

EXPLIZITE AUFLÖSUNG VON EBENEN KURVENSINGULARITÄTEN IN BELIEBIGER CHARAKTERISTIK

von Herwig HAUSER und Georg REGENSBURGER

INHALTSVERZEICHNIS

1. Einleitung	1
2. Beispiele	9
3. Die Ordnung	12
4. Das Newton-Polygon	12
5. Koordinatenwechsel	16
6. Die maximale Steigung	22
7. Die Auflösungsinvariante	25
8. Aufgelöste Punkte	26
9. Explosion eines Punktes	30
10. Total und Strikt Transformierte	32
11. Die Invariante fällt unter Explosion	34
12. Beweis des Hauptsatzes	39
A. Appendix	40
A.1 Potenzreihenringe	40
A.2 Gauß-Bruhat Zerlegung	60
A.3 Singuläre Punkte	62

1. EINLEITUNG

Die vorliegende Arbeit beschreibt die Konstruktion einer Auflösung von ebenen Kurvensingularitäten in beliebiger Charakteristik. Die Darstellung ist vollständig und detailliert – sie setzt nur die elementaren Grundkenntnisse der algebraischen Geometrie und kommutativen Algebra voraus. Prägnant formuliert lautet die zu beweisende Aussage wie folgt.

SATZ. Jede singuläre ebene algebraische Kurve ist der Schatten einer glatten algebraischen Kurve unter einer geeigneten Projektion.

Seit Mitte des neunzehnten Jahrhunderts ist die Auflösung der Singularitäten algebraischer Varietäten ein zentrales Thema der algebraischen Geometrie. Kronecker, Noether, Dedekind, Riemann, Weber, Picard, Jung, ... sowie die Geometer der italienischen Schule – Enriques, Chisini, Bertini, del Pezzo, Levi, ... – beweisen wiederholt und mit ähnlichen Methoden die Existenz von Auflösungen ebener algebraischer Kurven über \mathbb{C} . Siehe [Za, Sg, Ab1, Lp, Ha1] für Details über die historische Entwicklung. Die Arbeiten lassen vielfach die heutzutage selbstverständliche Präzision der Begriffe und Argumente vermissen. Grundlegendes Hilfsmittel war (und ist auch heute noch) die Explosion (Aufblasung) des umgebenden Raumes (der Ebene oder einer zweidimensionalen Mannigfaltigkeit) durch den lokalen Übergang zum Möbiusband (“Wendeltreppe”). Durch Kontraktion des Nullschnittes des Möbiusbandes auf einen Punkt erhält man eine Projektionsabbildung auf die Ebene, siehe Abbildung 1.

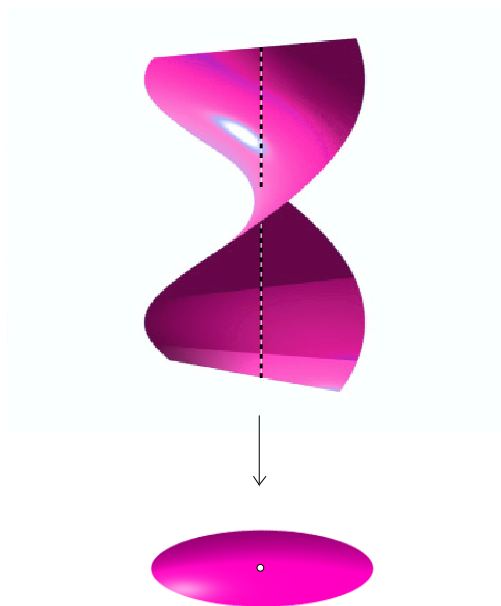


ABBILDUNG 1
Das Möbiusband

Das Hochziehen der gegebenen Kurve (wobei der singuläre Punkt gerade die Projektion des Nullschnittes sein soll) von der Ebene auf das Möbiusband soll die Singularität der Kurve entflechten. Geometrisch ist das einsichtig für gewöhnliche Doppelpunkte, d.h., transversale Selbstschnitte der Kurve, deren Zweige durch das Hochziehen getrennt werden, siehe Abbildung 2.

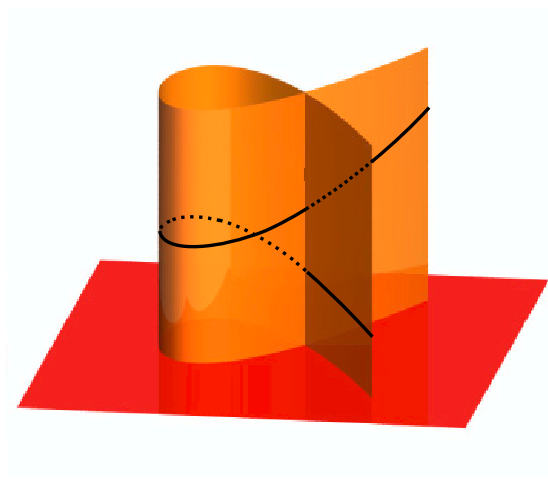


ABBILDUNG 2
Hochziehen der Schleife

Bei Spitzen benötigt man bereits eine algebraische Überlegung, um zu sehen, dass das Urbild der Kurve “weniger singulär” als die Ausgangssingularität ist. Für die einfachste Spitze mit Gleichung $x^3 = y^2$ erhält man in einem Transformations-Schritt eine glatte Kurve, siehe Abbildung 3. Bei komplizierteren Kurven sind mehrere Iterationen dieses Prozesses notwendig. Der Satz über die Existenz von Auflösungen von Kurven besagt, dass immer *endlich viele* Transformationen genügen, um auf diese Weise eine glatte Kurve zu erhalten.

Oben beschriebene Transformation der Ebene zum Möbiusband und das Hochziehen der eingebetteten Kurve nennt man die “Explosion des Nullpunktes in der Ebene” und den Übergang von der Kurve zu ihrer “strikt transformierten”. Diese Transformation war den algebraischen Geometern des neunzehnten Jahrhunderts geläufig. Sie ist auch unter den Namen “Punktaufblasung”, “quadratische Transformation”, “Hopf-Abbildung” oder “sigma-Prozess” bekannt. Dulac verwendet sie zur Vereinfachung und Klassifikation von (singulären) Differentialgleichungen.

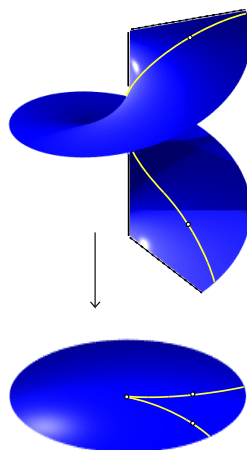


ABBILDUNG 3
Auflösung der Spitze

Mit Zariski findet um 1940 in der Auflösungsproblematik eine starke und sehr erfolgreiche Algebraisierung statt. Von nun an werden algebraische Varietäten über beliebigen Körpern oder über dem Ring der ganzen Zahlen \mathbf{Z} betrachtet. Zariski erkennt bereits, dass der Fall positiver Charakteristik wesentlich vertrackter ist, ebenso wie die arithmetische Situation. Schon zu Zeiten Zariski's war der Fall von Kurven in positiver Charakteristik als gelöst betrachtet worden. Sein Schüler Abhyankar beweist in einer spektakulären und technisch anspruchsvollen Arbeit Mitte der fünfziger Jahre die Existenz von Auflösungen für Flächen in Charakteristik $p > 0$ [Ab3].

Die in der Literatur vorliegenden Beweise der Kurvenauflösung lassen sich im wesentlichen in zwei Typen einteilen.

- (1) Auflösung durch Normalisierung: Der Koordinatenring R der (nicht notwendig ebenen) irreduziblen Kurve C wird in seinen Funktionenkörper $K = \text{Quot } R$ eingebettet. Man zeigt, dass der ganze Abschluss \tilde{R} von R in K wieder der Koordinatenring einer Kurve \tilde{C} ist. Diese Kurve \tilde{C} , die Normalisierung von C , erweist sich als glatte Kurve. Die Inklusion $R \subset \tilde{R}$ induziert die gewünschte Projektionsabbildung $\tilde{C} \rightarrow C$. Literatur: Zariski-Samuel [ZS, vol. II, p. 93], Mumford [Mu, III.8], Shafarevic [Sh, II.5].

Vorteil: Man erhält die Auflösung in einem Schritt. Charakteristikunabhän-

gig. War es ursprünglich mühsam, die Normalisierung zu berechnen, so gibt es heute dafür in Computeralgebra-Systeme integrierte Algorithmen.
Nachteil: Man verliert die Einbettung der Kurve. Die gleiche Methode via Normalisierung funktioniert für Flächen nur unter Hinzunahme von Explosionen, und versagt vollkommen in Dimension ≥ 3 .

- (2) Auflösung durch Folge von Punktexplosionen des umgebenden Raumes: Hier besteht das zentrale Problem darin, zu zeigen, dass man in endlich vielen Schritten eine glatte Kurve erhält. Dazu kann man drei verschiedene Argumente verwenden.

- (2a) Verwendung der Normalisierung: Die Normalisierung der Kurve faktorisiert über jede Explosion der Kurve, und da die Ringerweiterung $R \subset \tilde{R}$ endlich ist, muss die Folge der Explosionen stationär werden. Das bedeutet, dass die in hinreichend vielen Schritten erhaltene Kurve glatt ist. Literatur: Campillo [Cp, Thm. 1.5.10].

Vorteil: Sehr elegantes und schnelles Argument. Funktioniert auch für Raumkurven. Charakteristikunabhängig.

Nachteil: Argument versagt in höherer Dimension. Keine Aussage über die mindestens notwendige Anzahl von Explosionen.

- (2b) Induktion über das arithmetische Geschlecht: Für ebene (projektive) Kurven wird das arithmetische Geschlecht definiert als

$$\frac{1}{2}(d-1)(d-2) - \frac{1}{2} \sum_p r_p(r_p - 1),$$

wobei d der Grad der Kurve ist, die Summe über alle singulären Punkte p der Kurve läuft, und r_p die Multiplizität der Kurve in p bezeichnet. Das Geschlecht fällt unter Explosion in einem singulären Punkt der Kurve. Da das Geschlecht nicht negativ werden kann, muss nach endlich vielen Schritten die Kurve glatt geworden sein. Die Argumentation geht auf Bertini zurück. Literatur: Fulton [Fu, chap. 7], Hartshorne [Hs, Thm. 3.9, chap. V].

Vorteil: Induktionsinvariante kann direkt definiert werden. Charakteristikunabhängig.

Nachteil: Funktioniert nicht für Raumkurven. Verwendet wesentlich die Theorie der Flächen. Argument versagt in höherer Dimension.

- (2c) Induktion über Ordnung und Steigung des Newton-Polygons: Jedem singulären Punkt der Kurve wird ein Paar von Zahlen zugeordnet. Die erste Komponente ist die Ordnung der Taylorentwicklung des definierenden Polynoms im Punkt (Multiplizität), die zweite die Steigung eines genau spezifizierten Segments des Newton-Polygons des Polynoms. Das

Paar wird bezüglich der lexikographischen Ordnung betrachtet. Es fällt unter jeder Explosion, solange der Punkt singular ist. Da die lexikographische Ordnung eine Wohlordnung ist, sind nach endlich vielen Explosionen alle Punkte regulär. Literatur: Brieskorn-Knörrer [BK] in Charakteristik Null, Abhyankar [Ab2] und Orbanz [Or] in beliebiger Charakteristik.

Vorteil: Sehr explizit und elementar. Charakteristikunabhängig. Funktioniert mit entsprechenden Erweiterungen auch in höherer Dimension, allerdings bis jetzt nur in Charakteristik Null. Beinhaltet bereits die zentrale Idee, eine Induktion über die Dimension des umgebenden Raumes zu verwenden.

Nachteil: Etwas rechnerisch. Keine tiefere Einsicht in die Geometrie der Singularitäten. Funktioniert in beliebiger Charakteristik nicht direkt für Raumkurven.

Es gibt weitere Beweise für die Kurvenauflösung, siehe etwa Casas [Cs, sec. 3.7] für eine etwas andere Induktionsinvariante in Charakteristik 0, oder Oka [Ok] und Goldin-Teissier [GT] für einen Zugang über torische Modifikationen.

Die vorliegende Arbeit beweist die Auflösung von ebenen Kurvensingularitäten durch Induktion über das Paar (Ordnung, Steigung) wie in (2c). Eine ähnlich explizite Darstellung, allerdings beschränkt auf den Fall der Charakteristik Null, findet sich im Buch von Brieskorn-Knörrer, das sich gut als begleitende Lektüre zu diesem Artikel eignet. Die Darstellung von Abhyankar in [Ab2] ist sehr suggestiv, wenn auch im Detail nicht ganz leicht nachzuvollziehen. Wir empfehlen auch den Artikel von Orbanz [Or] als Ergänzung und Abrundung.

Hier ist eine präzise Version des Satzes, mit dessen Beweis wir uns beschäftigen wollen.

SATZ. Sei C eine ebene algebraische Kurve definiert über einem algebraisch abgeschlossenen Körper beliebiger Charakteristik. Sei a ein Punkt von C und $f(x, y) = 0$ eine definierende Gleichung von C in einer Umgebung von a in der umgebenden zweidimensionalen Mannigfaltigkeit M . Dann gibt es zu C und a ein Paar $(r, s) \in \mathbf{N}^2$, das unabhängig von der Wahl lokaler Koordinaten von M in a ist, und das für singuläres a unter der Punktexplosion von M in a in jedem Punkt a' der strikt transformierten C' von C bezüglich der lexikographischen Ordnung auf \mathbf{N}^2 fällt,

$$(r', s') <_{\text{lex}} (r, s).$$

Insbesondere wird jede ebene Kurve durch iteriertes Explodieren ihrer singulären Punkte in endlich vielen Schritten aufgelöst.

Als erstes müssen natürlich die verwendeten Begriffe definiert und erläutert werden. Als Erleichterung für den Leser schicken wir dem Text einige Beispiele voraus. In unserer Präsentation denken wir vor allem an den Vortragenden, der sein Manuskript zur Vorlesung Algebraische Geometrie vorbereitet. Im Hauptteil entwickeln wir die wesentlichen Ideen und Konzepte, im Anhang werden die notwendigen Hilfsmittel aus der kommutativen Algebra bereitgestellt.

Die Auflösung von Kurvensingularitäten ist ein klassisches und wichtiges Thema der algebraischen Geometrie. Die Beweistechnik beruht, ausgehend von geometrischen Überlegungen, auf Begriffen und Sätzen der kommutativen Algebra, die jeder Studierende einmal *in realiter* angewandt gesehen haben sollte. Die verwendete Induktion über ein lexikographisch geordnetes Paar von Invarianten ist ein Musterbeispiel für elegante und ökonomische Beweisführung. Schlussendlich ist der Kurvenfall als Vorläufer des Falles beliebiger Dimension ein ausgezeichnetes Beispiel, um Hironaka's Beweis für beliebige Varietäten in Charakteristik Null zu verstehen. Siehe dazu die Originalarbeit von Hironaka [Hi] und die nachfolgenden Weiterentwicklungen, bzw. Vereinfachungen seines Beweises durch Aroca, Vicente, Villamayor, Encinas, Bierstone-Milman und Hauser [AHV1, AHV2, Vi1, Vi2, EV, BM, EH, Ha2].

Gleichzeitig ist ein tiefes Verständnis des Kurvenfalls in positiver Charakteristik die Voraussetzung dafür, das bislang noch immer ungelöste Problems der Auflösung algebraischer Varietäten beliebiger Dimension in positiver Charakteristik $p > 0$ anzugehen, siehe etwa [Ha3, Ha4] für eine Beschreibung der auftretenden Probleme.

Wir beschreiben nun kurz das in dieser Arbeit verfolgte und klassisch vielfach verwendete Beweisschema. Eine Kurve hat nur endlich viele Singularitäten, also genügt es, jede einzeln zu betrachten und aufzulösen. Wir können uns hiermit auf lokale Überlegungen beschränken und die Kurve als in die affine Ebene A^2 eingebettet sehen. Unter Explosion geht ein singulärer Punkt der Kurve in höchstens endlich viele singuläre Punkte der transformierten Kurve über. Wieder genügt es, einen herauszugreifen. Damit erhalten wir einen Homomorphismus der zugehörigen lokalen Koordinatenringe als hauptsächliches Objekt unserer Untersuchungen.

Ein wesentliche Vereinfachung stellt nun der Übergang zu den Vervollständigungen der lokalen Ringe dar. Damit können wir im Ring der formalen Potenzreihen arbeiten. Dies erleichtert die Konstruktion der Invarianten. Die

Vervollständigung des lokalen Koordinatenringes der Kurve ist ein Faktoring des formalen Potenzreihenrings in zwei Variablen nach einem Hauptideal, nämlich dem Ideal, das von der definierenden Gleichung der Kurve erzeugt wird. Jedem solchen Faktoring wollen wir ein Paar von Zahlen zuordnen, und zwar so, dass das Paar unter Explosion lexikographisch fällt. Dazu ist es natürlich notwendig, das Paar intrinsisch zu wählen, d.h., unabhängig von der Wahl von Koordinaten oder anderen Hilfsmitteln.

Die erste Komponente des Paares wird die Ordnung der Taylorentwicklung des die Kurve definierenden Polynoms im singulären Punkt sein. Klarerweise ist sie intrinsisch. Die zweite Komponente wird durch die Wahl von lokalen Koordinaten und die Betrachtung des Newton-Polygons der Kurve eingeführt. Sie wird definiert als ein (geeignetes) Vielfaches der Steigung eines ausgezeichneten Segments des Newton-Polygons. Um diese Steigung koordinatenu-nabhängig zu machen, wird ihr Maximum über alle Koordinaten als Invariante genommen. Man erhält ein Paar von Zahlen (r, s) in \mathbf{N}^2 (bis auf Multiplikation mit einer fixen positiven Zahl, die etwaige Nenner bereinigt). Dieses Paar heißt die lokale Auflösungsinvariante der Kurve im betrachteten Punkt.

Dem Verhalten dieses Paares unter Explosion gilt nun unser Hauptaugenmerk. Es ist leicht zu zeigen, dass die erste Komponente, die Ordnung, unter Explosion nicht steigen kann, wenn man von der Kurve zu ihrer strikt transformierten übergeht. Damit kann man sich, per Induktion über die Ordnung, im weiteren auf den Fall beschränken, wo diese Ordnung gleich bleibt (ist sie gefallen, ist auch das Paar (r, s) lexikographisch gefallen). Die Konstanz der Ordnung einer Kurve unter der Explosion hat Konsequenzen auf das Newton-Polygon der definierenden Gleichung vor und nach der Explosion. Durch die explizite Konstruktion von Koordinatenwechseln, die die maximale Steigung des ausgezeichneten Segments realisieren, gelingt es, die der Explosion zugrunde liegende Koordinatentransformation monomial zu machen. Nun ist es ein Leichtes, die Veränderung der Steigung am Newton-Polygon abzulesen. Und in der Tat, die maximale Steigung fällt, wenn die Ordnung gleich geblieben ist. Damit ist der Induktionsschritt vollständig durchgeführt: Das der Singularität zugeordnete Paar von Zahlen fällt unter Explosion,

$$(r', s') <_{lex} (r, s).$$

Da \mathbf{N}^2 mit der lexikographischen Ordnung wohlgeordnet ist, also jede absteigende Folge stationär wird, können wir Induktion über unsere Invariante anwenden. Nach endlich vielen Explosionen erreicht in jedem Punkt die lokale Auflösungsinvariante ihr Minimum. Dies tritt ein, wenn die Ordnung der Taylorentwicklung des definierenden Polynoms auf 1 gesunken ist (in welchem

Fall die maximale Steigung irrelevant ist). Das heißt aber gerade, dass die Kurve im betrachteten Punkt glatt ist. Genau das war zu zeigen.

2. BEISPIELE

Wir diskutieren die wesentlichen Punkte der Konstruktion der Auflösungs-invariante an den folgenden drei Beispielen. Sei

$$f(y, z) = y^3 + z^4.$$

Die Variablensubstitution

$$(y, z) \mapsto (yz, z)$$

in f entspricht der Explosion des Nullpunktes in \mathbf{A}^2 (betrachtet in einer affinen Karte). Wir erhalten als total Transformierte f^* von f

$$f^* = f(yz, z) = y^3 z^3 + z^4.$$

Wir können aus f^* das irrelevante Monom z^3 faktorisieren (dieses entspricht der exzeptionellen Komponente) und erhalten das Polynom

$$f'(y, z) = y^3 + z,$$

die strikt Transformierte von f in der betrachteten Karte. Die Ordnung von f' im Nullpunkt dieser Karte ist

$$\text{ord}_0 f' = 1 < 3 = \text{ord}_0 f,$$

also hat sich die Singularität von f verbessert (jeweils im Nullpunkt der Karten). Wir sind sogar nach einer Explosion bei einer regulären (einer Kurve mit Ordnung 1) angelangt.

Sei nun

$$f = y^3 + z^7.$$

Dann ist

$$f^* = f(yz, z) = y^3 z^3 + z^7 \quad \text{und} \quad f'(y, z) = y^3 + z^4.$$

Also gilt für die Ordnung

$$\text{ord}_0 f' = \text{ord}_0 f = 3.$$

Trotzdem hat sich die Situation verbessert, denn wir wissen vom vorherigen Beispiel, daß wir nach einer weiteren Explosion eine reguläre Kurve erhalten. Um dies auch anhand unserer Auflösungs-invariante zu sehen, betrachten wir

die zweite Komponente der Invariante, die ‘‘Steigung’’ des Newton-Polygons. Die genaue Definition des Newton-Polygons und der zweiten Komponente der Invariante geben wir in den folgenden Abschnitten. In den Beispielen entspricht sie dem (kleinsten) Exponenten der Terme, die nur die Variable z enthalten (da das Newton-Polygon nur aus zwei Ecken besteht), also z^7 und z^4 . Wir sehen, da

$$\text{stg}_0 f' = 4 < 7 = \text{stg}_0 f.$$

Damit ist

$$(\text{ord}_0 f', \text{stg}_0 f') <_{\text{lex}} (\text{ord}_0 f, \text{stg}_0 f),$$

und die Auflosungsinvariante ist (im Newton-Polygon der betrachteten Karte) gefallen.

Wir betrachten nun ein Beispiel, in dem die Definition und die Beobachtung der Auflosungsinvariante

$$(r, s) = (\text{ord}_a f, \text{stg}_a f)$$

etwas subtiler ist. Sei

$$f(y, z) = y^3 z^2 + z^8 + y^9 + z^{12}.$$

Als Grundkorper wahlen wir einen Korper der Charakteristik 3. Analoge Beispiele gibt es fur jede beliebige Charakteristik.

Wie zuvor berechnen wir die total und strikt Transformierte von f , also

$$f^*(y, z) = f(yz, z) = y^3 z^5 + z^8 + y^9 z^9 + z^{12}$$

und

$$f'(y, z) = y^3 + z^3 + y^9 z^4 + z^7.$$

Die Ordnung von f' im Nullpunkt ist gefallen

$$\text{ord}_0 f' = 3 < 5 = \text{ord}_0 f,$$

und die Singularitat von f hat sich verbessert. Wir explodieren nochmals den Nullpunkt. Eine analoge Rechnung wie vorher liefert als strikt Transformierte

$$f''(y, z) = y^3 + 1 + y^9 z^{10} + z^4,$$

mit $\text{ord}_0 f'' = 0$. Im Nullpunkt der betrachteten Karte ist die Ordnung wieder gefallen (die Kurve $V(f'')$ enthalt nicht diesen Punkt). Hingegen gibt es einen Punkt in dieser Karte, namliche $a = (1, 0)$, in dem die Ordnung von f'' nicht gefallen ist. In der Tat, die Translation $y \mapsto y - 1$ liefert die Taylorentwicklung

$$f''(y - 1, z) = y^3 + y^9 z^{10} - z^{10} + z^4$$

mit

$$\text{ord}_a f'' = 3.$$

Wir sind hier gezwungen, die zweite Komponente $\text{stg}_a f$ der Invariante zu betrachten. Wir sehen

$$\text{stg}_0 f' = 3 \text{ und } \text{stg}_a f'' = 4.$$

Unsere Auflösungsinvariante ist (scheinbar) gestiegen. Doch Halt! Unsere Berechnung der Steigung von f' war zu naiv: Wechselt man etwa in f' die Koordinaten (was ja nicht verboten sein kann) vermöge

$$(y, z) \mapsto (y - z, z),$$

so hat f' die Taylorentwicklung

$$f' = f'(y - z, z) = y^3 + y^9 z^4 - z^{13} + z^7$$

im Nullpunkt. Die Ordnung ist mit $\text{ord}_0 f' = 3$ unter diesem Koordinatenwechsel natürlich unverändert geblieben, aber die Steigung ist nun

$$\text{stg}_0 f' = 7.$$

Dies zeigt, daß unsere Definition der Steigung koordinatenabhängig war. Damit kann sie aber nicht aussagekräftig sein. Wir müssen als Maß der Komplexität der Singularität der Kurve ihrem Polynom f Invarianten zuordnen, die nicht von der Wahl von Koordinaten abhängen. Die Ordnung der Taylorentwicklung tut dies von vornherein. Bei der Steigung bietet sich an (und bewährt sich a posteriori bestens), das Supremum aller koordinatenabhängigen Steigungen zu wählen. Sofern es existiert, hängt es natürlich nicht von den Koordinaten ab.

In unserem Beispiel erkennen wir mit dieser Definition, daß

$$\text{stg}_0 f' = 7$$

maximal ist (unter allen Koordinatenwechseln) und ebenso

$$\text{stg}_a f'' = 4.$$

Zusammen sehen wir:

$$(\text{ord}_a f'', \text{stg}_a f'') <_{\text{lex}} (\text{ord}_0 f', \text{stg}_0 f').$$

Diese Ungleichung zeigt, daß die Singularität beim Übergang von f' auf f'' in den betrachteten Punkten wirklich besser geworden ist.

Ein wichtiger Bestandteil des Auflösungsbeweises wird also das Studium der Steigung eines Polynoms in einem Punkt unter Koordinatenwechsel sein, sowie das Verhalten der maximalen Steigung unter Explosionen.

3. DIE ORDNUNG

In diesem Abschnitt definieren wir die Ordnung einer Potenzreihe und erklären, was wir unter einem lokalen Koordinatenwechsel verstehen. Eine detaillierte Einführung zu Potenzreihen geben wir im Abschnitt A.1.

Sei k ein Körper. Bezeichne im folgenden R den formalen Potenzreihenring in zwei Variablen über k und $G = \mathbf{Aut}_k(R)$ die Gruppe der stetigen (=lokalen) k -Algebraautomorphismen. Mit \mathfrak{m} bezeichnen wir das maximale Ideal von R . Seien $\mathbf{y} = (y, z)$ ein reguläres Parametersystem von R und $\varphi \in G$. Dann ist

$$\varphi(\mathbf{y}) = (\varphi(y), \varphi(z)) = (\varphi_1, \varphi_2) = (\tilde{y}, \tilde{z}) = \tilde{\mathbf{y}}$$

wieder ein reguläres Parametersystem von R . Umgekehrt induziert ein reguläres Parametersystem $\tilde{\mathbf{y}} = (\tilde{y}, \tilde{z})$ von R ein $\varphi \in G$ mit $\varphi(y) = \varphi_1(y, z) = \tilde{y}$ und $\varphi(z) = \varphi_2(y, z) = \tilde{z}$ (da \tilde{y} und \tilde{z} modulo \mathfrak{m}^2 linear unabhängig über $k = R/\mathfrak{m}$ sind).

Für eine Potenzreihe $f \in R$ mit $f = f(y, z)$ und ein $\varphi \in G$ ist $\text{ord} f = \text{ord} \varphi(f)$ (denn $\text{ord} f \leq \text{ord} \varphi(f) \leq \text{ord} \varphi^{-1} \varphi(f)$), d.h., die Ordnung einer Potenzreihe ist invariant unter Anwendung eines $\varphi \in G$ bzw. nach obiger Überlegung invariant bei einem Wechsel des regulären Parametersystems von R . Die Ordnung einer Potenzreihe f kann man auch nur mit Hilfe des maximalen Ideals \mathfrak{m} von R durch $\text{ord} f = \sup\{n \in \mathbf{N}_0 \text{ mit } f \in \mathfrak{m}^n\}$ definieren. Mit dieser Definition ist die Ordnung offensichtlich invariant bei einem Wechsel des Parametersystems (Koordinatenwechsel).

4. DAS NEWTON-POLYGON

Wir definieren in diesem Abschnitt für eine Potenzreihe $f \in R$ das Newton-Polygon. Mit Hilfe dieses Polygons ordnen wir f eine Zahl zu. Das Newton-Polygon ist aber abhängig von der Wahl des regulären Parametersystems $\mathbf{y} = (y, z)$. Wir untersuchen daher im Abschnitt 5 das Verhalten dieser Zahl bei Anwendung eines $\varphi \in G$ auf f . Im Teil 6 definieren wir schließlich eine weitere Invariante neben der Ordnung und untersuchen deren Eigenschaften.

Sei im folgenden $\mathbf{y} = (y, z)$ ein reguläres Parametersystem von R . Wir kennzeichnen durch den Index \mathbf{y} , daß eine Definition von der Wahl des Parametersystems abhängt. Seien $f \in R$, $f \neq 0$, und

$$(4.1) \quad f = f(y, z) = \sum_{\alpha} c_{\alpha} y^{\alpha_1} z^{\alpha_2} = \sum_{\alpha} c_{\alpha} \mathbf{y}^{\alpha}, \quad \text{mit } \alpha = (\alpha_1, \alpha_2) \in \mathbf{N}_0^2.$$

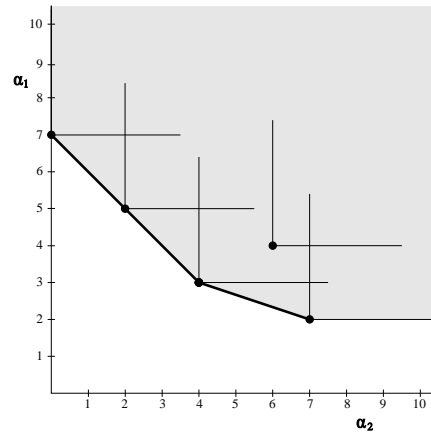


ABBILDUNG 4
Newton-Polygon

Die Menge

$$\Delta_y(f) = \{\alpha \in \mathbf{N}_0^2 \text{ mit } c_\alpha \neq 0\}$$

nennen wir den *Träger* von f . Der Rand der konvexen Menge

$$\text{conv}\left(\bigcup_{\alpha \in \Delta_y(f)} \{\alpha + \mathbf{R}_{\geq 0}^2\}\right) \subset \mathbf{R}_{\geq 0}^2$$

zerfällt in zwei Halbgeraden und einen kompakten Streckenzug. Diesen Streckenzug nennt man das *Newton-Polygon* von f . Die endliche Menge der Ecken des Newton-Polygons bezeichnen wir mit $\text{NP}_y(f)$. Das Newton-Polygon von f besteht genau dann aus nur einem Punkt, wenn $f = y^{\alpha_1} z^{\alpha_2} e$ mit $e \in R$ invertierbar.

BEISPIEL 4.1. Das Newton-Polygon von $f = y^7 + y^5 z^2 + y^3 z^4 + y^4 z^6 + y^2 z^7$ und dessen Konstruktion ist in Abbildung 4 zu sehen. Die Menge der Ecken, $\text{NP}_y(f)$, ist $\{(7, 0), (3, 4), (2, 7)\}$.

Aus der Definition des Trägers und der Multiplikation zweier Potenzreihen folgt unmittelbar für $f, g \in R$ mit $f, g \neq 0$.

$$(4.2) \quad \Delta_y(fg) \subset \Delta_y(f) + \Delta_y(g).$$

Seien $f, e \in R, f \neq 0$ und e invertierbar. Im allgemeinen ist nicht jedes Element des Trägers von f im Träger von fe enthalten. Zum Beispiel ist $(y + yz)(1 - z) = y - yz^2$. Es gilt aber folgendes Lemma.

LEMMA 4.2. Wenn $\delta \in \text{NP}_y(f)$, dann ist $\delta \in \Delta_y(fe)$.

Beweis. Wenn f auch invertierbar ist, gilt die Aussage trivialerweise. Seien f wie in (4.1) mit $\text{ord}f \geq 1$,

$$e = \sum_{\beta} d_{\beta} \mathbf{y}^{\beta} \quad \text{und}$$

$$fe = \sum_{\gamma} b_{\gamma} \mathbf{y}^{\gamma}, \quad \text{mit } b_{\gamma} = \sum_{\alpha+\beta=\gamma} c_{\alpha} d_{\beta}.$$

Angenommen $b_{\delta} = 0$. Dann gäbe es, da $c_{\delta} d_0 \neq 0$, ein $c_{\alpha} \neq 0$ mit $\alpha \neq \delta$ und $\alpha_1 \leq \delta_1$, $\alpha_2 \leq \delta_2$. Also ein Widerspruch zur Annahme, daß δ eine Ecke des Newton-Polygons von f ist. \square

Mit diesem Lemma, (4.2) und der Definition des Newton-Polygons folgt:

LEMMA 4.3. Seien $f, e \in R$, $f \neq 0$ und e invertierbar. Dann ist

$$\text{NP}_y(f) = \text{NP}_y(fe).$$

Seien $f \in \mathfrak{m}$, $f \neq 0$, wie in (4.1) und $r = \text{ord}f$. Wir setzen

$$\text{stg}_y f = \inf \left\{ \frac{r\alpha_2}{r - \alpha_1} \text{ mit } \alpha \in \text{NP}_y(f), \alpha \neq (r, 0) \right\} \in \mathbf{Q}_{>0} \cup \{\infty\},$$

mit $\inf \emptyset = \infty$. Wenn $\alpha \in \text{NP}_y(f)$, $\alpha \neq (r, 0)$, dann ist $(0, \frac{r\alpha_2}{r - \alpha_1})$ die Projektion von (α_1, α_2) durch $(r, 0)$ auf die α_2 -Achse der Schnittpunkt der Geraden

$$l = \left\{ (\beta_1, \beta_2) \text{ mit } \frac{\alpha_2}{r - \alpha_1} \beta_1 + \beta_2 = \frac{r\alpha_2}{r - \alpha_1} \right\}$$

durch $(r, 0)$ und (α_1, α_2) mit der α_2 -Achse. Also ist $s = \text{stg}_y f$ das Minus r -fache der Steigung des steilsten Segments des Newton-Polygons von f . Siehe Abbildung 5.

LEMMA 4.4. Seien $f \in \mathfrak{m}$, $f \neq 0$ und $r = \text{ord}f$. Dann gilt:

- (i) $\text{stg}_y f \in \{ \frac{p}{q} \in \mathbf{Q}_{>0} \text{ mit } p \text{ und } q \text{ teilerfremd und } 1 \leq q \leq r \} \cup \{\infty\}$.
- (ii) $r \leq \text{stg}_y f \leq \infty$.
- (iii) $\text{stg}_y f = r$ genau dann, wenn es ein $\alpha \in \text{NP}_y(f)$, $\alpha \neq (r, 0)$, mit $\alpha_1 + \alpha_2 = r$, gibt.
- (iv) $\text{stg}_y f > r$ genau dann, wenn die Initialform f_r von f gleich cy^r mit $c \neq 0$ ist, siehe Abschnitt A.1.1.

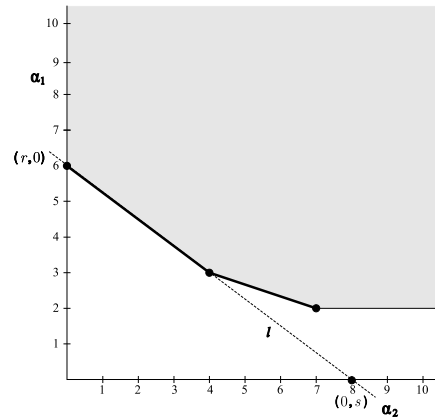


ABBILDUNG 5
Die Steigung

(v) $\text{stg}_y f = \infty$ genau dann, wenn $f = y^r e$ mit $e \in R$ invertierbar.

Beweis. Klar. \square

Seien $f \in \mathfrak{m}$, $f \neq 0$, wie in (4.1), $r = \text{ord} f$ und $t \in \mathbf{R}$ mit $t \geq r$. Wir schreiben

$$F_t = \sum_{\alpha} c_{\alpha} y^{\alpha}, \quad \text{für } \alpha \text{ mit } \frac{t}{r} \alpha_1 + \alpha_2 = t \text{ bzw.}$$

$$F_{>t} = \sum_{\alpha} c_{\alpha} y^{\alpha}, \quad \text{für } \alpha \text{ mit } \frac{t}{r} \alpha_1 + \alpha_2 > t.$$

Dann bestehen F_t bzw. $F_{>t}$ aus allen Termen von f deren Exponenten auf bzw. oberhalb der Geraden durch $(r, 0)$ und $(0, t)$ liegen.

Sei $s = \text{stg}_y f < \infty$. Dann können wir f zerlegen in

$$(4.3) \quad f = F_s + F_{>s}.$$

Wenn $r < s$, dann besteht F_s nach Definition von s neben cy^r aus noch mindestens einem Term.

LEMMA 4.5. Sei umgekehrt $r \leq t \in \mathbf{R}$ so, daß

$$f = F_t + F_{>t}.$$

Wenn es in F_t einen Term $c_{\alpha} y^{\alpha_1} z^{\alpha_2}$ mit $\alpha \neq (r, 0)$ gibt, dann ist $\text{stg}_y f = t$.

Beweis. Sei $\alpha \in \Delta_{\mathbf{y}}(f)$, $\alpha_1 < r$. Aus $\frac{t}{r}\alpha_1 + \alpha_2 \geq t$ folgt

$$\frac{r\alpha_2}{r - \alpha_1} \geq t.$$

Nach Voraussetzung gibt es ein $\alpha \in \text{NP}_{\mathbf{y}}(f)$ mit $\frac{t}{r}\alpha_1 + \alpha_2 = t$, d.h.,

$$t = \frac{r\alpha_2}{r - \alpha_1}.$$

Damit ist $\text{stg}_{\mathbf{y}}f = t$. \square

5. KOORDINATENWECHSEL

Um die Beziehung zwischen $\text{stg}_{\mathbf{y}}f$ und $\text{stg}_{\mathbf{y}}\varphi(f) = \text{stg}_{\varphi^{-1}\mathbf{y}}f$ für ein $\varphi \in G$ zu untersuchen, verwenden wir die Möglichkeit der Gauß-Bruhat-Zerlegung $\varphi = ulp$ von φ mit $u \in U$, $l \in L$ und $p \in P$, siehe Abschnitt A.2.

Sei zunächst $u \in U$. Dann ist

$$(5.1) \quad \begin{aligned} u_1 = u(y) &= ay + yh_1, & \text{mit } \text{ord } h_1 \geq 1, a \neq 0, \\ u_2 = u(z) &= cz + by + h_2, & \text{mit } \text{ord } h_2 \geq 2, c \neq 0. \end{aligned}$$

Das Newton-Polygon von f ist im allgemeinen nicht gleich dem Newton-Polygon von $u(f)$. Betrachte zum Beispiel $f = z$ und u mit den zu $\bar{u} = (y, y+z)$ gehörigen Substitutionshomomorphismus, d. h., $u(f) = f(y, y+z) = y+z$. Siehe Abschnitt A.1.3.

LEMMA 5.1. *Seien $f = y^{\alpha_1}z^{\alpha_2}$ mit $\alpha \neq 0$ und $u \in U$. Dann gilt (siehe Abbildung 6):*

- (i) $(\alpha_1, \alpha_2) \in \Delta_{\mathbf{y}}(u(f))$.
- (ii)

$$\begin{aligned} \Delta_{\mathbf{y}}(u(f)) &\subset \{\beta \in \mathbf{N}_0^2 \text{ mit } \beta_1 - \alpha_1 \geq \alpha_2 - \beta_2 \text{ und } \beta_2 \geq \alpha_2\} \\ &= \text{conv}(\{(\alpha_1 + \alpha_2, 0) + \mathbf{R}_{\geq 0}^2\} \cup \{(\alpha_1, \alpha_2) + \mathbf{R}_{\geq 0}^2\}). \end{aligned}$$

Beweis. Es ist

$$\begin{aligned} u(f) &= u_1^{\alpha_1} u_2^{\alpha_2} = (ay + yh_1)^{\alpha_1} ((cz + by) + h_2)^{\alpha_2} \\ &= dy^{\alpha_1} z^{\alpha_2} + y^{\alpha_1} \sum_{k=1}^{\alpha_2} d_k y^k z^{\alpha_2 - k} + y^{\alpha_1} h \end{aligned}$$

mit $d \neq 0$ und $\text{ord } h > \alpha_2$. Daraus folgt die Behauptung. \square

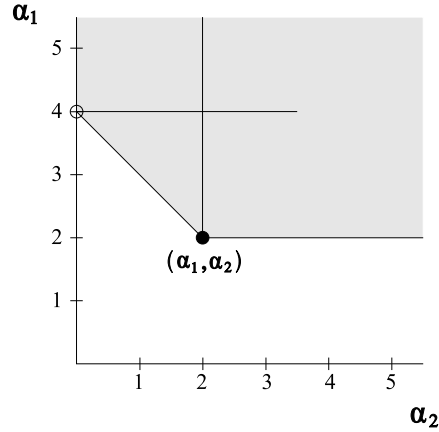


ABBILDUNG 6
Koordinatenwechsel: $u(y^{\alpha_1} z^{\alpha_2})$

LEMMA 5.2. Seien $f \in \mathfrak{m}$, $f \neq 0$, $r = \text{ord } f$ und $u \in U$. Dann gilt:

- (i) Wenn $\text{stg}_y f > r$, dann ist $\text{NP}_y(f) = \text{NP}_y(u(f))$.
- (ii) $\text{stg}_y f = \text{stg}_y u(f)$.

Beweis. Zu (i): Da $\text{stg}_y f > r$, ist mit Lemma 4.4 $(r, 0) \in \Delta_y(f)$. Mit der vorherigen Behauptung und der Definition des Newton-Polygons folgt daraus $\text{NP}_y(f) = \text{NP}_y(u(f))$.

Zu (ii): Sei $\text{stg}_y f = r$. Nach Lemma 4.4 gibt es ein $\alpha \in \text{NP}_y(f)$, $\alpha \neq (r, 0)$, mit $\alpha_1 + \alpha_2 = r$. Wenn es zwei solche $\alpha \in \text{NP}_y(f)$ gibt, dann betrachten wir das mit der kleineren α_1 -Koordinate. Nach der vorherigen Behauptung ist dann $\alpha \in \text{NP}_y(u(f))$ und damit $\text{stg}_y u(f) = \text{stg}_y f = r$. \square

Sei nun $l \in L$. Dann ist

$$(5.2) \quad \begin{aligned} l_1 = l(y) &= y + g, & \text{mit } g \in k[[z]], \text{ ord } g \geq 1, \\ l_2 = l(z) &= z. \end{aligned}$$

Wenn wir $\text{stg}_y f$ und $\text{stg}_y l(f)$ vergleichen, können wir im allgemeinen nichts aussagen, wie folgendes Beispiel belegt:

BEISPIEL 5.3. Sei $l(y) = y + z$.

- Mit $f = y^2 + z^3$ ist $l(f) = y^2 + 2yz + z^2 + z^3$, also $2 = \text{stg}_y l(f) < \text{stg}_y f = 3$.
- Mit $f = y^2 + yz$ ist $l(f) = y^2 + 3yz + 2z^2$, also $2 = \text{stg}_y l(f) = \text{stg}_y f = 2$.

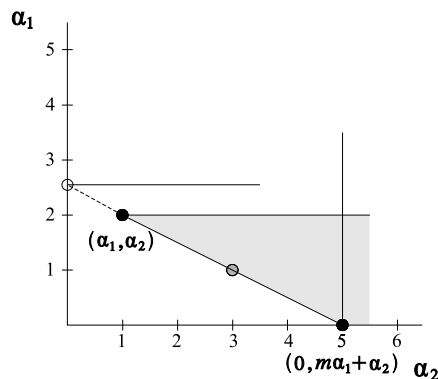


ABBILDUNG 7

Koordinatenwechsel: $l(y^{\alpha_1} z^{\alpha_2})$

- Mit $f = y^2 - 2yz + z^2 + z^3 = (y - z)^2 + z^3$ ist $l(f) = y^2 + z^3$, also $3 = \text{stg}_y l(f) > \text{stg}_y f = 2$.
- Mit $f = y^2 - 2yz + z^2 = (y - z)^2$ ist $l(f) = y^2$, also $\text{stg}_y l(f) = \infty$.

Außerdem kann $\text{stg}_y l(f)$ von der Charakteristik von k abhängen. Mit l wie im vorherigen Beispiel und $f = y^2 + z^2$ ist $l(f) = y^2 + 2yz + 2z^2$. Wenn $\text{char} k = 2$, dann ist $\text{stg}_y l(f) = \infty$, sonst $\text{stg}_y l(f) = 2$.

Sei $l \in L$ wie in (5.2). Wir werden nun den Zusammenhang zwischen

$$\text{stg}_y f, \text{stg}_y l(f) \text{ und } m = \text{ord } g$$

untersuchen.

LEMMA 5.4. Seien $f = y^{\alpha_1} z^{\alpha_2}$ mit $\alpha \neq 0$ und $l \in L$. Dann gilt (siehe Abbildung 7):

- $(\alpha_1, \alpha_2), (0, m\alpha_1 + \alpha_2) \in \Delta_y(l(f))$.
-

$$\begin{aligned} \Delta_y(l(f)) &\subset \{\beta \in \mathbf{N}_0^2 \text{ mit } \beta_2 - \alpha_2 \geq m(\alpha_1 - \beta_1) \text{ und } \beta_1 \leq \alpha_1\} \\ &\subset \text{conv}\left(\left\{\left(\frac{m\alpha_1 + \alpha_2}{m}, 0\right) + \mathbf{R}_{\geq 0}^2\right\} \cup \{(0, m\alpha_1 + \alpha_2) + \mathbf{R}_{\geq 0}^2\}\right). \end{aligned}$$

- Wenn $\text{char} k = 0$, dann ist außerdem $(\alpha_1 - k, mk + \alpha_2) \in \Delta_y(l(f))$ für $k = 1, \dots, \alpha_1 - 1$.

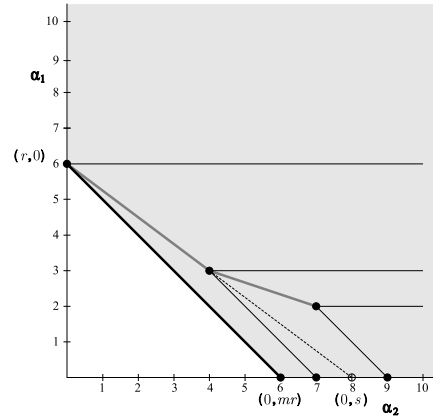


ABBILDUNG 8
Koordinatenwechsel: $l(f)$ mit $m < \frac{s}{r}$

Beweis. Es ist

$$(5.3) \quad l(f) = (y + g)^{\alpha_1} z^{\alpha_2} = y^{\alpha_1} z^{\alpha_2} + g^{\alpha_1} z^{\alpha_2} + \left(\sum_{k=1}^{\alpha_1-1} \binom{\alpha_1}{k} y^{\alpha_1-k} g^k \right) z^{\alpha_2}.$$

Daraus folgt die Behauptung. \square

Sei jetzt wieder $f \in \mathfrak{m}$, $f \neq 0$ und bezeichne $r = \text{ord} f$, $s = \text{stg}_y f$ und $m = \text{ord} g$.

LEMMA 5.5. Wenn $m < \frac{s}{r}$, dann ist $\text{stg}_y l(f) = mr$ (siehe Abbildung 8).

Beweis. Sei zunächst $\text{stg}_y f < \infty$. Wir zerlegen f in (siehe (4.3))

$$f = cy^r + \sum_{\alpha} c_{\alpha} y^{\alpha}, \quad \text{mit } \frac{s}{r} \alpha_1 + \alpha_2 \geq s, \alpha \neq (r, 0) \text{ und } c \neq 0.$$

Aus

$$\frac{s}{r} \alpha_1 + \alpha_2 \geq s \text{ und } \alpha \neq (r, 0)$$

folgt für $\alpha_1 \geq r$, daß $m\alpha_1 + \alpha_2 > mr$. Wenn $\alpha_1 < r$, dann impliziert

$$\frac{r\alpha_2}{r - \alpha_1} \geq s > mr$$

wieder $m\alpha_1 + \alpha_2 > mr$. Mit der vorherigen Behauptung ist damit

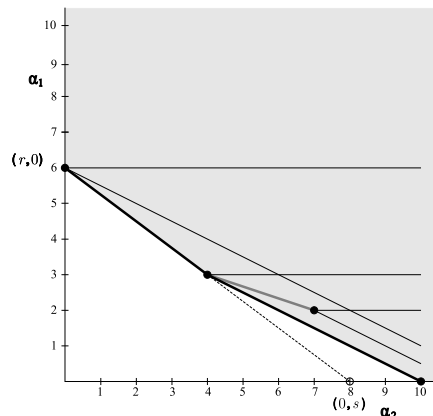


ABBILDUNG 9

Koordinatenwechsel: $l(f)$ mit $m \geq \frac{s}{r}$

$$\Delta_{\mathbf{y}}(l(cy^r)) \subset \Delta_{\mathbf{y}}(l(f)) \quad \text{und} \quad \{(r, 0), (0, mr)\} = \text{NP}_{\mathbf{y}}(l(f)),$$

also $\text{stg}_{\mathbf{y}} l(f) = mr$.

Wenn $\text{stg}_{\mathbf{y}} f = \infty$, dann ist

$$f = y^r e, \quad \text{mit } e \in R \text{ invertierbar.}$$

Damit ist

$$l(f) = l(y^r)e(y + g, z).$$

Daraus folgt mit dem vorherigen Lemma und Lemma 4.3 die Behauptung. \square

LEMMA 5.6. Wenn $m > \frac{s}{r}$, dann ist $\text{stg}_{\mathbf{y}} f = \text{stg}_{\mathbf{y}} l(f)$ (siehe Abbildung 9).

Beweis. Wir zerlegen f wie in (4.3) in

$$f = F_s + F_{>s}.$$

Die Exponenten α der Terme $c_a y^{\alpha_1} z^{\alpha_2}$ von $F_{>s}$ erfüllen nach Definition

$$\frac{s}{r} \alpha_1 + \alpha_2 > s.$$

Mit Lemma 5.4 und der Voraussetzung gilt diese Ungleichung auch für die Exponenten der Terme von $l(F_{>s})$. Für einen Term $c_a y^{\alpha_1} z^{\alpha_2}$ von F_s erkennt

man mit dem gleichen Argument, daß $l(c_a y^{\alpha_1} z^{\alpha_2})$ aus $c_a y^{\alpha_1} z^{\alpha_2}$ und Termen besteht, deren Exponenten wieder die obigen Ungleichung erfüllen. Also ist

$$l(f) = F_s + F'_{>s}.$$

Mit Lemma 4.5 gilt dann $\text{stg}_y l(f) = \text{stg}_y f$. \square

LEMMA 5.7. Wenn $m \neq \frac{s}{r}$, dann ist $\text{stg}_y l(f) \leq \text{stg}_y f$.

Beweis. Klar mit den zwei vorherigen Lemmata. \square

SATZ 5.8. Seien $f \in \mathfrak{m}$, $f \neq 0$, mit $s = \text{stg}_y f < \infty$, $r = \text{ord} f$ und $f = F_s + F_{>s}$ wie in (4.3). Dann sind äquivalent:

1. Es gibt ein $l \in L$ mit $\text{stg}_y l(f) > \text{stg}_y f$.
2. $\frac{s}{r} \in \mathbf{N}$ und

$$F_s = c \left(y - dz^{\frac{s}{r}} \right)^r, \quad \text{mit } c, d \in k, c, d \neq 0.$$

Beweis. Sei $\frac{s}{r} \in \mathbf{N}$ und

$$F_s = c \left(y - dz^{\frac{s}{r}} \right)^r.$$

Sei l der zu $\bar{l} = (y + dz^{\frac{s}{r}}, z)$ gehörige Einsetzungshomomorphismus. Dann ist

$$l(f) = l(F_s) + l(F_{>s}) = cy^r + l(F_{>s}).$$

Mit Lemma (5.4) sieht man, daß $l(F_{>s}) = F'_{>s}$. Daraus folgt entweder $\text{NP}_y(l(f)) = \{(r, 0)\}$, also $\text{stg}_y l(f) = \infty$, oder

$$\frac{r\alpha_2}{r - \alpha_1} > s, \quad \text{für } \alpha \in \text{NP}_y(f), \alpha \neq (r, 0).$$

Damit gilt wieder $\text{stg}_y l(f) > \text{stg}_y f$.

Sei nun umgekehrt $l \in L$ mit $\text{stg}_y l(f) > \text{stg}_y f$. Seien $l(y) = y + g$ und

$$g = \sum_{i=m}^{\infty} a_i z^i \in zk[[z]], \quad \text{mit } m = \text{ord} g.$$

Aus Lemma 5.7 folgt $\frac{s}{r} = m \in \mathbf{N}$. Wie zuvor ist $l(F_{>s}) = F'_{>s}$. Weiters ist (siehe (5.3))

$$l(F_s) = F_s(y + g, z) = F_s(y + a_m z^m, z) + G_{>s}$$

und damit

$$l(f) = F_s(y + a_m z^m, z) + H_{>s}.$$

Weil

$$F_s(y + a_m z^m, z) = F'_s,$$

und nach Voraussetzung $\text{stg}_y l(f) > \text{stg}_y(f)$, muß dann

$$F_s(y + a_m z^{\frac{s}{r}}, z) = cy^r, \quad \text{mit } c \neq 0$$

gelten. Also ist

$$F_s(y, z) = c (y - a_m z^{\frac{s}{r}})^r.$$

□

Sei p die Vertauschung von y und z . Dann ergibt sich mit Lemma 4.4:

LEMMA 5.9. *Seien $f \in \mathfrak{m}$, $f \neq 0$ und $r = \text{ord} f$. Dann gilt:*

- (i) $\text{stg}_y p(f) = r$ genau dann, wenn es ein $\alpha \in \text{NP}_y(f)$, $\alpha \neq (0, r)$, mit $\alpha_1 + \alpha_2 = r$, gibt.
- (ii) $\text{stg}_y p(f) > r$ genau dann, wenn die Initialform f_r von f gleich cz^r mit $c \neq 0$ ist.
- (iii) $\text{stg}_y p(f) = \infty$ genau dann, wenn $f = z^r e$ mit $e \in R$ invertierbar.

6. DIE MAXIMALE STEIGUNG

Seien $f \in \mathfrak{m}$, $f \neq 0$, $r = \text{ord} f$ und

$$\begin{aligned} S &= \{\text{stg}_y \varphi(f) \text{ mit } \varphi \in G\} \\ &= \{\text{stg}_y f \text{ mit } \mathbf{y} = (y, z) \text{ reguläres Parametersystem von } R\}. \end{aligned}$$

Wir definieren

$$\text{stg} f = \sup S,$$

als das Supremum über alle koordinatenabhängigen Steigungen, vgl. [Ab1] (in [BK] folgt aus maximalem Kontakt die Maximalität der Steigung). Offenbar ist $\text{stg} f$ invariant bei einem Wechsel des Parametersystems. Nach Satz A.35 (Gauß-Bruhat Zerlegung) können wir jedes $\varphi \in G$ schreiben $\varphi = ulp$ mit $u \in U$, $l \in L$ und $p \in P$. Mit Lemma 5.2 ist dann

$$\text{stg}_y \varphi(f) = \text{stg}_y ulp(f) = \text{stg}_y u^{-1}(ulp(f)) = \text{stg}_y lp(f).$$

Also ist

$$S = \{\text{stg}_y lp(f) \text{ mit } l \in L \text{ und } p \in P\}.$$

Wenn $\text{stg}f < \infty$, dann erkennt man mit Lemma 4.4 (i), daß S eine endliche Menge ist. Also ist in diesem Fall das Supremum ein Maximum, d.h., es gibt ein $l \in L$ so, daß nach einer eventuellen Vertauschung $p \in P$ der Variablen $\text{stg}_y lp(f) = \text{stg}f$. Insbesondere gibt es ein reguläres Parametersystem $\tilde{y} = (\tilde{y}, \tilde{z})$ von R mit

$$\text{stg}_{\tilde{y}}f = \text{stg}f, \quad \text{mit } f = f(\tilde{y}, \tilde{z}).$$

Wir sagen dann, das Parametersystem $\tilde{y} = (\tilde{y}, \tilde{z})$ realisiert $\text{stg}f$. Unmittelbar aus Lemma 4.3 folgt:

LEMMA 6.1. *Seien $f \in \mathfrak{m}$, $f \neq 0$ und $e \in R$ invertierbar. Dann ist $\text{stg}f = \text{stg}fe$.*

Wir kommen nun zum Fall $\text{stg}f = \infty$. Zunächst folgendes Lemma.

LEMMA 6.2. *Sei $f = f(y, z) \in R$ y -allgemein der Ordnung 1, d.h., $\text{ord}f(y, 0) = 1$. Siehe Abschnitt A.1.5. Dann gibt es genau ein $l \in L$ mit $\text{stg}_y l(f) = \infty$.*

Beweis. Da f y -allgemein der Ordnung 1 ist, gibt es nach dem Weierstraßschen Vorbereitungssatz (Satz A.13) eindeutig ein $g \in \mathfrak{z}k[[z]]$ und eine Einheit $e \in R$ so, daß

$$f = (y + g)e.$$

Mit $l \in L$ dem zu $\bar{l} = (y - g, z)$ gehörigen Einsetzungshomomorphismus ist dann

$$l(f) = f(y - g, z) = ye(y - g, z)$$

und damit $\text{stg}_y l(f) = \infty$. \square

Mit einer möglichen Vertauschung $p \in P$ der Variablen folgt daraus das nächste Lemma.

LEMMA 6.3. *Sei $f \in R$ mit $\text{ord}f = 1$. Dann ist $\text{stg}f = \infty$.*

SATZ 6.4. *Sei $f = f(y, z) \in \mathfrak{m}$, $f \neq 0$ mit $r = \text{ord}f < \text{stg}_y f$. Dann ist $\text{stg}f = \infty$ genau dann, wenn es ein $l \in L$ gibt so, daß $\text{stg}_y l(f) = \infty$.*

Beweis. Sei also $\text{stg}f = \infty$. Wir konstruieren das gesuchte $l \in L$ mit $\text{stg}_y l(f) = \infty$ induktiv. Sei $s_1 = \text{stg}_y f$. Falls $s_1 = \infty$ ist, sind wir fertig. Sonst folgt aus der Voraussetzung, daß es ein $l_1 \in L$ und ein $p_1 \in P$ gibt

mit $s_1 < \text{stg}_y l_1 p_1(f)$. Angenommen p_1 ist nicht die Identität. Da $f_r = cy^r$ mit $c \in k$, $c \neq 0$ ist, wäre dann aber $\text{stg}_y l_1 p_1(f) = r$. Also ist p_1 die Identität. Mit Satz 5.8 folgt daher

$$m_1 = \frac{s_1}{r} \in \mathbf{N} \quad \text{und} \quad f = c(y - a_1 z^{m_1})^r + F_{>s_1}, \quad \text{mit } c, a_1 \in k, c, a_1 \neq 0.$$

Wie im Beweis zu Satz 5.8 erkennt man, daß

$$s_1 < s_2 = \text{stg}_y f(y + a_1 z^{m_1}, z).$$

Wenn $s_2 = \infty$ ist, sind wir am Ziel, sonst beginnen wir wieder von neuem. Entweder sind wir nach endlich vielen Schritten fertig, oder wir haben für jedes $n \in \mathbf{N}$ ein $a_n \in k$ und ein $s_n \in \mathbf{N}$ mit $s_1 < s_2 < \dots < s_n$ und $m_n = s_n/r \in \mathbf{N}$ so, daß

$$f(y + \sum_{i=1}^n a_i z^{m_i}, z) = cy^r + B_n,$$

$$B_n = \sum c_\alpha^n y^{\alpha_1} z^{\alpha_2}, \quad \text{mit } \frac{s_{n+1}}{r} \alpha_1 + \alpha_2 \geq s_{n+1}, \alpha \neq (r, 0) \text{ und } c \neq 0.$$

Die Summe B_n zerlegen wir in

$$B_n = y^r C_n + D_n,$$

$$C_n = \sum c_\alpha^n y^{\alpha_1 - r} z^{\alpha_2}, \quad \text{mit } \alpha_1 \geq r \text{ und}$$

$$D_n = \sum c_\alpha^n y^{\alpha_1} z^{\alpha_2}, \quad \text{mit } \alpha_1 < r.$$

Aus den beiden Ungleichungen für die Exponenten der Terme von D_n folgt, daß die Ordnung von D_n beliebig groß wird, d.h., $\lim D_n = 0$. Siehe Abschnitt A.1.2 für den Konvergenzbegriff für Potenzreihen. Sei $g = \sum_{i=1}^{\infty} a_i z^{m_i}$. Mit Lemma A.16 ist für $n \in \mathbf{N}$

$$\begin{aligned} f(y + g, z) &= f(y + \sum_{i=1}^n a_i z^{m_i} + \sum_{i=n+1}^{\infty} a_i z^{m_i}, z) \\ &= f(y + \sum_{i=1}^n a_i z^{m_i}, z) + h_n, \quad \text{mit } \text{ord } h_n \geq m_{n+1}. \end{aligned}$$

Damit konvergiert C_n in R und mit $C = \lim C_n$ ist

$$f(y + g, z) = cy^r + y^r C.$$

Für l mit $\bar{l} = (y + g, z)$ ist dann $\text{stg}_y l(f) = \infty$.

Die umgekehrte Implikation ist trivial. \square

KOROLLAR 6.5. Sei $f = f(y, z) \in \mathfrak{m}$, $f \neq 0$. Dann gibt es ein $l \in L$ und ein $p \in P$ so, daß $\text{stg}f = \text{stg}_y lp(f)$.

Beweis. Seien $\text{stg}f = \infty$ und $\text{stg}_y f = \text{ord}f = r$. Dann gibt es ein $l_0 \in L$ und ein $p_0 \in P$ mit $\text{stg}_y l_0 p_0(f) > r$, und wir können den vorherigen Satz anwenden. Wenn $\text{stg}f$ endlich ist, haben wir uns schon zu Beginn des Abschnittes überlegt, daß es ein $l \in L$ und ein $p \in P$ gibt mit $\text{stg}f = \text{stg}_y lp(f)$. \square

Insbesondere bedeutet dieses Korollar, daß es für jede Potenzreihe $f \in R$ ein reguläres Parametersystem $\mathbf{y} = (y, z)$ von R gibt, das $\text{stg}f$ realisiert, also so, daß

$$\text{stg}_y f = \text{stg}f, \quad \text{mit } f = f(y, z).$$

Eine zum ersten Teil des Beweises von Satz 6.4 analoge Argumentation zeigt auch folgenden Satz.

SATZ 6.6. Sei $f = f(y, z) \in \mathfrak{m}$, $f \neq 0$ mit $\text{stg}f < \infty$. Dann gibt es ein Polynom

$$g = \sum_{i=1}^n a_i z^{m_i} \in zk[z]$$

und ein $p \in P$ so, daß $\text{stg}f = \text{stg}_y lp(f)$ mit $\bar{l} = (y + g, z)$.

7. DIE AUFLÖSUNGSINVARIANTE

Wir fassen im folgenden durch die Taylorentwicklung von Polynomen im Nullpunkt den Polynomring $k[y, z]$ als Unterring von $k[[y, z]]$ auf. Damit können wir die Begriffe bzw. Ergebnisse von Abschnitt 6 auch auf Polynome anwenden. Sei $f \in k[y, z] \setminus k$. Wenn $r = \text{ord}f \geq 1$, dann setzen wir

$$\text{stg}_0 f = \text{stg}f,$$

und $\text{stg}_0 f = \infty$, wenn $\text{ord}f = 0$. Für einen beliebigen Punkt $a = (a_1, a_2) \in \mathbf{A}^2$ definieren wir

$$\text{stg}_a f = \text{stg}_0 \tilde{f}, \quad \text{mit } \tilde{f}(y, z) = f(y + a_1, z + a_2).$$

LEMMA 7.1. Sei $a \in \mathbf{A}^2$. Dann gilt:

(i) Wenn a ein regulärer Punkt von f ist, dann ist $\text{stg}_a f = \infty$.

- (ii) Wenn a ein singulärer Punkt von f ist, dann ist $\text{stg}_a f \in S_r$ mit $r = \text{ord}_a f$ und

$$S_r = \left\{ s = \frac{p}{q} \in \mathbf{Q}_{>0} \text{ mit } r \leq s, p \text{ und } q \text{ teilerfremd, } 1 \leq q \leq r \right\} \cup \{\infty\}.$$

Beweis. Zu (i): Folgt mit Lemma 6.3.

Zu (ii): Siehe Lemma 4.4. \square

Seien S_r mit $r \geq 2$ wie oben und $S_1 = S_0 = \{\infty\}$. Sei

$$I = \bigcup_{r \in \mathbf{N}_0} \{r\} \times S_r \subset \mathbf{N}_0 \times (\mathbf{Q}_{\geq 0} \cup \{\infty\}).$$

Für einen Punkt $a \in \mathbf{A}^2$ ist dann die *Auflösungsinvariante* von f in a definiert als das Paar

$$\text{inv}_a f = (\text{ord}_a f, \text{stg}_a f) \in I.$$

Bezeichne $<_{\text{lex}}$ die lexikographische Ordnung auf I , d.h., $(r', s') <_{\text{lex}} (r, s)$ genau dann, wenn $r' < r$ oder $(r' = r \text{ und } s' < s)$. Offensichtlich ist $<_{\text{lex}}$ eine totale Ordnung (d.h., je zwei Elemente sind vergleichbar), und $(0, \infty)$ ist das kleinste Element von I . Um einen Induktionsbeweis über die Menge I der Invarianten führen zu können, brauchen wir das folgende Lemma.

LEMMA 7.2. *Die Menge I mit der Ordnung $<_{\text{lex}}$ ist eine wohlgeordnete Menge (d.h., jede nicht-leere Teilmenge $J \subset I$ besitzt ein kleinstes Element).*

Beweis. Sei $J \subset I$, J nicht-leer. Seien $p_1: J \rightarrow \mathbf{N}_0$ die Projektion auf die erste Komponente und $r = \min\{p_1(J)\} \in \mathbf{N}_0$. Wenn $r = 0$ bzw. $r = 1$, dann ist $(0, \infty)$ bzw. $(1, \infty)$ das kleinste Element von J . Sei also $r \geq 2$. Setze $K = J \cap \{r\} \times S_r$ und

$$f: K \rightarrow \mathbf{N} \cup \{\infty\}, (r, s) \mapsto r!s.$$

Die Abbildung ist bijektiv und erhält die Ordnung. Da $\mathbf{N} \cup \{\infty\}$ eine wohlgeordnete Menge ist, gibt es ein kleinstes Element von $f(K)$ und damit auch von K bzw. J . \square

8. AUFGELÖSTE PUNKTE

Sei $f \in k[y, z] \setminus k$ das definierende Polynom einer algebraischen Kurve in \mathbf{A}^2 . Für die Definition von regulären und singulären Punkte einer Kurve und der Herleitung der benötigten Behauptungen siehe Abschnitt A.3.

Wir nennen den Nullpunkt einen *aufgelösten* Punkt von f , wenn $0 \notin V(f)$, oder wenn es Polynome $g, h \in k[y, z]$ mit $\text{ord}_0 g = 1$ und $\text{ord}_0 h = 0$ und ein $n \in \mathbf{N}$ gibt so, daß

$$(8.1) \quad f = g^n h.$$

Einen beliebigen Punkt $a = (a_1, a_2) \in \mathbf{A}^2$ nennen wir einen *aufgelösten* Punkt von f , wenn der Nullpunkt von $\tilde{f} = f(y + a_1, z + a_2)$ aufgelöst ist.

Sei $f = cf_1^{b_1} \cdots f_r^{b_r}$ die Primfaktorzerlegung von f in $k[x, y]$. Bezeichne

$$f_{red} = f_1 \cdots f_r$$

die *Reduktion* von f (f_{red} ist eindeutig bis auf einen konstanten Faktor). Es gilt $V(f) = V(f_{red})$. Sei $a \in V(f)$. Dann ist a genau dann ein aufgelöster Punkt von f , wenn a ein regulärer Punkt von f_{red} ist. Nach Definition sind alle Punkte $a \in \mathbf{A}^2 \setminus V(f)$ aufgelöst. Also ist

$$\{a \in \mathbf{A}^2 \text{ mit } a \text{ nicht aufgelöster Punkt von } f\} = \text{Sing}(f_{red}).$$

Mit Satz A.41 folgt daher insbesondere:

SATZ 8.1. *Seien k ein algebraisch abgeschlossener Körper und $f \in k[y, z] \setminus k$. Dann ist die Menge der nicht aufgelösten Punkte von f endlich.*

Sei $a \in V(f)$. Wir wollen im folgenden beweisen, daß a genau dann ein aufgelöster Punkt von f ist, wenn $\text{stg}_a f = \infty$, siehe Satz 8.6. Nach einer Translation in \mathbf{A}^2 können wir uns auf den Nullpunkt beschränken.

SATZ 8.2. *Seien k ein algebraisch abgeschlossener Körper und $f \in k[y, z]$ irreduzibel. Dann ist $f \in k[[y, z]]$ reduziert.*

Beweis. Angenommen, f ist als Potenzreihe nicht reduziert. Dann ist

$$f = g^2 h, \quad \text{mit } g, h \in k[[y, z]] \text{ und } \text{ord } g \geq 1.$$

Für $\text{ord } f = 0$ und $\text{ord } f = 1$ folgt daraus ein Widerspruch. Sei also $\text{ord } f \geq 2$. Angenommen $\partial_y f \neq 0$. Dann sind $\partial_y f$ und f teilerfremd in $k[[y, z]]$, weil f irreduzibel und $\deg \partial_y f \leq \deg f - 1$ ist. Weiters ist $\text{ord } \partial_y f \geq 1$. Mit der Produktregel folgt

$$\partial_y f = \partial_y(g^2 h) = g(g \partial_y h + 2h \partial_y g).$$

Daher ist g ein echter gemeinsamer Teiler von f und $\partial_y f$ in $k[[y, z]]$. Das ist aber ein Widerspruch zu Korollar A.33. Also ist $\partial_y f = 0$. Analog dazu

schließt man, daß auch $\partial_z f = 0$ ist. Aber $\partial_y f = \partial_z f = 0$ impliziert $f \in k$, wenn $\text{char } k = 0$. Widerspruch.

Wenn $\text{char } k = p > 0$, dann bedeutet das Verschwinden der partiellen Ableitungen, daß f nur aus Termen der Form $c_\alpha y^{p\alpha_1} z^{p\alpha_2}$ besteht. Indem man die Identität $(a+b)^p = a^p + b^p$ für einen Körper der Charakteristik p anwendet und benützt, daß es in einem algebraisch abgeschlossenen Körper insbesondere auch p -te Wurzeln gibt, erkennt man, daß

$$f = \sum c_\alpha y^{p\alpha_1} z^{p\alpha_2} = \left(\sum d_\alpha y^{\alpha_1} z^{\alpha_2} \right)^p, \quad \text{mit } d_\alpha^p = c_\alpha.$$

Dies ist ein Widerspruch zur Irreduzibilität von f . \square

Ein Körper k heißt *perfekt*, wenn $\text{char } k = 0$ oder wenn für $\text{char } k = p$ jedes Element in k eine p -te Wurzel besitzt. Neben algebraisch abgeschlossenen Körpern sind zum Beispiel auch alle endlichen Körper perfekt. Im Beweis zum vorherigen Satz verwenden wir nur diese Eigenschaft von k . Damit sind Satz 8.2, Lemma 8.4 und Satz 8.6 auch für perfekte Körper gültig.

Wir erinnern hier kurz an ein Ergebnis des Abschnitts 6 und leiten einige einfache Folgerungen daraus ab, die wir für die Beweise der nächsten Lemmata benötigen.

Bezeichne G wieder die Gruppe der stetigen k -Algebraautomorphismen von $k[[y, z]]$ und $\mathfrak{m} = (y, z) \subset k[[y, z]]$ das maximale Ideal von $k[[y, z]]$. Sei $f \in k[[y, z]]$, $f \neq 0$, mit $\text{stg } f = \infty$ und $r = \text{ord } f \geq 1$. Nach Korollar 6.5 und Lemma 4.4 (v) gibt es ein $\varphi \in G$ mit

$$\varphi(f) = y^r \tilde{z}, \quad \text{mit } \tilde{z} \in k[[y, z]] \text{ invertierbar.}$$

Also ist

$$f = g^r e, \quad \text{mit } e \in k[[y, z]] \text{ invertierbar}$$

und $g = \varphi^{-1}(y) \in k[[y, z]]$ irreduzibel, weil $\text{ord } g = 1$ ist. Wir verwenden weiters, daß $k[[y, z]]$ ein faktorieller Ring ist, siehe Satz A.20.

LEMMA 8.3. *Seien k ein Körper und $f \in k[[y, z]]$, $f \neq 0$, mit $\text{stg } f < \infty$ und $r = \text{ord } f \geq 1$. Sei $n \in \mathbf{N}$. Dann ist $\text{stg } f^n < \infty$.*

Beweis. Angenommen $\text{stg } f^n = \infty$. Dann ist $f^n = g^m e$ mit $g = \varphi^{-1}(y)$ und φ wie oben. Aus der Eindeutigkeit der Primfaktorzerlegung folgt $f = g^r \tilde{z}$. Also ist

$$\varphi(f) = y^r e', \quad \text{mit } e' \in k[[y, z]] \text{ invertierbar}$$

und damit $\text{stg } f = \infty$. Widerspruch. \square

LEMMA 8.4. *Seien k ein algebraisch abgeschlossener Körper und $f \in k[y, z]$ irreduzibel mit $r = \text{ord} f \geq 2$ (d.h., 0 ist ein singulärer Punkt von f). Dann ist $\text{stg}_0 f < \infty$.*

Beweis. Indirekt. Sei $\text{stg}_0 f = \infty$. Nach obiger Überlegung ist dann aber f als Potenzreihe nicht reduziert, da $r \geq 2$ ist. Also folgt ein Widerspruch zu Satz 8.2. \square

LEMMA 8.5. *Seien k ein Körper und $f, g \in k[y, z]$ teilerfremd mit $f, g \in \mathfrak{m}$. Dann ist $\text{stg}_0(fg) < \infty$.*

Beweis. Angenommen $\text{stg}_0(fg) = \infty$. Dann ist

$$fg = g^r e, \quad \text{mit } g, e \in k[[y, z]], \quad g \text{ irreduzibel und } e \text{ invertierbar.}$$

Aus der Eindeutigkeit der Primfaktorzerlegung in $k[[y, z]]$ folgt, daß g ein echter Teiler von f und g in $k[[y, z]]$ ist. Das ist ein Widerspruch zu Korollar A.33. \square

SATZ 8.6. *Seien k ein algebraisch abgeschlossener Körper und $f \in k[y, z] \setminus k$. Dann sind äquivalent:*

1. 0 ist ein aufgelöster Punkt von f .
2. $\text{stg}_0 f = \infty$.

Beweis. Sei zunächst 0 ein aufgelöster Punkt von f . Wenn $0 \notin V(f)$ ist, dann ist $\text{stg}_0 f = \infty$ nach Definition von stg_0 . Sei also $0 \in V(f)$. Dann ist $f = g^n h$ wie in (8.1). Nach Lemma 6.3 ist $\text{stg}_0 g = \infty$. Also gibt es ein $\varphi \in G$ mit $\varphi(g) = y\tilde{e}$ mit $\tilde{e} \in k[[y, z]]$ invertierbar. Für dieses φ ist dann

$$\varphi(f) = \varphi(g^n h) = y^n e, \quad \text{mit } e \in k[[y, z]] \text{ invertierbar.}$$

Damit ist $\text{stg}_0 f = \infty$.

Sei umgekehrt $\text{stg}_0 f = \infty$. Wenn $\text{ord} f = 0$ ist, dann ist 0 nach Definition ein aufgelöster Punkt von f . Sei also $\text{ord} f \geq 1$. Sei

$$f = c f_1^{b_1} \cdots f_r^{b_r}$$

die Primfaktorzerlegung von f . Angenommen es gibt $i, j \in \{1, \dots, r\}$, $i \neq j$, mit $\text{ord} f_i \geq 1$ und $\text{ord} f_j \geq 1$. Dann können wir f schreiben als $f = \tilde{f} \tilde{g} h$ mit $\tilde{f}, \tilde{g} \in k[y, z]$ teilerfremd, $\tilde{f}, \tilde{g} \in \mathfrak{m}$ und $h \in k[y, z]$ mit $\text{ord} h = 0$. Mit Lemma 6.1 ist dann aber $\text{stg}_0 f = \text{stg}_0(\tilde{f} \tilde{g}) = \infty$. Das ist ein Widerspruch zu Lemma 8.5. Also gibt es genau ein $i \in \{1, \dots, r\}$ mit $\text{ord} f_i \geq 1$. Angenommen es gilt $\text{ord} f_i > 1$. Nach Voraussetzung und Lemma 6.1 gilt $\text{stg}_0 f = \text{stg}_0 f_i^{b_i} = \infty$.

Nach Lemma 8.4 und Lemma 8.3 ist aber $\text{stg}_0 f_i^{b_i} < \infty$. Widerspruch. Also ist $\text{ord} f_i = 1$ und damit 0 ein aufgelöster Punkt von f . \square

9. EXPLOSION EINES PUNKTES

Wir erklären zunächst, was wir unter der Explosion des Nullpunktes im \mathbf{A}^2 verstehen. Durch eine Translation ist dann die Explosion eines beliebigen Punktes definiert.

Sei k ein algebraisch abgeschlossener Körper. Bezeichne $k[y, z]$ den affinen Koordinatenring von \mathbf{A}^2 und $(a, b) \in k^2$ die Punkte von \mathbf{A}^2 . Wir betrachten zwei weitere affine Räume $U_1 = \mathbf{A}^2$ bzw. $U_2 = \mathbf{A}^2$. Seien

$$\begin{aligned}\bar{\pi}_1: U_1 &\rightarrow \mathbf{A}^2, (a, b) \mapsto (ab, b), \\ \bar{\pi}_2: U_2 &\rightarrow \mathbf{A}^2, (a, b) \mapsto (a, ab).\end{aligned}$$

Die zu $\bar{\pi}_1$ bzw. $\bar{\pi}_2$ gehörigen Abbildungen π_1 bzw. π_2 auf $k[y, z]$ sind dann

$$\begin{aligned}\pi_1: k[y, z] &\rightarrow k[y, z], f(y, z) \mapsto f(yz, z), \\ \pi_2: k[y, z] &\rightarrow k[y, z], f(y, z) \mapsto f(y, yz).\end{aligned}$$

Wir definieren die offenen Mengen

$$\begin{aligned}U_{12} &= \{(a, b) \in U_1 \text{ mit } a \neq 0\} = U_1 \setminus V(y), \\ U_{21} &= \{(a, b) \in U_2 \text{ mit } b \neq 0\} = U_2 \setminus V(z).\end{aligned}$$

und die Abbildungen

$$\begin{aligned}\bar{h}_{12}: U_{12} &\rightarrow U_{21}, (a, b) \mapsto (ab, 1/a), \\ \bar{h}_{21}: U_{21} &\rightarrow U_{12}, (a, b) \mapsto (1/b, ab).\end{aligned}$$

Dann ist

$$(9.1) \quad \bar{h}_{12}\bar{h}_{21} = \text{Id} \quad \text{und} \quad \bar{h}_{21}\bar{h}_{12} = \text{Id},$$

und wir haben folgendes kommutatives Diagramm:

$$\begin{array}{ccc} U_{12} & \xrightleftharpoons{\bar{h}_{12}} & U_{21} \\ \cup & \bar{h}_{21} & \cup \\ U_1 & & U_2 \\ \searrow \bar{\pi}_1 & & \swarrow \bar{\pi}_2 \\ & \mathbf{A}^2 & \end{array}$$

Bezeichne $T = U_1 \sqcup U_2$ die topologische Summe von U_1 und U_2 . Das heißt T ist als Menge die disjunkte Vereinigung der beiden Mengen U_1 und U_2 und eine Teilmenge von T ist offen genau dann, wenn ihr Durchschnitt mit U_1 bzw. U_2 offen ist. Wir setzen $U_{11} = U_1$ bzw. $U_{22} = U_2$ und

$$(9.2) \quad \bar{h}_{11} = \text{Id}: U_{11} \rightarrow U_{11} \text{ bzw. } \bar{h}_{22} = \text{Id}: U_{22} \rightarrow U_{22}.$$

Damit können wir eine Äquivalenzrelation \sim auf T definieren. Wir sagen t und u aus T sind äquivalent, wenn $t \in U_{ij}$, $u \in U_{ji}$ und $u = \bar{h}_{ij}(t)$ für ein i bzw. ein j aus $\{1, 2\}$. Mit (9.1) und (9.2) erkennt man, daß \sim tatsächlich eine Äquivalenzrelation ist.

Wir schreiben nun $W' = T/\sim$ für den Quotientenraum (d.h., die Menge der Äquivalenzklassen versehen mit der Quotiententopologie) und $p: T \rightarrow W'$ für die kanonische Abbildung. Dann ist W' eine reguläre Varietät, die, wie man sagt, durch das Zusammenkleben von U_1 und U_2 entsteht. Wir nennen W' die *Explosion des Nullpunktes* von \mathbf{A}^2 . Über die kanonische Abbildung können wir U_1 bzw. U_2 mit den in W' offenen Mengen $p(U_1)$ bzw. $p(U_2)$ identifizieren. Es ist $W' = p(U_1) \cup p(U_2)$.

Die Abbildung $\bar{\pi}: W' \rightarrow \mathbf{A}^2$ mit

$$\bar{\pi}(w) = \begin{cases} \bar{\pi}_1(w), & \text{wenn } w \in U_1, \\ \bar{\pi}_2(w), & \text{wenn } w \in U_2, \end{cases}$$

ist wohldefiniert, da das obige Diagramm kommutativ ist.

LEMMA 9.1. Für $\bar{\pi}: W' \rightarrow \mathbf{A}^2$ und $E = \bar{\pi}^{-1}(0)$ gilt:

- (i) $E \cap U_1 = V(z)$ bzw. $E \cap U_2 = V(y)$.
- (ii) $E \simeq \mathbf{P}^1$.
- (iii) $\bar{\pi}: W' \setminus E \rightarrow \mathbf{A}^2 \setminus \{0\}$ ist ein Isomorphismus.

Beweis. Die Behauptung (i) ist klar nach Definition von $\bar{\pi}$.

Zu (ii): Man prüft leicht nach, daß die Abbildung $\bar{\varphi}: E \rightarrow \mathbf{P}^1$ mit

$$\bar{\varphi}(e) = \begin{cases} (a : 1), & \text{wenn } e = (a, 0) \in E \cap U_1, \\ (1 : b), & \text{wenn } e = (0, b) \in E \cap U_2, \end{cases}$$

wohldefiniert und bijektiv ist.

Zu (iii): Sei $w \in (W' \setminus E) \cap U_1$. Dann ist $w = (a, b)$ mit $b \neq 0$. Also ist $\bar{\pi}(w) = (ab, b) \in \mathbf{A}^2 \setminus \{0\}$. Analog schließt man für $w \in (W' \setminus E) \cap U_2$. Wir definieren $\bar{\varphi}: \mathbf{A}^2 \setminus \{0\} \rightarrow W' \setminus E$ durch

$$\bar{\varphi}(a) = \begin{cases} (a/b, b) \in U_1 \setminus E, & \text{wenn } a \in \mathbf{A}^2 \setminus V(z), \\ (a, b/a) \in U_2 \setminus E, & \text{wenn } a \in \mathbf{A}^2 \setminus V(y). \end{cases}$$

Die Abbildung ist wohldefiniert, denn für ein $(a, b) \in \mathbf{A}^2 \setminus V(yz)$ ist

$$\bar{h}_{12}(a/b, b) = ((a/b)b, 1/(a/b)) = (a, b/a).$$

Weiters sind $\bar{\varphi}\bar{\pi} = \text{Id}$ auf $W' \setminus E$ bzw. $\bar{\pi}\bar{\varphi} = \text{Id}$ auf $\mathbf{A}^2 \setminus \{0\}$. \square

Wir nennen E den *exzeptionellen Divisor* von $\bar{\pi}: W' \rightarrow \mathbf{A}^2$.

10. TOTAL UND STRIKT TRANSFORMIERTE

Seien $f \in k[y, z] \setminus k$,

$$f = \sum_{\alpha} c_{\alpha} y^{\alpha_1} z^{\alpha_2}$$

und $0 \in C = V(f)$, d.h., $r = \text{ord} f \geq 1$. Wir überlegen uns, wie das Urbild von C unter $\bar{\pi}$ aussieht. Dazu berechnen wir $\bar{\pi}^{-1}(C)$ in U_1 bzw. U_2 . Bezeichne

$$f_1^* = f_1^*(y, z) = \pi_1(f) = f(yz, z)$$

bzw. $f_2^* = \pi_2(f) = f(y, yz)$. Wir führen alle folgenden Überlegungen nur für f_1^* und U_1 aus und schreiben f^* für f_1^* . Für f_2^* und U_2 gelten die analogen Aussagen. Es gilt

$$\begin{aligned} \bar{\pi}^{-1}(C) \cap U_1 &= \{a = (a_1, a_2) \in U_1 \text{ mit } \bar{\pi}_1(a) = (a_1 a_2, a_2) \in C\} \\ &= \{a \in U_1 \text{ mit } f(a_1 a_2, a_2) = 0\} = V(f^*). \end{aligned}$$

Man nennt $\bar{\pi}^{-1}(C) \subset W'$ die *total Transformierte* von C bzw. f^* die *total Transformierte* von f in U_1 . Wir können f^* zerlegen in

$$\begin{aligned} (10.1) \quad f^* = f(yz, z) &= \sum_{\alpha} c_{\alpha} y^{\alpha_1} z^{\alpha_1 + \alpha_2} \\ &= z^r \sum_{\alpha} c_{\alpha} y^{\alpha_1} z^{\alpha_1 + \alpha_2 - r} = z^r f'(y, z) = z^r f'. \end{aligned}$$

Dann ist

$$V(f^*) = V(z^r f') = V(z^r) \cup V(f') = (E \cap U_1) \cup V(f').$$

Wir nennen f' die *strikt Transformierte* von f in U_1 . Um die Primfaktoren von f' zu untersuchen, überlegen wir uns zunächst, daß f' nicht durch z teilbar ist. Wir schreiben

$$f = f_r + f_{r+1} + \cdots + f_d, \quad \text{mit } d = \text{deg} f$$

als Summe von homogenen Polynomen. Dann ist

$$\begin{aligned} f^* = f(yz, z) &= f_r(yz, z) + f_{r+1}(yz, z) + \cdots + f_d(yz, z) \\ &= z^r(f_r(y, 1) + zf_{r+1}(y, 1) + \cdots + z^{d-r}f_d(y, 1)) = z^r f' \end{aligned}$$

mit $f_r(y, 1) \neq 0$, also teilt z nicht f' . Aus dieser Darstellung der strikt Transformierten von f folgt das nächste Lemma.

LEMMA 10.1. *Es gilt*

$$(E \cap U_1) \cap V(f') = V(z) \cap V(f') = \{(t, 0) \text{ mit } f_r(t, 1) = 0\}.$$

Insbesondere ist diese Menge endlich.

LEMMA 10.2. *Sei $f \neq cz$ mit $c \in k \setminus 0$ und f irreduzibel bzw. reduziert. Dann ist auch f' irreduzibel bzw. reduziert.*

Beweis. Angenommen f' ist reduzibel, d.h.,

$$f' = gh, \quad \text{mit } g, h \in k[y, z] \setminus k.$$

Wenn wir nun y/z für y einsetzen, ist mit (10.1)

$$f = z^r g(y/z, z) h(y/z, z).$$

Indem wir diese Gleichung mit einer genügend hohen Potenz von z multiplizieren, ist

$$z^n f = z^r \tilde{g} \tilde{h}, \quad \text{mit } n \in \mathbf{N}_0 \text{ und } \tilde{g}, \tilde{h} \in k[y, z].$$

Da \tilde{g} und \tilde{h} jeweils einen Primfaktor ungleich z besitzen (sonst wäre f' durch z teilbar), folgt ein Widerspruch zur Irreduzibilität von f . Eine ähnliche Argumentation zeigt auch, daß die Reduziertheit von f die Reduziertheit von f' impliziert. \square

Sei $a' = (t, 0) \in E \cap U_1$. Uns interessiert die Invariante $\text{inv}_{a'} f'$ von f' im Punkt a' . Nach Definition ist

$$\text{inv}_{a'} f' = \text{inv}_0 f'(y + t, z) = \text{inv}_0 v(f')$$

mit

$$v: k[y, z] \rightarrow k[y, z]$$

dem zu $\bar{v} = (y + t, z)$ gehörigen Einsetzungshomomorphismus (v ist nur auf dem Polynomring definiert!). Es gibt aber eine für unsere Zwecke günstigere Möglichkeit, $\text{inv}_{a'} f'$ zu berechnen. Sei dazu

$$w: k[y, z] \rightarrow k[y, z], \quad \text{mit } \bar{w} = (y + tz, z).$$

LEMMA 10.3. *In dieser Situation ist*

$$\begin{array}{ccc} k[y, z] & \xrightarrow{v} & k[y, z] \\ \pi_1 \uparrow & & \uparrow \pi_1 \\ k[y, z] & \xrightarrow{w} & k[y, z] \end{array}$$

kommutativ, und es gilt

$$f'(y + t, z) = v(f') = w(f)' = f(y + tz, z)'$$

(vgl. Lemma 11.7).

Beweis. Das obige Diagramm kommutiert, denn

$$v\pi_1(y) = v(yz) = yz + tz = \pi_1(y + tz) = \pi_1 w(y)$$

und

$$v\pi_1(z) = z = \pi_1 w(z).$$

Aus der Kommutativität (und da $\text{ord } w(f) = r$) folgt dann

$$z^r v(f') = v(z^r f') = v\pi_1(f) = \pi_1 w(f) = z^r w(f)'$$

□

11. DIE INVARIANTE FÄLLT UNTER EXPLOSION

In diesem Abschnitt zeigen wir, dass die Auflösungsinvariante einer Kurve unter Explosion fällt. Wir beschäftigen uns mit dem Beweis des folgenden Satzes.

SATZ 11.1. *Seien k ein algebraisch abgeschlossener Körper, $f \in k[y, z] \setminus k$ und $a \in \mathbf{A}^2$ ein nicht aufgelöster Punkt von f . Wir betrachten die Explosion des Punktes $a \in \mathbf{A}^2$. Dann ist die Invariante der strikt transformierten von f in jedem Punkt des exzeptionellen Divisors kleiner als die Invariante von f im Punkt a ,*

$$\text{inv}_{a'} f' < \text{inv}_a f, \quad \text{für } a' \in E.$$

Nach einer Translation in \mathbf{A}^2 können wir annehmen, daß a der Nullpunkt ist. Sei

$$a' = (t, 0) \in E \cap U_1.$$

Bezeichne l_t den zu $\bar{l}_t = (y + tz, z)$ gehörigen Substitutionshomomorphismus. Dann ist mit Lemma 10.3

$$(11.1) \quad \text{inv}_{a'} f' = \text{inv}_0 l_t(f)' = (\text{ord}_0 l_t(f)', \text{stg}_0 l_t(f)').$$

Wir können also, um die Invariante von f' in jedem Punkt von $E \cap U_1$ zu untersuchen, auch $\text{ord}_0 l_t(f)'$ bzw. $\text{stg}_0 l_t(f)'$ für $t \in k$ betrachten. Wir werden dies im folgenden gleich für beliebige Potenzreihen tun. Um die Invariante in jedem Punkt des exzeptionellen Divisors zu kennen, müssen wir auch noch $\text{inv}_0 f'_2$ in U_2 untersuchen.

Wir verwenden in diesem Abschnitt folgende Bezeichnungen, die unter anderem den Begriff der total und strikt transformierten auf Potenzreihen verallgemeinern. Sei R ein Potenzreihenring in zwei Variablen über einem Körper k und $\mathbf{y} = (y, z)$ ein reguläres Parametersystem von R . Sei $f \in R$ mit $f \neq 0$, $r = \text{ord} f \geq 1$ und

$$(11.2) \quad f = f(y, z) = \sum_{\alpha} c_{\alpha} y^{\alpha_1} z^{\alpha_2}.$$

Sei weiters $\pi_1: R \rightarrow R$ bzw. $\pi_2: R \rightarrow R$ die zu $\bar{\pi}_1 = (yz, z)$ bzw. $\bar{\pi}_2 = (y, yz)$ gehörigen Substitutionshomomorphismen. Bezeichne

$$\begin{aligned} f^* = \pi_1(f) = f(yz, z) &= \sum_{\alpha} c_{\alpha} y^{\alpha_1} z^{\alpha_1 + \alpha_2} \\ &= z^r \sum_{\alpha} c_{\alpha} y^{\alpha_1} z^{\alpha_1 + \alpha_2 - r} = z^r f'(y, z) = z^r f' \end{aligned}$$

und

$$f_2^* = \pi_2(f) = f(y, yz) = y^r f'_2.$$

LEMMA 11.2. *Es gilt:*

- (i) $\Delta_{\mathbf{y}}(f') = \{(\alpha_1, \alpha_1 + \alpha_2 - r) \text{ mit } (\alpha_1, \alpha_2) \in \Delta_{\mathbf{y}}(f)\}$.
- (ii) $\text{ord} f' \leq \text{ord} f = r$.

Beweis. Zu (ii): Sei $\alpha \in \Delta_{\mathbf{y}}(f)$ mit $\alpha_1 + \alpha_2 = r$, dann ist

$$\alpha_1 + (\alpha_1 + \alpha_2 - r) \leq r.$$

Also ist $\text{ord} f' \leq r$. \square

LEMMA 11.3. *Sei $\text{stg} f = \text{ord} f = r$. Dann sind*

$$\text{ord} l_t(f)' < \text{ord} f, \quad \text{für } t \in k$$

und $\text{ord} f'_2 < \text{ord} f$.

Beweis. Für jedes $t \in k$ gibt es ein $\alpha \in \Delta_{\mathbf{y}}(l_t(f))$ mit $\alpha_1 + \alpha_2 = r$ und $\alpha \neq (r, 0)$ (sonst wäre $\text{stg} f \geq \text{stg}_{\mathbf{y}} l_t(f) > r$). Für dieses α ist dann $\alpha_1 + (\alpha_1 + \alpha_2 - r) = \alpha_1 < r$. Also folgt, da $(\alpha_1, \alpha_1 + \alpha_2 - r) \in \Delta_{\mathbf{y}}(f')$, die Behauptung.

Außerdem gibt es einen Term $c_{\alpha} y^{\alpha_1} z^{\alpha_2}$ von f mit $\alpha_1 + \alpha_2 = r$ und $\alpha \neq (0, r)$ (sonst wäre $\text{stg} f \geq \text{stg}_{\mathbf{y}} p(f) > r$ mit p der Vertauschung von y und z), und damit ist auch $\text{ord} f'_2 < r$. \square

LEMMA 11.4. Seien $\text{stg} f > \text{ord} f = r$ und $\mathbf{y} = (y, z)$ ein reguläres Parametersystem von R so, daß $\text{stg}_{\mathbf{y}} f > r$. Dann sind

$$\text{ord} l_t(f)' = 0, \quad \text{für } t \in k, t \neq 0,$$

und $\text{ord} f'_2 = 0$.

Beweis. Wie im Beweis zu Lemma 5.5 erkennt man, daß in $l_t(f)$ der Koeffizient von z^r nicht Null ist. Also ist $\text{ord} l_t(f)' = 0$. Da $f_r = cy^r$, $c \neq 0$, ist auch $\text{ord}(f'_2) = 0$. \square

LEMMA 11.5. $\text{ord} f' < \text{ord} f = r$ genau dann, wenn $\text{stg}_{\mathbf{y}} f < 2 \text{ord} f$.

Beweis. Angenommen $s = \text{stg}_{\mathbf{y}} f \geq 2r$. Sei $\alpha \in \Delta_{\mathbf{y}}(f)$. Dann ist

$$\frac{s}{r} \alpha_1 + \alpha_2 \geq s$$

und damit

$$2\alpha_1 + \alpha_2 \geq 2r \text{ bzw. } \alpha_1 + (\alpha_1 + \alpha_2 - r) \geq r.$$

Also folgt mit Lemma 11.2, daß $\text{ord} f' \geq r$. Wenn $\text{stg}_{\mathbf{y}} f < 2r$, dann gibt es ein $\alpha \in \text{NP}_{\mathbf{y}}(f)$, $\alpha \neq (r, 0)$, mit

$$\frac{r\alpha_2}{r - \alpha_1} < 2r.$$

Für dieses α ist dann $\alpha_1 + (\alpha_1 + \alpha_2 - r) < r$, also ist $\text{ord} f' < r$. \square

Wir erinnern an eine Notation von Abschnitt 4, die wir im folgenden verwenden. Seien f wie in (11.2) und $t \in \mathbf{R}$, $t \geq r = \text{ord} f$. Dann schreiben wir

$$F_t = \sum_{\alpha} c_{\alpha} \mathbf{y}^{\alpha}, \quad \text{für } \alpha \text{ mit } \frac{t}{r} \alpha_1 + \alpha_2 = t \text{ bzw.}$$

$$F_{>t} = \sum_{\alpha} c_{\alpha} \mathbf{y}^{\alpha}, \quad \text{für } \alpha \text{ mit } \frac{t}{r} \alpha_1 + \alpha_2 > t.$$

LEMMA 11.6. Sei $\infty > \text{stg}_y f \geq 2 \text{ord} f$. Dann ist

$$\text{stg}_y f' = \text{stg}_y f - \text{ord} f$$

(siehe Abbildung 10).

Beweis. Seien $r = \text{ord} f$, $s = \text{stg}_y f$ und $s' = s - r$. Nach der vorherigen Lemma und Lemma 11.2 ist $r = \text{ord} f'$. Wir zerlegen f in

$$f = F_s + F_{>s}.$$

Sei $c_\alpha y^{\alpha_1} z^{\alpha_2}$ ein beliebiger Term von F_s mit $\alpha \neq (r, 0)$. Dann ist

$$\frac{r\alpha_2}{r - \alpha_1} = s$$

und deshalb

$$\frac{r(\alpha_1 + \alpha_2 - r)}{r - \alpha_1} = \frac{r\alpha_2}{r - \alpha_1} - r = s - r = s'.$$

Also ist

$$\frac{s'}{r} \alpha_1 + (\alpha_1 + \alpha_2 - r) = s'.$$

Für einen Term $c_\alpha y^{\alpha_1} z^{\alpha_2}$ von $F_{>s}$ mit $\alpha_1 < r$ ist

$$\frac{r\alpha_2}{r - \alpha_1} > s,$$

und damit folgt wie zuvor

$$\frac{s'}{r} \alpha_1 + (\alpha_1 + \alpha_2 - r) > s'.$$

Wenn $\alpha_1 \geq r$ ist, dann gilt diese Ungleichung trivialerweise. Also können wir f' zerlegen in

$$f' = F'_{s'} + F'_{>s'}.$$

Mit Lemma 4.5 folgt die Behauptung. \square

LEMMA 11.7. Sei l der zu $\bar{l} = (y + g, z)$ gehörige Substitutionshomomorphismus mit $g \in zk[[z]]$. Sei m der zu $\bar{m} = (y + zg, z)$ gehörige Substitutionshomomorphismus. Dann ist folgendes Diagramm kommutativ,

$$\begin{array}{ccc} R & \xrightarrow{l} & R \\ \pi_1 \uparrow & & \uparrow \pi_1 \\ R & \xrightarrow{m} & R \end{array}$$

und es gilt

$$l(f') = m(f)'$$

Beweis. Nachrechnen, analog zum Beweis von Lemma 10.3. \square

LEMMA 11.8. Seien $\infty > \text{stg} f \geq 2 \text{ord} f$ und $\mathbf{y} = (y, z)$ ein reguläres Parametersystem von R so, daß $\text{stg}_{\mathbf{y}} f = \text{stg} f$. Dann wird $\text{stg} f'$ durch $\mathbf{y} = (y, z)$ realisiert, d.h.,

$$\text{stg} f' = \text{stg}_{\mathbf{y}} f'.$$

Beweis. Angenommen $\text{stg} f' > \text{stg}_{\mathbf{y}} f' = s'$. Dann gibt es ein $l \in L'$ und ein $p \in P'$ mit $\text{stg}_{\mathbf{y}} lp(f') > s'$. Wenn $s' > r = \text{ord} f$, dann ist p die Identität. Wenn $s' = r$ und p die Vertauschung von y und z ist, dann folgt, da f' y -allgemein der Ordnung r ist, mit Satz 5.8, daß

$$p(f') = c(y + dz)^r + F_{>r}, \quad \text{mit } c, d \in k, c, d \neq 0.$$

Also ist

$$f' = cd^r(y + d^{-1}z)^r + \tilde{F}_{>r}.$$

Wir können daher annehmen, daß p die Identität ist. Mit m wie im vorherigen Lemma folgt

$$l(f') = m(f)'$$

Dann ist $\text{stg}_{\mathbf{y}} m(f) \geq 2r$. Sonst wäre nach Lemma 11.5

$$\text{ord}(f') = \text{ord} l(f') = \text{ord} m(f)' < r.$$

Mit Lemma 11.6 folgt dann

$$\text{stg} f - r = s' < \text{stg}_{\mathbf{y}} l(f') = \text{stg}_{\mathbf{y}} m(f)' = \text{stg}_{\mathbf{y}} m(f) - r \leq \text{stg} f - r,$$

also ein Widerspruch. \square

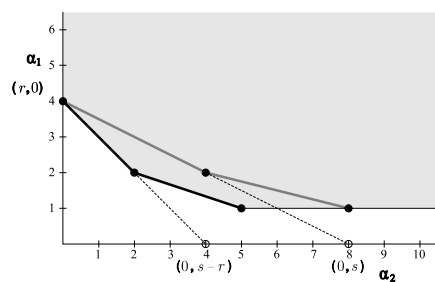


ABBILDUNG 10

Die Steigung fällt: $\text{stg}_{\mathbf{y}} f' = \text{stg}_{\mathbf{y}} f - \text{ord} f$

SATZ 11.9. Seien $f \in R$, $f \neq 0$, $r = \text{ord}f \geq 1$. Sei $\infty > \text{stg}f \geq 2 \text{ord}f$. Dann ist

$$\text{stg}f' = \text{stg}f - \text{ord}f.$$

Beweis. Klar nach dem vorherigen Lemma und Lemma 11.6. \square

Wir wenden die Ergebnisse dieses Abschnitts auf ebene Kurven an und beweisen den Satz vom Beginn dieses Abschnitts.

Beweis von Satz 11.1. Seien also k ein algebraisch abgeschlossener Körper, $f \in k[y, z] \setminus k$, $r = \text{ord}_0 f \geq 1$ und 0 ein nicht aufgelöster Punkt von f .

Wenn $\text{stg}_0 f = \text{ord}_0 f$ ist, dann ist mit (11.1) und Lemma 11.3

$$\text{inv}_{a'} f' < \text{inv}_0 f, \quad \text{für } a' \in E \cap U_1.$$

Weiters gilt $\text{inv}_0 f'_2 < \text{inv}_0 f$.

Sei nun $\text{stg}_0 f > \text{ord}_0 f$. Da nach Annahme der Nullpunkt ein nicht aufgelöster Punkt ist, folgt $\text{stg}_0 f < \infty$ mit Satz 8.6. Daher können wir mit Satz 6.6 annehmen, daß nach einem polynomialen Koordinatenwechsel $\text{stg}_0 f = \text{stg}_y f$ gilt. Lemma 11.4 zeigt, daß es genügt, $\text{inv}_0 f'$ und $\text{inv}_0 f$ zu vergleichen. Wir unterscheiden zwei Fälle:

- (1) Wenn $\text{stg}_0 f < 2 \text{ord}_0 f$ ist, dann ist nach Lemma 11.5 $\text{ord}f' < \text{ord}f$ und damit $\text{inv}_0 f' < \text{inv}_0 f$.
- (2) Wenn $\text{stg}_0 f \geq 2 \text{ord}_0 f$. Dann ist $\text{ord}f' = \text{ord}f$ und mit dem vorherigen Satz $\text{stg}_0 f' = \text{stg}_0 f - \text{ord}_0 f < \text{stg}_0 f$. Es gilt wieder $\text{inv}_0 f' < \text{inv}_0 f$.

Also haben wir auch für den Fall $\text{stg}_0 f > \text{ord}_0 f$ gezeigt, daß

$$\text{inv}_{a'} f' < \text{inv}_0 f, \quad \text{für } a' \in E$$

gilt. \square

12. BEWEIS DES HAUPTSATZES

Zum Abschluß zeigen wir, wie mit den bisherigen Ergebnissen bewiesen werden kann, daß durch eine endliche Folge von Explosionen von Punkten die singulären (bzw. nicht aufgelösten) Punkte einer ebenen algebraischen Kurve aufgelöst werden können.

Seien k ein algebraisch abgeschlossener Körper und $f \in k[y, z] \setminus k$. Nach Satz 8.1 gibt es nur endlich viele nicht aufgelöste Punkte von f . Sei a ein

nicht aufgelöster Punkt von f . Wir explodieren den Punkt a . Lemma 10.1 besagt, daß in nur endlich vielen Punkten des exzeptionellen Divisors die Ordnung der strikt Transformierten größer als Null ist. Sei $a' \in E$ ein solcher Punkt. Wenn a' ein aufgelöster Punkt der strikt Transformierten ist, dann sind wir fertig. Sonst ist nach Satz 11.1 die Invariante der strikt Transformierten in a' kleiner als die Invariante von f im Nullpunkt. Durch Induktion über die Invariante (vgl. Abschnitt 7) folgt die Behauptung. \square

A. APPENDIX

A.1 POTENZREIHENRINGE

In diesem Abschnitt werden die verwendeten Begriffe und Ergebnisse über formale Potenzreihen diskutiert bzw. hergeleitet.

A.1.1 DEFINITION Seien A ein kommutativer Ring mit Einselement und $A[x_1, \dots, x_n] = A[x]$ mit $x = (x_1, \dots, x_n)$ der Polynomring in n Variablen über A . Unter einer *formalen Potenzreihe in n Unbekannten über A* verstehen wir eine unendliche Folge $f = (f_0, f_1, \dots, f_k, \dots)$ von Polynomen $f_k \in F_k$ mit F_k dem Modul der homogenen Polynome vom Grad k in $A[x]$. Addition und Multiplikation zweier Potenzreihen f und g definieren wir wie folgt:

$$f + g = (f_0 + g_0, f_1 + g_1, \dots, f_k + g_k, \dots),$$

$$fg = (h_0, h_1, \dots, h_k, \dots), \quad \text{mit } h_k = \sum_{i+j=k} f_i g_j.$$

Damit wird die Menge aller formalen Potenzreihen in n Variablen über A zu einem kommutativen Ring mit Einselement. Diesen Ring bezeichnen wir mit $A[[x_1, \dots, x_n]] = A[[x]]$ mit $x = (x_1, \dots, x_n)$. Mit der kanonischen Identifikation ist $A = F_0 \subset A[[x]]$ bzw. $A[x] \subset A[[x]]$.

Sei f eine formale Potenzreihe ungleich Null. Den kleinsten Index q mit $f_q \neq 0$ nennen wir die *Ordnung* von f , kurz $\text{ord} f$, und f_q die *Initialform*. Weiters setzen wir $\text{ord} f = \infty$ für $f = 0$. Mit dieser Definition gilt folgendes

LEMMA A.1. Für $f, g \in A[[x]]$ gilt

$$\text{ord}(f + g) \geq \min(\text{ord} f, \text{ord} g),$$

$$\text{ord}(fg) \geq \text{ord} f + \text{ord} g.$$

Wenn A ein Integritätsring ist, dann ist auch $A[[x]]$ ein Integritätsring und es gilt

$$\text{ord}(fg) = \text{ord}f + \text{ord}g.$$

Beweis. Ähnlich zum Beweis der analogen Aussagen für den Grad eines Polynoms im Polynomring $A[x]$, nur muß man den höchsten Term ungleich Null durch die Initialform ersetzen. \square

SATZ A.2. Eine Potenzreihe f ist genau dann eine Einheit in $A[[x]]$, wenn f_0 in A invertierbar ist.

Beweis. Wenn $gf = 1$, dann ist $g_0f_0 = 1$ und damit f_0 invertierbar in A . Sei umgekehrt f_0 invertierbar, dann können wir induktiv $g_0, g_1, \dots, g_k, \dots$ mit $g_k \in F_k$ konstruieren so, daß

$$\begin{aligned} f_0g_0 &= 1, \\ f_0g_1 + f_1g_0 &= 0, \dots, \\ f_0g_k + f_1g_{k-1} + \dots + f_kg_0 &= 0, \dots \end{aligned}$$

Für den Induktionsanfang setzen wir $g_0 = f_0^{-1}$. Wenn wir g_0, g_1, \dots, g_{k-1} bereits bestimmt haben, können wir aus der letzten Gleichung g_k berechnen und erhalten

$$g_k = -f_0^{-1}(f_1g_{k-1} + \dots + f_kg_0).$$

Mit dem so konstruierten $g = (g_0, g_1, \dots, g_k, \dots)$ gilt nach der Definition der Multiplikation $fg = 1$. \square

Für das nächste Korollar brauchen wir noch folgende Beobachtungen. Die Potenzreihen mit einer positiven Ordnung bilden nach Lemma A.1 ein Ideal \mathfrak{m} , das von x_1, \dots, x_n erzeugt wird. Das Ideal \mathfrak{m}^q besteht aus allen Potenzreihen f mit $\text{ord}f \geq q$ und wird erzeugt von allen Monomen $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ mit $|\alpha_1, \dots, \alpha_n| = \alpha_1 + \dots + \alpha_n = q$.

KOROLLAR A.3. Sei k ein Körper. Dann ist $k[[x]]$ ein lokaler Ring mit maximalem Ideal $\mathfrak{m} = (x_1, \dots, x_n)$.

Beweis. Klar, da mit Satz A.2 jedes Element von $k[[x]] \setminus \mathfrak{m}$ invertierbar ist. \square

SATZ A.4. Wenn A ein noetherscher Ring ist, dann ist auch $A[[x]]$ mit $x = (x_1, \dots, x_n)$ noethersch.

Beweis. Siehe z.B. [La, S. 210]. \square

A.1.2 DIE \mathfrak{q} -ADISCHE TOPOLOGIE Bevor wir eine Topologie auf dem Ring der formalen Potenzreihen einführen, erklären wir zunächst die allgemeine Konstruktion der sogenannten \mathfrak{q} -adischen Topologie auf einem beliebigen Ring.

Ein Ring A , der zugleich ein topologischer Raum ist, heißt *topologischer Ring*, wenn er bezüglich der Addition eine topologische Gruppe (d.h., $A \times A \rightarrow A, (a, b) \mapsto a + b$ ist stetig) ist, und wenn die Multiplikation stetig ist. In einer topologischen Gruppe ist die Translation ($T_a: A \rightarrow A, b \mapsto a + b, a \in A$) ein Homöomorphismus (mit der stetigen Umkehrabbildung T_{-a}). Damit ist eine Topologie auf A durch die Umgebungen der Null eindeutig bestimmt. Wenn U eine Umgebung der Null ist, so ist $a + U$ eine Umgebung von a .

LEMMA A.5. *Wenn $\{0\}$ in A abgeschlossen ist, dann ist A Hausdorffsch.*

Beweis. Aus der Abgeschlossenheit von $\{0\}$ folgt mit der Stetigkeit von $A \times A \rightarrow A, (a, b) \mapsto a - b$, daß die Diagonale ($\{(a, a) \subseteq A \times A: a \in A\}$) als Urbild der Null abgeschlossen ist, und damit ist A Hausdorffsch. \square

Für einen beliebigen Ring A und ein gegebenes Ideal $\mathfrak{q} \subseteq A$ definiert man die \mathfrak{q} -adische Topologie, die A zu einem topologischen Ring macht, folgendermaßen. Wir betrachten die absteigende Folge

$$\mathfrak{q}^0 = A \supseteq \mathfrak{q}^1 \supseteq \cdots \supseteq \mathfrak{q}^n \supseteq \cdots$$

von Idealen. Eine Teilmenge $U \subseteq A$ ist eine Umgebung von $a \in A$ genau dann, wenn es ein $n \in \mathbf{N}_0$ gibt mit $a + \mathfrak{q}^n \subseteq U$. Mit dieser Definition wird, wie man leicht sieht, A zu einem topologischen Raum und $\{a + \mathfrak{q}^n\}_{n \geq 0}$ zu einer Umgebungsbasis von $a \in A$.

LEMMA A.6. *Seien A ein Ring, $\mathfrak{q} \subseteq A$ ein Ideal und A mit der \mathfrak{q} -adischen Topologie versehen. Dann gilt:*

- (i) A ist ein topologischer Ring.
- (ii) \mathfrak{q}^n mit $n \geq 0$ ist offen und abgeschlossen.
- (iii) A ist genau dann Hausdorffsch, wenn $\bigcap_{n=0}^{\infty} \mathfrak{q}^n = \{0\}$.

Beweis. Zu (i): Nachprüfen.

Zu (ii): Wenn $a \in \mathfrak{q}^n$ ist, dann ist $a + \mathfrak{q}^n \subseteq \mathfrak{q}^n$ und damit \mathfrak{q}^n offen. Andererseits ist $A \setminus \{\mathfrak{q}^n\} = \bigcup_{b \notin \mathfrak{q}^n} b + \mathfrak{q}^n$ offen und daher \mathfrak{q}^n abgeschlossen.

Zu (iii): Klar mit der vorherigen Lemmata und da in einem Hausdorffraum jede einelementige Teilmenge abgeschlossen ist. \square

Im allgemeinen ist die q -adische Topologie nicht metrisierbar, trotzdem läßt sich der Begriff der Cauchyfolge auf einen topologischen Ring (wie im Fall von topologischen Vektorräumen) verallgemeinern. Man nennt eine Folge $(a_i)_{i \in \mathbf{N}_0}$ eine *Cauchyfolge* genau dann, wenn es zu jeder Nullumgebung U ein $m \in \mathbf{N}_0$ mit $a_k - a_l \in U$ für $k, l > m$. Ein topologischer Ring heißt *vollständig* genau dann, wenn jede Cauchyfolge konvergiert.

Sei im folgenden $A[[x_1, \dots, x_n]] = A[[x]]$ mit der im vorigen Abschnitt definierten Topologie bezüglich des Ideals $\mathfrak{m} = (x_1, \dots, x_n)$ versehen.

Wie oben bemerkt ist $f \in \mathfrak{m}^q$ mit $f \in A[[x]]$ und $q \in \mathbf{N}_0$ genau dann, wenn $\text{ord} f \geq q$ (also ist eine Potenzreihe f in dieser Topologie "nahe" bei Null, wenn die Ordnung von f groß ist). Da offensichtlich $\bigcap_{q=0}^{\infty} \mathfrak{m}^q = \{0\}$ gilt, ist $A[[x]]$ Hausdorffsch.

LEMMA A.7. $A[[x]]$ ist vollständig.

Beweis. Sei $(f^i)_{i \in \mathbf{N}_0}$ eine Cauchyfolge in $A[[x]]$. Zu jedem $q \in \mathbf{N}_0$ gibt es dann ein minimales $m(q)$ mit $\text{ord}(f^i - f^j) > q$ für $i, j > m(q)$, d.h., die Potenzreihen stimmen bis zur Ordnung q überein. Mit

$$f = (f_0^{m(0)}, f_1^{m(1)}, \dots, f_k^{m(k)}, \dots)$$

gilt dann $\text{ord}(f - f^i) \geq q$ für $i \geq m(q)$ und damit $\lim f^i = f$. \square

Aus der Stetigkeit der Addition bzw. Multiplikation folgt $\lim(f^i + g^i) = \lim f^i + \lim g^i$ bzw. $\lim f^i g^i = \lim f^i \lim g^i$.

Wenn $(f^i)_{i \in \mathbf{N}_0}$ eine Nullfolge ist, dann ist die Folge der Partialsummen $h^i = \sum_{k=0}^i f^k$ eine Cauchyfolge und somit konvergent. Wir definieren wie immer $\sum_{i=0}^{\infty} f^i = \lim h^i$. Es gelten dann die üblichen Rechenregeln:

$$(A.1) \quad \begin{aligned} \sum_{i=0}^{\infty} f^i + \sum_{i=0}^{\infty} g^i &= \sum_{i=0}^{\infty} (f^i + g^i), \\ \sum_{i=0}^{\infty} f^i \sum_{i=0}^{\infty} g^i &= \sum_{i=0}^{\infty} h^i, \quad \text{mit } h^i = \sum_{j+k=i} f^j g^k, \\ g \sum_{i=0}^{\infty} f^i &= \sum_{i=0}^{\infty} g f^i. \end{aligned}$$

Mit dieser Definition können wir jede formale Potenzreihe

$$f = (f_0, f_1, \dots, f_k, \dots)$$

als unendliche Reihe $f = \sum_{i=0}^{\infty} f_i$ schreiben. Manchmal notieren wir auch genauer

$$f = f(x_1, \dots, x_n) = \sum_{\alpha} c_{\alpha} x^{\alpha} = \sum_{\alpha} c_{\alpha} x_1^{\alpha_1} \cdots x_n^{\alpha_n}$$

mit $c_{\alpha} \in A$, $\alpha = (\alpha_1, \dots, \alpha_n) \in \mathbf{N}_0^n$,
 $x = (x_1, \dots, x_n)$ und $x^{\alpha} = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$.

Wenn $c_{\alpha} \neq 0$, so nennen wir $c_{\alpha} x^{\alpha}$ einen *Term* der Potenzreihe f .

Da wir jede Potenzreihe als Limes von Polynomen schreiben können, ist $A[x]$ eine dichte Teilmenge von $A[[x]]$. Dichte Teilmengen, die gleichzeitig ein Unterring von $A[[x]]$ sind, charakterisiert folgendes Lemma.

LEMMA A.8. *Sei S ein Unterring von $A[[x]]$. S ist genau dann dicht in $A[[x]]$, wenn es für jedes homogene Polynom $g \in A[x]$ mindestens ein $f \in S$ gibt so, daß g die Initialform von f ist.*

Beweis. Sei also S dicht in $A[[x]]$ und $g \in A[x]$ ein homogenes Polynom vom Grad k . Weil S dicht ist, gibt es ein $f \in S$ mit $\text{ord}(f - g) > k$. Daraus folgt, daß g die Initialform von f ist. (Für diese Implikation brauchen wir nicht, daß S ein Unterring ist.)

Sei umgekehrt $h \in A[[x]]$. Wir konstruieren induktiv eine Folge $(h^i)_{i \in \mathbf{N}_0}$ in S mit $\text{ord}(h^i - h) \geq i$. Setze $h^0 = 0$. Seien h^0, h^1, \dots, h^{i-1} bereits konstruiert. Wenn $\text{ord}(h^{i-1} - h) \geq i$, dann setzen wir $h^i = h^{i-1}$, sonst haben wir $\text{ord}(h^{i-1} - h) = i - 1$. Sei g die Initialform von $h - h^{i-1}$ und $f \in S$ mit Initialform g . Setze $h^i = h^{i-1} + f$ (hier brauchen wir, daß S additiv abgeschlossen ist), dann ist $\text{ord}(h^i - h) = \text{ord}(h^{i-1} + f - h) \geq i$. \square

A.1.3 SUBSTITUTIONSHOMOMORPHISMEN Seien A, A' kommutative Ringe mit Einselement, $\varphi: A \rightarrow A'$ ein Ringhomomorphismus und $a_1, \dots, a_n \in A'$. Für den Polynomring $A[x_1, \dots, x_n]$ gibt es dann einen eindeutigen Substitutionshomomorphismus

$$\bar{\varphi}: A[x_1, \dots, x_n] \rightarrow A', \quad \text{mit } \bar{\varphi}|_A = \varphi \text{ und } \bar{\varphi}(x_i) = a_i, \quad \text{für } i = 1, \dots, n.$$

“Man setzt a_i für x_i ein”. Für den Ring der formalen Potenzreihen muß man beim “Einsetzen” Vorsicht walten lassen, denn im allgemeinen haben

wir keinen geeigneten Konvergenzbegriff zur Verfügung. Mit der zuvor definierten Topologie können wir aber sagen, wann Potenzreihen in Potenzreihen eingesetzt konvergieren.

Seien dazu $f = \sum_{i=0}^{\infty} f_i \in A[[y_1, \dots, y_m]] = A[[y]]$ und $\varphi_1, \dots, \varphi_m \in A[[x_1, \dots, x_n]] = A[[x]]$ Potenzreihen mit $\text{ord } \varphi_j \geq 1$ für alle j . Jedes f_i ist ein homogenes Polynom vom Grad i oder 0. Damit ist $\bar{f}_i = f_i(\varphi_1, \dots, \varphi_m)$ eine Potenzreihe in $A[[x]]$ mit $\text{ord } \bar{f}_i \geq i$ (nach Lemma A.1), d.h., $(\bar{f}_i)_{i \in \mathbb{N}_0}$ ist eine Nullfolge. Somit ist

$$f(\varphi_1, \dots, \varphi_m) = \sum_{i=0}^{\infty} f_i(\varphi_1, \dots, \varphi_m) = \sum_{i=0}^{\infty} \bar{f}_i$$

eine wohldefinierte Potenzreihe, die, wie man sagt, aus Substitution von y_j durch φ_j entsteht. Durch die Zuordnung

$$f = f(y_1, \dots, y_m) \mapsto f(\varphi_1, \dots, \varphi_m)$$

ist eine Abbildung $\varphi: A[[y]] \rightarrow A[[x]]$ definiert. Mit (A.1) sieht man, daß φ ein A -Algebrahomomorphismus ist. Man nennt φ den zu $\bar{\varphi} = (\varphi_1, \dots, \varphi_m)$ gehörigen *Substitutionshomomorphismus* (oder Einsetzungshomomorphismus).

Das Bild von φ ist ein Unterring von $A[[x]]$, den wir mit $A[[\varphi_1, \dots, \varphi_m]]$ bezeichnen. Nach Definition von φ ist

$$\begin{aligned} \varphi(y_j) &= \varphi_j, \quad \text{für } j = 1, \dots, m, \\ \varphi(f(y_1, \dots, y_m)) &= f(\varphi_1, \dots, \varphi_m). \end{aligned}$$

Wenn $\varphi_j = 0$ für alle j , dann ist $\varphi(f) = f(0, \dots, 0) = f_0$, der *konstante Term* von f (d.h., wir können φ als einen Homomorphismus $\varphi: A[[y]] \rightarrow A$ interpretieren). Aus $\text{ord}(f) \geq q$ folgt $\text{ord}(f(\varphi_1, \dots, \varphi_m)) \geq q$, damit ist φ stetig. Offensichtlich ist die Komposition zweier Substitutionshomomorphismen wieder ein solcher.

SATZ A.9. *Wenn $\psi: A[[y]] \rightarrow A[[x]]$ ein stetiger A -Algebrahomomorphismus ist, dann ist $\text{ord}(\psi(y_j)) \geq 1$ und ψ der zu $(\psi(y_1), \dots, \psi(y_m))$ gehörige Substitutionshomomorphismus.*

Beweis. Aus der Stetigkeit von ψ folgt $\text{ord}(\psi(y_j)) \geq 1$. Sei φ der zu $(\psi(y_1), \dots, \psi(y_m))$ gehörige Substitutionshomomorphismus. Dann stimmen φ und ψ auf $A[[y]]$ überein. Da beide Abbildungen stetig sind, auf einer dichten Teilmenge übereinstimmen und $A[[x]]$ Hausdorffsch ist, sind sie gleich. \square

Wir können also einen stetigen A -Algebrahomomorphismus $\varphi: A[[y]] \rightarrow A[[x]]$ mit dem zu

$$\bar{\varphi} = (\varphi_1, \dots, \varphi_m) \in (\mathfrak{m})A[[x]]^m, \quad \text{mit } \varphi_j = \varphi(y_j) \text{ für } j = 1, \dots, m,$$

gehörigen Substitutionshomomorphismus identifizieren. Wenn wir in Zukunft schreiben “sei $\varphi: A[[y]] \rightarrow A[[x]]$ der zu $\bar{\varphi} = (\varphi_1, \dots, \varphi_m)$ gehörige Substitutionshomomorphismus”, dann nehmen wir stillschweigend $\text{ord } \varphi_j \geq 1$ für $j = 1, \dots, m$ an.

A.1.4 PARTIELLE ABLEITUNG Im folgenden werden wir erläutern, wie man die (formale) partielle Ableitung von Polynomen auf formale Potenzreihen erweitert. Sei dazu $f = \sum_{i=0}^{\infty} f_i \in A[[x]]$. Wir definieren

$$\frac{\partial f}{\partial x_j} = \partial_j f = \sum_{i=0}^{\infty} \partial_j f_i, \quad \text{für } j = 1, \dots, n,$$

wobei $\partial_j f_i$ die übliche partielle Ableitung von Polynomen ist. Die Abbildung $\partial_j: A[[x]] \rightarrow A[[x]]$, $f \mapsto \partial_j f$ ist A -linear. Aus $\text{ord}(\partial_j f) \geq \text{ord} f - 1$ folgt die Stetigkeit von ∂_j . Man beachte, daß im allgemeinen für ein homogenes Polynom g vom Grad $n > 1$ aus $g \neq 0$ nicht $\partial_j g \neq 0$ folgt. Zum Beispiel ist $\partial_j x_j^n = n x_j^{n-1} = 0$, wenn $\text{char } A \mid n$.

LEMMA A.10 (Produktregel). Für ∂_j gilt die Produktregel, d.h.,

$$\partial_j(fg) = f \partial_j g + g \partial_j f, \quad \text{für } f, g \in A[[x_1, \dots, x_n]] \text{ und } j = 1, \dots, n.$$

Beweis. Die Abbildungen $(f, g) \mapsto \partial_j(fg)$ und $(f, g) \mapsto f \partial_j g + g \partial_j f$ stimmen auf $A[x]$ überein (die Produktregel gilt für Polynome), damit sind sie auf ganz $A[[x]]$ gleich. \square

Durch Induktion über α folgt aus der Produktregel

$$(A.2) \quad \partial_j f^\alpha = \alpha f^{\alpha-1} \partial_j f, \quad \text{für } j = 1, \dots, n \text{ und } \alpha \in \mathbf{N}.$$

LEMMA A.11 (Kettenregel). Sei $\varphi: A[[y]] \rightarrow A[[x]]$ der zu $\bar{\varphi} = (\varphi_1, \dots, \varphi_m)$ gehörigen Substitutionshomomorphismus. Dann gilt für jedes $f \in A[[y]]$

$$\frac{\partial}{\partial x_j} \varphi(f) = \frac{\partial}{\partial x_j} f(\varphi_1, \dots, \varphi_m) = \sum_{k=1}^m \varphi \left(\frac{\partial f}{\partial y_k} \right) \frac{\partial \varphi_k}{\partial x_j}, \quad \text{für } j = 1, \dots, n.$$

Beweis. Sei zunächst $f = cy_1^{\alpha_1} \cdots y_m^{\alpha_m}$ mit $c \in A$. Dann gilt mit der Produktregel und (A.2)

$$\begin{aligned} \frac{\partial}{\partial x_j} \varphi(f) &= \frac{\partial}{\partial x_j} c \varphi_1^{\alpha_1} \cdots \varphi_m^{\alpha_m} \\ &= \sum_{k=1}^m c \varphi_1^{\alpha_1} \cdots \varphi_{k-1}^{\alpha_{k-1}} \alpha_k \varphi_k^{\alpha_k-1} \frac{\partial \varphi_k}{\partial x_j} \varphi_{k+1}^{\alpha_{k+1}} \cdots \varphi_m^{\alpha_m} = \sum_{k=1}^m \varphi \left(\frac{\partial f}{\partial y_k} \right) \frac{\partial \varphi_k}{\partial x_j}, \end{aligned}$$

also die Kettenregel für Monome und damit auch für Polynome. Wieder folgt aus der Dichtheit von $A[y]$ in $A[[y]]$ die Kettenregel für alle $f \in A[[y]]$. \square

Sei $f = \sum_{\alpha} c_{\alpha} x^{\alpha} \in A[[x]]$. Da $\partial_i \partial_j = \partial_j \partial_i$ für alle $i, j \in \{1, \dots, n\}$, können wir höhere partielle Ableitungen durch Iteration definieren. Es gilt wie für Polynome die Taylorformel, d.h.:

$$\begin{aligned} \alpha! c_{\alpha} &= \alpha_1! \cdots \alpha_n! c_{\alpha} = \partial_1^{\alpha_1} \cdots \partial_n^{\alpha_n} f(0) \\ \alpha &= (\alpha_1, \dots, \alpha_n) \in \mathbf{N}_0^n. \end{aligned}$$

Für die spätere Charakterisierung der Isomorphismen unter den Einsetzungshomomorphismen benötigen wir die folgende “algebraische Version” des Differentials. Sei dazu $\varphi: A[[y]] \rightarrow A[[x]]$ der zu $\bar{\varphi} = (\varphi_1, \dots, \varphi_m)$ gehörige Substitutionshomomorphismus. Seien weiters $\mathfrak{m}_y = (y_1, \dots, y_m)$ und $\mathfrak{m}_x = (x_1, \dots, x_n)$. Da $\varphi(\mathfrak{m}_y) \subseteq \mathfrak{m}_x$ und $\varphi(\mathfrak{m}_y^2) \subseteq \mathfrak{m}_x^2$, induziert φ einen A -linearen Homomorphismus

$$d\varphi: \mathfrak{m}_y/\mathfrak{m}_y^2 \rightarrow \mathfrak{m}_x/\mathfrak{m}_x^2.$$

Die Restklassen \bar{y}_j , $j = 1, \dots, m$, bzw. \bar{x}_k , $k = 1, \dots, n$, bilden eine A -Basis von $\mathfrak{m}_y/\mathfrak{m}_y^2$ bzw. $\mathfrak{m}_x/\mathfrak{m}_x^2$. Wir können also $\mathfrak{m}_y/\mathfrak{m}_y^2$ mit $M_1 = \bigoplus_{j=1}^m Ay_j$ und $\mathfrak{m}_x/\mathfrak{m}_x^2$ mit $N_1 = \bigoplus_{k=1}^n Ax_k$ identifizieren. Damit ist $d\varphi: M_1 \rightarrow N_1$, und es gilt

$$d\varphi(y_j) = \sum_{k=1}^n \frac{\partial \varphi_j}{\partial x_k}(0) x_k, \quad \text{für } j = 1, \dots, m.$$

Die zu $d\varphi$ gehörige $(n \times m)$ -Matrix bezüglich der Basen $y = (y_1, \dots, y_m)$ und $x = (x_1, \dots, x_n)$ ist also

$$\left(\frac{\partial \varphi_j}{\partial x_k}(0) \right)^T.$$

Mit der Kettenregel sieht man, daß für die Komposition $\psi \circ \varphi$ zweier Substitutionshomomorphismen $d(\psi \circ \varphi) = d\psi \circ d\varphi$ gilt.

Wenn $l: M_1 \rightarrow N_1$ eine beliebige A -lineare Abbildung ist, definieren wir den zu l gehörigen linearen Substitutionshomomorphismus φ_l durch, $\varphi_l(y_j) = l(y_j)$, $j = 1, \dots, m$. Für φ_l gilt $d\varphi_l = l$.

A.1.5 DER WEIERSTRASSSCHE VORBEREITUNGSSATZ Um die zwei nächsten Sätze formulieren zu können, benötigen wir die folgende Definition. Seien k ein Körper und $g \in R$ mit $R = k[[x_1, \dots, x_n, y]] = k[[x, y]]$. Bezeichne $g(0, y)$ das Bild des Substitutionshomomorphismus, der x_i auf 0 für $i = 1, \dots, n$ und y auf y abbildet. Eine Potenzreihe $g \in R$ heißt y -*allgemein* (auch y -regulär) der Ordnung $m \in \mathbf{N}_0$, wenn $g(0, y) \in k[[y]]$ eine Potenzreihe der Ordnung m ist, d.h.,

$$g(0, y) = \sum_{\alpha=m}^{\infty} c_{\alpha} y^{\alpha}, \quad \text{mit } c_m \neq 0.$$

Wir kommen zunächst zu einer Verallgemeinerung der Division mit Rest im Polynomring in einer Unbekannten über einem Körper für “geeignete” formale Potenzreihen.

SATZ A.12 (Divisionssatz). *Seien k ein Körper, $g \in R$, $R = k[[x, y]]$, und g y -allgemein der Ordnung m . Dann gibt es zu jedem $f \in R$ eindeutig bestimmte $q \in R$ und $r \in R'[y]$, $R' = k[[x]]$, mit $\deg r < m$ so, daß*

$$f = qg + r.$$

Beweis. Siehe z.B. [SS, S. 241]. \square

SATZ A.13 (Weierstraßscher Vorbereitungssatz). *Seien k ein Körper, $g \in R$, $R = k[[x, y]]$, und g y -allgemein der Ordnung m . Dann gibt es eine eindeutig bestimmte Einheit $u \in R$ und ein Weierstraßpolynom*

$$p = y^m + c_{m-1}y^{m-1} + \dots + c_0 \in R'[y], \quad \text{mit } R' = k[[x]],$$

so, daß

$$ug = p.$$

Die Koeffizienten c_i von p sind eindeutig bestimmt. Es gilt $\text{ord } c_i \geq 1$ für $i = 0, \dots, m-1$.

Beweis. Nach dem Divisionssatz gibt es eindeutig bestimmte $q \in R$ und $r \in R'[y]$ mit $\deg r < m$ und

$$y^m = qg + r.$$

Wenn wir jetzt in dieser Gleichung $x_i = 0$ für $i = 1, \dots, n$ setzen, erhalten wir

$$y^m = q'g' + r'.$$

Da $g' = g(0, y) = y^m u'$ mit u' invertierbar in $k[[y]]$ und $\deg r' < m$, folgt $r' = 0$ und $1 = q' u'$, d.h., q' invertierbar. Damit ist auch q invertierbar. Mit $p = y^m - r$ und $u = q$ gilt dann

$$ug = p.$$

Weiters ist $\text{ord } c_i \geq 1$ für $i = 0, \dots, m-1$, da $r(0, y) = r' = 0$. Die Eindeutigkeit folgt aus dem Divisionssatz. \square

LEMMA A.14. *Der kanonische Ringhomomorphismus*

$$\Phi: R'[y]/pR'[y] \rightarrow R/pR = R/gR, f + pR'[y] \mapsto f + pR,$$

ist ein Isomorphismus.

Beweis. Die Abbildung Φ ist wohldefiniert und $pR = gR$. Sei $\bar{f} \in R/pR$. Nach dem Divisionssatz gibt es eindeutige $q \in R$ und $r \in R'[y]$ mit $f = qp + r$. Dann ist $\Phi(\bar{r}) = \bar{r} = \overline{qp + r} = \bar{f}$ und damit ist Φ surjektiv. Sei nun $f \in R'[y]$ mit $\Phi(\bar{f}) = \bar{f} = \bar{0}$ in R/pR , d.h.,

$$f = qp + 0, \quad \text{mit } q \in R.$$

Da p als Polynom in y einen invertierbaren Leitkoeffizienten (nämlich 1) in R' hat, können wir (Polynomdivision!)

$$f = q'p + r, \quad \text{mit } q' \in R'[y] \text{ und } \deg r < m$$

schreiben. Aus der Eindeutigkeit im Divisionssatz folgt $r = 0$ und $q' = q \in R'[y]$, also $\bar{f} = \bar{0}$ in R'/pR' . Damit ist Φ injektiv. \square

A.1.6 STETIGE ISOMORPHISMEN In diesem Abschnitt werden wir die Isomorphismen unter den Einsetzungshomomorphismen charakterisieren.

LEMMA A.15. *Sei $\varphi: A[[x]] \rightarrow A[[x]]$ der zu $\bar{\varphi} = (\varphi_1, \dots, \varphi_n)$ gehörige Substitutionshomomorphismus mit $d\varphi = \text{Id}$ (d.h., die Initialform von φ_j ist x_j für $j = 1, \dots, n$). Dann ist φ ein Automorphismus.*

Beweis. Sei $f \in A[[x]]$ ungleich Null. Da φ_j die Initialform x_j für alle $j = 1, \dots, n$ besitzt, haben $\varphi(f) = f(\varphi_1, \dots, \varphi_n)$ und f die gleiche Initialform. Also ist der Kern von φ Null und φ injektiv. Weiters erkennt man damit und mit Lemma A.8, daß $A[[\varphi_1, \dots, \varphi_n]]$ dicht in $A[[x]]$ ist. Wir zeigen noch, daß $A[[\varphi_1, \dots, \varphi_n]]$ abgeschlossen ist, daraus folgt die Behauptung. Sei dazu $(\varphi(f^i))_{i \in \mathbb{N}_0}$ eine konvergente Folge in $A[[\varphi_1, \dots, \varphi_n]]$ mit $f^i \in A[[x]]$ und $\lim \varphi(f^i) = g$. Da die Ordnungen von $\varphi(f^i) - \varphi(f^j)$ und $f^i - f^j$ gleich sind, ist $(f^i)_{i \in \mathbb{N}_0}$ eine Cauchyfolge in $A[[x]]$. Sei $f = \lim f_i$. Dann folgt aus der Stetigkeit von φ $g = \varphi(f) = f(\varphi_1, \dots, \varphi_n)$, also $g \in A[[\varphi_1, \dots, \varphi_n]]$. \square

Sei φ wie im Lemma. Wir können den zu φ inversen Substitutionshomomorphismus auch induktiv konstruieren. Dazu zunächst folgendes Lemma.

LEMMA A.16. *Seien $f, \varphi_j, \psi_j \in A[[x]]$, $j = 1, \dots, n$, mit $\text{ord } \varphi_j \geq 1$ und $\text{ord } \psi_j \geq 1$. Sei φ der zu $\bar{\varphi} = (\varphi_1, \dots, \varphi_n)$ gehörige Substitutionshomomorphismus. Dann gilt*

$$\begin{aligned} f(\varphi_1 + \psi_1, \dots, \varphi_n + \psi_n) &= f(\varphi_1, \dots, \varphi_n) \\ &+ \sum_{j=1}^n (\partial_j f)(\varphi_1, \dots, \varphi_n) \psi_j + h = \varphi(f) + \sum_{j=1}^n \varphi(\partial_j f) \psi_j + h \end{aligned}$$

mit $\text{ord } h \geq 2q$ (d.h., $h \in \mathfrak{m}^{2q}$), wenn $\text{ord } \psi_j \geq q$ für $j = 1, \dots, n$.

Beweis. Wir betrachten die stetige Abbildung

$$f \mapsto f(\varphi_1 + \psi_1, \dots, \varphi_n + \psi_n) - \varphi(f) + \sum_{j=1}^n \varphi(\partial_j f) \psi_j$$

von $A[[x]]$ in sich selbst. Es genügt zu zeigen, daß das Bild von $A[x]$ in \mathfrak{m}^{2q} liegt, wenn $\psi_j \in \mathfrak{m}^q$ für $j = 1, \dots, n$. Da $A[x]$ in $A[[x]]$ dicht und \mathfrak{m}^{2q} abgeschlossen sind, folgt damit die Behauptung. Sei dazu zunächst $f = x^\alpha$. Dann ist

$$\begin{aligned} f(\varphi_1 + \psi_1, \dots, \varphi_n + \psi_n) &= (\varphi_1 + \psi_1)^{\alpha_1} \cdots (\varphi_n + \psi_n)^{\alpha_n} \\ &= \varphi_1^{\alpha_1} \cdots \varphi_n^{\alpha_n} + \sum_{j=1}^n \alpha_j \varphi_1^{\alpha_1} \cdots \varphi_{j-1}^{\alpha_{j-1}} \varphi_j^{\alpha_j-1} \varphi_{j+1}^{\alpha_{j+1}} \cdots \varphi_n^{\alpha_n} \psi_j \\ &+ \sum_{\substack{0 \leq j_i \leq \alpha_i \\ |j| \geq 2}} c_j \varphi_1^{\alpha_1} \psi_1^{\alpha_1-j_1} \cdots \varphi_n^{\alpha_n} \psi_n^{\alpha_n-j_n}, \quad \text{mit } c_j = c_{j_1 \dots j_n} \in A. \end{aligned}$$

Also gilt die Behauptung für Monome und damit für $A[x]$. \square

Sei φ wieder wie in Lemma A.15. Wir suchen einen Substitutionshomomorphismus ψ mit $\psi \circ \varphi = \text{Id}$. Dazu schreiben wir $\varphi_j = x_j + h_j$ mit $\text{ord } h_j \geq 2$ für $j = 1, \dots, n$. Wir möchten g_j mit $\text{ord } g_j \geq 2$, mit $\psi_j = x_j + g_j$ finden so, daß

$$\begin{aligned} x_j &= (\psi \circ \varphi)(x_j) = \psi(x_j + h_j) = x_j + g_j + \psi(h_j) \\ &= x_j + g_j + h_j(x_1 + g_1, \dots, x_n + g_n), \quad \text{für } j = 1, \dots, n. \end{aligned}$$

Seien $g = (g_1, \dots, g_n)$, $h = (h_1, \dots, h_n)$ und $x = (x_1, \dots, x_n)$, dann lautet die obige Gleichung

$$x = x + g + h(x + g), \quad \text{mit } h(x + g) = (h_1(x + g), \dots, h_n(x + g)).$$

Anders ausgedrückt muß also g ein Fixpunkt der nach Lemma A.16 stetigen Abbildung

$$F: (\mathfrak{m}^2)A[[x]]^n \rightarrow (\mathfrak{m}^2)A[[x]]^n, \quad g \mapsto -h(x + g)$$

sein. Wir definieren rekursiv die Folge $(g^i)_{i \in \mathbb{N}_0} \subseteq (\mathfrak{m}^2)A[[x]]^n$ durch

$$g^0 = 0 \quad \text{und} \quad g^{i+1} = F(g^i) = -h(x + g^i).$$

LEMMA A.17. *Es gilt: $g^{i+1} - g^i \in (\mathfrak{m}^{i+2})A[[x]]^n$ für alle $i \in \mathbb{N}_0$.*

Beweis. Induktion über i . Für $i = 0$ ist $g^1 - g^0 = -h(x) \in (\mathfrak{m}^2)A[[x]]^n$. Sei $i \geq 1$. Dann gilt mit Lemma A.16 und der Induktionsvoraussetzung für alle j

$$\begin{aligned} g_j^{i+1} - g_j^i &= -h_j(x + g^i) + h_j(x + g^{i-1}) \\ &= -h_j(x + g^{i-1} + (g^i - g^{i-1})) + h_j(x + g^{i-1}) \\ &= \sum_{k=1}^n (\partial_k h_j)(x + g^{i-1})(g_j^i - g_j^{i-1}) + \tilde{h}_j \in \mathfrak{m}^{i+2}. \end{aligned}$$

□

Damit ist die Folge $(g^i)_{i \in \mathbb{N}_0}$ konvergent. Mit $g = \lim g^i$ gilt dann

$$-h(x + g) = F(g) = F(\lim g^i) = \lim F(g^i) = \lim g^{i+1} = g.$$

SATZ A.18. *Sei $\varphi: A[[y]] \rightarrow A[[x]]$ ein Substitutionshomomorphismus. Dann ist φ genau dann ein Isomorphismus, wenn $d\varphi$ ein Isomorphismus ist.*

Beweis. Wenn φ ein Isomorphismus ist, dann ist $\text{Id} = d(\varphi \circ \varphi^{-1}) = d\varphi \circ d\varphi^{-1}$ und $\text{Id} = d(\varphi^{-1} \circ \varphi) = d\varphi^{-1} \circ d\varphi$, also ist auch $d\varphi$ ein Isomorphismus. Sei umgekehrt $l = d\varphi$ ein Isomorphismus. Dann ist φ_l (der zu l gehörige lineare Substitutionshomomorphismus) ein Isomorphismus (mit $\varphi_l^{-1} = \varphi_{l^{-1}}$). Mit $\tilde{\varphi} = \varphi_{l^{-1}} \circ \varphi$ genügt es also zu zeigen, daß $\tilde{\varphi}: A[[y]] \rightarrow A[[y]]$ ein Isomorphismus ist. Da aber $d\tilde{\varphi} = d(\varphi_{l^{-1}} \circ \varphi) = \text{Id}$ folgt mit Lemma A.15 die Behauptung. □

Zum Schluß dieses Abschnittes beweisen wir noch einen Satz über Automorphismen, den wir im folgenden benötigen.

SATZ A.19. *Seien k ein Körper und $f \in k[[x]]$ ungleich 0. Dann gibt es einen Substitutionsautomorphismus $\varphi: k[[x]] \rightarrow k[[x]]$ mit*

$$\bar{\varphi} = (x_1 + x_n^{m_1}, \dots, x_{n-1} + x_n^{m_{n-1}}, x_n),$$

$m_i \geq 1$ für $i = 1, \dots, n-1$ so, daß $\varphi(f)$ x_n -allgemein ist.

Wenn k unendlich ist, dann gibt es einen linearen Substitutionsautomorphismus φ mit

$$\bar{\varphi} = (x_1 + a_1 x_n, \dots, x_{n-1} + a_{n-1} x_n, x_n),$$

$a_i \in k$ für $i = 1, \dots, n-1$ so, daß $\varphi(f)$ x_n -allgemein der Ordnung $\text{ord} f$ ist.

Beweis. Zunächst der Fall für k unendlich. Seien φ ein linearer Substitutionsautomorphismus wie oben $f \in k[[x]]$ und

$$f = \sum_{i=0}^{\infty} f_i = \sum_{\alpha} c_{\alpha} x_1^{\alpha_1} \cdots x_n^{\alpha_n}, \quad \text{mit } c_{\alpha} \in A, \alpha \in \mathbf{N}_0^n.$$

Dann ist

$$\varphi(f)(0, x_n) = \sum_{i=0}^{\infty} x_n^i f_i(a_1, \dots, a_{n-1}, 1).$$

Da f_q mit $q = \text{ord} f$ ein homogenes Polynom vom Grad q ungleich Null und k unendlich sind, gibt es $a_i \in k$, $i = 1, \dots, n-1$ mit $f_q(a_1, \dots, a_{n-1}, 1) \neq 0$. Für diese a_i ist dann $\varphi(f)$ x_n -allgemein der Ordnung q .

Sei nun k beliebig. Mit $>_{\text{lex}}$ bezeichnen wir die lexikographische Ordnung auf \mathbf{N}_0^n mit $\alpha_1 > \cdots > \alpha_n$. Sei

$$\beta = \min_{>_{\text{lex}}} \{ \alpha \in \mathbf{N}_0^n \text{ mit } c_{\alpha} \neq 0 \}.$$

Wir wählen nun $m_i \in \mathbf{N}_0$ so, daß

$$m_i > \beta_n + \sum_{j=i+1}^{n-1} \beta_j m_j, \quad \text{für } i = n-1, \dots, 1.$$

Setze $q = \beta_n + \sum_{j=1}^{n-1} \beta_j m_j$.

(A.3) Dann ist $\beta \geq_{\text{lex}} \alpha$, für $\alpha \in \mathbf{N}_0^n$ mit $\alpha_n + \sum_{j=1}^{n-1} \alpha_j m_j = q$.

Für die so gewählten m_i und das zugehörige φ wie im Satz ist dann

$$\varphi(f)(0, x_n) = \sum_a c_a x_n^{\alpha_1 m_1} \cdots x_n^{\alpha_{n-1} m_{n-1}} x_n^{\alpha_n} \neq 0,$$

da sich der Term $c_\beta x_n^{\beta_1 m_1} \cdots x_n^{\beta_{n-1} m_{n-1}} x_n^{\beta_n} = c_\beta x_n^q \neq 0$ nach Wahl von β und (A.3) nicht wegheben kann.

Zu (A.3): Indirekt. Seien $\alpha >_{lex} \beta$ und k so, daß $\alpha_i = \beta_i$ für $i < k$ und $\alpha_k > \beta_k$. Dann ist

$$\begin{aligned} 0 &= \sum_{j=1}^{n-1} \alpha_j m_j + \alpha_n - \sum_{j=1}^{n-1} \beta_j m_j - \beta_n \\ &= (\alpha_k - \beta_k) m_k + \sum_{j=k+1}^{n-1} (\alpha_j - \beta_j) m_j + \alpha_n - \beta_n \geq m_k - \sum_{j=k+1}^{n-1} \beta_j m_j - \beta_n > 0. \end{aligned}$$

Widerspruch. \square

A.1.7 POTENZREIHENRINGE ÜBER k SIND FAKTORIELL

SATZ A.20. *Sei k ein Körper. Dann ist $k[[x_1, \dots, x_n]]$ faktoriell.*

Beweis. Induktion über n . Der Fall $n = 1$ ist trivial, da wir jede Potenzreihe $f \in k[[x_1]]$ schreiben können als $f = x_1^{\text{ord} f} u$ mit u invertierbar.

Seien also $f \in k[[x]] = R$, f nicht invertierbar, und $k[[x_1, \dots, x_{n-1}]] = R'$ faktoriell. Nach dem Satz A.19 gibt es einen Automorphismus φ so, daß $\varphi(f)$ x_n -allgemein ist. Es genügt also zu zeigen, daß $\varphi(f)$ ein Produkt von Primelementen ist. Da $\varphi(f)$ nach dem Weierstraßschen Vorbereitungssatz assoziiert zu einem Weierstraßpolynom ist, können wir o.B.d.A. annehmen, daß

$$f = x_n^m + c_{m-1} x_n^{m-1} + \cdots + c_0 \in R'[x_n]$$

mit $m \geq 1$ und $\text{ord} c_i \geq 1$ für $i = 0, \dots, m-1$. Der Polynomring $R'[x_n]$ in x_n ist nach einem Satz von Gauß faktoriell, da R' faktoriell ist. Also ist

$$f = p_1 \cdots p_k, \quad \text{mit } p_i \text{ prim in } R'[x_n].$$

Die p_i können wir o.B.d.A. normiert annehmen, da f normiert ist.

Wir zeigen noch, daß diese p_i prim in R sind. Wenn wir in der obigen Gleichung $x_j = 0$ für $j = 1, \dots, n-1$ und $x_n = x_n$ einsetzen, erhalten wir $f' = x_n^m = p'_1 \cdots p'_k$. Damit sind auch die p_i Weierstraßpolynome. Mit Lemma A.14 folgt dann, daß $R'[x_n]/p_i R'[x_n] \cong R/p_i R$. Also sind die p_i , $i = 1, \dots, k$, auch Primelemente in R . \square

A.1.8 IDEALE IM POLYNOM- UND POTENZREIHENRING Seien k ein Körper und $k[x] = k[x_1, \dots, x_n]$ der Polynomring in n Variablen. Sei $\mathfrak{a} \subset k[x]$ ein Ideal. Bezeichne $\widehat{\mathfrak{a}}$ das von \mathfrak{a} erzeugte Ideal im Potenzreihenring $k[[x]]$ (die Erweiterung von \mathfrak{a}). Dabei fassen wir $k[x]$ als Unterring von $k[[x]]$ auf. Wir untersuchen in diesem Abschnitt, welche Beziehung zwischen dem Ideal $\widehat{\mathfrak{a}}$ und dessen Kontraktion (dem Zusammenziehen), also $\widehat{\mathfrak{a}} \cap k[x]$, besteht. Mit den Ergebnissen läßt sich leicht herleiten, wann ein Polynom ein anderes Polynom im Potenzreihenring teilt. Weiters beweisen wir noch, daß zwei teilerfremde Polynome auch als Potenzreihen teilerfremd sind. Da wir dazu vom Polynomring zunächst zur Lokalisierung des Polynomrings im (maximalen) Ideal $\mathfrak{m} = (x_1, \dots, x_n)$ übergehen, beginnen wir mit einigen Tatsachen über die Quotientenringbildung.

Seien A ein kommutativer Ring und $S \subset A$ eine multiplikative Menge (d.h., $1 \in S$ und aus $s, t \in S$ folgt $st \in S$). Bezeichne $S^{-1}A$ den Quotientenring von A nach S . Sei f die Abbildung

$$f: A \rightarrow S^{-1}A, \quad a \mapsto \frac{a}{1}.$$

(f ist genau dann injektiv, wenn S aus lauter Nichtnullteilern besteht.) Sei $\mathfrak{a} \subset A$ ein Ideal. Dann ist das von $f(\mathfrak{a})$ erzeugte Ideal in $S^{-1}A$ die Menge

$$\left\{ \frac{a}{s} \text{ mit } a \in \mathfrak{a} \text{ und } s \in S \right\}$$

(auf gemeinsamen Nenner bringen). Wir bezeichnen dieses Ideal mit $S^{-1}\mathfrak{a}$.

LEMMA A.21. *Seien $\mathfrak{a}, \mathfrak{b} \subset A$ Ideale und $\mathfrak{p} \subset A$ ein Primideal. Dann gilt:*

- (i) *Wenn $\mathfrak{a} \cap S \neq \emptyset$, dann ist $S^{-1}\mathfrak{a} = S^{-1}A$.*
- (ii) *$S^{-1}(\mathfrak{a} \cap \mathfrak{b}) = S^{-1}\mathfrak{a} \cap S^{-1}\mathfrak{b}$.*
- (iii) *Wenn $\mathfrak{p} \cap S = \emptyset$, dann ist $S^{-1}\mathfrak{p}$ ein Primideal von $S^{-1}A$.*

Beweis. Zu (i): Sei $a \in S \cap \mathfrak{a}$. Dann ist $a/1 \in S^{-1}\mathfrak{a}$ invertierbar. Also folgt die Behauptung.

Zu (ii): Sei $a/s = b/t \in S^{-1}\mathfrak{a} \cap S^{-1}\mathfrak{b}$ mit $a \in \mathfrak{a}$, $b \in \mathfrak{b}$ und $s, t \in S$. Dann gibt es ein $u \in S$ mit $u(ta - sb) = 0$. Damit sind $c = uta = usb \in \mathfrak{a} \cap \mathfrak{b}$ und $a/s = c/stu \in S^{-1}(\mathfrak{a} \cap \mathfrak{b})$. Die umgekehrte Inklusion ist offensichtlich.

Zu (iii): Sei

$$\frac{a}{s} = \frac{b}{t} = \frac{p}{u} \in S^{-1}\mathfrak{p}$$

mit $p \in \mathfrak{p}$. Dann gibt es ein $v \in S$ mit $vuab = vstp \in \mathfrak{p}$. Da nach Voraussetzung $v, u \notin \mathfrak{p}$ sind, folgt $a \in \mathfrak{p}$ oder $b \in \mathfrak{p}$. Also ist $a/s \in S^{-1}\mathfrak{p}$ oder $b/t \in S^{-1}\mathfrak{p}$. \square

LEMMA A.22. Sei $\mathfrak{q} \subset A$ ein Primärideal (d.h., aus $ab \in \mathfrak{q}$ und $a \notin \mathfrak{q}$ folgt $b^n \in \mathfrak{q}$ für ein $n \in \mathbf{N}$) Dann gilt:

- (i) Wenn $S \cap \mathfrak{q} \neq \emptyset$, dann ist $f^{-1}(S^{-1}\mathfrak{q}) = A$.
- (ii) Wenn $S \cap \mathfrak{q} = \emptyset$, dann ist $f^{-1}(S^{-1}\mathfrak{q}) = \mathfrak{q}$.

Beweis. Zu (i): klar.

Zu (ii): Sei $a \in f^{-1}(S^{-1}\mathfrak{q})$, also $a/1 = q/s$ mit $q \in \mathfrak{q}$. Dann gibt es ein $t \in S$ mit

$$tsa = tq \in \mathfrak{q}.$$

Angenommen $a \notin \mathfrak{q}$. Dann ist aber $u = t^n s^n \in \mathfrak{q}$ für ein $n \in \mathbf{N}$ und $u \in S$. Widerspruch. \square

LEMMA A.23. Seien A ein faktorieller Ring und $S \subset A \setminus \{0\}$. Seien $a, b \in A$ und $p \in A$ prim. Dann gilt:

- (i) $a/1 \in S^{-1}A$ ist genau dann invertierbar, wenn $(a) \cap S \neq \emptyset$.
- (ii) Wenn $(p) \cap S = \emptyset$, dann ist $p/1 \in S^{-1}A$ prim.
- (iii) $S^{-1}A$ ist ein faktorieller Ring.
- (iv) Wenn a und b teilerfremd in A und keine Einheiten in $S^{-1}A$ sind, dann sind sie auch teilerfremd in $S^{-1}A$.

Beweis. Zu (i): Sei $b/s \in S^{-1}A$ mit $(b/s)(a/1) = 1/1$. Dann ist $ba = s$, und damit ist $(a) \cap S \neq \emptyset$. Sei umgekehrt $(a) \cap S \neq \emptyset$. Dann gibt es ein $b \in A$ und ein $s \in S$ so, daß $ba = s$. Damit ist $(b/s)(a/1) = 1/1$.

Zu (ii): Wenn $(p) \cap S = \emptyset$, dann ist nach Lemma A.21 (iii) $S^{-1}(p) = (p/1)$ ein Primideal von $S^{-1}A$. Also ist $p/1$ prim.

Zu (iii): Offensichtlich ist $S^{-1}A$ wieder ein Integritätsbereich. Seien $a/s \in S^{-1}A$ und $a = up_1^{b_1} \cdots p_r^{b_r}$ die Primfaktorzerlegung von a in A (d.h., die p_i 's sind prim und paarweise nicht-assoziert, und u ist eine Einheit). Dann ist nach (i) und (ii)

$$\frac{a}{s} = u' \prod_i \frac{p_i^{b_i}}{1}, \quad \text{mit } (p_i) \cap S = \emptyset$$

die Primfaktorzerlegung von a/s in $S^{-1}A$.

Zu (iv): Klar mit der vorherigen Gleichung. \square

Sei im folgenden $S = k[x] \setminus \mathfrak{m}$ mit $\mathfrak{m} = (x_1, \dots, x_n)$ (S ist multiplikativ). Bezeichne $k[x]_{\mathfrak{m}} = S^{-1}k[x]$ die Lokalisierung von $k[x]$ in \mathfrak{m} . Dann ist $k[x]_{\mathfrak{m}}$ ein lokaler, noetherscher Ring mit maximalem Ideal $S^{-1}\mathfrak{m}$, das wir wieder mit \mathfrak{m} bezeichnen. Da $k[x]$ ein Integritätsbereich ist, ist die obige Abbildung f

injektiv und damit $k[x] \subset k[x]_{\mathfrak{m}}$. Die Elemente von S haben Ordnung Null und sind deshalb als Potenzreihen nach Satz A.2 invertierbar. Wir können daher den Ring $k[x]_{\mathfrak{m}}$ in den Potenzreihenring $k[[x]]$ durch die wohldefinierte und injektive Abbildung

$$k[x]_{\mathfrak{m}} \rightarrow k[[x]], \frac{f}{g} \mapsto fg^{-1}$$

einbetten. Also haben wir folgende Inklusion von Ringen

$$k[x] \subset k[x]_{\mathfrak{m}} \subset k[[x]].$$

Der Potenzreihenring $k[[x]]$ ist nach Korollar A.3 und Satz A.4 ein lokaler, noetherscher Ring. Nach Satz A.20 ist $k[[x]]$ außerdem ein faktorieller Ring.

Sei $\mathfrak{c} \subset k[x]_{\mathfrak{m}}$ ein Ideal, und bezeichne $\widehat{\mathfrak{c}}$ die Erweiterung des Ideals \mathfrak{c} in $k[[x]]$. Für das maximale Ideal $\mathfrak{m} \subset k[x]_{\mathfrak{m}}$ ist $\widehat{\mathfrak{m}}$ das maximale Ideal von $k[[x]]$. Weiters gilt

$$\widehat{\mathfrak{m}}^n \cap k[x]_{\mathfrak{m}} = \mathfrak{m}^n, \quad \text{für } n \in \mathbf{N}.$$

Der nächste Satz gibt Auskunft über die Beziehungen zwischen beliebigen Idealen von $k[x]_{\mathfrak{m}}$ und $k[[x]]$. Für den Beweis brauchen wir folgende Behauptungen.

LEMMA A.24 (Lemma von Nakayama). *Seien A ein kommutativer Ring und $\mathfrak{a} \subset A$ ein Ideal so, daß jedes Element von $1 + \mathfrak{a}$ invertierbar ist. Sei M ein endlicher A -Modul mit $\mathfrak{a}M = M$ ($\mathfrak{a}M$ bezeichnet den von allen am mit $a \in \mathfrak{a}$ und $m \in M$ erzeugten Untermodul von M). Dann ist $M = 0$.*

Beweis. Sei m_1, \dots, m_n ein Erzeugendensystem von M mit minimalem n . Angenommen $M \neq 0$, dann ist $n \geq 1$. Da $\mathfrak{a}M = M$ ist, gibt es $a_1, \dots, a_n \in \mathfrak{a}$ mit $m_1 = a_1 m_1 + \dots + a_n m_n$. Also ist

$$(1 - a_1)m_1 = a_2 m_2 + \dots + a_n m_n.$$

Nach Voraussetzung ist aber $1 - a_1$ invertierbar. Für $n = 1$ folgt daraus $m_1 = 0$, also $M = 0$. Wenn $n \geq 2$ ist, dann ist damit bereits m_2, \dots, m_n ein Erzeugendensystem von M , also ein Widerspruch zur Minimalität von n . \square

LEMMA A.25. *Seien A ein noetherscher Ring, $\mathfrak{a} \subset A$ ein Ideal so, daß jedes Element von $1 + \mathfrak{a}$ invertierbar ist. Dann ist $\bigcap_{n>0} (\mathfrak{b} + \mathfrak{a}^n) = \mathfrak{b}$ für jedes Ideal $\mathfrak{b} \subset A$.*

Beweis. Sei $p: A \rightarrow A/\mathfrak{b}$ die kanonische Abbildung. Wenn wir nun das Lemma von Nakayama auf den endlichen (da A noethersch ist) A -Modul $M = \bigcap_{n>0} p(\mathfrak{a}^n)$ anwenden, folgt $M = 0$. Damit ist

$$\mathfrak{b} = p^{-1}(0) = p^{-1}\left(\bigcap_{n>0} p(\mathfrak{a}^n)\right) = \bigcap_{n>0} p^{-1}p(\mathfrak{a}^n) = \bigcap_{n>0} \mathfrak{b} + \mathfrak{a}^n.$$

□

LEMMA A.26. *Sei A ein lokaler Ring mit maximalem Ideal \mathfrak{m} . Dann ist jedes Element von $A \setminus \mathfrak{m}$ eine Einheit. Insbesondere ist jedes Element von $1 + \mathfrak{m}$ invertierbar.*

Beweis. Angenommen es gibt ein $a \in A \setminus \mathfrak{m}$, das nicht invertierbar ist. Dann ist a nach dem Lemma von Zorn in einem maximalen Ideal enthalten. Da A nur das maximale Ideal \mathfrak{m} besitzt, folgt $a \in \mathfrak{m}$. Widerspruch. Sei $m \in \mathfrak{m}$. Dann ist $1 + m \in A \setminus \mathfrak{m}$, sonst wäre $1 \in \mathfrak{m}$. □

SATZ A.27. *Seien $\mathfrak{c} \subset k[x]_{\mathfrak{m}}$ Ideale. Dann ist $\widehat{\mathfrak{c}} \cap k[x]_{\mathfrak{m}} = \mathfrak{c}$.*

Beweis. Es genügt die Inklusion $\widehat{\mathfrak{c}} \cap k[x]_{\mathfrak{m}} \subset \mathfrak{c}$ zu zeigen. Sei $\mathfrak{c} = (c_1, \dots, c_m)$ ein Erzeugendensystem von \mathfrak{c} . Sei $c \in \widehat{\mathfrak{c}} \cap k[x]_{\mathfrak{m}}$. Dann ist $c = \sum c_i \gamma_i$ mit $\gamma_i \in k[[x]]$. Sei $n \in \mathbf{N}$. Wir können γ_i schreiben als

$$\gamma_i = d_i + \delta_i, \quad \text{mit } d_i \in k[x] \subset k[x]_{\mathfrak{m}} \quad \text{und} \quad \delta_i \in \widehat{\mathfrak{m}}^n.$$

Mit $d = \sum c_i d_i \in \mathfrak{c}$ ist dann

$$c - d \in \widehat{\mathfrak{m}}^n \cap k[x]_{\mathfrak{m}} = \mathfrak{m}^n.$$

Also ist

$$c \in \bigcap_{n>0} (\mathfrak{c} + \mathfrak{m}^n) = \mathfrak{c},$$

wobei das letzte Gleichheitszeichen aus den zwei vorherigen Lemmata folgt. □

KOROLLAR A.28. *Seien $c, d \in k[x]_{\mathfrak{m}}$. Aus $c \mid d$ in $k[[x]]$ folgt $c \mid d$ in $k[x]_{\mathfrak{m}}$.*

Beweis. Aus $c \mid d$ in $k[[x]]$ folgt mit dem vorherigen Satz

$$d \in (\widehat{\mathfrak{c}}) \cap k[x]_{\mathfrak{m}} = (c).$$

Also $c \mid d$ in $k[x]_{\mathfrak{m}}$. □

Sei $\mathfrak{a} \subset k[x]$ ein Ideal. Dann ist

$$\widehat{S^{-1}\mathfrak{a}} = \widehat{\mathfrak{a}}.$$

LEMMA A.29. Seien $f \in k[x]$ und $f = cf_1^{b_1} \cdots f_r^{b_r}$ die Primfaktorzerlegung von f . Dann ist $\widehat{(f)} \cap k[x] = (h)$ mit $h = \prod_i f_i^{b_i}$ mit $f_i \in \mathfrak{m}$.

Beweis. Jedes Ideal $(f_i^{b_i})$ ist ein Primärideal. Das folgende Lemma zeigt, daß

$$(f_1^{b_1}) \cap \cdots \cap (f_r^{b_r}) = (f).$$

Dann ist mit Satz A.27

$$\widehat{(f)} \cap k[x] = \widehat{(S^{-1}(f) \cap k[x]_{\mathfrak{m}})} \cap k[x] = S^{-1}(f) \cap k[x].$$

Mit Lemma A.21 (ii) und Lemma A.22 folgt weiter

$$\begin{aligned} S^{-1}(f) \cap k[x] &= S^{-1}((f_1^{b_1}) \cap \cdots \cap (f_r^{b_r})) \cap k[x] \\ &= (S^{-1}(f_1^{b_1}) \cap k[x]) \cap \cdots \cap (S^{-1}(f_r^{b_r}) \cap k[x]) = (h). \end{aligned}$$

□

LEMMA A.30. Sei A ein faktorieller Ring. Seien $a_1, \dots, a_r \in A$ und $v = \text{kgV}(a_1, \dots, a_r)$. Dann ist

$$(a_1) \cap \cdots \cap (a_r) = (v).$$

Beweis. Wir zeigen, daß für $a, b \in A$ und $v = \text{kgV}(a, b)$

$$(a) \cap (b) = (v)$$

gilt. Die Behauptung folgt dann durch Induktion über r . Da v ein Vielfaches von a und b ist, folgt $(a) \cap (b) \supset (v)$. Sei umgekehrt $c \in (a) \cap (b)$. Dann ist c ein gemeinsames Vielfaches von a und b und damit, nach Definition von v , auch ein Vielfaches von v . Also ist $(a) \cap (b) \subset (v)$. □

Wenn man jetzt die Existenz einer Primärzerlegung eines Ideals $\mathfrak{a} \subset k[x]$ (d.h., \mathfrak{a} läßt sich als Durchschnitt endlich vieler Primärideale schreiben) benützt, kann man analog zu Lemma A.29 herleiten, wie die Kontraktion eines beliebigen Ideals aussieht.

LEMMA A.31. Seien $f, g \in k[x]$ und $f = cf_1^{b_1} \cdots f_r^{b_r}$ die Primfaktorzerlegung von f . Sei $h = \prod_i f_i^{b_i}$ mit $f_i \in \mathfrak{m}$ und gelte $f \mid g$ in $k[[x]]$. Dann $h \mid g$ in $k[x]$.

Beweis. Aus $f \mid g$ in $k[[x]]$ folgt mit Lemma A.29

$$g \in (f) \cap k[x] = (h).$$

Also $h \mid g$ in $k[x]$. \square

SATZ A.32. *Seien $c, d \in k[x]_{\mathfrak{m}}$. Wenn c und d teilerfremd in $k[x]_{\mathfrak{m}}$ sind, dann sind sie auch teilerfremd in $k[[x]]$.*

Beweis. Angenommen c und d sind nicht teilerfremd in $k[[x]]$. Sei α ein größter gemeinsamer Teiler von c und d in $k[[x]]$ (α ist nach Annahme ein echter Teiler von c bzw. d). Dann können wir c und d schreiben als $c = \alpha\gamma$ und $d = \alpha\delta$ mit $\gamma, \delta \in k[[x]]$ teilerfremd. Also ist $c\delta - d\gamma = 0$. Für $n \in \mathbf{N}$ zerlegen wir γ und δ in $\gamma = s_n + \sigma_n$ und $\delta = t_n + \tau_n$ mit $s_n, t_n \in k[x] \subset k[x]_{\mathfrak{m}}$ und $\sigma_n, \tau_n \in \widehat{\mathfrak{m}}^n$. Dann ist

$$ct_n - ds_n \in (\widehat{c, d})\mathfrak{m}^n \cap k[x]_{\mathfrak{m}} = (c, d)\mathfrak{m}^n,$$

wobei das letzte Gleichheitszeichen mit Satz A.27 folgt. Daher gibt es $u_n, v_n \in \mathfrak{m}^n$ so, daß $ct_n - ds_n = cv_n + du_n$. Also ist

$$c(t_n - v_n) = d(s_n + u_n),$$

und damit (kürzen)

$$\gamma(t_n - v_n) = \delta(s_n + u_n).$$

Da γ und δ teilerfremd in $k[[x]]$ sind, ist $(s_n + u_n)$ durch γ in $k[[x]]$ teilbar, d.h.,

$$(s_n + u_n) = \lambda\gamma, \quad \text{mit } \lambda \in k[[x]].$$

Sei $n = \text{ord } \gamma + 1$. Dann ist $\text{ord}(s_n + u_n) = \text{ord } \gamma$ (weil $\gamma = s_n + \sigma_n$ und $u_n \in \mathfrak{m}^n$). Also ist $\text{ord } \lambda = 0$, d.h., λ ist invertierbar. Daher $(s_n + u_n) \mid \gamma$ in $k[[x]]$. Da γ ein Teiler von c in $k[[x]]$ ist, folgt daraus mit Korollar A.28, daß $(s_n + u_n) \mid c$ in $k[x]_{\mathfrak{m}}$, d.h.,

$$c = e(s_n + u_n), \quad \text{mit } e \in k[x]_{\mathfrak{m}}.$$

Aber $c(t_n - v_n) = d(s_n + u_n)$, und deshalb ist (kürzen) $e(t_n - v_n) = d$. Weil c und d teilerfremd in $k[x]_{\mathfrak{m}}$, ist e invertierbar in $k[x]_{\mathfrak{m}}$. Damit ist

$$(c) = (s_n + u_n) = (\gamma), \quad \text{in } k[[x]].$$

Dann kann aber α kein echter Teiler von γ in $k[[x]]$ sein. Widerspruch. \square

KOROLLAR A.33. *Seien $f, g \in k[x]$ und $f, g \in \mathfrak{m}$. Wenn f und g teilerfremd in $k[x]$ sind, dann sind sie auch teilerfremd in $k[[x]]$.*

Beweis. Klar mit dem vorherigen Satz und Lemma A.23 (iv). \square

A.2 GAUSS-BRUHAT ZERLEGUNG

Sei k ein Körper. Bezeichne im folgenden R den formalen Potenzreihenring in zwei Variablen über k und $G = \mathbf{Aut}_k(R)$ die Gruppe der stetigen (=lokalen) k -Algebraautomorphismen. Eine Matrix $A \in GL_n(k)$ kann man bekanntlich zerlegen in $A = PLU$ mit U eine obere (upper) Dreiecksmatrix, L eine untere (lower) Dreiecksmatrix mit Einsen in der Hauptdiagonale und P einer Permutationsmatrix (Gaußalgorithmus mit elementaren Zeilenoperationen und Zeilenvertauschungen). Wir möchten nun analog dazu ein $\varphi \in G$ schreiben als $\varphi = plu$. Dabei sollen l und u aus geeigneten Untergruppen von G und p eine eventuelle Vertauschung der Variablen sein.

Sei $\mathbf{y} = (y, z)$ ein reguläres Parametersystem von R , d.h., das maximale Ideal \mathfrak{m} von R wird von y und z erzeugt. Wir identifizieren wieder ein $\varphi \in G$ mit dem zu

$$\bar{\varphi} = (\varphi_1, \varphi_2) \in (\mathfrak{m})R^2, \quad \text{mit } \varphi_1(y, z) = \varphi(y), \varphi_2(y, z) = \varphi(z)$$

gehörigen Substitutionshomomorphismus. Die Identität von G bezeichnen wir mit Id . Wir definieren

$$L = \{\varphi \in G \text{ mit } \varphi_1 - y \in zk[[z]] \text{ und } \varphi_2 = z\},$$

$$U = \{\varphi \in G \text{ mit } \varphi_1 - y \in yR\},$$

$$P = \{\text{Id}, p\}, \quad \text{mit } \bar{p} = (z, y).$$

Diese Definition hängt natürlich von der Wahl des regulären Parametersystems ab. Wir werden im folgenden zeigen, daß L bzw. U Untergruppen von G sind (P ist offensichtlich eine). Durch Nachrechnen sieht man, daß L und U bezüglich Komposition abgeschlossen sind. Weiters ist für $l \in L$ bzw. $u \in U$ die zu dl bzw. du gehörige Matrix bzgl. der Basis (y, z) (siehe Abschnitt A.1.4) eine unipotente untere Dreiecksmatrix bzw. eine obere Dreiecksmatrix. Der durch dl induzierte lineare Substitutionshomomorphismus bildet also y auf $y + az$ mit $a \in k$ und z auf z ab. Damit ist er wieder in L . Analog dazu ist auch der von du induzierte Substitutionshomomorphismus wieder in U .

Seien $l \in L$ mit $\bar{l} = (y + g(z), z)$ und m der zu $\bar{m} = (y - g(z), z)$ gehörige Einsetzungshomomorphismus. Dann ist

$$lm = ml = \text{Id},$$

also $l^{-1} = m \in L$. Damit ist L eine Untergruppe von G . Mit folgender Behauptung ist auch U eine Untergruppe.

LEMMA A.34. *Sei $u \in U$. Dann ist $u^{-1} \in U$.*

Beweis. Da der von du induzierte lineare Substitutionshomomorphismus wieder in U ist, können wir o.B.d.A. annehmen, daß $du = \text{Id}$. Sei also $\bar{u} = (y + h_1, z + h_2)$ mit $\text{ord}(h_i) \geq 2$, $i = 1, 2$, und $h_1 = yf(y, z)$. Nach Abschnitt A.1.6 ist $\bar{u}^{-1} = (y + g_1, z + g_2)$, wobei $g = (g_1, g_2) = \lim g^i$ mit $g^0 = 0$ und $g^{i+1} = F(g^i)$. Dabei ist

$$F: (\mathfrak{m}^2)R^2 \rightarrow (\mathfrak{m}^2)R^2, \\ (g_1, g_2) \mapsto -h(y + g_1, z + g_2), \quad \text{mit } h = (h_1, h_2).$$

Durch Induktion über i folgt, daß $g_1^i = yf^i(y, z)$ für $i \geq 1$ und damit die Behauptung. Der Fall $i = 1$ ist klar. Sei also $g_1^i = yf^i(y, z)$. Dann ist

$$g_1^{i+1} = h_1(y + g_1^i, z + g_2^i) \\ = (y + g_1^i)f(y + g_1^i, z + g_2^i) = (y + yf^i(y, z))f(y + g_1^i, z + g_2^i) \\ = yf^{i+1}(y, z).$$

□

Sei $\varphi \in G$ mit $\bar{\varphi} = (\varphi_1, \varphi_2)$. Wir schreiben

$$\varphi_1 = ay + bz + h_1, \\ \varphi_2 = cy + dz + h_2,$$

mit $a, b, c, d \in k$ und $\text{ord}(h_i) \geq 2$ für $i = 1, 2$. Die zu $d\varphi$ gehörige Matrix

$$A = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$$

ist invertierbar. Sei p die Vertauschung von y und z , d.h., $\bar{p} = (z, y)$. Die zu $d(\varphi p) = d\varphi dp$ bzw. $d(p\varphi) = dpd\varphi$ gehörige Matrix ist die Matrix A mit vertauschten Spalten bzw. Zeilen. Da A invertierbar ist, gibt es immer ein $p \in P$ so, daß $(p\varphi)_1 = (p\varphi)(y) = ay + bz + h_1$ mit $a, b \in k$, $a \neq 0$ und $\text{ord}(h_1) \geq 2$ (d.h., $(p\varphi)_1$ ist y -allgemein der Ordnung 1). Analog gibt es ein $p \in P$ mit $(\varphi p)_1 = ay + bz + h_1$ mit a, b, h_1 wie zuvor.

Für eine allgemeinere Version des folgenden Satzes in beliebiger Dimension siehe [Ha5].

SATZ A.35. *Mit den Bezeichnungen wie oben gilt*

$$G = PLU = ULP = PUL = LUP.$$

Beweis. Sei $\varphi \in G$. Wir zeigen zunächst $G = PLU$. Sei $p \in P$ so, daß $(p\varphi)_1$ y -allgemein der Ordnung 1 ist. Nach dem Weierstraßschen

Vorbereitungssatz gibt es dann ein $g \in zk[[z]]$ und eine Einheit $e \in k[[y, z]]$ so, daß

$$(p\varphi)_1 = (p\varphi)(y) = (y + g)e.$$

Sei l der zu $\bar{l} = (y + g, z)$ gehörige Substitutionshomomorphismus. Dann ist $l \in L$ und

$$\begin{aligned} (l^{-1}p\varphi)(y) &= l^{-1}((y + g(z))e(y, z)) \\ &= (y - g(z) + g(z))(e(y - g(z), z)) = ye(y - g(z), z). \end{aligned}$$

Damit ist $l^{-1}p\varphi = u \in U$ und $\varphi = p^{-1}lu$, also $G = PLU$. Durch Inversion folgt daraus $G = ULP$.

Sei nun $p \in P$ so, daß $(\varphi^{-1}p)_1$ y -allgemein der Ordnung 1 ist. Wie zuvor finden wir dann ein l so, daß $l^{-1}\varphi^{-1}p = u \in U$. Dann ist $\varphi^{-1} = lup^{-1}$ und damit $\varphi = pu^{-1}l^{-1}$, also $G = PUL$. \square

A.3 SINGULÄRE PUNKTE

Wir werden in diesem Abschnitt möglichst elementar einige Begriffe und Behauptungen der algebraischen Geometrie für den Spezialfall von Nullstellenmengen von Polynomen in zwei Variablen über einem Körper definieren bzw. herleiten.

LEMMA A.36. *Sei A ein faktorieller Ring und bezeichne k den Quotientenkörper von A . Seien $f, g \in A[x]$ teilerfremd in $A[x]$. Dann sind f und g auch teilerfremd in $k[x]$.*

Beweis. Angenommen es gibt ein $\tilde{h} \in k[x]$ mit $\deg \tilde{h} \geq 1$ so, daß

$$f = \tilde{f}\tilde{h} \text{ und } g = \tilde{g}\tilde{h}, \quad \text{mit } \tilde{f}, \tilde{g} \in k[x].$$

Sei $d \in A$ so, daß $d\tilde{f}$, $d\tilde{g}$ und $d\tilde{h}$ in $A[x]$ sind. Dann sind

$$d^2f = (d\tilde{f})(d\tilde{h}) \text{ bzw. } d^2g = (d\tilde{g})(d\tilde{h}).$$

Sei h ein irreduzibler Faktor von $d\tilde{h}$ in $A[x]$ mit $\deg h \geq 1$. Dann ist h ein irreduzibler Faktor von d^2f bzw. d^2g und damit auch von f bzw. g . Daraus folgt ein Widerspruch zur Annahme, daß f und g teilerfremd in $A[x]$ sind. \square

Sei k ein Körper. Für $f_1, \dots, f_n \in k[y, z]$ bezeichne

$$V(f_1, \dots, f_n) = \{a = (a_1, a_2) \in \mathbf{A}^2 \text{ mit } f_i(a) = 0 \text{ für } i = 1, \dots, n\}$$

die Menge der gemeinsamen Nullstellen von f_1, \dots, f_n .

LEMMA A.37. Seien k ein algebraisch abgeschlossener Körper und $f \in k[y, z] \setminus k$. Dann ist $V(f)$ eine unendliche Menge.

Beweis. Wir schreiben dazu

$$f = a_0(y) + a_1(y)z + \cdots + a_n(y)z^n \in k[y][z].$$

Wenn $n = 0$, dann ist $f(0, a_2) = 0$ für alle $a_2 \in k$. Also folgt, da k als algebraisch abgeschlossener Körper unendlich ist, die Behauptung. Andernfalls hat $a_n(y)$ nur endlich viele Nullstellen, und für jedes a_1 mit $a_n(a_1) \neq 0$ hat das Polynom $f(a_1, z) \in k[z]$ eine Nullstelle. \square

SATZ A.38. Seien k ein Körper und $f, g \in k[y, z]$ teilerfremd. Dann ist $V(f, g) = V(f) \cap V(g)$ endlich.

Beweis. Nach Lemma A.36 ist $\text{ggT}(f, g) = 1$ in $k(y)[z]$. Also gibt es r und s in $k(y)[z]$ so, daß

$$1 = rf + sg.$$

Sei $d \in k[y]$ so, daß dr und ds in $k[y, z]$ sind. Dann ist

$$d = (dr)f + (ds)g.$$

Für ein $a = (a_1, a_2) \in V(f) \cap V(g)$ ist also $d(a_1) = 0$. Damit gibt es nur endlich viele Möglichkeiten für a_1 . Ein analoges Argument zeigt, daß für a_2 auch nur endlich viele Werte in Frage kommen. \square

Sei $f \in k[y, z]$. Wir definieren die *Ordnung* von f im Nullpunkt durch

$$\text{ord}_0 f = \text{ord} f = \sup\{n \in \mathbf{N}_0 \text{ mit } f \in (y, z)^n\}.$$

Dabei sind

$$(y, z)^n = (y^{\alpha_1} z^{\alpha_2} \text{ mit } \alpha = (\alpha_1, \alpha_2) \in \mathbf{N}_0^2 \text{ und } \alpha_1 + \alpha_2 = n)$$

das n -fache Produkt des von y und z erzeugten Ideals und $(y, z)^0 = k[y, z]$. Nach Definition ist $\text{ord} f = \infty$ genau dann, wenn $f = 0$. Für einen beliebigen Punkt $a = (a_1, a_2) \in \mathbf{A}^2$ definieren wir die Ordnung von f in a durch

$$\text{ord}_a f = \text{ord}_0 \tilde{f}, \quad \text{mit } \tilde{f}(y, z) = f(y + a_1, z + a_2).$$

Es gilt

$$f(y + a_1, z + a_2) = f(a) + \partial_y f(a)y + \partial_z f(a)z + h(y, z), \quad \text{mit } \text{ord} h \geq 2.$$

Also ist $a \in V(f)$ genau dann, wenn $\text{ord}_a f \geq 1$.

Sei nun $f \in k[y, z] \setminus k$. Wir nennen einen Punkt $a \in \mathbf{A}^2$ *singulär* (oder einen *singulären Punkt* von f), wenn $\text{ord}_a f > 1$. Wenn $\text{ord}_a f = 1$, dann nennt man a ein *regulären Punkt* von f . Ein $a \in \mathbf{A}^2$ ist genau dann ein singulärer Punkt, wenn

$$a \in V(f) \cap V(\partial_y f) \cap V(\partial_z f) = V(f, \partial_y f, \partial_z f).$$

Mit

$$\text{Sing}(f) = \{a \in \mathbf{A}^2 \text{ mit } \text{ord}_a f > 1\} = V(f, \partial_y f, \partial_z f)$$

bezeichnen wir die Menge der singulären Punkte von f .

SATZ A.39. *Seien k ein algebraisch abgeschlossener Körper und $f \in k[y, z]$ irreduzibel. Dann ist die Menge $\text{Sing}(f)$ endlich.*

Beweis. Angenommen $\text{Sing}(f)$ ist eine unendliche Menge. Da f irreduzibel ist und $\deg \partial_y f < \deg f$, können f und $\partial_y f$ nach Satz A.38 aber nur dann unendlich viele gemeinsame Nullstellen haben, wenn $\partial_y f = 0$. Das Gleiche gilt für $\partial_z f$. Aber $\partial_y f = \partial_z f = 0$ impliziert $f \in k$, wenn $\text{char } k = 0$. Für $\text{char } k > 0$ folgt aus $\partial_y f = \partial_z f = 0$ wie im Beweis zu Satz 8.2 ein Widerspruch zur Irreduzibilität von f . \square

Seien $f, g \in k[y, z] \setminus k$ und $a \in V(f) \cap V(g) = V(fg)$. Dann ist a ein singulärer Punkt von fg , denn

$$\text{ord}_a fg = \text{ord}_a f + \text{ord}_a g \geq 2.$$

Also ist $\text{Sing}(f^2) = V(f)$ für ein $f \in k[y, z] \setminus k$. Für ein nicht konstantes Polynom f über einem algebraisch abgeschlossenen Körper ist die Menge $\text{Sing}(f^2)$ unendlich. Dies motiviert unter anderem folgenden Begriff, den wir gleich für einen beliebigen faktoriellen Ring definieren.

Seien A ein faktorieller Ring, $a \in A$ und

$$a = up_1^{b_1} \cdots p_r^{b_r}$$

die Primfaktorzerlegung von a mit einer Einheit u und paarweise nicht-assoziierten Primelementen p_i . Man nennt a *reduziert* (bzw. *quadratfrei*), wenn $b_i = 1$ für $i = 1, \dots, r$.

LEMMA A.40. *Seien A ein faktorieller Ring, $a \in A$ und $a = up_1^{b_1} \cdots p_r^{b_r}$ die Primfaktorzerlegung von a . Dann ist*

$$\sqrt{(a)} = (p_1 \cdots p_r).$$

Beweis. Sei $n = \max_i b_i$. Dann ist

$$u(p_1 \cdots p_r)^n = p_1^{n-b_1} \cdots p_r^{n-b_r} a,$$

also ist $(p_1 \cdots p_r) \subset \sqrt{(a)}$. Seien umgekehrt $b \in \sqrt{(a)}$ und $b = v q_1^{c_1} \cdots q_s^{c_s}$ die Primfaktorzerlegung von b . Dann gibt es ein $n \in \mathbf{N}$ so, daß $b^n = da$ mit $d \in A$. Also ist

$$v^n q_1^{nc_1} \cdots q_s^{nc_s} = d u p_1^{b_1} \cdots p_r^{b_r}.$$

Aus der Eindeutigkeit der Primfaktorzerlegung (bis auf Assoziiertheit und Reihenfolge) folgt, daß jedes p_i zu einem q_j assoziiert ist, und damit ist $g \in (p_1 \cdots p_r)$. \square

Ein Ideal \mathfrak{a} eines beliebigen kommutativen Ringes nennt man *reduziert* bzw. *Radikalideal*, wenn $\mathfrak{a} = \sqrt{\mathfrak{a}}$ gilt. In einem Integritätsbereich sind zwei Hauptideale genau dann gleich, wenn die erzeugenden zueinander assoziiert sind. Deshalb folgt mit der Eindeutigkeit der Primfaktorzerlegung (bis auf Assoziiertheit und Reihenfolge) und diesem Lemma, daß a genau dann reduziert ist, wenn das von a erzeugte Hauptideal (a) reduziert ist.

SATZ A.41. *Seien k ein algebraisch abgeschlossener Körper und $f \in k[y, z] \setminus k$ reduziert. Dann ist die Menge $\text{Sing}(f)$ endlich.*

Beweis. Sei $f = cf_1 \cdots f_r$ die Primfaktorzerlegung von f . Dann ist

$$V(cf) = V(f_1 \cdots f_r) = \bigcup_{i=1}^r V(f_i).$$

Nach Satz A.39 ist $\text{Sing}(f_i)$ endlich für $i = 1, \dots, r$. Außerdem gibt es nach Satz A.38 höchstens endlich viele Punkte $a \in V(f_1 \cdots f_r)$ mit $a \in V(f_i) \cap V(f_j)$ für zwei verschiedene $i, j \in \{1, \dots, r\}$. \square

LITERATUR

- [Ab1] ABHYANKAR, S. Desingularization of plane curves. *In: Summer Institute on Algebraic Geometry. Arcata 1981, Proc. Symp. Pure Appl. Math. 40 Amer. Math. Soc.*
- [Ab2] — Algebraic Geometry for Scientists and Engineers. *Math. Surveys and Monographs 35. Amer. Math. Soc.* 1990.
- [Ab3] — Local uniformization of algebraic surfaces over ground fields of characteristic $p \neq 0$. *Ann. Math.* 63 (1956), 491-526.
- [AM] ATIYAH, M. F. and MACDONALD I. G. *Introduction to Commutative Algebra*. Addison-Wesley, Reading, Mass., 1969.

- [AHV1] AROCA, J.-M., HIRONAKA, H. and VICENTE, J.-L. The theory of the maximal contact. *Memorias Mat. Inst. Jorge Juan Madrid* 29 (1975).
- [AHV2] ——— Desingularization theorems. *Memorias Mat. Inst. Jorge Juan Madrid* 29 (1975).
- [BK] BRIESKORN, E. and KNÖRRER, H. *Ebene algebraische Kurven*. Birkhäuser 1981. English translation: *Plane algebraic curves*. Birkhäuser 1986.
- [BM] BIERSTONE, E. and MILMAN, P. Canonical desingularization in characteristic zero by blowing up the maximum strata of a local invariant. *Invent. Math.* 128 (1998), 207-302.
- [Bo] BOSCH, S. *Algebra*. Springer-Verlag, Berlin Heidelberg New York, 1991.
- [BIV] BRÜSKE, R., ISCHEBECK, F. and VOGEL, F. *Kommutative Algebra*. BI Wissenschaftsverlag, Mannheim, Wien, Zürich, 1989.
- [Cp] CAMPILLO, A. Albegroid curves in positive characteristic. *Lecture Notes in Math.* 813, Springer-Verlag 1980.
- [Cs] CASAS, E. *Singularities of plane curves*. Cambridge Univ. Press 2000.
- [CLS] COX, D., LITTLE, J. and O'SHEA, D. *Ideals, varieties, and algorithms*. Springer-Verlag, New York, 1992.
- [EH] ENCINAS, S. and HAUSER, H. Strong resolution of singularities in characteristic zero. *Comment. Math. Helv.* 77 (2002), 421-445.
- [EV] ENCINAS, S. and VILLAMAYOR, O. Good points and constructive resolution of singularities. *Acta Math.* 181 (1998), 109-158.
- [Fu] FULTON, W. *Algebraic Curves*. Benjamin 1969.
- [GT] GOLDIN, R. and TEISSIER, B. Resolving singularities of plane analytic branches with one toric morphism. In: *Resolution of Singularities, Progress in Math.* 181. Birkhäuser 2000.
- [GR] GRAUERT, H. and REMMERT, R. *Analytische Stellenalgebren*. Springer-Verlag, Berlin Heidelberg New York, 1971.
- [Hs] HARTSHORNE, R. *Algebraic Geometry*. Springer-Verlag 1977.
- [Ha1] HAUSER, H. Resolution of singularities 1860-1999. In: *Resolution of Singularities, Progress in Math.* 181. Birkhäuser 2000.
- [Ha2] ——— The Hironaka Theorem on resolution of singularities (Or: A proof that we always wanted to understand). *Bull. Amer. Math. Soc.* 40 (2003), 323-403.
- [Ha3] ——— Seventeen obstacles for resolution of singularities. In: *Singularities, The Brieskorn Anniversary volume (ed.: V.I. Arnold, G.-M. Greuel, J. Steenbrink)*. Birkhäuser 1998.
- [Ha4] ——— Mysterious resolution in positive characteristic. *Preprint Universität Innsbruck*.
- [Ha5] ——— Three power series techniques. *Proc. London. Math. Soc.* (2003).
- [Hi] HIRONAKA, H. Resolution of singularities of an algebraic variety over a field of characteristic zero. *Ann. of Math.* 79 (1964), 109-326.
- [La] LANG, S. *Algebra. Revised third edition*. Graduate Texts in Mathematics, 211. Springer-Verlag, New York, 2002.
- [Lp] LIPMAN, J. Introduction to resolution of singularities. *Proceedings Symp. Pure Appl. Math.* 29 Amer. Math. Soc. 1975, 187-230.
- [Ma] MATSUMURA, H. *Commutative Algebra*. Benjamin, New York, 1970.

- [Mu] MUMFORD, D. The Red Book of Varieties and Schemes. *Lecture Notes in Math.* 1358, Springer-Verlag 1988.
- [Na] NAGATA, M. *Local Rings*. Robert E. Krieger Publishing Company, New York, 1975.
- [Ok] OKA, M. Geometry of plane curves via toroidal resolution. In: *Algebraic geometry and singularities, Progress in Math.* 134. Birkhäuser, Basel, 1996.
- [OO] ORZECH, G. and ORZECH, M. *Plane algebraic curves*. Marcel Dekker, New York, 1981.
- [Or] ORBANZ, U. Embedded resolution of algebraic surfaces after Abhyankar (characteristic 0). In: *Resolution of surface singularities. Lecture Notes in Math.* 1101, Springer-Verlag 1984.
- [Ru] RUIZ, J., M. *The basic theory of power series*. Vieweg, Braunschweig, 1993.
- [SS] SCHEJA, G. and STORCH, U. *Lehrbuch der Algebra, Teil 2*. B. G. Teubner, Stuttgart, 1988.
- [Sg] SEGRE, B. Sullo scioglimento delle singolarità delle varietà algebriche. *Ann. Mat. Pura Appl.* 33 (1952), 5-48.
- [Se] SEIDENBERG, A. *Elements of the theory of algebraic curves*. Addison-Wesley, Menlo Park, California, 1968.
- [Sh] SHAFAREVICH, I. R. *Basic Algebraic Geometry 1 und 2, Second Edition*. Springer-Verlag, Berlin Heidelberg New York, 1994.
- [Vi1] VILLAMAYOR, O. Constructiveness of Hironaka's resolution. *Ann. Scient. Ec. Norm. Sup. Paris* 22 (1989), 1-32.
- [Vi2] ——— Patching local uniformizations. *Ann. Scient. Ec. Norm. Sup. Paris* 25 (1992), 629-677.
- [Za] ZARISKI, O. *Algebraic Surfaces*. Ergebnisse der Mathematik, vol 61, 2nd edition, Springer-Verlag 1971.
- [ZS] ZARISKI, O. and SAMUEL P. *Commutative Algebra, vol. I, II*. Van Nostrand 1958, 1960. Reprints: Graduate Texts in Mathematics 28, 29. Springer-Verlag 1975.

(Reçu le ...)

Herwig Hauser und Georg Regensburger

Institut für Mathematik
Universität Innsbruck
A-6020 Innsbruck
Austria
e-mail: herwig.hauser@uibk.ac.at, georg.regensburger@uibk.ac.at