# FAKTORISIEREN IN QUADRATISCHEN ZAHLKÖRPERN

SABRINA GALFETTI

## 1. Erinnerung

Wir beginnen mit eine kürze Erinnerung von den notwendigen Konzepte, die wir in dieser Kapitel benötigen.

**Definition 1.** *$\mathcal{O}_K$ ist der Ring der ganzen Zahlen von $K$, die ganz-algebraisch sind. Diese ist ein Ring und es gilt*

$$\mathcal{O}_K \cap \mathbb{Q} = \mathbb{Z}.$$

**Definition 2.** *Ein quadratischer Zahlkörper ist ein Körper der Form $\mathbb{Q}(\sqrt{d})$. Er entsteht aus den rationalen Zahlen durch Hinzunahme eine Quadratwurzel.*

## 2. Rechnen mit Idealen

In diesem Abschnitt wollen wir zeigen, dass nicht alle Ringe der ganzen algebraischen Zahlen in (quadratische) Zahlkörpern faktorielle Ring sind. Das bedeutet dass, die Primfaktorzerlegung nicht eindeutig ist.

**Beispiel 3.** *$\mathbb{Q}(\sqrt{-5})$ hat keine eindeutige Zerlegung:*

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

Um das zu sagen sollten wir natürlich überprüfen dass, 2, 3, $1 \pm \sqrt{-5}$ alle verschieden sind (trivial) und dass alle irreduzibel in $\mathcal{O}_K$ sind. Das geht ziemlich einfach mit dem Norm. Wir machen als Beispiel das erste Fall, für die andere geht es völlig analog.

**Beispiel 4.** *Wäre nämlich $2 = x \cdot y$ mit $x, y$ nicht Einheiten, so wurde aus der Norm an beide Seiten dann folgen $4 = N(x) \cdot N(y)$. $x$ hat die folgende Form: $x = a + \sqrt{-5}b$ und dann ist $N(x) = a^2 + 5b^2$. Die Norm von $x$ hat folgende mögliche Werten: $0, 1, 4, 5$ undsoweiter. Aber wenn wir die obige Gleichungen mit Normen schauen, sehen wir dass, eine Norm soll $4$ sein und die andere $1$. Norm $1$ ist eine Einheit, entsprechend folgt dass, $x$ oder $y$ eine Einheit ist und insbesondere ist dann $2$ irreduzibel.*

Es liegen also zwei verschiedene Primzerlegungen der Zahl 6 vor. Historisch hat Kummer die Idee gehabt, dass es "idealer Zahlen" gibt wo man wieder eindeutig faktorisieren kann. Um diese Problem zu lösen ist eine Idee gekommen, indem wir in einen grösseren Bereich finden können, wobei die Eindeutikeit der Primfaktorzerlegung wieder gültig ist. Aus diesem Grund führen wir das Konzept von Ideal ein.

**Definition 5.** *Ein Ideal von $\mathcal{O}_K$ ist eine Teilmenge $\mathfrak{a} \subset \mathcal{O}_K$, die die folgende Bedingung erfüllt:*

*(1)* $\mathfrak{a} \neq \varnothing$.
*(2)* $\forall a, b \in \mathfrak{a} : a + b \in \mathfrak{a}$.
*(3)* $\forall x \in \mathcal{O}_K, \forall a \in \mathfrak{a} : xa \in \mathfrak{a}$.

Diese Eigenschaften zeigen wie ein Ideal eine additive Untergruppe von $\mathcal{O}_K$ ist.

**Definition 6.** *Für jedes Element $a \in \mathcal{O}_K$ ist die Menge*

$$a\mathcal{O}_K = \{ax | x \in \mathcal{O}_K\}$$

*ein Ideal von $\mathcal{O}_K$, genannt das von $a$ erzeugt Hauptideal.*

*Bemerkung* 7. Ein Ideal $\mathfrak{a} \subset \mathcal{O}_K$ heisst Hauptideal wenn es ein $a \in \mathcal{O}_K$ mit $\mathfrak{a} = (a)$ gibt.

*Beweis.* Wir sollten zeigen, dass ein Hauptideal ein Ideal ist. Wir prüfen einfach die Eigenschaften:
(1) $a \in (a) \neq \varnothing$.

(2) Gegeben $xa, ya \in (a)$ folgt $xa + ya = (x + y)a \in (a)$
(3) Gegeben $t \in \mathcal{O}_K, xa \in (a)$ folgt $t \cdot (xa) = (tx)a \in (a)$

□

**Beispiel 8.** *Ein Beispiel von Idealen sind das Nullideal* $(0) = \{0\}$ *und das Einsideal* $(1) = \mathcal{O}_K$. *Diese sind beide Hauptidealen.*

Natürlich Hauptideale sind nicht eindeutig bestimmt, mit dem folgende Lemma sehen wir genauer warum.

**Lemma 9.** *Zwei Hauptideale* $(a)$ *und* $(b)$ *von Elementen* $a, b \in \mathcal{O}_K$ *sind genau dann gleich, wenn* $a$ *und* $b$ *assoziiert sind, d.h.*

$$(a) = (b) \Leftrightarrow a \sim b$$

*Beweis.* Aus $a \in (b)$ folgt, dass ein $x \in \mathcal{O}_K$ mit $a = xb$ existiert. Also gilt $b|a$. Analog schliesst man $a|b$, also $a \sim b$. Die Rückrichtung ist offensichtlich. □

**Definition 10.** *Seien* $\mathfrak{a}, \mathfrak{b} \subset \mathcal{O}_K$ *Ideale. Ihre Summe und ihr Produkt sind in folgender Weise definiert:*

$$\mathfrak{a} + \mathfrak{b} = \{a + b | a \in \mathfrak{a}, b \in \mathfrak{b}\}, \qquad \mathfrak{ab} = \{ \sum_{endl.} a_i b_i | a_i \in \mathfrak{a}, b_i \in \mathfrak{b}\}$$

Es ist leicht zu verifizieren, dass $\mathfrak{a} + \mathfrak{b}$, $\mathfrak{ab}$ wieder Ideale sind. Wir bezeichnen die Summe von Hauptidealen $(a_1) + \ldots + (a_n)$ mit $(a_1, \ldots, a_n)$.

Wir benötigen für unsere weiteren Untersuchungen einige Begrifflichkeiten aus der Faktorringstheorie, welche wir nun kurz wiederholen. Diese sind grundlegender Fakten aus der Algebra, welches wir ohne Beweis angeben.

## 3. Faktorringe

**Definition 11.** *Sei* $\mathfrak{a} \subset \mathcal{O}_K$ *ein Ideal. Für jedes* $x \in \mathcal{O}_K$ *heisst die Teilmenge*

$$x + \mathfrak{a} := \{x + a | a \in \mathfrak{a}\} \subset \mathcal{O}_K$$

*eine Nebenklasse von* $\mathfrak{a}$. *Wir bezeichnen die Menge aller Nebenklassen wie folgt:*

$$\mathcal{O}_K/\mathfrak{a} := \{x + \mathfrak{a} | x \in \mathcal{O}_K\}.$$

**Satz 12.** *Die Menge* $\mathcal{O}_K/\mathfrak{a}$ *besitzt eine eindeutige Ringstruktur, so dass gilt:*
*(1)* $\forall x, x' \in \mathcal{O}_K : (x + \mathfrak{a}) + (x' + \mathfrak{a}) = (x + x') + \mathfrak{a}$.
*(2)* $\forall x, x' \in \mathcal{O}_K : (x + \mathfrak{a}) \cdot (x' + \mathfrak{a}) = xx' + \mathfrak{a}$.

*Für diese gilt weiter:*
*(1) Das Nullelement von* $\mathcal{O}_K/\mathfrak{a}$ *ist* $0 + \mathfrak{a} = \mathfrak{a}$.
*(2) Das Einselement von* $\mathcal{O}_K/\mathfrak{a}$ *ist* $1 + \mathfrak{a}$.
*(3)* $\pi : \mathcal{O}_K \to \mathcal{O}_K/\mathfrak{a}, x \mapsto x + \mathfrak{a}$ *ist ein surjektiver Ringhomomorphismus mit Kern* $\mathfrak{a}$.

**Definition 13.** *Der Ring* $\mathcal{O}_K/\mathfrak{a}$ *heisst Faktorring von* $\mathcal{O}_K$ *nach* $\mathfrak{a}$.

Für uns von besonderem Interesse in Ringe sind Ideale und vor allem Primideale.

## 4. Primideale

**Definition 14.** *Ein Primideal von* $\mathcal{O}_K$ *ist ein echtes Ideal* $\mathfrak{p} \subsetneq \mathcal{O}_K$ *mit der Eigenschaft:*

$$\forall a, b \in \mathcal{O}_K : ab \in \mathfrak{p} \to (a \in \mathfrak{p} \vee b \in \mathfrak{p}).$$

**Satz 15.** *Ein Ideal* $\mathfrak{p}$ *von* $\mathcal{O}_K$ *ist ein Primideal genau dann, wenn der Faktorring* $\mathcal{O}_K/\mathfrak{p}$ *ein Integritätsring ist.*

Wir machen das Beweis nicht, es geht einfach mit Eigenschaften von Ideale und Primideale.

**Definition 16.** *Ein Ideal* $\mathfrak{m} \subsetneq \mathcal{O}_K$ *heisst Maximalideal, wenn es kein Ideal* $\mathfrak{a}$ *mit* $\mathfrak{m} \subsetneq \mathfrak{a} \subsetneq \mathcal{O}_K$ *gibt.*

**Satz 17.** *Ein Ideal* $\mathfrak{m} \subsetneq \mathcal{O}_K$ *ist maximal genau dann, wenn der Faktorring* $\mathcal{O}_K/\mathfrak{m}$ *ein Körper ist.*

*Beweis.* Wir überprüfen zuerst die Nichtrivialität: $\mathfrak{m} \neq \mathcal{O}_K \Leftrightarrow \mathcal{O}_K/\mathfrak{m} \neq 0$.
Ist $\mathfrak{m}$ maximal, sei $x + \mathfrak{m} \in (\mathcal{O}_K/\mathfrak{m})\backslash\{0\}$, dies bedeutet $x \notin \mathfrak{m}$. Dann ist $\mathfrak{m} \subsetneq \mathfrak{m} + (x) \subseteq \mathcal{O}_K$. Die Maximalität impliziert dann, dass das letzte Symbol der obige Gleichung eine Gleichheit ist. Somit ist $1 \in \mathfrak{m} + (x)$. So folgt, dass $\exists n \in \mathfrak{m}, b \in \mathcal{O}_K : n + bx = 1$, das impliziert $bx + \mathfrak{m} = 1 + \mathfrak{m}$. Somit ist $x + \mathfrak{m}$ in $\mathcal{O}_K/\mathfrak{m}$ invertierbar. Somit ist $\mathcal{O}_K/\mathfrak{m}$ ein Körper.
Umgekehrt ist $\mathcal{O}_K/\mathfrak{m}$ ein Körper, betrachten wir $\mathfrak{m} \subsetneq \mathfrak{a} \subseteq \mathcal{O}_K$. Wie sollten prüfen, dass $\mathfrak{a} = \mathcal{O}_K$. Wähle $x \in \mathfrak{a}\backslash\mathfrak{m}$, dann folgt $0 \neq x + \mathfrak{m} \in \mathcal{O}_K/\mathfrak{m}$. Dann existiert $b \in \mathcal{O}_K : (b + \mathfrak{m})(x + \mathfrak{m}) = 1 + \mathfrak{m}$. Dann ist $1 \in bx + \mathfrak{m} \subseteq \mathfrak{a}$. Dies impliziert $1 \in \mathfrak{a}$, das Äquivalent ist zu sagen $\mathfrak{a} = \mathcal{O}_K$. □

**Korollar 18.** *Jedes maximales Ideal ist ein Primideal.*

*Beweis.* Sei $\mathfrak{m}$ maximal. Dann ist $\mathcal{O}_K/\mathfrak{m}$ ein Körper, und ausserdem ein Integritätsring. Deswegen ist $\mathfrak{m}$ ein Primideal. □

## 5. Beispiel

Jetzt gehen wir weiter mit der vorherige Beispiel, wir wollen diesesmal eine eindeutige Primfaktorisierung mit Ideale finden. Um das zu machen brauchen wir das folgende Theorem.

**Theorem 19.** *Jedes von* (0) *und* (1) *verschiedene Ideal* $\mathfrak{a} \subset \mathcal{O}_K$ *hat eine bis auf Reihenfolge der Faktoren eindeutige Zerlegung in ein Produkt von Primidealen*

$$\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_n.$$

Das Beweis dieses Theorem kommt später im Seminar.
Somit können wir jedes ganze Ideal $\mathfrak{a} \neq (0)$ eindeutig in der Form

$$\mathfrak{a} = \prod_{\mathfrak{p}\ Primideal} \mathfrak{p}^{e_\mathfrak{p}}$$

schreiben. Die Exponenten $e_\mathfrak{p}$ sind nicht negative ganze Zahlen und es gilt $e_\mathfrak{p} = 0$ für alle bis auf endliche viele $\mathfrak{p}$.

Das Ideal (2) ist nicht ein Primideal. Wir können diese Ideal mit Hilfe des vorheriges Theorem in Primideale faktorisieren. Wir erhalten:

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

Wir setzen $\mathfrak{p} := (2, 1 + \sqrt{-5})$. Um zu zeigen, dass $\mathfrak{p}$ Primideal ist, benutzen wir die vorherige Sektion über Faktorringe. Wir zeigen, dass $\mathbb{Z}[\sqrt{-5}]/\mathfrak{p}$ ein Körper ist.
Wir haben die folgende Isomorphismus:

$$\mathbb{Z}[\sqrt{-5}] \cong \mathbb{Z}[X]/(X^2 + 5)$$

das heisst isomorph zur Polynomring $\mathbb{Z}[X]$ modulo das Ideal $(X^2 + 5)$. Aus selben Grunden gilt das folgende Isomorphismus:

$$\mathbb{Z}[\sqrt{-5}]/\mathfrak{p} \cong \mathbb{Z}[X]/(X^2 + 5, 2, 1 + X) \cong \mathbb{Z}/2\mathbb{Z}.$$

Das letzte ist ein klarerweise ein Körper mit genau zwei Elementen. Somit haben wir bewiesen dass $\mathfrak{p}$ ein Primideal ist (mit der Hilfe der obigen Sätze). Ähnlicher zeigen wir, dass $(3, 1 \pm \sqrt{-5})$ Primideale sind.

Wir machen dasselbe Prozess auch für die andere Fälle und wie erhalten das folgende:

$$(3) = (3, 1 + \sqrt{-5}) \cdot (3, 1 - \sqrt{-5})$$

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

$$(1 - \sqrt{-5}) = (2, 1 - \sqrt{-5}) \cdot (3, 1 - \sqrt{-5})$$

Somit erhalten wir

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

wobei wir haben die folgende Eigenschaft benutzt: $(2, 1 + \sqrt{-5}) = (2, 1 - \sqrt{-5})$.
Wir haben somit eine eindeutige Zerlegung in Primidealen erhalten.

## 6. Das Zerlegungsgesetz

In diesen Kapitel brauchen wir die folgende Unterschied, wir bezeichnen mit $n\mathbb{Z}$ das von $n$ erzeugte Hauptideal in $\mathbb{Z}$, und mit $n\mathcal{O}_K$ das von n in $\mathcal{O}_K$ erzeugte Hauptideal.

**Lemma 20.** *Für $n \in \mathbb{Z}$ gilt*

$$n\mathcal{O}_K \cap \mathbb{Z} = n\mathbb{Z}.$$

*Insbesondere gilt für $n, m \in \mathbb{Z}$ : $n\mathcal{O}_K = m\mathcal{O}_K \Leftrightarrow n\mathbb{Z} = m\mathbb{Z}$.*

Um das Lemma zu beweisen brauchen wir eine vorherige Satz, die wir ohne Beweis geben.

**Satz 21.** *Eine rationale Zahl ist genau dann ganz-algebraisch, wenn sie in $\mathbb{Z}$ liegt.*

*Beweis.* Für $n = 0$ ist die aussage trivial. Sei $n \neq 0$. Die Inklusion $n\mathbb{Z} \subset n\mathcal{O}_K \cap \mathbb{Z}$ ist offensichtlich. Für ein beliebig gewähltes Element $a \in n\mathcal{O}_K \cap \mathbb{Z}$ existiert nach Definition ein $x \in \mathcal{O}_K$ mit $a = nx$. Nun liegt $x = a/n$ in $\mathbb{Q}$. Somit ist $x$ eine ganz algebraische rationale Zahl, und daher folgt $x \in \mathbb{Z}$, und daher gilt $a \in n\mathbb{Z}$. □

**Definition 22.** *Eine Primzahl $p$ heisst in $K$*

- *träge, wenn $p\mathcal{O}_K$ ein Primideal ist,*
- *zerlegt, wenn $p\mathcal{O}_K = \mathfrak{p}_1 \cdot \mathfrak{p}_2$ mit Primidealen $\mathfrak{p}_1 \neq \mathfrak{p}_2$ in $\mathcal{O}_K$,*
- *verzweigt, wenn $p\mathcal{O}_K = \mathfrak{p}^2$ für ein Primideal $\mathfrak{p}$ in $\mathcal{O}_K$.*

Wir erinnern dass $(1, w)$ Ganzheitsbasis des Ringes $\mathcal{O}_K$. Das heisst $w = \sqrt{d}$ wenn $d \not\equiv 1 \, mod \, 4$, und $w = (1 + \sqrt{d})/2$ wenn $d \equiv 1 \, mod \, 4$ ist.

Sei nun $f_w$ das Minimalpolynom von $w$, das heisst

$$f_w(X) = \begin{cases} X^2 - d, & wenn \, d \not\equiv 1 \, mod \, 4, \\ X^2 - X - \frac{d-1}{4}, & wenn \, d \equiv 1 \, mod \, 4. \end{cases}$$

**Satz 23.** *Eine Primzahl $p$ heisst in $K$*

- *träge, wenn $f_w$ irreduzibel modulo $p$ ist,*
- *zerlegt, wenn $f_w$ modulo $p$ in zwei verschiedene Linearfaktoren zerfällt,*
- *verzweigt, wenn $f_w$ modulo $p$ eine doppelte Nullstelle hat.*

*Beweis.* Sei $f \in \mathbb{Z}[X]$ so dass $\bar{f}$ ein Primteiler von $\bar{f}_w$ in $\mathbb{Z}/p\mathbb{Z}[X]$ ist. Wir betrachten das ganze Ideal $\mathfrak{p} = p\mathcal{O}_K + f(w)\mathcal{O}_K$.
Behaupthung: $\mathfrak{p} \neq \mathcal{O}_K$.
Beweis: Anderenfalls wäre $1 \in p\mathcal{O}_K + f(w)\mathcal{O}_K$, d.h es gäbe $x, y \in \mathcal{O}_K$ mit $xp + yf(w) = 1$. Sei $g \in \mathbb{Z}[X]$ ein lineares Polynom mit $x = g(w)$ und sei $h \in \mathbb{Z}[X]$ ein lineares Polynom mit $y = h(w)$. Die Polynome $g$ und $h$ existieren, weil $(1, w)$ eine Ganzbasis ist. Dann gilt

$$g(w)p + h(w)f(w) - 1 = 0.$$

Daher gilt

$$f_w | (gp + hf - 1),$$

und modulo $p$ betrachtet erhalten wir: $\bar{f}|\bar{f}_w|(\bar{h}\bar{f} - \bar{1})$. Also gilt $\bar{f}|\bar{1}$ in $\mathbb{Z}/p\mathbb{Z}[X]$, im Widerspruch dazu, dass $\bar{f}$ ein Primpolynom ist. Also ist $p$ ein echtes Ideal.
Behauptung: $\mathfrak{p}$ ist ein Primideal.
Beweis: Seien $x, y \in \mathcal{O}_K$ mit $xy \in \mathfrak{p}$. Es existieren (lineare) Polynome $F, G \in \mathbb{Z}[X]$ mit $x = F(w), y = G(w)$. Wäre $(\bar{f}, \bar{F}\bar{G}) = 1 \in \mathbb{Z}/p\mathbb{Z}[X]$, so gäbe es Polynome $h, g \in \mathbb{Z}[X]$ mit $\bar{h}\bar{f} + \bar{g}\bar{F}\bar{G} = 1$. Hieraus folgt

$$1 \equiv h(w)f(w) + g(w)F(w)G(w) \ \ mod \, p\mathcal{O}_K.$$

Wegen $p\mathcal{O}_K \subset \mathfrak{p}, f(w) \in \mathfrak{p}$ und $F(w)G(w) = xy \in \mathfrak{p}$ erhalten wir den Widerspruch $1 \in \mathfrak{p}$. Damit wird $\bar{f}$ von einem der beiden Primpolynome $\bar{F}$ oder $\bar{G}$ geteilt. Je nachdem folgt $x \in \mathfrak{p}$ oder $y \in \mathfrak{p}$. Also ist $\mathfrak{p}$ ein Primideal.
Nehmen wir nun an, dass $f_w$ modulo $p$ irreduzibel ist. Dann können wir $f = f_w$ setzen und es gilt $0 = f(w)$, folglich $\mathfrak{p} = p\mathcal{O}_K$.
Zerfällt $f_w$ modulo $p$ in die Linearfaktoren $\bar{f}_1$ und $\bar{f}_2$, dann gilt

$$0 = f_w(w) \equiv f_1(w)f_2(w) \, mod \, p\mathcal{O}_K.$$

Bilden wir die Primideale $\mathfrak{p}_1, \mathfrak{p}_2$ wie oben, so folgt, dass

$$\mathfrak{p}_1\mathfrak{p}_2 = p^2\mathcal{O}_K + pf_1(w)\mathcal{O}_K + pf_2(w)\mathcal{O}_K + f_1(w)f_2(w)\mathcal{O}_K \subset p\mathcal{O}_K.$$

Daher gilt $p\mathcal{O}_K|\mathfrak{p}_1\mathfrak{p}_2$ und es verbleiben die Möglichkeiten $p\mathcal{O}_K = \mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_1\mathfrak{p}_2$.
Wäre $p\mathcal{O}_K = \mathfrak{p}_1$, so wäre $f_1(w) \in p\mathcal{O}_K$. Also existiert ein Polynom $g \in \mathbb{Z}[X]$ mit $f_1(w) = pg(w)$. Es folgt $f_w|(f_1 - pg)$ und modulo $p$ erhalten wir den Widerspruch $\bar{f}_w|\bar{f}_1$. Analog schließen wir die Möglichkeit $p\mathcal{O}_K = \mathfrak{p}_2$ aus und erhalten

$$p\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2.$$

Hat $f_w$ modulo $p$ eine Doppelnullstelle, so könnenn wir $f_1 = f_2$ wählen und erhalten $\mathfrak{p}_1 = \mathfrak{p}_2$. Es bleibt zu zeigen, dass $\bar{f}_1 \neq \bar{f}_2$ auch $\mathfrak{p}_1 \neq \mathfrak{p}_2$ impliziert. Dies folgt aus der linearen Kombinierbarkeit des grössten gemeinsamen Teilers. Wir wählen Polynome $g, h \in \mathbb{Z}[X]$ mit $\bar{f}_1\bar{g} + \bar{f}_2\bar{h} = 1 \in \mathbb{Z}/p\mathbb{Z}[X]$. Dann gibt es ein Polynom $F \in \mathbb{Z}[X]$ mit $f_1g + f_2h - pF = 1$. Einsetzen von $w$ ergibt

$$f_1(w)g(w) + f_2(w)h(w) - pF(w) = 1.$$

Wäre nun $\mathfrak{p}_1 = \mathfrak{p}_2$, so wäre der Ausdruck auf der linken Seite in $\mathfrak{p}_1$ und wir erhalten einen Widerspruch. □

**Definition 24.** *Die Zahl*

$$\Delta_K = \left|\begin{pmatrix} 1 & w \\ 1 & \sigma(w) \end{pmatrix}\right|^2 = \begin{cases} 4d, & \text{wenn } d \not\equiv 1 \bmod 4, \\ d, & \text{wenn } d \equiv 1 \bmod 4. \end{cases}$$

*Heisst die Diskriminante des quadratisches Zahlkörpers $K$.*

**Satz 25.** *Eine Primzahl $p$ ist genau dann in $K$ verzweigt, wenn sie die Diskriminante $\Delta_K$ von $K$ teilt.*

*Beweis.* Angenommen, die Primzahl $p$ ist verzweigt in $\mathcal{O}_K$, das heisst $p\mathcal{O}_K = \mathfrak{p}^2$. Dann gilt $\sigma(\mathfrak{p})^2 = \sigma(p)\mathcal{O}_K = p\mathcal{O}_K = \mathfrak{p}^2$. Wegen der Eindeutigkeit der Primidealzerlegung folgt $\mathfrak{p} = \sigma(\mathfrak{p})$. Angenommen, für jedes $a + bw \in \mathfrak{p}$, wäre $b \in p\mathbb{Z}$. Dann wäre jedes auftretende $a \in \mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$. Hieraus würde $\mathfrak{p} = p\mathcal{O}_K$ folgen. Also findet man $a, b \in \mathbb{Z}, 0 < b < p$ mit $a + bw \in \mathfrak{p}$. Wegen $\mathfrak{p} = \sigma(\mathfrak{p})$ ist auch $a + b\sigma(w) \in \mathfrak{p}$. Wir schliessen $b(w - \sigma(w)) \in \mathfrak{p}$ und $b^2\Delta_K \in \mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$. Wegen $0 < b < p$ folgt $p|\Delta_K$.
Sei umgekehrt $\Delta_K$ durch $p$ teilbar. Wir betrachten zunächst den Fall $d \not\equiv 1 \bmod 4$. Dann gilt $f_w = X^2 - d$. Für ungerades $p$ folgt aus $p|\Delta_K$ auch $p|d$ und $f_w$ hat modulo $p$ eine doppelte Nullstelle. Modulo 2 hat $X^2 - d$ für ungerades $d$ die Doppelnullstelle 1 und für geardes $d$ die Doppelnullstelle 0. Nun betrachten wir den Fall $d \equiv 1 \bmod 4$. Dann gilt $\Delta_K = d$ und $f_w = X^2 - X - \frac{d-1}{4}$. Ein Diskriminantenteiler $p$ ist notwendig ungerade und modulo $p$ gilt $f_w = (X - 1/2)^2$. □

**Korollar 26.** *Mindestens eine und höchstens endlich viele Primzahlen verzweigen in $K$.*

*Beweis.* Folgt direkt von obige Satz und daraus dass der Betrag von $\Delta_K$ stets grösser als 1 ist. □

**Theorem 27.** *Sei $K = \mathbb{Q}(\sqrt{d})$ ein quadratischer Zahlkörper mit Diskriminante $\Delta_K$. Dann gilt:*

*(1) Eine ungerade Primzahl $p$ heisst in $K$*
- *träge, wenn $(\frac{\Delta_K}{p}) = -1$,*
- *zerlegt, wenn $(\frac{\Delta_K}{p}) = +1$,*
- *verzweigt, wenn $(\frac{\Delta_K}{p}) = 0$.*

*(2) Die Primzahl 2 ist in $K$*
- *träge, wenn $\Delta_K \equiv 5 \bmod 8$,*
- *zerlegt, wenn $\Delta_K \equiv 1 \bmod 8$,*
- *verzweigt, wenn $\Delta_K \equiv 0 \bmod 2$.*

*Beweis.* Sei $p$ ungerade. Ist $d \not\equiv 1 \bmod 4$, so ist das Minimalpolynom $f_w = X^2 - d$ genau dann, irreduzibel modulo $p$, wenn $d$ kein quadratischer Rest modulo $p$ ist. Wenn $d \equiv 1 \bmod 4$ ist, so gilt $f_w = X^2 - X - \frac{d-1}{4}$. Die Substitution $f_w(X + 1/2) = X^2 - d/4$ zeigt dann das gleiche Ergebnis. Nun betrachten wir den Fall $p = 2$. Ist $d \not\equiv 1 \bmod 4$, so ist $\Delta_K = 4d$ gerade und 2 ist verzweigt. Sei $\Delta_K = d \equiv 1 \bmod 4$. Dann ist $f_w$ genau dann irreduzibel modulo 2, wenn $(d - 1)/4$ ungerade ist. □

## References

[1] A. Schmidt, Einführung in die algebraische Zahlentheorie. Springer, Berlin, 2007

*Email address*: sabringa@student.ethz.ch