<u>Quaternionen und Vierquadratesatz</u>

Thierry Matthey und Marcel Steiner

10. Mai 1994

1. Algebren

Definition 1.1 (Reelle Algebren) *Ein VR V über* $\mathbf{R}$ *mit einer Produktabbildung* $V \times V \to V$, $(x, y) \mapsto x \cdot y$ *heisst eine Algebra* $\mathcal{A}$ *über* $\mathbf{R}$ *(*$\mathbf{R}$*-Algebra), wenn die beiden Distributivgesetze*

$$(\alpha x + \beta y)z = \alpha xz + \beta yz \qquad \forall \alpha, \beta \in \mathbf{R}$$
$$x(\alpha y + \beta z) = \alpha xy + \beta xz \qquad \forall x, y, z \in V$$

erfüllt sind.

Die Dimension des $\mathbf{R}$-VR heisst *Dimension* der Algebra $\mathcal{A}$.
Gilt das Assoziativgesetz $x(yz) = (xy)z \ \forall x, y, z \in \mathcal{A}$, so heisst die Algebra *assoziativ.*
Gilt das Kommutativgesetz $xy = yx \ \forall x, y \in \mathcal{A}$, so heisst die Algebra *kommutativ.*
Eine Algebra heisst *alternativ*, falls $x(xy) = x^2y$ und $(xy)y = xy^2 \ \forall x, y \in \mathcal{A}$ gilt.
Eine Algebra $\mathcal{A}$ mit Einselement e heisst *quadratisch*, wenn $\forall x \in \mathcal{A}$ einer quadratischen Gleichung $x^2 = \alpha e + \beta x$ mit $\alpha, \beta \in \mathbf{R}$ genügt.
Eine Algebra $\mathcal{A}$ heisst *potenz-assoziativ*, falls $x^m x^n = x^{m+n} \ \forall x \in \mathcal{A}$ und alle $m \geq 1$, $n \geq 1$.
Jede assoziative Algebra ist alternativ und jede alternative Algebra ist potenz-assoziativ.

Definition 1.2 (R-Unteralgebra) *Ein reeller Unter-VR U einer* $\mathbf{R}$*-Algebra* $\mathcal{A} = (V, \cdot)$ *heisst eine* $\mathbf{R}$*-Unteralgebra von* $\mathcal{A}$*, wenn* $x \cdot y \in U \ \forall x, y \in U$ *gilt.*

Definition 1.3 (R-Algebra-Homomorphismus) $\mathcal{A} = (V, \cdot)$, $\mathcal{B} = (W, \cdot)$ *zwei* $\mathbf{R}$*-Algebren, so heisst eine* $\mathbf{R}$*-lineare Abbildung* $f : V \to W$ *ein* $\mathbf{R}$*-Algebra-Homomorphismus, wenn gilt* $f(xy) = f(x)f(y) \ \forall x, y \in V$.

Definition 1.4 (Divisionsalgebren) *Eine Algebra* $\mathcal{A} \neq \emptyset$ *heisst Divisionsalgebra, wenn* $\forall \alpha \in V$, $\alpha \neq 0$ *die beiden Gleichungen* $\alpha x = \beta$ *und* $y\alpha = \beta \ \forall \beta \in V$ *eindeutig in* $\mathcal{A}$ *lösbar sind.*

Definition 1.5 (Abstrakte Lie-Algebren) *Sei* $\mathcal{L}$ *eine* $\mathbf{R}$*-Algebra über V mit* $J, K, H \in V$*, und gilt folgendes:*

1) $[aH + bJ, K] = a[H, K] + b[J, K]$ *mit* $a, b \in \mathbf{R}$*, bilinear.*

2) $[J, K] = -[K, J]$*, antikommutativ.*

3) $[[H, J], K] + [[J, K], H] + [[K, H], J] = 0$*, Jacobi-Identität.*

So ist $\mathcal{L}$ *eine Lie-Algebra.*

Lemma 1.6 *Ist $\mathcal{A}$ eine assoziative Divisionsalgebra, so ist $\mathcal{G} := \mathcal{A}\backslash\{0\}$ bezüglich der Multiplikation in $\mathcal{A}$ ein Gruppe.*

Beispiele 1.7 *Reelle Algebren bzw. Divisionsalgebren*

i) Die Körper $\mathbf{R}$ und $\mathbf{C}$ sind assoziative und kommutative $\mathbf{R}$-Algebren.

ii) Der $\mathbf{R}$-VR Mat($n \times n$,$\mathbf{R}$) ist bezüglich der Matrizenmultiplikation eine assoziative nicht kommutative $\mathbf{R}$-Algebra.

iii) Das Produkt zweier Vektoren aus $\mathbf{R}^3$ wird als Vektorprodukt $\mathbf{R}^3$ definiert, so wird der VR $\mathbf{R}^3$ zu einer dreidimensionalen $\mathbf{R}$-Algebra, die nicht assoziativ und antikommutativ ist. Auch ein Beispiel einer nicht trivialen Lie-Algebra.

iv) Die Hamiltonsche Algebra $\mathbf{H}$ der Quaternionen ist eine nicht-kommutative und reelle Divisionsalgebra.

v) $\mathbf{R}$, $\mathbf{C}$ und $\mathbf{H}$ sind alternative, quadratische Divisionsalgebren.

Bemerkung 1.8 *Explizite Konstruktion einer $\mathbf{R}$-Algebra $\mathcal{A}$. Sei V ein reeller, n-dimensionaler VR. Wähle man eine Basis $\{e_0, e_1, e_2, \ldots, e_{n-1}\}$. So definiert man das Produkt $(x, y) \to xy$ in V aufgrund des Distributivgesetz durch $xy = \sum_{i,j=0}^{n-1}(\alpha_i\beta_j)\ e_i \cdot e_j$. So ist die $\mathbf{R}$-Algebra $\mathcal{A}$ durch Festlegen der n^2 Einzelprodukte $e_i \cdot e_k$ vollständig bestimmt.*

2. Quaternionen

Definition 2.1 (Die Algebra H der Quaternionen) *Es sei $e, i, j, k \in \mathbf{H}$, so definiert man die Hamiltonsche Multiplikation wie folgt:*

$$i^2 = j^2 = k^2 = ijk = -e \text{ und } ij = -ji = k \qquad .$$

$\cdot$	e	i	j	k
e	e	i	j	k
i	i	$-e$	k	j
j	j	$-k$	$-e$	i
k	k	j	$-i$	$-e$

Die Quaternionen-Algebra $\mathbf{H}$ ist assoziativ, aber nicht kommutativ, $\mathbf{H}$ ist ein *Schiefkörper.*

Notation 2.2 *Für $x \in \mathbf{H}$ $x = \alpha e + \beta i + \gamma j + \delta k$ oder $x = x_0e_0 + x_1e_1 + x_2e_2 + x_3e_3$ mit $\alpha, \beta, \gamma, \delta, e_0, e_1, e_2, e_3 \in \mathbf{R}$.*

Lemma 2.3 *Die Gruppe $(Q = \{e, -e, i, -i, j, -j, k, -k\}, \cdot)$ ist eine nichtkommutative Untergruppe von $\mathbf{H}$ und alle Elemente ausser $\pm e$ haben Ordnung 4. Alle eigentlichen Untergruppen von Q sind kommutativ.*

Satz 2.4 *Die Menge $\mathcal{H} := \left\{\begin{pmatrix} w & -z \\ \bar{z} & \bar{w} \end{pmatrix}; w, z \in \mathbf{C}\right\}$ ist ein $\mathbf{R}$-Unteralgebra von Mat(2×2,$\mathbf{C}$) mit Einselement $E := \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. $\mathcal{H}$ ist eine 4-dimensionale, assoziative Divisionsalgebra.*

Lemma 2.5 *Durch die Abbildung* $F : \mathbf{H} \longrightarrow \mathcal{H}$ *mit* $(\alpha, \beta, \gamma, \delta) \longrightarrow \begin{pmatrix} \alpha + \beta i & -\gamma - \delta i \\ \gamma - \delta i & \alpha - \beta i \end{pmatrix}$ *wird ein* $\mathbf{R}$*-Algebra-Isomorphismus definiert. Es gilt:*

$$F(e) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} =: E \qquad F(j) = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} =: J$$

$$F(i) = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} =: I \qquad F(k) = \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix} =: K$$

Notation 2.6 $X \in \mathcal{H}$, $X = \alpha E + \beta I + \gamma J + \delta K$; $\alpha, \beta, \gamma, \delta \in \mathbf{R}$.

Bemerkung 2.7 *Es gibt weiter noch einen Monomorphismus* $\bar{F} : \mathbf{H} \rightarrow Mat(4 \times 4, \mathbf{R})$ *mit*

$$\bar{F}(e) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} =: E \qquad \bar{F}(j) = \begin{pmatrix} 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{pmatrix} =: J$$

$$\bar{F}(i) = \begin{pmatrix} 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \end{pmatrix} =: I \qquad \bar{F}(k) = \begin{pmatrix} 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \\ 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix} =: K$$

mit Hilfe des Monomorphismuses $\varphi : \mathbf{C} \rightarrow Mat(2 \times 2, \mathbf{R})$, $(\alpha + i\beta) \rightarrow \begin{pmatrix} \alpha & -\beta \\ \beta & \alpha \end{pmatrix}$

Definition 2.8 (Quaternionenaddition und -Produkt) $x, x' \in \mathbf{H}$.
$x + x' := (\alpha + \alpha')e + (\beta + \beta')i + (\gamma + \gamma')j + (\delta + \delta')k.$
$xx' := (\alpha\alpha' - \beta\beta' - \gamma\gamma' - \delta\delta')e + (\alpha\beta' + \beta\alpha' + \gamma\delta' - \delta\gamma')i$
$+(\alpha\gamma' - \beta\delta' + \gamma\alpha' + \delta\beta')j + (\alpha\delta' + \beta\gamma' - \gamma\beta' + \delta\alpha')k.$

Definition 2.9 (H als euklidischer Vektorraum) $x, x' \in \mathbf{H}$.

1. $< x, x' >= \alpha\alpha' + \beta\beta' + \gamma\gamma' + \delta\delta' \in \mathbf{R}$ *(kanonisches Skalarprodukt).*
2. $|x|^2 = \alpha^2 + \beta^2 + \gamma^2 + \delta^2 \geq 0.$
3. $|X|^2 = det(X)$ *für* $X \in \mathcal{H} \subset Mat(2 \times 2, \mathbf{C})$.

Definition 2.10 (Konjugation) $\mathbf{H} \rightarrow \mathbf{H}$, $x \rightarrow \bar{x} := \alpha e - \vec{u}$.

1. $\bar{\bar{x}} = x.$
2. $|x| = |\bar{x}|$ *(Längentreue).*
3. $\overline{x + y} = \bar{x} + \bar{y}.$
4. $\overline{xy} = \bar{y}\bar{x}.$

Lemma 2.11 (Inverses eines Quaternions) *Sei* $x \neq 0$,
so gilt $x^{-1} = \frac{1}{|x|^2}\bar{x} = \frac{1}{\alpha^2+\beta^2+\gamma^2+\delta^2}(\alpha e - \beta i - \gamma j - \delta k).$

Lemma 2.12 (Eigenschaften des Skalarproduktes in H) $x, y \in \mathbf{H}$.

1. $|x|^2 = x\bar{x} = \bar{x}x =< x, x >$.
2. $< x, y >= \frac{1}{2}(x\bar{y} + y\bar{x}) = \Re(x\bar{y}) = \Re(y\bar{x})$, *speziell* $< x, e >= \Re(x)$.
3. $< x, y >= 0 \Leftrightarrow x\bar{y} = -y\bar{x} \in \Im\mathbf{H}$ *(Orthogonalitätskriterium).*
4. $e, i, j, k \in \mathbf{H}$ *bilden eine Orthonormalbasis.*
5. $|xy| = |x||y|$ *(Produktregel).*
6. $yxy = 2 < \bar{x}, y > y- < y, y > \bar{x}$ *(Dreier-Identität).*

Definition 2.13 (Skalar) q *Skalar, falls* $q = \alpha e$, $q \in \mathbf{H}$.

Definition 2.14 (Vektor) $\vec{u}$ *Vektor, falls* $\vec{u} = \beta i + \gamma j + \delta k$, $\vec{u} \in \mathbf{H}$.

Definition 2.15 (Basisinvariante Darstellung) $x = \alpha e + \vec{u}$; $\alpha \in \Re\mathbf{H}, \vec{u} \in \Im\mathbf{H}$.

Definition 2.16 (Real- und Imaginärteil) $\mathbf{H} = \Re\mathbf{H} \oplus \Im\mathbf{H}$. $x = \alpha e + \vec{u}, x \in \mathbf{H}$.
$\Re(x) : x \to \alpha e$. $\Re\mathbf{H}=\mathbf{R}$, $\Re(e) = 1$.
$\Im(x) : x \to \vec{u}$. $\Im\mathbf{H}= \{x \in \mathbf{H} : \bar{x} = -x\} = Kern\Re\mathbf{H} = \mathbf{R}i \oplus \mathbf{R}j \oplus \mathbf{R}k$.

Lemma 2.17 (Eigenschaften von $\Re$ und $\Im$) $x, y \in \mathbf{H}$.

1. $\Re(x) = \Re(\bar{x})$.
2. $\Re(xy) = \Re(yx)$.
3. $x^2 = 2\Re(x)x - |x|^2 e$ *(quadratische Gleichung).*
4. $x + \bar{x} = 2\Re(x)e$.
5. $x - \bar{x} = 2\Im(x)e$.
6. $\Im\mathbf{H}$ *ist keine* $\mathbf{R}$*-Unteralgebra.*

Definition 2.18 (Skalarprodukt in $\Im$H) $< \vec{u}, \vec{v} >= u_1v_1 + u_2v_2 + u_3v_3$, $\vec{u}, \vec{v} \in \Im\mathbf{H}$.

Definition 2.19 (Vektorprodukt in $\Im$H) *Analogon zum Vektorprodukt im* $\mathbf{R}^3$.
$\vec{u} \times \vec{v} = (u_2v_3 - u_3v_2)i + (u_3v_1 - u_1v_3)j + (u_1v_2 - u_2v_1)k$, $\vec{u}, \vec{v} \in \Im\mathbf{H}$.
Das Vektorprodukt ist bilinear und antikommutativ, jedoch nicht assoziativ.

Lemma 2.20 (Eigenschaften des Skalar- und Vektorproduktes in $\Im$H) $\vec{u}, \vec{v}, \vec{w} \in \Im\mathbf{H}$.

1. $\vec{u} \times \vec{v} = \frac{1}{2}(\vec{u}\vec{v} - \vec{v}\vec{u}) = \begin{vmatrix} i & j & k \\ u_1 & u_2 & u_3 \\ v_1 & v_2 & v_3 \end{vmatrix}$.
2. $< \vec{u}, \vec{v} > e = \vec{u} \times \vec{v} - \vec{u}\vec{v}$.
3. $< \vec{u} \times \vec{v}, \vec{w} >=< \vec{u}, \vec{v} \times \vec{w} >$ *(Vertauschungsregel).*

Definition 2.21 (Grassman-Identität) $\vec{u}, \vec{v} \in \Im \mathbf{H}$.
$\vec{u} \times (\vec{v} \times \vec{w}) =< \vec{u}, \vec{w} > \vec{v} - < \vec{u}, \vec{v} > \vec{w}$.

Definition 2.22 (Jacobi-Identität) $\vec{u}, \vec{v}, \vec{w} \in \Im \mathbf{H}$.
$(\vec{v} \times \vec{u}) \times \vec{w} + (\vec{u} \times \vec{w}) \times \vec{v} + (\vec{w} \times \vec{v}) \times \vec{u} = 0$.

Definition 2.23 (Lorentzmetrik) $\Re(xx') = \alpha\alpha' - \beta\beta' - \gamma\gamma' - \delta\delta'$.

Bemerkung 2.24 (Polynome über H) *Die Tatsache, dass* **H** *nicht kommutaiv ist, hat viele ungewohnte Konsequenzen: So können Polynome mehr Nullstellen haben über* **H** *als ihr Grad angibt.*

Beispiel: $f(x) = x^2 + e \in \mathbf{H}(x)$.
$f(x)$ hat als Nullstellen alle Vektoren $\vec{u} = \beta i + \gamma j + \delta k$ mit der Länge $\beta^2 + \gamma^2 + \delta^2 = 1$. Die Quaternionen $x = 0e + \vec{u}$ bilden die Oberfläche der Einheitskugel in $\mathbf{R}^3$, da $\vec{u}\vec{u} =(-\beta^2 - \gamma^2 - \delta^2)e + (\gamma\delta - \delta\gamma)i + (-\beta\delta + \delta\beta)j + (\beta\gamma - \gamma\beta)k = -e$ also $f(\vec{u}) = -e + e = 0$. Der Grund für dieses Phänomen ist, dass sich Polynome über Schiefkörper nicht mehr in der gewohnten Art faktorisieren lassen.
Z.B.: Gilt $(X - x)(X - y) = X^2 - xX - Xy + xy$ so darf man die Linearglieder nicht zu $-(x + y)X$ zusammenfassen, da **H** nicht kommutativ ist.

Satz 2.25 (Satz von Frobenius (1877)) *Es sei $\mathcal{A}$ eine assoziative endliche dimensionale reelle Divisionsalgebra. Dann sind drei Fälle möglich:*

1. *$\mathcal{A}$ ist isomorph zum Körper* **R** *der reellen Zahlen.*
2. *$\mathcal{A}$ ist isomorph zum Körper* **C** *der komplexen Zahlen.*
3. *$\mathcal{A}$ ist isomorph zum Schiefkörper (***R***-Algebra)* **H** *der Quaternionen.*

Beweis: *Siehe Zahlen[6], p.189.*

Auch wenn man die Gültigkeit des Assoziativgesetzes der Multiplikation nicht ausdrücklich postuliert, ist der Körper der komplexen Zahlen **C** der einzige kommutative Erweiterungskörper endlichen Grades über dem Körper der reellen Zahlen (Hopf 1940, Schweizer Mathematiker).

3. Rotationen

Definition 3.1 (3-Sphäre) *Die Menge $S^3 := \{x \in \mathbf{H} : |x| = 1\}$ aller Quaternionen der Norm 1 ist bezüglich der Multiplikation in* **H** *eine Untergruppe von $\mathbf{H}\backslash\{0\}$.*

Definition 3.2 (Spezielle unitäre Gruppe) $SU(2) = \{A \in U(2) \subset GL(2,\mathbf{C})$ *mit* $det A = 1\}$.

Satz 3.3 $SU(2) = \{A \in \mathcal{H} : det A = 1\}$, *speziell* $SU(2) \subset \mathcal{H}$.

Satz 3.4 (Isomorphiesatz) *Der Algebra-Isomorphismus $F : \mathbf{H} \rightarrow \mathcal{H}$ bildet die Gruppe S^3 aller Quaternionen mit Norm 1 isomorph auf $SU(2)$ ab.*

Definition 3.5 (Orthogonale Abbildung) *V ist ein endlich dimensionaler VR. Eine lineare Abbildung $f : V \to V$ heisst orthogonal, wenn $< f(x), f(y) >=< x, y > \forall x, y \in V$.*

Satz 3.6 (Orthogonale Gruppe) *Die orthogonalen Abbildungen von V bildet unter Komposition eine Gruppe $O(V)$.*

Definition 3.7 *Sei V endlichdimensionaler VR.*
$SO(V) := O^+ = \{f \in O(V) \text{ mit } det f = 1\}$, *Drehungen.*
$0^- := \{f \in O(V) \text{ mit } det f = -1\}$, *Drehspiegelungen.*

Satz 3.8 (Satz von Cayley) *Zu jeder orthogonalen Abbildung $f : \mathbf{H} \to \mathbf{H}$ gibt es zwei Quaternionen $a, b \in S^3$ mit*

1. $f(x) = axb$, *falls* $f \in O^+(\mathbf{H})$.
2. $f(x) = a\bar{x}b$, *falls* $f \in O^-(\mathbf{H})$.

Satz 3.9 (Satz von Hamilton) *Zu jeder orthogonalen Abbildung $f : \Im\mathbf{H} \to \Im\mathbf{H}$ gibt es ein Quaternion $a \in S^3$ mit*

1. $f(\vec{u}) = a\vec{u}\bar{a}$, *falls* $f \in O^+(\Im\mathbf{H})$.
2. $f(\vec{u}) = -a\vec{u}\bar{a}$, *falls* $f \in O^-(\Im\mathbf{H})$.

Beweis: *Zahlen[6], p.150.*

4. Oktaven

Für die Algebren **C, H** bzw. **O** hat man die Darstellungen

$$\mathbf{C} = \mathbf{R} \oplus \mathbf{R}i,\ \mathbf{H} = \mathbf{C} \oplus \mathbf{C}j \text{ und } \mathbf{O} = \mathbf{H} \oplus \mathbf{H}p$$

als direkte Summe von VR, wenn **R** in **C** mit den Paaren $(\alpha, 0); \alpha \in \mathbf{R}$ und **C** in **H** mit den Quaternionen $(\alpha, \beta, 0, 0); \alpha, \beta \in \mathbf{R}$ identifiziert wird.
Dabei sind **R** bzw. **C** Unteralgebren von **C** bzw. **H**, die jeweils das Einselemnt von **R** bzw. **C** enthalten. Summendarstellung sind orthogonal bezüglich des natürlichen Skalarproduktes in **C** bzw. **H**. Eine analoge Situation besteht für die sogenannten Oktaven **O**.

Definition 4.1 (Multiplikationstafel für O) *$V := \mathbf{R}^8$ mit der natürlichen Basis $\{e_0 := (1, 0, \ldots, 0), \ldots, e_7 := (0, \ldots, 0, 1)\}$*

$\cdot$	e_0	e_1	e_2	e_3	e_4	e_5	e_6	e_7
e_0	e_0	e_1	e_2	e_3	e_4	e_5	e_6	e_7
e_1	e_1	$-e_0$	e_3	$-e_2$	e_5	$-e_4$	$-e_7$	e_6
e_2	e_2	$-e_3$	$-e_0$	e_1	e_6	e_7	$-e_4$	$-e_5$
e_3	e_3	e_2	$-e_1$	$-e_0$	e_7	$-e_6$	e_5	$-e_4$
e_4	e_4	$-e_5$	$-e_6$	$-e_7$	$-e_0$	e_1	e_2	e_3
e_5	e_5	e_4	$-e_7$	e_6	$-e_1$	$-e_0$	$-e_3$	e_2
e_6	e_6	e_7	e_4	$-e_5$	$-e_2$	e_3	$-e_0$	$-e_1$
e_7	e_7	$-e_6$	e_5	e_4	$-e_3$	$-e_2$	e_1	$-e_0$

Aus dieser Tafel liest man sofort die Nicht-Assoziativität der Oktaven **O** ab. Die Algebra **O** ist eine alternative Divisionsalgebra.
Z.B.: $e_4(e_5e_6) = -e_7$, aber $(e_4e_5)e_6 = e_7$.

Satz 4.2 (Einzigkeit der Oktaven (Zorn (1933))) *Jede reelle, endlich dimensionale, alternative, nicht-assoziative Divisionsalgebra $\mathcal{A}$ ist zu den Oktaven* **O** *isomorph.*
Beweis: *Zahle[6], p.215.*

Satz 4.3 (Verallgemeinerung des Satzes von Frobenius) *Jede reelle, alternative, endlich dimensionale Divisionsalgebra ist isomorph zu* **R**, **C**, **H** *oder* **O**.

5. Vierquadratesatz

Satz 5.1 (Fermat (1659)) *Jede natürlichen Zahl ist die Summe von vier Quadraten von ganzen Zahlen (i.a. nicht eindeutig).*

Beweis (Langrange (1770)): Für $n = 1$ und $n = 2$ gibt es die Darstellung

$$1 = 1^2 + 0^2 + 0^2 + 0^2 \text{ und } 2 = 1^2 + 1^2 + 0^2 + 0^2.$$

Für den weitern Verlauf des Beweises ist die folgende *Euler-Identität* wichtig:

$$\begin{aligned}
&(\alpha^2 + \beta^2 + \gamma^2 + \delta^2)(\alpha'^2 + \beta'^2 + \gamma'^2 + \delta'^2) \\
&= (\alpha\alpha' - \beta\beta' - \gamma\gamma' - \delta\delta')^2 + (\alpha\beta' + \beta\alpha' + \gamma\delta' - \delta\gamma')^2 \\
&+ (\alpha\gamma' - \beta\delta' + \gamma\alpha' + \delta\beta')^2 + (\alpha\delta' + \beta\gamma' - \gamma\beta' + \delta\alpha')^2.
\end{aligned}$$

Die Indentität besagt, dass das Produkt aus zwei Faktoren als Summe von vier Quadraten dargestellt werden kann, wenn dies für die beiden Faktoren möglich ist. Mit der Darstellbarkeit von 1 und 2, lässt sich der Beweis auf ungerade Primzahlen reduzieren.
Beweis: Siehe Proben[7], p.14-17.

6. Literaturverzeichnis

[1] A. Blanchard. Les corps noncommutatifs. Presses Universitaires de France, Paris (1972). p.7-8.

[2] W. Blaschke. Kinematik und Quaternionen. Deutscher Verlag der Wissenschaft. Berlin (1960). p.1-4.

[3] E. Peschl. Analytische Geometrie. BI-Hochschultaschenbücher Band 15/15a. Mannheim (1961). p.118-128.

[4] Ch. Small. Sums of three squares and levels of quadradic number fields. Amer. Math. Monthly 93 (1986). p.276-279.

[5] J. Dieudonné. Algèbre linéaire et Géométrie élémentaire. Hermann. Paris (1968). p.197-207.

[6] M. Koecher, R. Remmert. Zahlen. Springer-Verlag. Berlin (1992). p.149-232.

[7] W. Ness. Proben der elementaren additiven Zahlentheorie.