Journal of Number Theory 151 (2015) 7–17

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

Images of 2-adic representations associated to hyperelliptic Jacobians

Jeffrey Yelton

The Pennsylvania State University, Mathematics Department, University Park, State College, PA 16802, United States

ARTICLE INFO

Article history:
Received 24 November 2013
Received in revised form 10 October 2014
Accepted 10 October 2014
Available online 9 January 2015
Communicated by Kenneth A. Ribet

Keywords:
Galois group
Elliptic curve
Hyperelliptic curve
Jacobian variety
Tate module

ABSTRACT

Text. Let k be a subfield of $\mathbb{C}$ which contains all 2-power roots of unity, and let $K = k(\alpha_1, \alpha_2, \ldots, \alpha_{2g+1})$, where the α_i's are independent and transcendental over k, and g is a positive integer. We investigate the image of the 2-adic Galois action associated to the Jacobian J of the hyperelliptic curve over K given by $y^2 = \prod_{i=1}^{2g+1}(x - \alpha_i)$. Our main result states that the image of Galois in $\mathrm{Sp}(T_2(J))$ coincides with the principal congruence subgroup $\Gamma(2) \lhd \mathrm{Sp}(T_2(J))$. As an application, we find generators for the algebraic extension $K(J[4])/K$ generated by coordinates of the 4-torsion points of J.

Video. For a video summary of this paper, please visit http://youtu.be/VXEGYxA6N8w.

1. Introduction

Fix a positive integer g. An affine model for a hyperelliptic curve over $\mathbb{C}$ of genus g may be given by

$$y^2 = \prod_{i=1}^{2g+1}(x - \alpha_i), \tag{1}$$

E-mail address: yelton@math.psu.edu.

http://dx.doi.org/10.1016/j.jnt.2014.10.020
0022-314X/

with α_i's distinct complex numbers. Now let $\alpha_1, \ldots, \alpha_{2g+1}$ be transcendental and independent over $\mathbb{C}$, and let L be the subfield of $\mathbb{C}(\alpha) := \mathbb{C}(\alpha_1, \ldots, \alpha_{2g+1})$ generated over $\mathbb{C}$ by the elementary symmetric functions of the α_i's. For any positive integer N, let $J[N]$ denote the N-torsion subgroup of $J(\bar{L})$. For each $n \geq 0$, let $L_n = L(J[2^n])$ denote the extension of L over which the 2^n-torsion of J is defined. Set

$$L_\infty := \bigcup_{n=1}^{\infty} L_n.$$

Note that $\mathbb{C}(\alpha_1, \ldots \alpha_{2g+1})$ is Galois over L with Galois group isomorphic to S_{2g+1}. It is well known [5, Corollary 2.11] that $\mathbb{C}(\alpha_1, \ldots, \alpha_{2g+1}) = L_1$, so $\mathrm{Gal}(L_1/L) \cong S_{2g+1}$. Fix an algebraic closure $\bar{L}$ of L, and write G_L for the absolute Galois group $\mathrm{Gal}(\bar{L}/L)$.

Let C be the curve defined over L by Eq. (1), and let J/L be its Jacobian. For any prime ℓ, let

$$T_\ell(J) := \lim_{\leftarrow n} J\left[\ell^n\right]$$

denote the ℓ-adic Tate module of J; it is a free $\mathbb{Z}_\ell$-module of rank $2g$ (see [6, §18]). For the rest of this paper, we write $\rho_\ell : G_L \to \mathrm{Aut}(T_\ell(J))$ for the continuous homomorphism induced by the natural Galois action on $T_\ell(J)$. Write $\mathrm{SL}(T_\ell(J))$ (resp. $\mathrm{Sp}(T_\ell(J))$) for the subgroup of automorphisms of the 2-adic Tate module $T_\ell(J)$ with determinant 1 (resp. automorphisms of $T_\ell(J)$ which preserve the Weil pairing). Since L contains all 2-power roots of unity, the Weil pairing on $T_2(J)$ is Galois invariant, and it follows that the image of ρ_2 is contained in $\mathrm{Sp}(T_2(J))$. For each $n \geq 0$, we denote by

$$\Gamma\left(2^n\right) := \left\{g \in \mathrm{Sp}\left(T_2(J)\right) \mid g \equiv 1 \pmod{2^n}\right\} \lhd \mathrm{Sp}\left(T_2(J)\right)$$

the level-2^n principal congruence subgroup of $\mathrm{Sp}(T_2(J))$.

Our main theorem is the following.

Theorem 1.1. *With the above notation, the image under ρ_2 of the Galois subgroup fixing L_1 is $\Gamma(2) \lhd \mathrm{Sp}(T_2(J))$.*

Before setting out to prove this theorem, we state some easy corollaries.

Corollary 1.2. *Let G denote the image under ρ_2 of all of G_L. Then we have the following:*

a) G contains $\Gamma(2) \lhd \mathrm{Sp}(T_2(J))$, and $G/\Gamma(2) \cong S_{2g+1}$.

b) In the case that $g = 1$, $G = \mathrm{Sp}(T_2(J)) = \mathrm{SL}(T_2(J))$.

c) For each $n \geq 1$, the homomorphism ρ_2 induces an isomorphism

$$\bar{\rho}_2^{(n)} : \mathrm{Gal}(L_n/L_1) \xrightarrow{\sim} \Gamma(2)/\Gamma\left(2^n\right)$$

via the restriction map $\mathrm{Gal}(\bar{L}/L_1) \twoheadrightarrow \mathrm{Gal}(L_n/L_1)$.