VARIETIES WITHOUT EXTRA AUTOMORPHISMS I: CURVES

BJORN POONEN

Abstract. For any field k and integer $g \geq 3$, we exhibit a curve X over k of genus g such that X has no non-trivial automorphisms over $\overline{k}$.

1. Statement of the result

Let k be a field, and let p be its characteristic, which may be zero. All our curves are smooth, projective, and geometrically integral over k. If X is a curve over k, let $\operatorname{Aut} X$ denote the group of automorphisms of X over $\overline{k}$.

Hurwitz stated that for any $g \geq 3$, there exists a curve of genus g over $\mathbf{C}$ such that $\operatorname{Aut} X = \{1\}$, and a rigorous proof was provided by Baily [Ba]. The result was generalized to algebraically closed fields of arbitrary characteristic by Monsky [Mo]. The literature also contains some explicit constructions of curves with $\operatorname{Aut} X = \{1\}$. Accola at the end of [Ac] observes that there exist triple branched covers X of $\mathbf{P}^1_{\mathbf{C}}$ of genus $g \geq 5$ with $\operatorname{Aut} X = \{1\}$. Mednyh [Me] constructs some other examples analytically, as quotients of the complex unit disk. Turbek [Tu] constructs explicit families of examples of X with $\operatorname{Aut} X = \{1\}$, over algebraically closed fields k of characteristic $p \neq 2$, and $g = (m-1)(n-1)/2$ for some integers m, n with $(m, n) = 1$, $n > m + 1 > 3$, and p not dividing $(m-1)mn$. He uses gap sequences at Weierstrass points to control automorphisms.

Fix $g \geq 3$, and let $\mathcal{M}_{g,3K}$ over $\mathbf{Z}$ denote the moduli space of curves equipped with a basis of the global sections of the third tensor power of the canonical bundle. Katz and Sarnak [KS, Lemma 10.6.13] show that there is a open subset U_g of $\mathcal{M}_{g,3K}$ corresponding to the curves with trivial automorphism group. The result of Monsky above implies that U_g meets every geometric fiber of $\mathcal{M}_{g,3K} \to \operatorname{Spec} \mathbf{Z}$. This, together with the Lang-Weil method, can be used to show that there exists $N_g > 0$ such that for any field k with $\#k > N_g$ (in particular, any infinite field), there exists a curve X of genus g over k with $\operatorname{Aut} X = \{1\}$ [KS, Remark 10.6.24]. Our main result is that such curves exist even over small finite fields:

Theorem 1. *For any field k and integer $g \geq 3$, there exists a curve X over k of genus g such that* $\operatorname{Aut} X = \{1\}$.

Remark. Our result gives an independent proof that U_g meets every geometric fiber of $\mathcal{M}_{g,3K} \to \operatorname{Spec} \mathbf{Z}$.

We cannot hope to prove Theorem 1 by writing down for each g a single equation with coefficients independent of p, because a curve over $\mathbf{Q}$ of positive genus must have bad reduction at some prime; this follows from the title result of [Fo]. Therefore subdivision into cases seems unavoidable.

Date: November 23, 1999.

Most of this research was done while the author was at Princeton University supported by an NSF Mathematical Sciences Postdoctoral Research Fellowship. The author is currently supported by NSF grant DMS-9801104, a Sloan Fellowship, and a Packard Fellowship.

	Case	Equation of curve
I	$p = 3,\ g \equiv 0$ or $1 \pmod 3$	$y^3 + y^2 = x^{g+1} - x^3 + 1$
II	$p = 3,\ g \equiv 2 \pmod 3$	$y^3 + y^2 = x^2(x-1)^2(x^{g-1} - x^3 + 1)$
III	$p \neq 3,\ g \not\equiv 2 \pmod 3,\ g \not\equiv 0, -1 \pmod p$	$y^3 - 3y = gx^{g+1} - (g+1)x^g + 1$
IV	$p \neq 3,\ g \not\equiv 2 \pmod 3,\ g \equiv 0$ or $-1 \pmod p$	$y^3 - 3y = x^{g+1} + x^g + 1$
V	$p \neq 3,\ g \equiv 2 \pmod 3,\ g \not\equiv 0, 1 \pmod p$	$y^3 - 3y = 2g^{-1}x^{g-1} + (4 - 4g^{-1})x^{-1} - 2$
VI	$p \neq 3,\ g \equiv 2 \pmod 3,\ g \equiv 0$ or $1 \pmod p$	$y^3 - 3y = x^{g-1} - x^{-1} + 1$

TABLE 1. Curves X of genus $g \geq 3$ with $\operatorname{Aut} X = \{1\}$.

The curves we construct are the smooth projective models of the curves given by the equations in Table 1. They are all triple branched covers of $\mathbf{P}^1$. Of course, we could not use double covers of $\mathbf{P}^1$, because these automatically have a non-trivial involution.

Each of these curves is totally ramified above ∞ on the x-line, and separable over the x-line, so each is geometrically integral. We let $h(y)$ denote the cubic in y on the left in each equation, and we let $f(x)$ denote the rational function in x on the right.

2. Computing the genus

The following lemma will let us verify that the curves in Table 1 have genus g in each case.

Lemma 2. *Let $h(y)$ be a cubic polynomial over a field k, and let $f(x)$ be a rational function of degree d over k. Assume that $h'(y)$ is not identically zero, that all poles of f are of order prime to 3, and that f has a pole at $x = \infty$. Let m denote the number of distinct poles of f. Let X be the curve $h(y) = f(x)$ over k. Assume that all affine singularities of X are nodes, and let n denote the number of such nodes. Then the genus g of X is given by the formula*

$$g = d + m - n - 2.$$

Proof. It would be tempting to apply the Hurwitz formula to the 3-to-1 map from $x : X \to \mathbf{P}^1$, but this would require special arguments in characteristic 2 and 3 to handle the wild ramification. Instead we will compute the degree of the divisor of the differential

$$\omega := \frac{dx}{h'(y)} = \frac{dy}{f'(x)} \tag{1}$$

directly. We will still need to be careful in characteristic 3, however.

At an affine node, x and y are both uniformizers at the two corresponding points P_1, P_2 on the nonsingular model, and $f'(x)$ and $h'(y)$ each vanish with multiplicity one, so $v_{P_1}(\omega) = v_{P_2}(\omega) = -1$. By assumption, every other affine point P on X is nonsingular already, so either $f'(x)$ or $h'(y)$ is nonvanishing at P. Thus ω is regular at P. Moreover, if $f'(x)$ is nonvanishing at P, then y is a uniformizer at P, so ω has no zero or pole at P. Similarly if $h'(y)$ is nonvanishing at P, then again ω has no zero or pole at P.

For each pole t of $f(x)$, let c_t denote the order of the pole, which by assumption is prime to 3. Let v_t be the valuation on X corresponding to the point P_t above t. We have $v_\infty(x) = -3$ and $v_\infty(y) = -c_\infty$. In characteristic not 3, we have

$$v_\infty(\omega) = v_\infty(dx) - v_\infty(h'(y)) = v_\infty(x) - 1 - 2v_\infty(y) = -3 - 1 - 2(-c_\infty) = 2c_\infty - 4.$$

In characteristic 3, we have

$$v_\infty(\omega) = v_\infty(dy) - v_\infty(f'(x)) = v_\infty(y) - 1 - (c_\infty - 1)v_\infty(x) = -c_\infty - 1 - (c_\infty - 1)(-3) = 2c_\infty - 4$$

again.

At any other pole t of $f(x)$, we have $v_t(x-t) = 3$, $v_t(y) = -c_t$, $v_t(f(x)) = -3c_t$, so in characteristic not 3, we have

$$v_t(\omega) = v_t(dx) - v_t(h'(y)) = v_t(x-t) - 1 - 2v_t(y) = 3 - 1 - 2(-c_t) = 2c_t + 2.$$

In characteristic 3, we have

$$v_t(\omega) = v_t(dy) - v_t(f'(x)) = v_t(y) - 1 - 3(-c_t - 1) = -c_t - 1 - 3(-c_t - 1) = 2c_t + 2$$

again.

Thus

$$\begin{aligned} 2g - 2 &= \deg \omega \\ &= -2n + (2c_\infty - 4) + \sum_{\text{poles } t \neq \infty} (2c_t + 2) \\ &= -2n - 6 + \sum_{\text{all poles } t} (2c_t + 2) \\ &= -2n - 6 + 2d + 2m, \end{aligned}$$

and we obtain

$$g = d + m - n - 2.$$

□

Lemma 3. *The curves in Table 1 have no affine singularities except for the nodes at* $(0,0)$ *and* $(1,0)$ *in Case II.*

Proof. In general, we find an affine singularity only when $h(y)$ and $-f(x)$ have a common critical value.

In Cases I and II, 0 is the only critical value of $h(y)$, so it suffices to show that $f(x)$ has no multiple zeros, except for 0 and 1 in Case II. In Case I, $f'(x) = (g+1)x^g$ vanishes only at $x = 0$, which is not a zero of f. In Case II, the polynomial $x^{g-1} - x^3 + 1$ does not vanish at 0 or 1, and its derivative is x^{g-2}, which vanishes only at 0.

In Cases III through VI, the critical values of $h(y)$ are ± 2, so it suffices to show that $f(x)$ does not have 2 or -2 as a critical value. In Case III, $f'(x) = g(g+1)x^{g-1}(x-1)$ vanishes only at 0 or 1, but $f(0) = 1$ and $f(1) = 0$ do not equal ± 2, since $p \neq 2, 3$.

In Case IV, $f'(x) = x^g$ if $g \equiv 0 \pmod{p}$, and $f'(x) = -x^{g-1}$ if $g \equiv -1 \pmod{p}$. In either case, $f'(x)$ vanishes only at 0, but $f(0) = 1 \neq \pm 2$.

In Case V, first note that $p \neq 2, 3$. If the derivative

$$f'(x) = \frac{2(g-1)}{g} x^{g-2} - \frac{4(g-1)}{g} x^{-2}$$

vanishes at t, then we find $t^g = 2$, so that

$$f(t) = 2g^{-1}(2t^{-1}) + (4 - 4g^{-1})t^{-1} - 2 = 4t^{-1} - 2.$$

If moreover $f(t) = \pm 2$, then $t = 1$ (t may not be infinite), but this contradicts $t^g = 2$.

In Case VI, let us first suppose $g \equiv 0 \pmod p$. If $f'(x) = -x^{g-2} + x^{-2}$ vanishes at t, then $t^g = 1$, and

$$f(t) = 1 \cdot t^{-1} - t^{-1} + 1 = 1 \neq \pm 2.$$

If instead $g \equiv 1 \pmod p$, then $f'(x) = x^{-2}$, which does not vanish at all away from the poles of f. □

Proposition 4. *In each case of Table 1, the curve X has genus g.*

Proof. We apply Lemma 2. In Cases I, III, and IV, we have

$$d = g + 1, \quad m = 1, \quad n = 0.$$

In Case II, we have

$$d = g + 3, \quad m = 1, \quad n = 2.$$

In Cases V and VI, we have

$$d = g, \quad m = 2, \quad n = 0.$$

Thus we always have $d + m - n - 2 = g$, and the result follows from Lemma 2. □

3. Computing the automorphism group: genus at least 4

The following lemma is classical, but its proof is short, so we will give it.

Lemma 5. *If X is a curve of genus $g \geq 5$, and σ_1, σ_2 are two maps from X to $\mathbf{P}^1$ of degree 3, then $\sigma_2 = \alpha \circ \sigma_1$ for some automorphism α of $\mathbf{P}^1$.*

Proof. Let D be the image of $X \stackrel{(\sigma_1,\sigma_2)}{\longrightarrow} \mathbf{P}^1 \times \mathbf{P}^1$. Let s denote the degree of $X \to D$, and let r_1, r_2 denote the degrees of the two projection maps $D \to \mathbf{P}^1$. We have $r_1 s = r_2 s = 3$, so either $s = 1$ and $r_1 = r_2 = 3$, or $s = 3$ and $r_1 = r_2 = 1$. In the first case, D is a divisor of type $(3, 3)$ on $\mathbf{P}^1 \times \mathbf{P}^1$, and the adjunction formula yields $p_a(D) = 4$. Then the normalization of D has genus at most 4, which contradicts the fact that D is birational to X. Thus $s = 3$ and $r_1 = r_2 = 1$. This means that D is the graph of an automorphism $\alpha : \mathbf{P}^1 \to \mathbf{P}^1$, and we obtain the desired result. □

The result of Lemma 5 is not true in general for $g < 5$, but it is true for certain curves of genus 4, and we have chosen our genus 4 curves in Table 1 to be of this type, as we now show.

Lemma 6. *Let X be a curve of genus 4 given by an equation $h(y) = f(x)$ where h and f are polynomials of degree 3 and 5 respectively. Let σ_1 denote the map $x : X \to \mathbf{P}^1$. If σ_2 is any other map from X to $\mathbf{P}^1$ of degree 3, then $\sigma_2 = \alpha \circ \sigma_1$ for some automorphism α of $\mathbf{P}^1$.*

Proof. By Lemma 2, X necessarily has no affine singularities. Hence the functions $f'(x)$ and $h'(y)$ cannot simultaneously vanish at an affine point P on X. Let ω denote the differential

$$\omega := \frac{dx}{h'(y)} = \frac{dy}{f'(x)}$$

on X. One of the two definitions shows that ω is regular at P. If ω had a zero at P, then dx and dy would both have a zero at P, contradicting the fact that P is nonsingular. Thus ω has no affine zeros or poles. Since $\operatorname{div}(\omega)$ is of degree $2g - 2 = 6$, we have $\operatorname{div}(\omega) = 6P_\infty$, where P_∞ denotes the point at infinity on X. We have $v_\infty(x) = -3$ and $v_\infty(y) = -5$. Hence

ω, $x\omega$, $x^2\omega$, and $y\omega$ are all regular differentials, and they form a basis for $H^0(X, \Omega^1_X)$. The canonical embedding of X is

$$X \to \mathbf{P}^3$$
$$(x, y) \mapsto (1 : x : x^2 : y).$$

and its image lies on the singular quadric $t_0 t_2 = t_1^2$, where t_0, t_1, t_2, t_3 are the homogeneous coordinates on $\mathbf{P}^3$. Hence, by [Ha, Example IV.5.5.2], X has a unique g^1_3, which is to say that X has a unique map to $\mathbf{P}^1$ of degree 3, up to composition with an automorphism of $\mathbf{P}^1$. □

The importance of Lemmas 5 and 6 for our purposes is that they imply that any automorphism of X induces an automorphism of the underlying $\mathbf{P}^1$, the x-line.

Proposition 7. *If $g \geq 4$, then $\operatorname{Aut} X$ is trivial.*

Proof. Suppose $\gamma \in \operatorname{Aut} X$. Let α be the automorphism of $\mathbf{P}^1$ induced by γ. If we knew that α were the identity, then we would be done, since the map $X \to \mathbf{P}^1$ has ramification points of index 2 as well as 3, in each case. We may exploit the fact that α preserves the projection R of the ramification divisor in $\mathbf{P}^1$. In particular, α fixes ∞ in Cases I through IV, and α preserves $\{0, \infty\}$ in Cases V and VI, because these are the points that occur in R with multiplicity greater than one.

Cases I and II.

The points in R of multiplicity one are the zeros of $j(x) := x^n - x^3 + 1$ where $n = g + 1$ in Case I and $n = g - 1$ in Case II. Hence α is a linear map $x \mapsto \lambda x + \mu$ with $\lambda \neq 0$ such that $j(\lambda x + \mu)$ is a multiple of $j(x)$. In this case, comparing leading coefficients yields

$$j(\lambda x + \mu) = \lambda^n j(x),$$

so

$$(\lambda x + \mu)^n - \lambda^3 x^3 - \mu^3 + 1 = \lambda^n (x^n - x^3 + 1).$$

Comparing coefficients of x^1 and noting that $n \not\equiv 0 \pmod 3$, we find $\mu = 0$. Comparing coefficients of x^3 and x^0, we see $\lambda^{n-3} = \lambda^n = 1$, but $\gcd(n - 3, n) = 1$, so $\lambda = 1$.

Case III.

The points in R of multiplicity one are the zeros of $j(x) := (f(x)+2)(f(x)-2)$, and again α is a linear map $x \mapsto \lambda x + \mu$ with $\lambda \neq 0$ such that $j(\lambda x + \mu) = \lambda^{\deg j} j(x)$. It follows that $j'(\lambda x + \mu) = \lambda^{(\deg j)-1} j'(x)$, but

$$j'(x) = 2f(x) \left[g(g + 1)(x^g - x^{g-1}) \right],$$

which, by the computation in the proof of Lemma 3, has distinct zeros except for the zero of multiplicity $g - 1$ at $x = 0$. Thus α must preserve 0; i.e., $\mu = 0$. Since $j(x)$ has terms of degree $2g + 2$ as well as $2g + 1$, $j(\lambda x)$ can be a multiple of $j(x)$ only if $\lambda = 1$.

Case IV.

	Case	Equation of curve
I	$p=3$	$Y^3Z+Y^2Z^2-X^4+X^3Z-Z^4=0$
III	$p\neq 2,3$	$Y^3Z-3YZ^3-3X^4+4X^3Z-Z^4=0$
IV	$p=2$	$Y^3Z+YZ^3+X^4+X^3Z+Z^4=0$

Table 2. Homogeneous equations for the curves X in the case $g=3$.

Just as in Case III, α must be a linear map of the form $x \mapsto \lambda x+\mu$, and μ must be 0. The coefficients of x^{2g+2} and x^{2g+1} in

$$j(x) := (f(x)+2)(f(x)-2) = (x^{g+1}+x^g)^2+2(x^{g+1}+x^g)-3$$

are nonzero if $p\neq 2$, so that $j(\lambda x)$ can be a multiple of $j(x)$ only if $\lambda=1$. If $p=2$, then the coefficients of x^{2g+2} and x^{2g} are nonzero, so we obtain only $\lambda^2=1$, but in characteristic 2, this implies $\lambda=1$ again.

Case V.

Since α preserves $\{0,\infty\}$, it is of the form λx or λx^{-1} for some $\lambda\neq 0$. The points occurring in R with multiplicity one are the zeros of the polynomial

$$\begin{aligned} j(x) &:= x^2(f(x)+2)(f(x)-2) \\ &= (4g^{-2})x^{2g}-(8g^{-1})x^{g+1}+(16g^{-1}-16g^{-2})x^g-(16-16g^{-1})x+(4-4g^{-1})^2, \end{aligned}$$

and each of the five coefficients is nonzero, by definition of Case V. If $\alpha(x)=\lambda x^{-1}$, then $x^{2g}j(\lambda x^{-1})$ would be a multiple of $j(x)$, which is impossible, since the exponents occurring in $j(x)$ are not symmetric. If $\alpha(x)=\lambda x$, then $j(\lambda x)$ is a multiple of $j(x)$, which implies $\lambda=1$, since the coefficients of x^1 and x^0 in $j(x)$ are nonzero.

Case VI.

Again α is λx or λx^{-1} for some $\lambda\neq 0$. The points occurring in R with multiplicity one are the zeros of the polynomial

$$\begin{aligned} j(x) &:= x^2(f(x)+2)(f(x)-2) \\ &= x^{2g}+2x^{g+1}-2x^g-3x^2-2x+1. \end{aligned}$$

If $\alpha(x)=\lambda x^{-1}$, then $x^{2g}j(\lambda x^{-1})$ would be a multiple of $j(x)$, which is impossible, since the exponents occurring in $j(x)$ are not symmetric (even when $p=2$). If $\alpha(x)=\lambda x$, then $j(\lambda x)$ is a multiple of $j(x)$. The coefficients of x^1 and x^0 are nonzero if $p\neq 2$, so $\lambda=1$. If $p=2$, then the coefficients of x^2 and x^0 are nonzero, so $\lambda^2=1$, and we again have $\lambda=1$. □

4. Computing the automorphism group: genus 3

From now on, we assume $g=3$. It will be convenient to rewrite the equations of our curves as the zero set of a homogeneous polynomial $F(X,Y,Z)$. These are given in Table 2. Note that we are in Case I, III, or IV, respectively, depending on the value of p. We trust that the use of X as a homogeneous coordinate as well as for the curve will not create confusion.

Proposition 8. *If $g=3$, then* $\operatorname{Aut} X$ *is trivial.*

Proof. We can no longer say that automorphisms of X induce automorphisms of the x-line. Instead, we know that X is a smooth plane quartic, so X equals its canonical embedding in $\mathbf{P}^2$, and any possible automorphism γ is induced by an automorphism of $\mathbf{P}^2$. We represent such an automorphism of $\mathbf{P}^2$ by a matrix $L = \{\ell_{ij}\}_{1\le i,j\le 3}$. By scaling L, we may assume $F \circ L = F$, where we are identifying L with the corresponding linear change of coordinates. Let A denote the Hessian matrix of F, i.e., the 3×3 matrix of second partial derivatives of F.

As usual, it will suffice to show that γ induces the identity of the x-line, since we know in each case that the 3-to-1 map $X/Z : X \to \mathbf{P}^1$ has ramification points of index 2 and 3. But we stress that *a priori*, it is not clear that γ induces an automorphism of $\mathbf{P}^1$ at all; in other words the x-coordinate of $\gamma(P)$ is not obviously a function of the x-coordinate of P only.

Case I: $p = 3$.

We compute

$$A = \begin{bmatrix} 0 & 0 & 0 \\ 0 & -Z^2 & YZ \\ 0 & YZ & -Y^2 \end{bmatrix}.$$

In particular, $\partial F/\partial X$ is killed by all the first order differential operators $\partial/\partial X$, $\partial/\partial Y$, $\partial/\partial Z$, so the same is true for

$$\frac{\partial(F\circ L)}{\partial X} = \ell_{11}\frac{\partial F}{\partial X}\circ L + \ell_{21}\frac{\partial F}{\partial Y}\circ L + \ell_{31}\frac{\partial F}{\partial Z}\circ L.$$

But the only $\overline{k}$-linear combinations of the columns of A that are zero are the multiples of the first column, so $\ell_{21} = \ell_{31} = 0$. In other words, X occurs only in the first coordinate of $L(X, Y, Z)$. Without loss of generality we may also assume $\ell_{11} = 1$. Hence the coefficient of X^1 in $F \circ L$ equals that in

$$-(X + \ell_{12}Y + \ell_{13}Z)^4 + (X + \ell_{12}Y + \ell_{13}Z)^3(\ell_{32}Y + \ell_{33}Z),$$

which is $-\ell_{12}^3Y^3 - \ell_{13}^3Z^3$. On the other hand, this must equal the coefficient of X^1 in F, which is zero, so $\ell_{12} = \ell_{13} = 0$. Equating coefficients of X^3 in F and in $F \circ L$, we obtain

$$Z = \ell_{32}Y + \ell_{33}Z,$$

so $\ell_{32} = 0$ and $\ell_{33} = 1$.

We now know that L is of the form $(X, Y, Z) \mapsto (X, \ell_{22}Y + \ell_{23}Z, Z)$. In particular, γ must induce the identity on $\mathbf{P}^1$, as desired.

Case III: $p \ne 2, 3$

We compute

$$A = \begin{bmatrix} -36X^2 + 24XZ & 0 & 12X^2 \\ 0 & 6YZ & 3Y^2 - 9Z^2 \\ 12X^2 & 3Y^2 - 9Z^2 & -18YZ - 12Z^2 \end{bmatrix}.$$

The entries of the first column are $\overline{k}$-linearly dependent, because of the 0. The same is true for the second column. But using the fact that the six distinct nonzero entries of A are linearly independent over $\overline{k}$, we see that the only $\overline{k}$-linear combinations of the columns whose entries are $\overline{k}$-linearly dependent are multiples of the first column or multiples of the second column. This implies that L has one of the following two shapes:

$$\begin{bmatrix} * & 0 & * \\ 0 & * & * \\ 0 & 0 & * \end{bmatrix} \quad \text{or} \quad \begin{bmatrix} 0 & * & * \\ * & 0 & * \\ 0 & 0 & * \end{bmatrix},$$

and we may assume $\ell_{33} = 1$. In other words, γ gives an affine linear automorphism of the curve

$$y^3 - 3y = 3x^4 - 4x^3 + 1,$$

which we are writing in inhomogenous form again, and is of the form $(x, y) \mapsto (\ell_{11}x + \ell_{13}, \ell_{22}y + \ell_{23})$ or $(x, y) \mapsto (\ell_{12}y + \ell_{13}, \ell_{21}x + \ell_{23})$. The second is impossible, since the defining equation is cubic in y but quartic in x. The first implies that γ induces an automorphism of the x-line, and

$$(\ell_{22}y + \ell_{23})^3 - 3(\ell_{22}y + \ell_{23}) - 3(\ell_{11}x + \ell_{13})^4 + 4(\ell_{11}x + \ell_{13})^3 - 1 = \mu(y^3 - 3y - 3x^4 + 4x^3 - 1) \tag{2}$$

for some $\mu \in \overline{k}^*$. Equating coefficients of x^2 and x^1 in (2) yields

$$-18\ell_{11}^2\ell_{13}^2 + 12\ell_{11}^2\ell_{13} = 0, \tag{3}$$

$$-12\ell_{11}\ell_{13}^3 + 12\ell_{11}\ell_{13}^2 = 0. \tag{4}$$

Multiplying (3) and (4) by ℓ_{13} and ℓ_{11}, respectively, and subtracting, we obtain

$$-6\ell_{11}^2\ell_{13}^3 = 0.$$

But $\ell_{11} \neq 0$, since L must be invertible. Therefore $\ell_{13} = 0$. Equating coefficients of x^4 in (2) shows that $\mu = \ell_{11}^4$. Equating coefficients of x^3 in (2) shows that

$$4\ell_{11}^3 = \ell_{11}^4 \cdot 4$$

so $\ell_{11} = 1$. Thus γ induces the identity on $\mathbf{P}^1$.

Case IV: $p = 2$.

We compute

$$A = \begin{bmatrix} 0 & 0 & X^2 \\ 0 & 0 & Y^2 + Z^2 \\ X^2 & Y^2 + Z^2 & 0 \end{bmatrix}.$$

The $\overline{k}$-linear combinations of the columns that give a column vector whose entries span a $\overline{k}$-linear space of dimension at most one are the combinations of the first two columns. It follows that L has the shape

$$\begin{bmatrix} * & * & * \\ * & * & * \\ 0 & 0 & * \end{bmatrix},$$

and we may assume $\ell_{33} = 1$. In other words, γ gives an affine linear automorphism $(x, y) \mapsto (\ell_{11}x + \ell_{12}y + \ell_{13}, \ell_{21}x + \ell_{22}y + \ell_{23})$ of the curve

$$y^3 + y = x^4 + x^3 + 1,$$

which we are writing in inhomogenous form again. By looking at the terms of highest degree, we see that $\ell_{12} = 0$, so that γ induces an automorphism $x \mapsto \ell_{11}x + \ell_{13}$ of the x-line. Moreover,

$$(\ell_{11}x + \ell_{13})^4 + (\ell_{11}x + \ell_{13})^3 + 1 = \mu(x^4 + x^3 + 1)$$

for some $\mu \in \overline{k}^*$, since the branch points of $x : X \to \mathbf{P}^1$ are located at the zeros of $x^4 + x^3 + 1$. Equating coefficients of x^1 shows $3\ell_{11}\ell_{13}^2 = 0$, but $\ell_{11} \neq 0$, so $\ell_{13} = 0$. Equating coefficients of x^4 shows $\mu = \ell_{11}^4$. Then equating coefficients of x^3 shows $\ell_{11}^3 = \ell_{11}^4$, so $\ell_{11} = 1$. Thus γ again induces the identity on the x-line, as desired. □

This completes the proof of Theorem 1. In the second paper [Po2] of this series, we will prove the existence of hyperelliptic curves X of any genus $g \geq 2$ over any field k, such that $\operatorname{Aut} X = \{1, \iota\}$, where ι denotes the hyperelliptic involution. In the third paper [Po3], we will prove the existence of smooth hypersurfaces $X \subset \mathbf{P}^{n+1}$ of degree d with $\operatorname{Aut} X = \{1\}$, for prescribed n and d (satisfying minor constraints).

Acknowledgements

I thank Nick Katz for bringing the problem considered in this paper to my attention.

References

[Ac] Accola, R., Strongly branched coverings of closed Riemann surfaces, *Proc. Amer. Math. Soc.* **26** (1970), 315–322.

[Ba] Baily, W., On the automorphism group of a generic curve of genus > 2, *J. Math. Kyoto Univ.* **1** (1961/1962), 101–108; correction, 325.

[Fo] Fontaine, J.-M., Il n'y a pas de variété abélienne sur **Z**, *Invent. Math.* **81** (1985), no. 3, 515–538.

[Ha] Hartshorne, R., *Algebraic geometry*, Springer-Verlag, New York, 1977.

[KS] Katz, N. M., and Sarnak, P., *Random matrices, Frobenius eigenvalues, and monodromy*, American Mathematical Society Colloquium Publications **45**, American Mathematical Society, Providence, RI, 1999.

[Me] Mednyh, A. D., An example of a compact Riemann surface with a trivial group of automorphisms, *Dokl. Akad. Nauk SSSR* **237** (1977), no. 1, 32–34. English translation in *Soviet Math. Dokl.* **18** (1977), no. 6, 1396–1403.

[Mo] Monsky, P., Thesis, Univ. of Chicago, Chicago, Ill., 1962.

[Po2] Poonen, B., Varieties without extra automorphisms II: hyperelliptic curves, preprint, 1999.

[Po3] Poonen, B., Varieties without extra automorphisms III: hypersurfaces, preprint, 1999.

[Tu] Turbek, P., An explicit family of curves with trivial automorphism group, *Proc. Amer. Math. Soc.* **122** (1994), no. 3, 657–664.

Department of Mathematics, University of California, Berkeley, CA 94720-3840, USA
E-mail address: `poonen@math.berkeley.edu`