ANNALS OF MATHEMATICS
Vol. 62, No. 1, July, 1955
Printed in U.S.A.

ABELIAN VARIETIES OVER P-ADIC GROUND FIELDS†

BY ARTHUR MATTUCK*

(Received September 17, 1954)

Modern algebraic geometry has opened up a new approach to the classical problem of Diophantine analysis, for the study of the existence and nature of rational solutions to algebraic equations may be interpreted as the study of the rational points on the algebraic varieties defined by these equations.[1] However, the general theory of varieties defined over number fields being undoubtedly very difficult, it is perhaps not out of place to study simpler but related questions to see what light they may shed on the more general problem. One method of simplification, the one adopted here, is to study varieties over fields with an arithmetical structure simpler than that of a number field, namely, the p-adic fields.

The first person to undertake such a study was E. Lutz in 1937 [16], who proved the following theorem:

The group of rational points on the curve $y^2 = x^3 - Ax - B$ *defined over a* p-*adic field contains a subgroup of finite index isomorphic to the additive group of integers of the ground field.*

The goal of the present paper is to prove a theorem which may be regarded as a generalization of Lutz' result:

Let A *be an abelian variety of dimension* d *defined over a field* k *of characteristic* 0 *complete under a non-archimedean absolute value. The group of points of* A *rational with respect to* k *contains a subgroup analytically isomorphic and homeomorphic to* $I \oplus I \oplus \cdots \oplus I$ *(*d *summands) where* I *is the additive group of integers of the ground field. If* k *is locally compact, the subgroup is of finite index.*

If the ground field is the complex numbers, then it is known that the group in question is isomorphic to the complex d-dimensional torus; the group I thus appears as the natural p-adic analogue of the complex period parallelogram.

The proof given here of this theorem requires a certain amount of spadework —some of it quite routine—and the first two parts are devoted to this. In particular part I is given over to a study of power series in several variables over a complete ultrametric (non-archimedean valued) field; though a few things in here may also be found in Chabauty [6], there does not seem to be any inclusive treatment of these fundamentals available, so it is given here. In part II an invariant definition of a p-adic algebroid variety is given which exhibits it as a point set; the definition rests on the non-archimedean version of a theorem of Cartan, which depends in turn on a key lemma given at the appropriate place

† This paper forms the substance of a dissertation presented to the faculty of Princeton University, June 1954; Presented to the American Mathematical Society April 24, 1954.
* National Science Foundation Predoctoral Fellow 1953–4.

[1] For a discussion of this point of view and of the relevant literature, see Weil [17].

in Part I. Actually the usual non-invariant definition of the algebroid variety as the set of common zeros of a finite number of power series could with some awkwardness be made to serve for the applications of this notion in part VI, and so part II is strictly speaking not essential for the present purpose. The results are however of some independent interest, and since it ought to be convenient for future applications as well as this one to have such an algebroid variety available, this material is included in the present paper. Parts III and IV are devoted to explicit preparations for the theorem, and in parts V and VI the main theorem is proved, first for the special case of jacobian varieties in part V, then for the general abelian variety in part VI by imbedding it in a suitable jacobian variety.

It is a pleasure to express here my appreciation to Professor Emil Artin, who supervised this work, and to Dr. Serge Lang for many stimulating discussions on this and other matters. I would like also to take this opportunity to record here my indebtedness to the late Professor Arnold Dresden, an inspiring teacher as well as a wise and humane counselor who guided my first steps, as he has those of so many other mathematicians, with patience, sympathy, and imaginative insight.

I. Power series over P-adic fields

1. Preliminaries. Throughout these first two parts, k will be a field complete under an ultrametric absolute value, that is, a non-archimedean valuation with the reals as value group. This absolute value may be then extended uniquely to $\bar{k}$, the algebraic closure of k; if $\tilde{k}$ is the completion of $\bar{k}$, it is known that $\tilde{k}$ is also algebraically closed.

We consider power series in several variables over k, and write them

$$f(x) = f(x_1, \cdots, x_n) = \sum a_{r_1 \cdots r_n} x_1^{r_1} x_2^{r_2} \dots x_n^{r_n}, \qquad a_{r_1 \cdots r_n} \in k.$$

For such series, the Jordan definition of convergence is used: $f(x)$ converges for the value $\alpha = (\alpha_1, \cdots, \alpha_n)$, $\alpha_i \in \tilde{k}$, to a limit denoted by $f(\alpha)$ if and only if every sequential series made up of all the terms of

$$\sum a_{r_1 \cdots r_n} \alpha_1^{r_1} \dots \alpha_n^{r_n}$$

converges, and all to the same limit, $f(\alpha)$. Since a sequential series of terms from an ultrametric field converges if and only if the absolute value of the general term goes to zero, the following statements are clear:

1. If one sequential series converges, then they all do, and to the same limit.
2. $f(x)$ converges for $x = \alpha$ if and only if

$$| a_{r_1 \cdots r_n} \alpha_1^{r_1} \dots \alpha_n^{r_n} | \to 0.$$

3. If $f(x)$ converges for $x = \alpha$, then it converges under any method of finitely iterated summation and always to the same limit.

To prove (3), one may proceed by proving with standard arguments that a double series may be summed by rows; the general case then follows by induction on the number of iterations.

2. For the sequel we need the following fundamental theorems about addition, multiplication, substitution, and inversion of power series in several variables. These are all familiar for power series in one variable (see, e.g., [12]), but proofs for the general case do not seem to be available.

We shall use the abridged notation

$$f(x) = \sum a_{r_1 \cdots r_n} x_1^{r_1} \cdots x_n^{r_n} = \sum a_R x^R$$

where R stands here for the general n-tuple of non-negative integers, so that for example $R + S = T$ means the ordinary vector addition

$$(r_1 + s_1, \cdots, r_n + s_n) = (t_1, \cdots, t_n);$$

by $| R |$ we mean $\max_i [r_i]$. Summation ranges will be omitted whenever possible, or abbreviated by $\bar{R}$. The partial sums of $f(x)$ will be denoted by

$$f_n(x) = \sum_{|R| \leqq n} a_R x^R.$$

Clearly $f(x)$ converging for $x = \alpha$ is equivalent to $f_n(\alpha) \to f(\alpha)$.

Addition theorem. *Let $f(x) + g(x) = h(x)$. If $f(x)$ and $g(x)$ converge for $x = \alpha$, so does $h(x)$, and $f(\alpha) + g(\alpha) = h(\alpha)$.*

Proof. If $f(x) = \sum a_R x^R$, $g(x) = \sum b_S x^S$, then $h(x) = \sum (a_R + b_R) x^R$ and $h(x)$ converges for $x = \alpha$, since $| (a_R + b_R)\alpha^R | \to 0$. Now $f_n(\alpha) + g_n(\alpha) = h_n(\alpha)$; the rest follows by taking limits.

Multiplication theorem. *Let $f(x)g(x) = h(x)$. If $f(x)$ and $g(x)$ converge for $x = \alpha$, so does $h(x)$, and $f(\alpha)g(\alpha) = h(\alpha)$.*

Proof. Letting $f(x)$ and $g(x)$ be as above, we have

$$h(x) = \sum_T \sum_{R+S=T} a_R b_S x^{R+S}.$$

Now

$$f_n(\alpha)g_n(\alpha) = h_n(\alpha) + \sum_{\bar{R}} a_R b_S \alpha^{R+S}$$

where the sum is over the range $\bar{R}$: $| R + S | > n$, $| R | \leqq n$, $| S | \leqq n$. We need only show that the limit of the last term is 0 as $n \to \infty$. Let

$$M = \max_{R,S} [\, | a_R \alpha^R |, | b_S \alpha^S | \,].$$

Given ε, there exists $n_0(\varepsilon)$ such that $| a_R \alpha^R | < \varepsilon$, $| b_S \alpha^S | < \varepsilon$ for $| R |, | S | > n_0(\varepsilon)$. But if $| R + S | > n$, either $| R | > n/2$ or $| S | > n/2$; therefore by taking $n > 2n_0(\varepsilon)$,

$$\Big| \sum_{\bar{R}} a_R b_S \alpha^{R+S} \Big| \leqq \max_{\bar{R}} | a_R \alpha^R \cdot b_S \alpha^S | \leqq M\varepsilon.$$

Substitution theorem. *Given $f(x_1, \cdots, x_n) = \sum a_R x^R$ and $g_i(u_1, \cdots, u_m) = \sum b_{iS} u^S$ for $i = 1, \cdots, n$. Suppose that we are given two neighborhoods of the origin, U and V, such that*

1. *$f(x)$ converges in $U = \{(\beta_1, \cdots, \beta_n) \mid | \beta_i | \leqq \delta_i\}$,*
2. *all the $g_i(u)$ converge in V and $(g_1(V), \cdots, g_n(V)) \subset U$,* i.e., $| g_i(\alpha) | \leqq \delta_i$ *for $\alpha \in V$,*

3. $\max_S |b_{iS}\alpha^S| \leqq \delta_i$ *for all* $\alpha \in V$.
Then if $F(u_1, \cdots, u_m) = f(g_1(u), \cdots, g_n(u))$, *it follows that* $F(u)$ *converges for all* $\alpha \in V$ *and* $F(\alpha) = f(g_1(\alpha), \cdots, g_n(\alpha))$.

PROOF. We have $[g_1(u)]^{r_1}[g_2(u)]^{r_2} \cdots [g_n(u)]^{r_n} = \sum c_S^{(R)} u^S$ where (R) is the indexing symbol $(r_1, \cdots, r_n)$. By the multiplication theorem, $\sum c_S^{(R)} u^S$ converges for $\alpha \in V$ and $\sum c_S^{(R)} \alpha^S = \prod_i [g_i(\alpha)]^{r_i}$. Therefore we have

$$f(g_1(\alpha), \cdots, g_n(\alpha)) = \sum a_R \sum c_S^{(R)} \alpha^S = \sum_R \sum_S a_R c_S^{(R)} \alpha^S.$$

But $F(\alpha) = \sum_S (\sum_R a_R c_S^{(R)})\alpha^S$, so that what has to be proved is that the summation order can be interchanged; by §1 it suffices for this to show that the multiple series $\sum_{R,S} a_R c_S^{(R)} \alpha^S$ converges; this in turn will follow if we show that $|a_R c_S^{(R)} \alpha^S| \to 0$ for $\alpha \in V$ as $|R|, |S| \to \infty$.

For this we need the explicit expression for $c_S^{(R)}$. Let $[g_i(u)]^r = \sum b_{iS}^{(r)} u^S$, where $b_{iS}^{(r)} = \sum b_{iT_1} b_{iT_2} \cdots b_{iT_r}$, the sum taken over all distinct partitions of the m-vector S into the sum of r m-vectors $T_1, \cdots, T_r$. Then we have $c_S^{(R)} = \sum b_{1T_1}^{(r_1)} \cdots b_{nT_n}^{(r_n)}$, the sum taken over all distinct partitions of the m-vector S into the sum of n m-vectors $T_1, \cdots, T_n$. Since by hypothesis, $|b_{iS}\alpha^S| \leqq \delta_i$ for $\alpha \in V$, it follows that $|b_{iS}^{(r)}\alpha^S| \leqq \delta_i^r$, and from this in turn that $|c_S^{(R)}\alpha^S| \leqq \delta_1^{r_1} \cdots \delta_n^{r_n}$. Therefore $|a_R c_S^{(R)} \alpha^S| \leqq |a_R \beta^R|$, where $\beta = (\beta_1, \cdots, \beta_n)$ is any element of U such that $|\beta_i| = \delta_i$. Now $f(x)$ converges for β, so that $|a_R\beta^R| \to 0$; this implies that $|a_R c_S^{(R)} \alpha^S| \to 0$, which was what had to be proved.

REMARK. If the $g_i(u)$ have no constant term, then the condition $|b_{iS}\alpha^S| \leqq \delta_i$ for all $\alpha \in V$ and all S and i can always be met by picking V small enough. For if $g_i(u)$ converges for $u = \alpha$, then $|b_{iS}\alpha^S| \to 0$ so that the terms far out will all be $\leqq \delta_i$ in absolute value, and by picking V_i small we can make the finite number of terms before these also $\leqq \delta_i$ in absolute value; now set $V = \bigcap V_i$ and the condition (3) will be satisfied.

3. Recall that a power series $f(x) = f(x_1, \cdots, x_n)$ is *regular in* x_n if it has no constant term (i.e., is a non-unit) and if $f(0, \cdots, 0, x_n)$ is not identically zero; this last implies that the series contains pure x_n terms, ax_n^i, with $a \in k$. The *degree* s of $f(x)$ is then the smallest value of i for which $f(x)$ contains such a term. A power series of the form $x_n^s + A_1x_n^{s-1} + \cdots + A_n$ where $A_i \in k[[x_1, \cdots, x_{n-1}]]$ and $A_i(0, \cdots, 0) = 0$ is called *distinguished* of degree s in x_n.

For convenience, neighborhoods of the origin in the affine n-space over the field k will be called simply "neighborhoods" and taken to be closed hypercubes U_r^n (or simply U), unless otherwise specified: $U_r^n = \{(x_1, \cdots, x_n) \mid |x_i| \leqq r\}$, where r is a real number belonging to the value group of $\bar{k}$. Then $f(x)$ is *holomorphic in* U if it converges on some neighborhood of U; $f(x)$ is *convergent* if it is convergent in some neighborhood of $(0, \cdots, 0)$.

THEOREM 1. $\mathfrak{F}$ *denotes the ring of convergent power series in n variables over k.*

A. WEIERSTRASS PREPARATION THEOREM. *Let* $p(x) \in \mathfrak{F}$ *be regular in* x_n, *of degree s. Then*

(i) *for any* $b(x) \in \mathfrak{F}$, *we can write* $b(x) = p(x)q(x) - h(x)$ *where* $h(x)$ *is a polynomial in* x_n *of degree* $s - 1$ *and where* $q(x)$, $h(x)$ *both lie in* $\mathfrak{F}$,

(ii) $p(x) = f(x)g(x)$, *where* $f(x)$ *is a unit in* $\mathfrak{F}$ (f *has a constant term*) *and where* $g(x)$ *is distinguished in* x_n, *of degree* s, *and with convergent coefficients.*

B. *If in part* A, i, $p(x)$ *is actually distinguished in* x_n (*and not merely regular*), *then there exists a neighborhood* U *depending only on* $p(x)$ *such that in the identity* $b(x) = p(x)q(x) - h(x)$, *if* $b(x)$ *is holomorphic in* $V \subset U$, *then* $q(x)$ *and* $h(x)$ *will be holomorphic in* V *also.*

Proof. The validity of A, i and A, ii as formal identities is well known. The proofs of the convergence of $q(x)$ and $h(x)$, $f(x)$ and $g(x)$, given that of $b(x)$, may be made by the method of majorant series [2b, 5]; the proofs for the classical case where the ground field is the complex numbers are valid here too since the archimedean triangle inequality is replaced throughout by the stronger ultrametric non-archimedean inequality. A direct proof of the preparation theorem for non-archimedean fields was first given by Chabauty [6].

To prove part B, write $b(x)$, $p(x)$, and $q(x)$ as power series in x_n :

$$b(x) = \sum_\mu \sum_\nu b_{\mu\nu} x_n^\mu \; ; \; q(x) = \sum_\mu \sum_\nu q_{\mu\nu} x_n^\mu \; ;$$

$$p(x) = x_n^s + p_{s-1} x_n^{s-1} + \cdots + p_0$$

where $p_\mu = \sum_{\nu=0}^{\infty} p_{\mu\nu}$; here the $b_{\mu\nu}$, $q_{\mu\nu}$, $p_{\mu\nu}$ are homogeneous polynomials of degree ν in the remaining variables, $x_1, \cdots, x_{n-1}$. Also, we have assumed the coefficient of x_n^s in $p(x)$ is 1, which is no restriction of generality. The recursion formula for determining $q(x)$, once $b(x)$ and $p(x)$ are given, appears in Bochner and Martin [2b] as

$$q_{mn} \equiv b_{m+s,n} - \sum_{\mu=0}^{m+s} \sum_{\nu=0}^{n-1} q_{\mu\nu} p_{m+s-\mu,n-\nu} + \sum_{\mu=0}^{m-1} q_{\mu n} p_{m+s-\mu,0}$$

where if $n = 0$, the middle term is to be taken as 0. Now since $p(x)$ is distinguished, we have $p_{\mu\nu} = 0$ for $\nu > 0$, $\mu \geqq s$, so that the formula becomes

$$q_{mn} \equiv b_{m+s,n} - \sum_{\mu=m+1}^{m+s} \sum_{\nu=0}^{n-1} q_{\mu\nu} p_{m+s-\mu,n-\nu} .$$

Moreover, the p_μ have no constant terms, which means that inside some U_r^{n-1} depending only on $p(x)$, all the homogeneous terms of $p_0, \cdots, p_{s-1}$ will have absolute value less than 1 (cf. remark, §2): $|p_{\mu\nu}| \leqq 1$, for $|x_1| \leqq r, \cdots, |x_{n-1}| \leqq r$. We maintain that $U_r^n = U$ is the desired neighborhood.

Suppose therefore that $b(x)$ converges inside $U_{r'}^n$ where $r' \leqq r$. Picking π such that $|\pi| = r'$ and setting $x_n = \pi y$, we see that

$$b'(x_1, \cdots, x_{n-1}, y) = \pi^s \sum \left(\sum b_{\mu\nu} \pi^{\mu-s}\right) y^\mu$$

converges for $|x_1| \leqq r', \cdots, |x_{n-1}| \leqq r', |y| \leqq 1$. Multiplying the recursion formula through by π^m we get

$$q_{mn}\pi^m \equiv b_{m+s,n}\pi^m - \sum_{\mu=m+1}^{m+s} \sum_{\nu=0}^{n-1} (q_{\mu\nu}\pi^\mu)(p_{m+s-\mu,n-\nu}\pi^{m-\mu})$$

and if we observe that the convergence of b' implies that $|b_{\mu\nu}(\pi, \cdots, \pi)\pi^{\mu-s}| \to 0$, we conclude that

$$|q_{mn}\pi^m| \leqq \max_{0 \leqq \mu \leqq m+ns, 0 \leqq \nu \leqq n} |b_{\mu\nu}\pi^{\mu-s}| \leqq M$$

for some fixed constant M and for all $(x_1, \cdots, x_{n-1}) \in U_{r'}^{n-1}$. Since therefore the $q_{mn}\pi^m$ are uniformly bounded inside $U_{r'}^{n-1}$, we know that $q' = \sum (\sum q_{\mu\nu}\pi^\mu)y^\mu$ converges for $(x_1, \cdots, x_{n-1}) \in U_{r'}^{n-1}$, $|y| < 1$, or in other words, $q(x_1, \cdots, x_n)$ converges for $|x_1| \leqq r', \cdots, |x_{n-1}| \leqq r'$, $|x_n| < r'$. The convergence of $h(x)$ in the same region now follows, and with it the theorem, if we recall the definition of "holomorphic in a neighborhood."

IMPLICIT FUNCTION THEOREM. *Let $f_i(w_1, \cdots, w_n, x_1, \cdots, x_r)$, $i = 1, \cdots, n$, converge in a neighborhood of the origin and vanish there, and suppose that*

$$J_0(f_1, \cdots, f_n; w_1, \cdots, w_n) = \left|\frac{\partial(f_1, \cdots, f_n)}{\partial(w_1, \cdots, w_n)}\right|_{\substack{x=0\\ w=0}} \neq 0.$$

Then there exist unique series $w_i = g_i(x_1, \cdots, x_r) \in k[[x_1, \cdots, x_r]]$ such that

(1) *the g_i are convergent, $g_i(0, \cdots, 0) = 0$, and they satisfy the $f_j(w, x) = 0$ identically, and*

(2) *the g_i give exactly the complete local solution of the system $f_j(w, x) = 0$; that is, for (x^0), (w^0) in some neighborhood of the origin in $X \times W$ space, we have $f_j(w^0, x^0) = 0$ (all j) $\Leftrightarrow w_i^0 = g_i(x_1^0, \cdots, x_r^0)$ (all i).*

PROOF. We proceed by induction. Pick a non-zero minor of order $n - 1$ in $J_0(f_1, \cdots, f_n; w_1, \cdots, w_n)$; we can assume it is $J_0(f_1, \cdots, f_{n-1}; w_1, \cdots, w_{n-1})$. By the induction assumption, we can then solve for $w_1, \cdots, w_{n-1}$ as power series in the x_i and w_n, with $w_i(w_n, x_1, \cdots, x_r) = 0$ at the origin. Also, for (x^0, w^0) in some neighborhood U of the origin, $f_1 = \cdots = f_{n-1} = 0 \Leftrightarrow w_i^0 = w_i(w_n^0, x_1^0, \cdots, x_r^0)$. Substituting these into $f_n(w, x)$ gives us a new power series $h(w_n, x_1, \cdots, x_r)$ convergent in a neighborhood of the origin and vanishing there. By a standard computation [11],

$$(\partial h/\partial w_n)\cdot J(f_1, \cdots, f_{n-1}; w_1, \cdots, w_{n-1}) = J(f_1, \cdots, f_n; w_1, \cdots, w_n),$$

whence $\partial h/\partial w_n \neq 0$ at the origin. This means that $h(w_n, x)$ is regular of degree 1 in w_n, so by Theorem 1, part A we can write $h = [w_n - A_0(x_1, \cdots, x_r)]\cdot q$ where q is a unit and $A_0(0, \cdots, 0) = 0$. Then $w_n = A_0(x_1, \cdots, x_r)$ and $w_i = w_i(A_0, x_1, \cdots, x_r)$, $i = 1, \cdots, n - 1$, clearly satisfy conclusion (1) above. If $w_i^0 = w_i(x_1^0, \cdots, x_r^0)$, then $f_j(w^0, x^0) = 0$ by the substitution theorem, applicable here since the w_i have no constant term (see remark, §2). And if $f_1 = \cdots = f_n = 0$ for (x^0, w^0) in a suitable $V \subset U$, we must have $h(w_n^0, x^0) = 0$, or $w_n^0 = A_0(x_1^0, \cdots, x_r^0)$, $w_i^0 = w_i(A_0(x_1^0, \cdots, x_r^0), x_1^0, \cdots, x_r^0)$ by the induction assumption, substitution theorem, and since q is not zero in a neighborhood of the origin.

For $n = 1$, we have but one series $f(w, x_1, \cdots, x_r)$ together with the condition $\partial f/\partial w \neq 0$ at the origin, so it may be handled directly, by the above procedure.

COROLLARY. (INVERSION THEOREM). *Let $x_i = f_i(w_1, \cdots, w_n) = \sum a_{ij}w_j +$ (higher powers), $i = 1, \cdots, n$, where the f_i converge in a neighborhood of the origin, and* det $|a_{ij}| \neq 0$. *Then the system can be inverted; that is, we can write $w_i = g_i(x_1, \cdots, x_n)$, such that*

(i) *$x_i \equiv f_i(g_1, \cdots, g_n)$, the g_i are convergent, and $g_i(0) = 0$,*

(ii) $x_i^0 = f_i^0(w_1^0, \cdots, w_n^0)$ *if and only if* $w_i^0 = g_i(x_1^0, \cdots, x_n^0)$, *for* (x^0) *and* (w^0) *in a suitable neighborhood of the origin.*

II. P-ADIC ALGEBROID VARIETIES

4. Naively, an algebroid variety over a complete ultrametric field k, which goes through a point (henceforth assumed to be the origin) of affine n-space A^n over k, is the set of common zeros of an ideal $\mathfrak{a}$ in the ring of holomorphic functions at the origin (convergent power series in n variables). Since, however, the convergent power series have arbitrarily small radii of convergence, it is clear that only $(0, \cdots, 0)$ itself is a zero of *every* function in $\mathfrak{a}$. We may therefore proceed noninvariantly by selecting a basis $(f_1, \cdots, f_r)$ for $\mathfrak{a}$—finite, since the convergent power series form a Noetherian ring—and taking the common zeros of only the f_i; the variety then will be attached to the basis $(f_1, \cdots, f_r)$ rather than to $\mathfrak{a}$ itself. However, it is readily seen that the varieties attached to two different bases of $\mathfrak{a}$ will coincide in some neighborhood of the origin. This suggests introducing an equivalence relation at (0) by calling two sets containing (0) equivalent if they coincide in some neighborhood of (0); then the "algebroid variety of $\mathfrak{a}$" will be that single equivalence class of sets to which the set of common zeros of any basis of $\mathfrak{a}$ belongs. This is the procedure adopted by Cartan for algebroid varieties over the complex numbers [4a].

One can however make the variety a more substantial object by actually attaching to the ideal $\mathfrak{a}$ a genuine point set.[2] The possibility of doing this rests upon the following non-archimedean version of a theorem proved by Cartan for the complex numbers [4b].

As before, denote by $\mathfrak{F}$ (or $\mathfrak{F}_n$) the ring of convergent power series in n variables over a complete ultrametric field. Then $\mathfrak{F}^q = \mathfrak{F} \oplus \cdots \oplus \mathfrak{F}$ (q summands) is the q-dimensional module over $\mathfrak{F}$ consisting of all q-vectors with components from $\mathfrak{F}$, or alternatively, of all holomorphic mappings of a neighborhood of (0) in A^n into A^q. By a *q-dimensional module* is meant a submodule $\mathfrak{M}^q$ of $\mathfrak{F}^q$; a one-dimensional module is therefore simply an ideal in $\mathfrak{F}$. Elements of modules will be denoted by capital letters $F, G, \cdots$; elements of $\mathfrak{F}$ by small letters f, $g, \cdots$. Finally, the q-vector $F = (f_1, \cdots, f_q)$ is said to be holomorphic in $U \subset A^n$ if all the f_i are holomorphic there.

THEOREM 2. *Suppose we have given a finite number of modules* $\mathfrak{M}_1^{q_1}, \cdots, \mathfrak{M}_s^{q_s}$ *over* $\mathfrak{F}$. *Then given any set of bases* $\mathfrak{B}_1, \cdots, \mathfrak{B}_s$ *for these modules*, $\mathfrak{B}_j = \{B_{(j)}^i\}$, *there exists a neighborhood* U^n *of the origin depending only upon the bases such that if* $F \in \mathfrak{M}_j$ *is holomorphic on* $V \subset U^n$, *then* $F = \sum_i g_i B_{(j)}^i$ where the g_i are holomorphic on V.

PROOF. (a) *The construction of a special basis.* The core of the argument is the construction by an inductive procedure of a set of bases having neighborhoods with the property stated in the theorem; such bases will be called provisionally

[2] The possibility of this definition was suggested to me by Professor Artin. Professor Chow has informed me that he has used a similar definition in his papers on *Foundations of Algebroid Geometry* (over the complex numbers), to appear soon.

"special" and U will be called the "associated neighborhood". We follow in outline Cartan's proof.

The result being trivial for $n = 0$, suppose that such a special set of bases can be constructed for modules over $\mathfrak{F}_{n-1}$. To obtain special bases for modules over $\mathfrak{F}_n$, we first consider the case in which all the $q_j = 1$, so that the $\mathfrak{M}_j$ are simply ideals $\mathfrak{a}_j$ in $\mathfrak{F}_n$, assumed to be non-zero. By a preliminary rotation of axes, which does not disturb any cubical neighborhoods that will be used, we can assure ourselves that each $\mathfrak{a}_j$ contains a $p_j'(x)$ regular in x_n, and therefore by Theorem 1, part A also a $p_j(x)$ distinguished in x_n of degree s_j. Applying part B of that theorem, we have a neighborhood W_j^n associated with $p_j(x)$ such that: $b(x)$ holomorphic in $V \subset W_j$ implies that $b(x) = p_j(x)q(x) - h(x)$ where $q(x)$, $h(x)$ are holomorphic in V and $h(x)$ is a polynomial in x_n of degree $s_j - 1$.

Denote by $\mathfrak{M}_j'$ the elements of $\mathfrak{a}_j$ which are polynomials in x_n of degree $\leqq s_j - 1$; $\mathfrak{M}_j'$ is seen to be a module over $\mathfrak{F}_{n-1}$, of dimension s_j, and in the above equation, $b(x) \in \mathfrak{a}_j$ implies $h(x) \in \mathfrak{M}_j'$. By the induction, $\mathfrak{M}_j$ has a special basis $\mathfrak{C}_j = C_{(j)}^1, \cdots, C_{(j)}^r$ which can be thought of as polynomials $c_{(j)}^1(x), \cdots, c_{(j)}^r(x)$ in x_n, from $\mathfrak{F}_n$. With $\mathfrak{C}_j$ goes an associated neighborhood U_j^{n-1}. Now let U_j^n be the cubical neighborhood in n-space whose slice by the hyperplane $x_n = 0$ is U_j^{n-1}, and let U be the smallest of the U_j^n and W_j^n. Then we claim that

$$\{p_j(x), c_{(j)}^1(x), \cdots, c_{(j)}^r(x)\} = \mathfrak{B}_j$$

is the required special basis of $\mathfrak{a}_j$ and U is the neighborhood associated with the $\mathfrak{B}_j$.

Namely, $b(x) \in \mathfrak{a}_j$, $b(x)$ holomorphic in $V \subset U$ implies that b is holomorphic in $V \subset W_j$, which in turn means that we can write $b = qp_j - h$ with q, h holomorphic in V. But if $h(x)$ is holomorphic in $V \subset U_j^n$ and $h(x) \in \mathfrak{M}_j'$, then the coefficients of $h(x)$ (written as a polynomial in x_n) are holomorphic in $V^{n-1} \subset U_j^{n-1}$ where V^{n-1} is the obvious slice of V by $x_n = 0$. That is, $h = \sum_1^r g_i c_{(j)}^i$ with $g_i(x_1, \cdots, x_{n-1})$ holomorphic in V^{n-1}; summing up, we have

$$b = qp_j - g_1 c_{(j)}^1 - \cdots - g_r c_{(j)}^r, \qquad q(x) \text{ and all } g_i(x) \text{ holomorphic in } V.$$

This completes the proof for the case $q_j = 1$.

The general case of the construction follows quite simply from this. Considering first the case of a single module $\mathfrak{M}^q$, form the ideals $\mathfrak{a}_j$ consisting of the j^{th} components of those elements of $\mathfrak{M}$ whose first $j - 1$ components are zero. For each j pick vectors $F_{(j)}^1, \cdots, F_{(j)}^{m_j}$ in $\mathfrak{M}$ whose first $j - 1$ components are zero and whose j^{th} components are a special basis for $\mathfrak{a}_j$ with associated neighborhood U'; if then $U \subset U'$ is a neighborhood in which all the $F_{(j)}^i$ are holomorphic, the set $\{F_{(j)}^i\}$ forms the desired basis, with neighborhood U. Finally, if we are given a set of modules $\mathfrak{M}_k^{q_k}$, picking a special basis for each, with associated neighborhood U equal to the smallest of the associated neighborhoods U_k, completes the induction and therefore the construction.

(b) *The theorem for arbitrary bases.* We must now show that all sets of bases are "special" in the sense of part (a). Call the special bases we have constructed

$\mathfrak{C}_j = \{C^i_{(j)}\}$, and the associated neighborhood W. Suppose we are given an arbitrary set of bases, $\mathfrak{B}_1, \cdots, \mathfrak{B}_s$, where $\mathfrak{B}_j = \{B^i_{(j)}\}$. Then we may write

$$C^i_{(j)} = \sum_k a^{(j)}_{ik} B^k_{(j)} \quad \text{where} \quad a^{(j)}_{ik} \in \mathfrak{F}.$$

Let $U \subset W$ be a neighborhood on which all the $a^{(j)}_{ik}$ are holomorphic. If F is holomorphic on $V \subset U$ and $F \in \mathfrak{M}_j$, then we may write

$$F = \sum_i g^{(j)}_i C^i_{(j)} \quad \text{with the } g^{(i)}_i \text{ holomorphic on } V,$$

and therefore

$$F = \sum_{i,k} g^{(j)}_i a^{(j)}_{ik} B^k_{(j)} = \sum_k h^{(j)}_k B^k_{(j)}$$

where $h^{(j)}_k = \sum_i g^{(j)}_i a^{(j)}_{ik}$ is holomorphic on V. Therefore $\mathfrak{B}_j$ is a special basis, with associated neighborhood U. This completes the proof.

5. Given an ideal $\mathfrak{a} \in \mathfrak{F}$, we use Theorem 2 to attach a point set in A^n to $\mathfrak{a}$ which will be called *the algebroid variety of* $\mathfrak{a}$. Namely, with each basis of $\mathfrak{a}$ there is associated a certain neighborhood satisfying the properties of Theorem 2; we now assume that the neighborhood selected for this purpose is the largest one with these properties—this determines it uniquely, since our neighborhoods are by agreement hypercubes. Let $(b_1, \cdots, b_r)$ be a basis of $\mathfrak{a}$ whose associated neighborhood U in this new sense is the biggest of any neighborhood associated with any basis. Then A, the algebroid variety of $\mathfrak{a}$, is defined to be that portion of the common zeros of the b_i which lies inside U.

The justification for this definition lies in the following two statements:

1. *If $f \in \mathfrak{a}$ is holomorphic on $V \subset U$, then f vanishes on $A \cap V$.* (In other words, A annihilates every power series in $\mathfrak{a}$, insofar as it could be reasonably expected to.) Namely, write $f = \sum a_i b_i$. Then by the choice of U, the a_i are holomorphic on V. Since all the b_i vanish at every point of $A \cap V$, so does f.

2. *Given any other basis $(c_1, \cdots, c_s)$ of $\mathfrak{a}$, with associated neighbohood V, let A' be that part of the set of common zeros of the c_i which lies inside V. Then $A' = A \cap V$.* For by the above, $A \cap V \subset A'$ since the c_j are holomorphic on $V \subset U$ and therefore vanish on $A \cap V$. Similarly, the b_i are holomorphic on U, therefore *a fortiori* on V; hence in $b_i = \sum a_{ij} c_j$, the a_{ij} are holomorphic on V; since $c_j = 0$ on A', we have $b_i = 0$ on A', whence $A' \subset A \cap V$.

Statement 2 above shows that all bases with the maximal associated neighborhood U give the same variety A. It will be convenient on occasion to relax the definition slightly: by "an algebroid variety of $\mathfrak{a}$" we will mean the intersection of A with a neighborhood of (0).

By the *field of definition* of A we mean simply k itself. If $\mathfrak{a}$ is a prime ideal $\mathfrak{p}$, then A is *irreducible* and its dimension is defined to be the dimension of $\mathfrak{p}$ in the ring $\mathfrak{F}_n$, i.e., the length of the longest chain of proper prime ideals properly containing $\mathfrak{p}$. If $\mathfrak{a}$ is not prime, its dimension is the biggest dimension of any of the associated prime ideals; in this case A splits up into irreducible components through (0) and the dimension is simply the largest dimension of any of these components.

A *regular* transformation of the space is one defined by convergent power series $u_i = \sum_j a_{ij}x_j +$ (higher powers), where $a_{ij} \in k$ and det $|a_{ij}| \neq 0$. Such a transformation defines an automorphism of the ring $\mathfrak{F}_n$ and therefore it preserves the dimension of algebroid varieties.

If we are given an ideal $\mathfrak{a}'$ in $k[x_1, \cdots, x_n]$, we can lift it up to an ideal $\mathfrak{a}''$ in $k[[x_1, \cdots, x_n]]$—i.e., we pass to the completion of the local ring at (0)—and from there pass to the algebroid ideal $\mathfrak{a}$ in $\mathfrak{F}_n$ which is simply the subset of all *convergent* power series in $\mathfrak{a}''$. Geometrically, we start with the bunch of algebraic varieties A'; A is then the algebroid variety formed by the intersection with a certain neighborhood of (0) of those components of A' which pass through (0). The suppression of the other components arises in a well-known fashion from the killing in the passage to the local ring at (0) of all prime ideals not contained in the maximal ideal $(x_1, \cdots, x_n)$. Finally, we know from the theory of local rings that the algebraic dimension of any component of A' through (0) is the same as the algebroid dimension of the corresponding components of A into which it splits [7, 15b].

These remarks will suffice for the sequel.

III. The topology on the places

6. Varieties over topological ground fields. Throughout this section k is a Hausdorff topological field. Affine n-space over k is thus a topological space endowed with the product topology. We set up in the usual way the projective n-space S^n over k and give it the local Cartesian product topology, so that the neighborhoods of a point are just the neighborhoods of the point in an affine space containing it. This description of the topology does not depend on the affine space selected, because any two are in birational, everywhere biregular correspondence, which guarantees that the associated topological transformation is bicontinuous and 1–1, hence a homeomorphism.

It is easily seen that any variety in affine space is a closed set. Namely, a polynomial in n variables over k is a continuous function, so that its zeros form a closed set since they are the inverse image of the closed set 0 under the continuous map defined by the polynomial. Every hypersurface thus being a closed set, so is every affine variety as a finite intersection of hypersurfaces. It follows immediately that every projective variety is also closed, for if P is a limit of points lying on the variety, P will also be the limit of points lying on any affine model of the variety whose ambient affine space contains P. Since the affine variety is closed, P lies on it and thus lies on the projective variety as well.

If k is locally compact (and non-discrete), then it is known that the topology on k is induced by an absolute value, and that the totality of elements $\{a\}$ such that $|a| \leqq 1$ forms a compact set [3]. Taking $(x_0, \cdots, x_n)$ as projective coordinates, S^n is seen to be the union of the $n + 1$ sets:

$$\{(1, x_1/x_0, \cdots, x_n/x_0) \mid |x_i/x_0| \leqq 1\}, \cdots,$$
$$\{(x_0/x_n, \cdots, x_{n-1}/x_n, 1) \mid |x_i/x_n| \leqq 1\}.$$

Each of these is evidently compact, and S^n is therefore also compact. Since a variety in S^n is a closed subset of a compact space, we conclude that a projective variety over a locally compact non-discrete field is compact.

We note finally that if Ω is a universal domain for k which also carries a Hausdorff topology preserving the topology of k, then the preceding remarks are to be interpreted as applying to the set of points rational with respect to k on any variety over Ω which has k for a field of definition.

7. The topology on the places. We deal throughout this and the next few sections with a separably generated function field in one variable K/k over a complete absolute-valued (and therefore Hausdorff) ground field k of arbitrary characteristic. For the proof of the main theorem the characteristic will be 0, but it is not necessary to assume this here. Familiar examples of such ground fields are the real and complex numbers, the p-adic fields, power series fields in one variable over arbitrary trivially-valued constant fields, and more generally, the completion under a rank 1 valuation of any function field in several variables.

The set $\mathfrak{R}$ of rational places of K/k has a natural topology induced by the topology on k. This may be defined invariantly, as Lang has introduced it [14], but for our purpose the following non-invariant definition is more convenient. The points rational with respect to k on any non-singular curve whose rational function field is K/k form by the preceding section a topological space. The rational points are however also in a 1–1 canonical correspondence with the elements of $\mathfrak{R}$, so that we may topologize $\mathfrak{R}$ by requiring this correspondence to be a homeomorphism. The topology thus defined is independent of the choice of the non-singular curve, because if we are given two such curves, the map sending a point of one into that point of the other which corresponds to the same place of K/k defines a birational everywhere biregular correspondence between the two curves, which is therefore a homeomorphism.

In connection with this topology we have the following two fundamental theorems about the local topological and analytic structure of $\mathfrak{R}$. Both are standard when the ground field is the complex numbers (see, e.g. Chevalley [8b]); the first of these was also proved by Lang for arbitrary locally compact ground fields [14]. (In the statements, by $t\mathfrak{p}$ we mean as usual the value of t under the place mapping $\mathfrak{p}$, so that $t\mathfrak{p} \in k$ if $\mathfrak{p}$ is a rational place.)

THEOREM 3. *Given K/k as described, let $\mathfrak{q}$ be a rational place of K and t a separating local uniformizing parameter at $\mathfrak{q}$.*

Then the map $\mathfrak{p} \rightarrow t\mathfrak{p}$ defines a homeomorphism of a neighborhood of $\mathfrak{q}$ with a neighborhood of 0 in k.

THEOREM 4. *With the hypotheses and notations of Theorem 3, let $x \in K$ be given and let its t-adic expansion in $K(\mathfrak{q})$, the completion of K at $\mathfrak{q}$, be $\sum a_\nu t^\nu$, $a_\nu \in k$.*

Then there exists a neighborhood U of $\mathfrak{q}$ in $\mathfrak{R}$ such that if $\mathfrak{p} \in U$, the series $\sum a_\nu(t\mathfrak{p})^\nu$ converges (except possibly for $\mathfrak{p} = \mathfrak{q}$), and to the limit $x\mathfrak{p}$.

PROOFS. Proving Theorem 3 first, we begin by finding a $y \in K$ such that $K = k(t, y)$, $t\mathfrak{q} = y\mathfrak{q} = 0$, and such that if $f(t, y) = 0$ is the irreducible polynomial equation over k satisfied by y and t, then $f_y(0, 0) \neq 0$. Thus $\mathfrak{q}$ is represented by the non-singular point $(0, 0)$ on the curve whose generic point is (t, y), so that the topology on $\mathfrak{R}$ in the neighborhood of $\mathfrak{q}$ is just the topology on the curve in the neighborhood of $(0, 0)$. The existence of such y for given t is proved for example in [14]. Now the map ϕ: $\mathfrak{p} \rightarrow t\mathfrak{p}$ is single-valued and continuous for all $\mathfrak{p}$, by definition of the topology on $\mathfrak{R}$. From the implicit function theorem, we know that for some neighborhood U of $(0, 0)$ on the curve, the complete solution of $f(t, y) = 0$ is given by a convergent power series $y = \sum b_\nu t^\nu = g(t)$. In other words, the map ψ: $t_0 \rightarrow (t_0, g(t_0))$ defines a single-valued continuous mapping of a neighborhood of 0 on the t-axis onto U. Since ψ is just the local inverse of ϕ, the mappings are locally homeomorphisms, which proves Theorem 3.

We prove Theorem 4 now, first for the special case $x = y$. Let $h(t) = \sum a_\nu t^\nu$ be the t-adic representation of y as an element of $K(\mathfrak{q})$; what has to be shown then is that $h(t)$ and $g(t)$ are identical power series. Since $h(t)$ satisfies $f(t, h(t)) = 0$ identically, and since it is convergent (the convergent power series being algebraically closed in the formal power series [1b]), it follows by the Substitution Theorem that $f(t_0, h(t_0)) = 0$ for t_0 lying within a suitable neighborhood T_0 of 0 on the t-axis. Furthermore, $h(0) = y\mathfrak{q} = 0$, so that the map $t_0 \rightarrow (t_0, h(t_0))$ sends T_0 onto a neighborhood of $(0, 0)$ which we may suppose is U, according to the way U was chosen above. Thus $h(t)$ and $g(t)$ agree on an interval containing 0, which means they are identical, since a non-zero power series can have only isolated zeros.

To complete the proof of Theorem 4, if x is an arbitrary element of K, we can write $x = G(t, y)/H(t, y)$. For $\mathfrak{p}$ in a neighborhood of $\mathfrak{q}$, (except possibly for $\mathfrak{p} = \mathfrak{q}$), we have $h(t\mathfrak{p}, y\mathfrak{p}) \neq 0$, so in this neighborhood:

$$x\mathfrak{p} = \frac{G(t\mathfrak{p}, y\mathfrak{p})}{H(t\mathfrak{p}, y\mathfrak{p})} = \frac{G(t\mathfrak{p}, h(t\mathfrak{p}))}{H(t\mathfrak{p}, h(t\mathfrak{p}))} = \sum a_\nu (t\mathfrak{p})^\nu.$$

The successive equalities use in turn that $h(t\mathfrak{p}, y\mathfrak{p}) \neq 0$, the proof of Theorem 4 for the case $x = y$, and the imbedding of K in $K(\mathfrak{q})$ together with the Substitution Theorem.

IV. THE TOPOLOGY ON THE DIVISOR CLASSES

In this part, as in the previous one, we will consider a separably generated function field in one variable K/k over a complete absolute-valued ground field k. In addition, we make two further assumptions: K/k must have a rational place, and it must be genus-preserving under extension of the constant field from k to $\bar{k}$, the (algebraically closed) completion of the algebraic closure of k. K/k is always genus-preserving if the characteristic is 0, as it will be in the principal application. It will be noticed that $\bar{k}$ is not necessarily a universal domain for k, since the two fields may very well be the same; by Ω therefore we will mean a field which is a universal domain for $\bar{k}$ as well as for k. We shall assume that the generic points of our varieties are generic with respect to $\bar{k}$. The varieties themselves, which will be defined over k, will be viewed as carrying only points with coordinates in $\bar{k}$, not in Ω, so that for example the generic points do not lie on the variety.

Our main object in this part is to define for use in the sequel two topologies on the group of divisor classes of degree 0 of K and then to prove them equivalent.

8. The Jacobi topology on the divisor class group of degree 0. With the above assumptions and conventions, let E denote any complete field between k and $\bar{k}$, KE/E the corresponding constant field extension of K/k; let Γ/k be a non-singular curve with rational function field K, and let Γ/E be the curve viewed over the ground field E and with rational function field KE. By taking the rational divisors of degree n of Γ/E and putting two of them into the same class if their difference is the divisor of zeros and poles of a function from KE, we obtain the set $\mathfrak{D}_n(E)$ of divisor classes of degree n of KE/E or of Γ/E; all the $\mathfrak{D}_n(E)$ are then united as usual to form $\mathfrak{D}(E)$, the group of rational divisor classes of Γ/E. Proceeding in a different way, from the group $\mathfrak{D}(\bar{k})$, we may select the subgroup $\mathfrak{D}'(E)$ consisting of those divisor classes of $\Gamma/\bar{k}$ which contain a divisor expressible as the difference of two positive divisors which are both rational with respect to E. We have then a canonical homomorphism of $\mathfrak{D}(E)$ onto $\mathfrak{D}'(E)$, which is an isomorphism if and only if the genera of KE/E and $K\bar{k}/\bar{k}$ are equal [1c]. Since we have assumed K/k to be in fact genus preserving, it is legitimate to identify the two groups.

Now according to a construction due to Chow [10], there exists a non-singular projective variety J/k, the Jacobi variety[3] of Γ, whose points correspond in a 1–1 algebraic fashion to the elements of the group $\mathfrak{D}_0(k)$. If $\mathfrak{D}_1'(E)$ is not empty, then Chow has also proved that this correspondence associates to the points rational with respect to E exactly the elements of $\mathfrak{D}_0'(E)$. In the present case, our assumption that K/k has a rational place guarantees that $\mathfrak{D}_1'(E)$ is never empty; coupling this with the genus-preserving assumption we see that the points of J rational with respect to E represent perfectly the group $\mathfrak{D}_0(E)$.

The group structure on $\mathfrak{D}_0(\bar{k})$ induces a group composition law on J, which may be described as a subvariety W of $J \times J \times J$ defined over k and everywhere regular over $J \times J$. Under the standard topology of §6, *J is a topological group*. For if a generic point of the composition law W is given by $(x, y, x*y)$

[3] By analogy with the use of the terms "Picard variety" and "abelian variety," we adopt the following usage: a variety is the "Jacobi variety" of a definite given curve or function field, while it is a "jacobian variety" by virtue of its possessing whatever intrinsic properties there are which single out jacobian varieties from general abelian varieties, i.e., it is a "jacobian variety" when the related curve or function field is unspecified and irrelevant.

where (x) and (y) are independent generic points of J, then since W is regular over $J \times J$ we have $k(x, y) = k(x, y, x*y)$; therefore the coordinates of $x*y$ are rational functions, everywhere defined, and hence continuous functions of (x) and (y). Similarly, the graph of (x, x^{-1}) is a subvariety $pr_{12}[W \cdot (J \times J \times e)]$ of $J \times J$ regular over J, whence the coordinates of (x^{-1}) are rational, continuous functions of (x).

The structure of a topological group is thus induced in turn on $\mathfrak{D}_0(E)$, and this structure is independent of the choice of J. Namely, any two Jacobi varieties for K/k are in birational, everywhere biregular correspondence under the mapping which sends a point of one into that point of the other which corresponds to the same element of $\mathfrak{D}_0(\bar{k})$. This map is therefore a homeomorphism as well as an isomorphism.

Let us remark finally that all the foregoing requires only that the ground field be topological.

9. The local topology on $\mathfrak{D}_0(E)$. Continuing now in the same situation, denote by g the genus of K/k and let $\mathfrak{M}$ be a fixed positive divisor of degree g, rational with respect to k. Then the set $\mathfrak{D}_g(E)$, (which we shall denote simply by $\mathfrak{D}_g$, since E will be fixed throughout), may be obtained by translating $\mathfrak{D}_0 = \mathfrak{D}_0(E)$ by $\mathfrak{M}$. We are going to define the second topology on $\mathfrak{D}_0$ by defining it on $\mathfrak{D}_g$ first and carrying it back by the opposite translation. However to give the topology on $\mathfrak{D}_g$, $\mathfrak{M}$ cannot be selected at random—it must be well-behaved, or as we shall say, "ordinary", in the following sense:

DEFINITION. A divisor $\mathfrak{M}$ of degree g will be called *ordinary* if

(i) it can be written $\mathfrak{M} = \mathfrak{m}_1 + \cdots + \mathfrak{m}_g$, where the $\mathfrak{m}_i$ are distinct places rational with respect to k, and

(ii) it is non-special,[4] i.e., dim $(-\mathfrak{M}) = 1$.

LEMMA. *For function fields of the type under consideration, there always exist ordinary divisors $\mathfrak{M} = \mathfrak{m}_1 + \cdots + \mathfrak{m}_g$ with the further property that no $\mathfrak{m}_i$ belongs to a preassigned finite set of places $\mathfrak{a}_1, \cdots, \mathfrak{a}_r$.*

PROOF. By assumption, K/k has a rational place $\mathfrak{q}$; let t be a separating local uniformizing parameter at $\mathfrak{q}$. By Theorem 3, t maps a neighborhood of $\mathfrak{q}$ homeomorphically onto a neighborhood of 0 in k. Any function $\phi \in K$ has a t-adic expansion $\phi(t) = \sum a_\nu t^\nu$, and by Theorem 4, $\phi(t\mathfrak{p}) = \phi\mathfrak{p}$ for $\mathfrak{p}$ in a neighborhood of $\mathfrak{q}$, so that it makes sense to view ϕ as a single-valued function of t in a neighborhood of 0 on the t-axis.

Let $\phi_1\, dz, \cdots, \phi_g\, dz$ be g linearly independent differentials of the first kind of K/k, so that the ϕ_i and $z \in K$. We claim first of all that det $|\phi_i\mathfrak{p}_j|$ is not identically 0 for all sets of rational places $\{\mathfrak{p}_j\}$ of K. For suppose det $|\phi_i\mathfrak{p}_j| \equiv 0$. Then det $|\phi_i(t_j)| \equiv 0$ for $t_1, \cdots, t_g$ taking values in some neighborhood of the origin (t_i is just a relabelling of t). Pick the smallest minor which is $\equiv 0$; let its

[4] By dim $(-\mathfrak{M})$ we mean the dimension of the vector space of elements of K which are $> -\mathfrak{M}$; the geometric dimension of the complete linear series determined by $\mathfrak{M}$ would of course be dim $(-\mathfrak{M}) - 1$.

rank be r. If $r = 1$, then $\phi_i(t) \equiv 0$. If $r > 1$, expand the minor by the r^{th} column, getting (after suitable renumbering)

$$\phi_1(t_r)h_1(t_1, \cdots, t_{r-1}) + \cdots + \phi_r(t_r)h_r(t_1, \cdots, t_{r-1}) \equiv 0.$$

Since $h_1(t_1, \cdots, t_{r-1})$ is a minor of rank $r - 1$, it is not $\equiv 0$; substituting in values for $t_1, \cdots, t_{r-1}$ which make it non-zero, we have

$$c_1\phi_1(t_r) + \cdots + c_r\phi_r(t_r) \equiv 0,$$

with $c_i \in k$, $c_1 \neq 0$. Therefore the t-adic expansion of $\sum c_i\phi_i$ is 0, which means that $\sum c_i\phi_i = 0$, contradicting the linear independence of the ϕ_i. In other words, if $(a_1, \cdots, a_g)$ are any set of values near 0 for the t_i for which

$$\det | \phi_i(a_j) | \neq 0,$$

then $\det | \phi_i\mathfrak{p}_j | \neq 0$, where $t\mathfrak{p}_j = a_j$.

We consider now the non-singular curve Γ/k whose function field is K/k, and we form the g-fold product $\Gamma^{(g)} = \Gamma \times \Gamma \times \cdots \times \Gamma$ (g factors). Then $\det | \phi_i\mathfrak{p}_j |$ is in a natural way a function on $\Gamma^{(g)}$ which we have just shown to be non-zero. Its locus of zeros and poles is therefore a $g - 1$ dimensional subvariety S of $\Gamma^{(g)}$. Furthermore, denoting for simplicity the points on Γ by the German letters representing the corresponding places, we see that the points $(\mathfrak{p}_1, \cdots, \mathfrak{p}_g)$ on $\Gamma^{(g)}$ for which two of the $\mathfrak{p}_i$ are the same or for which one of the $\mathfrak{p}_i$ coincides with one of the assigned places $\mathfrak{a}_1, \cdots, \mathfrak{a}_r$ lie on a bunch T of $g - 1$ dimensional subvarieties of $\Gamma^{(g)}$. Since the rational point $(\mathfrak{q}, \cdots, \mathfrak{q})$ has by Theorem 3 a whole g-dimensional neighborhood of rational points, it follows that S and T do not exhaust the rational points on $\Gamma^{(g)}$; let $(\mathfrak{m}_1, \cdots, \mathfrak{m}_g)$ be therefore a rational point not on S or T.

Then $\mathfrak{M} = \mathfrak{m}_1 + \cdots + \mathfrak{m}_g$ is the required ordinary divisor. Indeed, we have only to verify that it is non-special. We have, since $(\mathfrak{m}_1, \cdots, \mathfrak{m}_g) \notin S$, that $\det | \phi_i\mathfrak{m}_j | \neq 0$, so that the g linear equations $\sum_i c_i(\phi_i\mathfrak{m}_j) = 0$ have no non-trivial solution for the c_i. Since however $\phi_1, \cdots, \phi_g$ are a basis for the g-dimensional module of functions $> -(dz)$, (the divisor of dz being written (dz)), we conclude that there is no function $> -(dz)$ with zeros at $\mathfrak{m}_1, \cdots, \mathfrak{m}_g$. Thus $\dim(\mathfrak{M} - (dz)) = 0$, so that by the Riemann-Roch theorem, $\dim(-\mathfrak{M}) = 1$ and $\mathfrak{M}$ is consequently non-special. This completes the proof.

Continuing now the line of thought of the lemma, since the subvariety S is a closed set, the point $(\mathfrak{m}_1, \cdots, \mathfrak{m}_g)$ will have a neighborhood U_1 not meeting S. Moreover, since $\mathfrak{m}_i \neq \mathfrak{m}_j$, each $\mathfrak{m}_i$ is the center of a small neighborhood not containing any other $\mathfrak{m}_j$; the product of these forms a neighborhood U_2 of $(\mathfrak{m}_1, \cdots, \mathfrak{m}_g)$ since the natural Cartesian product topology on $\Gamma^{(g)}$ is the same as the topology it inherits from the ambient space. If to each point $(\mathfrak{p}_1, \cdots, \mathfrak{p}_g)$ rational with respect to E in $U = U_1 \cap U_2$ we associate the divisor

$$\mathfrak{P} = \mathfrak{p}_1 + \cdots + \mathfrak{p}_g,$$

we see that no divisor $\mathfrak{P}$ corresponds to two points of U and that the divisors $\mathfrak{P}$ are all non-special (applying the argument of the last paragraph of the lemma).

Now by the Riemann-Roch theorem, every divisor class in $\mathfrak{D}_g$ contains a positive divisor of degree g, and if this positive divisor is non-special, then it is the only one in its class. Let us agree to denote by $\{\mathfrak{P}\}$ the class of a given positive divisor $\mathfrak{P} = \mathfrak{p}_1 + \cdots + \mathfrak{p}_g$, and by U^* the set of all $\{\mathfrak{P}\} \in \mathfrak{D}_g$ such that $(\mathfrak{p}_1, \cdots, \mathfrak{p}_g) \in U$. Then what we have described is a 1–1 correspondence between the elements of a certain subset U^* of $\mathfrak{D}_g$ and the points on $\Gamma^{(g)}$ lying in a certain neighborhood U of $(\mathfrak{m}_1, \cdots, \mathfrak{m}_g)$. We now can define a topology on U^* by stipulating that this correspondence be a homeomorphism between the two sets; the so-defined topology in the neighborhood of $\{\mathfrak{M}\}$ is independent of the choice of Γ, and it is also clearly the same as that induced on $\mathfrak{D}_g$ by the corresponding local topology on $\mathfrak{D}_g(\bar{k})$ in the neighborhood of M.

If we now translate $\mathfrak{D}_g$ back by $-\mathfrak{M}$, by requiring the translation to be locally a homeomorphism, we get a topology defined on the classes of $\mathfrak{D}_0$ which belong to the translate of U^* by $-\mathfrak{M}$. We call this the local $\mathfrak{D}_0$ topology in the neighborhood of 0. It will follow from the next section that this topology is compatible with the group structure on $\mathfrak{D}_0$ and is independent of the choice of the ordinary divisor $\mathfrak{M}$ used to define it.

10. The local equivalence of the two topologies. We show now that the Jacobi topology and the local topology on $\mathfrak{D}_0$ coincide on a neighborhood of 0 for which the latter topology is defined. To do this, we must look a little more closely at the nature of the correspondence between the points on J rational with respect to E and the elements of $\mathfrak{D}_0$.

Let Γ be as before, with generic point $(x_1, \cdots, x_n)$, and let

$$\{A_i = (x_1^{(i)}, \cdots, x_n^{(i)})\},$$

$i = 1, \cdots, g$, be g generic points of Γ which are independent over $\bar{k}$. Then the function field of J is the so-called abelian function field, or symmetric compositum, $\bar{k}(A_1, \cdots, A_g)_S$: this is the subfield of $\bar{k}(A_1, \cdots, A_g)$ left fixed by the $g!$ automorphisms defined by the permutations $(A_1, \cdots, A_g) \to (A_{i_1}, \cdots, A_{i_g})$. An element $z \in \bar{k}(A_1, \cdots, A_g)_S$ is therefore a rational symmetric function of g points on Γ, and is consequently well-defined on positive divisors of degree g. Let $z_1, \cdots, z_r$ be the affine coordinates of J (we assume the identity point is at finite distance); then $\bar{k}(z) = \bar{k}(M)_S$, and $(z_1, \cdots, z_r)$ defines over k a rational mapping Φ of $\Gamma^{(g)}$ into J [19c].

Let $\mathfrak{M} = \mathfrak{m}_1 + \cdots + \mathfrak{m}_g$ be the ordinary divisor used in the construction of the local topology on $\mathfrak{D}_0$. It is convenient to assume that for each i the i^{th} coordinates of the g points $\mathfrak{m}_1, \cdots, \mathfrak{m}_g$ are all distinct: $x_i\mathfrak{m}_j \neq x_i\mathfrak{m}_k$ for $j \neq k$. This can always be arranged by multiplying the x_i by suitable constants—a trivial biregular transformation of Γ which will not disturb the local topology on $\mathfrak{D}_0$.

Also, we remark that we can turn $\mathfrak{D}_g$ in a non-canonical way into a group by defining $\{\mathfrak{A}\} + \{\mathfrak{B}\} = \{\mathfrak{A} + \mathfrak{B} - \mathfrak{M}\}$. This makes $\{\mathfrak{M}\}$ the identity element of $\mathfrak{D}_g$ and the translation map $\mu:\mathfrak{D}_0 \to \mathfrak{D}_g$ defined by $\{\mathfrak{A}_0\} \to \{\mathfrak{A}_0 + \mathfrak{M}\}$ is now an isomorphic mapping of $\mathfrak{D}_0$ onto $\mathfrak{D}_g$.

We have now schematically the mappings

$$\mathfrak{D}_0 \xrightarrow[\mu]{} \mathfrak{D}_g \xleftarrow[\Psi]{} \Gamma^{(g)} \xrightarrow[\Phi]{} J$$

where Ψ is the map of §9: $\Psi(\mathfrak{p}_1, \cdots, \mathfrak{p}_g) = \{\mathfrak{P}\} = \{\sum \mathfrak{p}_i\}$. Ψ^{-1} is in the large many-valued, but $\Phi\Psi^{-1}$ is single-valued, for that is partly what we mean by saying that J is the Jacobi variety of Γ.

THEOREM 5. *$\Phi\Psi^{-1}$ is an isomorphism and local homeomorphism between $\mathfrak{D}_g$ (topologized by the local topology in the neighborhood of $\{\mathfrak{M}\}$) and the points of J rational with respect to E.*

PROOF. $\Phi\Psi^{-1}$ is the explicit 1–1 correspondence between the points of J rational with respect to E and $\mathfrak{D}_g$; by definition of the group law on J, it is an isomorphism.

The map Ψ is 1–1 in a certain neighborhood U of $(\mathfrak{m}_1, \cdots, \mathfrak{m}_g)$, and by definition bicontinuous there, according to the previous section, so it is a homeomorphism. The map Φ is given by rational functions on $\Gamma^{(g)}$, and

$$\Phi(\mathfrak{m}_1, \cdots, \mathfrak{m}_g) = \Phi\Psi^{-1}\mu(0),$$

the identity point of J, which is at finite distance; therefore the denominators of the rational functions are not 0 in a neighborhood of $(\mathfrak{m}_1, \cdots, \mathfrak{m}_g)$ and Φ is consequently continuous. If $\Phi^{-1}(U) = V$, then Φ^{-1} must be single-valued on V since $\Psi\Phi^{-1}$ and Ψ are both locally 1–1. To prove the continuity of Φ^{-1}, we observe that it is given by the set of functions $(x_1^{(1)}, \cdots, x_n^{(g)})$. We know $x_j^{(i)}$ is algebraic over $k(z_1, \cdots, z_r)$; suppose the equation it satisfies is

$$f_j(x_j^{(i)}, z_1, \cdots, z_r) = 0.$$

Then the other roots are exactly $x_j^{(k)}$, $k = 1, \cdots, g$, so that if the coordinates of the identity point on J are $(e_1, \cdots, e_r)$, the roots of $f_j(x_j^{(i)}, e_1, \cdots, e_r) = 0$ are $x_j^{(1)}\mathfrak{m}_1, \cdots, x_j^{(g)}\mathfrak{m}_g$. Since these are assumed distinct, $\partial f_j/\partial x_j^{(i)} \neq 0$ at $(x_j^{(i)}\mathfrak{m}_i, e_1, \cdots, e_r)$, so according to the implicit function theorem, $x_j^{(i)}$ is locally a power series in $z_1, \cdots, z_r$ and therefore a continuous function. Φ^{-1} is therefore continuous, and so Φ, Ψ, and Φ^{-1} are locally homeomorphisms.

COROLLARY. *The local topology and the Jacobi topology on $\mathfrak{D}_0$ are locally equivalent. Under the local topology, therefore, $\mathfrak{D}_0$ and $\mathfrak{D}_g$ are locally topological groups, and the local topology is independent of the choice of the ordinary divisor $\mathfrak{M}$ which is used to define it.*

V. THE MAIN THEOREM FOR JACOBIAN VARIETIES

11. We can now prove the main theorem for the case of jacobian varieties; it is more convenient however to formulate it first as a statement about the group $\mathfrak{D}_0$. From now on, the ground field is of characteristic zero. We remark that the assumption made below in the statement of the theorem that K has a rational place will be later removed (Corollary to Theorem 7).

THEOREM 6. *Let K/k be a function field in one variable of genus g over a complete ultrametric field k of characteristic 0. Suppose K has a rational place $\mathfrak{o}$.*

Then the group $\mathfrak{D}_0 = \mathfrak{D}_0(k)$ of rational divisor classes of degree 0 of K contains a subgroup, of finite index if k is locally compact, analytically isomorphic and homeomorphic to $I \oplus I \oplus \cdots \oplus I$ (g summands), where I is the additive group of integers of k: $I = \{\alpha \mid \alpha \in k, \mid \alpha \mid \leqq 1\}$.

PROOF. We begin by selecting a non-singular model Γ of K, together with g linearly independent differentials of the first kind; these will be of the form $\phi_i\, dz$, for some fixed $z \in K$, and with $\Phi_i \in K$. We then choose by the Lemma of §9 an ordinary divisor $\mathfrak{O} = \mathfrak{o}_1 + \cdots + \mathfrak{o}_g$, where the $\mathfrak{o}_i$ avoid the finite number of places ramified or infinite with respect to $k(z)$. According to the proof of that Lemma, det $\mid \phi_i \mathfrak{o}_j \mid \neq 0$, a fact which we shall make use of shortly. Finally, by the approximation theorem [8a], we can find g elements $t_1, \cdots, t_g$ from K such that t_i uniformizes $\mathfrak{o}_i$ and has ordinal zero at $\mathfrak{o}_j$ ($j \neq i$).

With these choices of $\mathfrak{o}_i$, ϕ_i, and t_i we are in a position to imitate the classical Abel-Jacobi mapping. In order not to have to change neighborhoods continually, we remark that a finite number of times assertions will be made that some property holds in some neighborhood of 0 or a particular divisor; the conclusion of the argument will then be valid for the finite intersection of these neighborhoods; indeed, to avoid clumsiness we shall sometimes not even state explicitly that a result is valid only in a neighborhood, if it is obviously so. Finally, for convenience we shall let our spaces and varieties contain only points with coordinates in k; we can therefore drop the word "rational" in describing these points.

(1) **The map σ.** We define a map σ' of a neighborhood of $\mathfrak{O} = \sum_1^g \mathfrak{o}_i$, considered as a point on $\Gamma^{(g)}$, onto a neighborhood of (0) in T, an affine g-dimensional space over k:

$$\sigma' : (\mathfrak{p}_1, \cdots, \mathfrak{p}_g) \to (t_1\mathfrak{p}_1, \cdots, t_g\mathfrak{p}_g)$$

where we have for simplicity denoted a point of $\Gamma^{(g)}$ by German letters representing the corresponding places. By Theorem 4, and since the topology on $\Gamma^{(g)}$ is the same as the Cartesian product topology, σ' is locally a homeomorphism. From §§8, 9 we have the map

$$\Psi : \{\mathfrak{p}_1 + \cdots + \mathfrak{p}_g\} \to (\mathfrak{p}_1, \cdots, \mathfrak{p}_g)$$

of a subset of $\mathfrak{D}_g$ into $\Gamma^{(g)}$; this defines a local homeomorphism between the divisor classes of degree g in the neighborhood of $\{\mathfrak{O}\}$ and a neighborhood of

$$(\mathfrak{o}_1, \cdots, \mathfrak{o}_g)$$

on $\Gamma^{(g)}$ since $\mathfrak{O}$ is an ordinary divisor. The composite map $\sigma = \sigma'\Psi$ therefore is a homeomorphism between a neighborhood of $\{\mathfrak{O}\}$ in $\mathfrak{D}_g$ and a neighborhood of (0) in T:

$$\sigma : \mathfrak{D}_g \to T \quad \text{(locally) by} \quad \{\textstyle\sum_1^g \mathfrak{p}_i\} \to (t_1\mathfrak{p}_1, \cdots, t_g\mathfrak{p}_g).$$

(2) **The map τ.** Since $\phi_i\, dz/dt_j$ is an element of K, it is also an element of $K(\mathfrak{o}_j)$, the completion of K at $\mathfrak{o}_j$. As such it is therefore a power series in t_j, $\sum_{\nu=0}^{\infty} a_\nu^{(i,j)} t_j^\nu$ where $a_\nu^{(i,j)} \in k$; the series has no negative powers since $\phi_i\, dz$ is a differential of the first kind, and it converges in a neighborhood of zero by Theorem 5.

We interrupt at this point to remark that although Γ, z, ϕ_i, t_i, and $\mathfrak{o}_i$ are all defined over k, actually they are defined over a smaller field k_0 which is finitely generated over the rational numbers Q (or rather, the canonical image of Q in k). Namely, let a generic point of Γ over k be $(x) = (x_1, \cdots, x_n)$. To Q we adjoin the coefficients of the finite set of polynomial equations which $x_1, \cdots, x_n$ satisfy and which define Γ, the coefficients occurring in the expression of z, ϕ_i, and t_i as rational functions of the x_i, and the quantities $x_i \mathfrak{o}_j$. This gives in all only a finite number of adjunctions; the resulting field we call k_0, and we set $K_0 = k_0(x)$. K arises from K_0 by constant field extension. We can consider the $\mathfrak{o}_i$ to be rational places of K_0, the t_i as elements of K_0, and the $\phi_i\, dz$ as differentials of the first kind of K_0. K_0 is imbedded in $K_0(\mathfrak{o}_i)$ which is in turn imbedded in $K(\mathfrak{o}_i)$; therefore in the above power series expansion of $\phi_i\, dz/dt_j$, the $a_\nu^{(i,j)}$ belong not only to k, but to k_0 as well.

Resuming, we now set

$$f_i(t_j) = \int_0^{t_j} \phi_i\, dz = \sum_{\nu=0}^{\infty} \frac{a_\nu^{(i,j)} t_j^{\nu+1}}{\nu + 1}$$

where the integral sign is meant in a purely formal sense. The integrated series clearly converges, though perhaps in a smaller neighborhood than the original one.[5] Let U be a second affine g-space over k; we define a map τ of a neighborhood of the origin in T space into a similar neighborhood in U space by the equations:

$$u_i = F_i(t_1, \cdots, t_g) = f_i(t_1) + \cdots + f_i(t_g).$$

We claim that τ defines a local homeomorphism between the T and U spaces. Since mappings given by power series are continuous, it suffices to show that τ is invertible, i.e., that the system $u_i = F_i(t_1, \cdots, t_g)$ can be solved for the t_i as power series in the u_i, $t_i = G_i(u_1, \cdots, u_g)$. By the Inversion Theorem (§3), this will be the case provided det $| a_0^{(i,j)} | \neq 0$. Let $\phi_i\, dz/dt_j = g_{ij}$. We have, by choice of $\mathfrak{o}_i$,

$$0 \neq \det | \phi_i \mathfrak{o}_j | = \det \left| g_{ij} \mathfrak{o}_j \cdot \left(\frac{dt_j}{dz}\right) \mathfrak{o}_j \right| = \left(\frac{dt_1}{dz}\right) \mathfrak{o}_1 \cdots \left(\frac{dt_g}{dz}\right) \mathfrak{o}_g \det | g_{ij} \mathfrak{o}_j |$$

---

[5] If the valuation on K induces the trivial valuation on the rationals, the new series will have the same radius of convergence as the old. Suppose, however, it induces a p-adic valuation, the only other possibility. If the original series converges for $t = t_0$, i.e., if $| a_\nu t_0^\nu | \to 0$, then since, as may be verified, $| p^{\nu+1}/(\nu + 1) | \to 0$, we have $| a_\nu (t_0 p)^{\nu+1}/(\nu + 1) | \to 0$, so that the integrated series converges for $t = t_0 p$.

which means that $\det |a_0^{(i,j)}| = \det |g_{ij}\mathfrak{o}_j| \neq 0$, for since no $\mathfrak{o}_i$ is ramified over $k(z)$, $(dt_i/dz)\mathfrak{o}_i \neq \infty$.

(3) **Statement of the isomorphism problem.** We have established that $\tau\sigma$ is a local homeomorphism, therefore in particular 1–1. We have now to show that in a suitable neighborhood it is an isomorphism between $\mathfrak{D}_g$ and a neighborhood of (0) in the additive g-dimensional k-module U.

We choose $\mathfrak{O}$ as reference divisor; $\{\mathfrak{O}\}$ is thus the identity element in the topological group $\mathfrak{D}_g$. The classes in a neighborhood of $\{\mathfrak{O}\}$ are represented by the unique positive divisor of degree g they contain, so the addition of classes can be expressed by the addition of the divisors. Letting $\mathfrak{A} = \sum_1^g \mathfrak{a}_i$, $\mathfrak{B} = \sum_1^g \mathfrak{b}_i$, $\mathfrak{C} = \sum_1^g \mathfrak{c}_i$, we adopt the notation

$$t_i^a = t_i\mathfrak{a}_i, \qquad u_i^a = F_i(t_1^a, \cdots, t_g^a) = F_i(t^a),$$

so that $\sigma(A) = (t^a) = (t_1^a, \cdots, t_g^a)$ and $\tau(t^a) = (u^a)$, for example. Our task is to prove that $\mathfrak{A} + \mathfrak{B} = \mathfrak{C} \Leftrightarrow (u_1^a + u_1^b, \cdots, u_g^a + u_g^b) = (u_1^c, \cdots, u_g^c)$ for $\mathfrak{A}$, $\mathfrak{B}$ in a suitable neighborhood of $\mathfrak{O}$. Since $\tau\sigma$ is 1–1 it suffices to prove the implication in either direction.

(4) **The group law in T.** The first task is to study how $\mathfrak{A} + \mathfrak{B} = \mathfrak{C}$ looks after σ has been applied to it: what is the form of the group composition law when it is expressed in terms of the parameters $t_1, \cdots, t_g$?

Let $\mathfrak{A}$, $\mathfrak{B}$ be near $\mathfrak{O}$, rational with respect to k as usual, but at the same time independently generic with respect to k_0. In other words, if

$$(x) = x = (x_1, \cdots, x_n)$$

is a generic point of Γ/k, and if we write

$$(x^{a_i}) \quad \text{for} \quad (x_1^{a_i}, \cdots, x_n^{a_i}) = (x_1\mathfrak{a}_i, \cdots, x_n\mathfrak{a}_i),$$

then the requirement is that $k_0(x^{a_1}, \cdots, x^{a_g}, x^{b_1}, \cdots, x^{b_g})$ shall be contained in k and have transcendence degree $2g$ over k_0. Setting $k' = k_0(x^{a_1}, \cdots, x^{a_g})$, it is then known [19b] that the divisor $\mathfrak{C} = \mathfrak{A} + \mathfrak{B}$ is generic over k' and that $k'(x^{b_1}, \cdots, x^{b_g})_S = k'(x^{c_1}, \cdots, x^{c_g})_S$ where the subscript S means the symmetric compositum (§9).

Now $t_i^c = t_i\mathfrak{c}_i$ is a rational function of (x^{c_i}) and hence satisfies an irreducible equation over $k'(x^{b_1}, \cdots, x^{b_g})_S$; the other roots of this equation are exactly $t_i\mathfrak{c}_j$, $(j = 1, \cdots, g)$, the images of t_i^c under the automorphisms of $k'(x^c)$ over $k'(x^c)_S$. If we expand $x_1^{a_j}, \cdots, x_n^{a_j}$ as power series in t_j^a, and $x_1^{b_j}, \cdots, x_n^{b_j}$ as power series in t_i^b, and substitute these series into the equation for t_i^c, we conclude that t_i^c satisfies an equation with coefficients in $k_0[[t_1^a, \cdots, t_g^a, t_1^b, \cdots, t_g^b]]$, say $H_i(t^a, t^b; X) = 0$. Clearly, if $\mathfrak{A}'$, $\mathfrak{B}'$, $\mathfrak{C}'$ are another set of generic divisors, then $t_i^{c'}$ will satisfy the equation obtained by substituting $t_1^{a'}, \cdots, t_g^{b'}$ for $t_1^a, \cdots, t_g^b$ in the coefficients of $H_i(X) = 0$.

Let now $\mathfrak{A}$ and $\mathfrak{B}$ be any rational divisors of degree g near $\mathfrak{O}$, not necessarily generic, and let $\mathfrak{C} = \mathfrak{A} + \mathfrak{B}$. We know that $\mathfrak{C}$ varies continuously with $\mathfrak{A}$ and

$\mathfrak{B}$, so that $t_i^c = f(t^a, t^b)$, a continuous function of t^a and t^b. Further, since $\mathfrak{D} + \mathfrak{D} = \mathfrak{D}$, the g roots of $H_i(t^a, t^b; X) = 0$ at $(t^a) = (t^b) = 0$ are just $t_i\mathfrak{o}_j$ $(j = 1, \cdots, g)$. By the choice of t_i, we have $t_i\mathfrak{o}_i = 0$, $t_i\mathfrak{o}_j \neq 0$ $(i \neq j)$, which means that the root $X = 0$ of the equation $H_i(0, 0; X) = 0$ is simple. Consequently $\partial H_i/\partial X \neq 0$ at $(0, 0; 0)$ and we are thus free to apply the implicit function theorem, according to which the complete solution of $H_i(t^a, t^b; X) = 0$ in a neighborhood of $(0, 0; 0)$ is given by a power series $X = g(t^a, t^b)$. We claim now that $f(t^a, t^b)$ and $g(t^a, t^b)$ are precisely the same function. Namely, if $\mathfrak{A}$ and $\mathfrak{B}$ are generic divisors, we have established that t_i^c is a root of $H_i(t^a, t^b; X) = 0$, which means (since $g(t^a, t^b)$ gives locally the *complete* solution) that for generic values of (t^a) and (t^b), $f(t^a, t^b) = g(t^a, t^b)$. But since every element of k_0 is a limit of elements of k which are transcendental over k_0,[6] the continuity of the two functions implies their equality for all values of (t^a) and (t^b).

Summarizing our results:

t_i^c is that unique root of $H_i(t^a, t^b; X) = 0$ which is 0 when $(t^a) = (t^b) = (0)$. A triplet (t^a, t^b, t^c) in a sufficiently small neighborhood of $(0, 0, 0)$ *satisfies all the* $H_i = 0$ *if and only if* $\mathfrak{A} + \mathfrak{B} = \mathfrak{C}$.

(5) **The isomorphism proof continued.** The crux of the isomorphism proof is now the assertion that (with an obvious abridged notation), $G_i(u^a + u^b)$, $G(u^a)$, and $G(u^b)$ satisfy $H_i(t^a, t^b; t_i^c) = 0$ identically; here the G_i are the functions of part 2 of this proof which define τ^{-1}. This result we take over directly from the classical case as follows.

Letting k_0 be as before—say $k_0 = Q(\alpha_1, \cdots, \alpha_r; \beta_1, \cdots, \beta_s)$ where $\alpha_1, \cdots, \alpha_r$ is a transcendence base for k_0 over Q—we construct in the complex numbers an isomorphic replica of k_0 by choosing r independent transcendental complex numbers $\alpha_1^*, \cdots, \alpha_r^*$ and extending $Q(\alpha_1, \cdots, \alpha_r) \to Q(\alpha_1^*, \cdots, \alpha_r^*)$ to an isomorphism j of $k_0 : k_0 \to Q(\alpha_1^*, \cdots, \alpha_r^*; \beta_1^*, \cdots, \beta_s^*)$, where images under j are denoted by asterisks. We can extend j to $K_0 = k_0(x_1, \cdots, x_n)$; with the image field $K_0^* = k_0^*(x_1^*, \cdots, x_n^*)$ will be associated the images $\mathfrak{o}_i^*$, t_i^*, and $\phi_i^*\, dz^*$, and they will have all the algebraic properties of $\mathfrak{o}_i$, t_i , and $\phi_i\, dz$: rationality, non-speciality, ordinal at a prime are such properties, for example. Extending now the constant field to the complex number field, we can construct σ^*, the isomorphic replica of σ, with all the attendant properties. Also τ^* is constructed by setting $f_i^*(t_j^*) = \sum a_\nu^{(i,j)*}(t_j^*)^{\nu+1}/(\nu + 1)$; this can be done since the coefficients $a_\nu^{(i,j)}$ were in k_0, not merely in k. We get in this way the mappings

$$\{\mathfrak{p}_1^* + \cdots + \mathfrak{p}_g^*\} \xrightarrow[\sigma^*]{} (t_1^{*p^*}, \cdots, t_g^{*p^*}) \xrightarrow[\tau^*]{} [F_1^*(t^{*p^*}), \cdots F_g^*(t^{*p^*})]$$

together with $\tau^{*-1} : t_i^* = G_i^*(u_1^*, \cdots, u_g^*)$, since the coefficients of the series which solve an inversion problem are rational functions of the coefficients of

[6] Let β be any element of k which is transcendental over k_0, and such that $|\beta| < 1$. Then if $\alpha \in \bar{k}_0$, the elements $\alpha + \beta, \alpha + \beta^2, \cdots, \alpha + \beta^n, \cdots$ are all transcendental over k_0 and form a sequence converging to α.

the series which define the problem [2a]; here both the coefficients of F_i and G_i thus belong to k_0 so that they have images F_i^* and G_i^* under j in a natural way.

Again, since $K_0 = K_0^*$, the algebraic addition theorems for the positive divisors of degree g are the same for both fields; in particular, therefore, $t_i^{*c^*}$ is that unique root of $H_i^*(t^{*a^*}, t^{*b^*}; X) = 0$ which is 0 for $(t^{*a^*}) = (t^{*b^*}) = (0)$.

The classical Abel-Jacobi theorem to the effect that the composite mapping $\tau^*\sigma^*$ establishes an isomorphism between the divisor classes of degree g and the space U^* reduced modulo periods, now appears in our setting as the local (and therefore weaker) statement that in a neighborhood of the origin,

$$G_i^*(u^{*a^*} + u^{*b^*}), \qquad G^*(u^{*a^*}),$$

and $G^*(u^{*b^*})$ satisfy $H_i^* = 0$ for all values of the variables, and hence identically. Applying j^{-1}, we get precisely the same statement for $G_i(u^a + u^b)$, $G(u^a)$, $G(u^b)$, and $H_i = 0$.

(6) **Completion of the proof.** The proof is now quickly finished. Clearly $G_i(u^a + u^b)$ is a continuous function of (t^a) and (t^b); it satisfies the equation $H_i(t^a, t^b; X) = 0$; and since $u^a = u^b = 0$ when $t^a = t^b = 0$, it vanishes for $t^a = t^b = 0$. It follows from part 4 that $G_i(u^a + u^b) = t_i^c$, and so $\sigma^{-1}\tau^{-1}$ maps $u^a + u^b$ onto $\mathfrak{C} = \mathfrak{A} + \mathfrak{B}$.

For any real number $r > 0$ belonging to the value group of k, the set V_r: $\{(u_1, \cdots, u_g) \| u_i | \leqq r\}$ forms a subgroup of the additive group U, isomorphic to $I \oplus I \oplus \cdots \oplus I$ (g summands). Pick r small enough so that V_r is contained in all of the "sufficiently small" neighborhoods of (0) in U, so that $\tau^{-1}(V_r)$ is contained in all of the corresponding neighborhoods of T, and $\sigma^{-1}\tau^{-1}(V_r) = \mathfrak{H}_r$ in the corresponding neighborhoods of $\{\mathfrak{O}\}$ in $\mathfrak{D}_g$. Then $\sigma\tau$ will be defined in the neighborhood $\mathfrak{H}_r$ and it maps $\mathfrak{H}_r$ isomorphically onto V_r. $\mathfrak{H}_0 = \mathfrak{H}_r - \mathfrak{O}$ is then the required subgroup of $\mathfrak{D}_0$.

If k is locally compact, then by §§6, 7 $\mathfrak{D}_0$ is a compact topological group. $\mathfrak{H}_0$ is an open subgroup of $\mathfrak{D}_0$, hence it is of finite index.

12. From the equivalence of the two topologies on $\mathfrak{D}_0$ proved in §9 and the statements given in part III about the Jacobi variety we deduce immediately the following corollary.

COROLLARY. *Let* Γ *be a curve of genus* g *defined over a complete ultrametric field of characteristic* 0. *Suppose* Γ *has a non-singular rational point. Then the group of rational points on the Jacobi variety* J *of* Γ *contains a subgroup with the previous structure, of finite index if* k *is locally compact.*

For use in the next part, we add a few remarks. Let the varieties once more carry points from $\bar{k}$, though they are still defined over k. The isomorphism of the corollary may be envisaged as given by the local mapping $\tau\rho$ of J into U, where ρ is the map $\sigma(\Phi\Psi^{-1})^{-1}$. If J, T, and U carry points from $\bar{k}$, the results are exactly the same, except that now $\mathfrak{D}_g(\bar{k})$ must be substituted for $\mathfrak{D}_g$; viewed from this level, ρ and τ are still locally 1–1 and they carry points rational over E into points rational over E, where $k \subset E \subset \bar{k}$ and E is complete. Further, denoting as before by (z) the generic point of J and by (t) the set of local uniformizing parameters defining the map σ, we see that ρ is in the large an algebraic correspondence, given by the subvariety W of $J \times T$ whose generic point is (z, t); W is thus defined over k, and so therefore is ρ.

VI. The main theorem for abelian varieties

13. By an *abelian variety* is meant a group variety in projective space, that is, one whose points (with coordinates taken from some universal domain over the field of definition) form a group under an algebraic composition law which is defined everywhere.[7] It then follows that the group must be abelian and the variety nonsingular [19a]. If k is any field of definition for an abelian variety and its composition law, then the points on the variety which are rational with respect to k form a subgroup of the full group of points.

Theorem 7. *Let A be an abelian variety of dimension d, defined together with its composition law over k, a complete ultrametric field of characteristic* 0. *Then the group of points on A rational with respect to k contains a subgroup, of finite index if k is locally compact, analytically isomorphic and homeomorphic to $I \oplus I \oplus \cdots \oplus I$ (d summands), where I is as before* (*Theorem* 6) *the additive group of integers of k.*

Proof. We begin by imbedding A in a suitable jacobian variety, and to do this we make use of Chow and Matsusaka's abstract theory of Picard varieties.[8] The Picard variety of a given variety V/k is obtained by taking a generic 1-section $C(u)$ on V, defined over some purely transcendental extension $k(u)$ of k, and constructing the Jacobi variety $J(u)$ of the 1-section; $J(u)$ is thus also defined over $k(u)$. The Picard variety of V is then the maximal abelian subvariety of $J(u)$ which is defined over k. Applying this to our situation, we observe that A is defined over some field k_0 finitely generated over the rational

[7] Since Weil has proved that his abstract abelian varieties can be imbedded in projective space [18] and Matsusaka has shown that this can be done without extending the ground field, the notion of abelian variety as defined in [19] essentially coincides with the one used here.

[8] In view of the difficulty of the abstract theory and since not all of it has been published yet, we indicate two alternative routes which may be followed to make this imbedding.

(i) Since we are in characteristic 0, we may use instead the transcendental (complex) theory of Picard varieties which is both considerably simpler and published [9, 13]. One only needs to construct the appropriate isomorphism to take over the required results from that theory, all of which appear in [9].

(ii) On the other hand, the theory of Picard varieties may be avoided entirely. By two elementary theorems of Weil, [19, prop. 130, p. 125; th. 21, p. 77], every abelian variety A^d is a homeomorphic image of a product of the Jacobi varieties $J_1 \times \cdots \times J_d$ of d curves $C_1, \cdots, C_d$ on A. In essentially the same way as above, it is easily seen that one can choose the C_i so that each is defined over k and has a rational point. Now it follows from Poincaré's theorem [19, cor. 2, p. 95] that A is isogenous to an abelian subvariety B of $J_1 \times \cdots \times J_d$, also defined over k. Since our theorem is a local one, and since A and B, being isogenous, are locally isomorphic, it suffices to prove the theorem for B.

One has therefore to prove the theorem for an abelian subvariety of a product of Jacobi varieties of curves with rational points; this can then be done just as in the text, *mutatis mutandis*.

numbers; so therefore is A', its Picard variety. By the duality theory, A is in turn the Picard variety of A'. The identity of A' is a non-singular point, rational with respect to k_0, which means that we can find a point P nearby which is rational with respect to k, but generic with respect to k_0 [14]. We pass the generic 1-section $C(u)$ through P, choosing $(u) \in k$ but generic with respect to k_0, and we construct $J(u)$, which is therefore defined over k. Now A is contained in $J(u)$, since it is the Picard variety of A', and we have thus achieved the following situation:

(1) *A^d is a subvariety of the Jacobi variety J^g of some curve C with a non-singular rational point P; all are defined over k.*

We can now apply the corollary to Theorem 6. Let J_0 be the subgroup of the rational points of J which is isomorphic to $I \oplus \cdots \oplus I$ (g summands). Under the algebraic correspondence ρ defined in §12, A goes into a bunch of algebraic varieties $\rho(A)$, and $J_0 \cap A$ goes into a subset A_T of $\rho(A)$. The map τ now carries A_T into a subset A_U of U-space; the diagram is therefore:

$$\begin{array}{ccccc} J & \xrightarrow{\quad\rho\quad} & T & \xrightarrow{\quad\tau\quad} & U \\ | & & | & & | \\ A & \longrightarrow & \rho(A) & \longrightarrow & \tau\rho(A) \\ | & & | & & | \\ J_0 \cap A & \longrightarrow & A_T & \longrightarrow & A_U \end{array}$$

We assert now that

(2) *A_T and A_U are algebroid varieties of dimension d, defined over k.*

This is almost self-evident in view of the concluding remarks of §§5 and 13. We know that J, A, and ρ are defined over k; therefore $\rho(A)$ is a bunch of algebraic varieties, defined over k. Since ρ is 1–1 in a neighborhood of the identity on J, it has no fundamental points there, and so the dimension of any component of the bunch passing through (0) is d, the dimension of A. Thus A_T is seen to be an algebroid variety of dimension d, defined over k. The statement for A_U follows from the observation that τ is a regular transformation, defined over k (§5).

We now work definitely over $\bar{k}$, so that the spaces and algebroid varieties in them carry points from $\bar{k}$. As previously remarked, the system of mappings and isomorphisms are not disturbed by the addition of these new points.

Given a prime algebroid ideal $\mathfrak{p}$ of dimension d defined over k, using a construction described by Lefschetz [15a], one can make a non-singular linear transformation over k of the coordinates $(u_1, \cdots, u_g)$ such that, if we denote the new coordinates and the new ideal still by (u) and $\mathfrak{p}$, then $\mathfrak{p}$ contains a set of convergent power series of the form:

$$g_i(u_1, \cdots, u_d, u_{d+1}, \cdots, u_{d+i}) \qquad i = 1, \cdots, g - d$$

where each g_i is a polynomial in the last variable u_{d+i}, whose leading coefficient $c_i(u_1, \cdots, u_d)$ is a convergent power series in the first d variables only. The

g_i have this further important property: setting $c(u_1, \cdots, u_d) = \prod_i c_i(u)$, then an arbitrarily given convergent series $g \in \mathfrak{p}$ if and only if one can write $c^\alpha g = \sum \gamma_i g_i$ for some α and some set of convergent power series γ_i.[9]

Let B denote the set of common zeros of the g_i inside some neighborhood U_1 in which c and the g_i are holomorphic. Let $(f_1, \cdots, f_s)$ be a basis for $\mathfrak{p}$ and let U_2 be the associated neighborhood in the sense of §5, so that an algebroid variety A of $\mathfrak{p}$ is given by the common zeros of the f_i lying inside U_2. First of all, within any neighborhood $V \subset U_1 \cap U_2$ we have, since A is an algebroid variety,

$$A \cap V \subset B \cap V.$$

In the second place, according to the above we can write the $c^{\alpha_j} f_j = \sum \gamma_i^{(j)} g_i$ for each series f_j, so that if $V \subset U_1 \cap U_2$ is now chosen to be a neighborhood in which all the $\gamma_i^{(j)}$ are holomorphic, we see that within V a common zero of the g_i either annihilates all the f_i or else makes c vanish. Denoting the set of zeros of c by C, we have therefore inside V,

$$B - B \cap C \subset A \subset B.$$

If $(a_1, \cdots, a_d)$ is any point in $U_1 \times \cdots \times U_d$ near (0) and not on C, it follows that $c_i(a_1, \cdots, a_d) \neq 0$, $i = 1, \cdots, g - d$; from this, from the above inclusion relations, and from the form of the g_i we conclude that A intersects the linear variety $\{u_1 = a_1, \cdots, u_d = a_d\}$ in at least one, but only finitely many points.

We will now apply these remarks to A_U to prove

(3) *A_U is the intersection of a neighborhood of the origin in U with a linear variety L through* (0), *of dimension d and defined over k.*

Each of the irreducible components of A_U is of dimension d and defined over k; call the corresponding ideals $\mathfrak{p}_1, \cdots, \mathfrak{p}_n$, with series $c^1, \cdots, c^n$ respectively associated by Lefschetz' theorem with them. It is easily seen that a linear transformation can be made such that all the $\mathfrak{p}_i$ will simultaneously contain special sets of power series with the above properties. Suppose this done. Since J_0 and A are groups, so is $J_0 \cap A$, and since $\tau\rho$ is an isomorphism, A_U is a subgroup of U. By the above, the projection of A_U on $U_1 \times \cdots \times U_d$ is a neighborhood of (0) with perhaps some of the common zeros of the c^i deleted; it is also however a subgroup since the projection map is a homomorphism. It must be then that the projection is actually the whole neighborhood of (0), and the projection map is thus locally an epimorphism. Since by the above, for "general" choice of $(a_1, \cdots, a_d)$, there are only finitely many points of the form

$$(a_1, \cdots, a_d, a_{d+1}, \cdots, a_g)$$

on A_U, the fact that the projection is a homomorphism implies that for *all* choices of $(a_1, \cdots, a_d)$ this is true, in particular therefore for $(a_1, \cdots, a_d) =$

[9] Lefschetz proves this only for formal power series; it is easily seen, however, that if one starts with the ring of convergent power series, then his arguments still go through, yielding in the end convergent power series with the same formal properties.

$(0, \cdots, 0)$. Now the kernel consists exactly of the set of points in A_U of the form $(0, \cdots, 0, a_{d+1}, \cdots, a_g)$. If one of the a_i were non-zero, then the infinite set of points $(0, \cdots, 0, na_{d+1}, \cdots, na_g)$ for $n = 1, 2, \cdots$ would all be different, all in the neighborhood because $\bar{k}$ is ultrametric, and all in A_U, which we have seen to be impossible. Therefore all the $a_i = 0$, and the kernel consists of $(0, \cdots, 0)$ only.

This means that the projection map is locally an isomorphism, so that over each point $(a_1, \cdots, a_d, 0, \cdots, 0)$ there lies exactly one point of A_U. Consequently, as one can see directly from the set of equations, A_U must consist of one component only, a linear branch, i.e., the g_i must be linear in the last variable. Thus the set can be written:

$$u_{d+i} = h_i(u_1, \cdots, u_d), \qquad i = 1, \cdots, g - d, \qquad h_i \in k((u_1, \cdots, u_d)).$$

Since A_U is a group this means that the h_i satisfy

$$h_i(u_1 + v_1, \cdots, u_d + v_d) = h_i(u_1, \cdots, u_d) + h_i(v_1, \cdots, v_d)$$

for all values of (u) and (v) in the neighborhood. But this implies that the relation is a formal identity between the power series in (u) and (v), therefore, by constructing the appropriate isomorphism and taking over the corresponding result from the complex numbers, the h_i must be linear polynomials in $u_1, \cdots, u_d$. This shows that A_U is contained in a linear variety of dimension d defined over k; since A_U is of dimension d, (3) follows immediately.

The proof is now clear. We pass down to k again, so that we are considering now only the points rational with respect to k. We know that $\tau\rho$ is an analytic isomorphism and homeomorphism of some suitable subgroup J_0 of J with the corresponding subgroup U_0 of U; it therefore carries $A_0 = A \cap J_0$, a subgroup of the point group of A, isomorphically onto $A_U \subset U$, a subgroup of the group of points on the linear variety L, formed of the points lying in a certain neighborhood of (0) on L. Since L is of dimension d and defined over k, its group of points is isomorphic and homeomorphic to $k \oplus k \oplus \cdots \oplus k$ (d summands); therefore A_U is isomorphic and homeomorphic to $I \oplus I \oplus \cdots \oplus I$ (d summands).

If k is locally compact, the finite index of A_0 in A follows either directly as before, or from the finite index of J_0 in J.

By applying Theorem 7 to the case $A = J$, the Jacobi variety of a curve over k, we deduce immediately the

COROLLARY. *Theorem* 6 *is valid without the assumption that K contains a rational place*; *the corollary is valid without the assumption that* Γ *contains a non-singular rational point.*

14. We conclude with three observations which supplement Theorem 7.

1. *Theorem* 7 *remains true if k is itself not complete, but is nevertheless an infinite algebraic extension of a complete field F.* For any point on A rational with respect to k is actually rational with respect to some finite algebraic extension $F(\alpha)$ of F, over which A and all the mappings are defined. $F(\alpha)$ is automatically itself

complete, and Theorem 7 applies to A over $F(\alpha)$; this tells us what element of d-dimensional k-space our point gets mapped into. The rest follows from the compatibility of the isomorphic mapping with constant field extension.

2. *The isomorphism is unique up to a homogeneous linear transformation of the space U.* If Φ_1 and Φ_2 are two such isomorphisms of a subgroup of A^d onto a neighborhood of (0) in U^d, then $\Phi_1\Phi_2^{-1}$ defines an analytic isomorphism of the neighborhood onto itself. Such an isomorphism can only be a homogeneous linear transformation by the same reasoning with power series identities used in the proof of statement 3 of Theorem 7.

3. *Let $A^n \supset B^m$ be abelian varieties, and let C^{n-m} be an abelian subvariety of A such that if x is any point of A, $x = y + z$, where y, z are points of B, C respectively* [19d]. *Then the local isomorphism carrying A^n onto a neighborhood V_0 of* (0) *in V^n takes B^m and C^{n-m} onto neighborhoods W_0 and X_0 of* (0) *in two complementary linear subspaces W^m and X_{n-m} of V^n*; i.e. *to the algebraic splitting of A corresponds an analytic splitting*. Imbed A in a jacobian variety J^g. What Theorem 7 proves is that the isomorphism of J onto $U_0 \subset U^g$ carries any abelian subvariety of J onto a neighborhood of (0) in a linear subspace of U^g; applying this in turn to A, B, and C the result follows, W and X being complementary because they span U^n and have complementary dimensions.

PRINCETON UNIVERSITY AND MASSACHUSETTS INSTITUTE OF TECHNOLOGY

BIBLIOGRAPHY

[1] E. ARTIN, Algebraic numbers and algebraic functions, part I, Mimeographed lecture notes, publ. New York Univ. (1951); (a) p. 40; (b) p. 44; (c) p. 301.

[2] S. BOCHNER and W. T. MARTIN, Several complex variables, Princeton 1948; (a) chapter I; (b) chapter IX.

[3] N. BOURBAKI, Eléments de mathématique, Livre III, chap. IX, Actualités Scientifiques et Industrielles, no. 1045, Paris, Hermann et Cie, 1948, p. 59.

[4] H. CARTAN, *Idéaux de fonctions analytique de n variables complexes*, Ann. École Norm., 61 (1944); (a) part I; (b) p. 191.

[5] H. CARTAN, Théorie des fonctions de plusieurs variables, Mimeographed seminar notes (1951–2), chap. X.

[6] C. CHABAUTY, *Sur les équations diophantiennes liées aux unités d'un corps de nombres algébriques fini*, Annali di Math. (IV), 17 (1938), pp. 130–8.

[7] C. CHEVALLEY, *Intersections of algebraic and algebroid varieties*, Trans. Amer. Math. Soc., 57 (1945), p. 59.

[8] C. CHEVALLEY, *Introduction to the theory of algebraic functions of one variable*, Math. Surveys, no. VI, Amer. Math. Soc. (1951); (a) p. 12; (b) pp. 135–7.

[9] W.-L. CHOW, *On Picard varieties*, Amer. J. Math., 74 (1952), p. 895.

[10] W.-L. CHOW, *The Jacobian variety of an algebraic curve*, Amer. J. Math., 76 (1954), p. 453.

[11] E. GOURSAT and E. R. HEDRICK, A course in mathematical analysis, vol. I, Ginn and Co. 1904, p. 49.

[12] H. HASSE, Zahlentheorie, Berlin, Akademie-Verlag 1949, p. 191.

[13] J. IGUSA, *On the Picard varieties attached to algebraic varieties*, Amer. J. Math., 74 (1952), p. 1.

[14] S. LANG, *Some applications of the local uniformization theorem*, Amer. J. Math., 76 (1954), p. 362.

[15] S. LEFSCHETZ, Algebraic geometry, Princeton 1953; (a) pp. 83–4; (b) p. 90.
[16] E. LUTZ, *Sur l'équation* $y^2 = x^3 - Ax - B$ *dans les corps* p-*adiques*, J. Reine Angew. Math., 177 (1937), p. 204.
[17] A. WEIL, *Number-theory and algebraic geometry*, Proc. Int. Cong. Math., II (1950), p. 90.
[18] A. WEIL, *On the projective imbedding of abelian varieties*, Ann. of Math. Study in honor of S. Lefschetz (to appear), Princeton.
[19] A. WEIL, Variétés abéliennes et courbes algébriques, Actualités Scientifiques et Industrielles, no. 1064 (Publ. Inst. Math., Strasbourg, VIII) Paris, Hermann et Cie 1948; (a) pp. 18, 25; (b) p. 62; (c) §36; (d) p. 94.