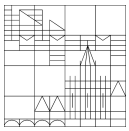
Universität Konstanz
Fachbereich Mathematik und Statistik
C. Scheiderer
WS 2014/15



Basiswissen Kommutative Algebra

zur Vorlesung

Algorithmische algebraische Geometrie

Die hier zusammengestellten Definitionen, Notationen und Resultate aus der kommutativen Algebra werden in der Vorlesung Algorithmische algebraische Geometrie gebraucht. Sie sollten aus den Vorlesungen B1–B4 bekannt sein. Soweit das nicht der Fall ist, konsultiere man ein Lehrbuch der kommutativen Algebra, z.B.

- M. Atiyah, B. I. Macdonald: Introduction to Commutative Algebra. Addison-Wesley, 1969.

1. Alle betrachteten Ringe sind kommutativ und haben eine Eins (im allgemeinen bezeichnet mit 1). 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 $A^* = \{a \in A \colon \exists\, b \in A\ ab = 1\}$ wird die Menge der Einheiten von A bezeichnet. Dies ist eine abelsche 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 $X = \{a_1, \ldots, a_n\}$ schreibt man auch $(a_1, \ldots, a_n)$. Ist $\{I_\lambda \colon \lambda \in \Lambda\}$ 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 $I_1, \ldots, I_r$ in A hat man das Idealprodukt

$$I_1 \cdots I_r \;:=\; \big(a_1 \cdots a_r \colon a_1 \in I_1, \ldots, a_r \in I_r\big).$$

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 $I_1, \ldots, I_r$ aber paarweise relativ prim, d.h. gilt $I_i + I_j = (1)$ für $i \neq j$, so ist $I_1 \cdots I_r = I_1 \cap \cdots \cap I_r$.

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

$$\overline{\varphi} \colon A/\ker(\varphi) \to B, \quad \overline{\varphi}(\overline{a}) \;:=\; \varphi(a) \quad (a \in A)$$

ein (wohldefinierter) Ringisomorphismus.

3. Der Ring A heißt *noethersch*, wenn jedes Ideal von A durch endlich viele Elemente erzeugt werden kann. Der Basissatz von Hilbert besagt: Für jeden noetherschen Ring A ist auch der Polynomring $A[x]$ noethersch.

4. Ein A-Modul ist eine abelsche Gruppe $(M, +)$ zusammen mit einer Abbildung $A \times M \to M$, $(a, x) \mapsto a \cdot x = ax$, 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 A-Modul M heißt *treu*, wenn zu jedem $0 \neq a \in A$ ein $x \in M$ existiert mit $ax \neq 0$.

Ein Ring A ist genau dann noethersch, wenn jeder Untermodul jedes endlich erzeugten A-Moduls selbst 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 *integer*, oder *nullteilerfrei*, 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 $\operatorname{Spec}(A)$ bezeichnet und heißt das *Zariski-Spektrum* von A. Ist $\varphi\colon B \to A$ ein Ringhomomorphismus, so induziert φ die Abbildung

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

(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 Jedes maximale Ideal ist also ein Primideal. Die Menge der maximalen Ideale von A wird mit $\operatorname{Max}(A)$ bezeichnet, das ist eine Teilmenge von $\operatorname{Spec}(A)$. Jedes Ideal $I \neq (1)$ ist in einem maximalen Ideal von A enthalten. Insbesondere ist $\operatorname{Max}(A)$ (und damit auch $\operatorname{Spec}(A)$) nicht leer, sofern $A \neq \{0\}$ ist.

8. Für jede multiplikative Teilmenge S von A (stets mit $1 \in S$) haben wir den Ring der Brüche $A_S = \{\frac{a}{s}\colon a \in A,\, s \in S\}$, 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 $\varphi_S\colon A \to A_S$, $a \mapsto \frac{a}{1}$ erfüllt $\varphi_S(S) \subseteq (A_S)^*$ und ist "universell" für diese Eigenschaft. Genau dann ist φ_S injektiv, wenn S aus Nichtnullteilern von A besteht.

Die Abbildung $\varphi_S^*\colon \operatorname{Spec}(A_S) \to \operatorname{Spec}(A)$ ist eine Bijektion von $\operatorname{Spec}(A_S)$ auf die Teilmenge

$$D(S) := \{\mathfrak{p} \in \operatorname{Spec}(A)\colon \mathfrak{p} \cap S = \varnothing\}$$

von $\operatorname{Spec}(A)$. Die Umkehrabbildung ist $\mathfrak{p} \mapsto \mathfrak{p}A_S =: \mathfrak{p}_S$.

9. Ist $S \subseteq A$ eine multiplikative Menge und M ein A-Modul, so ist der A_S-Modul M_S definiert als Menge aller formalen Brüche $\frac{x}{s}$ ($x \in M$, $s \in S$), mit Gleichheitsdefinition

$$\frac{x_1}{s_1} = \frac{x_2}{s_2} \quad \Leftrightarrow \quad \exists\, s \in S \ \text{ mit } \ ss_1x_2 = ss_2x_1,$$

und mit Addition $\frac{x}{s} + \frac{y}{t} = \frac{tx+sy}{st}$ und Skalarmultiplikation $\frac{a}{s} \cdot \frac{x}{t} = \frac{ax}{st}$.

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

11. 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 8. steht $\mathrm{Spec}(A_\mathfrak{p})$ 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.

12. 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 $\overline{S} := \{s + I \colon s \in S\}$ das Bild von S in A/I bezeichnet (eine multiplikative Teilmenge von A/I).

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

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

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

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

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

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.

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

16. Sei $\varphi \colon A \to B$ ein Ringhomomorphismus. Ein Element $b \in B$ heißt *ganz über* A, wenn es $n \in \mathbb{N}$ und $a_1, \ldots, a_n \in A$ gibt mit

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

Genau dann ist b ganz über A, wenn es einen treuen $A[b]$-Modul gibt, der als A-Modul endlich erzeugt ist.

Die Menge aller über A ganzen Elemente von B bildet einen Teilring, und somit eine A-Teilalgebra, von B. Ist jedes Element von B ganz über A, so nennt man B eine *ganze A-Algebra*, oder φ einen *ganzen Ringhomomorphismus*. Sind $\varphi \colon A \to B$ und $\psi \colon B \to C$ ganze Ringhomomorphismen, so ist auch die Komposition $\psi \circ \varphi \colon A \to C$ ein ganzer Ringhomomorphismus.