MULTIPLICITY ESTIMATES ON GROUP VARIETIES

BY

G. Wüstholz

Sonderforschungsbereich 40
Theoretische Mathematik
Beringstraße 4
D-5300 Bonn 1

Max-Planck-Institut
für Mathematik
Gottfried-Claren-Str. 26
D-5300 Bonn 3

SFB/MPI 8/ '3

1. Introduction. In the present paper we shall prove a zeroes estimate on algebraic groups that also takes into account multplicities with respect to a given analytic subgroup. This is part of an extensive program which was started by D.W. Masser and the author with [13] and continued with [14] . It is attached directly to section 9 of [13] and lays out another stage of this program. We shall outline this more precisely in the last section.

Before we can state the main result of this paper we have to introduce some concepts and notations. Let G be a quasi-projective connected commutative algebraic group of dimension $n \geq 1$ defined over a subfield K of the complex numbers. We shall assume that this field is algebraically closed. In most applications the field K will be the field $\overline{\mathbb{Q}}$ of algebraic numbers. We remark at this point that the results remain true if we take instead of the field of complex numbers $\mathbb{C}$ its p-adic analoge $\mathbb{C}_p$ for some fixed prime p and for K a corresponding subfield K_p of $\mathbb{C}_p$. We restrict ourselves to the complex case in order to avoid some minor complications appearing in the p-adic domain. These complications always arise when analytic functions come in. Our functions are defined globally in the case of complex numbers but only locally in the case when we are dealt with the p-adic domain. These difficulties can be avoided by a purely algebraic approach. If we took this approach the only condition on the groundfield would be that it should be algebraically closed and of characteric zero. But we prefer to avoid such an approach in order to keep the text understandable also for those who are mainly interested in the applications in transcendence.

Let $z_1, \ldots, z_n$ be the coordinates in the tangent space $T(G)$ at the neutral element of the algebraic group G . This group can be compactified and this compactified group $\overline{G}$ can be embedded in some projective space

$\mathbb{P}^N$ by means of a very ample divisor D in $\overline{G}$ defined over K (for details see [17]). Then the exponential map $\exp_G : T(G) \longrightarrow G$ is given by holomorphic functions $f_0(z_1,\ldots,z_n),\ldots,f_N(z_1,\ldots,z_n)$ with no common zero. The embedding just described has the property that the partial derivatives $\frac{\partial}{\partial z_1}, \ldots, \frac{\partial}{\partial z_n}$ are derivations of the ring $K[f_1/f_0,\ldots,f_N/f_0]$ (see [17],§ 1,1.3. and [18], Propostion 1.2.3) since they are a basis of the Lie algebra $L(G)$ of translation invariant vector fields on G. We remark at this point that the function f_0 does not play an exceptional role. Instead of it we could take any linear combination g of $f_0,\ldots,f_N$ with coefficients in K. This changes the embedding by a projective automorphism of $\mathbb{P}^N$. This makes it for example possible to choose the embedding in such a way that for any set of points in G defined over some finitely generated extension of $\mathbb{Q}$ the function f_0 does not vanish at any point of this set.

For an integer d with $1 \leq d \leq n$ let now be $\varphi : \mathbb{C}^d \longrightarrow G$ a d-parameter subgroup of G. By definition this is a group homomorphism φ which makes the Lie group $\mathbb{C}^d$ into a Lie subgroup of G. (for details see for example [19]). We frequently identify a Lie subgroup of G with its image in G. We say that a subgroup A of G is an analytic subgroup if it is the image of a Lie subgroup. We point out that the topology of A is in general not the topology induced by the topology of G. We say that a subgroup H of G is algebraic if it is analytic and closed in the Zariski topology of G. Now it is clear that the image $\varphi(\mathbb{C}^d)$ of $\mathbb{C}^d$ is an analytic subgroup A of G and the differential $d\varphi$ of φ can be used to identify $\mathbb{C}^d$ with the tangent space $T(A)$ of A at the neutral element of G. Since $T(A)$ is a subspace of $T(G)$ we can write φ as

$$\varphi = \exp_G \circ L$$

where L is a linear map $L : T(A) \longrightarrow T(G)$. Let $\zeta_1,\ldots,\zeta_d$ be the coordinates in $T(A)$. Then we can write L as

$$z_i = L_i(\zeta_1,\ldots,\zeta_d) \qquad (1 \leq i \leq n)$$

with linear forms $L_1,..,L_n$ in $\zeta_1,..,\zeta_d$. These linear forms have rank d. It follows that there are $n - d$ linearly independent linear forms $M_1, \ldots, M_{n-d}$ with

$$M_j(L_1, \ldots, L_n) = 0 \qquad (1 \leq j \leq n-d) .$$

Therefore we can define the space $T(A)$ in $T(G)$ by the relations

$$M_j(z_1, \ldots, z_n) = 0 \qquad (1 \leq j \leq n-d).$$

Therefore the analytic homomorphism φ is given by the analytic functions

$$g_i = f_i \circ L \qquad (0 \leq i \leq N)$$

and we can write $g_i = g_i(\zeta_1,..,\zeta_d)$ for $0 \leq i \leq N$. The Lie algebra $\mathfrak{l}(A)$ of A is a subalgebra of $\mathfrak{l}(G)$ and the partial derivations $\frac{\partial}{\partial\zeta_1},\ldots,\frac{\partial}{\partial\zeta_d}$ form a basic of $\mathfrak{l}(A)$. We say that φ or equivalently A is defined over K if the coefficients of $M_1,\ldots,M_{n-d}$ are in K. If follows then that the linear forms $L_1,\ldots,L_n$ can be chosen in such a way that the coefficients are in K. If these coefficients are in K then conversely φ and A are defined over K.

Next we define the order of a homogenous polynomial in the coordinates $X_0,\ldots,X_N$ of $\mathbf{P}^N$ with respect to a d-parameter subgroup φ of G in the following way. Let $P(X_0,\ldots,X_N)$ be a homogenous polynomial. Let x be in $T(G)$ and g in G defined by $g = \exp_G(x)$. Without loss of generality we may assume that $f_0(x) \neq 0$. Then we define $\Psi(\zeta)$ for $\zeta = (\zeta_1,\ldots,\zeta_d)$

as

$$\Psi(\zeta) = P(1, f_1/f_0, \ldots, f_N/f_0)(x + L(\zeta)) \quad .$$

This function is analytic at $\zeta = 0$. If Ψ is identically zero we let the order of P in g along φ be infinite. Otherwise this order is the greatest integer $T \geq 0$ such that

$$(\frac{\partial}{\partial \zeta_1})^{t_1} \ldots (\frac{\partial}{\partial \zeta_d})^{t_d} \Psi(0) = 0$$

for all non-negative integers $t_1, \ldots, t_d$ with $t_1 + \ldots + t_d < T$. This number is denoted by $\mathrm{ord}_g(\varphi, P)$.

All spaces which occure in this paper are complex spaces. They have therefore a well-defined dimension. If X and Y are complex spaces and if $X \subseteq Y$ as sets then we denote by $\mathrm{cod}_Y X$ or - if there is no danger for confusion - by $\mathrm{cod}\, X$ the codimension of X in Y. This is by definition the number

$$\mathrm{cod}_Y X = \dim Y - \dim X \quad .$$

Next we define for integers r with $1 \leq r \leq n$ non-negative integers τ_r in the following way. Let $A = \varphi(\mathbb{C}^d)$ be the analytic subgroup defined by φ. Suppose A is defined over K. Then let τ_r be the minimum over all codimensions $\mathrm{cod}_A\, V \cap A$ where V runs through all algebraic subvarieties of G of codimension r which are defined over K and do contain an element of A. Then we obviously have $0 \leq \tau_r \leq \min(r,d)$. With these numbers we define the exponent $\tau(\varphi;G)_K$ as

$$\tau_K := \tau(\varphi;G)_K = \min_{1 \leq r \leq n} (\tau_r / r)$$

If $K = \mathbb{C}$ we simply suppress the subspricpt and simply write $\tau = \tau(\varphi;G)$.

This exponent corresponds in a certain sense to the exponent $\nu(\Gamma;G)$ in [13]. The exponent $\sigma(\varphi;G)_K$ that corresponds to the exponent $\mu(\Gamma;G)$ in [13] is defined in the following way. For integers r with $1 \le r \le n$ we let σ_r be $\min(r,d)$ if G does not contain an algebraic subgroup of codimension r defined over K. Otherwise we let σ_r be the minimal codimension $\mathrm{cod}_A H \cap A$ where H runs through all algebraic subgroups of G of codimension r which are defined over K. Then we put

$$\sigma_K = \sigma(\varphi;G)_K = \min_{1 \le r \le n} (\sigma_r/r) .$$

Again we have $0 \le \sigma_r \le \min(r,d)$ and it follows that $0 \le \sigma,\tau \le d/n$. Furthermore a necessary and sufficient condition for A to be dense in the Zariski topology is that $\sigma > 0$. Since A and φ correspond to each other uniquely we also write $\sigma(A;G)_K$ instead of $\sigma(\varphi;G)_K$ and in the same way $\tau(A;G)_K$ instead of $\tau(\varphi;G)_K$.

To any subset V of G we associate the set $S(V)$ consisting of all g in G such that $g+V \subseteq V$. This is obviously a subgroup of G. If V is an irreducible algebraic variety then $S(V)$ is an algebraic subgroup of G.

Let Ω and Ω^* be two finite subsets of $G(K)$, the group of K-rational points on G, with $0 \in \Omega^*$.

Then for each irreducible subvariety V of G we define $\ell(V)$ as the number of different residue classes in Ω^* modulo $S(V)$. Then for integers r with $1 \le r \le n$ we define the integer ℓ_r to be the minimum of $\ell(V)$ taken over all irreducible subvarieties V of codimension r.

Next for integers r with $1 \le r \le n$ we define

$$\Omega_r = \bigcap_{\gamma \in (r-1)\Omega^*} (\Omega - \gamma) \qquad (1 \le r \le n)$$

where we denote by $(r-1)\,\Omega^*$ the set of linear combinations $\omega_1+\ldots+\omega_{r-1}$, $\omega_i \in \Omega^*$. Note that

$$\Omega = \Omega_1 \supseteq \Omega_2 \supseteq \ldots \supseteq \Omega_n$$

since the neutral element 0 is in Ω^*. Furthermore it is easily verified that for $1 \le r \le n-1$

$$\Omega_{r+1} = \bigcap_{\gamma \in \Omega^*} (\Omega_r - \gamma) .$$

Here the equality was pointed out to me by D.W. Masser. Then we have the following result.

Main Theorem. There exists a positive constant c depending only on G with the following property. For real numbers $D \ge 0$, $T \ge 1$ let $P(X_0,\ldots,X_N)$ be a homogenous polynomial of degree at most D that vanishes to order at least T with respect to φ on Ω. Then if

(1) $$(T/n)^{T_r} \ell_r \ge (cD)^r \qquad (1 \le r < n)$$
$$(T/n)^T |\Omega_n| \ge (cD)^n$$

and

(2) $$\ell_r \ge (cD)^{r-T_r} \qquad (1 \le r < n)$$

the polynomial P vanishes on all of G.

In general the conditions (1) and (2) are not easy to verify since the computation of the numbers $\ell_r (1 \le r \le n)$ is for general Ω^* very delicate. But in most applications in transcendence theory the sets Ω and Ω^* are very simple. For example there are nice subsets of finitely generated groups. Then the Main Theorem can be stated much more explicitely. This we want to do now.

For this let Γ be a finitely generated subgroup of G defined over K.

Let Γ be generated by the elements $\gamma_1,\ldots,\gamma_m$ and let ℓ be the rank of Γ. Then we define for integers r with $1 \le r \le n$ the non-negative integers q_r as in [13].

Accordingly q_r is the minimal corank of subgroups Γ' of Γ in Γ such that there exists an algebraic subvariety V of G of codimension r which is defined over K and satisfies

$$V + \Gamma' \subset V .$$

We remark that in contrast to the definition in [13] we consider only those subvarieties V of G which are defined over some subfield K of $\mathbb{C}$. Similarily we define the number p_r of [13] to be the minimal corank of subgroups Γ' of Γ in Γ such that there exists an algebraic subgroup H of G of codimension r which is defined over K and contains Γ'. If there does not exist an algebraic subgroup H of G of codimension r defined over K then we put $p_r = \ell$.

Then we put

$$\mu_K = \mu(\Gamma;G)_K = \min_{1\le r\le n} p_r/r$$

and

$$\nu_K = \nu(\Gamma;G)_K = \min_{1\le r\le n} q_r/r .$$

It is easy to see that the proof of Lemma 9 in [13] can be modified to establish the equality $\mu(\Gamma;G)_K = \nu(\Gamma;G)_K$. For real numbers $S \ge 0$ we denote as usual by $\Gamma(S)$ the set of γ in Γ of the form $s_1\gamma_1+\ldots+s_m\gamma_m$ with $0 \le s_1,\ldots,s_m \le S$.

Main Theorem*. There exists a positive constant c depending only on G with the following property. For real numbers $S \ge 0$, $\nu < 0$ and $T \ge 1$ let

$P(X_0,\dots,X_N)$ be a homogeneous polynomial of degree at most D that vanishes to order at least T with respect to φ on $\Gamma(S)$. Then if

$$(1)^* \qquad (T/n)^{\tau_r}(S/n)^{q_r} \geq (cD)^r \qquad (1 \leq r < n)$$
$$(T/n)^{\tau_n}|\Gamma(S/n)| \geq (cD)^n$$

and

$$(2)^* \qquad S^{q_r} \geq (cD)^{r-\tau_r} \qquad (1 \leq r < n)$$

the polynomial P vanishes on all of G.

This theorem implies the Main Theorem in [13] as well as Theorem A in section 9 of [13]. The second condition in (1)* is even slightly weaker than the corresponding condition in the Main Theorem in [13].

So we do not get any real improvement in that condition. But to state it in this way becomes interesting when dealing with Baker's method where in certain circumstances the group Γ is a torsion group. The last condition (2)* in the Main Theorem* is the most troublesome one. But it is possible to eliminate this condition by the use of new ideas developed in [20]. But apart from this the Main Theorem* is essentially best possible. This can be shown in the same way as done in section 7 of [13] with the Main Theorem there.

The condition (1)* is certainly implied by the condition

$$(T/n)^{\sigma}(S/n)^{\mu} \geq cD$$

since we shall show that $\sigma = \tau$ and since $|\Gamma(S/n)| \geq (S/n)^{q_n}$. This condition can be verified very easily in many cases appearing in transcendence.

Most of this paper is devoted to a proof of the Main Theorem together with an explicit calculation of the constant c. We shall make essential use of two

different tools. On the one hand we shall use the techniques developed in [13]. On the other hand we make use of an estimate of the length of a primary ideal in terms of the order with respect to an analytic subgroup. In section 2 we give some prelimiaries about the derivations and differential operators which we shall use. In particular we introduce a third exponent connected with them which turns out to be very useful to simplify the proofs.

In section 3 we continue with estimating lengths of primary ideals in terms of the order of vanishing with respect to certain differential operators. This is one of the main tools for the proof of the Main Theorem. In section 4 we shall deduce the Main Theorem* from the Main Theorem. In section 5 we shall state and prove a proposition from which we shall deduce in section 6 the Main Theorem.

Section 7 is devoted to an analysis of the different exponents σ_K, τ_K and the exponents ρ_r which are introduced in section 2. In particular we shall prove that the numbers ρ_r and q_r are equal. The main result in this section will be the proof of the equality of σ_K and τ_K. This makes it particularily simple to calculate the numbers τ_r appearing in the Main Theorem. Normally they can't be calculated in a simple way. But the numbers σ_r can be calculated very easily and since $\sigma_K = \tau_K$ we get the right estimates for the numbers τ_r via the numbers σ_r.

In section 8 we shall give an application of the Main Theorem to Baker's method and state and prove the multiplicity estimates used there in order to obtain linear independence results for logarithms and elliptic logarithms. In particular multiplicity estimates of this type can be used to obtain very good effective bonds for linear forms in elliptic logarithms whose non-vanishing was proved by Bertrand and Masser [4]. It is clear that the same can be obtained now more generally for linear forms in abelian logarithms.

In section 9 we shall discuss some of the applications which are consequences of our Main Theorem. The first application asserts that an analytic subgroup defined over $\overline{\mathbb{Q}}$ does not possess a non-trivial algebraic point in general. This has an interesting application to trancendence properties of elliptic and more general abelian integrals of arbitrary kind. Finally we shall give a lower bound for linear forms in logarithms on an arbitrary commutative and quasi-projective group variety. The proofs of these results will appear in forthcoming papers. In this paper we shall often make explicitly or not use of the following property of the field K. Suppose that for some integer $k \geq 1$ we have an arbitrary set of non-zero polynomials $P(t_1,\ldots,t_k)$ in the ring $L[t_1,\ldots,t_k]$ for some field $L \subseteq \mathbb{C}$ that is finitely generated over the rationals. Suppose that all the polynomials of this set have bounded degree. Then there exists elements $\tau_1, \ldots, \tau_k$ in K such that $P(\tau_1,..,\tau_k) \neq 0$ for every polynomial P in this set. This follows easily from the fact that the field K contains elements of arbitrary large degree over L.

Finally we should remark that this paper profits from many useful discusions of the author with D.W. Masser.

2. Some preliminary remarks. We begin this section with introducing two rings of differential operators $\mathcal{D}(G)$ and $\mathcal{D}(A)$ that belong to G and A. The ring $\mathcal{D}(A)$ will be a certain subring of $\mathcal{D}(G)$ which itself is a commutative ring of dimension n.

In order to define these rings we consider an arbitrary affine part $\mathbb{A}^N$ of $\mathbb{P}^N$. We may assume without loss of generality that this part is given by $X_0 \neq 0$ and we shall fix this part from now on. We denote the affine coordinates of this part by $x_1,\ldots,x_N$ so that we may write $x_\ell = X_\ell/X_0$ $(1 \leq \ell \leq N)$. Let $I(G)$ be the homogeneous ideal of G. Then the dehomogenized ideal $I(G)^{aff}$ is the affine ideal of $G \cap \mathbb{A}$ in the polynomial ring $K[x_1,\ldots,x_N]$. Let $K[G]$ be the residue class ring $K[x_1,\ldots,x_N] / I(G)^{aff}$ and $K(G)$ be the quotient field. We denote by $K[G]^{an}$ and $K(G)^{an}$ the corresponding ring and field which we obtain after having replaced the residue classes $x_i + I(G)^{aff}$ by the functions f_i/f_0 for $1 \leq i \leq N$. If we replace these residue classes $x_i + I(G)^{aff}$ in $K[G]$ by the functions g_i/g_0 for $1 \leq i \leq N$ when we obtain the ring $K[G]^{\varphi}$ and its quotient field $K(G)^{\varphi}$. We put

$$F_i = f_i/f_0 \qquad (1 \leq i \leq N)$$

and

$$G_i = g_i/g_0 \qquad (1 \leq i \leq N)$$

As we have remarked already at the beginning, the ring $K[G]^{an}$ is mapped into itself by the partial derivations $\frac{\partial}{\partial z_i}$ for $1 \leq i \leq n$ (see[18]). Therefore the functions $F_1,\ldots,F_N$ satisfy a system of partial differential equations

$$(3) \qquad \frac{\partial}{\partial z_i} F_i = H_{ij}(F_1,\ldots,F_N)$$

for $1 \leq i \leq n$ and $1 \leq j \leq N$ with polynomials $H_{ij}(x_1,\ldots,x_N)$. The corresponding system of partial differential equations for the functions $G_1,\ldots,G_N$ is then given by

$$(4) \qquad \frac{\partial}{\partial \zeta_i} G_j = \sum_{k=1}^{n} \frac{\partial L_k}{\partial \zeta_i} \cdot H_{kj}\,(G_1,\ldots,G_N)$$

for $1 \leq i \leq d$ and $1 \leq j \leq N$. It follows that the ring $K[G]^{\varphi}$ is also mapped into itself by the parial derivations $\frac{\partial}{\partial \zeta_i}$ for $1 \leq i \leq d$.

This can be translated now to the ring $K[G]$ and its quotient field. For this we define the derivations ∂_i for $1 \leq i \leq n$ by

$$\partial_i P(x_1,\ldots,x_N) = \sum_{j=1}^{N} H_{ij}(x_1,\ldots,x_N) \frac{\partial}{\partial x_j} P(x_1,\ldots,x_N)$$

for polynomials $P(x_1,\ldots,x_N)$. Since we have

$$\partial_i\, I(G)^{aff} \subset I(G)^{aff} \quad (1 \leq i \leq n)$$

these derivations induce derivations of the ring $K[G]$ and its quotient field $K(G)$. There they are pairwise commutative and we denote them again with $\partial_i (1 \leq i \leq n)$. Then we can write

$$(5) \qquad \partial_i = \sum_{j=1}^{N} H_{ij} \frac{\partial}{\partial x_j} \qquad (1 \leq i \leq n)\ .$$

By this we have defined the algebraic counterpart of (3). The algebraic counterpart of (4) is given on $K[x_1,\ldots,x_N]$ and then also on $K[G]$ by

$$(6) \qquad \Delta_i = \sum_{i=1}^{n} \ell_{ki}\, \partial_K \qquad (1 \leq i \leq d)\ .$$

where we have put $\ell_{ki} = \frac{\partial L_R}{\partial \zeta_i} \in \mathbb{C}$ for $1 \leq k \leq n$ and $1 \leq i \leq d$. Now we define $\mathcal{D}(G)$ to be the polynomial ring generated by $\partial_1,\ldots,\partial_n$ over the field K. In the same way we define $\mathcal{D}(A)$ to be the subring generated by $\Delta_1,\ldots,\Delta_d$ over K. Since G is commutative both rings are rings of commutative differential operators. Next we recall some notations from

[13] which we shall need later on. Let Σ be the group generated by the elements of Ω and Ω^*. Then this is a subgroup of $G(L)$ for some finitely generated subfield L of K. Then unless otherwise stated the operator of contracted extension (see [13]) denoted as usual by a star is defined with respect to the group Σ. Further the operators $E(\gamma)$ and $E(\gamma)$ for γ in Σ are defined as in [13]. These operators can be defined over K using the property of the field K stated at the end of section 1 instead of the corresponding on in [13]. We remark that $E(\gamma)$ represents on a Zariski open set the morphism from G to G given by the translation by an element γ in Σ. This open set contains Σ. We denote by b the degree of $E(\gamma)$, i.e. the number a in Lemma 1 in [13].

Finally let V be an irreducible subvariety of G and r its codimension. Then we take a basis $P_1,\ldots,P_\ell$ of the prime ideal $I(V)$ in $K[G]$ consisting of the elements of $K[G]$ that vanish on V. We define the Jacobian matrix $J(P_1,\ldots,P_\ell;\mathcal{D}(A))$ as the matrix

$$\begin{bmatrix} \Delta_1 P_1 \pmod{I(V)} & \ldots & \Delta_d P_1 \pmod{I(V)} \\ \vdots & & \vdots \\ \Delta_1 P_\ell \pmod{I(V)} & \ldots & \Delta_d P_\ell \pmod{I(V)} \end{bmatrix}$$

Its rank $\rho(V)$ over the quotient field $K(V)$ of the ring $K[V] = K[G]/I(V)$ is independent of the choice of the basis $P_1,\ldots,P_\ell$ as can easily be verified. Then for integers r with $1 \leq r \leq n$ we define the numbers ρ_r to be the minimum of the ranks of these Jacobian matrices taken over all irreducible subvarieties V of G of codimension r. Since the vector fields $\Delta_1,\ldots,\Delta_d$ are translation invariant vector fields on G we deduce that $\rho(V) = \rho(V + g)$ for all g in G.

3. Differential operators and length of ideals. In this section we shall show how to estimate the length of a primary ideal by means of the differential operators $\Delta_1,\ldots,\Delta_d$. In order to do this we need that prime ideals in $K[G]$ have the property to be locally at every simple point a complete intersection. This is the content of the following auxiliary Lemma.

Lemma 1. Let $\mathfrak{P}$ be a prime ideal in $K[G]$ of rank r satisfying $1 \leq r \leq n$ and $\mathfrak{m}$ a maximal ideal containing $\mathfrak{P}$ corresponding to a simple point of the variety of $\mathfrak{P}$. Then there exist elements $P_1,\ldots,P_r$ in $K[G]$ such that

$$\mathfrak{P}M^{-1} = (P_1,\ldots,P_r)\, M^{-1}$$

for $M = K[G] \setminus \mathfrak{m}$ in $K[G]M^{-1}$.

Proof. Let p be the comonical homomorphism from $K[x_1,\ldots,x_N]$ onto $K[G]$. Then we apply Theorem 1.16 in [15] to $p^{-1}(\mathfrak{P})$ and $p^{-1}(M)$. The ideal $p^{-1}(\mathfrak{P})$ has rank $N - n + r$ and $p^{-1}(M)$ is a multplicative set in $K[x_1,\ldots,x_N]$ corresponding to $p^{-1}(\mathfrak{m})$. It follows that there are polynomials $Q_1, \ldots, Q_{N-n}$ and $P_1', \ldots, P_r'$ in $p^{-1}(\mathfrak{P})$ such that

$$p^{-1}(\mathfrak{P})\, p^{-1}(M)^{-1} = (Q_1,\ldots,Q_{N-n},P_1',\ldots,P_r')\, p^{-1}(M)^{-1}$$

and

$$p(Q_i) = 0 \qquad (1 \leq i \leq N-n)\ .$$

Since the formation of residue class rings and the localisation commute (see [21]) it follows that we have

$$\mathfrak{P}M^{-1} = (P_1,\ldots,P_r)M^{-1}$$

for $P_i = p(P_i')$ and $1 \leq i \leq r$. But this is that we wanted to show and

therefore concludes the proof of the Lemma.

Before we come to the main result of this section we need some further technical lemma which we have to use in the subsequent Lemma.

Lemma 2. Let I be an ideal and M a multiplicative set in $K[G]$. Then for all non-negative integers $t_1,\dots,t_d$ we have

$$\Delta_1^{t_1} \dots \Delta_d^{t_d} (IM^{-1}) \subseteq \Big(\sum_{\tau_1 \le t_1, \dots, \tau_d \le t_d} \Delta_1^{\tau_1} \dots \Delta_d^{\tau_d} I \Big) M^{-1}.$$

Proof. The proof ot this Lemma is done by induction on $T = t_1+\dots+t_d$. For $T = 1$ and integers i with $1 \le i \le d$ we obtain

$$\Delta_i(q/m) = (m\,\Delta_i(q) - q\Delta_i(m)/m^2$$

for elements q in I and m in M. This is an element of $(I + \Delta_i I)M^{-1}$ and we have proved the required assertion. We may therefore assume that the assertion is already proved for T. Applying to the corresponding relation the derivation Δ_i for $1 \le i \le d$ we obtain

$$\Delta_i(\Delta_1^{t_1} \dots \Delta_d^{t_d} (IM^{-1}) \subseteq \Delta_i\Big(\sum_{\tau_1 \le t_1, \dots, \tau_d \le t_d} \Delta_1^{\tau_1} \dots \Delta_d^{\tau_d} I \Big) M^{-1}.$$

Now we recall that the derivations Δ_i and Δ_j commute for $1 \le i,j \le d$ and therefore the right hand side lies in

$$\Big(\sum_{\tau_1 \le t_1, \dots, \tau_i \le t_i+1, \dots, \tau_d \le t_d} \Delta_1^{\tau_1} \dots \Delta_d^{\tau_d} I \Big) M^{-1}.$$

From this the assertion of the Lemma follows immediately and concludes the proof of the Lemma.

Lemma 3. Let $\mathfrak{P}$ be a prime ideal in $K[G]$ of rank $1 \le r \le n$ and $\mathfrak{Q}$ a primary ideal of length ℓ with associated prime $\mathfrak{P}$. Suppose $\rho_r > 0$ and let T be an integer with

$$\binom{T+\rho_r}{\rho_r} \geq \ell + 1 .$$

Then there exist non-negative integers $t_1,\ldots,t_d$ with $t_1+\ldots+t_d \leq T$ and

$$\Delta_1^{t_1} \ldots \Delta_d^{t_d} \mathfrak{Q} \not\subseteq \mathfrak{P} .$$

Proof. We shall prove the Lemma by contradiction.and assume that the conclusion of the Lemma is false. Then it is an immediate consequence of Lemma 2 that for any multiplicative set M in $K[G]$ we have

$$\Delta_1^{t_1} \ldots \Delta_d^{t_d} \mathfrak{Q} M^{-1} \subset \mathfrak{P} M^{-1}$$

for all non-negative integers $t_1,\ldots,t_d$ with $t_1+\ldots+t_d \leq T$. Therefore we are completely free in localizing with respect to suitable multiplicative sets.

The set of simple points on the variety V in G belonging to $\mathfrak{P}$ is a non-empty Zariski open set. There we choose a generic point g. Then let M be the multiplicative set in $K[G]$ consisting of those functions that do not vanish in g. By Lemma 1 we find elements $P_1,\ldots,P_r$ in $K[G]$ such that

$$\mathfrak{P} M^{-1} = (P_1,\ldots,P_r) M^{-1} .$$

Let $Q_1,\ldots,Q_\ell$ be a basis of the ideal $\mathfrak{P}$ and $\rho \geq \rho_r$ be the rank over $K(V)$ of the Jacobian matrix $J(Q_1,\ldots,Q_\ell;\mathfrak{D}(A))$. Since we have

$$(Q_1,\ldots,Q_\ell)M^{-1} = (P_1,\ldots,P_r)M^{-1}$$

the rank over $K(V)$ of this matrix is the same as the rank over $K(V)$ of the matrix

$$\begin{bmatrix} \Delta_1 P_1 \pmod{P M^{-1}} & \dots & \Delta_d P_1 \pmod{P M^{-1}} \\ \vdots & & \vdots \\ \Delta_1 P_r \pmod{P M^{-1}} & \dots & \Delta_d P_r \pmod{P M^{-1}} \end{bmatrix}$$

Here we have used the fact that the rings $K[V]$ and $K[G]M^{-1}/P M^{-1}$ have the same quotient field. It follows that $\rho \leq r$ and we may assume without loss of generality that the determinant

$$\det \begin{bmatrix} \Delta_1 P_1 & \dots & \Delta_\rho P_1 \\ \vdots & & \vdots \\ \Delta_1 P_\rho & \dots & \Delta_\rho P_\rho \end{bmatrix}$$

does not vanish at g. Let $D = D(P_1,\dots,P_\rho)$ be this determinant. Then D is the multplicative set M. It follows that we may solve for all integers k with $1 \leq k \leq \rho$ the system of linear equationes

$$\delta_{k,\ell} = \alpha_{k,1} \Delta_\ell P_1 + \dots + \alpha_{k,\rho} \Delta_\ell P_\rho$$

for $1 \leq \ell \leq \rho$ in elements $\alpha_{k,j}$ in $K[G]M^{-1}$ for $1 \leq k,\ell \leq \rho$. For integers k with $1 \leq k \leq \rho$ we define elements Q_k by

$$Q_k = \alpha_{k,1} P_1 + \dots + \alpha_{k,\rho} P_\rho \ .$$

Then we have

$$P M^{-1} = (Q_1,\dots,Q_\rho,P_{\rho+1},\dots,P_r)M^{-1}$$

since the determinant of the matrix $(\alpha_{j,k})$ is equal to P^{-1} and this is contained in M^{-1}. It follows that

$$\Delta_\ell Q_k = \delta_{\ell,k} \pmod{P M^{-1}}$$

for $1 \leq k,\ell \leq \rho$. Therefore we may assume from now on without loss of generality that

$$\Delta_k P_\ell = \delta_{k,\ell} \pmod{P S^{-1}} \tag{7}$$

for every multiplicative set S of $K[G]$ that contains M and for all k,ℓ with $1 \leq k,\ell \leq \rho$. We use this in order to show that for all non-negative integers $\ell_1,\ldots,\ell_\rho,t_1,\ldots,t_\rho$ with $L = \ell_1+\ldots+\ell_\rho \leq t_1+\ldots+t_\rho = T$ we have

$$(8)\qquad \frac{1}{\ell_1!\ldots\ell_\rho!}\ \Delta_1^{\ell_1}\ldots\Delta_\rho^{\ell_\rho}\,(P_1^{t_1}\ldots P_\rho^{t_\rho}) \equiv \binom{t_1}{\ell_1}\ldots\binom{t_\rho}{\ell_\rho}\,P_1^{t_1-\ell_1}\ldots P_\rho^{t_\rho-\ell_\rho}$$

$$(\mathrm{mod}(\mathfrak{P}\,S^{-1})^{T-L+1})\ .$$

This is shown by induction on L. For $L = 0$ this is clear. Therefore we may assume that this is true for $L < T$. If we apply Δ_i for $1 \leq i \leq \rho$ to (8) we obtain

$$\frac{1}{\ell_1!\ldots\ell_\rho!}\ \Delta_1^{\ell_1}\ldots\Delta_i^{\ell_i+1}\ldots\Delta_\rho^{\ell_\rho}\,(P_1^{t_1}\ldots P_\rho^{t_\rho}) \equiv$$

$$\binom{t_1}{\ell_1}\ldots\binom{t_\rho}{\ell_\rho}\,\Delta_i\,(P_1^{t_1-\ell_1}\ldots P_\rho^{t_\rho-\ell_\rho})\quad(\mathrm{mod}(\mathfrak{P}\,S^{-1})^{T-L}$$

since Δ_i and Δ_j commute for $1 \leq i,j \leq d$. Furthermore we have for $1 \leq i,j \leq \rho$ for non-negative integers k either $\Delta_i P_j^{\,k} \equiv P_j^{\,k}\Delta_i\ (\mathrm{mod}(\mathfrak{P}\,S^{-1})^k)$ for $i \neq j$ or $\Delta_i P_i^{\,k} \equiv k\,P_i^{k-1}\ (\mathrm{mod}(\mathfrak{P}\,S^{-1})^k)$.

Now we may assume that $\ell_1 \leq t_1,\ldots,\ell_\rho \leq t_\rho$, since otherwise the right hand side of (8) is zero. Therefore it follows that

$$\Delta_i P_1^{t_1-\ell_1}\ldots P_\rho^{t_\rho-\ell_\rho} \equiv (t_i-\ell_i)\,P_1^{t_1-\ell_1}\ldots P_i^{t_i-\ell_i-1}\ldots P_\rho^{t_\rho-\ell_\rho}$$

modulo $(\mathfrak{P}\,S^{-1})^{T-L}$. If we put this together we obtain (8) with L replaced by $L+1$ and this concludes the inductive step.

We now choose the multiplicative set S as $K[G]-\mathfrak{P}$. By definition the length of the primary ideal $\mathfrak{Q}$ is equal to the length of the primary ideal $\mathfrak{Q}\,S^{-1}$ in $K[G]S^{-1}$. In order to compute this we define for non-negative

integers i the ideals $\mathfrak{Q}_i = (\mathfrak{Q}, P^i)$ with $P^i = K[G]$ for $i = 0$. Then $\mathfrak{Q}_0 = K[G]$ and

$$P S^{-1} = \mathfrak{Q}_1 S^{-1} \supset \ldots \supset \mathfrak{Q}_{T+1} S^{-1} \supset \mathfrak{Q} S^{-1}$$

is a descending chain of primary ideals in $K[G]S^{-1}$. The length of $\mathfrak{Q} S^{-1}$ is then at least equal to the length of $\mathfrak{Q}_{T+1} S^{-1}$ and this is equal to the sum of the lengths of the modules

$$M_i = \mathfrak{Q}_i S^{-1} / \mathfrak{Q}_{i+1} S^{-1} \qquad (i = 0, \ldots, T)$$

over the ring $K[G]S^{-1}$ (see [21]). For each i with $0 \leq i \leq T$ the maximal prime ideal $P S^{-1}$ annilitates the module M_i. Therefore we may regard the modules M_i as vectorspaces over the residue class field $F = K[G]S^{-1} / PS^{-1}$. The length of M_i is then equal to the dimension of the vector space M_i over the field F. We shall show that this dimension is at least equal to $\binom{i+\rho-1}{\rho-1}$. Then we obtain for the length $\ell(\mathfrak{Q})$ of $\mathfrak{Q}$ the estimate

$$\ell(\mathfrak{Q}) \geq \sum_{i=0}^{T} \dim(M_i) \geq \sum_{i=0}^{T} \binom{i+\rho-1}{\rho-1}$$

and this gives $\ell(\mathfrak{Q}) \geq \binom{T+\rho}{\rho}$. But the last inequalities contradict the hypothesis. It remains to verify that the dimension of M_i is at least equal to the number $\binom{i+\rho-1}{\rho-1}$. In order to verify this lower bound for the dimension of the vector space M_i over F we shall show that the monomials

$$P_1^{i_1} \ldots P_\rho^{i_\rho} \qquad (i = i_1 + \ldots + i_\rho, i_1, \ldots, i_\rho \geq 0)$$

in $P_1, \ldots, P_\rho$ are linearly independent modulo $\mathfrak{Q}_{i+1} S^{-1}$ over the field F. Then the dimension over F of the vectorspace M_i under consideration is at least equal to the number of these monomials. The number of such

monomials is equal to $\binom{i+\rho-1}{\rho-1}$ and from this the desired estimates follow. In order to verify the linear independence modulo $\mathfrak{Q}_{i+1}S^{-1}$ of these monomials over the field F let $Q(Y_1,\ldots,Y_\rho)$ be a homogenous polynomial of degree i with coefficients in $K[G]S^{-1}$ in the variables $Y_1,\ldots,Y_\rho$. If we have

$$Q(P_1,\ldots,P_\rho) \in \mathfrak{Q}_{i+1}\, S^{-1} ,$$

then we obtain for arbitrary non-negative integers $i_1,\ldots, i_\rho$ with $i = i_1+\ldots+ i_\rho$

$$\Delta_1^{i_1} \ldots \Delta_\rho^{i_\rho}\ Q(P_1,\ldots,P_\rho) \in \Delta_1^{i_1} \ldots \Delta_\rho^{i_\rho}\, \mathfrak{Q}_{i+1}\, S^{-1} .$$

Since we have assumed at the beginning of the proof of this lemma that.

$$\Delta_1^{j_1} \ldots \Delta_\rho^{j_\rho}\, \mathfrak{Q} \subseteq \mathfrak{P}$$

for non-negative integers $j_1, \ldots,j_\rho$ with $j_1+\ldots+j_\varphi \leq T$ and since for non-negative integers $j_1,\ldots,j_\rho, \ell$ with $j = j_1 +\ldots+j_\rho \leq \ell$ we have

$$\Delta_1^{j_1} \ldots \Delta_\rho^{j_\rho}\ \mathfrak{P}^{\ell} \subseteq \mathfrak{P}^{\ell-j}$$

we obtain by the use of Lemma 2 the relation

$$(9) \qquad \Delta_1^{i_1} \ldots \Delta_\rho^{i_\rho}\ Q(P_1,\ldots, P_\rho) \equiv 0 \pmod{\mathfrak{P}\, S^{-1}} .$$

If $q_{i_1,\ldots,i_\rho}$ denotes the coefficient of the monomial $Y_1^{i_1}\ldots Y_\rho^{i_\rho}$ in Q then it follows from (8) and (9) that

$$q_{i_1,\ldots,i_\rho} \equiv 0 \pmod{\mathfrak{P}\, S^{-1}} .$$

Since we have chosen $i_1,\ldots,i_\rho$ arbitrarily with $i = i_1+\ldots+i_\rho$ we obtain from this that

$$Q(Y_1,\ldots,Y_\rho) \equiv 0 \qquad (\mathrm{mod}\ P\ S^{-1}) \quad .$$

This means that the monomials under consideration are indeed linearly independent modulo $Q_{i+1}\ S^{-1}$ over the field F. This proves Lemma 3.

4. Proof of the Main Theorem*. We shall show in this section how the Main Theorem* is deduced from the Main Theorem. Essentially one has to verify that the conditions (1)* and (2)* imply the conditions (1) and (2).

For positive integers m let be $\mathbb{Z}^m$ the usual additive group of elements $\sigma = (s_1,\ldots,s_m)$ for integers $s_1,..,s_m$, and for real non-negative S we denote by $\mathbb{Z}^m(S)$ the subset of $\mathbb{Z}^m$ with $0 \leq s_1,..,s_m \leq S$. Then the following Lemma was proved in [11].

Lemma 4. Suppose for some real $S \geq 0$ there is an equivalance relation on $\mathbb{Z}^m(S)$ with B equivalence classes, where $B \leq S^{m+1-q}$ for some integer q with $1 \leq q \leq m$. Then there are elements $\sigma_1, \sigma_1', \ldots, \sigma_q, \sigma_q'$ of $\mathbb{Z}^m(S)$ such that σ_i is equivalent to σ_i' for $1 \leq i \leq q$ and the differences $\sigma_1 - \sigma_1', \ldots, \sigma_q - \sigma_q'$ are linearly independent.

We define now $\Omega^* = \Gamma(S/n)$ and $\Omega = \Gamma(S)$. Then we want to apply the Main Theorem. For this we need the following result.

Lemma 5. For $1 \leq r \leq n$ we have $\ell_r(\Omega^*) > (S/n)^{qr}$.

Proof. We assume that there is some r with $1 \leq r \leq n$ such that $\ell_r \leq (S/n)^{qr}$. Let V be an irreducible subvariety of G of codimension r such that $\ell_r = \ell(V)$. We have a corresponding disjoint union $\Omega^* = \Omega_1^* \cup \ldots \cup \Omega_{\ell(V)}^*$ of Ω^* as described in section 1. We recall that for $1 \leq i \leq \ell(V)$ we have $\Omega_i^* = (S(V) + \gamma_i) \cap \Omega^*$ for some γ_i in Ω^*. Next let $\Phi : \mathbb{Z}^m \to \Gamma$ be the homomorphism that maps the element $(s_1, \ldots, s_m)$ of $\mathbb{Z}^m$ into $s_1\gamma_1 + \ldots + s_m\gamma_m$. The homomorphism Φ gives us a covering of $\mathbb{Z}^m(S/n)$ by the sets $\Phi^{-1}(\Omega_i^*) \cap \mathbb{Z}^m(S/n)$ for $1 \leq i \leq \ell(V)$. These sets are pairwise disjoint since this is true for the sets Ω_i^* for $1 \leq c \leq \ell(V)$. They define on

$\mathbb{Z}^m(S/n)$ an equivalence relation with ℓ_r equivalence classes. Since we have $\ell_r \leq (S/n)^{m+1-q}$ for $q = m + 1 - q_r$ we obtain by Lemma 4 elements $\sigma_1, \sigma_1', \ldots, \sigma_q, \sigma_q'$ in $\mathbb{Z}^m(S/n)$ such that σ_i is equivalent to σ_i' for $1 \leq i \leq q$ and the difference $\sigma_1 - \sigma_1', \ldots, \sigma_q - \sigma_q'$ generate a subgroup Z of $\mathbb{Z}^m$ of rank q. Let Γ' be its image in Γ under Φ. Since the rank of the kernel of Φ is $m - \ell$ we get for the rank of Γ' the lower bound $q - m + \ell = \ell - q_r + 1$ and therefore the corank of Γ' in Γ is at most equal to $q_r - 1$. Since $\Gamma' \subseteq S(V)$, this contradicts the definition of q_r. If follow that we have indeed the inequality $\ell_r > (S/n)^{q_r}$ for $1 \leq r \leq n$.

From Lemma 5 it follows that the conditions (1) and (2) for $r < n$ are implied by the conditions (1)* and (2)*. It remains to show that the same holds for $r = n$. For this it is sufficient to show that $|\Omega_n| \geq |\Gamma(S/n)|$. Since we have $\Gamma(S/n) + (n - 1)\,\Gamma(S/n) \subseteq \Gamma(S)$ if follows that $\Omega_n \supseteq \Gamma(S/n)$ and the desired inequality follows immediately. This completes the proof that the Main Theorem implies the Main Theorem*.

5. The Proposition. In this section we shall state and prove a Projection. We shall show in the next section that it implies the Main Theorem. Let G, Ω,Ω^*,A and $P \notin I(G)$ be as in the Main Theorem. We recall that b is the degree of the operator $E(\gamma)$ and a the maximum of the degrees of the polynomials H_{ij} for $1 \leq i \leq n$ and $1 \leq j \leq N$ which appear in the system of partial differential equations (3). Furthermore we denote by $\deg(G)$ the degree of G and remind that the integers q_r for $1 \leq r \leq n$ are defined as in [13].

Then we put $T' = \min(T/n, cD), S' = S/n$, $D_1 = D$, $D_{r+1} = (r+1)ab^r \max(D,T')$ for $1 \leq r \leq n$ and $B_1 = D_1 \ldots D_r \deg(G)$ for $1 \leq r \leq n$. In particular we have the inequalities

$$B_{r+1} \leq \frac{c}{(r+1)!} D \max(D,T')^r$$

if the constant c in the Main Theorem is chosen as

$$c = (n!)^2 (ab^n)^n \deg(G) .$$

We shall prove the Main Theorem by contradiction and assume that the conclustion of the Main Theorem is false. We choose the embedding of the group variety G in such a way that the homogenous coordinate X_0 satisfies $X_0(\gamma) \neq 0$ for all γ in Σ. This implies that the differential operators $\partial_1, \ldots, \partial_n$ and the order are defined for all γ in $\Gamma(S)$.

We shall show in section 7 that for all integers r with $1 \leq r \leq n$ we have

$$(10) \qquad \tau_r = \rho_r \qquad (1 \leq r \leq n)$$

and therefore we may replace the integers τ_r by the integers ρ_r.

For a homogenous ideal I in $K[X_0,\ldots,X_N]$ we define the order of I at the

point g of G with $X_0(g) \neq 0$ to be the minimum of the orders of elements of I in the point g. The *-operator in the subsequent proposition is defined as in [13] with respect to Σ .

Proposition. For every integer r with $1 \leq r \leq n$ there exist homogenous polynomials $P_1,\ldots,P_r$ of degrees at most $D_1,\ldots,D_r$ respectively such that the following holds. The ideal $I_r = (I(G),P_1,\ldots,P_r)$ vanishes on Ω_r to order at least equal to $\frac{n-r+1}{n} T$. Furthermore

(i) the rank of I_r^* is equal to $N-n+r$,

(ii) the degree of I_r^* is at most equal to B_r .

Proof. We shall prove the Proposition by induction on r and point out again that the proof is carried out along the same lines as the proof of the corresponding Proposition in section 6 of [13]. The only and essential difference consists in the fact that we shall take also multiplicities into account. This is also done in [14] but there we have only multiplicities in one direction and the methods of [6] are applicable in this situation. This is no longer the case in the present situtation and our approach is based on the results of section 3 accompanied by the results of section 7. In the proof of the Proposition we shall therefore work out those details only in which it differs from the corresponding Proposition in [13].

As it is shown in section 4 of [13] there exist homogenous polynomials $Q_1,\ldots,Q_h$ for $h = N-n$ such that the ideal $I(G)$ of G can be written simultanously as a complete intersection locally in Γ. In other words we have

$$(Q_1,\ldots,Q_h)^* = I(G) .$$

Since we did not care in [13] about the field of definition for $Q_1,\ldots,Q_h$

we should make a short remark about it at this place. Since the ideal $I(G)$ and Γ are defined over a field L that is finitely generated over the rationals the proof of Lemma 6 in [13] can be copied using the remark at the end of section 1 instead of the remark at the end of section 1 of [13]. From this we deduce that indeed the polynomials $Q_1, \ldots, Q_h$ can be defined over K.

We begin the proof of the Proposition with the case $r = 1$. The case $h = 0$ is treated in the same way as in the Proposition of [13] in section 6 using the polynomial $P_1(X_0,\ldots,X_N) = P(X_0,\ldots,X_N)$. The same is done in the case $h > 0$ where we only have to note that we have $(I(G),P_1)^* = (Q_1,\ldots,Q_h,P_1)^*$.

Now we assume that the Proposition is proved for integers r with $1 \leq r < n$ and we proceed to do the inductive step from r to $r + 1$. For this we start with the construction of an appropriate polynomial P_{r+1}. First of all we remark that

$$I_r^* = (Q_1,\ldots,Q_h,P_1,\ldots,P_r)^* \quad .$$

Since the rank of I_r^* is equal to $N+r-n$ the ideal I_r^* has to be unmixed because of Lemma 7 of [13]. For a homogenous ideal I in $K[X_0,\ldots,X_N]$ we denote by I' the corresponding dehomogenized ideal in $K[x_1,\ldots,x_N]$. We recall once more that we denoted by p the canonical projrction from $K[x_1,\ldots,x_N]$ onto $K[G]$.

Let $\mathfrak{Q}$ be a primary component of I_r^*. Then we distinguish two different cases. Either there exist non-negative integers $t_1,\ldots,t_d$ with $t_1+\ldots+t_d \leq T'$ such that

$$(11) \qquad \Delta_1^{t_1} \cdots \Delta_d^{t_d} \, \mathfrak{Q}' \not\subseteq \mathfrak{P}' \, ,$$

where $\mathfrak{P}'$ denotes the radical of $\mathfrak{Q}'$. Or for all non-negative integers

$t_1, \ldots, t_d$ with $t_1 + \ldots + t_d \leq T'$ we have

(12) $\qquad \Delta_1^{t_1} \ldots \Delta_d^{t_d} \mathfrak{Q}' \subseteq \mathfrak{P}'.$

Since $\mathfrak{P}$ is a component of I_r^* it vanishes for some γ in Σ. Since furthermore $X_0(\gamma) \neq 0$ the dehomogenized prime ideal $\mathfrak{P}'$ vanishes at γ. We continue to prove that the length of a primary ideal $\mathfrak{Q}'$ that satisfies (12) is at least equal to $\binom{T'+\rho}{\rho}$ where we have put $\rho = \rho_r$ for the sake of shortness.

In order to see this we note first that the length of $\mathfrak{Q}$ is equal to the length of $\mathfrak{Q}'$. Furthermore it is clear that we may replace in (12) the ideals $\mathfrak{P}'$ and $\mathfrak{Q}'$ by the ideals $\mathfrak{p}(\mathfrak{P}')$ and $\mathfrak{p}(\mathfrak{Q}')$ and we note that the length of $\mathfrak{p}(\mathfrak{Q}')$ is the same as the length of $\mathfrak{Q}'$. It suffices therefore to estimate the length of $\mathfrak{p}(\mathfrak{Q}')$. This is done by means of Lemma 3. Either we have $\rho > 0$ and then all the hypotheses of Lemma 3 are satisfied and the length of $\mathfrak{p}(\mathfrak{Q}')$, and then also that of $\mathfrak{Q}$ is at least equal to $\binom{T'+\rho}{\rho}$. Or we have $\rho = 0$ and we simply estimate the length of $\mathfrak{Q}$ by $1 = \binom{T'}{0}$.

It is a well-known fact (see [7] or [21]) that the sum of the lengths of the primary components of an unmixed ideal is at most equal to the degree of this ideal. The degree of I_r^* is at most equal to B_r. Therefore the number of those primary components that satisfy (12) is at most equal to $B_r \binom{T'+\rho}{\rho}^{-1}$.

We fix now an associated prime ideal $\mathfrak{P}$ of I_r^* and we proceed to show that there exist non-negative integers $t_1, \ldots, t_d$ with $t_1 + \ldots + t_d \leq T'$ and an element γ in Ω^* such that

(13) $\qquad \Delta_1^{t_1} \ldots \Delta_d^{t_d} (I_r^*)' \not\subseteq (\mathfrak{E}(-\gamma)\mathfrak{P})'.$

If this does not hold then for all γ in Ω^* and all non-negative integers $t_1,\ldots,t_d$ with $t_1+\ldots+t_d \leq T'$ we have

$$(14) \qquad \Delta_1^{t_1} \ldots \Delta_d^{t_d} (I_r^*)' \subseteq (E(-\gamma)\mathfrak{P})'.$$

For γ in Ω^* let M_γ be the multiplicative set $K[x_1,\ldots,x_N] \setminus (E(-\gamma)\mathfrak{P})'$ and $\mathfrak{Q}_\gamma$ be the primary component of I_r^* belonging to $E(-\gamma)\mathfrak{P}$. The latter is a component of I_r^* as follows from (14). Then we localize the relation (14) with respect to M_γ and obtain by use of Lemma 2 firstly

$$\Delta_1^{t_1} \ldots \Delta_d^{t_d} \mathfrak{Q}_\gamma' M_\gamma^{-1} \subseteq (E(-\gamma)\mathfrak{P})' M_\gamma^{-1}$$

and then a fortiori

$$(15) \qquad \Delta_1^{t_1} \ldots \Delta_d^{t_d} \mathfrak{Q}_\gamma' \subseteq (E(-\gamma)\mathfrak{P})'.$$

This is exactly the situation in (12) and the length of the primary ideal $\mathfrak{Q}_\gamma$ is therefore at least equal to $\binom{T'+\rho}{\rho}$. We conclude that for each γ in Ω^* the ideal $E(-\gamma)\mathfrak{P}$ is an associated prime ideal of I_r^* since both ideals have the same rank. Furthermore the corresponding primary component has length at least equal to $\binom{T'+\rho}{\rho}$

We define now an equivalence relation on the set Ω^* in the following way. Two elements γ and γ' are equivalent if and only if $E(-\gamma)\mathfrak{P} = E(-\gamma')\mathfrak{P}$ or equivalently $E(\gamma-\gamma')\mathfrak{P} = \mathfrak{P}$. This again is equivalent to the condition that $\gamma-\gamma'$ is in $S(V)$ where V is the variety of $\mathfrak{P}$ in G (see also [14]). This last condition is furthermore equivalent to the condition that γ is in $(S(V)+\gamma') \cap \Omega^*$. But this set is one of the sets Ω_i^* for $1 \leq i \leq \ell(V)$. Therefore this equivalence relation is the same as the equivalence relation given by the sets Ω_i^* for $1 \leq i \leq \ell(V)$. By the definition of the numbers ℓ_r we have $\ell(V) \geq \ell_r$. Hence the number of distinct prime ideals among the

prime ideals $E(-\gamma)\mathfrak{P}$ of I_r^* is at least equal to ℓ_r. It follows that the degree of I_r^* is at least equal to $\ell_r(T'+\rho)$. On the other hand it is at most equal to B_r . Hence we obtain the inquality (recall that $\rho=\rho_r \leq r$)

$$\ell_r T'^{\rho} < (cD)^r \ .$$

This contradicts (2) if $T' = cD$ and (1) if $T' = T/n$. We conclude that (14) cannot hold and this implies that (13) is true.

Now we can construct the polynomial P_{r+1} . The idea for the contruction of the polynomial P_{r+1} is the following. First we construct for each prime component of I_r^* a polynomial that does not lie in this component. Then by taking a suitable linear combination of these polynomials we shall obtain a homogenous polynomial P_{r+1} that does not lie in any of the prime components associated to I_r^* . Then we shall verify that the so constructed polynomial has the required properties.

We have seen that we can find an element γ in Ω^* and non-negative integers $t_1,\ldots,t_d$ with $t_1+\ldots+t_d \leq T$ and that (13) holds. Then at least one of the elements $P_1,\ldots,P_r$ which generate together with $I(G)$ the ideal I_r , say Q , must satisfy

$$(16) \qquad \Delta_1^{t_1} \ldots \Delta_d^{t_d} Q' \notin (E(-\gamma)\mathfrak{P})' \ .$$

Let Q_{h+r+1} be the homogenized left hand side of (16). If follows from (16) together with Lemma 3 in [13] that

$$(17) \qquad E(\gamma)Q_{h+r+1} \notin \mathfrak{P} \ .$$

Since the prime ideal $\mathfrak{P}$ was an arbitrary associated prime ideal of I_r^* this can be adieved for every associated prime ideal of I_r^* . In the same way as in [6], [11] or [13] we construct the polynomial P_{r+1} as a linear combination with coefficients in K of these polynomials

$E(\gamma)Q_{h+r+1}$ multiplied with a suitable power of a linear form. This linear form is chosen in such a way that its coefficients are in K and such that it does not vanish at any point of Γ. The existence of such a linear form follows from the remark at the end of section 1. We choose the powers smallest possible to make all the resulting polynomials homogenous of the same degree.

It remains to verify that the polynomial P_{r+1} has all the properties which are required in the proposition.

First of all it is easily seen that the degree of the polynomials $E(\gamma)Q_{h+r+1}$ is at most equal to $b(D_r + aT') \leq D_{r+1}$. Therefore we can take such a power of the linear form just mentioned that the degree of P_{r+1} is at most equal to D_{r+1}.

Secondly since the polynomials $E(\gamma)Q_{h+r+1}$ are obtained from the polynomials $P_1,\ldots,P_r$ by applying a differential operator of order at most T' and by translating by an element in Ω^* and since $P_1,..,P_r$ vanish Ω_r to order at least $\frac{n-r+1}{n}T$ it follows that the polynimials $E(\gamma)Q_{h+r+r}$ vanish on Ω_{r+1} to order at least $\frac{n-r}{n}T$. The same holds then for the polynomial P_{r+1}.

Finally Lemma 3 of [6] tells us that the rank or the ideal $I = (I_r^*, P_{r+1})$ is equal to $N + r + 1 - n$ and its degree is at most equal to $D_{r+1}B_r \leq B_{r+1}$. Since it is contained in $I_{r+1}^* = (I_r, P_{r+1})^*$ since the latter ideal possess a zero in G and is therefore not the whole ring $K[X_0,\ldots,X_N]$ the rank of I_{r+1}^* is at least equal to $N + r + 1 - n$ and at most equal to $N + r + 1 - n$ because of Lemma 7 in [13]. Hence its rank is equal to $N + r + 1 - n$. Furthermore its degree is at most equal to the degree of I since it contains this ideal and both have the same rank. It follows that the degree of I_{r+1}^* is at most equal to B_{r+1} and this proves the last assertion of the Proposition.

6. Proof of the Main Theorem. We are now prepared to deduce the Main Theorem very easily from the Proposition. But we point out that we do this under the hypothesis that we have $\rho_r = \tau_r$ for all integers r with $1 \leq r \leq n$. We shall show in the next section that this hypothesis is indeed true. Then the Main Theorem will be proved completely as it stands.

For the proof of the Main Theorem we put $r = n$ in the Proposition. We obtain then the ideal I_n^* whose degree can be estimated by

$$\deg I_n^* \leq B_n \leq \frac{c}{n!} D \max (T', D)^{n-1} \quad . \tag{18}$$

This ideal vanishes on Ω_n to order at least equal to T/n. By Lemma 3 the sum of the lengths of all primary components of I_n^* is strictly greater than $|\Omega_n|(T/n)^{\rho_n}/n!$. On the other hand this sum is equal to the degree of I_n^* which we have estimated in (18). Therefore we have the lower bound

$$\deg I_n^* > |\Omega_n|(T/n)^{\rho_n}/n! \tag{19}$$

for this degree.

Since by the definition of the number T' we have $T' \leq cD$ it follows that the right hand side of (18) is at most equal to $(cD)^n/n!$. Then together with (19) we obtain

$$|\Omega_n|(T/n)^{\rho_n} < (cD)^n \quad .$$

Since $\rho_n = \tau_n$ this inequality contradicts the hypothesis (1) for $r = n$ of the Main Theorem. This contradiction completes the proof of the Main Theorem.

7. Analytic subgroups and Jacobians. In this section we shall do some calculations concerning the exponents τ_r, σ_r and ρ_r. In the proof of the Main Theorem we had used the fact that for integers r with $1 \leq r \leq n$ we have $\rho_r = \tau_r$. This we shall verify now. The exponents τ_r as well as their analogues q_r cannot be calculated in practice directly from their definition. Therefore we have introduced the exponents σ_r. And these are very easily calculated in all known applications. We shall further show in this section that we have $\sigma = \tau$. This will give us the posibility of calculating the numbers τ_r in most cases explicitly and in all other case we obtain lower bounds.

In order to carry all this out we begin with recalling some basic facts from the theory of Lie-groups. For further details we refer to the books of Hochschild [8], Warner [19] and Narasimhan [16].

Let M be a complex manifold and $T(M)$ be the tangent bundle of M. As a set this is the disjoint union of all tangent spaces $T_m(M)$ where m runs through all points of M. For each m in M we define the cotangent space at m to be the dual space $T_m(M)^*$ of the tangent space $T_m(M)$ at m. In the same way as the tangent bundle is constructed one constructs the cotangent bundle $T^*(M)$. Let $z_1,\ldots,z_n$ be local coordinates for a neighbourhood of m in M where n is the dimension of M. Then a basis of $T_m(M)$ is given by the partial derivatives $(\frac{\partial}{\partial z_1})_m, \ldots, (\frac{\partial}{\partial z_n})_m$ in the point m. We further denote by $(dz_1)_m,\ldots,(dz_n)_m$ the dual basis in $T_m(M)^*$. Then we have by definition

$$< (\frac{\partial}{\partial z_i})_m , (dz_j)_m > = \delta_{ij} \quad (1 \leq i,j \leq n)$$

where δ_{ij} is the Kronecker symbol.

From now on let M be a group variety G and $\mathfrak{g}$ be the algebra of left invariant vectorfields on G. This is the Lie-algebra of G. This algebra possesses a basis given by $\frac{\partial}{\partial z_1}, \ldots, \frac{\partial}{\partial z_n}$. We denote by g^* the space of left invariant 1-forms. This space is generated by the 1-forms $dz_1, \ldots, dz_n$, the differentials of $z_1, \ldots, z_n$. It is well-known that g is isomorphic to $T_0(G)$, the tangent space of G at the neutral element of the group G.

Let now Y be an irreducible subvariety of the group G codimension r. This means that its dimension is equal to $n-r$. Then we may assume without loss of generality that V is not contained in the hyperplane section of G defined by $X_0 = 0$. Then let $P_1, \ldots, P_\ell$ be a set of generators for the ideal $I(V)$ in $K[G]$ of elements that vanish on V. Let $\Phi_1, \ldots, \Phi_\ell$ be the corresponding functions on the tangent space $T_0(G)$. This means that

$$\Phi_i = P_i \cdot \exp_G \qquad (1 \leq i \leq \ell).$$

Here $\exp_G$ denotes the exponential map of G which was introduced at the beginning of section 1. Then the functions Φ_i are functions of the coordinates $z_1, \ldots, z_n$ of $T_0(G)$ and we can write them as $\Phi_i = \Phi_i(z_1, \ldots, z_n)$ for $1 \leq i \leq \ell$.

We consider now the analytic subgroup A of G of dimension d. Then with the notations of section 1 the subgroup A is defined in the tangent space $T_0(G)$ by the vanishing of the linear forms $M_1(z_1, \ldots, z_n), \ldots M_{n-d}(z_1, \ldots, z_n)$. These linear forms have rank $n - d$ and therefore the associated differential forms $dM_1, \ldots, dM_{n-d}$ have rank $n - d$ at every point of $T_0(G)$.

We denote by R the ring of functions on $T_0(G)$ of the form $f \circ \exp_G$ where f is any element of $K[G]$. In other words it is just $\exp_G^*(K[G])$. Then we define the R-modul $M(V)$ as

$$M(V) = Rd\Phi_1 + \ldots + Rd\Phi_\ell + RdM_1 + \ldots + RdM_{n-d}$$

and let $\overline{M(V)}$ be defined by

$$\overline{M(V)} = M(V) \pmod{\exp_G^*(I(V))} \quad .$$

Finally we let $m(V)$ be the restriction of $M(V)$ to $\exp_G^{-1}(V)$. The module $m(V)$ is generated by the restrictions $\omega_1,\ldots,\omega_{n-d}$ of $dM_1,\ldots,dM_{n-d}$ to $\exp_G^{-1}(V)$ since the restrictions of $d\Phi_1,\ldots,d\Phi_\ell$ all vanish on V.

Now we put

$$\frac{\partial}{\partial \zeta_i} = \ell_{1i} \frac{\partial}{\partial z_1} + \ldots + \ell_{ni} \frac{\partial}{\partial z_n} \qquad (1 \leq i \leq d)$$

(see section 2). These are invariant vector fields belonging to the analytic subgroup A and correspond to the derivations $\Delta_1,\ldots,\Delta_d$ of section 2.

Without loss of generality we may assume that a basis of $\mathfrak{g}$ is given by $\frac{\partial}{\partial \zeta_1}, \ldots, \frac{\partial}{\partial \zeta_d}$ together with $\frac{\partial}{\partial z_{d+1}},\ldots,\frac{\partial}{\partial z_n}$.

Lemma 6. We have

$$\operatorname{rank}(J(P_1,\ldots,P_\ell;\mathcal{D}(A)) = d - n + \operatorname{rank} \overline{M(V)} \quad .$$

Proof. The rank of $\overline{M(V)}$ is equal to the rank of the Jacobian matrix with respect to an arbitrary basis of $\mathfrak{g}$ of the functions $\Phi_1,\ldots,\Phi_\ell$ and $M_1,\ldots,M_{n-d}$ where the entries are taken modulo $\exp_G^*(I(V))$ respectively. By the definition of the linear forms M_j we have

$$\frac{\partial}{\partial \zeta_i} M_j = 0 \qquad (1 \leq i \leq d; 0 \leq j \leq n-d)$$

(see section 1). Hence the Jacobian matrix in question has the form

$$\begin{bmatrix} \frac{\partial}{\partial\zeta_1}\Phi_1 & \cdots & \frac{\partial}{\partial\zeta_d}\Phi_1 & \frac{\partial}{\partial z_{d+1}}\Phi_1 & \cdots & \frac{\partial}{\partial z_n}\Phi_1 \\ \vdots & & \vdots & \vdots & & \vdots \\ \frac{\partial}{\partial\zeta_1}\Phi_\ell & \cdots & \frac{\partial}{\partial\zeta_d}\Phi_1 & \frac{\partial}{\partial z_{d+1}}\Phi_\ell & \cdots & \frac{\partial}{\partial z_n}\Phi_\ell \\ 0 & \cdots & 0 & \frac{\partial}{\partial z_{d+1}}M_1 & \cdots & \frac{\partial}{\partial z_n}M_1 \\ \vdots & & \vdots & \vdots & & \vdots \\ 0 & \cdots & 0 & \frac{\partial}{\partial z_{d+1}}M_{n-d} & \cdots & \frac{\partial}{\partial z_n}M_{n-d} \end{bmatrix}$$

and every entry has to be taken modulo $\exp_G^*(I(V))$. The rank of this matrix is obviously equal to

$$n + d \qquad \text{rank} \begin{bmatrix} \frac{\partial}{\partial\zeta_1}\Phi_1 & \cdots & \frac{\partial}{\partial\zeta_d}\Phi_1 \\ \vdots & & \vdots \\ \frac{\partial}{\partial\zeta_1}\Phi_\ell & \cdots & \frac{\partial}{\partial\zeta_d}\Phi_\ell \end{bmatrix} .$$

Here again the matrix has to be taken modulo $\exp_G^*(I(V))$. Since the rings R and $K[G]$ are isomorphic and since the derivations $\frac{\partial}{\partial\zeta_i}$ and Δ_i correspond under this isomorphism for $1 \le i \le d$ the rank of this matrix is equal to

$$\text{rank } (J(P_1,\ldots,P_\ell;\mathcal{D}(A))$$

such that we finally obtain

$$\text{rank } \overline{M(V)} = n - d + \text{rank } J(P_1,\ldots,P_\ell;\mathcal{D}(A))$$

is claimed. This proves the Lemma.

We use this Lemma to fill the last gap in the proof of the Main Theorem. This is the following Proposition.

Proposition 1. For every integer r with $1 \leq r \leq n$ we have $\tau_r = \rho_r$. In particular we have $\tau(A;G)_K = \rho(A;G)_K$.

Proof. Let V be an irreducible algebraic subvariety of G of codimension r and defined over K such that $A \cap V$ is non-empty. Then we have

$$\operatorname{cod} A \cap V \geq \operatorname{rank} M(V)$$

as can be easily verified. Furthermore we obviously have

$$\operatorname{rank} M(V) \geq \operatorname{rank} \overline{M(V)} ,$$

$$\operatorname{cod} A \cap V = n - d + \tau(V)$$

and since by Lemma 6 we have

$$\operatorname{rank} \overline{M(V)} = n - d + \rho(V)$$

we obtain

$$n - d + \tau(V) = \operatorname{cod} A \cap V \geq \operatorname{rank} \overline{M(V)} = n - d + \rho(V) .$$

From this we obtain

$$\rho(V) \leq \tau(V) .$$

In order to show the opposite inequality let $\rho' \leq n - d + r$ be the rank of $\overline{M(V)}$. Without loss of generality we may assume that $d\Phi_1, \ldots, d\Phi_r$ are linearly independent modulo $\exp_G^*(I(V))$.

Then there exist linear forms

$$L_j(X_1,\ldots,X_{n-d},Y_1,\ldots,Y_r) \qquad (1 \leq j \leq n-d+r-\rho')$$

with coefficients in R which are linearly independent modulo $\exp_G^*(I(V))$ such that

$$L_j(dM_1,\ldots,dM_{n-d},d\Phi_1,\ldots,d\Phi_r) \equiv 0 \qquad (\text{modulo } \exp_G^*(I(V)))$$

for $1 \leq j \leq n-d+r-\rho'$. Consider the quotient field L of the ring $S = \exp_G^*(K[G])/\exp_G^*(I(V))$. This is a K-module and we denote by $\Omega^1_{L/K}$ its associated module of relative differentials. Then we look at the images ξ_j of $L_j(dM_1,\ldots,d\Phi_r)$ in $\Omega^1_{L/K}$. Since the images of $d\Phi_1,\ldots, d\Phi_r$ are zero we can write

$$\xi_j = \lambda_j(\omega_1,\ldots,\omega_{n-d}) = 0 \qquad (1 \leq j \leq n-d+r-\rho')$$

for linear forms $\lambda_j(X_1,\ldots,X_{n-d})$ in the polynomial ring $L[X_1,\ldots,X_{n-d}]$ which are linearly independent. The same arguments as in the proof of Theorem 1 in [1] show that the linear forms $\lambda_1,\ldots,\lambda_{n-d+r-\rho'}$ have already coefficients in K and therefore

$$\lambda_1(dM_1,\ldots,dM_{n-d}),\ldots,\lambda_{n-d+r-\rho'}(dM_1,\ldots,dM_{n-d})$$

are linearly independent invariant holomorphic differential forms on $T(G)$ which are completely integrable (see again [1], loc. cit.). Therefore there exists an unique maximal integral manifold B through the neutral element 0 in G . This is an analytic subgroup of codimension $n-d+r-\rho'$ that satisfies $B \supset A$ and $B \supset V$ .We choose an analytic subgroup $C \supset A$ such that $A = B \cap C$ and the codimension of C is equal to $\rho' - r$. If follows that

$$\operatorname{cod} A \cap V = \operatorname{cod} C \cap V \leq \rho' .$$

On the other hand

$$\operatorname{cod} A \cap V = \operatorname{cod}_A A \cap V + \operatorname{cod} A = \tau(V) + n - d.$$

This gives

$$\tau(V) \leq \rho' + d - n \ .$$

We use now that Lemma 6 asserts that $\rho' = n - d + \rho(V)$ to deduce that

$$\tau(V) \leq \rho(V) \ .$$

Hence we have proved that $\tau(V) = \rho(V)$. If we take the minimum we obtain $\tau_r = \rho_r$ for $1 \leq r \leq n$ and this finishes the proof of the Proposition.

We end this section with the proof of the already announced equality of the exponents $\sigma(A;G)_K$ and $\tau(A;G)_K$.

Lemma 8. We have $\sigma(A;G)_K = \tau(A;G)_K$.

Proof. Since we trivially have $\tau_r \leq \sigma_r$ we obtain $\tau \leq \sigma$. Hence it remains to prove the opposite inequality. For this we choose r in such a way that $\tau = \tau_r/r$. Then we find an algebraic subvariety V of G of codimension r with $\operatorname{cod}_A V \cap A = \tau_r$. Let $\tilde{K}$ be a component of $V \cap A$ in an open subset (in the complex topology) of G with $\operatorname{cod}_A \tilde{K} = \tau_r$ and W the Zariski-closure of $\tilde{K}$. We may assume without loss of generality that W is equal to V . Then by [1],Theorem 1, there exists an analytic subgroup B of G with the following properties: B contains A and V and the codimension satisfies

$$\operatorname{cod} B \geq \operatorname{cod} A + \operatorname{cod} V - \operatorname{cod} \tilde{K} \ .$$

Since $\operatorname{cod}_A \tilde{K} + \operatorname{cod} A = \operatorname{cod} \tilde{K}$ we obtain the lower bound

$$\operatorname{cod} B \geq r - \tau_r$$

for the codimension of B. As in the proof of Proposition 1 we may further assume without loss of generality that the neutral element 0 of G is

contained in V. Let H be the algebraic subgroup of G generated by V. Then H is contained in B (see [1] or [5], Chap. I, § 2). We denote by r' the codimension of H. The subgroups A and B are defined by linear equations in the tangent space. Hence we can find an analytic subgroup C of G such that $A = B \cap C$ and $\operatorname{cod} A = \operatorname{cod} B + \operatorname{cod} C$. Since B contains the algebraic subgroup H we obtain $H \cap A = H \cap C$. It follows that

$$\operatorname{cod} H \cap A = \operatorname{cod} H \cap C \leq \operatorname{cod} H + \operatorname{cod} C.$$

If we express the codimension of C in terms of the codimensions of A and B and notice that

$$\operatorname{cod} H \cap A = \operatorname{cod}_A H \cap A + \operatorname{cod} A$$

we obtain

$$\operatorname{cod}_A H \cap A \leq \operatorname{cod} H - \operatorname{cod} B.$$

The left hand side of this inequality is at least equal to $\sigma_{r'}$ and the right hand side at most equal to $r' - r + \tau_r$. Hence we obtain

$$\sigma_{r'} + r - r' \leq \tau_r .$$

If $r' \neq 0$ we conclude that

$$\sigma \leq \sigma_{r'}/r' \leq \tau_r/r = \tau .$$

If $r' = 0$ it follows directly that $\tau \geq 1$. On the other hand we have $\tau \leq d/n$ and thus $\tau = d/n$. This implies that $d = n$ and together with $\sigma \geq \tau$ and $\sigma \leq d/n$ we conclude that $\sigma = \tau = 1$. This proves Lemma 8 completely

8. Baker's method. In this section we shall give an application of the Main Theorem in the context of Baker's method. In his famous series of papers Baker proved among others the following result (for a survey of these results we refer to [2] or [3]). Let $\alpha_1, \ldots, \alpha_n$ be algebraic numbers such that their logarithms in some determination are $\mathbb{Q}$-linearly independent. Then Baker's Theorem in its qualitative version says that these logarithms are then also $\overline{\mathbb{Q}}$-linearly independent.

The elliptic analogue of this is the following problem. Let E be an elliptic curve defined over the field $\overline{\mathbb{Q}}$ and let $\operatorname{End} E$ be the ring of endomorphisms of E and put $K = (\operatorname{End} E) \otimes \mathbb{Q}$. Then it is a well-known fact that K is either the field $\mathbb{Q}$ or an imaginary quadratic extension of $\mathbb{Q}$. In the latter case we say that E possesses complex multiplication. The exponential map of the complex Lie group E can be explicitly given by use of the Weierstraß elliptic function $\wp(z)$.

Let $u_1, \ldots, u_n$ be complex numbers such that for all i with $1 \leq i \leq n$ the number $\wp(u_i)$ are defined and algebraic. Such numbers u_i are often called elliptic logarithms. Then we suppose that these numbers are linearly independent over K. Then D.W. Masser proved in his thesis [10] that under the hypothesis of complex multiplication these numbers are also $\overline{\mathbb{Q}}$-linearly independent. For the proof of this Masser used Baker's method. The extension of Masser's result to the case when E does not possess complex multiplication was a difficult open problem. It was solved recently by D. Bertrand and D.W. Masser [4] in a very surprising way. They showed that this was a consequence of an old criterion of Schneider generalized by Lang. D.W. Masser [12] has recently used this method to give an alternative proof of Baker's Theorem above.

The disadvantage of this method is that it does not provide reasonable lower bounds for linear forms. So the only way to obtain good lower bounds seems to

be Baker's method.

This can now be done with the help of the Main Theorem of this paper. In this section we want to give an example of our results in the connection with this problem.

Let $\mathbb{G}$ be either the multiplicative group of complex numbers, also denoted by $\mathbb{G}_m$, or an elliptic curve E defined over $\overline{\mathbb{Q}}$. Then let G be the product $\mathbb{G}^n$ and $\exp : T(G) \longrightarrow G$ the exponential map from the tangent space $T(G)$ at the neutral element of G into G. We identify from now on the complex vector space $T(G)$ with $\mathbb{C}^n$. Let $u = (u_1, \ldots, u_n)$ be in $T(G)$ such that $\exp(u)$ is an algebraic point of G and hence lies in $G(\overline{\mathbb{Q}})$. We assume that the components $u_1, \ldots, u_n$ of u are linearly independent over $K := (\mathrm{End}\ \mathbb{G}) \otimes \mathbb{Q}$. Then it follows from the results of Baker, Masser and Bertrand and Masser that the numbers $u_1, \ldots, u_n$ are also linearly independent over $K \otimes \overline{\mathbb{Q}}$. In order to prove this result by Baker's method one needs the following zero estimate.

Let A be the analytic subgroup of G of codimension 1 defined in the tangent space $T(G)$ by the linear form

$$L = \beta_1 z_1 + \ldots + \beta_{n-1} z_{n-1} + z_n = 0 .$$

We assume that the coefficients $1, \beta_1, \ldots, \beta_{n-1}$ are algebraic numbers which are linearly independent over K. In order to obtain the simplest version of a classical zero estimate we suppose further that the point $\exp(u)$ has infinite order. We deonte by Γ the subgroup of G generated by this point. As usual we embed the algebraic group G into some projective space $\mathbb{P}^N$. Then one obtains the following result.

Theorem. There exists a positive constant c depending only on G with the following property. For real numbers $S \geq 0$, $D \geq 0$ and $T \geq 1$ with $T \geq S$

let $P(X_0, \ldots, X_N)$ be a homogenous polynomial of degree at most equal to D that vanishes on $\Gamma(S)$ to order at least equal to T along A. Then if

$$(T/n)^{n-1}(S/n) \geq (c\ D)^n$$

the polynomial P vanishes on all of G.

This Theorem is an immediate consequence of the Main Theorem and the following Proposition.

Propostion 1. We have $\tau(A;G) = n - 1/n$.

Proof of the Proposition. Since $\tau(A;G) = \sigma(A;G)$ it suffices to prove the Proposition with σ instead of τ. Suppose $\sigma < n - 1/n$. Then there exists an algebraic subgroup H of codimension r which is contained in A. In $T(G)$ this subgroup is defined by the vanishing of linear forms $L_1(z_1,\ldots, z_n),\ldots,L_r(z_1, \ldots ,z_n)$. These linear forms may be chosen in such a way that they have coefficients in K. Since H is contained in A it follows that the rank of the system of linear forms $L,L_1,\ldots,L_r$ is equal to r. This is less than n. If we regard the matrix of coefficients of this system of linear forms it follows that all minors of type $(r+1\ ,\ r+1)$ have vanishing determinant. Since the rank of the system $L_1,\ldots,L_r$ is equal to r we deduce a non-trivial linear relation with coefficients in K between $1,\beta_1,\ldots,\beta_{n-1}$. This is a contradiction and proves that $\sigma = n-1/n$.

9. Some further applications. Throughout this section we denote by C either the field of complex numbers or its p-adic analogue for some prime p. We shall discuss now some of the results that can be obtained as a consequence of the Main Theorem of this paper.

The main application is the answer to the fallowing question: Let G be a commutative group variety of dimension n defined over $\overline{\mathbb{Q}}$. Let A be an analytic subgroup of G also defined over the field $\overline{\mathbb{Q}}$. By this we mean that the tangent space $T(A)$ is a subspace of $T(G)$ which is defined over $\overline{\mathbb{Q}}$.

Alternatively, if one does not consider A as a subset of G but embedded by some embedding φ, we mean by this that the differential $d\varphi$ of φ is a linear map that is defined over $\overline{\mathbb{Q}}$. It is natural to ask now whether the set $A(\overline{\mathbb{Q}})$ of $\overline{\mathbb{Q}}$ - rational points is non-trivial. We have the following result.

Theorem X. Let $\varphi : C^{n-1} \longrightarrow G$ be an analytic subgroup of G of codimension 1 defined over $\overline{\mathbb{Q}}$. If then $\varphi^{-1}(G(\overline{\mathbb{Q}})) \neq \{0\}$ then there exists an algebraic subgroup H of G such that $\dim H > 0$ and $H \subseteq \varphi(C^{n-1})$.

One can verify that all the known qualitative results on linear forms in logarithms or abelian logarithms, such as the results of Baker, Masser, Coates-Lang, Bertrand-Masser, are a consequences of Theorem X.

One of the applications of Theorem X is the following. Let C be an algebraic curve defined over $\overline{\mathbb{Q}}$ which we may assume to be smooth and ξ a meromorphic defferential form on C which is not exact, i.e. of the form $d\alpha$ for some rational function α on C. Let D be qual-to the polar divisor of ξ and γ be a closed path on $C - D$ representing a homology class $[\gamma]$ in $H_1(C - D, \mathbb{Z})$. Then we have the following result (here we put $C = \mathbb{C}$).

Theorem Y. Let ξ be defined over $\overline{\mathbb{Q}}$. Then the integral $\int_\gamma \xi$ is either zero or transcendental.

We should remark that it is possible to determine when the integral in Theorem Y is zero. In the last section we have given as an example for the Main Theorem the zero estimate for proving the linear independence of logarithms and elliptic logarithms. We shall now state a first general lower bound for linear forms in arbitrary logarithms. For this let as before C be either the field of complex numbers of its p-adic analogue and G be a commutative group variety defined over $\overline{\mathbb{Q}} \subseteq C$. Let u be an element of the tangent space $T(G)$ of G at the neutral element of G such that $\exp_G(u)$ is in the set of algebraic points $G(\overline{\mathbb{Q}})$ of G, let the height of $\exp_G(u)$ be bounded by $\Omega \geq 4$ and let $L = \beta_1 z_1 + \ldots + \beta_n z_n$ be a linear form on $T(G)$ with algebraic coefficient not all zero and heights bounded by $B \geq 4$. Then we have the following result.

Theorem Z. If $L(u) \neq 0$ then

$$|L(u)| \geq (B \log \Omega)^{-(\log B \cdot \log \Omega)^n}$$

for some effective computable positive constant c. Obviously this is not the best possible result that one can obtain in special cases. For example the dependence in B in Baker's result is much better. But the dependence in Ω is essential the best one can obtain till now even in special cases.

References

[1] J. Ax, Some topics in differential algebraic geometry, Amer. J. Math 94 (1972), 1195-1213.

[2] A. Baker, Transcendental Number Theory, Cambridge University Press, Cambridge 1975.

[3] A. Baker, D.W, Masser, Transcendence theory: Advances and Applications, Academic Press, London and New York 1977.

[4] D. Bertrand, D.W. Masser, Linear forms in elliptic integrals, Inventiones math. 58, 283-288 (1980).

[5] A. Borel, Linear algebraic groups, W.A. Benjamin (1969), New York.

[6] D. Brownawell, D.W. Masser, Multiplicity estimates for analytic functions II, Duke Math. J. 47 (1980), 273-295.

[7] W. Gröbner, Algebraische Geometrie II, BI Hochschulskripten, 737/737a* (1970).

[8] G. Hochschild, The Structure of Lie groups, Holden-Day, San Francisco-London-Amsterdam 1965.

[9] E.R. Kolchin, Algebraic groups and algebraic independence, Am. J. Math. 90 (1968), 1151-1164.

[10] D.W. Masser, Elliptic functions and transcendence, Lecture Notes in Mathematics, No. 437, Springer Verlag, Berlin 1975.

[11] D.W. Masser, On polynomials and exponential polynomials in several variables, Inventiones math. 63, 81-95 (1981).

[12] D.W. Masser. A note on Baker's theorem, Recent progress in analytic number theory, vol.2, Academic Press, London (1981), 153-158.

[13] D.W. Masser, G. Wüstholz, Zero estimates on group varieties I, Inventiones math. 64,489-516 (1981).

[14] D.W. Masser, G. Wüstholz, Zero estimates on group varieties II, preprint.

[15] D. Mumford, Algebraic geometry I-complex projective varieties, Springer Verlag, Berlin-Heidelberg-New York 1976.

[16] Narasimham, Analysis on Real and Complex Manifold, Mason & Cie., Paris 1973.

[17] J.P. Serre, Quelques propriétés des groupes algébriques commutatifs, in Astérisque 69-70 (1979), 191-202.

[18] M. Waldschmidt, Nombres transcendants et groupes algébriques, Astérisque 69-70 (1979).

[19] F.W. Warner, Foundations of diffentiable manifolds and Lie groups, Springer Verlag, 1983 (2^{nd} edition).

[20] G. Wüstholz, Über das abelsche Analogen des Lindemannschen Satzes, Inventiones math. 72 , 363-388 (1983).

[21] O. Zariski, P. Samuel, Commutative Algebra vol. I,II. Springer-Verlag, New York-Heidelberg-Berlin 1960.