Canad. J. Math. Vol. **56** (3), 2004 pp. 612–637

Solvable Points on Projective Algebraic Curves

Ambrus Pál

Abstract. We examine the problem of finding rational points defined over solvable extensions on algebraic curves defined over general fields. We construct non-singular, geometrically irreducible projective curves without solvable points of genus g, when g is at least 40, over fields of arbitrary characteristic. We prove that every smooth, geometrically irreducible projective curve of genus 0, 2, 3 or 4 defined over any field has a solvable point. Finally we prove that every genus 1 curve defined over a local field of characteristic zero with residue field of characteristic p has a divisor of degree prime to $6p$ defined over a solvable extension.

1 Introduction

Definition 1.1 Let X be a quasi-projective variety over a field F. We say that P is a solvable point of X over F if P is a rational point of X defined over a solvable extension of F. Similarly we say that D is a solvable divisor of X over F if D is a rational divisor of X defined over a solvable extension of F.

In this paper we will examine the following question:

Question 1.2 Given a field F and a natural number g, is there any smooth, geometrically irreducible projective curve of genus g over the field F which does not have solvable points over F?

Remark 1.3 The condition of geometric irreducibility in the question is necessary to have a nontrivial problem. For example we can take a smooth projective curve which is not geometrically irreducible such that the absolute Galois group acts on the set of its irreducible components over the separable closure of F through a non-solvable quotient. A natural condition to rule out these pathological examples is to require that the curve is geometrically irreducible.

Our first theorem suggests that the phenomenon of smooth, geometrically irreducible projective curves without solvable points is quite general:

Theorem 1.4 *If there is a quasi-projective, geometrically irreducible variety over an algebraic extension K of the perfect field F which does not have solvable points over K, then there is a smooth, geometrically irreducible projective curve over F which does not have solvable points over F.*

Our second result shows that for any prime p there is a field F of characteristic p such that for any positive integer g which is at least 40 there is a smooth, geometrically

Received by the editors August 27, 2002.
AMS subject classification: 14H25,11D88.

irreducible curve defined over F of genus equal to g without solvable points. More precisely:

Theorem 1.5 *Let F be a local field such that the absolute Galois group of its residue field has quotients isomorphic to S_5, $\mathrm{PSL}_3(\mathbb{F}_2)$ and $\mathrm{PSL}_3(\mathbb{F}_3)$. Then there is a non-singular, geometrically irreducible projective curve defined over F of genus g without solvable points when g is equal to* 6, 8, 10, 11, 15, 16, 20, 21, 22, 25, 26, 27, 28, 29, 30, 31, 32, 34, 35, 36, 37, 38 *or at least* 40.

The structure of the proof of the theorem is the following. First we construct a connected, but geometrically reducible stable curve of arithmetic genus g without solvable points over the residue field using the assumption on its absolute Galois group. This construction is essentially combinatorial in nature. Then we use the results of [2] on the moduli of stable curves to construct a flat projective curve over the spectrum of the discrete valuation ring of F such that its generic fiber is smooth and geometrically irreducible and its special fiber is the stable curve above. The generic fiber will be of genus g without solvable points. The theorem above obviously does not apply when F is the completion of a number field, because the hypothesis on the absolute Galois group of the residue field does not hold. Actually the claim is false in this case, as the absolute Galois group of F is solvable. However, the method of the theorem does apply when F is finitely generated of transcendence degree at least one over an algebraically closed field of uncountable cardinality (Theorem 4.11) and for certain function fields over more general fields (Theorems 4.13 and 4.14) where the method and Theorem 1.4 will be used to prove less precise results.

On the other hand our third theorem says that there are natural numbers g such that there are not any smooth, geometrically irreducible projective curves of genus g defined over an arbitrary field without solvable points:

Theorem 1.6 *Let F be any field and let X be a smooth, geometrically irreducible projective curve defined over F such that its genus is* 0, 2, 3, *or* 4. *Then X has a solvable point.*

There is a similar result for surfaces. We will call a variety X defined over a field F geometrically rational if it is irreducible and rational over the algebraic closure of F. The theorem is the following:

Theorem 1.7 *Let F be any field and let X be a smooth, geometrically rational projective surface defined over F. Then X has a solvable point.*

We will prove these results by examining the canonical linear system on X in order to construct zero-dimensional cycles on X of low degree defined over a solvable extension of F. In order to prove the second theorem we will also show that the Merkurjev-Suslin theorem implies that every Brauer-Severi variety defined over an arbitrary field has a solvable point.

We will also use this result when we examine the following question related to the one above:

Question 1.8 Given a field F and natural numbers g and d, is there any smooth, geometrically irreducible projective curve of genus g over the field F which does not have solvable divisors of degree d defined over F?

https://doi.org/10.4153/CJM-2004-028-0 Published online by Cambridge University Press

It is clear that if a curve X has a solvable point then it has a solvable divisor of degree d defined over F for any natural number d. On the other hand we will see that there are smooth, geometrically irreducible projective curves without solvable points but with a solvable divisor of arbitrary degree.

Our first result about this question is the following:

Theorem 1.9 *Let F be a perfect field of characteristic p or a local field of characteristic zero with a residue field of characteristic p. Let X be a smooth, geometrically irreducible projective curve of genus 1 defined over F. Then there is a solvable divisor on X whose degree is relatively prime to $6p$.*

As an application of this result and the construction used in Theorem 1.5 we have finally a result which answers a question similar to 1.8 in a non-trivial case:

Theorem 1.10 *Let F be a local field of characteristic zero with a residue field of characteristic p where $p = 5$ or $p = 7$. Assume that the absolute Galois group of the residue field of F has a quotient isomorphic to S_5, if $p = 5$, and has a quotient isomorphic to $\mathrm{PSL}_3(\mathbb{F}_2)$, if $p = 7$. Then there is a smooth, geometrically irreducible projective curve of genus g without a solvable divisor whose degree is relatively prime to p if and only if p divides $g - 1$ and g is at least 2.*

Notation 1.11 In this paper, if not otherwise stated, we will use the following terminology and notation. By a local field we mean a field complete with respect to a discrete valuation. By a solvable extension we mean a separable extension with a solvable Galois group. Let S_n denote the symmetric group on n letters for any natural number n. For any abelian category $\mathcal{A}$ and any object M of $\mathcal{A}$ let $M[n]$ denote the kernel of multiplication by n in M. For any field F let $\bar{F}$, F^p denote its separable closure and its perfection, respectively. Let X be a regular, geometrically irreducible projective variety defined over the field F. Let $\mathrm{Div}(X)$, $\mathrm{Pic}(X)$, $\mathrm{Pr}(X)$ and $\mathrm{Rt}(X)$ denote the functors from the category of extensions of F to the category of abelian groups which assigns to every extension K of F the group of divisors on X defined over K, the group of linear equivalence classes of divisors on X defined over K, the group of principal divisors on X defined over K and the multiplicative group of nonzero rational functions on X defined over K, respectively. If X is a regular, geometrically irreducible projective curve defined over the field F, then let $\mathrm{Div}_0(X)$, $\mathrm{Pic}_0(X)$ denote the functors from the category of extensions of F to the category of abelian groups which assigns to every extension K of F the group of degree zero divisors on X defined over K, and the group of linear equivalence classes of degree zero divisors on X defined over K, respectively. Restricted to finite separable extensions of a fixed extension K, the functors $\mathrm{Div}(X)$, $\mathrm{Pr}(X)$ and $\mathrm{Rt}(X)$ are sheaves on the étale topology, but $\mathrm{Pic}(X)$, $\mathrm{Pic}_0(X)$ are only presheaves. Let $\underline{\mathrm{Pic}}(X)$, $\underline{\mathrm{Pic}}_0(X)$ denote their sheafification. Let $r_{L|K}$ denote by abuse of notation all natural restriction homomorphisms on the cohomology groups of the functors such as $\underline{\mathrm{Pic}}(X)$, $\mathrm{Pr}(X)$ or $\mathbf{G}_m$ for any pair of extensions $K \subseteq L$ of F.

https://doi.org/10.4153/CJM-2004-028-0 Published online by Cambridge University Press

2 A General Reduction

Definition 2.1 Let $K|F$ be a finite extension of fields and let X be a quasi-projective variety defined over the field K. We define the norm $N_{K|F}(X)$ of X as the functor from $\mathrm{Spec}(F)$-schemes to sets which assigns to each $\mathrm{Spec}(F)$-scheme Z the set of all $\mathrm{Spec}(K)$-morphisms from the base change $Z \times_{\mathrm{Spec}(F)} \mathrm{Spec}(K)$ to X. We will examine the representability of this functor in the next proposition. If the functor is representable, we will denote the scheme, which represents it, by the same symbol.

Proposition 2.2 *Assume that the extension $K|F$ is separable. Then the functor $N_{K|F}(X)$ is representable by a quasi-projective variety over F. If X is geometrically irreducible, then the norm $N_{K|F}(X)$ is also geometrically irreducible.*

Proof Let L be a finite Galois extension of F with Galois group G over F which contains the field K. Let X also denote the base change $X \times_{\mathrm{Spec}(K)} \mathrm{Spec}(L)$ by abuse of notation. Then the variety $N_{L|F}(X)$ exists and it is isomorphic to the product $\prod_{g\in G} X^g$ over L, where X^g is the g-conjugate of X (see [13, 1.3, pp. 4–7]). Let H be the subgroup of G fixing the field K. The group H acts naturally on the functor $N_{L|F}(X)$, and the sub-functor of H-invariant maps is naturally isomorphic to the functor $N_{K|F}(X)$ by Galois theory. This functor is representable by the fixed variety of the F-rational action of H on $N_{L|F}(X)$. This variety is obviously quasi-projective. It is also geometrically irreducible, because it is isomorphic to the product $\prod_{g\in R} X^g$ over L, where R is a set of representatives of the cosets of H in G, as the product of geometrically irreducible varieties is also geometrically irreducible. ■

Theorem 2.3 *If there is a quasi-projective, geometrically irreducible variety over an algebraic extension K of the perfect field F which does not have solvable points over K, then there is a smooth, geometrically irreducible projective curve over F which does not have solvable points over F.*

Proof We can assume that F has a non-solvable extension, otherwise the claim of the theorem is trivial. This assumption also implies that F must be infinite. Let X be a quasi-projective, geometrically irreducible variety over an algebraic extension K of F such that it does not have solvable points. We can actually assume that $K|F$ is finite. The norm $N_{K|F}(X)$ of the variety X is geometrically irreducible by Proposition 2.2. Also if it has a point over an extension L of F then X has a point over the composite of K and L simply by its universal property. If L is solvable, this extension of K is also solvable, hence we can assume that X is defined over F. By Bertini's theorem applied to some projective embedding of X (see [5, Theorem 6.3, parts (2), (3) and (4), pp. 66–67]) the set of hyper-plane sections of X which are regular and geometrically irreducible is non-empty. Successively applying this remark we can conclude that there is an quasi-projective, regular, geometrically irreducible curve U which does not have solvable points over F.

The curve U can be embedded in a regular projective curve C. We will construct a finite cover D of C which is regular, geometrically irreducible and the Galois group of the field of definition of each geometric point in the pre-image of the complement of U is non-solvable. Because any variety over F having an $\mathrm{Spec}(F)$-morphism into U

https://doi.org/10.4153/CJM-2004-028-0 Published online by Cambridge University Press

does not have solvable points over F, this curve D does not have solvable points either over F. Let P denote the divisor which is the sum of all points in the complement of U. Take a very ample divisor class $\mathcal{L}$ on C defined over F. Because F is infinite, there is a divisor Q in $\mathcal{L}$ whose support is disjoint from the support of P. Then the divisor class of $P+Q$ is very ample, so there is a divisor R linearly equivalent to $P+Q$, whose support is disjoint from the support of $P+Q$. With this definitions there is a map $f: C \to \mathbf{P}^1$ such that the pre-image of 0, 1 are the divisors $P+Q$ and R, respectively.

Lemma 2.4 *Let $p(x) \in F[x]$ be a separable polynomial of degree n. Then there is an affine plane curve $X \subset \mathbf{A}^2_F$ defined by the polynomial $q(x,y) \in F[x,y]$ such that*

(a) $q(x,0) = p(x)$,
(b) $\deg(q) = n$,
(c) $q(x,1) = x^n$,
(d) *The point $(0,1) \in X$ is regular.*

Proof Write $p(x) = \sum_{k=0}^{n} a_k x^k$. Consider the polynomial

$$q(x,y) = \sum_{k=0}^{n} p_k(y) x^k,$$

where $p_0(y) = a_0 + ay + by^2$, $p_n(y) = a_n + (1-a_n)y$ and $p_k(y) = a_k - a_k y$ for all other k. Then $q_y(0,1) = p_0'(1)$ and $q(x,1) = p_0(1) + x^n$, hence the polynomial $q(x,y)$ will satisfy the requirements of the lemma if $p_0(1) \neq 0$ and $p_0(1) = 0$. This means for a, b that $a_0 + a + b = 0$ and $a + 2b \neq 0$. By substitution we can reduce this to the condition $2a_0 \neq a$, which can always be satisfied. ∎

Let us return to the proof of the theorem. Take an irreducible polynomial $p(x) \in F[x]$, whose Galois group is not solvable and let X denote Zariski closure in the projective plane of the plane curve constructed in Lemma 2.4. The center of projection to the y-coordinate axis is not in X, hence it defines a degree n covering $X \to \mathbf{P}^1$. We define the covering $D \to C$ as the normalization of the pull-back of this covering above with respect to f, which is denoted by E.

The geometric points of E in the pre-image of R are regular, hence the normalization map $D \to E$ is one to one in a Zariski neighborhood of those points. D is geometrically irreducible if it is geometrically connected. If it is not geometrically connected, then D will have at least two geometric points in the pre-image of any geometric point of C with respect to the cover map $D \to C$. But this cannot be true for the pre-image of R. On the other hand the natural map $D \to X$ is Galois-invariant, hence the action on the pre-image of $P+Q$ does not factor through a solvable quotient. ∎

3 Combinatorics

Definition 3.1 For any graph G let $\mathcal{V}(G)$ and $\mathcal{E}(G)$ denote its set of vertices and edges, respectively. An automorphism of G is a pair (π_1, π_2) where π_1, π_2 is a permutation of $\mathcal{V}(G)$ and $\mathcal{E}(G)$, respectively such that a vertex $v \in \mathcal{V}(G)$ is on an edge

https://doi.org/10.4153/CJM-2004-028-0 Published online by Cambridge University Press

$e \in \mathcal{E}(G)$ then $\pi_1(v)$ is on $\pi_2(e)$. If G is a simple graph then π_1 uniquely determines π_2. The set of automorphisms of G forms a group with respect to composition which is denoted by $\mathrm{Aut}(G)$. We say that G is without solvable orbits if $\mathrm{Aut}(G)$ acts on the orbit of any vertex in $\mathcal{V}(G)$ and any edge in $\mathcal{E}(G)$ through a non-solvable quotient. A group Γ acts on a graph G if a homomorphism $\Gamma \to \mathrm{Aut}(G)$ is given. We say that Γ acts on G without solvable orbits if Γ acts on the orbit of any vertex in $\mathcal{V}(G)$ and any edge in $\mathcal{V}(G)$ through a non-solvable quotient.

Lemma 3.2 *The graph G is without solvable orbits if and only there is a group Γ which acts on G without solvable orbits.*

Proof We only have to prove that the second assumption implies the first. For any vertex $v \in \mathcal{V}(G)$ the Γ-orbit of v is contained in its $\mathrm{Aut}(G)$-orbit. By assumption Γ acts on this orbit through a non-solvable quotient, so $\mathrm{Aut}(G)$ acts on the orbit of v through a group which has a non-solvable subgroup and therefore it is itself non-solvable. A similar argument for any edge in $\mathcal{E}(G)$ concludes the proof. ∎

Definition 3.3 We define the Euler characteristic of a graph G, denoted by $e(G)$, as the sum $1 + |\mathcal{E}(G)| - |\mathcal{V}(G)|$, where $|X|$ denotes the cardinality of a set X. A graph G is stable, if it is connected and the degree of any vertex in $\mathcal{V}(G)$ is at least 3.

Proposition 3.4 *There is a stable graph without solvable orbits of Euler characteristic equal to* 6, 8, 10, 11, 15, 16, 20, 21, 22, 25, 26, 27, 28, 29, 30, 31, 32, 34, 35, 36, 37, 38 *or at least* 40.

Proof Let n, x be natural numbers such that n is bigger than 4. We define the graph $S_n(x)$ as follows. Its set of vertices is $1, 2, \ldots, n$. Its set of edges contains one edge connecting any two different vertices and for each vertex i exactly x loops fitting on i. $S_n(x)$ is clearly stable and its Euler characteristic

$$e(S_n(x)) = \frac{n(n-3)}{2} + nx + 1.$$

S_n acts on $S_n(x)$ as follows. For each vertex i we index its loops by $i_1, i_2, \ldots, i_x$. If $\pi \in S_n$ is a permutation, *i.e.*, a bijective function $\pi\colon \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$, we extend its natural action on the simple graph spanned by $\mathcal{V}(S_n(x))$ to an automorphism $\tilde{\pi} \in \mathrm{Aut}(S_n(x))$ whose action on the loops is given by the formula $\tilde{\pi}(i_j) = \pi(i)_j$ for all $1 \le i \le n$ and $1 \le j \le x$.

Let n, m, x, y be natural numbers such that n, m are bigger than 4. We define the graph $S_{n,m}(x, y)$ as follows. Its set of vertices is $1, 2, \ldots, n + m$. Its set of edges contains exactly one edge between i and j for all $i \le n$ and $n + 1 \le j \le n + m$, for each vertex $i \le n$ exactly x loops fitting on i, and for each vertex $n + 1 \le j \le n + m$ exactly y loops fitting on j. $S_{n,m}(x, y)$ is stable and its Euler characteristic

$$e(S_{n,m}(x, y)) = (n-1)(m-1) + nx + my.$$

The direct product $S_n \times S_m$ acts on $S_{n,m}(x, y)$ as follows. For each vertex $i \le n$, $n + 1 \le j \le n + m$ we index its loops by $i_1, i_2, \ldots, i_x$ and $j_1, j_2, \ldots, j_y$, respectively. If $(\pi_1, \pi_2) \in S_n \times S_m$ is a pair of permutations, *i.e.*, two bijective functions

https://doi.org/10.4153/CJM-2004-028-0 Published online by Cambridge University Press

$\pi_1\colon \{1,2,\dots,n\} \to \{1,\dots,n\}$ and $\pi_2\colon \{1,2,\dots,m\} \to \{1,\dots,m\}$, then we extend the natural action of (π_1,π_2) on the simple graph spanned by $\mathcal{V}(S_{n,m}(x,y))$ to an automorphism $\tilde{\pi} \in \mathrm{Aut}(S_{n,m}(x,y))$ whose action on the loops is given by the formulas $\tilde{\pi}(i_k) = \pi_1(i)_k$, $\tilde{\pi}(j_l) = (\pi_2(j-n)+n)_l$, for all $1 \le i \le n$, $1 \le k \le x$, and $n+1 \le j \le n+m$, $1 \le l \le y$, respectively.

Finally let q be a power of a prime and let x be a natural number. We define the graph $P_q(x)$ as follows. Its set of vertices is the disjoint union of $\mathbf{P}_2(\mathbb{F}_q)$, $\hat{\mathbf{P}}_2(\mathbb{F}_q)$, the set of points and lines of the projective plane over the finite field $\mathbb{F}_q$, respectively. Its set of edges contains exactly one edge between two different vertices i, j if $i \in \mathbf{P}_2(\mathbb{F}_q)$, $j \in \hat{\mathbf{P}}_2(\mathbb{F}_q)$ and the point i is on the line j, and for each vertex $i \in \mathbf{P}_2(\mathbb{F}_q)$ exactly x loops fitting on i. $P_q(x)$ is stable and its Euler characteristic

$$e(P_q(x)) = (q-1+x)(q^2+q+1)+1.$$

The projective linear group $\mathrm{PGL}_3(\mathbb{F}_q)$ acts on $P_q(x)$ as follows. For each vertex $i \in \mathbf{P}_2(\mathbb{F}_q)$ we index its loops by $i_1, i_2, \dots, i_x$. The group $\mathrm{PGL}_3(\mathbb{F}_q)$ acts on the simple graph spanned by $\mathcal{V}(P_q(x))$ naturally. If $\pi \in \mathrm{PGL}_3(\mathbb{F}_q)$ is considered here as a bijective function $\pi\colon \mathbf{P}_2(\mathbb{F}_q) \to \mathbf{P}_2(\mathbb{F}_q)$, we extend its action above to an automorphism $\tilde{\pi} \in \mathrm{Aut}(P_q(x))$ whose action on the loops is given by the formula $\tilde{\pi}(i_j) = \pi(i)_j$ for all $i \in \mathbf{P}_2(\mathbb{F}_q)$ and $1 \le j \le x$.

By the formulas above, $S_5(0)$, $S_5(1)$, $S_5(2)$, $S_5(3)$ has Euler characteristic 6, 11, 16, 21, respectively. Moreover $P_2(0)$, $P_2(1)$, $P_2(2)$, $P_2(3)$, $P_2(4)$ and $P_3(0)$ has Euler characteristic 8, 15, 22, 29, 36 and 27. Since every integer greater than or equal to 40 can be written is the form $20+5x+6y$ for some non-negative integers x and y, and $e(S_{5,6}(x,y)) = 20+5x+6y$, every positive integer $n \ge 40$ occurs as the Euler characteristic of the graph $S_{5,6}(x,y)$ for some x, y. Finally the numbers 20, 25, 26, 30, 31, 32, 35, 36, 37 and 38 are elements of the set of Euler characteristics of the graphs $S_{5,6}(x,y)$ for $x \le 3$ and $y \le 3$. ■

The following combinatorial result implies that there are natural numbers g which do not occur as the Euler characteristic of a connected graph without solvable orbits, hence our method of proving Theorem 1.5. cannot be generalized to construct smooth, geometrically irreducible projective curve of genus g without solvable points. This is particularly interesting in the cases $g = 5$, $g = 7$ and $g = 9$, since in these cases we cannot prove that every smooth, geometrically irreducible projective curve of genus g has a solvable point.

Proposition 3.5 *If G is a connected graph without solvable orbits of Euler characteristic less than* 10 *then its Euler characteristic is equal to* 6 *or* 8.

Proof Assume that G has a loop. The set of vertices with loops is invariant with respect to the action of $\mathrm{Aut}(G)$. Since any subgroup of the symmetric group on four letters is solvable, the cardinality of the set above is at least five if it is not empty. This implies that the number of loops is also bigger than four, so the Euler characteristic of the graph $\tilde{G}$ which is G with all the loops removed is at most 4. $\tilde{G}$ is without solvable orbits, so we can assume that G has not any loops.

https://doi.org/10.4153/CJM-2004-028-0 Published online by Cambridge University Press

Assume that G has a multiple edge. $\mathrm{Aut}(G)$ acts on the set of unordered pairs of vertices (v, u), where there are more then one edge connecting v with u. Let Γ denote the quotient by the kernel of this action. If $\pi \in \mathrm{Aut}(G)$ fixes all pairs of vertices above, then it acts on the set of vertices which are connected to another vertex with more than one edge as an involution. Hence $\mathrm{Aut}(G)$ acts on the set of vertices above through a quotient which is the extension of Γ by a 2-torsion group. Since this quotient is not solvable, Γ is not either, so the number of the unordered pairs above is at least 5. This implies that if we substitute each multiple edge by a single one in G, then the Euler characteristic of the new graph will be at most 4. This graph is also without solvable orbits and connected, hence we can assume that G has not any multiple edges, so it is a simple graph.

If we remove each vertex of degree 1 from G then the new graph is still connected and without solvable orbits, and has the same Euler characteristic as the old graph. Similarly, if we remove each vertex of degree 2 and connect any remaining pair of vertices (which might coincide) if they were connected by a path of vertices of degree 2, then the new graph is again connected and without solvable orbits, and has the same Euler characteristic as the old graph (although it might not be simple). Using the reductions of the first two paragraphs, if it is necessary, we can assume that G is a simple graph such that the degree of each vertex is at least 3.

Let r_d denote the number of vertices of degree d. Since $\mathrm{Aut}(G)$ leaves the set of vertices of degree d invariant for each positive d, we have $r_d \geq 5$ for each d such that r_d is non-zero. Since we have $9 \geq e(G) = 1 + \sum(d/2 - 1)r_d$, at most r_3 and r_4 can be non-zero. But both of them cannot be non-zero at once, unless $r_3 = 6$ and $r_4 = 5$. Otherwise $e(G) = 6$ or 8, or G is either 3-regular and $r_3 = 6$, 8, 12 or 16, or G is 4-regular and $r_4 = 6$ or 8.

Assume that there is an orbit O of vertices with respect to the action of $\mathrm{Aut}(G)$ such that its cardinality is divisible by a prime p different from 2 or 3. Let P be another orbit which has a vertex adjacent to a vertex in O. The number of edges connecting a vertex in O to vertices in P is the same because the action of $\mathrm{Aut}(G)$ is transitive on O, and similarly the number of edges connecting a vertex in P to vertices in O is the same. These two numbers are not divisible by primes other than 2 and 3, because they are less than 5, hence the cardinality of P is also divisible by p. Since G is connected this implies that the cardinality of each orbit is divisible by p, which is impossible by the above.

Let $v \in \mathcal{V}(G)$ be vertex. $\mathrm{Aut}(G)$ acts on the orbit of v through a quotient which we denote by Γ. Let Γ_i be the subgroup of Γ which fixes all vertices connected to v by a path of length at most i. Clearly Γ_{i+1} is a normal subgroup in Γ_i. The factor set Γ/Γ_0 can be identified with the orbit of v, so it not divisible by primes other than 2 or 3. The same holds for the quotient group Γ_i/Γ_{i+1}. This group acts faithfully on the set X_i of vertices which are connected to v by a path of length i but not connected by a path of length less than i. The set of vertices connected to any vertex fixed by Γ_i is left invariant by Γ_i/Γ_{i+1}. These sets cover X and each has cardinality less than 5, hence Γ_i/Γ_{i+1} injects into a direct product power of S_4. Because the groups Γ_i define a filtration on the group Γ, the order of the latter is not divisible by primes other than 2 or 3. But such a group must be solvable by Burnside's $p^a q^b$ theorem (see [1, pp. 221–222]). ■

https://doi.org/10.4153/CJM-2004-028-0 Published online by Cambridge University Press

4 Constructions

For any scheme S and any stable curve $\pi\colon C \to S$ of genus g let $\omega_{C/S}$ denote relative dualizing sheaf. The sheaf $\omega_{C/S}^{\otimes 3}$ is relatively very ample by Theorem 1.2 of [2, p. 77] and its corollary. This result implies that the functor which assigns to each scheme S the set of stable curves $\pi\colon C \to S$, and an isomorphism $\mathbf{P}(\pi_*(\omega_{C/S}^{\otimes 3})) \cong \mathbf{P}_S^{5g-6}$ (modulo isomorphism) is represented by a fine moduli scheme $\mathfrak{H}_g$. The following two results are Corollary 1.7 of [2, p. 83] and the main result of [2, pp. 92–96], respectively.

Theorem 4.2 *The scheme $\mathfrak{H}_g$ is smooth over the spectrum of $\mathbb{Z}$ and the base change $(\mathfrak{H}_g)_{\mathrm{Spec}(F)}$ is irreducible for any algebraically closed field F.* ∎

Lemma 4.3 *Let R be a discrete valuation ring and let $\mathbf{f}$, F denote its residue field and quotient field, respectively. Let $\mathcal{X}$ be a smooth scheme of finite type over $\mathrm{Spec}(R)$. Let X^0 be an open dense sub-scheme of the base change $\mathcal{X}_{\mathrm{Spec}(F)}$. Then for any morphism $p\colon \mathrm{Spec}(\mathbf{f}) \to \mathcal{X}$ over $\mathrm{Spec}(R)$ there is a morphism $\mathrm{Spec}(R) \to \mathcal{X}$ whose specialization to $\mathrm{Spec}(\mathbf{f})$ is p, and its restriction to $\mathrm{Spec}(F)$ maps into X^0.*

Proof By Proposition 3.24 of [10, p. 31] we can assume that $\mathcal{X} = \mathrm{Spec}(A)$, where

$$A = R[T_1, T_2, \dots, T_n]/(P_1, P_2, \dots, P_m),\ P_i \in R[T_1, T_2, \dots, T_n], \quad m \leq n$$

and the ideal generated by the $m \times m$ minors of $(\partial P_i/\partial T_j)$ is A. Let $\mathfrak{p} \lhd A$ be the maximal ideal which is the kernel of the homomorphism $p^*\colon A \to \mathbf{f}$ corresponding to the morphism p. One of the minors above is not in $\mathfrak{p}$. We can assume that this minor is $\det(\partial P_i/\partial T_j)_{i,j=1}^m$. Since $p^*|_R$ is surjective for each $n-m+1 \leq j \leq n$ there is an $a_j \in R$ such that the polynomial $P_j = T_j - a_j \in \mathfrak{p}$. Because $\det(\partial P_i/\partial T_j)_{i,j=1}^n$ is not in the ideal $\mathfrak{p}$ as well, by Theorem 4.2 of [10, pp. 32–34] there are $a_i \in R$ for each $1 \leq i \leq n-m$ such that $P_j(a_1, a_2, \dots, a_n) = 0$ for each $1 \leq i \leq n$. The projection map $\pi\colon \mathcal{X} \to \mathbf{A}_R^{n-m}$ to the last $n-m$ coordinates is étale in a Zariski neighborhood of the point $(a_1, \dots, a_n)$. Hence the image of the closed complement of the intersection of X^0 with this neighborhood is a proper constructible subset of $\mathbf{A}_R^{n-m}$. The intersection I of the complement of this set with the unit open ball around the point $(0, 0, \dots, 0)$ with respect to the valuation of R is non-empty. The projection map π has an inverse on a sufficiently small ball contained in the unit ball around $(0, 0, \dots, 0)$ mapping $(0, 0, \dots, 0)$ to $(a_1, a_2, \dots, a_n)$ by the inverse function theorem. The image of a point in I with respect to this inverse is an R-valued point satisfying the properties in the claim above. ∎

Corollary 4.4 *Let R, $\mathbf{f}$ and F be as above. Let C be a stable curve over $\mathrm{Spec}(\mathbf{f})$. Then there is a stable curve $\pi\colon \mathcal{C} \to \mathrm{Spec}(R)$ such that the base change $\mathcal{C}_{\mathrm{Spec}(F)}$ is a smooth, geometrically irreducible projective curve and $\mathcal{C}_{\mathrm{Spec}(\mathbf{f})}$ is isomorphic to C.*

Proof Assume that the stable curve C has genus g. Define X^0 as the open sub-variety of $(\mathfrak{p}_g)_{\mathrm{Spec}(F)}$ of tri-canonical non-singular curves. This sub-variety is also dense, since it is a non-empty and $(\mathfrak{H}_g)_{\mathrm{Spec}(F)}$ is irreducible. The curve C defines a morphism $p\colon \mathrm{Spec}(\mathbf{f}) \to (\mathfrak{H}_g)_{\mathrm{Spec}(R)}$ over $\mathrm{Spec}(R)$. The claim follows from applying the lemma above to $\mathcal{X} = (\mathfrak{H}_g)_{\mathrm{Spec}(R)}$, p and X_0. ∎

https://doi.org/10.4153/CJM-2004-028-0 Published online by Cambridge University Press

Definition 4.5 A stable curve with rational components over F is a stable curve C over $\mathrm{Spec}(F)$ whose base change to $\mathrm{Spec}(\bar{F})$ has only rational curves as components. Let C be a stable curve with rational components over F. Let C_0 denote the the base change of C to $\mathrm{Spec}(\bar{F})$. We denote by $\Gamma(C)$ the graph whose set of vertices is the set of irreducible components of C_0, its set of edges of $\Gamma(C)$ is the set of singular points of C_0, and the extremities of an edge $v \in \mathcal{E}(\Gamma(C))$ are the irreducible components on which v lies. Note that the arithmetic genus of C is equal to $e(\Gamma(C))$, and the absolute Galois group $\mathrm{Gal}(\bar{F}|F)$ of F acts on the graph $\Gamma(C)$.

Proposition 4.6 *Let G be a stable graph with an action by $\mathrm{Gal}(\bar{F}|F)$. Assume that F is infinite. Then there exists a stable curve C with rational components over F such that there is a Galois-equivariant isomorphism between G and $\Gamma(C)$.*

Proof Let $\tilde{G}$ be the oriented graph whose set of vertices is $\mathcal{V}(G)$ and for each $e \in \mathcal{E}(G)$ there are exactly two edges of $\tilde{G}$ whose orientation is opposite and their extremities are the same as the extremities of e. The absolute Galois group $\Gamma = \mathrm{Gal}(\bar{F}|F)$ acts on $\tilde{G}$, too. Let $O_1, O_2, \ldots, O_n$ denote the orbits of Γ on the set of edges of $\tilde{G}$. Choose an edge $o_j \in O_j$ for every orbit. For each edge o_j let Γ_j, Γ_j^i and Γ_i^t denote the stabilizer of the edge o_j, its initial and terminal vertex in Γ, respectively. Moreover let F_j, F_j^i and F_j^t denote the sub-field of $\bar{F}$ fixed by Γ_j, Γ_j^i and Γ_j^t, respectively. Since these subgroups are of finite index in the absolute Galois group Γ, the fields above are finite separable extensions of F. Since $\Gamma_j \subseteq \Gamma_j^i$, $\Gamma_j \subseteq \Gamma_j^t$ for each j, we have closed immersions $j^i\colon \mathrm{Spec}(F_j) \to \mathrm{Spec}(F_j^i)$ and $j^t\colon \mathrm{Spec}(F_j) \to \mathrm{Spec}(F_j^t)$ as well. Choose for each edge o_j a different point $p_j\colon \mathbf{P}^0_F \to \mathbf{P}^1_F$ of the projective line over $\mathrm{Spec}(F)$. This is possible because F is infinite. Define the schemes X and Y over $\mathrm{Spec}(F)$ as

$$X = \coprod_j \mathrm{Spec}(F_j^i) \times_F \mathbf{P}^1_F \cup \coprod_j \mathrm{Spec}(F_j^t) \times_F \mathbf{P}^1_F$$

and

$$Y = \coprod_j \mathrm{Spec}(F_j) = \coprod_j \mathrm{Spec}(F_j) \times_F \mathbf{P}^0_F,$$

and the $\mathrm{Spec}(F)$-morphisms $i\colon Y \to X$ and $t\colon Y \to X$ as $i = \coprod_j j^i \times p_j$, $t = \coprod_j j^t \times p_j$, respectively.

Lemma 4.7 *Let X, Y be two quasi-projective varieties over $\mathrm{Spec}(K)$ and let i, t be two $\mathrm{Spec}(K)$-morphisms $Y \to X$, where K is an extension of F. Assume that Y is zero-dimensional. Then there is a unique scheme X/Y over $\mathrm{Spec}(K)$ along with a $\mathrm{Spec}(K)$-morphism $p\colon X \to X/Y$ such that*

(a) *the morphisms $p \circ i$ and $p \circ t$ are equal,*
(b) *for any $\mathrm{Spec}(K)$-morphism $h\colon X \to Z$ such that the morphisms $h \circ i$ and $h \circ t$ are equal there is a unique $\mathrm{Spec}(K)$-morphism $z\colon X/Y \to Z$ such that the morphisms $z \circ p$ and h are equal.*

Moreover the formation of X/Y commutes with base change.

Proof The uniqueness of X/Y and p, as well as the the fact that the formation of these objects commutes with base change follows from the universal property. The

https://doi.org/10.4153/CJM-2004-028-0 Published online by Cambridge University Press

variety Y is the co-product of spectrums of finite extensions of K, so in particular it is affine. Assume first that X is affine, too. Let $X = \mathrm{Spec}(A)$, $Y = \mathrm{Spec}(B)$ and let $i_0 \colon B \to A$, $t_0 \colon B \to A$ be the K algebra-homomorphisms corresponding to the morphisms i, t, respectively. Define X/Y as $\mathrm{Spec}(A/I)$, where I is the ideal generated by $i_0(x) - t_0(x)$ for all $x \in B$, and define p as the morphism corresponding to the factor map $A \to A/I$.

These objects clearly satisfy (a) of the claim. It is also clear that p induces an isomorphism between the complement of the images of i and t in X and $p \circ i = p \circ t$ in X/Y, respectively. So in order to check that (b) also holds, it will be sufficient to show that we can define z uniquely on an open neighborhood of the image of $p \circ i = p \circ t$. For any point $y \in Y$ there is an open affine sub-variety U in Z which contains the point $h \circ i(y) = h \circ t(y)$ and an open affine sub-variety V of X containing the image of $i(y)$ and $t(y)$ which maps into U via h. The map z clearly extends to the image of V in X/Y by the definition of the ideal I. If we do not assume that X is affine, then we can still choose an open affine sub-variety V of X containing the image of i and t, then glue V/Y and the complement of the image of i and t in X in order to get X/Y. ∎

Let us return to the proof of the proposition. Consider the scheme $C = X/Y$ associated by Lemma 4.7 to X, Y, i and t above. C is automatically flat, because it is defined over a field, and since it is dominated by a proper scheme, it is also proper. It is birational to X, so it is 1-dimensional. In order to check that it is reduced, has only ordinary double points and its geometric components are rational, we can assume that F is algebraically closed, when this is obvious from the construction. It is also clear that there is a Galois-equivariant isomorphism between G and $\Gamma(C)$, which implies that C is stable, because G is. ∎

Theorem 4.8 *Let F be a local field such that the absolute Galois group of its residue field has quotients isomorphic to S_5, $\mathrm{PSL}_3(\mathbb{F}_2)$ and $\mathrm{PSL}_3(\mathbb{F}_3)$. Then there is a non-singular, geometrically irreducible projective curve defined over F of genus g without solvable points when g is equal to* 6, 8, 10, 11, 15, 16, 20, 21, 22, 25, 26, 27, 28, 29, 30, 31, 32, 34, 35, 36, 37, 38 *or at least* 40.

Proof We will prove the slightly stronger statement that there is a non-singular, geometrically irreducible projective curve defined over F of genus g without solvable points over the perfection of F. Let g be one of the natural numbers in the claim. First we prove that there is a stable graph Γ of Euler characteristic equal to g such that either S_5, $\mathrm{PSL}_3(\mathbb{F}_2)$ or $\mathrm{PSL}_3(\mathbb{F}_3)$ acts on Γ without solvable orbits. It is clear that the graphs constructed in the proof of Proposition 3.4 satisfy these properties except that one of the three groups above acts on the graphs $S_{5,6}(x, y)$ without solvable orbits. The symmetric group S_5 acts on the set of its 5-Sylow subgroups transitively by conjugation. By the Sylow theorems the number of 5-Sylow subgroups divides the order of S_5, but it is also congruent to 1 modulo 5. Since the order of S_5 is 120, the only possibility is 6. Define the homomorphism $h \colon S_5 \to S_5 \times S_6$ as the direct product of the identity with the homomorphism defined by the action above. Clearly the action of S_5 on $S_{5,6}(x, y)$ defined via this homomorphism is without solvable orbits.

https://doi.org/10.4153/CJM-2004-028-0 Published online by Cambridge University Press

Let $\mathbf{f}$, R denote the residue field of F and its discrete valuation ring, respectively. By assumption there is an action of $\mathrm{Gal}(\bar{\mathbf{f}}|\mathbf{f})$ on Γ without solvable orbits. By Proposition 4.6 there is a stable curve C with rational components over $\mathbf{f}$ such that there is a Galois-equivariant isomorphism between Γ and $\Gamma(C)$. By Corollary 4.4 there is a stable curve $\pi\colon \mathcal{C} \to \mathrm{Spec}(R)$ such that the base change $\mathcal{C}_{\mathrm{Spec}(F)}$ is a smooth, geometrically irreducible projective curve and $\mathcal{C}_{\mathrm{Spec}(\mathbf{f})}$ is isomorphic to C. By flatness the genus of $\mathcal{C}_{\mathrm{Spec}(F)}$ is equal to the arithmetic genus of C, which is g. The curve C is without solvable points over the perfection $\mathbf{f}^p$. Now the claim of the theorem follows from the following lemma. ∎

Lemma 4.9 *Let R be discrete valuation ring with residue field $\mathbf{f}$ and quotient field F. Let X be a projective scheme over $\mathrm{Spec}(R)$. If the base change $X_{\mathrm{Spec}(\mathbf{f})}$ does not have solvable points over the perfection $\mathbf{f}^p$, then the base change $X_{\mathrm{Spec}(F)}$ does not have either.*

Proof Let L be any solvable extension of a purely inseparable extension of F and let S be the integral closure of R in L. S is a discrete valuation ring, so by the valuative criterion of properness any L-valued point of $X_{\mathrm{Spec}(F)}$ gives an S-valued point of X. This S-valued point reduces to a point in the special fiber of X with respect to the maximal ideal of S. This point is defined over the residue field of this ideal which is a solvable extension of a purely inseparable extension of $\mathbf{f}$. By assumption there is no such point, so $X_{\mathrm{Spec}(F)}$ has no solvable points over F^p. ∎

Remark 4.10 Some of the curves constructed above have a solvable divisor of degree 1. Consider a curve X which degenerates over $\mathbf{f}$ to a stable curve C with rational components whose graph $\Gamma(C)$ is isomorphic to the graph $S_{5,6}(x)$. C has two smooth points defined over a degree 5 and degree 6 extension of $\mathbf{f}$, respectively. By the Hensel lemma we can lift these points to two points of X defined over a degree 5 and degree 6 extension of F, respectively. Their difference is a divisor of degree 1 defined over F.

Theorem 4.11 *Let F be field which is finitely generated of transcendence degree at least one over an algebraically closed field $\mathbf{C}$ of uncountable cardinality. Then there are infinitely many natural numbers g such that there is a smooth, geometrically irreducible projective curve of genus g over F without solvable points.*

Proof First we remark that if there is a smooth, geometrically irreducible projective curve X over F without solvable points, then the stronger property in the claim above also holds for F. The genus of the curve X is not zero by Theorem 5.4 which we will prove later. As we saw in the proof of Theorem 2.3 there is a ramified separable cover of X by a smooth, geometrically irreducible projective curve. This curve is without solvable points and its genus is strictly larger than the genus of X by the Hurwitz formula. Repeating this argument infinitely many times we can conclude the proof of the remark.

Next we will show that if the generalized continuum hypothesis holds then for every S finite subset of $\mathbf{C}$ there is an isomorphism ι from the algebraic closure $\mathbf{D}$ of $\mathbf{C}((t))$ onto $\mathbf{C}$ such that $\iota(s) = s$ for all $s \in S$. The proof below is a slight variant of a standard argument, but we will include it for the sake of completeness. By assumption there is an uncountable cardinal κ such that there are two bijections $i\colon \kappa \to \mathbf{C}$

https://doi.org/10.4153/CJM-2004-028-0 Published online by Cambridge University Press

and $j\colon \kappa \to \mathbf{D}$. We will define by transfinite induction two sets of subfields $\mathbf{C}_\alpha \subset \mathbf{C}$ and $\mathbf{D}_\alpha \subset \mathbf{D}$ and an isomorphism $\iota_\alpha\colon \mathbf{D}_\alpha \to \mathbf{C}_\alpha$ of fields for all $\alpha \in \kappa$ such that

(a) $i(\alpha) \in \mathbf{C}_\alpha \subseteq \mathbf{C}_\beta$ and $j(\alpha) \in \mathbf{D}_\alpha \subseteq \mathbf{D}_\beta$ for any $\alpha \in \beta \in \kappa$,
(b) $\iota_\beta|_{\mathbf{D}_\alpha} = \iota_\alpha$ for any $\alpha \in \beta \in \kappa$,
(c) $S \subseteq \mathbf{C}_\varnothing$, $S \subseteq \mathbf{D}_\varnothing$, and the restriction of $\iota_\varnothing$ onto S is the identity,
(d) the cardinality of $\mathbf{C}_\alpha$ and $\mathbf{D}_\alpha$ are less than κ.

It is clear that $\mathbf{C} = \bigcup_{\alpha\in\kappa} \mathbf{C}_\alpha$, $\mathbf{D} = \bigcup_{\alpha\in\kappa} \mathbf{D}_\alpha$, and the limit ι of the isomorphisms ι_α has the required property. We start the proof of the claim above by the following remark: if K is a subfield of $\mathbf{C}$ whose cardinality is less then κ, there is an embedding $\epsilon\colon K \to \mathbf{D}$, and an element $x \in \mathbf{C}$, then ϵ extends to an embedding $\epsilon\colon K(x) \to \mathbf{D}$. The latter is clear if x is algebraic over K as $\mathbf{D}$ is algebraically closed. If x is transcendental over K then the same conclusion holds as the algebraic closure of $\epsilon(K)$ is a proper subset of $\mathbf{D}$ since its cardinality is less than κ, so there is an element of $\mathbf{D}$ transcendental over $\epsilon(K)$. Obviously the same holds if the roles of $\mathbf{C}$ and $\mathbf{D}$ are interchanged. Let $C_\varnothing \subset \mathbf{C}$ be the field generated by S and $i(\varnothing)$ over the prime field and let $\mathbf{D}_\varnothing \subset \mathbf{D}$ be the field generated by $C_\varnothing$ and $j(\varnothing)$ over the prime field. By the above the inclusion map $C_\varnothing \to \mathbf{C}$ extends to an embedding $\iota_\varnothing\colon \mathbf{D}_\varnothing \to \mathbf{D}$. Set $\mathbf{C}_\varnothing = \iota_\varnothing(\mathbf{D}_\varnothing)$. Clearly these choices satisfy (a), (c) and (d). In general, if $\mathbf{C}_\alpha$, $\mathbf{D}_\alpha$ and ι_α are already defined for all $\alpha \in \beta$, then define $\mathbf{C}_\beta$, $\mathbf{D}_\beta$ and ι_β as follows. Let $C_\beta \subset \mathbf{C}$ be the field generated by $\bigcup_{\alpha\in\beta} \mathbf{C}_\alpha$ and $i(\beta)$ over the prime field. Since κ is a cardinal, condition (d) implies that the cardinality of $\bigcup_{\alpha\in\beta} \mathbf{C}_\alpha$ is less than κ, so there is an embedding $\epsilon_\beta\colon C_\beta \to \mathbf{D}$ extending ι_α^{-1} for all $\alpha \in \beta$. Let $\mathbf{D}_\beta \subset \mathbf{D}$ be the field generated by $\epsilon_\beta(C_\beta)$ and $j(\beta)$ over the prime field. Again the cardinality of $\epsilon_\beta(C_\beta)$ is less than κ, so there is an embedding $\iota_\beta\colon \mathbf{D}_\beta \to \mathbf{C}$ extending ϵ_β^{-1}. If we set $\mathbf{C}_\beta = \iota_\beta(\mathbf{D}_\beta)$, then these choices satisfy the four conditions above.

Let F be generated by $x_1, x_2, \ldots, x_n$ over $\mathbf{C}$ subject to a finite set of polynomial relations whose set of coefficients will be denoted by S. Clearly S lies in $\mathbf{C} \subset \mathbf{C}((t))$ with respect to the embedding of $\mathbf{C}((t))$ in $\mathbf{C}$ via the isomorphism ι constructed above. Let $F'' \subset F'$ denote the function fields $\mathbf{C}(x_1, x_2, \ldots, x_n) \subset \mathbf{C}((t))(x_1, x_2, \ldots, x_n)$ which are subfields of $F = \mathbf{D}(x_1, x_2, \ldots, x_n)$. Note that F'' is canonically isomorphic to F. Since the Galois group of the algebraic extension $F|F'$ is a subgroup of the absolute Galois group of the field $\mathbf{C}((t))$ which is solvable, it will be sufficient to construct a smooth, geometrically irreducible projective curve X over F' without solvable points over $(F')^p$, since it will not have solvable points over F either.

By a theorem of Harbater (see [3, Corollary 1.3, p. 284]) every finite group G occurs as a Galois group over F''. Hence there is a $f(t) \in F''[t]$ separable monique polynomial of degree 5 whose Galois group is S_5. Let K be the splitting field of $f(t)$ and write $f(t) = \prod_{i=1}^5 (t - \alpha_i)$, where $\alpha_i \in K$ are the roots of $f(t)$. Define

$$q_0(x_0, x_1, x_2) = \prod_{i=1}^{5} (x_0 - \alpha_i x_1 + \alpha_i^2 x_2).$$

The polynomial q_0 is homogeneous of degree 5 and its coefficients are in F''. It is also clear that it defines a stable curve $Q_0 \in \mathbf{P}^2$ of degree 5 whose graph $\Gamma(Q_0)$ is isomorphic to $S_5(0)$ and $\mathrm{Gal}(\overline{F''}|F'')$ acts on this graph without solvable orbits.

https://doi.org/10.4153/CJM-2004-028-0 Published online by Cambridge University Press

Let q_1 be a homogeneous polynomial of degree 5 in $F''[x_0, x_1, x_2]$ whose zero scheme Q_1 is smooth. Such a polynomial exits by Bertini's theorem. Define

$$q(x_0, x_1, x_2) = (1-t)q_0(x_0, x_1, x_2) + tq_1(x_0, x_1, x_2) \in F''[t][x_0, x_1, x_2].$$

This polynomial defines a projective scheme Q over the spectrum of $F''[t]$ and by base change a curve Q_η over the fields $F''(t) \subset F'$. By Lemma 4.9 it is clear that Q_η has no solvable points over the perfection of $F''((t))$. The latter field contains $(F')^p$ as a subfield, so in order to conclude our proof we have to prove that Q_η is geometrically irreducible and smooth. Since the property of a finite type map being smooth is open, it is clear that Q_η is geometrically smooth. Since it is also a plane curve, Lefschetz's theorem on hyperplane sections also implies that Q_η is geometrically irreducible. ■

Example 4.12 The method of the proof of the theorem above can be easily modified to construct an explicit example of a non-singular geometrically connected curve of genus 6 without solvable points over $\mathbb{C}(x)$ from Q_η we must embed the field $\mathbb{C}((t))$ in $\mathbb{C}$. The image of t under this embedding can be any number transcendental over $\mathbb{Q}$, for example π. Since the coefficients of q_0 and q_1 are actually in $\mathbb{Q}(x)$, their image under the map induced by the embedding above are themselves. Therefore the zero scheme of the homogeneous polynomial $(1-\pi)q_0(x_0, x_1, x_2) + \pi q_1(x_0, x_1, x_2)$ is a non-singular geometrically connected curve of genus 6 without solvable points over $\mathbb{C}(x)$.

Theorem 4.13 *Let F be field which is finitely generated of transcendence degree at least two over an algebraically closed field. Then there are infinitely many natural numbers g such that there is a smooth, geometrically irreducible projective curve of genus g over the perfection F^p without solvable points.*

Proof It will be sufficient to construct just one smooth, irreducible projective curve over F^p without solvable points, as we already remarked at the start of the proof above. The field F is the function field of a smooth, geometrically irreducible projective curve C defined over a field $\mathbf{f}$ which is finitely generated of transcendence degree at least one over an algebraically closed field. We can also assume that C has a $\mathbf{f}$-valued point p by extending $\mathbf{f}$, if necessary, by Theorem 2.3. By the theorem of Harbater quoted above S_n occurs as a Galois group over $\mathbf{f}$. The group S_n, $n \geq 5$ acts on the graph $S_n(0)$ without solvable orbits, therefore by Propositions 3.4 and 4.6 there is a stable curve $\mathcal{C}$ over $\mathbf{f}$ without solvable points over $\mathbf{f}^p$. Let g be the arithmetic genus of $\mathcal{C}$. The curve $\mathcal{C}$ defines a $\mathbf{f}$-valued point $q \in (\mathfrak{H}_g)_{\mathrm{Spec}(\mathbf{f})}(\mathbf{f})$.

$(\mathfrak{H}_g)_{\mathrm{Spec}(\mathbf{f})}$ is a smooth variety, hence q has an open affine neighborhood U which has an étale map into an affine space $\mathbf{A}^n_{\mathbf{f}}$. The image of the closed sub-variety of tri-canonical singular curves is a proper constructible subset of $\mathbf{A}^n_{\mathbf{f}}$. Take a line through the image of q in $\mathbf{A}^n_{\mathbf{f}}$ which intersects the complement of this image. Let D' denote the component of the inverse image of this line in U which contains q. D' is smooth at q and it is geometrically irreducible, because it has a $\mathbf{f}$-valued point. The normalization D of D' is a smooth, geometrically irreducible curve defined over $\mathbf{f}$ with a $\mathbf{f}$-valued point r and a $\mathbf{f}$-morphism $d\colon D \to (\mathfrak{H}_g)_{\mathrm{Spec}(\mathbf{k})}$ such that $d(r)$ is q and the image of d intersects the open sub-variety of tri-canonical non-singular curves.

https://doi.org/10.4153/CJM-2004-028-0 Published online by Cambridge University Press

Applying the same argument to the variety $C \times D$ and the point $p \times r$, we get a smooth, geometrically irreducible curve E defined over $\mathbf{f}$ with a $\mathbf{f}$-valued point s and a $\mathbf{f}$-morphism $e\colon E \to C \times D$ such that $e(s) = p \times r$ and the compositions of e with the projections to the factors are non-trivial. The pull-back of the universal family over $\mathfrak{H}_g$ in respect to $e \circ d$ is a stable curve whose fiber $\mathcal{D}$ over the generic point of E is a smooth, geometrically irreducible curve and its fiber over s is isomorphic to C. The latter and Lemma 4.9 implies that the base change of $\mathcal{D}$ to the perfection K^p of the function field K of E is without solvable points over K^p. This implies by Theorem 2.3 that there is a smooth, geometrically irreducible projective curve X over F^p, because K^p is a finite extension of F. ∎

Theorem 4.14 *Let F be a finitely generated field. Assume moreover that its transcendence degree is at least two, if its characteristic is positive, and it is at least one, otherwise. Then there are infinitely many natural numbers g such that there is a smooth, geometrically irreducible projective curve of genus g over the perfection F^p without solvable points.*

Proof Define K as the composition of F and the algebraic closure of the prime field of F in some algebraic closure of F. This field is finitely generated of transcendence degree at least two over an algebraically closed field, unless F is the function field of a smooth, geometrically irreducible projective curve defined over a number field. In the former case the claim follows from Theorem 4.13 and Theorem 2.3. In the latter case the claim will follow using the same argument as above if we show that the absolute Galois group of every number field is not solvable. This follows from Hilbert's irreducibility theorem. ∎

5 Existence Results: Solvable Points

Proposition 5.1 *Let F be a field and let $c \in H^2(F, \mathbf{G}_m)$ be a cohomology class. Then there is a solvable extension L of F such that the image of c with respect to the natural restriction homomorphism $r_{L|F}\colon H^2(F, \mathbf{G}_m) \to H^2(L, \mathbf{G}_m)$ is zero.*

Proof First assume that F has zero characteristic. The Brauer group $H^2(F, \mathbf{G}_m)$ is torsion, so there is a natural number n such that c is of order n. By a cyclic extension, if necessary, we can assume that F contains the n-th roots of unity. Let $K_2(L)$ denote the Milnor K-group for any field L. There is a Chern character homomorphism $c_2\colon K_2(K)/nK_2(K) \to H^2(F, \mathbb{Z}/n\mathbb{Z})$ for any field containing the n-th roots of unity which is an isomorphism by the Merkurjev-Suslin theorem (see [9]). Also for every extension L of F there is a commutative diagram:

$$\begin{array}{ccc} K_2(F)/nK_2(F) & \xrightarrow{c_2} & H^2(F, \mathbb{Z}/n\mathbb{Z}) \\ \downarrow{\scriptstyle r_{L|F}} & & \downarrow{\scriptstyle r_{L|F}} \\ K_2(L)/nK_2(L) & \xrightarrow{c_2} & H^2(L, \mathbb{Z}/n\mathbb{Z}) \end{array}$$

where the vertical maps are the restriction maps and the horizontal maps are the Chern character homomorphisms.

https://doi.org/10.4153/CJM-2004-028-0 Published online by Cambridge University Press

By Hilbert's Theorem 90, the cohomology class c is the image of a class in $H^2(F, \mathbb{Z}/n\mathbb{Z})$ in the long cohomological exact sequence of the Kummer exact sequence, hence by the above it will be sufficient to prove that for every element $c \in K_2(F)/nK_2(F)$ there is an abelian extension L of F such that the image of c respect to the natural restriction homomorphism in $K_2(F)/nK_2(F)$ is zero. Write c as $\sum_{i=1}^{r} a_i \wedge b_i$ where $a_i, b_i \in F^*$. Let L be the field which we get by adjoining the n-th roots of $a_1, a_2, \ldots, a_r$. Then $c = n\sum_{i=1}^{r} a_i^{1/n} \wedge b_i \in nK_2(L)$ where $a_i^{1/n}$ is an n-th root of a_i in L for all i.

Now assume that F is a perfect field of positive characteristic. Clearly a cohomology class $c \in H^2(F, \mathbf{G}_m)$ satisfies the property in the claim if and only if a Brauer-Severi variety representing c has a solvable point. Let $\mathbf{W}(F)$ denote the ring of Witt vectors of F and let $\mathbf{Q}(F)$ denote its quotient field. It is a discrete valuation ring with residue field F. By Corollary 2.13 of [10, p. 148] the canonical homomorphism $H^2\big(\mathrm{Spec}(\mathbf{W}(F)), \mathbf{G}_m\big) \to H^2(F, \mathbf{G}_m)$ is an isomorphism. Represent the cohomology class $c \in H^2\big(\mathrm{Spec}(\mathbf{W}(F)), \mathbf{G}_m\big)$ by a Brauer-Severi scheme $\mathbf{B}$ over $\mathrm{Spec}(\mathbf{W}(F))$. The base change $\mathbf{B}_{\mathrm{Spec}(\mathbf{Q}(F))}$ has a solvable point, since the characteristic of $\mathbf{Q}(F)$ is zero. By Lemma 4.9 the special fiber of $\mathbf{B}$ must have a solvable point. But the Brauer-Severi variety $\mathbf{B}_{\mathrm{Spec}(F)}$ represents the cohomology class c. Assume finally that F is an arbitrary field of positive characteristic. Represent the cohomology class $c \in H^2(F, \mathbf{G}_m)$ by a division algebra A of rank d over F. By the above there is a solvable extension K of F^p such that $A \otimes_F K \cong M_d(K)$. In particular there is a set of elements $e_{ij} \in A \otimes_F K \cong M_d(K)$, $1 \leq i, j \leq d$ such that $e_{ij}e_{kl} = \delta_{jk}e_{il}$ for each $1 \leq i, j, k, l \leq d$, where δ_{jk} is the Kronecker-delta. K is the perfection a solvable extension L of F. The latter follows from the topological invariance of the étale fundamental group (see Theorem 3.23 of [10, pp. 30–31]) applied to the map $\mathrm{Spec}(F^p) \to \mathrm{Spec}(F)$. For a sufficiently high natural number m we have $(\mathrm{id}_A \otimes \mathrm{Fr}^m)e_{ij} \in A \otimes_F L$ (for all $1 \leq i$, $j \leq d$). The elements $(\mathrm{id}_A \otimes \mathrm{Fr}^m)e_{ij}$ also satisfy the identities above, so A splits over L. ∎

An immediate corollary to this theorem is the following:

Corollary 5.2 *A Brauer-Severi variety defined over an arbitrary field F has a solvable point over F.* ∎

Proposition 5.3 *Let X be a regular, geometrically irreducible projective variety defined over the field K. Then for every $c \in \underline{\mathrm{Pic}}(X)(K)$ there is a solvable extension L of K and divisor $D \in \mathrm{Div}(X)(L)$ defined over L whose linear equivalence class is the restriction $r_{L|K}(c)$.*

Proof We are going to give two proofs of the claim. The first one is purely cohomological: consider the exact sequence

$$0 \longrightarrow \mathrm{Pr}(X) \longrightarrow \mathrm{Div}(X) \longrightarrow \underline{\mathrm{Pic}}(X) \longrightarrow 0$$

of Galois modules, where the second map associates to each divisor its linear equivalence class. The co-boundary map in the cohomological exact sequence of this exact sequence gives a homomorphism $\delta\colon \underline{\mathrm{Pic}}(X)(K) \to H^1(K, \mathrm{Pr}(X))$. By exactness it

https://doi.org/10.4153/CJM-2004-028-0 Published online by Cambridge University Press

is sufficient to prove that the cohomology class $\delta\big(r_{L|K}(c)\big)$ is zero for some solvable extension L of K. The exact sequence of Galois modules

$$0 \longrightarrow \mathbf{G}_m \longrightarrow \mathrm{Rt}(X) \longrightarrow \mathrm{Pr}(X) \longrightarrow 0$$

induces a long cohomological exact sequence:

$$\cdots \longrightarrow H^1\big(L, \mathrm{Rt}(X)\big) \longrightarrow H^1\big(L, \mathrm{Pr}(X)\big) \xrightarrow{\delta} H^2(L, \mathbf{G}_m) \longrightarrow \cdots$$

for any extension L of K. Let $L(X)$ denote the function field of X over any extension L of K. Then we have the equality of cohomology groups $H^1(L, \mathrm{Rt}(X)) = H^1(\mathrm{Gal}(\overline{L}(X)|L(X)), \mathbf{G}_m)$. The latter group is trivial by Hilbert's Theorem 90, so the co-boundary map δ is injective. The claim now follows from Proposition 5.1.

We will only sketch the second proof. Take a line bundle l on X defined over F which is very ample over F. For large enough n the line bundle $c + n \cdot l$ is very ample over the algebraic closure of F. The functor from the category of extensions of F to the category of sets which assigns to every extension K of F the set of sections defined over K can be represented by a Brauer-Severi scheme over F. By Proposition 5.1 the latter has a solvable point over F, which is a divisor defined over a solvable extension L whose linear equivalence class is the restriction $r_{L|K}(c + n \cdot l)$. The difference of this divisor and n-th multiple of any divisor defined over F, whose linear equivalence class is l, has the properties required in the claim. ∎

Theorem 5.4 *Let F be any field and let X be a smooth, geometrically irreducible projective curve defined over F such that its genus is* 0, 2, 3 *or* 4. *Then X has a solvable point.*

Proof We can assume that F is infinite, otherwise the claim is obvious. If X has genus zero then it is a Brauer-Severi variety and hence has a solvable point. Note that a genus 0 curve has a rational point then it is a rational curve, and the set of rational points is infinite, so X has a Zariski-dense set of solvable points. Now assume that the genus g of X is at least 2. We first remark that there is a divisor defined over F on the curve X such that its class is the canonical divisor class. By applying the Riemann-Roch theorem to any such divisor we get that there is g-dimensional linear system of effective divisors on X defined over F whose linear equivalence class is the canonical divisor class. Now X is either hyper-elliptic and the image of X respect to the canonical linear system above is a curve of genus zero or the canonical linear system defines an embedding of X. If X is hyper-elliptic, then the canonical map is a separable twofold cover, because the genus of X is not zero. Its image has a Zariski-dense set of solvable points by the above, so there is a solvable point on the image of X which is not in the ramification locus of the cover by X. Any geometric point in the pre-image of this point is also defined over a solvable extension, hence we can assume that X is not hyper-elliptic.

If g is 3 then the degree of the canonical divisor class is 4. By Bertini's theorem there are smooth hyper-plane sections respect to the canonical embedding. The geometric points of these hyper-plane sections are defined over a separable extension of X, because every smooth map of co-dimension zero is étale. The Galois group of

https://doi.org/10.4153/CJM-2004-028-0 Published online by Cambridge University Press

the field of definition of the geometric points of such a divisor in the linear system defined over F is solvable since it is a subgroup of the symmetric group on four letters which is solvable. If the genus of X is 4, the canonical map gives an embedding into $\mathbf{P}^3$ by assumption. Over the algebraic closure $\mathbf{F}$ of F the curve X is the complete intersection of a unique non-singular quadric and a non-singular cubic hyper-surface in $\mathbf{P}^3$. We first prove that these surfaces are defined over F. Consider the restriction map of sections:

$$H^0(\mathbf{P}^3, H^d) \to H^0(X, K_X^d),$$

where d is a positive integer, H is the tautological bundle on $\mathbf{P}^3$, and K_X is the canonical class of X. The kernel of this map for $d = 2, 3$ is one-dimensional after tensoring with $\mathbf{F}$, so it is one-dimensional. Any non-zero section in these kernels will define the surfaces above over F. By the next theorem, after a solvable extension, if necessary, the quadric will have a rational point and hence it will be isomorphic to $\mathbf{P}^1 \times \mathbf{P}^1$ and the two pencils of lines will be defined over this field. The projection of X to either of these factors is a map of degree 3, so it is either purely inseparable or separable. The former case is impossible, since the genus of X is not zero, so the intersection of a generic line in the pencils above with the curve will be smooth, hence it will be a divisor of degree 3 whose geometric points are defined over a separable extension of F. ■

Theorem 5.5 *Let F be any field and let X be a smooth, geometrically rational projective surface defined over F. Then X has a solvable point.*

Proof We can assume, as usual that F is infinite. The minimal model theorem for surfaces says the following (see [7, Theorem 2.2, p. 169]):

Theorem 5.6 *Let X be a smooth proper surface over F. Then there is a sequence of contractions $X \to X_1 \to \cdots \to X_n = X'$ such that X' satisfies one of the following conditions:*

(a) *its canonical bundle $K_{X'}$ is nef,*
(b) *X' is a conic bundle over a curve C,*
(c) *$-K_{X'}$ is ample.*

It will be sufficient to prove that X' has an L-valued point for some solvable extension L, because the pre-image of any L-valued point respect to a contraction defined over F is either an L-valued point or a rational curve defined over L. If X is geometrically rational then (a) is impossible. If (b) holds then the curve C must have genus 0, hence it has a solvable point. If a genus 0 curve has a rational point then it is a rational curve, and the set of rational points is infinite. Hence we can assume that C has a solvable point whose pre-image in X' is a smooth curve of genus 0. This curve also has a solvable point over its field of definition, so X' has a solvable point over F.

Otherwise X' is a Del Pezzo surface. By Propositions 3.4 of [7, p. 173] and 3.9 of [7, p. 176]:

Theorem 5.7 *Let X' be a Del Pezzo surface over F. Then*

(a) *the linear system $|-mK_{X'}|$ is free if $m(K_{X'}^2) \geq 2$,*

https://doi.org/10.4153/CJM-2004-028-0 Published online by Cambridge University Press

(b) *over the algebraic closure $\bar{F}$ the surface X' is either isomorphic to $\mathbf{P}^2$, $\mathbf{P}^1 \times \mathbf{P}^1$ or it is obtained from $\mathbf{P}^2$ by blowing up $9 - (K_{X'}^2)$ points of $\mathbf{P}^2$.*

By the above the linear system $|-mK_{X'}|$ is free, so it defines a map into a projective space, and its image degree is at most 4, where $m = 2$, if $(K_{X'}^2) = 1$, and $m = 1$, if $2 \leq (K_{X'}^2) \leq 4$. If $(K_{X'}^2) \leq 4$, then X' is obtained from $\mathbf{P}^2$ by blowing up finitely many points over $\bar{F}$, because $(K_{\mathbf{P}^1 \times \mathbf{P}^1}^2) = 8$. Then the linear system of divisors obtained by pulling back the full linear system $|-mK_{\mathbf{P}^2}|$ and adding $-m$ times the sum of exceptional divisors is a subsystem of the linear system $|-mK_{X'}|$. The restriction of the former linear system to the complement of the exceptional divisors is very ample, so the linear system $|-mK_{X'}|$ is immersion on the same open sub-variety. By Bertini's theorem there is a line defined over F whose intersection with X' is smooth, which does not lie in the image of X' and does not intersect the image of the union of exceptional divisors, because the latter is at most one dimensional. This line gives a zero-dimensional cycle of degree 4 on X' whose geometric points are defined over a separable extension, and therefore a solvable point.

Lemma 5.8 *Let $\Lambda = \{(a_1, a_2, \ldots, a_d) \in \mathbb{Z}^d : 3|a_1 + a_2 + \cdots + a_d\}$, where $d \leq 4$. Define the quadratic form q on Λ by the formula*

$$q(a_1, a_2, \ldots, a_d) = \sum_{i=1}^{d} a_i^2 - \frac{1}{9}\Big(\sum_{i=1}^{d} a_i\Big)^2.$$

Then the automorphism group of the quadratic form q is a finite, solvable group.

Proof (See also [8, Theorem 23.9, p. 115]) For any $(a_1, a_2, \ldots, a_d) \in \Lambda$ we have the estimate:

$$q(a_1, a_2, \ldots, a_d) \geq \frac{9-d}{9} \sum_{i=1}^{d} a_i^2.$$

If $d = 1$, then the claim is obvious. If $d = 2$, then for any $(a_1, a_2) \in \Lambda$ such that $q(a_1, a_2) = 4$, we have $a_1^2 + a_2^2 \leq 5$. This implies that the set of such vectors consists of $\pm(1, 2)$ and $\pm(2, 1)$. These vectors span Λ, hence automorphism group of the quadratic form q acts on them faithfully, so it is an extension of $\mathbb{Z}/2\mathbb{Z}$ by itself. If $d \geq 3$, then for any $(a_1, a_2, \ldots, a_d) \in \Lambda$ such that $q(a_1, a_2) = 2$, we have $\sum_{i=1}^{d} a_i^2 \leq 3$. Therefore the set of such vectors consists of vectors $\mathbf{v}$ such that exactly three of the coordinates of $\mathbf{v}$ is nonzero, and each non-zero coordinate is either equal to 1 or -1. If $d = 4$ then these vectors span Λ, hence automorphism group of the quadratic form q acts on them faithfully. The automorphism group permutes the four pairs of the form $(\mathbf{v}, -\mathbf{v})$ in the set above, hence it is an extension of S_4 by $\mathbb{Z}/2\mathbb{Z}$. If $d = 3$, then they do not span Λ, because there are two of them, but vectors $\mathbf{v}$ with $q(\mathbf{v}) = 4$ do span Λ, since by the above this set consists of $\pm(2, 1, 0)$ and all other vectors which can be obtained by permuting the coordinates of these two vectors. The automorphism group permutes the pairs of triples of these vectors of the form $\pm(\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3)$ with $\mathbf{v}_1 + \mathbf{v}_2 + \mathbf{v}_3 = \pm(3, 3, 3)$, so it has a normal filtration with Jordan-Hölder components $\mathbb{Z}/2\mathbb{Z}$ and S_3. ∎

https://doi.org/10.4153/CJM-2004-028-0 Published online by Cambridge University Press

Assume now that $(K_{X'}^2) \geq 5$. Note that the Picard scheme of any geometrically rational surface X' is geometrically reduced, as its tangent space, being isomorphic to $H^1(X', \mathcal{O}_{X'})$, is equal to zero. Hence every line bundle of X' defined over the algebraic closure of F is defined actually over $\bar{F}$. We claim that the absolute Galois group acts on $\mathrm{Pic}(X')(\bar{F})$ through a solvable quotient. If the surface X' is isomorphic to $\mathbf{P}^1 \times \mathbf{P}^1$ over the algebraic closure $\bar{F}$, then $\mathrm{Pic}(X')(\bar{F}) \cong \mathbb{Z}^2$. $\mathrm{Gal}(\bar{F}|F)$ fixes the non-trivial class $K_{X'}$, so it is of order at most two. Otherwise $\mathrm{Pic}(X')(\bar{F}) \cong \mathbb{Z}^{1+d}$, where $d \leq 4$. The group is generated by H, the pull-back of the tautological class on $\mathbf{P}^2$, and the classes of the exceptional divisors $E_1, \ldots, E_d$. The canonical divisor class is $-3H + E_1 + \cdots + E_d$ which is fixed by $\mathrm{Gal}(\bar{F}|F)$, so its orthogonal complement is left invariant by $\mathrm{Gal}(\bar{F}|F)$. This complement equipped with the restriction of the intersection pairing is isomorphic to Λ equipped with q, so its automorphism group is solvable by the lemma above. Any Galois conjugation acts trivially on $\mathrm{Pic}(X')(\bar{F})$, if it fixes this complement. So $\mathrm{Gal}(\bar{F}|F)$ acts on $\mathrm{Pic}(X')(\bar{F})$ through a solvable quotient, as claimed. Hence by Proposition 5.1 the full linear system $|H|$ is defined over a solvable extension of F. This linear system gives a birational morphism from X' onto $\mathbf{P}^2$, therefore X' has a solvable point. ∎

6 Existence Results: Solvable Divisors

Lemma 6.1 *Let R be discrete valuation ring with a perfect residue field* **f** *and quotient field F. Let X be a stable curve over* $\mathrm{Spec}(R)$. *If the base change $X_{\mathrm{Spec}(\mathbf{f})}$ does not have solvable divisors of degree d over* **f**, *then the base change $X_{\mathrm{Spec}(F)}$ does not have either.*

Proof We can assume in any case that d is positive. $\mathrm{Hilb}_d(X)$, the Hilbert scheme representing the functor which assigns to each scheme S the set of rank d, finite, flat sub-schemes of the scheme X_S is projective. The claim follows from Lemma 4.9 applied to $\mathrm{Hilb}_d(X)$. ∎

Lemma 6.2 *Let F be an arbitrary field and let n be a positive integer. The following two claims are equivalent:*

(i) *Every smooth, geometrically irreducible projective curve X of genus 1 over F has a solvable divisor over F whose degree is relatively prime to n.*
(ii) *For every elliptic curve E over F and cohomology class $c \in H^1(F, E)[n]$ there is a solvable extension $K|F$ such that the cohomology class $r_{K|F}(c) \in H^1(K, E)[n]$ is zero.*

Proof First we are going to show that (ii) implies (i). There is an exact sequence

$$0 \longrightarrow \underline{\mathrm{Pic}}_0(X) \longrightarrow \underline{\mathrm{Pic}}(X) \xrightarrow{\deg} \mathbb{Z} \longrightarrow 0$$

of Galois modules over any extension K of F, where $\deg(L)$ for any line bundle L is equal to its degree. The co-boundary map in the cohomological exact sequence of this exact sequence gives a homomorphism $\delta\colon \mathbb{Z} \to H^1\big(K, \underline{\mathrm{Pic}}_0(X)\big)$. Let $o_{X|K}$ denote the cohomology class $\delta(1)$. Clearly X has a class $c \in \underline{\mathrm{Pic}}(X)(K)$ of degree d if and only if $do_{X|K} = 0$. Therefore $o_{X|F}$ is torsion, so there is a positive integer m

https://doi.org/10.4153/CJM-2004-028-0 Published online by Cambridge University Press

relatively prime to n such that $mo_{X|F}$ is n-torsion. The class $o_{X|K}$ is natural, in other words $r_{K|F}(o_{X|F}) = o_{X|K}$ for every extension K of F. Hence by Proposition 5.3 it is sufficient to prove that there is a solvable extension $K|F$ such that the cohomology class $mo_{K|F} \in H^1\big(K, \underline{\mathrm{Pic}}_0(X)\big)[n]$ is zero which follows from ii applied to the elliptic curve representing $\underline{\mathrm{Pic}}_0(X)$. Next we are going to show that (i) implies (ii). By the general theory of torsors over algebraic groups there is a smooth, geometrically irreducible projective curve X of genus 1 over F whose Jacobian is E and whose cohomological invariant is the class c. Since it is n-torsion the class c is represented by a divisor of degree dividing n on X defined over a solvable extension by 5.3. By (i) there is a solvable divisor on X over F whose degree is relatively prime to n, too. A suitable linear combination of these divisors is a solvable divisor of degree 1. By the Riemann-Roch theorem this divisor has a non-zero section, so the curve X has a rational point over a solvable extension K of F hence it is isomorphic to E over the field K. Therefore the cohomological invariant of its base change to $\mathrm{Spec}(K)$ is zero, but this is $r_{K|F}(c)$ by naturality. ■

Theorem 6.3 *Let F be a perfect field of positive characteristic p or a local field of characteristic zero with a residue field of characteristic p. Let X be a smooth, geometrically irreducible projective curve of genus 1 defined over F. Then there is a solvable divisor on X whose degree is relatively prime to $6p$.*

Proof First assume that F is a perfect field of characteristic p. By Lemma 6.2 we only have to show that for every elliptic curve E over F and cohomology class $c \in H^1(F, E)[6p]$ there is a solvable extension $K|F$ such that the cohomology class $r_{K|F}(c) \in H^1(K, E)[6p]$ is zero. Let X be a genus 1 over F which is a torsor over E with cohomological invariant c. Let D be a divisor of degree d dividing $6p$ on X representing c. Then there is a map $X \to E$ of degree d which assigns the class of $dP - D$ to each geometric point P of X. Over the algebraic closure of F the curve X is isomorphic to E and the map above is the composition of a translation and multiplication by d. Therefore S_{red}, the reduction of the preimage S of the zero element of E under this map is a torsor over the smooth algebraic group $E[d]^{\mathrm{et}}$, the étale part of the finite flat group scheme $E[d]$. Let $e \in H^1(F, E[d]^{\mathrm{et}})$ be the corresponding cohomology class. On the other hand $E[d]^{\mathrm{et}}(\overline{F}) \leq E[6p]^{et}(\overline{F}) = \mathbb{F}_2^2 \oplus \mathbb{F}_3^2 \oplus \mathbb{F}_p^i$, where $i = 0$ or 1, when E is supersingular or ordinary, respectively. Since the automorphism group of the group above is solvable, we may assume that the group scheme $E[6p]^{\mathrm{et}}$ is constant. In this case the Kummer and Artin-Schreier theories imply that the restriction of the cohomology class e, hence the torsor S_{red} becomes trivial after a solvable extension. We may conclude that there is a solvable extension $K|F$ such that all geometric points of S_{red} are defined over K, therefore the geometric points of S are defined over a purely inseparable extension of K. Since it is a Galois extension of a perfect field, K is also perfect, so the geometric points of S are actually defined over K by the above. Hence X has a K-valued point, so $r_{K|F}(c) \in H^1(K, E)[6p]$ is zero.

Lemma 6.4 *Let F be a local field of characteristic 0 with a residue field of characteristic p. Let $L|F$ be a finite Galois extension. Then there is a solvable extension K of F such that the extension $KL|K$ is unramified, where KL is the composition of K and L.*

Proof During the proof we will always adjoin sufficiently many roots of unity to F

https://doi.org/10.4153/CJM-2004-028-0 Published online by Cambridge University Press

so all Kummer extensions encountered will become cyclic extensions without extra notice. First assume that $L|F$ is tamely ramified. Let T be the largest unramified subextension of F in the field L. Since the tame inertia group is isomorphic to $\oplus_{l\neq p}\mathbb{Z}_l$, the Galois group $\mathrm{Gal}(L|T)$ is cyclic of order m, where m is relatively prime to p. By Kummer theory the extension $L|T$ is the spitting field of a polynomial $x^m - u\pi^k$, where π is a uniformizer of F and u is a unit in the discrete valuation ring of the extension T. Over the splitting field K of $x^m - \pi^k$ the composition field LK is unramified. Now let $L|F$ be any finite Galois extension, and let T denote the largest tamely ramified subextension of F in the field L. By the above we can actually assume that $T|F$ is unramified by taking a tamely ramified cyclic extension, if necessary. In this case we will prove the existence of K by induction on the order of $\mathrm{Gal}(L|T)$. The Galois group of the extension $L|T$ is wildly ramified, so it is a p-group. Hence there is a $w \in L - T$ whose minimal polynomial is of the form $x^p - u\pi^k$, where π is again a uniformizer of F, and u is a unit in the discrete valuation ring of the extension T. Let $q(t) \in R[t]$ be a polynomial, where R is the discrete valuation ring of F such that its reduction modulo the maximal ideal is the minimal polynomial of the reduction of u. After a sequence of cyclic of extensions, if necessary, we can assume that all coefficients of $q(t)$ has a p-th root in F. If $r(t)$ is a polynomial whose k-th coefficient is a p-th root of the k-th coefficient of $q(t)$, then the splitting field U of $r(t)$ is unramified over F. It has a root v such that u/v^p is congruent to 1 modulo the maximal ideal. Since the extension $TU|F$ is unramified this implies that u/v^p is in F. Therefore the composition K of the splitting fields of $x^p - \pi^k$ and $x^p - u/v^p$ is a solvable extension of F such that $T(w)K|K$ is unramified. Since the order of $\mathrm{Gal}(LK|T(w)K)$ is strictly less then the order of $\mathrm{Gal}(L|T)$, the induction hypothesis can be applied. ■

Now assume that F is a local field of characteristic 0 with a perfect residue field $\mathbf{f}$ of characteristic p. Let E denote the elliptic curve $\underline{\mathrm{Pic}}_0(X)$. It is sufficient to prove that for any cohomology class $c \in H^1(F, E)[l]$, where $l = 2, 3$ or p, there is a solvable extension L of F such that $r_{L|F}(c) \in H^1(L, E)[l]$ is zero. Let R denote the discrete valuation ring of F. The cohomology class c is the image of a class $d \in H^1(F, E[l])$ by the Kummer exact sequence. We may assume that the action of the absolute Galois group on $E[l]$ is unramified and the class d is represented by a cocycle defined over an unramified extension of F, using Lemma 6.4. In this case the cohomology class $c \in H^1(F, E)[l]$ is the inflation of a cohomology class in $H^1(\mathrm{Spec}(R), \mathcal{E})[l]$, where $\mathcal{E}$ is the Néron model of E over R. By Remark 3.11 (a) of [10, p. 116] the canonical homomorphism $H^1(\mathrm{Spec}(R), \mathcal{E}) \to H^1(\mathbf{f}, \mathcal{E}_0)$ is an isomorphism, where $\mathcal{E}_0$ is the fiber of the Néron model over $\mathrm{Spec}(\mathbf{f})$. The latter is either an elliptic curve or the extension of a finite abelian étale group scheme by $\mathbf{G}_m$ or $\mathbf{G}_a$. In the latter case the group of geometric points of this étale group scheme is either cyclic or has order at most 4, so its automorphism group is solvable. Therefore in each case for every cohomology class $c \in H^1(\mathbf{f}, \mathcal{E}_0)[l]$ there is a solvable extension $\mathbf{k}$ of $\mathbf{f}$ such that $r_{\mathbf{k}|\mathbf{f}}(c) \in H^1(\mathbf{k}, \mathcal{E}_0)[l]$ is zero. This extension gives a solvable unramified extension of F such that the image of c under the isomorphism above is zero.

Consider finally the case of a local field F of characteristic 0 with a not necessarily perfect residue field $\mathbf{f}$ of characteristic p. We may use the same arguments as above to reduce the claim to the following: if $\mathcal{E}_0$ is the fiber of the Néron model over $\mathrm{Spec}(\mathbf{f})$

https://doi.org/10.4153/CJM-2004-028-0 Published online by Cambridge University Press

of an elliptic curve defined over F and $c \in H^1(\mathbf{f}, \mathcal{E}_0)[l]$ is a cohomology class, then there is a solvable extension K with residue field $\mathbf{k}$ such that $r_{\mathbf{k}|\mathbf{f}}(c) \in H^1(\mathbf{k}, \mathcal{E}_0)[l]$ is zero. We have already shown that there is a solvable extension $\mathbf{l}$ of the perfection of $\mathbf{f}$ such that $r_{\mathbf{l}|\mathbf{f}}(c) \in H^1(\mathbf{l}, \mathcal{E}_0)[l]$ is zero. Take a zero-dimensional cocycle defined over $\mathbf{l}$ whose coboundary is $r_{\mathbf{l}|\mathbf{f}}(c)$. Since this cocycle is actually defined over a finite extension of $\mathbf{f}$, there is a finite extension $\mathbf{k}$ of $\mathbf{f}$ which is a solvable extension of a purely inseparable extension of $\mathbf{f}$ such that $r_{\mathbf{k}|\mathbf{f}}(c) \in H^1(\mathbf{k}, \mathcal{E}_0)[l]$ is zero. The field $\mathbf{k}$ is the chain of extensions $\mathbf{f} = \mathbf{k}_0 \leq \mathbf{k}_1 \leq \mathbf{k}_2 \leq \cdots \leq \mathbf{k}_n = \mathbf{k}$ such that $\mathbf{k}_j = \mathbf{k}_{j-1}(a_j^{1/n(j)})$ for all $j = 1, 2, \ldots, n$, where $a_j \in \mathbf{k}_{j-1}$ and $n(j) \in \mathbb{N}$. We define by induction a chain of extensions $F = K_0 \leq K_1 \leq K_2 \leq \cdots \leq K_n = K$ such that $K|F$ is solvable and the residue field of K_j is $\mathbf{k}_j$ as follows. If K_{j-1} is already defined, the we set $K_j = K_{j-1}(b_j^{1/n(j)})$, where b_j is an element of the discrete valuation ring of K_{j-1} such that the reduction of b_j modulo the maximal ideal of the valuation ring is equal to a_j. ■

Remark 6.5 If a smooth, geometrically irreducible curve of genus 1 has a solvable divisor of degree 1, then by the Riemann-Roch theorem applied to this divisor there is a solvable point on this curve. Therefore Theorem 6.3 can be considered as a partial result towards the problem of constructing solvable points on algebraic curves.

Theorem 6.6 *Let F be a local field of characteristic zero with a residue field of characteristic p where $p = 5$ or $p = 7$. Assume that the absolute Galois group of the residue field of F has a quotient isomorphic to S_5, if $p = 5$, and has a quotient isomorphic to* $\mathrm{PSL}_3(\mathbb{F}_2)$, *if $p = 7$. Then there is a smooth, geometrically irreducible projective curve of genus g without a solvable divisor whose degree is relatively prime to p if and only if p divides $g - 1$ and g is at least* 2.

Proof If p does not divide $g - 1$ and g is at least 2, then any divisor of any smooth, geometrically irreducible projective curve X of genus g defined over F whose class is the canonical divisor class, is a divisor whose degree is relatively prime to p. If the genus of X is 0 or 1 then there is a solvable divisor on X whose degree is relatively prime to p by Corollary 5.2 and Theorem 6.3, respectively. Assume that p divides $g - 1$ and g is at least 2. Let R be the discrete valuation ring of F, a let $\mathbf{f}$ denote its residue field. Fix a quotient G of $\mathrm{Gal}(\tilde{\mathbf{f}}|\mathbf{f})$ which is isomorphic to S_5, if $p = 5$, and it is isomorphic to $\mathrm{PSL}_3(\mathbb{F}_2)$, if $p = 7$. By Corollary 4.4 and Proposition 4.6 there is a stable curve $\pi\colon \mathcal{C} \to \mathrm{Spec}(R)$ such that the base change $\mathcal{C}_{\mathrm{Spec}(F)}$ is a smooth, geometrically irreducible projective curve of genus g and $\mathcal{C}_{\mathrm{Spec}(\mathbf{f})}$ is a stable curve with rational components such that $\Gamma(\mathcal{C}_{\mathrm{Spec}(\mathbf{f})})$ is isomorphic to $S_5(\frac{g-6}{5})$ with the action of G described in Proposition 3.4, if $p = 5$, and it is isomorphic to $P_2(\frac{g-8}{7})$ with the action of G described in Proposition 3.4, if $p = 7$. The curve $\mathcal{C}_{\mathrm{Spec}(\mathbf{f}^p)}$ does not have solvable divisors of degree relatively prime to p, hence $\mathcal{C}_{\mathrm{Spec}(F)}$ does not have either by Lemma 6.1. ■

Proposition 6.7

(i) *If E is an elliptic curve defined over a field F of characteristic* 0, *the absolute Galois group of F acts on $E[p]$ through a non-solvable quotient for some prime p, and*

https://doi.org/10.4153/CJM-2004-028-0 Published online by Cambridge University Press

$c \in H^1(F, E[p])$ is a non-zero cohomology class, then for every solvable extension $K|F$ the cohomology class $r_{K|F}(c) \in H^1(K, E[p])$ is non-zero, too.

(ii) *There is a local field F of characteristic zero with a residue field of characteristic 5, an elliptic curve E defined over F and a non-zero cohomology class $c \in H^1(F, E[5])$.*

Proof We will first prove (i). Let $L = F(E[p])$ be the field of definition of the geometric points of the p-torsion of E and let G denote the image of the absolute Galois group of F on $\mathrm{GL}(E[p])$. By Lemma 6.8 below we know that $H^q(G, \mathbb{F}_p^2) = 0$ for all $q \in \mathbb{N}$, so we get $H^1(F, E[p]) = H^1(L, E[p])^G$ by looking at the Hochschild-Serre spectral sequence $H^p(G, H^q(L, E[p])) \Rightarrow H^{p+q}(F, E[p])$. Therefore the cohomology class $c \in H^1(F, E[p])$ corresponds to an extension $Q|F$ with Galois group isomorphic to the semidirect product $\mathbb{F}_p^2 \ltimes G$, where the action of G on $\mathbb{F}_p^2$ via conjugation is given by identifying the latter with $E[p]$. If K is a solvable extension of F such that $r_{K|F}(c)$ is zero, then the composition fields KQ and KL are equal. As the action of Galois on $E[p]$ does not trivialize over K the Galois group $\mathrm{Gal}(KL|K)$ is non-trivial and it is isomorphic to a normal subgroup H of G via the natural embedding $\mathrm{Gal}(KL|K) \to \mathrm{Gal}(K|F)$. Since the extension $KQ|KL$ is trivial, the action of H on $\mathbb{F}_p^2$ is also trivial, which is a contradiction.

Now we prove part (ii). We may assume that the field F has an unramified modular Galois representation $\rho\colon \mathrm{Gal}(\bar{F}|F) \to \mathrm{GL}_2(\mathbb{F}_5)$ with surjective image. If F is the quotient field of the Witt vectors of the perfection of a finitely generated field of transcendence degree one over an algebraically closed field, then there is such an Galois representation by Harbater's theorem quoted above. The affine curve X_ρ, the twist of the modular curve $X(5)$ corresponding to ρ has genus zero. Therefore its completion has a solvable point, so a Zariski-dense set of solvable points. Because X_ρ parameterize isomorphism classes of pairs (E, ϕ) where E is an elliptic curve and ϕ is an isomorphism between the Galois modules $E[5]$ and ρ, there are elliptic curves over a solvable extension K of F such that the absolute Galois group of K acts on their 5-torsion through a non-solvable quotient. As we saw above non-zero cohomology classes $c \in H^1(K, E[p])$ correspond to extensions $L|K$ with Galois groups isomorphic to $\mathbb{F}_p^2 \ltimes G$, where G is the image of the absolute Galois group of K on $\mathrm{GL}(E[p])$ and it acts on $\mathbb{F}_p^2$ via identifying the latter with $E[p]$. By Harbater's theorem there are such extensions of the residue field which remain non-trivial after solvable extensions by the argument above. ∎

Lemma 6.8 *Let G be a subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$. Then G is either solvable or $H^i(G, \mathbb{F}_p^2) = 0$ for all $i \in \mathbb{N}$, where G acts on $\mathbb{F}_p^2$ as a subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$.*

Proof The claim of this lemma might be deduced from the classification of subgroups of $\mathrm{GL}_2(\mathbb{F}_p)$, but we prefer to give a short, simple direct proof instead. Let $H = G \cap \mathrm{SL}_2(\mathbb{F}_p)$. It is clear that G is solvable if H is. If $H^0(G, \mathbb{F}_p) \neq 0$, then G is a subgroup of a Borel subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$, so it is solvable. If p does not divide the order of G, then $H^i(G, \mathbb{F}_p^2) = 0$ for all positive i as the exponent of the latter group divides both p and $|G|$. Therefore we may assume that p divides $|G|$, hence $|H|$, as the index of H in G divides $p - 1$. In this case any p-Sylow subgroup of H is cyclic of order p, and it is also a p-Sylow of $\mathrm{SL}_2(\mathbb{F}_p)$. By the Sylow theorem the number of

https://doi.org/10.4153/CJM-2004-028-0 Published online by Cambridge University Press

p-Sylows of H is congruent to 1 modulo p, so H either contains exactly one p-Sylow subgroup, or it contains all p-Sylows of $\mathrm{SL}_2(\mathbb{F}_p)$, since the latter has $p+1$ copies of p-Sylow subgroups. In the former case H is contained in a Borel subgroup of $\mathrm{SL}_2(\mathbb{F}_p)$, the normalizer of some p-Sylow of $\mathrm{SL}_2(\mathbb{F}_p)$, so it is solvable. In the latter case H contains a normal subgroup of $\mathrm{SL}_2(\mathbb{F}_p)$, the subgroup generated by the conjugate p-Sylows. If p is less than 5, then $\mathrm{SL}_2(\mathbb{F}_p)$ is solvable, so all of its subgroups are solvable, too. If p is at least 5, then the only proper normal subgroup of $\mathrm{SL}_2(\mathbb{F}_p)$ is its center $Z = Z(\mathrm{SL}_2(\mathbb{F}_p))$ which has order two. Therefore G must contain Z. In this case consider the Hochschild-Serre spectral sequence $H^p(G/Z, H^q(Z, \mathbb{F}_p^2)) \Rightarrow H^{p+q}(G, \mathbb{F}_p^2)$. Clearly $H^q(Z, \mathbb{F}_p^2) = 0$ for all $q \in \mathbb{N}$, so all entries of the spectral sequence are zero and therefore $H^i(G, \mathbb{F}_p^2) = 0$ for all $i \in \mathbb{N}$, too. ∎

The previous proposition may interpreted as follows: we cannot prove the existence of a solvable divisor whose degree is relatively prime to 5 for the unique genus 1 curve X whose Jacobian is the elliptic curve E in part (ii) and whose obstruction class $o_{X|F}$ is the image of c above in $H^1(F, E)[5]$ by examining the cohomology group $H^1(F, E[5])$ only, although we know that there is a solvable point on X by Theorem 6.3. Let us analyze further the phenomenon described in the proof of Proposition 6.7. Let E be an elliptic curve defined over the field F such that the absolute Galois group acts on its 5-torsion through a non-solvable quotient. If the j-invariant of the elliptic curve E has negative valuation then it has a Tate uniformization $\theta\colon \bar{F}^*/q^{\mathbb{Z}} \to E(\bar{F})$ which is $\mathrm{Gal}(\bar{F}|K)$-invariant for a quadratic extension K of F. In this case the p^n-th roots of unity form a $\mathrm{Gal}(\bar{F}|K)$-submodule in $E[p^n]$, therefore the absolute Galois group acts on the latter through a solvable quotient, a contradiction.

Hence the j-invariant of the elliptic curve E has non-negative valuation. Consider the Legendre family $y^2 = x(x-1)(x-\lambda)$ of elliptic curves over the scheme $\mathrm{Spec}(R[\lambda, \frac{1}{\lambda(\lambda-1)}])$. The j-invariant map $j\colon \mathrm{Spec}(R[\lambda, \frac{1}{\lambda(\lambda-1)}]) \to \mathbf{A}^1_R$ is an étale, Galois cover with Galois group S_3. The j-invariant of E gives an R-valued point of $\mathbf{A}^1_R$. The pre-image of this point in $\mathrm{Spec}(R[\lambda, \frac{1}{\lambda(\lambda-1)}])$ is the spectrum of a discrete valuation ring S which is étale over $\mathrm{Spec}(R)$ with Galois group S_3. By the above there is an elliptic curve E' with good reduction over the quotient field of S, denoted by F by abuse of notation, whose j invariant is equal to the j-invariant of E. Therefore E' is the twist of E respect to a cohomology class $c \in H^1(F, \mathrm{Aut}(E))$. But the automorphism group of elliptic curve E has order 2, 4, 6 or 12, hence the absolute Galois group acts on it through an abelian quotient. So there is an abelian extension K of F such that $r_{K|F}(c)$ is trivial, so E' isomorphic to E over K. Because the base change of the elliptic curve E' still has good reduction, there is a solvable extension of F, denoted by F by abuse of notation such that E has good reduction. Over this extension the absolute Galois group still acts on $E[5]$ through a non-solvable quotient.

Let E_n denote the Galois module over F which assigns to every finite extension K of F the kernel of the reduction modulo the n-th power of the maximal ideal of the discrete valuation ring of K. Let K be an unramified Galois extension of F such that the geometric points of $E[5]$ are defined over K. The Galois module $E[5]$ is absolutely irreducible, so any reduction map is either injective or trivial. Therefore $E[5]$ is contained in E_1, so E has supersingular reduction. Also there is a natural number n such

https://doi.org/10.4153/CJM-2004-028-0 Published online by Cambridge University Press

that $E[5]$ is contained in $E_n(K)$, but $E[5]$ injects into $E_n(K)/E_{n+1}(K)$. For any unramified Galois extension K of F the quotients $E_n(K)/E_{n+1}(K)$ are isomorphic to $\mathbf{G}_a(\mathbf{k})$ as a $\mathrm{Gal}(K|F)$-module, where $\mathbf{k}$ is the residue field of K. Therefore our result gives a new way to construct additive polynomials whose Galois group is a prescribed Galois group after a solvable extension. On the other hand the implicit function theorem implies that E_n is isomorphic to A_1, where A_1 is the functor which assigns to each finite extension K the additive group of those elements of K whose valuation is positive for some $n \in \mathbb{N}$. Since $H^1(F, A_1) = 0$, we get an alternative proof of Theorem 6.3.

Acknowledgments I wish to thank Henri Darmon for his help and encouragement. I also wish to thank the CICMA for its warm hospitality and the pleasant environment it created for productive research.

References

[1] C. W. Curtis and I. Reiner, *Methods of representation theory, vol I*. John Wiley & Sons, Inc., New York, 1981.
[2] P. Deligne and D. Mumford, *The irreducibility of the space of curves of given genus*. Publ. Math. IHES **36**(1969), 75–109.
[3] D. Harbater, *Mock covers and Galois extensions*. J. Algebra **91**(1984), 281–293.
[4] R. Hartshorne, *Algebraic geometry*. Springer-Verlag, New York, Berlin, 1977.
[5] J.-P. Jouanolou, *Théorèmes de Bertini et applications*. Birkhäuser, Boston, Basel, Stuttgart, 1983.
[6] N. Katz and B. Mazur, *Arithmetic moduli of elliptic curves*. Princeton University Press, Princeton, 1985.
[7] J. Kollár, *Rational curves on algebraic varieties*. Springer-Verlag, New York, Berlin, 1996.
[8] Yu. I. Manin, *Cubic forms: algebra, geometry, arithmetic*. North-Holland Publishing Company, Amsterdam, 1974.
[9] A. S. Merkurjev and A. S. Suslin, *K-cohomology of Severi-Brauer varieties and the norm residue homomorphism*. Izv. Akad. Nauk SSSR Ser. Mat. **46**(1982), 1011–1046.
[10] J. Milne, *Étale cohomology*. Princeton University Press, Princeton, New Jersey, 1980.
[11] J.-P. Serre, *Corps locaux*. Hermann, Paris, 1962.
[12] J. Silverman, *Advanced topics in the arithmetic of elliptic curves*. Springer-Verlag, New York, Berlin, 1994.
[13] A. Weil, *Adéles and algebraic groups*. Birkhäuser, Boston, Basel, Stuttgart, 1982.

Centre de recherches mathématiques
Université e Montréal
C.P. 6128, Succ. Centre-ville
Montréal, Quebec
H3C3J7
email: pal@math.mcgill.ca