**RWTH Aachen**
**Fakultät für Mathematik, Informatik und Naturwissenschaften**

# Euklidischer Algorithmus und Faktorisieren in Quaternionenalgebren und Oktaven

Bachelorarbeit

in Mathematik

vorgelegt von
Christian Staerk
am 9. September 2011

**Gutachter**

Prof. Dr. G. Nebe
Prof. Dr. E. Zerz

# Inhaltsverzeichnis

# Einleitung

Die vorliegende Bachelorarbeit handelt von Quaternionenalgebren und Oktaven und jeweils zugehörigen Maximalordnungen von „ganzen Zahlen“. Ziel der Arbeit ist es, in diesen Maximalordnungen zu Resultaten über die Existenz euklidischer Algorithmen und die Eindeutigkeit von Primfaktorzerlegungen zu gelangen. Die gefundenen Algorithmen werden dann in dem Computeralgebrasystem Magma implementiert.

Die Bachelorarbeit ist folgendermaßen aufgebaut:
Im ersten Kapitel werden die Quaternionen und Oktaven als weiterführende, höherdimensionale Zahlenbereiche eingeführt. Es wird sich zeigen, dass die Oktaven gewissermaßen das Ende des Zahlenbegriffs markieren. Dazu wird ein allgemeines Konzept vorgestellt, welches ausgehend von einer gegebenen Algebra $A$ über dem Körper $K$ durch „Verdoppelung“ immer größere Algebren über $K$ liefert. In diesem Zusammenhang werden allgemeine Quaternionenalgebren und Oktavenalgebren eingeführt, die die zuvor definierten Begriffe erweitern. Es wird untersucht, welche Eigenschaften ein sogenanntes Dickson-Double $A \times A$ in Abhängigkeit von der Ausgangsalgebra $A$ besitzt. So kann ein verallgemeinerter Satz von Hurwitz bewiesen werden, der normierte Algebren über einem beliebigen Körper $K$ klassifiziert.
Als einen Spezialfall dieses Satzes erhält man für $K = \mathbb{R}$ den ursprünglichen Satz von Hurwitz, der besagt, dass es über den reellen Zahlen nur vier normierte Algebren gibt, nämlich die eindimensionalen reellen Zahlen $\mathbb{R}$, die zweidimensionalen komplexen Zahlen $\mathbb{C}$, die vierdimensionalen Quaternionen $\mathbb{H}$ und die achtdimensionalen Oktaven $\mathbb{O}$. Dabei wird sich herausstellen, dass, von $\mathbb{R}$ ausgehend, bei jeder Zahlenbereichserweiterung eine wichtige Eigenschaft verloren geht: Von $\mathbb{R}$ nach $\mathbb{C}$ verlieren wir die Anordnung, von $\mathbb{C}$ nach $\mathbb{H}$ die Kommutativität der Multiplikation und von $\mathbb{H}$ nach $\mathbb{O}$ sogar die Assoziativität der Multiplikation. Die fehlende Assoziativiät von $\mathbb{O}$ wird dann das entscheinende Argument dafür sein, dass die (16-dimensionale) Erweiterung von $\mathbb{O}$ nicht mehr den gewünschten Eigenschaften eines Zahlenbereichs genügt.
Im zweiten Kapitel der Bachelorarbeit werden die notwendigen Begriffe definiert, um Zahlentheorie auch in den Quaternionen und Oktaven zu betreiben. Es stellt sich dabei insbesondere die Frage, wie die Eigenschaft „ganzzahlig“ in den Zahlenbereichen der Quaternionen und Oktaven definiert werden kann. Dazu wird der Begriff der Maximalordnung auf nichtassoziative Algebren erweitert.
Dies wird im dritten Kapitel der Arbeit schließlich zu einer Maximalordnung der Hurwitz Quaternionen $H$ und zu einer Maximalordnung $C$ in den Oktaven führen. Im Zentrum dieses Kapitels wird der Euklidische Algorithmus stehen, welcher in den Hurwitz Quaternionen ganz gewöhnlich funktioniert, sobald man eine Division mit Rest hat. Die Eindeutigkeit der Primfaktorzerlegung bis auf die Multiplikation mit einer Einheit gilt in den Hurwitz Quaternionen jedoch nicht, da aufgrund der fehlenden Kommutativität verschiedene Einheiten zwischen die einzelnen Primfaktoren eingeschoben werden können.

Bei den ganzzahligen Oktaven $C$ wird einem trotz Division mit Rest die fehlende Assoziativität zum Verhängnis, sodass sogar der bekannte Euklidische Algorithmus nicht immer korrekt terminiert. Es gibt jedoch einen modifizierten euklidischen Algorithmus für $C$, der von Hans Peter Rehm im Jahr 1993 veröffentlicht wurde. Mithilfe dieses Algorithmus kann eine eindeutige Primfakorzerlegung in $C$ bewiesen werden, wenn genügend starke Einschränkungen an die zulässigen Primfaktoren gestellt werden.
Schließlich werden einige Quaternionenalgebren über quadratischen Zahlkörpern auf die Eigenschaft euklidisch untersucht, wobei dort mit der gleichen Methode gearbeitet werden kann, die schon bei der Maximalordnung $C$ in den Oktaven verwendet wurde: Man zeigt, dass die jeweilige Maximalordnung zu dem Gitter $\mathbb{E}_8$ isomorph ist. Eine bekannte Eigenschaft dieses Gitters führt dann zu euklidischen Algorithmen.

In dem Computeralgebrasystem Magma habe ich sowohl die in einem bestimmten Sinn eindeutige Primfaktorzerlegung in den ganzzahligen Oktaven $C$ als auch die euklidischen Algorithmen in den betrachten Quaternionenalgebren über quadratischen Zahlkörpern implementiert. In beiden Programmen muss zu einem beliebigen Punkt im $\mathbb{Q}^8$ ein Gitterpunkt von $\mathbb{E}_8$ gefunden werden, der kürzesten Abstand hat. Ein Algorithmus, der dies für ein beliebiges Gitter leistet, ist in Magma schon implementiert („ClosestVectors“). Für das Gitter $\mathbb{E}_8$ gibt es jedoch einen sehr einfachen elementaren Algorithmus, der wesentlich schneller ist als „ClosestVectors“. Diesen habe ich ebenfalls programmiert. Die Quelltexte aller Programme finden sich im Anhang der Bachelorarbeit.

# 1 Der Satz von Hurwitz

## 1.1 Quaternionen und Oktaven

Zunächst wollen wir die Zahlenbereiche der Quaternionen und der Oktaven einführen. Es gibt prinzipiell zwei Wege, die Quaternionen zu definieren: Man kann sie einerseits aus den reellen Zahlen konstruieren, indem man Quaternionen mit den Vektoren des $\mathbb{R}^4$ identifiziert und dort eine Multiplikation definiert. Andererseits kann man die Quaternionen nicht nur als Quartetts von reellen Zahlen ($\mathbb{H} = \mathbb{R}^4$), sondern auch als Paare von komplexen Zahlen ($\mathbb{H} = \mathbb{C}^2$) auffassen. Hierbei geht man ganz analog zur Konstruktion der komplexen Zahlen aus den reellen Zahlen vor.

**(1.1) Definition**
Die Menge der *Quaternionen* ist der folgende komplexe Matrizenring

$$\mathbb{H} := \{ \begin{pmatrix} a & b \\ -\overline{b} & \overline{a} \end{pmatrix};\ a, b \in \mathbb{C} \} \cong \{(a, b);\ a, b \in \mathbb{C}\} = \mathbb{C} \times \mathbb{C}.$$

**(1.2) Bemerkung**
$\mathbb{H}$ ist eine reelle Unteralgebra von $\mathbb{C}^{2\times 2}$ mit folgender (von der Matrixmultiplikation induzierten) Multiplikation auf $\mathbb{H} \cong \mathbb{C} \times \mathbb{C}$:

$$(a, b)(c, d) = (ac - b\overline{d}, ad + b\overline{c}). \tag{1}$$

Im Folgenden identifiziere $\mathbb{H}$ mit $\mathbb{C} \times \mathbb{C}$ und dieser Multiplikation. Wir werden später in einem allgemeineren Rahmen sehen, dass die Multiplikation auf $\mathbb{H}$ aufgrund der Matrixmultiplikation natürlich assoziativ, jedoch nicht mehr kommutativ ist.

Nun wollen wir die Möglichkeit kennen lernen, die Quaternionen als Quartetts von reellen Zahlen aufzufassen. Dies war schließlich die Art und Weise, wie William Rowan Hamilton sie im Jahre 1843 entdeckte (daher auch der Name $\mathbb{H}$).

**(1.3) Definition**
$\mathbb{H} := \{x = x_0 + x_1 i + x_2 j + x_3 k;\ x_0, x_1, x_2, x_3 \in \mathbb{R}\}$ heißt die Menge der *Quaternionen*. Dabei sei $(1, i, j, k)$ eine Orthonormalbasis bezüglich des Standardskalarproduktes des $\mathbb{R}^4$. Auf $\mathbb{H}$ definiere die Addition komponentenweise und die Multiplikation nach den berühmten *Hamilton-Regeln* auf den Basiselementen:

$$i^2 = j^2 = k^2 = -1$$

$$ij = -ji = k; \quad ki = -ik = j; \quad jk = -kj = i, \tag{2}$$

sowie $1 \cdot r = r \cdot 1$ für $r \in \{1, i, j, k\}$.

**(1.4) Bemerkung**
Die so definierten Quaternionen stimmen mit denen aus Definition (1.1) überein, denn identifiziere die Basiselemente durch

$$1 = (1,0) \quad i = (i,0) \quad j = (0,1) \quad k = (0,i).$$

Einsetzen aller Kombinationen dieser in die Multiplikationsvorschrift (1) liefert die Hamilton-Regeln. Zum Beispiel ist

$$ki = (0,i)(i,0) = (0+0, 0+i\bar{i}) = (0,1) = j.$$

Die Multiplikation auf den Basiselementen legt die Multiplikation auf ganz $\mathbb{H}$ fest, da wir für eine Algebra natürlich die Distributivgesetze und die Kommutativität der Addition fordern, das heißt für $x, y \in \mathbb{H}$ ist:

$$xy = (x_0 + x_1 i + x_2 j + x_3 k)(y_0 + y_1 i + y_2 j + y_3 k) = x_0y_0 - x_1y_1 - x_2y_2 - x_3y_3 +$$

$$(x_0y_1 + x_1y_0 + x_2y_3 - x_3y_2)i + (x_0y_2 + x_2y_0 + x_3y_1 - x_1y_3)j + (x_0y_3 + x_3y_0 + x_1y_2 - x_2y_1)k$$

Nachdem wir nun die Quaternionen auf zwei verschiedene Wege eingeführt haben, wollen wir dies mit den sogenannten Oktaven (oder Oktonionen) $\mathbb{O}$ ebenfalls tun. Hier ist jedoch eine Konstruktion als Matrizenring nicht mehr möglich (siehe [Esch]). Dennoch kann man die Oktaven wieder als Paare von Quaternionen ($\mathbb{O} = \mathbb{H} \times \mathbb{H}$) oder als Oktetts von reellen Zahlen ($\mathbb{O} = \mathbb{R}^8$) auffassen.

**(1.5) Definition**
$\mathbb{O} := \{(a,b);\ a,b \in \mathbb{H}\}$ heißt die Menge der *Oktaven*. Auf dieser Menge definiere die Addition werteweise und die Multiplikation für $(a,b),(c,d) \in \mathbb{O}$ wie folgt

$$(a,b)(c,d) := (ac - \bar{d}b, da + b\bar{c}). \tag{3}$$

Da die Quaternionen natürlicherweise in die Oktaven eingebettet sind, ist die Multiplikation auf $\mathbb{O}$ ebenfalls nicht kommutativ; wir werden später zeigen, dass sie sogar nicht mehr assoziativ ist.

Den ersten Abschnitt beenden wir, indem wir die Oktaven auch als Oktetts von reellen Zahlen auffassen.

**(1.6) Definition**
$\mathbb{O} := \{x = \sum_{i=0}^{7} x_i;\ x_0,..,x_7 \in \mathbb{R}\}$ heißt die Menge der *Oktaven*. Dabei sei $(1, e_1, .., e_7)$ eine Orthonormalbasis bezüglich des Standardskalarproduktes des $\mathbb{R}^8$. Auf $\mathbb{O}$ definiere die Addition komponentenweise und die Multiplikation nach folgenden Regeln auf den Basiselementen:

$$e_n^2 = -1 \tag{4}$$

$$e_n e_{n+1} = e_{n+3} = -e_{n+1} e_n \tag{5}$$

$$e_{n+1} e_{n+3} = e_n = -e_{n+3} e_{n+1} \tag{6}$$

$$e_{n+3} e_n = e_{n+1} = -e_n e_{n+3} \tag{7}$$

wobei die Indizes modulo 7 mit dem Vertretersystem $\{1, 2, .., 7\}$ gelesen werden müssen. Wie üblich sei $1 \cdot r = r \cdot 1$ für $r \in \{1, e_1, e_2, e_3, e_4, e_5, e_6, e_7\}$.

Ähnlich wie oben kann man die hier definierten Oktaven mit denen aus Definition (1.7) identifizieren. Wir begnügen uns hier, um die Notation der Definition zu verdeutlichen, mit einem kleinen

**(1.7) Beispiel**
Es ist $e_2 e_3 = e_5$ nach (5), $e_7 e_5 = -e_4$ nach (6) und $e_5 e_1 = -e_6$ nach (7).

Zusammenfassend haben wir also folgende Kette von Zahlenbereichserweiterungen:

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C} \subset \mathbb{H} \subset \mathbb{O}.$$

Es fällt auf, dass ab den reellen Zahlen $\mathbb{R}$ die Konstruktion eines höherdimensionalen Zahlenbereichs immer in einer Verdopplung besteht. Dieses Phänomen werden wir nun in einem allgemeineren Kontext untersuchen. So werden wir insbesondere sehen, dass es im Rahmen der Zahlentheorie nicht besonders sinnvoll ist, die obige Inklusionskette weiter fortzusetzen.

## 1.2 Normierte Algebren

Unser Ziel ist es, einen verallgemeinerten Satz von Hurwitz zu beweisen, der eine Klassifikation aller normierten Algebren über einem beliebigen Körper K liefert. Der hier ausgeführte Beweis orientiert sich an [Jac] und [Con]. Um die Begriffe zu klären, zunächst eine

**(1.8) Definition**
Sei $K$ ein Körper.

a) $A$ heißt *Algebra* über $K$, falls A ein $K$-Vektorraum ist, auf dem eine $K$-bilinearen Multiplikation $A \times A \to A$ erklärt ist.

b) Eine Algebra $A$ heißt *Divisionsalgebra*, wenn jede Gleichung vom Typ $ux = v$ oder $xu = v$ mit $u, v \in A, u \neq 0$ eine eindeutig bestimmte Lösung $x \in A$ besitzt.

c) Sei $A$ ein $K$-Vektorraum. Dann heißt $N : A \to K$ *quadratische Form* auf $A$, falls

$$N(\lambda x) = \lambda^2 N(x) \quad \forall x \in A, \lambda \in K$$

und die Abbildung $b : A \times A \to K$ definiert durch

$$b(x, y) = N(x + y) - N(x) - N(y)$$

bilinear ist.
Ist $char(K) \neq 2$, so ist $(-|-) : A \times A \to K$ mit

$$(x|y) = \frac{1}{2}(N(x+y) - N(x) - N(y))$$

eine symmetrische Bilinearform und heißt das *Skalarprodukt* bezüglich $N$.

d) Eine Algebra $A$ über $K$ mit $char(K) \neq 2$ heißt *normierte Algebra*, wenn sie ein multiplikativ neutrales Element besitzt und mit einer quadratischen Form $N : A \to K$ ausgestattet ist, die multiplikativ, anisoptrop und deren Skalarprodukt nicht ausgeartet ist, das heißt es gilt

$$N(xy) = N(x)N(y) \quad \forall x, y \in A,$$
$$N(x) = 0 \Leftrightarrow x = 0 \quad \forall x \in A$$

und für alle $x \in A$ gilt

$$(x|y) = 0 \ \ \forall y \in A \Rightarrow x = 0.$$

e) $A$ heißt *Schiefkörper*, falls $A$ eine assoziative Divisionsalgebra ist.

**(1.9) Bemerkung**
Sei $A$ eine normierte Algebra. Gilt für $x, y \in A$, dass $(x|t) = (y|t)$ für alle $t \in A$, so folgt aus der Bilinearität des Skalarprodukts $(x - y|t) = 0$. Da das Skalarprodukt nicht ausgeartet ist, gilt $x - y = 0$, also $x = y$.
Diese Eigenschaft werden wir im Folgenden immer wieder benutzen.

Nun wollen wir den Beweis des verallgemeinerten Satzes von Hurwitz vorbereiten. Dies ist eine Erweiterung des Satzes von Hurwitz aus dem Jahre 1898, welcher besagt, dass es nur vier normierte Algebren über $\mathbb{R}$ gibt; diese sind $\mathbb{R}$, $\mathbb{C}$, $\mathbb{H}$ und $\mathbb{O}$. Es gibt einen stärkeren Satz, der auf die Zusatzannahme der Normiertheit verzichtet und aussagt, dass diese vier Algebren sogar die einzigen endlich dimensionalen Divisionsalgebren über $\mathbb{R}$ sind. Er wurde 1958 von M. Kervaire mit topologischen Methoden gezeigt und ist schwieriger zu beweisen.

Sei im Folgenden jedoch vorerst ganz allgemein $A$ eine normierte Algebra über dem Körper $K$ mit quadratischer Form $N$ und Skalarprodukt $(-|-)$ (insbesondere gilt $char(K) \neq 2$).
Zunächst beweisen wir einige Hilfsaussagen.

**(1.10) Lemma**
Es gilt für alle $x, y, z, u \in A$:

$$(xy|xz) = N(x)\,(y|z) \text{ und } (xz|yz) = (x|y)\,N(z) \tag{8}$$

$$(xy|uz) = 2\,(x|u)\,(y|z) - (xz|uy) \tag{9}$$

**Beweis**
(8): $2\,(xy|\,xz) = N(xy+xz) - N(xy) - N(xz) = N(x(y+z)) - N(xy) - N(xz)$

$= N(x)N(y+z) - N(x)N(y) - N(x)N(z) = N(x)[N(y+z) - N(y) - N(z)] = 2N(x)\,(y|\,z)$

Mit Division durch 2 folgt die erste Behauptung von (8). Die zweite folgt analog.

(9): Mit (8) und mit der Bilinearität und Symmetrie von $(-|-)$ folgt

$$\begin{aligned}
& & N(x+u)\,(y|\,z) &= ((x+u)y|\,(x+u)z) \\
\Rightarrow & & [N(x)+N(u)+2\,(x|\,u)]\,(y|\,z) &= (xy+uy|\,xz+uz) \\
\Rightarrow & (xy|\,xz)+(uy|\,uz)+2\,(x|\,u)\,(y|\,z) &= (xy|\,xz)+(xy|\,uz)+(uy|\,xz)+(uy|\,uz) \\
\Rightarrow & & 2\,(x|\,u)\,(y|\,z) &= (xy|\,uz)+(uy|\,xz) \\
\Rightarrow & & 2\,(x|\,u)\,(y|\,z)-(xz|\,uy) &= (xy|\,uz)
\end{aligned}$$ □

Für $x \in A$ führen wir die formale Konjugation $\bar{x} := 2\,(x|\,1) - x$ ein. Sie hat folgende Eigenschaften:

**(1.11) Lemma**
Es gilt für alle $x, y, z \in A$:

$$(xy|\,z) = (y|\,\bar{x}z) \quad \textit{und} \quad (xy|\,z) = (x|\,z\bar{y}) \tag{10}$$

$$\bar{\bar{x}} = x \tag{11}$$

$$\overline{xy} = \bar{y}\bar{x} \tag{12}$$

$$\overline{x+y} = \bar{x} + \bar{y} \tag{13}$$

$$\bar{x}x = N(x) = x\bar{x} = N(\bar{x}) \tag{14}$$

$$\bar{x}(xy) = (\bar{x}x)y \quad \textit{und} \quad y(x\bar{x}) = (yx)\bar{x} \tag{15}$$

**Beweis**
(10): Mit der Definition und $u = 1$ in (9) folgt

$$(y|\,\bar{x}z) = (y|\,2\,(x|\,1)\,z - xz) = (y|\,2\,(x|\,1)\,z) - (y|\,xz) = 2\,(x|\,1)\,(y|\,z) - (xz|\,y) \overset{(9)}{=} (xy|\,z)\,.$$

Die zweite Behauptung folgt analog.
(11): Setze $y = 1$ und $z = t$ in (10), dann

$$(x|\,t) = (x1|\,t) = (1|\,\bar{x}t) = (\bar{\bar{x}}1|\,t) = (\bar{\bar{x}}|\,t) \;\; \forall t \in A.$$

(12): Verwende wiederholt (10) und erhalte

$$(\bar{y}\bar{x}|\,t) = \left(\bar{x}\middle|\,yt\right) = (\bar{x}\bar{t}|\,y) = (\bar{t}|\,xy) = \left(\bar{t}\middle|\,(xy)1\right) = \left(\overline{(xy)}\bar{t}\middle|\,1\right) = (\overline{xy}|\,t) \quad \forall t \in A.$$

(13): Dies folgt sofort aus der Definition, denn

$$\overline{x+y} = 2\,(x+y|\,1) - (x+y) = 2\,(x|\,1) - x + 2\,(y|\,1) - y = \bar{x} + \bar{y}.$$

(14): Aus

$$(\,N(x)|\,t) = N(x)\,(1|\,t) = (\,x|\,xt) = (\,\bar{x}x|\,t) \quad \forall t \in A$$

folgt die erste Gleichung und analog (beachte $N(x) \in K$) die zweite Gleichung. Für $x$ sezte nun $\bar{x}$ in die erste Gleichung ein und erhalte $N(\bar{x}) = \bar{\bar{x}}\bar{x} = x\bar{x}$.
(15): Es ist für alle $t \in A$

$$\begin{aligned}
(\,\bar{x}(xy)|\,t) = (\,(2\,(x|\,1) - x)(xy)|\,t) &= 2\,(x|\,1)\,(xy|\,t) - (\,x(xy)|\,t) \\
&\overset{(9)}{=} (\,x(xy)|\,1 \cdot t) + (\,xt|\,xy) - (\,x(xy)|\,t) \\
&= (\,xt|\,xy) \\
&= N(x)\,(t|\,y) \\
&= (\,N(x)y|\,t) \\
&= (\,(\bar{x}x)y|\,t)\,.
\end{aligned}$$

Die zweite Behauptung folgt analog. □

Ist eine Algebra nicht assoziativ, so kann man analog zum Konzept des Kommutators mithilfe des Assoziators „messen“, wie weit diese Algebra von der Assoziativität entfernt ist. Erfüllt sie eine schwächere Form der Assoziativität, so heißt sie alternativ:

**(1.12) Definition**
Sei $A$ eine Algebra über $K$.

a) Für $x, y, z \in A$ heißt $[x, y, z] := (xy)z - x(yz)$ der *Assoziator* von $x, y, z$ in $A$.

b) $A$ heißt *alternativ*, falls $[x, x, y] = [y, x, x] = 0$ für alle $x, y \in A$.

**(1.13) Bemerkung**
Aufgrund der $K$-Linearität der Multiplikation in $A$ ist der Assoziator offensichtlich in jeder Komponente $K$-linear.

**(1.14) Satz**
Jede normierte Algebra ist alternativ.

**Beweis**
Sei $A$ eine normierte Algebra über $K$. Für $x, y \in A$ ist $\bar{x}(xy) = (\bar{x}x)y$ und $y(x\bar{x}) = (yx)\bar{x}$ (Gleichung (15)), also $[\bar{x}, x, y] = [y, x, \bar{x}] = 0$. Aus der Linearität des Assoziators folgt

$$0 = [\bar{x}, x, y] = [\underbrace{2\,(x|\,1)}_{\in K}, x, x] - [x, x, y] = 0 - [x, x, y] = -[x, x, y].$$

Analog zeigt man $[y, x, x] = 0$. Somit ist $A$ alternativ. □

Gewisse Unteralgebren einer normierten Algebra sind sogar assoziativ. Dies ist Inhalt des folgdenden zentralen Satzes von Artin, den wir hier nicht beweisen wollen, aber im Verlauf der Arbeit immer wieder benutzen werden.

**(1.15) Satz (Artin)**
Jede Unteralgebra einer normierten Algebra, die nur von höchstens zwei Elementen erzeugt wird, ist assoziativ.

**Beweis**
Siehe beispielsweise [Esch]. □

**(1.16) Satz**
Jede normierte Algebra ist eine Divisionsalgebra.

**Beweis**
Sei $A$ eine normierte Algebra über $K$ und $u \in A \setminus \{0\}$. Aus $u\bar{u} = N(u)$ folgt $u\frac{\bar{u}}{N(u)} = 1$ (beachte $N(u) \neq 0$, da $N$ anisotrop ist ), folglich existiert das multiplikative inverse Element $u^{-1} = \frac{\bar{u}}{N(u)}$.
Ist nun die Gleichung $ux = v$ mit $v \in A$ gegeben, so folgt $u^{-1}(ux) = (u^{-1}u)x$ mit dem Satz von Artin, also

$$x = u^{-1}v = \frac{\bar{u}}{N(u)}v.$$

Dieses $x \in A$ löst mit (15) tatsächlich die Gleichung, da

$$ux = u(\frac{\bar{u}}{N(u)}v) = \frac{1}{N(u)}(u\bar{u})v = \frac{1}{N(u)}N(u)v = v.$$

Die Gleichung $xu = v$ löst man durch Rechtsmultiplikation von $u^{-1}$ völlig analog, sodass $A$ eine Divisionsalgebra ist. □

Dieser Satz zeigt also, dass der Satz von Hurwitz schwächer ist als der von Kervaire. Tatsächlich ist es so, dass die Divisionsalgebra die Struktur ist, die Zahlenbereiche auszeichnet. Sie fordert gerade, dass Gleichungen durch Division in diesen Zahlenbereichen eindeutig lösbar sind. Dennoch wollen wir hier aus oben gennanten Gründen den Satz von Hurwitz betrachten.

## 1.3 Der Cayley-Dickson-Prozess

Nun beginnen wir mit dem sogenannten *Cayley-Dickson-Prozess*, bei dem wir Schritt für Schritt durch „Verdoppelung“ immer größere Algebren bekommen.

**(1.17) Definition**
Sei $H$ eine normierte Algebra über dem Körper $K$ und $\alpha \in K^*$, sodass $\alpha \notin N(H) = \{N(h);\ h \in H\}$. Die Algebra $DD(H, \alpha) := H \times H$ mit der Multiplikation

$$(a, b)(c, d) := (ac + \alpha d\bar{b}, cb + \bar{a}d)$$

für $(a,b),(c,d) \in DD(H,\alpha)$ heißt das *Dickson Double* von $H$ bezüglich $\alpha$. Wir identifizieren $H \oplus iH$ mit $H \times H$ durch $a+ib := (a,b)$. Dann übersetzt sich die Multiplikation zu

$$(a+ib)(c+id) = (ac+\alpha d\bar{b}) + i(cb+\bar{a}d). \tag{16}$$

Auf $DD(H,\alpha)$ definiere ein Skalarprodukt für $(a,b),(c,d) \in DD(H,\alpha)$ folgendermaßen:

$$(a+ib|\, c+id) := (a|\, c) - \alpha\,(b|\, d)\,.$$

Dieses Skalarprodukt setzt das Skalarprodukt auf $H$ fort.

**(1.18) Lemma**
Das in Definition (1.17) definierte Dickson Double $DD(H,\alpha)$ ist ausgestattet mit der anisotropen quadratischen Form

$$N(a+ib) := N(a) - \alpha N(b) = (a+ib|\, a+ib)\,, \tag{17}$$

für $a+ib \in DD(H,\alpha)$.

**Beweis**
Für $a+ib \in DD(H,\alpha)$ gilt

$$N(a+ib) = N(a) - \alpha N(b) = (a|\, a) - \alpha\,(b|\, b) = (a+ib|\, a+ib)\,.$$

Für $a,b \neq 0$ gilt $N(a) - \alpha N(b) = 0$ genau dann, wenn $\alpha = \frac{N(a)}{N(b)} = N(\frac{a}{b}) \in N(H)$. Dies haben wir aber in der Definition ausgeschlossen, also ist $N$ anisotrop. □

Wir werden sehen, dass $DD(H,\alpha)$ genau dann wieder eine normierte Algebra ist (die quadratische Form also auch multiplikativ ist), falls $H$ assoziativ ist.

**(1.19) Lemma**
Sei $H$ eine assoziative, normierte Algebra über $K$ und $\alpha,\beta \in K^*$ mit $\alpha,\beta \notin N(H)$. Dann gilt $DD(H,\alpha) \cong DD(H,\beta)$, falls $N(\frac{\alpha}{\beta}) \in N(H)$ ist.

**Beweis**
Sei $x \in H$ mit $N(x) = \frac{\alpha}{\beta}$. Definiere $\phi : DD(H,\alpha) \to DD(H,\beta)$ durch $\phi(a+ib) := a+jbx$ für $a+ib \in H$. Wegen $x \neq 0$ ist $\phi$ offensichtlich bijektiv. Im Folgenden lassen wir bei Produkten in $H$ aufgrund der Assoziativität die Klammern weg. Es gilt

$$\phi((a+ib)(c+id)) = \phi(ac+\alpha d\bar{b} + i(cb+\bar{a}d)) = ac+\alpha d\bar{b} + j(cbx+\bar{a}dx)$$

und

$$\phi(a+ib)\phi(c+id) = (a+jbx)(c+jdx) = ac + \underbrace{\beta dx(\overline{bx})}_{=\beta N(x) d\bar{b}} + j(cbx+\bar{a}dx)$$

und mit $N(x) = \frac{\alpha}{\beta}$ folgt die Gleichheit $\phi((a+ib)(c+id)) = \phi(a+ib)\phi(c+id)$ für alle $a,b,c,d \in H$. Somit ist $\phi$ ein Algebrenisomorphismus und $DD(H,\alpha) \cong DD(H,\beta)$. □

Wir schauen uns nun an, was passiert, falls wir diesen Verdoppelungsschritt auf eine Unteralgebra einer normierten Algebra anwenden.

**(1.20) Lemma**
Sei $A$ eine normierte Algebra über dem Körper $K$.
Weiter sei $H$ eine echte Unteralgebra von $A$, $i \in A$ mit $N(i) = -\alpha, \alpha \in K \setminus \{0\}$ und $i \in H^\perp := \{x \in A,\ (x|h) = 0\ \forall h \in H\}$. (Ein solches $i \in A$ existiert immer, da das Skalarprodukt nicht ausgeartet ist, sodass $A = H \oplus H^\perp$.)
Dann ist $H + iH = \{a + ib;\ a, b \in H\}$ wieder eine Unteralgebra von $A$ und es gilt für $a, b, c, d \in H$:

$$\overline{a + ib} = \bar{a} - ib \tag{18}$$

$$ib = \bar{b}i \quad \text{und} \quad i\bar{b} = bi \tag{19}$$

$$(a + ib)(c + id) = (ac + \alpha d\bar{b}) + i(cb + \bar{a}d) \tag{20}$$

Wir bemerken, dass aus der Definition der Konjugation $\bar{i} = -i$ folgt. Insbesondere ist $\alpha \notin N(H)$ und $H + iH \cong DD(H, \alpha)$ kanonisch isomorph.

**Beweis**
(18): Wegen $(ib|1) = 0$ gilt

$$\overline{a + ib} = 2\,(a + ib|1) - a - ib = 2\,(a|1) - a + 2\,(ib|1) - ib = \bar{a} - ib.$$

(19): Dies folgt aus (18): $ib = -\overline{ib} = -\bar{b}\bar{i} = \bar{b}i$. Die zweite Behauptung folgt dann mit (11).

(20): Zeige

$$((a + ib)(c + id)|t) = \big((ac + \alpha d\bar{b}) + i(cb + \bar{a}d)\big|t\big)\ \ \forall t \in A.$$

Dies ist mit der Distributivität von $A$ äquivalent zu

$$(ac + a(id) + (ib)c + (ib)(id)|t) = \big(ac + \alpha d\bar{b} + i(cb) + i(\bar{a}d)\big|t\big)\ \ \forall t \in A,$$

was mit der Bilinearität wiederum heißt, dass für alle $t \in A$

$$(ac|t) + (a(id)|t) + ((ib)c|t) + ((ib)(id)|t) = (ac|t) + (i(\bar{a}d)|t) + (i(cb)|t) + \big(\alpha d\bar{b}\big|t\big).$$

Zu zeigen sind also noch die folgende drei Gleichungen:

$$(a(id)|t) = (i(\bar{a}d)|t) \tag{21}$$

$$((ib)c|t) = (i(cb)|t) \tag{22}$$

$$((ib)(id)|t) = \big(\alpha d\bar{b}\big|t\big) \tag{23}$$

(21): $(a(id)|t) = (id|\bar{a}t) \overset{(9)}{=} 2\underbrace{(i|\bar{a})}_{=0}(d|t) - (it|\bar{a}d) = -\big(t\big|\bar{i}(\bar{a}d)\big) = (i(\bar{a}d)|t)$.

(22): $((ib)c|\,t) = (ib|\,t\bar{c}) = \left(\bar{b}i\middle|\,t\bar{c}\right) \overset{(9)}{=} 0 - \left(\bar{b}\bar{c}\middle|\,ti\right) = \left((\bar{b}\bar{c})i\middle|\,t\right) = \left(\overline{(cb)}i\middle|\,t\right) = (i(cb)|\,t)\,.$

(23): $((ib)(id)|\,t) = \left(ib\middle|\,t\overline{(id)}\right) = \left(ib\middle|\,t(\bar{d}\cdot\bar{i})\right) = -\left(ib\middle|\,t(\bar{d}i)\right) = -(ib|\,t(id))$

$$\overset{(9)}{=} 0 + (i(id)|\,tb) = -(id|\,i(tb)) = -N(i)\,(d|\,tb) = \left(\alpha d\bar{b}\middle|\,t\right).$$

Damit folgt Behauptung (20) und somit ist $H + iH$ eine Unteralgebra von $A$, denn (20) besagt gerade, dass die Multiplikation auf $H + iH$ abgeschlossen ist.
Dass $N(\alpha) \notin N(H)$ gilt, sieht man analog zum Beweis des Lemmas (1.18). □

Gleichung (20) liefert also gerade die Multiplikationsvorschrift (16). Statt wie in (20) das orthogonale Element $i$ von links an die Algebra $H$ zu multiplizieren, können wir dies auch von rechts, sodass wir die zu $H + iH$ isomorphe Algebra $H + Hi$ betrachten ($H + iH \ni a + ib \mapsto a + \bar{b}i \in H + Hi$ ist Algebrenisomorphismus). Man erhält dann die folgende Multiplikationsvorschrift.

$$(a + bi)(c + di) = (ac + \alpha\bar{d}b) + (da + b\bar{c})i \qquad (20b)$$

Denn mit (19) und (20) folgt:

$$(a + bi)(c + di) = (a + i\bar{b})(c + i\bar{d}) = (ac + \alpha\bar{d}\bar{\bar{b}}) + i(c\bar{b} + \bar{a}\bar{d})$$
$$= (ac + \alpha\bar{d}b) + \overline{(c\bar{b} + \bar{a}\bar{d})}i = (ac + \alpha\bar{d}b) + (da + b\bar{c}).$$

**(1.21) Bemerkung**
Sehen wir uns den wichtigen Spezialfall $K = \mathbb{R}$ und $N(i) = 1$ an:
Wenn wir dann die Multiplikation (20b) mit den Multiplikationen auf $\mathbb{C} = \mathbb{R} \times \mathbb{R}$, auf $\mathbb{H} = \mathbb{C} \times \mathbb{C}$ (1) und auf $\mathbb{O} = \mathbb{H} \times \mathbb{H}$ (3) vergleichen, so stimmen sie überein. Denn in $\mathbb{R}$ gilt die Kommutativität der Multiplikation und wir haben eine triviale Konjugation (das heißt die Konjugation ist die Identität auf $\mathbb{R}$), sodass (20b) mit der üblichen Multiplikation auf $\mathbb{C}$ übereinstimmt. In $\mathbb{C}$ gilt die Kommutativität der Multiplikation, sodass (20b) gerade die Multiplikation (1) auf $\mathbb{H}$ ist. Und die Multiplikation (3) auf $\mathbb{O}$ ist exakt die Multiplikation (20b).

Wir betrachten jetzt aber wieder ohne Einschränkung die Algebra $H + iH$. Das folgende zentrale Lemma gibt uns Auskunft darüber, welche Eigenschaften ein „Dickson-Double“ in Abhängigkeit von seinem Ursprung besitzt.

**(1.22) Lemma**
Sei $A$ eine normierte Algebra über $K$, $Y$ eine Unteralgebra von $A$, $i \in Y^{\perp}$ mit $N(i) = -\alpha$, $\alpha \in K \setminus \{0\}$ und $Z := Y + iY$. Dann gilt:

a) $Z$ ist eine normierte Unteralgebra von $A \Leftrightarrow Y$ ist eine assoziative, normierte Unteralgebra von $A$.

b) $Z$ ist eine assoziative normierte Unteralgebra von $A \Leftrightarrow Y$ ist eine kommutative, assoziative normierte Unteralgebra von $A$.

c) $Z$ ist eine kommutative, assoziative normierte Unteralgebra von $A \Leftrightarrow Y$ ist eine kommutative, assoziative normierte Unteralgebra von $A$ mit trivialer Konjugation.

**Beweis**

a) $Z$ ist nach (20) genau dann eine normierte Algebra, falls für alle $a, b, c, d \in A$:

$$N(a+ib)N(c+id) = N((a+ib)(c+id)) = N((ac+\alpha d\bar{b}) + i(cb+\bar{a}d))$$

Forme diese Bedingung nun äquivalent um. Wegen (17) ist dies äquivalent zu

$$(N(a)-\alpha N(b))(N(c)-\alpha N(d)) = N(ac+\alpha d\bar{b}) - \alpha N(cb+\bar{a}d),$$

was wiederum gleichwertig ist mit

$$(N(a)-\alpha N(b))(N(c)-\alpha N(d))$$

$$= N(ac) + \alpha^2 N(d\bar{b}) + 2\left(ac\middle|\, \alpha d\bar{b}\right) - \alpha N(cb) - \alpha N(\bar{a}d) - 2\alpha\,(cb|\,\bar{a}d)\,.$$

Nutzen wir die Multiplikativität der Norm (ist $Z$ eine normierte Unteralgebra, dann erst recht $Y$), so erhalten wir

$$N(a)N(c) - \alpha N(a)N(d) - \alpha N(b)N(c) + \alpha^2 N(b)N(d)$$

$$= N(a)N(c) + \alpha^2 N(d)N(\bar{b}) + 2\alpha\left(ac\middle|\, d\bar{b}\right) - \alpha N(c)N(b) - \alpha N(\bar{a})N(d) - 2\alpha\,(cb|\,\bar{a}d)\,.$$

Beachte, dass $N(\bar{b}) = N(\bar{b})N(i) = N(\bar{b}i) = N(ib) = N(i)N(b) = N(b)$ und erhalte so durch Streichen und Umsortieren einiger Terme

$$2\alpha\left(ac\middle|\, d\bar{b}\right) = 2\alpha\,(cb|\,\bar{a}d)\,.$$

Division durch $2\alpha \in K^*$ und Anwenden von (10) liefert

$$(\,(ac)b|\,d) = (\,a(cb)|\,d) \quad \forall d \in Y$$

und somit

$$(ac)b = a(cb),$$

was genau dann für alle $a, b, c \in Y$ gilt, falls Y eine assoziative normierte Algebra ist. Dies beweist Behauptung a).

b) „⇒“ Sei $Z$ eine assoziative normierte Algebra, dann muss $Y$ diese Eigenschaften natürlich auch haben. Weiter gilt

$$i(bc) = (ib)c \overset{(20)}{=} 0 + i(cb) = i(cb) \quad \forall c, b \in Y$$

Dies heißt aber, dass $bc = cb \ \ \forall c, b \in Y$ und somit $Y$ kommutativ ist.

„$\Leftarrow$“ Sei $Y$ eine kommutative, assoziative normierte Algebra. Dann ist $Z$ nach a) eine normierte Algebra und für alle $a, b, c, d, e, f \in Y$ gilt:

$$\begin{aligned}
[(a+ib)(c+id)](e+if) &= (ac+\alpha d\bar{b}+i(cb+\bar{a}d))(e+if) \\
&= (ac+\alpha d\bar{b})e+\alpha f(\bar{b}\bar{c}+\bar{d}a)+i[e(cb+\bar{a}d)+(\bar{c}\bar{a}+\alpha b\bar{d})f] \\
&= (ac)e+\alpha(d\bar{b})e+\alpha f(\bar{b}\bar{c})+\alpha f(\bar{d}a)+i[e(cb)+e(\bar{a}d)+(\bar{c}\bar{a})f+\alpha(b\bar{d})f] \\
&\overset{(*)}{=} a(ce)+a(\alpha f\bar{d})+\alpha(ed)\bar{b}+\alpha(\bar{c}f)\bar{b}+i[(ce)b+\alpha(f\bar{d})b+\bar{a}(ed)+\bar{a}(\bar{c}f)] \\
&= a(ce+\alpha f\bar{d})+\alpha(ed+\bar{c}f)\bar{b}+i[(ce+\alpha f\bar{d})b+\bar{a}(ed+\bar{c}f)] \\
&= (a+ib)[(ce+\alpha f\bar{d})+i(ed+\bar{c}f)] = (a+ib)[(c+id)(e+if)],
\end{aligned}$$

wobei $(*)$ wegen der Kommutativität und Assoziativität von Y gilt. Also ist $Z$ assoziativ.

c) „$\Rightarrow$“ Sei $Z$ eine kommutative, assoziative normierte Algebra, dann muss $Y$ diese Eigenschaften auch haben. Wegen (19) und der Kommutativität in $Y$ gilt $ie = \bar{e}i = i\bar{e} \ \ \forall e \in Y$, also $e = \bar{e} \ \ \forall e \in Y$, das heißt die Konjugation auf $Y$ ist trivial.

„$\Leftarrow$“ Sei $Y$ eine kommutative, assoziative normierte Algebra mit trivialer Konjugation, dann ist nach b) $Z$ eine assoziative normierte Algebra und $\forall a, b, c, d \in Y$:

$$(a+ib)(c+id) = (ac+\alpha d\bar{b})+i(cb+\bar{a}d) \overset{(*)}{=} (ca+\alpha b\bar{d})+i(ad+\bar{c}b) = (c+id)(a+ib)$$

wobei $(*)$ wegen der Kommutativität und der trivialen Konjugation in $Y$ gilt. Also ist Z auch kommutativ. □

## 1.4 Quaternionenalgebren und Oktavenalgebren

Lemma (1.22) liefert die Grundlage für die folgende Definition, die den *Cayley-Dickson-Prozess* zusammenfasst:

**(1.23) Definition**
Sei $K$ ein Körper mit $char(K) \neq 2$, sowie $\alpha_1, \alpha_2, \alpha_3 \in K^*$.
Dann ist $A_1 := K$ natürlich eine eindimensionale Algebra über $K$ mit der quadratischen Form $N(x) = x^2, x \in K$ und trivialer Konjugation.

a) Die über $K$ zweidimensionale normierte Algebra

$$A_2 := DD(A_1, \alpha_1)$$

heißt *quadratische Algebra* über $K$. Sie ist nach Lemma (1.22)(c) kommutativ und assoziativ, jedoch ist die Konjugation auf $A_2$ nicht mehr die Identität (Man beachte $\bar{i} = -i$ und $char(K) \neq 2$).

b) Die über $K$ vierdimensionale normierte Algebra

$$A_4 := (\frac{\alpha_1, \alpha_2}{K}) := DD(K, \alpha_1, \alpha_2) := DD(A_2, \alpha_2)$$

heißt *Quaternionenalgebra* über $K$. Sie ist nach Lemma (1.22)(b) assoziativ, jedoch nach Lemma (1.22)(c) nicht kommutativ, da die Konjugation auf $A_2$ nicht trivial ist.

c) Die über $K$ achtdimensionale normierte Algebra

$$A_8 := (\frac{\alpha_1, \alpha_2, \alpha_3}{K}) := DD(K, \alpha_1, \alpha_2, \alpha_3) := DD(A_4, \alpha_3)$$

heißt *Oktavenalgebra* über $K$. Sie ist nach Lemma (1.22)(a) nur noch alternativ und nach Lemma (1.22)(b) nicht mehr assoziativ, da $A_3$ nicht kommutativ ist.

Quaternionen- und Oktavenalgebren sind die natürliche Verallgemeinerung der zuvor definierten Quaternionen und Oktaven. Es ist nach Bemerkung (1.21)

$$\mathbb{H} \cong (\frac{-1, -1}{\mathbb{R}})$$

und

$$\mathbb{O} \cong (\frac{-1, -1, -1}{\mathbb{R}}).$$

Ähnlich wie im ersten Kapitel können wir für die allgemeinen Algebren $K$-Basen und deren Multiplikation angeben. Dies ist hier nur für die Quaternionenalgebren ausgeführt, da allgemeine Oktavenalgebren im weiteren Verlauf der Bachelorarbeit keine Rolle spielen werden.

**(1.24) Lemma**
Die Quaternionenalgebra $A := (\frac{\alpha_1, \alpha_2}{K})$ mit $\alpha_1, \alpha_2 \in K^*$ besitzt als vierdimensionale $K$-Algebra die Basis $(1, i, j, k)$ mit

$$i^2 = \alpha_1,\ j^2 = \alpha_2,\ ij = -ji = k.$$

**Beweis**
Es ist $A \cong DD(A_1, \alpha_2)$ mit $A_1 := DD(K, \alpha_1)$. Also existiert ein $i \in A_1$ mit $i^2 \overset{(20)}{=} -N(i) = \alpha$ und ein $j \in A$ mit $(j|\, i) = 0$ und $j^2 = -N(j) = \alpha$. Weiter ist $(1, i, j, k)$ mit $k := ij$ eine Basis von $(\frac{\alpha_1, \alpha_2}{K})$ und $k = (i + 0 \cdot j)(0 + 1 \cdot j) = j\bar{i} = -ji$ (nach(20)). □

Folgendes Lemma beschreibt expilizit die Konjugation, die quadratische Form und die sogenannte Spur in Quaternionalgebren.

**(1.25) Lemma**
Für $x = x_0 + x_1 i + x_2 j + x_3 k \in A := (\frac{\alpha_1,\alpha_2}{K})$ gilt:

$$\bar{x} = x_0 - x_1 i - x_2 j - x_3 k \tag{24}$$

$$N(x) = x\bar{x} = x_0^2 - \alpha_1 x_1^2 - \alpha_2 x_2^2 + \alpha_1\alpha_2 x_3^2 \tag{25}$$

$$tr(x) := x + \bar{x} = 2x_0 \tag{26}$$

Die $K$-lineare Abbildung $tr : A \to K$ heißt die Spur von $x$.

**Beweis**
(24) folgt durch zweifache Anwendung der Regel (18) für das Dickson Double, (25) ebenso mit (16) oder durch direktes Ausrechnen. Die $K$-Linearität von $tr$ ist klar. □

## 1.5 Der verallgemeinerte Satz von Hurwitz

Durch Anwenden von Lemma (1.22) auf immer größere Unteralgebren von $A$ bekommen wir den verallgemeinerten Satz von Hurwitz.

**(1.26) Satz**
Sei $K$ ein Körper mit $char(K) \neq 2$.
Ist $A$ eine normierte Algebra über $K$, so ist entweder $A = K$ oder $A$ eine quadratische Algebra oder $A$ eine Quaternionenalgebra oder $A$ eine Oktavenalgebra.

**Beweis**
Sei $A$ eine gegebene normierte Algebra über $K$.
Angenommen es ist $K \subset A \neq K$, dann gibt es nach Lemma (1.20) ein $i_1 \in K^\perp$ mit $N(i_1) = -\alpha_1$, $-\alpha_1 \in K^* \setminus N(K)$. Also ist nach Lemma (1.22)(c) die quadratische Algebra $A_2 := K + i_1 K \cong DD(K, \alpha_1)$ eine kommutative, assoziative normierte Unteralgebra von $A$, da $K$ eine kommutative, assoziative normierte Algebra mit trivialer Konjugation ist (Beache $\bar{x} = 2\,(x|\,1) - x = 2x - x = x$ für alle $x \in K$).
Wenn $A_2 \subset A \neq A_2$, dann gibt es ein $i_2 \in A_2^\perp$ mit $N(i_2) = -\alpha_2$, $-\alpha_2 \in K^* \setminus N(A_1)$. Also ist nach Lemma (1.22)(b) die Quaternionenalgebra $A_4 := A_2 + i_2 A_2 \cong DD(A_2, \alpha_2)$ eine assoziative normierte Unteralgebra von $A$, die nach (1.22)(c) nicht kommutativ ist, da die Konjugation auf $A_2$ nicht trivial ist (Beachte $\bar{i} = -i$).
Wenn $A_4 \subset A \neq A_4$, dann gibt es ein $i_3 \in A_4^\perp$ mit $N(i_3) = -\alpha_3$, $-\alpha_3 \in K^* \setminus N(A_4)$. Also ist nach Lemma (1.22)(a) die Oktavenalgebra $A_8 := A_4 + i_3 A_4 \cong DD(A_4, \alpha_3)$ eine normierte Unteralgebra von $A$, die nach (1.22)(b) nicht assoziativ ist, da $A_4$ nicht kommutativ ist.
Wenn nun $A_8 \subset A \neq A_8$, dann gibt es zwar ein $i_4 \in A_8^\perp$ mit $N(i_4) = -\alpha_4$, $-\alpha_4 \in K^* \setminus N(A_8)$. Aber die Algebra $A_{16} := A_8 + i_4 A_8$ ist nach Lemma (1.22)(a) nicht normiert, da $A_8$ nicht assoziativ ist. Dieser Fall kann also nicht eintreten. □

Als Spezialfall dieses Satzes erhalten wir für $K = \mathbb{R}$ die ursprünglichen Satz von Hurwitz.

**(1.27) Satz**
$\mathbb{R}, \mathbb{C}, \mathbb{H}$ und $\mathbb{O}$ sind bis auf Isomorphie die einzigen normierten Algebren über den reellen Zahlen.

**Beweis**
Wegen Lemma (1.19) und $N(\mathbb{R}) = \mathbb{R}_{\geq 0}$ können wir bei dem Cayley-Dickson-Prozess aus Definition (1.23) ohne Einschränkung $i_1, i_2, i_3$ mit $N(i_1) = N(i_2) = N(i_3) = 1$ wählen. Wir haben oben schon gesehen, dass dann die Multiplikation des Dickson Doubles (bzw. des dualen Dickson Doubles aus (1.21)) jeweils mit der Multiplikation in $\mathbb{R}, \mathbb{C}, \mathbb{H}$ beziehungsweise $\mathbb{O}$ übereinstimmt. Somit sind diese nach Satz (1.26) bis auf Isomorphie die einzigen normierten Algebren über $\mathbb{R}$. □

# 2 Zahlentheoretische Grundlagen

## 2.1 Gitter

Ein wichtiges Werkzeug in der Zahlentheorie ist die Gittertheorie, aus der wir die für uns relevanten Definitionen und Sätze zitieren. Als Referenz diene [Con2].

**(2.1) Definition**

a) Sei $R$ ein Ring mit Quotientenkörper $K$, $V$ ein $n$-dimensionaler $K$-Vektorraum sowie $(b_1, .., b_r) \in V$ ein linear unanbhängiges Tupel.
Dann heißt $L := \langle b_1, .., b_r \rangle_R$ ein *R-Gitter* in $V$.
Ist $B = (b_1, .., b_n)$ eine Basis von $V$, so heißt $L$ *volles R-Gitter* und $B$ eine *Gitterbasis* von $L$.

b) Ist speziell $E = (V, (.|.))$ ein euklidischer Vektorraum mit Skalarprodukt $(.|.)$, $B = (b_1, .., b_n)$ eine Gitterbasis von $L$ und $R = \mathbb{Z}$, so heißt $L := (B, (.|.))) := \langle b_1, .., b_r \rangle_{\mathbb{Z}}$ ein *Z-Gitter* in $V$ oder einfach nur *Gitter*.
Sei im Folgenden $L = (B, (.|.))$ ein $\mathbb{Z}$-Gitter mit Gitterbasis $B = (b_1, .., b_n)$.

c) $\mathbb{G}(B) := ((b_i|\, b_j)) \in \mathbb{R}^{n \times n}$ heißt die *Grammatix* von $L$ und $det(L) := det(\mathbb{G}(B))$ die *Determinante* von $L$.
Das Skalarprodukt $(.|.)$ heißt *positiv definit*, falls $(v|\, v) > 0$ für alle $v \in V$ und $(v|\, v) = 0$ genau dann, wenn $v = 0$ ist.

d) $L$ heißt *ganz*, falls $(b_i|\, b_j) \in \mathbb{Z}$ für alle $b_i, b_j \in B$, $i, j \in \{1, .., n\}$, das heißt $\mathbb{G}(B)$ ganz ist.

e) $L$ heißt *gerade*, falls $L$ ganz ist und $(b_i|\, b_i) \in 2\mathbb{Z}$ für alle $b_i \in B$, $i \in \{1, .., n\}$ gilt.

f) $L$ heißt *unimodular*, falls $L$ ganz ist und $|det(L)| = 1$ gilt.

**(2.2) Satz (siehe [Con2])**

Das sogenannte *Gosset-Gitter* $\mathbb{E}_8$, gegeben durch die Grammatrix

$$\mathbb{G}_{\mathbb{E}_8} = \begin{pmatrix} 2 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ -1 & 2 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 2 & -1 & 0 & 0 & 0 & -1 \\ 0 & 0 & -1 & 2 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 2 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 2 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 2 & 0 \\ 0 & 0 & -1 & 0 & 0 & 0 & 0 & 2 \end{pmatrix},$$

ist das (bis auf Isometrie) eindeutige Gitter im $\mathbb{R}^8$, welches gerade (und damit ganz), positiv definit und unimodular ist.

**(2.3) Definition**

a) Sei $L$ ein volles $\mathbb{Z}$-Gitter in $E = (V, (.|.))$ und das Skalarprodukt $(.|.)$ nicht ausgeartet. Dann ist

$$L^{\#} := \{v \in V;\ (v|\, l) \in \mathbb{Z}\ \forall l \in L\}$$

ebenfalls ein volles $\mathbb{Z}$-Gitter in $E$, das zu $L$ *duale Gitter*.

b) $L$ heißt *selbstdual*, falls $L^{\#} = L$.

**(2.4) Lemma**

Es gilt $det(L^{\#})det(L) = 1$. Ist also $L$ selbstdual, so folgt $det(L)^2 = 1$, das heißt $L$ ist unimodular.

**Beweis**

Sei $B = (b_1, .., b_b)$ eine Gitterbasis von $L$ und sei $B^* = (b_1^*, .., b_n^*)$ die Dualbasis von $B$, das heißt $\left(b_i \middle| b_j^*\right) = \delta_{ij}$. Dann ist $L^{\#} = \langle b_1^*, .., b_n^* \rangle$ und $\mathbb{G}(B)^{-1}$ die Basiswechselmatrix von $B$ nach $B^*$. Also gilt $\mathbb{G}(B^*) = \mathbb{G}(B)^{-1}\mathbb{G}(B)\mathbb{G}(B)^{-tr} = \mathbb{G}(B)^{-1}$, folglich ist $\mathbb{G}(B^*)\mathbb{G}(B) = I_n$ und $det(L^{\#})det(L) = 1$. □

**(2.5) Definition**

Die *Überdeckungszahl* eines Gitters $L$ über einem euklidischen Vektorraum $(V, (.|.))$ ist das kleinste $r > 0$, sodass die Kugeln mit Radius $r$ um die Punkte des Gitters $l \in L$ den kompletten Raum $V$ überdecken. Dies bedeutet, dass zu jedem $P \in V$ ein $l \in L$ existiert, sodass

$$(P - l|\, P - l) \leq r.$$

Mithilfe der Überdeckungszahl eines Gitters kann oft entschieden werden, ob eine sogenannte Ordnung von „ganzen Elementen“ euklidisch ist.

## 2.2 Algebraische Zahlkörper

Da wir später Quaternionenalgebren über quadratischen Zahlkörpern untersuchen wollen, werden hier die dafür wichtigsten Resultate über Zahlkörper zusammengestellt, wobei die Beweise nicht ausgeführt sind. Als Referenz diene beispielsweise [Neu].

**(2.6) Definition**

Ein *algebraischer Zahlkörper* $K$ ist eine endliche Körpererweiterung der rationalen Zahlen $\mathbb{Q}$. Ein Element $a \in K$ heißt *ganz*, falls es ein $n \in \mathbb{N}$ und $b_1, .., b_n \in \mathbb{Z}$ gibt, sodass

$$a^n + b_1 a^{n-1} + .. + b_{n-1}a + b_n = 0.$$

Der Ring $\mathbb{Z}_K := \{a \in K;\ a \text{ ist ganz}\}$ heißt der *Ganzheitsring* von $K$. $\mathbb{Z}_K$ ist ein endlich erzeugter $\mathbb{Z}$-Modul und jede $\mathbb{Z}$-Basis von $\mathbb{Z}_K$ heißt *Ganzheitsbasis*.

**(2.7) Bemerkung**
Im Fall einer quadratischen Körpererweiterung $K = \mathbb{Q}(\sqrt{d}) = \{x + y\sqrt{d};\ x, y \in \mathbb{Q}\}$ mit $d \in \mathbb{Z} \setminus \{0, 1\}$ quadratfrei kann man die zugehörigen Ganzheitsringe leicht bestimmen. Es gilt

$$\mathbb{Z}_K = \begin{cases} \mathbb{Z}[\frac{1+\sqrt{d}}{2}], & \text{falls } d \equiv_4 1 \\ \mathbb{Z}[\sqrt{d}], & \text{falls } d \equiv_4 2 \text{ oder } d \equiv_4 3. \end{cases}$$

**(2.8) Definition**
Sei $K$ ein algebraischer Zahlkörper.

a) $K$ heißt *total reell*, falls jede Einbettung $\sigma : K \to \mathbb{C}$ reell ist, das heißt $\sigma(K) \subseteq \mathbb{R}$.

b) Ist $K$ total reell, so heißt $a \in K$ *total positiv*, falls $\sigma(a) > 0$ für jede Einbettung $\sigma : K \to \mathbb{R}$ gilt.

**(2.9) Bemerkung**
Ist $K = \mathbb{Q}(\sqrt{d})$ eine quadratische Körpererweiterung, so sind die zwei Einbettungen von $K$ nach $\mathbb{C}$ gegeben durch $\sigma_1(x + y\sqrt{d}) = x + y\sqrt{d}$ und $\sigma_2(x + y\sqrt{d}) = x - y\sqrt{d}$. Ist $d > 0$, so ist $K$ total reell.

**(2.10) Definition**
Sei $K$ ein algebraischer Zahlkörper. Die *Spur* und die *Norm* eines Elements $a \in K$ sind als die Spur und die Determinante der $\mathbb{Q}$-linearen Abbildung

$$T_a : K \to K, \quad T_a(x) = ax$$

des $\mathbb{Q}$-Vektorraums $K$ definiert:

$$Tr_{K|\mathbb{Q}}(a) := Tr(T_a), \quad N_{K|\mathbb{Q}} := det(T_a).$$

**(2.11) Bemerkung**
a) Die Spur $Tr_{K|\mathbb{Q}}$ ist $\mathbb{Q}$-linear, die Norm $Nr_{K|\mathbb{Q}}$ ist multiplikativ und anisotrop.
Für $a \in \mathbb{Z}_K$ gilt $Tr_{K|\mathbb{Q}}(a), Nr_{K|\mathbb{Q}}(a) \in \mathbb{Z}$.

b) Sind $\sigma_1, .., \sigma_n : K \to \mathbb{C}$ die Einbettungen von K in die komplexen Zahlen $\mathbb{C} = \overline{\mathbb{Q}}$, so gilt $Tr_{K|\mathbb{Q}}(x) = \sum_{i=1}^{n} \sigma_i x$ und $Nr_{K|\mathbb{Q}}(x) = \prod_{i=1}^{n} \sigma_i x$.

c) Ist $K$ total reell und $a \in K$ total positiv, so gilt nach b) mit der *Ungleichung vom arithmetischen und geometrischen Mittel*, dass

$$\frac{1}{n} Tr_{K|\mathbb{Q}}(a) \geq Nr_{K|\mathbb{Q}}(a)^{\frac{1}{n}}.$$

d) Ist $K = \mathbb{Q}(\sqrt{d})$ ein quadratischer Zahlkörper so folgt aus b)

$$Tr_{K|\mathbb{Q}}(x + y\sqrt{d}) = (x + y\sqrt{d}) + (x - y\sqrt{d}) = 2x$$

$$Nr_{K|\mathbb{Q}}(x + y\sqrt{d}) = (x + y\sqrt{d})(x - y\sqrt{d}) = x^2 - dy^2.$$

**(2.12) Definition**
Sei $K$ ein algebraischer Zahlkörper mit Ganzheitsbasis $B = (b_1, .., b_n) \in K^n$.

a) Die Determinante der *Grammatrix*

$$Gram(B) := (Tr_{K|\mathbb{Q}}(b_i b_j))_{i,j=1}^{n}$$

heißt die Diskriminante $d_K$ von $K$. Sie ist unabhängig von der Wahl der Basis.

b) Die *inverse Differente* von $\mathbb{Z}_K$ ist das duale Gitter bezüglich der nicht ausgearteten Spurbilinearform $Tr_{K|\mathbb{Q}}$

$$\mathbb{Z}_K^{\#} = \{a \in K;\ Tr_{K|\mathbb{Q}}(az) \in \mathbb{Z}\ \forall z \in \mathbb{Z}_K\}.$$

**(2.13) Bemerkung**
1. Ist $K = \mathbb{Q}(\sqrt{d})$ ein quadratischer Zahlkörper, so gilt $d_K = d$ für $d \equiv_4 1$ und $d_K = 4d$ sonst.
2. Es gilt allgemein $|d_K| = \left|\mathbb{Z}_K^{\#}/\mathbb{Z}_K\right|$ und für $K = \mathbb{Q}(\sqrt{d})$ speziell $\mathbb{Z}_K^{\#} = \frac{1}{\sqrt{d}}\mathbb{Z}_K$ für $d \equiv_4 1$ und $\mathbb{Z}_K^{\#} = \frac{1}{2\sqrt{d}}\mathbb{Z}_K$ sonst.

## 2.3 Ordnungen

Untersuchungsgegenstand der Zahlentheorie sind vor allem „maximale Mengen von ganzen Elementen“ in einem gegebenen Ring. Im nichtkommutativen Fall bildet die Menge der ganzen Zahlen im Sinne von Definition (2.6) jedoch keinen Ring mehr, daher wird das Konzept der Maximalordnung eingeführt. Die folgende Definition erweitert den Begriff der Maximalordnung auf auch nichtassoziative Algebren.

**(2.14) Definition**
Sei $A$ eine normierte Algebra über dem Zahlkörper $K$ mit Ganzheitsring $R = \mathbb{Z}_K$.
$\mathcal{O} \subset A$ heißt *R-Ordnung* (oder kurz *Ordnung*) in $A$, falls

a) $\mathcal{O}$ eine Unteralgebra von $A$ ist mit $1 \in \mathcal{O}$,

b) $\mathcal{O}$ ein volles $R$-Gitter in $A$ ist und

c) jedes Element von $\mathcal{O}$ *ganzzahlig* ist, das heißt für alle $a \in \mathcal{O}$ gilt $N(a) \in R$ und $tr(a) := 2\,(x|\,1) \in R$.

Eine $R$-Ordnung $M \subset A$ heißt *R-Maximalordnung* (oder kurz *Maximalordnung*) in $A$, falls für jede $R$-Ordnung $M'$ mit $M \subseteq M' \subseteq A$ folgt, dass $M = M'$ ist.

**(2.15) Bemerkung**
a) Bedingung c) der Definition einer Ordnung bedeutet, dass für jedes $a \in \mathcal{O}$ die Koeffizienten des Polynoms

$$x^2 - tr(a)x + N(a)$$

im Ganzheitsring $R$ liegen.

b) Ist $A = K$ ein algebraischer Zahlkörper, so ist $\mathbb{Z}_K$ die eindeutige Maximalordnung in $K$.

c) Man kann zeigen, dass in einer normierten Algebra immer eine Maximalordnung existiert, die jedoch im Allgemeinen nicht eindeutig ist.

**(2.16) Definition**
Die Abbildung $Nr : A \to \mathbb{Q}$ definiert durch

$$Nr(a) := N_{K|\mathbb{Q}}(N(a))$$

heißt *Norm* auf $A$.

**(2.17) Bemerkung**
Sei $\mathcal{O}$ eine $R$-Ordnung in der normierten Algebra $A$.
Da $N(a) \in R$ für alle $a \in \mathcal{O}$, gilt $Nr(\mathcal{O}) \subseteq \mathbb{Z}$, das heißt die Einschränkung der Norm auf $\mathcal{O}$ ist ganzzahlig.
Da nach Lemma (2.11)(a) $N_{K|\mathbb{Q}}$ und nach Definition $N$ anisotrop und multiplikativ sind, ist auch $Nr$ anisotrop und multiplikativ.

Wir definieren in einer nicht notwendigerweise kommutativen Ordnung die Begriffe Ideal, Primideal und Teilbarkeit wie folgt:

**(2.18) Definition**
Sei $\mathcal{O}$ eine $R-$Ordnung in $A$ und $I$ ein $R-$Gitter in $A$.

a) $I$ heißt *Rechtsideal (Linksideal)* in $\mathcal{O}$, falls $I\mathcal{O} \subseteq I$ (bzw. $\mathcal{O}I \subseteq I$).
$I$ heißt *zweiseitiges Ideal* in $\mathcal{O}$, falls $I$ Rechts- und Linksideal ist.

b) $I$ heißt *Rechtshauptideal (Linkshauptideal)* in $\mathcal{O}$, falls $I = a\mathcal{O}$ ($I = \mathcal{O}a$) für ein $a \in \mathcal{O}$ ist.
$I$ heißt *Hauptideal* in $\mathcal{O}$, falls $I$ Rechts- und Linkshauptideal ist.

c) Ein zweiseitiges Ideal $\mathcal{P} \neq \mathcal{O}$ in $\mathcal{O}$ heißt *Primideal* von $\mathcal{O}$, falls für zweiseitige Ideale $I, I'$ in $\mathcal{O}$ mit $II' \subseteq \mathcal{P}$ stets $I \subseteq \mathcal{P}$ oder $I' \subseteq \mathcal{P}$ folgt.

d) $y \in \mathcal{O}$ heißt *Linksteiler* (*Rechtsteiler*) von $z \in \mathcal{O}$, falls $y^{-1}z \in \mathcal{O}$ ($zy^{-1} \in \mathcal{O}$). Falls $y$ Linksteiler von $z$ ist, so sagen wir auch $y$ teilt $z$ und schreiben $y|z$.

Wir kommen nun zu der Eigenschaft von Ordnungen, die im Zentrum dieser Bachelorarbeit stehen wird.

**(2.19) Definition**
Eine Ordnung $\mathcal{O}$ in $A$ heißt *linkseuklidisch* (bzw. *rechtseuklidisch*), falls

$$\forall a, b \in \mathcal{O},\ b \neq 0\ \ \exists q, r \in \mathcal{O},\ \text{sodass } a = qb + r \text{ (bzw. } a = bq + r) \text{ und } |Nr(r)| < |Nr(b)|\,.$$

$\mathcal{O}$ heißt *euklidisch*, falls $\mathcal{O}$ links- und rechtseuklidisch ist.

Die folgende Charakterisierung der Eigenschaft euklidisch wird im weiteren Verlauf sehr nützlich sein.

**(2.20) Lemma**
Eine Ordnung $\mathcal{O}$ in $A$ ist euklidisch genau dann, wenn

$$\forall h \in A \;\; \exists q \in \mathcal{O}, \text{ sodass } |Nr(h-q)| < 1.$$

Insbesondere ist $\mathcal{O}$ genau dann linkseuklidisch, falls $\mathcal{O}$ rechtseukldisch ist.

**Beweis**
„$\Rightarrow$“: Sei $h \in A = K \otimes_R \mathcal{O}$, sowie $0 \neq n \in R$, sodass $nh \in \mathcal{O}$. Dann gibt es $q, r \in \mathcal{O}$, sodass $nh = nq + r$ und $|Nr(r)| < |Nr(n)|$. Also gilt $|Nr(h-q)| = \left|Nr(\frac{r}{n})\right| = \frac{|Nr(r)|}{|Nr(n)|} < 1$.
„$\Leftarrow$“: Seien $a, b \in \mathcal{O}, b \neq 0$. Setze $h := b^{-1}a \in A$, dann gibt es ein $q \in \mathcal{O}$ mit $|Nr(h-q)| < 1$; setze weiter $r := a - bq \in \mathcal{O}$. Dann gilt mit dem Satz von Artin

$$\begin{aligned} |Nr(r)| = |Nr(a-bq)| = \left|Nr((bb^{-1})a - bq)\right| &= \left|Nr(b(b^{-1}a) - ba)\right| \\ &= |Nr(b)| \left|Nr(b^{-1}a - q)\right| \\ &< |Nr(b)|, \end{aligned}$$

also ist $\mathcal{O}$ rechtseuklidisch. Für den Beweis der Eigenschaft linkseuklidisch setze $h := ab^{-1}$ und verfahre analog. □

Aus diesem Lemma folgt, dass wir uns bei der Suche nach euklidischen Ordnungen auf Maximalordnungen beschränken können.

**(2.21) Satz**
Ist die Ordnung $\mathcal{O}$ in der normierten Algebra $A$ euklidisch, so ist $\mathcal{O}$ eine Maximalordnung.

**Beweis**
Angenommen $\mathcal{O}$ wäre keine Maximalordnung in $A$, dann existiert eine Ordnung $\mathcal{O}'$ in $A$ mit $\mathcal{O} \subsetneq \mathcal{O}'$. Sei $a' \in \mathcal{O}' \setminus \mathcal{O}$. Dann existiert nach Lemma (2.20) ein $a \in \mathcal{O}$ mit $|Nr(a-a')| < 1$. Da aber $a - a' \in \mathcal{O}'$, gilt $|Nr(a-a')| \in \mathbb{Z}_{\geq 0}$, also $Nr(a-a') = 0$. Da $Nr$ anisotrop ist, folgt $a = a'$, also $\mathcal{O} = \mathcal{O}'$, Widerspruch. □

# 3 Euklidischer Algorithmus und Primfaktorzerlegung

Wir wollen im Folgenden Zahlentheorie in Quaternionen und Oktaven betreiben. Dazu werden uns nicht mehr die Algebren $\mathbb{H}$ und $\mathbb{O}$ über $\mathbb{R}$ als Ausgangspunkt dienen, sondern (vorerst) die Quaternionen und Oktaven über $\mathbb{Q}$. Wir definieren die *Quaternionen (über* $\mathbb{Q}$*)*

$$\mathbb{H} := \mathbb{Q}(i,j,k) := (\frac{-1,-1}{\mathbb{Q}})$$

und die *Oktaven (über* $\mathbb{Q}$*)*

$$\mathbb{O} := \mathbb{Q}(e_0,..,e_7) := (\frac{-1,-1,-1}{\mathbb{Q}}).$$

Dass wir für die Algebren über $\mathbb{Q}$ die gleichen Symbole verwenden wie für die Algebren über $\mathbb{R}$, dient nur der einfacheren Notation und soll nicht über die Unterschiede hinwegtäuschen.
In einer normierten Algebra $A$ über $\mathbb{Q}$ gilt für die Norm $Nr(a) = N_{\mathbb{Q}|\mathbb{Q}}(N(a)) = N(a)$ für $a \in A$ und wir bezeichnen daher in diesen Fällen die Norm von $a$ mit $N(a)$ statt mit $Nr(a)$.
Später werden wir uns auch mit Quaternionenalgebren

$$(\frac{-1,-1}{\mathbb{Q}(\sqrt{d})})$$

über quadratischen Zahlkörpern beschäftigen (für spezielle Werte $d \in \mathbb{Z}$).
Ziel ist es, in einigen dieser Algebren euklidische Maximalordnungen zu finden und dort euklidische Algorithmen und eindeutige Primfaktorzerlegungen zu studieren. Bevor wir dies tun, sei an den eindimensionalen Fall der ganzen Zahlen $\mathbb{Z} \subset \mathbb{Q}$ erinnert. $\mathbb{Z}$ ist nach Bemerkung (2.15)(b) die eindeutig Maximalordnung in $\mathbb{Q}$.

## 3.1 Der eindimensionale Fall

**(3.1) Lemma**
Sind $a, b \in \mathbb{Z}$ mit $b \neq 0$, so gibt es $q, r \in \mathbb{Z}$ mit

$$a = qb + r \quad \text{und} \quad |r| < |b|\,.$$

Dass wir aus dieser Division mit Rest den euklidischen Algorithmus erhalten, der für zwei ganze Zahlen $a, b \in \mathbb{Z}$ den größten gemeinsamen Teiler $ggT(a,b)$ bestimmt, sagt uns folgendes

**(3.2) Lemma**
Sind $a, b \in \mathbb{Z}$ und $a = qb + r$ für $q, r \in \mathbb{Z}$, dann gilt $ggT(a,b) = ggT(b,r)$.

Die Beweise der Lemmata wurden in einer der Grundvorlesungen behandelt und werden hier daher nicht ausgeführt. Es sei jedoch bemerkt, dass zum Beweis von Lemma (3.2) lediglich die Assoziativität von $\mathbb{Z}$ gebraucht wird. Dies wird das Argument dafür sein, dass der gewöhnliche euklidische Algorithmus in den Hurwitz Quaternionen funktioniert. Für die ganzzahligen Oktaven brauchen wir dann eine andere Idee.
Nun erstmal zum bekannten *euklidischen Algorithmus*:
Seien $a, b \in \mathbb{Z}$ gegeben, gesucht ist $ggT(a,b) \in \mathbb{Z}$.
Dann gibt es nach der Division mit Rest eine abbrechende Folge von ganzen Zahlen $q_1, q_2, ..q_{n+1}$ und $r_1, r_2, .., r_n$, sodass

$$\begin{aligned} a &= q_1 b + r_1 \quad \text{mit} \quad |r_1| < |b| \\ b &= q_2 r_1 + r_2 \quad \text{mit} \quad |r_2| < |r_1| \\ &\ldots \\ r_{n-2} &= q_n r_{n-1} + r_n \quad \text{mit} \quad |r_n| < |r_{n-1}| \\ r_{n-1} &= q_{n+1} r_n + 0. \end{aligned} \tag{27}$$

Dann ist nach Lemma (3.2) $ggT(a,b) = r_n$.

Ganz allgemein ist jeder euklidische kommutative Ring ein Hauptidealbereich und somit faktoriell, das heißt es gibt eine bis auf Einheiten eindeutige Primfaktorzerlegung. Insbesondere ist $\mathbb{Z}$ bekanntlich faktoriell.

## 3.2 Euklidischer Algorithmus in den Hurwitz Quaternionen

Nun wollen wir Ordnungen in den Quaternionen $\mathbb{H}$ über $\mathbb{Q}$ betrachten. Zunächst könnte man vermuten, dass eine Maximalordnung genau wie die Gaußschen Zahlen in der komplexen Ebene auszusehen hat.

**(3.3) Definition**
$L := \mathbb{Z}[1,i,j,k] := \{z_1 + z_2 i + z_3 j + z_4 k \in \mathbb{H};\ z_1, z_2, z_3, z_4 \in \mathbb{Z}\}$ heißt die Menge der *Lipschitz Quaternionen*.

Wir haben die positiv definite Norm

$$N : L \to \mathbb{N}_0,\ N(z) := z\bar{z} = z_1^2 + z_2^2 + z_3^2 + z_4^2 \quad \text{für} \quad z = z_1 + z_2 i + z_3 j + z_4 k \in L.$$

$L$ ist offensichtlich eine Ordnung, jedoch gibt es in dieser keine Division mit Rest im Sinne einer strikten Normreduktion.

**(3.4) Satz**
Sind $a, b \in L$ mit $b \neq 0$, so gibt es $q, r \in L$ mit

$$a = qb + r \quad \text{und} \quad N(r) \leq N(b).$$

Es gilt $N(r) = N(b)$ genau dann, wenn für $ab^{-1} = c_1 + c_2 i + c_3 j + c_4 k \in \mathbb{H}$ gilt:

$$c_i \in \mathbb{Z} + \frac{1}{2}, \quad i = 1, .., 4.$$

**Beweis**
Setze $c := ab^{-1} = c_1 + c_2 i + c_3 j + c_4 k \in \mathbb{H}$ und für $i = 1, .., 4$ sei $c_i = q_i + s_i$ mit $q_i \in \mathbb{Z}$ und $|s_i| \leq \frac{1}{2}$. Dazu wähle $q_i := \lfloor c_i \rfloor$, falls $c_i - \lfloor c_i \rfloor \leq \frac{1}{2}$, sonst $q_i := \lfloor c_i \rfloor + 1$.
Weiter sei $q := q_1 + q_2 i + q_3 j + q_4 k \in L$, $s := s_1 + s_2 i + s_3 j + s_4 k \in \mathbb{H}$ und $r := sb$. Dann ist

$$a = cb = (q + s)b = qb + sb = qb + r,$$

also $r = a - qb \in L$, und

$$N(r) = N(s)N(b) = (s_1^2 + s_2^2 + s_3^2 + s_4^2)N(b) \leq ((1/2)^2 + .. + (1/2)^2)N(b) = N(b).$$

Dabei gilt $N(r) = N(b) \Leftrightarrow |s_i| = \frac{1}{2} \ \forall i \in \{1, .., 4\} \Leftrightarrow c_i \in \mathbb{Z} + \frac{1}{2} \ \forall i \in \{1, .., 4\}$. □

**(3.5) Bemerkung**
Der duale Satz für die Zerlegung $a = bq + r$ gilt natürlich völlig analog, wobei man im Beweis $c := b^{-1}a$ setze.

Da bei der Division mit Rest in $L$ der Rest betragsmäßig nicht immer echt kleiner wird, scheitert unser Euklidischer Algorithmus (27). Denn dieser terminiert ja gerade aufgrund der strikten Normreduktion in jedem Schritt.
Satz (3.4) gibt uns aber schon den entscheidenden Hinweis, wie wir dieses Problem umgehen können.

**(3.6) Definition**
$H := \{z_1 + z_2 i + z_3 j + z_4 k \in \mathbb{H};\ z_1, z_2, z_3, z_4 \in \mathbb{Z} \text{ oder } z_1, z_2, z_3, z_4 \in \mathbb{Z} + \frac{1}{2}\}$ heißt die Menge der *Hurwitz Quaternionen*.

Man rechnet leicht nach, dass $H$ mit der Einschränkung der Multiplikation von $\mathbb{H}$ einen Ring bildet, der von der $\mathbb{Z}$-Basis $(1, i, j, \frac{1}{2}(1 + i + j + ij))$ erzeugt wird, und ebenso, dass $N(h) \in \mathbb{Z}$ und $2\,(h|\,1) = 2h_0 \in \mathbb{Z}$ für alle $h \in H$. Also bilden die Hurwitz Quaternionen als volles Gitter eine Ordnung in $\mathbb{H}$.
Aus Satz (3.4) und Bemerkung (3.5) folgt jetzt sofort, dass die Hurwitz Quaternionen eine „echte“ Division mit Rest besitzen, also eine euklidische Ordnung sind:

**(3.7) Korollar**
Sind $a, b \in H$ mit $b \neq 0$, so gibt es $q, r, q', r' \in H$ mit

$$a = qb + r \quad \text{und} \quad N(r) < N(b),$$

$$a = bq' + r' \quad \text{und} \quad N(r') < N(b).$$

**Beweis**
Definiere $c, q, r$ wie oben, sodass $a = qb + r$. Entweder gilt dann schon $N(r) < N(b)$ oder es gilt $N(r) = N(b)$, wobei dann $c_i \in \mathbb{Z} + \frac{1}{2}$ für $i = 1, .., 4$, also $c = c_1 + c_2 i + c_3 j + c_4 k \in L$ und $a = cb + 0$ (Beachte $N(0) < N(b)$). Die zweite Behauptung folgt analog mit Bemerkung (3.5). □

**(3.8) Bemerkung**
Man kann sogar zeigen, dass in Korollar (3.7) immer $N(r) \leq \frac{1}{2}N(b)$ gilt.
Dazu fasst man $H$ als $\mathbb{Z}$-Gitter mit dem reskalierten Skalarprodukt $2\,(.|.)$ auf. Dann ist

$$\mathbb{G}(B) = \begin{pmatrix} 2 & 0 & 0 & 1 \\ 0 & 2 & 0 & 1 \\ 0 & 0 & 2 & 1 \\ 1 & 1 & 1 & 2 \end{pmatrix}$$

die Grammatrix von $(B, 2\,(.|.))$ mit $B = (1, i, j, \frac{1}{2}(1 + i + j + ij))$ eine $\mathbb{Z}$-Basis von $H$. Folglich ist $(B, 2\,(.|.))$ ein positiv definites, gerades Wurzelgitter (d.h. für alle Basiselemente $b \in B$ gilt $(b|\,b) = 2$) mit $det(\mathbb{G}(B)) = 4$, also ist $(B, 2\,(.|.)) \cong \mathbb{D}_4$ ($\mathbb{D}_4$ ist nach [Ebe, Theorem (1.2)] das eindeutige Gitter im $\mathbb{Q}^4$ mit diesen Eigenschaften). Es ist bekannt, dass die Überdeckungszahl des Gitters $\mathbb{D}_4$ gleich 1 ist, also folgt die Behauptung, da wir das Skalarprodukt mit 2 reskaliert haben.

Aus oben genannten Gründen ($H$ ist assoziativ) ist der Euklidische Algorithmus (27) also auch in $H$ durchführbar, wobei man dann je nach verwendeter Faktorisierung einen größten Links- beziehungsweise Rechtsteiler bekommt.

**(3.9) Korollar**
a) Die Hurwitz Quaternionen $H$ bilden eine Maximalordnung in $\mathbb{H}$.

b) Jedes Rechtsideal (bzw. Linksideal) von $H$ ist Rechtshauptideal (Linkshauptideal).

c) Jede Maximalordnung in $\mathbb{H}$ ist konjugiert zu den Hurwitz Quaternionen $H$.

**Beweis**
a) folgt aus Korollar (3.7) und Satz (2.21).

b) folgt aus der Existenz eines Euklidischen Algorithmus.

c) Sei $M$ eine Maximalordnung in $\mathbb{H}$ mit $\mathbb{Z}$-Basis $B_M$ und $B_H$ eine $\mathbb{Z}$-Basis von $H$. Definiere $I := MH := \langle b_M b_H |\ b_M \in B_M,\ b_H \in B_H \rangle_{\mathbb{Z}}$. Dann ist $I$ ein Rechtsideal von $H$ und nach (b) also ein Rechtshauptideal, das heißt es existiert ein $x \in \mathbb{H}^*$ mit $I = xH$. Weiter ist $MI \subseteq I$ und mit $1 \in M$ folgt $I \subseteq MI$, also $MI = I$. Damit ist $MxH = xH$, also $x^{-1}MxH = H$ und somit $x^{-1}Mx \subseteq H$. Da $M$ und folglich auch $x^{-1}Mx$ eine Maximalordnung ist, folgt $x^{-1}Mx = H$. Dies zeigt, dass $M$ und $H$ konjugiert sind. □

## 3.3 Primfaktorzerlegung in den Hurwitz Quaternionen

Da die Quaternionen nicht kommutativ sind, können wir nicht wie in $\mathbb{Z}$ und $\mathbb{Z}[i]$ folgern, dass wegen der euklidischen Eigenschaft sofort eine bis auf Einheiten eindeutige Primfaktorzerlegung existiert. Zunächst führen wir einige Begriffe für den nichtkommutativen Ring der Hurwitz Quaternionen ein.

**(3.10) Definition**

a) $z \in H$ heißt *Hurwitz-Primzahl*, falls $N(z) \in \mathbb{Z}$ eine Primzahl ist.

b) $z \in H$ heißt *primitiv*, falls die größte natürliche Zahl, die z teilt, gleich 1 ist.

c) Sei $Q = P_0 \cdot .. \cdot P_k \in H$ primitiv und seien $P_0, .., P_k \in H$ Hurwitz-Primzahlen mit $N(P_0) = p_0, .., N(P_k) = p_k,\ k \in \mathbb{N}$. Dann heißt die Faktorisierung $p_0 \cdot .. \cdot p_k$ von $N(Q)$ das *Modell* der Faktorisierung $P_0 \cdot .. \cdot P_k$ von $Q$.

Das Konzept des Modells wird eingeführt um zu berücksichtigen, dass es bei der Faktorisieung der Norm von Q auf die Reihenfolge der Primfaktoren ankommt. Um bei gegebenem Modell zu einer Eindeutigkeit der Primfaktorisierung in $H$ zu gelangen, fehlt uns noch das Studium der Einheiten in $H$.

**(3.11) Lemma**

Es gilt $H^* = \{z \in H;\ z^{-1} \in H\} = \{z \in H;\ N(z) = 1\}$, das heißt die Einheiten von $H$ sind genau die Elemente mit Norm 1.
Somit ist $H^* = \{\pm 1,\ \pm i,\ \pm j,\ \pm k,\ \pm\frac{1}{2} \pm \frac{1}{2}i \pm \frac{1}{2}j \pm \frac{1}{2}k\}$ , also $|H^*| = 24$.

**Beweis**

Zeige zuerst $H^* = \{z \in H;\ N(z) = 1\}$.
Sei $z \in H^*$, dann gilt $z^{-1} \in H$ und $zz^{-1} = 1$. Anwenden der multiplikativen Norm auf beide Seiten der Gleichung liefert $N(z)N(z^{-1}) = 1$. Aus $N(H) \subseteq \mathbb{N}_0$ folgt $N(z) = N(z^{-1}) = 1$.
Sei $z \in H$ mit $N(z) = 1$. Dann ist $z^{-1} = \bar{z} \in H$, da $N(z) = z\bar{z} = 1$. Also folgt $z \in H^*$.
Bestimme nun die Einheiten von $H$:
Wegen $N(z) = 1$ für $z = z_0 + z_1 i + z_2 j + z_3 k \in L^*$ eine Einheit in den Lipschitz Quaternionen muss $|z_l| \geq 1$ für ein $l \in \{0, .., 3\}$ sowie $\sum_{m=0}^{3} z_m^2 = 1$ gelten. Folglich gibt es ein $l \in \{0, .., 3\}$ mit $z_l = \pm 1$ und $z_m = 0$ für $m \neq l$. Ist $z \in H^* \setminus L^*$, so gilt $|z_l| \geq \frac{1}{2}$ für alle $l \in \{0, .., 3\}$ und wegen $\sum_{m=0}^{3} z_m^2 = 1$ folgt $z_l = \pm\frac{1}{2}$ für alle $l \in \{0, .., 3\}$. □

Wir kommen nun zur Primfaktorzerlegung eines primitiven Hurwitz Quaternions.

**(3.12) Satz**

Sei $Q \in H$ primitiv. Dann ist jede Faktorisierung $N(Q) = p_0 \cdot .. \cdot p_k$ von $N(Q)$ ein Modell einer Faktorisierung $Q = P_0 \cdot .. \cdot P_k$ von $Q$ mit $P_0, .., P_k \in H$ Hurwitz-Primzahlen und $N(P_0) = p_0, .., N(P_k) = p_k$.

Ist weiter $Q = P_0 \cdot .. \cdot P_k$ irgendeine Faktorisierung von $Q$ mit dem Modell $p_0 \cdot .. \cdot p_k$, so hat jede weitere Faktorisierung von $Q$ die Form $Q = (P_0U_1)(U_1^{-1}P_1U_2) \cdot .. \cdot (U_{k-1}^{-1}P_{k-1}U_k)(U_k^{-1}P_k)$ mit $U_i \in H^*$ für $i \in \{1, .., k\}$, das heißt die Faktorisierung zu einem gegebenen Modell ist eindeutig bis auf das Einfügen von Einheiten.

**Beweis**
Sei $Q \in H$ primitiv und $N(Q) = p_0 \cdot .. \cdot p_k$ eine Primfaktorisierung von $Q$.
Da $H$ einen euklidischen Algorithmus besitzt, ist jedes Rechtsideal ein Rechtshauptideal, das heißt es ist $p_0H + QH = \{p_0h_0 + Qh_1;\ h_0, h_1 \in H\} = P_0H$ für ein $P_0 \in H$. Wegen $p_0H \subseteq P_0H$ gilt $N(P_0)|N(p_0) = p_0^2$, also $N(P_0) = 1,\ N(P_0) = p_0$ oder $N(P_0) = p_0^2$.
Im ersten Fall $N(P_0) = 1$ wäre $p_0H + QH = H$. Für $p_0h_0 + Qh_1 \in p_0H + QH$ ist aber

$$\begin{aligned} N(p_0h_0 + Qh_1) &= N(p_0h_0) + 2\,(p_0h_0|\,Qh_1) + N(Qh_1) \\ &= p_0^2N(h_0) + 2p_0\,(h_0|\,Qh_1) + N(Q)N(h_1) \\ &= p_0(p_0N(h_0) + 2\,(h_0|\,Qh_1) + p_1p_2..p_kN(h_1)) \end{aligned}$$

durch $p_0 > 1$ teilbar im Widerspruch zu $p_0H + QH = H$.
Im dritten Fall $N(P_0) = p_0^2 = N(p_0)$ wäre $P_0 = p_0U$ für eine Einheit $U \in H^*$. Aus $QH \subseteq P_0H$ folgt aber $Q = P_0P' = p_0UP'$ für ein $P' \in H$, also $p_0|Q$ im Widerspruch zur Primitivität von $Q$.
Also bleibt nur noch der zweite Fall $N(P_0) = p_0$, sodass $P_0$ eine Hurwitz-Primzahl ist, die wegen $QH \subseteq P_0H$ Linksteiler von $Q$ ist ($P_0^{-1}Q \in H$). Wir erhalten somit $Q = P_0Q_1$ mit $Q_1 \in H$ und $N(Q_1) = p_1..p_k$, wobei $P_0$ eindeutig bis auf Rechtsmultiplikation mit einer Einheit ist.
Mit der gleichen Argumentation erhalten wir sukzessive die Faktorisierungen

$$Q_1 = P_1Q_2,\ Q_2 = P_2Q_3,\ .....\ ,\ Q_{k-1} = P_{k-1}Q_k$$

mit $P_1, .., P_{k-1}, Q_k \in H$ Hurwitz-Primzahlen von Norm

$$N(P_1) = p_1, .., N(P_{k-1}) = p_{k-1}, N(Q_k) = p_k.$$

Setzen wir $P_k := Q_k$, so erhalten wir die gewünschte Faktorisierung $Q = P_1 \cdot .. \cdot P_k$.
Ist $P \in H$ eine beliebige Hurwitz-Primzahl, so sind aufgrund der Multiplikativität der Norm die einzigen Faktorisierungen von $P$ in Hurwitz Quaternionen von der Form $P = (PU^{-1}) \cdot U$ und $P = V \cdot (V^{-1}P)$ mit $U, V \in H^*$. Hieraus folgt die Eindeutigkeit der Primfaktorzerlegung bis auf das Einfügen von Einheiten. □

**(3.13) Beispiel**
Sei $Q \in H$ primitiv mit $N(Q) = 100$. Dann gibt es bis auf das Einfügen von Einheiten nur $6 = \binom{4}{2}$ Faktorisierungen von $Q$ in Hurwitz-Primzahlen, basierend auf den Modellen

$$2 \cdot 2 \cdot 5 \cdot 5,\quad 2 \cdot 5 \cdot 2 \cdot 5,\quad 5 \cdot 2 \cdot 2 \cdot 5,\quad 5 \cdot 2 \cdot 5 \cdot 2,\quad 5 \cdot 5 \cdot 2 \cdot 2,\quad 2 \cdot 5 \cdot 5 \cdot 2.$$

Da die 24 Einheiten an 3 möglichen Stellen eingefügt werden können, ergeben sich insgesamt $24^3 \cdot 6 = 82944$ mögliche Faktorisierungen von $Q$.

Setzen wir keine Primitivität von $Q$ voraus, so können wir nicht so leicht von einer eindeutigen Faktorisierung reden, da es dann einige Faktorisierungsmöglichkeiten mehr gibt. Ist $p \in \mathbb{N}$ eine ungerade Primzahl, so gibt es mehr als $24 = |H^*|$ Elemente in $x \in H$ mit Norm $p$, was zu verschiedenen, nicht assoziierten Faktorisierungen $p = N(x) = x\bar{x}$ führt.

**(3.14) Lemma**
In $H$ gibt es 24 Elemente der Norm 2 und $24(p+1)$ Elemente mit Norm $p > 2$ für $p$ eine Primzahl.

**Beweis**
Für den Beweis greifen wir ein wenig voraus und verwenden die Bezeichnungen aus Kapitel (3.6). Es ist $H \cong \mathbb{D}_4$ bezüglich des mit 2 reskalierten Skalarprodukts (siehe Bemerkung (3.8)). Damit ist die Diskriminate der Algebra $\mathbb{H}$ gleich $2M = (2)$, das heißt $\mathbb{H}$ verzweigt nur an $(2)$; nach [Rei, Theorem (13.2)] besitzt $H$ daher nur ein ganzes Ideal der Norm 2, welches $24 = |H^*|$ Erzeuger hat. Ist $p > 2$ eine Primzahl, dann ist die Komplettierung $H_{(p)} \cong \mathbb{Z}_{(p)}^{2\times 2}$, da $H$ nicht an $(p) = pM$ verzweigt . Also ist $M/pM \cong \mathbb{F}_p^{2\times 2}$. Die maximalen Rechtsideale von $\mathbb{F}_p^{2\times 2}$ stehen bekanntlich in Bijektion zu den $p+1$ Geraden im $\mathbb{F}^{2\times 1}$. Damit folgt die Behauptung.

## 3.4 Euklidischer Algorithmus in ganzzahligen Oktaven

Man kann zeigen, dass es in den Oktaven $\mathbb{O}$ über $\mathbb{Q}$ sieben Maximalordnungen gibt, die zueinander isomorph sind. Wir fixieren für unsere Zwecke eine davon:

**(3.15) Definition**
$C := \{a_0 + a_1e_1 + a_2e_2 + a_3e_3 + a_4h + a_5(e_1h) + a_6(e_2h) + a_7(e_3h);\ a_0, .., a_7 \in \mathbb{Z}\}$ heißt Coxeters Menge der ganzzahligen Oktaven, wobei $h := \frac{1}{2}(e_1 + e_2 + e_3 - e_4)$.

Wir haben auf $C$ wie üblich die positiv definite Norm

$$N : C \to \mathbb{N}_0,\ N(z) := z\bar{z} = z_0^2 + z_1^2 + .. + z_7^2 \quad \text{für } z \in C.$$

Um auch in $C$ eine Division mit Rest zu bekommen und somit zu sehen, dass $C$ wirklich eine Maximalordnung in $\mathbb{O}$ ist, werden wir zuerst zeigen, dass $C$ mit dem Gitter $\mathbb{E}_8$ identifiziert werden kann. Dann werden wir eine bekannte Überdeckungseigenschaft von $\mathbb{E}_8$ nutzen.

**(3.16) Satz**
Coxeters Menge der ganzzahligen Oktaven $C$ ist, vesehen mit dem (nicht mit 2 reskalierten) Skalarprodukt $(u, v)_2 := N(u + v) - N(u) - N(v)$, isometrisch zum Gitter $\mathbb{E}_8$.

**Beweis**
Nach Definition ist

$$B := (1, e_1, e_2, e_3, h, e_1h, e_2h, e_3h)$$

eine $\mathbb{Z}$-Basis von $C$. Explizites Ausrechnen der letzten drei Basiselemente liefert:

$$e_1 h = \frac{1}{2}(-1 + e_2 + e_4 + e_7)$$

$$e_2 h = \frac{1}{2}(-1 - e_1 - e_4 + e_5)$$

$$e_3 h = \frac{1}{2}(-1 - e_5 - e_6 - e_7)$$

Bezeichne $S := (e_0, .., e_7)$ die Standardbasis des $\mathbb{Q}^8$, so erhalten wir folgende Basiswechselmatrix:

$${}^S Id^B = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & -\frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} \\ 0 & 1 & 0 & 0 & \frac{1}{2} & 0 & -\frac{1}{2} & 0 \\ 0 & 0 & 1 & 0 & \frac{1}{2} & \frac{1}{2} & 0 & 0 \\ 0 & 0 & 0 & 1 & \frac{1}{2} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -\frac{1}{2} & \frac{1}{2} & -\frac{1}{2} & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{2} & -\frac{1}{2} \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & -\frac{1}{2} \\ 0 & 0 & 0 & 0 & 0 & \frac{1}{2} & 0 & -\frac{1}{2} \end{pmatrix}$$

Nun gilt für die Grammatrix (bezüglich $(-|-)_2$)

$$\mathbb{G}(B) = ({}^S Id^B)^{tr} \cdot \mathbb{G}(S) \cdot {}^S Id^B = ({}^S Id^B)^{tr} \cdot 2 \cdot I_8 \cdot {}^S Id^B.$$

Ausgerechnet:

$$\mathbb{G}(B) = \begin{pmatrix} 2 & 0 & 0 & 0 & 0 & -1 & -1 & -1 \\ 0 & 2 & 0 & 0 & 1 & 0 & -1 & 0 \\ 0 & 0 & 2 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 2 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 2 & 0 & 0 & 0 \\ -1 & 0 & 1 & 0 & 0 & 2 & 0 & 0 \\ -1 & -1 & 0 & 0 & 0 & 0 & 2 & 0 \\ -1 & 0 & 0 & 0 & 0 & 0 & 0 & 2 \end{pmatrix}$$

Da $det(\mathbb{G}(B)) = 1$ ist, liegt offensichtlich ein ganzes, gerades, positiv definites und unimodulares Gitter im $\mathbb{R}^8$ vor. Mit Satz (2.2) folgt also, dass $C$ nur isometrisch zum Gitter $\mathbb{E}_8$ sein kann. □

**(3.17) Satz (vgl. [Con2])**
Die Überdeckungszahl des Gitters $\mathbb{E}_8$ beträgt $r = 1$.

Da wir im Beweis von Satz (3.16) das Skalarprodukt nicht mit 2 reskaliert haben, erhalten wir folgenden

**(3.18) Satz**
Für jedes $\lambda \in \mathbb{O}$ gibt es ein $\gamma \in C$, sodass

$$N(\lambda - \gamma) = (\lambda - \gamma | \lambda - \gamma) \leq \frac{1}{2}.$$

Aus diesem Satz folgt nun mit Lemma (2.20), dass $C$ euklidisch ist.

**(3.19) Korollar**
Sind $a, b \in C$ und $b \neq 0$, so gibt es $q, r, q', r' \in C$, sodass

$$a = qb + r \quad \text{und} \quad N(r) \leq \frac{1}{2}N(b),$$

$$a = bq' + r' \quad \text{und} \quad N(r') \leq \frac{1}{2}N(b).$$

Mithilfe der Division mit Rest können wir nun zeigen, dass die Definition von $C$ „richtig“ war.

**(3.20) Korollar**
$C =< 1, e_1, e_2, e_3 >_{\mathbb{Z}} \oplus < 1, e_1, e_2, e_3 >_{\mathbb{Z}} h$ mit $h = \frac{1}{2}(e_1 + e_2 + e_3 - e_4)$ ist eine Maximalordnung in $\mathbb{O}$.

**Beweis**
Dass $C$ multiplikativ abgschlossen ist, kann man durch leichte, ohne Computer jedoch längliche Rechnungen bestätigen. Somit ist $C$ eine Unteralgebra von $\mathbb{O}$ mit $1 \in C$.
Weiter ist $tr(a) = 2a_0 \in \mathbb{Z}$, sowie $N(a) \in \mathbb{Z}$, also ist $C$ als volles Gitter eine Ordnung in $\mathbb{O}$.
Dass $C$ auch eine Maximalordnung ist, folgt aus der Division mit Rest und Satz (2.21). □

Wir schauen uns noch ein wenig die Struktur der Maximalordnung $C$ an. Es gilt allgemein:

**(3.21) Lemma**
Sei $\mathcal{O}$ eine Ordnung in den Oktaven $\mathbb{O}$.

a) Für $m = \sum_{i=0}^{7} m_i e_i \in \mathcal{O}$ gilt, dass $2m_j \in \mathbb{Z}$ für alle $j \in \{0, .., 7\}$.

b) Die Koordinaten $m_i$ von $m \in \mathcal{O}$, die nicht in $\mathbb{Z}$ liegen, bilden das sogenannte *Halfing-Set* $H(m) := \{i \in \{0, .., 7\};\ m_i \in \frac{1}{2}\mathbb{Z} \setminus \mathbb{Z}\}$ von $m$ der Länge $|H(m)|$. Es gilt $4 | |H(m)|$ für alle $m \in \mathcal{O}$.

**Beweis**
a) Sei $m \in \mathcal{O}$ und $j \in \{0, .., 7\}$. Dann ist $tr((\sum_{i=0}^{7} m_i e_i)e_j) = \pm 2m_j \in \mathbb{Z}$ nach der Definition einer Ordnung.

b) Es ist $N(m) = m_0^2 + .. + m_7^2 \equiv \frac{|H(m)|}{4} \pmod 1$. Wegen $N(m) \in \mathbb{Z}$ gilt also $4 | |H(m)|$. □

Für unsere feste Maximalordnung $C \subset \mathbb{O}$ erhalten wir speziell folgendes

**(3.22) Lemma**
Es bezeichne $H(C) = \{H(m);\ m \in C\}$ die Menge aller möglichen Halfing-Sets von Elementen in $C$. Dann besteht $H(C)$ aus 14 Mengen der Länge 4:

$$\{1,2,3,4\},\quad \{0,2,4,7\},\quad \{0,1,4,5\},\quad \{0,2,3,5\},\quad \{0,1,3,7\},\quad \{1,2,5,7\},\quad \{0,1,2,6\},$$

$$\{0,5,6,7\},\quad \{1,3,5,6\},\quad \{2,3,6,7\},\quad \{1,4,6,7\},\quad \{2,4,5,6\},\quad \{0,3,4,6\},\quad \{3,4,5,7\},$$

einer Menge der Länge 8: $\{0,1,2,3,4,5,6,7\}$ und einer Menge der Länge 0: $\emptyset$.

**Beweis**
Man starte mit den Basiselemten $h, e_1h, e_2h, e_3h \in C$ und bilde sukzessive alle möglichen Linearkombinationen mit Koeffizienten in $\{0,1\}$. Zum Beispiel müssen jeweils die Komplemente der errechneten Halfing-Sets wieder Halfing-Sets sein, da $h + e_3h = 1/2 + 1/2e_1 + .. + 1/2e_7 \in C$. Die Komplemente stehen in der obigen Liste jeweils übereinander. Durch leichte Rechnungen sieht man, dass dies alle Halfing-Sets sind. □

**(3.23) Bemerkung**
Gilt $m \in \frac{1}{2}\langle e_0, .., e_7\rangle_{\mathbb{Z}}$ und $H(m) \in H(C)$, so gibt es ein $n \in C$, sodass $H(m) = H(n)$. Daraus folgt $m - n \in \langle e_0, .., e_7\rangle_{\mathbb{Z}} \subset C$ und somit $m \in C$.

Die Begriffe *Primoktave*, *Modell*, sowie *Primitivität* seien in $C$ analog definiert wie in $H$ (siehe Definition (3.10)). Es stellt sich die folgende Aufgabe:
Falls $p|N(\alpha)$ für ein primitives $\alpha \in C$ und eine Primzahl $p$, so finde die Linksteiler $\pi|\alpha$ von $\alpha$ mit $N(\pi) = p$.
Man beachte dass wegen $\overline{C} = C$ die Konjugation zu einer „Links-Rechts-Dualität“ führt, das heißt jede Aussage über Linksteiler liefert eine duale Aussage über Rechtsteiler.

Betrachten wir dazu zunächst die Einheiten und die Elmente mit Norm 2 in $C$ (die Anzahl dieser benötigen wir später bei der Primfaktorisierung):

**(3.24) Lemma**
Es gibt 240 Einheiten in $C$, das heißt

$$\left|C^\times\right| = \left|\{\epsilon \in C;\ \epsilon^{-1} \in C\}\right| = |\{\epsilon \in C;\ N(\epsilon) = 1\}| = 240.$$

Es gibt 2160 Elemente mit Norm 2 in $C$.

**Beweis**
Es ist bekannt (siehe [Con2]), dass es in $\mathbb{E}_8$ genau 240 Wurzeln gibt. Folglich gibt es nach Satz (3.16) auch genau 240 Elemente in $C$ mit Norm 1.
Wir können die Elemente mit Norm 1 auch leicht kombinatorisch mit Lemma (3.22) und Bemerkung (3.23) abzählen: Sei $a \in C$ mit $N(a) = a_0^2 + .. + a_7^2 = 1$. Es ist $|H(a)| \neq 8$, denn sonst wäre $N(a) \geq 2$. Ist $|H(a)| = 4$, dann sind genau vier Koordinaten von $a$ gleich $\pm\frac{1}{2}$

und die restlichen Koordinaten 0, also gibt es $14 \cdot 2^4 = 224$ Möglichkeiten für ein $a \in C^*$ mit $|H(a)| = 0$, da es 14 Halfing-Sets mit Länge 4 gibt. Ist $|H(a)| = 0$, so ist eine Koordinate von $a$ gleich $\pm 1$ und die restlichen Koordinaten 0, also gibt es hier $2 \cdot 8 = 16$ Möglichkeiten. Insgesamt gibt es somit $0 + 16 + 224 = 240$ Elemente mit Norm 1 in $C$.
Sei nun $a \in C$ mit $N(a) = 2$. Ist $|H(a)| = 8$, so sind alle Koordinaten von $a$ gleich $\pm\frac{1}{2}$, also gibt es dann $2^8 = 256$ Möglichkeiten. Ist $|H(a)| = 4$, so sind vier Koordinaten gleich $\pm\frac{1}{2}$, eine Koordinate gleich $\pm 1$ und die restlichen Koordinaten 0, was $14 \cdot 2^4 \cdot \binom{4}{1} \cdot 2 = 1792$ Möglichkeiten ergibt. Ist schließlich $|H(a)| = 0$, so sind zwei Koordinaten gleich $\pm 1$ und die restlichen Koordinaten 0, also gibt es hier $\binom{8}{2} \cdot 2^2 = 112$ Möglichkeiten, insgesamt also $256 + 1792 + 112 = 2160$ Elemente mit Norm 2 in $C$. □

In manchen Fällen erweist es sich als sinnvoll, $C$ „modulo 2“ zu betrachten. Dazu zunächst eine

**(3.25) Bemerkung**
Für $p$ eine Primzahl sei $\overline{C} := C/pC$. Man rechnet schnell nach, dass $\overline{C}$ eine normierte Algebra ist mit der wohldefinierten, multiplikativen quadratischer Form

$$\overline{B} : \overline{C} \to \mathbb{F}_p, \quad \overline{N}(\overline{a}) := \overline{N(a)}.$$

Wir wollen uns im Fall $p = 2$ die Einheiten von $\overline{C}$ ansehen.

**(3.26) Lemma**
Es gilt $|(C/2C)^*| = \left|\{\bar{c} \in C/2C;\ \overline{N}(\bar{c}) = 1\}\right| = 120$.

**Beweis**
Wir identifizieren nach Satz (3.16) $C/2C$ mit $\mathbb{E}_8/2\mathbb{E}_8$. Ist nun V ein Vertretersystem der $2^8 = 256$ Äquivalenzklassen in $\mathbb{E}_8/2\mathbb{E}_8$, so kann man (beispielsweise mit Magma [Bos]) sehen, dass es genau 120 Vertretern gibt, deren Norm nicht in $4\mathbb{Z}$ liegt. Durch die Reskalierung mit 2 (siehe oben) erhalten wir also genau 120 Klassen in $C/2C$, deren Norm nicht in $2\mathbb{Z}$ liegt, das heißt es gilt $|(C/2C)^*| = 120$.

Wie oben schon erwähnt, terminiert der bekannte Euklidische Algorithmus (27) mit Startwerten $a$ und $b$ nicht zwangsläufig zu einem gemeinsamen Rechts- bzw. Linksteiler von $a$ und $b$. Denn es gibt Beispiele $a = a_0\pi$, $b = b_0\pi$ mit $a_0, b_0, \pi \in C$, $N(\pi) = 11$, bei dem der Algorithmus bei einem Element $r_n$ mit $N(r_n) = 1$ stoppt, während er für andere $a_0, b_0$ bei einem $r_n$ mit $N(r_n) = 11$ terminiert, aber $r_n$ ist weder Rechtsteiler von $a$ noch von $b$.
Dass solch ein Verhalten auftreten kann, liegt daran, dass wir von $a = qb + r$ nicht auf $r = r_0\pi$ für ein $r_0 \in C$ schließen können. Denn

$$r = a - qb = a_0\pi - q(b_0\pi) \overset{(*)}{=} a_0\pi - (qb_0)\pi = (a_0 - qb_0)\pi$$

ist im Allgemeinen keine gültige Rechnung, da $C$ nicht assoziativ ist und somit in $(*)$ nicht zwangsläufig Gleichheit gilt.

Hans Peter Rehm veröffentlichte jedoch im Jahre 1993 einen erweiterten Euklidischen Algorithmus, der dieses Problem umgeht. Der Algorithmus wird im Beweis des folgenden Satzes beschrieben.

**(3.27) Satz**
Sei $0 \neq \alpha \in C$, $m \in \mathbb{N}$, sodass $m|N(\alpha)$. Dann gibt es mindestens 240 Linksteiler (und 240 Rechtsteiler) $\mu$ von $\alpha$ mit $N(\mu) = m$.

**Beweis**
Starte mit $\rho_1 := \alpha$, $m_0 := m$, $m_1 := N(\alpha)/m$, sodass also $N(\rho_1) = m_0 m_1$.
Wähle nach Korollar (3.19) im ersten Schritt $\gamma_1, \rho_2 \in C$ so, dass

$$\rho_1 = \gamma_1 m_1 + \overline{\rho_2} \text{ und } N(\overline{\rho_2}) \leq \frac{1}{2} N(m_1) = \frac{1}{2} m_1^2,$$

wobei wir hier aus einem technischen Grund den Rest $\rho_2$ konjugieren.
Nun gilt

$$N(\overline{\rho_2}) = N(\rho_2) = N(\rho_1 - \gamma_1 m_1) = N(\rho_1) - 2\,(\rho_1|\,\gamma_1 m_1) + N(\gamma_1 m_1)$$

$$= m_0 m_1 - 2m_1\,(\rho_1|\,\gamma_1) + m_1^2 N(\gamma_1) \equiv 0 \mod m_1.$$

Also gibt es ein $m_2 \in \mathbb{N}$ mit $N(\rho_2) = m_1 m_2$.
Weiter gilt $m_2 < m_1$, denn $m_1 m_2 = N(\rho_1) \leq \frac{1}{2} m_1^2$ also $m_2 \leq \frac{1}{2} m_1 < m_1$.
Falls $m_2 > 0$, können wir mit den gleichen Argumenten $\rho_3, m_3$ finden mit $N(\rho_2) = m_2 m_3$ und $m_3 < m_2$. Dies wiederholen wir solange, bis wir $m_{N+1} = 0$ erreichen für ein $N \in \mathbb{N}$, denn die positiven ganzzahligen $m_i$ werden bei jedem Schritt strikt kleiner und müssen somit irgendwann 0 werden.
Wir bekommen also folgendes Schema, welches wir den *Vorwärtsschritt* des Algorithmus von Rehm nennen wollen:

| | | |
|---|---|---|
| $\rho_1 = \gamma_1 m_1 + \overline{\rho_2}$ | $N(\rho_1) = m_0 m_1$ | |
| $\rho_2 = \gamma_2 m_2 + \overline{\rho_3}$ | $N(\rho_2) = m_1 m_2$ | $m_1 > m_2$ |
| ... | ... | ... |
| $\rho_{N-1} = \gamma_{N-1} m_{N-1} + \overline{\rho_N}$ | $N(\rho_{N-1}) = m_{N-2} m_{N-1}$ | $m_{N-2} > m_{N-1}$ |
| $\rho_N = \gamma_N m_N + 0$ | $N(\rho_N) = m_{N-1} m_N$ | $m_{N-1} > m_N > 0$ |

Nun kommen wir zum sogenannten *Rückwärtsschritt*.
Sei $\mu_N \in C$ mit $N(\mu_N) = m_N$. Ein solches $\mu_N$ existiert, denn nach dem Vier-Quadrate-Satz von Lagrange kann jede natürliche Zahl als Summe von vier Quadratzahlen (und somit erst recht von acht) dargestellt werden. Nach Lemma (3.24) gibt es mindestens 240 verschiedene $\lambda \in C$, sodass $N(\lambda) = m_N$.
Es gilt mit dem Satz von Artin

$$\rho_N = \gamma_N m_N = \gamma_N(\mu_N \overline{\mu_N}) = \underbrace{(\gamma_N \mu_N)}_{=:\mu_{N-1}} \overline{\mu_N}$$

Setze $\mu_{N-1} := \gamma_N \mu_N$, dann ist $\mu_{N-1}$ Linksteiler von $\rho_N$ mit $N(\mu_{N-1}) = m_{N-1}$, da ja $N(\rho_N) = m_{N-1}m_N$. Weiter ist $\overline{\mu_{N-1}}$ Rechtsteiler von $\overline{p_N} = \overline{\mu_{N-1}\overline{\mu_N}} = \mu_N\overline{\mu_{N-1}}$ und von $m_{N-1} = \mu_{N-1}\overline{\mu_{N-1}}$. Also ist $\overline{\mu_{N-1}}$ auch Rechtsteiler von $\rho_{N-1}$, da mit dem Satz von Artin

$$\rho_{N-1} = \gamma_{N-1}m_{N-1} + \overline{p_N} = (\gamma_{N-1}\mu_{N-1})\overline{\mu_{N-1}} + \mu_N\overline{\mu_{N-1}} = \underbrace{(\gamma_{N-1}\mu_{N-1} + \mu_N)}_{=:\mu_{N-2}}\overline{\mu_{N-1}}.$$

Setze also weiter $\mu_{N-2} := \gamma_{N-1}\mu_{N-1} + \mu_N$, so erhalten wir einen Linksteiler von $p_{N-1}$ mit Norm $N(\mu_{N-2}) = m_{N-2}$. Mit diesen Setzungen fährt man nun fort, bis wir einen Linksteiler $\mu_0$ von $\rho_1 = \alpha$ mit Norm $m = m_0$ und einen korrespondierenden Rechtsteiler $\overline{\mu_1}$ mit Norm $m_1$ erhalten.
Zusammengefasst sieht der *Rückwärtsschritt* also wie folgt aus:

| | | |
|---|---|---|
| | | $N(\mu_N) = m_N$ |
| $\rho_N = \mu_{N-1}\overline{\mu_N}$ | $\mu_{N-1} = \gamma_N\mu_N$ | $N(\mu_{N-1}) = m_{N-1}$ |
| $\rho_{N-1} = \mu_{N-2}\overline{\mu_{N-1}}$ | $\mu_{N-2} = \gamma_{N-1}\mu_{N-1} + \mu_N$ | $N(\mu_{N-2}) = m_{N-2}$ |
| ... | ... | ... |
| $\rho_2 = \mu_1\overline{\mu_2}$ | $\mu_1 = \gamma_2\mu_2 + \mu_3$ | $N(\mu_1) = m_1$ |
| $\rho_1 = \mu_0\overline{\mu_1}$ | $\mu_0 = \gamma_1\mu_1 + \mu_2$ | $N(\mu_0) = m_0$ |

Beachte, dass wir wegen $\rho_i = \mu_{i-1}\overline{\mu_i}$ für die mindestens 240 möglichen Wahlen von $\mu_N$ auch 240 verschiedene Linksteiler $\mu_0$ und 240 verschiedene Rechtsteiler $\overline{\mu_1}$ von $\alpha$ bekommen. □

Falls $m_N > 1$ gibt es sogar mehr als 240 Rechts- und Linksteiler von $\alpha$ mit Norm $m$. Man kann jedoch zeigen, dass es genau 240 Rechts- und Linksteiler gibt, falls $\alpha$ primitiv und $m = p$ eine ungerade Primzahl ist oder falls $m$ und $N(\alpha)/m$ teilerfremd sind (siehe [Rehm]). Dann muss der Vorwärtsschritt des Algorithmus also bei $m_N = 1$ terminieren. So können wir unsere Aufgabe, alle primen Rechts- bzw. Linksteiler eines primitiven $\alpha$ zu bestimmen, effizient lösen, indem wir eine Tabelle der 240 Einheiten von $C$ nehmen und so Gleichungen vom Typ $N(\lambda) = l$ für $l > 1$ nicht lösen müssen (dies ist eine nichttriviale, sehr rechenintensive Aufgabe, deren Aufwand exponentiell in $l$ ist).
Diese Aussage habe ich beim Programmieren der eindeutigen Primfaktorzerlegung verwendet; dort werden aufgrund der vorausgesetzten Primitivität die Voraussetzungen erfüllt sein.

Wir haben also gesehen, dass auch $C$ gewissermaßen einen euklidischen Bereich bildet, wobei der euklidische Algorithmus an die Nichtassoziativität von $C$ angepasst werden muss.

## 3.5 Primfaktorzerlegung in ganzzahligen Oktaven

Aus Satz (3.27) folgt nun mit vollständiger Induktion unmittelbar die Existenz einer „Primoktavenzerlegung“ zu einem gegebenem ganzzahligen Oktaven $\alpha \in C$ und einem vorgegebenem Modell.

**(3.28) Satz**
Sei $\alpha \in C$ mit Modell $N(\alpha) = p_1 \cdot .. \cdot p_n$, mit $p_1, .., p_n \in \mathbb{N}$ Primzahlen.
Dann gibt es $P_1, ..., P_n \in C$ mit $N(P_1) = p_1, .., N(P_n) = p_n$, sodass

$$\alpha = P_1(P_2(..(P_{n-1}P_n)..)).$$

Von Eindeutigkeit der Faktorisierung im Sinne von Satz (3.12) kann jedoch nicht die Rede sein, denn andere Klamnmerungen in der Primfaktorzerlegung der Norm $N(\alpha) = p_1 \cdot .. \cdot p_n$ liefern aufgrund der fehlenden Assoziativität im Allgemeinen verschiedene Faktorisierungen von $\alpha$.

**(3.29) Beispiel**
Sei $\alpha \in C$ mit $N(\alpha) = 100 = 2 \cdot 2 \cdot 5 \cdot 5$. Dann gibt es nach Beispiel (3.13) 6 Modelle von $\alpha$ und bei jedem Modell gibt es 5 Möglichkeiten der Klammerung, zum Beispiel:

$$100 = ((2 \cdot 2)5)5 = (2(2 \cdot 5))5 = 2((2 \cdot 5)5) = 2(2(5 \cdot 5)) = (2 \cdot 2)(5 \cdot 5),$$

also insgesamt $5 \cdot 6 = 30$ Faktorisierungen von $N(\alpha)$, die zu verschiedenen Faktorisierungen von $\alpha$ führen.

Des Weiteren können wir auch durch das Einfügen von Einheiten verschiedene Faktorisierungen bekommen, denn im Allgemeinen gilt nicht $(P_1u)(u^{-1}P_2) = P_1P_2$ für eine Einheit $u \in C^*$. Stellt man jedoch zusätzliche Bedingungen an die Primoktaven in der Faktorisierung, so erhält man diesbezüglich eine Eindeutigkeit der Zerlegung. Dazu zunächst ein paar Lemmata:

**(3.30) Lemma**
Seien $\tau, \tau', \mu, \mu' \in C \setminus \{0\}$ mit $\alpha = \mu\tau = \mu'\tau'$, $N(\mu) = N(\mu')$ ungerade, sowie $N(\tau)$ und $N(\mu)$ teilerfremd.
Ist $\mu \equiv \mu'$ mod 2 (das heißt $\mu - \mu' \in 2C$), so folgt $\mu = \mu'$ oder $\mu = -\mu'$.

**Beweis**
Angenommen es ist $\mu \equiv \mu'$ mod 2, aber $\mu \neq \mu'$ und $\mu \neq -\mu'$ (also auch $\tau \neq \tau'$). Dann gilt mir der Cauchy-Schwarz-Ungleichung

$$\left|\left(\mu \middle| \mu'\right)\right| < |\mu| \left|\mu'\right| = \sqrt{N(\mu)}\sqrt{N(\mu')} = N(\mu)$$

wobei $|\mu| := \sqrt{N(\mu)}$ den gewöhnlichen euklidischen Betrag bezeichne. Damit ist

$$N(\mu' - \mu) = N(\mu') - 2\left(\mu' \middle| \mu\right) + N(\mu) = 2(N(\mu) - \left(\mu' \middle| \mu\right)) \leq 2(N(\mu) + \left|\left(\mu' \middle| \mu\right)\right|) < 4 \cdot N(\mu).$$

Also gilt für $\gamma := \frac{1}{2}(\mu' - \mu) \in C$ (beachte $\mu' - \mu \in 2C$), dass $0 < N(\gamma) < N(\mu)$.
Weiter gilt $\mu\tau = \mu'\tau' = (2\gamma + \mu)\tau'$, also

$$\mu(\tau - \tau') = \gamma(2\tau'). \tag{28}$$

Einerseits folgt daraus $4 \cdot N(\tau') = N(2\tau') \mid N(\mu)N(\tau - \tau')$, da $N(\gamma) \in \mathbb{Z}$. Weil $N(\mu)$ ungerade und teilerfremd zu $N(\tau')$ ist, gilt $N(2\tau') \mid N(\tau - \tau')$.
Andererseits folgt aber aus (28) auch

$$N(\mu)N(\tau - \tau') = N(\gamma)N(2\tau') < N(\mu)N(2\tau'),$$

also $N(\tau - \tau') < N(2\tau')$ im Widerspruch zu $N(2\tau')|N(\tau - \tau')$ und $N(\tau - \tau') > 0$. □

Um nur eine der beiden Möglichkeiten $\mu = \mu'$ und $\mu = -\mu'$ für die Faktorisierung von $\alpha$ zuzulassen, versehen wir $C$ mit der bekannten lexikographischen Ordnung bezüglich Coxeters $\mathbb{Z}$-Basis $(f_0, .., f_7) := (1, e_1, e_2, e_3, h, e_1h, e_2h, e_3h)$, das heißt für $s = \sum_{i=0}^{7} s_i f_i, t = \sum_{i=0}^{7} t_i f_i \in C$ gelte

$$s < t \Leftrightarrow \exists\, k \in \{0, .., 7\} :\ s_k < t_k \text{ und } s_j = t_j \ \ \forall j \in \mathbb{Z} \text{ mit } 0 \leq j < k.$$

**(3.31) Korollar**
Sei $\alpha \in C$ mit $N(\alpha) = mu$, $m$ ungerade und $m, u \in \mathbb{N}$ teilerfremd. Dann gibt es genau 240 Linksteiler $\mu \in C$ von $\alpha$ mit $N(\mu) = m$, wobei es genau einen Linksteiler $\mu \in C$ gibt mit $\mu \equiv 1 \pmod 2$ und $\mu > 0$ ist.

**Beweis**
Zerlege die Menge $M := \{\mu \in C;\ N(\mu) = m,\ \mu|\alpha\}$ in Klassen mod 2. Nach Lemma (3.30) enthält jede Klasse zwei Elemente und nach Satz (3.27) gilt $|M| \geq 240$, also enthält $M$ mindestens 120 solche Klassen.
Da $m$ ungerade ist, gilt $N(\mu) \equiv 1 \pmod 2$, folglich gilt für jede Äquivalenzklasse $\bar{\mu} \in (C/2C)^*$. Nach Lemma (3.26) ist $|(C/2C)^*| = 120$, das heißt es existieren genau 120 Klassen, also $\{\bar{\mu};\ \mu \in M\} = (C/2C)^*$.
Somit gibt es genau 240 Linksteiler $\mu \in C$ mit $N(\mu) = m$. Weiter hat $\bar{1} = \bar{\mu}$ eine Lösung $\mu$ in $M$, welche durch die Forderung $\mu > 0$ nach Lemma (3.30) eindeutig ist. □

**(3.32) Korollar**
Seien $\alpha \in C$ mit $N(\alpha) = 2^{r_0} \cdot p_1^{r_1} \cdot .. \cdot p_n^{r_n}$, $2 = p_0 < p_1 < .. < p_n$ Primzahlen und $r_0, .., r_n \in \mathbb{N}_0$. Dann gibt es genau ein Tupel $(P_0, .., P_n) \in C^{n+1}$, sodass

a) $\alpha = P_0(P_1(..(P_{n-1}P_n)..))$

b) $N(P_i) = p_i^{r_i}$ für $i = 0, .., n$

c) $P_i \equiv 1 \bmod 2$ für $i = 1, .., n$ und

d) $P_i > 0$ für $i = 1, .., n$.

Fassen wir in der Primfaktorzerlegung von $N(\alpha)$ also gleiche Faktoren zusammen, so bekommen wir eine dazugehörige, im Sinne von Korollar (3.32) eindeutige Faktorisierung von $\alpha$ in ganzzahlige Oktaven. Diese Faktorisierung ist natürlich nur dann eine Primfaktorzerlegung von $\alpha$, falls $r_i \leq 1$ für $i = 0, .., n$.
Um auch in den restlichen Fällen etwas über die Eindeutigkeit der Primfaktorzerlegung in $C$ aussagen zu können, benötigen wir folgende Erweiterung von Lemma (3.30).

**(3.33) Lemma**
Seien $p$ eine ungerade Primzahl, $\alpha \in C$ mit $p|N(\alpha)$ und $p$ kein Teiler von $\alpha$. Seien weiter $\tau, \tau', \mu, \mu' \in C$ mit $\alpha = \mu\tau = \mu'\tau'$ und $N(\mu) = N(\mu') = p$.
Ist $\mu \equiv \mu' \bmod 2$, so folgt $\mu = \mu'$ oder $\mu = -\mu'$.

**Beweis**
Nach Korollar (3.19) gibt es $q, r \in C$ mit $\alpha = pq + r$ und $0 \neq N(r) \leq \frac{1}{2}N(p) = \frac{1}{2}p^2$.
Da $p|N(\alpha) = N(pq + r) = p^2N(q) + 2p\,(q|\,r) + N(r)$, folgt $p|N(r)$, also $pl = N(r) \leq \frac{1}{2}p^2$ für ein $l \in \mathbb{N}$. Aus $l \leq \frac{1}{2}p$ folgt nun, dass $l$ und $p$ teilerfremd sind. Also können wir Lemma (3.30) anwenden um $r$ zu faktorisieren. Die Linksteiler $\mu$ von $\alpha$ und $r$ mit Norm $p$ sind aber identisch: Denn falls $r = \mu\sigma$ für ein $\sigma \in C$ und $N(\mu) = \mu\bar{\mu} = p$, so gilt mit dem Satz von Artin $\alpha = pq + r = (\mu\bar{\mu})q + \mu\sigma = \mu(\bar{\mu}q + \sigma)$, also ist $\mu$ auch Linksteiler von $\alpha$. Analog folgt die umgekehrte Richtung und damit die Behauptung. □

Analog zu Korollar (3.32) erhalten wir nun folgendes Korollar.

**(3.34) Korollar**
Sei $p$ eine ungerade Primzahl, $\alpha \in C$ mit $p|N(\alpha)$ und $p$ teilt nicht $\alpha$.
Dann gibt es genau 240 Linksteiler $\pi \in C$ von $\alpha$ mit $N(\pi) = p$, wobei es genau einen Linksteiler $\pi$ gibt, der $\pi \equiv 1 \bmod 2$ und $\pi > 0$ erfüllt.

Jetzt fehlt nur noch der Fall $p = 2$:

**(3.35) Lemma**
Ist $p > 2$ eine Primzahl, so definiere $X(p) := \{P \in C;\ N(P) = p,\ P > 0,\ P \equiv 1 \bmod 2\}$.
Im Fall $p = 2$ definiere $X(2) := \{\pi_1, .., \pi_9\}$ mit

$\pi_1 = (1,1,0,0,0,0,0,0)$, $\pi_2 = \frac{1}{2}(2,1,1,1,1,0,0,0)$, $\pi_3 = \frac{1}{2}(2,1,1,1,-1,0,0,0)$,
$\pi_4 = \frac{1}{2}(2,1,1,0,0,1,0,1)$, $\pi_5 = \frac{1}{2}(2,1,1,0,0,1,0,-1)$, $\pi_6 = \frac{1}{2}(2,1,0,1,0,1,1,0)$,
$\pi_7 = \frac{1}{2}(2,1,0,1,0,1,-1,0)$, $\pi_8 = \frac{1}{2}(1,2,1,1,0,1,0,0)$, $\pi_9 = \frac{1}{2}(1,2,-1,-1,0,-1,0,0)$.

Ist nun $\alpha \in C$ primitiv mit $p|N(\alpha)$, dann gibt es genau einen Linksteiler $P$ von $\alpha$ in $X(p)$.

**Beweis**
Sei $p = 2$. Dann existieren $q, r \in C$, sodass $\alpha = 2q + r$ und $N(r) \leq \frac{1}{2}N(2) = 2$.
Wegen $N(\alpha) = N(2q + r) = 4N(q) + 2\,(2q|\,r) + N(r)$ folgt aus $2|N(\alpha)$ auch $2|N(r)$. Da $\alpha$ primitiv ist, ist $r \neq 0$, also folgt $N(r) = 2$.
Man kann nun mithilfe eines Computeralgebrasystems (zum Beispiel mit Magma) sehen, dass alle Primoktaven $\tau \in C$ mit Norm 2 darstellbar sind durch genau ein $u \in C^*$ und genau ein $\rho \in X(p)$, sodass $\tau = \rho u$. Denn nach Lemma (3.24) gibt es genau 240 Einheiten und 2160 Elemente mit Norm 2 in C, sodass es ausreicht, alle möglichen $240 \cdot 8 = 2160$ Produkte $\rho u$ mit $u \in C^*, \rho \in X(p)$ auszurechnen und nachzuprüfen, dass diese paarweise verschieden sind.
Wir haben oben schon gesehen, dass die Linksteiler $\pi$ mit $N(\pi) = p$ von $\alpha$ und $r$ übereinstimmen, sodass die Behauptung im Fall $p = 2$ folgt.
Für $p > 2$ gilt die Aussage nach Lamma (3.34). □

Mit vollständiger Induktion erhalten wir nun einen Eindeutigkeitssatz für die Primfaktorzerlegung von ganzzahligen, primitiven Oktaven.

**(3.36) Satz**
Sei $\alpha \in C$ primitiv mit $N(\alpha) = p_1 \cdot .. \cdot p_n$ mit (nicht notwendigerweise verschiedenen) Primzahlen $p_1, .., p_n \in \mathbb{N}$.
Dann gibt es eine Einheit $P_0 \in C^*$ und Primoktaven $P_i \in X(p_i)$, sodass

$$\alpha = P_0(P_1(..(P_{n-1}P_n)..)),$$

wobei das Tupel $(P_0, .., P_n) \in C^{n+1}$ eindeutig ist.

## 3.6 Euklidische Quaternionenalgebren über quadratischen Zahlkörpern

Bisher haben wir die Algebren des Cayley-Dickson-Prozesses im Fall $K = \mathbb{Q}$ und $N(i_j) = 1$ untersucht. Nun wollen wir als Grundkörper nicht mehr die rationalen Zahlen $\mathbb{Q}$ betrachten, sondern quadratische Zahlkörper $K := \mathbb{Q}(\sqrt{d})$.
Wir behandeln in diesem Abschnitt Quaternionenalgebren

$$A := (\frac{-1, -1}{\mathbb{Q}(\sqrt{d})})$$

für $d \in \{2, 5, 13\}$. In diesen Fällen können wir mit einer ähnlichen Argumentation wie in den ganzzahligen Oktaven mithilfe des Gitters $\mathbb{E}_8$ zeigen, dass Maximalordnungen in diesen Algebren euklidisch sind.

Zunächst wird erläutert, warum wir gerade diese Quaternionenalgebren betrachten. Dabei ist vor allem das Verzweigungsverhalten von Quaternionenalgebren entscheidend.

**(3.37) Definition**
Sei $A$ eine Quaternionenalgebra über dem algebraischen Zahlkörper $K$ und $M$ eine Maximalordnung in $A$.

a) Sei $\mathfrak{p}$ ein Primideal von $\mathbb{Z}_K$ oder aber eine Einbettung von $K$ nach $\mathbb{C}$. Dann bezeichne $K_\mathfrak{p}$ die Komplettierung von $K$ an $\mathfrak{p}$. Man sagt, $A$ verzweigt an $\mathfrak{p}$, falls $A_\mathfrak{p} := A \otimes_K K_\mathfrak{p}$ ein Schiefkörper ist.

b) $A$ heißt total definit, falls $A$ an allen Einbettungen von $K$ nach $\mathbb{C}$ verzweigt.

c) Es bezeichne $M^\# = \{x \in A;\ tr(xM) \subseteq Z_K\}$ das zu $M$ bezüglich $tr$ duale $\mathbb{Z}_K$-Gitter.

d) Sei $d_A^{-1}$ das von $\{N(x);\ x \in M^\#\}$ erzeugte gebrochene Ideal in $K$. Dann heißt $d_A$ die Diskriminante von $A$.

**(3.38) Bemerkung**

a) Nach dem bekannten Wedderburnschen Struktursatz gilt für eine beliebige zentraleinfache Algebra $A$, dass es eine eindeutige natürliche Zahl $n \in \mathbb{N}$ und einen Schiefkörper $D$ gibt, sodass $A \cong D^{n\times n}$. Man kann zeigen, dass jede Quaternionenalgebra $A$ zentraleinfach ist, also erhält man aus $4 = \dim_K A = k^2 \dim_K D$, dass entweder $k = 1$ und $A \cong D$ ein Schiefkörper ist, oder dass $k = 2$ und $A \cong K^{2\times 2}$ ist.

b) Ist $A$ total definit, so muss $K$ total reell sein, da $\mathbb{C}$ als algebraisch abgeschlossener Körper keine echten Schiefkörpererweiterungen besitzt.

c) Es ist $A$ genau dann definit, wenn $A \times A \to \mathbb{Q}, (x, y) \mapsto Tr_{K|\mathbb{Q}}(x\bar{y})$ positiv definit ist (Eichlers Normsatz, [Rei, Theorem 34.8]).

Um positiv definite Gitter benutzen zu können, beschränken wir uns hier auf Quaternionenalgebren über reell-quadratischen Zahlkörper.

**(3.39) Satz**

Sei $A$ eine Quaternionenalgebra über einen Zahlkörper $K$. Dann gilt

1. Es ist $d_A$ das Produkt der Primideale von $\mathbb{Z}_K$, an welchen $A$ verzweigt. Insbesondere ist $d_A$ wohldefiniert.
2. Sei $A'$ eine weitere Quaternionenalgebra über $K$. Sind $A$ und $A'$ beide positiv definit, so sind $A$ und $A'$ genau dann isomorphe $K$-Algebren, wenn $d_A = d_{A'}$ gilt.

**Beweis**

Siehe [Rei, Theorem 25.2 und Corollary 25.10] für (a).
Nach [Rei, Theorem 32.11] sind $A$ und $A'$ genau dann isomorph, wenn $A_\mathfrak{p}$ und $A'_\mathfrak{p}$ isomorph sind für alle Primideale und Einbettungen $\mathfrak{p}$. Da $A$ und $A'$ beide total definit sind, sind sie also genau dann isomorph, wenn sie an den selben Primidealen verzweigen, sodass (b) aus (a) folgt. □

**(3.40) Korollar**

Sei $A$ eine Quaternionenalgebra über dem algebraischen Zahlkörper $K$. Weiter sei $M$ eine Maximalordnung in $A$. Dann gilt $M^\# = M$ genau dann, wenn $d_A = \mathbb{Z}_K$ ist.

**Beweis**

Es ist $M \subseteq M^\#$ stets. Weiter ist der Index $[M^\# : M]$ (als abelsche Gruppen) gerade $N_{K|\mathbb{Q}}(d_A^2) := [\mathbb{Z}_K : d_A^2]$ (vgl. [Rei, Theorems 24.9 und 24.11]). □

Sei jetzt $A$ eine total definite Quaternionenalgebra über dem quadratischen Zahlkörper $K = \mathbb{Q}(\sqrt{d})$. Nach Bemerkung (3.38)(b) ist $d > 1$ quadratfrei. Damit eine (Maximal-)Ordnung $M$ in $A$ euklidisch ist, muss jedes Rechtsideal von $M$ ein Rechtshauptideal sein. In [KV] wurde gezeigt, daß es nur 13 solche Ordnungen gibt (bis auf Isomorphie). Diese sind gegeben durch

| $d$ | 2 | 5 | 13 | 17 |
|---|---|---|---|---|
| $N_{K\|\mathbb{Q}}(d_A)$ | 1 | 1 | 1 | 1 |
| | 14 | 20 | 12 | |
| | 14 | 44 | 12 | |
| | 18 | 44 | | |
| | 50 | | | |

Dabei bezeichne $A$ die Quaternionenalgebra über $K = \mathbb{Q}(\sqrt{d})$ und $N_{K|\mathbb{Q}}(d_A)$ die Norm der Diskriminante von $A$. Bei mehrfach vorkommenden Werte von $N_{K|\mathbb{Q}}(d_A)$ verzweigt $A$ an verschiedenen Primidealen. Wir werden zeigen, dass Maximalordnungen in $A$ mit $d \in \{2, 5, 13\}$ und $N_{K|\mathbb{Q}}(d_A) = 1$ euklidisch sind. In diesen Fällen gilt $A = (\frac{-1,-1}{\mathbb{Q}(\sqrt{d})})$.

Sei also ab jetzt $d \in \{2, 5, 13\}$ und $M$ eine Maximalordnung in $A$. Wir haben auf $M$ die multiplikative und anisotrope Norm $Nr(a) = N_{K|\mathbb{Q}}(N(a)) \in \mathbb{Z}$ für $a \in N$. Um $M$ mit dem Gitter $\mathbb{E}_8$ zu vergleichen, fehlt uns noch eine geeignete Bilinearform auf $M$.

**(3.41) Lemma**
Sei $\alpha \in \mathbb{Z}_K$ so gewählt, dass für die inverse Differente $Z_K^{\#} = \alpha Z_K$ gilt und $\alpha$ *total positiv* ist. Dann ist

$$B : M \times M \to \mathbb{Z},\ B(x, y) := T_{K|\mathbb{Q}}(\alpha \cdot tr(x\bar{y}))$$

eine positiv definite, symmetrische Bilinearform auf $A$.

**Beweis**
Ein $\alpha \in \mathbb{Z}_K$ mit den geforderten Eigenschaft existiert in den Fällen $K = \mathbb{Q}(\sqrt{d}),\ d = 2, 5, 13$, denn für $d = 2$ setze $\alpha_2 := \frac{1}{4}(\sqrt{2} + 2)$, für $d = 5$ setze $\alpha_5 := \frac{1}{10}(-\sqrt{5} + 5)$ und für $d = 13$ setze $\alpha_{13} := \frac{1}{26}(-3\sqrt{13} + 13)$. Zur Konstruktion verwende man Bemerkung (2.13): Ist $d \equiv_4 1$, so wähle eine Einheit $\delta \in \mathbb{Z}_K^*$ geeignet, sodass $\alpha = \frac{1}{\sqrt{d}}\delta$ positiv definit ist. Ist $d \equiv_4 2, 3$, so wähle $\delta \in \mathbb{Z}_K^*$, sodass $\alpha = \frac{1}{2\sqrt{d}}\delta$ positiv definit ist.
$B$ ist wohldefiniert, denn für $x, y \in M$ gilt $tr(x\bar{y}) \in K$ und somit $T_{K|\mathbb{Q}}(\alpha \cdot tr(x\bar{y})) \in \mathbb{Z}$ nach Definition der inversen Differenten.
Dass $B$ bilinear ist, ist klar, da die Spuren $T_{K|\mathbb{Q}}$ und $tr$ sowie die Konjugation linear sind. Weiter ist $B$ symmetrisch, da $tr(x\bar{y}) = tr(\overline{x\bar{y}}) = tr(y\bar{x})$ für $x, y \in M$.
Zu zeigen ist noch, dass $B$ positiv definit ist, das heißt es gilt $B(x, x) > 0$ für alle $0 \neq x \in M$. Wegen $tr(x\bar{x}) = tr(N(x)) = 2N(x)$ gilt aber für $x \neq 0$

$$B(x, x) = T_{K|\mathbb{Q}}(\alpha \cdot tr(x\bar{x})) = 2T_{K|\mathbb{Q}}(\alpha N(x)) = 2(\sigma_1(\alpha)\sigma_1(N(x)) + \sigma_2(\alpha)\sigma_2(N(x))) > 0,$$

denn nach Voraussetzung ist für alle Einbettungen $\sigma_i(\alpha) > 0$. Außerdem gilt für $x = x_1 + .. + x_4 \in M$, dass $N(x) = x_1^2 + .. + x_4^2$ und $\overline{N(x)} = N(\bar{x})$, also $\sigma_i(N(x)) > 0$ für $x \neq 0$. □

$M$ ist nach Definition ein volles $\mathbb{Z}_K$-Gitter. Daher ist $M$ gleichzeitig aber auch ein $\mathbb{Z}$-Gitter von Rang 8 versehen mit der Bilinearform $B$, welches wir ebenfalls mit $M = (Z, B)$ bezeichnen, wobei $Z$ eine $\mathbb{Z}$-Basis von $M$ ist.

**(3.42) Satz**
Für $K = \mathbb{Q}(\sqrt{d})$, $d \in \{2, 5, 13\}$ und $d_A = \mathbb{Z}_K$ ist das Gitter $M = (Z, B)$ isometrisch zum Gitter $\mathbb{E}_8$.

**Beweis**
$\mathbb{E}_8$ ist das einzige 8-dimensionale ganze Gitter, welches gerade, positiv definit und unimodular ist (siehe Satz (2.2)). Wir haben schon in Lemma (3.41) gesehen, dass $M$ ganz und positiv definit ist. Zu zeigen ist also noch, dass $M$ gerade und unimodular ist.
Für $x \in M$ ist $B(x, x) = 2T_{K|\mathbb{Q}}(\alpha N(x)) \in 2\mathbb{Z}$, also ist $M$ gerade.
Um zu sehen, dass $M$ unimodular ist, reicht es nach Bemerkung (2.4) zu zeigen, dass $M$ selbstdual ist, also $M^B = M$, wobei

$$M^B := \{x \in A;\ B(x, M) \subset \mathbb{Z}\}.$$

Wegen $d_A = \mathbb{Z}_K$ ist nach Korollar (3.40)

$$M^\# = \{x \in A;\ tr(xM) \subset \mathbb{Z}_K\} = M,$$

also müssen wir nur $M^B = M^\#$ zeigen (bei der Notation $M^\#$ fassen wir $M$ als vierdimensionales $\mathbb{Z}_K$-Gitter auf):

$$\begin{aligned} x \in M^B \Leftrightarrow B(x, M) \subset \mathbb{Z} &\Leftrightarrow T_{K|\mathbb{Q}}(\alpha \cdot tr(x\bar{y})) \in Z\ \forall y \in M \\ &\Leftrightarrow \alpha \cdot tr(x\bar{y}) \in \mathbb{Z}_K^\# = \alpha\mathbb{Z}_K\ \forall y \in M \\ &\Leftrightarrow tr(x\bar{y}) \in \mathbb{Z}_K \forall y \in M \\ &\Leftrightarrow x \in M^\#. \end{aligned}$$

□

Nun können wir wieder die bekannte Überdeckungseigenschaft von $\mathbb{E}_8$ nutzen und so beweisen, dass $M$ euklidisch ist.

**(3.43) Satz**
Seien $K = \mathbb{Q}(\sqrt{d})$, $d \in \{2, 5, 13\}$, $A = (\frac{-1,-1}{K})$, $d_A = \mathbb{Z}_K$ und $M$ eine Maximalordnung in $A$. Dann ist $M$ euklidisch.

**Beweis**
Nach Satz (3.17) gibt es für alle $y \in \mathbb{Q}^8$ ein $x \in \mathbb{E}_8$ mit $(x - y|\, x - y) \leq 1$. Da $M = (Z, B)$ isometrisch zum Gitter $\mathbb{E}_8$ ist, gilt also: Für jedes $y \in A$ existiert ein $x \in M$ mit

$$T_{K|\mathbb{Q}}(\alpha \cdot tr((x - y)(\overline{x - y}))) \leq 1.$$

Setze $z := x - y$. Mit $tr(z\bar{z}) = 2N(z)$ und der Ungleichung vom arithmetischen und geometrischen Mittel $\frac{1}{2}Tr_{K|\mathbb{Q}}(z) \geq N_{K|\mathbb{Q}}(z)^{1/2}$ (beachte Bemerkung (2.11)(d) und $\alpha \cdot tr(z\bar{z})$ total positiv) folgt

$$1 \geq 2N_{K|\mathbb{Q}}(2\alpha N(z))^{1/2} = 4N_{K|\mathbb{Q}}(\alpha)^{1/2} Nr_{K|\mathbb{Q}}(N(z))^{1/2}.$$

Quadrieren wir auf beiden Seiten, so erhalten wir

$$\frac{1}{16} \geq N_{K|\mathbb{Q}}(\alpha) N_{K|\mathbb{Q}}(N(z)).$$

Mit $N_{K|\mathbb{Q}}(\alpha) = d_K^{-1}$ (siehe Bemerkung (2.13)) folgt schließlich

$$Nr(x-y) = N_{K|\mathbb{Q}}(N(z)) \leq \frac{1}{16} d_K < 1,$$

denn $d_K \in \{4, 5, 13\}$. Somit ist $M$ nach Lemma (2.20) euklidisch. □

**(3.44) Satz**
Sei $A$ eine Quaternionenalgebra über $K = \mathbb{Q}(\sqrt{d})$, $d \in \{2, 5, 13\}$ und $d_A \neq Z_K$. Dann ist keine Maximalordung $M$ von $A$ Euklidisch.

**Beweis**
Siehe [Chau]. □

**(3.45) Bemerkung**
Im Fall $d = 17, d_A = \mathbb{Z}_K$ ist nicht bekannt, ob Maximalordnungen in $A$ euklidisch sind. Im Beweis von Satz (3.43) ist die Schranke $\frac{1}{16} d_K = \frac{17}{16} > 1$ minimal zu groß, sodass man vermuten könnte, dass auch in diesem Fall die Maximalordnungen eukldisch sein müssen.

# A Anhang: Programmlisting

## A.1 ClosestVectors in E8 und D8

Wie in der Einleitung angedeutet, gibt es einen effizienten elementaren Algorithmus, der zu einem beliebigen Punkt im Raum $\mathbb{Q}^8$ einen Gitterpunkt des Gitters $\mathbb{E}_8$ findet, der bezüglich des Standardskalarprodukts $(.|.)$ kürzesten Abstand hat. Dabei verwendet man, dass

$$\mathbb{E}_8 = \mathbb{D}_8 \dot{\cup} (\mathbb{D}_8 + h), \tag{29}$$

wobei $h := (\frac{1}{2}, .., \frac{1}{2}) \in \mathbb{Q}^8$. Hier bezeichnet

$$\mathbb{D}_8 := \{x \in \mathbb{Z}^8;\ \sum_{i=1}^{8} x_i \in 2\mathbb{Z}\}$$

das Gitter mit den Punkten aus $\mathbb{Z}^8$, deren Koordinatensumme gerade ist. Man kann das Gitter $\mathbb{E}_8$ anders als in Satz (2.2) über die Grammatrix auch so beschreiben: $\mathbb{E}_8$ besteht aus allen Punkten $\mathbb{Z}^8$ und $(\mathbb{Z} + \frac{1}{2})^8$, deren Koordinatensumme gerade ist. Also ist die Gleichung (29) offensichtlich richtig.
Um einen nächsten Punkt des Gitters $\mathbb{E}_8$ zu einem gegebenen $x \in \mathbb{Q}^8$ zu finden, kann man nun einen nächstmöglichen Gitterpunkt $z \in \mathbb{D}_8$ zu $x$ suchen und einen nächstmöglichen Gitterpunkt $z' \in \mathbb{D}_8$ zu $x + h$. Gilt dann $(x - z|\, x - z) \leq (x - z'|\, x - z')$, so ist $z$ ein nächster Gitterpunkt zu $x$ in $\mathbb{E}_8$, andernfalls erhalten wir $z' - h$ als beste Approximation an $x$ in $\mathbb{E}_8$.
Das Problem reduziert sich somit darauf, nächstgelegene Gitterpunkte in $\mathbb{D}_8$ zu finden. Die Aufgabe lautet: Für ein gegebenes $x \in \mathbb{Q}^8$ finde $z \in \mathbb{D}_8$, sodass

$$\min_{y \in \mathbb{D}_8}((x - y|\, x - y)) = (x - z|\, x - z)\,.$$

Dazu runde zunächst den Vektor $x$ ganz gewöhnlich komponentenweise und bezeichne diesen mit $f(x)$. Ist die Summe der Komponenten von $f(x)$ gerade, so gilt $f(x) \in \mathbb{D}_8$ und wir sind fertig. Ist die Summe ungerade, so runde genau eine Koordinate von $x$ falsch, die am weitesten von einer ganzen Zahl entfernt ist („falsch“ bedeutet hier, dass man auf die zweitnächste ganze Zahl rundet). Die restlichen Koordinaten seien normal gerundet, sodass wir zwangsläufig einen nächsten Vektor in $\mathbb{D}_8$ finden.
Damit ist der Algorithmus zum Finden eines nächsten Gitterpunktes in $\mathbb{E}_8$ vollständig beschrieben. Ist nun ein beliebiges Gitter $L$ gegeben, welches isometrisch zu $\mathbb{E}_8$ ist (beispielsweise die Maximalordnung $C \subset \mathbb{O}$), so muss zunächst eine Isometrie $T : C \to \mathbb{E}_8$ gefunden werden. Ein Algorithmus von W. Plesken und B. Souvignier, der dies leistet, ist in [PS] beschrieben und in Magma implementiert („IsIsometric“).

```
h:=Vector(Rationals(),[1/2,1/2,1/2,1/2,1/2,1/2,1/2,1/2]);

function r(x)  //gewoehnliches Runden einer rationalen Zahl
  return Round(x);
end function;

function d(x) //Fehler beim Runden
  return r(x)-x;
end function;

function f(x) //Komponentenweises Runden eines Vektors x im Q^8
  return Vector(RationalField(),[r(y): y in Eltseq(x)]);
end function;

function g(x) //Finde die Koordinate, die am weitesten von einer ganzen Zahl entfernt ist.
  max:=Abs(d(x[1])); maxi:=1;
  for i:=2 to 8 do
    if Abs(d(x[i])) gt max then max:=Abs(d(x[i])); maxi:=i; end if;
  end for;
  return maxi;
end function;

function ClosestD8(x) //Funktion, die ClosestVectors(D8,x) ersetzt
  fx:=f(x); //Runde zuerst normal
  sum:=0;
  for i:=1 to 8 do sum:=sum+fx[i]; end for;
  if sum in 2*IntegerRing()
    then return fx, Norm(fx-x); // liegt Summe der Komponenten in D8, sind wir fertig
    else m:=g(x); //sonst runde die Koordinate g(x) falsch...
      if d(x[m]) ge 0 then fx[m]:=fx[m]-1; else fx[m]:=fx[m]+1; end if;
  end if;
  return fx,Norm(fx-x);
end function;

function ClosestE8(x) //Funktion, die ClosestVectors(E8,x) ersetzt
//man verwendet, dass E8 die disjunkte Vereinigung von D8 und D8+h ist:
  x:=ChangeRing(x,RationalField());
  q,  r := ClosestD8(x);
  qq, rr:= ClosestD8(x+h);
  if r le rr then return q, r; end if;
  return qq-h, rr;
```

```
end function;
```

## A.2 Eindeutige Primfaktorzerlegung in den Oktaven

Mithilfe der Funktion „ClosestE8“ können wir nun die Division mit Rest nach Rehm in der Maximalordnung $C$ und darauf aufbauend die in Satz (3.36) bewiesene eindeutige Primfaktorzerlegung in $C$ implementieren. Die Kommentare des folgenden Programms erklären seine Funktionalität.

```
//Initialisiere das Gitter E8
E8:=Lattice("E",8);
B:= BasisMatrix(E8);

//Konstruiere die Agebra der Oktaven:
quat:=func<i,j,k| [<1,1,1,1>,<i,i,1,-1>,<j,j,1,-1>,<k,k,1,-1>,<1,i,i,1>,<i,1,i,1>,
<1,j,j,1>,<j,1,j,1>,<1,k,k,1>,<k,1,k,1>,<i,j,k,1>,<j,i,k,-1>,<j,k,i,1>,<k,j,i,-1>,
<k,i,j,1>,<i,k,j,-1>]>;
con:=&cat[quat((n+1) mod 7 +2, (n+2) mod 7 +2, (n+4) mod 7 +2):n in [0..6]];
O:=Algebra<Rationals(),8 | Setseq(Set(con))>;

one:= One(O); //Einselement in O

//Konstruiere Basis von Coxeter-Maximalordnung C:
f0:= O ! [1,0,0,0,0,0,0,0];
f1:= O ! [0,1,0,0,0,0,0,0];
f2:= O ! [0,0,1,0,0,0,0,0];
f3:= O ! [0,0,0,1,0,0,0,0];
f4:= O ! [0,1/2,1/2,1/2,-1/2,0,0,0];
f5:= O ! [-1/2,0,1/2,0,1/2,0,0,1/2];
f6:= O ! [-1/2,-1/2,0,0,-1/2,1/2,0,0];
f7:= O ! [-1/2,0,0,0,0,-1/2,-1/2,-1/2];
BasisC:=Matrix([f0,f1,f2,f3,f4,f5,f6,f7]);
BasisCInv:= BasisC^-1;
//Reskaliere Skalarprodukt mit 2:
C:=LatticeWithBasis(BasisC, MatrixRing(Rationals(), 8) ! 2);
//Bastle Isomorphismus T zwischen C und E8:
ok,T:=IsIsometric(C,E8);
assert ok;
T:=ChangeRing(T,Rationals());
```

```
//Basiswechsel von C nach E8, bzw. von E8 nach C:
BasisCnachE8:=BasisC^-1*T^-1*B;
BasisE8nachC:=B^-1*T*BasisC;

// Elemente in C mit Norm 1 (bzw. mit Norm 2, da C reskaliert):
muAlts:=ShortVectors(C,2,2);

//Fuer den Sonderfall Norm 2 in der Primfaktorzerlegung (siehe unten):
Pis:=[elt<O|1,1,0,0,0,0,0,0>,elt<O|1,1/2,1/2,1/2,1/2,0,0,0>,
elt<O|1,1/2,1/2,1/2,-1/2,0,0,0>,elt<O|1,1/2,1/2,0,0,1/2,0,1/2>,
elt<O|1,1/2,1/2,0,0,1/2,0,-1/2>,elt<O|1,1/2,0,1/2,0,1/2,1/2,0>,
elt<O|1,1/2,0,1/2,0,1/2,-1/2,0>,elt<O|1/2,1,1/2,1/2,0,1/2,0,0>,
elt<O|1/2,1,-1/2,-1/2,0,-1/2,0,0>];

function konju(x) //Konjugation
  return 2*InnerProduct(x,one)*one-x;
end function;

function norm(x) //quadrierter euklidischer Betrag
  return InnerProduct(x,x);
end function;

function invers(x) //Inverses Element
  return 1/InnerProduct(x,x)*konju(x);
end function;

function DivRestre(a, b) //Division mit Rest, sodass a=b*q+r
  a:= O ! a; b:= O ! b;
  lambda:=invers(b)*a;
  x:= ClosestE8(Vector(Eltseq(lambda))*BasisCnachE8)*BasisE8nachC;
  q:= O ! x;
  r:= a-b*q;
  return q, r;
end function;

function DivRestli(a, b) //Division mit Rest, sodass a=q*b+r
  a:= O ! a; b:= O ! b;
  lambda:=a*invers(b);
  x:=ClosestE8(Vector(Eltseq(lambda))*BasisCnachE8)*BasisE8nachC;
  q:=O ! x;
```

```
  r:=a-q*b;
  return q, r;
end function;

function Rehm(a, m)
//Algo von Rehm zur Konstruktion eines Linksteilers von a mit Norm m
  p:=a;
  Gammas:=[];
  m:=norm(a)*1/m;
//Vorwaertsschritt:
  while norm(p)  ne 0 do
    melt:=elt<O|m,0,0,0,0,0,0,0>;
    gamma,r:=DivRestli(p,melt);
    p:=konju(r);
    if norm(p) ne 0 then m:=norm(p)*1/m; end if;
    Append(~Gammas,gamma);
  end while;

//Rueckwaertsschritt fuer alle Einheiten muAlts
//bis gewuenschter Linksteiler (hinsichtlich Eindeutigkeit der Primfaktor-
//zerlegung) gefunden:
  for i:=1 to #muAlts do
  for l in [1..2] do
  //Magma gibt nur bezueglich lex. Ordnung positive Elemente der Norm 1 aus
    muAlt:=(-1)^l*muAlts[i][1];
    muAlt:=O ! Eltseq(muAlt);
    gamma:=Gammas[#Gammas];
    mu:=gamma*muAlt;
    for j:=1 to #Gammas-1 do
      gamma:=Gammas[#Gammas-j];
      muNeu:=gamma*mu+muAlt;
      muAlt:=mu;
      mu:=muNeu;
    end for;
    muV:=Vector(Eltseq(mu));
//Teste gefundenen Linksteiler mu (bzw. muV) auf Positivitaet
//(bzgl lex. Ordnung) und auf die Eigenschaft mu-e in 2*C:
    gr0:=false;
    for k in [1..8] do
      if muV[k] lt 0 then break k; end if;
      if muV[k] gt 0 then gr0:=true; break k; end if;
```

```
    end for;
    dif:=Vector(Eltseq(mu-one));
    if dif in 2*C and gr0 eq true then return mu, muAlt;  end if;
  end for;
  end for;
end function;

function Faktor(a) //eindeutige Primfaktorisierung eines primitiven a aus C
//in ganzzhalige Oktaven x_n,..,x_1,x_0 bezueglich Primfaktorisierung der Norm
//norm(a)=m_n*..*m_1, wobei die Primfaktoren der Norm absteigend geordnet sind
//und x_0 mit norm(x_0)=1 eine Einheit in C ist.
//Es gilt dann: a = x_n*(x_n-1*(*..*(x_1*x_0)..))  (Beachte Klammerung!)
//Eingabe: beliebiges a in C
//Ausgabe: [<x_n,norm(x_n)>,..,<x_0,norm(x_0)>],
//         und falls a nicht primitiv mit ggT = groesster natuerliche Teiler von a, dann
//         wird zuerst die Faktorisierung von a/ggT ausgegeben und dann der ggT.

  avec:=Vector(Eltseq(a));
  if not(avec in C) then error "Fehler! Element liegt nicht in C!"; end if;

//Teste ob a primitiv ist, d.h. bestimme groesste ganze Zahl ggT die a teilt:
  ggT:=1;
  ganzeKoeff:=true;
  for i:=1 to 8 do
    if not(avec[i] in IntegerRing()) then ganzeKoeff:=false; break; end if;
  end for;
  ggT:=GreatestCommonDivisor([IntegerRing()|2*avec[i]: i in [1..8]]);
  if 1/2*avec in C and ganzeKoeff eq false then ggT:=ggT*2; end if;
  if ganzeKoeff then ggT:=1/2*ggT; end if;

//Teile durch den ggT, sodass a primitiv wird:
  a:=a/ggT;

//Beginne mit der Faktorisierung von a
  m:=norm(a);
  m:=IntegerRing() ! m;
  x:=Factorization(m); //Primfaktorzerlegung der Norm von a
  Faktoren:=[];

  while #x ne 0 do
    p:=x[#x][1]; //Primfaktoren von a (absteigend)
```

```
    for i:=1 to x[#x][2] do //Haeufigkeit eines Primfaktors
      if p ne 2 then
        li,re:=Rehm(a,p);
      else    //Sonderfall p=2:
        for u in [1..9] do
          q,r:=DivRestre(a,Pis[u]);
          if norm(r) eq 0 then li:=Pis[u]; re:=konju(q); break; end if;
        end for;
      end if;
      Append(~Faktoren,<li,norm(li)>);
      a:=konju(re);
    end for;
    Prune(~x);
  end while;

Append(~Faktoren,<a,norm(a)>);

return Faktoren,ggT;
end function;
```

## A.3 Euklidischer Algorithmus in Quaternionenalgebren über quadratischen Zahlkörpern

Nach Satz (3.43) sind Maximalordnungen in Quaternionenalgebren $(\frac{-1,-1}{\mathbb{Q}(\sqrt{d})})$ für $d \in \{2,5,13\}$ euklidisch, also gibt es einen eukldischen Algorithmus. In dem folgenden Programm sind die euklidischen Algorithmen bezüglich der linkseuklidischen Division mit Rest programmiert, welche jeweils einen größten gemeinsamen Rechtsteiler liefern.

```
declare attributes AlgAssVOrd : E8;
BasisE8:=BasisMatrix("E",8);
wurzel:= function(K) //gibt zuerst die Wurzel von K zurueck, dann das Quadrat der Wurzel
  a:= PrimitiveElement(K);
  a -:= Trace(a)/2;
  q:= -Norm(a);
  d:= Denominator(q);
  if d ne 1 then
    q := Numerator(q) * d;
    a *:= d;
  else
```

```
    q:= Numerator(q);
  end if;

  q, v:= Squarefree(q);
  a /:= v;

  return a, q;
end function;

function sum(x,B)
  return &+ [ x[i] * B[i] : i in [1..8] ];
end function;

intrinsic EAli(a::AlgAssVOrdElt,b::AlgAssVOrdElt)->AlgAssVOrdElt {Euklidischer Algorithmus}
  M:= Parent(a);
  require Parent(b) eq M : "Elemente liegen nicht in der selben Ordnung";
  A:= Algebra(M);
  require Type(A) eq AlgQuat and IsDefinite(A): "Keine definite QA.";

  K:= BaseField(A);
  R:= Integers(K);
  require IsAbsoluteField(K) and Discriminant(R) in {5, 8, 13} : "Falscher Grundkoerper";

  require IsMaximal(M) and BaseRing(M) cmpeq R
          and Discriminant(M) eq 1*R : "Keine Maximalordnung mir triv. Diskr.";

  if not assigned M`E8 then
    B:=ZBasis(M);
    v,w:=wurzel(K);
    if w eq 2 then c:=1/4*(v+2); end if;
    if w eq 13 then c:=1/26*(-3*v+13); end if;
    if w eq 5 then c:=1/10*(-v+5); end if;
    G:=Matrix(8,[Integers()|Trace(c*Trace(x*Conjugate(y))):x,y in B]);
    Lat:=LatticeWithGram(G);
    ok,T:=IsIsometric(Lat,Lattice("E",8));
    T:=ChangeRing(T,RationalField());
    BasisWechsel:=Matrix(Rationals(), [&cat[Eltseq(x):x in Eltseq(A!b)]:b in B])^-1;
    BasisnachE8:=BasisWechsel*T^-1*BasisE8;
    BasisvonE8:=BasisE8^-1*T;
    E8:=<B,G,BasisnachE8,BasisvonE8>;
  else
```

```
    B, G, BasisnachE8, BasisvonE8 := Explode( M‘E8 );
  end if;

  while b ne 0 do
    lam:=a*1/b;
    lambda:=Vector([lam[1][1],lam[1][2],lam[2][1],lam[2][2],
      lam[3][1],lam[3][2],lam[4][1],lam[4][2]]);
    x:=ChangeRing(ClosestE8(lambda*BasisnachE8),RationalField())*BasisvonE8;
    q:=sum(x,B);
    r:=a-q*b;
    a:=M!b;
    b:=M!r;
  end while;

  return a;
end intrinsic;
```

# Literatur

[Bos] W. Bosma, J. J. Cannon, C. Fieker, A. Steel (eds.), „Handbook of Magma functions“, Edition 2.16, 5017 pages (2010)

[Chau] Jérôme Chaubert, „Minimum euclidien des ordres maximaux dans les algèbres centrales à division“, Dissertation (2006)

[Con] John H. Conway, Derek A. Smith, „On Quaternions and Octonions“, A.K. Peters (2003)

[Con2] John H. Conway, Neil J. A. Sloane „Sphere Packings, Lattices and Groups“, Springer, p.121, p.445 ff. (1998)

[Cox] H. S. M. Coxeter, „Integral Cayley Numbers“, Duke Math. J. Volume 13, Number 4 ,p. 561-578 (1946)

[Ebe] Wolfgang Ebeling, „Lattices and Codes“, Vieweg (2002)

[Esch] J.-H. Eschenburg, „Quaternionen und Oktaven“, Skript zur Vorlesung (2009)

[Jac] Nathan Jacobson, „Basic Algebra I“, W H Freeman & Co, p. 438-449 (1985)

[KV] Markus Kirschmer, John Voight, „Algorithmic enumeration of ideal classes for quaternion orders“, SIAM J. Comput. (SICOMP) 39, no. 5, p. 1714-1747 (2010)

[Neb1] Gabriele Nebe, „Vorlesung Gitter und Codes“, Skript zur Vorlesung (2008)

[Neb2] Gabriele Nebe, „Vorlesung Algebraische Zahlentheorie“, Skript zur Vorlesung (2011)

[Neu] Jürgen Neukirch, „Algebraische Zahlentheorie“, Springer (1992)

[PS] Wilhelm Plesken, Bernd Souvignier, „Computing Isometries of Lattices“, J. Symb. Comput. 24(3/4), p. 327-334 (1997)

[Rehm] Hans Peter Rehm, „Prime factorization on integral Cayley octaves“, Annales de la faculté des sciences de Toulouse 6 série, tome 2, no 2, p. 271-289 (1993)

[Rei] Irving Reiner, "Maximal Orders", Clarendon Press, Oxford, 2003.

# Ehrenwörtliche Erklärung

Hiermit erkläre ich, dass ich die vorliegende Arbeit selbstständig angefertig und die aus fremden Quellen direkt oder indirekt übernommenen Gedanken als solche kenntlich gemacht habe. Die Arbeit wurde bisher keiner anderen Prüfungsbehörde vorgelegt und auch noch nicht veröffentlicht.

Ich bin mir bewusst, dass eine unwahre Erklärung rechtliche Folgen haben wird.

Aachen, den 7. September _____

(Unterschrift)