Vorlesung Zahlentheorie I (Algebraische ZT)

WiSe '22/'23, hhu
K. Halupczok

Z10: Dedekindbereiche I

Stichworte: $\mathfrak{a}\cdot\mathfrak{b}$, Dedekindbereich z.B. HIB, ZR, gebrochenes (Haupt)Ideal, ganzes Ideal, Inverse von Primidealen, Eind. zerl. von $\mathfrak{a}$ in Primideale

---

10.1. **Einleitung:** Es gibt nicht faktorielle Zahlringe. Wir werden den Idealbegriff aber so erweitern, dass in Zahlringen stets eine eindeutige Zerlegung in Primideale möglich ist.

10.2. • Erinnerung an Algebra, kap. A13: Sei A ein IB.

Ein $x\in A$ heißt irreduzibel $:\Leftrightarrow x\notin A^\times$ und $\forall a,b\in A: (x=ab \Rightarrow a\in A^\times \vee b\in A^\times)$.

Ein $x\in A$ heißt prim (primes El.) $:\Leftrightarrow \forall a,b\in A: x\mid ab \Rightarrow x\mid a \vee x\mid b$.

Sofort klar: x prim $\Rightarrow x$ irred. In faktoriellen Ringen gilt: x irred. $\Leftrightarrow x$ prim. [„$\Rightarrow$": A13.19]

Bsp.: In $A=\mathbb{Z}[\sqrt{-5}]$ gilt $6=2\cdot 3=(1+\sqrt{-5})\cdot(1-\sqrt{-5})$, wo $2, 3, 1+\sqrt{-5}, 1-\sqrt{-5}$ irreduzibel.

[• Wäre $2=a\cdot b$, $a,b\notin A^\times$, folgt $4=N(2)=N(a)N(b)$, also $N(a)=\pm 2=N(b)$, da weder a noch b Norm ± 1 haben können. Aber $N(u+v\sqrt{-5})=u^2+5v^2\overset{!}{=}\pm 2$ ist mit $u,v\in\mathbb{Z}$ unmöglich.
• Analog sind $3, 1+\sqrt{-5}, 1-\sqrt{-5}$ irred.] Damit ist $\mathbb{Z}[\sqrt{-5}]$ nicht faktoriell!

• Erinnerung an Algebra: Idealtheorie, kap. A11: Sei A ein IB. Die A-Teilmoduln sind genau die Ideale. [A16.7 (13)]

$\mathfrak{p}\subsetneq A$ prim/Primideal $:\Leftrightarrow \forall a,b\in A: (a\cdot b\in\mathfrak{p} \Rightarrow a\in\mathfrak{p} \vee b\in\mathfrak{p})$.

A12.24: $\mathfrak{a}$ maximal $\Rightarrow \mathfrak{a}$ prim, i.a. nicht „$\Leftarrow$".

Wollen zunächst die Zerlegbarkeit von Idealen in Produkte untersuchen.

10.3. **Def.:** Sei A ein kommutativer Ring, seien $\mathfrak{a},\mathfrak{b}\subseteq A$ Ideale. Dann heißt $\mathfrak{a}\cdot\mathfrak{b}=\{\sum_{i=1}^{n} a_i b_i;\ n\in\mathbb{N},\ a_i\in\mathfrak{a},\ b_i\in\mathfrak{b}\}$ das von den Produkten $a\cdot b$ mit $a\in\mathfrak{a}$, $b\in\mathfrak{b}$ erzeugte Ideal.

10.4. **Bem.:** Ist $\mathfrak{a}=(a_1,\dots,a_m)$ ($:=Aa_1+\dots+Aa_m$), $\mathfrak{b}=(b_1,\dots,b_n)$ ($:=Ab_1+\dots+Ab_n$), so ist $\mathfrak{a}\cdot\mathfrak{b}=(a_1b_1,\dots,a_1b_n,\ \dots\dots,\ a_mb_n)$.

10.5. **Lemma:** Sei $\mathfrak{p}\subsetneq A$ Primideal, $\mathfrak{a}_1,\dots,\mathfrak{a}_m\subseteq A$ Ideale mit $\mathfrak{a}_1\cdots\mathfrak{a}_m\subseteq\mathfrak{p}$. Dann ex. ein $i\in\{1,\dots,m\}$ mit $\mathfrak{a}_i\subseteq\mathfrak{p}$.

Bew.: Sonst sei $a_i\in\mathfrak{a}_i\setminus\mathfrak{p}$ für alle $1\le i\le m$. Dann ist $a_1\cdots a_m\in\mathfrak{a}_1\cdots\mathfrak{a}_m\setminus\mathfrak{p}=\emptyset$ ↯. □

10.6. **Lemma:** In einem noetherschen Integritätsbereich A enthält jedes Ideal $\neq 0$ ein Produkt von Primidealen $\neq 0$.

Erinnerung/Def.: Ein IB A mit der Eigenschaft

$\exists$ keine unendl., echt aufsteigende Folge $\mathfrak{a}_0 \subsetneq \mathfrak{a}_1 \subsetneq \mathfrak{a}_2 \subsetneq \dots$ von Idealen in A

heißt noethersch. [Vgl. (FA) in Algebra A13.15, dort war dies nur mit Hauptidealen ausgedrückt.]

Bew.: Andernfalls ist $\{\mathfrak{a}; \mathfrak{a} \text{ Ideal} \neq 0, \mathfrak{a} \text{ enthält kein Produkt von Primidealen} \neq 0\} \neq \emptyset$.

Da A noethersch, enthält diese Menge ein maximales Element $\mathfrak{a}$.

Dann ist $\mathfrak{a}$ nicht prim, da $\mathfrak{a}$ sonst kein Gegenbeispiel wäre.

Seien also $x, y \in A \setminus \mathfrak{a}$ mit $x \cdot y \in \mathfrak{a}$. [$\mathfrak{a}$ nicht prim $\Leftrightarrow \exists x,y \in A : x \cdot y \in \mathfrak{a} \wedge x, y \notin \mathfrak{a}$]

Es folgt: $\mathfrak{a} \subsetneq \mathfrak{a} + (x)$ und $\mathfrak{a} \subsetneq \mathfrak{a} + (y)$.

Da $\mathfrak{a}$ maximal war, ex. Primideale $\mathfrak{q}_1, \dots, \mathfrak{q}_m, \mathfrak{p}_1, \dots \mathfrak{p}_n \neq 0$ mit $\mathfrak{q}_1 \cdots \mathfrak{q}_m \subseteq \mathfrak{a} + (x)$ und $\mathfrak{p}_1 \cdots \mathfrak{p}_n \subseteq \mathfrak{a} + (y)$.

Es folgt: $\mathfrak{q}_1 \cdots \mathfrak{q}_m \cdot \mathfrak{p}_1 \cdots \mathfrak{p}_n \subseteq (\mathfrak{a}+(x))(\mathfrak{a}+(y)) = \mathfrak{a} + (xy) = \mathfrak{a}$,

im $\lightning$ zur Wahl von $\mathfrak{a}$. □

10.7. **Def.:** Ein Dedekindbereich ist ein ganz abgeschlossener, noetherscher Integritätsbereich, in dem jedes Primideal $\neq 0$ maximal ist. ↙ s. 23.11

10.8. **Bsp.:** Hauptidealbereiche sind Dedekindbereiche.

10.9. **Satz:** Zahlringe sind Dedekindbereiche.

Bew.: Sei A Zahlring des Zahlkörpers K. Klar: A ganz abgeschlossen [23, 3.14].

Sei $\mathfrak{a} \subseteq A$ Ideal, dann ist $\mathfrak{a}$ insb. UG der additiven Gruppe von $A \cong \mathbb{Z}^n$, vgl. 8.4. Da UG endl. erzeugter ab. Gruppen endl. erzeugt sind (Algebra A6.15), ist $\mathfrak{a}$ endlich erzeugt, sogar als abelsche Gruppe. Also ist A noethersch, da jedes Ideal endl. erzeugt. Sei nun $\mathfrak{p} \neq 0$ ein Primideal in A, und $0 \neq x \in \mathfrak{p}$. Betrachte $(x) = Ax \subseteq \mathfrak{p} \subseteq A$. Dann ist A/Ax endlich, da nach 8.10 $\#\, A/Ax = |N(x)|$ ist. Somit ist $A/\mathfrak{p}$ endlicher IB, also Körper, d.h. $\mathfrak{p}$ ist maximal. □

10.10. **Def.:** Sei A noetherscher IB mit Quotientenkörper K.
Ein **gebrochenes Ideal** (von A) ist dann ein A-Modul $I \subseteq K$ mit $bI \subseteq A$ für ein $0 \neq b \in A$. [$\rightsquigarrow I \subseteq \frac{1}{b} \cdot A$]

10.11. **Bem.:** Es ist $bI =: \mathfrak{a}$ ein Ideal in A, also $\mathfrak{a} = \sum_{i=1}^{n} Ax_i$ endlich erzeugt.
Somit ist $I = \sum_{i=1}^{n} A \frac{x_i}{b}$ ein endl. erz. A-Modul.
Umgekehrt ist jeder endl. erz. A-Modul I in K ein gebrochenes Ideal wegen $I = \sum_{i=1}^{n} A \frac{a_i}{b_i} \Rightarrow \left(\prod_{i=1}^{n} b_i\right) I \subseteq A$.

10.12. **Def.:** Gebrochene Ideale der Gestalt $I = Az$ mit $z \in K$ heißen **gebrochene Hauptideale**.

10.13. **Bem.:** (1) Ist A HIB, so ist jedes gebrochene Ideal gebrochenes Hauptideal.
[$b \cdot I = A \cdot a \Rightarrow I = A \cdot \frac{a}{b}$]
(2) Seien $I, J \subseteq K$ gebrochene Ideale. Dann sind $I \cap J$, $I + J$ und $I \cdot J$ (= der von $\{xy;\ x \in I, y \in J\}$ erzeugte A-Modul) gebrochene Ideale.

10.14. **Def.:** Ideale $\mathfrak{a} \subseteq A$ heißen auch **ganze Ideale**.
Sei $I(A)$ die Menge aller gebrochenen Ideale $\neq 0$ von A,
und $F(A)$ die Menge aller gebrochenen Hauptideale $\neq 0$ von A.

10.15. **Bem.:** (1) $I(A)$ ist bezüglich $(I, J) \mapsto IJ$ eine abelsche Halbgruppe mit neutralem Element A.
(2) Sei $\Phi : K^\times \to I(A)$, $y \mapsto Ay$. Dann ist $\operatorname{im} \Phi = F(A) \subseteq I(A)$.
Also ist $\Phi : K^\times \to F(A)$, $y \mapsto Ay$, ein surjektiver Gruppenhomomorphismus, dieser hat $\ker \Phi = A^\times$. Also folgt: $F(A) \cong K^\times / A^\times$.
(3) Ist A faktoriell, P ein Repräsentantensystem für die Primelemente modulo Assoziiertheit, so ist $F(A)$ eine freie abelsche Gruppe mit Basis Ap $(p \in P)$.
[Behr. $F(A) \ni Az$ mit $z \in K$, $z = u p_1^{e_1} \cdots p_r^{e_r}$, die $e_i \in \mathbb{Z}$, $p_i \in P$, $u \in A^\times$.
Dann ist $Az = (Ap_1)^{e_1} \cdots (Ap_r)^{e_r} \cdot \underbrace{(Au)}_{=A} = (Ap_1)^{e_1} \cdots (Ap_r)^{e_r}$.]
(4) Es gilt: A HIB $\Leftrightarrow F(A) = I(A)$.

10.16. **Voraussetzung:** Im folgenden sei A stets ein Dedekindbereich.
Ferner sei $\mathcal{P} = \{\mathfrak{p};\ 0 \neq \mathfrak{p} \subseteq A \text{ prim}\}$.

10.17. **Lemma:** Seien $I, J \subseteq I(A)$ mit $IJ \subseteq J$. Dann ist $I \subseteq A$.
Bew.: Sei $x \in I$. Für alle $n \in \mathbb{N}$ gilt dann: $x^n J \subseteq J$ (Vollst. Ind. nach n).
Sei $0 \neq b \in J$. Dann ist also $\sum_{n \in \mathbb{N}} A x^n \cdot b = A[x] \cdot b \subseteq J$.
Als A-Teilmodul des endl. erz. A-Moduls J ist $A[x] \cdot b$ endl. erz.
Also ist auch $A[x]$ endl. erz., d.h. x ist ganz über A.
Somit ist $x \in A$, da A ganz abgeschlossen in k ist. Also folgt $I \subseteq A$. □

10.18. **Lemma:** Jedes $\mathfrak{p} \in \mathcal{P}$ ist invertierbar, d.h. $\exists\, I \in I(A)$ mit $I \cdot \mathfrak{p} = A$.
Bew.: Setzen $I := \{x \in K;\ x\mathfrak{p} \subseteq A\}$, ist gebrochenes Ideal.
⌜Denn: $0 \neq b \in \mathfrak{p} \Rightarrow I \cdot b \in A$.⌟
Es gilt: $A \subseteq I$, und $I\mathfrak{p} \subseteq A$. Somit: $\mathfrak{p} \subseteq I\mathfrak{p} \subseteq A$.
Da $\mathfrak{p}$ maximal (im Dedekindbereich A), ist $I\mathfrak{p} = \mathfrak{p}$ oder $I\mathfrak{p} = A$.
Ann.: Sei $I\mathfrak{p} = \mathfrak{p}$. Mit 10.17 folgt dann: $I = A$.
Sei $0 \neq b \in \mathfrak{p}$. Nach 10.6 enthält $(b) = Ab$ ein Produkt aus Primidealen $\neq 0$, etwa $\mathfrak{p}_1 \cdots \mathfrak{p}_s \subseteq Ab$, $0 < s$ minimal.

Wegen 10.5 sei $0 < \mathfrak{p}_1 \subseteq \mathfrak{p}$. Es folgt $\mathfrak{p}_1 = \mathfrak{p}$, da beide Ideale maximal, da A Dedekindbereich.
Sei nun $a \in \mathfrak{p}_2 \cdots \mathfrak{p}_s \setminus Ab$ ⌜Falls $s = 1$, nehme $a \in A \setminus Ab$. s minimal!⌟
Es folgt: $x := \frac{a}{b} \notin A$. Ferner ist $a\mathfrak{p} \subseteq Ab$, d.h. $x \cdot \mathfrak{p} \subseteq A$,
also ist $x \in \underbrace{I}_{(\text{Def. } I)} = A$ ↯. □

10.19. **Bem.:** Das Inverse I von $\mathfrak{p}$ ist eindeutig bestimmt.
Bew.: Seien I, I' Inverse von $\mathfrak{p}$, d.h. $I\mathfrak{p} = A = I'\mathfrak{p}$.
Dann ist $I = I \cdot A = I \cdot \mathfrak{p} I' = A \cdot I' = I'$. □

Notation: $\mathfrak{p}^{-1} := I$, $\mathfrak{p}^{-e} := (\mathfrak{p}^{-1})^e$ für $e \in \mathbb{N}_{>1}$.

10.20. **Lemma:** Jedes Ideal $0 \neq \mathfrak{a} \subsetneq A$ ist Produkt von Primidealen $\neq 0$.

Bew.: Andernfalls sei $\mathfrak{a}$ ein bezüglich $\subseteq$ maximales Gegenbeispiel; $\mathfrak{a}$ existiert, da A noethersch. Dann ist $\mathfrak{a}$ nicht prim und $\mathfrak{a} \neq A$ (A = leeres Pl. von Primidealen). Sei $\mathfrak{p} \in \mathcal{P}$ prim mit $\mathfrak{a} \subseteq \mathfrak{p}$.
Mit 10.18. folgt: $\mathfrak{p}^{-1}\mathfrak{p} = A$, also $\mathfrak{p}^{-1}\mathfrak{a} \subseteq A$.
Da $A \subsetneq \mathfrak{p}^{-1} \not\subseteq A$, folgt mit 10.17 dann: $\mathfrak{a} \subsetneq \mathfrak{p}^{-1}\mathfrak{a} \subseteq A$.
($A \subseteq \mathfrak{p}^{-1} \Rightarrow \mathfrak{a} \subseteq \mathfrak{p}^{-1}\mathfrak{a}$ ✓, zu "$\neq$": Sonst $\mathfrak{a} = \mathfrak{p}^{-1}\mathfrak{a} \subseteq \mathfrak{a} \overset{10.17}{\Rightarrow} \mathfrak{p}^{-1} \subseteq A$ ↯.)
Somit ist $\mathfrak{p}^{-1}\mathfrak{a}$ Produkt von Primidealen $\neq 0$,
etwa $\mathfrak{p}^{-1}\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_s$, also ist $\mathfrak{a} = \mathfrak{p} \cdot \mathfrak{p}_1 \cdots \mathfrak{p}_s$, ↯. □