Fields' off-site summer school at the University of Ottawa
Analytic Number Theory and Diophantine Approximation, June 30 – July 11, 2008

Zero Estimates
Lectures 1 and 2

Damien Roy (*University of Ottawa*)

The natural context for transcendental number theory is that of a commutative algebraic group G. The object of a zero estimate is basically to provide constraints on the degree of a polynomial vanishing on certain types of subsets of G reflecting the group structure of G. Thanks mainly to the work of D. Masser [5], J.-C. Moreau [6], D. Masser and G. Wüstholz [7], and P. Philippon [9], we dispose of very efficient results of that sort. Here we consider the most simple situation, namely the case where the algebraic group G is a power of the multiplicative group. It provides nevertheless a good illustration of the general strategy involved in the proof of the more general zero estimates and, as we will see in the last lecture, this special case has important applications in the study of the transcendence or the algebraic independence of the values of the usual exponential function. In fact, the first zero estimates by D. Masser [5] were precisely concerned with the multiplicative group and motivated by the construction of an auxiliary function by M. Waldschmidt [13] dealing with values of the exponential function. The zero estimate that we prove in these lectures incorporates to the work of D. Masser a crucial idea of P. Philippon which makes possible to take into account the degree of the so-called *obstruction subgroup*.

1. Some Algebraic Geometry

Let K be an algebraically closed field of characteristic zero (for example $\mathbb{C}$ or the algebraic closure of $\mathbb{Q}$ in $\mathbb{C}$), and let n be a positive integer. We denote by $K[\underline{X}] = K[X_1, \dots, X_n]$ the polynomial ring in n variables over K, and for each integer $D \geq 0$, we denote by $K[\underline{X}]_{\leq D}$ the subspace of $K[\underline{X}]$ consisting of all polynomials of degree at most D. A basis of this vector space is given by the monomials

$$\underline{X}^{\mathbf{i}} = X_1^{i_1} \cdots X_n^{i_n} \quad \text{with } \mathbf{i} = (i_1, \dots, i_n) \in \mathbb{N}^n \text{ of } \textit{length } |\mathbf{i}| := i_1 + \cdots + i_n \leq D,$$

and so we have

$$\dim_K K[\underline{X}]_D = \binom{D+n}{n}.$$

If Σ is a subset of K^n with finite cardinality denoted $\mathrm{Card}(\Sigma)$, asking that a polynomial P of $K[\underline{X}]_{\leq D}$ vanishes at each point of Σ is equivalent to a system of $\mathrm{Card}(\Sigma)$ linear equations in the $\binom{D+n}{n}$ unknown coefficients of P . So, when $\mathrm{Card}(\Sigma) < \binom{D+n}{n}$, there exists a non-zero polynomial of $K[\underline{X}]_{\leq D}$ vanishing at each point of Σ.

For $n = 1$, this statement is optimal as a non-zero polynomial of degree $\leq D$ in one variable has at most D zeros. However, the converse is far from being true when $n \geq 2$ because in that case a non-zero polynomial P has an infinite set of zeros

$$Z(P) = \{\mathbf{x} := (x_1, \ldots, x_n) \in K^n \,;\, P(\mathbf{x}) = 0\}.$$

Thus, in order to get information on a polynomial P from the knowledge that it vanishes on some set Σ, we need additional structure on Σ. As we mentioned in the presentation, the structure that we will consider later comes from the group law of some algebraic group.

1.1. **Algebraic Subsets of K^n.** References for this section are [17, Ch. VII, §3] and [4, Ch. 1,§1]. For simplicity, we limit the presentation to closed algebraic sets:

Definition 1. A (closed) *algebraic subset* of K^n is a subset of K^n which is the set of common zeros of a family $\mathcal{F}$ of polynomials in $K[\underline{X}] = K[X_1, \ldots, X_n]$, denoted $Z(\mathcal{F})$.

From this, it follows that the intersection of a family of algebraic subsets of K^n is again an algebraic subset of K^n and that a finite union of algebraic subsets of K^n is also an algebraic subset of K^n.

Definition 2. An algebraic subset of K^n is called (geometrically) *irreducible* if it is not empty and cannot be written as the union of two algebraic subsets of K^n properly contained in it. An irreducible algebraic subset of K^n is also called an *algebraic subvariety* of K^n or simply a *subvariety* of K^n.

Thus, if an algebraic subvariety of K^n is contained in a finite union of algebraic subsets of K^n, then it is contained in one of them. The space K^n and the points of K^n are examples of subvarieties of K^n, but the empty set is excluded. One can show that each algebraic subset W of K^n is a finite (possibly empty) union of subvarieties $W_1, \ldots, W_s$ of K^n:

$$W = W_1 \cup \cdots \cup W_s.$$

In this decomposition of W, one can impose the condition $W_i \not\subseteq W_j$ for $i \neq j$. In this case the subvarieties W_i are uniquely determined: they are the maximal subvarieties of K^n contained in W, and are called the *irreducible components* of W.

Definition 3. The *dimension* of an algebraic subvariety W of K^n is the largest integer d for which there exists a strictly increasing chain

$$W_0 \subset W_1 \subset \cdots \subset W_d = W$$

of subvarieties of K^n ending with W.

It can be shown that this integer always exists and is $\leq n$. In fact, any chain like the above can be refined to a maximal one by inserting subvarieties before W_0 or between two consecutive ones until this becomes impossible without introducing repetitions, and the number of subvarieties in any such maximal chain ending with W is $d + 1$ where d is the

dimension of W. It follows from the definition that if $W_1 \subset W_2$ are two distinct subvarieties of K^n, then $\dim(W_1) < \dim(W_2)$. The dimension of a point is 0, and for K^n it is n.

Definition 4. The *dimension* of a non-empty algebraic subset of K^n is the maximum of the dimensions of its irreducible components.

Thus, if W, W' are non-empty algebraic subsets of K^n with $W' \subseteq W$, then we have $\dim(W') \leq \dim(W)$, *with equality if and only if* W *and* W' *have a common irreducible component of dimension* $\dim(W)$. This follows from the fact that each irreducible component of W' is contained in one of W. *In particular, an algebraic subset* W *of* K^n *of dimension* d *contains only finitely many subvarieties of* K^n *of dimension* d.

Definition 5. An algebraic subset of K^n is said to be *equidimensional* if all its irreducible components have the same dimension.

1.2. **Hilbert–Samuel Polynomial.** Let W be a non-empty algebraic subset of K^n and let $K[W]$ be the set of all maps from W to K induced by polynomials in $K[X_1, \ldots, X_n]$. Then $K[W]$ is a subring of the ring of all functions from W to K and the restriction map

$$\mathrm{res}_W \colon K[\underline{X}] \longrightarrow K[W]$$

is a surjective homomorphism of rings. Its kernel is thus an ideal of $K[\underline{X}]$. It consists of all polynomials of $K[\underline{X}]$ vanishing identically on W. It is called the *ideal* of W and denoted $I(W)$. The above map therefore induces an isomorphism of rings

$$K[\underline{X}]/I(W) \sim K[W] \ .$$

Observe that if W_1 and W_2 are two algebraic subsets of K^n, then we have $W_1 \subseteq W_2$ if and only if $I(W_2) \subseteq I(W_1)$. This follows from the fact that W_i is the set of common zeros of the elements of $I(W_i)$. In particular, W_1 and W_2 are equal if and only if $I(W_1) = I(W_2)$. Another property that we will need is that an algebraic subset W of K^n is irreducible if and only if $I(W)$ is a prime ideal of $K[\underline{X}]$.

Definition 6. The *Hilbert function* of an algebraic subset $W \neq \emptyset$ of K^n is the map $H(W;-)\colon \mathbb{N} \to \mathbb{N}$ given by

$$H(W;D) = \dim_K \left(\mathrm{res}_W K[\underline{X}]_{\leq D}\right)$$

for each integer $D \in \mathbb{N}$. This is also given by

$$H(W;D) = \dim_K \left((K[\underline{X}]_{\leq D} + I)/I\right)$$

where $I = I(W)$ is the ideal of W.

This function carries many informations about W. First of all, it can be shown that for all sufficiently large $D \in \mathbb{N}$, its value at D is given by a polynomial in D whose degree is the dimension of W:

$$H(W;D) = \sum_{i=0}^{d} a_i D^i \qquad \text{with} \quad d = \dim(W).$$

This polynomial is called the *Hilbert–Samuel polynomial* of W. It can be shown that all its coefficients are rational numbers and that $d!$ is a common denominator for them. In particular, the product $d!a_d$ is a positive integer. It is called the *degree* of W and denoted $\deg(W)$. Geometrically, the intersection of W with a linear affine subvariety L of K^n of dimension $n-d$ is *in general* finite with cardinality is equal to $\deg(W)$. In fact, when $W \cap L$ is finite, its cardinality is at most equal to $\deg(W)$. A reference for this is [4, Ch. 1, §7] upon noting that the definition given above for the Hilbert function of W coincides with that of its Zariski closure in the projective space $\mathbb{P}_n(K)$ under the natural embedding of K^n in $\mathbb{P}_n(K)$.

Following an idea of P. Philippon, it is useful to encode both invariants (the dimension and the degree) in a single object:

Definition 7. For any non-empty algebraic subset W of K^n, we denote by

$$\mathcal{H}(W;D) = \deg(W)D^{\dim(W)}$$

the leading term of the Hilbert-Samuel polynomial of W multiplied by $\dim(W)!$.

Example 1. For $W = K^n$, we have

$$H(K^n;D) = \dim_K\left(K[\underline{X}]_{\leq D}\right) = \binom{D+n}{n} = \frac{1}{n!}D^n + \cdots,$$

hence the degree of K^n is 1, and we have $\mathcal{H}(K^n;D) = D^n$.

We state without proof the following important fact (see [4, Ch. 1, Prop. 7.6 (b)] or [12, Thm. 8]):

Proposition 1.1. *If W is an algebraic subset of K^n of dimension d and if $W_1, \ldots, W_r$ are its irreducible components of dimension d, then*

$$\mathcal{H}(W;D) = \sum_{i=1}^{r} \mathcal{H}(W_i;D).$$

In other words, the degree of W is the sum of the degrees of its irreducible components with largest dimension.

1.3. **Philippon's Upper Bound.** The following result is a special case of P. Philippon's general upper bound for the function $\mathcal{H}$, which plays a central role in the proof of zero estimates (see [9, Prop. 3.3]).

Theorem 1.2. *Let U be an algebraic subset of K^n and let E be the set of common zeros in U of a family $\mathcal{F}$ of polynomials of $K[\underline{X}]_{\leq D}$. Assume that E is not empty. Then, we have*

$$\mathcal{H}(E;D) \leq \mathcal{H}(U;D).$$

In order to prove the theorem, we first consider the case where U is irreducible and $\mathcal{F}$ consists of just one polynomial. This amounts to showing:

Lemma 1.3. *Let W be an algebraic subvariety of K^n of dimension $d \geq 1$, let $P \in K[\underline{X}]_{\leq D}$ for some positive integer D, and let $Z = Z(P)$ denote the zero set of P in K^n. Assume that $W \cap Z$ is not empty and distinct from W. Then, $W \cap Z$ is an equidimensional algebraic subset of K^n of dimension $d-1$, and we have*

$$\mathcal{H}(W \cap Z; D) \leq \mathcal{H}(W; D).$$

Proof. The fact that $W \cap Z$ is equidimensional of dimension $d-1$ follows from Krull's principal ideal theorem applied to the quotient $K[\underline{X}]/I(W)$. The inequality involving the function $\mathcal{H}$ follows from [9, Lemma 3.1]. It is however simple to give a direct proof of this inequality. For any integer $T \in \mathbb{N}$, the restriction map

$$\mathrm{res}_W\left(K[\underline{X}]_{\leq T+D}\right) \longrightarrow \mathrm{res}_{Z\cap W}\left(K[\underline{X}]_{\leq T+D}\right)$$

is linear, surjective and, since P vanishes identically on Z, its kernel contains the image of $\mathrm{res}_W\left(K[\underline{X}]_{\leq T}\right)$ under multiplication by $\mathrm{res}_W(P)$. Moreover, the multiplication by $\mathrm{res}_W(P)$ is injective on $K[W] = \mathrm{res}_W\big(K[\underline{X}]\big)$ because W is irreducible and not contained in Z. Comparing dimensions, this implies

$$\begin{aligned} H\big(Z \cap W; T+D\big) &= \dim_K\left(\mathrm{res}_{Z\cap W}\left(K[\underline{X}]_{\leq T+D}\right)\right) \\ &\leq \dim_K\left(\mathrm{res}_W\left(K[\underline{X}]_{\leq T+D}\right)\right) - \dim_K\left(\mathrm{res}_W\left(K[\underline{X}]_{\leq T}\right)\right) \\ &= H\big(W; T+D\big) - H\big(W; T\big). \end{aligned}$$

Now, fix a choice of $C \in \mathbb{N}$ and, for each integer $t \geq 0$, define

$$p(t) = H\big(W; C+tD\big) \quad \text{and} \quad q(t) = H\big(Z \cap W; C+tD\big).$$

Then, assuming that C is sufficiently large, the integers $p(t)$ and $q(t)$ are given by polynomials in t of degree d and $d-1$ respectively and the preceding observation applied with $T = C + (t-1)D$ gives

$$q(t) \leq p(t) - p(t-1).$$

Going back to the definition of the function $\mathcal{H}$, we deduce that

$$\mathcal{H}\big(Z \cap W; D\big) = (d-1)! \lim_{t\to\infty} \frac{q(t)}{t^{d-1}} \leq (d-1)! \lim_{t\to\infty} \frac{p(t)-p(t-1)}{t^{d-1}} = d! \lim_{t\to\infty} \frac{p(t)}{t^d} = \mathcal{H}\big(W; D\big).$$

□

Proof of Theorem 1.2. Let $d = \dim(U)$ and $r = d - \dim(E)$. By induction on the integer $i = 0, \ldots, r$, we shall construct an equidimensional algebraic subset $E_i \subseteq U$ of dimension $d-i$ which contains E and satisfies

$$\mathcal{H}(E_i; D) \leq \mathcal{H}(U; D). \tag{1}$$

For $i = 0$, we set $E_0 = U$. Assume that E_i is constructed for an integer $i \geq 0$ with $i < r$, and let $W_1, \ldots, W_s$ be its irreducible components. We have

$$E \subseteq W_1 \cup \cdots \cup W_s.$$

Since $\dim(W_j) = d - i > \dim(E)$, there exists for each j a polynomial $P_j \in \mathcal{F}$ which does not vanish everywhere on W_j; let Z_j be the set of zeros of P_j in K^n. We define

$$E_{i+1} = (W_1 \cap Z_1) \cup \cdots \cup (W_s \cap Z_s).$$

By construction, E_{i+1} contains E, therefore it is not empty. Without loss of generality, we may assume that there exists an integer $t \geq 1$ such that $W_j \cap Z_j \neq \emptyset$ for $j = 1, \ldots, t$, and $W_j \cap Z_j = \emptyset$ for $j > t$. Then, Lemma 1.3 shows that $W_j \cap Z_j$ is an equidimensional algebraic subset of K^n of dimension $d - i - 1$ for $j = 1, \ldots, t$. Therefore, E_{i+1} is also equidimensional of dimension $d - i - 1$ and its irreducible components are the union of those of $W_j \cap Z_j$ for $j = 1, \ldots, t$. By virtue of Proposition 1.1, this gives

$$\mathcal{H}(E_{i+1}; D) \leq \sum_{j=1}^{t} \mathcal{H}(W_j \cap Z_j; D).$$

Since each P_j is of degree $\leq D$, we also have, by Lemma 1.3,

$$\sum_{j=1}^{t} \mathcal{H}(W_j \cap Z_j; D) \leq \sum_{j=1}^{t} \mathcal{H}(W_j; D).$$

Moreover, since $W_1, \ldots, W_t$ are among the irreducible components of E_i of dimension $d - i$, Proposition 1.1 gives furthermore

$$\sum_{j=1}^{t} \mathcal{H}(W_j; D) \leq \mathcal{H}(E_i; D).$$

Combining these inequalities with (1), we get $\mathcal{H}(E_{i+1}; D) \leq \mathcal{H}(U; D)$ as required. This shows the existence of $E_0, \ldots, E_r$.

Since E and E_r have the same dimension $d - r$, the inclusion $E \subseteq E_r$ implies that the irreducible components of V of dimension $d - r$ are among those of E_r; therefore applying Proposition 1.1 once again and using the relation (1) with $i = r$, we get

$$\mathcal{H}(E; D) \leq \mathcal{H}(E_r; D) \leq \mathcal{H}(U; D).$$

The proof is complete. □

2. The Group $\mathbb{T}$ and its Algebraic Subgroups

An *affine algebraic group* is an algebraic subset U of K^n which also has a group structure with the group law $(\mathbf{x}, \mathbf{y}) \mapsto \mathbf{x} \cdot \mathbf{y}$ and the map $\mathbf{x} \mapsto \mathbf{x}^{-1}$ given by polynomials:

$$\mathbf{x} \cdot \mathbf{y} = (P_1(\mathbf{x}, \mathbf{y}), \ldots, P_n(\mathbf{x}, \mathbf{y})), \qquad \mathbf{x}^{-1} = (Q_1(\mathbf{x}), \ldots, Q_n(\mathbf{x}))$$

with $P_1, \ldots, P_n \in K[\underline{X}, \underline{Y}]$ and $Q_1, \ldots, Q_n \in K[\underline{X}]$. An *algebraic subgroup* of U is a subgroup of U which, as a set, is also an algebraic subset of K^n.

Let d be a positive integer, and let $\mathbb{T}$ denote the product $(K^\times)^d$ of d copies of the multiplicative group $K^\times$ of all non-zero elements of K. Then, $\mathbb{T}$ is a commutative group for the product structure. Its group law is given by

$$(x_1, \dots, x_d) \cdot (x'_1, \dots, x'_d) = (x_1 x'_1, \dots, x_d x'_d).$$

However, $\mathbb{T}$ is not an affine algebraic group in our sense because it is not an algebraic subset of K^d and the map $g \mapsto g^{-1}$ is not given by polynomials.

To correct this situation, we put $n = 2d$ and consider the algebraic subset U of K^n given by

$$U = \{(\mathbf{x}, \mathbf{y}) \in K^d \times K^d \ ; \ x_1 y_1 = \cdots = x_d y_d = 1\}.$$

This is a subgroup of $(K^\times)^{2d}$ and since the inverse of an element $(\mathbf{x}, \mathbf{y})$ of U is given by $(\mathbf{y}, \mathbf{x})$, we see that U is an affine algebraic group. Moreover, the projection map π from $K^d \times K^d$ to K^d which sends a point $(\mathbf{x}, \mathbf{y})$ to $\mathbf{x}$ induces a group isomorphism $\pi : U \to \mathbb{T}$. We will use it to carry on $\mathbb{T}$ the structures that apply to U.

(i) A *regular map* or simply a *polynomial* on $\mathbb{T}$ will be a map $f : \mathbb{T} \to K$ such that $f \circ \pi : U \to K$ is induced by a polynomial on K^n. These maps form a ring which we will denote $K[\mathbb{T}]$. Since for all $(\mathbf{x}, \mathbf{y}) \in U$ we have $y_i = x_i^{-1}$ $(i = 1, \dots, d)$, this ring is simply the ring of all maps from $\mathbb{T}$ to K induced by polynomials in $X_1, \dots, X_d, X_1^{-1}, \dots, X_d^{-1}$. Thus $K[\mathbb{T}]$ is isomorphic to $K[\underline{X}^{\pm 1}]$ and we will identify both rings.

(ii) An *algebraic subset* of $\mathbb{T}$ will be a subset E of $\mathbb{T}$ such that $\pi^{-1}(E)$ is an algebraic subset of K^n. By virtue of (i), an algebraic subset of $\mathbb{T}$ is therefore the set of common zeros in $\mathbb{T}$ of a family of polynomials in $K[\mathbb{T}] = K[\underline{X}^{\pm 1}]$. When $E \neq \emptyset$, we will denote by $K[E]$ the ring of all maps from E to K induced by elements of $K[\mathbb{T}]$. It is isomorphic to $K[\mathbb{T}]/I$ where I is the ideal of all elements of $K[\mathbb{T}]$ vanishing identically on E. This ideal I will be called the *ideal* of E, and denoted $I(E)$. In particular, a subgroup $\mathbb{T}^*$ of $\mathbb{T}$ will be said to be *algebraic* if it is an algebraic subset of $\mathbb{T}$.

(iii) We say that a polynomial $P \in K[\mathbb{T}]$ has *degree* $\leq D$, for a given integer $D \geq 0$, if the map $P \circ \pi : U \to K$ is induced by an element of $K[\underline{X}, \underline{Y}]$ of total degree $\leq D$. Explicitly, this means that there exists $Q \in K[\underline{X}, \underline{Y}]_{\leq D}$ such that

$$P = Q(X_1, \dots, X_d, X_1^{-1}, \dots, X_d^{-1}).$$

We denote by $K[\mathbb{T}]_{\leq D}$ the subspace of $K[\mathbb{T}]$ consisting of all polynomials of degree at most D. A basis for this vector space is the set of monomials

$$\underline{X}^{\mathbf{i}} = X_1^{i_1} \cdots X_n^{i_n} \quad \text{with } \mathbf{i} = (i_1, \dots, i_d) \in \mathbb{Z}^d \text{ and } |\mathbf{i}| := |i_1| + \cdots + |i_n| \leq D.$$

Given an algebraic subset $E \neq \emptyset$ of $\mathbb{T}$, we define its *Hilbert function* $H(E; D)$ in two equivalent ways either as $H(\pi^{-1}(E); D)$ or as the dimension over K of the space of maps $f : E \to K$ induced by elements of $K[\mathbb{T}]$ of degree $\leq D$. We also define the *dimension* of E as the dimension of $\pi^{-1}(E)$. When this dimension is m, we define $\mathcal{H}(E; D)$ as the product by $m!$

of the homogeneous part of degree m of the polynomial in D which coincides with $H(E;D)$ for large integral values of D.

2.1. **Structure of the Algebraic Subgroups.** For each $\mathbf{i} = (i_1, \ldots, i_d) \in \mathbb{Z}^d$, the map

$$\begin{array}{rccc} \chi_{\mathbf{i}} & : & \mathbb{T} & \longrightarrow & K^\times \\ & & \mathbf{x} & \longmapsto & \mathbf{x}^{\mathbf{i}} = x_1^{i_1} \cdots x_d^{i_d} \end{array} \tag{2}$$

induced by the monomial $\underline{X}^{\mathbf{i}}$ is a *character* of $\mathbb{T}$, namely a group homomorphism from $\mathbb{T}$ to the multiplicative group $K^\times$ of the field K. The kernel of $\chi_{\mathbf{i}}$ is the zero set of $\underline{X}^{\mathbf{i}} - 1$ in $\mathbb{T}$. It is therefore an algebraic subgroup of $\mathbb{T}$. More generally, if S is any subset of $\mathbb{Z}^d$, the intersection of the kernels of the characters $\chi_{\mathbf{i}}$ with $\mathbf{i} \in S$ is the set of zeros in $\mathbb{T}$ of the ideal of $K[\mathbb{T}]$ generated by the polynomials $\underline{X}^{\mathbf{i}} - 1$ with $\mathbf{i} \in S$, and so it is an algebraic subgroup $\mathbb{T}_S$ of $\mathbb{T}$. We also note that the set $\hat{\mathbb{T}}$ of characters of $\mathbb{T}$ in $K^\times$ forms a group under multiplication and that

$$\chi_{\mathbf{i}} \cdot \chi_{\mathbf{j}} = \chi_{\mathbf{i}+\mathbf{j}} \quad \text{and} \quad \chi_{\mathbf{i}}^{-1} = \chi_{-\mathbf{i}}$$

for any $\mathbf{i}, \mathbf{j} \in \mathbb{Z}^d$. Therefore, we have $\mathbb{T}_S = \mathbb{T}_\Phi$ where Φ denotes the subgroup of $\mathbb{Z}^d$ generated by S. We will show that each algebraic subgroup of $\mathbb{T}$ is of this form. For this we will need the following lemma due to E. Artin.

Lemma 2.1. *Distinct characters of a group G into $K^\times$ are linearly independent over K.*

Proof. Suppose on the contrary that there exist distinct characters $\chi_1, \ldots, \chi_m$ of G into $K^\times$ which are linearly dependent over K, and assume that this set is minimal with this property. Then there are non-zero elements $a_1, \ldots, a_m$ of K such that

$$a_1\chi_1(g) + \cdots + a_m\chi_m(g) = 0$$

for each $g \in G$. Since a character of G is a non-zero map (it maps the neutral element of G to 1), we must have $m \geq 2$. This means that $\chi_1 \neq \chi_m$ and so there exists $g_1 \in G$ such that $\chi_1(g_1) \neq \chi_m(g_1)$. For each $g \in G$, we find

$$0 = \chi_m(g_1)\left(\sum_{i=1}^{m} a_i\chi_i(g)\right) - \sum_{i=1}^{m} a_i\chi_i(g_1 g) = \sum_{i=1}^{m-1} b_i\chi_i(g)$$

where $b_i = (\chi_m(g_1) - \chi_i(g_1))a_i$ for $i = 1, \ldots, m-1$. Since $b_1 \neq 0$, this shows that $\chi_1, \ldots, \chi_{m-1}$ are linearly dependent over K, a contradiction. □

Proposition 2.2. *Let $\mathbb{T}^*$ be an algebraic subgroup of $\mathbb{T}$. Then there exist a subgroup Φ of $\mathbb{Z}^d$ such that*

$$\mathbb{T}^* = \mathbb{T}_\Phi.$$

The ideal of $\mathbb{T}_\Phi$ is generated by the polynomials $\underline{X}^{\mathbf{i}} - 1$ with $\mathbf{i} \in \Phi$. Moreover, if this ideal contains a non-zero element of $K[\mathbb{T}]_{\leq D}$ for some integer $D \geq 1$, then Φ contains a non-zero element $\mathbf{i}$ with $|\mathbf{i}| \leq D$.

Proof. Define Φ to be the set of all $\mathbf{i} \in \mathbb{Z}^d$ such that $\mathbb{T}^*$ is contained in the kernel of $\chi_{\mathbf{i}}$, and let I denote the ideal of $K[\mathbb{T}]$ generated by the polynomials $\underline{X}^{\mathbf{i}} - 1$ with $\mathbf{i} \in \Phi$. Then, Φ is a subgroup of $\mathbb{Z}^d$ and since $I \subseteq I(\mathbb{T}^*)$ we have $\mathbb{T}^* \subseteq \mathbb{T}_\Phi$.

Now, choose a set S of representatives of the classes of $\mathbb{Z}^d$ modulo Φ, and denote by F the subspace of $K[\mathbb{T}]$ spanned by the monomials $\underline{X}^{\mathbf{i}}$ with $\mathbf{i} \in S$. For every $\mathbf{j} \in \mathbb{Z}^d$, there exists $\mathbf{i} \in S$ such that $\mathbf{j} - \mathbf{i} \in \Phi$ and so, $\underline{X}^{\mathbf{j}} = \underline{X}^{\mathbf{i}} + \underline{X}^{\mathbf{i}}(\underline{X}^{\mathbf{j}-\mathbf{i}} - 1)$ is congruent to $\underline{X}^{\mathbf{i}}$ modulo I. This shows that every element of $K[\mathbb{T}]$ is congruent modulo I to an element of F. Now, consider the restriction map from $K[\mathbb{T}]$ to $K[\mathbb{T}^*]$. By Artin's lemma 2.1, it is injective on F because it sends the monomials $\underline{X}^{\mathbf{i}}$ with $\mathbf{i} \in S$ to distinct characters of $\mathbb{T}^*$ (the restriction of $\chi_{\mathbf{i}}$ to $\mathbb{T}^*$). Since its kernel contains I, we conclude that $K[\mathbb{T}] = I \oplus F$ and that $I = I(\mathbb{T}^*)$, so $\mathbb{T}^* = \mathbb{T}_\Phi$.

Finally, if $I(\mathbb{T}^*)$ contains a non-zero element P of $K[\mathbb{T}]_{\leq D}$ for some $D \geq 1$, there should be at least two distinct monomials $\underline{X}^{\mathbf{i}}$ and $\underline{X}^{\mathbf{j}}$ appearing in P which induce the same character on $\mathbb{T}^*$. Then, Φ contains the non-zero point $\mathbf{i} - \mathbf{j} \in \mathbb{Z}^d$ with length $\leq D$. □

The above argument shows that the Hilbert function $H(\mathbb{T}_\Phi;\, D)$ of $\mathbb{T}_\Phi$ at an integer $D \geq 0$ is the number of distinct cosets of Φ of the form $\mathbf{i} + \Phi$ with $\mathbf{i} \in \mathbb{Z}^d$ of length $|\mathbf{i}| \leq D$. It is a good exercise to show that, if Φ has rank r, then $H(\mathbb{T}_\Phi;\, D)$ is bounded above and below by constant multiples of D^{d-r} and so $\mathbb{T}_\Phi$ has dimension $d - r$. In particular, when $\Phi = \{0\}$, one finds that

$$2^d \binom{D+d-1}{d} \leq H(\mathbb{T};\, D) \leq 2^d \binom{D+d}{d}$$

for each integer $D \geq 0$. So $\mathbb{T}$ has dimension d, and

$$\mathcal{H}(\mathbb{T};\, D) = (2D)^d.$$

2.2. **Translations.** For each $g \in \mathbb{T}$, we denote by $\tau_g \colon \mathbb{T} \to \mathbb{T}$, the translation by g in $\mathbb{T}$:

$$\tau_g(\mathbf{x}) = g\,\mathbf{x} \qquad \text{for each } \mathbf{x} \in \mathbb{T}.$$

Considering the group law in $\mathbb{T}$, we see that each τ_g is given in coordinates by polynomials of degree 1. We will need these operators in the proofs of the next three lemmas.

Lemma 2.3. *Let V be a non-empty algebraic subset of $\mathbb{T}$ and let $g \in \mathbb{T}$. Then, gV is an algebraic subset of $\mathbb{T}$ with the same dimension as V and we have*

$$\mathcal{H}(gV;\, D) = \mathcal{H}(V;\, D) \tag{3}$$

for each $D \in \mathbb{N}$. Moreover, gV is irreducible if V is irreducible.

Proof. By hypothesis, V is the set of common zeros in $\mathbb{T}$ of a family of polynomials $\{P_j\}_{j \in J}$. Therefore, $gV = \tau_g(V)$ is the set of common zeros in $\mathbb{T}$ of the polynomials $P_j \circ \tau_{-g}$ with $j \in J$. This proves that gV is an algebraic subset of $\mathbb{T}$.

The vector space of functions from gV to K is isomorphic to the vector space of functions from V to K under the map which sends a function $f \colon gV \to K$ to the composite $f \circ \tau_g \colon V \to$

K. If f is induced by a polynomial of degree $\leq D$, then $f \circ \tau_g$ is also induced by a polynomial of degree $\leq D$, and conversely. We therefore (3) holds for each $D \in \mathbb{N}$. In particular, V and gV have the same Hilbert-Samuel polynomial. Consequently, they have the same dimension, and the polynomials $\mathcal{H}(gV;\, D)$ and $\mathcal{H}(V;\, D)$ coincide.

Finally, assume that V is irreducible. If gV were not irreducible, it could be written as the union of two algebraic subsets V_1, V_2 of $\mathbb{T}$ both distinct from gV; then V would be the union of $g^{-1}V_1$ and $g^{-1}V_2$, and this is a contradiction since both are algebraic subsets of $\mathbb{T}$ which are distinct from V. Therefore gV is irreducible. □

Lemma 2.4. *Let $\mathbb{T}^*$ be an algebraic subgroup of $\mathbb{T}$, and let E be a finite and non-empty union of translates of $\mathbb{T}^*$ in $\mathbb{T}$. Then, E is an algebraic subset of $\mathbb{T}$ and, for each $D \in \mathbb{N}$, we have*

$$\mathcal{H}(E;\, D) = \mathrm{Card}(E/\,\mathbb{T}^*)\mathcal{H}(\mathbb{T}^*;\, D).$$

Proof. Let d^* be the dimension of $\mathbb{T}^*$. Lemma 2.3 shows that each translate $g\mathbb{T}^*$ of $\mathbb{T}^*$ is an algebraic subset of $\mathbb{T}$ of dimension d^* and that the polynomials $\mathcal{H}(g\mathbb{T}^*;\, D)$ and $\mathcal{H}(\mathbb{T}^*;\, D)$ coincide. Since E is a finite disjoint union of translates of $\mathbb{T}^*$, E is therefore an algebraic subset of $\mathbb{T}$ of dimension d^*, and the conclusion follows from Proposition 1.1. □

Lemma 2.5. *Let V and W be algebraic subsets of $\mathbb{T}$. Define*

$$E = \{g \in \mathbb{T}\,;\, gV \subseteq W\}.$$

Then E is an algebraic subset of $\mathbb{T}$. Moreover, if W is defined in $\mathbb{T}$ by polynomials of degree $\leq D$, then E is also defined in $\mathbb{T}$ by polynomials of degree $\leq D$.

Proof. Let $\{P_j\}_{j\in J}$ be a family of polynomials whose set of common zeros in $\mathbb{T}$ is W. We have

$$\begin{aligned} E &= \{g \in \mathbb{T}\,;\, gv \in W \text{ for all } v \in V\} \\ &= \{g \in \mathbb{T}\,;\, P_j(gv) = 0 \text{ for all } j \in J,\ v \in V\}. \end{aligned}$$

This shows that E is the set of common zeros in $\mathbb{T}$ of the polynomials $P_j \circ \tau_v$ with $j \in J$ and $v \in V$. Therefore E is an algebraic subset of $\mathbb{T}$. Furthermore, if the polynomials P_j are of degree $\leq D$, then the same holds for the polynomials $P_j \circ \tau_v$. This proves the second part of the lemma. □

3. The Main Result

The zero estimate that we now state and prove is due to Masser [5] and Philippon [9].

Theorem 3.1. *Let Σ be a subset of $\mathbb{T}$ containing the neutral element $e = (1, \ldots, 1)$ of $\mathbb{T}$. Assume that, for a given integer $D \geq 0$, there exists a non-zero element P of $K[\mathbb{T}]$ of degree $\leq D$ which vanishes at each point of the set*

$$\Sigma[d] := \left\{\sigma_1 \cdots \sigma_d\,;\, (\sigma_1, \ldots, \sigma_d) \in \Sigma^d\right\}.$$

Then there exists a non-zero subgroup Φ *of* $\mathbb{Z}^d$ *such that*

$$\mathrm{Card}\big((\Sigma\,\mathbb{T}_\Phi)/\,\mathbb{T}_\Phi\big)\,\mathcal{H}(\mathbb{T}_\Phi;\,D) \le \mathcal{H}(\mathbb{T};\,D). \tag{4}$$

Moreover, we may assume that Φ *contains a non-zero element* $\mathbf{i}$ *with* $|\mathbf{i}| \le D$.

In the above inequality, the expression $(\Sigma\,\mathbb{T}_\Phi)/\,\mathbb{T}_\Phi$ stands for the image of Σ under the canonical map from $\mathbb{T}$ to $\mathbb{T}\,/\,\mathbb{T}_\Phi$. It consists of all translates $\sigma\,\mathbb{T}_\Phi$ of $\mathbb{T}_\Phi$ with $\sigma \in \Sigma$. The conclusion of the theorem implies that it is a finite set even though Σ may be infinite.

Before we go into the proof of the above zero estimate, it is worthwhile to note that, if an integer $D \ge 1$ satisfies

$$\mathrm{Card}\big((\Sigma\,\mathbb{T}^*)/\,\mathbb{T}^*\big)\,H(\mathbb{T}^*;\,D) < H(\mathbb{T};\,D)$$

for a finite subset Σ of $\mathbb{T}$ and an algebraic subgroup $\mathbb{T}^*$ of $\mathbb{T}$, then the set $E = \cup_{\sigma\in\Sigma}(\sigma\,\mathbb{T}^*)$ satisfies $H(E;D) < H(\mathbb{T};\,D)$ and so there exists a non-zero polynomial $P \in K[\mathbb{T}]_{\le D}$ which vanishes at each point of $\Sigma \subseteq E$. The comparison of this condition with the main condition (4) of the theorem stresses the relevance of the asymptotic Hilbert-Samuel polynomial $\mathcal{H}$.

Proof. Let W_1 be the set of zeros of P in $\mathbb{T}$. For each integer $r \ge 2$, we define

$$W_r = \bigcap_{(\sigma_1,\dots,\sigma_{r-1})\in\Sigma^{r-1}} \big(\sigma_1^{-1}\cdots\sigma_{r-1}^{-1}\,W_1\big).$$

Alternatively, W_r is the set of common zeros in $\mathbb{T}$ of the polynomials $P\circ\tau_{\sigma_1\cdots\sigma_{r-1}}$ with $(\sigma_1,\dots,\sigma_{r-1}) \in \Sigma^{r-1}$. Therefore, it is defined in $\mathbb{T}$ by polynomials of degree $\le D$. The sets $W_1, W_2, \dots$ are related by the formulas

$$W_{r+1} = \bigcap_{\sigma\in\Sigma} \big(\sigma^{-1}W_r\big), \qquad (r \ge 1). \tag{5}$$

Since $e \in \Sigma$, this implies that they form a non-increasing sequence

$$W_1 \supseteq W_2 \supseteq \cdots \supseteq W_{d+1} \supseteq \cdots$$

Since P vanishes on $\Sigma[d]$, the set W_{d+1} contains e ; therefore the latter is not empty. On the other hand, since P is not identically zero on $\mathbb{T}$, Lemma 1.3 gives $\dim(W_1) = d-1$. Consequently, there exists a positive integer $r \le d$ such that

$$\dim(W_r) = \dim(W_{r+1}).$$

Let m be the common dimension of W_r and W_{r+1}, and let V be an irreducible component of dimension m of W_{r+1}. Using (5), we get

$$V \subseteq \bigcap_{\sigma\in\Sigma} \big(\sigma^{-1}W_r\big).$$

Hence, for each $\sigma \in \Sigma$, $\sigma\,V$ is contained in W_r. This means that the set

$$E = \{g \in \mathbb{T}\,;\, gV \subseteq W_r\}$$

contains Σ. We also define

$$\mathbb{T}^* = \{g \in \mathbb{T}\,;\, gV = V\} \quad \text{and} \quad R = \{gV\,;\, g \in E\}.$$

From Lemma 2.3 we deduce that the elements of the set R are, like V, algebraic subvarieties of $\mathbb{T}$ of dimension m. Since they are contained in W_r, and since W_r has dimension m, R is a finite set. We also note that $\mathbb{T}^*$ is a subgroup of $\mathbb{T}$, that E is stable under translation by the elements of $\mathbb{T}^*$, and that the map from E to R sending g to gV induces a bijection

$$\begin{array}{ccc} E/\mathbb{T}^* & \longrightarrow & R \\ g\,\mathbb{T}^* & \longmapsto & gV. \end{array}$$

Therefore E is a finite union of translates of $\mathbb{T}^*$. Now recall that, by Lemma 2.3, the translates of V are irreducible subsets of $\mathbb{T}$ of the same dimension as V. So, for any $g \in \mathbb{T}$, the condition $g\,V \subseteq V$ is equivalent to $g\,V = V$. Then Lemma 2.5, with $W = V$, shows that $\mathbb{T}^*$ is an algebraic subset of $\mathbb{T}$. Hence $\mathbb{T}^*$ is an algebraic subgroup of $\mathbb{T}$. Since it is contained in $v^{-1}V$ for any $v \in V$, its dimension is $\le m < d$. Applying again Lemma 2.5, but with $W = W_r$, shows that E is an algebraic subset of $\mathbb{T}$ which is defined, like W_r, by polynomials of degree $\le D$. Since E is a finite union of translates of $\mathbb{T}^*$, Lemma 2.4 gives

$$\mathrm{Card}(E/\mathbb{T}^*)\mathcal{H}(\mathbb{T}^*;\, D) = \mathcal{H}(E;\, D).$$

Moreover, since E is defined in $\mathbb{T}$ by polynomials of degree $\le D$, Theorem 1.2 provides an upper bound for the right hand side of the previous equality:

$$\mathcal{H}(E;\, D) \le \mathcal{H}(\mathbb{T};\, D).$$

Since $\Sigma \subseteq E$, we also note that

$$\mathrm{Card}\big((\Sigma\,\mathbb{T}^*)/\mathbb{T}^*\big) \le \mathrm{Card}(E/\mathbb{T}^*).$$

Finally, as $\mathbb{T}^*$ is contained in E, its ideal contains some non-zero element of $K[\mathbb{T}]_{\le D}$ and so Proposition 2.2 shows that $\mathbb{T}^* = \mathbb{T}_\Phi$ for a subgroup Φ of $\mathbb{Z}^d$ which contains a non-zero element of $\mathbb{Z}^d$ of length $\le D$. The conclusion (4) follows by combining the last relations. □

4. An application

When discussing Gel'fond's problem in Lecture 5, we will need the following consequence of the above zero estimate.

Proposition 4.1. *Let $\underline{\gamma}_j = (\gamma_{1,j}, \dots, \gamma_{d,j}) \in \mathbb{T}$ for $j = 1, \dots, \ell$, and let D, $S \in \mathbb{N}^*$. Suppose that*

$$\prod_{i=1}^{d} \prod_{j=1}^{\ell} \gamma_{i,j}^{m_i s_j} \neq 1 \tag{6}$$

for each choice of $m_1, \dots, m_d, s_1, \dots, s_\ell \in \mathbb{Z}$ with

$$0 < |m_1| + \cdots + |m_d| \le D \quad \text{and} \quad 0 < \max\{|s_1|, \dots, |s_\ell|\} \le S.$$

Suppose also that there exists a non-zero polynomial $P \in K[\mathbb{T}]_{\leq D}$ which vanishes at each point of the set

$$\Gamma(S) := \{\underline{\gamma}_1^{s_1} \cdots \underline{\gamma}_\ell^{s_\ell} \, ; \, 0 \leq s_1, \ldots, s_\ell \leq S\}.$$

Then, we have $(2D)^d \geq (S/d)^\ell$.

Proof. Define $\Sigma = \Gamma([S/d])$. Since

$$\Sigma[d] = \Gamma(d[S/d]) \subseteq \Gamma(S) \subseteq Z(P),$$

the zero estimate of the previous section shows the existence of a subgroup Φ of $\mathbb{Z}^d$ of rank r with $1 \leq r \leq d$ satisfying (4). Since $\mathcal{H}(\mathbb{T}_\Phi; D) \geq D^{d-r}$ and $\mathcal{H}(\mathbb{T}; D) = (2D)^d$, this means that

$$\mathrm{Card}\big((\Sigma\, \mathbb{T}_\Phi)/\, \mathbb{T}_\Phi\big) \leq 2^d D^r. \tag{7}$$

Moreover, we may assume that Φ contains at least one non-zero element $(m_1, \ldots, m_d)$ with $|m_1| + \cdots + |m_d| \leq D$. Now, suppose that we have

$$\underline{\gamma}_1^{s_1} \cdots \underline{\gamma}_\ell^{s_\ell}\, \mathbb{T}_\Phi \;=\; \underline{\gamma}_1^{s'_1} \cdots \underline{\gamma}_\ell^{s'_\ell}\, \mathbb{T}_\Phi$$

for integers $s_1, \ldots, s_\ell, s'_1, \ldots, s'_\ell$ taken from the set $\{0, 1, \ldots, [S/d]\}$. Then,

$$\underline{\gamma}_1^{s''_1} \cdots \underline{\gamma}_\ell^{s''_\ell} \in \mathbb{T}_\Phi$$

with $s''_j = s_j - s'_j$ for $j = 1, \ldots, \ell$, and so

$$\prod_{i=1}^{d} \left(\prod_{j=1}^{\ell} \gamma_{i,j}^{s''_j} \right)^{m_i} = 1.$$

Since the integers s''_j have absolute value $|s''_j| \leq [S/d] \leq S$ for $j = 1, \ldots, \ell$, the hypothesis forces them to vanish, and so we have $s_j = s'_j$ for each j. This means that

$$\mathrm{Card}\big((\Sigma\, \mathbb{T}_\Phi)/\, \mathbb{T}_\Phi\big) \geq \big([S/d] + 1\big)^\ell > (S/d)^\ell.$$

Substituting this estimate into (7) and taking into account that $r \leq d$, we conclude that $(S/d)^\ell \leq (2D)^d$. □

Note that the condition (6) is fulfilled if we choose

$$\underline{\gamma}_j = (e^{x_1 y_j}, \ldots, e^{x_d y_j}) \quad (j = 1, \ldots, \ell)$$

where $x_1, \ldots, x_d \in \mathbb{R}$ and $y_1, \ldots, y_\ell$ are sequences of $\mathbb{Q}$-linearly independent real numbers. This is because, for integers $m_1, \ldots, m_d, s_1, \ldots, s_\ell$, the product

$$\prod_{i=1}^{d} \prod_{j=1}^{\ell} \big(e^{x_i y_j}\big)^{m_i s_j} = e^{(\sum m_i x_i)(\sum s_j y_j)}$$

is not equal to 1 unless $\sum m_i x_i = 0$ or $\sum s_j y_j = 0$, that is unless all $m_1, \ldots, m_d$ or all $s_1, \ldots, s_\ell$ are zero.

5. Further reading

For a more complete presentation of zero estimates on linear algebraic groups, the reader may look at Chapters 5 and 8 of [14]. An exposition of zero estimates for general commutative algebraic groups including their applications to transcendental number theory can be found in the Bourbaki lecture of D. Bertrand [1]. One may also look at [11]. However, the reader is encouraged to look at the original papers of W. D. Brownawell and D. W. Masser [2], D. W. Masser [5], D. W. Masser and G. Wüstholz [7], J.-C. Moreau [6] (which gives a geometric exposition of the zero estimates of [7], together with a generalization to multi-projective space), G. Wüstholz [15, 16], P. Philippon [9], as well as the more recent works of L. Denis [3], M. Nakayame [8] and P. Philippon [10].

6. Exercises

Exercise 1. Use Theorem 1.2 to show that if F is a finite algebraic subset of K^n defined by polynomials of $K[X_1, \dots, X_n]$ of degree $\leq D$, then the cardinality of F is $\leq D^n$.

Hint. Show that for a finite algebraic subset F of K^n, the polynomial $\mathcal{H}(F; D)$ is constant, equal to the cardinality of F.

Exercise 2. Show that for subgroups Φ and Ψ of $\mathbb{Z}^d$, one has $\mathbb{T}_\Phi \subseteq \mathbb{T}_\Psi$ if and only if $\Psi \subseteq \Phi$. Deduce that the assignment $\Phi \mapsto T_\Phi$ defines a bijection between the set of subgroups of $\mathbb{Z}^d$ and the set of algebraic subgroups of $\mathbb{T}$.

Exercise 3. Let $D \in \mathbb{N}$. Show that if an algebraic subgroup $\mathbb{T}^*$ of $\mathbb{T}$ is contained in an algebraic subset E of $\mathbb{T}$ of the same dimension t, defined by elements of $K[\mathbb{T}]_{\leq D}$, then $\mathbb{T}^* = \mathbb{T}_\Phi$ for a subgroup Φ of $\mathbb{Z}^d$ of rank $d - t$ containing $d - t$ linearly independent elements of $\mathbb{Z}^d$ of length $\leq D$.

Remark. Using geometry of numbers, one can even show the existence of linearly independent points $\mathbf{i}_1, \dots, \mathbf{i}_{d-t}$ satisfying $|\mathbf{i}_1| \leq \cdots \leq |\mathbf{i}_{d-t}| \leq D$ and $\deg(\mathbb{T}^*) \asymp |\mathbf{i}_1| \cdots |\mathbf{i}_{d-t}|$ with implied constants depending only on d.

Exercise 4. Let H be an algebraic subgroup of $\mathbb{T}$ of dimension m and let V be an irreducible component of H of the same dimension. Define

$$H_0 = \{g \in \mathbb{T}\,;\, gV = V\} \quad \text{and} \quad R = \{gV\,;\, g \in H\}.$$

(a) Show that H_0 is an algebraic subgroup of H, that R is the set of all irreducible components of H and that the quotient H/H_0 is in bijection with R.

(b) Deduce from (a) that H is equidimensional, that its irreducible components are disjoint and that the one which contains e is an algebraic subgroup of H.

References

[1] D. Bertrand, Lemmes de zéros et nombres transcendants, in: Séminaire Bourbaki 1985/86, *Astérisque* **145-146** (1987), 21–44.

[2] W. D. Brownawell and D. W. Masser, Multiplicity estimates for analytic functions II, *Duke Math. J.* **47** (1980), 273–295.

[3] L. Denis, Lemmes de multiplicités et intersection, *Comment. Math. Helvetici* **70** (1995), 235-247.

[4] R. Hartshorne, *Algebraic Geometry*, Springer Verlag, New-York-Heidelberg-Berlin, 1977.

[5] D. W. Masser, On polynomials and exponential polynomials in several variables, *Invent. Math.* **63** (1981), 81–95.

[6] J.-C. Moreau, Démonstrations géométriques de lemmes de zéros, II, in: *Approximation diophantienne et nombres transcendants*, Luminy 1982, Birkhaüser Progress in Math. **31** (1983), 191–197.

[7] D. W. Masser and G. Wüstholz, Zero Estimates on Group Varieties I, *Invent. Math.* **64** (1981), 489–516; II, *Invent. Math.* **80** (1985), 233–267.

[8] M. Nakayame, Multiplicity estimates and the product theorem, *Bull. Soc. Math. France* **123** (1995), 155-188.

[9] P. Philippon, Lemmes de zéros dans les groupes algébriques commutatifs, *Bull. Soc. Math. France* **114** (1986), 355–383; Errata et addenda, *ibidem* **155** (1987), 397–398.

[10] P. Philippon, Nouveaux lemmes de zéros dans les groupes algébriques commutatifs, *Rocky Mountain J. Math.* **26** (1996), 1069–1088).

[11] D. Roy, Zero estimates on commutative algebraic groups, in:*Introduction to algebraic independence theory*, Yu. V. Nesterenko and P. Philippon eds, Lecture Notes in Mathematics Vol. 1752, Springer-Verlag, Berlin, 2001, 167–185.

[12] B. V. L. Van der Waerden, On Hilbert's functions, series of composition of ideals and a generalization of a theorem of Bezout, *Proc. Royal Acad. Amsterdam* **31** (1928), 749-770.

[13] M. Waldschmidt, Transcendance et exponentielles en plusieurs variables, *Invent. Math.* **63** (1981), 97–127.

[14] M. Waldschmidt, *Diophantine approximation on linear algebraic groups*, Grundlehren der math. Wiss. **326**, Springer, 2000.

[15] G. Wüstholz, Recent progress in transcendence theory, in: *Number Theory, Noordwijkerhout 1983*, H. Jager ed., Springer Lecture Notes in Math., vol. 1068 (1984), 280–296.

[16] G. Wüstholz, Multiplicity estimates on group varieties, *Annals of Math.* **129** (1989), 471–500.

[17] O. Zariski and P. Samuel, *Commutative Algebra*, Vol. I, II, Springer Verlag, New-York, 1968.

Département de Mathématiques, Université d'Ottawa,

585 King Edward, Ottawa, Ontario K1N 6N5, Canada

droy@uottawa.ca