Dedekind Ringe und Klassengruppen

Ana Marija Vego

1 Gebrochene Ideale

Im folgenden Abschnitt bezeichnet $\mathcal{O}$ einen beliebigen Dedekindring, und K seinen Quotientenkörper.

Lemma 1.1. *Zu jedem Ideal $\mathfrak{a} \neq 0$ von $\mathcal{O}$, existiert ein $r \in \mathbb{N}$ und von Null verschiedene Primideale $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_r$ mit*

$$\mathfrak{a} \supseteq \mathfrak{p}_1 \mathfrak{p}_2 \ldots \mathfrak{p}_r$$

Beweis: Sei M die Menge aller Ideale $\mathfrak{a}$ s.d. keine Primideale mit der obigen Eigenschaft existieren. Angenommen M sei nicht leer. Da $\mathcal{O}$ noethersch ist, bricht jede aufsteigende Idealkette ab. M ist daher hinsichtlich der Inklusion induktiv geordnet und besitzt somit nach dem Zornschen Lemma ein maximales Element $\mathfrak{a}$. Dieses kann kein Primideal sein, d.h. es gibt Elemente $b_1, b_2 \in \mathcal{O}$ mit $b_1 b_2 \in \mathfrak{a}$, aber $b_1, b_2 \notin \mathfrak{a}$. Setzen wir $\mathfrak{a}_1 = (b_1) + \mathfrak{a}$, $\mathfrak{a}_2 = (b_2) + \mathfrak{a}$, so ist $\mathfrak{a} \subsetneq \mathfrak{a}_1$, $\mathfrak{a} \subsetneq \mathfrak{a}_2$ und $\mathfrak{a}_1 \mathfrak{a}_2 \subseteq \mathfrak{a}$. Wegen der Maximalität enthalten $\mathfrak{a}_1$ und $\mathfrak{a}_2$ Primidealprodukte, deren Produkt in $\mathfrak{a}$ liegt, Widerspruch. $\square$

Lemma 1.2. *Ist $\mathfrak{p}$ ein Primideal von $\mathcal{O}$ und*

$$\mathfrak{p}^{-1} = \{x \in K \mid x\mathfrak{p} \subseteq \mathcal{O}\}$$

so ist $\mathfrak{a}\mathfrak{p}^{-1} := \left\{\sum_i a_i x_i \mid a_i \in \mathfrak{a}, x_i \in \mathfrak{p}^{-1}\right\} \neq \mathfrak{a}$ für jedes Ideal $\mathfrak{a} \neq 0$.

Beweis: Sei $a \in \mathfrak{p}, a \neq 0$, und $\mathfrak{p}_1 \mathfrak{p}_2 \ldots \mathfrak{p}_r \subseteq (a) \subseteq \mathfrak{p}$ mit minimalem r, wobei $\mathfrak{p}_1$, ..., $\mathfrak{p}_r$ Primideale wie in Lemma 1.1 sind. Dann ist eines der $\mathfrak{p}_i$, o.B.d.A. $\mathfrak{p}_1$, in $\mathfrak{p}$ enthalten, also $\mathfrak{p}_1 = \mathfrak{p}$ wegen der Maximalität von $\mathfrak{p}_1$. Denn sonst gäbe es für jedes i ein $a_i \in \mathfrak{p}_i \backslash \mathfrak{p}$ mit $a_1 \ldots a_r \in \mathfrak{p}$. Wegen $\mathfrak{p}_2 \ldots \mathfrak{p}_r \subsetneq (a)$ gibt es ein $b \in \mathfrak{p}_2 \ldots \mathfrak{p}_r$ mit $b \notin a\mathcal{O}$ also $a^{-1}b \notin \mathcal{O}$. Andererseits ist aber $b\mathfrak{p} \subseteq (a)$, also $a^{-1}b\mathfrak{p} \subseteq \mathcal{O}$, und somit $a^{-1}b \in \mathfrak{p}^{-1}$. Damit ist $\mathfrak{p}^{-1} \neq \mathcal{O}$. Sei nun $\mathfrak{a} \neq 0$ ein Ideal von $\mathcal{O}$ und $\alpha_1, \ldots, \alpha_n$ ein Erzeugendensystem. Nehmen wir an, das $\mathfrak{a}\mathfrak{p}^{-1} = \mathfrak{a}$. Dann ist für jedes $x \in \mathfrak{p}^{-1}$

$$x\alpha_i = \sum_j a_{ij}\alpha_j, \quad a_{ij} \in \mathcal{O}$$

Ist A die Matrix $(x\delta_{ij} - a_{ij})$, so ist also $A(\alpha_1, \ldots, \alpha_n)^t = \underline{0}$. Für die Determinante $d := det(A)$ folgt $d\alpha_1 = \ldots = d\alpha_n = 0$ und somit $d = 0$. Daher ist x als

Nullstelle des normierten Polynoms $f(x) = det(X\delta_{ij} - a_{ij}) \in \mathcal{O}[X]$ ganz über $\mathcal{O}$, d.h. $x \in \mathcal{O}$. Es ergibt sich somit $\mathfrak{p}^{-1} = \mathcal{O}$, Widerspruch. $\square$

Satz 1.3. *Jedes von* (0) *und* (1) *verschiedene Ideal* $\mathfrak{a}$ *von* $\mathcal{O}$ *besitzt eine, bis auf Vertauschung, eindeutige Zerlegung*

$$\mathfrak{a} = \mathfrak{p}_1 \dots \mathfrak{p}_r$$

in Primideale $\mathfrak{p}_i$ *von* $\mathcal{O}$.

Beweis:
I. Existenz der Primzerlegung.
Sei $\mathfrak{M}$ die Menge aller von (0) und (1) verschiedenen Ideale, die keine Primzerlegung besitzen. Ist $\mathfrak{M}$ nicht leer, so schließen wir wie bei (1.1), dass es ein maximales Element, sage $\mathfrak{a}$, in $\mathfrak{M}$ gibt. Es liegt in einem maximalen Ideal $\mathfrak{p}$, und wir erhalten wegen $\mathcal{O} \subseteq \mathfrak{p}^{-1}$:

$$\mathfrak{a} \subseteq \mathfrak{a}\mathfrak{p}^{-1} \subseteq \mathfrak{p}\mathfrak{p}^{-1} \subseteq \mathcal{O}$$

Nach Lemma 1.2 ist $\mathfrak{a} \subsetneq \mathfrak{a}\mathfrak{p}^{-1}$ und $\mathfrak{p} \subsetneq \mathfrak{p}\mathfrak{p}^{-1} \subseteq \mathcal{O}$. Da $\mathfrak{p}$ ein maximales Ideal ist, so folgt $\mathfrak{p}\mathfrak{p}^{-1} = \mathcal{O}$. Wegen der Maximalität von $\mathfrak{a}$ in $\mathfrak{M}$ und wegen $\mathfrak{a} \neq \mathfrak{p}$, also $\mathfrak{a}\mathfrak{p}^{-1} \neq \mathcal{O}$, besitzt $\mathfrak{a}\mathfrak{p}^{-1}$ eine Primzerlegung $\mathfrak{a}\mathfrak{p}^{-1} = \mathfrak{p}_1 \dots \mathfrak{p}_r$ also auch $\mathfrak{a} = \mathfrak{a}\mathfrak{p}^{-1}\mathfrak{p} = \mathfrak{p}_1 \dots \mathfrak{p}_r\mathfrak{p}$, Widerspruch.
II. Eindeutigkeit der Primzerlegung.
Für ein Primideal $\mathfrak{p}$ gilt nach Definition: $\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{p} \Rightarrow \mathfrak{a} \subseteq \mathfrak{p}$ oder $\mathfrak{b} \subseteq \mathfrak{p}$, d.h. $\mathfrak{p}|\mathfrak{a}\mathfrak{b} \Rightarrow \mathfrak{p}|\mathfrak{a}$ oder $\mathfrak{p}|\mathfrak{b}$. Seien nun

$$\mathfrak{a} = \mathfrak{p}_1\mathfrak{p}_2 \dots \mathfrak{p}_r = \mathfrak{q}_1\mathfrak{q}_2 \dots \mathfrak{q}_s$$

zwei Primzerlegungen von $\mathfrak{a}$. Dann teilt $\mathfrak{p}_1$ einen Faktor $\mathfrak{q}_i$, etwa $\mathfrak{q}_1$, und ist wegen der Maximalität $= \mathfrak{q}_1$. Wir multiplizieren mit $\mathfrak{p}_1^{-1}$ und erhalten wegen $\mathfrak{p}_1 \neq \mathfrak{p}_1\mathfrak{p}_1^{-1} = \mathcal{O}$

$$\mathfrak{p}_2 \dots \mathfrak{p}_r = \mathfrak{q}_2 \dots \mathfrak{q}_s$$

So fortfahrend erhalten wir $r = s$ und nach eventueller Umordnung $\mathfrak{p}_i = \mathfrak{q}_i, i = 1, \dots, r$. $\square$

Definition 1.1 (gebrochenes Ideal)**.** Sei $\mathcal{O}$ ein Dedekind Ring und K sein Quotientenkörper. Ein **gebrochenes Ideal** von K ist ein endlich erzeugter $\mathcal{O}$-Untermodul $\mathfrak{a} \neq 0$ von K. Ein **ganzes Ideal** von K ist ein Ideal von $\mathcal{O}$.

Die Definition vom ganzen Ideal ist jetzt nötig um unterscheiden zu können von gebrochenen Idealen.

Satz 1.4. *Die gebrochenen Ideale bilden eine abelsche Gruppe, die Idealgruppe* J_K *von K. Das Einselement (1)* $= \mathcal{O}$*, und das Inverse zu* $\mathfrak{a}$ *ist*

$$\mathfrak{a}^{-1} = \{x \in K : x\mathfrak{a} \subseteq \mathcal{O}\}$$

Beweis: Assoziativität, Kommutativität und $\mathfrak{a}(1) = \mathfrak{a}$ sind klar. Für ein Primideal $\mathfrak{p}$ ist nach Lemma (1.1) $\mathfrak{p} \subsetneq \mathfrak{p}\mathfrak{p}^{-1}$, also $\mathfrak{p}\mathfrak{p}^{-1} = \mathcal{O}$ wegen der Maximalität von $\mathfrak{p}$. Ist $\mathfrak{a} = \mathfrak{p}_1 ... \mathfrak{p}_r$ ein ganzes Ideal, so ist $\mathfrak{b} = \mathfrak{p}_1^{-1} ... \mathfrak{p}_r^{-1}$ ein Inverses. Wegen $\mathfrak{b}\mathfrak{a} = \mathcal{O}$ ist $\mathfrak{b} \subseteq \mathfrak{a}^{-1}$. Ist umgekehrt $x\mathfrak{a} \subseteq \mathcal{O}$, so ist $x\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{b}$, also $x \in \mathfrak{b}$ wegen $\mathfrak{a}\mathfrak{b} = \mathcal{O}$. Daher ist $\mathfrak{b} = \mathfrak{a}^{-1}$. Ist $\mathfrak{a}$ ein gebrochenes Ideal und $\mathfrak{c} \in \mathcal{O}$, $\mathfrak{c} \neq 0$, mit $\mathfrak{c}\mathfrak{a} \subseteq \mathcal{O}$, so ist $(\mathfrak{c}\mathfrak{a})^{-1} = \mathfrak{c}^{-1}\mathfrak{a}^{-1}$ das Inverse von $\mathfrak{c}\mathfrak{a}$, also $\mathfrak{a}\mathfrak{a}^{-1} = \mathcal{O}$. □

Bemerkung: Da $\mathcal{O}$ noeterisch ist, ist ein $\mathcal{O}$-Untermodul $\mathfrak{a} \neq 0$ von $K = \mathrm{Quot}(\mathcal{O})$ ein gebrochenes Ideal g.d.w. ein $0 \neq c \in \mathcal{O}$ existiert mit $c\mathfrak{a} \subseteq \mathcal{O}$. Die gebrochene Ideale multipliziert man genauso wie Ideale von $\mathcal{O}$.

Korollar 1.4.1. *Jedes gebrochene Ideal $\mathfrak{a}$ besitzt eine eindeutige Produktdarstellung*

$$\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{\nu_\mathfrak{p}}$$

mit $\nu_\mathfrak{p} \in \mathbb{Z}$ und $\nu_\mathfrak{p} = 0$ für fast alle $\mathfrak{p}$. Mit anderen Worten: J_K ist die durch die Primideale $\mathfrak{p} \neq 0$ erzeugte freie abelsche Gruppe.

Beweis: Jedes gebrochene Ideal $\mathfrak{a}$ ist Quotient $\mathfrak{a} = \mathfrak{b}/\mathfrak{c}$ zweier ganzer Ideale $\mathfrak{b}$ und $\mathfrak{c}$, die nach (1.3) eine Primfaktorzerlegung besitzen. Daher besitzt $\mathfrak{a}$ eine Primzerlegung im Sinne des Korollars. Sie ist nach (1.3) eindeutig, wenn $\mathfrak{a}$ ganz ist, und damit auch im allgemeinen Fall. □

Das Korollar 1.4.1 gibt einen Zusammenhang zu den lokalen Bewertungen. Nach dem Satz (11.5) in [MP11] [2] erhalten wir dass zu jedem Primideal $\mathfrak{p} \neq 0$ in $\mathcal{O}$ ein zugehöriger diskreter Bewertungsring $\mathcal{O}_\mathfrak{p}$ mit der entsprechenden Bewertung des Quotientenkörpers:

$$v_\mathfrak{p} : K^\times \to \mathbb{Z}$$

existiert. Diese Bewertung hat eine beziehung zur Primzerlegung. Ist $x \in K^\times$ und

$$(x) = \prod_{\mathfrak{p}} \mathfrak{p}^{\nu_p}$$

die Primzerlegung des Hauptideals (x), so ist

$$\nu_\mathfrak{p} = v_\mathfrak{p}(x)$$

für alle $\mathfrak{p}$. Denn für ein festes Primideal $\mathfrak{q} \neq 0$ von $\mathcal{O}$ folgt (wegen $\mathfrak{p}\mathcal{O}_\mathfrak{q} = \mathcal{O}_\mathfrak{q}$ für $\mathfrak{p} \neq \mathfrak{q}$) aus der ersten Gleichung

$$x\mathcal{O}_\mathfrak{q} = (\prod_{\mathfrak{p}} \mathfrak{p}^{\nu_p})\mathcal{O}_\mathfrak{q} = \mathfrak{q}^{\nu_\mathfrak{q}}\mathcal{O}_\mathfrak{q} = {\mathfrak{m}_\mathfrak{q}}^{\nu_\mathfrak{q}}$$

also in der Tat $v_\mathfrak{q}(x) = \nu_\mathfrak{q}$.

2 Die Klassengruppe

Definition-Proposition 2.1. Die Klassengruppe ist definiert als die Faktorgruppe

$$Cl_K = J_K/P_K.$$

wobei P_K aus den gebrochenen Hauptidealen $(a) = a\mathcal{O}$, $a \in K^\times$ besteht.
Bemerkung: P_K ist eine Untergruppe der Idealgruppe J_K.

Generell rechnet man in der Gruppe der gebrochenen Ideale mit der entsprechenden Äquivalenzrelation lieber als in der Klassengruppe von K. Man setzt hierbei für zwei gebrochene Ideale $\mathcal{I}, \mathcal{J}$:

$$\begin{aligned} \mathcal{I} \sim \mathcal{J} &\iff \mathcal{I}P_K = \mathcal{J}P_K \\ &\iff \exists x \in K^\times : \mathcal{I} = (x)\mathcal{J} \\ &\iff \exists x \in K^\times : \mathcal{I} = x\mathcal{J} \end{aligned} \tag{1}$$

Bemerkung: Ein Dedekindring ist ein Hauptidealring wenn die Klassengruppe trivial ist.

Beispiel: Sei $K := \mathbb{Q}(\sqrt{d})$, für $d \in \mathbb{Z}$ quadratfrei. Die negativen quadratfreien Zahlen $d < 0$ für die die Klassengruppe von K trivial ist, sind:

$$d = -1, -2, -3, -7, -11, -19, -43, -67, -163$$

References

[1] [N92] J. Neukirch, Algebraische Zahlentheorie. Springer-Verlag, Berlin, 1992

[2] [MP11] S. Müller-Stach und J. Piontkowski, Elementare und algebraische Zahlentheorie, 2., erweiterte Auflage, Springer, Berlin, 2011

Email address: avego@student.ethz.ch