Prof. Dr. H. Brenner **Osnabrück WS 2024/2025**

Elemente der Algebra

Vorlesung 8

Hauptidealbereiche

Die Summe von Hauptidealen und der Durchschnitt von Hauptidealen ist wieder ein Ideal, aber im Allgemeinen kein Hauptideal. Damit hängt zusammen, dass weder ein größter gemeinsamer Teiler noch ein kleinstes gemeinsames Vielfaches von Elementen $a, b \in R$ existieren muss. Eine besondere Situation liegt daher vor, wenn überhaupt jedes Ideal ein Hauptideal ist. Dies trifft auf $\mathbb{Z}$ und auf $K[X]$ (K ein Körper) zu.

Definition 8.1. Ein kommutativer Ring, in dem jedes Ideal ein Hauptideal ist, heißt *Hauptidealring*. Ein integrer Hauptidealring heißt *Hauptidealbereich*.

Euklidische Bereiche sind Hauptidealbereiche

Satz 8.2. *Ein euklidischer Bereich ist ein Hauptidealbereich.*

Beweis. Es sei I ein von 0 verschiedenes Ideal. Betrachte die nichtleere Menge

$$\{\delta(a) \mid a \in I,\, a \neq 0\}\,.$$

Diese Menge hat ein Minimum m, das von einem Element $b \in I$, $b \neq 0$, herrührt, sagen wir $m = \delta(b)$. Wir behaupten, dass $I = (b)$ ist. Dabei ist die Inklusion „$\supseteq$“ klar. Zum Beweis der Inklusion „$\subseteq$“ sei $a \in I$ gegeben. Aufgrund der Definition eines euklidischen Bereiches gilt $a = qb + r$ mit $r = 0$ oder $\delta(r) < \delta(b)$. Wegen $r \in I$ und der Minimalität von $\delta(b)$ kann der zweite Fall nicht eintreten. Also ist $r = 0$ und a ist ein Vielfaches von b.

□

Die beiden folgenden Sätze folgen direkt aus Satz 8.2, da sowohl $\mathbb{Z}$ als auch $K[X]$ euklidische Bereiche sind. Wir geben zusätzlich noch jeweils einen spezifischen Beweis an.

Satz 8.3. *Ein Polynomring über einem Körperist ein Hauptidealbereich.*

Beweis. Es sei I ein von 0 verschiedenes Ideal in $K[X]$. Betrachte die nichtleere Menge

$$\{\operatorname{grad}(P) \mid P \in I,\, P \neq 0\}\,.$$

Diese Menge hat ein Minimum $m \in \mathbb{N}$, das von einem Element $F \in I$, $F \neq 0$, herrührt, sagen wir $m = \operatorname{grad}(F)$. Wir behaupten, dass $I = (F)$ ist.

Die Inklusion $\supseteq$ ist klar. Zum Beweis von $\subseteq$ sei $P \in I$ gegeben. Aufgrund von Satz 5.3 gilt

$$P = FQ + R \text{ mit } \operatorname{grad}(R) < \operatorname{grad}(F) \text{ oder } R = 0\,.$$

Wegen $R \in I$ und der Minimalität von $\operatorname{grad}(F)$ kann der erste Fall nicht eintreten. Also ist $R = 0$ und P ist ein Vielfaches von F.

□

SATZ 8.4. *Der Ring $\mathbb{Z}$ der ganzen Zahlenist ein Hauptidealbereich.*

Beweis. Zunächst ist $\mathbb{Z}$ ein Integritätsbereich. Es sei $I \subseteq \mathbb{Z}$ ein Ideal. Damit ist I insbesondere eine (additive) Untergruppe von $\mathbb{Z}$ und hat nach Satz 5.2 die Gestalt $I = \mathbb{Z}d$. Damit handelt es sich um ein Hauptideal.

□

Teilbarkeitslehre in Hauptidealbereichen

Die folgende Aussage heißt *Lemma von Bezout*.

SATZ 8.5. *Es sei R ein Hauptidealring. Dann gilt: Elemente $a_1, \ldots, a_n$ besitzen stets einen größten gemeinsamen Teiler d, und dieser lässt sich als Linearkombination der $a_1, \ldots, a_n$ darstellen, d.h. es gibt Elemente $r_1, \ldots, r_n \in R$ mit $r_1a_1 + r_2a_2 + \cdots + r_na_n = d$. Insbesondere besitzen teilerfremde Elemente $a_1, \ldots, a_n$ eine Darstellung der 1.*

Beweis. Sei $I = (a_1, \ldots, a_n)$ das von den Elementen erzeugte Ideal. Da wir in einem Hauptidealring sind, handelt es sich um ein Hauptideal; es gibt also ein Element d mit $I = (d)$. Wir behaupten, dass d ein größter gemeinsamer Teiler der $a_1, \ldots, a_n$ ist. Die Inklusionen $(a_i) \subseteq I = (d)$ zeigen, dass es sich um einen gemeinsamen Teiler handelt. Es sei e ein weiterer gemeinsamer Teiler der $a_1, \ldots, a_n$. Dann ist wieder $(d) = I \subseteq (e)$, was wiederum $e|d$ bedeutet. Die Darstellungsaussage folgt unmittelbar aus $d \in I = (a_1, \ldots, a_n)$. Im teilerfremden Fall ist $I = (a_1, \ldots, a_n) = R$.

□

Die folgende Kurzform wird auch oft als *Lemma von Bezout* bezeichnet.

KOROLLAR 8.6. *Es sei R ein Hauptidealbereichund seien $a, b \in R$ teilerfremde Elemente.Dann kann man die 1 als Linearkombination von a und b darstellen, d.h. es gibt Elemente $r, s \in R$ mit $ra + sb = 1$.*

Beweis. Dies folgt direkt aus

Satz 8.5. □

Die folgende Aussage heißt *Lemma von Euklid*.

Satz 8.7. *Es sei R ein Hauptidealbereich und $a, b, c \in R$. Es seien a und b teilerfremd und a teile das Produkt bc. Dann teilt a den Faktor c.*

Beweis. Da a und b teilerfremd sind, gibt es nach dem Lemma von Bezout Elemente $r, s \in R$ mit $ra + sb = 1$. Die Voraussetzung, dass a das Produkt bc teilt, schreiben wir als $bc = da$. Damit gilt

$$c = c1 = c(ra + sb) = cra + csb = acr + ads = a(cr + ds),$$

was zeigt, dass c ein Vielfaches von a ist.

$\square$

Satz 8.8. *Es sei R ein Hauptidealbereich.Dann ist ein Element genau dann prim,wenn es irreduzibel ist.*

Beweis. Ein Primelement in einem Integritätsbereich ist nach Lemma 6.7 stets irreduzibel. Es sei also umgekehrt p irreduzibel, und nehmen wir an, dass p das Produkt ab teilt, sagen wir $pc = ab$. Nehmen wir an, dass a kein Vielfaches von p ist. Dann sind aber a und p teilerfremd, da eine echte Inklusionskette $(p) \subset (p, a) = (d) \subset R$ der Irreduzibilität von p widerspricht. Damit teilt p nach dem Lemma von Euklid den anderen Faktor b.

$\square$

Lemma 8.9. *In einem Hauptidealbereich lässt sich jede Nichteinheit $a \neq 0$ als ein Produkt von irreduziblen Elementen darstellen.*

Beweis. Angenommen, jede Zerlegung $a = p_1 \cdots p_k$ enthalte nicht irreduzible Elemente. Dann gibt es in jedem solchen Produkt einen Faktor, der ebenfalls keine Zerlegung in irreduzible Faktoren besitzt. Wir erhalten also eine unendliche Kette $a_1 = a, a_2, a_3, \ldots$, wobei a_{n+1} ein nicht-trivialer Teiler von a_n ist. Somit haben wir eine echt aufsteigende Idealkette

$$(a_1) \subset (a_2) \subset (a_3) \subset \cdots .$$

Die Vereinigung dieser Ideale ist aber nach Aufgabe 7.5 ebenfalls ein Ideal und nach Voraussetzung ein Hauptideal. Dies ist ein Widerspruch.

$\square$

Euklidischer Algorithmus

Definition 8.10. Es seien Elemente a, b (mit $b \neq 0$) eines euklidischen Bereichs R mit euklidischer Funktion δ gegeben. Dann nennt man die durch die Anfangsbedingungen $r_0 = a$ und $r_1 = b$ und die mittels der Division mit Rest

$$r_i = q_i r_{i+1} + r_{i+2}$$

rekursiv bestimmte Folge r_i die *Folge der euklidischen Reste*.

Satz 8.11. *Es seien zwei Elemente $r_0 = a, r_1 = b \neq 0$ eines euklidischen Bereiches R mit euklidischer Funktion δ gegeben. Dann besitzt die Folge r_i, $i = 0, 1, 2, \ldots$, der euklidischen Reste folgende Eigenschaften.*

(1) *Es ist $r_{i+2} = 0$ oder $\delta(r_{i+2}) < \delta(r_{i+1})$.*
(2) *Es gibt ein (minimales) $k \geq 2$ mit $r_k = 0$.*
(3) *Es ist*
$$\mathrm{ggT}(r_{i+1}, r_i) = \mathrm{ggT}(r_i, r_{i-1}).$$
(4) *Es sei $k \geq 2$ der erste Index derart, dass $r_k = 0$ ist. Dann ist*
$$\mathrm{ggT}(a, b) = r_{k-1}.$$

Beweis. (1) Dies folgt unmittelbar aus der Definition der Division mit Rest.
(2) Solange $r_i \neq 0$ ist, wird die Folge der natürlichen Zahlen $\delta(r_i)$ immer kleiner, so dass irgendwann der Fall $r_i = 0$ eintreten muss.
(3) Wenn t ein gemeinsamer Teiler von r_{i+1} und von r_{i+2} ist, so zeigt die Beziehung
$$r_i = q_i r_{i+1} + r_{i+2},$$
dass t auch ein Teiler von r_i und damit ein gemeinsamer Teiler von r_{i+1} und von r_i ist. Die Umkehrung folgt genauso.
(4) Dies folgt aus (3) mit der Gleichungskette
$$\mathrm{ggT}(a, b) = \mathrm{ggT}(b, r_2) = \mathrm{ggT}(r_2, r_3) = \ldots = \mathrm{ggT}(r_{k-2}, r_{k-1}) = \mathrm{ggT}(r_{k-1}, r_k) = \mathrm{ggT}(r_{k-1}, 0) =$$
$\square$

Mit dem euklidischen Algorithmus berechnet man also einen größten gemeinsamen Teiler. Indem man die im Algorithmus auftretenden Gleichungen von hinten nach vorne verwendet, erhält man auch eine Darstellung eines größten gemeinsamen Teilers als Linearkombination von a und b.

Abbildungsverzeichnis