Dedekindringe

Benjamin Reinhard

Ziel:

Dedekindringe einführen

$\mathcal{O}_K$ ist ein Dedekindring

Kapitel:

Module

Ganzheit

Spur und Diskriminante

Noethersch

Dedekindringe

1. Module

A Ring.

Definition 1. *Ein Tupel* $(M, +, \cdot, 0)$ *mit* $0 \in M$ *und Abbildungen*

$$+ : M \times M \to M$$

$$\cdot : A \times M \to M$$

nennen wir ein A-Modul, falls für alle $m, m_1, m_2 \in M$ *und* $a, a_1, a_2 \in A$ *gilt*

- $(M, +, 0)$ *ist eine abelsche Gruppe.*
- $(a_1 a_2) \cdot m = a_1 \cdot (a_2 \cdot m)$
- $(a_1 + a_2) \cdot m = a_1 \cdot m + a_2 \cdot m$
- $a \cdot (m_1 + m_2) = a \cdot m_1 + a \cdot m_2$
- $1 \cdot m = m$

Ersetzt A mit K, so haben wir die Def. Vektorraumes

Beispiele:

1. Alle Vektorräume sind Module
2. $A \subseteq B$ Ringe, $\cdot : A \times B \to B$, $(a,b) \mapsto ab \Rightarrow B$ A-Modul

Definition 3. *Sei* I *eine Indexmenge, so sagen wir* $\{m_i \in M : i \in I\}$ *erzeugt* M*, falls*

$$M = \left\{ \sum_{j \in J} a_j m_j : J \subseteq I \text{ endlich}, \ a_i \in A \right\}$$

und nennen die Menge K *A-linear unabhängig, falls*

$$\sum_{j \in J} a_j m_j = 0 \text{ und } a_j \in A, \ J \subseteq I \text{ endlich} \Rightarrow a_j = 0.$$

Letztendlich nennen wir die Menge eine A-Basis, falls sie M *erzeugen und A-linear unabhängig sind.* M *nennt man frei, falls es eine A-Basis besitzt.*

Proposition-Definition 4. *Besitzt* M *zwei A-Basen, so ist ihre Anzahl gleich. Also ist*

$$\mathrm{Rang}(M) = \text{ Anzahl Elemente einer Basis}$$

wohldefiniert und heisst der Rang von B.

$\mathrm{Rang}(V) = \dim_K(V)$

Lemma 5. *Ist A ein Hauptidealring und* M *frei, so ist jeder A-Untermodul* $N \subseteq M$ *frei und es gilt*

$$\mathrm{Rang}(N) \leqslant \mathrm{Rang}(M).$$

2. Ganzheit

Seien $A \subseteq B$ Ringe. "gü" = ganz über

Definition 6. *$b \in B$ heisst ganz über A, falls es ein nicht-konstantes, normiertes Polynom $f \in A[x]$ gibt mit*

$$f(b) = b^n + a_{n-1}b^{n-1} + ... + a_0 = 0.$$

B heisst ganz über A, falls alle Elemente in B ganz über A sind.

Lemma 7. *Folgende Aussagen sind äquivalent:* $b_i \in B$

(1) *$A[b_1, ..., b_n]$ ist ganz über A.*
(2) *$b_1, ..., b_n \in B$ sind ganz über A.*
(3) *$A[b_1, ..., b_n]$ ist ein endlich erzeugter A-Modul.*

- $1 \Rightarrow 2$: $b_1, \dots, b_n \in A[b_1, \dots, b_n]$
- $2 \Rightarrow 3$: Induktion über n:

  $n=1$: $b = b_1$. $A[b]$ gü $A \Rightarrow b$ gü $A \Rightarrow f \in A[x]$:

  $f(b) = b^n + \dots + a_0 = 0$. $A[b] = A \cdot 1 + A \cdot b + A b^2 + \dots + A b^{n-1}$

  $g(b) \in A[b]$: $g \in A[x]$: $g = pf + r$ $k = \deg r < \deg f = n$:

  $g(b) = p(b)\underbrace{\cancel{f(b)}}_{0} + r(b) = r(b) = \tilde{a}_k b^k + \dots + \tilde{a}_0 \in A \cdot 1 + \dots + A b^{n-1}$

  $A[b] \subseteq A \cdot 1 + \dots + A b^{n-1}$ $\quad \supseteq$: klar.

  $n \to n+1$: $A[b_1, \dots, b_n] = A[b_1][b_2] \dots [b_n]$.
- $3 \Rightarrow 1$: Skript.

$\square$

Definition 9. *Wir definieren den ganzen Abschluss von A in B als*

$$\bar{A} = \{b \in B : b \text{ ganz über } A\}$$

und nennen A ganzabgeschlossen in B, wenn $\bar{A} = A$ gilt. Ist A ein Integritätsbereich, so nennen wir A normal, wenn A ganzabgeschlossen in seinem Quotientenkörper ist.

Satz 10. *$\bar{A}$ ist ein Ring.*

- $b_1, b_2 \in \bar{A} \Rightarrow b_1, b_2$ gü $A \Rightarrow A[b_1, b_2]$ gü $A \Rightarrow$
  $b_1 + b_2, b_1 \cdot b_2, -b_1 \in A[b_1, b_2] \Rightarrow \bar{A}$ abg. unter Mult., Add.
- $\bar{A} \subseteq B$.

$\square$

$K|\mathbb{Q}$ algebraischer Zahlkörper. $K|\mathbb{Q}$ endl. Körpererweiterung.

Definition 11. *Wir definieren den Ring der ganzen Zahlen von K als*

$$\mathcal{O}_K := \mathbb{Z}_K := \{b \in K : b \text{ ganz über } \mathbb{Z}\}.$$

Bemerkung 12. Die bisher definierten quadratischen Zahlringe sind die ganzen Zahlen von $\mathbb{Q}(\sqrt{d})$

$$\mathcal{O}_d = \{b \in \mathbb{Q}(\sqrt{d}) : \operatorname{tr}(b) \in \mathbb{Z}, \mathrm{N}(b) \in \mathbb{Z}\} = \mathcal{O}_{\mathbb{Q}(\sqrt{d})}.$$

3. Spur und Diskriminante

$K|\mathbb{Q}$ alg. Zahlkörper $\Rightarrow$ endl. dim. $\mathbb{Q}$-VR $\Rightarrow$ $v_1, \dots, v_n \in K$ $\mathbb{Q}$-Basis von K.

$v \in K$: $T_v : K \to K$, $x \mapsto vx$, $T_v \in \mathrm{Mat}_{n \times n}(\mathbb{Q})$

Proposition-Definition 13. *Sei $v \in K$, so ist $T_v : K \to K, x \mapsto vx$ $\mathbb{Q}$-linear. Die Abbildung*

$$\mathrm{Tr}_{K/\mathbb{Q}} : K \to \mathbb{Q},\ v \mapsto \mathrm{trace}(T_v)$$

nennen wir Spur und sie ist auch $\mathbb{Q}$-linear.

Bemerkung 14. Die bisher definierte Spur für quadratische Zahlkörper

$$\mathrm{tr} : \mathbb{Q}(\sqrt{d}) \to \mathbb{Q}, a + b\sqrt{d} \mapsto 2a$$

stimmt mit der oben definierten Spur überein.

Proposition 15. *Folgende Abbildung ist eine nicht-ausgeartete $\mathbb{Q}$-Bilinearform*

$$\beta : K \times K \to \mathbb{Q}, (v, w) \mapsto \mathrm{Tr}_{K/\mathbb{Q}}(vw)$$

Definition 16. *Sei $v_1, \dots, v_n \in K$ eine $\mathbb{Q}$-Basis von K, so definieren wir*

$$d(v_1, \dots, v_n) := \det\left(\underbrace{(\beta(v_i, v_j))_{ij}}_{M \in \mathrm{Mat}_{n \times n}(\mathbb{Q})}\right)$$

als die Diskriminante der Basis.

· Bemerkung:

Man kann zeigen, dass $K = \{\frac{b}{a} : b \in \mathcal{O}_K, a \in \mathbb{Z}, a \neq 0\}$ (Übung).

$v_1, \dots, v_n \in K$ $\mathbb{Q}$-Basis K $\Rightarrow$ $v_i = \frac{b_i}{a_i}$ $\Rightarrow$ $b_1, \dots, b_n \in \mathcal{O}_K$ bilden eine $\mathbb{Q}$-Basis. (Übung).

$v_1, \dots, v_n$ $\mathbb{Q}$-Basis $w_1, \dots, w_n$ $\mathbb{Q}$-Basis

$$\boxed{d(v_1, \dots, v_n) = \det(T)^2 d(w_1, \dots, w_n)}$$

Lemma 18. *Sei $b_1, ..., b_n$ eine in $\mathcal{O}_K$ gelegene $\mathbb{Q}$-Basis von K und d die Diskriminante, so gilt*

$$d\mathcal{O}_K \subseteq \mathbb{Z}b_1 + ... + \mathbb{Z}b_n.$$

- $b \in \mathcal{O}_K \Rightarrow b = \sum_{j=1}^{n} l_j b_j$, $l_i \in \mathbb{Q}$: $\beta(b_i, b) = \sum_{j=1}^{n} l_j \beta(b_i, b_j)$
- $$\underbrace{\begin{pmatrix} \beta(b_1, b) \\ \vdots \\ \beta(b_n, b) \end{pmatrix}}_{=: e} = \underbrace{\begin{pmatrix} \beta(b_1, b_1) & \cdots & \beta(b_1, b_n) \\ \vdots & & \vdots \\ \beta(b_n, b_1) & \cdots & \beta(b_n, b_n) \end{pmatrix}}_{=: M} \cdot \underbrace{\begin{pmatrix} l_1 \\ \vdots \\ l_n \end{pmatrix}}_{= l}$$
- Neukirch: $\beta(b_i, b_j)$, $\beta(b_i, b) \in \mathbb{Z} \Rightarrow e, M$ haben Einträge in $\mathbb{Z}$, $\det(M) \neq 0$
- Cramersche Regel: $l_i = \frac{c_i}{\underbrace{\det(M)}_{= d}}$ für passende $c_i \in \mathbb{Z}$, $\det(M) = d$

$$\Rightarrow \quad db = \sum_{j=1}^{n} d l_j b_j = \sum_{j=1}^{n} c_j b_j \in \mathbb{Z}b_1 + ... + \mathbb{Z}b_n \Rightarrow d\mathcal{O}_K \subseteq \mathbb{Z}b_1 + ... + \mathbb{Z}b_n. \quad \square$$

Satz 19. *$\mathcal{O}_K$ besitzt eine endliche $\mathbb{Z}$-Basis mit* $\mathrm{Rang}(\mathcal{O}_K) = [K : \mathbb{Q}]$.

$d\mathcal{O}_K \subseteq \mathbb{Z}b_1 + ... + \mathbb{Z}b_n =: M \Rightarrow M, d\mathcal{O}_K$ $\mathbb{Z}$-Module, M frei

Lemma 5. *Ist A ein Hauptidealring und M frei, so ist jeder A-Untermodul $N \subseteq M$ frei und es gilt*

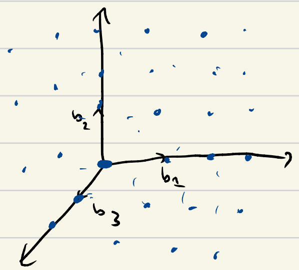
$$\mathrm{Rang}(N) \leqslant \mathrm{Rang}(M).$$

$\Rightarrow d\mathcal{O}_K$ freier $\mathbb{Z}$-Modul $\Rightarrow \mathcal{O}_K$ freier $\mathbb{Z}$-Modul. $\square$

Korollar 20. *Ist $b_1, ..., b_n \in \mathcal{O}_K$ eine $\mathbb{Z}$-Basis von $\mathcal{O}_K$, so ist $b_1, ..., b_n$ eine $\mathbb{Q}$-Basis von K.*

Vorstellung:

K



4. Noethersch

Definition 21. *B heisst noethersch, falls jede aufsteigende Folge von Idealen*

$$B_0 \subseteq B_1 \subseteq \dots$$

stationär wird, d.h. es existiert ein $n \geqslant 0$ mit $B_n = B_i$ für alle $i \geqslant n$.

Lemma 22. *Ist B/I endlich für jedes Ideal $I \neq 0$, so ist B noehtersch.*

- $B_0 \subseteq B_1 \subseteq \dots \Rightarrow B_0/B_0 \subseteq B_1/B_0 \subseteq \dots \subseteq B/B_0 \leftarrow$ Endlich

$\Rightarrow \exists n : B_n/B_0 = B_i/B_0 \ \forall i \geq n \Rightarrow B_n = B_i \ \forall i \geq n.$ $\square$

Satz 23. *$\mathcal{O}_K$ ist noehtersch.*

- $0 \neq I \subseteq \mathcal{O}_K \Rightarrow \underline{I \cap \mathbb{Z} \neq \emptyset}$ da: $a \in I \cap \mathbb{Z}$.

$a\mathcal{O}_K \subseteq I$

- $a \in I \cap \mathbb{Z} \Rightarrow \boxed{\mathcal{O}_K / I} \hookrightarrow \boxed{\mathcal{O}_K / a\mathcal{O}_K}$, $b + I \mapsto b + a\mathcal{O}_K$.

Zeige $\mathcal{O}_K/a\mathcal{O}_K$ ist endlich:

$\mathcal{O}_K$ hat eine $\mathbb{Z}$-Basis $\Rightarrow \mathcal{O}_K \simeq \mathbb{Z}^n$ abelsche Gruppen $\Rightarrow$

$$\mathcal{O}_K / a\mathcal{O}_K \simeq \mathbb{Z}^n / a\mathbb{Z}^n \simeq \underline{\mathbb{Z}/a\mathbb{Z}} \oplus \dots \oplus \underline{\mathbb{Z}/a\mathbb{Z}}$$

$\Rightarrow \mathcal{O}_K/a\mathcal{O}_K$ endlich $\Rightarrow \mathcal{O}_K$ noethersch. $\square$

5. Dedekindringe

Definition 24. *Ein noetherscher, normaler Integritätsbereich, bei dem jedes von Null verschiedene Primideal ein Maximalideal ist, nennen wir Dedekindring.* $\mathcal{O}$

Satz 23. *$\mathcal{O}_K$ ist ein Dedekindring.*

- noethersch: ✓
- normal: ✓

Lemma 8. *Seien $A \subseteq B \subseteq C$ Ringe, C ganz über B und B ganz über A, so ist C ganz über A.*

- Primideale sind maximal:

$0 \neq \mathfrak{p} \leq \mathcal{O}_K$ Primideal, zeige $\mathcal{O}_K / \mathfrak{p}$ ist ein Körper.

Lemma 25. *Ist B ganz über A, so ist B ein Körper genau dann, wenn A ein Körper ist.*

- $\mathbb{Z} \cap \mathfrak{p}$ Primideal in $\mathbb{Z}$ $\Rightarrow$ $\mathbb{Z} \cap \mathfrak{p} = p\mathbb{Z}$ $\Rightarrow$ $\mathbb{Z}/p\mathbb{Z}$ Körper.

$\mathbb{Z}/p\mathbb{Z} \hookrightarrow \mathcal{O}_K/\mathfrak{p}$, $a + p\mathbb{Z} \longmapsto a + \mathfrak{p}$ inj. Hom.

$\underline{\mathcal{O}_K/\mathfrak{p}}$ ganz über $\underbrace{\mathbb{Z}/p\mathbb{Z}}_{\text{Körper}}$ (da $\mathcal{O}_K$ ganz über $\mathbb{Z}$).

$\Rightarrow \mathcal{O}_K/\mathfrak{p}$ Körper $\Rightarrow$ $\mathfrak{p}$ maximal. $\square$