Seminar Gruppentheorie und Geometrie SS 2016

Quaternionen

13.06.2016

Cheng Hu Shan (E-Mail: c.shan@web.de)

20. Juni 2016

Inhaltsverzeichnis

Einleitung

Dies ist die Ausarbeitung der Kapitel 2.5 und 2.6 (bzw. 2.4 und 2.5 nach Nummerierung des pdf) des Buches Elementary Number Theory, Group Theory, and Ramanujan Graphs von Davidoff, Sarnak und Vallette für das Seminar Gruppentheorie und Geometrie. Das gesamte zweite Kapitel steht leicht isoliert zum Rest des Buches, da es sich hier um die Betrachtung des zahlentheoretischen Problems handelt, ob und wie oft sich natürliche Zahlen als Summen von Quadratzahlen darstellen lassen.
In den Kapiteln 2.5 und 2.6 wird der Ring der Quaternionen über $\mathbb{Z}$ betrachtet, eingeleitet über das Problem, ob man natürliche Zahlen als Summen von genau vier Quadratzahlen schreiben kann. Die Idee ist es, sich Faktorisierungen im Ring der Quaternionen genauer zu betrachten. Während die Primzerlegung analog zu den natürlichen Zahlen kein befriedigendes Ergebnis liefert, wird schließlich gezeigt, dass bestimmte Quaternionen sich vor allem als Produkt aus reduzierten Wörtern schreiben lassen.

1 Quaternion

1.1 Definition

Sei R ein kommutativer Ring mit Eins. Die hamiltonische Quaternionen Algebra über R $\mathbb{H}(R)$ ist eine assoziative Algebra mit Neutralelement mit folgenden Eigenschaften:

- $\mathbb{H}(R)$ ist der freie R Modul mit der Basis 1, i, j, k in der Form $\mathbb{H}(R) = \{a_0 + a_1 i + a_2 j + a_3 k : a_0, a_1, a_2, a_3 \in \mathbb{R}\}$
- 1 ist das multiplikative Neutralelement
- $i^2 = j^2 = k^2 = -1$
- $ij = -ji = k; jk = -kj = i; ki = -ik = j$

Der Ring der Quaternionen über $\mathbb{Z}$ ist nicht kommutativ.

1.2 Definition

Das zu einem Quaternion $q = a_0 + a_1 i + a_2 j + a_3 k$ konjugierte Quaternion $\bar{q}$ ist definiert als $\bar{q} = a_0 - a_1 i - a_2 j - a_3 k$.
Die Norm eines Quaternions q wird definiert als

$$N(q) = q\bar{q} = \bar{q}q = a_0^2 + a_1^2 + a_2^2 + a_3^2.$$

und es gilt für q_1, $q_2 \in \mathbb{H}(R)$,

$$N(q_1 q_2) = N(q_1)N(q_2)$$

Weil die Norm als Produkt von zueinander konjugierten Quaternionen definiert ist, kann man die letzte Gleichung beweisen, in dem man ausnutzt, dass $\overline{q_1 q_2} = \overline{q_2 q_1}$ gilt, was wiederum durch Ausmultiplizieren gezeigt werden kann.

1.3 Proposition

Sei K ein Körper, der nicht die Charakteristik 2 hat. Seien x, $y \in K$, sodass $x^2 + y^2 + 1 = 0$. Dann ist $\mathbb{H}(K)$ isomorph zu der Algebra $M_2(K)$ der 2x2 Matrizen über K.

Beweis.
Sei ψ: $\mathbb{H}(K) \to M_2(K)$ definiert als

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

Es gilt $\psi(q_1 q_2) = \psi(q_1)\psi(q_2)$ für q_1,$q_2 \in \mathbb{H}(K)$. Da ψ eine k-lineare Abbildung zwischen zwei K-Vektorräumen der Dimension vier ist, muss nur gezeigt werden, dass ψ injektiv ist, sodass ψ ein Isomorphismus ist.

Betrachte den Kern $\psi(a_0 + a_1 i + a_2 j + a_3 k) = 0$. Ein lineares Gleichungssystem ist eindeutig lösbar genau dann, wenn die dazugehörige Koeffizientenmatrix eine Determinante ungleich 0 hat.. Die Matrix hat die Determinante:

$$det \begin{pmatrix} 1 & x & 0 & y \\ 0 & -y & 1 & x \\ 0 & -y & -1 & x \\ 1 & -x & 0 & -y \end{pmatrix} = -4(x^2 + y^2) = 4 \neq 0,$$

da die Charakteristik von K ungleich 2 ist. Somit enthält der Kern genau ein Element und die Abbildung ist bijektiv.

1.4 Proposition

Sei q eine ungerade Primzahlpotenz. Dann existieren x, $y \in \mathbb{F}_q$, so dass $x^2 + y^2 + 1 = 0$ erfüllt wird.

Beweis.
Es wird zunächst gezeigt, dass es in $\mathbb{F}_q$ genau $\frac{q+1}{2}$ Quadratzahlen gibt, wenn man die Null mitzählt. Betrachte den Gruppenhomomorphismus
f: $(\mathbb{F}_q - \{0\}, *) \to (\mathbb{F}_q - \{0\}, *)$ mit $n \mapsto n^2$, $n \in \mathbb{F}_q - \{0\}$. Dessen Kern enthält genau die Zahlen ± 1. Nach dem Homomorphie-Satz hat das Bild genauso viele Elemente wie die Definitionsmenge geteilt durch die Anzahl der Elemente im Kern. Fügt man noch die $\{0\}$ hinzu, so hat man genau $\frac{q+1}{2}$ Quadratzahlen.

Nun werden die Mengen

$$A_+ = \{1 + x^2 : x \in \mathbb{F}_q\}; A_- = \{-y^2 : y \in \mathbb{F}_q\}$$

betrachtet. Sie enthalten jeweils $\frac{q+1}{2}$ Elemente. Die Schnittmenge der Mengen A_+ und A_- kann nicht leer sein, da sonst die die Vereinigung die Anzahl der Zahlen im Körper übersteigt. Folglich gibt es mindestens eine Zahl, die gestellte Gleichung erfüllt.

2 Arithmetik der Quaternionen

2.1 Bemerkung

Im Folgenden beschränkt man sich auf den Ring $\mathbb{H}(\mathbb{Z})$. Die Einheiten des Ringes sind genau ± 1, $\pm i$, $\pm j$ und $\pm k$. Dies gilt, da die Norm multiplikativ ist und die Norm immer eine positive natürliche Zahl ist.

2.2 Definitionen

- Ein Quaternion $\alpha \in \mathbb{H}(\mathbb{Z})$ ist ungerade/gerade, wenn ihre Norm eine ungerade/gerade ganze Zahl ist.
- Ein Quaternion $\alpha \in \mathbb{H}(\mathbb{Z})$ ist prim, wenn α keine Einheit in $\mathbb{H}(\mathbb{Z})$ ist und wenn immer gilt $\alpha = \beta\gamma$ in $\mathbb{H}(\mathbb{Z})$, dann ist entweder β oder γ eine Einheit.
- Zwei Quaternionen α, α' sind zueinander assoziiert, wenn Einheiten ε, ε' existieren, so dass $\alpha' = \varepsilon\alpha\varepsilon'$.
- $\delta \in \mathbb{H}(\mathbb{Z})$ ist ein rechtsseitiger Teiler von $\alpha \in \mathbb{H}(\mathbb{Z})$, wenn es ein γ aus $\mathbb{H}(\mathbb{Z})$ gibt, so dass $\alpha = \gamma\delta$.

2.3 Proposition

Jedes Quaternion $\alpha \in \mathbb{H}(\mathbb{Z})$ kann als Produkt von Primquaternionen geschrieben werden.

Beweis.
Man beweist dies durch eine Induktion über die Norm $N(\alpha)$. Der Fall $N(\alpha) = 1$ ist trivial. Folglich betrachte $N(\alpha) > 1$. Wenn α bereits prim ist, gibt es nichts zu zeigen. Andernfalls schreibe $\alpha = \beta\gamma$ in $\mathbb{H}(\mathbb{Z})$ so, dass weder β noch γ Einheiten in $\mathbb{H}(\mathbb{Z})$ sind. Da die Norm multiplikativ ist gilt nun $N(\beta) < N(\alpha)$ und $N(\gamma) < N(\alpha)$. Nach Induktionsannahme sind nun β und γ Produkte aus Primzahlen und somit auch α.

2.4 Bemerkung

Die Primzerlegung in $\mathbb{H}(\mathbb{Z})$ ist nicht eindeutig, auch nicht eindeutig bis auf Assoziierte. Beispielsweise gilt:

$$13 = (1 + 2i + 2j + 2k)(1 - 2i - 2j - 2k) = (3 + 2i)(3 - 2i)$$

Dass die Faktoren von 13 wirklich Primquaternionen sind, sieht man mithilfe von Korollar (2.12).

2.5 Lemma: Teilen mit Rest

Sei α und $\beta \in \mathbb{H}(\mathbb{Z})$ und β ungerade. Dann existieren γ, $\delta \in \mathbb{H}(\mathbb{Z})$ derart, dass

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

Beweis
Man beweist zuerst folgende Behauptung: Sei $\sigma = s_0 + s_1 i + s_2 j + s_3 k \in \mathbb{H}(\mathbb{Z})$ und m

sei eine ungerade positive Zahl. Dann existiert ein $\gamma \in \mathbb{H}(\mathbb{Z})$ so, dass $N(\sigma - \gamma m) < m^2$. Man findet zu jedem s_i ein r_i aus $\mathbb{Z}$ so, dass gilt

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

Diese Ungleichungen sind echt, da m ungerade ist. Setzt man nun $s_i = mr_i + t_i$ mit $|t_i| < \frac{m}{2}$ und $\gamma = r_0 + r_1 i + r_2 j + r_3 k$. Dies führt dazu, dass

$$N(\sigma - \gamma m) = t_0^2 + t_1^2 + t_2^2 + t_3^2 < 4\left(\frac{m}{2}\right)^2 = m^2$$

gilt, was diese Behauptung beweist.

Um das Lemma zu beweisen, setzt man nun $m = N(\beta) = \beta\bar{\beta}$ und $\sigma = \alpha\bar{\beta}$. Aufgrund der Behauptung gilt nun:

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

Setzt man nun $\delta = \alpha - \gamma\beta$ und kürzt $N(\overline{\beta})$, erhält man wie gewünscht $N(\delta) < N(\beta)$.

2.6 Definition

Seien α, β Quaternionen. Man nennt $\delta \in \mathbb{H}(\mathbb{Z})$ den größten gemeinsamen rechtsseitiger Teiler von α und β (im Folgenden als $(\alpha, \beta)_r$ notiert), wenn gilt

- δ ist ein rechtsseitiger Teiler von α und β,
- wenn δ_0 ein weiterer rechtsseitiger Teiler von α und β ist, dann ist δ_0 auch ein rechtsseitiger Teiler von δ.

Im Ring der Quaternionen $\mathbb{H}(\mathbb{Z})$ sind die größten gemeinsamen rechtsseitigen Teiler nur eindeutig bis auf Assoziierte und existieren nicht notwendigerweise zu jedem Zahlenpaar α und β.

2.7 Lemma: Faktorisierung

Sei $\alpha \in \mathbb{H}(\mathbb{Z})$. Dann hat α die eindeutige Faktorisierung

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

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

Beweis
Existenz
Sei $\alpha \in \mathbb{H}(\mathbb{Z})$ beliebig, sei 2^l die höchste Potenz von 2, die α teilt. Man setzt nun $\alpha' = \frac{\alpha}{2^l}$ und schreibt es als

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

so, dass eines der a_is ungerade ist, da so viele Potenzen von 2 wie möglich bereits entfernt sind. Multiplikation mit Einheiten vertauscht die Position der a_is. Man kann deshalb annehmen, dass a_0 ungerade ist. Ist α ungerade, dann setze $\alpha = 2^l\alpha'$ und man ist fertig. Deshalb sei α gerade und man kann zwei Fälle unterscheiden

Fall (a) $N(\alpha') \equiv 2(\text{mod. } 4)$

Dann sind genau zwei der a_is ungerade, eines davon sei a_0. Wenn beispielsweise a_0 und a_1 ungerade sind, dann setze

$$\alpha_0 = \frac{a_0 + a_1}{2} + \left(\frac{a_1 - a_2}{2}\right) i + \left(\frac{a_2 + a_3}{2}\right) j + \left(\frac{a_2 - a_3}{2}\right) k.$$

α_0 ist in $\mathbb{H}(\mathbb{Z})$, ist ungerade und es gilt $\alpha' = (1+i)\alpha_0$. Die anderen Möglichkeiten (a_0 und a_2 sind ungerade, a_0 und a_3 sind ungerade) benötigen jeweils die Faktoren (1+j) oder (1+k) und können analog bestimmt werden.

Fall (b) $N(\alpha') \equiv 0(\text{mod. } 4)$

In diesem Fall sind alle a_is ungerade. Man betrachtet nun die Situation als Summe modulo 4. Die ungeraden Zahlen sind $\equiv \pm 1(\text{mod. } 4)$. Betrachtet man alle Kombinationen von Kongruenzen modulo 4, die zu dem gewünschten Ergebnis führen, dann zählt man 16 verschiedene Möglichkeiten, die man aufgrund folgenden beiden Behauptungen in zwei Gruppen zu je acht Kombinationen geteilt werden können; abhängig davon, ob die Summe eine ungerade Anzahl Summanden kongruent zu 1 mod. 4 enthält oder eine gerade Anzahl Summanden kongruent zu 1 mod 4.

Behauptung A
Wenn sich eine gerade Anzahl der Summanden modulo 1 mod 4 in der Summe befinden, dann existiert ein ungerades Quaternion α_1 so, dass $\alpha' = (1+i)(1+j)\alpha_1$.

Beweis der Behauptung A
Da eine Multiplikation mit einer Einheit die Position der a_is verschiebt, kann man annehmen, dass $a_0 \equiv 1 \text{ (mod. } 4)$ ist. Man nehme zuerst an, dass $a_0 \equiv a_1 \equiv 1 \text{ (mod. } 4)$ und $a_2 = a_3 \equiv \pm 1 \text{ (mod 4.)}$. In diesem Fall setzen wir $\alpha' = (1+i)\alpha_0$ mit

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

Da $\frac{a_0+a_1}{2}$ und $\frac{a_1-a_2}{2}$ ungerade sind während $\frac{a_2+a_3}{2}$ und $\frac{a_2-a_3}{2}$ gerade sind kann man α_0 wie im obigen Fall (a) schreiben als $\alpha_0 = (1+j)\alpha_1$ mit einem ungeraden α_1, da $N(\alpha_0) \equiv 2 \text{ (mod. } 4)$. Somit Lässt sich α' wie gewünscht schreiben als $\alpha' = (1+i)(1+j)\alpha_1$.
Für die anderen Möglichkeiten die a_is zu wählen erhält man jeweils die Faktoren (1+j)(1+k) und (1+k)(1+i), jedoch gilt (1+j)(1+k)=(1+k)(1+i)=(1+i)(i+j).

Behauptung B
Wenn eine ungerade Anzahl der a_is kongruent zu 1 (mod. 4) ist, dann existiert ein ungerades Quaternion α_1, so dass $\alpha' = (1+i)(1-k)\alpha_1$.

Beweis der Behauptung B
Man nimmt erneut an, dass a_0 unter den drei a_is, die kongruent zu 1 (mod. 4) sind. Wenn $a_0 \equiv a_1 \equiv a_2 \equiv 1 \text{ (mod. } 4)$ und $a_3 \equiv -1 \text{ (mod. } 4)$, dann hat man wie im Fall (a) $\alpha' = (1+i)a_0$ mit

$$\begin{aligned} a_0 &= \frac{a_0 + a_1}{2} + \left(\frac{a_1 - a_2}{2}\right) i + \left(\frac{a_2 + a_3}{2}\right) j + \left(\frac{a_2 - a_3}{2}\right) k \\ &= b_0 + b_1 i + b_2 j + b_3 k \end{aligned}$$

Da b_0 und b_3 ungerade sind, während b_1 und b_2 gerade sind, lässt sich dies schreiben als

$$\begin{aligned}\alpha_0 &= (1-k)\left(\frac{b_0+b_3}{2} + \left(\frac{b_1-b_2}{2}\right)i + \left(\frac{b_1+b_2}{2}\right)j + \left(\frac{b_0+b_3}{2}\right)k\right)\\ &= (1-k)\alpha_1,\end{aligned}$$

sodass α_1 ungerade ist. Man setzt $\alpha_0 = (1+i)(1+k)\alpha_1$. Die verbleibenden Kombinationen können analog gezeigt werden.

Eindeutigkeit
Um die Eindeutigkeit der Faktorisierung zu zeigen, nehme man zuerst an, es gäbe eine zweite Faktorisierung desselben Quaternions α der Form

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

Man erkennt schnell, dass $l = k$ sein muss, indem man l und k maximal wählt, da andernfalls verbleibende Faktoren von Zweierpotenzen dazu führen würde, dass α_0 nicht länger ungerade sein könnte.
Betrachtet man nun den Fall, dass $\pi\alpha_0$ ungerade sei, so folgt, dass die Norm von π ebenfalls ungerade sein muss. Folglich muss $\pi = \widetilde{\pi} = 1$ gelten und die Zerlegung ist eindeutig.
Nun sei $\pi\alpha_0$ gerade und analog zum Beweis im Existenzteil äquivalent zu 2 modulo 4. Damit α_0 gerade sein kann, muss die Norm von π gleich zwei sein. Ohne Beschränkung der Allgemeinheit nehme man an, dass gelte $\pi = (1+i)$ und $\widetilde{\pi} = (1+j)$. Man könnte folgendes auch mit jeder anderen Kombination von π zeigen, die die Norm gleich zwei haben. Da gilt

$$(1+i)\alpha_0 = (1+j)\widetilde{\alpha_0}$$

und die π der Norm zwei Primquaternionen sind, muss der Faktor $(1+j)$ entweder $(1+i)$ oder α_0 teilen. Offensichtlich teilen sich die π nicht gegenseitig und da α_0 ungerade ist, kann $(1+j)$ auch nicht α_0 teilen. Ein Widerspruch. Also gilt $\pi = \widetilde{\pi}$ und somit ist die Zerlegung eindeutig.
Schließlich sei $\pi\alpha_0 \equiv 2 \pmod 4$. Damit α_0 ungerade sein kann, muss die Norm von π gleich 4 sein. Dann sei ohne Beschränkung der Allgemeinheit $\pi = (1+i)(1+j)$ und $\widetilde{\pi} = (1+i)(1-k)$. Dann gilt

$$(1+i)(1+j)\alpha_0 = (1+i)(1-k)\widetilde{\alpha_0}$$

Nachdem man $(1+i)$ kürzt, erhält man analog zum obigen Fall die Situation, in der gilt, dass das Primquaternion $(1-k)$ entweder $(1+i)$ oder α_0 teilen muss, dies aber nicht zutrifft. Folglich ist auch hier $\pi = \widetilde{\pi}$ und die Eindeutigkeit ist bewiesen.

2.8 Theorem: Euklidischer Algorithmus und das Lemma von Bézout

Sei α, $\beta \in \mathbb{H}(\mathbb{Z})$ und β sei ungerade. Dann existiert ein größter gemeinsamer rechtsseitiger Teiler $(\alpha,\beta)_r$. Zudem gilt eine Variante des Lemma von Bézout: Dann existieren γ, $\delta \in \mathbb{H}(\mathbb{Z}[\frac{1}{2}])$ mit

$$\mathbb{Z}\left[\frac{1}{2}\right] = \left\{\frac{k}{2^n} : k \in \mathbb{Z}, n \in \mathbb{N}\right\},$$

sodass

$$(\alpha,\beta)_r = \gamma\alpha + \delta\beta$$

Beweis
Man verwende nun die Struktur des euklidischen Algorithmus für den Beweis. Aufgrund des obigen Lemmas (2.5) lassen sich γ_0, $\delta_0 \in \mathbb{H}(\mathbb{Z})$ finden mit $N(\delta_0) < N(\beta)$ so, dass

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

Mit dem Lemma (2.7) ist es möglich, δ_0 zu schreiben als $\delta_0 = 2^{l_0}\pi_0\delta_0'$ mit δ_0' ungerade und $N(\delta_0') \leq N(\delta_0) < N(\beta)$. Wendet man die beiden Lemma (2.5 und 2.7)erneut an, erhält man:

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

mit $\delta_1 = 2^{l_1}\pi_1\delta_1'$, $N(\delta_1') \leq N(\delta_1) < N(\delta_0')$ und δ_1' ist ungerade. Wendet man wiederholt die Lemmas an, so findet man immer weiter Quaternionen δ_i, δ_i, $\delta_i' \in \mathbb{H}(\mathbb{Z})$ so, dass

$$\delta_i' = \gamma_{i+1}\delta_i' + \delta_{i+1},$$

mit $\delta_{i+1} = 2^{l_i+}\pi_{i+1}\delta_{i+1}'$, $N(\delta_{i+1}')leN(\delta_{i+1}) < N(\delta_i')$ und δ_{i+1}' ist ungerade.
Die letzten beiden Gleichungen werden

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

sein, da die δ_is eine Folge streng fallender Quaternionen in $\mathbb{H}(\mathbb{Z})$ sind. Dann setzt man $(\alpha, \beta)_r = \delta_k'$. Per Konstruktion ist δ_k' ein rechtshändiger Teiler von $\delta_{k-1}', \delta_{k-2}', ..., \beta, \alpha$. Wenn δ ein weiterer rechtsseitiger Teiler von α und β ist, dann ist er auch ein rechtshändiger Teiler von δ_0 und damit auch von δ_0', da die Faktorisierung aus Lemma (2.7) eindeutig ist. Geht man die obigen Gleichungen weiter durch, so sieht man, dass δ auch ein Teiler von δ_k' sein muss. Damit ist δ_k' der größte gemeinsame rechtsseitige Teiler.

Für Bézouts Lemma schreibt man die obigen Gleichungen um.

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

Da π_i in $\mathbb{H}(\mathbb{Z}[\frac{1}{2}])$ invertierbar ist, lässt sich δ_k' schreiben als

$$\delta_k' = \gamma\alpha + \delta\beta$$

mit γ, $\delta \in \mathbb{H}(\mathbb{Z}[\frac{1}{2}])$.

2.9 Lemma

Sei $\alpha \in \mathbb{H}(\mathbb{Z})$, m $\in \mathbb{Z}$ und m ungerade. Dann gilt

$$(m, \alpha)_r = 1 \qquad \text{genau dann wenn} \qquad (m, N(\alpha))_r = 1.$$

Beweis
„⇒“ Sei $(m, \alpha)_r = 1$. Nach dem Lemma von Bézout existieren γ, $\delta \in \mathbb{H}(\mathbb{Z}[\frac{1}{2}])$ mit

$$(m, \alpha)_r = 1 = \gamma m + \delta\alpha.$$

Dann gilt

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

umgestellt zu

$$1 = N(\delta)N(\alpha) + (\gamma + \overline{\gamma}))m + N(\gamma)m^2.$$

Da $N(\delta)$, $N(\gamma)$ und $\gamma + \overline{\gamma}$ Elemente aus $\mathbb{Z}[\frac{1}{2}]$ sind, kann man $k \in \mathbb{N}$ finden, so dass $2^k N(\delta)$, $2^k N(\gamma)$ und $2^k(\gamma + \overline{\gamma})$ ganze Zahlen sind. Sei $\beta \in \mathbb{H}(\mathbb{Z})$ ein rechtsseitiger Teiler von $N(\alpha)$ und m; da m ungerade ist, muss β auch ungerade sein. Nun schreibt man

$$2^k \cdot 1 = (2^k N(\delta))N(\alpha) + (2^k(\gamma + \overline{\gamma}))m - (2^k N(\gamma))m^2.$$

Alle drei Terme der rechten Seite werden von β geteilt. Folglich teilt β auch 2^k. Da $N(\beta)$ ungerade ist, muss $N(\beta) = 1$ sein, also ist β eine Einheit.

„⇐“ Sei $(m, N(\alpha))_r = 1$. Sei $\beta \in \mathbb{H}(\mathbb{Z})$ und teile sowohl m als auch α. Dann teilt β auch m und $N(\alpha) = \alpha\overline{\alpha}$ und ist damit ein Teiler des größten gemeinsamen Teilers 1.

2.10 Lemma

Sei p *in* $\mathbb{N}$ eine ungerade Primzahl. Man nimmt an, dass es ein $\alpha \in \mathbb{H}(\mathbb{Z})$ existiert, so, dass α kein Teiler von p ist, dafür aber $N(\alpha)$ p teilt. Dann setze $(\alpha, p)_r = \delta$. Dann ist δ prim in $\mathbb{H}(\mathbb{Z})$ und $N(\delta) = p$.

Beweis
Setzte $p = \gamma\delta$ für ein geeignetes $\gamma \in \mathbb{H}(\mathbb{Z})$ und betrachte die Norm

$$p^2 = N(p) = N(\gamma)N(\delta).$$

Man zeige zunächst, dass weder $N(\gamma)$ noch $N(\delta)$ gleich eins sein können. $N(\gamma) \neq 1$, da p und δ sonst zueinander assoziiert sein würde und damit p α teilen würde. $N(\delta) \neq 1$, da sonst das Lemma (2.9) besagen würde, dass sich p $N(\alpha)$ nicht teilen würden. Da p eine Primzahl in $\mathbb{N}$ ist, gilt $N(\gamma) = N(\delta) = p$.
Aufgrund von $N(\delta) = p$ ist δ prim in $\mathbb{H}(\mathbb{Z})$. Denn wenn für geeignete x und y $\in \mathbb{H}(\mathbb{Z})$ $\delta = xy$ gilt, dann gilt für die Normen $N(\delta) = p = N(x)N(y)$. Daher ist entweder $N(x)$ oder $N(y)$ gleich 1, sodass entweder x oder y eine Einheit ist.

2.11 Theorem: Primzahlen in $\mathbb{N}$ sind keine Primzahlen in $\mathbb{H}(\mathbb{Z})$

Für jede ungerade Primzahl p $\in \mathbb{N}$ existiert eine Primzahl $\delta \in \mathbb{H}(\mathbb{Z})$, so, dass $N(\delta) = p = \delta\overline{\delta}$ gilt. Insbesondere ist p keine Primzahl in $\mathbb{H}(\mathbb{Z})$.

Beweis
Nach Proposition (1.4) existieren x, $y \in \mathbb{Z}$, sodass $1 + x^2 + y^2 \equiv 0$ (mod. p). Setze $\alpha = 1 + xi + yj$. Offensichtlich teilt p α nicht, aber p teilt $N(\alpha)$. Da nun Lemma (2.10) gilt, ist $\delta = (\alpha, p)_r$ die gesuchte Primzahl in $\mathbb{H}(\mathbb{Z})$.

2.12 Korollar

$\delta \in \mathbb{H}(\mathbb{Z})$ ist prim in $\mathbb{H}(\mathbb{Z})$ genau dann wenn $N(\delta)$ prim in $\mathbb{N}$.

Beweis
Die Rückrichtung befindet sich im Beweis von Lemma (2.10).
Für die Hinrichtung sei δ eine Primzahl in $\mathbb{H}(\mathbb{Z})$. Man nehme zuerst an, dass δ gerade sei. Mit Lemma (2.7) lässt sich δ sich schreiben als $\delta = 2^l \pi \delta_0$ mit $l \in \mathbb{N}$, $\pi \in \{1, 1+i, 1+j, 1+k, (1+i)(1+j), (1+i)(1-k)\}$ und δ_0 ist ungerade. Da 2 nicht prim in $\mathbb{H}(\mathbb{Z})$ ist, muss $l = 0$, $N(\delta_0) = 1$ (da δ_0 ungerade ist) und $\pi \in \{1+i, 1+j, 1+k\}$, so dass $N(\delta) = 2$, wie erwünscht ist.
Nun sei δ ungerade. Sei $p \in \mathbb{N}$ eine ungerade ganze Primzahl, die $N(\delta)$ teilt. Setze $\alpha = (p, \delta)_r$, dann ist $\delta = \gamma\alpha$ für ein geeignetes $\gamma \in \mathbb{H}(\mathbb{Z})$. Aus Lemma (2.9) folgt, dass α keine Einheit sein kann. Da δ eine Primzahl in $\mathbb{H}(\mathbb{Z})$ ist, muss γ eine Einheit in $\mathbb{H}(\mathbb{Z})$ sein, so dass α und δ assoziiert sind. Daher ist δ auch ein rechtsseitiger Teiler von p mit $p = \psi\delta$ für ein geeignetes $\psi \in \mathbb{H}(\mathbb{Z})$. Betrachtet man nun die Norm von p und die Tatsache, dass p $N(\delta)$ teilt, erhält man

$$p = N(\psi)\left(\frac{N(\delta)}{p}\right)$$

Wenn $N(\psi) = 1$ wäre, dann wären p und δ assoziiert, so dass p prim in $\mathbb{H}(\mathbb{Z})$ wäre, was dem vorangehenden Theorem (2.11) widerspricht. Folglich muss $\frac{N(\delta)}{p} = 1$ gelten, sodass $N(\delta) = p$.

2.13 Korollar

Jede natürliche Zahl ist Summe von vier Quadraten.

Beweis
Sei $n \in \mathbb{N}$. Da die Aussage für $n = 0$ und $n = 1$ trivial ist, sei $n \geq 2$. Sei $n = 2^{r_0} p_1^{r_1} ... p_k^{r_k}$ die Primfaktorzerlegung von n mit p_i ungerade. Nach dem Theorem (2.11) kann man $\delta_i \in \mathbb{H}(\mathbb{Z})$ finden mit $p_i = N(\delta_i) = \delta_i \overline{\delta_i}$, während $2 = (1+i)(1+j)$ gilt. Aufgrund der Definition der Norm ist eine natürliche Zahl als Summe von vier Quadratzahlen darstellbar, wenn es die Norm eines Quaternions ist. Mit der obigen Zerlegung ist nun $\delta = (1+i)^{r_0} {\delta_i}^{r_i}$ aufgrund der Multiplikativität der Norm das gesuchte Quaternion mit $N(\delta) = n$.

2.14 Bemerkung

Im vorangegangenen Kapitel 2.4 (bzw. 2.3) im Buch von Davidoff, Sarnak und Valette wird gezeigt, dass es für die Gleichung

$$a_0^2 + a_1^2 + a_2^2 + a_3^2 = n$$

für ganze Zahlen a_i und natürliche n genau $\sum_{d|n} d$ mögliche Kombination gibt, die diese Gleichung lösen. Setzt man für n eine ungerade Primzahl p ein, so gibt es entsprechend $8(p+1)$ Lösungsmöglichkeiten, die jeweils in Form eines Quaternions $\alpha = a_0 + a_1 i + a_2 j + a_3 k$ der Norm p darstellbar ist.

Aufgrund der Tatsache, dass Multiplikation mit den acht Einheiten zu Permutationen unter den a_is und dadurch zu assoziierten Lösungsmöglichkeiten führen, die separat gezählt werden, möchte man nun die Menge der Lösungen einschränken. Man vergewissert sich, dass die ungerade Primzahlen p entweder $\equiv 1$ (mod. 4) oder $\equiv 3$

(mod. 4) sind und dass wenn $p \equiv 1$ (mod. 4), genau eines der a_is ungerade ist. Wenn $p \equiv 3$ (mod. 4), dann ist genau ein a_i gerade. Ein a_i ist in solcher Weise ausgezeichnet, dass man aus den acht Möglichkeiten dasjenige Quaternion α auswählt, bei dem der ausgezeichnete Summand der nullte Summand $a_0 \geq 0$ ist. Ist $a_0 = 0$, dann sind zwei Assoziierte gleichartig gesondert und die Wahl ist beliebig. Dadurch hat man $p + 1$ repräsentierende Lösungen von

$$a_0^2 + a_1^2 + a_2^2 + a_3^2 = p.$$

Der Grund der obigen Betrachtung ist die Tatsache, dass durch die Wahl der Repräsentanten entweder $\alpha \equiv 1$ (mod. 2) oder $\alpha \equiv i + j + k$ (mod. 2) gilt. Diese Eigenschaft wird im Beweis von Korollar (2.17) benötigt.

Man beachte, dass wenn α Repräsentant ist, auch $\overline{\alpha}$ ein Repräsentant sein wird, während, falls $a_0 = 0$ gilt, es nur eine Lösung und damit nur einen Repräsentanten gibt.
Mithilfe der Repräsentanten konstruiert man die Menge

$$S_p = \{\alpha_1, \overline{\alpha_1}, ..., \alpha_s, \overline{\alpha_s}, \beta_1, ..., \beta_t\}.$$

Die α haben einen nullten Summanden a_0 größer null, während die β einen nullten Summanden gleich null haben. Des Weiteren gilt $\alpha_i\overline{\alpha_i} = -\beta_i^2 = p$ und $2s + t = |S_p| = p + 1$.

2.15 Definition

Ein reduziertes Wort über S_p ist ein Wort über dem Alphabet S_p, das kein Teilwort der Form $\alpha_i\overline{\alpha_i}$, $\overline{\alpha_i}\alpha_i$, β_j^2 (mit $i = 1, ..., s$ und $j = 1, ..., t$). Die Länge des Wortes ist die Anzahl der auftauchenden Elemente.

2.16 Theorem: Faktorisierung mit Worten

Sei $k \in \mathbb{N}$, sei $\alpha \in \mathbb{H}(\mathbb{Z})$ so, dass $N(\alpha) = p^k$. Dann existiert eine eindeutige Faktorisierung für α der Form $\alpha = \epsilon p^r \omega_m$ mit ϵ sei eine Einheit und ω_m sei ein reduziertes Wort der Länge m über S_p und $k = 2r + m$.

Beweis
Existenz
Man wähle ein beliebiges $\alpha \in \mathbb{H}(\mathbb{Z})$ mit $N(\alpha) = p^k$. Nach Proposition (2.3) ist α ein Produkt aus Primzahlen:

$$\alpha = \delta_1, ...\delta_n.$$

Entsprechend Korollar (2.12) gilt $N(\delta_i) = p$ und daher $n = k$. Da $N(\delta_i) = p$, findet man eine Einheit ϵ_i und $\gamma_i \in S_p$, so $\delta_i = \epsilon_i\gamma_i$; daher gilt

$$\alpha = \epsilon_1\gamma_1\epsilon_2\gamma_2...\epsilon_k\gamma_k$$

Da Multiplikation mit Einheiten im Wesentlichen Vorzeichen und Position der Summanden eines Quaternions vertauschen, findet man für jedes $\gamma \in S_p$ und jede Einheit ϵ von $\mathbb{H}(\mathbb{Z})$ geeignete $\gamma' \in S_p$ und Einheiten ϵ', so dass $\gamma\epsilon = \epsilon'\gamma'$. Dies erlaubt die Verschiebung aller Einheiten in der obigen Faktorisierung , sodass nun gilt

$$\alpha = \epsilon\gamma_1'...\gamma_k'$$

mit $\gamma' \in S_p$ und ϵ ist eine Einheit in $\mathbb{H}(\mathbb{Z})$. α ist nun ein Produkt aus einer Einheit und einem Wort über dem Alphabet S_p. Sollte dieses Wort nicht reduziert sein, so kann alle Faktoren p bilden und nach links ziehen, so dass die gewünschte Form entsteht.

Eindeutigkeit
Um die Eindeutigkeit zu zeigen, beweist man, dass es genau so viele Möglichkeiten ein α für ein festes p^k zu wählen, wie es Möglichkeiten gibt unterschiedliche $\epsilon p^r \omega_m$ zu konstruieren. Nach Jacobis Theorem (siehe Bemerkung 2.14) gibt es genau

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

Quaternionen $\alpha \in \mathbb{H}(\mathbb{Z})$ mit $N(\alpha) = p^k$.
Die Anzahl der möglichen reduzierte Wörter der Länge m über S_p bestimmt man kombinatorisch. Es gibt $p+1$ Möglichkeiten für den ersten Buchstaben eines Wortes und p Möglichkeiten für jeden darauffolgenden, da man die Kombinationen $\alpha_i\overline{\alpha_i}$, $\overline{\alpha_i}\alpha_i$, β_j^2 vermeiden möchte. Folglich ist die Anzahl der möglichen reduzierten Worte

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

Damit ist die Gesamtzahl an Möglichkeiten für $\epsilon p^r \omega_m$ gleich

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

In beiden Fällen findet man $8\frac{p^{k+1}-1}{p-1}$ Möglichkeiten, was mit der Gesamtzahl von möglichen $\alpha \in \mathbb{H}(\mathbb{Z})$ mit $N(\alpha) = p^k$ übereinstimmt. Da jedes α so faktorisiert werden kann, muss die Faktorisierung eindeutig sein.

2.17 Korollar

Sei

$$\begin{aligned}\Lambda' = \{\alpha = a_0 + a_1 i + a_2 j + a_3 k \in \mathbb{H}(\mathbb{Z}) : \alpha \equiv 1 (mod. 2) \text{ oder} \\ \alpha \equiv i+j+k (mod. 2), N(\alpha) \text{ eine Potenz einer Primzahl } p\}.\end{aligned}$$

Jedes Element $\alpha \in \Lambda'$ mit $N(\alpha) = p^k$ hat eine eindeutige Faktorisierung der Form $\alpha = \pm p^r \omega_m$, mit $r \in \mathbb{N}$, ω_m sei ein reduziertes Wort der Länge m über S_p und $k = 2r+m$.

Beweis
Nach dem Theorem (2.16) existiert eine Faktorisierung von α der Form $\alpha = \epsilon p^r \omega_m$, mit r und ω_m passend und ϵ ist eine Einheit in $\mathbb{H}(\mathbb{Z})$. Reduziert man mod. 2, erhält man $\alpha \equiv \epsilon\omega_m$ (mod. 2). Alle α_i, $\beta_i \in S_p$, die in ω_m auftreten sind $\equiv 1$ (mod. 2) oder $\equiv i+j+k$ (mod. 2). Bezeichne die Letzteren als γ. Dann erhält man modulo 2 folgende Kongruenzen:

$$\alpha \equiv \begin{cases} \epsilon & \text{wenn die Anzahl der auftretenden } \gamma \text{ in } \omega_m \text{ gerade ist} \\ \epsilon(i+j+k) & \text{wenn die Anzahl der auftretenden } \gamma \text{ in } \omega_m \text{ ungerade ist} \end{cases}$$

Andererseits ist $\alpha \in \Lambda'$, daher ist α selbst entweder $\alpha \equiv 1$ (mod. 2) oder $\alpha \equiv (i+j+k)$ (mod. 2). In beiden Fällen muss $\epsilon \equiv 1$ (mod. 2) gelten, also ist $\epsilon \pm 1$.

Literatur

[1] Davidoff, Sarnak, Vallette: *Elementary Number Theory, Group Theory, and Ramanujan Graphs*