Quadratische Zahlkörper

Clara Nadenau

15.10.2010

Inhaltsverzeichnis

Kapitel 1

Einleitung

Ein algebraischer Zahlkörper ist ein endlicher Erweiterungskörper E von $\mathbb{Q}$, also $[E : \mathbb{Q}] < \infty$. Als Verallgemeinerung der Beziehung zwischen den ganzen Zahlen $\mathbb{Z}$ und den rationalen Zahlen $\mathbb{Q}$ definiert man den Ganzheitsring eines Zahlkörpers.
Wir werden hauptsächlich quadratische Zahlkörper, also Zahlkörper E mit $[E : \mathbb{Q}] = 2$, behandeln. Man unterscheidet reell- und imaginär-quadratische Zahlkörper. Als Erstes werden wir den Ganzheitsring eines quadratischen Zahlkörpers bestimmen. Dann werden wir dessen Einheiten charakterisieren. Im Falle imaginär-quadratischer Zahlkörper kann man diese Einheiten konkret benennen. Um die Einheiten des Ganzheitsringes eines reell-quadratischen Zahlkörpers zu bestimmen, werden Kettenbrüche eingeführt, mit deren Hilfe man eine „Grundeinheit“ berechnen kann. Mit dieser Grundeinheit kann man nun alle weiteren Einheiten multiplikativ erzeugen.

Die Verallgemeinerung dieses Ergebnises ist der auf Dirichlet (1805-1859) zurückgehende Einheitensatz.

Die meisten Aussagen und Beweise dieser Ausarbeitung stammen aus Koch: Zahlentheorie, algebraische Zahlen und Funktionen ([Koc97]).

Kapitel 2

Ganze Zahlen in quadratischen Zahlkörpern

Als Erstes werden wir einige grundlegende Begriffe definieren, die speziell in diesem Kapitel, aber auch später immer wieder nützlich sind.

2.1 Definition (quadratischer Zahlkörper)
Einen Körper der Form $E := \mathbb{Q}[\sqrt{d}] = \mathbb{Q}(\sqrt{d}) = \{u + v\sqrt{d} | u, v \in \mathbb{Q}\}$ mit $d \in \mathbb{Z}$ quadratfrei nennt man einen *quadratischen Zahlkörper*.
E ist *imaginär-quadratisch* falls $d < 0$ und *reell-quadratisch* falls $d > 0$.
Ein Element $a \notin \mathbb{Q}$ aus einem reell-quadratischen Zahlkörper nennt man *quadratische Irrationalzahl*.

Die folgenden Definitionen sind analog zu denen in den komplexen Zahlen:

2.2 Definition (konjugiertes Element, Norm, Spur)
Sei $E = \mathbb{Q}[\sqrt{d}]$ ein quadratischer Zahlkörper und

$$\sigma : \ E \to E, \quad (u + v\sqrt{d}) \mapsto (u - v\sqrt{d}) \, ,$$

so heißt $\sigma(a)$ das *konjugierte Element* von a in $\mathbb{Q}[\sqrt{d}]$. Seien

$$\mathcal{N} : \ E \to \mathbb{Q}, \quad (u + v\sqrt{d}) \mapsto (u + v\sqrt{d})(u - v\sqrt{d}) = u^2 - v^2 d$$

und

$$\mathcal{S} : \ E \to \mathbb{Q}, \quad (u + v\sqrt{d}) \mapsto (u + v\sqrt{d}) + (u - v\sqrt{d}) = 2u \, ,$$

dann heißen $\mathcal{N}(a)$ die *Norm* und $\mathcal{S}(a)$ die *Spur* von a in $\mathbb{Q}[\sqrt{d}]$.

2.3 Bemerkung
1. Die Konjugation σ ist ein Automorphismus.

2. Die Norm $\mathcal{N}$ ist als Produkt von zwei Homomorphismen (Identität und Konjugation) multiplikativ, d.h. $\mathcal{N}(a \cdot b) = \mathcal{N}(a) \cdot \mathcal{N}(b)$.

3. In imaginär-quadratischen Zahlkörpern gilt $\mathcal{N}(a) > 0$ für alle $a \in \mathbb{Q}[\sqrt{d}] \setminus \{0\}$.

2.4 Bemerkung
$B(x, y) := \frac{1}{2}\mathcal{S}(x \cdot \sigma(y))$ ist eine Bilinearform auf $E \cong \mathbb{Q}^2$.
Dabei ist $B(x, x) = \frac{1}{2}\mathcal{S}(x \cdot \sigma(x)) = \mathcal{N}(x)$ die zugehörige Norm; dies entspricht der in der Linearen Algebra definierten Norm.

2.5 Definition (Körpererweiterung)
Sind K, E Körper, so dass K ein Teilring von E ist, so heißt E ein Erweiterungskörper von K und K ein Teilkörper von E und E/K eine *Körpererweiterung*.

2.6 Bemerkung
Hier wird $K := \mathbb{Q}$ und $E := \mathbb{Q}[\sqrt{d}]$ mit $d \in \mathbb{Z}$ quadratfrei, d.h. $d = p_1, ..., p_n$ mit $p_i \in \mathbb{P}$ paarweise verschieden und $n \in \mathbb{N}$ betrachtet.

2.7 Definition (algebraisch)
Es sei E/K eine Körpererweiterung.
Ein Element $a \in E$ heißt *algebraisch* über K, wenn ein Polynom $0 \neq P \in K[X]$ existiert mit $P(a) = 0$.

2.8 Definition (ganze Zahlen)
Sei E/K (hier: $\mathbb{Q}[\sqrt{d}]/\mathbb{Q}$) eine Körpererweiterung und Γ (hier: $\mathbb{Z}$) ein Ring mit $\mathrm{Quot}(\Gamma) = K$.
$a \in E$ heißt *ganz* bezüglich Γ, wenn ein normiertes $P \in \Gamma[X]$ existiert, so dass $P(a) = 0$ gilt.

Wir nennen hier $\mathcal{O}_E := \{a \in E \mid \text{a ist ganz bezüglich } \Gamma\}$ den ganzen Abschluss von Γ in E.

2.9 Satz
$\mathcal{O}_E$, der ganze Abschluss von Γ in E, ist ein Ring. Er wird auch Ganzheitsring genannt.

Um diesen Satz zu zeigen, benötigen wir eine Folgerung aus dem Laplacschen Entwicklungssatz zur Berechnung von Determinanten:

2.10 Satz (Laplacescher Entwicklungssatz)
Sei $A = (a_{ij})$ eine $(r \times r)$-Matrix über einem kommutativen Ring R mit Eins und $A^* = (a^*_{ij})$ die adjungierte Matrix, d.h. $a^*_{ij} = (-1)^{i+j} \det(A_{ij})$, wobei A_{ij} aus A durch Herausstreichen der i-ten Zeile und der j-ten Spalte entsteht. Dann gilt

$$AA^* = A^*A = \det(A)E\,,$$

wobei E die Einheitsmatrix vom Grad r ist.

2.11 Folgerung
Sei A wie in Satz 2.10 und $x \in R^n$ ein Vektor. Dann gilt:

$$Ax = 0 \quad \Rightarrow \quad (\det(A))x = 0\,.$$

Beweis:

$$\begin{aligned} & Ax = 0 \quad \Rightarrow \quad A^*Ax = 0 \quad \Rightarrow \quad \det(A)Ex = 0 \\ \Rightarrow \quad & \det(A)x = 0\,. \end{aligned}$$

□

Damit können wir den folgenden Satz beweisen, aus dem wiederum wir Satz 2.9 folgern:

2.12 Satz
Sei E/K eine Körpererweiterung. Endlich viele Elemente $a_1, \ldots, a_n \in E$ sind genau dann ganz über $\Gamma \subset K$, wenn $\Gamma[a_1, \ldots, a_n] \subseteq E$ endlich erzeugt ist.

Beweis:
„⇒“ : Mit vollständiger Induktion:

IA: $n = 0$:
Sei $a \in E$ ganz. Dann gibt es ein normiertes $f(X) \in \Gamma[X]$ vom Grad $k \in \mathbb{N}$ mit $f(a) = 0$. Sei weiter $g(X) \in \Gamma[X]$ beliebig. Dann gibt es $q(X), r(X) \in \Gamma[X]$, $r(X) = \sum_{i=0}^{k-1} b_i X^i$ und $\deg(r(X)) < k$, so dass

$$g(X) = q(X) \cdot f(X) + r(X)\,,$$

dann ist

$$g(a) = 0 + r(a) = \sum_{i=0}^{k-1} b_i a^i\,.$$

Also wird jedes $g(a) \in \Gamma[a]$ von $1, a, a^2, \ldots, a^{k-1}$ erzeugt.

IS: $n \to n{+}1$: Sei $R := \Gamma[a_1, \ldots, a_n]$. Dann ist $\Gamma[a_1, \ldots, a_n, a_{n+1}] = R[a_{n+1}]$ und wir können wie oben zeigen, dass es endlich erzeugt ist.

„⇒“ : Sei $\Gamma[a_1, \ldots, a_n]$ als Γ-Modul endlich erzeugt und $w_1, \ldots w_k$ ein Erzeugendensystem. Ist nun $b \in \Gamma[a_1, \ldots, a_n]$ beliebig, dann gibt es für $i, j \in \{1, \ldots, k\}$ $c_{ij} \in \Gamma$, so dass

$$bw_i = \sum_{j=1}^{r} c_{ij} w_j \quad \text{für } i = 1, \ldots, k$$

$$\Rightarrow \quad 0 = bw_i - \sum_{j=1}^{r} c_{ij} w_j$$

also

$$0 = \begin{pmatrix} (b-c_{11})w_1 - c_{12}w_2 - c_{13}w_3 - \ldots - c_{1k}w_k \\ -c_{11}w_1 + (b-c_{12})w_2 - c_{13}w_3 - \ldots - c_{1k}w_k \\ \ddots \\ -c_{11}w_1 - c_{12}w_2 - c_{13}w_3 - \ldots + (b-c_{1k})w_k \end{pmatrix} = (bE - (c_{ij}))w\,,$$

wobei E die Einheitsmatrix und $w = (w_1, \ldots, w_k)^{tr}$ ist. Nun gilt mit Folgerung 2.11

$$\det(bE - (c_{ij}))w = 0 \quad \Rightarrow \quad \det(bE - (c_{ij})) = 0\,.$$

Damit ist $h(x) := \det(xE - (c_{ij}))$ normiert und es gilt $h(b) = 0$. Deshalb folgt, dass b ganz in Γ ist. □

Beweis: (von Satz 2.9)
Es reicht zu zeigen, dass $\mathcal{O}_E$ abgeschlossen bezüglich Addition und Multiplikation ist:
Seien $a, b \in \mathcal{O}_E$. Dann wissen wir aus Satz 2.12, dass $\Gamma[a, b]$ endlich erzeugt ist.
Da $a + b$ und $a \cdot b$ in $\Gamma[a, b]$ liegen, ist $\Gamma[a, b] = \Gamma[a, b, a + b] = \Gamma[a, b, a \cdot b]$ und $a + b$ sowie $a \cdot b$ sind ganz. □

2.13 Definition (Minimalpolynom)
Sei E/K eine Körpererweiterung und $a \in E$ algebraisch über K. Ein normiertes Polynom $\mu_a \in K[X]$ von minimalem Grad, für das gilt $\mu_a(a) = 0$, nennt man *Minimalpolynom* von a.

2.14 Lemma
Das Minimalpolynom von $a \in E$ ist irreduzibel und eindeutig. Weiter teilt es jedes andere $P \in K[X]$ mit $P(a) = 0$.

Beweis:
Die Abbildung

$$\varphi_a :\ K[X] \to E, \quad p(X) \mapsto p(a)$$

ist ein Homomorphismus. Also ist das Bild $\varphi_a(K[X])$ und damit auch $K[X]/\text{Kern}(\varphi_a)$ ein Integritätsbereich, damit ist $\text{Kern}(\varphi_a)$ ein Primideal (Bem 2.12, [Neb10]).

Weiter ist $\text{Kern}(\varphi_a)$ ein Hauptideal, da K[X] ein Hauptidealbereich ist (A2, [Neb10]).
Daher gilt $\langle \mu_a(X) \rangle = \text{Kern}(\varphi_a)$. Wäre nämlich $\mu_a(a) = 0$ und es gäbe ein $p(X) \in K[X]$, so dass $p(X)$ nicht in $\langle \mu_a(X) \rangle$ liegt, dann wäre das ein Widerspruch dazu, dass μ_a minimalen Grad hat.
Also ist $\langle \mu_a(X) \rangle$ ein Primideal und damit $\mu_a(X)$ irreduzibel.
Die Eindeutigkeit folgt, da das Minimalpolynom Erzeuger eines Hauptideals und normiert ist. □

Nun beginnt die konkrete Charakterisierung des Ganzheitsringes eines quadratischen Zahlkörpers:

2.15 Lemma
$\mathbb{Q}[\sqrt{d}]/\mathbb{Q}$ ist eine algebraische Körpererweiterung, d.h. alle Elemente aus $\mathbb{Q}[\sqrt{d}]$ sind algebraisch bezüglich $\mathbb{Q}$.
Die Minimalpolynome sind gegeben durch $\mu_a(x) = x - a$, falls $a \in \mathbb{Q}$ und durch $\mu_a(x) = x^2 - \mathcal{S}(a)x + \mathcal{N}(a)$, falls $a \in \mathbb{Q}[\sqrt{d}] \setminus \mathbb{Q}$.

Beweis:
Sei $a \in \mathbb{Q}[\sqrt{d}]$. Dann gibt es $u, v \in \mathbb{Q}$ mit $a := u + v\sqrt{d}$.

1.Fall: $v = 0$:

$$\Rightarrow \mu_a(x) = x - u \in \mathbb{Q}[X].$$

2.Fall: $v \neq 0$: Da a irrational ist, muss $\deg(\mu_a(x))$ größer als 1 sein. Sei $P(x) = x^2 - \mathcal{S}(a)x + \mathcal{N}(a)$. Dann gilt

$$\begin{aligned} P(a) &= a^2 - \mathcal{S}(a)a + \mathcal{N}(a) \\ &= a^2 - (a + \sigma(a))a + a\sigma(a) \\ &= a^2 - a^2 - \sigma(a)a + \sigma(a)a = 0 \end{aligned}$$

Also $\mu_a(x) = P(x)$. □

2.16 Bemerkung
Die ganzen Zahlen in $\mathbb{Q}[\sqrt{d}]$ bezüglich $\mathbb{Z}$ sind genau die, deren Minimalpolynom in $\mathbb{Z}[X]$ liegt.

Beweis:
Sei $a \in \mathbb{Q}[\sqrt{d}]$ mit $\mu_a(x) \in \mathbb{Z}[X]$. Dann folgt direkt, dass a ganz ist.

Sei nun $a \in \mathbb{Q}[\sqrt{d}] \setminus \mathbb{Z}$ ganz. Dann gibt es ein $g \in \mathbb{Z}[X], g$ normiert mit $g(a) = 0$.
Wählt man g so, dass es minimalen Grad hat, dann ist g irreduzibel in $\mathbb{Z}$. Also ist es (mit Satz 2.29, [Neb10]) auch irreduzibel in $\mathbb{Q}$ und damit gilt $\mu_a(X) = g(X) \in \mathbb{Z}[X]$. □

2.17 Satz
Die Menge der ganzen Zahlen von $\mathbb{Q}[\sqrt{d}]$ bezüglich $\mathbb{Z}$ ist

$$\mathbb{Z}_{\mathbb{Q}[\sqrt{d}]} := \mathcal{O}_{\mathbb{Q}[\sqrt{d}]} = \begin{cases} \mathbb{Z}[\frac{1+\sqrt{d}}{2}], & \text{falls } d \equiv 1 \pmod 4 \\ \mathbb{Z}[\sqrt{d}], & \text{falls } d \equiv 2 \pmod 4 \text{ oder } d \equiv 3 \pmod 4 \end{cases}.$$

Beweis:
Aus Bemerkung 2.16 folgt $\mathbb{Z} \subset \mathbb{Z}_{\mathbb{Q}[\sqrt{d}]}$.

Sei $w := \sqrt{d}$ falls $d \equiv 2 \pmod 4$ oder $d \equiv 3 \pmod 4$ und sei $w := \frac{1+\sqrt{d}}{2}$ falls $d \equiv 1 \pmod 4$. Sei weiter $a := u + v\sqrt{d} \in \mathbb{Q}[\sqrt{d}]$ mit $v \neq 0$ und $\mu_a(x) = x^2 - \mathcal{S}(a)x + \mathcal{N}(a)$.
a ist genau dann ganz, wenn $\mathcal{S}(a) = 2u \in \mathbb{Z}$ und $\mathcal{N}(a) \in \mathbb{Z}$
$\Rightarrow u \in \frac{1}{2}\mathbb{Z}$ und $\mathcal{N}(a) \in \mathbb{Z}$.

$\mathbb{Z}[w] \subseteq \mathbb{Z}_{\mathbb{Q}[\sqrt{d}]}$: Es gilt $S(w) \in \mathbb{Z}$ und $\mathcal{N}(w) \in \mathbb{Z}$, also folgt $\mathbb{Z}[w] \subseteq \mathbb{Z}_{\mathbb{Q}[\sqrt{d}]}$, da wir aus Satz 2.9, wissen, dass $\mathbb{Z}[\sqrt{d}]$ ein Ring ist.

$\mathbb{Z}[w] \supseteq \mathbb{Z}_{\mathbb{Q}[\sqrt{d}]}$: Sei $a \in \mathbb{Z}_{\mathbb{Q}[\sqrt{d}]}$. Dann gilt $\mathcal{S}(a)$ und $\mathcal{N}(a) \in \mathbb{Z}$. Ist $u \in \mathbb{Z}$, so folgt auch $v \in \mathbb{Z}$, also $a \in \mathbb{Z}[w]$. Sei nun $u \in \frac{1}{2}\mathbb{Z} \setminus \mathbb{Z}$:

$$
\begin{aligned}
& u \in \frac{1}{2}\mathbb{Z} \setminus \mathbb{Z} \quad \Rightarrow \quad u = \frac{\gamma}{2} \quad \text{mit} \quad \gamma \in \mathbb{Z} \quad \text{und} \quad \gamma \not\equiv 0 \pmod 2 \\
& \Rightarrow \quad \gamma^2 \equiv 1 \pmod 4 \\
& \Rightarrow \quad \frac{\gamma^2}{4} - v^2 d \in \mathbb{Z} \\
& \Rightarrow \quad v = \frac{\varepsilon}{2} \quad \text{mit} \quad \varepsilon \in \mathbb{Z} \quad \text{und} \quad \varepsilon^2 d \equiv 1 \pmod 4 \\
& \Rightarrow \quad d \equiv 1 \pmod 4 \quad \text{und} \quad \epsilon \equiv 1 \pmod 2 \\
& \Rightarrow \quad \mathbb{Z}_{\mathbb{Q}[\sqrt{d}]} = \mathbb{Z}[\frac{1+\sqrt{d}}{2}] \,.
\end{aligned}
$$

□

2.18 Beispiel
$d := 21, E := \mathbb{Q}[\sqrt{21}], K := \mathbb{Q}$.
$21 \equiv 1 \pmod 4 \Rightarrow \mathbb{Z}_{\mathbb{Q}[\sqrt{21}]} = \mathbb{Z}[\frac{1+\sqrt{21}}{2}]$
Sei $w := \frac{1+\sqrt{21}}{2}$. Dann ergeben sich folgende Werte:

Element a	Koeffizient zu 1	Koeffizient zu w	$\mu_a(x)$	ganz?
9	9	0	$x - 9$	ja
$\frac{1+\sqrt{21}}{2}$	0	1	$x^2 - x - 5$	ja
$3 - 10\sqrt{21}$	13	-20	$x^2 - 26x - 8321$	ja
$1 + \frac{\sqrt{21}}{2}$	–	–	$x^2 - 2x - \frac{19}{2}$	nein
$\frac{2}{8} + \frac{23\sqrt{21}}{8}$	–	–	$x^2 - \frac{1}{2} - \frac{11105}{64}$	nein

Kapitel 3

Einheiten in quadratischen Zahlkörpern

Vereinbarung: In diesem Kapitel sei immer $d \in \mathbb{Z}$ quadratfrei.

3.1 Satz
$a \in \mathbb{Z}_{\mathbb{Q}[\sqrt{d}]}$ ist genau dann eine Einheit, wenn $\mathcal{N}(a) \in \mathbb{Z}^* = \{-1, 1\}$.

Beweis:
„$\Rightarrow$“: Angenommen $a \in \mathbb{Z}_{\mathbb{Q}[\sqrt{d}]}$ ist eine Einheit. Dann gibt es ein $b \in \mathbb{Z}_{\mathbb{Q}[\sqrt{d}]}$, so dass $ab = 1$.
Dann gilt mit (Bemerkung 2.3): $1 = \mathcal{N}(ab) = \mathcal{N}(a)\mathcal{N}(b)$
$\Rightarrow \mathcal{N}(a), \mathcal{N}(b) \in \mathbb{Z}^* = \{-1, 1\}$.

„$\Leftarrow$“: $\pm 1 = \mathcal{N}(a) = a \cdot \sigma(a) \;\Rightarrow\; a^{-1} = \pm\sigma(a)$. □

3.1 Einheiten in imaginär-quadratischen Zahlkörpern

3.2 Satz
Sei $\mathbb{Q}[\sqrt{d}]$ ein imaginär-quadratischer Zahlkörper, also $d < 0$ und sei $c \in \mathbb{Q}_{>0}$ beliebig, aber fest. Dann gilt:

$$\{a \in \mathcal{O}_{\mathbb{Q}[\sqrt{d}]} \mid \mathcal{N}(a) \leq c\} < \infty.$$

Beweis:
Da $\mathbb{Z}$ diskret und $\mathcal{O}_{\mathbb{Q}[\sqrt{d}]}$ ein endlich erzeugtes $\mathbb{Z}$-Modul ist (vgl. Satz 2.17), ist auch $\mathcal{O}_{\mathbb{Q}[\sqrt{d}]}$ diskret.
Weiter ist $B_{\mathcal{N}\leq c} := \{a \in \mathbb{Q}[\sqrt{d}] \mid \mathcal{N}(a) \leq c\}$ kompakt, weil für $d < 0$ die Norm positiv definit ist.
Deshalb ist

$$\{a \in \mathcal{O}_{\mathbb{Q}[\sqrt{d}]} \mid \mathcal{N}(a) \leq c\} = \mathcal{O}_{\mathbb{Q}[\sqrt{d}]} \cap B_{\mathcal{N}\leq c}$$

endlich. □

Mit diesem Satz folgt schon, dass jeder imaginär-quadratische Zahlkörper nur endlich viele Einheiten haben kann, da die Norm ja beschränkt ist. In reell-quadratischen Zahlkörpern ist dagegen die Norm nicht positiv definit, weshalb wir das Kompaktheitsargument nicht nutzen können.

3.3 Satz
Die Einheiten von einem imaginär-quadratischen Zahlkörper $\mathbb{Z}_{\mathbb{Q}[\sqrt{d}]}$, mit $d < 0$, sind

$$\mathbb{Z}^*_{\mathbb{Q}[\sqrt{d}]} = \begin{cases} \langle i \rangle, & \text{falls } d = -1 \\ \langle w \rangle = \langle \frac{1+\sqrt{d}}{2} \rangle = \{\pm 1\} \cup \{\pm\frac{1}{2} \pm \frac{1}{2}\sqrt{-3}\}, & \text{falls } d = -3 \\ \{\pm 1\}, & \text{falls } d \notin \{-1, -3\} \end{cases} .$$

Beweis:
$d = -1$: Sei $a := u + v\sqrt{-1} \in \mathbb{Z}_{\mathbb{Q}[\sqrt{-1}]}$ eine Einheit. Dann gilt mit (Satz 3.1):
$1 = \mathcal{N}(a) = u^2 + v^2$
$\Rightarrow (u, v) \in \{(0, \pm 1), (\pm 1, 0)\}$
$\Rightarrow a \in \{\pm 1, \pm i\} = \langle i \rangle$.

$d = -3$: Sei $a := y + z\frac{\sqrt{-3}}{2} = \frac{2y+z}{2} + \frac{z\sqrt{-3}}{2} = \frac{u}{2} + \frac{z\sqrt{-3}}{2} \in \mathbb{Z}_{\mathbb{Q}[\sqrt{-3}]}$ mit $y, z \in \mathbb{Z}$ und $u = (2y + z) \in \mathbb{Z}$ eine Einheit.

Dann gilt:
$1 = \mathcal{N}(a) = \mathcal{N}(\frac{1}{2})\mathcal{N}(u + z\sqrt{-3}) = \frac{1}{4}(u^2 + 3z^2)$
$\Rightarrow u^2 + 3z^2 = 4$
$\Rightarrow (u \in \{\pm 1\}$ und $z \in \{\pm 1\})$ oder $(u \in \{\pm 2\}$ und $z = 0)$
$\Rightarrow a = \pm\frac{1}{2} \pm \frac{\sqrt{-3}}{2}$ oder $a = \pm 1$.

$d \notin \{-1, -3\}$: *1. Fall:* $d \equiv 2, 3 \pmod 4$: $\Rightarrow \mathbb{Z}_{\mathbb{Q}[\sqrt{d}]} = \mathbb{Z} \oplus \mathbb{Z}\sqrt{d}$.
Sei nun $a \in \mathbb{Z}_{\mathbb{Q}[\sqrt{d}]}$, dann gibt es $u, v \in \mathbb{Z}$ mit $a = u + v\sqrt{d}$.
Ist a eine Einheit, so gilt $\mathcal{N}(a) = u^2 - v^2 d = 1 \overset{d \leq -1}{\Rightarrow} u \in \{\pm 1\}$ und $v = 0$
$\Rightarrow a \in \{\pm 1\}$.

2. Fall: $d \equiv 1 \pmod 4$: $\Rightarrow \mathbb{Z}_{\mathbb{Q}[\sqrt{d}]} = \mathbb{Z} \oplus \mathbb{Z}\frac{1+\sqrt{d}}{2}$.
Sei k so, dass $-d = -4k - 1$ mit $k \in \mathbb{N}$. Sei $a \in \mathbb{Z}_{\mathbb{Q}[\sqrt{d}]}$ eine Einheit. Dann gibt es $r, s \in \mathbb{Z}$ mit $a = r + s\frac{1+\sqrt{d}}{2} = \frac{2r+s}{2} + \frac{s\sqrt{d}}{2}$.
Setze $u := 2r + s$.
$\Rightarrow 1 = \mathcal{N}(a) = \frac{u^2 - s^2 d}{4} = \frac{u^2 + s^2(4k+1)}{4} \overset{k \geq 0}{\Rightarrow} u \in \{\pm 2\}, s = 0$.
$\Rightarrow a \in \{\pm 1\}$. □

3.4 Folgerung
Die Einheiten des Ganzheitsrings eines imaginär-quadratischen Zahlkörpers sind genau die Einheitswurzeln, d.h.

$$a \in \mathbb{Z}^*_{\mathbb{Q}[\sqrt{d}]} \quad \Leftrightarrow \quad \exists n \in \mathbb{N} : a^n = 1 \,.$$

Beweis:
„⇒“: Folgt aus Satz 3.3.

„⇐“: Sei $a \in \mathbb{Z}_{\mathbb{Q}[\sqrt{d}]}$ eine Einheitswurzel. Dann gibt es ein $n \in \mathbb{N}$, so dass $a^n = 1$.
Deshalb ist $1 = \mathcal{N}(a^n) = \mathcal{N}(a)^n$ und damit gilt $\mathcal{N}(a) = 1$. □

3.2 Einheiten in reell-quadratischen Zahlkörpern

3.5 Definition (reduziert)
Eine Zahl $\lambda > 1$ in einem reell-quadratischen Zahlkörper heißt *reduziert*, wenn $-\frac{1}{\sigma(\lambda)} > 1$ ist.

3.6 Lemma
Sei $\lambda \in \mathbb{Q}[\sqrt{d}]$ mit $d > 0$ eine quadratische Irrationalzahl.
Dann gibt es $\alpha, \beta, \gamma \in \mathbb{Z}$ mit $\mathrm{ggT}(\alpha, \beta, \gamma) = 1$ und $\alpha > 0$, so dass gilt

$$\alpha\lambda^2 - \beta\lambda - \gamma = 0 \,.$$

3.7 Lemma
Ist umgekehrt $\lambda \in \mathbb{R} \setminus \mathbb{Q}$ eine Lösung einer quadratischen Gleichung

$$\alpha\lambda^2 - \beta\lambda - \gamma = 0 \,,$$

so ist λ Element aus einem reell-quadratischen Zahlkörper.

Beweis:
Mit der p,q-Formel gilt: $\lambda \in \left\{ \frac{\beta}{2\alpha} \pm \sqrt{\frac{\beta^2}{4\alpha^2} + \frac{\gamma}{\alpha}} \right\}$.
Da $\lambda \in \mathbb{R} \setminus \mathbb{Q}$ ist, wissen wir, dass der Term unter der Wurzel größer 0 ist, daher gibt es ein $d \in \mathbb{N}$, $d > 1$ quadratfrei und ein $g \in \mathbb{Q}$, so dass $\lambda \in \left\{ \frac{\beta}{2\alpha} \pm g\sqrt{d} \right\}$. □

Beweis:
Da λ nicht in $\mathbb{Q}$ liegt, gilt für das Minimalpolynom $\mu_a(X)$ von a: $\deg(\mu_a(X)) = 2$.
Multipliziere $\mu_a(X)$ noch mit einer geeigneten Zahl aus $\mathbb{Q}$, so dass alle Koeffizienten aus $\mathbb{Z}$ sind und ihr größter gemeinsamer Teiler Eins ist, dann folgt die Behauptung. □

3.8 Definition (Diskriminante)
Sei $\lambda \in \mathbb{Q}[\sqrt{d}]$ mit $d > 0$ eine quadratische Irrationalzahl.
Gemäß Lemma 3.6 gibt es dann $\alpha, \beta, \gamma \in \mathbb{Z}$ mit $\mathrm{ggT}(\alpha, \beta, \gamma) = 1$ und $\alpha > 0$, so dass gilt

$$\alpha\lambda^2 - \beta\lambda - \gamma = 0\,.$$

Die Diskriminante $D := \beta^2 + 4\alpha\gamma$ dieser quadratischen Gleichung nennt man *Diskriminante* von λ.

3.2.1 Kettenbrüche

Die Kettenbruchentwicklung dient hier als Hilfsmittel, um die Grundeinheit zu konstruieren.

3.9 Definition
Die Kettenbruchentwicklung von $\alpha \in \mathbb{R}$ hat die Form

$$\alpha = c_0 + \cfrac{1}{c_1 + \cfrac{1}{c_2 + \cfrac{1}{c_3 + \cdots}}} =: [c_0, c_1, c_2, c_3, \ldots]\,,$$

wobei die Folgen $r_1, r_2, \ldots$ und $c_0, c_1, \ldots$ rekursiv definiert sind durch

$$r_0 := \alpha, \quad r_i := \frac{1}{r_{i-1} - c_{i-1}} \qquad \text{und} \qquad c_i := \lfloor r_i \rfloor\,.$$

Man nennt die c_i Teilnenner und die r_i Restzahlen. $[c_0, c_1, \ldots, c_n]$ heißt der n-te Näherungsbruch von α.

Vereinbarung: Im Folgenden seien immer r_i die Restzahlen und c_i die Teilnenner des betrachteten Kettenbruchs.

3.10 Bemerkung
Sei $[c_0, c_1, \ldots]$ die Kettenbruchentwicklung von α. Dann gilt:

1. $r_i = c_i + \frac{1}{r_{i+1}}$.
2. $r_i \geq 1$ für alle $i \geq 1$.

Beweis:

1. $c_i + \frac{1}{r_{i+1}} = c_i + \frac{1}{\frac{1}{r_i - c_i}} = c_i + r_i - c_i = r_i$.
2. $0 < r_i - \lfloor r_i \rfloor \leq 1 \quad \Rightarrow \quad r_i = \frac{1}{r_i - \lfloor r_i \rfloor} \geq 1$. □

3.11 Beispiel
Wir suchen die Kettenbruchentwicklung von $\frac{23}{5}$ und $\frac{1+\sqrt{5}}{2}$:

i	r_i	c_i
0	$\frac{23}{5}$	4
1	$\frac{5}{3}$	1
2	$\frac{3}{2}$	1
3	2	2

Also ist
$$\frac{23}{5} = [4,1,1,2] = 4 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{2}}}.$$

i	r_i	c_i
0	$\frac{1+\sqrt{5}}{2}$	1
1	$\frac{1+\sqrt{5}}{2}$	1
2	$\frac{1+\sqrt{5}}{2}$	1
$\vdots$	$\vdots$	$\vdots$

$r_0 = \frac{1+\sqrt{5}}{2} = 1 + \frac{\sqrt{5}-1}{2} \Rightarrow c_0 = 1$

$r_1 = \frac{1}{\frac{\sqrt{5}-1}{2}} = \frac{2}{\sqrt{5}-1} = \frac{1+\sqrt{5}}{2} = r_0$

Also ist $\frac{1+\sqrt{5}}{2} = [1,\bar{1}]$.

3.12 Satz
Die Kettenbruchentwicklung von $\alpha \in \mathbb{R}$ bricht genau dann ab, wenn α rational ist.

Beweis:

„$\Rightarrow$“: Bricht die Kettenbruchentwicklung ab, so erhält man die rationale Zahl, indem man die Nenner gleich macht.

„$\Leftarrow$“: Sei nun α rational, dann gibt es $a, b \in \mathbb{Z}$, so dass $\alpha = \frac{a}{b}$ und ggT(a,b)=1. Vergleicht man den Euklidischen Algorithmus für a und b mit dem Kettenbruchalgorithmus für α, so stellt man fest, dass diese sich entsprechen:

$$\begin{aligned} a &= c_0 b + y_0 \\ b &= c_1 x_1 + y_1 \\ x_1 &= c_2 x_2 + y_2 \\ &\vdots \\ x_{n-1} &= c_n x_n + 0 \end{aligned}$$

$$\rightsquigarrow a = [c_0, c_1, c_2, \ldots, c_n], \qquad r_i = \frac{x_{i-1}}{x_i} \text{ für } i \in \{1, \ldots, n\},\ r_n = a_n\,.$$

Daher muss auch der Kettenbruchalgorithmus nach endlich vielen Schritten abbrechen. □

3.13 Definition
Seien $\alpha, \beta, \gamma, \delta \in \mathbb{R}$.

$\begin{pmatrix}\alpha\\ \beta\end{pmatrix}$ und $\begin{pmatrix}\gamma\\ \delta\end{pmatrix}$ heißen äquivalent, falls $\alpha\delta = \beta\gamma$ gilt.

Wir schreiben $\begin{pmatrix}\alpha\\ \beta\end{pmatrix} \sim \begin{pmatrix}\gamma\\ \delta\end{pmatrix}$.

3.14 Bemerkung
Gilt

$$\begin{pmatrix}\alpha\\ \beta\end{pmatrix} \sim \begin{pmatrix}\gamma\\ \delta\end{pmatrix},$$

dann gibt es ein $\varepsilon \in \mathbb{R}$, so dass

$$\varepsilon \begin{pmatrix}\alpha\\ \beta\end{pmatrix} = \begin{pmatrix}\gamma\\ \delta\end{pmatrix}.$$

Beweis:

$$\begin{pmatrix}\alpha\\ \beta\end{pmatrix} \sim \begin{pmatrix}\gamma\\ \delta\end{pmatrix}$$
$$\Rightarrow \quad \alpha\delta = \beta\gamma \quad \Leftrightarrow \quad \alpha\delta\frac{\delta}{\beta} = \gamma\beta\frac{\delta}{\beta}$$
$$\Leftrightarrow \quad \left(\alpha\frac{\delta}{\beta}\right)\delta = \gamma\delta \quad \Rightarrow \quad \gamma = \alpha\frac{\delta}{\beta}$$

also folgt

$$\frac{\delta}{\beta}\begin{pmatrix}\alpha\\ \beta\end{pmatrix} = \begin{pmatrix}\gamma\\ \delta\end{pmatrix}.$$ □

3.15 Lemma
Sei $\alpha \in \mathbb{R}$ und $[c_0, c_1, \ldots]$ die zugehörige Kettenbruchentwicklung. Einen Schritt in der Kettenbruchentwicklung können wir (wie in Bemerkung 3.10) darstellen als

$$r_i = c_i + \frac{1}{r_{i+1}} \quad \Leftrightarrow \quad \begin{pmatrix}r_i\\ 1\end{pmatrix} \sim A_i \begin{pmatrix}r_{i+1}\\ 1\end{pmatrix}$$

wobei

$$A_i := \begin{pmatrix}c_i & 1\\ 1 & 0\end{pmatrix}.$$

Beweis:

$$r_i = c_i + \frac{1}{r_{i+1}} \quad \Leftrightarrow \quad r_i \cdot r_{i+1} = c_i \cdot r_{i+1} + 1$$

$$\Leftrightarrow \begin{pmatrix} r_i \\ 1 \end{pmatrix} \sim \begin{pmatrix} c_i r_{i+1} + 1 \\ r_{i+1} \end{pmatrix} = \begin{pmatrix} c_i & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} r_{i+1} \\ 1 \end{pmatrix} =: A_i \begin{pmatrix} r_{i+1} \\ 1 \end{pmatrix}. \qquad \square$$

3.16 Definition
Seien A_i wie in Lemma 3.15. Weiter definieren wir

$$P_{-1} := \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad P_i := A_0 \cdots A_i =: \begin{pmatrix} p_i & p_{i-1} \\ q_i & q_{i-1} \end{pmatrix} \ \forall i \geq 0\,.$$

Da $P_{i+1} = P_i A_{i+1}$ gilt, folgt nun für $i = 0, 1, 2, \ldots$:

$$p_{i+1} = c_{i+1} p_i + p_{i-1} \quad \text{und}$$
$$q_{i+1} = c_{i+1} q_i + q_{i-1}\,.$$

3.17 Definition
Seien A_i wie in Lemma 3.15. Weiter definieren wir

$$P_{-1} := \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad P_i := A_0 \cdots A_i =: \begin{pmatrix} p_i & p_{i-1} \\ q_i & q_{i-1} \end{pmatrix} \ \forall i \geq 0\,.$$

Da $P_{i+1} = P_i A_{i+1}$ gilt, folgt nun für $i = 0, 1, 2, \ldots$:

$$p_{i+1} = c_{i+1} p_i + p_{i-1} \quad \text{und}$$
$$q_{i+1} = c_{i+1} q_i + q_{i-1}\,.$$

Vereinbarung: Ist $r \in \mathbb{R}$ und $[c_0, \ldots, c_n]$ die zugehörige Kettenbruchentwicklung, so sind im Folgenden P_i, sowie p_i und q_i immer definiert wie in Definition 3.17.

3.18 Folgerung
Sei $r \in \mathbb{R}$, dann gilt:

1. $\begin{pmatrix} r \\ 1 \end{pmatrix} \sim P_n \begin{pmatrix} r_{n+1} \\ 1 \end{pmatrix}$.
2. $\det(A_i) = -1 \ \forall i \quad \text{und} \quad \det(P_i) = (-1)^{i+1}$.

3. $\mathrm{ggT}(p_n, q_n) = 1$.

4. $0 < p_i < p_{i+1}$ sowie $0 < q_i < q_{i+1}$ $\forall i$.

Beweis:
1. und 2.: folgen direkt aus der Definition von A_n und P_n.

3.: Wegen $p_n q_{n-1} - q_n p_{n-1} = \det(P_n) \in \{\pm 1\}$ und
$\mathrm{ggT}(p_n, q_n) \mid (p_n q_{n-1} - q_n p_{n-1})$
folgt $\mathrm{ggT}(p_n, q_n) = 1$.

4.: Es ist $c_i \geq 1$ (vgl. Bemerkung 3.10). Weiter gilt $p_{-1}, q_0 = 0$ und $p_0, q_{-1} = 1$. Damit sind die Folgen $(p_i)_{i\geq 0}$ und $(q_i)_{i\geq 0}$ streng monoton wachsend. □

3.19 Satz
Ist $r \in \mathbb{R}$ irrational, so gilt

$$|r - \frac{p_n}{q_n}| < \frac{1}{q_n^2}$$

also

$$r = \lim_{n\to\infty} \frac{p_n}{q_n} .$$

Beweis:
Da

$$\begin{pmatrix} r \\ 1 \end{pmatrix} \sim P_n \begin{pmatrix} r_{n+1} \\ 1 \end{pmatrix}$$

gilt

$$r(q_n r_{n+1} + q_{n-1}) = p_n r_{n+1} + p_{n-1} \quad \Leftrightarrow \quad r = \frac{p_n r_{n+1} + p_{n-1}}{q_n r_{n+1} + q_{n-1}} .$$

Es folgt

$$\begin{aligned} r - \frac{p_n}{q_n} &= \frac{p_n r_{n+1} + p_{n-1}}{q_n r_{n+1} + q_{n-1}} - \frac{p_n}{q_n} \\ &= \frac{p_n q_n r_{n+1} + q_n p_{n-1} - p_n q_n r_{n+1} - p_n q_{n-1}}{q_n(q_n r_{n+1} + q_{n-1})} \\ &= \frac{\det(P_n)}{q_n(q_n r_{n+1} + q_{n-1})} = \frac{(-1)^{n+1}}{q_n(q_n r_{n+1} + q_{n-1})} \end{aligned}$$

und daher

$$|r - \frac{p_n}{q_n}| = \frac{1}{q_n(q_n r_{n+1} + q_{n-1})} < \frac{1}{q_n^2} . \qquad \square$$

3.20 Satz
Sei $\beta_n = [a_0, \ldots, a_n] \in \mathbb{Q}$, mit $n \geq 1$ und $a_i \in \mathbb{N}\ \forall i \in \{0, \ldots n\}$. Dann ist $\beta_n > 1$ und die Kettenbruchentwicklung von β_n ist gleich $[a_1, \ldots, a_n]$, falls $a_n > 1$ und $[a_1, \ldots, a_{n-2}, a_{n-1} + 1]$ falls $a_n = 1$.

Beweis:
Mit vollständiger Induktion:

I.A.: $n = 1$: Es gilt $\beta_1 = a_0 + \frac{1}{a_1}$.

$a_1 = 1$: Dann ist $c_0 = \lfloor \beta_1 \rfloor = \lfloor a_0 + \frac{1}{a_1} \rfloor = \lfloor a_0 + 1 \rfloor = a_0 + 1 = \beta_1$.
Also hat β_1 die Kettenbruchentwicklung $[a_0 + 1]$.

$a_1 > 1$: $c_0 = \lfloor \beta_1 \rfloor = a_0$ und $r_1 = \frac{1}{a_0 + \frac{1}{a_1} - a_0} = a_1 = c_1$.
Also hat β_1 die Kettenbruchentwicklung $[a_0, a_1]$.

I.S.: $n \to n + 1$: Es gilt $\beta_n = a_0 + \frac{1}{a_1, \ldots, a_n}$.

$$\Rightarrow c_0 = \lfloor \beta_n \rfloor = a_0$$
$$\Rightarrow r_1 = \frac{1}{\beta_n - a_0} = [a_1, \ldots, a_n]$$

Also hat r_1 die Kettenbruchentwicklung $[a_1, \ldots, a_n]$, falls $a_n > 1$ und $[a_1, \ldots, a_{n-2}, a_{n-1} + 1]$, falls $a_n = 1$ ist.
β_n hat damit die Kettenbruchentwicklung $[a_0, a_1, \ldots, a_n]$, falls $a_n > 1$ und $[a_0, a_1, \ldots, a_{n-2}, a_{n-1} + 1]$, falls $a_n = 1$ ist. □

3.21 Satz
Die Zahl $\alpha \in \mathbb{R}$ mit $\alpha > 1$ habe die Näherungsbrüche $[c_0, \ldots, c_n]$ für $n = 0, 1, \ldots$. Dann gilt

$$[c_0, \ldots, c_n] = \frac{p_n}{q_n}\,.$$

Beweis:
Sei $\beta_n := [c_0, \ldots, c_n]$.
Für $n = 0$ folgt die Behauptung, da $p_0 = c_i$ und $q_0 = 1$ ist.
Für $n \geq 1$ kennen wir aus Satz 3.20 die Kettenbruchentwicklung von β_n, nämlich $[c_0, \ldots, c_n]$ oder $[c_0, \ldots, c_{n-1} + 1]$.

$c_n > 1$: Dann gilt für die Kettenbruchentwicklung $\beta_n := [c_0, \ldots, c_n]$.

$$\Rightarrow \begin{pmatrix} \beta_n \\ 1 \end{pmatrix} \sim P_{n-1} \begin{pmatrix} c_n \\ 1 \end{pmatrix}$$

also

$$\beta_n \cdot (p_{n-1}c_n + p_{n-2}) = q_{n-1}c_n + q_{n-2}$$
$$\Rightarrow \beta_n = \frac{q_{n-1}c_n + q_{n-2}}{p_{n-1}c_n + p_{n-2}} = \frac{p_n}{q_n}\,.$$

$c_n = 1$: Dann ist die Kettenbruchentwicklung $\beta_n := [c_0, \ldots, c_{n-1} + 1]$.

$$\Rightarrow \begin{pmatrix} \beta_n \\ 1 \end{pmatrix} \sim P_{n-2} \begin{pmatrix} c_{n-1} + 1 \\ 1 \end{pmatrix}$$

also

$$\begin{aligned} &\beta_n \cdot (p_{n-2}(c_{n-1}+1) + p_{n-3}) = q_{n-2}(c_{n-1}+1) + q_{n-3} \\ \Rightarrow \beta_n = &\frac{q_{n-2}(c_{n-1}+1) + q_{n-3}}{p_{n-2}(c_{n-1}+1) + p_{n-3}} = \frac{p_{n-1} + p_{n-2}}{q_{n-1} + q_{n-2}} \overset{c_n=1}{=} \frac{p_n}{q_n} . \end{aligned}$$ □

3.22 Folgerung
Die Zahl $\alpha > 1$ habe die Näherungsbrüche $[c_0, \ldots c_n]$, dann gilt mit Satz 3.19 und Satz 3.21

$$\alpha = \lim_{n\to\infty} \frac{p_n}{q_n} = \lim_{n\to\infty} [c_0, \ldots, c_n] .$$

3.23 Lemma
Die Zahl $\alpha > 1$ habe die Näherungsbrüche $[c_0, \ldots, c_n]$. Dann konvergiert die Folge der $(\frac{p_n}{q_n})_{n\geq 0}$ oszillierend gegen α und es gilt

$$\frac{p_1}{q_1} < \frac{p_3}{q_3} < \ldots < \alpha < \ldots < \frac{p_4}{q_4} < \frac{p_2}{q_2} .$$

Beweis:
Es gilt

$$\begin{aligned} &p_n q_{n-2} - q_n p_{n-2} \\ &= (c_n p_{n-1} + p_{n-2}) \cdot q_{n-2} - (c_n q_{n-1} + q_{n-2}) \cdot p_{n-2} \\ &= c_n (p_{n-1} q_{n-2} - q_{n-1} p_{n-2}) \\ &= c_n \det(P_{n-1}) = c_n (-1)^n , \end{aligned}$$

also

$$\frac{p_n}{q_n} - \frac{p_{n-2}}{q_{n-2}} = \frac{p_n q_{n-2} - q_n p_{n-2}}{q_n q_{n-2}} = \frac{c_n (-1)^n}{q_n q_{n-2}} ,$$

es folgt

$$\frac{p_1}{q_1} < \frac{p_3}{q_3} < \ldots < \frac{p_4}{q_4} < \frac{p_2}{q_2} .$$

Da wir schon wissen, dass $\frac{p_n}{q_n}$ gegen α konvergiert, gilt

$$\frac{p_1}{q_1} < \frac{p_3}{q_3} < \ldots < \alpha < \ldots < \frac{p_4}{q_4} < \frac{p_2}{q_2} .$$ □

3.24 Satz
Seien $a_0, a_1, \ldots$ beliebige natürliche Zahlen. Dann existiert

$$\alpha := \lim_{n\to\infty} [a_0, \ldots, a_n]$$

und die Kettenbruchentwicklung von α ist $[a_0, a_1, \ldots]$.

Beweis:
Da

$$\frac{p_n}{q_n} - \frac{p_{n-1}}{q_{n-1}} = \frac{p_n q_{n-1} - q_n p_{n-1}}{q_n q_{n-1}} = \frac{\det(P_n)}{q_n q_{n-1}} = \frac{(-1)^{n+1}}{q_n q_{n-1}} ,$$

konvergiert die Folge $\frac{p_n}{q_n}$ gegen ein $\alpha \in \mathbb{R}$. Aus Satz 3.20 folgt, dass $[a_1, \ldots a_n]$ oder $[a_1, \ldots a_{n-1} + 1]$ die Kettenbruchentwicklung von $\frac{p_n}{q_n}$ ist. Also gilt

$$\alpha = \lim_{n\to\infty} \frac{p_n}{q_n} = \lim_{n\to\infty} [a_0, \ldots, a_n]$$

und $[a_0, a_1, \ldots]$ ist die Kettenbruchentwicklung von α. □

3.2.2 Periodische Kettenbrüche

3.25 Definition (periodische Kettenbrüche)
Der Kettenbruch einer (nicht rationalen wg. Satz 3.12) Zahl $\alpha = [c_0, c_1, \ldots]$ heißt periodisch, wenn es ein $n_0 \geq 0$ und ein $k \geq 1$ gibt, so dass

$$c_{n+k} = c_n \; \forall n \geq n_0 .$$

Wir schreiben dafür $\alpha = [c_0, \ldots, c_{n_0-1}, \overline{c_{n_0}, c_{n_0+1}, \ldots, c_{n_0+k-1}}]$.
α heißt rein periodisch, wenn $n_0 = 0$ ist.

3.26 Satz (Euler)
Jeder periodische Kettenbruch stellt eine quadratische Irrationalzahl dar.

Beweis:
Sei $\alpha = [c_0, \ldots, c_{n_0-1}, \overline{c_{n_0}, c_{n_0+1}, \ldots, c_{n_0+k-1}}]$ und seien r_i mit $i \geq 0$ die zugehörigen Restzahlen, dann ist $r_{n_0} = [\overline{c_{n_0}, c_{n_0+1}, \ldots, c_{n_0+k-1}}]$.
Wegen

$$\begin{pmatrix} \alpha \\ 1 \end{pmatrix} \sim P_{n_0} \begin{pmatrix} r_{n_0} \\ 1 \end{pmatrix}$$

gilt

$$\begin{aligned} & \alpha \cdot (r_{n_0} q_{n_0} + q_{n_0-1}) = r_{n_0} p_{n_0} + p_{n_0-1} \\ \Leftrightarrow \quad & \alpha = \frac{r_{n_0} p_{n_0} + p_{n_0-1}}{r_{n_0} q_{n_0} + q_{n_0-1}} . \end{aligned}$$

also

$$\alpha \in \mathbb{Q}[\sqrt{d}] \text{ für ein } d \in \mathbb{N} \;\Leftrightarrow\; r_{n_0} \in \mathbb{Q}[\sqrt{d}]\,.$$

Deshalb können wir o.B.d.A. annehmen, dass α eine rein periodische Kettenbruchdarstellung hat. Sei

$$\alpha = [\overline{c_0, \ldots, c_k}]$$

diese periodische Kettenbruchentwicklung von α. Dann ist

$$\alpha = [c_0, \ldots, c_k, \alpha]\,.$$

Daher können wir schreiben

$$\begin{aligned} & \begin{pmatrix} \alpha \\ 1 \end{pmatrix} \sim P_k \begin{pmatrix} \alpha \\ 1 \end{pmatrix} \\ \Leftrightarrow \quad & \alpha(q_k\alpha + q_{k-1}) = p_k\alpha + p_{k-1} \\ \Leftrightarrow \quad & q_k\alpha^2 - (p_k - q_{k-1})\alpha - p_{k-1} = 0\,. \end{aligned}$$

Da α nicht rational ist, folgt die Behauptung mit Lemma 3.7. □

3.27 Satz
Sei $\vartheta > 1$ eine quadratische Irrationalzahl mit Diskriminante D. Dann ist D auch die Diskriminante von allen Restzahlen ϑ_n von ϑ.

Beweis:
Durch vollständige Induktion:

IA: $\vartheta =: \vartheta_0$ hat Diskriminante $D := \beta^2 + 4\alpha\gamma$ mit zugehöriger quadratischer Gleichung $\alpha\vartheta^2 - \beta\vartheta - \gamma = 0$, wobei $\mathrm{ggT}(\alpha, \beta, \gamma) = 1$ und $\alpha > 0$ gilt.

IS: Sei $[c_0, c_1, c_2, c_3, \ldots]$ die Kettenbruchdarstellung von ϑ. Wir wissen aus Bemerkung 3.10:

$$\begin{aligned} & \vartheta_n = c_n + \frac{1}{\vartheta_{n+1}} \\ \Rightarrow \quad & \alpha\left(c_n + \frac{1}{\vartheta_{n+1}}\right)^2 - \beta\left(c_n + \frac{1}{\vartheta_{n+1}}\right) - \gamma = 0 \\ \Leftrightarrow \quad & \alpha c_n^2\vartheta_{n+1}^2 + 2\alpha c_n\vartheta_{n+1} + \alpha - \beta c_n\vartheta_{n+1}^2 - \beta\vartheta_{n+1} - \gamma\vartheta_{n+1}^2 = 0 \\ \Leftrightarrow \quad & (\beta c_n + \gamma - \alpha c_n^2)\vartheta_{n+1}^2 - (2\alpha c_n - \beta)\vartheta_{n+1} - \alpha = 0 \end{aligned}$$

Nun gilt $\mathrm{ggT}(\alpha, 2\alpha c_n - \beta) = \mathrm{ggT}(\alpha, \beta)$ und $\mathrm{ggT}(\alpha, \beta)$ ist entweder gleich 1 oder $t := \mathrm{ggT}(\alpha, \beta) \nmid (\underbrace{\beta c_n}_{t\mid} + \underbrace{\gamma}_{t\nmid} - \underbrace{\alpha c_n^2}_{t\mid})$.
Also ist $\mathrm{ggT}(\beta c_n + \gamma - \alpha c_n^2, 2\alpha c_n - \beta, \alpha) = 1$.

Wir nehmen o.B.d.A. an, dass $(\beta c_n + \gamma - \alpha c_n^2) > 0$ ist, denn sonst kann man die quadratische Gleichung mit -1 multiplizieren. Die Diskriminante wird dadurch nicht verändert.

Die Diskriminante von ϑ_{n+1} ist deshalb

$$\begin{aligned} D_{\vartheta_{n+1}} &= (2\alpha c_n - \beta)^2 + 4\alpha(\beta c_n + \gamma - \alpha c_n^2) \\ &= 4\alpha^2 c_n^2 - 4\alpha c_n \beta + \beta^2 + 4\alpha\beta c_n + 4\alpha\gamma - 4\alpha^2 c_n^2 \\ &= \beta^2 + 4\alpha\gamma = D_{\vartheta_n} = D\,. \end{aligned}$$ □

3.28 Satz
Zu einer festen Diskriminante gibt es nur endlich viele reduzierte Irrationalzahlen.

Beweis:
Sei ϑ reduziert und seien $\alpha, \beta, \gamma \in \mathbb{Z}$ mit $\alpha\vartheta^2 - \beta\vartheta - \gamma = 0$, wobei $\mathrm{ggT}(\alpha, \beta, \gamma) = 1$ und $\alpha > 0$ gelten.
Dann gilt $\vartheta \in \{\frac{\beta \pm \sqrt{D}}{2\alpha}\}$ mit $D = \beta^2 + 4\alpha\gamma$.
Da $\vartheta > 1$ und $-\frac{1}{\sigma(\vartheta)} > 1$ sind, ist $\vartheta = \frac{\beta + \sqrt{D}}{2\alpha}$ und $\sigma(\vartheta) = \frac{\beta - \sqrt{D}}{2\alpha}$.

Da $|\sigma(\vartheta)| < 1$ ist, gilt $\mathcal{S}(\vartheta) = \vartheta + \sigma(\vartheta) = \frac{\beta}{\alpha} > 0$, daher ist $\beta > 0$.
Da $\sigma(\vartheta) < 0$ ist, ist auch $\beta - \sqrt{D} < 0$.
Also gilt $\beta \in (0, \sqrt{D})$.

Weiter gilt

$$\vartheta = \frac{\beta + \sqrt{D}}{2\alpha} \quad \Leftrightarrow \quad \alpha = \frac{\beta + \sqrt{D}}{2\vartheta} \quad \overset{\vartheta > 1}{\Longleftrightarrow} \quad \alpha < \frac{\beta + \sqrt{D}}{2}$$

und

$$\sigma(\vartheta) = \frac{\beta - \sqrt{D}}{2\alpha} \quad \Leftrightarrow \quad \alpha = \frac{\beta - \sqrt{D}}{2\sigma(\vartheta)} \quad \overset{\sigma(\vartheta) > -1}{\Longleftrightarrow} \quad \alpha > \frac{-\beta + \sqrt{D}}{2}$$

und deshalb

$$\alpha \in \left(\frac{-\beta + \sqrt{D}}{2}, \frac{\beta + \sqrt{D}}{2} \right) .$$

Da c durch a, b und D eindeutig bestimmt ist und da gilt $a, b, c \in \mathbb{Z}$, ist die Menge der reduzierten Zahlen zu einer bestimmten Diskriminante D endlich. □

3.29 Bemerkung
Wir benutzen hier das Konjugierte $\sigma(\vartheta)$ wie in Definition 2.2 mit $d := D$, D ist hier i.A. aber nicht quadratfrei.
Beispiel: $\alpha = 4,\ \beta = 8,\ \gamma = 1 \quad \Rightarrow D = 80$.
Die Nullstelle $1 + \sqrt{1 + \frac{1}{4}}$ der zugehörigen quadratischen Gleichung ist reduziert.

3.30 Satz
Sei $\vartheta > 1$ eine quadratische Irrationalzahl. Dann sind die Restzahlen ϑ_n der Kettenbruchentwicklung von ϑ von einer Stelle $n = n_0$ an reduziert.

Beweis:
Wegen Bemerkung 3.10 ist $\vartheta_n \geq 1$ für alle $i \geq 1$. Wäre $\vartheta_n = 1$, so würde der Kettenbruch abbrechen, ϑ_n wäre also keine quadratische Irrationalzahl.
Sei $\vartheta = u + v\sqrt{D} = [c_0, c_1, \ldots]$ und $\vartheta_{n+1} = r + s\sqrt{D}$, wobei D die Diskriminante von ϑ ist, dann gilt

$$\begin{pmatrix} \vartheta \\ 1 \end{pmatrix} \sim P_n \begin{pmatrix} \vartheta_{n+1} \\ 1 \end{pmatrix} \quad \text{mit} \quad P_n = \begin{pmatrix} p_n & p_{n-1} \\ q_n & q_{n-1} \end{pmatrix}$$
$$\Rightarrow \begin{pmatrix} \vartheta_{n+1} \\ 1 \end{pmatrix} \sim P_n^{-1} \begin{pmatrix} \vartheta \\ 1 \end{pmatrix} \quad \text{mit} \quad P_n^{-1} = \begin{pmatrix} q_{n-1} & -p_{n-1} \\ -q_n & p_n \end{pmatrix}$$
$$\Leftrightarrow \begin{pmatrix} u + v\sqrt{D} \\ 1 \end{pmatrix} \sim P_n^{-1} \begin{pmatrix} r + s\sqrt{D} \\ 1 \end{pmatrix}$$

Es folgt

$$\begin{pmatrix} u - v\sqrt{D} \\ 1 \end{pmatrix} \sim P_n^{-1} \begin{pmatrix} r - s\sqrt{D} \\ 1 \end{pmatrix}$$
$$\Leftrightarrow \begin{pmatrix} \sigma(\vartheta_{n+1}) \\ 1 \end{pmatrix} \sim P_n^{-1} \begin{pmatrix} \sigma(\vartheta) \\ 1 \end{pmatrix}$$

also

$$\sigma(\vartheta_{n+1}) \cdot (-q_n\sigma(\vartheta) + p_n) \;=\; q_{n-1}\sigma(\vartheta) - p_{n-1}$$
$$\Leftrightarrow -\frac{1}{\sigma(\vartheta_{n+1})} \;=\; \frac{(q_n\sigma(\vartheta) - p_n)q_{n-1}}{(q_{n-1}\sigma(\vartheta) - p_{n-1})q_{n-1}} \;=\; \frac{q_n\sigma(\vartheta)q_{n-1} - p_nq_{n-1}}{(q_{n-1}\sigma(\vartheta) - p_{n-1})q_{n-1}}$$
$$= \frac{q_n\sigma(\vartheta)q_{n-1} - q_np_{n-1} + q_np_{n-1} - p_nq_{n-1}}{(q_{n-1}\sigma(\vartheta) - p_{n-1})q_{n-1}}$$
$$= \frac{q_n}{q_{n-1}} - \frac{\det(P_n)}{(q_{n-1}\sigma(\vartheta) - p_{n-1})q_{n-1}} \;=\; \frac{q_n}{q_{n-1}} - \frac{(-1)^{n+1}}{(q_{n-1}\sigma(\vartheta) - p_{n-1})q_{n-1}}$$
$$\Leftrightarrow \; -\frac{1}{\sigma(\vartheta_{n+1})} - 1 \;=\; \frac{q_n - q_{n-1}}{q_{n-1}} - \frac{(-1)^{n+1}}{(q_{n-1}\sigma(\vartheta) - p_{n-1})q_{n-1}}$$
$$= \frac{1}{q_{n-1}} \cdot \left(q_n - q_{n-1} - \frac{(-1)^{n+1}}{q_{n-1}\left(\sigma(\vartheta) - \frac{p_{n-1}}{q_{n-1}}\right)} \right)$$

Da

$$\lim_{n\to\infty}\left(\sigma(\vartheta)-\frac{p_{n-1}}{q_{n-1}}\right) \;=\; \sigma(\vartheta)-\vartheta \;\neq\; 0 \quad \text{(vgl. Satz 3.19)}$$

sowie

$$\lim_{n\to\infty}\frac{1}{q_{n-1}} \;=\; 0 \quad \text{und} \quad q_n - q_{n-1} \geq 1 \text{ für } n > 2 \quad \text{(vgl. Folgerung 3.18)}$$

gelten, gibt es ein $n_0 \in \mathbb{N}$, so dass für alle $n \geq n_0$ gilt

$$-\frac{1}{\sigma(\vartheta_{n+1})} > 1\,. \qquad \square$$

3.31 Satz (Lagrange)
Sei ϑ eine quadratische Irrationalzahl. Dann hat ϑ eine periodische Kettenbruchentwicklung.

Beweis:
Diesen Satz folgern wir mithilfe der vorangehenden Sätze:
Sei ϑ eine quadratische Irrationalzahl. Dann folgt mit Satz 3.27, dass alle Restzahlen von ϑ die gleiche Diskriminante haben. Mit Satz 3.30 gilt, dass es ein $n_0 \in \mathbb{N}$ gibt, so dass alle Restzahlen ϑ_n mit $n \geq n_0$ reduziert sind, und schließlich folgt daraus mit Satz 3.28, dass es ein $n_0 \in \mathbb{N}$ und ein $k \in \mathbb{N}$ gibt, so dass $\vartheta_{n_0} = \vartheta_{n_0+k}$ ist. Also ist die Kettenbruchentwicklung periodisch. $\square$

3.32 Satz (Galois)
Eine quadratische Irrationalzahl ϑ hat eine rein periodische Kettenbruchentwicklung genau dann, wenn ϑ reduziert ist.

Beweis:
„⇒“: Angenommen, ϑ ist rein periodisch, also $\vartheta = [\overline{c_0, \ldots, c_k}]$.
Dann gibt es mit Satz 3.30 ein n_0, so dass ϑ_n für alle $n \geq n_0$ reduziert ist. Da ϑ rein periodisch ist, müssen alle Restzahlen, also auch ϑ selbst reduziert sein.

„⇒“: Angenommen, ϑ ist reduziert.
Wir zeigen durch vollständige Induktion, dass mit ϑ alle weiteren Restzahlen ϑ_n reduziert sind:

I.A.: $\vartheta = \vartheta_0$ ist reduziert.

I.S.: $\vartheta_n \to \vartheta_{n+1}$:
Da $\vartheta_{n+1} > 1$ und

$$\vartheta_n \;=\; c_n + \frac{1}{\vartheta_{n+1}} \quad \text{(Bemerkung 3.10)}$$

folgt

$$\begin{aligned} \sigma(\vartheta_n) &= c_n + \frac{1}{\sigma(\vartheta_{n+1})} \\ \Rightarrow \quad \frac{1}{\sigma(\vartheta_{n+1})} &= \sigma(\vartheta_n) - c_n < -c_n \leq -1\,. \end{aligned}$$

Also ist ϑ_{n+1} ebenfalls reduziert.

Nun zeigen wir, dass mit $\vartheta_n = \vartheta_{n+k}$ (wir wissen wegen dem Satz von Lagrange (Satz 3.31), dass es so ein n und so ein k gibt) auch $\vartheta_{n-1} = \vartheta_{n-1+k}$ gilt:
Wir wissen

$$\begin{aligned} & \vartheta_{n-1} = c_{n-1} + \frac{1}{\vartheta_n} \quad \text{und} \quad \vartheta_{n-1+k} = c_{n-1+k} + \frac{1}{\vartheta_{n+k}} = c_{n-1+k} + \frac{1}{\vartheta_n} \\ \Rightarrow \quad & \sigma(\vartheta_{n-1}) = c_{n-1} + \frac{1}{\sigma(\vartheta_n)} \quad \text{und} \quad \sigma(\vartheta_{n-1+k}) = c_{n-1+k} + \frac{1}{\sigma(\vartheta_n)} \\ \Rightarrow \quad & c_{n-1} = -\frac{1}{\sigma(\vartheta_n)} + \sigma(\vartheta_{n-1}) \quad \text{und} \quad c_{n-1+k} = -\frac{1}{\sigma(\vartheta_n)} + \sigma(\vartheta_{n-1+k}) \end{aligned}$$

$\sigma(\vartheta_{n-1})$ und $\sigma(\vartheta_{n-1+k})$ sind reduziert, also gilt

$$-\frac{1}{\sigma(\vartheta_{n-1})} < -1 \quad \text{und} - \frac{1}{\sigma(\vartheta_{n-1+k})} < -1\,.$$

Damit ist

$$0 < -\sigma(\vartheta_{n-1}) < 1 \quad \text{und} \quad 0 < -\sigma(\vartheta_{n-1+k}) < 1\,,$$

also

$$\begin{aligned} & c_{n-1} = \left\lfloor -\frac{1}{\sigma(\vartheta_n)} \right\rfloor \quad \text{und} \quad c_{n-1+k} = \left\lfloor -\frac{1}{\sigma(\vartheta_n)} \right\rfloor \\ \Rightarrow \quad & \frac{1}{\vartheta_{n-1} - c_{n-1}} = \vartheta_n = \frac{1}{\vartheta_{n-1+k} - c_{n-1}} \\ \Rightarrow \quad & \vartheta_{n-1} = \vartheta_{n-1+k}\,. \end{aligned}$$

□

3.2.3 Berechnung der Grundeinheit einer Ordnung

In diesem Abschnitt werden wir nun die Einheiten eines reell-quadratischen Zahlkörpers mit Hilfe der Kettenbrüche bestimmen. Das geht nicht nur für den Ganzheitsring $\mathcal{O}_{\mathbb{Q}[\sqrt{d}]}$, sondern auch für allgemeinere Ordnungen, die wir zu Beginn definieren.

Vereinbarung: In diesem Abschnitt sei w definiert durch

$$w := \begin{cases} \sqrt{d}, & \text{falls } d \equiv 2 \pmod 4 \text{ oder } d \equiv 3 \pmod 4\,, \\ \frac{1+\sqrt{d}}{2}, & \text{falls } d \equiv 1 \pmod 4\,. \end{cases}$$

3.33 Definition (Ordnung)
Sei Γ ein Hauptidealring. Ein Ring $\{0\} \neq \mathcal{O} \subseteq \mathcal{O}_{\mathbb{Q}[\sqrt{d}]}$ ist eine Ordnung, falls gilt:

1. $\Gamma \subseteq \mathcal{O}$,
2. $\mathcal{O}$ ist ein freier Γ-Modul in E vom Rang 2.

3.34 Satz
Der Ganzheitsring $\mathcal{O}_{\mathbb{Q}[\sqrt{d}]}$ ist eine Ordnung. Da

$$\mathcal{O} \subseteq \mathcal{O}_{\mathbb{Q}[\sqrt{d}]}$$

für alle Ordnungen $\mathcal{O}$ in E, nennt man ihn auch die Maximalordnung von $\mathbb{Q}[\sqrt{d}]$.

Beweis:
$\mathbb{Z}$ ist ein Hauptidealring und beide Voraussetzungen an $\mathcal{O}_{\mathbb{Q}[\sqrt{d}]}$ sind erfüllt:

1. $\mathbb{Z} \subseteq \mathcal{O}_{\mathbb{Q}[\sqrt{d}]}$ (, denn $a \in \mathbb{Z} \Rightarrow \mu_a(x) = x - a \in \mathbb{Z}$).
2. $\mathcal{O}_{\mathbb{Q}[\sqrt{d}]}$ ist ein $\mathbb{Z}$-Modul in $\mathbb{Q}[\sqrt{d}]$, der von $\langle 1, w\rangle$ erzeugt ist. □

3.35 Lemma
Sei $\mathcal{O}$ eine Ordnung. Dann gilt $\mathcal{O} = \{\alpha \in E \mid \alpha\mathcal{O} \subseteq \mathcal{O}\}$.

Beweis:
Sei $R := \{\alpha \in K | \alpha\mathcal{O} \subseteq \mathcal{O}\}$. Dann gilt $\mathcal{O} \subseteq R$ wegen der Abgeschlossenheit der Multiplikation in einem Ring.
Sei nun $\alpha \in E \setminus \mathcal{O}$. Dann ist $\alpha 1_{\mathcal{O}} = \alpha \notin \mathcal{O}$. Also $\mathcal{O} = R$. □

Vereinbarung: Da wir nun nur noch den Fall reell-quadratischer Zahlkörper betrachten, setzen wir $E = \mathbb{Q}[\sqrt{d}]$ und $\mathcal{O}_E = \mathcal{O}_{\mathbb{Q}[\sqrt{d}]}$. Außerdem sei immer $d \in \mathbb{N}$ quadratfrei.

3.36 Satz
Sei $\mathcal{O}$ eine Ordnung in $\mathbb{Q}[\sqrt{d}]$. Dann ist $F(\mathcal{O}) := \{x \in \mathbb{Q} \mid x\mathbb{Z}_E \subseteq \mathcal{O}\} \trianglelefteq \mathbb{Z}$ und es gibt ein $f \in \mathbb{N}$, so dass $F(\mathcal{O}) = f\mathbb{Z}$.

Ferner wird $\mathcal{O}$ von $(1, fw)$ erzeugt.

Beweis:
$F(\mathcal{O}) \subseteq \mathbb{Z}$, denn

1. Fall: $w = \sqrt{d}$:
   Sei $x \in \mathbb{Q} \setminus \mathbb{Z}$
   $\Rightarrow x \cdot 1 \notin \mathcal{O} \subseteq \mathbb{Z}_E \Rightarrow F(\mathcal{O}) \subseteq \mathbb{Z}$.

2.Fall: $w = \frac{1+\sqrt{d}}{2}$:
   Angenommen es gilt $x \in \mathbb{Q} \setminus \frac{1}{2}\mathbb{Z}$, dann folgt wie oben $x \cdot 1 \notin \mathcal{O}$.
   Für $x \in \frac{1}{2}\mathbb{Z} \setminus \mathbb{Z}$ gilt $x \cdot \frac{1+\sqrt{d}}{2} \notin \mathcal{O} \subseteq \mathbb{Z}_E$.
   Daher folgt $F(\mathcal{O}) \subseteq \mathbb{Z}$.

Sei $\varphi: \quad \mathbb{Z} \to \mathbb{Z}_E/\mathcal{O},\ x \mapsto x(\mathbb{Z}_E/\mathcal{O})$.
Dann ist φ ein Ringhomomorphismus und $\mathrm{Kern}(\varphi) = F(\mathcal{O})$, also gilt $F(\mathcal{O}) \trianglelefteq \mathbb{Z}$.

Da $\mathbb{Z}$ ein Hauptidealring ist, gibt es nun ein $f \in \mathbb{Z}$, so dass $f\mathbb{Z} = F(\mathcal{O})$.

Es bleibt noch zu zeigen, dass $\mathcal{O}$ von $(1, fw)$ erzeugt wird:

$\langle 1, fw\rangle_{\mathbb{Z}} \subseteq \mathcal{O}$: Da $f\mathbb{Z} = \{x \in \mathbb{Q} \mid x\mathbb{Z}_E \subseteq \mathcal{O}\}$, folgt diese Inklusion direkt aus der Definition von f.

$\langle 1, fw\rangle_{\mathbb{Z}} \supseteq \mathcal{O}$: Sei $x \in \mathcal{O}$

$$\Rightarrow \quad x \in \mathcal{O}_E\,,$$

dann gibt es $a, b \in \mathbb{Z}$, so dass $x = a + bw$

$$\Rightarrow \quad x - a = bw \in \mathcal{O}_E \quad \Rightarrow \quad b \in F(\mathcal{O})$$
$$\Rightarrow \quad f \mid b \quad \Rightarrow \quad x \in \langle 1, fw\rangle_{\mathbb{Z}}\,. \qquad \square$$

3.37 Definition (Führer)
Sei $\mathcal{O}$ eine $\mathbb{Z}$-Ordnung. Dann nennt man f aus Satz 3.36 den Führer von $\mathcal{O}$.

Die folgende Definition einer Diskriminante bezieht sich nicht auf Elemente aus einem Ring, sondern auf eine Ordnung. Man kann aber nachrechnen, dass die Diskriminante des Erzeugers w eines Ganzheitsringes eines quadratischen Zahlkörpers der Diskriminante des Ganzheitsringes entspricht. Das gilt auch für allgemeinere Ordnungen.

3.38 Definition (Diskriminante einer Ordnung)
Sei $\mathcal{O}$ eine $\mathbb{Z}$-Ordnung mit $\mathbb{Z}$-Basis C. Weiter sei $\Phi(x, y) := \mathcal{S}(x \cdot y)$ eine Bilinearform und G die zugehörige Gram-Matrix. Dann nennt man $\Delta(\mathcal{O}) := \det(G)$ die Diskriminante von $\mathcal{O}$.

3.39 Satz
Die Diskriminante von $\mathcal{O}_E$ ist

$$d_E := \Delta(\mathcal{O}_E) = \begin{cases} d, & \text{falls } d \equiv 1 \pmod 4 \\ 4d, & \text{falls } d \equiv 2 \pmod 4 \text{ oder } d \equiv 3 \pmod 4 \end{cases}.$$

Vereinbarung: Im Folgenden bezeichne d_E immer die Diskriminante von $\mathcal{O}_E$.

Beweis:
Die $\mathbb{Z}$-Basis von $\mathcal{O}_E$ ist $(1, w)$, deshalb ist die Gram-Matrix für
$d \equiv 1 \pmod 4$, also $w = \frac{1+\sqrt{d}}{2}$:

$$G = \begin{pmatrix} \Phi(1,1) & \Phi(1,w) \\ \Phi(w,1) & \Phi(w,w) \end{pmatrix} = \begin{pmatrix} \mathcal{S}(1) & \mathcal{S}(\frac{1+\sqrt{d}}{2}) \\ \mathcal{S}(\frac{1+\sqrt{d}}{2}) & \mathcal{S}(\frac{1+2\sqrt{d}+d}{4}) \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & \frac{1+d}{2} \end{pmatrix}$$

$$\Rightarrow d_E = \det(G) = d\,.$$

Analog für $d \equiv 2 \pmod 4$ oder $d \equiv 3 \pmod 4$, also $w = \sqrt{d}$:

$$G = \begin{pmatrix} \Phi(1,1) & \Phi(1,w) \\ \Phi(w,1) & \Phi(w,w) \end{pmatrix} = \begin{pmatrix} \mathcal{S}(1) & \mathcal{S}(\sqrt{d}) \\ \mathcal{S}(\sqrt{d}) & \mathcal{S}(d) \end{pmatrix} = \begin{pmatrix} 2 & 0 \\ 0 & 2d \end{pmatrix}$$

$$\Rightarrow d_E = \det(G) = 4d\,.$$ □

3.40 Bemerkung (Zusammenhang mit der Diskriminante in 3.2)
Aus Lemma 2.15 kennen wir das Minimalpolynom von w,
$\mu_w(x) = x^2 - \mathcal{S}(w)x + \mathcal{N}(w)$. Da w ganz ist, ist die Diskriminante D von w

$$D = \mathcal{S}(w)^2 - 4\mathcal{N}(w) = \begin{cases} 4d, & \text{falls } w = \sqrt{d} \\ d, & \text{falls } w = \frac{1+\sqrt{d}}{2} \end{cases}.$$

3.41 Satz
Die Diskriminante einer Ordnung $\mathcal{O} \subset \mathbb{Z}_E$ ist $\Delta(\mathcal{O}) = f^2 \cdot d_E$, wobei f der Führer von $\mathcal{O}$ ist.

Beweis:
Seien $C = (1, w)$ und $C' = (1, fw)$ die $\mathbb{Z}$-Basen von $\mathcal{O}_E$ und $\mathcal{O}$, außerdem sei G die Gram-Matrix aus dem Beweis von Satz 3.39, also $\det(G) = d_E$. Dann ist die Basiswechselmatrix

$${}^C\mathrm{Id}^{C'} = \begin{pmatrix} 1 & 0 \\ 0 & f \end{pmatrix},$$

also folgt für $\Delta(\mathcal{O})$

$$\Delta(\mathcal{O}) = \det(({}^C\mathrm{Id}^{C'})^{tr}) \det(G) \det({}^C\mathrm{Id}^{C'}) = f^2 \cdot d_E\,.$$ □

3.42 Satz
Sei $\mathcal{O}$ eine Ordnung in $\mathbb{Q}[\sqrt{d}]$ und f der Führer von $\mathcal{O}$. Dann ist die erste Restzahl $\vartheta := \frac{1}{fw - \lfloor fw \rfloor}$ von fw reduziert.

Beweis:
w und damit auch fw ist irrational. Also gilt für die erste Restzahl ϑ von fw: $\vartheta > 1$. Für $-\frac{1}{\sigma(\vartheta)}$ gilt

$$\begin{aligned} -\frac{1}{\sigma(\vartheta)} &= -\sigma(fw - \lfloor fw \rfloor) \overset{\lfloor fw \rfloor \in \mathbb{Z}}{=} \lfloor fw \rfloor - \sigma(fw) \\ &= \lfloor fw \rfloor - f\sigma(w) \geq f\lfloor w \rfloor - f\sigma(w) \\ &> f\lfloor w \rfloor \geq 1 \end{aligned}$$

Also ist ϑ reduziert. □

Nun kommt das entscheidende Ergebnis dieses Abschnitts, das im Wesentlichen die Aussagen des Dirichletschen Einheitensatzes für reell-quadratische Zahlkörper beinhaltet.

3.43 Satz (über Grundeinheiten)
Sei $\mathcal{O}$ eine Ordnung mit Führer f, ϑ eine reduzierte Zahl in E mit der Diskriminante $d_E f^2$ und $[c_0, \ldots, c_k]$ die Kettenbruchentwicklung von ϑ mit kleinstmöglicher Periode k. Dann ist $\varepsilon_0 = q_k\vartheta + q_{k-1} > 1$ die Grundeinheit von $\mathcal{O}$, das heißt, alle Einheiten ε von $\mathcal{O}$ lassen sich durch $\varepsilon = \pm\varepsilon_0^h$ mit $h \in \mathbb{Z}$ darstellen.

Für den Beweis brauchen wir noch einige Hilfssätze:

3.44 Lemma
Sei $\varepsilon = \frac{u+vf\sqrt{d_E}}{2} > 1$ mit $u, v \in \mathbb{Z}$ eine Einheit einer Ordnung $\mathcal{O}$ mit Führer f. Dann ist $u \geq 1$ und $v \geq 1$.

Beweis:
Da ε eine Einheit ist, gilt $\mathcal{N}(\varepsilon) = \varepsilon\sigma(\varepsilon) \in \{\pm 1\}$. Daraus folgt $\sigma(\varepsilon) \in \{\pm\frac{1}{\varepsilon}\}$. Deshalb ist $\{\pm\varepsilon, \pm\frac{1}{\varepsilon}\} = \{\frac{\pm u \pm vf\sqrt{d_E}}{2}\}$. Da $\varepsilon \neq 1$, ist genau eine dieser Zahlen größer als 1. Wir wissen, dass das ε ist und damit gilt $u \geq 1, v \geq 1$. □

3.45 Bemerkung
Sei $\mathcal{O}$ eine Ordnung in $\mathbb{Q}[\sqrt{d}]$ mit Führer f. Ein Element $a \in \mathbb{Q}[\sqrt{d}]$ liegt genau dann in $\mathcal{O}$, wenn a die Darstellung

$$a = \frac{y}{2} + \frac{zf\sqrt{d_E}}{2}$$

mit

$$y \equiv zfd_E \pmod 2$$

hat.

Beweis:
„⇒“: Sei $a \in \mathcal{O}$. Dann gibt es $u, v \in \mathbb{Z}$, so dass $a = u + vfw$.

$w = \frac{1+\sqrt{d}}{2}$: Dann ist

$$a = \frac{2u}{2} + \frac{vf + vf\sqrt{d}}{2} = \frac{2u+vf}{2} + \frac{vf\sqrt{d}}{2} = \frac{2u+vf}{2} + \frac{vf\sqrt{d_E}}{2}\,,$$

also $y = 2u + vf, z = v$ und $y \equiv zf \pmod 2$.
Da $d_E = d \equiv 1 \pmod 4$ ist, ist auch $y \equiv zfd_E \pmod 2$.

$w = \sqrt{d}$: Dann ist

$$a = \frac{2u}{2} + \frac{2vf\sqrt{d}}{2} = \frac{2u}{2} + \frac{vf\sqrt{4d}}{2} = \frac{2u}{2} + \frac{vf\sqrt{d_E}}{2}\,.$$

Das bedeutet, $y = 2u \equiv 0 \pmod 2$ und $z = v$.
Da $d_E = 4d \equiv 0 \pmod 2$ ist, folgt $y \equiv zfd_E \equiv 0 \pmod 2$.

„$\Leftarrow$“: a habe die Darstellung $a = \frac{y}{2} + \frac{zf\sqrt{d_E}}{2}$ mit $y, z \in \mathbb{Z}$ und $y \equiv zfd_E \pmod 2$.

$w = \frac{1+\sqrt{d}}{2}$:

$$\begin{aligned} a &= \frac{y}{2} + \frac{zf\sqrt{d_E}}{2} = \frac{y-zf}{2} + \frac{zf + zf\sqrt{d_E}}{2} \\ &= \frac{y-zf}{2} + \frac{zf(1+\sqrt{d})}{2} = \frac{y-zf}{2} + \frac{zfw}{2}\,. \end{aligned}$$

Da $y \equiv zf \pmod 2$ ist, folgt

$$a = \frac{y-zf}{2} + \frac{zfw}{2} \in \mathcal{O}\,.$$

$w = \sqrt{d}$: Da $y \equiv zfd_E \pmod 2$ und $d_E = 4d$ ist, ist $y \equiv zfd_E \equiv 0 \pmod 2$. Damit ist $\frac{y}{2} \in \mathbb{Z}$ und

$$a = \frac{y}{2} + \frac{zf\sqrt{d_E}}{2} = \frac{y}{2} + \frac{2zf\sqrt{d}}{2} = \frac{y}{2} + zf\sqrt{d} \in \mathcal{O}. \qquad \square$$

3.46 Satz
Sei $\mathcal{O}$ eine Ordnung mit Führer f. $\vartheta \in E$ sei reduziert und habe die Diskriminante $f^2 d_E$. k bezeichne die Länge der Periode des Kettenbruchs von ϑ. Dann ist $\varepsilon_0 = q_k\vartheta + q_{k-1}$ eine Einheit in $\mathcal{O}$.

Beweis:
Da ϑ reduziert ist, ist der Kettenbruch von ϑ rein periodisch (vgl. Satz 3.32). Daher gibt es auch ein $k \in \mathbb{N}$ mit $\vartheta = \vartheta_k$. Dann gilt (mit Folgerung 3.18)

$$\begin{pmatrix}\vartheta\\1\end{pmatrix} \sim P_k \begin{pmatrix}\vartheta_k + 1\\1\end{pmatrix} = P_k \begin{pmatrix}\vartheta\\1\end{pmatrix},$$

mit Bemerkung 3.14 folgt

$$(q_k\vartheta + q_{k-1})\begin{pmatrix}\vartheta\\1\end{pmatrix} = P_k\begin{pmatrix}\vartheta\\1\end{pmatrix},$$

also sei $\varepsilon := q_k\vartheta + q_{k-1}$. Dann folgt

$$(P_k - \varepsilon_0 E)\begin{pmatrix}\vartheta\\1\end{pmatrix} = \begin{pmatrix}0\\0\end{pmatrix},$$

wobei E die Einheitsmatrix ist. Weiter folgt (mit Folgerung 2.11)

$$\begin{aligned}
&\det(P_k - \varepsilon_0 E)\begin{pmatrix}\vartheta\\1\end{pmatrix} = 0\\
\Leftrightarrow\quad &0 = \det(P_k - \varepsilon_0 E) = \det\left(\begin{pmatrix}p_k - \varepsilon_0 & p_{k-1}\\ q_k & q_k - \varepsilon_0\end{pmatrix}\right)\\
&= \varepsilon_0^2 - (p_k - q_{k-1})\varepsilon_0 + \det(P_k)\,.
\end{aligned}$$

Da ε_0 irrational ist, bedeutet das

$$\mu_{\varepsilon_0}(x) = x^2 - (p_k - q_{k-1})x + \det(P_k)\,.$$

Aus Lemma 2.15 wissen wir nun $\mathcal{N}(\varepsilon_0) = \det(P_k) \in \{\pm 1\}$. Also ist (mit Satz 3.1) ε_0 eine Einheit in $\mathcal{O}_E$.

Nun möchten wir noch zeigen, dass ε_0 in $\mathcal{O}$ liegt. Dazu nutzen wir wieder

$$\begin{aligned}
&\begin{pmatrix}\vartheta\\1\end{pmatrix} \sim P_k\begin{pmatrix}\vartheta\\1\end{pmatrix} = \begin{pmatrix}p_k & p_{k-1}\\ q_k & q_{k-1}\end{pmatrix}\begin{pmatrix}\vartheta\\1\end{pmatrix}\\
\Rightarrow\quad &\vartheta = \frac{p_k\vartheta + p_{k-1}}{q_k\vartheta + q_{k-1}}\\
\Leftrightarrow\quad &q_k\vartheta^2 + (q_{k-1} - p_k)\vartheta - p_{k-1} = 0\,.
\end{aligned}$$

Sei $t := \mathrm{ggT}(q_k, q_{k-1} - p_k, p_{k-1})$, dann gilt

$$\frac{q_k}{t}\vartheta^2 + \frac{(q_{k-1} - p_k)}{t}\vartheta - \frac{p_{k-1}}{t} = 0\,.$$

ϑ hat die Diskriminante $f^2 d_E$. Mit der p,q-Formel ist

$$\begin{aligned}
&\vartheta = \frac{p_k - q_{k-1}}{2q_k} + \frac{t}{2q_k}\sqrt{f^2 d_E}\,.\\
\Rightarrow\quad &\varepsilon_0 = q_k\vartheta + q_{k-1} = q_k\left(\frac{p_k - q_{k-1}}{2q_k} + \frac{t}{2q_k}\sqrt{f^2 d_E}\right) + q_{k-1}\\
&= \frac{p_k + q_{k-1}}{2} + \frac{tf}{2}\sqrt{d_E}\,.
\end{aligned}$$

Da ε_0 ganz ist, gilt $p_k + q_{k-1} \equiv tfd_E \pmod 2$ und mit Bemerkung 3.45 folgt

$$\varepsilon_0 = \frac{p_k + q_{k-1}}{2} + \frac{tf}{2}\sqrt{d_E} \in \mathcal{O}\,. \qquad \square$$

3.47 Satz
Sei $\mathcal{O}$ eine Ordnung mit Führer f und ε eine Einheit in $\mathcal{O}$ mit $\varepsilon > 1$. Sei $\vartheta \in E$ reduziert und habe die Diskriminante $f^2 d_E$. k bezeichne die minimale Periode des Kettenbruchs $[\overline{c_0, \ldots, c_k}]$ von ϑ. ε_0 sei definiert durch $\varepsilon_0 = q_k\vartheta + q_{k-1}$. Dann gibt es eine natürliche Zahl h mit

$$\varepsilon = \varepsilon_0^h\,.$$

Beweis:
Wir suchen eine Matrix P, für die gilt

$$\varepsilon \begin{pmatrix} \vartheta \\ 1 \end{pmatrix} = P \begin{pmatrix} \vartheta \\ 1 \end{pmatrix},$$

außerdem soll es c_i' für $i = 0, \ldots, s$ geben, so dass

$$P = \prod_{i=0}^{s} \begin{pmatrix} c_i' & 1 \\ 1 & 0 \end{pmatrix}$$

ist. Denn definiert man nun $\vartheta' := [c_0', \ldots, c_s', \vartheta]$, dann folgt

$$\begin{pmatrix} \vartheta' \\ 1 \end{pmatrix} \sim P \begin{pmatrix} \vartheta \\ 1 \end{pmatrix} = \varepsilon \begin{pmatrix} \vartheta \\ 1 \end{pmatrix} \sim \begin{pmatrix} \vartheta \\ 1 \end{pmatrix}\,.$$

Also ist $\vartheta' = \vartheta$ und damit $\vartheta = [c_0', \ldots, c_s']$. Daraus kann man folgern, dass s ein Vielfaches von k und $c_0', \ldots, c_s'$ eine $\frac{s}{k}$-fache Wiederholung von $c_0, \ldots, c_k$ ist. Setzt man $h := \frac{s}{k}$, so gilt

$$P = P_k^h \quad \Rightarrow \quad \varepsilon = \varepsilon_0^h\,.$$

ε hat die Form $\frac{u+vf\sqrt{d_E}}{2}$ und es ist $u \equiv vfd_E \pmod 2$ wegen Bemerkung 3.45. Außerdem wissen wir schon, dass $u, v \geq 1$ sind. Wähle nun $\alpha \in \mathbb{N}$ und $\beta\gamma \in \mathbb{Z}$ so, dass $\mathrm{ggT}(\alpha, \beta, \gamma) = 1$ ist und $\vartheta^2\alpha - \beta\vartheta - \gamma = 0$ gilt. Dann ist (p,q-Formel)

$$\alpha\vartheta = \frac{\beta}{2} + \frac{f\sqrt{d_E}}{2} \quad \text{und} \quad d_E f^2 = \beta^2 + 4\alpha\gamma\,.$$

Deshalb ist das Minimalpolynom von $\alpha\vartheta$

$$\mu_{\alpha\vartheta}(x) = x^2 - \beta x - \alpha\gamma\,.$$

Da alle Koeffizienten aus $\mathbb{Z}$ sind, ist $\alpha\vartheta$ ganz und deshalb gilt

$$fD \equiv \beta \pmod 2 \quad \Leftrightarrow \quad vfD \equiv v\beta \equiv u \pmod 2.$$

Setze nun

$$P := \begin{pmatrix} p & p^* \\ q & q^* \end{pmatrix} := \begin{pmatrix} \frac{u+\beta v}{2} & \gamma v \\ \alpha v & \frac{u-\beta v}{2} \end{pmatrix}$$

Nachrechnen: 1. Zeile:

$$\begin{aligned}
&\frac{u+\beta v}{2}\vartheta + \gamma v \;=\; \frac{u + vf\sqrt{d_E}}{2}\vartheta \\
\Leftrightarrow\quad &\frac{\beta}{2}\vartheta + \gamma \;=\; \frac{f\sqrt{d_E}}{2}\vartheta \\
\Leftrightarrow\quad &\gamma \;=\; (\frac{f\sqrt{d_E}}{2} - \frac{\beta}{2})\vartheta \\
\Leftrightarrow\quad &4\alpha\gamma \;=\; 4\alpha\vartheta(\frac{f\sqrt{d_E}}{2} - \frac{\beta}{2}) \;=\; 2(\beta + f\sqrt{d_E})(\frac{f\sqrt{d_E} - \beta}{2}) \;=\; f^2 d_E - \beta^2 \\
\Leftrightarrow\quad &d_E f^2 \;=\; \beta^2 + 4\alpha\gamma\,.
\end{aligned}$$

2. Zeile:

$$\begin{aligned}
&\alpha v\vartheta + \frac{u - \beta v}{2} \;=\; \frac{u + vf\sqrt{d_E}}{2} \\
\Leftrightarrow\quad &\alpha\vartheta + \frac{-\beta}{2} \;=\; \frac{f\sqrt{d_E}}{2} \\
\Leftrightarrow\quad &\alpha\vartheta \;=\; \frac{\beta}{2} + \frac{f\sqrt{d_E}}{2}\,.
\end{aligned}$$

Damit gilt

$$\varepsilon \begin{pmatrix} \vartheta \\ 1 \end{pmatrix} = P \begin{pmatrix} \vartheta \\ 1 \end{pmatrix}.$$

Nun wollen wir noch zeigen, dass P die Form

$$P = \prod_{i=1}^{s} \begin{pmatrix} c_i' & 1 \\ 1 & 0 \end{pmatrix}$$

hat. Da ϑ reduziert ist, gilt (wie im Beweis von Satz 3.28)

$$0 < \beta < f\sqrt{D} \quad \text{und} \quad \frac{-\beta + f\sqrt{d_E}}{2} < \alpha < \frac{\beta + f\sqrt{d_E}}{2}$$
$$\Rightarrow \quad -\beta > -f\sqrt{d_E}, \beta + 2\alpha > f\sqrt{d_E} \text{ und } -2\alpha + \beta > -f\sqrt{d_E}\,.$$

Mit $\varepsilon > 1$ folgt

$$q^* = \frac{u - v\beta}{2} > \frac{u - vf\sqrt{d_E}}{2} = \sigma(\varepsilon) = \frac{\mathcal{N}(\varepsilon)}{\varepsilon}$$
$$> \begin{cases} 0, & \text{falls } \mathcal{N}(\varepsilon) = 1 \\ -1, & \text{falls } \mathcal{N}(\varepsilon) = -1 \end{cases},$$
$$q - q^* = \frac{-u + (2\alpha + \beta)v}{2} > \frac{-u + vf\sqrt{d_E}}{2} = -\sigma(\varepsilon) = -\frac{\mathcal{N}(\varepsilon)}{\varepsilon}$$
$$> \begin{cases} -1, & \text{falls } \mathcal{N}(\varepsilon) = 1 \\ 0, & \text{falls } \mathcal{N}(\varepsilon) = -1 \end{cases},$$

und

$$p - q = \frac{u - (2\alpha - \beta)v}{2} > \frac{u - vf\sqrt{d_E}}{2} = \sigma(\varepsilon) = \frac{\mathcal{N}(\varepsilon)}{\varepsilon}$$
$$> \begin{cases} 0, & \text{falls } \mathcal{N}(\varepsilon) = 1 \\ -1, & \text{falls } \mathcal{N}(\varepsilon) = -1 \end{cases}.$$

Daraus folgt

$$0 < q^* \leq q, \quad \frac{p}{q} > 1 \quad \text{für} \quad \mathcal{N}(\varepsilon) = 1$$

und

$$0 \leq q^* < q, \quad \frac{p}{q} \leq 1 \quad \text{für} \quad \mathcal{N}(\varepsilon) = -1.$$

Nun werden $c'_0, \ldots, c'_s$ definiert:

1.Fall: $\frac{p}{q} = 1$: Das geht nur, falls $\mathcal{N}(\varepsilon) = -1$. Wir setzen $c'_0 = 1$ und $t = 0$. Da $\det(P) = \mathcal{N}(\varepsilon) = -1$ ist, ist $\mathrm{ggT}(p, q) = 1$, also $p = q = 1$ und $q^* = 0$. Dann bleibt noch $p^* = -\det(P) = 1$.

2.Fall: $\frac{p}{q} > 1$: Da $\frac{p}{q}$ rational ist, habe es die endliche Kettenbruchentwicklung

$$\frac{p}{q} = [b_0, \ldots, b_s] = [b_0, \ldots, b_{s-1}, b_s - 1, 1].$$

Nun soll $\det(P) = \mathcal{N}(\varepsilon)$ gelten. Daher setzen wir $t = s$ und $c'_i = b_i$ für $i = 0 \dots s$, falls $\mathcal{N}(\varepsilon) = (-1)^{s+1}$ und $t = s+1$ und $c'_i = b_i$ für $i = 0 \dots s-1$, sowie $c'_s = b_s - 1$ und $c'_{s+1} = 1$ falls $\mathcal{N}(\varepsilon) = (-1)^s$. Dann folgt

$$\det(P) = pq^* - qp^* = (-1)^t.$$

Sei nun

$$P'_t = \begin{pmatrix} p'_t & p'_{t-1} \\ q'_t & q'_{t-1} \end{pmatrix} := \prod_{i=0}^{s} \begin{pmatrix} c'_i & 1 \\ 1 & 0 \end{pmatrix}.$$

Dann gilt

$$p'_t q'_{t-1} - p'_{t-1} q'_t = (-1)^t$$

und nach Definition der c'_i

$$\frac{p}{q} = [c'_0, \dots, c'_t] = \frac{p'_t}{q'_t}.$$

Da $\mathrm{ggT}(p,q) = 1$ und $\mathrm{ggT}(p'_t, q'_t) = 1$ und weil $p, q > 0$ sind (da $u, b, v, a > 0$), gilt $p = p'_t, q = q'_t$. Deshalb gilt

$$\begin{aligned} & pq'_{t-1} - p'_{t-1} q = (-1)^t = pq^* - p^* q\,, \\ \Leftrightarrow \quad & p(q_{t-1} - q^*) = q(p'_{t-1} - p^*) \\ \overset{\mathrm{ggT}(p,q)=1}{\Leftrightarrow} \quad & q \mid (q_{t-1} - q^*)\,. \end{aligned}$$

$0 < q^* < q$: Wegen $0 \le q'_{t-1} \le q_t = q$ gilt

$$|q^* - q_{t-1}| \le |q^* - q| \le q - 1 < q\,.$$

Da aber $q \mid (q_{t-1} - q^*)$ gilt, muss $(q_{t-1} - q^*) = 0$ sein. Also folgt $q_{t-1} = q^*$ und $p'_{t-1} = p^*$.

$0 < q^* = q$: Dann ist $1 = \mathcal{N}(\varepsilon) = pq - p^*q = q(p - p^*)$. Da $q, p > 0$ sind, folgt $q = q^* = 1$ und deshalb $\frac{p}{q} = p = \lfloor p \rfloor$. Daraus ergibt sich $t = 1$ und $q'_0 = 1 = q^*$ und damit $p^* = p'_0$.

$q^* = 0$: In diesem Fall ist $\mathcal{N}(\varepsilon) = -1$. Wegen $-1 = \mathcal{N}(\varepsilon) = -p^*q$ folgt $q = 1$. Deshalb folgt wieder $\frac{p}{q} = p = \lfloor p \rfloor$. Da $\mathcal{N}(\varepsilon) = -1$ setzen wir $t = 1, q'_{t-1} = q'_{-1} = 0$ und $p'_{t-1} = p^* = 1$.

Also gilt insgesamt $p^* = p'_{t-1}$ und $q^* = q'_{t-1}$. P erfüllt also alle Voraussetzungen und, wie zu Beginn des Beweises erklärt, können wir nun

$$P = P_k^h \quad \text{und damit} \quad \varepsilon = \varepsilon_0^h$$

folgern. □

Damit folgt nun der Beweis von Satz 3.43:

Beweis: (von Satz 3.43)
Im Beweis von Lemma 3.44 haben wir schon gesehen, dass von den Einheiten $\pm\varepsilon$ und $\pm\sigma(\varepsilon) = \pm\frac{1}{\varepsilon}$ genau eine grösser als 1 ist. Diese können wir wegen Satz 3.46 und Satz 3.47 durch $\varepsilon_0 = q_k\vartheta + q_{k-1}$ darstellen. □

3.48 Satz (Dirichletscher Einheitensatz für reell-quadratische Zahlkörper)
Ist $d > 0$ quadratfrei und $\mathcal{O} \subseteq \mathcal{O}_{\mathbb{Q}[\sqrt{d}]}$ eine Ordnung, dann gilt

$$\mathcal{O}^* = \langle -1 \rangle \times \langle \varepsilon_0 \rangle \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}\,.$$

3.49 Bemerkung
Der „Dirichletscher Einheitensatz“ gilt in einer verallgemeinerten Fassung für alle Zahlkörper.

Literaturverzeichnis

[Chr92] A. Christian. *Vorlesung Elementare Zahlentheorie von Prof. Dr. B.H. Matzat.* SoSe 1992.

[Koc97] Helmut Koch. *Zahlentheorie: Algebraische Zahlen und Funktionen.* Vieweg studium, 1997.

[Neb10] Gabriele Nebe. *Skript zur Computeralgebra.* RWTH Aachen, SoSe 2010.

[Sch07] Alexander Schmidt. *Einführung in die algebraische Zahlentheorie.* Springer, 2007.