Division points on curves.

by SERGE LANG (a New York)

In memory of Guido Castelnuovo in the recurrence of the first centenary of his birth.

Summary. - *A curve contained in a product of multiplicative groups passing through the origin, and containing infinitely many torsion points is a subgroup. The analogous statement on abelian varieties is discussed and reduced to an analogue of the irreducibility of the cyclotomic equation.*

Let A be an abelian variety, or a product of multiplicative groups (or a group extension of these), defined over the complex numbers, say. Let Γ_0 be a finitely generated subgroup of A, and let V be a curve (subvariety of dimension 1) in A, passing through the origin, say. When A is an abelian variety, the MORDELL conjecture has been expressed as asserting that *if the intersection of V with Γ_0 is infinite, then V is a group subvariety* (cf. [2], [3]). When A is a product of multiplicative groups, then I proved the analogous statement in [2], [3].

A few years ago, MUMFORD asked me the following question:

If a curve in its Jacobian contains infinitely many points of finite period, is the curve of genus 1? The same question arose in MANIN'S investigations of the PICARD-FUCHS equations [4]. At the time I did not see how to make a conjecture which would include all the above statements, but now it seems to me that one can formulate such a conjecture as follows: *Let Γ be the division group of Γ_0, i.e. the group of points P on A such that there exists some integer $n \geqq 1$ (depending on P) such that nP lies in Γ_0. If the intersection of V with Γ is infinite, then V is a group subvariety.* In other words, from a diophantine point of view, when one considered previously a finitely generated group, one may as well consider its division group. Taking Γ_0 to be the unit element of A yields the special case when Γ consists of all points of finite period on A.

When A is a product of multiplicative groups, then the conjecture admits a particularly elementary formulation:

Let Γ_0 be a finitely generated multiplicative group of complex numbers, and let Γ be the group of complex numbers z such that z^n lies in Γ_0 for some n (depending on z).

Let $f(X, Y) = 0$ be a curve in the plane (absolutely irreducible) passing through the multiplicative origin, i.e. $f(1, 1) = 0$. If there exist infinitely many elements $x, y \in \Gamma$ such that $f(x, y) = 0$, then the curve is actually a group, whence f is a polynomial of type $aX^m + bY^n = 0$ or $X^nY^m + c = 0$.

As a special case, one then has the statement: *Let $g(X)$ be a rational function, and assume that there exist infinitely many elements $x \in \Gamma$ such that $g(x) \in \Gamma$. Then $g(X) = cX^n$ for some constant c and some integer n.*

When we take elements in Γ_0 instead of Γ, then of course this is a special case of the theorem proved in [2]. For instance, the line

$$aX + bY = c$$

with $abc \neq 0$ has only a finite number of points with coordinates in Γ_0.

IHARA, SERRE, and TATE have shown to me how to prove the conjecture in the case Γ consists of roots of unity, and I shall reproduce here IHARA'S and TATE'S proofs. (SERRE'S proof is similar to TATE'S.) I shall then describe a geometric interpretation for these proofs, and indicate how they lead to certain «irreducibility» criteria on abelian varieties, related to recent work of SERRE concerning the GALOIS group of division points of elliptic curves over number fields [5].

§ 1. IHARA'S PROOF. - Let us begin with IHARA'S proof, given only for a rational function. Let g be a rational function, and assume that there exist infinitely many roots of unity ζ such that $g(\zeta)$ is a root of unity. Then g has coefficients in some cyclotomic field. (Proof: Let F be the field obtained by adjoining al roots of unity to the rationals, let K be the field obtained from F by adjoining the coefficients of g. If $K \neq F$, there exists an isomorphism σ of K over F such that $g^\sigma \neq g$, and then g^σ, g take on the same values at infinitely many roots of unity, which is impossible). We may assume that this field of coefficients of g is finite over $\boldsymbol{Q}$, generated by a primitive m—*th* root of unity, say $k = \boldsymbol{Q}(\zeta_m)$. After a multiplicative translation, we may also assume that $g(1) = 1$.

Let $\{\zeta_n\}$ be a sequence of roots of unity such that $g(\zeta_n)$ is a root of unity, with $n = n_1, n_2, \ldots, n \to \infty$, and each ζ_n is a primitive n—*th* root of unity. For each n, there exists an automorphism σ_n of $\boldsymbol{Q}(\zeta_n)$ over $\boldsymbol{Q}$ such that

$$\sigma_n \zeta_n = e^{2\pi i/n}.$$

Extend σ_n to F. Then

$$(\sigma_n g)(\sigma_n \zeta_n) = \sigma_n(g(\zeta_n))$$

is contained in the field $\boldsymbol{Q}(\zeta_m, \zeta_n)$, and hence is a $2mn$ — *th* root of unity (not necessarily primitive). For infinitely many n, the restriction of σ_n to k

induces the same isomorphism on k. Taking a subsequence of $\{n\}$, and dealing with a conjugate of g if necessary, we can assume without loss of generality that for infinitely many n there exists an integer d_n such that

$$g(e^{2\pi i/n}) = e^{2\pi i d_n/2mn}.$$

The roots of unity $e^{2\pi i/n}$ approach 1 as n tends to infinite. Without loss of generality, we may assume that $2\pi i d_n/2mn$ approaches 0. We have (by the mean value theorem):

$$| e^{2\pi i d_n/2mn} - 1 | = | g(e^{2\pi i/n}) - g(1) | \leqq C | e^{2\pi i/n} - 1 |$$

for some constant $C > 0$, whence

$$| d_n/2mn | \leqq C' | 1/n |$$

for some other constant $C' > 0$. This implies that the numbers d_n are bounded, and hence taking a subsequence of n if necessary, that they are all equal to the same number. But then one concludes at once that there exist infinitely many roots of unity $\zeta (= e^{2\pi i/n})$ and a fixed integer D such that

$$g(\zeta)^{2m} = \zeta^D,$$

whence $g(X)^{2m} = X^D$ identically, as was to be shown.

§ 2. TATE'S PROOF. - Let $f(X, Y)$ be an irreducible polynomial in $\boldsymbol{C}[X, Y]$, and assume that there exist infinitely many pairs of roots of unity $\zeta = (\zeta', \zeta'')$ such that $f(\zeta) = 0$. Then the coefficients of f lie in some field $\boldsymbol{Q}(\zeta_m) = k$, generated over $\boldsymbol{Q}$ by a primitive $m - th$ root of unity. (As before, one sees this by considering conjugates of f over the field F obtained by adjoining all roots of unity to the rationals).

Let n be the period of ζ (i.e. the least common multiple of the periods of ζ', ζ''). Let d be a positive integer prime to n. There exists an automorphism σ of $\boldsymbol{Q}(\zeta)$ such that $\sigma\zeta = \zeta^d$. If in addition $d \equiv 1 \pmod{m}$, then σ can be extended to an automorphism of $k(\zeta)$ inducing the identity on k. Then $f(\zeta^d) = 0$, so that ζ is a zero of $f(X, Y)$ and also of $f(X^d, Y^d)$. But

$$[k(\zeta) : k] \geqq \varphi(n)/m.$$

Applying any automorphism τ of $k(\zeta)$ over k, we find that $\tau\zeta$ is also a common zero of these two polynomials, which have therefore at least $\varphi(n)/m$ zeros in common. However, by BEZOUT'S theorem, these polynomials have at most $(\deg f)^2 d$ common zeros, unless $f(X, Y)$ divides $f(X^d, Y^d)$. As soon as n is

large enough, we can use the prime number theorem giving the existence of of primes in arithmetic progressions to find a prime number d satisfying the above conditions, such that d is much smaller than $\varphi(n)$. Hence we conclude that $f(X, Y)$ divides $f(X^d, Y^d)$, and it is then an exercise to show that $f(X, Y) = 0$ defines a subgroup variety of $\boldsymbol{C}^* \times \boldsymbol{C}^*$. This concludes the proof, which also shows that n is bounded in terms of deg f and m.

Note that we can avoid the congruence condition $d \equiv 1 \pmod{m}$ by using the following variation of TATE'S argument. Let $r = [k : \boldsymbol{Q}]$. We extend σ to an automorphism of $k(\zeta)$. Then σ^r induces the identity on k, and

$$\sigma^r \zeta = \zeta^{d^r}.$$

Then $f(\zeta^{d^r}) = 0$, so that ζ is a zero of $f(X, Y)$ and also $f(X^{d^r}, Y^{d^r})$. We can then argue as before, using only the lemma:

LEMMA. - *Given an integer s, there exists an integer n_0 such that for all $n > n_0$, there exists a prime number p not dividing n, such that $p^s \leqq n$.*

PROOF. - The worst case occurs when n is a product of distinct primes, in which case the assertion is an immediate consequence of the fact $\pi(N)$ is of the order of magnitude of $N/\log N$.

§ 3. ABELIAN VARIETIES. - We shall now see how this variation can be formulated on abelian varieties.

Let A be an abelian variety, defined over the complex numbers, and let V be a curve (subvariety of dimension 1) in A. We assume that V contains infinitely many torsion points. After a translation, we may assume that V passes through the origin. Let k be a field of definition for A and V, finitely generated over the rationals. We shall reduce the proof that V is of genus 1 to a statement analogous to the irreducibility of the cyclotomic equation.

Let m be an integer $\geqq 1$. Let $\lambda_m : A \to A$ be multiplication by m. As a cycle, $\lambda_m(V) = \mu \cdot V^{(m)}$, where $V^{(m)}$ consists of all points mx, with $x \in V$. Then $\mu \cdot V^{(m)}$ is algebraically equivalent to $m^2 \cdot V$. If $V \neq V^{(m)}$, then $V \cap V^{(m)}$ has at most $m^2(\deg V)^2$ points, by a routine generalization of BEZOUT'S theorem. (Cf. for instance [2], Lemma 4, Chapter III, § 3. We can view V and $V^{(m)}$ as divisors on their sum in A).

If $V = V^{(m)}$, then λ_m gives an unramified covering of V over itself, of degree m^2, and hence V is of genus 1, so is an abelian subvariety.

Let Γ be the group of torsion points of A. We reduce the proof of the conjecture in this case to the following hypothesis:

(*) *Let A be an abelian variety defined over k. There exists an integer $c \geqq 1$ with the following property. Let x be a point of period n on A. Let G_n*

be the multiplicative group of integers prime to n, mod n. Let G be the subgroup of G_n consisting of those integers d such that dx is conjugate to x over k. Then

$$(G_n : G) \leqq c.$$

To apply (*), suppose that there exist points x_n of period n, $n \to \infty$, lying on V. Let d be a positive integer prime to n. By (*), there exists an automorphism σ of $k(x)$ over k such that $\sigma x = d^r x$, where r is a positive integer bounded by c. Then

$$\sigma x = d^r x \in V \cap V^{(d^r)}.$$

Furthermore, if τ is in the group of automorphisms of $k(x_n)$ over k, then

$$\tau d^r x \in V \cap V^{(d^r)}.$$

If $V \neq V^{(d^r)}$, we obtain the inequalities, using (*):

$$\frac{\varphi(n)}{c} \leqq \text{Number of points on } V \cap V^{(d^r)} \leqq d^{2r}(\deg V)^2.$$

We note that $\varphi(n) \geqq n^{1/2}$ for sufficiently large n. By the lemma, taking d to be a sufficiently small prime number not dividing n, we get a contradiction as soon as n is sufficiently large, as desired.

At present, very little is known concerning (*). Recent work of SERRE has been concerned with the size of the GALOIS groups of period points of elliptic curves over number fields, and SERRE has ben able to prove «finite index» property for most elliptic curves, when n is a prime power [5]. SERRE also tells me that property (*) is true when elliptic curve has complex multiplication. Furthemore, if the elliptic curve has a transcendental j-invariant over the rationals, then the truth of (*) follows from results of IGUSA [1]. Nothing seems to be known in more general cases.

§ 4. APPENDIX. - We conclude by a remark concerning the exercise about $f(X^d, Y^d)$ made previously. Let G be a commutative group variety (in characteristic 0), and let V be a curve on G, passing through the origin. Assume that there exists an integer $d > 1$ such that for all $x \in V$, the point dx also lies in V. (We write the group law additively). Then V is a subgroup of G. Indeed, let p be a prime number dividing d. If k_0 is a field of definition for G and V, finitely generated over the rationals, we can embed k_0 in a finite extension of the p-adic field $\boldsymbol{Q}_p$, and let k denote the completion of the algebraic closure of $\boldsymbol{Q}_p$. If x is a point of V_k sufficiently close to the origin, then dx lies in V_k, and the points $d^n x$ approach 0 as n tends to

infinity (for the p-adic topology on V_k). Taking the inverse image by the exponential map of a sufficiently small neighborhood U of 0 in V_k, we find on the tangent space at the origin that $\exp^{-1}(U)$ has an infinite intersection with a straight line, having 0 as point of accumulation. This implies that $\exp^{-1}(U)$ contains a small (infinite) subgroup, and hence that U contains a small subgroup. Since V is a curve, this small subgroup is ZARISKI dense in V, and hence V is a group, as was to be shown.

BIBLIOGRAPHY

[1] J. IGUSA, *Fiber systems of elliptic curves*, American Journal of Mathematics 81 (1959), pp. 453-476.

[2] S. LANG, *Diophantine Geometry*, Intersience, 1962.

[3] — —, *Integral points on curves*, Publication l'I.H.E.S., No. 6 (1960) pp. 27-43.

[4] J. MANIN, *Rational points of algebraic curves over function fields* (in Russian), Izvestia Akademia Nauk 27 (1963), pp. 1395-1440.

[5] J.P. SERRE, *Groupes de Lie l-adiques attachés aux courbes elliptiques*, Colloque de Clermond-Ferrand (1964) pp. 197-212.