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

Algebraische Zahlentheorie

Vorlesung 11

Die Ordnung an einem Primideal

Zu einem Dedekindbereich R und einem Primideal $\mathfrak{p} \neq 0$ ist nach Korollar 10.18 die Lokalisierung $R_{\mathfrak{p}}$ ein diskreter Bewertungsring und somit ergibt sich insgesamt eine Abbildung

$$R \setminus \{0\} \longrightarrow R_{\mathfrak{p}} \setminus \{0\} \stackrel{\operatorname{ord}}{\longrightarrow} \mathbb{N}\,.$$

DEFINITION 11.1. Sei R ein Dedekindbereich, $\mathfrak{p} \neq 0$ ein Primideal in R und $f \in R$, $f \neq 0$. Dann heißt die Ordnung $\operatorname{ord}(f)$ 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 $\operatorname{ord}_{\mathfrak{p}}(f)$ bezeichnet.

LEMMA 11.2. *Es sei R ein Dedekindbereich und $\mathfrak{p} \neq 0$ ein Primideal in R. Dann hat die Ordnung an $\mathfrak{p}$, also die Abbildung*

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

folgende Eigenschaften.

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

Beweis. (1) und (2) folgen direkt aus Lemma 10.15. Bei (3) ist zu beachten, dass für $f \in R$ gilt, dass $f \in \mathfrak{p}$ genau dann gilt, wenn $f \in \mathfrak{p}R_{\mathfrak{p}}$ ist. Letzteres bedeutet nämlich, dass $f = q_1 f_1 + \cdots + q_n f_n$ mit $f_i \in \mathfrak{p}$ und $q_i \in R_{\mathfrak{p}}$ ist, 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 10.15. □

DEFINITION 11.3. Es sei R ein Dedekindbereich und $f \in R$, $f \neq 0$. Dann heißt die Abbildung, die jedem Primideal $\mathfrak{p} \neq 0$ in R die Ordnung $\operatorname{ord}_{\mathfrak{p}}(f)$ zuordnet, der durch f definierte *Hauptdivisor*. Er wird mit $\operatorname{div}(f)$ bezeichnet und als formale Summe

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

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 verschwindet.

Bemerkung 11.4. Es sei R ein faktorieller Dedekindbereich. 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 11.5. *Es sei R ein Dedekindbereich. 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)
$$\operatorname{div}(f+g) \geq \min(\operatorname{div}(f), \operatorname{div}(g)).$$

(3) *Es ist f genau dann eine Einheit, wenn $\operatorname{div}(f) = 0$ ist.*

Beweis. Dies folgt direkt aus Lemma 11.2 durch Betrachtung an den einzelnen Primidealen. □

Lemma 11.6. *Es sei R ein Dedekindbereich 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. Es ist $R/(f)$ nulldimensional, deshalb folgt die Aussage aus Aufgabe 11.1. □

Im zahlentheoretischen Kontext folgt die letzte Aussage auch direkt aus der Endlichkeit der Restklassenringe.

Beispiel 11.7. Wir betrachten im quadratischen Zahlbereich R zu $D = -5$, also $R = A_{-5} = \mathbb{Z}[\sqrt{-5}] = \mathbb{Z}[X]/(X^2+5)$, das Ideal

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

Nach Beispiel 10.7 ist dies kein Hauptideal. Wir wollen die Hauptdivisoren zu den beiden Idealerzeugern 2 und $1+\sqrt{-5}$ berechnen. Der erste Schritt ist dabei, die Primideale oberhalb des Elementes zu bestimmen, was am einfachsten durch eine Restklassenbetrachtung geschieht. Der Restklassenring modulo 2 ist

$$\begin{aligned} R/(2) &= \mathbb{Z}[X]/(X^2+5,2) \\ &= \mathbb{Z}/(2)[X]/(X^2+5) \\ &= \mathbb{Z}/(2)[X]/(X^2+1) \\ &= \mathbb{Z}/(2)[X]/(X+1)^2. \end{aligned}$$

Dies ist ein nichtreduzierter Ring mit nur einem maximalen Ideal. In der Lokalisierung $R_{(2,1+\sqrt{-5})}$ gilt

$$2 = \frac{1}{\left(-2+\sqrt{5}\right)}\left(1+\sqrt{-5}\right)^2,$$

was zeigt, dass $1+\sqrt{-5}$ dort ein Erzeuger des maximalen Ideals ist und dass die Ordnung von 2 dort gleich 2 ist. Deshalb gilt

$$\operatorname{div}(2) = 2\mathfrak{p}.$$

Wegen

$$R/(1+\sqrt{-5}) = \mathbb{Z}[X]/(X^2+5, 1+X) = \mathbb{Z}/(6) = \mathbb{Z}/(2) \times \mathbb{Z}/(3)$$

ist $1+\sqrt{-5}$ auch noch im Primideal $\mathfrak{q} = (3, 1+\sqrt{-5})$ enthalten und besitzt dort ebenfalls die Ordnung 1. Daher ist

$$\operatorname{div}\left(1+\sqrt{-5}\right) = \mathfrak{p}+\mathfrak{q}.$$

Effektive Divisoren

Definition 11.8. Es sei R ein Dedekindbereich. 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 $\mathfrak{p}$.

Lemma 11.6 zeigt, dass ein Hauptdivisor zu einem Ringelement $\neq 0$ wirklich ein effektiver Divisor ist. 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. Wir werden im Weiteren sehen, dass die Frage, welche Divisoren Hauptdivisoren sind, eng mit der Frage nach der Faktorialität von Dedekindbereichen 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. Die Menge der effektiven Divisoren wird mit $\operatorname{Eff}\operatorname{Div}(R)$ bezeichnet, es handelt sich um ein kommutatives additives Monoid, das als Monoid von den *Primdivisoren* $\mathfrak{p}$ erzeugt wird.

Definition 11.9. Es sei R ein Dedekindbereich 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

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

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

Bemerkung 11.10. Man kann den Divisor zu einem Ideal auch durch

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

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 11.11. *Es sei R ein Dedekindbereich. Dann erfüllt die Zuordnung (für von 0 verschiedene Ideale)*

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

folgende Eigenschaften.

(1)
$$\operatorname{div}(\mathfrak{p}) = 1 \cdot \mathfrak{p}$$
für ein Primideal $\mathfrak{p} \neq 0$.

(2)
$$\operatorname{div}(\mathfrak{a} \cdot \mathfrak{b}) = \operatorname{div}(\mathfrak{a}) + \operatorname{div}(\mathfrak{b}).$$

(3) *Für* $\mathfrak{a} \subseteq \mathfrak{b}$ *ist* $\operatorname{div}(\mathfrak{a}) \geq \operatorname{div}\operatorname{div}(\mathfrak{b})$.

(4)
$$\operatorname{div}(\mathfrak{a}+\mathfrak{b}) \;=\; \min\{\operatorname{div}(\mathfrak{a}),\operatorname{div}(\mathfrak{b})\}.$$

Beweis. (1) Für jedes Element $f \in \mathfrak{p}$ gilt auch $f \in \mathfrak{p}R_{\mathfrak{p}}$ und daher ist $\operatorname{ord}_{\mathfrak{p}}(f) \geq 1$. Umgekehrt besitzt der diskrete Bewertungsring $R_{\mathfrak{p}}$ ein Element p, das das maximale Ideal $\mathfrak{p}R_{\mathfrak{p}}$ erzeugt und die Ordnung 1 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 Ideale 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 11.5
$$\begin{aligned}\operatorname{div}(h) &\geq \min\{\operatorname{div}(f_i g_i) : i = 1,\dots,k\}\\ &\geq \min\{\operatorname{div}(f_i)+\operatorname{div}(g_i) : i = 1,\dots,k\}\\ &\geq \operatorname{div}(\mathfrak{a})+\operatorname{div}(\mathfrak{b}).\end{aligned}$$
Für die Umkehrung schreiben wir $\operatorname{div}(\mathfrak{a}) = \sum_{\mathfrak{q}} n_{\mathfrak{q}}\cdot\mathfrak{q}$ und $\operatorname{div}(\mathfrak{b}) = \sum_{\mathfrak{q}} m_{\mathfrak{q}}\cdot\mathfrak{q}$. Zu fixiertem $\mathfrak{p}$ gibt es ein $f \in \mathfrak{a}$ und ein $g \in \mathfrak{b}$ mit $\operatorname{ord}_{\mathfrak{p}}(f) = n_{\mathfrak{p}}$ und $\operatorname{ord}_{\mathfrak{p}}(g) = m_{\mathfrak{p}}$. Dann ist $fg \in \mathfrak{a}\mathfrak{b}$ und
$$\operatorname{ord}_{\mathfrak{p}}(fg) \;=\; \operatorname{ord}_{\mathfrak{p}}(f)+\operatorname{ord}_{\mathfrak{p}}(g) \;=\; n_{\mathfrak{p}}+m_{\mathfrak{p}}.$$

(3) Das ist trivial.

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

□

Definition 11.12. Es sei R ein Dedekindbereich 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
$$\{f \in R \mid \operatorname{div}(f) \geq D\}$$
das *Ideal zum Divisor* D. Es wird mit $\operatorname{Id}(D)$ bezeichnet.

In der vorstehenden Definition verwenden wir die Konvention, dass in Ungleichungen der Ausdruck $\operatorname{div}(0)$ als ∞ zu verstehen ist. Damit gehört also 0 zu $\operatorname{Id}(D)$. 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 $\mathfrak{p}_i$, $i = 1,\dots,k$, mit $n_i = n_{\mathfrak{p}_i} > 0$ Elemente $0 \neq f_i \in \mathfrak{p}_i$ mit $\operatorname{ord}_{\mathfrak{p}_i}(f_i) = 1$ 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 Dedekindbereich invers zueinander sind. Dies sollte man als eine einfache und übersichtliche Beschreibung für die Menge aller Ideale ansehen.

SATZ 11.13. *Es sei R ein Dedekindbereich. 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 $\operatorname{ord}_{\mathfrak{p}}(f) \geq \min\{\operatorname{ord}_{\mathfrak{p}}(g) \mid g \in \mathfrak{a}\}$ 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 4.19 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 11.11 (1) in Verbindung mit Lemma 11.11 (2), was auch den Zusatz ergibt. □

Abbildungsverzeichnis