

Zero estimates on group varieties II

D.W. Masser¹ and G. Wüstholz²

¹ Department of Mathematics, University of Michigan, Ann Arbor, MI 48109, USA

² Max-Planck-Institut für Mathematik, Gottfried-Claren-Strasse 26, D-5300 Bonn 3,
Federal Republic of Germany

1. Introduction

The object of this paper is to generalize the basic zero estimates which were obtained in our earlier article [4]. Let G be a commutative group variety embedded in some projective space, and let Γ be a finitely generated subgroup (not necessarily algebraic) of G . In [4] we gave sharp upper bounds for the number of zeroes in Γ , counted without multiplicity, of an arbitrary homogeneous polynomial. In the present paper, we introduce a natural concept of multiplicity along a one-parameter subgroup, and by using the methods of [2] we obtain the analogous estimates which take this multiplicity into account.

We also incorporate several more new features into our results. Firstly, the estimates of [4] are very weak when Γ contains torsion points of high order, and so we use a more refined counting function on Γ which is capable of detecting such points. Secondly, we show how the results can be improved when G splits into a product $G_1 \times \dots \times G_k$ of group varieties G_1, \dots, G_k . For this we need to consider multiprojective embeddings rather than simply projective embeddings; see also the article [13] of Moreau for similar considerations. Lastly, by using more delicate properties of multiprojective varieties, we show how the estimates can be even further sharpened when the groups G_1, \dots, G_k satisfy a certain natural disjointness condition.

The results of this paper have several applications to transcendence theory and related areas. They enable fairly rapid proofs to be given of Baker's theorem on linear forms in logarithms (cf. [9]), and also of the elliptic analogue in the case of complex multiplication (see [12] for a particularly sharp refinement in this context). Furthermore they have already been used to establish the elliptic analogues of Gelfond's theorems on the algebraic independence of values of the exponential function (see [5]), and it is also possible to give a simplified proof of an interesting related result of Philippon [7] on the p -adic Weierstrass zeta function. More recently, our estimates have played an important part in the second author's proof of the elliptic and abelian analogues of Lindemann's theorem [11]. It is also probable that they will lead to small

improvements in the results of [6] on the Néron-Tate height and division points on an abelian variety.

In order to state our results we start by discussing our multiprojective embedding and the concept of multiplicity. In [4] we considered a group variety embedded in projective space \mathbb{P}_N for some integer $N \geq 1$. In this situation we shall say that the group variety is linear if the addition laws (see Sect. 2 (p. 492) of [4]) can be defined by bilinear forms. For an integer $k \geq 1$ let now G_1, \dots, G_k be arbitrary commutative group varieties, defined over $K = \mathbb{C}$ or the analogous p -adic field \mathbb{C}_p , and embedded in projective spaces $\mathbb{P}_{N_1}, \dots, \mathbb{P}_{N_k}$ for integers $N_1 \geq 1, \dots, N_k \geq 1$. The group variety $G = G_1 \times \dots \times G_k$ is then embedded in $\mathcal{X} = \mathbb{P}_{N_1} \times \dots \times \mathbb{P}_{N_k}$. Although this can in turn be embedded in projective space by means of the Segre mapping, it is not convenient to do this in the context of the present paper. So we introduce variables $X_{i,0}, \dots, X_{i,N_i}$ on \mathbb{P}_{N_i} ($1 \leq i \leq k$), and we work in the ring

$$\mathfrak{R} = K[X_{1,0}, \dots, X_{1,N_1}, \dots, X_{k,0}, \dots, X_{k,N_k}].$$

with multihomogeneous polynomials which are homogeneous separately in the variables of $\mathbb{P}_{N_1}, \dots, \mathbb{P}_{N_k}$. Each point of \mathcal{X} can be described in terms of multiprojective coordinates in the usual way (see for example [10]).

Now G , being smooth, has the natural structure of an analytic manifold over K . By a one-parameter subgroup of G we shall mean a non-trivial analytic map Φ from K to G which is also a homomorphism of additive groups, and we use the same symbol Φ for $\Phi(K)$; thus $\Phi \neq 0$ the origin of G . The map Φ will be fixed from now on throughout the paper. For an element g of G and a multihomogeneous polynomial P in \mathfrak{R} we define the order of vanishing $\text{ord}_g P$ of P at g along Φ as follows. It is well-known that the map T_g from G to G representing translation by g is analytic. Hence the composition

$$\Psi(z) = \Psi_g(z) = T_g(\Phi(z))$$

is an analytic map from K to G . In particular, there exist functions

$$\psi_{1,0}(z), \dots, \psi_{1,N_1}(z), \dots, \psi_{k,0}(z), \dots, \psi_{k,N_k}(z), \tag{1.1}$$

analytic near $z=0$, such that for all z sufficiently small their values are multiprojective coordinates of $\Psi(z)$. If now the function

$$f(z) = P(\psi_{1,0}(z), \dots, \psi_{1,N_1}(z), \dots, \psi_{k,0}(z), \dots, \psi_{k,N_k}(z))$$

is identically zero we write $\text{ord}_g P = \infty$, this symbol being subject to the usual conventions. Otherwise we define $\text{ord}_g P$ as the order of zero of $f(z)$ at $z=0$. It is easily seen that this definition is independent of the choice of functions (1.1) representing $\Psi(z)$. Furthermore $\text{ord}_g P > 0$ if and only if P vanishes at g . If for some $T \geq 0$ we have $\text{ord}_g P \geq T$, we shall say that P vanishes at g to order at least T along Φ .

Now let X be a finite subset of G containing the origin. Suppose the dimensions of G_1, \dots, G_k are $n_1 \geq 1, \dots, n_k \geq 1$ respectively, and put $n = n_1 + \dots + n_k$. For integers r with $1 \leq r \leq n$ we define quantities $Q_r(X)$ as follows. Firstly,

if G has no algebraic subgroup of codimension r , we put

$$Q_r(X) = |X|$$

the cardinality of X . Otherwise, for each subgroup H of G we write $|X/H|$ for the maximum number of elements of X that are distinct modulo H , and we put

$$Q_r(X) = \min |X/H|$$

as H runs over all connected algebraic subgroups of G of codimension r . We also write G_{tors} for the group of torsion points of G .

For an integer $r \geq 1$ we write $X^{(r)}$ for the r -fold iterated sum consisting of all expressions $x_1 + \dots + x_r$ for x_1, \dots, x_r in X . Since X contains 0 , we have $X \subseteq X^{(r)}$ ($r \geq 1$). Finally for integers $d_1 \geq 0, \dots, d_k \geq 0$ we say that a multihomogeneous polynomial P in \mathbb{G} has multidegree (d_1, \dots, d_k) if its degrees in the variables of $\mathbb{P}_{N_1}, \dots, \mathbb{P}_{N_k}$ are d_1, \dots, d_k respectively. For real $D_1 \geq 0, \dots, D_k \geq 0$ we shall say that its multidegree is at most (D_1, \dots, D_k) if we have $d_1 \leq D_1, \dots, d_k \leq D_k$. We can now state our first result.

Main Theorem (general version). *For commutative group varieties G_1, \dots, G_k there exists a constant $c > 0$ with the following property. Let Φ be a one-parameter subgroup of $G = G_1 \times \dots \times G_k$, and let X be a finite subset of G containing the origin. Suppose for integers $D_1 \geq 1, \dots, D_k \geq 1$ and $T \geq 1$ there is a polynomial P in \mathfrak{R} , multihomogeneous of multidegree at most (D_1, \dots, D_k) , that vanishes at each point of $X^{(n)}$ to order at least T along Φ . If G_1, \dots, G_k are all linear put $E = T$; otherwise let E denote the minimum of all those D_i for which G_i is not linear ($1 \leq i \leq k$). For an integer r with $1 \leq r \leq n$ let Δ_r be the maximum of the products r at a time of the numbers D_1, \dots, D_1 (n_1 times), \dots, D_k, \dots, D_k (n_k times).*

Suppose that

$$TQ_r(X) \geq c \Delta_r \quad (1 \leq r \leq n)$$

and if $n > 1$ that

$$EQ_r(X) \geq c \Delta_r \quad (1 \leq r < n).$$

Suppose further that either

$$EQ_n(X) \geq c \Delta_n$$

or

$$|X/G_{\text{tors}}| = |X|.$$

Then P vanishes on all of $g + \Phi$ for some g in the subgroup of G generated by the elements of X .

Before we state our other result we need a definition. We say that the groups G_1, \dots, G_k are mutually disjoint (or just disjoint) if every connected algebraic subgroup H of $G = G_1 \times \dots \times G_k$ has the form $H = H_1 \times \dots \times H_k$ for algebraic subgroups H_1, \dots, H_k of G_1, \dots, G_k respectively. The subgroups H_1, \dots, H_k are then necessarily connected. In this case, if X is a finite subset of G containing the origin, we can split up the above functions $Q_r(X)$ in the following way. For integers r_1, \dots, r_k with

$$0 \leq r_1 \leq n_1, \dots, 0 \leq r_k \leq n_k, \quad r_1 + \dots + r_k \geq 1$$

we define quantities $Q_{r_1, \dots, r_k}(X)$ as follows. Firstly, if there exists i with $1 \leq i \leq k$ such that G_i has no algebraic subgroup of codimension r_i , we put

$$Q_{r_1, \dots, r_k}(X) = |X|.$$

Otherwise we let

$$Q_{r_1, \dots, r_k}(X) = \min |X/H|$$

as H runs over all connected algebraic subgroups of G of the form $H_1 \times \dots \times H_k$ with H_i a connected algebraic subgroup of G_i of codimension r_i ($1 \leq i \leq k$). We can now state our second result.

Main Theorem (disjoint version). *For mutually disjoint commutative group varieties G_1, \dots, G_k there exists a constant $c > 0$ with the following property. Let Φ be a one-parameter subgroup of $G = G_1 \times \dots \times G_k$, and let X be a finite subset of G containing the origin. Suppose for integers $D_1 \geq 1, \dots, D_k \geq 1$ and $T \geq 1$ there is a polynomial P in \mathfrak{R} , multihomogeneous of multidegree at most (D_1, \dots, D_k) , that vanishes at each point of $X^{(m)}$ to order at least T along Φ . If G_1, \dots, G_k are all linear put $E = T$; otherwise let E denote the minimum of all those D_i for which G_i is not linear ($1 \leq i \leq k$).*

Suppose that

$$TQ_{r_1, \dots, r_k}(X) \geq c D_1^{r_1} \dots D_k^{r_k} \quad (0 \leq r_1 \leq n_1, \dots, 0 \leq r_k \leq n_k, r_1 + \dots + r_k \geq 1)$$

and if $n > 1$ that

$$EQ_{r_1, \dots, r_k}(X) \geq c D_1^{r_1} \dots D_k^{r_k} \quad (0 \leq r_1 \leq n_1, \dots, 0 \leq r_k \leq n_k, 1 \leq r_1 + \dots + r_k < n).$$

Suppose further that either

$$EQ_{n_1, \dots, n_k}(X) \geq c D_1^{n_1} \dots D_k^{n_k} \tag{1.2}$$

or

$$|X/G_{\text{tors}}| = |X|. \tag{1.3}$$

Then P vanishes on all of $g + \Phi$ for some g in the subgroup of G generated by the elements of X .

Let us make here a remark about the conditions (1.2) and (1.3). The effect of (1.2) in practice is to restrict the number T of derivatives to the same order of magnitude as E . This suffices for the applications in [11]. By imposing instead the condition (1.3) on X we can sometimes take T roughly up to E^2 , and this is crucial for the work of [5]. Similar remarks apply to the general version of the Main Theorem.

The arrangement of this paper is as follows. In Sect. 2 we set up the operators which provide the algebraic description of translation by elements of X . This is essentially the generalization to multiprojective space of Sects. 2 and 3 of [4], but a few additional considerations are needed. Then in Sect. 3 we set up the derivation operator which is the algebraic equivalent of differentiating along Φ , and we obtain some of its properties.

Next we give in Sect. 4 a technical estimate which in geometric terms generalizes to multiprojective space the result that the degree of a subvariety of G does not change much under translation. The result for a single projective

space is probably not new, but we could not find a suitable reference, so our proof is self-contained. Then in Sect. 5 we derive another technical estimate, this time for the number of connected components of certain stabilizer groups; this is rather more delicate and it plays a central part in our overall proof.

Then we prove our Main Theorems. As the proofs are very similar, we are able to present them in parallel. In Sect. 6 we state a Proposition and we verify that it implies the Main Theorems. We subsequently prove the Proposition in Sect. 7.

Finally in Sect. 8 we show that the general version of our Main Theorem implies all the zero estimates announced in Sect. 9 of [4]. We also give some practical criteria for establishing the disjointness of given group varieties.

For the convenience of the reader we include an Appendix which summarizes some fairly classical facts about degree theory for multihomogeneous ideals. The main reference here is [10] but this is not quite adequate for all our purposes.

We end this introduction with a few comments on terminology. We shall be working in the product space $\mathcal{X} = \mathbb{P}_{N_1} \times \dots \times \mathbb{P}_{N_k}$ using the Zariski topology for which the closed sets are those defined by the vanishing of multihomogeneous polynomials in \mathfrak{R} . For a subset S of \mathcal{X} we write \bar{S} for the closure in \mathcal{X} , and we shall sometimes write S_G for the intersection $G \cap S$. If already $S \subseteq G$ it is easy to see from the continuity of the group laws on G that

$$G \cap \overline{g + S} = g + (G \cap \bar{S}) \tag{1.4}$$

for any g in G . If further S is closed in G , that is, $S = G \cap X$ for some closed set X in \mathcal{X} , then $G \cap \bar{S} = S$; for example, this holds if S is an algebraic subgroup of G .

Next if $V \subseteq \bar{G}$ is an irreducible variety meeting G , the set $G \cap V = V_G$ is a non-empty open subset of V , and so

$$\overline{G \cap V} = V. \tag{1.5}$$

These remarks will be useful in Sects. 2 and 5; they enable us to avoid the construction of a theory of quasiprojective varieties in \mathcal{X} .

Finally for integers j_1, \dots, j_k we write $\mathbf{j} = (j_1, \dots, j_k)$ for the corresponding element of \mathbb{Z}^k , and we put

$$|\mathbf{j}| = |j_1| + \dots + |j_k|.$$

2. Translation operators

Let G_1, \dots, G_k be as in Sect. 1, not necessarily disjoint, and let Γ be a finitely generated subgroup of $G = G_1 \times \dots \times G_k$. Our object here is to define for each γ in Γ an endomorphism $E(\gamma)$ of the associated polynomial ring \mathfrak{R} and a corresponding operator $\mathcal{E}(\gamma)$ acting on ideals of \mathfrak{R} . These will generalize the constructions of Sects. 2 and 3 of [4] for the case $k = 1$.

Fix an integer i with $1 \leq i \leq k$. Let π_i denote the projection from G to G_i , and write $\Gamma_i = \pi_i(\Gamma)$. The arguments of the proof of Lemma 1 of [4] (especially

p. 493) show that there exists an addition law on G_i valid on $\Gamma_i \times \Gamma_i$. To be more precise, there exists an integer $a_i \geq 1$, independent of Γ_i , an open subset \mathcal{O}_i of $G_i \times G_i$ containing $\Gamma_i \times \Gamma_i$, and polynomials $A_{i,0}, \dots, A_{i,N_i}$ in $K[X_{i,0}, \dots, X_{i,N_i}, Y_{i,0}, \dots, Y_{i,N_i}]$ homogeneous of degree a_i in each of the two sets of variables, such that for any g, h in G_i with projective coordinates ξ_0, \dots, ξ_{N_i} and $\eta_0, \dots, \eta_{N_i}$ with (g, h) in \mathcal{O}_i the numbers

$$A_{i,j}(\xi_0, \dots, \xi_{N_i}, \eta_0, \dots, \eta_{N_i}) \quad (0 \leq j \leq N_i)$$

are projective coordinates of $g+h$. We note that if G_i is linear in the terminology of Sect. 1, then we can assume $a_i=1$, and henceforth we shall make this assumption. For γ in Γ let $\eta_{i,0}, \dots, \eta_{i,N_i}$ be projective coordinates of $\pi_i(\gamma)$, and define

$$E(\gamma)X_{i,j} = A_{i,j}(X_{i,0}, \dots, X_{i,N_i}, \eta_{i,0}, \dots, \eta_{i,N_i}) \quad (0 \leq j \leq N_i).$$

We can extend $E(\gamma)$ uniquely to an endomorphism of \mathfrak{R} considered as an algebra over K . Note that if P in \mathfrak{R} is multihomogeneous of multidegree (D_1, \dots, D_k) then $E(\gamma)P$ is multihomogeneous of multidegree $(a_1 D_1, \dots, a_k D_k)$.

Next we let \mathfrak{G} be the multihomogeneous ideal of \mathfrak{R} generated by all multihomogeneous polynomials vanishing on G . Let also \mathcal{M} be the multiplicative set of \mathfrak{R} consisting of all polynomials not vanishing at any point of Γ . As in Lemma 2 (p. 494) of [4], it is easy to see that for any γ in Γ we have $E(\gamma)\mathfrak{G} \subseteq \mathfrak{G}$ and $E(\gamma)\mathcal{M} \subseteq \mathcal{M}$. For an ideal \mathfrak{I} of \mathfrak{R} we write \mathfrak{I}^* for the corresponding contracted extension of \mathfrak{I} with respect to \mathcal{M} . Finally for γ in Γ and an ideal \mathfrak{I} of \mathfrak{R} define

$$\mathcal{E}(\gamma)\mathfrak{I} = (E(\gamma)\mathfrak{I}, \mathfrak{G})^*.$$

We say that \mathfrak{I} is special if $\mathfrak{G} \subseteq \mathfrak{I}$ and $\mathfrak{I}^* = \mathfrak{I}$. Then we have the following properties.

Lemma 1. (i) For any multihomogeneous ideal \mathfrak{I} of \mathfrak{R} and any γ, δ in Γ the ideal $\mathcal{E}(\gamma)\mathfrak{I}$ is multihomogeneous and special, and we have

$$\mathfrak{I} \subseteq \mathcal{E}(0)\mathfrak{I}, \quad \mathcal{E}(\gamma + \delta)\mathfrak{I} = \mathcal{E}(\gamma)\mathcal{E}(\delta)\mathfrak{I}.$$

(ii) If further \mathfrak{I} is special then $\mathfrak{I} = \mathcal{E}(0)\mathfrak{I}$.

(iii) If further \mathfrak{I} is non-zero and proper then $\mathcal{E}(\gamma)\mathfrak{I}$ has the same rank as \mathfrak{I} .

(iv) If further \mathfrak{I} is unmixed then $\mathcal{E}(\gamma)\mathfrak{I}$ is unmixed.

(v) If further \mathfrak{I} is primary of length l with associated prime \mathfrak{P} , then $\mathcal{E}(\gamma)\mathfrak{I}$ is primary of length l with associated prime $\mathcal{E}(\gamma)\mathfrak{P}$.

Proof. The properties (i), (ii) and (iii), as well as property (v) for $l=1$, can be proved as in Sects. 2 and 3 of [4], with only trivial changes arising from the multihomogeneous nature of everything. We excuse ourselves from giving the details.

We next establish property (v) for arbitrary $l \geq 1$. To show that $\mathcal{E}(\gamma)\mathfrak{I}$ is primary it suffices to verify that if P, Q are multihomogeneous polynomials of \mathfrak{R} with PQ in $\mathcal{E}(\gamma)\mathfrak{I}$ but P not in $\mathcal{E}(\gamma)\mathfrak{I}$, then Q^e is in $\mathcal{E}(\gamma)\mathfrak{I}$ for some integer

$e \geq 1$. On applying $E(-\gamma)$ we see that $P'Q'$ lies in $E(-\gamma)\mathcal{E}(\gamma)\mathfrak{I}$, where $P'=E(-\gamma)P$, $Q'=E(-\gamma)Q$. But

$$E(-\gamma)\mathcal{E}(\gamma)\mathfrak{I} \subseteq \mathcal{E}(-\gamma)\mathcal{E}(\gamma)\mathfrak{I} = \mathcal{E}(0)\mathfrak{I} = \mathfrak{I}$$

by (i) and (ii) above. So $P'Q'$ lies in \mathfrak{I} . But P' is not in \mathfrak{I} . For otherwise $E(-\gamma)(P) \subseteq \mathfrak{I}$, whence

$$\mathcal{E}(-\gamma)(P) \subseteq (\mathfrak{I}, \mathfrak{G})^* = \mathfrak{I}^* = \mathfrak{I},$$

which on applying $\mathcal{E}(\gamma)$ and using (i) above would give $(P) \subseteq \mathcal{E}(\gamma)\mathfrak{I}$, contradicting the fact that P is not in $\mathcal{E}(\gamma)\mathfrak{I}$. Since \mathfrak{I} is primary, it follows that Q^e is in \mathfrak{I} for some integer $e \geq 1$. So

$$\mathcal{E}(-\gamma)(Q^e) = (E(-\gamma)(Q^e), \mathfrak{G})^* \subseteq (\mathfrak{I}, \mathfrak{G})^* = \mathfrak{I},$$

whence applying $\mathcal{E}(\gamma)$ and using (i) and (ii) we conclude that Q^e lies in \mathfrak{I} as required. Hence $\mathcal{E}(\gamma)\mathfrak{I}$ is indeed primary.

Next suppose \mathfrak{I} has rank r . Then so does its associated prime \mathfrak{P} , and, as $\mathfrak{I} \subseteq \mathfrak{P}$, it follows that \mathfrak{P} is special and $\mathcal{E}(\gamma)\mathfrak{I} \subseteq \mathcal{E}(\gamma)\mathfrak{P}$. By (iii) above $\mathcal{E}(\gamma)\mathfrak{I}$ has rank r , and by (v) above with $l=1$ we see that $\mathcal{E}(\gamma)\mathfrak{P}$ is prime of rank r . Hence $\mathcal{E}(\gamma)\mathfrak{P}$ must be the associated prime of $\mathcal{E}(\gamma)\mathfrak{I}$.

Finally if \mathfrak{I} has length l then there is a strictly increasing chain

$$\mathfrak{I} = \mathfrak{Q}_0 \subsetneq \mathfrak{Q}_1 \dots \subsetneq \mathfrak{Q}_{l-1} = \mathfrak{P}$$

of multihomogeneous special primary ideals of \mathfrak{R} , and on applying $\mathcal{E}(\gamma)$ we obtain an increasing chain

$$\mathcal{E}(\gamma)\mathfrak{I} = \mathcal{E}(\gamma)\mathfrak{Q}_0 \subseteq \mathcal{E}(\gamma)\mathfrak{Q}_1 \dots \subseteq \mathcal{E}(\gamma)\mathfrak{Q}_{l-1} = \mathcal{E}(\gamma)\mathfrak{P}.$$

This too must be strictly increasing, since from $\mathcal{E}(\gamma)\mathfrak{Q}_i = \mathcal{E}(\gamma)\mathfrak{Q}_{i+1}$ would follow $\mathfrak{Q}_i = \mathfrak{Q}_{i+1}$ on applying $\mathcal{E}(-\gamma)$. As the ideals in this new chain are primary, it follows that the length m of $\mathcal{E}(\gamma)\mathfrak{I}$ is at least l . But by a similar argument the length of $\mathcal{E}(-\gamma)\mathcal{E}(\gamma)\mathfrak{I}$ is at least m . As this ideal is \mathfrak{I} itself, we conclude that $m=l$. This proves (v) in general.

It remains to verify (iv). Suppose \mathfrak{I} has rank r . Then we can write $\mathfrak{I} = \bigcap \mathfrak{Q}$ taken over a collection of multihomogeneous primary ideals \mathfrak{Q} . Since \mathfrak{I} is special, so is each \mathfrak{Q} . From $\mathfrak{I} \subseteq \mathfrak{Q}$ we deduce immediately

$$\mathcal{E}(\gamma)\mathfrak{I} \subseteq \bigcap \mathcal{E}(\gamma)\mathfrak{Q}. \tag{2.1}$$

To obtain the opposite inclusion, let P be an arbitrary multihomogeneous polynomial in the right-hand side of (2.1). Then $Q = E(-\gamma)P$ lies in $\mathcal{E}(-\gamma)\mathcal{E}(\gamma)\mathfrak{Q} = \mathfrak{Q}$ for each \mathfrak{Q} , so Q is in \mathfrak{I} . This leads to $\mathcal{E}(-\gamma)(P) \subseteq \mathfrak{I}$, so

$$(P) \subseteq \mathcal{E}(0)(P) = \mathcal{E}(\gamma)\mathcal{E}(-\gamma)(P) \subseteq \mathcal{E}(\gamma)\mathfrak{I}.$$

Hence P is in $\mathcal{E}(\gamma)\mathfrak{I}$, and since P was arbitrary, we get the opposite inclusion to (2.1). Therefore $\mathcal{E}(\gamma)\mathfrak{I} = \bigcap \mathcal{E}(\gamma)\mathfrak{Q}$, and it follows at once, possibly by omit-

ting redundant components, that $\mathcal{E}(\gamma)\mathfrak{I}$ is unmixed. This establishes (iv) and so completes the proof of Lemma 1.

We note here that it is in fact possible to prove Lemma 1 using directly the corresponding result for $k=1$ given as Lemmas 3 and 4 of [4]. One embeds G in a single projective space by means of the Segre map and then one works with homogeneous polynomials in the corresponding polynomial ring in $(N_1+1)\dots(N_k+1)$ variables. But the details are tedious.

Finally we shall need the following lemma, which reveals explicitly the geometric significance of the operators $\mathcal{E}(\gamma)$. Note that a multihomogeneous prime ideal \mathfrak{P} of \mathfrak{R} is special if and only if its associated multiprojective variety V in \mathcal{X} meets Γ and is contained in \overline{G} . In this case $V_G = G \cap V$ is a non-empty open subset of V , so $\overline{G \cap V} = V$, by (1.5).

Lemma 2. *Let \mathfrak{P} be a multihomogeneous special prime ideal of \mathfrak{R} with associated variety V in \mathcal{X} . Then the associated variety W of $\mathcal{E}(\gamma)\mathfrak{P}$ satisfies*

$$\gamma + W_G = V_G.$$

Proof. Recall that the translation polynomials defining $E(\gamma)$ are valid on an open subset \mathcal{O} of G containing Γ . Since $\mathcal{E}(\gamma)\mathfrak{P}$ is special, W meets Γ , and therefore $\mathcal{O} \cap W_G$ is a non-empty open subset of W . Pick any x in $\mathcal{O} \cap W_G$ and any P in \mathfrak{P} . Then $E(\gamma)P$ is in $\mathcal{E}(\gamma)\mathfrak{P}$, so vanishes at x . This means that P vanishes at $\gamma+x$. Since P was arbitrary, it follows that $\gamma+x$ is in V_G . Since x was arbitrary, we see that $\gamma+(\mathcal{O} \cap W_G) \subseteq V_G$. Taking the closure, and intersecting with G using (1.4), we get $\gamma+W_G \subseteq V_G$. The opposite inclusion can be obtained by applying the same argument to the prime ideals $\mathcal{E}(\gamma)\mathfrak{P}$ and $\mathcal{E}(-\gamma)\mathcal{E}(\gamma)\mathfrak{P} = \mathfrak{P}$. This proves Lemma 2.

The following is a useful consequence of this result. Suppose \mathfrak{P} is a multihomogeneous prime ideal of \mathfrak{R} containing \mathfrak{G} , and let γ be any point of G . Let V be the variety of \mathfrak{P} , and let Γ be any finitely generated subgroup of G meeting V and containing γ . At first sight it might seem that the ideal $\mathcal{E}(\gamma)\mathfrak{P}$ depends not only on the choice of Γ but also on the choice of addition laws valid on $\Gamma \times \Gamma$. However, Lemma 2 shows that $\mathcal{E}(\gamma)\mathfrak{P}$ is the ideal corresponding to $\overline{V_G - \gamma}$, and so is in fact independent of all these choices.

3. Differentiation operators

Let G_1, \dots, G_k be as in Sect. 1, not necessarily disjoint, let Γ be a finitely generated subgroup of $G = G_1 \times \dots \times G_k$, and let Φ be a one-parameter subgroup of G . In this section we define a derivation Δ on the associated polynomial ring \mathfrak{R} which provides the algebraic equivalent of differentiating along Φ .

Let

$$\varphi_{1,0}(z), \dots, \varphi_{1,N_1}(z), \dots, \varphi_{k,0}(z), \dots, \varphi_{k,N_k}(z)$$

be functions, analytic near $z=0$, that represent the map Φ locally near the origin. Fix an integer i with $1 \leq i \leq k$. As in Sect. 2, we have polynomials

$A_{i,0}, \dots, A_{i,N_i}$ in $K[X_{i,0}, \dots, X_{i,N_i}, Y_{i,0}, \dots, Y_{i,N_i}]$ representing the addition law on an open subset \mathcal{O}_i of $G_i \times G_i$ containing $\Gamma_i \times \Gamma_i$, where $\Gamma_i = \pi_i(\Gamma)$. We define

$$\Delta X_{i,j} = (d/dw)(A_{i,j}(X_{i,0}, \dots, X_{i,N_i}, \varphi_{i,0}(w), \dots, \varphi_{i,N_i}(w)))|_{w=0} \quad (0 \leq j \leq N_i),$$

and we extend Δ uniquely to a derivation on \mathfrak{R} considered as an algebra over K . Note that if P in \mathfrak{R} is multihomogeneous of multidegree (D_1, \dots, D_k) then ΔP is multihomogeneous of multidegree $(D_1 + a_1 - 1, \dots, D_k + a_k - 1)$.

Lemma 3. (i) *We have $\Delta \mathfrak{G} \subseteq \mathfrak{G}$.*

(ii) *Let P be any multihomogeneous polynomial of \mathfrak{R} and let γ, δ be in Γ . Then if $\text{ord}_\delta P$ is infinite, so is $\text{ord}_{\delta-\gamma} E(\gamma)P$; and otherwise*

$$\text{ord}_{\delta-\gamma} E(\gamma)P = \text{ord}_\delta P.$$

(iii) *If $\text{ord}_\delta P$ is infinite so is $\text{ord}_\delta \Delta P$; and otherwise*

$$\text{ord}_\delta \Delta P = \text{ord}_\delta P - 1$$

provided $\text{ord}_\delta P \geq 1$.

Proof. We prove (ii) first. Let

$$\mathfrak{g}_{1,0}(z), \dots, \mathfrak{g}_{1,N_1}(z), \dots, \mathfrak{g}_{k,0}(z), \dots, \mathfrak{g}_{k,N_k}(z) \tag{3.1}$$

be functions, analytic near $z=0$, that represent the map

$$\Theta(z) = T_{\delta-\gamma}(\Phi(z)) = \delta - \gamma + \Phi(z)$$

near $z=0$. Using the addition laws, we see that the functions

$$\psi_{i,j}(z) = A_{i,j}(\mathfrak{g}_{i,0}(z), \dots, \mathfrak{g}_{i,N_i}(z), \eta_{i,0}, \dots, \eta_{i,N_i}) \quad (1 \leq i \leq k, 0 \leq j \leq N_i) \tag{3.2}$$

represent the map $\Psi(z) = T_\delta(\Phi(z))$ near $z=0$, where $\eta_{i,0}, \dots, \eta_{i,N_i}$ are projective coordinates of $\pi_i(\gamma)$ in \mathbb{P}_{N_i} ($1 \leq i \leq k$). Thus if we evaluate $\text{ord}_{\delta-\gamma} E(\gamma)P$ using (3.1) and $\text{ord}_\delta P$ using (3.2) it becomes clear that these two numbers are either both infinite, or both finite and equal. This proves (ii).

Next let \mathcal{O} be the open subset of G consisting of all g such that $(\pi_i(g), 0)$ lies in the open subset \mathcal{O}_i of $G_i \times G_i$ for all i with $1 \leq i \leq k$. It contains Γ , and so is non-empty. We now prove (iii) for any δ in \mathcal{O} .

Suppose first that $t = \text{ord}_\delta P$ is finite and positive. This implies that the power series development of the function

$$f(z+w) = P(\psi_{1,0}(z+w), \dots, \psi_{1,N_1}(z+w), \dots, \psi_{k,0}(z+w), \dots, \psi_{k,N_k}(z+w)) \tag{3.3}$$

starts with $c(z+w)^t$ for some $c \neq 0$. But on recalling that $\Psi = T_\delta(\Phi)$ we see that

$$\Psi(z+w) = \delta + \Phi(z+w) = \delta + \Phi(z) + \Phi(w) = \Psi(z) + \Phi(w),$$

and for z, w sufficiently small we can add the two terms on the extreme right-hand side by means of our addition formulae. Thus if we write

$$\alpha_{i,j}(z, w) = A_{i,j}(\psi_{i,0}(z), \dots, \psi_{i,N_i}(z), \varphi_{i,0}(w), \dots, \varphi_{i,N_i}(w)) \quad (1 \leq i \leq k, 1 \leq j \leq N_i)$$

it follows easily that the power series development of the function

$$f(z, w) = P(\alpha_{1,0}(z, w), \dots, \alpha_{1,N_1}(z, w), \dots, \alpha_{k,0}(z, w), \dots, \alpha_{k,N_k}(z, w))$$

starts with $c'(z+w)^t$ for some $c' \neq 0$. Hence

$$f_w(z, 0) = (\partial/\partial w)f(z, w)|_{w=0}$$

starts with $c' t z^{t-1}$. But from our definition of Δ we find after a short calculation that

$$f_w(z, 0) = \Delta P(\psi_{1,0}(z), \dots, \psi_{1,N_1}(z), \dots, \psi_{k,0}(z), \dots, \psi_{k,N_k}(z)).$$

It follows that $\text{ord}_\delta \Delta P = t - 1$ as required.

A similar argument works if $\text{ord}_\delta P = \infty$, for then the function in (3.3) and $f(z, w)$ are both identically zero. This proves (iii) for any δ in \mathcal{O} , and in particular for any δ in Γ .

Finally to prove (i) let P be an arbitrary multihomogeneous polynomial in \mathfrak{G} . Then $\text{ord}_\delta P = \infty$ for all δ in \mathcal{O} . So by the above remarks we see that $\text{ord}_\delta \Delta P = \infty$ for all δ in \mathcal{O} . In particular ΔP vanishes on \mathcal{O} . Since \mathcal{O} is a non-empty open subset of G , it follows that ΔP is in \mathfrak{G} . This establishes (i), and thereby completes the proof of Lemma 3.

Lastly it is convenient here to isolate in the following lemma the basic argument of Sect. 6 of [2]. For a multihomogenous ideal \mathfrak{I} of \mathfrak{R} and g in G we write $\text{ord}_g \mathfrak{I}$ for the minimum of $\text{ord}_g P$ as P runs over all multihomogeneous polynomials of \mathfrak{I} . Put $N = N_1 + \dots + N_k$.

Lemma 4. *For $1 \leq r \leq N$ let \mathfrak{I} be a multihomogeneous special unmixed ideal of rank r . Suppose \mathfrak{P} is a multihomogeneous prime ideal of rank r such that for some $T > 0$ we have*

$$\Delta^t \mathfrak{I} \subseteq \mathfrak{P} \quad (0 \leq t < T). \tag{3.4}$$

Assume that there exists γ in Γ such that $\text{ord}_\gamma \mathfrak{P}$ is finite and non-zero. Then \mathfrak{I} has a primary component \mathfrak{Q} of length at least T whose associated prime ideal is \mathfrak{P} .

Proof. Taking $t=0$ in (3.4) we see at once that \mathfrak{P} must be a prime component of \mathfrak{I} . Let \mathfrak{Q} be the corresponding primary component, and let e be its exponent. We shall show that $e \geq T$. Let $\omega = \text{ord}_\gamma \mathfrak{P}$, and pick P in \mathfrak{P} with $\text{ord}_\gamma P = \omega$. Then by (iii) of Lemma 3 we have

$$\text{ord}_\gamma \Delta P = \omega - 1 < \text{ord}_\gamma \mathfrak{P},$$

and so ΔP is not in \mathfrak{P} . If now \mathfrak{Q} is the only primary component of \mathfrak{I} , we put $Q=1$; otherwise we define Q as follows. For each of the other primary components $\mathfrak{Q}' \neq \mathfrak{Q}$ of \mathfrak{I} , their associated primes \mathfrak{P}' satisfy $\mathfrak{P}' \neq \mathfrak{P}$. Since \mathfrak{I} is unmixed, the ranks of $\mathfrak{P}, \mathfrak{P}'$ are equal, and so $\mathfrak{P}' \not\subseteq \mathfrak{P}$. Hence for each such \mathfrak{P}' we can find P' in \mathfrak{P}' but not in \mathfrak{P} . So if e' is the exponent of \mathfrak{Q}' the polynomial $P'^{e'}$ is in \mathfrak{Q}' but not in \mathfrak{P} . Now put $Q = \prod P'^{e'}$, where the product is over all $\mathfrak{Q}' \neq \mathfrak{Q}$ as above. Thus in both cases $P^e Q$ lies in \mathfrak{I} , but Q does not lie in \mathfrak{P} . Since

P lies in \mathfrak{P} , we see that

$$\Delta^e(P^e Q) \equiv e!(\Delta P)^e Q \pmod{\mathfrak{P}};$$

and since ΔP does not lie in \mathfrak{P} , we conclude that $\Delta^e(P^e Q)$ is not in \mathfrak{P} . So by (3.4) we cannot have $e < T$; thus indeed $e \geq T$.

Hence by Lemma 1 (p. 278) of [2] we see that the length of \mathfrak{Q} is also at least T . This completes the proof of Lemma 4.

4. Degree estimates

Let G_1, \dots, G_k be as in Sect. 1, not necessarily disjoint, and let Γ be a finitely generated subgroup of $G = G_1 \times \dots \times G_k$. Let a_1, \dots, a_k be as in Sect. 2, and define the operators $E(\gamma)$, $\mathcal{E}(\gamma)$ on the associated polynomial ring \mathfrak{R} as in Sect. 2. For an integer r let $\mathcal{N}(r)$ denote the set of all $\mathbf{j} = (j_1, \dots, j_k)$ in \mathbb{Z}^k with

$$0 \leq j_1 \leq N_1, \dots, 0 \leq j_k \leq N_k, \quad j_1 + \dots + j_k = r.$$

Thus $\mathcal{N}(r)$ is empty unless

$$0 \leq r \leq N = N_1 + \dots + N_k.$$

We recall (see the Appendix) that if \mathfrak{Z} is a multihomogeneous ideal of \mathfrak{R} whose rank r satisfies $1 \leq r \leq N$, then for any \mathbf{j} in $\mathcal{N}(r)$ there is a non-negative integer $\delta_{\mathbf{j}}(\mathfrak{Z})$ measuring the corresponding degree of \mathfrak{Z} . We further define $\delta_{\mathbf{j}}(\mathfrak{Z}) = 0$ for any \mathbf{j} in \mathbb{Z}^k not in $\mathcal{N}(r)$. We shall need the following comparison result.

Lemma 5. *For $1 \leq r \leq N$ let \mathfrak{P} be a multihomogeneous special prime ideal of \mathfrak{R} of rank r . Then for any $\mathbf{j} = (j_1, \dots, j_k)$ in $\mathcal{N}(r)$ and any γ in Γ we have*

$$\delta_{\mathbf{j}}(\mathfrak{P}) \leq a_1^{N_1 - j_1} \dots a_k^{N_k - j_k} \delta_{\mathbf{j}}(\mathcal{E}(\gamma) \mathfrak{P}).$$

Proof. We do this by considering the associated varieties in $\mathcal{X} = \mathbb{P}_{N_1} \times \dots \times \mathbb{P}_{N_k}$, and we argue by decreasing induction on r . If $r = N$ the result is easy. For any multihomogeneous special ideal \mathfrak{Z} is contained in the maximal multihomogeneous ideal $\mathfrak{R}(\gamma_0)$ corresponding to some point γ_0 in Γ , and so, if prime of rank N , it must be equal to $\mathfrak{R}(\gamma_0)$. Then the only possible value for \mathbf{j} is (N_1, \dots, N_k) , for which $\delta_{\mathbf{j}}(\mathfrak{Z}) = 1$. By parts (iii) and (iv) of Lemma 1, this argument applies to $\mathcal{E}(\gamma) \mathfrak{P}$ as well as to \mathfrak{P} . This does the case $r = N$.

Now assume the lemma holds for ideals of rank $r + 1 \leq N$, and let \mathfrak{P} be as above of rank r . Pick $\mathbf{j} = (j_1, \dots, j_k)$ in $\mathcal{N}(r)$. As $|\mathbf{j}| = r < N$, we can assume without loss of generality that $j_1 < N_1$. Since \mathfrak{P} is special, its associated variety V in \mathcal{X} is contained in the Zariski closure \bar{G} of G in \mathcal{X} . Let $G_\infty = \bar{G} \setminus G$ and $V_\infty = G_\infty \cap V$. Note that $V_\infty \neq V$, since V contains an element γ_0 of $\Gamma \subseteq G$. Thus either V_∞ is empty or its codimension r_∞ in \mathcal{X} satisfies $r_\infty \geq r + 1$. We choose a linear form L in $\mathfrak{R}_1 = K[X_{1,0}, \dots, X_{1,N_1}]$ as follows. If V_∞ is empty, then all we demand is that L should not vanish at γ_0 . However, if V_∞ is not empty, let W_1, \dots, W_t be its irreducible components, and fix w_l on W_l ($1 \leq l \leq t$). Then choose L so that it does not vanish at γ_0 or w_1, \dots, w_t .

In either case, since L does not vanish at γ_0 on V , we see that L does not lie in \mathfrak{P} . Hence the ideal $\mathfrak{T}=(\mathfrak{P}, L)$ is of rank $r + 1$, and we can write

$$\mathfrak{T} = \mathfrak{Q}_1 \cap \dots \cap \mathfrak{Q}_h \cap \mathfrak{T}'$$

for some $h \geq 1$, where $\mathfrak{Q}_1, \dots, \mathfrak{Q}_h$ are multihomogeneous primary ideals of \mathfrak{R} of rank $r + 1$ and \mathfrak{T}' is either \mathfrak{R} or of rank exceeding $r + 1$. Furthermore we can assume that the associated primes $\mathfrak{P}_1, \dots, \mathfrak{P}_h$ are distinct. Let V_1, \dots, V_h be the associated irreducible varieties in \mathcal{X} . We claim first that V_1, \dots, V_h all meet G .

For suppose not, and that $G \cap V_i$ is empty for some i with $1 \leq i \leq h$. Then as $V \subseteq \bar{V} \subseteq \bar{G}$, it would follow that

$$V_i = \bar{G} \cap V_i = (G_\infty \cap V_i) \cup (G \cap V_i) = G_\infty \cap V_i \subseteq V_\infty.$$

In particular V_∞ must be non-empty, whence $V_i \subseteq W_l$ for some l with $1 \leq l \leq t$. But the codimension of V_i in \mathcal{X} is $r + 1$, whereas the codimension of W_l in \mathcal{X} is at least $r_\infty \geq r + 1$. It follows that $V_i = W_l$. But this is not possible, as L vanishes on V_i but not at the point w_l of W_l . Hence indeed each V_i ($1 \leq i \leq h$) meets G .

Therefore for each i with $1 \leq i \leq h$ we can fix a point v_i of G on V_i . By the remark after Lemma 2, we may without loss of generality assume that Γ contains v_1, \dots, v_h , as by enlarging Γ we do not in fact change the ideal $\mathcal{E}(\gamma)\mathfrak{P}$. It follows now that, in the earlier notation for contracted extensions, we have $\mathfrak{P}_i^* = \mathfrak{P}_i$ ($1 \leq i \leq h$), and, since

$$\mathfrak{G} \subseteq \mathfrak{P} \subseteq (\mathfrak{P}, L) = \mathfrak{T} \subseteq \mathfrak{P}_i \quad (1 \leq i \leq h),$$

we see that $\mathfrak{P}_1, \dots, \mathfrak{P}_h$ are special.

Now write $\mathbf{e} = (1, 0, \dots, 0)$. Since $j_1 < N_1$, the vector $\mathbf{j} + \mathbf{e}$ is in $\mathcal{N}(r + 1)$, and because L is in \mathfrak{R}_1 we have by Lemma A5 of the Appendix with $(D_1, \dots, D_k) = \mathbf{e}$ the relation $\delta_{\mathbf{j}}(\mathfrak{P}) = \delta_{\mathbf{j} + \mathbf{e}}(\mathfrak{T})$. Also by Lemmas A2 and A3 of the Appendix we have

$$\delta_{\mathbf{j} + \mathbf{e}}(\mathfrak{T}) = \sum_{i=1}^h \delta_{\mathbf{j} + \mathbf{e}}(\mathfrak{Q}_i) = \sum_{i=1}^h l_i \delta_{\mathbf{j} + \mathbf{e}}(\mathfrak{P}_i),$$

where l_i is the length of \mathfrak{Q}_i ($1 \leq i \leq h$). The induction hypothesis therefore shows that

$$\delta_{\mathbf{j}}(\mathfrak{P}) \leq a_1^{-1} A \sum_{i=1}^h l_i \delta_{\mathbf{j} + \mathbf{e}}(\mathcal{E}(\gamma)\mathfrak{P}_i),$$

where

$$A = a_1^{N_1 - j_1} \dots a_k^{N_k - j_k}.$$

Using part (v) of Lemma 1 we get

$$\delta_{\mathbf{j}}(\mathfrak{P}) \leq a_1^{-1} A \sum_{i=1}^h \delta_{\mathbf{j} + \mathbf{e}}(\mathcal{E}(\gamma)\mathfrak{Q}_i). \tag{4.1}$$

Finally to get an upper bound for the right-hand side of (4.1) we consider the ideal $\mathfrak{T} = (\mathcal{E}(\gamma)\mathfrak{P}, E(\gamma)L)$. Now if $E(\gamma)L$ were in $\mathcal{E}(\gamma)\mathfrak{P}$, we should deduce at once that $\mathcal{E}(\gamma)(L) \subseteq \mathcal{E}(\gamma)\mathfrak{P}$. Applying $\mathcal{E}(-\gamma)$ and using parts (i) and (ii) of Lemma 1, we find that $(L) \subseteq \mathfrak{P}$, which is impossible, as remarked above. It

follows that \mathfrak{J} is of rank $r + 1$. Also, from the definition of $E(\gamma)$, we see that $E(\gamma)L$ lies in \mathfrak{R}_1 and is homogeneous of degree a_1 . So by Lemma A5 we have

$$a_1 \delta_j(\mathcal{E}(\gamma) \mathfrak{P}) = \delta_{j+e}(\mathfrak{J}). \tag{4.2}$$

But since $\mathfrak{J} = (\mathfrak{P}, L) \subseteq \mathfrak{Q}_i$, we deduce

$$\mathfrak{J} \subseteq \mathcal{E}(\gamma) \mathfrak{J} \subseteq \mathcal{E}(\gamma) \mathfrak{Q}_i \quad (1 \leq i \leq h).$$

It follows that \mathfrak{J} has an isolated primary component \mathfrak{Q}_i of rank $r + 1$ whose associated prime is $\mathcal{E}(\gamma) \mathfrak{P}_i$, and on localizing at this prime, we see that $\mathfrak{Q}_i \subseteq \mathcal{E}(\gamma) \mathfrak{Q}_i$ ($1 \leq i \leq h$). As $\mathcal{E}(\gamma) \mathfrak{P}_1, \dots, \mathcal{E}(\gamma) \mathfrak{P}_h$ are all different, it follows from Lemmas A2 and A4 of the Appendix that

$$\delta_{j+e}(\mathfrak{J}) \geq \sum_{i=1}^h \delta_{j+e}(\mathfrak{Q}_i) \geq \sum_{i=1}^h \delta_{j+e}(\mathcal{E}(\gamma) \mathfrak{Q}_i).$$

Substituting this into (4.1) and using (4.2), we obtain the desired conclusion

$$\delta_j(\mathfrak{P}) \leq A \delta_j(\mathcal{E}(\gamma) \mathfrak{P}).$$

This completes the proof of Lemma 5.

We remark that the lower bound $\delta_j(\mathfrak{P}) \geq A^{-1} \delta_j(\mathcal{E}(\gamma) \mathfrak{P})$ follows immediately by applying the lemma with $-\gamma$ instead of γ . However, it is possible to prove the exact equality $\delta_j(\mathfrak{P}) = \delta_j(\mathcal{E}(\gamma) \mathfrak{P})$ provided the projective embeddings of G_1, \dots, G_k are sufficiently well-behaved; this observation is due to Moreau [13] in the case $k = 1$.

5. Connectivity estimates

This section is concerned with the connectivity of certain stabilizers in \mathcal{X} . Let G_1, \dots, G_k be as in Sect. 1, not necessarily disjoint, with $G = G_1 \times \dots \times G_k$ embedded in \mathcal{X} . For any subset V of \mathcal{X} with $V_G = G \cap V$ non-empty, we write $\text{stab}_G V$ for the set of elements g in G such that $g + V_G = V_G$. This is clearly a subgroup of G . If $V = \overline{V}$ it is even an algebraic subgroup; for example, it can be seen using (1.4) that in this case

$$\text{stab}_G V = G \cap \overline{V_G - v},$$

where the second intersection is taken over all v in V_G (see also [1] p. 97).

For any algebraic subgroup H of G , let H_0 be the neutral connected component of H ; that is, the component of H through the origin of G , and write $\kappa(H) = [H : H_0]$ for the total number of connected components of H . We make a further definition if in fact G_1, \dots, G_k are disjoint. In this case H_0 has the form $H_1 \times \dots \times H_k$, where H_1, \dots, H_k are connected algebraic subgroups of G_1, \dots, G_k respectively. We say that H has type $\mathbf{s} = (s_1, \dots, s_k)$ if H_i is of codimension s_i in G_i ($1 \leq i \leq k$).

Finally we say that a subset S of G is defined in G by multihomogeneous polynomials P_1, \dots, P_m in the associated polynomial ring \mathfrak{R} if G intersects the

variety of the ideal (P_1, \dots, P_m) exactly in S . Recall the integers n_1, \dots, n_k , with $n = n_1 + \dots + n_k$, and put

$$h_i = N_i - n_i \quad (1 \leq i \leq k)$$

with

$$\mathbf{h} = (h_1, \dots, h_k), \quad h = |\mathbf{h}| = h_1 + \dots + h_k = N - n.$$

For integers d_1, \dots, d_k with $\mathbf{d} = (d_1, \dots, d_k)$ we put $C(\mathbf{d}) = 0$ if $d_i < 0$ for some i with $1 \leq i \leq k$, and otherwise we let $C(\mathbf{d})$ be the multinomial coefficient

$$C(\mathbf{d}) = (d_1 + \dots + d_k)! / (d_1! \dots d_k!).$$

Lemma 6. *For integers $D_1 \geq 1, \dots, D_k \geq 1$ let S be a subset of G defined in G by multihomogeneous polynomials in \mathfrak{R} of multidegrees at most (D_1, \dots, D_k) . For $0 \leq r \leq n$ let V be an irreducible component of \bar{S} , of codimension r in \bar{G} , with associated prime ideal \mathfrak{P} . Assume $G \cap V$ is non-empty, and let $H = \text{stab}_G V$. Then the codimension s of H in G satisfies $r \leq s \leq n$, and there exists $\mathbf{j} = (j_1, \dots, j_k)$ in $\mathcal{N}(h+s)$ such that*

$$\kappa(H) \leq a_1^{N_1 - j_1} \dots a_k^{N_k - j_k} \sum C(\mathbf{d}) \delta_{\mathbf{j} - \mathbf{d}}(\mathfrak{P}) D_1^{d_1} \dots D_k^{d_k}, \tag{5.1}$$

where the sum extends over all $\mathbf{d} = (d_1, \dots, d_k)$ with $|\mathbf{d}| = s - r$. In addition, if G_1, \dots, G_k are disjoint, we can suppose that $\mathbf{j} - \mathbf{h}$ is the type of H .

Proof. The definition of H shows that

$$H = \bigcap (V_G - v),$$

where the intersection is taken over all v in V_G . Let \mathcal{O} be a non-empty open subset of V_G , to be chosen shortly. We note that even

$$H = \bigcap (V_G - v) \tag{5.2}$$

where the intersection is taken only over v in \mathcal{O} . For suppose that x is in $V_G - v$ for all v in \mathcal{O} . Then $\mathcal{O} \subseteq V_G - x$. Taking the closure gives $V \subseteq \overline{V_G - x}$, and intersecting with G using (1.4), (1.5) yields $V_G \subseteq V_G - x$. It follows that

$$\overline{V_G}, \quad \overline{V_G + x}, \quad \overline{V_G + 2x}, \dots$$

is a non-increasing sequence of closed sets in \mathcal{X} . So by the Noetherian property there exists a non-negative integer l such that

$$\overline{V_G + lx} = \overline{V_G + (l+1)x},$$

and once again use of (1.4), (1.5) leads to $V_G = V_G + x$. So x lies in $H = \text{stab}_G V$. Since x was arbitrary, this proves (5.2).

Next, a similar appeal to the Noetherian property of \mathcal{X} shows that we can find a positive integer m and elements v_0, \dots, v_m of \mathcal{O} such that

$$H = \bigcap_{i=0}^m (V_G - v_i). \tag{5.3}$$

Let H_0 be the neutral connected component of H . We can find a subset R of H , of cardinality $\kappa(H)$, such that

$$H = \bigcup (\rho + H_0),$$

where the union is taken over all ρ in R and the $H_\rho = \rho + H_0$ are all the connected components of H . Thus for each ρ in R the set H_ρ is a component of the right-hand side of (5.3) in an appropriate sense. We shall soon choose the set \mathcal{O} such that each H_ρ is even a component of

$$(V_G - v_0) \cap \bigcap_{i=0}^m (S - v_i). \tag{5.4}$$

We first define an open subset $\tilde{\mathcal{O}}$ of V as follows. If V is the only irreducible component of \bar{S} meeting G , put $\tilde{\mathcal{O}} = V$; otherwise let

$$\tilde{\mathcal{O}} = V \setminus T, \tag{5.5}$$

where

$$T = \bigcup \overline{W_G - \rho}$$

with the union taken over all ρ in R and all those irreducible components $W \neq V$ of \bar{S} that meet G .

Next we verify that $\tilde{\mathcal{O}}$ is non-empty. This is trivial if V is the only component of \bar{S} meeting G . Otherwise, suppose (5.5) holds and $\tilde{\mathcal{O}}$ is empty. Then $V \subseteq T$. Since V is irreducible, it follows that

$$V \subseteq \overline{W_G - \rho} \tag{5.6}$$

for some ρ in R and some component $W \neq V$ of \bar{S} meeting G . In particular $W \subseteq \bar{G}$, and so intersecting (5.6) with G using (1.4), (1.5) gives $V_G \subseteq W_G - \rho$. Thus $\rho + V_G \subseteq W_G$. But $\rho + V_G = V_G$ since ρ is in $H = \text{stab}_G V$. Hence $V_G \subseteq W_G$, and now taking the closure gives $V \subseteq W$, which is not possible as V, W are different components of \bar{S} . Thus indeed $\tilde{\mathcal{O}}$ is a non-empty open subset of V .

Therefore

$$\mathcal{O} = G \cap \tilde{\mathcal{O}} = V_G \cap \tilde{\mathcal{O}}$$

is a non-empty open subset of V_G .

Having thus chosen \mathcal{O} and v_0, \dots, v_m , we proceed to interpret the assertion about (5.4) in terms of ideals, and then prove it. Let Γ be the subgroup of G generated by v_0, \dots, v_m and the elements of R , and for γ in Γ write $E(\gamma), \mathcal{E}(\gamma)$ for the corresponding operators defined in Sect. 2. Let \mathfrak{I} be the ideal generated by $\mathcal{E}(v_0)\mathfrak{P}$ together with the polynomials $E(v_0)P, \dots, E(v_m)P$ as P runs over the given polynomials defining S in G . Further for each ρ in R let \mathfrak{P}_ρ be the associated prime ideal of H_ρ , and let $\mathfrak{I}^{(\rho)}$ be the contracted extension of \mathfrak{I} with respect to ρ . We shall eventually show that \mathfrak{P}_ρ is a prime component of $\mathfrak{I}^{(\rho)}$ with the same rank as $\mathfrak{I}^{(\rho)}$.

To start with, we shall verify that

$$\mathfrak{I} \subseteq \mathfrak{P}_\rho \tag{5.7}$$

for any ρ in R . From (5.3) we have $\overline{H}_\rho \subseteq \overline{V_G - v_0}$, whence $\mathcal{E}(v_0)\mathfrak{P} \subseteq \mathfrak{P}_\rho$ by Lemma 2. To prove (5.7) it therefore suffices to show that $Q = E(v_i)P$ lies in \mathfrak{P}_ρ for any i with $0 \leq i \leq m$ and any multihomogeneous polynomial P vanishing on S . Let \mathcal{O}_i be an open subset of G containing Γ on which $E(v_i)$ represents translation by v_i . Since \mathcal{O}_i contains $\rho + v_i$, the set

$$\mathcal{O}_{i,\rho} = (\mathcal{O}_i - v_i) \cap H_\rho$$

is a non-empty open subset of H_ρ . Let h be an arbitrary point of $\mathcal{O}_{i,\rho}$. Then $v_i + h$ lies in

$$V_G + h = V_G \subseteq G \cap \overline{S} = S.$$

Consequently P vanishes at $v_i + h$. Since $v_i + h$ is in \mathcal{O}_i , it follows that $Q = E(v_i)P$ vanishes at h . Since h was arbitrary, Q vanishes on $\overline{\mathcal{O}_{i,\rho}} = \overline{H}_\rho$, and so lies in \mathfrak{P}_ρ . This completes the proof of (5.7), and by localizing at ρ we deduce that

$$\mathfrak{Z}^{(\rho)} \subseteq \mathfrak{P}_\rho. \tag{5.8}$$

This does not quite imply that \mathfrak{P}_ρ is a prime component of $\mathfrak{Z}^{(\rho)}$. To prove this, fix any prime component \mathfrak{P}' of $\mathfrak{Z}^{(\rho)}$ with the same rank as $\mathfrak{Z}^{(\rho)}$. By (5.8) \mathfrak{P}' exists, as $\mathfrak{Z}^{(\rho)} \neq \mathfrak{R}$. Let V' be the variety of \mathfrak{P}' in \mathcal{X} , and fix an arbitrary integer i with $0 \leq i \leq m$. Since V' contains ρ , the set $\mathcal{O}'_i = V' \cap \mathcal{O}_i$ is a non-empty open subset of V' . Pick an arbitrary v' in \mathcal{O}'_i , and let P be chosen arbitrarily from the collection of given polynomials defining S in G . Then $Q = E(v_i)P$ lies in \mathfrak{Z} and so in \mathfrak{P}' . So Q vanishes at v' , and it follows that P vanishes at $v' + v_i$. Since P was arbitrary, we deduce that $v' + v_i$ lies in

$$G \cap \overline{S} = \bigcup W_G,$$

where the union is taken over all irreducible components W of \overline{S} meeting G . Hence v' lies in $\bigcup (W_G - v_i)$. As v' was arbitrary, we get $\mathcal{O}'_i \subseteq \bigcup (W_G - v_i)$, and taking the closure gives $V' \subseteq \bigcup \overline{W_G - v_i}$. Therefore $V' \subseteq \overline{W_G - v_i}$ for some W , whence intersecting with G yields

$$V'_G \subseteq W_G - v_i. \tag{5.9}$$

In particular ρ lies in $W_G - v_i$, so v_i lies in $W_G - \rho$. Now our choice of \mathcal{O} implies that $W = V$. This is trivial if V is the only component of \overline{S} meeting G ; otherwise suppose $W \neq V$. Then v_i lies in the set T , contradicting the fact that it lies in $\mathcal{O} \subseteq \overline{\mathcal{O}}$. We conclude from (5.9) that

$$V'_G \subseteq V_G - v_i.$$

Since i was arbitrary, it follows from (5.3) that $V'_G \subseteq H$. Taking the closure, we get $V' \subseteq \bigcup \overline{H}_\sigma$, where the union is taken over all σ in R . Thus

$$V' \subseteq \overline{H}_\sigma \tag{5.10}$$

for some σ in R , and since H_σ is closed in G , we get $V'_G \subseteq H_\sigma$. As ρ is in V'_G , it follows that in fact $\sigma = \rho$. Now we conclude from (5.10) that $V' \subseteq \overline{H}_\rho$.

So in terms of ideals we have $\mathfrak{P}_\rho \subseteq \mathfrak{P}'$. Thus the rank of \mathfrak{P}_ρ is at most the rank of \mathfrak{P}' , which by assumption is the rank of $\mathfrak{I}^{(\rho)}$. The opposite inequality follows from (5.8). Hence \mathfrak{P}_ρ is indeed a prime component of $\mathfrak{I}^{(\rho)}$ of the same rank as $\mathfrak{I}^{(\rho)}$ (and in fact $\mathfrak{P}_\rho = \mathfrak{P}'$, so it is the only such component; but we don't need this).

Now let $s \leq n$ be the codimension of H in G . Then the ideal \mathfrak{P}_ρ has rank $h+s$ for each ρ in R . So each $\mathfrak{I}^{(\rho)}$ has rank $h+s$. Let \mathfrak{I}^* be the contracted extension of \mathfrak{I} with respect to all the points of R simultaneously. Then \mathfrak{I}^* also has rank $h+s$, and it has a prime component \mathfrak{P}_ρ for each ρ in R . It follows that the radical

$$\sqrt{\mathfrak{I}^*} = \sqrt{(\mathfrak{I}^*)} = (\sqrt{\mathfrak{I}})^*$$

also has rank $h+s$ and prime components \mathfrak{P}_ρ for each ρ in R . Thus we have by Lemma A2 of the Appendix

$$\sum \delta_j(\mathfrak{P}_\rho) \leq \delta_j(\sqrt{\mathfrak{I}^*}) \tag{5.11}$$

for any \mathbf{j} in $\mathcal{N}(h+s)$, where the sum is taken over all ρ in R . We proceed to estimate the right-hand side of (5.11). This could be done using a suitable degree theory for quasiprojective varieties in \mathcal{X} , but we prefer instead to apply the considerations of the Appendix directly to radical ideals. For this we recall that an ideal is said to be quasi-unmixed if all its isolated components have the same rank.

Now we have $\mathfrak{I} = (\mathfrak{P}_0, \mathfrak{Q})$, where $\mathfrak{P}_0 = \mathcal{E}(\gamma_0) \mathfrak{P}$ and \mathfrak{Q} is generated by the polynomials $E(v_0)P, \dots, E(v_m)P$ of multidegrees at most $(a_1 D_1, \dots, a_k D_k)$. In particular the rank of \mathfrak{I} is at least the rank $h+r$ of \mathfrak{P}_0 , and so $h+s \geq h+r$. Thus $r \leq s \leq n$. We now inductively construct ideals $\mathfrak{I}_0, \dots, \mathfrak{I}_{s-r}$ such that

- (i)_l $\mathfrak{P}_0 \subseteq \mathfrak{I}_l \subseteq \mathfrak{I}$ ($0 \leq l \leq s-r$)
- (ii)_l The ideal \mathfrak{I}_l^* is quasi-unmixed of rank $h+r+l$ ($0 \leq l \leq s-r$)
- (iii)_l For any \mathbf{j} in $\mathcal{N}(h+r+l)$ we have

$$\delta_j(\sqrt{\mathfrak{I}_l^*}) \leq \sum C(\mathbf{d}) \delta_{\mathbf{j}-\mathbf{d}}(\mathfrak{P}_0) (a_1 D_1)^{d_1} \dots (a_k D_k)^{d_k} \quad (0 \leq l \leq s-r),$$

where the sum is taken over all $\mathbf{d} = (d_1, \dots, d_k)$ with $|\mathbf{d}| = l$.

For $l=0$ we take $\mathfrak{I}_0 = \mathfrak{P}_0$. Since $\mathfrak{P}_0^* \subseteq \mathfrak{I}^*$ we have $\mathfrak{P}_0^* \neq \mathfrak{R}$, and so $\mathfrak{P}_0^* = \mathfrak{P}_0$. Thus (i)₀ and (ii)₀ are clear. Also $\sqrt{\mathfrak{I}_0^*} = \mathfrak{P}_0$, so that (iii)₀ is obvious. So we are finished if $s=r$. Henceforth assume $s > r$ and that for some l with $0 \leq l < s-r$ we have found \mathfrak{I}_l satisfying (i)_l, (ii)_l and (iii)_l. We proceed to construct \mathfrak{I}_{l+1} satisfying (i)_{l+1}, (ii)_{l+1} and (iii)_{l+1}.

Firstly, note that since \mathfrak{I}_l^* is quasi-unmixed of rank $h+r+l$, its radical $\sqrt{\mathfrak{I}_l^*}$ is unmixed of rank $h+r+l$. Let \mathfrak{Q} be any prime component of $\sqrt{\mathfrak{I}_l^*}$. Then \mathfrak{Q} is of rank $h+r+l$ and $\mathfrak{Q}^* = \mathfrak{Q}$. Now $\mathfrak{Q} \not\subseteq \mathfrak{I}_l$, otherwise, since $\mathfrak{P}_0 \subseteq \mathfrak{I}_l \subseteq \sqrt{\mathfrak{I}_l^*} \subseteq \mathfrak{Q}$ we should deduce $\mathfrak{I} = (\mathfrak{P}_0, \mathfrak{Q}) \subseteq \mathfrak{Q}$ and so $\mathfrak{I}^* \subseteq \mathfrak{Q}$, which is impossible on comparing ranks. Hence at least one of the generators of \mathfrak{Q} is not in \mathfrak{I}_l . The usual techniques (cf. Sect. 7) now enable us to find a multihomogeneous polynomial Q of \mathfrak{Q} , of multidegree exactly $(a_1 D_1, \dots, a_k D_k)$, which does not lie in any of the prime components of $\sqrt{\mathfrak{I}_l^*}$. We put $\mathfrak{I}_{l+1} = (\mathfrak{I}_l, Q)$. Then

(i)_{l+1} is obvious, as

$$\mathfrak{P}_0 \subseteq \mathfrak{I}_l \subseteq \mathfrak{I}_{l+1} \subseteq (\mathfrak{I}, \mathfrak{Q}) = \mathfrak{I}.$$

Also $\sqrt{\mathfrak{I}_l^*} : (\mathfrak{Q}) = \sqrt{\mathfrak{I}_l^*}$, and so the ideal $\mathfrak{I} = (\sqrt{\mathfrak{I}_l^*}, \mathfrak{Q})$ has rank $h+r+l+1$. Furthermore, for any \mathbf{j} in $\mathcal{N}(h+r+l+1)$ we have by Lemma A5

$$\delta_{\mathbf{j}}(\mathfrak{I}) = \sum_{i=1}^k a_i D_i \delta_{\mathbf{j}-\mathbf{e}_i}(\sqrt{\mathfrak{I}_l^*}),$$

where $\mathbf{e}_1, \dots, \mathbf{e}_k$ are the standard basis vectors of \mathbf{Z}^k . From (iii)_l this gives easily

$$\delta_{\mathbf{j}}(\mathfrak{I}) \leq \sum C(\mathbf{d}) \delta_{\mathbf{j}-\mathbf{d}}(\mathfrak{P}_0) (a_1 D_1)^{d_1} \dots (a_k D_k)^{d_k} \tag{5.12}$$

where the sum is over all $\mathbf{d} = (d_1, \dots, d_k)$ with $|\mathbf{d}| = l+1$.

Next by Satz 57 (p. 170) of [8] the ideal $\mathfrak{R} = (\mathfrak{I}_l^*, \mathfrak{Q})$ is quasi-unmixed of rank $h+r+l+1$. So either $\mathfrak{R}^* = \mathfrak{R}$ or \mathfrak{R}^* is also quasi-unmixed of rank $h+r+l+1$. But as $\mathfrak{R} \subseteq \mathfrak{I}_{l+1}^* \subseteq \mathfrak{I}^*$ we see that $\mathfrak{R}^* \subseteq \mathfrak{I}^*$; thus $\mathfrak{R}^* \neq \mathfrak{R}$. Hence \mathfrak{R}^* is quasi-unmixed of rank $h+r+l+1$. But it is easily seen that $\mathfrak{I}_{l+1}^* = \mathfrak{R}^*$; and this proves (ii)_{l+1}. Finally (iii)_{l+1} is immediate from (5.12) using Lemma A4 and the inclusions

$$\mathfrak{I} = (\sqrt{\mathfrak{I}_l^*}, \mathfrak{Q}) \subseteq \sqrt{(\mathfrak{I}_l^*, \mathfrak{Q})} \subseteq \sqrt{(\mathfrak{I}_l, \mathfrak{Q})^*} = \sqrt{\mathfrak{I}_{l+1}^*},$$

since $\mathfrak{I}, \sqrt{\mathfrak{I}_{l+1}^*}$ have the same ranks.

This completes the inductive construction of $\mathfrak{I}_0, \dots, \mathfrak{I}_{s-r}$. Now we note that $\sqrt{\mathfrak{I}_{s-r}^*} \subseteq \sqrt{\mathfrak{I}^*}$ and that these ideals have the same rank $h+s$. Hence from (5.11) and the estimate (iii)_{s-r} we get finally for any \mathbf{j} in $\mathcal{N}(h+s)$

$$\sum \delta_{\mathbf{j}}(\mathfrak{P}_\rho) \leq \sum C(\mathbf{d}) \delta_{\mathbf{j}-\mathbf{d}}(\mathfrak{P}_0) (a_1 D_1)^{d_1} \dots (a_k D_k)^{d_k}, \tag{5.13}$$

where the first sum is over all ρ in R and the second sum is over all $\mathbf{d} = (d_1, \dots, d_k)$ with $|\mathbf{d}| = s-r$.

Now let σ be the element of R giving rise to $H_\sigma = H_0$. By Lemma A1 of the Appendix there exists \mathbf{j} in $\mathcal{N}(h+s)$ such that

$$\delta_{\mathbf{j}}(\mathfrak{P}_\sigma) > 0. \tag{5.14}$$

But from Lemma 2 we have $\mathfrak{P}_\rho = \mathcal{E}(\sigma - \rho) \mathfrak{P}_\sigma$; therefore by Lemma 5 we have $\delta_{\mathbf{j}}(\mathfrak{P}_\rho) > 0$ for all ρ in R . So $\delta_{\mathbf{j}}(\mathfrak{P}_\rho) \geq 1$ for all ρ in R , and now (5.13) gives the required estimate (5.1) for the cardinality $\kappa(H)$ of R , after using once more Lemma 5 to replace $\mathfrak{P}_0 = \mathcal{E}(\gamma_0) \mathfrak{P}$ by \mathfrak{P} . This proves Lemma 6 without the disjointness condition.

Finally if G_1, \dots, G_k are disjoint then we can be more specific about the \mathbf{j} satisfying (5.14). For if $\mathbf{s} = (s_1, \dots, s_k)$ is the type of H , we have $H_\sigma = H_1 \times \dots \times H_k$ where H_i is a connected algebraic subgroup of G_i of codimension s_i ($1 \leq i \leq k$). Thus we have

$$\mathfrak{P}_\sigma = (\mathfrak{I}_1, \dots, \mathfrak{I}_k),$$

where \mathfrak{I}_i in $K[X_{i,0}, \dots, X_{i,N_i}]$ is the homogeneous ideal of rank $h_i + s_i$ associated with H_i ($1 \leq i \leq k$). It follows from Lemma A6 of the Appendix that

$$\delta_{\mathbf{h}+\mathbf{s}}(\mathfrak{P}_\sigma) = \delta_1 \dots \delta_k > 0,$$

where δ_i is the degree of \mathfrak{F}_i ($1 \leq i \leq k$). Hence (5.14), and therefore also the estimate (5.1) for $\kappa(H)$, holds with $\mathbf{j} = \mathbf{h} + \mathbf{s}$. This completes the proof of Lemma 6.

6. The Proposition

In this section we state a Proposition and we show that it implies our Main Theorems. Let G_1, \dots, G_k be as in Sect. 1, not necessarily disjoint. Let X be a finite subset of $G = G_1 \times \dots \times G_k$ containing the origin, and take Γ as the subgroup of G generated by the elements of X . For an ideal \mathfrak{F} of the associated polynomial ring \mathfrak{R} let \mathfrak{F}^* denote the contracted extension with respect to Γ . Recall that for each i with $1 \leq i \leq k$ the number $h_i = N_i - n_i$ is such that either $h_i = 0$ or the prime ideal \mathfrak{G}_i of G_i in $\mathfrak{R}_i = K[X_{i,0}, \dots, X_{i,N_i}]$ is of rank $h_i \geq 1$. In the former case we set $b_i = 0$ and we let \mathfrak{F}_i be the zero ideal of \mathfrak{R}_i . In the latter case we let $b_i \geq 1$ be an integer such that the Zariski closure of G_i in \mathbb{P}_{N_i} can be defined by the vanishing of homogeneous polynomials in \mathfrak{R}_i of degrees at most b_i . Also by Lemma 6 (p. 499) of [4] we can find h_i homogeneous polynomials in \mathfrak{R}_i which generate an ideal \mathfrak{F}_i with $\mathfrak{F}_i^* = \mathfrak{G}_i$.

Next, if $h = h_1 + \dots + h_k = 0$, we write $\mathfrak{F}_0 = 0$. Otherwise, if $h \geq 1$ we write

$$\mathfrak{F}_0 = (\mathfrak{F}_1, \dots, \mathfrak{F}_k);$$

then this ideal is generated by h multihomogeneous polynomials of \mathfrak{R} , say P_1, \dots, P_h . In either case we note that $\mathfrak{F}_0^* = \mathfrak{G}$; this is trivial if $h = 0$, while if $h \geq 1$ then on the one hand

$$\mathfrak{F}_i \subseteq \mathfrak{F}_i^* = \mathfrak{G}_i \subseteq \mathfrak{G} \quad (1 \leq i \leq k)$$

so that $\mathfrak{F}_0 \subseteq \mathfrak{G}$ whence $\mathfrak{F}_0^* \subseteq \mathfrak{G}^* = \mathfrak{G}$, and on the other hand

$$\mathfrak{F}_0^* = (\mathfrak{F}_1, \dots, \mathfrak{F}_k)^* \supseteq (\mathfrak{F}_1^*, \dots, \mathfrak{F}_k^*) = (\mathfrak{G}_1, \dots, \mathfrak{G}_k) = \mathfrak{G}.$$

Furthermore, if $h \geq 1$ the rank of \mathfrak{F}_0^* is h , and we deduce by applying Lemma A6 of the Appendix to those \mathfrak{F}_i with $h_i \neq 0$ and using Lemma 5 (p. 499) of [4] that

$$\delta_{\mathbf{h}}(\mathfrak{F}_0^*) \leq b_1^{h_1} \dots b_k^{h_k} \tag{6.1}$$

while

$$\delta_{\mathbf{j}}(\mathfrak{F}_0^*) = 0 \tag{6.2}$$

for any $\mathbf{j} \neq \mathbf{h}$.

The main result of this section shows how to construct polynomials $P_{h+1}, \dots, P_{h+n+1}$ to get a local complete intersection. We take G_1, \dots, G_k, Φ, X satisfying the conditions of either version of the Main Theorem, and we suppose that for some integers $D_1 \geq 1, \dots, D_k \geq 1$ and $T \geq 1$ there is a polynomial P of \mathfrak{R} also satisfying the conditions of the Main Theorem, with the constant c given by

$$c = (2a)^{n^2} b^{N-n} k^n, \tag{6.3}$$

where

$$a = \max(a_1, \dots, a_k), \quad b = \max(b_1, \dots, b_k).$$

Thus in the general version of the Main Theorem we do not assume that G_1, \dots, G_k are disjoint, and we have

$$TQ_r(X) \geq c \Delta_r \quad (1 \leq r \leq n) \tag{6.4}$$

and if $n > 1$ also

$$EQ_r(X) \geq c \Delta_r \quad (1 \leq r < n). \tag{6.5}$$

Furthermore we have either

$$EQ_n(X) \geq c \Delta_n \tag{6.6}$$

or

$$|X/G_{\text{tors}}| = |X|, \tag{6.7}$$

and we shall refer to these as cases Ig, IIg respectively.

In the disjoint version of the Main Theorem, we assume that G_1, \dots, G_k are mutually disjoint. For $\mathbf{r} = (r_1, \dots, r_k)$ we abbreviate $Q_{r_1, \dots, r_k}(X)$ to $Q_{\mathbf{r}}(X)$ and $D_1^{r_1} \dots D_k^{r_k}$ to $D^{\mathbf{r}}$. We put $\mathbf{n} = (n_1, \dots, n_k)$. Then we have

$$TQ_{\mathbf{r}}(X) \geq c D^{\mathbf{r}} \quad (0 \leq r_1 \leq n_1, \dots, 0 \leq r_k \leq n_k, |\mathbf{r}| \geq 1) \tag{6.8}$$

and if $n > 1$ also

$$EQ_{\mathbf{r}}(X) \geq c D^{\mathbf{r}} \quad (0 \leq r_1 \leq n_1, \dots, 0 \leq r_k \leq n_k, |\mathbf{r}| \geq 1, \mathbf{r} \neq \mathbf{n}). \tag{6.9}$$

Furthermore we have either

$$EQ_{\mathbf{n}}(X) \geq c D^{\mathbf{n}} \tag{6.10}$$

or

$$|X/G_{\text{tors}}| = |X|, \tag{6.11}$$

and we shall refer to these as cases Id, IIId respectively.

Finally in the situation of either version of the Main Theorem we define

$$T' = \min(E, T/n)$$

and

$$T_r = T - (r - 1) T' \quad (1 \leq r \leq n).$$

Also in cases Ig, Id we put

$$T_{n+1} = T - n T'$$

whereas in cases IIg, IIId we put

$$T_{n+1} = T - (n - 1) T' - T/n.$$

We can now state our Proposition. We recall the multinomial coefficients $C(\mathbf{r})$ defined in Sect. 5, and we define $X^{(0)}$ as the origin of G .

Proposition. *Suppose, in addition to the above, that P vanishes at each point of Γ to finite (not necessarily positive) order along Φ . Then there are multihomogeneous polynomials $P_{n+1}, \dots, P_{n+n+1}$ of \mathfrak{R} which together with the ideals $\mathfrak{I}_r = (P_1, \dots, P_{n+r})$ satisfy*

- (i)_r, the multidegree of P_{h+r} is at most $(2a)^{r-1}(D_1, \dots, D_k)$ ($1 \leq r \leq n$)
- (ii)_r, P_{h+r} vanishes at each point of $X^{(n+1-r)}$ to order at least T_r along Φ ($1 \leq r \leq n+1$), with strict inequality if $r = n+1$.
- (iii)_r, the ideal \mathfrak{F}_r^* is of rank $h+r$ ($1 \leq r \leq n+1$)
- (iv)_r, for any \mathbf{j} in $\mathcal{N}(h+r)$ we have

$$\delta_{\mathbf{j}}(\mathfrak{F}_r^*) \leq C(\mathbf{j}-\mathbf{h})(2a)^{\frac{1}{2}r(r-1)}b^h D^{\mathbf{j}-\mathbf{h}} \quad (1 \leq r \leq n).$$

We prove this Proposition in the next section. But first we verify that it implies the Main Theorems with c given by (6.3). For if P satisfies the conditions of either version of the Main Theorem and also has finite order at each point of Γ , then we may apply the Proposition. We conclude from (iii)_{n+1} that the ideal \mathfrak{F}_{n+1}^* is multihomogeneous of rank $h+n+1 = N+1$; yet it vanishes at the origin $X^{(0)}$ of G , since by (ii)_{n+1} all the generators of \mathfrak{F}_{n+1} vanish there to order strictly greater than

$$T_{n+1} \geq T - (n-1)T' - T/n \geq 0.$$

But this is not possible; hence there is some g in Γ at which P vanishes to infinite order along Φ . It follows from the definition that P vanishes at $g + \Phi(z)$ for all z sufficiently small, and hence by analytic continuation it must vanish on all of $g + \Phi$.

7. Proof of Proposition

We carry over all the notation of the preceding section. We shall construct the desired polynomials $P_{h+1}, \dots, P_{h+n+1}$ by induction, starting with $r=1$. We take $P_{h+1} = P$; then (i)₁ and (ii)₁ are obvious. It remains to check (iii)₁ and (iv)₁. For this we note that P cannot lie in the prime ideal $\mathfrak{F}_0^* = \mathfrak{G}$, else it would vanish at all points of G to infinite order. If $h=0$ then $\mathfrak{F}_1 = (P)$, and since $X^{(n)}$ is non-empty we deduce $\mathfrak{F}_1^* \neq \mathfrak{R}$. Hence by Lemma 7 (p. 501) of [4] the rank of \mathfrak{F}_1^* is at most 1; so this rank must be exactly 1. This proves (iii)₁ in the case $h=0$. Also (iv)₁ is clear in this case from Lemma A4 of the Appendix since $(P) = \mathfrak{F}_1 \subseteq \mathfrak{F}_1^*$ and these ideals have the same ranks.

Next, still with $r=1$, assume $h \geq 1$. Then by Lemma A5 of the Appendix the ideal $\mathfrak{F} = (\mathfrak{F}_0^*, P)$ has rank $h+1$ and for any \mathbf{j} in $\mathcal{N}(h+1)$ we have

$$\delta_{\mathbf{j}}(\mathfrak{F}) \leq \sum_{i=1}^k D_i \delta_{\mathbf{j}-\mathbf{e}_i}(\mathfrak{F}_0^*).$$

By (6.2) this is non-zero only if $\mathbf{j}-\mathbf{e}_i = \mathbf{h}$ for some i with $1 \leq i \leq k$, and then (6.1) gives the estimate (iv)₁ with \mathfrak{F}_1^* replaced by \mathfrak{F} . Also

$$\mathfrak{F}_1^* = (\mathfrak{F}_0, P)^* \supseteq (\mathfrak{F}_0^*, P) = \mathfrak{F}. \tag{7.1}$$

Now $\mathfrak{F}_1^* \neq \mathfrak{R}$ since the generators of \mathfrak{F}_1 vanish on the non-empty set $X^{(n)}$; thus by (7.1) the rank of \mathfrak{F}_1^* is at least $h+1$. But by Lemma 7 of [4] this rank is also at most $h+1$. We deduce (iii)₁ for $h \geq 1$, and now (iv)₁ follows from Lemma A4,

the inclusion (7.1), and the estimate for $\delta_j(\mathfrak{I})$. This completes the construction of P_{h+1} .

Next suppose that for some r with $1 \leq r \leq n$ the polynomials P_{h+1}, \dots, P_{h+r} have been constructed to satisfy the conditions (i)_r, (ii)_r, (iii)_r, (iv)_r of the Proposition. We shall construct P_{h+r+1} so that the conditions (i)_{r+1}, (ii)_{r+1}, (iii)_{r+1}, (iv)_{r+1} hold.

Since by (iii)_r the rank of \mathfrak{I}_r^* is $h+r$, it is unmixed by Lemma 7 of [4]. Fix an arbitrary prime component \mathfrak{P} of \mathfrak{I}_r^* ; this is then multihomogeneous of rank $h+r$ and special in the sense of Sect. 2. Thus the variety V of \mathfrak{P} in \mathcal{X} passes through some γ in Γ . We shall eventually prove that there exists x in X and an integer t with $0 \leq t < T_r - T_{r+1}$ such that

$$\Delta^t(\mathcal{E}(x)\mathfrak{I}_r^*) \not\subseteq \mathfrak{P}. \tag{7.2}$$

For suppose (7.2) is false. Then for all x in X we have

$$\Delta^t(\mathcal{E}(x)\mathfrak{I}_r^*) \subseteq \mathfrak{P} \quad (0 \leq t < T_r - T_{r+1}). \tag{7.3}$$

By (iv) of Lemma 1 the ideal $\mathfrak{I} = \mathcal{E}(x)\mathfrak{I}_r^*$ is unmixed of rank $h+r$. Since \mathfrak{P} contains P and by hypothesis $\text{ord}_\gamma P$ is finite, so is $\text{ord}_\gamma \mathfrak{P}$. Since V passes through γ , we have in fact $\text{ord}_\gamma \mathfrak{P} > 0$. Hence we may apply Lemma 4. It follows that \mathfrak{I} has a primary component \mathfrak{Q} of length at least $T_r - T_{r+1}$ whose associated prime is \mathfrak{P} . In particular $\mathfrak{I} \subseteq \mathfrak{Q}$, whence $\mathfrak{I}_r^* \subseteq \mathcal{E}(-x)\mathfrak{Q}$. Comparing ranks, we see that \mathfrak{I}_r^* must have a primary component $\mathfrak{Q}_x \subseteq \mathcal{E}(-x)\mathfrak{Q}$ whose associated prime is $\mathfrak{E}(-x)\mathfrak{P}$. Furthermore the length l_x of \mathfrak{Q}_x is at least the length of $\mathcal{E}(-x)\mathfrak{Q}$; and so by (iv) of Lemma 1 we conclude that $l_x \geq T_r - T_{r+1}$.

Thus on our hypothesis (7.3) we see that for each x in X the ideal \mathfrak{I}_r^* has a primary component of length at least $T_r - T_{r+1}$ whose associated prime is $\mathcal{E}(-x)\mathfrak{P}$. We now define an equivalence relation on X by saying that x, x' in X are equivalent if $\mathcal{E}(-x)\mathfrak{P} = \mathcal{E}(-x')\mathfrak{P}$. Suppose X splits into $M \geq 1$ non-empty equivalence classes X_1, \dots, X_M under this relation. Pick x_1, \dots, x_M in X_1, \dots, X_M respectively. Then the ideals $\mathcal{E}(-x_1)\mathfrak{P}, \dots, \mathcal{E}(-x_M)\mathfrak{P}$ are different. So the above conclusion yields for any \mathbf{i} in $\mathcal{N}(h+r)$ the inequality

$$(T_r - T_{r+1}) \sum_{m=1}^M \delta_{\mathbf{i}}(\mathcal{E}(-x_m)\mathfrak{P}) \leq \delta_{\mathbf{i}}(\mathfrak{I}_r^*).$$

Using Lemma 5 we deduce

$$M(T_r - T_{r+1}) \delta_{\mathbf{i}}(\mathfrak{P}) \leq a^{n-r} \delta_{\mathbf{i}}(\mathfrak{I}_r^*),$$

and so by (iv)_r,

$$M(T_r - T_{r+1}) \delta_{\mathbf{i}}(\mathfrak{P}) \leq a^{n-r} (2a)^{\frac{1}{2}r(r-1)} b^h C(\mathbf{i} - \mathbf{h}) D^{\mathbf{i} - \mathbf{h}}. \tag{7.4}$$

This holds for all \mathbf{i} in $\mathcal{N}(h+r)$; but from our convention on $\delta_{\mathbf{i}}(\mathfrak{P})$ it actually holds for all \mathbf{i} in \mathbb{Z}^h .

We now study more carefully the above equivalence relation in order to obtain a lower bound for M in terms of the quantities $Q_s(X)$ or $Q_s(X)$. If x, x'

in X are equivalent then $\mathcal{E}(x-x')\mathfrak{P}=\mathfrak{P}$ and so $x-x'$ is in the stabilizer $H=\text{stab}_G V$ of V in G , by Lemma 2. In particular, $X_m-x_m\subseteq H$ ($1\leq m\leq M$). Also if $x-x_m, x'-x_m$ are elements of X_m-x_m in the same connected component of H , then $x-x'=(x-x_m)-(x'-x_m)$ is in the neutral component H_0 of H . It follows that

$$|X_m/H_0|\leq\kappa(H) \quad (1\leq m\leq M),$$

and consequently

$$|X/H_0|\leq M\kappa(H). \tag{7.5}$$

We estimate the right-hand side by introducing the subset S of G defined in G by the polynomials P_{h+1}, \dots, P_{h+r} of multidegrees at most $(2a)^{r-1}(D_1, \dots, D_k)$. Since the closure \bar{S} is defined by the ideal

$$\mathfrak{I}=(\mathfrak{G}, P_{h+1}, \dots, P_{h+r})=(\mathfrak{G}, \mathfrak{I}_r)$$

and since

$$\mathfrak{I}_r^*=(\mathfrak{G}, \mathfrak{I}_r^*)^*\supseteq\mathfrak{I}^*\supseteq(\mathfrak{G}^*, \mathfrak{I}_r^*)=(\mathfrak{G}, \mathfrak{I}_r^*)=\mathfrak{I}_r^*$$

we see that $\mathfrak{I}^*=\mathfrak{I}_r^*$. Hence \mathfrak{P} is a prime component of \mathfrak{I}^* , and therefore also of \mathfrak{I} . Thus V is an irreducible component of \bar{S} , and its codimension in G is r . We now split cases according to whether we are considering the general or the disjoint version of the Main Theorem.

Suppose first that we are in the situation of the general version of the Main Theorem. Let s be the codimension of H in G ; then by Lemma 6 we have $r\leq s\leq n$ and there exists \mathbf{j} in $\mathcal{N}(h+s)$ such that

$$\kappa(H)\leq a^{n-r}(2a)^{r(n-r)}\sum C(\mathbf{d})\delta_{\mathbf{j}-\mathbf{d}}(\mathfrak{P})D^{\mathbf{d}},$$

where the sum is taken over all \mathbf{d} with $|\mathbf{d}|=s-r$. By (7.5) and the definition of $Q_s(X)$ this gives

$$Q_s(X)\leq M a^{n-r}(2a)^{r(n-r)}\sum C(\mathbf{d})\delta_{\mathbf{j}-\mathbf{d}}(\mathfrak{P})D^{\mathbf{d}}. \tag{7.6}$$

So combining this with (7.4) yields

$$(T_r-T_{r+1})Q_s(X)\leq A_r b^h D^s \sum C(\mathbf{d})C(\mathbf{s}-\mathbf{d}) \tag{7.7}$$

where

$$\mathbf{s}=(s_1, \dots, s_k)=\mathbf{j}-\mathbf{h}$$

and

$$A_r=a^{2(n-r)}(2a)^{r(n-r)}(2a)^{\frac{1}{2}r(r-1)}.$$

By considering suitable generating functions it is easy to see that

$$\sum C(\mathbf{d})C(\mathbf{s}-\mathbf{d})=C(\mathbf{s})\leq k^s\leq k^n. \tag{7.8}$$

In particular (7.7) then implies $C(\mathbf{s})>0$, so that

$$s_i\geq 0 \quad (1\leq i\leq k). \tag{7.9}$$

It is not difficult to verify the inequality

$$A_r < (2a)^{n^2}/n, \tag{7.10}$$

and using this together with (6.3) and (7.8), we deduce from (7.7) that

$$(T_r - T_{r+1})Q_s(X) < (c/n)D^s. \tag{7.11}$$

Finally

$$s_i = j_i - h_i \leq N_i - h_i = n_i \quad (1 \leq i \leq k), \tag{7.12}$$

and it follows from (7.9), (7.12) and the definition of Δ_s that

$$D^s \leq \Delta_s. \tag{7.13}$$

We conclude from (7.11) and (7.13) that

$$(T_r - T_{r+1})Q_s(X) < (c/n)\Delta_s. \tag{7.14}$$

We now obtain a contradiction. In case Ig this is immediate, for

$$T_r - T_{r+1} = T' = \min(E, T/n) \tag{7.15}$$

and so (7.14) contradicts at least one of (6.4), (6.5) or (6.6). In case IIg the same argument works if $s \neq n$, for then $r \leq s < n$ and (7.15) is still valid. Thus (7.14) contradicts either (6.4) or (6.5). It remains in case IIg to consider the possibility $s = n$.

For this we go back to (7.4). There exists some \mathbf{i} in $\mathcal{N}(h+r)$ with $\delta_i(\mathfrak{P}) \geq 1$. In particular (7.4) then implies that $C(\mathbf{r}) > 0$ for

$$\mathbf{r} = (r_1, \dots, r_k) = \mathbf{i} - \mathbf{h},$$

so that

$$r_i \geq 0 \quad (1 \leq i \leq k). \tag{7.16}$$

In addition, from (6.3), (7.8) and (7.10), the inequality (7.4) also implies that

$$M(T_r - T_{r+1}) < (c/n)D^r. \tag{7.17}$$

But as $s = n$ the stabilizer H must be a finite subgroup of G , and so contained in G_{tors} . Since $X_m - x_m \in H$ ($1 \leq m \leq M$), the condition (6.7) implies that $M = |X|$. Since $Q_r(X) \leq |X|$ we deduce from (7.17) that

$$(T_r - T_{r+1})Q_r(X) < (c/n)D^r. \tag{7.18}$$

As in (7.12) we see that

$$r_i \leq n_i \quad (1 \leq i \leq k), \tag{7.19}$$

and it follows from (7.16), (7.19) and the definition of Δ_r that

$$D^r \leq \Delta_r. \tag{7.20}$$

We conclude from (7.18) and (7.20) that

$$(T_r - T_{r+1})Q_r(X) < (c/n)\Delta_r. \tag{7.21}$$

If $r \neq n$, then $r < n$ and (7.15) is still valid; hence (7.21) contradicts either (6.4) or (6.5). It remains only in case IIg to consider the possibility $r = n$.

But now $T_r - T_{r+1} = T/n$, whence (7.21) contradicts (6.4). These contradictions establish (7.2) in all cases for the general version of the Main Theorem.

Next suppose that we are in the situation of the disjoint version of the Main Theorem, so that G_1, \dots, G_k are disjoint. Now the algebraic subgroup H has a type $\mathbf{s} = (s_1, \dots, s_k)$ automatically satisfying

$$0 \leq s_i \leq n_i \quad (1 \leq i \leq k).$$

By Lemma 6 the codimension $s = |\mathbf{s}|$ of H in G satisfies $r \leq s \leq n$, and, putting $\mathbf{j} = \mathbf{h} + \mathbf{s}$, we have

$$\kappa(H) \leq a^{n-r} (2a)^{r(n-r)} \sum C(\mathbf{d}) \delta_{\mathbf{j}-\mathbf{d}}(\mathfrak{P}) D^{\mathbf{d}},$$

where the sum is taken over all \mathbf{d} with $|\mathbf{d}| = s - r$. By (7.5) and the definition of $Q_{\mathbf{s}}(X)$ this gives

$$Q_{\mathbf{s}}(X) \leq M a^{n-r} (2a)^{r(n-r)} \sum C(\mathbf{d}) \delta_{\mathbf{j}-\mathbf{d}}(\mathfrak{P}) D^{\mathbf{d}}. \tag{7.22}$$

So combining (7.4) and (7.22) and using (6.3), (7.8) and (7.10) yields

$$(T_r - T_{r+1}) Q_{\mathbf{s}}(X) < (c/n) D^{\mathbf{s}}. \tag{7.23}$$

We now obtain a contradiction. In case Id this is immediate, for (7.15) holds and so (7.23) contradicts at least one of (6.8), (6.9) or (6.10). In case IId the same argument works if $\mathbf{s} \neq \mathbf{n}$, for then $r \leq s < n$ and (7.15) is still valid. Thus (7.23) contradicts either (6.8) or (6.9). It remains in case IId to consider the possibility $\mathbf{s} = \mathbf{n}$.

For this we go back to (7.4). There exists some \mathbf{i} in $\mathcal{N}(h+r)$ with $\delta_{\mathbf{i}}(\mathfrak{P}) \geq 1$. In particular (7.4) then implies $C(\mathbf{r}) > 0$ for $\mathbf{r} = (r_1, \dots, r_k) = \mathbf{i} - \mathbf{h}$, so that (7.16) holds. In addition, from (6.3), (7.8) and (7.10), the inequality (7.4) also implies that (7.17) holds. But as $\mathbf{s} = \mathbf{n}$ the stabilizer H must be a finite subgroup of G , and therefore contained in G_{tors} . Since $X_m - x_m \subseteq H$ ($1 \leq m \leq M$), the condition (6.11) implies that $M = |X|$. The inequalities (7.19) are still valid, and together with (7.16) they show that $Q_{\mathbf{r}}(X)$ is defined. Then $Q_{\mathbf{r}}(X) \leq |X|$, and we deduce from (7.17) that

$$(T_r - T_{r+1}) Q_{\mathbf{r}}(X) < (c/n) D^{\mathbf{r}}. \tag{7.24}$$

If $\mathbf{r} \neq \mathbf{n}$, then $r < n$ and (7.15) still holds; hence (7.24) contradicts either (6.8) or (6.9). It remains only to consider in case IId the possibility $\mathbf{r} = \mathbf{n}$.

But now $r = n$ and so $T_r - T_{r+1} = T/n$, whence (7.24) contradicts (6.8). These contradictions establish (7.2) in all cases for the disjoint version of the Main Theorem.

Thus we have proved (7.2) unconditionally. The argument is now essentially routine and it does not depend on which version of the Main Theorem we are considering. There exists x in X and an integer t with $0 \leq t < T_r - T_{r+1}$ such that (7.2) holds. We may assume t is chosen minimally for this choice of x . We shall deduce that

$$\Delta'(E(x)\mathfrak{J}_t) \not\subseteq \mathfrak{P}. \tag{7.25}$$

For suppose on the contrary that $\Delta'(E(x)\mathfrak{J}_t) \subseteq \mathfrak{P}$. From the minimality of t it follows easily that $\Delta' \mathfrak{J} \subseteq \mathfrak{P}^* = \mathfrak{P}$, where $\mathfrak{J} = (E(x)\mathfrak{J}_t)^*$ is the contracted exten-

sion of the ideal generated by the elements of the set $E(x)\mathfrak{I}_r$. Since the multiplicative set \mathcal{M} of Sect. 2 satisfies $E(x)\mathcal{M} \subseteq \mathcal{M}$, we see that $E(x)\mathfrak{I}_r^* \subseteq \mathfrak{I}$, and therefore $\Delta^t(E(x)\mathfrak{I}_r^*) \subseteq \mathfrak{P}$. Now $\Delta^t\mathfrak{G} \subseteq \mathfrak{G} \subseteq \mathfrak{P}$ by (i) of Lemma 3, and it follows once again using the minimality of t that

$$\Delta^t(\mathcal{E}(x)\mathfrak{I}_r^*) \subseteq \mathfrak{P}^* = \mathfrak{P},$$

which contradicts (7.2). Thus (7.25) is established.

Therefore there exists j with $1 \leq j \leq h+r$ such that $P'_j = \Delta^t(E(x)P_j)$ is not in \mathfrak{P} . But in fact $j \geq h+1$. This is trivial if $h=0$; and otherwise we only have to observe that if $1 \leq i \leq h$ then P_i is in $(P_1, \dots, P_h)^* = \mathfrak{G}$, so that $E(x)P_i$ is in $E(x)\mathfrak{G} \subseteq \mathfrak{G}$. Hence $\Delta^t(E(x)P_i)$ is in $\Delta^t\mathfrak{G} \subseteq \mathfrak{G} \subseteq \mathfrak{P}$. Thus indeed $h+1 \leq j \leq h+r$.

Now by (i), the multidegree of P'_j is at most (D'_1, \dots, D'_k) , where

$$D'_i = (2a)^{r-1} a_i D_i + t(a_i - 1) \leq (2a)^{r-1} a D_i + (T_r - T_{r+1})(a_i - 1) \quad (1 \leq i \leq k).$$

Assume $r \neq n$. Then we observe that

$$(T_r - T_{r+1})(a_i - 1) \leq a D_i \quad (1 \leq i \leq k). \tag{7.26}$$

This is obvious if G_i is linear, since then $a_i = 1$; otherwise, if G_i is not linear then by the definition of E we have

$$T_r - T_{r+1} = \min(E, T/n) \leq E \leq D_i.$$

Hence (7.26) gives

$$D'_i \leq (2a)^r D_i \quad (1 \leq i \leq k; r \neq n).$$

Thus if $r \neq n$, multiplying P'_j by a suitable monomial $M_{\mathfrak{P}}$ in \mathcal{M} we obtain a multihomogeneous polynomial $P_{\mathfrak{P}} = M_{\mathfrak{P}} P'_j$ of multidegree exactly $(2a)^r(D_1, \dots, D_k)$ which again does not lie in \mathfrak{P} . If however $r = n$ then we define $P_{\mathfrak{P}}$ simply as P'_j .

Now we recall that this construction can be carried out for each prime component \mathfrak{P} of \mathfrak{I}_r^* . Thus using Lemma 5 (p.285) of [2] we can find a linear combination of the $P_{\mathfrak{P}}$, with coefficients in K , that does not lie in any of the prime components of \mathfrak{I}_r^* . This linear combination gives the required polynomial P_{h+r+1} , and we proceed to verify that it satisfies the conditions (i)_{r+1} (if $r \neq n$), (ii)_{r+1}, (iii)_{r+1}, and (iv)_{r+1} (if $r \neq n$) of the Proposition.

The above construction of each $P_{\mathfrak{P}}$ makes it clear that (i)_{r+1} holds (if $r \neq n$). Next, to prove (ii)_{r+1}, let y be any point of $X^{(n-r)}$. Then $z = y + x$ is in $X^{(n+1-r)}$, and so by (ii),

$$\text{ord}_z P_j \geq T_r \quad (h+1 \leq j \leq h+r).$$

Hence by (ii) of Lemma 3 we have

$$\text{ord}_y E(x)P_j = \text{ord}_z P_j \geq T_r \quad (h+1 \leq j \leq h+r),$$

and so by (iii) of Lemma 3

$$\text{ord}_y \Delta^t(E(x)P_j) \geq T_r - t \quad (h+1 \leq j \leq h+r)$$

as long as $T_r \geq t$. But in fact

$$T_r - t > T_{r+1} \geq 0.$$

So this holds, and we deduce that $\text{ord}_y P_{\mathfrak{A}}' > T_{r+1}$. Hence also $\text{ord}_y P_{h+r+1} > T_{r+1}$, and since y was arbitrary this proves $(ii)_{r+1}$ (with strict inequality).

The condition $(iii)_{r+1}$ follows by standard arguments. Indeed, the ideal $\mathfrak{J} = (\mathfrak{I}_r^*, P_{h+r+1})$ has rank $h+r+1$. Also, since $T_r \geq T_{n+1} \geq 0$, every generator of \mathfrak{I}_{r+1} vanishes on the non-empty set $X^{(n-r)}$, and in particular $\mathfrak{I}_{r+1}^* \neq \mathfrak{R}$. So by Lemma 7 of [4] the rank of \mathfrak{I}_{r+1}^* is at most $h+r+1$. Since $\mathfrak{J} \subseteq \mathfrak{I}_{r+1}^*$, this rank must be exactly $h+r+1$. This verifies $(iii)_{r+1}$.

Finally if $r = n$, then for any \mathbf{j} in $\mathcal{N}(h+r+1)$ we deduce from Lemma A5 that

$$\delta_{\mathbf{j}}(\mathfrak{J}) \leq (2a)^r \sum_{i=1}^k D_i \delta_{\mathbf{j}-\mathbf{e}_i}(\mathfrak{I}_r^*).$$

By (iv)_r, we have

$$\delta_{\mathbf{j}-\mathbf{e}_i}(\mathfrak{I}_r^*) \leq C(\mathbf{j}-\mathbf{h}-\mathbf{e}_i)(2a)^{\frac{1}{2}r(r-1)} b^h D^{j-\mathbf{h}}/D_i \quad (1 \leq i \leq k),$$

so we get

$$\delta_{\mathbf{j}}(\mathfrak{J}) \leq (2a)^{\frac{1}{2}r(r+1)} b^h D^{j-\mathbf{h}} \sum_{i=1}^k C(\mathbf{j}-\mathbf{h}-\mathbf{e}_i).$$

But with our convention on multinomial coefficients it is easily seen that $\sum_{i=1}^k C(\mathbf{j}-\mathbf{h}-\mathbf{e}_i) = C(\mathbf{j}-\mathbf{h})$, and hence

$$\delta_{\mathbf{j}}(\mathfrak{J}) \leq C(\mathbf{j}-\mathbf{h})(2a)^{\frac{1}{2}r(r+1)} b^h D^{j-\mathbf{h}}. \tag{7.27}$$

Since $\mathfrak{J} \subseteq \mathfrak{I}_{r+1}^*$ and these ideals have the same ranks $h+r+1 \leq N$, the condition $(iv)_{r+1}$ follows from (7.27) using Lemma A4. This completes the proof of the Proposition.

8. Further remarks

We discuss here the relationships between our Main Theorems and the results announced in Sect. 9 of [4]. To start with, we show that either Main Theorem implies a slightly weaker version, sufficient for all applications, of Theorem A (p. 514), in which the inequalities (42) of [4] should be replaced by

$$(S/n)^{Pr} \geq c D^{r-1} \quad (1 \leq r < n) \tag{*}$$

if $n > 1$. There is no loss of generality in supposing that $D \geq 1$ and D is an integer. It now suffices to take $k=1$ and $G_1=G$; then Γ is a subgroup of G generated by elements $\gamma_1, \dots, \gamma_m$ of G . If the rank l of Γ is zero, we take X as the origin of G . Otherwise, if $l \geq 1$, then without loss of generality we can assume that $\gamma_1, \dots, \gamma_l$ are linearly independent, and we take X as the set of elements of the form

$$s_1 \gamma_1 + \dots + s_l \gamma_l \quad (0 \leq s_1, \dots, s_l \leq S/n).$$

In the notation of [4], we have $X^{(n)} \subseteq \Gamma(S)$; and also

$$|X/G_{\text{tors}}| = |X|. \tag{8.1}$$

We next claim that

$$Q_r(X) \geq (S/n)^{p_r} \quad (1 \leq r \leq n). \tag{8.2}$$

If $p_r = 0$ this is trivial. Otherwise, suppose $p = p_r \geq 1$. If G has no algebraic subgroups of codimension r , put $H = 0$; else let H be any such algebraic subgroup. In either case, we can assume from the definition of p that $\gamma_1, \dots, \gamma_p$ are linearly independent modulo H . Now the elements

$$s_1 \gamma_1 + \dots + s_p \gamma_p \quad (0 \leq s_1, \dots, s_p \leq S/n)$$

are distinct modulo H , so that $|X/H| \geq (S/n)^p$. Taking the minimum over H , we deduce (8.2) in either case.

Now the conditions (41) and (*) of Theorem A imply the conditions

$$TQ_r(X) \geq c D^r \quad (1 \leq r \leq n) \tag{8.3}$$

and if $n > 1$ also

$$EQ_r(X) \geq c D^{r-1} \quad (1 \leq r < n) \tag{8.4}$$

of our Main Theorems, and we also have (8.1). Thus we can conclude that P vanishes on $\gamma + \Phi$ for some γ in Γ , and so the slightly weaker version of Theorem A is established, with $c = (2a)^{n^2} b^{N-n}$. At the same time we are able to verify an additional remark made in [4]; namely, that the conditions (*) can be omitted entirely if G is a linear group variety. For then by definition $E = T$; whence the conditions (8.3) and (8.4) are implied by (41) alone.

Similar arguments enable us to deduce Theorem B (p. 515) of [4] from the general version of our Main Theorem. We choose Φ in an arbitrary way and we take $T = 1$. By using induction on k and simple projection properties of the quantities p_r , it is not difficult to see that we may without loss of generality assume that D_1, \dots, D_k are positive integers. We could define X as above; but in fact it suffices here to take $X = \Gamma(S/n)$, since we no longer need the condition (8.1). We still have $X^{(n)} \subseteq \Gamma(S)$, and, as this X is certainly no smaller than the set defined above, (8.2) still holds.

Now the conditions of Theorem B imply the conditions

$$TQ_r(X) \geq c \Delta_r \quad (1 \leq r \leq n)$$

$$EQ_r(X) \geq c \Delta_r \quad (1 \leq r \leq n)$$

of the general version of our Main Theorem. Thus we conclude that for any one-parameter subgroup Φ of G there exists γ in Γ such that P vanishes on all of $\gamma + \Phi$.

It remains to verify that this implies the vanishing of P on all of G . We do this using only the countability of Γ . It is convenient to assume G embedded in some projective space \mathbb{P}_M ; for example, the Segre map does this with $M + 1 = (N_1 + 1) \dots (N_k + 1)$. Then P can be regarded as a homogeneous polynomial in the associated variables X_0, \dots, X_M . Without loss of generality we can assume

that $X_1/X_0, \dots, X_n/X_0$ are algebraically independent functions on G . Let π be the rational map from \mathbb{P}_M to \mathbb{P}_n obtained by taking only the coordinates X_0, \dots, X_n . Then π is defined on a non-empty open subset \mathcal{O} of G , and $\pi(\mathcal{O})$ is a constructible subset of \mathbb{P}_n which therefore contains a non-empty open subset \mathcal{O}' of \mathbb{P}_n (see for example [1] p.39). Thus there is a non-zero homogeneous polynomial $Q(X_0, \dots, X_n)$ which vanishes on the complement of \mathcal{O}' in \mathbb{P}_n .

Now suppose on the contrary that P does not vanish on all of G . Then the vanishing of P defines a proper closed subset S of G . Hence for each γ in Γ the set $S-\gamma$ is a closed subset of G of dimension at most $n-1$. Thus for each γ in Γ we can find a non-zero homogeneous polynomial $P_\gamma(X_0, \dots, X_n)$ which vanishes on $S-\gamma$. Since Γ is countable, it follows as in [4] (p.492) that there exist elements x_0, \dots, x_n of K such that $Q(x_0, \dots, x_n) \neq 0$ and $P_\gamma(x_0, \dots, x_n) \neq 0$ for all γ in Γ . In particular there exists g in $\mathcal{O} \subseteq G$ whose first $n+1$ projective coordinates are x_0, \dots, x_n ; and then P does not vanish at g for any γ in Γ . Therefore g is not in $S-\gamma$ for any γ in Γ , whence $\gamma+g$ is not in S for any γ in Γ . However, by using the exponential map on G it is easy to construct a one-parameter subgroup Φ of G that passes through g . Then there exists γ in Γ such that P vanishes on $\gamma+\Phi$. So $\gamma+\Phi \subseteq S$, whence $\gamma+g$ is in S , a contradiction.

Thus indeed P vanishes on all of G , which establishes Theorem B, with $c=(2a)^{n^2} b^{N-n} k^n$.

Next we deduce Theorem C (p.515) of [4] from either version of our Main Theorem. We note that in the statement of this result the numbers Σ_r should be defined as 1 if $p_r=0$. It suffices to take $k=1$ and $G_1=G$, with Φ arbitrary and $T=1$, and without loss of generality D a positive integer. We take

$$X = \Gamma_1(S_1/n) + \dots + \Gamma_h(S_h/n);$$

then clearly $X^{(n)} \subseteq \Gamma_1(S_1) + \dots + \Gamma_h(S_h)$. We claim that

$$Q_r(X) \geq \Sigma_r/n^{p_r} \quad (1 \leq r \leq n). \tag{8.5}$$

If $p_r=0$ this is trivial. Otherwise, suppose $p=p_r \geq 1$. If G has no algebraic subgroup of codimension r , put $H=0$; else let H be any such algebraic subgroup. In either case we can find p elements $\gamma_1, \dots, \gamma_p$ taken from the generators of $\Gamma_1, \dots, \Gamma_h$ that are linearly independent modulo H . Suppose q_i of these come from generators of Γ_i ($1 \leq i \leq h$). Then we have

$$0 \leq q_1 \leq l_1, \dots, 0 \leq q_h \leq l_h, \quad q_1 + \dots + q_h = p,$$

and now it is clear how to write down at least

$$(S_1/n)^{q_1} \dots (S_h/n)^{q_h} \geq \Sigma_r/n^p$$

elements of X that are distinct modulo H . Hence $|X/H| \geq \Sigma_r/n^p$. Taking the minimum over H , we deduce (8.5) in either case.

Now the conditions of Theorem B imply the conditions

$$\begin{aligned} TQ_r(X) &\geq c D^r & (1 \leq r \leq n) \\ EQ_r(X) &\geq c D^r & (1 \leq r \leq n) \end{aligned}$$

of our Main Theorems. Thus we conclude that for any one-parameter subgroup Φ of G there exists γ in Γ such that P vanishes on $\gamma + \Phi$. Exactly as above this implies that P vanishes on all of G . This establishes Theorem C, with $c = (2a)^{n^2} b^{N-n}$.

We leave it to the reader to prove that the general version of the Main Theorem implies a form of Theorem ABC (p. 515) of [4] in which the conditions $E \Sigma_r/n^{pr} \geq \Delta_r$ are replaced by $E \Sigma_r/n^{pr} \geq c \Delta_r$ ($1 \leq r < n$), even when E is defined as in the final sentence of [4]. Likewise, if he wishes, he can formulate a variant of this result when G_1, \dots, G_k are disjoint, and deduce such a result from the disjoint version of the Main Theorem.

We close this section with some practical methods for establishing that given commutative group varieties are disjoint. For a commutative group variety G we define a subquotient of G as a group of the form H/K , where H and K are algebraic subgroups of G with H connected and $K \subseteq H$. It too is connected, and is therefore a group variety.

Lemma 7. (i) *For commutative group varieties G_1, G_2 suppose that whenever Q_1, Q_2 are isomorphic subquotients of G_1, G_2 respectively, then $Q_1 = Q_2 = 0$. Then G_1, G_2 are disjoint.*

(ii) *For commutative group varieties G_1, G_2, G_3 suppose G_1, G_3 are disjoint and G_2, G_3 are disjoint. Then $G_1 \times G_2, G_3$ are disjoint.*

(iii) *For $k \geq 2$ and commutative group varieties G_1, \dots, G_k suppose G_i, G_j are disjoint whenever $1 \leq i < j \leq k$. Then G_1, \dots, G_k are disjoint.*

Proof. Let G_1, G_2 be commutative group varieties, with $G = G_1 \times G_2$, and let π_1, π_2 denote the projections from G to G_1, G_2 respectively. We start by noting, essentially as in [3], that the existence of an algebraic subgroup H of G implies the existence of algebraic subgroups $K_1 \subseteq H_1 = \pi_1(H)$, $K_2 \subseteq H_2 = \pi_2(H)$ and an isomorphism $\lambda: H_1/K_1 \rightarrow H_2/K_2$ such that (h_1, h_2) is in H if and only if $\lambda(h_1 + K_1) = h_2 + K_2$. For we may identify G_1, G_2 as algebraic subgroups of G in the natural way, and we let $K_1 = \pi_1(H \cap G_1)$ be the set of all h_1 in H_1 such that $(h_1, 0)$ is in H , and we let $K_2 = \pi_2(H \cap G_2)$ be the set of all h_2 in H_2 such that $(0, h_2)$ is in H . Then for any h_1 in H_1 there is some h_2 in H_2 such that (h_1, h_2) is in H , and it is easy to see that this induces the desired isomorphism λ between the subquotients $H_1/K_1, H_2/K_2$.

Now (i) is immediate. For let H be any connected algebraic subgroup of $G_1 \times G_2$. Then the resulting subgroups H_1, H_2 are connected, and so $Q_1 = H_1/K_1, Q_2 = H_2/K_2$ are subquotients. Thus by hypothesis $Q_1 = Q_2 = 0$, so $K_1 = H_1, K_2 = H_2$. This leads at once to $H = H_1 \times H_2$, so G_1, G_2 are disjoint as required.

Before we establish (ii) and (iii) we prove a converse to (i). Suppose G_1, G_2 are disjoint, and let $\lambda: Q_1 \rightarrow Q_2$ be an isomorphism of subquotients $Q_1 = H_1/K_1, Q_2 = H_2/K_2$ of G_1, G_2 respectively. We shall show that $Q_1 = Q_2 = 0$.

Define a map $\delta: H_1 \times H_2 \rightarrow Q_2$ by

$$\delta(h_1, h_2) = \lambda(h_1 + K_1) - (h_2 + K_2).$$

Its kernel H is an algebraic subgroup of G , and clearly $\pi_1(H) = H_1, \pi_2(H) = H_2$. By disjointness the neutral connected component H_0 of H is a product, and by

writing H as a union of translates of H_0 we see easily that in fact $H=H_0$. Thus $H=H_1 \times H_2$, and δ is zero. Hence $Q_2=0$, and $Q_1=0$ as well. This proves the required converse of (i).

Now to prove (ii) suppose G_1, G_3 as well as G_2, G_3 are disjoint. By (i), to prove $G=G_1 \times G_2, G_3$ disjoint it suffices to show that if $\lambda: Q_3 \rightarrow Q$ is an isomorphism of subquotients $Q_3=H_3/K_3, Q=H/K$ of G_3, G respectively, then $Q=0$. Let $H_1=\pi_1(H), H_2=\pi_2(H)$. The projections π_1, π_2 induce surjective maps from Q to $H_1/\pi_1(K), H_2/\pi_2(K)$, and these may be combined with λ to give surjective maps $\mu_1: Q_3 \rightarrow H_1/\pi_1(K), \mu_2: Q_3 \rightarrow H_2/\pi_2(K)$. Their kernels have the forms $L_1/K_3, L_2/K_3$ for algebraic subgroups L_1, L_2 with $K_3 \subseteq L_1, L_2 \subseteq H_3$, and we thus obtain isomorphisms between H_3/L_1 and $H_1/\pi_1(K)$ and between H_3/L_2 and $H_2/\pi_2(K)$. Since H_1, H_2, H_3 are connected, our disjointness hypothesis and the converse to (i) show that $H_1=\pi_1(K), H_2=\pi_2(K)$. Now $Q=0$, because any element of $Q=\lambda(Q_3)$ must be in the kernels of both π_1 and π_2 . This completes the proof of (ii).

Finally we prove (iii) by induction on k . It is trivial for $k=2$, so assume that it has been verified for some $k \geq 2$. Suppose G_1, \dots, G_{k+1} are pairwise disjoint, and let H be any connected algebraic subgroup of $G_1 \times \dots \times G_{k+1}$. By repeated use of (ii) we see that $G'=G_1 \times \dots \times G_k, G_{k+1}$ are disjoint. Hence $H=H' \times H_{k+1}$ for connected algebraic subgroups H', H_{k+1} of G', G_{k+1} respectively. By the induction hypothesis G_1, \dots, G_k are disjoint; hence H' splits further as $H_1 \times \dots \times H_k$. Thus H splits completely as required. This proves (iii), and thereby completes the proof of Lemma 7. We note here incidentally that, besides (i), the statements (ii), (iii) also have converses; however, these are trivially verified.

Appendix

Multihomogeneous ideals

We collect here a number of results about degree theory for multihomogeneous ideals. Our basic reference is [10], but we have to supplement this with a few additional considerations. These usually generalize the corresponding classical arguments for homogeneous ideals.

For $k \geq 1$ and integers $N_1 \geq 1, \dots, N_k \geq 1$ let

$$X_{1,0}, \dots, X_{1,N_1}, \dots, X_{k,0}, \dots, X_{k,N_k} \tag{A1}$$

be independent variables, and let \mathfrak{R} be the associated polynomial ring over some field K . We say that a polynomial P in \mathfrak{R} is multihomogeneous if it is homogeneous in each of the sets of variables $X_{i,0}, \dots, X_{i,N_i}$ ($1 \leq i \leq k$); if further its degree in these variables is t_i ($1 \leq i \leq k$), we say that its multidegree is (t_1, \dots, t_k) . As usual we say that an ideal \mathfrak{I} of \mathfrak{R} is multihomogeneous if it can be generated by multihomogeneous polynomials. For such an ideal \mathfrak{I} and integers $t_1 \geq 0, \dots, t_k \geq 0$ let $H(t_1, \dots, t_k; \mathfrak{I})$ be the maximum number of monomials of multidegree (t_1, \dots, t_k) that are linearly independent over K modulo \mathfrak{I} . Suppose the rank r of \mathfrak{I} satisfies $1 \leq r \leq N$, where

$$N = N_1 + \dots + N_k.$$

Let \mathcal{N} be the set of elements $\mathbf{j}=(j_1, \dots, j_k)$ of \mathbf{Z}^k with

$$0 \leq j_1 \leq N_1, \dots, 0 \leq j_k \leq N_k.$$

Then it is known that there exist integers a_j such that for all sufficiently large t_1, \dots, t_k we have

$$H(t_1, \dots, t_k; \mathfrak{I}) = \sum a_{\mathbf{j}} \binom{t_1}{N_1 - j_1} \dots \binom{t_k}{N_k - j_k}, \tag{A2}$$

where the sum is taken over all \mathbf{j} in \mathcal{N} with

$$|\mathbf{j}| = j_1 + \dots + j_k \geq r.$$

For a proof see Theorem 7 (p. 757) of [10].

Let $\mathcal{N}(r)$ denote the subset of \mathcal{N} consisting of all \mathbf{j} with $|\mathbf{j}| = r$. For \mathbf{j} in $\mathcal{N}(r)$ we denote the coefficients $a_{\mathbf{j}}$ by $\delta_{\mathbf{j}}(\mathfrak{I})$. It is convenient also to define $\delta_{\mathbf{j}}(\mathfrak{I})$ as 0 for any \mathbf{j} in \mathbb{Z}^k not in $\mathcal{N}(r)$.

Similarly it is useful to define the binomial coefficient $\binom{a}{b}$ as 0 for any integers a, b with $a \geq 0$ and either $b < 0$ or $b > a$.

Lemma A1. *For $1 \leq r \leq N$ let \mathfrak{I} be a multihomogeneous ideal of rank r . Then $\delta_{\mathbf{j}}(\mathfrak{I}) \geq 0$ for all \mathbf{j} in $\mathcal{N}(r)$. Furthermore, there exists at least one \mathbf{j} in $\mathcal{N}(r)$ such that $\delta_{\mathbf{j}}(\mathfrak{I}) > 0$.*

Proof. By Theorem 11 (p. 759) of [10] we know that $\delta_{\mathbf{j}}(\mathfrak{I}) \geq 0$ for all \mathbf{j} in $\mathcal{N}(r)$. To get a strict inequality we note that \mathfrak{I} is a homogeneous ideal of \mathfrak{R} , so that for an integer $t \geq 0$ we can define the usual Hilbert function $H(t; \mathfrak{I})$ that counts the maximum number of monomials of degree t that are linearly independent over K modulo \mathfrak{I} . It is easy to see that

$$H(t; \mathfrak{I}) = \sum H(t_1, \dots, t_k; \mathfrak{I}), \tag{A3}$$

where the sum is taken over all t_1, \dots, t_k with

$$t_1 \geq 0, \dots, t_k \geq 0, \quad t_1 + \dots + t_k = t.$$

We also have the identity

$$\binom{t+k-1}{r+k-1} = \sum \binom{t_1}{r_1} \dots \binom{t_k}{r_k}, \tag{A4}$$

where the sum is taken over the same range. This holds for any $r_1 \geq 0, \dots, r_k \geq 0$ with $r_1 + \dots + r_k = r$.

Now for t sufficiently large the function $H(t; \mathfrak{I})$ is a polynomial of degree $m = N + k - 1 - r$ with leading term $\delta t^m / m!$, where δ is the classical degree of \mathfrak{I} viewed as a homogeneous ideal. If we formally substitute (A2) and (A4) into (A3) we may in fact equate the resulting coefficients of t^m . This is because the terms with at least one of t_1, \dots, t_k bounded give rise to terms of order at most t^{m-1} . We obtain

$$\delta = \sum \delta_{\mathbf{j}}(\mathfrak{I}),$$

where the sum is over all \mathbf{j} in $\mathcal{N}(r)$. Since $\delta > 0$, the last part of the lemma follows at once.

Lemma A2. *For $1 \leq r \leq N$ let \mathfrak{I} be a multihomogeneous ideal of rank r , and let*

$$\mathfrak{I} = \mathfrak{Q}_1 \cap \dots \cap \mathfrak{Q}_n$$

be an irredundant primary decomposition with $\mathfrak{Q}_1, \dots, \mathfrak{Q}_m$ of rank r and the remaining ideals (if any) of rank larger than r . Then $\mathfrak{Q}_1, \dots, \mathfrak{Q}_m$ are also multihomogeneous and we have

$$\delta_{\mathbf{j}}(\mathfrak{I}) = \delta_{\mathbf{j}}(\mathfrak{Q}_1) + \dots + \delta_{\mathbf{j}}(\mathfrak{Q}_m)$$

for any \mathbf{j} in $\mathcal{N}(r)$.

Proof. The fact that $\mathfrak{Q}_1, \dots, \mathfrak{Q}_m$ are multihomogeneous follows easily from the fact that they are isolated components and therefore determined uniquely by \mathfrak{I} ; the full result is then proved as Theorem 8 (p. 758) of [10].

Lemma A3. *For $1 \leq r \leq N$ let \mathfrak{Q} be a multihomogeneous primary ideal of rank r and length l . Then the associated prime ideal \mathfrak{P} is multihomogeneous and we have*

$$\delta_{\mathbf{j}}(\mathfrak{Q}) = l \delta_{\mathbf{j}}(\mathfrak{P})$$

for any \mathbf{j} in $\mathcal{N}(r)$.

Proof. It is easy to see that \mathfrak{P} is multihomogeneous, and then the result is proved in § 32 (p. 767) of [10].

Lemma A4. For $1 \leq r \leq N$ suppose $\mathfrak{I}, \mathfrak{I}'$ are multihomogeneous ideals of rank r with $\mathfrak{I}' \subseteq \mathfrak{I}$. Then we have

$$\delta_j(\mathfrak{I}) \leq \delta_j(\mathfrak{I}')$$

for any \mathbf{j} in $\mathcal{N}(r)$.

Proof. The inequality $H(t_1, \dots, t_k; \mathfrak{I}) \leq H(t_1, \dots, t_k; \mathfrak{I}')$ is an obvious consequence of the hypotheses, but unfortunately it does not imply the corresponding inequalities for the leading coefficients if $k > 1$. Instead we argue as follows. We can write

$$\mathfrak{I} = \mathfrak{Q}_1 \cap \dots \cap \mathfrak{Q}_m \cap \mathfrak{J},$$

where $\mathfrak{Q}_1, \dots, \mathfrak{Q}_m$ are multihomogeneous primary ideals of rank r with distinct associated primes $\mathfrak{P}_1, \dots, \mathfrak{P}_m$, and either $\mathfrak{J} = \mathfrak{R}$ or \mathfrak{J} has rank larger than r . Since

$$\mathfrak{I}' \subseteq \mathfrak{I} \subseteq \mathfrak{Q}_i \subseteq \mathfrak{P}_i \quad (1 \leq i \leq m),$$

it follows that \mathfrak{I}' has an isolated primary component \mathfrak{Q}'_i of rank r with associated prime \mathfrak{P}_i ($1 \leq i \leq m$). We can therefore write

$$\mathfrak{I}' = \mathfrak{Q}'_1 \cap \dots \cap \mathfrak{Q}'_m \cap \mathfrak{J}',$$

where either $\mathfrak{J}' = \mathfrak{R}$ or \mathfrak{J}' has rank at least r (possibly equal to r). Localizing the inclusion $\mathfrak{I}' \subseteq \mathfrak{I}$ at \mathfrak{P}_i gives then $\mathfrak{Q}'_i \subseteq \mathfrak{Q}_i$ ($1 \leq i \leq m$), and so the lengths l'_i of \mathfrak{Q}'_i and l_i of \mathfrak{Q}_i are related by

$$l'_i \geq l_i \quad (1 \leq i \leq m).$$

Also by Lemmas A2 and A3 we have

$$\delta_j(\mathfrak{I}) = \sum_{i=1}^m \delta_j(\mathfrak{Q}_i) = \sum_{i=1}^m l_i \delta_j(\mathfrak{P}_i)$$

and

$$\delta_j(\mathfrak{I}') \geq \sum_{i=1}^m \delta_j(\mathfrak{Q}'_i) = \sum_{i=1}^m l'_i \delta_j(\mathfrak{P}_i)$$

for any \mathbf{j} in $\mathcal{N}(r)$. The inequality of the present lemma is now immediate.

Lemma A5. For $1 \leq r \leq N$ let \mathfrak{I} be a multihomogeneous ideal of rank r , and for integers $D_1 \geq 0, \dots, D_k \geq 0$ not all zero let P be a multihomogeneous polynomial of multidegree (D_1, \dots, D_k) such that $\mathfrak{I} : (P) = \mathfrak{I}$. Then the ideal $\mathfrak{I} = (\mathfrak{I}, P)$ is multihomogeneous of rank $r + 1$. Furthermore, if $r \neq N$ then we have

$$\delta_j(\mathfrak{I}) = \sum_{i=1}^k D_i \delta_{\mathbf{j} - \mathbf{e}_i}(\mathfrak{I})$$

for any \mathbf{j} in $\mathcal{N}(r + 1)$, where $\mathbf{e}_1, \dots, \mathbf{e}_k$ are the standard basis vectors of \mathbb{Z}^k .

Proof. Since P is in particular homogeneous of degree $D_1 + \dots + D_k > 0$ in the variables (A_1) , the fact that the rank of \mathfrak{I} is $r + 1$ follows immediately from the corresponding assertion for homogeneous ideals (see for example Lemma 3 (p. 281) of [2]). Then from Theorem 5 (p. 756) of [10] we get

$$H(t_1, \dots, t_k; \mathfrak{I}) = H(t_1, \dots, t_k; \mathfrak{I}) - H(t_1 - D_1, \dots, t_k - D_k; \mathfrak{I})$$

for any integers $t_i \geq D_1, \dots, t_k \geq D_k$. On making t_1, \dots, t_k sufficiently large, the required expression for $\delta_j(\mathfrak{I})$ follows without difficulty from the fact that for t large and m, D fixed the expression

$$\binom{t}{m} - \binom{t-D}{m} - D \binom{t}{m-1}$$

is of order at most t^{m-2} .

For the final lemma we write

$$\mathfrak{R}_i = K[X_{i,0}, \dots, X_{i,N_i}] \quad (1 \leq i \leq k).$$

Lemma A6. For integers r_1, \dots, r_k with $1 \leq r_1 \leq N_1, \dots, 1 \leq r_k \leq N_k$ let \mathfrak{P}_i be a homogeneous prime ideal of \mathfrak{R}_i of rank r_i and degree δ_i ($1 \leq i \leq k$). Then the ideal $\mathfrak{I} = (\mathfrak{P}_1, \dots, \mathfrak{P}_k)$ of \mathfrak{R} is multihomogeneous of rank $r = r_1 + \dots + r_k$ and we have

$$\delta_j(\mathfrak{I}) = \delta_1 \dots \delta_k$$

for $\mathbf{j} = \mathbf{r} = (r_1, \dots, r_k)$, while

$$\delta_{\mathbf{j}}(\mathfrak{I}) = 0$$

for all $\mathbf{j} \neq \mathbf{r}$ in $\mathcal{N}(\mathfrak{r})$.

Proof. It is obvious that \mathfrak{I} is multihomogeneous. Fix integers $t_1 \geq 0, \dots, t_k \geq 0$. Let $h_i = H(t_i; \mathfrak{P}_i) \geq 1$ be the usual Hilbert function of \mathfrak{P}_i in \mathfrak{R}_i , and let

$$M_i(1), \dots, M_i(h_i)$$

denote a maximal set of monomials of \mathfrak{R}_i of degree t_i that are linearly independent over K modulo \mathfrak{P}_i ($1 \leq i \leq k$). It is easy to see that the products

$$M(m_1, \dots, m_k) = M_1(m_1) \dots M_k(m_k) \quad (1 \leq m_1 \leq h_1, \dots, 1 \leq m_k \leq h_k)$$

span the vector space V over K of all multihomogeneous polynomials of \mathfrak{R} of multidegree (t_1, \dots, t_k) taken modulo \mathfrak{I} . It is not so easy to see that they are actually linearly independent over K in V . In fact we prove by induction that for any i with $1 \leq i \leq k$ the products

$$M_1(m_1) \dots M_i(m_i) \quad (1 \leq m_1 \leq h_1, \dots, 1 \leq m_i \leq h_i) \tag{A5}$$

are linearly independent over K modulo $\mathfrak{I}_i = (\mathfrak{P}_1, \dots, \mathfrak{P}_i)$. This is clear for $i = 1$; assume it holds for some i with $1 \leq i < k$. Suppose we have elements $\lambda(m_1, \dots, m_{i+1})$ of K such that

$$\sum \lambda(m_1, \dots, m_{i+1}) M_1(m_1) \dots M_{i+1}(m_{i+1}) \equiv 0 \pmod{\mathfrak{I}_{i+1}}, \tag{A6}$$

where the sum is over all m_1, \dots, m_{i+1} with $1 \leq m_1 \leq h_1, \dots, 1 \leq m_{i+1} \leq h_{i+1}$. Pick an arbitrary projective zero π of \mathfrak{P}_{i+1} and specify a set of projective coordinates for π . Let $\mu(m_{i+1})$ be the value of the monomial $M_{i+1}(m_{i+1})$ at π ($1 \leq m_{i+1} \leq h_{i+1}$). Specializing to π in (A6) and putting

$$\lambda'(m_1, \dots, m_i) = \sum_{m_{i+1}=1}^{h_{i+1}} \lambda(m_1, \dots, m_{i+1}) \mu(m_{i+1}), \tag{A7}$$

we get

$$\sum \lambda'(m_1, \dots, m_i) M_1(m_1) \dots M_i(m_i) \equiv 0 \pmod{\mathfrak{I}_i},$$

where the sum is over all m_1, \dots, m_i as in (A5). By the induction hypothesis we get $\lambda'(m_1, \dots, m_i) = 0$ for all m_1, \dots, m_i . Since π was arbitrary, by (A7) this implies that

$$\sum_{m_{i+1}=1}^{h_{i+1}} \lambda(m_1, \dots, m_{i+1}) M_{i+1}(m_{i+1}) \equiv 0 \pmod{\mathfrak{P}_{i+1}}.$$

Consequently $\lambda(m_1, \dots, m_{i+1}) = 0$ for all m_1, \dots, m_{i+1} . This does the induction step.

Now the linear independence of the monomials in (A5) for $i = k$ shows that

$$H(t_1, \dots, t_k; \mathfrak{I}) = H(t_1; \mathfrak{P}_1) \dots H(t_k; \mathfrak{P}_k).$$

From this and the positivity statement of Lemma A1 the assertions of Lemma A6 follow without difficulty.

References

1. Borel, A.: Linear algebraic groups. New York: W.A. Benjamin 1969
2. Brownawell, W.D., Masser, D.W.: Multiplicity estimates for analytic functions II. *Duke Math. J.* **47**, 273–295 (1980)
3. Kolchin, E.R.: Algebraic groups and algebraic dependence. *Amer. J. Math.* **90**, 1151–1164 (1968)
4. Masser, D.W., Wüstholz, G.: Zero estimates on group varieties I. *Invent. Math.* **64**, 489–516 (1981)
5. Masser, D.W., Wüstholz, G.: Algebraic independence of values of elliptic functions. In: *Journées Arithmétiques 1980* (J.V. Armitage (ed.)). L.M.S. Lect. Notes No. 56, Cambridge 1982

6. Masser, D.W.: Small values of the quadratic part of the Néron-Tate height on an abelian variety. *Compositio Math.* **53**, 153–170 (1984)
7. Philippon, P.: Indépendance algébrique de valeurs de fonctions elliptiques p -adiques. *Queen's Pap. Pure Appl. Math.* **54**, 223–235 (1980)
8. Renschuch, B.: *Elementare und praktische Idealtheorie*. Berlin: VEB Deutscher Verlag 1976
9. Sebti-Chaouni, N.: Le théorème de Baker par la méthode de Schneider. *Publications de l'Université P. et M. Curie No. 43* (1980/81)
10. van der Waerden, B.L.: On Hilbert's function, series of composition of ideals and a generalization of the theorem of Bezout. *Proc. R. Soc. Amsterdam* **31**, 749–770 (1929)
11. Wüstholz, G.: Über das Abelsche Analogon des Lindemannschen Satzes I. *Invent. Math.* **72**, 363–388 (1983)
12. Yu, K.: Linear forms in elliptic logarithms. *J. Number Theory* **20**, 1–69 (1985)
13. Moreau, J.C.: Démonstrations géométriques de lemmes de zéros II. *Approximations diophantiennes et nombres transcendants*. In: *Progress in Math.*, Vol. 31, pp. 191–197. Boston-Basel-Stuttgart: Birkhäuser 1982

Oblatum 15-V-1984 & 27-IX-1984