Satz 2.19. *Sei $a \in \mathbb{Z}$ kein Quadrat. Dann existieren unendlich viele Primzahlen p mit $\left(\frac{a}{p}\right) = -1$.*

Beweis. Sei zunächst $a = -1$. Nach dem 1. Ergänzungssatz zum QRG ist $\left(\frac{-1}{p}\right) = -1$ äquivalent zu $p \equiv -1 \bmod 4$. Nach Satz 2.13 gibt es unendlich viele solche Primzahlen. Im Fall $a = 2$ müssen wir nach dem 2. Ergänzungssatz zum QRG zeigen, dass es unendlich viele Primzahlen kongruent ± 3 modulo 8 gibt. Angenommen es gäbe nur endlich viele. Seien $p_1 = 3, p_2, \ldots, p_n$ diese Primzahlen und sei

$$N = 8p_2 \cdots p_n + 3.$$

Dann ist $N > 1$ ungerade und durch keines der p_i teilbar, d.h. N hat nur Primteiler kongruent $\pm 1 \bmod 8$. Das widerspricht $N \equiv 3 \bmod 8$. Daher gibt es unendlich viele Primzahlen p mit $\left(\frac{2}{p}\right) = -1$.

Im Fall $a = -2$ schließen wir so: Seien $p_1 = 5, p_2, \ldots, p_n$ alle ungeraden Primzahlen mit $\left(\frac{-2}{p}\right) = -1$ (das sind die kongruent $-1, -3 \bmod 8$). Sei

$$N = 8p_2 \cdots p_n + 5.$$

Dann ist $N > 1$ ungerade und durch keines der p_i teilbar. Daher hat N nur Primteiler kongruent $1, 3 \bmod 8$. Das widerspricht $N \equiv -3 \bmod 8$. Daher gibt es unendlich viele Primzahlen p mit $\left(\frac{-2}{p}\right) = -1$.

Da sich das Legendre-Symbol nicht ändert, wenn wir a um ein Quadrat abändern, können wir nun annehmen, dass $a = (-1)^\epsilon 2^e q_1 \cdots q_n$ mit paarweise verschiedenen ungeraden Primzahlen q_i und $n \geq 1$, $e, \epsilon \in \{0, 1\}$ gilt. Wir nehmen nun an, dass $p_1, \ldots, p_m$ alle Primzahlen mit $\left(\frac{a}{p}\right) = -1$ sind. Dann gilt insbesondere $p_i \neq q_j$ für beliebige i, j. Sei α ein quadratischer Nichtrest modulo q_n. Mit Hilfe des Chinesischen Restklassensatzes finden wir ein $N \in \mathbb{N}$ mit

$$\begin{aligned} N &\equiv 1 && \bmod 8, \\ N &\equiv 1 && \bmod p_1, \ldots, p_m, \\ N &\equiv 1 && \bmod q_1, \ldots, q_{n-1}, \\ N &\equiv \alpha && \bmod q_n. \end{aligned}$$

Sei

$$N = \ell_1 \cdots \ell_r$$

die Primfaktorzerlegung von N. Da N weder durch 2 noch durch eines der p_i oder q_i teilbar ist, sind die ℓ_i sämtlich ungerade und von den p_i und q_i verschieden. Daher gilt

$$\prod_i \left(\frac{a}{\ell_i}\right) = \prod_i \left(\frac{-1}{\ell_i}\right)^\epsilon \cdot \prod_i \left(\frac{2}{\ell_i}\right)^e \cdot \prod_{i,j} \left(\frac{q_j}{\ell_i}\right).$$

Wegen $N \equiv 1 \bmod 4$ ist eine gerade Anzahl der ℓ_i kongruent -1 modulo 4, weshalb der erste Faktor gleich 1 ist. Wegen $N \equiv 1 \bmod 8$ ist eine gerade Anzahl

der ℓ_i kongruent ± 3 modulo 8. Also ist der zweite Faktor gleich 1. Für festes q_j gilt

$$\prod_i \left(\frac{q_j}{\ell_i}\right) = \prod_i \left(\frac{\ell_i}{q_j}\right).$$

Entsprechend unserer Wahl von N erhalten wir die Gleichung

$$\prod_i \left(\frac{a}{\ell_i}\right) = \prod_{i,j} \left(\frac{\ell_i}{q_j}\right) = \prod_j \left(\frac{N}{q_j}\right) = -1.$$

Daher muss $\left(\frac{a}{\ell_i}\right) = -1$ für mindestens ein i gelten. Widerspruch. □

2.4 Quadratsummen

Wir wollen mit Hilfe des Quadratischen Reziprozitätsgesetzes Darstellungen von Primzahlen als Quadratsummen herleiten. Der folgende Satz ist ein Klassiker.

Satz 2.20 (Lagrange)**.** *Eine ungerade Primzahl ist genau dann als Summe zweier Quadrate darstellbar, wenn sie kongruent* 1 *modulo* 4 *ist.*

Da die Summe zweier Quadrate stets $\equiv 0, 1, 2 \bmod 4$ ist, ist die gegebene Bedingung notwendig. Auch die Primzahlbedingung ist notwendig, wie das Beispiel der Zahl 21 zeigt.

Beweis von Satz 2.20. Die Bedingung ist offenbar notwendig. Es verbleibt zu zeigen, dass die Bedingung hinreichend ist, also sei $p \equiv 1 \bmod 4$ eine Primzahl.

Wir betrachten den Ring der Gaußschen Zahlen $\mathbb{Z}[i] = \{a+bi \in \mathbb{C} \mid a, b \in \mathbb{Z}\}$ und seine Normfunktion $N(a+bi) = a^2 + b^2$. Diese ist eine euklidische Normfunktion, insbesondere ist $\mathbb{Z}[i]$ ein Hauptidealring. Eine Nichteinheit $z = a + bi$ hat stets eine Norm $N(z) > 1$ (ansonsten wäre wegen $N(z) = z\bar{z}$ die komplex Konjugierte $\bar{z}$ von z ein Inverses von z).

Nun ist p kein Primelement in $\mathbb{Z}[i]$. Um dies einzusehen, wähle $x \in \mathbb{Z}$ mit $x^2 \equiv -1 \bmod p$. Dann gilt in $\mathbb{Z}[i]$, dass $p \mid (x^2+1) = (x+i)(x-i)$, aber die Faktoren sind beide nicht durch p teilbar.

Weil p kein Primelement ist, ist es auch nicht irreduzibel, man findet also $z, z' \in \mathbb{Z}[i] \setminus \mathbb{Z}[i]^\times$ mit $zz' = p$. Hieraus folgt $N(z)N(z') = N(p) = p^2$, also $N(z) = N(z') = p$. Mit $z = a + bi$ erhalten wir $p = N(z) = a^2 + b^2$. □

Wir nennen eine ganze Zahl *Quadratzahl*, wenn sie das Quadrat einer ganzen Zahl ist, d.h. wir zählen die Zahl 0 mit zu den Quadratzahlen.

Theorem 2.21 (Lagrange)**.** *Jede natürliche Zahl ist Summe von vier Quadratzahlen.*

Zentral für den Beweis ist die folgende Bemerkung, die besagt, dass das Produkt zweier Summen von vier Quadraten wieder eine Summe von vier Quadraten ist.

Lemma 2.22 (Euler-Identität)**.** *Für $x_1, x_2, x_3, x_4, y_1, y_2, y_3, y_4 \in \mathbb{Z}$ gilt die Identität*

$$\begin{aligned}(x_1^2+x_2^2+x_3^2+x_4^2)(y_1^2+y_2^2+y_3^2+y_4^2) = \\ (x_1y_1+x_2y_2+x_3y_3+x_4y_4)^2 \\ +(x_1y_2-x_2y_1+x_3y_4-x_4y_3)^2 \\ +(x_1y_3-x_2y_4-x_3y_1+x_4y_2)^2 \\ +(x_1y_4+x_2y_3-x_3y_2-x_4y_1)^2.\end{aligned}$$

Zum Beweis ist nichts zu sagen, man multipliziert einfach aus. Ihren Ursprung hat diese Gleichung in den Quaternionen. Eine **Quaternion** (oder auch **hyperkomplexe Zahl**) ist ein Ausdruck der Form $z = x_1+x_2i+x_3j+x_4k$, wobei x_1, x_2, x_3, x_4 reelle Zahlen und i, j, k Symbole sind, die den Rechenregeln $-1 = i^2 = j^2 = k^2$ und $ij = -ji = k$, $jk = -kj = i$ und $ki = -ik = j$ genügen. Die Norm einer Quaternion ist durch $N(z) = x_1^2 + x_2^2 + x_3^2 + x_4^2$ definiert und die obige Identität entspricht genau dem Multiplikationsgesetz $N(z)N(z') = N(zz')$ für die Quaternionennorm.

Beweis von Theorem 2.21. Wegen der Euler-Identität genügt es zu zeigen, dass jede Primzahl Summe von vier Quadratzahlen ist. Sei p eine Primzahl, die wir ohne Einschränkung als ungerade annehmen können. Es gibt $(p+1)/2$ Quadrate modulo p, also auch genauso viele Restklassen der Form $-1-x^2$. Da es insgesamt nur p verschiedene Restklassen gibt, muss unter diesen wenigstens ein Quadrat sein, d.h. die Gleichung $x^2 + y^2 + 1 = 0$ hat eine Lösung modulo p. Wählen wir Repräsentanten x, y mit $-p/2 < x, y < p/2$, so folgt

$$0 < x^2 + y^2 + 1 < 3\left(\frac{p}{2}\right)^2 < p^2.$$

Also gibt es ein $n \in \mathbb{N}$, $n < p$, so dass np Summe von drei, also insbesondere auch von vier Quadraten ist. Sei m die kleinste natürliche Zahl, so dass mp Summe von vier Quadraten ist. Offenbar gilt $m < p$. Wir zeigen $m = 1$. Angenommen m wäre echt größer als 1 und

$$mp = x_1^2 + x_2^2 + x_3^2 + x_4^2. \qquad (*)$$

Sei nun $x_i \equiv y_i \bmod m$ mit $-m/2 < y_i \leq m/2$ für $i = 1, 2, 3, 4$. Dann gilt $y_1^2 + y_2^2 + y_3^2 + y_4^2 \equiv 0 \bmod m$, also existiert ein $r \in \mathbb{Z}$, $r \geq 0$, mit

$$rm = y_1^2 + y_2^2 + y_3^2 + y_4^2. \qquad (**)$$

Wegen $y_1^2 + y_2^2 + y_3^2 + y_4^2 \leq m^2/4 + m^2/4 + m^2/4 + m^2/4 = m^2$, gilt $r \leq m$. Multiplizieren wir die Gleichungen $(*)$ und $(**)$, so erhalten wir eine Darstellung von rpm^2 als Summe von vier Quadraten

$$rpm^2 = A^2 + B^2 + C^2 + D^2, \qquad (***)$$

wobei A, B, C und D gerade die Terme auf der rechten Seite der Euler-Identität sind. Wegen $x_i \equiv y_i \bmod m$ sind B, C und D durch m teilbar. Außerdem gilt

$$A = x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4 \equiv x_1^2 + x_2^2 + x_3^2 + x_4^2 = mp \equiv 0 \bmod m.$$

Folglich ist auch $rp = (A/m)^2 + (B/m)^2 + (C/m)^2 + (D/m)^2$ Summe von vier Quadraten. Wir zeigen nun, dass r weder gleich 0 noch gleich m sein kann:

Aus $r = 0$ folgt $y_1 = y_2 = y_3 = y_4 = 0$. Daher sind x_1, x_2, x_3, x_4 durch m teilbar und $(*)$ impliziert $m^2 | mp$, also $m|p$.

Aus $r = m$ folgt $y_i = m/2$ für $i = 1, 2, 3, 4$, insbesondere ist m gerade. Es gilt $x_i = m/2 + c_i m$ mit $c_i \in \mathbb{Z}$, $i = 1, 2, 3, 4$. Wir erhalten $x_i^2 = m^2/4 + c_i m^2 + c_i^2 m^2 \equiv m^2/4 \bmod m^2$. Durch Aufsummieren folgt $mp = x_1^2 + x_2^2 + x_3^2 + x_4^2 \equiv m^2 \bmod m^2$, woraus wieder $m \mid p$ folgt.

In beiden Fällen haben wir $m \mid p$ erhalten, was, da p eine Primzahl ist, im Widerspruch zu $1 < m < p$ steht. Daher gilt $1 \leq r \leq m - 1$. Dies steht wiederum im Widerspruch zur Minimalität von m. Die Annahme $m > 1$ ist damit zum Widerspruch geführt. Es folgt $m = 1$, und der Beweis ist beendet. □

Bemerkung: Wir haben gezeigt, dass jede natürliche Zahl Summe von vier Quadraten ist. Der Beweis benutzte zum einen die entsprechende Aussage über Primzahlen und zum anderen die von den Quaternionen herkommende Euler-Identität. Die Normgleichung $N(z)N(z') = N(zz')$ für komplexe Zahlen $z = x_1 + ix_2$, $z' = y_1 + iy_2$ impliziert die Identität

$$(x_1^2 + x_2^2)(y_1^2 + y_2^2) = (x_1y_2 + x_2y_1)^2 + (x_1y_1 - x_2y_2)^2,$$

und zeigt uns, dass auch das Produkt von Summen zweier Quadrate wieder Summe zweier Quadrate ist. Nach Satz 2.20 ist daher jedes Produkt von Primzahlen inkongruent 3 modulo 4 Summe zweier Quadrate. Um alle natürlichen Zahlen zu bestimmen, die Summe zweier Quadrate sind, brauchen wir allerdings mehr Einsicht in den Ring $\mathbb{Z}[i]$.

Ein Element in $\mathbb{Z}[i]$ ist genau dann Einheit, wenn es Norm 1 hat - dies sind die vier Elemente $\{\pm 1, \pm i\}$. Ein Element mit Primzahlnorm ist automatisch prim (wegen der Multiplikativität der Norm). Allerdings haben nicht alle Primelemente in $\mathbb{Z}[i]$ eine Primzahl als Norm. Zum Beispiel ist $3 \in \mathbb{Z}[i]$ irreduzibel, also ein Primelement, und es gilt $N(3) = 9$.

Satz 2.23. *Sei $\pi \in \mathbb{Z}[i]$ ein Primelement. Dann tritt genau einer der beiden folgenden Fälle auf:*

(a) $N(\pi) = p^2$ für eine Primzahl p und $\pi \mathrel{\hat{=}} p$.

(b) $N(\pi) = \pi\bar{\pi} = p$ ist eine Primzahl.

Umgekehrt ist jede Primzahl p entweder Primelement in $\mathbb{Z}[\,i\,]$ oder von der Form $p = \pi\bar{\pi}$ mit einem Primelement π der Norm p.

Beweis. Sei $p = \pi_1 \cdots \pi_n$ eine Primelementzerlegung der Primzahl p in $\mathbb{Z}[i]$. Dann gilt

$$p^2 = N(p) = N(\pi_1) \cdots N(\pi_n).$$

Es gilt $N(\pi_j) > 1$ für $j = 1, \ldots, n$; folglich ist $n \leq 2$. Im Fall $n = 1$ ist p Primelement. Im Fall $n = 2$ gilt $p = N(\pi_1) = \pi_1\bar{\pi}_1$. Sei nun $\pi \in \mathbb{Z}[i]$ ein Primelement. Dann teilt π die natürliche Zahl $N(\pi) > 1$ und deshalb auch eine Primzahl p. Ist p Primelement in $\mathbb{Z}[i]$, so folgt $\pi \mathrel{\hat{=}} p$ und $N(\pi) = N(p) = p^2$. Gilt $p = \pi_1\bar{\pi}_1$ mit einem Primelement π_1 der Norm p, so ist, wegen der Eindeutigkeit der Primzerlegung, π assoziiert zu π_1 oder zu $\bar{\pi}_1$. In jedem Fall gilt $\pi\bar{\pi} = N(\pi) = N(\pi_1) = p$. □ □

Es verbleibt zu klären, wann welcher Fall eintritt.

Satz 2.24. *Eine Primzahl p ist genau dann ein Primelement in $\mathbb{Z}[i]$, wenn p kongruent 3 modulo 4 ist.*

Beweis. Zunächst ist $2 = (1+i)(1-i)$ kein Primelement in $\mathbb{Z}[i]$. Sei $p \neq 2$ und kein Primelement. Nach Satz 2.23 gilt $p = \pi\bar{\pi}$ für ein Primelement π. Setzt man $\pi = a + bi$, $a, b \in \mathbb{Z}$, so folgt $p = a^2 + b^2$, also $p \equiv 1 \bmod 4$. Dies zeigt eine Richtung. Dass Primzahlen $p \equiv 1 \bmod 4$ keine Primelemente in $\mathbb{Z}[i]$ sind, haben wir bereits im Beweis von 2.20 eingesehen. □

Ist p von der Form $\pi\bar{\pi}$ und gilt $\pi \mathrel{\hat{=}} \bar{\pi}$, so erhalten wir mit $\pi = a + bi$

$$a + bi = u(a - bi), \quad u \in \{\pm 1, \pm i\}.$$

Aus $u = \pm 1$ würde folgen, dass p ein Quadrat ist, also scheidet diese Möglichkeit aus. Für $u = \pm i$ erhalten wir $a = \pm b$. Aus $p = N(\pi) = 2a^2$ folgt dann $p = 2$. In der Tat gilt $2 = (1+i)(1-i)$ und $(1-i) = (-i)(1+i)$.

Zusammenfassend erhalten wir das

Satz 2.25 (Zerlegungsgesetz in $\mathbb{Z}[i]$)**.** *Eine Primzahl p ist in $\mathbb{Z}[i]$*

Produkt zweier assoziierter Primelemente	$\iff$	$p = 2$,
Produkt zweier nicht assoziierter Primelemente	$\iff$	$p \equiv 1 \bmod 4$,
Primelement	$\iff$	$p \equiv 3 \bmod 4$.

Satz 2.26. *Eine natürliche Zahl ist genau dann Summe zweier Quadratzahlen, wenn in ihrer Primfaktorzerlegung jede Primzahl kongruent* 3 *modulo* 4 *in gerader Vielfachheit vorkommt.*

Beweis. Eine natürliche Zahl ist genau dann Summe zweier Quadrate, wenn sie als Norm einer Gaußschen Zahl $\alpha \in \mathbb{Z}[i]$ vorkommt. Sei nun $n = N(\alpha)$ und

$$\alpha = \pi_1 \cdots \pi_r$$

eine Primzerlegung von α in $\mathbb{Z}[i]$. Dann gilt

$$n = N(\alpha) = N(\pi_1) \cdots N(\pi_r).$$

Nach Satz 2.23 und dem Zerlegungsgesetz ist für ein Primelement $\pi \in \mathbb{Z}[i]$ die Norm $N(\pi)$ entweder gleich 2, eine Primzahl kongruent 1 modulo 4 oder das Quadrat einer Primzahl kongruent 3 modulo 4. Dies zeigt, dass die gegebene Bedingung notwendig ist.
Sei nun

$$n = (p_1 \cdots p_r) \cdot (n')^2$$

mit Primzahlen $p_i \not\equiv 3 \bmod 4$, $i = 1, \ldots, r$. Nach dem Zerlegungsgesetz finden wir Primelemente $\pi_i \in \mathbb{Z}[i]$ mit $N(\pi_i) = p_i$, $i = 1, \ldots, r$. Wir erhalten $n = N(\alpha)$ mit $\alpha = \pi_1 \cdots \pi_r \cdot n'$. □ □

Die Frage, welche natürlichen Zahlen sich als Summe dreier Quadrate darstellen lassen, lässt sich nicht durch Normgleichungen behandeln.

3 Ringe ganzer Zahlen

3.1 Quadratische Zahlringe

Wir betrachten nun allgemeinere Zahlbereiche. Sei $d \in \mathbb{Z}$ quadratfrei (d.h. durch keine Quadratzahl > 1 teilbar) und von 0 und 1 verschieden. Mit $\sqrt{d}$ bezeichnen wir eine (willkürlich, aber fest gewählte) komplexe Lösung der Gleichung $X^2 = d$ (die andere ist dann $-\sqrt{d}$). Die Menge der komplexen Zahlen

$$a + b\sqrt{d}, \quad a, b \in \mathbb{Z},$$

ist ein Ring und wird mit $\mathbb{Z}[\sqrt{d}]$ bezeichnet. Da d als quadratfrei angenommen ist, ist $\sqrt{d}$ keine rationale Zahl. Ist $a+b\sqrt{d} = a'+b'\sqrt{d}$, so gilt $(b'-b)\sqrt{d} = (a-a')$ und daher $a = a'$ und $b = b'$, d.h. die Darstellung ist eindeutig. Wir betrachten nun die folgende Normfunktion auf $\mathbb{Z}[\sqrt{d}]$:

$$N(a + b\sqrt{d}) = (a + b\sqrt{d})(a - b\sqrt{d}) = a^2 - db^2.$$

Ist d negativ, so ist $N(z)$, wie im Falle der Gaußschen Zahlen, gerade das Quadrat des Absolutbetrages von z als komplexe Zahl. Für positives d ist das nicht richtig, die Norm kann sogar negativ sein. So hat $\sqrt{2}-1 \in \mathbb{Z}[\sqrt{2}]$ die Norm $(-1)^2 - 2 \cdot 1^2 = -1$. Unabhängig vom Vorzeichen von d verifiziert man leicht die Regel $N(zz') = N(z)N(z')$. Ist $N(z) = 0$, so folgt aus der Quadratfreiheit von d, dass $z = 0$ ist.

Satz 3.1. *Die Funktion*

$$\nu : \mathbb{Z}[\sqrt{d}] \setminus \{0\} \longrightarrow \mathbb{N},\ z \longmapsto |N(z)|,$$

ist eine euklidische Normfunktion, falls

$$|x^2 - dy^2| < 1$$

für alle rationalen Zahlen $x, y \in \mathbb{Q}$ mit $|x| \leq \frac{1}{2}$, $|y| \leq \frac{1}{2}$ gilt.

Beweis. Wir bemerken zunächst, dass für komplexe Zahlen $x, y \in \mathbb{C}$ der Form $x = a + b\sqrt{d}$, $y = a' + b'\sqrt{d}$ mit $a, a', b, b' \in \mathbb{Q}$ auch die komplexen Zahlen $x + y$, xy und x/y von dieser Gestalt sind. Für den Quotienten (wir nehmen natürlich $y \neq 0$ an) sieht man das durch

$$\frac{x}{y} = \frac{a + b\sqrt{d}}{a' + b'\sqrt{d}} = \frac{(a + b\sqrt{d})(a' - b'\sqrt{d})}{a'^2 - db'^2} = \frac{aa' - bb'd}{a'^2 - db'^2} + \frac{a'b - ab'}{a'^2 - db'^2}\sqrt{d}.$$

Seien $a, b \in \mathbb{Z}[\sqrt{d}]$, $b \neq 0$. Wie wir gerade gesehen haben, hat die komplexe Zahl a/b die Gestalt

$$\frac{a}{b} = u + v\sqrt{d}$$

mit $u, v \in \mathbb{Q}$. Nun wählen wir ganze Zahlen $x, y \in \mathbb{Z}$ mit $|u - x| \leq 1/2$, $|v - y| \leq 1/2$. Mit $q = x + y\sqrt{d}$ erhalten wir nach Voraussetzung

$$\left|N\left(\frac{a}{b} - q\right)\right| = \left|(u - x)^2 - d(v - y)^2\right| < 1.$$

Setzen wir $r = a - bq \in \mathbb{Z}[\sqrt{d}]$, so gilt

$$\nu(r) = |N(r)| = \left|N(b)N\left(\frac{a}{b} - q\right)\right| < |N(b)| = \nu(b).$$

Also erfüllen q und r das Gewünschte. □

Korollar 3.2. *Für $d = -2, -1, 2, 3$ ist der Ring $\mathbb{Z}[\sqrt{d}]$ euklidisch und daher auch faktoriell.*

Beweis. Es gilt in den verschiedenen Fällen:

$$d = -2: \quad |x^2 + 2y^2| \leq \tfrac{3}{4} < 1; \qquad d = -1: \quad |x^2 + y^2| \leq \tfrac{1}{2} < 1;$$
$$d = +2: \quad |x^2 - 2y^2| \leq \tfrac{1}{2} < 1; \qquad d = +3: \quad |x^2 - 3y^2| \leq \tfrac{3}{4} < 1.$$

□

Leider ist der Ring $\mathbb{Z}[\sqrt{d}]$ oft nicht faktoriell (und damit insbesondere nicht euklidisch). So haben wir beispielsweise im Ring $\mathbb{Z}[\sqrt{-5}]$ die Zerlegung

$$(1+\sqrt{-5})(1-\sqrt{-5}) = 6 = 2 \cdot 3.$$

Die Elemente $1+\sqrt{-5}$, $1-\sqrt{-5}$, 2, 3 sind sämtlich irreduzibel, also ist $\mathbb{Z}[\sqrt{-5}]$ nicht faktoriell. Ein weiteres, ganz praktisches Problem ist das folgende. Die dritte Einheitswurzel

$$\zeta_3 = e^{2\pi i/3} = -\frac{1}{2} + \frac{1}{2}\sqrt{-3}$$

liegt nicht im Ring $\mathbb{Z}[\sqrt{-3}]$. Wir würden aber gerne mit ζ_3 arbeiten, um zum Beispiel zur Lösung der Fermat-Gleichung $X^3 + Y^3 = Z^3$ die Identität

$$X^3 + Y^3 = (X+Y)(X+\zeta_3 Y)(X-\zeta_3 Y)$$

heranziehen zu können. Wir werden uns diesem Problem im nächsten Abschnitt widmen.

3.2 Ganzheit

Sei $\phi : A \to B$ ein Ringhomomorphismus. Dann nennt man B eine A-Algebra. B wird zum A-Modul durch $a \cdot b \stackrel{df}{=} \phi(a) \cdot b$.
Insbesondere ist für $f \in A[X]$ und $b \in B$ das Element $f(b) \in B$ definiert

Definition 3.3. ϕ heißt endlich (und B endliche A-Algebra) wenn B als A-Modul endlich erzeugt ist.

Satz 3.4. *Sei $\phi : A \to B$ ein Ringhomomorphismus und $b \in B$. Dann sind äquivalent*

(i) *es existiert ein normiertes Polynom $f \in A[X]$ mit $f(b) = 0$.*

(ii) *der Unterring $A[b] \subset B$ ist als A-Modul endlich erzeugt.*

(iii) *es existiert ein endlich erzeugter A-Untermodul $M \subset B$ mit $1 \in M$ und $b \cdot M \subset M$.*

Beweis. Siehe Algebra 1, 3.3 oder beliebiges Algebra-Buch. □

Definition 3.5. $b \in B$ heißt **ganz** über A, wenn es die äquivalenten Bedingungen von 3.4 erfüllt. ϕ heißt **ganz** (bzw. B heißt ganz über A), wenn jedes Element $b \in B$ ganz über A ist.

Bemerkung 3.6. Endliche Ringhomomorphismen sind ganz (setze $M = B$ in (iii).

Satz 3.7. *Seien $A \xrightarrow{\phi} B \xrightarrow{\psi} C$ Ringhomomorphismen.*

(i) *sind ψ und ϕ endlich, so auch $\psi \circ \phi$.*

(ii) *sind ψ und ϕ ganz, so auch $\psi \circ \phi$.*

Beweis. Siehe Algebra 1, 3.49 und 3.52 oder beliebiges Algebra-Buch. □

Satz 3.8. *Sei $\phi : A \to B$ ein Ringhomomorphismus und $B = A[b_1, \ldots, b_n]$, also B ist e.e. A-Algebra. Sind $b_1, \ldots, b_n$ ganz über A, so ist B eine endliche A-Algebra.*

Beweis. Siehe Algebra 1, 3.50 oder beliebiges Algebra-Buch. □

Korollar 3.9. *Sind $b_1, b_2 \in B$ ganz über A, so auch $b_1 + b_2$ und $b_1 b_2$.*

Sei nun A nullteilerfrei und $K = Q(A)$ der Quotientenkörper. Sei $L|K$ eine algebraische Körpererweiterung

Definition 3.10.

$$A_L = \{x \in L \mid x \text{ ganz über } A\}$$

heißt der **Ganzabschluss** von A in L. A heißt ganzabgeschlossen, wenn $A = A_K$.

Bemerkung 3.11. Nach 3.9 ist A_L ein Ring. L ist der Quotientenkörper von A_L und A_L ist ganzabgeschlossen.

Beispiel 3.12 (eines nicht ganzabgeschlossenen Ringes). Sei $f = X^2 - Y^3 \in \mathbb{C}[X, Y]$ und $A = \mathbb{C}[X, Y]/(f)$. A ist nullteilerfrei weil f irreduzibel ist.

Sei x das Bild von X in A; wegen $f \nmid X$ gilt $x \neq 0$. Analog sei y das Bild von Y in A; wegen $f \nmid Y$ gilt $y \neq 0$. Es gilt $x^2 = y^3$ in A. Daher gilt

$$\left(\frac{x}{y}\right)^2 - y = \frac{x^2}{y^2} - y = \frac{x^2 y}{y^3} - y = y - y = 0.$$

Also ist $\frac{x}{y} \in Q(A)$ ganz über A. Aber $\frac{x}{y} \notin A$. Ansonsten wäre nämlich $x = y \cdot \frac{x}{y} \in Ay$ und somit $X \in (Y, X^2 - Y^3)$. Aber $(Y, X^2 - Y^3) = (Y, X^2) \not\ni X$. Also ist A nicht ganzabgeschlossen.