Seminar

Funktionentheorie

Sommersemester 2004
Universität Heidelberg

Zetafunktionen und quadratische Zahlkörper

Vortrag von

Hans Joachim Ferreau, Christian Kirches, Christian Schinnagel

12. Juli 2004

Inhaltsverzeichnis

Symbole

K	Quadratischer Zahlkörper (über $\mathbb{Q}$)
$\mathfrak{D}$	Ring der ganzen Zahlen eines quadratischen Zahlkörpers K
$\zeta(s)$	RIEMANN'sche Zetafunktion
$\zeta_K(s)$	DEDEKIND'sche Zetafunktion des quadratischen Zahlkörpers K
$\mathfrak{o}$	Nullideal von $\mathfrak{D}$
$\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$	Ideale von $\mathfrak{D}$
$\mathfrak{p}$, $\mathfrak{p}_i$	Primideale von $\mathfrak{D}$
$\mathfrak{P}$	Menge aller Primideale von $\mathfrak{D}$
$\mathbb{P}$	Menge aller natürlichen Primzahlen
$\langle\xi\rangle$	Das von ξ erzeugte Hauptideal
$\overline{\xi}$	Das in K konjugierte von ξ
D	Diskriminante des Rings $\mathfrak{D}$
$D(\mathfrak{a})$	Diskriminante eines Ideals $\mathfrak{a} \subseteq \mathfrak{D}$
$\mathcal{N}$	Norm eines Elements aus K oder eines Ideals von $\mathfrak{D}$
$\mathcal{S}$	Spur eines Elements aus K
χ_D	DIRICHLET'scher Charakter

1 Quadratische Zahlkörper

Wir führen in diesem Abschnitt einige Hauptatsachen über quadratische Zahlkörper ein.

Definition 1.1 Quadratischer Zahlkörper
Sei K ein Körper, $\mathbb{Q} \subset K$ und $[K : \mathbb{Q}] = 2$. Dann heißt K ein* quadratischer Zahlkörper.

K lässt sich dann schreiben als

$$K = \mathbb{Q}(\sqrt{d}), \quad d \in \mathbb{Z}. \tag{1.1}$$

Dabei setzt man d als *quadratfrei* voraus, d. h. d soll kein Quadrat als Teiler enthalten. Andernfalls wäre

$$d = x^2 d', x \in \mathbb{N}, \quad \text{und} \quad \mathbb{Q}(\sqrt{d}) = \mathbb{Q}(\sqrt{x^2 d'}) = \mathbb{Q}(x\sqrt{d'}) = \mathbb{Q}(d'),$$

und, falls d selbst ein Quadrat wäre

$$\mathbb{Q}(\sqrt{d}) = \mathbb{Q}.$$

Da $\sqrt{d}$ algebraisch über $\mathbb{Q}$ ist, besitzt jede Zahl $x \in K$ eine eindeutige Darstellung

$$x = \alpha + \beta\sqrt{d} \quad \text{mit } \alpha, \beta \in \mathbb{Q}. \tag{1.2}$$

Für $d < 0$ heißt K auch *imaginärquadratisch*, für $d > 0$ *reellquadratisch*. Nur auf reellquadratischen Körpern lässt sich eine Ordnungsrelation definieren, diese sind Teilmengen von $\mathbb{R}$. Imaginärquadratische Körper dagegen enthalten komplexe Elemente.

Definition 1.2 Konjugiertes in K
Unter dem Konjugierten *der Zahl $a = \alpha + \beta\sqrt{d} \in K$ versteht man die Zahl*

$$\overline{a} = \alpha - \beta\sqrt{d}.$$

In einem imaginärquadratischen Körper stimmt dieser Begriff mit dem komplex Konjugierten in $\mathbb{C}$ überein.

*Dies bedeutet, dass K ein zweidimensionaler $\mathbb{Q}$-Vektorraum ist.

Definition 1.3 Ring der ganzen Zahlen in K
Mit $\mathfrak{D} \subset K$ bezeichnet man den Ring derjenigen Zahlen aus K, welche eine Gleichung mit Koeffizienten in $\mathbb{Z}$ und höchstem Koeffizienten 1 erfüllen. Man nennt solche Zahlen „ganz“. Der Ring $\mathfrak{D}$ wird auch als Hauptordnung *von K bezeichnet.*

Wir bestimmen die Elemente dieses Rings explizit. Da die Körpererweiterung den Grad zwei hat, reicht es aus, die Lösungsmenge einer quadratischen Gleichung zu betrachten:

$$x^2 - sx + n = 0$$

ist erfüllt für

$$s = x + \overline{x} \quad \text{und} \quad n = x\overline{x}$$

Nach Definition 1.3 ist $x \in \mathfrak{D}$ genau dann, wenn $s, n \in \mathbb{Z}$ sind, also

$$x + \overline{x} = 2\alpha \in \mathbb{Z} \quad \text{und} \quad x\overline{x} = \alpha^2 - \beta^2 d \in \mathbb{Z}.$$

Aus

$$\begin{aligned} (2\beta)^2 d &= 4\alpha^2 - 4\alpha^2 + 4\beta^2 d \\ &= (\underbrace{2\alpha}_{\in\mathbb{Z}})^2 - 4(\underbrace{\alpha^2 - \beta^2 d}_{\in\mathbb{Z}}) \end{aligned}$$

folgt $(2\beta)^2 d \in \mathbb{Z}$. Weil d als quadratfrei vorausgesetzt wurde, folgt $2\beta \in \mathbb{Z}$. Setze nun

$$a = 2\alpha, \quad b = 2\beta, \quad x = \frac{a + b\sqrt{d}}{2}, \quad a, b \in \mathbb{Z} \text{ mit } a^2 - b^2 d \equiv 0 (mod\ 4).$$

Die letzte Kongruenz ist erfüllt

für $d \equiv 1 (mod\ 4)$	genau dann, wenn	$a \equiv b (mod\ 2)$.
für $d \equiv 2, 3 (mod\ 4)$	genau dann, wenn	a, b gerade sind, also $\alpha, \beta \in \mathbb{Z}$

Korollar 1.4
Der Ring $\mathfrak{D}$ besteht folglich aus den Elementen

$$\mathfrak{D} = \begin{cases} \mathbb{Z} + \mathbb{Z}\sqrt{d} & \text{falls } d \equiv 2, 3 (mod\ 4), \\ \mathbb{Z} + \mathbb{Z}\frac{1+\sqrt{d}}{2} & \text{falls } d \equiv 1 (mod\ 4) \end{cases} \tag{1.3}$$

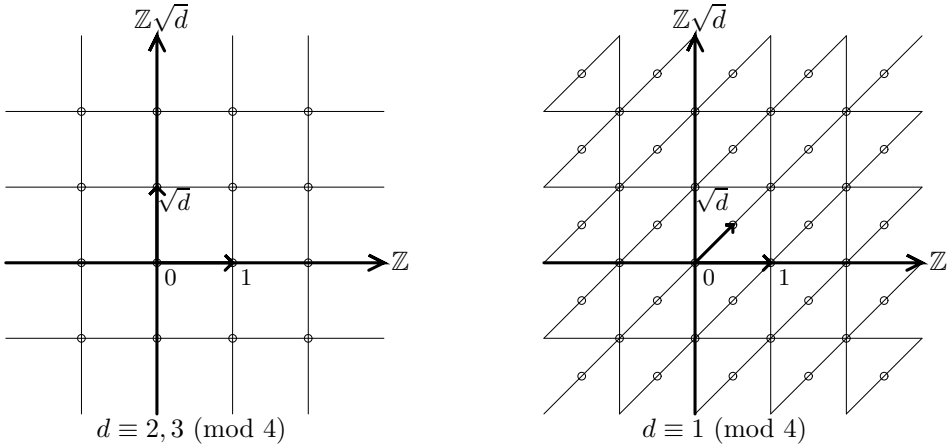

Abbildung 1: Veranschaulichung der Elemente von $\mathbb{Q}(\sqrt{d})$ als Gitterpunkte in der Ebene.

Definition 1.5 Spur und Norm in K
Sei $x \in K$. Man nennt

$$\begin{aligned} \mathcal{S}: &\quad K \to \mathbb{Q}, \quad x \mapsto x + \overline{x} \quad \text{die Spur von } x, \\ \mathcal{N}: &\quad K \to \mathbb{Q}, \quad x \mapsto x\overline{x} \quad \text{die Norm von } x. \end{aligned} \tag{1.4}$$

$\mathcal{S}$ und $\mathcal{N}$ sind additiv und multiplikativ, wie man durch elementares Nachrechnen zeigt.

Definition 1.6 Diskriminante von K
Als Diskriminante *des Körpers K bezeichnet man den Wert*

$$\left|\begin{pmatrix} \alpha & \beta \\ \overline{\alpha} & \overline{\beta} \end{pmatrix}\right|^2, \quad \mathfrak{D} = \alpha\mathbb{Z} + \beta\mathbb{Z}, \tag{1.5}$$

wobei (α, β) eine Basis des Rings $\mathfrak{D} \subset K$ bilden. Die Diskriminante ist von der Wahl der Basis unabhängig.

Beweis:
$(1, \psi)$ ist die Basis von $\mathfrak{D}$ aus Korollar 1.4, und man errechnet die Diskriminante

$$\left|\begin{pmatrix} 1 & \psi \\ 1 & \overline{\psi} \end{pmatrix}\right|^2 = (\overline{\psi} - \psi)^2.$$

Sei nun $(\lambda_1 + \mu_1\psi, \lambda_2 + \mu_2\psi)$ eine weitere Basis von $\mathfrak{D}$, dann errechnet man

$$\left|\begin{pmatrix} \lambda_1 + \mu_1\psi & \lambda_2 + \mu_2\psi \\ \lambda_1 + \mu_1\overline{\psi} & \lambda_2 + \mu_2\overline{\psi} \end{pmatrix}\right|^2 = (\lambda_1\mu_2 - \lambda_2\mu_1)^2(\overline{\psi} - \psi)^2.$$

Interpretiert man beide Basen als Gitter in $\mathbb{C}$, so gilt bekanntlich für die Matrix welche die Gitter ineinander überführt

$$\begin{pmatrix} \lambda_1 & \mu_1 \\ \lambda_2 & \mu_2 \end{pmatrix} \in SL(2, \mathbb{Z}), \qquad \det\begin{pmatrix} \lambda_1 & \mu_1 \\ \lambda_2 & \mu_2 \end{pmatrix} = \lambda_1\mu_2 - \lambda_2\mu_1 = 1,$$

und die Diskriminanten sind identisch.

□

Man findet also o. B. d. A. mit der Basis aus Korollar 1.4 die Diskriminanten

$$\begin{aligned} D = 4d \quad &\text{falls} \quad d \equiv 2,\ 3 \pmod 4 \\ D = d \quad &\text{falls} \quad d \equiv 1 \pmod 4. \end{aligned} \tag{1.6}$$

Beweis:
Für d ist

$$\begin{aligned} \left|\begin{pmatrix} 1 & \psi \\ 1 & \overline{\psi} \end{pmatrix}\right|^2 &= (\overline{\psi} - \psi)^2 \\ &= \left(\sqrt{d} - (-\sqrt{d})\right)^2 = 4d && \text{für } d \equiv 2,\ 3 \pmod 4 \\ &= \left(\frac{1}{2} + \frac{1}{2}\sqrt{d} - \left(\frac{1}{2} - \frac{1}{2}\sqrt{d}\right)\right)^2 = d && \text{für } d \equiv 1 \pmod 4 \end{aligned}$$

Diese entsprechen exakt den in [Za, §5] definierten *Fundamentaldiskriminanten*, folglich lässt sich jeder quadratische Körper eindeutig als $\mathbb{Q}(\sqrt{D})$ mit einer Fundamentaldiskriminante D schreiben.

Definition 1.7 Einheit
Sind $a, b \in \mathfrak{D}$ mit

$$ab = 1$$

so nennt man a und b Einheiten *des Rings $\mathfrak{D}$. Offensichtlich sind in einem Körper alle Elemente mit Ausnahme der 0 Einheiten.*

Wir wollen die Einheiten des Rings $\mathfrak{D} \subset \mathbb{Q}(\sqrt{d})$ bestimmen. Sei also $x + y\sqrt{d} \in \mathfrak{D}$ eine Einheit.

Entsprechend der Basisdarstellung sind x, y wie folgt zu wählen:

$$\begin{aligned} x,\ y \in \mathbb{Z} \quad &\text{für} \quad d \equiv 2, 3 \pmod 4 \\ 2x,\ 2y,\ x + y \in \mathbb{Z} \quad &\text{für} \quad d \equiv 1 \pmod 4 \end{aligned}$$

Nach Definition existiert eine Zahl $u + v\sqrt{d}$ so dass

$$(x + y\sqrt{d})(u + v\sqrt{d}) = 1.$$

Da notwendig $xv + yu = 0$ gilt, folgt, dass auch $x - y\sqrt{d}$ eine Einheit ist, denn

$$(x - y\sqrt{d})(u - v\sqrt{d}) = 1.$$

Dann ist auch

$$(x + y\sqrt{d})(x - y\sqrt{d}) = x^2 - dy^2 \in \mathbb{Z}$$

eine Einheit und man erhält, da $\mathbb{Z}$ nur die Einheiten ± 1 hat, die FERMAT'sche Gleichung

$$x^2 - dy^2 = \pm 1.$$

Umgekehrt ist $x + y\sqrt{d}$ Einheit falls diese FERMAT'sche Gleichung erfüllt ist.

Entsprechend einem Ergebnis aus $[Za, §8]$ haben wird dann folgendes Ergebnis für die Einheiten von $\mathfrak{D}$:

$d = -1$	$1, i, -1, -i$
$d = -3$	$1, \varepsilon, \varepsilon^2, \ldots, \varepsilon^5 \quad$ mit $\varepsilon = \exp\left(\frac{2\pi i}{6}\right)$
$d < 0,\ d \neq -1, -3$	$1, -1$
$d > 0$	$\pm\varepsilon^k,\ k \in \mathbb{Z},\ \varepsilon$ eine Grundeinheit

2 Ideale und Primfaktorzerlegung

Es werden einige grundlegende Tatsachen über Ideale eingeführt, und deren Eigenschaften in den Ringen $\mathfrak{D}$ untersucht. Dieser Abschnitt richtet sich weitgehend nach [ST].

Primfaktorzerlegungen von Idealen

Definition 2.1 (Ganzes) Ideal
Ein Ideal *von $\mathfrak{D}$ ist eine additive Untergruppe $\mathfrak{a} \subseteq \mathfrak{D}$ welche folgende Bedingung erfüllt:*

$$\forall\, \lambda \in \mathfrak{D},\ \alpha \in \mathfrak{a} :\ \lambda\alpha \in \mathfrak{a}. \tag{2.1}$$

Zusätzlich zur additiven Gruppenstruktur ist $\mathfrak{a}$ also auch unter der Multiplikation mit Skalaren aus $\mathfrak{D}$ abgeschlossen.

Definition 2.2 Produktideal
Sind $\mathfrak{a}, \mathfrak{b}$ Ideale, so ist das Produktideal $\mathfrak{ab}$ *durch*

$$\mathfrak{ab} = \left\{ \sum_{i=1}^{r} a_i b_i \;\middle|\; a_i \in \mathfrak{a},\, b_i \in \mathfrak{b},\, r \in \mathbb{N} \right\} \tag{2.2}$$

erklärt. Es ist das kleinste Ideal, welches alle Produkte ab mit $a \in \mathfrak{a}$, $b \in \mathfrak{b}$ enthält.

Definition 2.3 Hauptideal
Ein beliebiges Element $\xi \in \mathfrak{D}$ ($\xi \in K$) erzeugt das (gebrochene, → Definition 2.11) Ideal

$$\langle \xi \rangle := \left\{ \lambda\xi \;\middle|\; \lambda \in \mathfrak{D} \right\}, \tag{2.3}$$

es heißt das von ξ erzeugte Hauptideal. Dabei ist ξ bis auf eine Einheit aus $\mathfrak{D}$ (aus K) eindeutig bestimmt.

Ein Ring in welchem jedes Ideal sofort Hauptideal ist, d. h. von genau einem Element erzeugt wird, wird Hauptidealring genannt.

Korollar 2.4 Produkt von Hauptidealen
Sind $\xi, \eta \in K$, $\langle \xi \rangle$ und $\langle \eta \rangle$ Hauptideale, so gilt

$$\langle \xi\eta \rangle = \langle \xi \rangle \langle \eta \rangle \tag{2.4}$$

Beweis:
$\subseteq$: Sei $\lambda\xi\eta$, $\lambda \in \mathfrak{D}$, ein beliebiges Element aus $\langle \xi\eta \rangle$. Dann besitzt es wegen $a_1 := \lambda\xi \in \langle \xi \rangle$ und $b_1 := \eta \in \langle \eta \rangle$ die nachfolgende Darstellung und liegt somit in $\langle \xi \rangle \langle \eta \rangle$

$$\lambda\xi\eta = \sum_{i=1}^{1} a_i b_i.$$

$\supseteq$: Ein beliebiges Element aus $\langle \xi \rangle \langle \eta \rangle$ hat die nachfolgende Darstellung, folglich liegt jeder Summand und damit auch die ganze Summe x in $\langle \xi\eta \rangle$.

$$x = \sum_{i=1}^{r} \underbrace{a_i}_{\lambda_i \xi} \underbrace{b_i}_{\mu_i \eta} = \sum_{i=1}^{r} \lambda_i \mu_i \xi\eta\,, \quad \lambda_i,\, \mu_i \in \mathfrak{D}\,.$$

□

Definition 2.5 Maximales Ideal
Ein Ideal $\mathfrak{a} \subsetneq \mathfrak{D}$ heißt maximal, *wenn es* echt *ist ($\mathfrak{a} \neq \mathfrak{o}, \mathfrak{a} \neq \mathfrak{D}$) und zwischen $\mathfrak{a}$ und $\mathfrak{D}$ selbst keine weiteren Ideale liegen.*

Definition 2.6 Primideal
Ein Ideal $\mathfrak{a} \subsetneq \mathfrak{D}$ *heißt* prim*, wenn für alle Ideale* $\mathfrak{b}, \mathfrak{c} \subseteq \mathfrak{D}$ *mit* $\mathfrak{bc} \subseteq \mathfrak{a}$ *gilt:*

$$\mathfrak{b} \subseteq \mathfrak{a} \quad \textit{oder} \quad \mathfrak{c} \subseteq \mathfrak{a}.$$

Lemma 2.7
In allgemeinen Ringen R *gilt*

1. $\mathfrak{a}$ *ist ein maximales Ideal genau dann wenn* $R/\mathfrak{a}$ *ein Körper ist.*
2. $\mathfrak{a}$ *ist ein Primideal genau dann, wenn* $R/\mathfrak{a}$ *ein Integritätsring (ein nullteilerfreier Ring) ist.*

Beweis: *Elementare Algebra, z. B. [Bo, p. 40].*

Korollar 2.8 Maximale Ideale sind prim
In allgemeinen Ringen R *ist jedes maximale Ideal auch Primideal.*

Satz 2.9 Ideale sind endlich erzeugt
Jedes Ideal $\mathfrak{a} \subsetneq \mathfrak{D}$ *ist endlich erzeugt, d. h. es existieren* $\alpha_1, \ldots, \alpha_n$, $n \in \mathbb{N}$ *mit* $\mathfrak{a} = \mathbb{Z}\alpha_1 + \ldots + \mathbb{Z}\alpha_n$.

Beweis:
Es ist $(\mathfrak{D}, +)$ *eine abelsche Gruppe mit der Eigenschaft, das jedes Element aus* $\mathfrak{D}$ *eindeutig als Linearkombination der Länge* 2 *dargestellt werden kann (*$(\mathfrak{D}, +)$ *ist eine freie abelsche Gruppe vom Rang* 2*).*
Ist $\mathfrak{a}$ *ein Ideal, so ist* $(\mathfrak{a}, +)$ *ebenfalls eine abelsche Gruppe und die Länge der Linearkombination ist höchstens* 2*. Jede* $\mathbb{Z}$*-Basis von* $(\mathfrak{a}, +)$ *erzeugt also* $\mathfrak{a}$ *als Ideal, jedes Ideal von* $\mathfrak{D}$ *ist damit endlich erzeugt.* □

Satz 2.10 Primideale in $\mathfrak{D}$ sind maximal
Jedes Primideal $\mathfrak{a} \neq \mathfrak{o}$ *in* $\mathfrak{D}$ *ist auch maximal in* $\mathfrak{D}$*. Dies gilt in allgemeinen Ringen nicht !*

Beweis:
Sei also $\mathfrak{a} \neq \mathfrak{o}$ *ein Ideal von* $\mathfrak{D}$ *und sei* $0 \neq \alpha \in \mathfrak{p}$*. Sei* $N := \alpha\overline{\alpha}$*. Sicher ist* $N \in \mathfrak{p}$*, da* $\alpha \in \mathfrak{p}$ *ist, und folglich muss* $\langle N \rangle \subseteq \mathfrak{p}$ *gelten. Folglich ist* $\mathfrak{D}/\mathfrak{p}$ *ein Quotientenring von* $\mathfrak{D}/\langle N \rangle$*. Jener ist aber endlich, da er eine endlich erzeugte abelsche Gruppe von Elementen endlicher Ordnung ist. Daher ist auch* $\mathfrak{D}/\mathfrak{p}$ *endlich, und nach Lemma 2.7 ein Integritätsring. Endliche Integritätsringe sind aber bereits Schiefkörper, die Kommutativität ist in unserem Fall klar, gilt aber auch allgemein (Satz von* Wedderburn*). Folglich ist* $\mathfrak{p}$ *wieder nach Lemma 2.7 maximal.* □

Gebrochene Ideale

Die Multiplikation von ganzen Idealen aus $\mathfrak{D}$ ist assoziativ und kommutativ, $\mathfrak{D}$ selbst das neutrale Element. Inverse zu den ganzen Idealen aus $\mathfrak{D}$ sind mit den bisher eingeführten Begriffen noch nicht zu beschreiben, wir erhalten also noch keine multiplikative Gruppenstruktur. Diese zu erlangen motiviert die Einführung von gebrochenen Idealen.

Definition 2.11 Gebrochenes Ideal
Eine additive Untergruppe von K *(nicht mehr* $\mathfrak{D}$ *!) heißt ein* gebrochenes Ideal *von* $\mathfrak{D}$*, falls ein Element* $c \in K$ *existiert so dass* $\mathfrak{b} = c\mathfrak{a}$ *ein ganzes Ideal von* $\mathfrak{D}$ *ist.*

Das gebrochene Ideal $\mathfrak{a}$ besitzt dann die Darstellung $\mathfrak{a} = c^{-1}\mathfrak{b}$ und ist eine Teilmenge von K.

In Hauptidealringen sind gebrochene Ideale nur von geringem Interesse, denn sie sind von der einfachen Form

$$c^{-1}\langle d \rangle = (c^{-1}d)\mathfrak{D} = \alpha\mathfrak{D}, \quad \text{mit } \alpha \in K.$$

Tatsächlich sind aber nur sehr wenige Ringe $\mathfrak{D}$ auch Hauptidealringe (→ Bemerkung 2.22).

Satz 2.12 Die Gruppe gebrochener Ideale
Die gebrochene Ideale von $\mathfrak{D}$ bilden eine multiplikative abelsche Gruppe.

Wir zeigen diesen Satz zusammen mit dem wichtigsten Resultat dieses Abschnitts:

Satz 2.13 Eindeutige Primidealzerlegung in $\mathfrak{D}$
Jedes nichttriviale Ideal von $\mathfrak{D}$ besitzt eine bis auf die Reihenfolge eindeutige Darstellung als Produkt von Primidealen von $\mathfrak{D}$.

Der Beweis dieser beiden Sätze erfolgt in mehreren Schritten und wird einige weitere wichtige Resultate liefern:

Schritt 1: *Sei $\mathfrak{a} \neq \mathfrak{o}$ ein Ideal von $\mathfrak{D}$. Dann existieren Primideale $\mathfrak{p}_1, \ldots, p_r$ von $\mathfrak{D}$ so dass $\mathfrak{p}_1 \cdots \mathfrak{p}_r \subseteq \mathfrak{a}$.*

Beweis durch Widerspruch:

Gelte dies nicht. Dann können wir $\mathfrak{a}$ in $\mathfrak{D}$ maximal wählen, unter der Einschränkung dass solche Primideale nicht existieren. $\mathfrak{a}$ ist dann nicht prim, sonst wäre mit $\mathfrak{p}_1 = \mathfrak{a}$ der Widerspruch bereits gefunden. Nach Negation von Definition 2.6 existieren also Ideale $\mathfrak{b}, \mathfrak{c}$ von $\mathfrak{D}$ mit $\mathfrak{bc} \subseteq \mathfrak{a}$,$b \nsubseteq \mathfrak{a}$, $c \nsubseteq \mathfrak{a}$. Seien nun Ideale

$$\mathfrak{a}_1 := \mathfrak{a} + \mathfrak{b}, \quad \mathfrak{a}_2 := \mathfrak{a} + \mathfrak{c}$$

definiert. Dann gilt $\mathfrak{a}_1\mathfrak{a}_2 \subseteq \mathfrak{a}$ und $\mathfrak{a}_1, \mathfrak{a}_2 \supsetneq \mathfrak{a}$. Da $\mathfrak{a}$ maximal ist, existieren wegen Korollar 2.8 Primideale $\mathfrak{p}_1, \ldots, \mathfrak{p}_s, \mathfrak{p}_{s+1}, \ldots, p_r$ so dass

$$\begin{aligned} \mathfrak{p}_1 \cdots \mathfrak{p}_s &\subseteq \mathfrak{a}_1 \\ \mathfrak{p}_{s+1} \cdots \mathfrak{p}_r &\subseteq \mathfrak{a}_2 \end{aligned}$$

Damit folgt aber im Widerspruch zur Wahl von $\mathfrak{a}$

$$\mathfrak{p}_1 \cdots p_r \subseteq \mathfrak{a}_1\mathfrak{a}_2 \subseteq \mathfrak{a} \quad \lightning.$$

□

Schritt 2:

Definition 2.14 Inverses eines Ideals
Ist $\mathfrak{a}$ ein Ideal von $\mathfrak{D}$, so sei

$$\mathfrak{a}^{-1} := \{x \in K \mid x\mathfrak{a} \subseteq \mathfrak{D}\}.$$

Die Notation deutet an, dass $\mathfrak{a}^{-1}$ das inverse Ideal zu $\mathfrak{a}$ ist; diese Eigenschaft ist aber erst noch zu beweisen.

Beweis: Wir müssen $\mathfrak{a}\mathfrak{a}^{-1} = \mathfrak{D}$ zeigen.

Ist $\mathfrak{a} \neq 0$, so gilt für jedes $c \in \mathfrak{a}$, $c \neq 0$ dass $c\mathfrak{a}^{-1} \subseteq \mathfrak{D}$ ist; folglich ist $\mathfrak{a}^{-1}$ nach Definition 2.11 ein gebrochenes Ideal. Offensichtlich ist $\mathfrak{D} \subseteq \mathfrak{a}^{-1}$, also $\mathfrak{a} = \mathfrak{a}\mathfrak{D} \subseteq \mathfrak{a}\mathfrak{a}^{-1} = \mathfrak{a}^{-1}\mathfrak{a}$. Dies zeigt zunächst, dass $\mathfrak{a}\mathfrak{a}^{-1}$ ein Ideal von $\mathfrak{D}$ ist.

Offensichtlich gilt für Ideale $\mathfrak{a}, \mathfrak{p}$ von $\mathfrak{D}$

$$\mathfrak{a} \subseteq \mathfrak{p} \subseteq \mathfrak{D} \quad \Longleftrightarrow \quad \mathfrak{D} \subseteq \mathfrak{p}^{-1} \subseteq \mathfrak{a}^{-1}.$$

Schritt 3: *Ist $\mathfrak{a}$ echtes Ideal ($\mathfrak{a} \neq \mathfrak{o}$, $\mathfrak{a} \neq \mathfrak{D}$), dann ist $\mathfrak{a}^{-1} \supsetneq \mathfrak{D}$.*

Beweis:

Es ist $\mathfrak{a} \subseteq \mathfrak{p}$ für ein maximales Ideal $\mathfrak{p}$, und $\mathfrak{p}^{-1} \subseteq \mathfrak{a}^{-1}$. Daher genügt es, $\mathfrak{p}^{-1} \neq \mathfrak{D}$ für maximale Ideale $\mathfrak{p}$ zu zeigen; also z. B. ein nicht ganzes Element in $\mathfrak{p}^{-1}$ zu finden.

Beginnend mit einem Element $a \in \mathfrak{p}$, $a \neq 0$, wählt man unter Verwendung von Schritt 1 ein minimales r so dass

$$\mathfrak{p}_1 \cdots \mathfrak{p}_r \subseteq \langle a \rangle$$

für Primideale $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$. Da nun $\langle a \rangle \subseteq \mathfrak{p}$, und $\mathfrak{p}$ selbst prim (weil maximal) ist, liegt mindestens ein $\mathfrak{p}_i$ in $\mathfrak{p}$. Dies sei o. B. d. A. für das Primideal $\mathfrak{p}_1$ der Fall. Dann gilt $\mathfrak{p}_1 = \mathfrak{p}$ da in $\mathfrak{D}$ Primideale gleichzeitig maximal sind (Satz 2.10) und weiter muss gelten

$$\mathfrak{p}_2 \cdots \mathfrak{p}_r \nsubseteq \langle a \rangle$$

da r minimal gewählt ist.

Wir können also ein Element $b \in \mathfrak{p}_2 \cdots \mathfrak{p}_r \setminus \langle a \rangle$ wählen. Wegen $b\mathfrak{p} \subseteq \langle a \rangle$ gilt $b\mathfrak{a}^{-1} \subseteq \mathfrak{D}$ und $ba^{-1} \in \mathfrak{p}^{-1}$. Da aber $b \notin a\mathfrak{D}$, also $ba^{-1} \notin \mathfrak{D}$ gewählt wurde, folgt $p^{-1} \neq \mathfrak{D}$. □

Schritt 4: *Ist* $\mathfrak{a} \neq \mathfrak{o}$ *und* $\mathfrak{a}S \subseteq \mathfrak{a}$ *für jede Teilmenge* $S \subseteq K$*, dann ist* $S \subseteq \mathfrak{D}$*.*

Beweis:

Wir zeigen dass, wenn $a\theta \subseteq \mathfrak{a}$ für ein $\theta \in S$ gilt, $\theta \in \mathfrak{D}$ folgt.

Da jedes Ideal in $\mathfrak{D}$ endlich erzeugt ist, gilt

$$\mathfrak{a} = \langle a_1, \ldots, a_m \rangle$$

wobei nicht alle a_i Null sind. Dann bedeutet $\mathfrak{a}\theta \subseteq \mathfrak{a}$

$$a_i\theta = b_{i1}a_1 + \ldots + b_{im}a_m, \quad i = 1, \ldots, m,\ b_{ij} \in \mathfrak{D}.$$

Da $a_1, \ldots, a_m$ Lösungen von $\det((b_{ij}) - \theta\mathbb{E}) = \chi_B(\theta)$ sind, hat (b_{ij}) eine Determinante ungleich 0 und $\chi_B(\theta)$ ist ein Polynom in θ mit Koeffizienten aus $\mathfrak{D}$, also folgt wegen Definition 1.3 dass $\theta \in \mathfrak{D}$ liegt. □

Schritt 5: *Schluß des Beweises zu Definition 2.14.*

Ist $\mathfrak{p}$ *maximal, so ist* $\mathfrak{p}\mathfrak{p}^{-1} = \mathfrak{D}$*.*

Beweis:

Aus Schritt 2 wissen wir, dass $\mathfrak{p}\mathfrak{p}^{-1}$ ein Ideal ist, und es gilt $\mathfrak{p} \subseteq \mathfrak{p}\mathfrak{p}^{-1} \subseteq \mathfrak{D}$. Da $\mathfrak{p}$ maximal ist, muss $\mathfrak{p}\mathfrak{p}^{-1}$ entweder gleich $\mathfrak{p}$ selbst oder gleich $\mathfrak{D}$ sein. Wäre $\mathfrak{p}\mathfrak{p}^{-1} = \mathfrak{p}$, dann würde nach Schritt 4 $\mathfrak{p}^{-1} \subseteq \mathfrak{D}$ folgen, im Widerspruch zu Schritt 3. Es folgt also $\mathfrak{p}\mathfrak{p}^{-1} = \mathfrak{D}$. □

Erweiterung: Für jedes Ideal $\mathfrak{a} \neq 0$ *ist* $\mathfrak{a}\mathfrak{a}^{-1} = \mathfrak{D}$*.*

Beweis durch Widerspruch:

Gelte dies nicht. Dann wählt man $\mathfrak{a}$ maximal, unter der Bedingung dass $\mathfrak{a}\mathfrak{a}^{-1} \neq \mathfrak{D}$ sein soll. Dann ist $\mathfrak{a} \subseteq \mathfrak{p}$ für ein maximales Ideal $\mathfrak{p}$. Aus Schritt 2 folgt $\mathfrak{D} \subseteq \mathfrak{p}^{-1} \subseteq \mathfrak{a}^{-1}$, also

$$\mathfrak{a} \subseteq \mathfrak{a}\mathfrak{p}^{-1} \subseteq \mathfrak{a}\mathfrak{a}^{-1} \subseteq \mathfrak{D}.$$

Insbesondere bedeutet $\mathfrak{a}\mathfrak{p}^{-1} \subseteq \mathfrak{D}$ dass $\mathfrak{a}\mathfrak{p}^{-1}$ ein Ideal ist. $\mathfrak{a} = \mathfrak{a}\mathfrak{p}^{-1}$ würde aber $\mathfrak{p}^{-1} \subseteq \mathfrak{D}$ nach Schritt 4 bedeuten, und Schritt 3 widersprechen, also gilt $\mathfrak{a} \subsetneq \mathfrak{a}\mathfrak{p}^{-1}$, und da $\mathfrak{a}$ maximal gewählt wurde folgt für das Ideal $\mathfrak{a}\mathfrak{p}^{-1}$

$$\mathfrak{a}\mathfrak{p}^{-1}(\mathfrak{a}\mathfrak{p}^{-1})^{-1} = \mathfrak{D}.$$

Nach Definition von $\mathfrak{a}^{-1}$ bedeutet dies

$$\mathfrak{p}^{-1}(\mathfrak{a}\mathfrak{p}^{-1}) \subseteq \mathfrak{a}^{-1},$$

also

$$\mathfrak{D} = \mathfrak{a}\mathfrak{p}^{-1}(\mathfrak{a}\mathfrak{p}^{-1})^{-1} \subseteq \mathfrak{a}\mathfrak{a}^{-1} \subseteq \mathfrak{D}.$$

□

Damit haben wir der Menge der gebrochenen Ideale von $\mathfrak{D}$ eine multiplikative Gruppenstruktur aufgeprägt, und den ersten offenen Satz 2.12 bewiesen. □

Wir können jetzt den zweiten Satz 2.13 in zwei kurzen Schritten zeigen:

1. Jedes nichttriviale Ideal ist Produkt von Primidealen.

   Gelte dies nicht. Dann wählen wir $\mathfrak{a}$ maximal unter der Einschränkung, nicht Produkt von Primidealen zu sein. Dann ist $\mathfrak{a}$ selbst nicht prim, aber es gilt $\mathfrak{a} \subseteq \mathfrak{p}$ für ein maximales (also primes) Ideal, und wie oben folgt

   $$\mathfrak{a} \subsetneq \mathfrak{a}\mathfrak{p}^{-1} \subseteq \mathfrak{D}.$$

   Aufgrund der Maximalität von $\mathfrak{a}$ gilt für Primideale $\mathfrak{p}_2, \ldots, \mathfrak{p}_r$

   $$\mathfrak{a}\mathfrak{p}^{-1} = \mathfrak{p}_2 \cdots \mathfrak{p}_r,$$

   woraus folgt

   $$\mathfrak{a} = \mathfrak{p}\mathfrak{p}_2 \cdots \mathfrak{p}_r \quad \lightning.$$

2. Diese Faktorisierung ist eindeutig.

   Analog zur Teilbarkeit von Elementen in K definiert man zunächst

   Definition 2.15 Teilbarkeit von Idealen
   Für zwei Ideale $\mathfrak{a}, \mathfrak{b}$ von $\mathfrak{D}$ gilt

   $$\mathfrak{a} \mid \mathfrak{b}$$

   genau dann, wenn es ein Ideal $\mathfrak{c}$ von $\mathfrak{D}$ gibt, so dass

   $$\mathfrak{b} = \mathfrak{a}\mathfrak{c}.$$

   Äquivalent dazu ist die Bedingung

   $$\mathfrak{a} \supseteq \mathfrak{b},$$

   denn nur dann existiert $\mathfrak{c} = \mathfrak{a}^{-1}\mathfrak{b}$.

   Mit der Definition 2.6 des Primideals gilt dann, dass

   $$\mathfrak{p} \mid \mathfrak{a}\mathfrak{b} \Longrightarrow \mathfrak{p} \mid \mathfrak{a} \text{ oder } \mathfrak{p} \mid \mathfrak{b}.$$

   Haben wir nun Primideale $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$, $\mathfrak{q}_1, \ldots, \mathfrak{q}_s$ mit

   $$\mathfrak{p}_1 \cdots \mathfrak{p}_r = \mathfrak{q}_1 \cdots \mathfrak{q}_s,$$

   dann teilt $\mathfrak{p}_1$ mindestens ein $\mathfrak{q}_i$, und aufgrund der Maximalität folgt $\mathfrak{p}_1 = \mathfrak{q}_i$. Durch Multiplikation mit $\mathfrak{p}_1^{-1}$ und Induktion nach r und s folgt die Eindeutigkeit. □

Satz 2.16 Teilbarkeit von Idealen
Für zwei Ideale $\mathfrak{a}, \mathfrak{b}$ von $\mathfrak{D}$ gilt

$$\mathfrak{a} \mid \mathfrak{b} \quad \Longleftrightarrow \quad \mathfrak{a} \supseteq \mathfrak{b}.$$

Dies zeigt, dass die Teiler eines Ideals $\mathfrak{b}$ genau diejenigen Ideale sind, welche $\mathfrak{b}$ enthalten.

Die Norm eines Ideals

Lemma 2.17 ggT und kgV von Idealen
Sind $\mathfrak{a}, \mathfrak{b}$ Ideale von $\mathfrak{D}$ so gilt

$$\begin{aligned} ggT(\mathfrak{a}, \mathfrak{b}) &= \mathfrak{a} + \mathfrak{b} \\ kgV(\mathfrak{a}, \mathfrak{b}) &= \mathfrak{a} \cap \mathfrak{b} \end{aligned}$$

Beweis:
Aus Satz 2.16 wissen wir $\mathfrak{x} \mid \mathfrak{a}$ genau dann, wenn $\mathfrak{x} \supseteq \mathfrak{a}$. Folglich muss $ggT(\mathfrak{a}, \mathfrak{b})$ das kleinste Ideal sein, welches sowohl $\mathfrak{a}$ als auch $\mathfrak{b}$ enthält; dieses ist offensichtlich genau das Ideal $\mathfrak{a} + \mathfrak{b}$.

Ebenso muss $kgV(\mathfrak{a}, \mathfrak{b})$ das größte Ideal sein, welches sowohl in $\mathfrak{a}$ als auch in $\mathfrak{b}$ enthalten ist; dieses ist offensichtlich genau das Ideal $\mathfrak{a} \cap \mathfrak{b}$. □

Definition 2.18 Norm eines Ideals
Aus dem Beweis von Satz 2.9 wissen wir, dass für ein Ideal $\mathfrak{a}$ von $\mathfrak{D}$ der Faktorring $\mathfrak{D}/\mathfrak{a}$ endlich ist. Man definiert die Norm $\mathcal{N}(\mathfrak{a})$ eines Ideals als

$$\mathcal{N}(\mathfrak{a}) = ord(\mathfrak{D}/\mathfrak{a}) \in \mathbb{N}.$$

Korollar 2.19 Norm eines Hauptideals
Ist $\mathfrak{a}$ ein Hauptideal von $\mathfrak{D}$, $\mathfrak{a} = \langle a \rangle$ so gilt

$$\mathcal{N}(\mathfrak{a}) = |\mathcal{N}(a)| = |a\overline{a}|\,.$$

Beweis:
Eine $\mathbb{Z}$-Basis von $\mathfrak{a}$ hat man in $\{aw_1, aw_2\}$. Der Rest folgt aus dem Satz. □

Satz 2.20 Norm-erzeugtes Hauptideal
Ist $\mathfrak{a}$ ein Ideal von $\mathfrak{D}$, $\overline{\mathfrak{a}}$ sein konjugiertes, so erzeugt die Norm von $\mathfrak{a}$ das Produktideal.

$$\langle \mathcal{N}(\mathfrak{a}) \rangle = \mathfrak{a}\overline{\mathfrak{a}}.$$

Beweis, nach [He, Theorem 89]:
Sei $\mathfrak{a} = \langle \alpha_1, \alpha_2 \rangle = \langle \alpha_1 \rangle + \langle \alpha_2 \rangle = ggT(\langle \alpha_1 \rangle, \langle \alpha_2 \rangle)$. Man bildet zu $\mathfrak{a}$ das Polynom

$$P(x) = \alpha_1 x + \alpha_2 x^2$$

und betrachtet das Produkt der Polynome zu beiden Konjugierten

$$f(x) = P(x)\overline{P}(x) = (\alpha_1 x + \alpha_2 x^2)(\overline{\alpha}_1 x + \overline{\alpha}_2 x^2).$$

Dabei seien $\overline{\alpha}_1, \overline{\alpha}_2$ die Erzeugenden von $\overline{\mathfrak{a}}$.

Dieses Polynom hat ganzzahlige Koeffizienten (Nachrechnen), deren ggT wir mit a bezeichnen. Nun ist 1 linear kombinierbar aus den Koeffizienten von $(1/a)f(x)$, also ist $\langle a \rangle$ der ggT der von den Koeffizienten erzeugten Ideale. Daher folgt nach einem Resultat von Gauss *[He]*

$$\mathfrak{a}\overline{\mathfrak{a}} = \langle a \rangle.$$

Offensichtlich haben zueinander konjugierte Ideale identische Norm. Folglich gilt

$$\mathcal{N}(\mathfrak{a})\mathcal{N}(\overline{\mathfrak{a}}) = \mathcal{N}(\mathfrak{a})^2 = \mathcal{N}(\overline{\mathfrak{a}})^2 = |a|^2,$$

und weiter

$$\mathcal{N}(\mathfrak{a}) = \mathcal{N}(\overline{\mathfrak{a}}) = \pm a, \quad \langle \mathcal{N}(\mathfrak{a}) \rangle = \langle \mathcal{N}(\overline{\mathfrak{a}}) \rangle = \langle a \rangle = \mathfrak{a}\overline{\mathfrak{a}}.$$

□

Satz 2.21 Multiplikativität der Norm
Sind $\mathfrak{a} \neq \mathfrak{o}$, $\mathfrak{b} \neq \mathfrak{o}$ Ideale von $\mathfrak{D}$, dann gilt für ihre Normen

$$\mathcal{N}(\mathfrak{ab}) = \mathcal{N}(\mathfrak{a})\mathcal{N}(\mathfrak{b}).$$

Beweis:

$$\langle \mathcal{N}(\mathfrak{ab}) \rangle = (\mathfrak{ab})\,\overline{(\mathfrak{ab})} = (\mathfrak{a}\overline{\mathfrak{a}})\,(\mathfrak{b}\overline{\mathfrak{b}}) = \langle \mathcal{N}(\mathfrak{a}) \rangle \langle \mathcal{N}(\mathfrak{b}) \rangle = \langle \mathcal{N}(\mathfrak{a})\mathcal{N}(\mathfrak{b}) \rangle.$$

□

Bemerkung 2.22 Hauptidealringe, ZPE-Ringe[†]
Die Ringe $\mathfrak{D} \subset \mathbb{Q}(\sqrt{d})$ sind Hauptidealringe für genau folgende quadratfreie $d \in \mathbb{Z}$:

$$-1, -2, -3, -7, -11,$$
$$2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73.$$

In Hauptidealringen ist jedes Ideal bereits ein Hauptideal, wird also von einem Element des Rings alleine erzeugt. Hauptidealringe sind *faktoriell (ZPE-Ringe)*, d. h. es gilt der Satz von der eindeutigen Primfaktorzerlegung.

Darüber hinaus weiß man, dass $\mathbb{Q}(\sqrt{d})$ für genau folgende weitere negative d noch faktoriell ist:

$$-19, -43, -67, -163.$$

Man vermutet, dass es unendlich viele positive d gibt, für welche $\mathfrak{D}$ ebenfalls ein ZPE-Ring ist, von einem Beweis dieser Vermutung ist man jedoch weit entfernt.

[†]Die Angaben sind [Bo, §2.4] entnommen, zu den positiven Fällen siehe [Ha, §16.6]. Einen vollständigen Beweis für die negativen Fälle findet man in [ST].

3 Dedekind'sche Zetafunktion und Darstellungsanzahlen

Definition 3.1 Dedekind'sche Zetafunktion
Wir ordnen einem quadratischen Körper $K = \mathbb{Q}(\sqrt{D})$ die Dirichlet*'sche Reihe*

$$\zeta_K(s) = \sum_{\substack{\mathfrak{a} \subseteq \mathfrak{D} \\ \mathfrak{a} \neq \mathfrak{o}}} \frac{1}{\mathcal{N}(\mathfrak{a})^s} \tag{3.1}$$

zu. Sie heißt Dedekind*'sche Zetafunktion.*

Bemerkung 3.2 Riemann'sche Zetafunktion
Die Riemann*'sche Zetafunktion ist die* Dedekind*'sche Zetafunktion im Spezialfall $K = \mathbb{Q}$.*
Beweis:
Im Falle $K = \mathbb{Q}$ ist $\mathfrak{D} = \mathbb{Z}$. Die Ideale ($\neq \mathfrak{o}$) von $\mathbb{Z}$ haben die Form $n\mathbb{Z}$, $n \in \mathbb{N}$, und es gilt $ord(\mathbb{Z}/n\mathbb{Z}) = n$. Daraus folgt

$$\zeta_{\mathbb{Q}}(s) = \sum_{\substack{n\mathbb{Z} \subseteq \mathbb{Z} \\ n \in \mathbb{N}}} \frac{1}{\mathcal{N}(n\mathbb{Z})^s} = \sum_{n \in \mathbb{N}} \frac{1}{n^s} = \zeta(s) \tag{3.2}$$

□

Satz 3.3
Die Dedekind*'sche Zetafunktion eines quadratischen Zahlkörpers K besitzt die Darstellung*

$$\zeta_K(s) = \prod_{\mathfrak{p} \in \mathfrak{P}} \frac{1}{1 - \mathcal{N}(\mathfrak{p})^{-s}} \,. \tag{3.3}$$

und konvergiert im Bereich $\sigma := \Re e\, s > 1$ absolut. Dabei bezeichnet $\mathfrak{P}$ die Menge aller Primideale des Rings $\mathfrak{D} \subset K$.
Beweis:
Gemäß [Za], p. 30, besitzt die Riemann*'sche Zetafunktion die analoge Darstellung*

$$\zeta(s) = \prod_{\mathfrak{p} \in \mathbb{P}} \frac{1}{1 - p^{-s}} \,. \tag{3.4}$$

(wobei $\mathbb{P} := \{2, 3, 5, \ldots\}$ die Menge der natürlichen Primzahlen bezeichnet). Da jedes Ideal im Ring $\mathfrak{D}$ eine eindeutige *Primidealzerlegung besitzt, ergibt sich die behauptete Darstellung völlig analog zu (3.4), falls eine der beiden Seiten absoulut konvergiert.*

Wir zeigen die absolute Konvergenz für $\sigma > 1$: Wegen

$$\mathfrak{p}\overline{\mathfrak{p}} = \langle \mathcal{N}(\mathfrak{p}) \rangle \quad \Longrightarrow \quad \mathfrak{p} \mid \langle \mathcal{N}(\mathfrak{p}) \rangle \tag{3.5}$$

$$\mathcal{N}(\mathfrak{p}) = 2^{e_2} \cdot 3^{e_3} \cdots p_n^{e_n} \quad \Longrightarrow \quad \mathfrak{p} \mid \langle p_i \rangle \tag{3.6}$$

teilt jedes Primideal $\mathfrak{p} \subset \mathfrak{D}$ ein von einer natürlichen Primzahl erzeugte Hauptideal $\langle p_i \rangle$. Zur Vereinfachung der Notation setzen wir $p := p_i$ und ersetzen die Formulierung „das von einer natürlichen Primzahl erzeugte Hauptideal $\langle p \rangle$" durch „die Primzahl $\langle p \rangle$". Wir folgern weiter:

$$\begin{aligned} \mathfrak{p} \mid \langle p \rangle \quad &\Longrightarrow \quad \exists\, \mathfrak{c} \in \mathfrak{D} : \ \mathfrak{p}\mathfrak{c} = \langle p \rangle \\ &\Longrightarrow \quad \mathcal{N}(\mathfrak{p})\mathcal{N}(\mathfrak{c}) = \mathcal{N}(\mathfrak{p}\mathfrak{c}) = \mathcal{N}(\langle p \rangle) \\ &\Longrightarrow \quad \mathcal{N}(\mathfrak{p}) \mid \mathcal{N}(\langle p \rangle) = |p\overline{p}| = \left|p^2\right| = p^2 \end{aligned} \tag{3.7}$$

Daher muss entweder

$$\mathcal{N}(\mathfrak{p}) = p \quad \textit{oder} \quad \mathcal{N}(\mathfrak{p}) = p^2 \tag{3.8}$$

gelten ($\mathcal{N}(\mathfrak{p}) = 1 \ \Leftrightarrow \ ord(D/\mathfrak{p}) = 1 \ \Leftrightarrow \ \mathfrak{p} = \mathfrak{D}$ scheidet aus). Sei also

$$\langle p \rangle = \mathfrak{p}\mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_m \tag{3.9}$$

die Primidealzerlegung von $\langle p\rangle$ in $\mathfrak{D}$, so ergibt sich mit (3.7)

$$p^2 = \mathcal{N}(\langle p\rangle) = \mathcal{N}(\mathfrak{p})\mathcal{N}(\mathfrak{p}_1)\mathcal{N}(\mathfrak{p}_2)\cdots\mathcal{N}(\mathfrak{p}_m) \tag{3.10}$$

und es folgt $0 \le m \le 1$. Es gibt also genau drei Möglichkeiten:

1. $\langle p\rangle = \mathfrak{p}\mathfrak{p}_1$ *($\mathfrak{p} \neq \mathfrak{p}_1$) mit* $\mathcal{N}(\mathfrak{p}) = \mathcal{N}(\mathfrak{p}_1) = p$
2. $\langle p\rangle = \mathfrak{p}\mathfrak{p}$ *($\mathfrak{p} = \mathfrak{p}_1$) mit* $\mathcal{N}(\mathfrak{p}) = p$
3. $\langle p\rangle = \mathfrak{p}$ *mit* $\mathcal{N}(\mathfrak{p}) = p^2$

Wegen

$$\mathfrak{p}\overline{\mathfrak{p}} = \langle \mathcal{N}(\mathfrak{p})\rangle = \langle p\rangle = \mathfrak{p}\mathfrak{p}_1 \text{ bzw. } \mathfrak{p}\mathfrak{p} \tag{3.11}$$

gilt in den ersten beiden Fällen sogar $\mathfrak{p}_1 = \overline{\mathfrak{p}}$ bzw. $\mathfrak{p} = \overline{\mathfrak{p}}$, da die (gebrochenen) Ideale gemäß Satz 2.12 eine Gruppe bilden.

Außerdem sieht man, dass $\mathfrak{p}$ genau eine Primzahl $\langle p\rangle$ teilt. Denn würde es auch die Primzahl $\langle q\rangle$ teilen, so folgte (mit einer Einheit ε von $\mathfrak{D}$):

- $\langle p\rangle = \mathfrak{p} \ \wedge\ \langle q\rangle = \mathfrak{p} \implies p = \varepsilon q \implies p = q$
- $\langle p\rangle = \mathfrak{p} \ \wedge\ \langle q\rangle = \mathfrak{p}\overline{\mathfrak{p}} \implies \langle q\rangle = \langle p\rangle\overline{\langle p\rangle} = \langle \mathcal{N}(\langle p\rangle)\rangle = \langle p^2\rangle \implies q = \varepsilon p^2$ ↯
- $\langle p\rangle = \mathfrak{p}\overline{\mathfrak{p}} \ \wedge\ \langle q\rangle = \mathfrak{p}\overline{\mathfrak{p}} \implies p = \varepsilon q \implies p = q$

Auf Grund dieser Eindeutigkeit können wir (im Falle der absoluten Konvergenz dieser Umordnung)

$$\prod_{\mathfrak{p}\in\mathfrak{P}} \frac{1}{1-\mathcal{N}(\mathfrak{p})^{-s}} = \prod_{p\in\mathbb{P}} \left(\prod_{\mathfrak{p}\mid\langle p\rangle} \frac{1}{1-\mathcal{N}(\mathfrak{p})^{-s}} \right) \tag{3.12}$$

schreiben. Für das innere Produkt ergibt sich für die drei möglichen Fälle:

1.
$$\prod_{\mathfrak{p}\mid\langle p\rangle} \frac{1}{1-\mathcal{N}(\mathfrak{p})^{-s}} = \left(1-\mathcal{N}(\mathfrak{p})^{-s}\right)^{-1}\left(1-\mathcal{N}(\mathfrak{p}_1)^{-s}\right)^{-1} = \left(1-p^{-s}\right)^{-2} \tag{3.13}$$

2.
$$\prod_{\mathfrak{p}\mid\langle p\rangle} \frac{1}{1-\mathcal{N}(\mathfrak{p})^{-s}} = \left(1-\mathcal{N}(\mathfrak{p})^{-s}\right)^{-1} = \left(1-p^{-s}\right)^{-1} \tag{3.14}$$

3.
$$\prod_{\mathfrak{p}\mid\langle p\rangle} \frac{1}{1-\mathcal{N}(\mathfrak{p})^{-s}} = \left(1-\mathcal{N}(\mathfrak{p})^{-s}\right)^{-1} = \left(1-p^{-2s}\right)^{-1} \tag{3.15}$$

Damit folgern wir

$$\begin{aligned}
\prod_{\mathfrak{p}\in\mathfrak{P}} \left|\frac{1}{1-\mathcal{N}(\mathfrak{p})^{-s}}\right| &= \prod_{p\in\mathbb{P}} \left(\prod_{\mathfrak{p}\mid\langle p\rangle} \left|\frac{1}{1-\mathcal{N}(\mathfrak{p})^{-s}}\right| \right) \le \prod_{p\in\mathbb{P}} \left(\prod_{\mathfrak{p}\mid\langle p\rangle} \frac{1}{\left||1| - \left|\mathcal{N}(\mathfrak{p})^{-s}\right|\right|} \right) \\
&= \prod_{p\in\mathbb{P}} \left(\prod_{\mathfrak{p}\mid\langle p\rangle} \frac{1}{\left|1-\mathcal{N}(\mathfrak{p})^{-\sigma}\right|} \right) \le \prod_{p\in\mathbb{P}} \frac{1}{\left(1-p^{-\sigma}\right)^2} = \zeta(\sigma)^2 < \infty
\end{aligned} \tag{3.16}$$

Das Produkt konvergiert also. Für reelle $s > 1$ ist jeder Faktor $(1-\mathcal{N}(\mathfrak{p})^{-s})^{-1}$ größer als 1, das unendliche Produkt konvergiert dann sogar absolut (siehe [Pr], p. 621ff.). Damit ist die Gleichheit (3.3) für reelle $s > 1$ gezeigt. Dann ist aber die Reihe auf der linken Seite in der gesamten Halbebene $\Re e\, s > 1$ analytisch, lässt sich also lokal in absolut konvergente Potenzreihen entwickeln. Die Reihe – und damit auch das unendliche Produkt – konvergieren also wie behauptet in der gesamten Halbebene $\Re e\, s >$ absolut. □

Der Beweis motiviert folgende

Definition 3.4
Sei $\mathfrak{p} \subset \mathfrak{D}$ ein Primideal. Dann heißt eine Primzahl $p \in \mathbb{N}$

- zerlegt, *falls* $\langle p\rangle = \mathfrak{p}\overline{\mathfrak{p}}$, $\mathcal{N}(\mathfrak{p}) = \mathcal{N}(\overline{\mathfrak{p}}) = p$,
- verzweigt, *falls* $\langle p\rangle = \mathfrak{p}^2$, $\mathcal{N}(\mathfrak{p}) = p$, *und*
- träge, *falls* $\langle p\rangle = \mathfrak{p}$, $\mathcal{N}(\mathfrak{p}) = p^2$.

Wir wollen nun die DEDEKIND'sche Zetafunktion des Körpers $\mathbb{Q}(i) := \mathbb{Q}(\sqrt{-1}) = \mathbb{Q}(\sqrt{-4})$ etwas genauer untersuchen. Der Ring der ganzen Zahlen von $\mathbb{Q}(i)$

$$\mathfrak{D}_{\mathbb{Q}(i)} = \mathbb{Z}[i] = \{x + yi \mid x,\, y \in \mathbb{Z}\} \tag{3.17}$$

ist gemäß Bemerkung 2.22 ein Hauptidealring. Wir können also jedes Ideal – insbesondere auch jedes Primideal – in der Form $\langle a\rangle$ mit einem bis auf eine Einheit eindeutig bestimmten $a \in \mathfrak{D}_{\mathbb{Q}(i)}$ schreiben. Wir betrachten zunächst wie sich die Primzahlen in diesem Ring darstellen lassen:

Satz 3.5 Darstellung der Primzahlen im Ring $\mathfrak{D}_{\mathbb{Q}(i)}$
Die Primzahlen $p \in \mathbb{N}$ lassen sich im Ring $\mathfrak{D}_{\mathbb{Q}(i)}$ folgendermaßen als Produkt von Primelementen schreiben:

$$\begin{aligned} p = 2 &\iff \langle p\rangle = \langle q\rangle^2,\ \textit{(p ist verzweigt)} \\ p \equiv 1 \ (mod\ 4) &\iff \langle p\rangle = \langle q\rangle\overline{\langle q\rangle},\ \langle q\rangle \neq \overline{\langle q\rangle}\ \textit{(p ist zerlegt)} \\ p \equiv 3 \ (mod\ 4) &\iff \langle p\rangle = \langle q\rangle,\ \textit{(p ist träge)} \end{aligned}$$

Dabei bezeichne $\langle q\rangle$ ein Primideal.

Beweis:

- $p = 2 \implies \langle p\rangle = \langle q\rangle^2$:
  Es gilt $2 = (-i)(1+i)^2$ und somit $\langle 2\rangle = \langle (1+i)^2\rangle = \langle 1+i\rangle^2$ (nach Lemma 2.4). $(1+i)$ ist auch ein Primelement (und $\langle 1+i\rangle$ damit ein Primideal):

  $$\exists\, c,\, d \in \mathfrak{D}_{\mathbb{Q}(i)} :\ 1 + i = cd \implies 2 = \mathcal{N}(1+i) = \mathcal{N}(c)\mathcal{N}(d) \implies \mathcal{N}(c) = 1 \ \vee\ \mathcal{N}(d) = 1$$

  Man beachte, dass die Norm im Ring $\mathfrak{D}_{\mathbb{Q}(i)}$ stets nichtnegativ ist und genau die Einheiten die Norm 1 haben.

- $p = 2 \impliedby \langle p\rangle = \langle q\rangle^2$:
  Es gilt $q^2 = \varepsilon p$ mit einer Einheit $\varepsilon \in \{\pm 1, \pm i\}$. Wir setzen $q := x + yi$ und folgern

  1. $(x+yi)^2 = \pm p \implies x^2 + 2xyi - y^2 = \pm p \implies 2xyi = 0 \implies p = \mp x^2 \ \vee p = \mp y^2$ ↯
  2. $(x+yi)^2 = \pm ip \implies x^2 i - 2xy - y^2 i = \mp p \implies 2xy = \pm p \implies p = 2$

  Der 1. Fall führt zum Widerspruch, daher muss $p = 2$ gelten.

- $p \equiv 1 \ (mod\ 4) \implies \langle p\rangle = \langle q\rangle\overline{\langle q\rangle},\ \langle q\rangle \neq \overline{\langle q\rangle}$:
  Wegen $p \equiv 1 \ (mod\ 4)$ ($\Leftrightarrow\ p \equiv 1 \ (mod\ -4)$) gilt $1 = \chi_{-4}(p) := \left(\frac{-4}{p}\right)$. Daher können wir gemäß der Definiton des LEGENDRE*-Symbols eine Zahl $x \in \mathbb{Z}$ so wählen, dass $x^2 \equiv -4 \ (mod\ p)$ gilt. Es folgt $p \nmid (x - 2i)$, denn*

  $$\begin{aligned} p \mid (x-2i) &\implies \exists\,(a+bi) \in \mathfrak{D}_{\mathbb{Q}(i)} :\ p(a+bi) = (x-2i) \implies p(a-bi) = (x+2i) \\ &\implies p \mid (x+2i) \implies p \mid ((x-2i) - (x+2i)) = 4i \implies p \leq 4 \ \text{↯} \end{aligned}$$

  führt zum Widerspruch. Völlig analog ergibt sich $p \nmid (x+2i)$. p teilt also weder $(x-2i)$ noch $(x+2i)$, wohl aber (nach Wahl von x) das Produkt $(x-2i)(x+2i) = x^2 + 4$. Damit ist p kein Primelement und $\langle p\rangle$ besteht aus genau zwei Primidealfaktoren (gemäß Definition 3.4 sind es höchstens 2). Nach dem schon Bewiesenen können diese nicht gleich sein, da sonst $p = 2$ folgen würde. Also ist p zerlegt.

- $p \equiv 3 \ (mod\ 4) \implies \langle p \rangle = \langle q \rangle$:

  Ist $\langle p \rangle$ kein Primideal, dann besitzt es eine Darstellung

  $$\langle p \rangle = \langle a + bi \rangle \langle a - bi \rangle$$

  mit zwei nicht notwendig gleichen Primidealen $\langle a \pm bi \rangle$. Daraus folgt

  $$0 < p = \varepsilon(a + bi)(a - bi) = \varepsilon(a^2 + b^2), \quad \varepsilon \in \{\pm 1, \pm i\}$$

  Die Fälle $\varepsilon = -1, \pm i$ scheiden offensichtlich aus. Aber auch $p = a^2 + b^2$ ist nicht lösbar, denn Quadrate haben modulo 4 stest den Rest 0 oder 1. Die rechte Seite ist also kongruent 0, 1 oder 2 modulo 4, was der Voraussetzung widerspricht. (Dies beweist bereits, dass sich Primzahlen der Form $4n + 3$, $n \in \mathbb{N}$, nicht als Summe zweier Quadrate schreiben lassen.) $\langle p \rangle$ ist somit ein Primideal, p also träge.

- *Jede Primzahl ist entweder gerade oder kongruent 1 oder 3 modulo 4. Außerdem ist jede Primzahl entweder verzweigt, zerlegt oder träge. Daher müssen von den letzten beiden Implikationen auch die Umkehrungen gelten (die Rückrichtung im Falle $p = 2$ wurde zwischendurch benötigt).*

□

Ruft man sich die Definition des DIRICHLET'schen Charakters χ_{-4} in Erinnerung (siehe auch (3.25)), so kann man Satz 3.5 auch folgendermaßen formulieren:

Korollar 3.6
Für die Primzahlen $p \in \mathbb{N}$ gilt im Ring $\mathfrak{D}_{\mathbb{Q}(i)} = \mathfrak{D}_{\mathbb{Q}(\sqrt{-4})}$:

$$\begin{aligned} \chi_{-4}(p) = 0 &\iff p \text{ ist verzweigt} \\ \chi_{-4}(p) = 1 &\iff p \text{ ist zerlegt} \\ \chi_{-4}(p) = -1 &\iff p \text{ ist träge} \end{aligned}$$

Dieses Resultat lässt sich auf die DEDEKIND'sche Zetafunktion des Körpers $\mathbb{Q}(i)$ anwenden:

$$\begin{aligned} \zeta_{\mathbb{Q}(i)}(s) &= \prod_{\mathfrak{p} \in \mathfrak{P}} \frac{1}{1 - \mathcal{N}(\mathfrak{p})^{-s}} = \prod_{p \in \mathbb{P}} \left(\prod_{\mathfrak{p} | \langle p \rangle} \frac{1}{1 - \mathcal{N}(\mathfrak{p})^{-s}} \right) \\ &= \prod_{\substack{p \in \mathbb{P} \\ p \text{ verzweigt}}} \frac{1}{1 - p^{-s}} \cdot \prod_{\substack{p \in \mathbb{P} \\ p \text{ zerlegt}}} \frac{1}{(1 - p^{-s})^2} \cdot \prod_{\substack{p \in \mathbb{P} \\ p \text{ träge}}} \frac{1}{1 - p^{-2s}} \\ &= \prod_{\substack{p \in \mathbb{P} \\ p \text{ verzweigt}}} \frac{1}{1 - p^{-s}} \cdot \prod_{\substack{p \in \mathbb{P} \\ p \text{ zerlegt}}} \frac{1}{1 - p^{-s}} \frac{1}{1 - p^{-s}} \cdot \prod_{\substack{p \in \mathbb{P} \\ p \text{ träge}}} \frac{1}{1 - p^{-s}} \frac{1}{1 + p^{-s}} \\ &= \zeta(s) \cdot \prod_{\substack{p \in \mathbb{P} \\ p \text{ zerlegt}}} \frac{1}{1 - p^{-s}} \cdot \prod_{\substack{p \in \mathbb{P} \\ p \text{ träge}}} \frac{1}{1 + p^{-s}} \\ &= \zeta(s) \cdot \prod_{\substack{p \in \mathbb{P} \\ \chi_{-4}(p) = 1}} \frac{1}{1 - p^{-s}} \cdot \prod_{\substack{p \in \mathbb{P} \\ \chi_{-4}(p) = -1}} \frac{1}{1 - (-p^{-s})} \\ &= \zeta(s) \cdot \prod_{p \in \mathbb{P}} \frac{1}{1 - \chi_{-4}(p) p^{-s}} = \zeta(s) \cdot \sum_{k=1}^{\infty} \frac{\chi_{-4}(k)}{k^s} \\ &= \zeta(s) L(s, \chi_{-4}) \end{aligned} \tag{3.18}$$

Sowohl diese Aussage als auch Korollar 3.6 lässt sich über den von uns gezeigten Spezialfall $D = -4$ hinaus auf beliebige quadratische Zahlkörper verallgemeinern. Siehe dazu z. B. [Za], p. 100 ff., oder [SO], p. 172 f.

Darstellungsanzahlen

Als nächstes wollen wir aus der Zetafunktion des Körpers $\mathbb{Q}(i)$ eine Formel für die Anzahl der Darstellungen einer natürlichen Zahl als Summe zweier Quadrate ableiten. Wir definieren

$$A_2(n) := \left\{(x,y) \in \mathbb{Z}^2 \mid x^2 + y^2 = n\right\} \quad \forall\, n \in \mathbb{N} \tag{3.19}$$

Sei

$$\zeta_{\mathbb{Z}[i]}(s) := \sum_{\substack{a \in \mathbb{Z}[i] \\ a \neq 0}} \frac{1}{\mathcal{N}(a)^s} = \sum_{\substack{(x,y) \in \mathbb{Z}^2 \\ (x,y) \neq (0,0)}} \frac{1}{(x^2+y^2)^s} \tag{3.20}$$

eine Zetafunktion, bei der über alle *ganzen* Gauss*'schen Zahlen* mit Ausnahme der 0 summiert wird. Dann gilt offensichtlich

$$\zeta_{\mathbb{Z}[i]}(s) = \sum_{\substack{(x,y) \in \mathbb{Z}^2 \\ (x,y) \neq (0,0)}} \frac{1}{(x^2+y^2)^s} = \sum_{n=1}^{\infty} \frac{A_2(n)}{n^s} \tag{3.21}$$

Weiter besteht die Beziehung

$$\zeta_{\mathbb{Z}[i]}(s) = 4\zeta_{\mathbb{Q}(i)}(s) = 4\zeta(s)L(s,\chi_{-4}) \tag{3.22}$$

denn jeweils 4 ganze Gauss'sche Zahlen erzeugen dasselbe Ideal in $\mathfrak{D}_{\mathbb{Q}(i)}$: Der Ring $\mathfrak{D}_{\mathbb{Q}(i)}$ besitzt genau 4 verschiedene Einheiten und zwei Elemente erzeugen genau dann dasselbe Ideal, wenn sie sich nur um eine Einheit unterscheiden. Da $\mathfrak{D}_{\mathbb{Q}(i)}$ ein Hauptidealring ist, wird auch tatsächlich jedes ganze Ideal erzeugt.

Aus (3.21) und (3.22) ergibt sich

$$\sum_{n=1}^{\infty} A_2(n) n^{-s} = 4\zeta(s)L(s,\chi_{-4}) = 4\left(\sum_{m=1}^{\infty} \frac{1}{m^s}\right)\left(\sum_{k=1}^{\infty} \frac{\chi_{-4}(k)}{k^s}\right) = 4\sum_{n=1}^{\infty}\left(\sum_{k|n} \chi_{-4}(k)\right) n^{-s} \tag{3.23}$$

Koeffiezientenvergleich (der bei konvergenten Dirichlet-Reihen zulässig ist) beweist den folgenden

Satz 3.7 Darstellungen als Summe zweier Quadrate
Für die Anzahl der Darstellungen einer natürlichen Zahl $n \in \mathbb{N}$ als Summe zweier Quadrate gilt

$$A_2(n) = 4\sum_{k|n} \chi(k) \tag{3.24}$$

wobei χ der Dirichlet*'sche Charakter*

$$\chi(k) := \chi_{-4}(k) = \begin{cases} 1, & k = 4n+1 \\ 0, & k = 4n+2 \\ -1, & k = 4n+3 \\ 0, & k = 4n \end{cases} \quad \forall\, n \in \mathbb{N} \tag{3.25}$$

ist und über alle positiven Teiler k von n summiert wird.

Für Primzahlen vereinfacht sich die Summe auf zwei Summaden. Wir erhalten damit das

Korollar 3.8 Darstellungen von Primzahlen als Summe zweier Quadrate
Für die Anzahl der Darstellungen einer Primzahl $p \in \mathbb{N}$ als Summe zweier Quadrate gilt

$$\begin{aligned} p = 2 &\implies A_2(p) = 4 \\ p \equiv 1 \ (mod\ 4) &\implies A_2(p) = 8 \\ p \equiv 3 \ (mod\ 4) &\implies A_2(p) = 0 \end{aligned}$$

Beweis:

- $p = 2$*: siehe Tabelle 1*
- $p \equiv 1 \ (mod\ 4)$*:*

$$A_2(p) = 4\sum_{k|n} \chi(k) = 4\left(\chi(1) + \chi(p)\right) = 4\left(\chi(1) + \chi(4n+1)\right) = 4(1+1) = 8$$

- $p \equiv 3 \ (mod\ 4)$*:*

$$A_2(p) = 4\sum_{k|n} \chi(k) = 4\left(\chi(1) + \chi(p)\right) = 4\left(\chi(1) + \chi(4n+3)\right) = 4(1+(-1)) = 0$$

□

Wir wollen zum Schluss ein paar Darstellungsanzahlen konkret ausrechen:

n	k	$A_2(n)$
1	1	$4\chi(1) = 4 \cdot 1 = 4$
2	1, 2	$4\left(\chi(1) + \chi(2)\right) = 4\left(1+0\right) = 4$
3	1, 3	$4\left(\chi(1) + \chi(3)\right) = 4\left(1+(-1)\right) = 0$
4	1, 2, 4	$4\left(\chi(1) + \chi(2) + \chi(4)\right) = 4\left(1+0+0\right) = 4$
5	1, 5	$4\left(\chi(1) + \chi(5)\right) = 4\left(1+1\right) = 8$
6	1, 2, 3, 6	$4\left(\chi(1) + \chi(2) + \chi(3) + \chi(6)\right) = 4\left(1+0+(-1)+0\right) = 0$
7	1, 7	$4\left(\chi(1) + \chi(7)\right) = 4\left(1+(-1)\right) = 0$
25	1, 5, 25	$4\left(\chi(1) + \chi(5) + \chi(25)\right) = 4\left(1+1+1\right)) = 12$
125	1, 5, 25, 125	$4\left(\chi(1) + \chi(5) + \chi(25) + \chi(125)\right) = 4\left(1+1+1+1\right)) = 16$[‡]
4711	1, 7, 673, 4711	$4\left(\chi(1) + \chi(7) + \chi(673) + \chi(4711)\right) = 4\left(1+(-1)+1+(-1)\right) = 0$

Tabelle 1: Ausgewählte Darstellungsanzahlen nach Satz 3.7

[‡] $125 = (\pm 2)^2 + (\pm 11)^2 = (\pm 11)^2 + (\pm 2)^2 = (\pm 5)^2 + (\pm 10)^2 = (\pm 10)^2 + (\pm 5)^2$

4 Literatur

Bücher

[Za] Zagier, D. B.: *Zetafunktionen und quadratische Körper*,
Springer Verlag, Berlin-Heidelberg-New York (1981)

[SO] Scharlau, W., Opolka, H.: *Von Fermat bis Minkowski. Eine Vorlesung über Zahlentheorie und ihre Entwicklung*, Springer Verlag, Berlin-Heidelberg-New York (1980)

[ST] Stewart, I., Tall, D.: *Algebraic Number Theory*,
Chapman and Hall, London (1987)

[Bo] Bosch, S.: *Algebra*, 5. überarbeitete Auflage,
Springer Verlag, Berlin-Heidelberg-New York (2003)

[Ha] Hasse, H.: *Vorlesungen über Zahlentheorie*, Grundlagen der mathematischen Wissenschaften, Bd. 59, Springer Verlag, Berlin-Heidelberg-New York (1964)

[He] Hecke, E.: *Lectures on the Theory of Algebraic Numbers*,
(im Original: Vorlesungen über die Theorie der algebraischen Zahlen, Leipzig (1923))
Springer-Verlag, Berlin-Heidelberg-New York (1981)

[Pr] Pringheim, A.: *Komplexe Zahlen, Reihen mit komplexen Gliedern, unendliche Produkte und Kettenbrüche*, Teubner, Leipzig (1921)

Skripten

[Ma] Matzat, B. H.: *Elementare Zahlentheorie*, Vorlesungsskript
Universität Heidelberg (1992)

[Le] Lemmermeyer, F.: *Quadratische Zahlkörper*, Vorlesungsskript
Universität des Saarlands (1997)

Online

[Ma] `http://mathphys.fsk.uni-heidelberg.de/skripte/skripte_zahlentheorie.html`

[Le] `http://archiv.ub.uni-heidelberg.de/volltextserver/ volltexte/1999/16/ps/16_1.ps`

Dieses Handout ist zum Download verfügbar unter

`http://www.rzuser.uni-heidelberg.de/~ckirches`
`http://www.mathi.uni-heidelberg.de/~ferreau`