Prof. Dr. H. Brenner **Osnabrück WS 2020/2021**

Algebraische Zahlentheorie

Vorlesung 13

Divisoren

Die Menge der effektiven Divisoren zu einem Dedekindbereich bilden mit der natürlichen Addition ein kommutatives Monoid, aber keine Gruppe, da ja die Koeffizienten $n_{\mathfrak{p}}$ alle nichtnegativ sind. Lässt man auch negative ganze Zahlen zu, so gelangt man zum Begriff des Divisors, die eine Gruppe bilden. Auch den Begriff des Hauptdivisors kann man so erweitern, dass er nicht nur für ganze Elemente aus R, sondern auch für rationale Elemente, also Elemente aus dem Quotientenkörper $Q(R)$, definiert ist.

Definition 13.1. Es sei R ein Dedekindbereich. Ein *Divisor* ist eine formale Summe

$$\sum_{\mathfrak{p}} n_{\mathfrak{p}} \cdot \mathfrak{p}\,,$$

die sich über alle Primideale $\mathfrak{p} \neq 0$ aus R erstreckt und wobei $n_{\mathfrak{p}}$ ganze Zahlen mit $n_{\mathfrak{p}} = 0$ für fast alle $\mathfrak{p}$ sind.

Für einen diskreten Bewertungsring lässt sich die Ordnung $\operatorname{ord}\colon R \setminus \{0\} \to \mathbb{N}$, $q \mapsto \operatorname{ord}(q)$, zu einer Ordnungsfunktion auf dem Quotientenkörper fortsetzen,

$$\operatorname{ord}\colon Q(R) \setminus \{0\} \longrightarrow \mathbb{Z},\ q \longmapsto \operatorname{div}(q),$$

siehe Aufgabe 13.1, wobei sich die Eigenschaften von Lemma 10.15 hierher übertragen.

Definition 13.2. Es sei R ein Dedekindbereich und $q \in Q(R)$, $q \neq 0$. Dann heißt die Abbildung, die jedem Primideal $\mathfrak{p} \neq 0$ in R die Ordnung $\operatorname{ord}_{\mathfrak{p}}(q)$ zuordnet, der durch q definierte *Hauptdivisor*. Er wird mit $\operatorname{div}(q)$ bezeichnet und als formale Summe

$$\operatorname{div}(q) = \sum_{\mathfrak{p}} \operatorname{ord}_{\mathfrak{p}}(q) \cdot \mathfrak{p}$$

geschrieben.

Wenn man die rationale Funktion $q \in Q(R)$ als $q = \frac{f}{g}$ mit $f, g \in R$ ansetzt, so gilt

$$\operatorname{div}(q) = \operatorname{div}(f) - \operatorname{div}(g),$$

da dies punktweise an jedem Primideal gilt. Bei

$$\operatorname{ord}_{\mathfrak{p}}(q) < 0$$

sagt man auch, dass q einen *Pol* an der Stelle $\mathfrak{p}$ besitzt, und zwar mit der Polordnung $-\operatorname{ord}_{\mathfrak{p}}(q)$.

Die Menge der Divisoren bildet eine additive kommutative freie Gruppe, die wir mit $\operatorname{Div}(R)$ bezeichnen.

LEMMA 13.3. *Es sei R ein Dedekindbereich mit Quotientenkörper $Q(R)$, und seien $q, q_1, q_2 \in Q(R) \setminus \{0\}$. Dann gelten folgende Aussagen.*

(1) *Es ist* $\operatorname{div}(q_1q_2) = \operatorname{div}(q_1) + \operatorname{div}(q_2)$.
(2) *Es ist* $\operatorname{div}(q_1 + q_2) \geq \min\{\operatorname{div}(q_1), \operatorname{div}(q_2)\}$.
(3) *Es ist $q \in R$ genau dann, wenn der Hauptdivisor* $\operatorname{div}(q)$ *effektiv ist.*
(4) *Zu jedem Divisor D gibt es ein $h \in R$ derart, dass $D + \operatorname{div}(h)$ effektiv ist.*

Beweis. Für (1) und (2) siehe Aufgabe 13.2, für (3) siehe Aufgabe 13.3, für (4) siehe Aufgabe 13.4. □

Es liegt also insbesondere ein Gruppenhomomorphismus

$$(Q(R))^\times \longrightarrow \operatorname{Div}(R),\ q \longmapsto \operatorname{div}(q),$$

vor. Das Bild unter diesem Gruppenhomomorphismus ist die Untergruppe der Hauptdivisoren, die wir mit H bezeichnen.

Gebrochene Ideale

In Satz 11.13 haben wir eine Bijektion zwischen effektiven Divisoren und von 0 verschiedenen Idealen (und von effektiven Hauptdivisoren mit von 0 verschiedenen Hauptidealen) gestiftet. Von daher liegt die Frage nahe, welche „Ideal-ähnlichen“ Objekte den Divisoren entsprechen. Wir wollen also wissen, durch welche Objekte wir das Fragezeichen im folgenden Diagramm ersetzen müssen.

$$\begin{array}{ccc} \operatorname{Ideale}(R) & \xrightarrow{\sim} & \operatorname{Eff}\operatorname{Div}(R) \\ \downarrow & & \downarrow \\ ? & \xrightarrow{\sim} & \operatorname{Div}(R) \end{array}$$

Da wir einen Divisor D stets als $D = E - F$ mit effektiven Divisoren E und F schreiben können, liegt die Vermutung nahe, nach etwas wie dem Inversen (bezüglich der Multiplikation) eines Ideals zu suchen. Im Fall eines faktoriellen Dedekindbereichs entsprechen sich (bis auf die Einheiten) Elemente und Hauptdivisoren, und zwar sowohl auf der Ringebene (siehe Bemerkung 11.4) als auch auf der Ebene des Quotientenkörpers. Zu einer rationale Funktion q bzw. dem Hauptdivisor $\operatorname{div}(q)$ gehört in diesem Fall einfach der von q erzeugte R-Untermodul qR des Quotientenkörpers $Q(R)$. Im Fall der rationalen Zahlen sind dies Untergruppen der Form $\frac{1}{10}\mathbb{Z}$ oder $\frac{7}{3}\mathbb{Z}$. Für allgemeine Integritätsbereiche führt man ganz allgemein die sogenannten gebrochenen Ideale ein.

DEFINITION 13.4. Es sei R ein Integritätsbereich mit Quotientenkörper $Q(R)$. Dann nennt man einen endlich erzeugten R-Untermodul $\mathfrak{f}$ des R-Moduls $Q(R)$ ein *gebrochenes Ideal*.

LEMMA 13.5. *Es sei R ein Integritätsbereich mit Quotientenkörper $Q(R)$ und sei $\mathfrak{f} \subseteq Q(R)$ eine Teilmenge. Dann sind folgende Aussagen äquivalent.*

(1) *$\mathfrak{f}$ ist ein gebrochenes Ideal.*
(2) *Es gibt ein endlich erzeugtes*[1] *Ideal $\mathfrak{a}$ in R und ein Element $r \in R$, $r \neq 0$, derart, dass*
$$\mathfrak{f} = \frac{\mathfrak{a}}{r} = \left\{ \frac{a}{r} \mid a \in \mathfrak{a} \right\}$$
gilt.

Beweis. Sei zunächst $\mathfrak{f}$ ein gebrochenes Ideal. Dann ist
$$\mathfrak{f} = R\left(\frac{a_1}{r_1}, \ldots, \frac{a_n}{r_n}\right).$$
Nach Übergang zu einem Hauptnenner kann man annehmen, dass $r = r_1 = \ldots = r_n$ ist. Dann hat man mit dem Ideal $\mathfrak{a} = (a_1, \ldots, a_n)$ eine Beschreibung der gewünschten Art. Ist umgekehrt $\mathfrak{f} = \frac{\mathfrak{a}}{r}$, so ist dies natürlich ein endlich erzeugter R-Untermodul von $Q(R)$. □

Wie für Ideale spielen diejenigen gebrochenen Ideale, die von einem Element erzeugt sind, eine besondere Rolle.

DEFINITION 13.6. Es sei R ein Integritätsbereich mit Quotientenkörper $Q(R)$. Dann nennt man ein gebrochenes Ideal der Form $\mathfrak{f} = Rq$ mit $q \in Q(R)$ ein *gebrochenes Hauptideal*.

Aus Lemma 13.5 ergibt sich sofort, dass für einen Hauptidealbereich jedes gebrochene Ideal ein gebrochenes Hauptideal ist.

DEFINITION 13.7. Es sei R ein Integritätsbereich mit Quotientenkörper $Q(R)$. Dann definiert man für gebrochene Ideale $\mathfrak{f}$ und $\mathfrak{g}$ das *Produkt* $\mathfrak{f} \cdot \mathfrak{g}$ als den von allen Produkten erzeugten R-Untermodul von $Q(R)$, also
$$\mathfrak{f} \cdot \mathfrak{g} := R\langle gf : f \in \mathfrak{f}, g \in \mathfrak{g} \rangle,$$
wobei die Produkte in $Q(R)$ zu nehmen sind.

Wird das gebrochene Ideal $\mathfrak{f}$ als R-Modul von $f_1, \ldots, f_n$ erzeugt und wird das gebrochene Ideal $\mathfrak{g}$ von $g_1, \ldots, g_m$ erzeugt, so wird das Produkt $\mathfrak{fg}$ von den Produkten $f_i g_j$, $1 \leq i \leq n$, $1 \leq j \leq m$, erzeugt. Also ist das Produkt in der Tat wieder endlich erzeugt und damit ein gebrochenes Ideal. Für Ideale stimmt natürlich das Idealprodukt mit dem hier definierten Produkt von

[1] Dies ist bei R noethersch natürlich automatisch erfüllt.

gebrochenen Idealen überein. Das Produkt von gebrochenen Hauptidealen ist wieder ein gebrochenes Hauptideal.

In einem beliebigen Integritätsbereich bilden die gebrochenen Ideale $\neq 0$ keine Gruppe. Für stärkere Aussagen müssen wir jetzt wieder voraussetzen, dass R ein Dedekindbereich ist.

DEFINITION 13.8. Zu einem gebrochenen Ideal $\mathfrak{f} \neq 0$ in einem Dedekindbereich R nennt man

$$\mathfrak{f}^{-1} := \{q \in Q(R) \mid q \cdot \mathfrak{f} \subseteq R\}$$

das zugehörige *inverse gebrochene Ideal*.

LEMMA 13.9. *Es sei R ein Dedekindbereich. Dann gelten folgende Aussagen.*

(1) *Zu gebrochenen Idealen mit der Beziehung $\mathfrak{g} = r\mathfrak{f}$ mit $r \in Q(R)$, $r \neq 0$, gilt für die inversen gebrochenes Ideale die Beziehung $\mathfrak{g}^{-1} = r^{-1}\mathfrak{f}^{-1}$.*
(2) *Zu einem gebrochenen Ideal $\mathfrak{f}$ ist das inverse gebrochene Ideal in der Tat ein gebrochenes Ideal.*
(3) *Es ist $\mathfrak{f} \cdot \mathfrak{f}^{-1} = R$.*

Beweis. (1) Der R-Modulisomorphismus $\mathfrak{f} \to \mathfrak{g}$, $f \mapsto rf$, führt direkt zu einem Isomorphismus $\mathfrak{f}^{-1} \to r^{-1}\mathfrak{g}^{-1}$, $q \mapsto r^{-1}q$, da ja $q\mathfrak{f} \subseteq R$ zu $(r^{-1}q)(r\mathfrak{f}) \subseteq R$ äquivalent ist.

(2) Es ist klar, dass $\mathfrak{f}^{-1}$ ein von 0 verschiedener R-Untermodul von $Q(R)$ ist. Wenn $\mathfrak{f}$ durch $\frac{a_1}{b_1}, \ldots, \frac{a_n}{b_n}$ erzeugt wird, so betrachten wir $\mathfrak{g} = \frac{\mathfrak{f}}{a}$ mit $a = a_1 \cdots a_n$, wobei jetzt $\mathfrak{g}$ ein Erzeugendensystem der Form $\frac{1}{c_1}, \ldots, \frac{1}{c_n}$ mit $c_i \in R$ besitzt. Die Bedingung

$$q\frac{1}{c_i} \in R$$

impliziert $q \in R$. Daher ist das inverse gebrochene Ideal zu $\mathfrak{g}$ selbst ein Ideal, also endlich erzeugt. Dies überträgt sich wegen (1) auf $\mathfrak{f}$.

(3) Für das Produkt ist offenbar

$$\mathfrak{f} \cdot \mathfrak{f}^{-1} \subseteq R.$$

Wenn diese Inklusion echt wäre, so würde es auch ein maximales Ideal $\mathfrak{p}$ oberhalb von $\mathfrak{f} \cdot \mathfrak{f}^{-1}$ geben. Es sei $\mathfrak{f}_\mathfrak{p} = (\pi^n)$ mit einer Ortsuniformisierenden π und mit $n \in \mathbb{Z}$. Es gibt dann auch ein Element $f \in \mathfrak{f}$, das an der Stelle $\mathfrak{p}$ die Ordnung n besitzt. Dazu gibt es auch ein $q \in Q(R)$, das an der Stelle $\mathfrak{p}$ die Ordnung $-n$ und sonst überall eine hinreichend große Ordnung besitzt derart, dass $fq \in R$ ist. Dies ist ein Widerspruch, da fg an der Stelle $\mathfrak{p}$ die Ordnung 0 besitzt.

□

Beispiel 13.10. Wir betrachten im quadratischen Zahlbereich $\mathbb{Z}[\sqrt{-5}]$ das Ideal

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

Aufgrund der Gleichung

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

ist

$$\frac{1-\sqrt{-5}}{2} \cdot \mathfrak{a} \subseteq R, \frac{3}{1+\sqrt{-5}} \cdot \mathfrak{a} \subseteq R, 1 \cdot \mathfrak{a} \subseteq R\,.$$

Wir behaupten, dass das inverse gebrochene Ideal $\mathfrak{a}^{-1}$ gleich

$$\mathfrak{f} = R\left(1, \frac{1-\sqrt{-5}}{2}\right)$$

ist, wobei sich die Inklusion $\mathfrak{f} \subseteq \mathfrak{a}^{-1}$ aus der vorstehenden Zeile ergibt. Andererseits gilt wegen

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

für das Produkt

$$\mathfrak{a} \cdot \mathfrak{f} = R,$$

und dies impliziert nach Aufgabe 13.2 die Gleichheit $\mathfrak{f} = \mathfrak{a}^{-1}$.

Bemerkung 13.11. Ein gebrochenes Ideal $\mathfrak{f} \neq 0$ in einem Dedekindbereich ist ein sogenannter *invertierbarer Modul*. D.h. es ist *lokal isomorph* zum Ring selbst. Mit diesen Formulierungen ist folgendes gemeint: Für ein maximales Ideal (also für ein von 0 verschiedenes Primideal) $\mathfrak{p}$ ist $\mathfrak{f}R_{\mathfrak{p}} = \mathfrak{f}_{\mathfrak{p}}$ (dies ist die Lokalisierung eines Moduls an einem Primideal) ein endlich erzeugter $R_{\mathfrak{p}}$-Modul $\neq 0$, der zugleich im Quotientenkörper liegt. Solche Moduln sind isomorph zu $R_{\mathfrak{p}}$. Siehe Aufgabe 4.29.

Definition 13.12. Es sei R ein Dedekindbereich und

$$D = \sum_{\mathfrak{p}} n_{\mathfrak{p}} \cdot \mathfrak{p}$$

ein Divisor (wobei $\mathfrak{p}$ durch die Menge der Primideale $\neq 0$ läuft). Dann nennt man

$$\{f \in Q(R) \mid \operatorname{div}(f) \geq D\}$$

das *gebrochene Ideal zum Divisor* D. Es wird mit $\mathrm{Id}(D)$ bezeichnet.

Das folgende Lemma zeigt, dass man in der Tat ein gebrochenes Ideal erhält, und dass diese Definition mit der früheren Definition 11.12 verträglich ist.

Lemma 13.13. *Es sei R ein Dedekindbereich und $D = \sum_{\mathfrak{p}} n_{\mathfrak{p}} \cdot \mathfrak{p}$ ein Divisor. Dann ist die Menge $\{f \in Q(R) \mid \operatorname{div}(f) \geq D\}$ ein gebrochenes Ideal. Ist D ein effektiver Divisor, dann ist das so definierte gebrochene Ideal ein Ideal und stimmt mit dem Ideal überein, das einem effektiven Divisor gemäß der Definition 11.12 zugeordnet wird.*

Beweis. Es sei $\mathfrak{f} = \{f \in Q(R) \mid \operatorname{div}(f) \geq D\}$. Gemäß der Konvention, dass $\operatorname{div}(0) = \infty$ zu interpretieren ist, ist $0 \in \mathfrak{f}$. Für Elemente $f_1, f_2 \in Q(R)$ mit $\operatorname{div}(f_1), \operatorname{div}(f_2) \geq D$ gilt nach Lemma 13.3

$$\operatorname{div}(f_1 + f_2) \geq \min(\operatorname{div}(f_1), \operatorname{div}(f_2)) \geq D$$

und

$$\operatorname{div}(rf) = \operatorname{div}(r) + \operatorname{div}(f) \geq D$$

für $r \in R$, da ja $\operatorname{div}(r)$ effektiv ist. Also liegt in der Tat ein R-Modul vor.

Bevor wir die endliche Erzeugtheit nachweisen, betrachten wir die zweite Aussage. Es sei also E ein effektiver Divisor. Wir haben zu zeigen, dass

$$\{f \in Q(R) \mid \operatorname{div}(f) \geq E\} = \{f \in R \mid \operatorname{div}(f) \geq E\}$$

ist, wobei die Inklusion $\supseteq$ klar ist. Die andere Inklusion folgt aus Lemma 13.3 (3).

Zum Nachweis der endlichen Erzeugtheit bemerken wir, dass es nach Lemma 13.3 (4) zu jedem Divisor D ein $r \in R$ derart gibt, dass $D' = D + \operatorname{div}(r)$ effektiv ist. Das zu D' gehörige gebrochene Ideal ist dann ein Ideal, also endlich erzeugt, und dies überträgt sich auf das gebrochene Ideal zu D. □

Definition 13.14. Es sei R ein Dedekindbereich und $\mathfrak{f} \neq 0$ ein von 0 verschiedenes gebrochenes Ideal. Dann nennt man den Divisor

$$\operatorname{div}(\mathfrak{f}) = \sum_{\mathfrak{p}} m_{\mathfrak{p}} \cdot \mathfrak{p}$$

mit

$$m_{\mathfrak{p}} = \min(\operatorname{ord}_{\mathfrak{p}}(f) | f \in \mathfrak{f},\ f \neq 0)$$

den *Divisor zum gebrochenen Ideal* $\mathfrak{f}$.

Da das gebrochene Ideal $\mathfrak{f}$ nach Definition endlich erzeugt ist, muss man das Minimum nur über eine endliche Menge nehmen. Insbesondere ist der zugehörige Divisor wohldefiniert. Für ein Ideal stimmt diese Definition offensichtlich mit der alten überein.

Lemma 13.15. *Es sei R ein Dedekindbereich. Dann gelten folgende Aussagen.*

(1) *Es sei $\mathfrak{f}$ ein gebrochenes Ideal mit einer Darstellung $\mathfrak{f} = \frac{\mathfrak{a}}{h}$ mit $h \in R$ und einem Ideal $\mathfrak{a} \subseteq R$. Dann ist*

$$\operatorname{div}(\mathfrak{f}) = \operatorname{div}(\mathfrak{a}) - \operatorname{div}(h).$$

(2) *Zu einem Divisor D mit $E = D + \operatorname{div}(h)$ effektiv ist*

$$\operatorname{Id}(D) = \frac{\operatorname{Id}(E)}{h}.$$

Beweis. Siehe Aufgabe 13.24. □

Auch die Einzelheiten des Beweises des folgenden Satzes überlassen wir dem Leser, siehe Aufgabe 13.25.

Satz 13.16. *Es sei R ein Dedekindbereich. Dann sind die Zuordnungen*

$$\mathfrak{f} \longmapsto \operatorname{div}(\mathfrak{f}) \quad \textit{und} \quad D \longmapsto \operatorname{Id}(D)$$

zueinander inverse Abbildungen zwischen der Menge der von 0 verschiedenen gebrochenen Ideale und der Menge der Divisoren. Diese Bijektion ist ein Isomorphismus von Gruppen.

Beweis. Wir haben zu zeigen, dass die hintereinandergeschalteten Abbildungen jeweils die Identität ergeben. Dies kann man mittels Lemma 13.15 auf den effektiven Fall zurückführen. Die Zuordnung $\mathfrak{f} \mapsto \operatorname{div}(\mathfrak{f})$ führt die Multiplikation von gebrochenen Idealen in die Addition von Divisoren über, da dies an jedem diskreten Bewertungsring $R_{\mathfrak{p}}$ gilt. Wegen der Bijektivität liegt dann auch links eine Gruppe vor und die Abbildungen sind Gruppenisomorphismen. □

Abbildungsverzeichnis