ALGEBRAIC VARIETIES OVER SMALL FIELDS

by

Fedor Bogomolov and Yuri Tschinkel

Abstract. — We study curves and their Jacobians over $\bar{\mathbb{F}}_p$ and $\bar{\mathbb{Q}}$, and discuss applications to rational connectivity over these fields. We introduce certain dynamical systems on $\mathbb{P}^1$, induced by translates by torsion points on elliptic curves, and study fields related to these systems.

1. Introduction

Algebraic geometry deals with polynomial equations and sets of their solutions over different fields and rings. The structure of these sets reflects on the one hand the complexity of the defining equations, and on the other hand properties of the fields and rings in question. Individual fields and rings may have features which are not purely algebraic, but are inherited from a specific realization: topology, analytic structure, valuations etc. Algebraic varieties over *large fields*, such as complex, real, or p-adic numbers, are analytic manifolds. This is used in an essential way in their classification. The intuition from analysis and topology serves as a guide for many algebraic constructions, moreover, there are many purely algebraic results which have only analytic proofs, at present.

Our point of departure was the fact that algebraic varieties over *small* fields, such as finite fields and their closures, carry completely different, in some sense, orthogonal, additional structures, for example, the action of the Frobenius. In this note we discuss several new results and questions concerning the geometry of algebraic varieties over "small" algebraically closed fields.

Acknowledgments. This note was written while both authors were visiting the Centro di Ricerca Matematica "Ennio De Giorgi" of the Scuola Normale Superiore in Pisa. We are very grateful for ideal working conditions at this institute. The first author was partially supported by the NSF grant DMS-0404715. We thank B. Poonen for comments and suggestions.

2. Curves and their Jacobians over $\bar{\mathbb{F}}_p$

In this section, $k = \bar{\mathbb{F}}_p$ is the algebraic closure of a finite field. Let C be an irreducible smooth projective curve of genus g over k and $J = J_C$ its Jacobian. Let $k_0/\mathbb{F}_p$ be a finite extension such that both C, J are defined over k_0 and $C(k_0) \neq \emptyset$. We fix a $c_0 \in C(k_0)$ and the embedding

$$\begin{array}{ccc} C & \hookrightarrow & J \\ c & \mapsto & [c - c_0]. \end{array}$$

The abelian group $J(k)$ is torsion. For any set of primes S, put

$$J\{\mathsf{S}\} := \oplus_{\ell\in\mathsf{S}} J\{\ell\} \subset J(k), \quad \text{with} \quad J\{\ell\} := \bigcup_{n\in\mathbb{N}} J(k)[\ell^n],$$

the ℓ-primary part of $J(k)$. We have natural projection homomorphism:

$$\lambda_{\mathsf{S}} \, : \, J(k) \to J\{\mathsf{S}\},$$

which induces a map $\lambda_{\mathsf{S}} \, : \, C(k) \to J\{\mathsf{S}\}$ (which depends on the choice of c_0).

Theorem 2.1. — *Let S be a finite set of primes. There exists a set of primes P of density one, containing S, such that λ_{P} is surjective.*

The existence of such a set P of positive density was proved in [4]; the formulated result is shown in [15]. In down to earth terms this result says that given any n, there are points $c \in C(k)$ whose order is divisible by n. We also have the following, more geometric statement:

Theorem 2.2 ([4]). —

$$J(k) = \cup_{n\in\mathbb{N}} n\cdot C(k).$$

For $c \in C(k) \hookrightarrow J(k)$, let

- $\Delta(c)$ be the order of c in $J(k)$ and
- $\mathfrak{f}(c) = \prod_{\ell\mid\Delta(c)} \ell$ the corresponding product of primes.

These invariants depend on the embedding $C \hookrightarrow J$.

Conjecture 2.3. — For all $\epsilon > 0$ one has

$$\Delta(c) = O(\mathfrak{f}(c)^{2+\epsilon}).$$

It may well be that the exponent can be improved to $1+\epsilon$.

For a finite set of primes S let k_{S}/k_0 be the field extension generated by $J\{\mathsf{S}\}$ points, and let $\Gamma_{\mathsf{S}} = \mathrm{Gal}(k_{\mathsf{S}}/k_0)$ be the corresponding Galois group. It is a procyclic group, which contains a unique maximal subgroup Γ'_{S} of the form $\prod_{\ell\in\mathsf{S}} \mathbb{Z}_\ell$. Note that $\Gamma_{\mathsf{S}}/\Gamma'_{\mathsf{S}}$ is finite (it is a subgroup of $\prod_{\ell\in\mathsf{S}} \mathrm{GL}_{2\mathsf{g}}(\mathbb{Z}/\ell)$ and hence its order is trivially bounded by $\prod_{\ell\in\mathsf{S}} \ell^{2\mathsf{g}}$). The intuition behind Conjecture 2.3 is that while Theorem 2.1 guarantees the existence of sequences of points in $C(k)$ whose order is divisible by higher and higher powers of any positive integer, the main contribution to the sizes of these orders should, asymptotically, still be given by a product of distinct primes. The observation is that, while $C(k)$ and $C(k_{\mathsf{S}})$ are infinite, and moreover, the *projection*

$$\lambda_{\mathsf{S}} : C(k_{\mathsf{S}}) \to J\{\mathsf{S}\}$$

is surjective, one has the following:

Proposition 2.4 ([8], [9]). — *If S is a finite set of primes then the intersection*

$$C(k_{\mathsf{S}}) \cap J\{\mathsf{S}\}$$

is finite.

On the other hand, $J(k_{\mathsf{S}})/J\{\mathsf{S}\}$ is infinite. In fact,

$$J(k_{\mathsf{S}})/J\{\mathsf{S}\} = \oplus_{\ell\notin\mathsf{S}} A_\ell,$$

where $A_\ell \subset J\{\ell\}$ are finite and nontrivial for infinitely many ℓ. We expect a uniform bound of the shape

$$|A_\ell| \leq \ell^n, \tag{2.1}$$

for some $n \in \mathbb{N}$, independent of ℓ. Thus, to get points in $C(k_{\mathsf{S}})$ whose orders are divisible by high powers of ℓ, for $\ell \in \mathsf{S}$, we need to increase the number of factors outside S. This should lead to the estimate in Conjecture 2.3.

Remark 2.5. — It is possible that most of the time the exponent n in (2.1) equals 1. A related question for $\mathbb{G}_m$ can be formulated as follows: for fixed $a \in \mathbb{N}$ and $r \geq 2$, what is the density of primes ℓ such that

$$a^{\ell-1} = 1 \mod \ell^r.$$

This is a rare event. In fact for $\ell \leq 3 \cdot 10^9$ only $\ell = 1093, 3511$ satisfy this equation for $a = 2$ and $r = 2$. The expected density of such primes ℓ should be zero.

A generalization of this to algebraic numbers would be a step towards Conjecture 2.3, via the inequality (2.1).

3. Dominating varieties

We say that a smooth projective curve C dominates C', and write $C \Rightarrow C'$, if there exist an étale cover $\tilde{C} \to C$ and a surjection $\tilde{C} \to C'$.

Conjecture 3.1. — Let k be $\bar{\mathbb{F}}_p$ or $\bar{\mathbb{Q}}$ and C, C' curves over k with $\mathsf{g}(C), \mathsf{g}(C') \geq 2$. Then

$$C \Leftrightarrow C'.$$

If true, this suggests that there is a unique, universal noncommutative étale Galois module, playing the role of $\mathbb{C}^n$ for abelian varieties over $\mathbb{C}$, in the sense that different hyperbolic curves can be thought of as “lattices” in this object (modulo “denominators”).

For simplicity, we now assume that $p \geq 5$. Here is a sample of our results:

Theorem 3.2 ([3]). — *Let C be any hyperelliptic curve over $\bar{\mathbb{F}}_p$ of genus $\mathsf{g}(C) \geq 2$ and C' any curve. Then $C \Rightarrow C'$.*

In particular, $C \Leftrightarrow C'$ for any hyperbolic hyperelliptic curves C, C'. Further, if a curve C has a nonramified covering which surjects onto a hyperbolic hyperelliptic curve then C dominates any curve. Thus Conjecture 3.1, in characteristic $p \geq 5$, would follow from:

Conjecture 3.3. — Every curve C over $\bar{\mathbb{F}}_p$ admits a nonramified cover which dominates a hyperelliptic curve of genus ≥ 2.

The proof of Theorem 3.2 for $C = \mathsf{C}_6 : y^2 = x^6 - 1$, is based on the following observation: an arbitrary curve C' admits a map $C' \to \mathbb{P}^1$ with local ramification indices of order at most 2. Over $\bar{\mathbb{F}}_p$, all points on an elliptic curve are torsion. In particular, if E is realized as the double cover $E \to \mathbb{P}^1$, all points in $\mathbb{P}^1(\bar{\mathbb{F}}_p)$ are images of torsion points in E. We use the special curve $E : y^2 = x^3 - 1$. After a finite nonramified covering $E \to E$ the induced covering $\tau : \mathsf{C}_6 \to E \to \mathbb{P}^1$ will be doubly ramified over all preimages of ramifications points for $C' \to \mathbb{P}^1$. Taking a fibered product of $C' \to \mathbb{P}^1$ and $\tau : \mathsf{C}_6 \to \mathbb{P}^1$ over $\mathbb{P}^1$ gives a nonramified covering of C_6 surjecting onto C' (see [2]).

In our further investigations towards Conjecture 3.1, we make use of special hyperelliptic curves,

$$\mathsf{C}_n : y^2 = x^n - 1,$$

ramified in roots of 1.

Theorem 3.4 ([3]). — *Let C be any hyperelliptic curve over $\bar{\mathbb{Q}}$ of genus $\mathsf{g}(C) \geq 2$. Then $C \Rightarrow \mathsf{C}_6$ and $C \Rightarrow \mathsf{C}_8$.*

Our motivation to study covers of curves over small fields came from the theorem of Belyi: every curve over $\bar{\mathbb{Q}}$ admits a cover of $\mathbb{P}^1$ ramified over $0, 1, \infty$, and its analog: every curve over $\bar{\mathbb{F}}_p$ covers $\mathbb{P}^1$ with ramification over 0 and ∞. In fact, there are many such covers and one of the key issues is to have some control over the local ramification indices of Belyi's maps. By Belyi's theorem, Conjecture 3.1 over $\bar{\mathbb{Q}}$ would follow if we knew that

$$\mathsf{C}_6 \Rightarrow \mathsf{C}_n$$

for all $n \geq 6$. A partial result in this direction is:

THEOREM 3.5 ([5]). — *If $n \geq 6$ is divisible only by primes in $\{2,3,5\}$ then*

$$\mathsf{C}_6 \Leftrightarrow \mathsf{C}_n.$$

Further results in this direction, making use of modular curves of small genus, can be found in [16].

As already mentioned, the proofs of the above theorems are based on Abhyankar's lemma. One of the key issues is to be able to control ramification indices and to construct chains of coverings reducing ramification. In particular, it is important to find extensions of Belyi's result with imposed restrictions on ramification. In this direction, we proved that every curve C over $\bar{\mathbb{Q}}$ admits a dominant map $f : C \to \mathbb{P}^1$, branched over $\mathbb{A}^1(\mathbb{Z}) \subset \mathbb{P}^1(\mathbb{Q})$ and so that all local ramification indices have a 2-power order. Consequently, Theorem 3.5 for all n and Conjecture 3.1 would follow if we could show that for any finite set $M \subset \mathbb{Z} = \mathbb{A}^1(\mathbb{Z}) \subset \mathbb{P}^1(\mathbb{Q})$ there is a map $f : \mathbb{P}^1 \to \mathbb{P}^1$ with the property that

- the image under f of the union of M with the ramification locus of f is contained in $\{0,1,\infty\} \subset \mathbb{P}^1(\mathbb{Q})$;
- the only primes dividing the local ramification indices of f are $2,3,5$.

It is plausible that in higher dimensions there is also a rather small class of varieties with the property that their covers dominate every variety (this question was raised in [1]).

4. Elliptic curves over $\bar{\mathbb{Q}}$

This idea of collecting and spreading branching points, followed by application of Abhyankar's lemma, works to some extent over $\bar{\mathbb{Q}}$.

We will use the following notation:

- $\pi : E = E(a,b,c,d) \to \mathbb{P}^1$ an elliptic curve over $\bar{\mathbb{Q}}$, realized as a standard double cover, ramified over $a,b,c,d \in \mathbb{P}^1(\bar{\mathbb{Q}})$;
- $\mathrm{Bran}(\pi) = \{a,b,c,d\}$ the branching locus;
- $E[n] \subset E(\bar{\mathbb{Q}})$ the subgroup of torsion points of order dividing n and $E[\infty] := \cup_n E[n]$;
- $\Pi(E) := \pi(E[\infty]) \subset \mathbb{P}^1(\bar{\mathbb{Q}})$ the image of the torsion points of E.

Proposition 4.1. — *Let C be a projective hyperbolic curve with a map onto an elliptic curve $\sigma : C \to E$ such that all preimages over one branching point of σ have even local ramification indices. Let $\pi' : C' \to \mathbb{P}^1$ be such that all local ramification indices of π' are of order ≤ 2. Assume that the branching locus* $\mathrm{Bran}(\pi')$ *is contained in* $\Pi(E)$. *Then $C \Rightarrow C'$.*

Proof. — Let $E[n] \subset E$ be the subgroup of points of order dividing n, containing all the preimages of $\mathrm{Bran}(\pi')$. Consider $\phi_n : E \to E$, multiplication by n, and the induced unramified covering $\tilde{C} \to C$. Note that $\tilde{C} \to E$ is evenly ramified over the preimage of every point in $\mathrm{Bran}(\pi')$. Thus the fiber product $\tilde{C} \times_{\mathbb{P}^1} C'$ is unramified over $\tilde{C}$ and C. □

This argument leads to questions about the structure of the set $\Pi(E)$, modulo projective transformations. Note that multiplication by n on an elliptic curve E defines a map $\varphi_{n,E} : \mathbb{P}^1 \to \mathbb{P}^1$:

$$\begin{tikzcd} E \arrow[r, "\phi_n"] \arrow[d, "\pi"] & E \arrow[d, "\pi"] \\ \mathbb{P}^1 \arrow[r, "\varphi_{n,E}"'] & \mathbb{P}^1 \end{tikzcd}$$

with the property that $\Pi(E)$ is the set of periodic points for this dynamical system. This set is also invariant under the group $G(E) \subset \mathrm{PGL}_2(\bar{\mathbb{Q}})$ of projective transformations which preserve $\pi(E[2])$. Note that different elliptic curves E, E' give rise to almost disjoint set of points $\Pi(E), \Pi(E')$:

Theorem 4.2 ([4]). — *Let E, E' be elliptic curves over $\bar{\mathbb{Q}}$ and $\gamma \in$* $\mathrm{PGL}_2(\bar{\mathbb{Q}})$. *Then*

$$\Pi(E) \cap \gamma(\Pi(E'))$$

is finite provided $E' \neq E$ or $\gamma \notin G(E)$. Further, the intersection of $\Pi(E)$ *with the set of roots of unity* $\mathbb{G}_m[\infty] \subset \mathbb{P}^1(\bar{\mathbb{Q}})$ *is finite.*

Proof. — The degree 4 cover $\eta : E \times E' \to \mathbb{P}^1 \times \mathbb{P}^1$ is ramified over the union of divisors $\mathrm{Bran}(\pi) \times \mathbb{P}^1$ and $\mathbb{P}^1 \times \gamma(\mathrm{Bran}(\pi'))$. Let Δ be the diagonal in $\mathbb{P}^1 \times \mathbb{P}^1$ If $(x, x) \in \Pi(E) \times \gamma(\Pi(E'))$ then its preimage is contained in $\gamma^{-1}(\Delta)$. There are several cases :$\eta^{-1}(\Delta)$ is a union of two genus 1 curves, this means $\mathrm{Bran}(\pi) = \gamma(\mathrm{Bran}(\pi'))$, or Δ intersects the ramification divisor in more than 4 points and hence $\eta^{-1}(\Delta)$ consists of one component of genus $2, 3, 4$ or 5, depending on the size of $\mathrm{Bran}(\pi) \cap \gamma(\mathrm{Bran}(\pi'))$.

In all these cases $\eta^{-1}(\Delta)$ generates $E \times E'$. By Raynaud's theorem, the number of torsion points in $\eta^{-1}(\Delta)$ is finite. Similarly, $E \times \mathbb{G}_m \subset E \times \mathbb{P}^1$ is a double cover of $\mathbb{P}^1 \times \mathbb{P}^1$ ramified over $\mathrm{Bran}(\pi) \times \mathbb{P}^1$ and $\mathbb{P}^1 \times \{0, \infty\}$. The preimage of Δ in $E \times \mathbb{G}_m$ is a curve Δ^0, complement in E to finitely many points ($2, 3$ or 4, depending on whether or not $\mathrm{Bran}(\pi)$ contains $0, \infty$). A generalization of Raynaud's theorem proves finiteness of torsion points in the open curve $\Delta^0 \subset E \times \mathbb{G}_m$ (see [6], [7]). □

Remark 4.3. — By results of Hindry, David, Phillipon and others [12], [10], [11], it is possible to give effective upper bounds on the size of $\Pi(E) \cap \gamma(\Pi(E'))$ and $\Pi(E) \cap \mathbb{G}_m[\infty]$. These bounds are quite large and it would be interesting to get realistic estimates for them in our concrete setup.

There is a natural partial order on the set of elliptic curves over $\bar{\mathbb{Q}}$: $E \rightharpoondown E'$ if there exists a chain

$$\begin{tikzcd}
E = E_0 \arrow[d, "\pi_0"] & \cdots & E_n = E' \arrow[d, "\pi_n"] \\
\mathbb{P}^1 & & \mathbb{P}^1
\end{tikzcd}$$

(where the π_i are the standard maps) such that $\mathrm{Bran}(\pi_i) \subset \Pi(E_{i+1})$, for $i = 0, \dots, n-1$. Iterating the argument in Proposition 4.1, we find that a curve $C \to E$ as in that proposition, dominates any curve C' which is 2-ramified over points in $\Pi(E')$.

This leads to questions about the structure of the graph on the set of elliptic curves over $\bar{\mathbb{Q}}$, generated by the relation $E \rightharpoondown E'$. Note that this graph has *minimal* elements, for example the curve $E_0 : y^2 = x^3 - 1$. It does not have *maximal* elements: fields generated by torsion points are iterated extensions with Galois groups subgroups of $\mathrm{GL}_2(\mathbb{Z}/n)$ - and $\bar{\mathbb{Q}}$ cannot be obtained in this way (there are simple groups, occuring as Galois groups over the maximal abelian extension $\bar{\mathbb{Q}}^{ab}$ of $\mathbb{Q}$, without nontrivial two-dimensional representations over $\mathbb{F}_p$).

5. Apollonian fields

In this section, k is any field of characteristic $\neq 2$. In particular, we do not assume that k is algebraically closed.

Write $E := E(a,b,c,d) \to \mathbb{P}^1$ for a genus 1 curve over k, with the standard projection to $\mathbb{P}^1$, branched along $\{a,b,c,d\}$. All of the following constructions are PGL_2-equivariant, and we will freely identify a,b,c,d with elements of $k \cup \infty$, by selecting convenient coordinates on $\mathbb{P}^1$.

Consider the preimages of a,b,c,d in E (denoted by the same letters). Taking any of these points as the zero for the group law on E realizes these 4 points as $E[2] \simeq \mathbb{Z}/2 \oplus \mathbb{Z}/2$, the two-torsion subgroup. The subset $\Pi(E) \subset \mathbb{P}^1(\bar{k})$ does not depend on this choice and is equivariant with respect to the PGL_2-action on $\{a,b,c,d\} \subset \mathbb{P}^1(\bar{k})$. Note that the images in $\mathbb{P}^1$ of points of small order on E have special properties: the images of points of order 3 are PGL_2-equivalent to $\{1, \zeta_3, \zeta_3^2, \infty\}$ and the images of points of order exactly 4 are equivalent to $\{1,-1,i,-i,0,\infty\}$.

In this section we study subsets Ψ of points in $\mathbb{P}^1(\bar{k})$ obtained by an iterative procedure with the following basic step: starting with $\{a,b,c,d\} \in \Psi$, write $E := E(a,b,c,d)$ and put $\Psi = \Psi \cup \Pi(E)$. Out main result is that in many cases Ψ is projectively isomorphic to $\mathbb{P}^1(L) \subset \mathbb{P}^1(\bar{k})$, for some field L/k.

Definition 5.1. — *A* source $\mathcal{S} = \{S(a,b,c,d)\}$ *is a* PGL_2*-equivariant correspondence between 4-tuples of distinct points on* $\mathbb{P}^1(\bar{k})$ *and the set of subsets of* $\mathbb{P}^1(\bar{k})$*: for every* $\{a,b,c,d\} \subset \mathbb{P}^1(\bar{k})$ *there is given a set*

$$S(a,b,c,d) \subset \mathbb{P}^1(\bar{k})$$

such that

- $\pi(E(a,b,c,d)[4]) \subset S(a,b,c,d)$*;*
- *for all* $\gamma \in \mathrm{PGL}_2(\bar{k})$ *one has*

$$\gamma(S(a,b,c,d)) = S(\gamma(a), \gamma(b), \gamma(c), \gamma(d)).$$

We write $S(E) = S(E(a,b,c,d))$ when the branching locus is clear from the context.

Definition 5.2. — *Fix a curve E over k, with the standard projection $E \to \mathbb{P}^1$ and let*

$$\Psi_{\mathcal{S}}(E) \subset \mathbb{P}^1(\bar{k})$$

be the smallest set such that:

- *$S(E) \subset \Psi_{\mathcal{S}}(E)$;*
- *for every 4-tuple of distinct $a, b, c, d \in \Psi_{\mathcal{S}}(E)$ one has*

$$S(a, b, c, d) \subset \Psi_{\mathcal{S}}(E).$$

Example 5.3. — Special cases of $\Psi_{\mathcal{S}}(E)$ arise as follows: for n divisible by 4 (or $n = \infty$) let $\Psi_n(E) \subset \mathbb{P}^1(\bar{k})$ be the smallest subset such that

- $\pi(E[n]) \subset \Psi_n(E)$,
- for every $\gamma \in \mathrm{PGL}_2(\bar{k})$ and $\{a, b, c, d\} \subset \Psi_n(E)$ one has

$$\{\gamma(a), \gamma(b), \gamma(c), \gamma(d)\} \subset \Psi_n(E),$$

- for every quadruple $\{a, b, c, d\} \subset \Psi_n(E)$ one has

$$\pi(E(a, b, c, d)[n]) \subset \Psi_n(E).$$

For any choices of $\mathcal{S}$ as above, $\Psi_4(E) \subset \Psi_{\mathcal{S}}(E)$.

Lemma 5.4. — *For all $\gamma \in \mathrm{PGL}_2(\bar{k})$, and distinct $a, b, c, d \in \mathbb{P}^1(\bar{k})$*

$$\Psi_{\mathcal{S}}(E(\gamma(a), \gamma(b), \gamma(c), \gamma(d))) = \gamma(\Psi_{\mathcal{S}}(E(a, b, c, d))).$$

Moreover, if $\{\gamma(a), \gamma(b), \gamma(c), \gamma(d)\} \subset \Psi_{\mathcal{S}}(E(a, b, c, d))$ then

$$\Psi_{\mathcal{S}}(E(\gamma(a), \gamma(b), \gamma(c), \gamma(d))) \subseteq \Psi_{\mathcal{S}}(E(a, b, c, d)),$$

and if in addition $a, b, c, d \in \Psi_{\mathcal{S}}(E(\gamma(a), \gamma(b), \gamma(c), \gamma(d)))$, then

$$\Psi_{\mathcal{S}}(E(\gamma(a), \gamma(b), \gamma(c), \gamma(d))) = \Psi_{\mathcal{S}}(E(a, b, c, d))$$

and $\gamma \in \mathrm{Aut}(\Psi_{\mathcal{S}}(E(a, b, c, d))) \subset \mathrm{PGL}_2(\bar{k})$.

Proof. — Immediate from the definitions. □

Theorem 5.5. — *For any source $\mathcal{S}$ there exists a field $L_{\mathcal{S}}/k$ such that*

$$\Psi_{\mathcal{S}}(E(0, \infty, 1, -1)) = \mathbb{A}^1(L_{\mathcal{S}}) \cup \{\infty\} \subset \mathbb{P}^1(\bar{k}).$$

Proof. — Put $E := E(0, \infty, 1, -1)$.

Step 1. Consider the following pairs of points

$$\{0, \infty\}, \{1, -1\}, \{i, -i\} \tag{5.1}$$

Note that

$$\begin{array}{rcl} \{i, -i\} & \subset & \Psi_4(E) \subseteq \Psi_{\mathcal{S}}(E), \\ \{1, -1\} & \subset & \Psi_4(E(0, \infty, i, -i)), \\ \{0, \infty\} & \subset & \Psi_4(E(1, -1, i, -i)). \end{array}$$

Applying Lemma 5.4 we find that

$$\Psi_{\mathcal{S}}(E) = \Psi_{\mathcal{S}}(E(0, \infty, i, -i)) = \Psi_{\mathcal{S}}(E(1, -1, i, -i)).$$

Recall that there is a unique irreducible representation of the quaternion group $\mathfrak{Q}_8$ over $\bar{k}$ of dimension 2. It extends canonically to a representation of the central $\mathbb{Z}/2$-extension of $\mathfrak{S}_4$, which is the group of automorphisms of $\mathfrak{Q}_8$. It induces a natural projective action of $\mathfrak{S}_4$ and its normal subgroup $\mathbb{Z}/2 \oplus \mathbb{Z}/2 = \mathfrak{Q}_8/\mathbb{Z}/2$ on $\mathbb{P}^1$, with pairs of invariant points for the three involutions $\{1, -1\}, \{i, -i\}, \{0, \infty\}$. I.e., $\mathfrak{S}_4 \subset \mathrm{PGL}_2(\bar{k})$ acts on the 6-tuple $\{0, \infty, 1, -1, i, -i\}$ permuting the pairs in (5.1) and permuting the elements within the pairs, such that the total permutation in $\mathfrak{S}_6$ is even.

In particular, for every $\gamma \in \mathfrak{S}_4$ we have $\gamma(\Psi_{\mathcal{S}}(E)) = \Psi_{\mathcal{S}}(E)$, so that $\mathfrak{S}_4 \subset \mathrm{Aut}(\Psi_{\mathcal{S}}(E))$.

Note that for $a \in \Psi_{\mathcal{S}}(E) \setminus \{0, \infty\} \subset \bar{k}^* \subset \mathbb{P}^1(\bar{k})$ we have

$$-a, a^{-1}, -a^{-1} \in \Psi_{\mathcal{S}}(E). \tag{5.2}$$

Step 2. The set $\Psi_{\mathcal{S}}(E) \setminus \{0, \infty\}$ is a multiplicative group, i.e., every $a \in \Psi_{\mathcal{S}}(E) \setminus \{0, \infty\}$, considered as an element in $\bar{k}^* \subset \mathrm{PGL}_2(\bar{k})$, defines an bijection

$$a \cdot \Psi_{\mathcal{S}}(E) = \Psi_{\mathcal{S}}(E).$$

Indeed, by Step 1, for $a \in \Psi_{\mathcal{S}}(E)$, we have $-a \in \Psi_{\mathcal{S}}(E)$. Applying Lemma 5.4, we have

$$a \cdot \Psi_{\mathcal{S}}(E(1, -1, 0, \infty)) = \Psi_{\mathcal{S}}(E(a, -a, 0, \infty) \subseteq \Psi_{\mathcal{S}}(E(1, -1, 0, \infty))$$

The same holds for a^{-1} so that

$$a^{-1} \cdot \Psi_{\mathcal{S}}(E(1, -1, 0, \infty)) \subseteq \Psi_{\mathcal{S}}(E(1, -1, 0, \infty))$$

and

$$a \cdot a^{-1} \cdot \Psi_{\mathcal{S}}(E) = \Psi_{\mathcal{S}}(E) \subseteq a \cdot \Psi_{\mathcal{S}}(E) \subseteq \Psi_{\mathcal{S}}(E).$$

This implies that all of the above sets are equal, proving the claim.

Step 3. The group $\mathrm{Aut}(\Psi_{\mathcal{S}}(E))$ is transitive on $\Psi_{\mathcal{S}}(E)$. Indeed, by Step 2, $\Psi_{\mathcal{S}}(E) \setminus \{0, \infty\}$ is a group and hence transitive on itself. The group $\mathfrak{S}_4$ moves $\{0, \infty\}$ into its complement in $\Psi_{\mathcal{S}}(E)$.

Step 4. Pairs of distinct points in $\Psi_{\mathcal{S}}(E)$ are *equivalent* $(a, b) \sim (a', b')$ if there is a $\gamma \in \mathrm{Aut}(\Psi_{\mathcal{S}}(E))$ such that $(\gamma(a), \gamma(b)) = (a', b')$. We claim that for any ordered $(a, b) \subset \Psi_{\mathcal{S}}(E)$,

$$(a, b) \sim (1, \infty),$$

i.e., the group $\mathrm{Aut}(\Psi_{\mathcal{S}}(E))$ is doubly transitive on $\Psi_{\mathcal{S}}(E)$.

Indeed, if $(a, b) \neq (0, \infty)$ and $a \neq -b$, then $(a, b) \sim (1, b/a)$, by Step 2. The involution

$$x \mapsto (x + 1)/(x - 1) \tag{5.3}$$

preserves $\{0, 1, -1, \infty\}$ and hence induces an automorphism of $\Psi_{\mathcal{S}}(E)$.

Applying (5.3) and automorphisms from $\mathfrak{S}_4$, we find

$$(a, b) \sim (\infty, (b/a + 1)/(b/a - 1)) \sim (\infty, 1) \sim (1, \infty).$$

If $a = -b$ then

$$(a, b) \sim (1, -1) \sim (0, \infty).$$

If $a = 0$, and $b \neq \infty$, then

$$(a, b) \sim (0, 1) \sim (\infty, 1) \sim (1, \infty).$$

It remains to show that

$$(1, \infty) \sim (1, -1).$$

Choose an $a \in \Psi_{\mathcal{S}}(E) \setminus \{0, \infty, 1, -1, i, -i\}$ (such a exist) and consider the curve $E(a, -a, 0, \infty)$. The involution

$$\gamma_a : x \mapsto \frac{a(x + a)}{(x - a)}$$

on $\Psi_{\mathcal{S}}(E(a, -a, 0, \infty)) = \Psi_{\mathcal{S}}(E)$, induced by translation by points of order two on $E(a, -a, 0, \infty)$, acts by:

$$\gamma_a(a) = \infty,\ \gamma_a(\infty) = a,\ \gamma_a(-a) = 0,\ \gamma_a(0) = -a.$$

Then

$$\gamma_a(1) = a(1+a)/(1-a), \gamma_a(-1) = a(1-a)/(a+1).$$

In particular, $\gamma_a(1) \neq -\gamma_a(-1)$ (otherwise $a = \pm i$, contradicting our assumption). Then

$$(1,-1) \sim (\gamma_a(1), \gamma_a(-1)) \sim (1, \infty).$$

Step 5. The group $\mathrm{Aut}(\Psi_{\mathcal{S}}(E))$ acts 3-transitively on $\Psi_{\mathcal{S}}(E)$.

By Step 4, the action is transitive on pairs. Hence, for any distinct $a, b, c \in \Psi_{\mathcal{S}}(E)$ we have $(a, b, c) \sim (0, d, \infty)$, for some d. After multiplication by $d^{-1} \in \Psi_{\mathcal{S}}(E(0, \infty, 1, -1))$ it is equivalent to $(0, 1, \infty)$.

Step 6. We have $\Psi_{\mathcal{S}}(E) = \mathbb{P}^1(L_{\mathcal{S}})$, for some field $L_{\mathcal{S}}/k$.

It suffices to show that the set $\Psi_{\mathcal{S}}(E)$ is is preserved under the map $x \mapsto x+1$, this is equivalent to the fact that $x + 1 \in \Psi_{\mathcal{S}}(E)$, for any $x \in \Psi_{\mathcal{S}}(E)$. By Step 5, there is an automorphism $\gamma \in \mathrm{Aut}(\Psi_{\mathcal{S}}(E))$ with $(\gamma(-1), \gamma(0), \gamma(\infty)) = (0, 1, \infty)$. Such γ is unique and it gives the translation by 1. Thus $1 + \Psi_{\mathcal{S}}(E) = \Psi_{\mathcal{S}}(E)$, which finishes the proof. □

In general, any set of 4 points on $\mathbb{P}^1(\bar{k})$ is projectively equivalent to $\{a, -a, a^{-1}, -a^{-1}\}$. Note that

$$\pi(E(a, -a, a^{-1}, -a^{-1})[4]) = \{1, -1, 0, \infty, i, -i\}.$$

It follows that for any elliptic curve E the set $\Psi_{\mathcal{S}}(E)$, modulo a projective transformation, contains $\mathbb{P}^1(L_{\mathcal{S}})$.

We will use the following formulas for images of points of point of order 4:

- Let $E = E(0, a, b, \infty)$. Then $\pm\sqrt{ab} \in \pi(E[4])$.
- Let $E = E(-a, -a+1, b, \infty)$. Then $\pm\sqrt{a+b} - a \in \pi(E[4])$.

THEOREM 5.6. — *Let $k = \mathbb{F}_p$ or $\mathbb{Q}$ and $L_{\mathcal{S}}$ be the field from Theorem 5.5. For any elliptic curve E over $\bar{k}$, the set $\Psi_{\mathcal{S}}(E) \subset \mathbb{P}^1(\bar{k})$ is projectively equivalent to $\mathbb{P}^1(K_{\mathcal{S}})$, where $K_{\mathcal{S}}/L_{\mathcal{S}}$ is an algebraic extension.*

Proof. — After applying some $\gamma \in \mathrm{PGL}_2(\bar{k})$, we may assume that $E = E(a, -a, a^{-1}, -a^{-1})$, with $a \in \bar{k}$. In particular, $\Psi_{\mathcal{S}}(E)$ contains $\mathbb{P}^1(L_{\mathcal{S}})$.

Identifying $\{0,1,\infty\} \subset \pi(E[4])$ we may realize $\Psi_{\mathcal{S}}(E)\setminus\{0,\infty\}$ as a subset of $\bar{k}^*$. Let $G_{\mathcal{S}}(E) \subset \bar{k}^*$ be the (multiplicative) semi-group generated by points $\Psi_{\mathcal{S}}(E)\setminus\{0,\infty\} \subset \bar{k}^*$, and write $\Psi_{\mathcal{S}}(E)^r$ for the set of r-th powers of elements of $\Psi_{\mathcal{S}}(E)$.

Lemma 5.7. —

(1) *For all $z \in G_{\mathcal{S}}(E)$ there are $x \in \Psi_{\mathcal{S}}(E)$ and $m \in \mathbb{N}$ with $x^{2^m} = z$.*
(2) *For every $x \in \Psi_{\mathcal{S}}(E), x \notin L_{\mathcal{S}}$, and $l \in L_{\mathcal{S}}$, we have*

$$x + l \in \Psi_{\mathcal{S}}(E)^4 \subset G_{\mathcal{S}}(E).$$

Proof. — Let $z = \prod_{j=1}^m x_j \in G_{\mathcal{S}}(E)$, with $x_j \in \Psi_{\mathcal{S}}(E)$. Then $z = x^{2^r}$, with $x \in \Psi_{\mathcal{S}}(E)$ and $r \leq m$.

Indeed, this holds for $m = 2$ and $x_1 = x_2$. For $x_1 \neq x_2$:

$$\pm\sqrt{x_1x_2} \in \pi(E(0, x_1, x_2, \infty)[4]),$$

and hence $x_1x_2 \in \Psi_{\mathcal{S}}(E)^2$.

For the induction step, let $z = yx^{2^r}$, with $y \in \Psi_{\mathcal{S}}(E)$. Then $z = (\sqrt[2^r]{y} \cdot x)^{2^r}$. We know that

$$\sqrt[2^r]{y} \cdot x \in \Psi_{\mathcal{S}}(E)^2$$

(if $t \in \Psi_{\mathcal{S}}(E)$ then $\sqrt{t} \in \Psi_{\mathcal{S}}(E)$, using the curve $E(0,1,t,\infty)$). Thus there is an $\tilde{x} \in \Psi_{\mathcal{S}}(E)$ such that $\tilde{x}^2$ equals $\sqrt[2^r]{y} \cdot x$. This completes the induction and the proof of (1).

To show (2), observe that

$$(\pm\sqrt{x + l'} - l') \in \pi(E(-l', -l' + 1, x, \infty)[4]).$$

so that $-x - l' + (l')^2 \in \Psi_{\mathcal{S}}(E)^2$ and $x + l' - l'^2 \in \Psi_{\mathcal{S}}(E)^4$. Since $L_{\mathcal{S}}$ is closed under taking square roots, any $l \in L_{\mathcal{S}}$ has the form $l' - l'^2$, for some $l' \in L_{\mathcal{S}}$. It follows that $x + l \in \Psi_{\mathcal{S}}(E)^4$, as claimed. □

Lemma 5.8. — *Let $x \in \Psi_{\mathcal{S}}(E)$. If x is algebraic over $L_{\mathcal{S}}$ then $L_{\mathcal{S}}(x) \subset \Psi_{\mathcal{S}}(E)$.*

Proof. — Put $[L_{\mathcal{S}}(x) : L_{\mathcal{S}}] = m < \infty$. An element $z \in L_{\mathcal{S}}(x)$ has a representation

$$z = l_1 + x(l_2 + x(l_3 + x(\cdots + x(l_m + x)\cdots),$$

with $l_j \in L_{\mathcal{S}}$. In particular, any nonzero element is contained in $G_{\mathcal{S}}(E)$. Moreover, $L_{\mathcal{S}}(x) \subset \Psi_{\mathcal{S}}(E)^{2^m}$. The proof is inductive: if $z' \in \Psi_{\mathcal{S}}(E)^{2^{m-2}}$ then $t^{2^{m-1}} = z'x \in \Psi_{\mathcal{S}}(E)^{2^{m-1}}$ and

$$l + z'x = (l' + \zeta t)^{2^{m-1}},\ t \in \Psi_{\mathcal{S}}(E),$$

with ζ a root of 1. Since $(l' + \zeta t) \in \Psi_{\mathcal{S}}(E)^4$ we obtain the inductive statement: there is an $m \in \mathbb{N}$ such that any $z \in L_{\mathcal{S}}(x)$ has the form $z = y^{2^m}$, for some $y \in \Psi_{\mathcal{S}}(E)$.

Assume that there a $u \in L_{\mathcal{S}}(x)$ such that $u \notin \Psi_{\mathcal{S}}(E)$. Consider $u^{2^{m+1}}$. We proved that $u^{2^{m+1}} = y^{2^m}$ for some $y \in \Psi_{\mathcal{S}}(E)$. Then $u^2 = \zeta y$ where $\zeta \in L_{\mathcal{S}}$ is 2^{m+1}-th root of 1. Then $\zeta y \in \Psi_{\mathcal{S}}(E)^2$. Hence, $u^2 \in \Psi_{\mathcal{S}}(E)^2$ and one of the roots $\pm u \in \Psi_{\mathcal{S}}(E)$, and by assumption, $-u \in \Psi_{\mathcal{S}}(E)$. Applying this to $u^2 \notin \Psi_{\mathcal{S}}(E)$, we get $-u^2 \in \Psi_{\mathcal{S}}(E)$, which implies that $iu, -iu \in \Psi_{\mathcal{S}}(E)$. Note that $u, -u \in \pi(E(0, \infty, iu, -iu)[4])$ and hence both $u, -u \in \Psi_{\mathcal{S}}(E)$. This contradicts the assumption on u and proves the lemma. □

This concludes the proof of Theorem 5.6. □

Remark 5.9. — The universal fields $\Psi_n(E)$ and $\Psi_\infty(E)$ (in the notation of Example 5.3, where $S(a,b,c,d) = \pi(E(a,b,c,d)[n])$) have many remarkable properties:

- they depend on n: even for $k = \mathbb{F}_q$, restricting n we obtain proper subfields of $\bar{\mathbb{F}}_q$;
- L_∞ contains the maximal cyclotomic extension $k(\zeta_\infty)$;
- the fields L_n are 2-closed[1] if $x \in L_n$ then $\sqrt{x} \in L_n$;
- for distinct $a, b, c, d \in L_n$ we have $L_n = \Psi_n(E(a,b,c,d))$.

Conjecture 5.10. — Every elliptic curve $E(a,b,c,d)$, with $a, b, c, d \in L_\infty$, is minimal.

[1] *Apollonius of Perga*, 200 BC., author of the book *Conics*: “The most and prettiest of these theorems are new, and it was their discovery which made me aware that Euclid did not work out the synthesis of the locus with respect to three and four lines ... for it was not possible for the said synthesis to be completed without the aid of the additional theorems discovered by me...”

See `http://www-groups.dcs.st-and.ac.uk/~history/Mathematicians`

Remark 5.11. — If $\{a, b, c, d\}$ is not projectively equivalent to a subset of $\mathbb{P}^1(L_\infty)$ then $E(a, b, c, d)$ is not minimal and cannot be dominated by elliptic curves with ramification points in L_∞.

6. Surfaces

A smooth projective algebraic surface X over $\mathbb{C}$ has the following topological/algebraic invariants

- fundamental group $\pi_1(X)$;
- Brauer group $\mathrm{Br}(X)$;
- pluri-genera $\kappa_n(X)$.

These invariants do not depend on the choice of a smooth model of the function field $\mathbb{C}(X)$. They are trivial for $X = \mathbb{P}^2$.

Recall that a variety X over a field k is *rationally connected* if there exists a family of proper and connected curves $g : U \to Y$ over k whose geometric fibers have only rational components and a cycle morphism $U \to X$, such that $U \times_Y U \to X \times X$ is dominant. We say that X over k is *weakly rationally connected* there exists a Zariski open subset $X^\circ \subset X$ such two arbitrary points $x, x' \in X^\circ$ can be joined by a chain of rational curves, defined over k and contained in X. These connecting curves need not be contained in families sweeping out the variety X.

A fundamental result of classification theory of smooth projective surfaces over $\mathbb{C}$ is the equivalence of the following geometric properties:

1. rationality;
2. unirationality;
3. rational connectedness or chain-connectedness.

The situation over small fields is in many instances unclear. There are easy examples of unirational non-rational surfaces of general type:

$$x^{p+1} + y^{p+1} + z^{p+1} + t^{p+1} = 0$$

over a field of characteristic $p > 3$. Note that unirationality or uniruledness of the surface implies the triviality of its Brauer group. A sample question is

Conjecture 6.1 (Rudakov-Shafarevich [17]). — Let X be a K3 surface over a field of characteristic $p > 0$. Assume that its Brauer group $\mathrm{Br}(X)$ is trivial. Then X is unirational.

The rational connectivity notions recalled above coincide for algebraically closed k of characteristic zero, but differ over $\bar{\mathbb{F}}_p$. In fact, Theorem 2.2 implies the following

Theorem 6.2 ([5]). — *Let $X = \widetilde{A/\sigma}$ be a Kummer surface over $k = \bar{\mathbb{F}}_p$, with $p > 2$, i.e., the minimal desingularization of the quotient of an abelian surface by the standard involution. Then every finite subset of $X(k)$ in the complement to exceptional curves lies on an irreducible rational curve $R \subset X$, defined over k.*

Remark 6.3. — A similar statement holds for higher-dimensional Kummer varieties, provided that the corresponding abelian variety is dominated by a Jacobian of a hyperelliptic curve.

Conjecture 6.4. — Let A be an abelian variety over $\bar{\mathbb{F}}_p$. Then there exits a hyperelliptic curve C such that its Jacobian J_C surjects onto A.

Remark 6.5. — General abelian varieties over large fields, such as $\mathbb{C}$, of dimension ≥ 3 cannot be dominated by hyperelliptic Jacobians [14], [13]. However, Conjecture 6.4 could, theoretically, still hold over $\bar{\mathbb{Q}}$.

In fact, the proof of Theorem 6.2 gives a strong form of rational connectivity for Kummer over finite fields. Recall that on rationally connected varieties over number fields of even finite fields, it may not always be possible to connect two algebraic points by an irreducible rational curve defined over the ground field. Here we find that any finite set of $\bar{\mathbb{F}}_q$-points on a (singular) Kummer variety X, lies on an irreducible rational curve defined over $\mathbb{F}_q$, for some q depending only on X.

Using Theorem 6.2 one can construct examples of non-uniruled surfaces of general type over k with the same property [5].

Remark 6.6. — Let X be an Enriques surface over $\bar{\mathbb{F}}_p$ such that the covering K3 surface is a Kummer surface. Then X is weakly rationally connected and has a nontrivial fundamental group. In particular, both the Brauer and the fundamental group of a weakly rationally connected surfaces may be (simultaneously) nontrivial.

Conjecture 6.7. — Let X be a smooth projective surface over $\bar{\mathbb{F}}_p$ with $\mathrm{Br}(X) = 1$. Then X is weakly rationally connected. If in addition $\pi_1(X) = 1$ then X is unirational.

Question 6.8. — Does there exist a smooth weakly rationally connected surface X such that $\mathrm{Br}(X)$ and $\pi_1(X)$ are both infinite?

Question 6.9. — Are there surfaces of general type over $k = \bar{\mathbb{F}}_p$ such that

$$\cup_{R\in\mathcal{R}}\mathbb{P}(T_R),$$

over the set $\mathcal{R}$ of all rational curves on X over k, is Zariski dense in the projectivization of the tangent bundle $\mathbb{P}(T_X)$?

It is unclear how to describe the class of surfaces over $\bar{\mathbb{F}}_p$ which are *not* covered by rational curves. There are plenty of examples of such simply-connected surfaces.

Proposition 6.10. — *Let X be a smooth projective surface over $k = \bar{\mathbb{F}}_p$ so that there exist an $i > 0$ and a point $x \in X(k)$ with $H^0(X, \mathrm{Sym}^i(\Omega^1)) \neq 0$ and so that the map*

$$H^0(X, \mathrm{Sym}^i(\Omega^1)) \to H^0(x, \mathrm{Sym}^i(\Omega^1|_x)) \tag{6.1}$$

is surjective. Then X contains only a finite number of rational curves over k.

Sketch of proof. — Surjectivity in (6.1) holds on the complement of some divisor $D \subset X$. There can be no rational curves passing through the complement of D. □

A stronger result is valid in characteristic zero: if there are any nontrivial symmetric tensors then either X is ruled over a nonrational base or X contains only a finite number of rational curves. In positive characteristic, symmetric tensors can occur even on unirational surfaces.

Remark 6.11. — Let k be either $\bar{\mathbb{F}}_p$, with $p > 5$, or $\bar{\mathbb{Q}}$. Let K be an algebraically closed field containing k as a proper subfield. For any $\mathsf{g} > 0$ there exists an elliptic surface $\pi : X \to \mathbb{P}^1$ over K, without multiple fibers, such that any multisection has geometric genus $\geq \mathsf{g}$.

Indeed, consider an elliptic K3 surface X over k (non-uniruled, if k has characteristic > 0). The set of rational curves in each homology class of X is finite. Assume also that π has no section. For every rational multisection $R \subset X$ let $\rho_R \subset \mathbb{P}^1(K)$ be the set of all branching points of π restricted to R. We claim that

$$\cup_R \rho_R \subset \mathbb{P}^1(k).$$

Every R is defined over a finite extension of $\mathbb{F}_p$ or $\mathbb{Q}$, and the same holds for branching points of π.

Consider a sequence of double covers $\delta_i : \mathbb{P}^1_i \to \mathbb{P}^1_{i-1}$ with $i = 1, \ldots, \mathsf{g}$, such that for each i the image of the branching locus of δ_i under the projection $\delta_1 \circ \cdots \circ \delta_i : \mathbb{P}^1_1 \to \mathbb{P}^1_0 = \mathbb{P}^1$ is contained in $\mathbb{P}^1(K) \setminus \mathbb{P}^1(k)$. Then the pullback of the elliptic fibration over $\mathbb{P}^1_0$ to $\mathbb{P}^1_{\mathsf{g}}$ has the desired property.

Note that this construction may fail over k if the branching points of rational multisections of π fill $\mathbb{P}^1(k)$. It is not clear whether or not such surfaces can exist over $k = \bar{\mathbb{F}}_p$ or $\bar{\mathbb{Q}}$.

References

[1] F. Bogomolov and D. Husemoller – "Geometric properties of curves defined over number fields", 2000, `http://www.mpim-bonn.mpg.de`, Preprint MPI 2000-1.

[2] F. Bogomolov and Y. Tschinkel – "Unramified correspondences", Algebraic number theory and algebraic geometry, Contemp. Math., vol. 300, Amer. Math. Soc., Providence, RI, 2002, p. 17–25.

[3] ———, "Couniformization of curves over number fields", Geometric methods in algebra and number theory, Progr. Math., vol. 235, Birkhäuser Boston, Boston, MA, 2005, p. 43–57.

[4] ———, "Curves in abelian varieties over finite fields", *Int. Math. Res. Not.* (2005), no. 4, p. 233–238.

[5] ———, "Rational curves and points on $K3$ surfaces", *Amer. J. Math.* **127** (2005), no. 4, p. 825–835.

[6] E. Bombieri, D. Masser and U. Zannier – "Intersecting a curve with algebraic subgroups of multiplicative groups", *Internat. Math. Res. Notices* (1999), no. 20, p. 1119–1140.

[7] E. Bombieri and U. Zannier – "Algebraic points on subvarieties of $\mathbf{G}_m^n$", *Internat. Math. Res. Notices* (1995), no. 7, p. 333–347.

[8] J. Boxall – "Autour d'un problème de Coleman", *C. R. Acad. Sci. Paris Sér. I Math.* **315** (1992), no. 10, p. 1063–1066.

[9] ______, "Sous-variétés algébriques de variétés semi-abéliennes sur un corps fini", Number theory (Paris, 1992–1993), London Math. Soc. Lecture Note Ser., vol. 215, Cambridge Univ. Press, Cambridge, 1995, p. 69–80.

[10] S. David and M. Hindry – "Minoration de la hauteur de Néron-Tate sur les variétés abéliennes de type C. M", *J. Reine Angew. Math.* **529** (2000), p. 1–74.

[11] S. David and P. Philippon – "Minorations des hauteurs normalisées des sous-variétés de variétés abeliennes. II", *Comment. Math. Helv.* **77** (2002), no. 4, p. 639–700.

[12] M. Hindry – "Points de torsion sur les sous-variétés de variétés abéliennes", *C. R. Acad. Sci. Paris Sér. I Math.* **304** (1987), no. 12, p. 311–314.

[13] F. Oort and J. de Jong – "Hyperelliptic curves in abelian varieties", *J. Math. Sci.* **82** (1996), no. 1, p. 3211–3219, Algebraic geometry, 5.

[14] G. P. Pirola – "Curves on generic Kummer varieties", *Duke Math. J.* **59** (1989), no. 3, p. 701–708.

[15] B. Poonen – "Multiples of subvarieties in algebraic groups over finite fields", *Int. Math. Res. Not.* (2005), no. 24, p. 1487–1498.

[16] ______, "Unramified covers of Galois covers of low genus curves", *Math. Res. Lett.* **12** (2005), no. 4, p. 475–481.

[17] A. N. Rudakov and I. R. Šafarevič – "Supersingular $K3$ surfaces over fields of characteristic 2", *Izv. Akad. Nauk SSSR Ser. Mat.* **42** (1978), no. 4, p. 848–869.