Quaternionen und Oktaven

Ausarbeitung zum Seminar zur Computeralgebra, 26.11.2010

Christian Staerk

Die vorliegende Ausarbeitung handelt von den Zahlenbereichen der Quaternionen und Oktaven und jeweils zugehörigen „Ganzheitsringen“.
Im ersten Abschnitt der Ausarbeitung werden diese neuen Zahlenbereiche eingeführt und einige wichtige Eigenschaften studiert.
Es wird sich zeigen, dass die Oktaven gewissermaßen das Ende des Zahlenbegriffs markieren. Dazu wird im zweiten Abschnitt der Satz von Hurwitz bewiesen, der besagt, dass es über den reellen Zahlen nur vier normierte Algebren mit Eins 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 dritten Abschnitt der Ausarbeitung werden wir uns schließlich analog zum Ring der (ganzzahligen) Gaußschen Zahlen in der komplexen Ebene fragen, wie die Eigenschaft „ganzzahlig“ in den Zahlenbereichen der Quaternionen und Oktaven definiert werden kann. Dazu werden wir den Begriff der Maximalordnung auf nichtassoziative Algebren erweitern. Dies wird uns zu einer Maximalordnung der Hurwitz Quaternionen H und zu einer „Maximalordnung“ C in den Oktaven führen. Im Zentrum dieses Abschnittes wird der Euklidische Algorithmus stehen, welcher in den Gaußschen Zahlen und in den Hurwitz Quaternionen ganz gewöhnlich funktioniert, sofern man eine Division mit Rest hat. Bei den ganzzahligen Oktaven C hingegen wird uns trotz Division mit Rest wieder die fehlende Assoziativität zum Verhängnis, sodass 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. Dieser wird am Ende der Ausarbeitung ausführlich besprochen.

Inhaltsverzeichnis

§1 Definitionen und einige Eigenschaften

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 ($\mathbb{O} = \mathbb{R}^4$), sondern auch als Paare von komplexen Zahlen ($\mathbb{O} = \mathbb{C}^2$) auffassen. Hierbei geht man ganz analog zur Konstruktion der komplexen Zahlen aus den reellen Zahlen vor und bekommt so gleichzeitig einige geometrische Hintergründe für die Struktur der Quaternionen. Diesen Weg wollen wir zunächst gehen.

— *Die Quaternionen als komplexe Matrixgruppe* —

Erinnern wir uns, wie die komplexen Zahlen als Matrixgruppe aus den reellen Zahlen konstruiert werden können, so stoßen wir auf die Konzepte der *orthogonalen Gruppe*

$$\mathcal{O}_n = \{A \in \mathbb{R}^{n\times n};\ A^tA = I\}$$

und der *speziellen orthogonalen Gruppe*

$$\mathcal{SO}_n = \{A \in \mathbb{R}^{n\times n};\ A^tA = I,\ det(A) = 1\},$$

welche auch als Drehgruppe bezeichnet wird. Im Fall $n = 2$ erhält man

$$\mathcal{SO}_2 = \{\begin{pmatrix} a & b \\ -b & a \end{pmatrix};\ a^2 + b^2 = 1\}$$

und die komplexen Zahlen sind gerade die $\mathcal{SO}_2$ mit beliebiger Norm:

$$\mathbb{C} = \{\begin{pmatrix} a & b \\ -b & a \end{pmatrix};\ a, b \in \mathbb{R}\}.$$

Die komplexen Analoga zu diesen Gruppen sind die *unitäre Gruppe*

$$\mathcal{U}_n = \{A \in \mathbb{C}^{n\times n};\ A^*A = I\}$$

und als Untergruppe die *spezielle unitäre Gruppe*

$$\mathcal{SU}_n = \{A \in \mathbb{C}^{n\times n};\ A^*A = I,\ det(A) = 1\},$$

wobei $A^* = \overline{A^t}$ die adjungierte Matrix von A bezeichne. Die Zeilen (und Spalten) der unitären Gruppe und insbesondere der speziellen unitären Gruppe bilden also eine Orthonormalbasis für das *hermitesche Skalarprodukt* $\langle x, y\rangle = \sum_i \overline{x_i} y_i$.

Sei nun im Fall $n = 2$

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathcal{SU}_2 \text{ mit } a, b, c, d \in \mathbb{C}.$$

Dann ist $(a, b) \in \mathbb{C}^2$ ein frei wählbarer Einheitsvektor, das heißt $|a|^2 + |b|^2 = 1$ und $(c, d) \in \mathbb{C}^2$ ist ein Einheitsvektor im eindimensionalen komplexen Unterraum $(a, b)^\perp \subset \mathbb{C}^2$. In jedem eindimensionalen komplexen Unterraum gibt es jedoch unendlich viele Einheitsvektoren, da mit (c, d) auch (sc, sd) für $s \in \mathbb{C}$ mit $|s| = 1$ ein Einheisvektor ist. Nun wählt aber die Determinantenbedingung genau $(c, d) = (-\overline{b}, \overline{a})$ aus, denn gerade dann ist $det \begin{pmatrix} a & b \\ -\overline{b} & \overline{a} \end{pmatrix} = a\overline{a} + b\overline{b} = |a|^2 + |b|^2 = 1$.

Folglich ist

$$\mathcal{SU}_2 = \{\begin{pmatrix} a & b \\ -\overline{b} & \overline{a} \end{pmatrix};\ a, b \in \mathbb{C},\ |a|^2 + |b|^2 = 1\}.$$

Lassen wir wieder beliebige Normen zu, erhalten wir die Matrixgruppe der *Quaternionen*.

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

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

(1.2) Lemma

a) $\mathbb{H}$ ist ein reeller Untervektorraum der Matrixalgebra $\mathbb{C}^{2\times 2}$, jedoch kein komplexer Untervektorraum.

b) $\mathbb{H}$ 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.

c) Die Multiplikation (1) auf $\mathbb{H}$ ist assoziativ, jedoch nicht kommutativ. ◇

Beweis

a) Dass $\mathbb{H}$ ein reeller Untervektorraum ist, ist klar, da die komplexe Konjugation $\mathbb{R}$-linear ist. $\mathbb{H}$ ist jedoch kein $\mathbb{C}$-Vektorraum, da zum Beispiel

$$i\begin{pmatrix} a & b \\ -\overline{b} & \overline{a} \end{pmatrix} = \begin{pmatrix} ia & ib \\ \overline{ib} & -\overline{ia} \end{pmatrix} \notin \mathbb{H}.$$

b) Es gilt

$$\begin{pmatrix} a & b \\ -\overline{b} & \overline{a} \end{pmatrix}\begin{pmatrix} c & d \\ -\overline{d} & \overline{c} \end{pmatrix} = \begin{pmatrix} ac - b\overline{d} & ad + b\overline{c} \\ -\overline{b}c - \overline{a}\overline{d} & -\overline{b}d + \overline{a}\overline{c} \end{pmatrix} = \begin{pmatrix} u & v \\ -\overline{v} & \overline{u} \end{pmatrix}$$

mit $u = ac - b\overline{d}$ und $v = ad + b\overline{c}$ (Beachte wieder die Linearität der Konjugation und $\overline{ef} = \overline{f}\overline{e} \quad \forall e, f \in \mathbb{C}$). Die erste Zeile liefert gerade die Multiplikation in (1). Somit ist $\mathbb{H}$ eine Unteralgebra von $\mathbb{C}^{2\times 2}$.

c) Die Multiplikation ist als Matrixmultiplikation offensichtlich assoziativ, jedoch nicht kommutativ, da nach (1) zum Beispiel

$$(0,1)(i,0) = (0-0, 0+1\cdot\bar{i}) = (0,-i)$$

und

$$(i,0)(0,1) = (0-0, i\cdot 1+0) = (0,i)$$ □

Ganz analog zu den komplexen Zahlen definiert man eine Konjugation auf $\mathbb{H}$:

(1.3) Definition

Sei $(a,b) \in \mathbb{C}\times\mathbb{C} = \mathbb{H}$. Dann heißt $\overline{(a,b)} := (\overline{a}, -b)$ die *Konjungierte* zu (a,b).

Weiter sei $|(a,b)| := \sqrt{|a|^2 + |b|^2}$ der gewöhnliche euklidische Betrag. ◇

(1.4) Lemma

Für $x, y \in \mathbb{H}$ und $s \in \mathbb{R}$ gilt:

a) $\overline{x+y} = \bar{x} + \bar{y}$ und $\overline{sx} = s\bar{x}$

b) $x\bar{x} = |x|^2$

c) $\overline{xy} = \bar{y}\bar{x}$

d) $|xy| = |x|\,|y|$ ◇

Beweis

a) Mit der $\mathbb{R}$-Linearität der Konjugation in $\mathbb{C}$ und $x = (a, b),\ y = (c, d)$ mit $a, b, c, d \in \mathbb{C}$ folgt:

$$\overline{x+y} = \overline{(a,b)+(c,d)} = \overline{(a+c, b+d)} = (\overline{a+c}, -(b+d)) = (\bar{a}, -b) + (\bar{c}, -d) = \bar{x} + \bar{y}.$$

Genauso leicht folgt die zweite Aussage.

b) Mit (1) und $x = (a, b)$ folgt

$$x\bar{x} = (a,b)(\bar{a}, -b) = (a\bar{a} + b\bar{b}, -ab + ba) = |a|^2 + |b|^2 = |x|^2 .$$

c) Für Matrizen $A, B \in \mathbb{C}^{2\times 2}$ gilt $(AB)^* = B^*A^*$ und da die Multiplikation in $\mathbb{H}$ eine Matrixmultiplikation ist, folgt die Behauptung.

d) Mit b) und c) gilt

$$|xy|^2 = (xy)\overline{(xy)} = xy\bar{y}\bar{x} = |y|^2\, x\bar{x} = |y|^2\, |x|^2$$

und durch Wurzelziehen folgt die Behauptung. □

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 $\mathbb{H}$).

— *Die Quaternionen als Quartetts von reellen Zahlen* —

(1.5) Definition (Quaternionen2)

$\mathbb{H} := \{x = x_0 + x_1 i + x_2 j + x_3 k;\ x_0, x_1, x_2, x_3 \in \mathbb{R}\}$ 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 $1r = r1$ für $r \in \{1, i, j, k\}$. ◇

(1.6) 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:

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

$$(x_0 y_1 + x_1 y_0 + x_2 y_3 - x_3 y_2) i + (x_0 y_2 + x_2 y_0 + x_3 y_1 - x_1 y_3) j + (x_0 y_3 + x_3 y_0 + x_1 y_2 - x_2 y_1) k$$

Da wir die Quaternionen aus Definition (1.5) mit denen aus (1.1) identifiziert haben, wissen wir bereits, dass diese eine assoziative Algebra über den reellen Zahlen bilden. So können wir uns längliche Rechnungen mit dieser etwas komplizierten Multiplikation sparen. ◇

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 leider eine Konstruktion als Matrixgruppe 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.

— *Die Oktaven als Paare von Quaternionen* —

(1.7) Definition (Oktaven)
$\mathbb{O} := \{(a,b);\ a,b \in \mathbb{H}\}$ 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

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

◇

(1.8) Lemma

a) $\mathbb{O}$ wird mit der Multiplikation (3) zu einer $\mathbb{R}$-Algebra.

b) Die Multiplikation auf $\mathbb{O}$ ist weder kommutativ noch assoziativ. ◇

Beweis

a) Dass $\mathbb{O}$ ein $\mathbb{R}$-Vektorraum ist, ist klar. Die „skalare Assoziativität" und die Distributivgesetze rechnet man leicht nach, zum Beispiel ist für $(a,b),(c,d),(e,f) \in \mathbb{O}$:

$$(a,b)((c,d)+(e,f)) = (a,b)(c+e,d+f) = (a(c+e) - \overline{(d+f)}b, (d+f)a + b\overline{(c+e)})$$

$$\overset{(*)}{=} (ac - \bar{d}b, da + b\bar{c}) + (ae - \bar{f}b, fa + b\bar{e}) = (a,b)(c,d) + (a,b)(e,f),$$

wobei (*) wegen der Linearität der Konjugation und der Distributiviät in $\mathbb{H}$ gilt.

b) Die Multiplikation kann auf $\mathbb{O}$ nicht kommutativ sein, da sie ja schon in $\mathbb{H}$ nicht kommutativ ist und $\mathbb{H}$ natürlicherweise eingebettet ist in $\mathbb{O}$ durch

$$\mathbb{H} \ni h \mapsto (h,0) \in \mathbb{O}.$$

Die Multiplikation ist ebenfalls nicht assoziativ, da zum Beispiel mit der Multiplikation (3) und den Hamilton-Regeln (2) gilt:

$$(i,0)[(0,i)(j,0)] = (i,0)(0,i\bar{j}) = (i,0)(0,-ij) = (i,0)(0,-k) = (0,-ki) = (0,-j)$$

und

$$[(i,0)(0,i)](j,0) = (0,i^2)(j,0) = (0,-1)(j,0) = (0,-\bar{j}) = (0,j) \qquad \square$$

Wie üblich definieren wir eine Konjugation auf $\mathbb{O}$.

(1.9) Definition

Sei $(a,b) \in \mathbb{O}$. Dann heißt $\overline{(a,b)} := (\bar{a},-b)$ die *Konjungierte* zu (a,b).

Weiter sei $|(a,b)| := \sqrt{|a|^2 + |b|^2}$ der gewöhnliche euklidische Betrag. ◇

Und wieder gelten für die Konjugation auf $\mathbb{O}$ die gleichen Rechenregeln wie in Lemma (1.4).

(1.10) Lemma

Für $x,y \in \mathbb{O}$ und $s \in \mathbb{R}$ gilt:

a) $\overline{x+y} = \bar{x} + \bar{y}$ und $\overline{sx} = s\bar{x}$

b) $x\bar{x} = |x|^2$

c) $\overline{xy} = \bar{y}\bar{x}$

d) $|xy| = |x|\,|y|$ ◇

Beweis
Die Beweise von a)-c) laufen alle analog zu denen im Beweis von Lemma (1.4). Nur bei Eigenschaft d) muss man aufpassen. Argumentieren wir wie oben, so gilt

$$|xy|^2 = (xy)\overline{(xy)} = (xy)(\bar{y}\bar{x}) \overset{(*)}{=} x(y\bar{y})\bar{x} = x\,|y|^2\,\bar{x} = |y|^2\,x\bar{x} = |y|^2\,|x|^2\,.$$

Dass wir in $(*)$ die Reihenfolge der Multiplikation vertauschen dürfen, obwohl $\mathbb{O}$ nicht assoziativ ist, sagt uns der Satz von Artin. □

(1.11) Satz (Artin)
Jede Unteralgebra von $\mathbb{O}$, die nur von höchstens zwei Elementen erzeugt wird, ist assoziativ. Man nennt $\mathbb{O}$ auch eine *alternative Algebra*. ◇

Wir wollen diesen Satz hier nicht beweisen, werden ihn aber vor allem im dritten Abschnitt der Ausarbeitung immer wieder benutzen. In (*) gilt also die Gleichheit, da $x, y, \bar{x}, \bar{y}$ alle in der von $1, x$ und y erzeugten Unteralgebra liegen.
Den ersten Abschnitt beenden wir, indem wir, wie angekündigt, die Oktaven auch als Oktetts von reellen Zahlen auffassen.

— *Die Oktaven als Oktetts von reellen Zahlen* —

(1.12) Definition (Oktaven2)
$\mathbb{O} := \{x = x_0 + x_1e_1 + x_2e_2 + x_3e_3 + x_4e_4 + x_5e_5 + x_6e_6 + x_7e_7;\ x_0, x_1, .., x_7 \in \mathbb{R}\}$
heißt die Menge der *Oktaven*. Dabei sei $(1, e_1, e_2, e_3, e_4, e_5, e_6, e_7)$ 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:

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

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

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

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

wobei die Indizes modulo 7 mit dem Vertretersystem $\{1, 2, .., 7\}$ gelesen werden müssen. Wie üblich sei $1r = r1$ 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

(1.13) Beispiel
Es ist $e_2e_3 = e_5$ nach (5), $e_7e_5 = -e_4$ nach (6) und $e_5e_1 = -e_6$ nach (7). ◇

§2 Der Satz von Hurwitz

In diesem Abschnitt wollen wir den Satz von Hurwitz aus dem Jahre 1898 beweisen. Dieser besagt, dass es nur vier normierte Algebren mit Eins 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.

Um die Begriffe zu klären, zunächst eine

(2.1) Definition
Sei A eine Algebra über $\mathbb{R}$.

a) 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.

b) A heißt *normierte Algebra*, wenn sie mit einer Norm $|| : A \to \mathbb{R}$ versehen ist, die von einem Skalarprodukt $(-|-) : A \times A \to \mathbb{R}$ induziert wird, das heißt $|a| = \sqrt{(a|a)}$ für $a \in A$. Weiter soll die Norm multiplikativ sein, das heißt es soll $|xy| = |x|\,|y|$ für alle $x, y \in A$ gelten.

c) A heißt *Schiefkörper*, falls A eine assoziative Divisionsalgebra ist. ◇

(2.2) Satz
Jede normierte Algebra ist eine Divisionsalgebra. ◇

Beweis
Siehe [Esch]. □

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. Vorher können wir aber wenigstens zeigen, dass $\mathbb{H}$ und $\mathbb{O}$ wirklich Divisionsalgebren sind.

(2.3) Lemma
a) $\mathbb{H}$ ist eine Divisionsalgebra, und somit ein Schiefkörper.

b) $\mathbb{O}$ ist eine Divisionsalgebra. ◇

Beweis

a) Nach Lemma (1.4)(b) gilt für $u \in \mathbb{H}$, $u\bar{u} = |u|^2$, also $u\frac{\bar{u}}{|u|^2} = 1$ und somit $u^{-1} = \frac{\bar{u}}{|u|^2}$. Die Gleichung $ux = v$ für $u, v \in \mathbb{H}$ hat also wegen der Assoziativität von $\mathbb{H}$ die eindeutige Lösung $x = u^{-1}v = \bar{u}\frac{v}{|u|^2}$. Die andere Gleichung löse man analog mit Rechtsmultiplikation von u^{-1}. Somit ist $\mathbb{H}$ eine Divisionsalgebra und da das Assoziativgesetz gilt, sogar ein Schiefkörper.

b) Nach Lemma (1.10)(b) und mit der gleichen Argumentation wie in (a) existiert zu $u \in \mathbb{O}$ ein Inverses $u^{-1} = \frac{\bar{u}}{|u|^2}$. Wenn wir nun zum Beispiel die Gleichung $ux = v$ nach x durch Linksmultiplikation mit u^{-1} lösen wollen, müssen wir wegen der fehlenden Assoziativität von $\mathbb{O}$ aufpassen. Nach dem Satz von Artin (1.11) gilt aber $u^{-1}(ux) = (u^{-1}u)x = x$, sodass wir wieder die eindeutige Lösung $x = u^{-1}v = \bar{u}\frac{v}{|u|^2}$ bekommen. □

Nun wollen wir den Beweis des Satzes von Hurwitz vorbereiten. Sei im Folgenden A eine normierte Algebra über $\mathbb{R}$ mit Eins. Statt mit der Norm arbeiten wir hier lieber mit der von ihr induzierten *anisotropen quadratischen Form* $N : A \mapsto \mathbb{R}$, $N(x) := |x|^2$, die $N(xy) = N(x)N(y)$, $N(\lambda x) = \lambda^2 N(x)$ und $N(x) = 0 \Leftrightarrow x = 0$ für $x, y \in A$, $\lambda \in \mathbb{R}$ erfüllt. Dann ist

$$(x|\,y) = \frac{N(x+y) - N(x) - N(y)}{2}. \tag{8}$$

Wir werden immer wieder benutzen, dass $(x|\,t) = (y|\,t)$ für alle $t \in A$ auch $x = y$ impliziert. Zunächst beweisen wir einige Hilfsaussagen.

(2.4) Lemma

Es gilt für alle $x, y, z, u \in A$:

$$(xy|\,xz) = N(x)\,(y|\,z) \text{ und } (xz|\,yz) = (x|\,y)\,N(z) \tag{9}$$

$$(xy|\,uz) = 2\,(x|\,u)\,(y|\,z) - (xz|\,uy) \tag{10}$$

◇

Beweis

(9): $2\,(xy|\,xz) \overset{(8)}{=} N(xy+xz) - N(xy) - N(xz) = N(x(y+z)) - N(xy) - N(xz)$

$= N(x)N(y+z) - N(x)N(y) - N(x)N(z) = N(x)[N(y+z) - N(y) - N(z)] \overset{(8)}{=} 2N(x)\,(y|\,z)$

Mit Division durch 2 folgt die erste Behauptung von (9). Die zweite folgt analog.

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

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

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

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

$$(xy|\,z) = (y|\,\bar{x}z) \quad \textit{und} \quad (xy|\,z) = (x|\,z\bar{y}) \tag{11}$$

$$\bar{\bar{x}} = x \tag{12}$$

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

$$\overline{x+y} = \bar{x} + \bar{y} \tag{14}$$

$\diamond$

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

$$(y|\,\bar{x}z) = (y|\,2\,(x|\,1)\,z - xz) = (y|\,2\,(x|\,1)\,z) - (y|\,xz) = 2\,(x|\,1)\,(y|\,z) - (xz|\,y) \overset{(10)}{=} (xy|\,z)\,.$$

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

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

(13): Verwende wiederholt (11) und erhalte

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

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

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

Nun wollen wir mit dem sogenannten *Cayley-Dickson-Prozess* beginnen, bei dem wir Schritt für Schritt durch „Verdoppelung“ von Unteralgebren von A immer größere Unteralgebren bekommen. Schauen wir uns zunächst an, was bei einem solchen Verdoppelungsschritt passiert.

(2.6) Lemma
Sei H eine echte Unteralgebra von A mit Eins, $i \in A$ sei ein Einheitsvektor (d.h. $N(i) = 1$), der orthogonal auf H stehe. Dann ist $H + iH := \{a + ib;\ a, b \in H\}$ das sogenannte „Dickson-Double“ wieder eine Unteralgebra von A und es gilt für $a, b, c, d \in H$:

$$(a + ib|\, c + id) = (a|\, c) + (b|\, d) \tag{15}$$

$$\overline{a + ib} = \bar{a} - ib \tag{16}$$

$$ib = \bar{b}i \quad \text{und} \quad i\bar{b} = bi \tag{17}$$

$$(a + ib)(c + id) = (ac - d\bar{b}) + i(cb + \bar{a}d) \tag{18}$$

$\diamond$

Wir bemerken, dass für ein solches $i \in A$ und ein beliebiges $h \in H$: $(i|\, h) = 0$. Somit ist nach Definition der Konjugation $\bar{i} = -i$. Nun zum

Beweis
(15): Es ist wegen der Bilinearität

$$(a + ib|\, c + id) = (a|\, c) + (a|\, id) + (ib|\, c) + (ib|\, id)\,.$$

Mit der Bemerkung von eben gilt aber:

$$(a|\, id) \overset{(11)}{=} \left(a\bar{d}\middle|\, i\right) = 0$$

$$(ib|\, c) \overset{(11)}{=} \left(i\middle|\, c\bar{b}\right) = 0$$

$$(ib|\, id) \overset{(9)}{=} N(i)\,(b|\, d) = (b|\, d)$$

Mit diesen drei Gleichungen folgt die Behauptung (15).

(16): Wegen $(ib|\, 1) = 0$ gilt

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

(17): Dies folgt sofort aus (16): $ib = -\overline{ib} = -\bar{b}\bar{i} = \bar{b}i$. Die zweite Behauptung folgt dann mit (13).

(18): Zeige

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

Dies ist mit der Distributivität von A äquivalent zu

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

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

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

Zu zeigen sind also noch die folgende drei Gleichungen:

$$(\,a(id)|\,t) = (\,i(\bar{a}d)|\,t) \tag{19}$$

$$(\,(ib)c|\,t) = (\,i(cb)|\,t) \tag{20}$$

$$(\,(ib)(id)|\,t) = \big(-d\bar{b}\big|\,t\big) \tag{21}$$

(19): $(\,a(id)|\,t) \overset{(11)}{=} (\,id|\,\bar{a}t) \overset{(10)}{=} 2\underbrace{(\,i|\,\bar{a})}_{=0}(\,d|\,t) - (\,it|\,\bar{a}d) \overset{(11)}{=} -\big(t\big|\,\bar{i}(\bar{a}d)\big) = (\,i(\bar{a}d)|\,t)\,.$

(20): $(\,(ib)c|\,t) \overset{(11)}{=} (\,ib|\,t\bar{c}) \overset{(17)}{=} \big(\bar{b}i\big|\,t\bar{c}\big) \overset{(10)}{=} 0-\big(\bar{b}\bar{c}\big|\,ti\big) \overset{(11)}{=} \big((\bar{b}\bar{c})i\big|\,t\big) \overset{(13)}{=} \Big(\overline{(cb)}i\Big|\,t\Big)$

$$\overset{(17)}{=} (\,i(cb)|\,t)\,.$$

(21): $(\,(ib)(id)|\,t) \overset{(11)}{=} \Big(ib\Big|\,t\overline{(id)}\Big) \overset{(13)}{=} \big(ib\big|\,t(\bar{d}\cdot\bar{i})\big) = -\big(ib\big|\,t(\bar{d}i)\big) \overset{(17)}{=} -(\,ib|\,t(id))$

$$\overset{(10)}{=} 0+(\,i(id)|\,tb) \overset{(11)}{=} -(\,id|\,i(tb)) \overset{(9)}{=} -N(i)\,(\,d|\,tb) \overset{(11)}{=} \big(-d\bar{b}\big|\,t\big)\,.$$

Damit folgt Behauptung (18) und somit ist $H+iH$ eine Unteralgebra von A, denn (18) besagt gerade, dass die Multiplikation auf $H+iH$ abgeschlossen ist. □

Gleichung (18) gibt uns also eine Multiplikationsvorschrift für Elemente aus $H+iH$ an. Statt wie in (18) 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.

$$(a+bi)(c+di) = (ac-\bar{d}b)+(da+b\bar{c})i \tag{18b}$$

Denn mit (17) und (18) folgt:

$$(a+bi)(c+di) = (a+i\bar{b})(c+i\bar{d}) = (ac-d\bar{\bar{b}}) + i(c\bar{b}+\bar{a}\bar{d})$$

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

Wenn wir die Multiplikation (18b) nun 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 (18b) mit der üblichen Multiplikation auf $\mathbb{C}$ übereinstimmt. In $\mathbb{C}$ gilt die Kommutativität der Multiplikation, sodass (18b) gerade die Multiplikation (1) auf $\mathbb{H}$ ist. Und die Multiplikation (3) auf $\mathbb{O}$ ist exakt die Multiplikation (18b).

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

(2.7) Lemma
Sei A eine normierte Algebra über $\mathbb{R}$ mit Eins, Y eine Unteralgebra von A, $i \in A$ orthogonal zu Y mit $N(i) = 1$ und $Z := Y + iY$. Dann:

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

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

Forme diese Bedingung nun äquivalent um. Wegen (8) ist dies äquivalent zu

$$(N(a)+N(b)+\underbrace{2\,(a|\,ib)}_{=0})(N(c)+N(d)+\underbrace{2\,(c|\,id)}_{=0})$$

$$= N(ac - d\bar{b}) + N(i(cb + \bar{a}d)) - \underbrace{2\left(ac - d\bar{b}\middle| i(cb + \bar{a}d)\right)}_{=0},$$

was wiederum gleichwertig ist mit

$$(N(a) + N(b))(N(c) + N(d))$$

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

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

$$N(a)N(c) + N(a)N(d) + N(b)N(c) + N(b)N(d)$$

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

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

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

Division durch 2 und Anwenden von (11) liefert

$$\left((ac)b\middle| d\right) = \left(a(cb)\middle| d\right) \quad \forall d \in Y$$

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. Deshalb gilt

$$i(bc) = (ib)c \overset{(18)}{=} 0 + i(cb) = i(cb) \quad \forall c, b \in Y$$

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

„⇐“ 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:

$$[(a + ib)(c + id)](e + if) = (ac - d\bar{b} + i(cb + \bar{a}d))(e + if)$$

$$\overset{(13,14)}{=} (ac - d\bar{b})e - f(\bar{b}\bar{c} + \bar{d}a) + i[e(cb + \bar{a}d) + (\bar{c}\bar{a} - b\bar{d})f]$$

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

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

c) „⇒“ Sei Z eine kommutative, assoziative normierte Algebra, dann muss Y diese Eigenschaften auch haben. Wegen (17) 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.

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

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

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

Durch Anwenden dieses Lemmas auf immer größere Unteralgebren von A bekommen wir den Satz von Hurwitz.

(2.8) Satz (Hurwitz)
$\mathbb{R}, \mathbb{C}, \mathbb{H}$ und $\mathbb{O}$ sind die einzigen normierten Algebren mit Eins über den reellen Zahlen (bis auf Isomorphie). ◇

Beweis
Sei A eine gegebene normierte Algebra mit Eins über $\mathbb{R}$.
Wenn $\mathbb{R} \subset A \neq \mathbb{R}$, dann gibt es ein normiertes $i \in A$ orthogonal zu $\mathbb{R}$. Also ist nach Lemma (2.7)(c) $\mathbb{C} \cong \mathbb{R} + i\mathbb{R} \subset A$ (beachte Multiplikation (18b)) eine kommutative, assoziative normierte Unteralgebra von A, da $\mathbb{R}$ eine kommutative, assoziative normierte Algebra mit trivialer Konjugation ist.
Wenn $\mathbb{C} \subset A \neq \mathbb{C}$, dann gibt es ein normiertes $i' \in A$ orthogonal zu $\mathbb{C}$. Also ist nach Lemma (2.7)(b) $\mathbb{H} \cong \mathbb{C} + i'\mathbb{C} \subset A$ (beachte (18b)) eine assoziative normierte Unteralgebra von A, die nach (2.7)(c) nicht kommutativ ist, da die Konjugation auf $\mathbb{C}$ nicht trivial ist.
Wenn $\mathbb{H} \subset A \neq \mathbb{H}$, dann gibt es ein $i'' \in A$ orthogonal zu $\mathbb{H}$. Also ist nach Lemma (2.7)(a) $\mathbb{O} \cong \mathbb{H} + i''\mathbb{H} \subset A$ (beachte (18b)) eine normierte Unteralgebra von X, die

nach (2.7)(b) nicht assoziativ ist, da $\mathbb{H}$ nicht kommutativ ist.
Wenn nun $\mathbb{O} \subset A \neq \mathbb{O}$, dann gibt es ein $i''' \in A$ orthogonal zu $\mathbb{O}$. Weiter ist $\mathbb{O} + i'''\mathbb{O} \subset A$ zwar eine Unteralgebra von A, die aber nach Lemma (2.7)(a) nicht normiert ist, da $\mathbb{O}$ nicht assoziativ ist. Dieser Fall kann also nicht eintreten. □

§ 3 Vier euklidische Bereiche

In diesem Kapitel wollen wir uns mit „Ganzheitsringen“ in $\mathbb{H}$ und $\mathbb{O}$ beschäftigen und darin jeweils einen Euklidischen Algorithmus herleiten. Bevor wir dies tun, sei an den eindimensionalen Fall der ganzen Zahlen $\mathbb{Z}$ und an den zweidimensionalen Fall der Gaußschen Zahlen $\mathbb{Z}[i]$ erinnert. In beiden Fällen bekommen wir den euklidischen Algorithmus aus einer Division mit Rest.

— *Euklidischer Algorithmus in* $\mathbb{Z}$ —

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

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

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 $ggT(a, b) = ggT(b, r)$. $\diamond$

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) jediglich die Assoziativität von $\mathbb{Z}$ gebraucht wird. Dies wird das Argument dafür sein, dass der gewöhnliche euklidische Algorithmus in den Gaußschen Zahlen und in den Hurwitz Quaternionen funktioniert, denn in beiden gilt das Assoziativgesetz. 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

$$\begin{aligned} a &= q_1 b + r_1 \quad \text{mit} \quad |r_1| < |b| \\ b &= q_2 r_1 + r_2 \quad \text{mit} \quad |r_2| < |r_1| \\ &\ldots \\ r_{n-2} &= q_n r_{n-1} + r_n \quad \text{mit} \quad |r_n| < |r_{n-1}| \\ r_{n-1} &= q_{n+1} r_n + 0. \end{aligned} \tag{22}$$

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

— *Euklidischer Algorithmus in* $\mathbb{Z}[i]$ —

Kommen wir zum zweidimensionalen Fall der *Gaußschen Zahlen*

$$\mathbb{Z}[i] := \{z \in \mathbb{C};\ z = z_1 + z_2 i,\ \ z_1, z_2 \in \mathbb{Z}\}$$

versehen mit der *quadratischen Form* (im Folgenden auch mit *Norm* bezeichnet)

$$N : \mathbb{Z}[i] \to \mathbb{N}_0,\ N(z) := z\bar{z} = z_1^2 + z_2^2 \quad \text{für}\ \ z = z_1 + z_2 i \in \mathbb{Z}[i].$$

Hier bekommen wir wieder eine Division mit Rest.

(3.3) Satz
Sind $a, b \in \mathbb{Z}[i]$ mit $b \neq 0$, so gibt es $q, r \in \mathbb{Z}[i]$ mit

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

Beweis
Sei $c := a/b = c_1 + c_2 i \in \mathbb{Q}[i]$ mit $c_1, c_2 \in \mathbb{Q}$ und für $i = 1, 2$ 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 $q := q_1 + q_2 i \in \mathbb{Z}[i]$ und $s := s_1 + s_2 i \in \mathbb{Q}[i]$, sodass $c = q + s$. Dann ist $r := sb \in \mathbb{Z}[i]$, da $a = cb = (q + s)b = qb + sb = qb + r$ und somit $r = a - qb \in \mathbb{Z}[i]$.
Also ist

$$a = qb + r$$

und

$$N(r) = N(sb) = N(s)N(b) = (s_1^2 + s_2^2)N(b) \leq (\frac{1}{4} + \frac{1}{4})N(b) = \frac{1}{2}N(b). \qquad \square$$

Die Division mit Rest liefert aufgrund der Assoziativität von $\mathbb{Z}[i]$, wie oben schon bemerkt, den gleichen euklidischen Algorithmus wie in (22). Aus diesem bekommen wir das folgende

(3.4) Korollar
$\mathbb{Z}[i]$ ist ein Hauptidealbereich mit (bis auf Assoziiertheit) eindeutiger Primfaktorzerlegung. $\diamond$

— *Euklidischer Algorithmus in den Hurwitz Quaternionen* —

Nun wollen wir Ganzheitsringe über den Quaternionen betrachten. Zunächst könnte man vermuten, dass ein solcher Ganzheitsring genau wie die Gaußschen Zahlen in der komplexen Ebene auszusehen hat.

(3.5) 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 betrachten wieder die quadratische Form

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

L ist offensichtlich ein Ring, jedoch gibt es in diesem keine Division mit Rest im Sinne einer strikten Normreduktion.

(3.6) 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
Wir gehen analog zum Beweis von Satz (3.3) vor. Setze also $c := ab^{-1} = c_1 + c_2 i + c_3 j + c_4 k \in \mathbb{H}$ und durch Wahl von q_i, s_i wie oben bekommen wir $c_i = q_i + s_i$ mit $q_i \in \mathbb{Z}$ und $|s_i| \leq \frac{1}{2}$ für $i = 1, .., 4$.
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 $N(r) = N(b) \ \Leftrightarrow\ |s_i| = \frac{1}{2}\ \forall i \in \{1, .., 4\}\ \Leftrightarrow\ c_i \in \mathbb{Z} + \frac{1}{2}\ \forall i \in \{1, .., 4\}$. □

Da bei der Division mit Rest in L der Rest betragsmäßig nicht immer echt kleiner wird, scheitert unser Euklidischer Algorithmus (22). Denn dieser terminiert ja gerade aufgrund der strikten Normreduktion in jedem Schritt.
Satz (3.6) gibt uns aber schon den entscheidenden Hinweis, wie wir dieses Problem umgehen können.

(3.7) 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 die Fortsetzung der quadratischen Form N auf H ganzzahlig ist. Aus Satz (3.6) folgt jetzt sofort, dass die Hurwitz Quaternionen eine „echte“ Division mit Rest besitzen:

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

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

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 $N(0) < N(b)$). □

Aus oben genannten Gründen (H ist assoziativ) ist der Euklidische Algorithmus (22) also auch in H durchführbar.

— *Euklidischer Algorithmus in ganzzahligen Oktaven* —

Zunächst stellen wir uns die Frage, wann wir eine Oktave „ganzzahlig“ nennen wollen. Dazu ein allgemeines Konzept von Coxeter:

(3.9) Definition
Eine Teilmenge M einer Algebra A mit Eins heißt *maximale Menge von ganzzahligen Elementen* oder *Arithmetik*, falls sie die folgenden vier Bedingungen erfüllt:

a) Für jedes $m \in M$ sind die Koeffizienten des Minimalpolynoms von m ganzzahlig.

b) M ist abgeschlossen unter Addition und Multiplikation.

c) $1 \in M$

d) Falls $N \subseteq A$ die Eigenschaften a),b),c) erfüllt, so gilt bereits $N \subseteq M$.

Falls A assoziativ ist, so heißt M *Ordnung*, falls die Bedingungen a)-c) erfüllt sind. Gilt zusätzlich Bedingung d), so heißt M *Maximalordnung*. ◇

Diese Definition ist also das Analogon des Konzeptes einer Maximalordnung auf auch nichtassoziativen Algebren. Kommen wir nun zu unserer Algebra $\mathbb{O}$, dann hat ein Element $a = a_0 + a_1e_1 + .. + a_7e_7 \in \mathbb{O}$ das Minimalpolynom

$$x^2 - 2a_0x + (a_0^2 + a_1^2 + .. + a_7^2),$$

sodass die Bedingung a) der Definition bedeutet, dass die sogenannte Spur $tr(a) := 2a_0$ und die Norm $N(a) := a_0^2 + a_1^2 + .. + a_7^2$ ganzzahlig sind.
Man kann zeigen, dass es in $\mathbb{O}$ bis auf Konjugation sieben verschiedene maximale Mengen von ganzzahligen Elementen nach obiger Definition gibt. Wir fixieren für unsere Zwecke eine davon:

(3.10) 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 $h := \frac{1}{2}(e_1 + e_2 + e_3 - e_4)$. ◇

(3.11) Satz
C ist eine maximale Menge von ganzzahligen Elementen in $\mathbb{O}$. ◇

Beweis
Siehe [Cox]. □

Wir versehen C wie üblich mit der quadratischen Form

$$N : C \to \mathbb{N}_0,\ N(z) := z\bar{z} = z_0^2 + z_1^2 + .. + z_8^2 \quad \text{für } z \in C.$$

Um auch in C eine Division mit Rest zu bekommen, werden wir zuerst zeigen, dass C mit dem Gitter $\mathbb{E}_8$ identifiziert werden kann und dann werden wir eine bekannte Überdeckungseigenschaft von $\mathbb{E}_8$ nutzen. Dazu benötigen wir einige Definitionen und einen Satz aus der Gittertheorie.

(3.12) Definition
Seien $E = (V, (.|.))$, $E_1 = (V_1, (.|.)_1)$, $E_2 = (V_2, (.|.)_2)$ euklidische Vektorräume.

a) Eine Teilmenge $L \subset V$ heißt *Gitter*, falls ein linear unabhängiges Tupel $B = (b_1, .., b_m) \in V^m$ existiert, sodass $L = \langle b_1, .., b_m \rangle_{\mathbb{Z}}$. B heißt dann eine *Gitterbasis* von L und $m = dim(L)$ die *Dimension* von L.

b) Ein Gitter L heißt *Wurzelgitter*, falls $L = \langle \{l \in L;\ (l|\, l) = 2\} \rangle_{\mathbb{Z}}$.

c) $R(L) := \{l \in L;\ (l|\, l) = 2\}$ heißt Menge der *Wurzeln* in L.

d) Ist $B \in V^m$ eine Gitterbasis des Gitters L, so heißt $\mathbb{G}(B) := ((b_i|\, b_j)) \in \mathbb{R}^{m\times m}$ die *Grammatix* von L und $det(L) := det(\mathbb{G}(B))$ die *Determinante* von L.

e) Für zwei Gitter L_1 in V_1 und L_2 in V_2 bezeichnet $L_1 \perp L_2$ die *orthogonale Summe*. Dies ist ein Gitter in $V_1 \oplus V_2$ der Dimension dim(L_1)+dim(L_2). Sind B bzw. C Gitterbasen von L_1 bzw. L_2, so ist $((b_1, 0), .., (b_{dim(L_1)}, 0), (0, c_1), .., (0, c_{dim(L_2)}))$ eine Gitterbasis von $L_1 \perp L_2$ mit Grammatrix

$$\begin{pmatrix} \mathbb{G}(B) & 0 \\ 0 & \mathbb{G}(C) \end{pmatrix}. \tag{23}$$

◇

(3.13) Satz (vgl. Ebeling)
Jedes ganze Wurzelgitter ist orthogonale Summe von Wurzelgittern der Form $\mathbb{A}_n$, $\mathbb{D}_m$, $\mathbb{E}_6$, $\mathbb{E}_7$, $\mathbb{E}_8$. ◇

Was diese Gitter im Einzelnen sind, wird hier nicht besprochen. Wir benötigen nur die Aussage, dass $det(\mathbb{E}_8) = 1$ und die Determinanten der anderen Gitter alle echt größer als 1 sind (siehe [Nebe]).

(3.14) 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

$$B := (1, e_1, e_2, e_3, \underbrace{\frac{1}{2}(e_1 + e_2 + e_3 - e_4)}_{=h}, e_1h, e_2h, e_3h)$$

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

$$e_1h = \frac{1}{2}(-1 - e_2 + e_4 + e_7)$$

$$e_2h = \frac{1}{2}(-1 - e_1 - e_4 + e_5)$$

$$e_3h = \frac{1}{2}(-1 - e_5 - e_6 - e_7)$$

Bezeichne $S := (e_0, .., e_7)$ die Standardbasis des $\mathbb{R}^8$, 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:

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

Folglich liegt offensichtlich ein ganzes Wurzelgitter vor, welches nach Satz (3.13) orthogonale Summe der dort angegeben Wurzelgitter sein muss.
Weiter gilt $det(\mathbb{G}(B)) = 1$. Da nun die Grammatrix einer solchen orthogonalen Summe die Form (23) hat und nur das Gitter $\mathbb{E}_8$ Determinante 1 hat, folgt mit der Determinantenregel für Blockmatrizen, dass C nur isometrisch zum Gitter $\mathbb{E}_8$ sein kann.□

(3.15) Definition
Die *Überdeckungszahl* eines Gitters L über einem euklidischen Vekorraum V mit Norm $||$ 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

$$ |P - l| \leq r. $$ ◇

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

Da wir im Beweis von Satz (3.14) das Skalarprodukt nicht mit 2 reskaliert haben, erhalten wir folgenden

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

$$N(\lambda - \gamma) \leq \frac{1}{2}. \qquad \diamond$$

Aus diesem Satz bekommen wir nun endlich eine Division mit Rest auf C.

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

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

Beweis
Setze in Satz (3.17) $\lambda = ab^{-1} \in \mathbb{O}$, dann gibt es ein $q \in C$ mit $N(ab^{-1} - q) \leq \frac{1}{2}$; setze $r := a - qb \in C$. Dann ist

$$N(a - qb) = N(a(b^{-1}b) - qb) \overset{(*)}{=} N((ab^{-1} - q)b) = N(ab^{-1} - q)N(b) \leq \frac{1}{2}N(b),$$

also $N(r) < N(b)$, wobei $(*)$ wegen dem Satz von Artin gilt. $\square$

Wir wollen jetzt die Teilbarkeitsbeziehung sowie Primzahlen in C definieren.

(3.19) Definition

a) $\mu \in C$, $\mu \neq 0$ heißt *Rechtsteiler* (bzw. *Linksteiler*) von $\alpha \in C$, falls $\alpha\mu^{-1} \in C$ (bzw. $\mu^{-1}\alpha \in C$). Falls μ Rechtsteiler von α ist, so schreibe $\mu|\alpha$.

b) $\pi \in C$ heißt *Primzahl*, falls $N(\pi) = p$ eine Primzahl ist.

c) $\beta \in C$ heißt *primitiv*, falls die größte ganze Zahl, die β teilt, gleich 1 ist.

Es stellt sich die folgende Aufgabe:
Falls $p|N(\alpha)$ für ein primitives $\alpha \in C$ und p eine Primzahl, so finde die Rechtsteiler $\pi|\alpha$ von α mit $N(\pi) = p$.

Betrachten wir dazu zunächst die Einheiten in C:

(3.20) Lemma
Es gibt 240 Einheiten in C, das heißt

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

Beweis
Es ist bekannt (siehe [Con2]), dass es in $\mathbb{E}_8$ genau 240 Wurzeln gibt. Folglich gibt es nach Satz (3.14) auch genau 240 Elemente in C mit Norm 1. □

Wie oben schon erwähnt, terminiert der bekannte Euklidische Algorithmus (22) 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.

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

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 (3.18) 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 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 ρ_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 μ_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. Weiter gibt es mindestens 240 verschiedene $\lambda \in C$, sodass $N(\lambda) = m_N$ (Nehme eines und multipliziere es mit den 240 Einheiten, siehe Lemma (3.20)).
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 μ_{N-1} Linksteiler von ρ_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 ρ_{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 μ_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 μ_N auch 240 verschiedene Linksteiler μ_0 und 240 verschiedene Rechtsteiler $\overline{\mu_1}$ von α bekommen. □

Falls $m_N > 1$ gibt es sogar mehr als 240 Rechts- und Linksteiler von α mit Norm m. Man kann jedoch zeigen, dass es genau 240 Rechts- und Linksteiler gibt, falls α 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 α 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.

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

Literatur

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

[Con2] John H. Conway, „Sphere Packings, Lattices and Groups“, Springer (1998)

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

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

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

[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)