Johannes Gutenberg-Universität Mainz
Sommersemester 2016

Ebene algebraische Kurven

Ergänzungsvorlesung von Prof. Dr. Duco van Straten

Vorlesung Nr. 10 vom 13. Mai 2016

3.6 Algebraische Lupe: Potenzreihen

Im letzten Kapitel haben wir gesehen, dass schwierig aussehende Gleichungen eine interessante Topologie und Geometrie aufweisen. In diesem Kapitel möchten wir nun einen algebraischen Zugang dazu aufzeigen.

Beispiel 3.6.1. Betrachten wir das Polynom $f(X,Y) = Y^2 - X^2(1+X)$. Dies ist eine kubische Kurve mit einem Knotenpunkt.

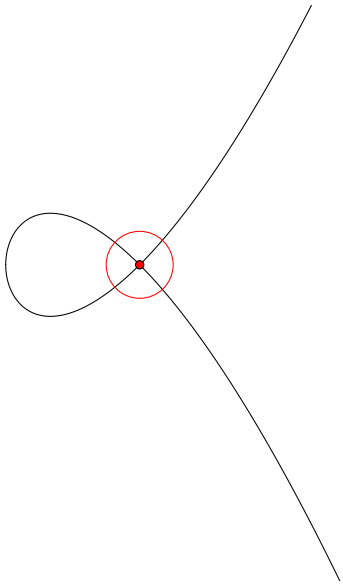

Abbildung 1: „*Newton'scher Knoten*“

Das Polynom f von Grad 3 ist irreduzibel. Wäre es reduzibel, so wären die Faktoren von Grad 1 und 2. Ein Polynom von Grad 1 bildet aber eine Gerade. Demnach müsste die Kurve eine Gerade enthalten, was aber nicht der Fall ist.

Trotzdem sehen wir zwei „Zweige“ durch 0. Wir möchten die Kurve aber eigentlich als Produkt von zwei Linearfaktoren faktorisieren. Da f allerdings ein irreduzibles Polynom ist, können wir dies nicht. Was wir aber können, ist, unseren Bereich zu vergrößern.

Schreiben wir dazu das Polynom als Produkt von zwei Linearfaktoren

$$f = \left(Y - X\sqrt{1+X}\right) \cdot \left(Y + X\sqrt{1+X}\right).$$

Fassen wir dies als Potenzreihe auf, so ergibt sich

$$\sqrt{1+X} = 1 + \frac{1}{2}X - \frac{1}{8}X^2 + \frac{1}{16}X^3 - \frac{5}{128}X^4 + \dots.$$

Diese hat den Konvergenzradius $R = 1$.

Wenn wir also den Bereich der Polynome verlassen und zum Bereich der Potenzreihen übergehen, gelingt es uns plötzlich, diese Gleichung zu faktorisieren. Daher werden wir den Rechenbereich vergrößern und den Polynomring in einer Variablen zum Potenzreihenring erweitern.

Definition 3.6.2. Der *Ring der formalen Potenzreihen in* X ist definiert als

$$\mathbb{C}[\![X]\!] := \left\{ f := \sum_{i=0}^{\infty} a_i X^i \mid a_i \in \mathbb{C} \text{ beliebig} \right\},$$

das heißt $f = a_0 + a_1 X + a_2 X^2 + ...$, wobei die $a_i \in \mathbb{C}$ beliebig sind und f nicht konvergieren muss.

Definition 3.6.3. Die *Ordnung von* f ist definiert als

$$\operatorname{Ord} f := \min\{k \mid a_k \neq 0\}.$$

Bemerkung 3.6.4. Wir vereinbaren die Konvention $\operatorname{Ord} 0 := \infty$.
Außerdem ist die Ordnung natürlich multiplikativ.

Beispiel 3.6.5. $\operatorname{Ord}\ (X^2 + X^3) = 2$, das heißt die Ordnung der Summe $f+g$ kann natürlich größer sein als die minimale Ordnung von $f = X^2$ und $g = X^3$.

Die Struktur dieses Rings $\mathbb{C}[\![X]\!]$ ist äußerst einfach, da nur in Körpern einfacher zu rechnen ist, als in diesem Ring.
Was genau meinen wir damit? Was uns nun beschäftigt ist die Frage, wann wir durch eine Potenzreihe teilen können? Anders formuliert: Was sind die Einheiten?

Lemma 3.6.6. *In* $\mathbb{C}[\![X]\!]$ *gilt*

$$f = a_0 + a_1 X + ... \text{ ist eine Einheit } \Leftrightarrow a_0 \neq 0$$
$$(\Leftrightarrow \operatorname{Ord} f = 0).$$

Das heißt also, wir haben eine Einheit in $\mathbb{C}[\![X]\!]$ genau dann, wenn wir durch Potenzreihen teilen können. Demnach schauen wir uns jetzt an, durch welche Potenzreihen wir teilen können.

Beweis. Die Hinrichtung ist klar.
Sei also $a_0 \neq 0$. Wir betrachten

$$\frac{1}{f} = \frac{1}{a_0 + a_1 X + ...} = \frac{1}{a_0} \cdot \frac{1}{\left(1 + \frac{a_1}{a_0} X + ...\right)} = \frac{1}{a_0 (1 + g)}$$

mit $g := 1 + \frac{a_1}{a_0} X + ... \in \mathbb{C}[\![X]\!]$. Wenden wir nun die geometrische Reihe an, so erhalten wir

$$\frac{1}{a_0 (1 + g)} = \frac{1}{a_0} \cdot \left(1 - g + g^2 - g^3 \pm ...\right).$$

Für g gilt folgende Identität

$$g = x \cdot h = \frac{1}{a_0} \cdot \left(1 - xh + x^2 h^2 - x^3 h^3 \pm ...\right)$$

mit einer Potenzeihe $h \in \mathbb{C}[\![X]\!]$. Auf diese Weise bekommen wir also eine Potenzreihe. □

Bemerkung 3.6.7. Notieren wir einige nützliche Eigenschaften zum Ring der formalen Potenzreihen $\mathbb{C}[\![X]\!]$.

- Wenn die Einheiten *einfach* sind, können wir jedes $f \in \mathbb{C}[\![X]\!]$ als

$$f = x^k \cdot u(x)$$

schreiben mit Ord $f = k$ und $u(x)$ eine Einheit. Denn nach vorigem Lemma können wir unsere Potenzreihe wie folgt umschreiben

$$f = a_k x^k + a_{k-1}x^{k+1} + \ldots \quad = \underbrace{x^k}_{\text{Element mit Ord } f} \cdot \underbrace{(a_k + a_{k+1}x + \ldots)}_{\text{Einheit } u(x)}.$$

Das heißt, jedes Element in diesem Ring hat eine Darstellung dieser Form.

- Nach vorigem Punkt ist die Teilbarkeit in dem Ring $\mathbb{C}[\![X]\!]$ wieder einfach. Es gilt

$$f \mid g \Leftrightarrow \text{Ord } f \leq \text{Ord } g,$$

denn $f = x^k \cdot u(x)$ und $g = x^l \cdot v(x)$ mit $u(x), v(x)$ Einheiten und Ord $f = k$, Ord $g = l$, wobei offensichtlich $l \geq k$ ist. Dann haben wir

$$\frac{g}{f} = x^{l-k} \cdot \frac{v(x)}{u(x)}.$$

Das bedeutet, die Teilbarkeit von solchen Reihen hängt nur von dem Verhältnis der Ordnungen beider Funktionen ab.

- Das heißt auch, dass jedes Ideal in diesem Ring ein Hauptideal ist. Haben wir nun das Ideal (X^k), also alle Funktionen, die teilbar sind durch X^k, dann sind das alle Funktionen mit Ordnung $\geq k$. Diese füllen den Ring auf, das bedeutet wir haben eine Filtrierung

$$\mathbb{C}[\![X]\!] \supset (X) \supset \left(X^2\right) \supset \left(X^3\right) \supset \cdots \supset (0)$$

mit Idealen $(X), (X^2), (X^3), \ldots$ und Ord $X \geq 1$, Ord $X^2 \geq 2$, Ord $X^3 \geq 3, \ldots$.
Somit gibt es eine absteigende Kette von Idealen (*noethersch*) und diese Ideale sind Hauptideale. Technisch betrachtet ist das ein *diskreter Bewertungsring*.

- Der Quotientenkörper $\mathcal{Q}(\mathbb{C}[\![X]\!])$ des Potenzreihenrings $\mathbb{C}[\![X]\!]$ ist definiert durch

$$\mathcal{Q}(\mathbb{C}[\![X]\!]) := \mathbb{C}[\![X]\!]\left[\frac{1}{X}\right] = \{f = \sum_{i \geq -N}^{\infty} a_i X^i\} \ni \frac{a_{-10}}{x^{10}} + \ldots + \frac{a_{-1}}{X} + a_0 + a_1 X + a_2 X^2 + \ldots .$$

Das ist offensichtlich ein nullteilerfreier Ring, sogar ein Körper. Nämlich der Quotientenkörper, der auch Brüche von Potenzreihen enthält. Nun gibt es natürlich eine Potenzreihe in X, somit liegen in diesem Ring auch die Inversen von X. Damit ist er geringfügig größer als der Potenzreihenring, da wir hier zusätzlich endlich viele negative Potenzen haben. Man nennt diesen Körper den *Körper der formalen Laurent-Reihe*, der hauptsächlich in der Funktionentheorie Anwendung findet.

Wir werden hier in diesem Ring arbeiten.

- Es gibt viele interessante Ringe zwischen $\mathbb{C}[X]$ und $\mathbb{C}[\![X]\!]$.

– Der *Ring der konvergenten Potenzreihen* ist definiert durch

$$\mathbb{C}\{X\} := \{f \in \mathbb{C}[\![X]\!] \mid \exists \rho, \text{ so dass } \sum_{i=1}^{\infty} |a_i|\ \rho^i < \infty\}.$$

Wir stellen hier also eine Konvergenzbedingung auf. Solche Potenzreihen kann man als Funktionen auf einer Kreisscheibe von Radius ρ in der komplexen Ebene auffassen. Aber jede der Potenzreihen hat einen eigenen Konvergenzradius, der durch Reihenentwicklung eindeutig festgelegt ist. Das heißt, es ist ein Unterring der formalen Potenzreihen.

– Der *Ring der algebraischen Potenzreihen* ist definiert durch

$$\mathbb{C} < X > := \{f \in \mathbb{C}[\![X]\!] \mid f \text{ ist algebraische Potenzreihe}\}.$$

– Der *Ring der rationalen Potenzreihen* ist definiert durch

$$\mathbb{C}[X]_{(X)} := \{f \in \mathbb{C}[\![X]\!] \mid f \text{ ist rationale Potenzreihe}\}.$$

Das heißt, wir haben eine rationale Funktion $f(X) = \frac{P(X)}{Q(X)}$ mit $Q \notin (X)$ und insbesondere $Q(0) \neq 0$, die in eine Potenzreihe entwickelbar ist.

Sei R ein Ring und $\wp \subset R$ ein Primideal, dann ist

$$R_\wp = \{\frac{r}{s} \mid r, s \in R, s \notin \wp\}$$

definiert als die *Lokalisierung von R nach $\wp$*.

Folglich ist $\mathcal{Q}(\mathbb{C}[\![X]\!])$ die Lokalisierung vom Potenzreihenring $\mathbb{C}[X]$ nach dem Primideal (X).

Einfach formuliert bedeutet das, wir lassen im Nenner Dinge zu, die nicht im Ideal liegen. Wir erlauben somit rationale Funktionen im Nenner. Im Ideal (X) zu liegen heißt damit, teilbar durch X zu sein.

Für die soeben definierten Ringe folgt nun

$$\mathbb{C}[X] \subsetneq \mathbb{C}[X]_{(X)} \subsetneq \mathbb{C} < X > \subsetneq \mathbb{C}\{X\} \subsetneq \mathbb{C}[\![X]\!].$$

Diese Ringe enthalten jeweils Elemente der folgenden Formen

- $\mathbb{C}[X] \ni 1 + x + x^2 + ... + x^n = f$
- $\mathbb{C}[X]_{(X)} \ni 1 + x + x^2 + ... = \frac{1}{1-x}$
- $\mathbb{C} < X > \ni \sqrt{1+x} = 1 + \frac{1}{2}x - \frac{1}{16}x^2 + ...$ mit Konvergenzradius $R = 1$
- $\mathbb{C}\{X\} \ni e^x = 1 + x + \frac{x^2}{2!} + ...$ mit Konvergenzradius $R = \infty$
- $\mathbb{C}[\![X]\!] \ni 1 + 1!\ X + 2!\ X^2 + ...$ mit Konvergenzradius $R = 0$

Das sind also die Werkzeuge, die wir benutzen werden, um auf singuläre Punkte und Schnittpunkte einzuzoomen, da man in diesem Bereich sozusagen mehr sehen kann.

3.7 Hensel'sches Lemma

Sei $\mathcal{C}$ eine Kurve.

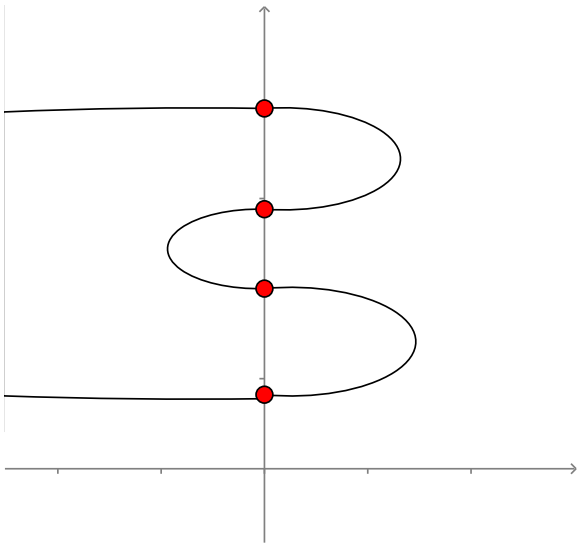

Abbildung 2: Kurve $\mathcal{C}$

Sei $f(X,Y) = Y^d + a_1(X)Y^{d-1} + ... + a_d(X) \in \mathbb{C}[X,Y]$. Dann ist $f(0,Y) \in \mathbb{C}[Y]$. Solche Polynome können wir vollständig in Linearfaktoren zerlegen, das heißt

$$f(0,Y) = \prod_{i=1}^{d} (Y - c_i).$$

Es gilt $f \in \mathbb{C}[X,Y] \subset \mathbb{C}[\![X]\!][Y]$.

Bemerkung 3.7.1. Wir möchten nun die Polynome $f \in \mathbb{C}[X,Y]$ als Polynome mit Koeffizienten in Potenzreihen auffassen, also als Elemente des Rings $\mathbb{C}[\![X]\!][Y]$.

Es gilt

$$\mathbb{C}[\![X]\!][Y] \neq \mathbb{C}[Y][\![X]\!].$$

Beispielsweise ist $1 + \underline{Y}X + \underline{Y^2}X^2 + \underline{Y^3}X^3 + \underline{Y^4}X^4 + ... \in \mathbb{C}[Y][\![X]\!]$, aber nicht in $\mathbb{C}[\![X]\!][Y]$.

Unser Ziel ist nun Folgendes: Wir möchten aus Polynomen $f(0,Y) = \prod_{i=1}^{d}(Y - c_i)$ in einer Variablen mit $c_i \neq c_j$ für $i \neq j$ Polynome

$$f(X,Y) = \prod_{i=1}^{d} (Y - c_i(X))$$

in zwei Variablen mit Potenzreihen $c_i(X) \in \mathbb{C}[\![X]\!]$ bekommen.

Satz 3.7.2. *(Hensel'sches Lemma) Sei* $f = Y^d + a_1(X)Y^{d-1} + ... + a_d(X) \in \mathbb{C}[\![X]\!][Y]$ *ein Polynom mit Koeffizienten* $a_i(X) \in \mathbb{C}[\![X]\!]$. *Angenommen,* $f(0,Y) = g_0 \cdot h_0$ *mit* $g_0, h_0 \in \mathbb{C}[Y]$ *und Grad* $g_0 = p$, *Grad* $h_0 = q$ *(mit* $p + q = d$*) sowie* $ggT(g_0, h_0) = 1$.

Dann existieren Polynome $g(X,Y) = g_0 + g_1X + g_2X^2 + ...$ *mit* $g_i \in \mathbb{C}[Y]$ *und Grad* $g_i \leq p - 1$ *und* $h(X,Y) = h_0 + h_1X + h_2X^2 + ...$ *mit* $h_i \in \mathbb{C}[Y]$ *und Grad* $h_i \leq q - 1$ *mit* $f(X,Y) = g(X,Y) \cdot h(X,Y)$.

Beweis. Gegeben sei

$$\begin{aligned} f &= Y^d + a_1(X)Y^{d-1} + \ldots + a_d(X) \text{ mit Potenzreihen } a_i(X) \in \mathbb{C}[\![X]\!] \\ &= f_0 + f_1X + f_2X^2 + \ldots \text{ mit Polynomen } f_i \in \mathbb{C}[Y] \end{aligned}$$

und Grad $f_i \leq d-1$ für $i \geq 1$.

Angenommen, wir haben bereits $g_1, g_2, \ldots, g_k \in \mathbb{C}[Y]$ und $h_1, h_2, \ldots, h_k \in \mathbb{C}[Y]$ konstruiert mit

$$\left(\sum_{i=0}^{k} g_iX^i\right)\left(\sum_{j=0}^{k} h_jX^j\right) = f_0 + \ldots + f_kX^k \mod X^{k+1}.$$

Dann suchen wir g_{k+1} und h_{k+1}. Wir haben

$$\left(g_0 + g_1X + \ldots + g_{k+1}X^{k+1}\right)\left(h_0 + h_1X + \ldots + h_{k+1}X^{k+1}\right) = f_0 + f_1X + \ldots + f_{k+1}X^{k+1} \mod X^{k+2}.$$

Was passiert nun mit dem X^{k+1}-Term?

Wir wissen, alle Terme vorher heben sich weg. Bleibt also nur noch der Term X^{k+1}. Das heißt, wir bekommen

$$g_0\underline{h_{k+1}} + g_1h_k + \ldots + g_kh_1 + \underline{g_{k+1}}h_0 = f_{k+1}.$$

Das können wir aber auch als

$$g_0\underline{h_{k+1}} + h_0\underline{g_{k+1}} = f_{k+1} - (g_1h_k + \ldots + g_kh_1)$$

schreiben. Damit haben wir ein Polynom vom Grad $\leq d-1$.

Nach Voraussetzung ist ggT $(g_0, h_0) = 1 = a\,g_0 + b\,h_0$. Wir können die Polynome somit mit Hilfe ihrer Bézout-Koeffizienten darstellen. Demnach ist dann für alle Polynome $A\,g_0 + B\,h_0$ der Grad $\leq p+q-1$, da Grad $A \leq q-1$ und Grad $B \leq p-1$ voraussetzbar sind. Falls der Grad größer ist, machen wir zuerst Teilung mit Rest. Somit können wir jedes Polynom beliebigen Grades auf diese Weise kombinieren.

Wir können also immer h_{k+1} und g_{k+1} finden. Folglich können wir die Faktorisierung fortsetzen. □

Folgerung 3.7.3. Setzen wir $X = 0$ in $f(X, Y)$, so haben wir

$$f(0, Y) = \prod_i (Y - c_i)$$

für $c_i \neq c_j$ und $i = 1, \ldots, d$. Dann hat der erste Faktor keinen gemeinsamen Teiler mit dem Produkt aller anderen Faktoren. Das heißt, wir können das Produkt als

$$f(0, Y) = (Y - c_i) \cdot \prod_{i>1}^{d} (Y - c_i)$$

schreiben. Diese beiden Terme sind dann unser g und h. Somit finden wir Reihen $f(X, Y)$ mittels Induktion, indem wir das Hensel'sche Lemma anwenden und die Faktoren liften. Die Bedingungen hierfür sind erfüllt, da die Nullstellen verschieden sind und wir somit immer ggT$(g_k, h_k) = 1$ haben. Damit erhalten wir:

$$c_i(x) \in \mathbb{C}[\![X]\!] \text{ mit } f(X, Y) = \prod_{i=1}^{d} (Y - c_i(x)).$$

Bemerkung 3.7.4. Die Reihen, die man bekommt, sind natürlich eindeutig. Man kann sogar zeigen, dass $c_i(x) \in \mathbb{C}\{X\}$ gilt, was bedeutet, dass diese konvergieren. Damit haben wir eine Konstruktion formaler Reihen.

Man kann auch zeigen, dass $c_i(x) \in \mathbb{C} < X >$. Das ist eigentlich logisch, weil die c_i's Lösungen einer algebraischen Gleichung sind. Noch unklar ist, aus welchem Grund man immer diese Faktorisierung wählt. Das heißt, die Reihen, die man erhält, sind zwar formale Potenzreihen, aber sie konvergieren. Das entspricht dem *Satz über implizierte Funktionen* aus der Analysis.

3.8 ohne Namen

Wir haben im letzten Kapitel gesehen, dass wir, sofern die Nullstellen verschieden sind, diese mit dem Hensel'schen Lemma liften können.

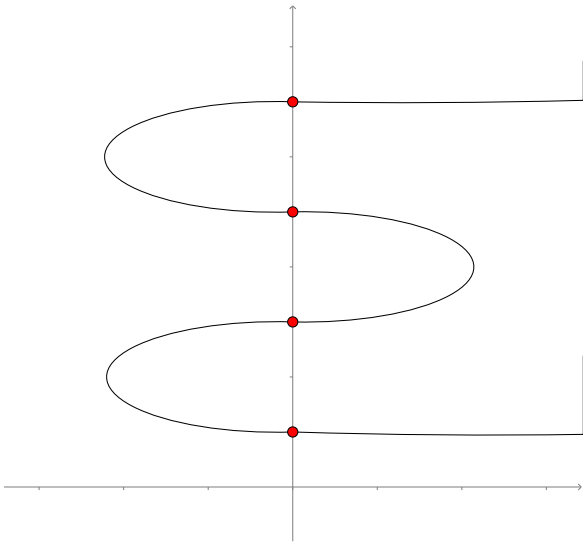

Abbildung 3: Kurve

Was passiert aber, wenn die Nullstellen zusammenfallen?

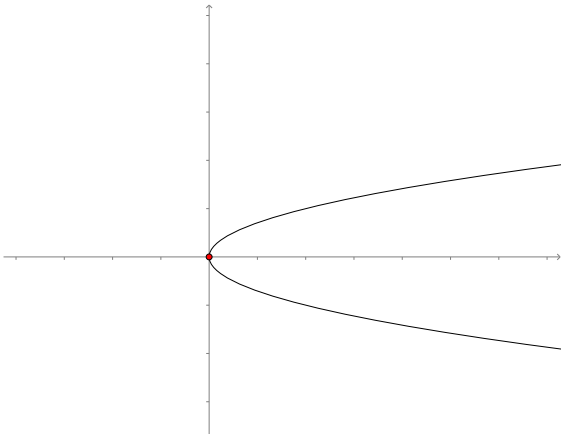

Abbildung 4: Parabel $Y^2 - X = 0$

Haben wir beispielsweise die Parabel

$$Y^2 - X = (Y + X^{\frac{1}{2}})(Y - X^{\frac{1}{2}}),$$

so können wir das Hensel'sche Lemma nicht anwenden, da die beiden Nullstellen für $X = 0$ zusammenfallen und sich nicht in eine Potenzreihe entwickeln lassen. Wir bekommen stattdessen eine gebrochene Potenzreihe.

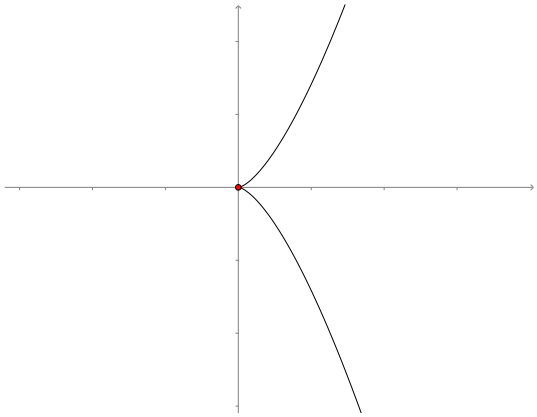

Abbildung 5: Kuspe $Y^2 - X^3 = 0$

Bei der Kuspe

$$Y^2 - X^3 = (Y + X^{\frac{3}{2}})(Y - X^{\frac{3}{2}})$$

haben wir in $X = 0$ eine Singularität. Auch diese können wir in die Form einer gebrochenen Potenzreihe bringen.

Das heißt, wenn wir bereit sind, Wurzeln aus X zu ziehen, können wir die Funktionen in gebrochenen Potenzreihen entwickeln.

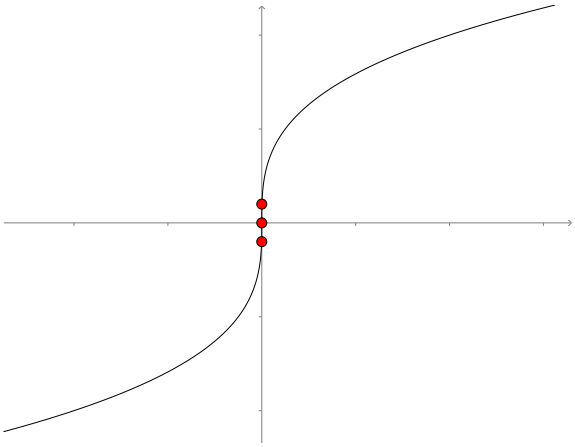

Abbildung 6: Kurve $Y^3 - X = 0$

Bei der Kurve

$$Y^3 - X = (Y - X^{\frac{1}{3}})(Y - \omega X^{\frac{1}{3}})(Y - \omega^2 X^{\frac{1}{3}}),$$

wobei ω die dritten Einheitswurzeln (Lösungen von $\omega^3 = 1$) sind, haben wir eine dreifache Nullstelle an der Stelle $X = 0$.

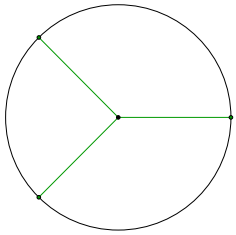

Abbildung 7: $\omega^3 = 1$

Wir sehen also, wenn wir Wurzeln zulassen, können wir auch in dem Fall, dass diese Lösungen sind, die Funktionen noch in Reihen entwickeln. Halten wir das als Satz fest:

Satz 3.8.1. *(Satz von Newton-Puiseux) Sei* $f(X,Y) = Y^d + a_1(X)Y^{d-1} + \cdots + a_d(X) \in \mathbb{C}[\![X]\!][Y]$ *mit* $a_i(x) \in \mathbb{C}[\![X]\!]$ *eine Potenzreihe.*

Dann existiert eine natürliche Zahl $N \geq 1$ *und Potenzreihen* $b_i(t) \in \mathbb{C}[\![t]\!]$*, sodass*

$$f(X,Y) = \prod_{i=1}^{d} (Y - b_i(t)) = f(t^N, Y) \in \mathbb{C}[\![t]\!][Y]$$

mit $X = t^N$ *bzw.* $t = X^{1/N}$*, das heißt die* $b_i(t)$ *sind Wurzelreihen von* f*.*

Beispiel 3.8.2. Sei $f(X,Y) = Y^4 + \underbrace{X^2}_{a_3} Y + \underbrace{X^3}_{a_4}$. Allgemein ist $f(X,Y) = \sum_{i,j} a_{ij} X^i Y^j$.

Wir erstellen nun ein *Newton-Diagramm*. Das bedeutet, wir zeichnen nicht die Kurve, sondern die Punkte in dem Gitter der Monome. Wir tragen also die Exponenten als Vektoren ein, das heißt $(i,j) \in \mathbb{N} \times \mathbb{N}$ korrespondiert mit $X^i Y^j$.

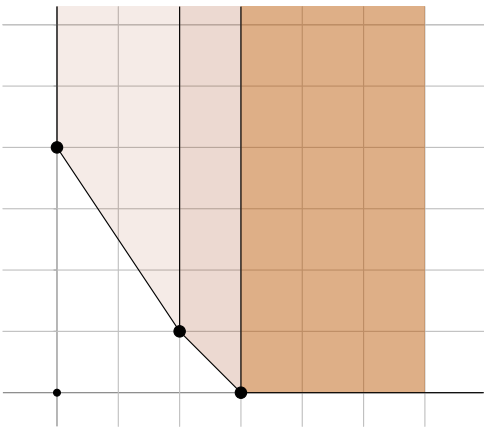

Abbildung 8: Newton-Diagramm von f

Sei $N(f) :=$ konvexe Hülle der Menge $\mathbb{N} \times \mathbb{N} + (i,j)$ für alle $(i,j) \in \mathbb{N} \times \mathbb{N}$ mit $a_{i,j} \neq 0$. Dann gilt $N(f) \subset \mathbb{R}^2$. Was sagt uns das jetzt?

Setzen wir $\rho_i := \mathrm{Ord}(a_i)$ und betrachten $\frac{\rho_i}{i}$. Weiter sei ρ als das Minimum $\rho := \min\left(\frac{\rho_i}{i}\right)$ definiert.

Erste Kante: Das sind die inversen Steigungen der Kanten, das heißt wir gehen im Gitter 3 nach unten und 2 nach rechts. Das ist dann $\frac{\rho_3}{3} = \frac{2}{3}$. Fahren wir nach diesem Schema fort, so erhalten wir $\frac{\rho_4}{4} = \frac{3}{4}$ und so weiter.

Nun wählen wir nach der Definition von ρ die kleinste (inverse) Steigung der Kante $\rho = \frac{2}{3}$, denn $\rho := \min\left(\frac{\rho_i}{i}\right)$ und $\frac{2}{3} < \frac{3}{4}$.

Substituieren wir nun $\rho = \frac{p}{q}$ und setzen $t := X^{\frac{1}{q}}$ bzw. $T^q := X$. Bei $q = 3$ haben wir dann beispielsweise $t = X^{\frac{1}{3}}$ bzw. $X = t^3$.

Setzen wir jetzt $Y = ZX^{\rho}$ in die Anfangsgleichung $f(X,Y) = Y^4 + X^2Y + X^3$ ein. Dann ist das $Y = ZX^{\frac{2}{3}} = Zt^2$ mit $X = t^3$ bzw. $t = X^{\frac{1}{3}}$.

Durch Einsetzen erhalten wir

$$Z^4t^8 + t^6Zt^2 + t^9 = t^8\left(Z^4 + Z + t\right).$$

Nun sind wir in der Situation, in der wir das Hensel'sche Lemma anwenden können, denn wenn wir $t = 0$ setzen, haben wir ein Polynom in verschiedenen Nullstellen. Mit $t = 0$ gilt

$$Z^4 + Z + t = Z(Z^3 + 1) = Z(Z - \alpha_0)(Z - \beta_0)(Z - \gamma_0),$$

wobei die Nullstellen α_0, β_0 und γ_0 die sechsten Einheitswurzeln sind und 0 eine weitere Nullstelle ist.

Da diese Nullstellen verschieden sind, können wir sie mit dem Hensel'schen Lemma liften. Das heißt, wir finden Reihen, sodass

$$\begin{aligned} &Z^4 + Z + t \\ &= \left(Z - (\delta_1 t + \delta_2 t^2 + \cdots)\right)\left(Z - (\alpha_0 + \alpha_1 t + \cdots)\right)\left(Z - (\beta_0 + \beta_1 t + \cdots)\right)\left(Z - (\gamma_0 + \gamma_1 t + \cdots)\right). \end{aligned}$$

Rücksubstituieren wir $Y = Zt^2$, so erhalten wir

$$Y^4 + X^2Y + X^3 = \left(Y - t^2(\delta_1 t + \cdots)\right)\left(Y - t^2(\alpha_0 + \alpha_1 t + \cdots)\right)(\ldots).$$

Wir haben die Gleichung also wieder mit einer Potenz von t multipliziert, sodass wir hier erneut Y bekommen. Somit finden wir $X = t^3$, da $Y = t^3$ und $t^3 = X$ war, $X^{\frac{2}{3}} = t^2$ und so weiter. Dann gilt

$$Y^4 + X^2Y + X^3 = (Y - \delta_1 X + \cdots)\left(Y - (\alpha_0 X^{\frac{2}{3}} + \cdots\right)\left(Y - (\beta_1 X^{\frac{2}{3}} + \cdots\right)\left(Y - (\gamma_1 X^{\frac{2}{3}} + \cdots\right)$$

und wir definieren

$$\tilde{f} := (Y^3 + X^2)(Y + X) = Y^4 + X^2Y + X^3 + \underline{Y^3X}.$$

Wir stellen somit fest, dass das Produkt $\tilde{f}$ einen Term mehr hat als unser ursprüngliches f. Zeichnen wir wieder das Newton-Diagramm, so sehen wir: Die beiden Newton-Diagramme sind identisch.

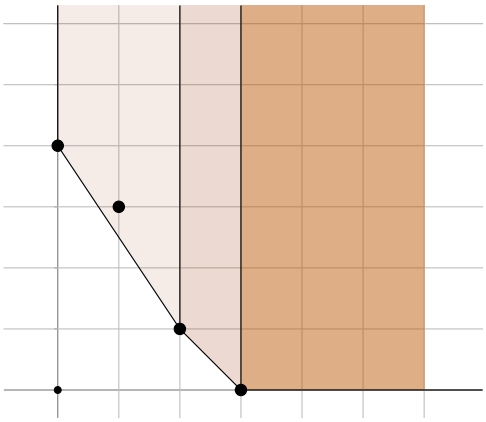

Abbildung 9: Newton-Diagramm von $\tilde{f}$

Es bleibt die Frage: Was sind diese Reihen?

Wir haben einmal $Y = -X$ als Lösung. Zusätzlich haben wir noch drei verschiedene Lösungen mit Termen aus sechsten Einheitswurzeln $X^{\frac{2}{3}}$. Das ist genau das, was wir aus unserer Anfangsgleichung f herausbekommen. Somit stellen wir fest, dass das Ergebnis richtig ist.

Aber wie sehen diese Kurven nun aus?

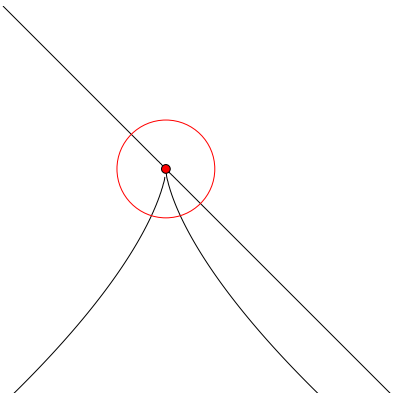

Abbildung 10: $\tilde{f} = 0$

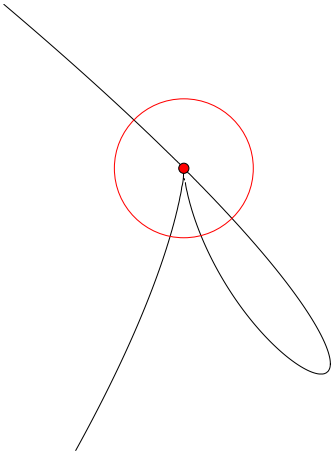

Abbildung 11: $f = 0$

Wir sehen, die Kurve $\tilde{f}$ besteht aus zwei Stücken, nämlich aus einer Geraden und einer Kuspe, während f selbst zusammenhängend ist.

Das Newton-Diagramm ist also eine effektive Methode um zu verstehen, wie eine Kurve aussieht. Wenn wir nun ein Monom weglassen, so wird die Gleichung irreduzibel. Dennoch gelingt es uns durch Potenzreihen festzustellen, was dort passiert.

Bei der anderen Gleichung geschieht im Prinzip das Gleiche. Wir führen unsere Gleichung also auf etwas bereits Bekanntes zurück. In diesem Sinne ist die Potenzreihenentwicklung die algebraische Lupe, um auf diesen einen Punkt einzuzoomen.

Der Beweis des Satzes verläuft analog zu unserer Rechnung im Beispiel.