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

Algebraische Zahlentheorie

Vorlesung 12

Der Satz von Dedekind

KOROLLAR 12.1. *Es sei R ein Dedekindbereich 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 $\mathfrak{b} \neq 0$ 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 11.11 (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 11.13 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 12.2. *Es sei R ein Dedekindbereich 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 11.13, 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 11.13. □

KOROLLAR 12.3. *Es sei R ein Dedekindbereich 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 12.2. □

Chinesischer Restsatz für Dedekindbereiche

Wir kommen zum chinesischen Restsatz für Dedekindbereiche, der den klassischen chinesischen Restsatz für ganze Zahlen wesentlich verallgemeinert. Dazu erinnern wir kurz an Produktringe und idempotente Elemente.

DEFINITION 12.4. Es seien $R_1, \ldots, R_n$ kommutative Ringe. Dann heißt das Produkt

$$R_1 \times \cdots \times R_n \,,$$

versehen mit komponentenweiser Addition und Multiplikation, der *Produktring* der R_i, $i = 1, \ldots, n$.

DEFINITION 12.5. Ein Element e eines kommutativen Ringes heißt *idempotent*, wenn $e^2 = e$ gilt.

Die Elemente 0 und 1 sind trivialerweise idempotent, man nennt sie die trivialen idempotenten Elemente. In einem Produktring sind auch diejenigen Elemente, die in allen Komponenten nur den Wert 0 oder 1 besitzen, idempotent, also beispielsweise $(1, 0)$.

LEMMA 12.6. *Es sei R ein kommutativer Ring und seien $\mathfrak{a}, \mathfrak{b} \subseteq R$ Ideale mit $\mathfrak{a} + \mathfrak{b} = R$. Dann ist*

$$\mathfrak{a} \cap \mathfrak{b} = \mathfrak{a}\mathfrak{b}.$$

Beweis. Die Inklusion $\supseteq$ gilt immer. Sei also $x \in \mathfrak{a} \cap \mathfrak{b}$ und seien $a \in \mathfrak{a}$ und $b \in \mathfrak{b}$ Elemente mit $a+b = 1$. Dann ist

$$x = x \cdot 1 = x(a+b) = xa + xb \in \mathfrak{ba} + \mathfrak{ab} = \mathfrak{ab}.$$

□

LEMMA 12.7. *Es sei R ein kommutativer Ring und seien $\mathfrak{a}_j$, $j = 1, \ldots, n$, Ideale mit $\mathfrak{a}_i + \mathfrak{a}_j = R$ für alle $i \neq j$. Dann ist*

$$R/\mathfrak{a}_1 \cdots \mathfrak{a}_n \cong R/\mathfrak{a}_1 \times \cdots \times R/\mathfrak{a}_n.$$

Beweis. Der allgemeine Fall folgt aus dem Fall für $n = 2$, so dass wir uns darauf beschränken. Die natürliche Abbildung

$$R \longrightarrow R/\mathfrak{a} \times R/\mathfrak{b}$$

hat den Durchschnitt $\mathfrak{a} \cap \mathfrak{b}$ als Kern. Dieser stimmt nach Lemma 12.6 mit dem Produkt $\mathfrak{a} \cdot \mathfrak{b}$ überein und wir erhalten einen injektiven Ringhomomorphismus

$$R/\mathfrak{a} \cdot \mathfrak{b} \longrightarrow R/\mathfrak{a} \times R/\mathfrak{b}.$$

Es ist also noch die Surjektivität nachzuweisen. Sei dazu (r, s) rechts gegeben. Es seien $a \in \mathfrak{a}$ und $b \in \mathfrak{b}$ mit $a+b = 1$. Dann ist $r - ar + s - sb$ ein Urbild. Dieses Element wird ja in der ersten Komponente auf

$$r - ar + s - sb = r + s - s(1-a) = r + s - s = r$$

abgebildet und entsprechend in der zweiten Kompoente auf s. □

SATZ 12.8. *Es sei $\mathfrak{a}$ ein Ideal $\neq 0$ in einem Dedekindbereich mit der eindeutigen Primidealzerlegung*

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

Dann gibt es einen natürlichen Ringisomorphismus

$$R/\mathfrak{a} \cong R/\mathfrak{p}_1^{r_1} \times \cdots \times R/\mathfrak{p}_k^{r_k}.$$

Beweis. Da Dedekindbereiche eindimensional sind und die Primideale in der Zerlegung verschieden sind, gilt $\mathfrak{p}_i + \mathfrak{p}_j = R$ für $i \neq j$. Dies überträgt sich direkt auf die Potenzen. Somit folgt die Aussage aus Lemma 12.7. □

BEISPIEL 12.9. Wir betrachten

$$\mathbb{Z} \subseteq R = \mathbb{Z}[X]/(X^2+3) \subseteq \mathbb{Z}[Y]/(Y^2+Y+1) = S$$

mit $X \mapsto 2Y+1$, die beide quadratische Erweiterungen von $\mathbb{Z}$ sind und wobei S der Ring der Eisenstein-Zahlen ist und die Normalisierung von R ist. Der Faserring zu R über 2 ist

$$\mathbb{Z}/(2)[X]/(X^2+3) = \mathbb{Z}/(2)[X]/(X^2+1) = \mathbb{Z}/(2)[X]/(X+1)^2,$$

er ist also nicht reduziert. Der Fasering zu S über 2 ist

$$\mathbb{Z}/(2)[Y]/(Y^2+Y+1)$$

und dies ist ein Körper mit vier Elementen. In S liegt die Zerlegung in Primideale $(2) = (2)$ vor. In R kann man hingegen das Ideal (2) nicht als ein

Produkt von Primidealen schreiben. Das einzige Primideal oberhalb von (2) in R ist $(2, X+1)$. Das Quadrat davon ist aber bereits

$$\begin{aligned}(2,X+1)\cdot(2,X+1) &= (4,2X+2,X^2+2X+1)\\ &= (4,2X+2,X^2-1)\\ &= (4,2X+2)\\ &\subset (2),\end{aligned}$$

wobei die letzte Inklusion echt ist. Der Restklassenring $R/(4,2X+2)$ besitzt 12 Elemente.

KOROLLAR 12.10. *Es sei R ein Zahlbereich und p eine Primzahl. In R gelte die Idealzerlegung*

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

Dann gilt für den Faserring über p die Produktzerlegung

$$R/pR = R/\mathfrak{p}_1^{r_1}\times\cdots\times R/\mathfrak{p}_k^{r_k}.$$

Beweis. Dies folgt direkt aus Satz 12.8. □

Wir formulieren explizit die beiden folgenden Spezialfälle des chinesischen Restsatzes.

KOROLLAR 12.11. *Es sei R ein Hauptidealbereich und $f\in R$, $f\neq 0$, ein Element mit kanonischer Primfaktorzerlegung*

$$f = p_1^{r_1}\cdots p_k^{r_k}.$$

Dann gilt für den Restklassenring $R/(f)$ die kanonische Isomorphie

$$R/(f) \cong R/(p_1^{r_1})\times\cdots\times R/(p_k^{r_k}).$$

KOROLLAR 12.12. *Es sei n eine positive natürliche Zahl mit kanonischer Primfaktorzerlegung*

$$n = p_1^{r_1}\cdot p_2^{r_2}\cdots p_k^{r_k}$$

(die p_i seien also verschieden und $r_i\geq 1$). Dann induzieren die kanonischen Ringhomomorphismen $\mathbb{Z}/(n)\to\mathbb{Z}/(p_i^{r_i})$ einen Ringisomorphismus

$$\mathbb{Z}/(n) \cong \mathbb{Z}/(p_1^{r_1})\times\mathbb{Z}/(p_2^{r_2})\times\cdots\times\mathbb{Z}/(p_k^{r_k}).$$

Zu gegebenen ganzen Zahlen $(a_1,a_2,\ldots,a_k)$ gibt es also genau eine natürliche Zahl $a<n$, die die simultanen Kongruenzen

$$a=a_1 \mod p_1^{r_1},\ a=a_2 \mod p_2^{r_2},\ \ldots,\ a=a_k \mod p_k^{r_k}$$

löst.

Die Multipliktivität der Norm

SATZ 12.13. *Es sei $\mathfrak{a}$ ein Ideal $\neq 0$ in einem Zahlbereich R mit der eindeutigen Primidealzerlegung*

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

Dann ist

$$N(\mathfrak{a}) = N(\mathfrak{p}_1)^{r_1} \cdots N(\mathfrak{p}_k)^{r_k}.$$

Beweis. Nach dem chinesischen Restsatz für Zahlbereiche ist

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

und somit ist

$$N(\mathfrak{a}) = N(\mathfrak{p}_1^{r_1}) \cdots N(\mathfrak{p}_k^{r_k}).$$

Es ist also nur noch die Aussage für eine Primidealpotenz $\mathfrak{p}^r$ zu zeigen. Dies geschieht durch Induktion über r, wobei der Induktionsanfang klar ist. Es liegt wegen $\mathfrak{p}^{r+1} \subseteq \mathfrak{p}^r$ eine kurze exakte Sequenz

$$0 \longrightarrow \mathfrak{p}^r/\mathfrak{p}^{r+1} \longrightarrow R/\mathfrak{p}^{r+1} \longrightarrow R/\mathfrak{p}^r \longrightarrow 0$$

vor. Dabei ist

$$\mathfrak{p}^r/\mathfrak{p}^{r+1} = \mathfrak{p}^r R_{\mathfrak{p}}/\mathfrak{p}^{r+1}R_{\mathfrak{p}} = R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}} = R/\mathfrak{p}.$$

Deshalb ist

$$\begin{aligned} N(\mathfrak{p}^{r+1}) &= \#\left(R/\mathfrak{p}^{r+1}\right) \\ &= \#\left(\mathfrak{p}^r/\mathfrak{p}^{r+1}\right) \cdot \#\left(R/\mathfrak{p}^r\right) \\ &= \#\left(R/\mathfrak{p}\right) \cdot \#\left(R/\mathfrak{p}^r\right) \\ &= N(\mathfrak{p}) \cdot N(\mathfrak{p})^r \\ &= N(\mathfrak{p})^{r+1}. \end{aligned}$$

□

KOROLLAR 12.14. *Es sei R ein Zahlbereich und seien $\mathfrak{a}, \mathfrak{b} \neq 0$ Ideale in R. Dann ist*

$$N(\mathfrak{a} \cdot \mathfrak{b}) = N(\mathfrak{a}) \cdot N(\mathfrak{b}).$$

Beweis. Dies folgt unmittelbar aus Satz 12.13. □

BEMERKUNG 12.15. Zu einem Zahlbereich R und einem Element $f \in R$, $f \neq 0$, kann man folgendermaßen den zugehörigen Hauptdivisor bzw. die Primidealzerlegung $(f) = \mathfrak{p}_1^{r_1} \cdots \mathfrak{p}_k^{r_k}$ algorithmisch berechnen. Dabei arbeitet man im Restklassenring $R/(f)$ und man setzt voraus, dass für R selbst eine Restklassendarstellung über $\mathbb{Z}$ vorliegt. Für den Restklassenring $R/(f)$ hat man dann ebenfalls eine Restklassendarstellung und man weiß, dass dieser endlich ist, also grundsätzlich algorithmisch beherrschbar ist. Das erste Problem ist, die Primideale in R zu bestimmen, in denen f enthalten ist, doch diese entsprechen den maximalen Idealen $\mathfrak{m}_1, \ldots, \mathfrak{m}_k$ von $R/(f)$ (die

zugehörigen Primideale in R seien mit $\mathfrak{p}_i$ bezeichnet). Dabei liegt dann ein Produktring

$$R/(f) \;=\; R_1 \times \cdots \times R_k$$

vor, wobei die R_j lokal mit Restklassenkörper $R/\mathfrak{m}_j \;=\; R/\mathfrak{p}_j$ sind. Wegen Satz 12.8 weiß man

$$R/\mathfrak{p}_j^{r_j} \;=\; R_j.$$

Man kann nun in R_j die Exponenten r_j jeweils als die minimalen Exponenten mit $\mathfrak{m}_j^r \;=\; 0$ bestimmen. Bei der Bestimmung der Exponenten hilft auch die Norm. Nach Satz 12.13 in Verbindung mit Lemma 10.6 ist

$$|N(f)| \;=\; \#\left(R/(f)\right) \;=\; N(\mathfrak{p}_1)^{r_1} \cdots N(\mathfrak{p}_k)^{r_k}$$

und aus

$$\#\left(R_j\right) \;=\; N(\mathfrak{p}_j)^{r_j}$$

kann man wieder die Exponenten r_j bestimmen.

Abbildungsverzeichnis