# APPROXIMATION THEORY AND THE RANK OF ABELIAN VARIETIES OVER LARGE ALGEBRAIC FIELDS

*By* GERHARD FREY *and* MOSHE JARDEN

**Introduction**

The following theorem is well known (cf. Lang, [**6**], p. 71).

*Let $k$ be a field of finite type (i.e. a field which is finitely generated over its prime field). Let $A$ be an abelian variety defined over $k$. Then the set $A(k)$ of the $k$-rational points of $A$ form a finitely generated abelian group.*

In particular it follows that the rank of $A(k)$ is finite.

One may ask what happens to the rank if we replace $k$ by a field $K$ which is of infinite type. To answer this question one has first to exclude the case where $K$ is an algebraic extension of a finite field, since in this case $A(K)$ is a torsion group. The first fields of interest are therefore the algebraically closed fields of which none is the algebraic closure of a finite field. For such a field $K$ it is relatively easy to show that the rank of $A(K)$ is equal to the cardinality of $K$. (We assume here once for all that $\dim A \geqslant 1$.) A proof of this fact is included in this work. Another proof was indicated by J.-P. Serre in a letter.

Our main result is the following.

*Let $k$ be an infinite field of finite type and let $e$ be a positive integer. Denote by $k_s$ the separable closure of $k$. For every $(\sigma) = (\sigma_1, \ldots, \sigma_e) \in \mathcal{G}(k_s/k)^e$ put $k_s(\sigma)$ for the fixed field in $k_s$ of $(\sigma_1, \ldots, \sigma_e)$. Then almost all $(\sigma) \in \mathcal{G}(k_s/k)^e$ have the following property: if $A$ is an abelian variety defined over $k_s(\sigma)$ and $\dim A \geqslant 1$ then the rank of $A(k_s(\sigma))$ is infinite.*

Here 'almost all' is used in the sense of the Haar measure defined on the group $\mathcal{G}(k_s/k)$ with respect to its Krull topology. (More details are given in § 1.)

This result may give the impression that the fields $k_s(\sigma)$ behave like algebraically closed fields. This is not the case since, for example, it can be shown that if $k$ is a field of finite type and $e \geqslant 2$ then for almost all $(\sigma) \in \mathcal{G}(k_s/k)^e$ the field $k_s(\sigma)$ contains only a finite number of roots of unity.

Two main steps are involved in the proof of the theorem. First, we establish a general approximation theory modulo real valuations (that is valuations with real values) for the fields $k_s(\sigma)$ which holds for an arbitrary abstract variety $V$. For global fields $k$, it can be formulated as follows.

*Let $v$ be a real valuation of $k$. Then for almost all $(\sigma) \in \mathcal{G}(k_s/k)^e$ and for every absolute variety $V$ defined over $k$, the set $V_{\mathrm{sim}}(k_s(\sigma) \cap k_v)$ of the $k_s(\sigma) \cap k_v$-rational simple points of $V$ is $v$-dense in the set $V_{\mathrm{sim}}(k_v)$.*

(Here $k_v$ is the completion of $k$ with respect to $v$.)

Secondly, we study abelian varieties over complete fields and by using the theory of Néron on minimal models ([**13**]), we prove the following theorem.

*Let $K$ be a complete field with respect to a discrete real valuation $v$, whose residue field is perfect and let $L$ be a proper, finite, unramified Galois extension of $K$. If $A$ is an abelian variety defined over $K$ then there exists a point $P \in A(L)$ and a $v$-open neighbourhood $U$ of $P$ in $A(L)$ such that for every $Q \in U$ and for every integer $m \neq 0$, $mQ \notin A(K)$.*

The authors wish to acknowledge their indebtedness to Bronislav Weinrab for suggesting the problem, to W. D. Geyer for his important contributions to the work, and to P. Roquette for his comments and encouragement.

## 1. The Haar measure of a Galois group

In this section we mention briefly some notions which have already been introduced in [**5**].

Let $k$ be any field, $k_s$ its separable closure, and $\mathcal{G}(k_s/k)$ the Galois group of $k_s$ over $k$. It is well known that $\mathcal{G}(k_s/k)$ is a compact group under the Krull topology. There is therefore a unique way to define a Haar measure $\mu$ on the Borel field of $\mathcal{G}(k_s/k)$ such that $\mu(\mathcal{G}(k_s/k)) = 1$. If $l$ is a finite separable extension of $k$ then $\mu(\mathcal{G}(k_s/l)) = 1/[l : k]$. We complete $\mu$ by adjoining to the Borel field all the subsets of measure 0 and denote the completion also by $\mu$. More generally, for a positive integer $e$, we shall consider the product space $\mathcal{G}(k_s/k)^e$ and denote by $\mu^e$ or $\mu$ again the appropriate product measure (also completed).

A sequence $(k_i/k)_{i=1}^{\infty}$ of algebraic field extensions is said to be *linearly disjoint* if, for every $n \geqslant 1$, $k_{n+1}$ is linearly disjoint from $k_1 \ldots k_n$ over $k$, in the usual sense, that is, if $[k_{n+1} : k] = [k_1 \ldots k_n k_{n+1} : k_1 \ldots k_n]$.

The following lemma is a special case of Lemma 1.10 of [**5**].

LEMMA 1.1. *Let $k'$ be a finite separable extension of $k$. If $(k_i/k')_{i=1}^{\infty}$ is a linearly disjoint sequence of finite extensions of the same degree then*

$$\mu\left(\bigcup_{i=1}^{\infty} \mathscr{G}(k_s/k_i)^e\right) = \frac{1}{[k' : k]^e}.$$

We shall frequently use the simple fact that the intersection of a denumerable number of sets of measure 1 is again a set of measure 1. It is also clear that if $\{S_i\}_{i=1}^{\infty}$ and $\{T_i\}_{i=1}^{\infty}$ are two denumerable sets of measurable sets such that, for every $i$, $S_i$ is almost equal to $T_i$ then $\bigcup_{i=1}^{\infty} S_i$ is almost equal to $\bigcup_{i=1}^{\infty} T_i$.

## 2. Linearly independent points on elliptic curves

In this section we illustrate our methods for the special case of an elliptic curve defined over the field $\mathbf{Q}$ of the rational numbers. The main result we achieve here will be stronger than the result for arbitrary abelian varieties.

Let $\mathscr{E}$ be an elliptic curve defined over $\mathbf{Q}$ which has a rational point over $\mathbf{Q}$. Without loss of generality we can suppose that $\mathscr{E}$ has an affine representative which is defined by an equation

$$Y^2 = X^3 + aX + b, \tag{1}$$

where $a, b \in \mathbf{Z}$ and $4a^3 + 27b^2 \neq 0$ (Cassels, [1], p. 211). Thus $\mathscr{E}$ turns out to be an abelian variety whose zero point is the point at infinity of (1).

If $p$ is a prime we denote by $v_p$ the appropriate valuation of the field $\mathbf{Q}_p$ of p-adic numbers. Similar notation holds for a prime ideal of an arbitrary number field $k$.

If $V$ is a variety defined over a field $k$, we denote by $V(k)$ the set of points of $V$ rational over $k$.

LEMMA 2.1. *Let $p$ be an odd prime. Put $c = 1 + ap^2 + bp^3$. Then $P = (1/p, \sqrt{(c/p)}/p)$ is a point of $\mathscr{E}$, rational over $\mathbf{Q}(\sqrt{(c/p)})$ and, for every integer $m \neq 0$, $mP$ is not rational over $\mathbf{Q}$.*

*Proof.* The field $k = \mathbf{Q}(\sqrt{(c/p)})$ is a quadratic extension of $\mathbf{Q}$ which ramifies totally over $p$. Therefore there exists a unique prime ideal $\mathfrak{p}$ of $k$ lying over $p$ and we have

$$v_{\mathfrak{p}}(z) = 2v_p(z) \quad \text{for all } z \in \mathbf{Q}_p. \tag{2}$$

If we put $\pi = \sqrt{(p/c)}$, we have $\pi \in k$ and $v_{\mathfrak{p}}(\pi) = 1$. We consider $\mathbf{Q}_p$ as a subfield of $k_{\mathfrak{p}}$. One can prove that every point $(x', y')$ satisfying (1) and rational over $k_{\mathfrak{p}}$ can be represented in the form $(x', y') = (\xi\pi^{-2n}, \eta\pi^{-3n})$, where $\eta$ and $\xi$ are integral in $k_{\mathfrak{p}}$ and $n = \max(0, -\frac{1}{2}v_{\mathfrak{p}}(x')) = \max(0, -\frac{1}{3}v_{\mathfrak{p}}(y'))$ is an integer. Thus we obtain a function $n = n(P')$ defined for every point

$P' \in \mathscr{E}(k_\mathfrak{p})$ $(P' \neq 0)$. This function has the following property (Lutz, [9]).

(3) $\quad n(P') \geqslant 1 \Rightarrow n(mP') = n(P') + 2v_p(m)$ for every integer $m \neq 0$.

From (2), it follows that if $P' = (x', y') \in \mathscr{E}(\mathbf{Q}_p)$ then $v_\mathfrak{p}(y')$ is even and hence $n(P')$ is even.

Now let $m$ be a non-zero integer. From the definitions, it follows that $P$ is a point of $\mathscr{E}(k)$ for which $n(P) = 1$. Hence, according to (3),

$$n(mP) = 1 + 2v_p(m)$$

that is, $n(mP)$ is an odd integer. This means that $mP \notin \mathscr{E}(\mathbf{Q}_p)$ and in particular $mP$ is not rational over $\mathbf{Q}$.

THEOREM 2.2. *There exists a linearly independent sequence*

$$(P) = (P_1, P_2, P_3, \ldots)$$

*of points of* $\mathscr{E}(\tilde{\mathbf{Q}})$. *Moreover, for every positive integer* $e$ *and for almost all* $(\sigma) = (\sigma_1, \ldots, \sigma_e) \in \mathscr{G}(\tilde{\mathbf{Q}}/\mathbf{Q})^e$ *there exists a subsequence* $(P_{n(1)}, P_{n(2)}, P_{n(3)}, \ldots)$ *of* $(P)$ *rational over* $\tilde{\mathbf{Q}}(\sigma)$.

*Proof.* We build by induction an infinite sequence $p_1, p_2, p_3, \ldots$ of odd primes such that if we put $c_i = 1 + ap_i^2 + bp_i^3$ and $k_i = \mathbf{Q}(\sqrt{(c_i/p_i)})$ then $v_{p_i}(c_i) = 0$ and $(k_i/\mathbf{Q})_{i=1}^{\infty}$ will be linearly disjoint.

Suppose we have already found odd primes $p_1, \ldots, p_{n-1}$, such that $v_{p_i}(c_i) = 0$ and $(k_i/\mathbf{Q})_{i=1}^{n-1}$ is linearly disjoint. Put $K = k_1 \ldots k_{n-1}$, then $K$ is a number field. It is not difficult to prove that the polynomial $g(X, Y) = X^3Y^2 - 1 - aX^2 - bX^3$ is absolutely irreducible. We can therefore find an odd prime $p_n$ which does not divide the denominators of $a$ and $b$ such that the polynomial $g(p_n, Y)$ is irreducible over $K$ (Lang, [6], p. 148). It follows immediately that $v_{p_n}(c_n) = 0$ and that $k_n$ is a quadratic extension of $\mathbf{Q}$, linearly independent of $K$. This ends the induction.

According to Lemma 2.1, $P_n = (1/p_n, \sqrt{(c_n/p_n)/p_n})$ is a point in $\mathscr{E}(k_n)$ and, for every non-zero integer $m$, $mP_n \notin \mathscr{E}(\mathbf{Q})$. Suppose now that there exist integers $m_1, \ldots, m_n$ such that $m_1P_1 + \ldots + m_{n-1}P_{n-1} + m_nP_n = 0$ and $m_n \neq 0$. $P_1, \ldots, P_{n-1}$ belong to $\mathscr{E}(k_1 \ldots k_{n-1})$, hence $m_nP_n \in \mathscr{E}(k_1 \ldots k_{n-1})$. On the other hand $m_nP_n \in \mathscr{E}(k_n)$, hence $m_nP_n$ is rational over $k_n \cap k_1 \ldots k_{n-1} = \mathbf{Q}$, which is a contradiction. This means that the sequence $(P) = (P_1, P_2, P_3, \ldots)$ is linearly independent.

By this we have proved the first part of the theorem. Now let $e$ be a positive integer. For every positive integer $r$, denote by $S_r$ the set of all $(\sigma) \in \mathscr{G}(\tilde{\mathbf{Q}}/\mathbf{Q})^e$ for which there exist $r$ points of the sequence $(P)$ which are rational over $\tilde{\mathbf{Q}}(\sigma)$. For every positive integer $t$, we put

$$K_t = k_{(t-1)r+1} \ldots k_{tr}.$$

We obtain in this way a linearly disjoint sequence of field extensions $(K_l/\mathbf{Q})_{l=1}^{\infty}$ of degree $2^r$. Furthermore, for every $t$, $P_{(t-1)r+1}, \ldots, P_{tr}$ are rational over $K_t$. Hence $\bigcup_{l=1}^{\infty} \mathcal{G}(\tilde{\mathbf{Q}}/K_l)^e \subseteq S_r$. According to Lemma 1.1 $\mu(\bigcup_{l=1}^{\infty} \mathcal{G}(\tilde{\mathbf{Q}}/K_l)^e) = 1$. Therefore $\mu(S_r) = 1$ and so $\mu(\bigcap_{r=1}^{\infty} S_r) = 1$. Since, for every $(\sigma) \in \bigcap_{r=1}^{\infty} S_r$, there certainly exists an infinite subsequence of $(P)$, our second assertion also holds.

(Note that the sequence $(P)$ is rational over $K = \mathbf{Q}(\{\sqrt{n} \mid n \in \mathbf{Z}\})$. Hence the rank of $\mathcal{E}(K)$ is $\aleph_0$.)

The authors are indebted to W. D. Geyer for calling their attention to Lutz's work.

## 3. Hilbertian fields with respect to a valuation

DEFINITION. Let $k$ be a field with a valuation $v$. $k$ is said to be *hilbertian with respect to* $v$ if every hilbertian set of $k$ contains a point whose coordinates have non-negative values by $v$.

The following lemma follows immediately from the definitions (compare: Lang, [**6**], Corollary 4, p. 148).

LEMMA 3.1. *Let $k$ be a hilbertian field with respect to a real valuation $v$. Then, for every positive integer $r$, the hilbertian sets of $k^r$ are dense in $k^r$ in the $v$-topology.*

In particular, it follows in this case, that if $k_v$ is the completion of $k$ with respect to $v$, $l$ is a finite separable extension of $k$, $f(t_1, \ldots, t_r, X)$ is an irreducible polynomial over $l$, and $(\alpha) = (\alpha_1, \ldots, \alpha_r) \in k_v^r$, then we can find a point $(a) \in k^r$, arbitrarily close to $(\alpha)$, such that $f(a, X)$ is irreducible over $l$. Note that we use here the fact that every hilbertian set over $l$ contains a hilbertian set over $k$ (Lang, [**6**], p. 152). A similar argument implies the following result.

LEMMA 3.2. *If $k$ is hilbertian with respect to a valuation $v$, if $l$ is a finite extension of $k$ and $w$ is an extension of $v$ to $l$ then $l$ is hilbertian with respect to $w$.*

Examples for hilbertian fields with respect to their valuations are given in the following lemma (cf. Lang, [**6**], Theorem 2, p. 155).

LEMMA 3.3. (1) *Number fields are hilbertian with respect to every valuation.*

(2) *Function fields of one variable over a field $k_0$ are hilbertian with respect to every discrete real valuation which is trivial on $k_0$.*

## 4. The p-adic approximation on hypersurfaces

Let $k$ be a field with a real valuation $v$. Denote by $k_v$ the completion of $k$ with respect to $v$. Let $\tilde{k}$ and $\tilde{k}_v$ be the algebraic closures of $k$ and $k_v$ respectively. We imbed $\tilde{k}$ in $\tilde{k}_v$ and then identify $\tilde{k}$ with its image. We also denote by $k_s$ the separable closure of $k$. Thus, the intersection $k_s \cap k_v$ has a meaning.

LEMMA 4.1. *Let $k$ be a field with a real valuation $v$, and $f \in k[T_1, \ldots, T_n, X]$ be a polynomial whose degree in $X$ is $d \geqslant 1$. Let $\tau_1, \ldots, \tau_n, \xi \in k_v$ be elements for which*

$$f(\tau, \xi) = 0, \quad (\partial f/\partial X)(\tau, \xi) \neq 0$$

*(where $(\tau) = (\tau_1, \ldots, \tau_n)$). Suppose that $A$ is a $v$-open neighbourhood of $(\tau, \xi)$ in ${k_v}^{n+1}$. Then there exist $a_1, \ldots, a_n, b \in k_s \cap k_v$ such that $f(a, b) = 0$, $(a, b) \in A$, and $(\partial f/\partial X)(a, b) \neq 0$.*

*Moreover, if $k$ is hilbertian with respect to $v$, $l$ is a finite separable extension of $k$, and $f$ is irreducible over $l$ then we can choose $(a, b)$ to satisfy in addition the condition that $k(a, b)$ be an extension of $k$ of degree $d$ which is linearly disjoint from $l$.*

*Proof.* The implicit function theorem implies that there exists a function $X = \varphi(T)$, into $k_v$, which is defined and continuous in a neighbourhood of $(\tau)$, such that, for every $(t, x) \in {k_v}^{n+1}$ sufficiently close to $(\tau, \xi)$, we have

$$x = \varphi(t) \Leftrightarrow f(t, x) = 0.$$

(See Mattuck, [**10**], p. 97, for the ultrametric case.)

We choose $a_1, \ldots, a_n \in k$ such that $(a)$ is sufficiently close to $(\tau)$. Put $b = \varphi(a)$. Then $f(a, b) = 0$, $(a, b) \in A$, and $(\partial f/\partial X)(a, b) \neq 0$. It follows also that $b \in k_s$.

If $k$ is hilbertian with respect to $v$, $l$ is a finite separable extension of $k$, and $f$ is irreducible over $l$, we can choose $(a)$ such that, in addition to being close to $(\tau)$, $f(a, X)$ is an irreducible polynomial over $l$, of degree $d$ (this is possible according to Lemma 3.1). Hence $k(a, b) = k(b)$ is an extension of $k$ of degree $d$, linearly disjoint from $l$ over $k$.

For every absolute variety $V$ defined over a field $K$, we denote by $V_{\mathrm{sim}}(K)$ the set of all $K$-rational points of $V$ which are simple. If $K \subseteq \tilde{k}_v$ then $v$ induces in a natural way, a topology on $V(K)$ and on $V_{\mathrm{sim}}(K)$ which will be called the *$v$-topology* (Weil, [**14**], p. 352).

By a *hypersurface* we mean an affine variety $V$ of dimension $r$, defined over a field $K$ in the affine space $S^{r+1}$, which is irreducible over $\tilde{K}$.

LEMMA 4.2. *Let $k$ be a denumerable field which is hilbertian with respect to a real valuation $v$. If $V$ is a hypersurface defined over $k$ then, for almost all $(\sigma) \in \mathcal{G}(k_s/k)^e$, $V_{\mathrm{sim}}(k_s(\sigma) \cap k_v)$ is $v$-dense in $V_{\mathrm{sim}}(k_v)$.*

*Proof.* Let $f \in k[T_1, \ldots, T_n, X]$ be a generator of the ideal of all polynomials in $k[T, X]$ vanishing on $V$. Then $f$ is an absolutely irreducible polynomial. Consider a non-empty $v$-open set $A \subseteq V_{\mathrm{sim}}(k_v)$. Choose a point $(\tau, \xi) \in A$. Then $f(\tau, \xi) = 0$ and without loss of generality we can assume that $(\partial f/\partial X)(\tau, \xi) \neq 0$. Let $d$ be the degree of $f(T, X)$ in $X$. Then by Lemma 4.1 we can construct by induction a sequence of points $(a^{(1)}), (a^{(2)}), (a^{(3)}), \ldots$ in $A$ such that $k(a^{(i)})/k$ is a separable extension of degree $d$ and the sequence $(k(a^{(i)})/k)_{i=1}^{\infty}$ is linearly disjoint (compare the proof of Theorem 2.2).

Put $S(A) = \bigcup_{i=1}^{\infty} \mathcal{G}(k_s/k(a^{(i)}))^e$. Then $V(k_s(\sigma) \cap k_v) \cap A$ is non-empty for every $(\sigma) \in S(A)$. According to Lemma 1.1, $\mu(S(A)) = 1$.

Since $k$ is denumerable, it follows that the $v$-topology of $V_{\mathrm{sim}}(k_v)$ has a denumerable base. The set of all $(\sigma) \in \mathcal{G}(k_s/k)^e$ for which $V_{\mathrm{sim}}(k_s(\sigma) \cap k_v)$ is $v$-dense in $V_{\mathrm{sim}}(k_v)$ contains therefore the intersection of countably many sets of the form $S(A)$; hence it has the measure 1.

## 5. The p-adic approximation on abstract varieties

We use the term *variety* in the sense of Weil ([**14**]), that is, to mean 'absolutely irreducible'.

The following lemma will help us to reduce the problem of p-adic approximation on an arbitrary variety to that on hypersurfaces.

LEMMA 5.1. *Let $V$ be an abstract variety defined over an infinite field $k$. Suppose that $P$ is a simple point of $V$ such that $k(P)$ is a separable extension of $k$. Then there exists a hypersurface $W$ defined over $k$ and a birational map $\varphi\colon V \to W$ defined over $k$ such that $\varphi$ is biregular at $P$.*

The lemma can be proved by using the same ideas which appear in the proof for the case of algebraically closed field $k$ (cf. Mumford, [**12**], Theorem 2, p. 373).

THEOREM 5.2. *Let $k$ be a denumerable field. Suppose that $k$ is hilbertian with respect to a real valuation $v$ and that $k_v$ is a separable extension of $k$. Then for almost all $(\sigma) \in \mathcal{G}(k_s/k)^e$ and for every absolute variety $V$ defined over $k$, $V_{\mathrm{sim}}(k_s(\sigma) \cap k_v)$ is $v$-dense in $V_{\mathrm{sim}}(k_v)$. In particular, for every group variety $G$ defined over $k$, $G(k_s(\sigma) \cap k_s)$ is dense in $G(k_v)$.*

*Proof.* The assumption that $k$ is denumerable implies that there are only countably many hypersurfaces $W$ defined over $k$. It follows therefore, from Lemma 4.2, that almost all the $(\sigma) \in \mathcal{G}(k_s/k)^e$ have the property that, for every hypersurface $W$ defined over $k$, $W_{\mathrm{sim}}(k_s(\sigma) \cap k_v)$ is $v$-dense in

$W_{\mathrm{sim}}(k_v)$. Denote by $S$ the set of all $(\sigma) \in \mathcal{G}(k_s/k)^e$ with this property. Let $V$ be an absolute variety defined over $k$ and let $P \in V_{\mathrm{sim}}(k_v)$. Then there exists, by Lemma 5.1, a hypersurface $W$ over $k$ and a birational map $\varphi\colon V \to W$ defined over $k$ which is biregular at $P$. It follows that $P$ can be approximated by points of $V_{\mathrm{sim}}(k_s(\sigma) \cap k_v)$ for all $(\sigma) \in S$.

The assertion for group varieties follows simply by the fact that every point of a group variety is simple (Lang, [7], p. 221).

REMARK. We could have proved Theorem 5.2 directly, without reducing it to a discussion of hypersurfaces. But this would not have been shorter.

## 6. A class of small fields

DEFINITION. A denumerable field $k$ is said to be an *FTP field* if it is

(i) a global field, or

(ii) a function field of one variable over the perfect closure, $k_0^{p^{-\infty}}$, of a hilbertian field $k_0$ of characteristic $p$.

Every finite extension of an FTP field is again an FTP field. Denote by $\mathfrak{V}_k$ the set of all real valuations $v$ of $k$ which are arbitrary in case (i) and trivial on $k_0$ in case (ii). According to Lemma 3.3, $k$ is hilbertian with respect to every valuation $v \in \mathfrak{V}_k$. Furthermore, $k_v$ is a separable extension of $k$ according to the following lemma.

LEMMA 6.1. *If $k$ is a field of one variable over a field $k_0$ and if $v$ is a discrete real valuation of $k$ over $k_0$ then $k_v$ is a separable extension of $k$.*

*Proof.*† It suffices to prove that if $l$ is a finite purely inseparable extension of $k$ then it is linearly disjoint from $k_v$ over $k$. Indeed, let $l$ be such a field. Then $v$ has exactly one extension to $l$, which we denote by $v$ too. Hence $[l_v : k_v] = [l : v]$ (cf. Chevalley, [**3**], p. 61). But $l_v = l.k_v$. Hence $l$ and $k_v$ are linearly disjoint over $k$.

For convenience we assume that $k$ and all the $k_v$ ($v \in \mathfrak{V}_k$) are imbedded in some fixed manner in the universal domain. In the case of an FTP field, Theorem 5.2 may be reformulated as follows.

THEOREM 6.2. *Let $k$ be an FTP field and let $v \in \mathfrak{V}_k$. Then for almost all $(\sigma) \in \mathcal{G}(k_s/k)^e$ and for every absolute variety $V$ defined over $k$, $V_{\mathrm{sim}}(k_s(\sigma) \cap k_v)$ is $v$-dense in $V_{\mathrm{sim}}(k_v)$. In particular, for every group variety $G$ defined over $k$, $G(k_s(\sigma) \cap k_v)$ is dense in $G(k_v)$.*

† We are indebted to P. Roquette for calling our attention to this simple proof.

If $k$ is a field with discrete valuation $v$, we denote by $\bar{k}_v$ the residue field of $k$ with respect to $v$.

LEMMA 6.3. *Let $L$ be an FTP field and $M$ a finite cyclic extension of $L$. Then there exists a discrete valuation $v \in \mathfrak{V}_L$, not ramified in $M$, which has a unique extension to $M$ (which will also be denoted by $v$). For this $v$, $\bar{L}_v$ is a perfect field and $M_v$ is an unramified extension of $L_v$ of degree $[M : L]$.*

*Proof.* The second part of the lemma follows from the first part according to the theory of discrete valuations (Cassels and Fröhlich, [2], Proposition 1, p. 40). We prove the first part.

Consider first the case where $L$ is a global field (case (i)). Let $\sigma$ be a generator of $\mathcal{G}(M/L)$. Then we can find, according to the Čebotarev density theorem, a discrete valuation $v \in \mathfrak{V}_L$, such that the corresponding Artin symbol will be equal to $\sigma$. This $v$ has a unique extension to $M$ (Cassels and Fröhlich, [2], p. 165).

Suppose now that $L$ is a finite separable extension of a field $k$, where $k = k_1(t)$, $k_1 = k_0^{1/p^\infty}$, and $k_0$ is a hilbertian field (case (ii)). Let $f \in k_1[t, X]$ be an irreducible polynomial over $k_1(t)$, a root of which generates $M$ over $k_1(t)$. We can suppose that the greatest common divisor (in $k_1[t]$) of the coefficients of $f$ is 1. Therefore $f$ is irreducible in $k_1[t, X]$ and hence also in $k_0'[t, X]$, for some finite extension $k_0'$ of $k_0$ contained in $k_1$. Since $k_0$ is a hilbertian field, $k_0'$ is also hilbertian and hence we can find an $a \in k_0'$ such that $f(a, X)$ is an irreducible polynomial and separable over $k_0'$, whose degree is equal to the degree of $f$ in $X$, and such that the place $\mathfrak{p}$ of $k_1(t)$ over $k_1$ determined by the specialization $t \to a$ is unramified in $M$ (notice that the last requirement can be fulfilled since there are only a finite number of places of $k_1(t)$ over $k_1$ which are ramified in $M$ (Chevalley, [3], p. 72, Lemme 3). Since $k_1$ is a purely inseparable extension of $k_0'$, $f(a, X)$ is also irreducible over $k_1$. Let $\mathfrak{P}$ be an extension of $\mathfrak{p}$ to $M$. Then the degree of $\bar{M}$ (the residue field of $M$ with respect to $\mathfrak{P}$) over $\bar{k}_\mathfrak{p}$ ( $= k_1$) is equal to the degree of $f(a, X)$, and hence to $[M : k_1(t)]$. This implies that $\mathfrak{P}$ is the unique extension of $\mathfrak{p}$ to $M$ (again: Cassels and Fröhlich, [2], Proposition 1, p. 40).

Take $v$ to be the valuation corresponding to the restriction of $\mathfrak{P}$ to $L$. This $v$ is the desired valuation for the lemma.

## 7. Abelian varieties over complete fields

Let $K$ be a complete field with respect to a discrete valuation $v$. Choose a finite non-ramified Galois extension $L$ of $K$ such that $[L : K] > 1$. Denote by $k$ and $l$ the residue fields of $K$ and $L$ respectively and suppose that $k$ is a perfect field. Then $L$ is the field obtained from $K$ by extending

$k$ to $l$. In particular, $l$ is a Galois extension of $k$ and there is a natural isomorphism of $\mathcal{G}(L/K)$ onto $\mathcal{G}(l/k)$.

LEMMA 7.1. *Let $A$ be an abelian variety of dimension $r > 0$, defined over $K$. Then there exists a point $P \in A(L)$ and a $v$-open neighbourhood $U$ of $P$ in $A(L)$ such that, for every $P' \in U$ and for every integer $m \neq 0$, $mP' \notin A(K)$.*

*Proof.* We shall use the theory of minimal models of abelian varieties, developed by Néron in [**13**]. He shows that there exists an abelian variety $A'$, isomorphic to $A$ over $K$, with some 'good' properties; he calls $A'$ a minimal model ([**13**], Theorem 2, p. 79). Without loss of generality we can assume that $A = A'$, that is, $A$ is a minimal model.

Let $\mathfrak{p}_K$ be the maximal ideal of the ring of integers of $K$ with respect to $v$. For every integer $\mu \geqslant 0$, denote by $\rho^\mu$ the map induced by the reduction modulo $\mathfrak{p}_K{}^{\mu+1}$ (we use here the notations of Néron). Then $\rho^\mu(A)$ is a commutative algebraic group defined over $k$, and there exist natural epimorphisms $\theta^{\mu+1}\colon \rho^{\mu+1}(A(K)) \to \rho^\mu(A(K))$, defined over $k$, whose kernel is canonically isomorphic to $(k^+)^r$ (where $k^+$ is the additive group of $k$) such that $A(K)$ is the projective limit of the sequence

$$\rho^0(A(K)) \xleftarrow{\theta^0} \rho^1(A(K)) \xleftarrow{\theta^1} \dots \xleftarrow{} \rho^\mu(A(K)) \xleftarrow{\theta^\mu} \rho^{\mu+1}(A(K)) \xleftarrow{} \dots$$

(Néron, [**13**], pp. 78 and 79). Define by induction a subsequence $(A^\mu(K))_{\mu=0,1,2,\dots}$ in the following manner:

$$A^0(K) = 0, \quad A^{\mu+1}(K) = (\theta^\mu)^{-1}(A^\mu(K)).$$

Then we have the commutative diagram

$$\begin{array}{ccccccccc}
\rho^0(A(K)) & \longleftarrow & \dots & \longleftarrow & \rho^\mu(A(K)) & \xleftarrow{\theta^\mu} & \rho^{\mu+1}(A(K)) & \longleftarrow & \dots \\
\uparrow & & & & \uparrow & & \uparrow & & \\
A^0(K) & \longleftarrow & \dots & \longleftarrow & A^\mu(K) & \xleftarrow{\theta^\mu} & A^{\mu+1}(K) & \longleftarrow & \dots
\end{array}$$

The projective limit of the second row is denoted by $A_0(K)$. It is the set of the $k$-rational points of the pro-algebraic subgroup $A_0$ of $A$ defined over $k$.

For every $\mu \geqslant 0$, $\rho^\mu(A_0(K)) = A^\mu(K)$. It is easy to see, by induction, that if $x \in \rho^{\mu+1}(A(K))$ and if $\theta^\mu(x) = 0$ then $x \in A^{\mu+1}(K)$. Therefore, the existence of the short exact sequence

$$0 \longrightarrow (k^+)^r \longrightarrow \rho^{\mu+1}(A(K)) \xrightarrow{\theta^\mu} \rho^\mu(A(K)) \longrightarrow 0$$

implies the existence of the short exact sequence

$$0 \longrightarrow (k^+)^r \longrightarrow A^{\mu+1}(K) \xrightarrow{\theta^\mu} A^\mu(K) \longrightarrow 0.$$

Now let $A_\mu(K)$ be the kernel of the epimorphism $\rho^\mu\colon A_0(K) \to A^\mu(K)$. $A_{\mu+1}$ is a sub-pro-algebraic group of $A_\mu$ defined over $k$. Applying the 'snake lemma' to the commutative diagram

$$\begin{array}{ccccccccc}
 & & & & 0 & & & & \\
 & & & & \uparrow & & & & \\
 & & & & A_\mu(K)/A_{\mu+1}(K) & & 0 & & \\
 & & & & \uparrow & & \uparrow & & \\
0 & \longrightarrow & A_\mu(K) & \hookrightarrow & A_0(K) & \xrightarrow{\rho^\mu} & A^\mu(K) & \longrightarrow & 0 \\
 & & \uparrow & & \| & & \uparrow & & \\
0 & \longrightarrow & A_{\mu+1}(K) & \hookrightarrow & A_0(K) & \xrightarrow{\rho^{\mu+1}} & A^{\mu+1}(K) & \longrightarrow & 0 \\
 & & \uparrow & & & & \uparrow & & \\
 & & 0 & & & & (k^+)^r & & \\
 & & & & & & \uparrow & & \\
 & & & & & & 0 & &
\end{array}$$

we conclude that $\rho^{\mu+1}$ induces a natural isomorphism $\bar{\rho}^{\mu+1}$ of $A_\mu(K)/A_{\mu+1}(K)$ onto $(k^+)^r$. We thus obtain the following exact sequence

$$0 \longrightarrow A_{\mu+1}(K) \hookrightarrow A_\mu(K) \xrightarrow{\bar{\rho}^{\mu+1}} (k^+)^r \longrightarrow 0 \tag{1}$$

The same construction for $L$ and $l$ instead of $K$ and $k$ gives an analogous sequence. The imbedding of $K$ in $L$ induces a natural imbedding of $A_\mu(K)$ in $A_\mu(L)$ such that $A_\mu(K)$ is exactly the set of the fixed points of the group $\mathcal{G}(L/K)$ in $A_\mu(L)$ and we have the following commutative diagram:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & A_{\mu+1}(L) & \hookrightarrow & A_\mu(L) & \xrightarrow{\bar{\rho}^{\mu+1}} & (l^+)^r & \longrightarrow & 0 \\
 & & \uparrow & & \uparrow & & \uparrow & & \\
0 & \longrightarrow & A_{\mu+1}(K) & \hookrightarrow & A_\mu(K) & \xrightarrow{\bar{\rho}^{\mu+1}} & (k^+)^r & \longrightarrow & 0
\end{array} \tag{2}$$

It is clear now that if $P \in A_\mu(L)$ and if $\bar{\rho}^{\mu+1}(P) \notin (k^+)^r$ then every point $P' \in A_\mu(L)$ which is congruent to $P$ modulo $\mathfrak{p}_L^{\mu+2}$ does not belong to $A_\mu(K)$.

*Assertion.* There exists $\mu_0$ such that for every $\mu \geqslant \mu_0$, $A_\mu(L)$ does not contain points of finite order.

Indeed, let $p$ be the characteristic of $k$ and let $m$ be a positive integer, relatively prime to $p$ (or arbitrary if $p = 0$). Then $A_0(L)$ has no point annihilated by $m$ except 0. For if $P \in A_0(L)$ and $mP = 0$, then

$$m\bar{\rho}^1(P) = 0 \Rightarrow \bar{\rho}^1(P) = 0 \Rightarrow P \in A_1(L)$$

(according to (2) for $\mu = 0$). Proceeding by induction, we have $P \in A_\mu(L)$ and $\bar{\rho}^{\mu+1}(P) = 0$ for every $\mu \geqslant 0$. It follows that $P = 0$. This means that the order of every point in $A_0(L)$ is either a power of $p$ or $\infty$. There are only finitely many points of order $p$ in $A$ (Mumford, [**11**], p. 39). Hence, we can find $\mu_0$ such that for every $\mu \geqslant \mu_0$, $A_\mu(L)$ does not contain points of order $p$. This implies that $A_\mu(L)$ even contains no points of a $p$-power order, that is, $A_\mu(L)$ is a torsion-free group.

Now take $\mu \geqslant \mu_0$ and a point $P \in A_\mu(L)$ such that $\bar{\rho}^{\mu+1}(P) \notin (k^+)^r$ (here we use the fact that $[l : k] > 1$). Put $U = \{P' \in A(L) \mid P' \equiv P \pmod{\mathfrak{p}_L^{\mu+2}}\}$. Then $U$ is a $v$-open neighbourhood of $P$ in $A_\mu(L)$. If, for some $P' \in U$, there exists an integer $m \neq 0$ such that $mP' \in A(K)$ then, for every $\sigma \in \mathcal{G}(L/K)$,

$$m(\sigma(P') - P) = \sigma(mP') - mP' = 0.$$

However, $\sigma(P') - P' \in A_\mu(L)$ since $\rho$ and $\sigma$ commute. Hence $\sigma(P') - P' = 0$. Therefore $P' \in A(K)$, which is a contradiction to our foregoing remark. We can take this pair, $P$ and $U$, to be the desired point and neighbourhood.

REMARK. The case where $K$ is a completion of a number field is easier to handle. In this case Lemma 7.1 follows readily from the work of Mattuck ([**10**]) which generalizes the work of Lutz ([**9**]). On the other hand, one can prove the lemma in more general cases, for example, when the residue field is not perfect.

## 8. Purely inseparable extensions

LEMMA 8.1. *Let $A$ be an abelian variety defined over a field $K$ and let $L$ be a purely inseparable extension of $K$. Then for every point $P \in A(L)$ there exists a positive integer $m$ such that $mP \in A(K)$.*

*Proof.* If $\mathrm{char}(K) = 0$, the result is trivial. If $\mathrm{char}(K) = p \neq 0$ then, following a suggestion of Roquette, the assertion may be reduced to a corresponding one for divisors on $\hat{A}$, the dual of $A$. However, the latter is obvious from the definition of a divisor.

The following lemma will reduce the proof of the main theorem from considering arbitrary fields of finite type to FTP fields.

LEMMA 8.2. *Let $K/k$ be a purely inseparable extension. Suppose that $K$ has the property that for almost all $(\sigma) \in \mathcal{G}(K_s/K)^e$ the following statement holds:*

(*) *for all abelian varieties $A$ of positive dimension which are defined over $K_s(\sigma)$, $\operatorname{rank}(A(K_s(\sigma))) = \infty$.*

*Then $k$ has the same property.*

*Proof.* $k_s$ is clearly linearly disjoint from $K$ over $k$. Hence, the restriction map, $\rho$, of the elements of $\mathcal{G}(K_s/K)$ to $k_s$ is an isomorphism of $\mathcal{G}(K_s/K)$ onto $\mathcal{G}(k_s/k)$. Obviously, the measure is preserved by $\rho$. In particular, if $S$ is the set of all $(\sigma) \in \mathcal{G}(K_s/K)^e$ for which the statement (*) holds, then $S$ has measure 1, and hence $S' = \rho S$ has measure 1 in $\mathcal{G}(k_s/k)^e$. We have only to prove that every $(\sigma') \in S'$ has the property (*). Indeed let $(\sigma') = \rho(\sigma) \in S'$ and let $A$ be an abelian variety of positive dimension defined over $k_s(\sigma')$. Then $A$ is also defined over $K_s(\sigma)$. Hence there exists a linearly independent sequence $P_1, P_2, P_3, \ldots$ of points of $A(K_s(\sigma))$. $K_s(\sigma)$ is a purely inseparable extension of $k_s(\sigma')$. Hence, by Lemma 8.1, there exists for every $i \geqslant 1$ a positive integer $m_i$ such that $m_i P_i \in A(k_s(\sigma'))$. The infinite sequence $m_1 P_1, m_2 P_2, m_3 P_3, \ldots$ is obviously linearly independent. Therefore $k$ has the desired property.

## 9. Infinite fields of finite type

A field $k$ is said to be of *finite type* if it is finitely generated over the prime field which is contained in it.

It is clear that if $k$ is an infinite field of finite type then a certain purely inseparable extension of $k$ is an FTP field (use Lemma 3.3).

The following theorem is our main result.

THEOREM 9.1. *Let $k$ be an infinite field of finite type. Then almost all $(\sigma) \in \mathcal{G}(k_s/k)^e$ have the following property:*

*for every abelian variety $A$ with positive dimension, the rank of $A(k_s(\sigma))$ is $\infty$.*

*Proof.* By the preceding remark and by Lemma 8.2 it is sufficient to prove the theorem for an FTP field $k$.

Since every abelian variety $A$ defined over a certain $k_s(\sigma)$ is already defined over a finite separable extension $l$ of $k$ and this $l$ is again an FTP field, and since $k$ is denumerable, it is sufficient to prove the following statement:

(') For a given abelian variety $A$ of positive dimension, defined over $k$, the rank of $A(k_s(\sigma))$ is $\infty$ for almost all $(\sigma) \in \mathcal{G}(k_s/k)^e$.

(Compare the deduction of Theorem 2.5 from Lemma 2.4 in [**5**].)

In order to prove (′), it is enough to prove by induction the following lemma.

LEMMA. *For every integer $n \geqslant 0$, there exists a denumerable set $T_n$ of linearly independent $n$-tuples $(P) = (P_1, \ldots, P_n)$, of points of $A(k_s)$, such that, for almost all $(\sigma) \in \mathcal{G}(k_s/k)^e$, one of the $n$-tuples of $T_n$ is rational over $k_s(\sigma)$.*

The proof of the lemma will be carried out in several steps.

*Step* 1: using the induction hypothesis.

For $n = 0$ there is nothing to prove. Suppose therefore that we have already constructed $T_n$, where

$$T_n = ((P^{(1)}), (P^{(2)}), (P^{(3)}), \ldots) \quad \text{and} \quad (P^{(i)}) = (P_1^{(i)}, \ldots, P_n^{(i)}).$$

Put $L_i = k(P^{(i)})$. Then $\bigcup_{i=1}^{\infty} \mathcal{G}(k_s/L_i)^e$ is the set of all $(\sigma) \in \mathcal{G}(k_s/k)^e$ for which there exists $i$ such that $(P^{(i)})$ is rational over $k_s(\sigma)$. According to the inductive hypothesis we have

$$\mu\left(\bigcup_{i=1}^{\infty} \mathcal{G}(k_s/L_i)^e\right) = 1. \tag{1}$$

*Step* 2: constructing a sequence of quadratic extensions.

Now let $i$ be fixed. The field $L_i$ is hilbertian, hence we can construct a linearly disjoint sequence, $(M_{ij}/L_i)_{j=1}^{\infty}$, of separable extensions of degree 2. (We can use for this purpose the polynomial $X^2 + t_1X + t_2$ which is absolutely irreducible and separable in $X$ over every field (compare the proof of Theorem 2.2).) Then we have, by Lemma 1.1,

$$\mu\left(\bigcup_{j=1}^{\infty} \mathcal{G}(k_s/M_{ij})^e\right) = \frac{1}{[L_i : k]^e}. \tag{2}$$

*Step* 3: using the local theory.

For every $j$, we choose, according to Lemma 6.3, a discrete valuation $v = v_{ij} \in \mathfrak{V}_{L_i}$ having only one extension to $M_{ij}$ and not ramified there. The field $\bar{L}_{i,v}$ is perfect and $M_{ij,v}$ is an unramified extension of $L_{i,v}$ of degree 2. Since $A$ is also defined over $L_{i,v}$, there exists, by Lemma 7.1, a point $P_{ij} \in A(M_{ij,v})$ and a $v$-open neighbourhood $U_{ij}$ of $P_{ij}$ in $A(M_{ij,v})$ such that, for every $P' \in U_{ij}$ and for every integer $m \neq 0$, $mP' \notin A(L_{iv})$. In particular, $mP' \notin A(L_i)$.

*Step* 4: using the approximation theory.

Applying Theorem 6.2, we see that there exists a subset $S_{ij} \subseteq \mathcal{G}(k_s/M_{ij})^e$ of measure $1/[M_{ij} : k]^e$ such that, for every $(\sigma) \in S_{ij}$,

$$A(k_s(\sigma)) \cap U_{ij} \neq \emptyset.$$

(Note that $M_{ij}$ is an FTP field.) Since there are only countably many points in $A(k_s)$, we can order the set $\bigcup_{(\sigma) \in S_{ij}} A(k_s(\sigma)) \cap U_{ij}$ in a sequence

$(P_{ijl})_{l=1,2,\ldots}$. If we put $N_{ijl} = M_{ij}(P_{ijl})$, we have $\mathcal{G}(k_s/N_{ijl})^e = S_{ij}$ and hence

$$\mu\left(\bigcup_{l=1}^{\infty} \mathcal{G}(k_s/N_{ijl})^e\right) = \frac{1}{[M_{ij} : k]^e}. \tag{3}$$

The remark made at the end of § 1 and equations (1), (2) and (3) together imply that

$$\mu\left(\bigcup_{i=1}^{\infty}\bigcup_{j=1}^{\infty}\bigcup_{l=1}^{\infty} \mathcal{G}(k_s/N_{ijl})^e\right) = 1.$$

*Step* 5: the definition of $T_{n+1}$.

We take $T_{n+1}$ to be the set of $(n+1)$-tuples $(P^{(i)}, P_{ijl})$ $(i,j,t = 1,2,3,\ldots)$. Then for almost all $(\sigma) \in \mathcal{G}(k_s/k)^e$ one of the $(n+1)$-tuples of $T_{n+1}$ is rational over $k_s(\sigma)$. It remains to prove that the $(P^{(i)}, P_{ijl})$ are linearly independent. Indeed, suppose that there exist integers $m_1, \ldots, m_n, m_{n+1}$, not all zero, such that $\sum_{\nu=1}^{n} m_\nu P_\nu^{(i)} + m_{n+1}P_{ijl} = 0$. The inductive hypothesis implies that $m_{n+1} \neq 0$. We have also

$$m_{n+1}P_{ijl} = \sum_{\nu=1}^{n} -m_\nu P_\nu^{(i)}.$$

The right-hand side is a sum of $L_i$-rational points, hence it is rational over $L_i$. It follows that $m_{n+1}P_{ijl}$ is rational over $L_i$, which is a contradiction to the fact that $P_{ijl} \in U_{ij}$. This concludes the induction and the proof of the theorem.

## 10. Abelian varieties over an algebraically closed field

A consequence of Theorem 9.1 is the following.

THEOREM 10.1. *If $A$ is an abelian variety of positive dimension defined over an algebraically closed field $K$ which is not the algebraic closure of a finite field then the rank of $A(K)$ is equal to the cardinality of $K$.*

*Proof.* We can certainly find a field of finite type $k$ contained in $K$ such that $A$ is defined over $k$. By Theorem 9.1, we can choose $\sigma \in \mathcal{G}(k_s/k)$ such that $\operatorname{rank}(A(k_s(\sigma))) = \infty$. Hence the group $A(K)$ has an infinite rank. This proves the theorem in the case where $K$ is denumerable.

Suppose now that $K$ has the cardinality $m$ and $m > \aleph_0$. Then, as before, we find an algebraically closed field $k$ which has a finite transcendental degree over the prime field, and such that $A$ is defined over $k$. Now take a transcendence base $\{t_\mu | \mu \in M\}$ for $K$ over $k$. The cardinality of $M$ is again $m$. For every $\mu \in M$, take a point $P_\mu \in A(\widetilde{k(t_\mu)}) \setminus A(k)$. (For this one has only to consider an affine representative of $A$ and to take a point in this representative which is rational over $\widetilde{k(t_\mu)}$ such that one of its coordinates is equal to $t_\mu$.) Then we have a subset $\{P_\mu | \mu \in M\}$ of points

of $A(K)$ whose cardinality is equal to $m$. We have only to prove that this subset is linearly independent over $\mathbf{Z}$. Indeed, suppose that we have a relation of the form $n_1P_{\mu_1}+\ldots+n_sP_{\mu_s}=0$ where the $n_i$ are non-zero integers. Then $n_1P_{\mu_1}=-n_2P_{\mu_2}-\ldots-n_sP_{\mu_s}$ and we have

$$n_1P_{\mu_1}\in A(L)\cap A(M)=A(k),$$

where $L$ and $M$ are the algebraic closures of $k(t_{\mu_1})$ and $k(t_{\mu_2},\ldots,t_{\mu_s})$ respectively (since $t_{\mu_1},t_{\mu_2},\ldots,t_{\mu_s}$ are algebraically independent over $k$). But $A(k)$ is a divisible group (Mumford, [**11**], p. 62), hence $P_{\mu_1}\in A(k)$, which is a contradiction. The set $\{P_\mu|\mu\in M\}$ is thus linearly independent.

REMARKS. (1) Another formulation of the theorem is the following. If $k$ is a field which is not an algebraic extension of a finite field and if $A$ is an abelian variety defined over $k$ then, for every integer $n$, we can find a finite extension $l$ of $k$ such that $\operatorname{rank}(A(l))\geqslant n$.

(2) If one wishes to prove Theorem 10.1 directly (that is, not to use measure-theoretic arguments), one can do it in the following way. First, consider an FTP field $k$ and an abelian variety $A$ defined over $k$. Now take a quadratic Galois extension $L$ of $k$ and let $v$ be any discrete real valuation on $L$ such that $L_v$ is a proper unramified extension of $k_w$ (where $w$ is the restriction of $v$ to $k$). Then choose a point $P\in A(L_v)$ and a $v$-neighbourhood $U$ of $P$ as in Lemma 7.1. Using a generalization of Hensel's lemma, proved by Greenberg ([**4**]), one can find a point $P'\in A(\tilde{k})\cap U$ and we have, for every integer $m\neq 0$, $mP'\notin A(k)$. In this way one can construct, by induction, a linearly independent sequence $P_1,P_2,P_3,\ldots$ of points in $A(k)$. It follows immediately that the rank of $A(K)$ is at least $\aleph_0$.

The rest of the proof goes now as before. Notice that the second part of the proof is independent of the former sections.

PROBLEM. For elliptic curves $\mathscr{E}$ defined over $\mathbf{Q}$, we proved that $\mathscr{E}(\mathbf{Q}_{\mathrm{ab}})$ has an infinite rank. ($\mathbf{Q}_{\mathrm{ab}}$ is the maximal abelian extension of $\mathbf{Q}$.) Does the same result hold for an arbitrary abelian variety $A$?

## REFERENCES


1. J. W. S. CASSELS, 'Diophantine equations with special reference to elliptic curves', *J. London Math. Soc.* 41 (1966) 193–291.
2. —— and A. FRÖHLICH, *Algebraic number theory* (Cambridge University Press, 1967).
3. C. CHEVALLEY, *Introduction to the theory of algebraic functions of one variable* (Amer. Math. Soc., Providence, 1951).
4. M. GREENBERG, 'Rational points in henselian discrete valuation rings', *Inst. Hautes Études Sci. Publ. Math.* 31 (1966) 563–67.
5. M. JARDEN, 'Elementary statements over large algebraic fields', *Trans. Amer. Math. Soc.* 164 (1972) 67–91.

**6.** S. LANG, *Diophantine geometry* (Interscience, New York, 1962).
**7.** —— *Introduction to algebraic geometry* (Interscience, New York, 1958).
**8.** —— *Abelian varieties* (Interscience, New York, 1959).
**9.** E. LUTZ, 'Sur l'équation $y^2 = x^3 - Ax - B$ dans les corps $p$-adiques', *J. Reine Angew. Math.* 177 (1937) 237–47.
**10.** A. MATTUCK, 'Abelian varieties over a $p$-adic ground field', *Ann. of Math.* 62 (1955) 92–119.
**11.** D. MUMFORD, *Abelian varieties* (Oxford University Press, 1970).
**12.** —— *Introduction to algebraic geometry*, Harvard Lecture Notes.
**13.** A. NÉRON, 'Modèles minimaux des variétés abéliennes sur les corps locaux et globaux', *Inst. Hautes Études Sci. Publ. Math.* 21 (1964).
**14.** A. WEIL, *Foundations of algebraic geometry* (Amer. Math. Soc., Providence, 1962).

*Mathematisches Institut*
*Universität Heidelberg*
69 *Heidelberg* 1
*BRD*