universität wien

DIPLOMARBEIT

Titel der Diplomarbeit

„Über maximale Ordnungen in Normrestalgebren“

Verfasser
Victoria Döller

angestrebter akademischer Grad
Magistra der Naturwissenschaften (Mag.rer.nat)

Wien, im Januar 2013

Studienkennzahl lt. Studienblatt:	A 405
Studienrichtung lt. Studienblatt:	Mathematik
Betreuer:	Univ.-Prof. Dr. Joachim Schwermer

Inhaltsverzeichnis

Einleitung

Die algebraische Zahlentheorie beschäftigt sich schon lange und in vielerlei Hinsicht mit Quaternionenalgebren, unter anderem auch mit der Frage nach maximalen Ordnungen darin. Weit weniger bekannt sind die sogenannten Normrestalgebren, die Thema dieser Arbeit sind und die Quaternionenalgebren als Spezialfall beinhalten. Diese Algebren setzen einen Körper K voraus, der zu $n \in \mathbb{N}$ eine primitive n-te Einheitswurzel ζ enthält und dessen Charakteristik n nicht teilt. Dann existiert eine n^2-dimensionale Algebra $A_\zeta(a, b \,|\, K)$, $a, b \in K^*$ mit K-Basis $\{u^i v^j, 0 \leq i, j \leq n-1\}$, sodass gilt

$$u^n = a \cdot 1_{A_\zeta}, \quad v^n = b \cdot 1_{A_\zeta} \quad \text{und} \quad uv = \zeta vu,$$

genannt die Normrestalgebra zu a, b über K.

Offensichtlich stimmt die 4-dimensionale Normrestalgebra $A_{-1}(a, b \,|\, K)$ mit der Quaternionenalgebra $Q(a, b \,|\, K)$ überein. Viele wohlbekannte Eigenschaften der Quaternionenalgebren lassen sich aus den allgemeineren Eigenschaften der Normrestalgebren ableiten, welche im zweiten Kapitel erarbeitet werden. Dort wird unter anderem gezeigt, dass diese zentral und einfach sind und ähnlich zu zyklischen Algebren, also zu Algebren, die eine zyklische Galoiserweiterung L von K enthalten, deren Grad $[L : K]$ gleich dem Grad der Algebra ist. Ist K ein lokaler oder globaler Körper, lässt sich sogar die Isomorphie zu einer zyklischen Algebra beweisen. Grundlegend für alle weiteren Resultate in dieser Arbeit sind die Isomorphieeigenschaften aus Satz 2.5 sowie der Zusammenhang mit Matrizenalgebren in Abhängigkeit der Elemente a und b aus Satz 2.6. Außerdem werden über lokalen Körpern, deren Restkörpercharakteristik den Grad der Normrestalgebra nicht teilt, alle Isomorphieklassen der Algebra bestimmt.

Sei K ein algebraischer Zahlkörper und R der Ring der ganzen Zahlen in K. Abgesehen von der Frage nach allgemeinen Eigenschaften dieser Algebren beschäftigt sich die vorliegende Arbeit mit R-Ordnungen in Normrestalgebren $\mathcal{A}$ über K, das heißt mit endlich erzeugten R-Moduln, die ein Ring mit $1_\mathcal{O} = 1_\mathcal{A}$ sind und eine K-Basis der Algebra enthalten. Von besonderem Interesse sind dabei maximale Ordnungen, also Ordnungen die in keiner anderen Ordnung echt enthalten sind. Soweit ersichtlich, gibt es in der Literatur bis jetzt noch keine Abhandlung über Ordnungen in Normrestalgebren, daher bietet sich an, zuerst Spezialfälle zu betrachten und anschließend zu versuchen, die gewonnenen Ergebnisse zu verallgemeinern. Das führt zurück zu den Quaternionenalgebren.

Unter den vielen Arbeiten, die es dort zu dem Thema schon gibt, findet sich ein Artikel von Stefan Lemurell [Lem]. Dort beschreibt er eine Methode, mit der man unter gewissen Voraussetzungen zu einer gegebenen Quaternionenalgebra eine isomorphe Algebra konstruieren und in der letzteren explizit Basiselemente einer maximalen Ordnung bestimmen kann, siehe [Lem, 2.10 Proposition, 6.9 Proposition]. Er löst das Problem damit in einer Allgemeinheit, die einem, wie er selbst sagt, in keiner anderen bisher bekannten Arbeit begegnet. Zusammenfassend lässt sich folgendes Theorem formulieren (siehe Theorem 5.12 und Theorem 5.15):

Theorem. *Seien K ein algebraischer Zahlkörper und R der Ring der ganzen Zahlen in K und sei $\mathcal{Q}$ eine Quaternionenalgebra über K, deren Diskriminante $d(\mathcal{Q})$ ein Hauptideal mit*

Erzeuger d ist, sodass $\sigma(d) < 0$ für alle reellen Stellen σ, bei denen $\mathcal{Q}$ verzweigt. Dann existiert ein Primelement a in R, sodass gilt

$$\mathcal{Q} \cong Q(a, d \,|\, K), \quad a \equiv m^2 \mod (4) \quad \textit{und} \quad d \equiv x^2 \mod (a),$$

mit $x, m \in R$ und die Elemente

$$e_1 = \frac{i - m}{2} \qquad \textit{und} \qquad e_2 = \frac{k - xi}{a}$$

erzeugen eine maximale R-Ordnung in $Q(a, d \,|\, K)$ mit Basis $\{1, e_1, e_2, e_1 e_2\}$.

Es sei darauf hingewiesen, dass es notwendig ist $\sigma(d) < 0$ vorauszusetzen für alle reellen Stellen σ, bei denen $\mathcal{Q}$ verzweigt, obwohl diese Voraussetzung in Lemurells Artikel nicht gefordert wird.

Ausgehend von Lemurells Artikel ist nun das Ziel dieser Arbeit eine ähnliche Methode allgemein für Normrestalgebren zu konstruieren. Dies wird für Normrestalgebren gelingen, deren Grad eine Primzahl ist und deren Diskriminante bestimmte günstige Eigenschaften mitbringt, wobei hier die Diskriminante $d(\mathcal{A})$ einer zentralen, einfachen, n^2-dimensionalen Algebra $\mathcal{A}$ definiert ist als das Ideal

$$d(\mathcal{A}) = \prod_{\mathfrak{p}} \mathfrak{p}^{n - \kappa_{\mathfrak{p}}}$$

und $\kappa_{\mathfrak{p}}$ die lokale Kapazität bezeichnet. Folgendes Theorem fasst die Ergebnisse zusammen, siehe Theorem 6.2 und Theorem 6.9:

Theorem. *Seien $n > 2$ eine Primzahl und K ein algebraischer Zahlkörper, der eine primitive n-te Einheitswurzel ζ enthält und bezeichne mit R den Ring der ganzen Zahlen in K. Sei weiters $\mathcal{A}_\zeta$ eine n^2-dimensionale Normrestalgebra über K, die bei allen Primstellen zerfällt, die (n) teilen und deren Diskriminante $d(\mathcal{A}_\zeta)$ ein Hauptideal mit Erzeuger d ist, sodass d eine $(n-1)$-te Wurzel δ in R besitzt. Dann existiert ein Primelement $a \in R$, sodass gilt*

$$\mathcal{A}_\zeta \cong A_\zeta(a, d \,|\, K), \quad a \equiv 1 \mod (n)^2 \quad \textit{und} \quad \delta \equiv x^n \mod (a)$$

für ein $x \in R$ und die Elemente

$$e_1 = \frac{u - 1}{1 - \zeta} \;\; \textit{und} \;\; e_2 = \frac{u^{n-1} v^{n-1} - x \delta^{n-2} u^{n-1}}{\delta^{n-2} a}$$

sind ganz. Außerdem sind die Elemente

$$1,\ e_1,\ e_1^2, ...,\ e_1^{n-1},\ e_2,\ e_1 e_2,\ e_1^2 e_2, ...,\ e_1^{n-1} e_2^{n-1}$$

K-linear unabhängig und der freie R-Modul $\mathcal{O}$, der von dieser Basis erzeugt wird, ist eine R-Ordnung in $A_\zeta(a, d \,|\, K)$ und maximal.

Im Folgenden soll ein Überblick gegeben werden über den Aufbau dieser Methode und die restlichen Kapitel dieser Arbeit.

Kapitel 3 beinhaltet alle notwendigen Definitionen und Resultate über Ordnungen. Dabei ist die Diskriminante $d(\mathcal{O})$ einer Ordnung $\mathcal{O}$ von besonderem Interesse, da Lemurells Methode auf folgenden zwei Ergebnissen beruht: Sei R ein Dedekindring, dessen Quotientenkörper K ein globaler Körper ist. Dann ist die Diskriminante einer maximalen R-Ordnung in einer

zentralen, einfachen, n^2-dimensionalen K-Algebra $\mathcal{A}$ eindeutig und zwar genau die n-te Potenz der Diskriminante $d(\mathcal{A})$ der Algebra (Satz 3.9). Sind weiters $\mathcal{O} \subset \mathcal{O}'$ zwei R-Ordnungen in $\mathcal{A}$, die eine Basis besitzen, so erfüllt die Determinante $[\mathcal{O}' : \mathcal{O}]$ der Übergangsmatrix der Basen folgende Gleichung:

$$d(\mathcal{O}) = [\mathcal{O}' : \mathcal{O}]^2 \cdot d(\mathcal{O}')$$

(Lemma 3.8). Kennt man nun die Diskriminante einer Ordnung mit Basis, so kennt man auch die Determinante der Übergangsmatrix zu einer maximalen Ordnung mit Basis (sofern eine solche existiert). Aus diesem Grund schließt dieses Kapitel mit der Berechnung der Diskriminante der Ordnung $\mathcal{O}_\zeta$ in einer Normrestalgebra $A_\zeta(a, b \,|\, K)$ über einem algebraischen Zahlkörper K, die von der Standardbasis $\{u^i v^j, 0 \leq i, j \leq n-1\}$ von $A_\zeta(a, b \,|\, K)$ über dem Ring der ganzen Zahlen R erzeugt wird.

Kapitel 4 behandelt das Hilbertsymbol und dessen Eigenschaften. Die Definition entstammt der Klassenkörpertheorie und setzt einen lokalen Körper K mit maximalem Ideal $\mathfrak{p}$ voraus, der die n-ten Einheitswurzeln μ_n enthält. Das n-te Hilbertsymbol ist eine Abbildung auf diesem Körper:

$$\left(\frac{\cdot,\cdot}{\mathfrak{p}}\right)_n : K^* \times K^* \longrightarrow \mu_n.$$

Es wird gezeigt, dass das n-te Hilbertsymbol $\left(\frac{a,b}{\mathfrak{p}}\right)_n$ die Isomorphieklasse der n^2-dimensionalen Normrestalgebra $A_\zeta(a, b \,|\, K)$ parametrisiert, wenn die Restkörpercharakteristik kein Teiler von n ist. Ist diese Bedingung nicht erfüllt, so gibt es keinen offensichtlichen Weg diesen Zusammenhang nachzuweisen. Darum fehlt die Möglichkeit, das Verzweigungsverhalten von Normrestalgebren bei den Stellen zu vergleichen, die das Ideal (n) teilen.

Kapitel 5 beschäftigt sich mit Quaternionenalgebren. Hier werden die bisherigen Ergebnisse zu einem Beweis des ersten oben erwähnten Theorems zusammengesetzt (etwas ausführlicher als in Lemurells Artikel). Erfüllt eine Quaternionenalgebra $\mathcal{Q}$ die Voraussetzungen des Theorems, so kann man eine isomorphe Algebra $Q(a, d \,|\, K)$ konstruieren, wobei a ein geeignetes Primelement ist und d ein Erzeuger der Diskriminante der Algebra $\mathcal{Q}$ mit den vorausgesetzten Eigenschaften. Der Beweis der Isomorphie beruht hauptsächlich auf dem Hilbertsymbol. Wegen des Zusammenhangs des zweiten Hilbertsymbols mit quadratischen Formen lässt sich hier das Verzweigungsverhalten auch bei den Stellen kontrollieren, die das Ideal (2) teilen (siehe Abschnitt 5.2 Quadratischer Defekt). Wendet man die Resultate aus Kapitel 3 auf diese neue Algebra an, so sieht man, dass sowohl die Diskriminante der Ordnung $\mathcal{O}_\zeta$ als auch die Determinante der Übergangsmatrix von einer maximalen Ordnung mit Basis, die $\mathcal{O}_\zeta$ enthält, zu $\mathcal{O}_\zeta$ besonders einfach aussehen. Daraufhin gelingt es Lemurell Basiselemente zu finden, die die gewünschten Gleichungen erfüllen und damit eine maximale Ordnung in $Q(a, d \,|\, K)$ erzeugen.

Kapitel 6 widmet sich nun der Aufgabe, die eben dargelegte Methode Lemurells auf Normrestalgebren zu verallgemeinern, soweit dies möglich ist. Dazu wird als erstes in Anlehnung an Kapitel 5 zu einer gegebenen Normrestalgebra $\mathcal{A}_\zeta$ über einem algebraischen Zahlkörper K eine isomorphen Algebra $A_\zeta(a, d \,|\, K)$ konstruiert, wobei d wieder einen Erzeuger der Diskriminante $d(\mathcal{A}_\zeta)$ bezeichne, die als Hauptideal vorausgesetzt ist. Mit Hilfe des Hilbertsymbols kann man das Verzweigungsverhalten der Algebren überall vergleichen, außer bei den Stellen, die (n) teilen, darum verlangt man weiters, dass $\mathcal{A}_\zeta$ bei diesen Stellen zerfällt, siehe Theorem 6.2. Während sich dieses Resultat noch unabhängig vom Grad der Algebra beweisen lässt, erweist es sich bei der Betrachtung von Ordnungen in der Algebra $A_\zeta(a, d \,|\, K)$ als erhebliche Erleichterung, wenn ihr Grad eine Primzahl ist und d eine $(n-1)$-te Wurzel δ

im Ring der ganzen Zahlen R in K besitzt. In diesem Fall lässt sich die Determinante der Übergangsmatrix einer maximalen Ordnung $\mathcal{O}_m$ mit Basis zu $\mathcal{O}_\zeta$ als Produkt ganzer Zahlen und einer Einheit in R schreiben. Darauf folgt der schwierigste Teil dieser Arbeit, das Finden von Elementen, die die eben erwähnte Gleichung erfüllen und somit eine maximale Ordnung erzeugen. Auch hier hilft es, zunächst für die ersten Spezielfälle eine Lösung zu suchen, also für 3^2-dimensionale und 5^2-dimensionale Normrestalgebren. Hat man erst in diesen Fällen Basiselemente einer maximalen Ordnung in $A_\zeta(a, d \,|\, K)$ gefunden, lässt sich an diesen eine allgemeine Lösung ablesen. Allerdings ist etwas mehr Aufwand notwendig um nachzuweisen, dass die gefundenen Elemente eine maximale Ordnung erzeugen. Vor allem die Berechnung der Determinante der Übergangsmatrix benötigt einige zusätzliche Überlegungen. Bei genauer Betrachtung der ersten Spezialfälle bemerkt man, dass sich die Basis der maximalen Ordnung und die Basis von $\mathcal{O}_\zeta$ in bestimmter Weise anordnen lassen, sodass die Übergangsmatrix obere Dreiecksform hat. Der Beweis dieser Tatsache im Allgemeinen liefert zugleich die Einträge der Hauptdiagonale und mit einiger weiterer, elementarer Rechenarbeit folgt das finale Ergebnis dieser Arbeit. Die Elemente erzeugen eine Ordnung mit Basis, die maximal ist. Das heißt unter obigen Voraussetzungen ist es gelungen, Lemurells Methode auf Normrestalgebren zu verallgemeinern.

1 Grundlagen

Dieses Kapitel beinhaltet alle wesentlichen Definitionen und Resultate, auf die die vorliegende Arbeit aufbaut. Um sich in diese grundlegenden Gebiete einzulesen, sind vor allem die Werke von J. Neukirch [Neu99] und I. Kersten [Ker07] zu empfehlen.

1.1 Bewertete, vollständige und lokale Körper

Ist A eine Algebra über einem algebraischen Zahlkörper K, so interessiert man sich auch für die Struktur von A über Vervollständigungen von K. Dort tauchen folgende Begriffe auf:

Definition 1.1. Sei R ein Dedekindring mit Quotientenkörper $\mathrm{Quot}(R) = K$ und sei A eine zentrale, einfache K-Algebra. Bezeichne mit K_ν die Vervollständigung von K an der Stelle ν und mit $A_\nu = K_\nu \otimes_K A$ die Algebra über K_ν. Nach dem Struktursatz von Wedderburn gibt es eine Divisionsalgebra D_ν, $[D_\nu : K_\nu] = m_\nu^2$, sodass $A_\nu \cong M_{\kappa_\nu}(D_\nu)$. Man nennt κ_ν die *lokale Kapazität* und m_ν den *lokalen Index* von A bei ν und man sagt A verzweigt bei ν, wenn $m_\nu > 1$, bzw. A zerfällt bei ν, wenn $m_\nu = 1$. Ist n der Grad von A über K, so gilt offensichtlich $n = \kappa_\nu \cdot m_\nu$.

Um mit Algebren über Vervollständigungen von Zahlkörpern oder allgemeiner über lokalen Körpern arbeiten zu können, seien hier alle Definitionen und Resultate, die später gebraucht werden, zusammengefasst, siehe auch [Neu99, Chapter II, The Theory of Valuations, S.99-S.182]. Um Unklarheiten zu vermeiden, sei darauf hingewiesen, dass Neukirch und die meisten anderen Autoren, auf die sich diese Arbeit bezieht, unter einem lokalen Körper einen diskret bewerteten, vollständigen Körper mit endlichem Restklassenkörper verstehen und im Folgenden mit dieser Definition gearbeitet wird.
In einem lokalen Körper K bezeichne mit R den Bewertungsring, mit $\mathfrak{p}$ das eindeutige maximale Ideal in R und mit p die Restkörpercharakteristik.

Lemma 1.2. *Die multiplikative Gruppe eines lokalen Körpers lässt sich zerlegen in*

$$K^* = \langle \pi \rangle \times \mu_{q-1} \times U^{(1)},$$

dabei ist π ein Primelement in R, $\langle \pi \rangle = \{\pi^k, k \in \mathbb{Z}\}$, q die Mächtigkeit des Restklassenkörpers $k = R/\mathfrak{p}$, weiters μ_{q-1} die Menge der $(q-1)$-ten Einheitswurzeln und $U^{(1)} = 1+\mathfrak{p}$ die Einseinheitengruppe. Insbesondere enthält K die $(q-1)$-ten Einheitswurzeln.

Beweis. [Neu99, 5.3 Proposition, S.136] □

Gilt weiters $\mu_n \subset K$ und $p \nmid n$, so ist $pr : \mu_n \to k^*, \zeta \mapsto \zeta \bmod \mathfrak{p}$ injektiv und damit $\mu_n \subset \mu_{q-1}$ und $n \mid q-1$.

Lemma 1.3. *Gilt $p \nmid n$ und $x \in K^*$, so ist die Körpererweiterung $K(\sqrt[n]{x})/K$ genau dann unverzweigt, wenn $x \in R^* \cdot K^{*n}$.*

Beweis. [Neu99, 3.3 Lemma, S.335] □

Satz 1.4 (Normensatz)**.** *Sei K ein lokaler Körper mit Bewertungsring R_K und L eine endliche, unverzweigte Körpererweiterung von K mit Bewertungsring R_L. Dann ist jede Einheit $x \in R_K^*$ Norm eines Elements $z \in R_L^*$.*

Beweis. [Ker07, 13.5 Normensatz, S.118] □

Satz 1.5 (Approximationssatz)**.** *Seien $|\ |_1, ..., |\ |_r$ paarweise inäquivalente Absolutbeträge auf einem beliebigen Körper K und seien Elemente $a_1, ..., a_r \in K$ gegeben. Dann existiert für jedes $\varepsilon > 0$ ein $x \in K$, sodass gilt*

$$|x - a_i|_i < \varepsilon \ \forall i = 1, ..., r$$

Beweis. [Neu99, 3.4 Approximation Theorem, S.117] □

Folgender Satz liefert zum einen Hensels Lemma, auf das sich viele Aussagen in dieser Arbeit stützen, und zum anderen ein Korollar, das immer dann hilfreich sein wird, wenn Hensels Lemma nicht zur Anwendung kommen kann.

Satz 1.6. *Sei K ein diskret bewerteter, vollständiger Körper mit Bewertungsring R und maximalem Ideal $\mathfrak{p}$ in R. Seien $g_0(X), h_0(X), f(X)$ Polynome in $R[X]$, sodass*

$$\deg f(X) = \deg g_0(X) + \deg h_0(X)$$

und sodass $f(X)$ und $g_0(X) \cdot h_0(X)$ den gleichen Leitkoeffizienten besitzen.
Sei weiters die Resultante

$$R(g_0, h_0) \not\equiv 0 \bmod \mathfrak{p}^{s+1} \text{ und } f(X) \equiv g_0(X) \cdot h_0(X) \bmod \mathfrak{p}^{2s+1}$$

für ein $s \geq 0$. Dann existieren Polynome $g(X), h(X)$ in $R[X]$, sodass

$$\deg g_0(X) = \deg g(X),\ \deg h_0(X) = \deg h(X),\ f(X) = g(X) \cdot h(X)$$

und

$$g(X) \equiv g_0(X) \mod \mathfrak{p}^{s+1},\ h(X) \equiv h_0(X) \mod \mathfrak{p}^{s+1}$$

Beweis. [Fes93, Ch. II, 1.1, Proposition, S.29] □

Korollar 1.7 (Hensels Lemma)**.** *Seien K ein vollständiger Körper und $\mathfrak{p}$ und R wie im Satz und sei $k := R/\mathfrak{p}$ der Restklassenkörper von K. Sei $f(X) \in R[X]$ ein normiertes Polynom, das modulo $\mathfrak{p}$ eine Faktorisierung*

$$f(X) \equiv \bar{g}(X) \cdot \bar{h}(X) \mod \mathfrak{p}$$

in relativ prime Polynome $\bar{g}(X), \bar{h}(X) \in k[X]$ besitzt. Dann existieren normierte Polynome $g(X), h(X) \in R[X]$, sodass gilt

$$f(X) = g(X)h(X),$$

$$g(X) \equiv \bar{g}(X) \mod \mathfrak{p} \quad \text{und} \quad h(X) \equiv \bar{h}(X) \mod \mathfrak{p}.$$

Beweis. [Fes93, Ch. II, 1.1, Corollary 1, S.30] □

Korollar 1.8. *Seien K ein vollständiger Körper und $\mathfrak{p}$ und R wie im Satz und seien $s \in \mathbb{N}$ und $f(X) \in R[X]$ normiert. Gibt es ein Element $\alpha \in R$ mit*

$$f(\alpha) \equiv 0 \bmod \mathfrak{p}^{2s+1},\ f'(\alpha) \not\equiv 0 \bmod \mathfrak{p}^{s+1},$$

dann existiert auch ein Element $a \in R$, für das gilt

$$a \equiv \alpha \bmod \mathfrak{p}^{s+1} \text{ und } f(a) = 0.$$

Beweis. [Fes93, Ch. II, 1.1, Corollary 2, S.30] □

Eines der Hauptresultate dieser Arbeit stützt sich auf Eigenschaften der schmalen Klassengruppe, eine Verallgemeinerung der Idealklassengruppe, siehe [Mac03, Definiton 0.6.9 & 0.6.10, S.28] und [Nar74, Ch. III, §2, S.92].

Definition 1.9. Sei K ein algebraischer Zahlkörper, R der Ring der ganzen Zahlen in K und sei Ω die Menge aller Stellen von K. Ein *Modulus* in K ist ein formales Produkt

$$\mathcal{M} = \prod_{\mathfrak{p} \in \Omega} \mathfrak{p}^{\nu(\mathfrak{p})}$$

über alle Stellen von K, sodass gilt $\nu_\mathfrak{p} \in \mathbb{N}_0$ und $\nu_\mathfrak{p} > 0$ für nur endlich viele Stellen $\mathfrak{p}$. Außerdem gelte für alle komplexen Stellen $\nu_\mathfrak{p} = 0$ und für alle reellen Stellen $\nu_\mathfrak{p} = 1, 0$. Sei $a \in K^*$. Man schreibt

$$a \equiv^* 1 \mod \mathcal{M}$$

wenn gilt

- $a \in R_\mathfrak{p}$ und $a \equiv 1 \mod \mathfrak{p}^{\nu(\mathfrak{p})}$ für alle endlichen Stellen $\mathfrak{p}$ mit $\nu(\mathfrak{p}) > 0$,
- $\sigma(a) > 0$ für alle Einbettungen σ, die einer unendlichen Stelle $\mathfrak{p}$ von K entsprechen und für die gilt $\nu(\mathfrak{p}) = 1$.

Bezeichne mit $I_K(\mathcal{M})$ die Gruppe der gebrochenen Ideale, die relativ prim sind zu allen Primidealen, deren Stellen $\mathcal{M}$ teilen und mit $P_K(\mathcal{M})$ die Gruppe der gebrochenen Hauptideale $\{aR \mid a \equiv^* 1 \bmod \mathcal{M}\}$. Dann definiert man die *schmale Klassengruppe mit Modulus* $\mathcal{M}$ als den Quotienten $I_K(\mathcal{M})/P_K(\mathcal{M})$.

Wählt man den Modulus $\mathcal{M}$ so, dass gilt $\nu(\mathfrak{p}) = 1$ für alle reellen Stellen $\mathfrak{p}$, so erhält man folgendes Korollar:

Korollar 1.10. *In jeder Klasse von $I_K(\mathcal{M})/P_K(\mathcal{M})$ liegen unendlich viele Primideale.*

Beweis. [Nar74, Korollar 7 zu Proposition 7.8., S. 323] □

1.2 Zyklische Algebren

Wie im nächsten Kapitel noch gezeigt wird, hängen die Algebren, die in dieser Arbeit behandelt werden, die sogenannten Normrestalgebren, eng zusammen mit zyklischen Algebren und erben von ihnen einige nützliche Eigenschaften, die hier kurz zusammengefasst werden. Siehe dazu [Ker07, 10 Zyklische Algebren, S.70-S.77]

Definition 1.11. Man nennt eine zentrale, einfache Algebra A über einem Köper K *zyklisch,* wenn sie eine Galoiserweiterung L von K enthält, deren Galoisgruppe $G(L/K)$ zyklisch ist und für die gilt $dim_K L = dim_L A$.

Satz 1.12. *Sei A eine n^2-dimensionale, zyklische K-Algebra, L die enthaltene zyklische Galoiserweiterung über K vom Grad n und σ ein erzeugendes Element der Galoisgruppe $G = \{\sigma^i, 1 \leq i \leq n\}$. Dann existiert ein $u \in A^*$, sodass $1, u, ..., u^{n-1}$ eine Basis von A über L bilden und es gilt:*

$$u \cdot x = \sigma(x) \cdot u \quad \textit{für alle } x \in L$$

$$u^n =: a \in K^*$$

Beweis. [Ker07, 10.2 Struktursatz, S.82] □

Satz 1.13. *Sei L eine Galoiserweiterung eines Körpers K vom Grad n mit zyklischer Galoisgruppe $\{\sigma^i, 1 \leq i \leq n\}$. Dann gibt es zu jedem $a \in K^*$ eine zyklische K-Algebra A für die gilt*

$$u \cdot x = \sigma(x) \cdot u \quad \forall x \in L \quad \textit{und} \quad u^n = a$$

Man schreibt $A =: (L/K, \sigma, a)$ und $(L/K, \sigma, a)$ entspricht genau dem verschränkten Produkt $(L/K, G, \gamma_a)$, wobei der 2-Kozykel $\gamma_a : G \times G \to L^*$ definiert ist durch

$$\gamma_a(\sigma^i, \sigma^j) = \begin{cases} 1, & \textit{falls } i + j < n \\ a, & \textit{falls } i + j \geq n \end{cases}$$

für $0 \leq i, j \leq n-1$. Weiters ist jede K-Algebra $B = \bigoplus_{i=0}^{n-1} Lv^i$, die $v^n = a$ und $v \cdot x = \sigma(x) \cdot v$ für alle $x \in L$ erfüllt, isomorph zu $(L/K, \sigma, a)$.

Beweis. [Ker07, 10.3 Existenzsatz, S.83] □

Lemma 1.14. *Seien L und σ wie oben und $a, b \in K^*$. Dann sind folgende Algebren ähnlich*

$$(L/K, \sigma, a) \otimes_K (L/K, \sigma, b) \sim (L/K, \sigma, ab).$$

Das heißt es existieren $r, s \in \mathbb{N}$, sodass gilt

$$(L/K, \sigma, a) \otimes_K (L/K, \sigma, b) \otimes_K M_r(K) \cong (L/K, \sigma, ab) \otimes_K M_s(K).$$

Beweis. [Ker07, 10.4 Multiplikativität, S.84] □

Lemma 1.15. *Seien L und σ wie oben. Dann gilt für $a, b \in K^*$*

$$(L/K, \sigma, a) \cong (L/K, \sigma, b) \iff \exists x \in L^* \textit{ mit } a = n_{L/K}(x) \cdot b$$

Beweis. [Ker07, 10.5 Isomorphiekriterium, S.84] □

2 Normrestalgebren

2.1 Konstruktion und allgemeine Eigenschaften

Die Algebren, die in dieser Arbeit im Mittelpunkt des Interesses stehen, sind die sogenannten Normrestalgebren, die als Verallgemeinerung der Quaternionenalgebren aufgefasst werden können. Dieses Kapitel beschäftigt sich mit deren Konstruktion und allgemeinen Eigenschaften, die weitestgehend unabhängig vom zu Grunde liegenden Körper sind, mit deren Zusammenhang mit zyklischen Algebren und im Weiteren mit der speziellen Struktur von Normrestalgebren über algebraischen Zahlkörpern und lokalen Körpern. Siehe auch [Ker07, 14 Normrestalgebren, S.125].

Seien K ein Körper und $n \geq 1$ eine ganze Zahl, sodass $\operatorname{char} K$ kein Teiler von n ist und sodass K eine primitive n-te Einheitswurzel ζ enthält. Seien $a, b \in K^*$ gegeben. Betrachte die kommutative K-Algebra $R = K[X]/(X^n - b)$ mit K-Basis $v^i,\ i = 0, ..., n-1$, wobei $v := X + (X^n - b)$. Die Abbildung

$$\omega : R \longrightarrow R, \qquad \sum_{i=0}^{n-1} a_i v^i \longmapsto \sum_{i=0}^{n-1} a_i \zeta^i v^i$$

ist ein Automorphismus der Ordnung n von R als K-Algebra.

Mit Hilfe von ω definiert man einen Schiefpolynomring $R_\omega[Y]$ mit folgender Multiplikation

$$\Big(\sum_{i\geq 0} a_i Y^i\Big)\Big(\sum_{j\geq 0} b_j Y^j\Big) = \sum_{i,j\geq 0} a_i \omega^i(b_j) Y^{i+j}$$

wobei $a_i, b_j \in R$. Die Ringaxiome sind leicht nachzuprüfen. Für $r \in R$ gilt:

$$Y \cdot r = \omega(r) \cdot Y \quad \text{und}$$

$$Y^n \cdot r = \omega^n(r) \cdot Y^n = r \cdot Y^n,$$

also liegt Y^n im Zentrum und $(Y^n - a)$ ist ein zweiseitiges Ideal in $R_\omega[Y]$. Damit ist $R_\omega[Y]/(Y^n - a) =: A_\zeta(a, b \,|\, K)$ ein Ring und freier R-Modul mit R-Basis u^i, $i = 0, ..., n-1$ wobei $u := Y + (Y^n - a)$.

Für u und v und $0 \leq i, j \leq n-1$ gilt:

$$u^n = a \cdot 1_{A_\zeta},\ v^n = b \cdot 1_{A_\zeta}$$

$$\text{und} \quad uv = \omega(v) \cdot u = \zeta vu.$$

Per Induktion zeigt man:

$$u^i v^j = \zeta^{i \cdot j} v^j u^i \quad \text{für } 1 \leq i, j \leq n.$$

Damit bilden die Elemente $u^i v^j$, $0 \leq i,j \leq n-1$ eine Basis von $A_\zeta(a,b\,|\,K)$ über K und $A_\zeta(a,b\,|\,K)$ ist eine K-Algebra der Dimension n^2, genannt die *Normrestalgebra* zu a,b über K.

Lemma 2.1. *Die Normrestalgebra $A_\zeta(a,b\,|\,K)$ zu $a,b \in K^*$ ist zentral und einfach.*

Beweis. 1. Sei $x \in Z(A_\zeta(a,b\,|\,K)),\ x = \sum_{i,j=0}^{n-1} a_{ij} u^i v^j$. Es gilt

$$u \cdot x = \Big(\sum a_{ij}\zeta^j u^i v^j\Big) \cdot u = \Big(\sum a_{ij} u^i v^j\Big) \cdot u$$

Da $a,b \neq 0$ gilt $a_{ij} = 0$ für $j > 0$ und x hat die Form $x = \sum_{i=0}^{n-1} a_i u^i$. Da aber auch

$$x \cdot v = v \cdot \Big(\sum a_i \zeta^i u^i\Big) = v \cdot \Big(\sum a_i u^i\Big),$$

gilt für $i > 0$ auch $a_i = 0$ und $x = a_0 \cdot 1_{A_\zeta} \in K \cdot 1_{A_\zeta}$. Umgekehrt liegt offensichtlich $K \cdot 1_{A_\zeta} \subset Z(A_\zeta(a,b\,|\,K))$ im Zentrum.

2. Sei $I \neq (0)$ ein zweiseitiges Ideal in $A_\zeta(a,b\,|\,K)$ und $I \ni x = \sum a_{ij} u^i v^j,\ x \neq 0$. Sei $\operatorname{supp}(x) := \{(i,j) \mid a_{ij} \neq 0\}$ der Träger von x. Falls $|\operatorname{supp}(x)| = 1$, so ist $x = a_{ij} u^i v^j$ eine Einheit mit Inversem $v^{n-j} u^{n-i} (a_{ij} ab)^{-1}$. Deshalb sei $1 < |\operatorname{supp}(x)|$ minimal angenommen. Setze
$$x' = \zeta^k vx - xv = \sum (\zeta^k - \zeta^i) a_{ij} \cdot v u^i v^j,$$
wobei k so gewählt sei, dass ein l existiert, sodass $(k,l) \in \operatorname{supp}(x)$. Dann ist $x' \in I$ und falls nicht gilt $a_{ij} = 0$ für alle $i \neq k$, so ist $x' \neq 0$ und $|\operatorname{supp}(x')| < |\operatorname{supp}(x)|$. Ist $x' = 0$, so setze
$$x'' = \zeta^l xu - ux = \sum (\zeta^l - \zeta^j) a_{ij} \cdot u^i v^j u$$
Dann ist $x'' \neq 0$, da sonst $|\operatorname{supp}(x)| = 1$, und x'' hat echt kleineren Träger als x. Da der Träger von x minimal gewählt war, ist das ein Widerspruch und es gilt $I = A_\zeta(a,b\,|\,K)$. □

Lemma 2.2. *Sei K wie oben mit primitiver n-ter Einheitswurzel ζ und $a,b \in K^*$. Ist A eine K-Algebra mit Elementen $x,y \in A$, sodass gilt $x^n = a, y^n = b$ und $xy = \zeta yx$, dann gibt es einen injektiven K-Algebrenhomomorphismus*

$$\varphi : A_\zeta(a,b\,|\,K) \longrightarrow A \quad \textit{mit} \quad \varphi(u) = x \ \textit{ und } \ \varphi(v) = y.$$

Beweis. Da die Elemente $u^i v^j, 0 \leq i,j \leq n-1$ eine Basis von $A_\zeta(a,b\,|\,K)$ als K-Vektorraum bilden, existiert eine lineare Abbildung φ von K-Vektorräumen mit $\varphi(u^i v^j) = x^i y^j$. Offensichtlich ist φ multiplikativ und, da $A_\zeta(a,b\,|\,K)$ einfach ist, auch injektiv. □

Korollar 2.3. *Im Fall $n = 2$ ist $A_{-1}(a,b\,|\,K)$ zur Quaternionenalgebra $Q(a,b\,|\,K)$ isomorph.*

Beweis. Bezeichne mit $\{1,i,j,k\}$ die Standardbasis von $Q(a,b\,|\,K)$. Dann gilt $i^2 = a, j^2 = b$ und $ij = -ji$, und die Aussage folgt sofort aus dem letzten Lemma. □

Lemma 2.4. *Ist n eine Primzahl, so ist $A_\zeta(a,b\,|\,K)$ eine Divisionsalgebra oder isomorph zu $M_n(K)$.*

Beweis. Da es nach dem Strukturssatz von Wedderburn zu jeder einfachen, endlich dimensionalen K-Algebra A eine Divisionsalgebra D über K und eine natürliche Zahl r gibt, sodass $A \cong M_r(D)$, gilt $n^2 = \dim_K A_\zeta(a,b\,|\,K) = r^2 \dim_K D$. Da n eine Primzahl ist können nur die Fälle $r = 1$ oder $r = n$ auftreten. Im ersten Fall ist $A_\zeta(a,b\,|\,K)$ isomorph zur Divisionsalgebra D, im zweiten Fall zu $M_n(K)$. □

Mit Hilfe von Lemma 2.2 lassen sich einige wichtige Eigenschaften der Normrestalgebren zeigen:

Satz 2.5. *Seien K ein Körper, $n \in \mathbb{N}$ teilerfremd zu $\operatorname{char} K$ und K enthalte eine primitive n-te Einheitswurzel ζ. Weiters sei $A_\zeta(a,b\,|\,K)$ die n^2-dimensionale Normrestalgebra zu $a,b \in K^*$. Dann sind als Algebren isomorph:*

1. $A_\zeta(a,b\,|\,K) \cong A_\zeta(\lambda^n a, \mu^n b\,|\,K)$ *für alle* $\lambda,\mu \in K^*$
2. $A_\zeta(a,b\,|\,K) \cong A_\zeta(a,(-1)^{n-1}ab\,|\,K) \cong A_\zeta((-1)^{n-1}ab,b\,|\,K)$
3. $A_\zeta(a,b\,|\,K) \cong A_\zeta(b^{n-1},a\,|\,K) \cong A_\zeta(b,a^{n-1}\,|\,K)$

Beweis.

1. Seien $u,v \in A_\zeta(\lambda^n a, \mu^n b\,|\,K)$ mit $u^n = \lambda^n a, v^n = \mu^n b$ und $uv = \zeta vu$. Dann sind $e_1 = \lambda^{-1}u$ und $e_2 = \mu^{-1}v$ Elemente in $A_\zeta(\lambda^n a, \mu^n b\,|\,K)$ für die gilt $e_1^n = a$ und $e_2^n = b$. Wegen Lemma 2.2 und Dimensionsgleichheit gilt $A_\zeta(a,b\,|\,K) \cong A_\zeta(\lambda^n a, \mu^n b\,|\,K)$.

2. Seien $u,v \in A_\zeta(a,(-1)^{n-1}ab\,|\,K)$ mit $u^n = a, v^n = (-1)^{n-1}ab$ und $uv = \zeta vu$. Die Elemente $e_1 = u$ und $e_2 = a^{-1}u^{n-1}v$ erfüllen $e_1e_2 = v = \zeta e_2e_1$ und ${e_1}^n = a$. Es gilt

$$ {e_2}^n = \zeta^{n(n-1)/2}a^{-n}u^{n(n-1)}v^n = $$

$$ \zeta^{n(n-1)/2}a^{-n}a^{n-1}(-1)^{n-1}ab. $$

   Dabei ist $\zeta^{n(n-1)/2}$ gleich 1, falls n ungerade ist, und gleich -1, falls n gerade ist. Daher gilt ${e_2}^n = b$ und wie oben folgt $A_\zeta(a,(-1)^{n-1}ab\,|\,K) \cong A_\zeta(a,b\,|\,K)$.
   Die zweite Aussage $A_\zeta(a,b\,|\,K) \cong A_\zeta((-1)^{n-1}ab,b\,|\,K)$ erhält man mittels der Elemente $e_1 = b^{-1}uv^{n-1}$ und $e_2 = v$ wobei u,v die Erzeuger von $A_\zeta((-1)^{n-1}ab,b)$ sind.

3. Seien $u,v \in A_\zeta(a,b\,|\,K)$ mit $u^n = a$ und $v^n = b$. Die Elemente $e_1 = v^{n-1}$ und $e_2 = u$ erfüllen ${e_1}^n = b^{n-1}, {e_2}^n = a$ und $e_1e_2 = v^{n-1}u = \zeta e_2e_1$ und analog zu oben gilt $A_\zeta(a,b\,|\,K) \cong A_\zeta(b^{n-1},a\,|\,K)$. Die Elemente $e_1 = v, e_2 = u^{n-1}$ liefern $A_\zeta(a,b\,|\,K) \cong A_\zeta(b,a^{n-1}\,|\,K)$.

□

Ist K ein algebraischer Zahlkörper, so folgt aus dem ersten Punkt des Satzes, dass a und b immer im Ring der ganzen Zahlen R angenommen werden können, da für alle $a',b' \in K^* = \operatorname{Quot}(R)^*$ passende $\mu,\nu \in R$ existieren, sodass $\mu^n a'$ und $\nu^n b'$ in R liegen.

Betrachte nun die Galoiserweiterung $L = K(\sqrt[n]{b})$. Dann ist L Zerfällungskörper von $A_\zeta(a,b\,|\,K)$ und ein Algebrenisomorphismus

$$ A_\zeta(a,b\,|\,K) \otimes_K L \cong A_\zeta(a,b\,|\,L) \longrightarrow M_n(L) $$

ist gegeben durch die Zuordnung

$$u \mapsto U = \begin{pmatrix} 0 & \cdots & 0 & a \\ 1 & \cdots & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \cdots & 1 & 0 \end{pmatrix} \quad \text{und} \quad v \mapsto V = \sqrt[n]{b} \begin{pmatrix} \zeta^{n-1} & 0 & \cdots & 0 \\ 0 & \zeta^{n-2} & & \\ \vdots & & \ddots & \vdots \\ 0 & \cdots & & 1 \end{pmatrix}$$

Man kann leicht nachrechnen, dass $U^n = a, V^n = b$ und $UV = \zeta VU$. Wegen der Dimensionsgleichheit folgt die Isomorphie als L-Algebren.

Enthält K eine n-te Wurzel von b, gilt also $A_\zeta(a, b \,|\, K) \cong M_n(K)$ und über den Isomorphismus $A_\zeta(a, b \,|\, K) \cong A_\zeta(b^{n-1}, a \,|\, K)$ erhält man das gleiche Ergebnis, falls K eine n-te Wurzel von a enthält.

Auch für Teiler r von n erhält man einen Isomorphismus zu einer Matrizenalgebra, falls K eine r-te Wurzel von a oder b enthält.

Satz 2.6. [Ker07, 14.4, Lemma (ii), S.127]
Sind K ein Körper und $n \in \mathbb{N}$, sodass $\operatorname{char} K \nmid n$ *und K eine primitive n-te Einheitswurzel ζ enthält, so gilt für alle Teiler r von n*

$$A_\zeta(a, b^r \,|\, K) \cong M_r(A_{\zeta^r}(a, b \,|\, K)) \cong A_\zeta(a^r, b \,|\, K)$$

wobei $A_{\zeta^r}(a, b \,|\, K)$ die $(n/r)^2$-dimensionale Normrestalgebra zu a, b mit primitiver n/r-ter Einheitswurzel ζ^r ist.

Beweis. Sei $n = mr$. Dann ist ζ^r eine primitive m-te Einheitswurzel. Die Algebra $A_{\zeta^r}(a, b \,|\, K)$ hat erzeugende Elemente u und v für die gilt $u^m = a, v^m = b$ und $uv = \zeta^r vu$. Setze in $M_r(A_{\zeta^r}(a, b \,|\, K))$

$$U = \begin{pmatrix} 0 & \cdots & 0 & u \\ 1 & \cdots & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \cdots & 1 & 0 \end{pmatrix} \quad \text{und} \quad V = \begin{pmatrix} \zeta^{r-1}v & 0 & \cdots & 0 \\ 0 & \zeta^{r-2}v & & \\ \vdots & & \ddots & \vdots \\ 0 & \cdots & & v \end{pmatrix}$$

Dann gilt $U^n = (U^r)^m = u^m = a$ und $V^n = v^n = b^r$ sowie $UV = \zeta VU$ und aus Lemma 2.2 und Dimensionsgleichheit folgt der erste Teil der Behauptung.
Aus Satz 2.5 Punkt 3. und $A_{\zeta^r}(b^{n-1}, a \,|\, K) \cong A_{\zeta^r}(b^{m-1}, a \,|\, K)$ erhält man den zweiten Teil der Aussage. □

Daraus lassen sich weitere Eigenschaften ableiten:

Korollar 2.7. *Sei a in K^*. Dann gilt:*

1. $A_\zeta(a, -a \,|\, K) \cong M_n(K)$
2. $A_\zeta(a, a \,|\, K) \cong M_n(K)$ *für n ungerade und*
   $A_\zeta(a, a \,|\, K) \cong M_{n/2}(Q(a, \zeta \,|\, K))$ *für n gerade.*

Beweis. 1. Wegen Satz 2.5 ist $A_\zeta(a, -a \,|\, K) \cong A_\zeta(a, (-1)^{n-1}(-a/a) \,|\, K)$, also gleich $A_\zeta(a, 1 \,|\, K) \cong M_n(K)$ für n gerade und gleich $A_\zeta(a, -1 \,|\, K) \cong A_\zeta((-1)^{n-1}, a \,|\, K) = A_\zeta(1, a \,|\, K) \cong M_n(K)$ für n ungerade.

2. Ebenso ist $A_\zeta(a,a\,|\,K) \cong A_\zeta(a,(-1)^{n-1}a/a\,|\,K)$, also gleich $A_\zeta(a,1\,|\,K) \cong M_n(K)$ für n ungerade und gleich $A_\zeta(a,-1\,|\,K) = A_\zeta(a,\zeta^{n/2}\,|\,K) \cong M_{n/2}(Q(a,\zeta\,|\,K))$ für n gerade nach Satz 2.6.

□

2.2 Normrestalgebren als zyklische Algebren

Wie die Konstruktion schon vermuten lässt, sind Normrestalgebren ähnlich zu zyklischen Algebren und erben dadurch einige grundlegende Eigenschaften, die im Weiteren oft gebraucht werden.

Satz 2.8. [Ker07, 14.5,Satz (i), S.128]
Seien K ein Körper und $n \in \mathbb{N}$, sodass $\operatorname{char} K \nmid n$ *und K eine primitive n-te Einheitswurzel ζ enthält. Sei $A_\zeta(a,b\,|\,K)$ die n^2-dimensionale Normrestalgebra zu $a,b \in K^*$. Dann ist $A_\zeta(a,b\,|\,K)$ ähnlich zur zyklischen Algebra $(K(\sqrt[n]{b})/K,\sigma,a)$ mit passendem $\sigma \in G(K(\sqrt[n]{b})/K)$.*

Beweis. Seien $L := K(\sqrt[n]{b}), m = [L:K]$ und $d = \frac{n}{m}$. Dann ist

$$(\sqrt[n]{b})^m = c \in K^* \text{ und } c^d = b.$$

Daher gilt $L = K(\sqrt[m]{c})$ und L ist eine Galoiserweiterung mit zyklischer Galoisgruppe, die erzeugt wird von

$$\sigma : \sqrt[m]{c} \mapsto \zeta^d \sqrt[m]{c}$$

Aus der Definition zyklischer Algebren und Satz 1.13 folgt nun, dass die m^2-dimensionale Normrestalgebra $A_{\zeta^d}(a,c\,|\,K)$ eine zyklische Algebra ist, nämlich $(L/K,\sigma,a)$. Nach Satz 2.6 gilt $A_\zeta(a,b\,|\,K) \cong M_d(A_{\zeta^d}(a,c\,|\,K))$ und die Ähnlichkeit ist gezeigt. □

Satz 2.9. *Sei zusätzlich zu obigen Voraussetzungen gefordert, dass K ein globaler oder lokaler Körper ist mit maximalem Ideal $\mathfrak{p}$ im Bewertungsring R, sodass $\mathfrak{p} \nmid (n)$ und $b \notin \mathfrak{p}$. Dann ist $A_\zeta(a,b\,|\,K)$ isomorph zu einer zyklischen Algebra.*

Beweis. Zu zeigen ist, dass zu jedem $b \in K$ und zu passendem $\kappa \in \mathbb{N}$, das nur Primteiler besitzt, die auch n teilen, eine κ-te Wurzel c von b gefunden werden kann, sodass $X^n - c$ irreduzibel ist. Dann gilt im Beweis des obigen Satzes $[K(\sqrt[n]{c}) : K] = n$ und $(K(\sqrt[n]{c})/K,\sigma,a^\kappa) \cong A_\zeta(a^\kappa,c\,|\,K)$. Da wegen $\mathfrak{p} \nmid (n)$ die Voraussetzunge von Satz 2.6 erfüllt sind, gilt weiter $(K(\sqrt[n]{c})/K,\sigma,a^\kappa) \cong A_\zeta(a,b\,|\,K)$.
Sei K ein lokaler Körper mit Bewertungsring R und maximalem Ideal $\mathfrak{p}$, sodass gilt $\mathfrak{p} \nmid (n)$. Existiert zu $x \in R^*$ ein $y \in R^*$ mit $x = y^r$, so ist klarerweise $x \equiv z^r \bmod \mathfrak{p}$ für ein $z \in R^*$. Da $\mathfrak{p} \nmid (n)$ liefert Hensels Lemma für alle Teiler r von n auch die Umkehrung:

$$x = y^r \text{ für ein } y \in R^* \iff x \equiv z^r \bmod \mathfrak{p} \text{ für ein } z \in R^*$$

Nach Lemma 1.2 enthält K eine primitive $(q-1)$-te Einheitswurzel ζ, q die Mächtigkeit des Restklassenkörpers, und es gilt $n \mid q-1$, da $\mathfrak{p} \nmid (n)$. Außerdem gibt es für jedes Element $x \in R^*$ ein $\zeta' \in \mu_{q-1}$, sodass gilt $x \equiv \zeta' \bmod \mathfrak{p}$. Sei nun κ die größtmögliche natürliche Zahl, die $q-1$ teilt, nur Primteiler besitzt, die auch n teilen und sodass $b \in R^*$ eine κ-te Wurzel y besitzt und sei $\gamma = \frac{q-1}{\kappa}$. Dann gilt

$$b = (\zeta^{i\gamma}y)^\kappa, \quad \text{für } i = 0,...,q-1.$$

Ist $y \equiv \zeta^\alpha \bmod \mathfrak{p}, 0 \leq \alpha \leq q-1$, so ist $\zeta^{i\gamma} y \equiv \zeta^{i\gamma+\alpha} \bmod \mathfrak{p}$. Folgende Aussagen sind äquivalent:

$X^n - \zeta^{i\gamma} y$ ist irreduzibel $\iff \zeta^{i\gamma} y$ hat keine r-te Wurzel für alle Teiler $r > 1$ von n

$\iff \zeta^{i\gamma+\alpha}$ hat keine r-te Wurzel für alle Teiler $r > 1$ von $n \iff ggT(n, i\gamma + \alpha) = 1$

Nach Konstruktion gilt ggT$(\alpha, \gamma, n) = 1$, da κ größtmöglich gewählt war. Setze nun

$$i = \prod_{\substack{q \mid n \\ q \nmid \alpha}} q,$$

wobei q über alle Primzahlen laufe, und betrachte die Primteiler p von n:

- Gilt $p \mid \alpha$, so $p \nmid \gamma$ und $p \nmid i$, also $p \nmid (\alpha + i\gamma)$
- Gilt andererseit $p \nmid \alpha$, so $p \mid i$ und $p \nmid (\alpha + i\gamma)$

Damit haben n und $\alpha + i\gamma$ keine gemeinsamen Teiler, also ist $\zeta^{i\gamma} y$ eine κ-te Wurzel von b und $X^n - \zeta^{i\gamma} y$ ist irreduzibel. Die Behauptung folgt für lokale Körper.
Da das Polynom $X^n - z, z \in K$ über einem globalen Körper K nur reduzibel sein kann, wenn es auch über jeder Vervollständigung reduzibel ist, folgt die Aussage. □

Bemerkung. Der Satz gilt auch für lokale Körper K, wenn gilt $\mathfrak{p} \nmid (n), b \in \mathfrak{p}$, da man eine Normrestalegbra $\mathcal{A}_\zeta$ über K auf die Form bringen kann $\mathcal{A}_\zeta \cong A_\zeta(\pi^j, u \,|\, K), u \in R^*, \pi$ ein Primelement in R, siehe nächster Abschnitt.

Satz 2.10. *Seien K ein beliebiger Körper und $n \in \mathbb{N}$, sodass* $\operatorname{char} K \nmid n$ *und sodass K eine primitive n-te Einheitswurzel ζ enthält und seien $a, a', b, b' \in K^*$. Dann sind die n^2-dimensionalen Normrestalgebren $A_\zeta(a, b \,|\, K)$ und $A_\zeta(a', b \,|\, K)$ genau dann isomorph, wenn es ein $c \in K(\sqrt[n]{b})^* =: L^*$ gibt mit $a' = n_{L/K}(c) \cdot a$. Analog gilt $A_\zeta(a, b \,|\, K) \cong A_\zeta(a, b' \,|\, K)$ genau dann wenn es ein $c' \in K(\sqrt[n]{a})^* =: L'^*$ gibt mit $b = n_{L'/K}(c') \cdot b'$.*

Beweis. Nach Lemma 1.15 gilt für zyklische K-Algebren: $(K'/K, \sigma, a) \cong (K'/K, \sigma, a')$ genau dann, wenn ein $c \in K'$ existiert, sodass gilt $a' = n_{K'/K}(c) \cdot a$ und da $A_\zeta(a, b \,|\, K)$ bzw. $A_\zeta(a', b \,|\, K)$ ähnlich sind zu $(L/K, \sigma, a)$ bzw. $(L/K, \sigma, a')$, folgt aus Dimensionsgleichheit unter obigen Bedingungen die Isomorphie. Die zweite Behauptung ergibt sich aus der Isomorphie $A_\zeta(a, b \,|\, K) \cong A_\zeta(b, a^{n-1} \,|\, K)$. □

Korollar 2.11. *Es gilt:*

$$A_\zeta(a, b) \cong M_n(K) \iff a \in n_{L/K}(L^*) \iff b \in n_{L'/K}(L'^*)$$

Obige Überlegung zu den zyklischen Algebren liefert außerdem die Multiplikativität der Normrestalgebren, die im Weiteren noch wichtig sein wird.

Lemma 2.12. *Seien $a, a', b, b' \in K^*$. Dann gilt:*

1. $A_\zeta(a, b) \otimes A_\zeta(a', b) \sim A_\zeta(aa', b)$
2. $A_\zeta(a, b) \otimes A_\zeta(a, b') \sim A_\zeta(a, bb')$

Beweis. Die Behauptungen folgen aus der analogen Aussage über die Multiplikativität von zyklischen Algebren aus Lemma 1.14 und $A_\zeta(a,b\,|\,K) \cong M_d(K) \otimes (L/K,\sigma,a)$ für einen Teiler d von n und der Isomorphie $A_\zeta(a,b\,|\,K) \cong A_\zeta(b,a^{n-1}\,|\,K)$. □

Aus dem Lemma erhält man auch allgemein für $r \in \mathbb{N}$

$$A_\zeta(a^r,b) \sim A_\zeta(a,b) \otimes ... \otimes A_\zeta(a,b) \sim A_\zeta(a,b^r)$$

und wegen Dimensionsgleichheit $A_\zeta(a^r,b) \cong A_\zeta(a,b^r)$.

2.3 Normrestalgebren über lokalen Körpern

Über lokalen Körpern kann man die Isomorphieklassen der Normrestalgebren ganz genau beschreiben. Sei also K in diesem Abschnitt stets ein lokaler Körper mit zugehörigem Primideal $\mathfrak{p}$, Primelement π, Bewertung ν und Bewertungsring R und sei q die Mächtigkeit des Restklassenkörpers $R/\mathfrak{p}$. Sei weiter $n \in \mathbb{N}$, sodass $\mathrm{char}(R/\mathfrak{p}) \nmid n$ und sodass K eine primitive n-te Einheitswurzel ζ enthält. Jedes Element a in R lässt sich eindeutig schreiben als $a = u\pi^\alpha, u \in R^*, \alpha = \nu(a)$. Die n^2-dimensionale Normrestalgebra $A_\zeta(a,b\,|\,K)$ zu $a,b \in R\backslash\{0\}$ ist daher gleich $A_\zeta(u_a\pi^\alpha, u_b\pi^\beta\,|\,K)$ für eindeutig bestimmte $u_a,u_b \in R^*, \alpha = \nu(a), \beta = \nu(b)$.

Nun ist die Normrestalgebra nach Lemma 2.12 ähnlich zum Tensorprodukt:

$$A_\zeta(a,b\,|\,K) = A_\zeta(u_a\pi^\alpha, u_b\pi^\beta\,|\,K) \sim$$
$$A_\zeta(u_a,u_b\,|\,K) \otimes A_\zeta(u_a,\pi^\beta\,|\,K) \otimes A_\zeta(\pi^\alpha,(-1)^\beta u_b\,|\,K) \otimes A_\zeta(\pi^\alpha,(-\pi)^\beta\,|\,K)$$

Nach Korollar 1.3 ist $K(\sqrt[n]{u_a})$ eine unverzweigte Körpererweiterung, daher ist die erste Algebra nach dem Normensatz 1.4 und Korollar 2.11 isomorph zu $M_n(K)$. Wegen der Multiplikativität und Korollar 2.7 gilt auch $A_\zeta(\pi^\alpha,(-\pi)^\beta\,|\,K) \cong M_n(K)$. Wegen der Eigenschaften von Normrestalgebren aus Satz 2.5 und Lemma 2.12 gilt nun weiter:

$$A_\zeta(a,b\,|\,K) \sim A_\zeta(\pi,u_a^{-\beta}\,|\,K) \otimes A_\zeta(\pi,(-1)^{\alpha\beta}u_b^\alpha\,|\,K) \sim$$
$$A_\zeta(\pi,(-1)^{\alpha\beta}u_b^\alpha u_a^{-\beta}\,|\,K) = A_\zeta(\pi,(-1)^{\alpha\beta}u_b^\alpha\pi^{\beta\alpha}/u_a^\beta\pi^{\alpha\beta}\,|\,K) =$$
$$A_\zeta(\pi,(-1)^{\alpha\beta}b^\alpha/a^\beta\,|\,K).$$

Aus Dimesionsgründen erhält man die Isomorphie der Algebren

$$A_\zeta(a,b\,|\,K) \cong A_\zeta(\pi,(-1)^{\alpha\beta}b^\alpha a^{-\beta}\,|\,K).$$

Suche nun $\kappa' \in \mathbb{N}, \kappa' \mid q-1$, sodass κ' nur Primteiler besitzt, die auch n teilen, K eine κ'-te Wurzel $u_\mathfrak{p}$ von $(-1)^{\alpha\beta}b^\alpha/a^\beta$ enthält und $X^n - u_\mathfrak{p}$ irreduzibel ist. Die Existenz folgt aus dem Beweis von Satz 2.9. Sei dann $\kappa \in \mathbb{N}$ die kleinste natürliche Zahl, sodass gilt $\kappa \equiv \kappa' \mod n$. Dann ist

$$u_\mathfrak{p}^\kappa \equiv (-1)^{\alpha\beta}b^\alpha/a^\beta \mod K^{*n}$$

und es gilt

$$A_\zeta(a,b\,|\,K) \cong A_\zeta(\pi^\kappa,u_\mathfrak{p}\,|\,K).$$

Im Folgenden soll deshalb die Struktur von Normrestalgebren der Form $A_\zeta(\pi^m,u\,|\,K)$, $u \in R^*$ und $X^n - u$ irreduzibel näher betrachtet werden.

Satz 2.13. *Sei K ein lokaler Körper mit Bewertungsring R und maximalem Ideal $\mathfrak{p}$ und sei n aus $\mathbb{N}$, sodass die Restkörpercharakteristik* $\operatorname{char} R/\mathfrak{p}$ *kein Teiler von n ist und sodass K eine primitive n-te Einheitswurzel ζ enthält. Seien weiters $m \in \mathbb{N}, 1 \leq m \leq n-1$ und $u \in R^*$, sodass K keine r-te Wurzel von u enthält für alle Teiler $r > 1$ von n. Dann gilt:*

1. $A_\zeta(u', u \,|\, K) \cong M_n(K)$ *für alle* $u' \in R^*$.
2. $A_\zeta(\pi^m, u \,|\, K)$ *ist Divisionsalgebra, falls* $\operatorname{ggT}(m, n) = 1$.
3. $A_\zeta(\pi^m, u \,|\, K) \cong M_d(A_{\zeta^d}(\pi^{m/d}, u \,|\, K))$ *für* $\operatorname{ggT}(m, n) = d$ *und die* $(n/d)^2$*-dimensionale Normrestalgebra* $A_{\zeta^d}(\pi^{m/d}, u \,|\, K)$ *ist eine Divisionsalgebra.*

Außerdem sind alle n Algebren paarweise nicht isomorph.

Beweis. 1. Folgt aus dem Normensatz und Korollar 2.11.

2. Nach Satz 2.9 ist $A_\zeta(\pi^m, u \,|\, K)$ isomorph zu einer zyklischen Algebra. Die Aussage folgt dann aus [Rei75, 31.1 Theorem, S.264]

3. Folgt aus Satz 2.6 und Punkt 2.

Um eine Isomorphie zwischen zwei solchen Algebren $A_\zeta(\pi^l, u \,|\, K)$ und $A_\zeta(\pi^m, u \,|\, K)$, $1 \leq m < l \leq n-1$ zu erhalten, müsste π^{l-m} Norm eines Elements in $L = K(\sqrt[n]{u})$ sein, was zu einem Widerspruch führt. □

Ist also $K_\mathfrak{p}$ die Vervollständigung eines algebraischen Zahlkörpers K an der Stelle $\mathfrak{p}$ und sind alle Voraussetzungen des Satzes erfüllt, so folgt, dass der größte gemeinsame Teiler von n und κ wie oben genau der lokalen Kapazität $\kappa_\mathfrak{p}$ von $A_\zeta(a, b \,|\, K)$ an der Stelle $\mathfrak{p}$ entspricht.

Aus dem Beweis von Punkt 2 folgt in [Rei75, 31.1 Theorem, S.264], dass es bis auf Isomorphie genau $\varphi(n)$ verschiedene, zentralen Divisionsalgebren vom Grad n gibt, nämlich genau die Algebren $A_\zeta(\pi^m, u \,|\, K)$ mit $\operatorname{ggT}(m, n) = 1$. Daraus ergibt sich, dass es genau n Isomorphieklassen von Normrestalgebren gibt, die durch die oben erwähnten Algebren repräsentiert werden.

3 Ordnungen

Das Ziel ist es maximale Ordnungen in Normrestalgebren zu finden. In diesem Kapitel sollen deshalb die grundlegenden Definitionen und die Theorie, die später gebraucht wird, zusammengefasst werden. Eines der Standardwerke auf diesem Gebiet ist [Rei75].

3.1 Norm und Spur

Sei K ein Körper und A eine m-dimensionale K-Algebra mit Basis $\underline{b}$. Bezeichne mit $M(\varphi_a)$ die darstellende Matrix des Algebrenhomomorphismus $\varphi_a : A \to A, v \mapsto av$ bezüglich der Basis $\underline{b}$.

Definition 3.1. Man definiert über die übliche Spur- und Determinantenabbildung von Matrizen zwei Abbildungen $A \to K$:
Die*Spur* von a:

$$\mathrm{Tr}_{\mathrm{A/K}}(a) := \mathrm{Tr}(M(\varphi_a)),$$

und die *Norm* von a:

$$\mathrm{N}_{\mathrm{A/K}}(a) := \det(M(\varphi_a)).$$

Weiters definiert man das *charakteristische Polynom* $p_a(X) \in K[X]$ von a:

$$p_a(X) := \det(X \cdot I_m - M(\varphi_a))$$

Bemerkung.

1. Wie schon aus der linearen Algebra bekannt, ist die Definition unabhängig von der Wahl der Basis.

2. Ebenfalls bekannt ist die Identität

   $$p_a(X) = X^m - \mathrm{Tr}_{\mathrm{A/K}}(a)X^{m-1} + ... + (-1)^m \mathrm{N}_{\mathrm{A/K}}(a),$$

   siehe [Rei75, S.3]

3. Ist $f_a(X)$ das Minimalpolynom von a, so gilt $f_a(X) \mid p_a(X)$, siehe [Rei75, 1.7 Theorem, S.3].

4. Ist ein Integritätsbereich R ganz abgeschlossen in seinem Quotientenkörper K und A eine endlich dimensionale K-Algebra, so ist ein Element $a \in A$ genau dann ganz über R, wenn das charakteristische Polynom $p_a(X)$ in $R[X]$ liegt. Siehe [Rei75, Exercise 1., S.7]

5. Aus den entsprechenden Eigenschaften von Spur und Determinante bei Matrizen erhält man:

   $$\mathrm{Tr}_{\mathrm{A/K}}(\lambda a + \mu b) = \lambda \,\mathrm{Tr}_{\mathrm{A/K}}(a) + \mu \,\mathrm{Tr}_{\mathrm{A/K}}(b) \qquad \mathrm{Tr}_{\mathrm{A/K}}(ab) = \mathrm{Tr}_{\mathrm{A/K}}(ba)$$
   $$\mathrm{N}_{\mathrm{A/K}}(ab) = \mathrm{N}_{\mathrm{A/K}}(a)\,\mathrm{N}_{\mathrm{A/K}}(b) \qquad \mathrm{N}_{\mathrm{A/K}}(\lambda a) = \lambda^m \,\mathrm{N}_{\mathrm{A/K}}(a)$$

   für $a, b \in A, \lambda, \mu \in K$.

Ist A eine zentrale, einfache K-Algebra vom Grad n, so existiert bekanntlich eine Körpererweiterung E von K, die A zerfällt, d.h. $E \otimes_K A \cong M_n(E)$. Sei nun $h : E \otimes_K A \to M_n(E)$ ein Isomorphismus. Man definiert:

Definition 3.2. In einer zentralen, einfachen K-Algebra A vom Grad n nennt man die Abbildungen $A \to K$

$$\mathrm{tr}_{\mathrm{A/K}}(a) := \mathrm{Tr}(h(1 \otimes a))$$

$$\mathrm{n}_{\mathrm{A/K}}(a) := \det(h(1 \otimes a))$$

die *reduzierte Spur* bzw. die *reduzierte Norm* von a und das Polynom

$$p_a^r(X) := \det(X \cdot I_n - h(1 \otimes a))$$

das *reduzierte charakteristische Polynom* von a.

Bemerkung.

1. Die Definitionen von reduzierter Spur und Norm sowie des reduzierten charakteristischen Polynoms sind unabhängig von der Wahl des Zerfällungskörpers E und des Isomorphismus h, siehe [Rei75, Ch. 9a, S.113].

2. Es gilt
$$\mathrm{Tr}_{\mathrm{A/K}}(a) = n \cdot \mathrm{tr}_{\mathrm{A/K}}(a),$$
$$\mathrm{N}_{\mathrm{A/K}}(a) = \mathrm{n}_{\mathrm{A/K}}(a)^n,$$
$$p_a(X) = (p_a^r(X))^n$$
und
$$p_a^r(X) = X^n - \mathrm{tr}_{\mathrm{A/K}}(a)X^{n-1} + ... + (-1)^n \,\mathrm{n}_{\mathrm{A/K}}(a).$$
Siehe [Rei75, Ch. 9a, S.115 f.].

3. Daraus ergibt sich:
$$\mathrm{tr}_{\mathrm{A/K}}(a+b) = \mathrm{tr}_{\mathrm{A/K}}(a) + \mathrm{tr}_{\mathrm{A/K}}(b) \quad \mathrm{n}_{\mathrm{A/K}}(ab) = \mathrm{n}_{\mathrm{A/K}}(a)\,\mathrm{n}_{\mathrm{A/K}}(b)$$
$$\mathrm{tr}_{\mathrm{A/K}}(\lambda a) = \lambda \cdot \mathrm{tr}_{\mathrm{A/K}}(a) \qquad \mathrm{n}_{\mathrm{A/K}}(\lambda a) = \lambda^n \cdot \mathrm{n}_{\mathrm{A/K}}(a)$$
$$\mathrm{tr}_{\mathrm{A/K}}(ab) = \mathrm{tr}_{\mathrm{A/K}}(ba)$$
für $a, b \in A, \lambda \in K$.

Beispiel : Quaternionenalgebren
In einer Quaternionenalgebra über einem Körper K lassen sich Norm und Spur besonders leicht berechnen. Sei dazu $\langle 1, i, j, k\rangle$ die Standardbasis der Quaternionenalgebra $\mathcal{Q} := Q(a, b \,|\, K), a, b \in K^*$. Wie im Kapitel 2.1 gezeigt wurde, ist $K(\sqrt{b})$ Zerfällungskörper von $\mathcal{Q}$ und die Bilder der Basiselemente unter h haben folgende Form:

$$h(1 \otimes i) = \begin{pmatrix} 0 & a \\ 1 & 0 \end{pmatrix},\ h(1 \otimes j) = \begin{pmatrix} -\sqrt{b} & 0 \\ 0 & \sqrt{b} \end{pmatrix},\ h(1 \otimes k) = \sqrt{b}\begin{pmatrix} 0 & a \\ -1 & 0 \end{pmatrix}.$$

Damit ist das Bild eines Elements $\mathcal{Q} \ni x = x_0 \cdot 1 + x_1 \cdot i + x_2 \cdot j + x_3 \cdot k$ gleich

$$\begin{pmatrix} x_0 - x_2\sqrt{b} & a(x_1 + x_3\sqrt{b}) \\ x_1 - x_3\sqrt{b} & x_0 + x_2\sqrt{b} \end{pmatrix}.$$

Nun lassen sich Norm und Spur berechnen

$$\mathrm{n}_{\mathcal{Q}/\mathrm{K}}(x) = x_0^2 - ax_1^2 - bx_2^2 + abx_3^2, \quad \mathrm{tr}_{\mathcal{Q}/\mathrm{K}}(x) = 2x_0.$$

Eine kurze Rechnung zeigt:

$$\mathrm{n}_{\mathcal{Q}/\mathrm{K}}(x) = x \cdot \bar{x}, \quad \mathrm{tr}_{\mathcal{Q}/\mathrm{K}}(x) = x + \bar{x}$$

wobei $\bar{x}$ das konjugierte Quaternion $\bar{x} = x_0 \cdot 1 - x_1 \cdot i - x_2 \cdot j - x_3 \cdot k$ bezeichne.
Da $\bar{x} = -x + 2x_0$ gilt, erhält man folgende Gleichung

$$n_{\mathcal{Q}/K}(x) = x \cdot \bar{x} = -x^2 + 2x_0 \cdot x$$

und damit

$$0 = x^2 - \mathrm{tr}_{\mathcal{Q}/\mathrm{K}}(x)x + \mathrm{n}_{\mathcal{Q}/\mathrm{K}}(x) = p_x^r(x)$$

was mit der obigen Bemerkung übereinstimmt.

Ist R ein Dedekindring und $\mathcal{Q}$ eine Quaternionenalgebra über seinem Quotientenkörper $K = \mathrm{Quot}(R)$, so folgt daraus, dass ein Element $x \in \mathcal{Q}$ ganz über R ist, wenn Norm und Spur in R liegen.

3.2 Ordnungen

Sei R ein Dedekindring, $K = \mathrm{Quot}(R)$ der Quotientenkörper von R und A eine einfache, m-dimensionale K-Algebra, deren Zentrum $Z(A)/K$ über K separabel ist.

Definition 3.3. Ein *vollständiges R-Gitter* Λ in A ist ein endlich erzeugter R-Modul, für den gilt $K \cdot \Lambda = A$.
Eine *R-Ordnung* $\mathcal{O}$ in A ist ein vollständiges R-Gitter in A, das zusätzlich ein Ring mit Einselement $1_{\mathcal{O}}$ ist, sodass gilt $1_{\mathcal{O}} = 1_A$. Man nennt die Ordnung $\mathcal{O}$ *maximal,* wenn sie in keiner anderen Ordnung enthalten ist.

Satz 3.4. *Sei $\mathcal{O}$ ein R umfassender Unterring von A, dessen Elemente ganz sind und für den gilt $K \cdot \mathcal{O} = A$. Dann ist $\mathcal{O}$ eine Ordnung. Umgekehrt erfüllt jede Ordnung diese Eigenschaften.*

Beweis. [Rei75, 10.3 Theorem, S.126] □

Beispiele.

1. Ist $a \in A$ ganz über R, so ist $R[a]$ eine R-Ordnung in der K-Algebra $K[a]$.
2. Ist $A = M_n(K)$ der Matrizenring über K, so ist $M_n(R)$ eine Ordnung in A.
3. Ist A kommutativ, so ist der ganze Abschluss von R in A eine maximale Ordnung. Dasselbe gilt für nicht kommutative Algebren, sofern der ganze Abschluss ein Ring ist.
4. Sei Λ ein vollständiges R-Gitter in A. Dann definiert man die Linksordnung $O_l(\Lambda) = \{x \in A \mid x \cdot \Lambda \subset \Lambda\}$ (siehe [Rei75, Ch. 8, Definitions and examples, S.109]). Analog kann man die Rechtsordnung $O_r(\Lambda)$ definieren.

Sei A weiterhin eine einfache, m-dimensionale K-Algebra, deren Zentrum $Z(A)/K$ über K separabel ist.

Satz 3.5. *Es existiert mindestens eine maximale R-Ordnung in A und jede R-Ordnung ist in einer maximalen R-Ordnung enthalten.*

Beweis. [Rei75, 10.4 Corollary, S.127] □

Definition 3.6. Die *Diskriminante* $d(\mathcal{O})$ einer R-Ordnung $\mathcal{O}$ in A ist definiert als das Ideal in R, das erzeugt wird von

$$\{\det(\mathrm{tr}_{\mathrm{A/K}}(x_i x_j)_{1\leq i,j\leq m}) \mid x_1, ..., x_m \in \mathcal{O}\}$$

Lemma 3.7. [Rei75, 10.2 Theorem, S.126]
Besitzt die R-Ordnung $\mathcal{O}$ eine R-Basis $(x_1, ..., x_m)$, dann ist die Diskriminante gleich dem Hauptideal

$$d(\mathcal{O}) = \det((\mathrm{tr}_{\mathrm{A/K}}(x_i x_j))_{i,j}) \cdot R$$

Beweis. Setze $d := \det((\mathrm{tr}_{\mathrm{A/K}}(x_i x_j))_{i,j})$. Klarerweise gilt $d \cdot R \subset d(\mathcal{O})$. Sind andererseits $y_1, ...y_m \in \mathcal{O}$, dann gibt es $a_{ij} \in R$ mit $y_i = \sum_{j=1}^m a_{ij} x_j$. Für die Determinante gilt dann

$$\det\left((\mathrm{tr}_{\mathrm{A/K}}(y_k y_l))_{k,l}\right) = \det\left(\left(\sum_{i=1}^m \sum_{j=1}^m a_{ki} a_{lj} \,\mathrm{tr}_{\mathrm{A/K}}(x_i x_j)\right)_{k,l}\right)$$

$$= \det\left((\mathrm{tr}_{\mathrm{A/K}}(x_i x_j))_{i,j}\right) \cdot \det\left((a_{kl})_{k,l}\right)^2 \in d \cdot R$$

Damit ist $d(\mathcal{O}) = d \cdot R$. □

Die nächsten zwei Sätze sind für das Vorhaben maximale Ordnungen zu finden essentiell.

Lemma 3.8. *Seien $\mathcal{O} \subset \mathcal{O}'$ zwei R-Ordnungen in A, die eine R-Basis besitzen. Dann gilt*

$$d(\mathcal{O}) = [\mathcal{O}' : \mathcal{O}]^2 \cdot d(\mathcal{O}')$$

wobei $[\mathcal{O}' : \mathcal{O}]$ die Determinante der Übergangsmatrix von der Basis von $\mathcal{O}'$ zur Basis von $\mathcal{O}$ bezeichne. Insbesondere stimmen die Ordnungen genau dann überein, wenn ihre Diskriminanten übereinstimmen.

Beweis. Seien $(x_1, ..., x_m)$ und $(y_1, ..., y_m)$ Basen von $\mathcal{O}'$ bzw. $\mathcal{O}$. Dann existieren $a_{ij} \in R$, sodass gilt $y_i = \sum_{j=1}^m a_{ij} x_j$ und es ist $[\mathcal{O}' : \mathcal{O}] = \det((a_{ij})_{i,j})$. Analog zum letzten Beweis folgt die Behauptung. □

Satz 3.9. *Sei R ein Dedekindring, dessen Quotientenkörper K ein globaler Körper ist und sei $\mathcal{O}$ eine maximale R-Ordnung in einer zentralen, einfachen K-Algebra A vom Grad n. Zu jedem Primideal $\mathfrak{p}$ in R bezeichne $\kappa_\mathfrak{p}$ die lokale Kapazität und $m_\mathfrak{p}$ den lokalen Index von A bei $\mathfrak{p}$. Dann gilt für die Diskriminante:*

$$d(\mathcal{O}) = \prod_{\mathfrak{p}} \mathfrak{p}^{(m_\mathfrak{p}-1)\kappa_\mathfrak{p} n}$$

Insbesondere ist die Determinante einer maximalen Ordnung in A eindeutig.

Beweis. [Rei75, 32.1 Theorem, S.273] □

3.3 Die Diskriminante von $\mathcal{O}_\zeta$

Betrachte nun wieder Normrestalgebren über einem algebraischen Zahlkörper K mit Ring der ganzen Zahlen R. Zu $n \in \mathbb{N}$ enthalte K eine primitive n-te Einheitswurzel ζ und $\mathcal{A}_\zeta := A_\zeta(a, b \mid K)$ bezeichne die n^2-dimensionale Normrestalgebra zu $a, b \in R \setminus \{0\}$. Wie in der Konstruktion aus Abschnitt 2.1 seien u und v erzeugende Elemente von $\mathcal{A}_\zeta$ über K für die gilt $u^n = a, v^n = b$ und $uv = \zeta vu$.

Der von $\{u^i v^j \mid 0 \leq i, j \leq n-1\}$ erzeugte R-Modul genannt $\mathcal{O}_\zeta$ ist offensichtlich eine R-Ordnung in $\mathcal{A}_\zeta$. Um maximale Ordnungen suchen zu können, die $\mathcal{O}_\zeta$ enthalten, ist es nach Lemma 3.8 sinnvoll, die Diskriminante von $\mathcal{O}_\zeta$ zu kennen und um diese zu bestimmen, muss man $\mathrm{tr}_{\mathcal{A}_\zeta/\mathrm{K}}(u^i v^j)$ berechnen. Nach Abschnitt 2.1 ist $K(\sqrt[n]{b})$ ein Zerfällungskörper von $\mathcal{A}_\zeta$ und $h : K(\sqrt[n]{b}) \otimes \mathcal{A}_\zeta \to M_n(K(\sqrt[n]{b}))$ gegeben durch

$$1 \otimes u \mapsto U = \begin{pmatrix} 0 & \cdots & 0 & a \\ 1 & \cdots & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \cdots & 1 & 0 \end{pmatrix} \quad , \quad 1 \otimes v \mapsto V = \sqrt[n]{b} \begin{pmatrix} \zeta^{n-1} & 0 & \cdots & 0 \\ 0 & \zeta^{n-2} & & \\ \vdots & & \ddots & \vdots \\ 0 & \cdots & & 1 \end{pmatrix}$$

ist ein Isomorphismus. Offensichtlich ist die Spur von U und allen Potenzen $U^i, i < n$, gleich 0, ebenso wie die Spur von $U^i V^j, 1 \leq i, j \leq n-1$. Die Spur von V ist gleich

$$\mathrm{tr}_{\mathcal{A}_\zeta/\mathrm{K}}(V) = \sqrt[n]{b} \cdot \sum_{j=0}^{n-1} \zeta^j = 0.$$

Sei nun $1 \leq r \leq n-1$. Setze $m = ggT(n, r), t = \frac{r}{m}, s = \frac{n}{m}, \zeta' = \zeta^m$ eine primitive s-te Einheitswurzel, dann ist die Spur von V^r

$$\mathrm{tr}_{\mathcal{A}_\zeta/\mathrm{K}}(V^r) = \sqrt[n]{b^r} \cdot \sum_{j=0}^{n-1} \zeta^{jr} = \sqrt[n]{b^r} \cdot \sum_{j=0}^{n-1} \zeta'^{jt} = \sqrt[n]{b^r} \cdot \sum_{j=0}^{n-1} \zeta'^{j} = m \cdot \sqrt[n]{b^r} \cdot \sum_{j=0}^{s-1} \zeta'^{j} = 0$$

Daher ist für $0 \leq i, j, k, l \leq n-1$ die Spur $\mathrm{tr}_{\mathcal{A}_\zeta/\mathrm{K}}(u^i v^j \cdot u^k v^l) \neq 0$ nur dann, wenn $i+k \in \{0, n\}$ und $j + l \in \{0, n\}$. Genauer gilt:

$$\mathrm{tr}_{\mathcal{A}_\zeta/\mathrm{K}}(u^i v^j \cdot u^k v^l) = \begin{cases} n, & \text{wenn } i = j = k = m = 0, \\ an, & \text{wenn } j = l = 0, i + k = n, \\ bn, & \text{wenn } i = k = 0, j + l = n, \\ \zeta^{ij} abn, & \text{wenn } i + k = n, j + l = n, \\ 0 & \text{sonst.} \end{cases}$$

In jeder Spalte und in jeder Zeile der $n^2 \times n^2$ Matrix $(\mathrm{tr}_{\mathcal{A}_\zeta/\mathrm{K}}(u^i v^j \cdot u^k v^l))$ steht also genau ein Eintrag und die Determinante ist

$$\det((\mathrm{tr}_{\mathcal{A}_\zeta/\mathrm{K}}(u^i v^j \cdot u^k v^l))) = n^{n^2} a^{n(n-1)} b^{n(n-1)} \zeta^x,$$

$x \in \mathbb{N}$. Damit ist die Diskriminante von $\mathcal{O}_\zeta$ bestimmt:

$$d(\mathcal{O}_\zeta) = (n^n a^{(n-1)} b^{(n-1)})^n \cdot R.$$

4 Das Hilbertsymbol

Das Verzweigungsverhalten von Normrestalgebren über algebraischen Zahlkörpern hängt eng zusammen mit dem Hilbertsymbol über lokalen Körper, welches sich auf tiefgreifende Resultate aus der Klassenkörpertheorie stützt, siehe [Neu99, Ch.IV §5 - Ch.V §3], [Fes93, Ch.IV §4-§5]. Später wird das Konzept des Hilbertsymbols in trivialer Weise auch auf $\mathbb{R}$ und $\mathbb{C}$ übertragen.

Ist L eine Galoiserweiterung eines lokalen Körpers K, so bezeichne mit $G(L/K)^{ab}$ den Quotienten der Galoisgruppe $G(L/K)$ modulo ihrer Kommutatoruntergruppe.

Satz 4.1. *Sei L/K eine endliche Galoiserweiterung von lokalen Körpern. Dann gibt es einen kanonischen Isomorphismus*

$$r_{L/K} : G(L/K)^{ab} \xrightarrow{\sim} K^*/n_{L/K}L^*$$

genannt die Reziprozitätsabbildung. Ist L/K unverzweigt so ist die Abbildung gegeben durch

$$r_{L/K}(\varphi_{L/K}) = \pi$$

dabei ist $\varphi_{L/K}$ der Frobeniusautomorphismus von L/K und π ein Primelement in K.

Beweis. [Neu99, 1.2 Theorem , S.320, 5.7 Proposition, S.295] □

Invertiert man die Reziprozitätsabbildung $r_{L/K}$ erhält man einen Morphismus

$$(\quad, L/K) : K^* \longrightarrow G(L/K)^{ab},$$

genannt das *lokale Normrestsymbol.*Die Abbildung $(\quad, L/K)$ ist surjektiv und hat Kern $n_{L/K}L^*$. Über das Normrestsymbol lässt sich nun das Hilbertsymbol definieren.

Definition 4.2. Sei $\mathfrak{p}$ das eindeutige maximale Ideal im Bewertungsring eines lokalen Körpers K und sei n aus $\mathbb{N}$, sodass $\operatorname{char} K \nmid n$ und K die n-ten Einheitswurzeln μ_n enthält. Das *n-te Hilbertsymbol*

$$\left(\frac{\cdot}{\mathfrak{p}}\right)_n : K^* \times K^* \longrightarrow \mu_n$$

ist gegeben durch

$$\left(\frac{a,b}{\mathfrak{p}}\right)_n = \frac{(a, K(\sqrt[n]{b})/K)(\sqrt[n]{b})}{\sqrt[n]{b}}.$$

Satz 4.3. [Neu99, S.334, Proposition 3.2] *Einige Eigenschaften des Hilbertsymbols*

1. $\left(\frac{aa',b}{\mathfrak{p}}\right)_n = \left(\frac{a,b}{\mathfrak{p}}\right)_n \cdot \left(\frac{a',b}{\mathfrak{p}}\right)_n$,
2. $\left(\frac{a,bb'}{\mathfrak{p}}\right)_n = \left(\frac{a,b}{\mathfrak{p}}\right)_n \cdot \left(\frac{a,b'}{\mathfrak{p}}\right)_n$,

3. $\left(\frac{a,b}{\mathfrak{p}}\right)_n = 1 \iff a$ *ist Norm eines Elements der Körpererweiterung* $K(\sqrt[n]{b})/K \iff b$ *ist Norm eines Elements der Körpererweiterung* $K(\sqrt[n]{a})/K$,

4. $\left(\frac{a,1}{\mathfrak{p}}\right)_n = \left(\frac{-a,a}{\mathfrak{p}}\right)_n = 1$. *Ist* n *ungerade, so gilt auch* $\left(\frac{a,a}{\mathfrak{p}}\right)_n = 1$.

5. $\left(\frac{a,b}{\mathfrak{p}}\right)_n = \left(\frac{b,a}{\mathfrak{p}}\right)_n^{-1} = \left(\frac{b^{n-1},a}{\mathfrak{p}}\right)_n = \left(\frac{b,a^{n-1}}{\mathfrak{p}}\right)_n$

6. $\left(\frac{a,b}{\mathfrak{p}}\right)_n = \left(\frac{a,(-1)^{n-1}ab}{\mathfrak{p}}\right)_n = \left(\frac{(-1)^{n-1}ab,b}{\mathfrak{p}}\right)_n$

Vgl. die Eigenschaften der n^2*-dimensionalen Normrestalgebra* $A_\zeta(a,b\,|\,K)$ *aus Satz 2.5 und Korollar 2.7.*

Beweis. Die Punkte 1. und 2. und die erste Aussage von Punkt 3. folgen direkt aus der Definition. Die zweite Aussage von Punkt 3. folgt aus Punkt 5. und bezieht sich daher selbst auf die erste Aussage von Punkt 3..

4. Nach Punkt 1. ist klar $\left(\frac{a,1}{\mathfrak{p}}\right)_n = \left(\frac{a,1^n}{\mathfrak{p}}\right)_n = \left(\frac{a,1}{\mathfrak{p}}\right)_n^n = 1$
Sei nun $x \in K^*$ sodass $x^n - a \neq 0$. Dann ist in der Körpererweiterung $L := K(\gamma)$ mit $\gamma^n = a$

$$x^n - a = \prod_{i=0}^{n-1}(x - \zeta^i\gamma)$$

wobei ζ eine primitive n-te Einheitswurzel ist. Sei $d = [L : K],\ d \cdot m = n$, dann existiert in K ein Element c, sodass $c^m = a$ und $\gamma^d = c$. Die Norm von $x - \zeta^i\gamma$ ist $n_{L/K}(x - \zeta^i\gamma) = \prod_{j=0}^{d-1}(x - \zeta^{i+jm}\gamma)$. Insgesamt erhält man

$$x^n - a = \prod_{i=0}^{m-1} n_{L/K}(x - \zeta^i\gamma)$$

und $x^n - a$ ist Norm eines Elements in $K(\gamma)$. Wählt man $x = 0$, folgt $-a$ ist Norm eines Elements in $K(\sqrt[n]{a})$ und die erste Aussage ist gezeigt. Ist n ungerade, so ist $-1 = n_{L/K}(-1)$ Norm und damit auch $(-1)\cdot(-a)$ und die zweite Aussage folgt.

5. Mittels Punkt 4. lässt sich berechnen

$$\left(\frac{a,b}{\mathfrak{p}}\right)_n \cdot \left(\frac{b,a}{\mathfrak{p}}\right)_n = \left(\frac{-b,b}{\mathfrak{p}}\right)_n \cdot \left(\frac{a,b}{\mathfrak{p}}\right)_n \cdot \left(\frac{b,a}{\mathfrak{p}}\right)_n \cdot \left(\frac{-a,a}{\mathfrak{p}}\right)_n$$

$$= \left(\frac{-ab,b}{\mathfrak{p}}\right)_n \cdot \left(\frac{-ab,a}{\mathfrak{p}}\right)_n = \left(\frac{-ab,ab}{\mathfrak{p}}\right)_n = 1$$

und damit $\left(\frac{a,b}{\mathfrak{p}}\right)_n = \left(\frac{b,a}{\mathfrak{p}}\right)_n^{-1}$. Außerdem gilt nach Punkt 1.

$$\left(\frac{b,a}{\mathfrak{p}}\right)_n \cdot \left(\frac{b^{n-1},a}{\mathfrak{p}}\right)_n = \left(\frac{b^n,a}{\mathfrak{p}}\right)_n = \left(\frac{b,a}{\mathfrak{p}}\right)_n^n = 1.$$

und auch $\left(\frac{b^{n-1},a}{\mathfrak{p}}\right)_n = \left(\frac{b,a}{\mathfrak{p}}\right)_n^{-1}$. Analog folgt $\left(\frac{b,a^{n-1}}{\mathfrak{p}}\right)_n = \left(\frac{b,a}{\mathfrak{p}}\right)_n^{-1}$.

6. Aus Punkt 1. und 4. folgt

$$\left(\frac{a,(-1)^{n-1}ab}{\mathfrak{p}}\right)_n = \left(\frac{a,(-1)^{n-1}a}{\mathfrak{p}}\right)_n \cdot \left(\frac{a,b}{\mathfrak{p}}\right)_n = \left(\frac{a,b}{\mathfrak{p}}\right)_n$$

und analog die zweite Aussage. □

Bemerkung. Mit Hilfe eben gezeigter Eigenschaften kann das n-te Hilbertsymbol $\left(\frac{a,b}{\mathfrak{p}}\right)_n$ über einem lokalen Körper K, dessen Restkörpercharakteristik kein Teiler von n ist, genau wie die Normrestalgebra $A_\zeta(a,b\,|\,K)$ in Abschnitt 2.3 umgeformt werden.
Nach Punkt 1., 2., 4. und 5. des letzten Satzes und dem Normensatz gilt für $a = u_a\pi^\alpha$, $b = u_b\pi^\beta, u_a, u_b \in R^*$:

$$\left(\frac{a,b}{\mathfrak{p}}\right)_n = \left(\frac{u_a\pi^\alpha, u_b\pi^\beta}{\mathfrak{p}}\right)_n =$$

$$\left(\frac{u_a,u_b}{\mathfrak{p}}\right)_n \cdot \left(\frac{u_a,\pi^\beta}{\mathfrak{p}}\right)_n \cdot \left(\frac{\pi^\alpha,(-1)^\beta u_b}{\mathfrak{p}}\right)_n \cdot \left(\frac{\pi^\alpha,(-\pi)^\beta}{\mathfrak{p}}\right)_n =$$

$$\left(\frac{\pi,u_a^{-\beta}}{\mathfrak{p}}\right)_n \cdot \left(\frac{\pi,(-1)^{\alpha\beta}u_b^\alpha}{\mathfrak{p}}\right)_n = \left(\frac{\pi,(-1)^{\alpha\beta}\frac{u_b^\alpha}{u_a^\beta}}{\mathfrak{p}}\right)_n =$$

$$\left(\frac{\pi,(-1)^{\alpha\beta}\frac{b^\alpha}{a^\beta}}{\mathfrak{p}}\right)_n$$

Es gilt also

$$\left(\frac{a,b}{\mathfrak{p}}\right)_n = \left(\frac{\pi,(-1)^{\alpha\beta}\frac{b^\alpha}{a^\beta}}{\mathfrak{p}}\right)_n$$

unabhängig vom gewählten Primelement.

Unter den obigen Voraussetzungen an den lokalen Körper gibt es somit eine Parametrisierung der Isomorphieklasse der n^2-dimensionalen Normrestalgebra $A_\zeta(a,b\,|\,K)$ durch das n-te Hilbertsymbol $\left(\frac{a,b}{\mathfrak{p}}\right)_n$.

Satz 4.4. *Seien $n \in \mathbb{N}$ und K ein lokaler Körper mit Bewertung ν, Bewertungsring R und maximalem Ideal $\mathfrak{p}$, sodass die Restkörpercharakteristik* $\operatorname{char} R/\mathfrak{p}$ *kein Teiler von n ist und sodass K eine primitive n-te Einheitswurzel ζ enthält. Seien $a,b,c,d \in K^*$. Dann gilt für die n^2-dimensionalen Normrestalgebren zu a,b bzw. zu c,d:*

$$A_\zeta(a,b\,|\,K) \cong A_\zeta(c,d\,|\,K) \Longleftrightarrow \left(\frac{a,b}{\mathfrak{p}}\right)_n = \left(\frac{c,d}{\mathfrak{p}}\right)_n$$

Beweis. Bezeichne mit π ein Primelement, mit $\alpha := \nu(a), \beta := \nu(b), \gamma := \nu(c), \delta := \nu(d)$ und mit $L := K(\sqrt[n]{\pi})$. Da nach den Überlegungen in Abschnitt 2.3 gilt

$$A_\zeta(a,b\,|\,K) \cong A_\zeta(\pi,(-b)^\alpha/(-a)^\beta\,|\,K) \quad \text{und} \quad A_\zeta(c,d\,|\,K) \cong A_\zeta(\pi,(-d)^\gamma/(-c)^\delta\,|\,K)$$

folgt

$$A_\zeta(a,b\,|\,K) \cong A_\zeta(c,d\,|\,K) \Longleftrightarrow \exists x \in L^* \text{ mit } \frac{(-b)^\alpha}{(-a)^\beta} = \frac{(-d)^\gamma}{(-c)^\delta} \cdot n_{L/K}(x).$$

Stimmen andererseits die Hilbertsymbole überein, so gilt wegen der letzten Bemerkung

$$\left(\frac{\pi,(-b)^\alpha/(-a)^\beta}{\mathfrak{p}}\right)_n = \left(\frac{a,b}{\mathfrak{p}}\right)_n = \left(\frac{c,d}{\mathfrak{p}}\right)_n = \left(\frac{\pi,(-d)^\gamma/(-c)^\delta}{\mathfrak{p}}\right)_n.$$

Nach Satz 4.3 Punkt 2. und 3. muss ein $x \in L^*$ existieren, sodass $\frac{(-b)^\alpha}{(-a)^\beta} = n_{L/K}(x) \cdot \frac{(-d)^\gamma}{(-c)^\delta}$. Daher gilt

$$\left(\frac{a,b}{\mathfrak{p}}\right)_n = \left(\frac{c,d}{\mathfrak{p}}\right)_n \iff \exists x \in L^* \text{ sodass } \frac{(-b)^\alpha}{(-a)^\beta} = \frac{(-d)^\gamma}{(-c)^\delta} \cdot n_{L/K}(x)$$

und die Behauptung ist gezeigt.

□

Außerdem kann man in diesem Fall eine explizite Formel für das Hilbertsymbol angeben. Wegen der Voraussetzungen an K und n gilt nach Lemma 1.2 und den Überlegungen dazu, dass $n \mid q-1$, wobei q die Mächtigkeit des Restklassenkörpers ist, und jedes Element x in R^* besitzt eine Zerlegung $x = \omega(X) \cdot \langle x \rangle$, wobei $\omega(x) \in \mu_{q-1}$ und $\langle x \rangle \in U^{(1)}$ sind.

Satz 4.5. [Neu99, 3.4 Proposition, S.335]
Seien n, K, ν, R und $\mathfrak{p}$ wie im letzten Satz. Dann gilt für $a, b \in K^*$

$$\left(\frac{a,b}{\mathfrak{p}}\right)_n = \omega\left((-b)^\alpha/(-a)^\beta\right)^{(q-1)/n}.$$

Beweis. Wegen der Bemerkung genügt es den Fall zu betrachten wo $b = u \in R^*$ und $a = \pi$ Primelement im Bewertungsring R. Da die Restkörpercharakteristik kein Teiler von n ist, ist $L = K(\sqrt[n]{u})$ eine unverzweigte Körpererweiterung. Nach Satz 4.1 gilt

$$\left(\frac{\pi,u}{\mathfrak{p}}\right)_n \cdot \sqrt[n]{u} = (\pi, L/K)(\sqrt[n]{u}) = \phi_{L/K}(\sqrt[n]{u}),$$

wobei $\phi_{L/K}$ der Frobeniusautomorphismus ist. Deshalb gilt

$$\left(\frac{\pi,u}{\mathfrak{p}}\right) = \frac{\phi_{L/K}(\sqrt[n]{u})}{\sqrt[n]{u}} \equiv \sqrt[n]{u}^{q-1} \equiv u^{(q-1)/n} \equiv \omega(u)^{(q-1)/n} \mod \mathfrak{p}$$

und da die beiden äußeren Seiten dieser Gleichung Einheitswurzeln sind, folgt $\left(\frac{\pi,u}{\mathfrak{p}}\right) = \omega(u)^{(q-1)/n}$. Aus der Bemerkung folgt die Behauptung. □

Da Normrestalgebren über algebraischen Zahlkörpern und deren Vervollständigungen von Interesse sind und für endliche Stellen bereits der Zusammenhang mit dem Hilbertsymbol gezeigt wurde, soll nun auch das Hilbertsymbol über $\mathbb{R}$ und $\mathbb{C}$ definiert werden. Dazu benötigt man wieder das Normrestsymbol $(\quad, L/K) : K^* \to G(L/K), L$ eine endliche Galoiserweiterung von K. Man überlege sich, dass die Abbildung nur im Fall $K = \mathbb{R}$ und $L = \mathbb{C}$ nicht trivial ist. Außerdem kann dieser Fall nur für $n = 2$ auftreten, da K eine primitive n-te Einheitswurzel enthalten muss.

Definition 4.6. Definiere das *Normrestsymbol*

$$(\quad, \mathbb{C}/\mathbb{R}) : \mathbb{R}^* \longrightarrow G(\mathbb{C}/\mathbb{R})$$

als

$$(a, \mathbb{C}/\mathbb{R})(\sqrt{-1}) = \sqrt{-1}^{sgn(a)}.$$

Der Kern ist $\mathbb{R}_+^* = n_{\mathbb{C}/\mathbb{R}}\mathbb{C}^*$.

Analog zum lokalen Fall definiert man das Hilbertsymbol.

Definition 4.7. Sei K ein algebraischer Zahlkörper und $n \in \mathbb{N}$, sodass K die n-ten Einheitswurzeln μ_n enthält. Bezeichne mit $\mathfrak{p}$ eine unendliche Stelle von K. Definiere das *n-te Hilbertsymbol* über der Vervollständigung $K_\mathfrak{p}$ von K:

$$\left(\frac{\cdot}{\mathfrak{p}}\right)_n : K_\mathfrak{p}^* \times K_\mathfrak{p}^* \longrightarrow \mu_n,$$

$$\left(\frac{a,b}{\mathfrak{p}}\right)_n = \frac{(a, K(\sqrt[n]{b}))(\sqrt[n]{b})}{\sqrt[n]{b}}.$$

Man beachte, dass fast immer gilt $\left(\frac{a,b}{\mathfrak{p}}\right)_n = 1$. Nur im Fall $n = 2$, die Stelle $\mathfrak{p}$ reell und $b < 0$ gilt

$$\left(\frac{a,b}{\mathfrak{p}}\right)_n = (-1)^{\frac{1-sgn(a)}{2}}.$$

Wie auch im lokalen Fall erfüllt das Hilbertsymbol die Eigenschaften aus Satz 4.3 und da $A_\zeta(a, b \,|\, K)$ für $K = \mathbb{R}$ oder $\mathbb{C}$ außer im Fall $n = 2, K = \mathbb{R}$ und $a, b < 0$ immer zerfällt, lässt sich auch Satz 4.4 auf den reellen und komplexen Fall erweitern:

Korollar 4.8. *Sei K ein algebraischer Zahlkörper, der eine primitive n-te Einheitswurzel ζ enthält, und seien $a, b, c, d \in K^*$. Ist $\mathfrak{p}$ eine unendliche Stelle, so gilt:*

$$A_\zeta(a, b \,|\, K_\mathfrak{p}) \cong A_\zeta(c, d \,|\, K_\mathfrak{p}) \Longleftrightarrow \left(\frac{a,b}{\mathfrak{p}}\right)_n = \left(\frac{c,d}{\mathfrak{p}}\right)_n$$

Korollar 4.9. *Bezeichne mit $\mathfrak{p}$ nun eine beliebige endliche oder unendliche Stelle von K. Dann gilt für alle Stellen $\mathfrak{p}$:*

$$A_\zeta(a, b \,|\, K_\mathfrak{p}) \textit{ zerfällt} \Longleftrightarrow \left(\tfrac{a,b}{\mathfrak{p}}\right)_n = 1$$

Beweis. Nach Korollar 2.11, Satz 4.3 Punkt 3. und Korollar 4.8 gilt für alle Stellen

$$A_\zeta(a, b \,|\, K) \cong M_n(K) \Longleftrightarrow a \in n_{K(\sqrt[n]{b})/K}(K(\sqrt[n]{b})^*) \Longleftrightarrow \left(\frac{a,b}{\mathfrak{p}}\right)_n = 1.$$

□

Folgendes Ergebnis aus der Klassenkörpertheorie wird später noch ein wichtiges Hilfsmittel darstellen:

Satz 4.10. *Seien K ein algebraischer Zahlkörper und $n \in \mathbb{N}, n \geq 2$, sodass K die n-ten Einheitswurzeln enthält. Bezeichne mit $\mathfrak{p}$ sowohl eine Stelle von K als auch das maximale Ideal in $K_\mathfrak{p}$ im endlichen Fall und mit Ω die Menge aller Stellen. Dann gilt für $a, b \in K^*$:*

$$\prod_{\mathfrak{p} \in \Omega} \left(\frac{a, b}{\mathfrak{p}} \right)_n = 1$$

Beweis. [Neu99, S.414, Theorem 8.1] □

Im Fall $n = 2$ lässt sich das Hilbertsymbol mit Hilfe quadratischer Formen bestimmen:

Lemma 4.11. *Sei K ein algebraischer Zahlkörper, $\mathfrak{p}$ eine endliche oder unendliche Stelle und $a, b \in K^*$. Dann gilt:*

$$\left(\frac{a, b}{\mathfrak{p}} \right)_2 = 1 \iff aX^2 + bY^2 = Z^2 \text{ hat eine nicht triviale Lösung in } K_\mathfrak{p}.$$

Beweis. Nach Punkt 3. in Satz 4.3 ist $\left(\frac{a,b}{\mathfrak{p}} \right)_2 = 1$ genau dann, wenn a Norm eines Elements der Körpererweiterung $K_\mathfrak{p}(\sqrt{b})$ ist. Angenommen a ist Norm von $x + y\sqrt{b}$, dann gilt $a = x^2 - y^2 b$ und $(1, y, x)$ ist eine Lösung von $aX^2 + bY^2 = Z^2$. Sei umgekehrt (x_1, x_2, x_3) eine Lösung. Ist $x_1 = 0$, so sind $x_2, x_3 \neq 0$ und $b = \left(\frac{x_3}{x_2} \right)^2$ ist ein Quadrat in K und

$$\left(\frac{a, b}{\mathfrak{p}} \right)_2 = \left(\frac{a, x_3 {x_2}^{-1}}{\mathfrak{p}} \right)_2^2 = 1.$$

Ist $x_1 \neq 0$, dann ist $a = \left(\frac{x_3}{x_1} \right)^2 - b \left(\frac{x_2}{x_1} \right)^2$ Norm von $\frac{x_3}{x_1} - \frac{x_2}{x_1}\sqrt{b}$. □

5 Der Fall $n = 2$, Quaternionenalgebren

Wie in Korollar 2.3 bereits gezeigt wurde, stimmt im Fall $n = 2$ die Normrestalgebra $A_{-1}(a, b \mid K)$ über einem Körper K mit der Quaternionenalgebra $\mathcal{Q} = Q(a, b \mid K)$ überein. Nach Lemma 2.4 können nur zwei Fälle eintreten: entweder ist $\mathcal{Q}$ eine Divisionsalgebra oder isomorph zur Matrizenalgebra $M_2(K)$.

Satz 5.1. *Sei $\mathcal{Q} = Q(a, b \mid K)$ mit $a, b \in K^*$. Dann sind folgende Aussagen äquivalent:*

1. *$\mathcal{Q}$ ist isomorph zu $M_2(K)$, also keine Divisionsalgebra.*
2. *Es gibt ein Element y in $L = K(\sqrt{b})$, sodass $a = n_{L/K}(y)$ Norm von y ist.*
3. *Die quadratische Form $aX^2 + bY^2 = Z^2$ hat eine nichttriviale Lösung in K.*

Beweis. 1. $\Leftrightarrow$ 2. ist genau die Aussage von Korollar 2.11
2. $\Leftrightarrow$ 3. lässt sich analog zu Lemma 4.11 beweisen. □

Satz 2.5 liefert in diesem Fall wohlbekannte Eigenschaften der Quaternionenalgebren.

Korollar 5.2. *Seien $a, b \in K^*$*

1. *$Q(a, b \mid K) \cong Q(a\lambda^2, b\mu^2 \mid K)$ für alle $\lambda, \mu \in K^*$,*
2. *$Q(a, b \mid K) \cong Q(a, -ab \mid K)$,*
3. *$Q(a, b \mid K) \cong Q(b, a \mid K)$.*

Das Ziel ist es maximale Ordnungen in Quaternionenalgebren über einem algebraischen Zahlkörper zu bestimmen. Seien also K ein algebraischer Zahlkörper und R der Ring der ganzen Zahlen in K. Um die Diskriminante einer maximalen R-Ordnung in $\mathcal{Q} := Q(a, b \mid K)$ bestimmen zu können, ist es nötig für alle Stellen $\mathfrak{p}$ die Struktur von $\mathcal{Q} \otimes K_\mathfrak{p} = Q(a, b \mid K_\mathfrak{p})$ zu kennen, wobei $K_\mathfrak{p}$ die Vervollständigung von K an der Stelle $\mathfrak{p}$ bezeichnet. Im Gegensatz zum allgemeinen Fall der Normrestalgebren, weiß man hier auch dann über die Isomorphieklassen von $\mathcal{Q}$ über $K_\mathfrak{p}$ Bescheid, wenn die Restkörpercharakteristik ein Teiler von n ist, also in diesem Fall von 2; man spricht von dyadischen Primidealen.

Definition 5.3. Man nennt ein Primideal $\mathfrak{p}$ und die zugehörige Primstelle in einem algebraischen Zahlkörper K *dyadisch,* wenn die Charakteristik des Restklassenkörpers $\operatorname{char} R_\mathfrak{p}/\mathfrak{p}$ gleich 2 ist.

Satz 5.4. *Seien K ein algebraischer Zahlkörper und $K_\mathfrak{p}$ die Vervollständigung bezüglich einer endlichen Stelle. Dann gibt es bis auf Isomorphie genau zwei Quaternionenalgebren über $K_\mathfrak{p}$, nämlich $M_2(K_\mathfrak{p})$ und eine Divisionsalgebra.*

Beweis. [Mac03, Theorem 2.6.3, S.95] □

Daraus ergibt sich ganz allgemein:

$$Q(a,b \mid K_\mathfrak{p}) \cong Q(c,d \mid K_\mathfrak{p}) \iff \left(\frac{a,b}{\mathfrak{p}}\right)_2 = \left(\frac{c,d}{\mathfrak{p}}\right)_2$$

für alle Stellen $\mathfrak{p}$ und $a,b,c,d \in K^*$. Nun zerfällt bzw. verzweigt eine Quaternionenalgebra $Q(a,b \mid K)$ genau dann an der Stelle $\mathfrak{p}$, wenn $aX^2+bY^2 = Z^2$ in $K_\mathfrak{p}$ nicht-trivial lösbar bzw. nicht lösbar ist. Dies lässt sich für die meisten Stellen leicht berechnen, nur die dyadischen Primstellen benötigen eine gesonderte Betrachtung.

5.1 Verzweigung im nicht dyadischen Fall

Siehe dazu [Mac03, §2.5-2.6, S. 92-98].

Satz 5.5. *Sei $\mathcal{Q} := Q(a,b \mid K)$ eine Quaternionenalgebra über einem algebraischen Zahlkörper K mit $a,b \in R \setminus \{0\}$ und sei Ω die Menge der Stellen.*

1. *Ist $\mathfrak{p} \in \Omega$ eine komplexe Stelle, so zerfällt $\mathcal{Q}$ bei $\mathfrak{p}$.*
2. *Sei $\mathfrak{p} \in \Omega$ eine reelle Stelle. $\mathcal{Q}$ verzweigt genau dann bei $\mathfrak{p}$, wenn für die entsprechende Einbettung $\sigma_\mathfrak{p} : K \to \mathbb{R}$ gilt $\sigma_\mathfrak{p}(a) < 0$ und $\sigma_\mathfrak{p}(b) < 0$.*
3. *Sei $\mathfrak{p}$ ein nicht dyadisches Primideal.*
   a) *Wenn $a,b \notin \mathfrak{p}$, dann ist das Hilbertsymbol $\left(\frac{a,b}{\mathfrak{p}}\right)_2 = 1$, also zerfällt $\mathcal{Q}$ bei $\mathfrak{p}$.*
   b) *Wenn $a \notin \mathfrak{p}, b \in \mathfrak{p} \setminus \mathfrak{p}^2$, dann ist das Hilbertsymbol $\left(\frac{a,b}{\mathfrak{p}}\right)_2 = \left(\frac{a}{\mathfrak{p}}\right)$ gleich dem Legendre Symbol, also zerfällt $\mathcal{Q}$ genau dann bei $\mathfrak{p}$, wenn $a \bmod \mathfrak{p}$ ein Quadrat ist.*
   c) *Wenn $a,b \in \mathfrak{p} \setminus \mathfrak{p}^2$, dann zerfällt $\mathcal{Q}$ genau dann bei $\mathfrak{p}$, wenn $-a^{-1}b$ ein Quadrat in $R_\mathfrak{p}/\mathfrak{p}$ ist.*

Beweis. Benutze die Eigenschaften aus Korollar 5.2.

1. Da für komplexe Stellen gilt $K_\mathfrak{p} = \mathbb{C}$ und weil in $\mathbb{C}$ jedes Element eine Wurzel besitzt, zerfällt $\mathcal{Q}$ dort immer.
2. Es ist $K_\mathfrak{p} = \mathbb{R}$ und da in $\mathbb{R}$ jedes Element als $\pm x^2$ dargestellt werden kann, hat jede Quaternionenalgebra über $\mathbb{R}$ die Form $Q(\pm 1, \pm 1 \mid \mathbb{R})$. Damit ist die einzige Quaternionenalgebra, die nicht zerfällt, die Hamiltonsche Quaternionenalgebra $\mathcal{H} = Q(-1,-1 \mid \mathbb{R})$, da -1 nicht Norm eines Elements in $\mathbb{R}(\sqrt{-1}) = \mathbb{R}(i)$ sein kann.
3. a) Da $a,b \notin \mathfrak{p}$ und $\mathfrak{p} \nmid (2)$ ist $K_\mathfrak{p}(\sqrt{b})$ nach Lemma 1.3 eine unverzweigte Körpererweiterung und a ist nach dem Normensatz Norm eines Elements $x \in K_\mathfrak{p}(\sqrt{b})$, also zerfällt $\mathcal{Q}$ bei $\mathfrak{p}$.
   b) Hat die Gleichung $aX^2 + bY^2 = Z^2$ eine nicht-triviale Lösung in $K_\mathfrak{p}$, so muss sie auch in $R_\mathfrak{p}/\mathfrak{p}$ eine besitzen. Hat aber a modulo $\mathfrak{p}$ keine Wurzel, so ist dies unmöglich. Ist andererseits a kongruent zu einem Quadrat in $R_\mathfrak{p}/\mathfrak{p}$, so ist nach Hensels Lemma $a = \mu^2$ selbst ein Quadrat in $K_\mathfrak{p}$ und $aX^2 + bY^2 = Z^2$ hat die Lösung $(1,0,\mu)$.
   c) Es ist $Q(a,b \mid K) \cong Q(-ab^{-1}, b \mid K)$, wobei das Element $-ab^{-1}$ in $R_\mathfrak{p}^*$ liegt. Die Aussage folgt dann aus (b).

□

5.2 Der dyadische Fall, Quadratischer Defekt

Wenn $\mathfrak{p}$ ein dyadisches Primideal ist, d.h. die Mächtigkeit des Restklassenkörpers ist eine Potenz von 2, lässt sich nicht so leicht feststellen, ob $\mathcal{Q}$ bei $\mathfrak{p}$ zerfällt. Man kann aber spezielle Elemente bestimmen, mit deren Hilfe man Aussagen über das Hilbertsymbol machen kann. Dazu sei $\mathfrak{p}$ dyadisch, $K_\mathfrak{p}$ die Vervollständigung eines algebraischen Zahlkörpers K bei $\mathfrak{p}$ und $R_\mathfrak{p}$ der Bewertungsring in $K_\mathfrak{p}$. Jedes Element $e \in K_\mathfrak{p}$ hat mindestens eine Darstellung

$$e = x^2 + y$$

mit $x, y \in K_\mathfrak{p}$.

Definition 5.6. Man definiert ein $R_\mathfrak{p}$-Ideal

$$\delta_\mathfrak{p}(e) := \bigcap_y y \cdot R_\mathfrak{p}$$

wobei y über alle möglichen Darstellungen von e wie eben läuft. Dieses Ideal $\delta_\mathfrak{p}(e)$ wird als *quadratischer Defekt* von e bezeichnet. Offensichtlich ist $\delta_\mathfrak{p}(x^2)$ immer gleich (0).

Lemma 5.7. *Der quadratische Defekt $\delta_\mathfrak{p}(e)$ einer Einheit $e \in R_\mathfrak{p}^*$ ist stets (0) oder eine ungerade Potenz von $\mathfrak{p}$, die $4R_\mathfrak{p}$ enthält. Das heißt $\delta_\mathfrak{p}(e)$ ist immer eines der Ideale*

$$(0) \subset 4R_\mathfrak{p} \subset 4\mathfrak{p}^{-1} \subset 4\mathfrak{p}^{-3} \subset ... \subset \mathfrak{p}^3 \subset \mathfrak{p}$$

Beweis. [O'M63, 63:2, S.160] □

Besonders nützliche Eigenschaften haben die Elemente $e \in R_\mathfrak{p}^*$ mit quadratischem Defekt $\delta_\mathfrak{p}(e) = 4R_\mathfrak{p}$, das heißt e ist ein Quadrat in $R_\mathfrak{p}/(4)$, aber e ist kein Quadrat in $R_\mathfrak{p}/4\mathfrak{p}$.

Lemma 5.8. *Sei e ein Element in $R_\mathfrak{p}^*$ mit quadratischen Defekt $\delta_\mathfrak{p}(e) = 4R_\mathfrak{p}$. Dann gilt:*

$$\left(\frac{e, \pi}{\mathfrak{p}}\right)_2 = -1 \text{ und } \left(\frac{e, u}{\mathfrak{p}}\right)_2 = 1,$$

wobei $u \in R_\mathfrak{p}^*$ und π ein Primelement in $R_\mathfrak{p}$ sind.

Beweis. [O'M63, 63:11a, S.165] □

Das nächste Lemma garantiert die Existenz eines solchen Elements

Lemma 5.9. *Es gibt immer ein Element e in $R_\mathfrak{p}^*$ mit quadratischem Defekt $\delta_\mathfrak{p}(e) = 4R_\mathfrak{p}$ und für alle weiteren Elemente $e' \in R_\mathfrak{p}^*$ mit $\delta_\mathfrak{p}(e') = 4R_\mathfrak{p}$ gilt:*

$$e' = e \cdot u^2$$

für ein $u \in R_\mathfrak{p}^*$.

Beweis. [O'M63, 63:4, S.161] □

5.3 Quaternionenalgebren und ihre Diskriminante

Die Ergebnisse aus diesem und dem nächsten Abschnitt stammen aus Lemurells Artikel [Lem], wo sie eher knapp ausgeführt sind. Im Rahmen dieser Arbeit spielen diese Ergebnisse eine zentrale Rolle, da sie es unter bestimmten Voraussetzungen ermöglichen, explizit eine Basis einer maximalen Ordnung in einer Quaternionenalgebra über einem algebraischen Zahlkörper zu finden. Dazu sind hier die zwei wesentlichen Theoreme und Beweise umfassend ausgearbeitet. Ausgehend von den folgenden Resultaten ist das Ziel dieser Arbeit, Ähnliches allgemein für Normrestalgebren zu zeigen.

Hat man das Verzweigungsverhalten einer Quaternionenalgebra $\mathcal{Q}$ über einem algebraischen Zahlkörper K bestimmt, so kennt man die Diskriminante einer maximalen Ordnung in $\mathcal{Q}$. In Anlehnung an diese kann man die Diskriminante von $\mathcal{Q}$ und einen Repräsentanten d derselben definieren, mit dessen Hilfe man ein Element a im Ring der ganzen Zahlen R in K finden kann, sodass $Q(a, d \mid K)$ isomorph ist zu $\mathcal{Q}$. Außerdem bringt a viele praktische Eigenschaften mit, die es letztendlich ermöglichen werden, explizit Basiselemente einer maximalen Ordnung in $Q(a, d \mid K)$ anzugeben.

Definition 5.10. Die Menge aller Stellen, bei denen eine Quaternionenalgebra $\mathcal{Q}$ verzweigt, wird mit $\mathrm{Ram}(\mathcal{Q})$ bezeichnet und mit $\mathrm{Ram}_\infty(\mathcal{Q})$ bzw. $\mathrm{Ram}_0(\mathcal{Q})$ die Teilmenge von $\mathrm{Ram}(\mathcal{Q})$ der unendlichen bzw. der endlichen Stellen. Die *Diskriminante* $d(\mathcal{Q})$ der Quaternionenalgebra $\mathcal{Q}$ ist definiert als das Ideal

$$d(\mathcal{Q}) = \prod_{\mathfrak{p} \in \mathrm{Ram}_0(\mathcal{Q})} \mathfrak{p}.$$

Definition 5.11. Sei $d(\mathcal{Q}) = \mathfrak{p}_1 \cdots \mathfrak{p}_r$ die Diskriminante einer Quaternionenalgebra und seien $n_i \in \mathbb{N}$, sodass $(d) = \mathfrak{p}_1^{n_1} \cdots \mathfrak{p}_r^{n_r}$ ein Hauptideal ist. Einen Erzeuger d dieses Ideals nennt man *Repräsentant* von $\mathrm{d}(\mathcal{Q})$.

Man beachte, dass wegen der Endlichkeit der Idealklassengruppe immer ein Repräsentant der Diskriminante existiert.

Theorem 5.12. [Lem, 2.10 Proposition]
Seien K ein algebraischer Zahlkörper, R der Ring der ganzen Zahlen in K und sei $\mathcal{Q} = Q(\alpha, \beta \mid K), \alpha, \beta \in R \setminus \{0\}$ eine Quaternionenalgebra über K, die folgendes erfüllt: Die Diskriminante von $\mathcal{Q}$ ist gleich $d(\mathcal{Q}) = R$ oder $d(\mathcal{Q}) = \mathfrak{p}_1 \cdots \mathfrak{p}_r$ und $d(\mathcal{Q})$ besitzt einen Repräsentanten $d, (d) = \mathfrak{p}_1^{n_1} \cdots \mathfrak{p}_r^{n_r}$, sodass alle n_i ungerade sind und $\sigma(d) < 0$ für alle reellen Stellen ν_σ, die in $\mathcal{Q}$ verzweigen. Dann existiert ein Primelement a in R, für das gilt $\mathrm{ggT}(a, d) = 1$ *und*

1. *$\sigma(a) < 0$, bei allen reellen Stellen ν_σ, die in $\mathcal{Q}$ verzweigen,*
2. *$\sigma(a) > 0$, bei allen reellen Stellen ν_σ, die in $\mathcal{Q}$ zerfallen,*
3. *$\left(\frac{a}{\mathfrak{p}}\right) = -1$, für alle nicht dyadischen Primstellen $\mathfrak{p}$, die in $\mathcal{Q}$ verzweigen,*
4. *$\delta_\mathfrak{p}(a) = 4R_\mathfrak{p}$ für alle dyadischen Stellen $\mathfrak{p}$.*

Es gilt $\mathcal{Q} \cong Q(a, d \mid K)$.

Beweis. Angenommen es existiert ein Element a mit obigen Eigenschaften. Vergleiche mit Hilfe von Satz 5.5 und Abschnitt 5.2 das Verzweigungsverhalten von $\mathcal{Q}$ und $\mathcal{Q}' := Q(a, d \mid K)$. Es gilt

$$\mathrm{Ram}_\infty(\mathcal{Q}') = \mathrm{Ram}_\infty(\mathcal{Q}),$$

denn für $\sigma \in \mathrm{Ram}_\infty(\mathcal{Q})$ gilt $\sigma(a) < 0$ und $\sigma(d) < 0$ und für alle $\sigma \notin \mathrm{Ram}_\infty(\mathcal{Q})$ gilt $\sigma(a) > 0$.

Für alle dyadischen Stellen $\mathfrak{p}$ gilt $\delta_\mathfrak{p}(a) = 4R_\mathfrak{p}$ und nach den Eigenschaften des quadratischen Defekts aus Lemma 5.8 gilt $\left(\frac{a,d}{\mathfrak{p}}\right)_2 = -1$ genau dann, wenn $(d) = \mathfrak{p}^{n_\mathfrak{p}} \cdot \mathfrak{q}, ggT(\mathfrak{p}, \mathfrak{q}) = 1$ und $n_\mathfrak{p}$ ungerade. Also gilt $\mathfrak{p} \in \mathrm{Ram}(\mathcal{Q}')$ genau dann wenn $\mathfrak{p} \in \mathrm{Ram}(\mathcal{Q})$.

Für die endlichen, nicht-dyadischen Stellen $\mathfrak{p} \in \mathrm{Ram}(\mathcal{Q})$ gilt

$$\left(\frac{a, d}{\mathfrak{p}}\right)_2 = \left(\frac{a}{\mathfrak{p}}\right) = -1,$$

da (d) das Produkt ungerader Potenzen der $\mathfrak{p}$ ist und daher $\mathfrak{p} \in \mathrm{Ram}(\mathcal{Q}')$.

Für alle endlichen Stellen $\mathfrak{p} \notin \mathrm{Ram}(\mathcal{Q}), \mathfrak{p} \neq (a)$, nicht dyadisch gilt $a, d \in R_\mathfrak{p}^*$ und nach dem Normensatz $\left(\frac{a,d}{\mathfrak{p}}\right)_2 = 1$. Daher können sich $\mathrm{Ram}(\mathcal{Q})$ und $\mathrm{Ram}(\mathcal{Q}')$ nur durch die Primstelle (a) unterscheiden, aber da nach Satz 4.10 $|\mathrm{Ram}(\mathcal{Q}')|$ gerade sein muss, kann (a) nicht zusätzlich in $\mathrm{Ram}(\mathcal{Q}')$ liegen. Es gilt $\mathrm{Ram}(\mathcal{Q}') = \mathrm{Ram}(\mathcal{Q})$ und

$$\mathcal{Q} \cong Q(a, d \mid K).$$

Zur Existenz von a: Für jede dyadische Stelle $\mathfrak{p}$ sei $e_\mathfrak{p} \in R_\mathfrak{p}^*$ ein Element mit $\delta_\mathfrak{p}(e_\mathfrak{p}) = 4R_\mathfrak{p}$ und für alle nicht dyadischen Stellen $\mathfrak{p} \in \mathrm{Ram}_0(\mathcal{Q})$ setze $u_\mathfrak{p} = (-1)^{\nu(\alpha)\nu(\beta)} \frac{\beta^{\nu(\alpha)}}{\alpha^{\nu(\beta)}}$ in $R_\mathfrak{p}^*, \nu$ die normierte Bewertung auf $K_\mathfrak{p}$. Dann ist $u_\mathfrak{p}$ nach den Überlegungen in Abschnitt 2.3 kein Quadrat in $K_\mathfrak{p}$. Der Approximationssatz 1.5 liefert für alle $\varepsilon > 0$ ein Element $\bar{a} \in K$ mit

$|\bar{a} - e_\mathfrak{p}|_\mathfrak{p} < \varepsilon$ für alle dyadischen Stellen $\mathfrak{p}$,

$|\bar{a} - u_\mathfrak{p}|_\mathfrak{p} < \varepsilon$ für alle endlichen, nicht dyadischen Stellen $\mathfrak{p} \in \mathrm{Ram}(\mathcal{Q})$,

$|\bar{a} + 1|_\nu < \varepsilon$ für alle reellen Stellen $\nu \in \mathrm{Ram}_\infty(\mathcal{Q})$,

$|\bar{a} - 1|_\nu < \varepsilon$ für alle reellen Stellen $\nu \notin \mathrm{Ram}_\infty(\mathcal{Q})$.

Für ε hinreichend klein gilt

$\bar{a} \equiv e_\mathfrak{p} \mod 4\mathfrak{p}$ für alle dyadischen Stellen $\mathfrak{p}$,

$\bar{a} \equiv u_\mathfrak{p} \mod \mathfrak{p}$ für alle endlichen, nicht dyadischen Stellen $\mathfrak{p} \in \mathrm{Ram}(\mathcal{Q})$,

$\sigma_\nu(\bar{a}) < 0$ für alle reellen Stellen ν bei denen $\mathcal{Q}$ verzweigt,

$\sigma_\nu(\bar{a}) > 0$ für alle reellen Stellen ν bei denen $\mathcal{Q}$ zerfällt.

Damit erfüllt $\bar{a}$ die Eigenschaften (1) bis (4) aus dem Theorem.

Betrachte nun die schmale Klassengruppe $I_K(\mathcal{M})/P_K(\mathcal{M})$ mit Modulus $\mathcal{M} = \prod_{\mathfrak{p}\in\Omega} \mathfrak{p}^{\nu_\mathfrak{p}}$, wobei Ω die Menge aller Stellen, $\nu_\mathfrak{p} = 1$ für alle reellen Stellen und $\nu_\mathfrak{p} = \nu_\mathfrak{p}(8d)$ sind. Das heißt $\mathfrak{p} \mid \mathcal{M}$ für alle $\mathfrak{p} \in \mathrm{Ram}(\mathcal{Q})$ und $4\mathfrak{p} \mid \mathcal{M}$ für alle $\mathfrak{p}$ dyadisch. Dann haben alle Ideale in der Klasse des Hauptideals $(\bar{a})$ in $I_K(\mathcal{M})/P_K(\mathcal{M})$ Erzeuger, die die Eigenschaften (1) bis (4) erfüllen. Aus Korollar 1.10 folgt, dass diese Klasse auch ein Primideal (a) enthält. □

Bemerkung. In Lemurells Artikel wird nicht verlangt, dass $\sigma(d) < 0$ für alle reellen Stellen ν_σ, die in $\mathcal{Q}$ verzweigen. Da zu einem Hauptideal nicht immer ein Erzeuger existiert, der diese Bedingung erfüllt, diese Eigenschaft für die Isomorphie aber notwendig ist, wie man im Beweis sieht, muss die Existenz vorausgesetzt werden.

Im Spezialfall $K = \mathbb{Q}$ hat obiger Satz folgende besonders einfache Form:

Korollar 5.13. *Sei $\mathcal{Q}$ eine Quaternionenalgebra über $\mathbb{Q}$ mit Diskriminante $d(\mathcal{Q}) = p_1 \cdots p_{2r} = d$, p_i paarweise verschiede Primzahlen, das heißt $\mathrm{Ram}_\infty(\mathcal{Q}) = \emptyset$. Dann existiert eine Primzahl p für die gilt*

$$p \equiv 5 \mod 8 \quad \text{und} \quad \left(\frac{p}{p_i}\right) = -1 \quad \text{für alle } p_i > 2,$$

und es gilt $\mathcal{Q} \cong Q(p, d \mid \mathbb{Q}) \cong Q(p, -d \mid \mathbb{Q})$.

Korollar 5.14. *Sei $\mathcal{Q}$ eine Quaternionenalgebra über $\mathbb{Q}$ mit Diskriminante $d(\mathcal{Q}) = p_1 \cdots p_{2r-1} = d$, p_i paarweise verschiede Primzahlen, also $\mathrm{Ram}_\infty(\mathcal{Q}) \neq \emptyset$. Dann existiert eine Primzahl p für die gilt*

$$p \equiv 3 \mod 8 \quad \text{und} \quad \left(\frac{p}{p_i}\right) = -1 \quad \text{für alle } p_i > 2,$$

und es gilt $\mathcal{Q} \cong Q(-p, -d \mid \mathbb{Q})$.

5.4 Basis einer maximalen Ordnung

Sei nun eine Quaternionenalgebra $\mathcal{Q}$ über einem algebraischen Zahlkörper K gegeben, deren Diskriminante $d(\mathcal{Q}) = (d)$ ein Hauptideal mit Erzeuger d ist, für den gilt $\sigma(d) < 0$ für alle σ, die in $\mathcal{Q}$ verzweigen. Nach Theorem 5.12 existiert ein Element a im Ring der ganzen Zahlen R in K, sodass $\mathcal{Q}$ isomorph ist zu $Q(a, d \mid K)$. Die zugehörige R-Ordnung $\mathcal{O}_{-1} = \langle 1, i, j, k\rangle$ hat nach Abschnitt 3.3 Diskriminante $d(\mathcal{O}_{-1}) = (4ad)^2$.
Nach den Überlegungen in Abschnitt 3.2 muss für die Diskriminante einer maximalen Ordnung $\mathcal{O}_m$ gelten $d(\mathcal{O}_m) = d(\mathcal{Q})^2 = (d)^2$. Da für zwei Ordnungen $\mathcal{O}_1 \supset \mathcal{O}_2$ mit Basis gilt $d(\mathcal{O}_2) = [\mathcal{O}_1 : \mathcal{O}_2]^2 \cdot d(\mathcal{O}_1)$, ist eine Ordnung $\mathcal{O} \supset \mathcal{O}_{-1}$ mit Basis genau dann maximal, wenn gilt $[\mathcal{O} : \mathcal{O}_{-1}] \cdot R = 4a \cdot R$.
Nach Konstruktion von a gilt

$$a \equiv m^2 \mod (4) \quad \text{für ein } m \in R,$$

$$d \equiv x^2 \mod (a) \quad \text{für ein } x \in R,$$

da $\mathcal{Q}$ bei (a) zerfällt.

Bezeichne mit $1, i, j, k$ die Standardbasis von $Q := Q(a, d \mid K)$ und setze

$$e_1 = \frac{i-m}{2} \qquad \text{und} \qquad e_2 = \frac{k-xi}{a}.$$

Dann ist

$$e_1 \cdot e_2 = \frac{1}{2a} \cdot (-xa + xmi + aj - mk).$$

Mit Hilfe der Formeln aus Abschnitt 3.1 lassen sich Norm und Spur berechnen:

$$\mathrm{n}_{\mathrm{Q/K}}(e_1) = \frac{m^2-a}{4}, \qquad \mathrm{tr}_{\mathrm{Q/K}}(e_1) = -m,$$

$$\mathrm{n}_{\mathrm{Q/K}}(e_2) = \frac{d-x^2}{a}, \qquad \mathrm{tr}_{\mathrm{Q/K}}(e_2) = 0$$

und

$$\mathrm{tr}_{\mathrm{Q/K}}(e_1 \cdot e_2) = -x.$$

Da außerdem für alle Elemente z in Q gilt $z^2 - \mathrm{tr}_{\mathrm{Q/K}}(z) \cdot z + \mathrm{n}_{\mathrm{Q/K}}(z) = 0$, erfüllen e_1, e_2 und e_1e_2 folgende Gleichungen:

$$e_1^2 = -m \cdot e_1 - \frac{m^2-a}{4}, \quad e_2^2 = -\frac{d-x^2}{a} \quad \text{und} \quad (e_1e_2)^2 = -x \cdot e_1e_2 - \frac{m^2-a}{4} \cdot \frac{d-x^2}{a}$$

und e_1, e_2 und e_1e_2 sind ganz. Mit ein wenig Rechenarbeit erhält man

$$e_2 \cdot e_1 = -e_1 \cdot e_2 - m \cdot e_2 - x.$$

Somit ist der endlich erzeugte R-Modul $\mathcal{O} = \langle 1, e_1, e_2, e_1e_2 \rangle$ abgeschlossen bezüglich der Multiplikation und damit ein Ring. Offensichtlich ist $K \cdot \mathcal{O} = Q(a, d \,|\, K)$ und $\mathcal{O}$ ist eine R-Ordnung. Weiters berechnet man $[\mathcal{O} : \mathcal{O}_{-1}] = 4a$ und $\mathcal{O}$ ist maximal in $Q(a, d \,|\, K)$.

Zusammenfassend kann man folgendes Theorem formulieren:

Theorem 5.15. [Lem, 6.9 Proposition]
Seien K ein algebraischer Zahlkörper und R der Ring der ganzen Zahlen in K und sei $\mathcal{Q}$ eine Quaternionenalgebra über K, deren Diskriminante $d(\mathcal{Q})$ ein Hauptideal mit Erzeuger d ist, sodass $\sigma(d) < 0$ für alle reellen Stellen σ, bei denen $\mathcal{Q}$ verzweigt. Sei a ein Primelement in R wie in Theorem 5.12, sodass $\mathcal{Q}$ isomorph ist zu $Q(a, d \,|\, K)$. Dann existieren Elemente $x, m \in R$ für die gilt

$$a \equiv m^2 \mod (4) \quad \textit{und} \quad d \equiv x^2 \mod (a),$$

und die Elemente

$$e_1 = \frac{i-m}{2} \qquad \textit{und} \qquad e_2 = \frac{k-xi}{a}$$

erzeugen eine maximale R-Ordnung $\mathcal{O}$ in $Q(a, d \,|\, K)$ mit Basis $\{1, e_1, e_2, e_1e_2\}$.

Beispiel. In einer Quaternionenalgebra $\mathcal{Q}$ über $\mathbb{Q}$ lassen sich nun ganz einfach maximale $\mathbb{Z}$-Ordnungen angeben.
Sei z.B. $\mathcal{Q} = Q(15, 7 \,|\, \mathbb{Q})$. Da $15 > 0$ und $7 > 0$ ist $\mathrm{Ram}_\infty(\mathcal{Q}) = \emptyset$. Verzweigen können nur das Ideal (2) und Primideale, die 7 oder 15 teilen, also (3), (5) und (7). In den letzten

drei Fällen liefert Hensels Lemma, dass $\mathcal{Q}$ genau dann bei (p) zerfällt, wenn 15 bzw. 7 ein Quadrat in $\mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{Z}/p\mathbb{Z}$ ist. Es gilt

$7 \equiv 1 \mod 3$, also (3) zerfällt, da 1 Quadrat in $\mathbb{Z}/3\mathbb{Z}$ ist.

$7 \equiv 2 \mod 5$, also (5) verzweigt, da 2 kein Quadrat in $\mathbb{Z}/5\mathbb{Z}$ ist.

$15 \equiv 1 \mod 7$, also (7) zerfällt, da 1 Quadrat in $\mathbb{Z}/7\mathbb{Z}$ ist.

Da aus Satz 4.10 folgt, dass $|\operatorname{Ram}(\mathcal{Q}')|$ gerade ist, muss $\mathcal{Q}$ bei (2) verzweigen, also ist $\operatorname{Ram}(\mathcal{Q}) = \{(2), (5)\}$ und $d(\mathcal{Q}) = 10$. Suche nun a wie in Korollar 5.13, also

$a \equiv 2$ oder $3 \mod 5$ und $a \equiv 5 \mod 8$

Eine mögliche Lösung ist $a = 13$.

Damit gilt $\mathcal{Q} \cong Q(13, 10\,|\,\mathbb{Q})$, weiters

$a = 13 \equiv 1^2 \mod 4$ und $d = 10 \equiv 6^2 \mod 13$, setze also $m = 1$ und $x = 6$.

Die maximale Ordnung $\mathcal{O}$ hat dann folgende Form

$$\mathcal{O} = \left\langle 1, \frac{i-1}{2}, \frac{k-6i}{13}, \frac{1}{26} \cdot (-78 + 6i + 13j - k) \right\rangle .$$

6 Verallgemeinerung

Nachdem es auf Quaternionenalgebren gelungen ist, maximale Ordnungen zu finden, möchte man ähnliche Methoden auch in höherdimensionalen Normrestalgebren anwenden. Dazu muss man zuerst Theorem 5.12 verallgemeinern. Der Beweis stützt sich ebenfalls auf das Hilbertsymbol, wobei alle notwendigen Ergebnisse bereits in Kapitel 4 gesammelt wurden. Ein Vorteil gegenüber dem Spezialfall der Quaternionenalgebren ist, dass in den höherdimensionalen Algebren alle unendlichen Stellen automatisch komplex sind. Ein Nachteil ist, dass sich das Konzept des quadratischen Defekts nicht so einfach verallgemeinern lässt, da es großteils auf Eigenschaften von quadratischen Formen basiert. Deshalb muss ab jetzt vorausgesetzt werden, dass die betrachteten Normrestalgebren bei allen Primstellen zerfallen, die ihren Grad teilen.

6.1 Normrestalgebren und ihre Diskriminante

Definition 6.1. Sei K ein algebraischer Zahlkörper und A eine zentrale, einfache, n^2-dimensionale K-Algebra. Definiere die *Diskriminante* der Algebra A als das Ideal

$$d(A) = \prod_{\mathfrak{p}} \mathfrak{p}^{n-\kappa_{\mathfrak{p}}}$$

wobei $\mathfrak{p}$ über alle Primideale laufe und $\kappa_{\mathfrak{p}}$ die lokale Kapazität von A bei $\mathfrak{p}$ bezeichne.

Theorem 6.2. *Setze $n > 2$ voraus. Seien K ein algebraischer Zahlkörper, der eine primitive n-te Einheitswurzel ζ enthält, R der Ring der ganzen Zahlen in K und $\mathcal{A}_\zeta := A_\zeta(\alpha, \beta \,|\, K)$ die n^2-dimensionale Normrestalgebra zu $\alpha, \beta \in R \setminus \{0\}$. Weiters sei vorausgesetzt, dass die Diskriminante $d(\mathcal{A}_\zeta)$ von $\mathcal{A}_\zeta$ ein Hauptideal mit Erzeuger d ist und dass $\mathcal{A}_\zeta$ bei allen Stellen zerfällt, die n enthalten. Dann existiert ein Primelement $a \in R$ mit* $\mathrm{ggT}(a, d) = 1$,

1. $a \equiv 1 \mod (n)^2\mathfrak{p}$ *für alle Primstellen $\mathfrak{p}$, die n teilen und*
2. $\left(\frac{a,d}{\mathfrak{p}}\right)_n = \left(\frac{\alpha,\beta}{\mathfrak{p}}\right)_n$ *für alle Stellen $\mathfrak{p}$.*

Es gilt $\mathcal{A}_\zeta \cong A_\zeta(a, d \,|\, K)$.

Beweis. Da K eine primitive n-te Einheitswurzel enthält und n echt größer als 2 ist, ist die Vervollständigung $K_\sigma = \mathbb{C}$ für alle unendlichen Stellen σ . In $\mathbb{C}$ besitzt jedes Element eine n-te Wurzel. Deshalb zerfällt jede Normrestalgebra bei allen unendlichen Stellen σ und es gilt $\left(\frac{a,d}{\sigma}\right)_n = \left(\frac{\alpha,\beta}{\sigma}\right)_n = 1$.

Für ein Primideal $\mathfrak{p}$, das (n) nicht teilt, und für ein Primelement π in $R_\mathfrak{p}$ sei $u_\mathfrak{p}$ eine Einheit in $R_\mathfrak{p}$ und $\kappa(\mathfrak{p})$ eine natürliche Zahl wie in Abschnitt 2.3, sodass gilt

$$\mathcal{A}_\zeta \otimes K_\mathfrak{p} \cong A_\zeta(\pi^{\kappa(\mathfrak{p})}, u_\mathfrak{p} \,|\, K_\mathfrak{p}).$$

Das heißt $u_\mathfrak{p}$ erfüllt $u_\mathfrak{p}^{\kappa(\mathfrak{p})} \equiv (-1)^{\nu(\alpha)\nu(\beta)} \frac{\beta^{\nu(\alpha)}}{\alpha^{\nu(\beta)}} \mod K^{*n}$ und $X^n - u_\mathfrak{p}$ ist irreduzibel. Dort wurde außerdem gefolgert, dass die lokale Kapazität $\kappa_\mathfrak{p}$ der größte gemeinesame Teiler von $\kappa(\mathfrak{p})$ und n ist. Setze $\lambda(\mathfrak{p}) = \frac{\kappa(\mathfrak{p})}{\kappa_\mathfrak{p}}$. Analog zum Beweis von Theorem 5.12 kann man mit Hilfe des Approximationssatzes und Korollar 1.10 zeigen, dass ein Primelement a in $R_\mathfrak{p}$ existiert, für das gilt

- $a \equiv 1 \mod (n)^2\mathfrak{p}$ für alle Primstellen $\mathfrak{p}$, die n teilen und
- $a \equiv u_\mathfrak{p}^{\lambda(\mathfrak{p})} \mod \mathfrak{p}$ im Bewertungsring $R_\mathfrak{p}$ von $K_\mathfrak{p}$ für alle Primstellen $\mathfrak{p}$, bei denen $\mathcal{A}_\zeta$ verzweigt.

Ist $\mathfrak{p}$ eine Primstelle, die in $\mathcal{A}_\zeta$ verzweigt, so hat die Diskriminante d in $K_\mathfrak{p}$ die Form $d = u\pi^{n-\kappa_\mathfrak{p}}$, wobei u eine Einheit in $R_\mathfrak{p}$ ist. Da in $R_\mathfrak{p}$ gilt $au_\mathfrak{p}^{-\lambda(\mathfrak{p})} \equiv 1 \bmod \mathfrak{p}$, folgt aus Hensels Lemma, dass $au_\mathfrak{p}^{-\lambda(\mathfrak{p})}$ eine n-te Potenz $z^n \in R_\mathfrak{p}$ ist. Es gilt:

$$A_\zeta(a, d \,|\, K_\mathfrak{p}) = A_\zeta(z^n u_\mathfrak{p}^{\lambda(\mathfrak{p})}, u\pi^{n-\kappa_\mathfrak{p}} \,|\, K_\mathfrak{p}) \cong$$

$$A_\zeta(u^{n-1}\pi^{\kappa_\mathfrak{p}}, u_\mathfrak{p}^{\lambda(\mathfrak{p})} \,|\, K_\mathfrak{p}) \cong A_\zeta(\pi^{\kappa(\mathfrak{p})}, u_\mathfrak{p} \,|\, K_\mathfrak{p}) \cong \mathcal{A}_\zeta \otimes K_\mathfrak{p}$$

nach dem Normensatz und Satz 2.5.

Sei $\mathfrak{p}$ nun ein Primideal, das (n) teilt und sei $s \in \mathbb{N}$, sodass $\mathfrak{p}^s$ in $K_\mathfrak{p}$ gleich dem Hauptideal (n) ist. Dann gilt

$$f(X) = X^n - a \equiv X^n - 1 \bmod \mathfrak{p}^{2s+1} \text{ und daher}$$
$$f(1) \equiv 0 \bmod \mathfrak{p}^{2s+1} \text{ und } f'(1) = n \cdot 1^{n-1} \not\equiv 0 \bmod \mathfrak{p}^{s+1}.$$

Dann folgt aus Korollar 1.8, dass ein Element $\gamma \in R_\mathfrak{p}^*$ existiert, für das gilt $f(\gamma) = 0$. Damit hat $a = \gamma^n$ eine n-te Wurzel in $R_\mathfrak{p}$ und auch $A_\zeta(a, d \,|\, K)$ zerfällt bei $\mathfrak{p}$.

Für alle Primstellen $\mathfrak{p} \neq (a)$ und $\mathfrak{p} \nmid (n)$, bei denen $\mathcal{A}_\zeta$ zerfällt, sind a und d Elemente in $R_\mathfrak{p}^*$ und wegen dem Normensatz zerfällt auch $A_\zeta(a, d \,|\, K)$ bei allen diesen Stellen. Aus Satz 4.4 und Korollar 4.9 folgt nun, dass die n-ten Hilbertsymbole von $\mathcal{A}_\zeta$ und $A_\zeta(a, d \,|\, K)$ in allen bisher behandelten Fällen übereinstimmen. Alleine der Fall $\mathfrak{p} = (a)$ ist noch zu überprüfen.

Bezeichne mit Ω die Menge aller Stellen auf K, dann gilt nach Satz 4.10:

$$1 = \prod_{\mathfrak{p} \in \Omega} \left(\frac{a, d}{\mathfrak{p}}\right)_n = \left(\frac{a, d}{(a)}\right)_n \cdot \prod_{\mathfrak{p} \neq (a)} \left(\frac{a, d}{\mathfrak{p}}\right)_n = \left(\frac{a, d}{(a)}\right)_n \cdot \prod_{\mathfrak{p} \neq (a)} \left(\frac{\alpha, \beta}{\mathfrak{p}}\right)_n$$

Da $\mathcal{A}_\zeta$ an der Stelle (a) zerfällt und damit das Hilbertsymbol von $\mathcal{A}_\zeta$ dort gleich 1 ist, muss das Produkt auf der rechten Seite gleich 1 sein und darum auch $\left(\frac{a,d}{(a)}\right)_n = 1$. Also zerfällt $A_\zeta(a, d \,|\, K)$ an der Stelle (a). Daher stimmen $\mathcal{A}_\zeta \otimes K_\mathfrak{p}$ und $A_\zeta(a, d \,|\, K) \otimes K_\mathfrak{p}$ bei allen Stellen $\mathfrak{p}$ überein und es folgt $\mathcal{A}_\zeta \cong A_\zeta(a, d \,|\, K)$. □

Bemerkung. Die Voraussetzung, dass die Diskriminante $d(\mathcal{A}_\zeta) = \mathfrak{p}_1^{n-\kappa_{\mathfrak{p}_1}} \cdots \mathfrak{p}_r^{n-\kappa_{\mathfrak{p}_r}}$ ein Hauptideal sein muss, kann durch eine schwächere Voraussetzung ersetzt werden. Es genügt, wenn die Diskriminante $d(\mathcal{A}_\zeta)$ einen Repräsentanten d besitzt, $(d) = \mathfrak{p}_1^{n_1} \cdots \mathfrak{p}_r^{n_r}, n_i \in \mathbb{N}$, sodass für alle $i = 1, ..., r$ gilt $n_i + \kappa_{\mathfrak{p}_i} \equiv 0 \bmod n$.

6.2 Ordnungen in höherdimensionalen Normrestalgebren

In den Quaternionenalgebren liefert Theorem 5.12 eine Möglichkeit explizit Basiselemente einer maximalen Ordnung anzugeben. Nachdem nun Theorem 6.2 dessen Aussage auf höherdimensionale Normrestalgebren verallgemeinert, will man auch dort Basiselemente einer maximalen Ordnungen bestimmen.

Seien K ein algebraischer Zahlkörper, R der Ring der ganzen Zahlen in K und $n > 2$ eine natürliche Zahl, sodass K eine primitive n-te Einheitswurzel ζ enthält. Es sei $\mathcal{A}_\zeta$ eine n^2-dimensionale Normrestalgebra, die alle Voraussetzungen aus Theorem 6.2 erfüllt, das heißt $\mathcal{A}_\zeta$ zerfällt bei allen Primstellen, die (n) teilen, und die Diskriminante von $\mathcal{A}_\zeta$ ist ein Hauptideal in R mit Erzeuger d. Dann liefert das Theorem ein Primelement $a \in R$, sodass $\mathcal{A}_\zeta$ isomorph ist zu $A_\zeta(a, d \,|\, K)$. Betrachte nun wieder die Ordnung $\mathcal{O}_\zeta$ in $A_\zeta(a, d \,|\, K)$, die von $\{u^i v^j \mid 0 \leq i, j \leq n-1\}$ erzeugt wird, u, v wie in der Konstruktion der Algebra in Abschnitt 2.1, und deren Diskriminante in Abschnitt 3.3 bereits bestimmt wurde:

$$d(\mathcal{O}_\zeta) = (n^n a^{n-1} d^{n-1})^n \cdot R.$$

Existiert in $A_\zeta(a, d \,|\, K)$ eine maximale Ordnung $\mathcal{O}_m$, die eine Basis besitzt und $\mathcal{O}_\zeta$ enthält, so muss nach Lemma 3.8 für die Determinante der Übergangsmatrix von $\mathcal{O}_m$ zu $\mathcal{O}_\zeta$ gelten:

$$[\mathcal{O}_m : \mathcal{O}_\zeta]^2 \cdot R = n^{n^2} a^{(n-1)n} d^{(n-2)n} \cdot R.$$

Die Gleichung macht auch für n ungerade Sinn, da (d) in diesem Fall nach Definition das Produkt gerader Potenzen von Primidealen ist und auch (n) ist Quadrat eines Ideals in R. Es ist nämlich $\mathbb{Z}[\zeta] \subset R$ und jeder Primteiler p von n mit $n = p^{\nu_p} \cdot q$ und $\mathrm{ggT}(p, q) = 1$ besitzt in $\mathbb{Z}[\zeta]$ eine Faktorisierung in

$$(p) = (\mathfrak{p}_1 \cdots \mathfrak{p}_r)^{\varphi(p^{\nu_p})}$$

wobei $\mathfrak{p}_i$ paarweise verschiedene Primideale in $\mathbb{Z}[\zeta]$ sind. Da die Eulersche φ-Funktion angewendet auf eine Potenz einer ungeraden Primzahl immer gerade ist, ist auch n Produkt gerader Potenzen von Primidealen, siehe [Neu99, 10.3 Proposition, S.61]. Ist n zusätzlich eine Primzahl, so ist $n \cdot R = (1-\zeta)^{n-1} \cdot R$, siehe [Neu99, 10.1 Lemma, S. 59].
Eine weitere Beobachtung wird im Folgenden wichtig sein:

Lemma 6.3. *Unter obigen Voraussetzunge an a und d existiert ein Element y in R, sodass gilt*

$$d \equiv y^n \mod (a).$$

Beweis. Da gilt $\left(\frac{a,d}{(a)}\right)_n = 1$, ist d Norm eines Elements $x = c_0 + c_1 \sqrt[n]{a} + ... + c_{n-1} \sqrt[n]{a}^{n-1}$ in der Körpererweiterung $L := K_{(a)}(\sqrt[n]{a})$ der Vervollständigung $K_{(a)}$ mit $c_i \in K_{(a)}$ und $[L : K_{(a)}] = n$. Sei ν die normierte Bewertung auf $K_{(a)}$. Dann ist

$$\omega : L \to \mathbb{Z} \cup \{\infty\}, \quad z \mapsto \nu(n_{L/K_{(a)}}(z))$$

die eindeutige Fortsetzung der Bewertung ν auf L. Es gilt

$$\omega(\sqrt[n]{a}) = 1 \qquad \text{und} \qquad \omega(c) = n \cdot \nu(c) \quad \text{für alle } c \in K_{(a)}.$$

Es ist $d = n_{L/K_{(a)}}(x) = \prod_{k=0}^{n-1} \sigma^k(x)$, wobei σ den Erzeuger der zyklischen Galoisgruppe $G(L/K)$ bezeichne, der gegeben ist durch $\sigma(\sqrt[n]{a}) = \zeta \sqrt[n]{a}$. Weiters gilt für alle $k, 0 \leq k \leq n-1$,

$$\omega(\sigma^k(x)) \geq \min\{\omega(c_i \zeta^{ik} \sqrt[n]{a}^i), 0 \leq i \leq n-1\} = \min\{\omega(c_i) + i, 0 \leq i \leq n-1\}.$$

Für alle i liegt $\omega(c_i)$ in $n \cdot \mathbb{Z}$, daher ist $\omega(c_i) + i \neq \omega(c_j) + j$ für $i \neq j$ und darum gilt $\omega(\sigma^k(x)) = \min\{\omega(c_i) + i, 0 \leq i \leq n-1\}$, das heißt die Bewertung stimmt für alle Potenzen von σ überein. Daher gilt

$$0 = \omega(d) = n \cdot \omega(x) = n \cdot \min\{\omega(c_i) + i, 0 \leq i \leq n-1\}.$$

Daraus ergibt sich, dass alle $c_i, 0 \leq i \leq n-1$ schon in $R_{(a)}$ liegen und es gilt

$$d = n_{L/K_{(a)}}(c_0 + c_1 \sqrt[n]{a} + ... + c_{n-1} \sqrt[n]{a}^{n-1}) = c_0^n + c \cdot a$$

mit c_0 und c in $R_{(a)}$. Also ist d eine n-te Potenz in $R_{(a)}/(a) \cong R/(a)$. □

Hat d eine $(n-1)$-te Wurzel $\delta \in R$, so gilt

$$1 = \left(\frac{a, d}{(a)}\right)_n = \left(\frac{a, \delta}{(a)}\right)_n^{n-1}$$

und da das Hilbertsymbol eine n-te Einheitswurzel ist, muss gelten $\left(\frac{a,\delta}{(a)}\right)_n = 1$. Also gibt es auch für δ ein Element x, sodass gilt

$$\delta \equiv x^n \mod (a).$$

Unter diesen zusätzlichen Voraussetzung, lässt sich $[\mathcal{O}_m : \mathcal{O}_\zeta]$ als Produkt ganzer Zahlen und einer Einheit schreiben:

Korollar 6.4. *Seien n eine Primzahl, K wie oben und $\mathcal{A}_\zeta$ eine n^2-dimensionale Normrestalgebra, die bei allen Primstellen zerfällt, die n teilen, und deren Diskriminante ein Hauptideal mit Erzeuger d ist, sodass d eine $(n-1)$-te Wurzel δ besitzt. Ist $A_\zeta(a, d \,|\, K)$ die zu $\mathcal{A}_\zeta$ isomorphe Algebra aus Theorem 6.2, dann gilt für die Determinante $[\mathcal{O}_m : \mathcal{O}_\zeta]$ der Übergangsmatrix einer maximalen Ordnung $\mathcal{O}_m$ mit Basis zu $\mathcal{O}_\zeta$ in $A_\zeta(a, d \,|\, K)$:*

$$[\mathcal{O}_m : \mathcal{O}_\zeta] \cdot R = (1-\zeta)^{n^2(n-1)/2} \; a^{n(n-1)/2} \; \delta^{n(n-1)(n-2)/2} \cdot R.$$

Man beachte, dass $[\mathcal{O}_m : \mathcal{O}_\zeta]$ im Fall $n > 2$ nicht mehr unabhängig von d ist. Mit Hilfe dieser Überlegungen und Theorem 6.2 lassen sich auch in höherdimensionalen Normrestalgebren maximale Ordnungen finden, zuerst für den Fall $n = 3$, dann für $n = 5$, um den allgemeinen Fall zu motivieren.

6.2.1 Der Fall $n = 3$

Sei K ein algebraischer Zahlkörper, der eine primitive dritte Einheitswurzel ζ enthält, bezeichne mit R den Ring der ganzen Zahlen in K und sei $\mathcal{A}_\zeta$ eine 9-dimensionale Normrestalgebra über K, die alle Voraussetzungen aus Theorem 6.2 erfüllt. Das heißt $\mathcal{A}_\zeta$ zerfällt bei allen Stellen, die (3) teilen und die Diskriminante $d(\mathcal{A}_\zeta)$ von $\mathcal{A}_\zeta$ ist ein Hauptideal mit Erzeuger d. Dann liefert das Theorem ein Element $a \in R$, sodass gilt

$$\mathcal{A}_\zeta \cong A_\zeta(a, d \mid K), \quad a \equiv 1 \mod 9 \quad \text{und} \quad \left(\frac{a, d}{(a)}\right)_n = 1.$$

Zusätzlich sei nun vorausgesetzt, dass d eine Wurzel δ in R besitzt. Nach obigen Überlegungen gilt

$$(1-\zeta)^2 \cdot R = 3 \cdot R \quad \text{und} \quad [\mathcal{O}_m : \mathcal{O}_\zeta] \cdot R = a^3\delta^3(1-\zeta)^9 \cdot R$$

für eine maximale Ordnung $\mathcal{O}_m$ in $A_\zeta(a, d \,|\, K)$ mit Basis, die $\mathcal{O}_\zeta$ enthält. Außerdem existiert ein Element $x \in R$ mit

$$\delta \equiv x^3 \mod (a).$$

Da in diesem Fall δ die Determinante $[\mathcal{O}_m : \mathcal{O}_\zeta]$ teilt, können auch die Basiselemente einer maximalen R-Ordnung $\mathcal{O}_m$ nicht mehr unabhängig von δ sein. In Ahnlehnung an den Fall $n = 2$ setze

$$e_1 = \frac{u-1}{1-\zeta} \quad \text{und} \quad e_2 = \frac{u^2v^2 - x\delta u^2}{\delta a}.$$

Es gilt

$$e_1^3 = -\frac{3}{1-\zeta}e_1^2 - \frac{3}{(1-\zeta)^2}e_1 + \frac{a-1}{(1-\zeta)^3}$$

und

$$e_2^3 = \frac{\delta - x^3}{a},$$

also sind e_1 und e_2 ganz. Da außerdem gilt $e_2e_1 = \zeta e_1e_2 - e_2 - x$, ist der endlich erzeugte R-Modul $\mathcal{O} := \langle 1, e_1, e_1^2, e_2, e_1 \cdot e_2, e_1^2 \cdot e_2, e_2^2, e_1 \cdot e_2^2, e_1^2 \cdot e_2^2 \rangle$ abgeschlossen unter Multiplikation und damit ein Ring. Man berechnet

$$u = (1-\zeta)e_1 + 1 \quad \text{und} \quad v^2 = (1-\zeta)\delta e_1e_2 + \delta e_2 + x\delta,$$

daher enthält $\mathcal{O}$ eine Basis von $\mathcal{O}_\zeta$ und es gilt $K \cdot \mathcal{O} = A_\zeta(a, d \,|\, K)$. Eine weitere Rechnung zeigt, dass die Determinante der Übergangsmatrix das gewünschte Ergebnis liefert:

$$[\mathcal{O} : \mathcal{O}_\zeta] \cdot R = a^3\delta^3(1-\zeta)^9 \cdot R.$$

Damit ist $\mathcal{O}$ eine maximale Ordnung in $A_\zeta(a, d \,|\, K)$. Zusammenfassend lässt sich folgender Satz formulieren:

Satz 6.5. *Sei K ein algebraischer Zahlkörper, der eine primitive dritte Einheitswurzel ζ enthält, bezeichne mit R den Ring der ganzen Zahlen in K und sei $\mathcal{A}_\zeta$ eine 9-dimensionale Normrestalgebra über K, die bei allen Primstellen zerfällt, die (3) teilen. Sei weiters die Diskriminante $d(\mathcal{A}_\zeta)$ ein Hauptideal mit Erzeuger d, sodass d eine Wurzel δ in R besitze, und sei a ein Primelement in R wie in Theorem 6.2, sodass gilt*

$$\mathcal{A}_\zeta \cong A_\zeta(a, d \,|\, K), \quad a \equiv 1 \mod (9) \quad \textit{und} \quad \delta \equiv x^3 \mod (a)$$

für ein $x \in R$. Setze

$$e_1 = \frac{u-1}{1-\zeta} \quad \textit{und} \quad e_2 = \frac{u^2v^2 - x\delta u^2}{\delta a}.$$

Dann ist $\mathcal{O} := \langle 1, e_1, e_1^2, e_2, e_1 \cdot e_2, e_1^2 \cdot e_2, e_2^2, e_1 \cdot e_2^2, e_1^2 \cdot e_2^2 \rangle$ eine maximale R-Ordnung mit Basis in $A_\zeta(a, d \,|\, K)$.

Beispiel. Der Ring der ganzen Zahlen $\mathbb{Z}[\zeta], \zeta = \frac{-1+\sqrt{-3}}{2}$ im dritten Kreisteilungskörper $\mathbb{Q}(\sqrt{-3})$ ist ein Hauptidealring, daher kann man mit Hilfe obiger Überlegungen in allen Normrestalgebren über $\mathbb{Q}(\sqrt{-3}) = K$, die bei $(1-\zeta)$ zerfallen, maximale Ordnungen angeben.
Sei zum Beispiel $\mathcal{A}_\zeta = A_\zeta(7, 17 \,|\, \mathbb{Q}(\sqrt{-3}))$. Es gilt $17 \equiv 5^3 \bmod 9 \cdot (1-\zeta)$, also ist 17 nach Korollar 1.8 eine dritte Potenz in der Vervollständigung $K_{(1-\zeta)}$ und $\mathcal{A}_\zeta$ zerfällt bei $(1-\zeta)$. Ansonsten kann $\mathcal{A}_\zeta$ nur bei Primidealen verzweigen, die 7 oder 17 teilen, also bei $(17), (2-\sqrt{-3})$ und $(2+\sqrt{-3})$. Um das nachzuprüfen, muss man wie in Abschnitt 2.3 bestimmen ob $(-1)^{\nu(7)\nu(17)} \frac{17^{\nu(7)}}{7^{\nu(17)}}$ eine dritte Wurzel in $K_\mathfrak{p}$ besitzt, $\mathfrak{p} \in \{(17), (2+\sqrt{-3}), (2-\sqrt{-3})\}$, ν die normierte Bewertung auf $K_\mathfrak{p}$.

Ist $\mathfrak{p} = (17)$, so ist

$$(-1)^{0\cdot 1} \frac{17^0}{7^1} = \frac{1}{7} \equiv \frac{35}{7} \equiv 5 \equiv 11^3 \mod (17),$$

und nach Hensels Lemma selbst eine dritte Potenz in $K_{(17)}$, also zerfällt $\mathcal{A}_\zeta$ bei (17).

Ist $\mathfrak{p}$ gleich $(2+\sqrt{-3})$ oder $(2-\sqrt{-3})$, so ist

$$(-1)^{1\cdot 0} \frac{17^1}{7^0} = 17 \equiv 3 \mod \mathfrak{p}.$$

Es ist $\mathbb{Z}[\zeta]/(2 \pm \sqrt{-3}) \cong \mathbb{Z}/7\,\mathbb{Z}$ und da 3 in $\mathbb{Z}/7\mathbb{Z}$ keine dritte Wurzel besitzt, verzweigt $\mathcal{A}_\zeta$ bei $(2+\sqrt{-3})$ und $(2-\sqrt{-3})$.
Damit sind d und δ bestimmt:

$$d = (2-\sqrt{-3})^2 \, (2+\sqrt{-3})^2 = 7^2 \text{ und } \delta = 7$$

Für a muss gelten:

$a \equiv 1 \mod 9 \cdot (1-\zeta)$ und

$a \equiv (-1)^{1\cdot 0} \frac{17^1}{7^0} \equiv 3 \mod \mathfrak{p}$, für $\mathfrak{p} \in \{(2+\sqrt{-3}), (2-\sqrt{-3})\}$.

Eine Möglichkeit für die Wahl ist $a = -53$ und $\mathcal{A}_\zeta$ ist isomorph zu $A_\zeta(-53, 49 \,|\, \mathbb{Q}(\sqrt{-3}))$.
Es gilt

$$\delta = 7 \equiv (-10)^3 \mod (53)$$

und damit ist alles zusammengetragen, um die Basis einer maximalen Ordnung aufschreiben zu können. Setze

$$e_1 = (3+\sqrt{-3})\frac{u-1}{6} \quad \text{und} \quad e_2 = -\frac{u^2v^2 + 70u^2}{371},$$

und der Ring, der von e_1 und e_2 erzeugt wird, ist eine maximale $\mathbb{Z}[\zeta]$-Ordnung in $A_\zeta(-53, 49 \,|\, \mathbb{Q}(\sqrt{-3}))$.

6.2.2 Der Fall $n = 5$

Auf 3^2-dimensionalen Normrestalgebren ist es bereits gelungen, Basiselemente einer maximalen Ordnung anzugeben. Als nächstes möchte man ebensolche Elemente auf 5^2-dimensionalen Normrestalgebren finden. Sobald man diese hat, wird eine Lösung für den allgemeinen Fall leicht abzulesen sein.

Sei also K ein algebraischer Zahlkörper mit einer primitiven fünften Einheitswurzel ζ, und R der Ring der ganzen Zahlen in K. Sei weiters $\mathcal{A}_\zeta$ eine 25-dimensionale Normrestalgebra, die alle Voraussetzungen aus Theorem 6.2 erfüllt, die also bei allen Stellen zerfällt, die (5) teilen, und deren Diskriminante $d(A_\zeta)$ ein Hauptideal mit Erzeuger d ist. Außerdem sei vorausgesetzt, dass d ein vierte Wurzel $\delta \in R$ besitzt. Dann existiert ein Primelement a in R, sodass gilt

$$\mathcal{A}_\zeta \cong A_\zeta(a, d \,|\, K), \qquad a \equiv 1 \mod 25 \qquad \text{und} \qquad \delta \equiv x^5 \mod a$$

für ein $x \in R$. Korollar 6.4 besagt, dass für eine maximalen R-Ordnung $\mathcal{O}_m$ in $A_\zeta(a, d \,|\, K)$, die eine Basis besitzt und $\mathcal{O}_\zeta$ enthält, die Determinante der Übergangsmatrix $[\mathcal{O}_m : \mathcal{O}_\zeta]$ von $\mathcal{O}_m$ zu $\mathcal{O}_\zeta$ Folgendes erfüllen muss:

$$[\mathcal{O}_m : \mathcal{O}_\zeta] \cdot R = a^{10}\ \delta^{30}\ (1-\zeta)^{50} \cdot R.$$

Deswegen und wegen der bereits behandelten Fälle $n = 2$ und $n = 3$ liegt die Vermutung nahe, dass die Basiselemente einer maximalen Ordnung für $n = 5$ von höheren Potenzen von δ abhängen. Setze

$$e_1 = \frac{u-1}{1-\zeta} \quad \text{und} \quad e_2 = \frac{u^4v^4 - x\delta^3u^4}{\delta^3 a}.$$

Es gilt

$$e_1^5 = -\frac{5}{1-\zeta}e_1^4 - \frac{10}{(1-\zeta)^2}e_1^3 - \frac{10}{(1-\zeta)^3}e_1^2 - \frac{5}{(1-\zeta)^4}e_1 + \frac{a-1}{(1-\zeta)^5},$$

$$e_2^5 = \frac{\delta - x^5}{a}$$

und

$$e_2e_1 = \zeta e_1e_2 - e_2 - x.$$

Die Elemente e_1 und e_2 sind daher ganz und der endlich erzeugte R-Modul $\mathcal{O} := \langle e_1^i e_2^j, 0 \le i, j \le n-1 \rangle$ ist abgeschlossen unter Multiplikation und somit ein Ring. Man berechnet

$$u = (1-\zeta)e_1 + 1 \quad \text{und} \quad v^4 = (1-\zeta)\delta^3 e_1e_2 + \delta^3 e_2 + x\delta^3,$$

daher enthält $\mathcal{O}$ eine Basis von $\mathcal{O}_\zeta$. Darum gilt $K \cdot \mathcal{O} = A_\zeta(a, d \,|\, K)$ und $\mathcal{O}$ ist eine R-Ordnung. Mit ein wenig Rechenaufwand erhält man

$$[\mathcal{O} : \mathcal{O}_\zeta] = a^{10}\ \delta^{30}\ (1-\zeta)^{50}$$

und es ist auch im Fall $n = 5$ gelungen, eine maximale R-Ordnung in $A_\zeta(a, d \,|\, K)$ zu finden.

6.2.3 Der allgemeine Fall

Ist n eine Primzahl, so kann man mit dem bisher gesammelten Wissen auch im Allgemeinen eine Vermutung aufstellen, wie die Erzeuger einer maximalen Ordnung aussehen könnten. Der Aufwand, das zu beweisen, ist allerdings höher als in den bereits behandelten Spezialfällen, da sich hier die Ganzheitsrelationen und die Determinante der Übergangsmatrix nicht so einfach berechnen lassen.
Seien $n > 2$ eine Primzahl und K ein algebraischer Zahlkörper, der eine primitive n-te Einheitswurzel ζ enthält und bezeichne mit R den Ring der ganzen Zahlen in K. Sei weiters $\mathcal{A}_\zeta$

eine n^2-dimensionale Normrestalgebra, die alle Voraussetzungen aus Theorem 6.2 erfüllt, die also bei allen Primstellen zerfällt, die n teilen und deren Diskriminante $d(A_\zeta)$ ein Hauptideal mit Erzeuger d ist. Sei zusätzlich vorausgesetzt, dass d eine $(n-1)$-te Wurzel δ besitzt. Dann existiert ein Primelement a in R, sodass gilt

$$\mathcal{A}_\zeta \cong A_\zeta(a, d \,|\, K) \qquad \text{und} \qquad a \equiv 1 \mod n^2\mathfrak{p} \quad \text{für alle } \mathfrak{p} \mid (n).$$

Nach den Überlegungen am Anfang des Kapitels gibt es ein $x \in R$ mit $\delta \equiv x^n \mod a$. Setze

$$e_1 = \frac{u-1}{1-\zeta} \quad \text{und} \quad e_2 = \frac{u^{n-1}v^{n-1} - x\delta^{n-2}u^{n-1}}{\delta^{n-2}a}.$$

Dann stimmen e_1 und e_2 mit den Basiselementen der bereits behandelten Fälle $n = 3$ und $n = 5$ überein. Dort wurde bereits gezeigt, dass sie eine maximale R-Ordnung erzeugen. Um das auch im allgemeinen Fall nachzuweisen, möchte man zeigen, dass e_1 und e_2 ganz sind, dass der endlich erzeugte R-Modul $\mathcal{O} := \langle e_1^i e_2^j \rangle$ eine Ordnung ist und dass die Determinante der Übergangsmatrix zu $\mathcal{O}_\zeta$ das gewünschte Ergebnis aus Korollar 6.4 liefert. Im allgemeinen Fall kann man diese Dinge aber nicht mehr einfach anschreiben, dafür ist etwas mehr Technik nötig, vor allem bei der Bestimmung der Diskriminante.

Als erstes ist zu zeigen, dass $\mathcal{O}$ eine Ordnung ist. Eine einfache Rechnung zeigt

$$e_2 e_1 = \zeta e_1 e_2 - e_2 - x.$$

Hat man also nachgewiesen, dass e_1 und e_2 ganz sind, so ist $\mathcal{O}$ abgeschlossen unter Multiplikation und daher ein Ring.
Die Ganzheitsrelation von e_1 beruht hauptsächlich auf dem Binomischen Lehrsatz:

Lemma 6.6. *Ist n eine Primzahl und $e_1 = \frac{u-1}{1-\zeta}$, dann ist e_1 ganz und es gilt*

$$e_1^n = -\sum_{i=1}^{n-1} \binom{n}{i} \frac{e_1^i}{(1-\zeta)^{n-i}} + \frac{a-1}{(1-\zeta)^n}.$$

Beweis. Es gilt

$$u^n = (u-1+1)^n = \sum_{i=0}^{n} \binom{n}{i} (u-1)^i = (u-1)^n + 1 + \sum_{i=1}^{n-1} \binom{n}{i} (u-1)^i$$

und daher

$$(u-1)^n = u^n - 1 - \sum_{i=1}^{n-1} \binom{n}{i} (u-1)^i.$$

Dividiert man den Ausdruck durch $(1-\zeta)^n$, so erhält man die Gleichung

$$\left(\frac{u-1}{1-\zeta}\right)^n = \frac{a-1}{(1-\zeta)^n} - \sum_{i=1}^{n-1} \frac{\binom{n}{i}}{(1-\zeta)^{n-i}} \left(\frac{u-1}{1-\zeta}\right)^i.$$

Ist n eine Primzahl, so gilt bekanntlich $(1-\zeta)^{n-1} \mid n$ in R und da $n^2 \mid a-1$ und $n \mid \binom{n}{j}$ für $1 \le j \le n-1$, liegen alle Koeffizienten in R und e_1 ist ganz. □

In allen bereits behandelten Fällen war zu beobachten, dass e_2^n bereits im Körper liegt und um das auch allgemein nachzuprüfen, benutze die Zentralität von $A_\zeta(a,d\,|\,K)$.

Lemma 6.7. *Das Element* $e_2 = \frac{u^{n-1}v^{n-1}-x\delta^{n-2}u^{n-1}}{\delta^{n-2}a}$*, mit* x,δ *und* a *wie oben definiert, ist ganz und es gilt*

$$e_2^n = \frac{\delta - x^n}{a}.$$

Beweis. Zu zeigen ist, dass e_2^n im Körper K liegt. Da Normrestalgebren nach Lemma 2.1 zentral sind, genügt es also, nachzuprüfen, ob e_2^n mit den Elementen u und v kommutiert. Betrachte

$$e_2 \cdot v = \frac{u^{n-1}v^{n-1} - x\delta^{n-2}u^{n-1}}{\delta^{n-2}a} \cdot v = \zeta^{-1}v \cdot \frac{u^{n-1}v^{n-1} - x\delta^{n-2}u^{n-1}}{\delta^{n-2}a}$$

und daher

$$e_2^n \cdot v = \zeta^{-n}v \cdot e_2^n = v \cdot e_2^n.$$

Um zu zeigen, dass e_2 mit u kommutiert, überlege man sich Folgendes:

$$e_2 \cdot u = \frac{u^{n-1}v^{n-1} - x\delta^{n-2}u^{n-1}}{\delta^{n-2}a} \cdot u =$$

$$\zeta u \cdot \frac{u^{n-1}v^{n-1} - x\delta^{n-2}u^{n-1}}{\delta^{n-2}a} + x(\zeta - 1) = \zeta u \cdot e_2 + x(\zeta - 1).$$

Im Weiteren gilt dann

$$e_2^n \cdot u = e_2^{n-1} \cdot (\zeta u \cdot e_2 + x(\zeta - 1)) = \zeta e_2^{n-1} \cdot u \cdot e_2 + x(\zeta - 1)e_2^{n-1} =$$

$$\zeta e_2^{n-2} \cdot (\zeta u \cdot e_2 + x(\zeta - 1)) \cdot e_2 + x(\zeta - 1)e_2^{n-1} = \zeta^2 e_2^{n-2} \cdot u \cdot e_2^2 + x(\zeta - 1)(1 + \zeta)e_2^{n-1} =$$
$$\zeta^3 e_2^{n-3} \cdot u \cdot e_2^3 + x(\zeta - 1)(1 + \zeta + \zeta^2)e_2^{n-1}.$$

Durch Iteration erhält man

$$e_2^n \cdot u = \zeta^n u \cdot e_2^n + x(\zeta - 1)(1 + \zeta + \zeta^2 + ... + \zeta^{n-1}) = u \cdot e_2^n.$$

Also kommutiert e_2^n mit u und v und liegt somit im Körper K. Daraus ergibt sich

$$e_2^n = \frac{(u^{n-1}v^{n-1})^n + (-x\delta^{n-2}u^{n-1})^n}{(a\delta^{n-2})^n} =$$

$$\frac{\zeta^{-n(n-1)/2}\delta^{(n-1)^2}a^{n-1} + (-1)^n x^n \delta^{n(n-2)}a^{n-1}}{a^n\delta^{n(n-2)}} = (-1)^{n-1}\,\frac{\delta - x^n}{a}.$$

Da n eine Primzahl > 2 ist, ist die Behauptung gezeigt. □

Damit sind beide Elemente e_1 und e_2 ganz und der Modul, den sie erzeugen, ist wie weiter oben schon ausgeführt einen Ring, genannt $\mathcal{O}$. Wie bereits zuvor berechnet man

$$u = (1 - \zeta)e_1 + 1 \quad \text{und} \quad v^{n-1} = (1 - \zeta)\delta^{n-2}e_1e_2 + \delta^{n-2}e_2 + x\delta^{n-2}$$

und $\mathcal{O}$ enthält eine Basis von $\mathcal{O}_\zeta$. Darum gilt $K \cdot \mathcal{O} = A_\zeta(a,d\,|\,K)$ und $\mathcal{O}$ ist eine R-Ordnung in $A_\zeta(a,d\,|\,K)$.

Um zu überprüfen, ob die Ordnung $\mathcal{O}$ maximal ist, muss man wieder die Determinante $[\mathcal{O} : \mathcal{O}_\zeta]$ der Übergangsmatrix von $\mathcal{O}$ zu $\mathcal{O}_\zeta$ berechnen. Im Gegensatz zu den bereits behandelten Fällen fixer Dimension kann diese Matrix im allgemeinen Fall nicht einfach aufgeschrieben werden und um Informationen über $[\mathcal{O} : \mathcal{O}_\zeta]$ zu bekommen, muss man ihre Eigenschaften genauer untersuchen. Man beachte, dass $[\mathcal{O} : \mathcal{O}_\zeta]$ gleich $[\mathcal{O}_\zeta : \mathcal{O}]^{-1}$. Der Trick ist, die Basen so anzuordnen, dass die Übergangsmatrix von $\mathcal{O}_\zeta$ zu $\mathcal{O}$ obere Dreiecksform hat. Sind die Einträge der Hauptdiagonale bestimmt, lässt sich die Determinante berechnen. Man beachte im folgenden Lemma, dass sich jede ganze Zahl $k, 0 \leq k \leq n^2 - 1$ eindeutig darstellen lässt als $k = j \cdot n + i,\ 0 \leq i, j \leq n - 1$.

Lemma 6.8. *Die Basen $\{e_1^i e_2^j, 0 \leq i, j \leq n-1\}$ von $\mathcal{O}$ und $\{u^i v^j, 0 \leq i, j \leq n-1\}$ von $\mathcal{O}_\zeta$ lassen sich so anordnen, dass die Übergangsmatrix zwischen den Basen eine obere Dreiecksmatrix ist, nämlich folgendermaßen:*
Ist $k \in \mathbb{N}_0, 0 \leq k \leq n^2 - 1, k = j \cdot n + i,\ 0 \leq i, j \leq n - 1$, dann stehe an der $(k+1)$-ten Stelle der Basis von $\mathcal{O}$ das Element $e_1^i e_2^j$ und an der $k+1$-ten Stelle der Basis von $\mathcal{O}_\zeta$ das Element $\begin{cases} u^{n-j+i} v^{n-j}, & \text{falls } 0 \leq i < j, \\ u^{i-j} v^{n-j}, & \text{falls } 0 < j \leq i, \\ u^i, & \text{falls } j = 0. \end{cases}$
Das heißt die geordneten Basen sehen folgendermaßen aus:

$$\mathcal{O} = \langle 1,\ e_1,\ e_1^2, ...,\ e_1^{n-1},\ e_2,\ e_1 e_2,\ e_1^2 e_2, ...,\ e_1^{n-1} e_2,$$
$$e_2^2,\ e_1 e_2^2, ...,\ e_1^{n-1} e_2^2,\ e_2^3,\ e_1 e_2^3, ...,\ e_1^{n-1} e_2^{n-1} \rangle$$

und

$$\mathcal{O}_\zeta = \langle 1, u, u^2, ..., u^{n-1}, u^{n-1} v^{n-1}, v^{n-1}, u v^{n-1}, u^2 v^{n-1}, ..., u^{n-2} v^{n-1}, u^{n-2} v^{n-2},$$
$$u^{n-1} v^{n-2}, v^{n-2}, u v^{n-2}, ..., u^{n-3} v^{n-2}, u^{n-3} v^{n-3}, u^{n-2} v^{n-3}, u^{n-1} v^{n-3}, ..., v \rangle$$

und über K stimmen für alle $k, 1 \leq k \leq n^2$, die Erzeugnisse der ersten k Elemente beider Basen überein.

Beweis. Offensichtlich stimmen über K die Erzeugnisse der ersten $j+1$ Elemente beider Basen überein, $0 \leq j \leq n-1$:

$$\langle 1, e_1,\ e_1^2, ...,\ e_1^j \rangle_K = \langle 1, u, u^2, ..., u^j \rangle_K$$

und ebenso die der ersten $n+1$ Elemente

$$\langle 1, e_1,\ e_1^2, ...,\ e_1^{n-1},\ e_2 \rangle_K = \langle 1, u, u^2, ..., u^{n-1}, u^{n-1} v^{n-1} \rangle_K.$$

Angenommen, die Erzeugnisse der ersten $j \cdot n,\ 2 \leq j \leq n-1$ Elemente beider Basen stimmen überein, also

$$\langle 1,\ e_1, ...,\ e_1^{n-1},\ e_2,\ e_1 e_2,\ e_1^2 e_2, ...,\ e_1^{n-1} e_2,\ e_2^2,\ e_1 e_2^2, ...,\ e_1^{n-1} e_2^{j-1} \rangle_K$$

sei gleich

$$\langle 1, u, u^2, ..., u^{n-1}, u^{n-1} v^{n-1}, v^{n-1}, u v^{n-1}, ..., u^{n-2} v^{n-1}, u^{n-2} v^{n-2},$$
$$u^{n-1} v^{n-2}, ..., u^{n-j+1} v^{n-j+1}, u^{n-j+2} v^{n-j+1} ..., u^{n-j} v^{n-j+1} \rangle_K =: V_{j-1}.$$

Es gilt $u^i x \in V_{j-1}\ \forall x \in V_{j-1}, i \in \mathbb{N}$ und

$$e_2^j = \frac{\zeta^* d^{j-1} u^{n-j} v^{n-j} + u^{n-j} v^{n-j+1} \left(\sum_{i=0}^{j-2} x_i v^i \right)}{a\delta^{j(n-2)}} + x = \frac{\zeta^* d^{j-1} u^{n-j} v^{n-j}}{a\delta^{j(n-2)}} + y$$

wobei x_i und x im Erzeugnis $\langle 1, u, u^2, ..., u^{n-1} \rangle$ und y in V_{j-1} liegen und ζ^* eine (nicht notwendig primitive) n-te Einheitswurzel ist. Daher erzeugen auch die ersten $j \cdot n+1$ Elemente der Basen über K denselben Vektorraum:

$$\langle 1,\ e_1, ...,\ e_1^{n-1},\ e_2,\ e_1 e_2,\ e_1^2 e_2, ...,\ e_1^{n-1} e_2^{j-1},\ e_2^j \rangle_K =$$

$$\langle 1, u, ..., u^{n-1}, u^{n-1} v^{n-1}, v^{n-1}, u v^{n-1}, ..., u^{n-j} v^{n-j+1}, u^{n-j} v^{n-j} \rangle_K.$$

Angenommen, die Erzeugnisse der ersten $j \cdot n + i,\ 1 \leq i, j \leq n-1$ Elemente beider Basen über Kstimmen überein, also

$$\langle 1,\ e_1,\ e_1^2, ...,\ e_1^{n-1},\ e_2,\ e_1 e_2,\ e_1^2 e_2, ...,\ e_1^{n-1} e_2,$$

$$e_2^2,\ e_1 e_2^2, ...,\ e_1^{n-1} e_2^2,\ e_2^3,\ e_1 e_2^3, ...,\ e_2^{j-1},\ e_1 e_2^j, ...,\ e_1^{i-1} e_2^j \rangle_K$$

sei gleich

$$\langle 1, u, u^2, ..., u^{n-1}, u^{n-1} v^{n-1}, v^{n-1}, u v^{n-1}, ..., u^{n-2} v^{n-1},$$
$$u^{n-2} v^{n-2}, u^{n-1} v^{n-2}, ..., u^{n-j} v^{n-j}, u^{n-j+1} v^{n-j}, ..., u^{n-j+i-1} v^{n-j} \rangle_K =$$
$$V_{j-1} \oplus \langle u^{n-j} v^{n-j}, u^{n-j+1} v^{n-j}, ..., u^{n-j+i-1} v^{n-j} \rangle_K =: V_{i-1,j-1}.$$

Betrachte $e_1^i e_2^j$:

$$e_1^i e_2^j = \frac{u^i + \sum_{k=0}^{i-1} \binom{i}{k} (-1)^{i-k} u^k}{(1-\zeta)^i} \cdot \frac{\zeta^* d^{j-1} u^{n-j} v^{n-j} + x}{a\delta^{j(n-2)}} =$$

$$\frac{\zeta^* d^{j-1} u^{n-j+i} v^{n-j} + \sum_{k=0}^{i-1} \binom{i}{k} (-1)^{i-k} \zeta^* d^{j-1} u^{n-j+k} v^{n-j}}{a\delta^{j(n-2)}(1-\zeta)^i} + x' =$$

$$\frac{\zeta^* d^{j-1} u^{n-j+i} v^{n-j}}{a\delta^{j(n-2)}(1-\zeta)^i} + y$$

wobei $x, x' \in V_{j-1}$ und $y \in V_{i-1,j-1}$.
Daher erzeugen auch die ersten $j \cdot n + i + 1$ Elemente beider Basen über K denselben Vektorraum:

$$\langle 1,\ e_1,\ e_1^2, ...,\ e_1^{n-1},\ e_2,\ e_1 e_2,\ e_1^2 e_2, ...,\ e_2^{j-1},\ e_1 e_2^j, ...,\ e_1^{i-1} e_2^j,\ e_1^i e_2^j \rangle_K =$$

$$\langle 1, u, u^2, ..., u^{n-1}, u^{n-1} v^{n-1}, v^{n-1}, u v^{n-1}, ..., u^{n-j} v^{n-j},$$
$$u^{n-j+1} v^{n-j}, ..., u^{n-j+i-1} v^{n-j}, u^{n-j+i} v^{n-j} \rangle_K.$$

Insgesamt betrachtet hat also die Übergangsmatrix der geordneten Basis von $\mathcal{O}_\zeta$ zu der geordneten Basis von $\mathcal{O}$ obere Dreiecksform. □

Beispiel. Zur Veranschaulichung sei hier die Übergangsmatrix von $\mathcal{O}_\zeta$ zu $\mathcal{O}$ für $n = 3$ mit geordneten Basen dargestellt:

$$\begin{array}{c} \\ 1 \\ u \\ u^2 \\ u^2v^2 \\ v^2 \\ uv^2 \\ uv \\ u^2v \\ v \end{array}
\begin{array}{c}
\begin{array}{ccccccccc} 1 & e_1 & e_1^2 & e_2 & e_1e_2 & e_1^2e_2 & e_2^2 & e_1e_2^2 & e_1^2e_2^2 \end{array} \\
\begin{pmatrix}
1 & \frac{-1}{1-\zeta} & \frac{1}{(1-\zeta)^2} & 0 & \frac{-x}{1-\zeta} & \frac{2x}{(1-\zeta)^2} & 0 & 0 & \frac{x^2}{(1-\zeta)^2} \\
0 & \frac{1}{1-\zeta} & \frac{-2}{(1-\zeta)^2} & 0 & 0 & \frac{-x}{(1-\zeta)^2} & \frac{x^2}{a} & \frac{-x^2}{a(1-\zeta)} & \frac{x^2}{a(1-\zeta)^2} \\
0 & 0 & \frac{1}{(1-\zeta)^2} & \frac{-x}{a} & \frac{x}{a(1-\zeta)} & \frac{-x}{a(1-\zeta)^2} & 0 & \frac{x^2}{a(1-\zeta)} & \frac{-2x^2}{a(1-\zeta)^2} \\
0 & 0 & 0 & \frac{1}{a\delta} & \frac{-1}{a\delta(1-\zeta)} & \frac{1}{a\delta(1-\zeta)^2} & 0 & \frac{\zeta x}{a\delta(1-\zeta)} & \frac{-2\zeta x}{a\delta(1-\zeta)^2} \\
0 & 0 & 0 & 0 & \frac{1}{\delta(1-\zeta)} & \frac{-2}{\delta(1-\zeta)^2} & 0 & 0 & \frac{\zeta x}{\delta(1-\zeta)^2} \\
0 & 0 & 0 & 0 & 0 & \frac{1}{\delta(1-\zeta)^2} & \frac{\zeta x}{a\delta} & \frac{-\zeta x}{a\delta(1-\zeta)} & \frac{\zeta x}{a\delta(1-\zeta)^2} \\
0 & 0 & 0 & 0 & 0 & 0 & \frac{\zeta^2 d}{a\delta^2} & \frac{-\zeta^2 d}{a\delta^2(1-\zeta)} & \frac{\zeta^2 d}{a\delta^2(1-\zeta)^2} \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & \frac{\zeta^2 d}{a\delta^2(1-\zeta)} & \frac{-2\zeta^2 d}{a\delta^2(1-\zeta)^2} \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \frac{\zeta^2 d}{\delta^2(1-\zeta)^2}
\end{pmatrix}
\end{array}$$

Die Determinante lässt sich einfach ablesen:

$$[\mathcal{O} : \mathcal{O}_\zeta]^{-1} = [\mathcal{O}_\zeta : \mathcal{O}] = \frac{d^3}{a^3\delta^9(1-\zeta)^9} = \frac{\delta^6}{a^3\delta^9(1-\zeta)^9} = \frac{1}{a^3\delta^3(1-\zeta)^9}.$$

Das Lemma ermöglicht es nun, die Determinante $[\mathcal{O}_\zeta : \mathcal{O}] = [\mathcal{O} : \mathcal{O}_\zeta]^{-1}$ der Übergangsmatrix der Basen von $\mathcal{O}_\zeta$ zu $\mathcal{O}$ auch im allgemeinen Fall zu bestimmen. Es wurde gezeigt, dass die Determinante das Produkt bestimmter Koeffizienten in $e_1^i e_2^j$ ist, nämlich der Koeffizienten

$$\text{von } \begin{cases} u^{n-j+i}v^{n-j}, & \text{falls } 0 \le i < j, \\ u^{i-j}v^{n-j}, & \text{falls } 0 < j \le i, \\ u^i, & \text{falls } j = 0. \end{cases}$$

Außerdem wurde für $0 \le i \le n-1, 0 < j \le n-1$ gezeigt:

$$e_1^i e_2^j = \frac{\zeta^* d^{j-1} u^{n-j+i} v^{n-j}}{a\delta^{j(n-2)}(1-\zeta)^i} + y$$

$y \in V_{i-1,j-1}$ und

$$e_1^i = \frac{u^i + \sum_{k=0}^{i-1} \binom{i}{k}(-1)^{i-k}u^k}{(1-\zeta)^i}.$$

Die gesuchten Koeffizienten c_{ij} in $e_1^i e_2^j, 0 \le i, j \le n-1$ muss man nur noch ablesen.

$$c_{ij} := \begin{cases} \frac{\zeta^* d^{j-1}}{a\delta^{j(n-2)}(1-\zeta)^i}, & \text{falls } 0 \le i < j, \\ \frac{\zeta^* a d^{j-1}}{a\delta^{j(n-2)}(1-\zeta)^i}, & \text{falls } 0 < j \le i, \\ \frac{1}{(1-\zeta)^i}, & \text{falls } j = 0 \end{cases}$$

mit ζ^* jeweils eine geeignete n-te Einheitswurzel.
Mit Hilfe von Abzählungsargumenten bestimmt man, wie oft a, d, δ und $1-\zeta$ im Produkt der c_{ij} vorkommen:

a : a kommt im Nenner von allen $c_{ij}, j \ge 1$ vor, also genau $n^2 - n$ mal und steht genau dann im Zähler, wenn $1 \le j \le i$. Im Produkt über alle c_{ij} steht dann folgende Potenz

von a:

$$\frac{a^{1+2+\ldots+n-1}}{a^{n(n-1)}} = \frac{a^{n(n-1)/2}}{a^{n(n-1)}}.$$

d: $d^{j-1}, 1 \leq j \leq n-1$ kommt im Zähler von allen $c_{ij}, 0 \leq i \leq n-1$ vor, also n mal und im Produkt über die c_{ij} steht

$$d^{n+2n+\ldots+(n-2)n} = d^{n(n-1)(n-2)/2}.$$

δ: $\delta^{(n-2)j}, 0 \leq j \leq n-1$ kommt im Nenner von allen $c_{ij}, 0 \leq i \leq n-1$ vor, also n mal und im Produkt steht

$$\left(\delta^{n(n-2)} \cdot \delta^{2n(n-2)} \cdot \ldots \cdot \delta^{(n-1)n(n-2)}\right)^{-1} = \left(\delta^{n^2(n-1)(n-2)/2}\right)^{-1}.$$

$1-\zeta$: $(1-\zeta)^i, 0 \leq i \leq n-1$ kommt im Nenner von allen $c_{ij}, 0 \leq j \leq n-1$ vor, also steht in der Determinante

$$\left((1-\zeta)^{n+2n+\ldots+(n-1)n}\right)^{-1} = \left((1-\zeta)^{n^2(n-1)/2}\right)^{-1}.$$

Insgesamt ist die Determinante $[\mathcal{O}_\zeta : \mathcal{O}]$ gleich

$$[\mathcal{O}_\zeta : \mathcal{O}] = \frac{\zeta^* a^{n(n-1)/2}\ d^{n(n-1)(n-2)/2}}{a^{n(n-1)}\ \delta^{n^2(n-1)(n-2)/2}\ (1-\zeta)^{n^2(n-1)/2}} =$$

$$\frac{\zeta^* a^{n(n-1)/2}\ \delta^{n(n-1)^2(n-2)/2}}{a^{n(n-1)}\ \delta^{n^2(n-1)(n-2)/2}\ (1-\zeta)^{n^2(n-1)/2}} = \frac{\zeta^*}{a^{n(n-1)/2}\ \delta^{n(n-1)(n-2)/2}\ (1-\zeta)^{n^2(n-1)/2}},$$

wobei ζ^* wieder eine geeignete n-te Einheitswurzel bezeichne. Damit gilt

$$[\mathcal{O} : \mathcal{O}_\zeta] \cdot R = a^{n(n-1)/2}\ \delta^{n(n-1)(n-2)/2}\ (1-\zeta)^{n^2(n-1)/2} \cdot R$$

und $\mathcal{O}$ ist nach Korollar 6.4 maximal.
Dieses Ergebnis sei in folgendem Theorem noch einmal zusammengefasst:

Theorem 6.9. *Seien $n > 2$ eine Primzahl und K ein algebraischer Zahlkörper, der eine primitive n-te Einheitswurzel ζ enthält und bezeichne mit R den Ring der ganzen Zahlen in K. Sei weiters $\mathcal{A}_\zeta$ eine n^2-dimensionale Normrestalgebra über K, die bei allen Primstellen zerfällt, die (n) teilen und deren Diskriminante $d(\mathcal{A}_\zeta)$ ein Hauptideal mit Erzeuger d ist, sodass d eine $(n-1)$-te Wurzel δ in R besitzt. Dann existiert ein Primelement $a \in R$, sodass gilt*

$$\mathcal{A}_\zeta \cong A_\zeta(a, d \,|\, K), \qquad a \equiv 1 \mod (n)^2 \qquad \textit{und} \qquad \delta \equiv x^n \mod (a)$$

für ein $x \in R$ und die Elemente

$$e_1 = \frac{u-1}{1-\zeta} \quad \textit{und} \quad e_2 = \frac{u^{n-1}v^{n-1} - x\delta^{n-2}u^{n-1}}{\delta^{n-2}a}$$

sind ganz und erfüllen $e_2e_1 = \zeta e_1e_2 - e_2 - x$. Außerdem sind die Elemente

$$1,\ e_1,\ e_1^2, \ldots,\ e_1^{n-1},\ e_2,\ e_1e_2,\ e_1^2e_2, \ldots,\ e_1^{n-1}e_2^{n-1}$$

K-linear unabhängig. Der freie R-Modul $\mathcal{O}$, der von dieser Basis erzeugt wird, enthält eine K-Basis von $A_\zeta(a, d \,|\, K)$ und ist damit eine R-Ordnung. Es gilt

$$[\mathcal{O} : \mathcal{O}_\zeta] \cdot R = a^{n(n-1)/2}\ \delta^{n(n-1)(n-2)/2}\ (1-\zeta)^{n^2(n-1)/2} \cdot R$$

und damit ist die R-Ordnung $\mathcal{O}$ maximal in $A_\zeta(a, d \,|\, K)$.

Bemerkung. Die Diskriminante d ist für n Primzahl das Produkt $n-1$-ter Potenzen von Primidealen. Ist R ein Hauptidealring, so hat d also immer eine $n-1$-te Wurzel und in jeder Normrestalgebra, deren Grad eine Primzahl ist und die bei allen Primstellen zerfällt, die den Grad teilen, kann man mit der hier entwickelten Methode eine maximale R-Ordnung bestimmen.

Zusammenfassung

Diese Arbeit beschäftigt sich mit maximalen Ordnungen in Normrestalgebren über algebraischen Zahlkörpern, im Speziellen mit der Verallgemeinerung einer Methode zur Konstruktion von maximalen Ordungen in Quaternionenalgebren aus [Lem].

Im ersten Kapitel sind alle grundlegenden Definitionen und Resultate über lokale Körper und zyklische Algebren gesammelt, die später benutzt werden, wie etwa Hensels Lemma, der Approximationssatz und der Normensatz.

Das zweite Kapitel behandelt die Konstruktion der Normrestalgebren $A_\zeta(a, b \,|\, K)$ und ihre allgemeinen Eigenschaften über beliebigen Körpern K, $a, b \in K^*$. Es werden deren Zentralität und Einfachheit gezeigt (Lemma 2.1) und der Zusammenhang mit Matrizenalgebren in Abhängigkeit von den Elementen a und b (Satz 2.6) sowie im zweiten Abschnitt die Ähnlichkeit bzw. Isomorphie zu einer zyklischen Algebra (Satz 2.8 und Satz 2.9). Im dritten Abschnitt werden die Isomorphieklassen von Normrestalgebren über lokalen Körpern bestimmt (Satz 2.13).

Das dritte Kapitel beinhaltet alle Definitionen und Resultate über Ordnungen, die im weiteren Verlauf gebraucht werden. Außerdem wird die Diskriminante der Ordnung in einer Normrestalgebra bestimmt, die von den Standardbasiselementen der Algebra erzeugt wird (Abschnitt 3.3).

Im vierten Kapitel wird das Hilbertsymbol eingeführt, wie es in der Klassenkörpertheorie definiert ist. Dieses hängt eng zusammen mit dem Verzweigungsverhalten von Normrestalgebren. Es wird gezeigt, dass das n-te Hilbertsymbol $\left(\frac{a,b}{\mathfrak{p}}\right)_n$ die Isomorphieklasse der n^2-dimensionalen Normrestalgebra $A_\zeta(a, b \,|\, K_\mathfrak{p})$ über der Vervollständigung eines algebraischen Zahlkörpers K bezüglich einer Stelle $\mathfrak{p}$ parametrisiert (Satz 4.4).

Das fünfte Kapitel beschäftigt sich mit Quaternionenalgebren über einem algebraischen Zahlkörper K und der Ausarbeitung der Methode aus [Lem]. Dabei wird zu einer gegebenen Quaternionenalgebra eine isomorphe Algebra $Q(a, d \,|\, K)$ konstruiert (Theorem 5.12), in der maximale Ordnungen besonders günstige Eigenschaften besitzen. Daraufhin werden explizit Basiselement angegeben, die in dieser Algebra eine maximale Ordnung erzeugen (Abschnitt 5.4).

Das letzte Kapitel verallgemeinert die Ergebnisse aus Kapitel fünf auf Normrestalgebren, deren Grad eine Primzahl ist. Im ersten Abschnitt wird Theorem 5.12 unter ähnlichen Voraussetzungen mit Hilfe des Hilbertsymbols verallgemeinert. Dabei wird wieder zu einer gegebenen Normrestalgebra eine isomorphe Algebra konstruiert, deren maximale Ordnungen sich günstig verhalten (Theorem 6.2). Der zweite Abschnitt beschreibt zwei Elemente e_1 und e_2 in der eben konstruierten Algebra und weist nach, dass diese ganz sind und dass der Ring, den sie erzeugen, eine maximale Ordnung in dieser Algebra ist (Theorem 6.9). Damit ist es gelungen Lemurells Methode zu verallgemeinern.

Summary (English)

This thesis deals with maximal orders in power norm residue algebras defined over an algebraic number field, in particular with the generalization of a technique of constructing maximal orders in quaternion algebras from [Lem].

In chapter one there are listed all the basic definitions and results about local fields and cyclic algebras, which will be used afterwards. For example we mention Hensel's Lemma and the approximation theorem.

The second chapter introduces the construction and basis properties of power norm residue algebras $A_\zeta(a, b \,|\, K)$ defined over arbitrary fields $K, a, b \in K^*$. We will prove that these algebras are central and simple (Lemma 2.1) and examine how they are related to matrix algebras according to the elements a and b (Satz 2.6). Moreover, we will show that they are similar or isomorphic to cyclic algebras (Satz 2.8, Satz 2.9). At the end of this chapter the isomorphism classes of power norm residue algebras over local fields are determined (Satz 2.13).

Chapter three contains definitions and basic results regarding orders. Given a power norm residue algebra, we consider the order, which is generated by the standard basis of the algebra, and determine the discriminant of this order (Section 3.3).

Chapter four introduces the Hilbertsymbol, which originates from class field theory. It is closely linked to the ramification of power norm residue algebras. We will show that the n-th Hilbertsymbol $\left(\frac{a,b}{\mathfrak{p}}\right)_n$ parametrizes the isomorphism class of the n^2-dimensional power norm residue algebra $A_\zeta(a, b \,|\, K_\mathfrak{p})$ over a completion of an algebraic number field K with respect to a place $\mathfrak{p}$ (Satz 4.4).

The fifth chapter deals with quaternion algebras over algebraic number fields and the elaboration of Lemurell's method of finding a maximal order [Lem]. Based on a given quaternion algebra we construct an isomorphic algebra, in which maximal orders have certain useful properties (Theorem 5.12). Thereupon we can find explicit elements, which generate a maximal order in this algebra (Section 5.4).

The last chapter generalizes the results from the previous chapter to power norm residue algebras whose degree is a prime number. In the first section we will prove a generalized version of Theorem 5.12 by use of the Hilbertsymbol. Once again based on a given power norm residue algebra we can construct an isomorphic algebra, in which maximal orders have convenient properties (Theorem 6.2). In the second section we manage to find two elements e_1 and e_2 in this algebra, which are similar to the generators of the maximal order in the last chapter. We will show that they are integral and that the ring generated by those elements is a maximal order and hence achieve our aim to generalize Lemurell's construction (Theorem 6.9).

Literaturverzeichnis

[Fes93] I. B. Fesenko, S. V. Vostokov, *Local fields and their extensions: A constructive approach,* American Mathematical Society, Providence, RI, 1993.

[Ker07] I. Kersten, *Brauergruppen,* Universitätsverlag Göttingen, 2007.

[Lem] S. Lemurell, *A Description of Quaternion Algebras,* www.math.chalmers.se/%7Esj/forskning/structure.ps, 23.10.2012, unpubliziert.

[Mac03] C. Maclachlan, A. W. Reid, *The Arithmetic of Hyperbolic 3-Manifolds,* Springer-Verlag, New York, 2003.

[Nar74] W. Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers,* Springer-Verlag, Berlin-Heidelberg-New York, 1st edition, 1974.

[Neu99] J. Neukirch, *Algebraic Number Theory,* Springer-Verlag, Berlin, 1999.

[O'M63] O. O'Meara, *Introduction to Quadratic Forms,* Springer-Verlag, Berlin-Heidelberg-New York, 1963.

[Rei75] I. Reiner, *Maximal Orders,* Academic Press, London, 1975.

Curriculum Vitae

Persönliche Daten

Name:	Victoria Elisabeth Döller
Geburtsdatum:	21. Mai 1988
Geburtsort:	Wien
Staatsbürgerschaft:	Österreich
E-Mail Adresse:	a0605208@unet.univie.ac.at

Schulbildung

1994 – 1995	Volksschule Notre Dame de Sion, Burggasse Wien
1995 – 1998	Volksschule, Falkenstein
1998 – 2006	Gymnasium, Laa an der Thaya Matura mit ausgezeichnetem Erfolg
30.01.-03.02.2006	Intensivkurs Angewandte Mathematik: Kryptographie für hochbegabte Schülerinnen und Schüler
seit 2006	Diplomstudium der Mathematik an der Universität Wien
seit 2007	Lehramtstudium der Mathematik, Psychologie und Philosophie an der Universität Wien

Stipendien

Leistungsstipendium für das Studienjahr 2009 - 2010 vergeben von der Universität Wien.