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

Algebraische Zahlentheorie

Vorlesung 10

Die Norm für Zahlbereiche

Nach Korollar 7.11 ist die Norm eines Elementes eines Zahlbereiches ganzzahlig.

LEMMA 10.1. *Es sei R der Ganzheitsring einer endlichen Körpererweiterung $\mathbb{Q} \subseteq L$. Dann ist $f \in R$ genau dann eine Einheit, wenn $N(f) = \pm 1$ ist.*

Beweis. Wenn $f \in R$ eine Einheit ist, so ist $fg = 1$ mit einem $g \in R$ und aus der Multiplikativität der Norm folgt

$$N(f)N(g) = N(1) = 1,$$

woraus nach Korollar 7.11 $N(f) = \pm 1$ folgt. Die Umkehrung folgt aus Korollar 8.6 und daraus, dass dann die Multiplikationsabbildung zu f auf $R \cong \mathbb{Z}^n$ bijektiv ist. □

LEMMA 10.2. *Es sei R ein Zahlbereich vom Grad d und $n \in \mathbb{Z}$. Dann ist die Norm von n in R gleich n^d.*

Beweis. Dies ist ein Spezialfall von Lemma 8.7 (Körper- und Galoistheorie (Osnabrück 2018-2019)). □

Die Norm von Idealen

DEFINITION 10.3. Zu einem Ideal $\mathfrak{a} \neq 0$ in einem Zahlbereich R heißt die (endliche) Anzahl des Restklassenringes $R/\mathfrak{a}$ die *Norm* von $\mathfrak{a}$. Sie wird mit

$$N(\mathfrak{a})$$

bezeichnet.

BEISPIEL 10.4. Zu einem von 0 verschiedenen Ideal $(n) \subseteq \mathbb{Z}$ mit $n > 0$ ist die Norm einfach gleich n, da ja der Restklassenring $\mathbb{Z}/(n)$ genau n Elemente besitzt.

LEMMA 10.5. *Es sei $\mathfrak{a} \neq 0$ ein Ideal in einem Zahlbereich R. Dann ist $N(\mathfrak{a}) \in \mathfrak{a}$.*

Beweis. Wir betrachten die Abbildung

$$\mathbb{Z} \longrightarrow R \longrightarrow R/\mathfrak{a}\,.$$

Der Ring rechts hat nach Definition $N(\mathfrak{a})$ Elemente. Deshalb gehört diese Zahl zum Kern der Gesamtabbildung. □

Die Norm eines Ideals berechnet man am besten, indem man nach und nach den Restklassenring vereinfacht. Ein entscheidender Schritt ist dabei, eine ganze Zahl $n \neq 0$ in dem Ideal zu finden, da man dann über dem endlichen Ring $\mathbb{Z}/(n)$ arbeiten und weiter vereinfachen kann. Dieses Verfahren hilft aufgrund der folgenden Aussage auch bei der Berechnung der Norm von Elementen.

Lemma 10.6. *Es sei R ein Zahlbereich und $f \in R$, $f \neq 0$. Dann ist der Betrag der Norm von f gleich der Norm des Hauptideals fR.*

Beweis. Das Hauptideal Rf ist das Bild des injektiven Gruppenhomomorphismus

$$R \longrightarrow R,\, 1 \longmapsto f.$$

Dieser wird unter einer Identifizierung $R = \mathbb{Z}^n$ (also der Wahl einer Ganzheitsbasis von R) durch die zu f gehörende Multiplikationsmatrix M_f beschrieben. Es liegt insgesamt dias kommutative Diagramm

$$\begin{array}{ccccccc} R & \xrightarrow{\mu_f} & R & \longrightarrow & R/fR & \longrightarrow & 0 \\ \downarrow & & \downarrow & & \downarrow & & \downarrow \\ \mathbb{Z}^n & \xrightarrow{M_f} & \mathbb{Z}^n & \longrightarrow & \mathbb{Z}^n/\operatorname{bild} M_f & \longrightarrow & 0 \end{array}$$

mit vertikalen Isomorpien vor. Die Determinante von M_f ist die Norm von f, und die Anzahl der Elemente in der Restklassengruppe R/fR ist die Norm des Hauptideals. Daher folgt die Aussage aus Satz Anhang 7.1. □

Beispiel 10.7. Wir betrachten im quadratischen Zahlbereich R zu $D = -5$ das Ideal

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

Wir behaupten, dass es kein Hauptideal ist und verwenden dabei, dass die Norm dieses Ideals gleich 2 ist. Wäre nämlich $\mathfrak{p} = (f)$ mit einem $f \in R$, so müsste nach . auch

$$|N(f)| = 2$$

gelten. Allerdings ist die Norm von $f = a + b\sqrt{-5}$ gleich $N(f) = a^2 + 5b^2$ und dies kann nicht gleich 2 sein.

Korollar 10.8. *Es sei f ein Element in einem Zahlbereich R. Dann ist $N(f) \in fR$. Insbesondere ist $\frac{N(f)}{f} \in R$ bei $f \neq 0$.*

Beweis. Dies folgt aus Lemma 10.6 und Lemma 10.5, angewendet auf das Hauptideal $\mathfrak{a} = (f)$. □

Die Norm $R \to \mathbb{Z}$ hat die Eigenschaft, dass oberhalb von 1 nur Einheiten liegen. Auch für die Elemente aus R, deren Norm gleich einer fixierten ganzen Zahl a ist, gibt es eine wichtige Gesetzmäßigkeit.

LEMMA 10.9. *Es sei R der Ganzheitsring einer endlichen Körpererweiterung $\mathbb{Q} \subseteq K$ und sei $a \in \mathbb{Z}$. Dann gibt es endlich viele Elemente $f_1, \ldots, f_m \in R$ derart, dass jedes $f \in R$ mit $|N(f)| = a$ zu einem der f_i assoziiert ist.*

Beweis. Der Restklassenring $R/(a)$ ist endlich nach Lemma 10.2 und Lemma 10.6. Wir behaupten, dass Elemente aus der gleichen Nebenklasse zu $R/(a)$, die beide die Norm a besitzen, zueinander assoziiert sind (für die f_j wählen wir zu jeder Nebenklasse von $R/(a)$ einen Repräsentanten mit Norm a aus, falls es überhaupt ein solches Element gibt). Seien dazu $f, g, h \in R$ mit

$$f = g + ah$$

und mit $N(f) = N(g) = a$. Dann ist in $Q(R)$

$$\frac{f}{g} = \frac{g+ah}{g} = 1 + a\frac{h}{g} = 1 + \frac{N(g)}{g}h$$

und dies gehört zu R, da $\frac{N(g)}{g}$ nach Korollar 10.8 zu R gehört. Dies gilt auch, wenn man die Rollen von f und g vertauscht. Also teilen sich f und g gegenseitig und sind daher assoziiert. □

Diskrete Bewertungsringe

DEFINITION 10.10. Ein *diskreter Bewertungsring* R ist ein Hauptidealbereich mit der Eigenschaft, dass es bis auf Assoziiertheit genau ein Primelement in R gibt.

Einen Erzeuger des maximalen Ideals in einem diskreten Bewertungsring nennt man auch eine *Ortsuniformisierende*. Wir wollen zeigen, dass zu einem Zahlbereich R die Lokalisierung an einem jeden maximalen Ideal ein diskreter Bewertungsring ist.

LEMMA 10.11. *Ein diskreter Bewertungsring ist ein lokaler, noetherscher Hauptidealbereich mit genau zwei Primidealen, nämlich* 0 *und dem maximalen Ideal* $\mathfrak{m}$.

Beweis. Ein diskreter Bewertungsring ist kein Körper. In einem Hauptidealbereich, der kein Körper ist, wird jedes maximale Ideal von einen Primelement erzeugt, und die Primerzeuger zu verschiedenen maximalen Idealen können nicht assoziiert sein. Also gibt es genau ein maximales Ideal. Nach Satz 9.18 ist ein Hauptidealbereich insbesondere ein Dedekindbereich, so dass es als weiteres Primideal nur noch das Nullideal gibt. □

Beispiel 10.12. Es sei K ein Körper, $K[X]$ der Polynomring und $R = K[X]_{(X)}$ die Lokalisierung am maximalen Ideal $\mathfrak{m} = (X)$. Dann ist R ein diskreter Bewertungsring. Die beiden einzigen Primideale von R sind $(0) \subset (X)$, und ein Hauptidealbereich liegt vor, da ja $K[X]$ ein Hauptidealbereich ist. Da es nur ein maximales Ideal gibt, kann es bis auf Assoziiertheit auch nur ein Primelement geben, nämlich X.

Beispiel 10.13. Es sei p eine Primzahl und sei $R = \mathbb{Z}_{(p)}$ die Lokalisierung am maximalen Ideal $\mathfrak{m} = (p)$. Dann ist R ein diskreter Bewertungsring. Die beiden einzigen Primideale von R sind $(0) \subset (p)$, und ein Hauptidealbereich liegt vor, da ja $\mathbb{Z}$ ein Hauptidealbereich ist. Da es nur ein maximales Ideal gibt, kann es bis auf Assoziiertheit auch nur ein Primelement geben, nämlich p.

Definition 10.14. Zu einem Element $f \in R$, $f \neq 0$, in einem diskreten Bewertungsring mit Primelement p heißt die Zahl $n \in \mathbb{N}$ mit der Eigenschaft $f = up^n$, wobei u eine Einheit bezeichnet, die *Ordnung* von f. Sie wird mit $\operatorname{ord}(f)$ bezeichnet.

Die Ordnung ist also nichts anderes als der Exponent zum (bis auf Assoziiertheit) einzigen Primelement in der Primfaktorzerlegung. Sie hat folgende Eigenschaften.

Lemma 10.15. *Es sei R ein diskreter Bewertungsring mit maximalem Ideal $\mathfrak{m} = (p)$. Dann hat die Ordnung*

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

folgende Eigenschaften.

(1) $\operatorname{ord}(fg) = \operatorname{ord}(f) + \operatorname{ord}(g)$.
(2) $\operatorname{ord}(f+g) \geq \min\{\operatorname{ord}(f), \operatorname{ord}(g)\}$.
(3) *Es ist $f \in \mathfrak{m}$ genau dann, wenn $\operatorname{ord}(f) \geq 1$ ist.*
(4) *Es ist $f \in R^\times$ genau dann, wenn $\operatorname{ord}(f) = 0$ ist.*

Beweis. Siehe Aufgabe 10.7. □

Wir wollen eine wichtige Charakterisierung für diskrete Bewertungsringe beweisen, die insbesondere beinhaltet, dass ein normaler lokaler Integritätsbereich mit genau zwei Primidealen bereits ein diskreter Bewertungsring ist. Dazu benötigen wir einige Vorbereitungen.

Lemma 10.16. *Sei S ein noetherscher lokaler kommutativer Ring. Es sei vorausgesetzt, dass das maximale Ideal $\mathfrak{m}$ das einzige Primideal von S ist. Dann gibt es einen Exponenten $n \in \mathbb{N}$ mit*

$$\mathfrak{m}^n = 0.$$

Beweis. Wir behaupten zunächst, dass jedes Element in R eine Einheit oder nilpotent ist. Sei hierzu $f \in R$ keine Einheit. Dann ist $f \in \mathfrak{m}$. Angenommen,

f ist nicht nilpotent. Dann gibt es nach Lemma 3.9 ein Primideal $\mathfrak{p}$ in R mit $f \notin \mathfrak{p}$. Damit ergibt sich der Widerspruch $\mathfrak{p} \neq \mathfrak{m}$.

Es ist also jedes Element im maximalen Ideal nilpotent. Insbesondere gibt es für ein endliches Erzeugendensystem $f_1, \ldots, f_k$ von $\mathfrak{m}$ eine natürliche Zahl m mit $f_i^m = 0$ für alle $i = 1, \ldots, k$. Sei $n = km$. Dann ist ein beliebiges Element aus $\mathfrak{m}^n$ von der Gestalt

$$\left(\sum_{i=1}^{k} a_{i1} f_i\right)\left(\sum_{i=1}^{k} a_{i2} f_i\right) \cdots \left(\sum_{i=1}^{k} a_{in} f_i\right).$$

Ausmultiplizieren ergibt eine Linearkombination mit Monomen $f_1^{r_1} \cdots f_k^{r_k}$ und $\sum_{i=1}^{k} r_i = n$, so dass ein f_i mit einem Exponenten $\geq n/k = m$ vorkommt. Daher ist das Produkt 0. □

Satz 10.17. *Es sei R ein noetherscher lokaler Integritätsbereich mit der Eigenschaft, dass es genau zwei Primideale $0 \subset \mathfrak{m}$ gibt. Dann sind folgende Aussagen äquivalent.*

(1) *R ist ein diskreter Bewertungsring.*
(2) *R ist ein Hauptidealbereich.*
(3) *R ist faktoriell.*
(4) *R ist normal.*
(5) *$\mathfrak{m}$ ist ein Hauptideal.*

Beweis. (1) ⇒ (2) folgt direkt aus der Definition 10.10.

(2) ⇒ (3) folgt aus Satz 2.19.

(3) ⇒ (4) folgt aus Satz 6.12.

(4) ⇒ (5). Sei $f \in \mathfrak{m}$, $f \neq 0$. Dann ist $R/(f)$ ein noetherscher lokaler Ring mit nur einem Primideal (nämlich $\tilde{\mathfrak{m}} = \mathfrak{m}R/(f)$). Daher gibt es nach Lemma 10.16 ein $n \in \mathbb{N}$ mit $\tilde{\mathfrak{m}}^n = 0$. Zurückübersetzt nach R heißt das, dass $\mathfrak{m}^n \subseteq (f)$ gilt. Wir wählen n minimal mit den Eigenschaften

$$\mathfrak{m}^n \subseteq (f) \text{ und } \mathfrak{m}^{n-1} \not\subseteq (f).$$

Wähle $g \in \mathfrak{m}^{n-1}$ mit $g \notin (f)$ und betrachte

$$h := \frac{f}{g} \in Q(R)$$

(es ist $g \neq 0$). Das Inverse, also $h^{-1} = \frac{g}{f}$, gehört nicht zu R, sonst wäre $g \in (f)$. Da R nach Voraussetzung normal ist, ist h^{-1} auch nicht ganz über R. Nach dem Modulkriterium Lemma 6.7 für die Ganzheit gilt insbesondere für das maximale Ideal $\mathfrak{m} \subset R$ die Beziehung

$$h^{-1}\mathfrak{m} \not\subseteq \mathfrak{m}$$

ist. Nach Wahl von g ist aber auch

$$h^{-1}\mathfrak{m} = \frac{g}{f}\mathfrak{m} \subseteq \frac{\mathfrak{m}^n}{f} \subseteq R.$$

Daher ist $h^{-1}\mathfrak{m}$ ein Ideal in R, das nicht im maximalen Ideal enthalten ist. Also ist $h^{-1}\mathfrak{m} = R$. Das heißt einerseits $h \in \mathfrak{m}$ und andererseits gilt für ein beliebiges $x \in \mathfrak{m}$ die Beziehung $h^{-1}x \in R$, also $x = h(h^{-1}x)$, also $x \in (h)$ und somit $(h) = \mathfrak{m}$.

(5) $\Rightarrow$ (1). Sei $\mathfrak{m} = (\pi)$. Dann ist π ein Primelement und zwar bis auf Assoziiertheit das einzige. Sei $f \in R$, $f \neq 0$ keine Einheit. Dann ist $f \in \mathfrak{m}$ und daher $f = \pi g_1$. Dann ist g_1 eine Einheit oder $g_1 \in \mathfrak{m}$. Im zweiten Fall ist wieder $g_1 = \pi g_2$ und $f = \pi^2 g_2$.

Wir behaupten, dass man $f = \pi^k u$ mit einem $k \in \mathbb{N}$ und einer Einheit u schreiben kann. Andernfalls könnte man $f = \pi^n g_n$ mit beliebig großem n schreiben. Nach Lemma 10.16 gibt es ein $m \in \mathbb{N}$ mit $(\pi^m) = \mathfrak{m}^m \subseteq (f)$. Bei $n \geq m+1$ ergibt sich $\pi^m = af = a\pi^{m+1}b$ und der Widerspruch $1 = ab\pi$.

Es lässt sich also jede Nichteinheit $\neq 0$ als Produkt einer Potenz des Primelements mit einer Einheit schreiben. Insbesondere ist R faktoriell. Für ein beliebiges Ideal $\mathfrak{a} = (f_1, \ldots, f_s)$ ist $f_i = \pi^{n_i} u_i$ mit Einheiten u_i. Dann sieht man leicht, dass $\mathfrak{a} = (\pi^n)$ ist mit $n = \min_i\{n_i\}$. □

Korollar 10.18. *Sei R ein Dedekindbereich und sei $\mathfrak{m}$ ein maximales Ideal in R. Dann ist die Lokalisierung*

$$R_{\mathfrak{m}}$$

ein diskreter Bewertungsring.

Beweis. Die Lokalisierung $R_{\mathfrak{m}}$ ist lokal nach Satz 4.15, so dass es lediglich die beiden Primideale 0 und $\mathfrak{m}R_{\mathfrak{m}}$ gibt. Ferner ist R noethersch. Da R normal ist, ist nach Lemma 6.15 auch die Lokalisierung $R_{\mathfrak{m}}$ normal. Wegen Satz 10.17 ist $R_{\mathfrak{m}}$ ein diskreter Bewertungsring. □

Bemerkung 10.19. Korollar 10.18 besagt in Verbindung mit Satz 10.17, dass wenn man bei einem Dedekindbereich und spezieller einem Zahlbereich R zur Lokalisierung $R_{\mathfrak{m}}$ an einem maximalen Ideal $\mathfrak{m}$ übergeht, dass dort die eindeutige Primfaktorzerlegung gilt.

Korollar 10.20. *Sei R ein Dedekindbereich. Dann ist R der Durchschnitt von diskreten Bewertungsringen.*

Beweis. Nach Satz 4.16 ist

$$R = \bigcap_{\mathfrak{m}} R_{\mathfrak{m}},$$

wobei $\mathfrak{m}$ durch alle maximalen Ideale von R läuft. Nach Korollar 10.18 sind die beteiligten Lokalisierungen $R_{\mathfrak{m}}$ allesamt diskrete Bewertungsringe. □

Abbildungsverzeichnis