

3.7 Quadratische Zahlringe

Wir haben in diesem Kapitel eine Fülle von Begriffen zur Ringtheorie eingeführt: Einheit, Primelement, irreduzibles Element, Ideal, Primideal, maximales Ideal, Hauptidealring, euklidischer Ring. Alle diese Begriffe sind für den grundlegenden Aufbau der Theorie unverzichtbar; andererseits ergeben sich im Rahmen einer einführenden Vorlesung Beispiele zunächst nur durch den Ring \mathbb{Z} der ganzen Zahlen und den Polynomring $K[X]$ über einem Körper.

In diesem Abschnitt betrachten wir eine weitere Klasse von Ringen, die aus der Zahlentheorie kommen, die sogenannten quadratischen Zahlringe, genauer: Ringe ganz-algebraischer Zahlen in quadratischen Zahlkörpern. Die Ergebnisse über solche Ringe, die wir im Folgenden entwickeln, liefern eine Fülle von Beispielen und neuen Phänomenen zu den genannten Begriffen. Außerdem haben sie Anwendungen auf Problemstellungen der „Zahlentheorie im engeren Sinne“, womit insbesondere die Theorie polynomialer diophantischer Gleichungen gemeint ist. Wir benutzen einige Grundbegriffe der Körpertheorie aus Abschnitt 4.1.

Definition und Bemerkung 3.7.1

- a) Ein *algebraischer Zahlkörper* ist eine endliche Körpererweiterung der rationalen Zahlen.
- b) Ein *quadratischer Zahlkörper* ist eine Erweiterung vom Grad $[K : \mathbb{Q}] = 2$. Er heißt *reell-quadratisch*, falls eine Einbettung $K \hookrightarrow \mathbb{R}$ existiert, anderenfalls *imaginär-quadratisch*.
- c) Jeder quadratische Zahlkörper K ist von der Form $\mathbb{Q}[\sqrt{d}]$, wobei $d \in \mathbb{Z} \setminus \{0, 1\}$ quadratfrei ist. Dabei ist d durch die Isomorphieklasse von K eindeutig bestimmt. K ist reell-quadratisch, wenn $d > 0$, und imaginär-quadratisch, wenn $d < 0$.

Unter einer quadratfreien ganzen Zahl verstehen wir dabei eine Zahl, die nicht von der Form $d_0 k^2$ mit $d_0 \in \mathbb{Z}$, $d_0 \neq 0$, $k \in \mathbb{N}$, $k > 1$ ist; dafür brauchen wir keine förmliche Definition. Wir erinnern an Abschnitt 3.4, insbesondere an Beispiel 3.4.11 (2) für die verschiedenen Bedeutungen von \sqrt{d} . Wenn wir im folgenden einen quadratischen Zahlkörper in der Form $\mathbb{Q}[\sqrt{d}]$ mit $d \in \mathbb{Z}$ schreiben, werden immer voraussetzen, dass d quadratfrei ist, ohne dieses ständig zu wiederholen.

Definition 3.7.2 Ein Element α eines Erweiterungskörpers $K : \mathbb{Q}$ heißt *ganz-algebraisch*, oder *ganze algebraische Zahl*, wenn es ein normiertes Polynom $f = a_0 + a_1 X + \cdots + X^n \in \mathbb{Z}[X]$ gibt mit $f(\alpha) = 0$. Die Menge aller ganz-algebraischen Elemente in K wird mit \mathbb{Z}_K bezeichnet.

Jede ganz-algebraische Zahl ist insbesondere algebraisch.

Beispiele

1. $\frac{1+\sqrt{5}}{2}$ ist eine ganz-algebraische Zahl.
2. Jede Einheitswurzel ist eine ganz-algebraische Zahl.
3. $\frac{1+\sqrt{2}}{2}$ ist keine ganz-algebraische Zahl.

Das negative Resultat im dritten Beispiel wird im nächsten Satz verallgemeinert und bewiesen.

Satz 3.7.3 *Eine algebraische Zahl ist genau dann ganz-algebraisch, wenn ihr Minimalpolynom Koeffizienten in \mathbb{Z} hat.*

Der Beweis folgt unmittelbar aus dem „Lemma von Gauß“ für Polynome, Satz 3.5.4.

Als nächstes wollen wir die ganz-algebraischen Zahlen in einem quadratischen Zahlkörper explizit bestimmen. Sei also $K = \mathbb{Q}[\sqrt{d}]$ mit $d \in \mathbb{Z} \setminus \{0, 1\}$ und d quadratfrei. Zu $\alpha = x + y\sqrt{d}$ mit $x, y \in \mathbb{Q}$ nennen wir $\alpha' = x - y\sqrt{d}$ die *konjugierte Zahl*. Man definiert für $\alpha \in K$ die *Norm* durch $N(\alpha) = \alpha\alpha'$ und die *Spur* durch $S(\alpha) = \alpha + \alpha'$. Die Norm und die Spur liegen in \mathbb{Q} . Genauer gilt

$$N(\alpha) = x^2 - dy^2, \quad S(\alpha) = 2x \quad \text{für } \alpha = x + y\sqrt{d}, \quad x, y \in \mathbb{Q}. \quad (3.7.1)$$

Die Norm ist multiplikativ, d.h.

$$N(\alpha\beta) = N(\alpha)N(\beta) \quad \text{für alle } \alpha, \beta \in \mathbb{Q}[\sqrt{d}]. \quad (3.7.2)$$

Das liegt daran, dass die Konjugation ein Körperautomorphismus ist, insbesondere $(\alpha\beta)' = \alpha'\beta'$ für alle $\alpha, \beta \in K$. Man beachte, dass $\alpha^2 - S(\alpha)\alpha + N(\alpha) = 0$ ist, also $S(\alpha)$ und $N(\alpha)$ die Koeffizienten des Minimalpolynoms von α sind, sobald $\alpha \notin \mathbb{Q}$, also $\alpha \neq \alpha'$ bzw. $y \neq 0$ ist. Unter Berücksichtigung von Satz 3.7.3 beweist dieses Teil a) des nächsten Satzes.

Satz 3.7.4 *Es sei $K = \mathbb{Q}[\sqrt{d}]$ ein quadratischer Zahlkörper, $N : K \rightarrow \mathbb{Q}$ die Norm und $S : K \rightarrow \mathbb{Q}$ die Spur. Dann gilt für Menge \mathbb{Z}_K der ganz-algebraischen Zahlen in K folgendes:*

a) $\mathbb{Z}_K = \{\alpha \in K \mid S(\alpha) \in \mathbb{Z} \text{ und } N(\alpha) \in \mathbb{Z}\};$

b) $\mathbb{Z}_K = \mathbb{Z} \cdot 1 + \mathbb{Z} \cdot \omega$, wobei $\omega = \begin{cases} \frac{1+\sqrt{d}}{2} & \text{für } d \equiv_4 1 \\ \sqrt{d} & \text{für } d \equiv_4 2, 3; \end{cases}$

c) $\mathbb{Z}_K = \mathbb{Z}[\omega]$, dabei ω wie in b);

d) \mathbb{Z}_K ist ein Teilring von K .

Die Bezeichnung \mathbb{Z}_K wird für jeden algebraischen Zahlkörper K benutzt (sogar für eine beliebige Erweiterung von \mathbb{Q} , d.h. für einen beliebigen Körper der Charakteristik Null). Man spricht auch kurz von den „ganzen Zahlen in K “. Der Teil d) des Satzes gilt für jeden Körper $K : \mathbb{Q}$; deshalb nennt man \mathbb{Z}_K auch den „Ring der ganzen Zahlen“ von K . Der Beweis ist komplizierter und wird in der algebraischen Zahlentheorie geführt.

Teil b) des Satzes besagt, dass \mathbb{Z}_K eine „ \mathbb{Z} -Basis“, genauer, eine Basis als \mathbb{Z} -Modul, aus zwei Elementen besitzt, nämlich $1, \omega$. Der hier verwendete Begriff des „Moduls“, genauer, R -Moduls für einen kommutativen Ring R , ist dabei eine natürliche Verallgemeinerung des Vektorraum-Begriffs, wobei die Skalare jetzt in einem kommutativen Ring R (hier $R = \mathbb{Z}$) statt eines Körpers liegen. Wenn der quadratische Zahlkörper K durch einen algebraischen Zahlkörper vom Grad $n = [K : \mathbb{Q}]$ ersetzt wird, gilt Teil b) entsprechend, wobei dann die \mathbb{Z} -Basis von \mathbb{Z}_K aus n Elementen besteht (und gleichzeitig auch eine Basis von K als \mathbb{Q} -Vektorraum ist).

Definition 3.7.5 Der Ring $\mathbb{Z} \left[\frac{1+\sqrt{-3}}{2} \right]$ der ganzen Zahlen in $\mathbb{Q}[\sqrt{-3}]$ heißt Ring der (ganzen) *Eisenstein'schen Zahlen*

Wesentliches Hilfsmittel für die weitere Untersuchung von \mathbb{Z}_K ist wieder die Normfunktion $N : \mathbb{Z}_K \rightarrow \mathbb{Z}$. Wir wenden uns zunächst den Einheiten zu.

Lemma 3.7.6 Es sei K ein quadratischer Zahlkörper. Ein $\alpha \in \mathbb{Z}_K$ ist Einheit in \mathbb{Z}_K genau dann, wenn $N(\alpha) = \pm 1$ ist.

Um diese Bedingung weiter auszuwerten, stellen wir α in der Basis aus Satz 3.7.4 b) dar: $\alpha = x + y\omega$, $x, y \in \mathbb{Z}$. Im Fall $d \equiv_4 2, 3$ ergibt sich formelmäßig gegenüber (3.7.1) keine Änderung:

$$N(\alpha) = x^2 - dy^2 = \pm 1, \quad x, y \in \mathbb{Z}. \quad (3.7.3)$$

Im Fall $d \equiv_4 1$ erhalten wir

$$N(\alpha) = x^2 + xy + \frac{1-d}{4}y^2 = \pm 1, \quad x, y \in \mathbb{Z}. \quad (3.7.4)$$

Als Funktion von x und y ist die Norm eine quadratische Form (wie aus der Linearen Algebra bzw. analytischen Geometrie bekannt); sie wird kurz als *Normform* bezeichnet. Die beiden Formen (3.7.3) und (3.7.4) sind über dem Körper \mathbb{Q} äquivalent (nicht jedoch über dem Ring \mathbb{Z} , bei geeigneter Erweiterung der Definition der Äquivalenz auf Ringe). Man spricht von einer *binären quadratischen Form*, weil die Anzahl der Variablen gleich zwei ist. Es gibt wesentliche Unterschiede zwischen den reell- und den imaginär-quadratischen Zahlkörpern, die sich bereits in folgender elementarer Unterscheidung der Normformen widerpiegeln.

Bemerkung 3.7.7 Die Normform eines imaginär-quadratischen Zahlkörpers ist positiv definit; die Normform eines reell-quadratischen Körpers ist indefinit von der Signatur $(1, 1)$.

Bei der Bestimmung der Einheiten von \mathbb{Z}_K ist der imaginär-quadratische Fall $d < 0$ der wesentlich einfachere.

Im Fall $d \equiv_4 2, 3$ wird die Gleichung (3.7.3) zu $x^2 + |d|y^2 = 1$. Für $d \neq -1$ gibt es nur die immer existierenden Lösungen $x = \pm 1, y = 0$, die zu den „trivialen Einheiten“ ± 1 gehören. Für $d = -1$ (also den Ring der Gauß'schen Zahlen) kommen noch die Lösungen $x = 0, y = \pm 1$, also die Einheiten $\pm i$ dazu.

Im Fall $d \equiv_4 1$ diagonalisieren wir die Gleichung (3.7.4) als $(x + \frac{1}{2}y)^2 + \frac{|d|}{4}y^2 = 1$. Für $d \neq -3$, also $|d| \geq 7$ gibt es wieder nur die trivialen Lösungen mit $y = 0$. Für $d = -3$ kommen noch Lösungen mit $|y| = 1$ dazu. Möglich ist dabei $x = 0, y = \pm 1$ und $x = \pm 1, y = \mp 1$. Wir haben folgenden Satz bewiesen; für die Formulierung erinnern wir noch an die Bezeichnung ζ_m für eine primitive m -te Einheitswurzel, also ein Element der Ordnung m in der multiplikativen Gruppe eines Körpers K ; für $K \subset \mathbb{C}$ kann man $\zeta_m = e^{\frac{2\pi i}{m}}$ wählen.

Satz 3.7.8 *Es sei $K = \mathbb{Q}[\sqrt{d}]$ ein imaginär-quadratischer Zahlkörper, also $d < 0$. Für die Einheitengruppe des Ringes \mathbb{Z}_K seiner ganzen Zahlen gilt*

$$\mathbb{Z}_K^* = \begin{cases} \{\pm 1, \frac{\pm 1 \pm \sqrt{-3}}{2}\} & = \langle \zeta_6 \rangle \quad \text{für } d = -3 \\ \{1, -1, i, -i\} & = \langle \zeta_4 \rangle \quad \text{für } d = -1 \\ \{1, -1\} & = \langle \zeta_2 \rangle \quad \text{für } d < -3. \end{cases}$$

Sie besteht aus den in K enthaltenen Einheitswurzeln.

Die Einheitengruppe der ganzen Zahlen eines imaginärquadratischen Zahlkörpers ist also bis auf zwei Ausnahmen „trivial“, besteht also wie bei \mathbb{Z} nur aus ± 1 ; lediglich für die Eisenstein'schen und die Gauß'schen Zahlen kommen noch die in dem Körper liegenden (weiteren) Einheitswurzeln hinzu.

Satz 3.7.9 *Für einen reell-quadratischen Zahlkörper $K = \mathbb{Q}[\sqrt{d}]$, also $d > 0$, hat der Ring der ganzen Zahlen \mathbb{Z}_K unendlich viele Einheiten. Genauer hat man eine Isomorphie*

$$\mathbb{Z}_K^* = \{\pm 1\} \cdot \langle \varepsilon_0 \rangle \cong \mathbb{Z}_2 \times \mathbb{Z}.$$

Nach Wahl einer Einbettung $K \hookrightarrow \mathbb{R}$ ist das erzeugende Element ε_0 des unendlich zyklischen Anteils durch die Forderung $\varepsilon_0 > 1$ eindeutig bestimmt und heißt die Grundeinheit von \mathbb{Z}_K (oder auch einfach von K).

Wenn der Satz bewiesen ist, ist die explizite Bestimmung der Grundeinheit im Prinzip sehr einfach: Unter allen Einheiten $\varepsilon > 1$ ist die Grundeinheit diejenige vom kleinsten Absolutbetrag. Dieses wiederum ist äquivalent dazu, dass in der Lösung von Gleichung (3.7.3) bzw. (3.7.4) y (oder x) kleinstmöglich ist. Das naive

Verfahren zur Lösung von (3.7.3) besteht also darin, dass man $y = 1, 2, 3, \dots$ laufen lässt und überprüft, wann zum ersten Mal $dy^2 \pm 1$ ein Quadrat in \mathbb{Z} ist. Die Gleichung (3.7.4) ersetzt man durch $x^2 - dy^2 = \pm 4$ mit der Nebenbedingung $x \equiv_2 y$ und verfährt analog. **Ein wesentlich effizienteres Verfahren zur Lösung der beiden Gleichungen, das auch theoretisch befriedigender ist, erhält man aus der Theorie der Kettenbrüche.**

Beispiele 3.7.10 Sei weiterhin $K = \mathbb{Q}[\sqrt{d}]$, $d > 0$.

a) Für $d \equiv_4 1$, $1 < d \leq 29$ sind die Grundeinheiten von \mathbb{Z}_K gleich

$$\frac{1 + \sqrt{5}}{2}, \frac{3 + \sqrt{13}}{2}, 4 + \sqrt{17}, \frac{5 + \sqrt{21}}{2}, \frac{5 + \sqrt{29}}{2}.$$

b) Für $d \equiv_4 2, 3$, $1 < d \leq 19$ sind die Grundeinheiten von \mathbb{Z}_K gleich

$$1 + \sqrt{2}, 2 + \sqrt{3}, 5 + 2\sqrt{6}, 8 + 3\sqrt{7}, 3 + \sqrt{10}, \\ 10 + 3\sqrt{11}, 15 + 4\sqrt{14}, 4 + \sqrt{15}, 170 + 39\sqrt{19}.$$

Wir kommen nun zu den unzerlegbaren bzw. zerlegbaren Elementen \mathbb{Z}_K . Wenn man eine Zerlegung $\gamma = \alpha\beta$ hat, so ergibt sich wegen der Multiplikativität der Norm eine entsprechende Zerlegung $N(\gamma) = N(\alpha)N(\beta)$. Insbesondere erhält man unter Benutzung von Lemma 3.7.6

Bemerkung 3.7.11 Sei $\gamma \in \mathbb{Z}_K$ so, dass $N(\gamma)$ eine Primzahl ist. Dann ist γ unzerlegbar.

Die Umkehrung der letzten Bemerkung gilt nicht. Es kommt häufig vor, dass eine Primzahl p auch in \mathbb{Z}_K unzerlegbar bleibt, jedoch gilt $N(p) = p^2$. Hierzu überlegt man sich leicht

Bemerkung 3.7.12 Eine Primzahl p ist genau dann im quadratischen Zahlring \mathbb{Z}_K zerlegbar, wenn p oder $-p$ die Norm eines Elementes aus \mathbb{Z}_K ist.

Zum Beispiel ist im Ring der Gauß'schen Zahlen das Element 3 unzerlegbar, denn die Gleichung $x^2 + y^2 = 3$, $x, y \in \mathbb{Z}$, ist nicht lösbar.

BEWEIS von 3.7.12: In einer Zerlegung $p = \alpha\beta$ einer Primzahl in zwei Faktoren in \mathbb{Z}_K , von denen keiner eine Einheit ist, muss nach Lemma 3.7.6 $N(\alpha) = N(\beta) = \pm p$ sein. Die beiden Faktoren sind dann übrigens notwendig irreduzibel. Wenn umgekehrt $\pm p = N(\alpha)$ ist, dann ist $p = \alpha \cdot \mp\alpha'$, und die beiden Faktoren liegen in \mathbb{Z}_K und sind keine Einheiten. \square

Man kann sich fragen, wann ein gemäß 3.7.11 unzerlegbares p sogar ein Primelement in \mathbb{Z}_K ist (vergl. 3.3.10). Allgemein ist das nicht der Fall:

Beispiel 3.7.13 Im Ring $\mathbb{Z}[\sqrt{-5}]$ sind die Elemente $2, 3, \beta = 1 + \sqrt{-5}, \bar{\beta} = 1 - \sqrt{-5}$ unzerlegbar, aber sämtlich keine Primelemente.

BEWEIS: Die Normen der angegebenen Elemente sind $4, 9$ und 6 , und die Unzerlegbarkeit folgt wie in Bemerkung 3.7.11 daraus, dass es keine Elemente der Normen 2 oder 3 gibt. Andererseits gilt $2 \cdot 3 = \beta \cdot \bar{\beta}$, d.h. 2 und 3 teilen das Produkt $\beta \cdot \bar{\beta}$, ohne einen der Faktoren zu teilen, können also nicht prim sein. Mit vertauschten Rollen der beiden Seiten unserer Gleichung ergibt sich entsprechend, dass β und $\bar{\beta}$ nicht prim sind. \square

Folgerung 3.7.14 Der Ring $\mathbb{Z}[\sqrt{-5}]$ ist kein Hauptidealring.

In der Tat, wenn $\mathbb{Z}[\sqrt{-5}]$ ein Hauptidealring wäre, so wäre jedes unzerlegbare Element auch Primelement, nach 3.3.11.

Es ist wünschenswert, einen direkten Beweis von 3.7.14 zu haben. Hierzu erinnern wir zunächst an die Kurznotation (a, b) für das von zwei Elementen $a, b \in R$ erzeugte Ideal in einem Ring R sowie (a) für das von a erzeugte Hauptideal:

$$(a, b) := Ra + Rb, \quad (a) = Ra.$$

Das folgende Beispiel benutzt die Zahlenwerte aus Beispiel 3.7.13.

Beispiel 3.7.15 Das Ideal $(2, \beta)$ in $\mathbb{Z}[\sqrt{-5}]$ ist kein Hauptideal.

BEWEIS durch Widerspruch: Angenommen $(2, \beta) = (\delta)$ für ein $\delta \in \mathbb{Z}[\sqrt{-5}]$. Durch Teilbarkeitsbetrachtungen können wir nun die Norm von δ weitgehend einschränken und so letztlich zu einem Widerspruch kommen:

$$\begin{aligned} 2 \in (\delta) &\iff \delta | 2 \implies N(\delta) | N(2) = 4 \\ \beta \in (\delta) &\iff \delta | \beta \implies N(\delta) | N(\beta) = 6. \end{aligned}$$

Also gilt $N(\delta) = 2$ oder $N(\delta) = 1$. Die erste Möglichkeit scheidet aus, weil $x^2 + 5y^2 = 2$ mit $x, y \in \mathbb{Z}$ nicht lösbar ist. Es bleibt die Möglichkeit $N(\delta) = 1$. Dann ist $(2, \beta) = (1)$, es existieren also $\xi, \eta \in \mathbb{Z}[\sqrt{-5}]$ mit $\xi \cdot 2 + \eta \cdot \beta = 1$. Der explizite Ansatz $\xi = x + y\sqrt{-5}, \eta = u + v\sqrt{-5}$ führt auf

$$2x + u - 5v = 1, \quad 2y + u + v = 0.$$

Aus der ersten Gleichung folgt $u + v \equiv 1 \pmod{2}$, aus der zweiten $u + v \equiv 0 \pmod{2}$; Widerspruch.

Alternativ, und mehr im Stil des ersten Teils des Beweises kann man sich überlegen, dass ein Element aus $(2, \beta)$ immer eine gerade Zahl als Norm hat, was wiederum die 1 ausschließt. \square

Wenn \mathbb{Z}_K kein Hauptidealring ist, hat die Frage nach den Primelementen keine glatte Antwort. Es war die historische Leistung von Richard Dedekind (1831 - 1916), stattdessen die Rolle der Primideale herauszustellen. Im folgenden Satz halten wir einige einfache, grundlegende Tatsachen über Ideale in \mathbb{Z}_K fest:

Satz 3.7.16 a) Jedes Ideal $I \triangleleft \mathbb{Z}_K$ enthält eine ganz-rationale Zahl $\neq 0$.

b) Jedes Ideal $I \triangleleft \mathbb{Z}_K$ hat endlichen Index in der abelschen Gruppe \mathbb{Z}_K .

c) Für jedes Primideal $P \triangleleft \mathbb{Z}_K$ gibt es eine eindeutige Primzahl p mit $p \in P$.

d) Jedes Primideal $P \triangleleft \mathbb{Z}_K$ ist maximal.

Das in den obigen Beispielen 3.7.13 und 3.7.15 demonstrierte Verhalten des Ringes $\mathbb{Z}[\sqrt{-5}]$ ist typisch für die Ringe $\mathbb{Z}[\sqrt{d}]$ mit negativem d . Man kann für alle $d \leq -3$ Ideale angeben, die keine Hauptideale sind, sowie irreduzible Elemente, die nicht prim sind. Die beiden verbleibenden Ringe dieser Bauart sind in der Tat Hauptidealringe, wie sich aus dem nächsten Satz 3.7.17 ergibt. Für die Ringe $\mathbb{Z}_K = \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$ mit $d \equiv_4 1$ ist die Situation völlig analog; hier erhält man einen Hauptidealring in den 7 Fällen $d = -3, -7, -11, -19, -43, -67, -163$, und für kein anderes d , was etwas aufwendiger zu beweisen ist.

Satz 3.7.17 Der Ring $\mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$ der Eisenstein'schen Zahlen, der Ring $\mathbb{Z}[i]$ der Gauß'schen Zahlen und der Ring $\mathbb{Z}[\sqrt{-2}]$ sind euklidisch mit der Normfunktion als Gradfunktion. Insbesondere sind sie Hauptidealringe.

BEWEIS: Setze kurz $R = \mathbb{Z}[\sqrt{d}]$, $d = -1, -2$. Für das geometrische Verständnis des folgenden Beweises ist es nützlich, $R = \mathbb{Z}1 \oplus \mathbb{Z}[\sqrt{d}] \subseteq \mathbb{C} \cong \mathbb{R} \times \mathbb{R}$ als ein sogenanntes Gitter in der euklidischen Ebene anzusehen, nämlich den \mathbb{Z} -Spann von zwei über \mathbb{R} linear unabhängigen Vektoren. Dabei haben wir für $d = -1$ genau das Standardgitter $\mathbb{Z}^2 \subset \mathbb{R}^2$. Entscheidend für den Beweis ist nun die folgende Approximationseigenschaft von R :

$$\text{Zu jedem } z \in \mathbb{C} \text{ gibt es ein } \zeta \in R \text{ mit } N(z - \zeta) < 1. \quad (3.7.5)$$

Man beachte, dass $N(z - \zeta)$ der euklidische Abstand von z zu ζ zum Quadrat ist. Die Behauptung zeigt man rechnerisch einfach durch Runden der beiden reellen Koordinaten von z : man schreibt $z = x + y\sqrt{d}$, $x, y \in \mathbb{R}$ und setze $\zeta = x' + y'\sqrt{d}$ mit $x', y' \in \mathbb{Z}$, $|x - x'| \leq \frac{1}{2}$, $|y - y'| \leq \frac{1}{2}$. Dann ist

$$N(z - \zeta) = (x - x')^2 - d(y - y')^2 \leq \frac{1}{4} + 2 \cdot \frac{1}{4} < 1.$$

Mittels (3.7.5) können wir nun unmittelbar feststellen, dass die Division mit Rest in R funktioniert. Für gegebene Elemente $a, b \in R$ mit $b \in R$ betrachte zunächst den gewöhnlichen Quotienten $z = \frac{a}{b} \in \mathbb{C}$; wähle dann gemäß (3.7.5) ein $q \in R$ mit $N(z - q) < 1$. Wir haben dann

$$a = zb = qb + (z - q)b,$$

wobei für den Rest $r = (z - q)b$ einerseits gilt $r = a - qb \in R$, andererseits $N(r) = N((z - q) \cdot b) = N(z - q)N(b) < N(b)$.

Für den Ring $R = \mathbb{Z}[\zeta_6]$ geht der Beweis völlig analog durch; die entscheidende Eigenschaft (3.7.5) gilt „erst recht“; statt des Quadrate-Gitters \mathbb{Z}^2 ist R jetzt das sogenannte „hexagonale Gitter“, das von zwei Einheitsvektoren im Winkel von 60° erzeugt wird. \square

Aus der bisher entwickelten Theorie folgt bereits eine Reihe von Sätzen der klassischen elementaren Zahlentheorie. Wir behandeln **exemplarisch** den folgenden, zuerst von Pierre Fermat (ca. 1607 - 1665) aufgestellten Satz:

Satz 3.7.18 (Zwei-Quadrate-Satz von Euler) ⁵

Eine Primzahl $p \neq 2$ ist Summe von zwei ganzen Quadraten genau dann, wenn $p \equiv 1 \pmod{4}$ ist.

BEWEIS: **Vorlesung am 22.07.** Ansatz: p ist Summe von zwei Quadraten genau dann, wenn p Norm eines Elementes in $\mathbb{Z}[i]$ ist, genau dann, wenn $p\mathbb{Z}[i]$ kein Primideal ist.

Wir wollen uns nun in voller Allgemeinheit der Frage widmen, wann eine Primzahl auch in \mathbb{Z}_k prim bleibt, oder wie alternativ die $p\mathbb{Z}_K$ echt umfassenden Primideale aussehen. Nach Satz 3.7.16 c) haben wir dann alle Primideale in \mathbb{Z}_K erfasst.

Definition 3.7.19 Es sei p eine Primzahl, $(p) := p\mathbb{Z}_K$ das von ihr erzeugte Ideal in \mathbb{Z}_K .

1. p heißt *träge* in K , falls (p) prim ist.
2. p heißt *zerlegt* in K , falls $(p) = PP'$ ist, wobei P und P' zwei verschiedene Primideale in \mathbb{Z}_K sind.
3. p heißt *verzweigt* in K , falls $(p) = P^2$ für ein Primideal P in \mathbb{Z}_K ist.

Der nächste Satz ist ein Spezialfall der allgemeinen Theorie algebraischer Zahlkörper und folgt in unserem Kontext alternativ aus den unten angegebenen Kriterien.

Satz 3.7.20 Jede Primzahl ist entweder träge, oder zerlegt oder verzweigt (und diese Bedingungen schließen sich gegenseitig aus).

Das folgende Kriterium ist in der Literatur über quadratische Zahlkörper meist nicht in dieser Form zu finden, wohl aber in der allgemeinen Theorie der algebraischen Zahlkörper.

Satz 3.7.21 Es sei ω wie oben ein Erzeugendes von \mathbb{Z}_K mit Minimalpolynom $p_\omega \in \mathbb{Z}[X]$. Mit $\bar{p}_\omega \in (\mathbb{Z}/p\mathbb{Z})[X]$ bezeichnen wir das modulo p reduzierte Polynom.

⁵Leonhard Euler, 1707 – 1783

1. p ist träge in K genau dann, wenn \bar{p}_ω irreduzibel ist.
2. p ist zerlegt in K genau dann, wenn \bar{p}_ω zwei verschiedene Nullstellen in $\mathbb{Z}/p\mathbb{Z}$ hat.
3. p ist verzweigt in K genau dann, wenn \bar{p}_ω eine doppelte Nullstelle in $\mathbb{Z}/p\mathbb{Z}$ hat.

Wohlbekannt sind die beiden folgenden expliziten Kriterien, die beide leicht aus dem vorigen Satz folgen; das erste benutzt das Legendre-Symbol.

Satz 3.7.22 Sei $K = \mathbb{Q}[\sqrt{d}]$, $p \neq 2$.

1. p ist träge in K genau dann, wenn $\left(\frac{d}{p}\right) = -1$.
2. p ist zerlegt in K genau dann, wenn $\left(\frac{d}{p}\right) = 1$.
3. p ist verzweigt in K genau dann, wenn $\left(\frac{d}{p}\right) = 0$, d.h. $p \mid d$.

Satz 3.7.23 Sei $K = \mathbb{Q}[\sqrt{d}]$, $p = 2$.

1. 2 ist träge in K genau dann, wenn $p \equiv 5 \pmod{8}$.
2. 2 ist zerlegt in K genau dann, wenn $p \equiv 1 \pmod{8}$.
3. 2 ist verzweigt in K genau dann, wenn $p \equiv 2, 3 \pmod{4}$.

Ausblick. Wie sich im Zwei-Quadrate Satz von Euler bereits andeutete, ist das eigentliche Ziel des Studiums quadratischer Zahlringe und ihrer Ideale zahlen-theoretischer Natur: es geht um die Darstellung von Primzahlen, allgemeiner auch zusammengesetzten Zahlen in der Form $p = x^2 + my^2$, allgemeiner um die Darstellung durch sogenannte *binäre quadratische Formen*, also $p = ax^2 + bxy + cy^2$. Ein prinzipielles Problem ist, dass es anders als beim Zwei-Quadrate-Satz im allgemeinen keine einfachen Kongruenzbedingungen gibt, die die Lösbarkeit garantieren. Dieses hat mit der im allgemeinen Fall fehlenden Hauptidealeigenschaft quadratischer Zahlringe zu tun. Es gibt eine ausgefeilte Theorie über Lösbarkeit und sogenannte *Klassenzahlen* quadratischer Formen und quadratischer Zahlkörper, die diese Probleme in allgemeineren Kontexten angeht.

Literaturhinweis: Unter der fast unüberschaubaren Literatur zu diesem Teil der Zahlentheorie sei nur ein Buch genannt; es stammt von einem führenden Experten, hat aber ausdrücklich den Charakter eines einführenden Lehrbuchs:

Don B. Zagier, *Zetafunktionen und quadratische Körper*,
(Untertitel: Eine Einführung in die höhere Zahlentheorie),
Springer-Verlag, Berlin-Heidelberg-New York, 1981