VARIETIES WITHOUT EXTRA AUTOMORPHISMS II: HYPERELLIPTIC CURVES

BJORN POONEN

ABSTRACT. For any field k and integer $g \geq 2$, we construct a hyperelliptic curve X over k of genus g such that $\#(\operatorname{Aut} X) = 2$. We also prove the existence of principally polarized abelian varieties (A, θ) over k of prescribed dimension $g \geq 1$ such that $\operatorname{Aut}(A, \theta) = \{\pm 1\}$.

1. INTRODUCTION

If X is a (smooth, projective, and geometrically integral) curve over a field k, let $\operatorname{Aut} X$ denote the group of automorphisms of X defined over $\overline{k}$. In [Po1], we proved that for any field k and integer $g \geq 3$, there exists a curve X over k of genus g such that $\operatorname{Aut} X = \{1\}$.

This paper studies the analogous problem for hyperelliptic curves. If X is a hyperelliptic curve, then X has a non-trivial automorphism, namely the hyperelliptic involution ι, so our result takes the following form:

Theorem 1. *For any field k and integer $g \geq 2$, there exists a hyperelliptic curve X over k of genus g such that* $\operatorname{Aut} X = \{1, \iota\}$.

As a corollary, we obtain a similar result for principally polarized abelian varieties. For an abelian variety A with polarization θ defined over k, let $\operatorname{Aut}(A, \theta)$ denote the group of automorphisms of A over $\overline{k}$ respecting the polarization (and the group structure of A).

Corollary 2. *For any field k and integer $g \geq 1$, there exists a g-dimensional principally polarized abelian variety (A, θ) over k such that* $\operatorname{Aut}(A, \theta) = \{\pm 1\}$.

Proof. For $g = 1$, it suffices to let A be an elliptic curve of j-invariant not 0 or 1728 [Si, Theorem III.10.1]. For $g \geq 2$, let A be the Jacobian of the curve given by Theorem 1; the desired property then follows from Torelli's theorem (see [Mi, Theorem 12.1]). □

Remarks. Corollary 2 is proved for k algebraically closed in [KS, Lemma 11.2.6], also with Jacobians. It is also true that for any polarized abelian scheme $\mathcal{A} \to S$ of relative dimension $g \geq 1$, the set of points $s \in S$ for which the automorphism group of the fiber $\mathcal{A}_s$ (as polarized abelian variety) is $\{\pm 1\}$ is open in S [KS, Lemma 11.2.5]. In particular, it follows that a generic principally polarized abelian variety of dimension $g \geq 1$ (corresponding to the generic point of the coarse moduli space of principally polarized abelian varieties of dimension g over an algebraically closed field k) has automorphism group $\{\pm 1\}$.

Date: November 26, 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. This article has been published in *Math. Res. Letters* **7** (2000), no. 1, 77–82.

2. Construction

In this section, we describe a hyperelliptic curve X for each k and g, by giving the equation of an affine curve whose smooth projective model is the desired X. The proof that X has genus g and that $\operatorname{Aut} X = \{1, \iota\}$ will be presented in Section 3.

We would like to exploit Galois action to control automorphisms in the proof of Theorem 1. Hence we will first reduce to the case where $k = \mathbf{Q}$ or $k = \mathbf{F}_p$ for some prime p. If $K \subseteq L$ are algebraically closed fields, and X is a curve of genus $g \geq 2$ over K, then the automorphisms of X defined over L are all defined over K, because the $\operatorname{Aut}(L/K)$-orbit of any new automorphism would be infinite, violating the theorem that $\operatorname{Aut} X$ is finite for any curve of genus $g \geq 2$ over an algebraically closed field [Sc]. Hence in proving Theorem 1, we may replace k by its minimal subfield. Let p be the characteristic of k, so that $k = \mathbf{F}_p$ if $p > 0$, and $k = \mathbf{Q}$ if $p = 0$.

Case I: $p = 2$.

Let X be the curve

$$y^2 + y = x^{2g-1} + \frac{1}{x}.$$

Case II: $p = 0$.

For fixed g, let $A = \{0, 1, 2, \ldots, 2g\}$, and let $A^{(3)}$ denote the set of ordered triples of distinct elements of A. For each pair of distinct triples $a = (a_1, a_2, a_3)$ and $b = (b_1, b_2, b_3)$ in $A^{(3)}$, there is a unique non-trivial automorphism ϕ_{ab} of $\mathbf{P}^1$ such that $\phi_{ab}(a_i) = b_i$ for $i = 1, 2, 3$. Let X be the curve

$$y^2 = x(x-1)(x-2)\ldots(x-2g)(x-t)$$

for some $t \in \mathbf{Q}$ outside the finite set

$$A \cup \bigcup_{a \neq b} \left(\phi_{ab}(A) \cup \{r \in \mathbf{Q} : \phi_{ab}(r) = r\}\right).$$

Case III: $p \geq 3$, $g \geq 4$.

Let $q(x) \in k[x]$ be an irreducible cubic. Let $j(x) \in \overline{k}(x)$ be an automorphism of $\mathbf{P}^1$ that acts as a 3-cycle on the roots of $q(x)$. Then j has at most two fixed points, so we may pick $c \in k$ such that $j(c) \neq c$. If $2g - 2 \not\equiv 0 \pmod 3$, choose $r(x) \in k[x]$ irreducible of degree $2g-2$; otherwise choose $r(x)$ to be the product of two irreducible polynomials in $k[x]$ of degrees 2 and $2g-4$. Let X be the curve $y^2 = f(x)$, where

$$f(x) := (x - c)q(x)r(x).$$

Case IV: $p \geq 3$, $g = 3$.

Let $q(x), r(x) \in k[x]$ be irreducible polynomials of degree 2 and 3, respectively. Let j be an automorphism of $\mathbf{P}^1$ that acts as a 3-cycle on the roots of $r(x)$. Since $\#\mathbf{P}^1(k) \geq 4$, we can choose distinct $a, b, c \in \mathbf{P}^1(k)$ such that j does *not* act as a 3-cycle on $\{a, b, c\}$. Let X

be the curve $y^2 = f(x)$, where

$$f(x) := (x-a)(x-b)(x-c)q(x)r(x).$$

(If $a = \infty$, then we interpret "$x - a$" as "1", since this accomplishes what we actually want: for the map $X \to \mathbf{P}^1$ to be ramified above a, b, c in addition to the roots of q and r. Similar interpretations should be made if $b = \infty$ or $c = \infty$.)

Case V: $p \geq 3$, $g = 2$.

Let $q(x), r(x) \in k[x]$ be irreducible polynomials of degree 2 and 3, respectively. Let q_1, q_2 be the roots of q in $\overline{k}$, and let r_1, r_2, r_3 be the roots of r in $\overline{k}$, ordered so that $r_1^p = r_2$. Let j be the automorphism of $\mathbf{P}^1$ fixing q_1 and q_2 and mapping r_1 to r_2. Pick $c \in k$ such that j does *not* map r_3 to c. Let X be the curve $y^2 = f(x)$, where

$$f(x) := (x-c)q(x)r(x).$$

3. Proof of Theorem 1

In each case, let S denote the set of branch points of the separable 2-to-1 map $X \to \mathbf{P}^1$. For $p \neq 2$, $\#S = 2g+2$, so that X has genus g by the Hurwitz formula. Any automorphism of X that is neither the identity nor the hyperelliptic involution must induce a non-trivial automorphism of $\mathbf{P}^1$ preserving S.

Case I: $p = 2$.

Let P_0 and P_∞ denote the points on X where $x = 0$ and $x = \infty$, respectively. The ramification divisor of the 2-to-1 map $X \to \mathbf{P}^1$ is $2gP_\infty + 2P_0$, so the genus of X is g by the Hurwitz formula. Any automorphism of X induces an automorphism of $\mathbf{P}^1$ preserving the projection of the ramification divisor to $\mathbf{P}^1$. The only such automorphisms of $\mathbf{P}^1$ are those of the form $x \mapsto \lambda x$ for $\lambda \in \overline{k}^*$, but the two function fields obtained by adjoining to $\overline{k}(x)$ a root y_1 of

$$y_1^2 + y_1 = x^{2g-1} + \frac{1}{x}$$

or a root y_2 of

$$y_2^2 + y_2 = (\lambda x)^{2g-1} + \frac{1}{\lambda x}$$

are distinct by Artin-Schreier theory, unless $\lambda = 1$. Hence all automorphisms of X induce the trivial automorphism of the quotient $\mathbf{P}^1$.

Case II: $p = 0$.

Since $g \geq 2$, if an automorphism h of $\mathbf{P}^1$ preserves $S = \{0, 1, \ldots, 2g, t\}$, then h maps some 3-element subset of $A = \{0, 1, \ldots, 2g\}$ to another 3-element subset of A. If h is non-trivial, then $h = \phi_{ab}$ for some $a, b \in A^{(3)}$. But then $h^{-1}(t) \notin S$, by choice of t, and this contradicts the definition of h.

Case III: $p \geq 3$, $g \geq 4$.

Let $\mathbf{F}$ denote the compositum of all finite extensions of $k = \mathbf{F}_p$ of degree prime to 3. Exactly $(2g+2)-3$ points in S are $\mathbf{F}$-rational. Suppose that h is a non-trivial automorphism of $\mathbf{P}^1$ preserving S. Then h must map at least $(2g+2)-6$ of these $\mathbf{F}$-rational points to other $\mathbf{F}$-rational points of S. But $(2g+2)-6 \geq 3$, and h is determined by its values at 3 points, so h must be defined over $\mathbf{F}$. In particular, h preserves the set of three non-$\mathbf{F}$-rational points of S, the roots of the cubic $q(x)$. If h fixed any one of them, then since they are all conjugate over $\mathbf{F}$, h would fix them all, and h would be trivial. Otherwise, h acts as a 3-cycle, and after replacing h by h^{-1} if necessary, we may assume $h = j$. Also, h is defined over k, since its values at the three roots of $q(x)$ are specified in a $\mathrm{Gal}(\overline{k}/k)$-stable way. Thus h maps c into a k-rational element of S, so $h(c) = c$, contradicting the choice of c.

Case IV: $p \geq 3$, $g = 3$.

Suppose that h is a non-trivial automorphism of $\mathbf{P}^1$ preserving S. Since six of the eight points in S are $\mathbf{F}_{p^3}$-rational, at least four $\mathbf{F}_{p^3}$-rational points in S are mapped by h to other $\mathbf{F}_{p^3}$-rational points, and hence h is defined over $\mathbf{F}_{p^3}$. In particular, h preserves the set of roots of the quadratic $q(x)$. If h mapped any of the three $\mathbf{F}_p$-rational points in S to any other, then this together with the action on the roots of $q(x)$ would give a $\mathrm{Gal}(\overline{\mathbf{F}}_p/\mathbf{F}_p)$-stable specification of h, so h would be defined over $\mathbf{F}_p$. Otherwise, h interchanges the set $\{a, b, c\}$ of three $\mathbf{F}_p$-rational points in S with the set of three roots of $r(x)$. In the latter case, if we let σ be a generator of $\mathrm{Gal}(\mathbf{F}_{p^6}/\mathbf{F}_{p^2})$, we obtain a new non-trivial automorphism $h' := {}^{\sigma}h \circ h^{-1}$ that maps a, b, c to themselves in some order. Thus in any case, we obtain a non-trivial $\mathbf{F}_p$-rational automorphism (which we rename h) of $\mathbf{P}^1$ preserving S. As in Case III, h must act as a 3-cycle on the roots of the cubic $r(x)$. After replacing h by h^{-1} if necessary, we have $h = j$. Since an automorphism of $\mathbf{P}^1$ is determined by three values, h must be of order 3, and it is k-rational, so it must either fix a, b, c pointwise or act as a 3-cycle on a, b, c. The former would make h trivial, and the latter was expressly ruled out by our assumptions.

Case V: $p \geq 3$, $g = 2$.

Label the roots $r_1, r_2, r_3, c, q_1, q_2$ with $1, 2, 3, 4, 5, 6$, respectively, so that the absolute Frobenius acts on S as the permutation $\sigma := (123)(56)$. Let H be the group of automorphisms of $\mathbf{P}^1$ preserving S, which we may faithfully view as a subgroup of S_6, since automorphisms are determined already by three values. The Frobenius automorphism acts on H as conjugation by σ. By choice of c, $(12)(34) \notin H$. Therefore the non-existence of non-trivial automorphisms follows from the purely group-theoretical Lemma 3 below.

Lemma 3. *Suppose that H is a subgroup of S_6 such that*

1. *Each non-trivial element of H has at most two fixed points.*
2. *H is normalized by $\sigma := (123)(56)$.*
3. *The permutation $(12)(34)$ is* not *in H.*

Then $H = \{1\}$.

Proof. Suppose that there exists an element $\pi \in H$ that does *not* commute with $\sigma^3 = (56)$. Define $\eta := \pi^{-1}\sigma^3\pi\sigma^{-3}$. Then $\eta \in H$, by condition (2), and η is the product of the two unequal transpositions $\pi^{-1}\sigma^3\pi$ and $\sigma^{-3} = (56)$. By condition (1), η has at most two fixed points, so η must be $(ab)(56)$ for some $a < b < 5$. Let $\eta' := \sigma\eta\sigma^{-1}$, which is in H, by

condition (2). Then $\eta' = (a'b')(56)$ for some $a' < b' < 5$. But the transposition $(a'b') = (123)(ab)(123)^{-1}$ cannot be disjoint from (ab), so $\eta\eta'$ violates condition (1).

Thus every element of H commutes with (56), and $H \subseteq S_4 \times S_2$. By condition (1), H maps isomorphically to its projection H' in S_4. If H' had an element of order 3, the corresponding element of H would be a 3-cycle, violating condition (1). Hence $\#H'$ divides $4!/3 = 8$. Assume H' is not trivial. Then H' contains an element of order 2, i.e., a transposition τ or an S_4-conjugate of (12)(34). In the former case, by condition (2), $(123)\tau(123)^{-1}\tau$ would be an element of order 3 in H', a contradiction. Thus H' contains an S_4-conjugate of (12)(34). All such conjugates are conjugate by powers of (123), so by condition (2), H' contains $V_4 := \{1, (12)(34), (13)(24), (14)(23)\}$. If we map V_4 via the inverse of the isomorphism $H \to H'$, and then map down to $S_2 = \{1, (56)\}$, the kernel is non-trivial, so at least one of (12)(34), (13)(24), (14)(23) is actually in H. Conjugating by powers of σ, and using condition (2), we find that all three are in H. This violates condition (3), so H' is trivial, and so is H. □

This completes the proof of Theorem 1. In the next paper of this series [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, and for remarking that Theorem 1 implies Corollary 2.

References

[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.

[Mi] Milne, J. S., Jacobian Varieties, in: Cornell, G., Silverman, J.H.(eds.), *Arithmetic geometry*, 167–212, Springer-Verlag, New York, 1986.

[Po1] Poonen, B., Varieties without extra automorphisms I: curves, preprint, 1999.

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

[Sc] Schmid, H. L., Über die Automorphismen eines algebraischen Funktionenkörpers von Primzahlcharakteristik, *J. Reine Angew. Math.* **179** (1938), 5–15.

[Si] Silverman, J., *The arithmetic of elliptic curves*, Graduate Texts in Mathematics **106**, Springer-Verlag, New York-Berlin, 1986.

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