Auflösung von "ebenen" Kurvensingularitäten

Diplomarbeit aus dem Fach Mathematik
zur Erlangung des Magistergrades
An der Naturwissenschaftlichen Fakultät
Der Leopold-Franzens-Universität Innsbruck

Eingereicht bei
a.o. Univ.-Prof. Dr. Herwig Hauser
Im Juli 1999 von

Georg Regensburger

Vorwort

Es ist ein wohlbekannter Satz, daß die Singularitäten einer "ebenen" algebraischen Kurve durch eine endliche Folge von elementaren Schritten, sogenannten Aufblasungen von Punkten, aufgelöst werden können.

In dieser Arbeit untersuchen wir einen solchen Auflösungsschritt mit Hilfe einer Invariante. Genauer ordnen wir jedem Punkt einer Kurve ein Element einer wohlgeordneten Menge zu, das angibt, wie singulär dieser ist. Wir zeigen, daß die Invariante bei Aufblasung eines nicht aufgelösten Punktes fällt. Induktiv läßt sich dann obiges Resultat beweisen.

Die für die Definition und Analyse der Invariante benötigten Ergebnisse über formale Potenzreihen werden im ersten Kapitel hergeleitet. Im zweiten Kapitel definieren wir eine Invariante für eine formale Potenzreihe in zwei Variablen über einem Körper. Das letzte Kapitel beginnt mit Begriffen und Behauptungen über Nullstellenmengen von Polynomen in zwei Variablen. Nach der Definition der eigentlichen Invariante erklären wir, was man unter einem aufgelösten Punkt eines Polynoms versteht. Es folgt die Beschreibung der Aufblasung eines Punktes in der Ebene. Anschließend erläutern wir den Begriff der Total- bzw. Strikt-Transformierten eines Polynoms. Im letzten Abschnitt zeigen wir schließlich, daß die Invariante bei Aufblasung kleiner wird.

An dieser Stelle möchte ich mich bei Prof. Herwig Hauser bedanken, der durch seine gute Betreuung und vor allem durch die viele Zeit, die er mir gewidmet hat, viel zum Gelingen der Diplomarbeit beigetragen hat.

Besonders bedanke ich mich auch bei meinen Eltern, die mich in meinem Studium immer in allen Belangen unterstützt und Verständnis gezeigt haben.

Imst, Juli 1999

Georg Regensburger

Inhaltsverzeichnis

Kapitel 1

Potenzreihenringe

1.1 Definition und wichtige Eigenschaften

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:

$$f + g = (f_0 + g_0, f_1 + g_1, \dots, f_k + g_k, \dots),$$
$$fg = (h_0, h_1, \dots, h_k, \dots) \text{ mit } h_k = \sum_{i+j=k} f_i g_j.$$

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 $\mathrm{ord} f$, und f_q die *Initialform*. Weiters setzen wir $\mathrm{ord} f = \infty$ für $f = 0$. Mit dieser Definition gilt folgendes

Lemma 1.1 *Für $f, g \in A[[x]]$ gilt*

$$\mathrm{ord}(f + g) \geq \min(\mathrm{ord} f, \mathrm{ord} g),$$
$$\mathrm{ord}(fg) \geq \mathrm{ord} f + \mathrm{ord} g.$$

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

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

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. ■

Satz 1.2 *Eine Potenzreihe f ist genau dann eine Einheit in $A[[x]]$, wenn f_0 in A invertierbar ist.*

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

$$\begin{aligned} f_0 g_0 &= 1, \\ f_0 g_1 + f_1 g_0 &= 0, \ldots, \\ f_0 g_k + f_1 g_{k-1} + \cdots + f_k g_0 &= 0, \ldots \end{aligned}$$

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

$$g_k = -f_0^{-1}(f_1 g_{k-1} + \cdots + f_k g_0).$$

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

Für das nächste Korollar brauchen wir noch folgende Beobachtungen. Die Potenzreihen mit einer positiven Ordnung bilden nach Lemma 1.1 ein Ideal $\mathfrak{m}$, das von $x_1, \ldots, x_n$ erzeugt wird. Das Ideal $\mathfrak{m}^q$ besteht aus allen Potenzreihen f mit $\operatorname{ord} f \geq q$ und wird erzeugt von allen Monomen $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ mit $|(\alpha_1, \ldots, \alpha_n)| = \alpha_1 + \cdots + \alpha_n = q$.

Korollar 1.3 *Sei k ein Körper. Dann ist $k[[x]]$ ein lokaler Ring mit maximalem Ideal $\mathfrak{m} = (x_1, \ldots, x_n)$.*

Beweis. Klar, da mit Satz 1.2 jedes Element von $k[[x]] \setminus \mathfrak{m}$ invertierbar ist. ■

Satz 1.4 *Wenn A ein noetherscher Ring ist, dann ist auch $A[[x]]$ mit $x = (x_1, \ldots, x_n)$ noethersch.*

Beweis. Siehe z.B. [17] S. 147. ■

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. $A \times A \longrightarrow A, (a,b) \longmapsto a-b$ ist stetig) is und wenn die Multiplikation stetig ist. In einer topologischen Gruppe ist die Translation ($T_a : A \longrightarrow A, b \longmapsto a+b$, $a \in A$) 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). Noch eine weitere

Proposition 1.5 *Wenn* $\{0\}$ *in* A *abgeschlossen ist, dann ist* A *Hausdorffsch.*

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

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 $n \in \mathbb{N}_0$ 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 $a \in A$.

Proposition 1.6 *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 $a + \mathfrak{q}^n \subset \mathfrak{q}^n$ und damit $\mathfrak{q}^n$ offen. Andrerseits 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 Proposition und da in einem Hausdorffraum jede einelementige Teilmenge abgeschlossen ist. ■

Im allgemeinen ist die $\mathfrak{q}-$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 $(a_i)_{i\in\mathbb{N}_0}$ eine *Cauchyfolge* genau dann, wenn es zu jeder Nullumgebung U ein $m \in \mathbb{N}_0$ 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 $q \in \mathbb{N}_0$ genau dann, wenn $\operatorname{ord} f \geq q$ (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.

Proposition 1.7 *$A[[x]]$ ist vollständig.*

Beweis. Sei $(f^i)_{i\in\mathbb{N}_0}$ eine Cauchyfolge in $A[[x]]$. Zu jedem $q \in \mathbb{N}_0$ gibt es dann ein minimales $m(q)$ mit $\operatorname{ord}(f^i - f^j) > q$ 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 $\operatorname{ord}(f - f^i) \geq q$ für $i \geq m(q)$ und damit $\lim f^i = f$. ■

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 $(f^i)_{i\in\mathbb{N}_0}$ 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:

$$\sum_{i=0}^{\infty} f^i + \sum_{i=0}^{\infty} g^i = \sum_{i=0}^{\infty} (f^i + g^i), \tag{1.1}$$

$$\sum_{i=0}^{\infty} f^i \sum_{i=0}^{\infty} g^i = \sum_{i=0}^{\infty} h^i \text{ mit } h^i = \sum_{j+k=i} f^j g^k,$$

$$g \sum_{i=0}^{\infty} f^i = \sum_{i=0}^{\infty} g f^i.$$

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

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

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 Teilemenge von $A[[x]]$. Dichte Teilmengen, die gleichzeitig ein Unterring von $A[[x]]$ sind, charakterisiert folgendes

Lemma 1.8 *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 $\operatorname{ord}(f - g) > k$. 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 $(h^i)_{i \in \mathbb{N}_0}$ in S mit $\operatorname{ord}(h^i - h) \geq i$. Setze $h^0 = 0$. Seien $h^0, h^1, \dots, h^{i-1}$ bereits konstruiert. Wenn $\operatorname{ord}(h^{i-1} - h) \geq i$, dann setzen wir $h^i = h^{i-1}$, sonst haben wir $\operatorname{ord}(h^{i-1} - h) = i - 1$. 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 $\operatorname{ord}(h^i - h) = \operatorname{ord}(h^{i-1} + f - h) \geq i$. ∎

1.3 Substitutionshomomorphismen

Seien A, A' kommutative Ringe mit Einselement, $\varphi : A \longrightarrow A'$ 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 $\bar{\varphi}$ mit $\bar{\varphi} \mid_A = \varphi$ und $\bar{\varphi}(x_i) = a_i$ 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 $\operatorname{ord} \varphi_j \geq 1$ 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 $\operatorname{ord} f_i \geq i$ (nach Lemma 1.1), d.h. $(\bar{f}_i)_{i\in\mathbb{N}_0}$ ist eine Nullfolge. Somit ist

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

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

$$f = f(y_1, \ldots, y_m) \longmapsto f(\varphi_1, \ldots, \varphi_m)$$

ist eine Abbildung $\varphi : A[[y]] \longrightarrow A[[x]]$ definiert. Mit (1.1) sieht man, daß φ ein $A-$Algebrahomomorphismus ist. Man nennt φ den zu $\bar{\varphi} = (\varphi_1, \ldots, \varphi_m)$ gehörigen *Substitutionshomomorphismus* (oder Einsetzungshomomorphismus).

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

$$\varphi(y_j) = \varphi_j \text{ für } j = 1, \ldots, m \text{ und } \varphi(f(y_1, \ldots, y_m)) = f(\varphi_1, \ldots, \varphi_m).$$

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

Satz 1.9 *Wenn $\psi : A[[y]] \longrightarrow A[[x]]$ ein stetiger $A-$Algebrahomomorphismus ist, dann ist $\operatorname{ord}(\psi(y_j)) \geq 1$ und ψ der zu $(\psi(y_1), \ldots, \psi(y_m))$ gehörige Substitutionshomomorphismus.*

Beweis. Aus der Stetigkeit von ψ folgt $\operatorname{ord}(\psi(y_j)) \geq 1$. Sei φ der zu $(\psi(y_1), \ldots, \psi(y_m))$ 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. ■

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

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

gehörigen Substitutionshomomorphismus identifizieren. Wenn wir in Zukunft schreiben "sei $\varphi : A[[y]] \longrightarrow A[[x]]$ der zu $\bar{\varphi} = (\varphi_1, \ldots, \varphi_m)$ gehörige Substitutionshomomorphismus", dann nehmen wir stillschweigend $\operatorname{ord} \varphi_j \geq 1$ für $j = 1, \ldots, n$ an.

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

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

wobei $\partial_j f_i$ die übliche partielle Ableitung von Polynomen ist. Die Abbildung $\partial_j : A[[x]] \longrightarrow A[[x]]$, $f \longmapsto \partial_j f$ ist $A-$linear. Aus $\operatorname{ord}(\partial_j f) \geq \operatorname{ord} f - 1$ 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. Z.B. ist $\partial_j x_j^n = n x_j^{n-1} = 0$, wenn die Charakteristik von A n teilt.

Proposition 1.10 (Produktregel) *Für ∂_j gilt die Produktregel, d.h.*

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

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

Durch Induktion über α folgt aus der Produktregel

$$\partial_j f^\alpha = \alpha f^{\alpha-1} \partial_j f \text{ für } j = 1, \ldots, n \text{ und } \alpha \in \mathbb{N}. \tag{1.2}$$

Proposition 1.11 (Kettenregel) *Sei $\varphi : A[[y]] \longrightarrow A[[x]]$ der zu $\bar{\varphi} = (\varphi_1, \ldots, \varphi_m)$ gehörigen Substitutionshomomorphismus. Dann gilt für jedes $f \in A[[y]]$*

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

Beweis. Sei zunächst $f = c y_1^{\alpha_1} \cdots y_m^{\alpha_m}$ mit $c \in A$. Dann gilt mit der Produktregel und (1.2)

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

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 $f \in A[[y]]$. ■

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.:

$$\alpha! c_\alpha = \alpha_1! \cdots \alpha_n! c_\alpha = \partial_1^{\alpha_1} \dots \partial_n^{\alpha_n} f(0)$$
$$\text{für alle } \alpha = (\alpha_1, \dots, \alpha_n) \in \mathbb{N}_0^n.$$

Für die spätere Charakterisierung der Isomorphismen unter den Einsetzungshomomorphismen benötigen wir die folgende "algebraische Version" des Differentials. Sei dazu $\varphi : A[[y]] \longrightarrow A[[x]]$ 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

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

Die Restklassen $\overline{y}_j$, $j = 1, \dots, m$, bzw. $\overline{x}_k$, $k = 1, \dots, n$, 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 $M_1 = \oplus_{j=1}^m A y_j$ und $\mathfrak{m}_x/\mathfrak{m}_x^2$ mit $N_1 = \oplus_{k=1}^n A x_k$ identifizieren. Damit ist $d\varphi : M_1 \longrightarrow N_1$, und es gilt

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

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 Substitionshomomorphismen $d(\psi \circ \varphi) = d\psi \circ d\varphi$ gilt.

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

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 $i = 1, \ldots, n$ und y auf y abbildet. Eine Potenzreihe $g \in R$ heißt *$y-$allgemein* (auch $y-$regulär) der Ordnung $m \in \mathbb{N}_0$, wenn $g(0,y) \in k[[y]]$ eine Potenzreihe der Ordnung m ist, d.h.

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

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

Satz 1.12 (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 $\operatorname{grad} r < m$ so, daß*

$$f = qg + r.$$

Beweis. Siehe z.B. [21] S. 241. ■

Satz 1.13 (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*

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

so, daß

$$ug = p.$$

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

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

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

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

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

Da $g' = g(0,y) = y^m u'$ mit u' invertierbar in $k[[y]]$ und $\operatorname{grad} r' < m$, 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 $\operatorname{ord} c_i \geq 1$ für $i = 0, \ldots, m-1$, da $r(0,y) = r' = 0$. Die Eindeutigkeit folgt aus dem Divisionssatz. ■

Proposition 1.14 *Der kanonische Ringhomorphismus*

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

ist ein Isomorphismus.

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

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

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

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

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

1.6 Stetige Isomorphismen

In diesem Abschnitt werden wir die Isomorphismen unter den Einsetzungshomomorphismen charakterisieren.

Lemma 1.15 *Sei $\varphi : A[[x]] \longrightarrow A[[x]]$ der zu $\bar{\varphi} = (\varphi_1, \ldots, \varphi_n)$ gehörige Substitutionshomomorphismus mit $d\varphi = Id$ (d.h. die Initialform von φ_j ist x_j für $j = 1, \ldots, n$). Dann ist φ ein Automorphismus.*

Beweis. Sei $f \in A[[x]]$ ungleich Null. Da φ_j die Initialform x_j für alle $j = 1, \ldots, n$ besitzt, haben $\varphi(f) = f(\varphi_1, \ldots, \varphi_n)$ und f die gleiche Initialform. Also ist der Kern von φ Null und φ injektiv. Weiters erkennt man damit

und mit Lemma 1.8, 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 $(\varphi(f^i))_{i\in\mathbb{N}_o}$ 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 $(f^i)_{i\in\mathbb{N}_o}$ 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 $g \in A[[\varphi_1,\dots,\varphi_n]]$. ■

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

Lemma 1.16 *Seien $f,\varphi_j,\psi_j \in A[[x]]$, $j=1,\dots,n$, mit $\operatorname{ord}\varphi_j \geq 1$ und $\operatorname{ord}\psi_j \geq 1$. Sei φ der zu $\bar\varphi = (\varphi_1,\dots,\varphi_n)$ gehörige Substitutionshomomorphismus. Dann gilt*

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

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

Beweis. Wir betrachten die stetige Abbildung

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

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

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

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

Sei φ wieder wie in Lemma 1.15. Wir suchen einen Substitutionshomomorphismus ψ mit $\psi\circ\varphi = \mathrm{Id}$. Dazu schreiben wir $\varphi_j = x_j + h_j$ mit $\operatorname{ord} h_j \geq 2$

für $j = 1, \ldots, n$. Wir möchten g_j mit $\operatorname{ord} g_j \geq 2$, mit $\psi_j = x_j + g_j$ finden so, daß

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

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

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

Anders ausgedrückt muß also g ein Fixpunkt der nach Lemma 1.16 stetigen Abbildung

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

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

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

Proposition 1.17 *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 1.16 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 1.18 *Sei* $\varphi : A[[y]] \longrightarrow A[[x]]$ *ein Substitutionshomomorphismus. Dann ist* φ *genau dann ein Isomorphismus, wenn* $d\varphi$ *ein Isomorphismus ist.*

Beweis. Wenn φ ein Isomorphismus ist, dann ist Id$= d(\varphi \circ \varphi^{-1}) = d\varphi \circ d\varphi^{-1}$ und 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 $\tilde{\varphi} : A[[y]] \longrightarrow A[[y]]$ ein Isomorphismus ist. Da aber $d\tilde{\varphi} = d(\varphi_{l^{-1}} \circ \varphi) =$Id, folgt mit Lemma 1.15 die Behauptung. ■

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

Satz 1.19 *Seien k ein Körper und $f \in k[[x]]$ ungleich 0. Dann gibt es einen Substitutionsautomorphismus $\varphi : k[[x]] \longrightarrow k[[x]]$ mit*

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

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

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

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

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

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

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

Dann ist

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

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

Sei nun k beliebig. Mit $>_{lex}$ bezeichnen wir die lexikographische Ordnung auf $\mathbb{N}_0^n$ mit $\alpha_1 > \cdots > \alpha_n$. Sei $\beta = \min_{>_{lex}}\{\alpha \in \mathbb{N}_0^n : c_\alpha \neq 0\}$. Wir wählen nun $m_i \in \mathbb{N}_0$ so, daß

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

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

$$\text{Dann ist } \beta \geq_{lex} \alpha \text{ für alle } \alpha \in \mathbb{N}_0^n \text{ mit } \alpha_n + \sum_{j=1}^{n-1} \alpha_j m_j = q. \tag{1.3}$$

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 (1.3) nicht wegheben kann.

Zu (1.3): Indirekt. Seien $\alpha >_{lex} \beta$ und k so, daß $\alpha_i = \beta_i$ für $i < k$ und $\alpha_k > \beta_k$. Dann ist

$$0 = \sum_{j=1}^{n-1} \alpha_j m_j + \alpha_n - \sum_{j=1}^{n-1} \beta_j m_j - \beta_n =$$

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

Widerspruch. ■

1.7 Potenzreihenringe über k sind faktoriell

Satz 1.20 *Sei k ein Körper. Dann ist $k[[x_1, \ldots, x_n]]$ faktoriell.*

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

Seien also $f \in k[[x]] = R$, f nicht invertierbar, und $k[[x_1, \ldots, x_{n-1}]] = R'$ faktoriell. Nach dem Satz 1.19 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 $\operatorname{ord} c_i \geq 1$ für $i = 0, \ldots, m-1$. Der Polynomring $R'[x_n]$ in x_n ist nach einem Satz von Gauß faktoriell, da R' faktoriell ist. Also ist

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

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 $j = 1, \ldots, n-1$ 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 Proposition 1.14 folgt dann, daß $R'[x_n]/p_i R'[x_n] \cong R/p_i R$. Also sind die p_i, $i = 1, \ldots, k$, auch Primelemente in R. ■

1.8 Ideale im Polynom- und Potenzreihenring

Seien k ein Körper und $k[x] = k[x_1, \ldots, x_n]$ 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 $\mathfrak{m} = (x_1, \ldots, x_n)$ 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

$$f : A \longrightarrow S^{-1}A, \; a \longmapsto \frac{a}{1}.$$

(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

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

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

Proposition 1.21 *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 $b/t \in S^{-1}\mathfrak{p}$. ■

Proposition 1.22 *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 $n \in \mathbb{N}$) 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 $n \in \mathbb{N}$ und $u \in S$. Widerspruch. ■

Proposition 1.23 *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 Proposition 1.21 (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 $a = up_1^{b_1} \cdots p_r^{b_r}$ eine Primfaktorzerlegung von a in A (d.h. die p_i's sind prim und paarweise nicht-assoziiert, und u ist eine Einheit). Dann ist nach (i) und (ii)

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

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

zu (iv): Klar mit der vorherigen Gleichung. ■

Sei im folgenden $S = k[x] \setminus \mathfrak{m}$ (S ist multiplikativ) mit $\mathfrak{m} = (x_1, \ldots, x_n)$. 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 maximalen 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 1.2 invertierbar. Wir können daher den Ring $k[x]_\mathfrak{m}$ in den Potenzreihenring $k[[x]]$ durch die wohldefinierte und injektive Abbildung

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

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 1.3 und Satz 1.4 ein lokaler, noetherscher Ring. Nach Satz 1.20 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

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

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.

Proposition 1.24 (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 $m_1, \ldots, m_n$ ein Erzeugendensystem von M mit minimalem n. Angenommen $M \neq 0$, dann ist $n \geq 1$. Da $\mathfrak{a}M = M$ ist, gibt es $a_1, \ldots, a_n \in \mathfrak{a}$ mit $m_1 = a_1 m_1 + \cdots + a_n m_n$. Also ist

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

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 $m_2, \ldots, m_n$ ein Erzeugendensystem von M, also ein Widerspruch zur Minimalität von n. ■

Proposition 1.25 *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 $p : A \longrightarrow A/\mathfrak{b}$ 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

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

■

Proposition 1.26 *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 1.27 *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 $\mathfrak{c} = (c_1, \ldots, c_m)$ 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 $n \in \mathbb{N}$. Wir können γ_i schreiben als

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

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 Propositionen folgt. ■

Korollar 1.28 *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

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

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

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

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

Proposition 1.29 *Seien $f \in k[x]$ und $f = c f_1^{b_1} \cdots f_r^{b_r}$ eine 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. Die folgende Proposition zeigt, daß

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

Dann ist mit Satz 1.27

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

Mit Proposition 1.21 (ii) und Proposition 1.22 folgt weiter

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

■

Proposition 1.30 *Sei A ein faktorieller Ring. Seien $a_1, \dots, a_r \in A$ und $v = \mathrm{kgV}(a_1, \dots, a_r)$. Dann ist*

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

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

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

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 Proposition 1.29 herleiten, wie die Kontraktion eines beliebigen Ideals aussieht.

Proposition 1.31 *Seien $f, g \in k[x]$ und $f = c f_1^{b_1} \cdots f_r^{b_r}$ eine 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 Proposition 1.29

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

Also $h \mid g$ in $k[x]$. ■

Satz 1.32 *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 $n \in \mathbb{N}$ 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 1.27 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.

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

Sei $n = \operatorname{ord}\gamma + 1$. Dann ist $\operatorname{ord}(s_n + u_n) = \operatorname{ord}\gamma$ (weil $\gamma = s_n + \sigma_n$ und $u_n \in \mathfrak{m}^n$). Also ist $\operatorname{ord}\lambda = 0$, 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 1.28, daß $(s_n + u_n) \mid c$ in $k[x]_{\mathfrak{m}}$, d.h.

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

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

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

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

Korollar 1.33 *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 Proposition 1.23 (iv). ■

Kapitel 2

Potenzreihen in zwei Variablen

2.1 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

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

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

$$\begin{aligned} L &= \{\varphi \in G \text{ mit } \varphi_1 - y \in zk[[z]] \text{ und } \varphi_2 = z\}, \\ U &= \{\varphi \in G \text{ mit } \varphi_1 - y \in yR\}, \\ P &= \{\mathrm{Id}, p\} \text{ mit } \bar{p} = (z, y). \end{aligned}$$

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 1.4) eine unipotente untere Dreiecksmatrix bzw. eine obere Dreiecksmatrix. Der durch dl induzierte lineare Substitutionshomorphismus 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

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

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

Proposition 2.1 *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 $du = \mathrm{Id}$. Sei also $\bar{u} = (y + h_1, z + h_2)$ mit $\mathrm{ord}(h_i) \geq 2$, $i = 1, 2$, und $h_1 = yf(y, z)$. Nach Abschnitt 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

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

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

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

■

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 $\mathrm{ord}(h_i) \geq 2$ 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 $\mathrm{ord}(h_1) \geq 2$ (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.

Satz 2.2 *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 $G = PUL$. ∎

2.2 Die Ordnung

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). Mit dem so definierten φ ist

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

genau dann, wenn

$$\tilde{f}(y,z) = \varphi^{-1}(f(y,z)).$$

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

Wir werden im nächsten Abschnitt für eine Potenzreihe $f \in R$ das sogenannte Newton-Polygon definieren. Mit Hilfe dieses Polygons ordnen wir f eine Zahl zu, die wir geometrisch interpretieren können. Das Newton-Polygon ist aber abhängig von der Wahl des regulären Parametersystems $\mathbf{y} = (y,z)$. Wir untersuchen daher im Abschnitt 2.4 das Verhalten dieser Zahl bei Anwendung eines $\varphi \in G$ auf f. Im Teil 2.5 definieren wir schließlich eine weitere Invariante neben der Ordnung und untersuchen deren Eigenschaften.

2.3 Das Newton-Polygon

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

$$f = f(y,z) = \sum_{\alpha} c_\alpha y^{\alpha_1} z^{\alpha_2} = \sum_{\alpha} c_\alpha \mathbf{y}^\alpha \text{ mit } \alpha = (\alpha_1, \alpha_2) \in \mathbb{N}_0^2. \tag{2.1}$$

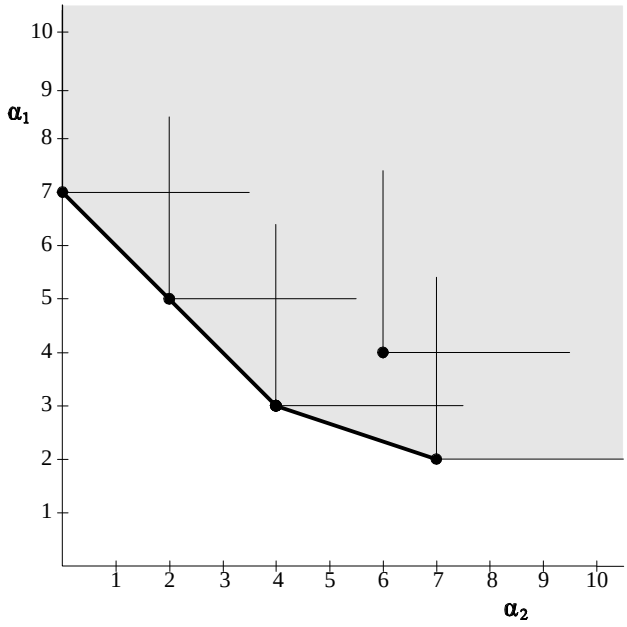
Die Menge

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

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

$$\operatorname{conv}\Big(\bigcup_{\alpha \in \Delta_{\mathbf{y}}(f)} \{\alpha + \mathbb{R}_+^2\}\Big) \subset \mathbb{R}_{\geq 0}^2$$

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 $NP_{\mathbf{y}}(f)$. 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 1 *Das Newton-Polygon von* $f = y^7 + y^5z^2 + y^3z^4 + y^4z^6 + y^2z^7$ *und dessen Konstruktion ist in Abbildung 1 zu sehen. Die Menge der Ecken,* $NP_{\mathbf{y}}(f)$*, 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 $f, g \neq 0$.

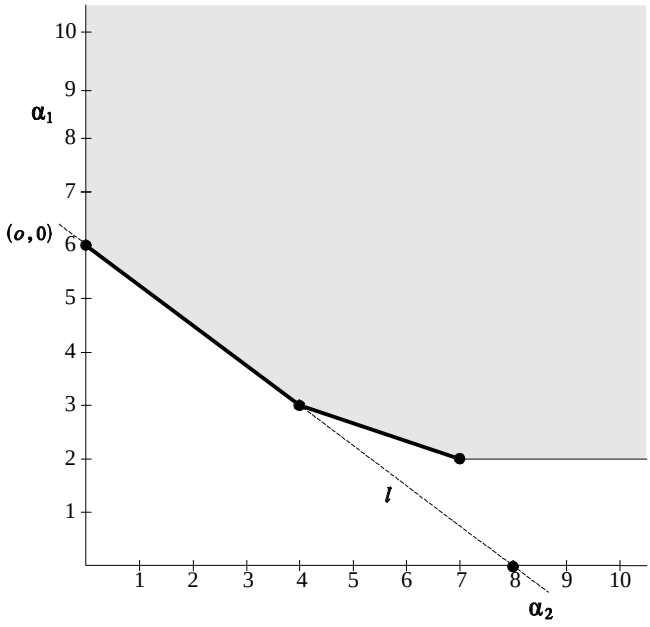
$$\Delta_{\mathbf{y}}(fg) \subset \Delta_{\mathbf{y}}(f) + \Delta_{\mathbf{y}}(g). \tag{2.2}$$

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. (z.B. $(y+yz)(1-z) = y - yz^2$), aber es gilt:

Proposition 2.3 *Wenn* $\delta \in NP_{\mathbf{y}}(f)$*, dann ist* $\delta \in \Delta_{\mathbf{y}}(fe)$*.*

Beweis. Wenn f auch invertierbar ist, gilt die Aussage trivialerweise. Seien f wie in (2.1) mit $\operatorname{ord} f \geq 1$,

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



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. ■

Mit dieser Proposition, (2.2) und der Definition des Newton-Polygons folgt:

Proposition 2.4 *Seien f, $e \in R$, $f \neq 0$ und e invertierbar. Dann ist*

$$NP_{\mathbf{y}}(f) = NP_{\mathbf{y}}(fe).$$

Seien $f \in \mathfrak{m}$, $f \neq 0$, wie in (2.1) und $o = \operatorname{ord} f$. Wir setzen

$$s_{\mathbf{y}} f = \inf \left\{ \frac{o\alpha_2}{o - \alpha_1} \text{ mit } \alpha \in NP_{\mathbf{y}}(f),\, \alpha \neq (o,0) \right\} \subset \mathbb{R}_+ \cup \{\infty\}.$$

Wenn $\alpha \in NP_{\mathbf{y}}(f)$, $\alpha \neq (o,0)$, dann ist $(0, \frac{o\alpha_2}{o-\alpha_1})$ die Projektion von (α_1, α_2) durch $(o,0)$ auf die α_2-Achse der Schnittpunkt der Geraden

$$l = \left\{ (\beta_1, \beta_2) : \frac{\alpha_2}{o - \alpha_1}\beta_1 + \beta_2 = \frac{o\alpha_2}{o - \alpha_1} \right\}$$

durch $(o,0)$ und (α_1, α_2) mit der α_2-Achse (siehe Abbildung 2.3).

Proposition 2.5 *Seien $f \in \mathfrak{m}$, $f \neq 0$ und $o = \operatorname{ord} f$. Dann gilt:*

(i) $s_{\mathbf{y}} f \in \{\frac{p}{q} \in \mathbb{Q}_+$ *mit p und q prim und* $1 \leq q \leq o\} \cup \{\infty\}$.

(ii) $o \leq s_{\mathbf{y}} f \leq \infty$.

(iii) $s_{\mathbf{y}} f = o$ *genau dann, wenn es ein* $\alpha \in NP_{\mathbf{y}}(f)$, $\alpha \neq (o,0)$, *mit* $\alpha_1 + \alpha_2 = o$ *gibt.*

(iv) $s_{\mathbf{y}} f > o$ *genau dann, wenn f_o, die Initialform von f, cy^o mit $c \neq 0$ ist.*

(v) $s_{\mathbf{y}} f = \infty$ *genau dann, wenn $f = y^o e$ mit $e \in R$ invertierbar.*

Beweis. Klar. ■

Seien $f \in \mathfrak{m}$, $f \neq 0$, wie in (2.1), $o = \operatorname{ord} f$ und $t \in \mathbb{R}$ mit $t \geq o$. Wir schreiben

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

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

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

Sei $s = s_{\mathbf{y}} f < \infty$. Dann können wir f zerlegen in

$$f = F_s + F_{>s}. \tag{2.3}$$

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

Proposition 2.6 *Sei umgekehrt $o \leq t \in \mathbb{R}$ so, daß*

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

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

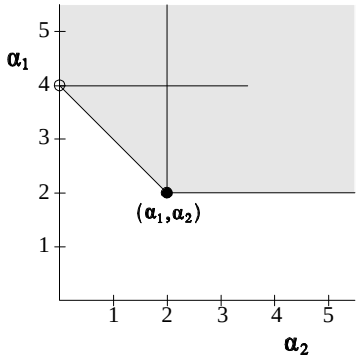
Beweis. Sei $\alpha \in \Delta_{\mathbf{y}}(f)$, $\alpha_1 < o$. Aus $\frac{t}{o}\alpha_1 + \alpha_2 \geq t$ folgt

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

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

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

Damit ist $s_{\mathbf{y}} f = t$. ■



2.4 Koordinatenwechsel

Um die Beziehung zwischen $s_{\mathbf{y}}f$ und $s_{\mathbf{y}}\varphi(f) = s_{\varphi^{-1}\mathbf{y}}f$ für ein $\varphi \in G$ zu untersuchen, verwenden wir die Möglichkeit der Zerlegung von φ in ein $u \in U$, $l \in L$ und $p \in P$ des Abschnitts 2.1.

Sei zunächst $u \in U$. Dann ist

$$\begin{aligned} u_1 &= u(y) = ay + yh_1 && \text{mit } \operatorname{ord} h_1 \geq 1, a \neq 0 \\ u_2 &= u(z) = cz + by + h_2 && \text{mit } \operatorname{ord} h_2 \geq 2, c \neq 0. \end{aligned} \tag{2.4}$$

Das Newton-Polygon von f ist im allgemeinen nicht gleich dem Newton-Polygon von $u(f)$. (z.B. $f = z$ und $\bar{u} = (y, y + z)$).

Proposition 2.7 *Seien $f = y^{\alpha_1}z^{\alpha_2}$ mit $\alpha \neq 0$ und $u \in U$. Dann gilt (siehe Abbildung 2.4):*

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

(ii)

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

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 $\operatorname{ord} h > \alpha_2$. Daraus folgt die Behauptung. ■

Proposition 2.8 *Seien $f \in \mathfrak{m}$, $f \neq 0$, $o = \operatorname{ord} f$ und $u \in U$. Dann gilt:*

(i) *Wenn $s_{\mathbf{y}} f > o$, dann ist $NP_{\mathbf{y}}(f) = NP_{\mathbf{y}}(u(f))$.*

(ii) $s_{\mathbf{y}} f = s_{\mathbf{y}} u(f)$.

Beweis. zu (i): Da $s_{\mathbf{y}} f > o$, ist mit Proposition 2.5 $(o, 0) \in \Delta_{\mathbf{y}}(f)$. Mit der vorherigen Behauptung und der Definition des Newtonpolygons folgt daraus $NP_{\mathbf{y}}(f) = NP_{\mathbf{y}}(u(f))$.

zu (ii): Sei $s_{\mathbf{y}} f = o$. Nach Propostion 2.5 gibt es ein $\alpha \in NP_{\mathbf{y}}(f)$, $\alpha \neq (o, 0)$, mit $\alpha_1 + \alpha_2 = o$. Wenn es zwei solche $\alpha \in NP_{\mathbf{y}}(f)$ gibt, dann betrachten wir das mit der kleineren α_1-Koordinate. Nach der vorherigen Behauptung ist dann $\alpha \in NP_{\mathbf{y}}(u(f))$ und damit $s_{\mathbf{y}} u(f) = s_{\mathbf{y}} f = o$. ■

Sei nun $l \in L$. Dann ist

$$\begin{aligned} l_1 &= l(y) = y + g \qquad \text{mit } g \in k[[z]], \operatorname{ord} g \geq 1 \\ l_2 &= l(z) = z. \end{aligned} \tag{2.5}$$

Wenn wir $s_{\mathbf{y}} f$ und $s_{\mathbf{y}} l(f)$ vergleichen, können wir im allgemeinen nichts aussagen, wie folgendes Beispiel belegt:

Beispiel 2 *Sei $l(y) = y + z$.*

- *Mit $f = y^2 + z^3$ ist $l(f) = y^2 + 2yz + z^2 + z^3$, also $2 = s_{\mathbf{y}} l(f) < s_{\mathbf{y}} f = 3$.*
- *Mit $f = y^2 + yz$ ist $l(f) = y^2 + 3yz + 2z^2$, also $2 = s_{\mathbf{y}} l(f) = s_{\mathbf{y}} f = 2$.*
- *Mit $f = y^2 - 2yz + z^2 + z^3 = (y - z)^2 + z^3$ ist $l(f) = y^2 + z^3$, also $3 = s_{\mathbf{y}} l(f) > s_{\mathbf{y}} f = 2$.*
- *Mit $f = y^2 - 2yz + z^2 = (y - z)^2$ ist $l(f) = y^2$, also $s_{\mathbf{y}} l(f) = \infty$.*

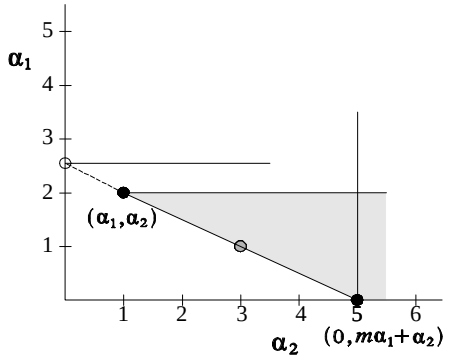
Außerdem kann $s_{\mathbf{y}} l(f)$ von der Charakteristik von k abhängen. Mit l wie im vorherigen Beispiel und $f = y^2 + z^2$ ist $l(f) = y^2 + 2yz + 2z^2$. Wenn $\operatorname{char} k = 2$, dann ist $s_{\mathbf{y}} l(f) = \infty$, sonst $s_{\mathbf{y}} l(f) = 2$.

Sei l wie in (2.5). Wir werden nun den Zusammenhang zwischen

$$s_{\mathbf{y}} f, s_{\mathbf{y}} l(f) \text{ und } m = \operatorname{ord} g$$

untersuchen.

Proposition 2.9 *Seien $f = y^{\alpha_1} z^{\alpha_2}$ mit $\alpha \neq 0$ und $l \in L$. Dann gilt (siehe Abbildung 2.4):*



(i) $(\alpha_1, \alpha_2), (0, m\alpha_1 + \alpha_2) \in \Delta_{\mathbf{y}}(l(f))$.

(ii)

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

(iii) *Wenn* $\operatorname{char} k = 0$, *dann ist außerdem* $(\alpha_1 - k, mk + \alpha_2) \in \Delta_{\mathbf{y}}(l(f))$ *für* $k = 1, \ldots, \alpha_1 - 1$.

Beweis. Es ist

$$l(f) = (y+g)^{\alpha_1} z^{\alpha_2} = y^{\alpha_1} z^{\alpha_2} + g^{\alpha_1} z^{\alpha_2} + \left(\sum_{k=1}^{\alpha_1 - 1} \binom{\alpha_1}{k} y^{\alpha_1 - k} g^k\right) z^{\alpha_2}. \quad (2.6)$$

Daraus folgt die Behauptung. ■

Sei jetzt wieder $f \in \mathfrak{m}$, $f \neq 0$ und bezeichne $o = \operatorname{ord} f$ und $s = s_{\mathbf{y}} f$.

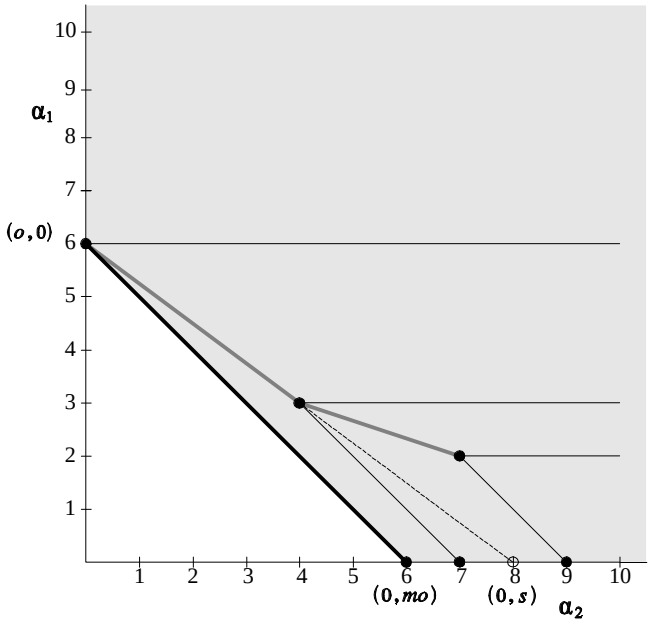
Proposition 2.10 *Wenn* $m < \frac{s}{o}$, *dann ist* $s_{\mathbf{y}} l(f) = mo$ *(siehe Abbildung 2.4).*

Beweis. Sei zunächst $s_{\mathbf{y}} f < \infty$. Wir zerlegen f in (siehe (2.3))

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

Aus

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



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

$$\frac{o\alpha_2}{o - \alpha_1} \geq s > mo$$

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

$$\Delta_{\mathbf{y}}(l(cy^o)) \subset \Delta_{\mathbf{y}}(l(f)) \text{ und } \{(o,0),(0,mo)\} = NP_{\mathbf{y}}(l(f)),$$

also $s_{\mathbf{y}}l(f) = mo$.

Wenn $s_{\mathbf{y}}f = \infty$, dann ist

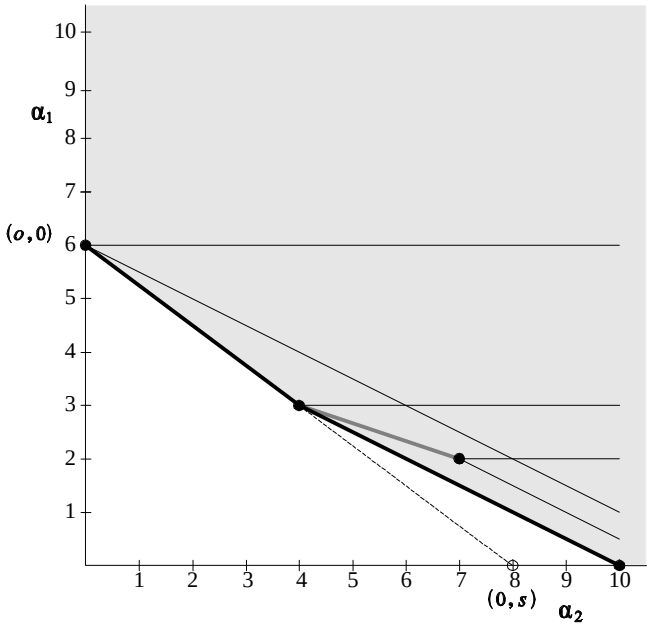
$$f = y^o e \text{ mit } e \in R \text{ invertierbar.}$$

Damit ist

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

und daraus folgt mit der vorherigen Proposition und Proposition 2.4 die Behauptung. ■

Proposition 2.11 *Wenn $m > \frac{s}{o}$, dann ist $s_{\mathbf{y}}f = s_{\mathbf{y}}l(f)$ (siehe Abbildung 2.4).*



Beweis. Wir zerlegen f wie in (2.3) 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

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

Mit Proposition 2.9 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 Terme, deren Exponenten wieder die obigen Ungleichung erfüllen, besteht. Also ist

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

Mit Proposition 2.6 gilt dann $s_{\mathbf{y}} l(f) = s_{\mathbf{y}} f$. ■

Lemma 2.12 *Wenn $m \neq \frac{s}{o}$, dann ist $s_{\mathbf{y}} l\,(f) \leq s_{\mathbf{y}} f$.*

Beweis. Klar mit den zwei vorherigen Propositionen. ■

Satz 2.13 *Seien $f \in \mathfrak{m}$, $f \neq 0$, mit $s = s_{\mathbf{y}} f < \infty$, $o = \operatorname{ord} f$ und $f = F_s + F_{>s}$ wie in (2.3). Dann sind äquivalent:*

1. *Es gibt ein $l \in L$ mit $s_{\mathbf{y}} l(f) > s_{\mathbf{y}} f$.*
2. *$\frac{s}{o} \in \mathbb{N}$ und*

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

Beweis. Sei $\frac{s}{o} \in \mathbb{N}$ und

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

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

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

Mit Proposition (2.9) sieht man, daß $l(F_{>s}) = F'_{>s}$. Daraus folgt entweder $NP_{\mathbf{y}}(l(f)) = \{(o, 0)\}$, also $s_{\mathbf{y}} l(f) = \infty$, oder

$$\frac{o\alpha_2}{o - \alpha_1} > s \text{ für alle } \alpha \in NP_{\mathbf{y}}(f),\ \alpha \neq (o, 0).$$

Damit gilt wieder $s_{\mathbf{y}} l(f) > s_{\mathbf{y}} f$.

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

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

Aus Lemma 2.12 folgt $\frac{s}{o} = m \in \mathbb{N}$. Wie zuvor ist $l(F_{>s}) = F'_{>s}$. Weiters ist (siehe (2.6))

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

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 $s_{\mathbf{y}} l(f) > s_{\mathbf{y}}(f)$, muß dann

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

Also ist

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

■

Sei p die Vertauschung von y und z. Dann ergibt sich mit Proposition 2.5:

Proposition 2.14 *Seien $f \in \mathfrak{m}$, $f \neq 0$ und $o = \operatorname{ord} f$. Dann gilt:*

(i) *$s_{\mathbf{y}}p(f) = o$ genau dann, wenn es ein $\alpha \in NP_{\mathbf{y}}(f)$, $\alpha \neq (0,o)$, mit $\alpha_1 + \alpha_2 = o$ gibt.*

(ii) *$s_{\mathbf{y}}p(f) > o$ genau dann, wenn f_o, die Initialform von f, cz^o mit $c \neq 0$ ist.*

(iii) *$s_{\mathbf{y}}p(f) = \infty$ genau dann, wenn $f = z^o e$ mit $e \in R$ invertierbar.*

2.5 Eine Invariante

Seien $f \in \mathfrak{m}$, $f \neq 0$, $o = \operatorname{ord} f$ und

$$S = \{s_{\mathbf{y}}\varphi(f) \text{ mit } \varphi \in G\} = \\ = \{s_{\mathbf{y}}f \text{ mit } \mathbf{y} = (y,z) \text{ reguläres Parametersystem von } R\}.$$

Wir definieren

$$s(f) = \sup S.$$

Offenbar ist $s(f)$ eine Invariante von f. Nach Satz 2.2 können wir jedes $\varphi \in G$ schreiben $\varphi = ulp$ mit $u \in U$, $l \in L$ und $p \in P$. Mit Propostion 2.8 ist dann

$$s_{\mathbf{y}}\varphi(f) = s_{\mathbf{y}}ulp(f) = s_{\mathbf{y}}u^{-1}(ulp(f)) = s_{\mathbf{y}}lp(f).$$

Also ist

$$S = \{s_{\mathbf{y}}lp(f) \text{ mit } l \in L \text{ und } p \in P\}.$$

Wenn $s(f) < \infty$, dann erkennt man mit Proposition 2.5 (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 $s_{\mathbf{y}} lp(f) = s(f)$. Insbesondere gibt es ein reguläres Parametersystem $\tilde{\mathbf{y}} = (\tilde{y}, \tilde{z})$ von R mit

$$s_{\tilde{\mathbf{y}}} f = s(f) \text{ mit } f = f(\tilde{y}, \tilde{z}).$$

Wir sagen dann, das Parametersystem $\tilde{\mathbf{y}} = (\tilde{y}, \tilde{z})$ *realisiert* $s(f)$.

Unmittelbar aus Proposition 2.4 folgt:

Proposition 2.15 *Seien $f \in \mathfrak{m}$, $f \neq 0$ und $e \in R$ invertierbar. Dann ist $s(f) = s(fe)$.*

Wir kommen nun zum Fall $s(f) = \infty$. Zunächst folgende

Proposition 2.16 *Sei $f = f(y, z) \in R$ $y-$allgemein der Ordnung 1. Dann gibt es genau ein $l \in L$ mit $s_{\mathbf{y}} l(f) = \infty$.*

Beweis. Angenommen es existiert ein $l \in L$ mit $s_{\mathbf{y}} l(f) = \infty$, d.h.

$$l(f) = ye \text{ mit } e \in R, \, e \text{ invertierbar.}$$

Dann ist mit $\bar{l} = (y + g, z)$, $g \in zk[[z]]$,

$$l^{-1} l(f) = f = (y - g)e(y - g, z).$$

Da $e(y-g, z)$ wieder invertierbar ist, existieren nach Voraussetzung und dem Weierstraßschen Vorbereitungssatz g und damit l eindeutig. ■

Daraus ergibt sich:

Proposition 2.17 *Sei $f \in R$ mit $\operatorname{ord} f = 1$. Dann ist $s(f) = \infty$.*

Satz 2.18 *Sei $f = f(y, z) \in \mathfrak{m}$, $f \neq 0$ mit $o = \operatorname{ord} f < s_{\mathbf{y}} f$. Dann ist $s(f) = \infty$ genau dann, wenn es ein $l \in L$ gibt so, daß $s_{\mathbf{y}} l(f) = \infty$.*

Beweis. Sei also $s(f) = \infty$. Wir konstruieren das gesuchte $l \in L$ mit $s_{\mathbf{y}} l(f) = \infty$ induktiv. Sei $s_1 = s_{\mathbf{y}} f$. 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 $s_1 < s_{\mathbf{y}} l_1 p_1(f)$. Angenommen p_1 ist nicht die Identität. Da $f_o = cy^o$ mit

$c \in k$, $c \neq 0$ ist, wäre dann aber $s_{\mathbf{y}} l_1 p_1(f) = o$. Also ist p_1 die Identität. Mit Satz 2.13 folgt daher

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

Wie im Beweis zu Satz 2.13 erkennt man, daß

$$s_1 < s_2 = s_{\mathbf{y}} f(y + a_1 z^{m_1}, z).$$

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 $n \in \mathbb{N}$ ein $a_n \in k$ und ein $s_n \in \mathbb{N}$ mit $s_1 < s_2 < \cdots < s_n$ und $m_n = \frac{s_n}{o} \in \mathbb{N}$ so, daß

$$f(y + \sum_{i=1}^{n} a_i z^{m_i}, z) = cy^o + S_n,$$
$$S_n = \sum c_\alpha^n y^{\alpha_1} z^{\alpha_2} \text{ mit } \frac{s_{n+1}}{o}\alpha_1 + \alpha_2 \geq s_{n+1},\ \alpha \neq (o, 0) \text{ und } c \neq 0.$$

Die Summe S_n zerlegen wir in

$$S_n = y^o M_n + R_n,$$
$$M_n = \sum c_\alpha^n y^{\alpha_1 - o} z^{\alpha_2} \text{ mit } \alpha_1 \geq o \text{ und}$$
$$R_n = \sum c_\alpha^n y^{\alpha_1} z^{\alpha_2} \text{ mit } \alpha_1 < o.$$

Aus den beiden Ungleichungen für die Exponenten der Terme von R_n folgt, daß die Ordnung von R_n beliebig groß wird, d.h. $\lim R_n = 0$. Mit Lemma 1.16 des vorherigen Kapitels und $g = \sum_{i=1}^{\infty} a_i z^{m_i}$ ist für $n \in \mathbb{N}$

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

Damit konvergiert M_n und mit $M = \lim M_n$ ist

$$f(y + g, z) = cy^o + y^o M.$$

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

Die umgekehrte Implikation ist trivial. ■

Korollar 2.19 *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 $s(f) = s_{\mathbf{y}} lp(f)$.*

Beweis. Seien $s(f) = \infty$ und $s_{\mathbf{y}} f = \operatorname{ord} f = o$. Dann gibt es ein $l_0 \in L$ und ein $p_0 \in P$ mit $s_{\mathbf{y}} l_0 p_0(f) > o$, und wir können den vorherigen Satz anwenden. Wenn $s(f)$ endlich ist, haben wir uns schon zu Beginn des Abschnittes überlegt, daß es ein $l \in L$ und ein $p \in P$ gibt mit $s(f) = s_{\mathbf{y}} lp(f)$. ■

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

$$s_{\mathbf{y}} f = s(f) \text{ mit } f = f(y,z).$$

Eine zum ersten Teil des Beweises von Satz 2.18 analoge Argumentation zeigt auch folgenden

Satz 2.20 *Sei $f = f(y,z) \in \mathfrak{m}$, $f \neq 0$ mit $s(f) < \infty$. 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 $s(f) = s_{\mathbf{y}} lp(f)$ mit $\bar{l} = (y+g, z)$.

2.6 Tschirnhaus-Transformation

Wenn $\operatorname{char} k = 0$ ist, dann kann man ein $\varphi \in G$ mit $s_{\mathbf{y}} \varphi(f) = s(f)$ auch durch eine sogenannte Tschirnhaus-Transformation konstruieren.

Sei dazu $f = f(y,z) \in \mathfrak{m}$. Zunächst gibt es nach Lemma 1.19 des vorherigen Kapitels ein $\varphi \in G$ so, daß $\tilde{f} = \varphi(f)$ $y-$allgemein der Ordnung $o = \operatorname{ord} f$ ist. Nach dem Weierstraßschen Vorbereitungssatz gibt es eine Einheit $e \in R$ und ein Weierstraßpolynom

$$h = y^o + c_{o-1}(z) y^{o-1} + \cdots + c_0(z) \in k[[z]][y],$$

so, daß $e\tilde{f} = h$. Mit Proposition 2.15 genügt es, für h ein $\varphi \in G$ mit $s_{\mathbf{y}} \varphi(h) = s(h)$ zu finden. Sei $l \in L$ der zu

$$\bar{l} = (y - \frac{1}{o} c_{o-1}(z), z)$$

gehörige Substitutionshomomorphismus (hier brauchen wir $\operatorname{char} k = 0$). Dann ist

$$\begin{aligned}\tilde{h} = l(h) = h(y - \frac{1}{o}c_{o-1}(z), z) = \\ = (y - \frac{1}{o}c_{o-1}(z))^o + c_{o-1}(z)(y - \frac{1}{o}c_{o-1}(z))^{o-1} + \cdots + c_0(z) = \\ = y^o + \tilde{c}_{o-2}(z)y^{o-2} + \cdots + \tilde{c}_0(z).\end{aligned}$$

Proposition 2.21 *Es gilt:* $s_{\mathbf{y}}\tilde{h} = s(h)$.

Beweis. Sei zunächst $o < s = s_{\mathbf{y}}\tilde{h}$. Wenn $s = \infty$, dann ist die Behauptung offensichtlich richtig. Sei also $s < \infty$. Angenommen es gibt ein $l_1 \in L$ und ein $p_1 \in P$ mit $s_y l_1 p_1(\tilde{h}) > s$. Wie im Beweis zu Satz 2.18 folgt daraus, daß p_1 die Identität ist und daß

$$m = \frac{s}{o} \in \mathbb{N} \text{ und } \tilde{h} = (y - az^m)^o + \tilde{H}_{>s} \text{ mit } a \in k,\ a \neq 0.$$

In Charakteristik Null ist aber $oay^{o-1}z^m \neq 0$. Also ein Widerspruch, denn $\tilde{h}$ besitzt keinen Term der Form $cy^{o-1}z^{\alpha_2}$ mit $\alpha_2 \in \mathbb{N}$.

Sei nun $o = s$. Wir nehmen wieder an, daß es $l_1 \in L$ und $p_1 \in P$ wie oben gibt. Wir brauchen uns nur noch den Fall zu überlegen, daß p_1 die Vertauschung von y und z ist. Da dann aber $p_1(\tilde{h})$ keine Terme der Form $cy^{\alpha_1}z^{o-1}$ mit $\alpha_1 \in \mathbb{N}$ besitzt, ergibt sich wie zuvor ein Widerspruch. ∎

Kapitel 3

Auflösung von Kurvensingularitäten in beliebiger Charakteristik

3.1 Polynome in zwei Variablen

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 3.1 *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

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

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

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

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

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

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

die Menge der gemeinsamen Nullstellen von $f_1, \ldots, f_n$.

Proposition 3.2 *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. ■

Satz 3.3 *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 der vorherigen Proposition ist $\mathrm{ggT}(f,g) = 1$ 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. ■

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

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

Dabei sind

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

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

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

Es gilt

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

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

$$\operatorname{Sing}(f) = \{a \in \mathbb{A}^2 \text{ mit } \operatorname{ord}_\alpha f > 1\} = V(f, \partial_y f, \partial_z f)$$

bezeichnen wir die Menge der singulären Punkte von f.

Satz 3.4 *Seien k ein algebraisch abgeschlossener Körper und $f \in k[y,z]$ irreduzibel. Dann ist die Menge* $\operatorname{Sing}(f)$ *endlich.*

Beweis. Angenommen $\operatorname{Sing}(f)$ ist eine unendliche Menge. Da f irreduzibel ist und $\deg \partial_y f < \deg f$, können f und $\partial_y f$ nach Satz 3.3 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 $\operatorname{char} k = 0$. Wenn $\operatorname{char} k = p > 0$, 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

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

Dies ist ein Widerspruch zur Irreduzibilität von f. ■

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

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

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

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

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

eine Primfaktorzerlegung von a mit einer Einheit u und paarweise nichtassoziierten Primelementen p_i. Man nennt a *reduziert* (bzw. *quadratfrei*), wenn $b_i = 1$ für $i = 1, \ldots, r$.

Proposition 3.5 *Seien A ein faktorieller Ring, $a \in A$ und $a = up_1^{b_1} \cdots p_r^{b_r}$ eine 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 $b = vq_1^{c_1} \cdots q_s^{c_s}$ eine Primfaktorzerlegung von b. Dann gibt es ein $n \in \mathbb{N}$ so, daß $b^n = da$ mit $d \in A$. Also ist

$$v^n q_1^{nc_1} \cdots q_s^{nc_s} = dup_1^{b_1} \cdots p_r^{b_r}.$$

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

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 dieser Proposition, daß a genau dann reduziert ist, wenn das von a erzeugte Hauptideal (a) reduziert ist.

Proposition 3.6 *Seien k ein algebraisch abgeschlossener Körper und $f \in k[y,z] \setminus k$ reduziert. Dann ist die Menge* $\mathrm{Sing}(f)$ *endlich.*

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

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

Nach Satz 3.4 ist $\mathrm{Sing}(f_i)$ endlich für $i = 1, \ldots, r$. Außerdem gibt es nach Satz 3.3 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 $i, j \in \{1, \ldots, r\}$. ■

3.2 Invarianten und Induktion

Wir fassen im folgenden $k[y,z]$ als Unterring von $k[[y,z]]$ auf. Damit können wir die Begriffe bzw. Ergebnisse von Kapitel 2 auch auf Polynome anwenden. Sei $f \in k[y,z] \setminus k$. Wenn $o = \operatorname{ord} f \geq 1$, dann setzen wir

$$s_0 f = s(f),$$

und $s_0 f = \infty$, wenn $\operatorname{ord} f = 0$. Für einen beliebigen Punkt $a = (a_1, a_2) \in \mathbb{A}^2$ definieren wir

$$s_a f = s_0 \tilde{f} \text{ mit } \tilde{f}(y,z) = f(y + a_1, z + a_2).$$

Proposition 3.7 *Sei $a \in \mathbb{A}^2$. Dann gilt:*

(i) *Wenn a ein regulärer Punkt von f ist, dann ist $s_a f = \infty$.*

(ii) *Wenn a ein singulärer Punkt von f ist, dann ist $s_a f \in S_o$ mit $o = \operatorname{ord}_a f$ und*

$$S_o = \{s = \frac{p}{q} \in \mathbb{Q}_+ \text{ mit } o \leq s, \text{ } p \text{ und } q \text{ prim und } 1 \leq q \leq o\} \cup \{\infty\}.$$

Beweis. zu (i): Folgt mit Proposition 2.17.
zu (ii): Siehe Proposition 2.5. ■

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

$$I = \bigcup_{o \in \mathbb{N}_0} \{o\} \times S_o \subset \mathbb{N}_0 \times (\mathbb{Q}_{\geq 0} \cup \{\infty\}).$$

Für einen Punkt $a \in \mathbb{A}^2$ ist dann die Invariante von f definiert als das Paar:

$$i_a f = (\operatorname{ord}_a f, s_a f) \in I.$$

Bezeichne $<_{lex}$ die lexikographische Ordnung auf I, d.h. $(o', s') <_{lex} (o, s)$ genau dann, wenn $o' < o$ oder ($o' = o$ und $s' < s$). Offensichtlich ist $<_{lex}$ 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

Proposition 3.8 *Die Menge I mit der Ordnung $<_{lex}$ 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 $p_1 : J \longrightarrow \mathbb{N}_0$ die Projektion auf die erste Komponente und $o = \min\{p_1(J)\} \subset \mathbb{N}_0$. Wenn $o = 0$ bzw. $o = 1$, dann ist $(0, \infty)$ bzw. $(1, \infty)$ das kleinste Element von J. Sei also $o \geq 2$. Setze $K = J \cap \{o\} \times S_o$ und

$$f : K \longrightarrow \mathbb{N} \cup \{\infty\}, (o, s) \longmapsto (o!)s.$$

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

In einer wohlgeordeneten Menge M mit Ordnung $<$ gilt nämlich

Proposition 3.9 (Indukionsprinzip) *Sei $A(m)$ eine Aussage über beliebige $m \in M$ und gelte: Aus $A(n)$ für $n < m$ folgt $A(m)$. Dann gilt $A(m)$ für alle $m \in M$.*

Beweis. Sonst gäbe es nämlich ein kleinstes $m \in M$ so, daß $A(m)$ nicht gilt. Aber dann gilt $A(n)$ für $n < m$ und damit nach Voraussetzung auch $A(m)$. ■

3.3 Aufgelöste Punkte

Sei $f \in k[y, z] \setminus k$. 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 $\operatorname{ord} g = 1$ und $\operatorname{ord} h = 0$ und ein $n \in \mathbb{N}$ gibt so, daß

$$f = g^n h. \tag{3.1}$$

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

Sei $f = cf_1^{b_1} \cdots f_r^{b_r}$ eine Primfaktorzerlegung von f. 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 $a \in \mathbb{A}^2 \setminus V(f)$ aufgelöst. Also ist

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

Mit Satz 3.6 folgt daher insbesondere:

Proposition 3.10 *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 in diesem Abschnitt beweisen, daß a genau dann ein aufgelöster Punkt von f ist, wenn $s_a f = \infty$. Nach einer Translation in $\mathbb{A}^2$ können wir uns im folgenden auf den Nullpunkt beschränken.

Satz 3.11 *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

$$f = \alpha^2\beta \text{ mit } \alpha, \beta \in k[[y,z]] \text{ und } \operatorname{ord}\alpha \geq 1.$$

Für $\operatorname{ord} f = 0$ und $\operatorname{ord} f = 1$ folgt daraus ein Widerspruch. Sei also $\operatorname{ord} f \geq 2$. 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 $\operatorname{ord}\partial_y f \geq 1$. Mit der Produktregel folgt

$$\partial_y f = \partial_y(\alpha^2\beta) = \alpha(\alpha\partial_y\beta + 2\beta\partial_y\alpha).$$

Daher ist α ein echter gemeinsamer Teiler von f und $\partial_y f$ in $k[[y,z]]$. Das ist aber ein Widerspruch zu Korollar 1.33. 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 $\operatorname{char} k = 0$. Für $\operatorname{char} k > 0$ folgt daraus wie im Beweis zu Satz 3.4 ein Widerspruch zur Irreduzibilität von f. ■

Wir erinnern hier kurz an ein Ergebnis des vorherigen Kapitels und leiten eine einfache Folgerung daraus ab, die wir für die Beweise der nächsten Propositionen benötigen. Bezeichne G die Gruppe der stetigen $k-$Algebraautomorphismen von $k[[y,z]]$ und $\mathfrak{m} = (y,z) \subset k[[y,z]]$. Sei $f \in k[[y,z]]$, $f \neq 0$, mit $s(f) = \infty$ und $o = \operatorname{ord} f \geq 1$. Nach Korollar 2.19 und Proposition 2.5 (v) gibt es ein $\varphi \in G$ mit

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

Also ist

$$f = \alpha^o e \text{ mit } e \in k[[y,z]] \text{ invertierbar}$$

und $\alpha = \varphi^{-1}(y) \in k[[y,z]]$ irreduzibel, weil $\operatorname{ord}\alpha = 1$ ist.

Proposition 3.12 *Seien k ein Körper und $f \in k[[y,z]]$, $f \neq 0$, mit $s(f) < \infty$ und $o = \operatorname{ord} f \geq 1$. Sei $n \in \mathbb{N}$. Dann ist $s(f^n) < \infty$.*

Beweis. Angenommen $s(f^n) = \infty$. Dann ist $f^n = \alpha^{on} e$ mit $\alpha = \varphi^{-1}(y)$ und φ wie oben. Aus der Eindeutigkeit der Primfaktorzerlegung folgt $f = \alpha^o \tilde{e}$. Also ist

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

und damit $s(f) = \infty$. Widerspruch. ■

Proposition 3.13 *Seien k ein algebraisch abgeschlossener Körper und $f \in k[y,z]$ irreduzibel mit $o = \operatorname{ord} f \geq 2$ (d.h. 0 ist ein singulärer Punkt von f). Dann ist $s_0 f < \infty$.*

Beweis. Indirekt. Sei $s_0 f = \infty$. Nach obiger Überlegung ist dann aber f als Potenzreihe nicht reduziert, da $o \geq 2$ ist. Also folgt ein Widerspruch zu Satz 3.11. ■

Proposition 3.14 *Seien k ein Körper und $f, g \in k[y,z]$ teilerfremd mit $f, g \in \mathfrak{m}$. Dann ist $s_0(fg) < \infty$.*

Beweis. Angenommen $s_0(fg) = \infty$. Dann ist

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

Aus der Eindeutigkeit der Primfaktorzerlegung in $k[[y,z]]$ folgt, daß α ein echter Teiler von f und g in $k[[y,z]]$ ist. Das ist ein Widerspruch zu Korollar 1.33. ■

Satz 3.15 *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. *$s_0 f = \infty$.*

Beweis. Sei zunächst 0 ein aufgelöster Punkt von f. Wenn $0 \notin V(f)$ ist, dann ist $s_0 f = \infty$ nach Definition von s_0. Sei also $0 \in V(f)$. Dann ist $f = g^n h$ wie in (3.1). Nach Proposition 2.17 ist $s_0 g = \infty$. 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

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

Damit ist $s_0 f = \infty$.

Sei umgekehrt $s_0 f = \infty$. Wenn $\operatorname{ord} f = 0$ ist, dann ist 0 nach Definition ein aufgelöster Punkt von f. Sei also $\operatorname{ord} f \geq 1$. Sei $f = c f_1^{b_1} \cdots f_r^{b_r}$ eine Primfaktorzerlegung von f. Angenommen es gibt $i, j \in \{1, \ldots, r\}$, $i \neq j$, mit $\operatorname{ord} f_i \geq 1$ und $\operatorname{ord} f_j \geq 1$. 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 $\operatorname{ord} h = 0$. Mit Propostion 2.15 ist dann aber $s_0 f = s_0(\tilde{f}\tilde{g}) = \infty$. Das ist ein Widerspruch zu Proposition 3.14. Also gibt es genau ein $i \in \{1, \ldots, r\}$ mit $\operatorname{ord} f_i \geq 1$. Angenommen es gilt $\operatorname{ord} f_i > 1$. Nach Voraussetzung und Proposition 2.15 gilt $s_0 f = s_0 f_i^{b_i} = \infty$. Nach Proposition 3.13 und Proposition 3.12 ist aber $s_0 f_i^{b_i} < \infty$. Widerspruch. Also ist $\operatorname{ord} f_i = 1$ und damit 0 ein aufgelöster Punkt von f. ■

3.4 Aufblasung eines Punktes

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

Sei k ein algebraisch abgeschlossener Körper. Bezeichne $k[y,z]$ den affinen Koordinatenring und $(a,b) \in k^2$ (versehen mit der Zariski-Topologie) die abgeschlossenen Punkte des $\mathbb{A}^2$. Wir betrachten zwei weitere affine Räume $U_1 = \mathbb{A}^2$ bzw. $U_2 = \mathbb{A}^2$. Seien

$$\bar{\pi}_1 : U_1 \longrightarrow \mathbb{A}^2, (a,b) \longmapsto (ab, b) \text{ bzw.}$$
$$\bar{\pi}_2 : U_2 \longrightarrow \mathbb{A}^2, (a,b) \longmapsto (a, ab).$$

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

$$\pi_1 : k[y,z] \longrightarrow k[y,z], f(y,z) \longmapsto f(yz, z) \text{ bzw.}$$
$$\pi_2 : k[y,z] \longrightarrow k[y,z], f(y,z) \longmapsto f(y, yz).$$

Wir definieren die offenen Mengen

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

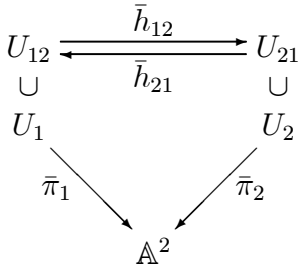
und die Abbildungen

$$\bar{h}_{12} : U_{12} \longrightarrow U_{21}, (a,b) \longmapsto (ab, 1/a)$$
$$\bar{h}_{21} : U_{21} \longrightarrow U_{12}, (a,b) \longmapsto (1/b, ab).$$

Dann ist

$$\bar{h}_{12}\bar{h}_{21} = Id \text{ und } \bar{h}_{21}\bar{h}_{12} = Id, \tag{3.2}$$

und wir haben folgendes kommutatives Diagramm:



Bezeichne $T = U_1 \sqcup U_2$ die topologische Summe von U_1 und U_2 (d.h. T ist als Menge die diskjunkte Vereinigung der beiden Mengen U_1 und U_2. 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

$$\bar{h}_{11} = id : U_{11} \longrightarrow U_{11} \text{ bzw. } \bar{h}_{22} = id : U_{22} \longrightarrow U_{22}. \tag{3.3}$$

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 (3.2) und (3.3) 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 $p : T \longrightarrow W'$ 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 *Aufblasung des Nullpunktes* von $\mathbb{A}^2$. 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 $\bar{\pi} : W' \longrightarrow \mathbb{A}^2$ 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.

Proposition 3.16 *Für $\bar{\pi} : W' \longrightarrow \mathbb{A}^2$ und $E = \bar{\pi}^{-1}(0)$ gilt:*

(i) $E \cap U_1 = V(z)$ *bzw.* $E \cap U_2 = V(y)$.

(ii) $E \simeq \mathbb{P}^1$.

(iii) $\bar{\pi} : W' \setminus E \longrightarrow \mathbb{A}^2 \setminus \{0\}$ *ist ein Isomorphismus.*

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

zu (ii): Man prüft leicht nach, daß die Abbildung $\bar{\varphi} : E \longrightarrow \mathbb{P}^1$ 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 $\bar{\pi}(w) = (ab,b) \in \mathbb{A}^2 \setminus \{0\}$. Analog schließt man für $w \in (W' \setminus E) \cap U_2$. Wir definieren $\bar{\varphi} : \mathbb{A}^2 \setminus \{0\} \longrightarrow W' \setminus E$ durch

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

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

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

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

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

3.5 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. $o = \operatorname{ord} f \geq 1$. 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

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

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

$$\begin{aligned} \bar{\pi}^{-1}(C) \cap U_1 = \{a = (a_1,a_2) \in U_1 \text{ mit } \bar{\pi}_1(a) = (a_1a_2, a_2) \in C\} = \\ = \{a \in U_1 \text{ mit } f(a_1a_2, a_2) = 0\} = V(f^*). \end{aligned}$$

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

$$f^* = f(yz, z) = \sum_\alpha c_\alpha y^{\alpha_1} z^{\alpha_1+\alpha_2} = \tag{3.4}$$
$$= z^o \sum_\alpha c_\alpha y^{\alpha_1} z^{\alpha_1+\alpha_2-o} = z^o f'(y, z) = z^o f'.$$

Dann ist

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

Wir nennen f' die *Strikt-Transformierte* f.

Um die Primfaktoren von f' zu untersuchen, überlegen wir uns zunächst, daß f' nicht durch z teilbar ist. Wir schreiben

$$f = f_o + f_{o+1} + \cdots + f_d \text{ mit } d = \deg f$$

als Summe von homogenen Polynomen. Dann ist

$$f^* = f(yz, z) = f_o(yz, z) + f_{o+1}(yz, z) + \cdots + f_d(yz, z) =$$
$$= z^o(f_o(y, 1) + z f_{o+1}(y, 1) + \cdots + z^{d-o} f_d(y, 1)) = z^o f'$$

mit $f_o(y, 1) \neq 0$, also $z \nmid f'$. Aus dieser Darstellung der Strikt-Transformierten von f folgt

Proposition 3.17 *Es gilt*

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

Insbesondere ist diese Menge endlich.

Proposition 3.18 *Sei $(f) \neq (z)$ und f irreduzibel bzw. reduziert. Dann ist auch f' irreduzibel bzw. reduziert.*

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

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

Wenn wir nun y/z für y einsetzen, ist mit (3.4)

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

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

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

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. ■

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

$$i_{a'}f' = i_0 f'(y+t,z) = i_0 v(f')$$

mit

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

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 $i_{a'}f'$ zu berechnen. Sei dazu

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

Proposition 3.19 *Dann 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. Proposition 3.25).

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 $\operatorname{ord} w(f) = o$) folgt dann

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

■

3.6 Invarianten fallen bei Aufblasung

Seien k ein algebraisch abgeschlossener Körper, $f \in k[y,z] \setminus k$ und 0 ein nicht aufgelöster Punkt von f. Wir betrachten die Aufblasung des Nullpunktes im $\mathbb{A}^2$. In diesem Abschnitt zeigen wir, daß die Invariante der Strikt-Transformierten von f in jedem Punkt des exzeptionellen Divisors kleiner als die Invariante von f im Nullpunkt ist, also daß $i_{a'}f' < i_0 f$ für alle $a' \in E \cap U_1$ gilt.

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 Proposition 3.19

$$i_{a'}f' = i_0 l_t(f)' = (\operatorname{ord} l_t(f)', s_0 l_t(f)'). \tag{3.5}$$

Wir können also, um die Invariante von f' in jedem Punkt von $E \cap U_1$ zu untersuchen, auch $\operatorname{ord} l_t(f)'$ bzw. $s_0 l_t(f)'$ für $t \in k$ betrachten. Wir werden dies im folgenden gleich für eine beliebige Potenzreihe tun. Um die Invariante in jedem Punkt des exzeptionellen Divisors zu kennen, müssen wir auch noch $i_0 f_2'$ untersuchen.

Seien R bzw. R' Potenzreihenringe in zwei Variablen über einem Körper k und $\mathbf{y} = (y,z)$ ein reguläres Parametersystem von R bzw. R'. Sei $f \in R$ mit $f \neq 0$, $o = \operatorname{ord} f \geq 1$ und

$$f = f(y,z) = \sum_{\alpha} c_\alpha y^{\alpha_1} z^{\alpha_2}. \tag{3.6}$$

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

$$f^* = \pi_1(f) = f(yz,z) = \sum_{\alpha} c_\alpha y^{\alpha_1} z^{\alpha_1+\alpha_2} =$$
$$= z^o \sum_{\alpha} c_\alpha y^{\alpha_1} z^{\alpha_1+\alpha_2-o} = z^o f'(y,z) = z^o f'$$

und

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

Mit diesen Bezeichnungen folgt

Proposition 3.20 *Es gilt:*

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

(ii) $\operatorname{ord} f' \leq o$.

Beweis. zu (ii): Sei $\alpha \in \Delta_{\mathbf{y}}(f)$ mit $\alpha_1+\alpha_2 = o$, dann ist $\alpha_1+(\alpha_1+\alpha_2-o) \leq o$. Also ist $\operatorname{ord} f' \leq o$. ■

Proposition 3.21 *Sei* $s(f) = o$. *Dann sind* $\operatorname{ord} l_t(f)' < o$ *für jedes* $t \in k$ *und* $\operatorname{ord} f_2' < o$.

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

Außerdem gibt es einen Term $c_\alpha y^{\alpha_1} z^{\alpha_2}$ von f mit $\alpha_1 + \alpha_2 = o$ und $\alpha \neq (0, o)$ (sonst wäre $s(f) \geq s_{\mathbf{y}} p(f) > o$ mit p der Vertauschung von y und z), und damit ist auch $\operatorname{ord} f_2' < o$. ■

Proposition 3.22 *Seien* $s(f) > o$ *und* $\mathbf{y} = (y, z)$ *ein reguläres Parametersystem von* R *so, daß* $s_{\mathbf{y}} f > o$. *Dann sind* $\operatorname{ord} l_t(f)' = 0$ *für* $t \in k$, $t \neq 0$, *und* $\operatorname{ord}(f_2') = 0$.

Beweis. Wie im Beweis zu Lemma 2.10 erkennt man, daß in $l_t(f)$ der Koeffizient von z^o nicht Null ist. Also ist $\operatorname{ord} l_t(f)' = 0$. Da $f_o = cy^o$, $c \neq 0$, ist auch $\operatorname{ord}(f_2') = 0$. ■

Proposition 3.23 $\operatorname{ord} f' < o$ *genau dann, wenn* $s_{\mathbf{y}} f < 2o$.

Beweis. Angenommen $s = s_{\mathbf{y}} f \geq 2o$. Sei $\alpha \in \Delta_{\mathbf{y}}(f)$. Dann ist

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

und damit

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

Also folgt mit Proposition 3.20, daß $\operatorname{ord} f' \geq o$. Wenn $s_{\mathbf{y}} f < 2o$, dann gibt es ein $\alpha \in NP_{\mathbf{y}}(f)$, $\alpha \neq (o, 0)$, mit

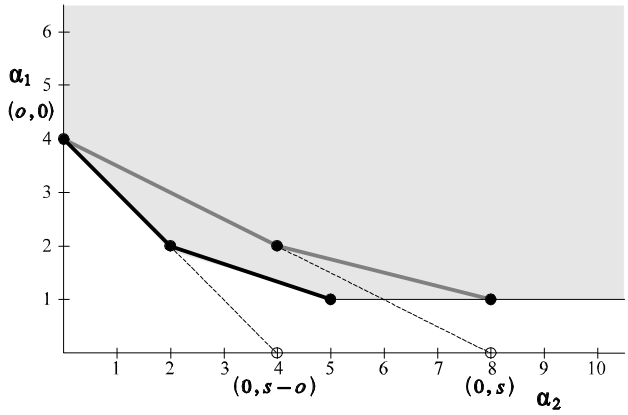
$$\frac{o\alpha_2}{o - \alpha_1} < 2o.$$

Für dieses α ist dann $\alpha_1 + (\alpha_1 + \alpha_2 - o) < o$, also ist $\operatorname{ord} f' < o$. ■

Wir erinnern an eine Notation von Abschnitt 2.3, die wir im folgenden verwenden. Seien f wie in (3.6) und $t \in \mathbb{R}$, $t \geq o$. Dann schreiben wir

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

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



Proposition 3.24 *Sei $\infty > s_{\mathbf{y}} f \geq 2o$. Dann ist (siehe Abbildung 3.6)*

$$s_{\mathbf{y}} f' = s_{\mathbf{y}} f - o.$$

Beweis. Seien $s = s_{\mathbf{y}} f$ und $s' = s - o$. Nach der vorherigen Proposition und Propostion 3.20 ist $o = \operatorname{ord} f'$. 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 $\alpha \neq (o, 0)$. Dann ist

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

und deshalb

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

Also ist

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

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

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

und damit folgt wie zuvor

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

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

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

Mit Proposition 2.6 folgt die Behauptung. ■

Proposition 3.25 *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 Einsetzungshomomorphismus. Dann ist*

$$\begin{array}{ccc} R' & \xrightarrow{l} & R' \\ {\scriptstyle \pi_1}\uparrow & & \uparrow{\scriptstyle \pi_1} \\ R & \xrightarrow[m]{} & R \end{array}$$

kommutativ, und es gilt

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

Beweis. Nachrechnen, analog zum Beweis von Proposition 3.19. ■

Lemma 3.26 *Seien $\infty > s(f) \geq 2o$ und $\mathbf{y} = (y, z)$ ein reguläres Parametersystem von R so, daß $s_{\mathbf{y}} f = s(f)$. Dann wird $s(f')$ durch $\mathbf{y} = (y, z)$ realisiert, d.h.*

$$s(f') = s_{\mathbf{y}} f'.$$

Beweis. Angenommen $s(f') > s_{\mathbf{y}} f' = s'$. Dann gibt es ein $l \in L'$ und ein $p \in P'$ mit $s_{\mathbf{y}} lp(f') > s'$. Wenn $s' > o$, dann ist p die Identität. Wenn $s' = o$ und p die Vertauschung von y und z ist, dann folgt, da f' $y-$allgemein der Ordnung o ist, mit Satz 2.13, daß

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

Also ist

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

Wir können daher annehmen, daß p die Identität ist. Mit m wie in der vorherigen Proposition folgt

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

Dann ist $s_{\mathbf{y}}m(f) \geq 2o$ (sonst wäre nach Proposition 3.23 $\operatorname{ord}(f') = \operatorname{ord} l(f') = \operatorname{ord} m(f)' < o$). Mit Proposition 3.24 folgt dann

$$s(f) - o = s' < s_{\mathbf{y}}l(f') = s_{\mathbf{y}}m(f)' = s_{\mathbf{y}}m(f) - o \leq s(f) - o,$$

also ein Widerspruch. ■

Satz 3.27 *Seien $f \in \mathfrak{m}$, $f \neq 0$, $o = \operatorname{ord} f$ und $\infty > s(f) \geq 2o$. Dann ist*

$$s(f') = s(f) - o.$$

Beweis. Klar nach dem vorherigen Lemma und Proposition 3.24. ■

Wir wenden jetzt die obigen Ergebnisse auf die Situation am Beginn dieses Abschnittes an. Seien also k ein algebraisch abgeschlossener Körper, $f \in k[y,z] \setminus k$, $o = \operatorname{ord} f$ und 0 ein nicht aufgelöster Punkt von f. Wenn $s_0 f = o$ ist, dann ist mit (3.5) und Proposition 3.21

$$i_{a'} f' < i_0 f \text{ für alle } a' \in E \cap U_1.$$

Weiters gilt $i_0 f'_2 < i_0 f$. Sei nun $o < s_0 f$. Nach Satz 3.15 ist $s_0 f < \infty$. Daher können wir mit Satz 2.20 annehmen, daß nach einem polynomialen Koordinatenwechsel $s_0 f = s_{\mathbf{y}} f$ gilt. Proposition 3.22 zeigt, daß es genügt, $i_0 f'$ und $i_0 f$ zu vergleichen. Wenn $s_0 f < 2o$ ist, dann ist nach Proposition 3.23 $\operatorname{ord} f' < \operatorname{ord} f$ und damit $i_0 f' < i_0 f$. Sei $s_0 f \geq 2o$. Dann ist $\operatorname{ord} f' = \operatorname{ord} f$ und mit dem vorherigen Satz $s_0 f' = s_0 f - o < s_0 f$. Also gilt wieder $i_0 f' < i_0 f$.

Zum Abschluß deuten wir noch an, wie mit den bisherigen Ergebnissen bewiesen werden kann, daß durch eine endliche Folge von Aufblasungen von Punkten die singulären Punkte einer "ebenen" algebraischen Kurve aufgelöst werden können. Seien k ein algebraisch abgeschlossener Körper und $f \in k[y,z] \setminus k$. Nach Proposition 3.10 gibt es nur endlich viele nicht aufgelöste Punkte von f. Sei a ein nicht aufgelöster Punkt von f. Nach einer Translation in $\mathbb{A}^2$ können wir annehmen, daß a der Nullpunkt ist. Wir blasen den Nullpunkt auf. Proposition 3.17 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 obiger Überlegung die Invariante der Strikt-Transformierten in a' kleiner als die Invariante von f im Nullpunkt. Durch Induktion über die Invariante (vgl. Abschnitt 3.2) folgt die Behauptung.

Literaturverzeichnis

[1] Abhyankar, S. S.: Desingularization of plane curves, Proc. Symp. in Pure Math. **40**, Part 1, AMS, 1983, 1-45.

[2] Abhyankar, S. S.: Resolution of singularities in various characteristics, Current Science, Vol. 63, No. 5, 1992, 229-232.

[3] Brieskorn, E., Knörrer, H.: Ebene algebraische Kurven, Birkhäuser, Basel, Boston, Stuttgart, 1981.

[4] Cossart, V., Giraud, J., Orbanz, U.: Resolution of Surface Singularities, Lect. Notes in Math. 1101, Springer-Verlag, Berlin Heidelberg New York, 1984.

[5] Cox, D., Little, J., O'Shea, D.: Ideals, varieties, and algorithms, Springer-Verlag, New York, 1992.

[6] Fulton, W.: Algebraic Curves, Benjamin, New York, Amsterdam, 1969.

[7] Hartshorne, R.: Algebraic Geometry, Springer-Verlag, Berlin Heidelberg New York, 1977.

[8] Hauser, H.: Resolution techniques, preprint 2000.

[9] Mumford, D.: The Red Book of Varieties and Schemes, Lect. Notes in Math. 1358, Springer-Verlag, 1988.

[10] Orzech, G., Orzech, M.: Plane algebraic curves, Marcel Dekker, New York, 1981.

[11] Seidenberg, A.: Elements of the theory of algebraic curves, Addison-Wesley, Menlo Park, California, 1968.

[12] Shafarevich, I. R.: Basic Algebraic Geometry 1 und 2, Second Edition, Springer-Verlag, Berlin Heidelberg New York, 1994.

[13] Atiyah, M. F., Macdonald I. G.: Introduction to Commutative Algebra, Addison-Wesley, Reading, Mass., 1969.

[14] Bosch, S.: Algebra, Springer-Verlag, Berlin Heidelberg New York, 1991.

[15] Brüske, R., Ischebeck, F.,Vogel, F.: Kommutative Algebra, BI Wissenschaftsverlag, Mannheim, Wien, Zürich, 1989.

[16] Grauert, H., Remmert, R.: Analytische Stellenalgebren, Springer-Verlag, Berlin Heidelberg New York, 1971.

[17] Lang, S.: Algebra, 2nd Edn., Addison-Wesley, Menlo Park, California, 1971.

[18] Matsumura, H.: Commutative Algebra, Benjamin, New York, 1970.

[19] Nagata, M.: Local Rings, Robert E. Krieger Publishing Company, New York, 1975.

[20] Ruiz, J., M.: The basic theory of power series, Vieweg, Braunschweig, 1993.

[21] Scheja, G., Storch, U.: Lehrbuch der Algebra, Teil 2, B. G. Teubner, Stuttgart, 1988.

[22] Zariski, O., Samuel, P.: Commutative Algebra, 2 vols, D. Van Nostrand Company, New Jersey, 1960.