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

Algebraische Zahlentheorie

Vorlesung 4

In diesem Kurs 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 10.17 und Bemerkung 10.9). Die zweite Version besagt, dass man auf der Ebene der Ideale eine eindeutige Faktorzerlegung in Primideale erhält (Satz 12.2). Für die erste Version benötigen wir die Begriffe Nenneraufnahme, Lokalisierung und diskreter Bewertungsring.

Multiplikative Systeme

Definition 4.1. Es 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. Wir erwähnen einige Beispiele von multiplikativen Systemen. Zunächst ist natürlich der Gesamtring, die Menge $\{1\}$, die Menge $\{0,1\}$ und die Einheitengruppe $R^\times$ ein multiplikatives System. Darüber hinaus erwähnen wir die folgenden Beispiele.

Beispiel 4.2. Es 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 4.3. 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 4.4. Die Nichtnullteiler bilden ein multiplikatives System in einem kommutativen Ring. Die 1 ist wie jede Einheit ein Nichtnullteiler, und wenn f und g Nichtnullteiler sind, so ist auch deren Produkt ein Nichtnullteiler, da aus $f(gh) = 0$ zunächst $gh = 0$ und daraus $h = 0$ folgt.

Beispiel 4.5. Es sei R ein faktorieller Bereich und sei M eine Menge von Primelementen. Dann ist die Menge aller Elemente aus R, in deren Primfaktorzerlegung ausschließlich Primelemente aus M vorkommen, ein multiplikatives System S. Es ist also

$$S = \left\{ up_1^{r_1} \cdots p_k^{r_k} \mid u \in R^\times, \, p_i \in M \right\}.$$

Beispiel 4.6. 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.

Nenneraufnahme

Die Idee für die Nenneraufnahme zu einem multiplikativen System $S \subseteq R$ ist es, die Elemente aus S zu Einheiten, zu Nennern, zu machen. Dabei soll natürlich wieder ein sinnvoller Ring entstehen. Von den rationalen Zahlen kennt man die Eigenschaft, dass $\frac{r}{s} = \frac{r'}{s'}$ genau dann gilt, wenn $rs' = r's$ gilt, wodurch dir Gleichheit von Brüchen auf die Gleicheit innerhalb der ganzen Zahlen zurückgeführt wird. Diesen Ansatz muss man wegen möglicher Nullteiler etwas modifizieren.

Definition 4.7. Es sei R ein kommutativer Ring und $S \subseteq R$ ein multiplikatives System. Auf der Produktmenge $R \times S$ nennt man die durch

$$(r, s) \sim (r', s'),$$

falls es ein $t \in S$ mit $rs't = r'st$ gibt, die durch das multiplikative System gegebene *Überkreuzrelation*.

Wenn S nur aus Nichtnullteilern besteht, so braucht man den zusätzlichen Faktor t nicht.

Lemma 4.8. *Es sei R ein kommutativer Ring und $S \subseteq R$ ein multiplikatives System. Dann ist die Überkreuzrelation auf der Produktmenge $R \times S$ eine Äquivalenzrelation. Für die Äquivalenzklassen $\frac{r}{s} := [(r, s)]$ ist durch*

$$\frac{r}{s} + \frac{r'}{s'} := \frac{rs' + r's}{ss'}$$

eine wohldefinierte Addition und durch

$$\frac{r}{s} \cdot \frac{r'}{s'} := \frac{rr'}{ss'}$$

eine wohldefinierte Multiplikation gegeben, derart, dass die Quotientenmenge ein kommutativer Ring wird.

Beweis. Siehe Aufgabe 4.9. □

Definition 4.9. Es sei R ein kommutativer Ring und $S \subseteq R$ ein multiplikatives System. Dann versteht man unter der *Nenneraufnahme* zu S die Quotientenmenge zur Überkreuzrelation auf $R \times S$ mit den in Lemma 4.8 beschriebenen Verknüpfungen. Die Nenneraufnahme wird mit R_S bezeichnet.

Es gibt einen natürlichen Ringhomomorphismus

$$R \longrightarrow R_S,\ r \longmapsto \frac{r}{1}.$$

Die Elemente $s \in S$ aus dem multiplikativen System werden in R_S zu Einheiten, und zwar ist $1/s$ das Inverse zu s. Wenn S nur aus Nuchtnullteilern besteht, so ist diese kanonische Abbildung injektiv. Wenn hingegen die 0 zu S gehört, so wird die Nenneraufnahme zum Nullring. Für die Nenneraufnahme an dem von einem Element f erzeugten multiplikativen System schreibt man einfach R_f statt $R_{\{f^n|n\in\mathbb{N}\}}$. Die Nenneraufnahme an $R^* = R \setminus \{0\}$ in einem Integritätsbereich spielt eine besondere Rolle. Dort werden sämtliche Elemente $\neq 0$ zu Einheiten und es entsteht ein Körper.

Definition 4.10. Zu einem Integritätsbereich R ist der *Quotientenkörper* $Q(R)$ als die Menge der formalen Brüche

$$Q(R) = \left\{ \frac{r}{s} \mid r,s \in R,\, s \neq 0 \right\}$$

mit natürlichen Identifizierungen und Operationen definiert.

Lemma 4.11. *Es seien R und A kommutative Ringe und sei $S \subseteq R$ ein multiplikatives System. Es sei*

$$\varphi\colon\ R \longrightarrow A$$

ein Ringhomomorphismus derart, dass $\varphi(s)$ eine Einheit in A für alle $s \in S$ ist. Dann gibt es einen eindeutig bestimmten Ringhomomorphismus

$$\tilde{\varphi}\colon\ R_S \longrightarrow A,$$

der φ fortsetzt.

Beweis. Damit die Ringhomomorphismen kommutieren muss

$$\tilde{\varphi}(1/s) = (\varphi(s))^{-1}$$

für $s \in S$ und damit $\tilde{\varphi}(a/s) = \varphi(a)(\varphi(s))^{-1}$ sein. Es kann also maximal einen solchen Ringhomomorphismus geben, der durch die letzte Gleichung definiert sein muss.

Es ist zu zeigen, dass dadurch ein wohldefinierter Ringhomomorphismus gegeben ist. Zum Nachweis der Wohldefiniertheit sei $\frac{a}{s} = \frac{b}{t}$ mit $s,t \in S$. Dies bedeutet, dass es ein $r \in S$ mit $rta = rsb$ gibt. Dann ist auch

$$\varphi(r)\varphi(t)\varphi(a) = \varphi(r)\varphi(s)\varphi(b)$$

und durch Multiplizieren mit der Einheit $\varphi(r)^{-1}\varphi(t)^{-1}\varphi(s)^{-1}$ folgt

$$\varphi(a)(\varphi(s))^{-1} = \varphi(b)(\varphi(t))^{-1}.$$

Wir zeigen exemplarisch für die Addition, dass ein Ringhomomorphismus vorliegt. Es ist

$$\begin{aligned}
\tilde{\varphi}\left(\frac{a}{s}+\frac{b}{t}\right) &= \tilde{\varphi}\left(\frac{at+bs}{st}\right) \\
&= \varphi(at+bs)\varphi(st)^{-1} \\
&= (\varphi(a)\varphi(t)+\varphi(s)\varphi(b))\varphi(s)^{-1}\varphi(t)^{-1} \\
&= \varphi(a)\varphi(s)^{-1}+\varphi(b)\varphi(t)^{-1}
\end{aligned}$$

$$= \tilde{\varphi}\Big(\frac{a}{s}\Big) + \tilde{\varphi}\Big(\frac{b}{t}\Big).$$

□

Lokale Ringe und Lokalisierung

DEFINITION 4.12. Ein kommutativer Ring R heißt *lokal*, wenn R genau ein maximales Ideal besitzt.

Jeder Körper ist ein lokaler Ring mit dem Nullideal als eindeutigem maximalen Ideal. Ein kommutativer Ring ist genau dann lokal, wenn seine Nichteinheiten ein Ideal bilden, das dann das einzige maximale Ideal ist.

DEFINITION 4.13. Zu einem kommutativen lokalen Ring R nennt man den Restklassenkörper $R/\mathfrak{m}$ zum einzigen maximalen Ideal $\mathfrak{m}$ von R den *Restekörper* von R.

DEFINITION 4.14. Sei R ein kommutativer Ring 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

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

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

Der folgende Satz zeigt, dass diese Namensgebung Sinn ergibt.

SATZ 4.15. *Sei R ein kommutativer Ring und sei $\mathfrak{p}$ ein Primideal in R. Dann ist die Lokalisierung $R_{\mathfrak{p}}$ ein lokaler Ring mit maximalem Ideal*

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

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

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

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 4.16. *Es 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. □

LEMMA 4.17. *Es sei R ein kommutativer Ring und sei $\mathfrak{p}$ ein Primideal. Dann ist der Quotientenkörper des Restklassenringes $R/\mathfrak{p}$ in natürlicher Weise isomorph zum Restekörper der Lokalisierung $R_{\mathfrak{p}}$. Es ist also*

$$Q(R/\mathfrak{p}) = R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}}.$$

Beweis. Wir betrachten das kommutative Diagramm

$$\begin{array}{ccccc} R & \longrightarrow & R/\mathfrak{p} & \longrightarrow & Q(R/\mathfrak{p}) \\ \downarrow & & \varphi \downarrow & & \downarrow \psi \\ R_{\mathfrak{p}} & \longrightarrow & R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}} & \longrightarrow & R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}} \end{array}$$

von Ringhomomorphismen, wobei φ und ψ zu konstruieren sind. Unter dem Ringhomomorphismus

$$R \longrightarrow R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}}$$

wird das Primideal $\mathfrak{p}$ auf 0 abgebildet, der Ringhomomorphismus φ ergibt sich als induzierter Homomorphismus. Unter φ werden Elemente $[r] \in R/\mathfrak{p}$, $[r] \neq 0$, die also durch $r \notin \mathfrak{p}$ repräsentiert werden, auf Einheiten abgebildet. Somit gibt es nach Lemma 4.11 eine Fortsetzung auf den Quotientenkörper

$$\psi \colon Q(R/\mathfrak{p}) \longrightarrow R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}}.$$

Diese ist als Ringhomomorphismus zwischen Körpern injektiv. Ein Element des Restekörpers, das in der Lokalisierung $R_{\mathfrak{p}}$ durch r/s mit $s \notin \mathfrak{p}$ repräsentiert wird, wird unter ψ durch das Element $[r]/[s]$ getroffen (beachte $[s] \neq 0$). □

Der Restekörper zu einem Primideal $\mathfrak{p}$ wird mit $\kappa(\mathfrak{p})$ bezeichnet. Wenn $\mathfrak{m}$ ein maximales Ideal ist, so ist insbesondere der Restklassenkörper $R/\mathfrak{m}$ gleich dem Restklassenkörper der Lokalisierung $R_{\mathfrak{m}}$.

Abbildungsverzeichnis