Kapitel 6
Gaußsche Zahlen und Quaternionen

Die algebraische Zahlentheorie untersucht neben den „klassischen“ ganzen Zahlen auch ganze Zahlen in Erweiterungskörpern von $\mathbb{Q}$; teilweise führt dies auch zu einem besseren Verständnis von Sätzen der elementaren Zahlentheorie. Hier wollen wir uns auf ein einziges Beispiel beschränken, die sogenannten GAUSSschen Zahlen, und dazu noch eine nichtkommutative Verallgemeinerung betrachten, die Quaternionen.

§1: Der Ring der Gaußschen Zahlen

GAUSSsche Zahlen sind komplexe Zahlen $x + iy$ mit $x, y \in \mathbb{Z}$; wir bezeichnen die Menge aller dieser Zahlen mit $\mathbb{Z}[i] = \mathbb{Z} \oplus i\mathbb{Z}$. Da Summen und Produkte GAUSSscher Zahlen wieder GAUSSsche Zahlen sind, überlegt man sich leicht, daß $\mathbb{Z}[i]$ ein Ring ist.

Definition: $z = x + iy$ sei eine GAUSSsche Zahl.
a) $\overline{z} = x - iy$ heißt die zu z *konjugiert komplexe* Zahl.
b) $N(z) = z\overline{z} = x^2 + y^2$ heißt die *Norm* von z.
c) $z \in \mathbb{Z}[i]$ heißt *Einheit,* wenn es eine Zahl $w \in \mathbb{Z}[i]$ gibt, so daß $zw = 1$ ist.
d) $z \in \mathbb{Z}[i]$ heißt *irreduzibel,* falls gilt: z ist keine Einheit, und ist $z = wq$ Produkt zweier GAUSSscher Zahlen, so muß w oder q eine Einheit sein.

Lemma: *a)* Für $z, w \in \mathbb{Z}[i]$ ist $N(zw) = N(z)N(w)$.
b) $z \in \mathbb{Z}[i]$ ist genau dann eine Einheit, wenn $N(z) = 1$ ist.
c) Die Einheiten sind genau die vier Zahlen $1, -1, i$ und $-i$.
d) Ist $N(z)$ eine Primzahl, so ist z irreduzibel.

Beweis: a) $N(zw) = zw \cdot \overline{zw} = zw\overline{z}\overline{w} = z\overline{z}w\overline{w} = N(z)N(w)$.

b) Ist z eine Einheit, so gibt es ein $w \in \mathbb{Z}[i]$ mit $zw = 1$, und nach *a)* ist $N(z)N(w) = N(zw) = N(1) = 1$. Da die Norm einer GAUSSschen Zahl in $\mathbb{N}_0$ liegt, folgt $N(z) = N(w) = 1$. Ist umgekehrt $N(z) = 1$, so ist nach Definition von $N(z) = z\overline{z}$ das Produkt $z\overline{z} = 1$, d.h. z ist eine Einheit.

c) $z = x+iy$ sei nach *b)* genau dann eine Einheit, wenn $N(z) = x^2+y^2 = 1$ ist. Da x und y ganze Zahlen sind, muß eine der beiden verschwinden und die andere ± 1 sein, was genau auf die vier angegebenen Fälle führt.

d) Ist $z = wq$, so ist nach *a)* auch $N(z) = N(w)N(q)$. Da alle Normen nichtnegative ganze Zahlen sind und $N(z)$ eine Primzahl, muß $N(w)$ oder $N(q)$ gleich eins sein, d.h. w oder q ist eine Einheit. ∎

Die Umkehrung von *d)* gilt nicht: Beispielsweise ist $N(3) = 3 \cdot 3 = 9$, aber trotzdem ist die Drei in $\mathbb{Z}[i]$ irreduzibel: Ist nämlich $3 = zw$, so ist $N(3) = N(z)N(w)$; falls weder z noch w eine Einheit ist, müssen also $N(z) = N(w) = 3$ sein. Es gibt aber keine GAUSSsche Zahl der Norm drei, denn die Gleichung $x^2 + y^2 = 3$ hat keine ganzzahligen Lösungen.

§2: Euklidische Ringe

In Kapitel I bewiesen wir die eindeutige Primzerlegung in $\mathbb{Z}$ mit Hilfe des EUKLIDischen Algorithmus. Um zu sehen, ob wir ähnliches auch für die GAUSSschen Zahlen beweisen können, liegt es daher nahe, Ringen zu untersuchen, in denen es einen EUKLIDischen Algorithmus gibt. Solche Ringe heißen EUKLIDische Ringe.

Wie wir gesehen haben, ist die Division mit Rest das wichtigste Werkzeug beim EUKLIDischen Algorithmus, und wie sich in diesem Abschnitt herausstellen wird, brauchen wir kein weiteres. Wir definieren daher

Definition: Ein EUKLIDischer Ring ist ein Integritätsbereich R zusammen mit einer Abbildung $\nu\colon R \setminus \{0\} \to \mathbb{N}_0$, so daß gilt: Ist $x|y$, so ist

$\nu(x) \leq \nu(y)$, und zu je zwei Elementen $x, y \in R$ gibt es Elemente $q, r \in R$ mit

$$x = qy + r \quad \text{und} \quad r = 0 \quad \text{oder} \quad \nu(r) < \nu(y)\,.$$

Wir schreiben auch $x : y = q$ Rest r und bezeichnen r als Divisionsrest bei der Division von x durch y.

Das Standardbeispiel ist natürlich der Ring $\mathbb{Z}$ der ganzen Zahlen mit $\nu(x) = |x|$. Ein anderes Beispiel ist der Polynomring $k[X]$ über einem Körper k: Hier können wir $\nu(f)$ für ein Polynom $f \neq 0$ als den Grad von f definieren; dann erfüllt auch die Polynomdivision mit Rest die Forderung an einen EUKLIDischen Ring.

Man beachte, daß weder der Quotient noch der Divisionsrest eindeutig bestimmt sein muß: Beispielsweise ist schon in $\mathbb{Z}$ einerseits $15 : 4 = 3$ Rest 3, andererseits aber auch 4 Rest -1, wobei letzteres im EUKLIDischen Algorithmus möglicherweise sogar schneller ans Ziel führt.

Lemma: In einem EUKLIDischen Ring R gibt es zu je zwei Elementen $x, y \in R$ einen ggT. Dieser kann nach dem EUKLIDischen Algorithmus berechnet werden und läßt sich als Linearkombination von x und y mit Koeffizienten aus R darstellen.

Beweis: In jedem Integritätsbereich folgt aus der Gleichung $x = qy + r$ mit $x, y, q, r \in R$, daß die gemeinsamen Teiler von x und y gleich denen von y und r sind. Speziell in einem EUKLIDischen Ring können wir dabei r als Divisionsrest wählen und, wie beim klassischen EUKLIDischen Algorithmus, danach y durch r dividieren *usw.,* wobei wir eine Folge von Divisionsresten r_i erhalten mit der Eigenschaft, daß in jedem Schritt die gemeinsamen Teiler von x und y gleich denen von r_{i-1} und r_i sind. Außerdem ist stets entweder $r_i = 0$ oder $\nu(r_i) < \nu(r_{i-1})$, so daß die Folge nach endlich vielen Schritten mit einem $r_n = 0$ abbrechen muß. Auch hier sind die gemeinsamen Teiler von r_{n-1} und $r_n = 0$ genau die gemeinsamen Teiler von x und y. Da jede Zahl Teiler der Null ist, sind die gemeinsamen Teiler von r_{n-1} und Null aber genau die Teiler von r_{n-1}, und unter diesen gibt es natürlich einen größten, nämlich r_{n-1} selbst. Somit haben auch x und y einen größten gemeinsamen Teiler,

nämlich den nach dem EUKLIDischen Algorithmus berechneten letzten von Null verschiedenen Divisionsrest r_{n-1}.

Auch die lineare Kombinierbarkeit folgt wie im klassischen Fall: Bei jeder Division mit Rest ist der Divisionsrest als Linearkombination von Dividend und Divisor darstellbar; beim EUKLIDischen Algorithmus beginnen wir mit Dividend x und Divisor y, die natürlich beide als Linearkombinationen von x und y darstellbar sind, und induktiv folgt, daß auch alle folgenden Dividenden und Divisoren sind als Reste einer vorangegangenen Division Linearkombinationen von x und y sind, also ist es auch ihr Divisionsrest. Insbesondere ist auch der ggT als letzter nichtverschwindender Divisionsrest Linearkombination von x und y, und die Koeffizienten können wie in Kapitel I mit dem erweiterten EUKLIDischen Algorithmus berechnet werden. ∎

Lemma: *a)* In einem EUKLIDischen Ring R ist jedes Element $x \neq 0$ mit $\nu(x) = 0$ eine Einheit.
b) Ist $x = yz \neq 0$, wobei y, z keine Einheiten sind, so ist $\nu(y) < \nu(x)$ und $\nu(z) < \nu(x)$.

Beweis: a) Wir dividieren eins durch x mit Rest: $1 : x = q$ Rest r. Dann ist entweder $r = 0$ oder aber $\nu(r) < \nu(x) = 0$. Letzteres ist nicht möglich, also ist $qx = 1$ und x eine Einheit.

b) Da y und z Teiler von x sind, sind $\nu(y), \nu(z) \leq \nu(x)$. Um zu zeigen, daß $\nu(y)$ echt kleiner als $\nu(x)$ ist, dividieren wir y mit Rest durch x; das Ergebnis sei q Rest r, d.h. $y = qx + r$ mit $r = 0$ oder $\nu(r) < \nu(x)$. Wäre $r = 0$, wäre y ein Vielfaches von x, es gäbe also ein $u \in R$ mit $y = ux = u(yz) = (uz)y$. Damit wäre $uz = 1$, also z eine Einheit, im Widerspruch zur Annahme. Somit ist $\nu(r) < \nu(x)$.

Als Teiler von x ist y auch Teiler von $r = y - qx = y(1 - qz)$, also muß $\nu(y) \leq \nu(r) < \nu(x)$ sein. Genauso folgt, daß auch $\nu(z) < \nu(x)$ ist. ∎

Satz: Jeder EUKLIDische Ring ist faktoriell.

Beweis: Wir müssen zeigen, daß jedes Element $x \neq 0$ aus R bis auf Reihenfolge und Assoziiertheit eindeutig als Produkt aus einer Einheit und

geeigneten Potenzen irreduzibler Elemente geschrieben werden kann. Wir beginnen damit, daß sich x überhaupt in dieser Weise darstellen läßt.

Dazu benutzen wir die Betragsfunktion $\nu\colon R \setminus \{0\} \to \mathbb{N}_0$ des EUKLIDischen Rings R und beweisen induktiv, daß für $n \in \mathbb{N}_0$ alle $x \neq 0$ mit $\nu(x) \leq n$ in der gewünschten Weise darstellbar sind.

Ist $\nu(x) = 0$, so ist x nach obigem Lemma eine Einheit. Diese kann als sich selbst mal dem leeren Produkt von Potenzen irreduzibler Elemente geschrieben werden.

Für $n > 1$ unterscheiden wir zwei Fälle: Ist x irreduzibel, so ist $x = x$ eine Darstellung der gewünschten Form, und wir sind fertig.

Andernfalls läßt sich $x = yz$ als Produkt zweier Elemente schreiben, die beide keine Einheiten sind. Somit sind nach obigem Lemma $\nu(y) < \nu(x)$ und $\nu(z) < \nu(x)$, beide lassen sich also nach Induktionsvoraussetzung als Produkte von Einheiten und Potenzen irreduzibler Elemente schreiben. Damit läßt sich auch $x = yz$ so darstellen.

Als nächstes müssen wir uns überlegen, daß diese Darstellung bis auf Reihenfolge und Einheiten eindeutig ist. Das wesentliche Hilfsmittel hierzu ist die folgende Zwischenbehauptung:

Falls ein irreduzibles Element p ein Produkt xy teilt, teilt es mindestens einen der beiden Faktoren.

Zum *Beweis* betrachten wir den ggT von x und p. Dieser ist insbesondere ein Teiler von p, also bis auf Assoziiertheit entweder p oder 1. Im ersten Fall ist p Teiler von x und wir sind fertig; andernfalls können wir

$$1 = \alpha p + \beta x$$

als Linearkombination von p und x schreiben. Multiplikation mit y macht daraus $y = \alpha p x + \beta x y$, und hier sind beide Summanden auf der rechten Seite durch p teilbar: Bei $\alpha p x$ ist das klar, und bei $\beta x y$ folgt es daraus, daß nach Voraussetzung p ein Teiler von xy ist. Also ist p Teiler von y, und die Zwischenbehauptung ist bewiesen.

Induktiv folgt sofort:

Falls ein irreduzibles Element p ein Produkt $\prod_{i=1}^{r} x_i$ teilt, teilt es mindestens einen der Faktoren x_i.

Um den Beweis des Satzes zu beenden, zeigen wir induktiv, daß für jedes $n \in \mathbb{N}_0$ alle Elemente mit $\nu(x) \leq n$ eine bis auf Reihenfolge und Einheiten eindeutige Primfaktorzerlegung haben.

Für $n = 0$ ist x eine Einheit; hier ist die Zerlegung $x = x$ eindeutig.

Seien nun

$$x = u \prod_{i=1}^{r} p_i^{e_i} = v \prod_{j=1}^{s} q_j^{f_j}$$

zwei Zerlegungen eines Elements $x \in R$, wobei wir annehmen können, daß alle $e_i, f_j \geq 1$ sind. Dann ist p_1 trivialerweise Teiler des ersten Produkts, also auch des zweiten. Wegen der Zwischenbehauptung teilt p_1 also mindestens eines der Elemente q_j, d.h. $p_1 = wq_j$ ist bis auf eine Einheit w gleich q_j. Da p_1 keine Einheit ist, ist $\nu(x/p_1) < \nu(x)$; nach Induktionsannahme hat also $x/p_1 = x/(wq_j)$ eine bis auf Reihenfolge und Einheiten eindeutige Zerlegung in irreduzible Elemente. Damit hat auch x diese Eigenschaft.

∎

Bemerkung: Die Umkehrung dieses Satzes gilt nicht: Beispielsweise sind nach einem Satz von GAUSS auch $\mathbb{Z}[X]$ sowie Polynomringe in mehr als einer Veränderlichen über $\mathbb{Z}$ oder einem Körper faktoriell, aber keiner dieser Ringe ist EUKLIDisch, da sich weder der ggT eins von zwei und X in $\mathbb{Z}[X]$ noch der ggT eins von X und Y in $k[X, Y]$ als Linearkombination der Ausgangselemente schreiben läßt.

Wir interessieren uns in diesem Kapitel vor allem für die GAUSSschen Zahlen und wollen uns überlegen, daß auch diese einen EUKLIDischen Ring bilden.

Dazu brauchen wir zunächst eine Abbildung ν nach $\mathbb{N}_0$. Für $\mathbb{Z}$ konnten wir einfach den Betrag nehmen; für die GAUSSschen Zahlen können wir unser Glück versuchen mit der Norm.

Falls $\mathbb{Z}[i]$ zusammen mit der Norm ein EUKLIDischer Ring ist, muß es zu je zwei Elementen $r, s \in \mathbb{Z}[i]$ mit $s \neq 0$ ein Element $q \in \mathbb{Z}[i]$

geben, so daß $\mathrm{N}(r - sq) < \mathrm{N}(s)$ ist. Division durch s macht daraus die Ungleichung

$$\mathrm{N}\Big(\frac{r}{s} - q\Big) < \mathrm{N}(1) = 1\,.$$

Da sich jedes Element von $\mathbb{Q}[i]$ als so ein Quotient r/s mit $r, s \in \mathbb{Z}[i]$ darstellen läßt, muß es also zu jedem $z \in \mathbb{Q}[i]$ ein $w \in \mathbb{Z}[i]$ geben, so daß $\mathrm{N}(z-w) < 1$ ist. Dazu schreiben wir $z = x+iy$ mit x, y aus $\mathbb{Q}$ und wählen ganze Zahlen u, v derart, daß $|x - u|$ und $|y - v|$ kleiner oder gleich $\frac{1}{2}$ sind. Für $w = u + iv$ ist dann $\mathrm{N}(z - w) = (x - u)^2 + ((y - v)^2 \leq \frac{1}{2} < 1$. Damit ist gezeigt, daß $\mathbb{Z}[i]$ ein EUKLIDischer und damit auch faktorieller Ring ist.

Betrachten wir als Beispiel die Division von $23 + 9i$ durch $2 - 3i$. In $\mathbb{Q}[i]$ ist

$$\frac{23 + 9i}{2 - 3i} = \frac{(23 + 9i)(2 + 3i)}{13} = \frac{19}{13} + \frac{87}{13}i\,.$$

Da $19 : 13 = 1$ Rest 6 und $87 : 13 = 6$ Rest 9 ist, liegt das Element $1 + 7i$ aus $\mathbb{Z}[i]$ am nächsten bei dieser Zahl. Die Norm von

$$\frac{19}{13} + \frac{87}{13}i - (1 + 7i) = \frac{6}{13} - \frac{4}{13}i$$

ist $(6^2 + 4^2)/13^2 = 52/169$ und damit deutlich kleiner als eins. Somit ist

$$(23 + 9i) : (2 - 3i) = (1 + 7i) \text{ Rest } -2i$$

ein mögliches Ergebnis der Division mit Rest. Ein anderes wäre

$$(23 + 9i) : (2 - 3i) = (1 + 6i) \text{ Rest } 3\,,$$

denn auch die Norm von 3 ist kleiner als die von $2 + 3i$. (Der Rest wurde jeweils als Dividend minus Divisor mal Quotient berechnet.)

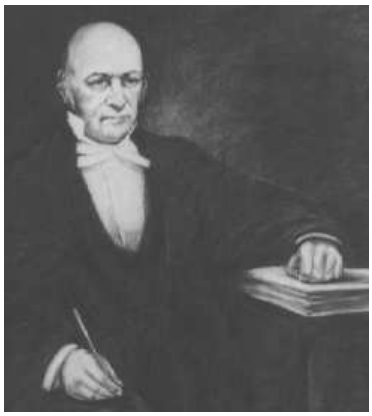
§3: Quaternionen

Nachdem durch die komplexen Zahlen $\mathbb{R}^2$ mit der Struktur eines Körpers versehen war, versuchten viele Mathematiker ähnliches auch für $\mathbb{R}^3$ zu erreichen. Natürlich kann weder $\mathbb{R}^3$ noch sonst ein $\mathbb{R}^n$ mit $n > 2$ zu einem Körper gemacht werden, denn ein solcher Körper wäre eine

algebraische Erweiterung von $\mathbb{R}$; da aber der algebraische Abschluß von $\mathbb{R}$ gleich $\mathbb{C}$ ist, muß dann $n = 1$ oder $n = 2$ sein.

Die damaligen Mathematiker waren jedoch bescheidener: Ihnen genügte es, einfach irgendeine Art von Multiplikation zu finden, die nicht unbedingt allen Körperaxiomen genügte – von Körpern sprach damals ohnehin noch niemand.

Erst 1940 konnte HEINZ HOPF (1894–1971) (auf dem Umweg über Vektorfelder auf Sphären) zeigen, daß das nicht möglich ist: Selbst eine bilineare Abbildung $\mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}^n$ kann nur dann existieren, wenn n eine Zweierpotenz ist, und 1958 zeigten dann unabhängig voneinander und mit verschiedenen Methoden JOHN MILNOR und MICHEL KERVAIRE, daß auch noch $n \leq 8$ sein muß, so daß nur die vier Möglichkeiten $n = 1, 2, 4$ und 8 in Frage kommen. Genau in diesen Fällen waren auch bereits entsprechende Produkte bekannt: Für $n = 1$ und 2 haben wir natürlich die reelle *bzw.* komplexe Multiplikation. Den Fall $n = 4$ löste HAMILTON 1843: Er fand eine Multiplikation auf $\mathbb{R}^4$, die zwar nicht kommutativ ist, ansonsten aber alle Körperaxiome erfüllt. Man spricht in so einem Fall von einem *Schiefkörper* oder, in der neueren Literatur, einer *Divisionsalgebra.* HAMILTON bezeichnete seine vierdimensionalen Zahlen als *Quaternionen.* Kurz danach konstruierte ARTHUR CAYLEY (1821–1895) ein nicht-assoziatives Produkt auf $\mathbb{R}^8$; die so erhaltenen „Zahlen“ nannte er *Oktaven.*



WILLIAM ROWEN HAMILTON (1805–1865) wurde in Dublin geboren; bereits mit fünf Jahren sprach er Latein, Griechisch und Hebräisch. Mit dreizehn begann er, mathematische Literatur zu lesen, mit 21 wurde er, noch als Student, Professor der Astronomie am Trinity College in Dublin. Er verlor allerdings schon bald sein Interesse an der Astronomie und beschäftigte sich stattdessen mit mathematischen und physikalischen Problemen. Am bekanntesten ist er für seine Entdeckung der Quaternionen, vorher publizierte er aber auch bedeutende Arbeiten über Optik, Dynamik und Algebra.

HAMILTON wählte eine Basis von $\mathbb{H} = \mathbb{R}^4$, die aus der Eins sowie drei „imaginären Einheiten“ $\mathbf{i}, \mathbf{j}, \mathbf{k}$ besteht, d.h. $\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -1$. Außerdem postulierte er, daß $\mathbf{ij} = -\mathbf{ji} = \mathbf{k}$ sein sollte; daraus lassen sich dann über

das Assoziativgesetz auch die anderen Produkte imaginärer Einheiten berechnen.

Damit ist, wenn man die Gültigkeit des Distributivgesetzes postuliert, eine Multiplikation auf $\mathbb{R}^4$ definiert; der Beweis, daß hierbei alle Körperaxiome außer der Kommutativität der Multiplikation erfüllt sind, enthält wie üblich nur einen etwas schwierigeren Punkt, die Existenz von Inversen; der Rest ist mühsame Abhakerei.

Zum Glück fand CAYLEY 1858 einen einfacheren Weg: Die vier komplexen 2×2-Matrizen

$$E = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},\ I = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},\ J = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \text{ und } K = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$$

erfüllen dieselben Relationen

$$I^2 = J^2 = K^2 = -E \quad \text{und} \quad IJ = -JI = K\,;$$

wir können also die Quaternion $a + bi + cj + dk$ identifizieren mit der Matrix

$$aE + bI + cJ + dK = \begin{pmatrix} a+di & b+ci \\ -b+ci & a-di \end{pmatrix} \in \mathbb{C}^{2\times 2}\,.$$

Da für Matrizen das Assoziativgesetz wie auch das Distributivgesetz gelten, ist klar, daß das Produkt zweier solcher Matrizen wieder von derselben Form ist und daß auch die Quaternionenmultiplikation Assoziativ- und Distributivgesetz erfüllt.

Die Quaternionen entsprechen somit genau den komplexen 2×2-Matrizen der Form

$$\begin{pmatrix} \alpha & \beta \\ -\overline{\beta} & \overline{\alpha} \end{pmatrix} \quad \text{mit} \quad \alpha = a + di, \beta = b + ci\,.$$

Die Determinante dieser Matrix ist $\alpha\overline{\alpha} + \beta\overline{\beta} = a^2 + b^2 + c^2 + d^2$.

Definieren wir in Analogie zum Fall der quadratischen Zahlkörper wieder das konjugierte Element zu $\gamma = a + bi + cj + dk$ als die Quaternion $\overline{\gamma} = a - bi - cj - dk$, so entspricht $\overline{\gamma}$ der Matrix

$$\begin{pmatrix} \overline{\alpha} & -\beta \\ \overline{\beta} & \alpha \end{pmatrix} \quad \text{und} \quad \begin{pmatrix} \alpha & \beta \\ -\overline{\beta} & \overline{\alpha} \end{pmatrix} \begin{pmatrix} \overline{\alpha} & -\beta \\ \overline{\beta} & \alpha \end{pmatrix} = (\alpha\overline{\alpha} + \beta\overline{\beta})E\,.$$

Damit folgt insbesondere, daß $\gamma\overline{\gamma}$ eine reelle Zahl ist, die genau dann verschwindet, wenn $\gamma = 0$ ist. Wir bezeichnen diese Zahl wieder als die *Norm* $\mathrm{N}(\gamma)$ der Quaternion γ, und wieder ist $\overline{\gamma}/\mathrm{N}(\gamma)$ das multiplikative Inverse zu γ – sowohl für die Links- als auch die Rechtsmultiplikation.

$\mathrm{N}(\gamma)$ ist gleichzeitig die Determinante der γ zugeordneten Matrix; aus dem Multiplikationssatz für Determinanten folgt daher sofort die Formel

$$\mathrm{N}(\gamma\delta) = \mathrm{N}(\gamma)\mathrm{N}(\delta)\,.$$