Quadratische Zahlkörper

Clara Nadenau

15.10.2010

Die meisten Aussagen und Beweise des Vortrags stammen aus KOCH: Zahlentheorie, algebraische Zahlen und Funktionen.

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 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 $\mathbb{Q}[\sqrt{d}]$.

3 Bemerkung

1. Die Norm $\mathcal{N}$ ist als Produkt von zwei Homomorphismen (Identität und Konjugation) multiplikativ, d.h. $\mathcal{N}(a \cdot b) = \mathcal{N}(a) \cdot \mathcal{N}(b)$.
2. In imaginärquadratischen Zahlkörpern gilt $\mathcal{N}(a) > 0$ für alle $a \in \mathbb{Q}[\sqrt{d}] \setminus \{0\}$.

4 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*.

5 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.

6 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 $P(a) = 0$.

7 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.

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

9 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.

10 Lemma
Sei A eine $(r \times r)$-Matrix über einem kommutativem Ring R mit Eins, $x \in R^n$ ein Vektor. Dann gilt:

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

11 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.

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

13 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 $a \in \mathbb{Q}[\sqrt{d}] \setminus \mathbb{Q}$.

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

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

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

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

17 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:

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

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

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

19 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

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

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.

20 Bemerkung
Sei $[c_0, c_1, \ldots]$ die Kettenbruchentwicklung von α. Dann gilt: $r_i = c_i + \frac{1}{r_{i+1}}$.

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

Zusammenhang mit dem euklidischen Algorithmus: Seien $a, b \in \mathbb{Z}$ mit $\mathrm{ggT}(a,b) = 1$ und $\alpha := \frac{a}{b}$.

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

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

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

23 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

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

24 Lemma
Sei $\alpha = [c_0, c_1, \ldots] \in \mathbb{R}$. Dann können wir r_i darstellen durch

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

wobei

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

25 Definition
Seien A_i wie im obigen Lemma. 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 $i = 0, 1, 2, \ldots$:

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

26 Satz
Die Zahl $\alpha > 1$ habe die Näherungsbrüche $[c_0, \ldots c_n]$, dann gilt

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

27 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 $[a_0, a_1, \ldots]$.

28 Definition (periodische Kettenbrüche)
Der Kettenbruch einer irrationalen 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.

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

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

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

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

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.

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 $\mathbb{Q}[\sqrt{d}]$.

35 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.

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

37 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 $\mathcal{O}$.

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

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

39 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.

40 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.

41 Satz (Dirichlet)
Ist $d > 0$ quadratfrei und $\mathcal{O} \subseteq \mathcal{O}_{\mathbb{Q}[\sqrt{d}]}$ eine Ordnung, dann gilt

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