

Werk

Titel: Journal für die reine und angewandte Mathematik

Verlag: de Gruyter

Jahr: 1986

Kollektion: Mathematica

Werk Id: PPN243919689_0369

PURL: http://resolver.sub.uni-goettingen.de/purl?PID=PPN243919689_0369|LOG_0012

Terms and Conditions

The Goettingen State and University Library provides access to digitized documents strictly for noncommercial educational, research and private purposes and makes no warranty with regard to their use for other purposes. Some of our collections are protected by copyright. Publication and/or broadcast in any form (including electronic) requires prior written permission from the Goettingen State- and University Library.

Each copy of any part of this document must contain there Terms and Conditions. With the usage of the library's online system to access or download a digitized document you accept the Terms and Conditions.

Reproductions of material on the web site may not be made for or donated to other repositories, nor may be further reproduced without written permission from the Goettingen State- and University Library.

For reproduction requests and permissions, please contact us. If citing materials, please give proper attribution of the source.

Contact

Niedersächsische Staats- und Universitätsbibliothek Göttingen
Georg-August-Universität Göttingen
Platz der Göttinger Sieben 1
37073 Göttingen
Germany
Email: gdz@sub.uni-goettingen.de

Reduzibilität ebener Kurven

Von Wolfgang Ruppert *) in Erlangen

Einführung

1. Ausgangspunkt der vorliegenden Arbeit ist die Frage nach einer effektiven Version des folgenden Satzes, der zuerst wohl bei Ostrowski [14] steht, dann bei Noether [13], Eichler [5], Deuring [3] etc. auftritt.

Satz A. Ist $f \in \mathbb{Z}[x, y]$ irreduzibel über $\mathbb{Q}$, so ist auch die Reduktion von f modulo p irreduzibel über $\mathbb{F}_p$ für alle bis auf endlich viele Primzahlen p .

Uns interessieren die Ausnahmeprimzahlen: Wie groß können diese werden in Abhängigkeit vom Grad und von der Höhe von f ?

Eine effektive Version findet sich bei W. M. Schmidt [16], S. 193, die aber recht wirklichkeitsfern erscheint. (In nachfolgendem Satz hat man die Ungleichung zu ersetzen durch $p > (4 \cdot L(f))^{k^{2k}}$, wo $k = \binom{d+1}{2}$ und $L(f)$ die Länge von f ist.)

Wir werden hier (als Korollar 2 zu Satz 3) die folgende effektive (homogene) Version des Satzes A von Ostrowski zeigen:

Satz B. Ist $f \in \mathbb{Z}[x_0, x_1, x_2]$, homogen vom Grad d mit Höhe H , irreduzibel über $\mathbb{Q}$, so ist f auch mod p irreduzibel über $\mathbb{F}_p$ für jede Primzahl p mit

$$p > d^{3d^2-3} \cdot H^{d^2-1}.$$

Wie kann man das beweisen? — Die Idee ist folgende: Im Linearsystem der ebenen algebraischen Kurven vom Grad d über $\mathbb{Q}$ bilden die reduziblen Kurven eine abgeschlossene Teilmenge, werden also durch Gleichungen $\varphi_1 = 0, \dots, \varphi_L = 0$ beschrieben, von denen wir annehmen wollen, daß sie ganze Koeffizienten haben. Ist nun ein $f \in \mathbb{Z}[x_0, x_1, x_2]$ irreduzibel über $\mathbb{Q}$, so gibt es ein φ_i mit $\varphi_i(f) \neq 0$. Mit $\varphi_i(f) \in \mathbb{Z}$ ist klar, daß dann für $p > |\varphi_i(f)|$ auch $\varphi_i(f) \not\equiv 0 \pmod{p}$ gilt, und man kann hoffen, daß dies die Irreduzibilität von $f \pmod{p}$ über $\mathbb{F}_p$ impliziert.

*) Dies ist die Dissertation des Autors, der an dieser Stelle nochmals seinem Doktorvater Prof. Dr. W.-D. Geyer herzlich danken möchte.

Es geht also darum, für die Mannigfaltigkeit der reduziblen Kurven Gleichungen möglichst kleinen Grades zu finden. Dazu ist die Reduzibilität einer Kurve „gut“ zu charakterisieren.

Hier haben wir folgendes Kriterium gefunden:

Reduzibilitätskriterium. f ist genau dann reduzibel, wenn es als Nenner einer geschlossenen 1-Form ($\neq 0$) der projektiven Ebene geschrieben werden kann.

(Dies gilt in Charakteristik 0 über einem algebraisch abgeschlossenen Körper; in Charakteristik p gilt noch die Richtung „ $\Rightarrow$ “.)

Eine exakte Formulierung und ein Beweis finden sich in § 1.

In § 2 erfolgt dann die Anwendung des Kriteriums: ein Reduzibilitätstest wird formuliert: eine Form $f \in \mathbb{Q}[x_0, x_1, x_2]$ vom Grad d ist genau dann reduzibel, wenn eine gewisse, aus den Koeffizienten von f gebildete $(d^2 - 1) \times (2d^2 - 3d + 1)$ -Matrix einen Rang $< d^2 - 1$ hat.

Hieraus wird obige effektive Version des Satzes von Ostrowski hergeleitet, sowie für die geometrische Situation:

Satz C. Im Linearsystem der ebenen Kurven vom Grad d (über $\mathbb{C}$) können die reduziblen Kurven durch Gleichungen vom Grad $d^2 - 1$ beschrieben werden.

2. Zur Verallgemeinerung obiger Aussagen auf Hyperflächen im $\mathbb{P}^n$ ($n \geq 3$) kann man das angegebene Reduzibilitätskriterium induktiv fortsetzen (vgl. Schluß von § 1), es zeigt sich aber, daß man mit folgendem Bertini-Argument (Hodge/Pedoe [10], S. 78 ff.) bessere Aussagen erhält:

„Ist eine Hyperfläche im $\mathbb{P}^n$ ($n \geq 3$) irreduzibel, so gibt es einen $\mathbb{P}^2 \subset \mathbb{P}^n$, so daß der Schnitt der Hyperfläche mit diesem $\mathbb{P}^2$ eine irreduzible Kurve ist.“

Damit kann alles auf Kurven in der Ebene zurückgeführt werden: Im Linearsystem der Hyperflächen vom Grad d des $\mathbb{P}^n$ (über $\mathbb{C}$) können die reduziblen Hyperflächen durch Gleichungen vom Grad $d^2 - 1$ beschrieben werden.

Die effektive Version des Satzes von Ostrowski verallgemeinert sich zu:

Satz B'. Ist $f \in \mathbb{Z}[x_0, \dots, x_n]$, homogen vom Grad d mit Höhe H , irreduzibel über $\mathbb{Q}$, so ist f auch mod p über $\mathbb{F}_p$ irreduzibel für jede Primzahl p mit

$$p > d^{3d^2-3} \cdot \left[\binom{n+d}{n} 3^d \right]^{d^2-1} \cdot H^{d^2-1}.$$

Die erzielten Abschätzungen hängen also nicht zu stark von n ab, und man kann sich zunächst auf Kurven im $\mathbb{P}^2$ beschränken.

3. Es bleibt die wichtige Frage: Wie nahe ist man mit den Abschätzungen an der Wirklichkeit?

Als Testobjekte werden hier Kurvenbüschel betrachtet (d.h. eindimensionale Linearsysteme von Kurven). Nach den Aussagen aus 1. ist klar, daß ein Büschel (über $\mathbb{C}$), dessen allgemeine Kurve irreduzibel ist, höchstens $d^2 - 1$ reduzible Kurven enthalten kann. Gibt es dafür Beispiele?

Wir werden sehen, daß es Büschel mit $3(d-1)$ reduziblen Kurven gibt (§ 5), wo die allgemeine Kurven nichtsingulär sind. In § 4 wird allerdings gezeigt, daß Büschel mit nichtsingulärer allgemeiner Kurve höchstens $3(d-1)$ reduzible Kurven enthalten können, so daß man auf diese Art nicht an die Zahl d^2-1 herankommt.

Die Zahl $3(d-1)$ ergibt sich dabei nach folgender Idee: Im Linearsystem aller ebenen Kurven vom Grad d bilden die singulären eine Hyperfläche vom Grad $3(d-1)^2$; eine reduzible Kurve hat (je nach Zerfallsart nach Bézout) mindestens $1 \cdot (d-1)$ Singularitäten. Da ein Büschel mit nichtsingulärer allgemeiner Kurve also höchstens $3(d-1)^2$ Singularitäten haben kann, kann es höchstens $\frac{3(d-1)^2}{(d-1)} = 3(d-1)$ reduzible Kurven enthalten.

Die arithmetische Version dieser Betrachtung verschärft Satz B wie folgt:

Satz D. Ist $f \in \mathbb{Z}[x_0, x_1, x_2]$, homogen vom Grad d mit Höhe H , nichtsingulär (speziell also irreduzibel) über $\mathbb{Q}$, so ist $f \bmod p$ irreduzibel über $\mathbb{F}_p$ für jede Primzahl p mit

$$p > \left(\frac{1}{4} \cdot d(d+1)(d+2) \right)^{3(d-1)} \cdot H^{3(d-1)}.$$

Modulo einer Vermutung von Bouniakowsky [1] kann man tatsächlich nichtsinguläre Kurven konstruieren, die $\bmod p$ reduzibel sind für eine Primzahl p mit $p \sim H^{3(d-1)}$.

Die Bouniakowsky-Vermutung (eine Verallgemeinerung des Dirichletschen Primzahlsatzes) besagt, daß für ein irreduzibles $F \in \mathbb{Z}[x]$ vom Grad ≥ 1 unendlich viele $n \in \mathbb{N}$ existieren, für die $\left| \frac{F(n)}{N} \right|$ prim ist, wo $N = \text{ggT} \{F(m) : m \in \mathbb{Z}\}$. Die Vermutung ist meines Wissens für $\text{grad}(F) > 1$ in keinem Fall bewiesen oder widerlegt, doch sprechen alle numerischen Experimente für ihre Gültigkeit, wie auch die Beispiele in § 6 zeigen sollen.

Für die nichtsingulären Kurven sehen die Ergebnisse also recht befriedigend aus, in Satz D ist höchstens noch der Faktor vor $H^{3(d-1)}$ verbesserungsfähig, der Exponent $3(d-1)$ ist scharf. Dies ist anders für singuläre Kurven. Eine allgemeine Aussage, die den Exponenten d^2-1 in Satz B herunterdrückt, fehlt für $d \geq 4$.

Man kann versuchen, durch Singularitätenzählen und Analyse der Basispunkte-Konfiguration die Zahl der reduziblen Kurven in einem Büschel mit singulärer, aber irreduzibler allgemeiner Kurve abzuschätzen. Dies scheint aber nicht der richtige Weg zu sein, da er mit vielen Fallunterscheidungen für $d \geq 4$ verbunden ist. Stattdessen wird in § 6 einfach eine Beispielklasse von Büscheln vorgestellt, die $2d-1$ reduzible Kurven enthalten (allgemeine Kurve irreduzibel, aber singulär), die größte Zahl, die wir gefunden haben (und die es für $d=3$ auch ist).

Könnte man zeigen, daß dies tatsächlich der schlimmste Fall ist, so hätte man wohl im Satz von Ostrowski die Abschätzung $p > C \cdot H^{3(d-1)}$ erreicht, d.h. man wäre an die exakte Schranke herangekommen.

Bezeichnungen. Unter der Höhe $H(f)$ eines Polynoms $f \in \mathbb{C}[x_1, \dots, x_n]$ bzw. eines Vektors $f \in \mathbb{C}^n$ verstehen wir das Maximum der Absolutbeträge der Koeffizienten von f , unter der Länge $L(f)$ die Summe der Absolutbeträge der Koeffizienten von f . Für $f \in \mathbb{C}[x_1, \dots, x_n]$, $a \in \mathbb{C}^n$ gilt dann die Abschätzung $|f(a)| \leq L(f) \cdot H(a)^{\text{grad } f}$.

Zu einem Körper K bezeichne $\bar{K}$ den algebraischen Abschluß von K .

I. Ein Reduzibilitätskriterium

§ 1. Geschlossene 1-Formen der projektiven Ebene

K sei ein algebraisch abgeschlossener Körper. Den Funktionenkörper (der projektiven Ebene über K) $K(x, y)$ in zwei Unbestimmten x, y betrachten wir eingebettet in den Funktionenkörper $K(x_0, x_1, x_2)$ in drei Unbestimmten x_0, x_1, x_2 durch $x = \frac{x_1}{x_0}$, $y = \frac{x_2}{x_0}$. Dadurch sind die K -Differentialle von $K(x, y)$ in natürlicher Weise eine Teilmenge der K -Differentialle von $K(x_0, x_1, x_2)$. Die K -Differentialle von $K(x, y)$ nennen wir auch 1-Formen der projektiven Ebene. Dann gilt das

Lemma 1. Die 1-Formen der projektiven Ebene sind genau die Differentialle von $K(x_0, x_1, x_2)$, die sich schreiben lassen als $\omega = \frac{1}{f}(r_0 dx_0 + r_1 dx_1 + r_2 dx_2)$ mit homogenen $r_0, r_1, r_2, f \in K[x_0, x_1, x_2]$ für die $r_0 x_0 + r_1 x_1 + r_2 x_2 = 0$ und $\text{grad}(f) - 1 = \text{grad}(r_i)$ gilt. (Diese Schreibweise soll zulassen, daß auch $r_j = 0$ vorkommen kann.)

Beweis. 1. Sei eine 1-Form der projektiven Ebene gegeben. Wir schreiben sie als $\omega = \frac{G(1, x, y)}{F(1, x, y)} dx + \frac{H(1, x, y)}{F(1, x, y)} dy$ mit homogenen gleichgradigen Polynomen F, G, H . Dann ergibt sich

$$\begin{aligned} \omega &= \frac{G(x_0, x_1, x_2)}{F(x_0, x_1, x_2)} \left(\frac{1}{x_0} dx_1 - \frac{x_1}{x_0^2} dx_0 \right) + \frac{H(x_0, x_1, x_2)}{F(x_0, x_1, x_2)} \left(\frac{1}{x_0} dx_2 - \frac{x_2}{x_0^2} dx_0 \right) \\ &= \frac{1}{x_0^2 F(x_0, x_1, x_2)} [(-G.x_1 - H.x_2) dx_0 + (G.x_0) dx_1 + (H.x_0) dx_2], \end{aligned}$$

woraus man sofort ersieht, daß ω die gewünschte Form hat.

2. Sei umgekehrt $\omega = \frac{1}{f}(r_0 dx_0 + r_1 dx_1 + r_2 dx_2)$ gegeben mit f, r_i homogen, $\text{grad}(f) - 1 = \text{grad}(r_i)$, $r_0 x_0 + r_1 x_1 + r_2 x_2 = 0$. Dann hat man

$$\begin{aligned} \omega &= \frac{1}{f} \left[\frac{-r_1 x_1 - r_2 x_2}{x_0} dx_0 + r_1 dx_1 + r_2 dx_2 \right] = \frac{1}{f} [x_0 r_1 dx + x_0 r_2 dy] \\ &= \frac{r_1(1, x, y)}{f(1, x, y)} dx + \frac{r_2(1, x, y)}{f(1, x, y)} dy, \end{aligned}$$

d.h. ω ist ein Differential der Ebene.

Im folgenden werden wir Differentialformen häufig in der Form des Lemmas schreiben. f heie dann ein Nenner der Differentialform. Eine Differentialform ω heit geschlossen, wenn $d\omega=0$ gilt. Die Geschlossenheit einer Differentialform ω mit $\omega = \frac{G}{F} dx + \frac{H}{F} dy = \frac{1}{f} (r_0 dx_0 + r_1 dx_1 + r_2 dx_2)$ drckt sich aus als $\frac{\partial}{\partial y} \left(\frac{G}{F} \right) = \frac{\partial}{\partial x} \left(\frac{H}{F} \right)$, oder quivalent $\frac{\partial}{\partial x_2} \left(\frac{r_1}{f} \right) = \frac{\partial}{\partial x_1} \left(\frac{r_2}{f} \right)$. Die Struktur geschlossener ebener 1-Formen ber einem Krper der Charakteristik 0 beschreibt folgender

Satz 1. *Ist ω eine geschlossene ebene 1-Form ber einem algebraisch abgeschlossenen Krper K der Charakteristik 0, so gibt es homogene Polynome $f_0, \dots, f_m$, $g, h \in K[x_0, x_1, x_2]$ mit $\text{grad } g = \text{grad } h$, $\lambda_0, \dots, \lambda_m \in K$, so da gilt:*

$$\omega = \sum_{i=0}^m \frac{\lambda_i}{\text{grad } f_i} \frac{df_i}{f_i} + d \left(\frac{g}{h} \right) \quad \text{und} \quad \sum_{i=0}^m \lambda_i = 0.$$

Umgekehrt ist jedes Differential dieser Gestalt eine geschlossene ebene 1-Form, unabhngig von der Charakteristik.

Wir ziehen sofort eine Folgerung aus dem Satz:

Korollar. *Jeder Nenner einer geschlossenen 1-Form $\neq 0$ ber einem algebraisch abgeschlossenen Krper der Charakteristik 0 ist reduzibel.*

Beweis des Korollars. Wir schreiben ω in der Form eines Satzes. O.E. seien die auftretenden f_i 's irreduzibel (denn: $f_i = u \cdot v$ impliziert

$$\frac{\lambda_i}{\text{grad } f_i} \cdot \frac{df_i}{f_i} = \frac{\lambda_i}{\text{grad } f_i} \cdot \frac{1}{\text{grad } f_i} \cdot \frac{du}{u} + \frac{\lambda_i}{\text{grad } f_i} \cdot \frac{1}{\text{grad } f_i} \cdot \frac{dv}{v},$$

und die Form des Satzes bleibt erhalten) und paarweise teilerfremd; ebenso seien g und h gekrzt gewhlt. Entwickelt man ω bzgl. dx_0, dx_1, dx_2 , so ist der Koeffizient bei dx_0

$$R_0 := \sum_{i=0}^m \frac{\lambda_i}{\text{grad } f_i} \cdot \frac{1}{f_i} \cdot \frac{\partial f_i}{\partial x_0} + \frac{1}{h} \frac{\partial g}{\partial x_0} - \frac{g}{h^2} \cdot \frac{\partial h}{\partial x_0}.$$

Ist $d \left(\frac{g}{h} \right) \neq 0$, so gibt es einen Primteiler p von h mit $p \nmid g$. O.E. $\frac{\partial p}{\partial x_0} \neq 0$, sonst betrachten wir statt R_0 einen anderen Koeffizienten von ω . Schreibt man $h = p^n \tilde{h}$ mit $p \nmid \tilde{h}$, so hat R_0 wegen $\frac{g}{h^2} \frac{\partial h}{\partial x_0} = \frac{g}{p^n \tilde{h}^2} \frac{\partial \tilde{h}}{\partial x_0} + \frac{ng \tilde{h}}{p^{n+1} \tilde{h}^2} \frac{\partial p}{\partial x_0}$ und $\text{char}(K)=0$ jedenfalls p^2 im Nenner stehen, der Nenner von ω ist also reduzibel.

Ist $d \left(\frac{g}{h} \right) = 0$, so steht jedes (als irreduzibel angenommene) f_i mit $\lambda_i \neq 0$ im Nenner von ω , und wegen $\sum \lambda_i = 0$ gibt es davon mindestens zwei, also ist der Nenner von ω reduzibel.

Diese Folgerung gilt nicht in Charakteristik p : Ist f von durch p teilbarem Grad, so ist $\frac{df}{f}$ nach Lemma 1 und Eulers Relation $\sum_{i=0}^2 \frac{\partial f}{\partial x_i} x_i = 0$ eine geschlossene 1-Form, auch für irreduzibles f . Daß die Folgerung auch nicht für $\text{grad } f < p$ gilt, zeigt folgendes Beispiel: Die Differentialform $\omega = \frac{y}{y^3 - x^4} dx + \frac{3x}{y^3 - x^4} dy$ ist über dem Körper $\mathbb{F}_5$ geschlossen und hat wegen $\omega = \frac{1}{x_0 x_2^3 - x_1^4} [x_0 x_1 x_2 dx_0 + x_0^2 x_2 dx_1 + 3 x_0^2 x_1 dx_2]$ den irreduziblen Nenner $x_0 x_2^3 - x_1^4$.

Charakteristikunabhängig gilt jedoch die Umkehrung des Korollars, was später für arithmetische Anwendungen benötigt wird:

Lemma 2. *Ist K ein algebraisch abgeschlossener Körper, $f \in K[x_0, x_1, x_2]$ homogen und reduzibel, so ist f Nenner einer abgeschlossenen 1-Form $\neq 0$.*

Beweis von Lemma 2. Nach Lemma 1 ist klar, daß mit f auch jedes homogene Vielfache aus $K[x_0, x_1, x_2]$ ein Nenner der gleichen geschlossenen 1-Form ist. Es genügt daher zu zeigen, daß für irreduzible homogene $g, h \in K[x_0, x_1, x_2]$ g^2 und gh als Nenner geschlossener 1-Formen $\neq 0$ auftreten. Sei $m = \text{grad } g$, $n = \text{grad } h$. Dann ist g^2 Nenner von $d\left(\frac{1}{g}\right)$ und gh Nenner von $\frac{1}{m} \frac{dg}{g} - \frac{1}{n} \frac{dh}{h}$, sofern $mn \neq 0$ in K . Ist aber z. B. $m=0$ in K , so ist $\frac{dg}{g} = \frac{hdg}{hg}$ eine geschlossene 1-Form mit Nenner gh .

Zum Beweis von Satz 1 zeigen wir zunächst eine inhomogene Form dieses Satzes:

Satz 2. *Ist ω eine geschlossene ebene 1-Form über einem algebraisch abgeschlossenen Körper K der Charakteristik 0, so gibt es $F_1, \dots, F_m, G, H \in K[x, y]$, $\mu_1, \dots, \mu_m \in K$ mit*

$$\omega = \sum_{i=1}^m \mu_i \frac{dF_i}{F_i} + d\left(\frac{G}{H}\right).$$

Beweis. 1. Wir schreiben $\omega = \frac{g}{f} dx + \frac{h}{f} dy$ mit $f, g, h \in K[x, y]$ und haben dann $\frac{\partial}{\partial y} \left(\frac{g}{f}\right) = \frac{\partial}{\partial x} \left(\frac{h}{f}\right)$. Wir betrachten f als Polynom in x mit Koeffizienten aus $K(y)$. L sei der Zerfällungskörper von f über $K(y)$. $\frac{\partial}{\partial x}, \frac{\partial}{\partial y}$ setzen sich dann auf $L(x)$ fort mit $\frac{\partial}{\partial x} L = 0, \frac{\partial}{\partial y} L \subset L$. Der Konstantenkörper bleibt K . Wir entwickeln nun $\frac{g}{f}, \frac{h}{f} \in L(x)$ in Partialbrüche:

$$\frac{g}{f} = \sum_{i=1}^n \sum_{j=1}^{m_n} \frac{a_{ij}}{(x - c_i)^j} + A, \quad \frac{h}{f} = \sum_{i=1}^n \sum_{j=1}^{m_n} \frac{b_{ij}}{(x - c_i)^j} + B,$$

mit $a_{ij}, b_{ij}, c_i \in L$, $A, B \in L[x]$. Läßt man die Galoisgruppe $\text{Gal}(L/K(y))$ hierauf operieren, so folgt aus der Eindeutigkeit der Partialbruchzerlegungen, daß $A, B \in K(y)[x]$ gilt, und daß für konjugierte $c_i, c_{i'}$ auch $a_{ij}, a_{i'j}$ konjugiert sind.

2. Es gilt

$$\begin{aligned}\frac{\partial}{\partial y} \left(\frac{g}{f} \right) &= \sum_{i=1}^n \sum_{j=1}^{m_n} \left[\frac{1}{(x-c_i)^j} \frac{\partial a_{ij}}{\partial y} + \frac{j a_{ij}}{(x-c_i)^{j+1}} \frac{\partial c_i}{\partial y} \right] + \frac{\partial A}{\partial y} \\ &= \sum_{i=1}^n \frac{1}{x-c_i} \frac{\partial a_{i1}}{\partial y} + \sum_{i=1}^n \sum_{j \geq 1} \left(\frac{\partial a_{i,j+1}}{\partial y} + j a_{ij} \frac{\partial c_i}{\partial y} \right) \cdot \frac{1}{(x-c_i)^{j+1}} + \frac{\partial A}{\partial y}, \\ \frac{\partial}{\partial x} \left(\frac{h}{f} \right) &= \sum_{i=1}^n \sum_{j=1}^{m_n} \frac{-j b_{ij}}{(x-c_i)^{j+1}} + \frac{\partial B}{\partial x}.\end{aligned}$$

Die Geschlossenheitsrelation für ω ausnutzend erhält man daher durch Vergleich der Partialbruchentwicklungen

$$\frac{\partial a_{i1}}{\partial y} = 0, \quad \frac{\partial a_{i,j+1}}{\partial y} + j a_{ij} \frac{\partial c_i}{\partial y} = -j b_{ij}, \quad \frac{\partial A}{\partial y} = \frac{\partial B}{\partial x}.$$

3. $\frac{\partial a_{i1}}{\partial y} = 0$ impliziert $a_{i1} \in K$; sei $\lambda_i := a_{i1}$. Wir wählen nun $C \in K(y)[x]$ mit

$\frac{\partial C}{\partial x} = A$. Ist c_i zu $c_{i'}$ konjugiert, so auch a_{ij} zu $a_{i'j}$, weswegen

$$\phi := \sum_{i=1}^n \sum_{j=2}^{m_n} \frac{-1}{j-1} \frac{a_{ij}}{(x-c_i)^{j-1}} + C$$

in $K(x, y)$ enthalten ist. Es gilt

$$\frac{g}{f} = \frac{\partial \phi}{\partial x} + \sum_{i=1}^n \frac{\lambda_i}{x-c_i}, \quad \frac{h}{f} = \frac{\partial \phi}{\partial y} + \sum_{i=1}^n \frac{-\lambda_i \frac{\partial c_i}{\partial y}}{x-c_i} + \left(B - \frac{\partial C}{\partial y} \right).$$

Ist c_i zu $c_{i'}$ konjugiert, so ist $\lambda_i = \lambda_{i'}$. Multipliziert man nun konjugierte $x-c_i$ auf, so erhält man $f_1, \dots, f_m \in K(y)[x]$ und o.E. (bzgl. der Numerierung der λ_i)

$$\frac{g}{f} = \frac{\partial \phi}{\partial x} + \sum_{j=1}^m \lambda_j \frac{\frac{\partial f_j}{\partial x}}{f_j}, \quad \frac{h}{f} = \frac{\partial \phi}{\partial y} + \sum_{j=1}^m \lambda_j \frac{\frac{\partial f_j}{\partial y}}{f_j} + \left(B - \frac{\partial C}{\partial y} \right).$$

Wegen $\frac{\partial}{\partial x} \left(B - \frac{\partial C}{\partial y} \right) = 0$ ist $B - \frac{\partial C}{\partial y} \in K(y)$, läßt sich also schreiben als $\lambda_0 \frac{\frac{\partial f_0}{\partial y}}{f_0} + \frac{\partial \psi}{\partial y}$ mit $f_0, \psi \in K(y)$, $\lambda_0 \in K$. Folglich ist $\omega = d(\phi + \psi) + \sum_{j=0}^m \lambda_j \frac{df_j}{f_j}$. (Rationale f_j 's lassen sich

sofort mit $\frac{d\left(\frac{u}{v}\right)}{\frac{u}{v}} = \frac{du}{u} - \frac{dv}{v}$ auf die gewünschte Form bringen.)

Nun bleibt noch Satz 1 zu beweisen.

Beweis von Satz 1. Sei eine geschlossene 1-Form ω gegeben. Nach Satz 2 gibt es $F_1, \dots, F_m, G, H \in K[x, y]$, $\mu_1, \dots, \mu_m \in K$ mit $\omega = \sum_{i=1}^m \mu_i \frac{dF_i}{F_i} + d\left(\frac{G}{H}\right)$. Wir wählen nun homogene Polynome $f_1, \dots, f_m, g, h \in K[x_0, x_1, x_2]$ mit $\text{grad } g = \text{grad } h$, $\text{grad } f_i = m_i$, so daß gilt: $F_i = f_i(1, x, y)$, $G = g(1, x, y)$, $H = h(1, x, y)$. Dann ist

$$\frac{G(x, y)}{H(x, y)} = \frac{g(1, x, y)}{h(1, x, y)} = \frac{g(x_0, x_1, x_2)}{h(x_0, x_1, x_2)},$$

also $d\left(\frac{G}{H}\right) = d\left(\frac{g}{h}\right)$, und

$$dF_i = d(f_i(1, x, y)) = d\left(\frac{f_i(x_0, x_1, x_2)}{x_0^{m_i}}\right) = \frac{1}{x_0^{m_i}} df_i - \frac{m_i f_i}{x_0^{m_i}} \frac{dx_0}{x_0},$$

also $\frac{dF_i}{F_i} = \frac{df_i}{f_i} - m_i \frac{dx_0}{x_0}$. Somit erhalten wir

$$\omega = \sum_{i=1}^m \mu_i \left(\frac{df_i}{f_i} - m_i \frac{dx_0}{x_0} \right) + d\left(\frac{g}{h}\right) = \left(- \sum_{i=1}^m m_i \mu_i \right) \frac{dx_0}{x_0} + \sum_{i=1}^m \frac{m_i \mu_i}{\text{grad } f_i} \frac{df_i}{f_i} + d\left(\frac{g}{h}\right),$$

eine Form, wie in Satz 1 behauptet. Die Umkehrung folgt sofort aus Lemma 1.

Bemerkungen. a) Die Darstellung von ω in Satz 1 bzw. Satz 2 ist (im wesentlichen) eindeutig, wenn man die f_i bzw. F_i irreduzibel und paarweise teilerfremd wählt.

b) Nicht nur die Charakteristik 0, sondern auch die algebraische Abgeschlossenheit von K ist notwendig für die Gültigkeit der Sätze 1 und 2. Denn schon für $n=1$ und $K=\mathbb{R}$ läßt sich die geschlossene 1-Form $\omega = \frac{dx}{1+x^2}$ nicht in der gewünschten Art schreiben, erst über $\mathbb{C}$ ist $\omega = \frac{1}{2i} \left(\frac{d(x+i)}{x+i} - \frac{d(x-i)}{x-i} \right)$.

c) Was hier für $n=2$ gemacht wurde, läßt sich allgemein für den $\mathbb{P}^n$ ($n \geq 2$) durchführen. Durch Induktion kann man beweisen: Eine Form $f \in \mathbb{C}[x_0, \dots, x_n]$ ist genau dann reduzibel, wenn sie Nenner einer nichttrivialen geschlossenen 1-Form des $\mathbb{P}^n$ ist.

§ 2. Reduzibilität ebener Kurven

Um die Reduzibilität eines homogenen Polynoms $f(x_0, x_1, x_2) \in K[x_0, x_1, x_2]$ vom Grad $d \geq 2$ über einem algebraisch abgeschlossenen Körper K zu untersuchen, ist es nach dem Korollar zu Satz 1 und Lemma 2 naheliegend, folgende Frage zu stellen: Wann ist f Nenner einer geschlossenen 1-Form $\neq 0$, d.h. wann gibt es $r_1, r_2 \in K[x_0, x_1, x_2]$ homogen vom Grad $d-1$, nicht beide gleich 0, mit $x_0 | r_1 x_1 + r_2 x_2$ (dann ist $r_0 = \frac{1}{x_0} (-r_1 x_1 - r_2 x_2)$) und $\frac{\partial}{\partial x_2} \left(\frac{r_1}{f} \right) = \frac{\partial}{\partial x_1} \left(\frac{r_2}{f} \right)$?

Wir machen den Ansatz $r_1 = \sum_{i+j+k=d-1} A_{ijk} x_0^i x_1^j x_2^k$, $r_2 = \sum_{i+j+k=d-1} B_{ijk} x_0^i x_1^j x_2^k$.

Wegen $x_0 | x_1 r_1 + x_2 r_2$ muß gelten

$$\begin{aligned} 0 &= x_1 \sum_{j+k=d-1} A_{0jk} x_1^j x_2^k + x_2 \sum_{j+k=d-1} B_{0jk} x_1^j x_2^k \\ &= \sum_{j=0}^{d-1} A_{0,j,d-1-j} x_1^{j+1} x_2^{d-1-j} + \sum_{j=0}^{d-1} B_{0,j,d-1-j} x_1^j x_2^{d-j} \\ &= \sum_{j=1}^d A_{0,j-1,d-j} x_1^j x_2^{d-j} + \sum_{j=0}^{d-1} B_{0,j,d-1-j} x_1^j x_2^{d-j} \\ &= A_{0,d-1,0} x_1^d + B_{0,0,d-1} x_2^d + \sum_{j=1}^{d-1} (A_{0,j-1,d-j} + B_{0,j,d-1-j}) x_1^j x_2^{d-j}, \end{aligned}$$

also $A_{0,d-1,0} = 0$, $B_{0,0,d-1} = 0$, $B_{0,j,d-1-j} = -A_{0,j-1,d-j}$ für $1 \leq j \leq d-1$.

Als nächstes untersuchen wir die Relation $\frac{\partial}{\partial x_2} \left(\frac{r_1}{f} \right) = \frac{\partial}{\partial x_1} \left(\frac{r_2}{f} \right)$. Diese ist gleichwertig mit $\frac{1}{f} \frac{\partial r_1}{\partial x_2} - \frac{r_1}{f^2} \frac{\partial f}{\partial x_2} = \frac{1}{f} \frac{\partial r_2}{\partial x_1} - \frac{r_2}{f^2} \frac{\partial f}{\partial x_1}$, also $f \frac{\partial r_1}{\partial x_2} - r_1 \frac{\partial f}{\partial x_2} - f \frac{\partial r_2}{\partial x_1} + r_2 \frac{\partial f}{\partial x_1} = 0$. Hier werden nun die Terme für r_1, r_2 eingesetzt:

$$\begin{aligned} 0 &= \sum_{i+j+k=d-1} A_{ijk} \left[k f x_0^i x_1^j x_2^{k-1} - \frac{\partial f}{\partial x_2} x_0^i x_1^j x_2^k \right] \\ &\quad - \sum_{i+j+k=d-1} B_{ijk} \left[j f x_0^i x_1^{j-1} x_2^k - \frac{\partial f}{\partial x_1} x_0^i x_1^j x_2^k \right]. \end{aligned}$$

Wir betrachten kurz alle Summanden mit $i=0$ und benutzen obige Relationen für die B_{0jk} :

$$\begin{aligned} &\sum_{j+k=d-1} A_{0jk} \left[k f x_1^j x_2^{k-1} - \frac{\partial f}{\partial x_2} x_1^j x_2^k \right] - \sum_{j+k=d-1} B_{0jk} \left[j f x_1^{j-1} x_2^k - \frac{\partial f}{\partial x_1} x_1^j x_2^k \right] \\ &= \sum_{j=0}^{d-2} A_{0,j,d-1-j} \left[(d-1-j) f x_1^j x_2^{d-2-j} - \frac{\partial f}{\partial x_2} x_1^j x_2^{d-1-j} \right] \\ &\quad + \sum_{j=1}^{d-1} A_{0,j-1,d-j} \left[j f x_1^{j-1} x_2^{d-1-j} - \frac{\partial f}{\partial x_1} x_1^j x_2^{d-1-j} \right] \\ &= \sum_{j=0}^{d-2} A_{0,j,d-1-j} \left[(d-1-j) f x_1^j x_2^{d-2-j} - \frac{\partial f}{\partial x_2} x_1^j x_2^{d-1-j} \right. \\ &\quad \left. + (j+1) f x_1^j x_2^{d-2-j} - \frac{\partial f}{\partial x_1} x_1^{j+1} x_2^{d-2-j} \right] \\ &= \sum_{j=0}^{d-2} A_{0,j,d-1-j} \left[\frac{\partial f}{\partial x_0} x_0 x_1^j x_2^{d-2-j} \right] \\ &\quad \left(\text{unter Benutzung von } d \cdot f = \frac{\partial f}{\partial x_0} x_0 + \frac{\partial f}{\partial x_1} x_1 + \frac{\partial f}{\partial x_2} x_2 \right). \end{aligned}$$

Damit gilt weiter, wenn wir gleich durch x_0 dividieren:

$$\begin{aligned} 0 = & \sum_{\substack{i+j+k=d-1 \\ i \geq 1}} A_{ijk} \left[kf x_0^{i-1} x_1^j x_2^{k-1} - \frac{\partial f}{\partial x_2} x_0^{i-1} x_1^j x_2^k \right] \\ & - \sum_{\substack{i+j+k=d-1 \\ i \geq 1}} B_{ijk} \left[jf x_0^{i-1} x_1^{j-1} x_2^k - \frac{\partial f}{\partial x_1} x_0^{i-1} x_1^j x_2^k \right] \\ & + \sum_{j=0}^{d-2} A_{0,j,d-1-j} \left[\frac{\partial f}{\partial x_0} x_1^j x_2^{d-2-j} \right]. \end{aligned}$$

Wir fassen das Erreichte zusammen in

Lemma 3. Eine Form $f \in K[x_0, x_1, x_2]$ vom Grad $d \geq 2$ über dem algebraisch abgeschlossenen Körper K der Charakteristik 0 ist Nenner einer nichttrivialen geschlossenen 1-Form genau dann, wenn die Formen

$$\begin{aligned} & \left(kf - \frac{\partial f}{\partial x_2} x_2 \right) \cdot x_0^{i-1} x_1^j x_2^{k-1}, & i+j+k=d-1, \quad i \geq 1, \\ & \left(jf - \frac{\partial f}{\partial x_1} x_1 \right) \cdot x_0^{i-1} x_1^{j-1} x_2^k, & i+j+k=d-1, \quad i \geq 1, \\ & \left(\frac{\partial f}{\partial x_0} \right) \cdot x_1^j x_2^{d-2-j}, & 0 \leq j \leq d-2 \end{aligned}$$

über K linear abhängig sind.

Die Anzahl dieser Formen beträgt $2 \left[\binom{2+d-1}{2} - d \right] + (d-1) = d^2 - 1$. Die Formen haben Grad $2d-3$, liegen also in dem durch $\{x_0^{2d-3}, \dots, x_2^{2d-3}\}$ aufgespannten Vektorraum der Dimension $\binom{2d-3+2}{2} = (2d-1)(d-1)$. Trägt man die Koeffizienten dieser Formen in eine Matrix ein, so erhält man eine $(d^2-1) \times (2d^2-3d+1)$ -Matrix M .

Wie sehen die Einträge dieser Matrix M aus? Ist $f = \sum_{i'+j'+k'=d} a_{i'j'k'} x_0^{i'} x_1^{j'} x_2^{k'}$, so wird

$$\left(kf - \frac{\partial f}{\partial x_2} x_2 \right) x_0^{i-1} x_1^j x_2^{k-1} = \sum_{i'+j'+k'=d} (k-k') a_{i'j'k'} x_0^{i'+i-1} x_1^{j'+j} x_2^{k'+k-1},$$

und analog für die anderen Formtypen, d.h. die Einträge der Matrix M sind jeweils ein Koeffizient der Form f multipliziert mit einer ganzen Zahl, deren Betrag $\leq d$ ist. Bilden wir nun alle möglichen (d^2-1) -Unterdeterminanten von M , so erhalten wir nach der Formel $\det((A_{mn})_{m,n}) = \sum_{\sigma \in S_N} (\text{sgn } \sigma) A_{1,\sigma_1} \cdots A_{N,\sigma_N}$ homogene Polynome $\varphi_l \in \mathbb{Z}[a_{ijk}]$ vom Grad d^2-1 der Länge $\leq (d^2-1)! d^{d^2-1} \leq (d^2)^{d^2-1} \cdot d^{d^2-1} = d^{3d^2-3}$.

Wir formulieren als Ergebnis den

Satz 3. Sei $d \geq 2$. Dann gibt es homogene Polynome

$$\varphi_1, \dots, \varphi_L \in \mathbb{Z}[a_{ijk} : i+j+k=d]$$

vom Grad $d^2 - 1$ der Länge $\leq d^{3d^2-3}$, die folgende Eigenschaft haben: Für jedes homogene Polynom f vom Grad d in x_0, x_1, x_2 über einem algebraisch abgeschlossenen Körper K mit Koeffizienten $\tilde{a}_{ijk}$, $i+j+k=d$ gilt:

1. Ist f reduzibel, so ist $\varphi_l(\tilde{a}_{ijk}) = 0$ in K für alle l .
2. Ist f irreduzibel und $\text{char}(K) = 0$, so gibt es ein l_0 mit $\varphi_{l_0}(\tilde{a}_{ijk}) \neq 0$ in K .

Beweis. Als φ_l nehmen wir natürlich die $(d^2 - 1)$ -Unterdeterminanten obiger Matrix M .

Ist f reduzibel, so ist f nach Lemma 2 Nenner einer nichttrivialen geschlossenen 1-Form, nach den Vorbereitungen hat die Matrix M also Rang $< d^2 - 1$, d.h. alle φ_l 's verschwinden auf f .

Ist $\text{char}(K) = 0$ und gilt $\varphi_l(\tilde{a}_{ijk}) = 0$ für alle l , so hat die Matrix M Rang $< d^2 - 1$, f ist also Nenner einer nichttrivialen geschlossenen 1-Form, und nach dem Korollar zu Satz 1 muß f reduzibel sein.

Wir ziehen zwei Folgerungen:

Korollar 1. Sei K algebraisch abgeschlossen, $\text{char}(K) = 0$. Im Linearsystem der ebenen Kurven vom Grad d bilden die reduziblen Kurven einen abgeschlossenen Teilraum, der sich durch Gleichungen vom Grad $d^2 - 1$ beschreiben läßt (nämlich durch die φ_l 's aus dem Satz).

Korollar 2 (Effektive Version des Satzes von Ostrowski). Ist $f \in \mathbb{Z}[x_0, x_1, x_2]$ homogen vom Grad d mit Höhe $\leq H$, irreduzibel über $\mathbb{Q}$, so ist auch die Reduktion von f modulo p irreduzibel über $\mathbb{F}_p$ für jede Primzahl p mit

$$p > d^{3d^2-3} \cdot H^{d^2-1}.$$

Beweis. Da f über $\mathbb{Q}$ irreduzibel ist, gibt es ein l_0 mit $\varphi_{l_0}(f) \neq 0$. Nun ist $\varphi_{l_0}(f) \in \mathbb{Z}$ und $|\varphi_{l_0}(f)| \leq L(\varphi_{l_0}) \cdot H^{d^2-1} \leq d^{3d^2-3} \cdot H^{d^2-1}$, also ist auch für jede Primzahl p mit $p > d^{3d^2-3} \cdot H^{d^2-1}$

$$\varphi_{l_0}(f) \not\equiv 0 \pmod{p},$$

d.h. f ist auch über $\mathbb{F}_p$ irreduzibel.

Zum Abschluß wollen wir noch beispielhaft den Reduzibilitätstest für Quadriken und Kubiken explizit angeben. $\left(K \text{ sei algebraisch abgeschlossen, } f_i \text{ stehe für } \frac{\partial f}{\partial x_i} \right)$

Quadriken. Für eine Quadrik $f = a_0 x_0^2 + a_1 x_0 x_1 + a_2 x_0 x_2 + a_3 x_1^2 + a_4 x_1 x_2 + a_5 x_2^2$ haben wir die K -lineare Abhängigkeit der drei Linearformen f_0, f_1, f_2 zu testen. Dies führt auf die Matrix

$$M = \begin{pmatrix} 2a_0 & a_1 & a_2 \\ a_1 & 2a_3 & a_4 \\ a_2 & a_4 & 2a_5 \end{pmatrix}.$$

In Charakteristik $\neq 2$ sind die Linearformen f_0, f_1, f_2 genau dann linear abhängig, wenn f singular ist, was bei drei Variablen äquivalent ist zur Reduzibilität von f . (Dies ist alles bekannt!)

Also: $(\text{char}(K) \neq 2): f \text{ reduzibel} \Leftrightarrow \det(M) = 0$.

Kubiken. Sei

$$f = a_0 x_0^3 + a_1 x_0^2 x_1 + a_2 x_0^2 x_2 + a_3 x_0 x_1^2 + a_4 x_0 x_1 x_2 \\ + a_5 x_0 x_2^2 + a_6 x_1^3 + a_7 x_1^2 x_2 + a_8 x_1 x_2^2 + a_9 x_2^3.$$

Wir haben die lineare Abhängigkeit der folgenden 8 Kubiken zu testen:

$$f_0 x_1, f_0 x_2, f_1 x_0, f_1 x_2, f_2 x_0, f_2 x_1, f - f_1 x_1, f - f_2 x_2.$$

Dies führt zu folgender 8×10 -Matrix M :

$$\begin{pmatrix} 0 & 3a_0 & 0 & 2a_1 & 2a_2 & 0 & a_3 & a_4 & a_5 & 0 \\ 0 & 0 & 3a_0 & 0 & 2a_1 & 2a_2 & 0 & a_3 & a_4 & a_5 \\ a_1 & 2a_3 & a_4 & 3a_6 & 2a_7 & a_8 & 0 & 0 & 0 & 0 \\ 0 & 0 & a_1 & 0 & 2a_3 & a_4 & 0 & 3a_6 & 2a_7 & a_8 \\ a_2 & a_4 & 2a_5 & a_7 & 2a_8 & 3a_9 & 0 & 0 & 0 & 0 \\ 0 & a_2 & 0 & a_4 & 2a_5 & 0 & a_7 & 2a_8 & 3a_9 & 0 \\ a_0 & 0 & a_2 & -a_3 & 0 & a_5 & -2a_6 & -a_7 & 0 & a_9 \\ a_0 & a_1 & 0 & a_3 & 0 & -a_5 & a_6 & 0 & -a_8 & -2a_9 \end{pmatrix}.$$

Für die irreduzible Kubik $f = x_0 x_2^2 + x_1^3$ ist wegen $f_2 = 2 \cdot x_0 x_2, f_1 = 3 \cdot x_1^2$ in Charakteristik 2 und 3 der Rang der Matrix $M < 8$, so daß hier der Reduzibilitätstest nicht funktioniert. Sonst gilt aber: In Char. $\neq 2, 3$ ist f genau dann reduzibel, wenn $\text{Rg}(M) < 8$ ist.

Beweis. Es bleibt nur noch „ $\Leftarrow$ “ zu zeigen. Mit der Eulerschen Relation

$$3 \cdot f = f_0 x_0 + f_1 x_1 + f_2 x_2$$

sieht man, daß die lineare Abhängigkeit der obigen 8 Formen eine Gleichung

$$f_0 l_0 + f_1 l_1 + f_2 l_2 = 0$$

liefert, mit Linearformen l_i , die nicht alle 0 sind. Ist z.B. $l_0 \neq 0$ und wäre f nichtsingulär, so verschwände f_0 nicht in den Schnittpunkten von $f_1 = 0, f_2 = 0$, Noethers $AF + BG$ Theorem (Griffiths/Harris [7], S. 703) würde also eine Gleichung $l_0 = f_1 L_1 + f_2 L_2$ mit Formen L_1, L_2 liefern, was aus Gradgründen nicht sein kann. Also muß f singular sein. Da die Eigenschaft, Nenner einer nichttrivialen geschlossenen 1-Form zu sein, nicht vom Koordinatensystem abhängt, kann man sich für die Untersuchung der singulären irreduziblen Kubiken auf $x_0 x_2^2 + x_1^3$ und $x_0 x_2^2 + x_0 x_1^2 + x_1^3$ beschränken. Bei diesen rechnet man leicht direkt nach, daß obige 8 Formen linear unabhängig sind. Damit ist die Behauptung gezeigt.

Bemerkung. Erfolgreiche Versuche mit dem Computer, Polynome vom Grad ≤ 7 zu finden, die auf den reduziblen Kubiken im Linearsystem aller ebenen Kubiken (über $\mathbb{C}$) verschwinden, legen nahe, daß für $d = 3$ Korollar 1 optimal ist.

§ 3. Reduzibilität von Hyperflächen im $\mathbb{P}^n$

Die Ergebnisse von § 2 wollen wir jetzt anwenden, um Aussagen über die Reduzibilität von Hyperflächen im $\mathbb{P}^n$ ($n \geq 2$) zu gewinnen. Das entscheidende Hilfsmittel ist das folgende

Lemma 4. *Ist F eine irreduzible Hyperfläche in $\mathbb{P}^n(K)$, wo K ein algebraisch abgeschlossener Körper ist, so gibt es einen 2-dimensionalen linearen Teilraum E von $\mathbb{P}^n$, so daß $F \cap E$ eine irreduzible Kurve in E ($=\mathbb{P}^2$) ist.*

Ein Beweis dieser Aussage ist z.B. in Hodge/Pedoe [10], S. 78ff. zu finden.

Sei $d \geq 2$. $\varphi_1, \dots, \varphi_L \in \mathbb{Z}[a_{ijk}]$ seien die homogenen Polynome von Satz 3 vom Grad $d^2 - 1$ der Länge $\leq d^{3d^2-3}$, die (in Charakteristik 0) die reduziblen Kurven beschreiben. Sei $F(z_0, z_1, \dots, z_n)$ das homogene Polynom vom Grad d mit unbestimmten Koeffizienten $A_{i_0 i_1 \dots i_n}$. Wir substituieren nun mit unbestimmten t_{ij}

$$z_i = t_{i0}x_0 + t_{i1}x_1 + t_{i2}x_2$$

und erhalten ein homogenes Polynom $f(x_0, x_1, x_2)$ in x_0, x_1, x_2 vom Grad d mit Koeffizienten $a_{ijk} \in \mathbb{Z}[A_{i_0 \dots i_n}, t_{ij}]$. Die a_{ijk} sind homogen in $A_{i_0 \dots i_n}$ vom Grad 1, homogen in t_{ij} vom Grad d und haben ganze Koeffizienten ≥ 0 . Da die Koeffizienten ≥ 0 sind, können wir die Länge von a_{ijk} einfach dadurch abschätzen, daß wir alle Unbestimmten 1 setzen: $A_{i_0 \dots i_n} = 1, x_0 = x_1 = x_2 = 1, t_{ij} = 1$ ergibt $z_i = 3$, also

$$L(a_{ijk}) \leq f(1, 1, 1) = \binom{n+d}{n} \cdot 3^d.$$

Mit dem gleichen Argument hat ein Monom in a_{ijk} vom Grad $d^2 - 1$ eine Länge

$$\leq \left[\binom{n+d}{n} \cdot 3^d \right]^{d^2-1}.$$

Setzen wir jetzt a_{ijk} in φ_l ein, so erhalten wir ein Polynom vom Grad $d^2 - 1$ in $A_{i_0 \dots i_n}$, Grad $d(d^2 - 1)$ in t_{ij} der Länge $\leq d^{3d^2-3} \cdot \left[\binom{n+d}{n} \cdot 3^d \right]^{d^2-1}$. Faßt man dies als Polynom in t_{ij} auf, so sind die Koeffizienten Polynome $\phi_{l1}, \dots, \phi_{lM} \in \mathbb{Z}[A_{i_0 \dots i_n}]$ der Länge $\leq d^{3d^2-3} \cdot \left[\binom{n+d}{n} \cdot 3^d \right]^{d^2-1}$. Wir erhalten so Polynome ϕ_{lm} , $1 \leq l \leq L$, $1 \leq m \leq M$, die das Gewünschte leisten, nämlich:

Satz 4. *Sei $d \geq 2$, $n \geq 3$. Dann gibt es homogene Polynome*

$$\phi_{lm} \in \mathbb{Z}[A_{i_0 \dots i_n} : i_0 + i_1 + \dots + i_n = d]$$

vom Grad $d^2 - 1$ der Länge $\leq d^{3d^2-3} \cdot \left[\binom{n+d}{n} \cdot 3^d \right]^{d^2-1}$, die folgende Eigenschaft besitzen: Ist $F \in K[z_0, z_1, \dots, z_n]$ homogen vom Grad d mit Koeffizienten $\tilde{A}_{i_0 \dots i_n}$, wo K ein algebraisch abgeschlossener Körper ist, so gilt:

1. *Ist F reduzibel, so gilt für alle Polynome ϕ_{lm}*

$$\phi_{lm}(\tilde{A}_{i_0 \dots i_n}) = 0 \text{ in } K.$$

2. Ist $\text{char}(K)=0$ und F irreduzibel, so gibt es ein Polynom

$$\phi_{l_0 m_0} \text{ mit } \phi_{l_0 m_0}(\tilde{A}_{i_0 \dots i_n}) \neq 0 \text{ in } K.$$

Beweis. Wir zeigen, daß die oben konstruierten Polynome ϕ_{lm} den Satz erfüllen.

Zu 1. F sei ein reduzibles Polynom in $z_0, \dots, z_n$. Für jede Wahl von t_{ij} ist dann auch $f(x_0, x_1, x_2)$ reduzibel, ϕ_l muß daher identisch verschwinden, d.h. $\phi_{lm}(\tilde{A}_{i_0 \dots i_n}) = 0$ für alle l, m .

Zu 2. Ist F irreduzibel, so gibt es, nach Lemma 4, $t_{ij} \in K$, so daß $f(x_0, x_1, x_2)$ irreduzibel ist. Dann gibt es ein ϕ_{l_0} mit $\phi_{l_0}(a_{ijk}) \neq 0$, also können nicht alle $\phi_{lm}(\tilde{A}_{i_0 \dots i_n}) = 0$ sein.

Wie im ebenen Fall können wir zwei unmittelbare Folgerungen ziehen:

Korollar 1. K sei algebraisch abgeschlossen, $\text{char}(K)=0$, $d \geq 2$, $n \geq 3$. Die reduziblen Hyperflächen bilden im Linearsystem aller Hyperflächen vom Grad d im $\mathbb{P}^n$ eine abgeschlossene Teilmenge, die durch Gleichungen vom Grad d^2-1 beschrieben werden kann.

Korollar 2 (Effektive Version des Satzes von Ostrowski). $f \in \mathbb{Z}[x_0, \dots, x_n]$ sei ein homogenes Polynom vom Grad $d \geq 2$ der Höhe $\leq H$, das irreduzibel über $\mathbb{Q}$ ist. Für jede Primzahl p mit

$$p > d^{3d^2-3} \cdot \left[\binom{n+d}{n} \cdot 3^d \right]^{d^2-1} \cdot H^{d^2-1}$$

ist dann auch das modulo p reduzierte Polynom f irreduzibel über $\mathbb{F}_p$.

Bemerkung. Statt hier alles auf Aussagen über den $\mathbb{P}^2$ zurückzuführen, kann man als Reduzibilitätstest auch die Schlußbemerkung von § 1 benutzen, d.h. man untersucht, ob ein $f \in K[x_0, \dots, x_n]$ (homogen vom Grad d) Nenner einer geschlossenen 1-Form des $\mathbb{P}^n$ ist. Bei gleicher Vorgehensweise wie in § 2 erhält man dann ein homogenes lineares Gleichungssystem mit

$$e_n(d) = (n+1) \binom{d+n-1}{n} - \binom{d+n}{n} = \frac{(d+n-1) \cdots (d+1)(d-1)}{(n-1)!}$$

Unbekannten, das auf nichttriviale Lösbarkeit zu untersuchen ist. Für die reduziblen Hyperflächen erhält man so in Charakteristik 0 beschreibende Gleichungen vom Grad $e_n(d)$, was bei festem n ein Polynom in d vom Grad n ist. Das in diesem Paragraphen benutzte Verfahren ist eindeutig besser, da die erzielten Abschätzungen (bis auf die Konstante in Korollar 2) nicht von n abhängen.

II. Beispielklassen

§ 4. Eine Abschätzung für nichtsinguläre Kurven

Die ebenen algebraischen Kurven vom Grad d über $\mathbb{C}$ bilden einen projektiven Raum $X \cong \mathbb{P}^D$ der Dimension $D = \frac{d(d+3)}{2}$. Wird eine Kurve durch die Form

$f = \sum_{i+j+k=d} a_{ijk} x_0^i x_1^j x_2^k$ beschrieben, so gehöre dazu im $\mathbb{P}^D$ der Punkt mit den homogenen

Koordinaten $(a_{d00} : \dots : a_{00d})$. (Wir werden im folgenden oft in der Sprechweise nicht zwischen Kurve und zugehöriger Form unterscheiden.) Die singulären Kurven bilden eine Hyperfläche W , die durch eine Gleichung $R=0$ gegeben ist mit $R \in \mathbb{C}[a_{ijk}]$. R ist die Resultante der drei Formen $\frac{\partial f}{\partial x_0}, \frac{\partial f}{\partial x_1}, \frac{\partial f}{\partial x_2}$, wo $f = \sum_{i+j+k=d} a_{ijk} x_0^i x_1^j x_2^k$. Es gilt

Lemma 5. Als beschreibende Gleichung für die Hyperfläche der singulären Kurven in X kann $R \in \mathbb{Z}[a_{ijk} : i+j+k=d]$ mit

$$|R(f)| \leq \left[\frac{d(d+1)(d+2)}{4} H(f) \right]^{3(d-1)^2}$$

gewählt werden. R ist homogen vom Grad $3(d-1)^2$.

Beweis. 1. Der Grad der Hyperfläche W der singulären Kurven ist die Anzahl der Schnittpunkte einer „allgemeinen“ Geraden in X mit W . Sei also $\lambda_0 f + \lambda_1 g$, $(\lambda_0 : \lambda_1) \in \mathbb{P}^1$, ein Büschel mit der Eigenschaft, daß die allgemeine Kurve nichtsingulär ist, und daß die Hyperfläche W nur transversal geschnitten wird. Dann ist $\text{grad } W = \# M$, wo

$$M = \left\{ ((\lambda_0 : \lambda_1), (y_0 : y_1 : y_2)) \in \mathbb{P}^1 \times \mathbb{P}^2 : \frac{\partial}{\partial x_i} (\lambda_0 f + \lambda_1 g)(y_0, y_1, y_2) = 0, \quad i = 0, 1, 2 \right\}.$$

$M \subseteq \mathbb{P}^1 \times \mathbb{P}^2$ ist Schnitt dreier Divisoren des Typs $E + (d-1) \cdot F$, wo E bzw. F dem Hyperebenenchnitt von $\mathbb{P}^1$ bzw. $\mathbb{P}^2$ in $\mathbb{P}^1 \times \mathbb{P}^2$ entspricht. Die Mächtigkeit von M ist daher $(E + (d-1)F)^3 = \binom{3}{1} \cdot E^1 \cdot (d-1)^2 F^2 = 3(d-1)^2$. Also $\text{grad } W = 3(d-1)^2$. (Siehe Shafarevich [18], S.198/199!)

2. Wir konstruieren nun eine Resultante R von $\frac{\partial f}{\partial x_0}, \frac{\partial f}{\partial x_1}, \frac{\partial f}{\partial x_2}$ nach Sylvester, der allerdings keinen Beweis angibt. (Siehe Sylvester [20] oder Netto [12], § 451!)

a) Sei Z der Vektorraum der Formen vom Grad $2d-3$ mit der Standardbasis $\{x_0^i x_1^j x_2^k : i+j+k=2d-3\}$; dann ist $\dim Z = \binom{2d-1}{2}$. Die Formen $x_0^i x_1^j x_2^k \frac{\partial f}{\partial x_0}$,

$x_0^i x_1^j x_2^k \frac{\partial f}{\partial x_1}$, $x_0^i x_1^j x_2^k \frac{\partial f}{\partial x_2}$, $i+j+k=d-2$, liegen in Z und mögen Formen des Typs I heißen. Ihre Anzahl ist $n_I = 3 \cdot \binom{d}{2}$. Die Länge einer solchen Form läßt sich wie folgt abschätzen:

$$\begin{aligned} L\left(x_0^i x_1^j x_2^k \frac{\partial f}{\partial x_0}\right) &= L\left(\frac{\partial f}{\partial x_0}\right) = L\left(\sum_{i+j+k=d} i \cdot a_{ijk} x_0^{i-1} x_1^j x_2^k\right) \\ &\leq \sum_{i+j+k=d} i \cdot H(f) = \frac{1}{6} d(d+1)(d+2) \cdot H(f). \end{aligned}$$

b) Zu jedem Tripel i, j, k ganzer Zahlen mit $i+j+k=d$, $i, j, k \geq 1$ wählen wir Formen F_{ij} mit

$$\begin{aligned} \frac{\partial f}{\partial x_0} &= F_{00} x_0^i + F_{01} x_1^j + F_{02} x_2^k, \\ (*) \quad \frac{\partial f}{\partial x_1} &= F_{10} x_0^i + F_{11} x_1^j + F_{12} x_2^k, \\ \frac{\partial f}{\partial x_2} &= F_{20} x_0^i + F_{21} x_1^j + F_{22} x_2^k. \end{aligned}$$

$\det(F_{ij})$ liegt dann in Z und werde Form vom Typ II genannt.

Ist $\tilde{F}_{ij}$ eine andere „Auflösung“ von (*), so kann man sehen, daß sich $\det(\tilde{F}_{ij})$ und $\det(F_{ij})$ nur um ein Element des von den Formen vom Typ I aufgespannten Vektorraums unterscheiden.

Wir haben $n_{II} = \binom{d-1}{2}$ Formen vom Typ II gewählt. Ist (o. E.) $L(F_{ij}) \leq L\left(\frac{\partial f}{\partial x_i}\right)$, so gilt:

$$L(\det(F_{ij})) \leq 6 \cdot L\left(\frac{\partial f}{\partial x_i}\right)^3 \leq 6 \cdot \left[\frac{1}{6} d(d+1)(d+2) \cdot H(f)\right]^3.$$

c) Nun hat man also $n_I + n_{II} = 3 \cdot \binom{d}{2} + \binom{d-1}{2} = \binom{2d-1}{2} = \dim Z$ Formen vom Typ I und II. Nimmt man die Koeffizienten bezüglich der Standardbasis von Z , so erhält man eine quadratische Matrix, deren Determinante $R(f)$ sein möge. (Nach der Bemerkung aus b) hängt sie nicht von der speziellen Wahl der F_{ij} 's ab.) Die Formen vom Typ I haben in a_{ijk} Grad 1, die vom Typ II Grad 3; daher hat R Grad $n_I + 3n_{II} = 3(d-1)^2 = \text{grad } W$ in den a_{ijk} 's. Hat eine Form f eine Singularität in $(y_0 : y_1 : y_2) \in \mathbb{P}^2$, so verschwinden alle Formen vom Typ I und II in $(y_0 : y_1 : y_2)$, können also nicht ganz Z aufspannen, d.h. $R(f) = 0$.

Aus Gradgründen beschreibt daher $R \in \mathbb{Z}[a_{ijk} : i+j+k=d]$ die Hyperfläche W .

d) Nach der Hadamardschen Determinantenabschätzungsformel läßt sich $R(f)$ für konkretes f durch das Produkt der Längen der Formen vom Typ I und II abschätzen, also (für $d \geq 2$)

$$\begin{aligned} |R(f)| &\leq \left[\frac{1}{6} d(d+1)(d+2) \cdot H(f) \right]^{n_1} \cdot \left[6 \cdot \left[\frac{1}{6} d(d+1)(d+2) \cdot H(f) \right]^3 \right]^{n_{II}} \\ &= \left[6^{\frac{-5d+4}{6d-6}} \cdot d(d+1)(d+2) \cdot H(f) \right]^{3(d-1)^2} \leq \left[\frac{1}{4} d(d+1)(d+2) \cdot H(f) \right]^{3(d-1)^2}. \end{aligned}$$

In einer ersten Version der Arbeit wurde eine Resultantenkonstruktion nach v. d. Waerden [22], § 88, benutzt. Dem Referenten verdanke ich den Hinweis auf die Sylvestersche Konstruktion, wodurch die Abschätzung in Satz 5 bzw. Satz D echt verbessert wurde.

Die reduziblen Kurven bilden in X eine abgeschlossene Teilmenge V . V ist Vereinigung von Bildern von Morphismen $\mathbb{P}^{D_1} \times \mathbb{P}^{D_2} \rightarrow X = \mathbb{P}^D$, wo $D_i = \frac{d_i(d_i+3)}{2}$, $d_1 + d_2 = d$, $d_i \geq 1$, und die Morphismen durch Formenmultiplikation gegeben sind.

Lemma 6. Die Resultante R verschwindet mindestens von der Ordnung $d-1$ in allen Punkten von X , die zu reduziblen Kurven gehören.

Beweis. Sei f eine reduzible Form, d.h. $f = f_1 f_2$ mit $\text{grad}(f_i) = d_i \geq 1$. Aus Stetigkeitsgründen können wir annehmen, daß sich die Kurven f_1 und f_2 transversal in $d_1 d_2$ verschiedenen Punkten schneiden, d.h. f besitzt mindestens $d_1 d_2 = d_1(d-d_1)$ verschiedene Singularitäten.

Wir betrachten jetzt ein Büschel $\lambda_0 f + \lambda_1 g$, $(\lambda_0 : \lambda_1) \in \mathbb{P}^1$, mit der Eigenschaft, daß die allgemeine Kurve nichtsingulär ist, daß die Hyperfläche $R=0$ für $(\lambda_0 : \lambda_1) \neq (1:0)$ nur transversal geschnitten wird, und daß das Büschel keine nichtreduzierten Kurven enthält. Aus Dimensionsgründen ist dies der allgemeine Fall. Die Teilmenge

$$M = \left\{ ((\lambda_0 : \lambda_1), (y_0 : y_1 : y_2)) \in \mathbb{P}^1 \times \mathbb{P}^2 : \frac{\partial}{\partial x_i} (\lambda_0 f + \lambda_1 g)(y_0, y_1, y_2) = 0, i=0, 1, 2 \right\}$$

von $\mathbb{P}^1 \times \mathbb{P}^2$ ist nach Voraussetzung endlich, und man sieht genau wie im Beweis von Lemma 5, daß die Mächtigkeit $\leq 3(d-1)^2$ ist. Zu $(\lambda_0 : \lambda_1) = (1:0)$ gehören nun mindestens $d_1(d-d_1)$ Punkte von M , d.h. für höchstens $3(d-1)^2 - d_1(d-d_1)$ Punkte $(\lambda_0 : \lambda_1) \in \mathbb{P}^1 \setminus \{(1:0)\}$ ist $\lambda_0 f + \lambda_1 g$ singulär. Nun hat $R(\lambda_0 f + \lambda_1 g)$ den Grad $3(d-1)^2$ in λ_0, λ_1 . Für $\lambda_1 \neq 0$ gibt es höchstens $3(d-1)^2 - d_1(d-d_1)$ Nullstellen, also gilt: $\lambda_1^{d_1(d-d_1)} | R(\lambda_0 f + \lambda_1 g)$, oder $t^{d_1(d-d_1)} | R(f + t g)$. Da g „allgemein“ gewählt war, verschwindet also R auf „fast allen“ Geraden durch f von der Ordnung $\geq d_1(d-d_1)$ in f , d.h. R verschwindet in f von der Ordnung $\geq d_1(d-d_1)$. Da für $1 \leq d_1 \leq d-1$ $d_1(d-d_1) \geq 1 \cdot (d-1) = d-1$ ist, folgt die Behauptung.

Als Anwendung ergibt sich der

Satz 5. Ist $f \in \mathbb{Z}[x_0, x_1, x_2]$ homogen vom Grad d , mit Höhe $\leq H$, die zugehörige komplexe Kurve nichtsingulär, so ist die Reduktion von f modulo p irreduzibel über $\mathbb{F}_p$ für jede Primzahl p mit

$$p > \left[\frac{1}{4} d(d+1)(d+2) \right]^{3(d-1)} \cdot H(f)^{3(d-1)}.$$

Beweis. Sei f wie im Satz angenommen und p eine Primzahl, modulo welcher f über $\mathbb{F}_p$ zerfällt. Sei K ein Zahlkörper, $\mathfrak{o}$ sein Ganzheitsring, so daß p in $K/\mathbb{Q}$ träge bleibt und f über $\mathfrak{o}/(p)$ zerfällt. Wir können also schreiben $f = g_1 g_2 + p \cdot h$ mit $g_1, g_2, h \in \mathfrak{o}[x_0, x_1, x_2]$. Für das Büschel $g_1 g_2 + t \cdot h$ ergibt sich dann:

$$R(g_1 g_2 + t \cdot h) \in \mathfrak{o}[t],$$

und in $t=0$ nach Lemma 6: $R(g_1 g_2 + t \cdot h) = t^{d-1} S(t)$ mit $S \in \mathfrak{o}[t]$. Setzt man jetzt $t=p$ ein, so hat man $R(f) = p^{d-1} \cdot S(p)$. $R(f)$ ist nach Voraussetzung $\neq 0$, Element von $\mathbb{Z}$, also auch $S(p) \in \mathbb{Z}$, d.h. $p^{d-1} \mid R(f)$. Die Behauptung folgt nun aus

$$p^{d-1} \leq \left[\frac{1}{4} \cdot d(d+1)(d+2) \cdot H(f) \right]^{3(d-1)^2}.$$

Bemerkung. Der Satz gibt eine weit bessere Abschätzung als das Korollar 2 zu Satz 3, gilt aber (zunächst) nur für nichtsinguläre Kurven. Im nächsten Paragraphen werden wir sehen, daß die gegebene Abschätzung in gewissem Sinn (unter geeigneten zahlentheoretischen Annahmen) auch optimal ist.

Wir wollen nun noch die geometrische Situation betrachten. Als Testobjekte nehmen wir Kurvenbüschel, die ja schon in den Beweisen von Lemma 6 und Satz 5 eine Rolle gespielt haben.

Sei also $\lambda_0 f + \lambda_1 g$ ein Büschel von Kurven vom Grad d über $\mathbb{C}$, dessen Kurven nicht alle reduzibel sind. Schränkt man die Gleichungen vom Grad d^2-1 , die wir für die Beschreibung der reduziblen Kurven im Linearsystem aller ebenen Kurven (vom Grad d) gefunden haben (vgl. § 2!), auf das Büschel ein, so werden also höchstens d^2-1 Punkte ausgeschnitten, d.h. höchstens d^2-1 Kurven sind reduzibel.

Enthält das Büschel eine nichtsinguläre Kurve, so ist $R(\lambda_0 f + \lambda_1 g) \neq 0$ und hat Grad $3(d-1)^2$ in λ_0, λ_1 . Da reduzible Kurven mindestens mit Vielfachheit $d-1$ zu zählen sind (Lemma 6), enthält das Büschel also höchstens $\frac{3(d-1)^2}{(d-1)} = 3(d-1)$ reduzible Kurven.

Wir fassen zusammen:

Satz 6. Gegeben sei ein Büschel ebener Kurven vom Grad d (über $\mathbb{C}$).

- a) Enthält das Büschel eine irreduzible Kurve, so höchstens $d^2 - 1$ reduzible.
- b) Enthält das Büschel eine nichtsinguläre Kurve, so höchstens $3(d-1)$ reduzible.

§ 5. Nichtsinguläre Kurven: Beispiele

Wir beginnen in der geometrischen Situation mit Beispielen von Kurvenbüscheln über $\mathbb{C}$, deren allgemeine Kurve nichtsingulär ist, und die so viele reduzible Kurven enthalten, wie die Abschätzung von Satz 6 angibt.

Beispiel. 1. Sei $d \geq 3$ und K irgendein algebraisch abgeschlossener Körper mit $\text{char}(K) \nmid d-1$. Wir betrachten das Netz von Kurven vom Grad d über K

$$f_{\lambda_0, \lambda_1, \lambda_2} = \lambda_0 x_0 (x_1^{d-1} - x_2^{d-1}) + \lambda_1 x_1 (x_2^{d-1} - x_0^{d-1}) + \lambda_2 x_2 (x_0^{d-1} - x_1^{d-1}),$$

$$(\lambda_0 : \lambda_1 : \lambda_2) \in \mathbb{P}^2.$$

2. Um zu zeigen, daß die allgemeine Kurve des Netzes nichtsingulär ist, genügt es nach Bertini nachzuweisen (siehe v. d. Waerden [23], S. 201!), daß in den Basispunkten des Netzes keine gemeinsamen Singularitäten vorliegen. Sei $\zeta \in K$ eine primitive $(d-1)$ -te Einheitswurzel, die es wegen $\text{char}(K) \nmid d-1$ gibt; als Basispunkte des Netzes findet man durch einfaches Rechnen:

$$(1:0:0), (0:1:0), (0:0:1), (1:\zeta^i:\zeta^j), \text{ für } 0 \leq i, j \leq d-2.$$

Nun ist

$$\frac{\partial f}{\partial x_0}(1, \zeta^i, \zeta^j) = (d-1)(-\zeta^i \lambda_1 + \zeta^j \lambda_2),$$

$$\frac{\partial f}{\partial x_1}(1, \zeta^i, \zeta^j) = -(d-1)\zeta^{j-i}(\lambda_2 - \zeta^{-j} \lambda_0),$$

$$\frac{\partial f}{\partial x_2}(1, \zeta^i, \zeta^j) = (d-1)\zeta^{i-j}(\lambda_1 - \zeta^{-i} \lambda_0),$$

und man sieht sofort, daß in $(1:\zeta^i:\zeta^j)$ nur die zu $(\lambda_0:\lambda_1:\lambda_2) = (1:\zeta^{-i}:\zeta^{-j})$ gehörige Kurve eine Singularität hat. Genauso findet man, daß in $(1:0:0)$ bzw. $(0:1:0)$ bzw. $(0:0:1)$ genau die zu $(\lambda_0:\lambda_1:\lambda_2) = (1:0:0)$ bzw. $(0:1:0)$ bzw. $(0:0:1)$ gehörige Kurve eine Singularität hat. Die allgemeine Kurve des Netzes ist also nichtsingulär.

3. Wir betrachten jetzt das Auftreten reduzibler Kurven. Die Gerade $x_1 - \zeta^i x_2$ ist ein Teiler von $f_{\lambda_0, \lambda_1, \lambda_2}$ genau dann, wenn $f_{\lambda_0, \lambda_1, \lambda_2}$ eingeschränkt auf $x_1 - \zeta^i x_2 = 0$ ergibt, d.h. wenn $f_{\lambda_0, \lambda_1, \lambda_2}(x_0, \zeta^i x_2, x_2) = (\lambda_1 - \zeta^{-i} \lambda_2) [\zeta^i x_2 (x_2^{d-1} - x_0^{d-1})] = 0$ gilt, also wenn $\lambda_1 - \zeta^{-i} \lambda_2 = 0$ ist.

Entsprechend findet man für das Abspalten der Geraden $x_2 - \zeta^i x_0$ die Bedingung $\lambda_2 - \zeta^{-i} \lambda_0 = 0$, sowie für die Gerade $x_0 - \zeta^i x_1$

$$\lambda_0 - \zeta^{-i} \lambda_1 = 0 \quad (0 \leq i \leq d-2).$$

Folglich ist $f_{\lambda_0, \lambda_1, \lambda_2}$ sicher reduzibel, wenn $(\lambda_0 : \lambda_1 : \lambda_2)$ Nullstelle der Form

$$\begin{aligned} S(\lambda_0, \lambda_1, \lambda_2) &= \prod_{i=0}^{d-2} [(\lambda_1 - \zeta^{-i} \lambda_2) (\lambda_2 - \zeta^{-i} \lambda_0) (\lambda_0 - \zeta^{-i} \lambda_1)] \\ &= (\lambda_1^{d-1} - \lambda_2^{d-1}) (\lambda_2^{d-1} - \lambda_0^{d-1}) (\lambda_0^{d-1} - \lambda_1^{d-1}) \end{aligned}$$

ist. S ist separabel und hat Grad $3(d-1)$.

4. Wählt man jetzt ein Büschel im Netz mit nichtsingulärer allgemeiner Kurve, so daß die Einschränkung von S darauf separabel bleibt (fast alle Büschel tun das: das Büschel darf nur nicht durch die endlich vielen Schnittpunkte der $3(d-1)$ Geraden $\lambda_0 - \zeta^{-i} \lambda_1 = 0$, $\lambda_1 - \zeta^{-j} \lambda_2 = 0$, $\lambda_2 - \zeta^{-k} \lambda_0 = 0$ gehen), so enthält das Büschel $3(d-1)$ reduzible Kurven.

5. Ist $K = \mathbb{C}$, so können wir Lemma 6 anwenden, und erhalten, wenn R_1 die Einschränkung der Resultante R auf das Netz ist: $S^{d-1} | R_1$, und aus Gradgründen bis auf eine Konstante $R_1 = S^{d-1}$.

Damit wäre gezeigt, daß die Abschätzung aus Satz 6 scharf ist.

Wir wollen uns nun der arithmetischen Situation zuwenden und zunächst eine Möglichkeit skizzieren, wie man versuchen kann, an die Abschätzung von Satz 5 heranzukommen:

1. Seien $f, g \in \mathbb{Z}[x_0, x_1, x_2]$ homogen vom Grad d , irreduzibel über $\overline{\mathbb{Q}}$, fest vorgegeben. Wir suchen $n \in \mathbb{Z}$, so daß $f + n \cdot g$ irreduzibel über $\overline{\mathbb{Q}}$ ist, aber modulo einer „großen“ Primzahl p zerfällt.

2. $\lambda_1, \dots, \lambda_t \in \overline{\mathbb{Q}}$ seien die t , so daß $f + t g$ über $\overline{\mathbb{Q}}$ zerfällt. Wir wählen einen Zahlkörper K , in dem dies alles geschieht, und schreiben $f + \lambda_i g = h_{1i} \cdot h_{2i}$; außerdem sei $N \in \mathbb{N}$ ein gemeinsamer Nenner der λ_i 's. Die Galoisgruppe $\text{Gal}(K/\mathbb{Q})$ permutiert die λ_i 's, so daß $F(t) := (t - \lambda_1) \cdots (t - \lambda_t) \in \mathbb{Q}[t]$ ist ($N^t F \in \mathbb{Z}[t]$).

3. Sei nun p eine Primzahl, $n \in \mathbb{Z}$ mit $p | F(n)$, $p \nmid N$. Dann gibt es eine Stelle $\mathfrak{p}$ von K mit $\mathfrak{p} | p$, $\mathfrak{p} | n - \lambda_i$ (für ein i), also mod $\mathfrak{p}$: $f + n g \equiv f + \lambda_i g \equiv h_{1i} h_{2i}$, d.h. $f + n g$ ist modulo p reduzibel (oder verschwindet identisch).

4. Um „große“ Primzahlen zu erreichen ($p \approx F(n)$), setzen wir jetzt voraus, daß die λ_i 's über $\mathbb{Q}$ konjugiert sind. Dann ist nämlich $F(t)$ über $\mathbb{Q}$ irreduzibel. Gilt eine Vermutung von Bouniakowsky, die unten erläutert wird, so gibt es eine Konstante c_1 (von F abhängig) mit der Eigenschaft: Es gibt unendlich viele $n \in \mathbb{N}$, so daß $F(n)$ einen Primteiler $p \geq c_1 n^t$ besitzt. Andererseits ist klar, daß es eine von f, g abhängige Konstante c_2 gibt, so daß $H(f + n g) \leq c_2 n$ ist. Man erhielte so:

$$p \geq c_1 \cdot n^t \geq c_1 \left(\frac{H}{c_2} \right)^t = \frac{c_1}{c_2^t} \cdot H^t,$$

und zwar für unendlich viele $n \in \mathbb{N}$.

5. Wir werden unten Büschel $f+tg$ konstruieren mit $3(d-1)$ reduziblen Kurven, so daß $f+ng \in \mathbb{Z}[x_0, x_1, x_2]$ nichtsingulär (über $\mathbb{C}$) ist. Modulo der erwähnten Vermutung wäre dann die Abschätzung in Satz 5 optimal.

Nun zu der angeführten zahlentheoretischen Vermutung. Sie findet sich in Bouniakowsky [1], S. 328 (vgl. auch Dickson [4], S. 333).

Bouniakowsky-Vermutung. Ist $f \in \mathbb{Z}[t]$ irreduzibel, $N = \text{ggT}\{f(n) : n \in \mathbb{N}\}$, so gibt es unendlich viele $n \in \mathbb{N}$, für die $\left| \frac{f(n)}{N} \right|$ prim ist.

Bemerkung. 100 Jahre nach Bouniakowsky (1857) stellte auch Schinzel eine Vermutung auf, die obige Vermutung als Spezialfall hat (Hypothese H). Siehe dazu Schinzel/Sierpiński [15], Halberstam/Richert [8], S. 2.

Die obigen Erörterungen werden wir nun benutzen, um im arithmetischen Fall Beispiele zu erhalten:

1. (Etwas Arithmetik) Das Polynom $x^3 - 3x - 1 \in \mathbb{Q}[x]$ ist irreduzibel über $\mathbb{Q}$, hat Diskriminante 3^4 ; also ist $\mathbb{Q}(\alpha)/\mathbb{Q}$ zyklisch vom Grad 3, wenn α eine Nullstelle des Polynoms ist. Die Konjugierten seien $\sigma\alpha = \alpha'$, $\sigma^2\alpha = \alpha''$, für die man wählen kann: $\alpha' = 2 - \alpha^2$, $\alpha'' = -2 - \alpha + \alpha^2$. Der Ganzheitsring ist $\mathbb{Z}[\alpha]$ (da die Körperdiskriminante wegen wilder Verzweigung der 3 mindestens 3^3 sein muß, andererseits sich nur um ein Quadrat von 3^4 unterscheiden kann, also gleich 3^4 ist). $\alpha, \alpha', \alpha''$ sind Einheiten. Bei der reellen Einbettung kann man wählen: $\alpha \approx -1.53$, $\alpha' \approx -0.35$, $\alpha'' \approx 1.88$.

Behauptung. Das Polynom $x^{d-1} - \alpha$ ist irreduzibel über $\mathbb{Q}(\alpha)$.

Beweis. Nach Lang [11], S. 221, genügt es zu zeigen, daß $\alpha \notin \mathbb{Q}(\alpha)^p$, für $p|d-1$, und $\alpha \notin -4 \cdot \mathbb{Q}(\alpha)^4$, falls $4|d-1$, ist. Eine gerade Potenz kann α aus Vorzeichengründen nicht sein, und ebenso ist α nicht von der Form $-4\beta^4$, da sonst auch α'' diese Form hätte. Es bleibt zu zeigen, daß es kein $\beta \in \mathbb{Q}(\alpha)$ gibt mit $\beta^n = \alpha$, wo $n \geq 3$ ungerade ist. Wir versuchen, die Gleichung von β aufzustellen: $\beta^3 - A \cdot \beta^2 + B \cdot \beta - 1 = 0$, mit $A = \beta + \beta' + \beta''$, $B = \beta\beta' + \beta\beta'' + \beta'\beta'' \in \mathbb{Z}$. Nun kann man abschätzen $-1.15 \lesssim \beta \lesssim -1$, $-1 \lesssim \beta' \lesssim -0.70$, $1 \lesssim \beta'' \lesssim 1.23$, und damit folgt wegen $A, B \in \mathbb{Z}$ schnell: $A = -1$, $B = -1$, also: $0 = \beta^3 + \beta^2 - \beta - 1 = (\beta + 1)(\beta^2 - 1)$, was natürlich nicht sein kann.

Die Wurzeln der Gleichung $x^{d-1} - \alpha = 0$ seien mit ξ_i , $1 \leq i \leq d-1$, bezeichnet, analog $\xi_i'^{d-1} = \alpha'$, $\xi_i''^{d-1} = \alpha''$. Die $3(d-1)$ Zahlen ξ_i, ξ_i', ξ_i'' sind dann konjugiert über $\mathbb{Q}$.

2. Sei nun $l_0 = x_0 + \alpha x_1 + \alpha^2 x_2$, $l_1 = \sigma l_0$, $l_2 = \sigma^2 l_0$. Wir betrachten das Netz

$$f_{\lambda_0, \lambda_1, \lambda_2} = \lambda_0 l_0 (l_1^{d-1} - \alpha l_2^{d-1}) + \lambda_1 l_1 (l_2^{d-1} - \alpha' l_0^{d-1}) + \lambda_2 l_2 (l_0^{d-1} - \alpha'' l_1^{d-1}).$$

Zur Abkürzung sei $f_0 = l_0 (l_1^{d-1} - \alpha l_2^{d-1})$, $f_1 = \sigma f_0$, $f_2 = \sigma^2 f_0$. Die Transformationsmatrix von den x_i zu den l_i hat Determinantenquadrat

$$\begin{vmatrix} 1 & \alpha & \alpha^2 \\ 1 & \alpha' & \alpha'^2 \\ 1 & \alpha'' & \alpha''^2 \end{vmatrix}^2 = \text{Diskriminante von } \alpha = 81,$$

und mit $\alpha\alpha'\alpha'' = 1$ kann man sich leicht überlegen, daß das Netz hier in das Netz des ersten Beispiels transformiert werden kann, falls $\text{char}(K) \neq 3$ ist. So findet man: Die allgemeine Kurve des Netzes ist nichtsingulär, falls $\text{char}(K) \nmid 3(d-1)$.

3. Wie in dem „geometrischen“ Beispiel findet man für das Abspalten gewisser Geraden von $f_{\lambda_0, \lambda_1, \lambda_2}$:

$$l_1 - \xi_i l_2 \text{ spaltet ab} \Leftrightarrow \xi_i \alpha' \lambda_1 - \lambda_2 = 0,$$

$$l_2 - \xi_i' l_0 \text{ spaltet ab} \Leftrightarrow \xi_i' \alpha'' \lambda_2 - \lambda_0 = 0,$$

$$l_0 - \xi_i'' l_1 \text{ spaltet ab} \Leftrightarrow \xi_i'' \alpha \lambda_0 - \lambda_1 = 0.$$

Ist wieder $S(\lambda_0, \lambda_1, \lambda_2)$ das Produkt dieser $3(d-1)$ Linearfaktoren ($S \in \mathbb{Q}(\alpha)[\lambda_0, \lambda_1, \lambda_2]$), die für $\text{char}(K) \nmid 3(d-1)$ alle verschieden sind, so ergibt sich über $\mathbb{C}$ für die Einschränkung der Resultante auf das Netz: $R_1 = S^{d-1}$.

4. Man überlegt sich leicht, daß genau dann $f_{\lambda_0, \lambda_1, \lambda_2} \in \mathbb{Q}[x_0, x_1, x_2]$ ist, wenn es sich schreiben läßt als $\text{Sp}(\omega f_0)$, wo $\omega \in \mathbb{Q}(\alpha)$. (Sp bezeichnet die Spurbildung von $\mathbb{Q}(\alpha)$ nach $\mathbb{Q}$.) Wir nehmen ein solches $\text{Sp}(\omega f_0)$ her. Dann ist $\lambda_0 = \omega$, $\lambda_1 = \omega'$, $\lambda_2 = \omega''$, und man sieht sofort, daß die $3(d-1)$ Linearfaktoren aus 3. wegen $\xi_i, \xi_i', \xi_i'' \notin \mathbb{Q}(\alpha)$ für $\omega \neq 0$ nicht verschwinden. Also ist

$$R_1(\omega, \omega', \omega'') \neq 0,$$

d.h. $\text{Sp}(\omega f_0)$ ist (über $\mathbb{C}$) nichtsingulär.

5. Wir betrachten nun ein Büschel $\text{Sp}(\beta f_0) + t \text{Sp}(\gamma f_0)$. Dann ist $\lambda_0 = \beta + t\gamma$, $\lambda_1 = \beta' + t\gamma'$, $\lambda_2 = \beta'' + t\gamma''$, und man sieht sofort, daß die aus $\xi_i \alpha' \lambda_1 - \lambda_2$ etc. entstehenden $3(d-1)$ linearen Polynome $\in \mathbb{Q}[t]$ über $\mathbb{Q}$ konjugiert und paarweise verschieden sind. Das Produkt sei $F(t)$. F ist aus $\mathbb{Q}[t]$, hat Grad $3(d-1)$ und ist irreduzibel über $\mathbb{Q}$. Damit sind wir schließlich in der Situation, die in der Vorbemerkung diskutiert wurde. Wir fassen das Entscheidende nochmals zusammen:

Ergebnis. Falls die Bouniakowsky-Vermutung richtig ist, gibt es für jedes $d \geq 3$ eine Konstante $C > 0$ und unendlich viele $f \in \mathbb{Z}[x_0, x_1, x_2]$ homogen vom Grad d , nichtsingulär (über $\mathbb{C}$), mit der Eigenschaft: Es gibt eine Primzahl p mit $p \geq C \cdot H(f)^{3(d-1)}$, so daß $f \bmod p$ über $\mathbb{F}_p$ zerfällt.

6. Zur Demonstration wird das Verfahren für $d=3$ an einem Beispiel durchgeführt: Wir wählen $\beta = \frac{5-2\alpha^2}{9}$, $\gamma = \frac{3+\alpha-\alpha^2}{9}$ und $g = \text{Sp}(\beta f_0)$, $h = \text{Sp}(\gamma f_0)$. Dann wird mit obigen Bezeichnungen $\lambda_0 = \beta + t\gamma$ usw., und durch einfaches Rechnen in $\mathbb{Q}(\alpha)$ findet man:

$$g = x_0^3 + 2x_0^2x_1 + 5x_0^2x_2 + 2x_0x_1^2 + 6x_0x_1x_2 + 5x_0x_2^2 - 2x_1^3 - x_1^2x_2 + 2x_1x_2^2 - 2x_2^3,$$

$$h = x_0^2x_2 + x_0x_1^2 + 3x_0x_2^2 + x_1^3 - 5x_1x_2^2 - x_2^3,$$

$$F(n) = \frac{n^6 + 6n^5 - 12n^4 + 20n^3 - 21n^2 - 12n + 37}{3^9}; \quad \tilde{F}(n) = 3^9 F(n).$$

In der folgenden Tabelle sind die $n \in \mathbb{Z}$ mit $|n| \leq 63$ aufgelistet, für die $\tilde{F}(n)$ prim ist. p bezeichnet die zugehörige Primzahl, H die Höhe von $g + nh$. Außerdem ist noch $\frac{\ln p}{\ln H}$ angegeben.

n	p	H	$\frac{\ln p}{\ln H}$
-51	15442246891	257	4.23
-45	7145524927	227	4.18
-42	4666025737	212	4.16
-39	2948419459	197	4.13
-29	462763999	147	4.00
-24	139057669	122	3.90
-9	82279	47	2.94
-8	4933	42	2.28
-5	13553	27	2.89
-3	2357	17	2.74
-2	503	12	2.50
0	37	6	2.02
1	19	8	1.42
3	1567	14	2.79
4	8101	18	3.11
9	819811	43	3.62
15	15402007	73	3.86
16	22358629	78	3.88
18	44199577	88	3.93
22	141693193	108	4.01
42	6237283033	208	4.23
49	15469263091	243	4.27
51	19587854719	253	4.28
54	27450952201	268	4.30
60	51170323717	298	4.33
63	68294002807	313	4.34

§ 6. Singuläre Kurven

Anders als im Fall der nichtsingulären Kurven, wo die Abschätzungen von § 4, Satz 5 und Satz 6, (modulo Bouniakowsky-Vermutung im arithmetischen Fall) durch Beispiele in § 5 als optimal nachgewiesen werden konnten, sind für die singulären Kurven Analoga der zitierten Sätze, die über die Aussagen von § 2 hinausgehen, noch nicht bekannt. Wir werden hier nur einen Typ (rationaler) singulärer Kurven betrachten und dafür Aussagen wie in § 5 machen.

Sei $d \geq 2$, K ein algebraisch abgeschlossener Körper. Wir betrachten im folgenden homogene Polynome $f = x_0 A(x_1, x_2) + B(x_1, x_2) \in K[x_0, x_1, x_2]$ mit $A, B \in K[x_1, x_2]$ vom Grad $d-1$ bzw. d . Solche Kurven haben Ordnung $\geq d-1$ im Punkt $(1:0:0)$. Bezeichnet F die (gewöhnliche) Resultante von B und A , $F = R(B, A)$, (siehe v. d. Waerden [21], § 34), so gilt:

Lemma 7. f ist genau dann reduzibel, wenn $F=0$ ist.

Beweis. „ $\Leftarrow$ “. $F=0$ impliziert, daß A und B einen nichtkonstanten gemeinsamen Faktor haben, der dann natürlich auch von f abspaltet.

„ $\Rightarrow$ “. Ist f reduzibel, so auch als lineares Polynom in x_0 über dem faktoriellen Ring $K[x_1, x_2]$. Daher müssen A und B einen gemeinsamen Faktor haben, d.h. $F=0$.

Setzt man A und B mit unbestimmten Koeffizienten an,

$$A = a_0 x_1^{d-1} + \cdots + a_{d-1} x_2^{d-1}, \quad B = b_0 x_1^d + \cdots + b_d x_2^d,$$

so ist bekanntlich

$$F = R(B, A) = \begin{vmatrix} b_0 & \cdots & b_d & & \\ & \ddots & & \ddots & \\ & & b_0 & \cdots & b_d \\ a_0 & \cdots & a_{d-1} & & \\ & \ddots & & \ddots & \\ & & a_0 & \cdots & a_{d-1} \end{vmatrix}$$

ein separables homogenes Polynom $\in K[a_i, b_i]$ vom Grad $d + (d-1) = 2d-1$, woraus sich unmittelbar ergibt:

Satz 7. Im Linearsystem der ebenen Kurven vom Grad d ($d \geq 2$), die in $(1:0:0)$ Multiplizität $\geq d-1$ haben, bilden die reduziblen Kurven eine Hyperfläche vom Grad $2d-1$.

Da eine „allgemeine“ Gerade in diesem Linearsystem die Hyperfläche der reduziblen Kurven in genau $2d-1$ Punkten schneiden wird, ergibt sich

Korollar 1 ($d \geq 3$). Es gibt Büschel von ebenen Kurven vom Grad d (über K), mit allgemeiner Kurve singulär irreduzibel, die genau $2d-1$ reduzible Kurven enthalten.

Da im Fall $d=3$ jedes Kurvenbüschel, dessen allgemeine Kurve singulär ist, eine Singularität der Ordnung ≥ 2 (in einem Basispunkt) hat, ergibt sich

Korollar 2. Ein Kubikenbüschel über K , dessen allgemeine Kurve singulär irreduzibel ist, besitzt, richtig gezählt, genau 5 reduzible Kurven.

Bemerkung. Bei Kubiken kann also ein Büschel, dessen allgemeine Kurve nichtsingulär ist, mehr reduzible Kurven enthalten (nämlich 6), als ein Büschel, dessen allgemeine Kurve singulär, aber irreduzibel ist. Wir wollen nun konkret ein Beispiel betrachten. (Man beachte, daß auch der Fall $d=2$ zugelassen ist, den wir in den vorhergehenden Paragraphen etwas vernachlässigt haben!):

1. Sei $f_n = x_0(x_1^{d-1} + nx_2^{d-1}) + (nx_1^d + 2x_2^d) \in \mathbb{Z}[x_0, x_1, x_2]$. Die zugehörige Resultante berechnet sich zu $F(n) = R(nx_1^d + 2, x_1^{d-1} + n) = n^{2d-1} + 2^{d-1}$. $F \in \mathbb{Z}[n]$ ist irreduzibel. (Nach Lang [11], S. 221, ist nur zu zeigen, daß $-2^{d-1} \notin \mathbb{Q}^p$ für $p|2d-1$ ist, was aber wegen $\text{ggT}(2d-1, d-1)=1$ klar ist.) Ist nun, für $n \in \mathbb{N}$, $n \geq 2$, $F(n) = p$ prim, so gilt mit $H = H(f_n) = n$: $p \geq H^{2d-1}$. Wir formulieren als

Ergebnis. Gilt die Bouniakowsky-Vermutung, so gibt es für jedes $d \geq 2$ unendlich viele $f \in \mathbb{Z}[x_0, x_1, x_2]$ homogen vom Grad d , irreduzibel über $\mathbb{Q}$, singulär für $d \geq 3$ (nichtsingulär für $d=2$), derart, daß die Reduktion von f modulo einer Primzahl p über $\mathbb{F}_p$ zerfällt mit

$$p \geq H(f)^{2d-1}.$$

2. Zur Illustration des obigen Beispiels wurden einige Kurven ausgewählt, für die $F(n)$ prim ist.

d	$H = n$	$p = F(n)$	$\frac{\ln p}{\ln H}$
2	5	127	3.01
2	45	91127	3.00
2	1283	2111932189	3.00
3	7	16811	5.00
3	73	2073071597	5.00
4	9	4782977	7.00
4	17	410338681	7.00
5	3	19699	9.00
7	3	1594387	13.00
9	3	129140419	17.00

Literatur

- [1] V. Bouniakowsky, Nouveaux théorèmes relatifs à la distinction des nombres premiers et à la décomposition des entiers en facteurs, Mém. acad. sc. St. Pétersbourg (6), Sc. math. et phys. 6 (1857), 305—329.
- [2] J. L. Coolidge, A Treatise on Algebraic Plane Curves, Oxford 1931.
- [3] M. Deuring, Reduktion algebraischer Funktionenkörper nach Primdivisoren des Konstantenkörpers, Math. Z. 47 (1942), 643—654.
- [4] L. E. Dickson, History of the Theory of Numbers. I, New York 1971.
- [5] M. Eichler, Zum Hilbertschen Irreduzibilitätssatz, Math. Ann. 116 (1939), 742—748.
- [6] M. Eichler, Einführung in die Theorie der algebraischen Zahlen und Funktionen, Boston 1963.
- [7] P. Griffiths and J. Harris, Principles of Algebraic Geometry, New York 1978.
- [8] H. Halberstam and H.-E. Richert, Sieve Methods, London-New York-San Francisco 1974.
- [9] R. Hartshorne, Algebraic Geometry, Berlin-Heidelberg-New York 1977.
- [10] W. V. D. Hodge and D. Pedoe, Methods of Algebraic Geometry. II, Cambridge 1952.
- [11] S. Lang, Algebra, Reading-Amsterdam-London 1965.
- [12] E. Netto, Vorlesungen über Algebra, zweiter Band, Stuttgart 1900.
- [13] E. Noether, Ein algebraisches Kriterium für absolute Irreduzibilität, Math. Ann. 85 (1922), 26—33.
- [14] A. Ostrowski, Zur arithmetischen Theorie der algebraischen Größen, Göttinger Nachrichten (1919), 279—298.
- [15] A. Schinzel et W. Sierpiński, Sur certaines hypothèses concernant les nombres premiers, Acta Arith. 4 (1958), 185—208, corrig. Acta Arith. 5 (1959), 259.
- [16] W. Schmidt, Equations over Finite Fields, Lecture Notes in Math. 536, Berlin-Heidelberg-New York 1976.
- [17] I. Shafarevich, Lectures on Minimal Models and Birational Transformations of Two Dimensional Schemes, Bombay 1966.
- [18] I. Shafarevich, Basic Algebraic Geometry, Berlin-Heidelberg-New York 1977.
- [19] G. Shimura, Reduction of Algebraic Varieties with Respect to a Discrete Valuation of the Basic Field, Amer. J. Math. 77 (1955), 134—176.
- [20] J. J. Sylvester, On a Linear Method of Eliminating between Double, Treble, and Other Systems of Algebraic Equations, Philosophical Magazine 18 (1841), 425—435.
- [21] B. L. v. d. Waerden, Algebra. I, 8. Auflage, Berlin-Heidelberg-New York 1971.
- [22] B. L. v. d. Waerden, Algebra. II, 3. Auflage, Berlin-Heidelberg-New York 1955.
- [23] B. L. v. d. Waerden, Einführung in die algebraische Geometrie, 2. Auflage, Berlin-Heidelberg-New York 1973.