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

Zahlentheorie

Vorlesung 22

In dieser und der nächsten Vorlesung beweisen wir zwei Versionen zur eindeutigen Primfaktorzerlegung in Zahlbereichen, die beide Abschwächungen zur eindeutigen Primfaktorzerlegung in $\mathbb{Z}$ sind. Die eine besagt, dass für einen Zahlbereich die eindeutige Primfaktorzerlegung von Elementen „lokal“ gilt (Satz 22.17 und Bemerkung 22.19). Die zweite Version besagt, dass man auf der Ebene der Ideale eine eindeutige Faktorzerlegung in Primideale erhält (Satz 23.14). Für die erste Version benötigen wir die Begriffe Nenneraufnahme, Lokalisierung und diskreter Bewertungsring.

Nenneraufnahme

Definition 22.1. Sei R ein kommutativer Ring. Eine Teilmenge $S \subseteq R$ heißt *multiplikatives System*, wenn die beiden Eigenschaften

(1) $1 \in S$
(2) Wenn $f, g \in S$, dann ist auch $fg \in S$

gelten.

Es handelt sich also einfach um ein Untermonoid des multiplikativen Monoids eines Ringes.

Beispiel 22.2. Sei R ein kommutativer Ring und $f \in R$ ein Element. Dann bilden die Potenzen f^n, $n \in \mathbb{N}$, ein multiplikatives System.

Beispiel 22.3. Sei R ein Integritätsbereich. Dann bilden alle von 0 verschiedenen Elemente in R ein multiplikatives System, das mit $R^* = R \setminus \{0\}$ bezeichnet wird.

Beispiel 22.4. Sei R ein kommutativer Ring und $\mathfrak{p}$ ein Primideal. Dann ist das Komplement $R \setminus \mathfrak{p}$ ein multiplikatives System. Dies folgt unmittelbar aus der Definition.

Definition 22.5. Sei R ein Integritätsbereich und sei $S \subseteq R$ ein multiplikatives System, $0 \notin S$. Dann nennt man den Unterring

$$R_S := \left\{ \frac{f}{g} | \, f \in R, \, g \in S \right\} \subseteq Q(R)$$

die *Nenneraufnahme* zu S.

Für die Nenneraufnahme an einem Element f schreibt man einfach R_f statt $R_{\{f^n | n \in \mathbb{N}\}}$. Man kann eine Nenneraufnahme auch dann definieren, wenn R kein Integritätsbereich ist, siehe Aufgabe 22.7.

DEFINITION 22.6. Sei R ein Integritätsbereich und sei $\mathfrak{p}$ ein Primideal. Dann nennt man die Nenneraufnahme an $S = R \setminus \mathfrak{p}$ die *Lokalisierung* von R an $\mathfrak{p}$. Man schreibt dafür $R_{\mathfrak{p}}$. Es ist also

$$R_{\mathfrak{p}} := \left\{ \frac{f}{g} | \, f \in R, \, g \notin \mathfrak{p} \right\} \subseteq Q(R).$$

Für eine Primzahl $p \in \mathbb{Z}$ besteht $\mathbb{Z}_{(p)}$ aus allen rationalen Zahlen, die man ohne p im Nenner schreiben kann.

DEFINITION 22.7. Ein kommutativer Ring R heißt *lokal*, wenn R genau ein maximales Ideal besitzt.

Der folgende Satz zeigt, dass diese Namensgebung Sinn ergibt.

SATZ 22.8. *Sei R ein Integritätsbereich und sei $\mathfrak{p}$ ein Primideal in R. Dann ist die Lokalisierung $R_{\mathfrak{p}}$ ein lokaler Ring mit maximalem Ideal*

$$\mathfrak{p}R_{\mathfrak{p}} := \left\{ \frac{f}{g} | \, f \in \mathfrak{p}, \, g \notin \mathfrak{p} \right\}.$$

Beweis. Die angegebene Menge ist in der Tat ein Ideal in der Lokalisierung

$$R_{\mathfrak{p}} = \left\{ \frac{f}{g} | \, f \in R, \, g \notin \mathfrak{p} \right\}.$$

Wir zeigen, dass das Komplement von $\mathfrak{p}R_{\mathfrak{p}}$ nur aus Einheiten besteht, so dass es sich um ein maximales Ideal handeln muss. Sei also $q = \frac{f}{g} \in R_{\mathfrak{p}}$, aber nicht in $\mathfrak{p}R_{\mathfrak{p}}$. Dann sind $f, g \notin \mathfrak{p}$ und somit gehört der inverse Bruch $\frac{g}{f}$ ebenfalls zur Lokalisierung. □

Das Ideal $\mathfrak{p}R_{\mathfrak{p}}$ ist dabei das Erweiterungsideal zu $\mathfrak{p}$ unter dem Ringhomomorphismus $R \to R_{\mathfrak{p}}$.

SATZ 22.9. *Sei R ein Integritätsbereich mit Quotientenkörper $Q(R)$. Dann gilt*

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

wobei der Durchschnitt über alle maximale Ideale läuft und in $Q(R)$ genommen wird.

Beweis. Die Inklusion $\subseteq$ ist klar. Sei also $q \in Q(R)$ und sei angenommen, q gehöre zum Durchschnitt rechts. Für jedes maximale Ideal $\mathfrak{m}$ ist also $q \in R_{\mathfrak{m}} \subset Q(R)$, d.h. es gibt $f_{\mathfrak{m}} \notin \mathfrak{m}$ und $a_{\mathfrak{m}} \in R$ mit $q = \frac{a_{\mathfrak{m}}}{f_{\mathfrak{m}}}$. Wir betrachten das Ideal

$$(f_{\mathfrak{m}} : \mathfrak{m} \text{ maximal}).$$

Dieses Ideal ist in keinem maximalen Ideal enthalten, also muss es nach dem Lemma von Zorn das Einheitsideal sein. Es gibt also endlich viele maximale Ideale $\mathfrak{m}_i$, $i = 1, \ldots, n$ und $r_i \in R$ mit

$$r_1 f_1 + \cdots + r_n f_n = 1,$$

wobei $f_i = f_{\mathfrak{m}_i}$ gesetzt wurde. Damit ist

$$q = \frac{a_1}{f_1} = \ldots = \frac{a_n}{f_n}.$$

Wir schreiben

$$q = q(r_1 f_1 + \cdots + r_n f_n) = q r_1 f_1 + \cdots + q r_n f_n = a_1 r_1 + \cdots + a_n r_n.$$

Also gehört q zu R. □

Satz 22.10. *Sei R ein normaler Integritätsbereich und sei $S \subseteq R$ ein multiplikatives System. Dann ist auch die Nenneraufnahme R_S normal.*

Beweis. Siehe Aufgabe 22.14. □

Diskrete Bewertungsringe

Definition 22.11. Ein *diskreter Bewertungsring* R ist ein Hauptidealbereich mit der Eigenschaft, dass es bis auf Assoziiertheit genau ein Primelement in R gibt.

Wir wollen zeigen, dass zu einem Zahlbereich R die Lokalisierung an einem jeden Primideal ein diskreter Bewertungsring ist.

Lemma 22.12. *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 19.1 ist ein Hauptidealbereich insbesondere ein Dedekindbereich, so dass es als weiteres Primideal nur noch das Nullideal gibt. □

Definition 22.13. 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 bezeichne, 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 22.14. *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) $f \in \mathfrak{m}$ *genau dann, wenn* $\operatorname{ord}(f) \geq 1$.
(4) $f \in R^\times$ *genau dann, wenn* $\operatorname{ord}(f) = 0$.

Beweis. Siehe Aufgabe 22.16. □

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 22.15. *Sei R ein kommutativer Ring und sei $f \in R$ nicht nilpotent. Dann gibt es ein Primideal $\mathfrak{p}$ in R mit $f \notin \mathfrak{p}$.*

Beweis. Wir betrachten die Menge der Ideale

$$M = \{\mathfrak{a} \text{ Ideal} \mid f^r \notin \mathfrak{a} \text{ für alle } r\}.$$

Diese Menge ist nicht leer, da sie das Nullideal enthält. Ferner ist sie induktiv geordnet (bezüglich der Inklusion). Ist nämlich $\mathfrak{a}_i$, $i \in I$, eine total geordnete Teilmenge von M, so ist deren Vereinigung ebenfalls ein Ideal, das keine Potenz von f enthält. Nach dem Lemma von Zorn gibt es daher maximale Elemente in M.

Wir behaupten, dass ein solches maximales Element $\mathfrak{p}$ ein Primideal ist. Sei dazu $g, h \in R$ und $gh \in \mathfrak{p}$, und sei $g, h \notin \mathfrak{p}$ angenommen. Dann hat man echte Inklusionen

$$\mathfrak{p} \subseteq \mathfrak{p} + (g), \mathfrak{p} + (h).$$

Wegen der Maximalität können die beiden Ideale rechts nicht zu M gehören, und das bedeutet, dass es Exponenten $r, s \in \mathbb{N}$ gibt mit

$$f^r \in \mathfrak{p} + (g) \text{ und } f^s \in \mathfrak{p} + (h).$$

Dann ergibt sich der Widerspruch

$$f^r f^s \in \mathfrak{p} + (gh) \subseteq \mathfrak{p}.$$

□

LEMMA 22.16. *Sei R ein noetherscher lokaler kommutativer Ring. Es sei vorausgesetzt, dass das maximale Ideal $\mathfrak{m}$ das einzige Primideal von R 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 22.15 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 22.17. *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 22.11.

(2) ⇒ (3) folgt aus Satz 3.7.

(3) ⇒ (4) folgt aus Satz 17.12.

(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 22.16 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 17.7 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 einer Einheit u schreiben kann. Andernfalls könnte man $f = \pi^n g_n$ mit beliebig großem n schreiben. Nach Lemma 22.16 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 22.18. *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 22.8, 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 Satz 22.10 auch die Lokalisierung $R_{\mathfrak{m}}$ normal. Wegen Satz 22.17 ist $R_{\mathfrak{m}}$ ein diskreter Bewertungsring. □

Bemerkung 22.19. Korollar 22.18 besagt in Verbindung mit Satz 22.17, 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 22.20. *Sei R ein Dedekindbereich. Dann ist R der Durchschnitt von diskreten Bewertungsringen.*

Beweis. Nach Satz 22.9 ist

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

wobei $\mathfrak{m}$ durch alle maximalen Ideale von R läuft. Nach Korollar 22.18 sind die beteiligten Lokalisierungen $R_{\mathfrak{m}}$ allesamt diskrete Bewertungsringe. □