Algebraische Zahlentheorie
SS 2013
– Kuhlmann –

17. Vorlesung am 20.06.2013

Sei R ein Integritätsbereich.

Lemma 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 ist das Produkt B ein Hauptideal, so ist jedes A_i invertierbar.]

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

Lemma 2: Für Produkte von invertierbaren (ganzen) Primidealen ist die Faktorisierung als Produkt von Primidealen eindeutig.

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

Beweis von Lemma 2.

Sei $A = \prod_i \mathfrak{p}_i$ $\quad$ $\mathfrak{p}_i$ invertierbare (ganze) Primideale.

Sei $A = \prod_j \mathfrak{q}_j$ $\quad$ wobei $\mathfrak{q}_j$ Primideal ist

Sei $\mathfrak{p}_1$ minimales (für Inklusion) Mitglied von $\{\mathfrak{p}_i\}$. Aus $\prod_j \mathfrak{q}_j \subseteq \mathfrak{p}_1$ folgt OE $\mathfrak{q}_1 \subseteq \mathfrak{p}_1$. 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 $\mathfrak{p}_1^{-1}\left(\prod_i \mathfrak{p}_i\right) = \mathfrak{q}_1^{-1}\left(\prod_j \mathfrak{q}_j\right)$

und damit bekommen wir:

$$\prod_{i \neq 1} \mathfrak{p}_i = \prod_{j \neq 1} \mathfrak{q}_j$$

Per Induktion fortsetzen. ∎

<u>Satz 1.</u> Sei R ein Dedekindring und $\mathfrak{p}$ echtes Primideal ($\mathfrak{p} \neq \{0\}$, $\mathfrak{p} \neq R$). Dann ist $\mathfrak{p}$ invertierbar und maximal.

<u>Beweis.</u> <u>Beh 1.</u> Sei $\mathfrak{p}$ ein echtes invertierbares Primideal. Dann ist $\mathfrak{p}$ maximal.

<u>Beweis von Beh. 1.</u> Sei $a \in R$, $a \notin \mathfrak{p}$ und betrachte

die Ideale $\mathfrak{p} + Ra$ und $\mathfrak{p} + Ra^2$.

Da R Dedekindring ist haben wir Faktorisierungen

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

mit $\mathfrak{P}_i$, $\mathfrak{q}_j$ Primideale.

Setze $\overline{R} := R/\mathfrak{p}$ und $\bar{a} := a \bmod \mathfrak{p}$.

Wir haben:

$$\left.\begin{aligned} (*) \quad & \overline{R}.\bar{a} = \prod (\mathfrak{P}_i/\mathfrak{p}) \\ (**) \quad & \overline{R}.\bar{a}^2 = \prod (\mathfrak{q}_j/\mathfrak{p}) \end{aligned}\right\} \text{ und } \begin{array}{c} \mathfrak{P}_i/\mathfrak{p} \\ \mathfrak{q}_j/\mathfrak{p} \\ \text{sind Primideale.} \end{array}$$

Nun sind $\overline{R}.\bar{a}$ und $\overline{R}.\bar{a}^2$ ~~sind~~ Hauptideale

also sind invertierbar, es folgt (Lemma 1):

$\mathfrak{P}_i/\mathfrak{p}$ und $\mathfrak{q}_j/\mathfrak{p}$ sind alle invertierbar. Aber

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

Vergleiche $(*)$, $(**)$ und $(***)$. Es folgt nun (Lemma 2)

daß 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 OE:

$$\mathfrak{q}_{2i} / \mathfrak{p} = \mathfrak{q}_{2i-1} / \mathfrak{p} = \mathfrak{p}_i / \mathfrak{p}.$$

Es folgt: $\mathfrak{q}_{2i} = \mathfrak{q}_{2i-1} = \mathfrak{p}_i$.

wir bekommen:

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

Daraus folgt:

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

[Begründung für (1): $\mathfrak{p} \subseteq \mathfrak{p} + Ra^2$ gilt immer, $\left(\begin{array}{c}\text{aus: Definition} \\ \text{Idealsummen}\end{array}\right)$

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:

$$(\mathfrak{p}+Ra)(\mathfrak{p}+Ra) = (\mathfrak{p}+Ra)\mathfrak{p} + (\mathfrak{p}+Ra)Ra$$

$$= \mathfrak{p}^2 + (\mathfrak{p}Ra + \mathfrak{p}Ra) + Ra\,Ra$$

Nun ist

$Ra\,Ra = a^2R$ 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 (+) 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 $\mathfrak{p}$ invertierbar ist per Annahme folgt:

$$\mathfrak{p}^{-1}\mathfrak{p} = \mathfrak{p}^{-1}\mathfrak{p}(\mathfrak{p} + Ra)$$

d.h

$$R = \mathfrak{p} + Ra .$$

Da $a \in R \setminus \mathfrak{p}$ beliebig ist folgt nun: $\mathfrak{p}$ ist maximal. $\blacksquare$ Beh 1

Beh. 2: jedes echtes Primideal ist invertierbar.

Beweis von Beh. 2: Sei $0 \neq b \in \mathfrak{p}$ ~~und~~ und schreibe

$$Rb = \prod_i \mathfrak{p}_i$$ mit $\mathfrak{p}_i$ Primideale (da R Dedekindring ist). Aus Lemma 1 folgt: jedes $\mathfrak{p}_i$ is invertierbar. Aus Beh 1 folgt: jedes $\mathfrak{p}_i$ ist maximal. Da aber $\mathfrak{p} \supseteq \prod_i \mathfrak{p}_i$ folgt OE $\mathfrak{p} \supseteq \mathfrak{p}_1$, und damit $\mathfrak{p} = \mathfrak{p}_1$ und $\mathfrak{p}$ ist invertierbar. $\blacksquare$

Korollar 1. Sei R Dedekindring, dann ist die Faktorisierung von Idealen (als Produkt von Primidealen) eindeutig.

Beweis. folgt unmittelbar aus Lemma 2 und Satz 1. ∎

Korollar 2 Sei R ein Dedekindring.
Jedes $0 \neq$ 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 2 16. Vorlesung) auch jedes gebrochenes Ideal $\neq 0$ ist invertierbar. ∎

Satz 2. Sei R Integritätsbereich. Es ist:
R ist Dedekindring $\Leftrightarrow$ jedes Ideal $\neq 0$ in R ist invertierbar.

Beweis. "$\Rightarrow$" folgt aus Satz 1 (beziehungsweise Kor 2).
"$\Leftarrow$" Lemma 3 16. Vorlesung impliziert daß R noethersch ist (jedes Ideal ist endlich erzeugt). Wir zeigen nun: jedes echtes Ideal ist

Produkt von maximalen Idealen (insbesondere R ist 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 $\mathfrak{a}$ strikt enthalten in einem maximalen Ideal $\mathfrak{m}$. Betrachte nun das (gebrochene) Ideal $\mathfrak{m}^{-1}\mathfrak{a}$.

<u>Beh 1.</u> $\mathfrak{m}^{-1}\mathfrak{a}$ ist ein ganzes Ideal.

Beweis von Beh 1: $\mathfrak{a} \subseteq \mathfrak{m} \Rightarrow \mathfrak{m}^{-1}\mathfrak{a} \subseteq R$.

Nun bemerke daß I gebrochenes Ideal und $I \subseteq R \Rightarrow I \triangleleft R$ ∎ Beh 1.

<u>Beh 2:</u> $\mathfrak{m}^{-1}\mathfrak{a} \supsetneq \mathfrak{a}$

Beweis von Beh 2: Es ist klar daß: $\mathfrak{m}^{-1}\mathfrak{a} = \mathfrak{a} \Rightarrow$

$\mathfrak{m}\,\mathfrak{a} = \mathfrak{a}$; das ist aber unmöglich wegen

Hilfslemma (siehe hier weiter unten). $\blacksquare$ Beh 2

Es folgt: $\mathfrak{m}^{-1}\mathfrak{a}$ ist 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. Widerspricht Wahl von $\mathfrak{a}$. $\blacksquare$

Hilfslemma: Seien $\mathfrak{a}$, $\mathfrak{m}$ Ideale (in einem Ring R) mit $\mathfrak{a}$ endlich erzeugt und $\mathfrak{m}\,\mathfrak{a} = \mathfrak{a}$. Dann $\exists\, z \in \mathfrak{m}$ so daß $(1-z)\,\mathfrak{a} = 0$. (Insbesondere ist $\mathfrak{m}\,\mathfrak{a} = \mathfrak{a}$ unmöglich wenn $\mathfrak{m} \not\ni 1$, $\mathfrak{a} \neq 0$ und R ein Integritätsbereich ist.)

Beweis. Sei $\{x_1, \dots, x_n\}$ erzeugend für $\mathfrak{a}$, und $\mathfrak{a}_i$ das Ideal erzeugt von $\{x_i, \dots, x_n\}$

(so $\mathfrak{a} = \mathfrak{a}_1$); und setze $\mathfrak{a}_{n+1} = \{0\}$.

Wir zeigen per Induktion nach 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 $\left.\begin{array}{l} (1-z_i)\,\mathfrak{a} \subset \mathfrak{a}_i \\ \text{und} \quad \mathfrak{a} \subset \mathfrak{m}\,\mathfrak{a} \end{array}\right\}$ folgt $(1-z_i)\,\mathfrak{a} \subseteq \mathfrak{m}\,\mathfrak{a}_i$

insbesondere gilt

$$(1-z_i)\,x_i = \sum_{j=1}^{n} z_{ij}\, x_j \qquad \text{für geeignete } z_{ij} \in \mathfrak{m}.$$

Also ist $(1 - z_i - z_{ii})\, x_i \in \mathfrak{a}_{i+1}$

und wir können nehmen:

$$1 - z_{i+1} := (1-z_i)(1 - z_i - z_{ii}). \qquad \blacksquare$$