SPECIALIZATIONS OF FINITELY GENERATED SUBGROUPS OF ABELIAN VARIETIES

D. W. MASSER

ABSTRACT. Given a generic Mordell-Weil group over a function field, we can specialize it down to a number field. It has been known for some time that the resulting homomorphism of groups is injective "infinitely often". We prove that this is in fact true "almost always", in a sense that is quantitatively nearly best possible.

1. INTRODUCTION

Let \( k \) be a global field, and let \( V \) be a variety defined over \( k \). Suppose \( A \) is an abelian variety defined over the function field \( k(V) \); we may think of this also as a family of abelian varieties parametrized by elements \( v \) of \( V \). Let \( \Gamma \) be a finitely generated subgroup of \( A(k(V)) \). Replacing \( V \) by a nonempty open subset if necessary, we can suppose that for all \( v \) in \( V(k) \) the corresponding specialization from \( k(V) \) to \( k(v) \) induces an abelian variety \( A_v \) defined over \( k(v) \) and a group homomorphism \( \sigma_v \) from \( \Gamma \) to \( A_v(k(v)) \). We say that \( v \) is exceptional if \( \sigma_v \) is not injective. The object of this paper is to prove that when \( k \) is a number field the exceptional points are scarce in a rather strong sense.

We shall measure the scarcity as follows. For \( v \) in \( V(\kbar) \) we have a relative degree \( d(v) = [k(v) : k] \). Assume henceforth that \( V \) is explicitly embedded in projective space. Then we also have a corresponding (logarithmic) Weil height \( h(v) \) relative to \( k \). For a finite subset \( S \) of \( V(\kbar) \) we write \( \omega(S) = \omega_v(S) \) for the least degree of any homogeneous polynomial, defined over \( \kbar \), that vanishes on \( S \) but not identically on \( V \). Clearly \( \omega \) is subadditive in the sense that

\[
\omega(S \cup S') \leq \omega(S) + \omega(S') \tag{1}
\]

for finite subsets \( S, S' \).

Let \( \mathcal{E} \) denote the set of exceptional points, and for \( d \geq 1 \), \( h \geq 1 \) let \( \mathcal{E}(d,h) \) be the set of all \( v \) in \( \mathcal{E} \) with \( d(v) \leq d \), \( h(v) \leq h \). From now on we assume that \( k \) is a number field; thus each \( \mathcal{E}(d,h) \) is a finite subset of \( V(\kbar) \).

Suppose \( A \) has dimension \( n \geq 1 \) and \( \Gamma \) has rank \( r \geq 0 \).
Main Theorem. For each $d \geq 1$ there exists $C$ depending only on $k$, $V$, $A$, $\Gamma$ and $d$, such that for any $h \geq 1$ we have

$$\omega(\mathcal{E}(d, h)) \leq Ch^\kappa,$$

where $\kappa = \max(0, (r + 2)(nr + r - 1))$.

For purposes of comparison we note that if $V(d, h)$ is the set of all points $v$ in $V(k)$ with $d(v) \leq d$, $h(v) \leq h$ then $\omega(V(d, h))$ usually increases exponentially with $h$, at least if $d$ is not too small. For example, in §4 we will prove the following result.

Scholium 1. Suppose $V$ has positive dimension, and let $\delta$ be the degree of $V$. Then there are constants $c > 0$, $h_0$, depending only on $k$ and $V$, such that for any $h \geq h_0$ we have

$$\omega(V(\delta, h)) \geq \exp(ch).$$

Thus, loosely speaking, we may say that the exceptional set $\mathcal{E}$ lies on a hypersurface of “logarithmically small degree”. So certainly $\sigma_v$ is injective for infinitely many $v$ in $V(k)$; and we even recover Néron’s result [Né] that if $V$ is affine space $A^m$ or projective space $P^m$, then the same is true for infinitely many $v$ in $V(k)$ itself. In particular, for these $v$ the rank of $A_v(k(v))$ is at least $r$. Such observations were used by Néron in [Né] to construct abelian varieties over number fields with Mordell-Weil groups of large rank.

Of course our Theorem actually implies that $\sigma_v$ is injective for “almost all” $v$ in a suitable sense. It follows that Néron’s constructions work for “almost all” choices of the parameters. We can illustrate this more clearly in terms of cardinalities, at least if $V = A^m$, by using the following simple result (to be proved in §4).

Scholium 2. Let $Z$ be a finite subset of $A$ with cardinality $|Z|$. Then for any finite subset $S$ of $A^m$ the cardinality of $S \cap Z^m$ satisfies

$$|S \cap Z^m| \leq \omega(S)|Z|^{m-1}.$$

We take $k = \mathbb{Q}$, and we let $g_2 = g_2(t)$, $g_3 = g_3(t)$ be elements of $k(V) = \mathbb{Q}(t) = \mathbb{Q}(t_1, \ldots, t_m)$ with $g_2^3 \neq 27g_3^2$. Denote by $E$ the Weierstrass elliptic curve with invariants $g_2$, $g_3$, and suppose the rank of $E(\mathbb{Q}(t))$ is $r$. For any rational integers $\tau_1, \ldots, \tau_m$ such that $g_2(\tau)$, $g_3(\tau)$ are defined at $\tau = (\tau_1, \ldots, \tau_m)$ and satisfy $g_2^3(\tau) \neq 27g_3^2(\tau)$, we have a specialized elliptic curve $E_{\tau}$ defined over $\mathbb{Q}$. Let $r_\tau$ be its rank. We find that for any $H \geq 2$ the set $S(H)$ of such $\tau$ with $r_\tau < r$ and

$$0 \leq \tau_1, \ldots, \tau_m \leq H$$

satisfies

$$\omega(S(H)) \leq C(\log H)^\kappa$$

where $\kappa = \max(0, (r + 2)(2r - 1))$ and $C$ depends only on $E$. Thus by Scholium 2 we see that the cardinality of $S(H)$ is $O(H^{m-1}(\log H)^\kappa)$ as $H \to \infty$. Since the number of $\tau$ satisfying (2) alone is at least $H^m$, we conclude that
specialization almost never, in a rather strong sense, reduces the Mordell-Weil rank.

Probably the best known concrete example is the following, also taken from [Né] (but watered down to give rank only 8). Select 8 generic points in \( \mathbb{A}^2 \) together with \((0, 0)\), and let \( E \) be the (unique) plane cubic through these 9 points. If we specify the group identity as \((0, 0)\), it is well known that \( E \) becomes an elliptic curve over \( k(V) \) with \( k = \mathbb{Q} \) and \( V = \mathbb{A}^{16} = (\mathbb{A}^2)^8 \) (in fact we can even choose \( g_2, g_3 \) in \( k(V) \) as above). And it is not hard to see (for example by moving one of the generic points along the curve) that the generic rank \( r \) is 8. Thus, with at most \( O(H^{15+\varepsilon}) \) exceptions as \( H \to \infty \), the elliptic curve through the integer points \((x_1, y_1), \ldots, (x_8, y_8), (0, 0)\) with \( 0 \leq x_1, y_1, \ldots, x_8, y_8 \leq H \) has rank at least 8 over \( \mathbb{Q} \).

Similar remarks apply to the explicit elliptic curves \( \Gamma(S, T, V) \) constructed by Nakata [Na]. These are defined over \( k(\mathbb{A}^3) = \mathbb{Q}(S, T, V) \), with points \( P_i(S, T, V) \) \((1 \leq i \leq 9)\) also defined over \( \mathbb{Q}(S, T, V) \). It is proved that there exists a modulus \( m \) \((= 20957209)\), together with residues \( s_0, t_0, v_0 \), such that for any integers \( s, t, v \) satisfying

\[
(3) \quad s \equiv s_0, \quad t \equiv t_0, \quad v \equiv v_0 \pmod{m}
\]

the specialized points \( P_i(s, t, v) \) \((1 \leq i \leq 9)\) are independent on the specialized curve \( \Gamma(s, t, v) \). Since the triples satisfying (3) do not lie on any fixed hypersurface, it follows easily that the generic curve \( \Gamma(S, T, V) \) has rank at least 9 over \( \mathbb{Q}(S, T, V) \). Our Main Theorem therefore implies that, with at most \( O(H^{2+\varepsilon}) \) exceptions as \( H \to \infty \), the elliptic curve \( \Gamma(s, t, v) \) has rank at least 9 over \( \mathbb{Q} \) for any integers \( s, t, v \) (not necessarily subject to (3)) with \( 0 \leq s, t, v \leq H \).

It is possible that the more elaborate examples of Néron [Né] for rank 10 and 11 can be treated in this way (see also the article [F] of Fried, especially Proposition 3.9 of p. 628 and the sentence at the top of p. 629; and a preprint [T] of Top).

Next we discuss to what extent the estimate of our Main Theorem can be improved. It is easy to find examples where the exceptional set \( \mathcal{E} \) is large but contained in a fixed hypersurface (so the exponent \( m - 1 \) is best possible in the cardinality estimate corresponding to (2)). But we can do much more by generalizing an example of Silverman as follows. Let \( A \) be any simple abelian variety of dimension \( n \) defined over a number field \( k \), and let \( l \) be the rank of \( A(k) \). If \( A \) is explicitly embedded in projective space, we can take \( V = A \) in the above, and so we can regard \( A \) as defined over its own function field \( k(A) \). Suppose also that the endomorphism rank of \( A \) is trivial. Then it is not hard to see that the rank \( r \) of \( \Gamma = A(k(A)) \) is \( l + 1 \).

For the exceptional set in this situation we will prove in §4 the following result.
Scholium 3. There are constants \( c > 0, h_0 \), depending only on \( k \) and \( A \), such that for any \( h \geq h_0 \) we have
\[
\omega(\mathcal{E}(1, h)) \geq ch^\lambda,
\]
where \( \lambda = \frac{1}{2}(r - 1)/n \).

Thus in general it appears that a positive power of \( h \) cannot be avoided. However, when \( A \) has no constant part (that is, when there is no nonzero abelian subvariety of \( A \) defined over \( k \)) some results of Silverman suggest that \( \omega(\mathcal{E}(d, h)) \) might be bounded independently of \( h \). In fact if \( V \) is a curve and \( A \) has no constant part, Silverman [S1, Theorem C, p. 208] proved that the set \( \mathcal{E} \) of all exceptional points over \( k \) is a set of bounded height in \( V \) (even for an arbitrary global field \( k \)). So in this case \( \omega(\mathcal{E}(d, h)) \) is indeed bounded independently of \( h \).

Finally let us remark that one may replace the abelian variety \( A \) in the Main Theorem by the multiplicative group \( \mathbb{G}_m \) and obtain analogous estimates. These are useful in recent work [PS] of van der Poorten and Schlickewei. The proofs are similar but easier; see §5 for a further discussion.

I am grateful to Joe Silverman for encouragement as well as much correspondence on these topics, including detailed comments on an earlier version of this paper; and also to Hans-Peter Schlickewei for indicating the above connexion with the multiplicative group. The work was supported in part by the National Science Foundation.

2. PRELIMINARIES

We shall need a Néron-Tate height on each of the specialized abelian varieties \( A_v \). To obtain these in a uniform manner, we first choose a very ample symmetric divisor \( D \), defined over \( k(V) \), on the generic abelian variety \( A \). Replacing \( V \) by a nonempty open subset if necessary, we can assume that for all \( v \) in \( V(k) \) this divisor specializes down to a very ample symmetric divisor \( D_v \), defined over \( k(v) \), on \( A_v \). Let \( q_v \) be the associated Néron-Tate height on \( A_v(k) \). This is positive definite on \( A_v(k) \) modulo torsion.

Define the quantity
\[
\mu_v = \inf q_v(Q),
\]
where \( Q \) runs over all nontorsion points of \( A_v(k(v)) \). Also define \( \tau_v \) as the cardinality of the torsion group of \( A_v(k(v)) \). For \( r \geq 1 \) and \( \mathbf{m} = (m_1, \ldots, m_r) \) in \( \mathbb{Z}^r \) write
\[
|\mathbf{m}| = \max(|m_1|, \ldots, |m_r|).
\]

Proposition 1. For \( q \geq \mu_v \) let \( Q_1, \ldots, Q_r \) be linearly dependent points of \( A_v(k(v)) \) with Néron-Tate heights at most \( q \). Then there exists \( \mathbf{m} \) in \( \mathbb{Z}^r \) with \( 0 < |\mathbf{m}| \leq r^{-1} \tau_v(q/\mu_v)^{(r-1)/2} \) such that
\[
m_1Q_1 + \cdots + m_rQ_r = 0.
\]

Proof. This follows immediately from Theorem A of [M2], with \( K = k(v) \).
To estimate $\mu_v$ and $\tau_v$ we appeal to the work of [M1]; again it may be necessary to replace $V$ by a nonempty open subset.

**Proposition 2.** For each $d \geq 1$ there exists $c > 0$, depending only on $k$, $V$, $A$, $D$ and $d$, such that for any $h \geq 1$ and any $v$ in $V(d, h)$ we have

$$\mu_v \geq (ch^{2n+1})^{-1}, \quad \tau_v \leq ch^n.$$  

*Proof.* This follows immediately from Corollaries 1 and 2 of [M1]; note that the constants $C_1$, $C_2$ therein depend only on the degree of $K = k(v)$.

To estimate $q$ we need to choose Weil heights uniformly on each $A_v$. For this we fix basis elements $\phi_0, \ldots, \phi_N$, defined over $k(V)$, of the linear system corresponding to the very ample divisor $D$ on $A$. Again replacing $V$ by a nonempty open subset, we may suppose that for all $v$ in $V(k)$ the specializations of $\phi_0, \ldots, \phi_N$ define a projective embedding of $A_v$ into $\mathbb{P}_N$. Let $h_v$ denote the associated Weil height on $A_v(k)$.

**Proposition 3.** For each $d \geq 1$ there exists $c$, depending only on $k$, $V$, $A$, $\phi_0, \ldots, \phi_N$ and $d$, such that for any $h \geq 1$, any $v$ in $V(d, h)$, and any $Q$ in $A_v(k)$ we have

$$|q_v(Q) - h_v(Q)| \leq ch.$$  

*Proof.* This is essentially Theorem A (p. 201) of [S1], due to Silverman and Tate.

### 3. Proof of the Main Theorem

We start by noting that our repeated removal of proper closed sets from $V$ has the effect of reducing the function $\omega$ by a bounded quantity. Thus no generality is lost in this procedure.

We may clearly assume that $\Gamma$ is nonzero. Our basic observation is that for each fixed nonzero $P$ in $\Gamma$ the set of $v$ in $V(k)$ for which $\sigma_v(P) = 0$ is contained in a proper closed subset of $V$. Thus if the rank $r$ of $\Gamma$ is zero this proves the Theorem at once, for we see that $\omega(E(d, h)) \leq C$ independently of $d$ and $h$. So henceforth we will suppose $r \geq 1$.

Let $P_1, \ldots, P_r$ be generators for the free part of $\Gamma$. For $m = (m_1, \ldots, m_r)$ in $\mathbb{Z}^r$ write $P_m = m_1P_1 + \cdots + m_rP_r$, and define $V_m$ as the set of all $v$ in $V(k)$ for which there exists a torsion point $P$ in $\Gamma$ such that

$$P_m + P \neq 0, \quad \sigma_v(P_m + P) = 0.$$  

Thus our exceptional set $E$ satisfies

$$E \subseteq \bigcup_m V_m.$$  

Each $V_m$ lies in a proper closed subset of $V$, and we start by estimating $\omega$ on $V_m$. Throughout this section, $c_1, c_2, \ldots$ will denote positive constants depending only on $k$, $V$, $A$, the basis elements $\phi_0, \ldots, \phi_N$ of §2, the generators $P_1, \ldots, P_r$, and (from Lemma 2 onwards) the positive integer $d$. 

License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use
**Lemma 1.** For any $m$ in $\mathbb{Z}$ and any finite subset $S$ of $V_m$ we have
\[ \omega(S) \leq c_1(|m|^2 + 1). \]

**Proof.** This is an easy deduction from the work of Altman [A]. We can find algebraically independent elements $t_1, \ldots, t_m$ of $k(V)$ and we can then write $k(V) = Q(t_1, \ldots, t_m, u)$ for $u$ integral of degree $q \geq 1$ over $\mathbb{Z}[t_1, \ldots, t_m]$. Now Theorem 3.5 (p. 159) of [A] shows that for any $m$ in $\mathbb{Z}$ and any torsion point $P$ in $A(k(V))$ the point $P_m + P$ has projective coordinates of the form
\[ \xi_j = \sum_{i=0}^{q-1} X_{ij}(t_1, \ldots, t_m)u^i \quad (0 \leq j \leq N), \]
where the $X_{ij}$ are polynomials in $\mathbb{Z}[t_1, \ldots, t_m]$ of total degrees at most $c_2(|m|^2 + 1)$ (we will not need bounds for their coefficients). Similarly the origin of $A(k(V))$ has projective coordinates of the form
\[ \alpha_j = \sum_{i=0}^{q-1} A_{ij}(t_1, \ldots, t_m)u^i \quad (0 \leq j \leq N) \]
for polynomials $A_{ij}$ in $\mathbb{Z}[t_1, \ldots, t_m]$ of degrees at most $c_3$.

Replacing $V$ by a nonempty open subset, we may suppose that the functions $t_1, \ldots, t_m, u$ are regular on $V$. Let $v$ be any point of $V_m$, so that (5) holds for some torsion $P$. Since $P_m + P \neq 0$, we can find $a, b$ with $0 \leq a, b \leq N$ such that $\delta = \xi_a \alpha_b - \xi_b \alpha_a$ is not zero in $k(V)$. In particular $\xi = \xi_e$ is nonzero for some $e$ (= $a$ or $b$), and $\alpha = \alpha_f$ is nonzero for some $f$ (= $a$ or $b$). Now we see that $\delta \xi \alpha$ must vanish at $v$. For if $\xi \alpha$ does not vanish at $v$, then the $\xi_j(v)$, $\alpha_j(v)$ ($0 \leq j \leq N$) must be projective coordinates of $\sigma_v(P_m + P) = 0$ and $\sigma_v(0) = 0$ respectively; thus $\delta$ vanishes at $v$. Hence all points of $V_m$ lie in the subsets, defined by $\delta \xi \alpha = 0$, which arise in such a way from the choices of $P$ and $a, b, e, f$. This leads easily to the required estimate for $\omega(S)$ when $S$ is any finite subset of $V_m$, and so completes the proof.

Next, it follows from (6) that each finite set $\mathcal{E}(d, h)$ is contained in a union of finitely many sets $V_m$.

**Lemma 2.** For any $d \geq 1$, $h \geq 1$ we have
\[ \mathcal{E}(d, h) \subseteq \bigcup_{|m| \leq M} V_m, \]
where $M \leq c_4 h^{n+r-1}$.

**Proof.** Let $v$ be an arbitrary element of $\mathcal{E}(d, h)$. If $v$ is in $V_0$ there is nothing to prove. Otherwise (6) shows that some linear combination, not identically zero, of $Q_1 = \sigma_v(P_1), \ldots, Q_r = \sigma_v(P_r)$ is a torsion point. Thus $Q_1, \ldots, Q_r$ are dependent. Therefore by Proposition 1 there is a relation (4) with $0 < |m| \leq r^{-1} \tau_v(q/\mu_v)^{(r-1)/2}$, where $q \geq \mu_v$ is an upper bound for the Néron-Tate heights of $Q_1, \ldots, Q_r$. Hence by Proposition 2 we have $0 < |m| \leq c_5 h^n(qh^{2n+1})^{(r-1)/2}$.
Also it is clear that the Weil heights $h_v(Q_1), \ldots, h_v(Q_r)$ do not exceed $c_6h$; and thus by Proposition 3 we can take $q \leq c_7h$. We conclude that $0 < \lvert m \rvert \leq c_8h^{nr+r-1}$. Since $m \neq 0$, we have $P_m \neq 0$; but $\sigma_v(P_m) = 0$ by (4), and therefore $v$ lies in $V_m$; which proves the lemma.

The Main Theorem follows immediately. From (1) and Lemma 2 we see that

$$\omega(\mathcal{E}(d,h)) \leq \sum_{\lvert m \rvert \leq M} \omega(S_m),$$

where $S_m = \mathcal{E}(d,h) \cap V_m$. And Lemma 1 gives $\omega(S_m) \leq c_9M^2$, whence

$$\omega(\mathcal{E}(d,h)) \leq c_{10}M^r \cdot M^2 \leq c_{11}h^{(r+2)(nr+r-1)}.$$

This completes the proof.

4. PROOF OF THE SCHOLIA

We shall need an auxiliary result on heights (also used in [M1]). Let $V$, $W$ be (quasiprojective) varieties, embedded in projective space and defined over our number field $k$. We write $h$ for the (logarithmic) height on both $V(k)$ and $W(k)$, and $d$ for the degree functions, all taken relative to $k$.

Heights Lemma. Let $f$ be a morphism from $V$ to $W$, defined over $k$. Then there is a constant $c$, depending only on $k$, $V$, $W$, and $f$, with the following property. Suppose $w$ in $W(k)$ is such that $f^{-1}(w)$ is a finite set of cardinality $p \geq 1$. Then $p \leq c$, and for any $v$ in $f^{-1}(w)$ we have

$$d(v) \leq pd(w), \quad h(v) \leq c(h(w) + 1).$$

Proof. I am grateful to Silverman for pointing out that this can be deduced from his work [S2], and also to Philippon for showing me another proof based on [P]. We give here a third proof relying on the methods of [MW2]. Here $c_1, c_2, \ldots$ depend only on $k$, $V$, $W$ and $f$.

To start with, it is clear by conjugation that $d(v) \leq pd(w)$. Next, writing $K = k(w)$ and introducing projective coordinates $X_0, \ldots, X_M$ for the space $P_M$ containing $V$, we see that the equations $f(v) = w$, together with the equations defining the Zariski closure $\bar{V}$, give rise to generators $P_1, \ldots, P_r$ of a homogeneous ideal in $K[X_0, \ldots, X_M]$ which has an isolated prime (maximal) component for each $v$ in $f^{-1}(w)$. It is classical that the number of such components can be bounded only in terms of the degrees of the generators (see for example [MW2, Theorem II, p. 419]). This shows that $p \leq c_1$.

It follows easily that we can find a linear form in $k[X_0, \ldots, X_M]$, with coefficients of heights at most $c_2$, which is nonzero at all points of $f^{-1}(w)$; and without loss of generality we can suppose that this linear form is $X_0$. Similarly, by considering the ideal of polynomials vanishing on $V - V$, we can find a homogeneous polynomial $Q_0$ in $k[X_0, \ldots, X_M]$, of degree at most $c_3$ and with coefficients of heights at most $c_3$, that vanishes on $V - V$ but not at any point of $f^{-1}(w)$.
Write also $Q_0, P_1, \ldots, P_r$ for the above polynomials evaluated at the affine coordinates $1, x_1 = X_1/X_0, \ldots, x_M = X_M/X_0$. Fix $x$ as one of these coordinates, and let $\xi_1, \ldots, \xi_p$ be the values of $x$ at the points of $f^{-1}_p(w)$. Then the Nullstellensatz applies to

$$Q = (x - \xi_1) \cdots (x - \xi_p)Q_0$$

and $P_1, \ldots, P_r$; and so by Theorem IV (p. 437) of [MW2] there exists a positive integer $e \leq c_4$ such that

$$Q^e = A_1' P_1 + \cdots + A_r' P_r$$

for polynomials $A_1', \ldots, A_r'$ in $K[x_1, \ldots, x_M]$ of degrees at most $c_5$. In particular, there are polynomials $A_0', A_1', \ldots, A_r'$ in $K[x_1, \ldots, x_M]$, of degrees at most $c_6$, such that

$$(7') \quad A_0'Q_0^e = A_1' P_1 + \cdots + A_r' P_r$$

with $A_0'$ in $K[x]$ of exact degree $ep \leq c_7$.

Now let $A_1', \ldots, A_r'$ be polynomials in $x_1, \ldots, x_M$ of degrees at most $c_6$, and let $A_0$ be a polynomial in $x$ of degree $ep$, all of whose coefficients are independent variables. The equation

$$A_0Q_0^e = A_1' P_1 + \cdots + A_r' P_r$$

is then equivalent to a system of homogeneous linear equations over $K$ in these coefficients. By $(7')$ this system has a solution over $K$ with one particular coefficient nonzero (that corresponding to the highest power in $A_0$). An explicit such solution over $K$ can now be written down using determinants, as in Lemma 4 (p. 442) of [MW2]. We find without difficulty that there are polynomials $A_0, A_1, \ldots, A_r$ in $K[x_1, \ldots, x_M]$, of degrees at most $c_6$, and with coefficients of height at most $c_9(h(w) + 1)$, such that

$$(7) \quad A_0Q_0^e = A_1 P_1 + \cdots + A_r P_r$$

with $A_0$ in $K[x]$ of exact degree $ep$; in particular $A_0 \neq 0$.

Now substituting the affine coordinates of each point of $f^{-1}(w)$ into $(7)$ shows that $\xi_1, \ldots, \xi_p$ must be zeroes of $A_0(x)$. It follows that $\xi_1, \ldots, \xi_p$ have heights at most $c_9(h(w) + 1)$. Finally on varying the particular affine coordinate chosen, we see that each $v$ in $f^{-1}(w)$ has height at most $c_10(h(w) + 1)$; and this completes the proof.

We proceed to prove Scholium 1. The constants now depend only on $k$ and $V$. Suppose $V$ has dimension $m \geq 1$ and is embedded in $P_M$, with projective coordinates $X_0, \ldots, X_M$. After making a linear transformation over $\bar{k}$, we can assume that the quotients $X_i/X_0, \ldots, X_M/X_0$ give a map $\pi$ from $V$ to $A^m$, defined over $\bar{k}$, that is generically surjective and of degree $\delta$. Replacing $V$ by a nonempty open subset, and choosing a suitable nonempty open subset $W$ of $A^m$, we may even suppose that $\pi$ is a morphism from $V$ to $W$ and that
\(\pi^{-1}(w)\) has cardinality at most \(\delta\) for each \(w\) in \(W\). We may further suppose that \(W = \mathbb{A}^m - X\) for some hypersurface \(X\) of \(\mathbb{A}^m\) defined over \(\bar{k}\). Also, by taking norms over the corresponding function fields, and clearing denominators, we can easily verify that

(8) \[ \omega(\pi(S)) \leq c_{11}(\omega(S) + 1) \]

for any finite set \(S\) in \(V\), where the \(\omega\) on the left is taken in \(\mathbb{A}^m\).

Choose now any \(h \geq 1\). For a positive number \(R\) shortly to be determined in terms of \(h\) let \(Z \subseteq A\) be the set of rational integers \(r\) with \(0 \leq r \leq R\). Thus for any \(w\) in \(Z^m \subseteq \mathbb{A}^m\) we have \(d(w) = 1\) and \(h(w) \leq [k : \mathbb{Q}]*\log R\). If further \(w\) is in \(W\) then \(w = \pi(v)\) for some \(v\) in \(V(\bar{k})\); and from the Heights Lemma we see that

\[ d(v) \leq \delta, \quad h(v) \leq c_{12}(\log R + 1). \]

So if \(R = \exp(c_{13}h)\) for sufficiently small \(c_{13}\), and \(h \geq 2c_{12}\), we conclude that \(h(v) \leq h\) and hence \(v\) lies in \(V(\delta,h)\). The set \(S\) of \(v\) arising in this way therefore satisfies

\[ S \subseteq V(\delta,h), \quad \pi(S) = Z^m \cap W. \]

Thus by (8)

(9) \[ \omega(V(\delta,h)) \geq \omega(S) \geq c_{14}\omega(\pi(S)) - 1 = c_{14}\omega(Z^m \cap W) - 1. \]

But by subadditivity (1)

\[ \omega(Z^m \cap W) \geq \omega(Z^m) - \omega(Z^m \cap X). \]

The second factor on the right is bounded independently of \(h\) by the degree of \(X\), and it is well known that the first factor on the right is just the cardinality \(|Z|\) of \(Z\). Since \(|Z| \geq R = \exp(c_{13}h)\), we obtain the estimate of Scholium 1 by putting all these together with (9).

Next we prove Scholium 2, using a minor variant of the proof of Lemma 3A (p. 147) of [Sch]. It suffices to show that, given any nonzero polynomial \(P(x_1, \ldots, x_m)\) of degree at most \(d\), the cardinality of the set \(T\) of \((z_1, \ldots, z_m)\) in \(Z^m\) with \(P(z_1, \ldots, z_m) = 0\) is at most \(d|Z|^{m-1}\). We do this by induction on \(m\), the case \(m = 1\) being trivial.

So assume the above statement holds with \(m\) replaced by \(m - 1 \geq 1\), and write

\[ P(x_1, \ldots, x_m) = \sum_{i=0}^{e} P_i(x_1, \ldots, x_{m-1})x_m^{e-i} \]

for some \(e \leq d\) and polynomials \(P_0, \ldots, P_e\), with nonzero \(P_0\) of degree at most \(d - e\). Split \(T\) into disjoint sets \(T_0, T_1\) according as to whether \(P_0(z_1, \ldots, z_{m-1})\) is zero or not. On \(T_0\) each \((z_1, \ldots, z_{m-1})\) determines at most \(|Z|\) values of \(z_m\), so the induction hypothesis gives

\[ |T_0| \leq (d - e)|Z|^{m-2} \cdot |Z|. \]
On $T_i$ each $(z_1, \ldots, z_{m-1})$ determines at most $e$ values of $z_m$, so

$$|T_i| \leq e|Z|^{m-1}.$$ 

Therefore

$$|T| = |T_0| + |T_1| \leq d|Z|^{m-1}$$

as required. This completes the proof.

Finally we prove Scholium 3. Here constants depend only on $k$ and $A$. Now the rank $r$ of $A(k(A))$ is $l + 1$ because of the extra generic point. So if this point is specialized to any $v$ in $A(k)$ the map $\sigma_v$ will fail to be injective. Hence $A(k) \subseteq \mathcal{E}$. Fix generators $Q_1, \ldots, Q_t$ of $A(k)$.

Choose any $h \geq 1$. For a positive number $R$ shortly to be determined in terms of $h$ let $S$ be the set of elements of the form $v = r_1Q_1 + \cdots + r_tQ_t$ for rational integers $r_1, \ldots, r_t$ with $0 \leq r_1, \ldots, r_t \leq R$. For any such $v$ we have $h(v) \leq c_{13}(R^2 + 1)$. Thus if $R = c_{16}h^{1/2}$ for sufficiently small $c_{16}$, and $h \geq 2c_{15}$, we conclude that $h(v) \leq h$, and therefore $v$ lies in $\mathcal{E}(1, h)$. So $S \subseteq \mathcal{E}(1, h)$ and

$$\omega(\mathcal{E}(1, h)) \geq \omega(S).$$

Now the Main Theorem of [MW1, p. 490] gives the lower bound $\omega(S) \geq c_{17}R^\mu$ where $\mu$ is the usual generalized Dirichlet exponent. But since $A$ is simple we find easily that $\mu = l/n$ (see for example [MW1, p. 510]). Hence

$$\omega(\mathcal{E}(1, h)) \geq c_{18}h^{(r-1)/2n}$$

as desired.

5. The multiplicative group

Again let $V$ be a variety defined over a number field $k$. Let $\Gamma$ be a finitely generated subgroup of $G_m(k(V))$ of rank $r$. As before we can suppose that for all $v$ in $V(k)$ there is a specialization map $\sigma_v$ from $\Gamma$ to $G_m(k(v))$, and we say that $v$ is exceptional if $\sigma_v$ is not injective. For $d \geq 1$, $h \geq 1$ denote by $\mathcal{E}(d, h)$ the corresponding finite subset of the exceptional set $\mathcal{E}$. Then we can prove the following analogue of the Main Theorem of §1.

**Theorem.** For each $d \geq 1$ there exists $C$, depending only on $k$, $V$, $\Gamma$ and $d$, such that for any $h \geq 1$ we have

$$\omega(\mathcal{E}(d, h)) \leq Ch^\kappa,$$

where $\kappa = \max(0, r^2 - 1)$.

We do not give the proof in detail; the method of §3 carries over, provided we have the appropriate versions of Propositions 1 and 2 in §2. In order to state these we first embed $G_m$ into $P_1$ in the standard way. This gives us a logarithmic Weil height on $G_m(k)$, which for uniformity we will also denote by $q$. For $v$ in $V(k)$ define

$$\mu_v = \inf q(Q).$$
where \( Q \) runs over all nontorsion points of \( \mathbb{G}_m(k(v)) \). Also define \( \tau_v \) as the cardinality of the torsion group of \( \mathbb{G}_m(k(v)) \). Then we can state the following multiplicative analogue of Proposition 1.

(I) For \( q \geq \mu_v \), let \( Q_1, \ldots, Q_r \) be linearly dependent points of \( \mathbb{G}_m(k(v)) \) with heights at most \( q \). Then there exists \( m \) in \( \mathbb{Z}^r \) with

\[
0 < |m| \leq r^{r-1} \tau_v(q/\mu_v)^{r-1}
\]

such that \( m_1Q_1 + \cdots + m_rQ_r = 0 \).

This is an immediate deduction from Theorem \( \mathbb{G}_m \) of [M2], with \( K = k(v) \).

We can also state the following multiplicative analogue of Proposition 2.

(II) For each \( d \geq 1 \) there exists \( c > 0 \), depending only on \( k \) and \( d \), such that for any \( h \geq 1 \) and any \( v \) in \( V(d, h) \) we have \( \mu_v \geq c^{-1} \), \( \tau_v \leq c \).

This follows from the classical observations (see for example §4 of [M2]) that if \( K \) is a number field, there is a positive constant \( c \), depending only on the degree of \( K \) over \( \mathbb{Q} \), such that every element of \( K \) which is not a root of unity has logarithmic height at least \( c^{-1} \); and such that the cardinality of the group of roots of unity of \( K \) is at most \( c \).

We could also mention that the analogue of Lemma 1 of §3 now takes the form \( \omega(S) \leq c(|m| + 1) \); and the estimate for Lemma 2 becomes \( M \leq ch^{r-1} \) (for \( r \geq 1 \)). The proof of the Theorem may now be safely left to the reader.

Taking into account Scholium 1, we deduce that \( \sigma_v \) is injective for infinitely many \( v \) in \( V(k) \); or, less precisely, that if given algebraic functions over \( k \) are multiplicatively independent, then so are their values at infinitely many points over \( k \). Strangely enough, this result does not seem to have been stated explicitly before. It was needed to complete an argument in [PS].

Again the positive power of \( h \) really is needed in the Theorem, although in this case there is a very simple example. We take \( k = \mathbb{Q} \) and \( V = \mathbb{A} \), with \( k(V) = \mathbb{Q}(t) \). Identifying \( \mathbb{G}_m(k(V)) \) with the multiplicative group of \( \mathbb{Q}(t) \), we see that the functions

\[
 t, p_1t, \ldots, p_{r-1}t
\]

are independent provided \( p_1, \ldots, p_{r-1} \) are multiplicatively independent in \( \mathbb{Q} \). But for integers \( e_1, \ldots, e_{r-1} \) and \( t = p_1^{e_1} \cdots p_{r-1}^{e_{r-1}} \) the values \( 10 \) become dependent. It follows easily that for any \( h \geq 1 \) we have in this example \( \omega(\mathcal{E}(1, h)) \geq ch^{r-1} \) with some \( c > 0 \) independent of \( h \).

References


DEPARTMENT OF MATHEMATICS, UNIVERSITY OF MICHIGAN, ANN ARBOR, MICHIGAN 48109-1003