4. Norm-euklidische quadratische Zahlkörper

4.1. Ein *euklidischer Ring* ist bekanntlich ein Integritätsbereich R zusammen mit einer Funktion $\phi : R \setminus \{0\} \to \mathbb{N}$, so dass folgendes gilt:

Zu je zwei Elementen $x, y \in R$, $y \neq 0$, existieren $q, r \in R$ mit

$$x = qy + r, \qquad \text{so dass} \quad \phi(r) < \phi(y) \quad \text{oder} \quad r = 0.$$

Jeder euklidische Ring R ist ein Hauptidealring: Sei $\mathfrak{a} \subset R$ ein Ideal $\neq (0)$. Dann gibt es ein Element $0 \neq a_0 \in \mathfrak{a}$ mit

$$\phi(a_0) = \min\{\phi(a) : a \in \mathfrak{a} \setminus \{0\}\}.$$

Es folgt, dass a_0 das Ideal $\mathfrak{a}$ erzeugt, denn für jedes $a \in \mathfrak{a}$ bleibt bei der Division

$$a = qa_0 + r$$

wegen der Minimaleigenschaft von $\phi(a_0)$ der Rest $r = 0$. Daraus folgt $\mathfrak{a} = Ra_0$.
Da jeder Hauptidealring faktoriell ist, ist insbesondere jeder euklidische Ring faktoriell.

Die bekanntesten Beispiele euklidischer Ringe sind
(i) der Ring $\mathbb{Z}$ der ganzen Zahlen mit $\phi(z) = |z|$ (in diesem Fall ist $\phi(z)$ auch für $z = 0$ definiert) und
(ii) der Polynomring $k[X]$ über einem Körper k mit der Funktion $\phi(f) := \deg f$ (der Grad des Null-Polynoms ist nicht definiert).

Definition. Ein quadratischer Zahlkörper K heißt *norm-euklidisch*, wenn sein Ganzheitsring $\mathfrak{O}_K$ euklidisch ist bzgl. der Funktion

$$\mathfrak{O}_K \to \mathbb{N}, \qquad \xi \mapsto |\mathrm{N}(\xi)|.$$

4.2. Satz. *Ein quadratischer Zahlkörper K mit Ganzheitsring $\mathfrak{O}_K$ ist genau dann norm-euklidisch, wenn zu jedem $\xi \in K$ ein $z \in \mathfrak{O}_K$ existiert, so dass*

$$|\mathrm{N}(\xi - z)| < 1.$$

Beweis. a) Wir zeigen zunächst, dass die Bedingung hinreichend ist. Seien $x, y \in \mathfrak{O}_K$, $y \neq 0$, vorgegeben. Dann ist $x/y \in K$, also existiert ein $q \in \mathfrak{O}_K$ mit $|\mathrm{N}(x/y - q)| < 1$. Wir setzen $r := y \cdot (x/y - q)$. Aus der Multiplikativität der Norm folgt $|\mathrm{N}(r)| < |\mathrm{N}(y)|$ und es gilt die Gleichung $x = qy + r$.

b) Sei jetzt vorausgesetzt, dass $\mathfrak{O}_K$ norm-euklidisch ist und sei $\xi \in K$ vorgegeben. Das Element ξ lässt sich schreiben als $\xi = x/y$ mit $x, y \in \mathfrak{O}_K$, $y \neq 0$. Euklidische Division $x = qy + r$ liefert Elemente $q, r \in \mathfrak{O}_K$ mit $|\mathrm{N}(r)| < |\mathrm{N}(y)|$. Es folgt

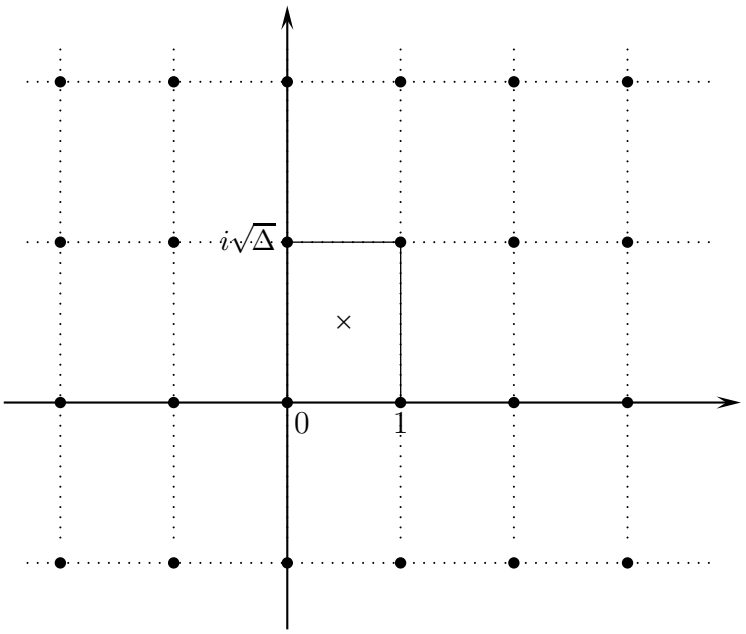
$$\xi - q = r/y \qquad \text{und} \quad |\mathrm{N}(r/y)| < 1.$$

4.3. Satz. *Sei $K := \mathbb{Q}(\sqrt{d})$, ($d < 0$ quadratfrei), ein imaginär-quadratischer Zahlkörper. Sein Ganzheitsring $\mathfrak{O}_K$ ist norm-euklidisch für $d = -1, -2, -3, -7, -11$, aber für kein anderes $d < 0$.*

Bemerkung. Es gibt noch weitere imaginär-quadratische Zahlkörper $\mathbb{Q}(\sqrt{d})$, für die der Ganzheitsring $\mathfrak{O}_K$ zwar nicht norm-euklidisch, aber trotzdem faktoriell ist, nämlich in den Fällen $d = -19, -43, -67, -163$. Wir werden darauf später noch zurückkommen.

Beweis. Wir denken uns $K = \mathbb{Q}(\sqrt{d})$ als Teilmenge komplexen Ebene $\mathbb{C}$. Der Ganzheitsring ist dann ein Gitter $\Lambda := \mathfrak{O}_K \subset \mathbb{C}$. Da die Norm in diesem Fall das Quadrat des gewöhnlichen euklidischen Betrages ist, ist K genau dann norm-euklisch, wenn jeder Punkt $z \in K \subset \mathbb{C}$ vom nächsten Gitterpunkt $\gamma \in \Lambda$ einen Abstand < 1 hat.

1. Fall: $d \equiv 2, 3 \bmod 4$. Dann ist $\Lambda = \mathbb{Z} + \mathbb{Z}\omega$ mit $\omega := i\sqrt{\Delta}$, $\Delta := |d|$, siehe Figur 4.1.



Figur 4.1

Es genügt offenbar, Punkte z im Fundamental-Rechteck

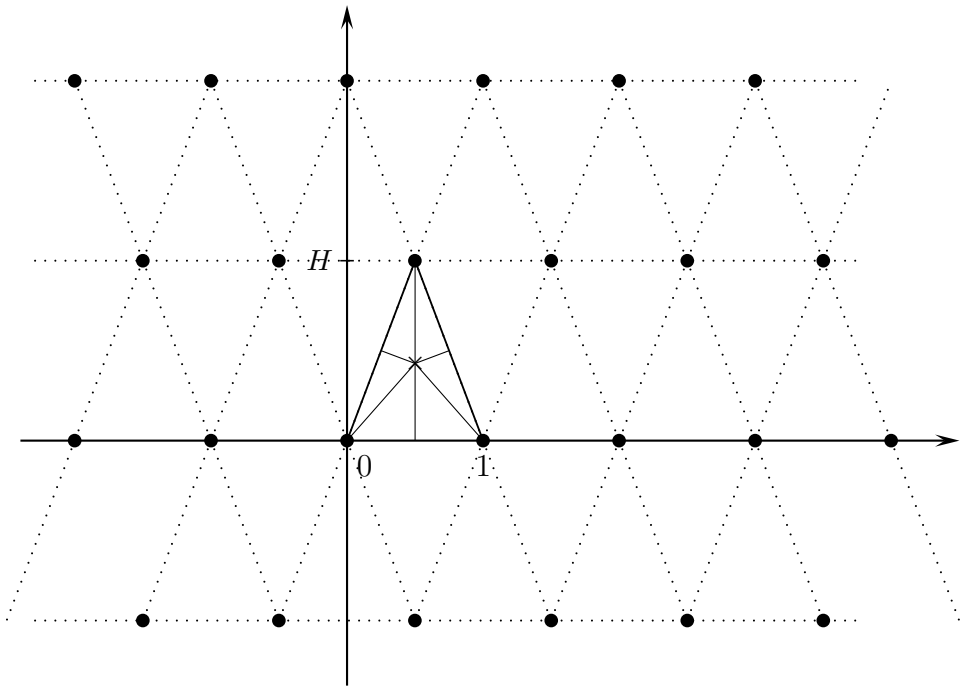
$$\{x + iy\sqrt{\Delta} : 0 \leqslant x \leqslant 1,\ 0 \leqslant y \leqslant 1\}$$

zu untersuchen. Der Punkt, der den größten Abstand von den Gitterpunkten hat, ist der Mittelpunkt des Rechtecks. Der Abstand beträgt in diesem Fall

$$\delta = \tfrac{1}{2}\sqrt{1 + \Delta^2} = \tfrac{1}{2}\sqrt{1 + d^2}.$$

Es gilt $\delta < 1$ für $d = -1, -2$, aber $\delta > 1$ für $d = -5$ und alle weiteren quadratfreien negativen ganzen Zahlen mit $d \equiv 2, 3 \bmod 4$. Daraus folgt die Behauptung des Satzes im Fall $d \equiv 2, 3 \bmod 4$.

2. Fall: $d \equiv 1 \bmod 4$. Dann ist $\Lambda = \mathbb{Z} + \mathbb{Z}\omega$ mit $\omega := \frac{1}{2}(1 + i\sqrt{|d|})$, siehe Figur 4.2. In diesem Fall wird die Ebene überdeckt von kongruenten Dreiecken, deren Ecken Gitterpunkte sind. Die Dreiecke sind gleichschenklig mit Grundlinie der Länge 1 und Höhe $H := \frac{1}{2}\sqrt{|d|}$.



Figur 4.2

Der Punkt des Dreiecks, der von den Eckpunkten den größten Abstand hat, ist der Umkreis-Mittelpunkt. Mit einer elementar-geometrischen Überlegung berechnet man diesen Abstand zu

$$\delta = \frac{H}{2} + \frac{1}{8H} = \frac{\sqrt{|d|}}{4} + \frac{1}{4\sqrt{|d|}}.$$

Für $d = -3, -7, -11$ ist $\delta < 1$, z.B. für $d = -11$

$$\delta = \tfrac{1}{4}(\sqrt{11} + 1/\sqrt{11}) = 0.904\ldots,$$

während für das nächste $d \equiv 1 \bmod 4$, nämlich $d = -15$, sich $\delta = 1.032\ldots$ ergibt. Also sind die Ganzheitsringe von $\mathbb{Q}(\sqrt{-3})$, $\mathbb{Q}(\sqrt{-7})$ und $\mathbb{Q}(\sqrt{-11})$ norm-euklidisch, aber keine weiteren mit $d \equiv 1 \bmod 4$ und $d < -11$.

4.4. Satz. *Sei $K := \mathbb{Q}(\sqrt{d})$, ($d > 1$ quadratfrei), ein reell-quadratischer Zahlkörper. Sein Ganzheitsring $\mathfrak{O}_K$ ist für $d = 2, 3, 5, 6, 7, 13, 17, 21, 29$ norm-euklidisch.*

Bemerkung. $\mathfrak{O}_K$ ist noch für weitere Werte von d norm-euklidisch, nämlich für $d = 11, 19, 33, 37, 41, 55, 73$. Dies ist aber viel schwieriger zu beweisen. Es gibt auch reell-quadratische Zahlkörper, deren Ganzheitsring faktoriell ist, ohne norm-euklidisch zu sein (z.B. $d = 14, 22, 28, \ldots, 93, 94, 97, 101, \ldots$) Einer unbewiesenen Vermutung zufolge könnte es davon sogar unendlich viele geben.

Beweis. Es ist zweckmäßig, den Zahlkörper $K := \mathbb{Q}(\sqrt{d})$ durch Trennung in Rational- und Irrational-Teil in den $\mathbb{R}^2$ einzubetten.

$$j : \mathbb{Q}(\sqrt{d}) \to \mathbb{R}^2, \qquad \xi = \xi_1 + \xi_2\sqrt{d} \;\mapsto\; j(\xi) = (\mathsf{rat}(\xi), \mathsf{irr}(\xi)) := (\xi_1, \xi_2\sqrt{d}).$$

Dabei wird der Ganzheitsring $\mathfrak{O}_K$ auf ein Gitter $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2 \subset \mathbb{R}^2$ abgebildet, wobei

$$\omega_1 := (1, 0), \qquad \omega_2 := \begin{cases} (0, \sqrt{d}), & \text{falls } d \equiv 2, 3 \bmod 4, \\ (\frac{1}{2}, \frac{1}{2}\sqrt{d}), & \text{falls } d \equiv 1 \bmod 4. \end{cases}$$

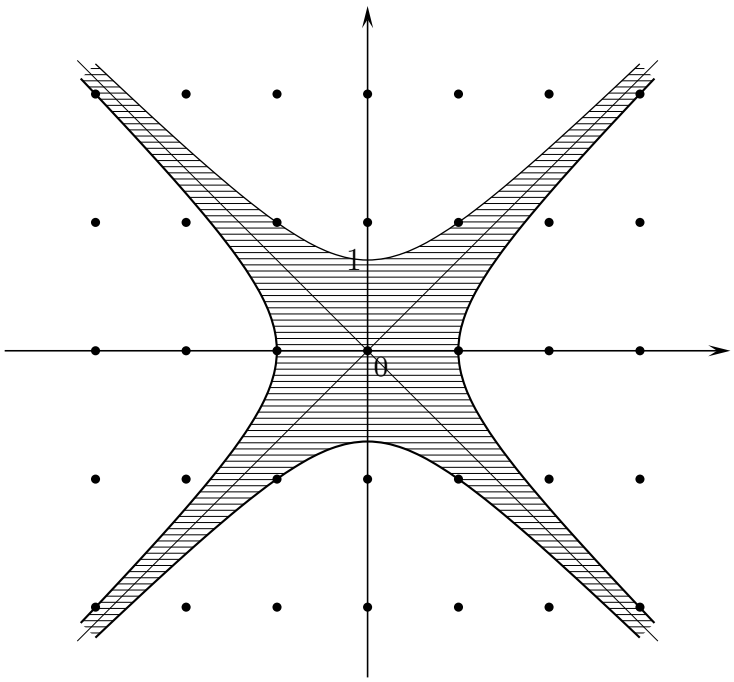
Die Normfunktion $\mathrm{N} : K \to \mathbb{Q}$ überträgt sich zu einer Funktion auf dem $\mathbb{R}^2$, die wir mit demselben Buchstaben bezeichnen.

$$\mathrm{N} : \mathbb{R}^2 \to \mathbb{R}, \qquad \mathrm{N}((x, y)) := x^2 - y^2.$$

Für alle $\xi \in K$ gilt $\mathrm{N}(\xi) = \mathrm{N}(j(\xi))$. Die Menge

$$B := \{z \in \mathbb{R}^2 : |\mathrm{N}(z)| \leqslant 1\}$$

ist eine von vier Hyperbelästen $\{x^2 - y^2 = \pm 1\}$ begrenzte Menge, die sich längs der Winkelhalbierenden $\{x = \pm y\}$ ins Unendliche erstreckt, siehe Figur 4.3.



Figur 4.3

Da B nicht konvex ist, kann man B nicht als Einheits-Ball einer Metrik auffassen. Um eine suggestive Sprechweise zu haben führen wir aber trotzdem eine N-Distanz δ_N zwischen Punkten $z, c \in \mathbb{R}^2$ ein:

$$\delta_N(z,c) := |\mathrm{N}(z-c)|^{1/2}.$$

δ_N genügt aber nicht der Dreiecks-Ungleichung. Mit der N-Distanz können wir nun formulieren: Genau dann ist K norm-euklidisch, wenn jeder Punkt $z \in j(K) \subset \mathbb{R}^2$ von wenigstens einem Gitterpunkt $c \in \Lambda$ eine N-Distanz < 1 hat. Geometrisch bedeutet das

$$\bigcup_{c\in\Lambda}(c + B^\circ) \supset j(K), \qquad\qquad (B^\circ \text{ Inneres von } B).$$

Da jeder Punkt $z \in \mathbb{R}^2$ modulo Λ zu einem Punkt des Rechtecks

$$Q_H := \{(x,y) \in \mathbb{R}^2 : |x| \leqslant \tfrac{1}{2},\ |y| \leqslant \tfrac{H}{2}\}, \qquad H := \begin{cases} \sqrt{d} & \text{für } d \equiv 2,3 \bmod 4, \\ \frac{1}{2}\sqrt{d} & \text{für } d \equiv 1 \bmod 4, \end{cases}$$

äquivalent ist, genügt es, Punkte $z \in j(K) \cap Q_H$ zu betrachten. Aus Symmetriegründen kann man sich sogar auf

$$Q_H^+ := \{(x,y) \in \mathbb{R}^2 : 0 \leqslant x \leqslant \tfrac{1}{2},\ 0 \leqslant y \leqslant \tfrac{H}{2}\}$$

beschränken.

Fall a) Wir betrachten zunächst die Werte $d = 2, 3, 5, 13$.

Die zugehörigen Werte von H sind $\sqrt{2}, \sqrt{3}, \frac{1}{2}\sqrt{5}, \frac{1}{2}\sqrt{13}$, die alle der Ungleichung $H < 2$ genügen. Für $H < 2$ gilt aber

$$Q_H \subset \{(x,y) \in \mathbb{R}^2 : |x| < 1,\ |y| < 1\},$$

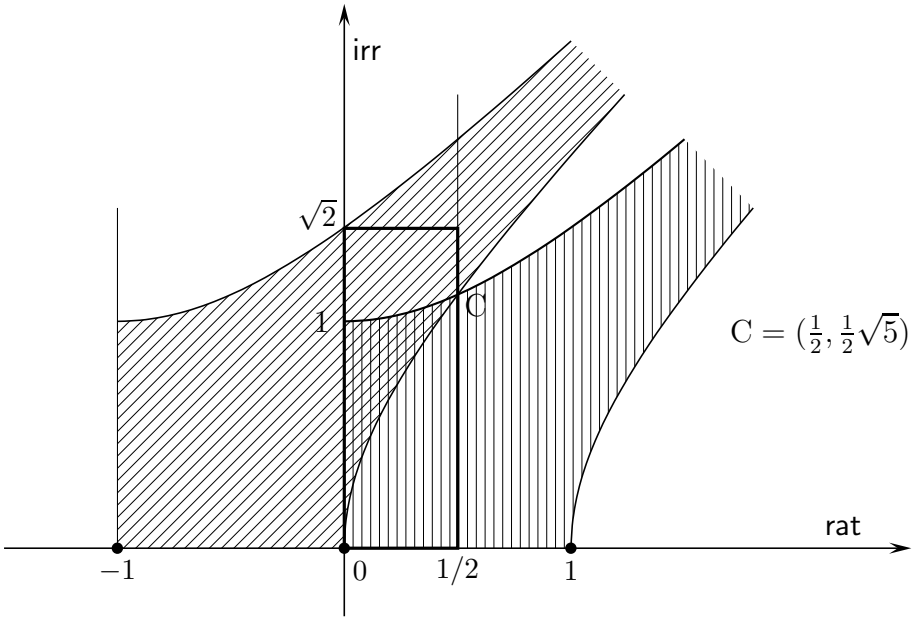
also haben alle Punkte $z \in Q_H$ vom Nullpunkt eine N-Distanz < 1. Damit ist die Norm-Euklidizität in diesen Fällen bewiesen.

Fall b) Wir betrachten jetzt die Werte $d = 6, 7, 17, 21, 29$.

Da $\sqrt{7} < \sqrt{8} = 2\sqrt{2}$ und $\frac{1}{2}\sqrt{29} < \frac{1}{2}\sqrt{32} = 2\sqrt{2}$, gilt für die zugehörigen H-Werte die Ungleichung $H < 2\sqrt{2}$, also

$$\mathbb{Q}_H^+ \subset Q_{2\sqrt{2}}^+ := Q := \{(x,y) \in \mathbb{R}^2 : 0 \leqslant x \leqslant \tfrac{1}{2},\ 0 \leqslant y \leqslant \sqrt{2}\}.$$

Dieses Rechteck ist in Figur 4.4 eingezeichnet. Alle Punkte von Q haben entweder vom Gitterpunkt $(0,0)$ oder vom Gitterpunkt $(-1,0)$ eine N-Distanz < 1, mit Ausnahme der Punkte $C = (\frac{1}{2}, \frac{1}{2}\sqrt{5})$ und $(0, \sqrt{2})$, welche die N-Distanz $= 1$ haben. Diese Punkte liegen aber nicht in $j(K)$, da $\sqrt{5}$ bzw. $\sqrt{2}$ keine rationalen Vielfachen von $\sqrt{d}$ für die betrachteten Werte von d sind.



Figur 4.4

Die Punkte von Q, die vom Nullpunkt eine N-Distanz < 1 haben, sind senkrecht schraffiert, es sind die Punkte

$$\{(x,y) \in \mathbb{R}^2 : 0 \leqslant x \leqslant \tfrac{1}{2},\ 0 \leqslant y < \sqrt{1+x^2}\}.$$

Die Punkte, die von $(-1,0)$ eine N-Distanz < 1 haben, sind schräg schraffiert. Sie werden gegeben durch die Ungleichungen

$$\{(x,y) \in \mathbb{R}^2 : 0 \leqslant x \leqslant \tfrac{1}{2},\ \sqrt{(1+x)^2-1} < y < \sqrt{(1+x)^2+1}\}$$

Da $\sqrt{(1+x)^2-1} < \sqrt{1+x^2}$ für $0 \leqslant x < \frac{1}{2}$, überdecken die beiden Bereiche tatsächlich das Rechteck Q mit Ausnahme der beiden erwähnten Punkte. Damit ist Satz 4.4 auch im Fall b) bewiesen.

Summen von zwei Quadraten

Aus der Faktorialität des Ringes $\mathbb{Z}[i]$ der ganzen Gaußschen Zahlen leiten wir nun Aussagen über die Darstellung einer natürlichen Zahl als Summe von zwei Quadratzahlen her.

4.5. Satz. *Eine Primzahl p lässt sich genau dann als Summe*

$$p = x^2 + y^2, \qquad x, y \in \mathbb{Z},$$

von zwei Quadratzahlen darstellen, wenn $p = 2$ oder $p \equiv 1 \bmod 4$.

Beweis. Der Fall $p = 2 = 1^2 + 1^2$ ist klar. Sei also jetzt p eine ungerade Primzahl.

a) Die Bedingung ist notwendig. Denn aus $p = x^2 + y^2$ folgt $x^2 \equiv -y^2 \bmod p$. Da offensichtlich $y \not\equiv 0 \bmod p$, folgt daraus, dass -1 ein Quadrat modulo p ist. Wegen $(\frac{-1}{p}) = (-1)^{(p-1)/2}$ bedeutet dies $p \equiv 1 \bmod 4$.

b) Die Bedingung ist hinreichend. Sei vorausgesetzt, dass $p \equiv 1 \bmod 4$. Der Ring $\mathbb{Z}[i]$ der ganzen Gaußschen Zahlen hat die Diskriminante $D = -4$. Wegen $(\frac{-4}{p}) = (\frac{-1}{p}) = 1$ spaltet die Primzahl p im Ring $\mathbb{Z}[i]$ nach Satz 3.10. Da $\mathbb{Z}[i]$ faktoriell ist, gibt es ein Primelement $\pi = x + iy \in \mathbb{Z}[i]$, das ein echter Teiler von p ist. Da $\mathrm{N}(p) = p^2$, folgt $\mathrm{N}(\pi) = p$, also $p = \pi \cdot \overline{\pi} = (x + iy)(x - iy) = x^2 + y^2$, q.e.d.

Bemerkung. Wegen der Eindeutigkeit der Primfaktor-Zerlegung in $\mathbb{Z}[i]$ sind in der Darstellung $p = x^2 + y^2 = (x + iy)(x - iy)$ die ganzen Zahlen x, y bis auf Reihenfolge und Vorzeichen eindeutig bestimmt.

4.6. Satz. *Eine natürliche Zahl $n > 1$ ist genau dann Summe von zwei Quadratzahlen, wenn in der Primfaktor-Zerlegung $n = p_1^{k_1} \cdot \ldots \cdot p_r^{k_r}$ alle Primfaktoren mit $p_j \equiv 3 \bmod 4$ einen geraden Exponenten k_j haben.*

Beweis. a) Sei $n = a^2 + b^2$. Die Zahl $\xi = a + ib$ kann man im Ring $\mathbb{Z}[i]$ in Primfaktoren zerlegen: $\xi = \pi_1 \cdot \ldots \cdot \pi_m$. Dann ist $n = \mathrm{N}(a + ib) = \mathrm{N}(\pi_1) \cdot \ldots \cdot \mathrm{N}(\pi_m)$. Jeder Faktor hat die Gestalt $\mathrm{N}(\pi_\mu) = p$, wobei $p = 2$ oder p eine Primzahl mit $p \equiv 1 \bmod 4$ ist, oder die Gestalt $\mathrm{N}(\pi) = p^2$, wobei p eine Primzahl mit $p \equiv 3 \bmod 4$ ist. Daraus ergibt sich die eine Implikationsrichtung des Satzes.

b) Zur Umkehrung. Wir stellen n dar als $n = c^2 n_1$, wobei n_1 nur Primfaktoren $p = 2$ oder $p \equiv 1 \bmod 4$ enthält. Jeder dieser Primfaktoren lässt sich als $\mathrm{N}(\pi_\mu)$ mit einem Primelement $\pi_\mu \in \mathbb{Z}[i]$ schreiben. Dann ist $n_1 = \mathrm{N}(\prod_\mu \pi_\mu)$, also $n_1 = a^2 + b^2$ mit natürlichen Zahlen a, b. Daraus folgt $n = (ca)^2 + (cb)^2$, q.e.d.

Bemerkung. Für zusammengesetzte Zahlen ist die Zerlegung in eine Summe von zwei Quadratzahlen, falls sie überhaupt existiert, nicht mehr eindeutig. Sei z.B. $n = p_1 p_2$ mit zwei Primzahlen $p_\nu \equiv 1 \bmod 4$, also $p_1 = \mathrm{N}(\xi)$, $p_2 = \mathrm{N}(\eta)$ mit Primelementen $\xi, \eta \in \mathbb{Z}[i]$. Dann liefern $n = \mathrm{N}(\xi\eta)$ und $n = \mathrm{N}(\xi\overline{\eta})$ zwei verschiedene Zerlegungen, denn $\xi\eta$ und $\xi\overline{\eta}$ sind nicht assoziiert.

Beispiel. Sei $n = 65 = 5 \cdot 13$. Mit $\xi = 2 + i$ und $\eta = 3 + 2i$ ist $5 = \mathrm{N}(\xi)$ und $13 = \mathrm{N}(\eta)$. Man berechnet

$$\begin{aligned} \xi\eta &= (2 + i)(3 + 2i) = 4 + 7i, \\ \xi\overline{\eta} &= (2 + i)(3 - 2i) = 8 + i. \end{aligned}$$

Dies ergibt die beiden Zerlegungen $65 = 4^2 + 7^2 = 8^2 + 1^2$.

4.7. Satz. *Sei p eine ungerade Primzahl.*

a) *Genau dann lässt sich p darstellen als*

$$p = x^2 + 2y^2 \qquad \textit{mit} \quad x, y \in \mathbb{Z},$$

wenn $p \equiv 1 \bmod 8$ oder $p \equiv 3 \bmod 8$.

b) *Genau dann lässt sich p darstellen als*

$$p = x^2 + 3y^2 \qquad \textit{mit} \quad x, y \in \mathbb{Z},$$

wenn $p = 3$ oder $p \equiv 1 \bmod 3$.

Beweis. Die Notwendigkeit der Bedingungen ist leicht direkt nachzuprüfen. Wir beweisen jetzt, dass die Bedingungen hinreichend sind.

a) Falls $p \equiv 1, 3 \bmod 8$ ist nach Satz 3.10 das Hauptideal $(p) \subset \mathbb{Z}[\sqrt{-2}]$ das Produkt zweier konjugierter Primideale. Da aber $\mathbb{Z}[\sqrt{-2}]$ ein Hauptidealring ist, existiert ein Element $\pi = x + y\sqrt{-2} \in \mathbb{Z}[\sqrt{-2}]$ mit $p = \pi\overline{\pi}$, d.h. $p = x^2 + 2y^2$.

b) Wir verwenden hier den Zahlkörper $\mathbb{Q}(\sqrt{-3})$ und seinen Ganzheitsring $\mathbb{Z}[\rho]$ mit $\rho = \frac{-1+\sqrt{-3}}{2}$, der nach Satz 4.4 ein Hauptidealring ist. Der Fall $p = 3$ ist trivial; falls $p \equiv 1 \bmod 3$ spaltet p. Wie in Teil a) erhält man ein Element $\pi \in \mathbb{Z}[\rho]$ mit $p = \pi\overline{\pi}$. Damit sind wir aber noch nicht am Ziel, denn die Elemente des Ganzheitsrings $\mathbb{Z}[\rho]$ haben möglicherweise eine 2 im Nenner. Nach dem folgenden Hilfssatz kann man aber π durch ein dazu assoziiertes $\pi_1 = x + y\sqrt{-3} \in \mathbb{Z}[\sqrt{-3}]$ ersetzen. Aus $p = \pi_1\overline{\pi}_1$ folgt die Behauptung.

4.8. Hilfssatz. *Jedes Element $\xi \in \mathbb{Z}[\frac{-1+\sqrt{-3}}{2}]$ ist assoziiert zu einem Element $\xi_1 \in \mathbb{Z}[\sqrt{-3}]$.*

Beweis. Wenn ξ nicht schon selbst in $\mathbb{Z}[\sqrt{-3}]$ liegt, hat es die Gestalt

$$\xi = \tfrac{1}{2}(x + y\sqrt{-3})$$

mit ungeraden Zahlen $x, y \in \mathbb{Z}$. Es gibt zwei Möglichkeiten:

(i) $x \equiv y \bmod 4$ oder (ii) $x \equiv -y \bmod 4$.

Im ersten Fall multiplizieren wir ξ mit der Einheit $\rho = \frac{1}{2}(-1 + \sqrt{-3})$:

$$\xi_1 := \xi\rho = \tfrac{1}{4}(x + y\sqrt{-3})(-1 + \sqrt{-3}) = \tfrac{1}{4}\left(-(x + 3y) + (x - y)\sqrt{-3}\right).$$

Aus der Voraussetzung (i) folgt $x + 3y \equiv 0 \bmod 4$ und $x - y \equiv 0 \bmod 4$, also $\xi_1 \in \mathbb{Z}[\sqrt{-3}]$. Im Fall (ii) zeigt man analog $\xi\overline{\rho} \in \mathbb{Z}[\sqrt{-3}]$.

* Fermat-Gleichung zum Exponenten 3

In diesem Abschnitt beschäftigen wir uns mit der Fermat-Gleichung

$$x^3 + y^3 = z^3, \tag{1}$$

die ja bekanntlich keine ganzzahlige Lösung $x, y, z \in \mathbb{Z} \setminus \{0\}$ besitzt. Um dies zu beweisen, verwenden wir den Zahlkörper $\mathbb{Q}(\sqrt{-3})$ und den Ring seiner ganzen Zahlen

$$R := \mathbb{Z}[\rho], \qquad \rho := \tfrac{1}{2}(-1 + i\sqrt{3}) = e^{2\pi i/3}.$$

Die Zahl ρ ist eine primitive 3-te Einheitswurzel. Die Einheiten von $\mathbb{Z}[\rho]$ sind alle 6-ten Einheitswurzeln, also außer den dritten Einheitswurzeln $1, \rho, \rho^2$ noch ihre Negativen $-1, -\rho, -\rho^2$. Es gilt die Relation $1 + \rho + \rho^2 = 0$.

Wie wir gesehen haben, ist $R = \mathbb{Z}[\rho]$ ein faktorieller Ring. Die Primzahl $3 \in \mathbb{Z}$ ist in R verzweigt, es gilt für das Hauptideal $3R = (3)$ die Gleichung

$$(3) = (\theta)^2, \quad \text{wobei } \theta := \sqrt{-3} := i\sqrt{3}.$$

Das Element $\theta \in R$ ist prim mit

$$R/(\theta) \cong \mathbb{F}_3 = \{\overline{0}, \overline{1}, -\overline{1}\}.$$

Es gilt $\theta = 1 + 2\rho = \rho - \rho^2$. Die Assoziierten von θ sind

$$\rho\theta = -1 + \rho^2, \quad \rho^2\theta = 1 - \rho, \quad \text{sowie } -\theta, \quad -\rho\theta, \quad -\rho^2\theta.$$

Der Restklassenring $R/(3)$ besteht aus 9 Elementen, ein vollständiges Repräsentantensystem wird gegeben durch die Elemente

$$\alpha + \beta\theta, \qquad \alpha, \beta \in \{0, 1, -1\}$$

4.9. Hilfssatz. *Sei $x \in \mathbb{Z}[\rho]$ mit $x \equiv \pm 1 \bmod (\theta)$. Dann gibt es eine dritte Einheitswurzel $\epsilon \in \{1, \rho, \rho^2\}$, so dass*

$$\epsilon x \equiv \pm 1 \bmod (3).$$

Beweis. a) Sei zunächst $x \equiv 1 \bmod (\theta)$. Dann gilt

$$x \equiv 1 + c\theta \bmod (3) \quad \text{mit } c \in \{0, 1, -1\}.$$

Der Fall $c = 0$ ist trivial (man wähle $\epsilon = 1$).

*Dieser Abschnitt wurde in der Vorlesung weggelassen

Falls $c = 1$, sei $\epsilon := \rho$. Da $\rho \equiv \rho^2 \equiv 1 \bmod (\theta)$ und $\rho = 1 - \rho^2\theta$, folgt $\rho \equiv 1 - \theta \bmod (3)$, also

$$\rho x \equiv (1-\theta)(1+\theta) \equiv 1 - \theta^2 \equiv 1 \bmod (3).$$

Falls $c = -1$, setzen wir $\epsilon := \rho^2$. Da $\rho^2 = 1 + \rho\theta \equiv 1 + \theta \bmod (3)$, folgt

$$\rho^2 x \equiv (1+\theta)(1-\theta) \equiv 1 \bmod (3).$$

b) Der Fall $x \equiv -1 \bmod (\theta)$ wird durch Übergang zu $-x$ auf Teil a) zurückgeführt.

4.10. Hilfssatz. *Sei u eine Einheit des Rings $R = \mathbb{Z}[\rho]$ mit*

$$u \equiv \pm 1 \bmod (3).$$

Dann folgt $u = \pm 1$.

Beweis. Für die Einheiten außer ± 1 gilt in $R/(3)$

$$\rho \equiv 1 - \theta, \quad \rho^2 \equiv 1 + \theta, \quad -\rho \equiv -1 + \theta, \quad -\rho^2 \equiv -1 - \theta,$$

also $u \not\equiv \pm 1 \bmod (3)$.

4.11. Hilfssatz. *Sei $x \in \mathbb{Z}[\rho]$ ein Element mit $x \equiv \pm 1 \bmod (3)$. Falls x bis auf eine Einheit ein Kubus in $\mathbb{Z}[\rho]$ ist, d.h. $x = u\xi^3$ mit $\xi \in \mathbb{Z}[\rho]$, $u \in \mathbb{Z}[\rho]^*$, ist x selbst schon ein Kubus, genauer $x = \eta^3$ mit $\eta = u\xi$.*

Beweis. Da $\theta \nmid x$, folgt $\theta \nmid \xi$, also $\xi \equiv \pm 1 \bmod (\theta)$. Daraus folgt $\xi^3 \equiv \pm 1 \bmod (3)$. Nun folgt aus $x = u\xi^3$, dass auch $u \equiv \pm 1 \bmod (3)$. Wegen Hilfssatz 4.10 gilt daher $u = \pm 1$, also $u = u^3$, d.h. $x = u\xi^3 = (u\xi)^3$, q.e.d.

Nach diesen Vorbereitungen sind wir nun in der Lage, die Unmöglichkeit einer nichttriviale Lösung der Fermat-Gleichung (1) zu beweisen, und zwar legen wir statt $\mathbb{Z}$ gleich allgemeiner den Ring $\mathbb{Z}[\rho]$ zugrunde. Da $-z^3 = (-z)^3$, kann man alle Kuben auf die linke Seite der Gleichung bringen.

4.12. Satz. *Die Gleichung*

$$x^3 + y^3 + z^3 = 0$$

besitzt keine Lösung $x, y, z \in \mathbb{Z}[\rho]$ mit $xyz \neq 0$.

Beweis. a) Wir beweisen zunächst den sog. 1. Fall der Fermatschen Vermutung:

Es gibt keine Lösung der Gleichung $x^3 + y^3 + z^3 = 0$ in $\mathbb{Z}[\rho]$ mit $\theta \nmid xyz$.

Angenommen, (x, y, z) sei doch so eine Lösung. Da $\theta \nmid x$, folgt $x \equiv \pm 1 \bmod (\theta)$. Nach Hilfssatz 4.9 kann man, indem man nötigenfalls x mit einer dritten Einheitswurzel multipliziert, annehmen, dass $x \equiv \pm 1 \bmod (3)$ (der Wert von x^3 bleibt unverändert). Deshalb gilt $x^3 \equiv \pm 1 \bmod (9)$. Analog ist $y^3 \equiv \pm 1 \bmod (9)$ und $z^3 \equiv \pm 1 \bmod (9)$. Die Gleichung $x^3 + y^3 + z^3 = 0$ würde deshalb implizieren, dass

$$\pm 1 \pm 1 \pm 1 \equiv 0 \bmod (9).$$

Dies ist aber bei jeder Vorzeichen-Kombination unmöglich. Damit ist der 1. Fall der Fermat-Vermutung für den Exponenten 3 bewiesen.

b) Nach Teil a) ist also bei jeder Lösung der Fermat-Gleichung mindestens eine der Zahlen x, y, z durch θ teilbar. Wir können annehmen, dass die Lösung primitiv ist, d.h. x, y, z keinen gemeinsamen Primfaktor besitzen, denn andernfalls kann man die ganze Gleichung durch diesen Faktor kürzen. Daraus folgt nun, dass x, y, z paarweise teilerfremd sind, denn ein gemeinsamer Primfaktor von zwei der Zahlen teilt auch die dritte. Also ist genau eine der Zahlen durch θ teilbar. Wir können annehmen, dass dies die Zahl z ist. Es sei θ^r die höchste Potenz von θ, die in z aufgeht, also $z = \theta^r z_1$, wobei $\theta \nmid z_1$. Wenn es also überhaupt eine Lösung der Fermat-Gleichung zum Exponenten 3 gibt, dann auch eine der Gestalt

$$x^3 + y^3 + (\theta^r z_1)^3 = 0, \tag{2}$$

wobei x, y, z_1 paarweise teilerfremd sind und keinen Faktor θ enthalten. Wir werden nun zeigen, dass aus der Existenz einer Gleichung der Gestalt (2) mit $r > 0$ sich eine analoge Gleichung mit einem um 1 verkleinerten Wert von r ableiten lässt (sog. *Abstieg*). Wiederholte Anwendung dieses Schlusses würde dann auf eine Lösung des 1. Falles der Fermat-Gleichung führen, die aber unmöglich ist. Der Satz 4.12 ist also bewiesen, wenn wir für die Gleichung (2) den Abstieg in r beweisen können. Dies führen wir jetzt durch.

Da $\theta \nmid x$, gilt $x \equiv \pm 1 \bmod (\theta)$, und analog $y \equiv \pm 1 \bmod (\theta)$. Da aber $x^3 + y^3 \equiv 0 \bmod (\theta)$, muss für eine der Zahlen x, y das Pluszeichen, für die andere das Minuszeichen gelten. Nach evtl. Vertauschung von x und y ist daher $x \equiv +1 \bmod (\theta)$ und $y \equiv -1 \bmod (\theta)$. Wegen Hilfssatz 4.9 können wir sogar annehmen, dass

$$x \equiv +1 \bmod (3) \quad \text{und} \quad y \equiv -1 \bmod (3).$$

Ein wesentlicher Trick ist nun die Zerlegung

$$x^3 + y^3 = (x + y)(x + \rho y)(x + \rho^2 y),$$

die aus der Polynom-Identität $X^3 + 1 = (X + 1)(X + \rho)(X + \rho^2)$ folgt. Wir untersuchen nun die drei Faktoren auf Teilbarkeit durch θ.

(i) $\quad x + y \equiv 0 \bmod (3), \quad$ also ist $x + y$ durch θ^2 teilbar.

(ii) $\qquad x + \rho y = (x + y) + (\rho - 1)y.$

Da $\rho - 1 = -\rho^2\theta$, sowie $\theta \nmid y$ und $\theta^2 \mid x + y$, folgt, dass

$$\theta \mid x + \rho y, \quad \text{aber} \quad \theta^2 \nmid x + \rho y.$$

(iii) $\qquad x + \rho^2 y = (x + y) + (\rho^2 - 1)y.$

Da $\rho^2 - 1 = \rho\theta$, folgt analog zu (ii), dass

$$\theta \mid x + \rho^2 y, \quad \text{aber} \quad \theta^2 \nmid x + \rho^2 y.$$

Wir definieren nun Elemente $a, b, c \in \mathbb{Z}[\rho]$ durch

$$\begin{aligned} a &:= \frac{x + y}{\theta}, \\ b &:= \rho \cdot \frac{x + \rho y}{\theta} = \rho\frac{x + y}{\theta} + \rho\frac{(\rho - 1)y}{\theta} = \rho a - y, \\ c &:= \rho^2 \cdot \frac{x + \rho^2 y}{\theta} = \rho^2\frac{x + y}{\theta} + \rho^2\frac{(\rho^2 - 1)y}{\theta} = \rho^2 a + y. \end{aligned}$$

Es gilt $\theta \mid a$, $\theta \nmid b$, $\theta \nmid c$ und

$$abc = \frac{x^3 + y^3}{\theta^3} = (-\theta^{r-1} z_1)^3. \tag{3}$$

Aus $1 + \rho + \rho^2 = 0$ folgt

$$a + b + c = 0. \tag{4}$$

Die Elemente a und b sind teilerfremd, denn wegen $b = \rho a - y$ wäre ein gemeinsamer Primteiler von a und b auch Teiler von y und wegen $\theta a = x + y$ auch Teiler von x im Widerspruch dazu, dass x und y teilerfremd sind. Aus (4) folgt dann, dass a, b, c paarweise teilerfremd sind. Nach (3) ist das Produkt abc ein Kubus und wegen der Teilerfremdheit sind a, b, c bis auf Einheiten selbst Kuben. Da $\theta \mid a$, folgt dann sogar $\theta^3 \mid a$, insbesondere $a \equiv 0 \bmod (3)$. Aus $b = \rho a - y$ ergibt sich daher

$$b \equiv -y \equiv -1 \bmod (3),$$

also ist b nach Hilfssatz 4.11 ein Kubus, d.h. $b = \xi^3$ mit einem $\xi \in \mathbb{Z}[\rho]$. Analog folgt aus $c = \rho^2 a + y$, dass $c \equiv 1 \bmod (3)$; also ist c ein Kubus, etwa $c = \eta^3$ mit $\eta \in \mathbb{Z}[\rho]$. Aus Gleichung (3) folgt nun, dass a ein Kubus der Gestalt $a = (\theta^{r-1}\zeta)^3$ ist, wobei $\zeta \in \mathbb{Z}[\rho]$ nicht durch θ teilbar ist. Setzt man dies in (4) ein, so erhält man

$$\xi^3 + \eta^3 + (\theta^{r-1}\zeta)^3 = 0,$$

also den gewünschten Abstieg von Gleichung (2), womit Satz 4.12 bewiesen ist.