Algebraische Zahlentheorie
Algebra B 4 - Sommersemester 2017
Prof'in Dr. Salma Kuhlmann

17.Vorlesung

3 Juli 2017

Sei R ein Integritätsbereich.

Lemma 17.1
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. $B^{-1}(\prod_i A_i) = R \Rightarrow A_i \underbrace{(B^{-1} \prod_{j \neq i} A_j)}_{:=A_i^{-1}} = R$ □

Lemma 17.2
Für Produkte von invertierbaren (ganzen) Primidealen ist die Faktorisierung als Produkt von Primidealen eindeutig.

Bemerkung 17.1
Sei $\mathfrak{p} \lhd R$ ein Primideal und $I, J \lhd R$. Es ist: $\mathfrak{p} \supseteq IJ \Rightarrow \mathfrak{p} \supseteq I$ oder $\mathfrak{p} \supseteq J$.

Beweis von Lemma 17.2. Sei $A = \prod_i \mathfrak{p}_i$, $\mathfrak{p}_i$ invertierbar (ganze) Primideale Sei $A = \prod_i \mathfrak{q}_i$, wobei $\mathfrak{q}_i$ 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. $\mathfrak{q}_1 \subseteq \mathfrak{p}_1$. 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 17.3
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 $\mathfrak{p} + Ra = \prod_{i=1}^{n} \mathfrak{p}_i$ 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 und es folgt (Lemma 17.1): $\mathfrak{p}_i/\mathfrak{p}$ und $\mathfrak{q}_j/\mathfrak{p}$ sind alle invertierbar. Aber

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

Vegleiche $(*), (**)$ und $(***)$. Es folgt nun (Lemma 17.2): Die Ideale $\{\mathfrak{q}_j/\mathfrak{p}\}$ sind die Ideale $\{\mathfrak{p}_i/\mathfrak{p}\}$ wiederholt zweimal, 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, 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 (da $I + I = I$ immer gilt)
$\mathfrak{p}Ra + \mathfrak{p}Ra = \mathfrak{p}Ra$, 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 $0 \neq b \in \mathfrak{p}$ und schreibe $Rb = \prod_i \mathfrak{p}_i$ mit $\mathfrak{p}_i$ Primideal (da R Dedekindring ist). Aus Lemma 17.1 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 $\mathfrak{p} \supseteq \mathfrak{p}_1$ und damit $\mathfrak{p} = \mathfrak{p}_1$ und $\mathfrak{p}$ ist invertierbar. □

□

Korollar 17.4
Sei R ein Dedekindring, dann ist die Faktorisierung von Idealen (als Produkt von Primidealen) eindeutig.

Beweis. Folgt unmittelbar aus Lemma 17.2 und Satz 17.3. □

Korollar 17.5
Sei R ein Dedekindring. Jedes $\neq 0$ gebrochenes Ideal ist invertierbar.

Beweis. Jedes (ganzes) Ideal $\neq 0$ ist Produkt von (invertierbaren) Primidealen, also ist jedes $\neq 0$ (ganzes) Ideal invertierbar und damit (Lemma 16.2) ist auch jedes gebrochenes Ideal $\neq 0$ invertierbar. □

Satz 17.6
Sei R ein Integritätsbereich. Es ist:
R ist ein Dedekindring$\Leftrightarrow$ jedes Ideal $\neq 0$ in R ist invertierbar.

Beweis. "$\Rightarrow$" folgt aus Satz 17.3 (beziehungsweise Korollar 17.5).
"$\Leftarrow$" Lemma 16.3 impliziert, daß R noethersch ist (jedes Ideal ist endlich erzeugt). Wir zeigen nun: jedes echtes Ideal ist Produkt von maximalen Idealen (insbesondere ist R ein Dedekindring). Sonst ist die Menge der echten Idealen, die kein solches Produkt sind, nicht leer. Sei $\mathfrak{a} \neq 0$ ein maximales Element davon ($\mathfrak{a}$ existiert, weil R noethersch ist). Da $\mathfrak{a}$ kein maximales Ideal ist, ist $\mathfrak{a}$ in einem maximalen Ideal $\mathfrak{m}$ strikt enthalten. Betrachte nun das (gebrochene) Ideal $\mathfrak{m}^{-1}\mathfrak{a}$.

Behauptung 1: $\mathfrak{m}^{-1}\mathfrak{a}$ ist ein ganzes Ideal.

Beweis. $\mathfrak{a} \subseteq \mathfrak{m} \Rightarrow \mathfrak{m}^{-1}\mathfrak{a} \subseteq R$. Bemerke nun: wenn I ein gebrochenes Ideal ist und $I \subseteq R$, ist dann $I \lhd R$. □

Behauptung 2: $\mathfrak{m}^{-1}\mathfrak{a} \supsetneq \mathfrak{a}$

Beweis. Es ist klar, daß $\mathfrak{m}^{-1}\mathfrak{a} = \mathfrak{a} \Rightarrow \mathfrak{m}\mathfrak{a} = \mathfrak{a}$; das ist aber wegen Hilfslemma (siehe hier weiter unten) unmöglich. □

Es folgt: $\mathfrak{m}^{-1}\mathfrak{a}$ ist ein Produkt von maximalen Idealen (folgt aus der Wahl von $\mathfrak{a}$), und damit ist $\mathfrak{a} = \mathfrak{m}(\mathfrak{m}^{-1}\mathfrak{a})$ auch solch ein Produkt: Widerspruch zur Wahl von $\mathfrak{a}$.

□

Hilfslemma
Seien $\mathfrak{a}, \mathfrak{m}$ Ideale in einem Ring R mit $\mathfrak{a}$ endlich erzeugt und $\mathfrak{m}\mathfrak{a} = \mathfrak{a}$. Dann existiert $z \in \mathfrak{m}$, so daß $(1 - z)\mathfrak{a} = 0$ (Insbesondere ist $\mathfrak{m}\mathfrak{a} = \mathfrak{a}$ unmöglich, wenn $1 \notin \mathfrak{m}$,$\mathfrak{a} \neq 0$ und R ein Integritätsbereich ist).

Beweis. Sei $\{x_1, \ldots, x_n\}$ erzeugend für $\mathfrak{a}$ und $\mathfrak{a}_i$ das von $\{x_i, \ldots, x_n\}$ erzeugte Ideal (also $\mathfrak{a} = \mathfrak{a}_1$), und setze $\mathfrak{a}_{n+1} = \{0\}$. Wir zeigen per Induktion über i: $\exists z_i \in \mathfrak{m}$, so daß $(1 - z_i)\mathfrak{a} \subseteq \mathfrak{a}_i$ (dann ist $z := z_{n+1}$ das gesuchte Element).
Für $i = 1$ setze $z_1 = 0$.
Aus $(1 - z_i)\mathfrak{a} \subset \mathfrak{a}_i$ und $\mathfrak{a} \subset \mathfrak{m}\mathfrak{a}$ folgt $(1 - z_i)\mathfrak{a} \subseteq \mathfrak{m}\mathfrak{a}_i$. Insbesondere gilt $(1 - z_i)x_i = \sum_{j=i}^{n} z_{ij}x_j$ für geeignete $z_{ij} \in \mathfrak{m}$, also ist $(1 - z_i - z_{ii})x_i \in \mathfrak{a}_{i+1}$ und wir können nehmen:
$1 - z_{i+1} := (1 - z_i)(1 - z_i - z_{ii})$. □