PUBLICATIONS MATHÉMATIQUES DE L'I.H.É.S.

SERGE LANG

Integral points on curves

Publications mathématiques de l'I.H.É.S., tome 6 (1960), p. 27-43
<http://www.numdam.org/item?id=PMIHES_1960__6__27_0>

INTEGRAL POINTS ON CURVES

by Serge LANG (1)

Siegel has shown in [14] that an affine curve $f(x, y) = 0$ with coefficients in a number field and of genus $\geqq 1$ has only a finite number of points whose coordinates are integers of that field. Mahler [8] has conjectured that a similar statement holds for points having only a finite number of primes in their denominators, and proved this for curves of genus 1 over the rationals by his p-adic analogue of the Thue-Siegel theorem.

In view of Roth's recent result, and the progress which has been made in the theory of abelian varieties (especially the Jacobian) since Siegel and Mahler's papers appeared, it seemed worth while to reconsider the question, and I give below a modernized exposition of Siegel and Mahler's proof, which automatically carries with it a proof of Mahler's conjecture. The Jacobian is used in order to take a pull-back over the given curve of the standard covering given by $u \to mu + a$ where m is a large integer, and $a \in J$ is a suitable translation.

Aside from Roth's theorem (whose statement is reproduced in § 1) we use only the classical properties of heights and the weak Mordell-Weil theorem. This paper is thus a natural sequel of [7].

A proof of Mordell's conjecture [10] that a curve of genus $\geqq 2$ has only a finite number of *rational* points would of course supersede the Siegel-Mahler theorem for such curves, but I would conjecture that the latter holds in fact for abelian varieties : If A is an abelian variety defined over a number field K, if U is an open affine subset, and R a subring of K of finite type over $\mathbf{Z}$, then there is only a finite number of points of U in R. The difficulty in trying to extend the proof to abelian varieties lies in the fact that there is a whole divisor at infinity, whereas for curves, there is only a finite number of points, which are all algebraic.

It is easy to see that if the conjecture is true, then it remains true if K is replaced by a field of finite type over $\mathbf{Q}$, and R by a subring of finite type over $\mathbf{Z}$. In § 7 we shall carry this out for curves. This could be applied to strengthen in a like manner Siegel's result on curves of genus 0 as on p. 47 of [14]. There is no point in carrying this out here, but it is worth while to go deeper into one of Siegel's arguments.

We observe that if G is a group variety, and Γ a subgroup of finite type, then there is a field K of finite type over the prime field over which G is defined, and over which all points of Γ are rational.

Now the argument of Siegel can be used to prove the following theorem.

(1) Sloan Fellow.

Let K *be a field of characteristic* 0, *and* Γ *a subgroup of finite type of its multiplicative group. Then the curve* $ax+by=1$ *with* $a, b \in K$ *and* $ab \neq 0$ *has only a finite number of points with* $x, y \in \Gamma$.

PROOF. If there were infinitely many, let m be an integer $\geqq 3$. Then infinitely many x (resp. y) would lie in the same coset mod Γ^m, so that for such x and y we can write $x=a_1\xi^m$ and $y=a_2\eta^m$, and we get infinitely many points in $\Gamma \times \Gamma$ on the curve

$$aa_1\xi^m + ba_2\eta^m = 1$$

which has genus $\geqq 1$. Contradiction.

The straight line just considered should in fact be regarded as a subvariety of the product of the multiplicative group with itself. Recall that an *algebraic torus* (*torus* for short) is a group variety which is a finite product of multiplicative groups. Infinitely many rational points on the line give rise to integral points on a curve of genus $\geqq 1$, and using this same idea, we get more generally :

Let G *be a torus in characteristic* 0. *Let* C *be a subvariety of dimension* 1 *of* G. *Let* Γ *be a subgroup of finite type of* G. *If* C *intersects* Γ *in an infinite number of points, then* C *is the translation in* G *of a subtorus of dimension* 1.

PROOF. We can find a field K of finite type over $\mathbf{Q}$ over which G is written as an n-fold product of multiplicative groups, over which all points of Γ are rational, and over which C is defined. Let $(x_1, \ldots, x_n)$ be a generic point of C over K. Then C has genus 0, and we can write $x_i = \varphi_i(t)$ where φ_i is a rational function of a parameter t, defined over K. We proceed as above. Let us take m large and relatively prime to the orders of zeros and poles of the functions $\varphi_i(t)$. For suitable elements $a_1, \ldots, a_n \in K$, the curve whose generic point is $(\xi_1, \ldots, \xi_n)$ where $\xi_i^m = a_i x_i$ (over possibly a finite extension of K) must also have genus 0. Consider first a covering of the t-line given by the equation $\xi^m = a\varphi(t)$ with a, φ any one of the a_i, φ_i. We use the classical formula for the genus of a covering :

$$2g' - 2 = m(2g-2) + \Sigma(e_P - 1).$$

Then $\varphi(t)$ can have at most one zero and one pole. Indeed, the degree is m, and the ramification index above such a zero or pole is m also. We have $m(2g-2) = -2m$, and if there were at least 3 distinct zeros and poles, then the term $\Sigma(e_P - 1)$ would grow at least like $3(m-1)$, so we would get a covering of genus $\geqq 1$, having infinitely many points with coordinates in Γ, which is impossible.

After a linear transformation, we can write say for $i=1$,

$$x_1 = a_1 t^{r_1}$$

for some integer $r_1 \neq 0$. From the same argument, $x_i = a_i\varphi_i(t)$ where $\varphi_i(t)$ is a power of some linear transformation of t. In fact, $\varphi_i(t) = t^{r_i}$ because our covering has the intermediate covering defined by the equation

$$\xi^m = a_1 x_1 (a_i x_i)^{\pm 1} = a t^{r_1} \varphi_i(t)^{\pm 1}$$

which would be of genus $\geqq 1$ unless $\varphi_i(t)$ is of the prescribed type. We thus conclude that C is the translation of a subtorus.

As Siegel already observed, the coset argument is formally the same as the one used to carry out the proof that curves of genus $\geqq 1$ have only a finite number of integral points, but using the Jacobian instead of the torus (cf. below Proposition 1).

The analogy between toruses and abelian varieties was again observed by Chabauty, who in two papers [2], [3] considers infinite intersections of a subvariety of a torus or an abelian variety with particular subgroups of finite type, namely subgroups of units and groups of rational points in a number field respectively. Thus one is led to generalize and reformulate a conjecture of Chabauty [2] in the following manner, which includes the Mordell conjecture.

Let G *be torus (resp. an abelian variety) in characteristic* 0. *Let* V *be a subvariety of* G, *having an infinite intersection with a subgroup of finite type* Γ *of* G. *Then* V *contains a finite number of translations of group subvarieties of* G *which contain all but a finite number of points of* $V \cap \Gamma$.

This statement has been proved above when V is of dimension 1 and G is a torus. When G is an abelian variety and again V is of dimension 1, this is Mordell's conjecture. Of course, one may ask whether such a statement would not be valid also for a commutative group extension of an abelian variety by a torus.

Returning to the question of integral points, we shall see that our theorems have analogues in function fields K (finitely generated regular extensions) over arbitrary constant fields k of characteristic 0, and the finiteness statement can be given a relative formulation : One proves that certain points have bounded heights (Theorems 2, 3). In view of Theorem 3 [7], one sees that the conjecture we made above concerning integral points on affine subsets of abelian varieties can also be formulated relatively : If A is defined over k, if (B, τ) is a K/k-trace, then integral points of A_k lie in a finite number of cosets of τB_k.

In this connection, the Mordell conjecture becomes a conjecture in algebraic geometry, and it is worth while to make further comments on it here. Let k be as above, $K=k(t)$ a function field over k, where t is the generic point of a variety T, and let C be a curve of genus $\geqq 2$, defined over K. Then $C=C_t$ can be viewed as the generic member of an algebraic family. *The conjecture then asserts that if* C_t *has infinitely many rational points in* $k(t)$ *(cross sections of the parameter variety* T *in the graph of the family), then* C_t *is birationally equivalent over* $k(t)$ *to a curve* C_0 *defined over* k, *and all but a finite number of these points arise from points of* C_0 *in* k.

Evidence for this comes from the special case where $C_t=C_0$ is already defined over k, and then one obtains a classical theorem of de Franchis, to the effect that *given a variety* V *and a curve* C *of genus* $\geqq 2$ *(in characteristic* 0*) there exists only a finite number of generically surjective rational maps of* V *on* C. We give a quick proof of this theorem. Taking a generic hyperplane section U of V and inducing the rational map on it, one reduces the theorem to the case where V is itself a curve. Indeed, two distinct generically surjective rational maps f, f' : $V \to C$ induce distinct generically surjective maps on U, as one sees by taking the induced homomorphisms on the Albanese varieties, using Theorem 4 of [5], Chapter VIII, § 2.

Assuming now that V is a curve, we have the formula for the genus :

$$2.g(V)-2=d[2.g(C)-2]+\lambda$$

where $\lambda \geqq 0$. Thus the degree of V over C is bounded. Taking suitable projective embeddings, we see that the degree of the graph of our rational maps f must be bounded. Hence these graphs Γ_f lie on finitely many algebraic families on $V \times C$. On the other hand, a generic element of such families is likewise a generically surjective rational map of V onto C (as one sees by projecting on both factors). Taking the induced homomorphisms on the Jacobians, and using the fact that an abelian variety has no algebraic family of abelian subvarieties, we see that all induced maps coming from the same family differ by translations. We use now the fact that C is not equal to a non-zero translation of itself in its Jacobian. (If it were, so would the divisor Θ, and it isn't, even up to linear equivalence by Th. 3 of Ch. VI, § 3, [5].) We conclude that a graph Γ_f actually must constitute by itself a maximal algebraic family on $V \times C$, and thus finally that there is only a finite number of such graphs, or maps f. This concludes the proof. (When V is a curve, we do not need characteristic 0, only the assumption that the map $f : V \to C$ is separable, to be able to use the genus formula above.)

The Mordell conjecture thus gives rise to diophantine criteria for lowering fields of definition, and we can actually prove such a criterion in the context of integral points (Proposition 2).

One remark on notation to conclude this introduction : If O is a set of geometric objects, and K a field, we denote by O_K the subset of O consisting of those objects which are rational over K. For example, if V is a variety defined over K, then V_K denotes the set of its rational points in K.

§ 1. Diophantine approximations.

Let K be a number field (by definition, a finite extension of the rationals $\mathbf{Q}$) and let $N=[K:\mathbf{Q}]$ be its degree over $\mathbf{Q}$. For each prime $\mathfrak{p}$ of K (finite or archimedean) let $N_\mathfrak{p}=[K_\mathfrak{p}:\mathbf{Q}_p]$ be the local degree of the completions. If $\mathfrak{p}$ is archimedean, then $\mathbf{Q}_p=\mathbf{R}$ is the field of real numbers. Otherwise, it is the field of p-adic numbers where p is a prime number. We denote by $|\xi|_\mathfrak{p}$ the absolute value on K corresponding to the prime $\mathfrak{p}$, which induces on $\mathbf{Q}$ the usual absolute value if $\mathfrak{p}$ is archimedean, and otherwise the p-adic absolute value, so that $|p|_\mathfrak{p}=1/p$. We assume that this absolute value is extended to the algebraic closure $\overline{K}$ of K in some way. This amounts to embedding $\overline{K}$ in $\overline{\mathbf{Q}}_\mathfrak{p}$ and taking the absolute value induced by that of $\overline{\mathbf{Q}}_\mathfrak{p}$.

If β is an element of K, we can define its height

$$H_K(\beta)=\prod_\mathfrak{p} \sup(1, |\beta|_\mathfrak{p})^{N_\mathfrak{p}}$$

the product being taken over all primes of K. More generally, if P is a point in projective n-space, with coordinates $(\xi_0, \ldots, \xi_n)$ rational over K, then

$$H_K(P) = \prod_{\mathfrak{p}} \sup_i [|\xi_i|_{\mathfrak{p}}^{N\mathfrak{p}}].$$

The product formula [1] guarantees that this does not depend on the choice of coordinates. Thus $H_K(\beta)$ is the height of the point having $(1, \beta)$ as coordinates in $\mathbf{P}^1$, and if $\beta \neq 0$ we see that $H_K(\beta) = H_K(1/\beta)$. If $\beta = m/n$ is a rational number, with m, n relatively prime integers, then $H_{\mathbf{Q}}(\beta) = \sup(|m|, |n|)$.

If K is fixed, and the reference to a projective space is fixed throughout a discussion, then we write H instead of H_K.

We recall that one can define the absolute height

$$h(P) = H_K(P)^{1/[K:\mathbf{Q}]}$$

which is then independent of the field in which P is rational. Thus H_K is a function on points in projective space rational over K while h is a function on points in projective space rational over $\overline{K}$. Note that $h(P) \geqq 1$ and $H_K(P) \geqq 1$.

Two positive functions λ, λ' on a set of points are called *equivalent* (we write $\lambda \sim \lambda'$) if there exist two numbers $c_1, c_2 > 0$ such that

$$c_1\lambda \leqq \lambda' \leqq c_2\lambda.$$

It will also be convenient to define λ, λ' to be *quasi-equivalent* (we write $\lambda \approx \lambda'$) if given $\varepsilon > 0$, there exist two numbers $c_1, c_2 > 0$, depending on ε, such that for all points P in the set, we have

$$c_1\lambda(P)^{1-\varepsilon} \leqq \lambda'(P) \leqq c_2\lambda(P)^{1+\varepsilon}.$$

These relations are obviously equivalence relations (symmetric, reflexive, transitive).

On the set of elements $\alpha \in K$ such that $K = \mathbf{Q}(\alpha)$, our function H_K is equivalent to the height function used for instance by Roth, i.e. the maximum value of the coefficients in the irreducible equation satisfied by β over $\mathbf{Z}$, the integers. This is trivially verified. If E is a subfield of K, then on E we have $H_K = H_E^{[K:E]}$. From this one sees immediately that the set of elements of K of bounded height is finite (such elements can satisfy only a finite number of equations over $\mathbf{Z}$).

The Thue-Siegel-Mahler-Roth theorem (Roth's theorem for short) can be stated as follows. *Let α be algebraic over* K. *Let $\varkappa$ be a number > 2, and let* S *be a finite set of primes of* K. *Then the solutions β in* K *of the inequality*

$$\prod_{\mathfrak{p} \in S} \inf(1, |\alpha - \beta|_{\mathfrak{p}}) \leqq \frac{1}{H(\beta)^{\varkappa}}$$

have bounded height.

For a proof, see for instance [12], which follows Roth closely, includes the Mahler version, and obviously generalizes to number fields. Of course, the set of elements of K with bounded height is finite, but we have stated the theorem in the above form so as to have a uniform terminology with the function field case (characteristic 0). We discuss this below. The above statement can be slightly strengthened (as in Mahler) : If $\mathfrak{b}$ is the ideal which is the denominator in the ideal factorization of β in K, and if one defines $|\mathfrak{b}|_{\mathfrak{p}}$ for finite primes $\mathfrak{p}$ in the obvious manner, then one can replace $|\alpha-\beta|_{\mathfrak{p}}$ by $|\alpha-\beta|_{\mathfrak{p}}|\mathfrak{b}|_{\mathfrak{p}}$ in the above inequality, for the finite primes appearing in S.

Actually, for the sequel, we need only the approximation for one prime : *The solutions* β *in* K *of*

$$|\alpha-\beta|_{\mathfrak{p}} \leqq \frac{1}{H(\beta)^{\varkappa}}$$

have bounded height. In fact, we shall need it in the following context, as in Mahler [8].

Let $G(Y)$ *be a polynomial in* $\overline{K}[Y]$, *and assume that the multiplicity of its roots is at most* r *for some integer* $r>0$. *Say* G *has leading coefficient* 1, *so* $G(Y)=\prod(Y-\alpha_i)^{e_i}$. *Let* $c>0$ *be a number, and* $\mathfrak{p}$ *a prime of* K. *Then the solutions* β *in* K *of*

$$|G(\beta)|_{\mathfrak{p}} \leqq \frac{c}{H(\beta)^{\varkappa r}}$$

have bounded height if $\varkappa>2$.

It is a trivial matter to get this from the preceding statement. Indeed, our absolute value comes from an embedding of $\overline{K}$ in $\overline{K}_{\mathfrak{p}}$. If β stays away from all the α_i, our statement is clear. If β comes close to one of them, then its distance from the others is greater than some fixed lower bound. Thus in evaluating $|G(\beta)|_{\mathfrak{p}}$ precisely one term $|\alpha_i-\beta|_{\mathfrak{p}}^{e_i}$ becomes small, and we get

$$|\alpha_i-\beta|_{\mathfrak{p}}^{e_i} \leqq \frac{c'}{H(\beta)^{\varkappa r}}$$

for a suitable $c'>0$, and a sequence of β's such that $H(\beta)\to\infty$. Since $e_i\leqq r$, we can replace it by r, still preserving the inequality, and then take an r-th root. By making $\varkappa$ a little smaller, but still >2, one can omit the constant c', and thus reduce our statement to the previous one.

Note that if we put $G(Y)=Y-\alpha$, we recover Roth's theorem in its original form.

We now discuss the function field case. Let K be a function field (of arbitrary dimension) over a constant field k of characteristic 0. Let W be a projective model of K over k, non-singular in codimension 1. Let w be a generic point of W over k, so that we can write $K=k(w)$. As in [7] we use W to compute heights. If $\mathfrak{p}$ is a prime rational divisor of W over k, then $\deg(\mathfrak{p})$ denotes its projective degree. We then have the absolute value

$$|\xi|_{\mathfrak{p}}=\gamma^{\deg(\mathfrak{p})\operatorname{ord}_{\mathfrak{p}}\xi}$$

where $\operatorname{ord}_{\mathfrak{p}}\xi$ is the order at the discrete valuation determined by $\mathfrak{p}$, and γ is a fixed number, $0<\gamma<1$. Thus

$$H(\xi)=H_W(\xi)=(1/\gamma)^{d(\xi)}$$

where $d(\xi)=\deg(\xi)_\infty$ is the degree of the divisor of poles of ξ. More generally, if $(\xi_0, \ldots, \xi_n)$ is a point in $\mathbf{P}^n$ over K, then

$$H(P)=(1/\gamma)^{\deg \sup_i (\xi_i)_\infty}.$$

Thus in function fields, it is convenient to take the log to the base γ.

For each $\mathfrak{p}$ we suppose our absolute value extended to $\overline{K}$ in some fixed way. *Then the statement we gave above of Roth's theorem holds in the present situation.* This is seen as follows. First, one reduces the situation to the case where K is of dimension 1 over k, by taking generic hyperplane sections. Let L_u be a generic hyperplane over k, and $(w_1, \ldots, w_n)$ an affine generic point of W over k. Let $t=u_1w_1+\ldots+u_nw_n$ and let $k'=k(u_1, \ldots, u_n, t)$ (cf. [4], Ch. VIII, § 6). The generic hyperplane section $W'=W.L_u$ is defined over k', assuming that $\dim W \geqq 2$. If $\mathfrak{p}$ is a prime rational divisor of W over k, then $\mathfrak{p}'=\mathfrak{p}.L_u$ is a prime rational divisor of W' over k'. If $\xi \in K$ is a function on W, and ξ' the induced function on W', then $(\xi')_\infty=(\xi)_\infty.L_u$. Thus the height remains invariant by going over to generic hyperplane sections :

$$H_W(P)=H_{W'}(P)$$

if P is a point in $\mathbf{P}^n$ rational over K. (Geometrically speaking, the point P gives rise to a rational map of W into $\mathbf{P}^n$ and the induced rational map of W' into $\mathbf{P}^n$.)

The absolute value $|\ |_\mathfrak{p}$ described previously extends to the field $\overline{K}(u_1, \ldots, u_n)$ in such a way that it is trivial on $k(u_1, \ldots, u_n, t)$, and corresponds to the prime divisor $\mathfrak{p}'$. Consequently, we see that if we prove Roth's theorem for the field $K'=K(u_1, \ldots, u_n)$ viewed as function field over the constant field k', relative to the model W' (which is projective and non-singular in codimension 1) then it will follow for (K, k, W). This brings us to the function fields in one variable.

As for those, a prime $\mathfrak{p}$ is then a conjugate set of points over k. One sees immediately that we may go over to the algebraic closure of k, and then, in terms of orders, to prove the theorem in the following form :

Let K *be a function field of one variable over an algebraically closed constant field k of characteristic* 0. *Let* S *be a finite set of primes of* K *over k. Let α be algebraic over* K. *Then the degrees $\deg(\beta)_\infty$ of elements β in* K *satisfying the inequality*

$$\sum_{\mathfrak{p}\in S} \operatorname{ord}_\mathfrak{p}(\alpha-\beta) \geqq \varkappa \deg(\beta)_\infty \qquad (\varkappa > 2)$$

are bounded.

Actually, one gets a finiteness statement, because of the following remark : Let β_1, β_2 be solutions of the above inequality such that $d(\beta_1)=d(\beta_2)=d$ is >0. Then $\beta_1=\beta_2$. Indeed, we get

$$\operatorname{ord}_\mathfrak{p}(\beta_1-\beta_2) \geqq \varkappa d.$$

But $\deg(\beta_1-\beta_2)_\infty \leqq 2\,d$. If $\beta_1 \neq \beta_2$, then $\beta_1-\beta_2$ has more zeros than poles, which is impossible.

We observe that $d(\beta)=0$ if and only if β is constant, i.e. lies in k. (In terms of heights, this means $H(\beta)=1$.) Thus finally, we can state Roth's theorem in dimension 1 in the following form, say for one prime $\mathfrak{p}$:

Let α be algebraic over K. *There is only a finite number of elements* $\beta \in K$ *which are not constant (i.e. not in k) such that*

$$\operatorname{ord}_{\mathfrak{p}}(\alpha-\beta) \geqq \varkappa d(\beta)$$

if $\varkappa > 2$.

The proof of Roth's theorem for function fields in one variable is essentially the same as Roth's own proof. One must use the Riemann-Roch theorem precisely in the place where Roth does his counting to get his crucial polynomial. By the way, in number fields at this point, it is best to use the known estimates giving the number of algebraic integers in given parallelotopes (as in Artin-Whaples Theorem 4 [1]). For an exposition, cf. mimeographed notes to appear in the near future.

§ 2. A geometric formulation of Roth's theorem.

In this section we give a formulation of Roth's theorem which is adapted to the use we wish to make of it afterwards. We let K be a *global field* : This means a number field, or a function field over a constant field k which we assume of characteristic zero for this section. In the function field case, heights are taken with respect to a model as described in § 1.

THEOREM 1. *Let* W *be a complete non-singular curve defined over* K. *Let z, y be two non-constant functions in* $K(W)$, *and let r be the largest of the orders of the zeros of z. Assume that y has no zero or pole among the zeros of z, and that y gives an injective mapping of this set of zeros into* $\overline{K}$. *Let $\varkappa$ be a number* >2, *and* $c>0$. *Then the points* $Q \in W_K$ *such that*

$$|z(Q)|_{\mathfrak{p}} \leqq \frac{c}{H(y(Q))^{\varkappa r}}$$

have bounded height H_y.

PROOF. Without loss of generality, we may assume that $K(z,y)=K(W)$. If necessary, we may consider the complete non-singular curve which is a model of $K(z,y)$ instead of W. Our assumptions will still be valid for this curve. We may also assume that the values $|y(Q)|_{\mathfrak{p}}$ are bounded. Indeed, if there is an infinite sequence of points Q whose height $H_y(Q)=H(y(Q))$ tends to infinity, and satisfying the above inequality, but with $|y(Q)|_{\mathfrak{p}}$ unbounded, then we may consider $1/y$ instead of y, together with an infinite subsequence of such points Q. Let Φ be the set of zeros of z. Since y has no pole in Φ, it is integral over the local ring $\mathfrak{o}$ of the point $z=0$ in the function field $K(z)$. Let $F(Y)$ be its irreducible equation over $\mathfrak{o}$. Then

$$F(Y) \equiv G(Y) \pmod{z}$$

where $G(Y)$ is a polynomial with coefficients in K, leading coefficient 1, and mod z means modulo the maximal ideal of $\mathfrak{o}$ generated by z.

By hypothesis, y induces an injection $Q \to y(Q)$ of Φ into $\overline{K}$. The multiplicity of a root of $G(Y)$ is thus $\leqq$ the multiplicity of a point on W in the inverse image of $z=0$, this being the multiplicity of a zero of z. (One can see this formally for instance as follows: Let $(y^{(1)})$ be an affine generic point of W over K all of whose coordinates are integral over $\mathfrak{o}$. If $(y^{(1)}, \ldots, y^{(M)})$ is a complete set of conjugates of $(y^{(1)})$ over $K(z)$, then the cycle on W which is the inverse image of $z=0$ consists of a specialization $(\bar{y}^{(1)}, \ldots, \bar{y}^{(M)})$ of $(y^{(1)}, \ldots, y^{(M)})$ over $z \to 0$. The conjugates of y correspond to the conjugates $(y^{(1)}, \ldots, y^{(M)})$, and one can then use [4], Theorem 2 of Chapter I, § 4, applied to the polynomial $F(Y)$.)

We can write

$$F(Y) = G(Y) + zA(z, Y)$$

where $A(z, Y)$ is a polynomial in Y with coefficients in $\mathfrak{o}$. Since $A(0, Y)$ is defined, so is $A(z(Q), Y)$ for small values of $|z(Q)|_{\mathfrak{p}}$, which is all that we need to consider. Thus the values

$$|A(z(Q), y(Q))|_{\mathfrak{p}}$$

remain bounded since we could assume that $|y(Q)|_{\mathfrak{p}}$ remains bounded. Since $F(y)=0$, we get an estimate for $G(y(Q))$, namely

$$\begin{aligned} |G(y(Q))|_{\mathfrak{p}} &\leqq c_1 \, |z(Q)|_{\mathfrak{p}} \\ &\leqq \frac{c_2}{H(y(Q))^{\kappa r}} \end{aligned}$$

which puts us precisely in the situation described in § 1, and concludes the proof.

§ 3. Behaviour of heights under projection.

We use the same notation as in [7]. For this section, K is a global field. Property 1 F of [7] is still clearly valid without the restriction $\dim K = 1$, and so are the other Properties 2, 3, 4 and Theorem 3, where $\dim K = 1$ is not assumed.

Let V be a variety defined over K. For each morphism $\varphi : V \to \mathbf{P}^n$ (everywhere defined rational map) defined over K, we have height functions on V_K and $V_{\overline{K}}$, namely

$$H_\varphi(P) = H(\varphi(P)) \quad \text{and} \quad h_\varphi(P) = h(\varphi(P)).$$

We do not repeat here the discussion establishing the correspondence between maps of V into $\mathbf{P}^n$ and linear systems on V, but to fix the notation, if V is complete, normal, if X is a divisor on V rational over K, and $\mathscr{L}(X)$ is its complete linear system, and if we assume that $\mathscr{L}(X)$ is without fixed point, then we denote by H_X (or h_X) the height associated with any map into projective space arising from this linear system. These are well defined up to equivalence.

Foremost among the properties of heights is Property 4 (due to Weil) that the heights associated with two linear systems without fixed points whose divisors are linearly equivalent to each other (i.e. having the same complete linear system) are equivalent. This property will be used constantly in what follows.

The local behaviour at a point on a variety is represented by local parameters, and it is frequently more convenient to deal with these than with the coordinates in a projective embedding. In the following discussion (which depends only on Property 4 of heights), we make a generic projection and compare the heights arising from the embedding and its projection. We adjust the discussion to the immediate application we have in mind, and thus restrict ourselves to the case of curves.

Let W be a projective non-singular curve defined over K. The height h (or H) is taken with respect to this embedding. Let $(y_0, \dots, y_n)$ with $y_0 = 1$ be functions in K(W) determining our given embedding. Let Φ be a finite set of points of W in $\overline{\mathrm{K}}$. Then there is some polynomial equation such that if $(a_0, \dots, a_n, b_0, \dots, b_n)$ are elements in k not satisfying this equation, then the function

$$y = \frac{a_0 y_0 + \dots + a_n y_n}{b_0 y_0 + \dots + b_n y_n}$$

has the following properties :

The function y is not constant, and has no zero or pole among the points of Φ.

If h_y is the height determined by the mapping of W *into* $\mathbf{P}^1$ *arising from the function y, then*

$$h_y \sim h,$$

and thus $\mathrm{H}_y \sim \mathrm{H}$ *(as functions on* W_{K}*).*

The mapping

$$\mathrm{Q} \to y(\mathrm{Q})$$

gives an injection of Φ into $\overline{\mathrm{K}}$.

These properties are easily proved. Indeed, let Q be a point of W in $\overline{\mathrm{K}}$. If t is a function of order 1 at Q, then each y_i has an expansion as a power series in t, say $y_i = \xi_i t^{e_i} + \dots$ with an integer e_i, which may be negative. We see that there is a polynomial G_{Q} (linear) such that for any set of elements $(a_0, \dots, a_n)$ in k for which $\mathrm{G}_{\mathrm{Q}}(a) \neq 0$, then $a_0 y_0 + \dots + a_n y_n$ has order e at Q, where $e = \inf e_i$. Taking Q from a finite set Φ, we then take the product of the G_{Q} for $\mathrm{Q} \in \Phi$, and achieve the same thing for all $\mathrm{Q} \in \Phi$.

If $\mathfrak{a}_0$ denotes the sup of the polar divisors of our given y_i, then we see that almost all linear combinations $a_0 y_0 + \dots + a_n y_n$ have precisely $\mathfrak{a}_0$ as polar divisor. Furthermore, applying the above remarks to zeros instead of poles, and taking into account that the linear system determined by $(1, y_1, \dots, y_n)$ is without fixed point, we see that we can make a sufficiently general choice of a_i and b_i such that the function y has no zero or pole in Φ, and its divisor

$$(y) = (y)_0 - (y)_\infty$$

is such that $(y)_\infty$ lies in the above linear system. According to Property 4 of heights, it follows that h_y is equivalent to h.

To insure that the map $Q \to y(Q)$ is injective, we select among the y_i (for each Q) that function having the highest order pole at Q and denote it by y_Q. All quotients y_i/y_Q are defined at Q, and we have

$$y(Q) = \frac{a_0 w_0(Q) + \ldots + a_n w_n(Q)}{b_0 w_0(Q) + \ldots + b_n w_n(Q)}$$

where $w_i = y_i/y_Q$. (Strictly speaking, each w_i should carry Q also as an index.) We can choose the b_i so that the denominator does not vanish, and the condition that $y(Q) \neq y(Q')$ when $Q \neq Q'$ are two distinct points of Φ is immediately seen to be implied by the non-vanishing of a polynomial in the a_i and b_i. This concludes the proof of our three statements.

REMARK. Given a subfield E of K(W) containing K, and such that K(W) is finite separable algebraic over E, then it is clear that in addition to the above conditions, we can also require y to be a generator of K(W) over E.

Putting the results of § 2 together with the technique of generic projections, we get a more useful version of Theorem 1 :

THEOREM 1'. *Let* W *be a projective non-singular curve defined over a global field of characteristic* 0. *Let z be a non-constant function in* K(W), *and let r be the largest of the orders of the zeros of z. Let $\varkappa$ be a number* >2 *and* $c>0$. *Then the points* $Q \in W_K$ *such that*

$$|z(Q)|_\mathfrak{p} \leqq \frac{c}{H(Q)^{\varkappa r}}$$

have bounded height.

PROOF. We let Φ be the set of zeros and poles of W, and apply Theorem 1, taking into account the properties of H_y and its relation to H, the height taken relative to the given embedding of W in a projective space.

§ 4. Another property of heights.

Let K be a global field. As pointed out already, linear equivalence of linear systems gives rise to equivalent height functions. We shall now prove that algebraic equivalence gives rise to quasi-equivalent height functions. We need a lemma from pure algebraic geometry.

LEMMA. *Let* V *be a complete non-singular variety. Let* X *be a divisor on* V *such that some multiple* eX *is ample* (e *an integer* >0). *Then there exists an integer* $e'>0$ *such that for any divisor* Z *on* V *algebraically equivalent to* 0, *the divisor* $Z+e'X$ *is ample.*

PROOF. Let $\hat{A}$ be the Picard variety of V. We can always find a Poincaré divisor D on $V \times \hat{A}$ which is positive : If V is an abelian variety, this is Theorem 10 of Chapter IV,

§ 4, [5], and otherwise, making a generic translation on D, the pull-back method of Weil gives a positive Poincaré divisor on $V \times \hat{A}$ (*ibid.*, Theorem 1 of Chapter VI, § 1).

By hypothesis, $Z \sim {}^tD(a) - {}^tD(0)$ for some point $a \in \hat{A}$. The intersections are defined after making a generic translation on D. It is well known that there exists an integer $e_1 > 0$ such that $-{}^tD(0) + e_1X$ is ample (see for instance [9], Lemma 1). Furthermore, the divisors ${}^tD(a)$ as a ranges over $\hat{A}$ are all algebraically equivalent to each other, are positive divisors, and have the same projective degree. Hence there exists an integer $e_2 > 0$ such that ${}^tD(a) + e_2X$ is ample, again by [9], Lemma 1. From this our lemma is immediate.

PROPERTY 5. *Let* V *be a complete non-singular variety defined over* K. *Let* $X, Y > 0$ *be two positive divisors on* V, *rational over* K. *Assume that a positive multiple of each is ample, and that the linear systems* $\mathscr{L}(X)$ *and* $\mathscr{L}(Y)$ *are without fixed points. If* X *and* Y *are algebraically equivalent, then* h_X *and* h_Y *are quasi-equivalent* (*and so are* H_X *and* H_Y).

PROOF. Using property 4, we shall reduce our assertion to a statement concerning linear equivalence classes of divisors on V. By the lemma, there exists an integer $e > 0$ such that for all $n > 0$ we have

$$n(X - Y) + eX \sim Z_n$$

where Z_n is a positive divisor on V, and $\mathscr{L}(Z_n)$ is without fixed points. Since $n(X - Y) + eX$ is rational over K, one may take Z_n rational over K. We get $nX + eX \sim nY + Z_n$, and taking heights,

$$h_X^{n+e} \sim h_Y^n h_{Z_n}.$$

Since $h_{Z_n}(P) \geqq 1$ for all P, taking an n-th root, we see that given $\varepsilon > 0$, there exists a number $c > 0$ such that

$$c h_X(P)^{1+\varepsilon} \geqq h_Y(P)$$

if we take n sufficiently large. The other inequality is obtained in a similar way, or by symmetry.

When V is a curve, the statement is due to Siegel [14] whose proof we essentially imitate here, except that of course Siegel uses the Riemann-Roch theorem where we have used the Picard variety (see for instance [15], p. 435). In the case of curves, algebraic equivalence is determined by the degree of the divisor, and hence if $\deg(X) = d$ and $\deg(Y) = d'$, then h_X is quasi equivalent to $h_Y^{d/d'}$.

In particular, we note that if a set of points on the curve V has bounded height in some projective embedding, then it has bounded height in every projective embedding : The notion of a set of bounded height is independent of the embedding.

§ 5. Inequalities from the theory of heights.

We come now to the proof of the diophantine theorem proper.

Let C *be a non-singular curve, of genus* $\geqq 1$, *imbedded in some projective space over the global field* K. *The height* H *as a function on* C_K *is determined by this embedding.*

Let x be a function on C, *defined over* K *and not constant.* Then $(1, x)$ determines a mapping of C into $\mathbf{P}^1$, and the corresponding linear system is of degree

$$r = [K(C) : K(x)],$$

a divisor in it being, for instance, the divisor of poles of x. We assume that K(C) over $K(x)$ is separable. (At the very end, and only then, do we need characteristic 0, to contradict Roth's theorem.)

Let S *be a finite set of primes of* K, *containing the archimedean primes, and let* R *be a subring of* K *all of whose elements are* $\mathfrak{p}$*-integral for* $\mathfrak{p}$ *not in* S. *Let* $\mathfrak{R}$ *be the set of points of* C *rational over* K, *and such that* $x(P)$ *lies in* R. *We wish to prove that the height of the points in* $\mathfrak{R}$ *is bounded.* We assume the contrary, derive a list of inequalities which eventually contradict Roth's theorem. We let $\mathfrak{R}_1$ be a subsequence of $\mathfrak{R}$ such that the height of the points in $\mathfrak{R}_1$ tends to infinity.

By assumption, we have $|\xi|_{\mathfrak{p}} \leqq 1$ for $\mathfrak{p} \notin S$ and $\xi \in R$. Hence for all $P \in \mathfrak{R}_1$, we get

$$H(x(P)) = \prod_{\mathfrak{p} \in S} \sup(1, |x(P)|_{\mathfrak{p}}^{N_{\mathfrak{p}}})$$

where $N_{\mathfrak{p}}$ is the local degree in number fields, and 1 in function fields. Let $N = [K : \mathbf{Q}]$ in number fields, and 1 in function fields. Let s be the number of primes in S. Rewriting our product in terms of the absolute values, we see that we have at most Ns terms in it, of type

$$\sup(1, |x(P)|_{\mathfrak{p}}).$$

Consequently, for each $P \in \mathfrak{R}_1$, there exists one $\mathfrak{p}$ in S such that $|x(P)|_{\mathfrak{p}} \geqq H(x(P))^{1/Ns}$. Hence there exists an infinite subset $\mathfrak{R}_2$ of $\mathfrak{R}_1$ such that for some $\mathfrak{p}$ in S and all points P in $\mathfrak{R}_2$ we have

$$H(x(P))^{1/Ns} \leqq |x(P)|_{\mathfrak{p}}.$$

In view of Property 5, we can compare $H(x(P))$ and $H(P)$. If d is the degree of C in its given projective embedding, and φ the mapping into $\mathbf{P}^1$ given by the function x, we conclude that there is a number $c_3 > 0$ depending on ε such that for P in C_K we have

$$H(P)^{r/d - \varepsilon} \leqq c_3 H(x(P)).$$

Combining this with the previous inequality, we see that there is a number $\rho > 0$ such that for some $\mathfrak{p} \in S$ and all $P \in \mathfrak{R}_2$ we have for suitable $c_4 > 0$:

$$H(P)^{\rho} \leqq c_4 |x(P)|_{\mathfrak{p}}.$$

This inequality will be improved by going over to a covering of C, derived from the weak Mordell-Weil theorem. Furthermore, the arguments will prove the following improvement of Theorem 1′, for curves of genus $\geqq 1$.

THEOREM 2. *Let* K *be a global field of characteristic* 0. *Let* ρ, c *be numbers* >0. *Let* C *be a curve of genus* $\geqq 1$ *defined over* K, *and* x *a non-constant function in* K(C). *Let* $\mathfrak{p}$ *be a prime of* K. *Then the height of points* P *in* C_K *such that*

$$|x(P)|_{\mathfrak{p}} \leqq \frac{c}{H(P)^{\rho}}$$

is bounded.

(To apply the theorem, use the function $1/x$ instead of x.)

§ 6. Inequalities from the Mordell-Weil theorem.

We assume that C is embedded in its Jacobian J over K, and take J embedded in projective space. We take the induced embedding on C. For any point $P \in J_K$ we let H(P) be the height determined by our embedding, which remains fixed throughout.

In view of the definition of the height, and of $|\ |_{\mathfrak{p}}$, we may, without loss of generality, in the function field case, assume that the constant field is algebraically closed. This insures that for an integer $m>1$ we have J_K/mJ_K finite.

PROPOSITION 1. *Let* m *be an integer* >0, *unequal to the characteristic of* K. *Let* $\mathfrak{S}$ *be an infinite set of rational points of* C *in* K. *Then there exists an unramified covering* $\omega : W \to C$ *defined over* K, *an infinite set of rational points* $\mathfrak{S}'$ *of* W *in* K *such that* ω *induces an injection of* $\mathfrak{S}'$ *into* $\mathfrak{S}$, *and a projective embedding of* W *over* K *such that* $H \circ \omega$ *is quasi-equivalent to* H^{m^2}. (*Of course, in* $H \circ \omega$ *the* H *refers to the height on* C, *while in* H^{m^2} *it refers to the height on* W.)

PROOF. Let $a_1, \ldots, a_t$ be representatives of cosets of J_K/mJ_K. Infinitely many $P \in S$ lie in the same coset, and so there exists one point, say a_1, and infinitely many points Q in J_K such that $mQ + a_1$ lies in $\mathfrak{S}$. We let $\mathfrak{S}'$ be this infinite set of points Q. The covering $\omega : J \to J$ given by $\omega u = mu + a_1$ is unramified, and its restriction W to C is non-degenerate, i.e. is an irreducible covering of the same degree [6]. The inverse image of a point in C lies in W. Thus $\mathfrak{S}'$ is actually a subset of W_K. Restricting one's attention to a subset of $\mathfrak{S}'$ guarantees that ω induces an injection on this subset.

To prove the relation concerning the heights, we may work on the Jacobian itself since we take W in the projective embedding induced by that of J. If X is a hyperplane section of J, then

$$\omega^{-1}(X) = (m\delta)^{-1}(X_{-a_1}) \equiv m^2 X$$

where $\equiv$ is the equivalence of the square, known to be the same as algebraic equivalence. But $h_{\omega^{-1}(X)} \sim h_X \circ \omega$ by Property 3 of heights (which is trivial) and $h_{\omega^{-1}(X)}$ behaves essentially like $h_{m^2X} \sim h_X^{m^2}$ by Property 5. Our proposition is now clear, since for rational points in K, these equivalences are valid for H.

We note that $x(P) = x(\omega Q)$. Let z be the function on W such that $z(Q) = x(\omega Q)$. Let $\varkappa$ be a number >2 and let m be large enough such that $m^2\rho > \varkappa r$. Then for a suitable constant c_5 our inequality becomes

$$|z(Q)|_{\mathfrak{p}} \leqq \frac{c_5}{H(Q)^{\varkappa r}}$$

which is precisely the case treated in Theorem 1′. The fact that W is unramified over C guarantees us that the orders of the zeros of z are bounded by r. This concludes the proof of the original statement and of Theorem 2.

It is striking that the use we made of the Jacobian is formally analogous to the one in class field theory [6]. In that case, Artin's reciprocity law was reduced to a formal computation in the isogeny $u \to u^{(q)} - u$ of the Jacobian. In the present case, the heart of the proof is reduced to a formal computation of heights in the isogeny $u \to mu + a$.

§ 7. Extensions of finite type.

We shall extend the Siegel finiteness statement to rings of finite type over **Z**, and its analogue in function fields, including the relative case. We reduce our theorem to the case of dimension 1 (number fields, or function fields of one variable). We begin by giving a criterion which allows us to lower the field of definition of a curve.

Let K *be a function field over the constant field* K_0, which need not be algebraically closed, but which we assume to be *of characteristic* 0. If its dimension is >1, we select a projective normal model, relative to which we take our heights.

Let C be a complete non-singular curve defined over K. If $\mathfrak{R}$ is a subset of C_K, and the height of the points in $\mathfrak{R}$ is bounded in some projective embedding of C, then it is bounded in any other, as mentioned above. The next proposition deals with such sets. For the K/K_0-trace, cf. [5], Chapter VIII.

PROPOSITION 2. *Let* K, K_0 *be as above, and* C *a complete non-singular curve of genus* $\geqq 1$, *defined over* K. *Let* $\mathfrak{R}$ *be an infinite subset of* C_K *of bounded height. Regard* C *as embedded in its Jacobian* J *over* K, *and let* (B, τ) *be a* K/K_0*-trace of* J. *Then* τ *is an isomorphism. The points of* $\mathfrak{R}$ *lie in a finite number of cosets of* τB_{K_0}, *and if infinitely many of them lie in one coset, so are of type* $a+\tau b$ *where* a *is some point of* J_K *and* b *ranges over an infinite subset of* B_{K_0}, *then* $C_0 = \tau^{-1}(C_{-a})$ *is defined over* K_0, *and* τ *induces an isomorphism of* C_0 *onto* C_{-a}.

PROOF. We may assume J, B embedded in projective space. Using the auxiliary model of K over K_0 as in [7], we see from Theorem 3 and Proposition 2 of [7] that the points of $\mathfrak{R}$ lie in a finite number of cosets of τB_{K_0}. Say infinitely many lie in the coset $a+\tau B_{K_0}$. We know that τ establishes an isomorphism between B and $\tau(B)$ by Cor. 2 of Th. 9, Ch. VIII, [5]. Since infinitely many points of τB_{K_0} lie in C_{-a}, it follows that their K-closure in τB or in J is precisely C_{-a}. Put $C_0 = \tau^{-1}(C_{-a})$. Then C_0 is a curve contained in B, and τ induces an isomorphism τ_0 of C_0 onto C_{-a}. Furthermore, C_0 contains infinitely many points b of B rational over K_0. It is then a trivial matter to conclude that C_0 is defined over K_0 because these infinitely many points are both K_0 and K-dense in C_0. Since τB contains a translation of C, it follows that $\tau B = J$ is the Jacobian, i.e. τ is an isomorphism.

REMARK. If we do not assume characteristic 0 in Proposition 2, then τ is merely bijective, and C_0 may be defined over a purely inseparable extension of K_0.

Corollary. *Let* K, K_0 *be as above. Let* C *be a complete non-singular curve of genus* $\geqq 2$ *defined over* K, *and let* $\mathfrak{R}$ *be an infinite subset of* C_K *consisting of points of bounded height. Then there exists a curve* C_0 *defined over* K_0 *and a birational transformation* $T : C_0 \to C$ *defined over* K *such that all but a finite number of points of* $\mathfrak{R}$ *are images under* T *of rational points of* C_0 *in* K_0.

Proof. Since the genus is $\geqq 2$, the curve cannot be equal to any translation of itself in its Jacobian. Hence there can only be one coset having infinitely many points of C and we apply the proposition.

Combining our corollary with the results obtained in the previous section, we get the relative formulation of Siegel's theorem.

Theorem 3. *Let* K *be a function field over a constant field* k *of characteristic* 0. *Let* R *be a subring of* K *of finite type over* k. *Let* C *be a complete non-singular curve of genus* $\geqq 1$ *defined over* K, *and* φ *a non-constant function on* C *also defined over* K. *Let* $\mathfrak{R}$ *be the subset of* C_K *consisting of those points* P *such that* $\varphi(P) \in R$. *If* $\mathfrak{R}$ *is infinite, then there exists a curve* C_0 *defined over* k, *and a birational transformation* $T : C_0 \to C$ *defined over* K. *If the genus is* $\geqq 2$, *then all but a finite number of points of* $\mathfrak{R}$ *are images under* T *of points of* C_{0k}. *If the genus is* 1, *then the points of* $\mathfrak{R}$ *lie in a finite number of cosets of* $T(C_{0k})$.

To deal with the absolutely algebraic case, we need a specialization argument.

Theorem 4. *Let* K *be a field of finite type over* $\mathbf{Q}$, *and* R *a subring of* K *of finite type over* $\mathbf{Z}$. *Let* C *be a non-singular curve of genus* $\geqq 1$ *defined over* K, *and let* φ *be a function in* K(C) *which is not constant. Let* $\mathfrak{R}$ *be the subset of* C_K *consisting of points* P *such that* $\varphi(P) \in R$. *Then* $\mathfrak{R}$ *is finite.*

Proof. We may assume C projective non-singular. Suppose $\mathfrak{R}$ infinite. Let k be the algebraic closure of $\mathbf{Q}$ in K. Then by Theorem 3, C is birationally equivalent over K to a curve C_0 defined over k. If the genus of C is 1, we restrict our attention to an infinite subset of points of $\mathfrak{R}$ which lie in the same coset of $T(C_{0k})$. Then, without loss of generality, we may assume $C = C_0$, and that we have infinitely many points of C in K such that $\varphi(P) \in R$, where φ is a function on C defined over K. We shall now prove our theorem by induction on the dimension of K over $\mathbf{Q}$.

Let F be a subfield of K containing k, and such that the dimension of K over F is 1. There exists a discrete valuation ring $\mathfrak{o}$ of K containing F and R whose residue class field $E = \mathfrak{o}/\mathfrak{m}$ is finite over F, and such that the reduction φ' of φ mod $\mathfrak{m}$ is a non-constant function $\varphi' : C \to \mathbf{P}^1$ (of the same degree as φ). For any point Q of C_K, we get a specialized point Q' in C_E, and $\varphi'(Q') = \varphi(Q)'$, using the compatibility of intersections and reductions, i.e. formally, using the graphs :

$$[\Gamma_\varphi \cdot (Q \times \mathbf{P}^1)]' = \Gamma'_\varphi \cdot (Q' \times \mathbf{P}^1)$$

the left hand side being $Q \times \varphi(Q)$ and the right hand side being $Q' \times \varphi'(Q')$. This yields infinitely many points Q' of C_E such that $\varphi'(Q')$ lies in the ring R', image of R in the homomorphism $\mathfrak{o} \to \mathfrak{o}/\mathfrak{m}$. Since E is of finite type over $\mathbf{Q}$, of dimension one less than that of K, and since R′ is still of finite type over $\mathbf{Z}$, this concludes the proof.

REMARK. The theorem could also be proved by using Néron's theorem which implies that say for an affine curve $f(X, Y) = 0$ of genus $\geqq 1$ with coefficients in R, there exists a homomorphism $R \to R'$ of R into a ring R′ contained in a number field such that if $f'(X, Y) = 0$ is the specialized curve, then its genus is also $\geqq 1$ and the homomorphism $R \to R'$ induces an injection of the points of f in R into those of f' in R′. (See [11], Th. 6.)

Columbia University, New York.

BIBLIOGRAPHY

[1] E. ARTIN and G. WHAPLES, Axiomatic characterization of fields by the product formula, *Bull. Am. Math. Soc.*, vol. 51, nº 7 (1945), pp. 469-492.

[2] C. CHABAUTY, Sur les équations diophantiennes liées aux unités d'un corps de nombres algébriques fini, thèse, *Annali di Math.*, 17 (1938), pp. 127-168.

[3] — Sur les points rationnels des variétés algébriques dont l'irrégularité est supérieure à la dimension, *Comptes rendus Académie des Sciences*, Paris, 212 (1941), pp. 1022-1024.

[4] S. LANG, Introduction to algebraic geometry, *Interscience*, New York, 1959.

[5] — Abelian varieties, *Interscience*, New York, 1959.

[6] — Unramified class field theory over function fields in several variables, *Annals of Math.*, vol. 64, nº 2 (1956), pp. 285-325.

[7] S. LANG and A. NÉRON, Rational points of abelian varieties in function fields, *Am. J. of Math.*, vol. 81, nº 1 (1959), pp. 95-118.

[8] K. MAHLER, Über die rationalen Punkte auf Kurven vom Geschlecht Eins, *J. Reine angew. Math.*, Bd. 170 (1934), pp. 168-178.

[9] T. MATSUSAKA, On algebraic families of positive divisors..., *J. Math. Soc. Japan*, vol. 5, nº 2 (1953), pp. 118-136.

[10] L. J. MORDELL, On the rational solutions of the indeterminate equation of the third and fourth degrees, *Proc. of the Cambridge Philos. Soc.*, 21 (1922).

[11] A. NÉRON, Problèmes arithmétiques et géométriques rattachés à la notion de rang d'une courbe algébrique dans un corps, *Bull. Soc. Math. France*, 80 (1952), pp. 101-166.

[12] D. RIDOUT, The *p*-adic generalization of the Thue-Siegel-Roth theorem, *Mathematika*, 5 (1958), pp. 40-48.

[13] K. F. ROTH, Rational approximations to algebraic numbers, *Mathematika*, 2 (1955), pp. 1-20.

[14] C. L. SIEGEL, Über einige Anwendungen Diophantischer Approximationen, *Abh. Preussischen Akademie der Wissenschaften*, Phys. Math. Klasse (1929), pp. 41-69.

[15] A. WEIL, Arithmetic on algebraic varieties, *Annals of Math.*, vol. 53, nº 3 (1951), pp. 412-444.

[16] — L'arithmétique sur les courbes algébriques, *Acta Mathematica*, 52 (1928), pp. 281-315.

Reçu le 20 mars 1960.