Berechnung relativer Ganzheitsbasen mit dem Round-2-Algorithmus

Diplomarbeit
von
Carsten Friedrichs
aus Detmold

Angefertigt am Fachbereich 3 Mathematik
der Technischen Universität Berlin 1997
überarbeitet 1998

Inhaltsverzeichnis

Kapitel I
Einleitung

Diese Arbeit beschäftigt sich mit der Berechnung von *ganzen algebraischen Zahlen,* das sind die komplexen Zahlen, die Nullstelle eines normierten Polynoms mit ganzzahligen Koeffizienten sind. Neben den gewöhnlichen *ganzen Zahlen* $0, 1, -1, 2, -2, 3, -3, \ldots$ gehören auch die Zahlen der Form $a+b\cdot\sqrt{-1}$ zu den ganzen algebraischen Zahlen, wobei sowohl a als auch b wieder ganze Zahlen sind. Diese Zahlen heißen *ganze Gaußsche Zahlen.* Die ganzen algebraischen Zahlen eines Zahlkörpers bilden einen Ring, die *Maximalordnung* des Zahlkörpers.

Es stellt sich die Frage, wie die Maximalordnung dargestellt werden kann. Häufig wird sie durch eine sogenannte *absolute Basis,* eine Basis über dem Ring der ganzen Zahlen, dargestellt. Eine solche Basis heißt *Ganzheitsbasis* des Zahlkörpers. Eine Hauptaufgabe der konstruktiven Zahlentheorie ist die Berechnung einer Ganzheitsbasis des Zahlkörpers, denn mit ihr kann man unter anderem die *Diskriminante* des Zahlkörpers berechnen.

Zur Berechnung der Ganzheitsbasis eines Zahlkörpers werden vor allem die beiden Algorithmen Round-2 und Round-4 verwendet, die theoretisch immer ein Ergebnis liefern. In der Praxis stößt man aber ziemlich schnell an die Grenzen dieser Algorithmen, die zum Beispiel im Grad der Körpererweiterung liegen.

Kennt man einen Teilkörper des Zahlkörpers, so möchte man diese Information natürlich ausnutzen, indem man den ursprünglichen Zahlkörper als Erweiterung des bekannten Teilkörpers betrachtet. Man erhofft sich dann eine Vereinfachung, da die Berechnung einer Ganzheitsbasis des Teilkörpers im allgemeinen nicht so aufwendig sein sollte. Versucht man aber eine *relative Ganzheitsbasis* des Zahlkörpers zu berechnen, das ist eine Basis der Maximalordnung des Zahlkörpers über der Maximalordnung des Teilkörpers, so wird man sehr häufig enttäuscht, denn eine relative Ganzheitsbasis muß nicht existieren.

Dennoch kann man die Maximalordnung eines Zahlkörpers auch relativ zu seinem Teilkörper darstellen: mit einer sogenannten *Pseudobasis*, die neben *Basiselementen* auch *Koeffizientenideale* enthält. In dieser Arbeit wird der bekannte Round-2-Algorithmus für Relativerweiterungen entwickelt.

Aus einer Pseudobasis der Maximalordnung kann man, wenn eine relative Ganzheitsbasis des Zahlkörpers existiert, eine solche berechnen. Durch Kombination mit einer Ganzheitsbasis des Teilkörpers erhält man dann eine Ganzheitsbasis des Zahlkörpers. Diese Methode ist häufig sehr viel günstiger als die direkte Berechnung einer Ganzheitsbasis.

Ein Schwerpunkt dieser Arbeit liegt in der Implementierung dieses Verfahrens in dem Computeralgebrasystem KANT-V4 [DFK+97], das die oben aufgeführten Algorithmen für die absolute Betrachtung bereits enthält. Bei dem Versuch, die bisher bekannten Ergebnisse auf Relativerweiterungen zu übertragen, treten eine Reihe von Problemen auf, die in erster Linie mit der Darstellung von Ordnungen in Relativerweiterungen zusammenhängen. Deshalb besteht diese Arbeit neben einem theoretischen aus einem konstruktiven Teil, der viele Aspekte zur Implementierung enthält. Einige Ergebnisse dieser Implementierung sind in Form von Beispielrechnungen aufgeführt, die mit dem Computeralgebrasystem KANT-V4 in der Oberfläche KASH ausgeführt wurden.

Bei der Implementierung fiel auf, daß ein wesentlicher Teil des Round-2-Algorithmus der *Division* und *Invertierung* von *relativen Idealen* sehr ähnlich ist. Bisher war die Invertierung und damit auch die Division von relativen Idealen in dem Computeralgebrasystem KANT-V4 nur bedingt möglich. Mit den neuen Methoden, die im Anhang dieser Arbeit festgehalten werden, können auch beliebige relative Ideale invertiert und die Division von relativen Idealen sogar direkt ausgeführt werden, das heißt, ohne vorher das Nenner-Ideal zu invertieren und danach mit dem Zähler-Ideal zu multiplizieren.

Ich danke Herrn Professor M. Pohst für die Bereitstellung des interessanten Themas sowie die Unterstützung bei dieser Arbeit. Weiterhin bedanke ich mich bei den Mitgliedern der KANT-Gruppe und insbesondere bei Claus Fieker für seine ständige Diskussionsbereitschaft und seine TEX-Ratschläge.

Mein Dank gilt schließlich meinen Eltern, die mir das Studium ermöglichten, und meiner Freundin Susanne für das Verständnis, das sie für mich und meine Arbeit aufgebracht hat.

Die vorliegende Arbeit ist die überarbeitete Version der ursprünglichen Diplomarbeit, die um ein zweites Verfahren zur Berechnung des $\mathfrak{p}$-Radikals für große $\mathfrak{p}$ erweitert wurde.

Kapitel II
Grundlagen

Die in diesem Kapitel aufgeführten Definitionen und Sätze in Verbindung mit algebraischen Zahlkörpern findet man in vielen Standardwerken der algebraischen Zahlentheorie [Poh93, PZ89, Coh93, Nar89, Neu92].

Die in diesem Abschnitt verwendeten Ringe sind stets Integritätsringe mit Eins.

II.1 Algebraische Zahlkörper

Es sei $\mathcal{F}/\mathbb{Q}$ eine endliche Körpererweiterung, wobei

$$\mathbb{Q} \subset \mathcal{F} \subset \mathbb{C}$$

gelte. Der Körper $\mathcal{F}$ heißt auch *algebraischer Zahlkörper.* Die Körpererweiterung $\mathcal{F}/\mathbb{Q}$ wird von einem Element $\theta \in \mathcal{F}$ erzeugt, wobei θ Nullstelle eines irreduziblen und normierten Polynoms $T_\mathcal{F}$ mit Koeffizienten aus $\mathbb{Z}$ ist. Es gilt

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

Es sei weiterhin

$$m := [\mathcal{F} : \mathbb{Q}] = \deg(T_\mathcal{F}),$$

der Grad der Körpererweiterung.

Die Elemente $x \in \mathcal{F}$ heißen *algebraische Zahlen.* Für eine algebraische Zahl $x \in \mathcal{F}$ definiert man die zwei folgenden Begriffe:

Definition II.1 *Die* Norm *und die* Spur *einer algebraischen Zahl $x \in \mathcal{F}$ sind durch die Determinante und die Spur der linearen Transformation*

$$\psi_{x,\mathbb{Q}} : \mathcal{F} \to \mathcal{F},$$

$$\psi_{x,\mathbb{Q}} : y \longmapsto x \cdot y$$

des $\mathbb{Q}$-Vektorraumes $\mathcal{F}$ gegeben. Sie werden mit

$$\mathrm{N}_{\mathcal{F}/\mathbb{Q}}(x) := \det(\psi_{x,\mathbb{Q}})$$

und

$$\mathrm{Tr}_{\mathcal{F}/\mathbb{Q}}(x) := \mathrm{Trace}(\psi_{x,\mathbb{Q}})$$

bezeichnet.

Das Polynom $T_\mathcal{F}$ zerfällt über $\mathbb{C}$ in Linearfaktoren:

$$T_\mathcal{F}(t) = \prod_{i=1}^{m} (t - \theta^{(i)}),$$

wobei die Nullstellen $\theta^{(i)}$ so numeriert seien, daß $\theta^{(1)} = \theta$ gelte. Für $1 \le i \le m$ heißt $\theta^{(i)}$ die *i-te Konjugierte* von θ, der *i-te Konjugiertenkörper* ist definiert als

$$\mathcal{F}^{(i)} := \mathbb{Q}(\theta^{(i)}).$$

Weiterhin sei für $1 \le i \le m$ die *i-te Konjugierten-Abbildung* definiert durch:

$$.^{(i)} : \mathcal{F} \to \mathcal{F}^{(i)}$$

$$.^{(i)} : x = x_1 + x_2\theta + \ldots + x_m\theta^{m-1} \longmapsto x^{(i)} := x_1 + x_2\theta^{(i)} + \ldots + x_m{\theta^{(i)}}^{m-1}.$$

Die i-te Konjugierten-Abbildung $.^{(i)}$ ist ein $\mathbb{Q}$-Isomorphismus von $\mathcal{F}$ in $\mathcal{F}^{(i)}$.

Satz II.2 *Es gilt*

$$\mathrm{Tr}_{\mathcal{F}/\mathbb{Q}}(x) = \sum_{i=1}^{m} x^{(i)},$$

und man sieht, daß die Spur eine $\mathbb{Q}$-lineare Abbildung von $\mathcal{F}$ in $\mathbb{Q}$ ist.

Satz II.3 *Es gilt*

$$\mathrm{N}_{\mathcal{F}/\mathbb{Q}}(x) = \prod_{i=1}^{m} x^{(i)}.$$

Die Norm ist folglich multiplikativ $\left(\mathrm{N}_{\mathcal{F}/\mathbb{Q}}(xy) = \mathrm{N}_{\mathcal{F}/\mathbb{Q}}(x) \cdot \mathrm{N}_{\mathcal{F}/\mathbb{Q}}(y)\right)$.

Mit den Abbildungen $.^{(1)}, \ldots, .^{(m)}$ erhält man die folgende Darstellung für das charakteristische Polynom:

Satz II.4 *Es sei $x \in \mathcal{F}$. Für das charakteristische Polynom von x über $\mathbb{Q}$ gilt:*

$$m_x(t) = \prod_{i=1}^{m} \left(t - x^{(i)}\right).$$

Mit der Spur kann die sogenannte Diskriminante definiert werden:

Definition II.5 *Bilden die Elemente $x_1, \ldots, x_m$ eine $\mathbb{Q}$-Basis von $\mathcal{F}$, so definiert man die* Diskriminante *von $x_1, \ldots, x_m$ wie folgt:*

$$\mathrm{disc}_{\mathcal{F}/\mathbb{Q}}(x_1, \ldots, x_m) := \det\left(\mathrm{Tr}_{\mathcal{F}/\mathbb{Q}}(x_i \cdot x_j)_{1 \le i,j \le m}\right).$$

Man sieht, daß die Diskriminante der Elemente $x_1, \ldots, x_m \in \mathcal{F}$ ein Element aus $\mathbb{Q}$ ist.

II.2 Ganze algebraische Zahlen

Zuerst wird der Begriff der ganzen algebraischen Zahl eingeführt:

Definition II.6 *(1) Eine algebraische Zahl $x \in \mathcal{F}$ heißt* ganze algebraische Zahl *(oder einfach nur* ganz*), wenn ein normiertes Polynom $f \in \mathbb{Z}[t]$ existiert mit*

$$f(x) = 0.$$

(2) Man definiert die Menge der ganzen algebraischen Zahlen von $\mathcal{F}$ *als:*

$$\mathfrak{o}_\mathcal{F} := \{x \in \mathcal{F} \mid x \textit{ ist ganz algebraisch}\}.$$

Die Menge der ganzen Zahlen $\mathfrak{o}_\mathcal{F}$ bildet einen Dedekindring. Eine der wesentlichen Eigenschaften eines Dedekindringes ist die eindeutige Zerlegung gebrochener Ideale in Primideale. Dazu wird zunächst der Begriff des gebrochenen Ideals erklärt.

Definition II.7 *Es sei $Q(R)$ der Quotientenkörper des Ringes R. Eine Teilmenge $\mathfrak{b} \subseteq Q(R)$ heißt* gebrochenes Ideal *von R, wenn ein Element $d \in R \setminus \{0\}$ und ein Ideal $\mathfrak{a} \subseteq R$ existieren mit*

$$\mathfrak{b} = \frac{1}{d} \cdot \mathfrak{a}.$$

Im folgenden ist mit einem Ideal $\mathfrak{a}$ in R immer ein gebrochenes Ideal $\neq \{0\}$ gemeint. Ein Ideal mit $\mathfrak{a} \subseteq R$ wird *ganzes Ideal* genannt und ein Primideal $\mathfrak{p}$ wird immer ein Primideal im üblichen Sinne sein. $\mathfrak{p}$ ist damit insbesondere ein ganzes Ideal. Die Aussage über die Primidealzerlegung kann man jetzt wie folgt formulieren:

Satz II.8 *Ist R ein Dedekindring, so gelten:*

(1) Die Ideale von R bilden eine multiplikative Gruppe.

(2) Für jedes Ideal $\mathfrak{a}$ in R existiert eine (bis auf die Reihenfolge) eindeutige Zerlegung in Primideale:

$$\mathfrak{a} = \mathfrak{p}_1^{e_1} \cdot \ldots \cdot \mathfrak{p}_s^{e_s},$$

wobei $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ paarweise verschiedene Primideale von R sind und die Exponenten $e_1, \ldots, e_s$ ganze Zahlen $\neq 0$ sind. Ist $\mathfrak{a}$ ein ganzes Ideal, so sind $e_1, \ldots, e_s$ positiv.

In einem Dedekindring kann man den Begriff der Teilbarkeit wie folgt definieren:

Definition II.9 *Es seien $\mathfrak{a}, \mathfrak{b}$ Ideale in dem Dedekindring R. Man sagt, daß $\mathfrak{a}$ das Ideal $\mathfrak{b}$* teilt $(\mathfrak{a} \mid \mathfrak{b})$, *wenn ein ganzes Ideal $\mathfrak{c}$ in R existiert mit*

$$\mathfrak{a} \cdot \mathfrak{c} = \mathfrak{b}.$$

Der Ring der ganzen Zahlen $o_\mathcal{F}$ ist zudem ein endlich erzeugter $\mathbb{Z}$-Modul vom Rang m. $o_\mathcal{F}$ kann daher durch eine $\mathbb{Z}$-Basis dargestellt werden:

$$o_\mathcal{F} = \mathbb{Z}\omega_1 + \ldots + \mathbb{Z}\omega_m,$$

wobei die Elemente $\omega_1, \ldots, \omega_m$ aus $o_\mathcal{F}$ stammen. Eine $\mathbb{Z}$-Basis von $o_\mathcal{F}$ heißt *absolute Ganzheitsbasis*. Eine wichtige Invariante des Zahlkörpers $\mathcal{F}$ ist seine Körperdiskriminante:

Definition II.10 *Ist $\omega_1, \ldots, \omega_m$ eine absolute Ganzheitsbasis von $\mathcal{F}$, so wird die* Körperdiskriminante $\mathfrak{d}_{\mathcal{F}/\mathbb{Q}}$ *definiert durch:*

$$\mathfrak{d}_{\mathcal{F}/\mathbb{Q}} := \operatorname{disc}_{\mathcal{F}/\mathbb{Q}}(\omega_1, \ldots, \omega_m).$$

Die Körperdiskriminante ist unabhängig von der Wahl der absoluten Ganzheitsbasis.

II.3 Absolute Ordnungen

Definition II.11 *Ein unitärer Teilring $\mathcal{O}$ von $o_\mathcal{F}$ heißt* absolute Ordnung *von $\mathcal{F}$, wenn $\mathcal{O}$ ein freier $\mathbb{Z}$-Modul vom Rang m ist.*

Im vorangegangenen Abschnitt wurde darauf hingewiesen, daß $o_\mathcal{F}$ ein freier $\mathbb{Z}$-Modul vom Rang m ist. Damit ist der Ring der ganzen Zahlen $o_\mathcal{F}$ auch eine absolute Ordnung von $\mathcal{F}$. Da keine größere („$\subset$") absolute Ordnung von $\mathcal{F}$ existiert, wird $o_\mathcal{F}$ auch *Maximalordnung* genannt. Die Menge

$$\mathbb{Z}[\theta] = \mathbb{Z} + \mathbb{Z}\theta + \ldots + \mathbb{Z}\theta^{m-1}$$

ist auch eine absolute Ordnung in $\mathcal{F}$. $\mathbb{Z}[\theta]$ heißt *Gleichungsordnung zu θ*. Wie die Maximalordnung kann jede absolute Ordnung $\mathcal{O}$ von $\mathcal{F}$ durch eine $\mathbb{Z}$-Basis dargestellt werden:

$$\mathcal{O} = \mathbb{Z}\omega_1 + \ldots + \mathbb{Z}\omega_m.$$

Zum Nachweis einer absoluten Ordnung kann der folgende Satz verwendet werden:

Satz II.12 *Eine Teilmenge $\mathcal{O} \subset \mathcal{F}$ ist genau dann eine absolute Ordnung in $\mathcal{F}$, wenn $\mathcal{O}$ sowohl ein Teilring von $o_\mathcal{F}$ als auch ein Oberring einer geeigneten Gleichungsordnung ist.*

Algebraische Zahlen, die nicht ganz sind, können immer in einfacher Weise durch eine ganze algebraische Zahl und einen ganzzahligen Nenner dargestellt werden:

Satz II.13 *Es sei $\omega_1, \ldots, \omega_m$ eine $\mathbb{Z}$-Basis einer absoluten Ordnung $\mathcal{O}$ von $\mathcal{F}$. Für eine beliebige algebraische Zahl $x \in \mathcal{F}$ erhält man immer eine Darstellung*

$$x = \frac{\operatorname{num}(x)}{\operatorname{den}(x)},$$

mit den Eigenschaften

(1) $\operatorname{num}(x) = x_1\omega_1 + \ldots + x_m\omega_m \in \mathcal{O}$,

(2) $\operatorname{den}(x) \in \mathbb{Z}^{>0}$ *und*

(3) $\gcd(\operatorname{den}(x), x_1, \ldots, x_m) = 1$.

Ein Ideal $\mathfrak{a}$ in einer beliebigen absoluten Ordnung $\mathcal{O}$ von $\mathcal{F}$ ist auch ein freier $\mathbb{Z}$-Modul vom Rang n. Es kann also durch eine $\mathbb{Z}$-Basis dargestellt werden:

$$\mathfrak{a} = \mathbb{Z}\eta_1 + \ldots + \mathbb{Z}\eta_m,$$

wobei die Elemente $\eta_1, \ldots, \eta_m$ aus $\mathfrak{a}$ stammen.

Für Ideale $\mathfrak{a}$ in der Maximalordnung $o_\mathcal{F}$ von $\mathcal{F}$ gibt es noch eine weitere Darstellung:

$$\mathfrak{a} = a_1 \cdot o_\mathcal{F} + a_2 \cdot o_\mathcal{F},$$

mit Elementen $a_1, a_2 \in \mathfrak{a}$, $a_1, a_2 \neq 0$. Eine solche Darstellung nennt man *2-Element-Darstellung*.

Eine besondere Form der 2-Element-Darstellung liefert:

Satz II.14 *Es seien $\mathfrak{a}_1, \ldots, \mathfrak{a}_r$ Ideale in der Maximalordnung $o_\mathcal{F}$ von $\mathcal{F}$. Dann existieren Elemente $a_{i,1}, a_{i,2} \in \mathfrak{a}_i$, $a_{i,1}, a_{i,2} \neq 0$, $(1 \leq i \leq r)$, so daß gelten:*

$$\mathfrak{a}_i = a_{i,1} \cdot o_\mathcal{F} + a_{i,2} \cdot o_\mathcal{F},$$

$$\prod_{i=1}^r \mathfrak{a}_i = \left(\prod_{i=1}^r a_{i,1}\right) \cdot o_\mathcal{F} + \left(\prod_{i=1}^r a_{i,2}\right) \cdot o_\mathcal{F},$$

$$\left(\prod_{i=1}^r \mathfrak{a}_i\right)^2 = \left(\prod_{i=1}^r a_{i,1}\right)^2 \cdot o_\mathcal{F} + \left(\prod_{i=1}^r a_{i,2}\right)^2 \cdot o_\mathcal{F}.$$

Für Primideale in absoluten Ordnungen gilt der wichtige Satz:

Satz II.15 *Sei $\mathcal{O}$ eine absolute Ordnung von $\mathcal{F}$. Dann ist jedes Primideal in $\mathcal{O}$ bereits ein maximales Ideal in $\mathcal{O}$.*

Ein wichtiger Begriff, der bisher noch fehlt, ist die Norm von Idealen in absoluten Ordnungen. Bevor er eingeführt wird, sei zunächst bemerkt, daß nach Satz II.15 für ein Primideal $\mathfrak{p}$ in einer absoluten Ordnung $\mathcal{O}$ von $\mathcal{F}$, der Körper $\mathcal{O}/\mathfrak{p}$ immer endlich ist. Außerdem existiert in $\mathfrak{p}$ eine eindeutig bestimmte Primzahl p. Man kann sogar zeigen, daß für ein geeignetes $k > 0$

$$\sharp(\mathcal{O}/\mathfrak{p}) = p^k$$

gilt. Ist $\mathfrak{a}$ ein ganzes Ideal in $\mathcal{O}$, so ist der Ring $\mathcal{O}/\mathfrak{a}$ auch endlich. Damit kann man die Idealnorm für beliebige Ideale in absoluten Ordnungen wie folgt definieren:

Definition II.16 *(1) Für ein ganzes Ideal $\mathfrak{a}$ in einer absoluten Ordnung $\mathcal{O}$ von $\mathcal{F}$ ist die* Idealnorm *definiert als:*

$$\mathrm{N}_{\mathcal{F}/\mathbb{Q}}(\mathfrak{a}) := \sharp(\mathcal{O}/\mathfrak{a}).$$

(2) Für ein beliebiges Ideal $\mathfrak{b}$ in einer absoluten Ordnung $\mathcal{O}$ von $\mathcal{F}$ mit einer Darstellung

$$\mathfrak{b} = \frac{1}{d} \cdot \mathfrak{a},$$

wobei $d > 0$ eine ganze Zahl und $\mathfrak{a}$ ein ganzes Ideal in $\mathcal{O}$ sind, ist die Idealnorm *definiert als:*

$$\mathrm{N}_{\mathcal{F}/\mathbb{Q}}(\mathfrak{b}) := \left(\frac{1}{d}\right)^m \cdot \mathrm{N}_{\mathcal{F}/\mathbb{Q}}(\mathfrak{a}).$$

Die Idealnorm hat die folgenden Eigenschaften:

Satz II.17 *Sei $\mathcal{O}$ eine absolute Ordnung in $\mathcal{F}$. Dann gelten:*

(1) Die Idealnorm ist multiplikativ:

$$\mathrm{N}_{\mathcal{F}/\mathbb{Q}}(\mathfrak{a}\mathfrak{b}) = \mathrm{N}_{\mathcal{F}/\mathbb{Q}}(\mathfrak{a}) \cdot \mathrm{N}_{\mathcal{F}/\mathbb{Q}}(\mathfrak{b})$$

für beliebige Ideale $\mathfrak{a}, \mathfrak{b}$ in der Maximalordnung $o_\mathcal{F}$,

(2)

$$\mathrm{N}_{\mathcal{F}/\mathbb{Q}}(\mathfrak{a}) \in \mathfrak{a}$$

für ein ganzes Ideal $\mathfrak{a}$ in $\mathcal{O}$,

(3)

$$\mathrm{N}_{\mathcal{F}/\mathbb{Q}}(\alpha\mathcal{O}) = \left|\mathrm{N}_{\mathcal{F}/\mathbb{Q}}(\alpha)\right|$$

für eine beliebige algebraische Zahl $\alpha \in \mathcal{F}$.

Zum Abschluß dieses Abschnitts werden zwei Sätze angeführt, die nur bedingt in Verbindung zu absoluten Ordnungen stehen:

Satz II.18 *Sei R ein beliebiger Ring. Ist $x \in R$ in jedem Primideal von R enthalten, so ist x nilpotent.*

Satz II.19 *Es seien R ein beliebiger Ring, $\mathfrak{a}$ ein ganzes Ideal in R und*

$$\varphi : R \to R/\mathfrak{a}$$

$$\varphi : x \longmapsto x + \mathfrak{a}$$

der kanonische Ringhomomorphismus. Weiterhin seien $\mathcal{I}_R^{\mathfrak{a}}$ die Menge der ganzen Ideale von R, die $\mathfrak{a}$ enthalten, und $\mathcal{I}_{R/\mathfrak{a}}$ die Menge der ganzen Ideale in $R/\mathfrak{a}$. Dann gelten:

(1) Die Abbildung

$$\psi : \mathcal{I}_R^{\mathfrak{a}} \to \mathcal{I}_{R/\mathfrak{a}}$$

$$\psi : \mathfrak{b} \longmapsto \varphi(\mathfrak{b}) = \mathfrak{b} + \mathfrak{a}$$

ist bijektiv.

(2) ψ ist eine Bijektion zwischen den Primidealen in R, die das Ideal $\mathfrak{a}$ enthalten, und den Primidealen von $R/\mathfrak{a}$.

II.4 Exponentielle Bewertungen

In diesem Abschnitt wird eine kurze Einführung in die Bewertung von Zahlkörpern gegeben.

Definition II.20 *Es seien $\mathcal{I}_{\mathcal{F}}$ die Menge der Ideale in $o_{\mathcal{F}}$ und $\mathfrak{p}$ ein Primideal in $o_{\mathcal{F}}$. Die durch*

$$\nu_{\mathfrak{p}} : \mathcal{I}_{\mathcal{F}} \to \mathbb{Z}$$

$$\nu_{\mathfrak{p}} : \mathfrak{a} \longmapsto \max\{k \in \mathbb{Z} : \mathfrak{p}^k | \mathfrak{a}\}$$

definierte Abbildung heißt $\mathfrak{p}$-exponentielle Bewertung *von $\mathcal{I}_{\mathcal{F}}$.*

Man kann die $\mathfrak{p}$-*exponentielle Bewertung* auch auf $\mathcal{F}$ definieren:

Definition II.21 *Sei $\mathfrak{p}$ ein Primideal in $o_{\mathcal{F}}$. Dann heißt die Abbildung*

$$\nu_{\mathfrak{p}} : \mathcal{F} \to \mathbb{Z}$$

$$\nu_{\mathfrak{p}} : x \longmapsto \nu_{\mathfrak{p}}(x o_{\mathcal{F}})$$

$\mathfrak{p}$-exponentielle Bewertung *von $\mathcal{F}$.*

Lemma II.22 *Es sei $\mathfrak{p}$ ein beliebiges Primideal in $o_{\mathcal{F}}$. Für die $\mathfrak{p}$-exponentielle Bewertung kann man die folgenden Eigenschaften leicht nachrechnen:*

(1) $$\nu_{\mathfrak{p}}(x) = \infty \Leftrightarrow x = 0,$$

(2) $$\nu_{\mathfrak{p}}(x \pm y) \geq \min(\nu_{\mathfrak{p}}(x), \nu_{\mathfrak{p}}(y)),$$

(3) $$\nu_{\mathfrak{p}}(x \cdot y) = \nu_{\mathfrak{p}}(x) + \nu_{\mathfrak{p}}(y),$$

(4) $$\nu_{\mathfrak{p}}(x/y) = \nu_{\mathfrak{p}}(x) - \nu_{\mathfrak{p}}(y),$$

(5) $$\nu_{\mathfrak{p}}(\pm 1) = 0.$$

Lemma II.23 *Für ein beliebiges Element $0 \neq x \in \mathcal{F}$ sei*

$$x o_{\mathcal{F}} = \mathfrak{p}_1^{e_1} \cdot \ldots \cdot \mathfrak{p}_s^{e_s}$$

die Primidealzerlegung von $x o_{\mathcal{F}}$ mit paarweise verschiedenen Primidealen $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ und ganzen Zahlen $e_i \neq 0$ $(1 \leq i \leq s)$. Es gilt dann für $1 \leq i \leq s$:

$$\nu_{\mathfrak{p}_i}(x) = e_i$$

und für alle Primideale $\mathfrak{q} \neq \mathfrak{p}_i$ $(1 \leq i \leq s)$:

$$\nu_{\mathfrak{q}}(x) = 0.$$

Satz II.24 *Für ein beliebiges Element $x \in \mathcal{F}$ gilt $x \in o_{\mathcal{F}}$ genau dann, wenn $\nu_{\mathfrak{p}}(x) \geq 0$ für alle Primideale $\mathfrak{p} \subseteq o_{\mathcal{F}}$.*

Satz II.25 *Seien $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ paarweise verschiedene Primideale in $o_{\mathcal{F}}$, und $e_1, \ldots, e_s$ ganze Zahlen. Dann existiert ein $x \in \mathcal{F}$ mit*

$$\nu_{\mathfrak{p}_i}(x) = e_i \ (1 \leq i \leq s)$$

und

$$\nu_{\mathfrak{q}}(x) \geq 0, \mathfrak{q} \notin \{\mathfrak{p}_1, \ldots, \mathfrak{p}_s\}.$$

Lemma II.26 *Es seien $\mathfrak{a}$ ein ganzes Ideal in $o_{\mathcal{F}}$ und $\mathfrak{p}$ ein Primideal in $o_{\mathcal{F}}$. Dann gilt:*

$$\nu_{\mathfrak{p}}(\mathfrak{a}) = \min\{\nu_{\mathfrak{p}}(x) \mid x \in \mathfrak{a}\}.$$

Lemma II.27 *Es seien $\mathfrak{a}$ ein ganzes Ideal in $o_{\mathcal{F}}$ und $\mathfrak{p}$ ein Primideal in $o_{\mathcal{F}}$. Für ein beliebiges $\alpha \in \mathfrak{a} \setminus \mathfrak{p}$ gilt dann*

$$\nu_{\mathfrak{p}}(\alpha) = \nu_{\mathfrak{p}}(\mathfrak{a}).$$

Beweis: Es gilt auf jeden Fall (man vergleiche Lemma II.26)

$$\nu_{\mathfrak{p}}(\alpha) \geq \nu_{\mathfrak{p}}(\mathfrak{a}) = \min\{\nu_{\mathfrak{p}}(\alpha) \mid \alpha \in \mathfrak{a}\}.$$

Es seien

$$\mathfrak{a} = \mathfrak{p}_1^{e_1} \cdot \ldots \cdot \mathfrak{p}_s^{e_s} \cdot \mathfrak{p}^{\nu_{\mathfrak{p}}(\mathfrak{a})},$$

$$\alpha o_{\mathcal{F}} = \mathfrak{p}_1^{\hat{e}_1} \cdot \ldots \cdot \mathfrak{p}_s^{\hat{e}_s} \cdot \mathfrak{p}^{\nu_{\mathfrak{p}}(\alpha)} \cdot \tilde{\mathfrak{p}}_1^{\tilde{e}_1} \cdot \ldots \cdot \tilde{\mathfrak{p}}_{\tilde{s}}^{\tilde{e}_{\tilde{s}}},$$

die Primidealzerlegungen von $\mathfrak{a}$ und $\alpha o_{\mathcal{F}}$, wobei die $\mathfrak{p}_1, \ldots, \mathfrak{p}_s, \mathfrak{p}, \tilde{\mathfrak{p}}_1, \ldots, \tilde{\mathfrak{p}}_{\tilde{s}}$ paarweise verschieden sind. Da $\alpha \in \mathfrak{a} \subseteq o_{\mathcal{F}}$, gilt

$$\hat{e}_i \geq e_i \geq 0 \ (1 \leq i \leq s),$$

$$\tilde{e}_i \geq 0 \ (1 \leq i \leq \tilde{s}).$$

Angenommen es gilt $\nu_{\mathfrak{p}}(\alpha) > \nu_{\mathfrak{p}}(\mathfrak{a})$, dann folgt

$$\alpha \in \mathfrak{p}_1^{\hat{e}_1} \cdot \ldots \cdot \mathfrak{p}_s^{\hat{e}_s} \cdot \mathfrak{p}^{\nu_{\mathfrak{p}}(\alpha)} \subseteq \mathfrak{p}_1^{e_1} \cdot \ldots \cdot \mathfrak{p}_s^{e_s} \cdot \mathfrak{p}^{\nu_{\mathfrak{p}}(\mathfrak{a})+1} = \mathfrak{a} \cdot \mathfrak{p} \subseteq \mathfrak{p}.$$

Dies ist aber ein Widerspruch zu der Wahl von α. Es gilt also

$$\nu_{\mathfrak{p}}(\alpha) = \nu_{\mathfrak{p}}(\mathfrak{a}).$$

□

II.5 Relative Erweiterungen

In der gesammten Arbeit werden die folgenden Körper betrachtet:

$$\mathbb{Q} \subset \mathcal{F} \subset \mathcal{E} \subset \mathbb{C},$$

wobei $\mathcal{E}/\mathcal{F}$ und $\mathcal{F}/\mathbb{Q}$ endliche Körpererweiterungen seien. Man sieht, daß $\mathcal{E}/\mathbb{Q}$ auch eine endliche Körpererweiterung ist. $\mathcal{E}$ ist demnach ein algebraischer Zahlkörper. Unter den Voraussetzung $\mathcal{F} \neq \mathbb{Q}$ und $\mathcal{E} \neq \mathcal{F}$ wird die Körpererweiterung $\mathcal{E}/\mathcal{F}$ auch *Relativerweiterung* genannt. Ähnlich wie im absoluten Fall, existiert ein irreduzibles und normiertes Polynom T mit Koeffizienten in $o_{\mathcal{F}}$, dem Ring der ganzen Zahlen des algebraischen Zahlkörpers $\mathcal{F}$, so daß für eine Nullstelle ρ von T

$$\mathcal{E} = \mathcal{F}(\rho)$$

gilt. Es sei weiterhin

$$n := [\mathcal{E} : \mathcal{F}] = \deg(T),$$

der Grad der Relativerweiterung.

Die Situation kann wie folgt dargestellt werden:

$$
\begin{tikzcd}
 & \mathcal{E} = \mathcal{F}(\rho) \arrow[dl, dash, "n"'] \\
\mathcal{F} = \mathbb{Q}(\theta) \arrow[d, dash, "m"] & \\
\mathbb{Q} &
\end{tikzcd}
$$

Die folgenden Definitionen und Sätze werden analog zum ersten Abschnitt dieses Kapitels formuliert. Für algebraische Zahlen $x \in \mathcal{E}$ kann man die Begriffe Relativnorm und Relativspur definieren:

Definition II.28 *Die* Relativnorm *und die* Relativspur *einer algebraischen Zahl $x \in \mathcal{E}$ sind durch die Determinante und die Spur der linearen Transformation*

$$\psi_{x,\mathcal{F}} : \mathcal{E} \to \mathcal{E},$$

$$\psi_{x,\mathcal{F}} : y \longmapsto x \cdot y$$

des $\mathcal{F}$-Vektorraumes $\mathcal{E}$ gegeben. Sie werden mit

$$\mathrm{N}_{\mathcal{E}/\mathcal{F}}(x) := \det(\psi_{x,\mathcal{F}})$$

und

$$\mathrm{Tr}_{\mathcal{E}/\mathcal{F}}(x) := \mathrm{Trace}(\psi_{x,\mathcal{F}})$$

bezeichnet.

Das Polynom T zerfällt über $\mathbb{C}$ in Linearfaktoren:

$$T(t) = \prod_{i=1}^{n} (t - \rho^{(i)}),$$

wobei die Nullstellen $\rho^{(i)}$ so numeriert seien, daß $\rho^{(1)} = \rho$ gelte. Für $1 \leq i \leq n$ heißt $\rho^{(i)}$ die *i-te Konjugierte* von ρ, der *i-te Konjugiertenkörper* ist definiert als

$$\mathcal{E}^{(i)} := \mathcal{F}(\rho^{(i)}).$$

Weiterhin sei für $1 \leq i \leq n$ die *i-te Konjugierten-Abbildung* definiert durch:

$$.^{(i)} : \mathcal{E} \to \mathcal{E}^{(i)}$$

$$.^{(i)} : x = x_1 + x_2\rho + \ldots + x_n\rho^{n-1} \longmapsto x^{(i)} := x_1 + x_2\rho^{(i)} + \ldots + x_n{\rho^{(i)}}^{n-1}.$$

Die i-te Konjugierten-Abbildung $.^{(i)}$ ist ein $\mathcal{F}$-Isomorphismus von $\mathcal{E}$ in $\mathcal{E}^{(i)}$. Man verzichtet an dieser Stelle auf den Hinweis *relativ*. Es wird aber immer aus dem Zusammenhang deutlich werden, ob die relativen oder die absoluten Konjugierten betrachtet werden.

Satz II.29 *Es gilt*

$$\mathrm{Tr}_{\mathcal{E}/\mathcal{F}}(x) = \sum_{i=1}^{n} x^{(i)},$$

und man sieht, daß die Relativspur eine $\mathcal{F}$-lineare Abbildung von $\mathcal{E}$ in $\mathcal{F}$ ist.

Satz II.30 *Es gilt*

$$\mathrm{N}_{\mathcal{E}/\mathcal{F}}(x) = \prod_{i=1}^{n} x^{(i)}.$$

Die Relativnorm ist folglich multiplikativ $\left(\mathrm{N}_{\mathcal{E}/\mathcal{F}}(xy) = \mathrm{N}_{\mathcal{E}/\mathcal{F}}(x) \cdot \mathrm{N}_{\mathcal{E}/\mathcal{F}}(y)\right)$.

Mit den Abbildungen $.^{(1)}, \ldots, .^{(n)}$ erhält man die folgende Darstellung für das charakteristische Polynom:

Satz II.31 *Es sei $x \in \mathcal{E}$. Für das charakteristische Polynom von x über $\mathcal{F}$ gilt:*

$$m_x(t) = \prod_{i=1}^{n} \left(t - x^{(i)}\right).$$

Mit der Relativspur kann die sogenannte Diskriminante definiert werden:

Definition II.32 *Bilden die Elemente $x_1, \ldots, x_n$ eine $\mathcal{F}$-Basis von $\mathcal{E}$, so definiert man die* Diskriminante *von $x_1, \ldots, x_n$ wie folgt:*

$$\mathrm{disc}_{\mathcal{E}/\mathcal{F}}(x_1, \ldots, x_n) := \det\left(\mathrm{Tr}_{\mathcal{E}/\mathcal{F}}(x_i \cdot x_j)_{1 \leq i,j \leq n}\right).$$

Man sieht, daß die Diskriminante der Elemente $x_1, \ldots, x_n \in \mathcal{E}$ ein Element aus $\mathcal{F}$ ist.

Es seien $o_{\mathcal{E}}$ der Ring der ganzen Zahlen von $\mathcal{E}$ und $o_{\mathcal{F}}$ der Ring der ganzen Zahlen von $\mathcal{F}$. Es gilt

$$o_{\mathcal{F}} \subset o_{\mathcal{E}}.$$

Satz II.33 *Eine algebraische Zahl $x \in \mathcal{E}$ ist genau dann ganz algebraisch, wenn ein normiertes Polynom $f \in o_{\mathcal{F}}[t]$ existiert, mit*

$$f(x) = 0.$$

Die Definition der relativen Körperdiskriminante weicht etwas von der Definition der (absoluten) Körperdiskriminante ab:

Definition II.34 *Die* relative Körperdiskriminante *von $\mathcal{E}$ über $\mathcal{F}$ wird definiert als:*

$$\mathfrak{d}_{\mathcal{E}/\mathcal{F}} := \left\langle \{\mathrm{disc}_{\mathcal{E}/\mathcal{F}}(\alpha_1, \ldots, \alpha_n) \mid \alpha_1, \ldots, \alpha_n \in o_{\mathcal{E}} \text{ bilden eine } \mathcal{F}\text{-Basis von } \mathcal{E}/\mathcal{F}\} \right\rangle.$$

Die relative Körperdiskriminante ist ein ganzes Ideal in $o_{\mathcal{F}}$. Es besteht der folgende Zusammenhang zu der (absoluten) Körperdiskriminante:

Satz II.35 *Es gilt:*

$$|\mathfrak{d}_{\mathcal{E}/\mathbb{Q}}| = \mathrm{N}_{\mathcal{F}/\mathbb{Q}}(\mathfrak{d}_{\mathcal{E}/\mathcal{F}}) \cdot |\mathfrak{d}_{\mathcal{F}/\mathbb{Q}}|^n.$$

Dabei sind $\mathfrak{d}_{\mathcal{E}/\mathbb{Q}}$ und $\mathfrak{d}_{\mathcal{F}/\mathbb{Q}}$ die in Definition II.10 definierten absoluten Körperdiskriminanten von $\mathcal{E}$ und $\mathcal{F}$, und $\mathrm{N}_{\mathcal{F}/\mathbb{Q}}(\mathfrak{d}_{\mathcal{E}/\mathcal{F}})$ ist die Idealnorm der relativen Körperdiskriminante.

II.6 Endlich erzeugte Moduln über Dedekindringen

Dieser Abschnitt stellt die wichtigsten Ergebnisse der Artikel [BP91, Coh96] dar. R sei ein beliebiger Dedekindring, und $Q(R)$ sei sein Quotientenkörper. (In den folgenden Abschnitten werden R immer der Ring der ganzen algebraischen Zahlen von $\mathcal{F}$ und $Q(R)$ natürlich der Körper $\mathcal{F}$ selbst sein.) $\mathcal{M}$ sei ein endlich erzeugter torsionsfreier R-Modul. Eine der wichtigsten Aussagen ist:

Theorem II.36 *Ist $V := \mathcal{M} \cdot Q(R)$ der $Q(R)$-Vektorraum, der von $\mathcal{M}$ aufgespannt wird, und ist $k := \dim_{Q(R)}(V)$, dann existieren gebrochene Ideale $\mathfrak{a}_1, \ldots, \mathfrak{a}_k$ in R und Elemente $\omega_1, \ldots, \omega_k \in V$, die über $Q(R)$-linear unabhängig sind, so daß*

$$\mathcal{M} = \mathfrak{a}_1\omega_1 + \ldots + \mathfrak{a}_k\omega_k.$$

Eine solche Darstellung heißt Pseudobasis *von $\mathcal{M}$. Die Ideale $\mathfrak{a}_1, \ldots, \mathfrak{a}_k$ werden auch* Koeffizientenideale *genannt. Die Dimension k des $Q(R)$-Vektorraumes V heißt der* Rang *von $\mathcal{M}$.*

Definition II.37 *Es sei $\mathcal{M} = \mathfrak{a}_1\omega_1 + \ldots + \mathfrak{a}_k\omega_k$ eine Pseudobasis von $\mathcal{M}$. Die Klasse des Ideals*

$$\mathfrak{a} := \mathfrak{a}_1 \cdot \ldots \cdot \mathfrak{a}_k$$

in der Klassengruppe von R heißt die Steinitzklasse *von $\mathcal{M}$.*

Die Steinitzklasse ist unabhängig von der Wahl der Pseudobasis. Es gilt die folgende Aussage:

Satz II.38 *Der R-Modul $\mathcal{M}$ ist genau dann frei, wenn die Steinitzklasse von $\mathcal{M}$ die triviale Klasse ist.*

Für eine beliebige Pseudobasis des Moduls $\mathcal{M}$ heißt dies, daß $\mathcal{M}$ genau dann frei ist, wenn das Produkt der Koeffizientenideale ein Hauptideal ist.

Für den folgenden Satz benötigt man eine Abbildung

$$\Gamma : \mathcal{M} \times \mathcal{M} \to R,$$

welche die folgenden Eigenschaften erfüllt:

- Für jedes Element $x \in \mathcal{M}$ sind die Abbildungen
$$\Gamma(\cdot, x) : \mathcal{M} \to R,$$
$$\Gamma(x, \cdot) : \mathcal{M} \to R$$
R-Modulhomomorphismen,
- und es gilt
$$\{x \in \mathcal{M} \mid \Gamma(x,y) = 0,\ \forall y \in \mathcal{M}\} =$$
$$\{y \in \mathcal{M} \mid \Gamma(x,y) = 0,\ \forall x \in \mathcal{M}\} = \{0\}.$$

Solche Abbildungen werden als *nicht-degenerierte Bilinearformen* bezeichnet. In den folgenden Abschnitten wird diese Aufgabe von der Spur erfüllt:

$$\Gamma(x,y) := \mathrm{Tr}_{\mathcal{E}/\mathcal{F}}(x \cdot y).$$

Satz II.39 *Sind $\mathcal{M} = \mathfrak{a}_1\omega_1 + \ldots + \mathfrak{a}_k\omega_k = \mathfrak{b}_1\eta_1 + \ldots + \mathfrak{b}_k\eta_k$ zwei Pseudobasen von $\mathcal{M}$, so gilt $(\mathfrak{a}_1 \cdot \ldots \cdot \mathfrak{a}_k)^2 \cdot \det\left(\Gamma(\omega_i,\omega_j)_{1\le i,j\le k}\right) = (\mathfrak{b}_1 \cdot \ldots \cdot \mathfrak{b}_k)^2 \cdot \det\left(\Gamma(\eta_i,\eta_j)_{1\le i,j\le k}\right)$. Man bezeichnet das Ideal*

$$\mathrm{disc}(\mathcal{M}) := (\mathfrak{a}_1 \cdot \ldots \cdot \mathfrak{a}_k)^2 \cdot \det\left(\Gamma(\omega_i,\omega_j)_{1\le i,j\le k}\right)$$

als Diskriminante *von $\mathcal{M}$.*

Um die *Hermite-Normalform über Dedekindringen* zu erklären, ist eine weitere Definition erforderlich:

Definition II.40 *Sind gebrochene Ideale $\mathfrak{a}_1, \ldots, \mathfrak{a}_l$ in R und Elemente $\omega_1, \ldots, \omega_l \in Q(R)$ gegeben mit*

$$\mathcal{M} = \mathfrak{a}_1\omega_1 + \ldots + \mathfrak{a}_l\omega_l,$$

so heißt das System $(\mathfrak{a}_i, \omega_i)_{1\le i\le l}$ ein Pseudoerzeugendensystem *von $\mathcal{M}$.*

Ist $A \in Q(R)^{k\times l}$ eine Matrix und sind $\mathfrak{a}_1, \ldots, \mathfrak{a}_l$ gebrochene Ideale in R, so ist

$$\mathcal{M} := \mathfrak{a}_1 A_{\cdot,1} + \ldots + \mathfrak{a}_l A_{\cdot,l}$$

ein Pseudoerzeugendensystem für den Modul $\mathcal{M}$.

Ein solcher Modul $\mathcal{M}$ wird im weiteren Verlauf der Arbeit wie folgt dargestellt:

$$\mathcal{M} = \begin{pmatrix} \mathfrak{a}_1 & \cdots & \mathfrak{a}_l \\ & A & \end{pmatrix}.$$

Theorem II.41 (Hermite-Normalform über Dedekindringen) *Seien gebrochene Ideale $\mathfrak{a}_1, \ldots, \mathfrak{a}_l$ in R sowie eine Matrix $A \in Q(R)^{k\times l}$ mit Rang k (also $l \ge k$) gegeben, und sei $\mathcal{M} := \sum_{i=1}^{l} \mathfrak{a}_i A_{\cdot,i}$ der zugehörige Modul. Dann existieren gebrochene Ideale $\mathfrak{c}_1, \ldots, \mathfrak{c}_l$ in R und eine Matrix $U \in Q(R)^{l\times l}$ mit den folgenden Eigenschaften:*

(1) Setzt man $\mathfrak{a} := \mathfrak{a}_1 \cdot \ldots \cdot \mathfrak{a}_l$, $\mathfrak{c} := \mathfrak{c}_1 \cdot \ldots \cdot \mathfrak{c}_l$, so gilt:

$$\mathfrak{a} = \det(U) \cdot \mathfrak{c}.$$

(2)
$$A \cdot U = \begin{array}{c} \begin{array}{cc} \overbrace{\hphantom{0\;\;0\;\;\cdots\;\;0}}^{l-k\ \text{Spalten}} & \overbrace{\hphantom{1\;\;*\;\;*\;\;\cdots\;\;*}}^{k\ \text{Spalten}} \end{array} \\ \begin{pmatrix} 0 & 0 & \cdots & 0 & 1 & * & * & \cdots & * \\ 0 & 0 & \cdots & 0 & 0 & 1 & * & \cdots & * \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \ddots & \ddots & * \\ 0 & 0 & \cdots & 0 & 0 & \cdots & \cdots & 0 & 1 \end{pmatrix} \end{array}.$$

(3) Definiert man die Matrix $B \in Q(R)^{k\times k}$ als die Matrix, die aus den letzten k Spalten der Matrix $A \cdot U$ besteht, und die gebrochenen Ideale $\mathfrak{b}_i$ durch $\mathfrak{b}_i := \mathfrak{c}_{l-k+i}$ $(1 \le i \le k)$, so gilt

$$\mathcal{M} = \mathfrak{b}_1 B_{\cdot,1} + \ldots + \mathfrak{b}_k B_{\cdot,k}, \tag{II-1}$$

und (II-1) *ist sogar eine Pseudobasis von $\mathcal{M}$.*

Theorem II.42 (Smith-Normalform) *Seien $\mathcal{M} \subseteq \mathcal{N}$ zwei torsionsfreie R-Moduln vom Rang k. Dann existieren gebrochene Ideale $\mathfrak{a}_1, \ldots, \mathfrak{a}_k$ in R, eine Basis $\omega_1, \ldots, \omega_k$ von $V := \mathcal{N} \cdot Q(R)$ und ganze Ideale $\mathfrak{b}_1, \ldots, \mathfrak{b}_k$ in R, mit den Eigenschaften*

$$\mathcal{N} = \mathfrak{a}_1\omega_1 + \ldots + \mathfrak{a}_k\omega_k, \tag{II-2}$$

$$\mathcal{M} = \mathfrak{a}_1\mathfrak{b}_1\omega_1 + \ldots + a_k\mathfrak{b}_k\omega_k. \tag{II-3}$$

Weiterhin gilt $\mathfrak{b}_{i-1} \subseteq \mathfrak{b}_i$ $(2 \le i \le k)$ und die Ideale $\mathfrak{b}_1, \ldots, \mathfrak{b}_k$ hängen nur von den Moduln $\mathcal{M}$ und $\mathcal{N}$ ab.

In [Coh96] wird sowohl eine Algorithmus zur Berechnung der Hermite-Normalform als auch eine Algorithmus zur Berechnung der Smith-Normalform über Dedekindringen angegeben.

Damit kann man den Index von einem R-Modul $\mathcal{N}$ zu einem darin enthaltenen R-Modul $\mathcal{M}$ definieren:

Definition II.43 *Seien $\mathcal{M} \subseteq \mathcal{N}$ zwei torsionsfreie R-Moduln vom Rang k, und die Pseudobasen von $\mathcal{M}$, $\mathcal{N}$ seien wie in* (II-2) *und* (II-3) *gegeben. Dann ist der* Index *von $\mathcal{N}$ zu $\mathcal{M}$ definiert als*

$$[\mathcal{N} : \mathcal{M}] := \mathfrak{b}_1 \cdot \ldots \cdot \mathfrak{b}_k.$$

Man erhält den folgenden Zusammenhang zu der Diskriminante:

Satz II.44 *Seien $\mathcal{M} \subseteq \mathcal{N}$ zwei torsionsfreie R-Moduln vom Rang k. Dann gilt:*

$$\mathrm{disc}(\mathcal{M}) = \mathrm{disc}(\mathcal{N}) \cdot [\mathcal{N} : \mathcal{M}]^2.$$

Beweis: Man erkennt dies sofort, wenn man die Pseudobasen aus Theorem II.42 und die Definition der Diskriminante betrachtet. □

II.7 Relative Ordnungen

In diesem Abschnitt wird ein der absoluten Ordnung sehr ähnlicher Begriff für die Relativerweiterung $\mathcal{E}/\mathcal{F}$ eingeführt.

Definition II.45 *Ein unitärer Teilring $\mathcal{O}$ von $o_\mathcal{E}$ heißt* relative Ordnung *von $\mathcal{E}$, wenn er eine absolute Ordnung von $\mathcal{E}$ und zusätzlich ein endlich erzeugter $o_\mathcal{F}$-Modul vom Rang n ist.*

Eine relative Ordnung wird manchmal auch einfach nur *Relativordnung* genannt. Der unitäre Teilring $\mathcal{O}$ von $o_\mathcal{E}$ ist also genau dann eine Relativordnung von $\mathcal{E}$, wenn $\mathcal{O}$ ein freier $\mathbb{Z}$-Modul vom Rang $n \cdot m$ und ein endlich erzeugter $o_\mathcal{F}$-Modul vom Rang n ist. Zum Nachweis einer relativen Ordnung kann der folgende Satz verwendet werden:

Satz II.46 *Eine Teilmenge $\mathcal{O} \subset \mathcal{E}$ ist genau dann eine relative Ordnung in $\mathcal{E}$, wenn $\mathcal{O}$ eine absolute Ordnung von $\mathcal{E}$ ist und zusätzlich noch der Ring $o_\mathcal{F}$ in $\mathcal{O}$ enthalten ist.*

Dieser Satz zeigt, angewendet auf den Ring der ganzen Zahlen von $\mathcal{E}$, daß $o_\mathcal{E}$ eine relative Ordnung von $\mathcal{E}$ ist. Da keine größere („$\subset$") relative Ordnung von $\mathcal{E}$ existiert, wird $o_\mathcal{E}$ auch *relative Maximalordnung* genannt. Der Begriff relative Maximalordnung wird verwendet, um hervorzuheben, daß man die Relativerweiterung $\mathcal{E}/\mathcal{F}$ betrachtet, denn $o_\mathcal{E}$ ist auch absolut gesehen die Maximalordnung von $\mathcal{E}$. Ein weiteres Beispiel ist eine *relative Gleichungsordnung:*

$$o_\mathcal{F}[\rho] := o_\mathcal{F} + o_\mathcal{F}\rho + \ldots + o_\mathcal{F}\rho^{n-1}.$$

Man beachte, daß ρ Nullstelle eines irreduziblen und normierten Polynoms T mit Koeffizienten aus $o_\mathcal{F}$ ist.

Satz II.47 *Nach den Ergebnissen des vorangegangenen Abschnitts kann eine Relativordnung $\mathcal{O}$ von $\mathcal{E}$ immer durch eine Pseudobasis dargestellt werden:*

$$\mathcal{O} = \mathfrak{a}_1\omega_1 + \ldots + \mathfrak{a}_n\omega_n,$$

wobei die Koeffizientenideale *$\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ Ideale in $o_\mathcal{F}$ sind und die* Basiselemente *$\omega_1, \ldots, \omega_n \in \mathcal{E}$ eine $\mathcal{F}$-Basis von $\mathcal{E}$ bilden.*

Definition II.48 *Ist $\mathcal{O}$ eine Relativordnung von $\mathcal{E}$ mit der Pseudobasis*

$$\mathcal{O} = \mathfrak{a}_1\omega_1 + \ldots + \mathfrak{a}_n\omega_n,$$

so definiert man die Diskriminante *der Relativordnung $\mathcal{O}$ als*

$$\mathfrak{d}_{\mathcal{E}/\mathcal{F}}(\mathcal{O}) := (\mathfrak{a}_1 \cdot \ldots \cdot \mathfrak{a}_n)^2 \cdot \det(\mathrm{Tr}_{\mathcal{E}/\mathcal{F}}(\omega_i \cdot \omega_j)_{1\le i,j\le n}) =$$

$$(\mathfrak{a}_1 \cdot \ldots \cdot \mathfrak{a}_n)^2 \cdot \mathrm{disc}_{\mathcal{E}/\mathcal{F}}(\omega_1, \ldots, \omega_n).$$

Die Diskriminante ist ein Ideal in $o_{\mathcal{F}}$. Um zu zeigen, daß sie sogar ein ganzes Ideal in $o_{\mathcal{F}}$ ist, benötigt man die Bedeutung der Diskriminante der relativen Maximalordnung $o_{\mathcal{E}}$.

Satz II.49 *Es seien $\mathfrak{d}_{\mathcal{E}/\mathcal{F}}(o_{\mathcal{E}})$ die Diskriminante der relativen Maximalordnung und $\mathfrak{d}_{\mathcal{E}/\mathcal{F}}$ die relative Körperdiskriminante. Dann gilt:*

$$\mathfrak{d}_{\mathcal{E}/\mathcal{F}}(o_{\mathcal{E}}) = \mathfrak{d}_{\mathcal{E}/\mathcal{F}}.$$

Beweis: Es sei $o_{\mathcal{E}} = \mathfrak{a}_1\omega_1 + \ldots + \mathfrak{a}_n\omega_n$ eine Pseudobasis von $o_{\mathcal{E}}$. Dabei kann man die Elemente $\omega_1, \ldots, \omega_n \in o_{\mathcal{E}}$ wählen. Es gilt dann

$$\mathfrak{d}_{\mathcal{E}/\mathcal{F}}(o_{\mathcal{E}}) = \left(\prod_{i=1}^{n} \mathfrak{a}_i\right)^2 \cdot \mathrm{disc}_{\mathcal{E}/\mathcal{F}}(\omega_1, \ldots, \omega_n).$$

Definiert man das Ideal $\mathfrak{a}$ durch $\mathfrak{a} := \prod_{i=1}^n \mathfrak{a}_i$ und sind $\mathfrak{a}_i = a_{i,1}o_{\mathcal{F}} + a_{i,2}o_{\mathcal{F}}$ $(1 \le i \le n)$ 2-Element-Darstellung wie in Satz II.14, so erhält man

$$\mathfrak{d}_{\mathcal{E}/\mathcal{F}}(o_{\mathcal{E}}) = \mathfrak{a}^2 \cdot \mathrm{disc}_{\mathcal{E}/\mathcal{F}}(\omega_1, \ldots, \omega_n) =$$

$$\left(\left(\prod_{i=1}^{n} a_{i,1}\right)^2 o_{\mathcal{F}} + \left(\prod_{i=1}^{n} a_{i,2}\right)^2 o_{\mathcal{F}}\right) \cdot \mathrm{disc}_{\mathcal{E}/\mathcal{F}}(\omega_1, \ldots, \omega_n) =$$

$$\left(\prod_{i=1}^{n} a_{i,1}\right)^2 \cdot \mathrm{disc}_{\mathcal{E}/\mathcal{F}}(\omega_1, \ldots, \omega_n) \cdot o_{\mathcal{F}} + \left(\prod_{i=1}^{n} a_{i,2}\right)^2 \cdot \mathrm{disc}_{\mathcal{E}/\mathcal{F}}(\omega_1, \ldots, \omega_n) \cdot o_{\mathcal{F}}.$$

Da $a_{i,1}, a_{i,2} \in \mathfrak{a}_i$ $(1 \le i \le n)$, folgt $a_{i,1}\omega_i, a_{i,2}\omega_i \in o_{\mathcal{E}}$ $(1 \le i \le n)$. Außerdem bilden die Elemente

$$\tilde{\omega}_i := a_{i,1}\omega_i \ (1 \le i \le n),$$

$$\hat{\omega}_i := a_{i,2}\omega_i \ (1 \le i \le n),$$

jeweils $\mathcal{F}$-Basen von $\mathcal{E}$. Es gilt

$$\mathfrak{d}_{\mathcal{E}/\mathcal{F}}(o_{\mathcal{E}}) =$$

$$\left(\prod_{i=1}^{n} a_{i,1}\right)^2 \cdot \det(\mathrm{Tr}_{\mathcal{E}/\mathcal{F}}(\omega_i \cdot \omega_j)_{1\le i,j\le n}) \cdot o_{\mathcal{F}} + \left(\prod_{i=1}^{n} a_{i,2}\right)^2 \cdot \det(\mathrm{Tr}_{\mathcal{E}/\mathcal{F}}(\omega_i \cdot \omega_j)_{1\le i,j\le n}) \cdot o_{\mathcal{F}} =$$

$$\det(\mathrm{Tr}_{\mathcal{E}/\mathcal{F}}(\tilde{\omega}_i \cdot \tilde{\omega}_j)_{1\le i,j\le n}) \cdot o_{\mathcal{F}} + \det(\mathrm{Tr}_{\mathcal{E}/\mathcal{F}}(\hat{\omega}_i \cdot \hat{\omega}_j)_{1\le i,j\le n}) \cdot o_{\mathcal{F}} =$$

$$\mathrm{disc}_{\mathcal{E}/\mathcal{F}}(\tilde{\omega}_1, \ldots, \tilde{\omega}_n) \cdot o_{\mathcal{F}} + \mathrm{disc}_{\mathcal{E}/\mathcal{F}}(\hat{\omega}_1, \ldots, \hat{\omega}_n) \cdot o_{\mathcal{F}} \subseteq \mathfrak{d}_{\mathcal{E}/\mathcal{F}} + \mathfrak{d}_{\mathcal{E}/\mathcal{F}} \subseteq \mathfrak{d}_{\mathcal{E}/\mathcal{F}}.$$

Sei jetzt $\alpha_1, \ldots, \alpha_n \in o_{\mathcal{E}}$ eine beliebige $\mathcal{F}$-Basis von $\mathcal{E}$. Es existiert eine Matrix A mit $(\omega_1, \ldots, \omega_n) \cdot A = (\alpha_1, \ldots, \alpha_n)$ und $A_{i,j} \in \mathfrak{a}_i$ $(1 \le i, j \le n)$. Damit sieht man

$$\alpha_i \cdot \alpha_j = [(\omega_1, \ldots, \omega_n) \cdot A_{\cdot,i}] \cdot [(\omega_1, \ldots, \omega_n) \cdot A_{\cdot,j}] = \left[\sum_{\nu=1}^{n} \omega_\nu \cdot A_{\nu,i}\right] \cdot \left[\sum_{\mu=1}^{n} \omega_\mu \cdot A_{\mu,j}\right] =$$

$$\sum_{\nu=1}^{n}\sum_{\mu=1}^{n} \omega_\nu \cdot A_{\nu,i} \cdot \omega_\mu \cdot A_{\mu,j} = \left(A^{tr}\right)_{i,\cdot} \cdot (\omega_\nu \cdot \omega_\mu)_{1\le\nu,\mu\le n} \cdot A_{\cdot,j}.$$

Aus Satz II.29 folgt

$$\mathrm{Tr}_{\mathcal{E}/\mathcal{F}}(\alpha_i \cdot \alpha_j) = \left(A^{tr}\right)_{i,\cdot} \cdot (\mathrm{Tr}_{\mathcal{E}/\mathcal{F}}(\omega_\nu \cdot \omega_\mu))_{1\le\nu,\mu\le n} \cdot A_{\cdot,j},$$

und daher

$$(\mathrm{Tr}_{\mathcal{E}/\mathcal{F}}(\alpha_i \cdot \alpha_j))_{1\le i,j\le n} = A^{tr} \cdot (\mathrm{Tr}_{\mathcal{E}/\mathcal{F}}(\omega_\nu \cdot \omega_\mu))_{1\le\nu,\mu\le n} \cdot A.$$

Aus der Definition der Determinante kann man ablesen, daß $\det(A) \in \mathfrak{a}$ gilt. Damit erhält man

$$\mathrm{disc}_{\mathcal{E}/\mathcal{F}}(\alpha_1, \ldots \alpha_n) = \det\left(\mathrm{Tr}_{\mathcal{E}/\mathcal{F}}(\alpha_i \cdot \alpha_j)_{1\le i,j\le n}\right) =$$

$$\det\left(A^{tr}\right) \cdot \mathrm{disc}_{\mathcal{E}/\mathcal{F}}(\omega_1, \ldots, \omega_n) \cdot \det(A) \in \mathfrak{a}^2 \cdot \mathrm{disc}_{\mathcal{E}/\mathcal{F}}(\omega_1, \ldots, \omega_n) = \mathfrak{d}_{\mathcal{E}/\mathcal{F}}(o_{\mathcal{E}}).$$

□

Die Definition des Index aus dem vorangegangenen Abschnitt kann man auf Relativordnungen übertragen:

Definition II.50 *Es seien $\mathcal{O}_1 \subseteq \mathcal{O}_2$ zwei Relativordnungen von $\mathcal{E}$ mit Pseudobasen wie in Theorem II.42:*

$$\mathcal{O}_2 = \mathfrak{a}_1\omega_1 + \ldots + \mathfrak{a}_n\omega_n,$$

$$\mathcal{O}_1 = \mathfrak{a}_1\mathfrak{b}_1\omega_1 + \ldots + \mathfrak{a}_n\mathfrak{b}_n\omega_n.$$

Der Index *von $\mathcal{O}_2$ zu $\mathcal{O}_1$ ist das ganze Ideal*

$$[\mathcal{O}_2 : \mathcal{O}_1] := \mathfrak{b}_1 \cdot \ldots \cdot \mathfrak{b}_n.$$

Es folgt dann die Behauptung von oben:

Satz II.51 *Ist $\mathcal{O}$ eine beliebige Relativordnung von $\mathcal{E}$, so ist die Diskriminante $\mathfrak{d}_{\mathcal{E}/\mathcal{F}}(\mathcal{O})$ von $\mathcal{O}$ ein ganzes Ideal in $o_{\mathcal{F}}$.*

Beweis: In Satz II.44 hat man gesehen, daß

$$\mathfrak{d}_{\mathcal{E}/\mathcal{F}}(\mathcal{O}) = \mathfrak{d}_{\mathcal{E}/\mathcal{F}}(o_{\mathcal{E}}) \cdot [o_{\mathcal{E}} : \mathcal{O}]^2 = \mathfrak{d}_{\mathcal{E}/\mathcal{F}} \cdot [o_{\mathcal{E}} : \mathcal{O}]^2$$

gilt. Die Behauptung folgt aus der Beobachtung, daß auf der rechten Seite nur ganze Ideale stehen. □

Satz II.52 *Jedes Ideal $\mathfrak{a}$ in einer Relativordnung $\mathcal{O}$ ist ein endlich erzeugter $o_{\mathcal{F}}$-Modul vom Rang n. Insbesondere kann $\mathfrak{a}$ durch eine Pseudobasis dargestellt werden:*

$$\mathfrak{a} = \mathfrak{b}_1\eta_1 + \ldots + \mathfrak{b}_n\eta_n,$$

wobei die Koeffizientenideale *$\mathfrak{b}_1, \ldots, \mathfrak{b}_n$ Ideale in $o_{\mathcal{F}}$ sind und die* Basiselemente *$\eta_1, \ldots, \eta_n \in \mathcal{E}$ eine $\mathcal{F}$-Basis von $\mathcal{E}$ bilden.*

Für Ideale $\mathfrak{a}$ in der relativen Maximalordnung $o_{\mathcal{E}}$ von $\mathcal{E}$ bietet sich eine weitere Darstellung an:

$$\mathfrak{a} = a_1 \cdot o_{\mathcal{E}} + a_2 \cdot o_{\mathcal{E}},$$

mit Elementen $a_1, a_2 \in \mathfrak{a}$, $a_1, a_2 \ne 0$.

Ein Ideal $\mathfrak{a}$ in einer Relativordnung $\mathcal{O}$ von $\mathcal{E}$ wird *Relativideal* genannt.

Definition II.53 *Für ein Ideal $\mathfrak{a}$ in einer Relativordnung $\mathcal{O}$ von $\mathcal{E}$ ist die* relative Idealnorm *definiert als:*

$$\mathrm{N}_{\mathcal{E}/\mathcal{F}}(\mathfrak{a}) := \left\langle \{\mathrm{N}_{\mathcal{E}/\mathcal{F}}(a) \mid a \in \mathfrak{a}\} \right\rangle,$$

das Ideal in der Maximalordnung $o_{\mathcal{F}}$, das von den Normen aller Elemente des Ideals $\mathfrak{a}$ erzeugt wird.

Die relative Idealnorm hat die folgenden Eigenschaften:

Satz II.54 *Sei $\mathcal{O}$ eine relative Ordnung in $\mathcal{E}$. Dann gelten:*

(1) Die relative Idealnorm ist multiplikativ:

$$\mathrm{N}_{\mathcal{E}/\mathcal{F}}(\mathfrak{a}\mathfrak{b}) = \mathrm{N}_{\mathcal{E}/\mathcal{F}}(\mathfrak{a}) \cdot \mathrm{N}_{\mathcal{E}/\mathcal{F}}(\mathfrak{b})$$

für beliebige Ideale $\mathfrak{a}, \mathfrak{b}$ in der relativen Maximalordnung $o_{\mathcal{E}}$,

(2)
$$\mathrm{N}_{\mathcal{E}/\mathcal{F}}(\mathfrak{a}) \subseteq \mathfrak{a}$$

für ein ganzes Ideal $\mathfrak{a}$ in $\mathcal{O}$,

(3)
$$\mathrm{N}_{\mathcal{E}/\mathcal{F}}(\alpha\mathcal{O}) = \mathrm{N}_{\mathcal{E}/\mathcal{F}}(\alpha)o_{\mathcal{F}}$$

für eine beliebige algebraische Zahl $\alpha \in \mathcal{E}$,

(4)
$$\mathrm{N}_{\mathcal{F}/\mathbb{Q}}\left(\mathrm{N}_{\mathcal{E}/\mathcal{F}}(\mathfrak{a})\right) = \mathrm{N}_{\mathcal{E}/\mathbb{Q}}(\mathfrak{a})$$

für ein beliebiges Ideal $\mathfrak{a}$ *in* $\mathcal{O}$.

In der relativen Maximalordnung $o_{\mathcal{E}}$ gibt es noch eine Besonderheit bei der Primidealzerlegung von Primidealen aus der absoluten Maximalordnung $o_{\mathcal{F}}$.

Satz II.55 *Es sei* $\mathfrak{p}$ *ein Primideal in der Maximalordnung* $o_{\mathcal{F}}$. *Ist*

$$\mathfrak{p}o_{\mathcal{E}} = \mathfrak{P}_1^{e_1} \cdot \ldots \cdot \mathfrak{P}_s^{e_s}$$

die Primidealzerlegung von $\mathfrak{p}o_{\mathcal{E}}$, *so gilt:*

$$s \leq n.$$

II.8 Relative Ganzheitsbasen

In diesem Abschnitt wird der Begriff der relativen Ganzheitsbasis eingeführt. Danach wird beschrieben, wie man eine solche Basis, wenn sie existiert, berechnen kann. Weiter vorne wurde der Begriff der absoluten Ganzheitsbasis definiert: Eine absolute Ganzheitsbasis ist eine $\mathbb{Z}$-Basis der Maximalordnung. Da die Maximalordnung ein freier $\mathbb{Z}$-Modul ist, existiert so eine Basis immer. Bei der relativen Ganzheitsbasis ist dies nicht der Fall.

Definition II.56 *Eine* $\mathcal{F}$*-Basis* $\omega_1, \ldots, \omega_n \in o_{\mathcal{E}}$ *von* $\mathcal{E}$ *heißt* relative Ganzheitsbasis *von* $\mathcal{E}$, *wenn sie eine* $o_{\mathcal{F}}$*-Basis von* $o_{\mathcal{E}}$ *ist, also wenn*

$$o_{\mathcal{E}} = o_{\mathcal{F}}\omega_1 + \ldots + o_{\mathcal{F}}\omega_n.$$

Wie oben schon bemerkt wurde, existiert eine solche Basis nicht immer, da ein endlich erzeugter torsionsfreier $o_{\mathcal{F}}$-Modul im allgemeinen nicht frei ist. Um dennoch eine Darstellung für diese Moduln zu erhalten, wurde der Begriff der Pseudobasis eingeführt.

Ein einfaches Beispiel ist $\mathcal{E} := \mathbb{Q}(\sqrt{5}, \sqrt{10}), \mathcal{F} := \mathbb{Q}(\sqrt{10})$. In [Edg79] wurde gezeigt, daß keine relative Ganzheitsbasis von $\mathcal{E}$ existiert. Weitere Ergebnisse hierzu findet man in [Dab93].

Ein Kriterium für die Existenz einer relativen Ganzheitsbasis geht auf E. Artin [Art65] zurück:

Satz II.57 (Artin-Kriterium) *Es existiert genau dann eine relative Ganzheitsbasis für* $\mathcal{E}/\mathcal{F}$, *wenn das Ideal*

$$\mathfrak{b} := \frac{\mathfrak{d}_{\mathcal{E}/\mathcal{F}}}{\mathrm{disc}_{\mathcal{E}/\mathcal{F}}(1, \rho, \rho^2, \ldots, \rho^{n-1})}$$

das Quadrat eines Hauptideals ist.

In Satz II.38 wurde ein zweites Kriterium für die Existenz einer relativen Ganzheitsbasis gezeigt.

Um in einer Relativordnung rechnen zu können, benötigt man eine Pseudobasis der Relativordnung. In den folgenden Kapiteln wird sich zeigen, daß man eine Pseudobasis für die relative Maximalordnung immer berechnen kann. Man kann also an dieser Stelle die Existenz einer Pseudobasis für die relative Maximalordnung voraussetzen:

$$o_{\mathcal{E}} = \mathfrak{a}_1\omega_1 + \ldots + \mathfrak{a}_n\omega_n.$$

Jetzt stellt sich die Frage, wie man, ausgehend von dieser Pseudobasis, eine relative Ganzheitsbasis berechnen kann, falls diese existiert. Das in Satz II.38 gezeigte Kriterium besagt, daß eine relative Ganzheitsbasis genau dann existiert, wenn das Ideal

$$\mathfrak{a} := \mathfrak{a}_1 \cdot \ldots \cdot \mathfrak{a}_n$$

ein Hauptideal ist.

Es existiert ein Algorithmus [O'M63], mit dem man eine beliebige Pseudobasis von $o_{\mathcal{E}}$ in eine Pseudobasis der Form

$$o_{\mathcal{E}} = o_{\mathcal{F}}\tilde{\omega}_1 + \ldots + o_{\mathcal{F}}\tilde{\omega}_{n-1} + \tilde{\mathfrak{a}}\tilde{\omega}_n$$

überführen kann, wobei $\tilde{\mathfrak{a}}$ ein Ideal in $o_{\mathcal{F}}$ ist. Diese Form der Pseudobasis nennt man *Steinitz-Form*. Das Kriterium besagt jetzt, daß man testen muß, ob das Ideal $\tilde{\mathfrak{a}}$ ein Hauptideal ist. Auch hierfür gibt es einen Algorithmus [PZ89, Heß96]. Ist das Ideal $\tilde{\mathfrak{a}}$ ein Hauptideal, also

$$\tilde{\mathfrak{a}} = \alpha o_{\mathcal{F}}$$

für ein Element $\alpha \in o_{\mathcal{F}}$, so ist klar, daß man dann durch

$$o_{\mathcal{E}} = o_{\mathcal{F}}\tilde{\omega}_1 + \ldots + o_{\mathcal{F}}\tilde{\omega}_{n-1} + o_{\mathcal{F}}(\alpha\tilde{\omega}_n)$$

eine relative Ganzheitsbasis von $\mathcal{E}$ erhält.

Man kann die letzten Schritte in dem folgenden Algorithmus zusammenfassen:

Algorithmus II.58 (Berechnung einer relativen Ganzheitsbasis)
Input: *Die relative Maximalordnung* $o_{\mathcal{E}} = \mathfrak{a}_1\omega_1 + \ldots + \mathfrak{a}_n\omega_n$.
Output: *Eine relative Ganzheitsbasis* $o_{\mathcal{E}} = o_{\mathcal{F}}\eta_1 + \ldots + o_{\mathcal{F}}\eta_n$ *oder* `FALSE`, *falls keine relative Ganzheitsbasis existiert.*

(1) *Überführe die Pseudobasis in die Steinitz-Form:*

$$o_{\mathcal{E}} = o_{\mathcal{F}}\tilde{\omega}_1 + \ldots + o_{\mathcal{F}}\tilde{\omega}_{n-1} + \tilde{\mathfrak{a}}\tilde{\omega}_n.$$

(2) *Teste, ob das Ideal* $\tilde{\mathfrak{a}}$ *ein Hauptideal ist. Ist* $\tilde{\mathfrak{a}}$ *kein Hauptideal, dann gib* `FALSE` *aus und halte an.*

(3) *Berechne einen Erzeuger von* $\tilde{\mathfrak{a}}$:

$$\tilde{\mathfrak{a}} = \alpha o_{\mathcal{F}}.$$

(4) *Berechne die neuen Basis-Elemente:*

$$(1 \leq i < n)\ \eta_i := \tilde{\omega}_i,$$

$$\eta_n := \alpha\tilde{\omega}_n.$$

(5) *ENDE.*

In der Praxis zeigt sich, daß die Berechnung der Steinitz-Form sehr viel Zeit benötigt. Deshalb ist es erfreulich, daß man im allgemeinen zum Rechnen in der relativen Maximalordnung keine Ganzheitsbasis benötigt. Die Pseudobasis reicht völlig aus.

Kapitel III
Die Theorie des relativen Round 2

Die theoretischen Grundlagen des relativen Round-2-Algorithmus werden in diesem Kapitel beschrieben. Dazu gehören insbesondere die Begriffe $\mathfrak{p}$-maximal, $\mathfrak{p}$-maximale Relativoberordnung, $\mathfrak{p}$-Radikal und Multiplikatorring. Das wichtige Theorem dieses Kapitels ist das sogenannte *lokale Maximalitätskriterium* oder auch *Theorem von Pohst und Zassenhaus*.

Während des ganzen Kapitels wird $\mathcal{O}$ stets eine Relativordnung von $\mathcal{E}$ und $\mathfrak{p}$ immer ein Primideal in der Maximalordnung $o_{\mathcal{F}}$ sein.

III.1 Die $\mathfrak{p}$-Maximalität

Zu Beginn dieses Abschnitts werden die beiden Begriffe $\mathfrak{p}$-*maximal* und $\mathfrak{p}$-*maximale Relativoberordnung* eingeführt.

Definition III.1 *Die Relativordnung $\mathcal{O}$ heißt* $\mathfrak{p}$-maximal, *wenn gilt*

$$\mathfrak{p} \nmid [o_{\mathcal{E}} : \mathcal{O}].$$

Mit anderen Worten: das Primideal $\mathfrak{p}$ darf den Index von $o_{\mathcal{E}}$ zu $\mathcal{O}$ nicht teilen.

Definition III.2 *Die* $\mathfrak{p}$-maximale Relativoberordnung $\mathcal{O}_{\mathfrak{p}}$ *zu der Relativordnung $\mathcal{O}$ wird wie folgt definiert:*

$$\mathcal{O}_{\mathfrak{p}} := \{x \in o_{\mathcal{E}} \mid \exists \nu \geq 0 : \mathfrak{p}^{\nu} x \subseteq \mathcal{O}\}.$$

Man sieht sofort, daß $\mathcal{O} \subseteq \mathcal{O}_{\mathfrak{p}}$ gilt. Wie man dem Namen schon entnehmen kann, ist die $\mathfrak{p}$-maximale Relativoberordnung $\mathcal{O}_{\mathfrak{p}}$ sowohl eine Relativordnung in $\mathcal{E}$ als auch bereits $\mathfrak{p}$-maximal. Diese Eigenschaften werden in dem folgenden Lemma zusammengefaßt.

Lemma III.3 *Die $\mathfrak{p}$-maximale Relativoberordnung $\mathcal{O}_{\mathfrak{p}}$ zu der Relativordnung $\mathcal{O}$ hat die folgenden Eigenschaften:*

(1) $\mathcal{O}_{\mathfrak{p}}$ ist eine Relativordnung von $\mathcal{E}$.

(2) Es existiert ein $\mu \geq 0$ mit

$$\mathfrak{p}^{\mu} \mathcal{O}_{\mathfrak{p}} \subseteq \mathcal{O}.$$

(3) $\mathcal{O}_{\mathfrak{p}}$ ist eine $\mathfrak{p}$-maximale Relativordnung in $\mathcal{E}$.

Beweis: *Zum ersten Teil:* Es gilt $\mathcal{O} \subseteq \mathcal{O}_{\mathfrak{p}}$ und $\mathcal{O}_{\mathfrak{p}}$ ist ein Teilring von $o_{\mathcal{E}}$: Es seien $x, y \in \mathcal{O}_{\mathfrak{p}}$ beliebig. Es existieren ganze Zahlen $\nu_1, \nu_2 \geq 0$ mit

$$\mathfrak{p}^{\nu_1} x \subseteq \mathcal{O}, \ \mathfrak{p}^{\nu_2} y \subseteq \mathcal{O}.$$

Setzt man $\nu := \max\{\nu_1, \nu_2\}$, so gilt

$$\mathfrak{p}^{\nu}(x-y) \subseteq \mathfrak{p}^{\nu} x - \mathfrak{p}^{\nu} y \subseteq \mathfrak{p}^{\nu_1} x - \mathfrak{p}^{\nu_2} y \subseteq \mathcal{O} - \mathcal{O} \subseteq \mathcal{O}$$

und damit $(x-y) \in \mathcal{O}_{\mathfrak{p}}$. Außerdem gilt

$$\mathfrak{p}^{\nu_1+\nu_2} xy = \mathfrak{p}^{\nu_1} x \cdot \mathfrak{p}^{\nu_2} y \subseteq \mathcal{O} \cdot \mathcal{O} \subseteq \mathcal{O},$$

also $xy \in \mathcal{O}_{\mathfrak{p}}$.

Damit ist $\mathcal{O}_{\mathfrak{p}}$ eine absolute Ordnung in $o_{\mathcal{E}}$. Wegen $o_{\mathcal{F}} \subseteq \mathcal{O} \subseteq \mathcal{O}_{\mathfrak{p}}$ ist $\mathcal{O}_{\mathfrak{p}}$ aber auch eine Relativordnung in $o_{\mathcal{E}}$.

Zum zweiten Teil: Als Relativordnung ist $\mathcal{O}_{\mathfrak{p}}$ ein endlich erzeugter $\mathbb{Z}$-Modul vom Rang nm. Deshalb sei $\tau_1, \ldots, \tau_{nm} \in o_{\mathcal{E}}$ eine $\mathbb{Z}$-Basis von $\mathcal{O}_{\mathfrak{p}}$. Für $1 \leq i \leq nm$ existiert wegen $\tau_i \in \mathcal{O}_{\mathfrak{p}}$, ein $\nu_i \geq 0$ mit

$$\mathfrak{p}^{\nu_i} \tau_i \subseteq \mathcal{O}.$$

Wählt man jetzt $\mu := \max\{\nu_1, \ldots, \nu_{nm}\}$, so gilt

$$\mathfrak{p}^{\mu} \tau_i \subseteq \mathcal{O} \ (1 \leq i \leq nm).$$

Ein beliebiges $x \in \mathcal{O}_{\mathfrak{p}}$ hat eine Darstellung

$$x = \alpha_1 \tau_1 + \ldots + \alpha_{nm} \tau_{nm},$$

mit $\alpha_i \in \mathbb{Z}$ $(1 \leq i \leq nm)$. Außerdem gilt

$$\mathfrak{p}^{\mu} x = \alpha_1 \mathfrak{p}^{\mu} \tau_1 + \ldots + \alpha_{nm} \mathfrak{p}^{\mu} \tau_{nm} \subseteq \alpha_1 \mathcal{O} + \ldots + \alpha_{nm} \mathcal{O} \subseteq \mathcal{O}.$$

Womit dann auch die Behauptung

$$\mathfrak{p}^{\mu} \mathcal{O}_{\mathfrak{p}} \subseteq \mathcal{O}$$

gezeigt ist.

Zum dritten Teil: Angenommen, die Relativordnung $\mathcal{O}_{\mathfrak{p}}$ ist nicht $\mathfrak{p}$-maximal, dann gilt

$$\mathfrak{p} \mid [o_{\mathcal{E}} : \mathcal{O}_{\mathfrak{p}}].$$

Man wählt die Pseudobasen von $o_{\mathcal{E}}$ und $\mathcal{O}_{\mathfrak{p}}$ wie in Theorem II.42:

$$o_{\mathcal{E}} = \mathfrak{a}_1 \omega_1 + \ldots + \mathfrak{a}_n \omega_n,$$

$$\mathcal{O}_{\mathfrak{p}} = \mathfrak{a}_1 \mathfrak{b}_1 \omega_1 + \ldots + \mathfrak{a}_n \mathfrak{b}_n \omega_n, \tag{III-1}$$

mit Idealen $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ in $o_{\mathcal{F}}$, Elementen $\omega_1, \ldots, \omega_n \in \mathcal{E}$ und Idealen $\mathfrak{b}_1, \ldots, \mathfrak{b}_n \subseteq o_{\mathcal{F}}$. Insbesondere gilt dann nach Definition II.43

$$[o_{\mathcal{E}} : \mathcal{O}_{\mathfrak{p}}] = \prod_{i=1}^{n} \mathfrak{b}_i.$$

Aus der Primidealeigenschaft von $\mathfrak{p}$ folgt, daß ein $j \in \{1, \ldots, n\}$ existiert mit

$$\mathfrak{p} \mid \mathfrak{b}_j.$$

Man wählt $\kappa \geq 1$ so, daß

$$\mathfrak{b}_j = \mathfrak{p}^{\kappa} \mathfrak{c}, \ \mathfrak{p} \nmid \mathfrak{c}$$

gilt, wobei $\mathfrak{c}$ ein ganzes Ideal in $o_{\mathcal{F}}$ ist. Aus $\kappa > 0$ folgt $\mathfrak{b}_j \subset \mathfrak{c}$. Damit existiert aber ein Element $\alpha \in \mathfrak{a}_j \mathfrak{c}$ mit der Eigenschaft

$$\alpha \omega_j \notin \mathcal{O}_{\mathfrak{p}}. \tag{III-2}$$

(Gilt $\alpha \omega_j \in \mathcal{O}_{\mathfrak{p}}$ für alle $\alpha \in \mathfrak{a}_j \mathfrak{c}$, so folgt unter Beachtung der Pseudobasis von $\mathcal{O}_{\mathfrak{p}}$: $\mathfrak{a}_j \mathfrak{c} \subseteq \mathfrak{a}_j \mathfrak{b}_j$. Das erzwingt aber $\mathfrak{c} \subseteq \mathfrak{b}_j$, einen Widerspruch zu $\mathfrak{b}_j \subset \mathfrak{c}$.) Es gilt aber

$$\mathfrak{p}^{\kappa} \alpha \subseteq \mathfrak{p}^{\kappa} \mathfrak{a}_j \mathfrak{c} = \mathfrak{a}_j \mathfrak{p}^{\kappa} \mathfrak{c} = \mathfrak{a}_j \mathfrak{b}_j$$

und nach (III-1)

$$\mathfrak{p}^{\kappa} \alpha \omega_j \subseteq \mathcal{O}_{\mathfrak{p}}.$$

Aus Lemma III.3.(2) folgt dann

$$\mathfrak{p}^{\mu} \mathfrak{p}^{\kappa} \alpha \omega_j \subseteq \mathfrak{p}^{\mu} \mathcal{O}_{\mathfrak{p}} \subseteq \mathcal{O}.$$

Damit erhält man aus Definition III.2

$$\alpha \omega_j \in \mathcal{O}_{\mathfrak{p}},$$

einen Widerspruch zu (III-2), der Wahl von α. Die Relativordnung $\mathcal{O}_{\mathfrak{p}}$ muß also $\mathfrak{p}$-maximal sein. □

III.2 Das $\mathfrak{p}$-Radikal

Definition III.4 *Das $\mathfrak{p}$-Radikal der Relativordnung $\mathcal{O}$ wird definiert als*

$$I_{\mathfrak{p}}(\mathcal{O}) := \{x \in \mathcal{O} \mid \exists \nu > 0 : x^{\nu} \in \mathfrak{p}\mathcal{O}\}.$$

Um die Eigenschaften dieser Menge zu beweisen, benötigt man das folgende Lemma:

Lemma III.5 *Für jede ganze Zahl $s > 0$ gilt*

$$[\mathcal{O} : \mathfrak{p}^s\mathcal{O}] = \mathfrak{p}^{ns}.$$

Beweis: Ausgehend von

$$\mathcal{O} = \mathfrak{a}_1\omega_1 + \ldots + \mathfrak{a}_n\omega_n,$$

einer Pseudobasis der Ordnung $\mathcal{O}$, erhält man durch

$$\mathfrak{p}^s\mathcal{O} = \mathfrak{p}^s\mathfrak{a}_1\omega_1 + \ldots + \mathfrak{p}^s\mathfrak{a}_n\omega_n \tag{III-3}$$

eine Pseudobasis des Ideals $\mathfrak{p}^s\mathcal{O}$. Dies wird unten gezeigt. Damit hat man dann Pseudobasen von den Moduln $\mathcal{O}$ und $\mathfrak{p}^s\mathcal{O}$ wie in Theorem II.42. Es gilt

$$[\mathcal{O} : \mathfrak{p}^s\mathcal{O}] = \prod_{i=1}^{n} \mathfrak{p}^s = \mathfrak{p}^{ns}.$$

Man muß nur noch beweisen, daß durch (III-3) eine Pseudobasis von $\mathfrak{p}^s\mathcal{O}$ gegeben ist.

Es sei zunächst $x \in \mathfrak{p}^s\mathfrak{a}_1\omega_1 + \ldots + \mathfrak{p}^s\mathfrak{a}_n\omega_n$. Dann existieren $k_i \geq 0$ $(1 \leq i \leq n)$ und $\alpha_{i,j} \in \mathfrak{a}_i,\ \pi_{i,j} \in \mathfrak{p}^s$ $(1 \leq i \leq n, 1 \leq j \leq k_i)$ mit

$$x = \sum_{i=1}^{n} \underbrace{\left(\sum_{j=1}^{k_i} \alpha_{i,j}\pi_{i,j}\right)}_{\in \mathfrak{a}_i\mathfrak{p}^s} \omega_i = \sum_{i=1}^{n}\sum_{j=1}^{k_i} \left(\underbrace{\pi_{i,j}}_{\in \mathfrak{p}^s} \underbrace{\alpha_{i,j}\omega_i}_{\in \mathcal{O}}\right) = \in \mathfrak{p}^s\mathcal{O}.$$

Es sei jetzt $x \in \mathfrak{p}^s\mathcal{O}$. Dann existieren Elemente $y_i \in \mathcal{O},\ \pi_i \in \mathfrak{p}^s$ $(1 \leq i \leq r)$ mit

$$x = \sum_{i=1}^{r} \pi_i y_i,$$

und Elemente $\alpha_{i,j} \in \mathfrak{a}_j$ $(1 \leq i \leq r, 1 \leq j \leq n)$ mit

$$y_i = \sum_{j=1}^{n} \alpha_{i,j}\omega_j.$$

Es folgt

$$x = \sum_{i=1}^{r} \pi_i \left(\sum_{j=1}^{n} \alpha_{i,j}\omega_j\right) = \sum_{i=1}^{r} \left(\sum_{j=1}^{n} \pi_i\alpha_{i,j}\omega_j\right) =$$

$$\sum_{j=1}^{n} \left(\sum_{i=1}^{r} \pi_i\alpha_{i,j}\omega_j\right) = \sum_{j=1}^{n} \underbrace{\left(\sum_{i=1}^{r} \pi_i\alpha_{i,j}\right)}_{\in \mathfrak{p}^s\mathfrak{a}_j} \omega_j \in \sum_{j=1}^{n} \mathfrak{p}^s\mathfrak{a}_j\omega_j.$$

Die Gleichung (III-3) ist damit gezeigt. Die Pseudobasiseigenschaft folgt dann direkt aus der $\mathcal{F}$-linearen Unabhängigkeit der Elemente $\omega_1, \ldots, \omega_n$. □

Lemma III.6 *Für das $\mathfrak{p}$-Radikal $I_{\mathfrak{p}}(\mathcal{O})$ der Relativordnung $\mathcal{O}$ gelten:*

(1) Die Menge $I_{\mathfrak{p}}(\mathcal{O})$ ist ein Ideal in der Relativordnung $\mathcal{O}$.

(2) $I_{\mathfrak{p}}(\mathcal{O})$ ist der Durchschnitt aller Primideale von $\mathcal{O}$, die das Ideal $\mathfrak{p}\mathcal{O}$ enthalten.

(3) Es gibt höchstens n Primideale von $\mathcal{O}$, die das Ideal $\mathfrak{p}\mathcal{O}$ enthalten.

(4) Es gilt

$$I_{\mathfrak{p}}(\mathcal{O})^n \subseteq \mathfrak{p}\mathcal{O}.$$

Beweis: *Zum ersten Teil:* Nach Definition III.4 gilt $I_{\mathfrak{p}}(\mathcal{O}) \subseteq \mathcal{O}$. Für zwei beliebige Elemente $x, y \in I_{\mathfrak{p}}(\mathcal{O})$ existieren ganze Zahlen $\nu, \mu > 0$ mit der Eigenschaft

$$x^{\nu}, y^{\mu} \in \mathfrak{p}\mathcal{O}.$$

Dann gilt aber auch

$$(x-y)^{\nu+\mu} = \sum_{i=0}^{\nu+\mu} \binom{\nu+\mu}{i} x^{\nu+\mu-i}(-1)^i y^i =$$

$$\sum_{i=0}^{\mu} \binom{\nu+\mu}{i} \underbrace{x^{\nu+\mu-i}}_{(\nu+\mu-i\geq\nu)\Rightarrow\in\mathfrak{p}\mathcal{O}} \underbrace{(-1)^i y^i}_{\in\mathcal{O}} + \sum_{i=\mu+1}^{\mu+\nu} \binom{\nu+\mu}{i} \underbrace{x^{\nu+\mu-i}(-1)^i}_{\in\mathcal{O}} \underbrace{y^i}_{(i>\mu)\Rightarrow\in\mathfrak{p}\mathcal{O}} \in \mathfrak{p}\mathcal{O}.$$

Man erhält somit $(x-y) \in I_{\mathfrak{p}}(\mathcal{O})$, sowie $0 \in I_{\mathfrak{p}}(\mathcal{O})$. Da $\mathfrak{p}\mathcal{O}$ ein Ideal in $\mathcal{O}$ ist, folgt aus $x \in I_{\mathfrak{p}}(\mathcal{O})$ und $y \in \mathcal{O}$ sofort $xy \in I_{\mathfrak{p}}(\mathcal{O})$, denn es existiert eine ganze Zahl $\nu > 0$ mit

$$x^{\nu} \in \mathfrak{p}\mathcal{O}.$$

Damit sieht man sofort

$$(xy)^{\nu} = y^{\nu} \cdot x^{\nu} \in \mathcal{O} \cdot \mathfrak{p}\mathcal{O} \subseteq \mathfrak{p}\mathcal{O},$$

also

$$xy \in I_{\mathfrak{p}}(\mathcal{O}).$$

Damit ist die Idealeigenschaft nachgewiesen.

Zum zweiten Teil: Es sei $\mathfrak{P}$ ein Primideal in $\mathcal{O}$ mit $\mathfrak{p}\mathcal{O} \subseteq \mathfrak{P}$. Ist jetzt $x \in I_{\mathfrak{p}}(\mathcal{O})$ beliebig, so folgt mit geeignetem $\nu > 0$

$$x^{\nu} \in \mathfrak{p}\mathcal{O} \subseteq \mathfrak{P}.$$

Die Primidealeigenschaft des Ideals $\mathfrak{P}$ liefert (per Induktion nach ν)

$$x \in \mathfrak{P}.$$

Man erhält damit für ein beliebiges Primideal $\mathfrak{P}$ in $\mathcal{O}$ mit $\mathfrak{p}\mathcal{O} \subseteq \mathfrak{P}$

$$I_{\mathfrak{p}}(\mathcal{O}) \subseteq \mathfrak{P},$$

und daher auch

$$I_{\mathfrak{p}}(\mathcal{O}) \subseteq \bigcap_{\mathfrak{p}\mathcal{O}\subseteq\mathfrak{P}} \mathfrak{P},$$

wobei die Ideale $\mathfrak{P}$ natürlich Primideale in $\mathcal{O}$ sind.

Es seien $x \in \bigcap_{\mathfrak{p}\mathcal{O}\subseteq\mathfrak{P}} \mathfrak{P}$ beliebig und

$$\varphi : \mathcal{O} \to \mathcal{O}/\mathfrak{p}\mathcal{O}$$

$$\varphi : y \longmapsto y + \mathfrak{p}$$

der kanonische Ringhomomorphismus. Man erhält $\varphi(x) \in \varphi(\mathfrak{P})$ für alle Primideale $\mathfrak{P}$ wie oben. Nach Satz II.19 sind diese $\varphi(\mathfrak{P})$ aber gerade die Primideale in $\mathcal{O}/\mathfrak{p}\mathcal{O}$. Aus Satz II.18 folgt, daß $\varphi(x)$ nilpotent ist. Man erhält

$$\varphi(x^{\nu}) = \varphi(x)^{\nu} = 0 + \mathfrak{p}\mathcal{O} = 0_{\mathcal{O}/\mathfrak{p}\mathcal{O}},$$

für ein $\nu > 0$, und damit

$$x^{\nu} \in \mathfrak{p}\mathcal{O}$$

oder

$$x \in I_{\mathfrak{p}}(\mathcal{O}).$$

Damit ist auch die andere Richtung gezeigt:

$$\bigcap_{\mathfrak{p}\mathcal{O}\subseteq\mathfrak{P}} \mathfrak{P} \subseteq I_{\mathfrak{p}}(\mathcal{O}).$$

Zum dritten Teil: Da die Maximalordnung $o_{\mathcal{E}}$ ein Dedekindring ist, existieren Primideale $\mathfrak{P}_1, \ldots, \mathfrak{P}_s \subseteq o_{\mathcal{E}}$ und ganze Zahlen $e_1, \ldots, e_s > 0$ mit

$$\mathfrak{p} o_{\mathcal{E}} = \mathfrak{P}_1^{e_1} \cdot \ldots \cdot \mathfrak{P}_s^{e_s}.$$

In Satz II.55 sieht man außerdem, daß $s \leq n$ gilt.

Es sei nun $\mathfrak{P}$ ein Primideal in $\mathcal{O}$, das $\mathfrak{p}\mathcal{O}$ enthält, also

$$\mathfrak{p} o_{\mathcal{E}} \subseteq \mathfrak{P} o_{\mathcal{E}}.$$

Dann folgt für die Primidealzerlegung von $\mathfrak{P} o_{\mathcal{E}}$:

$$\mathfrak{P} o_{\mathcal{E}} = \mathfrak{P}_1^{\tilde{e_1}} \cdot \ldots \cdot \mathfrak{P}_s^{\tilde{e_s}},$$

wobei $0 \leq \tilde{e_i} \leq e_i$ $(1 \leq i \leq s)$. Es gilt aber auch $\mathfrak{P} o_{\mathcal{E}} \subset o_{\mathcal{E}}$, daher existiert $j \in \{1, \ldots, s\}$ mit $\tilde{e_j} > 0$, also

$$\mathfrak{P} \subseteq \mathfrak{P}_j.$$

$\mathfrak{P}_j \cap \mathcal{O}$ ist ein Ideal in $\mathcal{O}$, welches die 1 nicht enthält. Es folgt daher

$$\mathfrak{P} = \mathfrak{P} \cap \mathcal{O} \subseteq \mathfrak{P}_j \cap \mathcal{O} \subset \mathcal{O}.$$

Nach Satz II.15 ist aber $\mathfrak{P}$ ein maximales Ideal in der (absoluten) Ordnung $\mathcal{O}$. Man erhält damit

$$\mathfrak{P} = \mathfrak{P}_j \cap \mathcal{O}.$$

Die Primideale in $\mathcal{O}$, die das Ideal $\mathfrak{p}\mathcal{O}$ enthalten, gehören also zu den Idealen

$$\mathfrak{P}_i \cap \mathcal{O} \ (1 \leq i \leq s \leq n),$$

und dies sind höchstens n Stück.

Zum vierten Teil: Dieser Beweis gliedert sich in zwei Schritte. Als erstes zeigt man, daß ein $\nu \geq 0$ existiert mit $I_{\mathfrak{p}}(\mathcal{O})^{\nu} \subseteq \mathfrak{p}\mathcal{O}$, danach zeigt man, daß man schon $\nu = n$ wählen kann.

$I_{\mathfrak{p}}(\mathcal{O})$ ist als Ideal in einer (absoluten) Ordnung ein endlich erzeugter $\mathbb{Z}$-Modul, daher existieren $\tau_1, \ldots, \tau_{nm} \in I_{\mathfrak{p}}(\mathcal{O})$ mit

(III-4) $$I_{\mathfrak{p}}(\mathcal{O}) = \tau_1\mathbb{Z} + \ldots + \tau_{nm}\mathbb{Z}.$$

Für jedes τ_i $(1 \leq i \leq nm)$ existiert ein Exponent $\nu_i > 0$ mit

$$\tau_i^{\nu_i} \in \mathfrak{p}\mathcal{O}.$$

Man setzt

$$\nu := \sum_{i=1}^{nm} \nu_i.$$

Es sei nun $x \in I_{\mathfrak{p}}(\mathcal{O})^{\nu}$ beliebig, mit einer Darstellung

(III-5) $$x = \prod_{i=1}^{\nu} x_i,$$

wobei $x_i \in I_{\mathfrak{p}}(\mathcal{O})$ gelte. Jedes dieser Elemente x_i wird in der $\mathbb{Z}$-Basis (III-4) wie folgt dargestellt:

$$x_i = \sum_{j=1}^{nm} \xi_{i,j}\tau_j,$$

mit $\xi_{i,j} \in \mathbb{Z}$ $(1 \leq i \leq \nu, 1 \leq j \leq nm)$. Man erhält dann

$$x = \prod_{i=1}^{\nu} x_i = \prod_{i=1}^{\nu} \left(\sum_{j=1}^{nm} \xi_{i,j}\tau_j \right) = \sum_{k=1}^{(nm)^{\nu}} \zeta_k \tau_1^{\mu_{k,1}} \cdot \ldots \cdot \tau_{nm}^{\mu_{k,nm}},$$

wobei $\zeta_k \in \mathbb{Z}$ $(1 \leq k \leq (nm)^{\nu})$ geeignet gewählt seien, und

$$\sum_{i=1}^{nm} \mu_{k,i} = \nu \ (1 \leq k \leq (nm)^{\nu})$$

gilt. Für jedes $1 \leq k \leq (nm)^{\nu}$ existiert dann ein $j_k \in \{1, \ldots, nm\}$ mit

$$\mu_{k,j_k} \geq \nu_{j_k}.$$

Man erhält schließlich

$$x = \sum_{k=1}^{(nm)^{\nu}} \zeta_k \tau_1^{\mu_{k,1}} \cdot \ldots \cdot \tau_{nm}^{\mu_{k,nm}} = \sum_{k=1}^{(nm)^{\nu}} \left(\zeta_k \cdot \underbrace{\tau_{j_k}^{\mu_{k,j_k}}}_{\in \mathfrak{p}\mathcal{O}} \cdot \underbrace{\prod_{i \neq j_k} \tau_i^{\mu_{k,i}}}_{\in \mathcal{O}} \right) \in \mathfrak{p}\mathcal{O}.$$

Da $\mathfrak{p}\mathcal{O}$ ein Ideal in $\mathcal{O}$ ist, folgt auch $I_{\mathfrak{p}}(\mathcal{O})^{\nu} \subseteq \mathfrak{p}\mathcal{O}$, da jedes Element $y \in I_{\mathfrak{p}}(\mathcal{O})^{\nu}$ eine endliche Summe von Elementen x wie in (III-5) ist. Damit ist der erste Schritt bewiesen.

Es gelte o.B.d.A $\nu > n$ (sonst ist nichts mehr zu beweisen). Um auch den Rest zu beweisen, bildet man für $i > 0$ die Ideale

$$\mathfrak{a}_i := I_{\mathfrak{p}}(\mathcal{O})^i + \mathfrak{p}\mathcal{O}.$$

Es gelten

$$\mathfrak{a}_1 = I_{\mathfrak{p}}(\mathcal{O})$$

und

$$\mathcal{O} \supseteq \mathfrak{a}_1 \supseteq \mathfrak{a}_2 \supseteq \ldots \supseteq \mathfrak{a}_n \supseteq \mathfrak{a}_{n+1} \supseteq \ldots \supseteq \mathfrak{p}\mathcal{O}.$$

Aus Lemma III.5 folgt

(III-6) $$[\mathcal{O} : \mathfrak{p}\mathcal{O}] = \mathfrak{p}^n.$$

Angenommen es gelte

$$\mathfrak{a}_1 \supset \mathfrak{a}_2 \supset \ldots \supset \mathfrak{a}_n \supset \mathfrak{a}_{n+1}.$$

Dann erhält man

$$\mathfrak{p} \mid [\mathfrak{a}_i : \mathfrak{a}_{i+1}] \ (1 \leq i \leq n)$$

und daher, wegen $\mathfrak{c} := [\mathcal{O} : \mathfrak{a}_1] \neq o_{\mathcal{F}}$,

$$[\mathcal{O} : \mathfrak{p}\mathcal{O}] = [\mathcal{O} : \mathfrak{a}_1] \cdot [\mathfrak{a}_1 : \mathfrak{a}_2] \cdot \ldots \cdot [\mathfrak{a}_n : \mathfrak{a}_{n+1}] \cdot [\mathfrak{a}_{n+1} : \mathfrak{p}\mathcal{O}] = \mathfrak{c}\mathfrak{p}^{\lambda} \cdot [\mathfrak{a}_{n+1} : \mathfrak{p}\mathcal{O}],$$

wobei $\lambda \geq n$. Man erhält

$$[\mathcal{O} : \mathfrak{p}\mathcal{O}] \subseteq \mathfrak{c}\mathfrak{p}^n \cdot [\mathfrak{a}_{n+1} : \mathfrak{p}\mathcal{O}] \subset \mathfrak{p}^n,$$

einen Widerspruch zu (III-6). Es existiert also ein $k \in \{1, \ldots, n\}$ mit

$$\mathfrak{a}_k = \mathfrak{a}_{k+1}.$$

Jetzt zeigt man per Induktion, daß $\mathfrak{a}_j = \mathfrak{a}_{j+1}$ für alle $j \geq k$ gilt:
Es gelte also $\mathfrak{a}_j = \mathfrak{a}_{j+1}$ für $j \geq k$. Dann ist zu zeigen, daß auch $\mathfrak{a}_{j+1} = \mathfrak{a}_{j+2}$ gilt. Trivialerweise gilt $\mathfrak{a}_{j+1} \supseteq \mathfrak{a}_{j+2}$. Sei jetzt $x \in I_{\mathfrak{p}}(\mathcal{O})^{j+1}$. Es gilt

$$x = \sum_{i=1}^{r} y_i z_i,$$

wobei $y_i \in I_{\mathfrak{p}}(\mathcal{O}), z_i \in I_{\mathfrak{p}}(\mathcal{O})^j$ $(1 \leq i \leq r)$. Da $I_{\mathfrak{p}}(\mathcal{O})^j \subseteq \mathfrak{a}_j = \mathfrak{a}_{j+1} = I_{\mathfrak{p}}(\mathcal{O})^{j+1} + \mathfrak{p}\mathcal{O}$, existieren $\tilde{z_i} \in I_{\mathfrak{p}}(\mathcal{O})^{j+1}, \hat{z_i} \in \mathfrak{p}\mathcal{O}$ $(1 \leq i \leq r)$ mit

$$z_i = \tilde{z_i} + \hat{z_i} \ (1 \leq i \leq r).$$

Man erhält zusammengefaßt

$$x = \sum_{i=1}^{r} (y_i\tilde{z_i} + y_i\hat{z_i}) = \underbrace{\sum_{i=1}^{r} y_i\tilde{z_i}}_{\in I_{\mathfrak{p}}(\mathcal{O})^{j+2}} + \underbrace{\sum_{i=1}^{r} y_i\hat{z_i}}_{\in \mathfrak{p}\mathcal{O}} \in I_{\mathfrak{p}}(\mathcal{O})^{j+2} + \mathfrak{p}\mathcal{O} = \mathfrak{a}_{j+2},$$

und auch

$$\mathfrak{a}_{j+1} = I_{\mathfrak{p}}(\mathcal{O})^{j+1} + \mathfrak{p}\mathcal{O} \subseteq I_{\mathfrak{p}}(\mathcal{O})^{j+2} + \mathfrak{p}\mathcal{O} = \mathfrak{a}_{j+2},$$

womit der Induktionsbeweis abgeschlossen ist. Beachtet man das Ergebnis aus dem ersten Teil, so zeigt sich

$$I_{\mathfrak{p}}(\mathcal{O})^n \subseteq \mathfrak{a}_n = \ldots = \mathfrak{a}_{\nu} = I_{\mathfrak{p}}(\mathcal{O})^{\nu} + \mathfrak{p}\mathcal{O} \subseteq \mathfrak{p}\mathcal{O} + \mathfrak{p}\mathcal{O} \subseteq \mathfrak{p}\mathcal{O}.$$

$\square$

III.3 Das lokale Maximalitätskriterium

Am Anfang dieses Abschnitts wird von der Vereinbarung, daß $\mathcal{O}$ eine Relativordnung in $\mathcal{E}$ ist, losgelassen. Für die nächste Definition und das darauffolgende Lemma sei $\mathcal{O}$ eine absolute Ordnung in $\mathcal{E}$.

Definition III.7 *Es sei $\mathfrak{a}$ ein Ideal in der absoluten Ordnung $\mathcal{O}$. Die Menge*

$$[\mathfrak{a}/\mathfrak{a}] := \{x \in \mathcal{E} \mid x\mathfrak{a} \subseteq \mathfrak{a}\}$$

heißt der Multiplikatorring *des Ideals $\mathfrak{a}$.*

Lemma III.8 *Es sei $\mathfrak{a}$ ein Ideal in der absoluten Ordnung $\mathcal{O}$. Für den Multiplikatorring von $\mathfrak{a}$ gelten die folgenden Aussagen:*

(1)
$$[\mathfrak{a}/\mathfrak{a}] \subseteq o_{\mathcal{E}},$$

(2) $[\mathfrak{a}/\mathfrak{a}]$ ist eine absolute Ordnung in $\mathcal{E}$.

(3) Ist $\mathcal{O}$ sogar eine Relativordnung in $\mathcal{E}$, so ist auch $[\mathfrak{a}/\mathfrak{a}]$ eine Relativordnung in $\mathcal{E}$.

Beweis: *Zum ersten Teil:* Angenommen, es existiert ein Element $y \in [\mathfrak{a}/\mathfrak{a}] \setminus o_{\mathcal{E}}$, dann gibt es nach Satz II.24 ein Primideal $\{0\} \neq \mathfrak{P} \subseteq o_{\mathcal{E}}$, so daß für die $\mathfrak{P}$-exponentielle Bewertung von y gilt

$$\nu_{\mathfrak{P}}(y) < 0.$$

Da die Menge $\{\nu_{\mathfrak{P}}(x) \mid x \in \mathfrak{a}\} \subset \mathbb{Z}$ nach unten beschränkt ist, kann man ein Element $x \in \mathfrak{a}$ auswählen, so daß $\nu_{\mathfrak{P}}(x)$ minimal ist. Dann gilt

$$\nu_{\mathfrak{P}}(xy) = \nu_{\mathfrak{P}}(x) + \nu_{\mathfrak{P}}(y) < \nu_{\mathfrak{P}}(x).$$

Dies ist ist aber ein Widerspruch zu der Minimalität von $\nu_{\mathfrak{P}}(x)$, da, wegen $y \in [\mathfrak{a}/\mathfrak{a}]$, auch $xy \in \mathfrak{a}$.

Zum zweiten Teil: Nach Definition III.7 und Lemma III.8.(1) gilt

$$\mathcal{O} \subseteq [\mathfrak{a}/\mathfrak{a}] \subseteq o_{\mathcal{E}}.$$

Es seien noch $x, y \in [\mathfrak{a}/\mathfrak{a}]$ beliebig, dann gilt

$$(x-y)\mathfrak{a} \subseteq x\mathfrak{a} - y\mathfrak{a} \subseteq \mathfrak{a} - \mathfrak{a} \subseteq \mathfrak{a},$$

also $(x-y) \in [\mathfrak{a}/\mathfrak{a}]$, und

$$(xy)\mathfrak{a} \subseteq x(y\mathfrak{a}) \subseteq x\mathfrak{a} \subseteq \mathfrak{a},$$

also auch $xy \in [\mathfrak{a}/\mathfrak{a}]$. Man sieht, daß $[\mathfrak{a}/\mathfrak{a}]$ ein Teilring von $o_{\mathcal{E}}$ und damit eine absolute Ordnung in $\mathcal{E}$ ist.

Zum dritten Teil: Da $\mathcal{O}$ eine Relativordnung in $\mathcal{E}$ ist, gelten $o_{\mathcal{F}} \subseteq \mathcal{O}$ und

$$o_{\mathcal{F}} \subseteq \mathcal{O} \subseteq [\mathfrak{a}/\mathfrak{a}].$$

$[\mathfrak{a}/\mathfrak{a}]$ ist daher eine Relativordnung in $\mathcal{E}$. □

Ab jetzt sei $\mathcal{O}$ wieder eine Relativordnung in $\mathcal{E}$. Ein entscheidender Schritt in diesem Abschnitt ist das nun folgende Lemma:

Lemma III.9 *Es gilt*

$$\mathcal{O}' := [I_{\mathfrak{p}}(\mathcal{O})/I_{\mathfrak{p}}(\mathcal{O})] \subseteq \mathcal{O}_{\mathfrak{p}},$$

wobei $\mathcal{O}_{\mathfrak{p}}$ die in Definition III.2 eingeführte $\mathfrak{p}$-maximale Relativoberordnung von $\mathcal{O}$ ist.

Beweis: In Lemma III.8.(1) hat man gesehen, daß

$$\mathcal{O}' \subseteq o_{\mathcal{E}}$$

gilt. Man erhält deshalb

$$\mathcal{O}' = \{x \in \mathcal{E} \mid xI_{\mathfrak{p}}(\mathcal{O}) \subseteq I_{\mathfrak{p}}(\mathcal{O})\} = \{x \in o_{\mathcal{E}} \mid xI_{\mathfrak{p}}(\mathcal{O}) \subseteq I_{\mathfrak{p}}(\mathcal{O})\}.$$

Wegen $I_{\mathfrak{p}}(\mathcal{O}) \subseteq \mathcal{O}$ gilt auch

$$\mathcal{O}' \subseteq \{x \in o_{\mathcal{E}} \mid xI_{\mathfrak{p}}(\mathcal{O}) \subseteq \mathcal{O}\}.$$

Weiterhin erhält man aus $\mathfrak{p} \subseteq I_{\mathfrak{p}}(\mathcal{O})$

$$\mathcal{O}' \subseteq \{x \in o_{\mathcal{E}} \mid x\mathfrak{p} \subseteq \mathcal{O}\} \subseteq \{x \in o_{\mathcal{E}} \mid \exists \nu \geq 0 : x\mathfrak{p}^{\nu} \subseteq \mathcal{O}\} = \mathcal{O}_{\mathfrak{p}}.$$

□

Man benötigt noch eine weitere kleine Aussage, bevor man das große Theorem dieses Kapitels beweisen kann.

Lemma III.10 *Es existiert eine ganze Zahl $\kappa \geq 0$ mit der Eigenschaft*

$$[\mathcal{O}_{\mathfrak{p}} : \mathcal{O}] = \mathfrak{p}^{\kappa}.$$

Beweis: In Lemma III.3.(2) hat man gesehen, daß eine ganze Zahl $\mu \geq 0$ existiert mit

$$\mathfrak{p}^{\mu}\mathcal{O}_{\mathfrak{p}} \subseteq \mathcal{O}.$$

Man erhält dann

$$\mathfrak{p}^{\mu}\mathcal{O}_{\mathfrak{p}} \subseteq \mathcal{O} \subseteq \mathcal{O}_{\mathfrak{p}}.$$

Ähnlich wie im Beweis zu Lemma III.5 zeigt man, daß man aus

$$\mathcal{O}_{\mathfrak{p}} = \mathfrak{a}_1\omega_1 + \ldots + \mathfrak{a}_n\omega_n,$$

einer Pseudobasis von $\mathcal{O}_{\mathfrak{p}}$,

$$\mathfrak{p}^{\mu}\mathcal{O}_{\mathfrak{p}} = \mathfrak{p}^{\mu}\mathfrak{a}_1\omega_1 + \ldots + \mathfrak{p}^{\mu}\mathfrak{a}_n\omega_n,$$

also eine Pseudobasis von $\mathfrak{p}^{\mu}\mathcal{O}_{\mathfrak{p}}$ erhält. Man sieht dann auch, daß

$$[\mathcal{O}_{\mathfrak{p}} : \mathcal{O}] \cdot [\mathcal{O} : \mathfrak{p}^{\mu}\mathcal{O}_{\mathfrak{p}}] = [\mathcal{O}_{\mathfrak{p}} : \mathfrak{p}^{\mu}\mathcal{O}_{\mathfrak{p}}] = \mathfrak{p}^{\mu n}$$

gilt, und daher

$$[\mathcal{O}_{\mathfrak{p}} : \mathcal{O}] \mid \mathfrak{p}^{\mu n}.$$

Hieraus folgt aber auch sofort, mit $\kappa \in \{0, \ldots, \mu n\}$ geeignet, die Behauptung. □

Theorem III.11 (Das lokale Maximalitätskriterium) *Setzt man wieder*

$$\mathcal{O}' := [I_{\mathfrak{p}}(\mathcal{O})/I_{\mathfrak{p}}(\mathcal{O})] \subseteq \mathcal{O}_{\mathfrak{p}},$$

dann gilt entweder

$$\mathcal{O} = \mathcal{O}',$$

und in diesem Fall ist die Relativordnung $\mathcal{O}$ bereits $\mathfrak{p}$-maximal, oder es gilt

$$\mathfrak{p} \mid [\mathcal{O}' : \mathcal{O}].$$

Beweis: $\mathcal{O}'$ ist der Multiplikatorring des Ideals $I_{\mathfrak{p}}(\mathcal{O})$. Es gilt also in jedem Fall

$$\mathcal{O} \subseteq \mathcal{O}'.$$

$\mathcal{O}_{\mathfrak{p}}$ sei die $\mathfrak{p}$-maximale Relativoberordnung von $\mathcal{O}$, die in Definition III.2 erklärt wurde.

Es gelte jetzt $\mathcal{O} = \mathcal{O}'$. Es ist also zu zeigen, daß $\mathcal{O}$ $\mathfrak{p}$-maximal ist. Nach Lemma III.3.(2) existiert eine ganze Zahl $\mu \geq 0$ mit

$$\mathfrak{p}^{\mu}\mathcal{O}_{\mathfrak{p}} \subseteq \mathcal{O},$$

und nach Lemma III.6.(4) gilt

$$I_{\mathfrak{p}}(\mathcal{O})^n \subseteq \mathfrak{p}\mathcal{O}.$$

Es folgt

$$\mathcal{O}_{\mathfrak{p}}I_{\mathfrak{p}}(\mathcal{O})^{n\mu} = \mathcal{O}_{\mathfrak{p}}\left(I_{\mathfrak{p}}(\mathcal{O})^n\right)^{\mu} \subseteq \mathcal{O}_{\mathfrak{p}}(\mathfrak{p}\mathcal{O})^{\mu} = \mathcal{O}_{\mathfrak{p}}\mathfrak{p}^{\mu}\mathcal{O}^{\mu} = \mathcal{O}_{\mathfrak{p}}\mathfrak{p}^{\mu}\mathcal{O} \subseteq \mathcal{O}\mathcal{O} = \mathcal{O}.$$

Angenommen, es gelte $\mathcal{O} \neq \mathcal{O}_{\mathfrak{p}}$, also $\mathcal{O} \not\supseteq \mathcal{O}_{\mathfrak{p}}$. Dann kann man $\lambda \in \{0, \ldots, \mu n\}$ maximal wählen mit der Eigenschaft

$$\mathcal{O}_{\mathfrak{p}}I_{\mathfrak{p}}(\mathcal{O})^{\lambda} \not\subseteq \mathcal{O}.$$

Dann gelten

$$\mathcal{O}_{\mathfrak{p}}I_{\mathfrak{p}}(\mathcal{O})^{\lambda+1} \subseteq \mathcal{O}$$

und auch

$$\mathcal{O}_{\mathfrak{p}}I_{\mathfrak{p}}(\mathcal{O})^{\lambda+n+1} = \mathcal{O}_{\mathfrak{p}}I_{\mathfrak{p}}(\mathcal{O})^{\lambda+1}I_{\mathfrak{p}}(\mathcal{O})^n \subseteq \mathcal{O}I_{\mathfrak{p}}(\mathcal{O})^n \subseteq I_{\mathfrak{p}}(\mathcal{O})^n \subseteq \mathfrak{p}\mathcal{O}.$$

Jetzt wählt man ein Element $x \in \mathcal{O}_{\mathfrak{p}}I_{\mathfrak{p}}(\mathcal{O})^{\lambda} \setminus \mathcal{O}$ fest und $y \in I_{\mathfrak{p}}(\mathcal{O})$ sei beliebig. Man sieht

$$(xy)^{\lambda+n+1} \in \left(\mathcal{O}_{\mathfrak{p}}I_{\mathfrak{p}}(\mathcal{O})^{\lambda+1}\right)^{\lambda+n+1} =$$

$$\mathcal{O}_{\mathfrak{p}}{}^{\lambda+n+1}I_{\mathfrak{p}}(\mathcal{O})^{(\lambda+1)(\lambda+n+1)} \subseteq \mathcal{O}_{\mathfrak{p}}I_{\mathfrak{p}}(\mathcal{O})^{\lambda+n+1} \subseteq \mathfrak{p}\mathcal{O}.$$

Es folgt

$$xy \in I_\mathfrak{p}(\mathcal{O}).$$

Da $y \in I_\mathfrak{p}(\mathcal{O})$ beliebig gewählt war, folgt sogar

$$xI_\mathfrak{p}(\mathcal{O}) \subseteq I_\mathfrak{p}(\mathcal{O}),$$

also

$$x \in [I_\mathfrak{p}(\mathcal{O})/I_\mathfrak{p}(\mathcal{O})] = \mathcal{O}'.$$

Dies ist aber ein Widerspruch, da $x \notin \mathcal{O} = \mathcal{O}'$. Es muß also $\mathcal{O} = \mathcal{O}_\mathfrak{p}$ gelten und $\mathcal{O}$ bereits $\mathfrak{p}$-maximal sein.

Es gelte jetzt $\mathcal{O} \neq \mathcal{O}'$, also $\mathcal{O} \subset \mathcal{O}'$. Damit gilt dann nach Lemma III.9

$$\mathcal{O} \subset \mathcal{O}' \subseteq \mathcal{O}_\mathfrak{p}.$$

Nach Lemma III.10 existiert eine ganze Zahl $\kappa \geq 0$ mit

$$[\mathcal{O}_\mathfrak{p} : \mathcal{O}'] \cdot [\mathcal{O}' : \mathcal{O}] = [\mathcal{O}_\mathfrak{p} : \mathcal{O}] = \mathfrak{p}^\kappa,$$

also

$$\mathfrak{p} \mid [\mathcal{O}' : \mathcal{O}] \mid \mathfrak{p}^\kappa.$$

□

III.4 Ein einfacher Algorithmus

Man kann jetzt einen einfachen Algorithmus angeben, mit dem man, ausgehend von einer Relativordnung $\mathcal{O}$ in $\mathcal{E}$, die Maximalordnung $o_\mathcal{E}$ von $\mathcal{E}$ berechnen kann.

Es sei $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_s\}$ die Menge der Primideale in $o_\mathcal{F}$, die die Diskriminante von $\mathcal{O}$ quadratisch teilen. Es gilt die folgende Aussage:

Lemma III.12 *Für eine beliebige Relativordnung $\mathcal{O}'$ mit*

$$\mathcal{O} \subseteq \mathcal{O}' \subseteq o_\mathcal{E}$$

gilt

$$[o_\mathcal{E} : \mathcal{O}'] = \mathfrak{p}_1^{e_1} \cdot \ldots \cdot \mathfrak{p}_s^{e_s},$$

wobei die Exponenten $e_i \in \mathbb{Z}^{\geq 0}$.

Beweis: Aus Satz II.44 folgt

$$\mathfrak{d}_{\mathcal{E}/\mathcal{F}}(\mathcal{O}) = \mathfrak{d}_{\mathcal{E}/\mathcal{F}}(o_\mathcal{E}) \cdot [o_\mathcal{E} : \mathcal{O}']^2 \cdot [\mathcal{O}' : \mathcal{O}]^2.$$

Die Behauptung folgt dann unmittelbar aus der Eindeutigkeit der Primidealzerlegung der Ideale in $o_\mathcal{F}$, man vergleiche hierzu Satz II.8:

$$\mathfrak{d}_{\mathcal{E}/\mathcal{F}}(\mathcal{O}) = \mathfrak{p}_1^{\hat{e}_1} \cdot \ldots \cdot \mathfrak{p}_s^{\hat{e}_s} \cdot \tilde{\mathfrak{p}}_1 \cdot \ldots \cdot \tilde{\mathfrak{p}}_{\tilde{s}},$$

wobei die Primideale $\mathfrak{p}_1, \ldots, \mathfrak{p}_s, \tilde{\mathfrak{p}}_1, \ldots, \tilde{\mathfrak{p}}_{\tilde{s}}$ paarweise verschieden sind, und für die Exponenten $\hat{e}_i \geq 2$ $(1 \leq i \leq s)$ gilt. Man sieht, daß außerdem $\hat{e}_i \geq 2e_i$ $(1 \leq i \leq s)$ gelten muß. □

Man definiert jetzt

$$\mathcal{O}_i := \mathcal{O}_{\mathfrak{p}_i} \ (1 \leq i \leq s),$$

also die $\mathfrak{p}_i$-maximale Relativoberordnungen der Relativordnung $\mathcal{O}$. Die Relativordnungen $\mathcal{O}_i$ kann man nach Theorem III.11 berechnen. Ein Algorithmus dafür wird unten angegeben. Die nächste Aussage beschreibt, wie man von den einzelnen $\mathfrak{p}$-maximalen Relativordnungen zu der Maximalordnung $o_\mathcal{E}$ kommt:

Lemma III.13

$$o_\mathcal{E} = \mathcal{O}_1 + \ldots + \mathcal{O}_s.$$

Beweis: Zur Vereinfachung der Schreibweise setzt man

$$\widetilde{\mathcal{O}} := \mathcal{O}_1 + \ldots + \mathcal{O}_s.$$

Trivialerweise gilt nach Definition III.2 $\mathcal{O}_i \subseteq o_\mathcal{E}$ $(1 \leq i \leq s)$ und damit auch

$$\widetilde{\mathcal{O}} \subseteq o_\mathcal{E}.$$

Als nächstes zeigt man, daß $\widetilde{\mathcal{O}}$ ein Ring ist. Es seien $x, y \in \widetilde{\mathcal{O}}$ zwei beliebige Elemente. Es existieren Elemente $x_i, y_i \in \mathcal{O}_i$ $(1 \leq i \leq s)$ mit

$$x = x_1 + \ldots + x_n,$$
$$y = y_1 + \ldots + y_n.$$

Dann gilt

$$x - y = \sum_{i=1}^{s} x_i - \sum_{i=1}^{s} y_i = \sum_{i=1}^{s} \underbrace{(x_i - y_i)}_{\in \mathcal{O}_i} \in \widetilde{\mathcal{O}}.$$

Weiterhin seien $i, j \in \{1, \ldots, s\} i \neq j$ fest gewählt. Nach Lemma III.3.(2) existieren $\mu_i, \mu_j \geq 0$ mit

$$\mathfrak{p}_i^{\mu_i} \mathcal{O}_{\mathfrak{p}_i} \subseteq \mathcal{O},$$
$$\mathfrak{p}_j^{\mu_j} \mathcal{O}_{\mathfrak{p}_j} \subseteq \mathcal{O},$$

Aus der Teilerfremdheit der Ideale $\mathfrak{p}_i^{\mu_i}, \mathfrak{p}_j^{\mu_j}$ folgt die Existenz der Elemente $\pi_i \in \mathfrak{p}_i^{\mu_i}, \pi_j \in \mathfrak{p}_j^{\mu_j}$ mit der Eigenschaft

$$\pi_i + \pi_j = 1.$$

Es folgt

$$x_i y_j = \underbrace{\pi_i x_i}_{\in \mathfrak{p}_i^{\mu_i} \mathcal{O}_{\mathfrak{p}_i}} \underbrace{y_j}_{\in \mathcal{O}_j} + \underbrace{\pi_j y_j}_{\in \mathfrak{p}_j^{\mu_j} \mathcal{O}_{\mathfrak{p}_j}} \underbrace{x_j}_{\in \mathcal{O}_i} \subseteq \mathcal{O} \cdot \mathcal{O}_j + \mathcal{O} \cdot \mathcal{O}_i \subseteq \mathcal{O}_j + \mathcal{O}_i.$$

Man erhält damit

$$xy = \left(\sum_{i=1}^{s} x_i \right) \cdot \left(\sum_{j=1}^{s} y_j \right) = \sum_{i=1}^{s} \sum_{j=1}^{s} \underbrace{x_i y_j}_{\in \mathcal{O}_i + \mathcal{O}_j} \in \widetilde{\mathcal{O}}.$$

Demnach ist $\widetilde{\mathcal{O}}$ ein Teilring von $o_\mathcal{E}$, und wegen $\mathcal{O} \subseteq \widetilde{\mathcal{O}}$ auch eine Relativordnung von $\mathcal{E}$.

Angenommen, es gilt $[o_\mathcal{E} : \widetilde{\mathcal{O}}] \neq o_\mathcal{F}$. Dann folgt aus Lemma III.12 die Existenz eines $j \in \{1, \ldots, s\}$ mit

$$\mathfrak{p}_j \mid [o_\mathcal{E} : \widetilde{\mathcal{O}}].$$

Es gilt aber

$$\mathcal{O}_{\mathfrak{p}_j} \subseteq \widetilde{\mathcal{O}} \subseteq o_\mathcal{E},$$

und damit

$$\mathfrak{p}_j \mid [o_\mathcal{E} : \widetilde{\mathcal{O}}] \mid [o_\mathcal{E} : \mathcal{O}_{\mathfrak{p}_j}].$$

Dies ist ein Widerspruch zu Lemma III.3.(3).

Man erhält damit insgesamt: $\widetilde{\mathcal{O}} \subseteq o_\mathcal{E}$ ist eine Relativordnung und $[o_\mathcal{E} : \widetilde{\mathcal{O}}] = o_\mathcal{F}$. Es folgt also

$$o_\mathcal{E} = \widetilde{\mathcal{O}}.$$

□

Zum Abschluß dieses Kapitels werden die Algorithmen zur Berechnung der $\mathfrak{p}$-maximalen Relativoberordnung und der Maximalordnung $o_\mathcal{E}$, ausgehend von einer beliebigen Relativordnung $\mathcal{O}$, angegeben. Eine Relativordnung oder ein Ideal in einer Relativordnung berechnen heißt, eine Pseudobasis wie in Satz II.47 oder Satz II.52 berechnen.

Einen Algorithmus zur Berechnung der $\mathfrak{p}$-maximalen Relativoberordnung zu einer gegebenen Relativordnung $\mathcal{O}$ und einem beliebigen Primideal $\mathfrak{p}$ in $o_\mathcal{F}$ erhält man aus Theorem III.11. Die Einzelheiten und die Algorithmen zur Berechnung des $\mathfrak{p}$-Radikals und des Multiplikatorringes werden in den folgenden Kapiteln behandelt.

Algorithmus III.14 (Berechnung der $\mathfrak{p}$-maximalen Relativoberordnung)

Input: *Relativordnung $\mathcal{O} = \mathfrak{a}_1\omega_1 + \ldots + \mathfrak{a}_n\omega_n$ und ein Primideal $\mathfrak{p}$ in $o_\mathcal{F}$.*
Output: *$\mathfrak{p}$-maximale Relativoberordnung $\mathcal{O}_\mathfrak{p} = \mathfrak{b}_1\tau_1 + \ldots + \mathfrak{b}_n\tau_n$.*
(1) *Setze $\mathcal{O}_2 := \mathcal{O}$.*
(2) *wiederhole*
(3) *Setze $\mathcal{O}_1 := \mathcal{O}_2$.*
(4) *Berechne das $\mathfrak{p}$-Radikal $I_\mathfrak{p}(\mathcal{O}_1)$ der Relativordnung $\mathcal{O}_1$.*
(5) *Berechne den Multiplikatorring: $\mathcal{O}_2 := [I_\mathfrak{p}(\mathcal{O}_1)/I_\mathfrak{p}(\mathcal{O}_1)]$.*
(6) *solange bis $\mathcal{O}_1 = \mathcal{O}_2$.*
(7) *Setze $\mathcal{O}_\mathfrak{p} := \mathcal{O}_1$.*
(8) *ENDE.*

Um den Algorithmus zur Berechnung der Maximalordnung aufzuschreiben, benötigt man noch einen Algorithmus, der es erlaubt, die einzelnen $\mathfrak{p}$-maximalen Relativordnungen zu einer Ordnung zusammenzusetzen. In Lemma III.13 hat man gesehen, daß die gewöhnliche Addition von Elementen aus den verschiedenen $\mathfrak{p}$-maximalen Ordnungen ausreicht, um alle Elemente der Maximalordnung zu erhalten. Es genügt also, die $o_{\mathcal{F}}$-Moduln zu addieren. Dies geschieht einfach durch Aneinanderreihen der Pseudobasen und der anschließenden Anwendung einer relativen Normalform wie in Theorem II.41:

Algorithmus III.15 (Addition der $\mathfrak{p}$-maximalen Relativoberordnungen)

Input: *Die Relativordnung $\mathcal{O} = \mathfrak{a}_1\omega_1 + \ldots + \mathfrak{a}_n\omega_n$ und die $\mathfrak{p}$-maximalen Relativoberordnungen: $\mathcal{O} \subseteq \mathcal{O}_{\mathfrak{p}_i} = \mathfrak{a}_{i,1}\omega_{i,1} + \ldots + \mathfrak{a}_{i,n}\omega_{i,n}$ $(1 \leq i \leq s)$.*

Output: *Die Summe der Ordnungen: $\widetilde{\mathcal{O}} = \mathfrak{b}_1\tau_1 + \ldots + \mathfrak{b}_n\tau_n$.*

(1) *Setze den Modul zusammen:*

$$\mathcal{M} := \begin{pmatrix} \mathfrak{a}_{1,1} & \cdots & \mathfrak{a}_{1,n} & \mathfrak{a}_{2,1} & \cdots & \mathfrak{a}_{2,n} & \cdots & \mathfrak{a}_{n,1} & \cdots & \mathfrak{a}_{n,n} \\ & M_1 & & & M_2 & & \cdots & & M_n & \end{pmatrix},$$

wobei die Matrizen $M_i \in \mathcal{F}^{n\times n}$ $(1 \leq i \leq s)$ die Matrizen mit der Eigenschaft

$$(\omega_1, \ldots, \omega_n) \cdot M_i = (\omega_{i,1}, \ldots, \omega_{i,n})$$

sind.

(2) *Wende eine relative Normalform wie in Theorem II.41 an:*

$$\begin{pmatrix} \mathfrak{b}_1 & \cdots & \mathfrak{b}_n \\ & \tilde{M} & \end{pmatrix} := \mathrm{HNF}(\mathcal{M}).$$

(3) *Berechne die Elemente τ_i $(1 \leq i \leq n)$:*

$$(\tau_1, \ldots, \tau_n) := (\omega_1, \ldots, \omega_n) \cdot \tilde{M}.$$

(4) *Setze:*

$$\widetilde{\mathcal{O}} = \mathfrak{b}_1\tau_1 + \ldots + \mathfrak{b}_n\tau_n.$$

(5) *ENDE.*

Der Algorithmus zur Berechnung der Maximalordnung, ausgehend von einer beliebigen Relativordnung $\mathcal{O}$, orientiert sich an den Aussagen zu Beginn dieses Abschnittes.

Algorithmus III.16 (Berechnung der relativen Maximalordnung)

Input: *Relativordnung $\mathcal{O} = \mathfrak{a}_1\omega_1 + \ldots + \mathfrak{a}_n\omega_n$.*

Output: *Maximalordnung $o_{\mathcal{E}} = \mathfrak{b}_1\tau_1 + \ldots + \mathfrak{b}_n\tau_n$.*

(1) *Berechne die Diskriminante $\mathfrak{d}_{\mathcal{E}/\mathcal{F}}(\mathcal{O})$ der Relativordnung $\mathcal{O}$. (Hierzu kann zum Beispiel Definition II.48 verwendet werden.)*

(2) *Es seien $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ die Primideale, die quadratisch in der Diskriminante aufgehen.*

(3) *Für $(1 \leq i \leq s)$ berechne mit Algorithmus III.14 die $\mathfrak{p}_i$-maximale Relativoberordnung $\mathcal{O}_{\mathfrak{p}_i}$ von $\mathcal{O}$.*

(4) *Bilde mit Algorithmus III.15 die Summe der Ordnungen:*

$$o_{\mathcal{E}} := \mathcal{O}_{\mathfrak{p}_1} + \ldots + \mathcal{O}_{\mathfrak{p}_s}.$$

(5) *ENDE.*

Kapitel IV
Das Dedekind-Kriterium

In diesem Kapitel soll ein Kriterium hergeleitet werden, das entscheidet, ob die Relativgleichungsordnung $o_{\mathcal{F}}[\rho]$ für ein Primideal $\mathfrak{p}$ in $o_{\mathcal{F}}$ bereits $\mathfrak{p}$-maximal ist. Ist die Relativgleichungsordnung $o_{\mathcal{F}}[\rho]$ nicht $\mathfrak{p}$-maximal, so kann der erste Schritt ($\mathcal{O}_2 := [I_{\mathfrak{p}}(o_{\mathcal{F}}[\rho])/I_{\mathfrak{p}}(o_{\mathcal{F}}[\rho])]$) von Algorithmus III.14 sofort angegeben werden. Für den Rest dieses Kapitels sei also $\mathfrak{p}$ ein Primideal in $o_{\mathcal{F}}$ fest gewählt. $T \in o_{\mathcal{F}}[\rho]$ sei das Polynom, das die Relativerweiterung $\mathcal{E}/\mathcal{F}$ erzeugt.

IV.1 Vorarbeiten

Man kann in den Ringen $o_{\mathcal{F}}$, $o_{\mathcal{F}}[\rho]$ und $o_{\mathcal{F}}[t]$ eine Reduktion modulo $\mathfrak{p}$ erklären. In den Ringen $o_{\mathcal{F}}[\rho]$ und $o_{\mathcal{F}}[t]$ arbeitet man dabei koeffizientenweise. Nach Satz II.15 ist das Primideal $\mathfrak{p}$ in der Maximalordnung $o_{\mathcal{F}}$ ein maximales Ideal. Der Restklassenring $o_{\mathcal{F}}/\mathfrak{p}$ ist daher ein Körper mit $\mathrm{N}_{\mathcal{F}/\mathbb{Q}}(\mathfrak{p}) = p^{\kappa}$ Elementen.

Im folgenden wird mit $\overline{x}$ immer die Klasse von x modulo $\mathfrak{p}$ bezeichnet (sowohl in $o_{\mathcal{F}}$, $o_{\mathcal{F}}[\rho]$ als auch in $o_{\mathcal{F}}[t]$). Ist ein Polynom $\overline{f} \in o_{\mathcal{F}}/\mathfrak{p}[t]$ gegeben, so wird mit $f \in o_{\mathcal{F}}[t]$ ein Repräsentant der Klasse $\overline{f}$ bezeichnet, der den gleichen Grad hat wie $\overline{f}$. Ist das Polynom $\overline{f}$ sogar normiert, dann kann man auch f normiert wählen.

Es sei

$$\overline{T} = \prod_{i=1}^{k} \overline{t_i}^{e_i}$$

die Faktorisierung des Polynoms T modulo $\mathfrak{p}$.

Die Polynome $t_i \in o_{\mathcal{F}}[t]$ $(1 \leq i \leq k)$ seien, wie oben vereinbart, normierte Repräsentanten der $\overline{t_i}$. Man definiert

$$g := \prod_{i=1}^{k} t_i \in o_{\mathcal{F}}[t].$$

Man sieht sofort, daß gilt

$$\overline{g} | \overline{T}.$$

Weiterhin definiert man das Polynom

$$\overline{h} := \overline{T}/\overline{g}.$$

Es sei $h \in o_{\mathcal{F}}[t]$ ein normierter Repräsentant von $\overline{h}$.

Satz IV.1 *Das $\mathfrak{p}$-Radikal der Relativgleichungsordnung $o_{\mathcal{F}}[\rho]$ ist gegeben durch*

$$I_{\mathfrak{p}}(o_{\mathcal{F}}[\rho]) = \mathfrak{p}o_{\mathcal{F}}[\rho] + g(\rho)o_{\mathcal{F}}[\rho].$$

Beweis: Es gilt $\mathfrak{p} \subseteq I_{\mathfrak{p}}(o_{\mathcal{F}}[\rho])$. Da die Exponenten $e_i \leq n$ sind, gilt wegen

$$\overline{g}^n = \prod_{i=1}^{k} \overline{t_i}^n = \prod_{i=1}^{k} \overline{t_i}^{e_i+(n-e_i)} = \overline{T} \cdot \prod_{i=1}^{k} \overline{t_i}^{n-e_i}$$

auch $\overline{T}|\overline{g}^n$. Somit gilt $g^n(\rho) \equiv 0 \mod \mathfrak{p}o_{\mathcal{F}}[\rho]$, also folgt $g(\rho) \in I_{\mathfrak{p}}(o_{\mathcal{F}}[\rho])$. Demnach ist bereits $\mathfrak{p}o_{\mathcal{F}}[\rho] + g(\rho)o_{\mathcal{F}}[\rho] \subseteq I_{\mathfrak{p}}(o_{\mathcal{F}}[\rho])$ gezeigt.

Für die andere Richtung überlegt man sich zuerst, daß $\overline{T}$ das Minimalpolynom von ρ über $o_{\mathcal{F}}/\mathfrak{p}$ ist: Es gilt $\overline{T}(\rho) = 0$. Also teilt das Minimalpolynom von ρ über $o_{\mathcal{F}}/\mathfrak{p}$ das Polynom $\overline{T}$. Auf der anderen Seite sind die Elemente $1, \rho, \ldots, \rho^{n-1}$ $o_{\mathcal{F}}/\mathfrak{p}$-linear unabhängig. (Man findet sonst ein Polynom $\overline{A_1} \in o_{\mathcal{F}}/\mathfrak{p}[t]$ mit den Eigenschaften $\deg(\overline{A_1}) < n$ und $\overline{A_1}(\rho) = 0$. Dann gilt aber $A_1(\rho) \in \mathfrak{p}$. Das Polynom $A_2 := A_1 - A_1(\rho)$ ist dann ein Polynom mit den Eigenschaften $A_2 \in o_{\mathcal{F}}[t]$, $\deg(A_2) < n$ und $A_2(\rho) = 0$. Dies ist aber ein Widerspruch zu der Minimalpolynom-Eigenschaft von T.) Das Minimalpolynom von ρ über $o_{\mathcal{F}}/\mathfrak{p}$ muß also mindestens den Grad n haben. Daraus folgt nun: Das Minimalpolynom von ρ über $o_{\mathcal{F}}/\mathfrak{p}$ ist $\overline{T}$.

Es sei $x \in I_{\mathfrak{p}}(o_{\mathcal{F}}[\rho])$. Es existiert ein Polynom $A \in o_{\mathcal{F}}[t]$ mit der Eigenschaft $A(\rho) = x$. Es existiert ein $r \in \mathbb{Z}^{>0}$ mit der Eigenschaft $x^r \in \mathfrak{p}o_{\mathcal{F}}[\rho]$. Daraus folgt $\overline{A}^r(\rho) = 0$. Es gilt $\overline{T}|\overline{A}^r$. Da die Exponenten e_i alle positiv sind, gilt $\overline{t_i}|\overline{A}^r$. Aus der Irreduzibilität der t_i folgt $\overline{t_i}|\overline{A}$. Weiterhin sind die t_i paarweise teilerfremd. Man erhält also $\overline{g}|\overline{A}$. Es muß ein Polynom $\overline{h_1} \in o_{\mathcal{F}}/\mathfrak{p}[t]$ existieren mit $\overline{A} = \overline{g}\overline{h_1}$, und ein Polynom $h_2 \in \mathfrak{p}[t]$ mit $A = gh_1 + h_2$. Zusammenfassend erhält man

$$x = A(\rho) = g(\rho) \cdot h_1(\rho) + h_2(\rho).$$

Es ist also $I_{\mathfrak{p}}(o_{\mathcal{F}}[\rho]) \subseteq \mathfrak{p}o_{\mathcal{F}}[\rho] + g(\rho)o_{\mathcal{F}}[\rho]$ gezeigt. □

Lemma IV.2 *Sei $\mathcal{O}$ eine (absolute) Ordnung in $\mathcal{F}$ und $\mathfrak{P}$ ein Primideal in $\mathcal{O}$. Dann existiert ein Element $\alpha \in \mathcal{F} \setminus \mathcal{O}$, so daß $\alpha\mathfrak{P} \subseteq \mathcal{O}$. Weiterhin gilt $\mathfrak{P}$ ist genau dann invertierbar in $\mathcal{O}$, wenn $\alpha\mathfrak{P} \not\subseteq \mathfrak{P}$ gilt. In diesem Fall gilt dann $\mathfrak{P}^{-1} = \mathcal{O} + \alpha\mathcal{O}$.*

Beweis: Den Beweis und einen Algorithmus zur Konstruktion eines solchen Elementes α kann man in [Coh93] nachlesen. □

Dieses Lemma, angewendet auf die Maximalordnung $o_{\mathcal{F}}$ und das Primideal $\mathfrak{p}$, zeigt die Existenz eines Elements $\tau \in \mathcal{F} \setminus o_{\mathcal{F}}$ mit der Eigenschaft

$$\mathfrak{p}^{-1} = o_{\mathcal{F}} + \tau o_{\mathcal{F}}$$

und den Bewertungen

$$\nu_{\mathfrak{p}}(\tau) = -1$$

und für Primideale $\mathfrak{q} \neq \mathfrak{p}$

$$\nu_{\mathfrak{q}}(\tau) \geq 0.$$

(Die Bewertungen rechnet man einfach nach.) Im folgenden sei τ wie oben gewählt.

Es sei $x \in \mathcal{O}' := [I_{\mathfrak{p}}(o_{\mathcal{F}}[\rho])/I_{\mathfrak{p}}(o_{\mathcal{F}}[\rho])]$. Dann gilt

$$xI_{\mathfrak{p}}(o_{\mathcal{F}}[\rho]) \subseteq I_{\mathfrak{p}}(o_{\mathcal{F}}[\rho]).$$

Beachtet man Satz IV.1 so sieht man, daß hieraus

$$x\mathfrak{p} \subseteq I_{\mathfrak{p}}(o_{\mathcal{F}}[\rho]) \subseteq o_{\mathcal{F}}[\rho]$$

folgt, oder

$$x \in \mathfrak{p}^{-1}o_{\mathcal{F}}[\rho] = o_{\mathcal{F}}[\rho] + \tau o_{\mathcal{F}}[\rho].$$

Es existieren also Polynome $A_1, A_2 \in o_{\mathcal{F}}[t]$ mit

$$x = A_1(\rho) + \tau A_2(\rho).$$

Um die Menge $\mathcal{O}'$ zu beschreiben, reicht es also aus, Elemente x mit einer solchen Darstellung

$$x = A_1(\rho) + \tau A_2(\rho)$$

mit Polynomen $A_1, A_2 \in o_{\mathcal{F}}[t]$ zu betrachten. Wegen $o_{\mathcal{F}}[\rho] \subseteq \mathcal{O}'$, gilt immer $A_1(\rho) \in \mathcal{O}'$. Es gilt also $x \in \mathcal{O}'$ genau dann, wenn $\tau A_2(\rho) \in \mathcal{O}'$.

Es werden noch die folgenden Definitionen eingeführt:

$$f := \tau(gh - T),$$

$$\overline{k} := \overline{g}/\gcd(\overline{f}, \overline{g}).$$

Das Polynom f liegt in $o_{\mathcal{F}}[t]$. Dies sieht man leicht ein, wenn man beachtet, daß $\overline{g}\overline{h} = \overline{T}$ und damit auch $(gh - T) \in \mathfrak{p}[t]$ gilt, und daß die Koeffizienten von f nach Lemma IV.2 in $\tau\mathfrak{p} \subseteq o_{\mathcal{F}}$ liegen. Wie üblich ist $k \in o_{\mathcal{F}}[t]$ ein normierter Repräsentant von $\overline{k}$.

Satz IV.3 *Sei $x = \tau A_1(\rho)$ mit einem Polynom $A_1 \in o_{\mathcal{F}}[t]$. Dann gelten:*

(1) $x\mathfrak{p} \subseteq I_{\mathfrak{p}}(o_{\mathcal{F}}[\rho])$ genau dann, wenn

$$\overline{g}|\overline{A_1},$$

(2) $xg(\rho) \in I_{\mathfrak{p}}(o_{\mathcal{F}}[\rho])$ genau dann, wenn

$$\overline{hk}|\overline{A_1}.$$

Beweis: *Zum ersten Teil:*

„$\Rightarrow$" Für ein beliebiges Element $y \in \mathfrak{p}$ gilt immer

$$\nu_{\mathfrak{p}}(\tau y) = \nu_{\mathfrak{p}}(\tau) + \nu_{\mathfrak{p}}(y) = \nu_{\mathfrak{p}}(y) - 1 \geq 1 - 1 = 0,$$

und für $\mathfrak{q} \neq \mathfrak{p}$

$$\nu_{\mathfrak{q}}(\tau y) = \nu_{\mathfrak{q}}(\tau) + \nu_{\mathfrak{q}}(y) \geq 0 + 0 = 0,$$

also auch $\tau y \in o_{\mathcal{F}}$.

Weiterhin sei $\pi \in \mathfrak{p} \setminus \mathfrak{p}^2$. Es gilt nach Lemma II.27

$$\nu_{\mathfrak{p}}(\tau\pi) = \nu_{\mathfrak{p}}(\pi) + \nu_{\mathfrak{p}}(\tau) = 1 - 1 = 0,$$

und damit $\tau\pi \notin \mathfrak{p}$.

Aus $\tau A_1(\rho)\mathfrak{p} \subseteq I_{\mathfrak{p}}(o_{\mathcal{F}}[\rho])$ folgt $\tau\pi A_1(\rho) \in I_{\mathfrak{p}}(o_{\mathcal{F}}[\rho]) = \mathfrak{p}o_{\mathcal{F}}[\rho] + g(\rho)o_{\mathcal{F}}[\rho]$, man beachte dabei Satz IV.1. Dies zeigt, daß Polynome $A_2 \in \mathfrak{p}[t], A_3 \in o_{\mathcal{F}}[t]$ existieren mit

$$\tau\pi A_1(\rho) = A_2(\rho) + g(\rho)A_3(\rho).$$

Es existiert daher ein Polynom $A_4 \in o_{\mathcal{F}}[t]$ mit

$$\tau\pi A_1 = A_2 + gA_3 + TA_4.$$

Man sieht, daß

$$\overline{g}|\overline{\tau\pi A_1}$$

gilt. Da aber $\overline{\tau\pi} \neq \overline{0}$ gilt, folgt hieraus

$$\overline{g}|\overline{A_1}.$$

„$\Leftarrow$" Es gelte nun

$$\overline{g}|\overline{A_1}.$$

Dann existieren Polynome $A_2 \in \mathfrak{p}[t], A_3 \in o_{\mathcal{F}}[t]$ mit

$$A_1 = A_2 + gA_3$$

und

$$A_1(\rho) = A_2(\rho) + g(\rho)A_3(\rho) \in \mathfrak{p}o_{\mathcal{F}}[\rho] + g(\rho)o_{\mathcal{F}}[\rho] = I_{\mathfrak{p}}(o_{\mathcal{F}}[\rho]).$$

Sei $y \in \mathfrak{p}$ beliebig. Da $\tau y \in o_{\mathcal{F}}$ und $I_{\mathfrak{p}}(o_{\mathcal{F}}[\rho])$ ein Ideal in $o_{\mathcal{F}}$ ist, folgt hieraus auch

$$\tau y A_1(\rho) \in I_{\mathfrak{p}}(o_{\mathcal{F}}[\rho]),$$

und daher natürlich $\tau A_1(\rho)\mathfrak{p} \subseteq I_{\mathfrak{p}}(o_{\mathcal{F}}[\rho])$.

Zum zweiten Teil:

„$\Rightarrow$" Es gelte $\tau A_1(\rho)g(\rho) \in I_{\mathfrak{p}}(o_{\mathcal{F}}[\rho])$. Nach Satz IV.1 folgt hieraus, daß Polynome $A_2 \in \mathfrak{p}[t], A_3 \in o_{\mathcal{F}}[t]$ existieren mit

$$A_1(\rho)g(\rho) = \tau^{-1}(A_2(\rho) + g(\rho)A_3(\rho)).$$

Man sieht, es existiert $A_4 \in o_{\mathcal{F}}[t]$ mit

$$A_1 g = \tau^{-1}(A_2 + gA_3) + A_4 T. \tag{IV-1}$$

Setzt man $A := A_2 + gA_3$, so folgt aus $A_1 g \in o_{\mathcal{F}}[t]$ sofort $\tau^{-1}A \in o_{\mathcal{F}}[t]$. Sei weiterhin $A = \sum_{i=1}^{s} \alpha_i t^i$. Es gilt die Abschätzung

$$\nu_{\mathfrak{p}}(\tau^{-1}\alpha_i) = \nu_{\mathfrak{p}}(\alpha_i) - \nu_{\mathfrak{p}}(\tau) \geq 0 - (-1) \geq 1 \ (1 \leq i \leq s),$$

und daher sogar $\tau^{-1}A \in \mathfrak{p}[t]$. Man erhält die folgende Gleichung:

$$A_1 g = \tau^{-1}A + A_4 T.$$

Betrachtet man diese Gleichung modulo $\mathfrak{p}$, so erhält man

$$\overline{A_1}\overline{g} = \overline{A_4 T},$$

oder mit Hilfe des Polynoms $\overline{h} = \overline{T}/\overline{g}$

$$\overline{A_1} = \overline{A_4 h}.$$

Daher existiert $A_5 \in \mathfrak{p}[t]$ mit

$$A_1 = A_4 h + A_5. \tag{IV-2}$$

Setzt man dieses Ergebnis in (IV-1) ein, so sieht man
$$g(A_4h + A_5) = \tau^{-1}(A_2 + gA_3) + A_4T.$$
Daraus folgt
$$(gh - T)A_4 = \tau^{-1}(A_2 + gA_3) - gA_5,$$
was wiederum
$$\tau(gh - T)A_4 = A_2 + gA_3 - \tau gA_5$$
impliziert und
$$fA_4 = A_2 + gA_3 - \tau gA_5$$
bedingt. Aus $A_5 \in \mathfrak{p}[t]$ folgt sofort mit Lemma IV.2 $A_6 := \tau A_5 \in o_{\mathcal{F}}[t]$ und daher die Gleichung
$$fA_4 = A_2 + g(A_3 + A_6).$$
Reduktion modulo $\mathfrak{p}$ zeigt
$$\overline{g}|\overline{fA_4}$$
oder unter Beachtung von $\overline{k} = \overline{g}/\gcd(\overline{f}, \overline{g})$
$$\overline{k}|\overline{A_4}.$$
Es existieren also Polynome $A_7 \in o_{\mathcal{F}}[t], A_8 \in \mathfrak{p}[t]$ mit
$$A_4 = kA_7 + A_8.$$
Setzt man das in die Gleichung (IV-2) ein, so erhält man
$$A_1 = hkA_7 + hA_8 + A_5,$$
wobei für die Polynome $A_5, A_8 \in \mathfrak{p}[t]$ gilt. Das zeigt aber auch $hA_8 + A_5 \in \mathfrak{p}[t]$, daher folgt durch Reduktion modulo $\mathfrak{p}$
$$\overline{hk}|\overline{A_1}.$$
„$\Leftarrow$“ Ausgehend von
$$\overline{hk}|\overline{A_1}$$
erhält man Polynome $A_2 \in o_{\mathcal{F}}[t], A_3 \in \mathfrak{p}[t]$ mit der Eigenschaft
$$A_1 = hkA_2 + A_3. \tag{IV-3}$$
Man sieht sofort
$$\overline{k}|\overline{kA_2},$$
also wegen $\overline{k} = \overline{g}/\gcd(\overline{f}, \overline{g})$ auch
$$\overline{g}|\overline{fkA_2}.$$
Dies sichert die Existenz der Polynome $A_4 \in o_{\mathcal{F}}[t], A_5 \in \mathfrak{p}[t]$ mit
$$fkA_2 = gA_4 + A_5,$$
oder unter Beachtung von $f = \tau(gh - T)$
$$\tau(gh - T)kA_2 = gA_4 + A_5.$$
Eine leichte Umformung bringt
$$\tau ghkA_2 = gA_4 + A_5 + \tau TkA_2.$$
Aus der Gleichung (IV-3) folgt
$$hkA_2 = A_1 - A_3.$$
Setzt man die beiden letzten Gleichungen zusammen, so bekommt man
$$\tau g(A_1 - A_3) = gA_4 + A_5 + \tau TkA_2$$
oder auch
$$\tau gA_1 = gA_4 + A_5 + \tau gA_3 + \tau TkA_2.$$
Nach Einsetzen von ρ in die obige Gleichung erhält man
$$\tau g(\rho)A_1(\rho) = g(\rho)A_4(\rho) + A_5(\rho) + \tau g(\rho)A_3(\rho).$$
Es folgt
$$\tau g(\rho)A_1(\rho) = g(\rho)(\tau A_3(\rho) + A_4(\rho)) + A_5(\rho),$$
also auch, man beachte Lemma IV.2: $\tau A_3(\rho) \in o_{\mathcal{F}}[\rho]$,
$$\tau g(\rho)A_1(\rho) \in g(\rho)o_{\mathcal{F}}[\rho] + \mathfrak{p}o_{\mathcal{F}}[\rho] = I_{\mathfrak{p}}(o_{\mathcal{F}}[\rho]).$$
□

IV.2 Das Kriterium

In diesem Abschnitt werden die Ergebnisse aus dem vorangegangenen Abschnitt zusammengefaßt. Es wird ein Kriterium angegeben, das entscheidet, ob die Relativgleichungsordnung $o_{\mathcal{F}}[\rho]$ $\mathfrak{p}$-maximal ist. Sollte die Relativgleichungsordnung $o_{\mathcal{F}}[\rho]$ nicht $\mathfrak{p}$-maximal sein, so kann der erste Schritt von Algorithmus III.14, also die relative Ordnung $[I_{\mathfrak{p}}(o_{\mathcal{F}}[\rho])/I_{\mathfrak{p}}(o_{\mathcal{F}}[\rho])]$, sofort angegeben werden.

Theorem IV.4 (Dedekind-Kriterium) *Es sei*
$$\overline{T} = \prod_{i=1}^{k} \overline{t_i}^{e_i}$$
die Faktorisierung des Polynoms T modulo $\mathfrak{p}$. Die Polynome $g, \overline{h}, f$ seien wie folgt definiert:
$$g := \prod_{i=1}^{k} t_i,$$
$$\overline{h} := \overline{T}/\overline{g}$$
und
$$f := \tau(gh - T),$$
wobei h ein normierter Repräsentant von $\overline{h}$ sei und $\tau \in \mathcal{F}$ wie in Lemma IV.2 gewählt sei. Dann gelten:

(1) Die Relativgleichungsordnung $o_{\mathcal{F}}[\rho]$ ist genau dann $\mathfrak{p}$-maximal, wenn
$$\gcd(\overline{f}, \overline{g}, \overline{h}) = 1.$$

(2) Sei weiterhin U ein normierter Repräsentant von $\overline{U} := \overline{T}/\gcd(\overline{f}, \overline{g}, \overline{h})$, so gilt sogar
$$[I_{\mathfrak{p}}(o_{\mathcal{F}}[\rho])/I_{\mathfrak{p}}(o_{\mathcal{F}}[\rho])] = o_{\mathcal{F}}[\rho] + \tau U(\rho)o_{\mathcal{F}}[\rho].$$

Beweis: Der erste Teil wird sofort aus dem zweiten Teil folgen.
Der zweite Teil: Für ein Element der Form
$$x = \tau A_1(\rho) + A_2(\rho) \tag{IV-4}$$
mit Polynomen $A_1 \in o_{\mathcal{F}}[t], A_2 \in \mathfrak{p}[t]$ gilt nach Satz IV.3.(1) $x\mathfrak{p} \subseteq I_{\mathfrak{p}}(o_{\mathcal{F}}[\rho])$ genau dann, wenn $\overline{g}|\overline{A_1}$ und nach Satz IV.3.(2) $xg(\rho) \in I_{\mathfrak{p}}(o_{\mathcal{F}}[\rho])$ genau dann, wenn $\overline{hk}|\overline{A_1}$. Beachtet man, daß nach Satz IV.1
$$I_{\mathfrak{p}}(o_{\mathcal{F}}[\rho]) = \mathfrak{p}o_{\mathcal{F}}[\rho] + g(\rho)o_{\mathcal{F}}[\rho]$$
gilt, so folgt sofort $x \in [I_{\mathfrak{p}}(o_{\mathcal{F}}[\rho])/I_{\mathfrak{p}}(o_{\mathcal{F}}[\rho])]$ genau dann, wenn $\operatorname{lcm}(\overline{g}, \overline{hk})|\overline{A_1}$. Da $o_{\mathcal{F}}/\mathfrak{p}[t]$ ein Hauptidealring ist, gelten für beliebige $\overline{A}, \overline{B}, \overline{C} \in o_{\mathcal{F}}/\mathfrak{p}[t]$ die beiden Regeln
$$\operatorname{lcm}(\overline{A}, \overline{B}) = \frac{\overline{AB}}{\gcd(\overline{A}, \overline{B})},$$
$$\operatorname{lcm}(\overline{CA}, \overline{CB}) = \overline{C} \cdot \operatorname{lcm}(\overline{A}, \overline{B}).$$
Damit gilt
$$\operatorname{lcm}(\overline{g}, \overline{hk}) = \operatorname{lcm}(\overline{k} \cdot \gcd(\overline{f}, \overline{g}), \overline{kh}) = \overline{k} \cdot \operatorname{lcm}(\gcd(\overline{f}, \overline{g}), \overline{h}) =$$
$$\frac{\overline{g}}{\gcd(\overline{f}, \overline{g})} \cdot \frac{\gcd(\overline{f}, \overline{g})\ \overline{h}}{\gcd(\gcd(\overline{f}, \overline{g}), \overline{h})} = \frac{\overline{gh}}{\gcd(\overline{f}, \overline{g}, \overline{h})} =$$
$$\frac{\overline{T}}{\gcd(\overline{f}, \overline{g}, \overline{h})} = \overline{U}.$$
Man sieht, daß $x \in [I_{\mathfrak{p}}(o_{\mathcal{F}}[\rho])/I_{\mathfrak{p}}(o_{\mathcal{F}}[\rho])]$ genau dann gilt, wenn $\overline{U}|\overline{A_1}$. Beachtet man noch, daß sich jedes Element $x \in [I_{\mathfrak{p}}(o_{\mathcal{F}}[\rho])/I_{\mathfrak{p}}(o_{\mathcal{F}}[\rho])]$ so darstellen läßt, wie in (IV-4), dann folgt
$$[I_{\mathfrak{p}}(o_{\mathcal{F}}[\rho])/I_{\mathfrak{p}}(o_{\mathcal{F}}[\rho])] = o_{\mathcal{F}}[\rho] + \tau U(\rho)o_{\mathcal{F}}[\rho].$$

Zum ersten Teil: Es gelte $\gcd(\overline{f},\overline{g},\overline{h}) = 1$. Das ist aber äquivalent zu

$$\overline{U} = \overline{T},$$

was wiederum äquivalent ist zu: Es existiert ein Polynom $A_2 \in \mathfrak{p}[t]$ mit

$$U = T + A_2.$$

Damit hat man

$$\tau U(\rho) = \tau T(\rho) + \tau A_2(\rho) = 0 + \tau A_2(\rho).$$

Weiterhin gilt $\tau A_2 \in o_{\mathcal{F}}[t]$, man beachte Lemma IV.2. Damit ist aber

$$\gcd(\overline{f},\overline{g},\overline{h}) = 1$$

äquivalent zu

$$\tau U(\rho) \in o_{\mathcal{F}}[\rho]$$

oder zu

$$[I_{\mathfrak{p}}(o_{\mathcal{F}}[\rho])/I_{\mathfrak{p}}(o_{\mathcal{F}}[\rho])] = o_{\mathcal{F}}[\rho].$$

□

Bemerkung IV.5 *Im absoluten Fall, also $\mathcal{F} = \mathbb{Q}$, wählt man als Element τ einfach p^{-1}, wobei natürlich $\mathfrak{p} = p\mathbb{Z}$ gilt.*

IV.3 Der Algorithmus

Es folgt der oben beschriebene Algorithmus. Falls die Relativgleichungsordnung $o_{\mathcal{F}}[\rho]$ schon $\mathfrak{p}$-maximal ist, wird `TRUE` ausgegeben, sonst erhält man die Relativoberordnung $\mathcal{O}' := [I_{\mathfrak{p}}(o_{\mathcal{F}}[\rho])/I_{\mathfrak{p}}(o_{\mathcal{F}}[\rho])]$ von $o_{\mathcal{F}}[\rho]$.

Algorithmus IV.6 (Dedekind-Test)
Input: *Das erzeugende Polynom $T \in o_{\mathcal{F}}[t]$ und ein Primideal $\mathfrak{p}$ in $o_{\mathcal{F}}$.*
Output: `TRUE`*, falls die Gleichungsordnung $o_{\mathcal{F}}[\rho]$ $\mathfrak{p}$-maximal ist, $\mathcal{O}' = [I_{\mathfrak{p}}(o_{\mathcal{F}}[\rho])/I_{\mathfrak{p}}(o_{\mathcal{F}}[\rho])]$, die Relativoberordnung von $o_{\mathcal{F}}[\rho]$ sonst.*

(1) *Faktorisiere das Polynom T modulo $\mathfrak{p}$:*

$$\overline{T} =: \prod_{i=1}^{k} \overline{t_i}^{e_i}.$$

(2) *Berechne die Polynome $g, \overline{g}, \overline{h}, h, f, \overline{f}$:*

$$g := \prod_{i=1}^{k} t_i,$$

$$\overline{h} := \overline{T}/\overline{g},$$

$$f := \tau(gh - T).$$

(3) *Berechne:*

$$\gcd(\overline{f},\overline{g},\overline{h}).$$

(4) *Ist $\gcd(\overline{f},\overline{g},\overline{h}) = 1$, dann gib* `TRUE` *aus und halte an.*
(5) *Setze:*

$$\overline{U} := \overline{T}/\gcd(\overline{f},\overline{g},\overline{h}).$$

(6) *Berechne:*

$$\mathcal{O}' := o_{\mathcal{F}}[\rho] + \tau U(\rho) o_{\mathcal{F}}[\rho].$$

(7) *ENDE.*

Es liegt also nahe, daß man mit dem Dedekind-Kriterium die $\mathfrak{p}$-Maximalität der Relativgleichungsordnung $o_{\mathcal{F}}[\rho]$ testet, bevor man mit Algorithmus III.14 startet, um die $\mathfrak{p}$-maximale Relativoberordnung von $o_{\mathcal{F}}[\rho]$ zu berechnen. In dem Fall der $\mathfrak{p}$-Maximalität berechnet Algorithmus III.14 zuerst die Relativoberordnung $\mathcal{O}' := [I_{\mathfrak{p}}(o_{\mathcal{F}}[\rho])/I_{\mathfrak{p}}(o_{\mathcal{F}}[\rho])]$ von $o_{\mathcal{F}}[\rho]$ und stellt danach fest, daß $\mathcal{O}' = o_{\mathcal{F}}[\rho]$ gilt, die Relativgleichungsordnung also schon $\mathfrak{p}$-maximal ist. In dem anderen Fall liefert das Dedekind-Kriterium auch die Relativoberordnung $\mathcal{O}' :=$

$[I_{\mathfrak{p}}(o_{\mathcal{F}}[\rho])/I_{\mathfrak{p}}(o_{\mathcal{F}}[\rho])]$ von $o_{\mathcal{F}}[\rho]$. Es geht also keine Information verloren. Da für das Dedekind-Kriterium im wesentlichen Arithmetik über endlichen Körpern (man arbeitet mit Polynomen aus $o_{\mathcal{F}}/\mathfrak{p}[t]$) benutzt wird, ist es in jedem Fall vorzuziehen.

Wenn man mit der relativen Gleichungsordnung $o_{\mathcal{F}}[\rho]$ startet, um die relative Maximalordnung $o_{\mathcal{E}}$ zu berechnen, kann man anstelle von Algorithmus III.14 also den folgenden modifizierten Algorithmus verwenden, um die $\mathfrak{p}$-maximale Relativoberordnung zu berechnen:

Algorithmus IV.7 (Berechnung der $\mathfrak{p}$-maximalen Relativoberordnung)
Input: *Relative Gleichungsordnung $o_{\mathcal{F}}[\rho] = o_{\mathcal{F}} + o_{\mathcal{F}}\rho + \ldots + o_{\mathcal{F}}\rho^{n-1}$ und das Primideal $\mathfrak{p}$ in $o_{\mathcal{F}}$.*
Output: *$\mathfrak{p}$-maximale Relativoberordnung $\mathcal{O}_{\mathfrak{p}}$.*

(1) *Teste mit Algorithmus IV.6 $o_{\mathcal{F}}[\rho]$ auf $\mathfrak{p}$-Maximalität.*
(2) *Ist $o_{\mathcal{F}}[\rho]$ $\mathfrak{p}$-maximal, dann gib $\mathcal{O}_{\mathfrak{p}} := o_{\mathcal{F}}[\rho]$ aus und breche ab.*
(3) *Sonst sei $\mathcal{O}_2$ die Ordnung, die Algorithmus IV.6 liefert.*
(4) *wiederhole*
(5) *Setze $\mathcal{O}_1 := \mathcal{O}_2$.*
(6) *Berechne das $\mathfrak{p}$-Radikal $I_{\mathfrak{p}}(\mathcal{O}_1)$ der Relativordnung $\mathcal{O}_1$.*
(7) *Berechne den Multiplikatorring: $\mathcal{O}_2 := [I_{\mathfrak{p}}(\mathcal{O}_1)/I_{\mathfrak{p}}(\mathcal{O}_1)]$.*
(8) *solange bis $\mathcal{O}_1 = \mathcal{O}_2$.*
(9) *Setze $\mathcal{O}_{\mathfrak{p}} := \mathcal{O}_1$.*
(10) *ENDE.*

Kapitel V
Die Berechnung des $\mathfrak{p}$-Radikals

In diesem Kapitel wird ein Verfahren angegeben, mit dem man das $\mathfrak{p}$-Radikal einer Relativordnung $\mathcal{O}$ von $\mathcal{E}$ berechnen kann. Das $\mathfrak{p}$-Radikal wurde in Definition III.4 definiert.

Auch in diesem Kapitel wird $\mathcal{O}$ stets eine Relativordnung von $\mathcal{E}$ und $\mathfrak{p}$ immer ein Primideal in der Maximalordnung $o_{\mathcal{F}}$ sein.

V.1 Die lineare Abbildung

Man definiert den folgenden Restklassenring

$$R := \mathcal{O}/\mathfrak{p}\mathcal{O}, \tag{V-1}$$

mit dem kanonischen Ringhomomorphismus

$$\varphi : \mathcal{O} \to R = \mathcal{O}/\mathfrak{p}\mathcal{O},$$

$$\varphi : x \longmapsto x + \mathfrak{p}.$$

Es sei außerdem die Abbildung ψ definiert durch:

$$\psi : R \to R, \tag{V-2}$$

$$\psi : x \longmapsto x^{q^\kappa},$$

wobei $q := \mathrm{N}_{\mathcal{F}/\mathbb{Q}}(\mathfrak{p})$, die Norm des Ideals $\mathfrak{p}$ ist, und $\kappa > 0$ eine ganze Zahl mit der Eigenschaft

$$q^{\kappa-1} < n \leq q^\kappa.$$

Es stellt sich heraus, daß ψ eine lineare Abbildung des $o_{\mathcal{F}}/\mathfrak{p}$-Vektorraumes R ist, und daß das Bild des $\mathfrak{p}$-Radikals $I_\mathfrak{p}(\mathcal{O})$ unter φ mit dem Kern von ψ übereinstimmt.

Lemma V.1 *Der in* (V-1) *definierte Restklassenring R ist ein $o_{\mathcal{F}}/\mathfrak{p}$-Vektorraum.*

Beweis: Nach Satz II.15 ist das Primideal $\mathfrak{p}$ ein maximales Ideal in dem Ring $o_{\mathcal{F}}$. Der Restklassenring $o_{\mathcal{F}}/\mathfrak{p}$ ist also ein Körper. $o_{\mathcal{F}}/\mathfrak{p}$ ist sogar ein endlicher Körper mit $q = p^\nu$ Elementen, wobei $p \geq 0$ die eindeutig bestimmte Primzahl mit $p \in \mathfrak{p}$ und $\nu \geq 1$ geeignet sind.

Da R ein Ring ist, bleibt als einzige Vektorraumeigenschaft nur noch die Wohldefiniertheit der skalaren Multiplikation

$$\cdot\ :\ o_{\mathcal{F}}/\mathfrak{p} \times R \to R \tag{V-3}$$

zu zeigen.

Dies bereitet auch kein Problem, da man den Körper $o_{\mathcal{F}}/\mathfrak{p}$ ganz einfach in den Ring R einbetten kann:

$$\sigma : o_{\mathcal{F}}/\mathfrak{p} \hookrightarrow R,$$

$$\sigma : x + \mathfrak{p} \longmapsto \varphi(x) = x + \mathfrak{p}\mathcal{O}, x \in o_{\mathcal{F}}.$$

Die Homomorphieeigenschaften von σ folgen damit direkt aus den Homomorphieeigenschaften von φ, da $o_{\mathcal{F}} \subseteq \mathcal{O}$. Es fehlt also noch die Injektivität von σ. Seien dazu $x, y \in o_{\mathcal{F}}$ mit

$$\sigma(x + \mathfrak{p}) = \sigma(y + \mathfrak{p}).$$

Damit gilt dann aber

$$x + \mathfrak{p}\mathcal{O} = \varphi(x) = \sigma(x + \mathfrak{p}) = \sigma(y + \mathfrak{p}) = \varphi(y) = y + \mathfrak{p}\mathcal{O},$$

also

$$x - y \in \mathfrak{p}\mathcal{O}.$$

Es gilt auch $x - y \in o_{\mathcal{F}}$ und daher

$$x - y \in \mathfrak{p},$$

woraus dann

$$x + \mathfrak{p} = y + \mathfrak{p}$$

folgt.

Damit erhält man eine wohldefinierte skalare Multiplikation, wie in (V-3), durch

$$\lambda \cdot x := \underbrace{\sigma(\lambda) \cdot x}_{Multiplikation\ in\ R}, \qquad \lambda \in o_{\mathcal{F}}/\mathfrak{p}, x \in R.$$

Man sieht: $R = \mathcal{O}/\mathfrak{p}\mathcal{O}$ ist ein $o_{\mathcal{F}}/\mathfrak{p}$-Vektorraum. □

Lemma V.2 *Die in* (V-2) *definierte Abbildung ψ ist $o_{\mathcal{F}}/\mathfrak{p}$-linear.*

Beweis: Die Abbildung ψ ist auf dem $o_{\mathcal{F}}/\mathfrak{p}$-Vektorraum R definiert. Es seien die Elemente $\lambda \in o_{\mathcal{F}},\ x, y \in \mathcal{O}$ beliebig gegeben. Es gilt

$$\psi\left(\underbrace{(\lambda + \mathfrak{p}) \cdot (x + \mathfrak{p}\mathcal{O})}_{skalare\ Multiplikation}\right) = \psi\left(\underbrace{(\lambda + \mathfrak{p}\mathcal{O}) \cdot (x + \mathfrak{p}\mathcal{O})}_{Multiplikation\ in\ R}\right) =$$

$$\psi\left(\underbrace{(\lambda x)}_{Multiplikation\ in\ \mathcal{O}} + \mathfrak{p}\mathcal{O}\right) = ((\lambda x) + \mathfrak{p}\mathcal{O})^{q^\kappa} = (\lambda x)^{q^\kappa} + \mathfrak{p}\mathcal{O} =$$

$$\lambda^{q^\kappa} x^{q^\kappa} + \mathfrak{p}\mathcal{O} = \underbrace{\left(\lambda^{q^\kappa} + \mathfrak{p}\mathcal{O}\right) \cdot \left(x^{q^\kappa} + \mathfrak{p}\mathcal{O}\right)}_{Multiplikation\ in\ R} =$$

$$\underbrace{\left(\lambda^{q^\kappa} + \mathfrak{p}\right) \cdot \left(x^{q^\kappa} + \mathfrak{p}\mathcal{O}\right)}_{skalare\ Multiplikation} = \underbrace{(\lambda + \mathfrak{p})^{q^\kappa} \cdot (x + \mathfrak{p}\mathcal{O})^{q^\kappa}}_{skalare\ Multiplikation} =$$

$$\underbrace{(\lambda + \mathfrak{p}) \cdot \psi\left(x + \mathfrak{p}\mathcal{O}\right)}_{skalare\ Multiplikation}.$$

Im letzten Schritt beachte man, daß $\psi|_{o_{\mathcal{F}}/\mathfrak{p}}$ die Identität auf $o_{\mathcal{F}}/\mathfrak{p}$ liefert, denn q ist gerade die Anzahl der Elemente des endlichen Körpers $o_{\mathcal{F}}/\mathfrak{p}$.

Es gilt

$$\psi\left((x + \mathfrak{p}\mathcal{O}) + (y + \mathfrak{p}\mathcal{O})\right) = \psi\left((x + y) + \mathfrak{p}\mathcal{O}\right) =$$

$$((x + y) + \mathfrak{p}\mathcal{O})^{q^\kappa} = (x + y)^{q^\kappa} + \mathfrak{p}\mathcal{O} =$$

$$\sum_{i=0}^{q^\kappa} \binom{q^\kappa}{i} x^i y^{q^\kappa - i} + \mathfrak{p}\mathcal{O}.$$

Man kann für $0 < i < q^\kappa$ zeigen

$$p \mid \binom{q^\kappa}{i}.$$

Es folgt, daß

$$\psi\left((x + \mathfrak{p}\mathcal{O}) + (y + \mathfrak{p}\mathcal{O})\right) = x^{q^\kappa} + y^{q^\kappa} + \mathfrak{p}\mathcal{O} =$$

$$\left(x^{q^\kappa} + \mathfrak{p}\mathcal{O}\right) + \left(y^{q^\kappa} + \mathfrak{p}\mathcal{O}\right) = \psi(x + \mathfrak{p}\mathcal{O}) + \psi(y + \mathfrak{p}\mathcal{O}).$$

□

Man kann jetzt den folgenden Zusammenhang zwischen dem $\mathfrak{p}$-Radikal und der $o_{\mathcal{F}}/\mathfrak{p}$-linearen Abbildung ψ herleiten:

Lemma V.3 *Für $x \in \mathcal{O}$ gilt $x \in I_\mathfrak{p}(\mathcal{O})$ genau dann, wenn $\varphi(x) \in \mathrm{Kern}(\psi)$.*

Beweis: Es sei zunächst $x \in I_{\mathfrak{p}}(\mathcal{O})$. Dann gilt nach Lemma III.6.(4)

$$x^n \in \mathfrak{p}\mathcal{O}.$$

Damit erhält man

$$\psi(\varphi(x)) = \psi(x + \mathfrak{p}\mathcal{O}) = x^{q^\kappa} + \mathfrak{p}\mathcal{O} =$$
$$x^{q^\kappa - n} x^n + \mathfrak{p}\mathcal{O} \subseteq x^{q^\kappa - n}\mathfrak{p}\mathcal{O} + \mathfrak{p}\mathcal{O} \subseteq \mathfrak{p}\mathcal{O} = 0_R.$$

Daraus folgt

$$\varphi(x) \in \mathrm{Kern}(\psi).$$

Jetzt sei $x \in \mathcal{O}$ mit $\varphi(x) = x + \mathfrak{p}\mathcal{O} \in \mathrm{Kern}(\psi)$. Es folgt

$$x^{q^\kappa} + \mathfrak{p}\mathcal{O} \in 0_R = \mathfrak{p}\mathcal{O},$$

also

$$x^{q^\kappa} \in \mathfrak{p}\mathcal{O}.$$

Damit gilt aber sofort $x \in I_{\mathfrak{p}}(\mathcal{O})$. □

Um das $\mathfrak{p}$-Radikal der Relativordnung $\mathcal{O}$ zu erhalten, reicht es aus, den Kern der linearen Abbildung ψ aus (V-2) zu bestimmen.

V.2 Eine Basis für den Vektorraum

Um die lineare Abbildung ψ aus (V-2) darzustellen, benötigt man eine $o_{\mathcal{F}}/\mathfrak{p}$-Basis des Vektorraumes R. Mit einer solchen Basis läßt sich die lineare Abbildung einfach durch die Bilder der Basiselemente darstellen. Hier soll eine solche Basis von R bestimmt werden, die noch eine weitere günstige Eigenschaft hat, die die Implementierung des Algorithmus vereinfacht.

Es müssen Elemente $\tau_1, \ldots, \tau_n \in R$ ausgewählt werden, so daß

(V-4) $$R = o_{\mathcal{F}}/\mathfrak{p} \cdot \tau_1 + \ldots + o_{\mathcal{F}}/\mathfrak{p} \cdot \tau_n$$

eine $o_{\mathcal{F}}/\mathfrak{p}$-Basis des $o_{\mathcal{F}}/\mathfrak{p}$-Vektorraumes R liefert.

Es sei eine Pseudobasis von $\mathcal{O}$ wie in Satz II.47 gegeben:

(V-5) $$\mathcal{O} = \mathfrak{a}_1\omega_1 + \ldots + \mathfrak{a}_n\omega_n,$$

mit ganzen Idealen $\mathfrak{a}_1, \ldots, \mathfrak{a}_n \subseteq o_{\mathcal{F}}$ und Elementen $\omega_1, \ldots, \omega_n \in \mathcal{E}$. (Sollte eine Pseudobasis mit gebrochenen Idealen $\mathfrak{a}_i$ gegeben sein, so multipliziert man einfach das Ideal $\mathfrak{a}_i$ mit seinem Nenner d_i und teilt dafür das Element ω_i durch den Nenner d_i und erhält so eine Pseudobasis mit der gewünschten Eigenschaft.)

Es seien $p > 0$ die eindeutig bestimmte Primzahl in dem Ideal $\mathfrak{p}$ und

(V-6) $$p o_{\mathcal{F}} = \mathfrak{p}_1^{e_1} \cdot \ldots \cdot \mathfrak{p}_s^{e_s}$$

die Primidealzerlegung von $p o_{\mathcal{F}}$, wobei die $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ paarweise verschieden sind. Es existiert ein $j \in \{1, \ldots, s\}$ mit

$$\mathfrak{p} = \mathfrak{p}_j.$$

Als erstes benötigt man Elemente $\alpha_i \in \mathfrak{a}_i$ $(1 \le i \le n)$ mit den Eigenschaften

(V-7) $$\nu_{\mathfrak{p}_j}(\alpha_i) = \nu_{\mathfrak{p}_j}(\mathfrak{a}_i) \ (1 \le j \le s).$$

Diese Elemente existieren nach Satz II.25, da nur an endlich viele Bewertungen eine Bedingung gestellt wird: die Bewertungen an den Primidealen $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ und an den Primidealen, die das Ideal $\mathfrak{a}_i$ teilen. An allen anderen Primidealen aus $o_{\mathcal{F}}$ wird nur eine nicht-negative Bewertung gefordert.

Die Elemente $\tau_1, \ldots, \tau_n$ werden jetzt wie folgt definiert:

(V-8) $$\tau_i := \varphi(\alpha_i\omega_i) \in \varphi(\mathfrak{a}_i\omega_i) \subseteq R.$$

Die Elemente $\tau_1, \ldots, \tau_n$ bilden eine $o_{\mathcal{F}}/\mathfrak{p}$-Basis von R.

Lemma V.4 $\{\tau_1, \ldots, \tau_n\}$ *ist eine* $o_{\mathcal{F}}/\mathfrak{p}$*-Basis von* R.

Beweis: Als erstes zeigt man, daß die Dimension von R höchstens n ist. Seien $x_1, \ldots, x_{n+1} \in \mathcal{O}$, beliebige Elemente. Da die Dimension des $\mathcal{F}$-Vektorraumes $\mathcal{E}$ n ist, müssen die Elemente $x_1, \ldots, x_{n+1}$ $\mathcal{F}$-linear abhängig sein, man erhält sogar $o_{\mathcal{F}}$-linear abhängig. Es existieren also $\lambda_1, \ldots, \lambda_{n+1} \in o_{\mathcal{F}}$, nicht alle in $\mathfrak{p}$, mit

$$\lambda_1 x_1 + \ldots + \lambda_{n+1} x_{n+1} = 0.$$

(Sollten alle Elemente $\lambda_1, \ldots, \lambda_{n+1}$ in $\mathfrak{p}$ liegen, so gilt $\nu_{\mathfrak{p}}(\lambda_i) > 0$ $(1 \le i \le n)$. Man multipliziert dann solange mit dem Element α aus Lemma IV.2, bis mindestens eins der λ_i nicht mehr in $\mathfrak{p}$ liegt. Man beachte, daß das Element α so gewählt ist, daß $\nu_{\mathfrak{p}}(\alpha) = -1$ und alle anderen Bewertungen nicht-negativ sind.) Daraus folgt aber

$$(\lambda_1 + \mathfrak{p})(x_1 + \mathfrak{p}\mathcal{O}) + \ldots + (\lambda_{n+1} + \mathfrak{p})(x_{n+1} + \mathfrak{p}\mathcal{O}) = 0 + \mathfrak{p}\mathcal{O},$$

und nicht alle $\lambda_i + \mathfrak{p} = 0 + \mathfrak{p}$. Es existieren also keine $n+1$ $o_{\mathcal{F}}/\mathfrak{p}$-linear unabhängigen Elemente in R.

Es genügt also zu zeigen, daß die Elemente $\tau_1, \ldots, \tau_n$ $o_{\mathcal{F}}/\mathfrak{p}$-linear unabhängig sind. Es seien $\lambda_1, \ldots, \lambda_n \in o_{\mathcal{F}}$, mit

$$(\lambda_1 + \mathfrak{p})\tau_1 + \ldots + (\lambda_n + \mathfrak{p})\tau_n = \mathfrak{p}\mathcal{O} = \mathfrak{p}\mathfrak{a}_1\omega_1 + \ldots + \mathfrak{p}\mathfrak{a}_n\omega_n.$$

Außerdem gilt

$$(\lambda_1 + \mathfrak{p})\tau_1 + \ldots + (\lambda_n + \mathfrak{p})\tau_n = (\lambda_1 + \mathfrak{p})(\alpha_1\omega_1 + \mathfrak{p}\mathcal{O}) + \ldots + (\lambda_n + \mathfrak{p})(\alpha_n\omega_n + \mathfrak{p}\mathcal{O}) =$$
$$(\lambda_1\alpha_1\omega_1 + \ldots + \lambda_n\alpha_n\omega_n) + \mathfrak{p}\mathcal{O} = (\lambda_1\alpha_1\omega_1 + \ldots + \lambda_n\alpha_n\omega_n) + (\mathfrak{p}\mathfrak{a}_1\omega_1 + \ldots + \mathfrak{p}\mathfrak{a}_n\omega_n) =$$
$$(\lambda_1\alpha_1 + \mathfrak{p}\mathfrak{a}_1)\omega_1 + \ldots + (\lambda_n\alpha_n + \mathfrak{p}\mathfrak{a}_n)\omega_n.$$

Es muß daher

$$\lambda_i\alpha_i + \mathfrak{p}\mathfrak{a}_i \subseteq \mathfrak{p}\mathfrak{a}_i \ (1 \le i \le n)$$

oder

$$\lambda_i\alpha_i \in \mathfrak{p}\mathfrak{a}_i \ (1 \le i \le n)$$

gelten. Man erhält

$$\nu_{\mathfrak{p}}(\lambda_i\alpha_i) \ge \nu_{\mathfrak{p}}(\mathfrak{p}\mathfrak{a}_i) = \nu_{\mathfrak{p}}(\mathfrak{p}) + \nu_{\mathfrak{p}}(\mathfrak{a}_i) = \nu_{\mathfrak{p}}(\mathfrak{a}_i) + 1,$$

man beachte dabei (V-7)

$$\nu_{\mathfrak{p}}(\lambda_i\alpha_i) = \nu_{\mathfrak{p}}(\lambda_i) + \nu_{\mathfrak{p}}(\alpha_i) = \nu_{\mathfrak{p}}(\lambda_i) + \nu_{\mathfrak{p}}(\mathfrak{a}_i).$$

Daraus folgt

$$\nu_{\mathfrak{p}}(\lambda_i) \ge 1,$$

oder

$$\lambda_i \in \mathfrak{p}.$$

Damit sind die Elemente $\tau_1, \ldots, \tau_n$ $o_{\mathcal{F}}/\mathfrak{p}$-linear unabhängig und bilden somit eine Basis. □

Lemma V.5 *Seien* $i \in \{1, \ldots, n\}$ *und* $x \in \mathfrak{a}_i$ *beliebig. Für die Darstellung*

$$x/\alpha_i = \frac{\mathrm{num}\,(x/\alpha_i)}{\mathrm{den}\,(x/\alpha_i)}$$

wie in Satz II.13 gilt dann

$$p \nmid \mathrm{den}\,(x/\alpha_i) \in \mathbb{Z}^{>0}.$$

Beweis: Angenommen $p \mid \mathrm{den}\,(x/\alpha_i)$. Beachtet man die Darstellung aus (V-6), dann muß ein $k \in \{1, \ldots, s\}$ existieren mit

$$\nu_{\mathfrak{p}_k}(x/\alpha_i) < 0.$$

(Es gilt nämlich $\nu_{\mathfrak{p}_l}(\mathrm{den}\,(x/\alpha_i)) \ge e_l$ $(1 \le l \le s)$, aber $\nu_{\mathfrak{p}_k}(\mathrm{num}\,(x/\alpha_i)) < e_k$ für ein k, wegen der Teilerfremdheit des Nenners und des Zählers.) Weiterhin folgt aus Lemma II.26

$$\nu_{\mathfrak{p}_k}(x/\alpha_i) = \nu_{\mathfrak{p}_k}(x) - \nu_{\mathfrak{p}_k}(\alpha_i) = \nu_{\mathfrak{p}_k}(x) - \nu_{\mathfrak{p}_k}(\mathfrak{a}_i) \ge \nu_{\mathfrak{p}_k}(\mathfrak{a}_i) - \nu_{\mathfrak{p}_k}(\mathfrak{a}_i) = 0.$$

Man erhält also einen Widerspruch zu $p \mid den\,(x/\alpha_i)$. □

Diese Eigenschaft erlaubt es, Elemente $x/\alpha_i \in \mathcal{F}$ $(1 \le i \le n)$ wie in Lemma V.5, in den Körper $o_{\mathcal{F}}/\mathfrak{p}$ abzubilden. Mit der Darstellung aus Satz II.13

$$x/\alpha_i = \frac{\mathrm{num}\,(x/\alpha_i)}{\mathrm{den}\,(x/\alpha_i)}$$

gilt

$$\mathrm{num}\,(x/\alpha_i) \in o_{\mathcal{F}}$$

und

$$\mathrm{den}\,(x/\alpha_i) \in \mathbb{Z}^{>0} \setminus p\mathbb{Z}.$$

Daraus folgt

$$\mathrm{den}\,(x/\alpha_i) + \mathfrak{p} \neq 0 + \mathfrak{p}.$$

Man kann also

$$x/\alpha_i \longmapsto \underbrace{(\mathrm{num}\,(x/\alpha_i) + \mathfrak{p}) \,/\, (\mathrm{den}\,(x/\alpha_i) + \mathfrak{p})}_{Division\ in\ o_{\mathcal{F}}/\mathfrak{p}} \in o_{\mathcal{F}}/\mathfrak{p}$$

abbilden.

Die wesentlichen Hilfsmittel sind damit geschaffen, um einen vollständigen Algorithmus zur Berechnung des $\mathfrak{p}$-Radikals der Relativordnung $\mathcal{O}$ anzugeben.

V.3 Der Algorithmus

Zunächst werden die Einzelheiten zusammengefügt, die für die Implementierung des Algorithmus zur Berechnung des $\mathfrak{p}$-Radikals der Relativordnung $\mathcal{O}$ benötigt werden.

Das $\mathfrak{p}$-Radikal $I_{\mathfrak{p}}(\mathcal{O})$ zu berechnen, heißt, eine Pseudobasis von $I_{\mathfrak{p}}(\mathcal{O})$ zu berechnen, also eine Darstellung der Form

$$I_{\mathfrak{p}}(\mathcal{O}) = \mathfrak{b}_1\vartheta_1 + \ldots + \mathfrak{b}_n\vartheta_n,$$

mit einer $\mathcal{F}$-Basis $\vartheta_1, \ldots, \vartheta_n$ von $\mathcal{E}$ und Idealen $\mathfrak{b}_1, \ldots, \mathfrak{b}_n$ in $o_{\mathcal{F}}$.

Die lineare Abbildung ψ wird durch die Bilder der Elemente $\tau_1, \ldots, \tau_n$ dargestellt. In der Ordnung $\mathcal{O}$ kann man die Elemente $(\alpha_1\omega_1)^{q^\kappa}, \ldots, (\alpha_n\omega_n)^{q^\kappa}$ ausrechnen, man erhält für $1 \leq i \leq n$ eine Darstellung

(V-9) $$(\alpha_i\omega_i)^{q^\kappa} = A_{1,i}\omega_1 + \ldots + A_{n,i}\omega_n,$$

also eine Darstellung in der Pseudobasis (V-5) von $\mathcal{O}$. Für die Elemente $A_{j,i}$ gilt dann

$$A_{j,i} \in \mathfrak{a}_j \ \ (1 \leq i, j \leq n).$$

Definiert man die Elemente $\tilde{A}_{j,i}$ durch

$$\tilde{A}_{j,i} := A_{j,i}/\alpha_j \ \ (1 \leq i, j \leq n),$$

so erhält man aus (V-9)

(V-10) $$(\alpha_i\omega_i)^{q^\kappa} = \tilde{A}_{1,i}(\alpha_1\omega_1) + \ldots + \tilde{A}_{n,i}(\alpha_n\omega_n).$$

Zusammenfassend gilt dann

$$\psi(\tau_i) = (\alpha_i\omega_i + \mathfrak{p}\mathcal{O})^{q^\kappa} = (\alpha_i\omega_i)^{q^\kappa} + \mathfrak{p}\mathcal{O} =$$
$$\left(\tilde{A}_{1,i}(\alpha_1\omega_1) + \ldots + \tilde{A}_{n,i}(\alpha_n\omega_n)\right) + \mathfrak{p}\mathcal{O} =$$
$$(\tilde{A}_{1,i} + \mathfrak{p})(\alpha_1\omega_1 + \mathfrak{p}\mathcal{O}) + \ldots + (\tilde{A}_{n,i} + \mathfrak{p})(\alpha_n\omega_n + \mathfrak{p}\mathcal{O}) \ \ (1 \leq i \leq n).$$

Für

$$\hat{A}_{j,i} := \tilde{A}_{j,i} + \mathfrak{p} \in o_{\mathcal{F}}/\mathfrak{p} \ \ (1 \leq i, j \leq n)$$

folgt

$$\psi(\tau_i) = \hat{A}_{1,i}\tau_1 + \ldots + \hat{A}_{n,i}\tau_n \ \ (1 \leq i \leq n),$$

eine Darstellung der linearen Abbildung ψ auf den Basiselementen $\tau_1, \ldots, \tau_n$.

Die Matrix $\hat{A} := \left(\hat{A}_{j,i}\right)_{1 \leq j,i \leq n}$ beschreibt die Abbildung ψ. Mit einem Algorithmus, der den $\mathrm{Kern}(\psi)$ mit Hilfe der Matrix $\hat{A}$ über dem endlichen Körper $o_{\mathcal{F}}/\mathfrak{p}$ berechnet, bekommt man eine Basis des Kerns in der Form

(V-11) $$\eta_i = \hat{B}_{1,i}\tau_1 + \ldots + \hat{B}_{n,i}\tau_n,$$

mit $\hat{B}_{j,i} \in o_{\mathcal{F}}/\mathfrak{p}$ $(1 \leq j \leq n,\ 1 \leq i \leq r \leq n)$, wobei $r := \dim(\mathrm{Kern}(\psi))$.

Man erhält das folgende Ergebnis:

Lemma V.6 *Für $x \in \mathcal{O}$ gilt:*
$x \in I_{\mathfrak{p}}(\mathcal{O})$ genau dann, wenn $\varphi(x) \in o_{\mathcal{F}}/\mathfrak{p} \cdot \eta_1 + \ldots + o_{\mathcal{F}}/\mathfrak{p} \cdot \eta_r$.

Beweis: Dies folgt sofort aus Lemma V.3 und den Ergebnissen von oben. □

Für das Element η_i $(1 \leq i \leq r)$ gilt

$$\eta_i = (B_{1,i} + \mathfrak{p})(\alpha_1\omega_1 + \mathfrak{p}\mathcal{O}) + \ldots + (B_{n,i} + \mathfrak{p})(\alpha_n\omega_n + \mathfrak{p}\mathcal{O}) =$$
$$(B_{1,i}\alpha_1\omega_1 + \ldots + B_{n,i}\alpha_n\omega_n) + \mathfrak{p}\mathcal{O},$$

wobei das Element $B_{j,i} \in o_{\mathcal{F}}$ $(1 \leq j \leq n)$ ein beliebiger Repräsentant der Klasse $\hat{B}_{j,i}$ sei.

Es gilt demnach $x \in I_{\mathfrak{p}}(\mathcal{O})$ genau dann, wenn

$$x + \mathfrak{p}\mathcal{O} \in (o_{\mathcal{F}} \cdot (B_{1,1}\alpha_1\omega_1 + \ldots + B_{n,1}\alpha_n\omega_n) + \ldots + o_{\mathcal{F}} \cdot (B_{1,r}\alpha_1\omega_1 + \ldots + B_{n,r}\alpha_n\omega_n)) + \mathfrak{p}\mathcal{O},$$

und dies ist genau dann erfüllt, wenn

$$x \in (o_{\mathcal{F}} \cdot (B_{1,1}\alpha_1\omega_1 + \ldots + B_{n,1}\alpha_n\omega_n) + \ldots + o_{\mathcal{F}} \cdot (B_{1,r}\alpha_1\omega_1 + \ldots + B_{n,r}\alpha_n\omega_n)) + \mathfrak{p}\mathcal{O}.$$

Mit $B := (B_{j,i}\alpha_j)_{1 \leq j \leq n, 1 \leq i \leq r}$ erhält man eine $n \times r$-Matrix über $o_{\mathcal{F}}$.

Es folgt dann: Ein Element $x \in \mathcal{O}$, mit der Darstellung

(V-12) $$x = \xi_1\omega_1 + \ldots + \xi_n\omega_n$$

in der Pseudobasis (V-5) von $\mathcal{O}$, liegt genau dann in $I_{\mathfrak{p}}(\mathcal{O})$, wenn der Vektor

$$\overline{x} := \begin{pmatrix} \xi_1 \\ \vdots \\ \xi_n \end{pmatrix}$$

in dem durch

(V-13) $$\mathcal{M} := \left(\begin{array}{ccc|cccccc} o_{\mathcal{F}} & \cdots & o_{\mathcal{F}} & \mathfrak{p} & \cdots & \cdots & \cdots & \mathfrak{p} \\ & & & 1 & 0 & \cdots & \cdots & 0 \\ & & & 0 & \ddots & \ddots & & \vdots \\ & B & & \vdots & \ddots & \ddots & \ddots & \vdots \\ & & & \vdots & & \ddots & \ddots & 0 \\ & & & 0 & \cdots & \cdots & 0 & 1 \end{array}\right)$$

definierten Modul über dem Dedekindring $o_{\mathcal{F}}$ liegt.

Mit einem Verfahren wie in Theorem II.41 erhält man dann mit

$$\begin{pmatrix} \mathfrak{b}_1 & \cdots & \mathfrak{b}_n \\ & \hat{M} & \end{pmatrix} := \mathrm{HNF}(\mathcal{M}) = \mathcal{M},$$

$$(\vartheta_1, \ldots, \vartheta_n) := (\omega_1, \ldots, \omega_n) \cdot \hat{M}$$

und

$$I_{\mathfrak{p}}(\mathcal{O}) := \mathfrak{b}_1\vartheta_1 + \ldots + \mathfrak{b}_n\vartheta_n$$

eine Pseudobasis wie in Satz II.52 für das Ideal $I_{\mathfrak{p}}(\mathcal{O})$.

Bemerkung V.7 *Um Elemente $\alpha_i \in \mathfrak{a}_i$ $(1 \leq i \leq n)$, wie in* (V-7) *zu erhalten, kann man nach* (Lemma II.27) *wie folgt vorgehen: Man erzeugt solange zufällige Elemente aus dem Ideal $\mathfrak{a}_i$, bis man eines gefunden hat mit der Eigenschaft*

$$\alpha_i \notin \mathfrak{p}_j\mathfrak{a}_i, 1 \leq j \leq s,$$

wobei die $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ die Primideale aus (V-6) *sind.*

Abschließend wird der vollständige Algorithmus angegeben:

Algorithmus V.8 (Berechnung des $\mathfrak{p}$-Radikals)

Input: *Relativordnung* $\mathcal{O} = \mathfrak{a}_1\omega_1 + \ldots + \mathfrak{a}_n\omega_n$ *und ein Primideal* $\mathfrak{p} \subseteq o_{\mathcal{F}}$.

Output: *Das* $\mathfrak{p}$*-Radikal von* $\mathcal{O}$: $I_{\mathfrak{p}}(\mathcal{O}) = \mathfrak{b}_1\vartheta_1 + \ldots + \mathfrak{b}_n\vartheta_n$.

(1) *Berechne die Elemente* $\alpha_i \in \mathfrak{a}_i$ $(1 \le i \le n)$ *mit der Eigenschaft* (V-7) *(eventuell unter Verwendung von Bemerkung V.7).*

(2) *Berechne die Elemente* $A_{j,i} \in \mathfrak{a}_j$ $(1 \le i, j \le n)$, *also*

$$(\alpha_i\omega_i)^{q^\kappa} = A_{1,i}\omega_1 + \ldots + A_{n,i}\omega_n.$$

(3) *Konstruiere die Matrix:*

$$\hat{A} := (A_{j,i}/\alpha_j + \mathfrak{p})_{1 \le j,i \le n}.$$

(4) *Wende ein Verfahren zur Berechnung des Kerns an:*

$$\hat{B} := \mathrm{Kern}\left(\hat{A}\right).$$

(5) *Wähle jeweils Repräsentanten* $B_{j,i}$ *aus* $\hat{B}_{j,i}$ $(1 \le j \le n, 1 \le i \le r \le n)$.

(6) *Konstruiere den* $o_{\mathcal{F}}$*-Modul* $\mathcal{M}$ *wie in* (V-13).

(7) *Berechne eine relative Normalform mit einem Verfahren wie in Theorem II.41:*

$$\begin{pmatrix} \mathfrak{b}_1 & \cdots & \mathfrak{b}_n \\ & \hat{M} & \end{pmatrix} := \mathrm{HNF}(\mathcal{M}).$$

(8) *Berechne die neuen Elemente:*

$$(\vartheta_1, \ldots, \vartheta_n) := (\omega_1, \ldots, \omega_n) \cdot \hat{M}.$$

(9) *Setze:*

$$I_{\mathfrak{p}}(\mathcal{O}) = \mathfrak{b}_1\vartheta_1 + \ldots + \mathfrak{b}_n\vartheta_n.$$

(10) *ENDE.*

Kapitel VI
Die Berechnung des $\mathfrak{p}$-Radikals für große Primideale

Im vorangegangenen Kapitel wurde ein Verfahren angegeben, mit dem man das $\mathfrak{p}$-Radikal einer Relativordnung $\mathcal{O}$ von $\mathcal{E}$ berechnen kann. Dabei durfte $\mathfrak{p}$ ein beliebiges Primideal in der Maximalordnung $o_{\mathcal{F}}$ sein. Die Potenzierung der Basiselemente bereitet aber bei größeren Beispielen Probleme, da man mindestens die $\mathrm{N}_{\mathcal{F}/\mathbb{Q}}(\mathfrak{p})$-ten Potenzen bilden muß und bei großen Beispielen häufig Primideale mit großen Normen auftreten.

In diesem Kapitel wird ein anderes Verfahren besprochen, das für fast alle Primideale in $o_{\mathcal{F}}$ anwendbar ist. In diesen Fällen stellt es eine Verbesserung des anderen Verfahrens dar, da die (hohen) Potenzen der Basiselemente nicht berechnet werden müssen. In den Fällen, in denen das hier beschriebene Verfahren nicht anwendbar ist, stellt das Potenzieren der Basiselemente kein Problem dar.

Die Einschränkung bezieht sich auf die Primzahl, die in dem Primideal $\mathfrak{p}$ liegt. Sie muß größer als der Grad der Relativerweiterung sein. Es sei $\mathfrak{p}$ deshalb ein Primideal in $o_{\mathcal{F}}$ mit

$$p > n,$$

wobei p die eindeutig bestimmte Primzahl in $\mathfrak{p}$ und n der Grad der Relativerweiterung $\mathcal{E}/\mathcal{F}$ sind. $\mathcal{O}$ sei wieder eine Relativordnung in $\mathcal{E}$.

VI.1 Symmetrische Polynome und die Newton-Relationen

Um die Eigenschaft des $\mathfrak{p}$-Radikals, die für die Berechnung verwendet wird, zu beweisen, braucht man die *Newton-Relationen.* Die Beweise zu den folgenden Aussagen und einige weitere wissenswerte Eigenschaften kann man in [PZ89] nachlesen.

Als erstes benötigt man eine Aussage über *symmetrische Polynome.* Das sind Polynome (in mehreren Variablen), die sich unter beliebiger Permutation der Variablen nicht ändern.

Theorem VI.1 *Es sei* R *ein kommutativer Ring mit Eins. Dann läßt sich jedes Polynom in* n *Variablen* $\xi_1, \ldots, \xi_n$ *über* R*, das sich unter beliebiger Permutation der Variablen nicht verändert, als Polynom in den* elementar-symmetrischen Funktionen

$$\sigma_i := \sigma_i(\xi_1, \ldots, \xi_n) := \sum_{1 \le j_1 < \ldots < j_i \le n} \xi_{j_1} \cdot \xi_{j_2} \cdot \ldots \cdot \xi_{j_i} \ (1 \le i \le n)$$

über R *darstellen.*

Betrachtet man zum Beispiel ein Polynom $P \in R[\xi_1, \ldots, \xi_n][t]$,

$$P = \prod_{i=1}^{n} (t - \xi_i), \tag{VI-1}$$

so gilt mit den elementar-symmetrischen Funktionen

$$P = t^n - \sigma_1 t^{n-1} + \sigma_2 t^{n-2} + \ldots + (-1)^n \sigma_n. \tag{VI-2}$$

Weiterhin benötigt man den Begriff der k-ten Potenz-Summe:

Definition VI.2 *Seien* R *ein kommutativer Ring mit Eins und* $\xi_1, \ldots, \xi_n$ *Variablen über* R*. Dann heißt*

$$S_k := \sum_{i=1}^{n} \xi_i^k \ (k \ge 0)$$

die k-te Potenz-Summe *von* $\xi_1, \ldots, \xi_n$.

Die k-te Potenz-Summe ist auch ein Polynom in den Variablen $\xi_1, \ldots, \xi_n$ über R.

Theorem VI.3 (Newton-Relationen) *Zwischen den elementar-symmetrischen Funktionen und den k-ten Potenz-Summen besteht der folgende Zusammenhang:*

$$\sigma_0 := 1,\ \sum_{i=0}^{k-1} (-1)^i \sigma_i S_{k-i} + (-1)^k k\sigma_k = 0\ (0 \leq k \leq n),$$

$$\sigma_0 := 1,\ \sum_{i=0}^{n} (-1)^i \sigma_i S_{k-i} = 0\ (k \geq n).$$

VI.2 Der Zusammenhang

Mit den Newton-Relationen kann man den folgenden Satz zeigen, der die Berechnung des $\mathfrak{p}$-Radikals vereinfacht, falls die Primzahl, die in $\mathfrak{p}$ liegt, größer ist als der Grad der Relativerweiterung.

Satz VI.4 *Es seien $I_\mathfrak{p}(\mathcal{O})$ das $\mathfrak{p}$-Radikal der Relativordnung $\mathcal{O}$ und die folgende Menge gegeben:*

$$\Lambda := \{x \in \mathcal{O} \mid \mathrm{Tr}_{\mathcal{E}/\mathcal{F}}(xy) \in \mathfrak{p}\ \forall y \in \mathcal{O}\}.$$

Es gilt:

$$I_\mathfrak{p}(\mathcal{O}) = \Lambda.$$

Beweis: In Lemma III.6.(2) hat man gesehen, daß $I_\mathfrak{p}(\mathcal{O})$ der Durchschnitt über alle Primideale von $\mathcal{O}$ ist, die über $\mathfrak{p}$ liegen. Es sei $\mathfrak{P}$ ein solches Primideal. Γ sei der Galois-Abschluß der Körpererweiterung $\mathcal{E}/\mathcal{F}$ mit der Maximalordnung $\mathcal{O}_\Gamma$ und $\sigma_1, \ldots, \sigma_n \in \mathrm{Gal}(\mathcal{E}/\mathcal{F})$, so daß $\sigma_1|_\mathcal{E}, \ldots, \sigma_n|_\mathcal{E}$ paarweise verschieden sind. $\tilde{\mathfrak{P}} \in \mathcal{O}_\Gamma$ sei ein Primideal, das $\mathfrak{P}$ teilt.

Es sei jetzt $x \in I_\mathfrak{p}(\mathcal{O})$ ein beliebiges Element. Dann gilt für jedes Element $y \in \mathcal{O}$

$$xy \in I_\mathfrak{p}(\mathcal{O}) \subseteq \mathfrak{P} \subseteq \tilde{\mathfrak{P}}.$$

Und daher folgt:

$$\mathrm{Tr}_{\mathcal{E}/\mathcal{F}}(xy) = \sum_{i=1}^{n} \sigma_i(xy) \in \sum_{i=1}^{n} \sigma_i(\tilde{\mathfrak{P}}).$$

Außerdem gilt $\mathrm{Tr}_{\mathcal{E}/\mathcal{F}}(xy) \in o_\mathcal{F}$. Damit folgt

$$\mathrm{Tr}_{\mathcal{E}/\mathcal{F}}(xy) \in \sum_{i=1}^{n} \tilde{\mathfrak{P}} \cap o_\mathcal{F} = \mathfrak{p}.$$

Damit ist $I_\mathfrak{p}(\mathcal{O}) \subseteq \Lambda$ gezeigt.

Es sei jetzt $x \in \Lambda$. Für jedes $\nu > 0$ erhält man

$$\mathrm{Tr}_{\mathcal{E}/\mathcal{F}}(x^\nu) \in \mathfrak{p},$$

da $x^{\nu-1} \in \mathcal{O}$. $m_x \in o_\mathcal{F}[t]$ sei das charakteristische Polynom von x. Nach Satz II.31 gilt

$$m_x(t) = \prod_{i=1}^{n} (t - x^{(i)}).$$

Setzt man $\xi_i := x^{(i)}$ $(1 \leq i \leq n)$ und beachtet man VI-1 und VI-2, so sieht man, daß

$$m_x(t) = t^n + \sum_{i=1}^{n} (-1)^i \sigma_i(x^{(1)}, \ldots, x^{(n)}) t^{n-i}.$$

Für $k \geq 0$ erhält man aus der Isomorphieeigenschaft der i-ten Konjugiertenabbildung $.^{(i)}$ die folgende Bedeutung für die k-ten Potenz-Summen:

$$S_k = \sum_{i=1}^{n} \left(x^{(i)}\right)^k = \sum_{i=1}^{n} \left(x^k\right)^{(i)} = \mathrm{Tr}_{\mathcal{E}/\mathcal{F}}(x^k) \in \mathfrak{p}.$$

Nach Theorem VI.3 gilt

$$\sigma_0 := 1,\ \sum_{i=0}^{k-1} (-1)^i \sigma_i S_{k-i} + (-1)^k k\sigma_k = 0\ (0 \leq k \leq n),$$

oder nach einer kleinen Umformung

$$(-1)^k k\sigma_k = -\sum_{i=0}^{k-1} \underbrace{(-1)^i \sigma_i}_{\in o_\mathcal{F}} \underbrace{S_{k-i}}_{\in \mathfrak{p}} \in \mathfrak{p}\ (0 < k \leq n).$$

Damit gilt aber auch $k\sigma_k \in \mathfrak{p}$ $(0 < k \leq n)$. Für die Primzahl p, die in $\mathfrak{p}$ liegt, gilt aber $p > n \geq k$ und damit folgt $k \notin \mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$ $(0 < k \leq n)$. Es gilt

$$\sigma_k \in \mathfrak{p}\ (0 < k \leq n).$$

(Dies ist die einzige Stelle, an der man die Einschränkung für das Primideal $\mathfrak{p}$ benötigt.)

Man erhält also

$$0 = m_x(x) = x^n + \sum_{i=1}^{n} (-1)^i \sigma_i x^{n-i},$$

oder

$$x^n = -\sum_{i=1}^{n} \underbrace{(-1)^i \sigma_i}_{\in \mathfrak{p}} \underbrace{x^{n-i}}_{\in \mathcal{O}} \in \mathfrak{p}\mathcal{O}.$$

Damit gilt aber

$$x \in I_\mathfrak{p}(\mathcal{O}),$$

und es ist auch

$$\Lambda \subseteq I_\mathfrak{p}(\mathcal{O})$$

gezeigt. □

Jetzt stellt sich die Frage, wie man die Menge Λ berechnen kann. Da Λ ein Ideal in der Relativordnung $\mathcal{O}$ ist, sucht man wieder nach einer Pseudobasis

$$\Lambda = \mathfrak{b}_1\vartheta_1 + \ldots + \mathfrak{b}_n\vartheta_n.$$

Es sei

$$\mathcal{O} = \mathfrak{a}_1\omega_1 + \ldots + \mathfrak{a}_n\omega_n$$

eine Pseudobasis von $\mathcal{O}$.

Ähnlich wie im vorangegangenen Kapitel wird sich herausstellen, daß das $\mathfrak{p}$-Radikal mit dem Kern einer linearen Abbildung übereinstimmt. Es seien also wie in V der Restklassenring

$$R := \mathcal{O}/\mathfrak{p}\mathcal{O}$$

mit dem kanonischen Ringhomomorphismus

$$\varphi : \mathcal{O} \to R = \mathcal{O}/\mathfrak{p}\mathcal{O},$$

$$\varphi : x \longmapsto x + \mathfrak{p}.$$

Im vorangegangenen Kapitel hat man gesehen, daß R ein $o_\mathcal{F}/\mathfrak{p}$-Vektorraum ist. Und durch die Elemente

$$\tau_i := \varphi(\alpha_i\omega_i)\ (1 \leq i \leq n)$$

mit Elementen $\alpha_i \in \mathfrak{a}_i$ $(1 \leq i \leq n)$ wie in (V-7) erhält man eine $o_\mathcal{F}/\mathfrak{p}$-Basis von R. Bevor die lineare Abbildung, deren Kern berechnet werden soll, angegeben werden kann, muß man noch einen weiteren $o_\mathcal{F}/\mathfrak{p}$-Vektorraum definieren:

$$\mathcal{L}(R, o_\mathcal{F}/\mathfrak{p}) := \{\psi : R \to o_\mathcal{F}/\mathfrak{p} \mid \psi\ \mathit{linear}\}$$

sei der $o_\mathcal{F}/\mathfrak{p}$-Vektorraum aller $o_\mathcal{F}/\mathfrak{p}$-linearen Abbildungen von R in $o_\mathcal{F}/\mathfrak{p}$. Jetzt kann man die entscheidende Abbildung angeben:

$$\text{(VI-3)} \qquad \psi : R \to \mathcal{L}(R, o_\mathcal{F}/\mathfrak{p})$$

$$\psi : x + \mathfrak{p}\mathcal{O} \longmapsto \left(y + \mathfrak{p}\mathcal{O} \mapsto \mathrm{Tr}_{\mathcal{E}/\mathcal{F}}(xy) + \mathfrak{p}\right).$$

Wie oben schon angedeutet, gilt die folgende Aussage:

Lemma VI.5 *Die in (VI-3) definierte Abbildung ψ ist $o_{\mathcal{F}}/\mathfrak{p}$-linear.*

Beweis: Zuerst muß man die Wohldefiniertheit der Abbildung ψ zeigen: Es sei dazu ein Element $x \in \mathcal{O}$ fest vorgegeben. Für ein Element aus der Relativordnung $\mathcal{O}$ liegt die Spur auf jeden Fall in der absoluten Maximalordnung $o_{\mathcal{F}}$. $\psi(x)$ definiert damit eine Abbildung von R in $o_{\mathcal{F}}/\mathfrak{p}$. Die Linearität dieser Abbildung folgt sofort aus der Linearität der Spur, man vergleiche dazu Satz II.29. Es seien jetzt Elemente $x_1, x_2, y_1, y_2 \in \mathcal{O}$ gegeben mit

$$x_1 + \mathfrak{p}\mathcal{O} = x_2 + \mathfrak{p}\mathcal{O},$$
$$y_1 + \mathfrak{p}\mathcal{O} = y_2 + \mathfrak{p}\mathcal{O}.$$

Man muß zeigen, daß

$$\psi(x_1 + \mathfrak{p}\mathcal{O})(y_1 + \mathfrak{p}\mathcal{O}) = \psi(x_2 + \mathfrak{p}\mathcal{O})(y_2 + \mathfrak{p}\mathcal{O})$$

gilt. Für x_1, x_2, y_1, y_2 existieren Darstellungen $\nu = 1, 2$

$$x_\nu = x_{\nu,1}\omega_1 + \ldots + x_{\nu,n}\omega_n,$$
$$y_\nu = y_{\nu,1}\omega_1 + \ldots + y_{\nu,n}\omega_n.$$

Es folgt

$$x_{1,i} + \mathfrak{p} = x_{2,i} + \mathfrak{p} \ (1 \leq i \leq n),$$
$$y_{1,i} + \mathfrak{p} = y_{2,i} + \mathfrak{p} \ (1 \leq i \leq n).$$

Es gilt

$$\psi(x_1 + \mathfrak{p}\mathcal{O})(y_1 + \mathfrak{p}\mathcal{O}) = \mathrm{Tr}_{\mathcal{E}/\mathcal{F}}(x_1 y_1) + \mathfrak{p} =$$
$$\sum_{i=1}^{n}\sum_{j=1}^{n} x_{1,i}y_{1,j}\mathrm{Tr}_{\mathcal{E}/\mathcal{F}}(\omega_i\omega_j) + \mathfrak{p} = \sum_{i=1}^{n}\sum_{j=1}^{n}(x_{1,i}+\mathfrak{p})(y_{1,j}+\mathfrak{p})\mathrm{Tr}_{\mathcal{E}/\mathcal{F}}(\omega_i\omega_j) =$$
$$\sum_{i=1}^{n}\sum_{j=1}^{n}(x_{2,i}+\mathfrak{p})(y_{2,j}+\mathfrak{p})\mathrm{Tr}_{\mathcal{E}/\mathcal{F}}(\omega_i\omega_j) = \sum_{i=1}^{n}\sum_{j=1}^{n} x_{2,i}y_{2,j}\mathrm{Tr}_{\mathcal{E}/\mathcal{F}}(\omega_i\omega_j) + \mathfrak{p} =$$
$$\mathrm{Tr}_{\mathcal{E}/\mathcal{F}}(x_2 y_2) + \mathfrak{p} = \psi(x_2 + \mathfrak{p}\mathcal{O})(y_2 + \mathfrak{p}\mathcal{O}).$$

Es bleibt also nur noch die Linearität der Abbildung ψ zu zeigen: Es seien die Elemente $\lambda \in o_{\mathcal{F}},\ x_1, x_2, y \in \mathcal{O}$ beliebig gegeben. Es gelten

$$\psi\left((\lambda + \mathfrak{p})(x_1 + \mathfrak{p}\mathcal{O})\right)(y + \mathfrak{p}\mathcal{O}) = \psi\left(\lambda x_1 + \mathfrak{p}\mathcal{O}\right)(y + \mathfrak{p}\mathcal{O}) = \mathrm{Tr}_{\mathcal{E}/\mathcal{F}}\left(\lambda x_1 y\right) + \mathfrak{p} =$$
$$\lambda \mathrm{Tr}_{\mathcal{E}/\mathcal{F}}(x_1 y) + \mathfrak{p} = (\lambda + \mathfrak{p})\left(\mathrm{Tr}_{\mathcal{E}/\mathcal{F}}(x_1 y) + \mathfrak{p}\right) = (\lambda + \mathfrak{p}) \cdot \psi\left(x_1 + \mathfrak{p}\mathcal{O}\right)(y + \mathfrak{p}\mathcal{O}),$$
$$\psi\left((x_1 + \mathfrak{p}\mathcal{O}) + (x_2 + \mathfrak{p}\mathcal{O})\right)(y + \mathfrak{p}\mathcal{O}) = \psi\left((x_1 + x_2) + \mathfrak{p}\mathcal{O}\right)(y + \mathfrak{p}\mathcal{O}) =$$
$$\mathrm{Tr}_{\mathcal{E}/\mathcal{F}}\left(x_1 y + x_2 y\right) + \mathfrak{p} = \left(\mathrm{Tr}_{\mathcal{E}/\mathcal{F}}\left(x_1 y\right) + \mathfrak{p}\right) + \left(\mathrm{Tr}_{\mathcal{E}/\mathcal{F}}\left(x_2 y\right) + \mathfrak{p}\right) =$$
$$\psi\left(x_1 + \mathfrak{p}\mathcal{O}\right)(y + \mathfrak{p}\mathcal{O}) + \psi\left(x_2 + \mathfrak{p}\mathcal{O}\right)(y + \mathfrak{p}\mathcal{O}).$$

□

Jetzt kann man den Zusammenhang zwischen der linearen Abbildung ψ und dem Ideal Λ zeigen:

Lemma VI.6 *Für $x \in \mathcal{O}$ gilt $x \in \Lambda$ genau dann, wenn $\varphi(x) \in \mathrm{Kern}(\psi)$.*

Beweis: Es sei zuerst $x \in \Lambda$ beliebig gegeben. Dann gilt für ein beliebiges Element $y \in \mathcal{O}$

$$\mathrm{Tr}_{\mathcal{E}/\mathcal{F}}(xy) \in \mathfrak{p}.$$

Damit folgt aber sofort

$$\psi(x + \mathfrak{p}\mathcal{O})(y + \mathfrak{p}\mathcal{O}) = \mathrm{Tr}_{\mathcal{E}/\mathcal{F}}(xy) + \mathfrak{p} \subseteq \mathfrak{p},$$

also $\psi(x + \mathfrak{p}\mathcal{O}) : (y + \mathfrak{p}\mathcal{O}) \longmapsto 0_{o_{\mathcal{F}}/\mathfrak{p}}$. Damit gilt $\varphi(x) \in \mathrm{Kern}(\psi)$.

Es sei jetzt $x \in \mathcal{O}$ mit $\varphi(x) \in \mathrm{Kern}(\psi)$. Damit folgt aber für beliebiges $y \in \mathcal{O}$

$$\psi(x + \mathfrak{p}\mathcal{O})(y + \mathfrak{p}\mathcal{O}) = \mathfrak{p},$$

also

$$\mathrm{Tr}_{\mathcal{E}/\mathcal{F}}(xy) \in \mathfrak{p}.$$

Damit erhält man auch

$$x \in \Lambda.$$

□

Um das $\mathfrak{p}$-Radikal der Relativordnung $\mathcal{O}$ zu erhalten, reicht es aus, den Kern der linearen Abbildung ψ aus (VI-3) zu bestimmen.

VI.3 Der erste Algorithmus

Lineare Abbildungen von R in $\mathcal{L}(R, o_{\mathcal{F}}/\mathfrak{p})$ lassen sich durch eine $(n \times n)$-Matrix mit Elementen aus $o_{\mathcal{F}}/\mathfrak{p}$ darstellen. $\lambda_i \in \mathcal{L}(R, o_{\mathcal{F}}/\mathfrak{p})$ $(1 \leq i \leq n)$ sei die Abbildung, die das Element τ_i auf das Element $1_{o_{\mathcal{F}}/\mathfrak{p}}$ und alle anderen Elemente τ_j $(j \neq i)$ auf das Element $0_{o_{\mathcal{F}}/\mathfrak{p}}$ abbildet. Die Elemente $\lambda_1, \ldots, \lambda_n$ bilden ein $o_{\mathcal{F}}/\mathfrak{p}$-Basis von $\mathcal{L}(R, o_{\mathcal{F}}/\mathfrak{p})$. Man benötigt eine Matrix $\hat{A} \in (o_{\mathcal{F}}/\mathfrak{p})^{n \times n}$, so daß

$$\psi(\tau_i) = \hat{A}_{1,i}\lambda_1 + \ldots + \hat{A}_{n,i}\lambda_n \ (1 \leq i \leq n)$$

gilt.

Die Matrix A sei die folgende Matrix:

$$A := \left(\mathrm{Tr}_{\mathcal{E}/\mathcal{F}}(\alpha_i\omega_i\alpha_j\omega_j)\right)_{1 \leq i,j \leq n}.$$

Man erhält die Matrix $\hat{A}$ durch:

$$\hat{A} := \left(A_{i,j} + \mathfrak{p}\right)_{1 \leq i,j \leq n}.$$

Es gilt dann

$$\psi(\tau_i)(\tau_j) = \mathrm{Tr}_{\mathcal{E}/\mathcal{F}}(\alpha_i\omega_i\alpha_j\omega_j) + \mathfrak{p} = \hat{A}_{i,j} \ \ (1 \leq i,j \leq n).$$

Und für $\overline{y} = y_1\tau_1 + \ldots + y_n\tau_n \in R$ erhält man

$$\psi(\tau_i)(\overline{y}) = y_1\hat{A}_{i,1} + \ldots + y_n\hat{A}_{i,n} \ (1 \leq i \leq n).$$

Die Matrix $\hat{A}$ beschreibt folglich die lineare Abbildung ψ.

Dann bestimmt man den $\mathrm{Kern}(\psi)$ mit Hilfe dieser Matrix wie in Abschnitt V.3. Man erhält eine Basis des Kerns in der Form

$$\eta_i = \hat{B}_{1,i}\tau_1 + \ldots + \hat{B}_{n,i}\tau_n, \tag{VI-4}$$

mit $\hat{B}_{j,i} \in o_{\mathcal{F}}/\mathfrak{p}$ $(1 \leq j \leq n,\ 1 \leq i \leq r \leq n)$, wobei $r := \dim(\mathrm{Kern}(\psi))$.

Man erhält das folgende Ergebnis:

Lemma VI.7 *Für ein $x \in \mathcal{O}$ gilt:*
$x \in \Lambda$ genau dann, wenn $\varphi(x) \in o_{\mathcal{F}}/\mathfrak{p} \cdot \eta_1 + \ldots + o_{\mathcal{F}}/\mathfrak{p} \cdot \eta_r$.

Beweis: Dies folgt sofort aus Lemma VI.6 und den Ergebnissen von oben. □

Für das Element η_i $(1 \leq i \leq r)$ gilt

$$\eta_i = (B_{1,i} + \mathfrak{p})(\alpha_1\omega_1 + \mathfrak{p}\mathcal{O}) + \ldots + (B_{n,i} + \mathfrak{p})(\alpha_n\omega_n + \mathfrak{p}\mathcal{O}) =$$
$$(B_{1,i}\alpha_1\omega_1 + \ldots + B_{n,i}\alpha_n\omega_n) + \mathfrak{p}\mathcal{O},$$

wobei das Element $B_{j,i} \in o_{\mathcal{F}}$ $(1 \leq j \leq n)$ ein beliebiger Repräsentant der Klasse $\hat{B}_{j,i}$ sei.

Es gilt demnach $x \in \Lambda$ genau dann, wenn

$$x + \mathfrak{p}\mathcal{O} \in (o_{\mathcal{F}} \cdot (B_{1,1}\alpha_1\omega_1 + \ldots + B_{n,1}\alpha_n\omega_n) + \ldots + o_{\mathcal{F}} \cdot (B_{1,r}\alpha_1\omega_1 + \ldots + B_{n,r}\alpha_n\omega_n)) + \mathfrak{p}\mathcal{O},$$

und dies ist genau dann erfüllt, wenn

$$x \in (o_{\mathcal{F}} \cdot (B_{1,1}\alpha_1\omega_1 + \ldots + B_{n,1}\alpha_n\omega_n) + \ldots + o_{\mathcal{F}} \cdot (B_{1,r}\alpha_1\omega_1 + \ldots + B_{n,r}\alpha_n\omega_n)) + \mathfrak{p}\mathcal{O}.$$

Mit $B := (B_{j,i}\alpha_j)_{1 \leq j \leq n, 1 \leq i \leq r}$ erhält man eine $n \times r$-Matrix über $o_{\mathcal{F}}$.

Es folgt dann: Ein Element $x \in \mathcal{O}$, mit der Darstellung

$$x = \xi_1\omega_1 + \ldots + \xi_n\omega_n \tag{VI-5}$$

in der Pseudobasis von $\mathcal{O}$, liegt genau dann in Λ, wenn der Vektor

$$\overline{x} := \begin{pmatrix} \xi_1 \\ \vdots \\ \xi_n \end{pmatrix}$$

in dem durch

$$\text{(VI-6)}\qquad \mathcal{M} := \begin{pmatrix} o_{\mathcal{F}} & \cdots & o_{\mathcal{F}} & \mathfrak{p} & \cdots & \cdots & \cdots & \mathfrak{p} \\ & & & 1 & 0 & \cdots & \cdots & 0 \\ & & & 0 & \ddots & \ddots & & \vdots \\ & B & & \vdots & \ddots & \ddots & \ddots & \vdots \\ & & & \vdots & & \ddots & \ddots & 0 \\ & & & 0 & \cdots & \cdots & 0 & 1 \end{pmatrix}$$

definierten Modul über dem Dedekindring $o_{\mathcal{F}}$ liegt.

Mit einem Verfahren wie in Theorem II.41 erhält man dann mit

$$\begin{pmatrix} \mathfrak{b}_1 & \cdots & \mathfrak{b}_n \\ & \hat{M} & \end{pmatrix} := \mathrm{HNF}(\mathcal{M}) = \mathcal{M},$$

$$(\vartheta_1, \ldots, \vartheta_n) := (\omega_1, \ldots, \omega_n) \cdot \hat{M}$$

und

$$\Lambda = \mathfrak{b}_1\vartheta_1 + \ldots + \mathfrak{b}_n\vartheta_n$$

eine Pseudobasis wie in Satz II.52 für das Ideal Λ.

Man kann also jetzt den folgenden Algorithmus angeben:

Algorithmus VI.8 (Berechnung des $\mathfrak{p}$-Radikals für große $\mathfrak{p}$)

Input: *Relativordnung $\mathcal{O} = \mathfrak{a}_1\omega_1 + \ldots + \mathfrak{a}_n\omega_n$ und ein Primideal $\mathfrak{p} \subseteq o_{\mathcal{F}}$.*

Output: *Das $\mathfrak{p}$-Radikal von $\mathcal{O}$: $I_{\mathfrak{p}}(\mathcal{O}) = \mathfrak{b}_1\vartheta_1 + \ldots + \mathfrak{b}_n\vartheta_n$.*

(1) *Berechne die Elemente $\alpha_i \in \mathfrak{a}_i$ $(1 \leq i \leq n)$ mit der Eigenschaft* (V-7) *(eventuell unter Verwendung von Bemerkung V.7).*

(2) *Berechne die Elemente $A_{i,j} \in o_{\mathcal{F}}$ $(1 \leq i, j \leq n)$, also*

$$A_{i,j} = A_{j,i} := \mathrm{Tr}_{\mathcal{E}/\mathcal{F}}(\alpha_i\omega_i\alpha_j\omega_j).$$

(3) *Konstruiere die Matrix:*

$$\hat{A} := (A_{j,i} + \mathfrak{p})_{1 \leq j,i \leq n}.$$

(4) *Wende Verfahren zur Berechnung des Kerns an:*

$$\hat{B} := \mathrm{Kern}\left(\hat{A}\right).$$

(5) *Wähle jeweils Repräsentanten $B_{j,i}$ aus $\hat{B}_{j,i}$ $(1 \leq j \leq n, 1 \leq i \leq r \leq n)$.*

(6) *Konstruiere den $o_{\mathcal{F}}$-Modul $\mathcal{M}$ wie in* (VI-6).

(7) *Berechne eine relative Normalform mit einem Verfahren wie in Theorem II.41:*

$$\begin{pmatrix} \mathfrak{b}_1 & \cdots & \mathfrak{b}_n \\ & \hat{M} & \end{pmatrix} := \mathrm{HNF}(\mathcal{M}).$$

(8) *Berechne die neuen Elemente:*

$$(\vartheta_1, \ldots, \vartheta_n) := (\omega_1, \ldots, \omega_n) \cdot \hat{M}.$$

(9) *Setze:*

$$I_{\mathfrak{p}}(\mathcal{O}) = \mathfrak{b}_1\vartheta_1 + \ldots + \mathfrak{b}_n\vartheta_n.$$

(10) *ENDE.*

VI.4 Der zweite Algorithmus

Es existiert noch eine weitere Möglichkeit, die Menge Λ zu berechnen. In der Praxis hat sich allerdings herausgestellt, das die vorangegangene Variante schneller zu berechnen ist, so daß dieser Abschnitt nur aus Gründen der Vollständigkeit angefügt wird.

Es sei eine Pseudobasis von $\mathcal{O}$ gegeben:

$$\mathcal{O} = \mathfrak{a}_1\omega_1 + \ldots + \mathfrak{a}_n\omega_n.$$

Ein Element $x \in \mathcal{E}$ kann man in der $\mathcal{F}$-Basis $\omega_1, \ldots, \omega_n$ wie folgt darstellen:

$$x = x_1\omega_1 + \ldots + x_n\omega_n,$$

wobei die Elemente $x_i \in \mathcal{F}$. Jetzt gilt $x \in \Lambda$ genau dann, wenn $x \in \mathcal{O}$ und für ein beliebiges Element $y \in \mathcal{O}$ immer $\mathrm{Tr}_{\mathcal{E}/\mathcal{F}}(xy) \in \mathfrak{p}$ gilt.

Die Elemente $y \in \mathcal{O}$ kann man auch in der Pseudobasis darstellen:

$$y = y_1\omega_1 + \ldots + y_n\omega_n,$$

mit den Elementen $y_i \in \mathfrak{a}_i$. Dann gilt:

$$\mathrm{Tr}_{\mathcal{E}/\mathcal{F}}(xy) = \mathrm{Tr}_{\mathcal{E}/\mathcal{F}}\left(\left(\sum_{i=1}^n x_i\omega_i\right) \cdot \left(\sum_{j=1}^n y_j\omega_j\right)\right) =$$

$$\mathrm{Tr}_{\mathcal{E}/\mathcal{F}}\left(\sum_{i=1}^n\sum_{j=1}^n (x_i\omega_i y_j\omega_j)\right) = \sum_{i=1}^n\sum_{j=1}^n (x_i y_j \mathrm{Tr}_{\mathcal{E}/\mathcal{F}}(\omega_i\omega_j)).$$

Damit erhält man $x \in \Lambda$ genau dann, wenn für jedes Element $y_j \in \mathfrak{a}_j$ $(1 \leq j \leq n)$ gilt

$$\sum_{i=1}^n\sum_{j=1}^n (x_i y_j \mathrm{Tr}_{\mathcal{E}/\mathcal{F}}(\omega_i\omega_j)) \in \mathfrak{p}$$

und $x_k \in \mathfrak{a}_k$ $(1 \leq k \leq n)$. Die Idealeigenschaft der $\mathfrak{a}_1, \ldots, \mathfrak{a}_n, \mathfrak{p}$ zeigt die Äquivalenz zu: Für beliebige Elemente $y_j \in \mathfrak{a}_j$ $(1 \leq j \leq n)$ gilt

$$(1 \leq i, j \leq n)\ x_i y_j \mathrm{Tr}_{\mathcal{E}/\mathcal{F}}(\omega_i\omega_j) \in \mathfrak{p}$$

und $x_k \in \mathfrak{a}_k$ $(1 \leq k \leq n)$. Hieraus erhält man leicht die äquivalente Bedingung

$$(1 \leq i, j \leq n)\ (\mathfrak{a}_j/\mathfrak{p})\, x_i \mathrm{Tr}_{\mathcal{E}/\mathcal{F}}(\omega_i\omega_j) \in o_{\mathcal{F}},$$

$$(1 \leq k \leq n)\ (1/\mathfrak{a}_k)\, x_k \in o_{\mathcal{F}}.$$

Wiederum zeigt die Idealeigenschaft von $(\mathfrak{a}_1/\mathfrak{p}), \ldots, (\mathfrak{a}_n/\mathfrak{p}), (1/\mathfrak{a}_1), \ldots, (1/\mathfrak{a}_n)$ und die Ringeigenschaft von $o_{\mathcal{F}}$, daß dies genau dann erfüllt ist, wenn für beliebige Wahl von $\gamma_j \in (\mathfrak{a}_j/\mathfrak{p})$ $(1 \leq j \leq n)$ und $\alpha_k \in (1/\mathfrak{a}_k)$ $(1 \leq k \leq n)$ gilt

$$\sum_{i=1}^n x_i \left(\sum_{j=1}^n (\gamma_j \mathrm{Tr}_{\mathcal{E}/\mathcal{F}}(\omega_i\omega_j)) + \alpha_i\right) \in o_{\mathcal{F}}.$$

Dies gilt dann und nur dann, wenn für beliebige Wahl von $\gamma_j \in (\mathfrak{a}_j/\mathfrak{p})$ $(1 \leq j \leq n)$ und $\alpha_k \in (1/\mathfrak{a}_k)$ $(1 \leq k \leq n)$

$$\sum_{i=1}^n x_i \left(\sum_{j=1}^n (\gamma_j (\mathrm{Tr}_{\mathcal{E}/\mathcal{F}}(\omega_i\omega_j)_{1 \leq i,j \leq n})_{\cdot,j}) + \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix}\right)_i \in o_{\mathcal{F}}.$$

Setzt man nun den Vektor

$$\overline{x} := \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix},$$

so erhält man die Äquivalenz zu: Für beliebige Wahl von $\gamma_j \in (\mathfrak{a}_j/\mathfrak{p})$ $(1 \leq j \leq n)$ und $\alpha_k \in (1/\mathfrak{a}_k)$ $(1 \leq k \leq n)$ gilt

$$\overline{x}^{tr} \cdot \left(\sum_{j=1}^n (\gamma_j (\mathrm{Tr}_{\mathcal{E}/\mathcal{F}}(\omega_i\omega_j)_{1 \leq i,j \leq n})_{\cdot,j}) + \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix}\right) \in o_{\mathcal{F}}.$$

Dies gilt exakt dann, wenn für jeden Vektor des Moduls

$$\overline{y} \in \begin{pmatrix} (\mathfrak{a}_1/\mathfrak{p}) & \cdots & (\mathfrak{a}_n/\mathfrak{p}) & (1/\mathfrak{a}_1) & \cdots & (1/\mathfrak{a}_n) \\ & & & 1 & \cdots & 0 \\ & (\mathrm{Tr}_{\mathcal{E}/\mathcal{F}}(\omega_i\omega_j)_{i,j}) & & \vdots & \ddots & \vdots \\ & & & 0 & \cdots & 1 \end{pmatrix},$$

gilt

$$\overline{x}^{tr} \cdot \overline{y} \in o_{\mathcal{F}}.$$

Es sei

$$\begin{pmatrix} \mathfrak{e}_1 & \cdots & \mathfrak{e}_n \\ & M & \end{pmatrix} = \begin{pmatrix} (\mathfrak{a}_1/\mathfrak{p}) & \cdots & (\mathfrak{a}_n/\mathfrak{p}) & (1/\mathfrak{a}_1) & \cdots & (1/\mathfrak{a}_n) \\ & & & 1 & \cdots & 0 \\ & (\mathrm{Tr}_{\mathcal{E}/\mathcal{F}}(\omega_i\omega_j)_{i,j}) & & \vdots & \ddots & \vdots \\ & & & 0 & \cdots & 1 \end{pmatrix}$$

eine Normalform, wie in (Theorem II.41), von dem Modul oben.

Dann folgt: $x \in \Lambda$ genau dann, wenn für jeden Vektor

$$\overline{y} \in \begin{pmatrix} \mathfrak{e}_1 & \cdots & \mathfrak{e}_n \\ & M & \end{pmatrix}$$

gilt

$$\overline{x}^{tr} \cdot \overline{y} \in o_{\mathcal{F}}.$$

Dies ist äquivalent zu: Für jede beliebige Wahl von $(1 \leq i \leq n)$ $\epsilon_i \in \mathfrak{e}_i$, gilt

$$\overline{x}^{tr} \cdot \left(\sum_{i=1}^{n} \epsilon_i M_{\cdot,i} \right) \in o_{\mathcal{F}}.$$

Dies gilt genau dann, wenn für jede beliebige Wahl von $(1 \leq i \leq n)$ $\epsilon_i \in \mathfrak{e}_i$,

$$\left(\sum_{i=1}^{n} \epsilon_i M^{tr}_{i,\cdot} \right) \cdot \overline{x} \in o_{\mathcal{F}}$$

erfüllt ist. Die Idealeigenschaft der $\mathfrak{e}_i$ und die Ringeigenschaft von $o_{\mathcal{F}}$ zeigen, daß dies exakt dann erfüllt ist, wenn auch für jede beliebige Wahl von $(1 \leq i \leq n)$ $\epsilon_i \in \mathfrak{e}_i$,

$$\epsilon_i \cdot M^{tr}_{i,\cdot} \cdot \overline{x} \in o_{\mathcal{F}}.$$

Dies ist dann und nur dann erfüllt, wenn

$$(1 \leq i \leq n)\ \mathfrak{e}_i \cdot M^{tr}_{i,\cdot} \cdot \overline{x} \subset o_{\mathcal{F}}.$$

Wobei die Äquivalenz zu

$$(1 \leq i \leq n)\ M^{tr}_{i,\cdot} \cdot \overline{x} \subset (1/\mathfrak{e}_i)$$

auffällt. Die obere Aussage gilt aber genau, wenn für $(1 \leq i \leq n)$ $\tilde{\epsilon}_i \in (1/\mathfrak{e}_i)$ existieren, mit

$$M^{tr} \cdot \overline{x} = \begin{pmatrix} \tilde{\epsilon}_1 \\ \vdots \\ \tilde{\epsilon}_n \end{pmatrix},$$

oder

$$\overline{x} = \left(M^{tr}\right)^{-1} \cdot \begin{pmatrix} \tilde{\epsilon}_1 \\ \vdots \\ \tilde{\epsilon}_n \end{pmatrix}.$$

Dies ist äquivalent zu der Existenz von $(1 \leq i \leq n)$ $\tilde{\epsilon}_i \in (1/\mathfrak{e}_i)$, mit der Eigenschaft

$$\overline{x} = \sum_{i=1}^{n} \tilde{\epsilon}_i \left(M^{tr}\right)^{-1}_{\cdot,i}.$$

Damit folgt, daß $x \in \Lambda$ genau dann gilt, wenn der Vektor $\overline{x}$ in dem Modul

$$\begin{pmatrix} (1/\mathfrak{e}_1) & \cdots & (1/\mathfrak{e}_n) \\ & \left(M^{tr}\right)^{-1} & \end{pmatrix}$$

enthalten ist.

Definiert man also

$$(\vartheta_1, \ldots, \vartheta_n) := (\omega_1, \ldots, \omega_n) \cdot \left(M^{tr}\right)^{-1},$$

so gilt

$$\Lambda = (1/\mathfrak{e}_1)\,\vartheta_1 + \ldots + (1/\mathfrak{e}_n)\,\vartheta_n.$$

Man kann also jetzt den folgenden Algorithmus angeben:

Algorithmus VI.9 (Berechnung des $\mathfrak{p}$-Radikals für große $\mathfrak{p}$)

Input: *Relativordnung* $\mathcal{O} = \mathfrak{a}_1\omega_1 + \ldots + \mathfrak{a}_n\omega_n$ *und ein Primideal* $\mathfrak{p} \subset o_{\mathcal{F}}$.

Output: *Das* $\mathfrak{p}$*-Radikal von* $\mathcal{O}$: $I_{\mathfrak{p}}(\mathcal{O}) = \mathfrak{b}_1\vartheta_1 + \ldots + \mathfrak{b}_n\vartheta_n$.

(1) *Konstruiere den Modul:*

$$Mod := \begin{pmatrix} (\mathfrak{a}_1/\mathfrak{p}) & \cdots & (\mathfrak{a}_n/\mathfrak{p}) & (1/\mathfrak{a}_1) & \cdots & (1/\mathfrak{a}_n) \\ & & & 1 & \cdots & 0 \\ & (\mathrm{Tr}_{\mathcal{E}/\mathcal{F}}(\omega_i\omega_j)_{i,j}) & & \vdots & \ddots & \vdots \\ & & & 0 & \cdots & 1 \end{pmatrix}.$$

(2) *Berechne die relative HNF:*

$$\begin{pmatrix} \mathfrak{e}_1 & \cdots & \mathfrak{e}_n \\ & M & \end{pmatrix} = HNF(Mod).$$

(3) *Erzeuge die neuen Koeffizientenideale:*

$$1 \leq i \leq n,\ \mathfrak{b}_i := (1/\mathfrak{e}_i).$$

(4) *Erzeuge die neuen Elemente:*

$$(\vartheta_1, \ldots, \vartheta_n) := (\omega_1, \ldots, \omega_n) \cdot \left(M^{tr}\right)^{-1}.$$

(5) *ENDE.*

Kapitel VII
Die Berechnung des Multiplikatorringes

Es wird ein Verfahren beschrieben, mit dem man den Multiplikatorring eines beliebigen Ideals $\mathfrak{a}$ in einer Relativordnung $\mathcal{O}$ von $\mathcal{E}$ berechnen kann. Der Multiplikatorring $[\mathfrak{a}/\mathfrak{a}]$ wurde in Definition III.7 wie folgt definiert:

$$[\mathfrak{a}/\mathfrak{a}] := \{x \in \mathcal{E} \mid x\mathfrak{a} \subseteq \mathfrak{a}\}.$$

Das Ideal $\mathfrak{a}$ muß nicht notwendig ein ganzes Ideal in $o_{\mathcal{F}}$ sein. Man kann den Multiplikatorring auch von gebrochenen Idealen berechnen.

Der Algorithmus besteht im wesentlichen aus der Berechnung einer Normalform eines großen Moduls.

Es sei eine Pseudobasis der Relativordnung $\mathcal{O}$ gegeben durch

(VII-1) $$\mathcal{O} = \mathfrak{a}_1\omega_1 + \ldots + \mathfrak{a}_n\omega_n,$$

und eine Pseudobasis des Ideals $\mathfrak{a}$

(VII-2) $$\mathfrak{a} = \mathfrak{c}_1\tau_1 + \ldots + \mathfrak{c}_n\tau_n.$$

Gesucht ist eine Pseudobasis

(VII-3) $$[\mathfrak{a}/\mathfrak{a}] = \mathfrak{d}_1\eta_1 + \ldots + \mathfrak{d}_n\eta_n$$

des Multiplikatorringes von $\mathfrak{a}$. Nach Lemma III.8.(3) weiß man, daß der Multiplikatorring eine Relativordnung in $\mathcal{E}$ ist. Damit ist die Existenz einer solchen Pseudobasis von $[\mathfrak{a}/\mathfrak{a}]$ gesichert.

VII.1 Der Algorithmus

Sowohl die Elemente $\omega_1, \ldots, \omega_n$ als auch die Elemente $\tau_1, \ldots, \tau_n$ bilden $\mathcal{F}$-Basen von $\mathcal{E}$. Es existiert daher eine invertierbare Matrix $S \in \mathcal{F}^{n \times n}$ mit der Eigenschaft

(VII-4) $$(\omega_1, \ldots, \omega_n) \cdot S = (\tau_1, \ldots, \tau_n)$$

oder auch

(VII-5) $$(\omega_1, \ldots, \omega_n) = (\tau_1, \ldots, \tau_n) \cdot S^{-1}.$$

Weiterhin existiert für jedes Element τ_i $(1 \le i \le n)$ eine sogenannte *Repräsentationsmatrix*. Das ist eine Matrix $M_{\tau_i} \in \mathcal{F}^{n \times n}$, für die gilt

(VII-6) $$\tau_i \cdot (\omega_1, \ldots, \omega_n) = (\omega_1, \ldots, \omega_n) \cdot M_{\tau_i}.$$

Diese Matrizen M_{τ_i} kann man wie folgt berechnen. Es gilt nach (VII-4)

$$\tau_i \cdot (\omega_1, \ldots, \omega_n) = (\omega_1, \ldots, \omega_n) \cdot S_{\cdot,i} \cdot (\omega_1, \ldots, \omega_n).$$

Man sieht, daß

$$M_{\tau_i} = S_{\cdot,i} \cdot (\omega_1, \ldots, \omega_n)$$

gilt.

Aus (VII-6) folgt

(VII-7) $$\tau_i \cdot \omega_j = (\omega_1, \ldots, \omega_n) \cdot (M_{\tau_i})_{\cdot,j} \ (1 \le i, j \le n).$$

Es sei $x \in \mathcal{E}$ beliebig. Das Element x hat eine Darstellung in der $\mathcal{F}$-Basis $\{\omega_1, \ldots, \omega_n\}$:

$$x = x_1\omega_1 + \ldots + x_n\omega_n$$

mit Elementen $x_i \in \mathcal{F}$ $(1 \le i \le n)$. Für $1 \le i \le n$ kann man, unter Berücksichtigung von (VII-5) und (VII-7), das Produkt $x\tau_i$ wie folgt schreiben:

$$x\tau_i = \sum_{j=1}^{n} x_j\omega_j\tau_i = \sum_{j=1}^{n} x_j\tau_i\omega_j =$$

$$\sum_{j=1}^{n} x_j \cdot (\omega_1, \ldots, \omega_n) \cdot (M_{\tau_i})_{\cdot,j} = \sum_{j=1}^{n} x_j \cdot (\tau_1, \ldots, \tau_n) \cdot S^{-1} \cdot (M_{\tau_i})_{\cdot,j}.$$

Definiert man den Vektor

$$\overline{x} := \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix},$$

so erhält man

$$x\tau_i = (\tau_1, \ldots, \tau_n) \cdot S^{-1} \cdot M_{\tau_i} \cdot \overline{x} = \sum_{\nu=1}^{n} \tau_\nu \cdot \left(S^{-1} \cdot M_{\tau_i}\right)_{\nu,\cdot} \cdot \overline{x}.$$

Hieraus ergibt sich nun die folgende Kette von Äquivalenzen: $x \in [\mathfrak{a}/\mathfrak{a}]$ genau dann, wenn $x \cdot \mathfrak{a} \subseteq \mathfrak{a}$. Dies gilt genau dann, wenn

$$x \cdot \mathfrak{a} = \sum_{i=1}^{n} x\mathfrak{c}_i\tau_i = \sum_{i=1}^{n} (x\tau_i)\mathfrak{c}_i \overset{!}{\subseteq} \sum_{j=1}^{n} \mathfrak{c}_j\tau_j.$$

Dies ist exakt dann erfüllt, wenn auch

$$\sum_{i=1}^{n}\sum_{\nu=1}^{n} \left(\tau_\nu \cdot \left(S^{-1} \cdot M_{\tau_i}\right)_{\nu,\cdot} \cdot \overline{x}\right) \cdot \mathfrak{c}_i \subseteq \sum_{j=1}^{n} \mathfrak{c}_j\tau_j$$

gilt. Eine kleine Umformung zeigt die Äquivalenz zu

$$\sum_{\nu=1}^{n} \tau_\nu \sum_{i=1}^{n} \left(\left(S^{-1} \cdot M_{\tau_i}\right)_{\nu,\cdot} \cdot \overline{x} \cdot \mathfrak{c}_i\right) \subseteq \sum_{j=1}^{n} \mathfrak{c}_j\tau_j.$$

Die Basiseigenschaft der Elemente $\tau_1, \ldots, \tau_n$ zeigt, daß dies genau dann erfüllt ist, wenn gilt

$$(1 \le \nu \le n) \ \sum_{i=1}^{n} \left(S^{-1} \cdot M_{\tau_i}\right)_{\nu,\cdot} \cdot \overline{x} \cdot \mathfrak{c}_i \subseteq \mathfrak{c}_\nu.$$

Die Idealeigenschaft der $\mathfrak{c}_\nu$ erlaubt es, die Summe zu entfernen, man erhält die Äquivalenz zu

$$(1 \le \nu, i \le n) \ \mathfrak{c}_i \cdot \left(S^{-1} \cdot M_{\tau_i}\right)_{\nu,\cdot} \cdot \overline{x} \subseteq \mathfrak{c}_\nu.$$

Dies gilt genau dann, wenn

$$(1 \le \nu, i \le n) \ (\mathfrak{c}_i/\mathfrak{c}_\nu) \cdot \left(S^{-1} \cdot M_{\tau_i}\right)_{\nu,\cdot} \cdot \overline{x} \subseteq o_{\mathcal{F}}.$$

Man wendet hier noch einmal die Idealeigenschaft an, diesmal auf die Ideale $(\mathfrak{c}_i/\mathfrak{c}_\nu)$, und sieht, daß dies exakt dann erfüllt ist, wenn man für jede beliebige Wahl von $(1 \le \nu, i \le n)$ $\gamma_{\nu,i} \in (\mathfrak{c}_i/\mathfrak{c}_\nu)$,

$$\left(\sum_{\nu=1}^{n}\sum_{i=1}^{n} \gamma_{\nu,i} \left(S^{-1} \cdot M_{\tau_i}\right)_{\nu,\cdot}\right) \cdot \overline{x} \in o_{\mathcal{F}}$$

erhält. Die nächste Äquivalenz folgt wieder aus einer kleinen Umformung: Für jede beliebige Wahl von $(1 \le \nu, i \le n)$ $\gamma_{\nu,i} \in (\mathfrak{c}_i/\mathfrak{c}_\nu)$, gilt

$$\overline{x}^{tr} \cdot \left(\sum_{\nu=1}^{n}\sum_{i=1}^{n} \gamma_{\nu,i} \left(S^{-1} \cdot M_{\tau_i}\right)^{tr}_{\cdot,\nu}\right) \in o_{\mathcal{F}}.$$

Für den weiteren Verlauf wird die Matrix $M \in \mathcal{F}^{n^2 \times n}$ definiert:

$$M := \begin{pmatrix} S^{-1} \cdot M_{\tau_1} \\ \hline S^{-1} \cdot M_{\tau_2} \\ \hline \vdots \\ \hline S^{-1} \cdot M_{\tau_n} \end{pmatrix}.$$

Faßt man die letzten Schritte zusammen, so erhält man $x \in [\mathfrak{a}/\mathfrak{a}]$ genau dann, wenn für jede beliebige Wahl von $(1 \le \nu, i \le n)$ $\gamma_{\nu,i} \in (\mathfrak{c}_i/\mathfrak{c}_\nu)$ gilt

$$\overline{x}^{tr} \cdot \left(\sum_{\nu=1}^{n} \sum_{i=1}^{n} \gamma_{\nu,i} \cdot M^{tr}_{\cdot,((i-1)n+\nu)} \right) \in o_{\mathcal{F}}.$$

Dies ist aber auch äquivalent zu: Für jeden Vektor des Moduls

$$y \in \mathcal{M} := \left(\begin{array}{ccccccc} (\mathfrak{c}_1/\mathfrak{c}_1) & (\mathfrak{c}_1/\mathfrak{c}_2) & \cdots & (\mathfrak{c}_1/\mathfrak{c}_n) & (\mathfrak{c}_2/\mathfrak{c}_1) & \cdots & (\mathfrak{c}_n/\mathfrak{c}_n) \\ & & & M^{tr} & & & \end{array} \right),$$

gilt

$$\overline{x}^{tr} \cdot y \in o_{\mathcal{F}}.$$

Es sei

$$\left(\begin{array}{ccc} \mathfrak{e}_1 & \cdots & \mathfrak{e}_n \\ & \hat{M} & \end{array} \right) := \mathrm{HNF}(\mathcal{M}) = \mathcal{M},$$

eine Normalform, wie in Theorem II.41, von dem Modul $\mathcal{M}$. Man erhält also $x \in [\mathfrak{a}/\mathfrak{a}]$ genau dann, wenn für jeden Vektor des Moduls

$$y \in \left(\begin{array}{ccc} \mathfrak{e}_1 & \cdots & \mathfrak{e}_n \\ & \hat{M} & \end{array} \right)$$

gilt

$$\overline{x}^{tr} \cdot y \in o_{\mathcal{F}}.$$

Dies ist äquivalent zu: Für jede beliebige Wahl von $(1 \le i \le n)$ $\epsilon_i \in \mathfrak{e}_i$ gilt

$$\overline{x}^{tr} \cdot \left(\sum_{i=1}^{n} \epsilon_i \hat{M}_{\cdot,i} \right) \in o_{\mathcal{F}}.$$

Dies gilt genau dann, wenn für jede beliebige Wahl von $(1 \le i \le n)$ $\epsilon_i \in \mathfrak{e}_i$

$$\left(\sum_{i=1}^{n} \epsilon_i \hat{M}^{tr}_{i,\cdot} \right) \cdot \overline{x} \in o_{\mathcal{F}}$$

erfüllt ist. Die Idealeigenschaft der $\mathfrak{e}_i$ und die Ringeigenschaft von $o_{\mathcal{F}}$ zeigen, daß dies exakt dann erfüllt ist, wenn auch für jede beliebige Wahl von $(1 \le i \le n)$ $\epsilon_i \in \mathfrak{e}_i$

$$\epsilon_i \cdot \hat{M}^{tr}_{i,\cdot} \cdot \overline{x} \in o_{\mathcal{F}}.$$

Dies ist dann und nur dann erfüllt, wenn

$$(1 \le i \le n)\ \mathfrak{e}_i \cdot \hat{M}^{tr}_{i,\cdot} \cdot \overline{x} \subseteq o_{\mathcal{F}}.$$

Wobei die Äquivalenz zu

$$(1 \le i \le n)\ \hat{M}^{tr}_{i,\cdot} \cdot \overline{x} \subseteq (1/\mathfrak{e}_i)$$

auffällt. Die obere Aussage gilt aber genau, wenn für $(1 \le i \le n)$ $\tilde{\epsilon}_i \in (1/\mathfrak{e}_i)$ existieren, mit

$$\hat{M}^{tr} \cdot \overline{x} = \begin{pmatrix} \tilde{\epsilon}_1 \\ \vdots \\ \tilde{\epsilon}_n \end{pmatrix},$$

oder

$$\overline{x} = \left(\hat{M}^{tr} \right)^{-1} \cdot \begin{pmatrix} \tilde{\epsilon}_1 \\ \vdots \\ \tilde{\epsilon}_n \end{pmatrix}.$$

Dies ist äquivalent zu der Existenz von $(1 \le i \le n)$ $\tilde{\epsilon}_i \in (1/\mathfrak{e}_i)$ mit der Eigenschaft

$$\overline{x} = \sum_{i=1}^{n} \tilde{\epsilon}_i \left(\hat{M}^{tr} \right)^{-1}_{\cdot,i}.$$

Damit folgt, daß $x \in [\mathfrak{a}/\mathfrak{a}]$ genau dann gilt, wenn der Vektor $\overline{x}$ in dem Modul

$$\left(\begin{array}{ccc} (1/\mathfrak{e}_1) & \cdots & (1/\mathfrak{e}_n) \\ & \left(\hat{M}^{tr}\right)^{-1} & \end{array} \right)$$

enthalten ist.

Definiert man also

$$(\eta_1, \ldots, \eta_n) := (\omega_1, \ldots, \omega_n) \cdot \left(\hat{M}^{tr} \right)^{-1},$$

so gilt

$$[\mathfrak{a}/\mathfrak{a}] = (1/\mathfrak{e}_1)\, \eta_1 + \ldots + (1/\mathfrak{e}_n)\, \eta_n.$$

Man kann also jetzt den folgenden Algorithmus angeben:

Algorithmus VII.1 (Berechnung des Multiplikatorringes)

Input: *Relativordnung* $\mathcal{O} = \mathfrak{a}_1\omega_1 + \ldots + \mathfrak{a}_n\omega_n$ *und ein Ideal* $\mathfrak{a} = \mathfrak{c}_1\tau_1 + \ldots + \mathfrak{c}_n\tau_n$ *in* $\mathcal{O}$.

Output: *Multiplikatorring* $[\mathfrak{a}/\mathfrak{a}] = \mathfrak{d}_1\eta_1 + \ldots + \mathfrak{d}_n\eta_n$.

(1) *Berechne die große Matrix M:*

$$M := \left(\begin{array}{c} S^{-1} \cdot M_{\tau_1} \\ \hline S^{-1} \cdot M_{\tau_2} \\ \hline \vdots \\ \hline S^{-1} \cdot M_{\tau_n} \end{array} \right).$$

(2) *Konstruiere den Modul:*

$$\mathcal{M} := \left(\begin{array}{ccccccc} (\mathfrak{c}_1/\mathfrak{c}_1) & (\mathfrak{c}_1/\mathfrak{c}_2) & \cdots & (\mathfrak{c}_1/\mathfrak{c}_n) & (\mathfrak{c}_2/\mathfrak{c}_1) & \cdots & (\mathfrak{c}_n/\mathfrak{c}_n) \\ & & & M^{tr} & & & \end{array} \right).$$

(3) *Berechne eine relative Normalform mit einem Verfahren wie in Theorem II.41:*

$$\left(\begin{array}{ccc} \mathfrak{e}_1 & \cdots & \mathfrak{e}_n \\ & \hat{M} & \end{array} \right) := \mathrm{HNF}(\mathcal{M}).$$

(4) *Erzeuge die neuen Koeffizientenideale:*

$$1 \le i \le n,\ \mathfrak{d}_i := (1/\mathfrak{e}_i).$$

(5) *Erzeuge die neuen Elemente:*

$$(\eta_1, \ldots, \eta_n) := (\omega_1, \ldots, \omega_n) \cdot \left(\hat{M}^{tr} \right)^{-1}.$$

(6) *Setze:*

$$[\mathfrak{a}/\mathfrak{a}] := \mathfrak{d}_1\eta_1 + \ldots + \mathfrak{d}_n\eta_n.$$

(7) *ENDE.*

Eine ähnliche Methode kann auch zur Invertierung und zur Division von Idealen in Relativordnungen verwendet werden, die durch ihre Pseudobasis gegeben sind. Die Algorithmen hierfür werden im Anhang beschrieben.

Kapitel VIII

Beispiele

Hier werden einige Beispiele aufgeführt, die mit dem Computeralgebrasystem KANT-V4 in der Oberfläche KASH gerechnet wurden. Alle Rechnungen wurden auf einem HP9000/735s mit 160 MB Speicher unter dem Betriebssystem HP-UX 9.04 durchgeführt.

VIII.1 Berechnung von Klassenkörpern

Bei diesen Beispielen handelt es sich um Klassenkörper von Grad 3 Körpern. Die Grundkörper $\mathcal{F}$ wurden der KASH-Datenbank entnommen [DW96]. Die Körper werden jeweils durch die erzeugenden Polynome angegeben:

$$\mathcal{F} = \mathbb{Q}(\theta) \;\; \text{mit } T_{\mathcal{F}/\mathbb{Q}}(\theta) = 0,$$
$$\mathcal{E} = \mathcal{F}(\rho) \;\; \text{mit } T_{\mathcal{E}/\mathcal{F}}(\rho) = 0,$$
$$\tilde{\mathcal{E}} = \mathbb{Q}(\zeta) \;\; \text{mit } T_{\tilde{\mathcal{E}}/\mathbb{Q}}(\zeta) = 0,$$

wobei

$$\tilde{\mathcal{E}} \simeq \mathcal{E}.$$

Die Zeit time$(\mathcal{E}/\mathcal{F})$ ist die Zeit, die benötigt wurde, um die relative Maximalordnung von $\mathcal{E}/\mathcal{F}$ zu berechnen und time$(\tilde{\mathcal{E}}/\mathbb{Q})$ ist die Zeit, die für die Berechnung der absoluten Maximalordnung von $\tilde{\mathcal{E}}/\mathbb{Q}$ benötigt wurde. In der Testphase des Algorithmus wurden sehr viel mehr Beispiele gerechnet. Die hier angegebenen Beispiele sind jeweils der Anfang der Liste und nicht besonders ausgewählt.

Die erste Serie enthält Grundkörper mit Klassengruppe C3.

$T_{\mathcal{F}/\mathbb{Q}}$	$T_{\mathcal{E}/\mathcal{F}}$	time$(\mathcal{E}/\mathcal{F})$
$T_{\tilde{\mathcal{E}}/\mathbb{Q}}$		time$(\tilde{\mathcal{E}}/\mathbb{Q})$
t^3+t^2+5t-1	$t^3-3\theta t+\left(1-4\theta-2\theta^2\right)$	750 msec
$t^9+3t^7+25t^6+45t^5+78t^4+144t^3-45t^2-81t+27$		370 msec
$t^3-3t+10$	t^3-3t+1	1.19 sec
$t^9-18t^7+33t^6+81t^5-99t^4-15t^3+1089t+1331$		3.38 sec
t^3+t^2+9t+1	$t^3-3t+\left(-2-\theta-2\theta^2\right)$	1.1 sec
$t^9-9t^7+29t^6+27t^5-174t^4+158t^3+261t^2-555t-467$		470 msec
t^3+6t+1	t^3-3t+1	1.13 sec
$t^9+9t^7+6t^6+81t^5+9t^4+120t^3+486t^2-1476t+251$		2.31 sec
t^3+t^2+5t+6	$t^3-3t+\left(-33671-2700\theta+22788\theta^2\right)$	1.57 sec
$t^9-9t^7-303405t^6+27t^5+1820430t^4+23018090232t^3-2730645t^2-69054270777t-46018413503$		2.78 sec
$t^3+t^2+5t+13$	$t^3+(-6-3\theta)\,t+\left(-30-6\theta+5\theta^2\right)$	430 msec
$t^9-15t^7-129t^6+117t^5+1038t^4+4148t^3-243t^2-1023t-127$		850 msec
$t^3-t^2-6t-12$	$t^3+\frac{-12-9\theta-3\theta^2}{2}t+\left(-3-3\theta-\theta^2\right)$	1.2 sec
$t^9-42t^7-25t^6+18t^5-60t^4-72t^3-36t^2-54t-27$		930 msec
t^3+t^2-2t+6	$t^3-3t+\left(-17+14\theta+8\theta^2\right)$	2.0 sec
$t^9-9t^7-25t^6+27t^5+150t^4+1292t^3-225t^2-3957t+2017$		810 msec

t^3+4t+6	$t^3-3t+\left(11+12\theta+\theta^2\right)$	1.24 sec
$t^9-9t^7+25t^6+27t^5-150t^4+968t^3+225t^2-2985t-1369$		680 msec
t^3+t^2+t+7	$t^3-3t+\left(119635+48654\theta-3888\theta^2\right)$	2.11 sec
$t^9-9t^7+314139t^6+27t^5-1884834t^4+30613800432t^3+2827251t^2-91841401377t-37455710399$		3.46 sec
t^3+t^2+7t+1	$t^3+3\theta t+\left(2+14\theta+\theta^2\right)$	1.24 sec
$t^9-3t^7-21t^6+63t^5+564t^4+1240t^3-243t^2-561t-19$		730 msec
t^3+7	$t^3-3t+\left(-527+252\theta+276\theta^2\right)$	1.87 sec
$t^9-9t^7-1581t^6+27t^5+9486t^4+2293752t^3-14229t^2-6881337t+2088001$		3.99 sec
$t^3+t^2-9t-21$	$t^3+\frac{-15-6\theta+3\theta^2}{2}t+\frac{-3+18\theta-5\theta^2}{2}$	1.21 sec
$t^9+9t^7-61t^6+135t^5-750t^4+1404t^3+153t^2-297t+27$		760 msec
$t^3+t^2+11t-1$	$t^3-3t+\left(2-2\theta-\theta^2\right)$	1.19 sec
$t^9-9t^7+29t^6+27t^5-174t^4+216t^3+261t^2-729t+351$		640 msec
$t^3+t^2+3t+15$	$t^3-3t+\frac{3-\theta^2}{2}$	980 msec
$t^9-9t^7+7t^6+27t^5-42t^4-18t^3+63t^2-27t-27$		480 msec
t^3-3t+8	t^3-3t+1	1.31 sec
$t^9-18t^7+27t^6+81t^5-81t^4-81t^3+729t+729$		520 msec
$t^3-6t+10$	$t^3-3t+\left(-19+3\theta+3\theta^2\right)$	1.61 sec
$t^9-9t^7-21t^6+27t^5+126t^4+228t^3-189t^2-765t-73$		1.61 sec
t^3+6t+6	$t^3+(-3-3\theta)\,t+\left(13+12\theta-3\theta^2\right)$	2.31 sec
$t^9-9t^7+75t^6+81t^5-720t^4+1956t^3+243t^2-711t+73$		2.9 sec

Man sieht an diesen kleinen Beispielen, daß es nicht unbedingt immer schneller ist, die Maximalordnung relativ auszurechnen. Aber schon die zweite Serie von Beispielen zeigt den Vorteil der relativen Methode.

Die zweite Serie von Beispielen enthält Grundkörper mit Klassengruppe C2×C2. Da die Berechnung der absoluten Maximalordnung hier zum Teil schon sehr zeitintensiv ist, wird nicht die Zeit time$(\tilde{\mathcal{E}}/\mathbb{Q})$ angegeben, sondern $\log_{10}(\mathfrak{d}_{\tilde{\mathcal{E}}/\mathbb{Q}}(\mathbb{Z}[\zeta]))$.

$T_{\mathcal{F}/\mathbb{Q}}$	$T_{\mathcal{E}/\mathcal{F}}$	time$(\mathcal{E}/\mathcal{F})$
$T_{\tilde{\mathcal{E}}/\mathbb{Q}}$		$\log_{10}(\mathfrak{d}_{\tilde{\mathcal{E}}/\mathbb{Q}}(\mathbb{Z}[\zeta]))$
$t^3+t^2-202t-1169$	$t^4+\left(6446+400\theta-50\theta^2\right)t^2+\left(-1709728-1063290\theta+13225\theta^2\right)$	1.46 sec
$t^{12}-1312t^{10}+401218t^8-18688474t^6+197120741t^4-328533334t^2+148035889$		134.89
$t^3+t^2-150t+649$	$t^4+\left(-5856+1754\theta-130\theta^2\right)t^2+\left(85045519-25534275\theta+1895910\theta^2\right)$	1.78 sec
$t^{12}-58452t^{10}+851729818t^8-5682387622t^6+6764222377t^4-2809479582t^2+367220569$		168.30
$t^3+t^2-57t-132$	$t^4+\left(144644+40468\theta-7274\theta^2\right)t^2+\left(-15943736420-4470628673\theta+797730906\theta^2\right)$	5.04 sec
$t^{12}-443046t^{10}+49764442415t^8-153081283399838t^6+72784209337098729t^4-1761522071268108 28t^2+106853444959340304$		250.07

$t^3+t^2-319t+2086$	$t^4+\left(-140272+263460-1236\theta^2\right)t^2 + \left(39352008084-7894500844\theta+3954209010\theta^2\right)$	7.92 sec
$t^{12}-1236966t^{10}+380112690415t^8-456419770620054t^6 + 137450568593256753t^4-10271442887640203 6t^2+18415119653382400$		266.57
$t^3-161t+775$	$t^4+\left(-2258+1358\theta-154\theta^2\right)t^2+\left(76480539-21352791\theta+1479376\theta^2\right)$	1.88 sec
$t^{12}-56362t^{10}+776635921t^8-930019147890t^6 + 292172962292206t^4-329947394834248t^2+93318478702201$		215.82
$t^3+t^2-82t-281$	$t^4+\left(40-30\theta-10\theta^2\right)t^2+\left(12789+6003\theta+702\theta^2\right)$	3.1 sec
$t^{12}-1500t^{10}+449894t^8-40993030t^6+777248109t^4-882200970t^2+95004009$		143.29
$t^3+t^2-236t+1313$	$t^4+\left(-354+20\theta+2\theta^2\right)t^2+\left(4330-253\theta-25\theta^2\right)$	1.76 sec
$t^{12}-136t^{10}+6638t^8-142690t^6+1387513t^4-5026810t^2+502681$		82.73
$t^3+t^2-108t+292$	$t^4+\left(298780-723000\theta-8364\theta^2\right)t^2 + \left(-60833405376+14850818352\theta+1660355824\theta^2\right)$	10.29 sec
$t^{12}-846348t^{10}+195006383728t^8-67689142255 47072t^6 + 619524501588790876 16t^4-114631785162752 0t^2+3838050304$		273.38
$t^3-t^2-204t+1024$	$t^4+\left(-1193170+327000\theta+6780\theta^2\right)t^2 + \left(83027620737-2274422220\theta-471884508\theta^2\right)$	10.44 sec
$t^{12}-773790t^{10}+54251623719t^8-30916992698500t^6 + 1596459691389375t^4-2247484218750t^2+284765625$		241.54
$t^3+t^2-58t+57$	$t^4+\left(-4682+5188\theta-684\theta^2\right)t^2+\left(101705161-115372148\theta+15267340\theta^2\right)$	1.42 sec
$t^{12}-99262t^{10}+2217306887t^8-234863562180t^6+6234602677119t^4 - 14659024197 42t^2+86523634201$		203.53
$t^3+t^2-81t+208$	$t^4+\left(-1463844+709396\theta-74424\theta^2\right)t^2 + 6314527349056-305765189128 0\theta+320229376480\theta^2$	5.73 sec
$t^{12}-17232040t^{10}+742729775803 04t^8-320323350979626816t^6 + 346260180112656674304t^4-1544484866154521687040t^2+1149413717110484647936$		313.51
$t^3+t^2-78t+190$	$t^4+\left(90430-176000\theta-5080\theta^2\right)t^2 + \left(-1880481519+346355712\theta+112579272\theta^2\right)$	11.11 sec
$t^{12}-508670t^{10}+76131144135t^8-29502655965 82980t^6 + 336395347934050224 63t^4-2071803669806430t^2+11483908569$		269.33

VIII.2 Ein großes Beispiel

In diesem Abschnitt wird ein Beispiel zu dem in der Einleitung beschriebenen Verfahren angegeben. Ausgehend von einer absoluten Erweiterung $\tilde{\mathcal{E}}/\mathbb{Q}$ wird zuerst ein Teilkörper [Klü95] $\tilde{\mathcal{F}}$ von $\tilde{\mathcal{E}}$ gesucht und danach die Maximalordnung von $\tilde{\mathcal{E}}$ relativ berechnet.

Der Körper $\tilde{\mathcal{E}}$ wird von einer Nullstelle des Polynoms

$T_{\tilde{\mathcal{E}}/\mathbb{Q}} = t^{60}+84t^{59}+3066t^{58}+61882t^{57}+700413t^{56}+3168102t^{55}-22705178t^{54}-388323306t^{53}-1243708137t^{52}+12334904436t^{51}+110093413374t^{50}-24492839868t^{49}-3570623856900t^{48}-8657503987986t^{47}+70643429188290t^{46}+333277349298648t^{45}-780629295051585t^{44}-6720592585518630t^{43}+1274592965191492t^{42}+71941390459943970t^{41}+43993286619709686t^{40}-278665978068165380t^{39}+960193920504845292t^{38}+3315384654237681186t^{37}+2252517348140221270t^{36}+158399835500040457302t^{35}+1017475399844510125302t^{34}+319977356490971740590t^{33}-16523303151700473119838t^{32}-40570180367270034601386t^{31}+129195943706761411501890t^{30}+858839587399521367592274t^{29}+2043829649509736587976043t^{28}+2584858480353796388811852t^{27}+7940554885475034535728666t^{26}+72086983221404118413481084t^{25}+279134342364669598099214392t^{24}+903209409482321441574827130t^{23}+3848049364087074745042150686t^{22}+11231908935957432263295366928t^{21}+33876482436007046369196083610t^{20}+133723063310218035575177804898t^{19}+464697711042454822841109498286t^{18}+2072535594563033094458289359376t^{17}+9093526361271265488008256766125t^{16}+32914361063044852937507303517258t^{15}+102602741068558928374528991322942t^{14}+269077089732302834998880270112000t^{13}+648131084652691297182665026591569t^{12}+1424284789909446342159039487719234t^{11}+2836258158848836494249152344689048t^{10}+5252680945056710906258688583079454t^{9}+9179279627405988982688302580342748t^{8}+14911390426499642448422499130328340t^{7}+21513968695033420618921974047636580t^{6}+27894701764403929784930583789571590t^{5}+35135389626457587788597704792573041t^{4}+32472716099804426526448196041700778t^{3}+12608018814971125833148827970444440t^{2}-803819785820971317456154323077172t+245569760773004609815662652389597$ erzeugt. $\tilde{\mathcal{E}}$ ist Zerfällungskörper des Polynoms $t^5+t^4-2t^3+t^2+t+1$ mit Galoisgruppe A5.

Ein Körper $\mathcal{F}$, der zu einem Teilkörper $\tilde{\mathcal{F}}$ von $\tilde{\mathcal{E}}$ isomorph ist, wird von einer Nullstelle des Polynoms

$T_{\mathcal{F}/\mathbb{Q}} = t^6+107070t^5+326554279347t^4-1524709002707300980t^3+254315639920311243715599t^2-14131391509203621423441736554t+245569760773004609815662652389597$ erzeugt.

Eine Ganzheitsbasis von $\mathcal{F}$ ist:

$$\omega_1 = 1,$$

$$\omega_2 = \frac{1+\theta}{2},$$

$$\omega_3 = \frac{9+2\theta+\theta^2}{12},$$

$$\omega_4 = \frac{63+7\theta+\theta^2+\theta^3}{72},$$

$$\omega_5 = \frac{81+56\theta+6\theta^2+\theta^4}{144},$$

$\omega_6 = (130629713447847000329484028365034253646345688232019803655150571346807807204943+225972467847690622985753905160235353689190819805765074748501520395480010141770\theta+100431829735033773463988479168715207615848715934846823089506819959876802428820\theta^2+219255375296269111484157855877365995458648083267404698589546140122021439822220\theta^3+74524905928263660959516917347203676352673076738410627746427641724194040555030\theta^4+\theta^5)/d$, wobei $d = 293539580015462219853035516319447187596717591833533732448050975092887295712224$.

Der zu $\tilde{\mathcal{E}}$ isomorphe Körper $\mathcal{E}$ wird von einer Nullstelle des Polynoms

$T_{\mathcal{E}/\mathcal{F}} = t^{10}+14t^9+(-546499422650765384298853306333856636360281681108743\omega_1-790353630175645891933479708303534630480662658901176\omega_2+388534506945620237484718946107647660175417299356280\omega_3+1512605134920954447506845591984664043040139080254792\omega_4+1028269024048058277038491489386848009024073165902856\omega_5-2812609848180968526764921132650802939687089355965452\omega_6)t^8+(-5619138061650184955058839097567673120885683113443956\omega_1-8126460855058226511365819077565968037075014252145276\omega_2+3994933838453095692405082665973086680719123239299664\omega_3+15552691793625895202031366160685766403484360436216474\omega_4+10572720429636562604388953771186287665207947176867056\omega_5-28919413992840554022721249898197338545741557108527072\omega_6)t^7+(-34594819303175242022147294693344511972731684972269894\omega_1-50031417945353922121607733892008708766747484135765542\omega_2+24595233780185574236220048601429371340590045880018650\omega_3+95751796160789849575477828437550357784102009915787210\omega_4+65092074405954751054878584793919101615527840010702258\omega_5-178045438723786881718835717521670772509218601889762294\omega_6)t^6+(-152255788555231723024178577141668818639511259450829566\omega_1-220194039027891768086500179746796573894721884679770888\omega_2+108246459710767118066744669863654976725395706317519570\omega_3+421414695139129527575678428104052167579394588050037080\omega_4+286477724613084509802311802436164449799284249358935634\omega_5-783598504561758090732153369707967600444816894318369078\omega_6)t^5+(470010513099372172658844131052153560468140818252960559\omega_1+679734506300098293534482629680479324661190344391357042\omega_2-334154612790910315040337510701323067271320433107218620\omega_3-1300898566612506165320204828121931134073428870634282506\omega_4-884350891447994224436736614366714484825611552412004308\omega_5+2418952597387584554329864513595847710698309193217163056\omega_6)t^4+(5963459552982104483258969543511744935171335200531542240\omega_1+8624422480162412991385031136715242604028589345708908954\omega_2-4239729670471603028771655486684521109843121160025316830\omega_3-16505707358264704362711014322182979010486640558567060466\omega_4-11220580444077785526048185567373588020043335871755071422\omega_5+30691496409255817788638497160594866473498859708245201906\omega_6)t^3+(6863671758509695448589931033513976639287642273125191811\omega_1+9926319527218990899766628661875564873662422133614057720\omega_2-4879736760917523837988066364306190761859927906372175590\omega_3-18997321343865764292703288886787547543834250474928657630\omega_4-12914379719334365904044073498479307047848678872005682666\omega_5+35324521824797062215434551364452832974243823897978487834\omega_6)t^2+(31124790112364262971046613963176513538885286574510395260\omega_1+45013022583707742149872421521161711014527182849866604544\omega_2-22128211812990884661719141566269127365853236037973736366\omega_3-86147423759283268923135328554536522159708106988331648220\omega_4-58563021708796368087787999670440103239053573852880626558\omega_5+160186612399303612860115914906945555420753827170717789818\omega_6)t+(-\omega_1+2\omega_2)$ über $\mathcal{F}$ erzeugt.

Es gilt $\log_{10}(\mathfrak{d}_{\tilde{\mathcal{E}}/\mathbb{Q}}(\mathbb{Z}[\zeta])) \approx 2439.0517$ für die Diskriminante der absoluten Gleichungsordnung $\mathbb{Z}[\zeta]$, wobei ζ Nullstelle von $T_{\tilde{\mathcal{E}}/\mathbb{Q}}$ ist. Die Berechnung der relativen Maximalordnung $o_{\mathcal{E}}$ von $\mathcal{E}/\mathcal{F}$ benötigte 67.6 Stunden. In der Diskriminante der relativen Gleichungsordnung zu $T_{\mathcal{E}/\mathcal{F}}$ gehen die folgenden Primideale auf:

$$\begin{aligned}
\mathfrak{p}_1 &= 2o_{\mathcal{F}} + (\omega_1 + \omega_2 + \omega_3 + \omega_4)o_{\mathcal{F}},\\
\mathfrak{p}_2 &= 2o_{\mathcal{F}} + (\omega_1 + \omega_3 + \omega_4 + \omega_6)o_{\mathcal{F}},\\
\mathfrak{p}_3 &= 3o_{\mathcal{F}} + (-\omega_1 + \omega_2 - \omega_3 + \omega_4)o_{\mathcal{F}},\\
\mathfrak{p}_4 &= 3o_{\mathcal{F}} + (\omega_2 + \omega_4 - \omega_6)o_{\mathcal{F}},\\
\mathfrak{p}_5 &= 13o_{\mathcal{F}} + (3\omega_1 + 2\omega_2)o_{\mathcal{F}},\\
\mathfrak{p}_6 &= 23o_{\mathcal{F}} + (4\omega_1 + 2\omega_2)o_{\mathcal{F}},\\
\mathfrak{p}_7 &= 23o_{\mathcal{F}} + (11\omega_1 + 2\omega_2)o_{\mathcal{F}},\\
\mathfrak{p}_8 &= 29o_{\mathcal{F}} + (5\omega_1 + 2\omega_2)o_{\mathcal{F}},\\
\mathfrak{p}_9 &= 29o_{\mathcal{F}} + (7\omega_1 + 2\omega_2)o_{\mathcal{F}},\\
\mathfrak{p}_{10} &= 29o_{\mathcal{F}} + (-19\omega_1 + 50\omega_2 + 12\omega_3)o_{\mathcal{F}},\\
\mathfrak{p}_{11} &= 43o_{\mathcal{F}} + (14\omega_1 + 2\omega_2)o_{\mathcal{F}},\\
\mathfrak{p}_{12} &= 109o_{\mathcal{F}} + (58\omega_1 + 2\omega_2)o_{\mathcal{F}},\\
\mathfrak{p}_{13} &= 911o_{\mathcal{F}} + (6\omega_1 + 2\omega_2)o_{\mathcal{F}},\\
\mathfrak{p}_{14} &= 911o_{\mathcal{F}} + (228\omega_1 + 2\omega_2)o_{\mathcal{F}},\\
\mathfrak{p}_{15} &= 911o_{\mathcal{F}} + (891\omega_1 + 2\omega_2)o_{\mathcal{F}},\\
\mathfrak{p}_{16} &= 654877o_{\mathcal{F}} + (508465\omega_1 + 2\omega_2)o_{\mathcal{F}},\\
\mathfrak{p}_{17} &= 1344821o_{\mathcal{F}} + (1073889\omega_1 + 2\omega_2)o_{\mathcal{F}},\\
\mathfrak{p}_{18} &= 85190379823o_{\mathcal{F}} + (43100541624\omega_1 + 2\omega_2)o_{\mathcal{F}},\\
\mathfrak{p}_{19} &= 95083939451o_{\mathcal{F}} + (36560949660\omega_1 + 2\omega_2)o_{\mathcal{F}},\\
\mathfrak{p}_{20} &= 95083939451o_{\mathcal{F}} + (50246264649\omega_1 + 2\omega_2)o_{\mathcal{F}},\\
\mathfrak{p}_{21} &= 5349810303917o_{\mathcal{F}} + (2654893653014\omega_1 + 2\omega_2)o_{\mathcal{F}},\\
\mathfrak{p}_{22} &= 34312285612559o_{\mathcal{F}} + (2458480287668\omega_1 + 2\omega_2)o_{\mathcal{F}},\\
\mathfrak{p}_{23} &= 12935629483888120619o_{\mathcal{F}} + (8595648034405811959\omega_1 + 2\omega_2)o_{\mathcal{F}},\\
\mathfrak{p}_{24} &= 13086888050349475486825 7o_{\mathcal{F}} + (27243418584508563047579\omega_1 + 2\omega_2)o_{\mathcal{F}}.
\end{aligned}$$

In der folgenden Tabelle sind einige Zeiten des relativen Round-2-Algorithmus angegeben. $\mathrm{time}(\mathcal{O}_{\mathfrak{p}})$ ist die Zeit, die zur Berechnung der $\mathfrak{p}$-maximalen Relativordnung benötigt wurde. Die Relativordnung $\mathcal{O}_{\mathfrak{p},1}$ ist das Ergebnis des Dedekindtests im $\mathfrak{p}$-ten Schritt. $o_{\mathcal{F}}[\rho]$ ist die relative Gleichungsordnung, wobei ρ eine Nullstelle des Polynoms $T_{\mathcal{E}/\mathcal{F}}$ ist.

$\mathfrak{p}$	$\nu_{\mathfrak{p}}(\mathfrak{d}_{\mathcal{E}/\mathcal{F}}(o_{\mathcal{F}}[\rho]))$	$\nu_{\mathfrak{p}}([o_{\mathcal{E}} : o_{\mathcal{F}}[\rho]])$	$\nu_{\mathfrak{p}}([\mathcal{O}_{\mathfrak{p},1} : o_{\mathcal{F}}[\rho]])$	$\nu_{\mathfrak{p}}(\mathfrak{d}_{\mathcal{E}/\mathcal{F}}(o_{\mathcal{E}}))$	$\mathrm{time}(\mathcal{O}_{\mathfrak{p}})$
$\mathfrak{p}_1$	10	5	5	0	227.76 sec
$\mathfrak{p}_2$	10	5	5	0	22.71 sec
$\mathfrak{p}_3$	89	42	2	5	23.57 h
$\mathfrak{p}_4$	111	53	2	5	42.66 h
$\mathfrak{p}_5$	2	1	1	0	21.72 sec
$\mathfrak{p}_6$	2	1	1	0	16.74 sec
$\mathfrak{p}_7$	4	2	2	0	41.93 sec
$\mathfrak{p}_8$	2	1	1	0	176.58 sec
$\mathfrak{p}_9$	2	1	1	0	15.44 sec
$\mathfrak{p}_{10}$	2	1	1	0	18.79 sec
$\mathfrak{p}_{11}$	4	2	2	0	38.92 sec
$\mathfrak{p}_{12}$	2	1	1	0	17.61 sec
$\mathfrak{p}_{13}$	2	1	1	0	16.40 sec
$\mathfrak{p}_{14}$	2	1	1	0	16.38 sec
$\mathfrak{p}_{15}$	2	1	1	0	19.10 sec
$\mathfrak{p}_{16}$	2	1	1	0	17.56 sec
$\mathfrak{p}_{17}$	2	1	1	0	17.44 sec
$\mathfrak{p}_{18}$	2	1	1	0	22.53 sec
$\mathfrak{p}_{19}$	2	1	1	0	21.34 sec
$\mathfrak{p}_{20}$	2	1	1	0	20.74 sec
$\mathfrak{p}_{21}$	2	1	1	0	28.27 sec
$\mathfrak{p}_{22}$	2	1	1	0	23.39 sec
$\mathfrak{p}_{23}$	2	1	1	0	33.02 sec
$\mathfrak{p}_{24}$	2	1	1	0	32.11 sec

Anhang A
Die Division von relativen Idealen

Hier sollen die Division und Invertierung von Idealen in Relativordnungen beschrieben werden. Um eine vernünftige Definition von Division und Invertierung zu gewährleisten, also um sicher zu stellen, daß wieder (gebrochene) Ideale entstehen, ist es notwendig, sich auf die relative Maximalordnung $o_\mathcal{E}$ zu beschränken. Es seien die beiden (gebrochenen) Ideale $\mathfrak{b}$ und $\mathfrak{c}$ in der relativen Maximalordnung $o_\mathcal{E}$ gegeben. Voraussetzung für die beiden hier beschriebenen Verfahren ist die Darstellung der relativen Ideale durch eine Pseudobasis wie in Satz II.52. Man benötigt auch eine Pseudobasis für die relative Maximalordnung $o_\mathcal{E}$.

Es seien

$$o_\mathcal{E} = \mathfrak{a}_1\omega_1 + \ldots + \mathfrak{a}_n\omega_n,$$
$$\mathfrak{b} = \mathfrak{b}_1\tau_1 + \ldots + \mathfrak{b}_n\tau_n,$$
$$\mathfrak{c} = \mathfrak{c}_1\eta_1 + \ldots + \mathfrak{c}_n\eta_n,$$

die Darstellungen durch Pseudobasen.

Gesucht ist eine Pseudobasis für das Ideal

$$\mathfrak{b}/\mathfrak{c} := \{x \in \mathcal{E} \mid x\mathfrak{c} \subseteq \mathfrak{b}\}.$$

Die Existenz dieser Pseudobasis ist gesichert, da die oben definierte Menge in dem Dedekindring $o_\mathcal{E}$ ein Ideal ist.

An der Definition des Ideals $\mathfrak{b}/\mathfrak{c}$ erkennt man sofort die schon in VII.1 erwähnte Ähnlichkeit zu dem Multiplikatorring. Zur Erinnerung wird hier noch einmal die Definition des Multiplikatorringes eines (gebrochenen) Ideals $\mathfrak{a}$ in $o_\mathcal{E}$ wiederholt:

$$[\mathfrak{a}/\mathfrak{a}] := \{x \in \mathcal{E} \mid x\mathfrak{a} \subseteq \mathfrak{a}\}.$$

Da sich auch viele der einzelnen Schritte sehr ähnlich sind, werden im folgenden nur die wesentlichen Schritte aufgeführt. Zum Verständnis der Zwischenschritte, die durch $(\ldots)$ gekennzeichnet sind, sei auf VII.1, den entsprechenden Abschnitt des Multiplikatorringes, verwiesen.

Da sowohl $\{\omega_1, \ldots, \omega_n\}$ als auch $\{\tau_1, \ldots, \tau_n\}$ $\mathcal{F}$-Basen von $\mathcal{E}$ sind, existiert eine invertierbare Matrix $S \in \mathcal{F}^{n\times n}$ mit den Eigenschaften

$$(\omega_1, \ldots, \omega_n) \cdot S = (\tau_1, \ldots, \tau_n),$$
$$(\tau_1, \ldots, \tau_n) \cdot S^{-1} = (\omega_1, \ldots, \omega_n).$$

Es seien $M_{\eta_i} \in \mathcal{F}^{n\times n}$ $(1 \le i \le n)$

$$\eta_i \cdot (\omega_1, \ldots, \omega_n) = (\omega_1, \ldots, \omega_n) \cdot M_{\eta_i}$$

wieder die sogenannten Repräsentationsmatrizen.

In Verbindung mit der Matrix S gilt dann

$$\eta_i \cdot (\omega_1, \ldots, \omega_n) = (\tau_1, \ldots, \tau_n) \cdot S^{-1} \cdot M_{\eta_i} \;\; (1 \le i \le n).$$

Es sei nun $x \in \mathcal{E}$ ein beliebiges Element. x hat eine Darstellung

$$x = x_1\omega_1 + \ldots + x_n\omega_n,$$

mit Elementen $x_i \in \mathcal{F}$ $(1 \le i \le n)$. Für $1 \le i \le n$ kann man dann das Produkt $x \cdot \eta_i$ wie folgt schreiben:

$$x \cdot \eta_i = \sum_{j=1}^{n} x_j\omega_j\eta_i = \ldots = (\tau_1, \ldots, \tau_n) \cdot S^{-1} \cdot M_{\eta_i} \cdot \overline{x},$$

wobei der Vektor $\overline{x}$ wie folgt definiert ist:

$$\overline{x} := \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}.$$

Hieraus ergibt sich dann die folgende Kette von Äquivalenzen: $x \in \mathfrak{b}/\mathfrak{c}$ genau dann, wenn $x \cdot \mathfrak{c} \subseteq \mathfrak{b}$. Dies ist aber äquivalent zu

$$\sum_{i=1}^{n} x\mathfrak{c}_i\eta_i \subseteq \sum_{j=1}^{n} \mathfrak{b}_j\tau_j.$$

Dies gilt dann und nur dann, wenn $(\ldots)$

$$(1 \le i, \nu \le n) \;\; (\mathfrak{c}_i/\mathfrak{b}_\nu) \cdot \left(S^{-1} \cdot M_{\eta_i}\right)_{\nu,\cdot} \cdot \overline{x} \subseteq o_\mathcal{F}.$$

$$(\ldots)$$

Mit der wie folgt definierten Matrix

$$M := \begin{pmatrix} S^{-1} \cdot M_{\eta_1} \\ \hline S^{-1} \cdot M_{\eta_2} \\ \hline \vdots \\ \hline S^{-1} \cdot M_{\eta_n} \end{pmatrix}$$

erhält man dann die Äquivalenz zu: Für jeden Vektor des Moduls

$$y \in \mathcal{M} := \left(\underbrace{(\mathfrak{c}_1/\mathfrak{b}_1) \;\; (\mathfrak{c}_1/\mathfrak{b}_2) \;\; \cdots \;\; (\mathfrak{c}_1/\mathfrak{b}_n) \;\; (\mathfrak{c}_2/\mathfrak{b}_1) \;\; \cdots \;\; (\mathfrak{c}_n/\mathfrak{b}_n)}_{M^{tr}} \right),$$

gilt

$$\overline{x}^{tr} \cdot y \in o_\mathcal{F}.$$

Es sei

$$\begin{pmatrix} \mathfrak{e}_1 & \cdots & \mathfrak{e}_n \\ & \hat{M} & \end{pmatrix} := \mathrm{HNF}(\mathcal{M}) = \mathcal{M},$$

eine Normalform, wie in Theorem II.41, von dem Modul $\mathcal{M}$. Man erhält also: $x \in \mathfrak{b}/\mathfrak{c}$ genau dann, wenn für jeden Vektor des Moduls

$$y \in \begin{pmatrix} \mathfrak{e}_1 & \cdots & \mathfrak{e}_n \\ & \hat{M} & \end{pmatrix}$$

gilt

$$\overline{x}^{tr} \cdot y \in o_\mathcal{F}.$$

$$(\ldots)$$

Man erhält abschließend

$$\mathfrak{b}/\mathfrak{c} = (1/\mathfrak{e}_1)\,\psi_1 + \ldots + (1/\mathfrak{e}_n)\,\psi_n,$$

wobei

$$(\psi_1, \ldots, \psi_n) := (\omega_1, \ldots, \omega_n) \cdot \left(\hat{M}^{tr}\right)^{-1}.$$

Daraus ergibt sich dann der folgende Algorithmus zur Division von relativen Idealen:

Algorithmus A.1 (Division relativer Ideale)
Input: *Die relative Maximalordnung* $o_\mathcal{E} = \mathfrak{a}_1\omega_1 + \ldots + \mathfrak{a}_n\omega_n$, *Ideale* $\mathfrak{b} = \mathfrak{b}_1\tau_1 + \ldots + \mathfrak{b}_n\tau_n$ *und* $\mathfrak{c} = \mathfrak{c}_1\eta_1 + \ldots + \mathfrak{c}_n\eta_n$ *in* $o_\mathcal{E}$.
Output: *Das Ideal* $\mathfrak{b}/\mathfrak{c} = \mathfrak{f}_1\psi_1 + \ldots + \mathfrak{f}_n\psi_n$.
(1) *Berechne die große Matrix M:*

$$M := \begin{pmatrix} S^{-1} \cdot M_{\eta_1} \\ \hline S^{-1} \cdot M_{\eta_2} \\ \hline \vdots \\ \hline S^{-1} \cdot M_{\eta_n} \end{pmatrix}.$$

(2) *Konstruiere den Modul:*

$$\mathcal{M} := \begin{pmatrix} (\mathfrak{c}_1/\mathfrak{b}_1) & (\mathfrak{c}_1/\mathfrak{b}_2) & \cdots & (\mathfrak{c}_1/\mathfrak{b}_n) & (\mathfrak{c}_2/\mathfrak{b}_1) & \cdots & (\mathfrak{c}_n/\mathfrak{b}_n) \\ & & & M^{tr} & & & \end{pmatrix}.$$

(3) *Berechne eine relative Normalform mit einem Verfahren wie in Theorem II.41:*

$$\begin{pmatrix} \mathfrak{e}_1 & \cdots & \mathfrak{e}_n \\ & \hat{M} & \end{pmatrix} := \mathrm{HNF}(\mathcal{M}).$$

(4) *Erzeuge die neuen Koeffizientenideale:*

$$\mathfrak{f}_i := (1/\mathfrak{e}_i) \;\; (1 \le i \le n).$$

(5) *Erzeuge die neuen Elemente:*

$$(\psi_1, \ldots, \psi_n) := (\omega_1, \ldots, \omega_n) \cdot \left(\hat{M}^{tr}\right)^{-1}.$$

(6) *Setze:*

$$\mathfrak{b}/\mathfrak{c} := \mathfrak{f}_1\psi_1 + \ldots + \mathfrak{f}_n\psi_n.$$

(7) *ENDE.*

Anhang B
Die Invertierung von relativen Idealen

Hier werden die gleichen Darstellungen der relativen Maximalordnung $o_\mathcal{E}$ und des (gebrochenen) Ideals $\mathfrak{c}$ verwendet, wie im vorangegangenen Abschnitt.

Gesucht ist hier das Ideal

$$1/\mathfrak{c} := \{x \in \mathcal{E} \mid x\mathfrak{c} \subseteq o_\mathcal{E}\}.$$

Vergleicht man dies mit der Division von relativen Idealen, so fällt auf, daß hier gilt

$$\mathfrak{b} = o_\mathcal{E} = \mathfrak{a}_1\omega_1 + \ldots + \mathfrak{a}_n\omega_n,$$

und insbesondere

$$S = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & 1 \end{pmatrix}.$$

Damit erhält man den Algorithmus zum Invertieren von relativen Idealen:

Algorithmus B.1 (Invertierung relativer Ideale)
Input: *Die relative Maximalordnung* $o_\mathcal{E} = \mathfrak{a}_1\omega_1 + \ldots + \mathfrak{a}_n\omega_n$ *und ein Ideal* $\mathfrak{c} = \mathfrak{c}_1\eta_1 + \ldots + \mathfrak{c}_n\eta_n$ *in* $o_\mathcal{E}$.
Output: *Das Ideal* $1/\mathfrak{c} = \mathfrak{f}_1\psi_1 + \ldots + \mathfrak{f}_n\psi_n$.

(1) *Berechne die große Matrix M:*

$$M := \begin{pmatrix} M_{\eta_1} \\ \hline M_{\eta_2} \\ \hline \vdots \\ \hline M_{\eta_n} \end{pmatrix}.$$

(2) *Konstruiere den Modul:*

$$\mathcal{M} := \begin{pmatrix} (\mathfrak{c}_1/\mathfrak{a}_1) & (\mathfrak{c}_1/\mathfrak{a}_2) & \cdots & (\mathfrak{c}_1/\mathfrak{a}_n) & (\mathfrak{c}_2/\mathfrak{a}_1) & \cdots & (\mathfrak{c}_n/\mathfrak{a}_n) \\ & & & M^{tr} & & & \end{pmatrix}.$$

(3) *Berechne eine relative Normalform mit einem Verfahren wie in Theorem II.41:*

$$\begin{pmatrix} \mathfrak{e}_1 & \cdots & \mathfrak{e}_n \\ & \hat{M} & \end{pmatrix} := \mathrm{HNF}(\mathcal{M}).$$

(4) *Erzeuge die neuen Koeffizientenideale:*

$$\mathfrak{f}_i := (1/\mathfrak{e}_i) \;\; (1 \le i \le n).$$

(5) *Erzeuge die neuen Elemente:*

$$(\psi_1, \ldots, \psi_n) := (\omega_1, \ldots, \omega_n) \cdot \left(\hat{M}^{tr}\right)^{-1}.$$

(6) *Setze:*

$$1/\mathfrak{c} := \mathfrak{f}_1\psi_1 + \ldots + \mathfrak{f}_n\psi_n.$$

(7) *ENDE.*

Bezeichnungen

In der vorliegenden Arbeit gelten die folgenden Bezeichnungen:

$\mathcal{F},\mathcal{E}$	algebraische Zahlkörper
R	ein beliebiger Ring
$Q(R)$	der Quotientenkörper von R
$o_{\mathcal{F}}, o_{\mathcal{E}}$	die Maximalordnung von $\mathcal{F}$ bzw. $\mathcal{E}$
$o_{\mathcal{F}}[\rho]$	die relative Gleichungsordnung zu ρ
$o_{\mathcal{F}}[t]$	der Polynomring über $o_{\mathcal{F}}$
$\mathcal{O}$	eine Ordnung eines Zahlkörpers
$\mathcal{O}_{\mathfrak{p}}$	die $\mathfrak{p}$-maximale Relativoberordnung zu $\mathcal{O}$
$\mathfrak{a},\mathfrak{b},\mathfrak{c}$	Ideale in einer Ordnung
$\mathfrak{p}$	ein Primideal in $o_{\mathcal{F}}$
$\mathfrak{P}$	ein Primideal in einer Relativordnung
$\mathfrak{d}_{\mathcal{F}/\mathbb{Q}}(O)$	die Diskriminante der absoluten Ordnung $\mathcal{O}$
$\mathfrak{d}_{\mathcal{E}/\mathcal{F}}(O)$	die Relativdiskriminante der Ordnung $\mathcal{O}$
$\mathfrak{d}_{\mathcal{F}/\mathbb{Q}}$	die absolute Körperdiskriminante
$\mathfrak{d}_{\mathcal{E}/\mathcal{F}}$	die relative Körperdiskriminante
$\mathrm{N}_{\mathcal{F}/\mathbb{Q}}(.)$	die absolute Norm von Elementen oder Idealen
$\mathrm{N}_{\mathcal{E}/\mathcal{F}}(.)$	die relative Norm von Elementen oder Idealen
$\mathrm{Tr}_{\mathcal{F}/\mathbb{Q}}(.)$	die absolute Spur von Elementen
$\mathrm{Tr}_{\mathcal{E}/\mathcal{F}}(.)$	die relative Spur von Elementen
$I_{\mathfrak{p}}(\mathcal{O})$	das $\mathfrak{p}$-Radikal einer Relativordnung $\mathcal{O}$
$[\mathfrak{a}/\mathfrak{a}]$	der Multiplikatorring eines Ideals $\mathfrak{a}$
$\mathcal{M},\mathcal{N}$	endlich erzeugte Moduln über Dedekindringen
$\nu_{\mathfrak{p}}(.)$	die $\mathfrak{p}$-exponentielle Bewertung
$.^{(i)}$	die i-te Konjugierten-Abbildung

Für beliebige Teilmengen M, N eines Ringes R gelten zusätzlich:

$M \subseteq N$	$x \in M \Rightarrow x \in N$
$M \subset N$	$M \subseteq N \wedge M \neq N$
$M + N$	$\{x + y \mid x \in M, y \in N\}$
$M - N$	$\{x - y \mid x \in M, y \in N\}$
$M \cdot N$	$\{\sum_{i=1}^{r} x_i y_i \mid r \geq 0, x_i \in M, y_i \in N \ (1 \leq i \leq r)\}$

Literaturverzeichnis

[Art65] Emil Artin. Questiones de base minimale dans la théorie des nombres algébrique. In J. Tate S. Lang, Herausgeber, *The collected papers of Emil Artin*, Seiten 229–231. Addison Wesley, 1965.

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

[Coh93] Henri Cohen. *A Course in Computational Algebraic Number Theory.* Springer, 1993.

[Coh96] Henri Cohen. Hermite and smith normal form algorithms over dedekind domains. *Math. Comput.*, **65** (1996), 1681–1699.

[Dab93] Mario Daberkow. Bestimmung relativer Ganzheitsbasen in relativquadratischen Zahlkörpern. Diplomarbeit, Heinrich-Heine-Universität Düsseldorf, 1993.

[DFK+97] Mario Daberkow, Claus Fieker, Jürgen Klüners, Micheal E. Pohst, Kathrine Roegner, Martin Schörnig, und Klaus Wildanger. KANT V4. *J. Symb. Comput.*, **24** (1997), 267–283.

[DW96] Mario Daberkow und Andreas Weber. A database for number fields. In J. Calmet und C. Limongelli, Herausgeber, *Design and Implementation of Symbolic Computation Systems*, Band 1128 aus *LNCS*, Seiten 320–330. Springer, 1996.

[Edg79] H. M. Edgar. A numberfield without an integral basis. *Math. Mag*, **52** (1979), 248–251.

[Heß96] Florian Heß. Zur Klassengruppenberechnung in algebraischen Zahlkörpern. Diplomarbeit, Technische Universität Berlin, 1996.

[Klü95] Jürgen Klüners. Über die Berechnung von Teilkörpern algebraischer Zahlkörper. Diplomarbeit, Technische Universität Berlin, 1995.

[Nar89] Władisław Narkiewicz. *Elementary and Analytic Theory of Algebraic Numbers.* Springer, zweite Auflage, 1989.

[Neu92] Jürgen Neukirch. *Algebraische Zahlentheorie.* Springer, 1992.

[O'M63] O. T. O'Meara. *Introduction to quadratic forms.* Springer, 1963.

[Poh93] Michael E. Pohst. *Computational algebraic number theory.* Deutsche Mathematiker-Vereinigung: DMV-Seminar. Birkhäuser, 1993.

[PZ89] Michael E. Pohst und Hans Zassenhaus. *Algorithmic Algebraic Number Theory.* Encyclopaedia of mathematics and its applications. Cambridge University Press, 1989.

Index