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

Zahlentheorie

Vorlesung 23

Die Ordnung an einem Primideal

Zu einem Zahlbereich R und einem Primideal $\mathfrak{p} \neq 0$ ist nach Korollar 22.18 die Lokalisierung $R_{\mathfrak{p}}$ ein diskreter Bewertungsring und somit ergibt sich insgesamt eine Abbildung

$$R \setminus \{0\} \longrightarrow R_{\mathfrak{p}} \setminus \{0\} \xrightarrow{\text{ord}} \mathbb{N}.$$

Definition 23.1. Sei R ein Zahlbereich, $\mathfrak{p} \neq 0$ ein Primideal in R und $f \in R$, $f \neq 0$. Dann heißt die Ordnung $\text{ord}(f)$ im diskreten Bewertungsring $R_{\mathfrak{p}}$ die *Ordnung* von f am Primideal $\mathfrak{p}$ (oder an der Primstelle $\mathfrak{p}$ oder in $R_{\mathfrak{p}}$). Sie wird mit $\text{ord}_{\mathfrak{p}}(f)$ bezeichnet.

Lemma 23.2. *Sei R ein Zahlbereich und $\mathfrak{p} \neq 0$ ein Primideal in R. Dann hat die Ordnung an $\mathfrak{p}$, also*

$$R \setminus \{0\} \longrightarrow \mathbb{N},\ f \longmapsto \text{ord}_{\mathfrak{p}}(f),$$

folgende Eigenschaften.

(1) $\text{ord}_{\mathfrak{p}}(fg) = \text{ord}_{\mathfrak{p}}(f) + \text{ord}_{\mathfrak{p}}(g)$.
(2) $\text{ord}_{\mathfrak{p}}(f+g) \geq \min\{\text{ord}_{\mathfrak{p}}(f), \text{ord}_{\mathfrak{p}}(g)\}$.
(3) $f \in \mathfrak{p}$ *genau dann, wenn* $\text{ord}_{\mathfrak{p}}(f) \geq 1$.

Beweis. (1) und (2) folgen direkt aus Lemma 22.14. Bei (3) ist zu beachten, dass für $f \in R$ gilt, dass $f \in \mathfrak{p}$ genau dann ist, wenn $f \in \mathfrak{p}R_{\mathfrak{p}}$ ist. Letzteres bedeutet nämlich, dass $f = q_1 f_1 + \cdots + q_n f_n$ ist mit $f_i \in \mathfrak{p}$ und $q_i \in R_{\mathfrak{p}}$, also $q_i = \frac{r_i}{s_i}$ mit $s_i \notin \mathfrak{p}$. Mit dem Hauptnenner $s = s_1 \cdots s_n$ ist dann $sf = a_1 f_1 + \cdots + a_n f_n \in \mathfrak{p}$, woraus $f \in \mathfrak{p}$ folgt. Damit folgt die Behauptung aus Lemma 22.14. □

Definition 23.3. Sei R ein Zahlbereich und $f \in R$, $f \neq 0$. Dann heißt die Abbildung, die jedem Primideal $\mathfrak{p} \neq 0$ in R die Ordnung $\text{ord}_{\mathfrak{p}}(f)$ zuordnet, der durch f definierte *Hauptdivisor*. Er wird mit $\text{div}(f)$ bezeichnet und als formale Summe

$$\text{div}(f) = \sum_{\mathfrak{p}} \text{ord}_{\mathfrak{p}}(f) \cdot \mathfrak{p}$$

geschrieben.

Die Ordnung an einem Primideal nennt man in diesem Zusammenhang auch die Verschwindungsordnung. Die Ordnung ist ja genau dann positiv, wenn f zum Primideal $\mathfrak{p}$ gehört, und dies ist genau dann der Fall, wenn unter der Abbildung

$$R \longrightarrow R/\mathfrak{p} \longrightarrow Q(R/\mathfrak{p})$$

das Element f auf 0 abgebildet wird, also an dieser Stelle verschwindet. Eine höhere Verschwindungsordnung bedeutet, dass f nicht nur einfach, sondern mit einer gewissen Vielfachheit verschwindet. Der Hauptdivisor zu f notiert also, mit welcher Verschwindungsordnung die Funktion f an den verschiedenen Primstellen verschwinden.

Bemerkung 23.4. Es sei R ein faktorieller Zahlbereich. Dann lässt sich der Hauptdivisor zu einem Ringelement $f \in R$, $f \neq 0$, unmittelbar aus der Primfaktorzerlegung ablesen. Wenn

$$f = up_1^{r_1} \cdots p_k^{r_k}$$

mit einer Einheit u und paarweise nicht assoziierten Primelementen p_i ist, so ist der Hauptdivisor zu f gleich

$$\operatorname{div}(f) = \sum_{i=1}^{k} r_i(p_i).$$

Dies beruht einfach darauf, dass die Ordnung von f in der Lokalisierung $R_{(p_i)}$ gleich r_i ist.

Lemma 23.5. *Sei R ein Zahlbereich. Dann hat die Abbildung, die einem Ringelement $\neq 0$ den Hauptdivisor zuordnet, also*

$$R \setminus \{0\} \longrightarrow \text{Hauptdivisoren}, \ f \longmapsto \operatorname{div}(f),$$

folgende Eigenschaften.

(1) $\operatorname{div}(fg) = \operatorname{div}(f) + \operatorname{div}(g)$.
(2) $\operatorname{div}(f+g) \geq \min\{\operatorname{div}(f), \operatorname{div}(g)\}$.

Hierbei sind die Operationen rechts punktweise definiert.

Beweis. Dies folgt direkt aus Lemma 23.2 durch Betrachtung an den einzelnen Primidealen. □

Lemma 23.6. *Sei R ein Zahlbereich und $f \in R$, $f \neq 0$. Dann ist nur für endlich viele Primideale $\mathfrak{p} \neq 0$ in R die Ordnung $\operatorname{ord}_{\mathfrak{p}}(f)$ von 0 verschieden. Das heißt, dass der Hauptdivisor $\operatorname{div}(f) = \sum_{\mathfrak{p}} \operatorname{ord}_{\mathfrak{p}}(f) \cdot \mathfrak{p}$ eine endliche Summe ist.*

Beweis. Sei $\mathfrak{p} \neq 0$ ein Primideal in R und $f \notin \mathfrak{p}$. Dann ist f in $R_{\mathfrak{p}}$ eine Einheit. Damit ist $\operatorname{ord}_{\mathfrak{p}}(f) = 0$. Da der Restklassenring $R/(f)$ nach Satz 18.14 endlich ist, folgt sofort, dass f nur in endlich vielen Primidealen enthalten ist, und nur für diese ist $\operatorname{ord}_{\mathfrak{p}}(f) > 0$. □

Effektive Divisoren

DEFINITION 23.7. Sei R ein Zahlbereich. Ein *effektiver 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 $n_{\mathfrak{p}}$ natürliche Zahlen sind mit $n_{\mathfrak{p}} = 0$ für fast alle $\mathfrak{p}$.

Obiges Lemma zeigt, dass ein Hauptdivisor zu einem Ringelement wirklich ein effektiver Divisor ist. Wir werden im Weiteren sehen, dass die Frage, welche Divisoren Hauptdivisoren sind, eng mit der Frage nach der Faktorialität von Zahlbereichen zusammenhängt. Der Zugang über Divisoren hat den Vorteil, dass er erlaubt (siehe weiter unten), eine Gruppe, die sogenannte *Divisorenklassengruppe* einzuführen, die die Abweichung von der Faktorialität messen kann.

Ein effektiver Divisor gibt für jede Primstelle eine Verschwindungsordnung an. Eine naheliegende Frage ist dann, ob dieses Ordnungsverhalten durch eine Funktion realisiert werden kann, also ob der Divisor ein Hauptdivisor ist.

DEFINITION 23.8. Sei R ein Zahlbereich und $\mathfrak{a} \neq 0$ ein von 0 verschiedenes Ideal in R. Dann nennt man den Divisor

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

mit

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

den *Divisor zum Ideal* $\mathfrak{a}$.

BEMERKUNG 23.9. Man kann den Divisor zu einem Ideal auch durch

$$\operatorname{div}(\mathfrak{a}) \;=\; \min\left\{\operatorname{div}(f) \middle|\; f \in \mathfrak{a},\; f \neq 0\right\}$$

definieren, wobei das Minimum über Divisoren komponentenweise erklärt ist. Es gibt im Allgemeinen kein Element, das an allen Primstellen simultan das Minimum annimmt. Da zu einem einzelnen Element $0 \neq f \in \mathfrak{a}$ der zugehörige Hauptdivisor nur an endlich vielen Stellen von 0 verschieden ist, gilt das erst recht für den Divisor zu einem Ideal.

Die Ordnung $\operatorname{ord}_{\mathfrak{p}}(\mathfrak{a})$ kann man auch als Ordnung des Ideals $\operatorname{ord}(\mathfrak{a}R_{\mathfrak{p}})$ im diskreten Bewertungsring $R_{\mathfrak{p}}$ ansehen. Dabei ist $\mathfrak{a}R_{\mathfrak{p}}$ das Erweiterungsideal zu $\mathfrak{a}$ in $R_{\mathfrak{p}}$. Dieses Ideal hat einen Erzeuger p^k, wobei p ein Primelement im diskreten Bewertungsring ist; die Ordnung ist dann k.

LEMMA 23.10. *Sei R ein Zahlbereich. Dann erfüllt die Zuordnung (für von 0 verschiedene Ideale)*

$$\mathfrak{a} \longmapsto \operatorname{div}(\mathfrak{a})$$

folgende Eigenschaften:

(1) $\mathrm{div}(\mathfrak{p}) = 1 \cdot \mathfrak{p}$ *für ein Primideal* $\mathfrak{p} \neq 0$.
(2) $\mathrm{div}(\mathfrak{a} \cdot \mathfrak{b}) = \mathrm{div}(\mathfrak{a}) + \mathrm{div}(\mathfrak{b})$.
(3) *Für* $\mathfrak{a} \subseteq \mathfrak{b}$ *ist* $\mathrm{div}(\mathfrak{a}) \geq \mathrm{div}(\mathfrak{b})$.
(4)
$$\mathrm{div}(\mathfrak{a} + \mathfrak{b}) = \min\{\mathrm{div}(\mathfrak{a}), \mathrm{div}(\mathfrak{b})\}.$$

Beweis. (1) Für jedes Element $f \in \mathfrak{p}$ gilt auch $f \in \mathfrak{p}R_{\mathfrak{p}}$ und daher ist $\mathrm{ord}_{\mathfrak{p}}(f) \geq 1$. Umgekehrt besitzt der diskrete Bewertungsring $R_{\mathfrak{p}}$ ein Element p, das das maximale Ideal $\mathfrak{p}R_{\mathfrak{p}}$ erzeugt und die Ordnung eins hat. Man kann $p = \frac{a}{b}$ mit $a, b \in R$ und $b \notin \mathfrak{p}$ schreiben. Dabei ist $a \in \mathfrak{p}$ und a hat in $R_{\mathfrak{p}}$ die Ordnung 1.

Sei nun $\mathfrak{q} \neq \mathfrak{p}$ ein weiteres Primideal $\neq 0$. Da beide maximal sind gibt es ein Element $g \in \mathfrak{p}$, $g \notin \mathfrak{q}$. Dieses hat dann in $\mathfrak{q}$ die Ordnung 0.

(2) Fixiere ein Primideal $\mathfrak{p}$. Sei $h \in \mathfrak{a} \cdot \mathfrak{b}$ und schreibe $h = \sum_{i=1}^{k} f_i g_i$ mit $f_i \in \mathfrak{a}$ und $g_i \in \mathfrak{b}$. Dann ist nach Lemma 23.5

$$\begin{array}{rcl} \mathrm{div}(h) & \geq & \min\{\mathrm{div}(f_i g_i) : i = 1, \ldots, k\} \\ & \geq & \min\{\mathrm{div}(f_i) + \mathrm{div}(g_i) : i = 1, \ldots, k\} \\ & \geq & \mathrm{div}(\mathfrak{a}) + \mathrm{div}(\mathfrak{b}). \end{array}$$

Für die Umkehrung schreiben wir $\mathrm{div}(\mathfrak{a}) = \sum_{\mathfrak{q}} n_{\mathfrak{q}} \cdot \mathfrak{q}$ und $\mathrm{div}(\mathfrak{b}) = \sum_{\mathfrak{q}} m_{\mathfrak{q}} \cdot \mathfrak{q}$. Zu fixiertem $\mathfrak{p}$ gibt es ein $f \in \mathfrak{a}$ und ein $g \in \mathfrak{b}$ mit $\mathrm{ord}_{\mathfrak{p}}(f) = n_{\mathfrak{p}}$ und $\mathrm{ord}_{\mathfrak{p}}(g) = m_{\mathfrak{p}}$. Dann ist $fg \in \mathfrak{a}\mathfrak{b}$ und

$$\mathrm{ord}_{\mathfrak{p}}(fg) = \mathrm{ord}_{\mathfrak{p}}(f) + \mathrm{ord}_{\mathfrak{p}}(g) = n_{\mathfrak{p}} + m_{\mathfrak{p}}.$$

(3) Das ist trivial.
(4) Die Abschätzung „$\geq$“ folgt aus $\mathrm{div}(f + g) \geq \min\{\mathrm{div}(f), \mathrm{div}(g)\}$. Die Abschätzung „$\leq$“ folgt aus Teil (3).

□

Definition 23.11. Sei R ein Zahlbereich und

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

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

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

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

In der vorstehenden Definition verwenden wir die Konvention, dass in Ungleichungen der Ausdruck $\mathrm{div}(0)$ als ∞ zu verstehen ist. Damit gehört also 0 zu $\mathrm{Id}(D)$. Es ergibt sich sofort, dass es sich in der Tat um ein Ideal handelt. Es ist auch nicht das Nullideal, da wir zu den endlich vielen Primidealen $\mathfrak{p}_i$, $i = 1, \ldots, k$, , mit $n_i = n_{\mathfrak{p}_i} > 0$ Elemente $0 \neq f_i \in \mathfrak{p}_i$ mit $\mathrm{ord}_{\mathfrak{p}_i}(f_i) = 1$ wählen können. Dann gehört aber das Produkt $f_1^{n_1} \cdots f_k^{n_k}$ zu dem zu D gehörenden Ideal.

Der folgende Satz zeigt, dass die beiden soeben eingeführten Zuordnungen zwischen den effektiven Divisoren und den von 0 verschiedenen Idealen in einem Zahlbereich invers zueinander sind. Dies sollte man als eine einfache und übersichtliche Beschreibung für die Menge aller Ideale ansehen.

Satz 23.12. *Sei R ein Zahlbereich. Dann sind die Zuordnungen*

$$\mathfrak{a} \longmapsto \operatorname{div}(\mathfrak{a}) \text{ und } D \longmapsto \operatorname{Id}(D)$$

zueinander inverse Abbildungen zwischen der Menge der von 0 verschiedenen Ideale und der Menge der effektiven Divisoren. Diese Bijektion übersetzt das Produkt von Idealen in die Summe von Divisoren.

Beweis. Wir starten mit einem Ideal $\mathfrak{a} \neq 0$ und vergleichen $\mathfrak{a}$ und $\operatorname{Id}(\operatorname{div}(\mathfrak{a}))$. Sei zunächst $f \in \mathfrak{a}$. Es ist dann $\operatorname{ord}_{\mathfrak{p}}(f) \geq \min\{\operatorname{ord}_{\mathfrak{p}}(g) | \, g \in \mathfrak{a}\}$ für jedes Primideal $\mathfrak{p} \neq 0$, so dass natürlich $\operatorname{div}(f) \geq \operatorname{div}(\mathfrak{a})$ gilt. Also ist $f \in \operatorname{Id}(\operatorname{div}(\mathfrak{a}))$. Ist hingegen $f \notin \mathfrak{a}$, so gibt es nach Aufgabe 22.15 auch ein Primideal $\mathfrak{p} \neq 0$ mit $f \notin \mathfrak{a}R_{\mathfrak{p}}$. Da $R_{\mathfrak{p}}$ ein diskreter Bewertungsring ist, gilt $\operatorname{ord}_{\mathfrak{p}}(f) < \operatorname{ord}_{\mathfrak{p}}(\mathfrak{a})$. Also ist $\operatorname{div}(f) \not\geq \operatorname{div}(\mathfrak{a})$ und somit $f \notin \operatorname{Id}(\operatorname{div}(\mathfrak{a}))$. Insbesondere ist die Abbildung injektiv. Die Surjektivität ergibt sich aus Lemma 23.10 (1) in Verbindung mit Lemma 23.10 (2), was auch den Zusatz ergibt. □

Korollar 23.13. *Sei R ein Zahlbereich und seien $\mathfrak{a}$ und $\mathfrak{b}$ Ideale in R. Dann gilt $\mathfrak{a} \subseteq \mathfrak{b}$ genau dann, wenn es ein Ideal $\mathfrak{c}$ mit $\mathfrak{a} = \mathfrak{b}\mathfrak{c}$ gibt. Bei $\mathfrak{b}$ ist $\mathfrak{c}$ eindeutig bestimmt.*

Beweis. Die Implikation „$\Leftarrow$“ gilt in beliebigen kommutativen Ringen. Die andere Implikation ist richtig, wenn $\mathfrak{a} = 0$ ist. Wir können also annehmen, dass die beteiligten Ideale von 0 verschieden sind. Die Bedingung impliziert nach Lemma 23.10 (3), dass $\operatorname{div}(\mathfrak{a}) \geq \operatorname{div}(\mathfrak{b})$ ist. Somit ist $\operatorname{div}(\mathfrak{a}) = \operatorname{div}(\mathfrak{b}) + E$ mit einem effektiven Divisor E. Nach Satz 23.12 übersetzt sich dies zurück zu $\mathfrak{a} = \mathfrak{b} \cdot \operatorname{Id}(E)$, so dass mit $\mathfrak{c} = \operatorname{Id}(E)$ die rechte Seite erfüllt ist. □

DDR Briefmarke

Die folgende Aussage heißt *Satz von Dedekind*. Sie liefert für jeden Zahlbereich auf der Idealebene einen Ersatz für die eindeutige Primfaktorzerlegung.

SATZ 23.14. *Sei R ein Zahlbereich und $\mathfrak{a} \neq 0$ ein Ideal in R. Dann gibt es eine Produktdarstellung*

$$\mathfrak{a} = \mathfrak{p}_1^{r_1} \cdots \mathfrak{p}_k^{r_k}$$

mit (bis auf die Reihenfolge) eindeutig bestimmten Primidealen $\mathfrak{p}_i \neq 0$ aus R und eindeutig bestimmten Exponenten r_i, $i = 1, \ldots, k$.

Beweis. Wir benutzen Satz 23.12, also die bijektive Beziehung zwischen Idealen $\neq 0$ und effektiven Divisoren. Auf der Seite der Divisoren haben wir offenbar eine eindeutige Darstellung

$$\operatorname{div}(\mathfrak{a}) = \sum_{i=1}^{k} r_i \mathfrak{p}_i$$

mit geeigneten Primidealen $\mathfrak{p}_i$. Wendet man auf diese Darstellung die Abbildung $D \mapsto \operatorname{Id}(D)$ an, so erhält man links das Ideal zurück. Es genügt also zu zeigen, dass der Divisor rechts auf das Ideal $\mathfrak{p}_1^{r_1} \cdots \mathfrak{p}_k^{r_k}$ abgebildet wird. Dies folgt aber direkt aus Satz 23.12. □

KOROLLAR 23.15. *Sei R ein Zahlbereich und $f \in R$, $f \neq 0$. Dann gibt es eine Produktdarstellung für das Hauptideal*

$$(f) = \mathfrak{p}_1^{r_1} \cdots \mathfrak{p}_k^{r_k}$$

mit (bis auf die Reihenfolge) eindeutig bestimmten Primidealen $\mathfrak{p}_i \neq 0$ aus R und eindeutig bestimmten Exponenten r_i, $i = 1, \ldots, k$.

Beweis. Dies folgt direkt aus Satz 23.14. □

Abbildungsverzeichnis