Prof. Dr. H. Brenner **Osnabrück SS 2015**

Elemente der Algebra

Vorlesung 7

Ideale

Definition 7.1. Eine nichtleere Teilmenge $\mathfrak{a}$ eines kommutativen Ringes R heißt *Ideal*, wenn die beiden folgenden Bedingungen erfüllt sind:

(1) Für alle $a, b \in \mathfrak{a}$ ist auch $a + b \in \mathfrak{a}$.
(2) Für alle $a \in \mathfrak{a}$ und $r \in R$ ist auch $ra \in \mathfrak{a}$.

Die Eigenschaft, nichtleer zu sein, kann man durch die Bedingung $0 \in \mathfrak{a}$ ersetzen. Ein Ideal ist eine Untergruppe der additiven Gruppe von R, die zusätzlich unter Skalarmultiplikation abgeschlossen ist.

Definition 7.2. Zu einer Familie von Elementen $a_1, a_2, \ldots, a_n \in R$ in einem kommutativen Ring R bezeichnet $(a_1, a_2, \ldots, a_n)$ das von diesen Elementen *erzeugte Ideal*. Es besteht aus allen *Linearkombinationen*

$$r_1a_1 + r_2a_2 + \cdots + r_na_n ,$$

wobei $r_1, r_2, \ldots, r_n \in R$ sind.

Definition 7.3. Ein Ideal $\mathfrak{a}$ in einem kommutativen Ring R der Form

$$\mathfrak{a} = (a) = Ra = \{ra : r \in R\}.$$

heißt *Hauptideal*.

Das Nullelement bildet in jedem Ring das sogenannte *Nullideal*, was wir einfach als $0 = (0) = \{0\}$ schreiben. Die 1 und überhaupt jede Einheit erzeugt als Ideal schon den ganzen Ring.

Definition 7.4. Das *Einheitsideal* in einem kommutativen Ring R ist der Ring selbst.

In einem Körper gibt es nur diese beiden Ideale.

Lemma 7.5. *Es sei R ein kommutativer Ring. Dann sind folgende Aussagen äquivalent.*

(1) *R ist ein Körper.*
(2) *Es gibt in R genau zwei Ideale.*

Beweis. Wenn R ein Körper ist, so gibt es das Nullideal und das Einheitsideal, die voneinander verschieden sind. Sei I ein von null verschiedenes Ideal in R. Dann enthält I ein Element $x \neq 0$, das eine Einheit ist. Damit ist $1 = xx^{-1} \in I$ und damit $I = R$.

Sei umgekehrt R ein kommutativer Ring mit genau zwei Idealen. Dann kann R nicht der Nullring sein. Sei nun x ein von null verschiedenes Element in R. Das von x erzeugte Hauptideal Rx ist $\neq 0$ und muss daher mit dem anderen Ideal, also mit dem Einheitsideal übereinstimmen. Das heißt insbesondere, dass $1 \in Rx$ ist. Das bedeutet also $1 = xr$ für ein $r \in R$, so dass x eine Einheit ist. $\square$

Operationen für Ideale

Der Durchschnitt von Idealen ist wieder ein Ideal (der Durchschnitt von Hauptidealen ist im Allgemeinen kein Hauptideal). Daneben gibt es noch zwei weitere Operationen für Ideale, die zu neuen Idealen führen.

Definition 7.6. Zu Idealen $\mathfrak{a}, \mathfrak{b} \subseteq R$ in einem kommutativen Ring R nennt man das Ideal

$$\mathfrak{a} + \mathfrak{b} \,=\, \{a + b |\, a \in \mathfrak{a},\, b \in \mathfrak{b}\}$$

die *Summe der Ideale*.

Die Summe ist wieder ein Ideal. Ein endlich erzeugtes Ideal ist die Summe von Hauptidealen, nämlich

$$(a_1, \ldots, a_n) \,=\, (a_1) + \cdots + (a_n).$$

Definition 7.7. Zu zwei Idealen $\mathfrak{a}$ und $\mathfrak{b}$ in einem kommutativen Ring wird das *Produkt* durch

$$\mathfrak{a}\mathfrak{b} \,=\, \{a_1 b_1 + a_2 b_2 + \cdots + a_k b_k\}$$

mit $a_i \in \mathfrak{a}$, $b_i \in \mathfrak{b}$ definiert. Das ist das Ideal, das von allen Produkten ab (mit $a \in \mathfrak{a}$, $b \in \mathfrak{b}$) erzeugt wird.

Die Menge aller Produkte $ab, a \in \mathfrak{a}, b \in \mathfrak{b}$ ist im Allgemeinen kein Ideal. Für Hauptideale ist $(a) \cdot (b) \,=\, (a \cdot b)$ (aber *nicht* $(a) + (b) \,=\, (a + b)$).

Wenn das Produkt eines Ideals mit sich selbst genommen wird, verwendet man die Potenzschreibweise, d.h. $\mathfrak{a}^n$ bedeutet das n-fache Produkt des Ideals mit sich selbst. In $K[X, Y]$ ist beispielsweise

$$(X, Y)^2 \,=\, (X^2, XY, Y^2).$$

Ideale und Teilbarkeitsbeziehungen

Mit dem Idealbegriff lassen sich Teilbarkeitsbeziehungen ausdrücken.

Lemma 7.8. *Sei R ein kommutativer Ring und $a, b \in R$. Dann gelten folgende Aussagen.*

(1) *Das Element a ist ein Teiler von b (also $a|b$), genau dann, wenn $(b) \subseteq (a)$.*
(2) *a ist eine Einheit genau dann, wenn $(a) = R = (1)$.*
(3) *Jede Einheit teilt jedes Element.*
(4) *Teilt a eine Einheit, so ist a selbst eine Einheit.*

Beweis. Siehe Aufgabe 7.6. □

Lemma 7.9. *Sei R ein kommutativer Ring, $a_1, \ldots, a_k \in R$ und $\mathfrak{a} = (a_1, \ldots, a_k)$ das davon erzeugte Ideal. Ein Element $t \in R$ ist ein gemeinsamer Teiler von $a_1, \ldots, a_k \in R$ genau dann, wenn $\mathfrak{a} \subseteq (t)$ ist, und t ist ein größter gemeinsamer Teiler genau dann, wenn für jedes $s \in R$ mit $\mathfrak{a} \subseteq (s)$ folgt, dass $(t) \subseteq (s)$ ist. Ein größter gemeinsamer Teiler erzeugt also ein minimales Hauptoberideal von $\mathfrak{a}$.*

Beweis. Aus $\mathfrak{a} = (a_1, \ldots, a_k) \subseteq (t)$ folgt sofort $(a_i) \subseteq (t)$ für $i = 1, \ldots, k$, was gerade bedeutet, dass t diese Elemente teilt, also ein gemeinsamer Teiler ist. Sei umgekehrt t ein gemeinsamer Teiler. Dann ist $a_i \in (t)$ und da $\mathfrak{a} = (a_1, \ldots, a_k)$ das kleinste Ideal ist, das alle a_i enthält, muss $\mathfrak{a} \subseteq (t)$ gelten. Der zweite Teil folgt sofort aus dem ersten. □

Lemma 7.10. *Sei R ein kommutativer Ring, $a_1, \ldots, a_k \in R$ und $\mathfrak{b} = (a_1) \cap \ldots \cap (a_k)$ der Durchschnitt der zugehörigen Hauptideale. Ein Element $r \in R$ ist ein gemeinsames Vielfaches von $a_1, \ldots, a_k \in R$ genau dann, wenn $(r) \subseteq \mathfrak{b}$ ist, und r ist ein kleinstes gemeinsames Vielfaches genau dann, wenn für jedes $s \in R$ mit $(s) \subseteq \mathfrak{b}$ folgt, dass $(s) \subseteq (r)$ ist. Ein kleinstes gemeinsames Vielfaches erzeugt also ein maximales Hauptdeal innerhalb von $\mathfrak{b}$.*

Beweis. Siehe Aufgabe 8.1. □

Das Radikal

Definition 7.11. Ein Ideal $\mathfrak{a}$ in einem kommutativen Ring R heißt *Radikal* (oder *Radikalideal*), wenn folgendes gilt: Falls $f^n \in \mathfrak{a}$ ist für ein $n \in \mathbb{N}$, so ist bereits $f \in \mathfrak{a}$.

Definition 7.12. Sei R ein kommutativer Ring und $\mathfrak{a} \subseteq R$ ein Ideal. Dann nennt man die Menge

$$\{f \in R | \text{ es gibt ein } r \text{ mit } f^r \in \mathfrak{a}\}$$

das *Radikal* zu $\mathfrak{a}$. Es wird mit $\operatorname{rad}(\mathfrak{a})$ bezeichnet.

Das Radikal zu einem Ideal ist selbst ein Radikal und insbesondere ein Ideal.

Lemma 7.13. *Sei R ein kommutativer Ring und $\mathfrak{a} \subseteq R$ ein Ideal. Dann ist das Radikal zu $\mathfrak{a}$ ein Radikalideal.*

Beweis. Wir zeigen zunächst, dass ein Ideal vorliegt. 0 gehört offenbar zum Radikal und mit $f \in \operatorname{rad}(\mathfrak{a})$, sagen wir $f^r \in \mathfrak{a}$, ist auch $(af)^r = a^r f^r \in \mathfrak{a}$, also gehört af zum Radikal. Zur Summeneigenschaft seien $f, g \in \operatorname{rad} \mathfrak{a}$ mit $f^r \in \mathfrak{a}$ und $g^s \in \mathfrak{a}$. Dann ist

$$(f+g)^{r+s} = \sum_{i+j=r+s} \binom{r+s}{i} f^i g^j = \sum_{i+j=r+s,\, i<r} \binom{r+s}{i} f^i g^j + \sum_{i+j=r+s,\, i \geq r} \binom{r+s}{i} f^i g^j \in \mathfrak{a}\,.$$

Sei nun $f^k \in \operatorname{rad}(\mathfrak{a})$. Dann ist $(f^k)^r = f^{kr} \in \mathfrak{a}$, also $f \in \operatorname{rad}(\mathfrak{a})$. □

Definition 7.14. Ein Ideal $\mathfrak{p}$ in einem kommutativen Ring R heißt *Primideal*, wenn $\mathfrak{p} \neq R$ ist und wenn für $r, s \in R$ mit $r \cdot s \in \mathfrak{p}$ folgt: $r \in \mathfrak{p}$ oder $s \in \mathfrak{p}$.

Lemma 7.15. *Sei R ein Integritätsbereich und $p \in R$, $p \neq 0$. Dann ist p genau dann ein Primelement, wenn das von p erzeugte Hauptideal (p) ein Primideal ist.*

Beweis. Siehe Aufgabe 7.14. □

Definition 7.16. Ein Ideal $\mathfrak{m}$ in einem kommutativen Ring R heißt *maximales Ideal*, wenn $\mathfrak{m} \neq R$ ist und wenn es zwischen $\mathfrak{m}$ und R keine weiteren Ideale gibt.

Lemma 7.17. *Sei R ein kommutativer Ring und $\mathfrak{m}$ ein maximales Ideal in R. Dann ist $\mathfrak{m}$ ein Primideal.*

Beweis. Siehe Aufgabe 7.20. □