Hauptidealring

In der Algebra, einem Teilgebiet der Mathematik, bezeichnet man Integritätsringe als **Hauptidealringe** oder **Hauptidealbereiche**, wenn jedes Ideal ein Hauptideal ist. Die wichtigsten Beispiele für Hauptidealringe sind der Ring der ganzen Zahlen sowie Polynomringe in einer Unbestimmten über einem Körper. Der Begriff des Hauptidealrings erlaubt es, Aussagen über diese beiden Spezialfälle einheitlich zu formulieren. Beispiele für Anwendungen der allgemeinen Theorie sind die Jordansche Normalform, die Partialbruchzerlegung oder die Strukturtheorie endlich erzeugter abelscher Gruppen

Inhaltsverzeichnis

Definition

Ein Integritätsring A (d. h. ein nullteilerfreier kommutativer Ring mit $1 \neq 0$) heißt **Hauptidealring**, wenn jedes Ideal $I \subseteq A$ ein Hauptideal ist, d. h. es gibt ein $x \in A$, so dass $I = A \cdot x = \{a \cdot x \mid a \in A\}$.

Im Folgenden sei A ein Hauptidealring und K sein Quotientenkörper. Außerdem sei $P \subset A$ eine Menge, die für jedes irreduzible $p \in A$ genau ein zu p assoziiertes Element enthält. Im Fall $A = \mathbb{Z}$ ist die Menge der (positiven) Primzahlen ein solches P, im Fall $A = k[T]$ für einen Körper k die Menge der irreduziblen Polynome mit Leitkoeffizient 1.

Beispiele, Folgerungen und Gegenbeispiele

Die folgenden Ringe sind Hauptidealringe:

- Körper
- $\mathbb{Z}$ (der Ring der ganzen Zahlen)
- $\mathbb{Z}[i]$ (der Ring der ganzen gaußschen Zahlen)
- Polynomringe $k[T]$ in einer Unbestimmten über einem Körper k
- formale Potenzreihenringe $k[[T]]$ in einer Unbestimmten über einem Körper k
- diskrete Bewertungsringe
- euklidische Ringe (diese Klasse umfasst zwar alle vorstehenden Beispiele, aber nicht jeder Hauptidealring ist euklidisch)

- Lokalisierungen von Hauptidealringen sind wieder Hauptidealringe.
- Der Ganzheitsring des Körpers $\mathbb{Q}(\sqrt{-3})$, d. h. der Ring der Eisenstein-Zahlen ist ein Hauptidealring. Es gilt sogar die folgende Aussage: Der Ganzheitsring eines quadratischen Zahlkörpers $K = \mathbb{Q}(\sqrt{d})$ mit negativem, quadratfreiem $d \in \mathbb{Z}$ ist genau dann ein Hauptidealring, wenn $d \in \{-1, -2, -3, -7, -11, -19, -43, -67, -163\}$. Der Beweis beruht auf der Untersuchung der Idealklassengruppe, welche bei Zahlkörpern als Maß dafür gesehen werden kann, wie weit ein Ring davon entfernt ist, ein Hauptidealring zu sein.

Hauptidealringe gehören zu den folgenden allgemeineren Klassen von Ringen:

- faktorielle Ringe.[1] Insbesondere gelten:
  - Ein Element $a \in A \setminus \{0\}$ ist genau dann prim, wenn es irreduzibel ist.
  - Jedes Element ungleich null des Quotientenkörpers von A lässt sich auf eindeutige Weise in der Form

    $$u \cdot \prod_{p \in P} p^{e_p}$$

    mit ganzen Zahlen e_p und einer Einheit $u \in A^\times$ schreiben.
  - Das Lemma von Gauß: Jedes irreduzible Element in $A[X]$ ist entweder ein irreduzibles Element von A (aufgefasst als konstantes Polynom) oder ein in $K[X]$ irreduzibles Polynom, dessen Koeffizienten teilerfremd sind.[2]
- Hauptidealringe sind trivialerweise noethersche Ringe, da jedes Ideal endlich erzeugt ist (von einem Element).
- Hauptidealringe sind stets Dedekind-Ringe (siehe auch unten)

Keine Hauptidealringe sind:

- Der Polynomring $\mathbb{Z}[X]$ über den ganzen Zahlen ist kein Hauptidealring, da das von 2 und X erzeugte Ideal nicht durch ein einzelnes Polynom erzeugt werden kann. Dieser Ring ist aber nach dem erwähnten Lemma von Gauß faktoriell, da er ein Polynomring über einem faktoriellen Ring ist.
- Der Ring $k[x, y]$ ist kein Hauptidealring, da das Ideal (x, y) kein Hauptideal ist.
- Der Ring $\mathbb{Z}/4\mathbb{Z}$ ist kein Hauptidealring, da er kein Integritätsring ist. Aber jedes Ideal in diesem Ring ist ein Hauptideal.

Teilbarkeit

- Der (bis auf Assoziiertheit eindeutige) größte gemeinsame Teiler von Elementen $x_1, \ldots, x_m$ ist der (bis auf Assoziiertheit eindeutige) Erzeuger des Ideals $(x_1, \ldots, x_m)$. Insbesondere gilt das *Lemma von Bézout*: Es existieren $a_1, \ldots, a_m \in A$ mit

  $$\operatorname{ggT}(x_1, \ldots, x_m) = a_1 x_1 + \cdots + a_m x_m.$$

  Spezialfall: $x_1, \ldots, x_k$ sind genau dann teilerfremd, wenn es $a_1, \ldots, a_m$ gibt mit

  $$1 = a_1 x_1 + \cdots + a_m x_m.$$
- Das kleinste gemeinsame Vielfache von $x_1, \ldots, x_m$ ist der Erzeuger des Ideals $(x_1) \cap \ldots \cap (x_m)$.
- Chinesischer Restsatz: Sind $x_1, \ldots, x_m$ paarweise teilerfremd, so ist der kanonische Ringhomomorphismus

  $$A/(x_1 \cdots x_m) \to \prod_{i=1}^{m} A/(x_i)$$

  ein Isomorphismus.[3]
- Eine Verschärfung des chinesischen Restsatzes ist der *Approximationssatz*: Gegeben seien $x_1, \ldots, x_m \in K$, paarweise verschiedene $p_1, \ldots, p_m \in P$ sowie Zahlen $n_1, \ldots, n_m \in \mathbb{N}$. Dann gibt es ein $x \in K$, das x_i bezüglich p_i in n_i-ter Ordnung approximiert und ansonsten regulär ist, d. h.

$$v_{p_i}(x - x_i) \geq n_i \text{ für } i = 1, \ldots, m$$

und

$$v_p(x) \geq 0 \text{ für } p \in P \setminus \{p_1, \ldots, p_m\}.$$

Dabei bezeichnet $v_p(x) \in \mathbb{Z}$ den Exponenten von p in der Primfaktorzerlegung von x.[4]

- Für $p \in A \setminus \{0\}$ sind äquivalent:
  - p ist irreduzibel
  - p ist ein Primelement
  - (p) ist ein Primideal
  - (p) ist ein maximales Ideal

  Das Nullideal ist ebenfalls ein Primideal, jedoch nur dann maximal, wenn A ein Körper ist.

Hauptidealringe als Dedekind-Ringe

Hauptartikel: Dedekind-Ring

Viele in algebraischer Zahlentheorie und algebraischer Geometrie natürlich auftretende Ringe sind keine Hauptidealringe, sondern gehören einer etwas allgemeineren Klasse von Ringen an, den Dedekind-Ringen. Sie sind die lokalisierte Version der Hauptidealringe, Ideale sind nicht mehr global, sondern nur noch lokal von einem Element erzeugt:

> Ist A ein noetherscher Integritätsbereich, für den der lokale Ring $A_\mathfrak{p}$ für jedes Primideal $\mathfrak{p}$ ein Hauptidealring ist, so heißt A *Dedekind-Ring*.[5]

Die folgenden Eigenschaften gelten für Hauptidealringe, aber auch allgemeiner für Dedekind-Ringe:

- Sie sind entweder Körper oder eindimensional, d. h. jedes Primideal ungleich (0) ist maximal.
- Sie sind ganzabgeschlossen in ihrem Quotientenkörper
- Sie sind regulär.
- Ihre lokalen Ringe sind entweder Körper oder diskrete Bewertungsringe
- der oben genannte Approximationssatz

Ist ein Dedekind-Ring faktoriell oder semilokal, so ist er ein Hauptidealring.[6]

Moduln über Hauptidealringen

Allgemeines

- Untermoduln freier Moduln sind frei.[7]
- Ist M ein endlich erzeugter Modul mit Torsionsuntermodul T, so gibt es einen freien Untermodul $F \subseteq M$, so dass $M = F \oplus T$. Torsionsfreie, endlich erzeugte Moduln sind frei.[8]
- Projektive Moduln sind frei.[9]
- Ein Modul ist injektiv genau dann, wenn er dividierbar ist. Quotienten injektiver Moduln sind injektiv, jeder Modul hat eine injektive Auflösung der Länge 1. Eine explizite injektive Auflösung von A ist[10]

$$0 \to A \to K \to K/A \to 0.$$

Endlich erzeugte Moduln: Elementarteilersatz

Der Elementarteilersatz beschreibt die Struktur einer Zerlegung eines endlich erzeugten Moduls in unzerlegbare Moduln. (Ein Modul M heißt unzerlegbar, wenn es keine Moduln $M_1, M_2 \neq 0$ gibt mit $M \cong M_1 \oplus M_2$.)

Es sei P wie oben ein Vertretersystem der irreduziblen Elemente (bis auf Assoziiertheit). Zu jedem endlich erzeugten Modul M gibt es eindeutig bestimmte nichtnegative ganze Zahlen m_0 und $m_{p,i}$ für $p \in P, i \in \mathbb{N}_{\geq 1}$, von denen fast alle null sind, so dass

$$M \cong A^{m_0} \oplus \bigoplus_{p \in P} \bigoplus_{i \geq 1} (A/(p^i))^{m_{p,i}}.$$

Die Zahlen $m_0, m_{p,i}$ sind durch M eindeutig festgelegt, und die einzelnen Faktoren A bzw. $A/(p^k)$ sind unzerlegbar. Die Ideale (p^i), für die $m_{p,i} \neq 0$ gilt, heißen *Elementarteiler* von M.[11]

Endlich erzeugte Moduln: Invariante Faktoren

Zu jedem endlich erzeugten Modul M gibt es eine endliche Folge $x_1, x_2, \ldots, x_m$ von Elementen von A, die nicht notwendigerweise von null verschieden sind, so dass

- $x_i \mid x_{i+1}$ für $i = 1, 2, \ldots, m-1$
- $M \cong \bigoplus_{i=1}^{m} A/(x_i)$.

Die Ideale (x_i) sind durch M eindeutig bestimmt und heißen die *invarianten Faktoren* von M. Die Elemente x_i sind folglich bis auf Assoziiertheit eindeutig bestimmt.[12]

Zu dieser Aussage über Moduln gibt es zwei konkurrierende Sichtweisen:

- Zu einem Modul M kann man Erzeuger $w_1, \ldots, w_m$ wählen und den Kern $U \subseteq A^m$ des zugehörigen Homomorphismus $A^m \to M$ betrachten.
- Zu einem Untermodul $U \subseteq A^m$ kann man Erzeuger $u_1, \ldots, u_n$ wählen und die $m \times n$-Matrix X mit Einträgen in A betrachten, die den Homomorphismus $A^n \to A^m$ mit Bild U beschreibt.

Umgekehrt ist das Bild einer $m \times n$-Matrix mit Einträgen in A ein Untermodul $U \subseteq A^m$, und der Quotientenmodul $M = A^m/U$ (der Kokern des durch X gegebenen Homomorphismus $A^n \to A^m$) ist ein endlich erzeugter A-Modul.

Für Untermoduln freier Moduln lautet die Aussage:

- Ist F ein freier A-Modul und U ein (ebenfalls freier) Untermodul von F vom Rang r, so gibt es n Elemente $e_1, \ldots, e_r \in F$, die Teil einer Basis von F sind, sowie Elemente $x_1, \ldots, x_r \in A$ mit $x_1 \mid x_2 \mid \cdots \mid x_r$, so dass $x_1 e_1, \ldots, x_r e_r$ eine Basis von U ist. Der von den e_k aufgespannte Teil $F' \subseteq F$ lässt sich invariant als das Urbild des Torsionsuntermoduls von F/U beschreiben. Die Ideale (x_k) sind die Invarianten (wie oben) des Moduls F'/U, evtl. ergänzt um $x_{k+1} = \cdots = x_m = 0$.[13]

Für Matrizen (Smith-Normalform):

- Ist X eine $m \times n$-Matrix von Rang r mit Einträgen in A, so gibt es invertierbare Matrizen $P \in \mathrm{GL}(m, A), Q \in \mathrm{GL}(n, A)$, so dass PXQ folgende Gestalt hat:

$$\begin{pmatrix} x_1 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ 0 & x_2 & \ddots & \vdots & \vdots & & \vdots \\ \vdots & \ddots & \ddots & 0 & \vdots & & \vdots \\ 0 & \cdots & 0 & x_r & 0 & \cdots & 0 \\ 0 & \cdots & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & & & \vdots & \vdots & & \vdots \\ 0 & \cdots & \cdots & 0 & 0 & \cdots & 0 \end{pmatrix}$$

Dabei sind $x_1 \mid x_2 \mid \cdots \mid x_r$ wieder die Invarianten wie oben.[14]

Torsionsmoduln

Es sei M ein (nicht notwendigerweise endlich erzeugter) Torsionsmodul über A, d. h. für jedes $m \in M$ existiert ein $a \in A \setminus \{0\}$ mit $am = 0$. Wieder sei $P \subset A$ ein Vertretersystem der irreduziblen Elemente. Dann gilt:[15] M ist die direkte Summe der p-primären Untermoduln $M_{(p)}$, d. h.

$$M = \bigoplus_{p \in P} M_{(p)}$$

mit

$$M_{(p)} = \left\{ m \in M \mid p^i m = 0 \text{ für ein } i \in \mathbb{N} \right\}.$$

Als Korollar ergibt sich, dass M genau dann halbeinfach ist, wenn $p \cdot M_{(p)} = 0$ für alle $p \in P$.[16]

Anwendungsbeispiele:

- Ist $A = \mathbb{Z}$ und $M = K/A = \mathbb{Q}/\mathbb{Z}$, so lautet die Aussage: Jede rationale Zahl besitzt eine eindeutige Darstellung

  $$a + \sum_{p \text{ prim}} \sum_{i=1}^{o_p} d_{p,i} p^{-i}$$

  mit $a \in \mathbb{Z}$, $o_p \geq 0$ (und fast alle $o_p = 0$) sowie $d_{p,i} \in \{0, 1, \ldots, p-1\}$ und $d_{p,o_p} \neq 0$.[17]

- Ist $A = k[T]$ (k ein Körper) und $M = K/A = k(T)/k[T]$, so entspricht $M_{(p)}$ den rationalen Funktionen, deren Nenner eine Potenz von p ist. Der Satz liefert also den ersten Schritt der Partialbruchzerlegung d. h. der eindeutigen Darstellung einer rationalen Funktion als

  $$a + \sum_{p} \sum_{i=1}^{o_p} d_{p,i} p^{-i}.$$

  Dabei durchläuft p die irreduziblen normierten Polynome in $k[T]$, die weiteren Komponenten sind der reguläre Anteil $a \in k[T]$, die Ordnungen $o_p \geq 0$ (fast alle $o_p = 0$) und geeignete Polynome $d_{p,i}$ für $i = 1, 2, \ldots, o_p$ mit $\deg(d_{p,i}) < \deg(p)$. Ist insbesondere p linear, so sind die $d_{p,i}$ Konstanten.[18]

- Ist $A = k[T]$ und M ein endlichdimensionaler k-Vektorraum zusammen mit einem Endomorphismus f (mit der A-Modulstruktur $Tv = f(v)$), so ist die obige Zerlegung die Aufspaltung in die Haupträume. Das Korollar besagt in diesem Fall, dass f genau dann halbeinfach ist, wenn das Minimalpolynom von f keine mehrfachen Faktoren enthält.[19]

Verallgemeinerung auf nicht-kommutative Ringe

Die Definitionen lassen sich auf nicht-kommutative Ringe verallgemeinern. Ein Rechts-Hauptideal I ist Rechts-Vielfaches gA eines einzelnen Elements $g \in A$; Ag ist ein Links-Hauptideal. Wie im kommutativen Fall sind $\{0\} = 0A = A0$ und $A = 1A = A1$ die trivialen (und zweiseitigen) Hauptideale.

Die Hurwitzquaternionen sind ein Beispiel für einen nicht-kommutativen Ring, der mit seiner Norm als euklidischer Norm sowohl links- als auch rechtseuklidisch und damit sowohl rechts- wie linksseitig ein Hauptidealring ist.

Verwandte Begriffe

- Wird nur gefordert, dass jedes Ideal endlich erzeugt ist, gelangt man zum Begriff des noetherschen Rings.
- Umgekehrt kann man an einen Integritätsbereich die Bedingung stellen, dass alle endlich erzeugten Ideale Hauptideale sind: Dies sind die sogenannten *Bézoutringe*. Hauptidealringe sind also genau die noetherschen Bézoutringe.
- Manchmal werden auch nicht nullteilerfreie Ringe in der Definition des Begriffs „Hauptidealring“ erlaubt, es wird also nur gefordert, dass jedes Ideal ein Hauptideal ist und $1 \neq 0$.[20] Im Englischen wird hierzu sprachlich zwischen *principal ideal ring* und *principal ideal domain* (*domain* = Integritätsbereich) unterschieden. Die entsprechende Unterscheidung der Begriffe Hauptidealring und Hauptidealbereich ist im Deutschen jedoch unüblich.[21]

Literatur

- Serge Lang: *Algebra.* Revised 3rd edition. Springer, Berlin u. a. 2002, ISBN 0-387-95385-X (*Graduate Texts in Mathematics* 211).
- Nicolas Bourbaki: *Algebra II. Chapters 4–7.* Springer, Berlin u. a. 1990, ISBN 3-540-19375-8 (*Elements of Mathematics*).
- Nicolas Bourbaki: *Eléments de mathématique. Algèbre Commutative* Band 10: *Chapitre 10.* Réimpression de l'édition de 1998. Springer, Berlin u. a. 2007, ISBN 978-3-540-34394-3
- Nicolas Bourbaki: *Commutative Algebra. Chapters 1–7.* 2nd printing. Springer, Berlin u. a. 1989, ISBN 3-540-19371-5 (*Elements of Mathematics*).
- Stefan Müller-Stach, Jens Piontkowski: *Elementare und algebraische Zahlentheorie. Ein moderner Zugang zu klassischen Themen.* Vieweg, Wiesbaden 2006, ISBN 3-8348-0211-5 (*Vieweg Studium*).

Einzelnachweise

1. Lang, Theorem II.5.2, S. 112
2. Lang, Theorem IV.2.3, S. 182
3. Lang, Corollary II.2.2, S. 95
4. Bourbaki, Commutative Algebra, Ch. VII, §2.4, Proposition 2
5. Bourbaki, Commutative Algebra, Ch. VII, §2
6. Stefan Müller-Stach, Jens Piontkowski: *Elementare und algebraische Zahlentheorie*. Vieweg-Verlag, 2006, S. 188. (Satz 18.16)
7. Bourbaki, Algebra, Ch. VII, § 3, Corollary 2; Lang, Theorem III.7.1
8. Bourbaki, Algebra, Ch. VII, § 4, No. 4, Corollary 1 und 2; Lang, Theorem III.7.3
9. Bourbaki, Algebra, Ch. VII, § 3, Corollary 3
10. Bourbaki, Algèbre, Ch. X, § 1, No. 7, Corollaire 2
11. Bourbaki, Algebra, Ch. VII, § 4, No. 8, Proposition 9; Lang, Theorem III.7.5
12. Bourbaki, Algebra, Ch. VII, § 4, No. 4, Theorem 2; Lang, Theorem III.7.7
13. Bourbaki, Algebra, Ch. VII, § 4, No. 3, Theorem 1; Lang, Theorem III.7.8
14. Bourbaki, Algebra, Ch. VII, § 4, No. 6, Corollary 1; Lang, Theorem III.7.9
15. Bourbaki, Algebra, Ch. VII, § 2, No. 2, Theorem 1
16. Bourbaki, Algebra, Ch. VII, § 2, No. 2, Corollary 4
17. Bourbaki, Algebra, Ch. VII, § 2, No. 3, I
18. Bourbaki, Algebra, Ch. VII, § 2, No. 3, II
19. Bourbaki, Algebra, Ch. VII, § 5, No. 8, Proposition 14
20. Lang, II, §1, S. 86
21. Rainer Schulze-Pillot: *Einführung in Algebra und Zahlentheorie*. Springer-Verlag, 2014, ISBN 978-3-642-55216-8, S. 34 (eingeschränkte Vorschau (https://books.google.de/books?id=EsluBAAAQBAJ&pg=PA34#v=onepage) in der Google-Buchsuche).