Methoden der kommutativen Algebra in Charakteristik Null und positiver Charakteristik

Martin Kreidl

6. Februar 2007

Inhaltsverzeichnis

Kapitel 1

Derivationen und 1-Formen

Wir beginnen mit einem Abschnitt, in dem wir grundlegende Begriffe wie die der Derivationen und der 1-Formen einführen und einige elementare Tatsachen über diese Objekte herleiten.
Es bezeichne R einen kommutativen Ring mit Einselement, A und B seien R-Algebren. Mit M bezeichnen wir stets einen A-Modul.

Definition 1.1. Eine *R-Derivation* von A in einen A-Modul M ist eine R-lineare Abbildung von A nach M, welche die *Produktregel*

$$\delta(fg) = \delta(f)g + f\delta(g), \quad f, g \in A$$

erfüllt.

Jede R-Derivation ist natürlich insbesondere eine $\mathbb{Z}$-Derivation. Aus der Produktregel folgt sofort, dass Elemente von R unter einer R-Derivation auf 0 abgebildet werden:

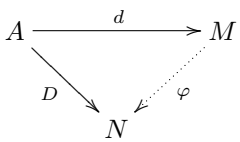
$$\delta(1) = \delta(1 \cdot 1) = 1 \cdot \delta(1) + \delta(1) \cdot 1 = 2\delta(1).$$

Die Menge aller R-Derivationen von A nach M bildet offensichtlich einen A-Modul, den wir mit $\mathrm{Der}_R(A, M)$ bezeichnen.

Beispiel 1.2. Sei $A = R[X]$ der Polynomring in einer Variablen über R. Die übliche Differentiation von Polynomen $\frac{d}{dX} : R[X] \to R[X]; f \mapsto f'$ ist eine R-Derivation von $R[X]$ nach $R[X]$. Da aufgrund der Produktregel jede R-Derivation auf $R[X]$ bereits durch die Vorgabe des Bildes von X festgelegt ist, hat jede solche Derivation die Form $P \cdot \frac{d}{dX}, P \in R[X]$, d.h., $\frac{d}{dX}$ erzeugt den Modul $\mathrm{Der}_R(R[X], R[X])$.

Derivationen lassen sich sehr einfach durch eine gewisse 'universelle' Derivation charakterisieren, die wir im Folgenden beschreiben und konstruieren werden.

Definition 1.3. Ein A-Modul M zusammen mit einer R-Derivation d von A nach M heißt *Modul der relativen 1-Formen* von A über R, wenn das Paar (M, d) folgende universelle Eigenschaft erfüllt:
Zu jeder R-Derivation D von A in einen A-Modul N existiert ein A-Homomorphismus φ, der das Diagramm



(1.1)

kommutativ macht.

Wie jedes Objekt, das durch eine universelle Eigenschaft definiert wird, ist das Paar (M, d), falls überhaupt existent, dadurch schon bis auf einen eindeutigen Isomorphismus festgelegt. Wir können also von *dem* Modul der relativen 1-Formen von A über R sprechen und schreiben $(\Omega^1_{A/R}, d_{A/R})$, oder einfach nur $\Omega^1_{A/R}$.

Der Modul $\Omega^1_{A/R}$ wird oft auch als der Modul der *Kähler-Differentiale* bezeichnet. Das Element $d_{A/R}(f), f \in A$, heißt das *(Kähler-)Differential* von f.

Bemerkung 1.4. Die eben formulierte universelle Eigenschaft ist gleichbedeutend mit

$$\mathrm{Der}_R(A, M) \simeq \mathrm{Hom}_A(\Omega^1_{A/R}, M), \quad \text{für alle } M \tag{1.2}$$

Daher können wir auf natürliche Weise eine Derivation mit einer A-linearen Abbildung identifizieren und werden im Folgenden auch nicht mehr zwischen diesen beiden Objekten unterscheiden.

Wir gehen nun daran, den Modul der 1-Formen für einen beliebigen Ring R und eine beliebige R-Algebra A zu konstruieren. Es ist leicht zu sehen, dass man diesen Modul erhält, indem man den freien Modul über den Symbolen $d_{A/R}(f), f \in A$, bildet und die Relationen $d_{A/R}(fg) - d_{A/R}(f)g - fd_{A/R}(g)$ bzw. $d_{A/R}(rf) - rd_{A/R}(f), r \in R, f, g \in A$, ausfaktorisiert. Wir wollen aber noch ein expliziteres Modell angeben:

Das Tensorprodukt $A \otimes_R A$ ist ein Ring mit der Multiplikation $(x \otimes y) \cdot (x' \otimes y') = (xx' \otimes yy')$. Vermöge der Inklusion $A \hookrightarrow A \otimes_R A, x \mapsto x \otimes 1$, erhält $A \otimes_R A$ außerdem eine Struktur als A-Modul. Auf diese Modulstruktur werden wir uns im Folgenden immer beziehen, wenn nicht ausdrücklich anders vermerkt. Wir betrachten weiters die 'Multiplikationsabbildung' $\mu : A \otimes_R A \to A$, die wir durch lineare Ausdehnung der Vorschrift $x \otimes y \mapsto xy$ erhalten, und setzen $I = \ker \mu$. Mit diesen Festlegungen gilt der

Hilfssatz 1.5. *Das Ideal I ist ein A-Untermodul von $A \otimes_R A$ und wird als solcher von Elementen der Form $(1 \otimes x - x \otimes 1), x \in A$, erzeugt.*

Beweis. Es ist klar, dass alle Elemente der angegebenen Form in I enthalten sind. Sei nun umgekehrt $f = \sum_{i=1}^n x_i \otimes y_i \in I = \ker(\mu)$. Wir formen um:

$$\begin{aligned} f &= \sum_{i=1}^n (x_i \otimes y_i - x_i y_i \otimes 1) + \sum_{i=1}^n (x_i y_i \otimes 1) = \\ &= \sum_{i=1}^n x_i \cdot (1 \otimes y_i - y_i \otimes 1) + \mu(f) \otimes 1. \end{aligned}$$

Da aber f nach Voraussetzung im Kern von μ liegt, verschwindet der letzte Summand und wir haben die gesuchte Darstellung von f als Linearkombination von Elementen der Form $(1 \otimes x - x \otimes 1), x \in A$ gefunden. □

Man sieht daraus, dass auch $I^n, n \in \mathbb{N}$, ein A-Untermodul von $A \otimes_R A$ ist, nämlich der, der von Elementen der Form $\prod_{i=1}^n (1 \otimes f_i - f_i \otimes 1)$ erzeugt wird. Wir können also den Faktormodul I/I^2 betrachten und feststellen:

Satz 1.6. *Der Faktormodul I/I^2 zusammen mit der Abbildung*

$$\begin{aligned} d : A &\longrightarrow I/I^2 \\ f &\mapsto 1 \otimes f - f \otimes 1 \end{aligned}$$

bildet den Modul der relativen 1-Formen von A über R.

Beweis. Die Abbildung d ist offensichtlich R-linear. Weiters gilt

$$d(fg) = 1 \otimes fg - fg \otimes 1 =$$
$$= (1 \otimes f - f \otimes 1) \cdot g + f \cdot (1 \otimes g - g \otimes 1) + (1 \otimes f - f \otimes 1)(1 \otimes g - g \otimes 1) =$$
$$d(f)g + fd(g),$$

d.h., die Produktregel ist erfüllt und wir haben d somit als R-Derivation erkannt. Aufgrund der universellen Eigenschaft von $\Omega^1_{A/R}$ existiert ein eindeutig bestimmter A-Homomorphismus $\varphi : \Omega^1_{A/R} \to I/I^2, df \mapsto (1 \otimes f - f \otimes 1)$. Es ist noch festzustellen, dass dieser Homomorphismus injektiv ist (die Surjektivität ist klar). Sei $T := A \ltimes \Omega^1_{A/R}$ der Ring, der durch die komponentenweise Addition und die Multiplikation der Form

$$(a, \eta)(b, \omega) = (ab, a\omega + b\eta)$$

gegeben ist. Wir konstruieren nun einen Isomorphismus $(A \otimes_R A)/I^2 \to T$ und erhalten die Inverse der Abbildung φ durch Einschränken auf I/I^2. Wir behaupten, dass die Vorschrift

$$\psi : A \otimes_R A \to T, a \otimes b \mapsto (ab, ad_{A,R}(b)),$$

einen R-Homomorphismus definiert. Da ein R-Homomorphismus $A \otimes_R A \to T$ gegeben ist durch zwei R-Homomorphismen $A \to T$, reicht es zu zeigen, dass $a \mapsto (a, 0)$ und $b \mapsto (b, d_{A/R}b)$ R-Homomorphismen sind. Das ist aber klar. Die Abbildung ψ induziert also einen R-Homomorphismus $A \otimes_R A/I^2 \to T$, dessen Einschränkung $I/I^2 \to T, (1 \otimes f - f \otimes 1) \mapsto (0, d_{A/R}f)$ offensichtlich invers zu φ ist. □

Bemerkung 1.7. Der im Beweis konstruierte Modul $T = A \ltimes \Omega^1_{A/R}$ verallgemeinert den Begriff der 1-Form bzw. Derivation: Abbildungen der Form

$$A \to A \otimes_R A/I^2 \xrightarrow{\varphi} A, f \mapsto 1 \otimes f, a \otimes f \mapsto a\varphi(f),$$

wobei φ ein A-Homomorphismus ist, heißen *Differentialoperatoren der Ordnung* $\leqslant 1$. Sie verallgemeinern den Begriff der Derivation. Noch allgemeiner erhält man Differentialoperatoren der Ordnung $\leqslant n$, indem man statt $(A \otimes_R A)/I^2$ den Modul $(A \otimes_R A)/I^{n+1}$ betrachtet. Diese Möglichkeit der Verallgemeinerung ist einer der Gründe, warum man den Modul der Kähler-Differentiale auf die eben gezeigte Weise explizit konstruiert.

Für die universelle Derivation $d_{A/R}$ schreiben wir im Folgenden einfach d.

Beispiel 1.8. Wir bestimmen $\Omega^1_{A/R}$ im Fall des Polynomrings $A = R[\mathfrak{X}]$ für ein beliebiges System von Unbestimmten $\mathfrak{X}$. Aufgrund der Produktregel ist

$$d(f) = \sum_{X \in \mathfrak{X}} \partial_X f \cdot d(X)$$

Der Modul $\Omega^1_{A/R}$ wird also von den Elementen $d(X), X \in \mathfrak{X}$, erzeugt. Dieses Erzeugendensystem ist sogar *frei*, denn aus $0 = \sum_{X \in \mathfrak{X}} a_X \cdot d(X)$ folgt $0 = \partial_Y(0) = \sum_{X \in \mathfrak{X}} a_X \cdot \partial_Y(dX) = a_Y$ für alle $Y \in \mathfrak{X}$. Die partielle Ableitung ∂_X interpretieren wir dabei gemäß (1.4) als A-Homomorphismus von $\Omega^1_{A/R}$ nach A.

Sei nun B eine A-Algebra. Wir fragen uns, wie die Strukturen der Moduln $\Omega^1_{A/R}, \Omega^1_{B/R}$ und $\Omega^1_{B/A}$ zusammenhängen. Klar ist, dass zwei kanonische B-lineare Abbildungen

$$\alpha : \Omega^1_{A/R} \otimes_A B \to \Omega^1_{B/R}; \quad (1 \otimes f - f \otimes 1) \otimes b \mapsto b \cdot (1 \otimes f - f \otimes 1),$$
$$\beta : \Omega^1_{B/R} \to \Omega^1_{B/A}; \quad (1 \otimes f - f \otimes 1) \mapsto (1 \otimes f - f \otimes 1)$$

existieren. Diese bilden aber sogar eine rechtsexakte Folge:

Satz 1.9. *Sei B eine A-Algebra. Dann ist die Sequenz*

$$\Omega^1_{A/R} \otimes_A B \xrightarrow{\alpha} \Omega^1_{B/R} \xrightarrow{\beta} \Omega^1_{B/A} \to 0, \tag{1.3}$$

mit α und β wie oben definiert, exakt.

Beweis. Es ist klar, das β surjektiv ist. Weiters ist $\beta \circ \alpha = 0$, da für $f \in A$ gilt:

$$\beta \circ \alpha((1 \otimes_R f - f \otimes_R 1) \otimes_A b) = \beta(b(1 \otimes_R f - f \otimes_R 1)) = b(1 \otimes_A f - f \otimes_A 1) = 0.$$

Es ist nun noch zu zeigen, dass $\ker(\beta) \subset \mathrm{im}(\alpha)$: Zusätzlich zu den Relationen im Tensorprodukt über R bestehen im Tensorprodukt über A die Relationen der Form

$$b_1 \otimes ab_2 - ab_1 \otimes b_2, a \in A, b_i \in B.$$

Der Kern von β besteht also aus lauter Linearkombinationen solcher Relationen, und es reicht daher zu zeigen, dass jede dieser Relationen im Bild von α enthalten ist. Und tatsächlich gilt

$$b_1 \otimes ab_2 - ab_1 \otimes b_2 = b_1(1 \otimes ab_2 - a \otimes b_2) =$$
$$= b_1(b_2 \otimes a - ab_2 \otimes 1) = b_1b_2(1 \otimes a - a \otimes 1) = \alpha((1 \otimes a - a \otimes 1) \otimes b_1b_2).$$

Beachte für die zweite Identität, dass $(1 \otimes a - a \otimes 1)(1 \otimes b_2 - b_2 \otimes 1) = 0$ ist. Daher ist $\ker(\beta) = \mathrm{im}(\alpha)$ und die Sequenz ist wie behauptet exakt. □

Als Anwendung dieses Satzes untersuchen wir, wie sich 1-Formen auf A auf Lokalisierungen von A fortsetzen. Sei dazu S ein multiplikatives System in $A - \{0\}$, d.h., S enthalte das Einselement von A und mit zwei Elementen von S sei auch deren Produkt in S. Sei A_S die Lokalisierung von A nach S und A_S eine A-Algebra vermöge der kanonischen Abbildung $a \mapsto \frac{a}{1}$.
Als erstes stellen wir fest, dass $\Omega^1_{A_S/A} = 0$, denn nach der Produktregel gilt für eine beliebige A-Derivation von A_S

$$0 = d(a) = d(s\frac{a}{s}) = d(s)\frac{a}{s} + sd(\frac{a}{s}) = sd(\frac{a}{s}), a \in A, s \in S.$$

Da s in S invertierbar ist, folgt $d(\frac{a}{s}) = 0$ und daher $\Omega^1_{A_S/A} = 0$. Zusammen mit Satz 1.9 erhalten wir das

Korollar 1.10. *Die Abbildung $\alpha : \Omega^1_{A/R} \otimes A_S \to \Omega^1_{A_S/R}$ ist bijektiv.*
In A_S gilt weiters die Quotientenregel*, d.h.,*

$$d(\frac{a}{s}) = \frac{sd(a) - ad(s)}{s^2}$$

und jede Derivation auf A setzt sich auf eindeutige *Weise auf die Lokalisierung A_S fort.*

Beweis. Die Surjektivität von α haben wir schon in den Bemerkungen vor der Formulierung des Korollars eingesehen. Die Quotientenregel ist eine direkte Konsequenz aus der Produktregel:

$$d(a) = d(s\frac{a}{s}) = sd(\frac{a}{s}) + d(s)\frac{a}{s}.$$

Wir zeigen noch die Injektivität von α, indem wir durch eine analoge Formel eine Derivation $\delta : A_S \to \Omega^1_{A/R} \otimes A_S$ festlegen. Aus der universellen Eigenschaft von $\Omega^1_{A_S/R}$ folgt dann, dass eine Abbildung $\varphi : \Omega^1_{A_S/R} \to \Omega^1_{A/R} \otimes A_S$ existiert, von der wir nachweisen werden, dass sie die Inverse von α ist. Wir definieren also δ durch

$$\delta(\frac{f}{s}) := (d(f)s - fd(s)) \otimes \frac{1}{s^2}.$$

Dadurch ist eine Derivation δ wohldefiniert, und es existiert genau eine A_S-lineare Abbildung $\varphi : \Omega^1_{A_S/R} \to \Omega^1_{A/R} \otimes A_S$, sodass $\varphi \circ d_{A_S/R} = \delta$. Für ein Element $f \in A$ gilt offensichtlich $\varphi(d_{A_S/R}(f)) = \delta(f) = d_{A/R}(f) \otimes 1$, d.h., auf den Differentialen von A sind die Abbildungen α und φ invers. Da aber die beiden A_S-Moduln $\Omega^1_{A_S/R}$ und $\Omega^1_{A/R} \otimes A_S$ schon von diesen Differentialen erzeugt werden, sind φ und α überhaupt invers, woraus die Bijektivität von α folgt. □

Da wir dieses Korollar v.a. in Kapitel 2 häufig im Spezialfall des Quotientenkörpers als Lokalisierung nach dem 0-Ideal verwenden, wollen wir noch einmal festhalten:

Korollar 1.11. *Sei A eine nullteilerfreie R-Algebra und K ihr Quotientenkörper. Dann ist $\Omega^1_{K/R}$ auf natürliche Weise isomorph zu $\Omega^1_{A/R} \otimes K$, oder anders formuliert: Jede R-Derivation von A in einen K-Vektorraum V besitzt eine eindeutige Fortsetzung auf K mittels der Quotientenregel und jede R-Derivation von K nach V hat diese Form.* □

Zusammen mit dem Beispiel 1.8 erhalten wir weiters das

Korollar 1.12. *Es sei L/K eine rein transzendente Körpererweiterung mit Transzendenzbasis $\mathfrak{X}$. Dann ist $(d_{L/K}(X))_{X \in \mathfrak{X}}$ eine L-Basis von $\Omega^1_{L/K}$.*

Beweis. Beispiel 1.8 und Korollar 1.11. □

Ähnlich verhält es sich auch mit dem Problem der Fortsetzung von Derivationen auf die Vervollständigung einer R-Algebra A bezüglich eines maximalen Ideals $\mathfrak{m}$. Wir werden die folgende Beobachtung in Kapitel 3 verwenden.

Hilfssatz 1.13. *Sei $\mathfrak{m}$ ein maximales Ideal in A und $\hat{A}$ die Vervollständigung von A bezüglich $\mathfrak{m}$. Dann induziert jede R-Derivation von A nach M auf natürliche Weise eine R-Derivation von $\hat{A}$ nach $\hat{M}$.*

Beweis. Jede Derivation D auf A ist gleichmäßig stetig auf A bezüglich der $\mathfrak{m}$-adischen Topologien auf A bzw. M im folgenden Sinne: Für $a, b \in A, a - b \in \mathfrak{m}^n$ ist $D(a) - D(b) = D(a - b) \in \mathfrak{m}^{n-1}M$ aufgrund der Produktregel. Wir können also eine Derivation $\hat{D}$ auf $\hat{A}$ durch die Festlegung

$$\hat{D}(a) = \hat{D}(\lim a_n) := \lim D(a_n),$$

mit $a_n \in A, a \in \hat{A}$, definieren. Umgekehrt muss natürlich jede Fortsetzung von D diese Gleichung erfüllen. □

Als letztes untersuchen wir noch, wie sich der Modul der relativen 1-Formen des Quotienten einer R-Algebra nach einem Ideal berechnet. Sei also wie bisher A eine R-Algebra, $\mathfrak{a}$ ein Ideal in A und $B = A/\mathfrak{a}$. Dann gilt der folgende

Satz 1.14. *Mit den eben eingeführten Bezeichnungen gilt*

$$\Omega^1_{B/R} \simeq \Omega := \Omega^1_{A/R}/(\mathfrak{a}\Omega^1_{A/R} + Ad(\mathfrak{a})) \simeq (\Omega^1_{A/R} \otimes_A B)/Bd(\mathfrak{a}).$$

Zusammen mit der Abbildung $d_{B/R} : B \to \Omega$, welche von d induziert wird, bildet Ω den Modul der relativen 1-Formen von B über R.

Beweis. Klarerweise ist Ω ein B-Modul. Da weiters d eine R-Derivation ist, gilt dasselbe auch für die davon induzierte Abbildung $d_{B/R}$. Wir müssen also noch die universelle Eigenschaft von $d_{B/R}$ nachprüfen. Dazu betrachten wir eine R-Derivation $\bar{\delta} : B \to M$. Die Zusammensetzung $\delta = \bar{\delta} \circ \pi$ mit der Restklassenabbildung ist dann eine R-Derivation von A nach M, wobei wir M als A-Modul auffassen.

Aufgrund der universellen Eigenschaft, faktorisiert δ durch eine A-lineare Abbildung $\varphi : \Omega^1_{A/R} \to M$. Wegen $\delta(\mathfrak{a}) = 0$, und weil M ein Modul über B ist, gilt $\varphi(\mathfrak{a}\Omega^1_{A/R} + Ad(\mathfrak{a})) = 0$. Also induziert φ eine B-lineare Abbildung $\bar{\varphi} : \Omega \to M$ mit $\bar{\delta} = \bar{\varphi} \circ d_{B/R}$. Die Eindeutigkeit von $\bar{\varphi}$ folgt aus der Eindeutigkeit von φ. □

Eine äquivalente Formulierung des Satzes lautet: Die Folge von Abbildungen

$$\mathfrak{a}/\mathfrak{a}^2 \xrightarrow{d_{A/R}} B \otimes_A \Omega^1_{A/R} \to \Omega^1_{B/R} \to 0 \tag{1.4}$$

ist exakt. Den A-Modul $\mathfrak{a}/\mathfrak{a}^2$ nennt man auch den *Conormal-Modul* von B/A und die Folge (1.4) entsprechend die *Conormalfolge*.

Korollar 1.15. *Der Modul von 1-Formen einer endlich erzeugten R-Algebra ist endlich erzeugt.* □

Kapitel 2

Inseparable Körpererweiterungen

Die Betrachtungen in diesem Abschnitt sind motiviert durch folgende Beobachtungen. Sei K ein Körper der Charakteristik $p > 0$ und $L = K[X]/(f)$ eine einfache algebraische Körpererweiterung, $f \in K[X]$ irreduzibel. Dann induziert jede K-Derivation D von L in einen L-Vektorraum V eine K-Derivation von $K[X]$ nach V durch Zusammensetzung mit der Restklassenabbildung: $K[X] \to L \to V$ - siehe dazu auch den Beweis von Satz 1.14. Welche Derivationen existieren nun auf L?

Eine K-Derivation auf L muss als Derivation auf $K[X]$ klarerweise das Ideal (f) anullieren. Das Bild von f unter einer solchen Derivation D ist aber gerade $f'(X) \cdot D(X)$. Falls nun f ein separables Polynom ist, ist das Bild von $f'(X) \neq 0$ in L und es folgt $D(X) = 0$. Die triviale Derivation auf K lässt sich also nur trivial fortsetzen.

Ist andererseits $f = g(X^p)$ inseparabel, so ist $f'(X) = 0$ und die Bedingung $D(f(X)) = f'(X) \cdot D(X) = 0$ ist offensichtlich für eine beliebige Wahl von $D(X)$ erfüllt. Es gibt in diesem Fall also eine ganze Familie von Fortsetzungen der trivialen Derivation auf K.

Wir werden in diesem Kapitel sehen, dass die Eigenschaft einer Körpererweiterung, zu einer Derivation auf dem Grundkörper mehrere *verschiedene* Fortsetzungen zuzulassen, in der Tat charakteristisch für inseparable Körpererweiterungen ist.

Diese Vorbetrachtungen lassen weiters erkennen, dass es oft leichter ist, Fortsetzungen von gewissen Derivationen zu suchen, als den Vektorraum $\Omega^1_{L/K}$ direkt zu berechnen. Das heißt, wir möchten lieber den Dualraum $\mathrm{Der}_K(L, L) = \mathrm{Hom}_L(\Omega^1_{L/K}, L)$ (siehe Bemerkung 1.4) bestimmen. Im Fall endlich erzeugter Körpererweiterungen ist aber $\Omega^1_{L/K}$ wegen Korollar 1.15 ein endlich-dimensionaler L-Vektorraum, und daher kommen beide Betrachtungsweisen auf dasselbe hinaus - Raum und Dualraum sind in der endlich-dimensionalen Situation bekanntlich isomorph.

Wir untersuchen nun also das Fortsetzungsproblem für Derivationen auf eine Körpererweiterung.

Satz 2.1. *Es sei $K \subset L = K(x_j; j \in J)$ eine Körpererweiterung, J eine beliebige Indexmenge. Weiters sei mit $\mathfrak{X} = (X_j)_{j\in J}$ $\pi : K[\mathfrak{X}] \to L$ der Einsetzungshomomorphismus. Für eine Derivation $\delta : K \to V$ in einen L-Vektorraum V und ein System $(v_j)_{j\in J}$ von Elementen in V sind äquivalent:*

1. *δ setzt sich fort zu einer Derivation $\delta' : L \to V$*

2. Für $f \in \ker \pi$ gilt

$$f^\delta(x) + \sum_{j \in J} (\partial_j) f(x) \cdot v_j = 0, \quad f \in ker(\pi), \tag{2.1}$$

wobei f^δ das 'Polynom' mit Koeffizienten in V bezeichne, das durch Anwendung von δ auf die Koeffizienten von f entsteht.

Beweis. Gilt (1), so ist für ein beliebiges Polynom $f \in K[\mathfrak{X}]$

$$\delta'(f(x)) = f^\delta(x) + \sum \frac{\partial f}{\partial X_j}(x) \cdot v_j, \tag{2.2}$$

d.h., δ' ist als Fortsetzung zu δ eindeutig festgelegt. Unter Verwendung von Korollar 1.11 ergibt sich die Eindeutigkeit auf $K(x)$. Per definitionem ist $f(x) = 0$ für $f \in \ker \pi$ und daher gelten die Gleichungen in (2).
Umgekehrt können wir, wenn wir V via π als $K[\mathfrak{X}]$-Modul auffassen, durch die Gleichungen in (2.2) eine Derivation δ' von $K[\mathfrak{X}]$ nach V festlegen. Wenn (2) gilt, so verschwindet δ' auf dem Kern des Einsetzungshomomorphismus π und induziert daher eine Derivation δ' von $K[\mathfrak{X}]/\ker \pi$ nach V, welche δ fortsetzt. Wiederum durch Anwendung von Korollar 1.11 erhalten wir eine Fortsetzung von δ' auf L. □

Wir wollen daraus nun Aussagen über Moduln von Differentialformen herleiten. Als erstes formulieren wir das

Korollar 2.2. *Für eine separable algebraische Körpererweiterung L/K setzt sich jede Derivation von K in einen L-Vektorraum V auf eindeutige Weise fort zu einer Derivation von L nach V. Insbesondere ist dann $\Omega^1_{L/K} = 0$.*

Beweis. Wir überprüfen, dass für $x \in L$ die Fortsetzung einer Derivation $\delta \in \mathrm{Der}(K, V)$ auf $K(x)$ eindeutig bestimmt ist. Sei $f \in K[X]$ das Minimalpolynom von x. Die Bedingung aus Satz 2.1 für die Fortsetzbarkeit von δ lautet in diesem Fall

$$f^\delta(x) + f'(x) \cdot v = 0;$$

Da f separabel ist, gilt $f'(x) \neq 0$ und eine Fortsetzung von δ ist durch $\delta(x) = v$ eindeutig bestimmt. Dies zeigt insbesondere die Eindeutigkeit der Fortsetzung auf *beliebige* Zwischenkörper von K und L. Um auch die Existenz einer solchen Fortsetzung einzusehen, versehen die Menge

$$\mathfrak{Z} = \{(K', \delta_{K'}); K \subset K' \subset L, \delta_{K'} \text{ Fortsetzung von } \delta\}$$

mit einer partiellen Ordnungsrelation, gegeben durch

$$(K', \delta_{K'}) \leqslant (K'', \delta_{K''}) \Leftrightarrow K' \subset K'' \text{ und } \delta_{K''}|_{K'} = \delta_{K'}.$$

Jede aufsteigende Kette in dieser Menge besitzt ein Supremum, und daher existiert nach dem Lemma von Zorn ein maximales Element in $\mathfrak{Z}$. Dieses maximale Element muss aber schon (L, δ_L) sein, da wir ansonsten ja eine Fortsetzung von δ auf eine endliche Erweiterung dieses Elements finden könnten, im Widerspruch zu seiner Maximalität.

Da sich also insbesondere die triviale Derivation von K nach L nur trivial fortsetzen lässt, folgt $\Omega^1_{L/K} = 0$, wie behauptet. □

Im Fall inseparabler Körpererweiterungen ist die Sache interessanter:

Korollar 2.3. *Es sei K ein Körper der Charakteristik $p > 0$ und $L = K(x)/K$ eine rein inseparable Körpererweiterung vom Grad p mit Minimalpolynom $f = X^p - c \in K[X]$. Für eine Derivation $\delta \in \mathrm{Der}(K, V)$ in einen L-Vektorraum V gilt:*
Es existiert eine Fortsetzung von δ auf L genau dann, wenn $\delta(c) = 0$. In diesem Fall kann man die Fortsetzung für den Erzeuger x der Körpererweiterung beliebig wählen. Insbesondere ist dann $\Omega^1_{L/K}$ ein 1-dimensionaler L-Vektorraum mit Basis $d_{L/K}(x)$.

Beweis. Nach Satz 2.1 existiert eine Fortsetzung mit $\delta(x) = v \in V$ genau dann, wenn

$$-\delta(c) + px^{p-1} \cdot v = -\delta(c) = 0.$$

Diese Gleichung gilt dann aber unabhängig von der Wahl von $v \in V$. Somit sind $\mathrm{Der}_K(L, L)$ und $\Omega^1_{L/K} = \mathrm{Der}_K(L, L)^*$ 1-dimensional über L. □

Daraus erhalten wir nun eine Charakterisierung separabler bzw. inseparabler Körpererweiterungen durch den zugehörigen Modul der relativen 1-Formen:

Satz 2.4. *Es sei $L = K(x_1, \ldots, x_r)$ eine endlich erzeugte Körpererweiterung von K. Dann ist*

$$\mathrm{transdeg}_K L \leqslant \dim_L \Omega^1_{L/K} \leqslant r,$$

wobei $\mathrm{transdeg}_K L = \dim_L \Omega^1_{L/K}$ *genau dann gilt, wenn L/K separabel ist.*

Für den Beweis dieses Satzes verwenden wir ein vorbereitendes

Lemma 2.5. *Eine endlich erzeugte Körpererweiterung L/K ist genau dann separabel algebraisch, wenn $\Omega^1_{L/K} = 0$.*

Beweis. Das Lemma folgt aus Korollar 2.2 bzw. Korollar 2.3 und Korollar 1.12. □

Beweis des Satzes: Aus den Sätzen aus Kapitel 1 über die 1-Formen auf einer endlich erzeugten K-Algebra und die Fortsetzung auf deren Quotientenkörper folgt, dass $\Omega^1_{L/K}$ von den Elementen $d_{L/K}(x_1), \ldots, d_{L/K}(x_r)$ erzeugt wird, also gilt die 2. Ungleichung des Satzes. Wir wählen nun eine Transzendenzbasis $y_1, \ldots, y_k$ von L über K. Die Elemente $d_{L/K}(y_1), \ldots, d_{L/K}(y_k)$ sind dann linear unabhängig über L und wir sehen

$$\mathrm{transdeg}_K L = \mathrm{transdeg}_K K(y_1, \ldots, y_k) \leqslant dim_L \Omega^1_{L/K}.$$

Aus der exakten Folge

$$\Omega^1_{K(y_1,\ldots,y_k)/K} \otimes_{K(y_1,\ldots,y_k)} L \to \Omega^1_{L/K} \to \Omega^1_{L/K(y_1,\ldots,y_k)} \to 0$$

ergibt sich

$$\mathrm{transdeg}_K K(y_1, \ldots, y_k) = \dim_L \Omega^1_{K(y_1,\ldots,y_k)/K} \otimes_{K(y_1,\ldots,y_k)} L = \dim_L \Omega^1_{L/K}$$

genau dann, wenn $\Omega^1_{L/K(y_1,\ldots,y_k)} = 0$, was nach dem Lemma gleichbedeutend ist mit der Aussage, dass $L/K(y_1, \ldots, y_k)$ separabel, also L/K separabel ist. □

Kapitel 3

Derivationen auf algebraischen Varietäten

3.1 Derivationen und Vektorfelder auf Varietäten

In diesem Kapitel werden wir die Begriffe, die wir in Kapitel 1 eingeführt haben, auf die algebraisch-geometrische Situation übertragen und dort näher studieren. Insbesondere werden wir uns an Begriffsbildungen der Differentialgeometrie anlehnen und z.B. Derivationen auf Varietäten als Vektorfelder interpretieren. Wir beginnen mit einer kurzen Klärung der in diesem Kapitel verwendeten Begriffe, wobei wir uns im Wesentlichen an (Har00) orientieren.

Im gesamten Kapitel bezeichne k einen algebraisch abgeschlossenen Körper (beliebiger Charakteristik) und $k[x] = k[x_1, \ldots, x_n]$ den Polynomring in n Variablen über k. Bekanntlich ist $k[x]$ ein noetherscher Ring.

Definition 3.1 (algebraische Menge)**.** Sei $\mathfrak{a}$ ein Ideal in $k[x]$. Die gemeinsame Verschwindungsmenge in k^n aller Polynome in $\mathfrak{a}$ bezeichnen wir mit $V(\mathfrak{a})$. Eine Teilmenge X von k^n heißt *algebraische Menge*, wenn $X = V(\mathfrak{a})$ für ein Ideal $\mathfrak{a}$ in $k[x]$.

Definition 3.2 (Koordinatenring)**.** Umgekehrt können wir zu jeder algebraischen Menge X in k^n ihr *Verschwindungsideal* betrachten, nämlich das Ideal aller Polynome in $k[x]$, welche auf X verschwinden. Wir bezeichnen dieses Ideal mit $I(X)$. Den Faktorring $A(X) = k[x]/I(X)$ nennt man den *Koordinatenring* der algebraischen Menge X.

Definition 3.3 (affiner Raum)**.** Das System der algebraischen Mengen in k^n erfüllt die Axiome für die abgeschlossenen Mengen einer Topologie auf k^n. Diese Topologie heißt die *Zariski-Topologie* auf k^n. Der Raum k^n zusammen mit der Zariski-Topologie heißt n-dimensionaler *affiner Raum* über k. Wir bezeichnen ihn mit $\mathbb{A}_k^n$.

Natürlich ist damit auch jede algebraische Menge X in $\mathbb{A}_k^n$ ein topologischer Raum mit der von $\mathbb{A}_k^n$ induzierten Topologie. Man spricht kurz von der Zariski-Topologie auf X.

Definition 3.4 (algebraische Varietät)**.** Ist $\mathfrak{p}$ ein Primideal in $k[x]$ so nennt man die Verschwindungsmenge $X = V(\mathfrak{p})$ eine *(affine) algebraische Varietät.*

Bemerkung 3.5. Für eine algebraische Menge X in k^n sind äquivalent:

- X ist eine algebraische Varietät.
- X ist als topologischer Raum mit der Zariski-Topologie irreduzibel.

- Das Verschwindungsideal $I(X)$ ist prim.

Definition 3.6 (Dimension)**.** Die Dimension $\dim(X)$ einer algebraischen Menge X ist das Supremum aller m, sodass algebraische Varietäten X_i mit

$$X_0 \subsetneq \cdots \subsetneq X_m \subset X$$

existieren.

Bemerkung 3.7. Die Dimension von X ist gleich der Krull-Dimension des Koordinatenrings $A(X)$, also der maximalen Länge einer echt aufsteigenden Folge von Primidealen in $A(X)$.

Definition 3.8. Sei k vollkommen. Eine algebraische Varietät $X = V(f_1, \ldots, f_{n-r})$ heißt *glatt im Punkt* P, bzw. P heißt ein *glatter Punkt* von X, wenn der Rang der Jacobimatrix J von $(f_1, \ldots, f_{n-r})$ in P gleich $n - \dim(X)$ ist. Dies ist gleichzeitig der maximal mögliche Rang von J auf X. Eine algebraische Menge heißt *glatt*, wenn sie glatt in jedem Punkt ist. Ein Punkt auf X, der nicht glatt ist, heißt *singulär*. Die Menge aller singulären Punkte von X bezeichnen wir mit $\mathrm{Sing}(X)$.

Bemerkung 3.9. Die eben formulierte Rangbedingung an die Jacobimatrix ist unabhängig von der Wahl der Erzeuger des Verschwindungsideals von X.

In diesem Abschnitt bezeichne der Begriff 'Derivation' stets eine k-Derivation. Wenn wir von einer Derivation auf der algebraischen Menge X sprechen, so meinen wir eine Derivation auf dem Koordinatenring von X, also ein Element in $\mathrm{Der}_k(A(X), A(X))$ - analog im Fall der 1-Formen.

Aus der Differentialgeometrie ist bekannt, dass auf $\mathcal{C}^\infty$-Mannigfaltigkeiten Derivationen und Vektorfelder im Grunde dieselben Objekte sind. Insbesondere lassen sich Derivationen auf einzelnen Punkten auswerten, und das Resultat ist *ein* Tangentialvektor. Welche Operation der 'Auswertung' einer Derivation oder 1-Form in unserem Sinne entspricht, werden wir nun untersuchen. Wir beginnen mit dem Fall der 1-Formen:

Sei $A = A(X)$ der Koordinatenring einer algebraischen Menge X. Weiters sei $\mathfrak{m}$ ein maximales Ideal in A und $P = V(\mathfrak{m}) \in X$ der Punkt auf X, auf dem $\mathfrak{m}$ verschwindet. Nach dem Hilbertschen Nullstellensatz ist dann $A/\mathfrak{m}$ isomorph zu $k \hookrightarrow A$. Wir erhalten aus $\Omega^1_{A/k}$ den *Zariski-Cotangentialraum* in P, indem wir mit $A/\mathfrak{m}$ tensorieren:

Satz 3.10. *In der eben beschriebenen Situation ist* $\Omega^1_{A/k} \otimes_A A/\mathfrak{m}$ *als* k*-Vektorraum isomorph zu* $\mathfrak{m}/\mathfrak{m}^2$.

Beweis. Wir betrachten die Abbildung

$$\omega : \Omega^1_{A/k} \otimes_A A/\mathfrak{m} \xrightarrow{\simeq} \mathfrak{m}/\mathfrak{m}^2$$
$$(1 \otimes f - f \otimes 1) \otimes \alpha \mapsto \alpha(f - \bar{f}),$$

wobei $\bar{f}$ die Restklasse von f in $A/\mathfrak{m}$ bezeichne. In der gegebenen Situation liegt also $\bar{f}$ sogar in k und $f - \bar{f}$ daher in $\mathfrak{m}$. Die Abbildung ω ist damit wohldefiniert, k-linear und surjektiv - ein Urbild von $f \in \mathfrak{m}$ ist $(1 \otimes f - f \otimes 1) \otimes 1$. Zu zeigen ist noch die Injektivität. Wir stellen dazu fest, dass jedes Element in $\Omega^1_{A/k} \otimes_A A/\mathfrak{m}$ die Form $(1 \otimes f - f \otimes 1) \otimes \alpha$ hat. Nehmen wir nun an, es sei $f - \bar{f} \in \mathfrak{m}^2$ bzw. o.E.d.A $f - \bar{f} = gh, g, h \in \mathfrak{m}$. Dann ist

$$(1 \otimes f - f \otimes 1) \otimes \alpha = (1 \otimes (f - \bar{f}) - (f - \bar{f}) \otimes 1) \otimes \alpha =$$
$$= (1 \otimes gh - gh \otimes 1) \otimes \alpha = (g \otimes h + h \otimes g - 2gh \otimes 1) \otimes \alpha =$$
$$= (1 \otimes h - h \otimes 1) \otimes g\alpha + (1 \otimes g - g \otimes 1) \otimes h\alpha = 0.$$

□

Bemerkung 3.11 (Geometrische Interpretation). Für ein Element $f \in A$ ist das Differential in P gegeben durch

$$d_P(f) = f - f(P) = \omega(d_{A/k}(f) \otimes 1) \qquad \mod \mathfrak{m}_P^2.$$

Die Tensorbildung mit $k = A/\mathfrak{m}$ entspricht hier also der 'Auswertung' der 1-Form im Punkt P.

Die Auswertung einer Funktion in P kann übrigens analog beschrieben werden:

$$\begin{aligned} A \otimes_k A/\mathfrak{m} &\to A/\mathfrak{m} \to k \\ f \otimes \bar{1} &\mapsto \bar{f} \mapsto f(P). \end{aligned}$$

Statt $\omega(\eta \otimes 1)$ schreiben wir in Zukunft kurz $\eta(P)$ und nennen dies die *Auswertung* der 1-Form $\eta \in \Omega^1_{A/k}$ im Punkt P.

Auf ähnliche Weise lassen sich auch Derivationen in Punkten auf X auswerten: Es existiert eine kanonische Abbildung

$$\begin{aligned} \tilde{\omega} : Hom_A(\Omega^1_{A/k}, A) \otimes_A A/\mathfrak{m} &\to Hom_A(\Omega^1_{A/k} \otimes_A A/\mathfrak{m}, A \otimes_A A/\mathfrak{m}) \\ \varphi \otimes 1_{A/\mathfrak{m}} &\mapsto \varphi \otimes 1_{Hom(A/\mathfrak{m}, A/\mathfrak{m})}. \end{aligned}$$

(siehe Bou89, II, §5, No 3). Unter Verwendung der Dualität (1.4) aus Kapitel 1 können wir dies umformulieren zu

$$\begin{aligned} \omega : Der_k(A,A) \otimes_A A/\mathfrak{m} &\to (\mathfrak{m}/\mathfrak{m}^2)^* \\ D \otimes 1 &\mapsto (d_P(f) \mapsto \overline{D(f)}). \end{aligned} \tag{3.1}$$

Auch hier schreiben wir wieder kurz $D(P)$ für $\omega(D \otimes 1)$ und nennen diese Abbildung die *Auswertung* der Dervation D im Punkt P.

Nachdem wir nun gesehen haben wie sich Derivationen in einem Punkt auf X auswerten lassen, können wir Derivationen auf X tatsächlich als Vektorfelder auf X bzw. als Schnitte ins Tangentialbündel von X auffassen. Analog interpretieren wir 1-Formen auf X als Schnitte ins Cotangentialbündel von X. Eine detaillierte Ausführung dieser Interpretationen findet sich in (Eis95).

Achtung: Die Situation ist hier nicht ganz analog wie im Fall der 1-Formen. Wir erhalten hier im Allgemeinen *nicht* (wie man vielleicht erwarten würde) den gesamten Zariski-Tangentialraum durch Auswerten von Derivationen. Die Auswertungsabbildung auf dem Modul der Derivationen ist also im Allgemeinen *kein* Isomorphismus wie im dualen Fall der 1-Formen bzw. Differentiale. Dies untersuchen wir nun näher.

Beispiel 3.12. Sei $A = \mathbb{C}[x,y]/(y^2 - x^3)$ und D eine Derivation auf A (damit meinen wir also $\mathbb{C}$-Derivationen von A nach A). Dann gilt $2yD(y) = 3x^2D(x)$, wenn wir D als Derivation auf $\mathbb{C}[x,y]$ auffassen. Wenn wir nun $D(x)$ und $D(y)$ mit unbestimmten Koeffizienten ansetzen, sehen wir aus dieser Relation $\mod y^2 - x^3$, dass die konstanten Terme von $D(x)$ und von $D(y)$ verschwinden. Es ist also $\omega(D \otimes 1) = 0$ und wir erkennen, dass ω weder surjektiv noch injektiv ist.

Die eben betrachtete Varietät ist im Nullpunkt singulär. Tatsächlich ist die Singularität der Grund dafür, dass die Auswertungsabbildung im Nullpunkt nicht surjektiv ist ('In Charakteristik 0 sind alle Derivationen tangential an den singulären Ort', wie wir noch sehen werden). Sehr wohl surjektiv ist ω aber in glatten Punkten, wie wir nun zeigen. Sei im Folgenden X eine Varietät der Dimension d, und $A = A(X) = k[x]/\mathfrak{p}$ ihr Koordinatenring. Sei $\mathfrak{p} = (f_1, \ldots, f_r)$.

Lemma 3.13 (Existenzlemma)**.** *Sei $P \in X$ ein glatter Punkt und $\mathfrak{m} = \{f \in A; f(P) = 0\}$ das zu P gehörige maximale Ideal. Dann ist die oben beschriebene Abbildung ω ein Epimorphismus von k-Vektorräumen, d.h., es existieren Derivationen auf A, deren Auswertungen in P den Zariski-Tangentialraum aufspannen.*

Beweis. Wir konstruieren geeignete Derivationen auf A induktiv. Durch eine lineare Transformation der Koordinaten können wir erreichen, dass P der Nullpunkt ist, $\mathfrak{m} = (x_1, \ldots, x_n)$ und

$$\begin{aligned} f_i &\equiv x_i \mod \mathfrak{m}^2, \quad i = 1, \ldots, n-d \\ f_i &\equiv 0 \mod \mathfrak{m}^2, \quad i = n-d+1, \ldots, r. \end{aligned} \tag{3.2}$$

(evtl. mit Umnummerierung der f_i). Konkret suchen wir nun Derivationen $D_{n-d+1}, \ldots, D_n$, sodass mit $n - d + 1 \leqslant i, j \leqslant n$ gilt

$$D_i(P) = \omega(D_i \otimes 1) = (dx_j \mapsto \delta_{ij}),$$

oder gleichbedeutend:

$$D_i(x_j) \equiv \delta_{ij} \mod \mathfrak{m}. \tag{3.3}$$

Diese wollen wir nun induktiv konstruieren. Für beliebige $n - d + 1 \leqslant i, j \leqslant n$ gilt klarerweise schon

$$\partial_i x_j \equiv \delta_{ij} \mod \mathfrak{m}.$$

Das Problem an diesen Derivationen ist noch, dass sie die Polynome f_i i.A. nicht nach $\mathfrak{p}$ abbilden und damit $\mathfrak{p}$ nicht stabilisieren. Dies ist ist aber notwendig, um sie als Derivationen auf dem Faktorring A auffassen zu können. Wir wollen diesen Mangel durch sukzessives Anpassen dieser Derivationen beheben.

Wir setzen $D_i^{(0)} := \partial_i$ für $i = 1, \ldots, n$, definieren

$$D_i^{(1)} := (D_1^{(0)} f_1) D_i^{(0)} - (D_i^{(0)} f_1) D_1^{(0)} = (\partial_1 f_1)\partial_i - (\partial_i f_1)\partial_1$$

und stellen fest, dass $D_i^{(1)}(f_1) = 0$.

Diese Konstruktion führen wir fort, indem wir für $l = 1, \ldots, n-d$ und $i = l+1, \ldots, n$ rekursiv definieren:

$$D_i^{(l)} := (D_l^{(l-1)} f_l) D_i^{(l-1)} - (D_i^{(l-1)} f_l) D_l^{(l-1)}. \tag{3.4}$$

Wieder beobachten wir durch Induktion, dass die Derivationen $D_i^{(l)}$ auf $\{f_1, \ldots, f_l\}$ verschwinden und daher das Ideal $(f_1, \ldots, f_l)$ in sich selbst abbilden. Wir schreiben im Folgenden $D_i := D_i^{(n-d)}$ für $i = n-d+1, \ldots, n$.

Ebenfalls mit Induktion sieht man aus der Gleichung (3.4), dass Gleichung (3.3) gilt, speziell sogar $D_i(x_j) = 0$ für $j > i$. Wir haben also Derivationen auf A mit den gewünschten Eigenschaften gefunden, falls $n - d = r$, also X ein vollständiger Durchschnitt ist. In diesem Fall sind wir hiermit fertig.

Andernfalls müssen wir noch nachweisen, dass die eben konstruierten Derivationen auch auf den restlichen Erzeugern des Ideals $\mathfrak{p}$ verschwinden, d.h. $D_i(f_j) = 0$ für $j = n-d+1, \ldots, r$.

Sei o.E.d.A $j = n-d+1$. Wegen $\dim(X) = d < d+1$ verschwinden alle $(d+1)$-Minoren von J auf ganz X und sind daher $= 0$ in A. Wir fassen nun A als Unterring seines Quotientenkörpers $K := Q(A)$ auf und können so feststellen:

Die ersten $n-d+1$ Zeilen von J sind K-linear abhängig. Es gibt also Elemente $a_l, l = 1, \ldots, n-d$, und $c \neq 0$ in R, sodass

$$\sum_{l=1}^{d} a_l d(f_l) = c\, d(f_{n-d+1}),$$

da nach dem Beispiel 1.8 in Kapitel 1

$$d(f_l) = \operatorname{grad}(f_l) \cdot (d(x_1), \ldots, d(x_n))^T.$$

Jede Derivation, also insbesondere eine Derivation D_i, ist aber die Hintereinanderausführung der universellen Derivation d mit einem A-Homomorphismus, also gilt auch

$$cD_i(f_{n-d+1}) = \sum_{l=1}^{d} a_l D_i(f_l) = 0.$$

Da $c \neq 0$ und $k[x]$ ein Integritätsring ist, folgt $D_i(f_{n-d+1}) = 0$. Somit haben wir gezeigt, dass $D_i(f_j) = 0$ für alle $j = 1, \ldots, r$ und dass $D_i(\mathfrak{p}) \subset \mathfrak{p}$ für alle $i = n - d + 1, \ldots, n$.
Wir haben damit d Derivationen auf A konstruiert, die die Bedingung (3.3) erfüllen. □

Bemerkung 3.14. Ein anderer Beweis dieses Lemmas findet sich in (HM93, Kap. 2, 'Existence Lemma').

Für alles weitere nummerieren wir nun die Variablen x_j und die eben konstruierten Derivationen D_i, $i, j \in \{1, \ldots, d\}$ um:

$$D_{n-d+i} \rightsquigarrow D_i,$$
$$x_{n-d+j} \rightsquigarrow x_j.$$

Wir haben also für $i, j \in \{1, \ldots, d\}$

$$D_i(x_j) \equiv \delta_{ij} \mod \mathfrak{m}. \tag{3.5}$$

Wenn wir nun diese Derivationen als Derivationen auf dem lokalen Ring A_m interpretieren, was nach Korollar 1.10 möglich ist, so erhalten wir durch Linearkombination Derivationen von noch einfacherer Form: Wir betrachten die Matrix $\mathcal{D} = (D_i(x_j))_{ij})$. Wegen (3.5) ist $\det(\mathcal{D}) \equiv 1 \mod \mathfrak{m}$, also in $A_\mathfrak{m}$ invertierbar. Das heißt aber, dass wir aus den D_i A_m-Linearkombinationen $\tilde{D}_i$ bilden können, mit

$$\tilde{D}_i(x_j) = d_{ij}. \tag{3.6}$$

Diese Derivationen sind natürlich *keine* Derivationen auf A sondern lediglich Derivationen auf der Lokalisierung A_m! Wir werden diese später noch verwenden.

Im Beispiel 3.12 vor dem Lemma haben wir gesehen, dass die Auswertung globaler Derivationen in einem Punkt einer Varietät nicht notwendigerweise den Zariski-Tangentialraum liefert, sondern im Allgemeinen nur einen Unterraum. Nach dem Lemma erhalten wir aber zumindest in glatten Punkte den gesamten Zariski--Tangentialraum durch Auswerten globaler Derivationen. Dass über Körpern der Charakteristik 0 die glatten Punkte einer Varietät durch diese Eigenschaft schon *charakterisiert* werden, werden wir im nächsten Abschnitt zeigen (siehe auch HM93). In positiver Charakteristik ist die Situation nicht so klar.

3.2 Determinantenideale und singuläre Punkte

Wir verwenden dieselben Bezeichnungen wie im vorigen Kapitel, insbesondere sei X eine algebraische Menge über einem Körper k von beliebiger Charakteristik.

Definition 3.15. Sei D eine Derivation auf X und I ein Ideal in $A = A(X)$. Die Derivation D nennen wir *tangential* an I, falls $D(I) \subset I$. Ist I radikal, so sagen wir auch, D sei tangential an die algebraische Menge $V(I)$.

Aus dieser Definition folgt unmittelbar der

Hilfssatz 3.16. *Sei I ein Radikalideal in A und $D \in \mathrm{Der}_k(A,A)$ eine Derivation auf X, welche tangential an $V(I)$ ist. Dann ist D schon eine Derivation auf $V(I)$.* □

Sei $Y = Y_1 \cup \cdots \cup Y_l$ eine (Zariski-)abgeschlossene Menge in X. Dabei seien die Komponenten Y_i irreduzibel und paarweise nicht ineinander enthalten. Sei weiters $I = I(Y) = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_l$ mit $Y_i = V(\mathfrak{p}_i)$. Dann gilt

Hilfssatz 3.17. *Ist die Derivation D tangential an Y, so auch an Y_i für alle i.*

Interpretation: Derivationen, die tangential an eine abgeschlossene Menge sind, sind auch tangential an jede ihrer (endlich vielen) irreduziblen Komponenten.

Beweis. Wir wählen $f \in \mathfrak{p}_1$ und $g \in \mathfrak{p}_2 \cap \cdots \cap \mathfrak{p}_l$ so, dass $g \notin \mathfrak{p}_1$. Dann ist $fg \in I$ und es gilt

$$gD(f) + fD(g) = D(fg) \in I \subset \mathfrak{p}_1.$$

Da $\mathfrak{p}_1$ prim ist und $g \notin \mathfrak{p}_1$, folgt $D(f) \in \mathfrak{p}_1$. □

Hilfssatz 3.18. *Sei* $\mathrm{char}(k) = 0$*, I ein Ideal in A und D eine Derivation auf X, welche tangential an I ist. Dann ist D schon tangential an $V(I)$.*

Beweis. Es ist zu zeigen, dass D auch das Radikal von I stabilisiert. Sei also $f \in \sqrt{I}, f^m \in I$. Da D das Ideal I stabilisiert, gilt

$$D(\ldots(D(f))\ldots) = m!D(f)^m + fg \in I, \quad \text{für ein } g \in A(X).$$

Also verschwindet $m!D(f)^m + fg$, und damit auch $D(f)$, auf ganz $V(I)$. Nach dem Hilbertschen Nullstellensatz ist daher $D(f) \in \sqrt{I}$. □

Die Voraussetzung $\mathrm{char}(k) = 0$ ist dabei wesentlich! Betrachten wir z.B. das Ideal $I = (x^p)$ in $k[x]$, wobei $k[x]$ (hier ausnahmsweise) den Polynomring in einer Variablen bezeichne, über einem Körper k der Charakteristik $p > 0$. Die Derivation ∂_x ist offensichtlich tangential an I, aber nicht an $\sqrt{I} = (x)$. Wir werden später noch auf solche Ideale, die von p-ten Potenzen erzeugt werden, zurückkommen.

Unser nächstes Ziel ist es zu zeigen, dass Derivationen auf X über Körpern der Charakteristik 0 stets tangential an den singulären Ort $\mathrm{Sing}(X)$ sind.

Sei dazu $I = I(X) =< f_1, \ldots, f_r >$ und $J = (\partial_j f_i)_{ij}$ die Jacobimatrix von $I(X)$. Das r-te *Determinantenideal* von J ist das Ideal in A, welches von allen $r \times r$-Minoren der Matrix J erzeugt wird - nennen wir es kurz das *r-te Determinantenideal von X.*

Satz 3.19. *Ist $D \in \mathrm{Der}_k(A,A)$ eine Derivation auf X, so stabilisiert D alle Determinantenideale von X.*

Im Beweis verwenden wir die Einsteinsche Summationskonvention, d.h.: hochgestellte Indizes indizieren Zeilen, tiefgestellte Indizes indizieren Spalten von Matrizen. Kommt derselbe Index in einer Formel sowohl hochgestellt als auch tiefgestellt vor, so ist über diesen Index zu summieren. Für $r \times r$-Minoren von J schreiben wir kurz

$$M^{i_1\ldots i_r}_{j_1\ldots j_r} = \det(J^{i_p}_{j_q})_{p,q\in\{1,\ldots,r\}}.$$

Insbesondere ist $J^i_j = M^i_j$. Es gilt dann die einfache Formel

$$M^{i_1\ldots i_r}_{j_1\ldots j_r} = \sum (-1)^{k+l} M^{i_k}_{j_l} M^{i_1\ldots \hat{i_k}\ldots i_r}_{j_1\ldots \hat{j_l}\ldots j_r}, \tag{3.7}$$

wobei in diesem Fall *wahlweise* über k oder l zu summieren ist. Diese Formel ist gerade die Entwicklung der Determinante nach der k-ten Zeile bzw. l-ten Spalte

Beweis. Die Derivation D hat einen Repräsentanten der Form

$$\tilde{D} = c^k \partial_k \in \mathrm{Der}_k(k[x], k[x]), c^k \in k[x].$$

Es gilt $\tilde{D}(I) \subset I$, oder etwas genauer: $\tilde{D}(f^i) = a^i_k f^k$ mit $a^i_k \in k[x]$. Wegen $M^i_j = J^i_j$ ist

$$\tilde{D}(M^i_j) = c^k \partial_k \partial_j f^i = \partial_j(c^k \partial_k f^i) - \partial_j(c^k)\partial_k f^i =$$
$$= \partial_j(\tilde{D} f^i) - \partial_j(c^k)\partial_k f^i = (\partial_j a^i_k) f^k + a^i_k \partial_j f^k - \partial_j c^k \partial_k f^i,$$

d.h.,

$$D(M^i_j) = a^i_k M^k_j + b^k_j M^i_k, \tag{3.8}$$

wenn wir $b^k_j = -\partial_j c^k$ setzen.

Damit haben wir den Satz für das 1. Determinantenideal von J gezeigt.
Wir zeigen nun mittels Induktion, dass allgemein

$$D(M^{i_1\dots i_r}_{j_1\dots j_r}) = a^{i_1}_k M^{k i_2\dots i_r}_{j_1\dots j_r} + \cdots + a^{i_r}_k M^{i_1\dots i_{r-1}k}_{j_1\dots j_r} + b^k_{j_1} M^{i_1\dots i_r}_{k j_2\dots j_r} + \cdots + b^k_{j_r} M^{i_1\dots i_r}_{j_1\dots j_{r-1}k}$$

gilt. Daraus folgt der Satz.

Nach Formel (3.7) gilt für einen $r+1$-Minor

$$D(M^{i_0\dots i_r}_{j_0\dots j_r}) = \sum_k (-1)^{k+l}(D(M^{i_k}_{j_l}) M^{i_0\dots \hat{i_k}\dots i_r}_{j_0\dots \hat{j_l}\dots j_r} + M^{i_k}_{j_l} D(M^{i_0\dots \hat{i_k}\dots i_r}_{j_0\dots \hat{j_l}\dots j_r})) =$$

$$= \sum_k (-1)^{k+l}(a^{i_k}_m M^m_{j_l} + b^m_{j_l} M^{i_k}_m) M^{i_0\dots \hat{i_k}\dots i_r}_{j_0\dots \hat{j_l}\dots j_r} +$$
$$+ \sum_k (-1)^{k+l} M^{i_k}_{j_l} [a^{i_0}_m M^{m i_1\dots \hat{i_k}\dots i_r}_{j_0\dots \hat{j_l}\dots j_r} + \cdots + a^{i_r}_m M^{i_0\dots \hat{i_k}\dots i_{r-1} m}_{j_0\dots \hat{j_l}\dots j_r} +$$
$$+ b^m_{j_0} M^{i_0\dots \hat{i_k}\dots i_r}_{m j_1\dots \hat{j_l}\dots j_r} + \cdots + b^m_{j_r} M^{i_0\dots \hat{i_k}\dots i_r}_{j_0\dots \hat{j_l}\dots j_{r-1} m}] =$$

$$= \sum_k (-1)^{k+l}[a^{i_k}_m M^m_{j_l} M^{i_0\dots \hat{i_k}\dots i_r}_{j_0\dots \hat{j_l}\dots j_r} + M^{i_k}_{j_l}(a^{i_0}_m M^{m i_1\dots \hat{i_k}\dots i_r}_{j_0\dots \hat{j_l}\dots j_r} + \cdots + a^{i_r}_m M^{i_0\dots \hat{i_k}\dots i_{r-1} m}_{j_0\dots \hat{j_l}\dots j_r})] +$$
$$+ \sum_k (-1)^{k+l}[b^m_{j_l} M^{i_k}_m M^{i_0\dots \hat{i_k}\dots i_r}_{j_0\dots \hat{j_l}\dots j_r} + M^{i_k}_{j_l}(b^m_{j_0} M^{i_0\dots \hat{i_k}\dots i_r}_{m j_1\dots \hat{j_l}\dots j_r} + \cdots + b^m_{j_r} M^{i_0\dots \hat{i_k}\dots i_r}_{j_0\dots \hat{j_l}\dots j_{r-1} m})] =$$

$$= a^{i_0}_m M^{m i_1\dots i_r}_{j_0\dots j_r} + \cdots + a^{i_r}_m M^{i_0\dots i_{r-1} m}_{j_0\dots j_r} + b^m_{j_0} M^{i_0\dots i_r}_{m j_1\dots j_r} + \cdots + b^m_{j_r} M^{i_0\dots i_r}_{j_0\dots j_{r-1} m} \qquad \blacksquare$$

Beachte für die letzte Identität z.B.:

1.

$$(-1)^l a^{i_0}_m M^m_{j_l} M^{\hat{i_0} i_1\dots i_r}_{j_0\dots \hat{j_l}\dots j_r} + \sum_{k=1}^r (-1)^{k+l} a^{i_0}_m M^{i_k}_{j_l} M^{m i_1\dots \hat{i_k}\dots i_r}_{j_0\dots \hat{j_l}\dots j_r} =$$
$$= a^{i_0}_m \sum_{k=0}^r (-1)^{k+l} M^{i_k}_{j_l} M^{m i_1\dots \hat{i_k}\dots i_r}_{j_0\dots \hat{j_l}\dots j_r} = a^{i_0}_m M^{m i_1\dots i_r}_{j_0\dots j_r},$$

und analog für die weiteren Terme mit Koeffizienten $a^{i_k}_m$.

2. Für die Terme mit Koeffizienten $b^m_{j_l}$ ist die Sache etwas einfacher, z.B.

$$\sum_k (-1)^{k+l} M^{i_k}_{j_l} b^m_{j_0} M^{i_0 \dots \hat{i_k} \dots i_r}_{m j_1 \dots \hat{j_l} \dots j_r} =$$
$$= b^m_{j_0} \sum_k (-1)^{k+l} M^{i_k}_{j_l} M^{i_0 \dots \hat{i_k} \dots i_r}_{m j_1 \dots \hat{j_l} \dots j_r} = b^m_{j_0} M^{i_0 \dots i_r}_{m j_1 \dots j_r}.$$

Damit ist der Satz bewiesen. □

Eine Derivation auf X ist also tangential an alle Determinantenideale von X. Wenn X eine Varietät ist und $d = \dim(X)$, so ist die gemeinsame Verschwindungsmenge aller $d \times d$-Minoren von J gerade der singuläre Ort von X. Zusammen mit Hilfssatz 3.18 erhalten wir also das

Korollar 3.20. *Sei* $\mathrm{char}(k) = 0$ *und* D *eine Derivation auf* X*. Dann ist* D *tangential an* $\mathrm{Sing}(X)$*.* □

Wir kommen nun zur angekündigten Charakterisierung singulärer Punkte durch die Dimension des Raumes der Auswertungen von globalen Derivationen.

Satz 3.21. *Sei* $\mathrm{char}(k) = 0$*,* X *eine Varietät und* $d = \dim(X)$*. Bezeichne weiters* $\mathbb{D}_X(P)$ *den* k*-Vektorraum, der von allen Auswertungen von Derivationen auf* X *in* P *aufgespannt wird. Dann ist* P *genau dann singulär, wenn* $\dim_k \mathbb{D}_X(P) < d$*.*

Beweis. Aus dem Existenzlemma 3.13 folgt, dass für glatte Punkte $\dim_k \mathbb{D}_X(P) = d$ ist. Sei nun umgekehrt $P \in Y$, Y eine irreduzible Komponente von $\mathrm{Sing}(X)$ und D eine Derivation auf X. Nach dem Korollar ist dann D schon eine Derivation auf $\mathrm{Sing}(X)$ und weiters nach Hilfssatz 3.17 eine Derivation auf Y. Die Auswertung einer Derivation auf X in $P \in Y$ liefert den Tangentialvektor

$$(d\bar{f} \mapsto \overline{D(f)}) \in (\overline{\mathfrak{m}}/\overline{\mathfrak{m}}^2)^*, \bar{f} \in A(Y)$$

und liegt also im Zariski-Tangentialraum an P *bezüglich* Y. Dieser Raum hat aber Dimension $\dim(Y) < d$, falls P glatt in Y ist. Für $P \in \mathrm{Sing}(Y)$ verfahren wir analog und sehen, dass tatsächlich $\dim_k \mathbb{D}_X(P) < d$, falls $P \in \mathrm{Sing}(X)$. □

Ein analoges Resultat im Fall von Keimen analytischer Varietäten über $\mathbb{C}$ findet sich in (HM93, Prop. 2.2).

Mit einem ähnlichen Argument erhalten wir

Satz 3.22. *Sei* $\mathrm{char}(k)$ *beliebig und* X *eine Varietät. Der singuläre Ort von* X *ist die größte echte abgeschlossene Teilmenge von* X*, an die alle Derivationen von* X *tangential sind. Insbesondere existieren keine solchen Teilmengen, wenn* X *glatt ist.*

Beweis. Die Verschwindungsmenge $V(I)$ sei unter allen Derivationen stabil. Wie im Beweis des vorhergehenden Satzes sehen wir, dass dann für $P \in V(I)$ gilt

$$\dim_k \mathbb{D}_X(P) < d.$$

Dies ist aber nach dem Existenzlemma 3.13 nur in singulären Punkten möglich. □

Insbesondere existieren im Fall $\mathrm{char}(k) = 0$ im Koorinatenring einer glatten Varietät keine echten Ideale, an die alle Derivationen tangential sind. Mit einem solchen Ideal I hätte nämlich auch sein Radikal $\sqrt{I}$ diese Eigenschaft. Das würde bedeuten, dass alle Derivationen tangential an die Varietät $V(I)$ sind, und daher $V(I) \subset \mathrm{Sing}(X) = \emptyset$, bzw. $I = A$.

Fundamental anders ist die Situation über Körpern positiver Charakteristik. In diesem Fall existieren sehr wohl Ideale im Koorinatenring einer glatten Varietät, die von allen Derivationen stabilisiert werden. Nach unseren bisherigen Überlegungen sind dies sicher keine Radikalideale. Im nächsten Abschnitt werden wir diese Ideale genauer untersuchen und charakterisieren.

Das Studium der Determinantenideale von X liefert aber noch ein anderes interessantes Resultat über die Struktur der Moduln $\Omega^1_{A/k}$ und $\mathrm{Der}_k(A,A)$ einer algebraischen Varietät. Wir zitieren dazu zwei Resultate aus der Theorie der Fitting-Ideale (siehe z.B. Eis95, Kap. 20.1):

Hilfssatz 3.23. *Sei $F \xrightarrow{\varphi} G \to M \to 0$ eine endliche Präsentierung des R-Moduls M mit freien R-Moduln F und G. Bezeichne r den Rang von G und $\mathrm{Fitt}_l(M)$ das $(r-l)$-te Determinantenideal einer Matrix von φ. Dann ist $\mathrm{Fitt}_l(M)$ unabhängig von der Wahl der Präsentierung und der Matrix von φ und damit eine Invariante des Moduls M.* □

Man nennt $\mathrm{Fitt}_l(M)$ das l-te *Fitting-Ideal* von M. Es gilt die Kette von Inklusionen

$$0 \subset \mathrm{Fitt}_0(M) \subset \cdots \subset \mathrm{Fitt}_r(M).$$

Satz 3.24. *(Eis95, Prop. 20.8) Der Modul M ist projektiv vom Rang r genau dann, wenn $0 = \mathrm{Fitt}_{r-1}(M) \subset \mathrm{Fitt}_r(M) = R$.* □

Betrachten wir diese Resultate nun im Fall $M = \Omega^1_{A/k}$. Die Conormalfolge (1.4) liefert eine Präsentierung von $\Omega^1_{A/k}$ mit $F = A^r, G = A \otimes_{k[x]} \Omega^1_{k[x]/k} \simeq A^n$, und

$$\varphi : e_i \mapsto \partial_1 f_i dx_1 + \cdots + \partial_n f_i dx_n.$$

Das l-te Fitting-Ideal von $\Omega^1_{A/k}$ ist also gerade das $(n-l)$-te Determinantenideal von J bzw. X.

Ist nun X eine *glatte* Varietät der Dimension d, so bedeutet dies, dass das $(n-d)$-te Determinantenideal von X bzw. $\mathrm{Fitt}_d(\Omega^1_{A/k})$ nirgends auf X verschwindet. Nach dem Hilbertschen Nullstellensatz ist dieses Ideal also schon der ganze Ring A. Außerdem ist klarerweise $\mathrm{Fitt}_{d-1}(\Omega^1_{A/k}) = 0$. Zusammen mit Satz 3.24 erhalten wir also

Satz 3.25. *Der Modul der Kähler-Differentiale auf der Varietät X ist projektiv vom Rang $\dim(X)$ genau dann, wenn X glatt ist.* □

Falls X glatt ist, spaltet also die exakte Folge

$$0 \to d_{k[x]/k}(\mathfrak{a}) \hookrightarrow A \otimes_{k[x]} \Omega^1_{k[x]/k} \to \Omega^1_{A/k} \to 0$$

(gewonnen aus der Conormalfolge (1.4)) auf, und wir sehen, dass

$$A \otimes_{k[x]} \Omega^1_{k[x]/k} \simeq d_{k[x]/k}(\mathfrak{a}) \oplus \Omega^1_{A/k},$$

bzw. durch Dualisieren:

$$\mathrm{Der}_k(k[x], A) \simeq \mathrm{Hom}_A(d_{k[x]/k}(\mathfrak{a}/\mathfrak{a}), A) \oplus \mathrm{Der}_k(A, A).$$

Den Modul $\mathrm{Der}_k(k[x], A)$ interpretieren wir dabei als den Modul von Schnitten ins (triviale) Tangentialbündel von $\mathbb{A}^n_k$, eingeschränkt auf die Varietät X.

Um die Situation zu illustrieren geben wir ein

Beispiel 3.26. Sei $f = x^2 + y^2 + z^2 - 1 \in \mathbb{C}[x, y, z]$ und $A = \mathbb{C}[x, y, z]/(f)$. Die 'komplexe Kugel' $V(f)$ ist glatt und von der komplexen Dimension 2. In diesem Fall ist $(f)/(f)^2 \simeq \mathbb{C}[x, y, z]/(f) = A$ und die universelle Derivation $d_{\mathbb{C}[x]/\mathbb{C}}$ ist auf $(f)/(f)^2$ injektiv. Wir haben die aufspaltende exakte Folge

$$0 \to (f)/(f)^2 \xrightarrow{d} \Omega^1_{\mathbb{C}[x,y,z]/\mathbb{C}} \otimes_{\mathbb{C}[x,y,z]} A \to \Omega^1_{A/\mathbb{C}},$$

mit $d(f) = 2(xdx + ydy + zdz)$. Dual zu diesem Differential ist offensichtlich die Derivation (bzw. das Vektorfeld) $\frac{1}{2}(x, y, z)^T$, also ein Vektorfeld, welches in jedem Punkt normal auf die Varietät steht. Es lässt sich also $\mathrm{Hom}_A((df), A)$ als der Modul der Schnitte ins Normalenbündel von X auffassen, während, wie wir schon diskutiert haben, $\mathrm{Der}_{\mathbb{C}}(A, A)$ der Modul der Schnitte ins Tangentialbündel von X ist. Die direkte Summe dieser beiden Moduln liefert den freien Modul vom Rang 3 der Schnitte ins triviale Bündel über $\mathbb{A}^3_{\mathbb{C}}$, eingeschränkt auf X. Die Situation ist also ganz analog wie im (anschaulicheren) reellen Fall.

3.3 Eine Charakterisierung von Idealen, die von p-ten Potenzen erzeugt werden

Die Frage, die wir uns in diesem Abschnitt stellen, ist die folgende: Sei A der Koordinatenring einer *glatten* algebraischen Varietät über einem algebraische abgeschlossenen Körper k. Welche sind im Fall $\mathrm{char}(k) = p > 0$ die Ideale, an die alle Derivationen tangential sind?

Sei also A der Koordinatenring einer glatten algebraischen Varietät über einem algebraische abgeschlossenen Körper k der Charakteristik $p > 0$ ('globaler Fall'), oder die Lokalisierung eines solchen in einem maximalen Ideal $\mathfrak{m}$ ('lokaler Fall').

Satz 3.27. *Die Ideale in A, welche ein Erzeugendensystem aus p-ten Potenzen von A besitzen, sind genau die, an die jede Derivation auf A tangential ist.*

Bemerkung 3.28. Eine Verallgemeinerung dieses Satzes für Differentialoperatoren höherer Ordnung findet sich in (Kaw06, Prop. 1.3.1.2).

Beweis. Eine Implikation ist einfach: Ist D eine Derivation auf A und $r \in A$, so ist $D(r^p) = pr^{p-1}D(r) = 0$ und nach der Produktregel gilt

$$D(sr^p) = D(s)r^p, s \in A.$$

Daher ist jedes Ideal I, das von p-ten Potenzen erzeugt wird, unter D stabil, d.h. D ist tangential an I.

Für die umgekehrte Richtung erinnern wir zunächst an einen Satz aus der kommutativen Algebra (siehe z.B. Lor96, Kap. II.8):

Lemma 3.29. *Seien A ein kommutativer Ring und M und N zwei A-Moduln. Ein Homomorphismus $\varphi : M \to N$ ist injektiv bzw. surjektiv genau dann, wenn für alle maximalen Ideale $\mathfrak{m}$ in A die lokalisierte Abbildung $\varphi_{\mathfrak{m}} : M_{\mathfrak{m}} \to N_{\mathfrak{m}}$ injektiv bzw. surjektiv ist.*

Diese Aussage folgt im wesentlichen aus der Tatsache, dass die Lokalisierung ein exakter Funktor ist, und dass ein A-Modul verschwindet, wenn alle seine Lokalisierungen nach maximalen Idealen von A verschwinden. □

Insbesondere gilt also für zwei Ideale $\mathfrak{b} \subset \mathfrak{a}$ genau dann $\mathfrak{b} = \mathfrak{a}$, wenn $A_\mathfrak{m}\mathfrak{b} = A_\mathfrak{m}\mathfrak{a}$ für alle maximalen Ideale $\mathfrak{m}$ in A. Diese Feststellung verwenden wir, um den globalen Fall des Satzes 3.27 aus dem lokalen zu folgern.

Nehmen wir dazu an, wir hätten die Aussage des Satzes im lokalen Fall (also für beliebige Lokalisierungen $A_\mathfrak{m}$ einer endlich erzeugten k-Algebra A) bereits bewiesen. Ist dann $\mathfrak{a}$ ein Ideal in A, das von allen Derivationen stabilisiert wird, so wird, wieder wegen Korollar 1.10 und der Produktregel, auch das Ideal $A_\mathfrak{m}\mathfrak{a}$ von allen Derivationen auf $A_\mathfrak{m}$ stabilisiert ($\mathfrak{m}$ in A maximal). Wir können dann schließen, dass das Ideal $A_\mathfrak{m}\mathfrak{a}$ von p-ten Potenzen in $A_\mathfrak{m}$, bzw. sogar von p-ten Potenzen, welche in $\mathfrak{a}$ liegen, erzeugt wird (indem wir Nenner geeignet wegmultiplizieren). Sei

$$E_\mathfrak{m} = \{f_{\mathfrak{m},i}^p; i = 1, \ldots, l_\mathfrak{m}, f_{\mathfrak{m},i} \in A\} \tag{3.9}$$

ein solches Erzeugendensystem von $A_\mathfrak{m}$. Wir betrachten nun das von allen solchen Erzeugendensystemen $E_\mathfrak{m}$ gemeinsam in A erzeugte Ideal $\mathfrak{b}$ und behaupten, dass $\mathfrak{a} = \mathfrak{b}$ ist. Denn nach Konstruktion ist $\mathfrak{b} \subset \mathfrak{a}$ und außerdem $A_\mathfrak{m}\mathfrak{a} = A_\mathfrak{m}\mathfrak{b}$ für alle maximalen Ideale $\mathfrak{m}$ in A. Damit folgt $\mathfrak{a} = \mathfrak{b}$ aus dem Lemma 3.29 und wir sehen, dass $\mathfrak{a}$ von p-ten Potenzen erzeugt wird.

Wir müssen also nur noch den lokalen Fall untersuchen. Sei dazu ein maximales Ideal $\mathfrak{m}$ in A fix gewählt und $A_\mathfrak{m}$ die Lokalisierung in $\mathfrak{m}$. Aus dem Lemma von Nakayama ($A_\mathfrak{m}$ ist ein noetherscher lokaler Ring!) folgt $\cap_{n\in\mathbb{N}}\mathfrak{m}^n = 0$, und daher ist $A_\mathfrak{m}$ ein Unterring der Vervollständigung $\widehat{A_\mathfrak{m}}$ bezüglich der $\mathfrak{m}$-adischen Topologie.

Wir wählen nun in der k-Algebra A wieder spezielle Koordinaten, sodass $A = k[x_1, \ldots, x_n]/(f_r, \ldots, f_n)$, $\mathfrak{m} = (x_1, \ldots, x_n)$ und

$$\begin{aligned} f_i &\equiv x_i \mod \mathfrak{m}^2, i = n-d+1, \ldots, n \\ f_i &\equiv 0 \mod \mathfrak{m}^2, i = r, \ldots, n-d+1. \end{aligned} \tag{3.10}$$

Hilfssatz 3.30. *Die kanonische Abbildung $\varphi : k[[x_1, \ldots, x_d]] \to \widehat{A_\mathfrak{m}}$ ist ein Isomorphismus. Außerdem ist $\widehat{A_\mathfrak{m}}/\widehat{A_\mathfrak{m}}^p$ ein k-Vektorraum, der von den Elementen $\prod x_i^{e_i}, 0 \leqslant e_i \leqslant p-1$ erzeugt wird.*

Beweis. Da wir die Relationen der Algebra A in (3.10) entsprechend gewählt haben, ist φ offensichtlich injektiv. Indem wir die Variablen $x_{n-d+1}, \ldots, x_n$ sukzessive unter Verwendung der Relationen (3.10) durch Elemente in $\mathfrak{m}^2$ ersetzen, sehen wir, dass die Abbildung auch surjektiv ist. □

Wir erinnern uns: In (3.5) haben wir Derivationen auf der Lokalisierung $A_\mathfrak{m}$ von der Form

$$D_i(x_j) = \delta_{ij}, \quad i, j \in 1, \ldots, d \tag{3.11}$$

konstruiert. Entsprechend dem Hilfssatz betrachten wir nun $A_\mathfrak{m}$ als Unterring von $k[[x_1, \ldots, x_d]]$ und stellen fest: Diese Derivationen sind auf $k[[x_1, \ldots, x_d]]$ nichts anderes als die gewöhnlichen Ableitungen nach den einzelnen Variablen. Der entscheidende Punkt aber, der aus unseren bisherigen Überlegungen folgt ist, dass der Unterring $A_\mathfrak{m}$ von diesen Derivationen *stabilisiert* wird.

Sei nun $\mathfrak{a}$ ein Ideal in $A_\mathfrak{m}$, das von allen Derivationen auf $A_\mathfrak{m}$ stabilisiert wird. Sei weiters $\hat{\mathfrak{a}} = \widehat{A_\mathfrak{m}}\mathfrak{a}$ das von $\mathfrak{a}$ in $\widehat{A_\mathfrak{m}}$ erzeugte Ideal. Unter Beachtung der Produktregel sehen wir nun aber, dass auch das Ideal $\hat{\mathfrak{a}}$ unter den Derivationen $D_i, i = 1, \ldots, d$ stabilisiert wird.

Jedes Element $f \in \widehat{A_\mathfrak{m}}$ lässt sich entsprechend der zweiten Aussage im Hilfssatz als eine Linearkombination

$$f = \sum_{e \in \{0,\dots,p-1\}^d} x^e \cdot g_e^p, \quad g_e \in \widehat{A_\mathfrak{m}} \tag{3.12}$$

darstellen. Insbesondere lässt sich auch jedes Element $f \in \mathfrak{a}$ auf diese Weise darstellen. Indem wir darauf geeignete Hintereinanderausführungen der Derivationen $D_i, i = 1, \dots, d$ anwenden, sehen wir, dass mit f auch schon *jeder* der Koeffizienten g_e^p in $\widehat{A_\mathfrak{m}}\mathfrak{a}$ enthalten sein muss. Da die verwendeten Derivationen aber Derivationen auf $A_\mathfrak{m}$ sind und daher $A_\mathfrak{m}$ stabilisieren, sind die Koeffizienten g_e^p schon in $\widehat{A_\mathfrak{m}}\mathfrak{a} \cap A_\mathfrak{m} = \mathfrak{a}$ enthalten.

Es bleibt noch die Frage, ob nicht nur die Elemente g_e^p, sondern auch schon ihre p-ten Wurzeln g_e in $A_\mathfrak{m}$ liegen. Falls ja, wäre $\mathfrak{a}$ tatsächlich von p-ten Potenzen in $A_\mathfrak{m}$ erzeugt und der Satz wäre bewiesen. Die gewünschte positive Antwort auf diese Frage liefert nun das

Lemma 3.31. *$A_\mathfrak{m} \cap (\widehat{A_\mathfrak{m}})^p = A_\mathfrak{m}^p$, wobei das p im Exponenten jeweils den Ring der p-ten Potenzen bezeichne.*

Beweis. Wir erinnern: Es ist $\widehat{A_\mathfrak{m}} = k[[x_1, \dots, x_d]]$ der Potenzreihenring in d Variablen. Seien nun f und g Polynome in den Variablen $x_1, \dots, x_d$ so, dass $g(0) \neq 0$ und $\frac{f}{g} = P$ eine Potenzreihe in $\widehat{A_\mathfrak{m}}^p$ ist. Wir zeigen, dass P schon ein Quotient von Polynomen in x_i^p ist, also in $A_\mathfrak{m}^p$ liegt.
Wir setzen f, g und P mit unbestimmten Koeffizienten an (und verwenden dabei i als Multiindex):

$$\begin{aligned} f &= \sum a_i x^i, \\ g &= \sum b_i x^i, \\ P &= \sum c_{pi} x^{pi}, \end{aligned}$$

wobei die ersten beiden Summen natürlich endlich sind, die letzte Summe i.a. aber unendlich ist (andernfalls wäre nichts mehr zu zeigen). Aus der Gleichung $f = gP$ folgt für genügend große Multiindizes i: $0 = a_i = \sum_{k+j=i} b_k c_j$, bzw., wenn wir nur Multiindizes der Form $p \cdot i$ beachten:

$$0 = a_{pi} = \sum_{k+j=i} b_{pk} c_{pj}.$$

Indem wir höchstens endlich viele Koeffizienten c_{pj} abändern (d.h. wir ersetzen P durch $P - h$, h Polynom in x^p), erreichen wir sogar

$$\begin{aligned} 1 &= b_0 c_0, \\ 0 &= \sum_{k+j=i} b_{pk} c_{pj}, i \neq 0. \end{aligned}$$

Das ist aber gleichbedeutend mit $P - h = (\sum_k b_{pk} x^{pk})^{-1}$. Also liegt P tatsächlich in $A_\mathfrak{m}^p$, woraus das Lemma folgt. □

Wir haben den Satz dieses Kapitels damit vollständig bewiesen.

Bemerkung 3.32. Wenn man diesen Beweis und die Konstruktion der zugehörigen Derivationen in den lokalen Ringen genauer studiert, erkennt man, dass wir an keiner wesentlichen Stelle die algebraische Abgeschlossenheit von k verwendet haben. Der Satz gilt in gleicher Weise also auch für eine Varietät über einem nicht algebraisch abgeschlossenen Körper k, wenn wir die Bedingung 'von p-ten Potenzen erzeugt' ersetzen durch 'von Elementen erzeugt, welche bei algebraischem Abschluss des Koeffizientenkörpers p-te Potenzen sind'.

Zum Abschluss wollen wir dieses Ergebnis noch im Fall endlich erzeugter algebraischer Körpererweiterungen interpretieren:
Sei k ein *nicht* algebraisch abgeschlossener Körper der Charakteristik $p > 0$ und l eine endliche Körpererweiterung $l \supset k$. Ein Erzeugendensystem $\alpha_1, \ldots, \alpha_n$ von l über k liefert uns eine natürliche Abbildung

$$s : k[x_1, \ldots, x_n] \to l; x_i \mapsto \alpha_i.$$

In Analogie zu den Bezeichnungen im vorigen Satz schreiben wir $A := k[x_1, \ldots, x_n]$ bzw. $I := \ker(s)$.

In dieser Situation gilt nun der

Satz 3.33. *Folgende Aussagen sind äquivalent:*

1. $\Omega^1_{A/k}/(I\Omega^1_{A/k}) \simeq \Omega^1_{A/k} \otimes_A l$.
2. $d_{A/k}(I) \subset I\Omega^1_{A/k}$.
3. *I wird von Polynomen in $k[x_1^p, \ldots, x_n^p]$ erzeugt.*

Sind diese Bedingungen erfüllt, so sind alle $\alpha_i, i = 1, \ldots, n$, inseparabel über k.

Bemerkung 3.34. Dieser Satz verallgemeinert die Tatsache, dass eine *einfache* algebraische Erweiterung genau dann inseparabel ist, wenn das Minimalpolynom des Erzeugers ein Polynom in x^p ist. Genau dann ist nach Kapitel 2 die Dimension $\dim_l \Omega^1_{l/k} = 1$; im separablen Fall wäre diese Dimension gleich 0.

Nun zum

Beweis. Die Aussage von Satz 1.14 liefert in unserer Situation einen l-linearen Isomorphismus

$$(\Omega^1_{A/k}/(I\Omega^1_{A/k}))/\overline{A \cdot d_{A/k}} \simeq \Omega^1_{l/k}$$

für die l-Vektorräume $\Omega^1_{A/k}/(I\Omega^1_{A/k})$ bzw. $\overline{A \cdot d_{A/k}}$. Daher gilt offensichtlich (1) $\Leftrightarrow$ (2).
Die Äquivalenz (2) $\Leftrightarrow$ (3) folgt im wesentlichen aus dem vorigen Satz: Aussage (3) bedeutet demnach, dass das Ideal I von allen k-Derivationen von A stabilisiert wird, bzw., dass $d_{A/k}(I)$ von allen $\varphi \in Hom_A(\Omega^1_{A/k}, A)$ nach I abgebildet wird. Da aber $\Omega^1_{A/k}$ frei ist, ist dies äquivalent zur Aussage (2).
Wir zeigen noch, dass unter diesen Umständen alle α_i inseparabel über k sind, indem wir o.E.d.A. annehmen, α_1 sei separabel über k. Das Ideal I enthält dann das Minimalpolynom f von α_1 in $k[x_1] \subset A$ und dies ist das Polynom kleinsten Grades in $k[x_1] \cap I$. Da aber α separabel ist, liegt f nicht in $k[x_1^p]$, und es ist $\partial_{x_1}(f) \neq 0$ vom Grad echt kleiner als $\deg(f)$. Das Differential $d_{A/k}(f)$ liegt also nicht in $I\Omega^1_{A/k}$, im Widerspruch zu (2).

□

Kapitel 4

Die Vermutung von Casas-Álvero

4.1 Einleitung

Sei $P = (aX - b)^d$ ein Polynom in einer Variablen vom Grad d über einem beliebigen Körper. Es ist klar, dass der größte gemeinsame Teiler von P mit jeder Ableitung von P der Ordnung $1, \ldots, d-1$ nichttrivial ist: Selbstverständlich ist $\mathrm{ggT}(P, P^{(i)}) = \alpha P^{(i)}$. Aber gilt dies auch umgekehrt? Mit anderen Worten: Angenommen, ein univariates Polynom vom Grad d hat mit allen seinen Ableitungen der Ordnung $1, \ldots, d-1$ einen nichttrivialen gemeinsamen Faktor. Ist das Polynom dann schon ein Monom? Nach einer Vermutung von Eduardo Casas-Álvero ist diese Frage im Fall von Polynomen in Charakteristik 0 positiv zu beantworten. (In positiver Charakteristik existieren sehr viele Gegenbeispiele). Ziel der folgenden Abschnitte ist es, mit möglichst elementaren Mitteln Resultate über die Vermutung von Casas-Álvero herzuleiten. In Abschnitt 4.5 zeigen wir deren Gültigkeit für Polynome vom Grad einer Primzahlpotenz in Charakteristik 0 (siehe auch vLSv06). Im folgenden Abschnitt untersuchen wir den Fall positiver Charakteristik und geben insbesondere Gegenbeispiele zur Vermutung in beliebiger positiver Charakteristik an. Wir werden zeigen, dass die Vermutung für Polynome vom Grad d in Charakteristik 0 gilt, falls sie für Polynome vom Grad d in Charakteristik p gilt. Um diese Resultate zu gewinnen verwenden wir hauptsächlich einfache zahlentheoretische Eigenschaften von Binomialkoeffizienten, sowie etwas Theorie der algebraischen Erweiterungen des Körpers der p-adischen Zahlen und den Hilbert'schen Nullstellensatz.

Im Abschnitt 4.7 werden wir aus unseren Überlegungen zur Vermutung von Casas-Álvero ein allgemeineres Resultat über die Reduktion modulo p von homogenen Gleichungssystemen mit ganzzahligen Koeffizienten ableiten. Daraus ergibt sich dann nocheinmal eine Verschärfung der Aussagen von Abschnitt 4.5: Die Vermutung gilt für Polynome vom Grad d in Charakteristik 0 genau dann, wenn sie für Polynome vom Grad d in Charakteristik p, für fast alle Primzahlen p, gilt.

4.2 Das Problem

Im Folgenden sei k ein Körper. Für ein univariates Polynom $P = \sum_{k=0}^{d} a_{d-k} X^k \in k[X]$ vom Grad d mit Koeffizienten in k bezeichne $P_i = \sum_{k=i}^{d} \binom{k}{i} a_{d-k} X^{k-i}$ die i-te Hasse-

Ableitung.
Wir untersuchen nun die Aussage

Hat ein Polynom P vom Grad d mit allen seinen Hasse-Ableitungen der Ordnungen 1 bis $d-1$ einen nichttrivialen Faktor gemein, oder äquivalent: eine gemeinsame Nullstelle im algebraischen Abschluss von k, so ist P eine Potenz eines Linearfaktors über dem algebraischen Abschluss von k.

Wir nennen sie kurz die *Casas-Álvero-Vermutung zum Grad d über dem Körper k*. Da die Polynome, die in der Casas-Álvero-Vermutung betrachtet werden, sämtlich eine k-rationale Nullstelle haben, können wir uns auf solche beschränken, die bei 0 verschwinden (indem wir eine Translation auf die Variable X anwenden). Weiters können wir o.B.d.A. das Polynom normiert voraussetzen, sodass sich das Problem reduziert auf die folgende Aussage:

Hat ein normiertes Polynom P vom Grad d ohne konstanten Term mit allen seinen Hasse-Ableitungen der Ordnungen 1 bis $d-1$ eine Nullstelle im algebraischen Abschluss von k gemein, so ist P ein Monom vom Grad d über k.

Fassen wir die Koeffizienten A_i eines solchen Polynoms $P = X^d + \sum_{k=1}^{d-1} A_{d-k}X^k \in k[X]$ als Unbestimmte auf und bezeichnen mit $R_i = \mathrm{Res}_X(P, P_i) \in \mathbb{Z}[A_1, ..., A_{d-1}]$ die Resultante von P mit seiner i-ten Hasse-Ableitung, so erhalten wir eine weitere äquivalente Formulierung der Vermutung:

Verschwinden alle Resultanten $R_i(a_1, ..., a_{d-1}), i = 1, \ldots, d-1$, so ist $a_1 = \ldots = a_{d-1} = 0$.

Die Casas-Álvero-Vermutung ist also äquivalent zur Aussage, dass das algebraische Gleichungssystem der Resultanten R_i lediglich die Nulllösung besitzt. (Und diese ist auch tatsächlich immer vorhanden, da ein Monom trivialerweise mit allen seinen fraglichen Ableitungen eine gemeinsame Nullstelle hat.)

Diese Formulierung liefert den

Hilfssatz 4.1. *Gilt die Casas-Álvero-Vermutung zum Grad d über einem algebraisch abgeschlossenen Körper k, so auch über jeder Erweiterung von k.*

Beweis. Sei k algebraisch abgeschlossen. Gilt die Casas-Álvero-Vermutung zum Grad d über k, so hat nach dem vorigen Absatz das Gleichungssystem der Resultanten R_i lediglich die Nulllösung. Aus dem Hilbert'schen Nullstellensatz folgt, dass das von diesen Resultanten in $k[A]$ erzeugte Ideal Potenzen aller Koeffizienten $A_1, \ldots, A_{d-1}$ enthält. Die Nullstellenmenge dieses Ideals enthält daher über keiner Erweiterung von k Punkte ungleich 0. □

Bemerkung 4.2. Wenn wir im Folgenden von 'Ableitungen' sprechen, meinen wir die 'Hasse-Ableitungen'. Wenn wir von 'allen' Ableitungen eines Polynoms sprechen, meinen wir 'alle Ableitungen dieses Polynoms bis einschließlich der Ordnung $d-1$'.

4.3 Ein Lemma über Binomialkoeffizienten

Wir werden in unseren Untersuchungen zur Casas-Álvero-Vermutung häufig mit zahlentheoretischen Eigenschaften von Binomialkoeffizienten argumentieren. Konkret verwenden wir folgendes Lemma und Spezialfälle davon.

Lemma 4.3. *Seien p prim und $n = \sum_{k=0}^{l} n_k p^k$ bzw. $m = \sum_{k=0}^{l} m_k p^k$ die p-adischen Entwicklungen von natürlichen Zahlen n bzw. m. Dann gilt:*

$$\binom{n}{m} \equiv \prod_{k=0}^{l} \binom{n_k}{m_k} \pmod{p}.$$

Insbesondere gelten

1. $\binom{n}{n_k p^k} \equiv 1 \pmod{p}$,
2. $\binom{n}{p^k} \equiv n_k \pmod{p}$,
3. $\binom{n_k p^k}{m} \equiv 0 \pmod{p}$ *für* $m \neq 0 \pmod{p}^k$,
4. $\frac{n_k p^k!}{(p^k!)^{n_k}} \equiv (n_k)! \pmod{p}$.

Beweis. Die Zahl $\binom{n}{m}$ ist der Koeffizient zur Potenz X^m im Polynom $P = (X+1)^n$. Nun ist aber $P = \prod_{k=0}^{l} (X+1)^{p^k n_k} \equiv \prod_{k=0}^{l} (X^{p^k}+1)^{n_k} \pmod{p}$. Der Koeffizient von X^m in letzterem Produkt ist das Produkt der Koeffizienten von $(X^{p^k})^{m_k}$ in $(X^{p^k}+1)^{n_k}$. Diese sind aber gerade die Zahlen $\binom{n_k}{m_k}$, woraus die behauptete Kongruenz folgt.
Die Punkte (1)-(3) sind direkte Folgerungen daraus. Für (4) verwende man die Identität $\frac{n_k p^k!}{(p^k!)^{n_k}} = \binom{n_k p^k}{p^k}\binom{(n_k-1)p^k}{p^k}\ldots\binom{p^k}{p^k}$ und setze die Identität (2) ein. □

Hilfssatz 4.4.

$$\binom{n-l}{n-k}\binom{n}{n-l} = \binom{k}{l}\binom{n}{n-k}.$$

Beweis. Einfache Rechnung. □

4.4 Ein kurzer Ausflug in die Theorie der p-adischen Zahlen

Wir werden für den Beweis der Casas-Álvero-Vermutung in speziellen Fällen über Körpern der Charakteristik 0 einige Standardtatsachen aus der Theorie der p-adischen Zahlen und ihrer algebraischen Erweiterungen verwenden. Die nötigen Begriffe und Resultate entwickeln wir in diesem Abschnitt, wobei wir uns im Wesentlichen an (Kob77) orientieren.

Sei p eine Primzahl.

Definition 4.5. Die *p-Ordnung* einer ganzen Zahl $n \neq 0$ ist die größte natürliche Zahl e, sodass n ein Vielfaches von p^e ist. Wir schreiben $\nu_p(n) := e$. Für eine rationale Zahl $q = \frac{n}{m} \neq 0, m, n \in \mathbb{N}$ definieren wir $\nu_p(q) := \nu_p(n) - \nu_p(m)$. Außerdem setzen wir $\nu_p(0) = \infty$.

Bemerkung 4.6. Für natürliche Zahlen n und m gilt:

1. $\nu_p(n) = \infty \Leftrightarrow n = 0$,

2. $\nu_p(nm) = \nu_p(n) + \nu_p(m)$,

3. $\nu_p(n+m) \geqslant \min\{\nu_p(n), \nu_p(m)\}$.

Definition 4.7. Sei $0 < \rho < 1$ eine reelle Zahl (die wir für alles Weitere fixiert denken). Wir nennen

$$\|q\|_p := \rho^{\nu_p(q)}$$

die *p-adische Norm* der rationalen Zahl q.

Bemerkung 4.8. Aus Bemerkung 4.6 folgt, dass $\|\cdot\|_p$ tatsächlich eine Norm auf dem Körper der rationalen Zahlen ist. Es gilt:

1. $\|q\|_p = 0 \Leftrightarrow q = 0$,

2. $\|q_1 q_2\|_p = \|q_1\|_p \|q_2\|_p$,

3. $\|q_1 + q_2\|_p \leqslant \max\{\|q_1\|_p, \|q_2\|_p\}$.

Es gilt also sogar eine strengere Form der Dreiecksungleichung. Man nennt eine Norm, die diesen Bedingungen genügt, eine 'nichtarchimedische Norm'.

Definition 4.9. Die Vervollständigung des Körpers $\mathbb{Q}$ der rationalen Zahlen bezüglich der p-adischen Norm heißt der Körper der *p-adischen Zahlen* und wird mit $\mathbb{Q}_p$ bezeichnet. Den Unterring $\mathbb{Z}_p = \{x \in \mathbb{Q}_p; \|x\|_p \leqslant 1\}$ heißt der Ring der *ganzen p-adischen Zahlen*.

Bemerkung 4.10. Es ist leicht zu sehen, dass $\mathbb{Z}_p \cap \mathbb{Q} = \mathbb{Z}$. Weiters ist klar, dass $\mathfrak{m} = \{x \in \mathbb{Q}_p; \|x\|_p < 1\} = p\mathbb{Z}_p$ ein Ideal in $\mathbb{Z}_p$ ist. Es ist offensichtlich das einzige maximale Ideal dieses Rings - $\mathbb{Z}_p$ ist also ein lokaler Ring. Der Residuenkörper $\mathbb{Z}_p/p\mathbb{Z}_p$ ist der endliche Körper mit p Elementen.

Wir stellen uns nun die Frage, auf welche Weise sich die p-adische Norm auf endliche Körpererweiterungen der rationalen Zahlen fortsetzen lässt. Um die Antwort vorwegzunehmen: Auf einer endlichen Erweiterungen von $\mathbb{Q}$ gibt es *genau eine* Fortsetzung der p-adischen Norm. Diese werden wir im Folgenden konstruieren.

Satz 4.11. *Der Körper $\mathbb{Q}_p$ ist lokalkompakt bezüglich der von der p-adischen Norm induzierten Topologie.*

Beweis. Jeder Punkt in $\mathbb{Q}_p$ besitzt eine zu $\mathbb{Z}_p$ homöomorphe Umgebung. Es reicht also aus, die Kompaktheit von $\mathbb{Z}_p$ nachzuweisen. Sei n eine natürliche Zahl. Dann bildet das System von Mengen $\mathfrak{M}_n = \{i + p^n\mathbb{Z}_p, i = 0, \ldots, p^n - 1\}$ eine Überdeckung von $\mathbb{Z}_p$. Sei a_k eine Folge in $\mathbb{Z}_p$. Es gibt dann zumindest ein $M_1 \in \mathfrak{M}_1$, sodass unendlich viele Folgenglieder von a_k in M_1 liegen. In gleicher Weise finden wir nun ein Element $M_2 \in \mathfrak{M}_2$, sodass M_2 Teilmenge ist in M_1 und unendlich viele Folgenglieder von a_k enthält. Indem wir diese Konstruktion fortführen, erhalten wir eine Folge von Mengen M_k, deren Mittelpunkte eine Cauchyfolge in $\mathbb{Z}_p$ bilden. Der Grenzwert dieser Folge ist offensichtlich auch ein Häufungspunkt der Folge a_k. Der Ring $\mathbb{Z}_p$ ist also kompakt und $\mathbb{Q}_p$ daher lokalkompakt. □

Definition 4.12. Sei K ein durch $\|\cdot\|_K$ normierter Körper und V ein Vektorraum über K. Eine Abbildung $\|\cdot\|_V : V \to \mathbb{R}_{\geqslant 0}$ nennen wir eine (Vektorraum-)*Norm* auf V, wenn folgende Bedingungen erfüllt sind:

1. $\|v\|_V = 0 \Leftrightarrow v = 0$,

2. $\|\alpha v\|_V = \|\alpha\|_K \|v\|_V, \quad \alpha \in K$,

3. $\|v + w\|_V \leqslant \|v\|_V + \|w\|_V$.

Satz 4.13. *Sei V ein endlichdimensionaler Vektorraum über einem lokalkompakten normierten Körper K. Dann sind alle Normen auf V äquivalent, d.h., für zwei Normen $\|\cdot\|_1$ und $\|\cdot\|_2$ gibt es positive reelle Konstanten C_1 und C_2, sodass für alle $v \in V$ gilt: $\|v\|_2 \leqslant C_1\|v\|_1$ und $\|v\|_1 \leqslant C_2\|v\|_2$.*

Beweis. Wir wählen eine Basis $v_1, \ldots, v_n$ von V und definieren die 'Supremumsnorm':

$$\|\alpha_1 v_1 + \cdots + \alpha_n v_n\|_{\sup} := \max\{\|\alpha_1\|, \ldots, \|\alpha_n\|\}.$$

Es reicht zu zeigen, dass jede weitere Norm $\|\cdot\|$ auf V äquivalent zur Supremumsnorm ist. Es gilt

$$\|v\| \leq \|\alpha_1\|\|v_1\| + \cdots + \|\alpha_n\|\|v_n\| \leq n \max\{\|v_1\|, \ldots, \|v_n\|\}\|v\|_{\sup}.$$

Eine der geforderten Ungleichungen haben wir hiermit erhalten. Um die andere Ungleichung zu beweisen, versehen wir V mit der durch $\|\cdot\|_{\sup}$ gegebenen Topologie. Wir stellen fest, dass die Einheitssphäre $S = \{v \in V; \|v\|_{\sup} = 1\}$ als abgeschlossene Teilmenge des Kompaktums $B = \{v \in V; \|v\|_{\sup} \leqslant 1\}$ ebenfalls kompakt ist. Weiters ist nach der eben bewiesenen Ungleichung die Norm $\|\cdot\|$ stetig auf V bzw. S und dort stets ungleich 0. Es existiert also eine positive reelle Zahl ϵ, sodass

$$0 < \epsilon \leqslant \|v\|$$

für alle $v \in S$. Nun gibt es aber für jedes $v \in V$ ein $\alpha \in K$, sodass $\|\alpha^{-1}v\|_{\sup} = 1$, was gleichbedeutend ist mit

$$\|\alpha\| = \|v\|_{\sup}.$$

Aus der Ungleichung $0 < \epsilon \leqslant \|\alpha^{-1}v\|$ folgt somit

$$\|v\|_{\sup} = \|\alpha\| \leqslant \frac{1}{\epsilon}\|v\|,$$

was gerade die zweite geforderte Ungleichung darstellt. □

Korollar 4.14. *Sei nun speziell V eine endliche Körpererweiterung von K. Dann gibt es höchstens eine (Körper-)Norm auf V, die die Norm von K fortsetzt.*

Unter einer 'Körpernorm' auf V verstehen wir eine Norm auf dem Vektorraum V, wobei zusätzlich gilt: $\|vw\|_V = \|v\|_V\|w\|_V, v, w \in V$.

Beweis. Seien $\|\cdot\|_1$ und $\|\cdot\|_2$ Normen auf V. Angenommen, es existiert ein $v \in V$, sodass $\|v\|_1 < \|v\|_2$. Nach dem Satz 4.13 gibt es eine Konstante C, sodass $\|v\|_2^n = \|v^n\|_2 \leqslant C\|v^n\|_1 = C\|v\|_1^n$ für alle n, was offensichtlich unmöglich ist. Es ist also $\|\cdot\|_1 = \|\cdot\|_2$. □

Korollar 4.15. *Sei K eine endliche Körpererweiterung von $\mathbb{Q}_p$. Dann existiert höchstens eine Norm auf K, die die p-adische Norm fortsetzt.* □

Wir untersuchen nun genauer, welche Form diese Norm auf K haben muss, falls sie existiert. Sei dazu K eine endliche Galoiserweiterung von $\mathbb{Q}_p$ und $n = [K : \mathbb{Q}_p]$ der Grad von K über $\mathbb{Q}_p$. (Es reicht, den galoisschen Fall zu betrachten, da sich jede endliche Körpererweiterung in eine endliche galoissche Erweiterung einbetten lässt.) Sei $\mathrm{Gal}(K : \mathbb{Q}_p) = \{\sigma_1, \ldots, \sigma_n\}$ die Galoisgruppe von K über $\mathbb{Q}_p$ und $\|\cdot\|$ eine Norm auf K, die die p-adische Norm fortsetzt.

Es ist leicht zu sehen, dass dann die Abbildungen $x \mapsto \|\sigma_i(x)\|, 1 \leqslant i \leqslant n$, ebenfalls Fortsetzungen der p-adischen Norm sind. Korollar 4.15 zeigt nun, dass alle

diese Normen $x \mapsto \|\sigma_i(x)\|, 1 \leqslant i \leqslant n$, gleich sind! Da außerdem $\sigma_1(x)\cdots\sigma_n(x) \in \mathbb{Q}_p$, erhalten wir:

$$\|\sigma_1(x)\cdots\sigma_n(x)\|_p = \prod \|\sigma_i(x)\| = \|x\|^n.$$

Wir haben also notwendigerweise

$$\|x\| := \|\sigma_1(x)\cdot\cdots\cdot\sigma_n(x)\|_p^{1/n}. \tag{4.1}$$

Bemerkung 4.16. Das Produkt $\sigma_1(x)\cdot\cdots\cdot\sigma_n(x)$ heißt auch die *Norm* von x bezüglich der Erweiterung $K : \mathbb{Q}_p$ und wird oft mit $N_{K:\mathbb{Q}_p}(x)$ bezeichnet.
Es gilt $N_{K:\mathbb{Q}_p}(x) = \det A(x)$, wenn wir K als $\mathbb{Q}_p$-Vektorraum auffassen und $A(x)$ die Matrix der Multiplikation mit dem Element x ist.
Für $K \supset \mathbb{Q}_p$ und $x \in K$ gilt dann

$$\|x\|_p = \|N_{K:\mathbb{Q}_p}(x)\|_p^{1/[K:\mathbb{Q}_p]}. \tag{4.2}$$

Diese Identität gilt dann insbesondere auch, wenn K *nicht* galoissch ist.

Jetzt zeigen wir, dass die eben gegebene Definition einer Fortsetzung der p-adischen Norm tatsächlich wieder eine Norm (auf K) liefert. Wir bezeichnen ab nun auch diese Fortsetzung wieder mit $\|\cdot\|_p$.

Satz 4.17. *Die durch die Gleichung* (4.1) *gegebene Abbildung von K nach $\mathbb{R}$ ist eine Norm auf K, die die Norm von $\mathbb{Q}_p$ fortsetzt.*

Beweis. Es ist klar, dass $\|\cdot\|_p$ mit der ursprünglichen Norm auf $\mathbb{Q}_p$ übereinstimmt, multiplikativ ist und $\|x\|_p$ genau dann verschwindet, wenn $x = 0$ ist. Der schwierige Teil dieses Satzes ist der Beweis der Dreiecksungleichung $\|a+b\|_p \leqslant \max\{\|a\|_p, \|b\|_p\}$. Aufgrund der Multiplikativität von $\|\cdot\|_p$ ist es genug, $\|1+\gamma\|_p \leqslant 1$ nachzuweisen, wenn $\|\gamma\|_p \leqslant 1$.

Wir nehmen vorerst an, γ sei ein primitives Element von K über $\mathbb{Q}_p$, d.h., $K = \mathbb{Q}_p(\gamma)$, und wählen $\{1, \gamma, \ldots, \gamma^{n-1}\}$ als Basis des $\mathbb{Q}_p$-Vektorraumes K. Sei A die Matrix der Multiplikation mit γ. Dann ist $\|\gamma\|_p = \|\det A\|_p^{1/n}$ und $\|1+\gamma\|_p = \|\det(1+A)\|_p^{1/n}$. Sei weiters $\|\cdot\|$ die Supremumsnorm auf dem n^2-dimensionalen $\mathbb{Q}_p$-Vektorraum der $n\times n$-Matrizen über $\mathbb{Q}_p$. Wir behaupten: $\{\|A^i\|\}$ ist beschränkt.

Wir nehmen das Gegenteil an. Sei i_j so, dass $\|A^{i_j}\| > j$. Sei β_j ein Eintrag in A^{i_j}, sodass $\beta_{i_j} = \|A^{i_j}\|$. Wir betrachten nun die Folge von Matrizen

$$B_j := A^{i_j}/\beta_j.$$

Es ist klar, dass $\|B_j\| = 1$ ist. Da die Einheitssphäre bezüglich der Supremumsnorm kompakt ist, existiert eine Teilfolge $\{B_{j_k}\}$, die gegen eine Matrix B konvergiert. Wegen $\det B_j = \det A^{i_j}/\beta_j^n$ gilt

$$\|\det B_j\|_p < \|\det A^{i_j}\|_p / j^n = \|\gamma\|_p^{ni_j}/j^n \leqslant 1/j^n.$$

Da $B_{j_k} \to B$ in der Supremumsnorm, konvergiert auch $\det B_{j_k}$ gegen $\det B$. Also ist $\det B = 0$.

Es existiert also ein Element $l \in K$, sodass $B \cdot l = 0$. Wir werden nun zeigen, dass dies schon $B = 0$ impliziert, im Widerspruch zu $\|B\| = 1$. Es reicht, $B(\gamma^i l) = 0$ für jedes i zu zeigen, da $\{\gamma^i l, 0 \leqslant i < n\}$ eine Basis von K ist. Aber

$$B(\gamma^i l) = \lim B_{j_k}(\gamma^i l) = \lim \gamma^i B_{j_k}(l) = \gamma^i \lim B_{j_k}(l) = \gamma^i B(l) = 0.$$

Also ist $\{\|A^i\|\}$ durch eine Konstante C beschränkt.

Aus der Dreiecksungleichung auf $\mathbb{Q}_p$ und der Entwicklung der Determinante von A folgt $\|\det A\|_p \leqslant \|A\|^n$. Sei nun N eine natürliche Zahl. Wir betrachten $(1+A)^N = 1 + \binom{N}{1}A + \cdots + A^N$. Wir haben

$$\|1+\gamma\|_p^N = \|\det(1+A)^N\|_p^{1/n} \leqslant \|(1+A)^N\| \leqslant \max\{\|\binom{N}{i}A^i\|\} \leqslant \max\|A^i\| \leqslant C.$$

Es ist also $\|1+\gamma\|_p \leqslant C^{1/N}$. Der Grenzübergang $N \to \infty$ liefert die geforderte Ungleichung $\|1+\gamma\|_p \leqslant 1$.

Ist γ kein primitives Element von K, so liefert die obige Rechnung mit K ersetzt durch $\mathbb{Q}_p(\gamma)$:

$$1 \geqslant \|N_{\mathbb{Q}_p(\gamma):\mathbb{Q}_p}(1+\gamma)\|_p^{1/[\mathbb{Q}_p(\gamma):\mathbb{Q}_p]} = N_{K:\mathbb{Q}_p}(1+\gamma)\|_p^{1/[K:\mathbb{Q}_p]} = \|1+\gamma\|_p.$$

Damit ist der Satz bewiesen. □

Der Körper K hat also als normierter Körper eine ganz ähnliche Struktur wie $\mathbb{Q}_p$ selbst. Wieder haben wir einen Unterring $A = \{x \in K; \|x\|_p \leqslant 1\}$ von K - man nennt ihn den Ganzheitsring von K. Auch dieser Ring A ist ein lokaler Ring mit dem maximalen Ideal $M = \{x \in K; \|x\|_p < 1\}$, und wir haben eine natürliche Inklusion von Restklassenkörpern

$$\mathbb{Z}_p/p\mathbb{Z}_p \hookrightarrow A/M.$$

Es ist leicht nachzurechnen, dass der sogenannte 'Restklassengrad' $f = [A/M : \mathbb{Z}_p/p\mathbb{Z}_p]$ dieser Körpererweiterung $\leqslant [K : \mathbb{Q}_p]$ ist. Insbesondere ist also A/M der endliche Körper mit p^f Elementen.
Dass der Ring A tatsächlich der Ganzheitsring von K im üblichen Sinne ist, zeigt der

Satz 4.18. *Der Unterring $A = \{x \in K; \|x\|_p \leqslant 1\}$ von K ist der ganze Abschluss von $\mathbb{Z}_p$ in K.*

Beweis. Sei $\alpha \in K$ ganz über $\mathbb{Z}_p$, d.h., α erfüllt eine Gleichung der Form $\alpha^m + a_1\alpha^{m-1} + \cdots + a_m = 0, a_i \in \mathbb{Z}_p$. Dann gilt

$$\|\alpha\|_p^m = \|\alpha^m\|_p = \|a_1\alpha^{m-1} + \cdots + a_m\|_p \leqslant \max\|a_i\alpha^{m-i}\|_p \leqslant$$
$$\leqslant \max\|\alpha^{m-i}\|_p,$$

was aber unmöglich ist, wenn $\|\alpha\|_p > 1$. Es ist also $\alpha \in A$.

Falls umgekehrt $\alpha \in A$ liegt, also $\|\alpha\|_p \leqslant 1$, so gilt dies auch für alle Konjugierten von α. Da aber die Koeffizienten des Minimalpolynoms von α gerade die symmetrischen Polynome in den Konjugierten von α sind, ist das Minimalpolynom von α normiert mit Koeffizienten in $\mathbb{Z}_p$, also α ganz über $\mathbb{Z}_p$. □

Indem wir den algebraischen Abschluss $\overline{\mathbb{Q}_p}$ von $\mathbb{Q}_p$ durch endliche Erweiterungen ausschöpfen, sehen wir, dass sich die p-adische Norm sogar auf $\overline{\mathbb{Q}_p}$ fortsetzt und dort wieder den Ganzheitsring $\overline{\mathbb{Z}_p} = \{x \in \overline{\mathbb{Q}_p}; \|x\|_p \leqslant 1\}$ festlegt. Es ist klar, dass auch dieser Ring lokal ist mit dem maximalen Ideal $\mathfrak{m} = \{x \in \overline{\mathbb{Q}_p}; \|x\|_p < 1\}$. Der Restklassenkörper ist $\overline{\mathbb{F}_p}$, der algebraische Abschluss von $\mathbb{F}_p$.

Genau diese Fakten verwenden wir im nächsten Abschnitt, um die Vermutung von Casas-Álvero in Charakteristik 0 zu untersuchen.

4.5 Die Casas-Álvero-Vermutung in Charakteristik 0

Satz 4.19. *Das Polynom $f = X^n + a_1X^{n-1} + \cdots + a_{n-1}X + a_n$ mit Koeffizienten im Ring $\overline{\mathbb{Z}_p}$ habe gemeinsame Nullstellen mit jeder seiner Ableitungen. Dann teilt $\binom{n}{k}$ den Koeffizienten a_k für $k = 0, \ldots, n$.*
Sei f_k die k-te Hasse-Ableitung von f. Mit der Bezeichnung $a_k = \binom{n}{k}c_k$ gilt: $f_{n-k} = \binom{n}{n-k}[X^k + \binom{k}{1}c_1X^{k-1} + \binom{k}{2}c_1X^{k-2} + \cdots + \binom{k}{k-1}c_{k-1}X^{k-1} + \binom{k}{k}c_k]$.

Beweis. Zuerst halten wir fest: $\overline{\mathbb{Z}_p}$ ist ganz abgeschlossen, d.h., alle Nullstellen von f liegen in $\overline{\mathbb{Z}_p}$. Also hat auch jede Ableitung von f zumindest eine Nullstelle in $\overline{\mathbb{Z}_p}$. Wir führen den Beweis durch Induktion über k: Für $k = 0$ ist die Behauptung trivial, da $\binom{n}{n} = 1$. Wir nehmen nun an, $\binom{n}{n-l}$ teilt a_l für alle $l < k$, d.h. $a_l = \binom{n}{n-l}c_l$ mit $c_l \in \overline{\mathbb{Z}_p}$. Dann ist

$$f_{n-k} = \binom{n}{n-k}X^k + \binom{n-1}{n-k}\binom{n}{n-1}c_1X^{k-1} +$$
$$+\binom{n-2}{n-k}\binom{n}{n-2}c_2X^{k-2} + \ldots + \binom{n-k+1}{n-k}\binom{n}{n-k+1}c_{k-1}X + a_k.$$

Wegen $\binom{n-l}{n-k}\binom{n}{n-l} = \binom{k}{l}\binom{n}{n-k}$ folgt

$$f_{n-k} = \binom{n}{n-k}[\binom{k}{0}X^k + \binom{k}{1}c_1X^{k-1} + \binom{k}{2}c_2X^{k-2} +$$
$$\cdots + \binom{k}{k-1}c_{k-1}X] + a_k.$$

Da f_{n-k} eine Nullstelle in $\overline{\mathbb{Z}_p}$ hat, ist a_k durch $\binom{n}{n-k} = \binom{n}{k}$ teilbar. Insbesondere erkennt man daraus die Darstellung von f_{n-k} wie behauptet. □

Korollar 4.20. *Wenn $d = p^k$ für eine Primzahl p, dann gilt die Casas-Álvero-Vermutung für Polynome vom Grad d in beliebigen Körpern der Charakteristik 0.*

Beweis. Nach dem Hilfssatz 4.1 im ersten Abschnitt reicht es aus, die Behauptung für den algebraischen Abschluss $\overline{\mathbb{Q}_p}$ des Körpers der p-adischen Zahlen $\mathbb{Q}_p$ zu zeigen. Sei also $P = \sum_{k=1}^{d} a_{d-k}X^k \in \overline{\mathbb{Q}_p}[X]$ ein normiertes Polynom mit Koeffizienten in $\overline{\mathbb{Q}_p}$ ohne konstanten Term. Durch eine Transformation ($X \mapsto \alpha X, \alpha \in \mathbb{Q}_p$) der Unbestimmten X lässt sich erreichen, dass alle Koeffizienten ganz sind, d.h. $\|a_l\|_p \leqslant 1$ für alle l. Wir nehmen nun an, es gäbe nichtverschwindende Koeffizienten $a_l, 1 \leqslant l \leqslant d-1$. Dann lässt sich durch die Skalierung der Variablen X sogar erreichen, dass zumindest einer dieser Koeffizienten die p-adische Norm = 1 hat. Aus Satz 4.19 folgt nun, dass der l-te Koeffizient durch $\binom{d}{l}$ teilbar ist ($l = 1, \ldots, d-1$). Nach dem Lemma 4.3, Spezialfall (3), ist $\binom{d}{l} \equiv 0 \pmod{p}$ für $l \geq 1$, weshalb jeder Koeffizient von P außer dem Leitkoeffizienten durch p teilbar ist, also in der p-adischen Norm echt kleiner als 1 ist. Dies ist aber ein Widerspruch. □

Durch eine ähnliche Argumentation können wir aus der Gültigkeit der Casas-Álvero-Vermutung in Charakteristik p auf deren Gültigkeit in Charakteristik 0 schließen:

Gegeben seien eine Primzahl p und ein normiertes Polynom P ohne konstanten Term mit Koeffizienten in $\overline{\mathbb{Z}_p}$, sodass P mit sämtlichen seiner Ableitungen eine

gemeinsame Nullstelle besitzt. Dann können wir P auch als Polynom über dem Ganzheitsring einer endlichen Körpererweiterung der p-adischen Zahlen $\mathbb{Q}_p$ interpretieren. Reduzieren wir dieses Polynom modulo dem maximalen Ideal des Ganzheitsringes dieser Körpererweiterung, so erhalten wir ein Polynom mit Koeffizienten in einer Körpererweiterung von $\mathbb{F}_p$, welches nach wie vor eine gemeinsame Nullstelle mit allen seinen Ableitungen hat.
Wenn nun die Casas-Álvero-Vermutung in Charakteristik p gilt, heißt das, dass diese Reduktion von P schon ein Monom ist, und es folgt, dass alle Koeffizienten von P, außer dem Leitkoeffizienten, eine p-adische Norm < 1 haben. Aus dieser Tatsache schließen wir wie im vorigen Beweis, dass P selbst schon ein Monom sein muss. Wir können also festhalten:

Satz 4.21. *Gilt die Casas-Álvero-Vermutung zum Grad d in Charakteristik p für zumindest eine Primzahl p, so gilt sie auch in Charakteristik 0.* □

Bemerkung 4.22. Es gilt sogar: Die Casas-Álvero-Vermutung zum Grad d gilt in Charakteristik 0 genau dann, wenn sie in Charakteristik p für fast alle Primzahlen p gilt. Wir beweisen dies im Abschnitt 4.7.

4.6 Die Casas-Álvero-Vermutung in positiver Charakteristik

Sei K ein Körper der Charakteristik $p > 0$. Ganz ähnlich wie in Charakteristik 0 gilt auch hier der

Satz 4.23. *Wenn $d = p^k$ oder $d = 2p^k$ für eine Primzahl p, dann gilt die Casas-Álvero-Vermutung für Polynome vom Grad d in beliebigen Körpern der Charakteristik p (und daher auch in Körpern der Charakteristik 0).*

Es gilt sogar allgemeiner:

Satz 4.24. *Sei $d = d_k p^k$ mit $0 \leq d_k < p$. In Charakteristik p gilt die Casas-Álvero-Vermutung zum Grad $d_k p^k$ genau dann, wenn sie zum Grad d_k gilt.*

Beweis. Sei $P = X^d + a_1 X^{d-1} + \cdots + a_{d-1}X \in K[X]$. Nach dem Lemma über Binomialkoeffizienten ist $\binom{d}{d-1} \equiv 0 \pmod{p}$ und daher $P_{d-1} = a_1$. Da P_{d-1} eine gemeinsame Nullstelle mit P hat, verschwindet a_1. Indem wir diese Schlussweise für $P_{d-2}, P_{d-3}, \ldots$ wiederholen, sehen wir, dass P die Form $P(X) = Q(X^{p^k})$ hat, wobei $Q = X^{d_k} + b_1 X^{d_k-1} + \cdots + b_{d_k-1}X$ ein Polynom vom Grad d_k ist. Insbesondere haben alle Ableitungen von P der Ordnung $m \neq 0 \pmod{p^k}$ eine gemeinsame Nullstelle mit P, nämlich die 0.

Weiters gilt für $m = p^k$:

$$P_m = \binom{d_k p^k}{p^k} X^{(d_k-1)p^k} + \binom{(d_k-1)p^k}{p^k} b_1 X^{(d_k-2)p^k} + \cdots + \binom{p^k}{p^k} b_{d_k-1}.$$

Mit dem Lemma über Binomialkoeffizienten folgt allgemein für $m = lp^k$:

$$P_m = Q_l(X^{p^k}), \quad Q_l \in K[X].$$

Da alle Ableitungen von P der Ordnung $m \neq 0 \pmod{p^k}$ von vornherein eine gemeinsame Nullstelle mit P haben, sind äquivalent (**):

1. P hat eine gemeinsame Nullstelle mit allen seinen Ableitungen.
2. Q hat eine gemeinsame Nullstelle mit allen seinen Ableitungen.

Daraus, und aus der einfachen Beobachtung, dass P ein Monom in X ist genau dann, wenn Q ein Monom ist, folgt die Behauptung. □

In Charakteristik p bleibt also die Gültigkeit der Casas-Álvero-Vermutung für Grade $d \leqslant p-1$ zu untersuchen.

Satz 4.25. *Seien $a, b \in K$.*

1. *In Charakteristik $p \geqslant 3$ sind die Polynome der Form $X^{p-1} + aX^{2k}, 0 < k < p-1$, Gegenbeispiele zur Casas-Álvero-Vermutung.*
2. *In Charakteristik $p > 7$ existieren Gegenbeispiele zur Casas-Álvero-Vermutung der Form $X^{(p-1)/2} + aX^3 + bX^2$.*

Beweis. Sei $P = X^{p-1} + aX^{2k}, 0 < k < (p-1)/2$. Wegen $\binom{p-1}{2k} \equiv \frac{(p-1)\cdots(p-2k)}{1\cdots 2k} \equiv \frac{(-1)\cdots(-2k)}{1\cdots 2k} \equiv (-1)^{2k} \equiv 1 \pmod p$ folgt $P_{2k} = X^{p-1-2k} + a$. Daher hat P eine gemeinsame Nullstelle mit allen seinen Ableitungen.

Wir setzen $d = (p-1)/2$ und $P = X^d + aX^3 + bX^2$. Um (2) zu zeigen, sind a und b so zu bestimmen, dass P_2 und P_3 gemeinsame Nullstellen mit P besitzen, oder äquivalent: $c_1 X^{-2} P(X) - P_2(X)$ und $c_2 X^{-2} P(X) - P_3(X)X$ besitzen gemeinsame Nullstellen mit $X^{-2}P(X)$, wobei $c_i \in K - \{0\}$ ist. Dazu berechnen wir:

$$P_2(X) = \frac{3}{8} X^{d-2} + 3aX + b,$$
$$P_3(X) = -\frac{5}{16} X^{d-3} + a,$$

und daher:

$$3X^{-2}P(X) - 8P_2(X) = -21aX - 5b,$$
$$5X^{-2}P(X) + 16P_3(X)X = 21aX + 5b =: g(X).$$

Es reicht also, die beiden Koeffizienten a und b so zu bestimmen, dass f eine gemeinsame Nullstelle mit g besitzt. Soll die gemeinsame Nullstelle z.B. 1 sein, so bleibt das lineare Gleichunssystem

$$a + b = -1$$
$$21a + 5b = 0$$

zu lösen. Die Determinante dieses Systems ist 16 und damit invertierbar ($p > 7$). Daher existiert genau eine Lösung $a \neq 0, b \neq 0$ und (2) ist bewiesen. □

Im allgemeinen existieren zu einem gegebenen Grad d in positiver Charakteristik aber wesentlich mehr Polynome, die die Casas-Álvero-Vermutung verletzen. Wir wollen hier noch einige Fälle beschreiben. Dabei betrachten wir Polynome, die durch Multiplikation der Variablen X mit einem Element in $\overline{\mathbb{F}_p}$ auseinander hervorgehen, als äquivalent, z.B.: $3X^2 + 3X^3 + X^5$ entsteht in Charakteristik 11 durch die Sutstitution ($X \mapsto -5X$) in $2X^2 + X^3 + X^5$. Wir geben daher immer jeweils nur einen Vertreter einer solchen Äquivalenzklasse an.

1. Wenn $d = 5$ und $p = 11$ existieren keine weiteren Gegenbeispiele.
2. Im Fall $d = 6$ und $p = 13$ existiert zusätzlich zu dem im Satz beschriebenen Polynom noch eines der Form
$$5X^3 + 2X^4 + X^6.$$
3. Für $d = 8$ und $p = 17$ existieren 112 Gegenbeispiele neben den im Satz beschriebenen. Siehe dazu die Liste von Gegenbeispielen im Anhang.

4.7 Homogene algebraische Gleichungssysteme mit ganzzahligen Koeffizienten

Sei $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}_1^n$.

Definition 4.26. Ein Monom der Form $x^e = x_1^{e_1} \cdots x_n^{e_n}$ habe den α-Grad m, wenn $\alpha \cdot e = m$. Ein Polynom heiße α-homogen vom α-Grad m, wenn es aus lauter Monomen vom α-Grad m besteht.

Definition 4.27. Eine algebraische Menge X in $\mathbb{A}_k^n$ nennen wir α-homogen, wenn zu jedem Punkt $(x_1, \ldots, x_n)$ von X auch der Punkt $(\lambda^{\alpha_1} x_1, \ldots, \lambda^{\alpha_n} x_n)$ in X liegt.

Hilfssatz 4.28. *Seien $P_1, \ldots, P_r$ Polynome in $k[x_1, \ldots, x_n]$. Sind diese Polynome α-homogen, so ist auch die durch sie definierte algebraische Menge im affinen Raum $\mathbb{A}_k^n$ α-homogen.*

Beweis. Die Behauptung folgt aus der Gleichung

$$P_i(\lambda^{\alpha_1} x_1, \ldots, \lambda^{\alpha_n} x_n) = \lambda^{m_i} P_i(x_1, \ldots, x_n),$$

wenn m_i der α-Grad von P_i ist. □

Satz 4.29. *Seien $P_1, \ldots, P_r$ α-homogene Polynome in $\overline{\mathbb{Z}_p}[x_1, \ldots, x_n]$ vom α-Grad $d > 0$, und $\overline{P_1}, \ldots, \overline{P_r}$ bezeichne deren Reduktionen modulo $\mathfrak{m} = \{x \in \overline{\mathbb{Z}_p}; \|x\|_p < 1\}$. Hat das System von Gleichungen*

$$\overline{P_1} = 0, \ldots, \overline{P_r} = 0$$

außer 0 keine weitere Lösung im algebraischen Abschluss $\overline{\mathbb{F}_p}$ von $\mathbb{F}_p$, so hat auch

$$P_1 = 0, \ldots, P_r = 0$$

keine weitere Lösung über $\overline{\mathbb{Q}_p}$.

Beweis. Da die betrachteten Polynome von der α-Ordnung > 0 sind, verschwinden alle ihre konstanten Terme und es gilt $0 \in X = V_{\overline{\mathbb{Q}_p}}(P_1, \ldots, P_r)$. Zu zeigen ist also noch, dass es keine weiteren Lösungen gibt.
Dazu verwenden wir dasselbe Argument wie im Beweis von Korollar 4.20: Nehmen wir an, wir hätten eine Nullstelle $0 \neq x = (x_1, \ldots, x_n) \in X$. Da X nach dem Hilfssatz 4.28 α-homogen ist, können wir o.E.d.A. annehmen, dass $x_i \in \overline{\mathbb{Z}_p}, i = 1, \ldots, n$. Wir können sogar annehmen, dass $\|x_i\|_p = 1$ für ein $i = 1, \ldots, n$. Indem wir diese Lösung modulo $\mathfrak{m}$ reduzieren, erhalten wir aber eine nichttriviale Lösung des reduzierten Gleichungssystems, die nach Voraussetzung nicht existiert, Widerspruch. □

Im Folgenden bezeichnen wir mit R den Ring der ganzen algebraischen Zahlen, also solche komplexen Zahlen, die eine ganzzahlige normierte polynomiale Gleichung über $\mathbb{Z}$ erfüllen. Dieser Ring ist nach Satz 4.18 ein Unterring von $\overline{\mathbb{Z}_p}$ für p prim.

Dann gilt sogar

Satz 4.30. *Seien $P_1, \ldots, P_r$ α-homogene Polynome in $R[x_1, \ldots, x_n]$ vom α-Grad $d > 0$, und $\overline{P_1}, \ldots, \overline{P_r}$ bezeichne deren Reduktionen modulo $\mathfrak{m} \cap R = \{x \in R; \|x\|_p < 1\}$. Bezeichne X die Lösungsmenge des Gleichungssystems über $\overline{\mathbb{Z}_p}$ und X_p die Lösungsmenge des Gleichungssystems über $\overline{\mathbb{Z}_p}/\mathfrak{m} = \overline{\mathbb{F}_p}$. Dann gilt $X = \{0\}$ genau dann, wenn $X_p = \{0\}$ für fast alle Primzahlen p.*

Beweis. Die eine Implikation folgt aus Satz 4.29. Zur umgekehrten Implikation: Nach dem Hilbertschen Nullstellensatz haben wir Gleichungen der Form

$$x_i^{r_i} = \sum_j a_{ij} P_j.$$

wobei die a_{ij} Polynome mit Koeffizienten in einer endlichen Erweiterung von $\mathbb{Q}$ sind. Indem wir diese Gleichungen mit geeigneten ganzen Zahlen multiplizieren, erhalten wir die polynomialen Gleichungen

$$c_i x_i^{r_i} = \sum_j b_{ij} P_j,$$

in denen alle Koeffizienten eine p-adische Norm $\leqslant 1$ haben, also ganz über $\mathbb{Z}_p$ sind. Dann gibt es höchstens endlich viele Primzahlen p, sodass eine der Zahlen c_i ein Vielfaches von p ist. Nach jeder anderen Primzahl lassen sich die Gleichungen reduzieren, ohne dass die Koeffizienten c_i verschwinden, woraus die Behauptung folgt. □

Wenn wir nun noch nachweisen, dass die Nullstellenmenge der Resultanten, die wir im Casas-Álvero-Problem betrachten, tatsächlich α-homogen ist, so ist die Bemerkung 4.22 gerechtfertigt. Dies holen wir nun noch nach.

Hilfssatz 4.31. *Fassen wir die Koeffizienten A_i eines Polynoms*

$$P = X^d + \sum_{k=1}^{d-1} A_{d-k} X^k \in k[X]$$

als Unbestimmte auf und bezeichnen wir die Resultante von P mit seiner i-ten Hasse-Ableitung mit $R_i = Res_X(P, P_i) \in \mathbb{Z}[A_1, ..., A_{d-1}]$.
Dann ist die Nullstellenmenge von R_i α-homogen im Sinne von Definition 4.27 mit $\alpha = (1, 2, \ldots, d-1)$.

Beweis. Es ist x eine gemeinsame Nullstelle von P und P_i, so ist αx eine gemeinsame Nullstelle von $X^d + \sum_{k=1}^{d-1} \alpha^{d-k} A_{d-k} X^k$ und seiner i-ten Hasse-Ableitung. Daher gilt: Ist $a = (a_1, \ldots, a_{d-1})$ eine Nullstelle von R_i, so auch $a = (\alpha a_1, \ldots, \alpha^{d-1} a_{d-1})$. Daher ist die Nullstellenmenge von R_i $(1, \ldots, d-1)$-homogen. □

Daraus folgt

Satz 4.32. *Die Casas-Álvero-Vermutung zum Grad d gilt in Charakteristik 0 genau dann, wenn sie in Charakteristik p für fast alle Primzahlen p gilt.* □

Kapitel 5

Verschwindungsordnungen auf Varietäten

5.1 Motivation

Es ist wohlbekannt, dass sich jede ganze Zahl n in der Form

$$n = \prod_{p \text{ Primzahl}} p^{nu_p(n)}$$

schreiben lässt, wobei der Exponent $\nu_p(n)$ auch die p-Ordnung von n oder die *Bewertung* von n im Primideal (p) heißt. Rein formal könnten wir dieses Produkt auch additiv schreiben und erhalten so für jede ganze Zahl eine Darstellung $n = \sum_{pPrimzahl} nu_p(n) \cdot (p)$ mit eindeutigen nichtnegativen Koeffizienten. Allgemeiner hat natürlich jede rationale Zahl eine solche Darstellung mit möglicherweise negativen Koeffizienten (siehe Abschnitt 4.4). Existiert für Koordinatenringe algebraischer Varietäten bzw. rationale Funktionenkörper ein analoges Konzept? Ein Ansatz ist das Konzept der Weil-Divisoren:

Sei X eine Varietät (oder allgemeiner: ein Schema) und K der Körper der rationalen Funktionen auf X. Dem Begriff der Primideals im Ring der ganzen Zahlen entspricht hier der Begriff der Untervarietät (bzw. des Unterschemas) der Codimension 1 in X. In Analogie nennt man diese die *Primdivisoren* auf X. Um die gewünschte Darstellung von f als Linearkombination von Primdivisoren zu erhalten, müssen wir klären, was unter der 'Bewertung von f' in einem Primdivisor von X zu verstehen ist.

Definition 5.1. Eine diskrete Bewertung des Körpers K ist eine Abbildung $\nu : K \to \mathbb{Z}$ mit den folgenden Eigenschaften:

1. $\nu(xy) = \nu(x) + \nu(y)$,
2. $\nu(x + y) \geq \min\{\nu(x), \nu(y)\}$.

Der Unterring $\{x \in K; \nu(x) \geq 0\} \subset K$ heißt *Bewertungs ring* von K. Ein Integritätsring A heißt *diskreter Bewertungsring*, falls A Bewertungsring bezüglich einer diskreten Bewertung seines Quotienten körpers ist.

Bemerkung 5.2. Es ist leicht zu sehen, dass diskrete Bewertungsringe gerade die lokalen Hauptidealringe sind. Weiters ist klar, dass ein diskreter Bewertungsring ein maximaler echter Unterring seines Quotientenkörpers ist.

Es gilt der

Satz 5.3. *Sei A ein noetherscher, lokaler Integritätsbereich der Dimension 1 mit maximalem Ideal $\mathfrak{m}$. Dann sind äquivalent:*

1. *A ist ein diskreter Bewertungsring;*
2. *A ist ganz abgeschlossen;*
3. *A ist regulär;*
4. *$\mathfrak{m}$ ist ein Hauptideal.*

Beweis. (AM69, 1, Prop. 9.2, S. 94). □

Sei nun Y eine Untervarietät von X der Codimension 1. Der lokale Ring bei Y ist also ein diskreter Bewertungsring genau dann, wenn er ganz abgeschlossen ist. Gilt dies für alle solchen Untervarietäten von X, so sagt man manchmal auch, X sei regulär in Codimension 1. Analog ist die Situation, wenn X ein noethersches, integrales und separiertes Schema ist ((Har00, II, 6)).

In diesem Fall können wir den einer rationalen Funktion f auf X zugeordneten 'Hauptdivisor' definieren:

$$div(f) := \sum \nu_Y(f)Y, \tag{5.1}$$

wobei Y Codimension 1 in X hat und $\nu_Y(f)$ die Bewertung von f im lokalen Ring bei Y ist. Man nennt $\nu_Y(f)$ auch die 'Verschwindungsordnung' von f in Y.

Die formalen Linearkombinationen von Primdivisoren auf X heißen *Weil-Divisoren* auf X und bilden offensichtlich eine additive Gruppe, die oft mit $\mathrm{Div}(X)$ bezeichnet wird. Das interessante dabei ist, dass im allgemeinen nicht jeder Weil-Divisor schon ein Hauptdivisor ist (also von einer rationalen Funktion kommt). Die Faktorgruppe $\mathrm{Div}(X)/\{\text{Hauptdivisoren auf } X\}$ heißt die Divisorenklassengruppe von X und enthält wichtige Information über die Geometrie von X.

Die nachfolgenden Betrachtungen sind motiviert durch die Frage, ob die Bedingung 'regulär in Codimension 1' wirklich wesentlich ist, oder ob sie sich vielleicht doch irgendwie umgehen lässt. Das Problem ist dabei letztlich, eine sinnvolle Definition der Verschwindungsordnung einer rationalen Funktion in (möglicherweise singulären) Unterschemata/-varietäten von X zu finden. Im Fall affiner Schemata (also z.B. affiner Varietäten) werden wir dafür einen Weg über die Normalisierung des Schemas vorschlagen und ihn im Fall von affinen Kurven mit einer alternativen Definition mithilfe der Schnittmultiplizität von Kurven vergleichen.

5.2 Der Fall affiner Schemata

Sei A ein noetherscher Integritätsbereich und $K = \mathrm{Quot}(A)$ sein Quotientenkörper. Die Unterschemata der Codimension 1 in $X = \mathrm{Spec}(A)$ sind gerade die Primideale der Höhe 1 in A. Für den $\mathfrak{p} \in \mathrm{Spec}(A)$ zugeordneten Primdivisor schreiben wir im Folgenden kurz $[\mathfrak{p}]$.

Sei $f \in K = \mathrm{Quot}(A)$. Um der Definition

$$div(f) := \sum \nu_{\mathfrak{p}}(f)[\mathfrak{p}] \tag{5.2}$$

(wobei die Summe über alle Primideale in A der Höhe 1 läuft), auch im Fall, dass nicht alle lokalen Ringe der Dimension 1 diskrete Bewertungsringe sind, einen Sinn zu geben, müssen wir den Ausdruck $\nu_{\mathfrak{p}}$ neu definieren. Dies versuchen wir nun.

Lemma 5.4. *Ist A ein noetherscher Integritätsbereich, so sind äquivalent:*

1. *A ist ganz abgeschlossen,*
2. *Für alle multiplikativen Mengen $S \subset A - \{0\}$ ist $S^{-1}A$ ganz abgeschlossen.*
3. *Für alle Primideale $\mathfrak{p}$ in A ist $A_{\mathfrak{p}}$ ganz abgeschlossen.*

Beweis. Sei A ganz abgeschlossen und $z = \frac{x}{y} \in K$ ganz über $S^{-1}A$. Dann erfüllt z eine ganze Gleichung der Form

$$z^n + a_1 z^{n-1} + \cdots + a_{n-1} z + a_n = 0, \quad a_i \in S^{-1}A$$

Sei $c \in S$ das Produkt der Nenner der Zahlen a_i. Multiplizieren wir obige Gleichung mit c, so erhalten wir

$$b_0 z^n + b_1 z^{n-1} + \cdots + b_{n-1} z + b_n = 0,$$

wobei nun alle b_i schon in A liegen. Nun erkennen wir, dass $b_0 z$ eine ganze Gleichung über A erfüllt, und da A ganz abgeschlossen ist, ist $b_0 z = cz \in A$ bzw. $z \in S^{-1}A$. Also gilt (1) $\Rightarrow$ (2).
Die Implikation von (2) nach (3) ist trivial.
Wir nehmen nun an, es gelte (3). Sei weiters $f \in K - \{0\}$ ganz über A, was insbesondere impliziert, dass f ganz über jedem lokalen Ring $A_{\mathfrak{p}}$ ist. Also ist $f \in \cap_{\mathfrak{p}} A_{\mathfrak{p}} = A$, woraus die Implikation (3) $\Rightarrow$ (1) folgt. □

Bemerkung 5.5. Dies zeigt insbesondere, dass für einen ganz abgeschlossenen noetherschen Integritätsbereich A alle Lokalisierungen in Primidealen der Höhe 1 ganz abgeschlossen und damit diskrete Bewertungsringe sind.

Sei A ein Ring und

$$i : A \hookrightarrow B$$

eine ganze Ringerweiterung von A. Wir betrachten die davon induzierte Abbildung auf den Spektren von A und B:

$$\psi : \mathrm{Spec}(B) \to \mathrm{Spec}(A); \mathfrak{P} \mapsto \mathfrak{P} \cap A.$$

Lemma 5.6. *Ist $\mathfrak{p}$ ein Primideal in A der Höhe 1 und $\mathfrak{P} \in \psi^{-1}(\mathfrak{p})$, so hat auch $\mathfrak{P}$ die Höhe 1.*

Beweis. Sei $0 \subset \mathfrak{Q} \subset \mathfrak{P}$ eine Kette von Primidealen in B mit $\mathfrak{P} \cap A = \mathfrak{Q} \cap A = \mathfrak{p}$. Wir betrachten die Inklusion

$$A/\mathfrak{p} \hookrightarrow B/\mathfrak{Q}.$$

Wir nehmen an, es gäbe ein Element $x \in \mathfrak{P} - \mathfrak{Q}$. Dann erfüllt $\bar{x} \in B/\mathfrak{Q}$ eine (irreduzible) ganze Gleichung über $A/\mathfrak{p}$ mit konstantem Term $\bar{a} \neq 0$. Das bedeutet aber gerade, dass $xB \cap A \nsubseteq \mathfrak{p}$, ein Widerspruch zu $\mathfrak{P} \cap A = \mathfrak{p}$. Also ist $\mathfrak{P} = \mathfrak{Q}$. Für ein Ideal $\mathfrak{P} \in \psi^{-1}(\mathfrak{p})$ bedeutet dies: jedes Ideal, das echt kleiner ist als $\mathfrak{P}$, reduziert sich in A zu 0 (da $\mathfrak{p}$ die Höhe 1 hat) und ist daher nach unserer Argumentation selbst schon 0. Also hat $\mathfrak{P}$ die Höhe 1. □

Aufgrund dieses Lemmas hat die folgende Definition einer Bewertung auf A Sinn:

Definition 5.7. Seien A ein noetherscher Integritätsbereich und B der ganze Abschluss von A im Quotientenkörper $K = \mathrm{Quot}(A)$. Für $\mathfrak{p}$ in A mit der Höhe 1 und $f \in K = \mathrm{Quot}(A) = \mathrm{Quot}(B)$ setzen wir

$$\nu_{\mathfrak{p}}(f) := \sum_{\mathfrak{P} \in \psi^{-1}(\mathfrak{p})} \nu_{\mathfrak{P}}(i(f)). \tag{5.3}$$

Falls $A_\mathfrak{p}$ schon ganz abgeschlossen ist, liefert diese Definition die ursprüngliche Bewertung, wie es sein soll, denn:
Sei $\mathfrak{P}$ ein Ideal in B über $\mathfrak{p}$ und $A_\mathfrak{p}$ ganz abgeschlossen. Wir haben dann die Inklusionen

$$A_\mathfrak{p} \hookrightarrow B_\mathfrak{P} \hookrightarrow K = \mathrm{Quot}(A),$$

wobei $A_\mathfrak{p}$ ein diskreter Bewertungsring ist. Das bedeutet aber nach Bemerkung 5.2, dass $B_\mathfrak{P} = A_\mathfrak{p}$ ist und außerdem $\mathfrak{P}$ als einziges Ideal über $\mathfrak{p}$ liegt. (Ansonsten könnten wir B noch nach einem zweiten Primideal über $\mathfrak{p}$ lokalisieren, und der Durchschnitt dieser beiden Lokalisierungen wäre echt kleiner als $B_\mathfrak{P}$ und enthielte $A_\mathfrak{p}$, Widerspruch).

Da wir nun den Begriff der Bewertung auf beliebige noethersche Integritätsringe erweitert haben, hat auch Gleichung (5.2) nun für solche Ringe einen Sinn!

Insbesondere gilt mit dieser Definition auch im allgemeinen Fall (eines nicht notwendigerweise ganz abgeschlossenen noetherschen Integritätsringes):

$$\nu_\mathfrak{p}(fg) = \nu_\mathfrak{p}(f) + \nu_\mathfrak{p}(g). \tag{5.4}$$

Bemerkung 5.8. Falls $A = k[x_1, \ldots, x_n]/\mathfrak{p}$ der Koordinatenring einer affinen Kurve ist, bietet sich eine alternative Definition der Verschwindungsordnung von f im Punkt $P = V(\mathfrak{m})$. Wir setzen

$$\mu_\mathfrak{m}(f) := \dim_k A_\mathfrak{m}/(f).$$

Wenn $A = k[x, y]/(g)$ der Ring einer ebenen affinen Kurve ist und f irreduzibel ist, ist dies gerade die Schnittmultiplizität der Kurven $V(f)$ und $V(g)$ im Punkt P.

Wir betrachten einige konkrete Beispiele im Fall (singulärer) affiner Kurven:

Beispiel 5.9. Wir wählen $A = \mathbb{C}[x, y]/(y^2 - x^2 - x^3)$ (die 'Schleife') und betrachten den Primdivisor $[\mathfrak{p}] = [(x)]$.

Dieser Primdivisor entspricht gerade dem Nullpunkt des Koordinatensystems. Wir untersuchen nun die Ordnung der Funktionen x, y und $x - y$ in $\mathfrak{p}$.
Dazu betten wir entsprechend unserer Definition den Ring A in seinen ganzen Abschluss ein:

$$\begin{aligned} i : A = \mathbb{C}[x, y]/(y^2 - x^2 - x^3) &\hookrightarrow \mathbb{C}[t, x]/(t^2 - 1 - x) =: B \\ y &\mapsto tx \\ x &\mapsto x. \end{aligned}$$

Über dem Primideal (x) liegen in B die zwei Primideale $(t + 1)$ bzw. $(t - 1)$. Aus der in B gültigen Gleichung $x = (t - 1)(t + 1)$ sehen wir, dass die Funktion x in diesen beiden Punkten die Ordnung 1 hat und daher unserer Definition nach $\nu_\mathfrak{p}(x) = \nu_{(t-1)}(x) + \nu_{(t+1)}(x) = 2$.
Ebenso sehen wir, dass $i(y) = xt$ ebenfalls Ordnung 1 in den beiden Primidealen über $\mathfrak{p}$ hat, und daher $\nu_\mathfrak{p}(i(y)) = 2$.
Was passiert mit $x - y$? Hier haben wir $i(x - y) = x(1 - t) = -(t + 1)(t - 1)^2$. Es ist daher $\nu_\mathfrak{p}(i(x - y)) = 1 + 2 = 3$.
Beachte: In jedem dieser Beispiele ist $\nu_\mathfrak{p}(i(f)) = \dim_\mathbb{C} A_\mathfrak{p}/(f)$! Nehmen wir z.B. $f = x - y$: Aus $y^2 - x^2 - x^3 = (y - x)(y + x) - x^3$ sehen wir, dass $A_\mathfrak{p}/(f) = \mathbb{C}[x, y]_{(x)}/(y - x, y^3) \simeq \mathbb{C}[y]/y^3$, was offensichtlich ein 3-dimensionaler $\mathbb{C}$-Vektorraum ist. □

Dasselbe passiert im

Beispiel 5.10. $A := \mathbb{C}[x,y]/(y^2 - x^5)$.

Wir bestimmen wieder die Einbettung von A in seinen ganzen Abschluss:

$$\begin{aligned} i : A = \mathbb{C}[x,y]/(y^2 - x^5) &\hookrightarrow \mathbb{C}[t,x]/(t^2 - x) =: B \\ y &\mapsto tx^2 \\ x &\mapsto x. \end{aligned}$$

Über dem Primideal (x) liegt in diesem Fall nur ein Primideal, nämlich (t). Die Funktion $f = y \in A$ hat damit in $\mathfrak{p} = (x)$ die Ordnung $\nu_{(x)}(y) = \nu_{(t)}(x^2 t) = \nu_{(t)}(t^5) = 5$. Und wiederum ist $5 = \dim_{\mathbb{C}} A_{\mathfrak{p}}/(f)$. □

Dass diese Übereinstimmung unserer Definitionen der Verschwindungsordnung, die wir in den Beispielen beobachtet haben, kein Zufall ist, sehen wir im Folgenden.

Satz 5.11. *Ist A eine nullteilerfreie endlich erzeugte k-Algebra der Dimension 1 über einem algebraisch abgeschlossenen Körper k. Sei weiters $\mathfrak{p} \neq 0$ ein Primideal in A und $f \in A$. Dann gilt:*

$$\nu_{\mathfrak{p}}(f) = \dim_k A_{\mathfrak{p}}/(f) = \mu_{\mathfrak{p}}(f) \tag{5.5}$$

Beweis. Sei B der ganze Abschluss von A. Dann ist auch $B_{\mathfrak{p}} := (A - \mathfrak{p})^{-1}B$ ein noetherscher, eindimensionaler Integritätsbereich, der überdies ganz abgeschlossen ist (siehe z.B. Ser79, §3). Insbesondere ist also $B_{\mathfrak{p}}$ ein Dedekindring, was bedeutet, dass $fB_{\mathfrak{p}}$ eine eindeutige Zerlegung in Primideale besitzt:

$$fB_{\mathfrak{p}} = \mathfrak{P}_1^{n_1} \cdots \mathfrak{P}_r^{n_r},$$

wobei $n_i = \nu_{\mathfrak{P}_i}(f)$ ist. Also gilt nach dem Chinesischen Restsatz

$$B_{\mathfrak{p}}/fB_{\mathfrak{p}} \simeq B_{\mathfrak{p}}/\mathfrak{P}_1^{n_1} \times \cdots \times B_{\mathfrak{p}}/\mathfrak{P}_r^{n_r}.$$

Jetzt ist klar, dass

$$\dim_k B_{\mathfrak{p}}/fB_{\mathfrak{p}} = \sum \nu_{\mathfrak{P}_i}(f) = \nu_{\mathfrak{p}}(f)$$

gilt. Es ist noch zu zeigen, dass

$$\dim_k B_{\mathfrak{p}}/fB_{\mathfrak{p}} = \dim_k A_{\mathfrak{p}}/fA_{\mathfrak{p}}$$

ist.

Da mit B nach Lemma 5.4 aber auch $B_{\mathfrak{p}} = (A - \mathfrak{p})^{-1}B$ ganz abgeschlossen ist, ist $B_{\mathfrak{p}}$ offensichtlich der ganze Abschluss von $A_{\mathfrak{p}}$. Die gewünschte Gleichung folgt daher aus dem Korollar 5.13 unten, womit der Satz bewiesen ist. □

Sei im folgenden A eine nullteilerfreie, eindimensionale noethersche k-Algebra über einem algebraisch abgeschlossenen Körper k. Sei $f \in A - \{0\}$ und z algebraisch über $K = \mathrm{Quot}(A)$.

Lemma 5.12. *Ist z in $K = \mathrm{Quot}(A)$ und außerdem ganz über A, so ist*

$$\dim_k A[z]/A[z]f = \dim_k A/Af$$

für $f \in A$.

Da der ganze Abschluss von A über A endlich erzeugt ist, erhalten wir durch wiederholtes Anwenden des Lemmas das

Korollar 5.13. *Ist B der ganze Abschluss von A, so ist*

$$\dim_k A/fA = \dim_k B/fB.$$

Bevor wir das Lemma beweisen, versuchen wir eine geometrische Interpretation: Sei A der Koordinatenring einer Kurve X und P ein glatter Punkt auf X. Die Inklusion von Algebren $A \hookrightarrow A[z]$ entspricht einer Abbildung $Y \to X$ von Varietäten. Falls z im Quotientenkörper von A liegt, so hat P *höchstens* einen Urbildpunkt in Y. Ein Beispiel wäre die Inklusion $k[x] \to k[x, 1/x]$, die der Einbettung der Geraden ohne Nullpunkt in die Gerade entspricht. Indem wir überhaupt alle Brüche von Elementen aus A zu A hinzunehmen, erhalten wir den Extremfall, in dem Y leer ist. Der Beweis dieser Beobachtung verläuft wie die Argumentation im Anschluss an Definition 5.7 (der lokale Ring an einem glatten Punkt einer Kurve ist ein diskreter Bewertungsring!).

Umgekehrt ist bekannt, dass ein ganzer Morphismus von Varietäten surjektiv ist, und daraus motiviert sich die Erkenntnis: Punkte können beim Übergang zu einer ganzen Ringerweiterung nicht verschwinden, sondern höchstens mehr werden!

Insbesondere sehen wir, dass die Faser eines glatten Punktes unter einem Morphismus $A \hookrightarrow A[z], z \in K$ ganz über A wieder genau einen Punkt enthält (der lokale Ring ist ein diskreter Bewertungsring und daher schon maximal in K).

Das Lemma sagt nun, dass dies für die Schnittpunkte mit $\{f = 0\}$ inklusive Vielfachheit und insbesondere auch in singulären Punkten gilt: Nach Erweiterung von A um ein Element im ganzen Abschluss von A hat die 'neue' Kurve genausoviele Schnittpunkte mit $\{f = 0\}$ wie die 'alte'.

Das ist intuitiv plausibel, wenn wir uns vergegenwärtigen, dass für einen singulären Punkt P alle Punkte einer geeigneten punktierten Umgebung von P glatt sind, und dass sich dort die Anzahl der Schnittpunkte mit $\{f = 0\}$ entsprechend verhält. Das Lemma besagt also, dass sich dieses Verhalten bezüglich der Anzahl der Schnittpunkte in den singulären Punkt P fortsetzt.

Nun zum

Beweis. Wir verwenden das

Lemma 5.14. *(Schlangenlemma) Sei*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & G' & \longrightarrow & G & \longrightarrow & G'' & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle g} & & \downarrow{\scriptstyle h} & & \\ 0 & \longrightarrow & H' & \longrightarrow & H & \longrightarrow & H'' & \longrightarrow & 0 \end{array} \tag{5.6}$$

ein kommutatives Diagramm von abelschen Gruppen mit exakten Zeilen. Dann existiert eine exakte Folge von abelschen Gruppen

$$0 \to \ker f \to \ker g \to \ker h \to \operatorname{coker} f \to \operatorname{coker} g \to \operatorname{coker} h \to 0.$$

Beweis. Diagrammjagd. □

Weiters verwenden wir eine Verallgemeinerung der sogenannten 'Kern-Bild - Formel' für Vektorräume:

Lemma 5.15. *Sei*

$$0 \xrightarrow{\varphi_0} V_1 \xrightarrow{\varphi_1} \dots \xrightarrow{\varphi_n} V_n \to 0$$

eine exakte Folge von endlichdimensionalen Vektorräumen. Dann ist

$$\sum_{i=1}^{n} (-1)^i \dim V_i = 0.$$

Beweis. Nach der bekannten Kern-Bild-Formel ist $\dim V_i = \dim \ker \varphi_i + \dim \operatorname{im} \varphi_i = \dim \ker \varphi_i + \dim \ker \varphi_{i+1}$. Diese Ausdrücke, mit alternierendem Vorzeichen aufsummiert, ergeben 0. □

Schreiben wir nun in unserer speziellen Situation $B = A[z]$ und betrachten das Diagramm von *k-Vektorräumen*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & Af & \longrightarrow & A & \longrightarrow & A/Af & \longrightarrow & 0\,. \\ & & \downarrow & & \downarrow & & \downarrow h & & \\ 0 & \longrightarrow & Bf & \longrightarrow & B & \longrightarrow & B/Bf & \longrightarrow & 0 \end{array}$$

Nach dem Schlangenlemma haben wir eine exakte Folge

$$0 \to \ker h \to Bf/Af \to B/A \to \operatorname{coker} h \to 0.$$

Eine weitere exakte Folge ist trivial:

$$0 \to \ker h \to A/Af \to B/Bf \to \operatorname{coker} h \to 0.$$

Wie wir in Kürze noch nachtragen werden, sind B/A und Bf/Af endlichdimensionale k-Vektorräume, ebenso wie A/Af bzw. B/Bf. Mit Lemma (5.15) erhalten wir also die zwei Gleichungen

$$\dim_k \operatorname{coker} h - \dim_k \ker h = \dim_k B/A - \dim_k Bf/Af,$$

$$\dim_k \operatorname{coker} h - \dim_k \ker h = \dim_k B/Bf - \dim_k A/Af.$$

Um unsere Behauptung $\dim_k B/Bf = \dim_k A/Af$ zu zeigen, reicht es also aus, $\dim_k B/A = \dim_k Bf/Af$ zu zeigen! Wir betrachten dazu die Abbildung $b \mapsto fb$ als k-lineare Abbildung von B nach fB. Die kanonische Abbildung

$$\text{can} : B/A \to Bf/Af.$$

ist surjektiv per definitionem und injektiv, da B ein Integritätsring ist: Wenn für $b \in B$ gilt $bf = af$ mit $a \in A$, so folgt natürlich $b = a \in A$. Die Abbildung can ist also ein k-Isomorphismus, woraus $\dim_k B/A = \dim_k Bf/Af$ folgt.

Um diese Argumentation zu rechtfertigen, ist, wie gesagt, noch nachzuweisen, dass B/A und Bf/Af tatsächlich endlichdimensional über k sind. Aufgrund des gerade konstruierten Isomorphismus genügt es, dies für B/A nachzuprüfen:
Nach Voraussetzung erfüllt z eine ganze Gleichung, sagen wir

$$z^{m+1} = \sum_{i=0}^{m} \alpha_i z^i, \tag{5.7}$$

mit Koeffizienten $\alpha_i \in A$. D.h., B wird als A-Modul von den Elementen $1, z, \dots, z^m$ erzeugt. Weiters ist z im Quotientenkörper von A, also $g = hz$ mit $g, h \in A$. Sei $(v_1^{(i)}, \dots, v_{d_i}^{(i)})$ eine k-Basis von A/Ah^i. Wir zeigen nun, dass die Elemente $v_j^{(i)} z^i, i =$

$0, \ldots, m, j = 0, \ldots, d_i$ ein Erzeugendensystem von B/A bilden. Nach Gleichung (5.7) ist jedes Element in B eine Summe von Elementen der Form az^i mit $0 \leqslant i \leqslant m$. Sei also o.E.d.A. $b = az^i$. Aus

$$b = az^i = (h^i + \xi_1 v_1 + \cdots + \xi_{d_i} v_{d_i})z^i = g^i + \xi_1 v_1 z^i + \cdots + \xi_{d_i} v_{d_i} z^i, \quad \xi_j \in k.$$

folgt also tatsächlich $\bar{b} \in \langle v_j^{(i)} z^i, i = 0, \ldots, m, j = 0, \ldots, d_i \rangle$, womit wir das Lemma bewiesen haben. □

Korollar 5.16.

$$\dim_k A_\mathfrak{p}/(fg) = \dim_k A_\mathfrak{p}/(f) + \dim_k A_\mathfrak{p}/(g).$$

Beweis. Gleichung (5.4) und Satz 5.11. □

Wir können Lemma (5.12) sogar auf beliebige ganze Erweiterungen von A verallgemeinern. Dazu ein

Hilfssatz 5.17. *Es sei z so gewählt, dass ein normiertes Minimalpolynom f_z von z (über $K = \mathrm{Quot}(A)$) mit Koeffizienten in A existiert, d.h., das Minimalpolynom von z ist schon* ganz. *Dann gilt*

$$\dim_k A[z]/A[z]f = \deg_z \cdot \dim_k A/Af,$$

wobei $\deg_z = \deg_{f_z}$ der Grad des Minimalpolynoms ist.

Beweis. Sei $n = \deg_z$. In dieser Situation ist

$$A[z] \simeq A \oplus Az \oplus Az^{n-1} \simeq A^n,$$

denn: Es ist klar, dass $A[z]$ als A-Modul von den Potenzen $1, z, \ldots, z^{n-1}$ erzeugt wird. Weiters bestehen aber zwischen diesen Elementen keine A-linearen Relationen, da sonst z Nullstelle eines Polynoms vom Grad $< n$ wäre, im Widerspruch zur Voraussetzung.
Weiters ist $fA[z] \simeq fA \oplus fAz \oplus fAz^{n-1} \simeq (fA)^n$. Und da direkte Summen mit Quotientenbildung vertauschen, gilt schließlich

$$A[z]/fA[z] \simeq A/fA \oplus Az/fAz \oplus Az^{n-1}/fAz^{n-1} \simeq (A/fA)^n.$$

Daraus folgt $\dim_k A[z]/A[z]f = n \cdot \dim_k A/Af$. □

Satz 5.18. *Ist z ganz über A und vom Grad $\deg_z$ über $K = \mathrm{Quot}(A)$, so ist*

$$\dim_k A[z]/A[z]f = \deg_z \cdot \dim_k A/Af$$

für $f \in A$. (Der Grad von z ist i.a. kleiner *als der Grad einer minimalen ganzen Gleichung, die z erfüllt! - siehe auch Lemma* (5.12)*.)*

Beweis. Wir schreiben $z = \frac{x}{y}$, sodass x ein Minimalpolynom wie im Hilfssatz hat und y in A liegt. Dann ist $A[z] = (A[x])[\frac{x}{y}]$ und wir erhalten die Behauptung aus den Gleichungen

$$\dim_k A[x]/A[x]f = \deg_x \cdot \dim_k A/Af$$

(nach dem Hilfssatz), und

$$\dim_k A[z]/A[z]f = \dim_k A[x]/A[x]f$$

(wegen Lemma (5.12)). Es ist klar dass $\deg_x = \deg_z$. □

Kapitel 6

Anhang

6.1 Gegenbeispiele zur Casas-Álvero-Vermutung vom Grad 8 in Charakteristik 17

$$15X^2 + X^3 + X^8$$
$$6X^2 + X^4 + X^8$$

$$X + 11X^2 + X^4 + X^5 + X^8$$
$$2X + 3X^3 + 10X^4 + X^5 + X^8$$
$$13X + 2X^2 + 3X^3 + 10X^4 + X^5 + X^8$$
$$15X^3 + 13X^4 + X^5 + X^8$$

$$3X + 7X^2 + 3X^3 + 3X^6 + X^8$$
$$8X + 9X^2 + 5X^3 + 3X^6 + X^8$$
$$9X + 9X^2 + 12X^3 + 3X^6 + X^8$$
$$14X + 7X^2 + 14X^3 + 3X^6 + X^8$$
$$2X + 4X^4 + 3X^6 + X^8$$
$$15X + 4X^4 + 3X^6 + X^8$$
$$11X + 11X^2 + X^3 + 4X^4 + 3X^6 + X^8$$
$$6X + 11X^2 + 16X^3 + 4X^4 + 3X^6 + X^8$$
$$11X^4 + 3X^6 + X^8$$
$$15X + 9X^2 + X^3 + 11X^4 + 3X^6 + X^8$$
$$2X + 9X^2 + 16X^3 + 11X^4 + 3X^6 + X^8$$
$$7X^2 + 14X^4 + 3X^6 + X^8$$
$$X + 14X^2 + 6X^3 + X^5 + 3X^6 + X^8$$
$$12X + 7X^2 + X^3 + 14X^4 + X^5 + 3X^6 + X^8$$

$$2X^5 + 3X^6 + X^8$$
$$16X + 11X^2 + 2X^5 + 3X^6 + X^8$$
$$13X + 11X^2 + 7X^3 + 6X^4 + 2X^5 + 3X^6 + X^8$$
$$16X + 2X^2 + 3X^3 + 12X^4 + 2X^5 + 3X^6 + X^8$$
$$10X^2 + 2X^3 + X^4 + 5X^5 + 3X^6 + X^8$$
$$14X^2 + 12X^3 + 2X^4 + 5X^5 + 3X^6 + X^8$$
$$15X^3 + 6X^5 + 3X^6 + X^8$$
$$5X + 7X^2 + 8X^3 + 10X^4 + 8X^5 + 3X^6 + X^8$$
$$12X + 7X^2 + 9X^3 + 10X^4 + 9X^5 + 3X^6 + X^8$$
$$2X^3 + 11X^5 + 3X^6 + X^8$$
$$10X^2 + 15X^3 + X^4 + 12X^5 + 3X^6 + X^8$$
$$14X^2 + 5X^3 + 2X^4 + 12X^5 + 3X^6 + X^8$$
$$15X^5 + 3X^6 + X^8$$
$$X + 11X^2 + 15X^5 + 3X^6 + X^8$$
$$4X + 11X^2 + 10X^3 + 6X^4 + 15X^5 + 3X^6 + X^8$$
$$X + 2X^2 + 14X^3 + 12X^4 + 15X^5 + 3X^6 + X^8$$
$$16X + 14X^2 + 11X^3 + 16X^5 + 3X^6 + X^8$$
$$5X + 7X^2 + 16X^3 + 14X^4 + 16X^5 + 3X^6 + X^8$$
$$5X^4 + X^6 + X^8$$
$$16X^2 + 11X^4 + X^6 + X^8$$

$$7X + 12X^2 + 4X^4 + X^7 + X^8$$
$$11X + 8X^3 + 11X^4 + X^7 + X^8$$
$$4X + 12X^2 + 8X^3 + 11X^4 + X^7 + X^8$$
$$4X + 13X^3 + X^4 + X^5 + X^7 + X^8$$
$$14X^2 + 13X^4 + X^5 + X^7 + X^8$$
$$13X^2 + 11X^3 + 2X^4 + 6X^5 + X^7 + X^8$$
$$11X + 3X^2 + 2X^3 + 14X^4 + 6X^5 + X^7 + X^8$$
$$10X^2 + 2X^4 + 7X^5 + X^7 + X^8$$
$$11X + 7X^2 + 12X^4 + 7X^5 + X^7 + X^8$$
$$X + 13X^2 + 11X^3 + 13X^4 + 10X^5 + X^7 + X^8$$
$$4X^2 + 4X^3 + 12X^5 + X^7 + X^8$$
$$9X + 2X^2 + 7X^3 + 12X^5 + X^7 + X^8$$
$$14X + X^3 + 5X^4 + 12X^5 + X^7 + X^8$$
$$15X^2 + 4X^3 + 10X^4 + 12X^5 + X^7 + X^8$$
$$6X + 10X^3 + 10X^4 + 12X^5 + X^7 + X^8$$
$$X^3 + 11X^4 + 12X^5 + X^7 + X^8$$
$$11X^2 + 4X^3 + 11X^4 + 12X^5 + X^7 + X^8$$

$$14X + 8X^4 + 15X^5 + X^7 + X^8$$
$$10X + 14X^2 + 6X^3 + 16X^5 + X^7 + X^8$$
$$7X + X^2 + 13X^4 + 16X^5 + X^7 + X^8$$
$$8X + 8X^2 + 10X^3 + X^4 + 5X^5 + 2X^6 + X^7 + X^8$$
$$15X + 15X^2 + 11X^3 + 3X^5 + 3X^6 + X^7 + X^8$$
$$X + 2X^3 + 2X^4 + 7X^5 + 3X^6 + X^7 + X^8$$
$$7X + 16X^2 + 15X^3 + 13X^5 + 3X^6 + X^7 + X^8$$
$$X + 10X^2 + 4X^3 + 4X^6 + X^7 + X^8$$
$$12X + 10X^3 + 13X^4 + 4X^6 + X^7 + X^8$$
$$5X + 12X^2 + 16X^4 + X^5 + 4X^6 + X^7 + X^8$$
$$6X + 11X^2 + 5X^4 + 14X^5 + 4X^6 + X^7 + X^8$$
$$5X + 8X^2 + 12X^3 + 15X^5 + 4X^6 + X^7 + X^8$$
$$16X + 9X^2 + 14X^3 + 5X^6 + X^7 + X^8$$
$$8X + X^2 + 4X^4 + 3X^5 + 5X^6 + X^7 + X^8$$
$$15X + 4X^2 + X^3 + 4X^4 + 3X^5 + 5X^6 + X^7 + X^8$$
$$3X + 9X^2 + 16X^5 + 5X^6 + X^7 + X^8$$
$$13X + 7X^3 + 13X^4 + 7X^6 + X^7 + X^8$$
$$11X + 8X^2 + 9X^3 + X^4 + 11X^5 + 7X^6 + X^7 + X^8$$
$$8X^2 + 5X^4 + 13X^5 + 7X^6 + X^7 + X^8$$
$$11X + 6X^2 + 11X^3 + 11X^4 + 6X^5 + 9X^6 + X^7 + X^8$$
$$11X + 2X^2 + 10X^6 + X^7 + X^8$$
$$2X + 15X^2 + 10X^6 + X^7 + X^8$$
$$16X + 14X^2 + 10X^3 + 2X^4 + 10X^6 + X^7 + X^8$$
$$2X + 11X^2 + 9X^3 + 5X^4 + 10X^6 + X^7 + X^8$$
$$2X + 14X^2 + 14X^3 + 3X^5 + 10X^6 + X^7 + X^8$$
$$3X + 7X^2 + 13X^4 + 4X^5 + 10X^6 + X^7 + X^8$$
$$11X + 8X^2 + 16X^4 + 4X^5 + 10X^6 + X^7 + X^8$$
$$8X + 5X^2 + 9X^3 + 15X^4 + 6X^5 + 10X^6 + X^7 + X^8$$
$$3X^3 + 14X^4 + 7X^5 + 10X^6 + X^7 + X^8$$
$$6X^3 + 9X^5 + 10X^6 + X^7 + X^8$$
$$5X^2 + 6X^3 + X^4 + 10X^5 + 10X^6 + X^7 + X^8$$
$$16X + 11X^3 + 11X^5 + 10X^6 + X^7 + X^8$$
$$8X + 15X^4 + 11X^5 + 10X^6 + X^7 + X^8$$
$$5X + 3X^2 + 12X^3 + 15X^4 + 11X^5 + 10X^6 + X^7 + X^8$$
$$4X + 4X^2 + 16X^3 + 15X^4 + 11X^5 + 10X^6 + X^7 + X^8$$
$$14X + 14X^2 + 10X^3 + 2X^4 + 15X^5 + 10X^6 + X^7 + X^8$$
$$13X + 2X^2 + 6X^3 + 5X^4 + 15X^5 + 10X^6 + X^7 + X^8$$
$$5X + 6X^2 + 12X^3 + 16X^5 + 10X^6 + X^7 + X^8$$

$$14X^2 + 16X^3 + 6X^4 + 13X^6 + X^7 + X^8$$
$$12X + 8X^4 + 4X^5 + 13X^6 + X^7 + X^8$$
$$2X + 11X^3 + 11X^4 + 11X^5 + 13X^6 + X^7 + X^8$$
$$12X + 4X^2 + 6X^3 + 16X^4 + 15X^5 + 13X^6 + X^7 + X^8$$
$$12X + 13X^2 + 11X^3 + 12X^4 + 15X^6 + X^7 + X^8$$
$$3X^2 + 3X^3 + 8X^4 + 6X^5 + 15X^6 + X^7 + X^8$$
$$9X + 2X^2 + 6X^3 + 10X^4 + 7X^5 + 15X^6 + X^7 + X^8$$
$$7X^2 + 2X^3 + 15X^4 + 15X^5 + 15X^6 + X^7 + X^8$$
$$16X + 3X^2 + 14X^3 + 16X^6 + X^7 + X^8$$
$$10X + 7X^2 + 14X^3 + 2X^5 + 16X^6 + X^7 + X^8$$
$$3X + 7X^2 + 7X^5 + 16X^6 + X^7 + X^8$$
$$4X + 12X^2 + 10X^3 + 7X^5 + 16X^6 + X^7 + X^8$$
$$2X + 6X^3 + X^4 + 7X^5 + 16X^6 + X^7 + X^8$$
$$16X + 16X^2 + 11X^4 + 7X^5 + 16X^6 + X^7 + X^8$$
$$9X + 14X^3 + 11X^4 + 7X^5 + 16X^6 + X^7 + X^8$$
$$12X + 7X^3 + 2X^4 + 12X^5 + 16X^6 + X^7 + X^8$$
$$16X + 4X^3 + 14X^4 + 15X^5 + 16X^6 + X^7 + X^8$$

Literaturverzeichnis

[AM69] M. F. Atiyah and I.G. Macdonald, *Introduction to commutative algebra*, Reading, Addison-Wesley, Mass., 1969.

[Bou89] Bourbaki, *Algebra*, 2. ed., Elements of Mathematics, 1989.

[Eis95] David Eisenbud, *Commutative algebra with a view toward algebraic geometry*, Graduate texts in mathematics ; 150, Springer, Berlin [u.a.], 1995.

[Har00] Robin Hartshorne, *Algebraic geometry*, Graduate texts in mathematics ; 52, Springer, New York [u.a.], 2000.

[HM93] Herwig Hauser and Gerd Mueller, *Affine varieties and lie algebras of vector bundles*, Manuscripta Mathematica **80** (1993), 309–373.

[Kaw06] Hiraku Kawanoue, *Toward resolution of singularities over a field of positive characteristic*, Part I.

[Kob77] Neal Koblitz, *P-adic numbers, p-adic analysis, and zeta-functions*, Graduate texts in mathematics ; 58, Springer, New York [u.a.], 1977.

[Lor96] Dino Lorenzini, *An invitation to arithmetic geometry*, Graduate studies in mathematics ; 9, American Mathematical Soc., Providence, RI, 1996.

[Ser79] Jean-Pierre Serre, *Local fields*, Graduate texts in mathematics ; 67, Springer, New York [u.a.], 1979.

[vLSv06] Hans-Christian Graf von Bothmer, Oliver Labs, Josef Schicho, and Christiaan van de Woestijne, *The casas-alvero conjecture for infinitely many degrees*, 2006.