B4: Algebra II
Sommersemester 2021
Frau Prof. Dr. Salma Kuhlmann

11.Vorlesung

20. Mai 2021

In diesem Skript werden wir gebrochene Ideale einführen, und ihre Eigenschaften studieren. Unser Hauptziel für diese Vorlesung ist Satz 11.6 für Dedekindringe zu beweisen. Der wird uns später ermöglichen, die Gruppenstruktur der Klassengruppe zu definieren.

Sei R stets ein kommutativer integer Ring mit Eins.

Definition 11.1 (i) Sei $K =$ Quot(R). Ein R-Untermodul $B \subseteq K$ heißt gebrochenes Ideal, wenn es $d \in R$ mit $d \neq 0$ gibt, so daß $B \subseteq \frac{1}{d}R$.

(ii) Ideale in R sind auch gebrochene Ideale ($d = 1$), wir nennen sie ganze Ideale.

(iii) Sei $x = \frac{a}{b} \in K$, $a, b \in R, b \neq 0$. Dann ist $B := Rx$ ein gebrochenes Hauptideal.

Bemerkung (i) B ist ein gebrochenes Ideal $\Leftrightarrow \exists d \neq 0$ in R und $A \lhd R$ so daß $B = (\frac{1}{d})A$.

(ii) Die Idealoperationen $+, ., \cap$ sind auf gebrochenen Idealen wohldefiniert:

$$B \subseteq (\tfrac{1}{d})R, B' \subseteq (\tfrac{1}{d'})R \Rightarrow \begin{cases} B + B' \subseteq (\frac{1}{dd'})R \\ BB' \subseteq (\frac{1}{dd'})R \\ B \cap B' \subseteq (\frac{1}{d})R\,. \end{cases}$$

Genauer: wenn $I, J \lhd R$ sind so dass $B = (\frac{1}{d})I$ und $B' = (\frac{1}{d'})J$, dann ist $BB' = (\frac{1}{dd'})IJ$.

Definition 11.2
Das gebrochene Ideal B ist invertierbar, wenn es ein gebrochenes Ideal B' gibt mit

$$BB' = R \qquad (*)$$

Bemerkung 11.1 (i) B invertierbar$\Rightarrow \exists! B'$, das $(*)$ erfüllt, d.h. $BB' = BB'' = R \Rightarrow B' = B''$. Wir bezeichnen $B' := B^{-1}$.

(ii) Ein gebrochenes Hauptideal $B = xR$ mit $x \in K$ und $x \neq 0$ ist invertierbar mit $B^{-1} = x^{-1}R$.

Notation
Seien B, B' gebrochene Ideale. Setze $(B : B') := \{x \in K \mid xB' \subseteq B\}$.

Bemerkung
$(B : B')$ ist ein R-Modul. Wenn $B' \neq \{0\}$, $B \subseteq \frac{1}{d}R$ und $a \in B'(d \neq 0, a \neq 0)$, dann ist $(B : B') \subseteq \frac{1}{da}R$.

Lemma 11.1
Sei A ein invertierbares gebrochenes Ideal, dann ist $A^{-1} = (R : A)$.
(Also: A invertierbar$\Leftrightarrow A.(R : A) = R$)

Beweis. Sei $AA' = R$. Dann ist $A' \subseteq (R : A)$. Andererseits ist $A.(R : A) \subseteq R$. Es folgt $(R : A) = A'A(R : A) \subseteq A'R = A'$ □

Lemma 11.2
Wenn jedes ganzes Ideal$\neq 0$ invertierbar ist, dann ist jedes $\neq 0$ gebrochenes Ideal invertierbar.

Beweis. Sei $B = \frac{1}{d}A$ ein gebrochenes Ideal (mit $A \lhd R, d \in R, d \neq 0$), dann ist $B^{-1} = dA^{-1}$. □

Lemma 11.3
Ein invertierbares gebrochenes Ideal ist ein endlich erzeugter R-Modul.

Beweis. $AA^{-1} = R \Rightarrow \exists\{x_i \,;\, i = 1, \cdots, n\} \subseteq A$ und $\{x_i'\} \subseteq A^{-1}$, so daß $\sum x_i x_i' = 1$. Es folgt: $x \in A \Rightarrow x = 1x = \sum \underbrace{xx_i'}_{\in R} x_i$. □

Lemma 11.4
Sei $\{A_i\}$ eine endliche Menge von $\neq 0$ ganzen Idealen, so daß $B := \prod_i A_i$ invertierbar ist . Dann ist A_i invertierbar für jedes i. Insbesondere gilt: Ist das Produkt B ein Hauptideal, so ist jedes A_i invertierbar.

Beweis. $B^{-1}(\prod_i A_i) = R \Rightarrow A_i \underbrace{(B^{-1} \prod_{j \neq i} A_j)}_{:= A_i^{-1}} = R$ □

Bemerkung 11.2
Sei $\mathfrak{p} \lhd R$ ein Primideal und $I, J \lhd R$. Es ist: $\mathfrak{p} \supseteq IJ \Rightarrow \mathfrak{p} \supseteq I$ oder $\mathfrak{p} \supseteq J$.

Lemma 11.5
Für Produkte von invertierbaren (ganzen) Primidealen ist die Faktorisierung als Produkt von Primidealen eindeutig.

Beweis. Sei $A = \prod_i \mathfrak{p}_i$, $\mathfrak{p}_i$ invertierbare Primideale. Sei $A = \prod_j \mathfrak{q}_j$, wobei $\mathfrak{q}_j$ Primideale sind. Sei $\mathfrak{p}_1$ ein minimales (für Inklusion) Mitglied von $\{\mathfrak{p}_i\}$. Aus $\prod_j \mathfrak{q}_j \subseteq \mathfrak{p}_1$ folgt o.E. $\mathfrak{q}_1 \subseteq \mathfrak{p}_1$ (Bemerkung 11.2). Analog folgt aus $\prod_i \mathfrak{p}_i \subseteq \mathfrak{q}_1$, daß $\mathfrak{p}_r \subseteq \mathfrak{q}_1$ für ein geeignetes r, also ist $\mathfrak{p}_r \subseteq \mathfrak{q}_1 \subseteq \mathfrak{p}_1$. Aus der Minimalität folgt nun $\mathfrak{p}_r = \mathfrak{p}_1 = \mathfrak{q}_1$, also $\mathfrak{p}_1^{-1}(\prod_i \mathfrak{p}_i) = \mathfrak{q}_1^{-1}(\prod_j \mathfrak{q}_j)$ und damit bekommen wir :
$\prod_{i \neq 1} \mathfrak{p}_i = \prod_{j \neq 1} \mathfrak{q}_j$. Per Induktion fortsetzen. □

Satz 11.6
Sei R ein Dedekindring und $\mathfrak{p}$ ein echtes Primideal ($\mathfrak{p} \neq \{0\}, \mathfrak{p} \neq R$). Dann ist $\mathfrak{p}$ invertierbar und maximal.

Beweis.

Behauptung 1: Sei $\mathfrak{p}$ ein echtes invertierbares Primideal. Dann ist $\mathfrak{p}$ maximal.

Beweis. Sei $a \in R$, $a \notin \mathfrak{p}$ und betrachte die Ideale $\mathfrak{p} + Ra$ und $\mathfrak{p} + Ra^2$. Da R ein Dedekindring ist, haben wir eine Faktorisierung

$$\mathfrak{p} + Ra = \prod_{i=1}^{n} \mathfrak{p}_i \text{ und } \mathfrak{p} + Ra^2 = \prod_{j=1}^{m} \mathfrak{q}_j$$

mit $\mathfrak{p}_i, \mathfrak{q}_j$ Primideale. Setze $\overline{R} := R/\mathfrak{p}$ und $\bar{a} := a \bmod \mathfrak{p}$.

Wir haben:

$(*)$ $\overline{R}.\bar{a} = \prod(\mathfrak{p}_i/\mathfrak{p})$

$(**)$ $\overline{R}.\bar{a}^2 = \prod(\mathfrak{q}_j/\mathfrak{p})$

und $\mathfrak{p}_i/\mathfrak{p}, \mathfrak{q}_j/\mathfrak{p}$ sind Primideale. Nun sind $\overline{R}.\bar{a}$ und $\overline{R}.\bar{a}^2$ Hauptideale, also sind sie invertierbar (Bemerkung 11.1) und es folgt (Lemma 11.4): $\mathfrak{p}_i/\mathfrak{p}$ und $\mathfrak{q}_j/\mathfrak{p}$ sind alle invertierbar. Aber

$$(***) \qquad \overline{R}\bar{a}^2 = (\overline{R}\bar{a})^2 = \prod_{i=1}^{n}(\mathfrak{p}_i/\mathfrak{p})^2$$

Wir folgern aus Lemma 11.5 und einem Vergleich von $(*)$, $(**)$ und $(***)$: Für jedes $j = 1, \cdots, m$ ist das Ideal $\mathfrak{q}_j/\mathfrak{p}$ ist in der Menge $\{\mathfrak{p}_i/\mathfrak{p}\}$ und wird zweimal wiederholt, d.h. $m = 2n$ und wir können umnummerieren, so daß o.E:
$\mathfrak{q}_{2i}/\mathfrak{p} = \mathfrak{q}_{2i-1}/\mathfrak{p} = \mathfrak{p}_i/\mathfrak{p}$. Es folgt: $\mathfrak{q}_{2i} = \mathfrak{q}_{2i-1} = \mathfrak{p}_i$. Wir bekommen:

$$(0) \qquad \mathfrak{p} + Ra^2 = \prod_{j=1}^{m}\mathfrak{q}_j = \prod_{i=1}^{n}\mathfrak{p}_i^2 = (\mathfrak{p} + Ra)^2$$

Daraus folgt

$$(\dagger) \qquad \mathfrak{p} \underset{(1)}{\subseteq} (\mathfrak{p} + Ra)^2 \underset{(2)}{\subseteq} \mathfrak{p}^2 + Ra$$

• Begründung für (1): $\mathfrak{p} \subseteq \mathfrak{p} + Ra^2$ gilt immer für Idealsummen, nun folgt (1) aus (0).
• Begründung für (2): I.A. gilt Distributivitätsgesetz für Ideale I, J_1, J_2: $I(J_1 + J_2) = IJ_1 + IJ_2$. Insbesondere gilt hier:

$$\begin{aligned}(\mathfrak{p} + Ra)(\mathfrak{p} + Ra) &= (\mathfrak{p} + Ra)\mathfrak{p} + (\mathfrak{p} + Ra)Ra \\ &= \mathfrak{p}^2 + (\mathfrak{p}Ra + \mathfrak{p}Ra) + RaRa\end{aligned}$$

Nun ist $RaRa = a^2R$ und $\mathfrak{p}Ra + \mathfrak{p}Ra = \mathfrak{p}Ra$ (da $I + I = I$ immer gilt).
Also $(\mathfrak{p} + Ra)^2 = \mathfrak{p}^2 + \mathfrak{p}Ra + Ra^2$. Da offensichtlich $\mathfrak{p}Ra \subseteq Ra$ und $Ra^2 \subseteq Ra$, bekommen wir: $(\mathfrak{p} + Ra)^2 \subseteq \mathfrak{p}^2 + Ra + Ra = \mathfrak{p}^2 + Ra$.

Aus $(\dagger)$ folgt: $\forall x \in \mathfrak{p} \exists y \in \mathfrak{p}^2, z \in R$ mit $x = y + za$, also $za = \underbrace{x - y}_{\in \mathfrak{p}}$, aber $a \notin \mathfrak{p}$, also $z \in \mathfrak{p}$. D.h.: $\mathfrak{p} \subseteq \mathfrak{p}^2 + \mathfrak{p}a$. Die andere Inklusion $\mathfrak{p} \supseteq \mathfrak{p}^2 + \mathfrak{p}a$ ist offensichtlich, also $\mathfrak{p} = \mathfrak{p}^2 + \mathfrak{p}a = \mathfrak{p}(\mathfrak{p} + Ra)$.
Da $\mathfrak{p}$ per Annahme invertierbar ist, folgt: $\mathfrak{p}\mathfrak{p}^{-1} = \mathfrak{p}^{-1}\mathfrak{p}(\mathfrak{p} + Ra)$, d.h. $R = \mathfrak{p} + Ra$.
Da $a \in R \backslash \mathfrak{p}$ beliebig ist, folgt nun: $\mathfrak{p}$ ist maximal.

□

Behauptung 2: Jedes echtes Primideal ist invertierbar

Beweis. Sei $0 \neq b \in \mathfrak{p}$. Da R Dedekindring ist; schreibe $Rb = \prod_i \mathfrak{p}_i$ mit $\mathfrak{p}_i$ Primideal. Aus Lemma 11.4 folgt: jedes $\mathfrak{p}_i$ ist invertierbar. Aus Behauptung 1 folgt: jedes $\mathfrak{p}_i$ ist maximal. Da aber $\mathfrak{p} \supseteq \prod_i \mathfrak{p}_i$ ist, folgt o.E., daß $\mathfrak{p} \supseteq \mathfrak{p}_1$ (Bemerkung 11.2) und damit $\mathfrak{p} = \mathfrak{p}_1$ und $\mathfrak{p}$ ist invertierbar. □

□