BULLETIN DE LA S. M. F.

M.L. BROWN

Endomorphisms of group schemes and rational points on curves

Bulletin de la S. M. F., tome 115 (1987), p. 1-17

<http://www.numdam.org/item?id=BSMF_1987__115__1_0>

Bull. Soc. math. France,
115, 1987, p. 1-17.

ENDOMORPHISMS OF GROUP SCHEMES AND RATIONAL POINTS ON CURVES

BY

M. L. BROWN (*)

RÉSUMÉ. — Nous considérons les points rationels sur les revêtements ramifiés abéliens des courbes. Une technique essentielle est l'étude de hauteurs de Weil sur les schémas en groupes commutatifs.

ABSTRACT. — We consider the rational points on abelian ramified covers on curves. A basic technique for this is a study of the behaviour of Weil heights on commutative group schemes.

1. Introduction

Let k be a number field or a function field over a finite field; let G/k be a smooth commutative group scheme. The object of this paper is to study the k-rational points on curves lying (as closed subschemes) in G/k and their inverse images under endomorphisms of G.

One knows from SERRE [7] that all abelian galois covers of curves are given by isogenies of their generalised jacobians. We consider here those abelian covers produced by isogenies of one group scheme to itself which generate a ring R of endomorphisms isomorphic to an order in a number field. The arithmetic of R enters into one of the main results (Theorems 3.6, 3.7) of this paper, that the inverse image r^*C of the curve C by the isogeny $r \in R$ has "trivial" k-rational points for almost all

(*) Texte reçu le 3 décembre 1985, revisé le 3 mai 1986

M. L. BROWN, Department of Mathematics, North, Park Road, Exeter, EX4 4QE (England).

BULLETIN DE LA SOCIÉTÉ MATHÉMATIQUE DE FRANCE - 0037-9484/1987/01 17/$3.70

r (under suitable conditions); this result is obtained by a simple sieving argument extending that of HEATH-BROWN [4]. One consequence of this (Example 1, §3) is that over any finitely generated extension k of the rationals $\mathbb{Q}$ Fermat's Last Theorem is true for "almost all" exponents (for $k=\mathbb{Q}$, this is due to HEATH-BROWN [4]). Naturally, we assume Mordell's conjecture for number fields (Faltings Theorem) and for function fields (Manin-Grauert-Samuel theorem).

Our results on rational points depend on estimates for the behaviour of the Weil height on commutative group schemes. We derive fairly precise estimates for this in paragraph 2, thus improving the quadratic upper bound of SERRE [6]; in fact, it is the lower bound that is essential for our application to rational points. We end this paper with some Diophantine equation examples.

It is a pleasure to thank the referee for his numerous suggestions and corrections to this paper and his generosity for suggesting further results leading from this work.

2. Heights on commutative group schemes

Throughout this section k will be a number field or a function field over a finite field k_0, with its usual proper set of normalised absolute values M_k, with its usual proper set of normalised absolute values M_k satisfying the product formula. For any point $x\in\mathbb{P}^n_k(k)$, we take $h(x)$ to be the logarithmic Weil height,

$$h(x)=\sum_{v\in M_k}\sup_i -v(x_i),$$

with respect to some choice of coordinates $x_0,\ldots,x_n$. If $\varphi: V\to\mathbb{P}^n_k$ is a morphism of k-schemes, we define $h_\varphi(x)$, for $x\in V(k)$, to be $h(\varphi(x))$.

Suppose that G k is a connected commutative group scheme of finite type. The object of this section is to determine how the height $h_\varphi(x)$, $x\in G(k)$, behaves with respect to the group law on G. For abelian varieties, a definitive answer to this was given by Néron [5]. In the general case, Serre showed that $h_\varphi(x)$ is at most a quadratic function of x, as x varies over a finitely generated subgroup of $G(k)$. Our main result (Theorem 2.6) gives sharp upper and lower bounds to h.

We derive these estimates by first examining the behaviour of the height on the additive and multiplicative group schemes $\mathbb{G}_a$ and $\mathbb{G}_m$ and then appealing to the structure theory of commutative group schemes which asserts that (many) such are extensions of abelian varieties by products of $\mathbb{G}_a$'s and $\mathbb{G}_m$'s; nevertheless, we have to assume in positive characteristic p that the unipotent part of G has period p, in order to construct a suitable compactification.

We first define some relations between real-valued functions f, g defined on a set S. Write $f \sim g$ if $f(s)-g(s)$ is a bounded function of $s \in S$. Write $f \ll g$ if there are constants $c_1 > 0$, c_2 such that $f(s) \leqslant c_1 g(s) + c_2$, for all $s \in S$ (note: this is slightly different from the number theorist's Vinogradov notation). Write $f \gg \ll g$ if we have both $f \gg g$ and $f \ll g$.

The next result is a particular case of a well-known theorem of Néron.

THEOREM 2.1 (Néron). — *Let A/k be an abelian variety with a projective embedding $\varphi: A \to \mathbb{P}^n_k$. Then there is a positive definite quadratic function p on $A(k)$ (i.e. $p = q + l$, q a quadratic form and l a linear function on the group $A(k)/A(k)_{tors}$) so that $h_\varphi \sim p$.*

We next state some well known general properties of Weil heights.

LEMMA 2.2. — *(a) Let,*

$$\varphi: \quad V \to \mathbb{P}^n_k, \qquad \psi: \quad V \to \mathbb{P}^m_k,$$

be morphisms of the k-scheme V to projective spaces. Suppose that φ is an immersion. Then $h_\psi \ll h_\varphi$. In particular, if both φ and ψ are immersions then $h_\varphi \gg \ll h_\psi$.

(b) Let $f: V \to W$ be a finite morphism of projective k-schemes, with closed immersions φ, ψ of V, W, respectively, into projective spaces. Then $h_\psi \circ f \gg \ll h_\varphi$.

The next result determines the behaviour of the height on a torus.

LEMMA 2.3. — *Let G/k be a torus with a projective embedding $\varphi: G \to \mathbb{P}^n_k$. Let i be the natural map from the abelian group $G(k)$ to the vector space $V = G(k) \otimes_{\mathbb{Z}} \mathbb{R}$. Then there is a norm $\| \ \|$ on V so that $h_\varphi(x) \gg \ll \| i(x) \|$, $x \in G(k)$.*

Proof. — As a torus is isotrivial, that is becomes isomorphic to $(\mathbb{G}_m)^r$ over some finite extension field k' of k, and as the (normalised) height is invariant under such a base change, we may assume that

$G \cong (\mathbb{G}_m)^s$. Further, by lemma 2.2 we may choose any projective embedding that is convenient in place of φ: therefore we embed $\mathbb{G}_m$ in $\mathbb{P}^1$, so that the point $x \in k^* = \mathbb{G}_m(k)$ is identified with the point $(1:x)$ on the projective line, and then φ is induced by this and the Segre embedding of $(\mathbb{P}^1)^s$. The Weil height on the latter is then the sum of the Weil heights on the component $\mathbb{P}^1$'s; we may therefore reduce to the case $G = \mathbb{G}_m$ with the specified projective embedding.

We then have,

$$h_\varphi(xy) = \sum_{v \in M_k} \max(-v(xy), 0) \leqslant h_\varphi(x) + h_\varphi(y),$$

for all $x, y \in k^*$. Further, $h_\varphi(a^t) = |t| h_\varphi(a)$ for any integer t. Finally, $h_\varphi(a) = 0$ if and only if a is a torsion point of $G(k)$, that is to say if and only if a is in the kernel of i. It therefore follows that h_φ extends to a norm on $\mathbb{G}_m(k) \otimes_{\mathbb{Z}} \mathbb{R}$, and we are finished.

We now estimate the height on a *unipotent* group scheme.

LEMMA 2.4. — *Let G/k be a unipotent commutative group scheme with projective embedding $\varphi: G \to \mathbb{P}^n_k$. Let Γ be a finitely generated subgroup of $G(k)$. Then, if k is a number field, there is a norm $\| \ \|$ on the real vector space $\Gamma \otimes_{\mathbb{Z}} \mathbb{R}$, with $i: \Gamma \to \Gamma \otimes_{\mathbb{Z}} \mathbb{R}$ the natural map, so that $h_\varphi(\gamma) \gg \ll \log \| i(\gamma) \|$, $\gamma \in \Gamma$, ($\log 0 = 0$). If k is a function field, then h_φ is bounded on Γ.*

Proof. — Suppose first that $\operatorname{char} k = p > 0$. Then G has a composition series with factors isomorphic to $\mathbb{G}_a$; it follows that $p^r G = 0$ for some $r > 0$, and therefore Γ is a finite group, whence h_φ is bounded; this completes the proof for a function field over a finite field.

Suppose now that k is a number field. Then G is isomorphic to $(\mathbb{G}_a)^s$, for some $s > 0$. Embed $(\mathbb{G}_a)^s$ in $\mathbb{P}^s_k$ so that the point $(x_1, \ldots, x_s) \in k^s$ corresponds to the point $(1 : x_1 : \ldots : x_s)$. Denote this embedding by φ; then by lemma 2.2 it is enough to evaluate the height given by this choice of projective embedding.

Let $\gamma_1, \ldots, \gamma_n$ be a basis for Γ over $\mathbb{Z}$; let γ_i have components $(\gamma_i)_j = \gamma_{ij}$. If v is non-archimedean, then we have,

$$v\left(\sum_i m_i \gamma_{ij}\right) \geqslant \min_i (v(m_i) + v(\gamma_{ij})) \geqslant \min_{i,j} v(\gamma_{ij}). \tag{2.1}$$

It follows from (2.1) that the non-archimedean valuations contribute little towards $h_\varphi(\gamma)$: that is to say, there is a constant C, depending on Γ, so

that,

$$(2.2) \qquad |h_\varphi(\gamma)-\textstyle\sum_{v,\,\mathrm{arch}} \max(0,\ \log|(\gamma)_j|;\ j=1,\ \ldots,\ s)|<C,$$

for all $\gamma\in\Gamma$.

Let k_v be the completion of k with respect to v. Condider the embedding,

$$\psi:\quad k^s\to(\textstyle\prod_{v,\,\mathrm{arch}} k_v)^s=K(\text{say}),$$

where $k_v=\mathbb{R}$ or $\mathbb{C}$ and where the product is taken over all the archimedean valuations of k. Now K is a vector space of dimension $s[k:\mathbb{Q}]$ over $\mathbb{R}$ and contains $\psi(\Gamma)$ as a discrete lattice.

The elementary inequality,

$$\max_j(|\Sigma_i a_{ij}|_v,\ 1)\leqslant\textstyle\sum_i \max_j(|a_{ij}|_v,\ 1),$$

implies,

$$(2=3) \quad \textstyle\prod_{v,\,\mathrm{arch}} \max_j(|\sum_i a_{ij}|_v,\ 1)$$
$$\leqslant\textstyle\prod_{v,\,\mathrm{arch}}(\sum_i \max_j(|a_{ij}|_v,\ 1))$$
$$\leqslant[\textstyle\sum_i\prod_{v,\,\mathrm{arch}} \max(|a_{ij}|_v,\ 1)]^{[k:\mathbb{Q}]}$$

Therefore, taking logarithms in (2.3), we have from (2.2),

$$(2.4) \qquad h_\varphi(\textstyle\sum m_i\gamma_i)\leqslant c_1+[k:\mathbb{Q}](c_2+\log(\sum|m_i|)),$$

for some constants c_1, c_2, and where $\log 0=0$. This gives our expected upper bound to h_φ.

We now derive a lower bound to h_φ. As $\psi(\Gamma)$ is a discrete lattice in K, it follows that for each archimedean valuation v on k there is a constant $d_v>0$ with the following property. For each $\gamma=\sum m_i\gamma_i\in\Gamma$, there is an archimedean valuation v and an integer j with,

$$|(\gamma)_j|_v\geqslant d_v\textstyle\sum|m_i|.$$

It follows that,

$$(2.5) \qquad \textstyle\prod_{v,\,\mathrm{arch}} \max_j(|\sum_i m_i\gamma_{ij}|,\ 1)\geqslant(\min_v d_v)\Sigma|m_i|,$$

for some constants c_1, $c_2>0$. The lemma follows from this and (2.4).

Remark. – The proof of this lemma shows that if k is a function field over an *arbitrary* field k_0, including characteristic zero, then h_φ is bounded on any finitely generated subgroup of $G(k)$.

We now consider the behaviour of the height on a commutative group scheme G/k of finite type. We shall need a slight generalization of SERRE's compactification [6] of commutative group schemes to the case of characteristic $p>0$. Unfortunately we shall have to impose a restriction on our group schemes in this case [*see* (★) below].

Suppose then that G/K is a smooth connected commutative group scheme, where k is any field.

Then G is an extension of an abelian variety A/k by a linear algebraic group L/k. Further, L contains a torus group T/k so that the quotient group scheme L/T is unipotent. We shall assume that, for characteristic $p>0$,

(★) $\qquad$ G/K has unipotent part of period $p=\text{char } k$,

that is to say, L/T is isomorphic to $(\mathbf{G}_a)^s$ for some $s\geqslant 0$ ([7], Ch. VII, Prop. 11]. Indeed, one then has the unique decomposition $L=T\times_k U$ in any characteristic, assuming (★) ([2], Exposé XVII, Th. 6.1.1.A) (ii)]. In characteristic zero, any commutative unipotent group is a product on $\mathbf{G}_a$'s; but in non-zero characteristic this is false, as group schemes of truncated Witt vectors show ([7], Ch. VII, §7, Cor. §§10-12].

Suppose now that k is algebraically closed and G/k satisfies (★), in the case of positive characteristic. Then one may construct a compactification $\bar{G}$ of G exactly as in [6]; we shall sketch this for the convenience of the reader. The linear algebraic subgroup L of G is now a direct product of copies of $\mathbf{G}_m$ and $\mathbf{G}_a$; say $L=\prod L_i$. Then we may embed each L_i in $\mathbf{P}^1$ so that the multiplication on L_i extends to a group action of L_i on $\mathbf{P}^1$: $L_i\times\mathbf{P}^1\to\mathbf{P}^1$. Take $\bar{L}$ as the product of these $\mathbf{P}^1$'s, then the multiplication on L extends to an action of L on $\bar{L}$: $L\times\bar{L}\to\bar{L}$. Now take $\bar{G}=G\times^L\bar{L}$, then we have an induced action of the group scheme G on $\bar{G}$ via $G\times\bar{G}$ via $G\times\bar{G}\to\bar{G}$. This $\bar{G}$ is our required smooth compactification of G.

Plainly, $G^\infty=\bar{G}-G$ is a positive divisor on $\bar{G}$. Suppose now that D is a positive divisor on $A=G/L$ and $\tilde{D}=p^*D$ is its pull back to G via $p:\bar{G}\to A$. As in [6] (Prop. 1 and Cor.) we now have,

LEMMA 2.5. — *Suppose that D is ample. Then there are integers $a \geqslant 1$, $b \geqslant 1$, so that $D_{a,b} = a\tilde{D} + bG^{\infty}$ is ample on $\bar{G}$.*

The next result is our main height estimate; we once again assume that k is a number field or a function field over a finite field.

PROPOSITION 2.6. — *Let G/k be a smooth commutative connected group scheme, satisfying (★) in the case of positive characteristic. Let Γ be a finitely generated subgroup of $G(k)$ and φ a projective embedding of G. Then there is a decomposition, $\Gamma/\Gamma_{tors} = \Gamma_1 \oplus \Gamma_2 \oplus \Gamma_3$ and positive definite quadratic forms q_i on Γ_i, $i = 1, 2, 3$, (Γ_3 and q_3 are zero if k is a function field) so that,*

$$h_{\varphi}|_{\Gamma} \gg \ll q_1 + \sqrt{q_2} + \log q_3 \qquad (\log 0 = 0).$$

Proof. — As the normalised height is invariant under finite base change, we may base change from k to the algebraic closure $\bar{k}$. By lemma 2.1, we may choose any convenient projective embedding to compute the height, so we take φ to be given by $D_{a,b}$ for suitable a, b by lemma 2.5. Therefore,

$$h_{\varphi} \sim a h_{\tilde{D}} + b h_{G^{\infty}}. \tag{2.6}$$

Now, $h_{\tilde{D}} \sim h_D \, p$ where p is the projection from $\bar{G}$ to A and h_D is the height on A relative to the divisor D. After Néron (Th. 2.1), $h_D \gg \ll q$ where q is a positive definite quadratic form on $A(k)/A(k)_{tors}$. Let Γ_1 be the group $p(\Gamma)/p(\Gamma)_{tors}$ and let Γ' be the kernel of the map $\Gamma \to \Gamma_1$. Then we have the splitting $\Gamma \cong \Gamma_1 \oplus \Gamma'$. Therefore by (2.6) we have,

$$h_{\varphi}|_{\Gamma} \gg \ll q|_{\Gamma_1} (= q_1) + h_{G^{\infty}}|_{\Gamma}. \tag{2.7}$$

So it only remains to estimate $h_{G^{\infty}}$.

Let f be the automorphism $x \to x + x_0$ of G. The compactification $\bar{G}$ was constructed in such a way that this extends to an automorphism of $\bar{G}$ and that $f^* G^{\infty} = G^{\infty}$. It follows that $h_{G^{\infty}} \, f \sim h_{G^{\infty}}$. Using $\sqrt{q_1}$ as a norm on Γ_1, it follows that for $\gamma_1 \in \Gamma_1$, $\gamma' \in \Gamma'$, we have the estimate,

$$-\sqrt{q_1}(\gamma_1) + h_{G^{\infty}}(\gamma') \ll h_{G^{\infty}}(\gamma_1 \oplus \gamma') \ll +\sqrt{q_1}(\gamma_1) + h_{G^{\infty}}(\gamma'), \tag{2.8}$$

for we may take a basis of Γ_1 and one by one remove elements from the component γ_1 using the "invariance" property of $h_{G^{\infty}}$ under

translation. Combining (2.7) and (2.8) we have

$$h_\phi|_{\Gamma'} \gg \ll q_1 + h_{G^\infty}|_{\Gamma'}. \tag{2.9}$$

Now, the group Γ' lies in a commutative group scheme which is a finite extension of the affine group scheme L. It follows that L' is an affine commutative group scheme, possibly disconnected. We now consider the cases of k being a number field or a function field separately.

Let k be a function field. Over the algebraic closure $\bar{k}$ of k, we have that $L' = T \times_{\bar{k}} U$ where T, U are multiplicative or unipotent group schemes, respectively. Let p_1, p_2: $L' \to T$, U be the projection morphisms. By the construction of G^∞, this divisor clearly induces very ample Cartier divisors on T, U; we again denote these by G^∞. Again we have (compare the proof of lemma 2.3),

$$h_{G^\infty}(x) = h_{G^\infty}(p_1(x)) + h_{G^\infty}(p_2(x)), \quad \text{for all } x \in L' = T \times U. \tag{2.10}$$

But, U is a torsion group in characteristic $p \neq 0$ so that the kernel of $p_1|_{\Gamma'}$ and the image of $p_2|_{\Gamma'}$ are finite groups. It follows from (2.10) and lemma 2.3 that there is a decomposition $\Gamma' \cong \Gamma_2 \oplus F$, where Γ_2 is torsion free and F is a torsion group, and a positive definite quadratic form q_2 on Γ_2 so that,

$$h_{G^\infty}|_{\Gamma'} \gg \ll \sqrt{q_2}.$$

The result now follows from (2.9).

Suppose now that k is a number field. There is an integer $m > 0$ so that $m\Gamma' \subset L$. The endomorphism $G \xrightarrow{m} G$ on G of multiplication by m extends to a *finite* morphism $\bar{G} \xrightarrow{m} \bar{G}$ by the construction of $\bar{G}$ (see, for example [6], Prop. 2), this is false in positive characteristic p as one sees by taking multiplication by p). By lemma 2.2 we have $h_{G^\infty} \circ m \gg \ll h_{G^\infty}$, where G^∞ now denotes the very ample Cartier divisor induced on L'. So it is enough to compute h_{G^∞} on $m\Gamma' \subseteq L$. Now, L is a product of a torus and a unipotent group; as the heights on these add to give the height on L, as in (2.10), the result follows from lemmas 2.3, 2.4 and (2.9).

COROLLARY 2.7. – *Suppose that G/k satisfies (★) in the function field case. Let U/k be the unipotent subgroup of G and $i: G \to G' = G/U$ the natural map. Then there is a norm $\| \ \|$ on $G'(k) \otimes_{\mathbf{Z}} \mathbf{R}$ and a constant c so*

that for all $x \in G(k)$,

$$h_\psi(x) \geqslant \| i(x) \| + c.$$

Proof. – If h_ψ denotes a height on G', for some projective embedding ψ of G', then by lemma 2.2, $h_\psi(i(x)) \ll h_\varphi(x)$. Now, G' is a group scheme of unipotent rank zero. As the estimates of lemma 2.3 and theorem 2.1 hold on all the k-rational points of the respective group schemes (instead of just finitely generated subgroups) we may use these in the proof of Proposition 2.6 (Γ_1 being finitely generated by Mordell-Weil) and the result, and more, follows.

It is a straighforward matter to extend the upper bound of Proposition 2.6 to function fields over number fields; for lemmas 2.3 and 2.4 easily extend to this case, and the generalization of Theorem 2.1 is known in this case. A sharp lower bound of the same kind can be shown now for affine group schemes, but the same lower bound for general commutative group schemes (as in Proposition 2.6) does not seem as simple to obtain.

3. Rational points on curves

Suppose that k is a number field or a function field over a finite field. By a curve C/k we mean a smooth geometrically irreducible 1-dimensional k-scheme (not necessarily projective). Let G/k be a smooth connected commutative group scheme and suppose that the curve C/k is a closed subscheme of G. Let R be a ring of endomorphisms of G/k which is isomorphic to an order in a number field. In this section, we shall study the k-rational points on the inverse images r^*C as r runs over the elements of R.

The group $G(k)$ inherits the structure of an R-module. As G is uniquely an extension of an abelian variety A/k by a linear algebraic group L/k, we also have that $A(k)$ and $L(k)$ have R-module structures. Now, L contains a unique torus T such that $U = L/T$ is a unipotent group scheme; again $T(k)$ and $U(k)$ inherit R-module structures (for generalitites on group schemes with R-actions see [1]).

After base changing by some purely inseparable extension k' of k, U becomes a subgroup of $L_{k'}$ so that $L_{k'} = T_{k'} \times U_{k'}$. It therefore makes

sense to define U' as the subgroup of $G(k)$ of points P for which $mP \in U_{k'}(k') \cap G(k)$ for some $0 \neq m \in \mathbb{Z}$; plainly, U' is independent of the choice of k'. As R is an order in a number field, we have that for each non-zero $r \in R$, there is $r' \in R$ so that rr' is a non-zero integer; the following lemma is therefore obvious.

LEMMA 3.1. — *The R-module $G(k)/U'$ is torsion free.*

As the units of R are k-automorphisms of G, they also induce k-automorphisms of L, T and U. Call 2 non-zero elements of R *equivalent* if their quotient is a unit of R. It follows that the number and distribution, relative to L, T, U, of rational points of r^*C depends only on the equivalence class of r. Put $\mathfrak{N}(r) = \sharp R/rR$.

PROPOSITION 3.2. — *If $Q \in G(k)$, $Q \notin U'$, then the set of principal ideals $\mathfrak{a} \subset R$ such that $Q \in \mathfrak{a} G(k)$ is finite. That is to say, $\varinjlim_{\text{principal}, \mathfrak{a} \subseteq R} \mathfrak{a} G(k) \subseteq U'$.*

Proof. — We may first extend the ground field, by a purely inseparable extension, so that U exists as a subgroup scheme of G. By considering the image of Q in G/U we may then reduce to the case when G_k has unipotent rank zero.

Take a projective embedding of G/k and let h be the associated Weil height on $G(k)$. Let G' be the torsion free R-module $G(k)/U'$ (lemma 3.1). Let M be the submodule of G' of those elements of the form sQ, for some $s \in \mathrm{fract}(R)$. Then $Q \to 1$ *identifies* M with an R-submodule of $\mathrm{fract}(R)$, also denoted by M. By Corollary 2.7 and as G has zero unipotent rank, there is a norm $\| \ \|$ on $M \otimes_{\mathbb{Z}} \mathbb{R}$ so that,

$$\|m\| \leqslant h(m) + c, \quad \text{for all } m \in M.$$

In particular, there are only finitely many $m \in M$ of given bounded norm, as the Weil height h has the same property. By considering a q-basis of $\mathrm{fract}(R)$ it now easily follows that M has a common denominator and so it is contained in λR for some $\lambda \in \mathrm{fract}(R)$. Therefore, if $Q \in M$, $Q \neq 0$, the set of ideals $\mathfrak{a} \subseteq R$ such that $Q \in \mathfrak{a} M$ is finite: for the ring $R(\lambda^{-1}Q)R$ is finite and so has only finitely many ideals.

We may apply this proposition to curves lying in G. If k is a function field over a field k_0, recall that the curve C/k is *isotrivial* if there is a finite extension K/k so that $C \otimes_k K$ is birationally isomorphic to $C' \otimes_{k_0} K$ where

C' is a curve defined over k_0. Suppose then that k is a number field (respectively, a function field over a finite field).

COROLLARY 3.3. — *Suppose that C/k is a smooth curve of genus $\geqslant 2$ (resp. and which is not isotrivial) in the group scheme G/k. Then,*

(1) *for all but finitely many equivalence classes of $r \in R$, the k-rational points of $r^* C$ are precisely $(r^*(C \cap U'))(k)$.*

(2) *if G has zero unipotent rank, then the k-rational points of $r^* C$ are torsion points of $G(k)$ for all but finitely many equivalence classes of $r \in R$.*

Proof. — Clearly, (1) implies (2). So to prove (1), by Faltings' theorem (respectively, Manin-Grauert-Samuel theorem) $C(k)$ is finite; thus $P \in (r^* C)(k)$ implies that rP lies in this finite set. The result follows immediately from Proposition 3.2.

Remarks. — (1) In characteristic zero, the restriction of an isogeny of G to U is necessarily an automorphism of U. Therefore, $r^* C$ in this case always contains the k-rational points $r^*(C(k) \cap U)$, if this is non-empty, and therefore always contains the points $(r^*(C \cap U'))(k)$.

(2) The corollary shows indirectly that if r is an isogeny, then the geometric components of $r^* C$ are not isotrivial. In fact, if $C' \to C$ is a finite morphism of curves of genus $\geqslant 2$ over the function field k/k_0, where k_0 is a finite field, then C is not isotrivial implies that C' is not isotrivial; one may see this either by considering the Kodaira-Spencer maps of C, C' ([8], Ch. 3, §0], or by using the analogue of the Mordell conjecture over function fields (C' is isotrivial if an only if $C'(K)$ is infinite for some finite extension field K/k).

We say that the closed subscheme X of the group scheme G/k has trivial k-rational points relative to G, if $X(k) \subseteq U'$. Corollary 3.3 then says, in particular, that $r^* C$ has trivial k-rational points for all but finitely many equivalence classes of $r \in R$, provided $g(C) \geqslant 2$.

For curves of genus $\leqslant 1$, one has a similar statement provided the covers are sufficiently ramified to take them above genus 2 (see theorem 3.6). In general one then only has a *density* result on the set of r for which $r^* C$ has trivial k-rational points. We now examine this case of curves of genus $\leqslant 1$.

LEMMA 3.4. — *Let r be an element of R which defines an isogeny on G. Then the degree* $\deg(r)$ *of this isogeny is divisible only by those primes*

dividing $\mathfrak{N}(r) = \sharp\, R/rR$. *In particular, if* $\operatorname{char} k \nmid \mathfrak{N}(r)$, *then* r *is a separable isogeny on* G.

Proof. – Let K be the Kernel of $G \xrightarrow{r} G$. Then K/k is a finite group scheme which is killed by $\mathfrak{N}(r)$. Now, $K = \operatorname{Spec} A$, where A is a finite k-algebra and where $\dim_k A = \deg r$.

There is an exact sequence of finite k-group schemes.

$$0 \to K^0 \to K \to K^{et} \to 0,$$

where K^0/k, K^{et}/k are connected and etale group schemes respectively. If K^0 is non-trivial, then k has positive characteristic p and K^0 has order p^μ, for some $\mu > 0$. Therefore, $\deg r = p^\mu \cdot \operatorname{order}(K^{et})$ and as $\mathfrak{N}(r)$ kills K^0 we must have that p divides $\mathfrak{N}(r)$([2], VII_A, 8.5]. To prove the lemma, it only remains to show that $m = \operatorname{order}(K^{et})$ is only divisible by primes dividing $\mathfrak{N}(r)$.

Now, $\mathfrak{N}(r)$ kills the étale group scheme K^{et}; base changing by the algebraic closure $\bar{k}$ of k, $K^{et} \otimes_k \bar{k}$ is a constant group scheme ([2], 1,4.1) given by a finite abelian group G of order m, and whose exponent divides $\mathfrak{N}(r)$: the result easily follows.

The next lemma delineates the possible separable ramified covers $r^* C$ of C.

LEMMA 3.5. – *Suppose that* $r^* C$ *is separable over* C [*in particular if* $\operatorname{char} k \nmid \mathfrak{N}(r)$] *and that* $r : G \to G$ *is an isogeny. Then the covering* $r : r^* C \to C$ *is principal with group* $\ker r$ *and so all geometric components of* $r^* C$ *have the same genus and same ramification over* C.

(1) *If* $g(C) = 1$, *then either the geometric components of* $r^* C$ *are elliptic curves isogenous to* C *or all have genus* $\geqslant 2$.

(2) *Suppose that* $\operatorname{char} k \nmid \mathfrak{N}(r)$ *and* $g(C) = 0$. *Then every geometric component of* $r^* C$ *is ramified over at least two points of* C; *further if* $r^* C$ *is ramified at exactly two points, then it is totally ramified and the geometric components of* $r^* C$ *have genus zero.*

(3) *If* $g(C) = 0$, *the geometric points of* $r^* C$ *are ramified over at least* 3 *points of* C, *and* $\mathfrak{N}(r)$ *is not divisible by* 2 *or* 3, *then the geometric components of* $r^* C$ *have genus* $\geqslant 2$.

Proof. — Let C' be a geometric component of r^*C. The Riemann-Hurwitz genus formula becomes, $d=\deg(r)$,

$$g(C')\geqslant g(C)+1-d+\frac{1}{2}\sum_P(d-m_P), \tag{3.1}$$

where the sum is over the branch points P of C and m_P are various integers dividing $d\,(e_P=d/m_P)$; further, we have equality in (3.1) if and only if the ramification is tame, in particular if $\operatorname{char} k \nmid \mathfrak{N}(r)$ after lemma 3.4. The latter remark now gives (2) easily from (3.1). The statement (1) is obvious.

(3) as $\mathfrak{N}(r)$ is not divisible by 2 or 3, neither is d by lemma 3.4. Therefore $m_P\leqslant d/5$ for each branch point P of C. The inequality (3.1) then becomes,

$$g(C')\geqslant 1-d+3/2\,(d-d/5)=1+d/5,$$

whence $g(C')\geqslant 2$ [in fact this argument shows that if r^*C is ramified over at least 5 points of C, then $g(C')\geqslant 2$ for any geometric component C' of r^*C whatever the value of $\mathfrak{N}(r)$].

Let $P(r)$ be a property of elements $r\in R$ which depends only on the equivalence class of r. We say that $P(r)$ *holds for almost all* $r\in R$ if,

$$\#\{\text{principal ideals } \mathfrak{a},\ \mathfrak{N}(\mathfrak{a})<x \text{ such that } P(\mathfrak{a})\}/M(x)\to 1, \text{ as } x\to\infty,$$

where $M(x)$ is the number of principal ideals $\mathfrak{a}$ of norm $\mathrm{N}(\mathfrak{a})<x$. We next have a simple sieving argument.

PROPOSITION 3.6. — *Let X be a subset of $G(k)$. Assume that $X\cap rG(k)$ is finite, except possibly for those r's lying in a finite number of proper ideals of R. Then for almost all $r\in R$, we have $X\cap rG(k)\subseteq U'(k)$.*

Proof. — Let $\mathfrak{a}_1,\ldots,\mathfrak{a}_s$ be the exceptional ideals, as in the Proposition. Let $\mathfrak{f}$ be the conductor of the order R in its integral closure. Let S be the set of principal prime ideals $\mathfrak{p}$ of R for which $\mathfrak{p}\nmid\mathfrak{f}$, $\mathfrak{a}_1,\ldots,\mathfrak{a}_s$. As S is obtained by deleting a finite set of primes from the set of all principal prime ideals of R, we have,

$$\sum_{\mathfrak{p}\in S}1/\mathfrak{N}(\mathfrak{p})=\infty,$$

by a theorem of Hecke (I thank Prof. R. Odoni for this observation). Therefore the product,

$$\prod_{\mathfrak{p}\in S}(1-1/\mathfrak{N}(\mathfrak{p})),$$

diverges to zero.

Select any $\varepsilon>0$ and choose a finite subset S' of S for which the product $\prod_{\mathfrak{p}\in S'}(1-1/\mathfrak{N}(\mathfrak{p}))<\varepsilon$. By Proposition 3.2, the set of principal ideals $\mathfrak{a}$, divisible by some $\mathfrak{p}$ in the finite set S', and for which $X\cap \mathfrak{a}\,G(k)\not\subseteq U'(k)$ has at most finitely many elements, say N'. Therefore,

$$\begin{aligned} N(x)&=\sharp\{\text{principal } \mathfrak{a}\subseteq R;\ \mathfrak{N}(\mathfrak{a})<x \text{ and } X\cap \mathfrak{a}\,G(k)\not\subseteq U'(k)\}\\ &\leqslant N'+\{\text{principal } \mathfrak{a};\ \mathfrak{N}(\mathfrak{a})<x \text{ and } \mathfrak{p}\not\mid\mathfrak{a} \text{ for all } \mathfrak{p}\in S'\}. \end{aligned}$$

Let μ be the Mobius function on the ideals of R (which behaves as one expects outside the primes in the conductor), let P be the product of all primes in S', and let $M(x)=cx+o(x)$ $(c>0)$ be the number of principal ideals of R of norm $<x$. Then we have from the above,

$$N(x)\leqslant N'+\sum_{\mathfrak{N}(\mathfrak{a})<x}\sum_{\mathfrak{b}\mid(P,\mathfrak{a})}\mu(\mathfrak{b}),$$

where the sums are over the principal ideals of the specified type; in fact the $\mathfrak{b}$'s still run over ideals prime to $\mathfrak{f}$. Therefore,

$$\begin{aligned} N(x)&\leqslant N'+\sum_{\mathfrak{b}\mid P}\mu(\mathfrak{b})\sum_{N(\mathfrak{a})<x,\,\mathfrak{b}\mid\mathfrak{a}}1\\ &\leqslant N'+\sum_{\mathfrak{b}\mid P}\mu(\mathfrak{b})\,M(x/\mathfrak{N}(\mathfrak{b}))\\ &\leqslant N'+c\,M(x)\sum_{\mathfrak{b}\mid P}\mu(\mathfrak{b})/\mathfrak{N}(\mathfrak{b})+o(x),\\ &\leqslant N'+c\,M(x)\prod_{\mathfrak{b}\mid P}(1-1/\mathfrak{N}(\mathfrak{p}))+o(x),\\ &\leqslant N'+c(\varepsilon+o(1))\,M(x). \end{aligned}$$

It follows that,

$$\limsup_{x\to\infty} N(x)/M(x)<\varepsilon c.$$

As $\varepsilon>0$ was arbitrary, we must have $\lim N(x)/M(x)=0$, as required.

We may now apply this proposition to the coverings r^*C of the curve C.

THEOREM 3.7. – *Suppose that k is a number field or a function field over a finite field. Suppose that the curve C/k is a closed subscheme of*

G/k and has genus 0 (resp. genus 1). Suppose also that for all $r \in R$, except possibly for those lying in a finite number of proper ideals of R, then $r: G \to G$ is a separable isogeny and the geometric components of $r^* C$ are ramified over at least 3 points of C (resp. ramified over C). Then $r^* C$ has trivial k-rational points, relative to G, for almost all $r \in R$.

Remark. — By lemma 3.4, $r: G \to G$ is a separable isogeny provided r does not lie in the finitely many prime ideals dividing char k, if this is non-zero.

Proof. — Let $\mathfrak{a}_1, \ldots, \mathfrak{a}_s$ be the exceptional ideals of the theorem; let $\mathfrak{a}_{s+1}, \ldots, \mathfrak{a}_t$ be the prime ideals dividing 2,3 or char k, if the latter is non-zero. Then by lemma 3.5(3) [resp. lemma 3.5(1)] and lemma 3.4, we have that for all $r \in R$, $r \notin \mathfrak{a}_i$ for all i, the geometric components of $r^* C$ are separable over C and have genus $\geqslant 2$. It follows from Faltings theorem, or the Manin-Grauert-Samuel theorem, that $r^* C(k)$ is finite, for such r. Therefore, $C(k) \cap rG(k)$ is finite for all $r \notin \mathfrak{a}_i$, $i = 1, \ldots, t$. The theorem now follows from Proposition 3.6 and lemma 3.1.

Examples. — (1) (Fermat curve over a number field). Let C be the line $X + Y = 1$ in the group scheme,

$$G = \mathbb{G}_m^2 = \operatorname{Spec} k[X^{\pm 1}, Y^{\pm 1}],$$

where k is a number field. Let R be the endomorphism ring $\mathbf{Z}$ on G. Then, $r^* C$, $t \in \mathbf{Z}$, is the Fermat curve,

$$X^r + Y^r = 1. \tag{3.2}$$

Theorem 3.6 now gives that for almost all integers $r > 0$, the only k-rational solutions have X, Y either being roots of unity in k or being zero (for $k = \mathbf{Q}$, this is due to HEATH-BROWN [4]).

In fact, if K is a function field over a number field k, then for almost all integers r, the equation (3.2) has only those K-rational solutions which are roots of unity in K or zero. For Mordell's conjecture is true in this case (by Faltings method, *see* [3], Chapter 6), and the remarks after Corollary 2.7 give suitable height estimates on G_K to prove an analogue of Theorem 3.6, which then says that for almost all r the K-rational solutions of (3.2) actually lie in k (k is algebraically closed in K); the previous paragraph now gives what we want.

(2) Let k be a function field over a finite field k_0, where k_0 is algebraically closed in k and of characteristic $p \neq 2,3$. Let C be the elliptic curve,

$$y^2 = x^3 + ax + b,$$

$a \in k_0$, $b \in k$ which is transcendental over k_0. Suppose that C/k is not isotrivial (this is always possible). Embed C in the group scheme $\mathbb{G}_m^2 = \mathrm{Spec}[X^{\pm 1}, Y^{\pm 1}]$ via $X \to x$, $Y \to y$ (omitting the points given by $xy = 0$). Then by theorem 3.6, taking $R = \mathbb{Z}$, the equation,

$$y^{2n} = x^{3n} + ax^n + b, \tag{3.3}$$

has only those k-rational solutions given by $x, y \in k_0$ or $xy = 0$. As b is transcendental over k_0 we cannot have both x and y in k_0. Further, the solutions given by $xy = 0$, involve taking $2n$'th or n'th roots of certain elements of k, and so only finitely many such n can have solutions of this kind in k. Thus we have that the equation (3.3) has no solutions in k for almost all n.

(3) (Generalised jacobians.) Let k be a number field and C/k a curve. Let $\mathfrak{m}$ be a *modulus* for C, with support S consisting of k-rational points, and let $\varphi : C \to J_{\mathfrak{m}}$ be the canonical map to the generalised jacobian [7], with respect to $\mathfrak{m}$. Suppose the hypotheses of Theorem 3.7 hold for C, $J_{\mathfrak{m}}$ and a ring of endomorphisms R of $J_{\mathfrak{m}}$.

The function, $f : R \to \mathbb{Z} \cup \{\infty\}$ given by,

$$f(r) = \#(^* C(k)),$$

is then *virtually periodic*: that is, there is a function $g : R \to \mathbb{Z}$ whose values depend only on the residue class of r modulo N for some integer N and so that $f(r) = g(r)$ for almost all r.

Furthermore, suppose that the field k is so large that maximal linear algebraic group L in $J_{\mathfrak{m}}$ splits completely: that is to say ([7], Ch. 5, § 3),

$$L \cong \mathbb{G}_m^{|S|-1} \times \mathbb{G}_a^{\deg \mathfrak{m} - |S|},$$

this can always be arranged by a finite extension of k. Then the maximum value of $g(r)$, and thus the maximum of $f(r)$ attained for a set of $r \in R$ of positive density, is,

$$g_{\max} = \#(C(k) \cap U') \times (\#\mu(k))^{|S|-1} \times \#J(k)_{\mathrm{tor}},$$

where $\mu(k)$ is the group of roots of unity of k and J is the ordinary jacobian of C/k.

Taking $U = \mathbb{G}_a^{\deg m - 1 - |S|}$, the above results are immediate consequences of Theorem 3.7 and the exact sequences,

$$0 \to \mathbb{G}_m^{\deg m - 1} \to J_m/U \to J \to 0$$
$$0 \to \mu(k)^{\deg m - 1} \to (J_m/U)_{\text{tor}} \to J_{\text{tor}} \to 0.$$

(4) With the same $C/k \to \mathbb{G}_m^2$ as in Example (1), where k is a number field, we now take R to be the order $\mathbb{Z}[\sqrt{n}]$, where n is non-square integer (not necessarily square free). Then R acts on $\mathbb{G}_m^2$ via the representation,

$$(a + b\sqrt{n}).(x, y) = \begin{bmatrix} a & b \\ bn & a \end{bmatrix} \times \begin{bmatrix} x \\ y \end{bmatrix} = (x^a y^b, x^{bn} y^a).$$

Therefore, $(a + b\sqrt{n})^* C$ is the curve,

$$x^a y^b + x^{bn} y^a = 1. \tag{3.3}$$

Then Theorem 3.7 gives that for almost all $(a, b) \in \mathbb{Z}^2$, the only k-rational solutions of (3.3) have x, y as roots of unity in k or $xy = 0$.

REFERENCES

[1] BERTRAND (D.). – Endomorphismes de groupes algébriques : applications arithmétiques, « Approximations diophantiennes et nombres transcendants », Luminy 1982, *Progress in Math.*, Vol. 31, 1983, pp. 1-45.

[2] DEMAZURE (M.) and GROTHENDIECK (A.). – Schémas en Groupes I, II, (SGA3), *Lecture Notes in Math.*, Nos. 151, 152, Verlag, New York, 1970.

[3] FALTINGS (G.) and WÜSTHOLZ (G.). – *Rational Points*, Vieweg, Braunschweig, 1984.

[4] HEATH-BROWN (D. R.). – Fermat's Last Theorem for "almost all" exponents, *Bull. London Math. Soc.*, Vol. 17, 1985, pp. 15-16.

[5] NERON (A.). – Quasi-fonctions et hauteurs sur les variétés abéliennes, *Annals of Math.*, Vol. 82, 1965, pp. 249-331.

[6] SERRE (J.-P.). – Quelques proprietes des groupes algébriques commutatifs, *Astérisque*, Vol. 69-70, 1979, pp. 191-202.

[7] SERRE (J.-P.). – *Groupes algébriques et corps de classes*, Hermann, Paris, 1959.

[8] SZPIRO (L.). – Seminaire sur les pinceaux de courbes de genre au moins de deux, *Astérisque*, Vol. 86, 1981.