt war, sind die $\mathfrak{b}_i$ nicht in $\mathcal{J}$. Es gibt also endliche Produkte Π_1, Π_2 von Primidealen ungleich $(0)_\mathcal{O}$ mit $\Pi_i \subset \mathfrak{b}_i$. Wegen $b_1 * b_2 \in \mathfrak{b}$ gilt dann

$$\begin{aligned} \Pi_1 * \Pi_2 &\subset \mathfrak{b}_1 * \mathfrak{b}_2 = (\mathfrak{b} + (b_1)_\mathcal{O}) * (\mathfrak{b} + (b_2)_\mathcal{O}) \\ &= \mathfrak{b}^2 + \mathfrak{b} * ((b_1)_\mathcal{O} + (b_2)_\mathcal{O}) + (b_1 * b_2)_\mathcal{O} \\ &\subset \mathfrak{b}. \end{aligned}$$

Somit ist $\Pi_1 * \Pi_2$ ein endliches Produkt von Primidealen ungleich $(0)_\mathcal{O}$, das in $\mathfrak{b}$ enthalten ist. Dies ist ein Widerspruch dazu, dass $\mathfrak{b}$ in $\mathcal{J}$ ist. Somit muss die Annahme falsch sein und es gilt $\mathcal{J} = \emptyset$. Damit ist in jedem Ideal $\mathfrak{a} \neq (0)_\mathcal{O}$ ein endliches Produkt von Primidealen ungleich $(0)_\mathcal{O}$ enthalten. □

Lemma 3.3.9. *Sei $\mathfrak{p} \neq (0)_\mathcal{O}$ ein Primideal in $\mathcal{O}$. Dann gilt*

$$\mathcal{O} \subsetneq \tilde{\mathfrak{p}} = \{x \in K \mid x * \mathfrak{p} \subset \mathcal{O}\}.$$

Beweis. Zunächst ist klar, dass $\mathcal{O} \subset \tilde{\mathfrak{p}}$ gilt, da für alle $x \in \mathcal{O}$ die Inklusion $x * \mathfrak{p} \subset \mathfrak{p} \subset \mathcal{O}$ gilt. Es ist also nur noch ein Element in $\tilde{\mathfrak{p}} \setminus \mathcal{O}$ zu finden. Sei dafür $a \in \mathfrak{p} \setminus \{0\}$. Nach Proposition 3.3.8 gibt es dann ein endliches Produkt $\prod_{i=1}^k \mathfrak{p}_i$ von Primidealen ungleich $(0)_\mathcal{O}$, so dass $\prod_{i=1}^k \mathfrak{p}_i \subset (a)_\mathcal{O}$ gilt. Sei ohne Beschränkung der Allgemeinheit das Produkt so gewählt, dass k minimal ist. Dann gilt

$$\prod_{i=1}^k \mathfrak{p}_i \subset (a)_\mathcal{O} \subset \mathfrak{p}.$$

Wegen der Primidealeigenschaft von $\mathfrak{p}$ muss dann für ein $i_0 \in \{1, \ldots, k\}$ das Primideal $\mathfrak{p}_{i_0}$ in $\mathfrak{p}$ enthalten sein. Da $\mathfrak{p}_{i_0}$ aber nach Proposition 3.3.7 maximal ist, gilt sogar $\mathfrak{p}_{i_0} = \mathfrak{p}$. Das Produkt wurde aber mit minimalem k gewählt, also ist $\prod_{i \neq i_0} \mathfrak{p}_i$ nicht in $(a)_\mathcal{O}$ enthalten. Sei nun $b \in (\prod_{i \neq i_0} \mathfrak{p}_i) \setminus (a)_\mathcal{O}$. Dann gilt wegen $\mathfrak{p} = \mathfrak{p}_{i_0}$

$$b * \mathfrak{p} \subset \prod_{i \neq i_0} \mathfrak{p}_i * \mathfrak{p} = \prod_{i=1}^k \mathfrak{p}_i \subset (a)_\mathcal{O}$$

Somit ist $a^{-1} * b * \mathfrak{p} \subset \mathcal{O}$, also $a^{-1} * b \in \tilde{\mathfrak{p}}$. Nach der Wahl von b gilt aber $a^{-1} * b \notin \mathcal{O}$. Somit wurde ein Element in $\tilde{\mathfrak{p}} \setminus \mathcal{O}$ gefunden und die Behauptung gezeigt. □

Lemma 3.3.10. *Sei $\mathfrak{p} \neq (0)_\mathcal{O}$ ein Primideal in $\mathcal{O}$. Dann ist $\mathfrak{p}$ genau dann invertierbar in $\mathcal{O}$, wenn Ord$(\mathfrak{p}) = \mathcal{O}$ gilt.*

Beweis. Sei zunächst $\mathrm{Ord}(\mathfrak{p}) = \mathcal{O}$. Da $\mathfrak{p}$ nach Proposition 3.3.7 maximal ist und $\mathfrak{p} * \tilde{\mathfrak{p}}$ ein ganzzahliges Ideal in $\mathcal{O}$ ist, gilt entweder $\mathfrak{p} = \mathfrak{p} * \tilde{\mathfrak{p}}$ oder $\mathfrak{p} * \tilde{\mathfrak{p}} = \mathcal{O}$. Im zweiten Fall ist $\mathfrak{p}$ invertierbar. Es ist somit nur der erste Fall zum Widerspruch zu führen. Angenommen es gilt $\mathfrak{p} = \mathfrak{p} * \tilde{\mathfrak{p}}$. Dann ist insbesondere $\tilde{\mathfrak{p}} * \mathfrak{p} \subset \mathfrak{p}$ und damit $\tilde{\mathfrak{p}} \subset \mathrm{Ord}(\mathfrak{p})$. Nach Voraussetzung ist aber $\mathrm{Ord}(\mathfrak{p}) = \mathcal{O}$ und somit $\tilde{\mathfrak{p}} \subset \mathrm{Ord}(\mathfrak{p}) = \mathcal{O}$. Dies ist ein Widerspruch zu Lemma 3.3.9, also muss $\mathfrak{p} * \tilde{\mathfrak{p}} = \mathcal{O}$ gelten und $\mathfrak{p}$ ist invertierbar.

Sei umgekehrt $\mathfrak{p}$ invertierbar. Wegen $\mathcal{O} * \mathfrak{p} \subset \mathfrak{p}$ gilt $\mathcal{O} \subset \mathrm{Ord}(\mathfrak{p})$. Sei nun $x \in \mathrm{Ord}(\mathfrak{p})$. Dann gilt $x * \mathfrak{p} \subset \mathfrak{p}$ und somit

$$x * \mathcal{O} = x * (1)_{\mathcal{O}} = x * \mathfrak{p} * \mathfrak{p}^{-1} \subset \mathfrak{p} * \mathfrak{p}^{-1} = (1)_{\mathcal{O}} = \mathcal{O}.$$

Insbesondere gilt also $x = x * 1 \in \mathcal{O}$. Damit ist auch $\mathrm{Ord}(\mathfrak{p}) \subset \mathcal{O}$ gezeigt und es folgt die Behauptung.

□

Proposition 3.3.11. *Sei $\mathfrak{p}$ ein Primideal in $\mathcal{O}$. Dann gelten die folgenden Teilmengenrelationen:*

$$\mathfrak{p} \subset \mathfrak{p} * \tilde{\mathfrak{p}} \subset \mathcal{O} \subset \mathit{Ord}(\mathfrak{p}) \subset \tilde{\mathfrak{p}} \tag{3.1}$$

$\mathfrak{p}$ ist genau dann invertierbar, wenn die folgenden Relationen gelten:

$$\mathfrak{p} \subsetneq \mathfrak{p} * \tilde{\mathfrak{p}} = \mathcal{O} = \mathit{Ord}(\mathfrak{p}) \tag{3.2}$$

$\mathfrak{p}$ ist genau dann nicht invertierbar, wenn die folgenden Relationen gelten:

$$\mathfrak{p} = \mathfrak{p} * \tilde{\mathfrak{p}} \subsetneq \mathcal{O} \subsetneq \mathit{Ord}(\mathfrak{p}) \tag{3.3}$$

Beweis. Zunächst werden die Relationen in (3.1) gezeigt:

$\mathfrak{p} \subset \mathfrak{p} * \tilde{\mathfrak{p}}$:	Da $\tilde{\mathfrak{p}}$ als $\{x \in K \mid x * \mathfrak{p} \subset \mathcal{O}\}$ definiert ist, gilt trivialerweise $1_K \in \tilde{\mathfrak{p}}$, da $1 * \mathfrak{p} = \mathfrak{p} \subset \mathcal{O}$ gilt. Somit ist $\mathfrak{p} = \mathfrak{p} * 1_K \subset \mathfrak{p} * \tilde{\mathfrak{p}}$.
$\mathfrak{p} * \tilde{\mathfrak{p}} \subset \mathcal{O}$:	Nach der Definition von $\tilde{\mathfrak{p}}$ gilt für alle $x \in \tilde{\mathfrak{p}}$ die Relation $x * \mathfrak{p} \subset \mathcal{O}$ und somit auch $\tilde{\mathfrak{p}} * \mathfrak{p} \subset \mathcal{O}$.
$\mathcal{O} \subset \mathrm{Ord}(\mathfrak{p})$:	$\mathrm{Ord}(\mathfrak{p})$ ist definiert als $\{x \in K \mid x * \mathfrak{p} \subset \mathfrak{p}\}$. Da $\mathfrak{p}$ ein Ideal in $\mathcal{O}$ ist, gilt aber $\mathcal{O} * \mathfrak{p} \subset \mathfrak{p}$ und somit auch $\mathcal{O} \subset \mathrm{Ord}(\mathfrak{p})$.
$\mathrm{Ord}(\mathfrak{p}) \subset \tilde{\mathfrak{p}}$:	Für $x \in \mathrm{Ord}(\mathfrak{p})$ gilt nach Definition $x * \mathfrak{p} \subset \mathfrak{p}$ und da $\mathfrak{p}$ ein ganzzahliges Ideal in $\mathcal{O}$ ist, folgt $x * \mathfrak{p} \subset \mathcal{O}$. Also gilt $x \in \tilde{\mathfrak{p}}$ und da $x \in \mathrm{Ord}(\mathfrak{p})$ beliebig gewählt war, gilt $\mathrm{Ord}(\mathfrak{p}) \subset \tilde{\mathfrak{p}}$.

Gilt (3.2) oder (3.3), so folgt aus $\mathfrak{p} * \tilde{\mathfrak{p}} = \mathcal{O}$ beziehungsweise $\mathfrak{p} * \tilde{\mathfrak{p}} \subsetneq \mathcal{O}$ sofort die Invertierbarkeit beziehungsweise Nichtinvertierbarkeit von $\mathfrak{p}$. Es sind also nur noch die umgekehrten Richtungen zu beweisen.

Sei dafür zunächst $\mathfrak{p}$ invertierbar. Dann gilt nach Proposition 3.1.30 die Gleichung $\mathfrak{p} * \tilde{\mathfrak{p}} = \mathcal{O}$ und nach Lemma 3.3.10 die Gleichung $\mathcal{O} = \mathrm{Ord}(\mathfrak{p})$. Wegen $\mathfrak{p}$ Primideal gilt dann auch $\mathfrak{p} \neq \mathcal{O} = \mathfrak{p} * \tilde{\mathfrak{p}}$.

Sei nun $\mathfrak{p}$ nicht invertierbar. Dann gilt nach Proposition 3.1.30 die Ungleichung $\mathfrak{p} * \tilde{\mathfrak{p}} \neq \mathcal{O}$ und nach Lemma 3.3.10 die Ungleichung $\mathcal{O} \neq \mathrm{Ord}(\mathfrak{p})$. Da $\mathfrak{p}$ nach Proposition 3.3.7 maximal ist und $\mathfrak{p} * \tilde{\mathfrak{p}}$ ein ganzzahliges Ideal in $\mathcal{O}$ ist, muss also $\mathfrak{p} = \mathfrak{p} * \tilde{\mathfrak{p}}$ gelten.

□

Bemerkung 3.3.12. *Um die Invertierbarkeit von $\mathfrak{p}$ zu überprüfen, reicht es bei einer der folgenden Relationen zu überprüfen, ob die Relation echt ist oder eine Gleichung ist:*

$$\begin{aligned} \mathfrak{p} &\subset \mathfrak{p} * \tilde{\mathfrak{p}} \\ \mathfrak{p} * \tilde{\mathfrak{p}} &\subset \mathcal{O} \\ \mathcal{O} &\subset Ord(p) \end{aligned}$$

Beweis. Da $\mathfrak{p}$ entweder invertierbar oder nicht invertierbar ist, gilt nach Proposition 3.3.11 genau eine der folgenden Relationsketten:

$$\mathfrak{p} \subsetneq \mathfrak{p} * \tilde{\mathfrak{p}} = \mathcal{O} = \mathrm{Ord}(\mathfrak{p})$$
$$\mathfrak{p} = \mathfrak{p} * \tilde{\mathfrak{p}} \subsetneq \mathcal{O} \subsetneq \mathrm{Ord}(\mathfrak{p})$$

Prüft man eine der drei Relationen in der Behauptung auf Gleichheit oder Echtheit, so ist dadurch klar, welche der Relationsketten gilt und somit nach Proposition 3.3.11 auch, ob $\mathfrak{p}$ invertierbar ist. □

3.3.2 Bewertung an Primidealen

In diesem Abschnitt wird gezeigt, dass man jedes Ideal $\mathfrak{a}$ eindeutig in eine Potenz eines invertierbaren Primideals $\mathfrak{p}$ und einen Rest $\mathfrak{b}$ zerlegen kann, so dass $\mathfrak{b}$ nicht in $\mathfrak{p}$ enthalten ist. Man nennt den entsprechenden Exponenten den Wert von $\mathfrak{a}$ an $\mathfrak{p}$. Dadurch kann man jedem Element in K den Wert des von ihm erzeugten Hauptideals zuordnen (bezüglich eines invertierbaren Primideals) und erhält eine diskrete Bewertung. Der Wert eines Ideals gibt den Exponenten eines invertierbaren Primideals in seiner (eventuell unvollständigen) Primidealzerlegung an. Dies wird in Abschnitt 3.3.4 noch genauer erläutert. Im Folgenden sei $\mathfrak{P}^*_{\mathcal{O}}$ die Menge der invertierbaren Primideale in $\mathcal{O}$.

Proposition 3.3.13. *Für jedes Ideal $\mathfrak{a} \neq (0)$ in $\mathcal{O}$ und jedes invertierbare Primideal $\mathfrak{p}$ in $\mathcal{O}$ gibt es ein Ideal $\mathfrak{b} \not\subset \mathfrak{p}$ und ein $\nu_{\mathfrak{p}}(\mathfrak{a}) \in \mathbb{N}_0$ mit*

$$\mathfrak{a} = \mathfrak{p}^{\nu_{\mathfrak{p}}(\mathfrak{a})} * \mathfrak{b} \tag{3.4}$$

$\mathfrak{b}$ und $\nu_{\mathfrak{p}}(\mathfrak{a})$ sind dabei eindeutig.

Beweis. 1. Eindeutigkeit: Seien $k_1, k_2 \in \mathbb{N}_0$ und $\mathfrak{b}_1, \mathfrak{b}_2 \not\subset \mathfrak{p}$ Ideale mit:

$$\mathfrak{p}^{k_1} * \mathfrak{b}_1 = \mathfrak{a} = \mathfrak{p}^{k_2} * \mathfrak{b}_2$$

Ohne Beschränkung der Allgemeinheit sei $k_1 \leq k_2$. Da $\mathfrak{p}$ invertierbar ist, kann man die Gleichung mit $\mathfrak{p}^{-k_1}$ multiplizieren und man bekommt

$$\mathfrak{b}_1 = \mathfrak{p}^{k_2-k_1} * \mathfrak{b}_2.$$

Angenommen $k_0 := k_2 - k_1 > 0$, dann gilt $\mathfrak{b}_1 = \mathfrak{p}^{k_0} * \mathfrak{b}_2 \subset \mathfrak{p}^{k_0} \subset \mathfrak{p}$. Dies ist ein Widerspruch zu $\mathfrak{b}_1 \not\subset \mathfrak{p}$. Es ist also $k_1 = k_2$ und es folgt sofort $\mathfrak{b}_1 = \mathfrak{p}^{k_2-k_1} * \mathfrak{b}_2 = \mathfrak{b}_2$.

2. Existenz: Angenommen es gibt Ideale ungleich $(0)_{\mathcal{O}}$, die sich nicht wie in (3.4) darstellen lassen. Sei $\mathfrak{M}$ die Menge dieser Ideale. $\mathfrak{M}$ ist durch die Inklusion halbgeordnet. Jede aufsteigende Kette von Elementen in $\mathfrak{M}$ hat eine obere Schranke, da sie als aufsteigende Kette von Idealen in einem noetherschen Ring $\mathcal{O}$ sogar ein maximales Element hat. Nach dem Lemma von Zorn gibt es also mindestens ein maximales $\mathfrak{a} \in \mathfrak{M}$, das heißt für alle $\mathfrak{c} \in \mathfrak{M}$ mit $\mathfrak{a} \subset \mathfrak{c}$ gilt sogar $\mathfrak{c} = \mathfrak{a}$. Man wähle nun ein maximales $\mathfrak{a} \in \mathfrak{M}$. Wäre $\mathfrak{a} \not\subset \mathfrak{p}$, so hätte man sofort eine Darstellung von $\mathfrak{a}$ wie in (3.4) mit $\mathfrak{b} = \mathfrak{a}$ und $\nu_{\mathfrak{p}}(\mathfrak{a}) = 0$. Dies wäre ein Widerspruch zu $\mathfrak{a} \in \mathfrak{M}$. Es gilt also $\mathfrak{a} \subset \mathfrak{p}$. Außerdem ist $\mathfrak{p}$ invertierbar, also ist auch $\mathfrak{c} := \mathfrak{p}^{-1} * \mathfrak{a} \subset \mathfrak{p}^{-1} * \mathfrak{p} = \mathcal{O}$ ein ganzzahliges Ideal. Angenommen $\mathfrak{c}$ wäre gleich $\mathfrak{a}$. Dann wäre

$$\mathfrak{a} = \mathfrak{p} * \mathfrak{p}^{-1} * \mathfrak{a} = \mathfrak{p} * \mathfrak{c} = \mathfrak{p} * \mathfrak{a}.$$

Betrachtet man nun diese Gleichung in der Lokalisierung an $\mathfrak{p}$, so ergibt sich nach Lemma 2.3.14 die Gleichung $\mathfrak{a}_{\mathfrak{p}} = \mathfrak{p}_{\mathfrak{p}} * \mathfrak{a}_{\mathfrak{p}}$. Da $\mathfrak{a}_{\mathfrak{p}}$ ein $\mathcal{O}_{\mathfrak{p}}$-Modul ist und $\mathfrak{p}_{\mathfrak{p}}$ als einziges maximales Ideal in $\mathcal{O}_{\mathfrak{p}}$ gleich dem Jacobson-Radikal ist, gilt nach Lemma 2.8.22 [Nakayama's Lemma] die Gleichung $\mathfrak{a}_{\mathfrak{p}} = (0)_{\mathcal{O}_{\mathfrak{p}}}$. Da $\mathcal{O}$ nullteilerfrei ist, ist nach Lemma 2.3.14 die Einbettung $\iota : \mathcal{O} \to \mathcal{O}_{\mathfrak{p}}$ injektiv. Es folgt also $\mathfrak{a} = (0)_{\mathcal{O}}$. Dies ist ein Widerspruch, da die Elemente von $\mathfrak{M}$ als ungleich $(0)_{\mathcal{O}}$ angenommen wurden. Das Ideal $\mathfrak{c}$ muss also echt größer sein als $\mathfrak{a}$ und ist somit wegen der Maximalität von $\mathfrak{a}$ und wegen $\mathfrak{a} \subsetneq \mathfrak{c}$ nicht in $\mathfrak{M}$. Also gibt es eine Darstellung $\mathfrak{c} = \mathfrak{p}^k * \mathfrak{b}$ mit Voraussetzungen wie in (3.4). Daraus ergibt sich sofort für $\mathfrak{a}$ die Darstellung

$$\mathfrak{a} = \mathfrak{p} * \mathfrak{p}^{-1} * \mathfrak{a} = \mathfrak{p} * \mathfrak{c} = \mathfrak{p} * \mathfrak{p}^k * \mathfrak{b} = \mathfrak{p}^{k+1} * \mathfrak{b}$$

Dies ist aber ein Widerspruch zu $\mathfrak{a} \in \mathfrak{M}$, also war die ursprüngliche Annahme falsch, dass $\mathfrak{M}$ nichtleer ist. Somit lässt sich jedes Ideal in der Form (3.4) darstellen.

□

Definition 3.3.14. Durch Proposition 3.3.13 wird eine Abbildung $\nu_{\mathfrak{p}}$ definiert, die jedem Ideal $\mathfrak{a} \neq (0)_{\mathcal{O}}$ eine Zahl $\nu_{\mathfrak{p}}(\mathfrak{a}) \in \mathbb{N}_0$ zuordnet (falls $\mathfrak{p}$ ein invertierbares Primideal ist). Außerdem definiert man $\nu_{\mathfrak{p}}((0)_{\mathcal{O}}) := \infty$. Die Zahl $\nu_{\mathfrak{p}}(\mathfrak{a})$ wird im Folgenden der **Wert** des Ideals $\mathfrak{a}$ an $\mathfrak{p}$ genannt.

Proposition 3.3.15. *Die Abbildung $\nu_{\mathfrak{p}}$ erfüllt für alle Ideale $\mathfrak{a}, \mathfrak{b}$ in $\mathcal{O}$ und alle invertierbaren Primideale $\mathfrak{p}, \mathfrak{q} \in \mathfrak{P}^*_{\mathcal{O}}$ mit $\mathfrak{p} \neq \mathfrak{q}$ folgende Eigenschaften:*

a) $\nu_{\mathfrak{p}}(\mathfrak{a}) = \infty \Leftrightarrow \mathfrak{a} = (0)_{\mathcal{O}}$

b) $\mathfrak{a} \subset \mathfrak{b} \Rightarrow \nu_{\mathfrak{p}}(\mathfrak{a}) \geq \nu_{\mathfrak{p}}(\mathfrak{b})$

c) $\nu_{\mathfrak{p}}(\mathfrak{a} + \mathfrak{b}) \geq \min\{\nu_{\mathfrak{p}}(\mathfrak{a}), \nu_{\mathfrak{p}}(\mathfrak{b})\}$

d) $\nu_\mathfrak{p}(\mathfrak{a} * \mathfrak{b}) = \nu_\mathfrak{p}(\mathfrak{a}) + \nu_\mathfrak{p}(\mathfrak{b})$

e) $\nu_\mathfrak{p}(\mathfrak{q}) = 0$

f) $\nu_\mathfrak{p}(\mathfrak{a} * \mathfrak{q}^n) = \nu_\mathfrak{p}(\mathfrak{a}) \qquad \forall\ n \in \mathbb{N}_0$

Dabei sei $\infty + m := \infty =: m + \infty$ *und* $\infty \geq m$ *für alle* $m \in \mathbb{N}_0 \cup \{\infty\}$

Beweis. Nach Proposition 3.3.13 gibt es eindeutig bestimmte Ideale $\mathfrak{a}', \mathfrak{b}'$ mit

$$\begin{aligned} \mathfrak{a} &= \mathfrak{p}^{\nu_\mathfrak{p}(\mathfrak{a})} * \mathfrak{a}' \\ \mathfrak{b} &= \mathfrak{p}^{\nu_\mathfrak{p}(\mathfrak{b})} * \mathfrak{b}' \\ \mathfrak{a}', \mathfrak{b}' &\not\subset \mathfrak{p} \end{aligned}$$

a) Diese Aussage ist klar, da die Idealzerlegung für alle Ideale außer das Nullideal einen Wert in $\mathbb{N}_0$ liefert und für das Nullideal der Wert auf ∞ gesetzt wurde.

b) Es gilt nach Voraussetzung

$$\mathfrak{p}^{\nu_\mathfrak{p}(\mathfrak{a})} * \mathfrak{a}' = \mathfrak{a} \subset \mathfrak{b} = \mathfrak{p}^{\nu_\mathfrak{p}(\mathfrak{b})} * \mathfrak{b}'.$$

Wäre nun $\nu_\mathfrak{p}(\mathfrak{a}) < \nu_\mathfrak{p}(\mathfrak{b})$, so wäre $\nu_\mathfrak{p}(\mathfrak{b}) - \nu_\mathfrak{p}(\mathfrak{a}) > 0$ und damit wegen der Invertierbarkeit von $\mathfrak{p}$

$$\mathfrak{a}' \subset \mathfrak{p}^{\nu_\mathfrak{p}(\mathfrak{b}) - \nu_\mathfrak{p}(\mathfrak{a})} * \mathfrak{b}' \subset \mathfrak{p}.$$

Dies ist aber ein Widerspruch, da $\mathfrak{a}'$ so definiert war, dass $\mathfrak{a}' \not\subset \mathfrak{p}$ gilt.

c) Man kann ohne Beschränkung der Allgemeinheit annehmen, dass $\mathfrak{b}$ den kleineren Wert hat, das heißt, dass $\min\{\nu_\mathfrak{p}(\mathfrak{a}), \nu_\mathfrak{p}(\mathfrak{b})\} = \nu_\mathfrak{p}(\mathfrak{b})$ gilt (ansonsten vertausche $\mathfrak{a}$ und $\mathfrak{b}$). Dann folgt:

$$\mathfrak{a} + \mathfrak{b} = \mathfrak{p}^{\nu_\mathfrak{p}(\mathfrak{a})} * \mathfrak{a}' + \mathfrak{p}^{\nu_\mathfrak{p}(\mathfrak{b})} * \mathfrak{b}' = \mathfrak{p}^{\nu_\mathfrak{p}(\mathfrak{b})} * (\mathfrak{p}^{\nu_\mathfrak{p}(\mathfrak{a}) - \nu_\mathfrak{p}(\mathfrak{b})} * \mathfrak{a}' + \mathfrak{b}') \subset \mathfrak{p}^{\nu_\mathfrak{p}(\mathfrak{b})}$$

Somit gilt nach b) die Ungleichung

$$\nu_\mathfrak{p}(\mathfrak{a} + \mathfrak{b}) \geq \nu_\mathfrak{p}\left(\mathfrak{p}^{\nu_\mathfrak{p}(\mathfrak{b})}\right) = \nu_\mathfrak{p}(\mathfrak{b}) = \min\{\nu_\mathfrak{p}(\mathfrak{a}), \nu_\mathfrak{p}(\mathfrak{b})\}.$$

d) Da $\mathfrak{p}$ ein Primideal ist, gilt:

$$\mathfrak{a}', \mathfrak{b}' \not\subset \mathfrak{p} \quad \Rightarrow \quad \mathfrak{c} := \mathfrak{a}' * \mathfrak{b}' \not\subset \mathfrak{p}$$

Somit ist die eindeutige Zerlegung nach Proposition 3.3.13 gegeben durch

$$\mathfrak{a} * \mathfrak{b} = \mathfrak{p}^{\nu_\mathfrak{p}(\mathfrak{a})} * \mathfrak{a}' * \mathfrak{p}^{\nu_\mathfrak{p}(\mathfrak{b})} * \mathfrak{b}' = \mathfrak{p}^{\nu_\mathfrak{p}(\mathfrak{a}) + \nu_\mathfrak{p}(\mathfrak{b})} * \mathfrak{c}$$

also ist $\nu_\mathfrak{p}(\mathfrak{a} * \mathfrak{b}) = \nu_\mathfrak{p}(\mathfrak{a}) + \nu_\mathfrak{p}(\mathfrak{b})$.

e) Da $\mathfrak{q}$ ein von $\mathfrak{p}$ verschiedenes Primideal ist und nach Proposition 3.3.7 jedes Primideal in $\mathcal{O}$ maximal ist, gilt $\mathfrak{p} \not\subset \mathfrak{q}$. Somit ist $\mathfrak{q} = \mathfrak{p}^0 * \mathfrak{q}$ die eindeutige Zerlegung nach Proposition 3.3.13, also $\nu_\mathfrak{p}(\mathfrak{q}) = 0$.

f) Wegen d) und e) gilt:

$$\nu_\mathfrak{p}(\mathfrak{a} * \mathfrak{q}^n) = \nu_\mathfrak{p}(\mathfrak{a}) + n * \nu_\mathfrak{p}(\mathfrak{q}) = \nu_\mathfrak{p}(\mathfrak{a})$$

□

Proposition 3.3.16. *Sei $\mathfrak{p}$ ein invertierbares Primideal. Die Abbildung*

$$\begin{aligned} \bar{\nu}_\mathfrak{p} : K &\to \mathbb{Z} \cup \{\infty\} \\ \frac{a}{b} &\mapsto \nu_\mathfrak{p}((a)_\mathcal{O}) - \nu_\mathfrak{p}((b)_\mathcal{O}) \end{aligned}$$

*mit $a \in \mathcal{O}$ und $b \in \mathcal{O} \setminus \{0\}$ ist eine (surjektive) diskrete Bewertung auf K. Im Folgenden wird $\bar{\nu}_\mathfrak{p}$ deshalb als die $\mathfrak{p}$-**Bewertung** auf K bezeichnet und $\bar{\nu}_\mathfrak{p}(a)$ als der **Wert** von $a \in K$ an $\mathfrak{p}$. Zur Vereinfachung der Notation wird die Abbildung $\bar{\nu}_\mathfrak{p}$ ab hier ebenfalls mit $\nu_\mathfrak{p}$ bezeichnet. Außerdem wird die Funktion $\nu_\mathfrak{p}$ auf den Idealen im Folgenden ebenfalls als $\mathfrak{p}$-**Bewertung** bezeichnet, da sie ähnliche Eigenschaften wie eine Bewertung erfüllt.*

Beweis. Die Abbildung

$$\bar{\nu}_\mathfrak{p} \restriction_{\mathcal{O}\setminus\{0\}} : \mathcal{O} \setminus \{0\} \to \mathbb{N}_0$$

ist eine Abbildung in die positive Menge $\mathbb{N}_0$ der total geordneten abelschen Gruppe $\mathbb{Z}$. Außerdem gilt für $\tilde{\nu} := \bar{\nu}_\mathfrak{p} \restriction_\mathcal{O}$ auch $\tilde{\nu}(0_R) = \infty$. Da für alle $a, b \in \mathcal{O} \setminus \{0\}$ die Teilmengenrelation $(a+b)_\mathcal{O} \subset (a)_\mathcal{O} + (b)_\mathcal{O}$ gilt, folgen nach Proposition 3.3.15 die Eigenschaften

$$\begin{aligned} i) \quad \tilde{\nu}(a+b) &= \nu_\mathfrak{p}((a+b)_\mathcal{O}) \\ &\geq \nu_\mathfrak{p}((a)_\mathcal{O} + (b)_\mathcal{O}) \\ &\geq \min\{\nu_\mathfrak{p}((a)_\mathcal{O}), \nu_\mathfrak{p}((b)_\mathcal{O})\} \\ &= \min\{\tilde{\nu}(a), \tilde{\nu}(b)\} \\ ii) \quad \tilde{\nu}(a*b) &= \nu_\mathfrak{p}((a*b)_\mathcal{O}) \\ &= \nu_\mathfrak{p}((a)_\mathcal{O} * (b)_\mathcal{O}) \\ &= \nu_\mathfrak{p}((a)_\mathcal{O}) + \nu_\mathfrak{p}((b)_\mathcal{O}) \\ &= \tilde{\nu}(a) + \tilde{\nu}(b) \end{aligned}$$

Nach Lemma 3.2.3 ist also $\bar{\nu}_\mathfrak{p}$ eine Bewertung. Da das Bild von $\bar{\nu}_\mathfrak{p}$ gleich $\mathbb{Z}_\infty$ ist, ist die Bewertung diskret und surjektiv. □

3.3.3 Zusammenhang mit Lokalisierung $\mathcal{O}_\mathfrak{p}$

In diesem Abschnitt wird gezeigt, dass für invertierbare Primideale $\mathfrak{p}$ der Bewertungsring der Bewertung an $\mathfrak{p}$ genau der Lokalisierung an $\mathfrak{p}$ entspricht. Außerdem werden weitere Äquivalenzen zu $\mathfrak{p}$ invertierbar gezeigt, die mit der Lokalisierung zusammenhängen.

Lemma 3.3.17. *Sei $\mathfrak{p} \neq (0)_\mathcal{O}$ ein Primideal in $\mathcal{O}$. Dann gilt:*

(i) Für jedes Primideal $\mathfrak{q}$ in $\mathcal{O}$ mit $(0)_\mathcal{O} \neq \mathfrak{q} \neq \mathfrak{p}$ gilt $\mathcal{O}_\mathfrak{p}\mathfrak{q} = \mathcal{O}_\mathfrak{p}$.

(ii) Das Ideal $\mathfrak{p}_\mathfrak{p} = \mathcal{O}_\mathfrak{p}\mathfrak{p}$ ist das einzige Primideal ungleich $(0)_{\mathcal{O}_\mathfrak{p}}$ in $\mathcal{O}_\mathfrak{p}$.

Beweis. (i) Da nach Proposition 3.3.7 jedes Primideal ungleich $(0)_\mathcal{O}$ in $\mathcal{O}$ maximal ist, gilt für jedes Primideal $\mathfrak{q} \neq \mathfrak{p}$ auch $\mathfrak{q} \not\subset \mathfrak{p}$. Wie im Abschnitt über Lokalisierung (vergleiche Lemma 2.3.14) betrachtet man dann ein Element $x \in \mathfrak{q} \setminus \mathfrak{p}$ und es folgt $1_{\mathcal{O}_\mathfrak{p}} = \frac{x}{x} \in \mathcal{O}_\mathfrak{p}\mathfrak{q}$ und damit $\mathcal{O}_\mathfrak{p}\mathfrak{q} = \mathcal{O}_\mathfrak{p}$.

(ii) Nach Proposition 2.3.11 gibt es eine Bijektion zwischen Primidealen in $\mathcal{O}_\mathfrak{p}$ und Primidealen $\mathfrak{q}$ in $\mathcal{O}$ mit $\mathfrak{q} \subset \mathfrak{p}$. Da letztere Menge wegen der Maximalität von Primidealen in $\mathcal{O}$ (außer dem Nullideal) nur ein Element enthält, gibt es auch in der ersten Menge (außer dem Nullideal) nur ein Element. Da nach Lemma 2.3.14 das Ideal $\mathfrak{p}_\mathfrak{p}$ ein maximales Ideal ist, sind somit $\mathfrak{p}_\mathfrak{p}$ und $(0)_{\mathcal{O}_\mathfrak{p}}$ die einzigen Primideale in $\mathcal{O}_\mathfrak{p}$.

□

Lemma 3.3.18. *Sei $\mathfrak{p}$ ein invertierbares Primideal in $\mathcal{O}$, $\mathfrak{m} := \mathfrak{p}_\mathfrak{p}$ das maximale Ideal in $\mathcal{O}_\mathfrak{p}$, $\mathfrak{a} \neq (0)_\mathcal{O}$ ein Ideal in $\mathcal{O}$. Dann gilt $\mathfrak{a}_\mathfrak{p} = \mathfrak{m}^{\nu_\mathfrak{p}(\mathfrak{a})}$.*

Beweis. Man beachte zunächst, dass $\mathcal{O}_\mathfrak{p}$ nach Lemma 2.3.14 ein lokaler Ring ist und somit das Ideal $\mathfrak{m}$ eindeutig ist. Nach Proposition 3.3.13 gibt es ein Ideal $\mathfrak{a}' \not\subset \mathfrak{p}$ mit $\mathfrak{a} = \mathfrak{p}^{\nu_\mathfrak{p}(\mathfrak{a})} * \mathfrak{a}'$. Daraus folgt wegen Proposition 2.3.11, dass $\mathfrak{a}_\mathfrak{p} = \mathfrak{m}^{\nu_\mathfrak{p}(\mathfrak{a})} * \mathfrak{a}'_\mathfrak{p}$ gilt. Wegen $\mathfrak{a}' \not\subset \mathfrak{p}$ folgt nach Lemma 2.3.14, dass $\mathfrak{a}'_\mathfrak{p} = (1)_{\mathcal{O}_\mathfrak{p}}$ gilt und somit die Behauptung. □

Lemma 3.3.19. *Sei $\mathfrak{p}$ ein invertierbares Primideal in $\mathcal{O}$, $\nu_\mathfrak{p}$ die $\mathfrak{p}$-Bewertung und $\mathcal{O}_{\nu_\mathfrak{p}}$ der dazugehörige Bewertungsring. Dann gilt $\mathcal{O}_\mathfrak{p} = \mathcal{O}_{\nu_\mathfrak{p}}$ (wenn man beide als Teilmengen von K betrachtet).*

Beweis. Sei zunächst $x \in \mathcal{O}_\mathfrak{p}$. Dann gibt es $a \in \mathcal{O}$ und $b \in \mathcal{O} \setminus \mathfrak{p}$ mit $x = \frac{a}{b}$. Somit ist $\mathfrak{a} := (a)_\mathcal{O}$ ein ganzzahliges Ideal und $\mathfrak{b} := (b)_\mathcal{O}$ ein ganzzahliges Ideal mit $\mathfrak{b} \not\subset \mathfrak{p}$. Also gilt $\nu_\mathfrak{p}(\mathfrak{a}) \geq 0$ und $\nu_\mathfrak{p}(\mathfrak{b}) = 0$. Daraus folgt

$$\nu_\mathfrak{p}(x) = \nu_\mathfrak{p}(\mathfrak{a}) - \nu_\mathfrak{p}(\mathfrak{b}) = \nu_\mathfrak{p}(\mathfrak{a}) \geq 0$$

und somit $x \in \mathcal{O}_{\nu_\mathfrak{p}}$.

Sei umgekehrt $x \in \mathcal{O}_{\nu_\mathfrak{p}}$, das heißt $x \in K$ mit $\nu_\mathfrak{p}(x) \geq 0$. Seien $a, b \in \mathcal{O}$ mit $\frac{a}{b} = x$. Dann gilt

$$\nu_\mathfrak{p}(a) = \nu_\mathfrak{p}(x) + \nu_\mathfrak{p}(b) \geq \nu_\mathfrak{p}(b).$$

Nach Lemma 3.3.18 sind die Bilder der Ideale $\mathfrak{a} := (a)_\mathcal{O}$ und $\mathfrak{b} := (b)_\mathcal{O}$ Potenzen vom maximalen Ideal $\mathfrak{m} := \mathfrak{p}_\mathfrak{p}$ mit der Bewertung als Exponent. Somit gilt wegen $\nu_\mathfrak{p}(a) \geq \nu_\mathfrak{p}(b)$ auch

$$\mathfrak{a}_\mathfrak{p} = \mathfrak{m}^{\nu_\mathfrak{p}(a)} \subset \mathfrak{m}^{\nu_\mathfrak{p}(b)} = \mathfrak{b}_\mathfrak{p}.$$

Wegen $\mathcal{O} \subset \mathcal{O}_\mathfrak{p}$ sind die Erzeuger a, b von $\mathfrak{a}, \mathfrak{b}$ in $\mathcal{O}$ gleichzeitig die Erzeuger von $\mathfrak{a}_\mathfrak{p}$, $\mathfrak{b}_\mathfrak{p}$ in $\mathcal{O}_\mathfrak{p}$. Es gilt also $(a)_{\mathcal{O}_\mathfrak{p}} \subset (b)_{\mathcal{O}_\mathfrak{p}}$. Somit gibt es ein $y \in \mathcal{O}_\mathfrak{p}$ mit $y * b = a$. Also ist $x = \frac{a}{b} = \frac{y*b}{b} = y \in \mathcal{O}_\mathfrak{p}$ und es folgt $\mathcal{O}_{\nu_\mathfrak{p}} \subset \mathcal{O}_\mathfrak{p}$.

□

Lemma 3.3.20. *Sei $\mathcal{R}$ ein kommutativer Ring mit Einselement, $\pi \in \mathcal{R}$ ein Primelement von $\mathcal{R}$ und $e \in \mathcal{R}^*$ eine Einheit. Dann ist $e * \pi$ ebenfalls ein Primelement von $\mathcal{R}$.*

Beweis. Seien $a, b \in \mathcal{R}$ mit $e * \pi \mid a * b$. Dann gilt wegen e Einheit auch $\pi \mid a * b * e^{-1}$. Da π ein Primelement ist, muss also $\pi \mid a \mid a * e^{-1}$ oder $\pi \mid b * e^{-1}$ gelten. Also gilt $e * \pi \mid a$ oder $e * \pi \mid b$. □

Lemma 3.3.21. *Sei $\mathcal{R}$ ein kommutativer Ring mit Einselement und $\mathfrak{p}$ ein Hauptideal in $\mathcal{R}$, das von π erzeugt wird. Dann ist $\mathfrak{p}$ genau dann ein Primideal, wenn π ein Primelement ist.*

Beweis. Sei $a \in \mathcal{R}$. Dann ist $\pi \mid a$ gleichbedeutend mit $\pi * x = a$ für ein $x \in \mathcal{R}$, was wiederum gleichbedeutend mit $a \in (\pi)_\mathcal{R}$ ist. Somit folgt die Behauptung direkt aus den Definitionen von Primideal und Primelement. □

Proposition 3.3.22. *Sei $\mathfrak{p} \neq (0)_\mathcal{O}$ ein Primideal in $\mathcal{O}$. Dann gelten die folgenden Äquivalenzen:*

(i) $\mathfrak{p}$ *ist invertierbar*

(ii) $\mathcal{O}_\mathfrak{p}$ *ist ein diskreter Bewertungsring*

(iii) $\mathfrak{p}$ *enthält ein Primelement π von $\mathcal{O}_\mathfrak{p}$*

Beweis. (i) $\Rightarrow$ (ii): Sei $\mathfrak{p}$ invertierbar. Dann gilt nach Lemma 3.3.19, dass $\mathcal{O}_\mathfrak{p}$ gleich dem diskreten Bewertungsring $\mathcal{O}_{\nu_\mathfrak{p}}$ ist.

(ii) $\Rightarrow$ (iii): Sei $\mathcal{O}_\mathfrak{p}$ ein diskreter Bewertungsring und $\nu : K \to \mathbb{Z}_\infty$ die dazugehörige (surjektive) Bewertung. Wegen der Surjektivität gibt es ein Element π mit $\nu(\pi) = 1$. Dieses ist nach Lemma 3.2.14 ein Primelement in $\mathcal{O}_\mathfrak{p}$. Da $\mathcal{O}_\mathfrak{p}$ der Bewertungsring von ν ist und die Ungleichung

$\nu(\pi) = 1 \geq 0$ gilt, gibt es $\pi_0 \in \mathcal{O}$ und $s \in \mathcal{O} \setminus \mathfrak{p}$ mit $\pi = \frac{\pi_0}{s}$. Dann ist s eine Einheit in $\mathcal{O}_\mathfrak{p}$ und somit $\pi_0 = \pi * s \in \mathcal{O}$ ebenfalls ein Primelement in $\mathcal{O}_\mathfrak{p}$ (siehe Lemma 3.3.20). Es bleibt noch zu zeigen, dass π_0 in $\mathfrak{p}$ ist. Wäre π_0 nicht in $\mathfrak{p}$, so wäre π_0 in $\mathcal{O} \setminus \mathfrak{p}$ und somit eine Einheit in $\mathcal{O}_\mathfrak{p}$. Dies ist aber ein Widerspruch dazu, dass π_0 ein Primelement ist. Somit muss das Primelement π_0 in $\mathfrak{p}$ sein.

(iii) $\Rightarrow$ (i): Sei $\pi \in \mathfrak{p}$ ein Primelement von $\mathcal{O}_\mathfrak{p}$. Dann ist $(\pi)_{\mathcal{O}_\mathfrak{p}}$ nach Lemma 3.3.21 ein Primideal und damit gleich dem maximalen Ideal $\mathfrak{p}_\mathfrak{p}$, da dieses nach Lemma 3.3.17 das einzige Primideal ungleich $(0)_{\mathcal{O}_\mathfrak{p}}$ in $\mathcal{O}_\mathfrak{p}$ ist (und π als Primelement ungleich 0 ist). Außerdem gilt

$$\mathfrak{p} \subset \mathfrak{p} * \tilde{\mathfrak{p}} \subset \mathcal{O},$$

wobei $\tilde{\mathfrak{p}}$ wieder als $\{x \in K \mid x * \mathfrak{p} \in \mathcal{O}\}$ definiert wird. Wegen der Maximalität von $\mathfrak{p}$ nach Proposition 3.3.7 gilt dann entweder $\mathfrak{p} = \mathfrak{p} * \tilde{\mathfrak{p}}$ oder $\mathfrak{p} * \tilde{\mathfrak{p}} = \mathcal{O}$. Man muss also nur ein Element in $(\mathfrak{p} * \tilde{\mathfrak{p}}) \setminus \mathfrak{p}$ finden. Sei $\pi_1, \ldots, \pi_k$ ein Erzeugendensystem von $\mathfrak{p}$ in $\mathcal{O}$. Dann sind $\pi_1, \ldots, \pi_k$ auch in $\mathfrak{p}_\mathfrak{p} = (\pi)_{\mathcal{O}_\mathfrak{p}}$, also gibt es Darstellungen $\pi_i = \pi * \frac{a_i}{s_i}$ mit $a_i \in \mathcal{O}$ und $s_i \in \mathcal{O} \setminus \mathfrak{p}$. Setzt man nun $s := \prod_{i=0}^{k} s_i$, so ist $s \in \mathcal{O} \setminus \mathfrak{p}$ wegen der Primidealeigenschaft und es gilt:

$$s * \pi_{i_0} = s * \pi * \frac{a_{i_0}}{s_{i_0}} = \pi * a_{i_0} * \prod_{i \neq i_0} s_i \in \pi * \mathcal{O} \qquad \forall\, i_0 \in \{1, \ldots, k\}$$

Damit ist $\frac{s}{\pi} * \pi_{i_0} \in \mathcal{O}$ für alle $i_0 \in \{1, \ldots, k\}$ und somit auch $\frac{s}{\pi} * \mathfrak{p} \in \mathcal{O}$, da die π_i ein Erzeugendensystem von $\mathfrak{p}$ sind. Also gilt $\frac{s}{\pi} \in \tilde{\mathfrak{p}}$. Wegen $\pi \in \mathfrak{p}$ ist also $s = \pi * \frac{s}{\pi} \in \mathfrak{p} * \tilde{\mathfrak{p}}$. Außerdem ist s nach Konstruktion nicht in $\mathfrak{p}$. Also ist $s \in (\mathfrak{p} * \tilde{\mathfrak{p}}) \setminus \mathfrak{p}$ und wegen der Maximalität von $\mathfrak{p}$ folgt $\mathfrak{p} \subsetneq \mathfrak{p} * \tilde{\mathfrak{p}} = \mathcal{O}$. Damit ist $\mathfrak{p}$ invertierbar mit Inversem $\tilde{\mathfrak{p}}$.

□

3.3.4 Zerlegung von Idealen in Primideale

In diesem Abschnitt wird gezeigt, wie man eine Menge von invertierbaren Primidealen $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ aus einem (gebrochenen) Ideal $\mathfrak{a}$ herausfaktorisieren kann und dass die Exponenten bei ganzzahligen Idealen genau den Bewertungen an den entsprechenden Primidealen entsprechen. Es wird außerdem gezeigt, dass sich $\mathfrak{a}$ vollständig faktorisieren lässt, falls $\mathfrak{a}$ ein gebrochenes Ideal in der Maximalordnung ist oder ein ganzzahliges Ideal, das teilerfremd zum Führer der Ordnung ist. Schließlich wird noch bewiesen, dass in der Maximalordnung alle (gebrochenen) Ideale invertierbar sind und gebrochene Ideale in der Maximalordnung genau dann ganzzahlig sind, wenn die Exponenten der Zerlegung alle in $\mathbb{N}_0$ sind. Ein Algorithmus für die (teilweise) Faktorisierung von Idealen in invertierbare Primideale ist in Abschnitt 4.3.10 zu finden.

Proposition 3.3.23. *Sei $\mathfrak{a} \neq (0)$ ein ganzzahliges Ideal in $\mathcal{O}$. Dann gibt es eine Zerlegung*

$$\mathfrak{a} = \tilde{\mathfrak{a}} * \prod_{\mathfrak{p} \in \mathfrak{P}_{\mathcal{O}}^*} \mathfrak{p}^{\nu(\mathfrak{p})}$$

mit $\tilde{\mathfrak{a}} \not\subset \mathfrak{p}$ und $\nu(\mathfrak{p}) \in \mathbb{N}_0$ für alle $\mathfrak{p} \in \mathfrak{P}_{\mathcal{O}}^*$. Diese Zerlegung ist eindeutig und die $\nu(\mathfrak{p})$ sind gegeben durch die $\mathfrak{p}$-Bewertungen $\nu_{\mathfrak{p}}(\mathfrak{a})$.

Beweis. Existenz: Sei $(\mathfrak{p}_i)_{i \in I}$ eine (endliche oder abzählbar unendliche) Folge von paarweise verschiedenen, invertierbaren Primidealen, die $\mathfrak{a}$ enthalten. Dabei sei die Indexmenge I im endlichen Fall durch $I = \{1, \ldots, k\}$ und im abzählbaren Fall durch $I = \mathbb{N}$ gegeben. Dann lässt sich mit Proposition 3.3.13 durch

$$\begin{aligned} \mathfrak{a}_0 &:= \mathfrak{a} \\ \mathfrak{a}_i &:= \mathfrak{a}_{i-1} * \mathfrak{p}_i^{-\nu_{\mathfrak{p}_i}(\mathfrak{a}_{i-1})} \qquad \forall\ i \in I \end{aligned}$$

eine Folge von Idealen $(\mathfrak{a}_i)_{i \in I_0}$ mit Indexmenge $I_0 := I \cup \{0\}$ konstruieren, die für alle $i \in I$ folgende Eigenschaften erfüllt:

$$\begin{aligned} \mathfrak{a}_{i-1} &\subset \mathfrak{a}_i \\ \mathfrak{a}_{i-1} &\subset \mathfrak{p}_i \\ \mathfrak{a}_i &\not\subset \mathfrak{p}_i \end{aligned}$$

Wegen diesen drei Eigenschaften ist die Folge $(\mathfrak{a}_i)_{i \in I_0}$ eine streng monoton aufsteigende Kette von Idealen. Da $\mathcal{O}$ noethersch ist, muss I also endlich sein. Somit können nur endlich viele invertierbare Primideale $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$ in $\mathfrak{a}$ enthalten sein und die Indexmenge I_0 ist gegeben durch $\{0, \ldots, k\}$. Ohne Beschränkung der Allgemeinheit sei k maximal, das heißt $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$ sind alle (paarweise verschiedenen) invertierbaren Primideale, die in $\mathfrak{a}$ enthalten sind. Setzt man nun die Elemente der Folge $(\mathfrak{a}_i)_{i \in I_0}$ ineinander ein, so erhält man

$$\mathfrak{a}_k = \mathfrak{a}_{k-1} * \mathfrak{p}_k^{-\nu_{\mathfrak{p}_k}(\mathfrak{a}_{k-1})} = \ldots = \mathfrak{a}_0 * \prod_{i=1}^{k} \mathfrak{p}_i^{-\nu_{\mathfrak{p}_i}(\mathfrak{a}_{i-1})}$$

und somit wegen $\mathfrak{a}_0 = \mathfrak{a}$ durch entsprechendes Umstellen der Gleichung eine Zerlegung von $\mathfrak{a}$:

$$\mathfrak{a} = \mathfrak{a}_k * \prod_{i=1}^{k} \mathfrak{p}_i^{\nu_{\mathfrak{p}_i}(\mathfrak{a}_{i-1})}$$

Wegen den Eigenschaften der Kette der $\mathfrak{a}_i$ gilt außerdem $\mathfrak{a}_k \not\subset \mathfrak{p}_i$ für alle $i \in \{1, \ldots, k\}$. Da die $\mathfrak{p}_i$ nach Voraussetzung paarweise verschieden sind, gilt nach Proposition 3.3.15 und nach der Konstruktion der $\mathfrak{a}_i$ auch

$$\nu_{\mathfrak{p}_i}(\mathfrak{a}_{i-1}) = \nu_{\mathfrak{p}_i}\left(\mathfrak{a}_{i-2} * \mathfrak{p}_{i-1}^{-\nu_{\mathfrak{p}_{i-1}}(\mathfrak{a}_{i-2})}\right) = \nu_{\mathfrak{p}_i}(\mathfrak{a}_{i-2}) = \ldots = \nu_{\mathfrak{p}_i}(\mathfrak{a}_0) = \nu_{\mathfrak{p}_i}(\mathfrak{a}).$$

Sei nun $\mathfrak{p}$ ein Primideal, das $\mathfrak{a}$ nicht enthält. Dann enthält auch $\mathfrak{a}_k$ das Primideal nicht und es gilt $\nu_\mathfrak{p}(\mathfrak{a}) = 0$. Somit ergibt sich durch $\bar{\mathfrak{a}} := \mathfrak{a}_k$ und $\nu(\mathfrak{p}) := \nu_\mathfrak{p}(\mathfrak{a})$ eine Zerlegung wie gefordert.

Eindeutigkeit: Sei

$$\mathfrak{a} = \tilde{\mathfrak{b}} * \prod_{\mathfrak{p} \in \mathfrak{P}^*_\mathcal{O}} \mathfrak{p}^{\bar{\nu}(\mathfrak{p})}$$

eine weitere Zerlegung von $\mathfrak{a}$ mit $\tilde{\mathfrak{b}} \not\subset \mathfrak{p}$ für alle $\mathfrak{p} \in \mathfrak{P}^*_\mathcal{O}$. Dann gilt zunächst $\bar{\nu}(\mathfrak{p}) = 0 = \nu_\mathfrak{p}(\mathfrak{a})$ für alle Primideale $\mathfrak{p}$, die $\mathfrak{a}$ nicht enthalten. Seien nun $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$ wieder alle paarweise verschiedenen Primideale, die $\mathfrak{a}$ enthalten und sei $i_0 \in \{1, \ldots, k\}$. Dann gilt:

$$\mathfrak{a} = \left(\tilde{\mathfrak{a}} * \prod_{i \neq i_0} \mathfrak{p}_i^{\nu_{\mathfrak{p}_i}(\mathfrak{a})} \right) * \mathfrak{p}_{i_0}^{\nu_{\mathfrak{p}_{i_0}}(\mathfrak{a})} = \left(\tilde{\mathfrak{b}} * \prod_{i \neq i_0} \mathfrak{p}_i^{\bar{\nu}(\mathfrak{p}_i)} \right) * \mathfrak{p}_{i_0}^{\bar{\nu}(\mathfrak{p}_{i_0})}$$

Wegen der Eindeutigkeit der $\mathfrak{p}_{i_0}$-Bewertung nach Proposition 3.3.13 folgt dann sofort, dass die Exponenten $\bar{\nu}(\mathfrak{p}_{i_0})$ und $\nu_{\mathfrak{p}_{i_0}}(\mathfrak{a})$ gleich sein müssen (da die Klammern jeweils keine Teilmengen von $\mathfrak{p}_{i_0}$ sind). Damit sind die Exponenten der Zerlegung eindeutig und durch Multiplikation mit den entsprechenden Potenzen der Primidealinversen folgt $\tilde{\mathfrak{a}} = \tilde{\mathfrak{b}}$.

□

Bemerkung 3.3.24. *Das Restideal $\tilde{a}$ aus Proposition 3.3.23 kann ein Produkt aus nicht-invertierbaren Primidealen sein. Es ist aber auch möglich, dass $\tilde{a}$ sich nicht als Produkt von Primidealen darstellen lässt. Beide Möglichkeiten werden im folgenden Beispiel gezeigt.*

Beispiel 3.3.25. Die Berechnungen im Beispiel wurden mit Hilfe der Sage-Algorithmen in Kapitel 4 durchgeführt. Sei $K = \mathbb{Q}(\sqrt[3]{100})$, $\mathcal{O} = \mathbb{Z}[\sqrt[3]{100}]$. Dann ist

$$\mathfrak{p}_2 \quad = \quad (2, \sqrt[3]{100}, \sqrt[3]{100}^2)_\mathcal{O}$$

das einzige Primideal über der Basisprimzahl 2 in $\mathcal{O}$. Außerdem ist $\mathfrak{p}_2$ nicht invertierbar in $\mathcal{O}$. Sei nun $\mathfrak{a} = \mathfrak{p}_2^2$ und $\mathfrak{b} = (2)_\mathcal{O}$. Da $\mathfrak{p}_2$ nicht invertierbar ist und $\mathfrak{p}_2$ das einzige Primideal über $\mathfrak{a}$ ist, liefert die Zerlegung in Proposition 3.3.23 das Ergebnis $\mathfrak{a} = \tilde{\mathfrak{a}}$. In diesem Fall ist $\tilde{\mathfrak{a}} = \mathfrak{a} = \mathfrak{p}_2^2$ also ein Produkt von nicht-invertierbaren Primidealen. Das Ideal $\mathfrak{b}$ hingegen enthält die Primzahl 2 und kann somit nur in Primidealen enthalten sein, die über der Basisprimzahl 2 liegen. Das Primideal $\mathfrak{p}_2$ ist aber das einzige Primideal über 2, also kann nur $\mathfrak{p}_2$ als Primideal-Faktor in $\mathfrak{b}$ vorkommen. Da aber $\mathfrak{b}$ als Hauptideal invertierbar ist und das Primideal $\mathfrak{p}_2$ nicht invertierbar ist, kann es keine vollständige Primidealzerlegung von $\mathfrak{b}$ geben, da ein Produkt von nicht invertierbaren Idealen nie invertierbar ist (vergleiche Proposition 3.1.29).

Proposition 3.3.26. *Sei $\mathfrak{p} \neq (0)_{\mathcal{O}_K}$ ein Primideal in der Maximalordnung $\mathcal{O}_K$. Dann ist $\mathfrak{p}$ invertierbar.*

Beweis. Es reicht zu zeigen, dass $\mathfrak{p} \neq \mathfrak{p} * \tilde{\mathfrak{p}}$ gilt. Dann folgt wegen der Maximalität von $\mathfrak{p}$, dass $\mathfrak{p} * \tilde{\mathfrak{p}} = \mathcal{O}_K$ gilt und somit $\mathfrak{p}$ invertierbar ist (vergleiche Bemerkung 3.3.12). Angenommen es wäre $\mathfrak{p} * \tilde{\mathfrak{p}} = \mathfrak{p}$. Dann gilt für jedes $x \in \tilde{\mathfrak{p}}$ die Relation $x * \mathfrak{p} \subset \tilde{\mathfrak{p}} * \mathfrak{p} = \mathfrak{p}$. Da $\mathfrak{p}$ ein endlich erzeugter $\mathcal{O}_K$-Modul ist, folgt daraus nach Lemma 2.4.2, dass x ganz über $\mathcal{O}_K$ ist. Nach Korollar 3.1.18 ist die Maximalordnung $\mathcal{O}_K$ gleichzeitig der Ganzheitsring in K und somit ganzabgeschlossen. Es ist also $x \in \mathcal{O}_K$ und da x beliebig aus $\tilde{\mathfrak{p}}$ gewählt war, gilt $\tilde{\mathfrak{p}} \subset \mathcal{O}_K$. Dies ist aber ein Widerspruch zu Lemma 3.3.9, also war die Annahme $\mathfrak{p} * \tilde{\mathfrak{p}} = \mathfrak{p}$ falsch. Da $\mathfrak{p}$ nach Proposition 3.3.7 maximal ist, gilt also $\mathfrak{p} \subsetneq \mathfrak{p} * \tilde{\mathfrak{p}} = \mathcal{O}_K$. Damit ist $\mathfrak{p}$ invertierbar. □

Theorem 3.3.27. *Sei $\mathfrak{a} \neq (0)_{\mathcal{O}_K}$ ein ganzzahliges Ideal in $\mathcal{O}_K$. Dann ist $\mathfrak{a}$ ein Produkt von invertierbaren Primidealen. Diese Zerlegung ist eindeutig.*

Beweis. Nach Proposition 3.3.23 gibt es eine eindeutige Zerlegung

$$\mathfrak{a} = \tilde{\mathfrak{a}} * \prod_{\mathfrak{p} \in \mathfrak{P}^*_{\mathcal{O}}} \mathfrak{p}^{\nu_{\mathfrak{p}}(\mathfrak{a})}$$

mit $\tilde{\mathfrak{a}} \not\subset \mathfrak{p}$ für alle invertierbaren Primideale $\mathfrak{p}$ in $\mathcal{O}_K$. In der Maximalordnung sind aber nach Proposition 3.3.26 alle Primideale invertierbar, das heißt $\tilde{\mathfrak{a}}$ ist in keinem Primideal enthalten. Da aber jedes Ideal außer $(1)_{\mathcal{O}_K}$ in einem maximalen Ideal und somit in einem Primideal enthalten ist, muss $\tilde{\mathfrak{a}} = (1)_{\mathcal{O}_K}$ gelten. Damit hat man eine Zerlegung von $\mathfrak{a}$ in Primideale. Man beachte dabei, dass die $\mathfrak{p}$-Bewertungen (und somit die Exponenten) größer gleich 0 sind. □

Theorem 3.3.28. *Sei $\mathfrak{p} \neq (0)_{\mathcal{O}}$ ein Primideal in $\mathcal{O}$. Dann ist $\mathfrak{p}$ genau dann invertierbar in $\mathcal{O}$ wenn $\mathfrak{F}_{\mathcal{O}}$ nicht in $\mathfrak{p}$ enthalten ist.*

Beweis. Sei zunächst $\mathfrak{F}_{\mathcal{O}}$ nicht in $\mathfrak{p}$ enthalten. Dann gibt es ein Element $t \in \mathfrak{F}_{\mathcal{O}} \setminus \mathfrak{p}$. Da t im Führer ist, gilt $t * \mathcal{O}_K \subset \mathcal{O}$ und somit auch $\mathcal{O}_K \subset t^{-1} * \mathcal{O}$. Man kann also den Ringhomomorphismus

$$\varphi : \mathcal{O}_K \quad \to \quad t^{-1} * \mathcal{O} \quad \to \quad \mathcal{O}_{\mathfrak{p}}$$

betrachten, der durch Inklusionen induziert wird. Dann ist $\mathfrak{P} := \varphi^{-1}(\mathfrak{p}_{\mathfrak{p}})$ als Kontraktion eines Primideals ein Primideal in $\mathcal{O}_K$ (vergleiche Lemma 2.1.5). Erweitert man den Ringhomomorphismus noch bis $\mathcal{O}$, so erhält man:

$$\begin{array}{rccccccc} \bar{\varphi} : \mathcal{O} & \to & \mathcal{O}_K & \to & t^{-1} * \mathcal{O} & \to & \mathcal{O}_{\mathfrak{p}} \\ x & \mapsto & x & \mapsto & x = t^{-1} * (t * x) & \mapsto & x = \frac{t*x}{t} \end{array}$$

Der Ringhomomorphismus besteht nur aus kanonischen Inklusionen. In diesem Fall entspricht die Kontraktion von Idealen dem Schnitt mit der Definitionsmenge der Abbildung. Außerdem wurde bereits gezeigt, dass $\mathfrak{p} = \mathfrak{p}_\mathfrak{p}|_\mathcal{O}$ gilt. Somit folgt:

$$\mathfrak{p} = \mathfrak{p}_\mathfrak{p} \cap \mathcal{O} = (\mathfrak{p}_\mathfrak{p} \cap \mathcal{O}_K) \cap \mathcal{O} = \mathfrak{P} \cap \mathcal{O}$$

Damit gilt nach Lemma 2.3.15 auch $\mathcal{O}_\mathfrak{p} \subset (\mathcal{O}_K)_\mathfrak{P}$. Sei $\frac{a}{s} \in (\mathcal{O}_K)_\mathfrak{P}$ mit $a \in \mathcal{O}_K$ und $s \in \mathcal{O}_K \setminus \mathfrak{P}$. Dann sind $t * a$ und $t * s$ in $t * \mathcal{O}_K \subset \mathcal{O}$. Wegen

$$t \in \mathfrak{F}_\mathcal{O} \setminus \mathfrak{p} \subset \mathcal{O} \setminus \mathfrak{p} = \mathcal{O} \setminus (\mathfrak{P} \cap \mathcal{O}) \subset \mathcal{O}_K \setminus \mathfrak{P}$$

und $s \in \mathcal{O}_K \setminus \mathfrak{P}$ ist nach der Primidealeigenschaft von $\mathfrak{P}$ auch $t * s \in \mathcal{O}_K \setminus \mathfrak{P}$. Es folgt also

$$t * s \in \mathcal{O} \cap (\mathcal{O}_K \setminus \mathfrak{P}) = \mathcal{O} \setminus (\mathfrak{P} \cap \mathcal{O}) = \mathcal{O} \setminus \mathfrak{p}$$

und damit $\frac{a}{s} = \frac{t*a}{t*s} \in \mathcal{O}_\mathfrak{p}$. Somit ist $\mathcal{O}_\mathfrak{p} = (\mathcal{O}_K)_\mathfrak{P}$. Nach Proposition 3.3.22 ist ein Primideal ungleich $(0)_\mathcal{O}$ genau invertierbar, wenn seine Lokalisierung ein diskreter Bewertungsring ist. Da $\mathfrak{P}$ als Primideal in der Maximalordnung invertierbar ist, ist also $\mathcal{O}_\mathfrak{p} = (\mathcal{O}_K)_\mathfrak{P}$ ein diskreter Bewertungsring und damit $\mathfrak{p}$ invertierbar.

Sei umgekehrt $\mathfrak{p}$ invertierbar. Dann ist $\mathcal{O}_\mathfrak{p}$ nach Proposition 3.3.22 ein diskreter Bewertungsring, also insbesondere ganzabgeschlossen nach Proposition 3.2.11. Da $\mathbb{Z} \subset \mathcal{O}_\mathfrak{p} \subset K$ gilt und $\mathcal{O}_K$ der ganze Abschluss von $\mathbb{Z}$ in K ist, gilt also $\mathcal{O}_K \subset \mathcal{O}_\mathfrak{p}$. Somit gibt es ein $\mathcal{O}$-Erzeugendensystem $(\frac{a_1}{s_1}, \ldots, \frac{a_k}{s_k})$ von $\mathcal{O}_K$ mit $a_i \in \mathcal{O}$ und $s_i \in \mathcal{O} \setminus \mathfrak{p}$. Sei s der Hauptnenner (in $\mathcal{O}$) der $\frac{a_i}{s_i}$. Dann ist $s \in \mathcal{O} \setminus \mathfrak{p}$, da ansonsten wegen der Primidealeigenschaft von $\mathfrak{p}$ das Element s mit mindestens einem s_i einen gemeinsamen Teiler (in $\mathcal{O}$) hätte, der in $\mathfrak{p}$ liegt. Dies ist aber nicht möglich, da dann s_i in $\mathfrak{p}$ wäre. Es gilt also $s * \frac{a_i}{s_i} \in \mathcal{O}$ für alle $i \in \{1, \ldots, k\}$, also auch $s * \mathcal{O}_K \subset \mathcal{O}$. Somit ist $s \in \mathfrak{F}_\mathcal{O}$, aber $s \notin \mathfrak{p}$ und damit ist der Führer nicht in $\mathfrak{p}$ enthalten.

□

Theorem 3.3.29. *Sei $\mathfrak{a} \neq (0)_\mathcal{O}$ ein ganzzahliges Ideal in $\mathcal{O}$, das teilerfremd zu $\mathfrak{F}_\mathcal{O}$ ist. Dann ist $\mathfrak{a}$ ein Produkt von invertierbaren Primidealen. Diese Zerlegung ist eindeutig.*

Beweis. Nach Proposition 3.3.23 gibt es eine eindeutige Zerlegung

$$\tilde{\mathfrak{a}} * \prod_{\mathfrak{p} \in \mathfrak{P}^*_\mathcal{O}} \mathfrak{p}^{\nu_\mathfrak{p}(\mathfrak{a})}$$

mit $\tilde{\mathfrak{a}} \not\subset \mathfrak{p}$ für alle invertierbaren Primideale $\mathfrak{p}$ in $\mathcal{O}_K$. Angenommen das Ideal $\tilde{\mathfrak{a}}$ wäre ungleich $(1)_\mathcal{O}$. Dann ist es in einem maximalen Ideal enthalten,

also insbesondere in einem Primideal. Da es in keinem invertierbaren Primideal enthalten ist, muss es also in einem nicht invertierbaren Primideal $\mathfrak{q}$ enthalten sein, wobei $\mathfrak{q} \neq (0)_{\mathcal{O}}$ gilt (wegen $\mathfrak{a} \neq (0)_{\mathcal{O}}$). Dann ist aber

$$\mathfrak{a} \subset \tilde{\mathfrak{a}} \subset \mathfrak{q}$$

und wegen $\mathfrak{q}$ nicht invertierbar gilt nach Theorem 3.3.28 zusätzlich $\mathfrak{F}_{\mathcal{O}} \subset \mathfrak{q}$. Damit folgt wegen der Teilerfremdheit von $\mathfrak{a}$ und $\mathfrak{F}_{\mathcal{O}}$:

$$(1)_{\mathcal{O}} = \mathfrak{a} + \mathfrak{F}_{\mathcal{O}} \subset \mathfrak{q} + \mathfrak{q} = \mathfrak{q}$$

Dies ist aber ein Widerspruch dazu, dass $\mathfrak{q}$ ein Primideal ist. Somit muss $\tilde{\mathfrak{a}} = (1)_{\mathcal{O}}$ gelten und die Behauptung ist gezeigt. □

Theorem 3.3.30. *Sei $\mathfrak{a} \neq (0)$ ein gebrochenes Ideal von $\mathcal{O}_K$. Dann gibt es eine (bis auf die Reihenfolge der $\mathfrak{p}_i$) eindeutige Zerlegung von $\mathfrak{a}$ in Potenzen von invertierbaren Primidealen $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$ von $\mathcal{O}_K$, das heißt*

$$\mathfrak{a} = \prod_{i=1}^{k} \mathfrak{p}_i^{\nu_i}$$

mit $k \in \mathbb{N}_0$ und $\nu_i \in \mathbb{Z}$. Dabei sei das leere Produkt für $k = 0$ durch das multiplikative neutrale Element $(1)_{\mathcal{O}_K}$ definiert.

Beweis. Nach Korollar 3.1.27 gibt es ein $\alpha \in \mathbb{Z}$, so dass

$$\mathfrak{b} := (\alpha)_{\mathcal{O}_K} * \mathfrak{a} = \alpha * \mathfrak{a} \subset \mathcal{O}_K$$

ein ganzzahliges Ideal in $\mathcal{O}_K$ ist. Mit Theorem 3.3.27 kann man nun die beiden ganzzahligen Ideale $(\alpha)_{\mathcal{O}_K}$ und $\mathfrak{b}$ in Primidealpotenzen zerlegen, wobei $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$ die Menge der Primideale ist, die $\mathfrak{a}$ oder $\mathfrak{b}$ enthalten (für den Beweis von $k < \infty$ vergleiche den Beweis von Proposition 3.3.23):

$$\begin{aligned} (\alpha)_{\mathcal{O}_K} &= \prod_{i=1}^{k} \mathfrak{p}_i^{\nu_{\mathfrak{p}}(\alpha)} \\ \mathfrak{b} &= \prod_{i=1}^{k} \mathfrak{p}_i^{\nu_{\mathfrak{p}}(\mathfrak{b})} \end{aligned}$$

$(\alpha)_{\mathcal{O}_K}$ ist ein Hauptideal und somit invertierbar. Wegen

$$\mathfrak{a} = {(\alpha)_{\mathcal{O}_K}}^{-1} * \mathfrak{b} = (\alpha^{-1})_{\mathcal{O}_K} * \mathfrak{b}$$

ergibt sich mit

$$\nu_i := \nu_{\mathfrak{p}}\big(\alpha^{-1}\big) + \nu_{\mathfrak{p}}(\mathfrak{b}) = -\nu_{\mathfrak{p}}(\alpha) + \nu_{\mathfrak{p}}(\mathfrak{b})$$

die Existenz der behaupteten Zerlegung und wegen der Eindeutigkeit der Zerlegung von $(\alpha)_{\mathcal{O}_K}$ und $\mathfrak{b}$ auch die Eindeutigkeit der Zerlegung von $\mathfrak{a}$. □

Korollar 3.3.31. *Sei $\mathfrak{a}$ ein gebrochenes Ideal von $\mathcal{O}_K$. Dann ist $\mathfrak{a}$ invertierbar in $\mathcal{O}_K$.*

Beweis. Nach Theorem 3.3.30 ist $\mathfrak{a}$ ein Produkt von Potenzen von invertierbaren Primidealen. Somit ist $\mathfrak{a}$ als Produkt von invertierbaren Idealen nach Proposition 3.1.29 ebenfalls invertierbar. □

Bemerkung 3.3.32. *Ein gebrochenes Ideal $\mathfrak{a}$ in $\mathcal{O}_K$ ist genau dann ganzzahlig, wenn in der Darstellung als Produkt von Primidealpotenzen (aus Theorem 3.3.30) alle ν_i in $\mathbb{N}_0$ sind.*

Beweis. Sind alle ν_i in $\mathbb{N}_0$, so ist $\mathfrak{a}$ ein Produkt von Primidealen, also insbesondere ein Produkt von ganzzahligen Idealen und somit ebenfalls ganzzahlig. Ist umgekehrt $\mathfrak{a}$ ganzzahlig, so folgt aus Theorem 3.3.27, dass $\mathfrak{a}$ ein Produkt von Primidealen ist und es somit eine Darstellung mit nicht-negativen Exponenten gibt. Wegen der Eindeutigkeit ist dies die gleiche Darstellung wie in Theorem 3.3.30 und somit gilt $\nu_i \in \mathbb{N}_0$. □

3.3.5 p-Maximalität

In diesem Abschnitt wird p-Maximalität definiert und gezeigt, dass eine Ordnung $\mathcal{O}$ genau dann p-maximal ist, wenn alle Primideale über der Primzahl p invertierbar in $\mathcal{O}$ sind. Außerdem wird angedeutet, wie man daraus einen Algorithmus zur Bestimmung der Maximalordnung ableiten kann (dieser wird dann in Abschnitt 4.3.5 vollständig angegeben).

Definition 3.3.33. Sei $p \in \mathbb{Z}$ prim. Die Ordnung $\mathcal{O}$ heißt **p-maximal**, falls $p \nmid (\mathcal{O}_K : \mathcal{O})$ gilt.

Bemerkung 3.3.34. *Die Ordnung $\mathcal{O}$ ist genau dann gleich der Maximalordnung $\mathcal{O}_K$, wenn $(\mathcal{O}_K : \mathcal{O}) = 1$ gilt. Dies ist genau dann der Fall, wenn die Ordnung p-maximal ist für alle Primzahlen $p \in \mathbb{Z}$.*

Lemma 3.3.35. *Sei $p \in \mathbb{Z}$ prim. Dann gelten die folgenden Äquivalenzen:*

(i) $\mathcal{O}$ ist p-maximal

(ii) $(p)_{\mathcal{O}_K}$ und $\mathfrak{F}_{\mathcal{O}}$ sind teilerfremd als Ideale in $\mathcal{O}_K$, das heißt es gilt $(p)_{\mathcal{O}_K} + \mathfrak{F}_{\mathcal{O}} = (1)_{\mathcal{O}_K}$

(iii) alle Primideale $\mathfrak{p}$ in $\mathcal{O}$ über p sind invertierbar

Beweis. (i) $\Rightarrow$ (ii): Sei $\mathcal{O}$ p-maximal, also $p \nmid (\mathcal{O}_K : \mathcal{O}) =: m$. Da $(\mathcal{O}_K : \mathcal{O})$ die Anzahl der Elemente in $\mathcal{O}_K/\mathcal{O}$ und somit die Gruppenordnung des Faktormoduls ist, gilt für jedes $\bar{x} \in \mathcal{O}_K/\mathcal{O}$ die Gleichung $m * \bar{x} = 0_{\mathcal{O}_K/\mathcal{O}}$. Also ist auch $m * x \in \mathcal{O}$ für jedes $x \in \mathcal{O}_K$. Das Hauptideal $(m)_{\mathcal{O}_K}$ ist dann ein Ideal in $\mathcal{O}_K$, das in $\mathcal{O}$ enthalten ist. Da der Führer von $\mathcal{O}$ das größte solche Ideal in $\mathcal{O}_K$ ist, muss also

$(m)_{\mathcal{O}_K} \subset \mathfrak{F}_\mathcal{O}$ gelten (ansonsten wäre $\mathfrak{b} := (m)_{\mathcal{O}_K} + \mathfrak{F}_\mathcal{O}$ ein größeres Ideal in $\mathcal{O}_K$ mit der Eigenschaft, dass $\mathfrak{b}$ in $\mathcal{O}$ liegt). Da p eine Primzahl ist und $p \nmid m$ gilt, sind p und m teilerfremd. Daraus folgt mit Lemma 2.6.4, dass auch $(p)_{\mathcal{O}_K}$ und $(m)_{\mathcal{O}_K}$ teilerfremd sind und somit $(p)_{\mathcal{O}_K} + (m)_{\mathcal{O}_K} = (1)_{\mathcal{O}_K}$ gilt. Wie oben gezeigt wurde, gilt aber $(m)_{\mathcal{O}_K} \subset \mathfrak{F}_\mathcal{O}$ und somit

$$(1)_{\mathcal{O}_K} = (p)_{\mathcal{O}_K} + (m)_{\mathcal{O}_K} \subset (p)_{\mathcal{O}_K} + \mathfrak{F}_\mathcal{O} \subset (1)_{\mathcal{O}_K}.$$

Somit gilt $(p)_{\mathcal{O}_K} + \mathfrak{F}_\mathcal{O} = (1)_{\mathcal{O}_K}$ und damit die Behauptung.

(ii) $\Rightarrow$ (iii): Angenommen es gäbe ein Primideal $\mathfrak{q}$ in $\mathcal{O}$ mit $(p)_\mathcal{O} \subset \mathfrak{q}$, das nicht invertierbar ist. Dann gilt nach Theorem 3.3.28 auch $\mathfrak{F}_\mathcal{O} \subset \mathfrak{q}$ und damit $(p)_\mathcal{O} + \mathfrak{F}_\mathcal{O} \subset \mathfrak{q} + \mathfrak{q} = \mathfrak{q}$. Dann wäre aber

$$(p)_{\mathcal{O}_K} + \mathfrak{F}_\mathcal{O} = \mathcal{O}_K((p)_\mathcal{O} + \mathfrak{F}_\mathcal{O}) \subset \mathcal{O}_K\mathfrak{q} \subsetneq (1)_{\mathcal{O}_K}.$$

Dies ist ein Widerspruch zu $(p)_{\mathcal{O}_K} + \mathfrak{F}_\mathcal{O} = (1)_{\mathcal{O}_K}$. Also muss jedes Primideal $\mathfrak{p}$ in $\mathcal{O}$ mit $(p)_\mathcal{O} \subset \mathfrak{p}$ invertierbar sein.

(iii) $\Rightarrow$ (i): Angenommen $\mathcal{O}$ ist nicht p-maximal. Dann teilt p den Index $(\mathcal{O}_K : \mathcal{O})$. Wegen $\mathfrak{F}_\mathcal{O} \subset \mathcal{O} \subset \mathcal{O}_K$ gilt aber nach Proposition 2.2.8 auch

$$(\mathcal{O}_K : \mathfrak{F}_\mathcal{O}) = (\mathcal{O}_K : \mathcal{O}) * (\mathcal{O} : \mathfrak{F}_\mathcal{O}).$$

Somit teilt p auch $(\mathcal{O}_K : \mathfrak{F}_\mathcal{O})$. Als Ideal in der Maximalordnung ist $\mathfrak{F}_\mathcal{O}$ nach Theorem 3.3.27 in Primideale zerlegbar, also $\mathfrak{F}_\mathcal{O} = \prod_{i=1}^r \mathfrak{P}_i^{e_i}$ für paarweise verschiedene, invertierbare Primideale $\mathfrak{P}_1, \ldots, \mathfrak{P}_r$ in $\mathcal{O}_K$. Also gilt nach dem Chinesischen Restsatz (Theorem 2.6.5) auch die Gleichung $(\mathcal{O}_K : \mathfrak{F}_\mathcal{O}) = \prod_{i=1}^r (\mathcal{O}_K : \mathfrak{P}_i)^{e_i}$. Da p eine Primzahl ist, teilt also p für ein i_0 den Index $(\mathcal{O}_K : \mathfrak{P}_{i_0})$. Der Index $(\mathcal{O}_K : \mathfrak{P}_{i_0})$ ist aber nach Proposition 3.3.2 eine Potenz der Basisprimzahl, also ist $\mathfrak{P}_{i_0}$ ein Primideal in $\mathcal{O}_K$ über p und somit $\mathfrak{p}_{i_0} := \mathfrak{P}_{i_0} \cap \mathcal{O}$ ein Primideal in $\mathcal{O}$ über p. Wegen der Primfaktorzerlegung von $\mathfrak{F}_\mathcal{O}$ gilt $\mathfrak{F}_\mathcal{O} \subset \mathfrak{P}_{i_0}$ und wegen $\mathfrak{F}_\mathcal{O} \subset \mathcal{O}$ auch $\mathfrak{F}_\mathcal{O} \subset \mathfrak{p}_{i_0}$. Nach Theorem 3.3.28 ist dann aber $\mathfrak{p}_{i_0}$ nicht invertierbar in $\mathcal{O}$, also sind nicht alle Primideale in $\mathcal{O}$ über p invertierbar. Dies ist ein Widerspruch zur Voraussetzung (iii). Also ist die Annahme falsch und $\mathcal{O}$ muss p-maximal sein.

□

Bemerkung 3.3.36. *Solange $\mathcal{O}$ nicht die Maximalordnung ist, findet man immer eine Primzahl p, so dass $\mathcal{O}$ nicht p-maximal ist. Dann muss es nach Lemma 3.3.35 auch ein Primideal $\mathfrak{p}$ über p geben, das nicht invertierbar ist. Die Ordnung Ord($\mathfrak{p}$) ist dann eine echte Obermenge von $\mathcal{O}$. Durch Iteration dieses Vorgangs erhält man einen Algorithmus, der am Ende die Maximalordnung liefert. Dieser Algorithmus wird in Abschnitt 4.3.5 noch genauer erklärt und bewiesen.*

Kapitel 4

Algorithmen

In diesem Kapitel soll das Rechnen in Zahlkörpern mit Moduln und gebrochenen Idealen algorithmisch dargestellt werden. In Abschnitt 4.1 wird zunächst erläutert, wie man mit Hilfe von Koordinatensystemen das Rechnen in einem Zahlkörper auf das Rechnen in $\mathbb{Q}^n$ zurückführen kann. Anschließend wird in Abschnitt 4.2 eine Übersicht über Klassen und Funktionen gegeben, mit denen das Rechnen mit Moduln, Idealen und Ordnungen in Zahlkörpern umgesetzt werden kann. In Abschnitt 4.3 werden einige Algorithmen beschrieben und bewiesen, die für das Rechnen in Zahlkörpern wichtig oder nützlich sind. Schließlich wird in Abschnitt 4.4 das Rechnen in Zahlkörpern mit Hilfe von Sage (siehe [S$^+$09]) umgesetzt. Dabei werden auch einige Klassen und Funktionen verwendet, die in Sage bereits implementiert sind. Zu Beginn jedes Abschnitts werden noch ausführlichere Informationen über den entsprechenden Abschnitt gegeben.

4.1 Koordinatensysteme in Zahlkörpern

Jeder Zahlkörper ist ein endlich erzeugter $\mathbb{Q}$-Vektorraum und somit isomorph zu $\mathbb{Q}^n$, wobei n der Grad von $K \mid \mathbb{Q}$ ist. In diesem Abschnitt wird gezeigt, wie man durch das Festlegen von einer Basis eines endlich erzeugten $\mathbb{Q}$-Vektorraums ein Koordinatensystem definieren kann und mit Hilfe dieses Koordinatensystems Elemente, Moduln und Abbildungen im Vektorraum auf Elemente, Moduln und Abbildungen in $\mathbb{Q}^n$ zurückführen kann. Außerdem wird beschrieben wie man Abbildungen in $\mathbb{Q}^n$ als Matrizen darstellt und was bei einem Wechsel des Koordinatensystems mit den einzelnen Objekten passiert.

Definition 4.1.1. Sei K ein $\mathbb{Q}$-Vektorraum, $B := b_1, \ldots, b_n$ eine $\mathbb{Q}$-Basis von K. Dann lässt sich jedes Element $a \in K$ eindeutig als $\mathbb{Q}$-Linearkombination $\sum_{i=1}^{n} a_i * b_i = a$ der Basiselemente schreiben. Die Abbildung

$$\begin{array}{rccc} \phi_B : K & \to & \mathbb{Q}^n \\ a & \mapsto & (a_1, \ldots, a_n) \end{array}$$

ist ein Isomorphismus und wird als **Koordinatenabbildung** bezüglich der Basis B bezeichnet. Die Menge $\mathbb{Q}^n$ wird auch als **Koordinatenraum** bezeichnet. Das Tupel $(a_1, \ldots, a_n) = \phi_B(a) \in \mathbb{Q}^n$ heißt **Koordinatenvektor** von $a \in K$ bezüglich B. Außerdem wird $(\mathbb{Q}^n, \phi_B)$ beziehungsweise $(\mathbb{Q}^n, \phi_B^{-1}, \phi_B)$ im Folgenden als **Koordinatensystem** von K bezüglich der Basis B bezeichnet.

Bemerkung 4.1.2. *Da ϕ_B ein Isomorphismus von $\mathbb{Q}$-Vektorräumen ist, werden ($\mathbb{Q}$- beziehungsweise $\mathbb{Z}$-)Linearkombinationen erhalten. Das Bild einer Linearkombination von Elementen ist also die Linearkombination (mit gleichen Koeffizienten) von den Bildern der Elemente. Daraus ergibt sich sofort, dass das Bild $\phi_B(\mathfrak{m})$ eines Moduls $\mathfrak{m} \subset K$ genau der $\mathbb{Z}$-Untermodul von $\mathbb{Q}^n$ ist, der von den Bildern eines Erzeugendensystem von $\mathfrak{m}$ erzeugt wird.*

Bemerkung 4.1.3. *Nach Theorem 2.4.10 wird K von einem einzigen Element erzeugt, das heißt es gibt ein Element $\alpha \in K$ mit $K = \mathbb{Q}[\alpha]$. Legt man für jeden Zahlkörper K einen kanonischen Erzeuger α_K fest, so erhält man durch $B_K = \left\{1, \alpha_K^1, \alpha_K^2, \ldots, \alpha_K^{n-1}\right\}$ eine kanonische Basis von K. Diese wird im Folgenden als **Standardbasis** von K bezeichnet. Dadurch erhält man auch ein **Standardkoordinatensystem** $(\mathbb{Q}^n, \phi_{B_K})$ des Zahlkörpers.*

Lemma 4.1.4. *Sei $f : V \to W$ eine lineare Abbildung zwischen $\mathbb{Q}$-Vektorräumen. Sei $B_V := \{v_1, \ldots, v_m\}$ eine Basis von V und $B_W := \{w_1, \ldots, w_n\}$ eine Basis von W. Dann gibt es eine lineare Abbildung $f_{B_V}^{B_W} : \mathbb{Q}^m \to \mathbb{Q}^n$, so dass das folgende Diagramm kommutiert:*

$$\begin{array}{ccc} V & \xrightarrow{f} & W \\ {\scriptstyle \phi_{B_V}}\downarrow & & \downarrow{\scriptstyle \phi_{B_W}} \\ \mathbb{Q}^m & \xrightarrow{f_{B_V}^{B_W}} & \mathbb{Q}^n \end{array} \tag{4.1}$$

Beweis. Die Abbildungen ϕ_{B_V} und ϕ_{B_W} sind Isomorphismen. Somit ist $f_{B_V}^{B_W} := \phi_{B_W} \circ f \circ \phi_{B_V}^{-1}$ eine Abbildung mit den gewünschten Eigenschaften. □

Bemerkung 4.1.5. *Umgekehrt kann man auch jeder Abbildung zwischen den Koordinatenräumen eine entsprechende Abbildung zwischen den $\mathbb{Q}$-Vektorräumen zuordnen (bei gegebenen Basen). Der Beweis ist völlig analog.*

Definition 4.1.6. Schreibt man die Bilder der Abbildung $f_{B_V}^{B_W}$ als Zeilen in eine Matrix $M_{B_V}^{B_W}(f)$, so gilt für jeden Vektor $v \in \mathbb{Q}^m$ die Gleichung

$$f_{B_V}^{B_W}(v) = v * M_{B_V}^{B_W}(f).$$

Somit definiert jede lineare Abbildung f zwischen $\mathbb{Q}$-Vektorräumen eine Matrix $M_{B_V}^{B_W}(f)$ bezüglich der Basen B_V und B_W. Man nennt diese Matrix

die **(Zeilen)-Darstellungsmatrix** von f bezüglich B_V und B_W. Umgekehrt definiert jede $m \times n$-Matrix A eine lineare Abbildung $f(A) : V \to W$ bezüglich der Basen B_V und B_W, indem man $f_{B_V}^{B_W}(A)(v) := v * A$ setzt und dann die Funktion f durch $\phi_{B_W}^{-1} \circ f_{B_V}^{B_W} \circ \phi_{B_V}$ definiert (vergleiche Diagramm 4.1).

Bemerkung 4.1.7. *Man kann die Darstellungsmatrizen auch so definieren, dass man die Bilder in die Spalten schreibt, anstatt in die Zeilen. Die Berechnungen laufen dann analog, man muss nur alle Matrizen durch ihre Transponierten ersetzen und alle Matrixmultiplikationen von rechts durch Matrixmultiplikationen von links austauschen und umgekehrt (wobei Vektoren hier auch als Matrizen gezählt werden). Im Folgenden werden jedoch immer Zeilen-Darstellungsmatrizen benutzt.*

Bemerkung 4.1.8. *In den vorherigen Definitionen und Lemmas wurde gezeigt, dass lineare Abbildungen zwischen $\mathbb{Q}$-Vektorräumen sich Matrizen mit Koeffizienten in $\mathbb{Q}$ zuordnen lassen und umgekehrt (bei geeigneter Zeilen- und Spaltenzahl). Das folgende Lemma zeigt nun, dass die Darstellungsmatrix einer Verknüpfung von linearen Abbildungen das Produkt der Darstellungsmatrizen der linearen Abbildungen ist. Da Multiplikation von Matrizen beziehungsweise Verknüpfung von linearen Abbildungen nicht kommutativ ist, sollte man aber genau auf die Reihenfolge im Lemma achten.*

Lemma 4.1.9. *Seien U, V, W $\mathbb{Q}$-Vektorräume mit Basen B_U, B_V, B_W. Seien $f : U \to V$, $g : V \to W$ lineare Abbildungen. Dann gilt*

$$M_{B_U}^{B_W}(g \circ f) = M_{B_U}^{B_V}(f) * M_{B_V}^{B_W}(g).$$

Beweis. Nach der Definition der Darstellungsmatrizen gilt für jeden Vektor $v \in \mathbb{Q}^m$:

$$\begin{aligned} v * M_{B_U}^{B_W}(g \circ f) &= (g_{B_V}^{B_W} \circ f_{B_U}^{B_V})(v) = g_{B_V}^{B_W}(f_{B_U}^{B_V}(v)) \\ &= g_{B_V}^{B_W}(v * M_{B_U}^{B_V}(f)) = (v * M_{B_U}^{B_V}(f)) * M_{B_V}^{B_W}(g) \\ &= v * (M_{B_U}^{B_V}(f) * M_{B_V}^{B_W}(g)) \end{aligned}$$

Insbesondere gilt diese Gleichung für die Einheitsvektoren e_i. Da $e_i * A$ gleich der i-ten Zeile einer Matrix A ist, sind also die Zeilen der Matrix auf der linken Seite gleich den Zeilen der Matrix auf der rechten Seiten. Somit sind die Matrizen gleich. □

Definition 4.1.10. Sei V ein $\mathbb{Q}$-Vektorraum, $n = (V : \mathbb{Q})$. Seien B, $\tilde{B}$ zwei Basen von V. Dann induziert die Identität folgendes kommutatives Diagramm:

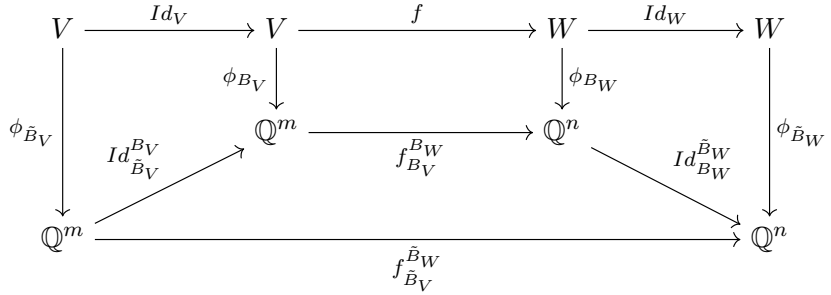
$$\begin{array}{ccc} V & \xrightarrow{\mathrm{Id}} & V \\ {\scriptstyle \phi_B}\downarrow & & \downarrow{\scriptstyle \phi_{\tilde{B}}} \\ \mathbb{Q}^n & \xrightarrow{\mathrm{Id}_B^{\tilde{B}}} & \mathbb{Q}^n \end{array}$$

Somit stellt die Abbildung $\mathrm{Id}_B^{\tilde{B}}$ den Koordinatenübergang von B zu $\tilde{B}$ dar. Wendet man also $Id_B^{\tilde{B}}$ auf die Koordinaten bezüglich der Basis B an, dann erhält man als Bilder die Koordinaten bezüglich der Basis $\tilde{B}$. Die dazugehörige Matrix $T_B^{\tilde{B}} := M_B^{\tilde{B}}(\mathrm{Id})$ nennt man **Transformationsmatrix** von B nach $\tilde{B}$.

Lemma 4.1.11. *Seien V, W $\mathbb{Q}$-Vektorräume mit Dimension $(V : \mathbb{Q}) = m$, $(W : \mathbb{Q}) = n$ und $f : V \to W$ eine lineare Abbildung. Seien B_V, $\tilde{B}_V$ Basen von V und B_W, $\tilde{B}_W$ Basen von W. Dann gilt:*

$$M_{\tilde{B}_V}^{\tilde{B}_W}(f) = T_{\tilde{B}_V}^{B_V} * M_{B_V}^{B_W}(f) * T_{B_W}^{\tilde{B}_W}.$$

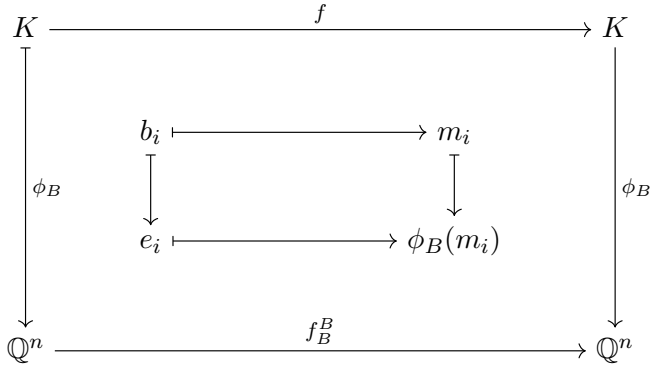
Beweis. Man erhält das folgende kommutative Diagramm:



Es gilt also $f_{\tilde{B}_V}^{\tilde{B}_W} = Id_{B_W}^{\tilde{B}_W} \circ f_{B_V}^{B_W} \circ Id_{\tilde{B}_V}^{B_V}$ und somit folgt wegen Lemma 4.1.9 die Behauptung. □

Definition 4.1.12. Sei K ein $\mathbb{Q}$-Vektorraum, $\mathfrak{m}$ ein endlich erzeugter $\mathbb{Z}$-Modul in K, B eine Basis von K und $m_1, \ldots, m_k$ ein $\mathbb{Z}$-Erzeugendensystem von $\mathfrak{m}$. Dann nennt man die $k \times n$-Matrix $A(m_1, \ldots, m_k)$, die aus den Zeilen $\phi_B(m_1), \ldots, \phi_B(m_k)$ besteht, eine **Erzeugermatrix** von $\mathfrak{m}$ bezüglich B.

Bemerkung 4.1.13. *$A(m_1, \ldots, m_k)$ ist die Darstellungsmatrix der Funktion $f : K \to K$, die b_i auf m_i abbildet.*



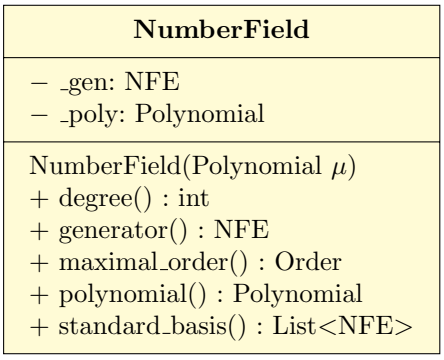
f_B^B bildet also $\mathbb{Z}^n$ surjektiv auf den Modul $\phi_B(\mathfrak{m})$ in $\mathbb{Q}^n$ ab.

Bemerkung 4.1.14. *Durch Berechnen der Hermite-Normalform einer Erzeugermatrix von $\mathfrak{m}$ bezüglich der Basis B und Entfernen der Nullzeilen erhält man eine neue Matrix, deren Zeilen die Koordinatenvektoren einer $\mathbb{Z}$-Basis des Moduls sind (bezüglich der Basis B). Man nennt diese Matrix dann die **Basismatrix** von $\mathfrak{m}$. Wegen der Eindeutigkeit der Hermite-Normalform erhält man auf diese Weise eine Basis des Moduls, die nicht vom Erzeugendensystem abhängt. Man sollte jedoch darauf achten, dass die Hermite-Normalform nur für Matrizen mit Koeffizienten in einem euklidischen Ring definiert ist (zum Beispiel $\mathbb{Z}$). Durch Basisänderungen kann man jedoch leicht die Koeffizienten in $\mathbb{Q}$ zu Koeffizienten in $\mathbb{Z}$ machen. Dies wird in Algorithmus 4.3.3 noch genauer erläutert.*

4.2 Übersicht über Funktionen

In diesem Abschnitt werden einige Funktionen beschrieben, die man für das Rechnen in Zahlkörpern implementieren sollte. Dabei werden als Übersicht über die Funktionen sogenannte UML-Diagramme (Unified Modeling Language) verwendet. Weitere Informationen zu UML findet man auf der offiziellen UML-Seite (`http://www.uml.org`) oder in diversen UML-Tutorials im Internet. Nach den UML-Diagrammen ist jeweils noch eine Tabelle mit einer Kurzbeschreibung der einzelnen Funktionen zu finden. Implementierungen der Funktionen sind im Abschnitt 4.4 zu finden. Einige grundlegende Klassen und Funktionen (zum Beispiel Matrizen, Listen und Polynome) werden hier nicht beschrieben, da sie üblicherweise schon implementiert sind und größtenteils auch nicht besonders interessant sind.

4.2.1 Zahlkörper



Funktionsname	Beschreibung
NumberField(ν)	Konstruktor des Zahlkörpers $\mathbb{Q}[\alpha]$, wobei α die Nullstelle des normierten, irreduziblen Polynoms μ ist.
this.degree()	Gibt den Grad des erzeugenden Polynoms _poly und somit den Grad des Zahlkörpers zurück.
this.generator()	Gibt das erzeugende Element des Zahlkörpers zurück, das heißt die Nullstelle des erzeugenden Polynoms _poly.
this.maximal_order()	Berechnet die Maximalordnung des Zahlkörpers (zum Beispiel mit Algorithmus 4.3.11) und gibt sie zurück.
this.polynomial()	Gibt das erzeugende Polynom _poly des Zahlkörpers zurück.
this.standard_basis()	Gibt [1, α, α^2, ..., α^{n-1}] zurück, wobei α := this.generator() und n := this.degree() gesetzt wird.

4.2.2 Elemente von Zahlkörpern

NFE

− _number_field: NumberField

NFE(Vector v, NumberField K, List<NFE> B)
+ operator+(NFE x, NFE y) : NFE
+ operator/(NFE a, NFE b) : NFE
+ operator==(NFE x) : bool
+ operator∗(NFE x, NFE y) : NFE
+ operator−() : NFE
+ operator−(NFE x, NFE y) : NFE
+ number_field() : NumberField
+ to_coordinates(List<NFE> B) : Vector

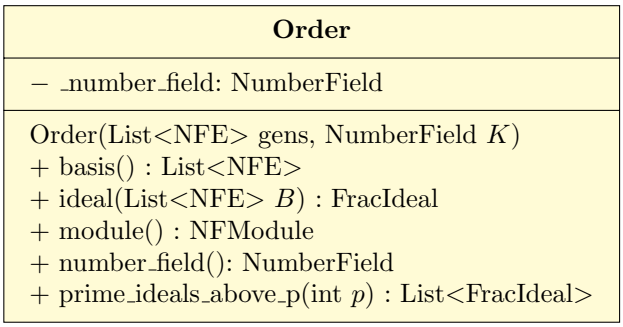
Funktionsname	Beschreibung
NFE(v, K, B)	Konstruktor des Zahlkörperelements, das vom Koordinatenvektor v im Zahlkörper K erzeugt wird (bezüglich der Basis B).
operator+(x, y)	Berechnet die Summe der Zahlkörperelemente x und y und gibt sie zurück.
operator/(a, b)	Berechnet den Quotienten $\frac{a}{b}$ der Zahlkörperelemente a, b und gibt ihn zurück.
this.operator==(x)	Testet, ob die Zahlkörperelemente this und x gleich sind und gibt den entsprechenden Wahrheitswert zurück.
operator∗(x, y)	Berechnet das Produkt der Zahlkörperelemente x und y und gibt es zurück.
this.operator−()	Berechnet das additive Inverse von this und gibt es zurück.
operator−(x, y)	Berechnet die Differenz $x - y$ der Zahlkörperelemente x, y und gibt sie zurück.
this.number_field()	Gibt den Zahlkörper _number_field zurück. Dies ist der Zahlkörper, in dem das Zahlkörperelement erzeugt wurde.
this.to_coordinates(B)	Berechnet die Koordinaten von this bezüglich der Basis B und gibt sie als Vektor zurück.

4.2.3 Moduln

NFModule
− _coord_basis: List<Vector> − _gens: List<NFE> − _number_field: NumberField − _number_field_basis: List<NFE>
NFModule(List<NFE> gens, NumberField K) + operator+(NFModule $\mathfrak{m}_1$, NFModule $\mathfrak{m}_2$) : NFModule + operator∋(NFE x) : bool + operator==(NFModule $\mathfrak{m}$) : bool + operator∗(NFModule $\mathfrak{m}_1$, NFModule $\mathfrak{m}_2$) : NFModule + coord_basis() : List<Vector> + discriminant() : int + factor_module(NFModule $\mathfrak{m}_1$, NFModule $\mathfrak{m}_2$) : List<Ring> + get_extended_basis() : List<NFE> + includes(NFModule $\mathfrak{m}$) : bool + index(NFModule $\mathfrak{m}_1$, NFModule $\mathfrak{m}_2$) : int + intersection(NFModule $\mathfrak{m}_1$, NFModule $\mathfrak{m}_2$) : NFModule + is_fract_ideal(Order $\mathcal{O}$) : bool + is_full() : bool + module_inverse(Order $\mathcal{O}$) : NFModule + module_order() : Order + number_field_basis() : List<NFE> + number_field() : NumberField + quotient(NFModule $\mathfrak{m}_1$, NFModule $\mathfrak{m}_2$) : NFModule + rank() : int + scale(int scalar) : NFModule

Funktionsname	Beschreibung
NFModule(gens, K)	Konstruktor des Moduls in K, der von den Elementen in gens erzeugt wird. Die Basis des Moduls sollte entweder hier im Konstruktor oder bei der ersten Benutzung einer der Funktionen this.number_field_basis() oder this.coord_basis() berechnet werden (mit Algorithmus 4.3.3).
operator+($\mathfrak{m}_1$, $\mathfrak{m}_2$)	Berechnet die Summe der Moduln $\mathfrak{m}_1$ und $\mathfrak{m}_2$ und gibt sie zurück.
this.operator$\ni$(x)	Testet, ob das Zahlkörperelement x im Modul this enthalten ist und gibt den entsprechenden Wahrheitswert zurück.
this.operator==($\mathfrak{m}$)	Testet, ob die Moduln this und $\mathfrak{m}$ gleich sind und gibt den entsprechenden Wahrheitswert zurück.
operator$*$($\mathfrak{m}_1$, $\mathfrak{m}_2$)	Berechnet das Produkt der Moduln $\mathfrak{m}_1$ und $\mathfrak{m}_2$ und gibt es zurück.
this.coord_basis()	Gibt die Koordinatenvektoren der Basiselemente des Moduls this bezüglich der Standardbasis des Zahlkörpers zurück.
this.discriminant()	Berechnet die Diskriminante des Moduls this und gibt sie zurück.
factor_module($\mathfrak{m}_1$, $\mathfrak{m}_2$)	Berechnet den Isomorphietyp des Faktormoduls $\mathfrak{m}_1/\mathfrak{m}_2$ mit Algorithmus 4.3.5 und gibt eine Liste der Faktoren im kartesischen Produkt zurück.
this.get_extended_basis()	Erweitert die Basis des Moduls zu einer $\mathbb{Q}$-Basis des Zahlkörpers und gibt diese erweiterte Basis zurück. In der neuen Basis sind alle Elemente der alten Basis (bis auf Reihenfolge) unverändert enthalten.
this.includes($\mathfrak{m}$)	Testet, ob der Modul $\mathfrak{m}$ im Modul this enthalten ist und gibt den entsprechenden Wahrheitswert zurück.
index($\mathfrak{m}_1$, $\mathfrak{m}_2$)	Berechnet den Index des Faktormoduls $\mathfrak{m}_1/\mathfrak{m}_2$ und gibt ihn zurück.
intersection($\mathfrak{m}_1$, $\mathfrak{m}_2$)	Berechnet den Schnitt der Moduln $\mathfrak{m}_1$ und $\mathfrak{m}_2$ mit Algorithmus 4.3.4 und gibt ihn zurück.
this.is_fract_ideal($\mathcal{O}$)	Testet, ob der Modul ein gebrochenes Ideal der Ordnung $\mathcal{O}$ ist und gibt den entsprechenden Wahrheitswert zurück.
this.is_full()	Testet, ob der Modul vollständig ist und gibt den entsprechenden Wahrheitswert zurück.
this.module_inverse($\mathcal{O}$)	Berechnet den Quotienten $\mathcal{O}$%this und gibt ihn zurück.
this.module_order()	Berechnet die Ordnung des Moduls this und gibt sie zurück. Die Ordnung ist gegeben durch den Quotienten this%this.
this.number_field_basis()	Gibt die (durch die Hermite-Normalform eindeutig gemachte) Basis des Moduls als Liste von Zahlkörperelementen zurück.
this.number_field()	Gibt den bei der Konstruktion des Moduls gesetzten Zahlkörper _number_field zurück.
quotient($\mathfrak{m}_1$, $\mathfrak{m}_2$)	Berechnet den Quotienten $\mathfrak{m}_1$%$\mathfrak{m}_2$ der Moduln $\mathfrak{m}_1$ und $\mathfrak{m}_2$ mit Algorithmus 4.3.6 und gibt ihn zurück.
this.rank()	Gibt den Rang des Moduls this zurück. Dieser ist gegeben durch die Anzahl der Elemente der Basis des Moduls.
this.scale(int scalar)	Gibt den Modul zurück, der das scalar-fache des Moduls this ist.

4.2.4 Ordnungen



Funktionsname	Beschreibung
Order(gens, K)	Konstruktor der Ordnung in K, die von den Zahlkörperelementen in gens erzeugt wird.
this.basis()	Gibt die $\mathbb{Z}$-Basis der Ordnung this zurück.
this.ideal(B)	Gibt das gebrochene Ideal der Ordnung this zurück, das von den Zahlkörperelementen in B erzeugt wird.
this.module()	Gibt einen Modul in _number_field zurück, der der Ordnung this entspricht. Alternativ kann man auch die Klasse Order von der Klasse NFModule erben lassen, dann wird diese Funktion nicht benötigt.
this.number_field()	Gibt den Zahlkörper _number_field zurück in dem die Ordnung konstruiert wurde.
this.prime_ideals_above_p(p)	Berechnet mit Algorithmus 4.3.8 die Primideale über der Primzahl p und gibt diese zurück.

4.2.5 Ideale

FracIdeal
− _gens: List<NFE> − _order: Order
FracIdeal(List<NFE> gens, Order $\mathcal{O}$) + operator+(FracIdeal $\mathfrak{a}_1$, FracIdeal $\mathfrak{a}_2$) : FracIdeal + operator∋(NFE x) : bool + operator==(FracIdeal $\mathfrak{a}$) : bool + operator∗(FracIdeal $\mathfrak{a}_1$, FracIdeal $\mathfrak{a}_2$) : FracIdeal + coord_basis() : List<Vector> + coprime(FracIdeal $\mathfrak{a}_1$, FracIdeal $\mathfrak{a}_2$) : bool + factor() : List<(FracIdeal, int)> + generators() : List<NFE> + includes(FracIdeal $\mathfrak{a}$) : bool + inverse() : FracIdeal + is_integral() : bool + is_invertible() : bool + module() : NFModule + number_field() : NumberField + number_field_basis() : List<NFE> + order() : Order + pseudo_inverse() : FracIdeal + scale(int scalar) : FracIdeal + valuation(FracIdeal $\mathfrak{a}$) : int, FracIdeal

Funktionsname	Beschreibung
FracIdeal(gens, $\mathcal{O}$)	Konstruktor des gebrochenen Ideals von $\mathcal{O}$, das von den Elementen gens erzeugt wird.
operator+($\mathfrak{a}_1$, $\mathfrak{a}_2$)	Berechnet die Summe der gebrochenen Ideale $\mathfrak{a}_1$ und $\mathfrak{a}_2$ und gibt sie zurück.
this.operator$\ni(x)$	Testet, ob das Zahlkörperelement x im gebrochenen Ideal this enthalten ist und gibt den entsprechenden Wahrheitswert zurück.
this.operator==($\mathfrak{a}$)	Testet, ob die beiden gebrochenen Ideale this und $\mathfrak{a}$ gleich sind und gibt den entsprechenden Wahrheitswert zurück.
operator*($\mathfrak{a}_1$, $\mathfrak{a}_2$)	Berechnet das Produkt der gebrochenen Ideale $\mathfrak{a}_1$ und $\mathfrak{a}_2$ und gibt es zurück.
this.coord_basis()	Gibt this.module().coord_basis() zurück.
coprime($\mathfrak{a}_1$, $\mathfrak{a}_2$)	Testet, ob die beiden gebrochenen Ideale teilerfremd sind und gibt den entsprechenden Wahrheitswert zurück.
this.factor()	Zerlegt das gebrochene Ideal mit Algorithmus 4.3.10 in ein Produkt von invertierbaren Primidealen und einen Rest, der in keinem invertierbaren Primideal enthalten ist. Gibt eine Liste mit den Faktoren und dazugehörigen Exponenten zurück. Das erste Element der Liste sollte der Rest mit Exponent 1 sein.
this.generators()	Gibt _gens zurück. Dies ist das bei der Konstruktion des gebrochenen Ideals angegebene $\mathcal{O}$-Erzeugendensystem von this, wobei $\mathcal{O}$ die Ordnung von this ist.
this.includes($\mathfrak{a}$)	Testet, ob das gebrochene Ideal $\mathfrak{a}$ in this enthalten ist und gibt den entsprechenden Wahrheitswert zurück.
this.inverse()	Berechnet das Inverse des gebrochenen Ideals this und gibt es zurück (falls es existiert).
this.is_integral()	Testet, ob das gebrochene Ideal this ein ganzzahliges Ideal seiner Ordnung ist und gibt den entsprechenden Wahrheitswert zurück.
this.is_invertible()	Testet, ob das gebrochene Ideal this invertierbar in seiner Ordnung ist und gibt den entsprechenden Wahrheitswert zurück.
this.module()	Gibt einen Modul im Zahlkörper this.number_field() zurück, der dem gebrochenen Ideal this entspricht. Alternativ kann man auch die Klasse FracIdeal von der Klasse NFModule erben lassen, dann wird diese Funktion nicht benötigt.
this.number_field()	Gibt den Zahlkörper this.order().number_field() zurück.
this.number_field_basis()	Gibt this.module().number_field_basis() zurück.
this.order()	Gibt die Ordnung zurück, mit der das gebrochene Ideal this erzeugt wurde.
this.pseudo_inverse()	Berechnet das gebrochene Ideal this.order()%this und gibt es zurück. Dieses Ideal entspricht dem Inversen von this, falls this invertierbar ist.
this.scale(x)	Gibt das gebrochene Ideal zurück, das das scalar-fache des gebrochenen Ideals this ist.
this.valuation($\mathfrak{a}$)	Berechnet die Bewertung des ganzzahligen Ideals this bezüglich des invertierbaren Primideals $\mathfrak{a}$ und gibt die Bewertung und den nicht in $\mathfrak{a}$ enthaltenen Rest zurück (vergleiche Algorithmus 4.3.9). Diese Funktion kann auch auf gebrochene Ideale this und invertierbare gebrochene Ideale $\mathfrak{a}$ erweitert werden (dies wird in Bemerkung 4.3.5 näher erläutert).

4.3 Beschreibung der Algorithmen

In diesem Abschnitt werden mehrere Algorithmen beschrieben und bewiesen, die für das Rechnen in Zahlkörpern nützlich oder sogar notwendig sind. Einige von diesen Algorithmen werden dann im Abschnitt 4.4 implementiert. Jeder Algorithmus wird durch eine Reihe von Schritten beschrieben,

die nacheinander ausgeführt werden. Wird in einem Schritt verlangt, zu einem anderen Schritt zu gehen, so geht der Algorithmus ab diesem Zeitpunkt vom neuen Schritt normal weiter. Eine mögliche Abfolge von Schritten sieht also beispielsweise so aus:

$$1, 2, 3, 4 : \text{gehe zu}(1), 1, 2, 3 : \text{gehe zu}(8), 8, 9.$$

Die einzelnen Schritte sind dabei in Textform/Pseudocode geschrieben. Die Beweise der Algorithmen verwenden die Sätze, die in den vorherigen Kapiteln vorgestellt wurden und verweisen an den entsprechenden Stellen auf die Satznummern.

4.3.1 Matrixalgorithmen

Die Hermite-Normalform und die Smith-Normalform sind in Sage bereits implementiert und werden deshalb nicht in Abschnitt 4.4 implementiert. Dafür werden die beiden Algorithmen in diesem Abschnitt jeweils an einem Beispiel veranschaulicht. Im Folgenden seien die betrachteten Matrizen immer Matrizen mit Koeffizienten in $\mathbb{Z}$ und die euklidische Norm von $\mathbb{Z}$ die übliche Betragsnorm. Außerdem seien die Repräsentantensysteme definiert durch $\text{Rep}(\mathbb{Z}) := \mathbb{N}_0$ und $\text{Rep}(\mathbb{Z}/(a)_{\mathbb{Z}}) := \{0, \ldots, |a| - 1\}$ für alle $a \in \mathbb{Z}$. Die Integerdivision a div b sei so definiert, dass a div $b = q$ genau dann gilt, wenn $a = b*q+r$ für ein $r \in \{0, \ldots, |b| - 1\}$ gilt. Für andere euklidische Ringe lassen sich die Algorithmen leicht anpassen, solange man eine Möglichkeit hat, die Division mit Rest durch einen endlichen Algorithmus zu berechnen.

Hermite-Normalform

Algorithmus 4.3.1. Der folgende Algorithmus bestimmt die Hermite-Normalform einer $m \times n$-Matrix $A = \{a_{ij}\}$. Dabei wird A zur Hermite-Normalform geändert. Der Wert i sei mit 0 initialisiert.

1. Setze $i := i + 1$.

2. Sind alle Zeilen i, $i + 1$, …, m Nullzeilen oder $i = m + 1$, so setze $r := i - 1$ und gehe zu Schritt 7. Ansonsten setze

$$s_i := \min\left\{j \in \{1, \ldots, n\} \mid \ \exists\, i' \geq i : a_{i'j} \neq 0\right\}$$

   und fahre fort mit Schritt 3.

3. Setze t gleich dem Zeilenindex eines Elements $a_{i's_i}$ mit kleinster Norm, wobei i' die Menge $\{i, \ldots, m\}$ durchläuft. Bei mehreren Elementen mit gleicher Norm kann ein beliebiges ausgewählt werden (beispielsweise immer das mit dem kleinsten/größten Zeilenindex).

4. Vertausche die Zeilen i und t.

5. Für jedes k in $\{i+1,\dots,m\}$ berechne $q := a_{ks_i}$ div a_{is_i} (Integerdivision in $\mathbb{Z}$) und ziehe das q-fache der Zeile i von der Zeile k ab.

6. Teste, ob alle Elemente $a_{i's_i}$ gleich 0 sind für $i' \in \{i+1,\dots,m\}$. Sind alle Elemente gleich 0, so gehe zu Schritt 1. Ansonsten gehe zurück zu Schritt 3.

7. Für jedes $i \in \{1,\dots,r\}$ multipliziere Zeile i mit -1, falls a_{is_i} negativ ist.

8. Für jedes $i \in \{1,\dots,r\}$ und jedes $k \in \{1,\dots,i-1\}$ berechne die Integerdivision $q := a_{ks_i}$ div a_{is_i} und ziehe das q-fache der Zeile i von der Zeile k ab.

9. Gib die Matrix A zurück.

Beweis. Dieser Algorithmus ist eine Möglichkeit das Verfahren auszuführen, das im Beweis der Existenz der Hermite-Normalform in Theorem 2.7.12 beschrieben wurde. Für ein besseres Verständnis des Algorithmus folgt gleich noch das Anwendungsbeispiel 4.3.2. □

Bemerkung 4.3.1. *Falls die Matrix A Koeffizienten in $\mathbb{Q}$ statt in $\mathbb{Z}$ hat, so kann man die Matrix zunächst mit dem Hauptnenner d der Koeffizienten multiplizieren (das heißt jedes Element der Matrix mit d multiplizieren) und dann die Hermite-Normalform bilden. Danach muss man jedoch die Ergebnismatrix noch mit $\frac{1}{d}$ multiplizieren. Dies entspricht der Berechnung der Hermite-Normalform mit Koeffizienten im Euklidischen Ring $\frac{1}{d} * \mathbb{Z}$ mit Einselement $\frac{1}{d}$ und Normfunktion $d * |\cdot|$. Bei Erzeugermatrizen von Moduln entspricht dieses Vorgehen einem Basiswechsel im Vektorraum, der die Koordinaten nach $\mathbb{Z}^n$ bringt und nach der Berechnung der Hermite-Normalform einem erneuten Basiswechsel in die ursprüngliche Basis.*

Beispiel 4.3.2. In diesem Beispiel wird die Anwendung von Algorithmus 4.3.1 auf die Matrix

$$A = \begin{pmatrix} 0 & 7 & -6 & -9 \\ 0 & -2 & 1 & 2 \\ 0 & 5 & 5 & 1 \end{pmatrix}$$

erklärt. Zunächst wird in Schritt 1 die Zeile $i = 1$ ausgewählt. In Schritt 2 wird $s_1 = 2$ gesetzt, da in der ersten Spalte nur Nullen auftreten.

$$\begin{array}{c} \overset{s_1}{\overbrace{\phantom{\begin{pmatrix} 0 & 7 & -6 & -9 \end{pmatrix}}}} \\ \left(\begin{array}{c|c|cc} 0 & 7 & -6 & -9 \\ 0 & -2 & 1 & 2 \\ 0 & 5 & 5 & 1 \end{array}\right) \end{array} \quad i$$

In Schritt 3 wird $t = 2$ gesetzt, da in Spalte s_1 das Element -2 die kleinste Norm (in diesem Fall die normale Betragsnorm von $\mathbb{Z}$) hat und dieses

Element in Zeile 2 steht.

$$\begin{array}{c} \overset{s_1}{\overbrace{\phantom{\begin{pmatrix}0\end{pmatrix}}}} \\ \left(\begin{array}{c|cc} 0 & 7 & -6 & -9 \\ 0 & \textcircled{-2} & 1 & 2 \\ 0 & 5 & 5 & 1 \end{array}\right) \end{array} \begin{array}{l} i \\ t \end{array}$$

Nun werden in Schritt 4 die Zeilen i und t vertauscht.

$$\begin{array}{c} \overset{s_1}{\overbrace{\phantom{\begin{pmatrix}0\end{pmatrix}}}} \\ \left(\begin{array}{c|cc} 0 & -2 & 1 & 2 \\ 0 & 7 & -6 & -9 \\ 0 & 5 & 5 & 1 \end{array}\right) \end{array} \begin{array}{l} i \end{array}$$

In Schritt 5 werden die Zeilen $i+1, \ldots, m$ so verändert, dass in Spalte s_i unterhalb von Zeile i die Reste der Division durch $a_{is_i} = -2$ stehen. Dafür berechnet man die Integerdivisionen

$$\begin{aligned} a_{i+1,s_i} \text{ div } a_{is_i} &= 7 \text{ div } -2 = -3 \\ a_{m,s_i} \text{ div } a_{is_i} &= 5 \text{ div } -2 = -2 \end{aligned}$$

und zieht das entsprechende Vielfache der i-ten Zeile von der dazugehörigen Zeile ab.

$$\begin{array}{c} \overset{s_1}{\overbrace{\phantom{\begin{pmatrix}0\end{pmatrix}}}} \\ \left(\begin{array}{c|cc} 0 & -2 & 1 & 2 \\ 0 & 1 & -3 & -3 \\ 0 & 1 & 7 & 5 \end{array}\right) \end{array} \begin{array}{l} i \end{array}$$

In Schritt 6 wird nun getestet, ob die Reste alle 0 geworden sind. In diesem Fall sind die Reste aber jeweils 1. Somit geht der Algorithmus wieder zu Schritt 3 und wählt wieder ein Element minimaler Norm. In diesem Fall gibt es zwei solche Elemente: $a_{i+1,s_1} = a_{22} = 1$ und $a_{ms_1} = a_{32} = 1$. Für dieses Beispiel wird angenommen, dass der Algorithmus immer das erste solche Element wählt. Es wird also $t = 2$ gesetzt.

$$\begin{array}{c} \overset{s_1}{\overbrace{\phantom{\begin{pmatrix}0\end{pmatrix}}}} \\ \left(\begin{array}{c|cc} 0 & -2 & 1 & 2 \\ 0 & \textcircled{1} & -3 & -3 \\ 0 & 1 & 7 & 5 \end{array}\right) \end{array} \begin{array}{l} i \\ t \end{array}$$

Nach der Vertauschung der Zeilen (Schritt 4) und der Resteberechnung (Schritt 5) ergibt sich dann folgende Matrix:

$$\begin{array}{c} \overset{s_1}{\overbrace{\phantom{\begin{pmatrix}0\end{pmatrix}}}} \\ \left(\begin{array}{c|cc} 0 & 1 & -3 & -3 \\ 0 & 0 & -5 & -4 \\ 0 & 0 & 10 & 8 \end{array}\right) \end{array} \begin{array}{l} i \end{array}$$

Diesmal sind alle Reste 0, also geht man wieder zurück zu Schritt 1 und setzt $i = 2$. In Schritt 2 wird dann $s_2 = 3$ gesetzt, da in den Zeilen $i = 2$ und $i + 1 = m = 3$ die ersten Elemente ungleich 0 in der Spalte 3 auftauchen.

$$\begin{array}{c} \\ \left(\begin{array}{cc|c|c} 0 & 1 & -3 & -3 \\ \hline 0 & 0 & -5 & -4 \\ 0 & 0 & 10 & 8 \end{array}\right) \end{array} \begin{array}{c} s_2 \\ \\ i \end{array}$$

Das Element mit kleinster Norm (in den Zeilen $\geq i$) ist nun die -5. Es wird also $t = 2$ in Schritt 3 gesetzt. Da aber i ebenfalls gleich 2 ist, passiert beim Zeilen vertauschen in Schritt 4 nichts, da die Zeile mit sich selbst getauscht wird. Durch die Resteberechnung in Schritt 5 ergibt sich dann folgende Matrix:

$$\begin{array}{c} \\ \left(\begin{array}{cc|c|c} 0 & 1 & -3 & -3 \\ \hline 0 & 0 & -5 & -4 \\ 0 & 0 & 0 & 0 \end{array}\right) \end{array} \begin{array}{c} s_2 \\ \\ i \end{array}$$

Die Reste sind hier alle 0, also geht man von Schritt 6 zurück zu Schritt 1 und setzt $i = 3$. In Schritt 2 stellt man fest, dass nun alle Zeilen $\geq i$ Nullzeilen sind, also geht man zu Schritt 7. Dort werden die Spaltenelemente in das Repräsentantensystem $\mathbb{N}_0$ von $\mathbb{Z}$ gebracht, indem man alle Zeilen i mit negativem Spaltenelement a_{is_i} mit der Einheit -1 multipliziert, also in diesem Fall nur die Zeile 2.

$$\begin{pmatrix} 0 & 1 & -3 & -3 \\ 0 & 0 & 5 & 4 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

Nun müssen in Schritt 8 noch die restlichen Elemente der Stufenspalten normiert werden. Dies geschieht wieder mit Hilfe der Integerdivision. An dieser Stelle ist es wichtig, dass die Integerdivision so definiert wurde, dass der Rest $a - (a \text{ div } b) * b$ in $\{0, \ldots, |b| - 1\}$ liegt, da dies das gewählte Repräsentantensystem für $\mathbb{Z}/(b)_{\mathbb{Z}}$ ist. Da die Spalte s_1 keine Elemente über dem Spaltenelement hat, muss nur die Spalte s_2 normiert werden. Nach diesem Schritt hat man die Matrix

$$\begin{array}{c} \\ \left(\begin{array}{cccc} 0 & 1 & 2 & 1 \\ 0 & 0 & 5 & 4 \\ 0 & 0 & 0 & 0 \end{array}\right) \end{array} \begin{array}{c} s_1 \quad s_2 \\ \\ \\ \end{array}$$

und diese ist die Hermite-Normalform von A.

Smith-Normalform

Algorithmus 4.3.2. Der folgende Algorithmus bestimmt die Smith-Normalform einer $m \times n$-Matrix $A = \{a_{ij}\}$. Dabei wird A zur Smith-Normalform geändert. Zu Beginn des Algorithmus sei $s = 0$.

1. Setze $s := s + 1$. Ist $s > \min\{m, n\}$, so gib die (veränderte) Matrix A als Smith-Normalform zurück.

2. Falls die Spalte s eine Nullspalte ist und die Zeile s eine Nullzeile ist, gehe zurück zu Schritt 1. Falls nur die Zeile s eine Nullzeile ist, überspringe Schritt 3.

3. Bestimme die Normen der Elemente $a_{ss}, \ldots, a_{sn}$ in der Zeile s und setze j gleich dem Spaltenindex des Elements mit der kleinsten Norm ungleich 0. Vertausche die Spalten s und j.

4. Bestimme die Normen der Elemente $a_{ss}, \ldots, a_{ms}$ in der Spalte s und setze i gleich dem Zeilenindex des Elements mit der kleinsten Norm ungleich 0. Vertausche die Zeilen s und i.

5. Wiederhole die Schritte 3 und 4 bis a_{ss} sowohl in der Zeile s als auch in der Spalte s das Element mit der kleinsten Norm ungleich 0 ist.

6. Gehe die Spaltenindizes $j > s$ durch. Berechne die Integerdivisionen $q_j := a_{sj} \operatorname{div} a_{ss}$ und ziehe das q_j-fache der Spalte s von der j-ten Spalte ab. Das Element a_{sj} ist dann entweder gleich 0 oder hat eine kleinere Norm als a_{ss}. Falls alle a_{sj} zu 0 werden, fahre fort mit dem nächsten Schritt, ansonsten gehe zurück zu Schritt 3.

7. Gehe die Zeilenindizes $i > s$ durch. Berechne die Integerdivisionen $q_i := a_{is} \operatorname{div} a_{ss}$ und ziehe das q_i-fache der Zeile s von der i-ten Zeile ab. Das Element a_{is} ist dann entweder gleich 0 oder hat eine kleinere Norm als a_{ss}. Falls alle a_{is} zu 0 werden, fahre fort mit dem nächsten Schritt, ansonsten gehe zurück zu Schritt 4.

8. Ist a_{ss} sowohl in Zeile s als auch in Spalte s das einzige Element ungleich 0, so fahre fort mit Schritt 9. Ansonsten gehe zurück zu Schritt 3.

9. Falls $s = 1$ ist oder $a_{s-1,s-1}$ das Element a_{ss} teilt, gehe zu Schritt 1. Ansonsten füge die Zeile s zur Zeile $s - 1$ hinzu, setze $s := s - 1$ und gehe zu Schritt 3.

Beweis. Der Algorithmus setzt das Verfahren um, das beim Beweis der Existenz der Smith-Normalform in Theorem 2.7.17 verwendet wurde. Für ein besseres Verständnis folgt gleich noch das Anwendungsbeispiel 4.3.4 □

Bemerkung 4.3.3. *Statt den Schritten 2 bis 5 des Algorithmus kann man auch in der Teilmatrix mit den Zeilen s bis m und den Spalten s bis n nach einem Element minimaler Norm (ungleich 0) suchen. Dieses Element kann man dann durch eine Zeilen- und eine Spaltenvertauschung an die Position a_{ss} bringen. In Schritt 6 und Schritt 7 kann man den Schritt auch unterbrechen, sobald eine der Divisionen einen Rest ungleich 0 liefert und sofort zur Vertauschung gehen, ohne alle größeren j zu betrachten. Welche Versionen des Algorithmus effizienter sind, hängt von der Matrix ab. Dies wird jedoch in dieser Arbeit nicht weiter untersucht.*

Beispiel 4.3.4. In diesem Beispiel wird die Anwendung des Algorithmus 4.3.2 auf die Matrix

$$A = \begin{pmatrix} 15 & 5 & 4 & -8 \\ 3 & 1 & 2 & -4 \\ 9 & -3 & 12 & -4 \end{pmatrix}$$

erläutert. Zunächst wird $s = 1$ gesetzt. Dann berechnet man die Normen der Elemente in Zeile $s = 1$ und setzt $j = 3$, da das Element $a_{13} = 4$ die kleinste Norm in der Zeile hat.

$$\begin{array}{c} \begin{array}{cccc} & & s & \\ & & \downarrow & \\ \end{array} \\ \left(\begin{array}{cccc} 15 & 5 & \textcircled{4} & -8 \\ \hline 3 & 1 & 2 & -4 \\ 9 & -3 & 12 & -4 \end{array}\right) \end{array} \begin{array}{c} \\ \\ s \end{array}$$

Dann vertauscht man Spalte 1 und Spalte j und sucht danach in der Spalte $s = 1$ das Element mit der kleinsten Norm, in diesem Fall $a_{23} = 2$. Es wird also $i = 2$ gesetzt, da a_{23} in Zeile 2 ist.

$$\begin{array}{c} \begin{array}{cccc} & s & & \\ & \downarrow & & \\ \end{array} \\ \left(\begin{array}{c|ccc} 4 & 5 & 15 & -8 \\ \textcircled{2} & 1 & 3 & -4 \\ 12 & -3 & 9 & -4 \end{array}\right) \end{array} \begin{array}{c} \\ s \\ i \end{array}$$

Nach dem Vertauschen von Zeile $s = 1$ und Zeile $i = 2$ sucht man erneut in der ersten Zeile nach Elementen minimaler Norm (da sich die erste Zeile durch die Zeilenvertauschung verändert hat). In diesem Fall ist $a_{12} = 1$ das Element mit der kleinsten Norm, also wird $j = 2$ gesetzt.

$$\begin{array}{c} \begin{array}{cccc} & s & j & \\ & \downarrow & \downarrow & \\ \end{array} \\ \left(\begin{array}{cccc} 2 & \textcircled{1} & 3 & -4 \\ \hline 4 & 5 & 15 & -8 \\ 12 & -3 & 9 & -4 \end{array}\right) \end{array} \begin{array}{c} \\ \\ s \end{array}$$

Vertauscht man nun wieder die Spalten $s = 1$ und $j = 2$, so ist $a_{ss} = 1$ sowohl in der Zeile $s = 1$ als auch in der Spalte $s = 1$ das Element mit der kleinsten Norm. Es müssen also zunächst keine weiteren Vertauschungen

vorgenommen werden. Man betrachtet sich als nächstes die Zeile $s = 1$ und geht nacheinander die Spalten $j > s$ durch. Dabei zieht man von der j-ten Spalte das (a_{sj} div a_{ss})-fache der Spalte $s = 1$ von der Spalte j ab.

$$\begin{array}{c} \begin{array}{cccc} s & j & \rightarrow & \end{array} \\ \left(\begin{array}{cccc} 1 & 2 & 3 & -4 \\ \hline 5 & 4 & 15 & -8 \\ -3 & 12 & 9 & -4 \end{array}\right) \end{array} \quad s$$

Da in diesem Fall alle Elemente a_{sj} durch a_{ss} teilbar sind, bekommt man dadurch die folgende Matrix:

$$\begin{array}{c} \begin{array}{cccc} s & & & \end{array} \\ \left(\begin{array}{cccc} 1 & 0 & 0 & 0 \\ \hline 5 & -6 & 0 & 12 \\ -3 & 18 & 0 & -16 \end{array}\right) \end{array} \quad s$$

Da in der Zeile nur Nullen entstanden sind und keine Elemente mit kleinerer Norm, wendet man nun ein analoges Verfahren auf die Spalte $s = 1$ an, indem man dieses mal das (a_{is} div a_{ss})-fache der Zeile $s = 1$ von der Zeile i abzieht, wobei i die Werte $s+1$ bis m durchläuft. Dabei entsteht erneut kein Element mit kleinerer Norm, also sieht die Matrix dann folgendermaßen aus:

$$\begin{array}{c} \begin{array}{cccc} s & & & \end{array} \\ \left(\begin{array}{c|ccc} 1 & 0 & 0 & 0 \\ 0 & -6 & 0 & 12 \\ 0 & 18 & 0 & -16 \end{array}\right) \end{array} \quad s$$

Da nun sowohl in der ersten Spalte als auch in der ersten Zeile das Element a_{11} das einzige Element ungleich 0 ist, setzt man $s = 2$ und sucht wieder in Zeile s nach Elementen mit möglichst kleiner Norm.

$$\begin{array}{c} \begin{array}{cccc} & s & & \end{array} \\ \left(\begin{array}{cccc} 1 & 0 & 0 & 0 \\ \hline 0 & \textcircled{-6} & 0 & 12 \\ \hline 0 & 18 & 0 & -16 \end{array}\right) \end{array} \quad s$$

In diesem Fall ist das Element mit der kleinsten Norm (ungleich 0) schon an der richtigen Stelle (a_{ss}), also müssen keine Spalten vertauscht werden. Ebenso ist es auch in der Spalte $s = 2$:

$$\begin{array}{c} \begin{array}{cccc} & s & & \end{array} \\ \left(\begin{array}{c|c|cc} 1 & 0 & 0 & 0 \\ 0 & \textcircled{-6} & 0 & 12 \\ 0 & 18 & 0 & -16 \end{array}\right) \end{array} \quad s$$

Somit geht man wieder zur Restberechnung über und zieht von der j-ten Spalte das $(a_{sj}$ div $a_{ss})$-fache der Spalte $s = 2$ von der Spalte j ab, wobei j die Werte $s + 1$ bis n durchläuft. Dadurch entsteht die folgende Matrix:

$$\begin{array}{c} \\ \left(\begin{array}{c|ccc} 1 & 0 & 0 & 0 \\ \hline 0 & -6 & 0 & 0 \\ \hline 0 & 18 & 0 & 20 \end{array}\right) \end{array} \begin{array}{c} s \\ \\ s \end{array}$$

Nachdem man auch in der Spalte $s = 2$ den entsprechenden Algorithmus angewendet hat, ergibt sich die Matrix

$$\begin{array}{c} \\ \left(\begin{array}{c|c|cc} 1 & 0 & 0 & 0 \\ 0 & -6 & 0 & 0 \\ 0 & 0 & 0 & 20 \end{array}\right) \end{array} \begin{array}{c} s \\ \\ s \end{array}$$

Nun ist -6 das einzige Element in Zeile $s = 2$ und Spalte $s = 2$, das ungleich 0 ist. Außerdem teilt $a_{s-1,s-1} = 1$ das Element $a_{ss} = -6$. Somit kann s wieder um 1 erhöht werden.

$$\begin{array}{c} \\ \left(\begin{array}{cccc} 1 & 0 & 0 & 0 \\ 0 & -6 & 0 & 0 \\ 0 & 0 & 0 & 20 \end{array}\right) \end{array} \begin{array}{c} s \\ \\ s \end{array}$$

An dieser Stelle wird wieder eine Zeilenvertauschung vorgenommen, da 20 die kleinste Norm ungleich 0 in der Zeile $s = 3$ hat.

$$\begin{array}{c} \\ \left(\begin{array}{cccc} 1 & 0 & 0 & 0 \\ 0 & -6 & 0 & 0 \\ \hline 0 & 0 & 20 & 0 \end{array}\right) \end{array} \begin{array}{c} s \\ \\ s \end{array}$$

Nun ist 20 wieder das Element mit der kleinsten Norm ungleich 0 in Zeile und Spalte $s = 3$. Dieses Mal teilt aber $a_{s-1,s-1}$ nicht das Element $a_{ss} = 20$. Man fügt deswegen die Zeile s zur Zeile $s - 1$ hinzu, erniedrigt s um 1 und geht wieder zu den Vertauschungen über.

$$\begin{array}{c} \\ \left(\begin{array}{cccc} 1 & 0 & 0 & 0 \\ \hline 0 & -6 & 20 & 0 \\ \hline 0 & 0 & 20 & 0 \end{array}\right) \end{array} \begin{array}{c} s \\ \\ s \end{array}$$

In diesem Fall sind keine Vertauschungen nötig und man kann direkt zur Restberechnung in Zeile $s = 2$ übergehen:

$$\begin{array}{c} \\ \left(\begin{array}{cccc} 1 & 0 & 0 & 0 \\ \hline 0 & -6 & 2 & 0 \\ \hline 0 & 0 & 20 & 0 \end{array}\right) \end{array} \begin{array}{c} s \\ \\ s \end{array}$$

Da 20 nicht durch -6 teilbar war, entsteht dieses Mal ein Element mit kleinerer Norm. Deshalb geht man nun wieder zu den Vertauschungen und vertauscht Zeile 3 mit Zeile 2:

$$\begin{array}{c} \\ \left(\begin{array}{c|ccc} 1 & 0 & 0 & 0 \\ \hline 0 & 2 & -6 & 0 \\ \hline 0 & 20 & 0 & 0 \end{array}\right) \end{array} \begin{array}{c} s \\ \\ s \end{array}$$

Nun kann man wieder die Reste in der Zeile s und danach auch die Reste in der Spalte s berechnen und erhält folgende Matrix:

$$\begin{array}{c} \\ \left(\begin{array}{c|ccc} 1 & 0 & 0 & 0 \\ \hline 0 & 2 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 \end{array}\right) \end{array} \begin{array}{c} s \\ \\ s \end{array}$$

Da 2 nun das einzige Element ungleich 0 in Zeile $s = 2$ und Spalte $s = 2$ ist und $a_{s-1,s-1} = 1$ das Element $a_{ss} = 2$ teilt, kann man s wieder um 1 erhöhen. Dieses Mal haben dann aber alle Elemente in Zeile und Spalte $s = 3$ den Wert 0, also kann s gleich wieder um 1 erhöht werden. Dann ist aber $s = 4 > 3 = \min\{m, n\}$ und somit wird die Matrix

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

als Smith-Normalform zurückgegeben.

4.3.2 Modulalgorithmen

Basisberechnung/Normalisierung

Algorithmus 4.3.3. Der folgende Algorithmus berechnet eine $\mathbb{Z}$-Basis für den Modul $\mathfrak{m}$ im Zahlkörper K mit $(K : \mathbb{Q}) = n$. Dabei hängt die Basis nur vom Modul $\mathfrak{m}$ ab und nicht vom Erzeugendensystem von $\mathfrak{m}$, das im Algorithmus verwendet wird.

1. Setze $G := \mathfrak{m}$.generators()
2. Berechne die Koordinatenvektoren $v_1, \ldots, v_{|G|}$ von den Erzeugern in G bezüglich einer Basis B von K und schreibe sie als Zeilen in eine Matrix M.
3. Berechne den Hauptnenner d der Matrix und setze $\tilde{M} := d * M$.
4. Berechne die Hermite-Normalform $\tilde{N}$ von $\tilde{M}$ und setze $N := \frac{1}{d} * \tilde{N}$.

5. Setze die Koordinatenvektoren $\tilde{v}_1, \ldots, \tilde{v}_{\mathrm{rg}(N)}$ gleich den nicht-Nullzeilen von N.

6. Berechne die Elemente $b_1, \ldots, b_{\mathrm{rg}(N)}$ in K, die den Koordinatenvektoren $\tilde{v}_1, \ldots, \tilde{v}_{\mathrm{rg}(N)}$ bezüglich der Basis B von K entsprechen.

7. Gib die Basis $\left\{b_1, \ldots, b_{\mathrm{rg}(N)}\right\}$ von $\mathfrak{m}$ zurück.

Beweis. Die Koordinatenabbildung $\phi_B : K \to \mathbb{Q}^n$ ist ein Isomorphismus. Somit erhält man durch ϕ_B eine Bijektion von $\mathbb{Z}$-Moduln in K und $\mathbb{Z}$-Moduln in $\mathbb{Q}^n$. Man kann also mit dem entsprechenden Modul im Koordinatensystem arbeiten, der von den Koordinatenvektoren $v_1, \ldots, v_{|G|}$ erzeugt wird. Falls die Erzeugermatrix nicht nur Koeffizienten in $\mathbb{Z}$ hat, muss man zunächst die Basis so verändern, dass die Koordinaten in $\mathbb{Z}$ sind (da nur für euklidische Ringe die Hermite-Normalform definiert wurde). Dafür kann man einfach die $\frac{1}{d}$-fache Basis nehmen, wodurch die Matrix in der neuen Basis das d-fache der alten Matrix ist und somit Koeffizienten in $\mathbb{Z}$ hat. Man kann nun die Hermite-Normalform $\tilde{N}$ der Matrix $\tilde{M}$ bilden und da die Koeffizienten der Matrix in $\mathbb{Z}$ sind, erzeugen die Zeilen von $\tilde{N}$ den gleichen $\mathbb{Z}$-Modul wie die Zeilen von $\tilde{M}$. Da die Hermite-Normalform in Zeilenstufenform ist, gilt nach Lemma 2.7.9 sogar, dass die nicht-Nullzeilen von $\tilde{N}$ eine $\mathbb{Z}$-Basis vom Modul im Koordinatensystem bezüglich der $\frac{1}{d}$-fachen Basis bilden. Um wieder in die ursprüngliche Basis B zu kommen, multipliziert man die Matrix noch mit $\frac{1}{d}$. Nun kann man die nicht-Nullzeilen mit ϕ_B^{-1} wieder zu Elementen im Zahlkörper umwandeln und erhält dadurch eine Basis von $\mathfrak{m}$. Da die Hermite-Normalform nur vom Modul abhängt und nicht vom Erzeugendensystem, hängt auch die berechnete Basis nur vom Modul ab. □

Schnitt von Moduln

Algorithmus 4.3.4. Der folgende Algorithmus berechnet den Schnitt von zwei Moduln $\mathfrak{m}_1, \mathfrak{m}_2$ im Zahlkörper K mit $(K : \mathbb{Q}) = n$.

1. Setze $G_1 := \mathfrak{m}_1$.generators(), $G_2 := \mathfrak{m}_2$.generators().

2. Wähle eine Basis B von K und berechne die Koordinatenvektoren $v_1, \ldots, v_{|G_1|}$ von den Elementen in G_1 und die Koordinatenvektoren $w_1, \ldots, w_{|G_2|}$ von den Elementen in G_2.

3. Schreibe die Vektoren $v_1, \ldots, v_{|G_1|}$ als Zeilen in eine $|G_1| \times n$ Matrix M_1 und die Vektoren $w_1, \ldots, w_{|G_2|}$ als Zeilen in eine $|G_2| \times n$-Matrix M_2.

4. Bilde die $(|G_1| + |G_2|) \times (n + n)$-Matrix

$$M_3 := \begin{pmatrix} M_1 & M_1 \\ M_2 & 0 \end{pmatrix}$$

5. Berechne den Hauptnenner d von M_3, setze $\tilde{M_3} := d * M_3$, berechne die Hermite-Normalform $\tilde{N}$ von $\tilde{M_3}$ und setze $N := \frac{1}{d} * \tilde{N}$.

6. Setze $i_0 := \min\{i \in \{1, \ldots, |G_1| + |G_2|\} \mid s_i(N) > n\}$ und teile die Matrix N vor Zeile i_0 und nach Spalte n. Benenne die entstehenden Matrizen folgendermaßen:

$$N =: \begin{pmatrix} X & Y \\ 0 & Z \end{pmatrix}$$

7. Setze $z_1, \ldots, z_{n-i_0+1}$ gleich den Zeilen von Z. Berechne die Elemente $c_1, \ldots, c_{n-i_0+1}$ in K, die den Koordinatenvektoren z_i bezüglich der Basis B entsprechen.

8. Gib den Modul zurück, der von $c_1, \ldots, c_{n-i_0+1}$ erzeugt wird.

Beweis. Zur Vereinfachung der Darstellung wird angenommen, dass $d = 1$ ist, also eine Basis B gewählt wurde, so dass die Koordinatenvektoren der Erzeuger in $\mathbb{Z}^n$ sind (vergleiche dazu auch den Beweis von Algorithmus 4.3.3). Dann gilt $M_3 = \tilde{M_3}$, $N = \tilde{N}$ und für die Koordinatenabbildung $\phi_B : K \to \mathbb{Q}^n$ bezüglich B gilt $\phi_B(\mathfrak{m}_i) \subset \mathbb{Z}^n$. Die Zeilen von M_3 sind dann nach Konstruktion von M_3 entweder von der Form

$$(\phi_B(m_1), \phi_B(m_1)) \in \mathbb{Z}^n \times \mathbb{Z}^n, m_1 \in M_1$$

oder von der Form

$$(\phi_B(m_2), 0_{\mathbb{Z}^n}) \in \mathbb{Z}^n \times \mathbb{Z}^n, m_2 \in M_2.$$

Da die Hermite-Normalform durch elementare Zeilenumformungen gebildet wird, ist jede Zeile $(0_{\mathbb{Z}^n}, z_i)$ in N eine $\mathbb{Z}$-Linearkombination von den Zeilen von M_3. Somit gilt für geeignete Elemente $a_1, \ldots, a_{|G_1|}, b_1, \ldots, b_{|G_2|} \in \mathbb{Z}$ die Gleichung

$$(0_{\mathbb{Z}^n}, z_i) = \sum_{k=1}^{|G_1|} a_k * (v_i, v_i) + \sum_{k=1}^{|G_2|} b_k * (w_i, 0_{\mathbb{Z}^n}).$$

Spaltet man diese Gleichung von Vektoren der Länge $2 * n$ in zwei Gleichungen von Vektoren der Länge n auf, so ergibt sich

$$z_i = \sum_{k=1}^{|G_1|} a_k * v_i = -\sum_{k=1}^{|G_2|} b_k * w_i.$$

Damit sind die z_i sowohl $\mathbb{Z}$-Linearkombinationen von den v_i als auch von den w_i. Also ist der von den z_i erzeugte Modul ein Teilmodul vom Modul $\phi_B(\mathfrak{m}_1 \cap \mathfrak{m}_2)$. Es bleibt noch zu zeigen, dass die umgekehrte Richtung gilt, das heißt, dass jedes Element vom Modul $\phi_B(\mathfrak{m}_1 \cap \mathfrak{m}_2)$ eine $\mathbb{Z}$-Linearkombination

von den Vektoren z_i ist. Sei also nun u die Koordinatendarstellung eines Elements in $\mathfrak{m}_1 \cap \mathfrak{m}_2$. Dann gibt es $a_1, \ldots, a_{|G_1|}, b_1, \ldots, b_{|G_2|}$ mit

$$\sum_{k=1}^{|G_1|} a_k * v_k = u = \sum_{k=1}^{|G_2|} b_k * w_k$$

Die Zeilen von M_3 erzeugen nach der Konstruktion von M_3 den Modul

$$\mathfrak{m}_3 := \{(\phi_B(m), \phi_B(m)) \in \mathbb{Z}^n \times \mathbb{Z}^n \mid m \in M_1\} + \phi_B(M_2) \times \{0_{\mathbb{Z}^n}\} \subset Z^{2*n}.$$

Somit sind die Vektoren

$$\begin{aligned} u_1 &:= \sum_{k=1}^{|G_1|} a_k * (v_k, v_k) \\ u_2 &:= \sum_{k=1}^{|G_2|} b_k * (w_k, 0_{\mathbb{Z}^n}) \end{aligned}$$

beide in $\mathfrak{m}_3$. Außerdem gilt $u_1 - u_2 = (0_{\mathbb{Z}^n}, u)$. In der Hermite-Normalform wird also $u_1 - u_2$ schon von den Zeilen erzeugt, deren Zeilenanfänge größer als n sind. Dies sind genau die Zeilen der Teilmatrix

$$\begin{pmatrix} 0 & Z \end{pmatrix}$$

von N. Damit wird u von den Zeilen der Matrix Z erzeugt. Es wurde also gezeigt, dass die Zeilen von Z genau den Modul $\phi_B(\mathfrak{m}_1 \cap \mathfrak{m}_2)$ erzeugen. Somit erzeugen die Urbilder $c_1, \ldots, c_{n-i_0+1}$ von den Zeilen den Modul $\mathfrak{m}_1 \cap \mathfrak{m}_2$. □

Faktormodul

Algorithmus 4.3.5. Der folgende Algorithmus berechnet den Isomorphietyp des Faktormoduls $\mathfrak{m}_1/\mathfrak{m}_2$und den Index $(\mathfrak{m}_1 : \mathfrak{m}_2)$, wobei $\mathfrak{m}_1, \mathfrak{m}_2$ Module in K sind mit $\mathfrak{m}_2 \subset \mathfrak{m}_1$.

1. Setze $B_1 := \mathfrak{m}_1$.basis(), $B_2 := \mathfrak{m}_2$.basis(), $r_i := |B_i|$. Vervollständige B_1 zu einer $\mathbb{Q}$-Basis B von K durch Hinzufügen geeigneter Elemente.

2. Berechne die Koordinatenvektoren $v_1, \ldots, v_{r_2}$ der Elemente von B_2 bezüglich der Basis B.

3. Schreibe die Vektoren $v_1, \ldots, v_{r_2}$ als Zeilen in eine $r_2 \times n$-Matrix A und bestimme ihre Smith-Normalform S.

4. Setze $d_1, \ldots, d_{r_2}$ gleich den Diagonalelementen von S, die ungleich 0 sind.

5. Gib das Produkt $\mathbb{Z}^{r_1-r_2} \times \prod_{i=1}^{r_2} \mathbb{Z}/(d_i)_\mathbb{Z}$ als Isomorphietyp des Faktormoduls $\mathfrak{m}_1/\mathfrak{m}_2$ zurück. Falls $r_1 = r_2$ gilt, gib $\prod_{i=1}^{r_2} d_i$ als Index zurück, ansonsten ∞.

Beweis. Da $\mathfrak{m}_2 \subset \mathfrak{m}_1$ gilt, sind alle Elemente von $\mathfrak{m}_2$ auch $\mathbb{Z}$-Linearkombinationen der Elemente von B_1, also insbesondere $\mathbb{Z}$-Linearkombinationen der Elemente von B. Somit hat die Matrix A Koeffizienten in $\mathbb{Z}$ und es kann ihre Smith-Normalform gebildet werden. Sei $\phi_B : K \to \mathbb{Q}^n$ die Koordinatenabbildung bezüglich der Basis B. Da B_1 eine Basis und eine Teilmenge von B ist, gilt $\phi_B(\mathfrak{m}_1) \cong \mathbb{Z}^{r_1}$. Da S die Smith-Normalform von A ist, gibt es invertierbare Matrizen U, V mit $A = U * S * V$. Die Matrix V induziert dann eine Basistransformation in $\phi_B(\mathfrak{m}_1) \cong \mathbb{Z}^{r_1}$, die $\mathbb{Z}^{r_1}$ auf sich selbst abbildet und die Zeilen von $U * S$ auf die Zeilen von A. Da die Zeilen von $U * S$ den gleichen Modul erzeugen wie die Zeilen von S, erhält man also einen Isomorphismus $\mathbb{Z}^{r_1}/[d_1 * e_1, \ldots, d_{r_2} * e_{r_2}]_\mathbb{Z} \cong \mathbb{Z}^{r_1}/[v_1, \ldots, v_{r_2}]_\mathbb{Z}$. Es gilt also insgesamt:

$$\begin{aligned} \phi_B(\mathfrak{m}_1)/\phi_B(\mathfrak{m}_2) &\cong Z^{r_1}/[v_1, \ldots, v_{r_2}]_\mathbb{Z} \\ &\cong \mathbb{Z}^{r_1}/[d_1 * e_1, \ldots, d_{r_2} * e_{r_2}]_\mathbb{Z} \\ &\cong \mathbb{Z}^{r_1-r_2} \times \prod_{i=1}^{r_2} \mathbb{Z}/(d_i)_\mathbb{Z} \end{aligned}$$

Der Index ergibt sich dann sofort aus dieser Darstellung. □

Quotient von Moduln

Algorithmus 4.3.6. Der folgende Algorithmus berechnet den Quotienten $\mathfrak{m}_1 \% \mathfrak{m}_2$ von zwei Moduln $\mathfrak{m}_1$, $\mathfrak{m}_2$.

1. Setze $B_2 := \mathfrak{m}_2$.basis(), $N := \{\}$.
2. Für jedes Element $b \in B_2$ berechne den Modul $b^{-1} * \mathfrak{m}_1$ und füge ihn zur Menge von Moduln N hinzu.
3. Berechne den Schnitt $\mathfrak{n}$ aller Moduln in N durch (mehrfache) Anwendung von Algorithmus 4.3.4 und gib den Modul $\mathfrak{n}$ zurück.

Beweis. Nach Proposition 3.1.7 ist der Quotient der Schnitt über die Moduln $m_i^{-1} * \mathfrak{m}_1$, wobei $m_1, \ldots, m_r$ eine Basis von $\mathfrak{m}_2$ ist. Somit ist der Quotient genau der Schnitt über die Moduln in N. □

4.3.3 Ordnungsalgorithmen

Zerlegung einer halbeinfachen Algebra

Algorithmus 4.3.7. Der folgende Algorithmus berechnet für eine Primzahl p und eine halbeinfache $\mathbb{F}_p$-Algebra A die Zerlegung $\bigoplus_{i=1}^{r} A_i$ von A in einfache Algebren $A_1, \ldots, A_r$.

1. Setze $\mathcal{A} := \{A\}$ und $r = 0$.

2. Wähle ein beliebiges Element B aus $\mathcal{A}$ und entferne es aus $\mathcal{A}$. Kann kein Element B aus $\mathcal{A}$ gewählt werden (weil $\mathcal{A} = \emptyset$), so sind $A_1, \ldots, A_r$ die gesuchten Elemente der Zerlegung.

3. Sei $\psi : B \to B$ die Abbildung, die $x \in B$ auf $x^p - x$ abbildet. Berechne $\ker \psi$ und seine Dimension k. Ist $k = 1$, so setze $r := r + 1$, $A_r := B$ und gehe zurück zu Schritt 2). Ist $r > 1$, so wähle ein $\alpha \in \ker \psi \setminus (\mathbb{F}_p * 1_B)$ und gehe zu Schritt 4).

4. Berechne das Minimalpolynom $\mu_\alpha \in \mathbb{F}_p[x]$ von α und zerlege es in zwei teilerfremde Polynome m_1 und m_2 in $\mathbb{F}_p[x]$. Berechne $u, v \in \mathbb{F}_p[x]$, so dass $u * m_1 + v * m_2 = 1_{\mathbb{F}_p[x]}$ gilt. Setze $\epsilon := (u * m_1)(\alpha) \in B$.

5. Setze $B_1 := \epsilon * B$ und $B_2 := (1 - \epsilon) * B$, füge B_1 und B_2 zu $\mathcal{A}$ hinzu und gehe zu Schritt 2).

Beweis. Erläuterung der einzelnen Schritte:

1) Die Menge $\mathcal{A}$ soll die Elemente der Zerlegung enthalten, bei denen noch nicht bekannt ist, ob sie weiter zerlegbar sind, das heißt ob sie einfach oder halbeinfach sind. Die Elemente $A_1, \ldots, A_r$ hingegen sind die Elemente der Zerlegung, bei denen schon bekannt ist, dass sie einfach sind. Am Anfang ist also $\mathcal{A} = \{A\}$ und $r = 0$.

2) Zu Beginn dieses Schrittes gilt immer $A = \bigoplus_{i=1}^{r} A_i \oplus \bigoplus_{B \in \mathcal{A}} B$, wobei die Elemente $A_1, \ldots, A_r$ einfach sind und die Elemente $B \in \mathcal{A}$ im Allgemeinen nur halbeinfach sind, aber auch schon einfach sein können. Gibt es also keine Elemente mehr in $\mathcal{A}$, so ist A vollständig in einfache Algebren zerlegt. Ansonsten wird ein Element B der Zerlegung ausgewählt, um es (falls möglich) weiter zu zerlegen.

3) Ist die Dimension des Kerns von ψ gleich 1, so gilt nach Lemma 2.8.32, dass B einfach ist. Somit fügt man B zu den einfachen Algebren $A_1, \ldots, A_r$ hinzu. Ansonsten bestimmt man mit Hilfe von Lemma 2.8.32 ein idempotentes Element von B, um B mit Hilfe von Proposition 2.8.29 weiter zu zerlegen. Für die Berechnung von teilerfremden m_1 und m_2 kann man beispielsweise das Polynom μ_α vollständig in Faktoren zerlegen und dann m_1 gleich der höchsten Potenz eines irreduziblen Faktors setzen und m_2 gleich dem Rest setzen. Natürlich kann man an dieser Stelle noch optimieren und muss μ_α nicht unbedingt vollständig zerlegen. Die Polynome u und v kann man mit dem erweiterten euklidischen Algorithmus bestimmen, da der größte gemeinsame Teiler von m_1 und m_2 gleich $1_{\mathbb{F}_p[x]}$ ist. Nach Lemma 2.8.32 ist dann $\epsilon = (u * m_1)(\alpha)$ ein nicht-triviales idempotentes Element von B.

5) Da im vorherigen Schritt ein nicht-triviales idempotentes Element ϵ von B gefunden wurde, ist B nach Proposition 2.8.29 die direkte Summe von $B_1 = \epsilon * B$ und $B_2 = (1-\epsilon) * B$. Da noch nicht bekannt ist, ob sich B_1 und B_2 weiter zerlegen lassen, werden sie zunächst beide zu $\mathcal{A}$ hinzugefügt und man geht wieder zu Schritt 2), um weitere Elemente zu zerlegen.

□

Bestimmung der Primideale über einer bestimmten Primzahl

Algorithmus 4.3.8. Der folgende Algorithmus berechnet die Primideale $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ in einer Ordnung $\mathcal{O}$, die über einer gegebenen Primzahl p liegen, das heißt es gilt $(p)_\mathcal{O} \subset \mathfrak{p}_i$.

1. Setze $B := \mathcal{O}/(p)_\mathcal{O}$ und berechne die Dimension n von B als $\mathbb{Z}/p\mathbb{Z}$-Vektorraum.

2. Wähle k so, dass $p^{k-1} < n \leq p^k$ gilt und setze $\mathcal{N}_B := \ker\left(\phi^k\right)$, wobei ϕ der Frobenius-Homomorphismus $\mathrm{Frob}(p)$ ist.

3. Setze $A := B/\mathcal{N}_B$, zerlege A mit Algorithmus 4.3.7 in eine direkte Summe $\bigoplus_{i=1}^{r} A_i$ von einfachen Algebren $A_1, \ldots, A_r$ und setze dann $\bar{\mathfrak{p}}_j := \sum_{i \neq j} A_i$ für jedes j in $\{1, \ldots, r\}$.

4. Berechne das Urbild $\mathfrak{p}_j := \iota^{-1}(\bar{\mathfrak{p}}_j)$ für alle j in $\{1, \ldots, r\}$, wobei

$$\begin{array}{ccccc} \iota : \mathcal{O} & \to & B = \mathcal{O}/(p)_\mathcal{O} & \to & A = B/\mathcal{N}_B \\ x & \mapsto & \bar{x} := x + (p)_\mathcal{O} & \mapsto & \bar{x} + \mathcal{N}_B \end{array}$$

   die kanonische Inklusion ist. Die $\mathfrak{p}_j$ sind dann die gesuchten Primideale über p.

Beweis. Erläuterung der einzelnen Schritte:

1) Nach Proposition 2.2.15 gibt es eine Bijektion zwischen den Primidealen in $\mathcal{O}$, die $(p)_\mathcal{O}$ enthalten und den Primidealen in $\mathcal{O}/(p)_\mathcal{O}$. Da in $\mathcal{O}$ alle Primideale maximal sind, sind nach der gleichen Proposition auch alle Primideale in B maximal.

2) Nach Lemma 2.8.24 ist das auf diese Weise erzeugte $\mathcal{N}_B$ das Nilradikal von B und somit nach 2.8.20 der Schnitt über alle Primideale in B (und da in B alle Primideale maximal sind, ist es gleichzeitig das Jacobson-Radikal in B). Somit enthalten alle Primideale in B das Ideal $\mathcal{N}_B$ und deshalb gibt es nach Proposition 2.2.15 eine Bijektion von den Primidealen in B und den Primidealen in $B/\mathcal{N}_B$.

3) B ist eine endlich erzeugte $\mathbb{F}_p$-Algebra, also ist nach Theorem 2.8.34 die $\mathbb{F}_p$-Algebra $A = B/\mathcal{N}_B$ halbeinfach. Somit kann A mit Algorithmus 4.3.7 zerlegt werden. Da die Zerlegung eine direkte Summe ist, bekommt man $A/\bar{\mathfrak{p}}_j = (\bigoplus_{i=1}^{r} A_i)/(\bigoplus_{i\neq j} A_i) = A_j$. Außerdem ist jedes A_j einfach, also nach Lemma 2.8.31 auch ein Körper. Somit ist nach Proposition 2.2.16 die Menge $\bar{\mathfrak{p}}_j$ ein Primideal in A. Diese $\bar{\mathfrak{p}}_j$ sind die einzigen Primideale in A.

4) Wie bereits in 1) und 2) angesprochen gibt es eine Bijektion zwischen den Primidealen über p in $\mathcal{O}$ und den Primidealen in A. Diese wird durch ι induziert. Da die $\bar{\mathfrak{p}}_j$ alle Primideale in A sind, bekommt man durch die Urbilder $\mathfrak{p}_j$ alle Primideale in $\mathcal{O}$, die über p liegen.

□

4.3.4 Idealalgorithmen

Bewertung bezüglich eines Primideals

Algorithmus 4.3.9. Der folgende Algorithmus berechnet eine Teilzerlegung eines Ideals $\mathfrak{a}$ in einer Ordnung $\mathcal{O}$ in eine Potenz eines invertierbaren Primideals $\mathfrak{p}$ (mit Exponent e) und einen Rest $\mathfrak{A}$, der nicht in $\mathfrak{p}$ enthalten ist.

1. Setze $e := 0$, $\mathfrak{A} := \mathfrak{a}$.
2. Berechne das Inverse $\mathfrak{p}^{-1}$ von $\mathfrak{p}$.
3. Ist $\mathfrak{A}$ in $\mathfrak{p}$ enthalten, so setze $e := e + 1$, $\mathfrak{A} := \mathfrak{p}^{-1} * \mathfrak{A}$. Ist $\mathfrak{A}$ nicht in $\mathfrak{p}$ enthalten, so gib $\mathfrak{A}$ und $\mathfrak{p}^e$ (oder $\mathfrak{A}$ und e) zurück.

Beweis. Zunächst ist nur die Zerlegung $\mathfrak{a} = \mathfrak{a} * \mathfrak{p}^0$ bekannt, also setzt man $\mathfrak{A} = \mathfrak{a}$ und $e = 0$. Da $\mathfrak{p}$ invertierbar ist, kann man das Inverse berechnen. Ist $\mathfrak{A}$ in $\mathfrak{p}$ enthalten, so gilt $\bar{\mathfrak{A}} = \mathfrak{A} * \mathfrak{p}^{-1} \subset \mathcal{O}$, also ist $\bar{\mathfrak{A}}$ ein ganzzahliges Ideal, für das $\mathfrak{A} = \mathfrak{A} * (1)_{\mathcal{O}} = \mathfrak{A} * \mathfrak{p}^{-1} * \mathfrak{p} = \bar{\mathfrak{A}} * \mathfrak{p}$ gilt. Deshalb erhöht man den Exponenten e um eins und setzt $\mathfrak{A}$ gleich $\mathfrak{A} * \mathfrak{p}^{-1}$. Ist hingegen $\mathfrak{A}$ nicht in $\mathfrak{p}$ enthalten, so hat man die gewünschte Darstellung gefunden. Diese ist nach Proposition 3.3.13 eindeutig.

Hinweis zur Endlichkeit des Algorithmus: Nach Proposition 3.3.13 gibt es genau eine Darstellung $\mathfrak{a} = \mathfrak{A} * \mathfrak{p}^e$ mit $\mathfrak{A} \not\subset \mathfrak{p}$ und bei dieser ist $e = \nu_{\mathfrak{p}}(\mathfrak{a}) \in \mathbb{N}_0$. Somit kommt man nach endlich vielen Schritten zu dieser Darstellung.

□

Bemerkung 4.3.5. *Grundsätzlich kann man diesen Algorithmus auch für gebrochene Ideale $\bar{\mathfrak{a}}$ und invertierbare gebrochene Ideale $\bar{\mathfrak{p}}$ definieren. Wie bei ganzzahligen Idealen folgt aus $\mathfrak{A} \subset \bar{\mathfrak{p}}$ auch $\bar{\mathfrak{A}} = \mathfrak{A} * \bar{\mathfrak{p}}^{-1} \subset \mathcal{O}$. Somit sind die*

$\mathfrak{A}$ *in allen weiteren Iterationen ganzzahlige Ideale. Man erhält also durch die* $\mathfrak{A}$ *in den Iterationsschritten eine aufsteigende Kette von ganzzahligen Idealen in* $\mathcal{O}$*. Da* $\mathcal{O}$ *noethersch ist, ist die Kette entweder endlich (das heißt der Algorithmus terminiert) oder die Kette muss stationär werden, das heißt* $\mathfrak{A} = \bar{\mathfrak{A}} = \mathfrak{A} * \bar{\mathfrak{p}}^{-1}$ *in einem Schritt und somit* $\mathfrak{A} = \mathfrak{A} * \bar{\mathfrak{p}}^{-1} * \bar{\mathfrak{p}} = \mathfrak{A} * \bar{\mathfrak{p}}$*. Damit muss aber die Kette (im unendlichen Fall) nur aus Gleichungen bestehen, da dann für zwei aufeinanderfolgende Elemente* $\mathfrak{B}$ *und* $\bar{\mathfrak{B}}$ *der Kette immer* $\bar{\mathfrak{B}} = \mathfrak{B} * \bar{\mathfrak{p}}^{-1}$ *und somit auch* $\mathfrak{B} = \bar{\mathfrak{B}} * \bar{\mathfrak{p}}$ *gilt. In diesem Fall würde der Algorithmus nicht terminieren. Deshalb sollte man* ∞ *und* $\bar{\mathfrak{a}}$ *zurückgeben, falls* $\bar{\mathfrak{a}} = \bar{\mathfrak{a}} * \bar{\mathfrak{p}}^{-1}$ *gilt. Ein triviales Beispiel für diesen Fall wäre* $\bar{\mathfrak{a}}$ *beliebig und* $\bar{\mathfrak{p}} = (1)_{\mathcal{O}}$*.*

Zerlegung eines Ideals in Primideale

Algorithmus 4.3.10. Der folgende Algorithmus berechnet die vollständige Zerlegung eines Ideals $\mathfrak{a}$ in einer Ordnung $\mathcal{O}$ in invertierbare Primideale $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ mit Exponenten $e_1, \ldots, e_s$ und einen Rest $\mathfrak{A}$, der in keinem invertierbaren Primideal enthalten ist.

1. Setze $s := 0$ und $\mathfrak{A} := \mathfrak{a}$.

2. Berechne die Diskriminante d von $\mathfrak{a}$ und ihre Primfaktorzerlegung $d = p_1^{e_1} * p_2^{e_2} * \ldots * p_r^{e_r}$, wobei $p_1, \ldots, p_r$ paarweise verschiedene Primzahlen sind.

3. Wähle eine Primzahl $p := p_i$ mit Exponent e_i größer gleich 2 und berechne die Primideale $\mathfrak{P}_1, \ldots, \mathfrak{P}_t$ über p (siehe Algorithmus 4.3.8).

4. Für jedes Primideal $\mathfrak{P} := \mathfrak{P}_i$ teste, ob $\mathfrak{P}$ invertierbar ist. Ist $\mathfrak{P}$ invertierbar, so zerlege $\mathfrak{A}$ mit Algorithmus 4.3.9 in ein Produkt $\bar{\mathfrak{A}} * \mathfrak{P}^e$ (wobei $\bar{\mathfrak{A}}$ nicht in $\mathfrak{P}$ enthalten ist) und setze $\mathfrak{A} := \bar{\mathfrak{A}}$, $s := s+1$, $\mathfrak{p}_s := \mathfrak{P}$ und $e_s := e$. Falls $\mathfrak{P}$ nicht invertierbar ist, gehe zum nächsten Primideal. Wurden alle Primideale überprüft, so gehe zurück zu Schritt 3) und wähle eine noch nicht gewählte Primzahl. Wurden bereits alle Primzahlen überprüft, so gib die invertierbaren Primideale $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ mit Exponenten $e_1, \ldots, e_s$ und den Rest $\mathfrak{A}$ zurück.

Beweis. Erläuterung der einzelnen Schritte:

1) Bisher wurden noch keine Primidealteiler von $\mathfrak{a}$ gefunden, also setzt man $s = 0$ und $\mathfrak{A} = \mathfrak{a}$.

2) und 3) Jedes Primideal $\mathfrak{p}$, das in einer Zerlegung von $\mathfrak{a}$ in Ideale auftaucht, muss $\mathfrak{a}$ enthalten. Nach Korollar 3.3.5 muss also die Basisprimzahl p von $\mathfrak{p}$ die Diskriminante von $\mathfrak{a}$ quadratisch teilen. Somit muss man nur die Primideale über den Primzahlen mit Exponent größer gleich 2 betrachten.

4) In diesem Schritt werden (im Verlauf des ganzen Algorithmus) alle invertierbaren Primideale, die über $\mathfrak{a}$ liegen könnten, betrachtet. Faktorisiert man diese mit Algorithmus 4.3.9 alle heraus, so bekommt man eine Zerlegung wie gefordert (vergleiche hierzu auch den Beweis von Proposition 3.3.23).

□

4.3.5 Zahlkörperalgorithmen

Berechnung der Maximalordnung

Algorithmus 4.3.11. Der folgende Algorithmus liefert nach endlich vielen Schritten die Maximalordnung $\mathcal{O}_K$ eines beliebigen Zahlkörpers K. Der Algorithmus ist auch als ROUND-1-Algorithmus von Zassenhaus bekannt.

1. Bestimme ein $\gamma \in K$ ganz über $\mathbb{Z}$ mit $K = \mathbb{Q}[\gamma]$ und setze $\mathcal{O} := \mathbb{Z}[\gamma]$.

2. Berechne die Diskriminante d von $\mathcal{O}$ und zusätzlich ihre Primfaktorzerlegung $d = p_1^{e_1} * p_2^{e_2} * \ldots * p_r^{e_r}$ mit paarweise verschiedenen Primzahlen $p_1, \ldots, p_r$.

3. Wähle eine Primzahl $p := p_i$, deren Exponent e_i größer gleich 2 ist und bestimme alle über $(p)_\mathcal{O}$ liegenden Primideale $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ (siehe Algorithmus 4.3.8).

4. Suche ein $i_0 \in \{1, \ldots, s\}$ mit $\mathrm{Ord}(\mathfrak{p}_{i_0}) \neq \mathcal{O}$. Wird ein i_0 gefunden, setze $\mathcal{O} := \mathrm{Ord}(\mathfrak{p}_{i_0})$ und gehe erneut zu Schritt 2). Falls kein solches i_0 vorhanden ist, gehe zu Schritt 3) und wähle eine Primzahl, die noch nicht gewählt wurde. Wurden bereits alle Primzahlen betrachtet, so setze $\mathcal{O}_K := \mathcal{O}$. Dies ist die Maximalordnung.

Beweis. Erläuterung der einzelnen Schritte:

1) Zunächst gibt es nach Theorem 2.4.12 ein über $\mathbb{Z}$ ganzes Element $\gamma \in K$, so dass $K = \mathbb{Q}[\gamma]$ gilt. Da γ ganz über $\mathbb{Z}$ ist, ist die Menge $\mathbb{Z}[\gamma]$ nach Lemma 2.4.4 ein endlich erzeugter $\mathbb{Z}$-Untermodul von K und somit ein Modul von K. Da γ außerdem K erzeugt ist $\mathbb{Z}[\gamma]$ vollständig und somit sogar eine Ordnung, da $\mathbb{Z}[\gamma]$ ein Ring ist.

2) und 3) Falls die Ordnung $\mathcal{O}$ nicht die Maximalordnung ist, so muss es nicht-invertierbare Primideale in $\mathcal{O}$ geben. Nach Proposition 3.3.2 liegt jedes Primideal über einer Primzahl p. Ist $\mathfrak{p}$ ein Primideal über p und nicht invertierbar, so muss nach Lemma 3.3.35 gelten, dass $\mathcal{O}$ nicht p-maximal ist, also $p \mid (\mathcal{O}_K : \mathcal{O})$ gilt. Wegen Lemma 3.1.10 [Diskriminanten-Index-Formel] gilt dann

$$p^2 \mid (\mathcal{O}_K : \mathcal{O})^2 * d(\mathcal{O}_K) = d(\mathcal{O}).$$

Somit muss man nur Primideale über Primzahlen betrachten, die mindestens quadratisch in der Primfaktorzerlegung der Diskriminante von $\mathcal{O}$ auftauchen. Diese bestimmt man mit Algorithmus 4.3.8.

4) Nach Proposition 3.3.11 ist $\mathfrak{p}_{i_0}$ genau dann nicht invertierbar, wenn $\mathcal{O} \subsetneq \mathrm{Ord}(\mathfrak{p}_{i_0})$ gilt. Damit bekommt man eine größere Ordnung. Von dieser kann man dann wieder die Diskriminante berechnen (die betragsmäßig kleiner ist) und wieder nach Primidealen suchen. Gilt bei jedem $\mathfrak{p}_i$ die Gleichung, so sind alle $\mathfrak{p}_i$ invertierbar und da die $\mathfrak{p}_i$ alle Primideale über p waren, ist $\mathcal{O}$ auch p-maximal. Somit kann man zur nächsten Primzahl übergehen. Wurden bereits alle Primzahlen betrachtet, so ist $\mathcal{O}$ für alle Primzahlen p-maximal und man hat deshalb die Maximalordnung gefunden, da alle Primideale invertierbar sind.

   Hinweis zur Endlichkeit des Algorithmus: Die Betrachtung jeder Ordnung $\mathcal{O}$ besteht aus endlich vielen Schritten, da die Diskriminante von $\mathcal{O}$ nur endlich viele Primzahlen enthält und für jede Primzahl nur endlich viele Primideale über dieser Primzahl existieren. Außerdem wird nur endlich oft eine neue (echt größere) Ordnung gesetzt, da jede streng monoton aufsteigende Kette von Ordnungen stationär wird (vergleiche Beweis von Theorem 3.1.16).

□

Bemerkung 4.3.6. *Wurde in Schritt 4) für eine Primzahl kein Primideal mit* $Ord(\mathfrak{p}_{i_0}) \neq \mathcal{O}$ *gefunden, so kann diese Primzahl auch in allen größeren Ordnungen ignoriert werden, da schon* $\mathcal{O}$ *p-maximal ist und diese Eigenschaft sich auf Ordnungen* $\tilde{\mathcal{O}}$ *mit* $\mathcal{O} \subset \tilde{\mathcal{O}}$ *überträgt.*

4.4 Umsetzung der Algorithmen in Sage

In diesem Abschnitt wird das Rechnen in Zahlkörpern in Sage (siehe [S+09]) umgesetzt. Sage ist eine frei erhältliche open-source Alternative zu bekannten mathematischen Systemen (Magma, Maple, Mathematica, Matlab) und kann sowohl online benutzt werden als auch auf den eigenen Computer heruntergeladen werden (für mehr Informationen siehe die angegebene Internetseite von [S+09]). Die Syntax der Sage-Algorithmen ist (bis auf minimale Unterschiede) die gleiche wie in der Programmiersprache Python (siehe auch `http://www.python.org`). Für ein vollständiges Verständnis der folgenden Algorithmen ist es also empfehlenswert, wenn man schon Kenntnisse in der Programmiersprache Python hat. Bei Kenntnissen in einer anderen Programmiersprache empfehle ich die Python-Funktionen 'map' und 'reduce' und den Begriff 'lambda expression' nachzuschlagen, da diese in den Funktionen an vielen Stellen verwendet werden und es nicht in allen Programmiersprachen eine Entsprechung davon gibt. Die Sage-Algorithmen orientieren

sich von der Struktur und den Variablennamen größtenteils an den vorher beschriebenen mathematischen Algorithmen, allerdings kann es an einzelnen Stellen zu Unterschieden kommen.

4.4.1 Vorbemerkungen

In der verwendeten Version von Sage (Version 5.4 vom 09.11.2012) gibt es bereits Klassen und Funktionen für Zahlkörper, Ordnungen und gebrochene Ideale, allerdings sind nur gebrochene Ideale in der Maximalordnung implementiert. Deshalb werden im Folgenden die neuen Klassen 'NFModule' und 'NFFractionalIdealInOrder' implementiert. Diese sind darauf ausgelegt mit den vorhandenen Klassen 'NumberField' und 'Order' zu funktionieren. Zusätzlich wird noch eine Klasse 'NFFunctions' implementiert, in der einige weitere (statische) Funktionen für Zahlkörper und Ordnungen enthalten sind. Darunter sind einige Hilfsfunktionen für die anderen Algorithmen, aber auch die Implementierung der in Abschnitt 4.3 beschriebenen Algorithmen zur Bestimmung von Primidealen über einer Primzahl und zur Berechnung der Maximalordnung. Die Algorithmen zur Bestimmung von Hermite- und Smith-Normalform einer Matrix M sind in Sage durch die Funktionen 'M.echelon_form()' und 'M.smith_form()' gegeben. Dokumentation und Autoren der verwendeten Klassen können im 'Sage Reference Manual' (`http://www.sagemath.org/doc/reference/index.html`) nachgeschlagen werden.

4.4.2 Zahlkörper

```
"""
NUMBER FIELD FUNCTIONS (Last Update: 28.2.2013)
"""

from sage.rings.quotient_ring import QuotientRing_generic

class NFFunctions():
    #Returns a tuple with the following objects:
    #0: Space of the coordinate system in the given basis (or the
        standard basis if coord_basis is None).
    #1: Map from the coordinate system to the number field
    #2: Map from the number field in the coordinate system.
    #Remark: If the given basis has less elements than the degree of
        the number field, then the coordinate system maps only the
        part generated from the given basis. An element of the number
        field that cannot be mapped in the coordinate system (because
        it is not in the QQ-subspace generated from the basis) is
        mapped to None with the corresponding function.
    @staticmethod
    def coordinate_system(number_field, coord_basis = None):
        standard_coordinate_system = number_field.
            absolute_vector_space()
        if(coord_basis is None):
            return standard_coordinate_system
        else:
            #0: coordinate system
            coord_basis = map(number_field, coord_basis)
            basis_vectors = map(standard_coordinate_system[2],
                coord_basis)
            vector_space = standard_coordinate_system[0].
                subspace_with_basis(basis_vectors)
```

```
        #1: map to number field
        to_number_field_function = lambda x:
            standard_coordinate_system[1](vector_space.
            linear_combination_of_basis(x))
        #2: map to coordinate system
        vectorize_function_with_check = lambda x, y: vector_space.
            coordinate_vector(x) if x in y else None
        to_coord_function = lambda x:
            vectorize_function_with_check(
            standard_coordinate_system[2](x), vector_space)
        return (vector_space, to_number_field_function,
            to_coord_function)

#Returns the standard basis of number_field
@staticmethod
def standard_basis(number_field):
    alpha = number_field.absolute_generator()
    return [alpha**i for i in range(number_field.degree())]

@staticmethod
def basis_change_function(number_field, basis_from, basis_to):
    cs_from = NFFunctions.coordinate_system(number_field,
        basis_from)
    cs_to = NFFunctions.coordinate_system(number_field, basis_to)
    change_func = lambda x: cs_to[2](cs_from[1](x))
    return change_func

@staticmethod
def basis_change_matrix(number_field, basis_from, basis_to):
    m = len(basis_from) if not(basis_from is None) else
        number_field.degree()
    n = len(basis_to) if not(basis_to is None) else number_field.
        degree()
    if not(m == n):
        raise ValueError('Can only create a basis change matrix if
            the bases have the same number of elements.')
    change_func = NFFunctions.basis_change_function(number_field,
        basis_from, basis_to)
    e = [[1 if i == j else 0 for i in range(m)] for j in range(m)]
    images = map(change_func, e)
    for i in images:
        if i is None:
            raise ValueError('The bases for the basis change
                matrix have to span the same QQ vector space in
                the number field')
    A = matrix(len(images), images)
    return A

#Matrix that corresponds to multiplication with element in terms
    of coord_basis (or standard basis of number_field if
    coord_basis == None)
@staticmethod
def multiplication_matrix(element, number_field, coord_basis =
    None):
    element = number_field(element)
    cs = NFFunctions.coordinate_system(number_field)
    M = matrix(number_field.degree(), map(cs[2], [element*b for b
        in NFFunctions.standard_basis(number_field)]))
    if not(coord_basis is None):
        B = NFFunctions.basis_change_matrix(number_field, None,
            coord_basis)
        M = B.inverse()*M*B
    return M

#This function is only implemented to work within
    prime_ideals_above_p(p, order). If you use this function in
    other situations, the behaviour is unknown.
@staticmethod
def _split_semisimple_algebra(A, p, cs):
    nilrad = A.defining_ideal()
    order = nilrad.order()
    number_field = order.number_field()
    Fp = Integers(p)
    generators_A = [j.lift() for j in A.gens()]
```

```
N = matrix(Fp, map(cs[2], generators_A))
N = N.echelon_form().submatrix(0, 0, N.rank(), N.ncols())
basis_A = map(cs[1], [[i[j].lift() for j in range(len(i))] for
     i in N.rows()])
#semisimple algebras are stored here as a tuple of a NFModule
    and an element in the number field that is the identity
    element in the algebra
semisimple_algebras = [[NFModule(basis_A, number_field),
    number_field(1)]]
#simple algebras will be stored only as a NFModule, because we
     don't need the unit outside this function
simple_algebras = list()
while len(semisimple_algebras) > 0:
    algebra = semisimple_algebras.pop()
    algebra_module = algebra[0]
    one = algebra[1]
    kernel_generator = [a.lift() for a in map(A,
        algebra_module.number_field_basis()) if a**p-a == A(0)
        ]
    M = matrix(Fp, map(cs[2], kernel_generator)).echelon_form
        ()
    M = M.echelon_form().submatrix(0, 0, M.rank(), M.ncols())
    kernel_basis = map(cs[1], [[v[i].lift() for i in range(len
        (v))] for v in M.rows()])
    dim = len(kernel_basis)
    if dim < 1:
        raise RuntimeWarning('Kernel has no elements. This
            should not happen. Please check parameters and
            algorithm.')
        return []
    elif dim == 1:
        simple_algebras = simple_algebras + [algebra_module]
    elif dim > 1:
        #Search for an alpha in kernel_basis, that is not in
            Fp*1_A
        alpha = None
        for k in kernel_basis:
            vector1 = cs[2](A(k).lift())
            vector2 = cs[2](A(one).lift())
            M = matrix(Fp, [vector1, vector2])
            if not(M.rank() == 1):
                alpha = A(k)
                break
        if alpha == None:
            raise RuntimeWarning('Could not find an alpha in
                kernel basis, that is not in Fp*1_A. Please
                check parameters and algorithm.')
        cs_A = NFFunctions.coordinate_system(number_field,
            basis_A)
        N = matrix(Fp, map(cs_A[2], [(alpha*A(a)).lift() for a
             in basis_A]))
        fact = N.minpoly('x').factor()
        m1 = fact[0][0]**fact[0][1]
        m2 = reduce(lambda l1, l2: l1+l2[0]**l2[1], [fact[j]
            for j in range(1, len(fact))], 0)
        unit, u, v = xgcd(m1, m2)
        if unit != 1:
            raise RuntimeWarning('Calculated polynomials are
                not coprime. Please check algorithm.')
        koeff = m1.coeffs()
        m1alpha = reduce(lambda l1, l2: l1 + l2[0]*alpha**l2
            [1], [(A(koeff[i]), i) for i in range(1, len(koeff
            ))], A(koeff[0]))
        epsilon = (A(u)*m1alpha).lift()
        algebra1 = [NFModule([epsilon*b for b in
            algebra_module.number_field_basis()], number_field
            ), epsilon]
        algebra2 = [NFModule([(1-epsilon)*b for b in
            algebra_module.number_field_basis()], number_field
            ), (1-epsilon)]
        semisimple_algebras = semisimple_algebras + [algebra1,
             algebra2]
return simple_algebras
```

```
    @staticmethod
    def prime_ideals_above_p(p, order):
        number_field = order.number_field()
        Fp = Integers(p)
        cs = NFFunctions.coordinate_system(number_field, order.basis()
            )
        pO = NFFractionalIdealInOrder([p], order)
        B = QuotientRing(order, pO, 'b')
        n = len(B.gens())
        k = min([k for k in range(n) if n <= p^k])
        R.<x> = PolynomialRing(ZZ)
        phik = x^(p^k)
        images = [phik(b) for b in B.gens()]
        im_vectors = map(cs[2], [i.lift() for i in images])
        M = matrix(Fp, im_vectors)
        ker = M.kernel()
        ker_basis = map(cs[1], [[v[i].lift() for i in range(len(v))]
            for v in ker.basis()])
        nilrad = NFFractionalIdealInOrder(pO.number_field_basis()+
            ker_basis, order)
        A = QuotientRing_generic(order, nilrad, 'a')
        simple_algebras = NFFunctions._split_semisimple_algebra(A, p,
            cs)
        prime_ideal_modules = [reduce(lambda l1, l2: l1 + l2, [
            simple_algebras[j] for j in range(len(simple_algebras)) if
             i != j], nilrad.module()) for i in range(len(
            simple_algebras))]
        return [NFFractionalIdealInOrder(pr_id.basis(), order) for
            pr_id in prime_ideal_modules]

    #This function calculates the maximal order of the number field
        with the round1 algorithm of zassenhaus
    @staticmethod
    def maximal_order_round1(number_field):
        alpha = number_field.absolute_generator()
        order = ZZ.extension(number_field.absolute_polynomial(), '
            alpha')
        maximal = false
        while not(maximal):
            new_order = None
            d = order.discriminant()
            fact = d.factor()
            pr_id = None
            for (p, i) in fact:
                if not(new_order is None):
                    break
                if i >= 2:
                    for pr_id in NFFunctions.prime_ideals_above_p(p,
                        order):
                        pr_id_order = pr_id.module().module_order()
                        if pr_id_order != order:
                            new_order = pr_id_order
                            break
            if new_order is None:
                maximal = true
            else:
                order = new_order
        return order

"""
END NUMBER FIELD FUNCTIONS
"""
```

4.4.3 Moduln

```
"""
NUMBER FIELD MODULE (Last Update: 28.2.2013)
"""

from sage.modules.free_module import FreeModule_generic_pid

class NFModule(FreeModule_generic_pid):
```

```
#Konstruktor, generators: Liste von Elementen im gleichen
    Zahlkörper
def __init__(self, generators, number_field):
    #gram matrix is only calculated if needed
    self._gram_matrix = None
    #coordinate system is only calculated if needed
    self._cs = None
    self._number_field = number_field
    #ensures that the generators are in number_field (results in
        error if the generator elements cannot be converted to
        elements of number_field)
    self._gens = map(number_field, generators)
    self._calculate_basis()
    FreeModule_generic_pid.__init__(self, ZZ, self.rank(), self.
        _number_field.degree())

def __add__(module1, module2):
    if module1.number_field() != module2.number_field():
        raise NotImplementedError('Sum of modules in different
            number fields not implemented.')
    #the following + is a concatenation of lists
    return NFModule(module1.basis() + module2.basis(), module1.
        number_field())

def __contains__(self, element):
    element = self.number_field()(element)
    cs = self.coordinate_system()
    vector = cs[2](element)
    if vector is None:
        return false
    for i in vector:
        if not(i in ZZ):
            return false
    return true

def __eq__(self, module):
    if not(self.number_field() == module.number_field()):
        raise NotImplementedError('Comparison of two modules in
            different number fields not implemented.')
    b1 = self.number_field_basis()
    b2 = module.number_field_basis()
    if len(b1) != len(b2):
        return false
    for i in range(len(b1)):
        if not(b1[i] == b2[i]):
            return false
    return true

def __mul__(module1, module2):
    if module1.number_field() != module2.number_field():
        raise NotImplementedError('Product of modules in different
             number fields not implemented.')
    return NFModule([i*j for i in module1.number_field_basis() for
         j in module2.number_field_basis()], module1.number_field
        ())

def __ne__(self, module):
    return not(self == module)

#returns the coordinates of the module basis in the standard basis
     of the number field
def basis(self):
    return self._coord_basis

def coordinate_system(self):
    if self._cs is None:
        self._cs = NFFunctions.coordinate_system(self.number_field
            (), self.number_field_basis())
    return self._cs

def discriminant(self):
    return self.gram_matrix().determinant()
```

```
#Returns a basis of the number field (in standard coordinates),
    that contains all basis elements of self. This is done by
    adding appropriate elements of the standard basis of the
    number field.
def get_extended_basis(self):
    basis = self.basis()
    extended_basis = list()
    number_field = self.number_field()
    n = number_field.degree()
    k = 0
    for i in range(n):
        extend = false
        if k >= len(basis):
            extend = true
        elif basis[k][i] == 0:
            extend = true
        if extend:
            extended_basis = extended_basis + [[1 if j == i else 0
                for j in range(n)]]
        else:
            extended_basis = extended_basis + [basis[k]]
            k = k + 1
    return extended_basis

#Needed for discriminant
def gram_matrix(self):
    if self._gram_matrix is None:
        B = self.basis_matrix()
        I = self.inner_product_matrix()
        self._gram_matrix = B*I*B.transpose()
    return self._gram_matrix

def includes(self, module):
    for i in module.number_field_basis():
        if not(i in self):
            return false
    return true

def index_and_factor_module(module1, module2):
    if module1.number_field() != module2.number_field():
        raise NotImplementedError('Factor module of modules in
            different number fields not implemented.')
    if not(module1.includes(module2)):
        raise ValueError('module2 must be contained in module1 to
            create the factor module module1/module2')
    number_field = module1.number_field()
    B = module1.get_extended_basis()
    B2 = module2.number_field_basis()
    #Calculates coordinate vectors v of B2 in terms of basis B
    v = map(NFFunctions.coordinate_system(number_field, B)[2], B2)
    A = matrix(ZZ, len(v), v)
    S, U, V = A.smith_form()
    d = [S[i][i] for i in range(S.rank())]
    r1 = len(module1.basis())
    r2 = len(B2)
    factors = [Integers(di) for di in d if di != 1]
    if r1 == r2:
        if len(factors) == 0:
            factor_module = Integers(1)
        elif len(factors) == 1:
            factor_module = factors[0]
        else:
            factor_module = cartesian_product(factors)
        index = prod(d)
    else:
        if len(factors) == 0:
            factor_module = ZZ^(r1-r2)
        else:
            factor_module = cartesian_product([ZZ^(r1-r2)]+factors
                )
        index = Infinity
    return index, factor_module

#Needed for gram_matrix/discriminant
```

```
def inner_product_matrix(self):
    number_field = self.number_field()
    n = number_field.degree()
    nf_basis = NFFunctions.standard_basis(number_field)
    I = column_matrix(n, n, [[NFFunctions.multiplication_matrix(i*
        j, self.number_field()).trace() for i in nf_basis] for j
        in nf_basis])
    return I

def intersection(module1, module2):
    if module1.number_field() != module2.number_field():
        raise NotImplementedError('Intersection of modules in
            different number fields not implemented.')
    number_field = module1.number_field()
    b1 = module1.basis()
    b2 = module2.basis()
    if ((len(b1) == 0) or (len(b2) == 0)):
        return NFModule([0], number_field)
    #Calculates the least common denominator of all coordinate
        vectors in b1 and b2
    d = reduce(lambda x, y: lcm(x, denominator(y)), list(b1+b2),
        1)
    M1 = matrix(ZZ, [d*v for v in b1])
    M2 = matrix(ZZ, [d*v for v in b2])
    M3 = block_matrix([[M1, M1], [M2, 0]])
    M3 = M3.echelon_form()
    M3 = 1/d*M3
    n = number_field.degree()
    rows = M3.rows()
    for i in range(len(rows)):
        if [rows[i][j] for j in range(n)] == [0 for j in range(n)
            ]:
            i0 = i
            break
    Z = M3.submatrix(i0, n)
    c = map(number_field, Z.rows())
    #alt: cs = NFFunctions.coordinate_system(number_field)
    #alt: c = map(cs[1], Z.rows())
    return NFModule(c, number_field)

def is_fract_ideal(self, order):
    number_field = self.number_field()
    n = number_field.degree()
    omega = map(number_field, order.basis())
    for i in omega:
        for b in self.number_field_basis():
            if not(i*b in self):
                return false
    return true

def is_full(self):
    return self.rank() == self.degree()

def module_inverse(self, order):
    if self.number_field() != order.number_field():
        raise NotImplementedError('Module inverse in order with
            different number field not implemented.')
    return NFModule.quotient(NFModule(order.basis(), order.
        number_field()), self)

def module_order(self):
    quotient = NFModule.quotient(self, self)
    O = self.number_field().order(quotient.number_field_basis())
    return O

def number_field_basis(self):
    return self._nf_basis

def number_field(self):
    return self._number_field

def quotient(module1, module2):
    if module1.number_field() != module2.number_field():
```

```
            raise NotImplementedError('Quotient of modules in
                different number fields not implemented.')
        number_field = module1.number_field()
        B1 = module1.number_field_basis()
        B2 = module2.number_field_basis()
        if len(B2) == 0:
            raise ValueError('m1%m2 not defined for m2 = {0}')
        N = list()
        for b in B2:
            N = N + [NFModule([m/b for m in B1], number_field)]
        m = N[0]
        for i in range(1, len(N)):
            m = NFModule.intersection(m, N[i])
        return m

    def rank(self):
        return len(self._nf_basis)

    def scale(self, element):
        return NFModule(map(lambda x: element*x, self.
            number_field_basis()), self.number_field())

    def str(self):
        return 'NFModule(%s)'%self.number_field_basis()

    def _calculate_basis(self):
        cs = NFFunctions.coordinate_system(self._number_field)
        #Calculates the coordinate vectors of the generators
        vectors = map(cs[2], self._gens)
        #Calculates the least common multiple of the denominators of
            the coordinate vectors
        d = reduce(lambda x, y: lcm(x, denominator(y)), list(vectors),
             1)
        M = matrix(ZZ, len(vectors), [d*v for v in vectors])
        #Calculates the HNF of a matrix
        M = M.echelon_form()
        #Removes zero rows of a matrix in HNF
        M = M.submatrix(0, 0, M.rank(), M.ncols())
        basis_vectors = [1/d*z for z in M.rows()]
        self._coord_basis = basis_vectors
        self._nf_basis = map(cs[1], basis_vectors)

    #this function is called if you print a NFModule m with 'print m'
    def _repr_(self):
        s = 'NumberFieldModule(%s, %s)\nbasis matrix in standard
            coordinates:\n%s'%(self.number_field_basis(), self.
            number_field(), self.basis_matrix())
        return s


"""
END NUMBER FIELD MODULE
"""
```

4.4.4 Ideale

```
"""
NUMBER FIELD IDEAL (Last Update: 28.2.2013)
"""

from sage.rings.ideal import Ideal_generic

#ToDo: Nullidealabfragen überall einfügen, wo sie nötig sind
class NFFractionalIdealInOrder(Ideal_generic):
    def __init__(self, generators, order):
        self._number_field = order.number_field()
        self._gens = map(self._number_field, generators)
        self._module = NFModule(generators, self._number_field)*
            NFModule(order.basis(), self._number_field)
        self._order = order
        Ideal_generic.__init__(self, order, generators, false)

    def __add__(ideal1, ideal2):
```

```
    if not(ideal1.order() == ideal2.order()):
        raise NotImplementedError('Adding two ideals in different
            orders is not defined.')
    return NFFractionalIdealInOrder(ideal1.number_field_basis()+
        ideal2.number_field_basis(), ideal1.order())

def __contains__(self, element):
    return element in self.module()

def __eq__(self, ideal):
    if not(self.order() == ideal.order()):
        raise NotImplementedError('Comparing two ideals in
            different orders not defined. If you want to compare
            them as modules in a number field use (self.module()
            == ideal.module()).')
    return self.module() == ideal.module()

def __mul__(ideal1, ideal2):
    if not(ideal1.order() == ideal2.order()):
        raise NotImplementedError('Multiplying two ideals in
            different orders is not defined.')
    product_module = ideal1.module()*ideal2.module()
    return NFFractionalIdealInOrder(product_module.
        number_field_basis(), ideal1.order())

def basis(self):
    return self._module.basis()

def coprime(ideal1, ideal2):
    if not(ideal1.order() == ideal2.order()):
        raise NotImplementedError('Check if two ideals in
            different orders are coprime is not defined.')
    return ideal1 + ideal2 == NFFractionalIdealInOrder([1], ideal1
        .order())

#This function can only factorize the ideal by its invertible
    prime ideals. That means if p1, p2 are invertible and q is not
     invertible, then the factorization of p1^2*p2^3*q^4 is
    remainder*p1^2*p2^3 where remainder equals to q^4.
def factor(self):
    order = self.order()
    remainder = self
    d = self.module().discriminant()
    fact = d.factor()
    factors = list()
    for (p, e) in fact:
        if e >= 2:
            prime_ideals = NFFunctions.prime_ideals_above_p(p,
                order)
            for pr_id in prime_ideals:
                if pr_id.is_invertible():
                    (valuation, remainder) = remainder.
                        valuation_and_remainder(pr_id)
                    factors.append((pr_id, valuation))
    factors = [(remainder, 1)] + factors
    return factors

def generators(self):
    return self._gens

def includes(self, ideal):
    for i in ideal.number_field_basis():
        if not(i in self):
            return false
    return true

def inverse(self):
    pseudo_inverse = self.pseudo_inverse()
    if self*self.pseudo_inverse() == NFFractionalIdealInOrder([1],
         self.order()):
        return pseudo_inverse
    else:
        raise ValueError('Cannot calculate inverse of non-
            invertible ideal. If you wanted to calculate the ideal
```

```
                Order%self please use the function self.
                pseudo_inverse().')

    def is_integral(self):
        for b in self.number_field_basis():
            if not(b in self.order()):
                return false
        return true

    def is_invertible(self):
        ideal = self
        inverse = self.pseudo_inverse()
        a = ideal*inverse
        return a == NFFractionalIdealInOrder([1], self.order())

    def module(self):
        return self._module

    def number_field(self):
        return self._number_field

    def number_field_basis(self):
        return self._module.number_field_basis()

    def order(self):
        return self._order

    def valuation_and_remainder(self, invertible_ideal):
        if not(self.order() == invertible_ideal.order()):
            raise NotImplementedError('Valuation only defined for
                ideals that are in the same order as the valuation
                ideal.')
        number_field = self.number_field
        ideal = self
        inverse = invertible_ideal.inverse()
        if ideal*inverse == ideal:
            return Infinity, self
        nu = 0
        while invertible_ideal.includes(ideal):
            nu = nu+1
            ideal = ideal*inverse
        return nu, ideal

    def pseudo_inverse(self):
        order = self.order()
        return NFFractionalIdealInOrder(self.module().module_inverse(
            order).basis(), order)

    def reduce(self, element):
        number_field = self.number_field()
        element = number_field(element)
        cs = self.module().coordinate_system()
        vector = cs[2](element)
        reduced_vector = list()
        for i in range(len(vector)):
            reduced_vector = reduced_vector + [vector[i] - ((vector[i
                ]-1/2).round('up'))]
        reduced_element = cs[1](reduced_vector)
        return reduced_element

    def scale(self, element):
        return NFFractionalIdealInOrder(map(lambda x: element*x, self.
            number_field_basis()), self.order())

    def str(self):
        a = tuple(self.number_field_basis())
        return str(a)

"""
END NUMBER FIELD IDEAL
"""
```

Kapitel 5

Zusammenfassung

Im Verlauf von Kapitel 3 wurde festgestellt, dass man ein invertierbares Primideal $\mathfrak{p}$ aus einem Ideal $\mathfrak{a}$ herausfaktorisieren kann, indem man $\mathfrak{a}$ mit dem Inversen von $\mathfrak{p}$ multipliziert, bis $\mathfrak{a}$ nicht mehr in $\mathfrak{p}$ enthalten ist. Dieses Vorgehen funktioniert in beliebigen Ordnungen und liefert die Exponenten aller invertierbaren Primideale in einer Idealzerlegung. Die Exponenten von nicht-invertierbaren Primidealen lassen sich nicht auf diese Weise bestimmen und es ist auch zunächst nicht klar, ob es überhaupt eine vollständige Zerlegung in Primideale gibt.

Da in der Maximalordnung $\mathcal{O}_K$ alle Primideale invertierbar sind, kann man in $\mathcal{O}_K$ alle Primideale herausfaktorisieren und erhält dadurch eine vollständige Zerlegung jedes Ideals in Primideale. In einer nicht-maximalen Ordnung $\mathcal{O}$ gibt es aber mindestens eine Primzahl p, so dass $\mathcal{O}$ nicht p-maximal ist. Damit gibt es auch mindestens ein Primideal $\mathfrak{p}$ über p, das nicht invertierbar ist. Jedes Ideal $\mathfrak{a}$, das in $\mathfrak{p}$ enthalten ist, kann man mit dem angegebenen Algorithmus nur teilweise in Primideale zerlegen, das heißt es bleibt bei der Zerlegung ein Restideal, das im Allgemeinen kein Primideal ist. Sowohl die vollständige Zerlegung als auch die teilweise Zerlegung in Primideale sind aber bis auf die Reihenfolge der Faktoren eindeutig.

Während man invertierbare Primideale für die Zerlegung von Idealen verwenden kann, kann man nicht-invertierbare Primideale dafür verwenden, die Maximalordnung zu bestimmen. Dies geschieht schrittweise mit dem vorgestellten Algorithmus von Zassenhaus. Die Invertierbarkeit von Primidealen lässt sich durch einige Äquivalenzen feststellen, die ebenfalls in diesem Kapitel gezeigt wurden.

In Kapitel 4 wurden Algorithmen für die Idealarithmetik und die Primidealzerlegung zunächst mathematisch beschrieben und bewiesen und dann in Sage (siehe [S$^+$09]) implementiert. Da Ideale und Ordnungen in Zahlkörpern freie $\mathbb{Z}$-Moduln sind, kann man mit Hilfe von Koordinatensystemen die Idealarithmetik zu einem großen Teil durch Matrizen mit Koeffizienten in $\mathbb{Z}$ darstellen. Durch Berechnungen in der Sage-Implementierung wurde

ein Beispiel für ein Ideal in einer nicht-maximalen Ordnung gefunden, bei dem eine Primidealzerlegung nicht möglich ist (vergleiche Beispiel 3.3.25). Dadurch wurde gezeigt, dass sich Ideale in nicht-maximalen Ordnungen im Allgemeinen nicht vollständig in Primideale zerlegen lassen - unabhängig vom Verfahren, das man für die Zerlegung verwendet.

Literaturverzeichnis

[BBR09] M. P. Brodmann, R. Boldini, and F. Rohrer, *Kommutative Algebra*, Universität Zürich, March 12, 2009. Vorlesungsskript[1].

[Fis08] G. Fischer, *Lineare Algebra*, Vieweg+Teubner Verlag, Wiesbaden, 2008. (16. Auflage).

[Fis11] ———, *Lehrbuch der Algebra*, Vieweg+Teubner Verlag, Wiesbaden, 2011. (2., überarbeitete Auflage).

[FS78] G. Fischer and R. Sacher, *Einführung in die Algebra*, Teubner, Stuttgart, 1978.

[Ger09] R. Gerkmann, *Algebraische Zahlentheorie I*, Johannes-Gutenberg-Universität, July 22, 2009. Vorlesungsskript.

[Kir04] M. Kirschmer, *Bewertungsringe, Dedekindringe, diskrete Bewertungen und gebrochene Ideale*[2], Universität Ulm, December 21, 2004.

[NW10] M. A. Nieper-Wißkirchen, *Algebra II*, Universität Augsburg, March 19, 2010. Vorlesungsskript[3].

[S+09] W. A. Stein et al., *Sage Mathematics Software (Version 5.4)*, The Sage Development Team, 2012, `http://www.sagemath.org`.

[1] http://www.math.uzh.ch/fileadmin/user/brodmann/publikation/Ka.Skript.5.Mai.09.pdf

[2] http://www.mathematik.uni-ulm.de/ReineMath/mitarbeiter/koenigsmann/ws04/files/kirschmer.pdf

[3] http://alg.math.uni-augsburg.de/lehre/vorlesungsskripte/script.pdf/at_download/file

Stichwortverzeichnis

algebraisch, 27, 61

Basismatrix, 101
Basisprimzahl, 79, 80, 122
Bewertung, 70–77
    an Primidealen, 86, 87, 90, 123
    diskrete, 75, 77, 86
    nicht-triviale, 73
    triviale, 73
Bewertungsring, 73–77, 87
    diskreter, 75, 88

Chinesischer Restsatz, 31–33, 95–96

Darstellungsmatrix
    der Spurform, 59, 64
    einer linearen Abbildung, 99
Diskriminante, 60, 64, 79, 80
Diskriminanten-Index-Formel, 64, 66, 79, 80

Erweiterung, 9–12, 22, 23, 87
Erzeugermatrix, 100, 101
Euklidischer Algorithmus, 28–30, 34, 40
    erweiterter, 30, 57, 120

Faktormodul, 13–18, 119
Faktorring, 19–21, 32, 47, 49, 80
Frobenius-Homomorphismus, 53, 55, 122
Führer, 67, 92, 93, 95

ganz, *siehe* Ganzheit
Ganzheit, 25, 26, 28, 66, 80
Ganzheitsring, *siehe* Maximalordnung
Grad
    einer Körpererweiterung, 27, 78, 79

Hauptideal, 68
Hermite-Normalform, 37–40, 101, 108–111, 116, 117
Homomorphiesatz, 13

Ideal
    erweitertes, 9, 22
    ganzzahliges, 68–70, 80, 90, 92, 93, 95
    gebrochenes, 68–70, 94, 95
    kontrahiertes, 10, 22
idempotent, 55–59
    nicht-trivial, 55
    trivial, 55
idempotentes Element, *siehe* idempotent
Index, 13, 16, 49, 78, 79, 95, 119
invertierbar, 69

Jacobson-Radikal, 50–54, 57, 83

Kontraktion, 9–12, 22, 79, 92
Koordinaten
    -abbildung, 98
    -raum, 98
    -system, 98
        Standard-, 98
    -vektor, 98

Lemma von Bézout, 30
Lemma von Zorn, 7, 44, 50, 52, 66, 80, 83
Lokalisierung, 21–24
    an Primidealen, 23, 24, 83, 87–89

Maximalordnung, 66, 67, 92, 94–96
Minimalpolynom, 25–27, 56–57, 79
Minor, 41, 42
Modul
    artinscher, 43–47, 57
    einfacher, 44, 55–59, 120
    freier, 48, 62
    halbeinfacher, 44, 55–59, 120
    in Zahlkörper, 62–64
    noetherscher, 43–47
    torsionsfreier, 48
    vollständiger, 62–66, 69, 78

multiplikativ, 21

Nakayama's Lemma, 51, 83
nilpotent, 50
Nilradikal, 50–54
Norm, 59
normiert, 37
Nullspalte, 33
Nullzeile, 33

Ordnung
    eines Moduls, 65, 66, 81–83
    in Zahlkörper, 65–68

p-maximal, 95, 96
Primelement, 76, 77, 88
Primideal
    über Primzahl, 78–80
    invertierbares, 81–83, 88, 92, 95–96

Quotient
    von Moduln, 63, 65, 67, 70, 120
Quotientenkörper, 22, 73–75
Quotientenring, *siehe* Faktorring

Radikal, 50
Rang
    eines Moduls, 36, 49, 62
Restklassenring, *siehe* Faktorring
Ring
    artinscher, 44, 46, 47, 52, 58
    lokaler, 23, 24, 87
    noetherscher, 44, 46, 47, 65, 80, 83, 123

Sequenz
    exakte, 45
Smith-Normalform, 40–43, 48, 49, 64, 78, 112–116, 119
Spaltenende, 33
Spur, 59
Spurform, 59
Standardbasis
    eines Zahlkörpers, 98
Stufenelement, 34
Stufenspalte, 34

teilerfremd, 31
Transformationsmatrix, 100

Wert
    an Primidealen, 84, 86

Zahlkörper, 61
Zeilenanfang, 33
Zeilenmodul, 35–37, 39, 48
Zeilenstufenform, 33–37