Reprinted from *Amer. Math. Soc. Transl. Ser.* 2, **50** (1966).

RATIONAL POINTS OF ALGEBRAIC CURVES OVER FUNCTION FIELDS

Ju. I. MANIN

Summary. Mordell's conjecture is proved for algebraic curves with function fields as ground fields.

Introduction

1. The principal goal of this paper is the proof of the following result.

Theorem. *Let K be a regular extension of the field k of characteristic 0 and let C be a curve of genus ≥ 2 defined over K. If there are infinitely many points on C rational over K, then it is birationally equivalent to a curve C_0 defined over k and all except possibly finitely many of the points correspond to points of C_0 defined over k.*

In particular, if C is a "nonconstant" curve, i.e., if its least field of definition is not absolutely algebraic, then it has only a finite number of points defined over any given field of finite type.

This theorem gives a proof of a part of Mordell's conjecture (cf. Lang [5], p. 29). In fact, Mordell [11] enunciated the conjecture only for curves over the field of rational numbers: the subsequent extension of the Mordell-Weil theorem to algebraic fields and then to function fields makes it natural to pose the question of the truth of the conjecture for all possible ground fields of finite type.

As Lang remarked, Mordell's conjecture is equivalent to the assertion that a curve lying in an abelian variety has only a finite number of points in common with any subgroup of finite type of the variety. This formulation contains no explicit reference to the ground field. Nevertheless, it seems probable that the proof of Mordell's conjecture cannot be achieved without using the arithmetic (in the wide sense of the word) of the ground field. If that is so, then our result can be regarded as a reduction of the general problem to the case when the ground field is an algebraic number field: a case which has so far remained inviolate to known methods. We leave it to the reader to judge how far the ideas of this paper can be useful when applied to that case.

2. This paper naturally falls into three parts, corresponding to the three chapters. The first chapter is devoted to the working out of a technique which is essential to the rest of the exposition; the second chapter proves the theorem enunciated above; and the third contains the proof of some strong finiteness theorems for elliptic curves.

We shall illustrate the fundamental idea of this paper by the example of the "general" elliptic curve $C: Y^2 = X(X-1)(X-t)$ and will take as our ground field a finite extension of $C(t)$, where C is the field of complex numbers. Let γ be a 1-dimensional cycle on the Riemann surface of C and let $\omega = Y^{-1}\,dX$ be a differential of the first kind on C. The period $\eta(t) = \int_\gamma \omega$, considered as a function of t, is an infinitely many-valued analytic function on the t-plane punctured at $t = 0, 1$. (For the precise meaning of this and the following assertions see §6.) The nature of these functions has been well known for a long time: they are solutions of the Gauss linear differential equation

$$4t(1-t)\frac{d^2\eta}{dt^2} + 4(1-2t)\frac{d\eta}{dt} - \eta = 0. \tag{1}$$

The space of solutions of this equation is 2-dimensional (over the complex field), having as basis an arbitrary pair of periods

$$\eta_1(t) = \int_{\gamma_1} \omega, \quad \eta_2(t) = \int_{\gamma_2} \omega$$

over linearly independent cycles γ_1, γ_2 generating the integral 1-dimensional homology of the Riemann surface of C.

On the other hand, functions of the type $\int_O^P \omega$ where O is the point at infinity, play a large role in the investigation of points on C with coordinates in K. This function is defined by P only up to a integral linear combination $m_1\eta_1(t) + m_2\eta_2(t)$ and satisfies the equation

$$\int_O^P \omega + \int_O^Q \omega = \int_O^{P+Q} \omega,$$

modulo such a linear combination, where $P + Q$ is the sum according to the group law on C which has O as its zero. It is natural to attempt to remove the indeterminacy of this last functional equation by acting on both sides with the Gauss differential operator which annihilates the periods $\eta_1(t)$ and $\eta_2(t)$. Then the function

$$\mu(P) = \left(4t(1-t)\frac{d^2}{dt^2} + 4(1-2t)\frac{d}{dt} - 1\right)\int_O^P \omega$$

becomes a finitely many-valued meromorphic function on the Riemann t-sphere. It becomes single-valued on the Riemann surface of K and thus may be identified with an element of K. A remarkable property of this function, which follows from the linearity of the Gauss operator, is that it defines a homomorphism of the group of points of C defined over K into the additive group of K:

$$\mu(P+Q)=\mu(P)+\mu(Q).$$

It is not difficult to express $\mu(P)$ explicitly in terms of the coordinates $(X(t), Y(t))$ of P:

$$\mu(P)=\frac{1}{2}\frac{Y(t)}{(X(t)-t)^2}-\frac{d}{dt}\left[2t(t-1)\frac{\frac{d}{dt}X(t)}{Y(t)}\right]-2t(t-1)\frac{d}{dt}X(t)\cdot\frac{d}{dt}\frac{1}{Y(t)}. \quad (2)$$

This formula is instructive in that it shows the nature of the function $\mu(P)$ obtained from the coordinates of P by applying a linear differential operator (in this case differentiation with respect to t). The proof of (2) depends on the following argument.

First of all the Gauss equation (1) is a consequence of the purely algebraic equation

$$\left[4t(1-t)\frac{\partial^2}{\partial t^2}+4(1-2t)\frac{\partial}{\partial t}-1\right](Y^{-1})\,dX=\frac{1}{2}\,d\frac{Y}{(X-t)^2}. \quad (3)$$

Here $\partial/\partial t$ denotes the operator "partial differentiation with respect to t keeping X fixed" and d is the differential in the field $K(X, Y)/K$, i.e., "keeping t fixed". The application of the Gauss operator to the period $\int_\gamma \omega$ is carried out by taking the operator under the integral sign; and then it is necessary only to note that the integral round a closed contour of the exact differential $d(Y/(X-t)^2)$ is zero.

The formula (2) is obtained analogously, but here it is necessary to consider the dependence on the parameter t of the limits of integration in

$$\int_O^P \omega=\int_\infty^{X(t)} Y^{-1}\,dX.$$

The first term in the right hand of (2) is the integral of $-d(Y/(X-t)^2)$ between the given limits, the remaining terms are the contribution of the change of the limits of integration. We note that if the value of X at P does not depend on t, then all the terms except the first vanish.

The construction described here can be carried out in a completely general situation: for an arbitrary system of algebraic varieties depending on parameters with respect to which one may differentiate in some sense. The generalization of the Gauss differential equation to periods of abelian integrals on curves of arbitrary genus was obtained by Picard and Fuchs (cf. [12]). We give a similar generalization to the case of arbitrary algebraic varieties. The key idea is that relations similar to (3) can be found for closed 1-dimensional differential forms of the first kind on arbitrary algebraic varieties on whose field of definition there is a derivation ∂ (corresponding to the differentiation d/dt). The first section of Chapter I

is devoted to the construction and theory of such relations, which we propose to call Picard-Fuchs equations. We should remark that Picard and Fuchs considered only equations of the type

$$\mathfrak{L} \int_\gamma \omega = 0,$$

where $\mathfrak{L}$ is a linear differential operator and ω is an abelian differential. There are good algebraic reasons, however, for considering the more general equations

$$\mu : \sum_{i=1}^{n} \mathfrak{L}_i \int_\gamma \omega_i = 0$$

since this allows us to endow the totality of equations with the structure of a module over the ring of differential operators and to find a finite number of generators.

§§2, 3 and 4 contain the definition and investigation of functions analogous to $\mu(P)$. Heuristically they are given by

$$\mu(P, Q) = \sum_{i=1}^{n} \mathfrak{L}_i \int_P^Q \omega_i,$$

but up to §6 we employ only an algebraic definition. Besides having essential methodological advantages our definition works in situations in which it would be unnatural to introduce analytical limitations (e.g., when the ground field is a field of formal power series).

The content of the fifth and sixth sections runs parallel to the theory described above for elliptic curves and consists essentially in carrying this theory over to abelian varieties of arbitrary dimension depending on parameters. We illustrated earlier only the construction of the homomorphism $P \longrightarrow \mu(P)$: a less trivial part of the theory is to investigate how far the homomorphism is nontrivial, i.e., the investigation of the kernel. Let us return to the curve $Y^2 = X(X-1)(X-t)$. Clearly all points of finite order are in the kernel. The following argument shows that the kernel contains no further points. If $\mu(P) = 0$, the integral $\int_O^P \omega$ must be a linear combination with constant coefficients of $\eta_1(t)$ and $\eta_2(t)$:

$$\int_O^P \omega = c_1\eta_1(t) + c_2\eta_2(t), \quad c_1, c_2 \in \mathbf{C}.$$

To establish that P is of finite order we must show that c_1, c_2 are *rational*. For this we make essential use of the fact that the coordinates of P are *algebraic* functions of t. The idea of the proof is as follows. The cycles γ_1, γ_2 can be chosen in such a way that circuits σ_1, σ_2 round the points $t = 0$, $t = 1$ respectively produce the following changes in the many-valued functions η_1, η_2:

$$\sigma_1: \begin{cases} \eta_1(t) \to \eta_1(t), \\ \eta_2(t) \to \eta_2(t) + \eta_1(t); \end{cases} \qquad \sigma_2: \begin{cases} \eta_1(t) \to \eta_1(t) + \eta_2(t), \\ \eta_2(t) \to \eta_2(t). \end{cases}$$

Hence one circuit adds $c_2\eta_1(t)$ or $c_1\eta_2(t)$ respectively to the integral $\int_O^P \omega$. But since the coordinates of P are algebraic functions, they must return to their original values after a finite number, say d, of circuits, and so $\int_O^P \omega$ must take a value differing from the original one by a linear combination of the periods η_1, η_2. Hence dc_1 and dc_2 are integral; that is, c_1 and c_2 are rational. This proves our assertion about the kernel of μ. The analogous result for abelian varieties is Theorem 2, which is formulated in §5 and proved in §6.

It is important to emphasize that Theorem 2, which describes the intersection of the kernels of all possible homomorphisms μ on an abelian variety, is then used to give information about the functions μ on algebraic curves. This is possible because the construction of these functions has functorial character and, in particular, for the points of a curve immersed in its jacobian the functions μ give the same result whether we start with the Picard-Fuchs equations for the whole variety, or only with their restrictions to the curve.

3. The second and third chapters are of a significantly more technical nature. The possibility of using functions of the type μ to prove finiteness theorems about points on curves is by no means obvious, and the argument is different in the cases genus ≥ 2 and genus 1.

In very general terms the contents of the second chapter are as follows. We suppose that there are infinitely many points on the curve C defined over K. We embed C in its jacobian and consider the values of the functions μ at points P of C. By the Mordell-Weil theorem (cf. [6]) and our Theorem 2 every such function takes its values in a subgroup of finite rank in the additive group of K.

On the other hand, as for an elliptic curve, each function $\mu(P)$ results from the operation of some differential operator on the coordinates of P. A rather obvious investigation of these operators leads to linear relations of the type

$$\Sigma z_i(P)\mu_i(P) = 0,$$

where the z_i are rational functions on C. If there are sufficiently many of these relations, we can deduce relations of the type

$$\mu_i(P) = c_i \in K$$

and apply the theorem about the intersection of the kernels of the μ (on the jacobian variety). To obtain sufficiently many relations we have to use not only C itself but certain unramified coverings, which also contain infinitely many points. The form of the function μ depends on the structure of the module of Picard-Fuchs equations on the curve and consequently one has to consider separately two cases.

It is difficult to sketch further particulars without going into the treatment in full.

In the third chapter, which treats the elliptic case, we have only the one function $\mu(P)$ and everything depends on it. This is connected with the fact that the module of Picard-Fuchs equations has only one generator. The idea of Theorem 4 (cf. its formulation in §11) consists in establishing a uniform continuity of the map $P \longrightarrow \mu(P)$ in the local topologies of the field K. Since the values of $\mu(P)$ lie in a subgroup of finite type of the additive group of K, which is discrete in every local topology, it follows that the group of rational points is discrete. In particular, in every local topology the point P cannot approach too closely to O. For the curve $Y^2 = X(X-1)(X-t)$ this means that the denominator of $X(t)$ cannot have zeros of arbitrary large multiplicity. This gives a variant for the function-field case of Mahler's theorem about the number of "integral" points on an elliptic curve. Actually Theorem 4, as is shown in §11, is a pretty strong statement and its analogue for algebraic number fields is false.

It is possible that the methods of the last two chapters can be applied to Lang's conjectures (cf. [5]) about integral points on affine subvarieties and rational points on closed subvarieties respectively of abelian varieties (of course, with a function field as ground field). Partly for these reasons the constructions of the first chapter have been carried out in somewhat greater generality than was immediately necessary for the investigation of curves. We also remark that it would be of interest to connect our arguments with the technique of principal homogeneous spaces (cf. [1]).

4. The fundamental ideas of the first chapter are already contained in [8] and [9]. The second of these explains the meaning of the Picard-Fuchs equations for curves over fields of finite characteristic, thus giving a general answer to the question posed by Igusa [13] and solved by him for elliptic curves [14]. The last chapter of this paper is a reworking of [10]. The essentially new part of this paper is the second chapter containing the proof of the function-field case of Mordell's conjecture. Nevertheless the paper has been written so that it can be read independently of the previous publications, which can be regarded as of a preliminary nature.

We shall use constantly and without special reference algebro-geometric concepts and results (in particular from the theory of abelian varieties) which are expounded in the two books of Lang [2], [3]. Besides, we shall need the elements of the theory of heights described in the papers of Lang [5] and Lang and Néron [6]. Further, we shall need the fundamental facts of the theory of abstract derivations (the theorems about extension and existence) and of differential forms. Finally, in §6 we shall use some simple topologico-analytic tools.

The numeration of sections, theorems, propositions, lemmas and formulas is continuous throughout the paper.

CHAPTER I

Picard-Fuchs equations and additive functions on abelian varities

§1. Picard-Fuchs equations

1. Let K be a field of characteristic 0 and let L be a regular extension (in the sense of Weil) of transcendence degree n. For any derivation $\partial: K \longrightarrow K$ and any transcendence base $x = (x_1, \cdots, x_n)$ of L/K we shall denote by ∂_x the unique derivation of L which vanishes on all the x_i, $1 \leq i \leq n$, and coincides with ∂ on K. In its turn, we extend ∂_x to a derivation of the L-module Ω of differential forms of L/K by putting

$$\partial_x \left(\sum u_{i_1 \ldots i_r} dx_{i_1} \wedge \ldots \wedge dx_{i_r} \right) = \sum \partial_x u_{i_1 \ldots i_r} dx_{i_1} \wedge \ldots \wedge dx_{i_r}.$$

Let $B, Z \subset \Omega$ be the K-subspaces of exact and closed forms respectively.

Lemma 1. $\partial_x(B) \subset B$, $\partial_x(Z) \subset Z$.

Proof. It is enough to check that $\partial_x(d\omega) = d(\partial_x \omega)$ for any form $\omega \subset \Omega$. In turn, for this it is enough to check that the map $\partial_x \circ d - d \circ \partial_x : L \longrightarrow \Omega$ is zero. But this is a derivation of L with values in the L-module Ω vanishing on $K \subset L$ and on the x_i, $1 \leq i \leq n$. Since L is a separable extension of $K(x_1, \cdots, x_n)$ a standard argument shows that $\partial_x \circ d - d \circ \partial_x$ is trivial on L. This proves the lemma.

The result just proved shows that ∂_x induces a derivation on the K-space Z/B of "de Rham cohomology" of L. We show now that it depends only on ∂ and not on the choice of transcendence basis x of L/K.

Lemma 2. *Let* $x = (x_1, \cdots, x_n)$, $y = (y_1, \cdots, y_n)$ *be two transcendence bases of* L/K *and let*

$$\omega = \sum_{i_1 < \ldots < i_r} u_{i_1 \ldots i_r} dx_{i_1} \wedge \ldots \wedge dx_{i_r} \subset Z.$$

Then

$$(\partial_y - \partial_x)\, \omega = d\phi$$

where

$$\varphi = \sum_{i_1 < \ldots < i_r} \sum_{\alpha=1}^{r} (-1)^{\alpha-1} u_{i_1 \ldots i_r} dx_{i_1} \wedge \ldots \wedge \partial_y x_{i_\alpha} \wedge \ldots \wedge \partial x_{i_r}.$$

Proof. This lemma was proved in [9]. For completeness we reproduce the proof for the only case, namely $r = 1$, which is needed below.

On putting

$$\omega = \sum_{i=1}^{n} u_i \, dx_i;$$

and since $d\omega = 0$ we have $\partial^{(i)} u_j = \partial^{(j)} u_i$ for all $1 \leq i, j \leq n$, where $\partial^{(i)}$ is the derivation of L which is trivial on K and satisfies $\partial^{(i)} x_j = \delta_{ij}$ (in other words, partial differentiation with respect to x_i).

On the other hand, $\partial_y - \partial_x$ is a derivation on L which is trivial on K and so is a linear combination of the $\partial^{(j)}$. It is easy to see that

$$\partial_y - \partial_x = \sum_{j=1}^{n} (\partial_y x_j) \, \partial^{(j)}.$$

In fact both sides coincide on K and the x_j, $1 \leq j \leq n$. Hence

$$(\partial_y - \partial_x)\,\omega = \sum_{i=1}^{n} \sum_{j=1}^{n} \partial_y x_j \cdot \partial^{(j)} u_i \, dx_i + \sum_{i=1}^{n} u_i \, d\,(\partial_y x_i)$$

$$= \sum_{j=1}^{n} \partial_y x_j \sum_{i=1}^{n} \partial^{(i)} u_j \, dx_i + \sum_{i=1}^{n} u_i \, d\,(\partial_y x_i)$$

$$= \sum_{j=1}^{n} \partial_y x_j \, du_j + \sum_{i=1}^{n} u_i \, d\,(\partial_y x_i) = d\left(\sum_{i=1}^{n} u_i \, \partial_y x_i\right).$$

This concludes the proof of the lemma.

2. Let V be a model of L/K and V_K the set of points of V defined over K. For any point $P \in V_K$ the symbol o_P will denote the local ring, which we identify with a subring of L. For every $x \in o_P$ the symbol x_P will denote the value of x at P and $m_P \subset o_P$ will be the maximal ideal of o_P.

A set $\mathbf{x} = (x_1, \cdots, x_n)$ of elements of $L = K(V)$ will be called a *system of quasiparameters* at $P \in V_K$ if P is simple, if $x_i \in o_P$, $1 \leq i \leq n$, and if the functions $(x_1 - x_{1P}, \cdots, x_n - x_{nP})$ form a system of parameters of the local ring o_P, i.e.,

$$m_P = \sum_{i=1}^{n} o_P \,(x_i - x_{iP}).$$

Clearly every system of quasiparameters is a transcendence basis of L/K.

Let $\mathbf{x}$ be a fixed transcendence basis, ∂ a derivation of K, and define $\partial^{(i)}$, $\partial_{\mathbf{x}}$ as above.

Lemma 3.[1] (a) *Let* $\mathbf{x}$ *be a system of quasiparameters at the simple point*

1) I am obliged to S. Lang for having found an error in the first version of the proof of this lemma.

$P \in V_K$. *Then* $\partial_x o_P \subset o_P$ *and* $\partial^{(i)} o_P \subset o_P$, $1 \leq i \leq n$.

(b) *Suppose, further, that* $\partial(x_{iP}) = 0$, $1 \leq i \leq n$. *Then* $(\partial_x u)_P = \partial(u_P)$ *for every* $u \in o_P$.

Proof. Put $o = o_P \cap K(x_1, \cdots, x_n)$ so that o consists of functions of the form FG^{-1}, where F, $G \in K[x_1, \cdots, x_n]$, $G(x_{1P}, \cdots, x_{nP}) \neq 0$, and an immediate verification shows that $\partial_x o \subset o$, $\partial^{(i)} o \subset o$.

The ring o_P is a localization of the integral closure $\bar{o}$ of o in L. Hence it is enough to check that $\partial_x \bar{o} \subset o_P$, $\partial^{(i)} \bar{o} \subset o_P$. But $\bar{o}$ is generated as an o-module by a finite number of elements $y_1, \cdots, y_r$. We shall denote by $F_i(X_1, \cdots, X_n, Y)$ irreducible polynomials with coefficients in K for which

$$F_i(x_1, \cdots, x_n, y_i) = 0, \quad 1 \leq i \leq r.$$

The symbol $F_i^{\tilde{\partial}}$ will denote the polynomial which is obtained from F_i by applying to all the coefficients a derivation $\tilde{\partial}$ of L which maps K into itself. Then we have identically ($1 \leq i \leq r$):

$$F_i^{\tilde{\partial}}(x_1, \ldots, x_n, y_i) + \sum_{j=1}^{n} \frac{\partial F_i}{\partial X_j}(x_1, \ldots, x_n, y_i)\,\tilde{\partial} x_j + \frac{\partial F_i}{\partial Y}(x_1, \ldots, x_n, y_i)\,\tilde{\partial} y_i = 0.$$

If $\tilde{\partial} = \partial_x$, we have $\tilde{\partial} x_j = 0$; and if $\tilde{\partial} = \partial^{(i)}$, we have $\tilde{\partial} x_j = \delta_{ij}$: and in both cases we have $\tilde{\partial}(K) \subset K$. Hence there is a $z \in o_P$ such that $z\tilde{\partial} y_i \in o_P$ for all $1 \leq i \leq r$, if when $\tilde{\partial}$ is one of the derivations ∂_x, $\partial^{(i)}$ (for example, we may take z to be $\prod_{i=1}^{r} \partial F_i / \partial Y\,(x_1, \cdots, x_n, y_i)$).

Since $\bar{o} = \sum_{i=1}^{r} o y_i$, the derivation $z\tilde{\partial}$ takes o_P into itself. From the elementary properties of derivations it follows that $(z\tilde{\partial})(m_P^2) \subset m_P$ and so by induction on N that $(z\tilde{\partial})(m_P^N) \subset m_P^{N-1}$ for all $N \geq 1$.

Let $u \in o_P$ be arbitrary and put

$$u \equiv \sum_{i_1 + \ldots + i_n \leq N} u_{i_1 \ldots i_r} (x_1 - x_{1P})^{i_1} \ldots (x_n - x_{nP})^{i_n} \bmod m_P^{N+1}, \qquad u_{i_1 \ldots i_n} \in K.$$

Then

$$z\tilde{\partial} u \equiv z \sum_{i_1 + \ldots + i_n \leq N} \tilde{\partial}\left(u_{i_1 \ldots i_n} (x_1 - x_{1P})^{i_1} \ldots (x_n - x_{nP})^{i_n}\right) \bmod m_P^N.$$

On going to the limit as $N \longrightarrow \infty$ and using the absence of divisors of zero in the completion of o_P we find that z can be cancelled in the last relation. Hence to compute $\tilde{\partial} u$ we may derive term by term the development of u in a formal power series in the parameters $x_i - x_{iP}$. Assertion (a) of the lemma follows almost immediately. Assertion (b) follows from the remark that $\partial(x_{iP}) = 0$ implies

$$\partial_x (x_i - x_{iP}) = 0$$

and so $\partial_x m_P \subset m_P$. This completes the proof of the lemma.

Corollary 1. *Let ω be a 1-dimensional closed differential form regular at the simple point $P \in V_K$ and let the transcendence basis $\mathbf{x}$ be a system of quasiparameters at P. Then the differential form $\partial_x \omega$ is regular at P.*

Proof. Let $\omega = \sum_{i=1}^{n} u_i dx_i$. Then $u_i \in o_P$ and the assertion follows from Lemma 3.

Corollary 2. *Let ω be a 1-dimensional differential form of the second kind on V. Then $\partial_y \omega$ is also of the second kind for any transcendence basis* y.

Proof. We have to check that at every simple point P of the model of L/K there is a decomposition $\partial_y \omega = \omega' + dw$, where the form ω' is regular at P and $\omega \in L$. Let $\omega = \omega'' + du$ be the corresponding decomposition when $\mathbf{x}$ is a system of quasiparameters at P. Then

$$\omega = \partial_x \omega + \{(\partial_y - \partial_x)\,\omega + du\}$$

does what is required by Corollary 1 and Lemma 2.

3. Now let $\{\partial_i\}$ be a family of derivations of K. The elements of the free multiplicative monoid with unit generated by the symbols $\{\partial_i\}$ can be regarded as operators acting on K. These elements have the form $D = \partial_{i_1}^{m_1} \cdots \partial_{i_s}^{m_s}$ and will be called *differential monomials*. The number $m_1 + \cdots + m_s$ is called the *order* of D. The K-linear space U generated by the differential monomials can also be regarded as a space of operators on K. The space U can be given a structure of associative ring. For this it is enough to define the product $D_1(aD_2)$, where D_1, D_2 are differential monomials and $a \in K$. If $D_1 = \partial$ is a derivation we put

$$\partial(aD_2) = (\partial a)\,D_2 + a(\partial D_2);$$

and induction on the order of D_1 shows how the definition is to be extended. The verification of the axioms and of the compatibility with the structure of a space of operators is carried out as usual. The elements of the algebra U will be called differential operators (with respect to the set of derivations $\{\partial_i\}$). We define the order of a differential operator $\mathfrak{Q} \in U$ to be the maximal order of a differential monomial occurring in $\mathfrak{Q}$ with a nonzero coefficient.

For any $\mathfrak{Q} \in U$ and any transcendence basis $\mathbf{x} = (x_1, \cdots, x_n)$ of L/K we denote by $\mathfrak{Q}_x$ the extension of $\mathfrak{Q}$ to the field L and to the L-module Ω obtained by replacing all the ∂_i in $\mathfrak{Q}$ by the derivations ∂_{ix} of L and Ω defined in subsection 1 above. The map $\mathfrak{Q} \longrightarrow \mathfrak{Q}_x$ gives a representation of the ring U in the ring of endomorphisms of the additive groups L and Ω. Further, $\mathfrak{Q}_x$ induces by Lemmas 1 and 2 an operator on the factor space Z/B and this operator is independent of the choice of x. Hence we have defined a representation of U in the additive group Z/B and we shall denote by $\mathfrak{Q}\bar{\omega}$ the class $\mathfrak{Q}_x \omega \bmod B$, where

$\bar{\omega} = \omega \mod B$, $\omega \in Z$, $\mathfrak{Q} \in U$.

Definition. *We define a Picard-Fuchs equation* μ *in the field* L *(relative to a family* $\{\partial_i\}$ *of derivations of* K*) to be any relation of the form*

$$\mu: \sum_{i=1}^{k} \mathfrak{Q}_i \bar{\omega}_i = 0,$$

where $\bar{\omega}_i$ *are the classes of the* 1*-dimensional differential forms of the first kind of* L/K*, and* $\mathfrak{Q}_i \in U$.

4. To every Picard-Fuchs equation μ there corresponds a class of relations in the group Ω of the type

$$\sum_{i=1}^{k} \mathfrak{Q}_{i\mathbf{x}} \omega_i = dz_{\mathbf{x}},$$

where $\mathbf{x}$ runs through all transcendence bases of L/K. We shall call each such relation a *representation* of the Picard-Fuchs equation.

Two Picard-Fuchs equations

$$\sum_{i=1}^{k} \mathfrak{Q}_i \bar{\omega}_t = 0, \quad \sum_{i=1}^{l} \mathfrak{Q}_i' \bar{\omega}_i' = 0$$

will be called *equivalent* if

$$\sum_{i=1}^{k} \mathfrak{Q}_{i\mathbf{x}} \omega_i = \sum_{i=1}^{l} \mathfrak{Q}_{i\mathbf{x}}' \omega_i'$$

for all bases $\mathbf{x} = (x_1, \cdots, x_n)$.

Let $\omega = (\omega_1, \cdots, \omega_g)$ be any basis of the 1-dimensional differential forms of the first kind of L/K. We shall say that a Picard-Fuchs equation is *reduced to the basis* ω if it is a relation between the classes of the forms of the basis, i.e., has the form $\sum_{i=1}^{g} \mathfrak{Q}_i \bar{\omega}_i = 0$. On replacing in any Picard-Fuchs equation the classes of the forms involved by their expressions as linear combinations of $\bar{\omega}_1, \cdots, \bar{\omega}_g$ and combining similar terms we obviously obtain an equivalent equation. For convenience of reference we formulate this result as:

Lemma 4. *Every Picard-Fuchs equation is equivalent to a reduced equation.*

A reduced Picard-Fuchs equation $\sum_{i=1}^{g} \mathfrak{Q}_i \bar{\omega}_i = 0$ can be identified with its set of coefficients $\mu = (\mathfrak{Q}_1, \cdots, \mathfrak{Q}_g) \in U^g$. Thus on the space M of all such equations there is a structure of left U-module and so of K-space. We shall show that if the K-space generated by the derivations $\{\partial_i\}$ is finite-dimensional, then the U-module M has a finite number of generators. (We put this result here only for aesthetic reasons: in what follows we shall need it only in the case of one derivation ∂ and then we shall establish a much more precise property of the module M from which the finite number of generators follows immediately.)

For we may suppose that there is a finite number of derivations $\{\partial_i\}$. Let g be the dimension of the space of 1-dimensional differential forms of the first kind

on L. Then the K-space $\Sigma_{i=1}^{g} U\bar{\omega}_i$ has dimension at most $2g$ since by Lemma 3 Corollary 2 it is spanned by the classes mod B of forms of the second kind. Let $U_i \subset U$ be the space of differential operators of order $\leq i$. There is a j such that

$$\sum_{i=1}^{g} U\,\bar{\omega}_i = \sum_{i=1}^{g} U_j\,\bar{\omega}_i.$$

The Picard-Fuchs equations of the type

$$\sum_{i=1}^{g'} \Omega_i\,\bar{\omega}_i = 0,$$

with $\Omega_i \in U_{j+1}$ clearly form a finite-dimensional space over K. We assert that any base b of this space spans the U-module M. Suppose that it has already been shown that every equation

$$\sum_{m=1}^{g} \Omega_i\bar{\omega}_i = 0, \qquad \Omega_i \in U_k,$$

is a consequence of the equations of b. We shall show that this is true for $\Omega_i \in U_{k+1}$ (the assertion being trivial for $k = j + 1$). First of all, the equation $\Sigma_{i=1}^{g} \Omega_i\bar{\omega}_i = 0$ is a linear combination over K of equations of the type

$$D\bar{\omega}_i + \sum_{m=1}^{g} \Omega_{im}\,\bar{\omega}_m = 0, \qquad \Omega_{im} \in U_j, \tag{4}$$

and elements of b, where D is a monomial of order $k + 1$. Let $D = \partial D'$ where D' is of order k. Then (4) can be put in the form

$$\partial\left(D'\bar{\omega}_i + \sum_{m=1}^{g} \Omega'_{im}\,\bar{\omega}_m\right) + \sum_{m=1}^{g} (\Omega_m - \partial\Omega'_m)\,\bar{\omega}_m = 0, \qquad \Omega'_m \in U_j,$$

where $D'\bar{\omega}_i + \Sigma_{m=1}^{g} \Omega'_{im}\,\bar{\omega}_m = 0$ is an equation of order k. This allows us to use induction.

5. The following technical result will be necessary in what follows.

Let K' be some extension of K linearly disjoint from L and put $L' = K'L$. We suppose that the derivations $\{\partial_i\}$ of K are somehow extensible to derivations of K'. Let U' be the corresponding algebra of differential operators, and M' the module of Picard-Fuchs equations of L'/K' reduced to the basis $\omega = (\omega_1, \cdots, \omega_g)$ of 1-dimensional differential forms of the first kind, which is also a base for L/K. As above, M is the U-module of equations for L/K and we may clearly consider it as naturally embedded in M'.

Lemma 5. *As a linear space over K, M' is generated by its K-subspace M.*

Proof. The result becomes obvious if we consider that the K'-space

$\Sigma_{i=1}^{g} U'\bar{\omega}_i$ is generated by its K-subspace $\Sigma_{i=1}^{g} U\bar{\omega}_i$ and interpret every element $\mu \in M$ (or $\mu' \in M'$) as a *linear* relation with coefficients in K (or in K') between elements of the type $D\bar{\omega}_i \in \Sigma_{i=1}^{g} U\bar{\omega}_i$, where D runs through all differential monomials. This proves the lemma.

Finally, a last remark.

Let L', L'' be independent regular extensions of K, let $\{\partial_i\}$ be a family of derivations of K and let U be the corresponding algebra. We shall consider the Picard-Fuchs equations for $L'L''/K$ reduced relative to a basis ω which is the union of bases ω', ω'' of 1-dimensional differential forms of the first kind for L'/K, L''/K respectively. We shall denote by M', M'', M the corresponding U-modules of Picard-Fuchs equations reduced relative to the respective bases ω', ω'', ω in the respective fields L', L'', $L'L''$. Then the following statement holds: M', M'' can be identified with U-submodules of M and $M = M' + M''$ (direct sum). Besides, the same statement is true for the representatives of the Picard-Fuchs equations taken relative to a transcendence base $\mathbf{x}$ of $L'L''/K$ which is a union of transcendence bases $\mathbf{x}'$, $\mathbf{x}''$ of L'/K, L''/K respectively. More precisely, let

$$\sum_{\omega_i \in \omega} \Omega_{i\mathbf{x}}\, \omega_i = dz$$

be a representative of some $\mu \in M$; Then we have

$$\sum_{\omega_i \in \omega'} \Omega_{i\mathbf{x}'}\, \omega_i = dz', \qquad \sum_{\omega_i \in \omega''} \Omega_{i\mathbf{x}''}\, \omega_i = dz'', \qquad z' \in L', \qquad z'' \in L'',$$

and $dz = dz' + dz''$. (Indeed if $dz = \omega_1 + \omega_2$ where ω_1 (or ω_2) is a 1-dimensional closed differential form of L' (or L''), then ω_1, ω_2 are themselves exact differentials.)

§2. The functions $\mu(P, Q)$

1. Let the transcendence basis $\mathbf{x}$ be a system of quasiparameters at $P \in V_K$. We shall say that this system is *admissible* at P if $\partial(x_{iP}) = 0$ for any derivation ∂ of K and $1 \le i \le n$.

Lemma 6. *Let P, Q, $R \in V_K$ be three simple points. If there is a common system of quasiparameters at P, Q, R, then there is a common system admissible at those points.*

Proof. Let $(x'_1, \cdots, x'_n)$ be a common system of quasiparameters. For each i, $1 \le i \le n$, we can find an x_i which is a fractional linear function of x'_i with coefficients in K, and which is such that the three values x_{iP}, x_{iQ}, x_{iR} lie in the prime subfield of K, and so are annihilated by any derivation. It is easily verified

that $(x_1, \cdots, x_n)$ again form a system of quasiparameters at each of P, Q, R. This completes the proof of the lemma.

We now fix attention on some Picard-Fuchs equation

$$\mu : \sum_{i=1}^{r} \mathfrak{Q}_i \bar{\omega}_i = 0, \quad \mathfrak{Q}_i \in U$$

in L (we sometimes say that μ is a Picard-Fuchs equation on V).

We shall suppose that the set of simple points in V_K is nonempty. Let P, $Q \in V_K$ be two simple points having a common admissible system of quasiparameters $\mathbf{x}$. By Lemma 3, Corollary 1, the differential $dz_{\mathbf{x}}$ defined by the representative

$$\sum_{i=1}^{r} \mathfrak{Q}_{i\mathbf{x}} \omega_i = dz_{\mathbf{x}}$$

of μ is regular at P and Q. Hence the value

$$\mu_{\mathbf{x}}(P, Q) = z_{\mathbf{x}Q} - z_{\mathbf{x}P} \in K \tag{5}$$

is well-defined. For any third point R at which $\mathbf{x}$ is an admissible system of quasiparameters we have the identity

$$\mu_{\mathbf{x}}(P, Q) = \mu_{\mathbf{x}}(P, R) + \mu_{\mathbf{x}}(R, Q). \tag{6}$$

The following important result holds.

Theorem 1. (a) *The value of $\mu_{\mathbf{x}}(P, Q)$ does not depend on the choice of the admissible system $\mathbf{x}$ of quasiparameters but is defined uniquely by μ, P, Q.*

(b) *On the set of all pairs of simple points of V_K there is a unique function $\mu(P, Q)$ with values in K which coincides with $\mu_{\mathbf{x}}(P, Q)$ for points having a common admissible system of quasiparameters $\mathbf{x}$ and satisfying the identity*

$$\mu(P, Q) = \mu(P, R) + \mu(R, Q) \tag{7}$$

throughout its field of definition.

2. The proof of this result is the aim of the following section. The plan of the proof is as follows. First we verify (a) directly. Then we use (7) to *define* a function of pairs of points without a common system of quasiparameters (I did not manage to find out whether such pairs actually exist. If not, the proof is somewhat simplified). For this, we have to choose a point R such that each of the pairs (P, R), (R, Q) has a common system of quasiparameters. To make such a choice possible we may have to extend the field of constants temporarily and so one must study the behavior of $\mu_{\mathbf{x}}(P, Q)$ under such an extension. When the existence and uniqueness of $\mu(P, Q)$ have been proved the verification of (7) presents no difficulty.

§3. Proof of Theorem 1

1. **Lemma 7.** *Let P, Q be simple points of V_K, and let* x, y *be two admissible systems of quasiparameters common to them. Suppose that $\omega \in Z$ is a 1-dimensional differential form of the first kind regular at P and Q and let $\mathfrak{Q}$ be any element of U. Put $(\mathfrak{Q}_y - \mathfrak{Q}_x)\omega = dz$, $z \in L$. Then $z \in o_P \cap o_Q$ and $z_P = z_Q$.*

Proof. The inclusion $z \in o_P \cap o_Q$ follows from Lemma 3, Corollary 1. If Lemma 7 is true for $\mathfrak{Q}'$, $\mathfrak{Q} \in U$, it is true for any linear combination of them over K. Hence we may suppose without loss of generality that $\mathfrak{Q}$ is a differential monomial. The proof is by induction on the order of the monomial.

Suppose that the order is unity, so that we have $\mathfrak{Q} = \partial$, $\omega = \Sigma_{i=1}^{n} u_i\, dx_i$. Then

$$(\partial_y - \partial_x)\,\omega = d\left(\sum_{i=1}^{n} u_i\, \partial_y x_i\right) = dz.$$

The conditions of the lemma imply that $u_i \in o_P \cap o_Q$ and

$$(\partial_y x_i)_P = (\partial_y x_i)_Q = \partial(x_{iP}) = \partial(x_{iQ}) = 0$$

and so $z_P = z_Q$.

Suppose now that the lemma has already been proved for monomials D of order m and consider the monomial ∂D of order $m+1$. We have

$$(\partial_y D_y - \partial_x D_x)\,\omega = \partial_y\,(D_y - D_x)\,\omega + (\partial_y - \partial_x)\,D_x\,\omega = dz.$$

Put

$$(D_y - D_x)\,\omega = dz_1, \qquad (\partial_y - \partial_x)\,\omega = dz_2.$$

By the inductive hypothesis we have $z_{1P} = z_{1Q}$ and $z_{2P} = z_{2Q}$, since $D_x\omega$ is regular at P, Q together with ω. Further

$$(\partial_y z_1)_P = \partial z_{1P} = \partial z_{1Q} = (\partial_y z_1)_Q$$

because y is an admissible system of quasiparameters. Hence $z_P = z_Q$ because $z = \partial_y z_1 + z_2 + c$ with $c \in K$.

This concludes the proof of the lemma.

Corollary. *Assertion* (a) *of Theorem* 1 *is true.*

Proof. For on putting

$$\sum_{i=1}^{r} \mathfrak{Q}_{ix}\,\omega_i = dz_x, \qquad \sum_{i=1}^{r} \mathfrak{Q}_{iy}\,\omega_i = dz_y;$$

we have

$$d\,(z_x - z_y) = \sum_{i=1}^{r} (\mathfrak{Q}_{ix} - \mathfrak{Q}_{iy})\,\omega_i$$

and so, by the lemma,

$$(z_x - z_y)_P = (z_x - z_y)_Q.$$

This equation is equivalent to the identity

$$\mu_{\mathbf{x}}(P, Q) = \mu_{\mathbf{y}}(P, Q).$$

2. Let $\mathbf{x}$ be any transcendence basis of L/K. Then there is a set $V_{\mathbf{x}} \subset V$ open in the Zariski K-topology such that $\mathbf{x}$ is a system of quasiparameters at any point of $V_K \cap V_{\mathbf{x}}$. For we may take for $V_{\mathbf{x}}$ the complement of the carrier of the divisor of the differential form $dx_1 \wedge \cdots \wedge dx_n$.

Let K' be a finite algebraic extension of K and suppose that $P, Q \in V_K \cap V_{\mathbf{x}}$. Let $\mathbf{y}$ be a common system of admissible quasiparameters at P, Q with $y_i \in K'L$. (Such a system exists by Lemma 6.) Let σ be an automorphism of K'/K. We use the same symbol to denote its extension to $K'L/L$. Further, σ acts on the points of $V_{K'}$ in such a way that $z^{\sigma}_{P^{\sigma}} = (z_P)^{\sigma}$ for all $z \in K'L$, $P \in V_{K'}$, for which the right-hand side has a meaning. Finally, σ acts in the obvious way on the differential forms of $K'L/K'$.

Every derivation ∂ of K can be uniquely extended to a derivation of K' and then

$$\partial_{\mathbf{y}^{\sigma}} z^{\sigma} = (\partial_{\mathbf{y}} z)^{\sigma}$$

for any transcendence basis $\mathbf{y}$ of $K'L/K'$ and any $z \in K'L$. To prove this, it is enough to note that the map $z \longrightarrow (\partial_{\mathbf{y}^{\sigma}} z^{\sigma})^{\sigma^{-1}}$ is a derivation and that it coincides with $\partial_{\mathbf{y}}$ on $K(y_1, \cdots, y_n)$.

We now have

Lemma 8. $\mu_{\mathbf{y}}(P, Q)^{\sigma} = \mu_{\mathbf{y}^{\sigma}}(P^{\sigma}, Q^{\sigma})$.

Proof. For if $\mathbf{y}$ is an admissible system of quasiparameters at P, Q then $\mathbf{y}^{\sigma}$ is a similar system at P^{σ}, Q^{σ}. Hence

$$\mu_{\mathbf{y}^{\sigma}}(P^{\sigma}, Q^{\sigma}) = (z_{\mathbf{y}^{\sigma}})_{Q^{\sigma}} - (z_{\mathbf{y}^{\sigma}})_{P^{\sigma}} = (z^{\sigma}_{\mathbf{y}})_{Q^{\sigma}} - (z^{\sigma}_{\mathbf{y}})_{P^{\sigma}} = \mu_{\mathbf{y}}(P, Q)^{\sigma}.$$

This completes the proof of the lemma.

3: We now go over to the proof of (b) of Theorem 1. Lemma 6, formula (6) and (a) of Theorem 1 together imply the existence and uniqueness of $\mu(P, Q)$ on the set of pairs P, Q of simple points in $V_K \cap V_{\mathbf{x}}$, where $\mathbf{x}$ is any transcendence basis of L/K. Suppose now that $P \in V_{\mathbf{x}}$ and $Q \in V_{\mathbf{y}} \setminus V_{\mathbf{x}}$. As stated above, we define $\mu(P, Q)$ by

$$\mu(P, Q) = \mu_{\mathbf{x}'}(P, R') + \mu_{\mathbf{y}'}(R', Q), \tag{8}$$

where R' is any point of $V_{\mathbf{x}} \cap V_{\mathbf{y}}$ defined over some finite normal extension K'/K and $\mathbf{x}', \mathbf{y}'$ are systems of quasiparameters admissible respectively for the pairs (P, R') and (R', Q). (They exist by Lemma 6.)

We must show that if the systems $\mathbf{x}''$, $\mathbf{y}''$ and the point R'' satisfy similar

conditions, then they give the same value of $\mu(P, Q)$.

First of all we may replace R' by any other point $R \in V_{x'} \cap V_{y'}$ since

$$\mu_{x'}(P, R') + \mu_{x'}(R', R) = \mu_{x'}(P, R),$$
$$\mu_{y'}(R, R') + \mu_{y'}(R', Q) = \mu_{y'}(R, Q)$$

and

$$\mu_{x'}(R', R) = -\mu_{y'}(R, R')$$

by (a) of Theorem 1. Hence we may suppose that

$$R' = R'' = R \in V_{x'} \cap V_{y'} \cap V_x \cap V_y,$$

when the equation

$$\mu_{x'}(P, R) + \mu_{y'}(R, Q) = \mu_{x''}(P, R) + \mu_{y''}(R, Q)$$

follows immediately from (a). Hence our function is well defined and we may omit the suffix indicating the system of quasiparameters used in computing $\mu(P, Q)$.

We shall show now that $\mu(P, Q) \in K$. For suppose that R is defined over the normal extension K' of K and let σ be a relative automorphism. Then Lemma 8, part (a) of Theorem 1 and the independence of the choice of R together imply that

$$\mu(P, Q)^\sigma = \mu(P, R^\sigma) + \mu(R^\sigma, Q) = \mu(P, Q).$$

Finally, we may verify the identity (7) by using an auxiliary point

$$S \in V_x \cap V_y \cap V_z$$

where x, y, z are admissible systems of quasiparameters at P, Q, R respectively. The argument is similar to the one above and is left to the reader.

This completes the proof of Theorem 1.

§4. Some properties of $\mu(P, Q)$

Let V' be an algebraic variety over K of the same dimension as V with field of functions L' and let $\phi: V' \longrightarrow V$ be an epimorphism. We identify L with a subfield of L'. Then every Picard-Fuchs equation μ in L gives a Picard-Fuchs equation $\phi^*\mu$ in L'.

Let $P, Q \in V'_K$ be simple points and let their images $\phi(P)$, $\phi(Q)$ be simple in V_K. Then we have

Lemma 9. $\phi^*\mu(P, Q) = \mu(\phi(P), \phi(Q))$.

Proof. We may suppose that the points $\phi(P)$, $\phi(Q)$ have a common system x of admissible quasiparameters and similarly that there is a system y for P, Q, since the general case is obtained from this one by the use of intermediate points.

As in the proof of (a) of Theorem 1 it is enough to check the following

analogue of Lemma 7. Suppose that $\omega \in Z$ is a form on V regular at P, Q, that $\mathfrak{Q}$ is any element of U and that $dz = (\mathfrak{Q}_y - \mathfrak{Q}_x)\omega$. Then $z \in o_P \cap o_Q$ and $z_P = z_Q$. The verification of this is a word-for-word repetition of the proof of Lemma 7.

This concludes the proof of the lemma.

Lemma 10. *Let V_1, V_2 be two algebraic varieties over K, let $V = V_1 \times V_2$ and let μ be a Picard-Fuchs equation on V. Then there are Picard-Fuchs equations μ_1, μ_2 on V_1, V_2 respectively such that*

$$\mu(P, Q) = \mu_1(P_1, Q_1) + \mu_2(P_2, Q_2)$$

for every pair of points $P = (P_1, P_2) \in V_K$, $Q = (Q_1, Q_2) \in V_K$ for which μ is defined.

(This is a translation into geometric language of the remark made at the end of subsection 3 of the previous section.)

Finally, our last result is a slightly disguised version of the obvious fact that the application of our construction to the zero derivation gives the zero function μ.

Lemma 11. *In the notation of subsection 1 of §2 we suppose that V is defined over some subfield $k \subset K$ on which the differential algebra U acts trivially. Then for every Picard-Fuchs equation μ on V and for any simple points P, $Q \in V$ defined over k we have $\mu(P, Q) = 0$.*

Proof. If the Picard-Fuchs equations μ_1, μ_2 are equivalent in the sense of subsection 4 of §1, then

$$\mu_1(P, Q) \equiv \mu_2(P, Q).$$

Hence it is enough by Lemma 4 to prove the lemma for equations reduced with respect to some basis of the forms of the first kind. We choose a basis which is defined over k. Then the representative of any Picard-Fuchs equation with respect to a transcendence basis x of the function field of V defined over k has the shape

$$\sum_{i=1}^{g} \mathfrak{Q}_{ix}\omega_i = 0.$$

The assertion of the lemma now follows almost immediately.

§5. Additive functions on abelian varieties.

The kernel theorem

1. From now until the end of this chapter L will denote the field of rational functions on an abelian variety A defined over K. We fix attention on some Picard-Fuchs equation μ on A and consider the corresponding function $\mu(P, Q)$ on $A_K \times A_K$.

Lemma 12. $\mu(P + R, Q + R) = \mu(P, Q)$ *for any* $P, Q, R \in A_K$ *(the addition of points being understood in the sense of the group law on* A*).*

Proof. We may suppose that P, Q have a common system $\mathbf{x}$ of admissible parameters. Let $\sigma = \sigma_R : L \longrightarrow L$ be the automorphism of L/K defined by $(u^\sigma)_P = u_{P-R}$ for any points P, Q and function u regular at $P - R$. As in subsection 2 of §4 we have

$$\partial_{\mathbf{x}^\sigma} u^\sigma = (\partial_{\mathbf{x}} u)^\sigma$$

and

$$\partial_{\mathbf{x}^\sigma} \omega^\sigma = (\partial_{\mathbf{x}} \omega)^\sigma$$

for any differential form ω on A. Since differential forms of the first kind are invariant with respect to translations on A, on applying σ to the representative

$$\sum_{i=1}^{k} \Omega_{i\mathbf{x}}\, \omega_i = dz$$

of μ we obtain

$$\sum_{i=1}^{k} \Omega_{i\mathbf{x}^\sigma}\, \omega_i = dz^\sigma.$$

The functions $(x_1^\sigma, \ldots, x_n^\sigma)$ are a system of admissible quasiparameters at the points $P + R, Q + R$. Hence

$$\mu(P + R, Q + R) = z^\sigma_{Q+R} - z^\sigma_{P+R} = z_Q - z_P = \mu(P, Q).$$

This proves the lemma.

In what follows we shall adopt the following notation for brevity: we shall put

$$\mu(P) = \mu(O, P)$$

for a Picard-Fuchs equation μ and $P \in A_K$, where $O \in A_K$ is the zero of the group law.

Proposition 1. $\mu(P + Q) = \mu(P) + \mu(Q)$.

Proof. By (7) and Lemma 12 we have

$$\mu(O, P + Q) = \mu(O, P) + \mu(P, P + Q) = \mu(O, P) + \mu(O, Q),$$

which is what was required.

Our fundamental aim to the end of this chapter is the description of the intersection A_K^0 of the kernels of all the homomorphisms corresponding to all the Picard-Fuchs equations (for a fixed set of derivations $\{\partial_i\}$ generating U).

The following results are easily obtained by combining the known properties of $\mu(P, Q)$.

Lemma 13. (a) *Let* $K' \supset K$ *be any extension of* K *which is linearly free with*

respect to L. Let the derivations $\{\partial_i\}$ of K which generate U be extended to K'. Then $A_K^0 = A_{K'}^0 \cap A_K$.

(b) *Let $\phi : A \longrightarrow B$ be an isogeny defined over K. Then*

$$A_K^0 = \varphi^{-1}(B_K^0), \qquad B_K^0 = \varphi(A_{\bar{K}}^0) \cap B_K,$$

where $\bar{K}$ is the algebraic closure of K.

(c) *Let $A = B \times C$. Then $A_K^0 = B_K^0 \times C_K^0$.*

Proof. Assertion (a) follows from Lemma 5 and the fact that the map $\mu \longrightarrow \mu(P)$ of the U' module of Picard-Fuchs equations into the U' module of functions $A_{K'} \longrightarrow K'$ is a module homomorphism, and so, in particular, is K'-linear.

Assertion (b) follows from Lemma 9, from (a) and from the fact that an isogeny of abelian varieties induces an isomorphism of the spaces of differential forms of the first kind compatible with the action of U.

The assertion (c) follows directly from Lemma 10. This proves the lemma. It implies

Proposition 2. *Suppose that U acts trivially on some subfield $k \subset K$. Let (B, τ) denote the K/k-trace of A. Suppose that for a $P \in A_K$ there is an integer $d \neq 0$ such that $dP \in \tau(B_k)$. Then $P \in A_K^0$.*

Proof. Let $(\tau, \phi) : B \times C \longrightarrow A$ be an isogeny defined over the algebraic closure $\bar{K}$ of K. By Lemma 13 we have

$$A_K^0 = (\tau, \varphi)(B_{\bar{K}}^0 \times C_{\bar{K}}^0) \cap A_K$$

and so $B_k^0 \subset B_{\bar{K}}^0$ by Lemma 11, since B is defined over k. Hence $\tau(B_k) \subset A_K^0$; and if $dP \in A_K^0$, then $P \in A_K^0$, since the additive group of a field of zero characteristic is torsion-free. This proves the proposition.

Considerably more difficult to prove is the converse of this assertion, which we shall refer to below as the "kernel theorem".

Theorem 2. *Let K be a regular extension of its subfield k and let the algebra U contain all the derivations of the field K that are trivial on k. Then the group $A_K^0 = A_{K/k}^0$ consists of those points $P \in A_K$ for which there exists an integer $d \neq 0$ such that $dP \in \tau(B_k)$.*

2. We shall show now that it is enough to prove the kernel theorem in the case when K is the field of rational functions on an algebraic curve with the complex field as constant field. This case presents fundamental difficulties requiring topologico-algebraic tools and will be treated in the next section.

In the proof of the following reduction theorem we shall, without special

reference to them, make use of properties of the K/k-trace established in Lang's book [3].

Proposition 3. *If Theorem 2 is true when K is the field of rational functions on an algebraic curve with the complex field as constant field, then it is universally true.*

Proof. Let the hypothesis of the proposition be satisfied.

(a) Theorem 2 is true if k is finitely generated over its prime subfield and the transcendence degree $\dim_k K$ is unity.

For then we may regard k as a subfield of the complex field C. We can extend the action of U to the compositum $K' = KC$ by making it act trivially on $C \subset K'$. Let (B', τ') be the K'/C-trace of A. If $P \in A^0_{K/k}$, then $P \in A^0_{K'/C}$ and so by hypothesis $dP \in \tau'(B'_C)$. But $\tau'(B'_C) \cap A_K = \tau(B_k)$ and the required result follows.

(b) Theorem 2 is true if k is finitely generated over its prime subfield and K/k is any regular extension.

We proceed by induction on the transcendence degree m of K/k, the case $m = 1$ being already proved. Suppose that the assertion is true for dimension m and let K/k have dimension $m + 1$. Consider a subfield K', $k \subset K' \subset K$, which is algebraically closed in K and such that $\dim_{K'} K = 1$. Let (B', τ') be the K/K'-trace of A and (B'', τ'') the K'/k-trace of B'. If $P \in A^0_{K/k}$, then P is annihilated by all homomorphisms μ obtained from Picard-Fuchs equations relating to derivations which are trivial on K' and so $P \in A^0_{K/K'}$. By part (a) of the proof we have $dP \in \tau'(B'_{K'})$. Let $dP = \tau'(P')$, so that by Lemma 13 we have $P' \in (B')^0_{K'/k}$, and thus, by the hypothesis of the induction, $d'P' \in \tau''(B''_k)$. Hence $d'dP \in \tau(B_k)$, which is what we had to show.

(c) Theorem 2 is true in general. For there exists a field $K_0 \subset K$ finitely generated over its prime subfield which is a field of definition of A and satisfies $K = kK_0$. From Lemma 13 it follows without difficulty that $A^0_{K/k}$ is the union of all $A^0_{K'/K' \cap k}$ when K' runs through all subfields of finite type of K containing K_0. The required result now follows from (b) above and the transitivity of the trace.

§6. Proof of the kernel theorem

1. In this section k is the field of complex functions and K is the field of meromorphic functions on the Riemann surface Γ of a complete nonsingular algebraic curve. Further, A is an abelian variety defined over K and L the field of functions on A defined over K. We shall prove Theorem 2 for A.

It is convenient to regard A as an algebraic family of abelian varieties parametrized by Γ. More precisely, we take a complete model $\mathfrak{A}$ of the field L/k such

that its canonical projection $p: \mathfrak{A} \longrightarrow \Gamma$ induced by the inclusion $K \subset L$ has the two following properties:

(1) There is a finite number of points $a_1, \cdots, a_s \in \Gamma$ such that for any point $a \in \Gamma \setminus \bigcup_{i=1}^{s} a_i$ the fiber $A_a = p^{-1}(a)$ is an abelian variety with a group law induced by that on A.

(2) On the set $\mathfrak{A} \setminus \bigcup_{i=1}^{s} p^{-1}(a_i)$ the projection p onto $\Gamma \setminus \bigcup_{i=1}^{s} a_i$ induces a structure of topological fiber space.

We shall suppose the model $\mathfrak{A}$ chosen once and for all. Let $\Gamma_0 = \Gamma \setminus \bigcup_{i=1}^{s} a_i$, and denote by $\tilde{\Gamma}$ the universal covering of Γ_0 with the induced complex-analytic structure. We denote the field of meromorphic functions on $\tilde{\Gamma}$ by $\tilde{K}$. The natural projection $\tilde{\Gamma} \longrightarrow \Gamma$ induces an embedding $K \subset \tilde{K}$. Every derivation ∂ of K/k extends canonically to a derivation of $\tilde{K}$ which we shall denote by the same symbol ∂.

We shall fix once and for all a point $a \in \Gamma_0$ and denote by $\pi_1(\Gamma_0)$ the fundamental group of Γ_0 relative to a. Instead of $\mathfrak{A}$ we shall consider its restriction $\mathfrak{A}_0$ to Γ_0; that is, we take out the singular fibers. Since the projection $p: \mathfrak{A}_0 \longrightarrow \Gamma_0$ is topologically a fiber bundle, we have the following:

(a) Every point $\tilde{b} \in \tilde{\Gamma}$ can be regarded as a homotopy class β of paths on Γ_0 with beginning at a and end $b = p(\tilde{b})$. Hence a point $\tilde{b}$ determines a homomorphism by "carrying a homology class along β":

$$\tilde{b}: H_1(A_a, \mathbf{Z}) \longrightarrow H_1(A_b, \mathbf{Z}).$$

We shall denote the image of a $\gamma \in H_1(A_a, \mathbf{Z})$ under $\tilde{b}$ by $\gamma\tilde{b}$.

(b) Let $\sigma \in \pi_1(\Gamma_0)$. The map $\beta \longrightarrow \sigma^{-1}\beta$, which makes correspond to every class of paths β on Γ_0 with beginning at a the class $\sigma^{-1}\beta$ of paths with the same beginning and end, defines an action of $\pi_1(\Gamma_0)$ on $\tilde{\Gamma}$. If β corresponds to the point $\tilde{b}$, then by definition the class $\sigma^{-1}\beta$ corresponds to the point $\sigma^{-1}\tilde{b}$.

On the other hand, let $\tilde{s} \in \tilde{\Gamma}$ be a point corresponding to the class $\sigma^{-1} \in \pi_1(\Gamma_0)$ of paths. By (a) above to every $\gamma \in H_1(A_a, \mathbf{Z})$ there corresponds a $\gamma\tilde{s} \in H_1(A_a, \mathbf{Z})$. It easily follows from the definitions that

$$(\gamma\tilde{s})\tilde{b} = \gamma(\sigma^{-1}\tilde{b}).$$

(c) Let $f \in \tilde{K}$ and $\sigma \in \pi_1(\Gamma_0)$. We define an automorphism $f \longrightarrow f^{\sigma}$ of $\tilde{K}$ by putting $f^{\sigma}(\tilde{b}) = f(\sigma^{-1}\tilde{b})$.

(d) Let $\gamma \in H_1(A_a, \mathbf{Z})$ and let ω be a closed 1-dimensional differential form of L/K. For almost all fibers A_b, $b \in \Gamma_0$ the form ω induces a closed 1-dimensional form ω_b which is invariant if ω is invariant; of the second kind if ω is of the second kind; and exact if ω is exact.

We shall denote by $\int_{\gamma}\omega$ the element of $\tilde{K}$ defined by

$$\left(\int_{\gamma}\omega\right)(\tilde{b}) = \int_{\gamma\tilde{b}} \omega_b,$$

where the right-hand side is the period of the form ω_b on the homology class $\gamma\tilde{b}$ in the fiber A_b. The element σ of $\pi_1(\Gamma_0)$ acts on $\int_\gamma\omega$ as follows:

$$\left(\int_{\gamma}\omega\right)^{\sigma} = \int_{\gamma\tilde{s}} \omega,$$

where $\tilde{s}$, as above, is the point of $\tilde{\Gamma}$ corresponding to σ^{-1}. In fact

$$\left(\int_{\gamma}\omega\right)^{\sigma}(\tilde{b}) = \left(\int_{\gamma}\omega\right)(\sigma^{-1}\tilde{b}) = \int_{\gamma(\sigma^{-1}\tilde{b})}\omega_b = \int_{(\gamma\tilde{s})\tilde{b}}\omega_b = \left(\int_{\gamma\tilde{s}}\omega\right)(\tilde{b}).$$

(e) Let K' be a finite normal extension of K unramified outside $a_1, \cdots, a_s$ and let Γ' be its Riemann surface with the inverse images of those points removed. We shall regard Γ' as an intermediate covering $\tilde{\Gamma} \longrightarrow \Gamma' \longrightarrow \Gamma_0$ corresponding to a normal divisor of finite index $\pi_1(\Gamma') \subset \pi_1(\Gamma_0)$. The field K' is contained in $\tilde{K}$ and consists precisely of those elements which are σ-invariant for all $\sigma \in \pi_1(\Gamma')$. The points $b' \in \Gamma'$ may be identified with classes $\pi_1(\Gamma')\beta$, where β runs through the homotopy classes of paths on Γ_0 starting at a.

The points $P \in A_{K'}$ are in 1-1 correspondence with the analytic Γ_0-morphisms $P : \Gamma' \longrightarrow \mathfrak{A}_0$. If $b' \in \Gamma'$ we shall denote by $P_{b'} \in A_b$, where b is the projection of b' on Γ_0, the image of b' under P. In particular, the zero O of the group $A_{K'}$, being already determined over K, satisfies the equations $O_{b'} = O_b$ (in the earlier notation).

Let $P \in A_{K'}$ and let $a' \in \Gamma'$ be a point corresponding to a class of paths in $\pi_1(\Gamma')$ (so it lies over $a \in \Gamma_0$). Denote by $\delta_P \subset A_a$ the homology class in $A_a \setminus \{O_a \cup P_{a'}\}$ of a path in A_a with origin O_a and endpoint $P_{a'}$. For any $\tilde{b} \in \tilde{\Gamma}$ we shall denote by $\delta_P\tilde{b}$ the homology class in $A_b \setminus \{O_b \cup P_{b'}\}$ with origin O_b and endpoint $P_{b'}$, where b' corresponds to $\pi_1(\Gamma')\beta$, of the path obtained from a path of δ_P by transport along β in such a way that the origin and end in each fiber A_c are correspondingly O_c and $P_{c'}$.

As above, we denote by $\int_{\delta_P}\omega$ the element of $\tilde{K}$ defined by

$$\left(\int_{\delta_P}\omega\right)(\tilde{b}) = \int_{\delta_P b} \omega_b$$

(in the same notation as in (d) above). Similarly, for every $\sigma \in \pi_1(\Gamma_0)$ we have

$$\left(\int_{\delta_P}\omega\right)^{\sigma} = \int_{\delta_P\tilde{s}} \omega.$$

The path $\delta_P\tilde{s}$ lies in A_a, has its origin at O_a and endpoint at $P_{a''}$, where a'' corresponds to $\pi_1(\Gamma')\sigma^{-1}$. It is easy to see that the path $\delta_P\tilde{s}$ may be interpreted

as δ_{P^σ}, where P^σ is the point conjugate to P under the action of σ in the field K'. Hence, if we allow for the indeterminacy in the choice of the path δ_Q given Q and do not intend to give a firm prescription for the choice, we at last obtain

$$\left(\int_{\delta_P} \omega\right)^\sigma = \int_{\delta_{P^\sigma}} \omega + \int_\gamma \omega, \quad \gamma = \gamma(\sigma) \in H_1(A_a, \mathbf{Z}).$$

(f) Finally we note the following facts. Let $P, Q \in A_K$, and suppose there is a $\gamma \in H_1(A_a, \mathbf{Z})$ such that

$$\int_{\delta_P} \omega = \int_{\delta_Q} \omega + \int_\gamma \omega$$

for any 1-dimensional form ω of the first kind for L/K. Then $P = Q$ (Abel's theorem).

Let $\int_\gamma \omega = 0$ for a given form ω and all $\gamma \in H_1(A_a, \mathbf{Z})$. Then ω is exact (the converse is also true).

Let ∂ be a derivation of $\tilde{K}$ which induces a derivation of K into itself. Then

$$\partial \int_\gamma \omega = \int_\gamma \partial_{\mathbf{x}} \omega$$

for any choice of transcendence basis $\mathbf{x} = (x_1, \cdots, x_n)$ of L/K provided that ω is of the second kind.

If, further, $\mathbf{x}$ is a system of quasiparameters at O and P and $\partial(x_{iO}) = \partial(x_{iP}) = 0$, $1 \le i \le n$ (the limits of integration are independent of the parameters) then also

$$\partial \int_{\delta_P} \omega = \int_{\delta_P} \partial_{\mathbf{x}} \omega$$

provided that ω is a form of the second kind regular at O and P. In particular for every equation $\mu : \Sigma_{i=1}^n \Omega_i \bar{\omega}_i = 0$ we have

$$\mu(P) = \sum_{i=1}^n \Omega_i \int_{\delta_P} \omega_i.$$

Finally, we have the usual linearity properties

$$\int_{\gamma_1+\gamma_2} \omega = \int_{\gamma_1} \omega + \int_{\gamma_2} \omega; \qquad \int_\gamma (\alpha\omega_1 + \beta\omega_2) = \alpha \int_\gamma \omega_1 + \beta \int_\gamma \omega_2, \quad \alpha, \beta \in \tilde{K},$$

and similarly for $\int_{\delta_P} \omega$.

2. After these preparatory remarks we proceed to the proof of the kernel theorem.

We shall fix some nontrivial derivation ∂ of K/k, so that U consists of differential operators of the type $\Sigma_{i=0}^m a_i \partial^i$, $a_i \in K$. Let $(\omega_1, \cdots, \omega_n)$ be a fixed

basis of the space of invariant differential forms of L/K, where $n = \dim A$. As in subsection 3 of §2 we denote by M the left U-module of Picard-Fuchs equations on A reduced to the basis $(\omega_1, \cdots, \omega_n)$. Let $\mu \in M$ have the form

$$\mu : \sum_{i=1}^{n} \Omega_i \bar{\omega}_i = 0,$$

and let $P \in A_k$. The condition $\mu(P) = 0$ is equivalent to

$$\sum_{i=1}^{n} \Omega_i \int_{\delta_P} \omega_i = 0.$$

Let us denote by X the linear space over the complex field of vectors $(\xi_1, \cdots, \xi_n)$, $\xi_i \in \tilde{K}$ such that

$$\sum_{i=1}^{n} \Omega_i \xi_i = 0$$

for any Picard-Fuchs equation $\mu \in M$. The space X contains the subspace X_0 spanned by vectors $(\int_\gamma \omega_1, \cdots, \int_\gamma \omega_n)$, $\gamma \in H_1(A_a, \mathbf{Z})$, since

$$\sum_{i=1}^{n} \Omega_i \int_\gamma \omega_i = \sum_{i=1}^{n} \int_\gamma \Omega_{ix} \omega_i = \int_\gamma dz = 0.$$

A fundamental role in the proof of the kernel theorem is played by

Proposition 4. $X = X_0$.

Before proving this we show how to deduce the kernel theorem from it. Let $\gamma = (\gamma_1, \cdots, \gamma_{2n})$ be a fixed basis for $H_1(A, \mathbf{Z})$. Proposition 4 implies that for every $P \in A^0_{K/k}$ and path δ_P there exists a complex column-vector

$$\mathbf{c} = \begin{pmatrix} c_1 \\ \cdot \\ \cdot \\ \cdot \\ c_{2n} \end{pmatrix}$$

such that

$$\int_{\delta_P} \omega = \sum_{i=1}^{2n} c_i \int_{\gamma_i} \omega = \left(\int_\gamma \omega\right) \mathbf{c}, \qquad \left(\int_\gamma \omega\right) = \left(\int_{\gamma_1} \omega, \ldots, \int_{\gamma_{2n}} \omega\right). \tag{9}$$

The representation (9) is, in general, not unique. Hence we replace it by one of the form

$$\int_{\delta_P} \omega = \sum_{i=1}^{2n} r_i \int_{\gamma_i} \omega = \left(\int_\gamma \omega\right) \mathbf{r}, \quad \mathbf{r} = \begin{pmatrix} r_1 \\ \cdot \\ \cdot \\ \cdot \\ r_{2n} \end{pmatrix}, \tag{10}$$

where the r_i are the *real* functions on $\widetilde{\Gamma}$ uniquely determined by

$$\sum_{i=1}^{2n} r_i \int_{\gamma_i} \omega_j = \sum_{i=1}^{2n} c_i \int_{\gamma_i} \omega_j \qquad (j = 1, \ldots, n).$$

$$\sum_{i=1}^{2n} r_i \overline{\int_{\gamma_i} \omega_j} = \sum_{i=1}^{2n} \bar{c}_i \overline{\int_{\gamma_i} \omega_j}$$

(the bar denoting the complex conjugate). Hence the map

$$(c_1, \cdots, c_{2n}) \longrightarrow (r_1(b), \cdots, r_{2n}(b)),$$

for any point $b \in \widetilde{\Gamma}$, is a linear map of linear spaces over the reals.

We shall apply $\sigma \in \pi_1(\Gamma_0)$ to the equation (9). Let

$$(\gamma_1\sigma^{-1}, \ldots, \gamma_{2n}\sigma^{-1}) = (\gamma_1, \ldots, \gamma_{2n})\, B_\sigma,$$

where B_σ is a real matrix of order $2n$. Then, since $P^\sigma = P$, we have

$$\Big(\int_{\delta_P} \omega\Big)^\sigma = \int_{\delta_P} \omega + \int_{\gamma(\sigma)} \omega, \quad \gamma(\sigma) \in H_1(A_a, \mathbf{Z}).$$

On the other hand, the right-hand side transforms to

$$\Big(\int_{\gamma} \omega\Big) B_\sigma \mathbf{c} = \Big(\int_{\gamma} \omega\Big) B_\sigma \mathbf{r},$$

if we take into account the linearity of the map $\mathbf{c} \longrightarrow \mathbf{r}$ and the uniqueness of the representation (10). Consequently, by computing $(\int_{\delta_P} \omega)^\sigma - \int_{\delta_P} \omega$ two ways we obtain

$$\int_{\gamma(\sigma)} \omega = \Big(\int_{\gamma} \omega\Big)(B_\sigma - E)\, \mathbf{r},$$

where E is the unit matrix. If

$$\gamma(\sigma) = (\gamma_1, \ldots, \gamma_{2n}) \begin{pmatrix} k_1(\sigma) \\ \cdot \\ \cdot \\ \cdot \\ k_{2n}(\sigma) \end{pmatrix}$$

and $\mathbf{k}(\sigma)$ denotes the last column, we obtain the following system of equations for the vector-function $\mathbf{r}$:

$$(B_\sigma - E)\, \mathbf{r} = \mathbf{k}(\sigma). \qquad \sigma \in \pi_1(\Gamma_0).$$

Let

$$\mathbf{r}^0 = \begin{pmatrix} r_1^0 \\ \cdot \\ \cdot \\ \cdot \\ r_n^0 \end{pmatrix}$$

be one rational solution of this system (i.e., the r_i^0 are rational numbers), which certainly exists since the system is solvable and has integral coefficients. On putting $\mathbf{r} = \mathbf{r}^0 + \mathbf{r}^1$ we obtain the real vector-function $\mathbf{r}^1$ which satisfies the homogeneous system

$$(B_\sigma - E)\mathbf{r}^1 = 0, \quad \sigma \in \pi_1(\Gamma_0).$$

Let $d \neq 0$ be a common divisor of the coordinates of $\mathbf{r}^0$ and consider the point $dP \in A^0_{K/k}$ and some path $\delta_{dP} \subset A_a$. Then

$$\int_{\delta_{dP}} \omega = d \int_{\delta_P} \omega + \int_{\gamma'} \omega = \int_{\gamma''} \omega + \left(\int_\gamma \omega\right) d\mathbf{r}^1,$$

where $\gamma'' = \gamma' + \gamma d\mathbf{r}^0 \in H_1(A_a, \mathbf{Z})$. We shall show that the point dP is infinitely divisible in A_K. For certainly for any integer $m \neq 0$ there is a finite normal extension K' of K unramified outside $a_1, \cdots, a_s \in \Gamma$ such that dP can be divided by m in $A_{K'}$:

$$dP = mQ, \qquad Q \in A_{K'}.$$

We may even suppose that all solutions of this equation are defined over K'. We shall show that one of them is defined over K. Let us take that one of the solutions for which there is a path $\delta_Q \subset A_a$ such that

$$\int_{\delta_Q} \omega = m^{-1}\left(\int_\gamma \omega\right) d\mathbf{r}^1.$$

On applying $\sigma \in \pi_1(\Gamma_0)$ to both sides and using the fact that $B_\sigma \mathbf{r}^1 = \mathbf{r}^1$ we obtain

$$\int_{\delta_{Q^\sigma}} \omega = \int_{\delta_Q} \omega + \int_{\gamma'(\sigma)} \omega, \quad \gamma'(\sigma) \in H_1(A_a, \mathbf{Z}).$$

By Abel's theorem this means that $Q^\sigma = Q$ for all σ. Hence $Q \in A_K$.

The above proof also shows that for any $P \in A^0_{K/k}$ there is an integer $d \neq 0$ such that dP is infinitely divisible in A_K. By the functional variant of the Mordell-Weil theorem it follows that $dP \in \tau(B_k)$ where (B, τ) is the K/k-trace of A. (The idea of using the infinite divisibility was suggested to me by I. R. Šafarevič. I could not directly prove the inclusion $dP \in \tau(B_k)$ without recourse to a strong theorem like the Mordell-Weil.)

This completes the proof of finiteness.

3. It remains to prove Proposition 4. To this end we shall describe a special system of generators of the U-module M which will be convenient for computing the complex dimension of X.

We shall put

$$\Omega_j = \sum_{i=1}^{n} U_j \bar{\omega}_i,$$

where $U_j \subset U$ is the space of operators of order $\leq j$, and

$$\Omega = \bigcup_{j=0}^{\infty} \Omega_j = \Omega_t,$$

where $t < \infty$ since the dimension of Ω does not exceed $2n$ and $\Omega_j \subset \Omega_{j+1}$. We shall suppose that t is taken as small as possible.

By the "Leibnitz formula" the map $\partial^i : \Omega_0 \to \Omega$ induces a K-linear map $\partial(i) : \Omega_0 \to \Omega/\Omega_{i-1}$. Put

$$\Omega^{(i)} = \operatorname{Ker} \partial\,(i) \subset \Omega_0.$$

Setting $\Omega_{-1} = \{0\}$, we have the increasing sequence of subspaces

$$\{0\} = \Omega^{(0)} \subset \Omega^{(1)} \subset \Omega^{(2)} \subset \ldots \subset \Omega^{(t)} \subset \Omega^{(t+1)} = \Omega_0.$$

On putting $r_i = \dim \Omega_0/\Omega^{(i)} = \dim \Omega_i/\Omega_{i-1}$ we clearly have

$$n = r_0 \geqslant r_1 \geqslant \ldots \geqslant r_t > r_{t+1} = 0.$$

We shall prove Proposition 4 for some special basis of Ω_0 which is enough for Theorem 2, although it is not difficult to see that it implies the corresponding result for any basis.

We choose the numbering of the forms $\omega_1, \cdots, \omega_n$ of the first kind, so that the classes $\bar{\omega}_n, \cdots, \bar{\omega}_{r_i+1}$ generate $\Omega^{(i)}$ for $i = 1, \cdots, t+1$. By the definition of the $\Omega^{(i)}$ we have equations of the form:

$$\mu_{ij} : \partial^i \bar{\omega}_j + \sum_{k=1}^{n} \Omega_{ijk} \bar{\omega}_k = 0, \quad \bar{\omega}_j \in \Omega^{(i)} \setminus \Omega^{(i-1)}, \quad \Omega_{ijk} \in U_{i-1}, \qquad (11)$$

where $i = 1, \cdots, t+1$ and for each value of i there are $r_i - r_{i-1}$ equations of order i corresponding to the j with $r_{i-1} \geq j \geq r_i + 1$.

Lemma 14. *The equations μ_{ij} span the U-module of Picard-Fuchs equations reduced to the basis $\omega_1, \cdots, \omega_n$.*

Proof. We first suppose that there is an equation of the type

$$\sum_{k=1}^{n} \Omega_k \bar{\omega}_k = 0, \quad \Omega_k \in U_{i_k - 1},$$

where the integers i_k, $1 \leq k \leq n$ are defined by the conditions $\bar{\omega}_k \in \Omega^{(i_k)} \setminus \Omega^{(i_k - 1)}$. We shall show that then $\Omega_k = 0$ for all $k = 1, \cdots, n$. For this it is enough to show that the elements

$$\bar{\omega}_1, \ldots, \bar{\omega}_n; \partial\bar{\omega}_1, \ldots, \partial\bar{\omega}_{r_1}; \ldots; \partial^k\bar{\omega}_1, \ldots, \partial^k\bar{\omega}_{r_k}; \ldots; \partial^t\bar{\omega}_1, \ldots, \partial^t\bar{\omega}_{r_t} \qquad (12)$$

are linearly independent, because the left-hand side of our equation is a linear combination of these elements over K in which "similar terms" corresponding to each $\bar{\omega}_k$ are collected together.

Thus we assume that the elements (12) are linearly dependent over K. Then this linear dependence has the form:

$$\sum_{i=1}^{r_k} \alpha_i \partial^k \bar{\omega}_i \in \Omega_{k-1}, \quad k \leqslant t, \text{ not all } \alpha_i = 0,$$

(where on the left-hand side we have put the terms of maximal order), from which we have

$$\partial^k \Big(\sum_{i=1}^{r_k} \alpha_i \bar{\omega}_i \Big) \in \Omega_{k-1},$$

and so

$$\sum_{i=1}^{r_k} \alpha_i \bar{\omega}_i \in \Omega^{(k)},$$

which is impossible because $\Omega^{(k)}$ is generated by $\bar{\omega}_{r_k+1}, \cdots, \bar{\omega}_n$. Hence there are no nontrivial equations of the type (11). Let us now consider any equation $\mu \in M$. It may be put in the form

$$\sum_{i=1}^{n} (\mathfrak{Q}_k + M_k \partial^{i_k}) \bar{\omega}_k = 0, \quad \mathfrak{Q}_k \in U_{i_k-1}, \quad M_k \in U. \tag{13}$$

On subtracting from this a linear combination of equations (11) of the type $\Sigma_{k=1}^{n} M_k \mu_{i_k,k}$ we come to an equation of the same type as (13):

$$\sum_{i=1}^{n} (\mathfrak{Q}'_k + M'_k \partial^{i_k}) \bar{\omega}_k = 0, \quad \mathfrak{Q}'_k \in U_{i_k-1}, \quad M'_k \in U,$$

in which, however, the order of M'_k is less by at least one than the order of M_k ($M'_k = 0$ if the order of M_k was zero, i.e., it was a constant). After a finite number of steps, on subtracting an element of $\Sigma_{i,j} U \mu_{ij}$ we thus ultimately come to the trivial equation. This proves the lemma.

Let us now consider the matrix $\mathbb{W}$ with $2n$ columns and infinitely many rows in which at the intersection of the ith column, $1 \leq i \leq 2n$ and the $(kn + j)$th row, $0 \leq k < \infty$, $1 \leq j \leq n$ is the element $\partial^k \int_{\gamma_i} \omega_j$ of $\widetilde{K}$. Let $\mathbb{W}_0$ denote the matrix consisting of the first n rows of $\mathbb{W}$.

Let p denote the number of columns of $\mathbb{W}_0$ linearly independent over the complex number field k and let p_1 be the rank of $\mathbb{W}$. Then we have the following inqualities:

(a) $p_1 \leq p$. For any linear dependence over k between the columns of $\mathbb{W}_0$ implies the same linear dependence between the columns with the same indices in $\mathbb{W}$.

(b) $p \leq \Sigma_{i=0}^{t} r_i$. For every column of $\mathbb{W}_0$ belongs to the space X of solutions of the equations (11). The complex dimension of X does not exceed $\Sigma_{i=0}^{t} r_i$, since it is easy to see that the system (11) is equivalent to a system of the type

$$\partial\,(\bar{\omega}_1, \ldots, \partial^t \bar{\omega}_{r_t}) = (\bar{\omega}_1, \ldots, \partial^t \bar{\omega}_{r_t})\, N$$

in matrix notation, where N is a matrix of order $\Sigma_{i=0}^{t} r_i$ with elements in K and ∂ acts on the row (12). The assertion about the dimension of the space of such solutions is well known (and essentially belongs to differential algebra).

(c) $p_1 \geq \Sigma_{i=0}^{t} r_i$. To prove this inequality we shall show that the rows of $\mathbb{W}$ with the indices $kn + j$; $1 \leq j \leq r_k$; $k = 0, \cdots, t$ are linearly independent over $\tilde{K}$. In fact, a linear dependence of the type

$$\sum_{k=0}^{t} \sum_{j=1}^{r_k} a_{kj} \partial^k \int_{\gamma} \omega_j = 0, \quad a_{kj} \in \tilde{K},$$

valid for all $\gamma \in H_1(A_a, \mathbb{Z})$ is equivalent to a Picard-Fuchs equation in the field $L\tilde{K}/\tilde{K}$ of the type

$$\sum_{k=0}^{t} \sum_{j=1}^{r_k} a_{kj} \partial^k \bar{\omega}_j = 0.$$

But the elements of (12) being linearly independent over K remain so over $\tilde{K}$. Hence $a_{kj} = 0$, and (c) is proved.

On comparing (a), (b) and (c) we see that the complex dimension of X is precisely $p = \Sigma_{i=0}^{t} r_i$ and that X is generated over k by columns of $\mathbb{W}_0$, i.e., by the space X_0. This completes the proof of Proposition 4 and thus of the kernel theorem.

4. We note that our result is essentially of a global character. It would be interesting to investigate the group $A^0_{K/k}$ by regarding K as a locally discrete normed field with field k of residues and considering only Picard-Fuchs equations relative to continuous derivations of K.

The structure of the U-module M in this case, as is shown by direct computation for elliptic curves, must reflect essential features of the "infinitesimal" behavior of A. It may be that one can also interpret the numbers r_i, $1 \leq i \leq t$ in other terms. It is easy to see that they are independent of the choice of ∂ and so depend only on A. For elliptic curves the only possible cases $r_1 = 0$ and $r_1 = 1$ are determined by whether ∂ annihilates the absolute invariant of the curve A or not.

CHAPTER II

Rational points on curves of genus ≥ 2

§7. Formulation of the problem

The aim of this chapter is the proof of the following result (the analogue of Mordell's conjecture for function fields).

Theorem 3. *Let K be a regular extension of the field k of characteristic zero and let C be a curve of genus ≥ 2 defined over K. If the set of points of C defined over K is infinite, then there is a curve C_0 which is birationally equivalent to C over K and defined over k. All the points C_K except a finite number are images of points of C_{0k}.*

For technical reasons it is convenient to suppose that the transcendence degree of K/k is one. The following simple result shows that we may confine consideration to this case.

Proposition 5. *If Theorem 3 is true for $\dim_k K = 1$, then it is true universally.*

Proof. Let $K' \subset K$ be a relatively algebraically closed subfield such that $\dim_{K'} K = 1$. If the set C_K is infinite, then by the hypothesis that Theorem 3 is true the curve C is birationally equivalent to a curve C' defined over K'. Since almost all the points C_K are images of points of $C'_{K'}$, this last set must also be infinite. Further, $\dim_k K' = \dim_k K - 1$ and so we may prove the proposition by induction on the transcendence degree.

Hence in future we confine attention to the case $\dim_k K = 1$. It is enough to establish the existence of the curve C_0 defined over k and birationally equivalent to C in order to get the whole of Theorem 3; for Theorem 3 then follows immediately from the theorem of de Franchis reproduced, for example, in Lang's book [4] (historical remarks to Chapter VII).

Since $\dim_k K = 1$ we can canonically define the height in the set of points defined over K of any projective algebraic variety V defined over K (cf. Lang [4]). We shall need only the most elementary facts about heights. More precisely, all that we need are the following properties of the concept "a set of points of bounded height".

If the set $F \subset V_K$ of points on the projective variety V has bounded height, then this property is preserved for any other projective embedding of V. Further, F remains a set of bounded height if we measure the height with respect to any finite extension K' of K or with respect to a field of the type Kk', where $k' \supset k$ is an extension of the constant field linearly disjoint to K.

Let $f: C' \to C$ be an epimorphism of algebraic curves (everything defined over K). If the set $f(C'_K) \subset C_K$ has bounded height, then C'_K also has bounded height.

Let A be an abelian variety defined over K, and let (B, τ) be its K/k-trace. Then the set $a + \tau(B_k) \subset A_k$ (where a is any point of A_K) has bounded height.

All these results are easily obtained from the properties of height described in Lang's book [4] and also in [5] and [6].

The following assertion is also proved without difficulty but because of its importance and for ease of reference we formulate it separately.

Proposition 6. *Let C be a curve over the field K and put $L = K(C)$. Let E be a finite-dimensional subspace of K over k. Then the set F of points $P \in C_K$ for which there is a $f^{(P)} \in E$ with $f^{(P)} \neq 0$ such that $f^{(P)}_P = 0$, has bounded height.*

Proof. Let $(y_1, \cdots, y_n)$ be a k-basis of E. We may suppose without loss of generality that $L = k(y_1, \cdots, y_n)$, on extending E if necessary, which only strengthens the assertion. Then the locus of the point $(1, y_1, \cdots, y_n)$ over K is birationally equivalent to C. We shall measure heights with respect to this embedding.

Let V be the locus of $(1, y_1, \cdots, y_n)$ over k in n-dimensional projective space and let κ be its degree in this embedding. Further, for any $P \in F$ we denote by $\tilde{P}$ the locus of $(1, y_{1P}, \cdots, y_{nP})$ over k in the same projective space. Then $\tilde{P}$ is either a point (and then the logarithmic height of P is zero) or a curve, and then the logarithmic height $h(P)$ is equal to the product of the degree d of the curve $\tilde{P}$ by $e_P = [K : k(y_{1P}, \cdots, y_{nP})]$ (cf. Lang and Néron [6], formula 2 on p. 104).

By the definition of F, the curve $\tilde{P}$ is a component of a hyperplane section of V and so $d \leq \kappa$. Hence if Proposition 6 is false, there must be a sequence of $P \in F$ for which e_P increases indefinitely. But it is possible to avoid this by adding an element of $K \backslash k$ to $(y_1, \cdots, y_n)$ (if E contains no such element, then we must again extend E). This proves the proposition.

Finally, we remark that if C satisfies the conditions of Theorem 3 and if C_K contains infinitely many points of bounded height, then Theorem 3 is true. This is shown, for example, in Lang's book [4] (Chapter VII, §2, Corollary to Proposition 2).

In view of these results it is enough for the proof of Theorem 3 to deduce a contradiction from the following statement.

(H) *There is a curve C of genus ≥ 2 defined over K and having points defined over K of arbitrarily large height.*

This will occupy us in what follows. In preparation we investigate more carefully the function $\mu(P, Q)$ on curves.

§8. The function $\mu(P, Q)$ on curves

1. Let C be a complete nonsingular curve of genus $g \geq 2$ over the field K and let J be its jacobian. We shall suppose that C_K is nonempty. We shall consider the canonical map $\phi: C \longrightarrow J$ defined over K and normalized by the condition that the image of some fixed $O \in C_K$ is the zero of the group law on J. We shall identify C with its image under ϕ.

Lemma 15. *Let $\mu: \Sigma_{i=1}^{n} \Omega_i \bar{\omega}_i = 0$ be a Picard-Fuchs equation on J, where ω_i are invariant differentials. Then on C there is a Picard-Fuchs equation $\mu': \Sigma_{i=1}^{n} \Omega_i \bar{\eta}_i = 0$, where the η_i are the differentials of the first kind on C induced by the forms ω_i. Conversely to every equation $\mu': \Sigma_{i=1}^{n} \Omega_i \bar{\eta}_i = 0$ on C there corresponds an equation $\mu: \Sigma_{i=1}^{n} \Omega_i \bar{\omega}_i = 0$ on J, where the ω_i are the unique invariant forms inducing the η_i on C. Further, $\mu(P, Q) = \mu'(P, Q)$ for all $P, Q \in C_K$.*

Proof. The map $\phi: C \longrightarrow J$ can be identified with the composition

$$C \xrightarrow{i} C^g \xrightarrow{j} J,$$

where C^g is the g-fold direct product of C with itself, $i(P) = (P, 0, \cdots, 0)$ for any $P \in C$; and $j(P_1, \cdots, P_g) = \phi(P_1) + \cdots + \phi(P_g)$. For any differential η on C we denote by $\eta^{(i)}$ the differential form on C^g, which is the inverse image of η under the projection $p_i: C^g \longrightarrow C$ onto the ith component. It is well known that if the differential form of the first kind ω on J induces the differential η on C, then its inverse image on C^g is $\Sigma_{k=1}^{g} \eta^{(k)}$.

The equation $\mu: \Sigma_{k=1}^{n} \Omega_k \bar{\omega}_k = 0$ on J corresponds to some equation $j^*\mu$ on C^g and by Lemma 9 we have the identity

$$j^*\mu(P, Q) = \mu(j(P), j(Q))$$

for all $P, Q \in C^g$.

By Lemma 10 there are Picard-Fuchs equations $\mu_1, \cdots, \mu_g$ on C such that

$$j^*\mu(P, Q) = \sum_{i=1}^{g} \mu_i(P_i, Q_i), \quad P = (P_1, \ldots, P_g), \quad Q = (Q_1, \ldots, Q_g).$$

It is easy to see that the μ_i are the inverse images under the projection $p_i: C^g \to C$ of one and the same equation $\mu': \Sigma_{k=1}^{n} \Omega_k \bar{\eta}_k = 0$ as defined in the enunciation of the lemma. More precisely, let v be a nonconstant function on C and $v^{(i)}$ the inverse image on C^g of v with respect to p_i, so that $\mathbf{v} = (v^{(1)}, \cdots, v^{(g)})$ is a transcendence basis for the function field on C^g. Then as a representative of the equation $j^*\mu$ on C^g and μ' on C we may take respectively

$$\sum_{i=1}^{n} \Omega_{iv}\Big(\sum_{k=1}^{g} \eta_i^{(k)}\Big) = \sum_{k=1}^{n} dz^{(k)}. \qquad \sum_{i=1}^{n} \Omega_{iv}\eta_i = dz.$$

It is easy to check that the subfield $K(J) \subset K(C^g)$, which may be identified with the subfield of the symmetric functions on C^g, is mapped into itself by any derivation of the type ∂_v of $K(C^g)$. Hence the argument may be reversed, which allows us to recover the Picard-Fuchs equation μ on J from the equation μ' on C. The last assertion of the lemma follows from

$$\mu(P, Q) = \mu(j(P, 0, \ldots, 0), j(Q, 0, \ldots 0)) = \mu_1(P, Q) = \mu'(P, Q).$$

This completes the proof of the lemma.

Corollary 1. *Let μ be a fixed Picard-Fuchs equation on C. Then the $\mu(P)$, $P \in C_K$ all lie in a finite-dimensional k-subspace of K (which, of course, depends on μ).*

(For, in fact by the Mordell-Weil theorem for function fields it follows from the kernel theorem that the values of $\mu(P)$ belong to an abelian subgroup of K of finite type.)

Corollary 2. *Let $c_\mu \in K$ be some choice of elements as μ runs through some system of generators of the U-module of Picard-Fuchs equations on C reduced to some basis or other. Then the set of $P \in C_K$ for which $\mu(P) = c_\mu$ has bounded height.*

(For by the Mordell-Weil theorem and the kernel theorem those points belong to a finite number of cosets modulo $\tau(B_k)$, where (B, τ) is the K/k-trace of J, and so have bounded height.)

2. In future, in conformity with the notation for abelian varieties we shall write $\mu(P)$ instead of $\mu(0, P)$ $(P \in C \subset J)$ for any Picard-Fuchs equation μ on C.

We shall show now that the function $\mu(P)$ may be computed for almost all $P \in C_K$ using only *one* representative of μ. ("Almost all" here and henceforward means "all except a finite number".)

Lemma 16. *Let ∂ be a derivation of K/k, let $\omega_i = u_i dv$ and let*

$$\sum_{i=1}^{n} \Omega_{iv}\omega_i = dz \quad \left(\Omega_i = \sum_{j=0}^{m} a_{ij}\partial^j, \quad a_{ij} \in K\right)$$

be a representative of μ, where v is a local parameter at O and $z_0 = 0$. Then

$$\mu(P) = z_P + \sum_{i=1}^{n}\sum_{j=1}^{m} a_{ij}M_i^j(P), \tag{14}$$

$$M_i^j(P) = \sum_{k=0}^{j-1} \partial^{j-1-k}[(\partial_v^k u_i)_P\, \partial v_P]. \tag{15}$$

We may use these formulas to compute $\mu(P)$ for all $P \in C_K$ except finitely many.

Proof. Indeed if P does not belong to the poles of v, the zeros of v or the

zeros of dv, then the function $w = vv_P^{-1}$ serves as a permissible local parameter at O and P. Hence

$$\mu(P) = z'_P - z'_O, \quad dz' = \sum_{i=1}^{n} \Omega_{iw}\,\omega_i.$$

We shall compute first $\partial_w^i (udv)$. We have

$$(\partial_w - \partial_v)(u\,dv) = d(uw\,\partial v_P)$$

(using Lemma 2 and the fact that $v = wv_P$). Let us suppose that we have already proved the identity

$$(\partial_w^j - \partial_v^j)(u\,dv) = d\left(w \sum_{k=0}^{j-1} \partial_w^{j-1-k} [\partial_v^k u \cdot \partial v_P]\right) = N^j (u\,dv) \tag{16}$$

for some $j \geq 1$. It is true for $j = 1$; let us check it for $j + 1$. We have

$$\begin{aligned}(\partial_w^{j+1} - \partial_v^{j+1})(udv) &= (\partial_w^j - \partial_v^j)\,\partial_v u \cdot dv + \partial_w^j (\partial_v - \partial_w)(udv) \\ &= d\left(w \sum_{k=0}^{j-1} \partial_w^{j-1-k} [\partial_P^{k+1} u \cdot \partial v_v]\right) + d(w\partial_w^j (u\,\partial v_P)) \\ &= d\left(w \sum_{k=0}^{j} \partial_w^{j-k} [\partial_v^k u \cdot \partial v_P]\right) = N^{j+1}(u\,dv),\end{aligned}$$

which completes the induction. Hence

$$\sum_{i=1}^{n} \Omega_{iw}\,\omega_i = \sum_{i=1}^{n} \Omega_{iv}\,\omega_i + \sum_{i=1}^{n} \sum_{j=1}^{m} a_{ij} N^j (u_i\,dv).$$

On comparing this with the formulas (14), (15) and (16) and noting that $w_O = 0$, $w_P = 1$ we see that it is enough to check the formula

$$(\partial_w^{j-1-k} [\partial_v^k u \cdot \partial v_P])_P = \partial^{j-1-k} [(\partial_v^k u)_P\,\partial v_P].$$

But this follows from Lemma 3 (b) since w is an admissible quasiparameter at P. This proves the lemma.

§9. Proof of Theorem 2. First case

From now until the end of the chapter we shall suppose that C satisfies the statement (H). The notation ∂, O are the same as in §8 and v denotes a function satisfying the conditions of Lemma 16.

In this section we reduce the statement (H) to an absurdity under the auxiliary supposition that *in the space of differentials of the first kind on C there are two linearly independent ones $\omega_1 = u_1 dv$, $\omega_2 = u_2 dv$, which satisfy equations of the type*

$$\begin{cases}\partial_v \omega_1 + \omega_1 = dw_1, \\ \partial_v \omega_2 + \omega_2 = dw_2,\end{cases} \tag{17}$$

where ω'_1, ω'_2 *are differentials of the first kind* (this supposition characterises our "first case").

Let μ_1, μ_2 be the Picard-Fuchs equation on C of which the first and second equation in (17) respectively are representatives. By Lemma 16 we have

$$\mu_1(P) = u_{1P}\partial v_P + w_{1P},$$
$$\mu_2(P) = u_{2P}\partial v_P + w_{2P} \tag{18}$$

for almost all P. On multiplying the first of these equations by u_{2P} and the second by $-u_{1P}$ and adding, we have

$$\mu_1(P)\, u_{2P} - \mu_2(P)\, u_{1P} - (w_1u_2 - w_2u_1)_P = 0 \tag{19}$$

for almost all $P \in C_K$.

We shall show now that $w_1u_2 - w_2u_1$ can be expressed K-linearly in terms of u_1 and u_2. For otherwise the function

$$f^{(P)} = \mu_1(P)\, u_2 - \mu_2(P)\, u_1 - (w_1u_2 - w_2u_1),$$

would be distinct from zero for all $P \in C_K$ and would lie by Lemma 15, Corollary 1 in a finite-dimensional k-subspace of L. From Proposition 6 and (19) it would then follow that the set C_k is a set of points of bounded height in contradiction to (H).

Hence

$$w_1u_2 - w_2u_1 = c_1u_2 - c_2u_1, \qquad c_1, c_2 \in K.$$

and so

$$f^{(P)} = (\mu_1(P) - c_1)\, u_2 - (\mu_2(P) - c_2)\, u_1.$$

Since u_1, u_2 are linearly independent over K, a similar argument using Proposition 6 shows that *for almost all* $P \in C_K$ we have

$$\mu_1(P) = c_1, \quad \mu_2(P) = c_2. \tag{20}$$

Now it is not difficult to establish that for *any* equation μ on C there is a $c = c_\mu \in K$ such that $\mu(P) = c_\mu$ for almost all $P \in C_K$. We shall do that in a moment.

From (18) and (20) follows the existence of a rational function w on C such that

$$\partial v_P = w_P \tag{21}$$

for almost all $P \in C_K$.

Lemma 17. *For any function* x *on* C *and any integer* $j \geq 2$ *there is a function* y *depending only on* x *and* j *such that* $\partial^j x_P = y_P$ *for all those* $P \in C_K$ *for which* (21) *holds.*

Proof. It is enough to clear up the case $j = 1$, since induction on j will then provide the necessary proof.

Let $F(X, V)$ be an irreducible polynomial over K such that $F(x, v) = 0$. The identity

$$(F^{\partial}(x, v))_P + \left(\frac{\partial F}{\partial X}(x, v)\right)_P \partial x_P + \left(\frac{\partial F}{\partial V}(x, v)\right)_P \partial v_P = 0,$$

obtained by differentiating the equation $F(x_P, v_P) = 0$ together with (21) proves the lemma.

On applying this to (14) and (15) we easily show that for any Picard-Fuchs equation μ on the curve there is a rational function x^{μ} depending only on μ such that

$$\mu(P) = x_P^{\mu}$$

for almost all $P \in C_K$. The hypothesis that $x^{\mu} \notin K$ leads immediately to a contradiction with assertion (H) in view of Proposition 6, since the function $f^{(P)} = \mu(P) - x^{\mu}$, which would be different from zero, belongs (by Lemma 15, Corollary 1) to a finite-dimensional k-linear subspace of L. The alternative, that $x^{\mu} \in K$ for all μ leads to a contradiction to assertion (H) by Lemma 15, Corollary 2.

This concludes the proof ot the first case of Theorem 3.

§10. Proof of Theorem 2. Second case

Let C again be a curve for which the assertion (H) is true. Then it is true also for field $K\bar{k}$, where $\bar{k}$ is the algebraic closure of k. Hence from now on we shall suppose that k is algebraically closed.

Amongst the curves C satisfying (H) we shall take one such that the dimension of the space of differentials ω of the first kind satisfying

$$\partial\bar{\omega} + \bar{\omega}' = 0 \tag{22}$$

(where ω' is also a differential of the first kind) is maximal. As was shown in the preceding section, this dimension must be either zero or 1, on the assumption that (H) can be satisfied at all.

In Lang's paper [5] (Proposition 1 on p. 40) it is shown that there is an unramified covering $p: C' \longrightarrow C$ of arbitrarily high degree defined over K and such that the truth of (H) for C implies its truth for C'. Let J, J' be the jacobians of C, C' respectively. Then there exists an abelian variety A defined over K and an isogeny $j: J' \longrightarrow J \times A$ also defined over K, the "first coordinate" of which coincides with the map induced by p. (Here and above we regard C' and C as embedded in their jacobians J' and J and passing through the zero points which are chosen so as to agree with p.) The isogeny induces an isomorphism of the spaces of differential forms of the first kind on J' and $J \times A$ respectively. The last space splits

as the direct sum of the spaces of forms which induce zero on J and A respectively. Interpreting this in terms of forms on C' we see that the subspace H of those differential forms of the first kind on C' which are induced by the differential forms on C has a uniquely defined complement H_1. The differentials of H_1 are induced on the image of C' by the sequence

$$C' \xrightarrow{\phi'} J' \xrightarrow{j} J \times A$$

of maps from the differential forms which vanish on J. There is a 1-1 correspondence between the Picard-Fuchs equations on A and the Picard-Fuchs equations on C' which connect differentials belonging to H_1. This correspondence preserves the values of the μ-function, as follows from Lemma 15 and Lemmas 10 and 11.

We shall show that the Picard-Fuchs equations on H_1 can be described very simply.

Lemma 18. *For any differential $\omega \in H_1$ there are uniquely determined ω', $\omega'' \in H_1$ such that there is an equation of the type*

$$\mu_\omega : \partial^2\bar{\omega} + \partial\bar{\omega}' + \bar{\omega}'' = 0. \tag{23}$$

The equations (23) reduced to any basis of H_1 generate the U-module of Picard-Fuchs equations in H_1 reduced to that basis. For any two differentials ω_1, $\omega_2 \in H_1$ and any two points P, $Q \in C'_K$ we have the identity

$$\mu_{\omega_1-\omega_2}(P, Q) = \mu_{\omega_1}(P, Q) - \mu_{\omega_2}(P, Q). \tag{24}$$

Proof. The classes $(\bar{\omega}_1, \cdots, \bar{\omega}_n, \partial\bar{\omega}_1, \cdots, \partial\bar{\omega}_n)$, where $(\omega_1, \cdots, \omega_n)$ is any basis of H_1, are linearly independent over K. For otherwise we should have an equation of the type

$$\bar{\omega} + \sum_{i=1}^{n} \alpha_i \partial\bar{\omega}_i = 0, \quad \omega \in H_1,$$

where not all the α_i are zero, i.e., an equation

$$\bar{\omega}' + \partial\left(\sum_{i=1}^{n} \alpha_i \bar{\omega}_i\right) = 0, \quad \omega' = \omega - \sum_{i=1}^{n} \partial\alpha_i \omega_i.$$

But this would mean that on C' the dimension of the space of differentials satisfying (22) would be greater than the number for C, contrary to our choice of C.

Since H_1 is induced by forms on the variety A, it follows that the classes $\partial^j\bar{\omega}$ for any $j \geq 2$ and $\omega \in H_1$ must depend linearly on the classes $\bar{\omega}_i$, $\partial\bar{\omega}_i$, $i = 1, \cdots, n$. Any relation of the type

$$\mu_\omega : \partial^2\bar{\omega} + \sum_{i=1}^{n} (\alpha_i \partial\bar{\omega}_i + \beta_i \bar{\omega}_i) = 0$$

is of the shape (23) on putting $\omega' = \Sigma_{i=1}^{n} \alpha_i \omega_i$, $\omega'' = \Sigma_{i=1}^{n} (\beta_i - \partial\alpha_i)\omega_i$. The uniqueness of ω' and ω'' is clear.

The equations μ_{ω_i}, $i = 1, \cdots, n$ generate the whole module of equations in H_1 reduced to the basis $(\omega_1, \cdots, \omega_n)$ by Lemma 14 and since in this case $n = r_0 = r_1$, $r_2 = 0$. Finally (24) follows from the uniqueness of (23). This concludes the proof of the lemma.

Let us consider (23). As above, let v be an element of $K(C)$ which is a local parameter at $O \in C'_K$ (it exists since the covering $C' \longrightarrow C$ is unramified). By Lemma 16 we have

$$\mu_\omega(P) = \omega_P + u'_P\, \partial v_P + (\partial_v u)_P\, \partial v_P + \partial(u_P\, \partial v_P) \tag{25}$$

for almost all $P \in C'_K$, where

$$\partial_v^2 \omega + \partial_v \omega' + \omega'' = dw, \quad w_O = 0, \quad \omega = u\, dv, \quad \omega' = u'\, dv.$$

In the proof of Lemma 17 we established the existence of $x^u, y^u \in K(C')$ such that

$$\partial u_P = x_P^u + y_P^u\, \partial v_P \tag{26}$$

for all $P \in C'_{\bar{K}}$, where $\bar{K}$ is the algebraic closure of K (except at the poles of u and v, where the equation becomes meaningless). It is easy to see that these functions are uniquely determined, for otherwise we would have an equation of the type $\partial v_P = v'_P$, $v' \in K(C')$ for all $P \in C'_{\bar{K}}$ and v' would have to take each of its values v'_P infinitely often, namely at all the Q where $v_Q = v_P + c$, $c \in k$. This is impossible because ∂v_P by the nontriviality of ∂ takes more than one value on $C'_{\bar{K}}$.

By (26) and (25) we have

$$\mu_\omega(P) = u_P\, \partial^2 v_P + y_P^u (\partial v_P)^2 + (x^u + \partial_v u + u')_P\, \partial v_P + w_P \tag{27}$$

for almost all $P \in C'_K$.

Take a basis $\omega_i = u_i dv$, $i = 1, \cdots, n$ of H_1 and consider the matrix T with three columns and n rows, the ith row having the form

$$T_i = (u_i, y^{u_i}, x^{u_i} + \partial_v u_i + u_i'). \tag{28}$$

The rank of this matrix is at most three. Hence *there is a covering $C' \longrightarrow C$ defined over K for which the rank of T constructed with respect to some basis of H_1 takes its maximal value $R \leq 3$* (the maximum being taken, of course, only over those unramified coverings for which C' satisfied (H)).

From now on we shall suppose that C' has been so chosen that the rank R of T is maximal.

Let us now consider a further unramified covering $C'' \longrightarrow C'$ of degree $m > 1$

such that C'' also satisfies (H). As above, the space $H + H_1$ of differentials of the first kind on C' has a uniquely determined complement H_2. The elements of H_2 correspond to forms on an abelian variety B which is determined by an isogeny

$$j' : J'' \longrightarrow J' \times B.$$

The "first coordinate" $J'' \longrightarrow J'$ of this isogeny is generated by the covering $C'' \longrightarrow C'$.

Let $\omega = udv$ be any element of H_2. We shall apply (27) to the relation μ_ω of the type (23) *in the space* H_2 and to the point $P \in C''_K$. By the choice of C' the row

$$T_u = (u, y^u, x^u + \partial_v u + u')$$

is a linear combination of the rows T_i, $i = 1, \cdots, R$ (cf. (28)):

$$T_u = \sum_{i=1}^{R} z_i T_i, \quad z_i \in K\ (C'').$$

Hence a relation of the type

$$\mu_\omega(P) = \sum_{i=0}^{R} z_{iP}\, \mu_i(P), \quad (\mu_0(P) = 1, \quad \mu_i(P) = \mu_{\omega_i}(P), \quad i = 1, \ldots, R), \tag{29}$$

is true for almost all $P \in C''_K$. Let $1, t_1, \cdots, t_S$ be a maximal subset of $1, z_1, \cdots, z_R$ linearly independent over K. On expressing the z_i in terms of the t_j and substituting in (29) we obtain

$$\mu_\omega(P) + \sum_{i=1}^{R} c_i \mu_i(P) + \sum_{j=1}^{S} t_{jP} \sum_{i=1}^{R} c_{ij}\, \mu_i(P) = 0, \quad c_i, c_{ij} \in K, \tag{30}$$

for almost all $P \in C''_K$. By Lemma 15, Corollary 1, the function

$$f^{(P)} = \mu_\omega(P) + \sum_{i=1}^{R} c_i \mu_i(P) + \sum_{j=1}^{S} t_j \sum_{i=1}^{R} c_{ij}\, \mu_i(P)$$

lies in a finite k-dimensional subspace of $K(C'')$ for fixed ω as P runs through the points of C''_K. Hence if C'' satisfies (H) we must have $f^{(P)} = 0$ for almost all $P \in C''_K$, i.e.,

$$\mu_\omega(P) + \sum_{i=1}^{R} c_i\, \mu_i(P) = 0, \quad c_i \in K, \tag{31}$$

for such P. We emphasize that c_i depends on ω but not on P.

We shall now suppose that the covering $C'' \longrightarrow C'$ is normal and has a cyclic Galois group generated by an automorphism $\sigma : C'' \longrightarrow C''$. Such a covering always exists over some finite extension of K and since the truth of (H) and all the previous constructions are compatible with such an extension we may suppose that the

covering is actually defined over K.

Since the $\mu_i(P)$, $i = 1, \cdots, R$ depend only on the projection of $P \in C''$ onto C' it follows from (31) that

$$\mu_\omega(P^{\sigma^{-1}}) = \mu_\omega(P) \tag{32}$$

for almost all $P \in C''_K$. The automorphism σ acts on $K(C'')$ and since $v^\sigma = v$ it is easy to see that $(x^u)^\sigma = x^{u^\sigma}$, $(y^u)^\sigma = y^{u^\sigma}$. Further, for any $z \in K(C'')$ we have

$$z_P^{\sigma^{-1}} = z_{P\sigma}.$$

Hence (27) implies

$$\mu_\omega(P^{\sigma^{-1}}) = \mu_{\omega^\sigma}(P).$$

On taking this with (32) and using (24) we have

$$\mu_{\omega-\omega^\sigma}(P) = 0 \tag{33}$$

for all $\omega \in H_2$ and almost all $P \in C''_K$.

The linear mapping $\omega \longrightarrow \omega^\sigma - \omega$ of H_2 into itself is clearly epimorphic. Since the μ_ω generate the module of Picard-Fuchs equations in H_2 it follows that $\mu(P) = 0$ for all such equations μ and for almost all $P \in C''_K$. But this means that the set $j'(C''_K)$ of rational points on the curve $j(C'')$ in the abelian variety B determined by the diagram $J'' \longrightarrow J' \times B$ has bounded height. This set does not reduce to a point because C'' generates J''. Hence the curve C'' cannot satisfy (H), which has led us to our required contradiction.

This completes the proof of Theorem 3.

CHAPTER III

Rational points on elliptic curves

§11. Formulation of the result

On an elliptic curve C over a field K of finite type (and also over a field of finite relative type K/k if C is not isomorphic to a curve defined over k) the points C_K form a finitely generated group, which may sometimes actually be finite. The functional variant of the Siegel-Mahler theorem shows that in any affine model of C there are only finitely many points with "integral coordinates" (i.e., coordinates lying in a given subring of finite type of K) (cf. [5]).

In this chapter we shall prove by means of the function $\mu(P)$ a finiteness theorem from which the Siegel-Mahler theorem follows and which is so strong that the analogue over number fields is false.

From the very beginning we restrict ourselves to a ground field K which is a field of algebraic functions of a single variable over an algebraically closed field $k \subset K$. The standard reduction, which we shall not repeat, permits one to make deductions for the case of fields of finite type or finite relative type.

Besides, we shall suppose that the curve C of genus one is not isomorphic to a curve defined over k even in any finite extension of K; the contrary case from our present point of view being trivial.

Let $L = K(C)$. We shall use the letters P, Q for prime divisors of L/K and will identify prime divisors of the first degree with points of C_K, which we shall consider infinite. We denote prime divisors (points) of K/k by p.

For any $v \in L$ we denote by (v), $(v)_0$, $(v)_\infty$ respectively the divisor, divisor of zeros and divisor of poles of v, and by $\nu_P(v)$ the order of v relative to the divisor P. As usual, v_P is the value of v at P. We shall use completely analogous notation for the elements of K. There can only be confusion in relation to symbols of the type (a) where $a \in K$ if we have not agreed whether a divisor in L or in K is meant, and usually the exact sense will be clear from the context.

It is convenient to introduce a function $\epsilon(x)$ of a real argument:

$$\epsilon(x) = \begin{cases} 0 & \text{if } x \leq 0, \\ x & \text{if } x > 0. \end{cases}$$

Theorem 4. *Let $y \in L \setminus K$ and let $r \geq 1$ be the maximum order of a zero of y. Then there is a constant h, depending only on y and K, such that*

$$\sum_p \epsilon(\nu_p((y_Q)) - 2r) < h \tag{34}$$

for all $Q \in C_K$.

(If $y_Q = 0, \infty$ we put $\nu_p(y_Q) = 0$, and the summation is extended over all points p of K.)

Corollary (Mahler's Theorem). *Let S be any finite set of points of K and let $x \in L \setminus K$. The set of points $Q \in C_K$ for which $\nu_P((x_Q)_\infty) = 0$ for $p \in S$ is finite.*

(One must put $y = x^{-1}$ and remember that any infinite set of points of C_K has unbounded height. If the condition $\nu_p((x_Q)_\infty) = 0$ for $p \notin S$ were satisfied for the points of such a set, then $\Sigma_{p \in S} \nu_p((x_Q^{-1})_0) \longrightarrow \infty$, contrary to (34).)

We shall prove Theorem 4 in the next two sections and here note only that the assertion of the theorem is trivially false when K is an algebraic number field (although the corollary remains true). For let K be the field of rational numbers and consider the function y^{-1} on a curve C in Weierstrass normal form $y^2 = x^3 + Ax + B$. Let $Q \in C_K$ be any point of infinite order. By a result of Lutz [7] some prime p divides the denominator of y_Q to a positive power. There is an integer $d \neq 0$ such that dQ belongs to the Lutz subgroup on C relative to p. Put

$$Q_n = p^n dQ.$$

It follows from the properties of the Lutz subgroup that $\nu_p((y_{Q_n}^{-1})_0)$ increases indefinitely as $n \longrightarrow \infty$ (as a linear function of n). Hence (34) cannot remain true.

§12. Auxiliary results

We shall fix some $v \in L \setminus K$ and some derivation ∂ of K. Without loss of generality we may suppose that there is a $t \in K$ for which $\partial t = 1$. We shall also fix the differential $\omega = u\,dv$ of the first kind on C. Since the K/k-trace of C is trivial, $\bar{\omega}$, $\partial\bar{\omega}$ are linearly independent over K. Hence we have

Lemma 19. *The module of Picard-Fuchs equations on C reduced to ω is generated by a single equation with a representative of the type*

$$(\partial_v^2 u + a\partial_v u + bu)\,dv = dw, \quad a, b \in K, \quad w \in L. \tag{35}$$

Lemma 20. *Let $e_p = \nu_p(dt) + 1$ ($t \in K$, $\partial t = 1$). Then for any $a \in K$ we have*

$$\nu_p(\partial a) \geq \nu_p(a) - e. \tag{36}$$

Proof. In K the derivation ∂ coincides with d/dt, and so

$$\nu_p(\partial a) = \nu_p(da) - \nu_p(dt) \geqslant \nu_p(a) - \nu_p(dt) - 1 = \nu_p(a) - e_p.$$

This proves the lemma.

Finally we shall need the following partial formulation of the "decomposition theorem" of A. Weil.

A function defined for all $P \in C_K$ and taking values in the group of divisors of K/k is called a *distribution*. The distributions f, g are called *equivalent* if the quotients $f^{-1}(P)\,g(P)$ and $f(P)\,g^{-1}(P)$ divide some fixed divisor of K/k for all $P \in C_K$. The distribution f is called *integral* if all its values are integral divisors of K/k.

The decomposition theorem asserts that there is a set of distributions $A(P)$ in 1-1 correspondence with the divisors A of L/K and with the following properties:

(a) If A is an integral divisor then $A(P)$ is an integral distribution.

(b) $(A_1 A_2)(P) = A_1(P)\,A_2(P)$.

(c) If g.c.d. $(A_1, A_2) = 1$, then g.c.d. $(A_1(P), A_2(P)) = 1$ for all P (where of course the first g.c.d. is in the sense of divisors on L/k and the second of divisors on K/k).

(d) $(v)(P) \sim (v_P)$ for any $v \in L$. (Of course (v_P) denotes the divisor of $v_P \in K$ in K/k. Further, we assign to v_P the unit divisor if $v_P = 0$ or ∞. Here $\sim$ is the symbol of equivalence for distributions.)

§13. Proof of Theorem 4

It is easy to see that it is enough to prove Theorem 4 for any finite extension of K. Hence we may suppose that the zeros of y are in C_K.

Let O be some fixed point of C_K and v a local parameter there. We shall give C_K the group law in which O is zero, so, as usual $P_1 + P_2 = P_3$ if the divisor P_1P_2/OP_3 is principal.

We define the finite set S of points of K/k by the two following conditions (the notation being the same as in Lemma 19 and the decomposition theorem).

(1) S contains all zeros and poles of a and factors of the divisor of the differential dt.

(2) If $p \notin S$ and $\nu_p(O(Q)) \neq 0$, then

$$\nu_p(x_Q) = \nu_O(x)\nu_p(O(Q)), \tag{37}$$

where x is any one of u, v, $\partial_v u$, w (w being normalized by the condition $w_O = 0$).

The existence of such a set follows at once from the decomposition theorem, which also implies the following replacement of (37) for $p \in S$.

(3) There is a constant c such that

$$|\nu_p(x_Q) - \nu_O(x)\nu_p(O(Q))| < c, \tag{38}$$

for all $p \in S$ and all $Q \in C_K$ with $\nu_p(O(Q)) \neq 0$, where x is one of u, au, v, $\partial_v u$, w.

We shall now consider the function $\mu(Q) = \mu(O, Q)$ belonging to (35). By Lemma 16

$$\mu(Q) = w_Q + au_Q\partial v_Q + (\partial_v u)_Q\,\partial v_Q + \partial\,(u_Q\,\partial v_Q).$$

for almost all $Q \in C_K$. We now make some estimations. Suppose first that $p \notin S$, $\nu_p(O(Q)) \neq 0$. Then

$$\nu_p(w_Q) = \nu_O(w)\,\nu_p(O(Q)) \geqslant \nu_p(O(Q)),$$
$$\nu_p(au_Q\partial v_Q) \geqslant (\nu_O(u) + \nu_O(v))\,\nu_p(O(Q)) - 1 = \nu_p(O(Q)) - 1$$

(on using 37), Lemma 20 and the fact that $\nu_O(v) = 1$, $\nu_O(u) = \nu_O(\omega/dv) = -\nu_O(dv) = 0$). Similarly on using Lemma 20 again and noting that $\partial_v u \in o_Q$ we have:

$$\nu_p((\partial_v u)_Q\,\partial v_Q) \geqslant \nu_p(O(Q)) - 1,$$
$$\nu_p(\partial\,(u_Q\partial v_Q)) \geqslant \nu_p(O(Q)) - 2.$$

Suppose now that $p \in S$, $\nu_p(O(Q)) \neq 0$. By the same arguments but using (38) instead of (37) we have

$$\nu_p(w_Q) \geqslant \nu_p(O(Q)) - c,$$
$$\nu_p(au_Q\,\partial v_Q) \geqslant \nu_p(O(Q)) - 2c - e,$$
$$\nu_p((\partial_v u)_Q\,\partial v_Q) \geqslant \nu_p(O(Q)) - 2 - e,$$
$$\nu_p(\partial\,(u_O\partial v_Q)) \geqslant \nu_p(O(Q)) - 2c - 2e,$$

where $e = \max_{p \in S}(\nu_p(dt) + 1)$. On combining all these estimates we get the following estimate for the order of the divisor of zeros of $\mu(Q) \in K$:

$$\deg \mu(Q) \geqslant \sum_{p \notin S} \varepsilon(\nu_p(O(Q)) - 2) + \sum_{p \in S} \varepsilon(\nu_p(O(Q)) - d), \quad d = 2c + 2e.$$

By the Mordell-Weil theorem and the kernel theorem $\deg \mu(Q)$ is bounded above on the set of $Q \in C_K$ of infinite order. Hence there is a constant h_0 such that

$$\sum_{p \notin S} \varepsilon(\nu_p(O(Q)) - 2) + \sum_{p \in S} \varepsilon(\nu_p(O(Q)) - d) < h_0 \tag{39}$$

for all $Q \in C_K$. In essence this is the strongest formulation of the theorem of finitude for elliptic curves which can be obtained in this way. The transition to (34) already weakens our result somewhat.

Let us take h_0 and S in such a way, that (34) remains true for all factors O_i of the divisor of zeros of y.

Let $(y)_0 = \Pi_i O_i^{r_i}$. From the obvious inequality

$$\varepsilon(x_1 + x_2) \leqslant \varepsilon(x_1) + \varepsilon(x_2)$$

we have

$$\sum_{p \notin S} \varepsilon(x_p(O_i^{r_i}(Q)) - 2r) + \sum_{p \in S} \varepsilon(\nu_p(O_i^{r_i}(Q)) - dr) < h_0 r_i, \tag{40}$$

where $r = \max r_i$. Now we use the coprimeness of $O_i(Q)$ and $O_j(Q)$ for $i \neq j$ and note that $\Sigma_i \varepsilon(x_i - s) = \varepsilon(\Sigma_i x_i - s)$ if there is at most one x_i distinct from zero and $s > 0$. On summing (40) with respect to i we thus obtain

$$\sum_{p \notin S} \varepsilon(\nu_p((y)_0(Q)) - 2r) + \sum_{p \in S} \varepsilon(\nu_p((y_0)(Q)) - dr) < h_0 \sum_i r_i. \tag{41}$$

Since there are only finitely many elements in the second sum we may replace it by

$$\sum_{p \in S} \varepsilon(\nu_p((y)_0(Q)) - 2r),$$

on replacing the constant on the right-hand side by a greater one. Finally (possibly again at the price of increasing the constant) we may replace the divisor $(y)_0(Q)$ by $(y_Q)_0$. Since clearly

$$\varepsilon(\nu_p((y_Q)_0) - 2r) = \varepsilon(\nu_p((y_Q)) - 2r),$$

we thus obtain (34).

BIBLIOGRAPHY

[1] I. R. Šafarevič, *Principal homogeneous spaces defined over a function field*, Trudy Mat. Inst. Steklov. 64 (1961), 316–346.

[2] S. Lang, *Introduction to algebraic geometry*, 1959.

[3] ———, *Abelian varieties*, Interscience Tracts in Pure and Applied Mathematics, No. 7, Interscience, New York, 1959. MR 21 #4959.

[4] ———, *Diophantine geometry*, Interscience Tracts in Pure and Applied Mathematics, No. 11, Interscience, New York, 1962. MR 26 #119.

[5] ———, *Integral points on curves*, Inst. Hautes Études Sci. Publ. Math. No. 6 (1960), 27–43. MR 24 #A86.

[6] S. Lang and A. Néron, *Rational points of abelian varieties over function fields*, Amer. J. Math. 81 (1959), 95–118. MR 21 #1311.

[7] E. Lutz, *Sur l'équation* $y^2 = x^3 - Ax - B$ *dans les corps p-adiques*, J. Reine Angew. Math. 177 (1937), 238–247.

[8] Ju. Manin, *Algebraic curves over fields with differentiation*, Izv. Akad. Nauk SSSR Ser. Mat. 22 (1958), 737–756. (Russian) MR 21 #2652.

[9] ———, *On the Hasse-Witt matrix of an algebraic curve*, ibid. 25 (1961), 153–172. (Russian) MR 23 #A1638.

[10] ———, *Diophantine equations over functional fields*, Dokl. Akad. Nauk SSSR 139 (1961), 806–809 = Soviet Math. Dokl. 2 (1961), 1009–1012. MR 24 #A2576.

[11] L. J. Mordell, *On the rational solutions of the indeterminate equation of the third and fourth degrees*, Proc. Cambridge Philos. Soc. 21 (1922), 179–192.

[12] E. Picard and G. Simart, *Théorie des fonctions algébraiques de deux variables independents*, Paris, 1897–1906.

[13] J. Igusa, *Abstract vanishing cycle theory*, Proc. Japan Acad 34 (1958), 589–594. MR 21 #50.

[14] ———, *Class number of a definite quaternion with prime discriminant*, Proc. Nat. Acad. Sci. U.S.A. 44 (1958), 312–314. MR 20 #5183.

Translated by:

J. W. S. Cassels