Vorlesung Zahlentheorie I (Algebraische ZT)

WiSe '22/'23, Uhu
K. Halupczok

Z11: Dedekindbereiche II

Stichworte: Eind. zerl. von $\mathfrak{a}$ in Primideale = PIZ, Dedekindbereich: faktoriell ($\Leftrightarrow$ HIB), $\mathfrak{b} \mid \mathfrak{a}$, Idealnorm $N(\mathfrak{a})$ ist multiplikativ

---

11.1. **Einleitung:** Jedes ganze Ideal $\mathfrak{a} \neq 0$ in einem Dedekindbereich ist eindeutig als Produkt von Primidealen darstellbar, d.h. es gilt der Satz von der eindeutigen Primidealzerlegung, kurz PIZ. Diese Eigenschaft charakterisiert genau die Dedekindbereiche. Faktoriell ist ein Dedekindbereich genau dann, wenn er HIB ist. Eine Konsequenz der PIZ ist, dass jedes Ideal im Dedekindbereich maximal 2 Erzeuger besitzt. Die multiplikative Idealnorm ist eine natürliche Fortsetzung der gewöhnlichen Norm auf ganze Ideale.

11.2. **Satz:** Sei A Dedekindbereich und $\mathcal{P} := \{\mathfrak{p} : 0 \neq \mathfrak{p} \subseteq A \text{ prim}\}$.
Dann ist $I(A)$ eine freie abelsche Gruppe mit Basis $\mathcal{P}$.
Insbesondere ist also jedes ganze Ideal $\mathfrak{a} \neq 0$ eindeutig (bis auf Reihenfolge) als ein Produkt von Primidealen darstellbar.

$\rightsquigarrow$ eindeutige PIZ (Primidealzerlegung)

Bew.: Betr. $G(A) := \{\mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r} : r \in \mathbb{N},\ \mathfrak{p}_1, \dots, \mathfrak{p}_r \in \mathcal{P},\ \text{die } e_i \in \mathbb{Z}\} \subseteq I(A)$,
ist Untergruppe von $I(A)$.

- z.z.: $G(A) = I(A)$ [dann $I(A)$ Gruppe]
  Sei $\mathfrak{I} \in I(A)$. Dann ex. $0 \neq b \in A$ mit $b\mathfrak{I} \subseteq A$.
  Mit 10.20 folgt: $\exists\, \mathfrak{p}_1, \dots, \mathfrak{p}_s, \mathfrak{q}_1, \dots, \mathfrak{q}_r \in \mathcal{P}$ mit $b\mathfrak{I} = \mathfrak{p}_1 \cdots \mathfrak{p}_s$ und $Ab = \mathfrak{q}_1 \cdots \mathfrak{q}_r$.
  Es ist also $\mathfrak{I} = (Ab)^{-1} \cdot (b\mathfrak{I}) = \mathfrak{q}_1^{-1} \cdots \mathfrak{q}_r^{-1} \cdot \mathfrak{p}_1 \cdots \mathfrak{p}_s \subseteq G(A)$.
- z.z.: $I(A)$ ist frei mit Basis $\mathcal{P}$.
  Andernfalls ex. $r \geq 1$, $\mathfrak{p}_1, \dots, \mathfrak{p}_r \in \mathcal{P}$ p.w.v., $e_1, \dots, e_r \in \mathbb{Z} \setminus \{0\}$ mit $\mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r} = A$. Seien OE $e_1, \dots, e_s > 0$, $e_{s+1}, \dots, e_r < 0$ mit $s < r$ [$s = r \Rightarrow \lightning$].
  Dann ist $\mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_s^{e_s} = \mathfrak{p}_{s+1}^{-e_{s+1}} \cdots \mathfrak{p}_r^{-e_r} \subseteq \mathfrak{p}_r$.
  Mit 10.5 folgt: $\exists\, 1 \leq i \leq s : \mathfrak{p}_i \subseteq \mathfrak{p}_r$, also $\mathfrak{p}_i = \mathfrak{p}_r$ $\lightning$ [A Dedekindbereich]. $\square$

11.3. **Satz:** Ein IB, in dem jedes Ideal eindeutig Produkt von max. Idealen ist, ist ein Dedekindbereich. (→Umkehrung von 11.2, Beweis siehe: [Brüske/Tscheßeck/Vogel: Kommutative Algebra, Satz 12.30])

11.4. **Def.:** Für $I \in \mathcal{I}(A)$, $\mathfrak{p} \in \mathcal{P}$ sei $n_{\mathfrak{p}}(I)$ der Exponent von $\mathfrak{p}$ in I, d.h. es ist $I = \prod_{\mathfrak{p} \in \mathcal{P}} \mathfrak{p}^{n_{\mathfrak{p}}(I)}$. (*) [Eind. PIZ]

11.5. **Lemma:** (i) $n_{\mathfrak{p}}(IJ) = n_{\mathfrak{p}}(I) + n_{\mathfrak{p}}(J)$.
(ii) $I \subseteq A \Leftrightarrow \forall \mathfrak{p} \in \mathcal{P}: n_{\mathfrak{p}}(I) \geq 0$.
(iii) $I \subseteq J \Leftrightarrow \forall \mathfrak{p} \in \mathcal{P}: n_{\mathfrak{p}}(I) \geq n_{\mathfrak{p}}(J)$.
(iv) $n_{\mathfrak{p}}(I+J) = \min\{n_{\mathfrak{p}}(I), n_{\mathfrak{p}}(J)\}$
(v) $n_{\mathfrak{p}}(I \cap J) = \max\{n_{\mathfrak{p}}(I), n_{\mathfrak{p}}(J)\}$.

Bew.: (i): Klar nach (*), der PIZ.
(ii): „⇒" nach 10.20, „⇐" klar.
(iii): $I \subseteq J \Leftrightarrow \prod_{\mathfrak{p} \in \mathcal{P}} \mathfrak{p}^{n_{\mathfrak{p}}(I) - n_{\mathfrak{p}}(J)} = I \cdot J^{-1} \subseteq A \overset{(ii)}{\Leftrightarrow} \forall \mathfrak{p} \in \mathcal{P}: n_{\mathfrak{p}}(I) \geq n_{\mathfrak{p}}(J)$.
(iv): Sei $n_{\mathfrak{p}} := \min\{n_{\mathfrak{p}}(I), n_{\mathfrak{p}}(J)\}$. z.z.: $\prod_{\mathfrak{p} \in \mathcal{P}} \mathfrak{p}^{n_{\mathfrak{p}}} = I+J \left(= \prod_{\mathfrak{p} \in \mathcal{P}} \mathfrak{p}^{n_{\mathfrak{p}}(I+J)}\right)$.
„⊇": klar wegen (iii), „⊆": Nach (iii) ist $n_{\mathfrak{p}}(I+J) \leq n_{\mathfrak{p}}(I), n_{\mathfrak{p}}(J)$, also $n_{\mathfrak{p}}(I+J) \leq n_{\mathfrak{p}}$. Es folgt [(iii)]: $\prod_{\mathfrak{p} \in \mathcal{P}} \mathfrak{p}^{n_{\mathfrak{p}}} \subseteq I+J$.

(v): Sei $n_{\mathfrak{p}} := \max\{n_{\mathfrak{p}}(I), n_{\mathfrak{p}}(J)\}$. z.z.: $\prod_{\mathfrak{p} \in \mathcal{P}} \mathfrak{p}^{n_{\mathfrak{p}}} \overset{!}{=} I \cap J \left(= \prod_{\mathfrak{p} \in \mathcal{P}} \mathfrak{p}^{n_{\mathfrak{p}}(I \cap J)}\right)$.
„⊆": klar wegen (iii), „⊇": Nach (ii) ist $n_{\mathfrak{p}}(I \cap J) \geq n_{\mathfrak{p}}(I), n_{\mathfrak{p}}(J)$, also $n_{\mathfrak{p}}(I \cap J) \geq n_{\mathfrak{p}}$.
Es folgt: $\prod_{\mathfrak{p} \in \mathcal{P}} \mathfrak{p}^{n_{\mathfrak{p}}} \supseteq I \cap J$. □

11.6. **Bsp.:** $K = \mathbb{Q}(\sqrt{-5})$, $A = \mathbb{Z}[\sqrt{-5}]$ ist nicht faktoriell, da $6 = 2 \cdot 3 = (1+\sqrt{-5}) \cdot (1-\sqrt{-5})$, vgl. 10.2. Aber Satz 11.3 zeigt, dass das Hauptideal $(6) = A \cdot 6$ eindeutig (bis auf Reihenfolge) als Produkt von Primidealen geschrieben werden kann.
Hier ist noch nicht zu sehen, wie. Dafür wird ab 11.10 die Norm eines Ideals eingeführt. In Z13 erhalten wir $(6) = \mathfrak{p}_2^2 \cdot \mathfrak{p}_3 \mathfrak{p}_3'$ mit den Primidealen $\mathfrak{p}_2 = (2, \sqrt{-5}+1)$, $\mathfrak{p}_3 = (3, \sqrt{-5}+1)$, $\mathfrak{p}_3' = (3, \sqrt{-5}-1)$ als eindeutige PIZ.

11.7. **Satz:** Ein Dedekindbereich ist genau dann faktoriell, wenn er Hauptidealbereich ist.

Bew.: „⇐": klar [Algebra A13.17], „⇒": Sei A faktorieller Dedekindbereich.

Ann.: A ist nicht HIB. Dann ex. ein Ideal $\mathfrak{r} \subsetneq A$, $\mathfrak{r}$ nicht Hauptideal.
Nach 11.2 ist $\mathfrak{r}$ Produkt von Primidealen $\neq 0$, daher ex. ein (Faktor!) Primideal $\mathfrak{p} \subsetneq A$, $\mathfrak{p}$ nicht Hauptideal. Sei $b \in \mathfrak{p}$ so, dass (b) bzgl. $\subsetneq$ maximal ist (A noethersch). Dann ist $0 \neq (b) \subsetneq \mathfrak{p}$. Nun ist (b) nicht prim [Sonst wäre (b) prim, also $(b) = \mathfrak{p}$ Hauptideal, ↯.] Dann ist b nicht prim. [⊛]
Also ist b reduzibel, da A faktoriell (vgl. 10.2 bzw. Algebra A13.19).
Somit ex. Nichteinheiten $a_1, a_2 \in A$ mit $b = a_1 \cdot a_2$. Da $\mathfrak{p}$ prim, sei dabei o.E. $a_1 \in \mathfrak{p}$. Dann gilt: $(b) \subsetneq (a_1) \subsetneq \mathfrak{p}$,
im ↯ zur Maximalität von (b). □ [Zu ⊛: b prim $\Rightarrow (b)$ prim, denn $xy \in (b) \Rightarrow xy = ab$, $a \in A$ $\Rightarrow b \mid x \vee b \mid y \Rightarrow x \in (b) \vee y \in (b)$ (b prim in A)]

11.8. **Notation:** $\mathfrak{b} \mid \mathfrak{r} \;:\Leftrightarrow\; \mathfrak{r} \subseteq \mathfrak{b}$.
„$\mathfrak{b}$ über $\mathfrak{r}$", bzw. „$\mathfrak{b}$ teilt $\mathfrak{r}$"

11.9. **Satz:** In einem Dedekindbereich A ist jedes Ideal von zwei Elementen erzeugt.
Genauer: Ist $0 \neq \mathfrak{r} \subsetneq A$ Ideal, so gilt: $\forall\, 0 \neq a \in \mathfrak{r}\; \exists\, b \in \mathfrak{r} : \mathfrak{r} = (a, b)$.

Bew.: Sei $0 \neq \mathfrak{r} \subsetneq A$ Ideal, etwa $\mathfrak{r} = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$ mit p.w.v. $\mathfrak{p}_i \in \mathcal{P}$, $e_i \in \mathbb{N}$.
Sei weiter $0 \neq a \in \mathfrak{r}$, also $(a) \subseteq \mathfrak{r}$ ($\Leftrightarrow \mathfrak{r} \mid (a)$).
Dann ist $(a) = Aa = \mathfrak{p}_1^{e_1'} \cdots \mathfrak{p}_r^{e_r'} \cdot \mathfrak{p}_{r+1}^{e_{r+1}'} \cdots \mathfrak{p}_s^{e_s'}$ mit $e_i' \geq e_i$ für $1 \leq i \leq r$.
Genügt, z.z.: $\exists\, b \in \mathfrak{r}$ mit $b \begin{cases} \in \mathfrak{p}_i^{e_i} \setminus \mathfrak{p}_i^{e_i+1}, & 1 \leq i \leq r \quad (n_{\mathfrak{p}}((b)) = e_i), \\ \notin \mathfrak{p}_i, & r < i \leq s. \end{cases}$

[Denn: $\mathfrak{p} \in \mathcal{P} \Rightarrow n_{\mathfrak{p}}((a,b)) = n_{\mathfrak{p}}((a)+(b)) \overset{n_5\,(iv)}{=} \min\{n_{\mathfrak{p}}((a)), n_{\mathfrak{p}}((b))\} = \begin{cases} 0, & \mathfrak{p} \neq \mathfrak{p}_1, \ldots, \mathfrak{p}_s; \\ e_i, & \mathfrak{p} = \mathfrak{p}_i,\ 1 \leq i \leq r; \\ 0, & \mathfrak{p} = \mathfrak{p}_i,\ r < i \leq s. \end{cases}$
$= n_{\mathfrak{p}}(\mathfrak{r})$, also $\mathfrak{r} = (a, b)$.]

Für $1 \leq i \leq r$ sei $c_i \in \mathfrak{p}_i^{e_i} \setminus \mathfrak{p}_i^{e_i+1}$ ($\neq \emptyset$, sonst ↯ zur eind. PIZ).
Nach dem chinesischen Restsatz [$\mathfrak{p}_1^{e_1+1}, \ldots, \mathfrak{p}_r^{e_r+1}$ p.w. teilerfremd]
ex. ein $b \in A$ mit $b \equiv c_i \pmod{\mathfrak{p}_i^{e_i+1}}$, $1 \leq i \leq r$,
und $b \equiv 1 \pmod{\mathfrak{p}_i}$, $r < i \leq s$. Dieses $b \in A$ tut's. □

11.10. **Def.:** Sei K Zahlkörper mit Zahlring A, $\mathfrak{a} \neq 0$ ganzes Ideal.
Dann heißt $N(\mathfrak{a}) := \#A/\mathfrak{a}$ die Norm (Idealnorm) von $\mathfrak{a}$.

11.11. **Bem.:** (1) Nach 8.10 ist $N((a)) = \#A/(a) = |N(a)|$, die Absolutnorm von a.
(2) Ist $(a) \subseteq \mathfrak{a} \subseteq A$, so ist $\#A/\mathfrak{a}$ endlich, da $\#A/(a)$ endlich nach 8.10.
(3) Sind M, N A-Moduln, $\pi: M \to N$ surjektiver A-Modul-Morphismus, so liefern die Abbildungen $\pi^{-1}(N') \hookleftarrow N'$ und $M' \hookrightarrow \pi(M')$ zueinander inverse Bijektionen zwischen der Menge aller Teilmoduln M' von M mit $\ker \pi \subseteq M'$ und der Menge aller Teilmoduln N' von N.
「Isomorphiesatz」
(4) Sei $\mathfrak{a} \subseteq A$ Ideal, M ein A-Modul. Dann ist $\mathfrak{a}M$ der von $\{ax;\ a \in \mathfrak{a},\ x \in M\}$ erzeugte Teilmodul von M.
Sei $N := M/\mathfrak{a}M$, ist A-Modul.
Es gilt: $\forall a \in \mathfrak{a}: aN = 0$, d.h. $\mathfrak{a} \subseteq \mathrm{Ann}(N)$.
Deshalb ist N in natürlicher Weise auch ein $A/\mathfrak{a}$-Modul:
$$\underbrace{(b + \mathfrak{a})}_{\in A/\mathfrak{a}} \cdot \underbrace{(x + \mathfrak{a}M)}_{\in N} := bx + \mathfrak{a}M \in N.$$

Es gilt die Multiplikativität der Idealnorm.

11.12. **Lemma:** Für ganze Ideale $\mathfrak{a}, \mathfrak{b} \neq 0$ in K gilt: $N(\mathfrak{a} \cdot \mathfrak{b}) = N(\mathfrak{a}) \cdot N(\mathfrak{b})$.
Bew.: Es genügt, dies für $\mathfrak{b} = \mathfrak{p}$ prim zu zeigen.
「$N(\mathfrak{a} \cdot \mathfrak{p}_1\mathfrak{p}_2) = N(\mathfrak{a}\mathfrak{p}_1)N(\mathfrak{p}_2) = N(\mathfrak{a})N(\mathfrak{p}_1)N(\mathfrak{p}_2)$
$= N(\mathfrak{a})N(\mathfrak{p}_1\mathfrak{p}_2)$, vollst. Ind.」
Es ist $N(\mathfrak{a} \cdot \mathfrak{p}) = \#A/\mathfrak{a}\mathfrak{p}$, $\mathfrak{a}\mathfrak{p} \subseteq \mathfrak{a} \subseteq A$
Es folgt: $\underbrace{\#A/\mathfrak{a}\mathfrak{p}}_{N(\mathfrak{a}\cdot\mathfrak{p})} = \underbrace{\#A/\mathfrak{a}}_{N(\mathfrak{a})} \cdot \#\mathfrak{a}/\mathfrak{a}\mathfrak{p}$.
Nun ist $\mathfrak{a}/\mathfrak{a}\mathfrak{p}$ ein $\underbrace{A/\mathfrak{p}}_{\text{Körper}}$-Modul, also $A/\mathfrak{p}$-Vektorraum.
↖ nach 11.11 (4)

z.z.: $\mathcal{O}_K/\mathcal{O}_K\mathfrak{p}$ ist eindimensionaler $A/\mathfrak{p}$-Vektorraum.
[Dann ist $\#\mathcal{O}_K/\mathcal{O}_K\mathfrak{p} = \#A/\mathfrak{p} = N(\mathfrak{p})$.]
Dazu genügt z.z.: $\mathcal{O}_K/\mathcal{O}_K\mathfrak{p}$ hat keine A-Teilmoduln außer 0 und $\mathcal{O}_K/\mathcal{O}_K\mathfrak{p}$.
Betrachte dazu $\pi: \mathcal{O}_K \to \mathcal{O}_K/\mathcal{O}_K\mathfrak{p}$, ist surjektiver A-Modulmorphismus.
Nun ist z.z.: Es gibt keine Ideale $\mathfrak{l}$ mit $\mathcal{O}_K\mathfrak{p} \subsetneq \mathfrak{l} \subsetneq \mathcal{O}_K$.
Dies ist aber klar wegen der eindeutigen PIZ von $\mathcal{O}_K$ und $\mathcal{O}_K\mathfrak{p}$. □

11.13. **Bem.:** (1) Ist $\#A/\mathcal{O}_K = N(\mathcal{O}_K)$ prim, so ist $\mathcal{O}_K$ prim.
[$\mathcal{O}_K = \mathcal{O}_{K_1} \cdot \mathcal{O}_{K_2}$ mit $\mathcal{O}_{K_i} \neq A$, d.h. $N(\mathcal{O}_{K_i}) \neq 1$, $i = 1,2$.
So folgt: $N(\mathcal{O}_K) = N(\mathcal{O}_{K_1}) \cdot N(\mathcal{O}_{K_2})$ nicht prim.]
(2) Dies gilt nicht umgekehrt! D.h. $N(\mathcal{O}_K)$ prim $\not\Rightarrow$ $\mathcal{O}_K$ prim. Bsp.: in $\mathbb{Q}(\sqrt{m})$, $\mathcal{O}$ RA:
Falls $p \in \mathbb{N}$ prim in A bleibt, so ist $(p) = \mathfrak{p}$ Primid. nach ⊛ in 11.7.
Also $N((p)) = |N(p)| = p^2$ nicht prim.

[Falls p in A zerlegt als $(p) = \mathfrak{p} \cdot \mathfrak{p}' \Rightarrow p^2 = |N(p)| = N((p)) = N(\mathfrak{p})N(\mathfrak{p}')$ (p nicht prim in A, sonst (p) prim wegen ⊛, ↯)
$\Rightarrow N(\mathfrak{p}) = p$ prim]

Somit: $\mathfrak{p}$ prim $\Rightarrow$ $N(\mathfrak{p})$ kann Primzahl sein, muss aber nicht.