Eine Seminararbeit
zu Kapitel 2.5 und 2.6 des Buches
Elementary Number Theory, Group Theory, and Ramanujan Graphs

Seminar Gruppentheorie und Geometrie:
Gruppen, Expandergraphen und Bäume
SS16

Quaternionen

Ina Vogler

Dozenten:
Prof. Dr. Linus Kramer
Dr. Olga Varghese

1 Quaternionen über einem Ring

Dieser Abschnitt führt in die Quaternionen ein und gibt dazu einige Definitionen.

Definition 1.1 (Quaternionen)**.** Die hamiltonschen Quaternionen über einem Ring R bestehen aus der Menge $\mathbb{H}(R) = \{a_0 + a_1 i + a_2 j + a_3 k : a_0, a_1, a_2, a_3 \in R\}$ auf der eine Addition und eine Multiplikation wie folgt definiert ist. Bei i, j, k handelt es sich um imaginäre Einheiten.

$+$: (komponentenweise)
$(a_0 + a_1 i + a_2 j + a_2 k) + (b_0 + b_1 i + b_2 j + b_2 k)$
$= ((a_0 + b_0) + (a_1 + b_1)i + (a_2 + b_2)j + (a_3 + b_3)k)$
mit dem Neutralelement $0 + 0i + 0j + 0k = 0$

$\cdot$: $(a_0 + a_1 i + a_2 j + a_2 k) \cdot (b_0 + b_1 i + b_2 j + b_2 k)$
ergibt sich durch Ausmultiplizieren , wobei
$i^2 = j^2 = k^2 = -1,\ ij = -ji = k,\ jk = -kj = i,\ ki = -ik = j$
mit dem Neutralelement $1 + 0i + 0j + 0k = 1$

Daraus ergibt sich folgende Multiplikationstabelle:

	1	i	j	k
1	1	i	j	k
i	i	-1	k	-j
j	j	-k	-1	i
k	k	j	-i	-1

Bemerkung 1.2. Bei den Quaternionen handelt es sich um eine R-Algebra. $\mathbb{H}(R)$ ist eine additive abelsche Gruppe, ist aber nicht kommutativ bzgl. der Multiplikation.

Definition 1.3 (Konjugierte Quaternion)**.** Die konjugierte Quaternion zu $q = a_0 + a_1 i + a_2 j + a_3 k$ ist $\overline{q} = a_0 - a_1 i - a_2 j - a_3 k$.

Definition 1.4 (Norm einer Quaternion)**.** Die Norm einer Quaternion q ist N(q)$=q\overline{q} = \overline{q}q = a_0^2 + a_1^2 + a_2^2 + a_3^2$. Ihre Norm ist multiplikativ, d.h. $N(q_1 q_2) = N(q_1)N(q_2)$.

Beweis. [Die Norm ist multiplikativ] Seien $\alpha, \beta \in \mathbb{H}(\mathbb{Z})$ mit $\alpha = a_0 + a_1 i + a_2 j + a_3 k$ und $\beta = b_0 + b_1 i + b_2 j + b_3 k$. Die Behauptung ist, dass gilt $N(\alpha\beta) = N(\alpha)N(\beta)$.

$$
\begin{aligned}
N(\alpha)N(\beta) &= a_0^2(b_0^2+b_1^2+b_2^2+b_3^2)\\
&+ a_1^2(b_0^2+b_1^2+b_2^2+b_3^2)\\
&+ a_2^2(b_0^2+b_1^2+b_2^2+b_3^2)\\
&+ a_3^2(b_0^2+b_1^2+b_2^2+b_3^2)\\
N(\alpha\beta) &= N(a_0b_0 + a_1b_1(-1) + a_2b_2(-1) + a_3b_3(-1)\\
&+ a_0b_1i + a_1b_0i + a_2b_3i + a_3b_2(-i)\\
&+ a_2b_2j + a_1b_3(-j) + a_2b_0j + a_3b_1j\\
&+ a_0b_3k + a_1b_2k + a_2b_1(-k) + a_2b_0k)\\
&= (a_0b_0 - a_1b_1 - a_2b_2 - a_3b_2)^2\\
&+ (a_0b_1 + a_1b_0 + a_2b_3 - a_3b_2)^2\\
&+ (a_0b_2 - a_1b_3 + a_2b_0 + a_3b_1)^2\\
&+ (a_0b_3 + a_1b_2 - a_2b_1 + a_3b_0)^2\\
&= a_0^2(b_0^2+b_1^2+b_2^2+b_3^2)\\
&+ a_1^2(b_0^2+b_1^2+b_2^2+b_3^2)\\
&+ a_2^2(b_0^2+b_1^2+b_2^2+b_3^2)\\
&+ a_3^2(b_0^2+b_1^2+b_2^2+b_3^2)
\end{aligned}
$$

Man stellt, wie gewünscht, fast, dass bei beiden Rechnungen das selbe Ergebnis herauskommt. □

Bemerkung 1.5. Jede natürliche Zahl lässt sich also genau dann als Summe von vier Quadratzahlen darstellen, wenn sie die Norm einer Quaternion über dem Ring $\mathbb{Z}$ ist. Dies reduziert das Problem der Darstellung jeder natürlichen Zahl als Summe von vier Quadratzahlen auf die Darstellung der Primzahlen als Summe von vier Quadratzahlen. Die Tatsache, dass sich jede natürliche Zahl als Summe von vier Quadratzahlen darstellen lässt, wird im 2. Abschnitt bewiesen.

Lemma 1.6. *Für ein $q \in \mathbb{H}(\mathbb{Z})$ sind folgende Aussagen äquivalent:*

1. *q ist eine Einheit in $\mathbb{H}(\mathbb{Z})$*
2. *$N(q) = 1$*
3. *$q \in \{\pm 1, \pm i, \pm j, \pm k\}$*

Beweis. $1 \Rightarrow 2$
Da q eine Einheit $\exists\, q'$ mit $qq' = 1$. Wir nehmen die Norm: $N(q)N(q') = N(1) = 1 \Rightarrow N(q) = 1$
$2 \Rightarrow 3$
Es gilt $N(\pm 1) = N(\pm i) = N(\pm j) = N(\pm k) = 1$. Sei $\alpha = a_0 + a_1 i + a_2 j + a_3 k \notin \{\pm 1, \pm i, \pm j, \pm k\}$ beliebig. Wir wollen nun zeigen, dass $N(\alpha) \neq 1$. Es müssen mindestens zwei $a_i \neq 0$ mit $i = 0, 1, 2, 3$. Daraus folgt, das $N(\alpha) = a_0^2 + a_1^2 + a_2^2 + a_3^2 \neq 1$ da $a_i^2 > 0$ für zwei i und für alle i $a_i^2 \geq 0$. Schließlich gilt $a_i \in \mathbb{Z}$.
$3 \Rightarrow 1$
Für $q = \pm 1, \pm i, \pm j, \pm k$ existiert eine Quaternion q' mit $qq' = 1$ und eine Quaternion q'' mit $q''q = 1$. ($\Leftrightarrow$) q ist eine Einheit in $\mathbb{H}(\mathbb{Z})$.
Für 1: $1 \cdot 1 = 1 \cdot 1 = 1$
Für -1: $-1 \cdot -1 = -1 \cdot -1 = 1$
Für $\pm i$: $(\pm i \cdot \mp i) = 1$
Für $\pm j$: $(\pm j \cdot \mp j) = 1$
Für $\pm j$: $(\pm k \cdot \mp k) = 1$ □

Satz 1.7. *Sei K ein Körper und seine Charakteristik ungleich 2. Es gebe $x, y \in K$ mit $x^2 + y^2 + 1 = 0$. Dann ist $\mathbb{H}(K)$ isomorph zu den $2x2 - Matrizen$ über K.*

Beweis. Sei $\Psi : \mathbb{K} \to K^{2x2}$ mit

$$\Psi(a_0 + a_1 i + a_2 j + a_3 k) = \begin{pmatrix} a_0 + a_1 x + a_3 y & -a_1 y + a_2 + a_3 x \\ -a_1 y - a_2 + a_3 x & a_0 - a_1 x - a_3 y \end{pmatrix}$$

eine Abbildung.
Behauptung: Ψ ist eine lineare Abb. d.h $\Psi(\alpha\beta) = \Psi(\alpha)\Psi(\beta)\ \forall\ \alpha\beta \in \mathbb{H}(K)$ und $\Psi(b\alpha) = b\Psi(\alpha)$ mit $b \in K$ und $\alpha \in \mathbb{H}(K)$.
Dies lässt sich nachrechnen.
$\mathbb{H}(K)$ ist ein K-Vektorraum der Dimension 4 und K^{2x2} ist ebenfalls ein K-Vektorraum der Dimension 4.
Weiter Hilfsbehauptung: Ψ injektiv $\Rightarrow$ Ψ surjektiv.
Ψ injektiv $\Rightarrow dim(ker(\Psi)) = 0$. Dann folgt mit der Rangformel, dass $dim(im(\Psi) = 4$ und daraus folgt: $im(\Psi) = K^{2x2}$, also Ψ surjektiv. Für den Beweis des Lemmas bleibt also zu zeigen, dass Ψ injektiv ist, also anders formuliert $\Psi(a_0 + a_1 i + a_2 j + a_3 k) = 0 \Rightarrow a_0 = a_1 = a_2 = a_3$.
Dafür kann man überprüfen das folgendes lineares Gleichungssystem eindeutig lösbar ist:

$$\begin{aligned} a_0 + a_1 x + a_3 y &= 0 \\ -a_1 y + a_2 + a_3 x &= 0 \\ -a_1 y - a_2 + a_3 x &= 0 \\ a_0 - a_1 x - a_3 y &= 0 \end{aligned}$$

Dies ist genau dann der Fall, wenn die Determinante der Matrix, die sich aus diesem LGS ergibt ungleich 0 ist.

$$det\left(\begin{pmatrix} 1 & x & 0 & y \\ 0 & -y & 1 & x \\ 0 & -y & -1 & x \\ 1 & -x & 0 & -y \end{pmatrix}\right)$$

Durch Anwenden von dem Laplace-Entwicklungssatz und der Regel von Sarrus erhält man $det = -4(x^2 + y^2)$. Nun setze man x und y, sodass $x^2 + y^2 = -1$, was nach Vorraussetzung möglich ist. Also $det = -4(-1) = 4$. Dies ist ungleich 0, da wir uns in einem Körper mit einer Charakteristik ungleich 2 befinden. Also ist das LGS eindeutig lösbar, damit ist Ψ injektiv, also auch surjektiv und damit ist Ψ ein Isomorphismus, was die Behauptung zeigt.

□

Satz 1.8. *Sei q eine ungerade Primzahl, dann gibt es $x, y \in \mathbb{F}_q$ mit $x^2 + y^2 + 1 = 0$*

Beweis. Wir bestimmen zunächst die Anzahl der Quadratzahlen in $\mathbb{F}_q$.

Wir betrachten folgende Abbildung: $\Phi : \mathbb{F}_q - \{0\} \to \mathbb{F}_q - \{0\}$ mit $\Phi(n) = n^2$. Das Bild dieser Abbildung sind genau die Quadratzahlen in $\mathbb{F}_q$ ohne die 0.
Der Kern der Abbildung:

$$\begin{aligned} a \in ker(\Phi) \text{ falls } a^2 &= 1 \\ \Leftrightarrow a^2 - 1 &= 0 \\ \Leftrightarrow (a-1)(a+1) &= 0 \\ \Rightarrow (a-1) = 0 \text{ oder } (a+1) &= 0 \\ \Rightarrow a &= \pm 1 \end{aligned}$$

Wir wenden den Homomorphiesatz auf die Abbildung $\Phi : \mathbb{F}_q - \{0\} \to im(\Phi(\mathbb{F}_q - \{0\}))$, die surjektiv ist an. Hinzu nehmen wir die Projektiion von $\mathbb{F}_q - \{0\}$ nach $\mathbb{F}_q - \{0\} \setminus ker(\Phi)$. Damit erhält man eine bijektive Abbildung von $\mathbb{F}_q - \{0\} \setminus ker(\Phi)$ nach $im(\Phi(\mathbb{F}_q - \{0\}))$. $\mathbb{F}_q - \{0\} \setminus ker(\Phi)$ hat $\frac{q-1}{2}$ Elemente, da der Kern zwei Elemente hat und $\mathbb{F}_q - \{0\}\ q-1$. Also gibt es ohne die 0 auch $\frac{q-1}{2}$ Quadratzahlen in $\mathbb{F}_q$. Insgesamt: $\frac{q-1}{2} + 1 = \frac{q+1}{2}$

Es gibt also $\frac{q+1}{2}$ Quadratzahlen in $\mathbb{F}_q$. Wir definieren uns folgende zwei Mengen:

$$\begin{aligned} A_+ &:= \{1 + x^2 : x \in \mathbb{F}_q\} \\ A_- &:= \{-y^2 : y \in \mathbb{F}_q\} \end{aligned}$$

Es gilt$|A_+| = \frac{q+1}{2} = |A_-|$. Da diese beiden Mengen zusammen also mehr Elemente haben, als $\mathbb{F}_q$ kann ihr Schnitt nicht leer sein und damit gibt es $x, y \in \mathbb{F}_q$ mit $x^2 + y^2 + 1 = 0$. □

Bemerkung 1.9. Also ist auch $\mathbb{H}(\mathbb{F}_q)\ \forall\ q \in \mathbb{P}$ und $q = 2$ isomorph zu den $2x2-Matrizen$ über $\mathbb{H}(\mathbb{F}_q)$. Ohnehin gilt für jeden algebraisch abgeschlossenen Körper K: $\mathbb{H}(K) \cong 2x2 - Matrizen$ über K.

2 Quaternionen über dem Ring $\mathbb{Z}$

Im folgenden wird mit einer Quaternion stets ein Element aus $\mathbb{H}(\mathbb{Z})$ bezeichnet. In diesem Abschnitt wird ein veränderter Euklidischer Algorithmus für $\mathbb{H}(\mathbb{Z})$ hergeleitet und für bestimmte Quaternionen eine Art von eindeutiger Primfaktorzerlegung. Außerdem wird die Aussage, dass sich jede natürliche Zahl als Summe von vier Quadratzahlen darstellen lässt bewiesen.

Definition 2.1 (Ungerade Quaternion)**.** Eine Quaternion $\alpha \in \mathbb{H}(\mathbb{Z})$ heißt ungerade, falls $N(\alpha)$ ungerade ist.

Definition 2.2 (Gerade Quaternion)**.** Eine Quaternion $\alpha \in \mathbb{H}(\mathbb{Z})$ heißt gerade, falls $N(\alpha)$ gerade ist.

Definition 2.3 (Prime Quaternion)**.** Eine Quaternion $\alpha \in \mathbb{H}(\mathbb{Z})$, α keine Einheit, heißt prim, falls für jede Zerlegung $\alpha = \beta\gamma$ mit $\beta, \gamma \in \mathbb{H}(\mathbb{Z})$ gilt β oder γ ist eine Einheit.
(Die Definition:
α ist prim $\Leftrightarrow$ α teilt ein Produkt xy, dann teilt α x oder y
ist nicht anwendbar in $\mathbb{H}(\mathbb{Z})$, da $\mathbb{H}(\mathbb{Z})$ nicht kommutativ bzgl. der Multiplikation ist.)

Definition 2.4 (Assoziierte Quaternionen)**.** $\alpha, \alpha' \in \mathbb{H}(\mathbb{Z})$ heißen assoziiert, falls $\exists$ Einheiten $\varepsilon, \varepsilon' \in \mathbb{H}(\mathbb{Z})$ mit $\alpha' = \varepsilon\alpha\varepsilon'$

Definition 2.5 (Rechtsseitiger Teiler)**.** $\delta \in \mathbb{H}(\mathbb{Z})$ heißt rechtsseitiger Teiler von $\alpha \in \mathbb{H}(\mathbb{Z})$, falls $\exists\ \gamma \in \mathbb{H}(\mathbb{Z})$ mit $\alpha = \gamma\delta$.
(Der linksseitige Teiler lässt sich entsprechend definieren.)

Definition 2.6 (Größter gemeinsamer Teiler)**.** $\delta \in \mathbb{H}(\mathbb{Z})$ heißt größter gemeinsamer rechtsseitiger Teiler von α und $\beta \in \mathbb{H}(\mathbb{Z})$, falls folgende Bedingungen erfüllt sind:

1. δ ist rechtsseitiger Teiler von α, β
2. Ist δ_0 ein weiterer rechtsseitiger Teiler von α und β, dann folgt, dass δ_0 ein rechtsseitiger Teiler von δ ist.

Man schreibt $\delta =: (\alpha, \beta)_r$.

Man kann nicht von <u>dem</u> größten gemeinsamen rechtsseitigen Teiler sprechen. Es kann eine Menge von größten gemeinsamen rechtsseitigen Teilern geben, die zueinander assoziiert sind. Eine genauere Aussage liefert der folgende Satz:

Satz 2.7. *Sei $0 \neq \delta := (\alpha, \beta)_r$ ein größter gemeinsamer rechtsseitiger Teiler von $\alpha, \beta \in \mathbb{H}(\mathbb{Z})$, dann ist die Menge aller größten gemeinsamen rechtsseitigen Teiler folgende: $\{\pm\delta, \pm i\delta, \pm j\delta, \pm k\delta\}$.*

Beweis. Sei $0 \neq \delta := (\alpha, \beta)_r$. Wir zeigen zunächst, dass für eine Einheit ε, $\varepsilon\delta$ auch ein größter gemeinsamer rechtsseitiger Teiler ist.
$\exists\ \gamma_1, \gamma_2 \in \mathbb{H}(\mathbb{Z})$ mit $\alpha = \gamma_1\delta$ und $\beta = \gamma_2\delta$. Man findet ein γ_1' und ein $\gamma_2' \in \mathbb{H}(\mathbb{Z})$ mit $\gamma_1 = \gamma_1'\varepsilon$ und $\gamma_2 = \gamma_2'\varepsilon$, indem man $\gamma_1' := \gamma_1\varepsilon^{-1}$ und $\gamma_2' := \gamma_2\varepsilon^{-1}$ setzt.
Damit folgt $\alpha = \gamma_1'(\varepsilon\delta)$ und $\beta = \gamma_2'(\varepsilon\delta)$
$\Rightarrow$ $\varepsilon\delta$ teilt α und β rechtsseitig.
Sei δ_0 ein weiterer beliebiger rechtsseitiger Teiler von α, β, damit teilt er bereits δ, dh. $\exists\ \gamma_3$ mit $\delta = \gamma_3\delta_0$
$\Rightarrow$ $\varepsilon\delta = \varepsilon\gamma_3\delta_0 \Rightarrow \delta_0$ teilt auch $\varepsilon\delta$. δ selber teilt auch $\varepsilon\delta$, da $\varepsilon\delta = (\varepsilon)(\delta)$.
$\Rightarrow$ $\varepsilon\delta$ ist ein größter gemeinsamer rechtsseitiger Teiler von α, β.
Wir wollen nun zeigen, dass alle größten gemeinsamen rechtsseitigen Teiler die Form $\varepsilon\delta$ haben, sofern δ einer ist.
Sei also δ_1 ein beliebiger größter gemeinsamer rechtsseitiger Teiler. Zu zeigen ist, dass eine Einheit ε in $\mathbb{H}(\mathbb{Z})$ existiert mit $\delta_1 = \varepsilon\delta$.
Hilfsbehauptung: Sei $\alpha \in \mathbb{H}(\mathbb{Z}) - \{0\}$ mit $\alpha = a_0 + a_1 i + a_2 j + a_3 k$ und $\beta \in \mathbb{H}(\mathbb{Z})$. Dann gilt:
$\alpha = \beta\alpha \Rightarrow \beta = 1$

Beweis. Wir nehmen die Norm $N(\alpha) = N(\beta)N(\alpha) \Rightarrow N(\beta) = 1$ (da $\alpha \neq 0$), also ist β eine Einheit. Bei folgenden Gleichungen kommt man mittels Koeffizientenvergleich stets auf einen Widerspruch:

$$\begin{aligned}
-1(a_0 + a_1 i + a_2 j + a_2 k) &= a_0 + a_1 i + a_2 j + a_3 k \\
\pm i(a_0 + a_1 i + a_2 j + a_2 k) &= a_0 + a_1 i + a_2 j + a_3 k \\
\pm j(a_0 + a_1 i + a_2 j + a_2 k) &= a_0 + a_1 i + a_2 j + a_3 k \\
\pm k(a_0 + a_1 i + a_2 j + a_2 k) &= a_0 + a_1 i + a_2 j + a_3 k
\end{aligned}$$

Daher muss $\beta = 1$ gelten. □

Da δ und δ_1 größte gemeinsame rechtsseitige Teiler sind $\exists\ \gamma_4, \gamma_5 \in \mathbb{H}(\mathbb{Z})$ mit $\delta_1 = \gamma_4\delta$ und $\delta = \gamma_5\delta_1$
$\Rightarrow \delta_1 = \gamma_4\delta = \gamma_4\gamma_5\delta_1$ und $\delta = \gamma_5\delta_1 = \gamma_5\gamma_4\delta$
Mit der Hilfsbehauptung folgt $\gamma_4\gamma_5 = 1$ und $\gamma_5\gamma_4 = 1$
$\Rightarrow \gamma_4 = \gamma_5^{-1}$
$\Rightarrow \gamma_4$ ist eine Einheit. Also $\delta_1 = \varepsilon\delta$ für eine Einheit ε □

Bemerkung 2.8. Hat $\alpha \in \mathbb{H}(\mathbb{Z})$ eine der folgenden Eigenschaften, so hat die ihr assoziierte Quaternion $\beta \in \mathbb{H}(\mathbb{Z})$ diese ebenfalls:

1. ungerade/gerade
2. prim
3. Einheit

Beweis. Seien α und $\beta \in \mathbb{H}(\mathbb{Z})$ assoziiert, dh. $\exists\ \varepsilon_1, \varepsilon_2$ Einheiten mit $\beta = \varepsilon_1\alpha\varepsilon_2$.
Zu 1:
Sei $N(\beta)$ gerade. Es gilt $N(\beta) = N(\varepsilon_1)N(\alpha)N(\varepsilon_2) = N(\alpha)$, da die Norm multiplikativ und die Norm von einer Einheit 1 ist. $\Rightarrow N(\alpha)$ ist gerade. Für ungerade folgt direkt die selbe Aussage, indem man jeweils gerade durch ungerade ersetzt.
Zu 2.
Sei β prim, und $\alpha = \gamma\delta$ eine beliebige Zerlegung von α. Es gilt $\beta = \varepsilon_1\alpha\varepsilon_2 = \varepsilon_1\gamma\delta\varepsilon_2$, da β prim, folgt, dass δ oder γ eine Einheit ist. $\Rightarrow \alpha$ ist prim, da die Zerlegung beliebig war.
Zu 3.
Sei β eine Einheit, also $N(\beta) = 1$. Es gilt $1 = N(\beta) = N(\varepsilon_1\alpha\varepsilon_2) = N(\varepsilon_1)N(\alpha)N(\varepsilon_2) = 1 \cdot N(\alpha) \cdot 1 = N(\alpha)$, da die Norm multiplikativ ist. $\Rightarrow \alpha$ ist eine Einheit.

□

Satz 2.9. *Jedes $\alpha \in \mathbb{H}(\mathbb{Z})$, α keine Einheit, lässt sich als Produkt von primen Quaternionen darstellen. (Nicht unbedingt auf eindeutige Weise!(auch nicht bis auf Assoziiertheit))*

Beweis. Der Satz wird über eine Induktion über $N(\alpha)$ bewiesen.
Induktionsanfang: $N(\alpha) = 1 \Rightarrow \alpha$ ist eine Einheit, für die wir keine Primfaktorzerlegung fordern.
Die Aussage gelte nun $\forall\ \alpha$ mit $N(\alpha) = k < n$. Nun ist zu zeigen, dass dann die Aussage für $N(\alpha) = n$ gilt.
Fall 1: α ist prim
$\Rightarrow \alpha$ selber ist der einzige Primfaktor in der Zerlegung.
Fall 2: α ist nicht prim.
Sei also $\alpha = \beta\delta$ eine Zerlegung mit $N(\delta) \neq 1$ und $N(\beta) \neq 1$. Diese existiert, da ansonsten α prim wäre. Durch anwenden der Norm erhält man $N(\alpha) = N(\beta)N(\delta)$ und daher $N(\beta) < N(\alpha)$ und $N(\delta) < N(\alpha)$. Somit gilt $N(\beta) < n$ und $N(\delta) < n$. β und δ lassen sich also nach der Induktionsvoraussetzung als Produkt von primen Quaternionen schreiben und somit auch α.

□

Beispiel 2.10. $13 = (1 + 2i + 2j + 2k)(1 - 2i - 2j - 2k) = (3 + 2i)(3 - 2i)$
Zwei verschiedene Zerlegungen in prime Quaternionen, die nicht assoziiert zueinander sind.

Das nächste Lemma weist große Ähnlichkeiten zur Definition eines euklidischen Ringes auf, daher zunächst Letztere zum Vergleich. Später wird auch eine Abwandlung des euklidischen Algorithmus(ein Rechtsseitige) bewiesen.

Definition 2.11 (euklidischer Ring)**.** Ein Integritätsring R (kommutativ mit Eins) mit einer Abbildung $\delta : R - \{0\} \to \mathbb{N}$ heißt ein euklidischer Ring, wenn gilt: Zu Elementen $f, g \in R$, $g \neq 0$, gibt es stets Elemente $q, r \in R$ mit

$$f = qg + r, \text{ wobei } \delta(r) < \delta(g) \text{ oder } r = 0.$$

Lemma 2.12. *Seien $\alpha, \beta \in \mathbb{H}(\mathbb{Z})$ mit β ungerade. Dann existieren $\delta, \gamma \in \mathbb{H}(\mathbb{Z})$ mit*

$$\alpha = \gamma\beta + \delta \text{ und } N(\delta) < N(\beta)$$

Bemerkung 2.13. Im Unterschied zur Definition des euklidischen Ringes wird gefordert, dass β ungerade ist und es ist entscheidend, dass β sich auf der rechten Seite von γ in der Gleichung befindet, da $\mathbb{H}(\mathbb{Z})$ nicht kommutativ ist. Man könnte β auch auf die linke Seite stellen, dann kann man andere δ und γ erhalten und im weiteren Verlauf dieses Abschnittes würde dies zu einer linksseitigen Abwandlung des Euklidische Algorithmus führen (statt zu einer Rechtsseitigen).

Beweis. (des Lemmas 2.12) Der folgende Beweis ähnelt dem des euklidischen Algorithmus.
Hilfsbehauptung:
Sei $\sigma = s_0 + s_1 i + s_2 j + s_3 k \in \mathbb{H}(\mathbb{Z})$ und $m \in \mathbb{Z}$ positiv und ungerade. Dann existiert $\gamma \in \mathbb{H}(\mathbb{Z})$ mit

$$N(\sigma - \gamma m) < m^2.$$

Beweis Hilfsbehauptung: Man findet $r_i \in \mathbb{Z} \; \forall \; i = 0, 1, 2, 3$, sodass gilt:

$$s_i \in \left[mr_i - \frac{m}{2}, mr_i + \frac{m}{2}\right]$$
$$\text{denn } m(r_i + 1) - \frac{m}{2} = mr_i + \frac{m}{2}$$

Da m ungerade, folgt, dass $\frac{m}{2} \notin \mathbb{Z}$ und somit auch $mr_i - \frac{m}{2}, \; mr_i + \frac{m}{2} \notin \mathbb{Z}$
$\Rightarrow \; s_i \in \left(mr_i - \frac{m}{2}, mr_i + \frac{m}{2}\right)$

$$\Rightarrow \; mr_i - \frac{m}{2} < s_i < mr_i + \frac{m}{2}$$

und $s_i = mr_i + t_i$ für ein t_i mit $|t_i| < \frac{m}{2}$. Setze das gesuchte $\gamma = r_0 + r_1 i + r_2 j + r_3 k$.

$$\begin{aligned}
\Rightarrow \; N(\sigma - \gamma m) &= N((s_o + s_1 i + s_2 j + s_3 k)(r_o + r_1 i + r_2 j + r_3 k)) \\
&= (s_o - r_o m)^2 + (s_1 - r_1 m)^2 + (s_2 - r_2 m)^2 + (s_3 - r_3 m)^2 \\
&= t_o^2 + t_1^2 + t_2^2 + t_3^2 \\
&< 4\left(\frac{m}{2}\right) \\
&= m^2
\end{aligned}$$

Damit folgt die Hilfsbehauptung. Setze nun $m = N(\beta) = \beta\overline{\beta}$ (möglich da β nach Voraussetzung ungerade) und $\sigma = \alpha\overline{\beta}$. Wegen der Hilfsbehauptung findet man ein $\gamma \in \mathbb{H}(\mathbb{Z})$ mit

$$\begin{aligned}
m^2 > N(\sigma - \gamma m) &= N(\alpha\overline{\beta} - \gamma\beta\overline{\beta}) \\
&= N(\alpha - \gamma\beta)N(\overline{\beta})
\end{aligned}$$

Und es gilt

$$\begin{aligned}
N(\beta)N(\overline{\beta}) &= N(\beta\overline{\beta}) = N(N(\beta)) \\
&= N(m) = m^2
\end{aligned}$$

Zusammenführt dies zu folgender Aussage

$$\begin{aligned}
&N(\beta)N(\overline{\beta}) > N(\alpha - \gamma\beta)N(\overline{\beta}) \;\; |: N(\overline{\beta}) \\
&\Leftrightarrow \; N(\beta) > \underbrace{N(\alpha - \gamma\beta)}_{=:\delta}
\end{aligned}$$

Mit $\gamma = r_0 + r_1 i + r_2 j + r_3 k$ und $\delta = \alpha - \gamma\beta$ sind für beliebige $\alpha, \beta \in \mathbb{H}(\mathbb{Z})$ mit β ungerade Quaternionen, die $\alpha = \gamma\beta + \delta$ und $N(\delta) < N(\beta)$ erfüllen, gefunden. □

Bevor im folgenden Lemma eine Möglichkeit bewiesen wird, wie man eine Quaternion eindeutig zerlegen kann, wird noch eine Hilfsrechnung für den Beweis benötigt.

Bemerkung 2.14 (Hilfsrechnung).

1. Durch Multplikation von $\alpha = a_0 + a_1 i + a_2 j + a_3 k$ von rechts mit einer Einheit ε lässt sich ein anderes a_i mit $i = 1, 2, 3$ an die 0. Stelle schieben. (Dabei werden die Vorzeichen nicht beachtet.)
   Fall: a_1 soll an die 0. Stelle.
   $(a_0 + a_1 i + a_2 j + a_3 k) \cdot i = a_0 i + a_1(-1) + a_2(-k) + a_3 j$
   Fall a_2 soll an die 0. Stelle
   $(a_0 + a_1 i + a_2 j + a_3 k) \cdot j = a_0 j + a_1 k + a2(-1) + a_3(-i)$
   Fall: a_3 soll an die 0. Stelle
   $(a_0 + a_1 i + a_2 j + a_3 k) \cdot k = a_0 k + a_1(-j) + a_2 i + a_3(-1)$
2. Durch Multiplikation von $\alpha = a_0 + a_1 i + a_2 j + a_3 k$ mit $a_i \neq 0$ für alle $i = 0, 1, 2, 3$ mit einer Einheit erhält man stets eine Quaternion mit wieder vier Komponenten die ungleich 0 sind.
   Dies ist an folgenden Gleichungen zu sehen:

$$
\begin{aligned}
|1 \cdot 1| = |1| \ , |1 \cdot i| = |i| \ , |1 \cdot j| = |j| \ , |1 \cdot k| = |k| \\
|i \cdot 1| = |i| \ , |i \cdot i| = |1| \ , |i \cdot j| = |k| \ , |i \cdot k| = |j| \\
|j \cdot 1| = |j| \ , |j \cdot i| = |k| \ , |j \cdot j| = |1| \ , |j \cdot k| = |i| \\
|k \cdot 1| = |k| \ , |k \cdot i| = |j| \ , |k \cdot j| = |i| \ , |k \cdot k| = |1|
\end{aligned}
$$

Lemma 2.15. *Sei $\alpha \in \mathbb{H}(\mathbb{Z})$. Dann gibt es eine eindeutige Zerlegung von α folgender Art:*

$$\alpha = 2^l \pi \alpha_0$$

mit $l \in \mathbb{N}$, $\pi \in \{1, 1+i, 1+j, 1+k, (1+i)(1+j), (1+i)(1-k)\}$ und $\alpha_0 \in \mathbb{H}(\mathbb{Z})$ ungerade.

Beweis. Zunächst wird die Existenz einer solchen Zerlegung für ein festes α gezeigt.
Wähle l größtmöglich, dass 2^l teilt α.
Sei $\alpha' := \frac{\alpha}{2^l}$ mit

$$\alpha' = a_0 + a_1 i + a_2 j + a_3 k$$

Ein a_i muss ungerade sein, sonst hätte man l größer gewählt. Falls a_0 noch nicht ungerade ist, können wir α' mit einer Einheit multiplizieren um ein ungerades a_i an die 0. Stelle zu schieben. Wir nehmen also an, dass a_0 ungerade ist.
Nun müssen zwei Fälle unterschieden werden:
Fall 1 α' ist ungerade und
Fall 2 α' ist gerade.
Fall 1
Wir können schreiben $\alpha = 2^l \alpha'$. Dies stellt bereits eine Zerlegung wie im Lemma gefordert dar, da α' ungerade ist und π wird 1 gesetzt.
Fall 2
Wir unterscheiden wiederum zwei Fälle:
Fall (a): $N(\alpha') \equiv 2 (mod 4)$ und
Fall (b) $N(\alpha') \equiv 0 (mod 4)$.
Fall (a)
Wegen $a_i^2 = 1$ (mod4) (falls a_i ungerade) und $a_i^2 = 0$ (mod4) (falls a_i gerade) sind im Fall (a) genau zwei a_i ungerade (a_0 und ein weiterer) und zwei a_i gerade.
Seien zunächst a_0 und a_1 ungerade. Dann ist mit

$$
\begin{aligned}
\alpha_0 &= \frac{a_0 + a_1}{2} + \frac{a_1 - a_0}{2} i + \frac{a_2 + a_3}{2} j + \frac{a_3 - a_2}{2} k \\
\pi &= (1 + i)
\end{aligned}
$$

eine Zerlegung, wie im Lemma gefordert, gegeben.

α_0 ist ungerade, denn:

$$\begin{aligned}
N(\alpha_0) &= \left(\frac{a_o + a_1}{2}\right)^2 + \left(\frac{a_1 - a_0}{2}\right)^2 + \left(\frac{a_2 + a_3}{2}\right)^2 + \left(\frac{a_3 - a_2}{2}\right)^2 \\
&= \frac{1}{4}(2a_0^2 + 2a_1^2 + 2a_2^2 + 2a_3^2) \\
&= \frac{1}{2}(a_0^2 + a_1^2 + a_2^2 + a_3^2) \\
&\equiv \frac{1}{2}(1 + 1 + 0 + 0)(mod 4) \\
&\equiv 1(mod 4) \\
&\Rightarrow \ \alpha_0 \ ungerade
\end{aligned}$$

$\alpha' = (1 + i)\alpha_0$, denn:

$$\begin{aligned}
&(1 + i)\alpha_0 \\
&= (1 + i)\left(\frac{a_0 + a_1}{2} + \frac{a_1 - a_0}{2}i + \frac{a_2 + a_3}{2}j + \frac{a_3 - a_2}{2}k\right) \\
&= \frac{a_0 + a_1}{2} + \frac{a_0 - a_1}{2} + \frac{a_0 + a_1}{2}i + \frac{a_1 - a_0}{2}i + \frac{a_2 + a_3}{2}j + \frac{a_2 - a_3}{2}j + \frac{a_2 + a_3}{2}k + \frac{a_3 - a_2}{2}k \\
&= \frac{2a_0}{2} + \frac{2a_1}{2}i + \frac{2a_2}{2}j + \frac{2a_3}{2}k \\
&= a_0 + a_1 i + a_2 j + a_3 k \\
&= \alpha'
\end{aligned}$$

Seien nun a_0 und a_2 ungerade. Dann ist mit

$$\begin{aligned}
\alpha_0 &= \frac{a_0 + a_2}{2} + \frac{a_1 - a_3}{2}i + \frac{a_2 - a_0}{2}j + \frac{a_3 + a_1}{2}k \\
\pi &= (1 + j)
\end{aligned}$$

eine Zerlegung, wie im Lemma gefordert, gegeben.
α_0 ist ungerade, denn:

$$\begin{aligned}
N(\alpha_0) &= \left(\frac{a_0 + a_2}{2}\right)^2 + \left(\frac{a_1 - a_3}{2}\right)^2 + \left(\frac{a_2 - a_0}{2}\right)^2 + \left(\frac{a_3 + a_1}{2}\right)^2 \\
&= \frac{1}{4}(2a_0^2 + 2a_1^2 + 2a_2^2 + 2a_3^2) \\
&\Rightarrow \ \alpha_0 \text{ ungerade (siehe Rechnung im Fall } a_0, a_1 \text{ungerade)}
\end{aligned}$$

$\alpha' = (1 + j)\alpha_0$, denn:

$$\begin{aligned}
&(1 + j)\alpha_0 \\
&= (1 + j)\left(\frac{a_0 + a_2}{2} + \frac{a_0 - a_3}{2}i + \frac{a_2 - a_0}{2}j + \frac{a_3 + a_1}{2}k\right) \\
&= \frac{a_0 + a_2}{2} + \frac{a_0 - a_2}{2} + \frac{a_1 - a_3}{2}i + \frac{a_3 + a_1}{2}i + \frac{a_2 - a_0}{2}j + \frac{a_0 + a_2}{2}j + \frac{a_3 + a_1}{2}k + \frac{a_3 - a_1}{2}k \\
&= \frac{2a_0}{2} + \frac{2a_1}{2}i + \frac{2a_2}{2}j + \frac{2a_3}{2}k \\
&= a_0 + a_1 i + a_2 j + a_3 k \\
&= \alpha'
\end{aligned}$$

Seien nun a_0 und a_3 ungerade. Dann ist mit

$$\begin{aligned}
\alpha_0 &= \frac{a_0 + a_3}{2} + \frac{a_1 + a_2}{2}i + \frac{a_2 - a_1}{2}j + \frac{a_3 - a_0}{2}k \\
\pi &= (1 + k)
\end{aligned}$$

eine Zerlegung, wie im Lemma gefordert, gegeben.
α_0 ist ungerade, denn:

$$\begin{aligned} N(\alpha_0) &= \left(\frac{a_0+a_3}{2}\right)^2 + \left(\frac{a_1+a_2}{2}\right)^2 + \left(\frac{a_2-a_1}{2}\right)^2 + \left(\frac{a_3-a_0}{2}\right)^2 \\ &= \frac{1}{4}(2a_0^2+2a_1^2+2a_2^2+2a_3^2) \\ &\Rightarrow \ \alpha_0 \text{ ungerade (siehe Rechnung im Fall } a_0, a_1 \text{ungerade)} \end{aligned}$$

$\alpha' = (1+k)\alpha_0$, denn:

$$\begin{aligned} &(1+k)\alpha_0 \\ &= (1+k)\left(\frac{a_0+a_3}{2} + \frac{a_1+a_2}{2}i + \frac{a_2-a_1}{2}j + \frac{a_3-a_0}{2}k\right) \\ &= \frac{a_0+a_3}{2} + \frac{a_0-a_3}{2} + \frac{a_1+a_2}{2}i + \frac{a_1-a_2}{2}i + \frac{a_2-a_1}{2}j + \frac{a_1+a_2}{2}j + \frac{a_3-a_0}{2}k + \frac{a_0+a_3}{2}k \\ &= \frac{2a_0}{2} + \frac{2a_1}{2}i + \frac{2a_2}{2}j + \frac{2a_3}{2}k \\ &= a_0 + a_1 i + a_2 j + a_3 k \\ &= \alpha' \end{aligned}$$

Kommen wir nun zum Fall (b) mit $N(\alpha') \equiv 0(\text{mod}4)$
Wegen $a_i^2 = 1$ (mod4) (falls a_i ungerade) und $a_i^2 \equiv 0$ (mod4) (falls a_i gerade) und a_0 ungerade sind alle a_i ungerade, also $a_i \equiv 1(\text{mod}4)$ oder $a_i \equiv -1(\text{mod}4)$ $\forall\ i = 0,1,2,3$.
In mod4 gerechnet, gibt es dann 16 Möglichkeiten für α'. Wir unterschieden diese in 2 Gruppen:

$$\begin{aligned} \textit{Gruppe } 1: \ & 1+1i+1j+1k \\ & 1+1i+(-1)j+(-1)k \\ & 1+(-1)i+1j+(-1)k \\ & 1+(-1)i+(-1)j+1k \\ & (-1)+(-1)i+1j+1k \\ & (-1)+1i+(-1)j+1k \\ & (-1)+1i+1j+(-1)k \\ & (-1)+(-1)i+(-1)j+(-1)k \\ \textit{Gruppe } 2: \ & (-1)+1i+1j+1k \\ & 1+(-1)i+1j+1k \\ & 1+1i+(-1)j+1k \\ & 1+1i+1j+(-1)k \\ & 1+(-1)i+(-1)j+(-1)k \\ & (-1)+1i+(-1)j+(-1)k \\ & (-1)+(-1)i+1j+(-1)k \\ & (-1)+(-1)i+(-1)j+1k \end{aligned}$$

Gruppe 1 umfasst alle Möglichkeiten für α', die eine gerade Anzahl an a_i haben mit $a_i \equiv 1(\text{mod}4)$ (also 0,2 oder 4 Stück). Falls α' diese Form hat für ein festes α, dann kann man zeigen, dass ein α_1 existiert mit $\alpha' = (1+i)(1+j)\alpha_1$. (Sei dies unsere Hilfsbehauptung 1) Damit wird dann eine Zerlegung wie im Lemma gefordert gefunden sein, mit $\pi = (1+i)(1+j)$ und $\alpha_0 = \alpha_1$.
Gruppe 2 umfasst alle Möglichkeiten für α', die eine ungerade Anzahl an a_i haben mit $a_i \equiv 1(\text{mod}4)$ (also 1 oder 3 Stück). Falls α' diese Form hat für ein festes α. Dann kann man zeigen, dass ein α_1 existiert mit $\alpha' = (1+i)(1-k)\alpha_1$. (Sei dies unsere Hilfsbehauptung 2) Damit wird dann eine Zerlegung wie im Lemma gefordert gefunden sein, mit $\pi = (1+i)(1-kj)$ und $\alpha_0 = \alpha_1$.
Um den Beweis der Existenz abzuschließen beweisen wir nun die beiden Hilfsbehauptungen.
Hilfsbehauptung 1:
Beweis: Gehört das α' zur 1. Gruppe (ist also eine gerade Anzahl der a_i (0,2,4) $\equiv 1$ (mod4)),

so existiert eine ungerade Quaternion α_1 mit $\alpha' = (1+i)(1+j)\alpha_1$.
Für die 8 Fälle gilt entweder bereits $a_0 \equiv 1 \pmod 4$, ansonsten multiplizieren wir mit der Einheit (-1) und erhalten dadurch ebenfalls eine Quaternion, für die gilt $a_0 \equiv 1 \pmod 4$:

$$\begin{aligned}
((-1)+(-1)i+1j+1k)(-1) &= 1+1i+(-1)j+(-1)k \\
((-1)+1i+(-1)j+1k)(-1) &= 1+(-1)i+1j+(-1)k \\
((-1)+1i+1j+(-1)k)(-1) &= 1+(-1)i+(-1)j+1k \\
((-1)+(-1)i+(-1)j+(-1)k)(-1) &= 1+1i+1j+1k
\end{aligned}$$

Wir unterscheiden nun 3 Fälle:
Fall A: $a_0 \equiv a_1 \equiv 1 \pmod 4$ und $a_2 \equiv a_3 \equiv \pm 1$
($a_2 \equiv a_3$ gilt da in der 1. Hilfsbehauptung nur Quaternionen mit einer geraden Anzahl an Koeffizienten mit $\equiv 1 \pmod 4$betrachtet werden.)
Fall B: $a_0 \equiv a_2 \equiv 1 \pmod 4$ und $a_1 \equiv a_3 \equiv \pm 1 \pmod 4$
Fall C: $a_0 \equiv a_3 \equiv 1 \pmod 4$ und $a_1 \equiv a_2 \equiv \pm 1 \pmod 4$
Nun zu Fall A: Wir können das α' in $\alpha = (1+i)\alpha_0$ mit

$$\alpha_0 = \frac{a_0+a_1}{2} + \frac{a_1-a_0}{2}i + \frac{a_2+a_3}{2}j + \frac{a3-a_2}{2}k$$

zerlegen.

$$\begin{aligned}
&(1+i)\left(\frac{a_0+a_1}{2} + \frac{a_1-a_0}{2}i + \frac{a_2+a_3}{2}j + \frac{a3-a_2}{2}k\right) \\
&= \frac{a_0+a_1}{2} + \frac{a_1-a_0}{2}i + \frac{a_2+a_3}{2}j + \frac{a3-a_2}{2}k \\
&+ \frac{a_0+a_1}{2}i + \frac{a_1-a_0}{2}(-1) + \frac{a_2+a_3}{2}(k) + \frac{a_3-a_2}{2}(-j) \\
&= \frac{2a_0}{2} + \frac{2a_1}{2}i + \frac{2a_2}{2}j + \frac{2a_3}{2}k \\
&= a_0 + a_1 i + a_2 j + a_3 k \\
&= \alpha'
\end{aligned}$$

α_0 ist nicht ungerade, daher ist noch nicht die geforderte Zerlegung gefunden. $\frac{a_0+a_1}{2}$ und $\frac{a_2+a_3}{2}$ sind ungerade, $\frac{a_1-a_0}{2}$ und $\frac{a_3-a_2}{2}$ sind gerade. Also hat α_0 die 0. und 2. Komponente ungerade und die 1. und 3. Komponente gerade und fällt damit in Fall 2(a). Wir finden also eine ungerade Quaternion α_1 mit $\alpha_0 = (1+j)\alpha_1$.
$\Rightarrow \alpha' = (1+i)(1+j)\alpha_0$. Die gewünschte Darstellung mit $\pi = (1+i)(1+j)$ ist damit gefunden. Falls die Quaternionen zu Anfang mit (-1) abgeändert wurden, verändert sich nur geringfügig die Darstellung (aber wir finden eine).

$$\begin{aligned}
\alpha'(-1) &= (1+i)(1+j)\alpha_0 \\
\Leftrightarrow \alpha' &= (1+i)(1+j)(\alpha_0(-1))
\end{aligned}$$

Dabei handelt es sich um eine Darstellung wie im Lemma gefordert, da $N(\alpha_0) = N(\alpha_0(-1)) = N(\alpha_0)$.
Fall B:
$a_0 \equiv a_2 \equiv 1 \pmod 4$ und $a_1 \equiv a_3 \equiv \pm 1 \pmod 4$
Wir können das α' in $\alpha' = (1+j)\alpha_0$ mit

$$\alpha_0 = \frac{a_0+a_2}{2} + \frac{a_1-a_3}{2}i + \frac{a_2-a_0}{2}j + \frac{a_3+a_1}{2}k$$

zerlegen.

$$\begin{aligned}
&(1+j)\left(\frac{a_0+a_2}{2}+\frac{a_1-a_3}{2}i+\frac{a_2-a_0}{2}j+\frac{a_3+a_1}{2}k\right)\\
&=\frac{a_0+a_2}{2}+\frac{a_1-a_3}{2}i+\frac{a_2-a_0}{2}j+\frac{a_3+a_1}{2}k\\
&+\frac{a_0+a_2}{2}j+\frac{a_1-a_3}{2}(-k)+\frac{a_2+a_0}{2}(-1)+\frac{a_3+a_1}{2}(i)\\
&=\frac{2a_0}{2}+\frac{2a_1}{2}i+\frac{2a_2}{2}j+\frac{2a_3}{2}k\\
&=a_0+a_1i+a_2j+a_3k\\
&=\alpha'
\end{aligned}$$

α_0 ist nicht ungerade, daher ist noch nicht die geforderte Zerlegung gefunden. $\frac{a_0+a_1}{2}$ und $\frac{a_3+a_1}{2}$ sind ungerade, $\frac{a_1-a_3}{2}$ und $\frac{a_2-a_0}{2}$ sind gerade. Also hat α_0 die 0. und 3. Komponente ungerade und die 1. und 2. Komponente gerade und fällt damit in Fall 2(a). Wir finden also eine ungerade Quaternion α_1 mit $\alpha_0=(1+k)\alpha_1$.

$$\begin{aligned}
\Rightarrow \alpha' &= (1+j)\alpha_0 = (1+j)(1+k)\alpha_1\\
&= (1+i)(1+j)\alpha_1\\
\text{da } (1+j)(1+k) &= (1+i)(1+j)\\
\Leftrightarrow\ 1+i+j+k &= 1+i+j+k
\end{aligned}$$

Damit ist eine gewünschte Zerlegung mit $\pi=(1+i)(1+j)$ gefunden. Die Abänderung durch eine Einheit läuft genauso wie im Fall A ab.
Fall C:
$a_0\equiv a_3\equiv 1\ (\text{mod}4)$ und $a_1\equiv a_2\equiv\pm 1\ (\text{mod}4)$
Wir können das α' in $\alpha'=(1+k)\alpha_0$ mit

$$\alpha_0=\frac{a_0+a_3}{2}+\frac{a_1+a_2}{2}i+\frac{a_2-a_1}{2}j+\frac{a_3-a_0}{2}k$$

zerlegen.

$$\begin{aligned}
&(1+k)\left(\frac{a_0+a_3}{2}+\frac{a_1+a_2}{2}i+\frac{a_2-a_1}{2}j+\frac{a_3-a_0}{2}k\right)\\
&=\frac{a_0+a_3}{2}+\frac{a_1+a_2}{2}i+\frac{a_2-a_1}{2}j+\frac{a_3-a_0}{2}k\\
&+\frac{a_0+a_3}{2}k+\frac{a_1+a_2}{2}j+\frac{a_2-a_1}{2}(-i)+\frac{a_3-a_0}{2}(-1)\\
&=\frac{2a_0}{2}+\frac{2a_1}{2}i+\frac{2a_2}{2}j+\frac{2a_3}{2}k\\
&=a_0+a_1i+a_2j+a_3k\\
&=\alpha'
\end{aligned}$$

α_0 ist nicht ungerade, daher ist noch nicht die geforderte Zerlegung gefunden. $\frac{a_0+a_3}{2}$ und $\frac{a_1+a_2}{2}$ sind ungerade, $\frac{a_2-a_1}{2}$ und $\frac{a_3-a_0}{2}$ sind gerade. Also hat α_0 die 0. und 1. Komponente ungerade und die 2. und 3. Komponente gerade und fällt damit in Fall 2(a). Wir finden also eine ungerade Quaternion α_1 mit $\alpha_0=(1+i)\alpha_1$.

$$\begin{aligned}
\Rightarrow \alpha' &= (1+k)(1+i)\alpha_1\\
&= (1+i)(1+j)\alpha_1\\
\text{da } (1+k)(1+i) &= (1+i)(1+j)\\
\Leftrightarrow 1+i+j+k &= 1+i+j+k
\end{aligned}$$

Die gewünschte Darstellung mit $\pi=(1+i)(1+j)$ ist damit gefunden. Die Abänderung durch eine Einheit läuft genauso wie im Fall A ab.
Damit ist die Hilfsbehauptung 1 gezeigt.

Hilfsbehauptung 2:
Gehört das α' zur 2. Gruppe (ist also eine ungerade Anzahl der a_i (1,3) $\equiv 1$ (mod4)), so existiert eine ungerade Quaternion α_1 mit $\alpha' = (1+i)(1-k)\alpha_1$.
Beweis der Hilfsbehauptung: Für die 8 Fälle aus Gruppe 2 gilt entweder bereits, dass 3 der $a_i \equiv 1$ (mod4) sind, darunter a_0 oder wir können sie mit einer Einheit multiplizieren, sodass dies der Fall ist:

$$\begin{aligned}((-1)+1i+1j+1k)(-i) &= 1+1i+(-1)j+1k\\ (1+(-1)i+(-1)j+(-1)k)(i) &= 1+1i+(-1)j+1k\\ ((-1)+1i+(-1)j+(-1)k)(-1) &= 1+(-1)i+1j+1k\\ ((-1)+(-1)i+1j+(-1)k)(-1) &= 1+1i+(-1)j+1k\\ ((-1)+(-1)i+(-1)j+1k)(i) &= 1+(-1)i+1j+1k\end{aligned}$$

Wir betrachten 3 verschiedene Fälle:
Fall A: $a_0 \equiv a_1 \equiv a_2 \equiv 1$ (mod4) und $a_3 \equiv -1$ (mod4)
Fall B: $a_0 \equiv a_1 \equiv a_3 \equiv 1$ (mod4) und $a_2 \equiv -1$ (mod4)
Fall C: $a_0 \equiv a_2 \equiv a_3 \equiv 1$ (mod4) und $a_1 \equiv -1$ (mod4)
α' lässt sich in jedem Fall in $\alpha' = (1+i)\alpha_0$ zerlegen mit:

$$a_0 = \frac{a_0+a_1}{2} + \frac{a_1-a_0}{2}i + \frac{a_2+a_3}{2}j + \frac{a_+3-a_2}{2}k$$

Das dies zutrifft, haben wir bereits in der Hilfsbehauptung 1 im Fall A gesehen.
Wir bezeichnen die Komponenten von α_0 mit:

$$\begin{aligned}b_0 &:= \frac{a_0+a_1}{2}\\ b_1 &:= \frac{a_1-a_0}{2}\\ b_2 &:= \frac{a_2+a_3}{2}\\ b_3 &:= \frac{a_3-a_2}{2}\end{aligned}$$

Im Fall A sind b_o und b_3 ungerade und b_1 und b_2 gerade. Dies erkennt man an einer Rechnung in mod4.

$$\begin{aligned}b_0 = \frac{a_0+a_1}{2} \equiv \frac{1+1}{2} \equiv 1 \Rightarrow\ & b_0\text{ungerade}\\ b_1 = \frac{a_1-a_0}{2} \equiv \frac{1-1}{2} = 0 \Rightarrow\ & b_1\text{gerade}\\ b_2 = \frac{a_2+a_3}{2} \equiv \frac{1-1}{2} = 0 \Rightarrow\ & b_2\text{gerade}\\ b_3 = \frac{a_3-a_2}{2} \equiv \frac{-1-1}{2} \equiv -1 \Rightarrow\ & b_3\text{ungerade}\\ \Rightarrow \alpha_0 \text{ ist gerade, da } N(\alpha_0) = b_0^2+b_1^2+b_2^2+b_3^2 &\equiv 1+0+0+1 \equiv 2\text{mod } 4\end{aligned}$$

Also stellt $\alpha' = (1+i)\alpha_0$ noch keine Zerlegung wie im Lemma gefordert dar. Wir können α_0 aber in $\alpha_0 = (1-k)\alpha_1$ mit

$$\alpha_1 = \left(\frac{b_0-b_3}{2} + \frac{b_1-b_2}{2}i + \frac{b_1+b_2}{2}j + \frac{b_0+b_3}{2}k\right)$$

zerlegen.

$$\begin{aligned}(1-k)\alpha_1 = (1-k)\left(\frac{b_0-b_3}{2} + \frac{b_1-b_2}{2}i + \frac{b_1+b_2}{2}j + \frac{b_0+b_3}{2}k\right)\\ = \frac{b_0-b_3}{2} + \frac{b_1-b_2}{2}i + \frac{b_1+b_2}{2}j + \frac{b_0+b_3}{2}k\\ + \frac{b_0-b_3}{2}(-k) + \frac{b_1-b_2}{2}(-j) + \frac{b_1+b_2}{2}i + \frac{b_0+b_3}{2}\\ = b_0+b_1i+b_2j+b_3k = \alpha_1\end{aligned}$$

$\Rightarrow \alpha' = (1+i)(1-k)\alpha_1$
Wir können $\pi = (1+i)(1-k)$ setzten. Es bleibt zu überprüfen, dass α_1 ungerade ist. Wir nehmen die Norm:

$$\begin{aligned} N(\alpha_0) &= N(1-k)N(\alpha_1) \\ \Rightarrow\ 2 &\equiv 2N(\alpha_1) \bmod 4 \\ \Rightarrow\ N(\alpha_1) &\equiv 1 \bmod 4 \\ \Rightarrow\ \alpha_1 &\text{ist ungerade.} \end{aligned}$$

Im Fall B und C könnten wir α' genauso in $(i+1)\alpha_0$ zerlegen, mit α_0 wie in Fall A. Weiter können wir α_0 ebenfalls in $(1-k)\alpha_1$ zerlegen, wobei α_1 genauso wie in Fall A definiert ist. Man muss nur überprüfen, dass $b_0, b_1, b_2, b_3 \in \mathbb{Z}$. Dies lässt sich wie in Fall A, an einer Rechnung in mod 4 sehen, dabei stellt man fest, dass in Fall B b_0 und b_3 ungerade sind und b_1 und b_2 gerade und im Fall C b_1 und b_2 ungerade sind und b_0 und b_3 gerade sind. Nun gilt noch zu überprüfen, dass $\alpha_1 \in \mathbb{H}(\mathbb{Z})$ ist, das also $(b_0 - b_3), (b_1 - b_2), (b_1 + b_2)$ und $b_0 + b_3$ im Fall B und C gerade ganze Zahlen sind. In jedem Fall wird entweder eine ungerade Zahl von einer ungeraden subtrahiert oder zwei gerade bzw. zwei ungerade Zahlen addiert. In mod 2 betrachtet finden also folgende Rechnungen statt:

$$\begin{aligned} 1 - 1 &\equiv 0 \\ 0 + 0 &\equiv 0 \\ 1 + 1 = 2 &\equiv 0 \end{aligned}$$

Man erhält also nur gerade Zahlen wie gefordert. Im Fall A wurde bereits gezeigt, dass α_1 ungerade ist, wie es für die Darstellung im Lemma gefordert ist, gezeigt, ohne Eigenschaften von α' zu benutzen, die für Fall A spezifisch sind. Die Existenz einer solchen Zerlegung ist hiermit also für alle $\alpha \in \mathbb{H}(\mathbb{Z})$ gezeigt.
Nun wird die Eindeutigkeit dieser Zerlegung bewiesen:
Für diesen Beweisteil benötigen wir die Norm für die verschiedenen π:

$$\begin{aligned} N(1) &= 1 \\ N(1+i) &= 2 \\ N(1+j) &= 2 \\ N(1+k) &= 2 \\ N((1+i)(1+j)) &= 4 \\ N((1+i)(1-k)) &= 4 \end{aligned}$$

Wir werden nun annehmen, dass ein beliebiges α zwei verschiedene Zerlegungen nach Art dieses Lemmas hat und diese Annahme zum Widerspruch führen:

$$\alpha = 2^l \pi \alpha_0 = 2^k \tilde{\pi} \tilde{\alpha_0}$$

Im folgenden werden wir den Fall 1: α ungerade und Fall 2: α gerade unterscheiden.
Fall 1: α ungerade
In diesem Fall ist $\alpha = 1 \cdot \alpha$ eine mögliche Zerlegung. Sei $2^l \pi \alpha_0$ eine weitere beliebige Zerlegung. Da α ungerade folgt direkt $l = 0$. Nun nehmen wir die Norm der Zerlegung und betrachten sie in mod 2:

$$\begin{aligned} N(\alpha) &= N(\pi)N(\alpha_0) \\ \Rightarrow\ 1 &\equiv N(\pi) \cdot 1 \bmod 2 \text{ (da } \alpha, \alpha_0 \text{ ungerade sind)} \\ \Rightarrow\ N(\pi) = 1 &\Rightarrow \pi = 1 \text{ siehe oben die Normen der } \pi\text{'s} \\ &\Rightarrow \alpha_0 = \alpha \end{aligned}$$

Damit folgt, dass die Zerlegung im Fall 1 eindeutig ist.
Fall 2: α gerade
Sei $\alpha = 2^l \pi \alpha_0 = 2^k \tilde{\pi} \tilde{\alpha_0}$ Behauptung: k und l müssen maximal gewählt werden und es gilt also

l=k.
Angenommen man würde k nicht maximal wählen. Dann enthielte eine Primfaktorzerlegung von $\tilde{\pi}\tilde{\alpha_0}$ den Faktor 2^r mit $r \in \mathbb{N}$. Da die Norm von $\tilde{\pi}\tilde{\alpha_0}$ also gerade ist und $\tilde{\alpha_0}$ ungerade nach Vorraussetzung, gilt $\tilde{\pi} \neq 1$. $\tilde{\pi}$ ist also entweder prim (d.h. $\tilde{\pi} = (1+i), (1+j), (1+k)$), dann könnte es aber nicht 2^r als Faktor enthalten. Es müsste also gelten $\tilde{\pi} = (1+i)(1+j) = 1+i+j+k$ oder $\tilde{\pi} = (1+i)(1-k) = 1+i-j-k$. Es müsste also eine Quaternion β geben mit $1+i+j+k = 2^r \cdot \beta$ bzw. mit $1+i-j-k = 2^r \cdot \beta$. Dies ist offensichtlich nicht der Fall. Also müsste $\tilde{\alpha_0}$ den Faktor 2^r enthalten, damit wäre $\tilde{\alpha_0}$ allerdings gerade, was einen Widerspruch darstellt. Daraus folgt, dass l=k gelten muss.
$\Rightarrow \pi\alpha_0 = \tilde{\pi}\tilde{\alpha_0}$
Wir unterscheiden wiederum zwei Fälle: Fall I: $\pi\alpha_0$ ungerade und Fall II: $\pi\alpha_0$ gerade.
Zu Fall I:
$N(\pi)N(\alpha_0)$ und $N(\tilde{\pi})N(\tilde{\alpha_0})$ sind ungerade
$\Rightarrow N(\pi)$ und $N(\tilde{\pi})$ sind ungerade.
$\Rightarrow \pi = \tilde{\pi} = 1$ Also gilt auch α_0=$\tilde{\alpha_0}$ und damit ist die Zerlegung in Fall I eindeutig.
Zu Fall II:
$\pi\alpha_0$ und $\tilde{\pi}\tilde{\alpha_0}$ sind nun gerade und folglich muss damit $\pi, \tilde{\pi}$ auch gerade sein, da $\alpha_0, \tilde{\alpha_0}$ nach Vorraussetzung ungerade sind. Das bedeutet $\pi \neq 1 \neq \tilde{\pi}$.
Behauptung: $N(\pi) = N(\tilde{\pi})$
Wäre $N(\tilde{\pi}) = 4$ im Fall von $N(\pi) = 2$ dann würde folgen:

$$\begin{aligned} N(\pi)N(\alpha_0) &= N(\tilde{\pi})N(\tilde{\alpha_0}) \\ \Rightarrow\ 2N(\alpha_0) &= 4N(\tilde{\alpha_0}) \\ \Leftrightarrow\ N(\alpha_0) &= 2N(\tilde{\alpha_0}) \end{aligned}$$

Daraus folgt, dass α_0 gerade ist, was ein Widerspruch zur Annahme darstellt. Damit ist bereits die Behauptung gezeigt, da sich die Rollen von π und $\tilde{\pi}$ beliebig vertauschen lassen.
Aus $N(\pi) = N(\tilde{\pi})$ folgt dann $N(\alpha_0) = N(\tilde{\alpha_0})$.
Nun unterscheiden wir bzgl. der Norm von π zwei Fälle: Fall A: $N(\pi) = 2$ und Fall B: $N(\pi) = 4$.
Zu Fall A: $\pi, \tilde{\pi} \in \{(1+i), (1+j), (1+k)\}$
Wir wollen zeigen, dass gelten muss $\pi = \tilde{\pi}$. Daraus folgt dann direkt, dass $\alpha_0 = \tilde{\alpha_0}$ gilt und somit, dass die Zerlegung eindeutig ist. Der Beweis wird durch eine Gegenannahme geführt: es gelte also $\pi = 1+i$ und $\tilde{\pi} = 1+j$ oder $\pi = 1+i$ und $\tilde{\pi} = 1+k$ oder $\pi = 1+j$ und $\tilde{\pi} = 1+k$. Es reicht diese drei Fälle zu betrachten, da man die Rollen von π und $\tilde{\pi}$ vertauschen kann.
Im ersten Fall gilt dann also $(1+i)\alpha_0 = (1+j)\tilde{\alpha_0}$. $(1+j)$ ist eine prime Quaternione und muss daher in einer Primfaktorzerlegung von $((1+i)\alpha_0)$ vorkommen, teilt also $(1+i)$ oder α_0. Da $(1+j)$ und $(1+i)$ nicht assoziiert zueinander sind und $(1+i)$ ebenfalls prim, kann $(1+j)$ die Quaternion $(1+i)$ nicht teilen, also müsste $(1+j)$ die Quaternion α_0 teilen. Die Norm von $(1+j)$ (=2) teilt nicht die Norm von α_0 (ungerade). Mit folgender Hilfsbehauptung folgt dann direkt, dass $(1+j)$ nicht α_0 teilt und damit stoßen wir auf einen Widerspruch. In den anderen beiden Fällen läuft die Argumentation ganz genauso ab, man muss nur einsehen, dass $(1+i)$ und $(1+j)$ bzw. $(1+j)$ und $(1+k)$ nicht zueinander assoziiert sind und alle prim.
Hilfsbehauptung: Seien $\alpha, \beta \in \mathbb{H}(\mathbb{Z})$ Falls $N(\alpha)$ nicht $N(\beta)$ teilt, dann folgt, dass α nicht β in $\mathbb{H}(\mathbb{Z})$ teilt.
Beweis: Angenommen es gäbe ein $\gamma \in \mathbb{H}(\mathbb{Z})$ mit $\beta = \gamma\alpha$. Dann würde gelten: $N(\beta) = N(\gamma)N(\alpha)$
$\Rightarrow N(\alpha)$ teilt $N(\beta)$. Dies ist ein Widerspruch zur Annahme und damit ist die Hilfsbehauptung bewiesen.
Nun zum Fall B: $\pi \in \{(1+i)(1+j), (1+i)(1-k)\}$
Wir wollen die Gegenannahme machen, dass $\pi = (1+i)(1+j)$ und $\tilde{\pi} = (1+i)(1-k)$. Aus dem Widerspruch, den wir herleiten werden, wird dann folgen, dass $\pi = \tilde{\pi}$ und damit, dass die Zerlegung nach Art des Lemmas eindeutig ist.
Es gelte also $(1+i)(1+j)\alpha_0 = (1+i)(1-k)\tilde{\alpha_0}$. $\Rightarrow (1+j)\alpha_0 = (1-k)\tilde{\alpha_0}$. Da $(1-k)$ ebenfalls prim und nicht assoziiert zu $(1+j)$ kommen wir genau wie im Fall A auf einen Widerspruch.
□

Als nächstes wollen wir unter bestimmten Umständen die Existenz des größten gemeinsamen rechtsseitigen Teilers zeigen. Dies führt uns zur rechtsseitigen Abwandlung des Euklidischen Algorithmus. Die Eindeutigkeit (bis auf Assoziiertheit) des größten gemeinsamen rechtsseitigen Teilers folgt direkt aus der Definition. Dafür müssen wir noch eine bestimmte Menge definieren.

Definition 2.16. Sei $\mathbb{Z}[\frac{1}{2}] = \{\frac{k}{2^n} : k \in \mathbb{Z}, n \in \mathbb{N}\}$. Es handelt sich um einen Untering von den rationalen Zahlen.

Satz 2.17. *Seien $\alpha, \beta \in \mathbb{H}(\mathbb{Z})$, β ungerade.*
Dann existiert der größte gemeinsame rechtsseitige Teiler $(\alpha, \beta)_r$ und $\exists \gamma, \delta \in \mathbb{H}(\mathbb{Z}[\frac{1}{2}])$ mit $(\alpha, \beta)_r = \gamma\alpha + \delta\beta$.

Beweis. Da β ungerade, finden wir nach Lemma 2.12 $\gamma_0, \delta_0 \in \mathbb{H}(\mathbb{Z})$ mit $N(\delta_0) < N(\beta)$ und

$$\alpha = \gamma_0\beta + \delta_0$$

Mit Lemma 2.15 finden wir dann für δ_0: $l_0 \in \mathbb{N}$, $\pi_0 \in \{1, 1+i, 1+j, 1+k, (1+i)(1+j), (1+i)(1-k)\}$ und $\delta_0' \in \mathbb{H}(\mathbb{Z})$ ungerade, sodass

$$\begin{aligned} \delta_0 &= 2^{l_0}\pi_0\delta_0' \\ \Rightarrow \mathbb{N}(\delta_0') \leq N(\delta_0) &< N(\beta) \text{ (Da die Norm multiplikativ ist)} \end{aligned}$$

Gleichheit gilt falls $\pi_0 = 1$ und $l_0 = 0$. Dann erhalten wir durch erneutes Anwenden von Lemma 2.12 auf β und δ_0' (ist ungerade), dass $\exists\ \gamma_1, \delta_1$ mit $N(\delta_1) < N(\delta_0')$ und

$$\beta = \gamma_1\delta_0' + \delta_1$$

Mit Lemma 2.15 finden wir dann für δ_1: $l_1 \in \mathbb{N}$, $\delta_1' \in \mathbb{H}(\mathbb{Z})$ und $\pi_1 \in \{1, 1+i, 1+j, 1+k, (1+i)(1+j), (1+i)(1-k)\}$, sodass

$$\begin{aligned} \delta_1 &= 2^{l_1}\pi_1\delta_1' \\ \Rightarrow\ N(\delta_1') \leq N(\delta_1) &< N(\delta_0') \end{aligned}$$

Durch wiederholtes Anwenden von Lemma 2.12 und Lemma 2.15 erhält man

$$\begin{aligned} \delta_{i-1}' &= \gamma_{i+1}\delta_i' + \delta_{i+1} \\ \text{und } \delta_{i+1} &= 2^{l_{i+1}}\pi_{i+1}\delta_{i+1}' \\ \text{mit } N(\delta_{i+1}') \leq N(\delta_{i+1}) < N(\delta_i') &\text{ mit } \delta_{i+1}' \text{ ist ungerade} \\ &\forall i \in \mathbb{N}\ mit\ \delta_{i+1} \neq 0 \end{aligned}$$

Wir erhalten

$$\begin{aligned} N(\delta_0) \geq N(\delta_0') > N(\delta_1) \geq N(\delta_1') > &..... \\ \Rightarrow\ N(\delta_0) > N(\delta_1) > &N(\delta_2).... \end{aligned}$$

eine streng monoton fallende Folge.
$\Rightarrow$ $\exists$ *ein* $k \in \mathbb{N}$ mit $\delta_{k+1} = 0$. Dieses k wird kleinstmöglich gewählt. Die letzten beiden Gleichungen sind dann folgende:

$$\begin{aligned} \delta_{k-2}' &= \gamma_k\delta_{k-1}' + \delta_k \\ \delta_{k-1}' &= \gamma_{k+1}\delta_k' + 0 \end{aligned}$$

Behauptung: $\delta_k' = (\alpha, \beta)_r$
Zu zeigen

1. δ_k' ist rechtsseitiger Teiler von α, β
2. Ist δ ein weiterer rechtsseitiger Teiler von α, β, dann folgt, dass δ ein rechtsseitiger Teiler von δ_k' ist.

Zu 1. (mit *teilt* ist stets rechtsseitiges teilen gemeint)
δ_k' teilt δ_{k-1}' (wegen $\delta_{k-1}' = \gamma_{k+1}\delta_k'$)
und δ_k' teilt δ_k (wegen $\delta_k = 2^{l_k}\pi_k\delta_k'$)
$\Rightarrow$ δ_k' teilt δ_{k-2}' (wegen $\delta_{k-2}' = \gamma_k\delta_{k-1}' + \delta_k$)
Durch Iteration folgt:
δ_k' teilt β und δ_k' teilt α.

Zu 2. Sei δ ein beliebiger rechtsseitiger Teiler von α und β. Aus $\alpha = \gamma_0\beta + \delta_0 (\Leftrightarrow \alpha - \gamma_0\beta = \delta_0)$ folgt, dass δ ein rechtsseitiger Teiler von δ_0 ist. Für δ_0 erhält man mit Lemma 2.15 die eindeutige Darstellung $2^{l_0}\pi_0\delta_0'$ und da δ rechtsseitiger Teiler von δ_0 ist $\exists\ \gamma$ mit $\delta_0 = \gamma\delta = 2^{l_j}\pi_j\gamma'\delta$ mit $\gamma' \in \mathbb{H}(\mathbb{Z})$ ungerade
$\Rightarrow \delta_0 = 2^{l_j}\pi_j(\gamma'\delta) = 2^{l_0}\pi_0\delta_0'$ und da die Darstellung nach Lemma 2.15 eindeutig ist folgt $l_j = l_0$ und $\pi_j = \pi_0$
$\Rightarrow \delta_0' = \gamma'\delta \Rightarrow$ δ ist ein rechtsseitiger Teiler von δ_0. Iterativ folgt dann, dass δ: $\delta_1, \delta_1', \delta_2, \delta_2' ... \delta_k, \delta_k'$ teilt.
$\Rightarrow \delta_k'$ ist größter gemeinsamer Teiler von α und β.

Die vorigen Gleichungen können wir umschreiben zu:

$$\begin{aligned}
\delta_0' &= 2^{-l_0}{\pi_0}^{-1}(\alpha - \gamma_0\beta) \\
\delta_1' &= 2^{-l_1}{\pi_1}^{-1}(\alpha - \gamma_1\delta_0') \\
&... \\
\delta_k' &= 2^{-l_k}{\pi_k}^{-1}(\delta_{k-2}' - \gamma_k\delta_{k-1}')
\end{aligned}$$

Wir erhalten aus der letzten Gleichung eine Gleichung der Form $\delta_k' = \gamma\alpha + \delta\beta$ mit $\gamma, \delta \in \mathbb{H}(\mathbb{Z}[\frac{1}{2}])$, wenn wir sukzessive die δ_i' jeweils durch $2^{-l_i}{\pi_i}^{-1}(\delta_{i-2}' - \gamma_i\delta_{i-1})$ ersetzen und danach α und β ausklammern. Wir können uns nicht auf eine Darstellung mit $\delta, \gamma \in \mathbb{H}(\mathbb{Z})$ beschränken, da π_i und 2^{l_i} keine Inversen in $\mathbb{H}(\mathbb{Z})$ haben. In $\mathbb{H}(\mathbb{Z}[\frac{1}{2}])$ ist dies aber sehr wohl der Fall, folgendes sind die Inversen:

$\frac{1}{2^i}$ für 2^i
1 für 1
$(\frac{1}{2}) - \frac{1}{2}i)$ für $(1+i)$
$(\frac{1}{2}) - \frac{1}{2}j)$ für $(1+j)$
$(\frac{1}{2}) - \frac{1}{2}k)$ für $(1+k)$
$(\frac{1}{2} - \frac{1}{2}j)(\frac{1}{2} - \frac{1}{2}k)$ für $(1+i)(1+j)$
$(\frac{1}{2} + \frac{1}{2}k)(\frac{1}{2} - \frac{1}{2}i)$ für $(1+i)(1-k)$

□

Lemma 2.18. *Sei $\alpha \in \mathbb{H}(\mathbb{Z})$ und $m \in \mathbb{Z}$ ungerade.*

$$(m, \alpha)_r = 1 \ \Leftrightarrow\ (m, N(\alpha))_r = 1$$

Beweis. Wir beginnen mit der Hinrichtung. Es gelte also $(m, \alpha)_r = 1$ für ein $\alpha \in \mathbb{H}(\mathbb{Z})$ und ein $m \in \mathbb{Z}$ ungerade.
Nach dem letzten Satz 2.17 $\exists\ \gamma, \delta \in \mathbb{Z}[\frac{1}{2}]$ mit

$$\begin{aligned}
(m, \alpha)_r = 1 = \gamma m + \delta\alpha & \\
\Rightarrow\ N(1) &= N(\gamma m)N(\delta\alpha) \\
\Leftrightarrow\ N(\delta)N(\alpha) &= N(1 - \gamma m) \\
&= (1 - \gamma m)\overline{(1 - \gamma m)} \\
&= (1 - \gamma m)(1 - m\overline{\gamma}) \\
&= 1 - (\gamma + \overline{\gamma})m + N(\gamma)m^2 \\
&\Rightarrow 1 = N(\delta)N(\alpha) + (\gamma + \overline{\gamma})m - N(\gamma)m^2
\end{aligned}$$

Da $N(\delta), N(\gamma)$ und $(\gamma + \overline{\gamma}) \in \mathbb{Z}[\frac{1}{2}]$ $\exists\ k \in \mathbb{N}$ mit $2^kN(\delta),\ 2^kN(\gamma),\ 2^k(\gamma + \overline{\gamma}) \in \mathbb{Z}$
Sei nun β ein beliebiger rechtsseitiger Teiler von $N(\alpha)$ und m. Es existiert also ein γ_1 mit $m = \gamma_1\beta \Rightarrow\ m^2 = N(m) = N(\gamma_1)N(\beta)\ \Rightarrow\ \beta$ ist ungerade, da m ungerade.

Die letzte Gleichung wird mit 2^k erweitert:

$$2^k = (2^k N(\delta))N(\alpha) + (2^k(\gamma + \overline{\gamma}))m - (2^k N(\gamma))m^2$$

$\Rightarrow \beta$ ist ein rechtsseitiger Teiler von 2^k

$\Rightarrow \exists\ \gamma_2\ mit\ 2^k = \gamma_2\beta$
$\Rightarrow\ N(2^k) = N(\gamma)N(\beta)$
$\Leftrightarrow\ 2^{2k} = N(\gamma)N(\beta)$
$\Rightarrow\ N(\beta) = 1 (da\ N(\beta)\ ungerade)$

Da β beliebig gewählt war, ist somit jeder rechtsseitiger Teiler von m und $N(\alpha) = 1$. Es gilt also $(m, N(\alpha))_r = 1$
Nun wird die Rückrichtung gezeigt. Es gelte also $(m, N(\alpha))_r = 1$ für ein $\alpha \in \mathbb{H}(\mathbb{Z})$ und ein $m \in \mathbb{Z}$ ungerade.
Sei $\delta \in \mathbb{H}(\mathbb{Z})$ ein beliebiger rechtsseitiger Teiler von m und α. Wir wollen nun zeigen, dass $\delta = 1$ (bis auf Assoziiertheit) gilt.
δ teilt auch m und $N(\alpha) = \overline{\alpha}\alpha$ (wegen $\alpha = \gamma_1\delta$ für ein $\gamma_1 \in \mathbb{H}(\mathbb{Z}) \Rightarrow \overline{\alpha}\alpha = \overline{\alpha}\gamma_1\delta$) und muss somit 1 rechtsseitig teilen, da 1 der größte gemeinsame rechtsseitige Teiler von m und $N(\alpha)$ ist :
$\Rightarrow\ \exists\ \gamma$ mit $1 = \gamma\delta$
$\Rightarrow\ 1 = N(1) = N(\gamma)N(\delta)$
$\Rightarrow\ N(\delta) = 1$
Also ist δ eine Einheit, also $\delta = 1$ (bis auf Assoziiertheit). □

Lemma 2.19. *Sei $p \in \mathbb{P}$ $p \neq 2$. Es gebe ein $\alpha \in \mathbb{H}(\mathbb{Z})$ mit*
p teilt nicht α
aber p teilt $N(\alpha)$.
Dann gilt: $\delta := (\alpha, p)_r$ ist prim in $\mathbb{H}(\mathbb{Z})$ und $N(\delta) = p$.

Beweis. Es existiert ein $\gamma \in \mathbb{H}(\mathbb{Z})$ mit $p = \gamma\delta$. γ ist keine Einheit(also $N(\gamma) \neq 1$), denn ansonsten würde folgen $\delta = \gamma^{-1}p$ und da δ die Quaternion α teilt existiert ein γ_1 mit $\alpha = \gamma_1\delta$. Daraus folgt, wenn man die beiden Gleichungen zusammenfügt: $\alpha = \gamma_1\gamma_1^{-1}p$
$\Rightarrow$ p teilt α: ein Widerspruch zur Annahme.
Aus $(p, N(\alpha))_r \neq 1$ folgt mit Lemma 2.18, dass $\delta = (p, \alpha)_r \neq 1$
$\Rightarrow N(\delta) \neq 1$ (mit Lemma 2.7 über die Menge der größten gemeinsamen rechtsseitigen Teiler)
Nun können wir zeigen,dass $N(\delta) \neq p$ ist.

$$N(p) = N(\gamma\delta)$$
$$\Leftrightarrow\ p^2 = N(\gamma)N(\delta)$$
$$\text{Da p prim und } \mathbb{N}(\gamma) \neq 1 \neq N(\delta)\ \Rightarrow\ N(\gamma) = p = N(\delta)$$

Es bleibt zu zeigen, dass δ prim ist.
Sei $\delta = xy$ eine beliebige Zerlegung.
$p = N(\delta) = N(x)N(y)$
$\Rightarrow\ N(x) = 1\ oder\ N(y) = 1$
$\Rightarrow$ x oder y sind Einheiten
$\Rightarrow \delta$ ist prim. □

Im folgenden wird bewiesen, dass sich jede ungerade Primzahl in $\mathbb{Z}$ als Norm einer primen Quaternion aus $\mathbb{H}(\mathbb{Z})$ darstellen lässt. Daraus folgt insbesondere, dass eine ungerade Primzahl in $\mathbb{N}$ nicht prim in $\mathbb{H}(\mathbb{Z})$ ist.

Satz 2.20. *Für jedes $p \in \mathbb{P}$ mit $p \neq 2$ $\exists\ \delta \in \mathbb{H}(\mathbb{Z})$ prim, mit $N(\delta) = p (= \delta\overline{\delta})$.*

Beweis. Wegen Satz 1.8 gibt es $x, y \in \mathbb{Z}$ mit $1 + x^2 + y^2 \equiv 0$ (mod p).
Sei $\alpha = 1 + xi + yj$. p teilt nicht α, da p nicht 1 teilt. Aber p teilt $N(\alpha) = 1 + x^2 + y^2$. Damit folgt mit Lemma 2.19, dass $\delta := (\alpha, p)_r$ prim in $\mathbb{H}(\mathbb{Z})$ ist und $N(\delta) = p$ ist. □

Korollar 2.21. *$\delta \in \mathbb{H}(\mathbb{Z})$ ist prim in $\mathbb{H}(\mathbb{Z}) \Leftrightarrow N(\delta)$ ist prim in $\mathbb{Z}$.*

Beweis. Zunächst die Rückrichtung. (Sie ist bereits im Beweis vom Lemma 2.19 enthalten)
Sei also $N(\delta) := p$ mit $p \in \mathbb{P}$. Sei $\delta = xy$ eine beliebige Zerlegung.
Also $p = N(\delta) = N(x)N(y)$ und daraus folgt $N(x) = 1$ oder $N(y) = 1$, das bedeutet x oder y ist eine Einheit und damit ist δ prim in $\mathbb{H}(\mathbb{Z})$.
Für die Hinrichtung nehmen wir an, dass $\delta \in \mathbb{H}(\mathbb{Z})$ prim in $\mathbb{H}(\mathbb{Z})$ ist. Wir unterscheiden zwei Fälle: Fall 1 δ ist gerade und Fall 2 δ ist ungerade.
Fall 1:
Wegen Lemma 2.15 gibt es eine Zerlegung der Form

$$\begin{aligned}\delta = 2^l \pi \delta_0 \quad & mit \quad l \in \mathbb{N} \\ & \pi \in \{1, 1+i, 1+j, 1+k, (1+i)(1+j)(1+i)(1-k)\} \\ & \text{und } \delta_0 \text{ ungerade}\end{aligned}$$

Da δ prim, kann die Zerlegung $2^l \pi \delta_0$ nur aus zwei Einheiten und einer weiteren Primzahl bestehen, weil zwei assoziierte Elemente entweder beide prim oder beide nicht prim sind. 2 ist nicht prim in $\mathbb{H}(\mathbb{Z})$ $(2 = (1+i)(1-i))$, daher folgt $l = 0$. Zueinander assoziierte Elemente sind auch beide entweder gerade oder ungerade und da δ gerade in diesem Fall und δ_0 ungerade, können sie nicht zueinander assoziiert sein sondern δ_0 muss eine Einheit sein. Folglich muss π prim und gerade sein. $(1+i)(1+j), (1+i)(1-k)$ sind nicht prim und 1 ist nicht gerade $\Rightarrow \ \pi \in \{1+i, 1+j, 1+k\}$, also $N(\pi) = 2 \Rightarrow \ N(\delta) = 2 \ \Rightarrow \ N(\delta)$ ist prim in $\mathbb{Z}$.

Fall 2 (δ ist ungerade)
Sei $p \in \mathbb{P}$ mit $p \neq 2$ und p teilt $N(\delta)$. Wir wollen zeigen $N(\delta) = p$ und damit δ prim in $\mathbb{Z}$.
Sei $\alpha := (p, \delta)_r$, es $\exists$ also ein γ mit $\delta = \gamma\alpha$. Aus $(p, \alpha)_r \neq 1$ folgt mit Lemma 2.18 $(p, N(\alpha))_r \neq 1$
$\Rightarrow \ N(\alpha) \neq 1$(da $(p, \varepsilon)_r = 1 \ \forall$ Einheiten ε)
$\Rightarrow \alpha$ ist keine Einheit.
Da $\delta = \gamma\alpha$ und δ prim, folgt, dass γ eine Einheit ist. Also sind δ und α assoziiert. α teilt p und damit teilt δ p auch. Es gibt also ein $\psi \in \mathbb{H}(\mathbb{Z})$ mit $p = \psi\delta$. Wir nehmen die Norm:

$$\begin{aligned} & N(p) = N(\psi)N(\delta) \\ \Leftrightarrow \quad & p^2 = N(\psi)N(\delta) \\ \Leftrightarrow \quad & p = N(\psi)\frac{N(\delta)}{p} \\ \Rightarrow \quad & N(\psi) = 1 \text{ oder } \left(\frac{N(\delta)}{p}\right) = 1 \end{aligned}$$

Betrachten wir zunächst den Fall $N(\psi) = 1$. ψ ist also eine Einheit und daher sind p und δ assoziiert wegen $p = \psi\delta$. p muss also auch prim in $\mathbb{H}(\mathbb{Z})$ sein sein, weil δ prim in $\mathbb{H}(\mathbb{Z})$ ist. Dies führt uns allerdings zu einem Widerspruch, da die Primzahlen in $\mathbb{Z}$ nicht prim in $\mathbb{H}(\mathbb{Z})$ sind. Also muss in jedem Fall gelten $\left(\frac{N(\delta)}{p}\right) = 1$. Es folgt $N(\delta) = p$. □

Unser nächstes Ziel ist es den berühmten Satz von Lagrange zu beweisen, der aussagt, dass jede natürliche Zahl sich als Summe von vier Quadratzahlen darstellen lässt. Dazu zeigen wir zunächst ein Theorem von Jacobi, das einerseits die Aussage für ungerade natürliche Zahlen liefert und sogar zusätzlich die genaue Anzahl an Darstellungen einer bestimmten natürlichen Zahl durch 4 Quadratzahlen. (Den Beweis von Lagrange werden wir allerdings ohne die Hilfe von dem Theorem von Jacobi beweisen,was aber auch möglich wäre.)

Definition 2.22. Sei $r_k(n)$ = die Anzahl der Darstellungen für eine natürliche Zahl n als Summe von k Quadraten, also $r_k(n) = |\{(x_0, x_1, ...x_{k-1}) \in \mathbb{Z}^k : \sum_{i=0}^{k-1} {x_i}^2 = n\}|$.

Satz 2.23 (Theorem von Jacobi)**.** *Sei $n \in \mathbb{N}$ ungerade. Dann gilt $r_4(n) = 8 \sum_{d|n} d$.*

Beweis. kommt später ;-) □

Jeder dieser Darstellungen für ein bestimmtes n entspricht eine Quaternion.

Bemerkung 2.24. Für $r_4(n)$ mit n gerade, gibt es auch eine Formel:

$$r_4(n) = 8 \sum_{d|n \ d \neq 0 (mod 4)} d$$

Diese Formel lassen wir an dieser Stelle unbewiesen.[1]

Korollar 2.25 (von Lagrange)**.** *Jede natürliche Zahl lässt sich als Summe von 4 Quadratzahlen darstellen.*

Beweis. Für $n = 0$ findet man folgende Summe $0^2 + 0^2 + 0^2 + 0^2 = 0$
Für $n = 1$ findet man zum Beispiel folgende Summe $1^2 + 0^2 + 0^2 + 0^2$
Sei nun $n \geq 2$ und $n = 2^{r_0} p_1^{r_1} \cdots p_k^{r_k}$ seine Primfaktorzerlegung mit p_i ungerade $\forall\ i = 1, ...k$ und $r_i \in \mathbb{N}$ für alle $i = 0, 1, ...k$. Wegen Theorem 2.20 findet man für alle p_i ein $\delta_i \in \mathbb{H}(\mathbb{Z})$ mit $pi = N(\delta_i) = a_0^2 + a_1^2 + a_2^2 + a_3^2$ mit $a_i \in \mathbb{Z}$ und $2 = N(1+i) = 1^2 + 1^2$. Da die Norm multiplikativ ist, ergibt sich folgendes:

$$\begin{aligned} n &= 2^{r_0} N(\delta_i)^{r_1} \cdots N(\delta_k)^{r_k} \\ &= N(1+i)^{r_0} N(\delta_1^{r_1} \cdots \delta_k^{r_k}) \\ &= N((1+i)^{r_0} \delta_1^{r_1} \cdots \delta_k^{r_k}) \\ &= b_0^2 + b_1^2 + b_2^2 + b_3^2 \text{für} b_i \in \mathbb{Z} \end{aligned}$$

□

Wir haben bereits gesehen, dass die Primfaktorzerlegung in $\mathbb{H}(\mathbb{Z})$ nicht eindeutig ist (nicht mal bis auf Assoziierheit). Wir werden uns daher im folgenden nur die $\alpha \in \mathbb{H}(\mathbb{Z})$ angucken, für die gilt $N(\alpha) = p^k$ für ein $p \in \mathbb{P}$, $p \neq 2$ und ein $k \in \mathbb{N}$, weil wir am Ende für diese bestimmten Quaternionen eine Art von eindeutiger Primfaktorzerlegung finden werden. Dafür konstruieren wir uns als erstes die Menge S_p um dann mit Hilfe von reduzierten Wörter die gewünschte Zerlegung zu erhalten. Bei S_p handelt es sich um das Alphabet für die reduzierten Wörter.

Bemerkung 2.26 (Konstruktion von S_p)**.** Sei $p \in \mathbb{P}$ $p \neq 2$. Für die Darstellung $p = a_0^2 + a_1^2 + a_2^2 + a_3^2$ mit $a_i \in \mathbb{Z}$ gibt es laut Jacobis Theorem 2.23 $8(p+1)$ Möglichkeiten. Davon entspricht jede einem $\alpha \in \mathbb{H}(\mathbb{Z})$ mit $N(\alpha) = p$. Von diesen $8(p+1)$ $\alpha' s$ werden wir nach einem bestimmten Verfahren $(p+1)$ auswählen und diese Quaternionen sollen dann die Menge S_p bilden.
Zu jedem α (von den $8(p+1)$ mit $N(\alpha) = p$) gbit es 8 assoziierte der Form:
$i\alpha, -i\alpha, j\alpha, -j\alpha, k\alpha, -k\alpha, 1\alpha, -1\alpha$ (alle mit Norm p). Würde man eine andere Quaternion der 8 als Ausgangspunkt wählen, würde man die selben 8 assoziierten erhalten, da $\varepsilon_1\varepsilon_2$ mit $\varepsilon_1, \varepsilon_2$ Einheiten, wiederum eine Einheit ist. (Da $\mathbb{N}(\varepsilon_1\varepsilon_2) = N(\varepsilon_1)N(\varepsilon_2) = 1$)
So erhält man p+1 Mengen mit je 8 Quaternionen.
Wie wählen wir nun eine Quaternion aus jeder Menge aus?
Es gilt entweder $p \equiv 1(mod 4)$ oder $p \equiv 3(mod 4)$. Im ersten Fall sind drei der a_i gerade und ein a_i ungerade.(Da $a_i^2 \equiv 1(\text{mod}4)$ mit a_i ungerade und $a_i^2 \equiv 0(\text{mod}4)$ mit a_i gerade) Wir bezeichnen das eine ungerade a_i mit ${a_i}^0$. Im zweiten Fall sind drei der a_i ungerade und ein a_i gerade. Wir bezeichnen wiederum das gerade mit ${a_i}^0$.
Auswahlverfahren im Fall ${a_i}^0 = 0$
Für eine Einheit ε gilt $\varepsilon\alpha$ und $-\varepsilon\alpha$ haben 0 als 0. Komponente. Es wird eine dieser beiden ausgewählt.
$\Rightarrow$ Die Quaternionen, die aus diesem Auswahlverfahren entspringen, nennen wir b_j mit einem Index $j \in \mathbb{N}$.
Auswahlverfahren im Fall ${a_i}^0 \neq 0$
Nur eine der Quaternionen aus einer 8.-Menge wird $|{a_i}^0|$ als 0. Komponente haben. Genau diese Quaternion wird ausgewählt.
$\Rightarrow$ Wenn ein α aus diesem Auswahlverfahren entspringt, tut dies auch $\overline{\alpha}$.(Da sich eine Quaternion und ihre Konjugierte in der 0. Komponente übereinstimmen.) Daher benennen wir die Quaternionen aus diesem Verfahren α_i und $\overline{\alpha_i}$ und nummerieren sie mit dem Index $i \in \mathbb{N}$ durch.
Wir erhalten letztendlich
$S_p = \{\alpha_1, \overline{\alpha_1}, ..., \alpha_s, \overline{\alpha_s}, \beta_1, \beta_2, ...\beta_t\}$ mit α_i hat $a_0 > 0$ und β_j hat $b_0 = 0$.
Außerdem gilt $\alpha_i\overline{\alpha_i} = N(\alpha_i) = p$
und $-{\beta_j}^2 = -(b_1 i + b_2 j + b_3 k)(b_1 i + b_2 j + b_3 k) = b_1^2 + b_2^2 + b_3^2 = p$
und $|S_p| = 2s + t = p + 1$

[1] Beweis zu finden in: G.H. HARDY & E.M. WRIGHT, An introduction to the theory of numbers, 5th ed.,Clarendon Press, Oxford, 1979.

Definition 2.27 (Wort)**.** Ein Wort ω über einer Menge (hier S_p) ist eine endliche Folge $\omega = x_1x_2....x_n$ mit $n \geq 0$ und x_i aus der Menge.

Definition 2.28 (reduziertes Wort über S_p)**.** Ein reduziertes Wort über S_p ist ein Wort, dass keine Teilwörter der Form $\alpha_i\overline{\alpha_i}$, $\overline{\alpha_i}\alpha_i$ oder ${\beta_j}^2$ mit $i = 1, ...s$ und $j = 1, ...t$ besitzt.

Definition 2.29 (Länge eines Wortes)**.** Die Länge eines Wortes ist die Anzahl der Zeichen.

Lemma 2.30 (Hilfslemma zum nächsten Satz)**.** *Sei $\gamma \in S_p$, ε eine Einheit in $\mathbb{H}(\mathbb{Z})$.*
Dann existiert ein $\gamma' \in S_p$ und eine Einheit ε', sodass $\gamma\varepsilon = \varepsilon'\gamma'$

Beweis. Die Aussage ist äquivalent dazu, dass ein $\gamma' \in S_p$ und ein ε' eine Einheit existiert, mit

$$\gamma' = \varepsilon'\gamma\varepsilon$$

Sei $\gamma = (a_0 + a_1i + a_2j + a_3k) \in S_p$
Fall 1 $a_o \neq 0$
$\gamma = a_0\varepsilon + a_1i\varepsilon + a_2j\varepsilon + a_3k\varepsilon$ und $\gamma' = \varepsilon'\gamma\varepsilon = \varepsilon'a_0\varepsilon + \varepsilon'a_1i\varepsilon + \varepsilon'a_2j\varepsilon + \varepsilon'a_3k\varepsilon$.
Zu zeigen ist, dass $\gamma' \in S_p$. Dafür muss $N(\gamma') = p$ gelten, dies ist der Fall: $N(\gamma') = N(\varepsilon'\gamma\varepsilon) = N(\varepsilon')N(\gamma)N(\varepsilon) = 1 \cdot p \cdot 1$. Da $\gamma \in S_p$ ist, ist a_o das einzige a_i mit $i = 0, 1, 2, 3$, dass gerade oder ungerade ist. Einheiten haben keinen Einfluss auf die Eigenschaft gerade/ungerade, also muss auch $\varepsilon'a_0\varepsilon$ die 0.Komponente sein, damit $\gamma' \in S_p$. Gefordert ist also $\varepsilon'a_0\varepsilon = \pm a_0$. Da $a_0 \in \mathbb{Z}$: $\varepsilon'a_0\varepsilon = a_0\varepsilon'\varepsilon$. Setze $\varepsilon' = \varepsilon^{-1}$.
Fall 2 $a_0 = 0$
Es gilt genauso $N(\varepsilon'\gamma\varepsilon) = p$.
$\gamma' = \varepsilon'\gamma\varepsilon = \varepsilon'a_1i\varepsilon + \varepsilon'a_2j\varepsilon + \varepsilon'a_3k\varepsilon$. Damit $\gamma' \in S_p$ muss gelten $\varepsilon'i\varepsilon \neq \pm 1$, $\varepsilon'j\varepsilon \neq \pm 1$ und $\varepsilon'k\varepsilon \neq \pm 1$. $|i\varepsilon|, |j\varepsilon|, |k\varepsilon| \in \{1, i, j, k\}$ mit $|i\varepsilon| \neq |j\varepsilon| \neq |k\varepsilon| \neq |i\varepsilon|$. Setze $|\varepsilon'| \in \{|i\varepsilon|, |j\varepsilon|, |k\varepsilon|\}$
$\Rightarrow \varepsilon' \cdot i\varepsilon \neq \pm 1$, $\varepsilon' \cdot j\varepsilon \neq \pm 1$, $\varepsilon' \cdot k\varepsilon \neq \pm 1 \Rightarrow \gamma' \in S_p$ □

Satz 2.31. *Sei $\alpha \in \mathbb{H}(\mathbb{Z})$, $k \in \mathbb{N}$ mit $N(\alpha) = p^k$.*
Dann hat α eine eindeutige Zerlegung folgender Form:
$\alpha = \varepsilon p^r\omega_m$ mit ε eine Einheit in $\mathbb{H}(\mathbb{Z})$, ω_m ein reduziertes Wort mit Länger m über S_p und $r \in \mathbb{N}$ mit $k = 2r + m$.

Beweis. Wegen Satz 2.9 lässt sich α als Produkt von primen Quaternionen δ_i (mit $N(\delta_i)$ ist prim in $\mathbb{Z}$) schreiben:
$\alpha = \delta_1....\delta_n$
Nehmen wir die Norm erhalten wir: $p^k = N(\delta_1)...N(\delta_n)$
Da $N(\delta_i)$ prim in $\mathbb{Z}$ erhalten wir $N(\delta_i) = p$ und $n = k$.
Da $N(\delta_i) = p$ finden wir ein $\gamma_i \in S_p$ und eine Einheit ε, sodass $\delta_i = \varepsilon_i\gamma_i$.
α lässt sich also folgendermaßen schreiben:
$\alpha = \varepsilon_1\gamma_1\varepsilon_2\gamma_2....\varepsilon_k\gamma_k$ mit $\gamma_i \in S_p$ und ε_i eine Einheit. Mit dem Hilfslemma 2.30 finden wir jeweils ein γ_i' und ein ε_i' mit $\varepsilon_i\gamma_i = \gamma_i'\varepsilon_i'$.
$\Rightarrow$ α lässt sich schreiben als $\alpha = \varepsilon\gamma_1'....\gamma_k'$.
$\gamma_1'....\gamma_k'$ ist zwar ein Wort aber noch kein reduziertes. Wir verschieben jeden Faktor $\alpha_i\overline{\alpha_i}$, $\overline{\alpha_i}\alpha_i$ oder ${\beta_i}^2$ $(= p)$ nach links und wiederholen diesen Prozess solange bis wir ein reduziertes Wort erhalten.
$\Rightarrow \alpha = \varepsilon p^r\omega_m$ wobei ω_m ein reduziertes Wort ist, r die Anzahl der Faktoren, die hinaus gezogen worden sind und jeweils das Wort um 2 verkürzt haben. Daher gilt $k = 2r + m$.
Hiermit ist die Existenz gezeigt, nun zur Eindeutigkeit.
Wir werden die Anzahl der $\alpha \in \mathbb{H}(\mathbb{Z})$ mit $N(\alpha) = p$ bestimmen und die Anzahl der Darstellungen $\varepsilon p^r\omega_m$ mit ε eine Einheit, $k = 2r + m$ und ω_m ein reduziertes Wort über S_p. Wir werden festestellen, dass diese beiden Anzahlen gleich groß sind, daher muss für ein α diese Darstellung (deren Existenz wir bereits gezeigt haben) eindeutig sein.
1) Anzahl der α
Laut dem Theorem von Jacobi 2.23 gibt es davon

$$8\sum_{d|p^k} d = 8\left(\sum_{i=0}^{k} p^i\right) = (\text{geom. Reihe}) = 8\left(\frac{1-p^{k+1}}{1-p}\right) = 8\left(\frac{p^{k+1}-1}{p-1}\right)$$

da ein α genau einer Darstellung von p^k mit 4 Quadratzahlen entspricht.
2) Anzahl der Darstellungen der Form $\varepsilon p^r \omega_m$
Die Anzahl der reduzierten Wörter mit Länger m über S_p:

$$\begin{cases} 1 & \text{falls } m = 0 \\ (p+1)p^{m-1} & \text{falls } m \geq 1 \end{cases}$$

Dies kommt zustande, da man für den 1. Buchstaben $p+1$ Möglichkeiten hat ($|S_p|$) und für jeden weiteren Buchstaben p. (Da wir Teilwörter der Form $\alpha_i\overline{\alpha_i}, \overline{\alpha_i}\alpha_i$ oder ${\beta_j}^2$ vermeiden). Damit ergibt sich für die Anzahl der Darstellungen der Form $\varepsilon p^r \omega_m$ folgendes:

$$\begin{cases} 8\left(1+\sum_{r=0}^{\frac{k}{2}-1}(p+1)p^{\overbrace{(k-2r)}^{=m}-1}\right) & \text{falls k gerade} \\ 8\left(\sum_{r=0}^{\frac{k-1}{2}}(p+1)p^{\overbrace{(k-2r)}^{=m}-1}\right) & \text{falls k ungerade} \end{cases}$$

wobei 8 die Möglichkeiten der Wahl der Einheit wieder gibt. Falls k gerade ist, gibt es für m folgende Möglichkeiten $k, k-2, ...2, 0$. Da $2r+m=k$ kann m jeweils nur um eine gerade Anzahl kleiner sein als k. Da $m = k-2r$ durchläuft die Summe genau diese m mit Ausnahme von $m=0$. Die Möglichkeiten für $m=0$ erhält man durch die Addition der 1. Falls k ungerade ist gibt es folgende Möglichkeiten für m: $k, k-2, ...3, 1$. Genau diese m durchläuft die Summe. Für den Beweis des Satzes bleibt nun zu zeigen:

$$8\left(1+\sum_{r=0}^{\frac{k}{2}-1}(p+1)p^{(k-2r)-1}\right) = 8\left(\sum_{r=0}^{\frac{k-1}{2}}(p+1)p^{(k-2r)-1}\right) = 8\left(\frac{p^{k+1}-1}{p-1}\right)$$

$$\Leftrightarrow \left(1+\sum_{r=0}^{\frac{k}{2}-1}(p+1)p^{(k-2r)-1}\right) = \left(\sum_{r=0}^{\frac{k-1}{2}}(p+1)p^{(k-2r)-1}\right) = \left(\frac{p^{k+1}-1}{p-1}\right)$$

Also:

$$
\begin{aligned}
&\left(1+\sum_{r=0}^{\frac{k}{2}-1}(p+1)p^{(k-2r)-1}\right)\\
&=\left(1+\sum_{r=0}^{\frac{k}{2}-1}p^k(p^{-2})^r+p^k(p^{-2})^rp^{-1}\right)\\
&=\left(1+p^k\left(\sum_{r=0}^{\frac{k}{2}-1}(p^{-2})^r\right)+p^{k-1}\left(\sum_{r=0}^{\frac{k}{2}-1}(p^{-2})^r\right)\right)\\
(\text{geom. Summe})&=\left(1+(p^k+p^{k-1})\left(\frac{1-(p^{-2})^{(\frac{k}{2}-1)+1}}{1-(p^{-2})}\right)\right)\\
&=\left(1+(p^k+p^{k-1})\left(\frac{1-p^{-k}}{1-p^{-2}}\right)\right)\\
&=\left(1+\frac{p^k-1+p^{k-1}-p^{-1}}{1-p^{-2}}\right)\ \Big|\cdot p^2\\
&=\left(1+\frac{p^{k+2}-p^2+p^{k+1}-p}{\underbrace{p^2-1}_{=(p+1)(p-1)}}\right)\ \Big|\text{Polynomdivision durch } (p+1)\\
&=\left(\frac{p-1}{p-1}+\frac{p^{k+1}-p}{p-1}\right)\\
&=\left(\frac{p^{k-1}-1}{p-1}\right)
\end{aligned}
$$

Und

$$
\begin{aligned}
&\sum_{r=0}^{\frac{k-1}{2}}(p+1)p^{(k-2r)-1}\\
&=\sum_{r=0}^{\frac{k-1}{2}}p^k(p^{-2})^r+p^{k-1}(p^{-2})^r\\
(geom.Summe)&=(p^k+p^{k-1})\left(\frac{1-(p^{-2})^{\frac{k-1}{2}+1}}{1-(p^{-2})}\right)\\
&=(p^k+p^{k-1})\left(\frac{1-p^{-k+1-2}}{1-(p^{-2})}\right)\\
&=\frac{p^k-p^{-1}+p^{k-2}-p^{-2}}{1-p^{-2}}\ \Big|\cdot p^2\\
&=\frac{p^{k+2}-p+p^{k+1}-1}{\underbrace{p^2-1}_{=(p+1)(p-1)}}\ \Big|\text{Polynomdivision durch } (p+1)\\
&=\frac{p^{k+1}-1}{p-1}
\end{aligned}
$$

□

Beispiel 2.32. Für $k=2$ und $\alpha=13$ mit $N(\alpha)=13^2$ trifft das Theorem zu und man hat folgende eindeutige Zerlegung:

$13 = 1 \cdot 13^1$ mit $\varepsilon = 1$ und dem leeren Wort.
$13 = (1 + 2i + 2j + 2k)(1 - 2i - 2j - 2k) = (3 + 2i)(3 - 2i)$ sind zwar auch Zerlegungen von 13, aber es handelt sich jeweils nicht um reduzierte Wörter, da dort ein Faktor der Form $\alpha\overline{\alpha}$ vorkommt.

Wir definieren nun noch eine Teilmenge von $\mathbb{H}(\mathbb{Z})$, in der wir die eben bewiesene eindeutige Zerlegung für α aus ganz $\mathbb{H}(\mathbb{Z})$ noch verfeinern wollen.

Definition 2.33 (von Λ)**.** Sei Λ eine Teilmenge von $\mathbb{H}(\mathbb{Z})$ mit
$\Lambda = \{\alpha = a_0 + a_1 i + a_2 j + a_3 k : N(\alpha) = p^k$ für *ein* $k \in \mathbb{N}$, $\alpha \equiv 1(mod 2)$ *oder* $\alpha \equiv i + j + k(mod 2)\}$
Es gilt S_p ist Teilmenge von Λ. Und mit einer Rechnung in mod2 sieht man schnell, dass Λ multiplikativ abgeschlossen ist:

$$\begin{aligned} 1 \cdot 1 &= 1 \\ 1 \cdot (i + j + k) &= i + j + k \\ (i + j + k) \cdot 1 &= i + j + k \\ (i + j + k)(i + j + k) &= -1 - k + j + k - 1 - i - j + i - 1 = -3 = 1 \end{aligned}$$

Für ein Produkt $\alpha\beta$ mit $\alpha, \beta \in \Lambda$ bleibt auch die Bedingung bzgl. der Norm gültig, denn $N(\alpha\beta) = N(\alpha)N(\beta) = p^{k_1} \cdot p^{k_2} = p^{k_1 + K_2}$ für $k_1, k_2 \in \mathbb{N}$

Korollar 2.34. *Sei $\alpha \in \Lambda$ mit $N(\alpha) = p^k$. α hat ein eindeutige Zerlegung der Form: $\alpha = \pm p^r \omega_m$ mit $r \in \mathbb{N}$ und ω_m ein reduziertes Wort der Länge m über S_p und es gilt $k = 2r + m$.*

Beweis. Wegen Theorem 2.31 finden wir eine Zerlegung folgender Form:
$\alpha = \varepsilon p^r \omega_m$ wobei ε eine Einheit ist und ω_m ein reduziertes Wort. Wir betrachten diese Zerlegung in mod2:
$\varepsilon p^r \omega_m \equiv \varepsilon \omega_m$
Für alle $\alpha_i, \beta_i \in S_p$ gilt $\equiv 1(mod 2)$ oder $\equiv i + j + k$. Es gilt $(i + j + k)(i + j + k) = 1(mod 2)$.

$$\alpha = \begin{cases} \varepsilon & \text{falls gerade Anzahl an Elementen in } \omega_m \ \equiv (i + j + k) \\ \varepsilon(i + j + k) & \text{falls ungerade Anzahl an Elementen in } \omega_m \ \equiv (i + j + k) \end{cases}$$

Da $\alpha \in \Lambda$ muss gelten $\alpha \equiv 1(mod 2)$ oder $\alpha \equiv i + j + k(mod 2)$
$\Rightarrow \ \varepsilon = 1(mod 2)$
$\Rightarrow \ \varepsilon = \pm 1$
Damit erhält man die gewünschte eindeutige Zerlegung. □

Bibliographie

1. G.DAVIDOFF & P.SARNAK & A.VALETTE, Elementary Number Theory, Group Theory, and Ramunujan Graphs, London Mathematical Society, Student Texts 55, 2003, Kapitel 2.

2. S.BOSCH, Algebra, Springer Spektrum, 8.Auflage,2010.