Prof. Dr. H. Brenner **Osnabrück WS 2016/2017**

Zahlentheorie

Vorlesung 24

Divisoren und gebrochene Ideale

Die Menge der effektiven Divisoren 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 24.1. Sei R ein Zahlbereich. 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,

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

siehe Aufgabe 22.16.

Definition 24.2. Sei R ein Zahlbereich 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 $q = \frac{f}{g}$ 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 $\mathrm{Div}(R)$ bezeichnen. Es liegt (siehe Aufgabe 24.1) unmittelbar ein Gruppenhomomorphismus

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

vor. Das Bild unter dieser Abbildung ist die Untergruppe der Hauptdivisoren, die wir mit H bezeichnen.

Da wir in der letzten Vorlesung eine Bijektion zwischen effektiven Divisoren und von 0 verschiedenen Idealen (und von effektiven Hauptdivisoren mit von 0 verschiedenen Hauptidealen) gestiftet haben, 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.

$$\begin{array}{ccc} \mathrm{Ideale}(R) & \xrightarrow{\sim} & \text{E-Div}(R) \\ \downarrow & & \downarrow \\ ? & \xrightarrow{\sim} & \mathrm{Div}(R) \end{array}$$

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 Zahlbereichs entsprechen sich (bis auf die Einheiten) Elemente und Hauptdivisoren, und zwar sowohl auf der Ringebene (siehe Bemerkung 23.4) als auch auf der Ebene des Quotientenkörpers. Zu einer rationale Funktion q bzw. dem Hauptdivisor $\mathrm{div}(q)$ gehört in diesem Fall einfach der von q erzeugte R-Untermodul qR. Im Fall der rationalen Zahlen sind dies Untergruppen der Form $\frac{1}{10}\mathbb{Z}$ oder $\frac{7}{3}\mathbb{Z}$. Für allgemeine Zahlbereiche führt die folgende Definition zum Ziel.

Definition 24.3. Sei R ein Zahlbereich mit Quotientenkörper $Q(R)$. Dann nennt man einen endlich erzeugten R-Untermodul $\mathfrak{f}$ des R-Moduls $Q(R)$ ein *gebrochenes Ideal*.

Lemma 24.4. *Sei R ein Zahlbereich 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 Ideal $\mathfrak{a}$ in R und ein Element $r \in R$, $r \neq 0$, so dass*

$$\mathfrak{f} = \frac{\mathfrak{a}}{r} = \left\{ \frac{a}{r} \middle| \, a \in \mathfrak{a} \right\}$$

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 24.5. Sei R ein Zahlbereich 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 24.4 ergibt sich sofort, dass für einen Hauptidealbereich jedes gebrochene Ideal ein gebrochenes Hauptideal ist.

Definition 24.6. Sei R ein Zahlbereich 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 gebrochenen Idealen überein. Das Produkt von gebrochenen Hauptidealen ist wieder ein gebrochenes Hauptideal. Man kann direkt zeigen, oder aber den Bijektionssatz weiter unten benutzen, dass die Menge der von 0 verschiedenen gebrochenen Ideale eine Gruppe bilden, und die von 0 verschiedenen gebrochenen Hauptideale darin eine Untergruppe.

Bemerkung 24.7. Zu einem gebrochenen Ideal $\mathfrak{f} \neq 0$ in einem Zahlbereich R nennt man

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

das zugehörige *inverse gebrochene Ideal*. Es ist klar, dass dies ein von 0 verschiedener R-Untermodul von $Q(R)$ ist, die endliche Erzeugtheit ist etwas schwieriger zu zeigen. Zunächst beachte man, dass zu zwei gebrochenen Idealen mit der Beziehung $\mathfrak{g} = r\mathfrak{f}$ mit $r \in Q(R)$ für die inversen Ideale die Beziehung $\mathfrak{g}^{-1} = r^{-1}\mathfrak{f}^{-1}$ gilt. Wenn nun $\mathfrak{f}$ durch $\frac{a_1}{b_1}, \ldots, \frac{a_n}{b_n}$ erzeugt wird, so ist $\mathfrak{f} \cong \frac{\mathfrak{f}}{a} = \mathfrak{g}$ mit $a = a_1 \cdots a_n$ und $\mathfrak{g}$ besitzt ein Erzeugendensystem der Form $\frac{1}{c_1}, \ldots, \frac{1}{c_n}$ mit $c_i \in R$. Die Bedingung

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

impliziert $q \in R$. Daher ist das inverse gebrochene Ideal selbst ein Ideal, also endlich erzeugt.

Für das Produkt ist offenbar

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

es ist aber nicht unmittelbar klar, dass hier sogar Gleichheit gilt. Dies folgt daraus, dass man die Gleichheit lokal testen kann, die Produktbildung lokal ist und die Lokalisierungen diskrete Bewertungsringe sind.

Beispiel 24.8. 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

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

für das Produkt

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

und dies impliziert nach Aufgabe 24.12 die Gleichheit $\mathfrak{f} = \mathfrak{a}^{-1}$.

Ein gebrochenes Ideal $\mathfrak{f} \neq 0$ in einem Zahlbereich 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 22.10.

Definition 24.9. Sei R ein Zahlbereich 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

$$\{f \in Q(R) |\ \mathrm{div}(f) \geq D\}$$

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 23.11 verträglich ist.

LEMMA 24.10. *Sei R ein Zahlbereich und $D = \sum_{\mathfrak{p}} n_{\mathfrak{p}} \cdot \mathfrak{p}$ ein Divisor. Dann ist die Menge $\{f \in Q(R) : \operatorname{div}(f) \geq D\}$ 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 23.11 zugeordnet wird.*

Beweis. Sei $\mathfrak{f} = \{f \in Q(R) | \operatorname{div}(f) \geq D\}$. Gemäß der Konvention, dass $\operatorname{div}(0) = \infty$ zu interpretieren ist, ist $0 \in \mathfrak{f}$. Für zwei Elemente $f_1, f_2 \in Q(R)$ mit $\operatorname{div}(f_1), \operatorname{div}(f_2) \geq D$ gilt

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

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 die zweite Aussage. Sei also E ein effektiver Divisor. Wir haben zu zeigen, dass

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

ist, wobei die Inklusion $\supseteq$ klar ist. Sei also $f \in Q(R)$ und angenommen, der zugehörige Hauptdivisor $\operatorname{div}(f)$ sei $\geq E$. Dann ist $\operatorname{div}(f)$ insbesondere effektiv. Die Effektivität bedeutet $\operatorname{ord}_{\mathfrak{p}}(f) \geq 0$ für jedes von 0 verschiedene Primideal $\mathfrak{p}$ und dies bedeutet $f \in R_{\mathfrak{p}}$. Das heißt, dass f zu jedem diskreten Bewertungsring zu jedem maximalen Ideal von R gehört. Dies bedeutet aber nach Satz 22.9, dass $f \in R$ ist.

Zum Nachweis der endlichen Erzeugtheit bemerken wir, dass es 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 24.11. Sei R ein Zahlbereich 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 24.12. *Sei R ein Zahlbereich. Dann gelten folgende Aussagen.*

(1) *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*
$$\operatorname{div}(\mathfrak{f}) \;=\; \operatorname{div}(a) - \operatorname{div}(h).$$
(2) *Zu einem Divisor D gibt es ein $h \in R$ derart, dass $D + \operatorname{div}(h)$ effektiv ist.*
(3) *Zu einem Divisor D mit $E = D + \operatorname{div}(h)$ effektiv ist*
$$\operatorname{Id}(D) \;=\; \frac{\operatorname{Id}(E)}{h}.$$

Beweis. Siehe Aufgabe 24.14. □

Auch die Einzelheiten des Beweises des folgenden Satzes überlassen wir dem Leser, siehe Aufgabe 24.15.

SATZ 24.13. *Sei R ein Zahlbereich. 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 24.12 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. □