THE RANK OF ABELIAN VARIETIES OVER LARGE ALGEBRAIC FIELDS*

by

Wulf-Dieter Geyer

Mathematisches Institut, Erlangen University

Bismarckstr. $1\frac{1}{2}$, Erlangen 91054, Germany

e-mail: geyer@mi.uni-erlangen.de

and

Moshe Jarden

School of Mathematics, Tel Aviv University

Ramat Aviv, Tel Aviv 69978, Israel

e-mail: jarden@post.tau.ac.il

Abstract

Improving a theorem of Frey-Jarden from 1974 we prove for an infinite finitely generated field and an Abelian variety A over K that $\mathrm{rank}(A(K_s[\boldsymbol{\sigma}])) = \infty$ for almost all $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$.

MR Classification: 12E30

Directory: \Jarden\Works\Paper82

29 June, 2005

* Research supported by the Minkowski Center for Geometry at Tel Aviv University, established by the Minerva Foundation.

Introduction

Let K be an infinite field which is finitely generated over its prime field (henceforth a **finitely generated field**) and A an Abelian variety over K. Then the Abelian group $A(K)$ of all K-rational points of A is finitely generated (Mordell-Weil), in particular $\mathrm{rank}(A(K)) < \infty$. In contrast, $\mathrm{rank}(A(K_s)) = \infty$ for the separable closure K_s of K. Thus, $A(K_s)$ has a sequence of linearly independent points $\mathbf{p}_1, \mathbf{p}_2, \mathbf{p}_3, \ldots$. Moreover, these points can be chosen to be M-rational if M is a separable algebraic extension of K which lies "close enough" to K_s. More precisely, the following holds:

Theorem A ([FreyJ, p. 112]): *Let K be an infinite finitely generated field, A an Abelian variety over K of positive dimension, and e a positive integer. Then* $\mathrm{rank}(A(K_s(\boldsymbol{\sigma}))) = \infty$ *for almost all* $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$.

Here $\mathrm{Gal}(K) = \mathrm{Gal}(K_s/K)$ is the **absolute Galois group** of K and for each $\boldsymbol{\sigma} = (\sigma_1, \ldots, \sigma_e) \in \mathrm{Gal}(K)^e$ we write $K_s(\boldsymbol{\sigma})$ for the fixed field of $\sigma_1, \ldots, \sigma_e$ in K_s. The expression "almost all $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$ " indicates that we ignore a subset of $\mathrm{Gal}(K)^e$ of Haar measure zero.

The proof of Theorem A in [FreyJ] uses two major tools: Néron's theory of minimal models of Abelian varieties over complete fields and approximation of simple points on algebraic varieties over complete fields by separable algebraic points.

The goal of this note is to sharpen Theorem A by using the stability of fields [Neu] and Im's method of constructing linearly independent points [Im]:

Theorem B: *Let K be an infinite finitely generated field and A an Abelian variety over K. Then* $\mathrm{rank}(A(K_s[\boldsymbol{\sigma}])) = \infty$ *for almost all* $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$.

Here $K_s[\boldsymbol{\sigma}]$ is the maximal Galois extension of K in $K_s(\boldsymbol{\sigma})$. It is known that for almost all $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^\sigma$ the field $K_s[\boldsymbol{\sigma}]$ is PAC with absolute Galois group isomorphic to $\hat{F}_\omega$ (the free profinite group on countably many generators) [Jar, Thm. 2.7]. Thus, $K_s[\boldsymbol{\sigma}]$ is much smaller than $K_s(\boldsymbol{\sigma})$, yet Theorem B shows that $K_s[\boldsymbol{\sigma}]$ is large enough for the rank of $A(K_s[\boldsymbol{\sigma}])$ (hence, also for the rank of $A(K_s(\boldsymbol{\sigma})))$ to be infinite.

1. Independent points on Abelian varieties

Let K be an infinite finitely generated field and A an Abelian variety of dimension $d \geq 1$ over K. It turns out that the finiteness part of $A_{\mathrm{tor}}(K)$ of the Mordell-Weil Theorem is an easy consequence of the existence of a good reduction of A with respect to a valuation with a finite residue field. This method has the advantage of proving the finiteness of the number of torsion points of A of bounded degree over K.

We denote the algebraic closure of a field K by $\tilde{K}$.

Proposition 1.1: *Let K be a finitely generated field, A an Abelian variety over K, and d a positive integer. Then there exists a positive integer c such that $|A_{\mathrm{tor}}(L)| \leq c$ for each finite extension L of K of degree at most d.*

Proof: Denote the set of all extensions L of K with $[L : K] \leq d$ by $\mathcal{L}$. Choose a prime number p and a place π of K with a residue field $\bar{K}$ of finite degree over $\mathbb{F}_p$ such that A has a good reduction at π [ShT, p. 95, Prop. 25]. Denote the unique extension of $\bar{K}$ of degree d by $\bar{K}_d$ and let $\bar{A}$ be the reduced Abelian variety. Now consider $L \in \mathcal{L}$ and a positive integer n with $p \nmid n$. Extend π to a place of L and denote the residue field by $\bar{L}$. Then $[\bar{L} : \bar{K}] \leq [L : K] \leq d$, so $\bar{L} \subseteq \bar{K}_{d!}$. Since $\bar{K}_{d!}$ is finite, the group $\bar{A}(\bar{K}_{d!})$ is finite with, say, c_p elements. By [SeT, Thm. 1 and Lemma 2], π maps $A_n(L)$ injectively into $\bar{A}_n(\bar{K}_{d!})$. Hence, $|A_n(L)| \leq |\bar{A}_n(\bar{K}_{d!})| \leq |\bar{A}(\bar{K}_{d!})| = c_p$.

Lemma 1.1 of [JaJ] allows us to choose a place π of K with a finite residue field $\bar{K}$ such that A has a good reduction at π and π maps $A_{p^i}(\tilde{K})$ bijectively onto $\bar{A}_{p^i}(\tilde{\bar{K}})$ for all $i \geq 1$. As in the preceding paragraph, there is a positive integer c' such that $|A_{p^i}(L)| \leq c'$ for all $i \geq 1$ and $L \in \mathcal{L}$. An arbitrary positive integer m can be written as $m = np^i$ with $p \nmid n$. For each $L \in \mathcal{L}$ we have $A_m(L) = A_n(L) \oplus A_{p^i}(L)$, so $|A_m(L)| \leq c_p c'$. Since $A_{\mathrm{tor}}(L)$ is the ascending union of all groups $A_{k!}(L)$ with k ranging on all positive integers, $|A_{\mathrm{tor}}(L)| \leq c_p c'$, as claimed. ∎

Remark 1.2: Related results. The proof of Proposition 1.1 is modelled after the proof of [Silverman, p. 4, Lemma] which deals with the case where K is a number field and A is an elliptic curve.

Merel has considerably strengthened Proposition 1.1 for elliptic curves over number fields. He proves that for each positive integer d there exists a constant c such that if L is an extension of degree at most d over $\mathbb{Q}$ and E is an elliptic curve over K, then $|E_{\rm tor}(L)| \le c$ [Mer]. It is conjectured that the same result holds for all Abelian varieties of a given dimension [Silverberg, Conj. 2.3.2]. ∎

Using [Silverman], Im proves Proposition 1.3 below for elliptic curves over number fields [Im, Lemma 3.11]. We apply Proposition 1.1 and generalize Im's result to Abelian varieties over infinite finitely generated fields:

PROPOSITION 1.3: *Let K be a finitely generated field, A an Abelian variety over K, and d a positive integer. Suppose K has a linearly disjoint sequence $L_1, L_2, L_3, \ldots$ of Galois extensions of degree d and for each i there is a point $\mathbf{p}_i \in A(L_i) \smallsetminus A(K)$. Then there exists a positive integer k such that the points $\mathbf{p}_k, \mathbf{p}_{k+1}, \mathbf{p}_{k+2}, \ldots$ are linearly independent. In particular,* $\mathrm{ord}(\mathbf{p}_i) = \infty$ *for each $i \ge k$.*

Proof: By Proposition 1.1, $\bigcup_{i=1}^\infty A_{\rm tor}(L_i)$ is a finite set. Denote the least common multiple of the orders of the points in $\bigcup_{i=1}^\infty A_{\rm tor}(L_i)$ by n. Thus, $n\mathbf{p} = 0$ for each $\mathbf{p} \in \bigcup_{i=1}^\infty A_{\rm tor}(L_i)$. Next choose generators $\mathbf{q}_1, \ldots, \mathbf{q}_m$ of $A(K)$ (Mordell-Weil [Lan, p. 138, Thm. 1]). For each $1 \le j \le m$ choose $\mathbf{q}'_j \in A(\tilde{K})$ with $n\mathbf{q}'_j = \mathbf{q}_j$. Put $F = K(A_n, \mathbf{q}'_1, \ldots, \mathbf{q}'_m)$. Then F/K is a finite extension and $A(F)$ contains each point $\mathbf{q}' \in A(\tilde{K})$ satisfying $n\mathbf{q}' \in A(K)$. Indeed, there are $a_1, \ldots, a_m \in \mathbb{Z}$ with $n\mathbf{q}' = \sum_{j=1}^m a_j\mathbf{q}_j$. Hence, $n\sum_{j=1}^m a_j\mathbf{q}'_j = \sum_{j=1}^m a_j\mathbf{q}_j = n\mathbf{q}'$, so $\mathbf{q}' - \sum_{j=1}^m a_j\mathbf{q}'_j \in A_n(\tilde{K}) \subseteq A(F)$. Thus, $\mathbf{q}' \in A(F)$.

Denote the maximal separable extension of K in F by E. Lemma 2.5.7 of [FriedJ] gives a positive integer k such that $E, L_k, L_{k+1}, L_{k+2}, \ldots$ are linearly disjoint over K. Since each of the extensions L_i/K is separable and F/E is purely inseparable, $F, L_k, L_{k+1}, L_{k+2}, \ldots$ are linearly disjoint over K.

Assume that the points $\mathbf{p}_k, \mathbf{p}_{k+1}, \mathbf{p}_{k+2}, \ldots$ are linearly dependent. Then there exists a nonempty finite subset I of $\{k, k+1, k+2, \ldots\}$ and for each $i \in I$ there exists a nonzero integer b_i such that

$$\sum_{i\in I} b_i\mathbf{p}_i = 0. \tag{1}$$

Put $L = \prod_{i\in I} L_i$, choose $j \in I$, and consider an element $\tau_j \in \mathrm{Gal}(L_j/K)$. Since the extensions L_i of K with $i \in I$ are linearly disjoint, there is a $\tau \in \mathrm{Gal}(L/K)$ with $\tau|_{L_j} = \tau_j$ and $\tau|_{L_i} = 1$ for each $i \in I \smallsetminus \{j\}$. Acting with τ on (1), we get $b_j\tau_j\mathbf{p}_j + \sum_{i\neq j} b_i\mathbf{p}_i = 0$. Subtracting the latter equality from (1), gives $b_j(\tau_j\mathbf{p}_j - \mathbf{p}_j) = 0$, so $\tau_j\mathbf{p}_j - \mathbf{p}_j \in A_{\mathrm{tor}}(L_j)$. By the first paragraph, $n(\tau_j\mathbf{p}_j - \mathbf{p}_j) = 0$, hence $\tau_j(n\mathbf{p}_j) = n\mathbf{p}_j$. Since the latter equality holds for each $\tau_j \in \mathrm{Gal}(L_j/K)$, we have $n\mathbf{p}_j \in A(K)$. Again, by the first paragraph, $\mathbf{p}_j \in A(F)$. Since $\mathbf{p}_j$ is also in $A(L_j)$, the linear disjointness of L_j and F over K implies that $\mathbf{p}_j \in A(K)$. This contradiction to the basic assumption on $\mathbf{p}_j$ implies that $\mathbf{p}_k, \mathbf{p}_{k+1}, \mathbf{p}_{k+2}, \ldots$ are linearly independent, as claimed. ∎

2. Application of the Stability of Fields

The construction of the fields L_i and the points $\mathbf{p}_i \in A(L_i) \smallsetminus A(K)$ as in Proposition 1.3 is made possible by a very general theorem about the stability of fields (surveyed in [FriedJ, Sec. 18.9]). It works for an arbitrary absolutely irreducible variety:

LEMMA 2.1: *Let V be an absolutely irreducible variety of positive dimension r over a Hilbertian field K. Then there exists an integer $d \geq 2$, a linearly disjoint sequence $L_1, L_2, L_3, \ldots$ of Galois extensions of K of degree d, and for each i there exists $\mathbf{p}_i \in V(L_i) \smallsetminus V(K)$.*

Proof: Choose a generic point $\mathbf{x}$ of V over K. Then $F = K(\mathbf{x})$ is a regular extension of K [FriedJ, Lemma 10.2.2]. The stability of fields gives $t_1, \ldots, t_r \in F$ which are algebraically independent over K such that $F/K(\mathbf{t})$ is finite and separable and the Galois closure $\hat{F}$ of $F/K(\mathbf{t})$ is regular over K [Neu, p. 222, Thm.]. If F is not a field of rational functions, then $d_0 = [F : K(\mathbf{t})] \geq 2$. If $F = K(u_1, \ldots, u_r)$ with $u_1, \ldots, u_r$ algebraically independent over K, we redefine $t_1, \ldots, t_r$ in the following way: For $i = 2, \ldots, r$ we put $t_i = u_i$. When $\mathrm{char}(K) \neq 2$, we let $t_1 = u_1^2$. Finally, when $\mathrm{char}(K) = 2$, we define t_1 to be $u_1^2 + u_1$. Then $t_1, \ldots, t_r$ are algebraically independent over K and $\hat{F} = F$ is a Galois extension of $K(\mathbf{t})$ of degree $d_0 = 2$ which is regular over K. In each case let $G = \mathrm{Gal}(\hat{F}/K(\mathbf{t}))$ and $d = [\hat{F} : K(\mathbf{t})]$.

Now choose a primitive element y for $F/K(\mathbf{t})$ which is integral over $K[\mathbf{t}]$ and let

$f \in K[T_1, \ldots, T_r, Y]$ be a polynomial such that $f(\mathbf{t}, Y) = \mathrm{irr}(y, K(\mathbf{t}))$. Then $\deg_Y(f) = d_0$ and $\mathrm{Gal}(f(\mathbf{t}, Y), L(\mathbf{t})) \cong G$, for each algebraic extension L of K. Let W be the hypersurface in $\mathbb{A}^{r+1}$ defined over K by the equation $f(\mathbf{T}, Y) = 0$. Then there exists a birational transformation $\varphi \colon W \to V$ over K. Since K is Hilbertian, we may inductively define a sequence $(\mathbf{a}_1, b_1), (\mathbf{a}_2, b_2), (\mathbf{a}_3, b_3), \ldots$ of points of $W(K_s)$ with the following properties:

(1a) For each i, $\mathbf{a}_i \in K^r$.

(1b) For each i, the extension $K(b_i)/K$ is separable of degree d_0.

(1c) For each i, φ is defined at $(\mathbf{a}_i, b_i)$.

(1d) For each i, $\mathrm{Gal}(f(\mathbf{a}_i, Y), K) \cong G$.

(1e) Denote the Galois closure of $K(b_i)/K$ by L_i. Then $L_1, L_2, L_3, \ldots$ are linearly disjoint Galois extensions of K of degree d.

Indeed, inductively suppose $(\mathbf{a}_1, b_1), \ldots, (\mathbf{a}_n, b_n)$ have already been constructed. Let L be the Galois closure of $K(b_1, \ldots, b_n)/K$. Then both $\mathrm{Gal}(f(\mathbf{t}, Y), K(\mathbf{t}))$ and $\mathrm{Gal}(f(\mathbf{t}, Y), L(\mathbf{t}))$ are isomorphic to G. A lemma of Hilbert gives a separable Hilbertian subset H_K of K^r such that $f(\mathbf{a}, Y)$ is irreducible and separable of degree d_0, φ is defined at $(\mathbf{a}, b)$ for each root b of $f(\mathbf{a}, Y)$, and $\mathrm{Gal}(f(\mathbf{a}, Y), K) \cong G$ for each $\mathbf{a} \in H_K$ [FriedJ, Lemma 13.1.1]. Likewise there exists a separable Hilbertian subset H_L of L^r such that $\mathrm{Gal}(f(\mathbf{a}, Y), L) \cong G$ for each $\mathbf{a} \in H_L$. By [FriedJ, Prop. 12.3.3], H_L contains a separable Hilbertian subset H'_L of K^r. Since K is Hilbertian, there exists $\mathbf{a}_{n+1} \in H_K \cap H'_L$. Choose a root b_{n+1} of $f(\mathbf{a}_{n+1}, Y)$ in K_s and let L_{n+1} be the Galois closure of $K(b_{n+1})/K$. Then Conditions (1a)-(1d) hold for $i = n+1$ and $L_1, \ldots, L_{n+1}$ are linearly disjoint. This concludes the induction step.

Finally, for each i let $\mathbf{p}_i = \varphi(\mathbf{a}_i, b_i)$. Then $\mathbf{p}_i$ belongs to $V(L_i)$ and $K(\mathbf{p}_i) = K(b_i)$ is an extension of degree d_0 of K, so $\mathbf{p}_i \notin V(K)$, as desired. ∎

We are now in a position to prove Theorem B:

Proposition 2.2: *Let A be an Abelian variety of positive dimension over a finitely generated field K. Then $\mathrm{rank}(A(K_s[\boldsymbol{\sigma}])) = \infty$ for almost all $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$.*

Proof: Let $r = \dim(A)$. By Lemma 2.1 there exists a positive integer d, a linearly disjoint sequence $L_1, L_2, L_3, \ldots$ of Galois extensions of K of degree d, and for each i there exists $\mathbf{p}_i \in A(L_i) \smallsetminus A(K)$. Proposition 1.3 gives a positive integer k such that the points $\mathbf{p}_k, \mathbf{p}_{k+1}, \mathbf{p}_{k+2}, \ldots$ are linearly independent. By Borel-Cantelli, for almost all $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$ there are infinitely many $i \geq k$ such that $L_i \subseteq K_s(\boldsymbol{\sigma})$ [FriedJ, Lemma 18.5.3(b)], hence $L_i \subseteq K_s[\boldsymbol{\sigma}]$. For each of these $\boldsymbol{\sigma}$'s the rank of $A(K_s[\boldsymbol{\sigma}])$ is infinite. ∎

Our final goal is to improve Theorem B by letting the Abelian varieties be defined over $K_s[\boldsymbol{\sigma}]$:

LEMMA 2.3: *Let N/K be a Galois extension of fields. Suppose $\mathrm{rank}(B(N)) = \infty$ for every Abelian variety B of positive dimension over K. Then $\mathrm{rank}(A(N)) = \infty$ for every Abelian variety A of positive dimension over N.*

Proof: Let A be an Abelian variety of positive dimension over N. Then K has a finite Galois extension L in N and there is an Abelian variety A' over L such that $A \cong A' \times_L N$. In particular, $A(N) \cong A'(N)$. Let $G = \mathrm{Gal}(L/K)$ and lift each $\tau \in G$ to an element $\tau \in \mathrm{Gal}(N/K)$. Weil's descent gives an Abelian variety B over K such that $B \times_K L \cong \prod_{\tau \in G} \tau A'$ [Weil, end of page 6]. Thus, $B(N) \cong \bigoplus_{\tau \in G} (\tau A')(N)$, so $B(N) \otimes \mathbb{Q} \cong \bigoplus_{\tau \in G} (\tau A')(N) \otimes \mathbb{Q}$. By assumption, $\mathrm{rank}(B(N)) = \infty$, so $\dim(B(N) \otimes \mathbb{Q}) = \infty$. Hence, there is a $\tau \in G$ with $\dim((\tau A')(N) \otimes \mathbb{Q}) = \infty$ and therefore $\mathrm{rank}(\tau(A'(N))) = \mathrm{rank}((\tau A')(N)) = \infty$ for at least one $\tau \in G$. Consequently, $\mathrm{rank}(A(N)) = \mathrm{rank}(A'(N)) = \mathrm{rank}(\tau(A'(N))) = \infty$, as claimed. ∎

The combination of Proposition 2.2 and Lemma 2.3 improves Theorem B:

THEOREM 2.4: *Let K be an infinite finitely generated field and e a positive integer. Then almost all $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$ have the following property: For each Abelian variety A of positive dimension over $K_s[\boldsymbol{\sigma}]$ the rank of $A(K_s[\boldsymbol{\sigma}])$ is infinite.*

Proof: By assumption K is countable. Hence, there are only countably many Abelian varieties B of positive dimension over K. It follows from Proposition 2.2, that almost all $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$ have the following property: If B is an Abelian variety over K, then $\mathrm{rank}(B(K_s[\boldsymbol{\sigma}])) = \infty$. We conclude from Lemma 2.3, that almost all $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$ have the property indicated in the Theorem. ∎

References

[FreyJ] G. Frey and M. Jarden, *Approximation theory and the rank of abelian varieties over large algebraic fields*, Proceedings of the London Mathematical Society **28** (1974), 112–128.

[FriedJ] M. D. Fried and M. Jarden, *Field Arithmetic, 2nd Edtion, revised and enlarged by Moshe Jarden*, Springer, Heidelberg, 2004.

[Im] Im B.-H., *Mordell-Weil groups and the rank of elliptic curves over large fields,* http://front.math.ucdavis.edu/ANT/ math.NT/0411533

[JaJ] M. Jacobson and M. Jarden, *Finiteness theorems for torsion of abelian varieties over large algebraic fields,* Acta Arithmetica **98** (2001), 15–31.

[Jar] M. Jarden, *Large normal extensions of Hilbertian fields*, Mathematische Zeitschrift **224** (1997), 555-565.

[Lan] S. Lang, *Fundamentals of Diophantine Geometry,* Springer-Verlag, New York, 1983.

[Mer] L. Merel, *Bornes pour la torsion des courbes elliptiques sur les corps de nombres,* Inventiones mathematicae **124** (1996), 437–449.

[Neu] K. Neumann, *Every finitely generated regular field extension has a stable transcendence base,* Israel Journal of Mathematics **104** (1998), 221–260.

[SeT] J.-P. Serre and J. Tate, *Good reduction of abelian varieties,* Annals of Mathematics **88** (1968), 492-571.

[Shi] G. Shimura, *Abelian Varieties with Complex Multiplication and Modular Functions,* Princeto University Press, Princeton, 1998.

[Silverberg] E. Silverberg, *Open questions in artihmetic algebraic geometry,* IAS Park City, Mathematics Series 9, AMS (2001), 83–142.

[Silverman] J. J. Silverman, *Integer points on curves of genus* 1, Journal of the London Mathematical Society **28** (1983), 1–7.

[Weil] A. Weil, *Adeles and Algebraic Groups,* Birkhäuser, Progress in Mathematics, Boston, 1982.