



Basiswissen Kommutative Algebra

zur Vorlesung

Algorithmische algebraische Geometrie

Dies ist eine Zusammenstellung von einigen grundlegenden Definitionen, Notationen und Resultaten aus der kommutativen Algebra, die aus den Vorlesungen B1–B4 bekannt sein sollten. Es bedeuten [LA], [A] bzw. [ZT] meine entsprechenden Vorlesungen aus SS 2009, WS 2009/10 bzw. SS 2010.

1. Alle betrachteten Ringe sind kommutativ und haben eine Eins. Zur Definition eines Ringhomomorphismus gehört, daß er Eins auf Eins abbildet. Im Nullring $A = \{0\}$ gilt $1 = 0$; in jedem anderen Ring ist $1 \neq 0$. Ein Teilring des Rings A muß die Eins von A enthalten. Mit $A^* = \{a \in A : \exists b \in A \ ab = 1\}$ wird die Menge der Einheiten von A bezeichnet; dies ist eine Gruppe unter Multiplikation.

2. Sei A ein Ring. Das von einer Teilmenge X von A erzeugte Ideal in A wird mit

$$(X) = \sum_{x \in X} Ax$$

bezeichnet; für $X = \{a_1, \dots, a_n\}$ schreibt man auch (a_1, \dots, a_n) . Ist $\{I_\lambda : \lambda \in \Lambda\}$ eine Familie von Idealen in A , so sind auch Summe $\sum_\lambda I_\lambda$ und Durchschnitt $\bigcap_\lambda I_\lambda$ wieder Ideale in A . Zu je endlich vielen Idealen I_1, \dots, I_r in A hat man das Idealprodukt

$$I_1 \cdots I_r := (a_1 \cdots a_r : a_1 \in I_1, \dots, a_r \in I_r).$$

Das ist ein Ideal von A mit $I_1 \cdots I_r \subseteq I_1 \cap \cdots \cap I_r$. Im allgemeinen gilt hier keine Gleichheit. Sind die Ideale I_1, \dots, I_r aber paarweise relativ prim, also $I_i + I_j = (1)$ für $i \neq j$, so ist $I_1 \cdots I_r = I_1 \cap \cdots \cap I_r$ ([LA] III.1.12 und III.3.11).

Zu jedem Ideal I von A hat man den Quotientenring A/I . Der Kern jedes Ringhomomorphismus $A \rightarrow B$ ist ein Ideal von A . Der Homomorphiesatz besagt: Ist $\varphi: A \rightarrow B$ ein surjektiver Ringhomomorphismus, so ist

$$\bar{\varphi}: A/\ker(\varphi) \rightarrow B, \quad \bar{\varphi}(\bar{a}) := \varphi(a) \quad (a \in A)$$

ein (wohldefinierter) Ringisomorphismus.

3. Der Ring A heißt *noethersch*, wenn jedes Ideal von A durch endlich viele Elemente erzeugt werden kann ([ZT] I.1). Der Basissatz von Hilbert besagt: Für jeden noetherschen Ring A sind auch die Polynomringe $A[x_1, \dots, x_n]$ ($n \in \mathbb{N}$) noethersch. (Siehe [ZT] I.1.10)

4. Ein A -Modul ist eine abelsche Gruppe $(M, +)$ zusammen mit einer Abbildung $A \times M \rightarrow M$, $(a, x) \mapsto a \cdot x = ax$, welche assoziativ und distributiv ist und $1 \cdot x = x$ für alle $x \in M$ erfüllt. Die grundlegenden Konzepte und Operationen für A -Moduln (wie lineare Abhängigkeit, Untermoduln, Summen und Durchschnitte, direkte Summen, Quotientenmoduln, lineare Abbildungen, Kern, Homomorphiesatz usw.) sind analog zur linearen Algebra über Körpern. Der wichtigste Unterschied zum Körperfall ist, daß ein A -Modul M im allgemeinen keine Basis (linear unabhängiges Erzeugendensystem) hat. Ein A -Modul, welcher eine Basis besitzt,

heißt *frei*. Die endlich erzeugten freien A -Moduln sind genau die zu $A^n := A \oplus \cdots \oplus A$ (n Summanden, $n \geq 0$) isomorphen A -Moduln.

Ein Ring A ist genau dann noethersch, wenn jeder Untermodul eines endlich erzeugten A -Moduls endlich erzeugt ist.

5. Ein Element $a \in A$ heißt ein *Nullteiler* von A , wenn es ein $b \in A$ mit $b \neq 0$ und $ab = 0$ gibt. Der Ring A heißt *nullteilerfrei*, oder *integer*, wenn er keine Nullteiler $\neq 0$ hat. (Den Nullring betrachtet man also nicht als integer.)

6. Ein Ideal \mathfrak{p} von A heißt ein *Primideal*, wenn $\mathfrak{p} \neq A$ ist und gilt: Aus $a, b \in A$ und $ab \in \mathfrak{p}$ folgt $a \in \mathfrak{p}$ oder $b \in \mathfrak{p}$. Äquivalent dazu ist, daß der Restklassenring A/\mathfrak{p} integer ist. Die Definition verallgemeinert sich zu folgender Charakterisierung: Ein Ideal $\mathfrak{p} \neq A$ von A ist genau dann ein Primideal, wenn für je zwei Ideale I, J von A mit $IJ \subseteq \mathfrak{p}$ gilt: $I \subseteq \mathfrak{p}$ oder $J \subseteq \mathfrak{p}$.

Die Menge aller Primideale von A wird mit $\text{Spec}(A)$ bezeichnet und heißt das *Zariski-Spektrum* von A . Ist $\varphi: B \rightarrow A$ ein Ringhomomorphismus, so induziert φ die Abbildung

$$\varphi^*: \text{Spec}(A) \rightarrow \text{Spec}(B), \quad \varphi^*(\mathfrak{p}) := \varphi^{-1}(\mathfrak{p})$$

(in “umgekehrter” Richtung). Insbesondere sind Urbilder von Primidealen stets wieder Primideale.

7. Ein Ideal I von A heißt ein *maximales Ideal* von A , wenn $I \neq (1)$ ist und für alle Ideale J von A mit $I \subseteq J$ gilt: $J = I$ oder $J = (1)$. Genau dann ist das Ideal I maximal, wenn der Ring A/I ein Körper ist ([LA] III.1.16). Jedes maximale Ideal ist also ein Primideal. Die Menge der maximalen Ideale von A wird mit $\text{Max}(A)$ bezeichnet, das ist eine Teilmenge von $\text{Spec}(A)$. Jedes Ideal $I \neq (1)$ ist in einem maximalen Ideal von A enthalten ([A] I.3.7). Insbesondere ist $\text{Max}(A)$ (und damit auch $\text{Spec}(A)$) nicht leer, sofern $A \neq \{0\}$ ist.

8. Zu Ringen von Brüchen und Lokalisierung siehe [A] I.2 und [ZT] I.3. Für jede multiplikative Teilmenge S von A (stets mit $1 \in S$) haben wir den Ring der Brüche $A_S = \left\{ \frac{a}{s} : a \in A, s \in S \right\}$, wobei die Gleichheit von Brüchen definiert ist durch $\frac{a_1}{s_1} = \frac{a_2}{s_2} : \Leftrightarrow \exists s \in S$ mit $ss_1a_2 = ss_2a_1$. Der Ringhomomorphismus $\varphi_S: A \rightarrow A_S$, $a \mapsto \frac{a}{1}$ erfüllt $\varphi_S(S) \subseteq (A_S)^*$ und ist “universell” für diese Eigenschaft ([A] 2.6). Genau dann ist φ_S injektiv, wenn S aus Nichtnullteilern von A besteht.

Die Abbildung $\varphi_S^*: \text{Spec}(A_S) \rightarrow \text{Spec}(A)$ ist eine Bijektion von $\text{Spec}(A_S)$ auf die Teilmenge

$$D(S) := \{ \mathfrak{p} \in \text{Spec}(A) : \mathfrak{p} \cap S = \emptyset \}$$

von $\text{Spec}(A)$. Die Umkehrabbildung ist $\mathfrak{p} \mapsto \mathfrak{p}A_S =: \mathfrak{p}_S$. ([A] I.3.13, [ZT] I.3.3)

9. Ist S die Menge aller Nichtnullteiler von A , so heißt der Ring $\text{Quot}(A) := A_S$ der *totale Quotientenring* von A . Der kanonische Homomorphismus $\varphi: A \rightarrow A_S$ ist injektiv. Wichtig ist vor allem der Fall, wo A integer ist. Dann ist $S = A \setminus \{0\}$, und $\text{Quot}(A)$ ist ein Körper, genannt der *Quotientenkörper* von A . ([A] I.2.8)

10. Ist \mathfrak{p} ein Primideal von A , so ist $S := A \setminus \mathfrak{p}$ eine multiplikative Menge in A . Man schreibt $A_{\mathfrak{p}} := A_S$ und nennt $A_{\mathfrak{p}}$ die *Lokalisierung* von A im Primideal \mathfrak{p} . Nach ?? steht $\text{Spec}(A_{\mathfrak{p}})$ in kanonischer Bijektion zur Menge der in \mathfrak{p} enthaltenen Primideale von A . Insbesondere hat $A_{\mathfrak{p}}$ genau ein maximales Ideal, nämlich $\mathfrak{p}A_{\mathfrak{p}}$. Generell heißt ein Ring ein *lokaler Ring*, wenn er genau ein maximales Ideal hat. ([A] I.3.14, [ZT] I.3.4)

11. Quotientenbildung und Lokalisierung vertauschen miteinander: Ist I ein Ideal von A und S eine multiplikative Teilmenge von A , so hat man den kanonischen Ringisomorphismus

$$A_S/IA_S \xrightarrow{\sim} (A/I)_{\overline{S}}, \quad \frac{a}{s} + IA_S \mapsto \frac{a+I}{s+I}$$

wobei $\bar{S} := \{s + I : s \in S\}$ das Bild von S in A/I bezeichnet (eine multiplikative Teilmenge von A/I). ([ZT] I.3.5)

12. Ist $I = \mathfrak{p}$ ein Primideal von A und $S = A \setminus \mathfrak{p}$, so ergibt sich insbesondere

$$A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}} \cong \text{Quot}(A/\mathfrak{p}) :$$

Der Restklassenkörper des lokalen Rings $A_{\mathfrak{p}}$ nach seinem maximalen Ideal $\mathfrak{p}A_{\mathfrak{p}}$ ist isomorph zum Quotientenkörper des integren Rings A/\mathfrak{p} . Man nennt diesen Körper den *Restklassenkörper* des Primideals \mathfrak{p} .

Jeder Ringhomomorphismus $\varphi: B \rightarrow A$ induziert Einbettungen der Restklassenkörper der Primideale. Genauer: Ist $\mathfrak{p} \in \text{Spec}(A)$, setzt man $\mathfrak{q} := \varphi^{-1}(\mathfrak{p}) \in \text{Spec}(B)$, und bezeichnen $\kappa(\mathfrak{p}) = \text{Quot}(A/\mathfrak{p})$, $\kappa(\mathfrak{q}) = \text{Quot}(B/\mathfrak{q})$ die Restklassenkörper, so induziert φ eine Einbettung $\kappa(\mathfrak{q}) \hookrightarrow \kappa(\mathfrak{p})$ durch $\bar{b} \mapsto \overline{\varphi(b)}$.

13. Sei L/K eine Körpererweiterung, und sei $\alpha \in L$. Das Element α heißt *transzendent* über K , wenn der Einsetzhomomorphismus

$$K[x] \rightarrow L, \quad f(x) \mapsto f(\alpha)$$

injektiv ist. Andernfalls heißt α *algebraisch* über K . Im letzteren Fall gibt es ein eindeutig bestimmtes normiertes Polynom $f(x) \in K[x]$ von kleinstem Grad mit $f(\alpha) = 0$, genannt das *Minimalpolynom* von α über K .

14. Sei R ein Ring. Eine *R-Algebra* ist ein Ring A zusammen mit einem Ringhomomorphismus $\alpha: R \rightarrow A$ (manchmal als Strukturhomomorphismus bezeichnet). Ist α aus dem Kontext klar oder nicht explizit wichtig, so wird α meist gar nicht erwähnt. Sind $\alpha: R \rightarrow A$ und $\beta: R \rightarrow B$ zwei *R-Algebren*, so versteht man unter einem *R-Homomorphismus* (oder *Homomorphismus von R-Algebren*) von A nach B einen Ringhomomorphismus $\varphi: A \rightarrow B$ mit $\varphi \circ \alpha = \beta$. Entsprechend heißen A und B *R-isomorph* (oder *isomorph als R-Algebren*), wenn es einen bijektiven *R-Homomorphismus* $A \rightarrow B$ gibt.

15. Sei $\varphi: A \rightarrow B$ ein Ringhomomorphismus. Ein Element $b \in B$ heißt *ganz über A*, wenn es eine *normierte Gleichung*

$$b^n + \varphi(a_1)b^{n-1} + \dots + \varphi(a_n) = 0$$

mit $n \in \mathbb{N}$ und $a_1, \dots, a_n \in A$ gibt (siehe¹ [ZT] I.2).

Die Menge aller über A ganzen Elemente von B bildet einen Teilring, und somit eine *A-Teilalgebra*, von B ([ZT] I.2.3). Ist jedes Element von B ganz über A , so nennt man B eine *ganze A-Algebra*, oder φ einen *ganzen Ringhomomorphismus*. Sind $\varphi: A \rightarrow B$ und $\psi: B \rightarrow C$ ganze Ringhomomorphismen, so ist auch die Komposition $\psi \circ \varphi: A \rightarrow C$ ein ganzer Ringhomomorphismus ([ZT] I.2.11).

¹Dort wurde zur Vereinfachung angenommen, daß A ein Teilring von B ist. Die allgemeine Definition wird sofort darauf zurückgeführt, denn b ist genau dann ganz über A , wenn b ganz über dem Teilring $\varphi(A)$ von B ist.