Gauß'sche Zahlen

Moritz Hiebler

19.10.2021

Der Aufbau dieser Arbeit orientiert sich an [1], die Resultate sind jedoch ein wenig umstrukturiert und an $\mathbb{Z}[\mathrm{i}]$ (statt $\mathbb{Z}[\phi]$) angepasst. Wie in [1] werden keine tieferen Vorkenntnisse über Algebra vorausgesetzt und die Anzahl neuer (algebraischer) Konzepte wurde bewusst gering gehalten.

1 Einleitung

Definition. Unter den *Gauß'schen Zahlen* (oder auch *Gauß'schen ganzen Zahlen*) versteht man die Teilmenge

$$\mathbb{Z}[\mathrm{i}] \coloneqq \{a + b\,\mathrm{i} \mid a, b \in \mathbb{Z}\}$$

der komplexen Zahlen, wobei i die imaginäre Einheit mit $\mathrm{i}^2 = -1$ bezeichnet.

Für zwei Elemente z, $w \in \mathbb{Z}[\mathrm{i}]$ liegen auch $z \pm w$ und $z \cdot w$ wieder in $\mathbb{Z}[\mathrm{i}]$. (Man sagt in diesem Fall, dass $\mathbb{Z}[\mathrm{i}]$ einen *Unterring* von $\mathbb{C}$ bildet.)

Wir werden im Folgenden für $\mathbb{Z}[\mathrm{i}]$ Teilbarkeitsuntersuchungen durchführen und einen Satz über Existenz und Eindeutigkeit der Primfaktorzerlegung beweisen, mit dessen Hilfe wir die Darstellung von natürlichen Zahlen als Summe zweier Quadratzahlen genauer verstehen können (Zwei-Quadrate-Satz).

Zuerst zu dieser zentralen Verbindung eine im Folgenden sehr nützliche

Definition. Für eine Gauß'sche Zahl z sei $\mathrm{N}(z) \coloneqq z \cdot \overline{z} = |z|^2$ die *Norm* von z.

Die Norm ist multiplikativ, d. h. $\mathrm{N}(wz) = wz \cdot \overline{wz} = w\overline{w} \cdot z\overline{z} = \mathrm{N}(w) \cdot \mathrm{N}(z)$. Bei $z = a + b\,\mathrm{i}$ mit a, $b \in \mathbb{Z}$ erhält man $\mathrm{N}(z) = a^2 + b^2 \in \mathbb{Z}_{\geq 0}$, die interessante Summe zweier Quadratzahlen. Wir werden uns neben dem Studium von $\mathbb{Z}[\mathrm{i}]$ an sich vor allem mit der Frage beschäftigen, welche ganzen Zahlen die Norm einer Gauß'schen Zahl sind. Nachdem $\mathrm{N}(z) = 0$ genau für $z = 0$ erfüllt ist, werden wir von nun an vor allem positive Normen studieren.

Zunächst können wir ein Resultat, analog zur Division mit Rest in $\mathbb{Z}$, zeigen:

Satz 1.1 (Division mit Rest in $\mathbb{Z}[\mathrm{i}]$)**.** *Seien z, $w \in \mathbb{Z}[\mathrm{i}]$ mit $z \neq 0$. Dann gibt es q, $r \in \mathbb{Z}[\mathrm{i}]$ mit $w = q \cdot z + r$ und $\mathrm{N}(r) < \mathrm{N}(z)$.*

Beweis. Sei $a \coloneqq \lfloor \mathrm{Re}(w/z) \rceil$, $b \coloneqq \lfloor \mathrm{Im}(w/z) \rceil$, $q \coloneqq a + b\,\mathrm{i}$ und $r \coloneqq w - qz$.[1] Nach Definition gilt

$$\left|\frac{r}{z}\right| = \left|\frac{w}{z} - q\right| \leq \sqrt{\left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2} = \sqrt{\frac{1}{2}}$$

[1] Dabei steht $\lfloor x \rceil$ bei $x \in \mathbb{R}$ für die ganze Zahl mit dem kleinsten Abstand zu x. Bei gleichem Abstand zu zwei ganzen Zahlen werde aufgerundet (*kaufmännisches Runden*).

und daraus folgt wegen $\mathrm{N}(z) > 0$ auch

$$w = qz + r \qquad \text{mit} \qquad \mathrm{N}(r) = |r|^2 \leq \frac{|z|^2}{2} = \frac{\mathrm{N}(z)}{2} < \mathrm{N}(z). \qquad \square$$

Die Zahlen q und r sind allerdings nicht eindeutig bestimmt, wie man beispielsweise gut bei der Division von $1 + \mathrm{i}$ durch 2 erkennen kann:

$$1 + \mathrm{i} = 0 \cdot 2 + (1 + \mathrm{i}) = \mathrm{i} \cdot 2 + (1 - \mathrm{i}) \qquad \text{und} \qquad 2 = \mathrm{N}(1 + \mathrm{i}) = \mathrm{N}(1 - \mathrm{i}) < \mathrm{N}(2) = 4$$

2 Teilbarkeit und Primfaktorzerlegung Gauß'scher Zahlen

Widmen wir uns nun der Teilbarkeit, die ganz analog zu der in $\mathbb{Z}$ definiert wird:

Definition. Seien z, $w \in \mathbb{Z}[\mathrm{i}]$. Wir sagen, *$z$ teilt w* oder *w ist (in $\mathbb{Z}[\mathrm{i}]$) durch z teilbar*, falls es ein $q \in \mathbb{Z}[\mathrm{i}]$ mit $w = z \cdot q$ gibt, und schreiben dafür $z \mid w$ (in $\mathbb{Z}[\mathrm{i}]$).

Für eine Primfaktorzerlegung braucht es eine Verallgemeinerung des Primzahlbegriffes der positiven ganzen Zahlen. Leider gibt es im Allgemeinen zwei Möglichkeiten dafür, die nicht zusammenfallen müssen. Wir werden aber bald sehen, dass sie das in $\mathbb{Z}[\mathrm{i}]$ doch tun.

Definition (Primelement)**.** Seien z und w zwei Gauß'sche Zahlen. Ein $\pi \in \mathbb{Z}[\mathrm{i}]$ mit $\mathrm{N}(\pi) > 1$ heißt ein *Primelement* in $\mathbb{Z}[\mathrm{i}]$, falls aus $\pi \mid z \cdot w$ sogar ($\pi \mid z$ oder $\pi \mid w$) folgt.

Wegen der Multiplikativität der komplexen Konjugation ist mit $\pi \in \mathbb{Z}[\mathrm{i}]$ auch $\overline{\pi}$ ein Primelement in $\mathbb{Z}[\mathrm{i}]$ (Check!). Neben den Primelementen interessieren wir uns auch noch für die Teiler von 1:

Definition. Eine Gauß'sche Zahl e mit $e \mid 1$ in $\mathbb{Z}[\mathrm{i}]$ heißt *Einheit* von $\mathbb{Z}[\mathrm{i}]$. Die Menge aller Einheiten von $\mathbb{Z}[\mathrm{i}]$ bezeichnen wir mit $\mathbb{Z}[\mathrm{i}]^\times$.

Lemma 2.1 (Charakterisierung von Einheiten)**.** *Für $e \in \mathbb{Z}[\mathrm{i}]$ sind äquivalent:*

(a) $e \in \mathbb{Z}[\mathrm{i}]^\times$ (b) $\mathrm{N}(e) = 1$ (c) $e \in \{\pm 1, \pm \mathrm{i}\}$ (d) $1/e \in \mathbb{Z}[\mathrm{i}]^\times$

Beweis. Wir zeigen 2.1.(a) $\Longrightarrow$ 2.1.(b) $\Longrightarrow$ 2.1.(c) $\Longrightarrow$ 2.1.(d) $\Longrightarrow$ 2.1.(a).

2.1.(a) $\Longrightarrow$ 2.1.(b): Sei $f \in \mathbb{Z}[\mathrm{i}]$ mit $ef = 1$. Es folgt $\mathrm{N}(e)\,\mathrm{N}(f) = \mathrm{N}(1) = 1$ und nachdem 1 nur sich selbst als positiven Teiler hat, auch $\mathrm{N}(e) = \mathrm{N}(f) = 1$.

2.1.(b) $\Longrightarrow$ 2.1.(c): Schreiben wir $e = a + b\,\mathrm{i}$ mit a, $b \in \mathbb{Z}$, so gilt nach Voraussetzung $a^2 + b^2 = 1$, was auf $a^2 \leq 1$, somit $a \in \{-1, 0, 1\}$ und nach Durchprobieren auf $(a, b) \in \{(0, \pm 1), (\pm 1, 0)\}$ führt. Daher ist e von der behaupteten Form.

2.1.(c) $\Longrightarrow$ 2.1.(d): Für diese vier Werte gilt offenbar $1/e = \overline{e} \in \mathbb{Z}[\mathrm{i}]$.

2.1.(d) $\Longrightarrow$ 2.1.(a): Wir erhalten mit $1/e \in \mathbb{Z}[\mathrm{i}]^\times \subseteq \mathbb{Z}[\mathrm{i}]$ aus $e \cdot (1/e) = 1$ direkt $e \mid 1$. $\square$

Wir können nun die erwähnte Äquivalenz beweisen.

Proposition 2.2. *Seien π, z und w Gauß'sche Zahlen mit $\mathrm{N}(\pi) > 1$. Dann sind äquivalent:*

(a) *π ist ein Primelement.*

(b) *π ist* unzerlegbar*: Aus $\pi = z \cdot w$ folgt $z \in \mathbb{Z}[\mathrm{i}]^\times$ oder $w \in \mathbb{Z}[\mathrm{i}]^\times$.*

Beweis. 2.2.(a) $\Longrightarrow$ 2.2.(b): Sei π ein Primelement in $\mathbb{Z}[\mathrm{i}]$ und $1 \cdot \pi = z \cdot w$. Daher gilt $\pi \mid z \cdot w$ und nach Voraussetzung $\pi \mid z$ oder $\pi \mid w$, o. B. d. A. $\pi \mid z$. Schreibe $z = \pi u$ für ein $u \in \mathbb{Z}[\mathrm{i}]$. Einsetzen liefert $\pi = (\pi u)w \iff 1 = uw$ und Lemma 2.1 ergibt $w \in \mathbb{Z}[\mathrm{i}]^\times$.

2.2.(a) $\Longrightarrow$ 2.2.(b): Sei nun π unzerlegbar und es gelte $\pi \mid z \cdot w$ sowie $\pi \nmid z$. Wir müssen $\pi \mid w$ beweisen. Dazu zeigen wir zuerst, dass es s, $t \in \mathbb{Z}[\mathrm{i}]$ mit $s\pi + tz \in \mathbb{Z}[\mathrm{i}]^\times$ gibt.

Unter allen Zahlen ζ aus $\mathbb{Z}[\mathrm{i}] \setminus \{0\}$ der Form $\lambda\pi + \mu z$ mit λ, $\mu \in \mathbb{Z}[\mathrm{i}]$ sei $e \coloneqq s\pi + tz$ (s, $t \in \mathbb{Z}[\mathrm{i}]$) eine mit kleinster Norm. Wir behaupten $e \mid \zeta$ und dividieren dazu ζ durch e mit Rest (vgl. Satz 1.1): Es gibt q, $r \in \mathbb{Z}[\mathrm{i}]$ mit $\zeta = qe + r$ und $\mathrm{N}(r) < \mathrm{N}(e)$. Aus $r = \zeta - qe = (\lambda - qs)\pi + (\mu - qt)z$ und der Voraussetzung, dass e unter allen diesen Zahlen $\neq 0$ minimale Norm hat, folgt $r = 0$; d. h. ζ ist durch e teilbar. Für $\zeta = 1 \cdot \pi + 0 \cdot z$ erhalten wir $e \mid \pi$, also ein $v \in \mathbb{Z}[\mathrm{i}]$ mit $\pi = e \cdot v$. Da π unzerlegbar ist, folgt $e \in \mathbb{Z}[\mathrm{i}]^\times$ oder $v \in \mathbb{Z}[\mathrm{i}]^\times$. In letzterem Fall ergibt sich für $\zeta = 0 \cdot \pi + 1 \cdot z = z$ der Widerspruch $\pi \mid \pi \cdot v^{-1} = e \mid z$ zur Annahme $\pi \nmid z$. Also bleibt nur $e \in \mathbb{Z}[\mathrm{i}]^\times$ übrig.

Wir schließen $w = (se^{-1}w)\pi + (e^{-1}t)zw$ durch Multiplikation von $e = s\pi + tz$ mit $e^{-1}w \in \mathbb{Z}[\mathrm{i}]$. Nun teilt π beide Summanden rechts, also auch w. □

Umgekehrt heißt π *zerlegbar*, falls es z, $w \in \mathbb{Z}[\mathrm{i}]$ mit $\mathrm{N}(z)$, $\mathrm{N}(w) > 1$ und $\pi = z \cdot w$ gibt. Unzerlegbare Elemente können nur in trivialer Weise als Produkt geschrieben werden.

Vor dem Satz über die Existenz und Eindeutigkeit der Primfaktorzerlegung in $\mathbb{Z}[\mathrm{i}]$ benötigen wir noch

Lemma 2.3. *Jede Gauß'sche Zahl z mit $\mathrm{N}(z) > 1$ besitzt ein Primelement in $\mathbb{Z}[\mathrm{i}]$ als Teiler.*

Beweis. Unter allen Teilern von z in $\mathbb{Z}[\mathrm{i}]$ mit Norm größer als 1 gibt es einen Teiler π mit minimaler Norm. Wir behaupten, dass π unzerlegbar und daher nach Proposition 2.2 ein Primelement ist. Angenommen, $\pi = u \cdot w$ für Gauß'sche Zahlen u und w mit Norm größer als 1. Dann folgt $u \mid \pi \mid z$ und $\mathrm{N}(\pi) = \mathrm{N}(u) \cdot \mathrm{N}(w) > \mathrm{N}(u)$, im Widerspruch zur Wahl von π. □

Wir erhalten schließlich den zuvor angekündigten

Satz 2.4 (Primfaktorzerlegung in $\mathbb{Z}[\mathrm{i}]$)**.** *Jede Gauß'sche Zahl $z \neq 0$ besitzt eine bis auf Reihenfolge und Einheiten eindeutige Darstellung als Produkt von Primelementen in $\mathbb{Z}[\mathrm{i}]$.*

Präziser: Es gibt eine Darstellung $z = e \cdot \pi_1 \cdots \pi_r$ mit ganzem $r \geq 0$, $e \in \mathbb{Z}[\mathrm{i}]^\times$ und Primelementen $\pi_1, \ldots, \pi_r$ in $\mathbb{Z}[\mathrm{i}]$. Für jede weitere Darstellung $z = f \cdot q_1 \cdots q_s$ mit ganzem $s \geq 0$, $f \in \mathbb{Z}[\mathrm{i}]^\times$ und Primelementen $q_1, \ldots, q_s$ in $\mathbb{Z}[\mathrm{i}]$ gilt $r = s$ und es gibt eine Permutation $q'_1, \ldots, q'_r$ dieser Elemente mit $q'_j/\pi_j \in \mathbb{Z}[\mathrm{i}]^\times$ für $j = 1, \ldots, r$.

Beweis. Wir führen einen Beweis durch vollständige Induktion über $n = \mathrm{N}(z)$.

Als Induktionsanfang betrachten wir $\mathrm{N}(z) = 1$. Gemäß Lemma 2.1 bedeutet das $z = e \in \mathbb{Z}[\mathrm{i}]^\times$. Hier liegt obige Darstellung mit $r = 0$ vor. Da Primelemente nach Definition eine Norm größer als 1 haben, muss in jeder weiteren Darstellung wie im Satz $s = 0$ gelten; damit ist hier auch die Eindeutigkeit gezeigt.

Wir dürfen nun für den Induktionsschritt annehmen, dass $n > 1$ gilt und jedes $w \in \mathbb{Z}[\mathrm{i}] \setminus \{0\}$ mit $\mathrm{N}(w) < n$ eine im Satz angeführte, bis auf Reihenfolge und Einheiten eindeutige Darstellung besitzt.

Zuerst zur *Existenz:* Wegen $\mathrm{N}(z) = n > 1$ ist Lemma 2.3 anwendbar und liefert ein Primelement π in $\mathbb{Z}[\mathrm{i}]$, das z teilt. Wir schreiben $z = \pi \cdot w$ für ein $w \in \mathbb{Z}[\mathrm{i}] \setminus \{0\}$. Anwendung der Norm liefert $n = \mathrm{N}(z) = \mathrm{N}(\pi) \cdot \mathrm{N}(w) > \mathrm{N}(w)$; laut Induktionsannahme gilt folglich $w = e \cdot \pi_1 \cdots \pi_r$ mit den Bezeichnungen im Satz. Insgesamt erhalten wir $z = w \cdot \pi = e \cdot \pi_1 \cdots \pi_r \pi$.

Nun zur *Eindeutigkeit:* Sei $z = f \cdot q_1 \cdots q_s$ eine weitere Darstellung mit den Bedingungen wie im Satz. Wegen $\pi \mid z$ gibt es (laut Definition nach Induktion) ein ganzes $1 \leq k \leq s$ mit $\pi \mid q_k$.[2] Wir schreiben $q_k = \varepsilon \cdot \pi$ für ein $\varepsilon \in \mathbb{Z}[\mathrm{i}]$. Da q_k nach Proposition 2.2 unzerlegbar ist, folgt $\varepsilon \in \mathbb{Z}[\mathrm{i}]^\times$. Erneutes Einsetzen liefert mit $z/\pi = (f/\varepsilon) \cdot q_1 \cdots q_{k-1} q_{k+1} \cdots q_s$ eine weitere Darstellung von w als Produkt von $s-1$ Primelementen. Daraus schließen wir nach Induktionsannahme $s - 1 = r$ und die Existenz einer Permutation $q'_1, \ldots, q'_{s-1}$ von $q_1, \ldots, q_{k-1}, q_{k+1}, \ldots, q_s$ mit $q'_j/\pi_j \in \mathbb{Z}[\mathrm{i}]^\times$ für $j = 1, \ldots, r$. Setzen wir schließlich $q'_s \coloneqq q_k$ und beachten $q_k/\pi = \varepsilon \in \mathbb{Z}[\mathrm{i}]^\times$, so beendet dies auch den Beweis der Eindeutigkeit. □

3 Primelemente der Gauß'schen Zahlen

3.1 Wie steht es um die Primzahlen?

Zum besseren Verständnis dieser Primfaktorzerlegung wollen wir schließlich noch die Primelemente in $\mathbb{Z}[\mathrm{i}]$ charakterisieren und beginnen mit den vielversprechenden Kandidaten, die wir bereits aus $\mathbb{Z}^+$ kennen:

Lemma 3.1. *Sei $z = a + b\,\mathrm{i} \in \mathbb{Z}[\mathrm{i}]$ mit a, $b \in \mathbb{Z}$ und $\mathrm{ggT}(a, b) = 1$. Dann ist jeder ungerade Primteiler (in $\mathbb{Z}$) von $\mathrm{N}(z)$ kongruent zu 1 modulo 4.*

Beweis. Sei p ein ungerader Primteiler von $\mathrm{N}(z) = a^2 + b^2$. Wäre b durch p teilbar, so auch $a^2 = \mathrm{N}(z) - b^2$ und folglich a, im Widerspruch zu $\mathrm{ggT}(a, b) = 1$. Damit gibt es eine Lösung $y \in \mathbb{Z}$ der linearen Kongruenz $by \equiv 1 \pmod{p}$. Multiplikation von $a^2 \equiv -b^2 \pmod{p}$ mit y^2 liefert $(ay)^2 \equiv -(by)^2 \equiv -1 \pmod{p}$ und -1 ist somit ein quadratischer Rest modulo p. Nach dem quadratischen Reziprozitätsgesetz gilt schließlich

$$\left(\frac{-1}{p}\right) = 1 \quad \Longleftrightarrow \quad (-1)^{(p-1)/2} = 1 \quad \Longleftrightarrow \quad 2 \mid (p-1)/2 \quad \Longleftrightarrow \quad p \equiv 1 \pmod{4}. \qquad \square$$

Lemma 3.2. *Eine Primzahl $p \in \mathbb{Z}^+$ mit $p \equiv 1 \pmod{4}$ ist kein Primelement.*

Beweis. Mit dem quadratischen Reziprozitätsgesetzes erkennen wir -1 als quadratischen Rest modulo p (wie im Beweis zu Lemma 3.1 oben). Sei also $x \in \mathbb{Z}$ eine ganze Zahl mit

$$x^2 \equiv -1 \pmod{p} \qquad \Longleftrightarrow \qquad p \mid 1 + x^2 = (1 + x\,\mathrm{i})(1 - x\,\mathrm{i}).$$

Hierin ist weder $1 + x\,\mathrm{i}$ noch $1 - x\,\mathrm{i}$ durch p teilbar, da jedes Vielfache von p in $\mathbb{Z}[\mathrm{i}]$ (wegen $p(a + b\,\mathrm{i}) = pa + pb\,\mathrm{i}$) für a, $b \in \mathbb{Z}$) einen durch p teilbaren Realteil hat.[3] □

Proposition 3.3. *Eine Primzahl $p \in \mathbb{Z}^+$ ist genau dann ein Primelement in $\mathbb{Z}[\mathrm{i}]$, wenn es kein $z \in \mathbb{Z}[\mathrm{i}]$ mit $p = \mathrm{N}(z)$ gibt.*

Beweis. Wir beweisen die logische Kontraposition (laut Proposition 2.2):

$$p \text{ ist zerlegbar} \quad \Longleftrightarrow \quad \exists z \in \mathbb{Z}[\mathrm{i}] \colon \mathrm{N}(z) = p$$

[2] Die Möglichkeit $\pi \mid f$ kann durch Anwendung der Norm ausgeschlossen werden.
[3] Danke an Paul Hametner für diesen schönen Beweis!

„$\Longrightarrow$“: Es gibt z und $w \in \mathbb{Z}[\mathrm{i}]$ mit $p = z \cdot w$ und $\mathrm{N}(z)$, $\mathrm{N}(w) > 1$. Anwendung der Norm liefert $p^2 = \mathrm{N}(p) = \mathrm{N}(z) \cdot \mathrm{N}(w)$. Wegen der Eindeutigkeit der Primfaktorzerlegung von positiven ganzen Zahlen und der Voraussetzung folgt $\mathrm{N}(z) = \mathrm{N}(w) = p$.

„$\Longleftarrow$“: Aus $p > 1$ folgt $p = \mathrm{N}(z) = \mathrm{N}(\overline{z}) > 1$. Nun erhalten wir mit $p = \mathrm{N}(z) = z \cdot \overline{z}$ die gewünschte Zerlegung. □

Proposition 3.4. *Eine Primzahl $p \in \mathbb{Z}^+$ ist genau dann ein Primelement in $\mathbb{Z}[\mathrm{i}]$, wenn $p \equiv 3 \pmod 4$ gilt.*

Beweis. Laut Proposition 3.3 ist p genau dann ein Primelement in $\mathbb{Z}[\mathrm{i}]$, wenn es kein $z \in \mathbb{Z}[\mathrm{i}]$ mit $\mathrm{N}(z) = p$ gibt. Wegen $\mathrm{N}(1 + \mathrm{i}) = 2$ ($\not\equiv 3 \pmod 4$) müssen wir nur mehr ungerade Primzahlen p betrachten. Lemma 3.2 zeigt, dass Primzahlen $p \equiv 1 \pmod 4$ keine Primelemente in $\mathbb{Z}[\mathrm{i}]$ sind. Als einzige Kandidaten bleiben somit nur $p \equiv 3 \pmod 4$ übrig.

Es bleibt noch zu beweisen, dass es zu Primzahlen $p \equiv 3 \pmod 4$ kein $z \in \mathbb{Z}[\mathrm{i}]$ mit $\mathrm{N}(z) = p$ gibt. Wir wählen den Ansatz $z = a + b\,\mathrm{i}$ mit a, $b \in \mathbb{Z}$. Für $d := \mathrm{ggT}(a, b)$ gilt $d^2 \mid \mathrm{N}(z)$, d. h. bei $d > 1$ kann $\mathrm{N}(z) = p$ nicht gelten. Bei $d = 1$ kommt jedoch Lemma 3.1 zu greifen, wonach $p \equiv 3 \pmod 4$ kein Primteiler der Norm einer solchen Gauß'schen Zahl sein kann. □

3.2 Charakterisierung der Primelemente

Das nächste Resultat gibt eine notwendige Bedingung für Primelemente an:

Lemma 3.5. *Jedes Primelement π in $\mathbb{Z}[\mathrm{i}]$ erfüllt $\mathrm{N}(\pi) = p$ oder $\mathrm{N}(\pi) = p^2$ für eine Primzahl $p \in \mathbb{Z}^+$. Bei $\mathrm{N}(\pi) = p^2$ gilt außerdem $\pi = e \cdot p$ für ein $e \in \mathbb{Z}[\mathrm{i}]^\times$.*

Bemerkung. Der Zusatz besagt, dass der zweite Fall nur für Primelemente auf den Achsen der Gauß'schen Zahlenebene eintreten kann.

Beweis. Ist $\mathrm{N}(\pi)$ eine Primzahl, bleibt nichts zu zeigen. Sonst gibt es positive ganze Zahlen a, $b > 1$ mit $\mathrm{N}(\pi) = ab$. Aus $\mathrm{N}(\pi) = \pi\overline{\pi} = ab$ ergibt sich $\pi \mid a$ oder $\pi \mid b$ in $\mathbb{Z}[\mathrm{i}]$, o. B. d. A. $\pi \mid a$. Wir schreiben $a = \pi e$ für ein $e \in \mathbb{Z}[\mathrm{i}]$ und erhalten daraus $\pi\overline{\pi} = ab = \pi eb$, d. h. $\overline{\pi} = eb$. Nachdem mit π auch $\overline{\pi}$ ein Primelement (und nach Proposition 2.2 unzerlegbar) ist, gilt $e \in \mathbb{Z}[\mathrm{i}]^\times$ oder $b \in \mathbb{Z}[\mathrm{i}]^\times$. Da Letzteres im Widerspruch zu $b > 1$ steht, bleibt nur $e \in \mathbb{Z}[\mathrm{i}]^\times$ zu untersuchen. Dann gilt aber $a^2 = \mathrm{N}(a) = \mathrm{N}(\pi) \cdot \mathrm{N}(e) = ab \cdot 1$, also $a = b$. Jede Zerlegung von $\mathrm{N}(\pi)$ in zwei positive ganze Faktoren größer als 1 führt also zur Gleichheit dieser beiden Faktoren. Folglich kann $\mathrm{N}(\pi)$ nur einen Primfaktor $p \in \mathbb{Z}^+$ und diesen nur mit Vielfachheit 2 haben. Notwendigerweise gilt $a = p$ in dieser (eindeutigen) Zerlegung, was wegen $\pi = (1/e)a = \overline{e}p$ auch den Zusatz beweist. □

Umgekehrt beweisen wir

Lemma 3.6. *Gilt $\mathrm{N}(z) = p$ für eine Primzahl $p \in \mathbb{Z}^+$, so ist z ein Primelement in $\mathbb{Z}[\mathrm{i}]$.*

Beweis. Es genügt nach Proposition 2.2, z als unzerlegbar nachzuweisen. Aus $z = u \cdot v$ für u, $v \in \mathbb{Z}[\mathrm{i}]$ folgt aber $\mathrm{N}(u)\,\mathrm{N}(v) = \mathrm{N}(z) = p$ und wegen der eindeutigen Primfaktorzerlegung in $\mathbb{Z}^+$ entweder $\mathrm{N}(u) = 1$ oder $\mathrm{N}(v) = 1$. Laut Lemma 2.1 erhalten wir entweder $u \in \mathbb{Z}[\mathrm{i}]^\times$ oder $v \in \mathbb{Z}[\mathrm{i}]^\times$. □

Endlich können wir die Primelemente von $\mathbb{Z}[\mathrm{i}]$ konkret angeben.

Satz 3.7 (Charakterisierung der Primelemente in $\mathbb{Z}[\mathrm{i}]$)**.** *Eine Gauß'sche Zahl π ist genau dann ein Primelement in $\mathbb{Z}[\mathrm{i}]$, wenn*

(a) $\mathrm{N}(\pi)$ *eine Primzahl in* $\mathbb{Z}^+$ *ist oder*

(b) $\pi = e \cdot p$ *mit* $e \in \mathbb{Z}[\mathrm{i}]^\times$ *und einer Primzahl* $p \in \mathbb{Z}^+$ *mit* $p \equiv 3 \pmod 4$ *gilt.*

Beweis. Sei zunächst $\pi \in \mathbb{Z}[\mathrm{i}]$ ein Primelement. Mit den Bezeichnungen aus Proposition 3.5 bleibt nur mehr zu zeigen, dass $p \equiv 3 \pmod 4$ gilt. Allerdings ist p notwendig unzerlegbar, also (nach Proposition 2.2) ein Primelement in $\mathbb{Z}[\mathrm{i}]$. Nun erhalten wir mit Proposition 3.4 das Gewünschte.

Erfüllt umgekehrt π eine der beiden angeführten Bedingungen, so garantiert Lemma 3.6 im ersten Fall und Proposition 3.4 im zweiten Fall (Zerlegbarkeit von p und $\pi = e \cdot p$ sind äquivalent), dass π ein Primelement ist. □

3.3 Darstellbarkeit als Norm einer Gauß'schen Zahl

Nun zeigen wir noch den anfangs erwähnten Zwei-Quadrate-Satz über die Darstellbarkeit von nichtnegativen ganzen Zahlen als Summe zweier Quadratzahlen, den wir hier zuerst bewusst in seiner Allgemeinheit formulieren.

Satz 3.8. *Eine positive ganze Zahl n ist genau dann die Norm einer Gauß'schen Zahl, wenn in der Primfaktorzerlegung von n über $\mathbb{Z}$ alle in $\mathbb{Z}[\mathrm{i}]$ unzerlegbaren Primzahlen nur in gerader Vielfachheit vorkommen.*

Beweis. Wir zeigen die beiden Implikationen einzeln:

„$\Longrightarrow$": Sei $n = \mathrm{N}(z)$ für ein $z \in \mathbb{Z}[\mathrm{i}]$. Laut Satz 2.4 gibt es eine Primfaktorzerlegung $z = e \cdot \pi_1 \cdots \pi_r$ in $\mathbb{Z}[\mathrm{i}]$ mit den Bezeichnnungen wie dort. Folglich ist $n = \mathrm{N}(z) = \mathrm{N}(\pi_1) \cdots \mathrm{N}(\pi_r)$. Sei nun $p \in \mathbb{Z}^+$ eine in $\mathbb{Z}[\mathrm{i}]$ unzerlegbare Primzahl. Nach Proposition 3.3 kann $\mathrm{N}(\pi_j) = p$ nicht gelten, laut Lemma 3.5 ist $\mathrm{v}_p(\mathrm{N}(\pi_j))$ für alle $j = 1, \ldots, r$ entweder 0 oder 2, insbesondere gerade. Folglich muss auch

$$\mathrm{v}_p(n) = \mathrm{v}_p(\mathrm{N}(\pi_1)) + \cdots + \mathrm{v}_p(\mathrm{N}(\pi_r))$$

gerade sein.

„$\Longleftarrow$": Alle in $\mathbb{Z}[\mathrm{i}]$ unzerlegbaren Primteiler von n mögen in gerader Vielfachheit vorkommen. Sei $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r} q_1^{\beta_1} \cdots q_s^{\beta_s}$ die Primfaktorzerlegung von n in $\mathbb{Z}$, wobei r, $s \in \mathbb{Z}_{\geq 0}$, $p_1, \ldots, p_r$ paarweise verschiedene, in $\mathbb{Z}[\mathrm{i}]$ unzerlegbare Primzahlen, $q_1, \ldots, q_s$ paarweise verschiedene, in $\mathbb{Z}[\mathrm{i}]$ zerlegbare Primzahlen, $\alpha_1, \ldots, \alpha_r, \beta_1, \ldots, \beta_s$ positive ganze Zahlen und $\alpha_1, \ldots, \alpha_r$ sämtlich gerade seien. Gemäß Proposition 3.3 gibt es $z_1, \ldots, z_s \in \mathbb{Z}[\mathrm{i}]$ mit $\mathrm{N}(z_j) = q_j$ für alle ganzen $1 \leq j \leq s$. Dann ist

$$z \coloneqq p_1^{\alpha_1/2} \cdots p_r^{\alpha_r/2} z_1^{\beta_1} \cdots z_s^{\beta_s}$$

eine Gauß'sche Zahl mit Norm n. □

Aus den Sätzen 3.7 und 3.8 erhalten wir schließlich direkt

Korollar 3.8.1 (Zwei-Quadrate-Satz)**.** *Eine positive ganze Zahl n ist genau dann als Summe zweier Quadratzahlen darstellbar, wenn in der Primfaktorzerlegung von n über $\mathbb{Z}$ alle Primzahlen kongruent zu 3 modulo 4 nur in gerader Vielfachheit vorkommen.*

Als Abschluss untersuchen wir, auf wie viele Arten man Primzahlen als die Summe zweier Quadratzahlen darstellen kann, d. h. wie viele Lösungen $(a, b) \in \mathbb{Z}^2$ die Gleichung

$$p = a^2 + b^2 \tag{$*$}$$

für eine Primzahl $p \in \mathbb{Z}^+$ besitzt. Für $p = 2$ erhält man die ganzzahligen Lösungen $(a, b) = (\pm 1, \pm 1)$ von $(*)$, wobei die Vorzeichen unabhängig voneinander gewählt werden können, somit insgesamt vier Lösungen.

Für $p \equiv 3 \pmod 4$ gibt es nach Proposition 3.4 keine Lösungen für $(*)$ und es bleibt nur noch $p \equiv 1 \pmod 4$ zu betrachten. Wir setzen $z \coloneqq a + b\,\mathrm{i}$ und erhalten äquivalent $\mathrm{N}(z) = a^2 + b^2 = p$. Bei $|a| = |b|$ wäre $p = 2a^2$ gerade, im Widerspruch zur Voraussetzung $p \equiv 3 \pmod 4$. Wegen $p = \mathrm{N}(e)\,\mathrm{N}(z) = \mathrm{N}(ez) = \mathrm{N}(e\overline{z})$ für alle $e \in \mathbb{Z}[\mathrm{i}]^\times$ erfüllen jedenfalls alle Gauß'schen Zahlen in der Menge

$$L \coloneqq \{ez \mid e \in \mathbb{Z}[\mathrm{i}]^\times\} \cup \{e\overline{z} \mid e \in \mathbb{Z}[\mathrm{i}]^\times\}$$

die äquivalente Normgleichung. Diese beiden Mengen sind disjunkt, denn aus $ez = f\overline{z}$ mit $e,\, f \in \mathbb{Z}[\mathrm{i}]^\times$ ergibt sich $z = \varepsilon\overline{z}$ mit $\varepsilon \coloneqq f/e = f \cdot (1/e) \in \mathbb{Z}[\mathrm{i}]^\times$ (die beiden Faktoren haben beide Norm 1), dann $z^2 = \varepsilon^2\overline{z}^2$ und schließlich $z^4 = z^2 \cdot \varepsilon^2\overline{z}^2 = \varepsilon^2\,\mathrm{N}(z)^2$, eine ganze Zahl. Mithilfe der Polardarstellung erkennen wir, dass das Argument von z ein ganzzahliges Vielfaches von $45°$ sein muss, was entweder $|a| = |b|$ oder $a = 0$ oder $b = 0$ nach sich zieht. Keiner dieser drei Fälle kann eintreten und L enthält genau $4 + 4 = 8$ Elemente.

Proposition 3.9. *Für Primzahlen $p \in \mathbb{Z}^+$ mit $p \equiv 1 \pmod 4$ hat die Gleichung $(*)$ genau 8 ganzzahlige Lösungen.*

Beweis. Nach der Vorarbeit bleibt nur noch zu zeigen, dass es außer den Lösungen, die den Elementen von L zugeordnet sind, keine weiteren mehr geben kann. Sei $w \in \mathbb{Z}[\mathrm{i}]$ eine beliebige Lösung von $\mathrm{N}(w) = p$ und z wie oben. Wir bemerken, dass z und w laut Lemma 3.6 Primelemente sind. Jetzt ergibt sich mit $z\overline{z} = \mathrm{N}(z) = p = w\overline{w}$ aber $z \mid w\overline{w}$ und folglich $z \mid w$ oder $z \mid \overline{w}$. In der Primfaktorzerlegung von w bzw. $\overline{w}$ in $\mathbb{Z}[\mathrm{i}]$ gemäß Satz 2.4 kann aber nur ein Faktor vorkommen, weil w bzw. $\overline{w}$ selbst Primelemente sind. Also gilt $w = ez$ oder $\overline{w} = ez \iff w = \overline{ez} = (1/e)\overline{z}$ für ein $e \in \mathbb{Z}[\mathrm{i}]^\times$ und folglich bereits $w \in L$. □

Literatur

[1] A. Bartholomé, J. Rung, and H. Kern. *Zahlentheorie für Einsteiger.* Vieweg+Teubner, 7th edition, 2010.