DEDEKINDRINGE

BENJAMIN REINHARD

In den folgenden Seiten wollen wir die Dedekindringe einführen, welche eine Grundlage für die Faktorisierung von Idealen bilden. Bis dahin müssen wir erstmals unsere Kenntnisse über die Ganzheit ausbauen und dafür werden Module nützlich sein, welche in Kommutativer Algebra sehr genau behandelt werden.

Unsere wichtigste Anwendung dieser Theorie ist beim Ring der ganzen Zahlen eines algebraischen Zahlkörpers. Wir wollen letztendlich zeigen, dass dieser ein Dedekindring ist und dafür müssen wir die bisher bekannten Werkzeuge Spur und Diskriminante auf allgemeine algebraische Zahlkörper erweitern.

1. Module

In diesem Abschnitt führen wir Module ein. Sie stellen eine Verallgemeinerung der Vektorräume dar und die meisten Eigenschaften lassen sich auch übertragen. Die Aussagen werden wir aber nicht beweisen, man findet sie ganz einfach in Textbüchern auf dem Internet.

Sei A ein Ring. Man sollte sich $\mathbb{Z}$ als zentrales Beispiel vorstellen.

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.*
- $(a_1 a_2) \cdot m = a_1 \cdot (a_2 \cdot m)$
- $(a_1 + a_2) \cdot m = a_1 \cdot m + a_2 \cdot m$
- $a \cdot (m_1 + m_2) = a \cdot m_1 + a \cdot m_2$
- $1 \cdot m = m$

Beispiel 2.

(1) Jeder K-Vektorraum ist ein K-Modul.
(2) Seien $A \subseteq B$ Ringe, so ist B ein A-Modul via $\cdot : A \times B \to B, (a, b) \mapsto ab$.

Sei M ein 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 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.

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 von nun an durchgehend $A \subseteq B$ Ringe.

Lemma 6. *Folgende Aussagen sind äquivalent:*

(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.*

Beweis. (1) $\Rightarrow$ (2) ist klar, da $b_1, ..., b_n \in A[b_1, ..., b_n]$. Die Implikation (2) $\Rightarrow$ (3) überlasse ich dem/der Leser/in als Aufgabe. Ansonsten findet man die Lösung im Buch von Neukirch [1, Satz I.2.2]. Wir zeigen nun (3) $\Rightarrow$ (1). Sei $A[b_1, ..., b_n]$ endlich erzeugt, das heisst

$$A[b_1, ..., b_n] = A\omega_1 + ... + \omega_m \text{ für geeignete } \omega_i \in A[b_1, ..., b_n]$$

Sei nun $c \in A[b_1, ..., b_n]$ beliebig, wir zeigen, dass es ganz über A ist. Seien $a_{ij} \in A$, sodass $c\omega_i = \sum_{j=1}^m a_{ij}\omega_i$, $M(x)$ die Matrix mit Einträgen $x\delta_{ij} - a_{ij} \in A[x]$ und $f(x) = \det(M(x)) \in A[x]$ ein nicht-konstantes normiertes Polynom.

Eine Folgerung der Cramerschen Regel liefert uns eine Matrix $N(x) \in \mathrm{Mat}_{m\times m}(A)$ mit

$$N(x)M(x) = \det(M(x))I_m$$

und für $\omega = (\omega_1, ..., \omega_m)^T$ kann man nachrechnen, dass $M(c)\omega = 0$ gilt, also ist mit der obigen Gleichung

$$\omega_i \det(M(c)) = 0 \text{ für alle } i.$$

Da schliesslich $1 \in A[b_1..., b_n]$ gilt, existieren $d_i \in A$, sodass $1 = \sum_{j=1}^m d_i\omega_i$ und daraus folgt $f(c) = 1 \cdot \det(M(c)) = \sum_{j=1}^m d_i\omega_i \det(M(c)) = 0$. Also ist c ganz über A. □

Lemma 7. *Seien* $A \subseteq B \subseteq C$ *Ringe,* C *ganz über* B *und* B *ganz über* A*, so ist* C *ganz über* A.

Beweis. Sei $c \in C$ so existiert ein $f \in B[x]$ mit $f(c) = c^n + b_{n-1}c^{n-1}... + b_0 = 0$ und somit ist c ganz über $R = A[b_{n-1}, ..., b_0]$. Da nun $b_{n-1}, ..., b_0$ ganz über A sind, ist wegen Lemma 6 R ein endlich erzeugter A-Modul und auch $R[c]$ ein endlich erzeugter R-Modul. Daraus kann man einfach schliessen, dass $R[c] = A[b_{n-1}, ..., b_0, c]$ ein endlich erzeugter A-Modul ist und somit wieder wegen Lemma 6 c ganz über A ist. □

Satz 8. *Der ganze Abschluss* $\bar{A}$ *von* A *in* B *ist ein Ring.*

Beweis. Es ist klar, dass $0, 1 \in \bar{A}$ gilt. Seien nun $b_1, b_2 \in \bar{A}$, so ist laut Lemma 6 $A[b_1, b_2]$ ganz über A und da $b_1 + b_2, -b_1, b_1b_2 \in A[b_1, b_2]$, so sind $b_1 + b_2, -b_1, b_1b_2$ ganz über A, also liegen sie in $\bar{A}$. Alle restlichen Ringeigenschaften folgen aus $\bar{A} \subseteq B$. □

Wir betrachten kurz unser zentrales Beispiel. Sei von nun an $K/\mathbb{Q}$ ein algebraischer Zahlkörper.

Definition 9. *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 10. Die bisher definierten quadratischen Zahlringe sind die ganzen Zahlen von $\mathbb{Q}(\sqrt{d})$

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

Sei $b \in \mathcal{O}_d$, so ist b die Nullstelle des Polynoms $x^2 - \mathrm{tr}(b)x + \mathrm{N}(b)$, wobei die Koeffizienten per Voraussetzung in $\mathbb{Z}$ liegen. Also liegt b in $\mathcal{O}_{\mathbb{Q}(\sqrt{b})}$.

Umgekehrt ist $b = x + \sqrt{d}y \in \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$, so existiert ein nicht-konstantes, normiertes Polynom $f \in \mathbb{Z}[x]$ mit $f(b) = 0$. Es gilt $f(x - \sqrt{d}y) = f(\bar{b}) = \overline{f(b)} = 0$, also ist $\bar{b}$ auch in $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ und da $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ ein Ring ist, ist $\mathrm{tr}(b) = b + \bar{b} = 2x, \mathrm{N}(b) = b\bar{b} = x^2 + y^2$ in $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$. Also sind $\mathrm{tr}(b), \mathrm{N}(b)$ ganz über $\mathbb{Z}$ und liegen offensichtlich in $\mathbb{Q}$. Es ist nun dem/der Leser/in überlassen zu zeigen, dass $\mathcal{O}_{\mathbb{Q}(\sqrt{d})} \cap \mathbb{Q} = \mathbb{Z}$ gilt. Daraus schliessen wir, dass $\mathrm{tr}(b)$ und $\mathrm{N}(b)$ tatsächlich in $\mathbb{Z}$ liegen und somit b in $\mathcal{O}_d$.

3. Spur und Diskriminante

Da $\mathbb{Z} \subseteq \mathcal{O}_K$ gilt, können wir $\mathcal{O}_K$ als $\mathbb{Z}$-Modul auffassen. Genauso können wir K als $\mathbb{Q}$-Vektorraum auffassen und da er per Definition endlich ist, besitzt er eine endliche $\mathbb{Q}$-Basis. Unser nächstes grosses Ziel ist es zu zeigen, dass $\mathcal{O}_K$ eine endliche $\mathbb{Z}$-Basis besitzt.

Proposition-Definition 11. *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.

Der Beweis ist nicht schwierig und ist dem/der Leser/in überlassen.

Bemerkung 12. 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 13. *Folgende Abbildung ist eine nicht-ausgeartete $\mathbb{Q}$-Bilinearform*

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

Dies ist ebenfalls nicht schwierig zu beweisen.

Definition 14. *Sei $v_1, ..., v_n \in K$ eine $\mathbb{Q}$-Basis von K, so definieren wir*

$$d(v_1, ..., v_n) := \det\left((\beta(v_i, v_j))_{ij}\right)$$

als die Diskriminante der Basis.

Bemerkung 15. Man kann zeigen, dass $K = (\mathbb{Z}\backslash\{0\})^{-1}\mathcal{O}_K$ gilt, also jedes Element von K dargestellt werden kann als $\frac{b}{a}$, wobei $b \in \mathcal{O}_K$ und $a \in \mathbb{Z}\backslash\{0\}$ liegt. Ist also $v_1 = \frac{b_1}{a_1}, ..., v_n = \frac{b_n}{a_n}$ eine $\mathbb{Q}$-Basis von K, so ist es leicht zu sehen, dass $b_1, ..., b_n$ auch eine $\mathbb{Q}$-Basis von K.

Lemma 16. *Sei $b_1, ..., b_n$ eine in $\mathcal{O}_K$ gelegene $\mathbb{Q}$-Basis von K und d die Diskriminante, so gilt*

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

Beweis. Sei $b \in \mathcal{O}_K$ mit $b = \sum_{i=1}^n \lambda_i b_i$ für $\lambda_i \in \mathbb{Q}$, so gilt $\beta(b_i, b) = \sum_{j=1}^n \beta(b_i, b_j)\lambda_j$ und somit

$$(\beta(b_1, b), ..., \beta(b_n, b))^T = M(\lambda_1, ..., \lambda_n)^T$$

wobei $M = (\beta(b_i, b_j))_{ij}$ ist. Im Buch von Neukirch [1] auf Seite 12 wird erklärt, dass wenn b ganz über $\mathbb{Z}$ ist, so ist $\mathrm{Tr}_{K/\mathbb{Q}}(b)$ in $\mathbb{Z}$ und daraus folgt, dass e und M Einträge in $\mathbb{Z}$ haben. Neukirch erklärt auch in [1, Satz I.2.8], dass $\det(M) = d \neq 0$ und somit können wir die Cramersche Regel anwenden, um geeignete $a_i \in \mathbb{Z}$ mit $\lambda_i = \frac{a_i}{d}$ zu erhalten, also $d\lambda_i = a_i$. Dies ergibt

$$db = \sum_{i=1}^n d\lambda_i b_i = \sum_{i=1}^n a_i b_i \in \mathbb{Z}b_1 + ... + \mathbb{Z}b_n.$$

□

Satz 17. *$\mathcal{O}_K$ besitzt eine endliche $\mathbb{Z}$-Basis mit* $\mathrm{Rang}(\mathcal{O}_K) = [K : \mathbb{Q}]$.

Beweis. Seien $b_1, ..., b_n$ und d wie im Lemma 16, so kann man einfach überprüfen, dass $M := \mathbb{Z}b_1 + ... + \mathbb{Z}b_n$ ein freier $\mathbb{Z}$-Modul ist mit $\mathrm{Rang}(M) = n$. Nun ist $d\mathcal{O}_K$ auch ein $\mathbb{Z}$-Modul mit $d\mathcal{O}_K \subseteq M$ und $\mathbb{Z}$ ein Hauptidealring, so erhalten wir aus Lemma 5, dass $d\mathcal{O}_K$ ein freier $\mathbb{Z}$-Modul ist mit $m = \mathrm{Rang}(d\mathcal{O}_K) \leqslant n$.

Sei $de_1, ..., de_m \in d\mathcal{O}_K$ eine $\mathbb{Z}$-Basis von $d\mathcal{O}_K$, so ist offensichtlich $e_1, ..., e_n \in \mathcal{O}_K$ eine $\mathbb{Z}$-Basis von $\mathcal{O}_K$.

Letztendlich haben wir $N := \mathbb{Z}b_1 + ... + \mathbb{Z}b_n \subseteq \mathcal{O}_K$ und N ist offensichtlich auch ein freier $\mathbb{Z}$-Modul mit $\mathrm{Rang}(N) = n$, also folgt wieder aus Lemma 5

$$n = \mathrm{Rang}(N) \leqslant \mathrm{Rang}(\mathcal{O}_K) = m \leqslant \mathrm{Rang}(M) = n$$

und somit $\mathrm{Rang}(\mathcal{O}_K) = m = n = [K : \mathbb{Q}]$. □

Korollar 18. *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.*

Beweis. Wir zeigen zuerst, dass $b_1 ..., b_n$ $\mathbb{Q}$-linear unabhängig sind. Sei also $\sum_{i=1}^n \frac{p_i}{q_i} b_i = 0$, so erhält man durch Umformen $c \sum_{i=1}^n c_i p_i b_i = 0$, wobei $c = \prod_{j=1}^n q_j$ und $c_i = \prod_{j \neq i} q_j$ ist. Da c nicht Null ist, muss $\sum_{i=1}^n c_i p_i b_i = 0$ sein und somit $c_i p_i = 0$ für alle i, da $b_1, ..., b_n$ $\mathbb{Z}$-linear unabhängig sind. Nun wegen $c_i \neq 0$ für alle i erhält man $p_i = 0$ und somit sind alle $\frac{p_i}{q_i}$ Null.

Also sind $b_1, ..., b_n$ $\mathbb{Q}$-linear unabhängig mit $n = [K : \mathbb{Q}]$. Aus der linearen Algebra wissen wir, dass $b_1 ..., b_n$ deswegen erzeugend sind und somit eine $\mathbb{Q}$-Basis bilden. □

4. Noethersch

Wir wollen kurz zeigen, dass $\mathcal{O}_K$ noethersch ist.

Lemma 19. *Ist B/I endlich für jedes Ideal $I \neq 0$, so ist B noehtersch.*

Beweis. Sei $B_0 \subseteq B_1 \subseteq ...$ eine aufsteigende Folge von Idealen in B, so ist auch $B_0/B_0 \subseteq B_1/B_0 \subseteq ...$ eine aufsteigende Folge in B/B_0 und da B/B_0 endlich ist, muss es ein n geben mit $B_i/B_0 = B_n/B_0$ für alle $i \geqslant n$ und somit auch $B_i = B_n$. □

Satz 20. *$\mathcal{O}_K$ ist noehtersch.*

Beweis. Sei $I \subseteq \mathcal{O}_K$ ein Ideal ungleich Null. Wir zeigen zuerst, dass $I \cap \mathbb{Z} \supsetneq 0$ gilt. Da I nicht Null ist, haben wir $0 \neq b \in I \subseteq \mathcal{O}_K$ und somit ist b ganz über $\mathbb{Z}$, also existiert ein $f \in \mathbb{Z}[x]$ mit $f(b) = b^n + ... + a_0 = 0$. Falls a_0 nicht Null ist, sieht man anhand der Gliechung, dass es in I liegen muss. Ansonsten ist es einfach zu folgern, dass ein anderes a_i in I liegen muss.

Sei nun $a \in I \cap \mathbb{Z}$, so gilt $a\mathcal{O}_K \subseteq I$ und somit $\mathcal{O}_K/I \subseteq \mathcal{O}_K/a\mathcal{O}_K$. Nun wir wissen, dass $\mathcal{O}_K$ eine $\mathbb{Z}$-Basis besitzt, also gilt $\mathcal{O}_K \simeq \mathbb{Z}^n$ als abelsche Gruppen, sowie auch $a\mathcal{O}_K \simeq a\mathbb{Z}^n$. Wir erhalten

$$\mathbb{Z}^n/a\mathbb{Z}^n \simeq \mathbb{Z}/a\mathbb{Z} \oplus ... \oplus \mathbb{Z}/a\mathbb{Z}$$

und daraus folgt, dass $\mathbb{Z}^n/a\mathbb{Z}^n$ endlich ist und somit auch $\mathcal{O}_K/I$. Wegen Lemma 19 folgt der Satz. □

5. Dedekindringe

Wir sind jetzt soweit, die Dedekindringe einzuführen.

Definition 21. *Ein noetherscher, normaler Integritätsbereich, bei dem jedes von Null verschiedene Primideal ein Maximalideal ist, nennen wir Dedekindring.*

Lemma 22. *Ist B ganz über A, so ist B ein Körper genau dann, wenn A ein Körper ist.*

Beweis. Sei B ein Körper, so reicht es zu zeigen, dass jedes Element in A ein multiplikatives Inverses in A besitzt. Sei also $a \in A$, so ist $a^{-1} \in B$. Da B ganz über A ist, existiert ein normiertes Polynom $f \in A[x]$ mit $f(a^{-1}) = (a^{-1})^n + ... + a_0 = 0$. Durch Umformen erhält man

$$a(-a_0 a^{n-1} - ... - a_{n-1}) = 1.$$

Also gilt $a^{-1} = (-a_0 a^{n-1} - ... - a_{n-1}) \in A$. Umgekehrt sei A ein Körper. Es reicht zu zeigen, dass jedes Element in B ein multiplikatives Inverses besitzt. Sei also $b \in B$, so existiert ein normiertes Polynom $f \in A[x]$ mit $f(b) = b^n + ... + a_0 = 0$. Durch Umformen erhält man

$$b(b^{n-1} + ... + a_1)(-a_0^{-1}) = 1.$$

Man bemerke, dass a_0^{-1} existiert, da A ein Körper ist. Also gilt $b^{-1} = (b^{n-1} + ... + a_1)(-a_0^{-1})$. □

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

Beweis. Noethersch wurde in Satz 20 gezeigt. Wir zeigen Nomralität. Sei $E \subseteq K$ der Quotientenkörper von $\mathcal{O}_K$ und C der ganze Abschluss von $\mathcal{O}_K$ in E, so ist offensichtlich C ganz über $\mathcal{O}_K$ und per Definition $\mathcal{O}_K$ ganz über $\mathbb{Z}$. Also folgt aus Lemma 7, dass C ganz über $\mathbb{Z}$ ist und somit $C \subseteq \mathcal{O}_K$. Die andere Inklusion ist klar.

Nun sei $\mathfrak{p} \subseteq \mathcal{O}_K$ ein von Null verschiedenes Ideal. Wir zeigen, dass $\mathcal{O}_K/\mathfrak{p}$ ein Körper ist, woraus folgt, dass $\mathfrak{p}$ maximal ist. $\mathfrak{p} \cap \mathbb{Z}$ ist ein Primideal in $\mathbb{Z}$ und deswegen von der Form $\mathbb{Z}/p\mathbb{Z}$ für ein Primelement $p \in \mathbb{Z}$. Wir können $\mathbb{Z}/p\mathbb{Z}$ ganz einfach in $\mathcal{O}_K/\mathfrak{p}$ einbetten mit folgender Abbildung

$$\mathbb{Z}/p\mathbb{Z} \hookrightarrow \mathcal{O}_K/\mathfrak{p},\ z + p\mathbb{Z} \mapsto z + \mathfrak{p}$$

und es ist auch nicht schwierig zu zeigen, dass $\mathcal{O}_K/\mathfrak{p}$ ganz über $\mathbb{Z}/p\mathbb{Z}$ ist. Da nun $\mathbb{Z}/p\mathbb{Z}$ ein Körper ist, folgt nach Lemma 22, dass $\mathcal{O}_K/\mathfrak{p}$ ein Körper ist. □

References

[1] J. Neukirch, *Algebraische Zahlentheorie*. Springer-Verlag, Berlin, 1992

Email address: breinhar@student.ethz.ch