15

LINEAR RELATIONS ON ALGEBRAIC GROUPS

D. W. Masser

1. Introduction

In this article we shall describe some aspects of the following type of problem, in particular its relationship with transcendence theory. Given non-zero algebraic numbers $\alpha_1, \ldots, \alpha_n$, how can we decide if they are multiplicatively dependent; that is, if there exist integers $m_1, \ldots, m_n$, not all zero, such that $\alpha_1^{m_1} \ldots \alpha_n^{m_n} = 1$?

The analogous question can be asked for an elliptic curve E defined over the field of algebraic numbers. Given points $P_1, \ldots, P_n$ of E also defined over this field, how can we decide if they are linearly dependent in the sense that there exist integers $m_1, \ldots, m_n$, not all zero, such that $m_1 P_1 + \ldots + m_n P_n$ is the origin O of E?

We shall see that there are elementary arguments from the geometry of numbers yielding certain estimates which enable the above problems to be solved fairly efficiently. In principle all the constants in these estimates are effectively computable. But it turns out that the fine structure of the constants can often be greatly improved by applying techniques from the theory of transcendental numbers. We present a short survey of such applications, without going into the proofs at all.

As is usual in the modern theory of transcendence, we generalize and unify the results and methods by stating them in terms of algebraic groups. Thus our setting is as follows. Let k be a number field, and let G be a commutative connected algebraic group, defined over k, with origin O. For a field K containing k denote by $G(K)$ the group of points in G defined over K. Let $\overline{k}$ be an algebraic closure of k, and suppose we are given points $P_1, \ldots, P_n$ in $G(\overline{k})$. We want to know if there exist integers $m_1, \ldots, m_n$, not all zero, such that

$$m_1 P_1 + \ldots + m_n P_n = O. \tag{1}$$

In fact we shall show how to find all $m = (m_1, \ldots, m_n)$ in $\mathbf{Z}^n$ such that (1) holds, in the sense that we shall find estimates for generators of the

additive group of all m in $\mathbf{Z}^n$ satisfying (1). For brevity we refer to this group as the "relation group" of $P_1, \ldots, P_n$. We will estimate the norms

$$|m| = \max(|m_1|, \ldots, |m_n|)$$

of such generators in terms of G and $P_1, \ldots, P_n$.

We lose no generality in supposing that $P_1, \ldots, P_n$ lie in $G(K)$ for some number field K. We will need a height function on $G(K)$, and for this we assume G is embedded in some projective space $\mathbf{P}_N$ by means of a very ample divisor $\mathcal{D}$ and a set of basis elements, defined over k, of the associated linear system. It follows that G may be identified with a quasi-projective variety in $\mathbf{P}_N$ whose defining equations are homogeneous polynomials in the corresponding variables $X_0, \ldots, X_N$ with coefficients in k. Then we have the usual logarithmic absolute Weil height h on $\mathbf{P}_N(K)$, defined as follows. For P in $\mathbf{P}_N(K)$ let $\xi_0, \ldots, \xi_N$ be projective coordinates in K of P, and put

$$h(P) = h(\xi_0, \ldots, \xi_N) = D^{-1} \sum_v \log \max(|\xi_0|_v, \ldots, |\xi_N|_v).$$

Here D is the degree of K and the sum is extended over all valuations v of K, normalized to extend the standard valuations on $\mathbf{Q}$ and to satisfy the sum formula $\sum_v \log |\xi|_v = 0$ for all non-zero ξ in K.

This function therefore induces a height on $G(K)$, which we also denote by h. Our estimates for the $|m|$ in (1) will involve an upper bound for $h(P_1), \ldots, h(P_n)$.

The plan of this article is as follows. In section 2 we prove a general result about generators of certain groups. This section could be omitted on a first reading. In sections 3, 4, 5 and 6 we discuss various special algebraic groups, namely $G = \mathbf{G}_a$ the additive group, $G = \mathbf{G}_m$ the multiplicative group, $G = E$ an elliptic curve, and $G = A$ an abelian variety of arbitrary dimension. For the last three of these we obtain quite precise estimates for the solutions of (1); however, the first is somewhat anomalous and we do not consider it in as much detail. Then in section 7 we show how to put all these results together to treat a general commutative algebraic group.

2. Geometry of numbers

Here we prove a proposition about bases of certain groups. This type of result has already appeared several times in the literature (see

for example [11] pp. 93, 96, 98 and [12] pp. 127, 203, 206), but we give a more general treatment. We say that a real-valued function f on $\mathbf{Z}^n$ is a convex distance function if it satisfies the following conditions:

(a) $f(m) \geq 0$ for all m in $\mathbf{Z}^n$,

(b) $f(tm) = |t|f(m)$ for all m in $\mathbf{Z}^n$ and all t in $\mathbf{Z}$,

(c) $f(m_1 + m_2) \leq f(m_1) + f(m_2)$ for all m_1, m_2 in $\mathbf{Z}^n$.

For such a function it is plain that the set $\Gamma = \Gamma(f)$ of all m in $\mathbf{Z}^n$ with $f(m) = 0$ is an additive group.

Proposition. Let f be a convex distance function on $\mathbf{Z}^n$. Further let E be such that $f(m) \leq E$ for each of the standard basis elements m of $\mathbf{Z}^n$, and suppose there exists $\epsilon > 0$ such that $f(m) \geq \epsilon$ for all m in $\mathbf{Z}^n$ with $f(m) \neq 0$. Finally let Γ_0 be a subgroup of $\Gamma(f)$ of finite index ν. Then Γ_0 is generated by elements m of $\mathbf{Z}^n$ with

$$|m| \leq n^{n-1}\nu(E/\epsilon)^{n-1}.$$

More precisely, if Γ_0 has rank $r \geq 1$, it has basis elements $m_1, \ldots, m_r$ satisfying

$$|m_1| \ldots |m_r| \leq n^{n-1}\nu(E/\epsilon)^{n-r}.$$

Proof. We work in $\mathbf{R}^n$ with Lebesgue measure μ_n and its induced measures μ_r on subspaces of dimension r. It is easy to see that f has a (unique) continuous extension to $\mathbf{R}^n$, which satisfies

$$f(x) \leq nE|x| \tag{2}$$

for all x in $\mathbf{R}^n$. Also the kernel of V of f is the space spanned over $\mathbf{R}$ by Γ; its dimension is the rank r of Γ.

If $r = 0$ the Proposition is trivial. So henceforth we assume $1 \leq r \leq n$. Now Γ is a lattice in V; we are going to prove that its determinant $\Delta(\Gamma)$ satisfies

$$\Delta(\Gamma) \leq (nE/\epsilon)^{n-r}. \tag{3}$$

It will suffice to show that every convex symmetric set S in V with

$$\mu_r(S) > 2^r(nE/\epsilon)^{n-r} \tag{4}$$

contains a non-zero point of Γ; for then (3) follows on taking S as a fundamental region for Γ, slightly reduced in size.

Thus let S be convex symmetric satisfying (4). Pick $\delta > 0$ with

$$\delta^{-1} > nE/\epsilon \tag{5}$$

$$\mu_r(S) > 2^r(\delta^{-1})^{n-r}. \tag{6}$$

We thicken S in V to S_δ in $\mathbf{R}^n$ as follows. Let W be the space perpendicular to V, and let C_W be the section cut out by W of the cube C defined by $|x| \leq 1$. Define S_δ as the sum $S + \delta C_W$. By Vaaler's cube-slicing theorem [25] we have $\mu_{n-r}(C_W) \geq 2^{n-r}$, and so by orthogonality

$$\mu_n(S_\delta) = \mu_r(S)\mu_{n-r}(\delta C_W) \geq 2^{n-r}\delta^{n-r}\mu_r(S)$$

which by (6) exceeds 2^n. Clearly S_δ is convex symmetric, and so by Minkowski's First Theorem ([8] p. 71) it contains a non-zero point m in $\mathbf{Z}^n$. Now $m = x + \delta y$ for x in S, y in C_W; and using (2) we obtain

$$f(m) \leq f(x) + f(\delta y) = f(\delta y) \leq n\delta E$$

which by (5) is strictly less than ϵ. Consequently $f(m) = 0$. Therefore m is in Γ, so in V, and so also in S. As remarked above, this establishes (3).

Since Γ_0 has index ν in Γ, we deduce

$$\Delta(\Gamma_0) \leq \nu(nE/\epsilon)^{n-r}. \tag{7}$$

Let now $\lambda_1, \ldots, \lambda_r$ be the successive minima of Γ_0 with respect to the distance function on V induced by $|x|$. By Minkowski's Second Theorem ([8] p. 203) we have $\lambda_1 \ldots \lambda_r \leq 2^r\Delta(\Gamma_0)/v$, where v is the volume of the section of C cut by V. Again by cube-slicing $v \geq 2^r$; so by (7) we find that

$$\lambda_1 \ldots \lambda_r \leq \nu(nE/\epsilon)^{n-r}. \tag{8}$$

Let $m_1', \ldots, m_r'$ be linearly independent points of Γ_0 with $|m_i'| \leq \lambda_i$, $1 \leq i \leq r$. Then Lemma 8 (p. 135) of [8] provides us with basis elements $m_1, \ldots, m_r$ of Γ_0 satisfying

$$\begin{aligned} |m_i| &\leq \max\{|m_i'|, \tfrac{1}{2}(|m_1'| + \ldots + |m_i'|)\} \\ &\leq \max(1, \tfrac{1}{2}i)\lambda_i, \qquad 1 \leq i \leq r. \end{aligned}$$

We conclude using (8) that

$$|m_1| \ldots |m_r| \leq r!2^{-r+1}\nu(nE/\epsilon)^{n-r},$$

and since $r!2^{-r+1} \leq r^r 2^{-r+1} \leq r^{r-1} \leq n^{r-1}$ the inequality of the Proposition follows at once.

Later we shall use this for $f = \varphi^{1/2}$ where φ is a positive semidefinite quadratic form; the condition (c) above is just the Cauchy-Schwarz inequality. In this case the Proposition resembles Satz 1 (p.36) of a recent paper of Schlickewei [19], with his integrality hypothesis replaced by the hypothesis that either $\varphi \geq \epsilon^2$ or $\varphi = 0$. However, Schlickewei's result applies more significantly to forms that are not definite.

3. The additive group

We identify the complex points of $\mathbf{G}_a$ with the additive group of complex numbers, and we embed this as usual in $\mathbf{P}_1$ by taking x to $(1, x)$. So $\mathbf{G}_a$ is $\mathbf{P}_1$ minus the single point $(0, 1)$, and we can suppose $k = \mathbf{Q}$. The points $P_1, \ldots, P_n$ of $G(K)$ correspond to algebraic numbers $\alpha_1, \ldots, \alpha_n$ of K, and the relation (1) reads

$$m_1\alpha_1 + \ldots + m_n\alpha_n = 0. \tag{9}$$

It is not difficult to prove that the relation group of all $m = (m_1, \ldots, m_n)$ in $\mathbf{Z}^n$ satisfying (9) is generated by m with

$$|m| \leq \exp(Ch), \tag{10}$$

where h is an upper bound for the heights $h(1, \alpha_1), \ldots, h(1, \alpha_n)$, and C depends only on the degree D of K. We leave the proof to the reader; he could for example use Lemma 4 (p. 442) of [16] together with suitable trace arguments.

Now select

$$\alpha_1 = 1, \quad \alpha_2 = g, \ldots, \alpha_n = g^{n-1}$$

for a positive integer g. Then well-known properties of g-adic expansions show that every solution $m \neq 0$ of (9) must satisfy $|m| \geq g$. Since we can take $h \leq (n-1)\log g$, it follows that the exponential dependence on h in (10) is necessary. As we shall soon see, the additive group is anomalous in this respect.

4. The multiplicative group

We identify the complex points of $\mathbf{G}_m$ with the multiplicative group of non-zero complex numbers, and we embed this again in $\mathbf{P}_1$ as in section 3. Then $\mathbf{G}_m$ is identified with $\mathbf{P}_1$ minus the points $(0,1)$ and $(1,0)$. Now $P_1,\dots,P_n$ correspond to non-zero algebraic numbers $\alpha_1,\dots,\alpha_n$ of K, and the relation (1) becomes

$$\alpha_1^{m_1}\dots\alpha_n^{m_n}=1.$$

In this case, estimates for $|m|$ were first obtained by Baker [2], [3] using the theory of linear forms in logarithms. A more elementary method was found by Stark [23] and van der Poorten and Loxton [17]. It is convenient for our purposes to introduce the quantities

$$\eta=\eta(\mathbf{G}_m,K)=\inf h(P),$$

where the infimum is taken over all non-torsion points P of $\mathbf{G}_m(K)$, and

$$\omega=\omega(\mathbf{G}_m,K)$$

the cardinality of the torsion part of $\mathbf{G}_m(K)$.

Theorem $\mathbf{G}_m$. Suppose $P_1,\dots,P_n$ on $\mathbf{G}_m(K)$ have heights at most $h\geq\eta$. Then the relation group of $P_1,\dots,P_n$ is generated by m with

$$|m|\leq n^{n-1}\omega(h/\eta)^{n-1}.$$

Proof. Let f be the function on $\mathbf{Z}^n$ defined by

$$f(m)=h(m_1P_1+\dots+m_nP_n).$$

Since the height $h(1,\alpha)$ satisfies $h(1,\alpha)\geq 0$, $h(1,\alpha^t)=|t|h(1,\alpha)$ and $h(1,\alpha_1\alpha_2)\leq h(1,\alpha_1)+h(1,\alpha_2)$, we obtain a convex distance function. The set $\Gamma=\Gamma(f)$ then consists of all m such that $m_1P_1+\dots+m_nP_n$ is a torsion point of $\mathbf{G}_m(K)$. We apply the Proposition to the relation group Γ_0 of $P_1,\dots,P_n$. Clearly the index ν of Γ_0 in Γ is at most ω. And we can take $E=h$, $\epsilon=\eta$. The theorem follows immediately.

In particular we see that the dependence on h is not exponential, in contrast to the additive case $G=\mathbf{G}_a$. We may also see that the exponent $n-1$ of h is best possible, by choosing $n-1$ independent points $Q_1,\dots,Q_{n-1}$ on $\mathbf{G}_m(K)$ and taking

$$P_1=-gQ_1,\quad P_2=Q_1-gQ_2,\dots,P_{n-1}=Q_{n-2}-gQ_{n-1},\quad P_n=Q_{n-1};$$

compare [17] (p. 300).

It thus remains to estimate the quantities η, ω in terms of K. A simple way of doing this is as follows. Let B be the number of points in $\mathbf{P}_1(K)$ with height at most 1, say. By considering the multiples bP, $0 \leq b \leq B$, and noting that $h(bP) = bh(P)$, it is easy to see that

$$\eta \geq B^{-1}, \qquad \omega \leq B.$$

Actually these give a very poor dependence on the degree D of K (at least exponential); and many authors have tried to do better. A classical question of Lehmer amounts to asking if $\eta \geq c^{-1}D^{-1}$, where c (and all the c's of this section) is a positive absolute constant; and the celebrated result of Dobrowolski [10] asserts that

$$\eta \geq c^{-1}D^{-1}(\mathcal{L}/\log \mathcal{L})^{-3}, \tag{11}$$

where for convenience we have written

$$\mathcal{L} = \log(D+2).$$

This was proved by techniques associated with transcendence theory, which were first applied in such a context by Stewart [24].

The analogous estimate for ω is much more elementary. Since the torsion part of $\mathbf{G}_m(K)$ is cyclic, and the field of Nth roots of unity has degree equal to Euler's function $\varphi(N)$, which satisfies $\varphi(N) \geq c^{-1}N/\log\log N$, $N \geq 3$, we deduce

$$\omega \leq cD \log \mathcal{L}. \tag{12}$$

Substituting (11) and (12) into Theorem $\mathbf{G}_m$, we obtain something like Theorem 1 (p. 84) of [17]; but for all relations m, not just one. On the other hand, [17] distinguishes between the heights of $\alpha_1, \ldots, \alpha_n$, and we do not. For some interesting refinements, which amount to working on the tangent space of $\mathbf{G}_m^n$ rather than $\mathbf{G}_m^n$ itself, see Waldschmidt [26], Bijlsma [6], and Bijlsma and Cijsouw [7].

5. Elliptic curves

It is convenient to embed our elliptic curve E in $\mathbf{P}_2$ using the Weierstrass form

$$y^2z = 4x^3 - g_2xz^2 - g_3z^3$$

Thus the invariants g_2, g_3 lie in the number field k. In this case the analogue of Theorem $\mathbf{G}_m$ requires the Néron-Tate height q on $E(K)$ defined by

$$q(P) = \lim_{t\to\infty} 2^{-2t} h(2^t P).$$

We put

$$\eta = \eta(E, K) = \inf q(P),$$

where the infimum is taken over all non-torsion P in $E(K)$, and we write

$$\omega = \omega(E, K)$$

for the cardinality of the torsion group of $E(K)$.

Theorem E. Suppose $P_1, \ldots, P_n$ on $E(K)$ have Néron-Tate heights at most $q \geq \eta$. Then the relation group of $P_1, \ldots, P_n$ is generated by m with

$$|m| \leq n^{n-1} \omega (q/\eta)^{\frac{1}{2}(n-1)}.$$

Proof. Let f be the function on $\mathbf{Z}^n$ defined by

$$f(m) = \{q(m_1 P_1 + \ldots + m_n P_n)\}^{1/2}.$$

Since q is a positive definite quadratic form, we obtain a convex distance function. Again the set $\Gamma = \Gamma(f)$ consists of all m such that $m_1 P_1 + \ldots + m_n P_n$ is a torsion point of $E(K)$, and we take Γ_0 as the relation group of $P_1, \ldots, P_n$. We can choose this time $E = q^{1/2}$, $\epsilon = \eta^{1/2}$, and the theorem follows immediately.

Once again the dependence on heights is not exponential, and an example exactly as in the previous section shows that the exponent $\frac{1}{2}(n-1)$ of q cannot be improved, at least if the rank of $E(K)$ is no less than $n-1$.

To apply the result in practice we must first estimate q in terms of the Weil height h. But in fact it is well-known that their difference is bounded on $E(\bar{k})$; thus

$$\delta = \delta(E) = \sup |q(P) - h(P)| \tag{13}$$

is independent of K, where the supremum is taken over all P in $E(K)$. So if h is an upper bound for $h(P_1), \ldots, h(P_n)$ we can take

$$q = \max(\eta, h + \delta).$$

Also since $q(P) \leq \delta$ implies $h(P) \leq 2\delta$, the simple counting argument of section 4 gives

$$\eta \geq \delta B^{-2}, \qquad \omega \leq B, \tag{14}$$

where B is the number of points P in $\mathbf{P}_2(K)$. But as before this leads to an exponential dependence on the degree D of K, whereas one expects $\eta \geq C^{-1}D^{-1}$, where C (and all the C's of this section) is a positive constant depending only on E. The techniques of Dobrowolski were ingeniously adapted by Laurent [13] in the case of complex multiplication, and he obtained exactly the same bound

$$\eta \geq C^{-1}D^{-1}(\mathcal{L}/\log \mathcal{L})^{-3}. \tag{CM 1}$$

In this case, best possible bounds are known for the order of torsion and it is not difficult to show (compare [4] p. 23) that

$$\omega \leq CD(\log \mathcal{L})^{1/2}. \tag{CM 2}$$

When there is no hypothesis of complex multiplication, the method of Stewart has to be used. Thus it was proved in [1] that $\eta \geq C^{-1}D^{-10}\mathcal{L}^{-6}$; but I recently sharpened this to

$$\eta \geq C^{-1}D^{-3}\mathcal{L}^{-2} \tag{15}$$

using an idea of Paula Cohen [9]. By rather different techniques Silverman [20] obtained $\eta >> D^{-2}$ when K is an abelian extension. As regards the torsion, Paula Cohen showed that every point of $E(K)$ has order at most $CD\mathcal{L}$; but her argument can be adapted to yield even

$$\omega \leq CD\mathcal{L}. \tag{16}$$

When there is no complex multiplication it can be proved that $\omega \ll (D \log \mathcal{L})^{1/2}$ (compare (CM 2)); but the implied constant is not always effective. The proof is a straightforward deduction from Serre's deep description [18] of the Galois group of the complete division fields $k(E_n)$ of level n, using the fact that if a subgroup of $(\mathbf{Z}/n\mathbf{Z})^2$ has index ν, then its stabilizer in $GL_2(\mathbf{Z}/n\mathbf{Z})$ has cardinality at most ν^2.

In all of the above estimates the constants C depend on the elliptic curve E. In her thesis [9] Paula Cohen showed how this dependence could be made explicit. In fact nothing is lost by taking a rather crude measure of the size of E; ignoring moduli space subtleties, we define

$$s = s(E) = \max\bigl(1, h(1, g_2, g_3)\bigr).$$

Thus for example the work of Zimmer [27] implies that for (13) we have

$$\delta \leq cs, \tag{17}$$

where now c depends only on k; and this is essentially best possible (see [21] p. 209). Even so, using (17) to calculate B in (14) we obtain only exponential dependence on s. Once again transcendence methods greatly improve matters, and we find for (15) and (16) the inequalities

$$\eta \geq c^{-1}s^{-1}D^{-3}(s+\mathcal{L})^{-2} \tag{18}$$

$$\omega \leq cs^{1/2}D(s+\mathcal{L}), \tag{19}$$

again for c depending only on k (and in fact c depends only on the degree d of k).

Actually, for fixed D at any rate, these fall somewhat short of what is predicted. A conjecture of Lang [11] (p. 92) implies that η should be bounded below independently of E (and should even tend to infinity as the logarithm of the discriminant). Silverman has made important progress on these and related questions: see [20], and also [22] for a more general account. And it is generally believed that ω should be bounded above independently of E (as in Mazur's famous result for $k = \mathbf{Q}$).

6. Abelian varieties

Up to now we have been able to find simple canonical embeddings of our algebraic group in projective space. For an abelian variety A this is usually not possible, and all our constants must depend on the embedding, or equivalently, on the divisor $\mathcal{D}$ that gives rise to the embedding. We suppress this dependence in our notation $\eta = \eta(A,K), \omega = \omega(A,K)$; these are defined as in the previous section now with reference to $A(K)$ and the corresponding Néron-Tate height q.

Theorem A. Suppose $P_1,\ldots,P_n$ on $A(K)$ have Néron-Tate heights at most $q \geq \eta$. Then the relation group of $P_1,\ldots,P_n$ is generated by m with

$$|m| \leq n^{n-1}\omega(q/\eta)^{\frac{1}{2}(n-1)}.$$

Proof. Exactly as for Theorem E.

Most of the remarks made in section 5 apply more generally here; thus, provided the embedding corresponds to a symmetric divisor, the quantity

$$\delta = \delta(A) = \sup\big|q(P) - h(P)\big| \tag{20}$$

is independent of K, where the supremum is taken over all P in $A(K)$. And the inequalities (14) hold, provided B now counts the points P in $\mathbf{P}_N(K)$ with $h(P) \leq 2\delta$.

Let g be the dimension of A. This time one expects $\eta \geq C^{-1}D^{-1/g}$, where C depends only on A. But if $g > 1$ no-one so far has been able to adapt Dobrowolski's work. Recently, building on earlier work for myself [14] and Bertrand [4], I proved that

$$\eta \geq C^{-1}D^{-(2g+1)}\mathcal{L}^{-2g}$$

(which in the case of complex multiplication can be sharpened to $\eta \geq C^{-1}D^{-2}\mathcal{L}^{-1}$). I also proved that

$$\omega \leq CD^g\mathcal{L}^g;$$

probably equally far from the truth, which is now connected with deep results of Bogolomov and Serre (see the discussion and references in [4]).

There has been some start in calculating the dependence of these constants C on the abelian variety A, at least for fixed D. It is convenient to express this in terms of families as follows. We take a variety V, defined over k, and an abelian variety $A_{\mathbf{gen}}$ defined over the function field $k(V)$. We pick a symmetric very ample divisor $\mathcal{D}_{\mathbf{gen}}$ on $A_{\mathbf{gen}}$ also defined over $k(V)$, and also basis elements for the corresponding linear system again defined over $k(V)$. Throwing away a proper Zariski closed subset of V if necessary, we can suppose that for each v in $V(k)$ the corresponding specialization on V yields an abelian variety A_v and a symmetric very ample divisor $\mathcal{D}_v$ both defined over $k(v) = k$. We can now measure the size of A_v simply by the height $h_V(v)$ of v in some fixed projective embedding of V; thus

$$s = s(A_v) = \max\bigl(1, h_V(v)\bigr).$$

For example, we can get every elliptic curve in this way by taking V as affine space $\mathbf{A}^2$, with coordinates t_2, t_3, minus the discriminant locus defined by $t_2^3 = 27t_3^2$. Define $E_{\mathbf{gen}}$ already in $\mathbf{P}_2$ by

$$y^2z = 4x^3 - t_2xz^2 - t_3z^3$$

(so that $\mathcal{D}_{\mathbf{gen}}$ is three times the divisor defined by the origin). For v in $V(k)$ with coordinates g_2, g_3 the specialized curve E_v is just that of section 5, of course; hence with the obvious embedding of V in $\mathbf{P}_2$ the size $s(E_v)$ agrees with the size defined there.

In general Silverman and Tate [21] (p. 201) proved that for (20) we have

$$\delta \leq cs$$

for c depending only on k, and it was shown in [15] that

$$\eta \geq C^{-1}s^{-(2g+1)}$$
$$\omega \leq Cs^g,$$

this time for C depending only on D and k (we may have to throw away another closed subset of V). As in the case of elliptic curves, these are probably very far from the truth. See [22] for an interesting discussion and some partial results.

7. The general case

Let G be a commutative connected algebraic group defined over a number field k. We say that the "dependence problem" can be solved for G if, given any points $P_1, \ldots, P_n$ on $G(\bar{k})$ we can find the relation group of all m satisfying (1), in the sense, for example, of the estimates of the previous sections. We do not make this definition very precise, because of the anomalous nature of the additive group in section 4 (however, Bertrand in [5] has suggested an interesting way round this difficulty). At any rate we regard this problem as having been solved for $G = \mathbf{G}_a$, $\mathbf{G}_m$, E and more generally an abelian variety A.

To deduce its solution for arbitrary G, it is convenient to store the relation group as a "relation matrix" whose rows are basis elements of the relation group. Suppose first that we have an exact sequence

$$O \longrightarrow G' \longrightarrow G \longrightarrow G'' \longrightarrow O$$

of commutative connected algebraic groups G', G, G'' defined over k, such that the maps α from G' to G and π from G to G'' are defined over k. Assume we can solve the dependence problem for G' and G''. We solve it for G as follows. Take points $P_1, \ldots, P_n$ in $G(\bar{k})$; then the images $P_i'' = \pi(P_i)$, $1 \leq i \leq n$, are in $G''(\bar{k})$. If these are independent then so are $P_1, \ldots, P_n$; otherwise we can find a relation matrix M'' for $P_1'', \ldots, P_n''$ with rows $m_j'' = (m_{j1}'', \ldots, m_{jn}'')$, $1 \leq j \leq \ell$, for some $\ell \geq 1$. Then the points

$$Q_j = m_{j1}''P_1 + \ldots + m_{jn}''P_n, \qquad 1 \leq j \leq \ell$$

satisfy $\pi(Q_j) = O$; so that we can write $Q_j = \alpha(P_j')$ for P_j' in $G'(\overline{k})$, $1 \leq j \leq \ell$. If $P_1', \ldots, P_\ell'$ are independent then so are $P_1, \ldots, P_n$; otherwise we can find a relation matrix M' for $P_1', \ldots, P_\ell'$. Now it is easily seen that the product $M'M''$ is a relation matrix for the original points $P_1, \ldots, P_n$.

In particular, if we can solve the dependence problem for G' and G'', then we can solve it for $G' \times G''$. Since every commutative linear group is a product of $\mathbf{G}_a$'s and $\mathbf{G}_m$'s, this solves the dependence problem for every such linear group.

Finally every G occurs in an exact sequence

$$O \longrightarrow L \longrightarrow G \longrightarrow A \longrightarrow O$$

where L is linear and A is an abelian variety. It follows that the dependence problem can be solved for any commutative connected algebraic group.

References

[1] M. Anderson and D. W. Masser, Lower bounds for heights on elliptic curves, *Math. Z.* **174** (1980), 23–34.

[2] A. Baker, Linear forms in the logarithms of algebraic numbers IV, *Mathematika* **15** (1968), 204–216.

[3] A. Baker, A sharpening of the bounds for linear forms in logarithms III, *Acta Arith.* **27** (1975), 247–252.

[4] D. Bertrand, Galois orbits on abelian varieties and zero estimates, *Diophantine analysis* (eds. J. H. Loxton and A. J. van der Poorten), London Math. Soc. Lecture Notes 109, Cambridge 1986, pp. 21–35.

[5] D. Bertrand, Galois representations and transcendental numbers, *New Advances in Transcendence Theory* (ed. A. Baker), Cambridge Univ. Press, 1988, Chapter 3.

[6] A. Bijlsma, Simultaneous approximations in transcendental number theory, Math. Centre Tracts 94 (Mathematisch Centrum, Amsterdam 1978).

[7] A. Bijlsma and P. Cijsouw, Degree-free bounds for dependence relations, *J. Australian Math. Soc.* **31** (1981), 496–507.

[8] J. W. S. Cassels, *An introduction to the geometry of numbers,* Springer, Berlin Göttingen Heidelberg 1959.

[9] P. Cohen, Explicit calculation of some effective constants in transcendence proofs, Ph.D. Thesis, University of Nottingham 1985 (Chapter 3).

[10] E. Dobrowolski, On a question of Lehmer and the number of irreducible factors of a polynomial, *Acta Arith.* **34** (1979), 391–401.

[11] S. Lang, *Elliptic curves: Diophantine analysis,* Springer, Berlin Heidelberg New York 1978.

[12] S. Lang, *Fundamentals of Diophantine geometry,* Springer, Berlin Heidelberg New York 1983.

[13] M. Laurent, Minoration de la hauteur de Néron-Tate, *Progress in Math. 38,* Birkhäuser, Boston Basel Stuttgart 1983 (pp. 137–151).

[14] D. W. Masser, Small values of the quadratic part of the Néron-Tate height, *Compositio Math.* **53** (1984), 153–170.

[15] D. W. Masser, Small values of heights on families of abelian varieties, *Proceedings of the Bonn Conference* (ed. G. Wüstholz), Springer Lecture Notes (to appear).

[16] D. W. Masser and G. Wüstholz, Fields of large transcendence degree generated by values of elliptic functions, *Inventiones Math.* **72** (1983), 407–464.

[17] A. J. van der Poorten and J. H. Loxton, Multiplicative relations in number fields, *Bull. Australian Math. Soc.* **16** (1977), 83–98 and ibid. **17** (1977), 151–155; see also a similar title in *Acta Arith.* **42** (1983), 291–302.

[18] J-P. Serre, Propriétés galoisiennes des points d'ordre fini des courbes elliptiques, *Inventiones Math.* **15** (1972), 259–331.

[19] H. P. Schlickewei, Kleine Nullstellen homogener quadratischer Gleichungen, *Monats. Math.* **100** (1985), 35–45.

[20] J. H. Silverman, Lower bound for the canonical height on elliptic curves, *Duke Math. J.* **48** (1981), 633-648.

[21] J. H. Silverman, Heights and the specialization maps for families of abelian varieties, *J. reine angew. Math.* **342** (1983), 197–211.

[22] J. H. Silverman, A quantitative version of Siegel's Theorem: integral points on elliptic curves and Catalan curves, *J. reine angew. Math.* **378** (1987), 60–100.

[23] H. Stark, Further advances in the theory of linear forms in logarithms, *Diophantine approximation and its applications,* Academic Press, New York London 1973 (pp. 255-293).

[24] C. L. Stewart, Algebraic integers whose conjugates lie near the unit circle, *Bull. Soc. Math. France* **106** (1978), 169–176.

[25] J. Vaaler, A geometric inequality with applications to linear forms, *Pacific J. Math.* **83** (1979), 543–553.

[26] M. Waldschmidt, A lower bound for linear forms in logarithms, *Acta Arith.* **37** (1980), 257–283.

[27] H. G. Zimmer, On the difference of the Weil height and the Néron-Tate height, *Math. Z.* **147** (1976), 35–51.