

Werk

Titel: Inventiones Mathematicae

Verlag: Springer

Jahr: 1983

Kollektion: Mathematica

Werk Id: PPN356556735_0072

PURL: http://resolver.sub.uni-goettingen.de/purl?PID=PPN356556735_0072 | LOG_0024

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

Über das Abelsche Analogon des Lindemannschen Satzes I

G. Wüstholz

Fachbereich 7 – Mathematik, Universität-Gesamthochschule,
Gaußstrasse 20, D-5600 Wuppertal, Bundesrepublik Deutschland

1. Einleitung und Ergebnisse

Genau vor hundert Jahren, im Jahre 1882, bewies F. Lindemann [7] ein bemerkenswertes Resultat über lineare Unabhängigkeit von Werten der Exponentialfunktion. Insbesondere bewies er das folgende Resultat. Es seien $\alpha_1, \dots, \alpha_n$ algebraische Zahlen, welche linear unabhängig über den rationalen Zahlen seien. Dann sind die Zahlen

$$e^{\alpha_1}, \dots, e^{\alpha_n}$$

algebraisch unabhängig über dem Körper der algebraischen Zahlen. Beinahe fünfzig Jahre lang war dies das einzige ernsthafte Resultat über algebraische Unabhängigkeit, bevor Siegel Lindemann's Methode auf sogenannte *E*-Funktionen ausdehnte und so zum Beispiel algebraische Unabhängigkeit von Werten der Besselfunktion bewies. Siegels Methode wurde später beträchtlich von Shidlovskij erweitert.

Erst kürzlich entwickelten nun D.W. Masser und der Autor [10, 11] eine neue Methode, um die algebraische Unabhängigkeit von Werten einer weiteren Klasse von Funktionen zu beweisen, welche zum Beispiel abelsche Funktionen enthält. Diese Funktionen treten auf als Komponenten der Exponentialabbildung einer algebraischen Gruppe. Die Methode gründet sich auf die sogenannten Nullstellenabschätzungen auf Gruppenvarietäten, welche von D.W. Masser und dem Autor in [9] eingeführt wurden. Zum Beispiel gilt das folgende Resultat. Es sei $\wp$ eine Weierstraßsche elliptische Funktion, welche über $\overline{\mathbb{Q}}$ definiert sei, und N und k seien positive ganze Zahlen mit $N \geq 3 \cdot 2^{k+2}(k+7)$. Dann sind wenigstens k der Zahlen

$$\wp(\pi), \dots, \wp(\pi^N)$$

algebraisch unabhängig über $\overline{\mathbb{Q}}$.

In einem Spezialfall verschärfte kürzlich P. Philippon [14, 15] diese Methode und erzielte das folgende Resultat. Sei $\wp$ wie oben die Weierstraßsche

elliptische Funktion und u eine komplexe Zahl sowie α eine algebraische Zahl vom Grade $d \geq 2$. Ist $\wp$ definiert für die Zahlen $u, \alpha u, \dots, \alpha^{d-1}u$, so sind wenigstens $d/6$ der Zahlen

$$\wp(u), \wp(\alpha u), \dots, \wp(\alpha^{d-1}u)$$

algebraisch unabhängig über $\mathbb{Q}$. Ist u ein algebraischer Punkt unendlicher Ordnung und besitzt $\wp$ komplexe Multiplikation, so ist Philippon unter Benutzung einer Idee des Autors, die wesentlich für die vorliegende Arbeit ist, in der Lage, die Zahl $d/6$ durch $\max(1, (d-2)/2)$ zu ersetzen.

In dieser Arbeit werden wir ein Resultat über die algebraische Unabhängigkeit von Werten abelscher Funktionen beweisen, das unter gewissen zusätzlichen Voraussetzungen das abelsche Analogon des Lindemannschen Ergebnisses liefert. Dieses Ergebnis wurde in [19] vom Autor angekündigt. Das erste Resultat in dieser Richtung und Schärfe stammt von G.V. Choodnovsky [4], der den elliptischen Fall unseres Resultats für $n \leq 3$ bewies.

Wir werden nun einige Bezeichnungen einführen, um unser Ergebnis dann anzugeben. Dazu sei A eine einfache abelsche Varietät, die über $\mathbb{Q}$ definiert sei und die Dimension d besitze. Der Ring der Endomorphismen $\text{End } A$ von A ist eine Divisionsalgebra und wir setzen $k = (\text{End } A) \otimes \mathbb{Q}$ und $m = [k:\mathbb{Q}]$. Sei $\mathcal{A}$ eine integrale Unterálgebra über k von $M_n(k)$ der Dimension n über k . Schließlich sei $\mathcal{O}$ ein Untermodul von $\mathcal{A}$ über $\text{End } A$, der gleichzeitig eine Ordnung in $\mathcal{A}$ sei.

Bezeichnen wir mit $T(A^n)$ den Tangentialraum der abelschen Varietät im neutralen Element der Gruppe, so operiert die Algebra $\mathcal{O}$ in natürlicher Weise auf diesem Vektorraum. Diese Operation kann in der folgenden Weise beschrieben werden. Es sei γ ein Element von $\mathcal{O}$. Da $\mathcal{O}$ eine Ordnung in $\mathcal{A}$ und eine Unterálgebra von $M_n(k)$ ist, kann γ als eine Matrix $\gamma = (\gamma_{ij})$ mit Elementen γ_{ij} aus $\text{End } A$ geschrieben werden. Diese können wir als Endomorphismen von $T(A)$, dem Tangentialraum von A im neutralen Element, auffassen, welche das Periodengitter stabilisieren. Sei $\mathbf{z} = (\mathbf{z}_1, \dots, \mathbf{z}_n)$ in $T(A^n)$ für $\mathbf{z}_i$ in $T(A)$ und $1 \leq i \leq n$. Dann setzen wir

$$\gamma \cdot \mathbf{z} = \mathbf{w},$$

wobei $\mathbf{w} = (\mathbf{w}_1, \dots, \mathbf{w}_n)$ definiert ist durch

$$\mathbf{w}_i = \gamma_{i,1} \mathbf{z}_1 + \dots + \gamma_{i,n} \mathbf{z}_n \quad (1 \leq i \leq n).$$

Hierdurch wird eine Operation von $\mathcal{O}$ auf A^n mittels der Exponentialabbildung definiert. Wir bezeichnen für Elemente γ in $\mathcal{O}$ und g in A^n mit $\gamma \cdot g$ das Bild von g unter dieser Operation. Ferner sei $\rho = \rho(g; \mathcal{O})$ die Dimension der kleinsten analytischen Untergruppe B (s. [21]) von A^n , welche über $\bar{\mathbb{Q}}$ definiert sei und die Bahn $\mathcal{O}g$ von g enthält. $\mathcal{O}$ stabilisiert dann B und man erhält damit eine Darstellung von $\mathcal{O}$ in der allgemeinen linearen Gruppe $GL(T(B), \bar{\mathbb{Q}})$. Diese Darstellung ordnet einem Element aus $\mathcal{O}$ sein Differential zu. Da die Elemente aus $\mathcal{O}$ wie auch B über $\bar{\mathbb{Q}}$ definiert sind, erhalten wir ein Element aus $GL(T(B), \bar{\mathbb{Q}})$ (siehe hierzu auch [14]). Ist $\rho = 1$, so ist $GL(T(B), \bar{\mathbb{Q}}) \cong \bar{\mathbb{Q}}^*$.

Satz 1. *Es sei $\alpha \neq 0$ ein Element in $T(A^n)(\bar{\mathbb{Q}})$ und $g = \exp_{A^n}(\alpha)$ sein Bild in A^n unter der Exponentialabbildung $\exp_{A^n}: T(A^n) \rightarrow A^n$ der Lieschen Gruppe A^n . Ist $X(g)$ der Abschluß von g über $\bar{\mathbb{Q}}$ in der Zariski-Topologie von A^n und gilt $\rho(g; \mathcal{O}) = 1$, so gilt*

$$2 \dim X(g) \geq nm.$$

Wir sollten an dieser Stelle bemerken, daß die Einschränkung $\rho(g; \mathcal{O}) = 1$ nicht wirklich notwendig ist. Im Beweis von Satz 1 werden wir sie an zwei Stellen benutzen. Zum einen werden wir sie im analytischen Teil benutzen, wo wir das Schwarzsche Lemma benötigen. Diese Einschränkung erlaubt es, im wesentlichen ein Schwarzsches Lemma in einer Variablen zu benutzen. Dies ist völlig klassisch. Lassen wir diese Einschränkung fallen, so müssen wir eine schwierigere Version eines nicht effektiven Schwarzschen Lemmas für mehrere Variablen anwenden. Diese wurde von J.C. Moreau bewiesen (s. [18], Corollaire 7.6.2). Das zweite Hindernis ist etwas ernsthafter. Die Bedingung $\rho(g; \mathcal{O}) = 1$ zieht nach sich, daß wir mit einer analytischen Untergruppe der Dimension eins arbeiten und daher nur eine Derivation zur Verfügung haben. Nun benötigen wir im Beweis des Satzes eine Nullstellenabschätzung mit Multiplizitäten. Da wir nur mit einer Derivation arbeiten, können wir ein Ergebnis von D.W. Masser und dem Autor [12] benutzen, wo die dafür notwendige Nullstellenabschätzung bewiesen wird. Vor kurzem hat nun der Autor diese Nullstellenabschätzungen mit Multiplizitäten erweitert auf Nullstellenabschätzungen mit Multiplizitäten, in die eine beliebige Anzahl von Derivationen eingehen können. Benutzt man diese Ergebnisse, so kann der Satz leicht auch ohne die Einschränkung $\rho(g; \mathcal{O}) = 1$ bewiesen werden. Mit den Bezeichnungen in Satz 1 erhalten wir dann

$$2\rho(g; \mathcal{O}) \dim X(g) \geq mn.$$

Da die Dimension der abelschen Varietät gleich nd ist, gibt uns Satz 1 die Abschätzung

$$nd \leq 2 \dim X(g) \leq 2nd.$$

Es ist bekannt, daß die Dimension m des Körpers k die Zahl $2d$ teilt. Damit erhalten wir offenbar die besten Ergebnisse, wenn $m = 2d$ ist. Dies ist der Fall, wenn die abelsche Varietät A vom Typ CM ist. Dann erhalten wir das folgende Resultat.

Korollar 1. *Mit denselben Bezeichnungen wie in Satz 1 erhalten wir für abelsche Varietäten vom Typ CM , daß $X(g) = A^n$ ist, falls $\rho(g; \mathcal{O}) = 1$ ist.*

Wir geben nun eine Anwendung dieses Resultats auf elliptische Kurven mit komplexer Multiplikation. Es sei E eine elliptische Kurve definiert über $\bar{\mathbb{Q}}$ mit komplexer Multiplikation und zugehörigem Körper k vom Grade 2 über den rationalen Zahlen. Sei $\wp$ die zugehörige Weierstraßsche elliptische Funktion. Ist F ein algebraischer Zahlkörper vom Grade n über k , so kann F dargestellt werden als eine Unter algebra über k von $M_n(k)$ der Dimension n . Eine Ordnung von F hat dann die Dimension $2n$ über $\bar{\mathbb{Q}}$. Benutzt man dies, so erhält man aus dem Korollar 1 leicht das folgende elliptische Analogon des Satzes von Lindemann.

Korollar 2. *Sei E eine elliptische Kurve definiert über $\bar{\mathbb{Q}}$ mit komplexer Multiplikation. Die algebraischen Zahlen $\alpha_1, \dots, \alpha_n$ seien linear unabhängig über k . Dann sind die Zahlen*

$$\wp(\alpha_1), \dots, \wp(\alpha_n)$$

algebraisch unabhängig über den rationalen Zahlen.

Wir beenden diesen Abschnitt mit einigen Bemerkungen zum Beweis von Satz 1. Der Beweis ist sehr kompliziert, doch haben wir versucht, ihn so transparent wie möglich zu machen, indem wir die verschiedenen Ingredienzien separiert haben. Wir hoffen, daß sie dadurch so in sich abgeschlossen wie möglich geworden sind. Die grobe Idee des Beweises ist sehr ähnlich zu der, welche der Lindemann-Siegelschen Methode zugrunde liegt. Diese ist sehr klar zum Beispiel in dem Buch von Th. Schneider [16] dargestellt. Der Unterschied besteht sehr grob und vereinfacht gesprochen darin, daß die lineare Algebra durch die kommutative Algebra ersetzt werden muß. Der Beweis von Satz 1 kann in fünf Hauptschritte unterteilt werden. Der erste Schritt besteht in der Konstruktion des Hilfsideals. Dies wird ein gewisses Ideal in einem Polynomring über einem Zahlkörper sein und die bisher gebräuchliche Hilfsfunktion ersetzen. Hier benützen wir unter anderem eine Idee von P. Philippon [13]. Sie besteht in der Verwendung von Polynomen in sehr vielen Variablen, um dadurch Polynome mit ganzen Koeffizienten zu erhalten. Dies wurde auch von D.W. Masser und dem Autor in [11] benutzt, sowie später auch von Philippon in [15]. Der zweite Schritt besteht in einer Verallgemeinerung einer Idee von D.W. Masser, die von M. Anderson in seiner Thesis [1] ausgearbeitet wurde, siehe auch Choodnovsky [4]. Wir erweitern diese ingeniose Idee auf beliebige algebraische Gruppen. Der nächste Schritt ist eine Nullstellenabschätzung mit hohen Multiplizitäten und nur wenigen Derivationen. Diese Hilfsmittel wurden von D.W. Masser und dem Autor in [9, 11, 12 und 20] entwickelt in dem Falle, daß die Multiplizität nicht zu hoch ist. Da wir aber mit hohen Multiplizitäten arbeiten müssen, müssen wir zusätzliche Betrachtungen anstellen, um diese Schwierigkeiten zu bewältigen. Diese Multiplizitätsabschätzungen erlauben es, den Spezialisierungstrick von Lindemann zu immitieren, um ein System von homogenen Polynomen zu gewinnen, welches keine nichttrivialen Nullstellen besitzt. Dies ist der vierte Schritt. Im letzten Schritt haben wir die Elimination durchzuführen. Hier wenden wir alte Techniken der Resultantenbildung an, wie sie zum Beispiel in dem Buch von Macaulay [8] dargestellt sind. Die Benutzung der Resultanten ersetzt das Lösen von linearen Gleichungssystemen, wie dies in der Lindemann-Siegelschen Methode gebräuchlich ist. Unsere Elimination spiegelt die Tatsache wider, daß die Projektion von einem Produkt $\mathbb{P}^n \times \mathbb{A}^m$ eines projektiven Raumes mit einem affinen Raum auf $\mathbb{A}^m$ eine abgeschlossene Abbildung ist. Dies ist nicht mehr länger der Fall, wenn man den projektiven Raum $\mathbb{P}^n$ durch einen affinen Raum $\mathbb{A}^n$ ersetzt. Dies ist auch der Grund für die Schwierigkeiten, die auftauchen, wenn man versucht, diese Methoden auf nicht-vollständige algebraische Gruppen auszudehnen. So sind wir zum Beispiel nicht in der Lage, mit Hilfe von unserer Methode einen neuen Beweis des Lindemannschen Satzes zu geben.

Alle von nun an auftretenden algebraischen Objekte seien über einem algebraischen Zahlkörper K definiert, sofern wir dies nicht ausdrücklich anders vermerken.

Diese Arbeit ist eine der Folgen einer sehr fruchtbaren Zusammenarbeit mit D.W. Masser, dem wir an dieser Stelle herzlichst danken möchten.

2. Additions- und Multiplikationsformeln

In diesem Abschnitt werden wir explizit einige Morphismen einer algebraischen Gruppe in eine zweite studieren. Wir werden hauptsächlich interessiert sein in dem Morphismus, der durch die Addition mehrerer Punkte der algebraischen Gruppe gegeben wird sowie in dem Morphismus, der durch die Multiplikation eines Punktes der Gruppe mit einer ganzen Zahl gegeben ist.

Es sei G eine kommutative algebraische Gruppe definiert über K und $\bar{G}$ ihre Kompaktifizierung (s. [17]). Wir können die Varietät $\bar{G}$ in einem projektiven Raum $\mathbb{P}^N$ für ein geeignetes N wie in [17] einbetten. Für eine positive ganze Zahl n sei G^n das n -fache Produkt von G mit sich selbst. Dies ist dann eingebettet in dem Produkt $\mathbb{P}^N \times \dots \times \mathbb{P}^N$ von n Exemplaren des projektiven Raums $\mathbb{P}^N$. Seien

$$\mathbf{X}_1 := (X_{0,1}, \dots, X_{N,1}), \dots, \mathbf{X}_n := (X_{0,n}, \dots, X_{N,n})$$

die homogenen Koordinaten der verschiedenen Faktoren. Wir nennen ein Polynom $P(\mathbf{X}_1, \dots, \mathbf{X}_n)$ multihomogen vom Multigrad $(D_1, \dots, D_n)$, falls es homogen vom Grade D_i in $\mathbf{X}_i$ für $1 \leq i \leq n$ ist. Weiter bezeichnen wir für $(P_1, \dots, P_n)$ in G^n mit $S(P_1, \dots, P_n)$ die Summe $P_1 + \dots + P_n$. Es seien $e_1, \dots, e_n$ fest gewählte Elemente aus dem Endomorphismenring von G . Die Summenbildung ist ein Morphismus von G^n nach G . Dann zieht die Definition eines Morphismus (s. [5]) sofort das folgende Resultat nach sich.

Lemma 1. *Es gibt eine endliche offene Überdeckung $\{U_i\}$ von G^n mit der folgenden Eigenschaft. Für jedes i existiert ein System von multihomogenen Polynomen mit Koeffizienten in K*

$$\mathcal{A}_i(\mathbf{X}_1, \dots, \mathbf{X}_n) = (A_{i,0}(\mathbf{X}_1, \dots, \mathbf{X}_n), \dots, A_{i,N}(\mathbf{X}_1, \dots, \mathbf{X}_n))$$

vom Multigrad $(d_i, \dots, d_i)$ für positives ganzes d_i , so daß für $(P_1, \dots, P_n)$ in U_i die homogenen Koordinaten von $e_1 P_1 + \dots + e_n P_n$ durch $\mathcal{A}_i(\mathbf{X}_1(P_1), \dots, \mathbf{X}_n(P_n))$ gegeben werden.

Beweis. Dies ist nichts anderes als eine lokale Beschreibung des Morphismus

$$S \circ (e_1, \dots, e_n): G^n \rightarrow G.$$

Im nächsten Lemma werden wir eine Beschreibung des Morphismus geben, der durch die Multiplikation mit einer festen ganzen Zahl gegeben wird. Dazu sei m eine solche ganze Zahl und $[m]_G: G \rightarrow G$ der Morphismus $P \mapsto mP$. Ferner definieren wir die Höhe eines Polynoms mit algebraischen Koeffizienten als das Maximum der Höhen dieser Koeffizienten (s. hierzu [18]).

Lemma 2. *Es gibt $N + 1$ homogene Polynome mit Koeffizienten in K*

$$\phi_0^{(m)}(X_0, \dots, X_N), \dots, \phi_N^{(m)}(X_0, \dots, X_N)$$

in den homogenen Koordinaten $\mathbf{X} := (X_0, \dots, X_N)$ von $\mathbb{P}^N$ mit den folgenden Eigenschaften. Der Grad dieser Polynome ist m^2 und die Höhe höchstens gleich $c_1^{m^2}$ für eine positive Konstante c_1 . Sie verschwinden nicht gleichzeitig in irgend einem Punkte von G . Ist P ein Punkt auf G , so werden die homogenen Koordinaten von mP gegeben durch

$$(\phi_0^{(m)}(\mathbf{X}), \dots, \phi_N^{(m)}(\mathbf{X})) = \phi^{(m)}(\mathbf{X}).$$

Beweis. Dies ist eine einfache Folgerung aus Corollaire 2 der Proposition 3 und Proposition 5 aus [17], sowie Lèmmes 7 aus [3].

Wir kombinieren nun diese zwei Lemmata in der folgenden Weise. Dazu setzen wir für ganze Zahlen $m_1, \dots, m_n$ $m = m_1 e_1 + \dots + m_n e_n$ und betrachten den Morphismus von G^n nach G , welcher durch

$$(P_1, \dots, P_n) \mapsto m_1 e_1 P_1 + \dots + m_n e_n P_n$$

gegeben wird. Dann haben wir die folgende algebraische Beschreibung dieses Morphismus.

Proposition 1. *Es gibt eine endliche offene Überdeckung $\{U_i\}$ von G^n mit der folgenden Eigenschaft. Für jedes i und für alle ganzen Zahlen $m_1, \dots, m_n$ gibt es $N + 1$ multihomogene Polynome*

$$\psi_0^{(i,m)}(\mathbf{X}_1, \dots, \mathbf{X}_n), \dots, \psi_N^{(i,m)}(\mathbf{X}_1, \dots, \mathbf{X}_n)$$

mit Koeffizienten in K , mit dem Multigrad $(m_1 d_i, \dots, m_n d_i)$ und mit Höhen höchstens $c_2^{m_1^2 + \dots + m_n^2}$, so daß für $(P_1, \dots, P_n)$ in U_i die homogenen Koordinaten von $m_1 e_1 P_1 + \dots + m_n e_n P_n$ durch

$$(\psi_0^{(i,m)}(\mathbf{X}_1(P_1), \dots, \mathbf{X}_n(P_n)), \dots, \psi_N^{(i,m)}(\mathbf{X}_1(P_1), \dots, \mathbf{X}_n(P_n)))$$

gegeben werden.

Beweis. Wir wählen die Überdeckung $\{U_i\}$ wie in Lemma 1 und definieren die Polynome $\psi_j^{(i,m)}$ für $0 \leq j \leq N$ durch

$$\psi_j^{(i,m)} = A_{i,j}(\phi^{(m_1)}(\mathbf{X}_1), \dots, \phi^{(m_n)}(\mathbf{X}_n)).$$

Dann prüft man die in der Proposition angegebenen Eigenschaften leicht unter Benutzung von Lemma 1 und Lemma 2 nach.

Seien $\mathbf{X} = (X_0, \dots, X_N)$ projektive Koordinaten von G . Dann können wir diese Proposition in dem Spezialfall $P_1 = \dots = P_n =: P$ anwenden. Es gilt dann $mP = m_1 e_1 P_1 + \dots + m_n e_n P_n$, und m ist ein Endomorphismus von G wie in Proposition 1 mit $\mathbf{X}_1 = \dots = \mathbf{X}_n = \mathbf{X}$.

3. Der Trick von Masser-Anderson für beliebige algebraische Gruppen

In seiner Thesis [1] arbeitete Anderson eine sehr ingenieure Idee von Masser aus, um sehr gute Schranken für den Grad und die Höhe von abgeleiteten elliptischen Polynomen zu erhalten. Dieses Hilfsmittel wurde darauf von einer großen Zahl von Autoren benutzt und wir werden es in diesem Abschnitt auf beliebige kommutative algebraische Gruppen ausdehnen. Um dies zu entwickeln, werden wir weiterhin mit der algebraischen Gruppe G wie im vorangegangenen Abschnitt arbeiten. Die Gruppe G ist in einem projektiven Raum $\mathbb{P}^N$ vermöge eines sehr amplen Divisors eingebettet. Dies ermöglicht es uns, ein System von Koordinaten $X_0, \dots, X_N$ so zu wählen, daß für eine endlich erzeugte Untergruppe Γ von G für alle γ in Γ gilt $X_0(\gamma) \neq 0$. Dann sind die projektiven Koordinaten der Elemente von Γ so gewählt, daß sie in einer endlich erzeugten Erweiterung von $\mathbb{Q}$ liegen, so gibt es eine Linearform X'_0 in $X_0, \dots, X_N$ mit algebraischen Koeffizienten, so daß $X'_0(\gamma) \neq 0$ gilt für alle γ aus Γ . Wir brauchen nun nur noch X_0 durch X'_0 zu ersetzen und erhalten die gewünschte Eigenschaft. Insbesondere gilt dann für das neutrale Element 0 der Gruppe $X_0(0) \neq 0$. Wir nehmen nun ein zweites Exemplar G' von G mit projektiven Koordinaten $X'_0, \dots, X'_N$ und betrachten das Produkt $G \times G'$ eingebettet in dem Raum $\mathbb{P}^N \times \mathbb{P}^N$. Auf der algebraischen Gruppe G der Dimension n können wir die Derivationen $\partial_1, \dots, \partial_n$ wie in [20] definieren und wir bezeichnen die zugehörigen Derivationen auf G' mit $\partial'_1, \dots, \partial'_n$. Wir wählen nun für eine fest vorgegebene positive ganze Zahl d in dem Vektorraum, der durch $\partial_1, \dots, \partial_n$ über dem Körper K erzeugt wird, d linear unabhängige Derivationen $\Delta_1, \dots, \Delta_d$ und bezeichnen die entsprechenden Derivationen auf G' mit $\Delta'_1, \dots, \Delta'_d$. Diese Wahl entspricht in eindeutiger Weise der Wahl einer analytischen Untergruppe von G (s. ebenfalls [20]).

Wir setzen nun $x_i = X_i/X_0$ für ganze Zahlen i mit $1 \leq i \leq N$ und $\mathbf{x} = (1, x_1, \dots, x_N)$. Dies sind affine Koordinaten für die affin offene Menge $X_0 \neq 0$ in $\mathbb{P}^N$. Wie üblich bezeichnen wir mit $x'_1, \dots, x'_N$ und $\mathbf{x}'$ die entsprechenden Koordinaten auf G' . Sei $\mathcal{A}$ eine Additionsformel, so daß $A_0(\mathbf{X}, \mathbf{x}'(0))$ nicht identisch verschwindet. Dann gilt auf der offenen Teilmenge $X_0 \neq 0$, $A_0(\mathbf{X}, \mathbf{x}'(0)) \neq 0$ von G

$$\Delta_1^{\tau_1} \dots \Delta_d^{\tau_d} (P(\mathbf{X})/X_0^D) = \Delta_1^{\tau_1} \dots \Delta_d^{\tau_d} (P \circ \mathcal{A}/A_0^D)(\mathbf{X}, \mathbf{x}'(0)) \quad (1)$$

für homogene Polynome $P(\mathbf{X})$ vom Grade D . Wir sollten bemerken, daß beide Seiten von (1) definiert sind, da sowohl $P(\mathbf{X})/X_0^D$ als auch $(P \circ \mathcal{A})/A_0^D$ rationale Funktionen auf G und $G \times G'_0$ sind, wenn wir mit G'_0 die offene Teilmenge von G' bezeichnen, wo $X'_0 \neq 0$ ist.

Für nichtnegative ganze Zahlen $\sigma_1, \dots, \sigma_d$, $\sigma'_1, \dots, \sigma'_d$ und $\tau_1, \dots, \tau_d$ setzen wir $\sigma = (\sigma_1, \dots, \sigma_d)$, $\sigma' = (\sigma'_1, \dots, \sigma'_d)$ und $\tau = (\tau_1, \dots, \tau_d)$. Dann definieren wir $\Delta^\sigma = \Delta_1^{\sigma_1} \dots \Delta_d^{\sigma_d}$ und entsprechend $\Delta^{\sigma'}$, sowie $\sigma! = \sigma_1! \dots \sigma_d!$. Wir schreiben $\sigma \leq \tau$ dann und nur dann, wenn $\sigma_1 \leq \tau_1, \dots, \sigma_d \leq \tau_d$ gilt. Damit können wir die rechte Seite von (1) schreiben als

$$\Delta^\tau (P \circ \mathcal{A}/A_0^D)(\mathbf{X}, \mathbf{x}'(0)) = \sum_{\sigma + \sigma' = \tau} \frac{\tau!}{\sigma! \sigma'!} \Delta^{\sigma'} (A_0^{-D}) \Delta^{\sigma} (P \circ \mathcal{A})(\mathbf{X}, \mathbf{x}'(0)), \quad (2)$$

wobei wir die Leibnitzsche Regel benützt haben. Bezeichnen wir mit M die multiplikative Menge der Potenzprodukte von X_0 und $A_0(\mathbf{X}, \mathbf{x}'(0))$ mit nicht-negativen Exponenten und mit $I(G)$ das definierende Ideal von G , welches dasselbe ist wie das von $\bar{G}$, dem Abschluß von G , so folgt aus (1) und (2)

$$\Delta^\tau(P(\mathbf{X})/X_0^D) \equiv \sum_{\sigma + \sigma' = \tau} \frac{\tau!}{\sigma! \sigma'!} \Delta'^\sigma(A_0^{-D}) \Delta'^{\sigma'}(P \circ \mathcal{A})(\mathbf{X}, \mathbf{x}'(0))$$

modulo $I(G)M^{-1}$. Deswegen können wir die Ausdrücke $\Delta^\tau(P(\mathbf{X})/X_0^D)$ modulo $I(G)M^{-1}$ ausdrücken durch die Ausdrücke $\Delta'^{\sigma'}(P \circ \mathcal{A})(\mathbf{X}, \mathbf{x}'(0))$. Es kann leicht verifiziert werden, daß das Gleichungssystem (3) sukzessive modulo $I(G)M^{-1}$ gelöst werden kann, da es Diagonalgestalt besitzt. Wir gehen etwas anders vor, um dieses Gleichungssystem zu lösen. Unser Vorgehen hat den Vorteil, daß wir einen expliziten Ausdruck erhalten. Wir schreiben

$$(P \circ \mathcal{A})(\mathbf{X}, \mathbf{x}') = A_0^D \cdot \frac{P \circ \mathcal{A}}{A_0^D}(\mathbf{X}, \mathbf{x}')$$

und wenden darauf den Differentialoperatoren Δ'^τ an. Dann erhalten wir mit Hilfe der Leibnitzschen Regel

$$\Delta^\tau(P \circ \mathcal{A})(\mathbf{X}, \mathbf{x}'(0)) = \sum_{\sigma + \sigma' = \tau} \frac{\tau!}{\sigma! \sigma'!} \Delta'^\sigma(A_0^D) \Delta'^{\sigma'}(P \circ \mathcal{A}/A_0^D)(\mathbf{X}, \mathbf{x}'(0)). \quad (4)$$

Darin ersetzen wir den Ausdruck $\Delta'^{\sigma'}(P \circ \mathcal{A}/A_0^D)(\mathbf{X}, \mathbf{x}'(0))$ durch $\Delta^{\sigma'}(P(\mathbf{X})/X_0^D)$ und erhalten dann schließlich

$$\Delta^\tau(P \circ \mathcal{A})(\mathbf{X}, \mathbf{x}'(0)) \equiv \sum_{\sigma + \sigma' = \tau} \frac{\tau!}{\sigma! \sigma'!} \Delta'^\sigma(A_0^D) \Delta^{\sigma'}(P(\mathbf{X})/X_0^D) \quad (5)$$

modulo $I(G)M^{-1}$. Dies fassen wir in der folgenden Proposition zusammen.

Proposition 2. *Es sei $P(\mathbf{X})$ ein homogenes Polynom vom Grade D und $\mathcal{A} = (A_0, \dots, A_N)$ eine Additionsformel, so daß $A_0(\mathbf{X}, \mathbf{x}'(0)) \neq 0$. Dann gilt für beliebiges $\tau \geq (0, \dots, 0)$*

$$\Delta^\tau(P(\mathbf{X})/X_0^D) \equiv \sum_{\sigma + \sigma' = \tau} \frac{\tau!}{\sigma! \sigma'!} \Delta'^\sigma(A_0^{-D}) \Delta'^{\sigma'}(P \circ \mathcal{A})(\mathbf{X}, \mathbf{x}'(0))$$

und

$$\Delta'(P \circ \mathcal{A})(\mathbf{X}, \mathbf{x}'(0)) \equiv \sum_{\sigma + \sigma' = \tau} \frac{\tau!}{\sigma! \sigma'!} \Delta'^\sigma(A_0^D)(\mathbf{X}, \mathbf{x}'(0)) \Delta^{\sigma'}(P(\mathbf{X})/X_0^D)$$

modulo dem Ideal $I(G)M^{-1}$.

4. Wurzelziehen

Ein sehr nützliches Hilfsmittel in der algebraischen Geometrie ist das Wurzelziehen. Diese Technik wurde in der Theorie der transzendenten Zahlen von D.W. Masser wiederentdeckt. In diesem Abschnitt geben wir eine Modifikation

davon in einer multiplikativen Version an. In diesem Abschnitt sei $\mathbb{C}$ der Grundkörper.

Es sei wiederum G eine kommutative algebraische Gruppe, die wie üblich projektiv eingebettet sei. Für eine positive ganze Zahl l sei $[l]_G$ der Endomorphismus $g \mapsto lg$ auf G . Da wir die Gruppe G festhalten wollen, schreiben wir dafür kurz $[l]$. Für genauere Einzelheiten verweisen wir auf [17]. Auf dem Tangentialraum $T(G)$ induziert dieser Morphismus eine lineare Abbildung, das Differential $d[l]$, und auf dem Körper der rationalen Funktionen $\mathbb{C}(G)$ einen Endomorphismus $[l]^*$. Er wird gegeben durch $F \mapsto [l]^*(F) = F \circ [l]$.

Wir können nun die Basis $\partial_1, \dots, \partial_n$ von $T(G)$ so wählen, daß

$$d[l](\partial_i) = l\partial_i \quad (1 \leq i \leq n),$$

wobei $n = \dim G$. Wir setzen $\partial'_i := d[l](\partial_i)$ für $1 \leq i \leq n$. Sei nun ∂ ein Element des Vektorraumes, der durch $\partial_1, \dots, \partial_n$ über dem Körper der komplexen Zahlen erzeugt wird. Dann gilt

$$\partial = \alpha_1 \partial_1 + \dots + \alpha_n \partial_n$$

für $\alpha_1, \dots, \alpha_n$ in $\mathbb{C}$. Wir erhalten dann

$$\partial' := d[l](\partial) = \alpha_1 d[l](\partial_1) + \dots + \alpha_n d[l](\partial_n) = l\partial.$$

Wir definieren nun die Verschwindungsordnung einer rationalen Funktion auf G und bestimmen ihr Verhalten unter dem Morphismus $[l]$.

Sei F ein Element aus dem Körper der rationalen Funktionen $\mathbb{C}(G)$ auf G . Weiter seien für eine ganze Zahl d mit $1 \leq d \leq n$ Derivationen $\Delta_1, \dots, \Delta_d$ aus dem Vektorraum fest gewählt, der von $\partial_1, \dots, \partial_n$ über dem Körper der komplexen Zahlen erzeugt wird. Wir definieren dann die Verschwindungsordnung von F im Punkte g aus G längs $\Delta_1, \dots, \Delta_d$ in der folgenden Weise. Zunächst schreiben wir $\Delta = (\Delta_1, \dots, \Delta_d)$. Dann sei ohne Beschränkung der Allgemeinheit $X_0(g) \neq 0$. Dann können wir F schreiben als

$$F(\mathbf{x}) = G(\mathbf{x})/H(\mathbf{x})$$

für Polynome G und H . Für ein Polynom $P(\mathbf{x})$ definieren wir nun die Verschwindungsordnung in g als die kleinste ganze Zahl $T \geq 0$ mit der Eigenschaft, daß es nichtnegative ganze Zahlen $t_1, \dots, t_d$ mit $t_1 + \dots + t_d = T$ gibt, so daß

$$\Delta_1^{t_1} \dots \Delta_d^{t_d}(P)(\mathbf{x}(g)) \neq 0$$

gilt. Wir schreiben dann $T = \text{ord}_{\Delta, g}(P)$ und definieren

$$\text{ord}_{\Delta, g}(F) = \text{ord}_{\Delta, g}(G) - \text{ord}_{\Delta, g}(H).$$

Es kann leicht gezeigt werden, daß diese Definition nicht von der Wahl von G und H abhängt. Sind weiter von Null verschiedene komplexe Zahlen $\alpha_1, \dots, \alpha_d$ gegeben und setzen wir $\alpha\Delta = (\alpha_1 \Delta_1, \dots, \alpha_d \Delta_d)$, so gilt

$$\text{ord}_{\alpha\Delta, g}(F) = \text{ord}_{\Delta, g}(F).$$

Sei nun g' in G so gewählt, daß $g' = lg$ gilt für ein g aus G . Dann erhalten wir für F aus $\mathbb{C}(G)$ und ganze Zahlen $0 \leq t_1, \dots, t_d$ mit $t = (t_1, \dots, t_d)$ und den Bezeichnungen aus Abschnitt 3 mit $\Delta' = l\Delta$

$$\Delta''(F)(\mathbf{x}(g')) = (l\Delta)'(F)(\mathbf{x}(lg)) = (l\Delta)'([l]^*(F))(\mathbf{x}(g)).$$

Daraus erhalten wir sofort das folgende Lemma.

Lemma 3. *Für eine positive ganze Zahl l sei $[l]$ der Endomorphismus von G , der gegeben wird durch $g \mapsto lg$. Dann gilt für alle nichttrivialen Derivationen $\Delta_1, \dots, \Delta_d$, welche in dem Punkte g aus G definiert sind,*

$$\text{ord}_{\Delta, lg}(F) = \text{ord}_{\Delta, g}([l]^*(F))$$

für alle rationalen Funktionen F auf G .

Wir werden dieses Lemma im nächsten Abschnitt benutzen, um eine Nullstellenabschätzung mit hohen Vielfachheiten zu beweisen. In [20] und [12] haben wir Einschränkungen an die Größe der Ordnung der Differentialoperatoren. Diese Restriktionen können mit Hilfe dieses Lemmas eliminiert werden. Weiter können wir mit Hilfe dieses Lemmas die Grad-Theorie für Produkte projektiver Räume in vielen Fällen vermeiden einschließlich des Falles, den wir später betrachten werden.

5. Eine neue Nullstellenabschätzung

In diesem Abschnitt werden wir die Theorie der Nullstellenabschätzungen weiter entwickeln, die von D.W. Masser und dem Autor in [9] begründet wurde und in [12] und [20] auf Multiplizitätsabschätzungen erweitert wurde. In all diesen Arbeiten hatten wir große Einschränkungen an die Größenordnung der Nullstellenordnungen zu machen, um bestmögliche Resultate zu erzielen. Dies war notwendig wegen der Nichtlinearität der Differentialgleichungen, die von den Funktionen erfüllt werden, die in der Exponentialabbildung der algebraischen Gruppe auftauchen. In vielen Problemen können diese Einschränkungen leicht in Kauf genommen werden. Ein gutes Beispiel hierfür ist Bakers Methode. Jedoch hier in dieser Arbeit haben wir ein Beispiel vorliegen, wo diese Einschränkungen ernsthafter Natur sind. Deswegen sind wir gezwungen, sie zu eliminieren. Dies kann mit Hilfe der Resultate in Abschnitt 4 zusammen mit einigen Erweiterungen der Nullstellenabschätzungen, die in [12] bewiesen wurden, sowie einigen sehr einfachen Ideen durchgeführt werden. Jedoch können diese Restriktionen wegen einiger technischer Schwierigkeiten nicht im allgemeinsten Falle eliminiert werden, sondern nur in einem Spezialfall, welcher den Fall umfaßt, an dem wir hauptsächlich interessiert sind.

Wie bereits bemerkt benutzen wir dazu ein Resultat, das in [12] bewiesen wurde. Der besseren Lesbarkeit halber wollen wir diese Resultate hier kurz referieren. Auch in diesem Abschnitt wählen wir $\mathbb{C}$ als Grundkörper.

Es seien $G_1, \dots, G_n$ kommutative algebraische Gruppen und $G = G_1 \times \dots \times G_n$ ihr Produkt. Für $1 \leq i \leq n$ bezeichnen wir mit d_i die Dimension von G_i und setzen $d = d_1 + \dots + d_n$. Wir stellen dann an die Gruppen $G_1, \dots, G_n$ die folgende Bedingung. Ist H eine zusammenhängende Untergruppe von G , dann gibt es zusammenhängende Untergruppen H_i von G_i für $1 \leq i \leq n$, so daß $H = H_1 \times \dots \times H_n$.

Sei Γ eine endliche Menge in G , die das neutrale Element 0 der Gruppe G enthalte. Dann definieren wir für positive ganze Zahlen r die Menge $r\Gamma$ als

$$r\Gamma = \Gamma + \dots + \Gamma,$$

die Menge aller Linearkombinationen von r Elementen aus Γ . Da Γ das neutrale Element der Gruppe enthält, gilt $\Gamma \subseteq r\Gamma$. Für nicht-negative ganze Zahlen $r_1, \dots, r_n$ mit $0 \leq r_i \leq d_i$ für $1 \leq i \leq n$ definieren wir die ganzen Zahlen $Q_{r_1, \dots, r_n}(\Gamma)$ in der folgenden Weise. Gibt es keine algebraische Untergruppe H von G der Form $H = H_1 \times \dots \times H_n$ mit $\text{cod } H_i = r_i$ für $1 \leq i \leq n$, so setzen wir

$$Q_{r_1, \dots, r_n}(\Gamma) = |\Gamma|.$$

Andernfalls setzen wir

$$Q_{r_1, \dots, r_n}(\Gamma) = \min(|(\Gamma + H)/H|),$$

wobei das Minimum über alle zusammenhängenden Untergruppen H von G genommen wird, für die $\text{cod } H_i = r_i$ für $1 \leq i \leq n$.

Die Gruppen G_i seien nun in einen projektiven Raum $\mathbb{P}^{N_i}$ und G deswegen im Raum $\mathbb{P}^{N_1} \times \dots \times \mathbb{P}^{N_n}$ eingebettet. Dann seien $\mathbf{X}_i = (X_{i,0}, \dots, X_{i,N_i})$ für $1 \leq i \leq n$ projektive Koordinaten von $\mathbb{P}^{N_i}$. Schließlich sei Δ eine Derivation auf G , die einer eindimensionalen Unteralgebra der Lie-Algebra von G entspreche. Sei weiter B die zugehörige eindimensionale analytische Untergruppe von G . Dann wurde in [12] das folgende Ergebnis bewiesen. Es verallgemeinert in einer Richtung das Theorem *ABC* aus [9].

Satz. Es gibt eine positive Konstante c , die nur von der Gruppe G abhängt, mit der folgenden Eigenschaft. Sei für ganze Zahlen $0 \leq D_1, \dots, D_n$ und $T > 0$ ein multihomogenes Polynom $P(\mathbf{X}_1, \dots, \mathbf{X}_n)$ vom Multigrad $(D_1, \dots, D_n)$ gegeben, welches auf $d\Gamma$ mindestens von der Ordnung T längs Δ verschwinde. Gilt dann

$$TQ_{r_1, \dots, r_n}(\Gamma) \geq (cD_1)^{r_1} \dots (cD_n)^{r_n} \quad (6)$$

für $0 \leq r_i \leq d_i$ und $1 \leq i \leq n$ mit $1 \leq r = r_1 + \dots + r_n$ und

$$Q_{r_1, \dots, r_n}(\Gamma) \geq (cD_1)^{r_1} \dots (cD_n)^{r_n} \delta^{-1} \quad (7)$$

für $1 \leq r < d$ mit $\delta = \max(1, \min(cD_i))$, wobei das innere Minimum über alle i genommen wird, für die die Gruppe G_i nichtlinear ist und das Minimum über einer leeren Menge als Null gesetzt wird, so verschwindet das Polynom P auf ganz $B + \gamma$ für ein γ in Γ .

Wir werden nun den Spezialfall betrachten, wo $n=2$ und $G_1 = A$ ist für eine abelsche Varietät A und G_2 das d_2 -fache Produkt der additiven Gruppe $\mathbb{G}_a$.

Wir werden dann zeigen, daß der Satz auch ohne die Bedingung (7) richtig ist. Um genau zu sein, seien $\mathbf{Z}$ die homogenen Koordinaten, welche der Gruppe G_2 entsprechen mögen und $\mathbf{X}$ die zur Gruppe A gehörigen homogenen Koordinaten.

Satz 2. Sei in dem Satz $G_1 = A$ für eine abelsche Varietät A , $G_2 = \mathbb{G}_a^{d_2}$ und P ein bihomogenes Polynom wie im Satz. Ist dann B dicht in G und gilt

$$TQ_{r_1, r_2}(\Gamma) \geq (cD_1)^{r_1} (cD_2)^{r_2} \quad (8)$$

für $0 \leq r_i \leq d_i$ und $i = 1, 2$ mit $r = r_1 + r_2 \geq 1$. Dann verschwindet P auf ganz G .

Bevor wir den Satz 2 beweisen, machen wir noch eine Bemerkung. Erstens ist es kein Problem, den Satz 2 auf den Fall auszudehnen, wo $G_1 = A_1, \dots, G_{n-1} = A_{n-1}$ und $G_n = \mathbb{G}_a^{d_n}$ ist, wobei $A_1, \dots, A_{n-1}$ abelsche Varietäten sind, sofern nur die Voraussetzungen vom Satz erfüllt sind. Dies erreicht man dadurch, daß man die Ergebnisse aus Abschnitt 4 auf diese etwas allgemeinere Situation ausdehnt. Zweitens ist es möglich, ohne größere Anstrengung ein Produkt von multiplikativen Gruppen mit einzubeziehen. Dafür sind keine neuen Ideen notwendig.

Beweis von Satz 2. Wir werden den Satz 2 aus dem Satz herleiten. Dazu wählen wir eine positive ganze Zahl l mit $cl^2D_1 \geq T$ und bezeichnen wie in Abschnitt 2 und Abschnitt 4 mit $[l]$ den Morphismus, der durch die Multiplikation $g \mapsto lg$ auf der Gruppe $G = A \times \mathbb{G}_a^{d_2}$ gegeben wird. Wir können dann den Satz auf das bihomogene Polynom $[l]^*(P)$ anwenden. Dieses hat den Bigrad (l^2D_1, D_2) . Dies folgt aus Lemma 2 aus Abschnitt 2 und der Tatsache, daß auf der Gruppe $\mathbb{G}_a^d$ die Multiplikation mit l durch Multiplikation der Koordinaten mit l gegeben ist. Für Γ nehmen wir die Menge $[l]^{-1}(\Gamma)$ und müssen nur die Zahlen $Q_{r_1, r_2}([l]^{-1}(\Gamma))$ berechnen. Um dies zu tun, sei H eine zusammenhängende algebraische Untergruppe der Form $H = H_1 \times H_2$ mit $\text{cod } H_1 = r_1$ und $\text{cod } H_2 = r_2$. Dann erhalten wir

$$([l]^{-1}(\Gamma) + H)/H = [\bar{l}]^{-1}((\Gamma + H)/H),$$

wobei $[\bar{l}]$ der Morphismus ist, der durch $[l]$ auf G/H induziert wird. Dessen Kern ist eine Untergruppe von G/H der Ordnung l^{2r_1} , so daß wir

$$|([l]^{-1}(\Gamma) + H)/H| = l^{2r_1} |(\Gamma + H)/H|$$

erhalten. Dies zieht

$$Q_{r_1, r_2}([l]^{-1}(\Gamma)) = l^{2r_1} Q_{r_1, r_2}(\Gamma)$$

nach sich. Weiter folgt aus Lemma 3, daß das Polynom $[l]^*(P)$ in $[l]^{-1}(\Gamma)$ wenigstens mit der Ordnung T längs A verschwindet. Daher gilt

$$TQ_{r_1, r_2}([l]^{-1}(\Gamma)) = Tl^{2r_1} Q_{r_1, r_2}(\Gamma).$$

Die rechte Seite ist wenigstens gleich $l^{2r_1} (cD_1)^{r_1} (cD_2)^{r_2}$ wegen (8). Deswegen erhalten wir

$$TQ_{r_1, r_2}([l]^{-1}(\Gamma)) \geq (cl^2D_1)^{r_1} (cD_2)^{r_2}, \quad (9)$$

und deswegen ist (6) für $[l]^*(P)$ erfüllt. Aufgrund der Wahl von l erhalten wir aus (9)

$$cl^2 D_1 Q_{r_1, r_2}([l]^{-1}(\Gamma)) \geq (cl^2 D_1)^{r_1} (cD_2)^{r_2},$$

und dies zieht (7) nach sich, da $G_2 = \mathbb{G}_a^{d_2}$ linear ist und somit $\delta = \max(1, cl^2 D_1)$ ist. Der Satz impliziert deshalb, daß $[l]^*(P)$ auf ganz G verschwindet und somit auch P , wie dies behauptet war. Damit ist der Satz 2 bewiesen.

Wir können nun Satz 2 auf die folgende Situation anwenden, wie sie später im Beweis von Satz 1 auftritt. Sei G die Gruppe $(\mathbb{G}_a \times A^n)^\kappa$ für ein $\kappa \geq 1$ und Δ eine Derivation auf $\mathbb{G}_a \times A^n$, welche einer dichten analytischen Untergruppe B von $\mathbb{G}_a \times A^n$ der Dimension 1 entspricht. Seien $\Delta_1, \dots, \Delta_\kappa$ κ Exemplare von Δ , die den verschiedenen Faktoren vom Typ $\mathbb{G}_a \times A^n$ von G entsprechen. Sei $g = (g', g'')$ ein Element von $\mathbb{G}_a \times A^n$. Dann definieren wir mit der Bezeichnung von Abschnitt 1 für γ in $\mathcal{O}$ das Element $\gamma g = (\gamma g', \gamma g'')$ und für Elemente $g_1, \dots, g_\kappa$ in $\mathbb{G}_a \times A^n$ die Mengen $\Gamma_i = \mathcal{O} g_i$ für $1 \leq i \leq \kappa$. Wie üblich definieren wir weiter $\Gamma_i(S)$ für reelle Zahlen $S \geq 0$ (s. [9]) und $\Gamma(S) = \Gamma_1(S) \times \dots \times \Gamma_\kappa(S)$ in $G = (\mathbb{G}_a \times A^n)^\kappa = \mathbb{G}_a^\kappa \times A^{n\kappa}$. Da die Operation von Γ auf $\mathbb{G}_a \times A^n$ auf dem ersten Faktor komplexe Multiplikation ist, erhalten wir

$$|\Gamma_i(S)| \geq S^{nm} \quad (1 \leq i \leq \kappa),$$

falls $g'_1 \neq 0, \dots, g'_\kappa \neq 0$ ist.

Korollar. Es gibt eine positive Konstante c mit der folgenden Eigenschaft. Für ganze Zahlen $S \geq 0$, $D \geq 0$, $L \geq 0$ und $T \geq 1$ sei $P(\mathbf{Z}_1, \mathbf{X}_1, \dots, \mathbf{Z}_\kappa, \mathbf{X}_\kappa)$ ein multihomogenes Polynom vom Multi-Bigrad (L, D) , welches auf $(nd+1)\Gamma(S)$ mindestens von der Ordnung T längs B^κ verschwindet, aber nicht identisch auf G . Gilt dann

$$T \geq (cL)^{nd} \quad (10)$$

und

$$TS^{mn} \geq cD(cL)^{nd}, \quad (11)$$

so ist wenigstens eines der Elemente $g'_1, \dots, g'_\kappa$ das neutrale Element der Gruppe $\mathbb{G}_a$.

Beweis. Wir sind in der Produkt-Situation von Satz 2. Ein einfaches Argument, das wir dem Leser überlassen können, zeigt, daß es genügt, das Korollar für den Fall $\kappa=1$ zu beweisen. Dazu müssen wir nur noch die Zahlen $Q_{r_1, r_2}(\Gamma(S))$ berechnen. Sei dazu $H = H_1 \times H_2$ eine algebraische Untergruppe von G , wobei H_1 in $\mathbb{G}_a$ und H_2 in A^n liegt und $\text{cod } H_i = r_i$ für $i=1, 2$ sei. Bezeichnen wir mit Γ' die Projektion von $\Gamma \cap H$ auf H_1 , so erzeugt Γ' einen Untervektorraum des komplexen Vektorraums H_1 dessen Kodimension wenigstens gleich r_1 ist. Deswegen ist der Korang von Γ' wenigstens gleich $r_1 mn$ und dies zieht

$$Q_{r_1, r_2}(\Gamma(S)) \geq S^{r_1 mn}$$

für alle r_1, r_2 mit $0 \leq r_1 \leq 1$, $0 \leq r_2 \leq dn$ und $r = r_1 + r_2 \geq 1$ nach sich. Gilt $r_1 = 0$, so folgt in Verbindung mit (10) die Ungleichung

$$TQ_{0, r_2}(\Gamma(S)) \geq (cL)^{nd} \geq (cL)^{r_2}.$$

Gilt $r_1 = 1$, so erhalten wir wegen (11) die Ungleichung

$$TQ_{1,r_2}(\Gamma(S)) \geq TS^{mn} \geq cD(cL)^{nd}.$$

In beiden Fällen erhalten wir schließlich

$$TQ_{r_1,r_2}(\Gamma(S)) \geq (cL)^{r_2}(cD)^{r_1}.$$

Wegen der Ungleichung (12) sind alle Voraussetzungen von Satz 2 erfüllt, und wir erhalten, daß das Polynom P auf ganz G verschwindet oder aber das Element g'_1 das neutrale Element der additiven Gruppe ist. Da das Polynom P nicht identisch auf G verschwindet, muß das letztere eintreten. Damit ist aber das Korollar bewiesen.

Wir beenden diesen Abschnitt mit einer zusätzlicher Bemerkung zum Beweis des Korollars von Satz 2. In unserer Anwendung dieses Korollars im Beweis von Satz 1 werden wir die Zahlen S , T , D und L so wählen, daß $D \geq cL$ gilt. Dann können wir das Wurzelziehen mit einer Zahl l so vornehmen, daß $c^{l^2}L = D$ gilt. Dann wird das Polynom $[l]^*(P)$ multihomogen vom Multigrad $(D, \dots, D)$. Wir erhalten dadurch ein homogenes Polynom vom Grade $2\kappa D$. In diesem Falle benötigen wir nicht den Satz für verschiedene Grade, sondern es genügt ein Resultat im Stile von Theorem A in [9].

6. Das Hilfsideal

In diesem Abschnitt werden wir in allgemeiner Form die Konstruktion des Hilfsideals durchführen. Dies werden wir später im Transzendenzbeweis benötigen. Von nun an sei der Grundkörper wieder der in Abschnitt 1 eingeführte algebraische Zahlkörper K .

Um dies durchzuführen sei $\mathcal{O}$ die Ordnung, die wir in Abschnitt 1 eingeführt haben. Wir halten dann ein für alle Mal eine Menge von freien Erzeugenden $e_1, \dots, e_{nm}$ von $\mathcal{O}$ über $\mathbb{Z}$ fest, die wir auch zur Definition von $\mathcal{O}^\kappa(S)$ benutzen. Diese bilden dann eine Basis von $\mathcal{O} \otimes \mathbb{Q}$ über $\mathbb{Q}$. In Abschnitt 1 haben wir weiter eine Operation von $\mathcal{O}$ als Endomorphismen von $\mathbb{G}_a$ und A^n definiert. Auf $\mathbb{G}_a$, wir erinnern nochmals daran, ist dies einfach die Multiplikation mit einer komplexen Zahl. Ihr algebraischer Grad ist daher gleich 1. Wir betrachten nun die Gruppe $G = \mathbb{G}_a \times A^n$ und für eine positive ganze Zahl κ die Gruppe G^κ . Wir betten G in das Produkt von projektiven Räumen $\mathbb{P} \times \mathbb{P}^N$ wie üblich ein. Dadurch wird die Gruppe G^κ in den Raum $(\mathbb{P} \times \mathbb{P}^N)^\kappa$ eingebettet. Seien $\mathbf{Z}_j = (Z_{j,0}, Z_{j,1})$ für $1 \leq j \leq \kappa$ projektive Koordinaten von $\mathbb{P}$ und $\mathbf{X}_j = (X_{j,0}, \dots, X_{j,N})$ projektive Koordinaten von $\mathbb{P}^N$. Weiter seien $\mathcal{A}_1, \dots, \mathcal{A}_u$ für eine positive ganze Zahl u ein vollständiges System von Additionsformeln, die den Morphismus der Addition vollständig beschreiben. Sei $P(\mathbf{Z}_1, \mathbf{X}_1, \dots, \mathbf{Z}_\kappa, \mathbf{X}_\kappa)$ ein multihomogenes Polynom und für ein weiteres System von affinen Variablen $\mathbf{z}'_j$ und $\mathbf{x}'_j$ wie in Abschnitt 2 $P \circ \mathcal{A}_i$ das Polynom

$$(P \circ \mathcal{A}_i)(\mathbf{Z}_1, \mathbf{X}_1, \dots, \mathbf{Z}_\kappa, \mathbf{X}_\kappa, \mathbf{z}'_1, \mathbf{x}'_1, \dots, \mathbf{z}'_\kappa, \mathbf{x}'_\kappa).$$

Dies ist wieder ein multihomogenes Polynom in denselben Variablen. Die Differentialoperatoren $\Delta'_1, \dots, \Delta'_\kappa$ aus Abschnitt 5 mit den Bezeichnungen aus Abschnitt 3 operieren auf den inhomogenen Variablen $\mathbf{z}'_1, \dots, \mathbf{x}'_\kappa$. Wie üblich setzen wir für nichtnegative ganze Zahlen $t_1, \dots, t_\kappa$

$$\Delta'^t = \Delta_1'^{t_1} \dots \Delta_\kappa'^{t_\kappa}$$

mit $t = (t_1, \dots, t_\kappa)$. Schließlich definieren wir für $\gamma_1, \dots, \gamma_\kappa$ in $\mathcal{O}$ den Endomorphismus $\gamma = (\gamma_1, \dots, \gamma_\kappa)$ von G^κ durch $g = (g_1, \dots, g_\kappa) \mapsto \gamma g = (\gamma_1 g_1, \dots, \gamma_\kappa g_\kappa)$. Dann folgt aus der Proposition 1 zusammen mit der Bemerkung nach ihrem Beweis und der Tatsache, daß auf dem linearen Faktor von G^κ diese Operation Multiplikation mit einer komplexen Zahl ist, daß es eine endliche offene Überdeckung $\{U_i\}$ von G gibt, so daß der Morphismus $[\gamma]$, der durch γ auf G^κ induziert wird, auf U_i eine überall definierte rationale Abbildung $[\gamma]_i$ ist. Diese wird gegeben durch homogene Polynome wie in der Proposition 1 in den Variablen $\mathbf{X}_j$ und durch lineare Polynome in den Variablen $\mathbf{Z}_j$. Ist $\gamma_j = s_{j,1} e_1 + \dots + s_{j,nm} e_{nm}$ für $1 \leq j \leq \kappa$ und P ein multihomogenes Polynom vom Multigrad $(D_1, L_1, \dots, D_\kappa, L_\kappa)$, so ist das Polynom $[\gamma]_i^*(P)$ multihomogen vom Multigrad

$$(D_1, (s_{1,1}^2 + \dots + s_{1,nm}^2) d_i L_1, \dots, D_\kappa, (s_{\kappa,1}^2 + \dots + s_{\kappa,nm}^2) d_i L_\kappa).$$

Nun definieren wir für ganze Zahlen $S \geq 0$ und $T \geq 1$ das Ideal $I(S, T)$ durch

$$I(S, T) = (\Delta'^t [\gamma]_i^* P \circ \mathcal{A}_j(\mathbf{Z}_1, \mathbf{X}_1, \dots, \mathbf{Z}_\kappa, \mathbf{X}_\kappa; \mathbf{z}'_1(0), \dots, \mathbf{x}'_\kappa(0)))$$

für $t = (t_1, \dots, t_\kappa)$ mit $t_1 + \dots + t_\kappa = |t| \leq T$, γ in $\mathcal{O}^\kappa(S)$, $1 \leq j \leq u$. Dabei durchläuft die Zahl i die endliche Indexmenge der offenen Überdeckung $\{U_i\}$.

Dies ist ein multihomogenes Ideal und wir bezeichnen mit $I(S, T)(1)$ das Ideal, das in $\mathbb{C}[\mathbf{X}_1, \dots, \mathbf{X}_\kappa]$ von denselben Polynomen wie $I(S, T)$ erzeugt wird, wobei nur die Variablen $\mathbf{Z}_1, \dots, \mathbf{Z}_\kappa$ durch $(1, 1), \dots, (1, 1)$ ersetzt werden.

Proposition 3. *Es sei h die Höhe des multihomogenen Polynoms $P(\mathbf{Z}_1, \mathbf{X}_1, \dots, \mathbf{Z}_\kappa, \mathbf{X}_\kappa)$, dessen Multigrad in den $\mathbf{Z}_i$ höchstens D und in den $\mathbf{X}_i$ höchstens L für $1 \leq i \leq \kappa$ sei. Dann wird das Ideal $I(S, T)$ erzeugt von multihomogenen Polynomen mit Höhen höchstens gleich*

$$T! c_1^{S^2 L + T + D \log S} h$$

für eine Konstante c_1 , die nur von der Gruppe G^κ abhängt, deren Multigrad höchstens D in den Variablen $\mathbf{Z}_i$ und $c_2 L S^2$ in den Variablen $\mathbf{X}_i$ ist für $1 \leq i \leq \kappa$. Dies gilt insbesondere für das Ideal $I(S, T)(1)$, das multihomogen in den Variablen $\mathbf{X}_i$ vom Multigrad höchstens $(c_2 L S^2, \dots, c_2 L S^2)$ ist, wo c_2 wiederum nur von der Gruppe G^κ abhängt.

Beweis. Die Abschätzungen für den Grad der Erzeugenden des Ideals $I(S, T)$ und a fortiori des Ideals $I(S, T)(1)$ folgen unmittelbar aus der Proposition 1. Die Abschätzungen für die Höhen dieser Erzeugenden folgen ebenfalls aus dieser Proposition zusammen mit der wohlbekannten Tatsache, daß der zusätzliche Beitrag, welcher von den Differentialoperatoren kommt, höchstens gleich $T! c_3^{T + L + D \log S}$ ist, wo c_3 ebenfalls nur von der Gruppe abhängt.

Bis jetzt hängen die Ideale $I(S, T)$ und $I(S, T)(1)$ noch von dem Polynom P ab. Wir werden es nun festlegen. Um dies zu tun, müssen wir die Parameter κ, S, T, D und L , die in dem Ideal $I(S, T)$ auftauchen, einschränken. Wir wählen eine positive Zahl $1/4 > \varepsilon > 0$ und definieren die positive ganze Zahl κ durch

$$\kappa = [N/\varepsilon] + 1. \quad (13)$$

Weiter wählen wir hinreichend große ganze Zahlen L und S mit $L^{nd/4\varepsilon} \geq S \geq L^{d/m}$. Es sei D ein Parameter, welcher nach unendlich geht. Dann setzen wir

$$T = [DL^{nd-\varepsilon}/S^{mn+2\varepsilon}]. \quad (14)$$

Wir bemerken hier, daß die Wahl von κ und T nach sich zieht, daß für eine beliebige Konstante $c_4 > 0$ gilt

$$T^\kappa S^{mn\kappa} (LS^2)^N \leq c_4 (DL^{nd})^\kappa \quad (15)$$

sobald nur L oder S hinreichend groß bezüglich dieser Konstanten sind.

Es sei $y = (y_0, \dots, y_N)$ ein weiteres System von unabhängigen Variablen. Damit definieren wir das multihomogene Ideal $m(y)$ durch

$$m(y) = (I(G^\kappa), Z_{i,0} - Z_{i,1}, X_{i,j}y_k - X_{i,k}y_j; 1 \leq i \leq \kappa, 0 \leq k, j \leq N).$$

Dies ist ein Ideal der Dimension Null in dem Polynomring $K[y][Z_1, \dots, X_\kappa]$ über $K[y]$. Das folgende Lemma beendet die Konstruktion des Hilfsideals.

Lemma 4. *Es gibt ein multihomogenes Polynom mit ganzzahligen Koeffizienten vom Multigrad höchstens D in den Z_i und L in den X_i für $1 \leq i \leq \kappa$, das nicht in $I(G^\kappa)$ liegt und dessen Höhe höchstens gleich*

$$T! c_5^{S^2 L + D \log S}$$

ist, so daß

$$(I(G^\kappa), I(S, T)) \subset m(y). \quad (16)$$

Bemerkung. Ist h ein Punkt aus A^n und spezialisieren wir y zu $(X_0(h), \dots, X_N(h))$, so bedeutet (16) nichts anderes, als daß das fragliche Polynom in $(\mathcal{O}(S)(1, 1, h))^\kappa$ mindestens mit der Ordnung T verschwindet.

Beweis. Da die Dimension von A^n gleich nd ist, gibt es $nd+1$ unter den Variablen X_i für jedes i mit $1 \leq i \leq \kappa$, die algebraisch unabhängig modulo dem Ideal von G sind. Ohne Beschränkung der Allgemeinheit seien dies die ersten $nd+1$ Variablen, d.h.

$$X'_i := (X_{i,0}, \dots, X_{i,nd+1}) \quad (1 \leq i \leq \kappa).$$

Dann gilt für jedes von Null verschiedene multihomogene Polynom $P(Z_1, X'_1, \dots, Z_\kappa, X'_\kappa)$

$$P \not\equiv 0 \pmod{I(G^\kappa)}.$$

Wir nehmen nun ein multihomogenes Polynom solch einer Gestalt mit Multigrad D in den Variablen Z_i und L in den Variablen X'_i für $1 \leq i \leq \kappa$ mit

unbestimmten Koeffizienten. Die Bedingung (16) ist äquivalent zu einem System von homogenen Gleichungen für diese Koeffizienten. Die Zahl dieser Gleichungen ist höchstens gleich $c_6 T^\kappa S^{nm\kappa} (LS^2)^N$. Die Koeffizienten dieses Systems liegen in einem algebraischen Zahlkörper und werden in der Proposition 1 abgeschätzt. Wegen (15) können wir das Siegelsche Lemma anwenden und erhalten ein von Null verschiedenes Polynom $P(\mathbf{Z}_1, \dots, \mathbf{X}'_\kappa)$, dessen zugehöriges Ideal die Bedingung (16) erfüllt. Dies beweist das Lemma.

7. Die Nullstellenabschätzung

In diesem Abschnitt werden wir den Hauptschritt im Beweis von Satz 1 tun. Wir werden zeigen, daß für geeignetes $S' \geq S$ das Ideal $I(S', T)(1)$ keine Nullstelle auf $A^{n\kappa}$ besitzt. Wir werden dies mit Hilfe des Korollars von Satz 2 beweisen. Um dieses Ergebnis anzuwenden, müssen wir eine weitere Bedingung an die Wahl unserer Parameter stellen. Wir wählen die Parameter, so daß

$$T \geq L^{nd+\varepsilon} \quad (17)$$

gilt. Da L groß genug gewählt war, impliziert diese Bedingung die Bedingung (10). Wir können nun die Nullstellenabschätzung angeben.

Proposition 4. *Es sei $S' = S(LS^2)^{2\varepsilon/mn}$. Dann hat unter der Voraussetzung (17) das Ideal $I(S', T)(1)$ keine Nullstelle auf $A^{n\kappa}$.*

Beweis. Wir nehmen an, daß das Ideal $I(S', T)(1)$ eine Nullstelle g'' besitzt. Dann können wir g'' schreiben in der Form $(g'_1, \dots, g'_\kappa)$ für $g'_1, \dots, g'_\kappa$ in A^n . Nun setzen wir $g'_i = (1, 1)$ für $1 \leq i \leq \kappa$ und $g_i = (g'_i, g'_i)$. Dann liegt g_i in G für $1 \leq i \leq \kappa$. Da $I(S', T)(1)$ in g'' verschwindet, verschwindet das Ideal $I(S', T)$ in $g = (g_1, \dots, g_\kappa)$. Wir können nun erreichen, daß der Orbit $\mathcal{O}g$ von g ganz in der offenen Menge $X_{0,1} \dots X_{0,\kappa} \neq 0$ liegt. Dies erreichen wir mit einer Änderung der Einbettung von A^n in $\mathbb{P}^N$ in der folgenden Weise. Sind $X_0, \dots, X_N$ die projektiven Koordinaten in $\mathbb{P}^N$, so wählen wir eine Linearform $L_0(X_0, \dots, X_N)$

mit algebraischen Koeffizienten mit $\frac{\partial}{\partial X_0} L_0 \neq 0$ und $L_0(X_0, \dots, X_N) (\gamma g) \neq 0$ für alle γ aus $\mathcal{O}$. Dies ist möglich, da wir die projektiven Koordinaten der Elemente aus $\mathcal{O}g$ so wählen können, daß sie in einem über $\mathbb{Q}$ endlich erzeugten Körper liegen. Wir definieren nun die lineare Abbildung L als $(Y_0, \dots, Y_N) = (L_0, X_1, \dots, X_N)$ und dies sind die neuen Koordinaten. Dieser Koordinatenwechsel induziert einen Wechsel der homogenen Koordinaten auf jedem Faktor der Gestalt $\mathbb{P} \times \mathbb{P}^N$. Wir bezeichnen diese Koordinatentransformation von $(\mathbb{P} \times \mathbb{P}^N)^\kappa$ mit $\mathcal{L}$ und mit $\mathcal{L}^{-1}$ die inverse. Dann definieren wir für multihomogene Polynome F das Polynom F_L durch $F \circ \mathcal{L}^{-1}$. Die neuen Additionsformeln $\mathcal{A}_{i,L}$ sind dann definiert durch

$$\mathcal{A}_{i,L} = (\mathcal{L} \times \mathcal{L}) \circ \mathcal{A} \circ (\mathcal{L}^{-1} \times \mathcal{L}^{-1}).$$

Da das Ideal $I(S', T)$ in g verschwindet, verschwinden die Polynome

$$(P \circ \mathcal{A}_j)_\gamma = P \circ \mathcal{A}_j(\mathbf{Z}_1(\gamma g), \dots, \mathbf{X}_\kappa(\gamma g); \mathbf{Z}'_1, \dots, \mathbf{X}'_\kappa)$$

mindestens mit der Ordnung $T+1$ in 0 für alle γ aus $\mathcal{O}^\kappa(S')$. Es folgt, daß das Polynom

$$(P_L \circ \mathcal{A}_{j,L})_\gamma = ((P \circ \mathcal{A}_j)_L)_\gamma$$

mindestens mit der Ordnung $T+1$ in 0 verschwindet. Nun können wir die Proposition 2 benützen, um die Derivationen $\Delta_1, \dots, \Delta_\kappa$ und $\Delta'_1, \dots, \Delta'_\kappa$ bezüglich der neuen Variablen in Verbindung zu bringen. Zunächst ergibt sich

$$\Delta''(P \circ \mathcal{A}_j)_L(\gamma g, 0) = 0$$

für alle $t = (t_1, \dots, t_\kappa)$ mit $t_1 + \dots + t_\kappa \leq T$ und alle γ aus $\mathcal{O}^\kappa(S')$. Wegen der Proposition 2 und wegen $Y_{0,i}(\gamma g) \neq 0$ für alle i und alle γ folgt, daß das Polynom

$$P_L / Z_{0,1}^{D_1} \dots Z_{0,\kappa}^{D_\kappa} Y_{0,1}^{L_1} \dots Y_{0,\kappa}^{L_\kappa}$$

mindestens mit der Ordnung $T+1$ in $\mathcal{O}^\kappa(S')$ g verschwindet, wobei D_i der Grad von P in den Variablen Z_i für $1 \leq i \leq \kappa$ ist und L_i der Grad von P in den Variablen X_i ebenfalls für $1 \leq i \leq \kappa$.

Mit anderen Worten haben wir hergeleitet, daß das Polynom P_L auf der Menge $\mathcal{O}^\kappa(S')$ mindestens mit der Ordnung T verschwindet. Dies ist genau die Situation in dem Korollar von Satz 2. Die Wahl der Parameter S', T, D und L implizieren unmittelbar die Bedingungen (10) und (11) und deswegen hat mindestens eines der Elemente g'_i für $1 \leq i \leq \kappa$ das neutrale Element der Gruppe $\mathbb{G}_a$ zu sein. Aber dies heißt nichts anderes als $g'_i = (1, 0)$ und dies ist ein Widerspruch zur Wahl von g'_i . Deswegen hat das multihomogene Ideal $I(S', T)$ keine Nullstelle auf der Gruppe $A^{n\kappa}$. Damit ist die Proposition bewiesen.

8. Das Approximationsideal

In Abschnitt 6 haben wir das Hilfsideal $I(S, T)$ und in Abschnitt 7 das Ideal $I(S', T)(1)$ eingeführt, von dem wir gezeigt haben, daß es auf $A^{n\kappa}$ keine Nullstelle besitzt. Wir nennen es das Approximationsideal und werden diese Bezeichnung später rechtfertigen. Wir beginnen nun damit, den Punkt α in $T(A^n)$ in Erinnerung zu rufen und setzen

$$g_i = (1, 1, \exp_{A^n}(\alpha))$$

für $1 \leq i \leq \kappa$ und weiter $g = (g_1, \dots, g_\kappa)$. Dann definieren wir wie gewöhnlich $\gamma \cdot g$ für γ in $\mathcal{O}^\kappa$. Das Ideal $I(S, T)$ war so konstruiert, daß es auf $\mathcal{O}^\kappa(S) \cdot g$ verschwindet.

Proposition 5. *Es gibt eine positive Konstante c_6 , die nur von G und α abhängt, so daß für die ausgezeichneten Erzeugenden $\Delta''[\gamma]_i^* P \circ \mathcal{A}_j$ von $I(S', T)$ gilt*

$$\log |\Delta''[\gamma]_i^* \mathcal{P} \circ \mathcal{A}_j(g, 0)| \leq -c_7 T S^{m^n} \log T \quad (18)$$

für alle i, j , für alle nichtnegativen ganzen Zahlen $t_1, \dots, t_\kappa$ mit $t_1 + \dots + t_\kappa \leq T$ und für alle γ in $\mathcal{O}^\kappa(S')$. Insbesondere genügen die ausgezeichneten Erzeugenden von $I(S', T)(1)$ dieser Abschätzung.

Beweis. Da nach Konstruktion das Ideal $I(S, T)$ auf $\mathcal{O}^\kappa(S) \cdot g$ verschwindet, erhalten wir für alle nichtnegativen ganzen Zahlen $t_1, \dots, t_\kappa$ mit $t_1 + \dots + t_\kappa \leq T$ und für γ in $\mathcal{O}^\kappa(S)$

$$\Delta'^t[\gamma]_i^* P \circ \mathcal{A}_j(g, 0) = 0.$$

Da wir annehmen können, daß für jedes γ in $\mathcal{O}^\kappa$ gilt $Z_{0,1} \dots Z_{0,\kappa} X_{0,1} \dots X_{0,\kappa}(\gamma g) \neq 0$, so können wir mit Hilfe von Proposition 2 dies auf die Derivationen $\Delta_1, \dots, \Delta_\kappa$ übertragen und erhalten

$$\Delta^t(P/Z_{0,1}^{D_1} X_{0,1}^{L_1} \dots Z_{0,\kappa}^{D_\kappa} X_{0,\kappa}^{L_\kappa})(\gamma g) = 0 \quad (19)$$

für γ in $\mathcal{O}^\kappa(S)$ und alle nichtnegativen ganzen Zahlen $t_1, \dots, t_\kappa$ mit $t_1 + \dots + t_\kappa \leq T$. Daraus folgt, daß das Polynom P auf $\mathcal{O}^\kappa(S)$ mindestens mit der Ordnung T verschwindet. Nun können wir das Schwarzsche Lemma für Produkte anwenden (s. [18], Proposition 7.2.1).

Es sei $\phi: \mathbb{C} \rightarrow A^n$ die analytische Darstellung der analytischen Untergruppe B , die zu Beginn eingeführt wurde. Wir können ohne Beschränkung der Allgemeinheit annehmen, daß B bereits $\mathcal{O}g$ enthält. Dann ist $\phi = (\phi_0, \dots, \phi_N)$, und wir können die Darstellung des Produktes B^κ schreiben als

$$\Phi = (\phi^1, \dots, \phi^\kappa): \mathbb{C}^\kappa \rightarrow A^{n\kappa},$$

wobei $\phi^i = \phi$ ist für $1 \leq i \leq \kappa$. Seien $z_1, \dots, z_\kappa$ die Koordinaten von B^κ . Dies ist nach Voraussetzung eine κ -dimensionale Untergruppe von $A^{n\kappa}$. Nun ersetzen wir in dem Polynom P die Variablen $\mathbf{Z}_i$ durch $(1, z_i)$ und $\mathbf{X}_i$ durch $\phi^i(z_i)$. Dadurch erhalten wir eine analytische Funktion in den Variablen $z_1, \dots, z_\kappa$. Die algebraischen Differentialoperatoren $\Delta_1, \dots, \Delta_\kappa$ entsprechen den analytischen Differentialoperatoren $\partial/\partial z_1, \dots, \partial/\partial z_\kappa$. Dann folgt aus (19), daß die daraus resultierende Funktion $\Psi(z_1, \dots, z_\kappa)$ eine Nullstelle mindestens der Ordnung T in den Punkten $\gamma(1, \dots, 1) = (\gamma_1, \dots, \gamma_\kappa)$ für Elemente $\gamma = (\gamma_1, \dots, \gamma_\kappa)$ in $\mathcal{O}^\kappa(S)$ hat. Die Funktionen, die in Φ auftauchen, haben alle die Wachstumsordnung zwei. Setzen wir $R = T^{1/4}$, so finden wir mit Hilfe des Schwarzschen Lemmas für Produkte und der Cauchyschen Ungleichung, daß für alle nichtnegativen ganzen Zahlen $t_1, \dots, t_\kappa$ mit $t_1 + \dots + t_\kappa \leq T$

$$\log \left| \left(\frac{\partial}{\partial z_1} \right)^{t_1} \dots \left(\frac{\partial}{\partial z_\kappa} \right)^{t_\kappa} (\Psi / (\phi_0^1)^{L_1} \dots (\phi_0^\kappa)^{L_\kappa}) \gamma(1, \dots, 1) \right| \leq -c_8 T S^{mn} \log T.$$

gilt für γ in $\mathcal{O}^\kappa(S')$. Dies können wir auch in der Form

$$\log |\Delta_1^{t_1} \dots \Delta_\kappa^{t_\kappa} (P/Z_{0,1}^{D_1} \dots X_{0,\kappa}^{L_\kappa})(\gamma g)| \leq -c_8 T S^{mn} \log T \quad (20)$$

schreiben. Um (18) zu erhalten, müssen wir nochmals die Proposition 2 anwenden. Eine einfache Rechnung zeigt dann, daß

$$\log |\Delta_1^{t_1} \dots \Delta_\kappa^{t_\kappa} [\gamma]_i^* P \circ \mathcal{A}_j(g, 0)| \leq -c_9 T S^{mn} \log T$$

gilt. Daraus folgt die behauptete Ungleichung in Proposition 5. Die zweite Behauptung ergibt sich unmittelbar hieraus und der Definition von $I(S', T)(1, 1)$.

9. Vollständige Durchschnitte

Ein wichtiges Hilfsmittel, um am Ende den gewünschten Widerspruch zu erhalten, wird die Resultante sein. Dazu ist es nützlich, das folgende Resultat zu haben. Wir betrachten für eine nichtnegative ganze Zahl M den Polynomring $K[Y_0, \dots, Y_M]$ und darin ein Ideal, welches von einer großen Zahl von homogenen Polynomen erzeugt wird. Wir möchten gerne die Anzahl der Erzeugenden möglichst weit reduzieren, ohne aber den Rang des Ideals zu verändern. Dies ist der Inhalt der folgenden Proposition.

Proposition 6. *Es sei v eine nichtnegative ganze Zahl und für eine positive ganze Zahl l seien $I_1, \dots, I_l$ homogene Ideale in dem Ring $K[Y_0, \dots, Y_M]$ mit den folgenden Eigenschaften. Für $1 \leq \lambda \leq l$ sei das Ideal I_λ durch homogene Polynome $P_{\lambda,1}, \dots, P_{\lambda,v}$ vom Grade D_λ erzeugt. Seien $\rho_1, \dots, \rho_l$ ganze Zahlen, so daß $r_\lambda = \rho_1 + \dots + \rho_\lambda$ der Rang des Ideals $(I_1, \dots, I_\lambda)$ ist für $1 \leq \lambda \leq l$. Dann gibt es für $1 \leq \lambda \leq l$, $1 \leq \mu \leq \rho_\lambda$ ganze Zahlen $u_{\lambda,\mu,v}$ mit $1 \leq v \leq v$ und den folgenden Eigenschaften. Der Absolutbetrag von $u_{\lambda,\mu,v}$ ist höchstens gleich $D_1^{\rho_1} \dots D_\lambda^{\rho_\lambda}$ und für $1 \leq \lambda \leq l$, $1 \leq \mu \leq \rho_\lambda$ sind höchstens $D_1^{\rho_1} \dots D_\lambda^{\rho_\lambda}$ der Zahlen $u_{\lambda,\mu,1}, \dots, u_{\lambda,\mu,v}$ von Null verschieden. Setzen wir*

$$F_{\lambda,\mu} = \sum_{v=1}^v u_{\lambda,\mu,v} P_{\lambda,v}$$

für $1 \leq \lambda \leq l$, $1 \leq \mu \leq \rho_\lambda$, dann hat das Ideal

$$(F_{1,1}, \dots, F_{1,\rho_1}, \dots, F_{\lambda,1}, \dots, F_{\lambda,\rho_\lambda})$$

den Rang r_λ für $1 \leq \lambda \leq l$.

Beweis. Wir beweisen diese Proposition durch Induktion. Wir können zunächst ohne Beschränkung der Allgemeinheit annehmen, daß alle ρ_λ von Null verschieden sind für $1 \leq \lambda \leq l$. Dann betrachten wir zuerst den Fall $\lambda=1$. Hier können wir annehmen, daß wir für ein ρ mit $1 \leq \rho \leq \rho_1$ wir bereits die Polynome $F_{1,1}, \dots, F_{1,\rho}$ so konstruiert haben, daß das von ihnen erzeugte Ideal I den Rang ρ besitzt. Gilt $\rho = \rho_1$, so sind wir fertig. Andernfalls können wir die Anzahl der Primärkomponenten von I durch D_1^ρ abschätzen. Da I_1 den Rang ρ_1 besitzt, finden wir für jede Primkomponente von I eines der I_1 erzeugenden Polynome, welches nicht in dieser Primkomponente liegt. Den Fall $\lambda=1$ erledigt man nun mit dem Lemma 1 aus Kap. IV in [11].

Wir können nun annehmen, daß die Proposition bereits für $1 \leq \lambda < l$ bewiesen ist. Dann betrachten wir den Fall $\lambda+1$. Wir bezeichnen mit I das von $F_{1,1}, \dots, F_{\lambda,\rho_\lambda}$ erzeugte Ideal. Die Anzahl der Primärkomponenten ist höchstens gleich dem Grad von I , welcher seinerseits durch $D_1^{\rho_1} \dots D_\lambda^{\rho_\lambda}$ beschränkt ist. Da I in $(I_1, \dots, I_\lambda)$ enthalten ist, hat es den Rang r_λ , und es gibt für jede Primkomponente von I eines der Erzeugenden von $I_{\lambda+1}$, welches nicht in dieser Primkomponente enthalten ist. Wiederum erledigt das Lemma 1 aus dem Kap. IV in [11] den vorliegenden Fall. Wir können daher annehmen, daß für $1 \leq \rho \leq \rho_{\lambda+1}$ die Polynome $F_{1,1}, \dots, F_{\lambda+1,\rho}$ bereits so konstruiert sind, daß sie ein Ideal J vom Rang $r_\lambda + \rho$ erzeugen und die in der Proposition geforderten Eigenschaften besitzen. Wir wollen dann das Polynom $F_{\lambda+1,\rho+1}$ konstruie-

ren. Wiederum ist die Anzahl der Primärkomponenten von J höchstens gleich dem Grad, welcher durch $D_1^{\rho_1} \dots D_\lambda^{\rho_\lambda} D_{\lambda+1}^{\rho_{\lambda+1}}$ abgeschätzt werden kann. Wieder können wir annehmen, daß $\rho < \rho_{\lambda+1}$ gilt. Da der Rang von J gleich $r_\lambda + \rho$ ist, finden wir wieder in dem Ideal $I_{\lambda+1}$ für jede Primärkomponente von J eines der Erzeugenden von $I_{\lambda+1}$, welches nicht in der entsprechenden Primkomponente liegt. Wiederum gibt uns das Lemma 1 aus Kap. IV in [11] das gewünschte Polynom $F_{\lambda+1, \rho+1}$. Damit ist der Induktionsschritt getan und die Proposition bewiesen.

Wir werden die Proposition in der folgenden Situation anwenden. Sei $I(A^{n\kappa})$ das Ideal von $A^{n\kappa}$ in dem Ring $K[X_1, \dots, X_\kappa]$ und J das Ideal, welches zur Diagonalen in $(\mathbb{P}^N)^\kappa$ gehört. Es wird erzeugt von den Polynomen $X_{i,j} X_{l,k} - X_{l,j} X_{i,k}$ für $1 \leq i, l \leq \kappa, 0 \leq j, k \leq N$. Weiter sei $I(S', T)(1)$ das Ideal, das in Abschnitt 8 konstruiert worden war.

Das Produkt von projektiven Räumen $(\mathbb{P}^N)^\kappa$ kann in dem projektiven Raum $\mathbb{P}^M$ für $M = (N+1)^\kappa - 1$ mit Hilfe der Segre-Einbettung eingebettet werden (siehe [6]). Die entsprechenden Koordinaten bezeichnen wir mit $Y_0, \dots, Y_M$. Die Varietät V in dem Raum $(\mathbb{P}^N)^\kappa$ sei durch die Polynome $G_i(X_1, \dots, X_\kappa)$ für $1 \leq i \leq m$ definiert. Dann können wir ohne Einschränkung der Allgemeinheit annehmen, daß für $1 \leq i \leq m$ der Grad von G_i in jedem Block von Variablen derselbe ist. Denn ist $D_{i,j}$ der Grad in den Variablen $X_{j,0}, \dots, X_{j,N}$, so setzen wir $D_i = \max_{1 \leq j \leq \kappa} (D_{i,j}) + 1$. Dann können wir G_i mit allen möglichen Monomen vom Multigrad $D_i - D_{i,j}$ in den Variablen $X_{j,0}, \dots, X_{j,N}$ multiplizieren. Diese haben keine gemeinsame Nullstelle in $(\mathbb{P}^N)^\kappa$ und so erhalten wir neue Polynome $G'_1, \dots, G'_{m'}$ für ein neues m' . Jedes G'_v ist ein Produkt eines G_μ mit einem Monom. Die Segre-Abbildung wird gegeben durch

$$X_{1,i_1} \dots X_{\kappa,i_\kappa} \mapsto Y_{i_1, \dots, i_\kappa} =: Y_j$$

für $0 \leq i_1, \dots, i_\kappa \leq N$ und eine beliebige Anordnung $Y_0, \dots, Y_M$ der obigen Variablen. Da der Grad von G_i für $1 \leq i \leq m$ in jedem Block von Variablen derselbe ist, können wir die Polynome $G_1, \dots, G_m$ schreiben als

$$G_i(X_1, \dots, X_\kappa) = H_i(Y_0, \dots, Y_M)$$

für $1 \leq i \leq m$ und homogene Polynome H_i vom selben Grad wie die Polynome G_i in $X_{j,0}, \dots, X_{j,N}$. Die Polynome $H_1, \dots, H_m$ sind natürlich nicht eindeutig bestimmt. Jedoch sind sie eindeutig modulo des definierenden Ideals des Bildes von $(\mathbb{P}^N)^\kappa$ in $\mathbb{P}^M$ unter der Segre-Abbildung. Dieses Ideal wird erzeugt in $K[Y_0, \dots, Y_M]$ durch Polynome der Form $Y_i Y_j - Y_{i',j'}$ für gewisse i, j, i', j' (für Details s. [6]). Wir bezeichnen dieses Ideal mit I_1 . Auf diese Weise erhalten wir aus dem Ideal $I(A^{n\kappa})$ ein Ideal I_2 und aus den Idealen J und $I(S', T)(1)$ die Ideale I_3 und I_5 in dem Polynomring $K[Y_0, \dots, Y_M]$. Wir wählen nun ein beliebiges multihomogene Ideal E in $K[X_1, \dots, X_\kappa]$ mit assoziiertem Ideal I_4 in $K[Y_0, \dots, Y_M]$. Gilt mit denselben Bezeichnungen wie in der Proposition 6 $\rho := \rho_4 = r_4 - r_3 > 0$, so erhalten wir die folgende Konsequenz aus der Proposition 6.

Lemma 5. *Wird das Ideal E durch multihomogene Polynome vom Multigrad höchstens D_0 und mit Höhe höchstens H_0 erzeugt, so gibt es homogene Polynome*

$F_1, \dots, F_{M-nd}, G_1, \dots, G_\rho, H_1, \dots, H_{nd+1-\rho}$ in $K[Y_0, \dots, Y_M]$ mit den folgenden Eigenschaften. Die Polynome $F_1, \dots, F_{M-nd}$ sind in dem von I_1, I_2 und I_3 erzeugten Ideal und ihre Höhe und ihr Grad sind durch eine Konstante beschränkt. Die Polynome $G_1, \dots, G_\rho$ sind in I_4 und haben höchstens den Grad D_0+1 und höchstens die Höhe $D_0^{2\rho} H_0$. Die Polynome $H_1, \dots, H_{nd+1-\rho}$ liegen in I_5 und ihr Grad ist höchstens $c_{13} LS'^2$ und ihre Höhe höchstens $D_0^{2\rho} c_{12}^{T \log T + LS'^2 + D \log S}$ für eine positive Konstante c_{13} . Schließlich ist der Rang des Ideals, welches von all diesen Polynomen erzeugt wird, gleich $M+1$.

Beweis. Das Ideal, das von $I(S', T)(1)$ und $I(A^{nk})$ erzeugt wird hat den Rang $M+1$. Dies folgt aus der Proposition 4. Aufgrund der Eigenschaften der Segre-Einbettung zieht dies nach sich, daß der Rang des von den Idealen $I_1, \dots, I_5$ erzeugten Ideals ebenfalls gleich $M+1$ ist. Nun folgt das Lemma aus der Proposition 6 zusammen mit den Abschätzungen in Proposition 3 and Lemma 4.

10. Die Resultante

In diesem Abschnitt werden wir das folgende Problem diskutieren. Gegeben seien $N+1$ homogene Polynome $F_0, \dots, F_N$ in den Variablen $X_0, \dots, X_N$. Ihre Höhe sei h_i und ihr Grad D_i für $0 \leq i \leq N$. Wir nehmen weiter an, daß sie keine nichttriviale gemeinsame Nullstelle besitzen mögen. Dann ist es wohlbekannt, daß das Radikal des von ihnen erzeugten Ideals das Ideal $(X_0, \dots, X_N)$ ist. Daher gibt es eine positive ganze Zahl $e \geq 1$ mit der Eigenschaft, daß

$$(X_0, \dots, X_N)^e \subseteq (F_0, \dots, F_N)$$

gilt. Insbesondere können wir X_0^e in der Form

$$X_0^e = H_0 F_0 + \dots + H_N F_N$$

darstellen. Hierin sind $H_0, \dots, H_N$ homogene Polynome. Wir sind nun interessiert in möglichst guten oberen Schranken für die Höhe und den Grad der Polynome $H_0, \dots, H_N$.

Wir beginnen mit einem Resultat, welches im wesentlichen von Macaulay [8] stammt. Um es anzugeben, müssen wir einige Bezeichnungen einführen. Es seien $G_0, \dots, G_N$ homogene Polynome in $X_0, \dots, X_N$ mit den Graden $D_0, \dots, D_N$ und unabhängige Variablen als Koeffizienten. Für $0 \leq i \leq N$ definieren wir die Zahlen $l_i + 1 = \binom{D_i + N}{N}$ und bezeichnen mit $\mathbf{g}_i = (g_{i,0}, \dots, g_{i,l_i})$ die Koeffizienten von G_i . Schließlich setzen wir

$$e = D_0 + \dots + D_N - N + 1$$

und $D = D_0 \dots D_N$. Dann gilt das folgende.

Proposition 7. *Es gibt ein multihomogenes Polynom*

$$R = R(\mathbf{g}_0, \dots, \mathbf{g}_N)$$

mit ganzzahligen Koeffizienten vom Grade D/D_i in den Variablen $g_{i,0}, \dots, g_{i,l_i}$ für $0 \leq i \leq N$ mit den folgenden Eigenschaften. Das Polynom R verschwindet für spezielle Werte $\mathbf{g}'_0, \dots, \mathbf{g}'_N$ von $\mathbf{g}_0, \dots, \mathbf{g}_N$ dann und nur dann, wenn die spezialisierten Polynome $G'_0, \dots, G'_N$, die man dadurch erhält, daß man die Koeffizienten $g_{i,j}$ von G_i durch die speziellen Werte $g'_{i,j}$ für $0 \leq i \leq N, 0 \leq j \leq l_i$ ersetzt, eine gemeinsame Nullstelle $(\xi_0, \dots, \xi_N)$ besitzen. Weiter ist die Höhe $h(R)$ von R höchstens gleich $\exp \left(\binom{e+N}{N} \right) \cdot \binom{e+N}{N} !$.

Beweis. Wir betrachten das Ideal in dem Polynomring $Z[\mathbf{g}_0, \dots, \mathbf{g}_N][X_0, \dots, X_N]$, welches durch die Polynome $G_0, \dots, G_N$ erzeugt wird. Es ist ein multihomogenes Ideal vom Rang $N+1$. Es folgt dann aus [8], S. 8, daß es Polynome A und R in $Z[\mathbf{g}_0, \dots, \mathbf{g}_N]$ mit den folgenden Eigenschaften. Beide Polynome sind koprim und multihomogen. Das Polynom R ist prim und verschwindet dann und nur dann für $\mathbf{g}'_0, \dots, \mathbf{g}'_N$, wenn die Polynome $G'_0, \dots, G'_N$, die man dadurch erhält, daß man die $\mathbf{g}_i$ durch die $\mathbf{g}'_i$ ersetzt, eine gemeinsame Nullstelle besitzen. Der Grad von R in den Variablen $g_{i,0}, \dots, g_{i,l_i}$ ist D/D_i für $0 \leq i \leq N$. Das Produkt AR ist eine Determinante einer $U \times U$ -Matrix mit $U \leq \binom{e+N}{N}$, deren Koeffizienten entweder gleich Null oder eine der Variablen ist. Es folgt, daß die Höhe $h(AR)$ durch die Anzahl der Glieder in der Determinante beschränkt ist, welche höchstens gleich $\binom{e+N}{N} !$ ist. Da aufgrund eines wohlbekannten Lemmas (s. z.B. [2], Chap. 12, Lemma 2) gilt

$$h(AR) e^{\deg(AR)} \geq h(R),$$

so erhalten wir für die Höhe $h(R)$ von R die gewünschte Schranke.

Wir werden nun die Proposition 7 dazu benutzen, das folgende Resultat herzuleiten, welches eine große Rolle im Beweis von Satz 1 spielt.

Proposition 8. *Es seien $F_0, \dots, F_N$ homogene Polynome der Grade $D_0, \dots, D_N$ und mit Höhen $h_0, \dots, h_N \geq 4$, deren Koeffizienten in einem algebraischen Zahlkörper K liegen. Diese Polynome seien ohne gemeinsame projektive Nullstelle. Dann gibt es eine nur von K abhängige positive Konstante $c_{14} \geq 1$ mit der folgenden Eigenschaft: Es sei X_l für $0 \leq l \leq N$ eine homogene Koordinate, ξ ein Punkt in $P^N(\mathbb{C})$ mit $X_l(\xi) \neq 0$ und $D = D_0 \dots D_N$ gesetzt. Dann gilt*

$$-c_{14} \left(N^2 e^N \log e + \sum_{i=0}^N (D/D_i) \log h_i \right) \leq \max_{0 \leq i \leq N} (\log |(F_i/X_l^{D_i})(\xi)|). \quad (21)$$

Beweis. Wir können ohne Beschränkung der Allgemeinheit annehmen, daß $X_l(\xi) = 1$ gilt. Damit identifizieren wir ξ mit einem Punkt in $A^{N+1}(\mathbb{C})$. Ferner können wir ohne Beschränkung der Allgemeinheit annehmen, daß $l=0$ gilt und setzen $X_0(\xi) = \xi_0$. Schließlich können wir noch annehmen, daß die rechte Seite von (21) negativ ist. Denn andernfalls folgt die Behauptung der Proposition trivialerweise.

Wir ersetzen nun die Koeffizienten von $F_0, \dots, F_N$ durch Variablen $\mathbf{g}_0, \dots, \mathbf{g}_N$ und bezeichnen mit $g_0, \dots, g_N$ die Koeffizienten der höchsten reinen

Potenzen von X_0 in $G_0, \dots, G_N$. Da für $g_0 = \dots = g_N = 0$ die Polynome $G_0, \dots, G_N$ die gemeinsame Nullstelle $(1, 0, \dots, 0)$ in $\mathbb{P}^N$ besitzen, verschwindet die Resultante R . Wir haben deshalb

$$R = R(\mathbf{g}_0, \dots, \mathbf{g}_N) \in (g_0, \dots, g_N).$$

Wir schreiben nun

$$R = \sum_{i_0=0}^{D/D_0} \dots \sum_{i_N=0}^{D/D_N} r_{i_0, \dots, i_N} g_0^{i_0} \dots g_N^{i_N},$$

wobei die Koeffizienten $r_{i_0, \dots, i_N}$ in $\mathbb{Z}[\mathbf{g}_0, \dots, \mathbf{g}_N]$ liegen und nicht von $g_0, \dots, g_N$ abhängen. Ihre Höhen sind beschränkt durch die Höhe $h(R)$ von R .

Ersetzen wir in $G_0, \dots, G_N$ die Koeffizienten $g_0, \dots, g_N$ durch $g_0 - G_0(\xi), \dots, g_N - G_N(\xi)$, so haben die daraus resultierenden Polynome $G_{j,\xi} = G_j(X) - G_j(\xi) X_0^{D_j}$ ($0 \leq j \leq N$) eine gemeinsame Nullstelle, nämlich ξ . Daher verschwindet ihre Resultante. Wir erhalten dann

$$0 = \sum_{i_0=0}^{D/D_0} \dots \sum_{i_N=0}^{D/D_N} r_{i_0, \dots, i_N} (g_0 - G_0(\xi))^{i_0} \dots (g_N - G_N(\xi))^{i_N}.$$

Wir können die rechte Seite als ein Polynom in $G_0(\xi), \dots, G_N(\xi)$ schreiben. Der konstante Term dieses Polynoms ist gerade die Resultante $R(\mathbf{g}_0, \dots, \mathbf{g}_N)$ und nun folgt die Proposition aus der Tatsache, daß die obige Relation gültig bleibt, wenn wir die Spezialisierung $\mathbf{g}_i \mapsto \mathbf{f}_i$ für $0 \leq i \leq N$ durchführen, wobei die $\mathbf{f}_i = (f_{i,0}, \dots, f_{i,l_i})$ die Koeffizienten von F_i sind. Der konstante Term $R(\mathbf{f}_0, \dots, \mathbf{f}_N)$ ist die Spezialisierung der Resultanten $R(\mathbf{g}_0, \dots, \mathbf{g}_N)$ und verschwindet nicht, da $F_0, \dots, F_N$ keine gemeinsame Nullstelle besitzen. Die Behauptung in der Proposition 8 folgt nun aus leicht durchzuführenden Abschätzungen.

11. Beweis von Satz 1

Wir sind nun in der Lage, den Beweis von Satz 1 zu beenden. Wir betrachten in $(A^n)^K$ den Punkt $\xi = (\exp_{A^n}(\alpha), \dots, \exp_{A^n}(\alpha))$. Sei W sein Zariski-Abschluß über $\mathbb{Q}$. Dies ist eine projektive Varietät in $(\mathbb{P}^N)^K$. Sei E' das entsprechende Ideal in $\mathbb{Q}[\mathbf{X}_1, \dots, \mathbf{X}_K]$. Dann besitzt E' eine Basis von Polynomen, die über einem algebraischen Zahlkörper definiert sind. Wir wollen in Zukunft daher annehmen, daß alle auftretende Objekte über einem algebraischen Zahlkörper K definiert sind. Wir setzen $E = E' \cap K[\mathbf{X}_1, \dots, \mathbf{X}_K]$. Mit den Bezeichnungen aus Abschnitt 9 erhalten wir die Ideale $I_1, \dots, I_5$ in $K[Y_0, \dots, Y_M]$. Wir nehmen nun an, daß der Satz 1 falsch ist und erhalten insbesondere, daß $\rho = \rho_4 > 0$. Nach Lemma 5 erhalten wir Polynome $F_1, \dots, F_{M-nd}$, $G_1, \dots, G_\rho$ und $H_1, \dots, H_{nd+1-\rho}$ in $K[Y_0, \dots, Y_M]$ mit den folgenden Eigenschaften. Die Polynome $F_1, \dots, F_{M-nd}$, $G_1, \dots, G_\rho$ liegen in dem Ideal, welches von den Idealen I_1, I_2, I_3 und I_4 erzeugt wird und ihre Höhe und ihr Grad sind durch eine Konstante c_{15} beschränkt. Sie verschwinden alle auf dem Bild von W in $\mathbb{P}^M$.

unter der Segre-Abbildung. Die Polynome $H_1, \dots, H_{nd-\rho+1}$ schließlich liegen in I_5 und ihr Grad ist höchstens gleich $c_{16}LS'^2$ und ihre Höhe höchstens gleich $c_{17}^{T \log T + LS'^2 + D \log S}$ für positive Konstanten c_{16} und c_{17} . Alle diese Polynome haben keine gemeinsame Nullstelle. Daher können wir die Proposition 8 anwenden und erhalten

$$\max(\log |F_1(\eta)|, \dots, \log |H_{nd+1-\rho}(\eta)|) \geq -V, \quad (22)$$

wo $V = c_{18}[(LS'^2)^N \log(LS') + (T \log T + D \log S)(LS'^2)^{nd-\rho}]$ und η das Bild von ξ unter der Segre-Abbildung ist. Da $F_1(\eta) = \dots = G_\rho(\eta) = 0$ ist, genügt es, die Absolutbeträge von $H_1(\eta), \dots, H_{nd-\rho+1}(\eta)$ abzuschätzen. Die Polynome H_i sind für $1 \leq i \leq nd - \rho + 1$ Linearkombinationen von höchstens $c_{19}(LS'^2)^{nd}$ der Erzeugenden von I_5 mit ganzzahligen Koeffizienten, deren Absolutbeträge die Zahl $c_{20}(LS'^2)^{nd}$ nicht übersteigen. Da weiter das Ideal I_5 das Bild von $I(S', T)(1)$ unter der Segre-Abbildung ist, erhalten wir schließlich aus der Proposition 5 die Abschätzung

$$\log |H_i(\eta)| \leq -c_{21} TS^{mn} \log T. \quad (23)$$

Nun vergleichen wir die Abschätzungen (22) und (23). Dazu wählen wir T so groß, daß $D \log S \leq T \log T$ ist. Dann sind (22) und (23) äquivalent zu der Ungleichung

$$2(nd - \rho) + 8\varepsilon(nd - \rho)/mn \geq mn.$$

Da dies für jedes positive ε richtig sein muß, muß

$$2(nd - \rho) \geq mn$$

gelten. Da aber ρ gleich der Kodimension des Zariski-Abschlusses von $\exp_{A^n}(\alpha)$ über $\mathbb{Q}$ ist und da die Dimension von A^n gleich nd ist, erhalten wir die gewünschte Abschätzung für die Dimension dieses Zariski-Abschlusses. Damit ist der Satz 1 vollständig bewiesen.

Literatur

1. Anderson, M.: Linear forms in algebraic points of an elliptic function, Ph.D. dissertation (Nottingham, 1978)
2. Baker, A.: Transcendental Number Theory, Cambridge University Press 1975
3. Bertrand, D.: Problèmes locaux. Soc. Math. de France, Astérisque **69-70**, 163-189 (1979)
4. Choodnovsky, G.V.: Algebraic independence of the values of elliptic function at algebraic points. Invent. math. **61**, 267-290 (1980)
5. Hartshorne, R.: Algebraic geometry. Berlin-Heidelberg-New York: Springer 1979
6. Hodge, W.V.D., Pedoe, D.: Methods of algebraic geometry, vol. 1, 2, Cambridge (1952)
7. Lindemann, F.: Über die Zahl π . Math. Ann. **20**, 213-225
8. Macaulay, F.S.: The algebraic theory of modular systems. Stechert-Hafner Service Agency, New York and London 1964 (reprinted)
9. Masser, D.W., Wüstholz, G.: Zero estimates on group varieties I. Invent. math. **64**, 489-516 (1981)
10. Masser, D.W., Wüstholz, G.: Algebraic independence properties of values of elliptic functions, Journées Arith. Exeter (1980), London M.S. Lecture Notes
11. Masser, D.W., Wüstholz, G.: Fields of large transcendence degree generated by values of elliptic functions. Invent. math.

12. Masser, D.W., Wüstholz, G.: Zero Estimates on Group Varieties II. in preparation
13. Philippon, P.: Indépendance algébrique de valeurs de fonctions p -adiques. J. reine u. angew. Math. **329**, 42–51 (1981)
14. Philippon, P.: Indépendance Algébrique et Variétés Abéliennes. C.R. Acad. Sci. Paris, Ser. I, t. 294, 257–259 (1982)
15. Philippon, P.: Variétés Abéliennes et Indépendance Algébrique I. (preprint)
16. Schneider, Th.: Einführung in die transzendenten Zahlen. Berlin-Heidelberg-New York: Springer 1957
17. Serre, JP.: Quelques propriétés des groupes algébriques commutatifs. Soc. Math. de France, Astérisque **69–70**, 191–202 (1979)
18. Waldschmidt, M.: Nombres transcendants et groupes algébriques. Soc. Math. de France Astérisque **69–70**, (1979)
19. Wüstholz, G.: Sur l'analogie abélien du Théorème de Lindemann. C.R. Acad. Sci. Paris Ser. I, t. 295, 35–37 (1982).
20. Wüstholz, G.: Multiplizitätsabschätzungen auf algebraischen Gruppen. Ann. of Math. (in press)
21. Hochschild, G.: The Structure of Lie Groups. San Francisco, London, Amsterdam: Holden-Day 1965

Oblatum 11-VIII & 22-XI-1982

Nachtrag bei der Korrektur

Der Beweis von Satz 1 wurde so geführt, daß man sofort ein Maß für die algebraische Unabhängigkeit erhält. Dazu seien die Voraussetzungen dieselben wie vom Korollar 1.

A^n sei wie üblich in einen projektiven Raum $\mathbb{P}^N$ eingebettet. Dann sei $Y \subset A^n$ eine Hyperfläche vom Grad $d(Y)$ definiert über einem algebraischen Zahlkörper K . Wir definieren dann die Höhe $H(Y)$ von Y als das Minimum über die Höhen aller homogener Polynome mit Koeffizienten in K , welche auf Y verschwinden und deren Grad durch $d(Y)$ beschränkt ist. Ist h ein Punkt auf A^n , so bezeichnen wir mit $\text{dist}(h; Y)$ den Abstand von h zu Y . Dann gilt der folgende Satz.

Satz 3. *Es gibt eine effektiv berechenbare Konstante $c_1 > 0$, welche nicht von $H(Y)$ abhängt, so daß unter den Voraussetzungen von Korollar 1 gilt*

$$\log(\text{dist}(g; Y)) \geq -c_1(1 + \log H(Y)).$$

Der Beweis von Satz 3 motiviert insbesondere das Lemma 5, welches wir nicht in voller Schärfe im Beweis von Satz 1 ausgenutzt haben. Die Konstante c_1 hängt natürlich von dem Grad $d(Y)$ von Y ab. In einer nachfolgenden Arbeit soll unter anderem diese Abhängigkeit genauer untersucht werden. Dies führt dann zu dem folgenden Ergebnis.

Satz 3'. *Es sei $\varepsilon > 0$ eine positive reelle Zahl. Dann gibt es eine effektive berechenbare Konstante $c_2 > 0$, die nicht von $d(Y)$ und $H(Y)$ abhängt, so daß unter den Voraussetzungen von Korollar 1 gilt*

$$\log(\text{dist}(g; Y)) \geq -c_2 d(Y)^{nd+\varepsilon} (d(Y) + \log H(Y)).$$