Universität Ulm
Fakultät für Mathematik und Wirtschaftswissenschaften

Konstruktive Idealtheorie in Quaternionenalgebren

Diplomarbeit

in Mathematik

vorgelegt von
Kirschmer, Markus
am 30. August 2005

Gutachter

Prof. Dr. G. Nebe
Prof. Dr. W. Lütkebohmert

Inhaltsverzeichnis

Kapitel 1

Einleitung

1.1 Problemstellung

Der Ausgangspunkt für die Diplomarbeit ist folgende Situation. Es sei A eine zentraleinfache K-Algebra über einem algebraischen Zahlkörper K mit $R = \mathbb{Z}_K$, dem ganzen Abschluß von $\mathbb{Z}$ in K. Dann gibt es nur endlich viele Konjugationsklassen $\mathfrak{M}_1, \ldots, \mathfrak{M}_T$ von R-Maximalordnungen in A. Ist $\mathfrak{M}$ eine R-Maximalordnung in A, so gibt es ebenfalls nur endlich viele Isomorphieklassen $I_1, \ldots, I_H$ von vollen Rechtsidealen von $\mathfrak{M}$. Dabei ist die Anzahl der Isomorphieklassen H unabhängig von $\mathfrak{M}$, und auch unabhängig davon, ob Rechts- oder Linksideale betrachtet werden.

Die Frage ist nun, wie man die Typenzahl T und die Klassenzahl H bestimmen kann, oder sogar Vertretersysteme $\mathfrak{M}_1, \ldots, \mathfrak{M}_T$ von Konjugationsklassen der R-Maximalordnungen und Vertretersysteme der Links- oder Rechtsidealklassen von $\mathfrak{M}$ konstruieren kann. Dies ist im Computeralgebrasystem Magma zur Zeit nur im Fall $K = \mathbb{Q}$ implementiert.

Die zentraleinfachen Algebren über einem globalen Körper kann man in zwei Klassen einteilen, je nachdem, ob die Algebra die Eichlerbedingung erfüllt, oder nicht.
Ist K ein algebraischer Zahlkörper, so erfüllt A die Eichlerbedingung genau dann, wenn A keine total definite Quaternionenalgebra ist.

Erfüllt A die Eichlerbedingung, so bilden die Rechtsidealklassen einer R-Maximalordnung eine endliche Gruppe, die isomorph zu einer vom Verzweigungsverhalten von A abhängigen Strahlklassengruppe von K ist. Hat man die Rechtsidealklassen einer einzigen R-Maximalordnung bestimmt, so kann man daraus $\mathfrak{M}_1, \ldots, \mathfrak{M}_T$ gewinnen. In diesem Fall können die Fragen daher auf das Rechnen in einer Strahlklassengruppe von K zurückgeführt werden.

Interessanter ist jedoch der Fall, wenn A die Eichlerbedingung verletzt. Dann bilden die Rechtsideale einer R-Maximalordnung im allgemeinen keine Gruppe. Das zentrale Hilfsmittel zum Lösen der Probleme ist dann die Normform $N\colon (x, y) \mapsto \mathrm{tr}_{A/K}(x\overline{y})$. Das ist eine total positiv definite symmetrische Bilinearform auf dem K-Vektorraum A.
Im folgenden werde daher der Fall betrachtet, in welchem A die Eichlerbedingung verletzt.

1.2 Bestimmung der R-Maximalordnungen

Um die Diskriminante der Algebra A zu bestimmen, benötigt man zuerst eine R-Maximalordnung. Dazu starten wir mit einer beliebigen R-Ordnung Λ, z.B. der Linksordnung des von einer K-Basis von A erzeugten R-Gitters. Nun gilt, daß eine R-Ordnung genau dann maximal ist, wenn sie an jeder Lokalisierung maximal ist. Ist $\Lambda_{\mathfrak{p}}$ für ein Primideal $\mathfrak{p}$ von R nicht maximal, so teilt $\mathfrak{p}$ die Diskriminante $d(\Lambda/R)$ von Λ. Daher haben wir nur an endlich vielen Primidealen zu untersuchen, ob sich Λ dort zu einer größeren Ordnung ergänzen läßt (siehe Abschnitt 5.2 auf Seite 87).

Mit Hilfe der Bilinearform N kann entschieden werden, ob zwei R-Maximalordnungen konjugiert sind. Dazu ist ein Isometrietest für zwei $\mathbb{Z}$-Gitter durchzuführen (siehe Satz 5.4.1). Ein solcher Algorithmus ist in [PS97] beschrieben und z.B. im Computeralgebrasystem MAGMA implementiert.

Ein anderes Problem ist es festzustellen, ob alle Konjugationsklassen von R-Maximalordnungen bereits bestimmt sind. Ein geometrischer Ansatz dazu ist die in Abschnitt 3.3 hergeleitete Minkowskischranke. Leider ist diese viel zu groß, um in einem konkreten Fall die Vollständigkeit eines Vertretersystems von R-Maximalordnungen zu gewährleisten (siehe Tabelle 3.1 auf Seite 73).

Einen Ausweg liefert die von Martin Eichler in [Eic55] gefundene Maßformel. Marie-France Vignéras bewies diese Formel in [Vig80] erneut mit Hilfe von Adelen und Idelen unter Verwendung von Maßtheorie.

Um festzustellen, ob alle Konjugationsklassen von R-Maximalordnungen bereits gefunden sind, ordnet man jeder Konjugationsklasse von R-Maximalordnungen ein Maß, also eine positive rationale Zahl zu. Die Summe der Maße aller Konjugationsklassen von R-Maximalordnungen läßt sich in Invarianten von K und A ausdrücken und ist somit schon a priori bekannt. In [Eic55] wurde gezeigt, daß sich dieses Maß bestimmen läßt, kennt man die Automorphismengruppe eines bestimmten $\mathbb{Z}$-Gitters (siehe auch [Neb98] und Satz 4.1.9). Das Maß kann daher mit dem in [PS97] beschriebenen Algorithmus zur Bestimmung von Automorphismengruppen berechnet werden, wenn nur $[K : \mathbb{Q}]$ nicht allzu groß ist.

Hat man eine R-Maximalordnung $\mathfrak{M}$ bestimmt, so findet man alle weiteren R-Maximalordnungen, indem man die Linksordnungen von ganzen Rechtsidealen von $\mathfrak{M}$ betrachtet. Aufgrund der Minkowskischranke muß man nur endlich viele solcher Rechtsideale betrachten. Man kann den Aufwand dadurch reduzieren, indem man nicht nur Rechtsideale von $\mathfrak{M}$ betrachtet, sondern zudem auch Rechtsideale von Vetretern schon gefundener Konjugationsklassen. Dann genügt es sogar, lediglich die maximalen Rechtsideale zu betrachten (vgl. Satz 2.5.33). Ist $\mathfrak{p}$ ein Primideal von R, dann findet man alle maximalen Rechtsideale $M_1, \ldots, M_k$ von $\mathfrak{M}$, die $\mathfrak{p}\mathfrak{M}$ enthalten, als Urbilder der maximalen Rechtsideale der endlich dimensionalen $\mathbb{F}_p$-Algebra $\mathfrak{M}/\mathfrak{p}\mathfrak{M}$, wobei $p\mathbb{Z} = \mathfrak{p} \cap \mathbb{Z}$ ist. Der Algorithmus zum Finden aller Konjugationsklassen von R-Maximalordnungen ist auf Seite 91 erklärt.

1.3 Konstruktion der Rechtsidealklassen

Um zu entscheiden, ob ein Rechtsideal von $\mathfrak{M}$ ein Hauptideal, also von der Gestalt $x\mathfrak{M}$ mit $x \in A^*$ ist, kann man ebenfalls $\mathbb{Z}$-Gitter verwenden. Man muß hierzu alle Vektoren x des Gitters einer bestimmten Länge betrachten und prüfen, ob sie der Bedingung $I = x\mathfrak{M}$ genügen. Der Algorithmus ist auf Seite 93 beschrieben.

Mit diesem Algorithmus kann man auch bestimmen, ob zwei Rechtsideale von $\mathfrak{M}$ isomorph sind. Denn die beiden Rechtsideale I und J von $\mathfrak{M}$ sind genau dann isomorph, wenn IJ^{-1} ein Hauptideal ist. Analog sind zwei Linksideale I und J von $\mathfrak{M}$ genau dann isomorph, wenn $J^{-1}I$ ein Hauptideal ist.

Die zweiseitigen Idealklassen einer R-Maximalordnung $\mathfrak{M}$ lassen sich leicht bestimmen. Denn verzweigt A an den Primidealen $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ von R, so liegt über jedem $\mathfrak{p}_i$ genau ein maximales zweiseitiges $\mathfrak{M}$-Ideal $\mathfrak{P}_i$. Dieses ist in diesem Fall jedoch auch ein maximal ganzes $\mathfrak{M}$-Rechtsideal und kann als solches wie schon zuvor bestimmt werden. Ist dann $\mathfrak{a}_1, \ldots, \mathfrak{a}_{h_K}$ ein Vertretersystem der Idealklassengruppe von K, so enthält

$$\left\{ \mathfrak{a}_i \prod_{j=1}^{s} \mathfrak{P}_j^{\alpha_j} \mid 1 \leq i \leq h_K,\ \alpha \in \{0,1\}^s \right\}$$

aus jeder zweiseitigen Idealklasse von $\mathfrak{M}$ mindestens einen Vertreter (vgl. Bemerkung 4.1.8).

Sind alle diese Algorithmen implementiert, so kann man zum letzten Problem, dem Bestimmen der Rechtsidealklassen einer R-Maximalordnung kommen. Man hat dazu zuerst Vertreter $\mathfrak{M}_1, \ldots, \mathfrak{M}_T$ aller Konjugationsklassen von R-Maximalordnungen zu bestimmen. Im zweiten Schritt muß man dann zu jedem $\mathfrak{M}_i$ Vertreter $\{I_{i,1}, \ldots, I_{i,H_i}\}$ der zweiseitigen Idealklassen von $\mathfrak{M}_i$ konstruieren. Die Menge $\{I_{i,j}\mathfrak{M}\}$ ist dann ein Vertretersystem der Rechtsidealklassen von $\mathfrak{M}$. Analog ist $\{\mathfrak{M}I_{i,j}\}$ ein Vertretersystem der Linksidealklassen von $\mathfrak{M}$ (siehe Korollar 2.6.7).

1.4 Gliederung

Die Arbeit gliedert sich in vier Teile. Im Kapitel 2 werden Grundlagen und Definitionen gegeben. Ab Abschnitt 2.5 werden wichtige Ergebnisse von zentraleinfachen Algebren bewiesen. Im dritten Kapitel werden Quaternionenalgebren behandelt. Insbesondere wird für total definite Quaternionenalgebren eine Minkowskischranke konstruiert. In Kapitel 4 werden die Grundlagen bereitgestellt, um die Eichlersche Maßformel auswerten zu können. Im fünften Kapitel werden die entwickelten Algorithmen beschrieben.

Im Anhang finden sich Tabellen mit ausgewählten Beispielen, für die ein Vertretersystem von R-Maximalordnungen konstruiert wurde. Außerdem sind dort die in MAGMA implementierten Algorithmen mitsamt einer kurzen Befehlsbeschreibung aufgeführt.

Kapitel 2

Zentraleinfache Algebren

In diesem einführenden Kapitel werden einige grundlegende Eigenschaften von zentraleinfachen Algebren bewiesen. Die meisten Sätze finden sich in [Rei03], [Lam91] und [Neb03].

2.1 Zentraleinfache Algebren

Es sei K ein Körper.

Definition 2.1.1 Ein Ring R heißt *einfach*, falls er nur die beiden zweiseitigen Ideale (0) und R besitzt.
Analog dazu wird ein R-Modul *einfach* genannt, falls er keine echten R-Teilmoduln enthält.
Für einen beliebigen Ring R bezeichne $Z(R) = \{x \in R \mid rx = xr \text{ für alle } r \in R\}$ das *Zentrum* von R.
Eine K-Algebra A heißt *einfach*, falls sie als Ring einfach ist. Eine *zentraleinfache* K-Algebra ist eine einfache K-Algebra mit $Z(A) = K$.

Alle in dieser Arbeit auftretenden K-Algebren sollen endlich dimensionale K-Vektorräume sein.

Satz 2.1.2 (Schurs Lemma) *Es sei R ein Ring und seien X, Y einfache R-Rechtsmoduln. Dann ist* $\mathrm{End}_R(X)$ *ein Schiefkörper, und es gilt*

$$\mathrm{Hom}_R(X,Y) \cong \begin{cases} \mathrm{End}_R(X) & \textit{falls } X \cong Y \\ 0 & \textit{sonst} \end{cases}$$

Beweis: Wähle ein $\varphi \in \mathrm{Hom}_R(X,Y)$ mit $\varphi \neq 0$. Dann sind $\ker(\varphi) \neq X$ und $\varphi(X) \neq 0$ Teilmoduln von X bzw. Y. Da X und Y einfach sind, gelten $\varphi(X) = Y$ sowie $\ker(\varphi) = 0$. Also ist $\varphi\colon X \to Y$ ein Isomorphismus. Insbesondere ist $\mathrm{End}_R(X)$ somit ein Schiefkörper und φ induziert den Isomorphismus

$$\mathrm{End}_R(X) \to \mathrm{Hom}_R(X,Y),\ f \mapsto \varphi \circ f\ . \qquad \square$$

Definition 2.1.3 Ein Ring R heißt rechts-artinsch (respektive links-artinsch), falls jede absteigende Kette von R-Rechtsidealen (respektive R-Linksidealen) stationär wird.

Definition 2.1.4 Definiert man auf einem Ring $(R, +, \cdot)$ die innere Verknüpfung

$$*\colon R \times R \to R, (x, y) \mapsto x * y := y \cdot x,$$

so bildet $(R, +, *)$ wieder einen Ring, der mit R^{opp} oder R^o bezeichnet wird.

Für ein $a \in R$ bezeichnen $\ell_a\colon R \to R$, $x \mapsto ax$ und $r_a\colon R \to R, x \mapsto xa$ die Links- bzw. Rechtsmultiplikation mit a.

$\mathrm{End}(R)$ wird nun auf zwei Arten zu einem Ring. Zum einen via $f \circ g\colon x \mapsto f(g(x))$ und zum anderen via $f \cdot g\colon x \mapsto g(f(x))$. Es gilt $\mathrm{End}(R, \circ) = \mathrm{End}(R, \cdot)^o$.

Im Theorieteil sind alle auftretenden Endomorphismenringe stets mit der Komposition „$\circ$“ aufgefaßt. Bei der Implementation der Algorithmen werden wir mit Zeilenvektoren arbeiten, da dies die Standardeinstellung des Computeralgebrasystems Magma ist. Das Anwenden eines Endomorphismus ist dann die Multiplikation einer Matrix von rechts mit einem Vektor. Dort fassen wir daher die Endomorphismenringe mit der Komposition $\cdot$ auf.

Bemerkung 2.1.5 Ist R ein Ring und M ein R-Rechtsmodul, so sind $\mathrm{End}_R(M^n)$ und $\mathrm{End}_R(M)^{n\times n}$ isomorphe Ringe.

Beweis: Es bezeichne $\pi_i\colon M^n \to M$ die Projektion auf die i-te Komponente sowie $j_k\colon M \to M^n$, $x \mapsto (x\delta_{kl})_l$. Dann ist ein Isomorpismus gegeben durch

$$\mathrm{End}_R(M^n) \to \mathrm{End}_R(M)^{n\times n},\ \varphi \mapsto (\pi_i \circ \varphi \circ j_k)_{i,k}\,. \qquad \square$$

Damit gilt der

Satz 2.1.6 (Struktursatz von Wedderburn) *Sei A ein links- oder rechts-artinscher einfacher Ring. Dann existiert ein Schiefkörper D und ein $n \in \mathbb{N}$ mit $A \cong D^{n\times n}$. Insbesondere gilt dies für jede zentraleinfache K-Algebra A. In diesem Fall ist dann $Z(D) = K$ und $\dim_K(D) < \infty$.*

Beweis: Es sei A rechts-artinsch und L ein minimales Rechtsideal von A. Da A einfach ist, ist das zweiseitige A-Ideal $A \cdot L$ gleich A. Also gibt es ein minimales n mit

$$1 = \sum_{k=1}^{n} a_k l_k \quad l_k \in L,\ a_k \in A\,.$$

Dies liefert einen Epimorphismus $\varphi\colon L^n \twoheadrightarrow A$, $(x_1, \ldots, x_n) \mapsto \sum_{k=1}^n a_k x_k$ von A-Rechtsmoduln. Angenommen, es existiert ein $(x_1, \ldots, x_n) \in \ker\varphi$ und $1 \le i \le n$ mit $x_i \neq 0$. Dann wäre $x_i A = L$, da L minimal ist. Es folgt $a_i L = a_i x_i A \subseteq \sum_{k\neq i} a_k L$, was aber der Minimalität von n widerspricht. Also ist φ ein Isomorphismus von A-Rechtsmoduln. Wir erhalten

$$A \cong \mathrm{End}_A(A) \cong \mathrm{End}_A(L^n) \cong \mathrm{End}_A(L)^{n\times n}\,.$$

Nach Schurs Lemma ist $\mathrm{End}_A(L)$ ein Schiefkörper. $\square$

Da die Ideale eines Matrixrings über einem Ring und die Ideale des Rings selbst bekanntlich korrespondieren, ist auch die Umkehrung des Satzes richtig. D.h. jeder Matrixring über einem Schiefkörper D ist eine einfache Algebra. Mit der selben Beweisidee zeigt man, daß $D^{1\times n}$ ein minimales Rechtsideal von $D^{n\times n}$ ist. Ferner haben wir gezeigt, daß ein einfacher Ring genau dann links-artinsch ist, wenn er rechts-artinsch ist.

Lemma 2.1.7 *Es sei A ein einfacher artinscher Ring. Weiter sei L ein minimales Rechtsideal von A und V ein einfacher A-Rechtsmodul. Ist $A \cong D^{n\times n}$ mit einem Schiefkörper D wie im Struktursatz von Wedderburn bestimmt, so gelten*

(a) $V \cong L \cong D^{1\times n}$ und $V^n \cong A$ als A-Rechtsmoduln.

(b) V ist ein treuer A-Modul, d.h. aus $Va = 0$ folgt $a = 0$ für $a \in A$.

(c) $(\mathrm{End}_A(V), \circ) \cong D$

Die analogen Aussagen gelten für die Linksmoduln und Linksideale von A.

Beweis:

(a) Im Beweis des Struktursatzes 2.1.6 haben wir $L^n \cong A$ gesehen. Damit ist $V = V \cdot A \cong V \cdot L^n$. Also ist $V \cdot L \neq 0$. Daher existiert ein $x \in V$ so, daß $L \to V$, $l \mapsto xl$ nicht überall verschwindet. Aus dem Lemma von Schur folgt $L \cong V$. Insbesondere gilt dies für das minimale Linksideal $L = D^{1\times n}$.

(b) Für $V = D^{1\times n}$ ist das klar. Wegen (a) genügt es, nur diesen Fall zu betrachten.

(c) Wir haben den Ringhomomorphismus $\sigma\colon D \to \mathrm{End}_{D^{n\times n}}(D^{1\times n})$, $d \mapsto (x \mapsto dx)$. Weil D^o einfach ist, ist σ ein Monomorphismus. Zum Beweis, daß σ surjektiv ist, sei $(e_1, \ldots, e_n)$ die Standardbasis von $D^{1\times n}$. Für ein $\varphi \in \mathrm{End}_{D^{n\times n}}(D^{1\times n})$ gibt es geeignete $d_k \in D$ mit $\varphi(e_1) = \sum_{k=1}^n d_k e_k$. Mit $E_{ij} = (\delta_{ik}\delta_{jl})_{kl} \in D^{n\times n}$ gilt

$$\varphi(e_k) = \varphi(e_1 E_{1k}) = \varphi(e_1)E_{1k} = d_1 e_1 E_{1k} = d_1 e_k \quad \text{für alle } 1 \leq k \leq n\,.$$

Also ist $\varphi = \sigma(d_1)$. □

Lemma 2.1.8 *Sind A und B zwei einfache K-Algebren mit $Z(A) = K$, so ist auch $A \otimes_K B$ eine einfache K-Algebra mit $Z(A \otimes_K B) = K \otimes_K Z(B) \cong Z(B)$.*

Beweis: Sei I ein von (0) verschiedenes Ideal in $A \otimes_K B$. Jedes $0 \neq x \in I$ besitzt dann eine Darstellung $x = \sum_{i=1}^m a_i \otimes b_i$ mit $a_i \in A \setminus \{0\}$ und linear unabhängigen $b_1, \ldots, b_m \in B$.
Wähle nun ein $x = \sum_{i=1}^m a_i \otimes b_i \in I \setminus \{0\}$, mit minimalem m. Da A eine einfache K-Algebra ist, gilt $Aa_1A = A$. Also ist $1 = \sum_{k=1}^l a'_k a_1 a''_k$ für geeignete $a'_k, a''_k \in A$. Es gilt

$$x' := \sum_{i=1}^m \left(\sum_{k=1}^l a'_k a_i a''_k \right) \otimes b_i = \sum_{k=1}^l (a'_k \otimes 1)x(a''_k \otimes 1) \in I.$$

Da die b_i linear unabhängig sind und der erste Term $1 \otimes b_1 \neq 0$ ist, ist $x' \neq 0$. Indem wir x durch x' ersetzen, können wir daher $a_1 = 1$ annehmen.
Wir behaupten nun es sei $m = 1$. Dann können wir, da B einfach ist, die obige Substitution auch für b_1 durchführen und zeigen so $1 \otimes 1 \in I$. Damit wäre die erste Aussage bewiesen.
Um die Behauptung $m = 1$ zu zeigen, nehmen wir $m > 1$ an. Dann kann a_2 sicher nicht in K liegen, denn sonst folgt aus $a_1 \otimes b_1 + a_2 \otimes b_2 = 1 \otimes b_1 + 1 \otimes a_2 b_2 = 1 \otimes (b_1 + a_2 b_2)$, daß x eine Darstellung mit weniger als m Summanden besitzt. Dies widerspräche jedoch der Minimalität von m.
Also ist $a_2 \in A \setminus K$. Da K das Zentrum von A ist, existiert ein $y \in A \otimes_K B$ mit $a_2 y \neq y a_2$. Damit gilt

$$I \ni \tilde{x} := (y \otimes 1)x - x(y \otimes 1) = \sum_{i=1}^{m} (y a_i - a_i y) \otimes b_i \overset{a_1=1}{=} \sum_{i=2}^{m} (y a_i - a_i y) \otimes b_i$$

Da die b_i sind linear unabhängig sind und der Summand $(y a_2 - a_2 y) \otimes b_2 \neq 0$ ist, muß auch $\tilde{x} \neq 0$ sein. Dann war m jedoch nicht minimal. Ein Widerspruch.

Nun müssen wir noch $Z(A \otimes_K B)$ bestimmen. Angenommen $x = \sum_{i=1}^{k} a_i \otimes b_i$ liege in $Z(A \otimes_K B)$, wobei die b_i (wie schon im ersten Teil) linear unabhängig sein sollen. Dann gilt für alle $a \in A$

$$0 = (a \otimes 1) \cdot x - x \cdot (a \otimes 1) = \sum_{i=1}^{k} (a a_i - a_i a) \otimes b_i \,.$$

Dies impliziert aber $a_i \in Z(A) = K$ für alle i. Damit wird $x = 1 \otimes \left(\sum_{i=1}^{k} a_i b_i \right)$. Da x auch mit allen $1 \otimes b$, $(b \in B)$ vertauscht, folgt $\sum_{i=1}^{k} a_i b_i \in Z(B)$. Dies zeigt $Z(A \otimes_K B) \subseteq K \otimes_K Z(B)$. Die umgekehrte Inklusion ist klar. □

Lemma 2.1.9 *Es sei A eine einfache K-Algebra, V ein A-Rechtsmodul und $E = (\mathrm{End}_A(V), \circ)$. Dann wird V ein $A \otimes_K E^o$-Rechtsmodul via*

$$v \cdot (a \otimes \varphi) := \varphi(v)a.$$

Fassen wir V als E^o-Rechtsmodul auf, so erhalten wir den Isomorphismus

$$\begin{array}{ccc} A & \xrightarrow{\sim} & \mathrm{End}_{E^o}(V) \\ a & \longmapsto & (v \mapsto va) \end{array}$$

Beweis: Die erste Aussage ist klar. Für die zweite können wir $A = D^{n \times n}$ und $V = D^{m \times n}$ mit einem Schiefkörper D annehmen. Dann gilt

$$E = \mathrm{End}_A(D^{m \times n}) \cong (\mathrm{End}_A(D^{1 \times n}))^{m \times m} \cong (D)^{m \times m}$$

und daher ist

$$\mathrm{End}_{E^o}(V) \cong \left(\mathrm{End}_{D^{m \times m}}(D^{m \times 1})\right)^{n \times n} \cong D^{n \times n}.$$

□

Definition 2.1.10 Es sei A eine zentraleinfache K-Algebra und B ein einfacher Ring mit $K \subseteq B \subseteq A$. Dann bezeichne

$$C_A(B) := \{x \in A \mid xb = bx \text{ für alle } b \in B\}$$

den *Zentralisator* von B in A.

Satz 2.1.11 *Mit den Bezeichnungen von Definition 2.1.10 gelten*

(a) $C_A(B)$ *ist einfach und es gilt die Doppelzentralisatoreigenschaft* $B = C_A(C_A(B))$.

(b) $[B : K][C_A(B) : K] = [A : K]$

(c) Ist $A \cong D^{n\times n}$, $V \cong D^{1\times n}$ *ein einfacher* A*-Rechtsmodul und* $D = (\mathrm{End}_A(V), \circ)$ *mit einem Schiefkörper* D*, so gilt*

$$\begin{array}{ccc} D \otimes_K B^o & \xrightarrow{\ \varphi\ } & \mathrm{End}_{C_A(B)}(V) \\ d \otimes b & \longmapsto & (x \mapsto d(x)b) \end{array}$$

Beweis: Es bezeichne $C = C_A(B)$. Wir erhalten

$$\begin{array}{ccc} d \otimes a & \longmapsto & x \mapsto d(x)a \\ D \otimes_K A^o & \longrightarrow & \mathrm{End}_K(V) \\ \uparrow & & \uparrow \\ D \otimes_K B^o & \xrightarrow{\ \varphi\ } & \mathrm{End}_C(V) \end{array}$$

denn es ist $d(xc)b = d(x)bc$ für alle $c \in C$, $x \in V, d \in D$ und $b \in B$. Aus Lemma 2.1.9 folgt weiter

$$\begin{array}{ccc} a & \longmapsto & v \mapsto va \\ A & \xrightarrow{\ \sim\ } & \mathrm{End}_{D^o}(V) \\ \uparrow & & \uparrow \\ C & \xrightarrow{\ \psi\ } & \mathrm{End}_{D^o \otimes_K B}(V) \end{array}$$

Ist $a \in A$ so, daß $(v \mapsto va) \in \mathrm{End}_{D^o \otimes B}(V)$ gilt, dann vertauscht a mit allen $b \in B$. Das heißt $a \in C$. Damit ist ψ surjektiv.
Sei nun W einfach über $D^o \otimes B$. Dann ist $\tilde{D} := \mathrm{End}_{D^o \otimes B}(W)$ ein Schiefkörper und es gilt $C \cong \tilde{D}^{r\times r}$ für ein $r \in \mathbb{N}$. Also ist C einfach. Mit Lemma 2.1.9 ist φ ein Isomorphismus und Teil (c) ist gezeigt.

Um den Beweis von Teil (a) zu beenden, sei $a \in C_A(C)$. Dann ist sicher $(v \mapsto va) \in \mathrm{End}_C(V)$. Da φ ein Isomorphismus ist, gilt $1 \otimes a \in D \otimes_K B^o$. Ist $(d_1 = 1, d_2, \ldots, d_n)$ eine K-Basis von D, dann ist $(d_1 \otimes 1, \ldots d_n \otimes 1)$ eine A-Basis von $D \otimes_K A^o$ bzw. eine B-Basis von $D \otimes_K B^o$. Daher existieren $b_k \in B$ mit $1 \otimes a = \sum_{k=1}^{n} (d_k \otimes 1)b_k$. Fassen wir die Gleichung über A auf und vergleichen den Koeffizienten von $1 = d_1$ so folgt $a = b_1 \in B$.

Nun zu (b): Es sei $D^o \otimes_K B \cong \tilde{D}^{m\times m}$ mit einem Schiefkörper $\tilde{D}$. Dann ist auch $V \cong \tilde{D}^{k\times m}$ für ein $k \geq 0$. Bezeichnen $b = \dim_K(B)$, $c = \dim_K(C_A(B))$, $d = \dim_K(D)$ und $\tilde{d} = \dim_K(\tilde{D})$, so gelten

$$\begin{aligned} k^2\tilde{d} = \dim_K(\mathrm{End}_{D^o\otimes B}(\tilde{D}^{k\times m})) = \dim_K(\mathrm{End}_{D^o\otimes B}(V)) = c \\ db = \dim_K(D^o \otimes_K B) = \dim_K(\tilde{D}^{m\times m}) = m^2\tilde{d} \\ km\tilde{d} = \dim_K(V) = \dim_K(D^{1\times n}) = nd \end{aligned}$$

Damit erhalten wir $bc = (d^{-1}m^2\tilde{d})(k^2\tilde{d}) = d^{-1}(nd)^2 = n^2d = \dim_K(A)$. □

Definition 2.1.12 Es sei A eine zentraleinfache K-Algebra und E/K eine endliche Körpererweiterung. E heißt *Zerfällungskörper* von A, falls $E \otimes_K A \cong E^{r\times r}$ für ein $r \in \mathbb{N}$ gilt. Man sagt dann auch E *zerfällt* A.

Bemerkung 2.1.13 Ist E ein Zerfällungskörper der K-Algebra A und E'/E eine endliche Körpererweiterung, so zerfällt auch E' die Algebra A.

Beweis: Es ist $E' \otimes_K A \cong E' \otimes_E (E \otimes_K A) \cong E' \otimes_E E^{r\times r} \cong E'^{r\times r}$ für ein $r \in \mathbb{N}$. □

Satz 2.1.14 *Es sei A eine zentraleinfache K-Algebra und D ein Schiefkörper mit $A \cong D^{k\times k}$ wie im Struktursatz von Wedderburn bestimmt. Dann gelten*

(a) K ist in jedem maximalen Teilkörper E von D enthalten und dieser zerfällt A. Mit $n := [E : K]$ gilt dann

$$E \otimes_K A \cong E^{nk\times nk} \quad \textit{und} \quad [D : K] = n^2 .$$

(b) D besitzt einen maximalen Teilkörper L, so daß L/K separabel ist.

Beweis: (a) Ohne Einschränkung ist $k = 1$, also $A = D$ ein Schiefkörper. Sei dann E ein maximaler Teilkörper von A. Dieser enthält sicherlich K, da man sonst durch Adjunktion von Elementen aus K einen größeren Teilkörper konstruieren kann.
Angenommen, es existiert ein $x \in C_A(E) \setminus E$, dann würde dieses mit allen Elementen in $E[x]$ kommutieren. Damit wäre $E(x) = E[x]$ ein Teilkörper von A, der E echt enthält, was nicht sein kann. Wir haben also $C_A(E) = E$ gezeigt. Nun verwenden wir Satz 2.1.11. Aus Teil (c) folgt $A \otimes_K E^o \cong \mathrm{End}_E(A) \cong E^{[A:E]^2}$ und Teil (b) zeigt $[A : K] = n^2$.

(b) Wir können $\mathrm{char}(K) = p$ annehmen und führen eine Induktion nach $m := [A : K]$. Der Fall $m = 1$ ist klar. Sei daher $m > 1$.
Zuerst wollen wir zeigen, daß es überhaupt einen von K verschiedenen Teilkörper E von A gibt, welcher separabel über K ist.
Angenommen jedes $x \in A \setminus K$ ist rein inseparabel über K. Für alle $x \in A \setminus K$ ist dann $\mu_{x,K}(X) = X^{p^e} - a$ mit $a \in K$ und $e \in \mathbb{N}$. Wegen $p \mid [K(x) : K]$ und $[K(x) : K] \mid m$ gilt auch $p \mid m$.

Sei F ein maximaler Teilkörper von A und $\varphi\colon F \otimes_K A \xrightarrow{\sim} F^{r\times r}$ mit $r^2 = m$ wie in (a) bestimmt. Dann gilt $\varphi(1\otimes x)^{p^e} = \varphi(1\otimes x^{p^e}) = \varphi(1\otimes a) = a \cdot I_r$. Damit ist $\mathrm{Tr}(\varphi(1\otimes x)) = a \cdot r = 0$, weil die Charakteristik p ein Teiler von m und somit auch von r ist. Die Menge $\{1\otimes x \mid x \in A\}$ erzeugt jedoch die F-Algebra $F\otimes_K A$ über F. Daher erzeugen ihre Bilder den Matrizenring $F^{r\times r}$. Damit hätte jede $r\times r$-Matrix über F Spur Null. Dies kann nicht sein.
Also existiert ein $x \in A \setminus K$, welches nicht rein inseparabel ist über K. Dann ist $\mu_{x,K}(X) = f(X^{p^e})$ für ein $e \in \mathbb{N}$ und ein separables Polynom $f \in K[X]$. Wählen wir $E := K(x^{p^e})$, so ist E/K eine nicht triviale separable Körpererweiterung.

Bezeichne nun $A' = C_A(E)$ den Zentralisator von E in A. Nach Satz 2.1.11 ist A' einfach und es gilt $E = C_A(A') \supseteq Z(A')$. Also ist $Z(A') = E$ und daher ist A' eine zentraleinfache E-Algebra mit $[A' : E] < m$. Nach der Induktionsvoraussetzung besitzt A' einen maximalen Teilkörper L, der separabel ist über E. Damit ist auch L/K separabel.
Ist nun $x \in A$ derart, daß $L(x)$ ein Teilkörper von A ist, so vertauscht x mit allen Elementen von L. Damit zentralisiert x aber auch E und deswegen ist $x \in C_A(E) = A'$. Es folgt $L(x) = L$, da L ein maximaler Teilkörper von A' ist. Also ist L auch ein maximaler Teilkörper von A. □

Ist A eine zentraleinfache K-Algebra, so induziert jedes Element $a \in A^*$ via $x \mapsto axa^{-1}$ einen (inneren) K-Automorphismus auf A. Der folgende Satz liefert als Spezialfall die Umkehrung dieser Aussage.

Satz 2.1.15 (Skolem-Noether) *Seien A eine zentraleinfache K-Algebra und B, B' zwei einfache Teilalgebren von A mit $K \subseteq B, B' \subseteq A$. Dann läßt sich jeder K-Isomorphismus $\sigma\colon B \hookrightarrow B'$ fortsetzen zu einem inneren Automorphismus auf A. Das heißt es existiert ein $a \in A^*$ mit $\sigma(b) = a^{-1}ba$ für alle $b \in B$.*

Beweis: Sei V ein einfacher A-Rechtsmodul und $D^o \cong \mathrm{End}_A(V)$. Nach Lemma 2.1.8 ist $D^o \otimes_K B$ eine einfache K-Algebra. V läßt sich nun auf zwei verschiedene Arten als ein $D^o \otimes_K B$-Rechtsmodul auffassen:
V_1 via $x *_1 (d\otimes b) = d(x)b$ und V_2 via $x *_2 (d\otimes b) = d(x)\sigma(b)$. Da beide dieselbe K-Dimension besitzen, sind sie isomorph als $D^o \otimes_K B$-Rechtsmoduln. Also existiert ein $\varphi \in \mathrm{Aut}_K(V)$ mit $\varphi(d(x)b) = \varphi(x *_1 (d\otimes b)) = \varphi(x) *_2 (d\otimes b) = d(\varphi(x))\sigma(b)$ für alle $x \in V$. Speziell folgt für $b = 1$, daß $\varphi \in \mathrm{End}_{D^o}(V) \cong A$. Damit ist φ durch Rechtsmultiplikation mit einem Element $a \in A^*$ gegeben. Mit $d = 1$ gilt:

$$(xb)a = \varphi(xb) = \varphi(x)\sigma(b) = xa\sigma(b) \quad \text{für alle } x \in V_1,\ b \in B.$$

Nach Lemma 2.1.7 ist V treu. Also gilt $a^{-1}ba = \sigma(b)$ für alle $b \in B$. □

Korollar 2.1.16 *In einer zentraleinfachen K-Algebra ist jeder K-Automorphismus inner.*

Korollar 2.1.17 *Jeder endliche Schiefkörper ist ein Körper.*

Beweis: Sei D ein endlicher Schiefkörper mit Zentrum K und L ein maximaler Teilkörper. Jeder maximale Teilkörper hat $\sqrt{[D:K]} \cdot |K|$ Elemente. Diese sind daher alle K-isomorph zu L und nach dem Satz von Skolem-Noether konjugiert. Also ist $D^* = \bigcup_{d \in D^*} dL^*d^{-1}$. Da es genügt, nur über ein Vertretersystem von Rechtsnebenklassen von L^* in D^* zu laufen und die 1 in allen Mengen dL^*d^{-1} auftaucht, gilt $|D^*| = 1 + \frac{|D^*|}{|L^*|} \cdot (|L^*| - 1)$. Dies zeigt $L^* = D^*$. □

2.2 Spur und Norm

Definition 2.2.1 Es seien K ein Körper, A eine endlich dimensionale K-Algebra und $\underline{x} = (x_1, \ldots, x_n)$ eine K-Basis von A.

(a) Ist $M \in K^{n \times n}$ eine Matrix, so bezeichne $\chi_M(X) := \det(X \cdot I_n - M)$ das *charakteristische Polynom* von M.

(b) Für ein $\varphi \in \mathrm{End}_K(A)$ existieren $\lambda_{ij} \in K$, so daß $\varphi(x_i) = \sum_{j=1}^n \lambda_{ij} x_j$ gilt. Dann heißt $M(\varphi)_{\underline{x}} := (\lambda_{ij})_{ij}$ die *darstellende Matrix* von φ bezüglich $\underline{x}$ und $\chi_\varphi(X) := \chi_{M(\varphi)_{\underline{x}}}(X)$ das *charakteristische Polynom* von φ.

(c) Für ein a in A bezeichne r_a wieder die Rechtsmultiplikation mit a. Wegen $r_a \in \mathrm{End}_K(A)$ können wir weiter definieren:

- $\chi_{a,A/K}(X) := \chi_{r_a}(X)$ das *charakteristische Polynom* von a,
- $\mathrm{Tr}_{A/K}(a) := \mathrm{Spur}(M(r_a)_{\underline{x}})$ die *Spur* von a und
- $\mathrm{Nr}_{A/K}(a) := \det(M(r_a)_{\underline{x}})$ die *Norm* von a.

Bemerkung 2.2.2 Es gelten die obigen Bezeichnungen.

(a) In der Linearen Algebra zeigt man die Identität

$$\chi_{a,A/K}(X) = X^n - \mathrm{Tr}_{A/K}(a) + \cdots + (-1)^n \mathrm{Nr}_{A/K}(a).$$

Weil $\chi_\varphi(X)$ unabhängig von der Wahl der Basis $\underline{x}$ ist, sind alle Begriffe in Definition 2.2.1 wohldefiniert.

(b) Die Abbildung $A \to \mathrm{End}_K(A)$, $a \mapsto r_a$ ist K-linear und erfüllt $r_{aa'} = r_{a'} \circ r_a$. Es gelten daher

$$\mathrm{Tr}_{A/K}(\lambda a + \lambda' a') = \lambda \,\mathrm{Tr}_{A/K}(a) + \lambda \,\mathrm{Tr}_{A/K}(a') \qquad \mathrm{Tr}_{A/K}(aa') = \mathrm{Tr}_{A/K}(a'a)$$
$$\mathrm{Nr}_{A/K}(aa') = \mathrm{Nr}_{A/K}(a)\,\mathrm{Nr}_{A/K}(a') \qquad \mathrm{Nr}_{A/K}(\lambda a) = \lambda^n \,\mathrm{Nr}_{A/K}(a)$$

für alle $a, a' \in A$ und $\lambda \in K$.

Insbesondere liefert $A \times A \to K,\ (x, y) \mapsto \mathrm{Tr}_{A/K}(xy)$ auf A eine symmetrische K-Bilinearform.

Definition 2.2.1 macht keinen Gebrauch von der speziellen Struktur der Algebra A. Wir werden in Satz 2.2.5 sehen, daß wenn die Charakteristik des Körpers $\dim_K(A)$ teilt, dann ist die Bilinearform $(x, y) \mapsto \mathrm{Tr}_{A/K}(xy)$ die Nullabbildung.

In einer zentraleinfachen Algebra lassen sich wesentlich brauchbarere Begriffe einführen, die insbesondere eine nicht ausgeartete Bilinearform induzieren. Dies wollen wir nun tun.

Satz 2.2.3 *Es sei A eine zentraleinfache K-Algebra und E ein Zerfällungskörper von A. Weiter sei $h\colon E \otimes_K A \xrightarrow{\sim} E^{n\times n}$ ein E-Algebrenisomorphismus. Dann ist $\chi_{h(1\otimes a)}(X) \in K[X]$ für alle $a \in A$ und unabhängig von der Wahl von h und E.*

Beweis: Zuerst zeigen wir, daß die Wahl des Isomorphismus h nicht entscheidend ist. Denn ist ein weiterer solcher Isomorphismus h' gegeben, so ist $h' \circ h^{-1}$ nach dem Satz von Skolem-Noether einen innerer E-Automorphismus auf $E^{n\times n}$. Also existiert $S \in \mathrm{GL}_n(E)$ mit $h'(x) = Sh(x)S^{-1}$ für alle $x \in E \otimes_K A$. Damit haben die Matritzen $h'(x)$ und $h(x)$ stets dasselbe charakteristische Polynom.

Nun haben wir zu zeigen, daß die Definition unabhängig von der Wahl des Zerfällungskörpers E ist. Sei dazu E' ein weiterer solcher. Dann ist $B = E \otimes_K E'$ eine endlich erzeugte kommutative K-Algebra. Bezeichne M darin ein maximales Ideal, so ist $\Omega := B/M$ ein Körper, der K enthält. Weil E einfach ist, ist $E \overset{\mathrm{id}_E \otimes 1}{\hookrightarrow} E \otimes E' \twoheadrightarrow \Omega$ eine K-lineare Einbettung $E \hookrightarrow \Omega$. Analog bekommt man eine K-lineare Einbettung $E' \hookrightarrow \Omega$.
Weiter gilt nun $\Omega \otimes_K A \cong \Omega \otimes_E (E \otimes_K A) \cong \Omega \otimes_K E^{n\times n} \cong \Omega^{n\times n}$. Also zerfällt auch Ω die K-Algebra A. Der letzte Isomorphismus faßt eine Matrix $h(x) \in E^{n\times n}$ als eine Matrix über Ω auf. Dadurch ändert sich ihr charakteristische Polynom jedoch nicht. Damit ist $\chi_E(h(1 \otimes_K a))$ unabhängig von der Wahl von E.

Es verbleibt noch zu zeigen, daß $\chi_E(h(1 \otimes_K a)) \in K[X]$ liegt. Nach Satz 2.1.14 dürfen wir insbesondere annehmen, daß E/K separabel ist. Die normale Hülle von E zerfällt dann ebenfalls A. Somit können wir ohne Einschränkung E/K als endlich und galoisch voraussetzen.
Für ein $\sigma \in \mathrm{Gal}(E/K)$ sei $\sigma^*\colon E^{n\times n} \xrightarrow{\sim} E^{n\times n},\ (e_{ij}) \mapsto (\sigma(e_{ij}))$. Dann gibt es genau einen E-Algebrenisomorphismus h', der das folgende Diagramm kommutieren läßt:

$$\begin{array}{ccc} E \otimes_K A & \xrightarrow{\sim\ \sigma \otimes \mathrm{id}_A} & E \otimes_K A \\ \downarrow{\scriptstyle h} & & \downarrow{\scriptstyle h'} \\ E^{n\times n} & \xrightarrow[\sim]{\quad\sigma^*\quad} & E^{n\times n} \end{array}$$

Insbesondere gilt dann $\sigma^*(h(1 \otimes a)) = h'((\sigma \otimes \mathrm{id}_A)(1 \otimes a)) = h'(1 \otimes a)$. Mit der Funktion $\tilde{\sigma}\colon E[X] \to E[X],\ \sum_{k=0}^m e_k X^k \mapsto \sum_{k=0}^m \sigma(e_k)X^k$ und dem schon gezeigten folgt nun $\chi_{h(1\otimes a)}(X) = \chi_{h'(1\otimes a)}(X) = \chi_{(\sigma^* \circ h)(1\otimes a)}(X) = \tilde{\sigma}(\chi_{h(1\otimes a)}(X))$. Also fixiert jedes $\sigma \in \mathrm{Gal}(E/K)$ die Koeffizienten von $\chi_{h(1\otimes a)}(X)$. □

Definition 2.2.4 Es sei A eine zentraleinfache K-Algebra und E ein Zerfällungskörper von A. Weiter sei $h\colon E \otimes_K A \xrightarrow{\sim} E^{n\times n}$ ein E-Algebrenisomorphismus. Für ein $a \in A$ bezeichnen

$$\begin{aligned} \mathrm{tr}_{A/K}(a) &:= \text{Spur von } h(1\otimes a) \\ \mathrm{nr}_{A/K}(a) &:= \det(h(1\otimes a)) \end{aligned}$$

die *reduzierte Spur* und die *reduzierte Norm* von a.

Es ist $\chi_{h(1\otimes a)}(X) = X^n - \mathrm{tr}_{A/K}(a)X^{n-1} + \cdots + (-1)^n \mathrm{nr}_{A/K}(a)$. Nach Satz 2.2.3 sind „$\mathrm{tr}_{A/K}$“ und „$\mathrm{nr}_{A/K}$“ unabhänging von h und E.

Satz 2.2.5 *Es sei A eine zentraleinfache K-Algebra mit $m^2 = [A : K]$. Dann gilt*

$$\begin{aligned} \mathrm{Tr}_{A/K}(a) &= m \cdot \mathrm{tr}_{A/K}(a) \\ \mathrm{Nr}_{A/K}(a) &= \mathrm{nr}_{A/K}(a)^m. \end{aligned}$$

Beweis: Es sei E ein Zerfällungskörper von A und $a \in A$. Weiter sei $(x_1, \ldots, x_m)$ eine E-Basis eines einfachen $E\otimes_K A$-Rechtsmoduls V. Dann liefert $x_i \cdot (e\otimes a) = \sum_j e_{ij}x_j$ einen E-Algebrenisomorphismus $h\colon E\otimes_K A \to E^{m\times m}$.
Es gilt $E\otimes_K A \cong V^m$ als $E\otimes_K A$-Rechtsmoduln. Damit können wir $h(1\otimes a)$ als eine Blockmatrix annehmen, in der jeder der m Blöcke die Rechtsmultiplikation von $1\otimes a$ auf V beschreibt. Somit ergibt sich $\chi_{1\otimes a,(E\otimes A)/E}(X) = \chi_{h(1\otimes a)}(X)^m$.
Da die Matrixdarstellung von r_a unter der Skalarerweiterung von K nach E invariant bleibt, folgt $\chi_{a,A/K}(X) = \chi_{1\otimes a,(E\otimes A)/E}(X)$. Damit gilt $(\chi_{h(1\otimes a)}(X))^m = \chi_{a,A/K}(X)$.□

Korollar 2.2.6 *Sei A eine zentraleinfache K-Algebra mit $m^2 = [A : K]$. Für alle a, $a' \in A$ und $\lambda \in K$ gelten*

$$\begin{aligned} \mathrm{nr}_{A/K}(aa') &= \mathrm{nr}_{A/K}(a)\,\mathrm{nr}_{A/K}(a') & \qquad \mathrm{nr}_{A/K}(\lambda a) &= \lambda^m \mathrm{nr}_{A/K}(a) \\ \mathrm{tr}_{A/K}(a+a') &= \mathrm{tr}_{A/K}(a) + \mathrm{tr}_{A/K}(a') & \qquad \mathrm{tr}_{A/K}(\lambda a) &= \lambda \cdot \mathrm{tr}_{A/K}(a) \\ \mathrm{tr}_{A/K}(aa') &= \mathrm{tr}_{A/K}(a'a) \end{aligned}$$

Außerdem ist $\tau\colon A\times A \to K$, $(x, y) \mapsto \mathrm{tr}_{A/K}(xy)$ eine nicht ausgeartete symmetrische K-Bilinearform.

Beweis: Die Identitäten für die reduzierte Spur bzw. Norm folgen aus dem vorherigen Lemma und den analogen Identitäten für $\mathrm{Tr}_{A/K}$ und $\mathrm{Nr}_{A/K}$.

Damit ist auch klar, daß τ bilinear und symmetrisch ist. Es sei E ein Zerfällungskörper von A. Die E-Bilinearform $\tau'\colon (E\otimes_K A)\times(E\otimes_K A) \longrightarrow E$, $(xy) \mapsto \mathrm{Tr}_{(E\otimes A)/E}(xy)$ ist dann eine Fortsetzung von τ. Identifizieren wir $E\otimes_K A$ mit $E^{m\times m}$, dann ist τ' die gewöhnliche Spur auf $E^{m\times m}$. Betrachten wir die Menge

$$I = \{X \in E^{m\times m} \mid \mathrm{Spur}(XY) = 0 \text{ für alle } Y \in E^{m\times m}\}.$$

I ist sicher ein Ideal in $E^{m\times m}$. Da aber z.B. die Einheitsmatrix nicht darin liegen kann und $E^{m\times m}$ einfach ist, muß $I = 0$ sein. Also ist τ' nicht ausgeartet. Angenommen, es wäre $\tau(a, b) = 0$ für alle $b \in A$, dann gilt auch $\tau'(1\otimes a, 1\otimes b) = 0$ für alle $b \in A$. Weil τ' E-bilinear ist, folgt $\tau'(1\otimes a, y) = 0$ für jedes $y \in E\otimes_K A$. Also ist $a = 0$. □

Korollar 2.2.7 *Ist F/K eine Körpererweiterung, so sind $\mathrm{nr}_{(F\otimes_K A)/F}$ und $\mathrm{tr}_{(F\otimes_K A)/F}$ Fortsetzungen von $\mathrm{nr}_{A/K}$ bzw. $\mathrm{tr}_{A/K}$.*

Beweis: Das charakteristische Polynom eines $x \in A$ bleibt invariant unter der Skalarerweiterung von F nach K. Damit gilt die Aussage für die gewöhnliche Spur bzw. Norm. Wegen $\dim_F(F \otimes_K A) = \dim_K(A)$ folgt die Behauptung. □

Definition 2.2.8 Ist F ein Teilkörper von K so, daß K/F eine separable Erweiterung ist, dann definieren wir auch bezüglich F eine reduzierte Spur und eine reduzierte Norm via

$$\mathrm{tr}_{A/F}(x) := \mathrm{Tr}_{K/F}(\mathrm{tr}_{A/K}(x)) \quad \text{und} \quad \mathrm{nr}_{A/F}(x) := \mathrm{Nr}_{K/F}(\mathrm{nr}_{A/K}(x)).$$

Die durch $\mathrm{tr}_{A/F}$ induzierte Bilinearform $\tau_{A/F}\colon A \times A \to K$, $(x, y) \mapsto \mathrm{tr}_{A/F}(xy)$ ist nicht ausgeartet, da τ nicht ausgeartet und K/F separabel ist.

Satz 2.2.9 *Es sei D ein Schiefkörper mit Zentrum K und $A = D^{m\times m}$. Für jedes $a = (a_{ij}) \in A$ gilt dann $\mathrm{tr}_{A/K}(a) = \sum_{i=1}^{m} \mathrm{tr}_{D/K}(a_{ii})$.*

Beweis: Sei E ein Zerfällungskörper von D und $h\colon D \xrightarrow{\simeq} E^{r\times r} \cong E \otimes_K D$. Dann ist auch $h'\colon A \to E^{mr\times mr} \cong E \otimes_K A$, $a = (a_{ij}) \mapsto (h(a_{ij}))$ ein Isomorphismus von E-Algebren. Damit folgt

$$\mathrm{tr}_{A/K}(a) = \mathrm{Spur}(h'(a)) = \sum_{i=1}^{m} \mathrm{Spur}(h(a_{ii})) = \sum_{i=1}^{m} \mathrm{tr}_{D/K}(a_{ii})\,.$$

□

2.3 Jacobson-Radikal und der Satz von Krull-Schmidt

Es sei S ein Ring.

Bemerkung 2.3.1 Für jedes $s \in S$ sind folgende Aussagen äquivalent:

(a) s liegt in jedem maximalen Rechtsideal von S.

(b) $Ms = 0$ für jeden einfachen S-Rechtsmodul M.

(c) Für alle $y \in S$ besitzt $1 - sy$ ein Rechtsinverses.

(d) Für alle $x, y \in S$ ist $1 - xsy \in S^*$.

(a')-(c') die entsprechenden Aussagen für „links“ anstatt „rechts“.

Beweis:
$(a) \Longrightarrow (c)$ Besitzt $1 - sy$ kein Rechtsinverses, so liegt $1 - sy$ in einem maximalen Rechtsideal $\mathfrak{m}$ von S. Damit ist $1 = (1 - sy) + sy \in \mathfrak{m}$ ein Widerspruch.

$(c) \Longrightarrow (b)$ Sei $ms \neq 0$ für ein $m \in M$ angenommen. Dann gilt $msS = M$. Also gibt es ein $y \in S$ mit $m = msy$ bzw. $m(1 - sy) = 0$. Da $1 - sy$ ein Rechtsinverses besitzt, folgt $m = 0$ und wir erhalten einen Widerspruch.

$(b) \Longrightarrow (a)$ Sei $\mathfrak{m}$ ein maximales Rechtsideal von S. Dann ist $(S/\mathfrak{m}) \cdot s = 0$, also $s \in \mathfrak{m}$.

$(b) \Longrightarrow (d)$ Es gilt $Mxsy \subseteq Msy = 0$ für alle einfachen Rechtsmoduln M. Mit der schon gezeigten Implikation $(b) \Longrightarrow (c)$ folgt, daß $1 - xsy$ ein Rechtsinverses $t \in S$ besitzt. Wegen $M(-x)syt = 0$ für jeden einfachen Rechtsmodul M ist auch $t = 1 + xsyt$ invertierbar von rechts. Also ist $t \in S^*$, und damit auch $1 - xsy \in S^*$.
Die Implikation $(d) \Longrightarrow (c)$ ist trivial. Aus der Symmetrie von Aussage (d) folgt die Äquivalenz mit $(a'), (b')$ und (c'). □

Definition 2.3.2 Das *Jacobson-Radikal* $\mathrm{rad}(S)$ eines Rings S ist die Menge aller $s \in S$, die die äquivalenten Bedingungen der vorherigen Bemerkung erfüllen. Insbesondere ist $\mathrm{rad}(S)$ ein zweiseitiges Ideal. Wir sagen, S ist *halbeinfach* (im Sinne von Jacobson), falls $\mathrm{rad}(S) = 0$ gilt.

Das Jacobson Radikal $\mathrm{rad}(S)$ ist somit der Schnitt aller maximalen Rechtsideale von S und auch der Schnitt aller maximalen Linksideale von S.

Lemma 2.3.3 *Für jeden Ring S ist $S/\mathrm{rad}(S)$ halbeinfach.*

Beweis: Es sei $\overline{S} := S/\mathrm{rad}(S)$ und $s \in S$ mit $s + \mathrm{rad}(S) \in \mathrm{rad}(\overline{S})$. Für jeden einfachen S-Rechtsmodul M gilt $M\mathrm{rad}(S) = 0$. Daher können wir M als einen einfachen $\overline{S}$-Rechtsmodul auffassen, und es gilt $M(s + \mathrm{rad}(S)) = Ms = 0$. Da dies für jeden einfachen S-Rechtsmodul M gilt, ist $s \in \mathrm{rad}(S)$ und damit $\mathrm{rad}(\overline{S}) = 0$. □

Lemma 2.3.4 (Nakayama) *Es sei M ein endlich erzeugter S-Rechtsmodul und N ein Teilmodul von M.*

(a) Gilt $M\,\mathrm{rad}(S) = M$, so ist $M = 0$.

(b) Gilt $N + M\,\mathrm{rad}(S) = M$, so ist $N = M$.

Beweis: Zu (a): Sei $M \neq 0$ angenommen und $m_1, \ldots, m_r$ ein S-Erzeugendensystem von M mit minimalem r. Da $m_1 \in M\,\mathrm{rad}(S)$ liegt, gibt es $s_i \in \mathrm{rad}(S)$ mit $m_1 = \sum_{k=1}^{r} m_k s_k$. Wegen $1 - s_1 \in S^*$ läßt sich m_1 darstellen als S-Linearkombination von $m_2, \ldots, m_r$. Also war r nicht minimal und wir erhalten einen Widerspruch. Teil (b) folgt, indem man (a) auf M/N anwendet. □

Lemma 2.3.5 *Ist $\mathfrak{a}$ ein maximales zweiseitiges Ideal von S, so gilt $\mathrm{rad}(S) \subseteq \mathfrak{a}$.*

Beweis: Läge $\mathrm{rad}(S)$ nicht in $\mathfrak{a}$, so wäre $\mathfrak{a} + \mathrm{rad}(S) = S$ und letztlich $\mathfrak{a} = S$ mit Nakayamas Lemma, was einen Widerspruch darstellt. □

Bemerkung 2.3.6 Folgende Aussagen sind äquivalent:

(a) S besitzt genau ein maximales Rechtsideal.

(b) S besitzt genau ein maximales Linksideal.

(c) $S \setminus S^*$ ist ein zweiseitiges Ideal von S.

Beweis:
$(a) \Longrightarrow (c)$ Da $\mathrm{rad}(S)$ als Schnitt aller maximalen Rechtsideale das einzige maximale Rechtsideal ist, ist $\mathrm{rad}(S) = S \setminus S^*$ ein zweiseitiges Ideal.

$(c) \Longrightarrow (a)$ Sei $\mathfrak{m}$ ein maximales Rechtsideal von S. Sicher gilt $\mathrm{rad}(S) \subseteq \mathfrak{m}$. Ist umgekehrt $s \in \mathfrak{m}$, so gilt $sy \in S \setminus S^*$ für alle $y \in S$. Damit ist $1 - sy$ für alle $y \in S$ eine Einheit. Also ist $s \in \mathrm{rad}(S)$. Daher gilt $\mathfrak{m} \subseteq \mathrm{rad}(S)$. Jedes maximale Rechtsideal ist also mit $\mathrm{rad}(S)$ identisch.

Der Beweis von $(b) \iff (c)$ geht analog. □

Definition 2.3.7 Ein Ring S heißt *lokal*, falls er die äquivalenten Aussagen der vorherigen Bemerkung erfüllt.

Insbesondere zeigt der Beweis der Bemerkung, daß für einen lokalen Ring S gilt:
$S \setminus S^* = \mathrm{rad}(S)$ ist das maximale Rechtsideal von S und auch das maximale Links- bzw. beidseitige Ideal.

Lemma 2.3.8 *Sei $f\colon S \to S'$ ein surjektiver Ringmorphismus.*
Dann gilt $f(\mathrm{rad}(S)) \subseteq \mathrm{rad}(S')$. Insbesondere induziert f einen surjektiven Ringmorphismus $S/\mathrm{rad}(S) \to S'/\mathrm{rad}(S')$.

Beweis: Es sei $x \in \mathrm{rad}(S)$. Weiter seien $r', s' \in S'$. Dann existieren $r, s \in S$ mit $f(r) = r'$ und $f(s) = s'$. Wegen $1 - rxs \in S^*$ ist $1 - r'f(x)s' \in S'^*$ und letztlich $f(x) \in \mathrm{rad}(S')$. □

Korollar 2.3.9 *Sei R ein kommutativer lokaler Ring mit maximalem Ideal $\mathfrak{p} = \mathrm{rad}(R)$. Weiter sei A eine R-Algebra, welche als R-Modul endlich erzeugt ist. Mit $\overline{A} := A/\mathfrak{p}A$ gilt*

$$A/\mathrm{rad}(A) \cong \overline{A}/\mathrm{rad}(\overline{A})\,.$$

Beweis: Es sei M ein einfacher A-Rechtsmodul. Dieser ist endlich erzeugt über R. Nach dem Lemma von Nakayama ist $M\mathfrak{p} \neq M$. Also ist $M\mathfrak{p} = 0$, und M wird somit von $A\mathfrak{p}$ annulliert. Dies zeigt $A\mathfrak{p} \subseteq \mathrm{rad}(A)$. Daher existiert ein surjektiver Ringmorphismus $f\colon \overline{A} \to A/\mathrm{rad}(A)$. Nach dem vorherigen Lemma ist dann $f(\mathrm{rad}(\overline{A})) \subseteq \mathrm{rad}(A/\mathrm{rad}(A)) = 0$. D.h. f induziert einen surjektiven Ringmorphismus von $\overline{A}/\mathrm{rad}(\overline{A}) \to A/\mathrm{rad}(A)$. Der kanonische Epimorphismus $A \to \overline{A}$ induziert aber genauso einen surjektiven Ringmorphismus $A/\mathrm{rad}(A) \to \overline{A}/\mathrm{rad}(\overline{A})$, invers zum vorherigen. □

Bemerkung 2.3.10 Es sei S ein Ring.

(a) Ist $\mathfrak{a}$ ein Rechtsideal, welches nur aus nilpotenten Elementen besteht, so gilt $\mathfrak{a} \subseteq \mathrm{rad}(S)$.

(b) Sind alle Elemente in $S \setminus S^*$ nilpotent, so ist S lokal.

Beweis: Zu (a): Es sei $\mathfrak{a}$ ein Rechtsideal und $a \in \mathfrak{a}$. Für alle $x \in S$ ist $ax \in \mathfrak{a}$ ebenfalls nilpotent. Daher besitzt $1 - ax$ ein Rechtsinverses, nämlich die endliche Summe $1 + ax + (ax)^2 + \ldots$.
Zum Beweis von (b) sei $x \in S \setminus S^*$. Es gibt daher ein minimales $k > 0$ mit $x^k = 0$. Wegen $x^{k-1} \cdot (xs) = 0$ kann xs für kein $s \in S$ eine Einheit sein. Daher besteht $xS \subseteq S \setminus S^*$ nur aus nilpotenten Elementen. Dies zeigt mit (a), daß $x \in xS \subseteq \mathrm{rad}(S)$ und somit $S \setminus S^* = \mathrm{rad}(S)$ gilt. Also ist S lokal. □

Lemma 2.3.11 *Ist S rechts-artinsch, so ist* $\mathrm{rad}(S)$ *nilpotent und enthält seinerseits alle nilpotenten Rechtsideale von S.*

Beweis: Bezeichne $J := \mathrm{rad}(S)$. Dann existiert ein $k > 0$ mit $J^k = J^{k+1}$. Wäre $J^k \neq 0$, so existiert ein Ideal $\mathfrak{a}$ mit $\mathfrak{a} \cdot J^k \neq 0$. Sei $\mathfrak{a}$ minimal mit dieser Eigenschaft. Es gibt ein $a \in \mathfrak{a}$ mit $aJ^k \neq 0$. Also ist auch $(aJ^k) \cdot J^k = aJ^k \neq 0$. Wegen der Wahl von $\mathfrak{a}$ folgt $aJ^k = \mathfrak{a}$. Damit ist $a = ay$ für ein $y \in J^k \subseteq J$. Wegen $1 - y \in S^*$ folgt $a = 0$, was nicht sein kann. Also war $J^k = 0$. Ist $\mathfrak{b}$ ein nilpotentes Rechtsideal, so sind alle Elemente von $\mathfrak{b}$ nilpotent. Mit Bemerkung 2.3.10 folgt $\mathfrak{b} \subseteq J$. □

Als nächstes benötigen wir noch einige Aussagen über primitive Idempotente in rechts-artinschen Ringen.

Definition 2.3.12 Ein *Idempotent* von S ist ein Element $s \in S \setminus \{0\}$ mit $s^2 = s$. Ein System $\{e_1, \ldots, e_k\}$ von Idempotenten e_i heißt *orthogonal*, falls $e_i e_j = \delta_{ij} e_i$ für alle $1 \leq i, j \leq k$ gilt. Ein Idempotent e wird *primitiv* genannt, falls es keine orthogonale Zerlegung von $e = e_1 + e_2$ in Idempotente gibt.

Bemerkung 2.3.13 Bekanntlich korrespondieren die orthogonalen Zerlegungen von $1 \in S$ in primitive Idempotente $1 = e_1 + \cdots + e_k$ zu den Zerlegungen von S in projektive unzerlegbare Rechtsideale von S via $S = \bigoplus_{i=1}^{k} e_i S$.

Bemerkung 2.3.14 Ist S ein halbeinfacher rechts-artinscher Ring, so ist jedes minimale Rechtsideal ein direkter Summand von S. Damit ist ein Rechtsideal genau dann unzerlegbar, wenn es minimal ist. Außerdem ist S somit eine direkte Summe von minimalen Rechtsidealen.

Beweis: Sei $\mathfrak{a}$ ein minimales Rechtsideal. Wegen $\mathrm{rad}(S) = 0$ existiert ein maximales Rechtsideal $\mathfrak{m}$, welches $\mathfrak{a}$ nicht enthält. Folglich ist $\mathfrak{a} \cap \mathfrak{m} = 0$ und daher $\mathfrak{a} \oplus \mathfrak{m} = S$. □

Satz 2.3.15 *Es sei S ein rechts-artinscher Ring und $\overline{S} := S/\mathrm{rad}(S)$. Für jedes $s \in S$ bezeichne $\overline{s} = s + \mathrm{rad}(S)$. Dann gelten:*

(a) Jedes Idempotent $\epsilon \in \overline{S}$ läßt sich zu einem Idempotent $e \in S$ liften, d.h. $\overline{e} = \epsilon$.

(b) Ist $\overline{1} = \epsilon_1 + \cdots + \epsilon_l$ eine orthogonale Zerlegung von $\overline{1}$ in Idempotente, so existiert ein orthogonales System $\{e_1, \ldots, e_l\}$ von Idempotenten von S mit $1 = e_1 + \cdots + e_l$ und $\overline{e_k} = \epsilon_k$.

(c) Ein Idempotent $e \in S$ ist primitiv genau dann, wenn $\overline{e}$ primitiv in $\overline{S}$ ist.

(d) Ist $1 = e_1 + \cdots + e_l$ eine orthogonale Zerlegung der 1 in primitive Idempotente, so ist

$$\overline{S} = \overline{e}_1\,\overline{S} \oplus \cdots \oplus \overline{e}_l\,\overline{S}$$

eine Zerlegung von $\overline{S}$ in minimale Linksideale.
Ferner ist $e_iS \cong e_jS$ (als S-Rechtsmoduln) genau dann, wenn $\overline{e}_i\,\overline{S} \cong \overline{e}_j\,\overline{S}$ (als $\overline{S}$-Rechtsmoduln) gilt.

Beweis:

(a) Sei $x_1 \in S$ mit $\overline{x}_1 = \epsilon$. Dann ist $r_1 := x_1^2 - x_1 \in \mathrm{rad}(S)$. Wir setzen induktiv

$$x_{i+1} := x_i + r_i - 2x_ir_i \quad \text{und} \quad r_{i+1} := x_{i+1}^2 - x_{i+1}\,.$$

Setzen wir $r = r_1$ und $x = x_1$. Dann ist $r = x^2 - x$ und damit

$$r_2 = (x + r - 2xr)^2 - x - r + 2xr \equiv x^2 - 4(x - x^2)r - x - r \equiv 0 \mod \mathrm{rad}(S)^2\,.$$

Per Induktion folgt $r_i \in \mathrm{rad}(S)^{(2^{i-1})}$. Da $\mathrm{rad}(S)$ nilpotent ist, existiert ein k mit $r_k = 0$. Mit $e := x_k$ gilt dann $e^2 - e = r_k = 0$ und $\overline{e} = \overline{x}_k = \cdots = \overline{x}_1 = \epsilon$.

(b) Im Falle $l = 1$ ist nichts zu zeigen. Sei daher $l > 1$. Wir setzen $\delta := \epsilon_{l-1} + \epsilon_l$. Nach der Induktionsvoraussetzung existiert ein orthogonales System von Idempotenten mit

$$1 = e_1 + \cdots + e_{l-2} + e, \quad \overline{e} = \delta \quad \text{und} \quad \overline{e_i} = \epsilon_i \text{ für } i = 1, \ldots, l-2\,.$$

Sei weiter $a \in S$ mit $\overline{a} = \epsilon_{l-1}$ beliebig und $x_1 := eae$. Dann gilt $\overline{x}_1 = \delta\epsilon_{l-1}\delta = \epsilon_{l-1}$ und $e_ix_1 = 0 = x_1e_i$ für alle $1 \le i \le l-2$. Führen wir nun ausgehend von x_1 dieselbe Konstruktion wie in Teil (a) durch, so liefert dies ein Idempotent $e_{l-1} \in S$. Dieses ist dann ein Polynom in x_1 ohne konstanten Term. Setzen wir nun $e_l := e - e_{l-1}$, so gilt daher $ee_{l-1} = e_{l-1}$ und (wie man leicht nachrechnet) besitzt $(e_1, \ldots, e_l)$ die gewünschten Eigenschaften.

(c) folgt sofort aus (a) und (b).

(d) Wir haben schon bewiesen, daß $\overline{e}_k\,\overline{S}$ unzerlegbare Rechtsideale von $\overline{S}$ sind. Weil $\overline{S}$ halbeinfach ist, sind diese Rechtsideale nach Bemerkung 2.3.14 minimal.
Ist $\varphi\colon e_iS \xrightarrow{\sim} e_jS$ ein Isomorphismus von S-Moduln, so gilt $\varphi(e_i\mathrm{rad}(S)) \subseteq e_j\mathrm{rad}(S)$, d.h. φ induziert einen $\overline{S}$-Modulisomorphismus $\overline{e}_i\,\overline{S} \cong \overline{e}_j\,\overline{S}$.
Sei umgekehrt ein Isomorphismus $f \xrightarrow{\sim} \overline{e}_j\,\overline{S}$ von $\overline{S}$-Moduln gegeben. Da alle e_kS

direkte Summanden von S sind, sind sie projektiv, d.h. es existieren Liftungen α und β von f bzw. f^{-1} so, daß das folgende Diagramm kommutiert:

$$\begin{array}{ccccc} e_iS & \xrightarrow{\alpha} & e_jS & \xrightarrow{\beta} & e_iS \\ \downarrow & & \downarrow & & \downarrow \\ \overline{e}_i\overline{S} & \xrightarrow{f} & \overline{e}_j\overline{S} & \xrightarrow{f^{-1}} & \overline{e}_i\overline{S} \end{array}$$

Bezeichne nun $\gamma := 1 - \beta \circ \alpha$. Weil $\beta \circ \alpha$ eine Liftung von $f^{-1} \circ f$ ist, folgt $\gamma(e_iS) \subseteq e_i\mathrm{rad}(S)$. Damit ist $\gamma^i(e_iS) \subseteq \mathrm{rad}(S)^i$ für alle $i \geq 1$. Nun existiert ein k mit $\mathrm{rad}(S)^k = 0$. Damit ist $\gamma^k = 0$ und $\sum_{i=0}^{k-1} \gamma^i$ das Inverse von $1-\gamma$. Also ist $\beta \circ \alpha = 1 - \gamma \in \mathrm{Aut}_S(e_iS)$. Analog zeigt man $\alpha \circ \beta \in \mathrm{Aut}_S(e_jS)$ und letztlich $e_iS \cong e_jS$. □

Zum Abschluß dieses Abschnitts wollen wir den Satz von Krull-Schmidt beweisen.

Definition 2.3.16 Ein S-Modul M heißt *noethersch*, falls jede aufsteigende Kette von Teilmoduln von M stationär wird.

Lemma 2.3.17 *Es sei S ein rechts-artinscher Ring und M ein endlich erzeugter S-Rechtsmodul. Weiter sei $E := \mathrm{End}_S(M)$. Dann gelten:*

(a) M besitzt eine Kompositionsreihe, d.h. es gibt eine endliche Kette von Teilmoduln $M = M_0 \supsetneq M_1 \supsetneq \cdots \supsetneq M_n = 0$ mit M_i/M_{i+1} einfach.

(b) M ist noethersch.

(c) **(Fitting)** *Für jedes $f \in E$ gibt es ein $k \in \mathbb{N}$ so daß $M = \ker(f^k) \oplus f^k(M)$.*

(d) Ist M unzerlegbar, so ist E ist ein lokaler Ring.

Beweis:

(a) Bezeichne $J := \mathrm{rad}(S)$ und $\overline{S} := S/J$. Weiter sei $M_i = MJ^i$. Da S rechts-artinsch ist, gibt es ein $n \in \mathbb{N}$ mit $J^n = 0$. Damit ist auch $M_n = 0$. Also genügt es zu zeigen, daß jeder Quotient M_i/M_{i+1} eine Kompositionsreihe besitzt. $\overline{S}$ ist ein halbeinfacher rechts-artinscher Ring und damit eine endliche direkte Summe von einfachen Rechtsidealen. Damit besitzt auch $\overline{S}^m$ für alle $m \in \mathbb{N}$ eine Kompositionsreihe. Die Quotienten M_i/M_{i+1} sind Faktormoduln von Kopien von $\overline{S}$, also besitzen diese ebenso eine Kompositionsreihe.

(b) Es bezeichne $\pi\colon M \to M/M_1$ die kanonische Projektion. Zunächst zeigen wir, daß je zwei Teilmoduln $B \subseteq A$ von M mit $A \cap M_1 = B \cap M_1$ und $\pi(A) = \pi(B)$ gleich sind. Sei dazu $a \in A$. Dann ist $\pi(a) = \pi(b)$ für ein $b \in B$. Also gilt $a - b \in \ker(\pi) = M_1$. Damit ist $a - b \in M_1 \cap A = M_1 \cap B$ und letztlich $a \in B$. Nun zeigen wir, daß M noethersch ist. Dazu führen wir eine Induktion nach der Länge n der Kompositionsreihe. Sei (N_i) eine beliebige aufsteigende Kette von Teilmoduln von M. Da M/M_1 eine Kompositionsreihe der Länge $n-1$ hat, gibt es ein $k \in \mathbb{N}$ mit $\pi(N_k) = \pi(N_l)$ und $N_k \cap M_1 = N_l \cap M_1$ für alle $l \geq k$. Nach dem gerade gezeigten folgt dann $N_k = N_l$ für alle $l \geq k$. Also ist M noethersch.

(c) Da M artinsch und noethersch ist, müssen die Ketten

$$\begin{aligned} M \supseteq f(M) \supseteq & f^2(M) \supseteq \dots \\ 0 \subseteq \ker(f) \subseteq & \ker(f^2) \subseteq \dots \end{aligned}$$

stabilisieren. Also existiert ein k mit $f^{k+i}(M) = f^k(M)$ und $\ker(f^{k+i}) = \ker(f^k)$ für alle $i \in \mathbb{N}$. Sei nun $x \in \ker(f^k) \cap f^k(M)$, d.h. es gibt ein $y \in M$ mit $x = f^k(y)$. Wegen $0 = f^k(x) = f^{2k}(y)$ ist $y \in \ker(f^{2k}) = \ker(f^k)$ und daher $x = f^k(y) = 0$. Ist $m \in M$ beliebig, so gibt es ein $m' \in M$ mit $f^k(m) = f^{2k}(m')$. Also ist $f^k(m - f^k(m')) = 0$. Das zeigt $m = (m - f^k(m')) + f^k(m') \in \ker(f^k) + f^k(M)$.

(d) Sei k wie oben bestimmt. Ist $f^k(M) = M$, so ist $\ker(f^k) = 0$, also $\ker(f) = 0$ und f ist ein Automorphismus. Andernfalls ist $f^k(M) = 0$. Alle Elemente in $E \setminus E^*$ sind daher nilpotent. Nach Teil (b) von Bemerkung 2.3.10 ist E lokal. □

Satz 2.3.18 (Krull-Schmidt) *Sei S ein rechts-artinscher Ring und M ein endlich erzeugter S-Rechtsmodul. Sind weiter*

$$M = \bigoplus_{i=1}^{l} M_i = \bigoplus_{j=1}^{k} N_i$$

zwei Zerlegungen von M in unzerlegbare S-Moduln, so gilt $l = k$ und nach geeigneter Umnummerierung $M_i \cong N_i$ für alle i.

Beweis: Ist $l = 1$, so ist nichts zu zeigen. Sei daher $l > 1$. Bezeichne $\alpha_i \colon M \to M_i$ und $\beta_j \colon M \to N_j$ die kanonischen Projektionen von M auf M_i bzw. N_j. Fassen wir diese als Elemente von $\mathrm{End}_S(M)$ auf, so gilt $1 = \beta_1 + \dots + \beta_k$ und daher $\alpha_1 = \alpha_1 \circ \beta_1 + \dots + \alpha_1 \circ \beta_k$. Die Einschränkung auf M_1 liefert $1_{M_1} = \sum_{j=1}^{k} \alpha_1 \circ \beta_j|_{M_1} \in E := \mathrm{End}_S(M_1)$. Da E lokal ist, können nicht alle Summanden im maximalen Ideal von E liegen. Also dürfen wir annehmen, daß z.B. $\alpha_1 \circ \beta_1|_{M_1}$ ein Automorphismus auf M_1 ist. Daher spaltet der Monomorphismus $\beta_1|_{M_1} \colon M_1 \to N_1$ auf. Weil N_1 unzerlegbar ist, ist $\beta_1|_{M_1}$ ein Isomorphismus.
Sicherlich ist $M_1 \cap \ker(\beta_1) = 0$. Ist $a \in N_1$, so gibt es ein $b \in M_1$ mit $a = \beta_1(b)$. Dann ist $\beta_1(a - b) = a - \beta_1(b) = 0$. Damit ist $a = b + (a - b) \in M_1 \oplus \ker(\beta_1)$, was $N_1 \subseteq M_1 \oplus \ker(\beta_1)$ beweist. Wir haben also

$$M = M_1 \oplus \ker(\beta_1) = M_1 \oplus N_2 \oplus \dots \oplus N_k$$

gezeigt. Nun können wir die Induktionshypothese auf

$$N_2 \oplus \dots \oplus N_k \cong M/M_1 \cong M_2 \oplus \dots \oplus M_l$$

anwenden. □

2.4 Stellen und Verzweigung

Wir wollen zunächst ein paar bekannte Tatsachen über Betragsabbildungen erwähnen und verzichten auf die Beweise. Sie finden sich bei [Rei03], [Neu92] und [FT91].

Definition 2.4.1 Es sei K ein Körper. Ein *Absolutbetrag auf* K ist eine Abbildung $|\,.\,|\colon K \to \mathbb{R}_{\geq 0}$ mit

(a) $|x| = 0 \iff x = 0$

(b) $|xy| = |x||y|$

(c) $|x + y| \leq |x| + |y|$

(d) Es gibt ein $x \in K^*$ mit $|x| \neq 1$.

Erfüllt ein Absolutbetrag anstatt (c) die stärkere Bedingung $|x+y| \leq \max(|x|, |y|)$ für alle $x, y \in K$, so heißt $|\,.\,|$ *nicht-archimedisch*, andernfalls *archimedisch*.

Zwei Absolutbeträge $|\,.\,|_1$ und $|\,.\,|_2$ heißen äquivalent, falls für alle $x \in K$ gilt

$$|x|_1 \leq 1 \iff |x|_2 \leq 1\,.$$

Wir bezeichnen mit $\hat{K}_{|.|}$ die *Vervollständigung* von K bezüglich $|\,.\,|$.

Definition 2.4.2 Es sei D ein Schiefkörper. Eine *diskrete Bewertung auf* D ist eine Abbildung $v\colon D \to \mathbb{Z} \cup \{\infty\}$ mit den folgenden Eigenschaften:

(a) $v(x) = \infty \iff x = 0$

(b) $v(xy) = v(x) + v(y)$ für alle $x, y \in D$

(c) $v(x + y) \geq \min(v(x), v(y))$ für alle $x, y \in D$

(d) $v(D^*) \neq \{0\}$.

Es bildet $\{x \in D \mid v(x) \geq 0\}$ einen Teilring von D, den sogenannten *Bewertungsring* von v.
Weiter ist $K \to \mathbb{R},\ x \mapsto \exp(-v(x))$ ein nicht-archimedischer Absolutbetrag.

Definition 2.4.3 Es sei R ein Integritätsbereich. Falls es eine diskrete Bewertung v auf $\mathrm{Quot}(R)$ gibt so, daß R der Bewertungsring von v ist, dann heißt R *diskreter Bewertungsring*.

Ist $\mathfrak{p}$ ein Primideal von R, so bezeichnet $R_{\mathfrak{p}} := \left\{ \frac{x}{y} \mid x \in R,\, y \in R \setminus \mathfrak{p} \right\}$ die *Lokalisierung* von R an $\mathfrak{p}$.

Man nennt R einen *Dedekindring*, falls $R_{\mathfrak{p}}$ für alle Primideale $\mathfrak{p}$ von R ein diskreter Bewertungsring ist.

Ist R ein diskreter Bewertungsring mit $K := \mathrm{Quot}(R)$ und dazugehöriger diskreter Bewertung v. Dann bezeichne $\hat{K}$ die Vervollständigung von K bezüglich v gerade die Vervollständigung von K bezüglich des durch v induzierten Absolutbetrags. Die diskrete Bewertung v läßt sich dann fortsetzen zu einer diskreten Bewertung $\hat{v}$ auf $\hat{K}$. Die Vervollständigung $\hat{R}$ von R ist dann der Bewertungsring von $\hat{v}$.

Ist R ein Dedekindring und $\mathfrak{p}$ ein Primideal von R, so bezeichnet $\hat{R}_\mathfrak{p}$ die Vervollständigung von $R_\mathfrak{p}$.

Im Folgenden sei R ein Dedekindring mit Quotientenkörper K und A eine zentraleinfache K-Algebra.

Bemerkung 2.4.4 Jedes (gebrochene) Hauptideal (x) von K besitzt dann bekanntlich eine eindeutige Faktorisierung $(x) = \prod_\mathfrak{p}(\mathfrak{p})^{v_\mathfrak{p}(x)}$ in Primideale von R. Für ein fixiertes Primideal $\mathfrak{p}$ liefert die Zuordnung $x \mapsto v_\mathfrak{p}(x)$ eine diskrete Bewertung und $x \mapsto \exp(-v_\mathfrak{p}(x))$ einen nicht-archimedischen Absolutbetrag auf K, den durch $\mathfrak{p}$ induzierten Absolutbetrag. Zwei verschiedene Primideale induzieren nichtäquivalente Beträge.

Definition 2.4.5 Eine Stelle von K ist eine Äquivalenzklasse von Absolutbeträgen. Sie heißt unendlich, falls die Absolutbeträge archimedisch sind, ansonsten endlich.
Eine Stelle heißt „R-Stelle“, falls die Stelle durch ein Primideal in R induziert wird, ansonsten „Nicht-R-Stelle“.
Des weiteren bezeichne $\hat{K}_P$ die Vervollständigung von K an der Stelle P und $\hat{A}_P := \hat{K}_P \otimes_K A$. Nach Lemma 2.1.8 ist $\hat{A}_\mathfrak{p}$ eine zentraleinfache $\hat{K}_\mathfrak{p}$-Algebra.

Da alle Primideale verschiedene „R-Stellen“ induzieren, werden wir nicht zwischen den Primidealen und ihren Stellen unterscheiden.

Definition 2.4.6 Ein *algebraischer Zahlkörper* ist eine endliche Körpererweiterung von $\mathbb{Q}$. Ein *Funktionenkörper* ist eine endliche Erweiterung von $\mathbb{F}_q(t)$. Ein *globaler Körper* ist entweder ein algebraischer Zahlkörper oder ein Funktionenkörper.

Bemerkung 2.4.7

(a) Für einen Zahlkörper K induziert jede Einbettung $\sigma\colon K \hookrightarrow \mathbb{C}$ via $x \mapsto |\sigma(x)|$ eine unendliche Stelle. Zwei Einbettungen erzeugen dabei dieselbe Stelle genau dann wenn sie entweder gleich oder aber komplex konjugiert sind. Eine solche unendliche Stelle P heißt reell falls das dazugehörige $\sigma(K) \subseteq \mathbb{R}$ ist, ansonsten komplex.
Weiter ist $\hat{K}_P$ dann isomorph zu $\mathbb{R}$ oder $\mathbb{C}$, je nachdem ob P reell ist oder aber komplex.
Neben den durch Primidealen induzierten „R-Stellen“, sind dies die einzigen Stellen von K. Insbesondere sind die unendlichen Stellen gerade die „Nicht-R-Stellen“.

(b) Ein Funktionenkörper $K = \mathbb{F}_q(t)$ besitzt nur endliche Stellen. Aber aber nicht alle sind „R-Stellen“, wie die durch die Gradbewertung auf K induzierte Stelle zeigt, wenn man $R = \mathbb{F}_q[t]$ wählt.

Definition 2.4.8 Sei A eine zentraleinfache K-Algebra. Nach dem Struktursatz von Wedderburn gilt: Für jede Stelle P von K ist $\hat{A}_P \cong D_P^{\kappa_P \times \kappa_P}$ für einen Schiefkörper D_P mit Zentrum $\hat{K}_P$. Ist $[D_P : \hat{K}_P] = m_P^2$, so heißt m_P der *lokale Index* und κ_P die *lokale Kapazität* von A an P. Ist $m_P > 1$, so sagt man P sei *verzweigt* in A.

Bemerkung 2.4.9 Ist K ein algebraischer Zahlkörper. Dann können keine komplexen unendlichen Stellen von K verzweigen, da $\mathbb{C}$ algebraisch abgeschlossen ist und somit keine echten endlichen Schiefkörpererweiterungen zuläßt. (Oder äquivalent dazu: die Brauergruppe von $\mathbb{C}$ ist trivial.)

2.5 Ideale, Ordnungen und das Brandtsche Gruppoid

Es sei R ein Dedekindring, $K = \mathrm{Quot}(R)$ sein Quotientenkörper und A eine einfache K-Algebra mit $Z(A)/K$ separabel.

Definition 2.5.1 Ein Element $a \in A$ heißt *ganz über* R, falls es ein normiertes Polynom $p(X) \in R[X]$ gibt mit $p(a) = 0$.

Lemma 2.5.2 *Für jedes $a \in A$ sind folgende Aussagen äquivalent:*

(a) a ist ganz über R.

(b) $R[a]$ ist ein endlich erzeugter R-Modul.

(c) a liegt in einem Teilring B von A, der als R-Modul endlich erzeugt ist.

(d) $\mu_{a,K}(X) \in R[X]$.

Beweis:
$(a) \Longrightarrow (b)$ Es existieren $r_0, \ldots, r_{n-1} \in R$ so, daß $a^n = \sum_{k=0}^{n-1} r_k a^k$. Damit ist $R[a] = \sum_{k=0}^{n-1} R a^k$.

$(b) \Longrightarrow (c)$ Man wähle $B = R[a]$.

$(c) \Longrightarrow (d)$ Sei $B = \sum_{k=1}^{n} Rb_k$ mit $b_1, \ldots, b_n \in B \setminus \{0\}$. Da B ein Ring ist, gilt $ab_i \in B$. Damit existieren $a_{ij} \in R$ mit $ab_i = \sum_{j=1}^{n} a_{ij} b_j$. Mit den Bezeichnungen $M = a \cdot I_n - (a_{ij})$ und $b = (b_1, \ldots, b_n)^{\mathrm{t}}$ gilt $M \cdot b = 0$. Damit ist $\det(M) \cdot I_n \cdot b = M^* \cdot M \cdot b = 0$ wobei M^* die zu M adjungierte Matrix bezeichne. Da R ein Integritätsbereich ist, folgt $\det(M) = 0$. Dies zeigt, daß a eine Nullstelle des normierten Polynoms $g(X) := \det(X \cdot I_n - (a_{ij})) \in R[X]$ ist. Es existiert somit ein normiertes Polynom $h(X) \in K[X]$ mit $g = \mu_{a,K} \cdot h$. Nach dem Lemma von Gauß ist dann $\mu_{a,K} \in R[X]$.

$(d) \Longrightarrow (a)$ Ist klar. □

Korollar 2.5.3 *Ist $a \in A$ ganz über R, so sind* $\mathrm{Tr}_{A/K}(a)$, $\mathrm{Nr}_{A/K}(a)$, $\mathrm{tr}_{A/K}(a)$ *und* $\mathrm{nr}_{A/K}(a)$ *in R.*

Beweis: Es genügt die Behauptung für $\mathrm{tr}_{A/K}(a)$ und $\mathrm{nr}_{A/K}(a)$ zu beweisen. Sei S der ganze Abschluß von R in $Z(A)$. Dann ist a auch ganz über S. Es sei E ein Zerfällungskörper von A und $h\colon E \otimes_{Z(K)} A \to E^{m \times m}$ ein E-Isomorphismus. Dann ist $h(1 \otimes a)$ ganz über S und damit ist $\mu_{h(1 \otimes a),E}(X) \in S[X]$. Das charakteristische Polynom von $h(1 \otimes a)$ teilt eine Potenz von $\mu_{h(1 \otimes a),E}(X)$ in $Z(A)[X]$. Nach dem Lemma von Gauß liegt es damit ebenso in $S[X]$. Nach Definition 2.2.8 sind dann $\mathrm{tr}_{A/K}(a)$ und $\mathrm{nr}_{A/K}(a)$ ganz über R. □

Definition 2.5.4 Ein *R-Gitter* ist ein endlich erzeugter, torsionsfreier R-Modul. Ein *volles R-Gitter* von A ist ein R-Gitter I mit $K \otimes_R I \simeq A$.
Eine *R-Ordnung* ist ein R umfassendes volles R-Gitter in A, das zugleich ein Teilring von A ist. Eine Ordnung heißt maximal, falls sie in keiner anderen enthalten ist. In diesem Fall sprechen wir von einer *R-Maximalordnung*.

Alle Gitter in dieser Arbeit seien als voll angenommen.

Definition 2.5.5 Sei I ein R-Gitter. Die zu I gehörende *Links-* bzw. *Rechtsordnung* ist

$$\mathcal{O}_l(I) := \{x \in A \mid xI \subseteq I\} \text{ bzw.}$$
$$\mathcal{O}_r(I) := \{x \in A \mid Ix \subseteq I\}.$$

Weiter ist das zu I *inverse Gitter* I^{-1} gegeben durch

$$I^{-1} := \{x \in A \mid IxI \subseteq I\} = \{x \in A \mid Ix \subseteq \mathcal{O}_l(I)\} = \{x \in A \mid xI \subseteq \mathcal{O}_r(I)\}\ .$$

Bemerkung 2.5.6 (Rechenregeln) Es seien I und J zwei R-Gitter in A. Dann gelten

(a) IJ ist ein R-Gitter.

(b) $\mathcal{O}_l(I)$ sowie $\mathcal{O}_r(I)$ sind R-Ordnungen.

(c) I^{-1} ist ein R-Gitter.

(d) $I \subseteq \mathcal{O}_l(I) \iff I \subseteq \mathcal{O}_r(I)$.

(e) $\mathcal{O}_l(I) \subseteq \mathcal{O}_l(IJ)$ und $\mathcal{O}_l(I) \subseteq \mathcal{O}_r(I^{-1})$

(f) $\mathcal{O}_r(J) \subseteq \mathcal{O}_r(IJ)$ und $\mathcal{O}_r(I) \subseteq \mathcal{O}_l(I^{-1})$

Ist $\mathcal{O}_l(I)$ bzw. $\mathcal{O}_r(I)$ eine R-Maximalordnung, so gilt in (d) respektive (e) stets „=“.

Beweis:

(a) Sicher ist IJ ein endlich erzeugter R-Modul. Da I und J beide eine K-Basis von A enthalten, enthält auch IJ ein K-Erzeugendensystem von A.

(b) $\mathcal{O}_l(I)$ ist ein Teilring von A sowie ein R-Modul, der R enthält. Für jedes $x \in A$ ist xI ebenfalls ein R-Gitter. Da xI über R endlich erzeugt ist, existiert ein $r \in R$ mit $rxI \subseteq I$. Daher ist $A = K \cdot \mathcal{O}_l(I)$.

(c) Sei $\Lambda = \mathcal{O}_l(I)$. Wie in (a) finden wir $r, s \in K^*$ mit $r\Lambda \subseteq I \subseteq s\Lambda$. Dann gilt $I^{-1} = \{x \in A \mid xI \subseteq \Lambda\} \subseteq \{x \in A \mid r\Lambda \subseteq \Lambda\} = r^{-1}\Lambda$ bzw. analog $s^{-1}\Lambda \subseteq I^{-1}$. Also ist I^{-1} ein volles R-Gitter.

(d) $I \subseteq \mathcal{O}_l(I) \iff II \subseteq I \iff I \subseteq \mathcal{O}_r(I)$.

(e) Die erste Inklusion folgt aus $\mathcal{O}_l(I)IJ = IJ \implies \mathcal{O}_l(I) \subseteq \mathcal{O}_l(IJ)$. Die zweite ist wegen $II^{-1} \cdot (\mathcal{O}_l(I)I) = II^{-1}I \subseteq I \implies I^{-1}\mathcal{O}_l(I) \subseteq I^{-1} \implies \mathcal{O}_l(I) \subseteq \mathcal{O}_r(I^{-1})$ richtig.

(f) Analog zu (d). □

Satz 2.5.7 *Es sei Λ ein R umfassender Teilring von A mit $K \otimes_K \Lambda \cong A$ und jedes $x \in \Lambda$ sei ganz über R. Dann ist Λ eine R-Ordnung. Umgekehrt besitzt jede R-Ordnung diese Eigenschaften.*

Beweis: Sei $(x_1, \ldots, x_m)$ eine K-Basis von A. Wir können annehmen, daß alle x_i in Λ liegen. Damit ist $I := \sum_{k=1}^m Rx_k \subseteq \Lambda$ ein volles R-Gitter. Weiter ist $d := \det(\mathrm{tr}_{A/K}(x_i x_j)) \in R$ und nicht 0, da die Spurbilinearform nicht ausgeartet ist.
Sei nun $x \in \Lambda$, so ist $x = \sum_{k=1}^m \lambda_k x_k$ mit $\lambda_k \in K$. Also gilt

$$\mathrm{tr}_{A/K}(xx_j) = \sum_{i=1}^m \lambda_i \,\mathrm{tr}_{A/K}(x_i x_j) \in R\,.$$

Lösen wir das lineare Gleichungssystem nach $\lambda_1, \ldots, \lambda_m$ auf, so zeigt die Cramersche Regel $\lambda_i = d^{-1}r_i$ für ein $r_i \in R$. Es ist also $I \subseteq \Lambda \subseteq d^{-1}I$. Daher ist Λ eine R-Ordnung.

Ist umgekehrt Λ eine R-Ordnung und $x \in \Lambda$. Dann ist $R[x] \subseteq \Lambda$ ein endlich erzeugter R-Modul, d.h. x ist ganz über R. □

Satz 2.5.8 *Es seien $I \subseteq J$ zwei volle R-Gitter in A. Dann existieren eine K-Basis $x_1, \ldots, x_m$ von A sowie gebrochene R-Ideale $\mathfrak{b}_1, \ldots, \mathfrak{b}_m$ in K und eine absteigende Kette $\mathfrak{a}_1 \supseteq \mathfrak{a}_2 \supseteq \ldots \supseteq \mathfrak{a}_m$ von ganzen R-Idealen so, daß gilt*

$$I = \bigoplus_{k=1}^{m} \mathfrak{b}_k x_k \quad \textit{und} \quad J = \bigoplus_{k=1}^{m} \mathfrak{b}_k \mathfrak{a}_k x_k.$$

Außerdem sind die Ideale $\mathfrak{a}_1, \ldots, \mathfrak{a}_m$ eindeutig bestimmt.

Beweis: Ein Beweis findet sich in [O'M00, Theorem 81:11, S. 214]. □

Definition 2.5.9 Sei M ein endlich erzeugter R-Modul und $\mathfrak{p}$ ein Primideal von R. Außerdem bezeichne $R_\mathfrak{p}$ die Lokalisierung von R an $\mathfrak{p}$ und $\hat{R}_\mathfrak{p}$ die $\mathfrak{p}$-adische Komplettierung von R mit dazugehörendem Quotientenkörper $\hat{K}_\mathfrak{p}$.

Weiter heißen $M_\mathfrak{p} := R_\mathfrak{p} \otimes_R M$ und $\hat{M}_\mathfrak{p} := \hat{R}_\mathfrak{p} \otimes_R M$ die *Lokalisierung* bzw. die *Komplettierung* von M an $\mathfrak{p}$.

Falls R lokal ist, werden wir bei den Komplettierungen den Index $\mathfrak{p}$ manchmal weglassen.

Wegen $\hat{M}_\mathfrak{p} = \hat{R}_\mathfrak{p} \otimes_R M \cong \hat{R}_\mathfrak{p} \otimes_{R_\mathfrak{p}} (R_\mathfrak{p} \otimes_R M) \cong \hat{R}_\mathfrak{p} \otimes_{R_\mathfrak{p}} M_\mathfrak{p}$ kann die Komplettierung eines R-Moduls M an $\mathfrak{p}$ in zwei Schritten durchgeführt werden; zuerst lokalisiert man an $\mathfrak{p}$ und dann komplettiert man.

Lemma 2.5.10 *Sei R ein diskreter Bewertungsring mit maximalem Ideal $R\pi$ und M ein endlich erzeugter R-Modul. Dann gelten*

(a) $R/\pi^k R \cong \hat{R}/\pi^k \hat{R}$ für alle $k \geq 1$.

(b) $M/\pi^k M \cong \hat{M}/\pi^k \hat{M}$ für alle $k \geq 1$.

Beweis: Bezeichne $f\colon R \hookrightarrow \hat{R} \to \hat{R}/\pi^k \hat{R}$ die Komposition der beiden kanonischen Morphismen. Da R dicht liegt in $\hat{R}$, ist f ein Epimorphismus. Weiter ist $\ker(f) = R \cap \pi^k \hat{R} = \pi^k R$. Daraus folgt (a).
Nach Satz 2.5.8 ist $M \cong \bigoplus_{i=1}^{r} R/\pi^{n_i} R$ mit $n_i \geq 0$. Daher können wir $M = R/\pi^n R$ mit $n \geq 0$ annehmen. Es wird

$$\hat{M} \cong \hat{R}/\pi^n \hat{R} \cong R/\pi^n R = M\,.$$

□

Wir können M also als Teilmenge von $\hat{M}$ auffassen und wir stellen uns $\hat{M} = \hat{R} \otimes_R M$ als $\hat{R}M$ vor. Damit folgt

Lemma 2.5.11 *Ist R ein diskreter Bewertungring mit maximalem Ideal $R\pi$, so liefern*

$$\begin{array}{rcl} I & \longrightarrow & \hat{R}I = \hat{I} \\ J \cap A & \longleftarrow & J \end{array}$$

inklusionserhaltende Bijektionen zwischen den R-Gittern von A und den $\hat{R}$-Gittern von $\hat{A}$. Insbesondere induzieren diese Abbildungen eine Bijektion zwischen den entsprechenden Ordnungen.

Beweis: Sei I ein R-Gitter in A. Dann ist eine R-Basis $(x_1, \ldots, x_n)$ von I auch eine K-Basis von A, eine $\hat{R}$-Basis von $\hat{I}$ und eine $\hat{K}$-Basis von $\hat{A}$. Damit ist $\hat{I}$ ein volles $\hat{R}$-Gitter in $\hat{A}$ mit

$$\hat{I} \cap A = \bigoplus_{k=1}^{n} (\hat{R} \cap K)x_k = \bigoplus_{k=1}^{n} Rx_k = I \, .$$

Umgekehrt sei J ein $\hat{R}$-Gitter von $\hat{A}$. Weiter sei v die Fortsetzung der zu R gehörenden diskreten Bewertung auf $\hat{K}$. Für eine K-Basis $(e_1, \ldots, e_n)$ von A existieren nun $r_{ij} \in \hat{K}$ so, daß $b_i = \sum_{j=1}^{n} r_{ij} e_j$ $(1 \leq i \leq n)$ eine $\hat{R}$-Basis von J ist. Da $(e_1, \ldots, e_n)$ ein volles $\hat{R}$-Gitter in $\hat{A}$ erzeugt, existiert ein $k \in \mathbb{N}$ mit $\pi^k e_i \in J$ für alle i. Jetzt wählen wir $r'_{ij} \in R$ mit $v(r_{ij} - r'_{ij}) > k$ und setzen $b'_i = \sum_{j=1}^{n} r'_{ij} e_j$. Ist J' das von $(b'_1, \ldots, b'_n)$ erzeugte $\hat{R}$-Gitter in $\hat{A}$, so gilt $J = J' + \pi J$. Mit Nakayamas Lemma folgt $J' = J$. Somit enthält $J \cap A$ die Elemente $b'_1, \ldots, b'_n$ und ist damit ein volles R-Gitter in A mit $\hat{R} \cdot (J \cap A) = J$. □

Satz 2.5.12 *Es seien I ein R-Gitter und Λ eine R-Ordnung in A. Dann gilt für alle $\mathfrak{p} \underset{\max}{\lhd} R$:*

(a) $\Lambda_\mathfrak{p}$ ist eine $R_\mathfrak{p}$-Ordnung in A.

(b) $\hat{\Lambda}_\mathfrak{p}$ ist eine $\hat{R}_\mathfrak{p}$-Ordnung in $\hat{A}_\mathfrak{p}$.

(c) $I_\mathfrak{p}$ ist ein $R_\mathfrak{p}$-Gitter in A mit $\mathcal{O}_l(I_\mathfrak{p}) = \mathcal{O}_l(I)_\mathfrak{p}$ und $\mathcal{O}_r(I_\mathfrak{p}) = \mathcal{O}_r(I)_\mathfrak{p}$.

(d) $\hat{I}_\mathfrak{p}$ ist ein $\hat{R}_\mathfrak{p}$-Gitter in $\hat{A}_\mathfrak{p}$ mit

$$\mathcal{O}_l(\hat{I}_\mathfrak{p}) = \widehat{\mathcal{O}_l(I_\mathfrak{p})} = \widehat{\mathcal{O}_l(I)}_\mathfrak{p} \text{ und } \mathcal{O}_r(\hat{I}_\mathfrak{p}) = \widehat{\mathcal{O}_r(I_\mathfrak{p})} = \widehat{\mathcal{O}_r(I)}_\mathfrak{p} \, .$$

Beweis: Es liefert das Lokalisieren von R-Gittern bzw. R-Ordnungen in A wieder ein $R_\mathfrak{p}$-Ideal bzw. eine $R_\mathfrak{p}$-Ordnung in $A_\mathfrak{p}$. Nach dem vorherigen Lemma gilt dies entsprechend auch für die Komplettierung.

(c) Sei $x \in \mathcal{O}_l(I_\mathfrak{p})$, dann gilt $xI_\mathfrak{p} \subseteq I_\mathfrak{p}$. Ein R-Erzeugendensystem $(x_1, \ldots, x_l)$ von I erzeugt ebenfalls $I_\mathfrak{p}$ über $R_\mathfrak{p}$. Also existieren $r_{ij} \in R$, $s_{ij} \in R \setminus \mathfrak{p}$ $(1 \leq i, j \leq l)$ mit $xx_i = \sum_{j=1}^{l} \frac{r_{ij}}{s_{ij}} x_j$. Mit $s := \prod_{i,j} s_{ij} \in R \setminus \mathfrak{p}$ gilt $sxI \subseteq I$. Dies zeigt $\mathcal{O}_l(I_\mathfrak{p}) \subseteq \mathcal{O}_l(I)_\mathfrak{p}$. Die umgekehrte Inklusion ist trivial.

(d) Sei $(b_1, \ldots, b_n)$ eine $R_\mathfrak{p}$-Basis von $I_\mathfrak{p}$. Dann gilt

$$\begin{aligned}\mathcal{O}_l(\hat{I}_\mathfrak{p}) \cap A_\mathfrak{p} &= \{x \in A_\mathfrak{p} \mid xb_i \in \hat{I}_\mathfrak{p} \text{ für alle } i\} \\ &= \{x \in A_\mathfrak{p} \mid xb_i \in I_\mathfrak{p} \text{ für alle } i\} \\ &= \mathcal{O}_l(I_\mathfrak{p}) = \mathcal{O}_l(I)_\mathfrak{p}\end{aligned}$$

Mit dem vorherigen Lemma folgt die Behauptung. □

Satz 2.5.13 *Zwei R-Gitter I und J in A sind genau dann gleich, wenn $I_\mathfrak{p} = J_\mathfrak{p}$ für alle $\mathfrak{p} \underset{\max}{\lhd} R$ gilt.*

Beweis: Sind I und J gleich, so stimmen sie natürlich an allen Lokalisierungen überein. Für die Umkehrung genügt es zu zeigen, daß jeder endlich erzeugte R-Modul M mit $M_\mathfrak{p} = 0$ für alle $\mathfrak{p} \underset{\max}{\lhd} R$ der Nullmodul sein muß. Denn dann wendet man die Aussage auf $(I + J)/I$ und $(I + J)/J$ an.
Sei nun ein solcher Modul M mit Erzeugendensystem $(x_1, \ldots, x_l)$ gegeben. Die Menge $\mathfrak{a} = \{r \in R \mid rM = 0\}$ bildet ein Ideal in R. Wäre $\mathfrak{a} \subsetneq R$, so existiert ein maximales Ideal $\mathfrak{p}$ von R mit $\mathfrak{a} \subseteq \mathfrak{p}$. Wegen $M_\mathfrak{p} = 0$ existieren $s_1, \ldots, s_l \in R \setminus \mathfrak{p}$ mit $s_k x_k = 0$. Mit $s := \prod_{k=1}^{l} s_k \in R \setminus \mathfrak{p}$ folgt $sM = 0$ und damit $s \in \mathfrak{a} \subseteq \mathfrak{p}$. Also kann ein solches Primideal $\mathfrak{p}$ nicht existieren. D.h. es ist $\mathfrak{a} = R$ und damit $M = 0$. □

Da die Gitter von $A_\mathfrak{p}$ und $\hat{A}_\mathfrak{p}$ korrespondieren, gilt Satz 2.5.13 auch für die Komplettierungen.

Definition 2.5.14 Zu einem R-Gitter I in A ist $I^\# := \{x \in A \mid \mathrm{tr}_{A/K}(xI) \subseteq R\}$ das *duale Gitter* bezüglich der Spurbilinearform τ.

Lemma 2.5.15 (Rechenregeln für duale Gitter) *Ist I ein R-Gitter in A, so gilt:*

(a) Ist J ein weiteres R-Gitter in A mit $J \subseteq I$, so folgt $I^\# \subseteq J^\#$.

(b) $I^\#$ ist ein R-Gitter.

(c) Für alle $\mathfrak{p} \underset{\max}{\lhd} R$ ist $(I^\#)_\mathfrak{p} = (I_\mathfrak{p})^\#$ und $\widehat{(I^\#)}_\mathfrak{p} = (\hat{I}_\mathfrak{p})^\#$.

(d) $(I^\#)^\# = I$.

(e) $\mathcal{O}_l(I) = \mathcal{O}_r(I^\#)$ und $\mathcal{O}_r(I) = \mathcal{O}_l(I^\#)$

(f) $I^{-1} = (\mathcal{O}_l(I)^\# \cdot I)^\# = (I \cdot \mathcal{O}_r(I)^\#)^\#$, insbesondere vertauscht Invertieren mit Lokalisieren und Komplettieren.

Beweis:

(a) Dies ist eine direkte Folgerung aus Definition 2.5.14.

(b) $I^\#$ ist sicher ein R-Modul. Außerdem gilt $(rI)^\# = r^{-1}(I^\#)$ für alle $r \in R$. Wir dürfen daher $I \subseteq \mathcal{O}_l(I)$ voraussetzen. Nach Satz 2.5.7 ist dann $\mathrm{tr}_{A/K}(I^2) \subseteq \mathrm{tr}_{A/K}(I) \subseteq \mathrm{tr}_{A/K}(\mathcal{O}_l(I)) \subseteq R$. Damit ist $I \subseteq I^\#$. Seien dann $x_1, \ldots, x_m \in I$ so, daß diese eine K-Basis von A bilden. Wir setzen $L := \sum_{k=1}^m Rx_k \subseteq I$. Da die Spurbilinearform nicht ausgeartet ist, existieren $x_1^*, \ldots, x_m^* \in A$ mit $\mathrm{tr}_{A/K}(x_i x_j^*) = \delta_{ij}$. Diese Elemente bilden eine R-Basis von $L^\#$. Also ist $L^\#$ ein R-Ideal in A und erfüllt $L \subseteq I \subseteq I^\# \subseteq L^\#$. Also ist $I^\#$ ein volles R-Gitter in A.

(c) Es sei $\frac{x}{r} \in (I^\#)_\mathfrak{p}$ mit $x \in I^\#$ und $r \in R \setminus \mathfrak{p}$. Dann gilt $\mathrm{tr}_{A/K}(\frac{x}{r}\frac{y}{s}) = \frac{1}{rs}\mathrm{tr}_{A/K}(xy) \in R_\mathfrak{p}$ für alle $y \in I$ und $s \in R \setminus \mathfrak{p}$. Dies zeigt $(I^\#)_\mathfrak{p} \subseteq (I_\mathfrak{p})^\#$.

Umgekehrt seien $x \in (I_\mathfrak{p})^\#$ und $(x_1, \ldots, x_m)$ eine $R_\mathfrak{p}$-Basis von $I_\mathfrak{p}$. Dann ist $\mathrm{tr}_{A/K}(xx_i) = \frac{r_i}{s_i}$ mit $r_i \in R$ und $s_i \in R \setminus \mathfrak{p}$. Setzen wir $s := \prod_i s_i$, so folgt $\mathrm{tr}_{A/K}(sxI) \subseteq R$. Also gilt $sx \in I^\#$ und damit $x \in (I^\#)_\mathfrak{p}$. Damit ist $(I^\#)_\mathfrak{p} = (I_\mathfrak{p})^\#$.

Da Dualisieren mit Lokalisieren vertauscht, können wir $R = R_\mathfrak{p}$ voraussetzen. Weiter sei dann $(x_1, \ldots, x_m)$ eine R-Basis von I. Nach Korollar 2.2.7 ist $\mathrm{tr}_{\hat{A}/\hat{K}}$ eine Fortsetzung von $\mathrm{tr}_{A/K}$. Mit $R = K \cap \hat{R}$ folgt somit

$$\begin{aligned} I^\# &= \{x \in A \mid \mathrm{tr}_{A/K}(xx_i) \in R \text{ für alle } i\} \\ &= \{x \in A \mid \mathrm{tr}_{\hat{A}/\hat{K}}(xx_i) \in \hat{R} \text{ für alle } i\} = (\hat{I})^\# \cap A\,. \end{aligned}$$

Mit Lemma 2.5.11 folgt hieraus $\widehat{(I^\#)} = (\hat{I})^\#$.

(d) Wir dürfen erneut R als lokal annehmen. Dann ist I ein freies R-Gitter mit einer R-Basis $\underline{x}$. Die zu $\underline{x}$ duale Basis $\underline{x}^*$ ist dann eine R-Basis von $I^\#$. Damit ist $\underline{x}$ wiederum zu $\underline{x}^*$ dual und somit eine R-Basis von $(I^\#)^\#$.

(e) Aus

$$x \in \mathcal{O}_l(I) \implies xI \subseteq I \implies \mathrm{tr}_{A/K}(I^\# xI) \subseteq \mathrm{tr}_{A/K}(I^\# I) \subseteq R \implies x \in \mathcal{O}_r(I^\#)$$

folgt

$$\mathcal{O}_l(I) \subseteq \mathcal{O}_r(I^\#)\,.$$

Genauso zeigt man $\mathcal{O}_r(I) \subseteq \mathcal{O}_l(I^\#)$. Mit $(I^\#)^\# = I$ folgt daraus die Behauptung.

(f) Es gilt

$$\begin{aligned} (\mathcal{O}_l(I)^\# \cdot I)^\# &= \{x \in A \mid \mathrm{tr}_{A/K}(\mathcal{O}_l(I)^\# Ix) \subseteq R\} \\ &= \{x \in A \mid Ix \subseteq (\mathcal{O}_l(I)^\#)^\# = \mathcal{O}_l(I)\} = I^{-1}\,. \end{aligned}$$

Analog folgert man die verbleibende Identität. □

Satz 2.5.16 *Jede R-Ordnung ist in einer R-Maximalordnung enthalten, und es existiert mindestens eine R-Maximalordnung.*

Beweis: Sei $x_1, \ldots, x_m$ eine K-Basis von A. Damit wird $I := \sum_{k=1}^{m} Rx_k$ ein R-Gitter in A. Somit existiert zumindest eine R-Ordnung, nämlich $\mathcal{O}_l(I)$. Es verbleibt noch zu zeigen, daß jede R-Ordnung Λ in einer R-Maximalordnung enthalten ist.
Sei Λ' eine beliebige R-Ordnung, welche Λ enthalte. Aus $\mathrm{tr}_{A/K}(\Lambda'\Lambda) = \mathrm{tr}_{A/K}(\Lambda') \subseteq R$ folgt $\Lambda' \subseteq \Lambda^{\#}$. Da $\Lambda^{\#}$ noethersch ist, existiert insbesondere eine R-Maximalordnung die Λ enthält. □

Satz 2.5.17 *Für eine R-Ordnung Λ in A sind äquivalent:*

(a) Λ ist eine R-Maximalordnung in A.

(b) Für alle Primideale $\mathfrak{p}$ von R ist $\Lambda_{\mathfrak{p}}$ eine $R_{\mathfrak{p}}$-Maximalordnung in A.

(c) Für alle Primideale $\mathfrak{p}$ von R ist $\hat{\Lambda}_{\mathfrak{p}}$ eine $\hat{R}_{\mathfrak{p}}$-Maximalordnung in $\hat{A}_{\mathfrak{p}}$.

Beweis:
$(a) \Longrightarrow (b)$ Sei Λ maximal und $\mathfrak{p} \underset{\max}{\lhd} R$. Nach Satz 2.5.16 gibt es eine $R_{\mathfrak{p}}$-Maximalordnung Ω mit $\Lambda_{\mathfrak{p}} \subseteq \Omega$. Dann existiert ein $r \in R \setminus \{0\}$, so daß $r\Omega \subseteq \Lambda_{\mathfrak{p}}$ gilt. $\Gamma := r\Omega \cap \Lambda$ ist dann ein R-Ideal in A. Wegen $\Gamma \cdot \Lambda \subseteq \Lambda \cdot \Lambda = \Lambda$ ist $\Lambda \subseteq \mathcal{O}_r(\Gamma)$. Da Λ eine R-Maximalordnung ist, gilt $\Lambda = \mathcal{O}_r(\Gamma)$.
Ist nun $x \in r\Omega$, so gibt es ein $s \in R \setminus \mathfrak{p}$ mit $sx \in \Lambda$, d.h. $x \in \Gamma_{\mathfrak{p}}$. Ist umgekehrt $x \in \Gamma_{\mathfrak{p}}$, so gibt es wiederum ein $s \in R \setminus \mathfrak{p}$ mit $sx \in \Gamma \subseteq r\Omega$. Damit folgt $x \in r\Omega$. Wir haben also $\Gamma_{\mathfrak{p}} = r\Omega$ gezeigt. Weiter wird jetzt

$$\Omega = \mathcal{O}_r(r\Omega) = \mathcal{O}_r(\Gamma_{\mathfrak{p}}) = \mathcal{O}_r(\Gamma)_{\mathfrak{p}} = \Lambda_{\mathfrak{p}} .$$

$(b) \Longrightarrow (a)$ ist eine einfache Folgerung aus Satz 2.5.13.

$(b) \Longleftrightarrow (c)$ wurde bereits in Lemma 2.5.11 gezeigt. □

Definition 2.5.18 Sei Λ eine R-Ordnung in A. Ein R-Gitter I in A heißt:

- Λ-*Linksideal*, falls $\Lambda = \mathcal{O}_l(I)$ gilt.
- Λ-*Rechtsideal*, falls $\Lambda = \mathcal{O}_r(I)$ gilt.
- *zweiseitiges* Λ-*Ideal*, falls $\Lambda = \mathcal{O}_l(I) = \mathcal{O}_r(I)$.
- *normal*, falls $\mathcal{O}_l(I)$ maximal ist.
- *ganz*, falls $I \subseteq \mathcal{O}_l(I)$.
- *Hauptideal*, falls es ein $x \in A^*$ gibt mit $I = \mathcal{O}_l(I)x$ und $I = x\mathcal{O}_r(I)$.

Ein ganzes zweiseitiges Λ-Ideal $\mathfrak{P} \neq \Lambda$ heißt *Primideal von* Λ, falls für zwei ganze zweiseitige Λ-Ideale I, J mit $IJ \subseteq \mathfrak{P}$ stets $I \subseteq \mathfrak{P}$ oder $J \subseteq \mathfrak{P}$ gilt.

Ein *maximal ganzes* Λ-*Linksideal* ist ein ganzes von Λ verschiedenes Λ-Linksideal, welches in keinem anderen ganzen von Λ verschiedenen Λ-Linksideal echt enthalten ist. Analog definieren wir *maximal ganze* Λ-*Rechtsideale* und *maximal ganze zweiseitige* Λ-*Ideale*.

Ferner sagen wir, das R-Gitter I sei *maximal ganz*, wenn es ein maximal ganzes $\mathcal{O}_l(I)$-Linksideal ist.

Wir haben bereits gesehen, daß ein $I \subseteq \mathcal{O}_l(I) \iff I \subseteq \mathcal{O}_r(I)$ gilt. In Satz 2.5.27 und Korollar 2.5.35 werden wir sehen, daß auch die Definitionen von „normal“ und „maximal ganz“ nur scheinbar asymmetrisch sind. Jetzt kommen wir zu ein paar einfachen Feststellungen.

Bemerkung 2.5.19 Ist Λ eine R-Ordnung und I ein ganzes zweiseitiges Λ-Ideal, so ist I ein zweiseitiges Ideal des Rings Λ im gewöhnlichen Sinne. Da A einfach ist, ist umgekehrt auch jedes gewöhnliche zweiseitige Ideal $I \neq (0)$ des Rings Λ ein volles R-Gitter in A mit $\Lambda \subseteq \mathcal{O}_l(I)$ und $\Lambda \subseteq \mathcal{O}_r(I)$. Ist Λ maximal, so gilt hier Gleichheit. Im Falle $A = K$ sind die R-Gitter in A gerade die gebrochenen R-Ideale von K. Dies erklärt auch, warum man die vollen R-Gitter einer einfachen K-Algebra manchmal *Ideale* nennt. Es ist eine Verallgemeinerung der gebrochenen R-Ideale in K.

Lemma 2.5.20 (Beschreibung der Hauptideale) *Sei Λ eine R-Ordnung in A. Es ist $I := \Lambda x$ genau dann ein volles R-Gitter, wenn $x \in A^*$ gilt. Ist dies der Fall, so gelten*

$$I^{-1} = x^{-1}\Lambda, \quad \mathcal{O}_l(I) = \Lambda = II^{-1} \quad \textit{und} \quad \mathcal{O}_r(I) = x^{-1}\Lambda x = I^{-1}I\,.$$

Insbesondere ist also $I = \mathcal{O}_l(I)x = x\mathcal{O}_r(I)$. Damit ist Λx ein Hauptideal und umgekehrt sind alle Hauptideale von dieser Gestalt. Analoge Aussagen gelten natürlich auch für $I = x\Lambda$.
Weiter ist Λx genau dann ein zweiseitiges Λ-Ideal, wenn neben $x \in A^*$ noch $x\Lambda = \Lambda x$ gilt.

Beweis: Es sei $I = \Lambda x$. Sicher ist I damit ein R-Gitter in A. Nun gilt $K \cdot I = K \cdot \Lambda \cdot x = A \cdot x$. Also ist I ein Ideal genau dann wenn $A \cdot x = A$ gilt, oder äquivalent dazu, wenn x in A invertierbar ist. Ist dies der Fall, so gelten

$$\begin{aligned}
\mathcal{O}_l(I) &= \{y \in A \mid y\Lambda x \subseteq \Lambda x\} = \{y \in A \mid y\Lambda \subseteq \Lambda\} = \mathcal{O}_r(\Lambda) = \Lambda\,,\\
\mathcal{O}_r(I) &= \{y \in A \mid \Lambda xy \subseteq \Lambda x\} = \{y \in A \mid x^{-1}\Lambda xy \subseteq x^{-1}\Lambda x\} = \mathcal{O}_r(x^{-1}\Lambda x) = x^{-1}\Lambda x\,,\\
I^{-1} &= \{y \in A \mid \Lambda xy \subseteq \Lambda\} = \{x^{-1}z \in A \mid \Lambda z \subseteq \Lambda\} = x^{-1}\mathcal{O}_r(\Lambda) = x^{-1}\Lambda\,.
\end{aligned}$$

Die anderen Aussagen sind einfache Folgerungen hieraus. □

Ist Λ eine R-Ordnung, so ist ein ganzes zweiseitiges Λ-Ideal $\mathfrak{P}$ per Definition 2.5.18 genau dann ein Primideal von Λ, wenn für alle gewöhnlichen zweiseitigen Ideale I und J von $\Lambda/\mathfrak{P}$ gilt

$$I \cdot J = 0 \implies I = 0 \text{ oder } J = 0\,. \qquad (*)$$

Lemma 2.5.21 *Sei $\mathfrak{M}$ eine R-Maximalordnung.*

(a) Die Primideale von $\mathfrak{M}$ sind gerade die maximal ganzen zweiseitigen $\mathfrak{M}$-Ideale. Für jedes Primideal $\mathfrak{P}$ von $\mathfrak{M}$ ist $\mathfrak{p} := \mathfrak{P} \cap R$ ein von (0) verschiedenes Primideal in R. Ferner ist $\overline{\mathfrak{M}} := \mathfrak{M}/\mathfrak{P}$ eine einfache endlichdimensionale $R/\mathfrak{p}$-Algebra.

(b) Jedes maximal ganze $\mathfrak{M}$-Linksideal enthält genau ein Primideal von $\mathfrak{M}$, nämlich $\mathfrak{P} := \{x \in \mathfrak{M} \mid x\mathfrak{M} \subseteq M\}$. Weiter ist $\mathfrak{M}/M$ ein einfacher Linksmodul von $\mathfrak{M}/\mathfrak{P}$ und es gilt $\mathfrak{P} \cap R = M \cap R$.

Beweis:

(a) Sei $\mathfrak{P}$ ein maximal ganzes zweiseitiges $\mathfrak{M}$-Ideal. Gilt dann $IJ \subseteq \mathfrak{P}$ für zwei ganze zweiseitige $\mathfrak{M}$-Ideale I und J, so gilt auch $(I+\mathfrak{P})(J+\mathfrak{P}) \subseteq \mathfrak{P}$. Aus der Maximalität folgt $(I+\mathfrak{P}) = \mathfrak{P}$ oder $(J+\mathfrak{P}) = \mathfrak{P}$. Also ist $\mathfrak{P}$ ein Primideal von $\mathfrak{M}$.

Sei nun umgekehrt $\mathfrak{P}$ ein Primideal von $\mathfrak{M}$. Dann ist $\mathfrak{p} := \mathfrak{P} \cap R \neq (0)$ ein Primideal von R. Also ist $\overline{\mathfrak{M}} := \mathfrak{M}/\mathfrak{P}$ eine endlichdimensionale Algebra über $R/\mathfrak{p}$. Nach Lemma 2.3.11 ist $\mathrm{rad}(\overline{\mathfrak{M}})$ daher nilpotent. Aus $(*)$ folgt dann $\mathrm{rad}(\overline{\mathfrak{M}}) = 0$, d.h. $\overline{\mathfrak{M}}$ ist halbeinfach. Damit ist $\overline{\mathfrak{M}}$ eine direkte Summe von einfachen $\overline{\mathfrak{M}}$-Rechtsidealen $\overline{I}_1, \ldots, \overline{I}_l$. Gruppieren wir jeweils isomorphe Rechtsideale zusammen, so erhalten wir eine Zerlegung $\overline{\mathfrak{M}} \cong n_1V_1 \oplus \cdots \oplus n_rV_r$ mit einfachen $\overline{\mathfrak{M}}$-Rechtsmoduln V_i. Dann ist

$$\begin{aligned}\overline{\mathfrak{M}} &\cong \mathrm{End}_{\overline{\mathfrak{M}}}(n_1V_1 \oplus \cdots \oplus n_rV_r) = \mathrm{End}_{\overline{\mathfrak{M}}}(n_1V_1) \times \cdots \times \mathrm{End}_{\overline{\mathfrak{M}}}(n_rV_r) \\ &= \mathrm{End}_{\overline{\mathfrak{M}}}(V_1)^{n_1 \times n_1} \times \cdots \times \mathrm{End}_{\overline{\mathfrak{M}}}(V_r)^{n_r \times n_r}\end{aligned}$$

Wäre $r > 1$, so gäbe es in $\overline{\mathfrak{M}}$ ein Paar zweiseitiger Ideale $I, J \neq 0$ mit $I \cdot J = 0$. Aus $(*)$ folgt daher $r = 1$. Also ist $\overline{\mathfrak{M}}$ als Matrixring über einem Schiefkörper einfach und $\mathfrak{P}$ ist somit ein maximal ganzes zweiseitiges $\mathfrak{M}$-Ideal.

(b) Wir setzen $\mathfrak{P} := \{x \in \mathfrak{M} \mid x\mathfrak{M} \subseteq M\}$. Dann gilt $\mathfrak{P} \subseteq M$. Man rechnet unschwer nach, daß $\mathfrak{P}$ ein zweiseitiges $\mathfrak{M}$-Ideal ist. Weil $\mathfrak{M}$ noethersch ist, existiert ein Primideal $\mathfrak{P}'$ von $\mathfrak{M}$ mit $\mathfrak{P} \subseteq \mathfrak{P}' \subseteq M$. Aus der Wahl von $\mathfrak{P}$ folgt nun aber $\mathfrak{P}' \subseteq \mathfrak{P}$. Damit ist $\mathfrak{P} = \mathfrak{P}'$ ein Primideal von $\mathfrak{M}$. Angenommen, es gäbe ein weiteres Primideal von $\mathfrak{M}$ mit $\mathfrak{P}'' \subseteq M$, so folgt wiederum $\mathfrak{P}'' \subseteq \mathfrak{P}$ und damit $\mathfrak{P}'' = \mathfrak{P}$. Da $\mathfrak{P} \cap R$ ein Primideal ist, und wegen $1 \notin M$, gilt $\mathfrak{M} \cap R = \mathfrak{P} \cap R$.$\square$

Wir wollen nun für normale R-Gitter noch weitere Rechenregeln finden und unter anderem zeigen, daß die zweiseitigen $\mathfrak{M}$-Ideale einer Maximalordnung $\mathfrak{M}$ eine freie abelsche Gruppe bilden, welche von den Primidealen von $\mathfrak{M}$ erzeugt wird. Dazu folgen wir dem Beweis bei Dedekindringen. Unser Vorgehen verwendet *nicht* die explizite Struktur der zentraleinfachen Algebren über einem diskret bewerteten Körper. (Wir verwendeten lediglich die Tatsache, daß jedes R-Gitter an seinen Lokalisierungen frei ist, als wir $I = (I^{\#})^{\#}$ gezeigt haben.) Alternativ kann man auch zuerst die Ergebnisse aus Abschnitt 2.7 beweisen. Dort wird gezeigt, daß über einem diskreten Bewertungsring jedes $\mathfrak{M}$-Linksideal bzw. $\mathfrak{M}$-Rechtsideal ein Hauptideal ist. Damit erhält man die Theorie der normalen R-Gitter etwas leichter, da man alle Beweise nur für Hauptideale führen muß.

Lemma 2.5.22 *Es sei Λ eine R-Ordnung in A. Jedes ganze zweiseitige Λ-Ideal enthält ein Produkt von Primidealen von Λ.*

Beweis: Angenommen, es existiert ein zweiseitiges Λ-Ideal, welches der Behauptung widerspricht. Dann existiert auch ein bezüglich Inklusion maximales Gegenbeispiel I, da Λ noethersch ist. Da I kein Primideal von Λ ist, existieren zweiseitige Λ-Ideale I_1, I_2 mit $I_i \not\subseteq \Lambda$ und $I_1 I_2 \subseteq I$. Ersetzen wir I_i durch $I_i + I$, so können wir $I \subsetneq I_i$ annehmen. Also enthalten I_1 und I_2 jeweils ein Produkt von Primidealen von Λ. Damit gilt dies auch für I, was der Wahl von I widerspricht. □

Lemma 2.5.23 *Es sei $\mathfrak{M}$ eine R-Maximalordnung und I ein zweiseitiges $\mathfrak{M}$-Ideal. Falls $I \subsetneq \mathfrak{M}$ gilt, dann ist $\mathfrak{M} \subsetneq I^{-1}$.*

Beweis: Es gilt sicher $\mathfrak{M} \subseteq I^{-1}$. Sei daher $\mathfrak{M} = I^{-1}$ angenommen. Es existiert ein Primideal $\mathfrak{P}$ von $\mathfrak{M}$ mit $I \subseteq \mathfrak{P} \subsetneq \mathfrak{M}$. Fixieren wir nun ein $r \in R \cap \mathfrak{P}$, so gibt es Primideale $\mathfrak{P}_1, \ldots, \mathfrak{P}_k$ von $\mathfrak{M}$ mit $\mathfrak{P}_1 \cdot \ldots \cdot \mathfrak{P}_k \subseteq r\mathfrak{M} \subseteq \mathfrak{P}$. Sei k diesbezüglich minimal. Da $\mathfrak{P}$ ein Primideal von $\mathfrak{M}$ ist, enthält es eines der $\mathfrak{P}_i$ und somit folgt $\mathfrak{P} = \mathfrak{P}_i$ für ein i. Seien dann $B := \mathfrak{P}_1 \cdot \ldots \cdot \mathfrak{P}_{i-1}$ und $C := \mathfrak{P}_{i+1} \cdot \ldots \cdot \mathfrak{P}_k$. So folgt

$$\begin{aligned} r^{-1}B\mathfrak{P}C \subseteq \mathfrak{M} &\implies Br^{-1}\mathfrak{P}CB \subseteq B \implies r^{-1}\mathfrak{P}CB \subseteq \mathcal{O}_r(B) = \mathfrak{M} = \mathcal{O}_l(\mathfrak{P}) \\ &\implies r^{-1}CB \subseteq \mathfrak{P}^{-1} = \mathfrak{M} \implies CB \subseteq r\mathfrak{M}\,. \end{aligned}$$

Dies zeigt, daß k nicht minimal gewesen sein kann. Daher ist $\mathfrak{M} \neq I^{-1}$. □

Korollar 2.5.24 *Es sei I ein R-Gitter. Ist $\mathcal{O}_l(I)$ maximal, dann gilt $II^{-1} = \mathcal{O}_l(I)$. Ist $\mathcal{O}_r(I)$ maximal, so gilt $I^{-1}I = \mathcal{O}_r(I)$.*

Beweis: Es sei $\mathfrak{M} := \mathcal{O}_l(I)$ maximal. Dann ist $J := II^{-1}$ ein zweiseitiges $\mathfrak{M}$-Ideal, welches wegen $J = II^{-1} \subseteq \mathfrak{M}$ ganz ist. Weiter gilt $II^{-1}J^{-1} = JJ^{-1} \subseteq \mathfrak{M}$. Daher ist $I^{-1}J^{-1} \subseteq I^{-1}$, was $J^{-1} \subseteq \mathcal{O}_r(I^{-1}) = \mathcal{O}_l(I) = \mathfrak{M}$ impliziert. Nach Lemma 2.5.23 muß $J = \mathfrak{M}$ gelten. Für $\mathcal{O}_r(I)$ geht der Beweis analog. □

Satz 2.5.25 *Es sei $\mathfrak{M}$ eine Maximalordnung. Jedes zweiseitige $\mathfrak{M}$-Ideal ist ein Produkt von Primidealen von $\mathfrak{M}$, und die Darstellung ist eindeutig, bis auf die Anordnung der Faktoren. (Wir vereinbaren $\mathfrak{M}$ sei das leere Produkt.)*
Ferner bilden die zweiseitigen $\mathfrak{M}$-Ideale eine freie abelsche Gruppe, die von den Primidealen von $\mathfrak{M}$ erzeugt wird. $\mathfrak{M}$ ist das neutrale Element und zu I ist I^{-1} das Inverse.

Beweis: Lediglich die erste Aussage und die Kommutativität bedürfen noch eines Beweises.
Existenz: Angenommen, es existieren zweiseitige $\mathfrak{M}$-Ideale die der Behauptung widersprechen. Sei dann I ein maximales Gegenbeispiel. Es ist I sicher kein Primideal von $\mathfrak{M}$. Also existiert ein Primideal $\mathfrak{P}$ von $\mathfrak{M}$ mit $I \subsetneq \mathfrak{P} \subsetneq \mathfrak{M}$. Damit wird $I \subseteq I\mathfrak{P}^{-1} \subseteq \mathfrak{P}\mathfrak{P}^{-1} = \mathfrak{M}$. Nun gilt $I\mathfrak{P}^{-1} \neq \mathfrak{M}$, denn sonst wäre $I = \mathfrak{P}$ nach dem vorhergegangenen Korollar. Andererseits ist $I \neq I\mathfrak{P}^{-1}$, denn sonst müßte $\mathfrak{P}^{-1}$ in $\mathcal{O}_r(I) = \mathfrak{M}$ liegen, was nicht sein kann. Wegen der Wahl von I ist $I\mathfrak{P}^{-1}$ daher ein Produkt von Primidealen von $\mathfrak{M}$. Damit gilt dies auch für I.

Kommutativität: Seien $\mathfrak{P}$ und $\mathfrak{P}'$ zwei verschiedene Primideale von $\mathfrak{M}$. Dann gelten $\mathfrak{P}^{-1}\mathfrak{P}'\mathfrak{P} \subseteq \mathfrak{P}^{-1}\mathfrak{M}\mathfrak{P} = \mathfrak{M}$ und $\mathfrak{P}(\mathfrak{P}^{-1}\mathfrak{P}'\mathfrak{P}) = \mathfrak{P}'\mathfrak{P} \subseteq \mathfrak{P}'$. Wegen $\mathfrak{P} \neq \mathfrak{P}'$ und $\mathfrak{P}'$ prim folgt $\mathfrak{P}^{-1}\mathfrak{P}'\mathfrak{P} \subseteq \mathfrak{P}'$. Damit ist $\mathfrak{P}'\mathfrak{P} \subseteq \mathfrak{P}\mathfrak{P}'$. Vertauschen wir $\mathfrak{P}$ und $\mathfrak{P}'$, so erhalten wir $\mathfrak{P}'\mathfrak{P} = \mathfrak{P}\mathfrak{P}'$.

Eindeutigkeit: Sei $\mathfrak{P}_1 \cdot \ldots \cdot \mathfrak{P}_r = \mathfrak{P}'_1 \cdot \ldots \cdot \mathfrak{P}'_s$. Also gibt es ein i mit $\mathfrak{P}'_i \subseteq \mathfrak{P}_1$ und somit $\mathfrak{P}'_i = \mathfrak{P}_1$. Multiplizieren wir mit $\mathfrak{P}_1^{-1}$ und verwenden die Kommutativität, so gilt (nach eventueller Umnummerierung) $\mathfrak{P}_2 \cdot \ldots \cdot \mathfrak{P}_r = \mathfrak{P}'_2 \cdot \ldots \cdot \mathfrak{P}'_s$. Die Behauptung folgt per Induktion. □

Insbesondere gilt also $(I^{-1})^{-1} = I$ für jedes zweiseitige $\mathfrak{M}$-Ideal I.

Lemma 2.5.26 *Es sei I ein R-Gitter. Ist die Links- oder Rechtsordnung von I maximal, so gelten*

(a) $I^{\#} = I^{-1} \cdot \mathcal{O}_l(I)^{\#} = \mathcal{O}_r(I)^{\#} \cdot I^{-1}$.

(b) $(I^{-1})^{-1} = I$.

Beweis:

(a) Wir setzen $\Lambda := \mathcal{O}_l(I)$. Dann gilt $\mathrm{tr}_{A/K}(II^{-1}\Lambda^{\#}) \subseteq \mathrm{tr}_{A/K}(\Lambda\Lambda^{\#}) \subseteq R$. Daraus folgt $I^{-1}\Lambda^{\#} \subseteq I^{\#}$. Umgekehrt zeigt $\mathrm{tr}_{A/K}(\Lambda II^{\#}) = \mathrm{tr}_{A/K}(II^{\#}) \subseteq R$ die Inklusion

$$II^{\#} \subseteq \Lambda^{\#} \qquad (*)$$

Wir unterscheiden nun zwei Fälle:
Fall 1: Falls $\mathcal{O}_r(I)$ maximal ist, so folgt aus $(*)$ sofort $I^{\#} = I^{-1}II^{\#} \subseteq I^{-1}\Lambda^{\#}$.
Fall 2: Falls Λ eine Maximalordnung ist, so ist $\Lambda^{\#}$ nach Lemma 2.5.15 ein zweiseitiges Λ-Ideal. Aus $(*)$ können wir dann schließen:

$$II^{\#} \subseteq \Lambda^{\#} \implies II^{\#}(\Lambda^{\#})^{-1} \subseteq \Lambda \implies I^{\#}(\Lambda^{\#})^{-1} \subseteq I^{-1} \implies I^{\#} \subseteq I^{-1}\Lambda^{\#}$$

In beiden Fällen haben wir somit $I^{\#} = I^{-1} \cdot \mathcal{O}_l(I)^{\#}$ gezeigt. Der Beweis der Identität $I^{\#} = \mathcal{O}_r(I)^{\#} \cdot I^{-1}$ geht analog.

(b) Falls $\mathcal{O}_l(I)$ maximal ist, so gilt $\mathcal{O}_l(I) = \mathcal{O}_r(I^{-1})$ und es folgt

$$(I^{-1})^{-1} \overset{2.5.15}{=} (I^{-1} \cdot \mathcal{O}_r(I^{-1})^{\#})^{\#} \overset{2.5.6}{=} (I^{-1} \cdot \mathcal{O}_l(I)^{\#})^{\#} \overset{(a)}{=} (I^{\#})^{\#} \overset{2.5.15}{=} I\,.$$

Falls $\mathcal{O}_r(I)$ maximal ist, so schließt man analog. □

Mit Hilfe der Identität $(I^{-1})^{-1} = I$ zeigen wir nun den folgenden fundamentalen

Satz 2.5.27 *Sei I ein R-Gitter. Dann ist $\mathcal{O}_l(I)$ maximal genau dann, wenn $\mathcal{O}_r(I)$ maximal ist.*

Beweis: Sei $\Lambda := \mathcal{O}_l(I)$ maximal und Λ'' eine R-Maximalordnung, welche $\Lambda' := \mathcal{O}_r(I)$ enthält. Weiter sei dann $L := I\Lambda''I^{-1}$. Wegen $1 \in \Lambda = II^{-1}$ und $L \cdot L \subseteq I\Lambda''\Lambda'\Lambda''I^{-1} \subseteq L$ ist L eine R-Ordnung. Damit folgt $\mathcal{O}_r(I^{-1}) \overset{2.5.6}{=} \mathcal{O}_l(I) = \Lambda = \mathcal{O}_l(L) = L = I\Lambda''I^{-1}$. Dies zeigt aber $I\Lambda'' \subseteq (I^{-1})^{-1} = I$ und letztlich $\Lambda'' \subseteq \Lambda'$. Also war $\mathcal{O}_r(I)$ bereits eine R-Maximalordnung. Die Umkehrung des Satzes zeigt man genauso. □

Wir haben die wichtigsten Eigenschaften von normalen R-Gittern gezeigt und wollen diese noch einmal zusammenstellen.

Korollar 2.5.28 *Sind I und J zwei normale R-Gitter, so gelten*

(a) $\mathcal{O}_l(IJ) = \mathcal{O}_l(I)$ *und* $\mathcal{O}_r(IJ) = \mathcal{O}_r(J)$.

(b) $\mathcal{O}_l(I) = \mathcal{O}_r(I^{-1}) = II^{-1}$ *und* $\mathcal{O}_r(I) = \mathcal{O}_l(I^{-1}) = I^{-1}I$.

(c) $(I^{-1})^{-1} = I$.

Definition 2.5.29 Seien Λ_1 und Λ_2 zwei R-Ordnungen. Falls ein R-Gitter I mit $\mathcal{O}_l(I) = \Lambda_1$ und $\mathcal{O}_r(I) = \Lambda_2$ existiert, dann heißen Λ_1 und Λ_2 (durch I) *verbunden*.

Bemerkung 2.5.30 Je zwei R-Maximalordnungen $\mathfrak{M}$ und $\mathfrak{M}'$ sind verbunden. Denn für $I := \mathfrak{M}\mathfrak{M}'$ gilt $\mathcal{O}_l(I) = \mathfrak{M}$ und $\mathcal{O}_r(I) = \mathfrak{M}'$.

Mit den vorangegangenen Ergebnissen erkennt man:

Satz 2.5.31 (Brandtsches Gruppoid) *Die normalen R-Gitter bilden das sogenannte* Brandtsche Gruppoid. *Die Objekte des Gruppoids sind die R-Maximalordnungen. Für zwei R-Maximalordnungen $\mathfrak{M}_1$ und $\mathfrak{M}_2$ ist*

$$\mathrm{Hom}_{Brandt}(\mathfrak{M}_1, \mathfrak{M}_2) = \{I \mid I \text{ ist ein } R\text{-Gitter, } \mathcal{O}_l(I) = \mathfrak{M}_1 \text{ und } \mathcal{O}_r(I) = \mathfrak{M}_2\}\,.$$

Wegen $\mathfrak{M}_1\mathfrak{M}_2 \in \mathrm{Hom}_{Brandt}(\mathfrak{M}_1, \mathfrak{M}_2)$ ist $\mathrm{Hom}_{Brandt}(\mathfrak{M}_1, \mathfrak{M}_2) \neq \emptyset$. Die Komposition zweier Morphismen $\mathfrak{M}_1 \xrightarrow{I} \mathfrak{M}_2$ und $\mathfrak{M}_2 \xrightarrow{J} \mathfrak{M}_3$ ist $I \cdot J$. Das Inverse eines Morphismus $\mathfrak{M}_1 \xrightarrow{I} \mathfrak{M}_2$ ist gegeben durch $\mathfrak{M}_2 \xrightarrow{I^{-1}} \mathfrak{M}_1$.

Definition 2.5.32 Das Produkt $I_1 \cdot \ldots \cdot I_n$ der n R-Ideale I_i wird *echt* genannt, falls $\mathcal{O}_r(I_i) = \mathcal{O}_l(I_{i+1})$ für alle $i \in \{1, \ldots, n-1\}$ gilt.

Zum Abschluß des Abschnitts wollen wir noch ein paar Ergebnisse über echte Produkte und maximal ganze $\mathfrak{M}$-Ideale einer Maximalordnung $\mathfrak{M}$ präsentieren. Der folgende Satz entspricht der Faktorisierung der zweiseitigen $\mathfrak{M}$-Ideale in Primideale von $\mathfrak{M}$.

Satz 2.5.33 *Es sei $\mathfrak{M}$ eine R-Maximalordnung. Weiter sei I ein ganzes $\mathfrak{M}$-Linksideal so, daß der $\mathfrak{M}$-Modul $\mathfrak{M}/I$ endliche Kompositionslänge k besitzt. Dann ist I ein echtes Produkt $I = I_1 \cdot \ldots \cdot I_k$ von maximal ganzen normalen R-Gittern $I_1, \ldots, I_k$. Insbesondere gilt damit $\mathfrak{M} = \mathcal{O}_l(I) = \mathcal{O}_l(I_1)$ und $\mathcal{O}_r(I) = \mathcal{O}_r(I_k)$.*

Beweis: Der Fall $k = 1$ ist klar. Sei daher $k > 1$ und I_1 ein maximal ganzes $\mathfrak{M}$-Linksideal mit $I \subsetneq I_1 \subsetneq \mathfrak{M}$. Dann hat I_1/I Kompositionslänge $k-1$. Setzen wir $\mathfrak{M}' := \mathcal{O}_r(I_1)$, so ist $I_1^{-1}I$ ein $\mathfrak{M}'$-Linksideal. Jeder $\mathfrak{M}$-Linksmodul M mit $I \subseteq M \subseteq I'$ korrespondiert nun via $M \mapsto I_1^{-1}M$ zu einem $\mathfrak{M}'$-Linksmodul M' mit $I_1^{-1}I \subseteq M' \subseteq \mathfrak{M}'$. Damit besitzt auch der $\mathfrak{M}'$-Linksmodul $\mathfrak{M}'/I_1^{-1}I$ Kompositionslänge $k-1$. Nach der Induktionshypothese gibt es daher ein echtes Produkt $I_1^{-1}I = I_2 \cdot \ldots \cdot I_k$ mit geeigneten maximal ganzen normalen R-Gittern. Also gilt $I = I_1 \cdot \ldots \cdot I_k$ und $\mathcal{O}_r(I_1) = \mathcal{O}_l(I_1^{-1}I) = \mathcal{O}_l(I_2)$. □

Lemma 2.5.34

(a) Ein echtes Produkt von ganzen normalen R-Gittern ist ganz.

(b) Seien I und J zwei normale R-Gitter. Dann gilt $I \subseteq J$ genau dann, wenn es ein echtes Produkt $I = I_1 \cdot J \cdot I_2$ mit zwei ganzen normalen R-Gittern I_1 und I_2 gibt.

Beweis:

(a) Ist IJ ein echtes Produkt zweier normaler R-Gitter, so gilt

$$IJ \subseteq I\mathcal{O}_l(J) = I\mathcal{O}_r(I) = I \subseteq \mathcal{O}_l(I) = \mathcal{O}_l(IJ)\,.$$

Die Behauptung folgt nun durch Induktion.

(b) Ist $I = I_1 \cdot J \cdot I_2$, so folgt $I \subseteq \mathcal{O}_r(I_1) \cdot J \cdot \mathcal{O}_l(I_2) = \mathcal{O}_r(J) \cdot J \cdot \mathcal{O}_l(J) = J$. Sei daher nun $I \subseteq J$ angenommen. Wir setzen $I_1 := I(\mathcal{O}_l(J)I)^{-1}$ sowie $I_2 := J^{-1}I$. Dies sind normale R-Gitter und es gilt:

$$(\mathcal{O}_l(J)I)^{-1}I = ((\mathcal{O}_l(J)I)^{-1} \cdot \mathcal{O}_l(J)) \cdot I = \mathcal{O}_r((\mathcal{O}_l(J)I)^{-1}) = \mathcal{O}_r(I)\,. \qquad (*)$$

Mit $(*)$ folgt $I = I_1 \cdot J \cdot I_2$. Weiter ist das Produkt echt. Wegen $(*)$ gilt $(\mathcal{O}_l(J)I)^{-1} \subseteq I^{-1}$ und somit $I_1 \subseteq II^{-1} = \mathcal{O}_l(I_1)$. Außerdem ist $I_2 = J^{-1}I \subseteq J^{-1}J = \mathcal{O}_l(I_2)$. Also sind I_1 und I_2 ganz. □

Korollar 2.5.35 *Ist I ein normales ganzes R-Gitter, so ist I genau dann ein maximal ganzes $\mathcal{O}_l(I)$-Linksideal, wenn I ein maximal ganzes $\mathcal{O}_r(I)$-Rechtsideal ist.*

Beweis: Angenommen, I ist ein maximal ganzes $\mathcal{O}_r(I)$-Rechtsideal. Wegen $I \subsetneq \mathcal{O}_r(I)$ ist I keine R-Ordnung. Also gilt $I \subsetneq \mathcal{O}_l(I)$. Angenommen, es gäbe nun ein $\mathcal{O}_l(I)$-Linksideal J mit $I \subseteq J \subsetneq \mathcal{O}_l(I)$. Nach dem vorherigen Lemma gibt es dann ein echtes Produkt $I = I_1 \cdot J \cdot I_2$ mit ganzen R-Gittern I_1 und I_2. In dem Beweis des Lemmas haben wir gezeigt, daß man $I_1 = I(\mathcal{O}_l(J)I)^{-1}$ wählen kann. Hier ist nun $\mathcal{O}_l(I) = \mathcal{O}_l(J)$, also ist $I_1 = \mathcal{O}_l(I)$ und damit $I = J \cdot I_2$. Wegen $J \neq \mathcal{O}_l(I)$ folgt nun $I = JI_2 \subsetneq \mathcal{O}_r(J)I_2 = I_2 \subseteq \mathcal{O}_r(I_2) = \mathcal{O}_r(I)$. Daher ist $I_2 = \mathcal{O}_r(I)$ und somit $I = J$. Der Fall, daß $\mathcal{O}_l(I)$ maximal ist, geht analog. □

Damit ist die Asymmetrie der Definition von „maximal ganz“ nun aufgehoben.

Satz 2.5.36 *Es sei $\mathfrak{M}$ eine R-Maximalordnung. Ein ganzes $\mathfrak{M}$-Linksideal I ist genau dann ein maximal ganzes $\mathfrak{M}$-Linksideal, wenn es ein Primideal $\mathfrak{p}$ von R derart gibt, daß $I_\mathfrak{p}$ ein maximal ganzes $\mathfrak{M}_\mathfrak{p}$-Linksideal ist und $I_{\mathfrak{p}'} = \mathfrak{M}_{\mathfrak{p}'}$ für alle von $\mathfrak{p}$ verschiedenen Primideale $\mathfrak{p}'$ von R gilt. Ist dies der Fall, so ist $\mathfrak{p} = I \cap R$.*
Analoges gilt für die Komplettierungen und $\mathfrak{M}$-Rechtsideale.

Beweis: Wir können $I \subsetneq \mathfrak{M}$ annehmen. Dann gilt $I_\mathfrak{p} \subseteq \mathfrak{M}_\mathfrak{p}$ für alle $\mathfrak{p} \underset{\max}{\lhd} R$. Wegen $I \subsetneq \mathfrak{M}$ gibt es mindestens ein $\mathfrak{p} \underset{\max}{\lhd} R$ mit $I_\mathfrak{p} \subsetneq \mathfrak{M}_\mathfrak{p}$. Bezeichnen wir nun mit $J_\mathfrak{p}$ ein maximal ganzes $\mathfrak{M}_\mathfrak{p}$-Linksideal, welches $I_\mathfrak{p}$ enthält. Dann ist $J := \mathfrak{M} \cap J_\mathfrak{p}$ ein ganzes $\mathfrak{M}$-Linksideal ungleich $\mathfrak{M}$ welches I umfasst. Weiter ist $J_\mathfrak{p}$ die Lokalisierung von J an $\mathfrak{p}$ und für alle Primideale $\mathfrak{p}' \neq \mathfrak{p}$ gilt $J_{\mathfrak{p}'} = \mathfrak{M}_{\mathfrak{p}'}$.

Ist I ein maximal ganzes $\mathfrak{M}$-Linksideal, so stimmen I und J an allen Lokalisierungen überein. Weiter ist dann $J_{\mathfrak{p}'} \cap R_{\mathfrak{p}'} = R_{\mathfrak{p}'}$ für alle Primideale $\mathfrak{p}' \neq \mathfrak{p}$. Bezeichnet $\mathfrak{P}$ das zu $J_\mathfrak{p}$ gehörende Primideal von $\mathfrak{M}_\mathfrak{p}$ gemäß Lemma 2.5.21, so haben wir dort in Teil (a) $\mathfrak{P} \cap R_\mathfrak{p} = \mathfrak{p}R_\mathfrak{p}$ und in Teil (b) $\mathfrak{P} \cap R_\mathfrak{p} = J_\mathfrak{p} \cap R_\mathfrak{p}$ gezeigt. Also gilt $I \cap R = \mathfrak{p}$.

Ist I kein maximal ganzes $\mathfrak{M}$-Linksideal, so ist $I \subsetneq J$, denn J ist nach dem gerade Gezeigten ein maximal ganzes $\mathfrak{M}$-Linksideal. Also gibt es ein Primideal $\mathfrak{q}$ von R mit $I_\mathfrak{q} \subsetneq J_\mathfrak{q}$. □

2.6 Äquivalenzklassen von Idealen und Ordnungen

Definition 2.6.1 Zwei R-Ordnungen Λ_1 und Λ_2 heißen *konjugiert* (oder *vom selben Typ*), falls $\Lambda_1 = d\Lambda_2 d^{-1}$ für ein $d \in A^*$ gilt.
Zwei R-Gitter I und J heißen *linksäquivalent* (respektive *rechtsäquivalent*), falls $I = dJ$ (respektive $I = Jd$) für ein $d \in A^*$ ist.
Wir schreiben dann $I \sim_l J$ bzw. $\Lambda_1 \sim \Lambda_2$.

Bemerkung 2.6.2 Sind zwei R-Ordnungen konjugiert, so sind sie isomorph. Ist A eine zentraleinfache K-Algebra und sind umgekehrt zwei R-Ordnungen isomorph, so lässt sich der Isomorphismus zu einem K-Algebrenautomorphismus auf A fortsetzen. Dieser wird nach dem Satz von Skolem-Noether durch Konjugation mit einem Element $d \in A^*$ induziert. Zwei R-Ordnungen in einer zentraleinfachen K-Algebra sind daher genau dann zueinander konjugiert, wenn sie isomorph zueinander sind.

Bemerkung 2.6.3 Sind zwei R-Gitter linksäquivalent, so haben sie dieselbe Rechtsordnung Λ und sind isomorph als Λ-Rechtsmoduln.
Nehmen wir umgekehrt an, die beiden Λ-Rechtsideale I und J seien isomorph. Dieser Isomorphismus lässt sich auf A fortsetzen und ist daher durch die Linksmultiplikation mit einem $d \in A^*$ gegeben. D.h. die Definition der Linksäquivalenz zweier R-Gitter entspricht gerade der Isomorphie zweier Λ-Rechtsmoduln.
Entsprechendes gilt für die Rechtsäquivalenz.

Wegen $(dI)^{-1} = I^{-1}d^{-1}$ für alle $d \in A^*$ und alle normalen R-Gitter I folgt: Zwei normale R-Gitter I und J sind genau dann linksäquivalent, wenn I^{-1} und J^{-1} rechtsäquivalent sind. Damit induziert $I \mapsto I^{-1}$ eine Bijektion zwischen den Links- und Rechtsidealklassen einer Maximalordnung.

Bemerkung 2.6.4 Zwei normale R-Gitter I und J mit $\mathcal{O}_l(I) = \mathcal{O}_r(I)$ und $\mathcal{O}_l(J) = \mathcal{O}_r(J)$ sind genau dann linksäquivalent, wenn sie rechtsäquivalent sind. In diesem Fall ist es somit angebracht, lediglich von Äquivalenz sprechen. Weiter bilden die Äquivalenzklassen eine abelsche Gruppe.

Beweis: Angenommen, es sei $I = dJ$ für ein $d \in A^*$. Die beiden R-Gitter besitzen dann dieselbe Rechts- bzw. Linksordnung $\mathfrak{M}$. Weiter ist $d\mathfrak{M} = IJ^{-1}$ ein zweiseitiges $\mathfrak{M}$-Ideal. Wegen $\mathfrak{M} = \mathcal{O}_l(IJ^{-1}) = \mathcal{O}_l(d\mathfrak{M}) = d\mathfrak{M}d^{-1}$ ist $d\mathfrak{M} = \mathfrak{M}d$. Es folgt

$$I = dJ = (d\mathfrak{M}) \cdot J = J \cdot (d\mathfrak{M}) = J \cdot (\mathfrak{M}d) = Jd \,,$$

da die zweiseitigen $\mathfrak{M}$-Ideale nach Satz 2.5.25 eine abelsche Gruppe bilden. Daß die Äquivalenzklassen eine abelsche Gruppe bilden, rechnet man nun leicht nach. □

Satz 2.6.5 *Je zwei linksäquivalente normale R-Gitter besitzen dieselbe Rechtsordnung und konjugierte Linksordnungen.*
Sind umgekehrt zwei normale R-Gitter I und J mit $\mathcal{O}_r(I) = \mathcal{O}_r(J)$ und konjugierten Linksordnungen gegeben, dann existiert ein zweiseitiges $\mathcal{O}_l(J)$-Ideal J' mit $I \sim_l J'J$. Weiter ist die Äquivalenzklasse von J' eindeutig bestimmt.

Beweis: Ist $I = dJ$ mit $d \in A^*$, so gilt $\mathcal{O}_l(I) = \mathcal{O}_l(dJ) = d\mathcal{O}_l(J)d^{-1}$.
Sei nun umgekehrt $\mathcal{O}_l(I) = d\mathcal{O}_l(J)d^{-1}$, so kann man $J' := d^{-1}IJ^{-1}$ wählen. Ist J'' ein weiteres zweiseitiges $\mathcal{O}_l(J)$-Ideal mit $I \sim_l J''J$, so folgt $J'J \sim_l J''J$ und damit $J' \sim_l J''$. □

Korollar 2.6.6 *Ist $\mathfrak{M}$ eine R-Maximalordnung und $\{I_i \mid i \in \mathcal{I}\}$ ein Vertretersystem von Rechtsidealklassen von $\mathfrak{M}$ bezüglich Linksäquivalenz, so enthält $\{\mathcal{O}_l(I_i) \mid i \in \mathcal{I}\}$ aus jeder Konjugationsklassen von R-Maximalordnungen wenigstens einen Vertreter.*

Beweis: Sei $\mathfrak{M}'$ eine R-Maximalordnung, so ist $\mathfrak{M}'\mathfrak{M}$ ein $\mathfrak{M}$-Rechtsideal, also linksäquivalent zu einem der I_i. Damit sind $\mathfrak{M}'$ und $\mathcal{O}_l(I_i)$ äquivalent. □

Korollar 2.6.7 *Ist $\mathfrak{M}$ eine R-Maximalordnung, $\{\mathfrak{M}_i \mid i \in \mathcal{I}\}$ ein Vertretersystem der Konjugationsklassen von R-Maximalordnungen und $\{I_{i,j} \mid j \in \mathcal{I}_i\}$ ein Repräsentantensystem der zweiseitigen $\mathfrak{M}_i$-Ideale, so ist $\{I_{i,j}\mathfrak{M} \mid j \in \mathcal{I}_i, i \in \mathcal{I}\}$ ein Vertretersystem der Rechtsidealklassen von $\mathfrak{M}$ bezüglich Linksäquivalenz.*

Beweis: Es sei I ein $\mathfrak{M}$-Rechtsideal. Wir zeigen zunächst, daß es ein Paar (i,j) derart gibt, daß $I \sim_l I_{i,j}\mathfrak{M}_i$ gilt. Es gibt ein i so, daß $\mathfrak{M}_i \sim \mathcal{O}_l(I)$. Damit besitzen I und $\mathfrak{M}_i\mathfrak{M}$ dieselbe Rechtsordnung und konjugierte Linksordnungen. Also existiert nach Satz 2.6.5 ein $j \in \mathcal{I}_i$ mit $I \sim_l I_{i,j}\mathfrak{M}_i\mathfrak{M} = I_{i,j}\mathfrak{M}$.
Nun zur Eindeutigkeit von i und j: Angenommen, es wäre $I_{i,j}\mathfrak{M} \sim_l I_{k,l}\mathfrak{M}$. Nach Satz 2.6.5 gilt $\mathfrak{M}_i = \mathcal{O}_l(I_{i,j}\mathfrak{M}) \sim \mathcal{O}_l(I_{k,l}\mathfrak{M}) = \mathcal{O}_l(\mathfrak{M}_k)$. Also ist $i = k$. Mit Satz 2.6.5 folgt damit dann $j = l$. □

Analog repräsentiert $\{\mathfrak{M}I_{i,j} \mid j \in \mathcal{I}_i, i \in \mathcal{I}\}$ alle Linksidealklassen von $\mathfrak{M}$ bezüglich Rechtsäquivalenz.

2.7 Zentraleinfache Algebren über diskret bewerteten Körpern

2.7.1 Schiefkörper

Es sei R ein vollständiger diskreter Bewertungsring mit Quotientenkörper K und maximalem Ideal $R\pi$. Weiter sei D ein Schiefkörper mit Zentrum K und $m^2 = [D : K]$.

Die zu R gehörende diskrete Bewertung auf K sei $v\colon K \to \mathbb{Z} \cup \{\infty\}$. Ohne Einschränkung ist v surjektiv.

Lemma 2.7.1 *Ist $a_nX^n + \cdots + a_1X + a_0 \in K[X]$ irreduzibel, so gilt*

$$v(a_i) \geq \min(v(a_n), v(a_0)) \quad \textit{für alle } 0 \leq i \leq n\,.$$

Beweis: Der Beweis beruht auf Hensels Lemma siehe [Rei03, Theorem 12.2, S. 135].□

Wir definieren nun

$$w\colon D \to \frac{1}{m}\mathbb{Z} \cup \{\infty\}, \quad x \mapsto \frac{1}{m}v(\mathrm{nr}_{D/K}(x))$$

und

$$\Delta := \{x \in D \mid w(x) \geq 0\}\,.$$

Lemma 2.7.2 *Für alle $x \in D$ sind folgende Aussagen äquivalent:*

(a) x ist ganz über R.

(b) $\mathrm{nr}_{D/K}(x) \in R$.

(c) $w(x) \geq 0$.

Beweis:
$(a) \Longrightarrow (b)$ wurde bereits in Satz 2.5.7 gezeigt.

$(b) \Longrightarrow (a)$ $\mathrm{Nr}(x) = \mathrm{nr}_{D/K}(x)^m \in R$ ist (bis auf das Vorzeichen) eine Potenz von $\mu_{x,K}(0)$. Also ist $v(\mu_{x,K}(0)) \geq 0$. Da $\mu_{x,K}(X)$ irreduzibel ist, folgt aus dem vorherigen Lemma $\mu_{x,K}(X) \in R[X]$.

$(b) \Longleftrightarrow (c)$ ist klar. □

Satz 2.7.3 *w ist eine diskrete Bewertung auf D, welche v fortsetzt.*

Beweis: Seien $x, y \in D$. So ist $w(x) = \infty \iff \mathrm{nr}_{D/K}(x) = 0 \iff x = 0$. Außerdem gilt $w(xy) = w(x)+w(y)$, da nr multiplikativ und v eine diskrete Bewertung ist. Weiter können wir $w(x) \geq w(y)$ annehmen. Dann ist $w(xy^{-1}) \geq 0$, d.h. xy^{-1} ist ganz über R. Aus Lemma 2.5.2 folgt, daß auch $1 + xy^{-1}$ ganz über R ist. Damit erhalten wir

$$w(x + y) = w(1 + xy^{-1}) + w(y) \geq w(y) = \min(w(x), w(y)).$$

Damit ist w eine diskrete Bewertung. Für jedes $x \in K$ gilt $w(x) = \frac{1}{m}v(x^m) = v(x)$. □

Definition 2.7.4 Ein Element $\pi_D \in D$ mit minimaler positiver Bewertung bezüglich w wollen wir *Primelement von D* nennen.

Im Folgenden bezeichne π_D ein Primelement von D.

Satz 2.7.5 *Es ist Δ der ganze Abschluß von R in D und somit die einzige R-Maximalordnung von D. Die Einheitengruppe von Δ ist $\Delta^* = \{x \in D \mid w(x) = 0\}$.*
Weiter sind alle normalen R-Gitter von der Form $\pi_D^k\Delta = \Delta\pi_D^k$ mit $k \in \mathbb{Z}$ und es gilt $\pi_D\Delta = \mathrm{rad}(\Delta) = \Delta\pi_D$.

Insbesondere ist jedes normale R-Gitter ein projektiver Δ-Modul.

Beweis: Da w eine diskrete Bewertung ist, welche v fortsetzt, bildet Δ einen Ring welcher R umfaßt. Weiter gilt $K\Delta = D$. Außerdem besteht Δ gerade aus den ganzen Elementen von D. Nach Satz 2.5.7 ist Δ somit eine R-Ordnung und enthält seinerseits alle anderen R-Ordnungen von D. Insbesondere ist jedes normale R-Gitter ein zweiseitiges Δ-Ideal.
Sei nun I ein zweiseitiges Δ-Ideal. Dann gibt es ein $x \in I$ mit $w(x) = \min(w(I))$. Ist $y \in I$ beliebig, so folgt $w(x^{-1}y) \geq 0$, also $y = x(x^{-1}y) \in x\Delta$. Also ist $I = x\Delta$. Genauso folgt $I = \Delta x$. Wegen $w(D^*) = w(\pi_D)\mathbb{Z} = \{w(\pi_D^k) \mid k \in \mathbb{Z}\}$ gibt es nun ein $k \in \mathbb{Z}$ mit $w(x) = w(\pi_D^k)$. Damit folgt $I = x\Delta = \pi_D^k\Delta = \Delta x = \Delta\pi_D^k$. Da $\pi_D\Delta$ das einzige maximal ganze Δ-Rechtsideal ist, gilt ferner $\pi_D\Delta = \mathrm{rad}(\Delta) = \Delta\pi_D$. □

Wir setzen $\overline{\Delta} := \Delta/\pi_D\Delta$ und $\overline{R} := R/\pi R$. Gerade haben wir gezeigt, daß $\overline{\Delta}$ ein Schiefkörper ist. Wegen $\pi_D\Delta \cap R = \pi R$ ist $\overline{\Delta}$ ein Vektorraum über $\overline{R}$.

Definition 2.7.6 Es existiert also ein $e \geq 1$ derart, daß $e \cdot w(D^*) = \mathbb{Z}$ gilt. Dieses e heißt der *Verzweigungsindex* von D/K. Weiter bezeichne $f := [\overline{\Delta} : \overline{R}]$ den *Trägheitsindex* von D/K.

Satz 2.7.7 *Mit den obigen Bezeichnungen gilt $e \cdot f = m^2$.*
Genauer: Sind $a_1, \ldots, a_f \in \Delta$ derart, daß ihre Bilder eine $\overline{R}$-Basis von $\overline{\Delta}$ bilden, und $b_0, \ldots, b_{e-1} \in \Delta$ mit $w(b_i) \not\equiv w(b_j) \mod \frac{1}{e}\mathbb{Z}$ für alle $i \neq j$, dann ist $\{a_i b_j \mid 1 \leq i \leq f,\ 0 \leq j \leq e-1\}$ eine R-Basis von Δ.

Beweis: Wir zeigen zunächst die lineare Unabhängigkeit von $\{a_i b_j\}$. Dabei wird sich auch f als endlich herausstellen. Angenommen, es gibt eine nichttriviale K-Linearkombination

$$\sum_{j=0}^{e-1} \left(\sum_{i=1}^{s} \lambda_{ji} a_i \right) b_j = 0 \,, \qquad (*)$$

so dürfen wir annehmen, daß es für jedes j ein $\lambda_{ji} \neq 0$ gibt. Ansonsten führe man den Beweis mit weniger b_j. Damit ist jedes $n_j := \min\{v(\lambda_{j1}), \ldots, v(\lambda_{js})\}$ endlich. Nun ersetzen wir alle λ_{ji} durch $\pi^{-n_j}\lambda_{ji} \in R$ und b_j durch $\pi^{n_j} b_j$. Damit bleibt $(*)$ gültig und die abgeänderten b_j erfüllen immer noch die Voraussetzung. Weiter sind alle $\lambda_{ji} \in R$ und für jedes j liegt mindestens eines der λ_{ji} nicht in πR. Nach einer Umnummerierung können wir $w(b_0) < \cdots < w(b_{e-1})$ und $\lambda_{01} \notin \pi R$ annehmen. Dies liefert

$$\sum_{j=0}^{e-1} \left(\sum_{i=1}^{s} \lambda_{ji} a_i \right) b_j b_0^{-1} = 0 \quad \text{mit } b_j b_0^{-1} \in \pi_D \Delta \text{ für alle } j \geq 1 \,.$$

Reduzieren wir nun modulo $\pi_D\Delta$, so erhalten wir eine nichttriviale Linearkombination $\sum_i \overline{\lambda}_{1i}\overline{a}_i = 0$, was der Wahl der a_i widerspricht. Damit ist $\{a_i b_j\}$ linear unabhängig und $e \cdot f \leq m^2$.

Nun zeigen wir, daß $\{a_i b_j\}$ ein R-Erzeugendensystem von Δ ist. Sei dazu $x \in \Delta \setminus \{0\}$. Dann ist $w(x) = k + \frac{j}{e}$ mit $k \geq 0$ und $0 \leq j < e$. Daher gilt $x = (\pi^k b_j)u$ für ein $u \in \Delta^*$. Dieses u besitzt eine Darstellung $u = \sum_{i=1}^{f} r_i a_i + x_1$ mit $r_i \in R$ und $x_1 \in \pi_D\Delta$. Damit wird $x = \sum_i (r_i \pi^k a_i) b_j + x_1$ mit $w(x) < w(x_1)$. Ist $x_1 \neq 0$, so wiederholen wir diese Konstruktion. Nach $n \cdot e$ Schritten erhalten wir

$$x = \sum_{j=0}^{e-1} \sum_{i=1}^{f} \left(\sum_{l=1}^{n} r_{ij}^{(l)} \pi^{k-1+\gamma_{ij}^{(l)}} \right) a_i b_j + y_n \text{ mit } \gamma_{ij}^{(l)} \geq l,\ w(y_n) \geq w(x) + n \,. \qquad (\dagger)$$

Für alle i, j bildet die Folge $\left(\sum_{l=1}^{n} r_{ij}^{(l)} \pi^{k-1+\gamma_{ij}^{(l)}} \right)_n$ eine Cauchyfolge in R und besitzt daher einen Grenzwert $s_{ij} \in R$. Setzen wir $x' := \sum_{ij} s_{ij} a_i b_j \in \Delta$, so folgt aus $(\dagger)$ für alle $n \geq 1$ die Ungleichung $w(x - x') \geq \min(w(y_n), k + n - 1)$. Dies zeigt $x = x'$, und daher ist $\{a_i b_j\}$ ein R-Erzeugendensystem von Δ. Somit ist auch $ef \geq m^2$. □

Korollar 2.7.8 *Ist $\overline{R}$ ein endlicher Körper, so gilt $e = f = m$.*

Beweis: In diesem Fall ist $\overline{\Delta}$ ein endlicher Schiefkörper, also nach Korollar 2.1.17 ein Körper. Weiter gibt es dann ein $a \in \Delta$ mit $\overline{\Delta} = \overline{R}(\overline{a})$. Nun gilt $m \geq [K(a) : K] \geq [\overline{R}(\overline{a}) : \overline{R}] = f$. Wegen $1 \leq e \leq m$ und $ef = m^2$ folgt die Behauptung. □

Satz 2.7.9 *Ist $\overline{R}$ ein endlicher Körper mit q Elementen, so gibt es eine primitive $(q^m - 1)$-te Einheitswurzel ζ in D. Es ist $L := K[\zeta]$ ein maximaler Teilkörper von D. Weiter ist L/K die bis auf Isomorphie eindeutig bestimmte unverzweigte Erweiterung von K von Grad m.*

Beweis: Ist $\overline{R} \cong \mathbb{F}_q$, so ist $\overline{\Delta}$ isomorph zu $\mathbb{F}_{q^m}$. Also hat das separable Polynom $X^{q^m-1} - 1 \in \overline{R}[X]$ in $\overline{\Delta}$ gerade $q^m - 1$ verschiedene Nullstellen. Diese lassen sich mit Hensels Lemma zu (verschiedenen) Nullstellen in Δ liften. Da $\overline{\Delta}$ eine primitive $(q^m - 1)$-te Einheitswurzel besitzt, gilt dies auch für Δ. Nach [Rei03, Theorem 5.8, S. 72] Teil (ii) ist L/K eine total unverzweigte Erweiterung von Grad m. Sei $L' \subset D$ ein Körper so, daß L'/K eine unverzweigte Erweiterung vom Grad m ist. Dann sind L und L' nach [Rei03, Theorem 5.8, S. 72] K-isomorph. Nach dem Satz von Skolem-Noether sind L und L' dann konjugiert. □

Bemerkung 2.7.10 Es gelten die obigen Bezeichnungen. Dann ist $\Delta = R[\zeta, \pi_D] := \sum_{i,j=0}^{m-1} R\zeta^i \pi_D^j$ bzw. $D = K[\zeta, \pi_D]$ nach Satz 2.7.7. Nach [Rei03, Theorem 5.8, S. 72] Teil (ii) ist der Bewertungsring O_L von L gerade $R[\zeta]$ und es gilt $\overline{O}_L := O_L/\pi O_L = \overline{R}[\overline{\zeta}]$. Es sei $\overline{R} \cong \mathbb{F}_q$. $\overline{R}[\overline{\zeta}]/\overline{R}$ ist eine separable Körpererweiterung. Die Galoisgruppe $\mathrm{Gal}(\overline{R}[\overline{\zeta}]/\overline{R})$ wird erzeugt vom Frobeniusautomorphismus $\overline{\zeta} \mapsto \overline{\zeta}^q$. Nach Teil (iv) von [Rei03, Theorem 5.8, S. 72] ist damit auch L/K galoisch und $\mathrm{Gal}(L/K)$ wird erzeugt von $\zeta \mapsto \zeta^q$.

Satz 2.7.11 *Es gelten die Voraussetzungen wie in Satz 2.7.9. Dann gibt es ein Primelement π'_D von D und ein $1 \leq r \leq m$ mit $\mathrm{ggT}(r, m) = 1$ so, daß $\pi'_D \zeta {\pi'_D}^{-1} = \zeta^{q^r}$ gilt und ${\pi'_D}^m$ ein Primelement von R ist.*

Beweis: Wegen dem K-Automorphismus $\zeta \mapsto \zeta^q$ gibt es nach dem Satz von Skolem-Noether ein $d \in D$ mit $d\zeta d^{-1} = \zeta^q$. Nachdem wir d mit einer geeigneten Potenz von π multipliziert haben, gilt $j := m \cdot w(d) \in \{0, \ldots, m-1\}$. Sei $h := \frac{m}{\mathrm{ggT}(j,m)}$. Dann gilt $d^h = u\pi^b$ für ein $b \geq 0$ und $u \in \Delta^*$, und h ist die kleinste positive Zahl mit dieser Eigenschaft. Es folgt

$$\zeta^{q^h} = d^h \zeta d^{-h} = u\pi^b \zeta \pi^{-b} u^{-1} = u\zeta u^{-1} \equiv \zeta \mod \pi_D \Delta$$

da $\overline{\Delta}$ ein Körper ist. Da $\overline{\zeta}$ eine primitive (q^m-1)-te Einheitswurzel in $\overline{\Delta}$ ist, folgt $h = m$ und somit $\mathrm{ggT}(j, m) = 1$. Seien nun $r, t \in \mathbb{Z}$ mit $rj - tm = 1$ und $1 \leq r \leq m$. Wir setzen $\pi'_D := \pi^{-t} d^r$. Damit gilt $\pi'_D \zeta {\pi'_D}^{-1} = \zeta^{q^r}$ und $w(\pi'_D) = rw(d) - tw(\pi) = rj/m - t = 1/m$. Also ist π'_D ein Primelement von D. Da ${\pi'_D}^m$ mit π'_D und ζ vertauscht, liegt es in $Z(D) = K$. Wegen $w({\pi'_D}^m) = 1$ ist ${\pi'_D}^m$ ein Primelement von R. □

Man kann π'_D so wählen, daß ${\pi'_D}^m$ ein vorher festgelegtes Primelement von R ist. Wir werden diese Tatsache im folgenden aber nicht verwenden, sondern von nun an $\pi := \pi_D^m$ wählen.

Sei wieder $L := K(\zeta)$. Dann wollen wir einen Isomorphismus von $L \otimes_K D$ nach $L^{m\times m}$ angeben.

Bemerkung 2.7.12 Sei r wie im obigen Satz. Erfülle das Primelement π_D von D die Identität $\pi_D \zeta \pi_D^{-1} = \zeta^{q^r}$. Sei dann $\theta \in \mathrm{Gal}(L/K)$ mit $\theta(\zeta) = \zeta^{q^r}$. Wir setzen

$$\pi_D^* := \begin{pmatrix} 0 & I_{m-1} \\ \pi & 0 \end{pmatrix} \in L^{m\times m}\,.$$

Für alle $\alpha \in L$ sei $\alpha^* := \mathrm{diag}\,(\alpha, \theta(\alpha), \ldots, \theta^{m-1}(\alpha))$. Dann ist die durch

$$\varphi\colon L \otimes_K D \to L^{m\times m}, \quad 1 \otimes \sum_{i,j=0}^{m} \pi_D^i \zeta^j \mapsto \sum_{i,j=0}^{m} (\pi_D^*)^i (\zeta^*)^j$$

definierte L-lineare Abbildung ein Isomorphismus von L-Algebren.

Beweis: Wie man leicht nachrechnet, gilt $(\pi_D^*)^m = \pi I_m$ und $\pi_D^* \zeta^* (\pi_D^*)^{-1} = (\zeta^*)^{q^r}$. Daher genügt es zu zeigen, daß φ ein Isomorphismus von L-Vektorräumen ist. Sicherlich liegt $D' := K[\zeta^*, \pi_D^*]$ im Bild von φ. Also haben wir zu zeigen, daß $\dim_K(D') = m^2$ ist, denn dann ist auch $\dim_L(\varphi(L \otimes_K A)) = m^2 = \dim_L(L \otimes_K A)$.
Jedes $a \in D'$ besitzt eine Darstellung $a = \sum_{j=0}^{m-1} \alpha_j^* (\pi_D^*)^j$ mit geeigneten $\alpha_j \in L$. Wegen

$$(\pi_D^*)^j = \begin{pmatrix} 0 & I_{m-j} \\ \pi I_j & 0 \end{pmatrix}$$

folgt

$$a = \begin{pmatrix} \alpha_0 & \alpha_1 & \alpha_2 & \cdots & \alpha_{m-1} \\ \pi\theta(\alpha_{m-1}) & \theta(\alpha_0) & \theta(\alpha_1) & \cdots & \theta(\alpha_{m-2}) \\ \pi\theta^2(\alpha_{m-2}) & \pi\theta^2(\alpha_{m-1}) & \theta^2(\alpha_0) & \cdots & \theta^2(\alpha_{m-3}) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \pi\theta^{m-1}(\alpha_1) & \pi\theta^{m-1}(\alpha_2) & \pi\theta^{m-1}(\alpha_3) & \cdots & \theta^{m-1}(\alpha_0) \end{pmatrix} \tag{2.1}$$

Insbesondere ist $a = 0$ genau dann, wenn alle $\alpha_i = 0$ sind. Also ist D' ein m-dimensionaler L-Vektorraum, und somit ist $\dim_K(D') = m^2$, was zu zeigen war. □

Insbesondere sei vermerkt, daß für die obige Wahl von π_D und π gilt

$$\mathrm{nr}_{D/K}(\pi_D) = \det(\pi_D^*) = \pi_D^m = \pi \quad \text{und} \quad \mathrm{Nr}_{D/K}(\pi_D) = \pi^m\,.$$

2.7.2 Der vollständige Fall

Sei R ein vollständiger diskreter Bewertungsring und $K = \mathrm{Quot}(R)$. Weiter sei D ein Schiefkörper mit Zentrum K und Δ die eindeutig bestimmte R-Maximalordnung von D. Um die R-Maximalordnungen und die normalen R-Gitter in einer beliebigen zentraleinfachen K-Algebra zu bestimmen, benötigen wir zunächst einige kategorielle Begriffe:

Definition 2.7.13 Ein Ring heißt *erblich*, falls jedes seiner Rechtsideale projektiv ist.

Lemma 2.7.14 *Ein Ring S ist genau dann erblich, wenn jeder Teilmodul eines freien endlich erzeugten S-Rechtsmoduls isomorph zu einer direkten Summe von Rechtsidealen von S ist.*

Beweis: Sei S erblich. Sei M ein freier S-Rechtsmodul mit Basis $(m_1, \ldots, m_k)$, und sei N ein Rechtsteilmodul von M. Ist $k \leq 1$, so ist nichts zu zeigen. Sei sei daher $k > 1$ und bezeichne $\pi\colon M = \bigoplus_{l=1}^{k} m_l S \to S$ die Projektion auf die erste Komponente. Dann bildet $\pi(N)$ ein Rechtsideal von S und es ist $\ker\pi = N \cap \left(\bigoplus_{l=2}^{k} m_l S\right)$ nach Induktionsvoraussetzung eine direkte Summe von Rechtsidealen von S. Da $\pi(N)$ nach Voraussetzung projektiv ist, spaltet die folgende exakte Sequenz nun auf:

$$0 \longrightarrow \ker\pi \longrightarrow N \xrightarrow{\pi} \pi(N) \longrightarrow 0\,.$$

Also ist $N \cong \pi(N) \oplus \ker\pi$ eine direkte Summe von Rechtsidealen von S. Die umgekehrte Implikation ist klar. □

Korollar 2.7.15 *Ein Ring S ist genau dann erblich, wenn alle Teilmoduln eines endlich erzeugten projektiven S-Moduls wieder projektiv sind.*

Bemerkung 2.7.16 *Endlich erzeugt* ist eine kategorielle Eigenschaft von Moduln. *Erblich* ist damit auch eine kategorielle Eigenschaft.
Sind also S und T Ringe und sind die Kategorien Mod-S und Mod-T äquivalent, so ist S erblich genau dann, wenn T erblich ist.

Beweis: Siehe [Row91, Proposition 4.1.3, S. 358] □

Satz 2.7.17 *Es sei S ein Ring und $n \in \mathbb{N}$. Dann sind* Mod-S *und* Mod-$S^{n\times n}$ *äquivalente Kategorien. Insbesondere ist S erblich genau dann, wenn $S^{n\times n}$ erblich ist.*

Beweis: Siehe [Row91, Theorem 1.1.17, S. 30 und Example 4.1.10, S. 359]. □

Korollar 2.7.18 *Für jedes $n \geq 1$ ist $\Delta^{n\times n}$ ein erblicher Ring.*

Beweis: Es sei $\mathfrak{a}$ ein von (0) verschiedenes ganzes Δ-Rechtsideal. Da D ein Schiefkörper ist, ist $\mathfrak{a}K = \mathfrak{a}\Delta K = \mathfrak{a}D = D$ und somit ist $\mathfrak{a}$ ein volles normales R-Gitter in der K-Algebra D, welches nach Satz 2.7.5 projektiv ist. Damit ist Δ und somit auch $\Delta^{n\times n}$ erblich. □

Satz 2.7.19 *$\Delta^{n\times n}$ ist eine Maximalordnung in $D^{n\times n}$. Bezeichnet π_D ein Primelement von Δ, so ist jedes zweiseitige $\Delta^{n\times n}$-Ideal eine Potenz von $\mathrm{rad}(\Delta^{n\times n}) = \pi_D\Delta^{n\times n}$. Insbesondere ist $\Delta^{n\times n}/\mathrm{rad}(\Delta^{n\times n}) \cong (\Delta/\pi_D\Delta)^{n\times n}$ ein Matrixring über einem Schiefkörper.*

Beweis: Sei Λ eine Ordnung, welche $\Delta^{n\times n}$ enthalte. Dann bezeiche $\Gamma \subseteq D$ die Menge aller Matrixeinträge, die in irgendeiner Matrix aus Λ vorkommen. Es gilt sicher $\Delta \subseteq \Gamma$. Weil $\Delta^{n\times n}$ alle Permutationsmatrizen sowie $E_1 := \mathrm{diag}\,(1, 0, \ldots, 0)$ enthält, ist $\Gamma = \{x \in D \mid x \cdot E_1 \in \Lambda\}$. Damit ist Γ eine R-Ordnung in D und stimmt daher mit Δ überein. Dies zeigt die erste Aussage. Da die (ganzen) zweiseitigen Ideale von Δ und $\Delta^{n\times n}$ korrespondieren, ist jedes zweiseitige $\Delta^{n\times n}$-Ideal eine Potenz von $\pi_D\Delta^{n\times n}$. Daher gibt es ein $k \geq 1$ mit $\mathrm{rad}(\Delta^{n\times n}) = \pi_D^k\Delta^{n\times n}$. Angenommen, es ist $k > 1$, so ist $\pi_D\Delta^{n\times n}/\mathrm{rad}(\Delta^{n\times n})$ ein nilpotentes nichttriviales Ideal des halbeinfachen Rings $\Delta^{n\times n}/\mathrm{rad}(\Delta^{n\times n})$, was Bemerkung 2.3.10 widerspricht. □

Nun wollen wir die R-Maximalordnungen und die normalen R-Gitter in $D^{n\times n}$ bestimmen. Dazu benötigen wir noch zwei weitere Ergebnisse:

Lemma 2.7.20 *Es sei k ein Körper und B eine endlich erzeugte k-Algebra so, daß $\overline{B} := B/\mathrm{rad}(B)$ einfach ist. Sind M, N zwei endlich erzeugte projektive B-Rechtsmoduln, dann gilt $M \cong N$ genau dann, wenn $\dim_k(M) = \dim_k(N)$ gilt.*

Beweis: Da B ein rechts-artinscher Ring ist, besitzt B eine Zerlegung in unzerlegbare Rechtsideale. Ist $1 = e_1 + \cdots + e_k$ die dazugehörende orthogonale Zerlegung der 1 in primitive Idempotente, so ist $B = e_1B \oplus \cdots \oplus e_kB$. In Satz 2.3.15 haben wir gesehen, daß $\overline{e}_i\overline{B}$ minimale Rechtsideale von $\overline{B}$ sind. Nach Lemma 2.1.7 sind diese zueinander paarweise isomorph. Mit Satz 2.3.15 folgt $e_iB \cong e_jB$ für alle i und j. Weiter sind M und N projektiv und somit direkte Summanden von B^k für ein k. Nach dem Satz von Krull-Schmidt sind M und N daher jeweils isomorph zu einer direkten Summe von Kopien von e_1B. Insbesondere sind sie genau dann zueinander isomorph, wenn sie dieselbe k-Dimension besitzen. □

Lemma 2.7.21 *Es seien Λ eine R-Ordnung in A und I, J zwei projektive Λ-Rechtsideale in A. Weiter seien $\overline{I} := I/\pi I$, $\overline{J} := J/\pi J$ und $\overline{\Lambda} := \Lambda/\pi\Lambda$. Dann sind I und J genau dann isomorph als Λ-Moduln, wenn $\overline{I}$ und $\overline{J}$ isomorph sind als $\overline{\Lambda}$-Moduln.*

Beweis: Sei $f\colon \overline{I} \to \overline{J}$ ein Isomorphismus von $\overline{\Lambda}$-Moduln. Da I und J projektiv sind, existieren Liftungen α und β von f bzw. f^{-1} so, daß das folgende Diagramm kommutiert:

$$\begin{array}{ccccc} I & \overset{\alpha}{\dashrightarrow} & J & \overset{\beta}{\dashrightarrow} & I \\ \downarrow & & \downarrow & & \downarrow \\ \overline{I} & \xrightarrow{f} & \overline{J} & \xrightarrow{f^{-1}} & \overline{I} \end{array}$$

Setzen wir $\gamma := \beta \circ \alpha$, so gilt $\gamma(x) - x \in \pi I$ für alle $x \in I$. Dies zeigt $I = \gamma(I) + \pi I$ und damit $I = \gamma(I)$. Da I ein noetherscher Λ-Modul ist, existiert ein $k > 0$ mit $\ker(\gamma^k) = \ker(\gamma^{k+1})$. Sei nun $x \in \ker(\gamma)$. Da γ^k epimorph ist, existiert ein $y \in I$ mit $x = \gamma^k(y)$. Wegen $0 = \gamma(x) = \gamma^{k+1}(y)$ folgt $y \in \ker(\gamma^k)$ und damit $x = \gamma^k(y) = 0$. Also ist γ ein Automorphismus auf I. Analog gilt dies für $\alpha \circ \beta$. Damit liefert $\alpha\colon I \to J$ einen Isomorphismus von Λ-Rechtsmoduln. Die umgekehrte Implikation ist trivial. □

Satz 2.7.22 *Alle $\Delta^{n\times n}$-Rechtsideale sind Hauptideale.*

Beweis: Es sei $\Lambda := \Delta^{n\times n}$ und $\overline{\Lambda} := \Lambda/\pi\Lambda$. Weiter sei I ein Λ-Rechtsideal. Da Λ erblich ist, ist I ein projektiver Λ-Rechtsmodul. Damit ist auch $\overline{I} := I/\pi I$ ein projektiver $\overline{\Lambda}$-Rechtsmodul. Es ist $\Lambda/\mathrm{rad}(\Lambda) \cong \overline{\Lambda}/\mathrm{rad}(\overline{\Lambda})$ nach Korollar 2.3.9. Nach Lemma 2.7.20 sind $\overline{I}$ und $\overline{\Lambda}$ daher isomorph, denn sie besitzen dieselbe $(R/\pi R)$-Dimension. Mit Lemma 2.7.21 läßt sich dieser Isomorphismus zu einem Λ-Isomorphismus $I \cong \Lambda$ liften. Nach Bemerkung 2.6.3 ist I ein Hauptideal. □

Satz 2.7.23 (Hauptsatz) *Sei K ein vollständig diskret bewerteter Körper mit Bewertungsring R. Weiter sei A eine zentraleinfache K-Algebra. Dann sind alle R-Maximalordnungen von A konjugiert. Weiter ist jedes normale R-Gitter I ein Hauptideal und damit ein projektiver $\mathcal{O}_l(I)$-Linksmodul und ein projektiver $\mathcal{O}_r(I)$-Rechtsmodul. Außerdem ist für jede R-Maximalordnung $\mathfrak{M}$ die Gruppe der zweiseitigen $\mathfrak{M}$-Ideale eine von* $\mathrm{rad}(\mathfrak{M})$ *erzeugte unendliche zyklische Gruppe. Ferner ist* $\mathfrak{M}/\mathrm{rad}(\mathfrak{M})$ *ein Matrixring über einem Schiefkörper.*

Beweis: Wir können $A = D^{n\times n}$ annehmen. Ist dann $\mathfrak{M}$ eine beliebige R-Maximalordnung, so gilt nach dem vorherigen Satz $\mathfrak{M} \cdot \Delta^{n\times n} = x\Delta^{n\times n}$ für ein $x \in A^*$. Damit folgt $\mathfrak{M} = \mathcal{O}_l(\mathfrak{M}\Delta^{n\times n}) = \mathcal{O}_l(x\Delta^{n\times n}) = x\Delta^{n\times n}x^{-1}$. Folglich sind alle R-Maximalordnungen konjugiert. Die Konjugation induziert eine inklusionserhaltende Korrespondenz der Links-/Rechts- bzw. zweiseitigen Ideale. D.h. alle obigen Behauptungen sind erfüllt, da sie für $\Delta^{n\times n}$ gelten. □

Korollar 2.7.24 *Sei R ein Dedekindring und $K = \mathrm{Quot}(R)$. Weiter sei A eine einfache K-Algebra so, daß $Z(A)/K$ eine endliche separable Körpererweiterung ist. Für jedes Primideal $\mathfrak{p}$ von R sind dann alle normalen $\hat{R}_\mathfrak{p}$-Gitter in $A \otimes_K \hat{K}_\mathfrak{p}$ Hauptideale. Ferner sind alle $\hat{R}_\mathfrak{p}$-Maximalordnungen von $\hat{A}_\mathfrak{p}$ konjugiert.*

Beweis: Wie schon im Beweis zuvor genügt es, lediglich die erste Aussage zu zeigen. Sei $E = Z(A)$ und S der ganze Abschluß von R in E. Dann gibt es Primideale $\mathfrak{p}_i$ von S mit $\mathfrak{p} = \prod_{i=1}^{s} \mathfrak{p}_i^{e_i}$. Damit wird $E \otimes \hat{K}_\mathfrak{p} = \bigoplus_{i=1}^{s} \hat{E}_{\mathfrak{p}_i}$. Zu dieser direkten Summe gehört eine orthogonale Zerlegung der 1 in primitive Idempotente $\epsilon_1, \ldots, \epsilon_s$. Setzen wir $A_i := (A \otimes_K \hat{K}_\mathfrak{p})\epsilon_i$, so gilt $A \otimes_K \hat{K}_\mathfrak{p} = \bigoplus_{i=1}^{s} A_i$. Weil $E \otimes_K \hat{K}_\mathfrak{p}$ eine direkte Summe von separablen Erweiterungskörpern von $\hat{K}_\mathfrak{p}$ ist, bildet der ganze Abschluß $\mathcal{O}$ von $\hat{R}_\mathfrak{p}$ in $E \otimes_K \hat{K}_\mathfrak{p}$ die einzige $\hat{R}_\mathfrak{p}$-Maximalordnung in $E \otimes_K \hat{K}_\mathfrak{p}$. Da jedes ϵ_i über $\hat{R}$ ganz ist, liegen alle $\epsilon_i \in \mathcal{O}$. Sei nun I ein normales $\hat{R}_\mathfrak{p}$-Gitter in $\hat{A}_\mathfrak{p}$. Weiter sei $\mathfrak{M} = \mathcal{O}_r(I)$. Dann ist $\mathfrak{M}$ eine $\hat{R}_\mathfrak{p}$-Maximalordnung von $A \otimes_K \hat{K}_\mathfrak{p}$. Es folgt $\mathfrak{M} = \bigoplus_{i=1}^{s} \mathfrak{M}\epsilon_i$. Jedes der $\mathfrak{M}\epsilon_i$ ist dann eine $\hat{S}_{\mathfrak{p}_i}$-Maximalordnung der zentraleinfachen $\hat{E}_{\mathfrak{p}_i}$-Algebra A_i. Nach dem vorherigen Satz existieren nun $x_i \in A_i$ mit $I = \bigoplus_{i=1}^{s} I\epsilon_i = x_i\epsilon_i\mathfrak{M}$. Setzen wir $x = \sum_{i=1}^{s} x_i\epsilon_i$, so gilt $I = x\mathfrak{M}$. □

2.7.3 Der allgemeine Fall

Sei R ein diskreter Bewertungsring (nicht mehr notwendigerweise vollständig) mit maximalem Ideal $R\pi$ und Quotientenkörper $K = \mathrm{Quot}(R)$. Weiter sei A eine zentraleinfache K-Algebra.

Satz 2.7.25 *Es sei $\mathfrak{M}$ eine R-Maximalordnung in A und $\overline{\mathfrak{M}} := \mathfrak{M}/\pi\mathfrak{M}$. Dann gilt*

$$\mathfrak{M}/\mathrm{rad}(\mathfrak{M}) \cong \overline{\mathfrak{M}}/\mathrm{rad}(\overline{\mathfrak{M}}) \cong \hat{\mathfrak{M}}/\mathrm{rad}(\hat{\mathfrak{M}}) .$$

Beweis: Die erste Isomorphie wurde schon in Korollar 2.3.9 gezeigt. Außerdem gilt $\hat{\mathfrak{M}}/\pi\hat{\mathfrak{M}} \cong \overline{\mathfrak{M}}$ nach Lemma 2.5.10. Wendet man nun Korollar 2.3.9 auf $\hat{\mathfrak{M}}$ an, so folgt $\overline{\mathfrak{M}}/\mathrm{rad}(\overline{\mathfrak{M}}) \cong \hat{\mathfrak{M}}/\mathrm{rad}(\hat{\mathfrak{M}})$. □

Satz 2.7.26 (Hauptsatz) *Alle R-Maximalordnungen in A sind konjugiert. Weiter ist jedes normale R-Gitter I ein Hauptideal und damit ein projektiver $\mathcal{O}_l(I)$-Linksmodul und ein projektiver $\mathcal{O}_r(I)$-Rechtsmodul. Außerdem ist für jede R-Maximalordnung $\mathfrak{M}$ die Gruppe der zweiseitigen $\mathfrak{M}$-Ideale eine von* $\mathrm{rad}(\mathfrak{M})$ *erzeugte unendliche zyklische Gruppe, und $\mathfrak{M}/\mathrm{rad}(\mathfrak{M})$ ist ein Matrixring über einem Schiefkörper. Weiter gilt* $\mathrm{rad}(\hat{\mathfrak{M}}) = \widehat{\mathrm{rad}(\mathfrak{M})}$.

Beweis: Sei $\mathfrak{M}$ eine R-Maximalordnung von A. Es sei I ein ganzes $\mathfrak{M}$-Rechtsideal. Da $\hat{\mathfrak{M}}$ erblich ist, ist $\hat{I}$ ein direkter Summand von $\hat{\mathfrak{M}}$. Nach Lemma 2.5.11 ist dann auch I ein direkter Summand von $\mathfrak{M}$. Also ist $\mathfrak{M}$ erblich. Weiter ist $\mathfrak{M}/\mathrm{rad}(\mathfrak{M}) \cong \hat{\mathfrak{M}}/\mathrm{rad}(\hat{\mathfrak{M}})$ ein Matrixring über einem Schiefkörper. Damit läßt sich der Beweis von Satz 2.7.22 nun auch für $\mathfrak{M}$ durchführen, denn er stellt an $\mathfrak{M}$ nur diese beiden Bedingungen. D.h. alle normalen R-Gitter sind in der Tat Hauptideale. Wie im Beweis von Satz 2.7.23 folgt nun, daß alle R-Maximalordnungen von A konjugiert sind.
Da $\mathfrak{M}/\mathrm{rad}(\mathfrak{M})$ einfach ist und $\mathrm{rad}(\mathfrak{M})$ nach Lemma 2.3.5 in jedem maximal ganzen zweiseitigen $\mathfrak{M}$-Ideal liegt, ist $\mathrm{rad}(\mathfrak{M})$ das einzige Primideal von $\mathfrak{M}$. Nach Satz 2.5.25 ist jedes zweiseitige $\mathfrak{M}$-Ideal daher eine Potenz von $\mathfrak{M}$. Aus Lemma 2.5.11 folgt schließlich, daß $\mathrm{rad}(\hat{\mathfrak{M}})$ die Komplettierung von $\mathrm{rad}(\mathfrak{M})$ ist. □

Satz 2.7.27 *Es sei R ein Dedekindring mit $K = \mathrm{Quot}(K)$ und A eine zentraleinfache K-Algebra. Ferner sei $\mathfrak{M}$ eine R-Maximalordnung von A. Ein zweiseitiges $\mathfrak{M}$-Ideal I ist genau dann ein Primideal von $\mathfrak{M}$, falls es ein Primideal $\mathfrak{p}$ von R gibt, mit*

$$I_{\mathfrak{p}'} = \begin{cases} \mathrm{rad}(\mathfrak{M}_{\mathfrak{p}}) & \textit{falls } \mathfrak{p}' = \mathfrak{p} \\ \mathfrak{M}_{\mathfrak{p}'} & \textit{sonst} \end{cases}$$

Ist dies der Fall, so gilt $\mathfrak{p} = I \cap R$.
Insbesondere gibt es also eine Korrespondenz zwischen den Primidealen von $\mathfrak{M}$ und den Primidealen von R via $\mathfrak{P} \mapsto \mathfrak{P} \cap R$ bzw. $\mathfrak{p} \mapsto \mathrm{rad}(\mathfrak{M}_{\mathfrak{p}}) \cap \mathfrak{M}$.

Analoges gilt für die Komplettierungen.

Beweis: Der Beweis geht analog zu Satz 2.5.36. □

2.8 Norm von R-Gittern

Es sei R ein Dedekindring, $K = \mathrm{Quot}(R)$ und A eine einfache K-Algebra mit $m := [A : K]$. Weiter sei $Z(A)/K$ separabel.

Definition 2.8.1 Es sei I ein R-Gitter mit $\Lambda := \mathcal{O}_l(I)$. Sei weiter $r \in R$ so, daß rI ein ganzes R-Gitter ist. Dann existieren nach Satz 2.5.8 eindeutig bestimmte ganze R-Ideale $\mathfrak{a}_1 \supseteq \ldots \supseteq \mathfrak{a}_l$ in K mit

$$\Lambda/rI \cong \bigoplus_{k=1}^{l} R/\mathfrak{a}_k.$$

Wir definieren die Norm von I als $\mathrm{Nr}_{A/K}(I) := r^{-m} \prod_{k=1}^{l} \mathfrak{a}_k$ als R-Ideal in K.

Um zu zeigen, daß die Definition nicht von der Wahl des Skalars r abhängt, benötigen wir zwei Lemmata:

Lemma 2.8.2 *Es sei R ein Hauptidealbereich und I ein R-Gitter in A. Sind weiter $(x_1, \ldots, x_m)$ und $(y_1, \ldots, y_m)$ R-Basen von I bzw. $\mathcal{O}_l(I)$ mit $x_i = \sum_{j=1}^{m} a_{ij} y_j$ und $a_{ij} \in K$, so gilt $\mathrm{Nr}_{A/K}(I) = \det(a_{ij}) \cdot R$.*

Beweis: Es sei rI ganz, d.h. $ra_{ij} \in R$. Nach eventuellen Basiswechseln dürfen wir weiter annehmen, daß (ra_{ij}) Diagonalgestalt besitzt mit $a_{11} \mid a_{22} \mid \cdots \mid a_{mm}$. Damit wird $\Lambda/rI \cong \prod_{k=1}^{m} R/R \cdot ra_{kk}$. Also gilt

$$\det(a_{ij}) \cdot R = r^{-m} \prod_{k=1}^{m} R \cdot ra_{kk} = \mathrm{Nr}_{A/K}(I).$$

□

Über einem Hauptidealbereich ist die Definition der Norm eines R-Gitters also unabhängig von der Wahl des Skalars r.

Da Tensorieren mit direkten Summen vertauscht und $\hat{R}_\mathfrak{p}$ ein flacher $R_\mathfrak{p}$-Modul ist, gilt das

Lemma 2.8.3 *Es sei I ein R-Gitter und $\mathfrak{p}$ ein von (0) verschiedenes Primideal von R. Dann gilt $(\mathrm{Nr}_{A/K}(I))_\mathfrak{p} = \mathrm{Nr}_{A_\mathfrak{p}/K_\mathfrak{p}}(I_\mathfrak{p})$, und $\mathrm{Nr}_{\hat{A}_\mathfrak{p}/\hat{K}_\mathfrak{p}}(\hat{I}_\mathfrak{p})$ ist die Komplettierung von $\mathrm{Nr}_{A/K}(I)$ an $\mathfrak{p}$.*

$\mathrm{Nr}_{A/K}(I)$ ist somit wohldefiniert, also unabhängig von der Wahl des Skalars r, da dies an jeder Lokalisierung zutrifft. Weiter haben wir gezeigt, daß Lemma 2.8.2 auch korrekt ist, wenn R kein Hauptidealbereich ist. Wir wollen in Zukunft dieses Lemma in diesem Zusammenhang verwenden, ohne stets von Neuem darauf hinzuweisen.

Satz 2.8.4

(a) Ist Λ eine R-Ordnung und $x \in A^*$, so gilt $\mathrm{Nr}_{A/K}(\Lambda x) = R \cdot \mathrm{Nr}_{A/K}(x)$.

(b) Für jedes normale R-Gitter I in A ist $\mathrm{Nr}_{A/K}(I)$ das von $\{\mathrm{Nr}_{A/K}(x) \mid x \in I\}$ erzeugte R-Ideal in K.

Beweis: Es genügt die Identitäten an allen Komplettierungen von R zu zeigen. Wegen Lemma 2.8.3 dürfen wir annehmen, daß R ein vollständiger diskreter Bewertungsring ist.

(a) Sei dann $(x_1, \ldots, x_m)$ eine R-Basis von Λ. Es existieren $a_{ij} \in K$ mit $x_i x = \sum_{j=1}^m a_{ij} x_j$. Damit folgt $\mathrm{Nr}_{A/K}(\Lambda x) = R \cdot \det(a_{ij}) = R \cdot \mathrm{Nr}_{A/K}(x)$, da (a_{ij}) eine Darstellungsmatrix der Rechtsmultiplikation mit x auf A ist.

(b) Sei N das von $\{\mathrm{Nr}_{A/K}(x) \mid x \in I\}$ erzeugte R-Ideal. Da R ein vollständiger diskreter Bewertungsring ist, existiert ein y in I mit $I = \Lambda y$. Nach (a) haben wir also $N = R \cdot \mathrm{Nr}_{A/K}(y)$ zu zeigen. Ist $x \in I$, so existiert ein $z \in \Lambda$ mit $x = zy$. Aus $\mathrm{Nr}_{A/K}(\Lambda) \subseteq R$ folgt

$$\mathrm{Nr}_{A/K}(x) \cdot R = \mathrm{Nr}_{A/K}(zy) \cdot R = \mathrm{Nr}_{A/K}(z)\,\mathrm{Nr}_{A/K}(y) \cdot R \subseteq \mathrm{Nr}_{A/K}(y) \cdot R\,.$$

Dies zeigt $N \subseteq \mathrm{Nr}_{A/K}(y) \cdot R$. Die umgekehrte Inklusion ist trivial. □

Wegen (b) ist die Definition von $\mathrm{Nr}_{A/K}$ für normale R-Gitter einer zentraleinfachen K-Algebra nicht asymmetrisch. Wir hätten auch die Rechtsordnung anstelle der Linksordnung verwenden können.

Satz 2.8.5 *Für ein echtes Produkt $I \cdot J$ zweier normaler R-Gitter gilt*

$$\mathrm{Nr}_{A/K}(I \cdot J) = \mathrm{Nr}_{A/K}(I) \cdot \mathrm{Nr}_{A/K}(J)\,.$$

Insbesondere ist $\mathrm{Nr}_{A/K}(I^{-1}) = \mathrm{Nr}_{A/K}(I)^{-1}$.

Beweis: Komplettieren vertauscht auch mit der Idealmultiplikation. Also dürfen wir wieder R als einen vollständigen diskreten Bewertungsring annehmen. Ferner seien dann $I = x\mathfrak{M}$ und $J = \mathfrak{M}y$ mit einer R-Maximalordnung $\mathfrak{M}$ und $x, y \in A^*$. Dann ist $\mathcal{O}_l(IJ) = x\mathfrak{M}x^{-1}$ und es existieren $a_{ij} \in K$ mit $xx_iy = \sum_{j=1}^m a_{ij}xx_jx^{-1}$, wobei $(x_1, \ldots, x_m)$ eine R-Basis von $\mathfrak{M}$ ist. Damit ist $\mathrm{Nr}_{A/K}(I \cdot J) = R \cdot \det(a_{ij})$. Aber es gilt auch $x_i(yx) = \sum_{j=1}^m a_{ij}x_j$. D.h. (a_{ij}) beschreibt die Linksmultiplikation mit yx auf A. Dies zeigt $\det(a_{ij}) = \mathrm{Nr}_{A/K}(yx) = \mathrm{Nr}_{A/K}(y)\,\mathrm{Nr}_{A/K}(x)$. Die Behauptung folgt nun mit Lemma 2.8.2 und Satz 2.8.4. □

Satz 2.8.6 *Sei K/F endlich und separabel. Weiter sei $S \subseteq K$ so, daß $F = \mathrm{Quot}(S)$, und so, daß R der ganze Abschluß von S in K ist. Es ist*

$$\mathrm{Nr}_{K/F}(\mathrm{Nr}_{A/K}(I)) = \mathrm{Nr}_{A/F}(I)$$

für jedes normale R-Gitter I von A.

Beweis: Es bezeichne $\mathfrak{M} = \mathcal{O}_l(I)$. Dies ist eine maximale R-Ordnung. Aus Satz 2.5.7 folgt, daß $\mathfrak{M}$ auch eine maximale S-Ordnung ist. Es genügt, wenn wir die Behauptung an allen Komplettierungen von S zeigen. Daher dürfen wir wieder annehmen, daß S ein vollständiger diskreter Bewertungsring ist. Es existiert somit ein $x \in A^*$ mit $I = \mathfrak{M}x$. Wegen $\mathrm{Nr}_{K/F}(Rr) = S \cdot \mathrm{Nr}_{K/F}(r)$ für alle $r \in R$ folgt

$$\begin{aligned}\mathrm{Nr}_{A/F}(I) &= S \cdot \mathrm{Nr}_{A/F}(x) = S \cdot \mathrm{Nr}_{K/F}(\mathrm{Nr}_{A/K}(x)) \\ &= \mathrm{Nr}_{K/F}(R \cdot \mathrm{Nr}_{A/K}(x)) = \mathrm{Nr}_{K/F}(\mathrm{Nr}_{A/K}(I))\,.\end{aligned}$$ □

Bei normalen R-Gittern hängen alle gezeigten Eigenschaften von „$\mathrm{Nr}_{A/K}$“ massiv von der Elementnorm ab, da man alle Beweise nur für Hauptideale führen muß. Dieses Prinzip hat zur Folge, daß wir auch für normale R-Gitter eine reduzierte Norm einführen können.

Definition 2.8.7 Sei A eine zentraleinfache K-Algebra, $n^2 := [A : K]$ und I ein normales R-Gitter von A. Dann existiert ein R-Ideal $\mathrm{nr}_{A/K}(I)$ in K so, daß $\mathrm{nr}_{A/K}(I)^n = \mathrm{Nr}_{A/K}(I)$ gilt. Da R ein Dedekindring ist, bilden die R-Ideale in K eine von den Primidealen von R erzeugte freie abelsche Gruppe. Das Ideal $\mathrm{nr}_{A/K}(I)$ ist somit eindeutig bestimmt und heißt *reduzierte Norm von I*.

Man muß sich lediglich klarmachen, daß $\mathrm{Nr}_{A/K}(I)$ eine n-te Potenz eines gebrochenen R-Ideal von K ist. Dies ist jedoch an jeder Lokalisierung der Fall. Außerdem ist klar, daß die Sätze 2.8.4 und 2.8.5 auch entsprechend für die reduzierte Norm gelten.

Satz 2.8.8 *Es sei A eine zentraleinfache K-Algebra mit $n^2 = [A : K]$ und $\mathfrak{M}$ eine R-Maximalordnung von A.*

(a) Es sei $\mathfrak{P}$ ein Primideal von $\mathfrak{M}$ mit $\mathfrak{p} := \mathfrak{P} \cap R$ derart, daß $R/\mathfrak{p}$ ein endlicher Körper ist. Ist dann $\hat{A}_\mathfrak{p} \cong D^{\kappa\times\kappa}$ für einen Schiefkörper D mit Zentrum $\hat{K}_\mathfrak{p}$, so sind

$$\mathrm{nr}_{A/K}(\mathfrak{P}) = \mathfrak{p}^\kappa \quad \textit{und} \quad \mathrm{Nr}_{A/K}(\mathfrak{P}) = \mathfrak{p}^{\kappa n}\,.$$

(b) Ist M ein maximal ganzes R-Gitter mit $\mathfrak{p} := M \cap R$ derart, daß $R/\mathfrak{p}$ ein endlicher Körper ist, so gelten

$$\mathrm{nr}_{A/K}(M) = \mathfrak{p} \quad \textit{und} \quad \mathrm{Nr}_{A/K}(M) = \mathfrak{p}^n \,.$$

Beweis: Nach Satz 2.7.27 bzw. Satz 2.5.36 dürfen wir annehmen, daß $R = \hat{R}_\mathfrak{p}$ gilt. Dann ist $A \cong D^{\kappa\times\kappa}$. Setzen wir $m^2 := [D : K]$. Bezeichne Δ die R-Maximalordnung von D, so sind $\mathfrak{M} \cong \Delta^{\kappa\times\kappa}$ und $\mathfrak{P} \cong \mathrm{rad}(\Delta^{\kappa\times\kappa})$ bzw. $\mathfrak{M}/\mathfrak{P} \cong (\Delta/\mathrm{rad}(\Delta))^{\kappa\times\kappa}$. Da $\Delta/\mathrm{rad}(\Delta)$ nach nach Korollar 2.7.8 ein Schiefkörper über $R/\mathfrak{p}$ von Dimension m ist, folgt $[\mathfrak{M}/\mathfrak{P} : R/\mathfrak{p}] = \kappa^2 m$. Also sind $\mathfrak{M}/\mathfrak{P}$ und $(R/\mathfrak{p})^{\kappa^2 m}$ isomorph als $R/\mathfrak{p}$-Moduln und damit auch als R-Moduln. Somit ist

$$\mathrm{Nr}_{A/K}(\mathfrak{P}) = \mathfrak{p}^{\kappa^2 m} = \mathfrak{p}^{\kappa n} \,.$$

Nun zu (b). Es sei $\mathfrak{M} := \mathcal{O}_l(M)$. Weiter sei $\mathfrak{P}$ wie in Lemma 2.5.21 gewählt. Dann gilt $\mathfrak{p} = M \cap R = \mathfrak{P} \cap R$. Nach Lemma 2.5.21 ist $\mathfrak{M}/M$ ein einfacher Linksmodul des einfachen links-artinschen Rings $\mathfrak{M}/\mathfrak{P}$. Nach Lemma 2.1.7 sind $\mathfrak{M}/\mathfrak{P}$ und $(\mathfrak{M}/M)^\kappa$ isomorph als $\mathfrak{M}/\mathfrak{P}$-Linksmoduln und damit auch als $\mathfrak{M}$-Linksmoduln. Es folgt

$$\mathrm{Nr}_{A/K}(M)^\kappa = \mathrm{Nr}_{A/K}(\mathfrak{P}) = \mathfrak{p}^{\kappa n} \,. \qquad \square$$

2.9 Differenten und Diskriminanten

Wie im vorherigen Abschnitt sei R ein Dedekindring, $K = \mathrm{Quot}(R)$ und A eine einfache K-Algebra mit $m = [A : K]$. Weiter sei $Z(A)/K$ separabel.

Definition 2.9.1 Für eine R-Ordnung Λ definieren wir die *Diskriminante* $d(\Lambda/R)$ von Λ bezüglich R als das von $\left\{\det\left((\mathrm{tr}_{A/K}(x_i x_j))_{i,j}\right) \mid x_1, \ldots, x_m \in \Lambda\right\}$ erzeugte Ideal in R. Im Falle $R = \mathbb{Z}$ bezeichne $d(\Lambda/\mathbb{Z}) = \det\left((\mathrm{tr}_{A/\mathbb{Q}}(x_i x_j))_{ij}\right)$ für eine beliebige $\mathbb{Z}$-Basis $(x_1, \ldots, x_m)$ von Λ.
$\Lambda^\# := \{x \in A \mid \mathrm{tr}_{A/K}(x\Lambda) \subseteq R\}$ heißt die *inverse Differente* und $\mathcal{D}(\Lambda/R) := (\Lambda^\#)^{-1}$ die *Differente* von Λ bezüglich R.

Lemma 2.9.2 *Besitzt die R-Ordnung Λ eine R-Basis $(x_1, \ldots, x_m)$, so gilt $d(\Lambda/R) = \det\left((\mathrm{tr}_{A/K}(x_i x_j))_{i,j}\right) \cdot R$.*

Beweis: Es sei $d := \det\left((\mathrm{tr}_{A/K}(x_i x_j))_{i,j}\right)$. Dann gilt $d \cdot R \subseteq d(\Lambda/R)$. Sind umgekehrt $y_1, \ldots, y_m \in \Lambda$, so existieren $a_{ij} \in R$ mit $y_i = \sum_{j=1}^m a_{ij} x_j$. Damit gilt

$$\begin{aligned}\det\left((\mathrm{tr}_{A/K}(y_i y_j))_{i,j}\right) &= \det\left(\left(\sum_{k=1}^m \sum_{l=1}^m a_{ik} a_{jl}\, \mathrm{tr}_{A/K}(x_k x_l)\right)_{i,j}\right) \\ &= \det\left((\mathrm{tr}_{A/K}(x_k x_l))_{k,l}\right) \cdot \det((a_{ij})_{i,j})^2 \in d \cdot R \,. \qquad \square\end{aligned}$$

Um R-Maximalordnungen zu konstruieren, wird sich der folgende Satz als nützlich erweisen.

Satz 2.9.3 *Ist R ein Hauptidealbereich und sind $\Lambda' \subseteq \Lambda$ zwei R-Ordnungen in A, so gilt $d(\Lambda/R) \mid d(\Lambda'/R)$. Ferner haben die beiden Ordnungen genau dann dieselbe Diskriminante, wenn sie übereinstimmen.*

Beweis: Seien $(x_1, \ldots, x_m)$ und $(y_1, \ldots, y_m)$ R-Basen von Λ bzw. Λ'. Dann gibt es $a_{ij} \in R$ mit $y_i = \sum_{j=1}^m a_{ij} x_j$. Im Beweis des vorherigen Lemmas haben wir schon $d(\Lambda'/R) = \det((a_{ij})_{i,j})^2 \cdot d(\Lambda/R)$ gesehen. Insbesondere stimmen die Diskriminanten genau dann überein, wenn $(a_{ij})_{i,j} \in \mathrm{GL}_m(R)$ gilt. □

Satz 2.9.4 *Ist $\mathfrak{M}$ eine R-Maximalordnung, so gilt $d(\mathfrak{M}/R) = \mathrm{Nr}_{A/K}(\mathcal{D}(\mathfrak{M}/R))$. Außerdem besitzen je zwei R-Maximalordnungen dieselbe Diskriminante.*

Beweis: Da Dualisieren, Invertieren und Normbilden alle mit Lokalisieren vertauschen, können wir annehmen, $\mathfrak{M}$ besitzt eine R-Basis $(x_1, \ldots, x_m)$. Bezeichnet $(x_1^*, \ldots, x_m^*)$ die hierzu duale Basis bezüglich der symmetrischen Bilinearform $(x, y) \mapsto \mathrm{tr}_{A/K}(xy)$, so existieren $a_{ij} \in K$ mit $x_i^* = \sum_{j=1}^m a_{ij} x_j$. Damit gilt

$$1 = \det\left((\mathrm{tr}_{A/K}(x_i^* x_j))_{i,j}\right) = \det\left(\left(\sum_{k=1}^m a_{ik} \,\mathrm{tr}_{A/K}(x_k x_j)\right)_{i,j}\right) = \det((a_{ij})_{i,j}) \cdot d(\mathfrak{M}/R)$$

$$= \mathrm{Nr}_{A/K}(\mathfrak{M}^{\#}) \cdot d(\mathfrak{M}/R)$$

Hieraus folgt die erste Behauptung, denn für alle normalen R-Gitter I gilt nach Satz 2.8.5 die Identität $\mathrm{Nr}_{A/K}(I)^{-1} = \mathrm{Nr}_{A/K}(I^{-1})$. Um zu zeigen, daß alle R-Maximalordnungen dieselbe Diskriminante besitzen, kann man entweder zu den Komplettierungen übergehen (denn alle $\hat{R}_\mathfrak{p}$-Maximalordnungen von $\hat{A}_\mathfrak{p}$ sind konjugiert), oder aber man bemüht die Idealarithmetik, denn $\mathfrak{M}^{\#}$ ist nach Lemma 2.5.15 ein zweiseitiges $\mathfrak{M}$-Ideal:
Sei $\mathfrak{M}'$ eine weitere R-Maximalordnung. Wir setzen $I := \mathfrak{M}\mathfrak{M}'$. Nach Korollar 2.5.28 gilt $I^{-1}\mathfrak{M}^{\#} = \mathfrak{M}'^{\#} I^{-1}$. Invertieren wir beide Seiten, so folgt $\mathcal{D}(\mathfrak{M}/R) I = I\,\mathcal{D}(\mathfrak{M}'/R)$ bzw. $\mathcal{D}(\mathfrak{M}/R) = I\,\mathcal{D}(\mathfrak{M}'/R) I^{-1}$. Nun bilden wir die Norm. □

Definition 2.9.5 Da alle R-Maximalordnungen dieselbe Diskriminante besitzen, ist dies eine Invariante der K-Algebra A, und wir schreiben hierfür $d(A/K)$.

Wir werden später das folgende Lemma (im Fall $S = \mathbb{Z}$) verwenden, um duale R-Gitter und Diskriminanten bzgl. R konkret berechnen zu können.

Lemma 2.9.6 *Sei K/F eine endliche separable Körpererweiterung und $S \subseteq F$ ein Dedekindring mit $F = \mathrm{Quot}(S)$ so, daß R der ganze Abschluß von S in K ist. Weiter sei A eine zentraleinfache K-Algebra.*

(a) Sei I ein R-Gitter I in A. Seien

$$I_S^{\#} = \{x \in A \mid \mathrm{tr}_{A/F}(xI) \subseteq S\} \quad \textit{und} \quad I_R^{\#} = \{x \in A \mid \mathrm{tr}_{A/K}(xI) \subseteq R\}$$

die jeweils dualen Gitter bezüglich R respektive S. Dann gilt $I_R^{\#} = \mathcal{D}(R/S) \cdot I_S^{\#}$.

(b) Ist $\mathfrak{M}$ eine R-Maximalordnung in A, so gelten

$$\mathcal{D}(\mathfrak{M}/S) = \mathcal{D}(R/S) \cdot \mathcal{D}(\mathfrak{M}/R) \quad \textit{und} \quad d(\mathfrak{M}/S) = d(R/S)^{[A:K]} \cdot \mathrm{Nr}_{K/F}(d(\mathfrak{M}/R)).$$

Beweis: Wir zeigen zunächst (a):

$$\begin{aligned} x \in I_S^{\#} &\iff \mathrm{tr}_{A/F}(xI) \subseteq S &&\iff \mathrm{Tr}_{K/F}(\mathrm{tr}_{A/K}(xI)) \subseteq S \\ &\iff \mathrm{tr}_{A/K}(xI) \subseteq \mathcal{D}(R/S)^{-1} &&\iff \mathrm{tr}_{A/K}(\mathcal{D}(R/S)xI) \subseteq R \\ &\iff \mathcal{D}(R/S)x \subseteq I_R^{\#} &&\iff x \in \mathcal{D}(R/S)^{-1} \cdot I_R^{\#} \end{aligned}$$

Da $\mathcal{D}(R/S)$ ein R-Ideal in K ist, folgt $I_R^{\#} = \mathcal{D}(R/S) \cdot I_S^{\#}$. Für $I = \mathfrak{M}$ ergibt sich daraus die erste Aussage von (b). Wenden wir darauf $\mathrm{Nr}_{A/K}$ und dann $\mathrm{Nr}_{K/F}$ an, so erhalten wir die zweite Identität. □

Nun wollen wir die Diskriminante einer zentraleinfachen K-Algebra konkret berechnen.

Satz 2.9.7 *Es sei R ein vollständiger diskreter Bewertungsring mit maximalem Ideal $\mathfrak{p}$ und endlichem Restklassenkörper. Weiter sei D ein Schiefkörper mit Zentrum $K = \mathrm{Quot}(R)$ und $m^2 := [D : K]$. Bezeichnet Δ die einzige R-Maximalordnung von D und $\mathfrak{P} = \mathrm{rad}(\Delta)$, so ist*

$$\mathcal{D}(\Delta/R) = \mathfrak{P}^{m-1} \quad \textit{und} \quad d(\Delta/R) = \mathfrak{p}^{m(m-1)}.$$

Beweis: Wir verwenden die Bezeichnungen von Abschnitt 2.7.1. Ohne Einschränkung ist π_D wie in Satz 2.7.11 gewählt. Dann ist $\pi := \pi_D^m$ ein Primelement von R. Da $\Delta^{\#}$ ein zweiseitiges Δ-Ideal ist, gilt $\Delta^{\#} = \pi_D^{-k}\Delta$ für ein $k \geq 0$.
In Gleichung 2.1 auf Seite 48 haben wir bereits

$$\mathrm{tr}_{A/K}(\sum_{j=0}^{m} \alpha_j \pi_D^j) = \mathrm{Tr}_{L/K}(\sum_{j=0}^{m} \alpha_j \pi_D^j) = \mathrm{Tr}_{L/K}(\alpha_0) \quad \text{für alle } \alpha_i \in L$$

gezeigt und wegen

$$\pi_D^{-(m-1)}\Delta = \pi^{-1}\pi_D\Delta = \bigoplus_{j=0}^{m-1} O_L \cdot \pi_D^j$$

folgt $\mathrm{tr}_{A/K}(\pi_D^{-(m-1)}\Delta) = \mathrm{Tr}_{L/K}(O_L) \subseteq R$. Daher ist $k \geq m-1$.

Angenommen, es ist $k > m-1$, so würde $\pi^{-1}\,\mathrm{tr}_{A/K}(\Delta) = \mathrm{tr}_{A/K}(\pi_D^{-m}\Delta) \subseteq R$ gelten. Damit wäre $\mathrm{tr}_{A/K}(\Delta) \subseteq \pi R$. Da $\overline{O_L}/\overline{R}$ separabel ist, ist $\mathrm{Tr}_{\overline{O_L}/\overline{R}}(\overline{\Delta}) \neq 0$. Da die Galoisgruppen von L/K und $\overline{O_L}/\overline{R}$ isomorph sind und L ein Zerfällungskörper von A ist, folgt $\mathrm{tr}_{A/K}(\Delta) \not\subseteq \pi R$. Also muß $k = m-1$ sein. Damit ist die erste Identität bewiesen; die zweite folgt nun aus Satz 2.8.8. □

Korollar 2.9.8 *Es sei R ein diskreter Bewertungsring mit maximalem Ideal $\mathfrak{p}$ und endlichem Restklassenkörper. Weiter sei $K := \mathrm{Quot}(R)$ und A eine zentraleinfache K-Algebra mit $n^2 = [A : K]$. Ist $\hat{K} \otimes_K A \cong D^{\kappa\times\kappa}$ für einen Schiefkörper D mit Zentrum K und $m^2 = [D : K]$, so gilt für jede R-Maximalordnung $\mathfrak{M}$ von A mit $\mathfrak{P} := \mathrm{rad}(\mathfrak{M})$:*

$$\mathcal{D}(\mathfrak{M}/R) = \mathfrak{P}^{m-1}\,, \quad \mathrm{nr}_{A/K}(\mathcal{D}(\mathfrak{M}/R)) = \mathfrak{P}^{(m-1)\kappa} \quad \textit{und} \quad d(\mathfrak{M}/R) = \mathfrak{P}^{(m-1)\kappa n}\,.$$

Beweis: Da Dualisieren mit Komplettieren vertauscht, können wir annehmen, R sei vollständig. Ist Δ dann die einzige R-Maximalordnung von D, so dürfen wir $\mathfrak{M} = \Delta^{\kappa\times\kappa}$ annehmen. Aus Satz 2.2.9 folgt $\mathcal{D}(\Delta/R)\cdot\Delta^{\kappa\times\kappa} \subseteq \mathcal{D}(\Delta^{\kappa\times\kappa}/R)$. Die umgekehrte Inklusion ist auch richtig, weil $\Delta^{\kappa\times\kappa}$ alle Elementarmatrizen, d.h. Matrizen die an genau einer Stelle eine 1 und sonst nur 0 stehen haben, enthält. Mit dem vorherigen Satz erhalten wir damit $\mathcal{D}(\mathfrak{M}/R) = \mathfrak{P}^{m-1}$. Aus Satz 2.8.8 folgen die beiden anderen Behauptungen. □

Satz 2.9.9 *Es sei R ein Dedekindring so, daß $K := \mathrm{Quot}(R)$ ein globaler Körper ist und A eine zentraleinfache K-Algebra mit $n^2 = [A : K]$. Weiter sei $\mathfrak{M}$ eine R-Maximalordnung von A. Für jedes Primideal $\mathfrak{p}$ von R bezeichnen $m_\mathfrak{p}$ und $\kappa_\mathfrak{p}$ der lokale Index bzw. die lokale Kapazität von A an $\mathfrak{p}$ und $\mathfrak{P} = \mathrm{rad}(\mathfrak{M}_\mathfrak{p})\cap\mathfrak{M}$ das zu $\mathfrak{p}$ korrespondierende Primideal von $\mathfrak{M}$ gemäß Satz 2.7.27. Dann ist $m_\mathfrak{p} > 1$ nur für endlich viele $\mathfrak{p}$ und es gelten:*

$$\mathfrak{p}\mathfrak{M} = \mathfrak{P}^{m_\mathfrak{p}} \qquad \mathcal{D}(\mathfrak{M}/R) = \prod_\mathfrak{p} \mathfrak{P}^{m_\mathfrak{p}-1}$$

$$\mathrm{nr}_{A/K}(\mathcal{D}(\mathfrak{M}/R)) = \prod_\mathfrak{p} \mathfrak{p}^{(m_\mathfrak{p}-1)\kappa_\mathfrak{p}} \qquad d(A/K) = d(\mathfrak{M}/R) = \prod_\mathfrak{p} \mathfrak{p}^{(m_\mathfrak{p}-1)\kappa_\mathfrak{p} n}\,.$$

Beweis: Die erste Identität folgt aus Korollar 2.7.8. Die anderen aus Korollar 2.9.8. Da $d(\mathfrak{M}/R)$ ein Ideal von R ist und alle $\kappa_\mathfrak{p} \geq 1$ sind, kann $m_\mathfrak{p} > 1$ nur endlich oft vorkommen. □

2.10 Eichlerbedingung und der Satz von Swan

Es sei R ein Dedekindring, $K = \mathrm{Quot}(R)$ ein globaler Körper und A eine zentraleinfache K-Algebra. Weiter sei $\mathfrak{M}$ eine R-Maximalordnung von A.

Betrachtet man die ($\mathfrak{M}$-Links-) oder $\mathfrak{M}$-Rechtsidealklassen bezüglich (Rechts-) oder Linksäquivalenz einer R-Maximalordnung, so kann man sich fragen, ob diese eine Gruppe bilden, welche durch die Idealmultiplikation induziert wird.
Im Allgemeinen ist dies zu verneinen, denn ist $I_i = c_i J_i \quad (i = 1, 2)$ so müssen $I_1 I_2 = c_1 J_1 c_2 J_2$ und $J_1 J_2$ nicht linksäquivalent sein.

Man kann die Situation dahingehend lösen, indem man eine andere (gröbere) Äquivalenz auf der Menge der $\mathfrak{M}$-Rechtsideale einführt.

Definition 2.10.1 Zwei $\mathfrak{M}$-Rechtsideale I und J heißen *stabil äquivalent*, falls ein $r \in \mathbb{N}_0$ existiert, so daß $I \oplus \mathfrak{M}^r$ und $J \oplus \mathfrak{M}^r$ zueinander isomorph sind als $\mathfrak{M}$-Rechtsmoduln.

Bezeichne $[I]$ die Klasse des $\mathfrak{M}$-Rechtsideals I unter stabiler Äquivalenz und $\mathrm{Cl}(\mathfrak{M})$ die Menge aller solcher Äquivakenzklassen. Dann gilt der

Satz 2.10.2 *Zu je zwei $\mathfrak{M}$-Rechtsidealen I_1 und I_2 existiert ein $\mathfrak{M}$-Rechtsideal J, so daß $I_1 \oplus I_2 \cong \Lambda \oplus J$ gilt.*
Definieren wir $[I_1] + [I_2] := [J]$, so wird $\mathrm{Cl}(\mathfrak{M})$ damit zu einer additiven Gruppe mit neutralem Element $[\mathfrak{M}]$.

Beweis: [Rei03, Theorem 35.5, S. 308]. □

Es impliziert Linksäquivalenz stets stabile Äquivalenz. Nun ist natürlich die Frage, in welchen zentraleinfachen K-Algebren die Umkehrung gilt. Man kann zeigen, daß dies meist der Fall ist:

Definition 2.10.3 Die zentraleinfache K-Algebra A erfüllt die *Eichlerbedingung bezüglich R*, falls eine der beiden nachfolgenden Bedingungen erfüllt ist.

- K ist ein algebraischer Zahlkörper und für A gilt $[A : K] \neq 4$ oder A verzweigt nicht an allen unendlichen Stellen von K.
- K ist ein Funktionenkörper und A verzweigt nicht an allen „Nicht-R-Stellen“.

Satz 2.10.4 *Erfüllt A die Eichlerbedingung bezüglich R, so sind zwei $\mathfrak{M}$-Rechtsideale genau dann stabil äquivalent, wenn sie linksäquivalent sind.*

Beweis: [Rei03, Corollary 35.13 part (i), S. 312]. □

Satz 2.10.5 (Swan) *Es sei $\mathfrak{M}$ eine R-Maximalordnung in A. Ist K ein Funktionenkörper und erfüllt A die Eichlerbedingung bezüglich R oder ist K ein algebraischer Zahlkörper, so ist*

$$\mathrm{Cl}(\mathfrak{M}) \to \mathrm{Cl}_A(R), \quad [I] \mapsto [\mathrm{nr}_{A/K}(I)]$$

ein Isomorphismus.
Dabei steht $\mathrm{Cl}_A(R)$ für die Strahlklassengruppe von R modulo der Menge der in A verzweigten unendlichen Stellen. Weiter bezeichne $[\mathrm{nr}_{A/K}(I)]$ die Klasse des Ideals $\mathrm{nr}_{A/K}(I)$ in der Strahlklassengruppe $\mathrm{Cl}_A(R)$.

Beweis: [Rei03, Theorem 35.14, S. 313]. □

Ist die Eichlerbedingung erfüllt, so folgt aus Satz 2.10.4 und Satz 2.10.5, daß die Klassengruppe der (Rechts-) Idealklassen einer R-Maximalordnung schon a priori bekannt ist. Kennt man alle Rechtsidealklassen einer R-Maximalordnung, so kennt man nach Korollar 2.6.6 insbesondere auch alle Isomorphieklassen von R-Maximalordnungen.
Es verbleiben also nur die beiden Fälle, in denen die Eichlerbedingung verletzt ist.

Unsere in der Einleitung gemachte Einschränkung, lediglich total definite Quaternionenalgebren über algebraischen Zahlkörpern zu betrachten, erfährt hiermit also ihre Rechtfertigung. Die in Kapitel 5 entwickelten Algorithmen lösen die verbleibende Frage in diesem Fall.

Kapitel 3

Quaternionenalgebren

3.1 Definitionen

Es sei R ein Dedekindring und $K = \mathrm{Quot}(R)$ sein Quotientenkörper. Weiter sei angenommen, daß $\mathrm{char}(K) \neq 2$ ist.

Definition 3.1.1 Eine *Quaternionenalgebra* $\mathfrak{D}$ über K ist eine vierdimensionale zentraleinfache K-Algebra.

Definition 3.1.2 Eine *Involution auf* $\mathfrak{D}$ ist eine K-lineare Abbildung $\varphi\colon \mathfrak{D} \to \mathfrak{D}$ mit $\varphi^2 = \mathrm{id}_{\mathfrak{D}}$ und $\varphi(xy) = \varphi(y)\varphi(x)$ für alle $x, y \in \mathfrak{D}$.

Satz 3.1.3 *Sei $\mathfrak{D}$ eine Quaternionenalgebra über K. Dann existiert genau eine Involution $\bar{}\colon \mathfrak{D} \to \mathfrak{D}$, $x \mapsto \overline{x}$ mit $x \cdot \overline{x} \in K$ für alle $x \in \mathfrak{D}$. Diese heißt* kanonische Involution *und erfüllt:*

(a) Für jede zweidimensionale Teilalgebra $L \subseteq \mathfrak{D}$ ist $L = \overline{L}$.

(b) Sei L eine zweidimensionale Teilalgebra von $\mathfrak{D}$ so, daß L/K separabel ist. Dann ist $\bar{}|_L$ der nichttriviale K-Automorphismus auf L.

(c) $K = \{x \in \mathfrak{D} \mid x = \overline{x}\}$.

(d) $\mathrm{tr}_{\mathfrak{D}/K}(x) = x + \overline{x} \in K \quad$ *und* $\quad \mathrm{nr}_{\mathfrak{D}/K}(x) = x\overline{x} \in K$.

Beweis: Die Existenz und Eindeutigkeit, sowie die Aussagen (a) und (b) sind in [Sch85, Theorem 11.2, S. 314] bewiesen.
Zu (c): Es gilt stets $K \subseteq \{x \in \mathfrak{D} \mid x = \overline{x}\}$. Für die umgekehrte Inklusion können wir nach dem Struktursatz von Wedderburn zwei Fälle unterscheiden. Ist $\mathfrak{D}$ ein Schiefkörper, so ist $K(x)/K$ für alle $x \in \mathfrak{D} \setminus K$ eine separable Körpererweiterung. Nach Teil (b) folgt $x \neq \overline{x}$. Ist $\mathfrak{D}$ kein Schiefkörper, so ist $\mathfrak{D}$ isomorph zu $K^{2\times 2}$. Die Matrizen

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, b_1 := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, b_2 := \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, b_3 := \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

erzeugen $K^{2\times 2}$. Für $i = 1, 3$ gilt $\mu_{b_i,K}(X) = (X-1)(X+1)$ und es ist $\mu_{b_2,K}(X) = X^2+1$. Nach Teil (b) ist daher $\overline{b_i} \neq b_i$. Andererseits ist $\overline{b_i}$ ebenso eine Nullstelle von $\mu_{b_i,K}(X)$, also gilt $\overline{b_i} = -b_i$. Sei nun $x = x_0 + x_1b_1 + x_2b_2 + x_3b_3 \in K^{2\times 2}$ mit $\overline{x} = x$. Dann folgt $2(x_1b_1 + x_2b_2 + x_3b_3) = 0$. Wegen $\mathrm{char}(K) \neq 2$ impliziert dies $x \in K$.

Zu (d): Für $x \in K$ ist die Aussage klar. Sei E ein maximaler separabler Teilkörper von $\mathfrak{D}$. Nach Satz 2.1.14 enthält dieser K und ist ein Zerfällungskörper von $\mathfrak{D}$. Daher gibt es einen E-Algebrenisomorphismus $h\colon E \otimes_K \mathfrak{D} \to E^{2\times 2}$. Für $x \in \mathfrak{D} \setminus K$ gilt nun $\overline{x + \overline{x}} = x + \overline{x}$. Also ist $x + \overline{x} \in K$. Daher ist x eine Nullstelle des normierten Polynoms $\mu(X) := X^2 - (x + \overline{x})X + x\overline{x} \in K[X]$. Wegen $x \notin K$ ist $\mu(X)$ das Minimalpolynom von x und auch von $h(x)$. Damit ergeben sich $\mathrm{tr}_{\mathfrak{D}/K}(x) = x + \overline{x}$ und $\mathrm{nr}_{\mathfrak{D}/K}(x) = x\overline{x}$.□

Lemma 3.1.4 *Jede Quaternionenalgebra $\mathfrak{D}$ besitzt eine K-Basis der Form $(1, \mathbf{i}, \mathbf{j}, \mathbf{k})$ mit $a := \mathbf{i}^2, b := \mathbf{j}^2 \in R$ und den Relationen $\overline{\mathbf{i}} = -\mathbf{i},\ \overline{\mathbf{j}} = -\mathbf{j},\ \overline{\mathbf{k}} = -\mathbf{k},\ \mathbf{k} = \mathbf{ij} = -\mathbf{ji}$. Wir schreiben dann $\mathfrak{D} = \left(\frac{a,\, b}{K}\right)$. Mit diesen Bezeichnungen gilt weiter*

$$\mathrm{tr}_{\mathfrak{D}/K}(x_1 + x_2\mathbf{i} + x_3\mathbf{j} + x_4\mathbf{k}) = 2x_1 \qquad \textit{sowie}$$
$$\mathrm{nr}_{\mathfrak{D}_K}(x_1 + x_2\mathbf{i} + x_3\mathbf{j} + x_4\mathbf{k}) = x_1^2 - ax_2^2 - bx_3^2 + abx_4^2\,.$$

Beweis: Der maximale Teilkörper von $\mathfrak{D}$ ist $L = K(\alpha)$ mit $\alpha \in \mathfrak{D} \setminus K$. Wegen $\overline{\alpha} \neq \alpha$ ist $\mathbf{i} := \alpha - \overline{\alpha} \neq 0$. Damit wird $\overline{\mathbf{i}} = -\mathbf{i}$. Wegen $\mathrm{char}(K) \neq 2$ bildet $(1, \mathbf{i})$ daher eine K-Basis von L. Weiter gilt $a := \mathbf{i}^2 = -(\mathbf{i}\overline{\mathbf{i}}) = -\mathrm{nr}_{\mathfrak{D}/K}(\mathbf{i}) \in K$.
Nach dem Satz von Skolem-Noether existiert nun ein $\mathbf{j} \in \mathfrak{D}^*$ mit $\overline{x} = \mathbf{j}x\mathbf{j}^{-1}$ für alle $x \in L$. Dann gilt $\mathbf{j}^2x\mathbf{j}^{-2} = \overline{\overline{x}} = x$ für jedes $x \in L$. Damit ist $\mathbf{j}^2 \in C_{\mathfrak{D}}(L) = L$. Wegen $\overline{\mathbf{j}^2} = \mathbf{j}\mathbf{j}^2\mathbf{j}^{-1} = \mathbf{j}^2$ ist dann sogar $b := \mathbf{j}^2 \in K$. Nach eventueller Multiplikation mit Elementen in R dürfen wir weiter annehmen, daß a und b in R liegen. Die letzten Identitäten folgen unmittelbar aus $-\mathbf{i} = \overline{\mathbf{i}} = \mathbf{j}\mathbf{i}\mathbf{j}^{-1}$ und $\overline{\mathbf{i}\mathbf{j}} = \overline{\mathbf{j}}\,\overline{\mathbf{i}}$. Wegen $\mathbf{j} \notin L$ bilden die vier Elemente $1, \mathbf{i}, \mathbf{j}, \mathbf{ij}$ eine K-Basis von $\mathfrak{D}$. □

Die K-Basis $(1, \mathbf{i}, \mathbf{j}, \mathbf{k})$ von $\mathfrak{D}$ wollen wir *K-Standardbasis von $\mathfrak{D}$* nennen.

Am bekanntesten sind die *Hamiltonschen Quaternionen* $\mathbb{H} = \left(\frac{-1,\, -1}{\mathbb{R}}\right)$, die eine besondere Rolle spielen werden.
Sie bilden bekanntlich (bis auf Isomorphie) die einzige zentraleinfache $\mathbb{R}$-Algebra, die nicht isomorph zu einem Matrixring über $\mathbb{R}$ ist.

Bemerkung 3.1.5 Es seien $r, s, a, b \in K$. Weiter seien $\mathfrak{D}_1 = \left(\frac{a,\, b}{K}\right)$ und $\mathfrak{D}_2 = \left(\frac{ar^2,\, bs^2}{K}\right)$. Bezeichnet $(1,\, \mathbf{i}_i,\, \mathbf{j}_i, \mathbf{k}_i)$ die K-Standardbasis von $\mathfrak{D}_i$, so induziert $\mathbf{i}_1 \mapsto r\mathbf{i}_2,\ \mathbf{j}_1 \mapsto s\mathbf{j}_2$ einen kanonischen K-Algebrenisomorphismus zwischen den beiden Quaternionenalgebren $\mathfrak{D}_1$ und $\mathfrak{D}_2$.

Bemerkung 3.1.6 Es seien K ein Zahlkörper und $\mathfrak{D} = \left(\frac{a,\,b}{K}\right)$ mit K-Standardbasis $(b_1 = 1, b_2 = \mathbf{i}, b_3 = \mathbf{j}, b_4 = \mathbf{k})$. Weiter sei P eine unendliche reelle Stelle von K, welche durch $\sigma\colon K \hookrightarrow \mathbb{R}$ induziert wird. Ferner bezeichne $\hat{\sigma}\colon K \otimes_K \mathbb{R} \to \mathbb{R}, \lambda \otimes x \mapsto \sigma(\lambda)x$ die Fortsetzung von σ auf $\hat{K}_P$ und $(b'_1 = 1, b'_2 = \mathbf{i}, b'_3 = \mathbf{j}, b'_4 = \mathbf{k})$ die $\mathbb{R}$-Standardbasis von $\left(\frac{\sigma(a),\,\sigma(b)}{\mathbb{R}}\right)$. Dann ist

$$\varphi\colon \hat{\mathfrak{D}}_P = \hat{K}_P \otimes_K \mathfrak{D} \cong \left(\frac{\sigma(a),\ \sigma(b)}{\mathbb{R}}\right),\ \sum_{k=1}^{4} x_k \otimes b_k \mapsto \sum_{k=1}^{4} \hat{\sigma}(x_k) \otimes b'_k$$

ein $\mathbb{R}$-Algebrenisomorphimus.

Beweis: Es sei $\mathbf{i}' := \varphi(1 \otimes \mathbf{i})$ und $\mathbf{j}' = \varphi(1 \otimes \mathbf{j})$. Da φ ein Ringhomomorphismus ist, gelten $\mathbf{i}'\mathbf{j}' = -\mathbf{j}'\mathbf{i}'$ und $\mathbf{i}'^2 = \varphi(1 \otimes a) = \sigma(a)$ und $\mathbf{j}'^2 = \sigma(b)$. Also ist $\varphi(\hat{\mathfrak{D}}_P) \cong \left(\frac{\sigma(a),\,\sigma(b)}{\mathbb{R}}\right)$. □

Definition 3.1.7 Eine Quaternionenalgebra $\mathfrak{D}$ über einem algebraischen Zahlkörper K heißt total definit, falls sie an allen unendlichen Stellen von K verzweigt.

Bemerkung 3.1.8 Wie wir schon in Bemerkung 2.4.9 gesehen haben, muß das Zentrum K einer total definiten Quaternionenalgebra $\mathfrak{D}$ ein total reller Zahlkörper sein. Ist dies der Fall und gilt weiter $\mathfrak{D} \cong \left(\frac{a,\,b}{K}\right)$, dann sind folgende Aussagen äquivalent:

(a) $\mathfrak{D}$ ist total definit.

(b) Für jede unendliche Stelle P von K gilt $\widehat{\mathfrak{D}}_P \cong \mathbb{H}$.

(c) Für alle $x \in \mathfrak{D} \setminus \{0\}$ ist $\mathrm{nr}_{\mathfrak{D}/K}(x)$ total positiv.

(d) $-a$ und $-b$ sind total positiv.

Beweis: $(a) \iff (b)$ ist die Aussage über die Brauergruppe von $\mathbb{R}$ und $(c) \iff (d)$ folgt mit Lemma 3.1.4. Aus $\left(\frac{x,\,y}{\mathbb{R}}\right) \cong \mathbb{H} \iff x \equiv y \equiv -1 \mod (\mathbb{R}^*)^2$ und Bemerkung 3.1.6 folgt $(b) \iff (d)$. □

Definition 3.1.9 Für ein R-Gitter I in einer Quaternionenalgebra $\mathfrak{D}$ bezeichne $\overline{I} := \{\overline{x} \mid x \in I\}$.

Lemma 3.1.10 *Es sei $\mathfrak{D}$ eine beliebige Quaternionenalgebra und I ein R-Gitter von $\mathfrak{D}$.*

(a) Für jede R-Ordnung Λ von $\mathfrak{D}$ gilt $\overline{\Lambda} = \Lambda$.

(b) $\overline{I}$ ist ein R-Gitter mit $\mathcal{O}_l(\overline{I}) = \mathcal{O}_r(I)$ und $\mathcal{O}_r(\overline{I}) = \mathcal{O}_l(I)$.

(c) Ist I normal, so gilt $I^{-1} = (\mathrm{nr}_{\mathfrak{D}/K}(I))^{-1} \cdot \overline{I}$.

Beweis:

(a) Folgt aus $x \in \Lambda \iff \overline{x} = x - \mathrm{tr}_{\mathfrak{D}/K}(x) \in \Lambda$.

(b) Es sei $\Lambda := \mathcal{O}_l(I)$. Dann gibt es $s_1, s_2 \in K$ mit $s_1\Lambda \subseteq I \subseteq s_2\Lambda$ und damit $s_1\Lambda \subseteq \overline{I} \subseteq s_2\Lambda$. Also ist I ein volles R-Gitter. Weiter gilt

$$\begin{aligned} x \in \mathcal{O}_l(\overline{I}) &\iff x\overline{y} \in \overline{I} \text{ für alle } y \in I &&\iff y\overline{x} \in I \text{ für alle } y \in I \\ &\iff \overline{x} \in \mathcal{O}_r(I) &&\iff x \in \mathcal{O}_r(I)\,. \end{aligned}$$

(c) Da die Konjugation mit Lokalisieren vertauscht, genügt es nach 2.7.26 die Behauptung nur für Hauptideale zu beweisen. Es sei also $I = x\mathfrak{M}$ mit einer R-Maximalordnung $\mathfrak{M}$. Dann ist $\overline{I} = \mathfrak{M}\overline{x}$ und damit gilt

$$\overline{I}I = \mathfrak{M}\overline{x}x\mathfrak{M} = \mathrm{nr}_{\mathfrak{D}/K}(x)\mathfrak{M} = \mathrm{nr}_{\mathfrak{D}/K}(I)\mathfrak{M}\,. \qquad \square$$

3.2 Zyklotomische Quaternionenalgebren

Satz 3.2.1 *Sei $n \geq 4$ eine gerade ganze Zahl und Φ_n das n-te Kreisteilungspolynom. Es bezeichne $A := \mathbb{Q}\langle Y, X\rangle$ die freie Algebra auf X und Y sowie $\mathcal{J}$ das von $(\Phi_n(Y),\ X^2+1,\ XYX^{-1}-Y^{-1})$ erzeugte zweiseitige Ideal von A.*
Dann ist $\mathfrak{D} := A/\mathcal{J}$ eine von $\zeta_n := Y + \mathcal{J}$ und $x := X + \mathcal{J}$ erzeugte $\mathbb{Q}$-Algebra mit folgenden Eigenschaften:

(a) Sei $\theta_n := \zeta_n + \zeta_n^{-1}$, so liegt $K := \mathbb{Q}[\theta_n]$ in $Z(\mathfrak{D})$. Außerdem ist K isomorph zum maximal reellen Teilkörper des n-ten Kreisteilungskörpers und es gilt $\mathbb{Z}_K = \mathbb{Z}[\theta_n]$.

(b) $\mathfrak{D}$ wird als K-Vektorraum erzeugt von $B := (1,\ \zeta_n,\ x,\ \zeta_n x)$.

(c) Sei $\tilde{\mathfrak{D}}$ die von $\zeta_n^* := \begin{pmatrix} \zeta_n & 0 \\ 0 & \zeta_n^{-1} \end{pmatrix}$ und $x^* := \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ erzeugte K-Algebra in $\mathbb{Q}[\zeta_n]^{2\times 2}$. Dann sind $\mathfrak{D}$ und $\tilde{\mathfrak{D}}$ isomorphe K-Algebren.

(d) Es ist $Z(\mathfrak{D}) = K$.

(e) B ist eine K-Basis von $\mathfrak{D}$.

(f) $\mathfrak{D}$ ist eine total definite Quaternionenalgebra über K und es gelten

$$\begin{aligned} \mathrm{tr}_{\mathfrak{D}/K}(d) &= 2d_1 + d_2\theta_n \\ \mathrm{nr}_{\mathfrak{D}/K}(d) &= d_1^2 + d_1d_2\theta_n + d_2^2 + d_3^2 + d_3d_4\theta_n + d_4^2\,. \end{aligned}$$

Beweis:

(a) Es gilt $\theta_n\zeta_n = \zeta_n\theta_n$ und $\theta_n x = \zeta_n x + \zeta_n^{-1}x = x\zeta_n^{-1} + x\zeta_n = x\theta_n$. Also liegt K in $Z(\mathfrak{D})$. Da ζ_n, eine n-te primitive Einheitswurzel ist, ist $K = \mathbb{Q}[\theta_n]$ nach [Was96, Proposition 2.16, S. 16] der maximal reelle Teilkörper von $\mathbb{Q}(\zeta_n)$ und es gilt $\mathbb{Z}_K = \mathbb{Z}[\theta_n]$.

(b) Wegen $x\zeta_n = \zeta_n^{-1}x$ sowie $x^2 = -1$ und $\Phi_n(\zeta_n) = 0$ ist $\{\zeta_n^i x^j \mid 0 \le i < n,\, j \in \{0,1\}\}$ ein K-Erzeugendensystem von $\mathfrak{D}$. Nun gilt $\zeta_n^2 = \theta_n\zeta_n - 1$. Also ist B ein K-Erzeugendensystem von $\mathfrak{D}$.

(c) Sei $\varphi\colon A \to \mathfrak{D}$ der durch $X \mapsto x^*$ und $Y \mapsto \zeta_n^*$ definierte K-Algebrenhomomorphismus. Dieser ist surjektiv. Weil ζ_n^* und x^* dieselben Relationen wie ζ_n und x erfüllen, gilt $\mathcal{J} \subseteq \ker(\varphi)$. Also induziert φ einen surjektiven K-Algebrenhomomorphismus $\overline{\varphi}\colon \mathfrak{D} \to \tilde{\mathfrak{D}}$. Nun ist $(I_2, \zeta_n^*, x^*, \zeta_n^* x^*)$ eine K-Basis von $\tilde{\mathfrak{D}}$. Wegen $\dim_K(\mathfrak{D}) \le 4$ ist $\overline{\varphi}$ daher ein K-Algebrenisomorphismus.

(d) Wir haben $Z(\mathfrak{D}) \subseteq K$ zu zeigen. Sei $z \in Z(\mathfrak{D})$. Dann gibt es $z_i \in K$ mit $z = z_1 + z_2\zeta_n + z_3 x + z_4\zeta_n x$. Dann gilt $zx = xz$, was $z_2 = z_4 = 0$ impliziert. Aus $\zeta_n z = z\zeta_n$ folgt nun $z_3 = 0$. Also ist $z \in K$.

(e) Wurde bereits in (c) gezeigt.

(f) $L := \mathbb{Q}(\zeta_n)$ ist ein maximaler separabler Teilkörper von $\mathfrak{D}$. Nun induziert $1 \otimes \zeta_n \mapsto \zeta_n^*$, $1 \otimes x \mapsto x^*$ einen L-Algebrenisomorphismus $1 \otimes_K \mathfrak{D} \to L^{2\times 2}$. Für ein $d := d_1 + d_2\zeta_n + d_3 x + d_4\zeta_n x \in \mathfrak{D}$, gelten daher

$$\begin{aligned} \mathrm{tr}_{\mathfrak{D}/K}(d) &= d_1 \,\mathrm{Spur}(I_2) + d_2 \,\mathrm{Spur}(\zeta_n^*) = 2d_1 + d_2\theta_n \qquad \text{sowie} \\ \mathrm{nr}_{\mathfrak{D}/K}(d) &= \det \begin{pmatrix} d_1 + d_2\zeta_n & d_3 + d_4\zeta_n \\ -d_3 - d_4\zeta_n^{-1} & d_1 + d_2\zeta_n^{-1} \end{pmatrix} \\ &= d_1^2 + d_1 d_2\theta_n + d_2^2 + d_3^2 + d_3 d_4\theta_n + d_4^2 \,. \end{aligned}$$

Ersetzen wir d_1 durch $d_1 - \theta_n d_2/2$ und d_3 durch $d_3 - \theta_n d_4/2$, so wird die rechte Seite der obigen Gleichung zu $d_1^2 + \frac{d_2^2}{4}(4-\theta_n^2) + d_3^2 + \frac{d_4^2}{4}(4-\theta_n^2)$. Wegen $|\sigma(\theta_n)| < 2$ für alle $\sigma\colon K \hookrightarrow \mathbb{R}$, ist $\mathrm{nr}_{\mathfrak{D}/K}(d)$ für alle $d \in \mathfrak{D}$ total positiv. Also ist $\mathfrak{D}$ total definit. □

Definition 3.2.2 Die total definite Quaternionenalgebra aus der vorherigen Bemerkung wollen wir *zyklotomisch* nennen und mit $\mathfrak{D}_{\theta_n}$ bezeichnen.

Wegen $\zeta_u = -\zeta_{2u}$ und $\Phi_u(X) = \Phi_{2u}(X)$ für alle ungeraden $u \in \mathbb{N}$ ist es keine Einschränkung, nur gerade n zu betrachten.

Satz 3.2.3 *Es sei $n \ge 4$ gerade und $R = \mathbb{Z}_{K(\theta_n)} = \mathbb{Z}[\theta_n]$.*

(a) $\mathfrak{D}_{\theta_4}$ verzweigt nur an einem Primideal, nämlich $2\mathbb{Z}$.
Ist $\frac{n}{2} = p^k$ für eine Primzahl $p \equiv 3 \mod 4$, so verzweigt nur ein Primideal von R in $\mathfrak{D}_{\theta_n}$, nämlich das Primideal über p.
In allen anderen Fällen verzweigt $\mathfrak{D}_{\theta_n}$ an keiner endlichen Stelle.

(b) Die zyklotomischen Quaternionenalgebren $\mathfrak{D}_{\theta_n}$ sind gerade die Schiefkörper D über $\mathbb{Q}$, so daß D ein direkter Summand von $\mathbb{Q}G$ für eine endliche Gruppe G ist.

Beweis: [Neb98, Theorem 6.1, S. 121]. □

Die zyklotomischen Quaternionenalgebren sind also interessante Algebren. Im folgenden Satz soll konkret durch theoretische Überlegungen eine R-Maximalordnung von $\mathfrak{D}_{\theta_n}$ angegeben werden. Diese lassen sich dann mit Hilfe der in Kapitel 5 entwickelten Algorithmen überpüfen.

Satz 3.2.4 *Es sei $n \geq 4$ gerade, $R = \mathbb{Z}[\theta_n]$ und $K = \mathbb{Q}(\theta_n)$. Weiter sei Λ die von $(1, \zeta_n, x, \zeta_n x)$ erzeugte R-Ordnung in $\mathfrak{D}_{\theta_n}$.*

(a) Ist $\frac{n}{2}$ keine Primzahlpotenz, so ist Λ eine R-Maximalordnung in $\mathfrak{D}_{\theta_n}$ und es gilt $d(\mathfrak{D}_{\theta_n}/K) = R$.

(b) Ist $\frac{n}{2} = p^k$ mit einer Primzahl $p \equiv 3 \mod 4$, so ist Λ eine R-Maximalordnung in $\mathfrak{D}_{\theta_n}$ und es gilt $d(\mathfrak{D}_{\theta_n}/K) = (2+\theta_n)^2$.

(c) Sei $\frac{n}{2} = p^k$ mit einer Primzahl $p \equiv 1 \mod 4$. Weiter sei $\alpha := \frac{1}{2+\theta_n}(2\zeta_n - \theta_n)$ sowie $t \in \mathbb{Z}$ mit $1 < t < p$ und $t^2 \equiv -1 \mod p$. Dann existieren genau zwei R-Ordnungen über Λ, nämlich $\mathfrak{M}_1 = \Lambda + (\alpha + t\alpha x)R$ und $\mathfrak{M}_2 = \Lambda + (\alpha - t\alpha x)R$. Ferner sind diese beiden maximal und zueinander konjugiert. Weiter gilt $d(\mathfrak{D}_{\theta_n}/K) = R$.

(d) Ist $n = 4$, so ist $< 1, \zeta_4, x, \frac{1}{2}(1 + \zeta_4 + x + \zeta_4 x) >$ die einzige R-Ordnung über Λ. Insbesondere ist sie maximal und es gilt $d(\mathfrak{D}_{\theta_4}/K) = 4\mathbb{Z}$.

(e) Sei $n = 2^k$ mit $k \geq 3$. Weiter seien $\alpha_1 := \frac{1}{\theta_n}(1 + x)$, $\alpha_2 = \frac{1}{\theta_n}(1 + \zeta_n x)$ und $\alpha_3 := \frac{1}{\theta_n}(1 + \zeta_n + x + \zeta_n x)$. Dann gibt es genau zwei R-Maximalordnungen über Λ, nämlich $\mathfrak{M}_1 := \Lambda + \alpha_1 R + \alpha_3 R$ und $\mathfrak{M}_2 := \Lambda + \alpha_2 R + \alpha_3 R$. Diese beiden sind konjugiert und es gilt $d(\mathfrak{D}_{\theta_n}/K) = R$.

Beweis: Die Elemente $b_1 := 1, b_2 := \zeta_n, b_3 := x$ und $b_4 := \zeta_n x$ sind ganz über R und das von ihnen erzeugte R-Gitter Λ bildet einen Ring. Nach Satz 2.5.7 ist Λ eine R-Ordnung. Im Beweis von Satz 3.2.1 haben wir bereits die reduzierte Spur von Elementen in $\mathfrak{D}_{\theta_n}$ bestimmt. Damit folgt

$$d(\Lambda/R) = R \cdot \det\left(\mathrm{tr}_{\mathfrak{D}_{\theta_n}/K}(b_i b_j)\right) = R \cdot \det \begin{pmatrix} 2 & \theta_n & 0 & 0 \\ \theta_n & \theta_n^2 - 2 & 0 & 0 \\ 0 & 0 & -2 & -\theta_n \\ 0 & 0 & -\theta_n & -2 \end{pmatrix} = (4 - \theta_n^2)^2 \,.$$

Ist n keine Zweierpotenz, so gilt nach [Was96, Proposition 2.8, S. 12] die Inklusion $2 - \theta_n = (1-\zeta_n)(1-\zeta_n^{-1}) \in \mathbb{Z}[\zeta_n]^* \cap K = R^*$. In diesem Fall ist also $d(\Lambda/R) = (2+\theta_n)^2$.

(a) Wir unterscheiden zwei Fälle. Ist $\frac{n}{2}$ ungerade, so gilt $2 + \theta_n = 2 - \theta_{\frac{n}{2}}$. Da $\frac{n}{2}$ keine Primzahlpotenz ist, folgt wie zuvor $2 + \theta_n \in R^*$. Andernfalls ist n durch 4 teilbar und es gilt $2 + \theta_n = (1 + \zeta_n)(1 + \zeta_n^{-1})$. Da $-\zeta_n$ in diesem Fall ebenso eine primitive Einheitswurzel ist, folgern wir wiederum, daß $2 + \theta_n$ eine Einheit von R ist. In beiden Fällen folgt $d(\Lambda/R) = R$. Λ ist damit eine R-Maximalordnung.

(b) Das eindeutig bestimmte Primideal von $\mathbb{Z}[\zeta_{p^k}]$ über p ist $(1-\zeta_{p^k})$. Damit ist $(2-\theta_{p^k}) = (1-\zeta_{p^k})(1-\zeta_{p^k}^{-1})$ das Primideal von $\mathbb{Z}[\theta_{p^k}]$ über p. Wegen $\zeta_{p^k} = -\zeta_n$ ist $(2+\theta_n)$ das Primideal von $R = \mathbb{Z}[\theta_n]$ über p. Aus Satz 3.2.3 folgt $d(\mathfrak{D}_{\theta_n}/K) = (2+\theta_n)^2$. Aus Satz 2.9.3 folgt nun, daß Λ eine R-Maximalordnung ist.

(c) Wie oben ist $(2+\theta_n)$ das Primideal über p. Alle R-Maximalordnungen über Λ liegen in $\Lambda^\#$ dem zu Λ bezüglich $\tau_{\mathfrak{D}_{\theta_n}/K}$ dualen Gitter. Invertieren wir die oben aufgestellte Matrix $\left(\mathrm{tr}_{\mathfrak{D}_{\theta_n}/K}(b_ib_j)\right)$, so liefern die Zeilen eine Basis von $\Lambda^\#$. Nun gilt

$$\Lambda^\#/\Lambda =< \overline{\alpha}, \overline{\alpha x} > \ .$$

Damit gewinnt man alle R-Maximalordnungen über Λ durch Hinzunahme eines einzigen ganzen Elements der Form $r\alpha + s\alpha x$ mit $r, s \in R/(2+\theta_n) \cong \mathbb{F}_p$. Die reduzierte Spur eines solchen Elements ist immer ganz, da es ja in $\Lambda^\#$ liegt. Also müssen wir nun alle Elemente der Form $r\alpha + s\alpha x$ mit $r, s \in \{0, \ldots, p-1\}$ bestimmen, die eine ganze reduzierte Norm haben. Es gilt $\mathrm{nr}_{\mathfrak{D}_{\theta_n}/K}(r\alpha + s\alpha x) = (r^2+s^2)(2-\theta_n)(2+\theta_n)^{-1}$.
Wegen $(2-\theta_n) \in R^*$, ist $r\alpha + s\alpha x$ genau dann ganz über R, wenn $(2+\theta_n)$ ein Teiler von r^2+s^2 in R ist. Das heißt $r^2+s^2 \in (2+\theta_n) \cap \mathbb{Z} = p\mathbb{Z}$. Ist $r = 0$, so folgt $s = 0$ und umgekehrt. Also dürfen wir ohne Einschränkung $r = 1$ wählen. Da $p \equiv 1 \mod 4$ gilt, gibt es nun zwei $s \in \mathbb{F}_p$ mit $s^2 = -1$ und diese liefern gerade die beiden R-Gitter $\mathfrak{M}_1$ und $\mathfrak{M}_2$ aus der Behauptung. Diese sind verschieden, denn angenommen nicht, so wäre $2\alpha \in \mathfrak{M}_1 = \mathfrak{M}_2$, was wegen $2\,\mathrm{nr}_{\mathfrak{D}/K}(\alpha) \notin R$ nicht sein kann.
Über Λ muß aber nach Satz 3.2.3 mindestens eine R-Ordnung liegen. $\mathfrak{M}_1$ bzw. $\mathfrak{M}_2$ waren die einzigen Kandidaten. Daher ist eines der beiden R-Gitter eine R-Maximalordnung über Λ. Sei nun $z := \zeta_n - \zeta_n^{-1}$. Dann gilt $xz = x(\zeta_n - \zeta_n^{-1}) = \zeta_n^{-1}x - \zeta_n x = -zx$. Daraus folgt $z\mathfrak{M}_1 z^{-1} = \mathfrak{M}_2$. Also sind die beiden R-Gitter konjugiert, d.h. $\mathfrak{M}_1$ und $\mathfrak{M}_2$ sind R-Maximalordnungen. Weiter ist $d(\mathfrak{D}_{\theta_n}/K) = R$ wie in Satz 3.2.3 erwähnt.

(d) Es ist $\theta_4 = 0$ und $R = \mathbb{Z}$. Nach Satz 3.2.3 ist $d(\mathfrak{D}_{\theta_4}/\mathbb{Q}) = 4\mathbb{Z}$. Weiter ist $\left(\mathrm{tr}_{\mathfrak{D}_{\theta_n}/K}(b_ib_j)\right) = \mathrm{diag}\,(2,-2,-2,-2)$. Also ist Λ nicht maximal. Die Zeilen von $\left(\mathrm{tr}_{\mathfrak{D}_{\theta_n}/K}(b_ib_j)\right)^{-1}$ liefern eine $\mathbb{Z}$-Basis von $\Lambda^\#$. Und jede R-Maximalordnung über Λ liegt in $\Lambda^\#$. Eine R-Ordnung über Λ gewinnt man also durch Hinzunahme von Elementen der Form $z = \frac{1}{2}(x_1 + x_2\zeta_4 + x_3x + x_4\zeta_4x)$ mit $x_i \in \{0,1\}$. Wegen $\mathrm{nr}_{\mathfrak{D}_{\theta_4}/\mathbb{Q}}(z) = \frac{1}{2}(x_1^2+x_2^2+x_3^2+x_4^2) \in \mathbb{Z}$ folgt $z = \frac{1}{2}(1+\zeta_4+x+\zeta_4x)$. Da $\mathfrak{M} :=< 1, \zeta_4, x, z >$ eine R-Ordnung bildet mit $d(\mathfrak{M}/\mathbb{Z}) = 4\mathbb{Z}$ ist es die einzige R-Ordnung über Λ und eine R-Maximalordnung.

(e) Ist $n = 2^k$ mit $k \geq 3$, so ist $(1-\zeta_n)$ das einzige Primideal von $\mathbb{Z}[\zeta_n]$ über 2. Damit gilt $2\mathbb{Z} = \mathrm{Nr}_{\mathbb{Z}[\zeta_n]/\mathbb{Z}}(1-\zeta_n) = \mathrm{Nr}_{R/\mathbb{Z}}((1-\zeta_n)(1-\zeta_n^{-1})) = \mathrm{Nr}_{R/\mathbb{Z}}(2-\theta_n)$. Wegen $k \geq 3$ folgt weiter $2R \subsetneq (2-\theta_n) \subsetneq R$. Insbesondere gilt damit $(2-\theta_n) = (\theta_n) = (2+\theta_n)$. Also ist $d(\Lambda/R) = (\theta_n)^4$ und $\Lambda^\# = \frac{1}{\theta_n}\Lambda$. Wir wissen bereits, daß $d(\mathfrak{D}_{\theta_n}/K) = R$ gilt. Daher erhält man jede R-Maximalordnung über Λ durch Hinzunahme zweier Elemente aus $\frac{1}{\theta_n}\Lambda$. Wegen $R/(\theta_n) \cong \mathbb{F}_2$ können wir annehmen, daß jedes dieser Elemente von der Form $z := \frac{1}{\theta}(x_1+x_2\zeta_n+x_3x+x_4\zeta_nx)$

mit $x_i \in \{0,1\}$ ist. Nun gilt

$$\mathrm{nr}_{\mathfrak{D}_{\theta_n}/K}(z) = \frac{1}{\theta_n^2}(x_1^2 + x_1x_2\theta_n + x_2^2 + x_3^2 + x_3x_4\theta_n + x_4^2)\,.$$

Damit $z \notin \Lambda$ und $\mathrm{nr}_{\mathfrak{D}_{\theta_n}/K}(z) \in R$ gelten, müssen also $(x_1, x_2) \neq (0,0)$ und $(x_3, x_4) \neq (0,0)$ sein. Nachdem wir z eventuell mit ζ_n^{-1} multipliziert haben, können wir annehmen, daß $x_1 = 1$ gilt. Ist dann $x_2 \neq 0$, so muß auch $x_3x_4 \neq 0$ sein, damit $\mathrm{nr}_{\mathfrak{D}_{\theta_n}/K}(z) \in R$ liegt. Analog folgert man, daß $x_2 = 0$ auch $x_3x_4 = 0$ impliziert. Dies läßt uns noch 3 Möglichkeiten, nämlich:

$$\alpha_1 := \frac{1}{\theta_n}(1+x), \quad \alpha_2 := \frac{1}{\theta_n}(1+\zeta_n x), \quad \alpha_3 := \frac{1}{\theta_n}(1+\zeta_n+x+\zeta_n x)\,.$$

Wegen $\mathrm{tr}_{\mathfrak{D}_{\theta_n}/K}(\alpha_1\alpha_2) = \frac{2-\theta_n}{\theta_n^2} \notin R$, dürfen wir α_1 und α_2 nicht gleichzeitig zu Λ hinzufügen. Also sind $\mathfrak{M}_1 := \Lambda + \alpha_1 R + \alpha_3 R$ und $\mathfrak{M}_2 := \Lambda + \alpha_2 R + \alpha_3 R$ die einzigen Möglichkeiten einer R-Maximalordnung über Λ. Wegen $\alpha_3\alpha_1 = \alpha_2\alpha_3$ sind die R-Gitter $\mathfrak{M}_1$ und $\mathfrak{M}_2$ konjugiert und somit R-Maximalordnungen. □

Einige solcher zyklotomischen Quaternionenalgebren sind im Anhang B.2 jemeils mit einem Vertretersystem aller R-Maximalordnungen aufgeführt.

3.3 Minkowski - Theorie

Es sei K ein total reeller Zahlkörper mit $n = [K : \mathbb{Q}]$. Weiter sei $R = \mathbb{Z}_K$ der ganze Abschluß von $\mathbb{Z}$ in K und $\mathfrak{D}$ eine total definite Quaternionenalgebra über K.

In diesem Abschnitt soll nun mit den von Minkowski eingeführten geometrischen Hilfsmitteln, analog zur Situation bei algebraischen Zahlkörpern, eine lediglich von n abhängige Schranke M_n gefunden werden so, daß jede Rechtsidealklasse einer R-Maximalordnung einen Vertreter I enthält mit $\mathrm{Nr}_{\mathfrak{D}/\mathbb{Q}}(I) \leq M_n \cdot \sqrt{d(\mathfrak{D}/\mathbb{Q})}$.

Die so gewonnene Schranke soll jedoch bei unserem Algorithmus **nicht** dazu verwendet werden, die Vollständigkeit eines Vertretersytems von Idealklassen einer R-Maximalordnung zu gewährleisten. Dazu wird sie sich einfach als zu groß erweisen (vgl. Abbildung 3.1 auf Seite 73). Jedoch liefert sie einen Beweis, daß der Algorithmus terminiert.

Bevor wir uns den Idealklassen widmen, wollen wir zuerst den Minkowskischen Gitterpunktsatz in der später verwendeten Form formulieren.

Satz 3.3.1 (Minkowskischer Gitterpunktsatz) *Sei Γ ein volles Gitter in einem euklidischen Vektorraum V und $X \subset V$ eine zentralsymmetrische und konvexe Teilmenge mit* $\mathrm{vol}\,(X) > 2^{\dim_{\mathbb{R}}(V)}\,\mathrm{vol}\,(\Gamma)$. *Dann enthält X einen von Null verschiedenen Gitterpunkt $x \in \Gamma$.*
Ist X zudem abgeschlossen (also kompakt), so darf in obiger Ungleichung „$\geq$“ stehen.

Beweis: Ein Beweis findet sich in [FT91, (2.6)(Blichfeldt's Lemma), S. 159]. □

Nun zur Herleitung unserer Minkowski-Konstanten. Wir beginnen mit einer Einbettung der Algebra $\mathfrak{D}$ in den $\mathbb{R}$-Vektorraum $\mathbb{R} \otimes_{\mathbb{Q}} \mathfrak{D} \simeq \mathbb{H}^n$.

Es bezeichnen $\sigma_1, \ldots, \sigma_k$ die Einbettungen $K \hookrightarrow \mathbb{R}$. Weiter sei $(1, \mathbf{i}, \mathbf{j}, \mathbf{k})$ die K-Standardbasis von $\mathfrak{D}$ mit $a := \mathbf{i}^2, b := \mathbf{j}^2 \in K$. Dann sind $\sigma_k(-a)$ sowie $\sigma_k(-b)$ stets positiv für alle $1 \leq k \leq n$. Daher induziert jedes σ_k eine Abbildung $\sigma_k \colon \mathfrak{D} \to \mathbb{H}$ via

$$x_1 + x_2\mathbf{i} + x_3\mathbf{j} + x_4\mathbf{k} \mapsto \sigma_k(x_1) + \sigma_k(-a)^{\frac{1}{2}}\sigma_k(x_2)\mathbf{i} + \sigma_k(-b)^{\frac{1}{2}}\sigma_K(x_3)\mathbf{j} + \sigma_k(ab)^{\frac{1}{2}}\sigma_k(x_4)\mathbf{k}$$

Wir erhalten die Inklusion:

$$\varphi \colon \mathfrak{D} \to \mathfrak{D}_{\mathbb{R}} := \prod_{k=1}^{n} \mathbb{H}, \quad x \mapsto (\sigma_k(x))_k \, .$$

Desweiteren versehen wir den $\mathbb{R}$-Vektorraum $\mathfrak{D}_{\mathbb{R}}$ mit dem Skalarprodukt

$$\langle x, y \rangle = \sum_{k=1}^{n} \mathrm{tr}_{\mathbb{H}/\mathbb{R}}(x_k \overline{y}_k) \, .$$

und setzen $(c_1, c_2, c_3, c_4) = (1, -a, -b, ab)$ sowie für $X = \mathfrak{D}$ oder $\mathbb{H}$

$$\rho_l \colon X \to \mathbb{R}, \quad \rho_l(x_1 + x_2\mathbf{i} + x_3\mathbf{j} + x_4\mathbf{k}) = x_l \, .$$

Bemerkung 3.3.2 Die oben definierten Abbildungen $\sigma_k \colon \mathfrak{D} \to \mathbb{H}$ sind $\mathbb{Q}$-Algebrenhomomorphismen, die mit der Konjugation verträglich sind.

Beweis: $\sigma_k(\mathbf{i}^2) = \sigma_k(a) = \sigma_k(-a)(-1) = \left(\sigma_k(-a)^{\frac{1}{2}}\mathbf{i}\right)^2 = \sigma_k(\mathbf{i})^2$. Analoges gilt für $\mathbf{j}$ sowie $\mathbf{k}$. Weiter ist $\sigma_k(\mathbf{ij}) = \sigma_k(ab)^{\frac{1}{2}}\mathbf{ij} = \sigma_k(-a)^{\frac{1}{2}}\mathbf{i}\,\sigma_k(-b)^{\frac{1}{2}}\mathbf{j} = \sigma_k(\mathbf{i})\sigma_k(\mathbf{j})$. Da σ_k $\mathbb{Q}$-linear ist, folgt $\sigma_k(xy) = \sigma_k(x)\sigma_k(y)$ sowie $\overline{\sigma_k(x)} = \sigma_k(\overline{x})$ für alle $x, y \in \mathfrak{D}$. □

Mit dieser Bemerkung ergeben sich folgende Rechenregeln, die im Laufe dieses Abschnittes noch häufiger verwendet werden.

Bemerkung 3.3.3 (Rechenregeln)
Für $\alpha = \alpha_1 + \alpha_2\mathbf{i} + \alpha_3\mathbf{j} + \alpha_4\mathbf{k}$ und $\beta = \beta_1 + \beta_2\mathbf{i} + \beta_3\mathbf{j} + \beta_4\mathbf{k} \in \mathfrak{D}$ gelten:

$$\begin{aligned}
\mathrm{tr}_{\mathbb{H}/\mathbb{R}}(\sigma_k(\alpha)) &= \sigma_k(\mathrm{tr}_{\mathfrak{D}/K}(\alpha)) \\
\mathrm{nr}_{\mathbb{H}/\mathbb{R}}(\sigma_k(\alpha)) &= \sigma_k(\mathrm{nr}_{\mathfrak{D}/K}(\alpha)) \\
(\rho_l \circ \sigma_k)(\alpha) &= (\sigma_k \circ \rho_l)(\alpha) \cdot \sigma_k(c_l)^{\frac{1}{2}} \\
\mathrm{tr}_{\mathfrak{D}/K}(\alpha\overline{\beta}) = 2\sum_{l=1}^{4} \alpha_l\beta_l c_l &= 2\sum_{l=1}^{4} \rho_l(\alpha)\rho_l(\beta)c_l \, .
\end{aligned}$$

Bezeichnen wir mit $(\_\,,\_)$ das Standardskalarprodukt des $\mathbb{R}^{4n}$, so gilt der

Satz 3.3.4 *Der $\mathbb{R}$-Isomorphismus*

$$f\colon \mathfrak{D}_{\mathbb{R}} \to \mathbb{R}^{4n},\ (x_k) \mapsto (z_\nu) \quad \textit{wobei } z_{4(k-1)+l} = \rho_l(x_k)$$

überführt das Skalarprodukt $\langle \_\,,\_ \rangle$ in $2\,(\_\,,\_)$.

Beweis: Es ist f ein Vektorraumisomorphismus. Nach obiger Bemerkung gilt (mit $\mathfrak{D} = \mathbb{H}$):

$$\langle x, y\rangle = \sum_{k=1}^{n} \mathrm{tr}_{\mathbb{H}/\mathbb{R}}(x_k \overline{y}_k) = \sum_{k=1}^{n} 2 \sum_{l=1}^{4} \rho_l(x_k)\rho_l(y_k) = 2\,(f(x), f(y))\,.$$

□

Korollar 3.3.5 *Für eine in $\mathfrak{D}_{\mathbb{R}}$ meßbare Menge X gilt:*

$$\mathrm{vol}\,(X) = 2^n \mathrm{vol}_{Lebesgue}\,(f(X))\,.$$

Lemma 3.3.6 *Sei I ein normales R-Gitter von $\mathfrak{D}$ mit $\mathbb{Z}$-Basis $(\alpha_1, \ldots, \alpha_{4n})$. Dann ist* $\det\left(\mathrm{tr}_{\mathfrak{D}/\mathbb{Q}}(\alpha_i\alpha_j)\right) = \mathrm{Nr}_{\mathfrak{D}/\mathbb{Q}}(I)^2 \cdot d(\mathfrak{D}/\mathbb{Q})$.

Beweis: Ohne Einschränkung ist I ganz. Nun folgt man dem Beweis von Satz 2.9.3.□

Satz 3.3.7 *Sei I ein normales ganzes R-Gitter, so ist $\Gamma = \varphi(I)$ ein volles $\mathbb{Z}$-Gitter in $\mathfrak{D}_{\mathbb{R}}$ mit* $\mathrm{vol}\,(\Gamma) = \mathrm{Nr}_{\mathfrak{D}/\mathbb{Q}}(I)\sqrt{|d(\mathfrak{D}/\mathbb{Q})|}$.

Beweis: Es sei $(\alpha_1, \ldots, \alpha_{4n})$ eine $\mathbb{Z}$-Basis von I und weiter

$$\tau_{4(k-1)+l}(x) = \rho_l(\sigma_k(x)) = \sigma_k(\rho_l(x)) \cdot \sigma_k(c_l)^{\frac{1}{2}}\,.$$

Die Matrizen $A = (\tau_j(\alpha_i))$ und $\overline{A} = \left(\overline{\tau_j(\alpha_i)}\right)$ erfüllen dann $|\det A| = |\det \overline{A}|$, da die Konjugation auf der K-Standardbasis $(1, \mathbf{i}, \mathbf{j}, \mathbf{k})$ von $\mathfrak{D}$ nur die Vorzeichen ändert. Es gelten:

$$\begin{aligned}
2A\overline{A}^{\mathrm{t}} &= \left(2\sum_k \tau_k(\alpha_i)\tau_k(\overline{\alpha_j})\right) = \left(2\sum_k\sum_l \sigma_k(\rho_l(\alpha_i))\sigma_k(\rho_l(\overline{\alpha_j}))\sigma_k(c_l)\right) \\
&= \left(\sum_k \sigma_k\left(2\sum_l \rho_l(\alpha_i)\rho_l(\overline{\alpha}_j)c_l\right)\right) = \left(\sum_k \sigma_k(\mathrm{tr}_{\mathfrak{D}/K}(\alpha_i\alpha_j))\right) \\
&= \left(\mathrm{tr}_{\mathfrak{D}/\mathbb{Q}}(\alpha_i\alpha_j)\right) \\
(\langle\varphi(\alpha_i), \varphi(\alpha_j)\rangle) &= \left(\sum_k \mathrm{tr}_{\mathbb{H}/\mathbb{R}}(\sigma_k(\alpha_i)\overline{\sigma_k(\alpha_j)})\right) = 2\left(\sum_k\sum_l \rho_l(\sigma_k(\alpha_i))\rho_l(\sigma_k(\alpha_j))\right) \\
&= 2\left(\sum_k \tau_k(\alpha_i)\tau_k(\alpha_j)\right) \\
&= 2AA^{\mathrm{t}}
\end{aligned}$$

Damit wird

$$\begin{aligned}\mathrm{vol}\,(\Gamma) &= |\det\left(\langle\varphi(\alpha_j),\varphi(\alpha_i)\rangle\right)|^{\frac{1}{2}} = |\det 2AA^{\mathrm{t}}|^{\frac{1}{2}} = |\det 2A\overline{A}^{\mathrm{t}}|^{\frac{1}{2}}\\ &= |\det\left(\mathrm{tr}_{\mathfrak{D}/\mathbb{Q}}(\alpha_j\alpha_i)\right)|^{\frac{1}{2}} = \mathrm{Nr}_{\mathfrak{D}/\mathbb{Q}}(I)\sqrt{|d(\mathcal{O}_l(I)/\mathbb{Z})|}\\ &= \mathrm{Nr}_{\mathfrak{D}/\mathbb{Q}}(I)\sqrt{|d(\mathfrak{D}/\mathbb{Q})|}\,.\end{aligned}$$

□

Definition 3.3.8 Für $x \in \mathbb{H}$ bezeichne $\|x\| = \sqrt{\mathrm{tr}_{\mathbb{H}/\mathbb{R}}(x\overline{x})} = \sqrt{2\,\mathrm{nr}_{\mathbb{H}/\mathbb{R}}(x)}$.

Für den Rest des Abschnitts seien die Konstanten $\mathbf{A_n}$ definiert als:

$$\mathbf{A_n} = \prod_{k=0}^{n-1}(32k^4+80k^3+70k^2+25k+3) \qquad (n\in\mathbb{N})$$

Lemma 3.3.9 *Die kompakte, zentralsymmetrische und konvexe Menge*

$$X_t = \left\{(x_k)\in\mathfrak{D}_{\mathbb{R}} \mid \sum_{k=1}^{n}\|x_k\| \le t\right\} \quad (t\ge 0)$$

hat das Volumen $\left(\frac{3}{4}\right)^n \pi^{2n}\mathbf{A_n^{-1}}t^{4n}$.

Beweis: Es ist klar, daß die Menge X_t kompakt sowie zentralsymmetrisch ist. Wendet man den Isomorphismus f auf sie an, so erhält man

$$\begin{aligned}f(X_t) &= \left\{(z_i)\in\mathbb{R}^{4n} \mid \sum_{k=0}^{n-1}\sqrt{2(z_{4k+1}^2+z_{4k+2}^2+z_{4k+3}^2+z_{4k+4}^2)} \le t\right\}\\ &= \left\{(z_i)\in\mathbb{R}^{4n} \mid \sum_{k=0}^{n-1}\|(z_{4k+1},z_{4k+2},z_{4k+3},z_{4k+4})\|_4 \le \frac{t}{\sqrt{2}}\right\}\\ &= \left\{z\in\mathbb{R}^{4n} \mid \sum_{k=1}^{n}\|\varrho_k(z)\|_4 \le \frac{t}{\sqrt{2}}\right\}.\end{aligned}$$

Dabei bezeichne $\|\,.\,\|_4$ die Standardnorm des $\mathbb{R}^4$ sowie

$$\varrho_k : \mathbb{R}^{4n}\to\mathbb{R}^4,\ \varrho_k(z_i) = (z_{4(k-1)+1}, z_{4(k-1)+2}, z_{4(k-1)+3}, z_{4k}).$$

Nun wollen wir zeigen, daß $f(X_t)$ konvex ist. Seien dazu $z,\tilde{z}\in f(X_t)$ sowie $\lambda\in[0,1]$ gegeben. Es gilt:

$$\begin{aligned}\sum_{k=1}^{n}\|\varrho(\lambda z+(1-\lambda)\tilde{z})\|_4 &= \sum_{k=1}^{n}\|\lambda\varrho(z)+(1-\lambda)\varrho(\tilde{z})\|_4\\ &\le \sum_{k=1}^{n}(\lambda\|\varrho(z)\|_4+(1-\lambda)\|\varrho(\tilde{z})\|_4)\\ &= \lambda\sum_{k=1}^{n}\|\varrho(z)\|_4+(1-\lambda)\sum_{k=1}^{n}\|\varrho(\tilde{z})\|_4\\ &\le \lambda\frac{t}{\sqrt{2}}+(1-\lambda)\frac{t}{\sqrt{2}} = \frac{t}{\sqrt{2}}\,.\end{aligned}$$

Also ist $f(X_t)$ und damit auch X_t konvex. Es bleibt noch zu zeigen, daß $f(X_t)$ das Lebesgue-Maß $V_n(t) = \left(\frac{3}{8}\right)^n \pi^{2n} \mathbf{A_n}^{-1} t^{4n}$ besitzt.

Im Falle $n = 1$ ist $f(X_t)$ eine vierdimensionale Kugel mit Radius $\frac{t}{\sqrt{2}}$. Das Volumen ergibt sich daher zu $V_1(t) = \frac{\pi^2}{8} t^4 = \frac{3}{8}\pi^2 3^{-1} t^4$.

Es sei nun $n > 1$. Nach dem Übergang zu Polarkoordinaten gilt:

$$\begin{aligned}
V_n(t) &= \int_0^{\frac{t}{\sqrt{2}}} \int_0^{2\pi} \int_0^{\pi} \int_0^{\pi} V_{n-1}(t - \sqrt{2}r) \cdot r^3 \sin\theta_1 (\sin\theta_2)^2 d\theta_2 d\theta_1 d\phi dr \\
&= 2\pi \cdot 2 \cdot \frac{\pi}{2} \cdot \int_0^{\frac{t}{\sqrt{2}}} V_{n-1}(t - \sqrt{2}r) \cdot r^3 dr \\
&= 2\pi^2 \cdot \left(\frac{3}{8}\right)^{n-1} \pi^{2(n-1)} \mathbf{A_{n-1}}^{-1} \int_0^{\frac{t}{\sqrt{2}}} (t - \sqrt{2}r)^{4(n-1)} \cdot r^3 dr \\
&= 2\left(\frac{3}{8}\right)^{n-1} \pi^{2n} \mathbf{A_{n-1}}^{-1} \frac{3}{16} (32(n-1)^4 + 80(n-1)^3 + 70(n-1)^2 + 25(n-1) + 3)^{-1} t^{4n} \\
&= \left(\frac{3}{8}\right)^n \pi^{2n} \mathbf{A_n}^{-1} t^{4n} .
\end{aligned}$$

□

Lemma 3.3.10 *Jedes normale ganze R-Gitter I in $\mathfrak{D}$ besitzt ein Element $x \in I \setminus \{0\}$ mit*

$$|\mathrm{Nr}_{\mathfrak{D}/\mathbb{Q}}(x)| \leq \left(\frac{2}{n}\right)^{4n} \frac{1}{3^n \pi^{2n}} \mathbf{A_n} \, \mathrm{Nr}_{\mathfrak{D}/\mathbb{Q}}(I) \sqrt{|d(\mathfrak{D}/\mathbb{Q})|} \, .$$

Beweis: Setzen wir $t_0^{4n} := \frac{2^{6n}}{3^n} \pi^{-2n} \mathbf{A_n} \, \mathrm{Nr}_{\mathfrak{D}/\mathbb{Q}}(I) \sqrt{|d(\mathfrak{D}/\mathbb{Q})|}$. Damit wird $\mathrm{vol}\,(X_{t_0}) = 2^{4n} \mathrm{vol}\,(\varphi(I))$. Nach dem Minkowskischen Gitterpunktsatz besitzt $\varphi(I)$ nun einen von Null verschiedenen Punkt $\varphi(x)$ und die Norm von x ergibt sich zu

$$\begin{aligned}
|\mathrm{Nr}_{\mathfrak{D}/\mathbb{Q}}(x)| &= \prod_{k=1}^{n} |\sigma_k(\mathrm{Nr}_{\mathfrak{D}/K}(x))| = \prod_{k=1}^{n} |\sigma_k(\mathrm{nr}_{\mathfrak{D}/K}(x)^2)| = \prod_{k=1}^{n} \mathrm{nr}_{\mathbb{H}/\mathbb{R}}(\sigma_k(x))^2 \\
&= \frac{1}{4^n} \left(\prod_{k=1}^{n} \sqrt{2 \, \mathrm{nr}_{\mathbb{H}/\mathbb{R}}(\sigma_k(x))} \right)^4 = \frac{1}{4^n} \left(\left(\prod_{k=1}^{n} \sqrt{2 \, \mathrm{nr}_{\mathbb{H}/\mathbb{R}}(\sigma_k(x))} \right)^{\frac{1}{n}} \right)^{4n} \\
&\leq \frac{1}{4^n} \left(\frac{1}{n} \sum_{k=1}^{n} \sqrt{2 \, \mathrm{nr}_{\mathbb{H}/\mathbb{R}}(\sigma_k(x))} \right)^{4n} = \frac{1}{4^n} \frac{1}{n^{4n}} t_0^{4n} \\
&= \left(\frac{2}{n}\right)^{4n} \frac{1}{3^n \pi^{2n}} \mathbf{A_n} \, \mathrm{Nr}_{\mathfrak{D}/\mathbb{Q}}(I) \sqrt{|d(\mathfrak{M}/\mathbb{Z})|} \, .
\end{aligned}$$

□

Satz 3.3.11 (Minkowski-Schranke) *Jede Rechtsidealklasse einer R-Maximalordnung $\mathfrak{M}$ (bezüglich Linksäquivalenz) enthält ein ganzes $\mathfrak{M}$-Rechtsideal I mit*

$$Nr_{\mathfrak{D}/\mathbb{Q}}(I) \leq \left(\frac{2}{n}\right)^{4n} \frac{1}{3^n \pi^{2n}} \mathbf{A_n} \sqrt{|d(\mathfrak{D}/\mathbb{Q})|}\,.$$

Beweis: Sei J ein $\mathfrak{M}$-Rechtsideal einer solchen Rechtsidealklasse und $y \in R \setminus \{0\}$ derart, daß $J^{-1}y$ ein ganzes R-Gitter ist. Dieses besitzt nach dem vorangegangenen Lemma ein Element $x \in J^{-1}y \setminus \{0\}$ mit

$$|\mathrm{Nr}_{\mathfrak{D}/\mathbb{Q}}(x)| \leq \left(\frac{2}{n}\right)^{4n} \frac{1}{3^n \pi^{2n}} A_n \mathrm{Nr}_{\mathfrak{D}/\mathbb{Q}}(J^{-1}y) \sqrt{|d(\mathfrak{D}/\mathbb{Q})|}\,.$$

Dann ist $I := xy^{-1}J \subseteq J^{-1}J$ ein zu J linksäquivalentes ganzes $\mathfrak{M}$-Rechtsideal mit

$$\mathrm{Nr}_{\mathfrak{D}/\mathbb{Q}}(I) = |\mathrm{Nr}_{\mathfrak{D}/\mathbb{Q}}(x)| \cdot \mathrm{Nr}_{\mathfrak{D}/\mathbb{Q}}(J^{-1}y)^{-1} \leq \left(\frac{2}{n}\right)^{4n} \frac{1}{3^n \pi^{2n}} \mathbf{A_n} \sqrt{|d(\mathfrak{D}/\mathbb{Q})|}\,.$$

□

Nach Lemma 2.9.6 gilt in obigem Satz

$$\mathrm{Nr}_{\mathfrak{D}/\mathbb{Q}}(I) \leq \left(\frac{2}{n}\right)^{4n} \frac{1}{3^n \pi^{2n}}\, \mathbf{A_n}\, d(K/\mathbb{Q})^2 \sqrt{|\mathrm{Nr}_{K/\mathbb{Q}}(d(\mathfrak{D}/\mathbb{Z}_K))|}\,.$$

Um zu verdeutlichen, daß die gerade bestimmte Schranke wegen ihrer Größe ungeeignet ist in einem konkreten Fall die Vollständigkeit eines Repräsentantensystems von Idealklassen zu gewährleisten, wollen wir zum Abschluß des Abschnitts den Term $(*) = \left(\frac{2}{n}\right)^{4n} \frac{1}{3^n \pi^{2n}}\, \mathbf{A_n}\, d(K/\mathbb{Q})^2$ nach unten abschätzen:

n	1	2	3	4	5	6	7	8
$(*) \leq$	2	18	667	53306	$7.69 \cdot 10^6$	$1.12 \cdot 10^9$	$1.72 \cdot 10^{12}$	$1.15 \cdot 10^{14}$

Abbildung 3.1: Abschätzung der Minkowskischranke nach unten

Dabei wurden für die Diskriminanten der Zahlkörper $d(K/\mathbb{Q})$ bekannte untere Schranken eingesetzt [1].

Korollar 3.3.12 *Es existieren nur endlich viele Rechtsidealklassen einer R-Maximalordnung $\mathfrak{M}$ von $\mathfrak{D}$.*

Beweis: Es genügt zu zeigen, daß es für jedes $k \in \mathbb{N}$ nur endlich viele ganze $\mathfrak{M}$-Rechtsideale I mit $\mathrm{Nr}_{\mathfrak{D}/\mathbb{Q}}(I) = k$ gibt. Sei also I ein solches $\mathfrak{M}$-Rechtsideal. Wir fassen $\mathfrak{M}$ und I als $\mathbb{Z}$-Gitter auf. Dann ist jeder Elementarteiler von I ein Teiler von k, also gilt $k\mathfrak{M} \subseteq I$. Da $\mathfrak{M}/k\mathfrak{M}$ eine endliche abelsche Gruppe bildet, kann es daher nur endlich viele solcher $\mathfrak{M}$-Rechtsideale geben. □

[1] [Odl89, Tabelle 1, S. 12]

Kapitel 4

Maßformel

In diesem Kapitel sei $\mathfrak{D}$ eine total definite Quaternionenalgebra mit $K := Z(\mathfrak{D})$ einem total reellen Zahlkörper. Weiter bezeichnen h_K die Klassenzahl von K sowie $R = \mathbb{Z}_K$ und $n = [K : \mathbb{Q}]$. Ferner seien die in $\mathfrak{D}$ verzweigten endlichen Stellen gegeben durch die Primideale $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ von R.

Es sollen nun die Hilfsmittel bereitgestellt werden, um in Kapitel 5 einen Algorithmus angeben zu können, der (bis auf Konjugation) alle R-Maximalordnungen von $\mathfrak{D}$ bestimmt.

4.1 Maßformel nach Eichler

Es sei $\mathfrak{M}$ eine R-Maximalordnung in $\mathfrak{D}$. In Korollar 3.3.12 haben wir gesehen, daß es nur endlich viele Rechtsidealklassen von $\mathfrak{M}$ gibt. Ist $\{I_1, \ldots, I_H\}$ ein Vertretersystem dieser Klassen, so enthält $\{\mathcal{O}_l(I_i) \mid 1 \leq i \leq H\}$ nach Korollar 2.6.6 ein Vertretersystem aller Typen von R-Maximalordnungen.

Für $1 \leq i \leq H$ setzen wir $\mathfrak{M}_i := \mathcal{O}_l(I_i)$, sowie $\omega_i := [\mathfrak{M}_i^* : R^*]$. Zwei isomorphe R-Maximalordnungen $\mathfrak{M}_i$ und $\mathfrak{M}_j$ besitzen dann denselben Einheitenindex $\omega_i = \omega_j$.

Nach Korollar 2.6.6 können wir annehmen, daß die ersten T R-Maximalordnungen alle Typen repräsentieren. Bezeichnen wir mit H_i die Anzahl der Isomorphieklassen von zweiseitigen $\mathfrak{M}_i$-Idealen, so haben wir in Satz 2.6.5 bereits gezeigt, daß $\mathfrak{M}_i$ für alle $1 \leq i \leq T$ zu genau H_i R-Maximalordnungen aus $\{\mathfrak{M}_1, \ldots, \mathfrak{M}_H\}$ konjugiert ist. Daher ist

$$\sum_{i=1}^{H} \omega_i^{-1} = \sum_{i=1}^{T} \omega_i^{-1} H_i \,.$$

Satz 4.1.1 (Eichler) *Es gelten die obigen Bezeichnungen. Weiter seien h_K die Klassenzahl von K und $D = d(\mathfrak{D}/K)$ die Diskriminante von $\mathfrak{D}$. Dann gilt die* Eichlersche Maßformel*:*

$$\sum_{i=1}^{T} \omega_i^{-1} H_i = \sum_{i=1}^{H} \omega_i^{-1} = 2^{1-n} |\zeta_K(-1)| h_K \prod_{\mathfrak{p} \mid D} \left(\mathrm{Nr}_{K/\mathbb{Q}}(\mathfrak{p}) - 1 \right)$$

Das Produkt laufe dabei über alle Primideale $\mathfrak{p}$ von $\mathbb{Z}_K$ die D teilen.

Beweis: Der Beweis ist im Vergleich zu den anderen Aussagen lang und erfordert einen nicht unerheblichen Aufwand an Maßtheorie auf den hier nicht eingegangen wurde. Daher verweisen wir auf [Vig80, Corollaire 2.3, S. 142]. □

Da alle ω_i positiv sind, liefert dieser Satz ein explizites Kriterium, wann alle Typen von R-Maximalordnungen gefunden sind.

4.1.1 Auswerten der Maßformel

Wir wollen nun die Summanden $\omega_i^{-1} H_i$ bei gegebenem $\mathfrak{M}_i$ explizit bestimmen. Hierzu seien

$$\begin{aligned} \mathfrak{M}_i^{*,1} &:= \left\{ x \in \mathfrak{M}_i \mid \mathrm{nr}_{\mathfrak{D}/K}(x) = 1 \right\} \\ \omega_i^1 &:= \left[\mathfrak{M}_i^{*,1} : \{\pm 1\} \right] = \frac{1}{2} |\mathfrak{M}_i^{*,1}| \\ \omega_i^{nq} &:= \left[\mathrm{nr}_{\mathfrak{D}/K}(\mathfrak{M}_i^*) : (R^*)^2 \right] . \end{aligned}$$

Ferner setzen wir

$$N \colon \mathfrak{D} \times \mathfrak{D} \to K,\ (x,y) \mapsto \mathrm{tr}_{\mathfrak{D}/K}(x\overline{y}) \quad \text{und} \quad N_{\mathbb{Q}} := \mathrm{Tr}_{K/\mathbb{Q}} \circ N \, .$$

Wegen $N(x,x) = 2\,\mathrm{nr}_{\mathfrak{D}/K}(x)$ für alle $x \in \mathfrak{D}$ ist N eine nicht ausgeartete Bilinearform auf $\mathfrak{D}$. Da $N(x,x)$ für alle $x \in \mathfrak{D}$ total positiv ist, ist $N_{\mathbb{Q}}$ positiv definit.

Die Ergebnisse dieses Abschnitts gehen auf Eichler zurück und finden sich z.B. in [Neb98].

Bemerkung 4.1.2 $\mathfrak{M}_i^{*,1}$ ist die Menge der kürzesten Vektoren des $\mathbb{Z}$-Gitters $(\mathfrak{M}_i, N_{\mathbb{Q}})$.

Beweis: Es sei α ein total positives Element von R. Weiter bezeichne G die Menge der Einbettungen $K \hookrightarrow \mathbb{R}$. Mit der Ungleichung zwischen arithmetischem und geometrischem Mittel erhalten wir

$$\frac{1}{n} \mathrm{Tr}_{K/\mathbb{Q}}(\alpha) = \frac{1}{n} \sum_{\sigma \in G} \sigma(\alpha) \geq \left(\prod_{\sigma \in G} \sigma(\alpha) \right)^{\frac{1}{n}} = \mathrm{Nr}_{K/\mathbb{Q}}(\alpha)^{\frac{1}{n}} \geq 1 \, . \qquad (*)$$

In der obigen Ungleichung gilt bekanntlich genau dann Gleichheit, wenn $\alpha = \sigma(\alpha)$ für alle $\sigma \in G$ ist und zusätzlich noch $\mathrm{Nr}_{K/\mathbb{Q}}(\alpha) = 1$ gilt. Also ist $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha) = n \iff \alpha = 1$. Außerdem folgt aus $(*)$ auch $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha) \geq n$ für alle total positiven $\alpha \in R$. Wegen $\mathrm{Tr}_{K/\mathbb{Q}}(1) = n$ sind die kürzesten Vektoren von $(\mathfrak{M}_i, N_{\mathbb{Q}})$ gerade die $x \in \mathfrak{M}_i$ mit $\mathrm{nr}_{\mathfrak{D}/K}(x) = 1$. □

Lemma 4.1.3 *Ist (L, ϕ) ein positiv definites $\mathbb{Z}$-Gitter im $\mathbb{R}^n$ und $l \in \mathbb{R}$ beliebig, so existieren nur endlich viele $x \in L$ mit $\phi(x,x) \leq l$.*

Beweis: Sei $\{b_1, \ldots, b_n\}$ eine $\mathbb{Z}$-Basis des Gitters L und $x = \sum_{i=1}^{n} x_i b_i \in L$ mit $\phi(x,x) \leq l$. Da alle $\phi(b_i, b_i)$ endlich und je zwei Normen auf $\mathbb{R}^n$ äquivalent sind, existiert eine Konstante $c > 0$ mit $\max |x_i| \leq c\sqrt{\phi(x,x)} \leq c\sqrt{l}$. Insbesondere gibt es für die Wahl der i-ten Koordinate x_i nur endlich viele Möglichkeiten. □

Lemma 4.1.4 *Es gilt $\omega_i = \omega_i^1 \omega_i^{nq}$. Weiter sind diese 3 Indizes alle endlich.*

Beweis: Wir haben folgende exakte Sequenzen:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathfrak{M}_i^{*,1} & \longrightarrow & \mathfrak{M}_i^{*} & \xrightarrow{\mathrm{nr}} & \mathrm{nr}_{\mathfrak{D}/K}(\mathfrak{M}_i^{*}) & \longrightarrow & 1 \\ & & \uparrow & & \uparrow & & \uparrow & & \\ 1 & \longrightarrow & \{\pm 1\} & \longrightarrow & R^{*} & \longrightarrow & (R^{*})^2 & \longrightarrow & 1 \end{array}$$

Mit dem Schlangenlemma folgt $\omega_i = \omega_i^1 \omega_i^{nq}$.

Der Dirichletsche Einheitensatz zeigt, daß $[R^* : (R^*)^2] = 2^{n+1}$ endlich ist. Daher gilt dies auch für ω_i^{nq}. Aus Lemma 4.1.3 und Bemerkung 4.1.2 folgt daß ω_i^1 und damit ω_i endlich sind. □

Im Folgenden soll nun der enge Zusammenhang zwischen $\omega_i^{-1} H_i$ und der Automorphismenanzahl des R-Gitters $(\mathfrak{M}_i, N)$ hergestellt werden.

Dazu sei $\mathfrak{D}_0 := \{x \in \mathfrak{D} \mid \mathrm{tr}_{\mathfrak{D}/K}(x) = 0\}$ der Kern der reduzierten Spur. Weiter sei

$$\mathrm{O}(\mathfrak{D}, N) := \{\varphi \in \mathfrak{D} \to \mathfrak{D} \mid \varphi \text{ ist } K\text{-linear}, \ N(x,x) = N(\varphi(x), \varphi(x)) \text{ für alle } x \in \mathfrak{D}\}$$

die *orthogonale Gruppe* und $\mathrm{SO}(\mathfrak{D}, N) = \{\varphi \in \mathrm{O}(\mathfrak{D}, N) \mid \det(\varphi) = 1\}$ die *spezielle orthogonale Gruppe* des K-Vektorraums $\mathfrak{D}$ bezüglich der quadratischen Form N.
Für ein R-Gitter Λ sei $\mathrm{O}(\Lambda, N) := \{\varphi \in \mathrm{O}(\mathfrak{D}, N) \mid \varphi(\Lambda) = \Lambda\}$ und $\mathrm{SO}(\Lambda, N) := \{\varphi \in \mathrm{SO}(\mathfrak{D}, N) \mid \varphi(\Lambda) = \Lambda\}$.

Es ist klar, daß $x \in \mathfrak{D}_0 \iff \overline{x} = -x$ gilt. Ist $\varphi \in \mathrm{SO}(\mathfrak{D}, N)$ und sind $x, y \in \mathfrak{D}$, so hat man die Identität

$$\begin{aligned} \mathrm{tr}_{\mathfrak{D}/K}(\varphi(x)\overline{\varphi(y)}) &= \mathrm{nr}_{\mathfrak{D}/K}(\varphi(x+y)) - \mathrm{nr}_{\mathfrak{D}/K}(\varphi(x)) - \mathrm{nr}_{\mathfrak{D}/K}(\varphi(y)) \\ &= \mathrm{nr}_{\mathfrak{D}/K}(x+y) - \mathrm{nr}_{\mathfrak{D}/K}(x) - \mathrm{nr}_{\mathfrak{D}/K}(y) \\ &= \mathrm{tr}_{\mathfrak{D}/K}(x\overline{y}) \,. \end{aligned}$$

Satz 4.1.5 *Es gilt* $\mathrm{SO}(\mathfrak{D}, N) = \{x \mapsto edxd^{-1} \mid e, d \in \mathfrak{D}^*, \ \mathrm{nr}_{\mathfrak{D}/K}(e) = 1, \}$.

Beweis: Man verifiziert, daß $\varphi\colon x \mapsto edxd^{-1}$ eine Isometrie bezüglich N ist. Wegen der Multiplikativität der Determinanten und $\det(y \mapsto y \cdot e) = \mathrm{Nr}_{\mathfrak{D}/K}(e) = 1$ folgt $\det \varphi = 1$.

Sei nun umgekehrt $\varphi \in \mathrm{SO}(\mathfrak{D}, N)$. Wir setzen $e := \varphi(1)$, damit wird $\mathrm{nr}_{\mathfrak{D}/K}(e) = 1$. Wegen des Satzes von Skolem-Noether genügt es zu zeigen, daß $\phi\colon x \mapsto e^{-1}\varphi(x)$ ein K-Algebrenautomorphismus ist:
Dazu sei $(1, \mathbf{i}, \mathbf{j}, \mathbf{ij})$ die K-Standardbasis von $\mathfrak{D}$ und $\mathfrak{D}_0 = \langle \mathbf{i}, \mathbf{j}, \mathbf{ij} \rangle$ der Kern der reduzierten Spur. Wir setzen $b_1 = \mathbf{i}, b_2 = \mathbf{j}, b_3 = \mathbf{ij}$. Wegen $\mathrm{tr}_{\mathfrak{D}/K}(\phi(b_i)1) = \mathrm{tr}_{\mathfrak{D}/K}(b_i) = 0$ ist $\mathfrak{D}_0$ ein ϕ-invarianter Teilraum der von $\{\phi(b_i) \mid i = 1, 2, 3\}$ erzeugt wird. Also gilt $\overline{\phi(b_i)} = -\phi(b_i)$ und somit $\mathrm{tr}_{\mathfrak{D}/K}(\phi(x)\phi(y)) = \mathrm{tr}_{\mathfrak{D}/K}(xy)$ für alle $x, y \in \mathfrak{D}_0$.
Für $i \neq j$ ist insbesondere $\mathrm{tr}_{\mathfrak{D}/K}(\phi(b_i)\phi(b_j)) = \mathrm{tr}_{\mathfrak{D}/K}(b_i b_j) = 0$, was $\phi(b_i)\phi(b_j) \in \mathfrak{D}_0$ zeigt. Daher existieren $x_1, x_2, x_3 \in K$ mit $\phi(\mathbf{i})\phi(\mathbf{j}) = \sum_{i=1}^{3} x_i \phi(b_i)$. Nun gilt

$$\begin{aligned} 0 &= \mathrm{tr}_{\mathfrak{D}/K}(\mathrm{nr}_{\mathfrak{D}/K}(\phi(\mathbf{i}))\phi(\mathbf{j})) = \mathrm{tr}_{\mathfrak{D}/K}(\phi(\mathbf{i})^2\phi(\mathbf{j})) \\ &= \sum_{i=1}^{3} x_i \,\mathrm{tr}_{\mathfrak{D}/K}(\phi(b_1)\phi(b_i)) = -x_1 \,\mathrm{tr}_{\mathfrak{D}/K}(\phi(\mathbf{i})\overline{\phi(\mathbf{i})}) \\ &= -2x_1 \,\mathrm{nr}_{\mathfrak{D}/K}(\mathbf{i})\,. \end{aligned}$$

Also ist $x_1 = 0$. Analog folgert man $x_2 = 0$ und $\mathrm{nr}_{\mathfrak{D}/K}(\mathbf{ij}) = \mathrm{nr}_{\mathfrak{D}/K}(\phi(\mathbf{i})\phi(\mathbf{j})) = \mathrm{nr}_{\mathfrak{D}/K}(x_3\phi(\mathbf{ij})) = x_3^2 \,\mathrm{nr}_{\mathfrak{D}/K}(\mathbf{ij})$ impliziert schließlich $x_3 = \pm 1$.

Gilt $x_3 = +1$, so ist ϕ multiplikativ und der Satz damit bewiesen. Andernfalls unterscheidet sich ϕ, wie wir gerade gesehen haben, auf $\langle \mathbf{ij} \rangle$ um eine Spiegelung von einem Element aus $\mathrm{SO}(\mathfrak{D}, N)$. Dann ergibt $\det(\varphi) = \det(\phi) = -1$ jedoch einen Widerspruch. □

Korollar 4.1.6 *Zwei R-Ordnungen Λ_1 und Λ_2 sind genau dann konjugiert, wenn die beiden R-Gitter (Λ_1, N) und (Λ_2, N) isometrisch sind.*

Beweis: Sind Λ_1 und Λ_2 konjugiert, so sind (Λ_1, N) und (Λ_2, N) isometrisch. Sei umgekehrt $\varphi\colon \Lambda_1 \to \Lambda_2$ eine Isometrie bezüglich N. Da die kanonische Involution einen K-Automorphismus auf $\mathfrak{D}$ mit Determinante -1 induziert und die beiden R-Ordnungen Λ_i fixiert, können wir annehmen, daß sich φ zu einem Element aus $\mathrm{SO}(\mathfrak{D}, N)$ fortsetzen läßt. Also existieren $e \in \mathfrak{D}$ mit $\mathrm{nr}_{\mathfrak{D}/K}(e) = 1$ und $d \in \mathfrak{D}^*$ derart, daß $\Lambda_1 = ed\Lambda_2 d^{-1}$. Wegen $1 \in \Lambda_2$ gilt $e \in \Lambda_1^*$ und damit ist $\Lambda_1 = d\Lambda_2 d^{-1}$. □

Korollar 4.1.7 *Für jede R-Ordnung Λ von $\mathfrak{D}$ gilt*

$$\mathrm{SO}(\Lambda, N) = \left\{ x \mapsto edxd^{-1} \mid e \in \Lambda,\ \mathrm{nr}_{\mathfrak{D}/K}(e) = 1,\ d \in \mathfrak{D}^*,\ d\Lambda = \Lambda d \right\}.$$

Beweis: Jedes Element aus $\mathrm{SO}(\Lambda, N)$ läßt sich eindeutig fortsetzen zu einem $\varphi \in \mathrm{SO}(\mathfrak{D}, N)$. Also ist $\varphi(x) = edxd^{-1}$ mit $d \in \mathfrak{D}^*$ und $\mathrm{nr}_{\mathfrak{D}/K}(e) = 1$. Es folgt $e = \varphi(1) \in \Lambda$ und damit $\Lambda = ed\Lambda d^{-1} = d\Lambda d^{-1}$. Die umgekehrte Inklusion ist klar. □

Wir führen nun folgende Bezeichnungen ein:

$\mathcal{J}_i$ die Gruppe der zweiseitigen $\mathfrak{M}_i$-Ideale
$\mathcal{P}_i = \{I \in \mathcal{J}_i \mid I \text{ ist ein Hauptideal}\}$
$\mathcal{Z}_i = \{\mathfrak{a}\mathfrak{M}_i \mid \mathfrak{a} \neq \{0\} \text{ ein gebrochenes } R\text{-Ideal in } K\}$
$\mathcal{H}_i = \{\lambda\mathfrak{M}_i \mid \lambda \in K^*\}$

Bemerkung 4.1.8 Es sei $\mathfrak{M}$ eine R-Maximalordnung. Ist $\mathfrak{a}$ ein gebrochenes R-Ideal in K, so gilt

$$\mathfrak{a}\mathfrak{M} = \mathfrak{M} \iff \mathfrak{a} = R\,.$$

Denn aus $\mathfrak{a}\mathfrak{M} = \mathfrak{M}$ folgt $\mathfrak{a} \subseteq (\mathfrak{a}\mathfrak{M}) \cap K = \mathfrak{M} \cap K = R$. Angenommen $\mathfrak{a}$ läge nun in einem maximalen Ideal $\mathfrak{p}$ von R, so liefert Nakayama's Lemma angewandt auf $\mathfrak{a}_\mathfrak{p}\mathfrak{M}_\mathfrak{p} = \mathfrak{M}_\mathfrak{p}$ den Widerspruch $\mathfrak{M}_\mathfrak{p} = 0$. Die Umkehrung der Aussage ist natürlich trivial.

Ist nun $\mathfrak{b}$ ein weiteres gebrochenes R-Ideal in K, so folgt aus der obigen Äquivalenz die Beziehung

$$\mathfrak{a}\mathfrak{M} = \mathfrak{b}\mathfrak{M} \iff \mathfrak{a} = \mathfrak{b}\,.$$

Insbesondere ist $[\mathcal{Z}_i : \mathcal{H}_i] = h_K$.

Ist das Primideal $\mathfrak{p}$ von R in $\mathfrak{D}$ verzweigt, so ist $\mathrm{rad}(\hat{\mathfrak{M}}_\mathfrak{p})$ das einzige maximal ganze zweiseitige $\hat{\mathfrak{M}}_\mathfrak{p}$-Ideal und alle anderen $\hat{\mathfrak{M}}_\mathfrak{p}$-Linksideale bzw. $\hat{\mathfrak{M}}_\mathfrak{p}$-Rechtsideale sind Potenzen von $\mathrm{rad}(\hat{\mathfrak{M}}_\mathfrak{p})$. Weiter ist $\mathrm{rad}(\hat{\mathfrak{M}}_\mathfrak{p})$ ein maximal ganzes $\hat{\mathfrak{M}}_\mathfrak{p}$-Linksideal und ein maximal ganzes $\hat{\mathfrak{M}}_\mathfrak{p}$-Rechtsideal von $\hat{\mathfrak{M}}_\mathfrak{p}$, denn $\hat{\mathfrak{D}}_\mathfrak{p}$ besitzt nur die eine R-Maximalordnung $\hat{\mathfrak{M}}_\mathfrak{p}$. Ferner gilt $\mathrm{rad}(\hat{\mathfrak{M}}_\mathfrak{p})^2 = \mathfrak{p}\hat{\mathfrak{M}}_\mathfrak{p}$.
Ist $\mathfrak{p}$ jedoch nicht verzweigt, so ist $\hat{\mathfrak{D}}_\mathfrak{p}$ isomorph zu $\hat{K}_\mathfrak{p}^{2\times 2}$ und die zweiseitigen $\hat{\mathfrak{M}}_\mathfrak{p}$-Ideale sind dann Potenzen von $\mathfrak{p}\hat{\mathfrak{M}}_\mathfrak{p}$.

Aus Satz 2.5.25 und Satz 2.7.27 folgt: Sind $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ die in $\mathfrak{D}$ verzweigten Primideale und $\mathfrak{P}_1, \ldots, \mathfrak{P}_s$ die darüberliegenden Primideale von $\mathfrak{M}$, so bildet

$$\left\{ \prod_{j=1}^{s} {\mathfrak{P}_j}^{\alpha_j} \mid (\alpha_1, \ldots, \alpha_s) \in \{0,1\}^s \right\}$$

ein Repräsentantensystem der Klassen von $\mathcal{J}_i/\mathcal{Z}_i$. Weiter sind die Primideale $\mathfrak{P}_i$ nach Satz 2.5.36 und Satz 2.7.27 maximal ganze $\mathfrak{M}$-Linksideale und maximal ganze $\mathfrak{M}$-Rechtsideale. Weiter gilt $[\mathcal{J}_i : \mathcal{H}_i] = 2^s \cdot h_K$.

Damit können wir den Zusammenhang der Automorphismenanzahl mit $\omega_i^{-1}H_i$ konkret angeben:

Satz 4.1.9 *Es gilt* $|\mathrm{O}(\mathfrak{M}_i, N)| = 2^{s+2} h_K \omega_i^1 \omega_i H_i^{-1}$.

Beweis: Die kanonische Involution läßt $\mathfrak{M}_i$ fest und induziert somit einen Automorphismus auf $\mathfrak{M}_i$ mit Determinante -1. Daher ist

$$A := |\mathrm{O}(\mathfrak{M}_i, N)| = 2\,|\mathrm{SO}(\mathfrak{M}_i, N)|\,.$$

Sei $U := \{y \mapsto xyx^{-1} \mid x \in \mathfrak{D}^*,\ x\mathfrak{M}_i x^{-1} = \mathfrak{M}_i\} \leq \mathrm{SO}(\mathfrak{M}_i, N)$. Nach Korollar 4.1.7 gilt $A = 4\omega_i^1\,|U|$.
Wir setzen nun $U_1 := \{y \mapsto xyx^{-1} \mid x \in \mathfrak{M}_i^*\}$. Dies ist ein Normalteiler von U. Für $x \in \mathfrak{M}_i^*$ gilt $y \mapsto xyx^{-1} = \mathrm{id}_{\mathfrak{M}_i}$ genau dann, wenn $x \in R^*$ liegt. Daher ist $|U_1| = [\mathfrak{M}_i^* : R^*] = \omega_i$.

Weiter sei $\varphi\colon \mathcal{P}_i \to U/U_1,\ x\mathfrak{M}_i \mapsto (y \mapsto xyx^{-1})$. Angenommen, es ist $x\mathfrak{M}_i = x'\mathfrak{M}_i$. Dann gilt auch $x^{-1}x' \in \mathfrak{M}_i^*$ und somit ist φ wohldefiniert und wir erhalten

$$\ker(\varphi) = \{x\mathfrak{M}_i \mid y = xyx^{-1} \text{ für alle } y \in \mathfrak{M}_i\} = \{x\mathfrak{M}_i \mid x \in K\} = \mathcal{H}_i\,.$$

Damit ist $U/U_1 \cong \mathcal{P}_i/\mathcal{H}_i$ und somit $[U : U_1] = [\mathcal{P}_i : \mathcal{H}_i]$. Zusammen folgt

$$\begin{aligned} A &= 4\omega_i^1|U| = 4\omega_i^1\omega_i \cdot [\mathcal{P}_i : \mathcal{H}_i] = 4\omega_i^1\omega_i \cdot [\mathcal{J}_i : \mathcal{H}_i] \cdot [\mathcal{J}_i : \mathcal{P}_i]^{-1} \\ &= 4\omega_i^1\omega_i \cdot (2^s h_K) \cdot H_i^{-1}\,. \end{aligned}$$

□

4.2 Galoisautomorphismen

Es sei $\mathfrak{D}$ eine total-definite Quaternionenalgebra mit $Z(\mathfrak{D}) = K$ ein total reeller Zahlkörper derart, daß $K/\mathbb{Q}$ galoisch ist. Weiter sei dann $R = \mathbb{Z}_K$ der ganze Abschluß von $\mathbb{Z}$ in K.

Wir wollen im Folgenden untersuchen, wann die Galoisautomorphismen von $K/\mathbb{Q}$ eine Operation auf den Konjugationsklassen der R-Maximalordnungen von $\mathfrak{D}$ induzieren. Dazu sei $\mathfrak{D} = \left(\frac{a,b}{K}\right)$ und $(b_1 = 1, b_2 = \mathbf{i}, b_3 = \mathbf{j}, b_4 = \mathbf{ij})$ die Standardbasis von $\mathfrak{D}$ über K.

Definition 4.2.1 Man sagt, $\mathfrak{D}$ habe *gleichmäßig verteilte Invarianten* (uniformly distributed invariants), falls für jede Primzahl p entweder alle Primideale von R über p in $\mathfrak{D}$ verzweigen oder aber keines.

Satz 4.2.2 *Es gibt genau dann für jedes $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ ein $\varphi_\sigma \in \mathrm{Aut}_{\mathbb{Q}}(\mathfrak{D})$ mit $\varphi_\sigma|_K = \sigma$, wenn $\mathfrak{D}$ gleichmäßig verteilte Invarianten besitzt.*

Beweis: Via $*\colon K \times \mathfrak{D} \to \mathfrak{D},\ (\lambda, d) \mapsto \lambda * d := \sigma(\lambda)d$ wird $(\mathfrak{D}, +, *)$ zu einer K-Algebra, welche wir mit $\tilde{\mathfrak{D}}$ bezeichnen wollen. Da jedes Element in $\mathfrak{D}$ invertierbar ist, ist auch $\tilde{\mathfrak{D}}$ ein Schiefkörper.
Für ein Primideal $\mathfrak{p}$ über pR bezeichne dann

$$\hat{\sigma}\colon K \otimes_{\mathbb{Q}} \hat{\mathbb{Q}}_p \to K \otimes_{\mathbb{Q}} \hat{\mathbb{Q}}_p,\ \lambda \otimes c \mapsto \sigma(\lambda) \otimes c$$

die Fortsetzung von σ. Ist $pR = \sum_{i=1}^k \mathfrak{p}_i^{e_i}$ eine Zerlegung in verschiedene Primideale, so gilt $K \otimes_{\mathbb{Q}} \hat{\mathbb{Q}}_p = \bigoplus_{i=1}^k \hat{K}_{\mathfrak{p}_i}$. Daher können wir $\hat{\sigma}$ als Fortsetzung von σ auf $\hat{K}_{\mathfrak{p}}$ für jedes Primideal $\mathfrak{p}$ über p auffassen. Damit wird

$$\hat{K}_{\mathfrak{p}} \otimes_K \tilde{\mathfrak{D}} \to \hat{K}_{\sigma(\mathfrak{p})} \otimes_K \mathfrak{D},\ \lambda \otimes \tilde{d} \mapsto \hat{\sigma}(\lambda) \otimes \tilde{d}$$

ein Isomorphismus, denn die Abbildung ist wohldefiniert, weil für jedes $c \in K$ gilt

$$\begin{array}{ccc} c\lambda \otimes \tilde{d} & \longrightarrow & \hat{\sigma}(c\lambda) \otimes \tilde{d} \\ \| & & \| \\ \lambda \otimes \sigma(c)\tilde{d} & \longrightarrow & \hat{\sigma}(\lambda) \otimes \sigma(c)\tilde{d}\,. \end{array}$$

Also verzweigt $\tilde{\mathfrak{D}}$ an einem Primideal $\mathfrak{p}$ genau dann, wenn $\mathfrak{D}$ an $\sigma(\mathfrak{p})$ verzweigt.

Ist nun $\varphi_\sigma \in \mathrm{Aut}_{\mathbb{Q}}(\mathfrak{D})$ mit $\varphi_\sigma|_K = \sigma$, so liefert $x \mapsto \varphi_\sigma(x)$ einen K-Isomorphismus $\mathfrak{D} \to \tilde{\mathfrak{D}}$, denn für alle $\lambda \in K$ und $x \in \mathfrak{D}$ gilt $\varphi_\sigma(\lambda x) = d * \varphi_\sigma(x)$.

Ist nun p eine Primzahl und $pR = \prod_{i=1}^{k} \mathfrak{p}_i^{e_i}$ eine Zerlegung in verschiedene Primideale, so operiert die Galoisgruppe von $K/\mathbb{Q}$ transitiv auf der Menge $\{\mathfrak{p}_i \mid 1 \le i \le k\}$ vgl. [Neu92, Satz 9.1, S. 56]. Also muß $\mathfrak{D}$ gleichmäßig verteilte Invarianten besitzen.

Sei umgekehrt angenommen, $\mathfrak{D}$ erfülle diese Bedingung. Dann sind $\mathfrak{D}$ und $\tilde{\mathfrak{D}}$ an jeder Komplettierung isomorph. Nach dem Satz von Hasse-Brauer-Noether-Albert [Rei03, 32.11, S. 276] sind dann auch $\mathfrak{D}$ und $\tilde{\mathfrak{D}}$ isomorph. Für jedes $\sigma \in \mathrm{Aut}_{\mathbb{Q}}(\mathfrak{D})$ existiert daher ein $\varphi_\sigma \in \mathrm{Aut}_{\mathbb{Q}}(\mathfrak{D})$ mit $\varphi_\sigma|_K = \sigma$. □

Bemerkung 4.2.3 Angenommen, $\mathfrak{D}$ habe gleichmäßig verteilte Invarianten. Für jedes $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ seien $\varphi_\sigma \in \mathrm{Aut}_{\mathbb{Q}}(\mathfrak{D})$ mit $\varphi_\sigma|_K = \sigma$. Bezeichnet $[\mathfrak{M}]$ die Konjugationsklasse einer R-Maximalordnung $\mathfrak{M}$, so liefert $\sigma \times [\mathfrak{M}] \mapsto [\varphi_\sigma(\mathfrak{M})]$ eine Operation von $\mathrm{Gal}(K/\mathbb{Q})$ auf den Konjugationsklassen der R-Maximalordnungen von $\mathfrak{D}$.

Diese Operation ist wohldefiniert, denn sind $\varphi_1, \varphi_2 \in \mathrm{Aut}_{\mathbb{Q}}(\mathfrak{D})$ mit $\varphi_i|_K = \sigma$ für $i = 1, 2$. Dann ist $\varphi_1^{-1} \circ \varphi_2 \in \mathrm{Aut}_K(\mathfrak{D})$, also durch Konjugation gegeben. Damit ist $[\varphi_1(\mathfrak{M})] = [\varphi_2(\mathfrak{M})]$.

Lemma 4.2.4 *Sei $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ und $\varphi \in \mathrm{Aut}_{\mathbb{Q}}(\mathfrak{D})$ mit $\varphi|_K = \sigma$. Eine R-Ordnung Λ ist genau dann zu $\varphi(\Lambda)$ konjugiert, wenn die R-Gitter (Λ, N) und $(\Lambda, \sigma \circ N)$ isometrisch sind.*

Beweis: Die Standardbasisvektoren $1, \mathbf{i}, \mathbf{j}, \mathbf{k}$ erfüllen alle $\varphi(\overline{x}) = \overline{\varphi(x)}$. Also gilt diese Identität für alle $x \in \mathfrak{D}$. Damit gilt auch $\mathrm{tr}_{\mathfrak{D}/K}(\varphi(x)) = \varphi(\mathrm{tr}_{\mathfrak{D}/K}(x)) = \sigma(\mathrm{tr}_{\mathfrak{D}/K}(x))$ für alle $x \in \mathfrak{D}$. Es folgt

$$\mathrm{tr}_{\mathfrak{D}/K}(\varphi(x)\overline{\varphi(y)}) = \mathrm{tr}_{\mathfrak{D}/K}(\varphi(x\overline{y}))) = \sigma(\mathrm{tr}_{\mathfrak{D}/K}(x\overline{y})) \text{ für alle } x, y \in \mathfrak{D}\,.$$

Die Behauptung folgt nun aus Korollar 4.1.6. □

Bemerkung 4.2.5 $\mathfrak{D} = \left(\frac{a,b}{K}\right)$ besitze gleichmäßig verteilte Invarianten.

(a) Sind a, $b \in \mathbb{Q}$, so ist ein $\varphi \in \mathrm{Aut}_{\mathbb{Q}}(\mathfrak{D})$ mit $\varphi|_K = \sigma$ leicht anzugeben. Ein solcher Automorphismus ist z.B. gegeben durch

$$\varphi\colon \mathfrak{D} \to \mathfrak{D},\ \sum_{k=1}^{4} x_k b_k \mapsto \sum_{k=1}^{4} \sigma(x_k) b_k\,.$$

Denn bezeichne $b_i' = \varphi(b_i)$, so gilt $b_i' b_j' = -b_j' b_i'$ für alle $2 \le i \ne j \le 4$. Wegen $a, b \in \mathbb{Q}$ ist $\varphi(b_i^2) = \sigma(b_i^2) = b_i^2 = \varphi(b_i)^2$. Also ist φ ein Automorphismus.

(b) Im Allgemeinen muß man jedoch ein quadratisches Gleichungssystem über K lösen. Man hat dazu die Bilder b_2', b_3' der Elemente b_2, b_3 zu konstruieren. Da $\mathrm{tr}_{\mathfrak{D}/K}(b_i) = 0$ für $i > 1$, kann man $b_2' = x_2b_2 + x_3b_3 + x_4b_4$ und $b_3' = y_2b_2 + y_3b_3 + y_4b_4$ mit $x_i, y_j \in K$ ansetzen. Setzen wir dann $b_1' = 1$ und $b_4' = b_2'b_3'$, so müssen die folgenden Gleichungen gelten, damit $\sum_{k=1}^4 x_kb_k \mapsto \sum_{k=1}^4 \sigma(x_k)b_k'$ einen geeigneten Automorphismus liefert:

$$b_2'b_3' = -b_3'b_2', \sigma(a) = (b_2')^2 = ax_2^2 + bx_3^2 + abx_4^2 \text{ und } \sigma(b) = (b_3')^2 = ay_2^2 + by_3^2 + aby_4^2.$$

Bemerkung 4.2.6 Es sei $\sigma\colon K \hookrightarrow \mathbb{Q}$ und $\varphi_\sigma \in \mathrm{Aut}_{\mathbb{Q}}(\mathfrak{D})$ mit $\varphi_\sigma|_K = \sigma$. Weiter sei $\mathfrak{M}$ eine R-Maximalordnung und $b_1, \ldots, b_m$ eine $\mathbb{Z}$-Basis von $\mathfrak{M}$. Ferner bezeichne $G = \mathrm{tr}_{\mathfrak{D}/\mathbb{Q}}(b_i\bar{b}_j)_{ij}$ die Grammatrix des $\mathbb{Z}$-Gitters $(\mathfrak{M}, N_{\mathbb{Q}})$.

Interessiert man sich für dichte $\mathbb{Z}$-Gitter in $\mathfrak{D}$, so ist das $\mathbb{Z}$-Gitter $(\mathfrak{M}, N_{\mathbb{Q}})$ nicht besonders interessant. Denn aus dem Beweis von Bemerkung 4.1.2 folgt

$$\min\{N_{\mathbb{Q}}(x,x) \mid x \in \mathfrak{M} \setminus \{0\}\} = 2n\,.$$

Es gibt jedoch wesentlich dichtere $\mathbb{Z}$-Gitter in Dimension $4n$.

Man kann aber hoffen, daß $\mathbb{Z}$-Gitter der Form $(\mathfrak{M}x, N_{\mathbb{Q}})$ mit $x \in \mathfrak{D}^*$ dichtere $\mathbb{Z}$-Gitter liefern. Die Grammatrix des $\mathbb{Z}$-Gitters $x\mathfrak{M}$ ist $(\mathrm{tr}_{\mathfrak{D}/\mathbb{Q}}(b_ix\overline{b_jx})) = x\bar{x}G = \mathrm{tr}_{\mathfrak{D}/K}(x)G$. Also wäre ein Ansatz, $\mathbb{Z}$-Gitter mit Grammatrix αG für total positive $\alpha \in K$ zu untersuchen.
Verfolgt man diesen Ansatz für $\mathfrak{M}$ und $\varphi_\sigma(\mathfrak{M})$ so würde man jeweils dieselben $\mathbb{Z}$-Gitter untersuchen, denn es ist

$$(\mathrm{tr}_{\mathfrak{D}/\mathbb{Q}}(\varphi_\sigma(b_i)x\overline{\varphi_\sigma(b_j)x}))_{ij} = \sigma(\mathrm{tr}_{\mathfrak{D}/K}(x))(\mathrm{Tr}_{K/\mathbb{Q}}(\sigma \circ \mathrm{tr}_{\mathfrak{D}/K}(b_i\bar{b}_j)))_{ij} = \sigma(\mathrm{tr}_{\mathfrak{D}/K}(x))G\,.$$

Selbst wenn man ein konkretes φ_σ nicht konstruieren kann, kann es also von Vorteil sein, lediglich die Bahnen der Galoisoperation auf den Konjugationsklassen von R-Maximalordnungen zu bestimmen.

Kapitel 5

Algorithmen

Es sei K ein algebraischer Zahlkörper und $R = \mathbb{Z}_K$ der ganze Abschluß von $\mathbb{Z}$ in K. Weiter sei $\mathfrak{D}$ eine total-definite Quaternionenalgebra mit $n := [K : \mathbb{Q}]$ und $m := 4n = [\mathfrak{D} : \mathbb{Q}]$.

Weiter wollen wir annehmen, daß wir in K bzw. R alle auftretenden Operationen wie das Invertieren und Faktorisieren von gebrochenen R-Idealen usw. durchführen können.

Als Konvention vereinbaren wir, daß Vektoren immer Zeilenvektoren sind. Für eine Matrix M bezeichne $M[i]$ die i-te Zeile von M, so wie dies auch im Computeralgebrasystem Magma (vgl. [CB05]) der Fall ist.

5.1 Arithmetik

Es sei $(1 = x_1, \ldots, x_4)$ eine beliebige K-Basis von $\mathfrak{D}$ und $(1 = r_1, \ldots, r_n)$ eine Ganzheitsbasis von K. Dann bildet $\underline{b} = (b_1, \ldots, b_m)$ mit $b_{4(k-1)+l} = x_k r_l$ eine $\mathbb{Q}$-Basis von $\mathfrak{D}$. Ein Element $x \in \mathfrak{D}$ werden wir entweder als Koeffizientenvektor bezüglich $(x_1, \ldots, x_4)$ oder aber bezüglich $\underline{b}$ darstellen.
Ein R-Gitter I von $\mathfrak{D}$ besitzt zwar eventuell keine R-Basis jedoch stets eine $\mathbb{Z}$-Basis $(y_1, \ldots, y_m)$. Schreiben wir die Koeffizienten der y_i bezüglich $\underline{b}$ untereinander, so erhalten wir eine sogenannte *Basismatrix* von I, welche im Programmlisting meist mit L bezeichnet wird.

Eine andere Möglichkeit ist die *rechtsreguläre Darstellung*: Sei dazu $y_j y_i = \sum_{k=1}^{m} \lambda_{jk}^{(i)} y_k$ mit $\lambda_{jk}^{(i)} \in \mathbb{Q}$. Dann setzen wir $Y_i := (\lambda_{jk}^{(i)})$. Das System $(Y_1, \ldots, Y_m)$ ist dann die rechtsreguläre Darstellung von I und beschreibt die Rechtsmultiplikation der Basis $y_1, \ldots, y_m$. Insbesondere besteht jede rechtsreguläre Darstellung einer R-Ordnung aus Maxtrizen mit Einträgen aus $\mathbb{Z}$, denn jede R-Ordnung ist ein Ring.

Im Folgenden bezeichne $\underline{B} = (B_1, \ldots, B_m)$ die rechtsreguläre Darstellung des von $\underline{b}$ erzeugten $\mathbb{Z}$-Gitters.

Es sei I ein R-Gitter mit Basis $\underline{y}$ und dazugehörender Basismatrix $L = (l_{ij})$. Setzen wir $Y_i = L(\sum_{j=1}^{m} \lambda_{ij} B_j) L^{-1}$ für $1 \leq i \leq m$, so bildet $Y_1, \ldots, Y_m$ die rechtsreguläre Darstellung von I bezüglich $\underline{y}$.

5.1.1 Bezeichnungen

Wir wollen nun für den Rest des Kapitels einige Objekte fixieren. Es sei $(1 = x_1, \ldots, x_4)$ eine K-Basis von $\mathfrak{D}$ und $(1 = r_1, \ldots, r_n)$ eine Ganzheitsbasis von K. Dann seien $b_{4(k-1)l} := x_k r_l$ und es bezeichne $\underline{b} = (b_1, \ldots, b_m)$ die $\mathbb{Q}$-*Standardbasis von* $\mathfrak{D}$. Weiter sei $\underline{B}$ die rechtsreguläre Darstellung von $\underline{b}$.

Es gibt $\lambda_{jk}^{(i)} \in \mathbb{Q}$ mit $b_j \overline{b}_i = \sum_{k=1}^m \lambda_{jk}^{(i)} b_k$. Wir setzen $B_i^o := (\lambda_{jk}^{(i)})$ und $\underline{B}^o = (B_1^o, \ldots, B_m^o)$. $\underline{B^o}$ beschreibt dann die Rechtsmultiplikation der $\overline{b_i}$ auf $\underline{b}$.

Ferner werden wir noch die folgenden symmetrischen rationalen Matrizen benötigen: $tr := (\mathrm{tr}_{\mathfrak{D}/K}(b_i \overline{b}_j))_{ij}$ und $\Psi_k := (\mathrm{tr}_{\mathfrak{D}/\mathbb{Q}}(r_k b_i \overline{b_j})_{ij}$ für $1 \leq k \leq n$.

5.1.2 Elementarithmetik

Es seien $x = \sum_{i=1}^m x_i b_i$ und $y = \sum_{i=1}^m y_i b_i$ zwei Elemente in $\mathfrak{D}$. Weiter bezeichne $\tilde{x} = (x_1, \ldots, x_m) \in \mathbb{Q}^m$.

Um $x \cdot y$ zu bestimmen, bilden wir zunächst $Y := \sum_{i=1}^m (y_i B_i)$. Dann beschreibt Y die Rechtsmultiplikation von y auf $\underline{b}$ und damit ist $\tilde{x}Y$ gerade der Koeffizientenvektor von xy bezüglich $\underline{b}$.

Weiter gilt $\tilde{x} \cdot (tr[1])^{\mathrm{t}} = \mathrm{tr}_{\mathfrak{D}/K}(\sum_{i=1}^m x_i \overline{b}_i) = \mathrm{tr}_{\mathfrak{D}/K}(\overline{x}) = \mathrm{tr}_{\mathfrak{D}/K}(x)$. Damit läßt sich die reduzierte Spur eines Elementes x leicht bestimmen.
Wegen $\frac{1}{2}(\tilde{x} \cdot tr \cdot \tilde{x}^{\mathrm{t}}) = \frac{1}{2} \mathrm{tr}_{\mathfrak{D}/K}(\sum_i \sum_j x_i b_i \overline{x_j b_j}) = \frac{1}{2} \mathrm{tr}_{\mathfrak{D}/K}(x\overline{x}) = \mathrm{nr}_{\mathfrak{D}/K}(x)$ gilt dies auch für die reduzierte Norm von x.

5.1.3 Gitterarithmetik

Es sei I ein R-Gitter in $\mathfrak{D}$ mit $\mathbb{Z}$-Basis $\underline{y}$ und dazugehörender Basismatrix $L = (\lambda_{ij})$. Weiter sei $\underline{B}$ wieder die rechtsreguläre Darstellung der fixierten $\mathbb{Q}$-Basis $\underline{b}$ von $\mathfrak{D}$ und $x = \sum_{i=1}^m x_i b_i$ ein beliebiges Element aus $\mathfrak{D}$.

Wenn man die folgenden Algorithmen implementieren will, so sollte man nicht irgendeine Basismatrix eines R-Gitter berechnen, sondern eine Hermitesche Normalform. Dies verhindert ein allzu starkes Wachstum der Koeffizienten.

Die reduzierte Norm eines normalen R-Gitters
Ist I normal, so wollen wir $\mathrm{nr}_{\mathfrak{D}/K}(I)$ berechnen. Im Kommentar zu Definition 2.8.7 haben wir bereits gesehen, daß $\mathrm{nr}_{\mathfrak{D}/K}(I)$ das von $\{\mathrm{nr}_{\mathfrak{D}/K}(x) \mid x \in I\}$ erzeugte R-Ideal ist. Für $x, y \in \mathfrak{D}$ gilt ferner

$$\mathrm{nr}_{\mathfrak{D}/K}(x+y) = (x+y) \cdot (\overline{x+y}) = \mathrm{nr}_{\mathfrak{D}/K}(x) + \mathrm{nr}_{\mathfrak{D}/K}(y) + \mathrm{tr}_{\mathfrak{D}/K}(x\overline{y}) \,.$$

Also wird $\mathrm{nr}_{\mathfrak{D}/K}(I)$ bereits erzeugt von

$$\{\mathrm{nr}_{\mathfrak{D}/K}(y_i) \mid 1 \leq i \leq m\} \cup \{\mathrm{tr}_{\mathfrak{D}/K}(y_i \overline{y}_j) \mid 1 \leq i < j \leq m\} \,.$$

Wie wir schon gesehen haben, gilt $LtrL^{\mathrm{t}} = (\mathrm{tr}_{\mathfrak{D}/K}(y_i \overline{y}_j))_{ij}$. Dabei ist der i-te Diagonaleintrag gerade $\mathrm{tr}_{\mathfrak{D}/K}(y_i \overline{y}_i) = 2\,\mathrm{nr}_{\mathfrak{D}/K}(y_i)$. Somit läßt sich $\mathrm{nr}_{\mathfrak{D}/K}(I)$ leicht bestimmen.

Die Produkte xI und Ix
Wir gehen wie beim Multiplizieren zweier Elemente aus $\mathfrak{D}$ vor, denn xI ist ja gerade das von $xy_1, \ldots, xy_m$ erzeugte $\mathbb{Z}$-Gitter. Es sei also $Y_i := \sum_{j=1}^{m} \lambda_{ij} B_j$. Schreiben wir nun die Vektoren $xY_1, \ldots, xY_m$ untereinander, so erhalten wir eine Basismatrix von xI bezüglich $\underline{b}$.

Analog ist $L(\sum_{i=1}^{m} x_i B_i)$ eine Basismatrix von Ix in Bezug auf $\underline{b}$.

Das Produkt zweier R-Gitter
Es sei J ein weiteres R-Gitter mit Basismatrix $L' = (\lambda'_{ij})$. Wir wollen $I \cdot J$ berechnen. Hat J die Basis $\underline{y'}$, so ist IJ das von $\{y_i y'_j \mid 1 \leq i, j \leq m\}$ erzeugte $\mathbb{Z}$-Gitter. Wir gehen daher wie beim Bilden von xI vor: Es sei $Y_i := \sum_{j=1}^{m} \lambda'_{ij} B_j$. Schreiben wir nun $LY_1, \ldots, LY_m$ untereinander, so enthält diese Matrix die Koeffizienten aller Produkte $y_i y'_j$. Bringen wir die Matrix auf Hermitesche Normalform, so haben wir eine Basis von IJ gefunden.

Es sei bemerkt, daß der Algorithmus auch $I\mathfrak{a}$ für jedes gebrochene R-Ideal $\mathfrak{a}$ von K bestimmen kann. Dazu wählt man als L' gerade die Basismatrix von $\mathfrak{a}$ bezüglich der zuvor fixierten Ganzheitsbasis $(r_1, \ldots, r_n)$ von K. Denn für $i = 1, \ldots, n$ beschreibt B_i gerade die Rechtsmultiplikation von r_i auf $\underline{b}$. Man bekommt dann natürlich nur n Matrizen $Y_1, \ldots, Y_n$ anstatt m wie oben.

Dualisieren eines R-Gitters
Um $I^{\#}$ bezüglich der reduzierten Spurbilinearform $\tau_{\mathfrak{D}/K} \colon (x, y) \mapsto \mathrm{tr}_{\mathfrak{D}/K}(xy)$ zu finden, werden wir I zuerst bezüglich $\tau_{\mathfrak{D}/\mathbb{Q}} \colon (x, y) \mapsto \mathrm{tr}_{\mathfrak{D}/\mathbb{Q}}(xy)$ dualisieren und dieses $\mathbb{Z}$-Gitter dann gemäß Lemma 2.9.6 mit der Diskriminante $d(K/\mathbb{Q})$ des Zahlkörpers K multiplizieren um $I^{\#}$ zu erhalten. Dazu sei $T := (\mathrm{tr}_{\mathfrak{D}/\mathbb{Q}}(b_i b_j))_{ij}$. Die Matrix T hängt nur von der Standardbasis ab und muß daher auch nur einmal berechnet werden. Da $\underline{y}$ eine $\mathbb{Q}$-Basis von $\mathfrak{D}$ ist und $\tau_{\mathfrak{D}/\mathbb{Q}}$ nach Definition 2.2.8 nicht ausgeartet ist, TL^{t} invertierbar. Wegen $(TL^{\mathrm{t}})^{-1} TL^{\mathrm{t}} = I_m$ bilden die Zeilen von $(TL^{\mathrm{t}})^{-1}$ eine Basis des zu I bezüglich $\tau_{\mathfrak{D}/\mathbb{Q}}$ dualen Gitters. Da der vorherige Algorithmus auch das Produkt eines vollständigen $\mathbb{Z}$-Gitters mit einem gebrochenen R-Ideal von K bestimmen kann, können wir nun $I^{\#}$ angeben.

Die Rechtsordnung eines R-Gitters
Wir wollen nun $\mathcal{O}_r(I)$ bestimmen. Dazu bezeichne $\underline{Y}$ die rechtsreguläre Darstellung von $\underline{y}$. Für $(v_1, \ldots, v_m) \in \mathbb{Q}^m$ gilt dann:

$$\sum_{i=1}^{m} v_i y_i \in \mathcal{O}_r(I) \iff \sum_{i=1}^{m} v_i v_j y_i \in I \text{ für alle } j \iff \sum_{i=1}^{m} v_i Y_i[j] \in \mathbb{Z}^{1\times m} \text{ für alle } j$$
$$\iff \sum_{i=1}^{m} v_i Y_i \in \mathbb{Z}^{m\times m} .$$

Wir schreiben daher die Zeilen der Matrizen Y_i nebeneinander und erhalten so m Vektoren der Länge m^2. Diese fassen wir dann zu einer $m \times m^2$-Matrix X über $\mathbb{Q}$ zusammen. Nach dem Elementarteilersatz existieren $P \in \mathrm{GL}_m(\mathbb{Z})$ und $Q \in \mathrm{GL}_{m^2}(\mathbb{Z})$

derart, daß $S := PXQ$ Diagonalgestalt besitzt. Für $1 \leq i \leq m$ teilen wir nun die i-te Zeile von P durch $S[i,i]$. Die Zeilen von P spannen dann über $\mathbb{Z}$ gerade die Menge der $v \in \mathbb{Q}^m$ auf, für die $vX \in \mathbb{Z}^{1\times m^2}$ liegt. Das heißt, P ist eine Basismatrix von $\mathcal{O}_r(I)$ bezüglich $\underline{y}$ und damit ist PL eine Darstellung von $\mathcal{O}_r(I)$ bezüglich der Standardbasis $\underline{b}$.

Algorithmus 5.1.1 : Bestimmung der Rechtsordnung eines R-Gitters.

Eingabe : Basismatrix L eines R-Gitters I.
Ausgabe : Eine Basismatrix von $\mathcal{O}_r(I)$.

$\underline{Y} \leftarrow$ rechtsreguläre Darstellung von I;
für $i := 1$ **bis** m **tue** $X[i] \leftarrow Y_i$ aufgefasst als Element von $\mathbb{Q}^{1\times m^2}$;
Finde $P \in \mathrm{GL}_m(\mathbb{Z})$ und $Q \in \mathrm{GL}_{m^2}(\mathbb{Z})$ mit $S := PXQ$ Diagonalgestalt;
für $i := 1$ **bis** m **tue** $P[i] \leftarrow P[i]/S[i,i]$;
zurück PL;

Die Linksordnung eines R-Gitters
Analog zum vorherigen Algorithmus soll nun $\mathcal{O}_l(I)$ berechnet werden.
Sei dazu $Z_i := L(\sum_{j=1}^m (\lambda_{ij} B_j^{\mathrm{o}})L^{-1}$. Ist $Z_i = (z_{jk}^{(i)})_{jk}$, so gilt $y_j\overline{y}_i = \sum_{k=1}^m z_{jk}^{(i)} y_k$ bzw. nach Konjugation $y_i\overline{y}_j = \sum_{k=1}^m z_{jk}^{(i)}\overline{y}_k$. Damit folgt

$$\begin{aligned}\sum_{i=1}^m v_i y_i \in \mathcal{O}_l(I) &\iff \sum_{i=1}^m v_i y_i \in \mathcal{O}_r(\overline{I}) &&\iff \sum_{i=1}^m v_i y_i \overline{y}_j \in \overline{I} \text{ für alle } j\\ &\iff \sum_{i=1}^m v_i Z_i[j] \in \mathbb{Z}^{1\times m} \text{ für alle } j &&\iff \sum_{i=1}^m v_i Z_i \in \mathbb{Z}^{m\times m}\,.\end{aligned}$$

Daher können wir nun den vorherigen Algorithmus mit $(Z_1, \ldots, Z_m)$ anstelle von $\underline{Y}$ verwenden um $\mathcal{O}_l(I)$ zu bestimmen.

Invertieren eines R-Gitters
Beim Invertieren von I haben wir mehrere Möglichkeiten:

(a) Ist I normal, so gilt $I^{-1} = (\mathrm{nr}_{\mathfrak{D}/K}(I))^{-1} \cdot \overline{I}$.

(b) Es ist stets $I^{-1} = (I \cdot \mathcal{O}_r(I)^{\#})^{\#} = (\mathcal{O}_l(I)^{\#} \cdot I)^{\#}$.

(c) Wir gehen wie beim Bestimmen der Links- bzw. Rechtsordnung vor:
Sei dazu $\underline{y'} = (y'_1, \ldots, y'_m)$ eine $\mathbb{Z}$-Basis von $\mathcal{O}_l(I)$ und L' die dazugehörige Basismatrix. Wir setzen $Z_i := L(\sum_{j=1}^m \lambda_{ij} B_j)L'^{-1}$. Ist dann $Z_i = (z_{jk}^{(i)})_{jk}$, so gilt $y_i y_j = \sum_{k=1}^m z_{jk}^{(i)} y'_k$. Es folgt

$$\begin{aligned}\sum_{i=1}^m v_i y_i \in I^{-1} &\iff \sum_{i=1}^m v_i y_j y_i \in \mathcal{O}_l(I) &&\iff \sum_{i=1}^m v_i Z_i[j] \in \mathbb{Z}^{1\times m} \text{ für alle } j\\ &\iff \sum_{i=1}^m v_i Z_i \in \mathbb{Z}^{m\times m}\,.\end{aligned}$$

Damit können wir den Algorithmus zur Bestimmung der Rechtsordnung auf $(Z_1, \ldots, Z_m)$ anwenden und erhalten so eine Basis von I^{-1}. Alternativ kann man natürlich auch $\mathcal{O}_r(I)$ verwenden, man muß lediglich die Matrizen Z_i derart anpassen, daß $y_j y_i = \sum_{k=1}^{m} z_{jk}^{(i)} y'_k$ für eine $\mathbb{Z}$-Basis $(y'_1, \ldots, y'_m)$ von $\mathcal{O}_r(I)$ gilt.

5.2 Konstruktion einer R-Maximalordnung

Ergänzen eines R-Gitters zu einer Ordnung.
In Satz 2.5.7 haben wir bereits gezeigt, daß ein volles R bzw. $\mathbb{Z}$-Gitter I genau dann eine R-Ordnung ist, wenn alle Elemente in I ganz über R sind, I ein Ring ist und $R \subseteq I$ gilt. Angenommen wir haben nun ein volles $\mathbb{Z}$-Gitter I mit $R \subseteq I$ und alle Elemente aus I seien ganz über R (d.h. $\mathrm{tr}_{\mathfrak{D}/K}(I) \subseteq R$ und $\mathrm{nr}_{\mathfrak{D}/K}(I) \subseteq R$). Um $I_0 := I$ zu einer R-Ordnung zu vervollständigen, bilden wir nun immer weiter $I_{i+1} := I_i + I_i^2$. Gibt es nun ein $x \in I_{i+1}$, welches nicht mehr ganz über R ist, so liegt I in keiner R-Ordnung. Gilt $I_i = I_{i+1}$, so ist I_i ein Ring mit $R \subset I_i$, der ganz ist über R, also eine R-Ordnung. Um zu zeigen, daß der Algorithmus terminiert, unterscheiden wir zwei Fälle. Ist I in einer R-Ordnung Λ enthalten, dann kann es keine nicht abbrechende echt aufsteigende Kette von R-Gittern (I_i) mit $I \subset I_i$ und $I_i \subset \Lambda$ geben, da Λ noethersch ist. Also terminiert der Algorithmus. Ist I aber in keiner R-Ordnung enthalten und angenommen, der Algorithmus terminiert nicht, so gibt es eine nicht abbrechende Kette $I = I_0 \subsetneq I_1 \subsetneq I_2 \subsetneq \ldots$. Dann ist $\bigcup_{i=0}^{\infty} I_i$ eine R-Ordnung welche I umfaßt. Was nicht sein kann.

Wir erhalten also folgenden Algorithmus:

Algorithmus 5.2.1 : Ergänzen eines R-Gitter zu einer Ordnung

Eingabe : Ein R-Gitter I mit $R \subset I$.
Ausgabe : Eine minimale R-Ordnung Λ mit $I \subseteq \Lambda$, falls eine solche existiert. Andernfalls **false**.
wiederhole
  $(b_1, \ldots, b_m) \leftarrow$ eine $\mathbb{Z}$-Basis von I;
  wenn *ein* b_i *nicht ganz* **dann zurück false**;
  $I' \leftarrow I$;
  $I \leftarrow$ das von $\{b_1, \ldots, b_m\} \cup \{b_i b_j \mid 1 \leq i, j \leq m\}$ erzeugte $\mathbb{Z}$-Gitter;
bis $I = I'$;
zurück I;

Konstruktion einer R-Maximalordnung
Wir starten mit einer beliebigen R-Ordnung Λ. Zum Beispiel der Linksordnung des von einer $\mathbb{Q}$-Basis von $\mathfrak{D}$ erzeugten $\mathbb{Z}$-Gitters.
Ist Λ in einer anderen R-Ordnung Λ' enthalten, so zeigt der Beweis von Satz 2.9.3 $d(\Lambda/\mathbb{Z}) = [\Lambda' : \Lambda]^2 \cdot d(\Lambda'/\mathbb{Z})$. Für eine Primzahl $p \in \mathbb{N}$ mit $p \mid [\Lambda' : \Lambda]$ gilt daher

$$\Lambda_p \subsetneq \frac{1}{p}\Lambda_p \cap \Lambda'_p \subsetneq \Lambda_p^{\#} .$$

Wegen $\Lambda \subseteq \Lambda'$ ist $\Lambda \subseteq \mathcal{O}_r(\frac{1}{p}\Lambda \cap \Lambda')$. Also existiert ein R-Gitter I in $\mathfrak{D}$ mit $\Lambda \subseteq \mathcal{O}_r(I)$ und

$$\Lambda \subsetneq I \subseteq \frac{1}{p}\Lambda \cap \Lambda^{\#} \subseteq \frac{1}{p}\Lambda\,.$$

Dieses R-Gitter I läßt sich nun mit Algorithmus 5.2 zu einer R-Ordnung Λ'' vervollständigen, die I enthält. Nun wiederholen wir diese Konstruktion, bis für keinen Primteiler p von $d(\Lambda/\mathbb{Z})$ ein solches R-Gitter I mehr existiert. Dann haben wir eine R-Maximalordnung von $\mathfrak{D}$ gefunden.

Um alle Kandidaten für I zu finden, muß man die minimalen Λ-Rechtsmoduln von $\Lambda/p\Lambda$ oder auch $(\Lambda \cap p\Lambda^{\#})/p\Lambda$ bestimmen.
Sei dazu $\underline{Y} = (Y_1, \ldots, Y_m)$ eine rechtsreguläre Darstellung von Λ. Wir fassen dann die $Y_i \in \mathbb{Z}^{m\times m}$ als Elemente von $\mathbb{F}_p^{m\times m}$ auf. Bezeichne nun $\underline{y}$ eine $\mathbb{Z}$-Basis von Λ, und $x = \sum_i v_i y_i \in \Lambda$, so ist $v := (v_1, \ldots, v_m) \in \mathbb{Z}^m$ und damit $vY_i \in \mathbb{Z}^m$ für alle i. Also sind die Teilmoduln der von $(Y_1, \ldots, Y_m)$ erzeugten Teilalgebra von $\mathbb{F}_p^{m\times m}$ gerade die Λ-Rechtsmoduln von $\Lambda/p\Lambda$ und diese wiederum korrespondieren zu den Λ-Rechtsmoduln zwischen Λ und $\frac{1}{p}\Lambda$.
Ein Algorithmus zum Finden aller (minimalen) Teilmoduln einer Matrixalgebra über einem endlichen Körper ist in [HR94] beschrieben und in MAGMA implementiert als `MinimalSubmodules`.

Alternativ kann man auch die Rechtsmultiplikation von Λ auf $\frac{1}{p}\Lambda \cap \Lambda^{\#}/\Lambda$ als Matrixalgebra über $\mathbb{F}_p$ darstellen und erhält so die minimalen Λ-Teilmoduln I zwischen Λ und $\frac{1}{p}\Lambda \cap \Lambda^{\#}$. Dies hat den Vorteil, daß man meist in einer kleineren Matrixalgebra arbeitet.

Da $d(\Lambda/\mathbb{Z})$ nach Satz 2.9.3 in jedem Schritt verkleinert wird und es nur endlich viele Teilmoduln von $\Lambda/p\Lambda$ gibt, terminiert der folgende Algorithmus:

Algorithmus 5.2.2 : Konstruktion einer R-Maximalordnung

Ausgabe : Eine R-Maximalordnung Λ.

```
1  Λ ← Linksordnung des von einer Q-Basis von 𝔇 erzeugten R-Gitters über R;
2  d ← d(Λ/ℤ);
3  für alle Primzahlen p mit p² | d tue
4  |   Bestimme die minimalen Λ-Rechtsmoduln von Λ/pΛ;
5  |   für alle minimalen Teilmoduln M von Λ/pΛ tue
6  |   |   I ← zu M korrespondierende R-Gitter zwischen Λ und (1/p)Λ;
7  |   |   wenn I in einer R-Ordnung Λ' liegt dann
8  |   |   |   Λ ← Λ';
9  |   |   |   gehe zu 4;
10 |   |   Ende
11 |   Ende
12 Ende
13 zurück Λ;
```

5.3 Bestimmung der Invarianten der Quaternionenalgebra

Ist eine R-Maximalordnung $\mathfrak{M}$ von $\mathfrak{D}$ bestimmt, so können wir nun die Invarianten von $\mathfrak{D}$ bestimmen. Die Diskriminante ist bekanntlich $d(\mathfrak{D}/R) = (\mathrm{nr}_{\mathfrak{D}/K}(\mathfrak{M}^{\#}))^{-2}$. Dies läßt sich wie wir schon gesehen haben leicht bestimmen. Damit kann man die Minkowskischranke berechnen.
Sind $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ die in $\mathfrak{D}$ verzweigten Primideale von R, so gilt $\mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_s = \mathrm{nr}_{\mathfrak{D}/K}(\mathfrak{M}^{\#})^{-1}$. Damit lassen sich die verzweigten Primideale sofort angeben. Hat man diese bestimmt, so kann man die rechte Seite der Eichlerschen Maßformel auswerten, sie hängt jetzt nur noch vom Grundkörper K ab.

5.4 Finden aller Klassen von R-Maximalordnungen

Es sei $\mathfrak{M}$ eine R-Maximalordnung von $\mathfrak{D}$ wie in Abschnitt 5.2 bestimmt. Wir wollen nun zeigen, mit welchen Mitteln man alle Konjugationsklassen von R-Maximalordnungen finden kann.

Finden der maximal ganzen $\mathfrak{M}$-Rechtsideale
Es sei $\mathfrak{p}$ ein Primideal von R. Wir wollen nun alle maximal ganzen $\mathfrak{M}$-Rechtsideale finden, die $\mathfrak{p}\mathfrak{M}$ enthalten.
Dazu sei $\underline{y}$ eine $\mathbb{Z}$-Basis von $\mathfrak{M}$ und p die Primzahl über der $\mathfrak{p}$ liegt. Nach dem Elementarteilersatz können wir annehmen, daß es ein $l \in \mathbb{N}$ gibt so, daß $(py_1, \ldots py_l, y_{l+1}, \ldots, y_m)$ eine $\mathbb{Z}$-Basis von $\mathfrak{p}\mathfrak{M}$ ist. Die rechtsreguläre Darstellung $\underline{Y}$ bezüglich $\underline{y}$ beschreibt nun auch die Rechtsmultiplikation von $\underline{y}$ auf $\mathfrak{M}/\mathfrak{p}\mathfrak{M}$. Fassen wir dies als eine Maxtrixalgebra von Dimension l über $\mathbb{F}_p$ auf, so entsprechen die maximalen Teilmoduln davon gerade den gesuchten maximal ganzen $\mathfrak{M}$-Rechtsidealen.

Ist $\mathfrak{p}$ in $\mathfrak{D}$ verzweigt, so gibt es nur ein maximal ganzes $\hat{\mathfrak{M}}_{\mathfrak{p}}$-Rechtsideal über $\mathfrak{p}\hat{\mathfrak{M}}_{\mathfrak{p}}$, nämlich $\mathrm{rad}(\hat{\mathfrak{M}}_{\mathfrak{p}})$. Nach Satz 2.5.36 existiert daher auch nur ein $\mathfrak{M}$-Rechtsideal über $\mathfrak{p}\mathfrak{M}$ und dieses ist zweiseitig.
Ist $\mathfrak{p}$ nicht verzweigt und $q := \mathrm{Nr}_{K/\mathbb{Q}}(\mathfrak{p}) = |R/\mathfrak{p}|$, so ist $\mathfrak{M}/\mathfrak{p}\mathfrak{M} \cong \mathbb{F}_q^{2\times 2}$ nach Korollar 2.7.8. Nun sind die Kategorie der $\mathbb{F}_q^{2\times 2}$-Rechtsteilmoduln von $\mathbb{F}_q^{2\times 2}$ und die Kategorie der $\mathbb{F}_q$-Vektorräume von $\mathbb{F}_q^2$ äquivalent (siehe [Row91, Theorem 1.1.17, S. 30 und Example 4.1.10, S. 359]). Also gibt es in diesem Fall genau $\frac{q^2-1}{q-1} = q+1$ der gesuchten maximal ganzen $\mathfrak{M}$-Rechtsideale.

Ist nun p eine Primzahl und $pR = \mathfrak{p}_1^{e_1} \cdot \ldots \cdot \mathfrak{p}_k^{e_k}$ mit paarweise verschiedenen Primidealen $\mathfrak{p}_i$ von R. Dann gilt $R/pR \cong \bigoplus_{i=1}^{s} R/\mathfrak{p}_i^{e_i}$. Weiter seien $\epsilon_1, \ldots, \epsilon_s$ die dazugehörenden Idempotente. Da $\mathfrak{M}/p\mathfrak{M}$ ein R/pR-Modul ist auch $\mathfrak{M}/p\mathfrak{M} \cong \bigoplus_{i=1}^{s} \mathfrak{M}/\mathfrak{p}_i^{e_i}\mathfrak{M}$. Jeder $\mathfrak{M}$-Rechtsteilmodul T von $\mathfrak{M}/p\mathfrak{M}$ ist daher isomorph zu $\bigoplus_{i=1}^{s} \epsilon_i T$. Insbesondere sind die maximal ganzen $\mathfrak{M}$-Rechtsideale zwischen $p\mathfrak{M}$ und $\mathfrak{M}$ gerade die maximalen ganzen $\mathfrak{M}$-Rechtsideale zwischen den einzelnen $\mathfrak{p}_i\mathfrak{M}$ und $\mathfrak{M}$.

Testen zweier R-Ordnungen auf Konjugation
Es seien Λ und Λ' zwei R-Ordnungen mit Basen $\underline{y}$ und $\underline{y'}$ sowie L bzw. L' die dazugehörenden Basismatrizen. Weiter seien $F_k := L\Psi_k\overline{L}^{\mathrm{t}}$ und $F'_k := L'\Psi_k\overline{L'}^{\mathrm{t}}$.

Satz 5.4.1 *Die beiden R-Ordnungen Λ und Λ' sind genau dann konjugiert, wenn es eine Matrix $T \in \mathrm{GL}_m(\mathbb{Z})$ gibt mit $F_k = TF'_kT^{\mathrm{t}}$ für alle k.*
Ist r_2 ein primitives Element von $K/\mathbb{Q}$, so genügt es, wenn T lediglich $F_k = TF'_kT^{\mathrm{t}}$ für $k = 1, 2$ erfüllt.

Beweis: Nach Korollar 4.1.6 sind Λ und Λ' genau dann konjugiert, wenn die beiden R-Gitter $(\Lambda, N_{\mathbb{Q}})$ und $(\Lambda, N_{\mathbb{Q}})$ isometrisch sind. Eine solche Isometrie erfüllt dann $\mathrm{Tr}_{K/\mathbb{Q}}(rN(x,y)) = \mathrm{Tr}_{K/\mathbb{Q}}(rN(\varphi(x),\varphi(y)))$ für alle $r \in R$ und alle $x, y \in \Lambda$. Die darstellende Matrix T von φ bezüglich $\underline{b}$ genügt daher der geforderten Bedingung.

Sei nun umgekehrt solch eine Matrix T gegeben. Für alle $1 \le k \le n$ gibt es dann $a_{ij}^{(k)} \in \mathbb{Q}$ mit $r_k y_i = \sum_{j=1}^m a_{ij}^{(k)} y_j$ und wir setzen $A_k := (a_{ij}^{(k)})$. Analog definieren wir A'_k. Wegen $r_1 = 1$ gilt $F_k = A_kF_1$ bzw. $F'_k = A'_kF'_1$, wie man leicht nachrechnet. Es folgt

$$A_kTF'_1T^{\mathrm{t}} = A_kF_1 = F_k = TF'_kT^{\mathrm{t}} = TA'_kF'_1T^{\mathrm{t}} .$$

Also gilt $A_k = TA'_kT^{-1}$ für alle k und somit entspricht T einem Element in $\mathrm{Aut}_K(\mathfrak{D})$. Sei $\varphi\colon \Lambda \to \Lambda'$ die durch T beschriebene R-lineare Abbildung. Dann gilt nach Voraussetzung $\mathrm{Tr}_{K/\mathbb{Q}}(r_kN(x,\overline{y})) = \mathrm{Tr}_{K/\mathbb{Q}}(r_kN(\varphi(x),\varphi(y)))$ für alle $x, y \in \Lambda$ und alle $1 \le k \le n$. Da $\mathrm{Tr}_{K/\mathbb{Q}}$ nicht ausgeartet ist, folgt $N(x,\overline{y}) = N(\varphi(x),\varphi(y))$ für alle $x, y \in \Lambda$. Also ist $\varphi\colon (\Lambda, N) \to (\Lambda', N)$ eine Isometrie von R-Gittern.

Sei nun $K = \mathbb{Q}(r_2)$. Dann können wir annehmen, es sei $r_k = r_2^{k-1}$ für $1 \le k \le n$. Mit den obigen Bezeichnungen gilt dann $A_k = A_2^{k-1}$ für alle $1 \le k \le n$. Weiter ist $F_k = A_kF_1 = A_2^{k-1}F_1$ und $F'_k = A_2^{k-1}F'_1$ für alle $1 \le k \le n$. Wir können daher die obige Argumentation auch anwenden, wenn T lediglich $F_k = TF'_kT^{\mathrm{t}}$ für $k = 1, 2$ erfüllt. □

Ein Algorithmus zum Finden einer solchen Matrix T ist in [PS97] beschrieben und steht in Magma unter dem Namen `IsIsometric` zur Verfügung.

Feststellen, ob alle Typen von R-Maximalordnungen gefunden sind
Es sei Λ eine R-Ordnung mit Basis $\underline{y}$ und dazugehörender Basismatrix L. Ferner sei $F_k := L\Psi_k\overline{L}^{\mathrm{t}}$. Aus Satz 5.4.1 mit $\overline{\Lambda} = \Lambda'$ folgt, daß $\varphi \in \mathrm{Aut}_{\mathbb{Z}}(\Lambda)$ genau dann ein Element von $\mathrm{Aut}_R(\Lambda, N)$ ist, wenn darstellende Matrix T von φ bezüglich $\underline{y}$ für alle $1 \le k \le n$ die Identität $TF_kT^{\mathrm{t}} = F_k$ erfüllt. Ist $K = \mathbb{Q}(r_2)$, so genügt es die Bedingung nur für $k = 1, 2$ zu fordern.

Mit dem in [PS97] beschriebenen und auch in Magma als `AutomorphismGroup` implementierten Algorithmus können wir daher $|\mathrm{Aut}_R(\Lambda, N)|$ bestimmen.
Mit Satz 4.1.9 ist es uns nun auch möglich, die Terme $\omega_i^{-1}H_i$ in der Eichlerschen Maßformel auszuwerten. Damit läßt sich letztlich überprüfen, ob wir schon alle Klassen von R-Maximalordnungen bestimmt haben, denn die rechte Seite der Maßformel haben wir bereits in Abschnitt 5.3 ausgewertet.

Finden aller Konjugationsklassen von R-Maximalordnungen
Wir wissen bereits, daß jede R-Maximalordnung die Linksordnung eines $\mathfrak{M}$-Rechtsideals I ist. Ohne Einschränkung können wir I als ganz voraussetzen. Bei der Bestimmung der Minkowskischranke wurde außerdem gezeigt, daß man nur $\mathfrak{M}$-Rechtsideale bis zu einer gewissen Norm untersuchen muß.

Nach Satz 2.5.33 besitzt jedes ganze $\mathfrak{M}$-Rechtsideal I eine Darstellung $I = I_1 \cdot \ldots \cdot I_k$ als ein echtes Produkt maximal ganzer R-Gitter. Eine Strategie zum Finden aller Konjugationsklassen von R-Maximalordnungen wäre daher die folgende:

Wir setzen uns eine obere Schranke. Für jede Primzahl p unterhalb dieser Schranke bestimmen wir dann die Linksordnungen aller maximal ganzen $\mathfrak{M}$-Rechtsideale. Auf diese Weise bekommen wir neue Konjugationsklassen von R-Maximalordnungen. Für einen Vertreter jeder dieser Klassen wiederholen wir dann diese Konstruktion um wiederum neue Konjugationsklassen zu bestimmen.

Die Frage ist nun, welche Primzahlen man zuerst untersuchen sollte, um möglichst schnell alle Konjugationsklassen von R-Maximalordnungen zu finden. Zuerst einmal sollte man versuchen, nur Primzahlen p zu testen, die wenige maximal ganze R-Gitter liefern. Wir haben bereits gezeigt, daß wenn $pR = \prod_{i=1}^{k} \mathfrak{p}_i^{e_i}$ eine Zerlegung in Primideale von R ist, so gibt es über $p\mathfrak{M}$ genau $k + \sum_{i=1}^{k} \mathrm{Nr}_{\mathfrak{D}/K}(\mathfrak{p}_i)$ maximal ganze $\mathfrak{M}$-Rechtsideale.

Satz 2.10.5 liefert einen weiteren Anhaltspunkt. Die Klasse der stabil äquivalenten $\mathfrak{M}$-Rechtsideale ist isomorph zur Strahlklassengruppe von K modulo der unendlichen Stellen von K. Also müssen die Klassen der reduzierten Normen der zu betrachtenden maximal ganzen R-Gitter alle Elemente der Strahlklassengruppe durchlaufen.
Man sollte also so vorgehen, daß man zuerst Primzahlen p testet, die wenige $\mathfrak{M}$-Rechtsideale liefern und andererseits sollen die Klassen der Primideale in R über diesen Primzahlen die Strahlklassengruppe von K erzeugen.

Ist M ein maximal ganzes $\mathfrak{M}$-Rechtsideal, so ist $\mathfrak{p} = M \cap R$ bekanntlich ein Primideal von R. Nach Satz 2.8.8 gilt $\mathrm{Nr}_{\mathfrak{D}/\mathbb{Q}}(M) = \mathrm{Nr}_{K/\mathbb{Q}}(\mathrm{Nr}_{\mathfrak{D}/K}(M)) = \mathrm{Nr}_{K/\mathbb{Q}}(\mathfrak{p}^2)$. Daher haben wir eine Primzahl p mit der Primidealfaktorisierung $pR = \mathfrak{p}_1^{e_1} \cdot \ldots \cdot \mathfrak{p}_k^{e_k}$ nur dann zu testen, wenn $\min\{\mathrm{Nr}_{K\mathbb{Q}}(\mathfrak{p}_i)^2 \; 1 \leq i \leq k\}$ kleiner oder gleich der Minkowskischranke ist.

Dies liefert folgenden Algorithmus.

Algorithmus 5.4.1 : Finden aller Klassen von R-Maximalordnungen

Eingabe : Eine R-Maximalordnung $\mathfrak{M}_1$ von $\mathfrak{D}$ und eine Menge $\mathcal{P}$ von Primidealen von R.

Ausgabe : Vertreter $\mathfrak{M}_1, \ldots, \mathfrak{M}_k$ der Konjugationsklassen von R-Maximalordnungen mit der Eigenschaft, daß $\mathfrak{M}_i$ die Linksordnung eines maximal ganzen $\mathfrak{M}_k$-Rechtsideals M mit $k < i$ und $M \cap R \in \mathcal{P}$ ist.

$V \leftarrow \{\mathfrak{M}_1\}$;
$Maß \leftarrow 2^{1-n}|\zeta_K(-1)|h_K \prod_i (\mathrm{Nr}_{\mathfrak{D}/K}(\mathfrak{p}_i) - 1)$ gemäß Satz 4.1.1;
$Maß\_Gefunden \leftarrow \omega_1^{-1} H_1$;
wiederhole
  $\mathfrak{M} \leftarrow$ eine noch nicht betrachtete R-Maximalordnung aus V;
  für alle $\mathfrak{p} \in \mathcal{P}$ **tue**
    Bestimme die maximalen Teilmoduln von $\mathfrak{M}/\mathfrak{p}\mathfrak{M}$;
    für alle *maximal ganzen $\mathfrak{M}$-Rechtsideale M mit $\mathfrak{p}\mathfrak{M} \subset M$* **tue**
      $\mathfrak{M}' \leftarrow \mathcal{O}_l(M)$;
      wenn $\mathfrak{M}'$ *zu keiner der R-Ordnungen in V konjugiert* **dann**
        $V \leftarrow V \cup \{\mathfrak{M}'\}$;
        $Maß\_Gefunden \leftarrow Maß\_Gefunden + w_i^{-1} H_i$ wie in Satz 4.1.1;
        wenn $Maß = Maß\_Gefunden$ **dann zurück** V;
      Ende
    Ende
  Ende
bis *alle R-Maximalordnungen aus V durchsucht*;
zurück V;

Bemerkung: Ist $K/\mathbb{Q}$ galoisch und besitzt $\mathfrak{D}$ gleichmäßig verteilte Invarianten (vgl. Abschnitt 4.2), so kann man mittels des obigen Algorithmus auch ein Vertretersystem der Bahnen der Galoisoperation auf den Konjugationsklassen von R-Maximalordnungen bestimmen.

Ist $\mathfrak{D} = \left(\frac{a,b}{K}\right)$ mit $a, b \in \mathbb{Q}$ so kann man aus einer solchen Galoisbahn wieder ein Vertretersystem aller Klassen von R-Maximalordnungen in dieser Bahn wie folgt gewinnen:
Ist $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ und $\mathfrak{M}$ eine R-Maximalordnung mit Basismatrix L. Sei dann $(r_1, \ldots, r_n)$ die zuvor fixierte $\mathbb{Q}$-Basis von K. Es gibt $\lambda_{ij} \in \mathbb{Q}$ mit $\sigma(r_i) = \sum_{j=1}^{n} \lambda_{ij} r_j$. Setzen wir die Matrix (λ_{ij}) vier mal diagonal untereinander, so erhalten wir eine $m \times m$-Matrix L_σ. Bezeichnen wir die Klasse von R-Maximalordnungen von $\mathfrak{M}$ mit $[\mathfrak{M}]$, so ist LL_σ nach Bemerkung 4.2.5 ein Vertreter von $\sigma([\mathfrak{M}])$.

Im Allgemeinen wird dies nicht gelingen, aber wenn man z.B. an dichten $\mathbb{Z}$-Gittern interessiert ist, so ist es nach Bemerkung 4.2.6 von Vorteil, nur Vertreter der Galoisbahnen zu bestimmen.

5.5 Die Klassengruppe zweiseitiger Ideale

Testen, ob ein normales R-Gitter ein Hauptideal ist
Für alle $x \in \mathfrak{D}^*$ ist $\mathrm{nr}_{\mathfrak{D}/K}(x\mathfrak{M}) = \mathrm{nr}_{\mathfrak{D}/K}(x) \cdot R$ ein gebrochenes Hauptideal von K mit einem total positiven Erzeuger $\mathrm{nr}_{\mathfrak{D}/K}(x)$.
Sei nun I ein beliebiges normales R-Gitter mit $\mathfrak{M} := \mathcal{O}_r(I)$. Wir wollen bestimmen, ob I ein Hauptideal ist und gegebenfalls ein $x \in I$ mit $I = x\mathfrak{M}$ finden. Dazu kann man wie folgt verfahren: Zuerst bestimmt man $\mathrm{nr}_{\mathfrak{D}/K}(I)$. Ist dies kein gebrochenes Hauptideal in K, dann kann I auch kein Hauptideal sein. Andernfalls sei $\mathrm{nr}_{\mathfrak{D}/K}(I) = aR$. Nun bestimmt man $\mod (R^*)^2$ alle die Einheiten $e_1, \ldots, e_k$ von R^*, für die ae_i total positiv ist. (Dazu muß man die Einheitengruppe von R bestimmen und dann ein lineares Gleichungssystem über $\mathbb{F}_2$ lösen vgl. das Programmlisting im Anhang.) Gibt es keine solche Einheit, dann ist I wiederum kein Hauptideal. Andernfalls muß man nun für jedes i alle Vektoren x des $\mathbb{Z}$-Gitters $(I, N_{\mathbb{Q}})$ mit Länge $2\,\mathrm{Tr}_{K/\mathbb{Q}}(e_i a)$ testen, ob eines die Identität $I = x\mathfrak{M}$ erfüllt.

Algorithmus 5.5.1 : Feststellen, ob ein normales R-Gitter ein Hauptideal ist.

Eingabe : Ein normales R-Gitter I.
Ausgabe : Ein $x \in A$ mit $I = x\mathcal{O}_r(I)$ falls I ein Hauptideal ist, andernfalls **false**.

$\mathfrak{M} \leftarrow \mathcal{O}_r(I)$;
wenn $\mathrm{nr}_{\mathfrak{D}/K}(I)$ *ist kein Hauptideal* **dann zurück false**;
Bestimme ein $a \in K$ mit $aR = \mathrm{nr}_{\mathfrak{D}/K}(I)$;
Finde alle $e_1, \ldots, e_k \in R^*$ für die ae_i total positiv ist;
für alle e_i **tue**
  für alle $x \in I$ *mit* $N_{\mathbb{Q}}(x,x) = 2\,\mathrm{Tr}_{\mathfrak{D}/K}(ae_i)$ **tue**
    wenn $x\mathfrak{M} = I$ **dann zurück** x;
  Ende
Ende
zurück false;

Das obige Verfahren funktoniert natürlich auch, wenn man $e_i a$ mit dem Quadrat einer Einheit e multipliziert, denn es gilt $\mathrm{nr}_{\mathfrak{D}/K}(e) = e^2$. Da $\mathrm{Tr}_{K/\mathbb{Q}}(e_i a)$ sehr groß werden kann, empfiehlt es sich zuerst ein $e \in R^*$ zu suchen, so daß $\mathrm{Tr}_{K/\mathbb{Q}}(e^2 e_i a)$ kleiner wird.

Weiter kann man noch vorab $\mathfrak{M}^{\cdot 1}$ bestimmen und merkt sich während des Algorithmus, welche Elemente $x \in \mathfrak{M}$ man schon auf $x\mathfrak{M} = I$ hin untersucht hat. Ein neues Element x' muß dann nur noch getestet werden, wenn $x^{-1}x' \notin \mathfrak{M}^{\cdot 1}$ gilt.

Feststellen, ob zwei normale R-Gitter linksäquivalent sind
Da zwei normale R-Gitter I und J genau dann linksäquivalent sind, wenn sie dieselbe Rechtsordnung besitzen und zudem IJ^{-1} ein Hauptideal ist, können wir nun auch zwei normale R-Gitter auf Äquivalenz testen. Insbesondere liefert der obige Algorithmus dann gegebenenfalls ein $x \in A$ mit $I = xJ$.

Feststellen, ob zwei normale R-Gitter rechtsäquivalent sind
Zwei normale R-Gitter I und J sind genau dann rechtsäquialent, wenn sie dieselbe

Linksordnung besitzen und $J^{-1}I$ ein Hauptideal ist. Dies können wir nun auch überprüfen.

Bestimmen der Gruppe zweiseitiger Idealklassen einer R-Maximalordnung

Es seien $\mathfrak{M}$ eine R-Maximalordnung und $\mathfrak{a}_1, \ldots, \mathfrak{a}_h$ ein Vertretersystem der Idealklassengruppe $\mathrm{Cl}(K)$ und $\mathfrak{P}_1, \ldots, \mathfrak{P}_s$ die Primideale von $\mathfrak{M}$, die über den in $\mathfrak{D}$ verzweigten Primidealen $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ liegen. In Bemerkung 4.1.8 haben wir bereits gesehen, daß $\{\mathfrak{a}_i \prod_{j=1}^{s} \mathfrak{P}_j^{\alpha_j} \mid 1 \leq i \leq h,\ \alpha \in \{0,1\}^s\}$ ein Repräsentantensystem der Klassen zweiseitiger $\mathfrak{M}$-Ideale enthält. Daraus können wir nun ein Vertretersystem extrahieren, denn wir wissen bereits wie man testet, ob zwei $\mathfrak{M}$-Ideale dieselbe Klasse repräsentieren.
Das zu $\mathfrak{p}_i$ korrespondierende Primideal $\mathfrak{P}_i$ von $\mathfrak{M}$ ist das einzige Primideal von $\mathfrak{M}$ mit $\mathfrak{p}_i\mathfrak{M}_i \subseteq \mathfrak{P}$. Nach Bemerkung 4.1.8 ist es auch das eindeutig bestimmte maximal ganze $\mathfrak{M}$-Rechtsideal mit dieser Eigenschaft. Also bestimmen wir $\mathfrak{P}_i$ wie schon zuvor als maximalen $\mathfrak{M}$-Teilmodul von $\mathfrak{M}/\mathfrak{p}_i\mathfrak{M}$.

Wir kommen zu folgendem Algorithmus:

Algorithmus 5.5.2 : Bestimmen der zweiseitigen $\mathfrak{M}$-Idealklassen

Eingabe : Eine Maximalordnung $\mathfrak{M}$ und die in A verzweigen Primideale $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$.
Ausgabe : Ein Vertretersystem der zweiseitgen $\mathfrak{M}$-Idealklassen.

$V \leftarrow \{\mathfrak{M}\}$;
für alle $\mathfrak{p}_i$ **tue**
  Bestimme das maximal ganze $\mathfrak{M}$-Rechtsideal M mit $\mathfrak{p}_i\mathfrak{M} \subseteq \mathfrak{M}$;
  wenn M *zu keinem* $J \in V$ *äquivalent* **dann**
    $V \leftarrow V \cup \{M\}$;
    für alle $I \in V$ **tue**
      wenn $M \cdot I$ *zu keinem* $J \in V$ *äquivalent* **dann** $V \leftarrow V \cup \{M \cdot I\}$;
    Ende
  Ende
Ende
Bestimme Idealklassenvertreter $\{\mathfrak{a}_1, \ldots, \mathfrak{a}_h\}$ von $\mathrm{Cl}(K)$;
für alle $\mathfrak{a}_i \nsim R$ **tue**
  wenn $\mathfrak{a}_i \cdot \mathfrak{M}$ *zu keinem* $J \in V$ *äquivalent* **dann**
    $V \leftarrow V \cup \{\mathfrak{a}_i \cdot \mathfrak{M}\}$;
    für alle $I \in V$ **tue**
      wenn $\mathfrak{a}_i \cdot I$ *zu keinem* $J \in V$ *äquivalent* **dann** $V \leftarrow V \cup \{\mathfrak{a}_i \cdot I\}$;
    Ende
  Ende
Ende
zurück V;

Die $\mathfrak{P}_i$ kann man wie schon zuvor als maximalen $\mathfrak{M}$-Teilmodul von $\mathfrak{M}/\mathfrak{p}_i\mathfrak{M}$ bestimmen. Alternativ kann man auch die maximalen $\mathfrak{M}$-Teilmoduln von $\mathfrak{M}/p\mathfrak{M}$ mit $p\mathbb{Z} = \mathfrak{p}_i \cap \mathbb{Z}$ bestimmen. Von denen nimmt man dann nur die zweiseitigen $\mathfrak{M}$-Ideale. Sicher ist $\mathfrak{P}_i$ eines davon. Wenn nicht alle Primideale von R über pR in $\mathfrak{D}$ verzweigen, so liefert

dies eventuell ein paar mehr Erzeuger als nötig. Verzweigen jedoch alle, so liefern die beiden Methoden genau dieselben Primideale von $\mathfrak{M}$.

5.6 Rechtsidealklassen einer R-Maximalordnung

Es sei $\mathfrak{M}$ eine Maximalordnung. Im vorherigen Abschnitt haben wir Repräsentanten der Klassen zweiseitiger $\mathfrak{M}$-Ideale bestimmt. Nun wollen wir ein Vertretersystem aller Rechtsidealklassen von $\mathfrak{M}$ bezüglich Linksäquivalenz bestimmen.

Finden aller Links- bzw. Rechtsidealklassen einer R-Maximalordnung
Kennt man alle Rechtsidealklassen von $\mathfrak{M}$, so kennt man nach Korollar 2.6.6 auch alle Typen $\mathfrak{M}_1, \ldots, \mathfrak{M}_T$ von R-Maximalordnungen. Man kann also nicht hoffen, die Rechtsidealklassen von $\mathfrak{M}$ leichter bestimmen zu können als alle Klassen von R-Maximalordnungen.

Wir wollen daher annehmen $\mathfrak{M}_1, \ldots, \mathfrak{M}_T$ seien schon bestimmt. Finden wir nun zu jeder dieser R-Maximalordnung $\mathfrak{M}_i$ ein Repräsentantensystem $\{I_{i,1}, \ldots, I_{i,H_i}\}$ der Klassen zweiseitiger $\mathfrak{M}_i$-Ideale, so ist $\{I_{i,j}\mathfrak{M}\}$ nach Korollar 2.6.7 ein Vertretersystem der Rechtsidealklassen von $\mathfrak{M}$.

Analog bestimmt man die Linksidealklassen von $\mathfrak{M}$ bezüglich Rechtsäquivalenz. Falls ein Vertretersystem schon bestimmt ist, kann man auch verwenden, daß $I \mapsto I^{-1}$ eine Bijektion zwischen den Links- und Rechtsidealklassen von $\mathfrak{M}$ induziert.

Bestimmen der Klassengruppe der stabil-äquivalenten $\mathfrak{M}$-Rechtsideale
Nach Satz 2.10.5 sind zwei $\mathfrak{M}$-Rechtsideale I und J genau dann stabil äquivalent, wenn $\mathrm{nr}_{\mathfrak{D}/K}(I)$ und $\mathrm{nr}_{\mathfrak{D}/K}(J)$ in der Strahlklassengruppe von K (modulo aller unendlichen Stellen von K) gleich sind.
Weil zwei linksäquivalente $\mathfrak{M}$-Rechtsideale immer auch stabil äquivalent sind, enthält jedes Vertretersystem von $\mathfrak{M}$-Rechtsidealen auch ein Vertretersystem bezüglich stabiler Äquivalenz. Also können wir nun die Klassengruppe der stabil-äquivalenten $\mathfrak{M}$-Rechtsideale angeben.

Anhang A

Anhang: Programmlisting

A.1 Beschreibung des Programms

Hier sind nun die einzelnen Befehle des Programms und ihre Syntax aufgeführt. Die Befehle sind in einzelne Gruppen unterteilt, wie bei der Beschreibung der Algorithmen auch.
Im folgenden sei K ein algebraischer Zahlkörper mit $n := [K/\mathbb{Q}]$ und $R = \mathbb{Z}_K$.

Konstruktion
Das Programm stellt eine Quaternionenalgebra $\mathfrak{D}$ über K intern in folgender Struktur dar:

```
Type_QA:= recformat <
  K: Fld, a: FldElt, b: FldElt,
  Names: SeqEnum,
  s: Integers(), h: Integers(), Minkowski: Integers(), Depth: Integers(),
  Mass: Rationals(), Found: Rationals(),
  T: AlgMatElt, tr: AlgMatElt, NQ: AlgMatElt,
  B, Bo, Places, Forms, Galois, MaxOrders: SeqEnum,
  PlacesZ: SetEnum >;|
```

`K` ist dabei der algebraische Zahlkörper K. Ist die Algebra als $\left(\frac{a,b}{K}\right)$ erzeugt worden, so sind die Elemente a und b ebenfalls abgelegt. `Names` enthält die Namen der Basiselemente. Die Anzahl der verzweigten R-Stellen ist in `s` gespeichert. `Minkowski` enthält die Minkowskischranke und `h` die Klassenzahl von K. In `Mass` wird die Summe der Eichlermaße aller Konjugationsklassen von R-Maximalordnungen festgehalten und in `Found` steht die Summe der Eichlermaße der bisher schon bestimmten Konjugationsklassen. `B` enthält die rechtsreguläre Darstellung einer fixierten $\mathbb{Q}$-Basis $\underline{b} = (b_1, \ldots, b_m)$ und `Bo` beschreibt die Rechtsmultiplikation der b_i^o auf $\underline{b}$.
`tr` ist die Matrix $tr := (\mathrm{tr}_{\mathfrak{D}/K}(b_i b_j))$ und `T` ist $(\mathrm{tr}_{\mathfrak{D}/\mathbb{Q}}(b_i b_j))$. In `NQ` ist die Normform bzgl $\mathbb{Q}$ abgelegt, also $\mathrm{tr}_{\mathfrak{D}/\mathbb{Q}}(b_i \bar{b}_j)$. Die verzweigten Primideale von R befinden sich in `Places` und in `PlacesZ` sind die Primzahlen, über denen ein in $\mathfrak{D}$ verzweigtes Primideal von R liegt. Die erste Matrix in der Liste `Forms` ist immer $\mathrm{tr}_{\mathfrak{D}/\mathbb{Q}}(\alpha b_i \bar{b}_j)$ mit einem primitiven Element α von K. Ist $K/\mathbb{Q}$ galoisch und soll die Galoisoperation auf den Konjugationsklassen von R-Maximalordnungen verwendet werden, so folgen in `Forms` auch noch die

Matrizen $\mathrm{tr}_{\mathfrak{D}/\mathbb{Q}}(\sigma(\alpha)b_i\overline{b}_j)$ mit $\sigma \in \mathrm{Gal}(K/\mathbb{Q}) \setminus \{\mathrm{id}_K\}$. Die Liste `MaxOrders` speichert die bereits gefundenen Vertreter der Konjugationsklassen von R-Maximalordnungen. Die Struktur eines Eintrags ist nachfolgend erklärt:

```
Type_MaxOrder:= recformat <
  L: AlgMatElt, I: AlgMatElt, T: AlgMatElt, F: AlgMatElt,
  Lat,
  AutNr: Integers(),
  Checked: SetEnum,
  Galois: SeqEnum >;
```

Sei $\mathfrak{M}$ eine R-Maximalordnung. Die obige Struktur verwaltet $\mathfrak{M}$ dann wie folgt: `L` ist eine Basismatrix von $\mathfrak{M}$ und `I` die Basismatrix des R-Gitters I, als dessen Linksordnung $\mathfrak{M}$ gefunden wurde. `Lat` ist das $\mathbb{Z}$-Gitter $(\mathfrak{M}, \mathbb{N}_{\mathbb{Q}})$ bezüglich der LLL-reduzierten Basis `T*L`. In `F` befindet sich die für die Isometrietest wichtige Matrix $\mathrm{tr}_{\mathfrak{D}/\mathbb{Q}}(\alpha y_i \overline{y}_j)$ wobei $(y_1, \ldots, y_m)$ die durch TL beschriebene $\mathbb{Z}$-Basis von $\mathfrak{M}$ ist. `AutNr` speichert $|\mathrm{O}(\mathfrak{M}, N)|$. In `checked` wird festgehalten, für welche Primzahlen p wir schon die Linksordnungen der maximalen $\mathfrak{M}$-Rechtsideale zwischen $p\mathfrak{M}$ und $\mathfrak{M}$ betrachtet haben. Wird die Galoisoperation betrachtet, und vertritt $\mathfrak{M}$ eine Konjugationsklasse, welche unter der Galoisoperation eine Bahn der Länge ungleich 1 hat, so enthält `Galois` noch einige Bilinearformen für die Isometrietests.

Wir kommen nun zum Erzeugen einer Quaternionenalgebra $\mathfrak{D}$. Mit

```
Init(K, A, B, Ao, Bo: OnlyMaxOrder:= false,
  Depth:= -1, zetak:= 0, UseGalois:= false) -> QA, LM
```

kann man eine beliebige Quaternionenalgebra $\mathfrak{D}$ über K mit der Basis $\underline{x} = (1 = x_1, x_2, x_3, x_1x_2)$ erzeugen. Die Matrix $A = (a_{ij}) \in K^{4\times 4}$ beschreibe dazu die Rechtsmultiplikation von x_2 auf $\underline{x}$. D.h. es gilt $x_ix_2 = \sum_{j=1}^{4} a_{ij}x_j$. Analog beschreiben die Matrizen `B`, `Ao` und `Bo` die Rechtsmultiplikation von x_3 respektive $\overline{x}_2$ bzw. $\overline{x}_3$. Die $\mathbb{Q}$-Standardbasis $(\underline{b}) = (b_1, \ldots, b_m)$ wird dann gewählt als $b_{4(k-1)l} := x_kr_l$ mit einer $\mathbb{Z}$-Basis $(r_1, \ldots, r_n)$ von R.

Die Funktion liefert dann eine Struktur `QA` vom Typ `Type_QA`, die die Algebra beschreibt und eine Basismatrix `LM` einer R-Maximalordnung.

Die optionalen Parameter bewirken:

Ist `OnlyMaxOrder` gesetzt, so werden nicht alle Felder der Struktur `QA` initialisiert. Einige Operationen sind dann aber nicht mehr durchführbar. Insbesondere ist es dann nicht mehr möglich, alle Konjugationsklassen von R-Maximalordnungen zu finden. Ist man nur an einer R-Maximalordnung interessiert, so ist dies schneller.

Der Parameter `Depth` wird an die MAGMAFunktion `IsIsometric` weitergegeben.

In `zetak` kann man, falls schon bekannt, $\zeta_K(-1)$ angeben. Andernfalls ruft das Programm PARI auf und versucht den Wert zu ermitteln. Bei $[K : \mathbb{Q}] \geq 7$ gelingt dies nicht immer, da eventuell der Stack von PARI überläuft oder die Anzahl der zu Beginn berechneten Primzahlen zu klein war. In diesem Fall hat man den Wert z.B. mittels

PARI selbst zu ermitteln. Das empfiehlt sich bei größeren Körpererweiterungen sowieso, damit man das Ergebnis erneut verwenden kann.

Ist `UseGalois` gesetzt, so werden, falls die Algebra gleichmäßig verteilte Invarianten besitzt, lediglich Vertreter der Bahnen der Galoisoperation auf den Konjugationsklassen von R-Maximalordnungen bestimmt. Es können dann aber nicht alle Konjugationsklassen bestimmt werden!

Da die Funktion `Init` unpraktisch zu handhaben ist, gibt es die Funktion

```
Initab(K, a, b: OnlyMaxOrder:= false, zetak:= 0, Depth:= -1, UseGalois)
```

Mit ihr kann man die Algebra $\mathfrak{D} = \left(\frac{a,b}{K}\right)$ direkt erzeugen. $-a, -b$ müssen total positiv sein. Die Rückgabewerte und optionalen Parameter sind identisch zu `Init`. Lediglich der Standardwert von `UseGalois` ist abhängig von K und a, b. `UseGalois` wird standardmäßig genau dann auf `true` gesetzt, wenn $K/\mathbb{Q}$ galoisch ist und $a, b \in \mathbb{Q}$ gilt. Da in diesem Fall aus einem Vertretersystem der Bahnen der Galoisoperation auf den Konjugationsklassen von R-Maximalordnungen alle Konjugationsklassen gewonnen werden können.

Zum Erzeugen der n-ten zyklotomischen Quaternionenalgebra $\mathfrak{D}_{\theta_n}$ verwendet man

```
InitCyclo:= (n: OnlyMaxOrder:= false, zetak:= 0,
  Depth:= -1, UseGalois:= false)
```

Die Rückgabewerte und die optionalen Parameter sind wie bei `Init`.

Beispiel Wir kommen nun zu unserem Beispiel $\mathfrak{D} = \left(\frac{-1,-7}{\mathbb{Q}(\sqrt{2})}\right)$, das wir parallel immer weiterverfolgen werden.

```
K:= QuadraticField(2);
QA, LM:= Initab(K, -1, -7);
verzweigte Stellen:  [
    Prime Ideal of R
    Two element generators:
        7
        $.2 + 3,
    Prime Ideal of R
    Two element generators:
        7
        $.2 + 4
]
Stellen ueber Z:= { 7 }
s:= 2
Mass:= 3/2
#1: AutNr:    32, wi1:   2, Mass:     1, #Bahn:   1
```

Die Algebra $\mathfrak{D}$ ist also verzweigt an den beiden Primidealen von R über $7\mathbb{Z}$. Ferner ist die Summe der Maße aller Konjugationsklassen von R-Maximalordnungen gleich $\frac{3}{2}$. Die letzte Zeile enthält Informationen zu der gefundenen ersten R-Maximalordnung

$\mathfrak{M}$. Die erste Zeile enthält die laufende Nummer der Konjugationsklassen, dann folgen $|\mathrm{O}(\mathfrak{M}, N)|$ und ω_i^1. Danach kommt das Eichlermaß der Konjugationsklasse und dann eventuell die Länge der Galoisbahn dieser Klasse.

Alle Informationen über eine R-Maximalordnung kann man mittels der Funktion `PrintInfo(QA, LM)` erfahren. Der zweite Parameter kann eine Basismatrix einer R-Maximalordnung sein, oder aber eine natürliche Zahl k, in diesem Fall werden die Informationen von `QA‘MaxOrders[k]`, dem Vertreter der k-ten Konjugationsklasse ausgelesen.
In unserem Beispiel:

```
> PrintInfo(QA, 1);
AutNr:    32, wi1:   2, winq:   1, Hi:   2
```

Die erste Zahl ist $|\mathrm{O}(\mathfrak{M}, N)|$, dann folgen die Daten, die in die Maßformel eingehen: $\omega_i^1, \omega_i^{nq}$ und die Anzahl H_i der zweiseitigen $\mathfrak{M}$-Ideale.

Element- und Gitterarithmetik Es beschreibe `QA` eine Quaternionenalgebra $\mathfrak{D}$. Weiter seien I und J zwei normale R-Gitter in $\mathfrak{D}$ mit den Basismatrizen `L1` und `L2`. Ferner seien $x, y \in \mathfrak{D}$ mit Koeffizientenvektoren $\mathtt{x} = (x_1, \ldots, x_m) \in \mathbb{Q}^m$ und $\mathtt{y} = (y_1, \ldots, y_m) \in \mathbb{Q}^m$ bzüglich der fixierten $\mathbb{Q}$-Standardbasis $\underline{b}$.

Um eine Darstellung von x in der K-Basis $x_1, \ldots, x_4$ zu erhalten, gibt es die Routine `KCoords(K, x)`. Das Gegenstück dazu bildet `EnlargeCoords(K, x)`, das eine Darstellung in der $\mathbb{Q}$-Basis $\underline{b}$ liefert.

Hat man eine Folge S von Koordinatenvektoren $v_1, \ldots, v_k \in K^4$ bezüglich der K-Basis $(x_1, \ldots, x_4)$, so konstruiert `SeqLat(K, S)` eine Basismatrix (bzgl. $\underline{b}$) des von den Vektoren in S erzeugten R-Gitters.

Für die Element- bzw. Gitterarithmetik stehen folgende Befehle zur Verfügung. Die Rückgabewerte sind, falls nicht anders vermerkt, stets Basismatrizen oder Koeffizientenvektoren bezüglich $\underline{b}$.

- `normx(QA, x)` berechnet $\mathrm{nr}_{\mathfrak{D}/K}(I)$ als Element von K.
- `norm(QA, L1)` liefert $\mathrm{nr}_{\mathfrak{D}/K}(I)$ als R-Ideal in K.
- `tracex(QA, x)` bestimmt $\mathrm{tr}_{\mathfrak{D}/K}(x) \in K$.
- `traces(QA, L1)` hat als Rückgabewert die Matrix $\mathrm{tr}_{\mathfrak{D}/K}(y_i y_j) \in K^{m \times m}$ wenn $\underline{y}$ die durch `L1` beschriebene $\mathbb{Z}$-Basis von I ist.
- `Productxy(QA, x, y)` bildet das Produkt xy.
- `ProductxI(QA, x, L1)` und `ProductIx(QA, L1, x)` liefen das Produkt xI respektive Ix.
- `Product(QA, L1, L2)` bestimmt eine Basismatrix von $I \cdot J$. Für `L2` kann auch die Basismatrix eines R-Ideals $\mathfrak{a}$ von K angegeben werden. Man erhält dann das Produkt $I\mathfrak{a} = \mathfrak{a}I$. Achtung: `L1` muß jedoch stets die Basismatrix eines R-Gitters in $\mathfrak{D}$ sein.

- `EqLats(L1, L2)` testet I und J auf Gleichheit.
- `IsROrder(QA, L1)` und `IsMaximalROrder(QA, L1)` prüfen, ob I eine (maximale) R-Ordnung ist.
- `IsNormalLat(QA, L1)` prüft, ob I ein normales R-Gitter ist.
- `LO(QA, L1)` und `RO(QA, L1)` konstruiert die Links- bzw. Rechtsordnung von I.
- `PrintLat(QA, L1)` gibt ein R-Erzeugendensystem von I auf dem Bildschirm aus. Die Elemente werden bezüglich der K-Basis $(x_1, \ldots, x_4)$ mit Koeffizienten in K geschrieben und nicht bezüglich R.

x kann mit Hilfe von `Invx(QA, x)` invertiert werden.

Um I zu invertieren gibt es 3 Moglichkeiten

- `Inv1(QA, L1)` verwendet die Formel $I^{-1} = \mathrm{nr}_{\mathfrak{D}/K}(I)^{-1}\overline{I}$.
- `Inv2(QA, L1: LRO, RODual)` invertiert I mittels $I^{-1} = (I \cdot \mathcal{O}_r(I)^{\#})^{\#}$. Falls bekannt, so kann man in `LRO` bzw. `RODual` eine Basismatrix von $\mathcal{O}_r(I)$ bzw. $\mathcal{O}_r(I)^{\#}$ mit übergeben. Besitzt man beide Informationen, so genügt `RODual`. Dies beschleunigt den Algorithmus erheblich.
- `Inv3(QA, L1: LLO, LRO)` bestimmt I^{-1} mittels der Definition. Falls bekannt, so kann man in `LLO` bzw. `LRO` eine Basismatrix der Links- oder Rechtsordnung von I übergeben. Das beschleunigt den Algorithmus merklich.

Alternativ kann man auch einfach `Inv(QA, L1: LLO, LRO, RODual)` aufrufen, dann wird eine passende Funktion gewählt.

Wir setzen nun unser Beispiel von oben fort:

```
> PrintLat(QA, LM);
< 1,
i,
1/2*(i+j),
1/2*(1+k) >
```

Also hat unsere erste R-Maximalordnung `LM` die R-Basis $\langle 1, \mathbf{i}, \frac{1}{2}(\mathbf{i}+\mathbf{j}), \frac{1}{2}(1+\mathbf{k})\rangle$.
Jetzt wollen wir mit einigen R-Gittern rechnen:

```
> S:= [[K.1, 0,0,0], [1,1,0,0], [0, K.1/2,K.1/2,0], [-1/2,1/2,1/2,1/2]];
> L:= SeqLat(K, S);
> IsNormalLat(QA, L);
true
```

Also haben wir ein normales Ideal eingegeben. Wir bestimmen nun dessen Rechtsordnung:

```
> LRO:= RO(QA, L);
> EqLats(LRO, LM);
true
```

Also ist I ein Rechtsideal von unserer ersten Maximalordnung.

```
> IInv:= Inv(QA, L);
> P:= Product(QA, IInv, L);
> EqLats(P, LRO);
true
```

Wie wir das auch erwartet haben, denn es gilt $I^{-1}I = \mathcal{O}_r(I)$.

Bestimmen aller Konjugationsklassen von R-Maximalordnungen
Zum Bestimmen aller Konjugationsklassen von R-Maximalordnungen dient `FindMaxOrders(~QA, k, p)`. Der erste Parameter ist eine Referenz auf eine Struktur `QA`. Der Index `k` muß auf einen schon gefunden Vertreter $\mathfrak{M}_k$ von R-Maximalordnungen von `QA` verweisen. Der Algorithmus bestimmt dann die Linksordnungen aller maximal ganzen $\mathfrak{M}_k$-Rechtsideale zwischen $p\mathfrak{M}_k$ und $\mathfrak{M}$. Von jeder neu gefundenen Konjugationsklasse wird ein Vertreter in `QA‘MaxOrders` abgelegt. Ferner wird die Summe der Eichlermaße der schon bestimmten Konjugationsklassen entsprechend erhöht.
Achtung: Die Struktur `QA` darf aber nicht mit dem Parameter `OnlyMaxOrder` erzeugt worden sein.

Um Festzustellen, ob alle Konjugationsklassen bereits gefunden sind, verwendet man `Done(QA)`.

Um das Finden zu automatisieren, gibt es die Funktion
`FindAllMaxOrders(~QA: Bound:= 0, primes:= [], RayClass:= true)`.

Der erste Parameter ist wieder eine Referenz auf eine Stuktur `QA`. Das Programm wendet dann den vorherigen Algorithmus `FindMaxOrders(~QA, k, p)` wiederholt an und versucht so, alle Konjugationsklassen von R-Maximalordnungen zu finden.

Ist `primes` durch den Benutzer auf eine Liste von Primzahlen gesetzt, so durchläuft das Programm nur die in der Liste befindlichen Primzahlen, in der angegebenen Reihenfolge.
Ist `primes` nicht gesetzt, so geht der Algorithmus wie folgt vor:

Ist `RayClass=true` (die Standardeinstellung), so werden zunächst Primideale $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$ von R, welche die Strahlklassengruppe von K (modulo aller unendlichen Stellen von K) erzeugen gesucht. Für alle Primzahlen p, über denen eines der $\mathfrak{p}_i$ liegt, wird nun `FindMaxOrders(~QA, 1, p)` aufgerufen.

Sollten so noch nicht alle Konjugationsklassen bestimmt sein, so durchläuft der Algorithmus nun alle bereits gefundenen R-Maximalordnungen und alle Primzahlen p zwischen 2 und `Bound`. Der Standardwert von `Bound` ist das Minimum von 500 und der Minkowskischranke. Dabei werden diese Primzahlen $p_1, \ldots, p_l$ so sortiert, das die Anzahl der maximal ganzen $\mathfrak{M}$-Rechtsideale zwischen $p\mathfrak{M}$ und $\mathfrak{M}$ für jede R-Maximalordnung $\mathfrak{M}$ aufsteigt. D.h. zuerst werden die Primzahlen getestet, die sehr wenige Rechtsideale liefern. Findet man nun eine neue Konjugationsklasse von R-Maximalordnungen, so werden zunächst diese neuen Klassen beginnend bei p_1 getestet. Der Algorithmus bricht ab, wenn alle Konjugationsklassen bestimmt sind, oder aber jede Kombination von bereits gefundenen Vertretern und Primzahlen $p_1, \ldots, p_l$ durchsucht wurde.

Um Vertreter aller schon gefundener Konjugationsklassen von R-Maximalordnungen aufzulistet, gibt es den Befehl `ListMaxOrders(QA: all:= false)`. Der Rückgabewert ist eine Liste mit Basismatrizen aller schon bestimmter Vertreter von Konjugationsklassen. Ist `all` gesetzt, so müssen bereits alle Konjugationsklassen bestimmt sein. Ansonsten wird eine entsprechende Fehlermeldung ausgegeben. Die Funktion ist besonders nützlich, wenn lediglich Vertreter der Galoisbahnen bestimmt worden sind und $\mathfrak{D}\left(\frac{a,b}{K}\right)$ mit $a, b \in \mathbb{Q}$ ist. Die Funktion liefert dann nämlich auch Vertreter der Konjugationsklassen, die in derselben Galoisbahn liegen.

In unseren Beispiel erhalten wir

```
> FindAllMaxOrders(~QA);
k =  1, p =   2, #Teilmoduln: 3
#2: wi1:   8, AutNr:   128, Mass:   1/2, #Bahn:   1
Fertig!
```

Die erste Zeile gibt an, daß gerade der erste Vertreter an der Primzahl $p = 2$ untersucht wird. Für jede gefundene Konjugationsklasse wird nun wie bei der Initialisierung von `QA` eine kurze Information zu dieser Klasse ausgegeben. In diesem Fall gibt es also genau zwei Konjugationsklassen.

Will man zwei R-Ordnungen auf Konjugation hin untersuchen, so kann man dies mit `ConjugateROrders(QA, L1, L2)` tun.

Konstruktion der zweiseitigen $\mathfrak{M}$-Idealklassen
Sei `LM` die Basismatrix einer R-Maximalordnung $\mathfrak{M}$ in $\mathfrak{D}$.

Die Routine `Listnorm1(QA, LM: all:= false)` liefert die Elemente von $\mathfrak{M}^{*,1}$ als eine Liste. Ist `all` gesetzt, werden wirklich alle Elemente geliefert, ansonsten (das ist die Standardeinstellung) wird von jedem Paar $(x, -x)$ immer jeweils eines genommen.

Mit Hilfe von `IsPrincipalIdeal(QA, L: LRO:= 0, norm1:= [])` kann für ein normales R-Gitter I mit Basismatrix `L` festgestellt werden, ob dieses ein Hauptideal ist. Falls bekannt, so können in `LRO` die Basismatrix von $\mathcal{O}_r(I)$ und in `norm1` die Elemente von $\mathfrak{M}^*$ mit reduzierter Norm 1 mit übergeben werden. Die Liste `norm1` darf aber nicht mit dem Parameter `all` (s.o.) gebildet worden sein. Der erste Rückgabewert ist ein boolscher Wert, der angibt, ob I ein Hauptideal ist. Falls dies der Fall ist, so liefert der zweite Rückgabewert ein `x` mit $I = x\mathcal{O}_r(I)$.

Zum Bestimmen der zweiseitigen $\mathfrak{M}$-Idealklassen gibt es den Befehl `ListIdealClasses(QA, LM)`. Der Rückgabewert ist eine Liste der Basismatrizen von Vertretern der Äquivalenzklassen zweiseitiger $\mathfrak{M}$-Ideale. Alternativ kann man auch `ListIdealClasses2(QA, LM)` verwenden. Die erste Funktion bestimmt die maximal ganzen $\mathfrak{M}$-Ideale zwischen $\mathfrak{p}\mathfrak{M}$ und $\mathfrak{M}$, wobei $\mathfrak{p}$ die in $\mathfrak{D}$ verzweigen Primideale von R durchläuft, während die zweite Funktion mit Primzahlen p arbeitet. Ersteres ist besser, wenn $\mathfrak{D}$ keine gleichmäßig verteilten Invarianten besitzt. Ansonsten ist die erste Methode ein klein wenig langsamer. (Vgl. die Beschreibung des Algorithmus auf Seite 94.)

Die Funktion `IdealClassGroup(QA, LM: list)` liefert drei Werte zurück. Der erste ist eine abelsche Gruppe, die isomorph zur Gruppe von Äquivalenzklassen zweiseitiger

$\mathfrak{M}$-Ideale ist. Der zweite Wert ist eine Abbildung von dieser Gruppe in ein Vertretersystem von Idealklassen und der dritte ist eine Funktion, mit deren Hilfe man einem beliebigen zweiseitigen $\mathfrak{M}$-Ideal das entsprechende Gruppenelement seiner Klasse zuordnen kann. Falls ein Vertretersystem von zweiseitigen $\mathfrak{M}$-Idealen schon bekannt ist, kann man dieses im optionalen Parameter `list` bereitstellen.

In unserem Beispiel:

```
> G, m, minv:= IdealClassGroup(QA, LM);
> #G;
2
>I:= m(G.2); I;
[1/2 5/2   0   0   0   0 1/2 1/2]
[  0 7/2   0   0   0   0   0 1/2]
[  0   0 1/2 5/2 1/2 1/2   0   0]
[  0   0   0 7/2   0 1/2   0   0]
[  0   0   0   0   1   0   0   0]
[  0   0   0   0   0   1   0   0]
[  0   0   0   0   0   0   1   0]
[  0   0   0   0   0   0   0   1]
> P:= Product(QA, I, I);
> minv(P);
Id(G)
> ok, x:= IsPrincipalIdeal(QA, P); ok;
true
> EqLats( ProductxI(QA, x, LM), P);
true
```

Es sei bemerkt, daß die zurückgegebene Funktion `minv(L)` nicht testet, ob die übergebene Matrix `L` ein zweiseitiges $\mathfrak{M}$-Ideal ist.

Bestimmen der Links- bzw. Rechtsidealklassen von $\mathfrak{M}$
Sei `LM` die Basismatrix einer R-Maximalordnung $\mathfrak{M}$ in $\mathfrak{D}$. Die Funktionen `ListLeftIdealClasses(QA, LM)` und `ListRightIdealClasses(QA, LM)` liefern jeweils eine Liste von Basismatrizen von Vertretern der Links- bzw. Rechtsidealklassen von $\mathfrak{M}$. Dazu müssen jedoch alle Konjugationsklassen von R-Maximalordnungen bereits bekannt sein.

Die Gruppe der stabil äquivalenten $\mathfrak{M}$-Rechtsideale kann man mit `StableIdealClassGroup(QA, LM: right:= true)` bestimmen. Die Funktion liefert wiederum drei Werte. Der erste ist die Strahlklassengruppe von K modulo aller unendlichen Stellen. Der zweite Wert ist eine Abbildung von dieser Gruppe in ein Vertretersystem der stabil äquivalenten Rechtsidealklassen von $\mathfrak{M}$. Der dritte Rückgabewert ist eine Funktion `f(L)`, mit deren Hilfe man jedem $\mathfrak{M}$-Rechtsideal das Gruppenelement seiner Klasse bezüglich stabiler Äquivalenz zuordnen kann. Wird der optionale Parameter `right` auf `false` gesetzt, so bestimmt die Funktion die Gruppe der stabil äquivalenten Linksidealklassen von $\mathfrak{M}$.

A.2 Programmlisting

Es folgen die von mir entwickelten und in MAGMA implementierten Algorithmen. Ich selbst habe die Version 2.12-6 von MAGMA benutzt. Frühere Versionen funktionieren zumeist nicht, da sie Fehler in den Routinen `IsIsometric` und `Factorization` besitzen. Dies verhindert z.B. das Bestimmen der in einer Quaternionenalgebra $\mathfrak{D}$ verzweigten Primideale von R.

Um die Algorithmen nicht unnötig zu verlangsamen, überprüfen die Routinen zumeist nicht, ob die eingegebenen Daten korrekt sind. Der Benutzer hat selbst dafür zu sorgen, daß z.B. Funktionen die nur mit normalen R-Gittern arbeiten, auch nur auf solche angewendet werden.

Man könnte die Algorithmen noch etwas beschleunigen, wenn die Basismatrix L eines R-Gitters nicht als Element von $\mathbb{Q}^{m\times m}$ schreibt, sondern man faktorisiert den Hauptnenner d von L heraus und erhält so ein Paar (d, L') mit $d \in \mathbb{Z}$ und $L' \in \mathbb{Z}^{m\times m}$. Das würde jedoch ebenfalls die Programme unnötigt komplizierter machen. Daher habe ich mich dagegen entschieden.

Die Routine `IdealClassGroup` verwendet nicht die Tatsache, daß die zweiseitigen $\mathfrak{M}$-Ideale eine R-Maximalordnung eine abelsche Gruppe bilden. Wollte man dies tun, so müßte man (zumindest bei den aktuellen Versionen von MAGMA) alle Algorithmen für R-Gitter als sogenannte „intrinsics“ implementieren. Dazu sollte man dann Datenstrukturen für R-Gitter, $\mathfrak{M}$-Idealklassen usw. einführen. Das hätte zwei große Nachteile. Zum einen werden die Programme dadurch unübersichtlicher. Zum anderen wäre die Implementation sehr stark an MAGMA gebunden. Ich habe deswegen darauf verzichtet.

```
Attach("sigfield");

Type_MaxOrder:= recformat <
  L: AlgMatElt, I: AlgMatElt, T: AlgMatElt, F: AlgMatElt,
  Lat,
  AutNr: Integers(),
  Checked: SetEnum,
  Galois: SeqEnum >;

Type_QA:= recformat <
  K: Fld, a: FldElt, b: FldElt,
  Names: SeqEnum,
  s: Integers(), h: Integers(), Minkowski: Integers(), Depth: Integers(),
  Mass: Rationals(), Found: Rationals(),
  T: AlgMatElt, tr: AlgMatElt, NQ: AlgMatElt,
  B, Bo, Places, Forms, Galois, MaxOrders: SeqEnum,
  PlacesZ: SetEnum >;


// Sind alle Maximalordnungen gefunden?
Done:= func < QA | QA`Mass eq QA`Found >;

//Hilfsfunktion. Liefert \sum{X_iS_i} bzw.[\sum{X_ijS_j]]_i
```

```
LinKomb:= function(S, X)
  if (Type(X) eq SeqEnum) or (Nrows(X) eq 1) then
    X:= Eltseq(X); // fuer Matrizen mit einer Zeile
    S:= Eltseq(S);
    return &+[X[i]*S[i]: i in [1..Min(#X, #S)] | (X[i] ne 0) and (S[i] ne 0)];
  end if;
  return
    [ &+[X[i,j]*S[j]: j in [1..Ncols(X)] | X[i,j] ne 0]: i in [1..Nrows(X)] ];
end function;

// Bestimmt den Hauptnenner aller Koeffizienten der Matrix M
MatrixDenom:= function(M)
  if (Type(BaseRing(M)) eq RngInt) then
    return 1;
  end if;
  return LCM( { Denominator(x): x in Eltseq(M) } );
end function;

// bringt eine Matrix M auf obere Dreicksform
HNF:= function(M)
  denom:= MatrixDenom(M);
  return ChangeRing(EchelonForm(ChangeRing(denom*M, Integers())), Rationals())/denom;
end function;

// Liefert die regulaere Darstellung von L.
// Die Folge B muss entweder QA‘B oder QA‘Bo sein.
RegularRep:= func < B, L |
  [ LQ*b*LQInv: b in LinKomb(B, LQ) ]
    where LQInv:= LQ^-1 where LQ:= ChangeRing(L, Rationals()) >;
RegularRepZ:= func < B, L |
  [ ChangeRing(L*b*LInv, Integers()): b in LinKomb(B, L) ] where LInv:= L^-1 >;

// Testet, ob zwei Gitter gleich sind
function EqLats(L1, L2)
  X:= L1*ChangeRing(L2, Rationals())^-1;
  return (X in ChangeRing(Parent(L1), Integers()))
           and (Abs(Determinant(X)) eq 1);
end function;

// Liefert das Produkt des Gitters L1 und L2. L2 darf auch die Basismatrix
// eines R-Ideals in K sein.
Product:= function(QA, L1, L2)
  Y:= [ChangeRing(b, Rationals()): b in LinKomb(QA‘B, L2)];
  X:= VerticalJoin([L1*y: y in Y]);
  denom:= MatrixDenom(X);
  X:= EchelonForm(ChangeRing(denom*X, Integers()));
  return RowSubmatrix(ChangeRing(X, Rationals()), Ncols(L1))/denom;
end function;

// Produkte von Gittern mit Elementen
```

```
ProductxI:= function(QA, x, L)
  x:= Vector(Rationals(), x);
  return Matrix([x*ChangeRing(b, Rationals()): b in LinKomb(QA‘B, L)]);
end function;

ProductIx:= func< QA, L, x | L*LinKomb(QA‘B, x) >;

// Produkt zweier Elemente
Productxy:= function(QA, x, y)
  return Vector(Rationals(), x)*ChangeRing(LinKomb(QA‘B, y), Rationals());
end function;

// Liefert die Involution eines R-Gitters bzw. Elements
Involution:= func < QA, L |
  L*Matrix(Rationals(), #QA‘B, #QA‘B, [b[1]: b in QA‘Bo]) >;
Involutionx:= func< QA, x |
  Vector(Rationals(), x)*Matrix(Rationals(), #QA‘B, #QA‘B, [b[1]: b in QA‘Bo])>;

// wandelt Koordinaten bzgl. K-Basis in Koord. bzgl. b_1,...,b_m
EnlargeCoords:= function(K, elt)
  if (Type(K) ne FldRat) then K:= AbsoluteField(K); end if;
  elt:= Eltseq(elt);
  R:= Integers(K);
  denom:= LCM([Denominator(e): e in elt]);
  return
    Vector(Rationals(), &cat[ Eltseq(R ! (denom * elt[i])): i in [1..4]])/denom;
end function;

// wandelt Koordinaten bzgl. b_1,...,b_m in Koord. bzgl. der K-Basis
KCoords:= function(K, elt)
  if (Type(K) eq FldRat) then
    return ChangeUniverse(Eltseq(elt), Rationals());
  end if;
  K1:= AbsoluteField(K);
  elt:= ChangeUniverse(Eltseq(elt), K1);
  if (#elt eq 4) then return elt; end if;
  n:= AbsoluteDegree(K1);
  B:= Basis(Integers(K1));
  return [ K ! (&+[B[j]*elt[n*i+j]: j in [1..n]]): i in [0..3] ];
end function;

// red. Spur und Norm eines Elements x
tracex:= func< QA, x | (QA‘tr[1]*Matrix(QA‘K, Ncols(QA‘tr), 1, Eltseq(x)))[1]>;

normx:= function(QA, x)
  x:= Eltseq(x);
  if (#x ne #(QA‘B)) then x:= EnlargeCoords(QA‘K, x); end if;
  return (Vector(QA‘K, x) * QA‘tr *
     Matrix(QA‘K, Ncols(QA‘tr), 1, Eltseq(x)))[1]/2;
end function;
```

```
// Liefert tr_{A/K}(y_iy_j) wenn L die Basismatrix bzgl. y_1,...,y_m ist.
traces:= func < QA, L | L * QA`tr * Transpose(L) >;

// red. Norm eines R-Gitters L
norm:= function(QA, L)
  tr:= traces(QA, L);
  m:= Ncols(L);
  gens:= { tr[i,i]/2: i in [1..m] } join Seqset(Eltseq(tr));

  // man kann MAGMA nur schwer "1/2 * Z" beibringen ...
  if m eq 4 then
    denom:= LCM({ Denominator(x): x in gens });
    return GCD([Integers() | denom * x: x in gens]) / denom;
  end if;

  return ideal < Integers(QA`K) | gens >;
end function;

// Akzeptiert eine Folge Y von m Matrizen des \Q^{mxm} und liefert den
// Unterraum V von Q^m  mit v in V \iff vy in \Z^{mxm} fuer alle y in Y
invariant_mult:= function(Y)
  X:= Matrix([Eltseq(y): y in Y]);
  denom:= MatrixDenom(X);
  S, P, _:= SmithForm(ChangeRing(denom*X, Integers()));
  P:= ChangeRing(P*denom, Rationals());
  return HNF(Matrix([P[i]/S[i,i] : i in [1..#Y]]));
end function;

// Rechts- bzw. Linksordnungen des R-Gitters L
RO:= func< QA, L | invariant_mult(RegularRep(QA`B, L))*L >;
LO:= func< QA, L | invariant_mult(RegularRep(QA`Bo, L))*L >;

// Liefert das zu L duale Gitter, bzgl. Z.
myDualZ:= func< QA, L | (QA`T*Transpose(L))^(-1) >;

// Liefert das zu L duale Gitter, bzgl. R.
myDualR:= function(QA, L)
  DZ:= myDualZ(QA, L);
  if (Type(QA`K) eq FldRat) then return DZ; end if;
  return Product(QA, DZ, BasisMatrix(Different(Integers(QA`K))));
end function;

// Invertiert das R-Gitter L mittels Involution und red. Norm
Inv1:= function(QA, L)
  if (Type(QA`K) eq FldRat) then
    return Involution(QA, L) / norm(QA, L);
  else
    return Product(QA, Involution(QA, L), BasisMatrix(norm(QA, L)^(-1)));
  end if;
```

```
end function;

// Invertiert das normale R-Gitter L mittels Dualisieren.
// Falls die RO oder das duale der RO bekannt sind, kann man dies mit angeben.
Inv2:= function(QA, L: RODual:= 0, LRO:= 0)
  if (RODual eq 0) then
    if (LRO eq 0) then LRO:= RO(QA, L); end if;
    RODual:= myDualR(QA, LRO);
  end if;
  return myDualR(QA, Product(QA, L, RODual));
end function;

// Invertiert ein beliebiges R-Gitter L mittels der Definition.
// Ist die LO oder RO bekannt, kann man diese mit angeben.
Inv3:= function(QA, L: LRO:= 0, LLO:= 0)
  B:= LinKomb(QA`B, L);
  if ((LRO ne 0) and (LLO eq 0)) then
    B:= [ Matrix([L[i]*b*LROInv: b in B ]): i in [1..Nrows(L)] ]
        where LROInv:= LRO^-1;
  else
    if (LLO eq 0) then LLO:= LO(QA, L); end if;
    B:= [ L*b*LLOInv: b in B ] where LLOInv:= LLO^-1;
  end if;
  return invariant_mult(B)*L;
end function;

// Invertiert ein Ideal.
Inv:= function(QA, L: LLO:= 0, LRO:= 0, RODual:= 0)
  if (Type(QA`K) eq FldRat) then return Inv1(QA, L); end if;
  if (RODual ne 0) then return Inv2(QA, L: RODual:= RODual); end if;
  if (LLO ne 0) or (LRO ne 0) then
    return Inv3(QA, L: LLO:= LLO, LRO:= LRO);
  end if;
  return Inv1(QA, L);
end function;

//Invertiert ein Element x
Invx:= function(QA, x)
  n:= AbsoluteDegree(QA`K);
  x:= Vector(QA`K, x);
  if (Degree(x) ne n) then x:= KCoords(QA`K, x); end if;
  MConj:= Matrix(QA`K, 4, 4, [ KCoords(QA`K, QA`Bo[1+n*i, 1]): i in [0..3] ]);
  return EnlargeCoords(QA`K, (Vector(QA`K, x) / normx(QA, x)) * MConj);
end function;

MG:= func < L, Tr | ChangeRing(L*Tr*Transpose(L), Integers()) >;
MGQ:= func < L, Tr | L*Tr*Transpose(L) >;

// Liefert alle Elemente der MO LM mit red. Norm 1. Ist all=false, so wird
// von jedem Paar (x, -x) immer nur Element ausgegeben.
```

```
function Listnorm1(QA, LM: all:= false)
  Signs:= all select [-1, 1] else [1];
  G, T:= LLLGram(MG(LM, QA`NQ));
  SV:= ShortestVectors(LatticeWithGram(G));
  TLM:= ChangeRing(T, Rationals())*LM;
  U:= [ Eltseq(sgn*Vector(Rationals(), s)*TLM) : s in SV, sgn in Signs ];
  return U;
end function;

// Liefert die Basismatrizen aller bisher bekannten Maximalordnungen von QA.
// Ist "all" gesetzt, so muessen alle MO schon bestimmt sein, andernfalls
// wird ein Fehler ausgegeben. Die Funktion ist vor allem dann nuetzlich,
// wenn einige MO mit der Galoisoperation gefunden wurden und QA daher nicht
// die Basismatrizen aller MO speichert.
ListMaxOrders:= function(QA: all:= false)
  error if all and not Done(QA), "Fehler: Es sind nicht noch alle "*
    "Maximalordnungen bestimmt.";
  Ratab:= (assigned QA`a) and (assigned QA`b) and
    (QA`a in Rationals()) and (QA`b in Rationals());
  result:= [];
  for MO in QA`MaxOrders do
    Append(~result, MO`L);
    if (assigned MO`Galois) then
      error if (all and not Ratab), "Fehler: Aus den Galoisbahnen koennen "*
        "nicht alle Maximalordnungen gewonnen werden.";
      if Ratab then
        result cat:= [ MO`L * QA`Galois[g[1]]: g in MO`Galois ];
      end if;
    end if;
  end for;
  return result;
end function;

// Wandelt eine Liste von R-Erzeugern eines R-Gitters in ein Z-Gitter
// Dazu wird jedes Element einer Ganzheitsbasis von K an jeden Vektor von S
// multipliziert und davon dann eine Z-Basis ausgewaehlt.
SeqLat:= function(K, S)
  if (Type(K) ne FldRat) then K:= AbsoluteField(K); end if;
  R:= Integers(K);
  RB:= Basis(R);
  S:= Matrix(S);
  denom:= MatrixDenom(S);
  S:= ChangeRing(denom*S, R);
  L:= Matrix(Integers(),
      [&cat [Eltseq(R ! (r*x)): x in Eltseq(S[i])]: r in RB, i in [1..Nrows(S)]]);
  return ChangeRing(RowSubmatrix(EchelonForm(L), Ncols(L)), Rationals()) / denom;
end function;

Field2IntX:= function(K, R, X)
  denom:= MatrixDenom(X);
```

```
  X:= ChangeRing(denom*X, R);
  RB:= Basis(R);
  S:= &cat[ Eltseq(R ! (X[i,j] * RB[k])): j in [1..4], k in [1..#RB], i in [1..4] ];
  return Matrix(Rationals(), 4*#RB, S)/denom;
end function;

//Generiert aus einer K-Basis von QA unsere Standardbasis bzgl. K
Field2Int:= function(K, A, B)
  M:= MatrixRing(Rationals(), 4);
  M1:= M ! 1;
  if (Type(K) eq FldRat) then
    return ChangeUniverse([M1, A, B, A*B], M);
  end if;

  n:= AbsoluteDegree(K);
  R:= Integers(K);

  // reg. Darstellung der Basis des Rings
  RB:= [ RepresentationMatrix(b, Rationals()): b in Basis(R) ];
  // ueber Z
  B1:= [ TensorProduct(M1, b): b in RB ];

  Amxm:= Field2IntX(K, R, A);
  for i:= 1 to n do Append(~B1, B1[i] * Amxm); end for;
  Bmxm:= Field2IntX(K, R, B);
  for i:= 1 to 2*n do Append(~B1, B1[i] * Bmxm); end for;

  return B1;
end function;

// Wandelt einen Teilmodul M vom Ergebnis von Submodules() in ein Ideal der Algebra
// indem die fehlenden Zeilen ergaenzt werden.
MorphismToMatrix:= function(M, p)
  M:= ChangeRing(ChangeRing(M, Integers()), Rationals());
  L:= ScalarMatrix(Rationals(), NumberOfColumns(M), p);
  for i:= 1 to NumberOfRows(M) do
    L[Depth(M[i])]:= M[i];
  end for;
  return L;
end function;

// Liefert eine R-Ordnung, die L enthaelt, falls eine solche existiert.
// Der dritte Parameter ist die Det. der Basismatrix dieser Ordnung.
OrderAbove:= function(QA, L)
  m:= Ncols(L);
  dn:= Abs(Determinant(L));
  tr_B:= ColumnSubmatrix(QA`tr, 1); // red. Spur der Standardbasis

  repeat
    if not ( forall{x : x in Eltseq(ChangeRing(L, QA`K)*tr_B) | IsIntegral(x)} and
```

```
          forall{i: i in [1..m] | IsIntegral(normx(QA, L[i]))} ) then
      return false, _, _;
    end if;

    X:= VerticalJoin(Append([L*b: b in LinKomb(QA‘B, L)], L));
    denom:= MatrixDenom(X);
    Y:= EchelonForm(ChangeRing(denom*X, Integers()));
    L:= ChangeRing(RowSubmatrix(Y, m), Rationals())/denom;

    d:= dn;
    dn:= Abs( &*[L[i,i]: i in [1..m]]);
  until d eq dn;

  return true, L, d;
end function;

// Konstruiert eine R-Maximalordnung, indem es die minimalen Teilmoduln von
// einer Ordnung L/pL fuer eine Ordnug L und eine Primzahl p durchsucht.
function FindMaxOrder2(QA)
  m:= #(QA‘B);
  M:= MatrixRing(Integers(), m);
  L:= LO(QA, M ! 1);
  B:= RegularRepZ(QA‘B, L);

  // Det. der Grammatrix von L bzgl. R d.h.
  // Det(L*QA‘T*Transpose(L))/Discr(R)^4 berechnen
  D1:= Determinant(QA‘T) / Discriminant(Integers(QA‘K))^4;
  DL:= &*[ L[i,i]: i in [1..m] ];
  DFac:= Factorization(Integers() ! (D1 * DL^2));
  for i:= 1 to #DFac do
    p:= DFac[i, 1];
    repeat
      Mod:= RModule(ChangeRing(sub<M | B>, GF(p)));
      S:=  MinimalSubmodules(Mod);

      ok:= false;
      for s in S do
        // kann man bei p schon aus Dimensionsgruenden nicht mehr aufsteigen?
        if (DFac[i,2] lt 2*Dimension(s)) then continue; end if;

        ok, LN, DLN:= OrderAbove(QA, MorphismToMatrix(Morphism(s, Mod), p)*L/p);
        if ok then
          // Det(L*QA‘NQ*Transpose(L))/Discr(R)^4 neu berechnen
          DFac[i, 2] -:= 2* Valuation(DL/DLN, p);
          L:= LN;
          DL:= DLN;
          B:= RegularRepZ(QA‘B, L);
          break;
        end if;
      end for;
```

```
    until (not ok) or (DFac[i, 2] eq 0);
  end for;

  return L, [d: d in DFac | d[2] ne 0];
end function;

// Dasselbe, diesmal werden die Teilmoduln von L/pL mit einem Primideal von R
// durchlaufen
function FindMaxOrder(QA)
  m:= #(QA`B);
  M:= MatrixRing(Integers(), m);
  L:= LO(QA, M ! 1);
  B:= RegularRepZ(QA`B, L);
  D1:= Determinant(QA`T) / Discriminant(Integers(QA`K))^4;
  DL:= &*[ L[i,i]: i in [1..m] ];
  DFac:= Factorization(Integers() ! (D1 * DL^2));
  for i:= 1 to #DFac do
    p:= DFac[i, 1];
    repeat

      LD:= myDualR(QA, L);
      S, P, Q:= SmithForm(ChangeRing(L*LD^-1, Integers()));
      P:= ChangeRing(P, Rationals());
      T:= [GCD(S[i,i], p): i in [1..m]];
      denom:= LCM(T);
      //if (denom eq 1) then break; end if;
      T:= DiagonalMatrix(GF(p), [denom/t: t in T]);
      T2:= MatrixRing(Rationals(), m) ! 1;
      UInv:= MatrixRing(Rationals(), m) ! 0;
      j:= 1;
      for i:= 1 to m do
        if (T[i, i] eq 0) then
          T2:= RemoveRow(T2, j);
          UInv[i,i]:= 1;
        else
          j+:= 1;
      end if;
      end for;
      k:= m-j+1;
      UInv:= (VerticalJoin(T2, RowSubmatrix(UInv, k))*P)^-1;
      U:= T2*P;

      BN:= [ChangeRing(ColumnSubmatrix(U*ChangeRing(b, Rationals())*UInv, 1, j-1),
             GF(p)): b in B];
      Mod:= RModule(BN);
      S:=  MinimalSubmodules(Mod);

      ok:= false;
      for s in S do
```

```
        if (DFac[i,2] lt 2*Dimension(s)) then continue; end if;
        LN:= VerticalJoin(L,
          ChangeRing(ChangeRing(Morphism(s, Mod), Integers()), Rationals())*U*L/p);
        ok, LN, DLN:= OrderAbove(QA, RowSubmatrix(HNF(LN), m));

        if ok then
          DFac[i, 2] -:= 2* Valuation(DL/DLN, p);
          L:= LN;
          DL:= DLN;
          B:= RegularRepZ(QA`B, L);
          break;
        end if;
      end for;

    until (not ok) or (DFac[i, 2] eq 0);
  end for;

  return L, [d: d in DFac | d[2] ne 0];
end function;

// Prueft, ob die Konjugationsklasse von LM schon bekannt ist. Wenn nicht, so
// wird LM in QA abgespeichert. Im Parameter I kann man das Ideal angeben, als
// dessen Rechtsordnung LM gefunden wurde.
InsertMaxOrder:= procedure(~QA, LM, I)
  G, T:= LLLGram(MG(LM, QA`NQ): Delta:= 0.999);
  Lat:= LatticeWithGram(G);
  KNr:= KissingNumber(Lat);
  OverQ:= #(QA`B) eq 4;

  if OverQ then
    for MO in QA`MaxOrders do
      if (KNr eq KissingNumber(MO`Lat)) and IsIsometric(Lat, MO`Lat) then
        return;
    end if;
    end for;
    AutNr:= #AutomorphismGroup(Lat);
  else
    TTr:= Transpose(T);
    F:= T*MG(LM, QA`Forms[1])*TTr;
    for MO in QA`MaxOrders do
      if (KNr eq KissingNumber(MO`Lat)) then
        if IsIsometric(Lat, [F], MO`Lat, [MO`F]) then return; end if;
        if (assigned MO`Galois) then
          for g in MO`Galois do
            if IsIsometric(Lat, [F], MO`Lat, [g[2]]) then return; end if;
          end for;
        end if;
      end if;
    end for;
    AutNr:= #AutomorphismGroup(Lat, [F]);
```

```
  end if;

  MO:= rec< Type_MaxOrder|
    L:= LM, I:= I, T:= T, Lat:= Lat, AutNr:= AutNr, Checked:= {} >;
  if not OverQ then MO`F:= F; end if;

  if (#(QA`Forms) gt 1) then
    Bahn:= [ <1, F> ];
    for i:= 2 to #(QA`Forms) do
      Fi:= T*MG(LM, QA`Forms[i])*TTr;

      for f in Bahn do
        if (IsIsometric(Lat, [Fi], Lat, [f[2]])) then continue i; end if;
      end for;

      Append(~Bahn, <i, Fi>);
    end for;
    if (#Bahn gt 1) then
      MO`Galois:= Remove(Bahn, 1);
    end if;
  else
    Bahn:= [1];
  end if;

  mass:= 2^(QA`s+1) * KNr * QA`h / AutNr;
  Append(~QA`MaxOrders, MO);
  QA`Found +:= mass * #Bahn;
  printf "#%o: AutNr: %5o, wi1: %3o, Mass: %5o",
    #(QA`MaxOrders), AutNr, KNr/2, mass;
  if (#(QA`Forms) gt 1) then
    printf ", #Bahn: %3o\n", #Bahn;
  else
    print "";
  end if;
  if Done(QA) then print "Fertig!"; end if;
end procedure;

// Ruft PARI auf um die Zetafunktion von K an -1 zu bestimmen.
function gpzetak(K)
  if (Type(K) eq FldRat) then return 1/12; end if;
  P<x>:= PolynomialRing(Integers());
  f:= Sprint(P ! DefiningPolynomial(SimpleExtension(K)));
  str:= "zk = zetak(zetakinit("* f *"), -1); denom = 16!;\n";
  str*:= "zkrat = round(denom*zk)/denom;\n";
  str*:= "print(numerator(zkrat), \" \" denominator(zkrat))";
  zetak:= StringToIntegerSequence(Pipe("gp -q -s 40000000 -p 5000000", str));
  return zetak[1] / zetak[2];
end function;

// Initialisiert die Struktur QA. Hat die Algebra die Basis (1, x2, x3, x2x3)
```

```
// so muessen A,B Rechtsmult. von x2 bzw. x3 auf dieser Basis beschreiben.
// Ao, Bo, beschreiben die Rechtsmult. von \bar{x}2 und \bar{x}3 auf dieser Basis
// Ist OnlyMaxOrder gesetzt, so wird nur eine MO konstruiert, und nicht alle Werte
// der Algebra initialisiert. Depth wird an IsIsometric weitergegeben.
// UseGalois legt fest, ob nur Vertreter der Galoisbahnen gesucht werden,
// oder alle Vertreter von MO.
Init:= function(K, A, B, Ao, Bo:
  OnlyMaxOrder:= false, Depth:= -1, zetak:= 0, UseGalois:= false)

  if (Type(K) eq FldRat) then
    h:= 1;
  else
    K:= AbsoluteField(K);
    h:= ClassNumber(K);
  end if;
  R:= Integers(K);

  if (zetak eq 0) then
    zetak:= gpzetak(K);
    if (zetak eq 0) then
      error "ZetaK(-1) nicht bekannt";
    end if;
  end if;

  n:= AbsoluteDegree(K);
  if (Depth lt 0) then
    if (n le 3) then Depth:= 2;
    elif (n eq 4) then Depth:= 3;
    else Depth:= 4;
    end if;
  end if;

  QA:= rec< Type_QA | K:= K, h:= h, Depth:= Depth,
        Mass:= 2^(1-n) * h * Abs(zetak), Found:= 0,
        MaxOrders:= [], Forms:= [] >;

  QA`B:= Field2Int(K, A, B);
  QA`Bo:= Field2Int(K, Ao, Bo);

  m:= 4*n;
  BxBQ:= [ [bi*qbj: qbj in QB ]: bi in QA`B ]
       where QB:= LinKomb(QA`B, Matrix([b[1]: b in QA`Bo]));

  QA`NQ:=
    Matrix(Rationals(), m, m, [[Trace(BxBQ[i, j])/2: j in [1..m]]: i in [1..m]]);
  QA`T:= Matrix(Rationals(), m, m, [Trace(bi*bj)/2: bj in QA`B, bi in QA`B]);

  Products:= [Vector(K, [1,0,0,0])] cat [Transpose(ChangeRing(X, K))[1] : X in [Ao, Bo, A
  QA`tr:= Matrix(K, 4, 4, [Products[i,j] + Products[j,i]: i,j in [1..4]]);
  if (n gt 1) then
```

```
  QA‘tr:= TensorProduct(QA‘tr, Matrix(K, n, n, [b1*b2: b1, b2 in Basis(R)]));
end if;

LM, D:= FindMaxOrder(QA);

G1:= MG(LM, QA‘T);
Det:= Determinant(G1);

An:= &*[ 32*k^4+80*k^3+70*k^2+25*k+3 : k in [0..n-1]];
QA‘Minkowski:= Floor((2/n)^m / (3 * Pi(RealField())^2)^n * An * Abs(Det)^(1/2));

// Red. Norm der Differenten = Produkt der verzweigten Stellen bestimmen.
if (n eq 1) then
  Disc:= Integers() ! (norm(QA, myDualR(QA, LM))^-1);
else
  Disc:= norm(QA, myDualR(QA, LM));
end if;
Fac:= Factorization(Disc);

error if exists{p: p in Fac | Abs(p[2]) ne 1}, "Ordnung nicht maximal!";
QA‘Places:= [p[1]: p in Fac];
QA‘PlacesZ:= (n eq 1) select Seqset(QA‘Places)
  else { Abs(Generator(p meet Integers())) : p in QA‘Places };
QA‘s:= #QA‘Places;

if (n gt 1) then
  M1:= ScalarMatrix(Rationals(), 4, 1);
  alpha:= R ! PrimitiveElement(K);
  Lalpha:= TensorProduct(M1, RepresentationMatrix(alpha, Rationals()));
  F:= Matrix(Rationals(), m, m,
    [ [Trace(Lalpha*BxBQ[i, j])/2: j in [1..m] ]: i in [1..m]]);
  Append(~(QA‘Forms), F);

  UseGalois:= UseGalois and IsNormal(K) and forall{p: p in QA‘PlacesZ |
      [f[1]: f in Factorization(p*R)] subset QA‘Places};

  if UseGalois then
    QA‘Galois:= [ ScalarMatrix(Rationals(), m, 1) ];
    for a in [ a: a in Automorphisms(K) | a(alpha) ne alpha ] do
      sigma:= TensorProduct(M1,
        Matrix(Rationals(), n, n, [Eltseq(R ! a(r)): r in Basis(R)]));
      Append(~QA‘Galois, sigma);
      Lalpha:= TensorProduct(M1, RepresentationMatrix(R!(a(alpha)), Rationals()));
      F:= Matrix(Rationals(), m, m,
        [ [Trace(Lalpha*BxBQ[i, j]/2): j in [1..m] ]: i in [1..m]]);
      Append(~(QA‘Forms), F);
    end for;
  end if;
end if;
```

```
  if (QA‘s gt 0) then
    QA‘Mass *:= &*[Norm(p)-1 : p in QA‘Places];
  end if;

  print "verzweigte Stellen: ", QA‘Places;
  print "Stellen ueber Z:=", QA‘PlacesZ;
  print "s:=", QA‘s;
  print "Mass:=", QA‘Mass;

  if not OnlyMaxOrder then
  // erste Maximalordnung einfuegen
    InsertMaxOrder(~QA, LM, LM);
  end if;

  return QA, LM;
end function;

// Liefert QA = ((a,b)/K) f"ur a, b total definit. Die Parameter sind wie oben.
Initab:= function(K, a, b:
  OnlyMaxOrder:= false, zetak:= 0, Depth:= -1, UseGalois:= -1)

  error if not IsTotallyPositive(K ! -a), "-a ist nicht total positiv!";
  error if not IsTotallyPositive(K ! -b), "-b ist nicht total positiv!";

  K4x4:= MatrixRing(K, 4);
  A  := K4x4 ! [0, 1, 0,0,     a,0,0,0,    0,0,0,-1,0,0,-a,0];
  B  := K4x4 ! [0, 0, 1,0,     0,0,0,1,    b,0,0, 0,0,b, 0,0];
  Ao:= K4x4 ! [0,-1, 0,0,    -a,0,0,0,    0,0,0,-1,    0,0,-a,0];
  Bo:= K4x4 ! [0, 0,-1,0,     0,0,0,1,   -b,0,0, 0,    0,b, 0,0];

  if (UseGalois cmpeq -1) then
    UseGalois:= (a in Rationals()) and (b in Rationals());
  end if;
  QA, LM:= Init(K, A, B, Ao, Bo: OnlyMaxOrder:= OnlyMaxOrder,
    zetak:= zetak, Depth:= Depth, UseGalois:= UseGalois);
  QA‘a:= K!a; QA‘b:= K!b;
  QA‘Names:= ["i", "j", "k"];

  return QA, LM;
end function;

// Liefert die n-te zyklotomische QA. Die Parameter sind wie oben.
InitCyclo:= function(n:
  OnlyMaxOrder:= false, zetak:= 0, Depth:= -1, UseGalois:= false)

  error if (n le 2), "n muss groesser als 2 sein.";
  case n:
    when 3: K:= Rationals(); s:= 1;
    when 4: K:= Rationals(); s:= 0;
    when 6: K:= Rationals(); s:= 1;
```

```
    else
      C<z>:= CyclotomicField(n);
      K:= NumberField(MinimalPolynomial(z+z^-1));
      AssignNames(~K, ["theta_"*IntegerToString(n)]);
      s:= K.1;
  end case;

  K4x4:= MatrixRing(K, 4);
  A  := K4x4 ! [0, 1, 0,0,  -1,s, 0,0,   0,0,s,-1,   0, 0,1,0];
  B  := K4x4 ! [0, 0, 1,0,   0,0, 0,1,  -1,0,0, 0,   0,-1,0,0];
  Ao:= K4x4 ! [s,-1, 0,0,   1,0, 0,0,   0,0,s,-1,   0, 0,1,0];
  Bo:= K4x4 ! [0, 0,-1,0,   0,0,-s,1,   1,0,0, 0,   s,-1,0,0];
  QA, LM:= Init(K, A, B, Ao, Bo: OnlyMaxOrder:= OnlyMaxOrder,
    zetak:= zetak, Depth:= Depth, UseGalois:= UseGalois);
  QA`Names:= ["zeta_"*IntegerToString(n), "x", "zeta_"*IntegerToString(n)*"x"];
  return QA, LM;
end function;

/* Routinen zur Ausgabe */
ReverseColumns:= function(X)
  n:= Ncols(X);
  for i:= 1 to n div 2 do
    SwapColumns(~X, i, n+1-i);
  end for;
  return X;
end function;

ReverseRows:= function(X)
  n:= Nrows(X);
  for i:= 1 to n div 2 do
    SwapRows(~X, i, n+1-i);
  end for;
  return X;
end function;

// wandelt L in untere Dreiecksmatrix
Beautify:= function(L)
  denom:= MatrixDenom(L);
  L:= ChangeRing(ReverseColumns(L)*denom, Integers());
  return 1/denom * ReverseRows(ReverseColumns(EchelonForm(L)));
end function;

// Wandelt das Gitter L in einen R-Modul
LatToModule:= function(QA, L)
  m:= Ncols(L);
  R:= Integers(QA`K);
  if (Type(QA`K) eq FldRat) then
    L:= Beautify(L);
    PB:= [];
    for i:= 1 to 4 do
```

```
      denom:= MatrixDenom(L[i]);
      v:= denom*L[i];
      num:= GCD(Eltseq(ChangeRing(v, Integers())));
      Append(~PB, <num/denom, ChangeRing(v/num, Integers())>);
    end for;
    return PB;
  end if;
  denom:= MatrixDenom(L);
  L:= ChangeRing(denom*L, Integers());
  // Elemente als Elemente ueber R interpretieren
  LR:= Matrix(4, ChangeUniverse(Partition(Eltseq(L), m div 4), R));
  M:= sub<Module(R, 4) | [ Eltseq(LR[i]): i in [1..m] ] >;
  PB:= PseudoBasis(M);
  for i:= 1 to #PB do
    PB[i,1]:= 1/denom * PB[i,1];
  end for;
  return PB, M;
end function;

OneElement:= function(S)
  S:= Eltseq(S);
  nonzero:= false;
  for i:= 1 to #S do
    if (S[i] ne 0) then
      if nonzero then
        return false;
      else
        nonzero:= true;
      end if;
     end if;
  end for;
  return true;
end function;

// gibt ein R-Erzeugendensystem des R-Gitters L aus
PrintLat:= procedure(QA, L)
  Names:= ["1"] cat
    (assigned QA`Names select QA`Names else ["$.1", "$.2", "$.3"]);

  R:= Integers(QA`K);
  PB:= LatToModule(QA, L);
  n:= #PB;

  printf "< ";
  for i:= 1 to n do
    if (Type(QA`K) eq FldRat) then
      gens:= [PB[i,1]];
    else
      ok, x:= IsPrincipal(PB[i,1]);
      gens:= ok select [x] else Generators(PB[i,1]);
```

```
    end if;
    for j:= 1 to #gens do
      if IsIntegral(gens[j]) and IsIntegral(gens[j]^-1) then
        scalar:= 1;
      else
        scalar:= QA‘K ! gens[j];
      end if;
      if  (scalar ne 1) then
        if (OneElement(scalar)) then
          printf "%o*", scalar;
        else
          printf "(%o)*", scalar;
        end if;
      end if;
      needbraces:= not OneElement(PB[i,2]) and (scalar ne 1);
      if needbraces then printf "("; end if;
      first:= true;
      for k:= 1 to 4 do
        scalar:= QA‘K ! PB[i, 2, k];
        if scalar ne 0 then
          if first then
            first:= false;
          else
            printf "+";
          end if;
          case scalar:
            when  1: printf  "%o", Names[k];
            when -1: printf "-%o", Names[k];
            else
              if OneElement(scalar) then
                printf "%o", scalar;
                if (k ne 1) then printf "*%o", Names[k]; end if;
              else
                printf "(%o)", scalar;
                if (k ne 1) then printf "*%o", Names[k]; end if;
              end if;
          end case;
        end if;
      end for;
      if needbraces then printf ")"; end if;
      if (i ne n) or (j ne #gens) then
        print ", ";
      end if;
    end for;
  end for;
  print " >";
end procedure;

// Fuer eine R-Maximalordnung LM und eine Primzahl p werden die Linksordnungen
// der LM-Rechtsmoduln von LM/pLM durchsucht.  Die gefundenen R-Ordnungen
```

```
// werden in QA abgespeichert und die Wert von QA‘Found wird angepasst.
FindMaxOrders:= procedure(~QA, k, p)
  if Done(QA) or (p in QA‘MaxOrders[k]‘Checked) then return; end if;

  LM:= QA‘MaxOrders[k]‘L;
  BM:= RegularRepZ(QA‘B, LM);
  M:= MatrixRing(Integers(), #BM);

  Mod:= RModule(ChangeRing(sub<M | BM>, GF(p)));
  S:= MaximalSubmodules(Mod);
  printf "k = %2o, p = %3o, #Teilmoduln: %-5o\n", k, p, #S;
  for s in S do
    I:= MorphismToMatrix(Morphism(s, Mod), p)*LM;
    LOrder:= LO(QA, I);
    InsertMaxOrder(~QA, LOrder, I);
    if Done(QA) then break; end if;
  end for;
  Include(~QA‘MaxOrders[k]‘Checked, p);
end procedure;

// Der erste Rueckgabewert ist eine Liste mit Primzahlen so, dass die
// darueberliegenden Primideale von R die Strahlklassengruppe von K erzeugen.
// Fuer jede PZ p <= Bound bestimmt die Fkt. danach den Index [MO:pMO], dabei
// sei MO eine bel. Maximalordnung von QA. Der 2. Rueckgabewert ist eine Liste
// von Paaren <[MO:pMO], p>, sortiert nach den Indizes.
// Damit kann man Abschaetzen, wielange FindMaxOrders(QA, _, p) benoetigt.
ListPrimes:= function(QA, Bound: RayClass:= true)
  R:= Integers(QA‘K);
  RayClassPrimes:= {};
  if (Type(QA‘K) ne FldRat) and RayClass then
    g, m:= RayClassGroup(1*R, [1..AbsoluteDegree(QA‘K)]);
    minv:= m^-1;
    for gen in Generators(g) do
      Fac:= Factorization(m(gen));
      for f in Fac do
        if minv(f[1]) eq gen then
          Include(~RayClassPrimes, Generator(f[1] meet Integers()));
          continue gen;
        end if;
      end for;
      for f in Fac do
        Include(~RayClassPrimes, Generator(f[1] meet Integers()));
      end for;
    end for;
  end if;

  p:= 2;
  primes:= [];
  while (p le Bound) do
    if (Type(QA‘K) eq FldRat) then
```

```
      Append(~primes, <p+1, p>);
    else
      Fac:= Factorization(p*R);
      Append(~primes, < &+[1+Norm(d[1]): d in Fac], p>);
    end if;
    p:= NextPrime(p);
  end while;
  Sort(~primes);
  return RayClassPrimes, primes;
end function;


// Sucht alle Klassen von R-Maximalordnungen, indem es den vorherigen Algorithmus
// fuer alle Primzahlen und schon gefundene Klassen anwendet.
FindAllMaxOrders:= procedure(~QA: Bound:= 0, primes:= [], RayClass:= true)
  RayClassPrimes:= {};
  if primes eq [] then
    if Bound eq 0 then Bound:= Min(500, QA`Minkowski); end if;
    RayClassPrimes, primes:= ListPrimes(QA, Bound: RayClass:= RayClass);
  else
    primes:= [ <0, p>: p in primes ];
  end if;

  for p in RayClassPrimes do
    FindMaxOrders(~QA, 1, p);
    if Done(QA) then return; end if;
  end for;

  j:= 1;
  while (j le #primes) do
    p:= primes[j, 2];
    T:= #QA`MaxOrders;
    for i:= 1 to T do
      FindMaxOrders(~QA, i, p);
      if Done(QA) then return; end if;
      if (T ne #QA`MaxOrders) then
        j:= 0;
        break;
      end if;
    end for;
    j +:= 1;
  end while;
end procedure;


// Testet, ob das Z-Gitter L eine R-Ordnung ist. Dazu wird geprueft, ob L
// einen Ring von ganzen Elementen erzeugt der R enthaelt.
IsROrder:= function(QA, L)
  if (Determinant(L) eq 0) then return false; end if;
  M:= MatrixRing(Integers(), #QA`B);
```

```
  R:= Integers(QA‘K);
  Y:= RegularRep(QA‘B, L);
  for i:= 1 to #QA‘B do
    if (Y[i] notin M) or (normx(QA, L[i]) notin R)
      or (tracex(QA, L[i]) notin R) then
        return false;
    end if;
  end for;
  denom:= MatrixDenom(L);

  // liegt R im Z-Gitter L ?
  M1:= M ! denom;
  L:= ChangeRing(L*denom, Integers());
  for i:= 1 to (#QA‘B div 4) do
    if not IsConsistent(L, M1[i]) then return false; end if;
  end for;
  return true;
end function;


// Testet, ob das Z-Gitter L eine R-Maximalordnung ist.
IsMaximalROrder:= func<QA, L |
  IsROrder(QA, L) and (Determinant(L) eq Determinant(QA‘MaxOrders[1]‘L)) >;


// Testet, on das Z-Gitter L ein normales R-Gitter ist.
IsNormalLat:= func<QA, L |
  (Determinant(L) ne 0) and IsMaximalROrder(QA, LO(QA,L)) >;

//Testet, ob die beiden R-Ordnungen L1 und L2 konjugiert sind.
ConjugateROrders:= function(QA, L1, L2)
  G1, T1:= LLLGram(MG(L1, QA‘NQ): Delta:= 0.999);
  G2, T2:= LLLGram(MG(L2, QA‘NQ): Delta:= 0.999);
  Forms1:= [G1];
  Forms2:= [G2];

  if (#(QA‘B) ne 4) then
    Append(~Forms1, T1*MG(L1, QA‘Forms[1])*Transpose(T1));
    Append(~Forms2, T2*MG(L2, QA‘Forms[1])*Transpose(T2));
  end if;

  return IsIsometric(Forms1, Forms2);
end function;

// Testet, ob B eine regulaere Darstellung ist.
IsRegular:= function(B)
  ok:= forall(t){<i,j>: i,j in [1..#B] | B[j]*B[i] eq LinKomb(B, Matrix(B[i,j]))};
  if ok then
    return true, _;
  else
```

```
    return false, t;
  end if;
end function;

forward IsPrincipalIdealQ;

// Testet, ob ein Gitter L ein Hauptideal ist. Ist die RO bekannt kann sie mit
// angegeben werden.  In norm1 koennen, falls bekannt, die Elemente der RO mit
// red. Norm 1 angegeben werden. Von einem Paar (x, -x) sollte aber nur eines
// in norm1 stehen!
IsPrincipalIdeal:= function(QA, L: LRO:= 0, norm1:= [])
  n:= AbsoluteDegree(QA`K);
  if (n eq 1) then
    return IsPrincipalIdealQ(QA, L: LRO:= LRO, norm1:= norm1);
  end if;

  L:= ChangeRing(L, Rationals());
  G, T:= LLLGram(MGQ(L, QA`NQ));

  ok, normI:= IsPrincipal(norm(QA, L));
  if (not ok) then return false, _, _; end if;
  ok, normes:= MakeTotallyPositive(normI);
  if (not ok) then return false, _, _; end if;

  if (LRO eq 0) then LRO:= RO(QA, L); end if;
  if norm1 eq [] then norm1:= Listnorm1(QA, LRO: all:= false); end if;
  U, map:= UnitGroup(QA`K);
  Rnorm1:= [ map(U.i): i in [2..n] ];
  M:= MatrixRing(Integers(), 4*n);
  LInv:= L^-1;

  touched:= {};
  normtouched:= {};
  for i:= 1 to #normes do
    nr:= normes[i];
    // Spur zuerst reduzieren
    minTrace:= Trace(nr);
    for unit in Rnorm1 do
      for exp in [2, -2] do
        unitdir:= unit^exp;

        flag:= false;
        x:= nr*unitdir;
        newTrace:= Trace(x);
        while newTrace lt minTrace do
          flag:= true;
          nr:= x;
          minTrace:= newTrace;
          x*:= unitdir;
          newTrace:= Trace(x);
```

```
        end while;
        if flag then break; end if;
      end for;
    end for;

    if (minTrace notin normtouched) then
      Include(~normtouched, minTrace);
      minTrace *:= 2;
      SV:= [s[1]: s in ShortVectors(LatticeWithGram(G), minTrace, minTrace)];
      // Vektoren bzgl. Standardbasis schreiben:
      SV:= [Vector(Rationals(), s)*TL: s in SV]
          where TL:= ChangeRing(T, Rationals())*L;

      for s in SV do
        if (s in touched) or (-s in touched) then continue; end if;
        X:= ProductxI(QA, s, LRO)*LInv;
        if ((X in M) and (Abs(Determinant(X)) eq 1)) then
          return true, s, LRO;
        end if;
        touched join:= {Productxy(QA, s, u): u in norm1};
      end for;
    end if;
  end for;
  return false, _, _;
end function;

// dasselbe ueber Q, da ist alles einfacher
IsPrincipalIdealQ:= function(QA, L: LRO:= 0, norm1:= [])
  if (#(QA`B) ne 4) then
    return IsPrincipalIdeal(QA, L: LRO:= LRO, norm1:= norm1);
  end if;

  if (LRO eq 0) then LRO:= RO(QA, L); end if;

  if norm1 eq [] then norm1:= Listnorm1(QA, LRO: all:= false); end if;

  L:= ChangeRing(L, Rationals());
  G, T:= LLLGram(MGQ(L, QA`NQ));
  M:= MatrixRing(Integers(), 4);
  LInv:= L^-1;
  touched := {};

  SV:= ShortestVectors(LatticeWithGram(G));
  SV:= [Vector(Rationals(), s)*TL: s in SV]
      where TL:= ChangeRing(T, Rationals())*L;
  for s in SV do
    if (s in touched) or (-s in touched) then continue; end if;
    X:= ProductxI(QA, s, LRO)*LInv;
    if ((X in M) and (Abs(Determinant(X)) eq 1)) then
      return true, s, LRO;
```

```
    end if;
    touched join:= { Productxy(QA, s, u): u in norm1 };
  end for;
  return false, _, _;
end function;

// Hilfsfunktion. Prueft, ob L zu einem der I mit I^-1 in Inverses konjugiert
// ist. Falls bekannt, so koennen LRO und norm1 wieder angegeben werden.
IsInList:= function(QA, L, Inverses: LRO:=0, norm1:= [])
  for I in Inverses do
    if IsPrincipalIdeal(QA, Product(QA, I, L): LRO:= LRO, norm1:= norm1) then
      return true;
    end if;
  end for;
  return false;
end function;

// Findet die Klassen zweiseitiger LM-Ideale, indem alle max. Rechtsideale
// zwischen pLM und LM fuer die PZ in QA‘PlacesZ untersucht werden.
ListIdealClasses2:= function(QA, LM)
  M:= MatrixRing(Integers(), #QA‘B);
  B:= RegularRepZ(QA‘B, LM);
  norm1:= Listnorm1(QA, LM: all:= false);

  list:= [ LM ];
  inverses:= [ LM ];
  LMInv:= LM^-1;
  for p in QA‘PlacesZ do

    Mod:= RModule(ChangeRing(sub<M | B>, GF(p)));
    S:= MaximalSubmodules(Mod);
    for s in S do
      L:= MorphismToMatrix(Morphism(s, Mod), p)*LM;

      // Ist L ein zweiseitiges Ideal einer neuen Klasse?
      X:= LO(QA, L) * LMInv;
      if ( (X in M) and (Abs(Determinant(X)) eq 1) and
           not IsInList(QA, L, inverses: LRO:= LM, norm1:= norm1) ) then

        size:= #list;
        Append(~list, L);
        Append(~inverses, Inv(QA, L: LRO:= LM));
        for i:= 2 to size do
          X:= Product(QA, list[i], L);
          if (not IsInList(QA, X, inverses: LRO:= LM, norm1:= norm1)) then
            Append(~list, X);
            Append(~inverses, Inv(QA, X: LRO:= LM));
          end if;
        end for;
```

```
      end if;
    end for;
  end for;

  if (QA`h eq 1) then return list; end if;

  G, map:= ClassGroup(QA`K);
  RIdeals:= [BasisMatrix(map(g)): g in G | g ne Id(G)];

  size:= #list;
  for i:= 1 to size do
    for a in RIdeals do
      X := Product(QA, list[i], a);
      if (not IsInList(QA, X, inverses: LRO:= LM, norm1:= norm1)) then
        Append(~list, X);
        Append(~inverses, Inv(QA, X : LRO:= LM));
      end if;
    end for;
  end for;
  return list;
end function;

// wie oben, nur diesmal werden die max. LM-Rechtsideale zwischen pLM und
// LM fuer die in QA verzweigen Primideale p von R durchsucht. Das ist
// schneller, wenn QA keine gleichmaessig verteilten Invarianten hat.
ListIdealClasses:= function(QA, LM)
  if Type(QA`K) eq FldRat then return ListIdealClasses2(QA, LM); end if;
  norm1:= Listnorm1(QA, LM: all:= false);
  list:= [ LM ];
  inverses:= [ LM ];
  LMInv:= LM^-1;
  for PI in QA`Places do
    p:= Abs(Generator(PI meet Integers()));
    L:= Product(QA, LM, BasisMatrix(PI));
    m:= #QA`B;
    S, P, Q:= SmithForm(ChangeRing(L*LMInv, Integers()));
    i:= 1;
    while (S[i,i] eq 1) do i +:= 1; end while;
    M:= MatrixRing(Integers(), m-i+1);
    QInvLM:= Q^-1 * LM;
    B:= RegularRepZ(QA`B, QInvLM);
    Y:= [ SubmatrixRange(B[j], i,i,m,m): j in [i..m] ];
    Mod:= RModule(ChangeRing(sub<M | Y>, GF(p)));
    S:= MaximalSubmodules(Mod);
    error if #S ne 1, "Fehler in ListIdealClasses()";
    L:= MorphismToMatrix(Morphism(S[1], Mod), p);
    L:= DiagonalJoin(MatrixRing(Rationals(), i-1) ! 1, L) * QInvLM;

    if ( not IsInList(QA, L, inverses: LRO:= LM, norm1:= norm1) ) then
      size:= #list;
```

```
      Append(~list, L);
      Append(~inverses, Inv(QA, L: LRO:= LM));
      for i:= 2 to size do
        X:= Product(QA, list[i], L);
        if (not IsInList(QA, X, inverses: LRO:= LM, norm1:= norm1)) then
          Append(~list, X);
          Append(~inverses, Inv(QA, X: LRO:= LM));
        end if;
      end for;
    end if;
  end for;

  if (QA`h eq 1) then return list; end if;

  G, map:= ClassGroup(QA`K);
  RIdeals:= [BasisMatrix(map(g)): g in G | g ne Id(G)];

  size:= #list;
  for i:= 1 to size do
    for a in RIdeals do
      X := Product(QA, list[i], a);
      if (not IsInList(QA, X, inverses: LRO:= LM, norm1:= norm1)) then
        Append(~list, X);
        Append(~inverses, Inv(QA, X : LRO:= LM));
      end if;
    end for;
  end for;
  return list;
end function;

// Findet die Gruppe der zweiseitigen Idealklassen von L
IdealClassGroup:= function(QA, L: list:= [])
  norm1:= Listnorm1(QA, L: all:= false);
  tmpMult:= func<X, Y | Product(QA, X, Y)>;
  tmpEq:= func<X, Y | IsPrincipalIdeal(QA, Product(QA, X,
      Inv(QA, Y: LRO:= L)): LRO:= L, norm1:= norm1) >;
  if (list eq []) then list:= ListIdealClasses(QA, L); end if;
  g, m:= GenericGroup( list : Mult:= tmpMult, Eq:= tmpEq, Id:= L );

  mi:= m^-1;
  pairing:= [ <l, mi(l)>: l in Codomain(m) ];
  minv:= function(I)
    IInv:= Inv(QA, I: LRO:= L);
    for p in pairing do
      if IsPrincipalIdeal(QA, Product(QA, p[1], IInv): LRO:= L, norm1:= norm1) then
        return p[2];
      end if;
    end for;
  end function;
  return g, m, minv;
```

```
end function;

// Rechts- bzw. Linksidealklassen eines normalen Ideals.
ListRightIdealClasses:= function(QA, L)
  MOs:= ListMaxOrders(QA: all:= true);
  return [ Product(QA, l2, L): l2 in ListIdealClasses(QA, MO), MO in MOs ];
end function;

ListLeftIdealClasses:= function(QA, L)
  MOs:= ListMaxOrders(QA: all:= true);
  return [ Product(QA, L, l2): l2 in ListIdealClasses(QA, MO), MO in MOs ];
end function;

// Bestimmt die Klasse der stabil aequivalenten Rechtsideale von LM
StableIdealClassGroup:= function(QA, LM: right:= true)
  if (Type(QA`K) eq FldRat) then
    G:= CyclicGroup(1);
    return G, map<G->[LM] | Id(G)->LM>, func<L|Id(G)>;
  end if;

  G, map:= RayClassGroup(1*Integers(QA`K), [1..AbsoluteDegree(QA`K)]);
  mapinv:= map^-1;
  if right then
    IdlClasses:= ListRightIdealClasses(QA, LM);
  else
    IdlClasses:= ListLeftIdealClasses(QA, LM);
  end if;

  inverse:= function(L)
    nrm:= norm(QA, L);
    return mapinv(Denominator(nrm)^2 * nrm);
  end function;

  mapping:= [];
  for I in IdlClasses do
    g:= inverse(I);
    for x in mapping do
      if x[1] eq g then continue I; end if;
    end for;
    Append(~mapping, <g, I>);
  end for;
  return G, map<G->{x[2]: x in mapping} | mapping>, inverse;
end function;

// Gibt alle Invarianten einer Maximalordnung aus. Ist der 2. Parameter eine
// ganze Zahl k, so wir die k-te schon bestimmte MO in QA untersucht.
// Andernfalls die im 2. Paramter uebergebene Maximalordnung.
PrintInfo:= procedure(QA, LM)
  Bahn:= 0;
  if (Type(LM) ne RngIntElt) then
```

```
    G, T:= LLLGram(MG(LM, QA‘NQ): Delta:= 0.999);
    Lat:= LatticeWithGram(G);

    KNr:= KissingNumber(Lat);
    if (#(QA‘B) eq 4) then
      AutNr:= #AutomorphismGroup(Lat);
    else
      TTr:= Transpose(T);
      F:= T*MG(LM, QA‘Forms[1])*TTr;
      AutNr:= #AutomorphismGroup(Lat, [F]);
      if (#(QA‘Forms) gt 1) then
        Bahn:= [ F ];
        for i:= 2 to #(QA‘Forms) do
          Fi:= T*MG(LM, QA‘Forms[i])*TTr;
          for f in Bahn do
            if (IsIsometric(Lat, [Fi], Lat, [f])) then continue i; end if;
          end for;
          Append(~Bahn, Fi);
        end for;
        Bahn:= #Bahn;
      end if;
    end if;
  else
    AutNr:= QA‘MaxOrders[LM]‘AutNr;
    KNr:= KissingNumber(QA‘MaxOrders[LM]‘Lat);
    if assigned QA‘MaxOrders[LM]‘Galois then
      Bahn:= 1+#QA‘MaxOrders[LM]‘Galois;
    end if;
    LM:= QA‘MaxOrders[LM]‘L;
  end if;

  wi1:= KNr/2;

  Hi:= #ListIdealClasses(QA, LM);
  wi:= AutNr * Hi / (QA‘h * 2^(QA‘s+2)*wi1);

  printf "AutNr: %5o, wi1: %3o, winq: %3o, Hi: %3o",
    AutNr, wi1, wi/wi1, Hi;
  if Bahn eq 0 then
    print "";
  else
    printf ", Galoisbahnenlaenge: %3o\n", Bahn;
  end if;
end procedure;
```

Des weiteren wird die Datei „sigfield“ benötigt:

```
// Signatur-Funktionen fuer total-reelle Zahlkoerper

intrinsic Conjugates(x::FldRatElt) -> ModTupFldElt
```

```
  { Liefert einen Vektor mit den Galoiskonjugierten von x, also [x]. }
  return [x];
end intrinsic;

intrinsic Signature(x::FldElt) -> ModTupFldElt
  { Liefert die Vorzeichen aller reellen Galoiskonjugierten von x als Vektor "uber F_2. }

  K:= Parent(x);
  require (Type(K) eq FldRat) or ISA(Type(K), FldAlg):
    "Element liegt nicht in einem Zahlkoerper";
  if (Type(K) ne FldRat) then K:= AbsoluteField(K); end if;
  r, s:= Signature(K);
  require (s eq 0): "Grundkoerper nicht total-reell";
  return Vector(GF(2), [(1-Sign(Real(c))) div 2 : c in Conjugates(K ! x)]);
end intrinsic;

intrinsic IsTotallyPositive(x::FldElt) -> BoolElt
  { Liefert genau dann true, wenn x total positiv ist. }

  return IsZero(Signature(x));
end intrinsic;


intrinsic SignatureMatrix(K::Fld) -> AlgMatElt
  { Liefert die Signaturen der Erzeuger von Z_K^* und die Erzeuger von Z_K^*. }

  require (Type(K) eq FldRat) or ISA(Type(K), FldAlg):
    "Koerper muss ein Zahlkoerper sein";
  U, map:= UnitGroup(Integers(K));
  Units:= [map(u): u in Generators(U)];
  return Matrix([Signature(u): u in Units]), Units;
end intrinsic;

intrinsic UnitWithSignature(K::Fld, sig::ModTupFldElt) -> BoolElt, SeqEnum
  { Liefert genau dann true, falls es eine Einheit von Z_K gibt, die
    den Signaturvektor sig besitzt. Ist dies der Fall, so ist der zweite
    Parameter eine Liste aller dieser Einheiten modulo (Z_K^*)^2. }

  S, Units:= SignatureMatrix(K);
  ok, x, V:= IsConsistent(S, sig);
  if ok then
    V:= [x+v: v in V];
    return true, [ &*([K | Units[i]: i in [1..#Units] | v[i] ne 0]): v in V ];
  else
    return false, _;
  end if;
end intrinsic;

intrinsic MakeTotallyPositive(x::FldElt) -> BoolElt, SeqEnum
  { Prueft, ob eine Einheit u von Z_K gibt mit x*u total-positiv. Ist dies der
```

```
    Fall, so liefert der zweite Rueckgabewert eine Liste aller total positiven
    Erzeuger von x*Z_K (modulo (Z_K^*)^2). }

  P:= Parent(x);
  if (Type(P) eq FldRat) then
    return true, [Sign(x)*x];
  end if;
  ok, U:= UnitWithSignature(P, Signature(x));
  if ok then
    return true, [x*u: u in U];
  else
    return false, _;
  end if;
end intrinsic;

// dasselbe fuer die Maximalordnungen

intrinsic Conjugates(x::RngIntElt) -> ModTupFldElt
  {}
  return [x];
end intrinsic;

intrinsic Signature(x::RngElt) -> ModTupFldElt
  {}
  return Signature(FieldOfFractions(Parent(x)) ! x);
end intrinsic;

intrinsic IsTotallyPositive(x::RngElt) -> BoolElt
  {}
  return IsZero(Signature(x));
end intrinsic;

intrinsic SignatureMatrix(R::Rng) -> AlgMatElt
  {}
  return SignatureMatrix(FieldOfFractions(R));
end intrinsic;

intrinsic UnitWithSignature(R::Rng, sig::ModTupFldElt) -> BoolElt, SeqEnum
  {}
  ok, U:= UnitWithSignature(FieldOfFractions(R), sig);
  if ok then
    return true, ChangeUniverse(U, R);
  end if;
  return false, _;
end intrinsic;

intrinsic MakeTotallyPositive(x::RngElt) -> BoolElt, SeqEnum
  {}
  R:= Parent(x);
  ok, U:= MakeTotallyPositive(FieldOfFractions(R) ! x);
```

```
  if ok then
    return true, ChangeUniverse(U, R);
  end if;
  return false, _;
end intrinsic;
```

Anhang B

Anhang: Beispiele

B.1 Total definite Quaternionenalgebren der Form $\left(\frac{a,b}{K}\right)$

Nachfolgend sind die Konjugationsklassen der Quaternionenalgebren von [Neb98, S. 15-16] aufgelistet. Alle diese Quaternionenalgebren $\mathfrak{D}$ sind total definit und $Z(\mathfrak{D})/\mathbb{Q}$ ist galoisch. Weiter besitzen alle $\mathfrak{D}$ gleichmäßig verteilte Invarianten.

Jede Quaternionenalgebra $\mathfrak{D}$ ist in einem eigenen Block aufgelistet. Dessen erste Zeile beschreibt die Algebra $\mathfrak{D}$. Die erste Spalte dieser Zeile besitzt folgenden Aufbau: $\alpha, \infty, p_1, \ldots, p_l$. Dabei ist $K = \mathbb{Q}(\alpha)$. Weiter sind die Primideale von R über den einzelnen $p_i\mathbb{Z}$ gerade die in $\mathfrak{D}$ verzweigten Primideale. Die nächste Spalte enthält eine konkrete Realisierung von $\mathfrak{D}$ als $\mathfrak{D} = \left(\frac{a,b}{K}\right)$. Die letzte Spalte enthält die Summe der Eichlermaße aller Konjugationsklassen von R-Maximalordnungen.
Die nachfolgenden Zeilen enthalten Vetreter $\mathfrak{M}_1, \ldots, \mathfrak{M}_T$ der Konjugationsklassen von R-Maximalordnungen. Die i-te dieser Zeilen ist folgendermaßen aufgebaut: Die erste Spalte enthält ein Paar (k, p). Das bedeutet, $\mathfrak{M}_i$ wurde als Linksordnung eines maximal ganzen $\mathfrak{M}_k$-Rechtsideals I mit $p\mathfrak{M}_k \subset I \subset \mathfrak{M}_k$ gefunden. Für $\mathfrak{M}_1$ ist der Eintrag leer. Die zweite Spalte enthält ein R-Erzeugendensystem von $\mathfrak{M}_i$ und die letzte Spalte das Eichlermaß der Konjugationsklasse von $\mathfrak{M}_i$ in der Form $(\omega_i^1 \cdot \omega_i^{nq})^{-1} \cdot H_i$ wie in Abschnitt 4.1 beschrieben.

Wie in [Neb98, S. 16] bezeichne ζ_n eine primitive n-te Einheitswurzel in $\mathbb{C}$ und $\theta_n := \zeta_n + \zeta_n^{-1}$. Sei L ein Teilkörper von $\mathbb{Q}(\theta_n)$ mit $G := \mathrm{Gal}(\mathbb{Q}[\zeta_n]/L)$. Ist L der einzige Teilkörper von $\mathbb{Q}(\theta_n)$ mit $\mathrm{Gal}(L/\mathbb{Q}) \cong C_3$, so bezeichnet $\omega_n := \sum_{g\in G} g(\zeta_n)$. Dies ist ein primitives Element von L. Ist L der einzige Teilkörper von $\mathbb{Q}(\theta_n)$ mit $\mathrm{Gal}(\mathbb{Q}(\theta_n)/L) \cong C_4$ respektive C_5, so bezeichnet η_n (respektive σ_n) das primitive Element $\sum_{g\in G} g(\zeta_n)$ von L.

Falls $\mathfrak{D} = \left(\frac{a,b}{K}\right)$ mit $a, b \in \mathbb{Q}$ gilt, so sind lediglich Vertreter der Galoisbahnen angegeben, da man daraus alle Konjugationsklassen von R-Maximalordnungen konstruieren kann (vgl. Bemerkung 4.2.5). Ist die Bahnenlänge eines Vertreters gleich m, so ist dies in der letzen Spalte durch ein vorangestelltes $m*$ kenntlich gemacht.

Alle aufgelisteten Beispiele in diesem Abschnitt konnten auf meinen Notebook (Pentium 4 mit 2,8GHz und 512 MB RAM) in jeweils unter einer Minute bearbeitet werden.

$K = \mathbb{Q}$:

2	$a = b = -1$	$\frac{1}{12}$
	$\langle 1, \mathbf{i}, \mathbf{j}, \frac{1}{2}(1+\mathbf{i}+\mathbf{j}+\mathbf{k})\rangle$	$(12\cdot 1)^{-1}\cdot 1$
3	$a = -1,\ b = -3$	$\frac{1}{6}$
	$\langle 1, \mathbf{i}, \frac{1}{2}(\mathbf{i}+\mathbf{j}), \frac{1}{2}(1+\mathbf{k})\rangle$	$(6\cdot 1)^{-1}\cdot 1$
5	$a = -2,\ b = -5$	$\frac{1}{3}$
	$\langle 1, \mathbf{i}, \frac{1}{2}(1+\mathbf{i}+\mathbf{j}), \frac{1}{4}(2+3\mathbf{i}+\mathbf{k})\rangle$	$(3\cdot 1)^{-1}\cdot 1$
2, 3, 5	$a = -3,\ b = -10$	$\frac{2}{3}$
	$\langle 1, \frac{1}{2}1(1+\mathbf{i}), \mathbf{j}, \frac{1}{2}(\mathbf{j}+\mathbf{k})\rangle$	$(3\cdot 1)^{-1}\cdot 2$
7	$a = -1,\ b = -7$	$\frac{1}{2}$
	$\langle 1, \mathbf{i}, \frac{1}{2}(\mathbf{i}+\mathbf{j}), \frac{1}{2}(1+\mathbf{k})\rangle$	$(2\cdot 1)^{-1}\cdot 1$
11	$a = -1,\ b = -11$	$\frac{5}{6}$
	$\langle 1, \mathbf{i}, \frac{1}{2}(\mathbf{i}+\mathbf{j}), \frac{1}{2}(1+\mathbf{k})\rangle$	$(2\cdot 1)^{-1}\cdot 1$
1, 2	$\langle 1, 2\mathbf{i}, \frac{1}{4}(2+7\mathbf{i}+\mathbf{j}), \frac{1}{2}(1+2\mathbf{i}+\mathbf{k})\rangle$	$(3\cdot 1)^{-1}\cdot 1$
13	$a = -2,\ b = -13$	1
	$\langle 1, \mathbf{i}, \frac{1}{2}(1+\mathbf{i}+\mathbf{j}), \frac{1}{4}(2+3\mathbf{i}+\mathbf{k})\rangle$	$(1\cdot 1)^{-1}\cdot 1$
17	$a = -3,\ b = -17$	$\frac{4}{3}$
	$\langle 1, \mathbf{i}, \frac{1}{2}(1+\mathbf{i}+\mathbf{j}), \frac{1}{6}(3+4\mathbf{i}+\mathbf{k})\rangle$	$(1\cdot 1)^{-1}\cdot 1$
1, 2	$\langle 1, \frac{1}{2}(1+\mathbf{i}), \mathbf{j}, \frac{1}{6}(3+\mathbf{i}+3\mathbf{j}+\mathbf{k})\rangle$	$(3\cdot 1)^{-1}\cdot 1$
19	$a = -1,\ b = -19$	$\frac{3}{2}$
	$\langle 1, \mathbf{i}, \frac{1}{2}(1+\mathbf{j}), \frac{1}{2}(\mathbf{i}+\mathbf{k})\rangle$	$(2\cdot 1)^{-1}\cdot 1$
1, 2	$\langle 1, 2\mathbf{i}, \frac{1}{2}(1+2\mathbf{i}+\mathbf{j}), \frac{1}{4}(2+3\mathbf{i}+\mathbf{k})\rangle$	$(1\cdot 1)^{-1}\cdot 1$

$[K : \mathbb{Q}] = 2$:

$\sqrt{2}, \infty$	$a = b = -1$	$\frac{1}{24}$
	$\langle 1, \frac{1}{2}\sqrt{2}(1+\mathbf{i}), \frac{1}{2}\sqrt{2}(1+\mathbf{j}), \frac{1}{2}(1+\mathbf{i}+\mathbf{j}+\mathbf{k})\rangle$	$(24\cdot 1)^{-1}\cdot 1$
$\sqrt{2}, \infty, 2, 3$	$a = -2-\sqrt{2}, b = -3$	$\frac{1}{3}$
	$\langle 1, \mathbf{i}, \frac{1}{2}(1+\mathbf{j}), \frac{1}{2}(\mathbf{i}+\mathbf{k})\rangle$	$(3\cdot 1)^{-1}\cdot 1$
$\sqrt{2}, \infty, 2, 5$	$a = -2-\sqrt{2}, b = -5$	1
	$\langle 1, \mathbf{i}, \frac{1}{2}(1+\sqrt{2}+\sqrt{2}\mathbf{i}+\mathbf{j}), \frac{1}{2}((1+\sqrt{2})\mathbf{i}+\mathbf{k})\rangle$	$(1\cdot 1)^{-1}\cdot 1$
$\sqrt{3}, \infty$	$a = b = -1$	$\frac{1}{12}$
	$\langle 1, \mathbf{i}, \frac{1}{2}(\sqrt{3}\mathbf{i}+\mathbf{j}), \frac{1}{2}(\sqrt{3}+\mathbf{k})\rangle$	$(12\cdot 2)^{-1}\cdot 1$
1, 2	$\langle 1, (1+\sqrt{3})\mathbf{i}, \frac{1}{4}(1+\sqrt{3})(2-\sqrt{3}\mathbf{i}+\mathbf{j}), \frac{1}{2}(2+\sqrt{3}\mathbf{i}+\mathbf{k})\rangle$	$(12\cdot 2)^{-1}\cdot 1$
$\sqrt{5}, \infty$	$a = b = -1$	$\frac{1}{60}$
	$\langle 1, \mathbf{i}, \frac{1}{2}(1+t+t\mathbf{i}+\mathbf{j}), \frac{1}{2}(t+(1+t)\mathbf{i}+\mathbf{k})\rangle$ mit $t := \frac{1}{2}(1+\sqrt{5})$	$(60\cdot 1)^{-1}\cdot 1$
$\sqrt{5}, \infty, 2, 3$	$a = -6, b = -5-\sqrt{5}$	$\frac{2}{5}$
	$\langle 1, \mathbf{i}, \frac{1}{4}((3+\sqrt{5})\mathbf{i}+2\mathbf{j}), \frac{1}{20}\sqrt{5}(\sqrt{5}-5-2\mathbf{j}+\mathbf{k})\rangle$	$(5\cdot 1)^{-1}\cdot 2$
$\sqrt{5}, \infty, 2, 5$	$a = -2, b = -5-\sqrt{5}$	$\frac{1}{5}$
	$\langle 1, \mathbf{i}, \frac{1}{2}(\frac{1}{2}(3+\sqrt{5})\mathbf{i}+\mathbf{j}), \frac{1}{4}(3+\sqrt{5}+\mathbf{k})\rangle$	$(5\cdot 1)^{-1}\cdot 1$
$\sqrt{5}, \infty, 3, 5$	$a = -3, b = -5-\sqrt{5}$	$\frac{8}{15}$
	$\langle 1, \frac{1}{2}(1+\mathbf{i}), \mathbf{j}, \frac{1}{4}((2+\sqrt{5})\mathbf{j}+\mathbf{k})\rangle$	$(3\cdot 1)^{-1}\cdot 1$

$1,2$	$\langle 1,\ \mathbf{i},\ \frac{1}{4}((1+\sqrt{5})(1+\mathbf{i})+4\mathbf{j}),\ \frac{1}{8}(4+(2+\sqrt{5})\mathbf{j}+\mathbf{k})\rangle$	$(5\cdot 1)^{-1}\cdot 1$
$\sqrt{6},\infty$	$a=-1,b=-1$	$\frac{1}{4}$
	$\langle 1,\ \frac{1}{2}(2+\sqrt{6})(1+\mathbf{i}),\ \frac{1}{2}(2+\sqrt{6})(1+\mathbf{j}),\ \frac{1}{2}(1+\mathbf{i}+\mathbf{j}+\mathbf{k})\rangle$	$(12\cdot 2)^{-1}\cdot 1$
$1,2$	$\langle 1,\mathbf{i},\ \frac{1}{2}(\sqrt{6}+\mathbf{i}+\mathbf{j}),\ \frac{1}{2}(1+\sqrt{6}\mathbf{i}+\mathbf{k})\rangle$	$(4\cdot 2)^{-1}\cdot 1$
$2,2$	$\langle 1,\ (2+\sqrt{6})\mathbf{i},\ \frac{1}{4}(2+\sqrt{6})(\sqrt{6}+\mathbf{i}+\mathbf{j}),\ \frac{1}{2}(1+\sqrt{6}\mathbf{i}+\mathbf{k})\rangle$	$(6\cdot 2)^{-1}\cdot 1$
$\sqrt{7},\infty$	$a=-1,b=-1$	$\frac{1}{3}$
	$\langle 1,\ \mathbf{i},\ \frac{1}{2}(\sqrt{7}\mathbf{i}+\mathbf{j}),\ \frac{1}{2}(\sqrt{7}+\mathbf{k})\rangle$	$(4\cdot 2)^{-1}\cdot 1$
$1,2$	$\langle 1,\ \frac{1}{2}(3+\sqrt{7})(1+\mathbf{i}),\ \frac{1}{2}(3+\sqrt{7})(1+\mathbf{j}),\ \frac{1}{2}(1+\mathbf{i}+\mathbf{j}+\mathbf{k})\rangle$	$(12\cdot 2)^{-1}\cdot 1$
$1,3$	$\langle 1,\ (5-2\sqrt{7})\mathbf{i},\ \frac{1}{2}(t\mathbf{i}+\mathbf{j}),\ \frac{1}{6}t(2+\sqrt{7}+\sqrt{7}\mathbf{i}+\mathbf{j}+\mathbf{k})\rangle$ mit $t:=\sqrt{7}-2$	$(3\cdot 2)^{-1}\cdot 1$
$\sqrt{10},\infty$	$a=-1,b=-1$	$\frac{7}{6}$
	$\langle 1,1+\mathbf{i},\frac{1}{2}\sqrt{10}(1+\mathbf{i}),1+\mathbf{j},\frac{1}{2}\sqrt{10}(1+\mathbf{j}),\ \frac{1}{2}(1+\mathbf{i}+\mathbf{j}+\mathbf{k})\rangle$	$(12\cdot 1)^{-1}\cdot 1$
$1,2$	$\langle 1,\ \mathbf{i},\ \frac{1}{2}(\sqrt{10}+\mathbf{i}+\mathbf{j}),\ \frac{1}{2}(1+\sqrt{10}\mathbf{i}+\mathbf{k})\rangle$	$(4\cdot 1)^{-1}\cdot 1$
$2,2$	$\langle 1,\ \frac{1}{2}t,\ \frac{1}{4}(8-\sqrt{10})t,\ \frac{1}{2}(1+(2+\sqrt{10})\mathbf{i}+\mathbf{k}),$ $(8+9\sqrt{10})\mathbf{i},\ \sqrt{10}\mathbf{i}\rangle$ mit $t:=2+\sqrt{10}+(1+2\sqrt{10})\mathbf{i}+\mathbf{j}$	$(2\cdot 1)^{-1}\cdot 1$
$3,2$	$\langle 1,\ 2\mathbf{i},\ t_1,\ \frac{1}{2}(10-\sqrt{10})t_1,\ t_2,\ \frac{1}{2}(10+5\sqrt{10})t_2\rangle$ mit $t_1:=\frac{1}{2}(2+\sqrt{10}+(2\sqrt{10}-3)\mathbf{i}+\mathbf{j})$ und $t_2:=\frac{1}{2}(2+\sqrt{10}+\frac{1}{2}(8+3\sqrt{10})\mathbf{i}+\frac{1}{2}\sqrt{10}\mathbf{j}+\mathbf{k})$	$(3\cdot 1)^{-1}\cdot 1$
$\sqrt{11},\infty$	$a=-1,b=-1$	$\frac{7}{12}$
	$\langle 1,\ \mathbf{i},\ \frac{1}{2}(\sqrt{11}\mathbf{i}+\mathbf{j}),\ \frac{1}{2}(\sqrt{11}+\mathbf{k})\rangle$	$(4\cdot 2)^{-1}\cdot 1$
$1,2$	$\langle 1,(3+\sqrt{11})\mathbf{i},\ \frac{1}{4}(3+\sqrt{11})(2+\sqrt{11}\mathbf{i}+\mathbf{j}),\ \frac{1}{2}(\sqrt{11}+2\mathbf{i}+\mathbf{k})\rangle$	$(2\cdot 2)^{-1}\cdot 1$
$1,2$	$\langle 1,\ \frac{1}{2}(3+\sqrt{11})(1+\mathbf{i}),\ \frac{1}{2}(3+\sqrt{11})(1+\mathbf{j}),\ \frac{1}{2}(1+\mathbf{i}+\mathbf{j}+\mathbf{k})\rangle$	$(12\cdot 2)^{-1}\cdot 1$
$2,2$	$\langle 1,\ 2\mathbf{i},\ \frac{1}{4}(2+\sqrt{11}\mathbf{i}+\mathbf{j}),\ \frac{1}{2}(\sqrt{11}+2\mathbf{i}+\mathbf{k})\rangle$	$(6\cdot 1)^{-1}\cdot 1$
$\sqrt{13},\infty$	$a=-1,b=-1$	$\frac{1}{12}$
	$\langle 1,\ \mathbf{i},\ \frac{1}{2}(t+(t+1)\mathbf{i}+\mathbf{j}),\ \frac{1}{2}(t+1+t\mathbf{i}+\mathbf{k})\rangle$ mit $t:=\frac{1}{2}(1+\sqrt{13})$	$(12\cdot 1)^{-1}\cdot 1$
$\sqrt{15},\infty$	$a=b=-1$	2
	$\langle 1,\ \mathbf{i},\ \frac{1}{2}(\sqrt{15}\mathbf{i}+\mathbf{j}),\frac{1}{2}(\sqrt{15}+\mathbf{k})\rangle$	$(1\cdot 4)^{-1}\cdot 1$
$1,2$	$\langle 1,\ 2\mathbf{i},\ (3+\sqrt{15})\mathbf{i},\ \frac{1}{2}(-\sqrt{15}\mathbf{i}+\mathbf{j}),$ $\frac{1}{4}(5\sqrt{15}+3)(-\sqrt{15}\mathbf{i}+\mathbf{j}),\ \frac{1}{2}(\sqrt{15}+k)\rangle$	$(2\cdot 2)^{-1}\cdot 1$
$1,2$	$\langle 1,\ 1+\mathbf{i},\ \frac{3}{2}(1+\sqrt{15})(1+\mathbf{i}),\ 1+\mathbf{j},$ $\frac{1}{2}(1-\sqrt{15})(1+\mathbf{j}),\ \frac{1}{2}(1+\mathbf{i}+\mathbf{j}+\mathbf{k})\rangle$	$(12\cdot 1)^{-1}\cdot 1$
$2,2$	$\langle 1,\ 2\mathbf{i},\ \frac{1}{4}(2+2\sqrt{15}+(4-\sqrt{15})\mathbf{i}+\mathbf{j}),$ $\frac{1}{2}(\sqrt{15}+(2+2\sqrt{15})\mathbf{i}+\mathbf{k})\rangle$	$(2\cdot 2)^{-1}\cdot 1$
$4,2$	$\langle 1,\ 4\mathbf{i},\ 126(1+\sqrt{15})\mathbf{i},\ \frac{1}{4}t,\ \frac{1}{2}(\sqrt{15}+(2+2\sqrt{15})\mathbf{i}+\mathbf{k}),$ $\frac{1}{8}(3+\sqrt{15})t\rangle$ mit $t=2+2\sqrt{15}+(4-\sqrt{15})\mathbf{i}+\mathbf{j}$	$(6\cdot 1)^{-1}\cdot 1$
$1,3$	$\langle 1,\ (57+14\sqrt{15})\mathbf{i},\ \sqrt{15}\mathbf{i},\ \frac{1}{2}((\sqrt{15}-2)\mathbf{i}+\mathbf{j}),\ \frac{1}{2}t,$ $\frac{2}{3}(3+\sqrt{15})t\rangle$ mit $t=(\sqrt{15}+(3\sqrt{15}-2)\mathbf{i}-\mathbf{j}+\mathbf{k})$	$(1\cdot 2)^{-1}\cdot 1$
$6,2$	$\langle 1,\ (3+\sqrt{15})\mathbf{i},\ ,t_1,\ \frac{1}{2}(11+3\sqrt{15})t_1,\ \frac{1}{2}t_2,\ \frac{2}{3}(3+\sqrt{15})t_2\rangle$ mit $t_1=\frac{1}{2}((4+\sqrt{15})\mathbf{i}+\mathbf{j})$, $t_2=\sqrt{15}+(4+3\sqrt{15})\mathbf{i}-\mathbf{j}+\mathbf{k}$	$(3\cdot 1)^{-1}\cdot 1$

$6,2$	$\langle 1,\ \frac{1}{2}(\sqrt{15}+3)(1+\mathbf{i}),\ \mathbf{i}+\mathbf{j},\ \frac{1}{2}(3\sqrt{15}+11)(\mathbf{i}+\mathbf{j}),\ t,$ $\frac{1}{3}(3+8\sqrt{15})t\rangle$ mit $t=\frac{1}{2}(3+\mathbf{i}-\mathbf{j}+\mathbf{k})$	$(3{\cdot}2)^{-1}{\cdot}1$
$\sqrt{17},\infty$	$a=-1,b=-3$	$\frac{1}{6}$
	$\langle 1,\ \mathbf{i},\ \frac{1}{2}(1+\mathbf{j}),\ \frac{1}{6}(\frac{3}{2}(3+\sqrt{17})+3\mathbf{i}-(\frac{1}{2}(3+\sqrt{17}))\mathbf{j}+\mathbf{k})\rangle$	$(6{\cdot}1)^{-1}{\cdot}1$
$\sqrt{21},\infty$	$a=b=-1$	$\frac{1}{6}$
	$\langle 1,\ \mathbf{i},\ \frac{1}{2}(1+t+t\mathbf{i}+\mathbf{j}),\ \frac{1}{2}(t+(1+t)\mathbf{i}+\mathbf{k})\rangle$ mit $t=\frac{1}{2}(1+\sqrt{21})$	$(12{\cdot}1)^{-1}{\cdot}1$
$1,3$	$\langle 1,\ t\mathbf{i},\ \frac{1}{2}(t+(1+t)\mathbf{i}+\mathbf{j}),\ \frac{1}{6}t(3-\mathbf{i}+\mathbf{j}+\mathbf{k})\rangle$ mit $t=\frac{1}{2}(3+\sqrt{21})$	$(6{\cdot}2)^{-1}{\cdot}1$
$\sqrt{33},\infty$	$a=-1,b=-3$	$\frac{1}{2}$
	$\langle 1,\ \mathbf{i},t_1(t_2-3+t_2\mathbf{i}+\mathbf{j}),t_1(t_2+(t_2-3)\mathbf{i}+\mathbf{k})\rangle$ mit $t_1=\frac{1}{6}(6+\sqrt{33}),t_2=\frac{1}{2}(3+\sqrt{33})$	$(2{\cdot}2)^{-1}{\cdot}1$
$1,2$	$\langle 1,\ \frac{1}{2}(5-\sqrt{33})\mathbf{i},\ \frac{1}{6}(6+\sqrt{33})(t-12+t\mathbf{i}+\mathbf{j}),$ $\frac{1}{24}(63+11\sqrt{33})(t+(t+9)\mathbf{i}+\mathbf{k})\rangle$ mit $t=\frac{1}{2}(3+\sqrt{33})$	$(3{\cdot}2)^{-1}{\cdot}1$
$1,2$	$\langle 1,\ \mathbf{i},\ \frac{1}{6}(6+\sqrt{33})(3\mathbf{i}+\mathbf{j}),\ \frac{1}{6}(6+\sqrt{33})(3+\mathbf{k})\rangle$	$(6{\cdot}2)^{-1}{\cdot}1$

$[K:\mathbb{Q}]=3$:

$\theta_7,\infty,7$	$a=-1,b=-7$	$\frac{1}{14}$
	$\langle 1,\ \mathbf{i},\ \frac{1}{14}(2\theta_7^2-\theta_7+1)(7+\mathbf{j}),\ \frac{1}{12}(2\theta_7^2-\theta_7+1)(7\mathbf{i}+\mathbf{k})\rangle$	$(14\cdot 1)^{-1}\cdot 1$
$\theta_7,\infty,2$	$a=b=-1$	$\frac{1}{12}$
	$\langle 1,\ \mathbf{i},\ \mathbf{j},\ \frac{1}{2}(1+\mathbf{i}+\mathbf{j}+\mathbf{k})\rangle$	$(12\cdot 1)^{-1}\cdot 1$
$\theta_7,\infty,3$	$a=-1,b=-3$	$\frac{13}{42}$
	$\langle 1,\ \mathbf{i},\ \frac{1}{2}(\mathbf{i}+\mathbf{j}),\ \frac{1}{2}(1+\mathbf{k})\rangle$	$(6\cdot 1)^{-1}\cdot 1$
$1,7$	$\langle 1,\ (-\theta_7^2+\theta_7+2)\mathbf{i},\ \frac{1}{2}(7\mathbf{i}+\mathbf{j}),$ $\frac{1}{14}(2\theta_7^2-\theta_7+1)(7-2\mathbf{i}+\mathbf{k})\rangle$	$(7\cdot 1)^{-1}\cdot 1$
$\theta_9,\infty,3$	$a=-1,b=-3$	$\frac{1}{18}$
	$\langle 1,\ \mathbf{i},\ \frac{1}{6}(\theta_9^2-2\theta_9+1)(3\mathbf{i}+\mathbf{j}),\ \frac{1}{6}(\theta_9^2-2\theta_9+1)(3+\mathbf{k})\rangle$	$(18\cdot 1)^{-1}\cdot 1$
$\theta_9,\infty,2$	$a=b=-1$	$\frac{7}{36}$
	$\langle 1,\ \mathbf{i},\ \mathbf{j},\ \frac{1}{2}(1+\mathbf{i}+\mathbf{j}+\mathbf{k})\rangle$	$(12\cdot 1)^{-1}\cdot 1$
$1,3$	$\langle 1,\ (1-\theta_9)\mathbf{i},\ \mathbf{i}-\mathbf{j},\ \frac{1}{6}(\theta_9^2-2\theta_9+1)(3-\mathbf{i}-\mathbf{j}+\mathbf{k})\rangle$	$(9\cdot 1)^{-1}\cdot 1$
$\omega_{13},\infty,13$	$a=-2,b=-13$	1
	$\langle 1,\ \mathbf{i},\ \frac{1}{26}t(13+13\mathbf{i}+\mathbf{j}),\ \frac{1}{52}t(26-13\mathbf{i}+\mathbf{k})\rangle$ mit $t=4\omega_{13}^2+7\omega_{13}-1$	$(1\cdot 1)^{-1}\cdot 1$
$\omega_{19},\infty,19$	$a=-1,b=-19$	$\frac{9}{2}$
	$\langle 1,\ \mathbf{i},\ t(19+\mathbf{j}),\ t(19\mathbf{i}+\mathbf{k})\rangle$ mit $t=\frac{1}{38}(-2\omega_{19}^2+5\omega_{19}+23)$	$(2\cdot 1)^{-1}\cdot 1$
$1,2$	$\langle 1,\ 2\mathbf{i},\ \frac{1}{38}t_1(19+t_2\mathbf{i}+\mathbf{j}),\ \frac{1}{76}t_1(t_2+(2\omega_{19}^2+61)\mathbf{i}+\mathbf{k})\rangle$ mit $t_1=(-2\omega_{19}^2+5\omega_{19}+23),t_2=(2\omega_{19}^2+2\omega_{19}+30)$	$3*(1\cdot 1)^{-1}\cdot 1$
$1,2$	$\langle 1,\ 2\mathbf{i},\ \frac{1}{38}t(19+38\mathbf{i}+\mathbf{j}),\ \frac{1}{76}t(38+19\mathbf{i}+\mathbf{k})\rangle$ mit $t=-2\omega_{19}^2+5\omega_{19}+23$	$(1\cdot 1)^{-1}\cdot 1$

$[K:\mathbb{Q}]=4$:

θ_{15},∞	$a=b=-1$	$\frac{1}{30}$
	$\langle 1,\ \mathbf{i},\ \frac{1}{2}(t+(1+t)\mathbf{i}+\mathbf{j}),\ \frac{1}{2}(1+t+t\mathbf{i}+\mathbf{k})\rangle$ mit $t=\theta_{15}^3+\theta_{15}$	$(60\cdot 1)^{-1}\cdot 1$
$1,5$	$\langle 1,\ (1-\theta_{15})\mathbf{i},\ \frac{1}{2}(t_1+(3+t_1)\mathbf{i}+\mathbf{j}),$ $\frac{1}{10}t_2(3+t_1+(\theta_{15}^3-3\theta_{15}+4)\mathbf{i}+\mathbf{k})\rangle$ mit $t_1=\theta_{15}^3+\theta_{15},\ t_2=1-\theta_{15}^3+3\theta_{15}^2-3\theta_{15}$	$(30\cdot 2)^{-1}\cdot 1$
θ_{16},∞	$a=b=-1$	$\frac{5}{48}$
	$\langle 1,\ \frac{1}{2}\theta_{16}^2(1+\mathbf{i}),\ \frac{1}{2}\theta_{16}^2(1+\mathbf{j}),\ \frac{1}{2}(1+\mathbf{i}+\mathbf{j}+\mathbf{k})\rangle$	$(24\cdot 1)^{-1}\cdot 1$
$1,2$	$\langle 1,\ \frac{1}{2}\theta_{16}^3(1+\mathbf{i}),\ \frac{1}{2}\theta_{16}(t+\mathbf{j}),\ \frac{1}{2}(t+t\mathbf{i}+\mathbf{j}+\mathbf{k})\rangle$ mit $t=\theta_{16}^2+1$	$(16\cdot 1)^{-1}\cdot 1$
θ_{20},∞	$a=b=-1$	$\frac{1}{12}$
	$\langle 1,\ t(1+\mathbf{i}),\ t(1+\mathbf{j}),\ \frac{1}{2}(1+\mathbf{i}+\mathbf{j}+\mathbf{k})\rangle$ mit $t=\frac{1}{2}(\theta_{20}^3+\theta_{20}^2-3\theta_{20}-2)$	$(12\cdot 2)^{-1}\cdot 1$
$1,2$	$\langle 1,\ \mathbf{i},\ \frac{1}{2}(\theta_{20}^2+(1+\theta_{20}^2)\mathbf{i}+\mathbf{j}),\ \frac{1}{2}(1+\theta_{20}^2+\theta_{20}^2\mathbf{i}+\mathbf{k})\rangle$	$(60\cdot 1)^{-1}\cdot 1$
$1,2$	$\langle 1,\ \mathbf{i},\ \frac{1}{2}(\theta_{20}^3+\mathbf{j}),\ \frac{1}{2}(\theta_{20}^3\mathbf{i}+\mathbf{k})\rangle$	$(20\cdot 2)^{-1}\cdot 1$
θ_{24},∞	$a=b=-1$	$\frac{1}{3}$
	$\langle 1,\ \frac{1}{2}(\theta_{24}^3-4\theta_{24}+1)(\theta_{24}^2+1+\mathbf{i}+\mathbf{j}),$ $\frac{1}{2}(7\theta_{24}^3-3\theta_{24}^2-27\theta_{24}+13)(1+\mathbf{i}),$ $\frac{1}{2}(\theta_{24}^2+\theta_{24}^2\mathbf{i}+\mathbf{j}+\mathbf{k})\rangle$	$(8\cdot 2)^{-1}\cdot 1$
$1,2$	$\langle 1,\ t(1+\mathbf{i}),\ t(1+\mathbf{j}),\ \frac{1}{2}(1+\mathbf{i}+\mathbf{j}+\mathbf{k})\rangle$ mit $t=\frac{1}{2}(2\theta_{24}^3-\theta_{24}^2-8\theta_{24}+5)$	$(24\cdot 1)^{-1}\cdot 1$
$1,2$	$\langle 1,\ \mathbf{i},\ \frac{1}{2}(\theta_{24}^2\mathbf{i}+\mathbf{j}),\ \frac{1}{2}(\theta_{24}^2+\mathbf{k})\rangle$	$(24\cdot 2)^{-1}\cdot 1$
η_{17},∞	$a=b=-1$	$\frac{1}{3}$
	$\langle 1,\ \mathbf{i},\ \frac{1}{2}(t+(t-1)\mathbf{i}+\mathbf{j}),\ \frac{1}{2}(t-1+t\mathbf{i}+\mathbf{k})\rangle$ mit $t=\frac{1}{2}(-\eta_{17}^3+8\eta_{17}-1)$	$2*(12\cdot 1)^{-1}\cdot 1$
$1,2$	$\langle 1,\ \frac{1}{2}(-5\eta_{17}^3-6\eta_{17}^2+28\eta_{17}+9)\mathbf{i},$ $\frac{1}{2}(\frac{1}{2}t_1+\frac{1}{2}(\eta_{17}^3+2\eta_{17}^2-2\eta_{17}-1)\mathbf{i}+\mathbf{j}),$ $\frac{1}{4}(\eta_{17}+1)(\frac{1}{2}(-\eta_{17}^3+6\eta_{17}-1)+\frac{1}{2}t_2\mathbf{i}+(\eta_{17}+1)\mathbf{j}+\mathbf{k})\rangle$ mit $t_1=(\eta_{17}^3+2\eta_{17}^2-6\eta_{17}-3), t_2=-\eta_{17}^3+12\eta_{17}-1$	$(6\cdot 1)^{-1}\cdot 1$
$\sqrt{2}+\sqrt{5},\infty$	$a=b=-1$	$\frac{7}{120}$
	$\langle 1,\ t(1+\mathbf{i}),\ t(1+\mathbf{j}),\ \frac{1}{2}(1+\mathbf{i}+\mathbf{j}+\mathbf{k})\rangle$ mit $\alpha=\sqrt{2}+\sqrt{5},\ t=\frac{1}{12}(\alpha^3-11\alpha)$	$(24\cdot 1)^{-1}\cdot 1$
$1,2$	$\langle 1,\ \mathbf{i},\ \frac{1}{2}(t+1+t\mathbf{i}+\mathbf{j}),\ \frac{1}{2}(t+(t+1)\mathbf{i}+\mathbf{k})\rangle$ mit $\alpha=\sqrt{2}+\sqrt{5},\ t=\frac{1}{12}(\alpha^3+7\alpha+6)$	$(60\cdot 1)^{-1}\cdot 1$
$\sqrt{2}+\sqrt{5},\infty,2,5$	$a=-2-\sqrt{2}, b=-5-\sqrt{5}$	$\frac{21}{5}$
	$\langle 1,\ \mathbf{i},\ t_1(t_2+\mathbf{j}),\ t_1(t_2\mathbf{i}+\mathbf{k})\rangle$ mit $\alpha=\sqrt{2}+\sqrt{5}$, $t_1=\frac{1}{24}(\alpha^3-11\alpha), t_2=\frac{1}{12}(\alpha^3-3\alpha^2+13\alpha-3)$	$(5\cdot 1)^{-1}\cdot 1$
$1,3$	[1]	$2*(1\cdot 1)^{-1}\cdot 2$

[1] Die R-Erzeugendensysteme der beiden fehlenden R-Maximalordnungen wurden nicht mit angegeben, da die Einträge sehr lang waren und mehrere Zeilen benötigt hätten. Die beiden R-Maximalordnungen liegen in derselben Galoisbahn, daher habe ich nur einen Eintrag für sie gemacht, obwohl a und b nicht in $\mathbb{Q}$ liegen.

η_{40}, ∞	$a = b = -1$	$\frac{41}{60}$
	$\langle 1,\ \mathbf{i},\ \frac{1}{2}(t + \mathbf{i} + \mathbf{j}),\ \frac{1}{2}(1 + t\mathbf{i} + \mathbf{k})\rangle$ mit $t = \frac{1}{2}(\eta_{40}^3 - 4\eta_{40})$	$(4{\cdot}2)^{-1}{\cdot}1$
$1, 5$	$\langle 1, \frac{1}{2}(\eta_{40}^3 - 3\eta_{40}^2 - 4\eta_{40} + 10)\mathbf{i}, t(5 + \frac{1}{2}(\eta_{40}^3 - 4)\mathbf{i} + \mathbf{k}),$ $\frac{1}{2}(\frac{1}{2}(\eta_{40}^3 - 4\eta_{40}) + 5\mathbf{i} + \mathbf{j})\rangle$ mit $t = \frac{1}{20}(89\eta_{40}^3 - 240\eta_{40}^2 - 250\eta_{40} + 670)$	$(2{\cdot}2)^{-1}{\cdot}1$
$1, 5$	$\langle 1, \frac{1}{2}(\eta_{40}^3 - 3\eta_{40}^2 - 4\eta_{40} + 10)\mathbf{i},$ $t(\frac{1}{2}(\eta_{40}^3 - 4\eta_{40}) + 3\mathbf{i} + \mathbf{j}), \frac{1}{2}(1 + \frac{1}{2}(\eta_{40}^3 - 4\eta_{40})\mathbf{i} + \mathbf{k})\rangle$ mit $t = \frac{1}{20}(89\eta_{40}^3 - 240\eta_{40}^2 - 250\eta_{40} + 670)$	$(12{\cdot}2)^{-1}{\cdot}1$
$1, 2$	$\langle 1,\ t\mathbf{i},\ t(\frac{1}{2}(\eta_{40}^3 - 4\eta_{40}) - \mathbf{i} + \mathbf{j}),$ $\frac{1}{2}(1 + \frac{1}{2}(\eta_{40}^3 - 4\eta_{40})\mathbf{i} + \mathbf{k})\rangle$ mit $t = \frac{1}{2}(\eta_{40}^3 + 2\eta_{40}^2 - 8\eta_{40} - 16)$	$(10{\cdot}2)^{-1}{\cdot}1$
$2, 2$	$\langle 1, \frac{1}{2}(\eta_{40}^3 - 6\eta_{40})\mathbf{i},\ t_2(5 + \frac{1}{2}(\eta_{40}^3 - 4)\mathbf{i} + \mathbf{k}),$ $t_1(\frac{1}{2}(\eta_{40}^3 - 4\eta_{40} + 4) + (\eta_{40}^3 + \eta_{40}^2 - 4\eta_{40} - 15)\mathbf{i} + \mathbf{j})\rangle$ mit $t_1 = \frac{1}{8}(\eta_{40}^3 + 2\eta_{40}^2 - 8\eta_{40} - 16)$, $t_2 = \frac{1}{20}(89\eta_{40}^3 - 240\eta_{40}^2 - 250\eta_{40} + 670)$	$(5{\cdot}1)^{-1}{\cdot}1$
$3, 2$	$\langle 1,\ \frac{1}{2}(\eta_{40}^3 - 6\eta_{40})\mathbf{i},\ \frac{1}{2}(1 + \frac{1}{2}(\eta_{40}^3 - 4\eta_{40})\mathbf{i} + \mathbf{k}),$ $\frac{1}{40}(23\eta_{40}^3 - 60\eta_{40}^2 - 60\eta_{40} + 160)(\frac{1}{2}\eta_{40}^3 - 2\eta_{40} - 7\mathbf{i} + \mathbf{j})\rangle$	$(60{\cdot}1)^{-1}{\cdot}1$
$\sqrt{3} + \sqrt{5}, \infty$	$a = b = -1$	$\frac{1}{5}$
	$\langle 1, \mathbf{i}, \frac{1}{2}((\alpha + 1)\mathbf{i} + \mathbf{j}), \frac{1}{2}(\alpha + 1 + \mathbf{k})\rangle$ mit $\alpha = \sqrt{3} + \sqrt{5}$	$(12{\cdot}2)^{-1}{\cdot}1$
$1, 11$	$\langle 1,\ \frac{1}{4}(10 - \alpha^2 - 2\alpha)\mathbf{i},\ \frac{1}{2}((\alpha + 11)\mathbf{i} + \mathbf{j}),$ $\frac{1}{88}(-\alpha^3 + \alpha^2 + 4\alpha + 18)(\alpha + 1 - 106\mathbf{i} + 4\mathbf{j} + \mathbf{k})\rangle$ mit $\alpha = \sqrt{3} + \sqrt{5}$	$(5{\cdot}2)^{-1}{\cdot}1$
$1, 2$	$\langle 1,\ \frac{1}{2}(\alpha^3 - 16\alpha)\mathbf{i},\ \frac{1}{2}(\alpha + 1 + 2\mathbf{i} + \mathbf{k}),$ $\frac{1}{8}(\alpha^3 - 16\alpha)(2 + \frac{1}{4}(\alpha^3 + 2\alpha)\mathbf{i} + \mathbf{j})\rangle$ mit $\alpha = \sqrt{3} + \sqrt{5}$	$(12{\cdot}2)^{-1}{\cdot}1$
$3, 2$	$\langle 1,\ 2\mathbf{i},\ \frac{1}{4}(\frac{1}{2}(\alpha^2 - 2\alpha - 2) + \frac{1}{4}(-\alpha^3 + 4\alpha^2 - 2\alpha)\mathbf{i} + \mathbf{j}),$ $\frac{1}{2}(\alpha + 1 + \frac{1}{2}(\alpha^2 - 2\alpha - 2)\mathbf{i} + \mathbf{k})\rangle$ mit $\alpha = \sqrt{3} + \sqrt{5}$	$(60{\cdot}1)^{-1}{\cdot}1$

$[K : \mathbb{Q}] = 5$:

$\theta_{11}, \infty, 11$	$a = -1, b = -11$	$\frac{25}{66}$
	$\langle 1, \mathbf{i},\ t(11 + \mathbf{j}),\ t(11\mathbf{i} + \mathbf{k})\rangle$ mit $t = \frac{1}{22}(-5\theta_{11}^4 + 2\theta_{11}^3 + 9\theta_{11}^2 + \theta_{11} + 4)$	$(22{\cdot}1)^{-1}{\cdot}1$
$1, 2$	$\langle 1,\ 2\theta_{11}^4\mathbf{i},\ t(11 + (2\theta_{11}^4 - 20\theta_{11} + 8)\mathbf{i} + \mathbf{j}),$ $\frac{1}{2}t(2\theta_{11}^4 - 20\theta_{11} + 8 + (-2\theta_{11}^4 - 2\theta_{11}^3 + 37)\mathbf{i} + \mathbf{k})\rangle, t$ s.o.	$(3{\cdot}1)^{-1}{\cdot}1$
$\theta_{11}, \infty, 2$	$a = -1, b = -1$	$\frac{155}{132}$
	$\langle 1,\ \mathbf{i},\ \mathbf{j},\ \frac{1}{2}(1 + \mathbf{i} + \mathbf{j} + \mathbf{k})\rangle$	$(12{\cdot}1)^{-1}{\cdot}1$
$1, 11$	$\langle 1,\ (-\theta_{11}^2 + \theta_{11} + 2)\mathbf{i}, 3\mathbf{i} + \mathbf{j},$ $\frac{1}{22}(15\theta_{11}^4 - 21\theta_{11}^3 - 36\theta_{11}^2 + 37\theta_{11} + 20)(11 + \mathbf{i} - 3\mathbf{j} + \mathbf{k})\rangle$	$(1{\cdot}1)^{-1}{\cdot}1$
$2, 11$	$\langle 1,\ (\theta_{11}^4 - 2\theta_{11}^3 - 3\theta_{11}^2 + 4\theta_{11} + 4)\mathbf{i},\ 3\mathbf{i} + \mathbf{j},$ $\frac{1}{22}(-5\theta_{11}^4 + 2\theta_{11}^3 + 9\theta_{11}^2 + \theta_{11} + 4)(11 + \mathbf{i} - 3\mathbf{j} + \mathbf{k})\rangle$	$(11{\cdot}1)^{-1}{\cdot}1$
$\theta_{11}, \infty, 3$	$a = -1, b = -3$	$\frac{55}{6}$
	$\langle 1,\ \mathbf{i},\ \frac{1}{2}(\mathbf{i} + \mathbf{j}),\ \frac{1}{2}(1 + \mathbf{k})\rangle$	$(6{\cdot}1)^{-1}{\cdot}1$

$1, 11$	$\langle 1,\ (-\theta_{11}^2+\theta_{11}+2)\mathbf{i},\ \frac{1}{2}(5\mathbf{i}+\mathbf{j}),$ $\frac{1}{22}(15\theta_{11}^4-21\theta_{11}^3-36\theta_{11}^2+37\theta_{11}+20)(11+2\mathbf{i}+4\mathbf{j}+\mathbf{k})\rangle$	$(1\cdot 1)^{-1}\cdot 2$
$2, 11$	$\langle 1,\ (\theta_{11}^4-2\theta_{11}^3-3\theta_{11}^2+4\theta_{11}+4)\mathbf{i},\ t(11+2\mathbf{i}+4\mathbf{j}+\mathbf{k}),$ $\frac{1}{2}(5\mathbf{i}+\mathbf{j})\rangle$ mit $t=\frac{1}{22}(-5\theta_{11}^4+2\theta_{11}^3+9\theta_{11}^2+\theta_{11}+4)$	$(1\cdot 1)^{-1}\cdot 2$
$2, 11$	$\langle 1, (\theta_{11}^4-2\theta_{11}^3-3\theta_{11}^2+4\theta_{11}+4)\mathbf{i}, \frac{1}{2}((3-10\theta_{11})\mathbf{i}+\mathbf{j}),$ $t(11+(2\theta_{11}^3+8\theta_{11}^2-10\theta_{11}+7)\mathbf{i}+(1-4\theta_{11})\mathbf{j}+\mathbf{k})\rangle, t$ s.o.	$5*(1\cdot 1)^{-1}\cdot 1$
$\sigma_{25}, \infty, 5$	$a=-2, b=-5$	$\frac{71}{3}$
	$\langle 1,\ \mathbf{i},\ t(5+5\mathbf{i}+\mathbf{j}),\ t(10+5\mathbf{i}+\mathbf{k})\rangle$ $t=\frac{1}{10}(\sigma_{25}^3+3\sigma_{25}^2+3\sigma_{25}+1)$	$(3\cdot 1)^{-1}\cdot 1$
$1, 2$	$*$	$5*(1\cdot 1)^{-1}\cdot 2$
$2, 2$	$*$	$5*(1\cdot 1)^{-1}\cdot 1$
$2, 2$	$*$	$5*(3\cdot 1)^{-1}\cdot 2$
$2, 2$	$*$	$5*(1\cdot 1)^{-1}\cdot 1$

Die R-Erzeugendensysteme der letzten vier Vertreter von Konjugationsklassen des letzten Beispiels waren sehr lang und unübersichtlich. Ich habe daher darauf verzichtet, sie hier mit anzugeben.

B.2 Zyklotomische Quaternionenalgebren

Im Folgenden sind alle Konjugationsklassen von R-Maximalordnungen der zyklotomischen Quaternionenalgebren $\mathfrak{D}_{\theta_n}$ mit geradem $n \geq 4$ und $[\mathbb{Q}(\theta_n):\mathbb{Q}] = \frac{1}{2}\varphi(n) < 8$ aufgelistet.

Nach Satz 3.2.4 gilt:

$$d(\mathfrak{D}_{\theta_n}) = \begin{cases} (2\mathbb{Z})^2 & \text{falls } n=4 \\ (2+\theta_n)^2 & \text{falls } \frac{n}{2}=p^k \text{ mit einer Primzahl } p\equiv 3 \mod 4 \\ \mathbb{Z}[\theta_n] & \text{sonst .} \end{cases}$$

Wir beschränken uns daher darauf, lediglich ein Vertretersystem von R-Maximalordnungen und die Zerlegung der Eichlerschen Maßformel anzugeben.

$n=4$		$\frac{1}{12}$
	$\langle 1,\ \zeta_4,\ x,\ \frac{1}{2}(1+\zeta_4+x\zeta_4 x)\rangle$	$(12\cdot 1)^{-1}\cdot 1$
$n=6$		$\frac{1}{6}$
	$\langle 1,\ \zeta_6,\ x,\ \zeta_6 x\rangle$	$(6\cdot 1)^{-1}\cdot 1$
$n=8$		$\frac{1}{24}$
	$\langle 1,\ \zeta_8,\ \frac{1}{2}\theta_8(1+x),\ \frac{1}{2}\theta_8(\zeta_8+\zeta_8 x)\rangle$	$(24\cdot 1)^{-1}\cdot 1$
$n=10$		$\frac{1}{60}$
	$\langle 1,\ \zeta_{10},\ x,\ \frac{1}{5}(1-2\theta_{10})(-2-2\zeta_{10}+x+\zeta_{10}x)\rangle$	$(60\cdot 1)^{-1}\cdot 1$
$n=12$		$\frac{1}{12}$
	$\langle 1,\ \zeta_{12},\ x,\ \zeta_{12}x\rangle$	$(12\cdot 2)^{-1}\cdot 1$
$1, 2$	$\langle 1,\ (1+\theta_{12})\zeta_{12},\ \frac{1}{2}(1+\theta_{12})(1+x),\ \zeta_{12}+\zeta_{12}x\rangle$	$(12\cdot 2)^{-1}\cdot 1$

$n = 14$		$\frac{1}{14}$
	$\langle 1,\, \zeta_{14},\, x,\, \zeta_{14}x\rangle$	$(14\cdot 1)^{-1}\cdot 1$
$n = 16$		$\frac{5}{48}$
	$\big\langle 1,\, \zeta_{16},\, \frac{1}{2}\theta_{16}^3(1+x),\, \frac{1}{2}\theta_{16}^3(\zeta_{16}+\zeta_{16}x)\big\rangle$	$(16\cdot 1)^{-1}\cdot 1$
$1,2$	$\big\langle 1,\, \theta_{16}\zeta_{16},\, \frac{1}{2}\theta_{16}^2(1+x),\, \frac{1}{2}\theta_{16}^3(\zeta_{16}+\zeta_{16}x)\big\rangle$	$(24\cdot 1)^{-1}\cdot 1$
$n = 18$		$\frac{1}{18}$
	$\langle 1,\, \zeta_{18},\, x,\, \zeta_{18}x\rangle$	$(18\cdot 1)^{-1}\cdot 1$
$n = 20$		$\frac{1}{12}$
	$\langle 1,\, \zeta_{20},\, x,\, \zeta_{20}x\rangle$	$(20\cdot 2)^{-1}\cdot 1$
$1,2$	$\big\langle 1,\, t\zeta_{20},\, \zeta_{20}+x,\, \frac{1}{2}t(1+\theta_{20}x+\zeta_{20}x)\big\rangle$ mit $t=\theta_{20}^3+\theta_{20}^2-3\theta_{20}-2$	$(12\cdot 2)^{-1}\cdot 1$
$2,2$	$\big\langle 1,\, 2\zeta_{20},\, \frac{1}{2}(t+2(t-1)\zeta_{20}+\theta_{20}x+\zeta_{20}x),\, t\zeta_{20}+x\big\rangle$ mit $t=\theta_{20}^3+\theta_{20}^2+\theta_{20}+1$	$(60\cdot 1)^{-1}\cdot 1$
$n = 22$		$\frac{25}{66}$
	$\langle 1,\, \zeta_{22},\, x,\, \zeta_{22}x\rangle$	$(22\cdot 1)^{-1}\cdot 1$
$1,2$	$\langle 1,\, (550\theta_{22}^4+308\theta_{22}^3-1056\theta_{22}^2-510\theta_{22}+220)\zeta_{22},$ $\frac{1}{2}(\theta_{22}+2(t-1)\zeta_{22}+(t-\theta_{22}^3-1)x+\zeta_{22}x),$ $(t-\theta_{22}^2)\zeta_{22}+x\rangle$ mit $t=\theta_{22}^4+\theta_{22}^3+\theta_{22}^2+\theta_{22}+1$	$(3\cdot 1)^{-1}\cdot 1$
$n = 24$		$\frac{1}{8}$
	$\langle 1,\, \zeta_{24},\, x,\, \zeta_{24}x\rangle$	$(24\cdot 2)^{-1}\cdot 1$
$1,2$	$\langle 1,\, (-\theta_{24}^3+4\theta_{24}-1)\zeta_{24},\, \zeta_{24}+\zeta_{24}x,$ $\frac{1}{2}(-7\theta_{24}^3+3\theta_{24}^2+27\theta_{24}-13)(1+x)\big\rangle$	$(8\cdot 2)^{-1}\cdot 1$
$1,2$	$\langle 1,\, t\zeta_{24},\, t(1+x),\, \zeta_{24}+\zeta_{24}x\rangle$ mit $t=2\theta_{24}^3-\theta_{24}^2-8\theta_{24}+5$	$(24\cdot 1)^{-1}\cdot 1$
$n = 26$		$\frac{19}{156}$
	$\big\langle 1,\, \zeta_{26},\, x,\, \frac{1}{13}t(-5-5\zeta_{26}+x+\zeta_{26}x)\big\rangle$ mit $t=90\theta_{26}^5-179\theta_{26}^4-235\theta_{26}^3+570\theta_{26}^2-145\theta_{26}-71$	$(26\cdot 1)^{-1}\cdot 1$
$1,13$	$\langle 1,\, (\theta_{26}^5-\theta_{26}^4-3\theta_{26}^3+3\theta_{26}^2-1)\zeta_{26},\, -4\zeta_{26}+x,$ $\frac{1}{13}t(2-3\theta_{26}+(\theta_{26}^2+5\theta_{26}+1)\zeta_{26}-(1+\theta_{26})x+\zeta_{26}x)\big\rangle$ mit $t=20\theta_{26}^5-46\theta_{26}^4-50\theta_{26}^3+155\theta_{26}^2-45\theta_{26}-20$	$(12\cdot 1)^{-1}\cdot 1$
$n = 28$		$\frac{13}{21}$
	$\langle 1,\, \zeta_{28},\, x,\, \zeta_{28}x\rangle$	$(28\cdot 2)^{-1}\cdot 1$
$1,7$	$\big\langle 1,\, \theta_{28}\zeta_{28},\, 2\zeta_{28}+x,\, \frac{1}{7}\theta_{28}^5((\theta_{28}+2)\zeta_{28}+3x+\zeta_{28}x)\big\rangle$	$(7\cdot 1)^{-1}\cdot 1$
$2,7$	$\langle 1,\, \theta_{28}^2\zeta_{28},\, (2-\theta_{28})\zeta_{28}+x,$ $\frac{1}{7}\theta_{28}^4(-\theta_{28}+(2-\theta_{28}^3+3\theta_{28}^2-2\theta_{28})\zeta_{28}+(2\theta_{28}+3)x+\zeta_{28}x)\big\rangle$	$(4\cdot 1)^{-1}\cdot 1$
$3,7$	$\langle 1,\, \theta_{28}^3\zeta_{28},\, (2-\theta_{28}^2-\theta_{28})\zeta_{28}+x,$ $\frac{1}{7}\theta_{28}^3(\theta_{28}^2-\theta_{28}+t\zeta_{28}+(3-\theta_{28}^2+2\theta_{28})x+\zeta_{28}x)\big\rangle$ mit $t=2-2\theta_{28}^5+\theta_{28}^2-2\theta_{28}$	$(3\cdot 2)^{-1}\cdot 1$
$4,7$	$\langle 1,\, \theta_{28}^4\zeta_{28},\, (\theta_{28}^3-\theta_{28}^2-\theta_{28}+2)\zeta_{28}+x,$ $\frac{1}{7}\theta_{28}^2(t_1+t_2\zeta_{28}+(3-3\theta_{28}^3-\theta_{28}^2+2\theta_{28})x+\zeta_{28}x)\big\rangle$ mit $t_1=3\theta_{28}^3+\theta_{28}^2-\theta_{28},\ t_2=\theta_{28}^5+3\theta_{28}^4+\theta_{28}^3+\theta_{28}^2+5\theta_{28}+9$	$(12\cdot 2)^{-1}\cdot 1$
$n = 30$		$\frac{1}{30}$
	$\langle 1,\, \zeta_{30},\, x,\, \zeta_{30}x\rangle$	$(30\cdot 2)^{-1}\cdot 1$
$1,5$	$\langle 1,\, (1-\theta_{30})\zeta_{30},\, x,$ $\frac{1}{5}(1-\theta_{30}^3+3\theta_{30}^2-3\theta_{30})(-1+2\zeta_{30}+2x+\zeta_{30}x)\big\rangle$	$(60\cdot 1)^{-1}\cdot 1$

$n = 36$		$\frac{31}{36}$
	$\langle 1,\ \zeta_{36},\ x,\ \zeta_{36}x\rangle$	$(36\cdot 2)^{-1}\cdot 1$
$1,3$	$\langle 1,\ \theta_{36}\zeta_{36},\ -\zeta_{36}+x,\ \frac{1}{3}\theta_{36}^5((\theta_{36}+1)\zeta_{36}+x+\zeta_{36}x)\rangle$	$(9\cdot 2)^{-1}\cdot 1$
$2,3$	$\langle 1,\ \theta_{36}^2\zeta_{36},\ (1+\theta_{36})\zeta_{36}+x,$ $\frac{1}{3}\theta_{36}^4(\theta_{36}+(\theta_{36}^3+\theta_{36}+1)\zeta_{36}+x+\zeta_{36}x)\rangle$	$(3\cdot 2)^{-1}\cdot 1$
$3,3$	$\langle 1,\ \theta_{36}^3\zeta_{36},\ \frac{1}{3}\theta_{36}^3(\theta_{36}^2+\theta_{36}+t\zeta_{36}+(1-\theta_{36}^2)x+\zeta_{36}x),$ $(1-\theta_{36}^2-\theta_{36})\zeta_{36}+x\rangle$ mit $t=\theta_{36}^5-\theta_{36}^3+\theta_{36}^2+\theta_{36}+1$	$(3\cdot 1)^{-1}\cdot 1$
$3,3$	$\langle 1,\ \theta_{36}^3\zeta_{36},\ (\theta_{36}+1)\zeta_{36}+x,$ $\frac{1}{3}\theta_{36}^3((\theta_{36}^2+\theta_{36})+(\theta_{36}^4+\theta_{36}^3+\theta_{36}+1)\zeta_{36}+x+\zeta_{36}x)\rangle$	$(12\cdot 2)^{-1}\cdot 1$
$4,3$	$\langle 1,\ \theta_{36}^4\zeta_{36},\ (\theta_{36}^3-\theta_{36}^2-\theta_{36}-1)\zeta_{36}+x,$ $\frac{1}{3}\theta_{36}^2(\theta_{36}^3+\theta_{36}^2+\theta_{36}-t\zeta_{36}+(1-\theta_{36}^3-\theta_{36}^2)x+\zeta_{36}x)\rangle$ mit $t=\theta_{36}^5-\theta_{36}^4-\theta_{36}^2-\theta_{36}+2$	$(4\cdot 1)^{-1}\cdot 1$

$n = 42$		$\frac{1}{6}$
	$\langle 1,\ \zeta_{42},\ x,\ \zeta_{42}x\rangle$	$(42\cdot 2)^{-1}\cdot 1$
$1,7$	$\langle 1,\ (-\theta_{42}+1)\zeta_{42},\ 3\zeta_{42}+x,\ \frac{1}{7}t(-3+(2\theta_{42}-3)\zeta_{42}+\zeta_{42}x)\rangle$ mit $t=-\theta_{42}^5+5\theta_{42}^4-10\theta_{42}^3+10\theta_{42}^2-5\theta_{42}+1$	$(7\cdot 2)^{-1}\cdot 1$
$1,3$	$\langle 1,\ (35\theta_{42}^5+147\theta_{42}^4+57\theta_{42}^3-278\theta_{42}^2-223\theta_{42}-27)\zeta_{42},$ $(1+\theta_{42})\zeta_{42}+x,\ \frac{1}{3}t_1(-\theta_{42}^2-1+t_2\zeta_{42}+(1-\theta_{42}^2)x+\zeta_{42}x)\rangle$ mit $t_1=\theta_{42}^5-\theta_{42}^4-5\theta_{42}^3+4\theta_{42}^2+6\theta_{42}, t_2=\theta_{42}^5-\theta_{42}^3+\theta_{42}^2+\theta_{42}$	$(12\cdot 1)^{-1}\cdot 1$

Die geraden $n\in\mathbb{N}$ mit $8=[\mathbb{Q}(\zeta_n):\mathbb{Q}]=\frac{1}{2}\varphi(n)$ sind $32, 34, 40, 48$ und 60. Für $n=32$ war es mir nicht möglich, alle Konjugationsklassen zu bestimmen. Denn bei einigen der zu testenden Vertreter war die Automorphismengruppe mit dem in MAGMA implementierten Algorithmus nicht innerhalb von 2 Tagen zu bestimmen. Für die anderen oben genannten n habe ich jeweils Vertreter der R-Maximalordnungen bestimmt. Da es jedoch sehr viele gibt, gebe ich hier nur die Zerlegung der Eichlerschen Maßformel an:

Da alle R-Maximalordnungen die Klassenzahl $H_i = 1$ haben, ist lediglich $\omega_i^1\cdot\omega_i^{nq}$ aufgelistet.
In der ersten Zeile steht jeweils wieder ein Paar k, p, darunter steht die Zerlegung $\omega_i^1\cdot\omega_i^{nq}$ von den Vertretern, die ich als Linksordnungen von Rechtsidealen des k-ten Vertreters $\mathfrak{M}_k$ zwischen $p\mathfrak{M}_k$ und $\mathfrak{M}_k$ gefunden habe. Haben m dieser Linksordnungen dieselbe Zerlegung $\omega_i^1\cdot\omega_i^{nq}$ ist dies durch ein „$m\times$“ deutlich gemacht.

$n=34:$ Typenzahl $T=7$, $Maß=\frac{146}{51}$

k,p		1,17	2,17	3,17	4,17
$\omega_i^1\cdot\omega_i^{nq}$	$34\cdot 1$	$2\cdot 1$	$2\times(1\cdot 1)$	$(6\cdot 1),\ (12\cdot 1)$	$12\cdot 1$

$n=40:$ $T=25$, $Maß=\frac{287}{24}$

k,p		1,2	1,5	1,3	2,2	2,5
$\omega_i^1\cdot\omega_i^{nq}$	$40\cdot 2$	$8\cdot 2$	$(60\cdot 1),\ (5\cdot 1)$	$2\times(1\cdot 2),\ (4\cdot 1)$	$(24\cdot 1),\ (8\cdot 1)$	$(12\cdot 1),\ (1\cdot 1)$

2,3	3,5	4,5	4,3	9,2
$4\times(1\cdot 1),\ 2\times(3\cdot 2)$	$3\cdot 1$	$4\times(2\cdot 1)$	$2\times(1\cdot 1)$	$2\cdot 1$

$n = 48: \quad T = 39, \quad Maß = 365/16$

k,p		1,2	2,2	3,2	4,2	5,2	7,2	8,2	9,2
$\omega_i^1 \cdot \omega_i^{nq}$	48·2	16·2	16·1	8·1	(8·1), (24·1)	4·1	2 × (4·1)	2·1	2·1

10,2	11,2	12,2	13,2	14,2	15,2	16,2	17,2	18,2
2 × (2·1)	2 × (2·1)	1·1	1·1	1·1	1·1	2 × (1·1)	2 × (1·1)	(3·1), (1·1)

19,2	20,2	21,2	25,2	27,2	28,2	29,2	30,2	31,2
(3·1), (1·1)	2 × (1·1)	2 × (1·1)	2 × (1·2)	2 × (1·2)	1·2	1·2	1·2	1·2

$n = 60: \quad T = 9, \quad Maß = 2$

k,p		1,2	1,3	2,2	1,5	1,59	8,2
$\omega_i^1 \cdot \omega_i^{nq}$	60·2	12·2	(60·1), (3·1)	2 × (4·1)	5·2	1·2	1·2

Literaturverzeichnis

[CB05] Cannon, John J. (Hrsg.) ; Basma, Wieb (Hrsg.): *Handbook of Magma Functions*. 2.12. Sydney: School of Mathematics and Statistics, University of Sydney, 2005. – siehe `http://magma.maths.usyd.edu.au/magma/`

[Deu68] Deuring, Max: *Ergebnisse der Mathematik und ihrer Grenzgebiete*. Bd. 41: *Algebren*. Springer-Verlag, 1968

[Eic55] Eichler, Martin: Zur Zahlentheorie der Quaternionen-Algebren. In: *J. Reine u. Angew. Math.* 195 (1955), S. 127–151. – Berichtigung in: *J. Reine u. Angew. Math.* 197 (1957), S. 220

[FT91] Fröhlich, Albrecht ; Taylor, Martin J.: *Cambridge studies in advanced mathematics*. Bd. 27: *Algebraic number theory*. Cambridge University Press, 1991

[HR94] Holt, Derek F. ; Rees, Sarah: Testing modules for irreducibility. In: *J. Austral. Math. Soc.* 57 (1994)

[Lam91] Lam, Tsit-Yuen: *Graduate Texts in Mathematics*. Bd. 131: *A First Course in Noncommutative Rings*. Springer-Verlag, 1991

[Neb98] Nebe, Gabriele: Finite quaternionic matrix groups. In: *Represent. Theory* 2 (1998), S. 106–223

[Neb03] Nebe, Gabriele: *Vorlesungsmitschrift Algebraische Zahlentheorie*. Universität Ulm, Sommersemester 2003

[Neu92] Neukirch, Jürgen: *Algebraische Zahlentheorie*. Springer-Verlag, 1992

[Odl89] Odlyzko, Andrew M.: Bounds for discriminants and related estimates for class numbers, regulators and zeros of zeta functions: a survey of recent results. In: *Seminaire de Theorie des Nombres, Bordeaux*, 1989 (1-15)

[O'M00] O'Meara, Onorato T.: *Introduction to Quadratic Forms*. Springer-Verlag, 2000

[PAR05] The PARI Group (Hrsg.): *PARI/GP, version* 2.2.10 (alpha). Bordeaux: The PARI Group, 2005. – available from `http://pari.math.u-bordeaux.fr/`

[PS97] Plesken, Wilhelm ; Souvignier, Bernd: Computing Isometries of Lattices. In: *Journal of Symbolic Computation* 24 (1997), S. 327–334

[Rei03] Reiner, Irving: *Maximal Orders*. Oxford Science Publications, 2003

[Row91] Rowen, Louis H.: *Ring Theory - Student Edition*. Academic Press, 1991

[Sch85] Scharlau, Winfried: *Quadratic and Hermitian Forms*. Springer-Verlag, 1985

[Vig80] Vignéras, Marie-France: *Lecture Notes in Mathematics*. Bd. 800: *Arithmétique des Algebrès de Quaternions*. Springer-Verlag, 1980

[Was96] Washington, Lawrence C.: *Graduate Texts in Mathematics*. Bd. 83: *Introduction to Cyclotomic Fields*. 2nd edition. Springer-Verlag, 1996

Ehrenwörtliche Erklärung

Ich erkläre hiermit ehrenwörtlich, dass ich die vorliegende Arbeit selbstständig angefertigt habe; die aus fremden Quellen direkt oder indirekt übernommenen Gedanken sind als solche kenntlich gemacht. Die Arbeit wurde bisher keiner anderen Prüfungsbehörde vorgelegt und auch noch nicht veröffentlicht.

Ich bin mir bewusst, dass eine unwahre Erklärung rechtliche Folgen haben wird.

Ulm, den 30. August 2005 _____

(Unterschrift)