A remark on the arithmetic invariant theory of hyperelliptic curves

Jack A. Thorne*

October 10, 2014

Abstract

Let C be a hyperelliptic curve over a field k of characteristic 0, and let $P \in C(k)$ be a marked Weierstrass point. As Bhargava and Gross have observed, the 2-descent on the Jacobian of C can be rephrased in terms of the language of arithmetic invariant theory, using the geometry of pencils of quadrics. We give a simple re-interpretation of their construction using instead the geometry of the curve C.

Contents

1 Introduction

Let k be a field of characteristic 0, and let $f \in k[x]$ be a monic polynomial of odd degree $N \geq 5$ with non-zero discriminant $\Delta(f) \neq 0$. The affine curve over k

$$C_f^0 : y^2 = f$$

is then smooth, and we write C_f for its smooth projective completion, and $J_f = \operatorname{Jac} C_f$ for its Jacobian variety. This note is about the 2-descent on the variety J_f.

Let $A_f = k[x]/(f)$. It is well-known (see [Sch95]) that there is an injective homomorphism, functorial in k:

$$J_f(k)/2J_f(k) \hookrightarrow A_f^\times / k^\times (A_f^\times)^2. \tag{1.1}$$

The existence of this map is usually derived using Galois cohomology from the existence of Kummer exact sequence

$$0 \longrightarrow J_f[2] \longrightarrow J_f \xrightarrow{[2]} J_f \longrightarrow 0$$

and the isomorphism $J_f[2] \cong (\operatorname{Res}_{A_f/k} \mu_2)/\mu_2$ of finite k-groups.

In the work [BG12a] of Bhargava and Gross, the map (1.1) is taken as the starting point for a relation between the arithmetic of the variety J_f and the arithmetic invariant theory of the pair (G, W_0), where:

- $G = \mathrm{SO}(V_0)$ is the special orthogonal group of a split orthogonal space V_0 over k of dimension $\dim V_0 = \deg f$;

*This research was partially conducted during the period the author served as a Clay Research Fellow.

- and $W_0 \subset \mathrm{End}_k(V_0)$ is the representation of G on the space of self-adjoint linear endomorphisms of V_0.

More precisely, the authors carry out the following steps:

1. To any element $\alpha \in A_f^\times / k^\times (A_f^\times)^2$, they associate an orthogonal space V of dimension $\dim V = \deg f$, and a self-adjoint linear operator $T \in W \subset \mathrm{End}_k(V)$ with characteristic polynomial f.
2. If α is in the image of the map (1.1), they show that there is a (non-canonical) isomorphism $V \cong V_0$ of orthogonal spaces. (In other words: V is split.) The element T then determines a G-orbit in W_0 with characteristic polynomial f.

The essential ingredient for the second step is a description of the elements of the Galois cohomology set $H^1(k, J_f[2])$ in terms of the geometry of pencils of quadrics.

In this note, we give another approach to the construction of G-orbits in W_0 from rational points of $J_f(k)$, which avoids both Galois cohomology and the geometry of pencils of quadrics. If $P \in J_f(k)$, then we can view P as being the isomorphism class of a line bundle $\mathcal{L}$ on the curve C_f. We construct an orthogonal space V directly from $\mathcal{L}$. We then show it is a split orthogonal space by writing down a maximal isotropic subspace in V, using the Mumford representation of the line bundle $\mathcal{L}$.

Given the elementary nature of this construction, it would be very interesting to try to generalize it to other situations (such as the families of non-hyperelliptic curves studied in [Tho14]). In particular, it is possible to adapt our construction when $k = \mathbb{Q}$ to give integral orbits, giving an alternative proof of [BG12b, Proposition 19]. The analogous problem for non-hyperelliptic curves has not yet been solved. Another motivation for our construction is that the orbits we construct can naturally be considered as sitting inside transverse slices to nilpotent orbits inside the Lie algebra of PGL_N, along the lines considered in eg. [Ngô99, §1.1]. This explains to some extent the appearance of these transverse slices in [Tho13].

We now describe the organization of this note. In §2, we recall some basic facts about orthogonal spaces. In §3, we recall the definition of the map (1.1), and its expression in terms of the Mumford representation. These first two sections are thus a review of existing ideas. Finally, in §4, we carry out the construction described above, and verify by explicit calculation that the '2-descent' map defined this way agrees with the cohomological one described in §3. In this way we give a new proof of [BG12b, Proposition 11].

2 Background

2.1 An orbit problem over k

Let k be a field of characteristic 0. Let $N = 2n + 1$ be a positive odd integer.

Definition 2.1. *An orthogonal space of dimension N over k is a pair $(V, \langle \cdot, \cdot \rangle)$, where:*

1. *V is a k-vector space of dimension N.*
2. *$\langle \cdot, \cdot \rangle : V \times V \to k$ is a non-degenerate symmetric bilinear pairing.*

A morphism $(V, \langle \cdot, \cdot \rangle_V) \to (W, \langle \cdot, \cdot \rangle_W)$ of orthogonal spaces is a linear map $\varphi : V \to W$ such that for all $x, y \in V$, $\langle \varphi(x), \varphi(y) \rangle_W = \langle x, y \rangle_V$.

When the pairing is clear from the context, we will drop it from the notation and simply refer to the vector space V as an orthogonal space. If V is an orthogonal space, then we define $\det V \in k^\times/(k^\times)^2$ for the determinant of the matrix $(\langle e_i, e_j \rangle)_{1 \le i,j \le N}$, where $e_1, \dots, e_N$ is any k-basis of V. (It is easy to see that this is well-defined.) Similarly, we define $\mathrm{disc}\, V = (-1)^{N(N-1)/2} \det V \in k^\times/(k^\times)^2$.

If V is an orthogonal space and $U \subset V$ is an isotropic subspace (that is, $\langle x, y \rangle_V = 0$ for all $x, y \in U$), then $\dim U \le n$. If equality holds, we say that the orthogonal space V is split. It follows from [MH73, Ch. III, §1] that if V, W are split orthogonal spaces of dimension N and $\mathrm{disc}\, V = \mathrm{disc}\, W$, then $V \cong W$.

An example of a split orthogonal space is the space V_0 with basis

$$e_{-n}, \dots, e_{-1}, e_0, e_1, \dots, e_n, \tag{2.1}$$

the pairing being defined by the formula $\langle e_i, e_{-j}\rangle = \delta_{ij}$. Then $\operatorname{disc} V_0 = 1$. If $T : V_0 \to V_0$ is a linear operator, then we write $T^* : V_0 \to V_0$ for its adjoint, defined by the formula $\langle Tv, w\rangle = \langle v, T^*w\rangle$ for all $v, w \in V_0$. We also consider the group

$$\mathrm{SO}(V_0) = \{g \in \mathrm{SL}(V_0) \mid gg^* = 1\}. \tag{2.2}$$

The group $\mathrm{SO}(V_0)$ acts by conjugation on $W_0 = \{T \in \mathrm{End}(V_0) \mid T = T^*\}$, the space of self-adjoint linear transformations of V_0. The characteristic polynomial of an element $T \in W_0$ is an invariant of its $\mathrm{SO}(V_0)$-orbit. In what follows, we will be interested in the set of $\mathrm{SO}(V_0)$-orbits in W_0 with fixed characteristic polynomial f, $\Delta(f) \neq 0$.

Lemma 2.2. *Let $f \in k[x]$ be a monic polynomial of degree $N = 2n + 1$ and of non-zero discriminant $\Delta(f) \neq 0$. Then the following two sets are in canonical bijection:*

1. *The set of $\mathrm{SO}(V_0)$-orbits in W_0 with characteristic polynomial f.*
2. *The set of isomorphism classes of pairs (V, T), where V is a split orthogonal space of dimension N and discriminant 1, and $T \in \mathrm{End}_k(V)$ is a self-adjoint linear operator with characteristic polynomial f. (By definition, an isomorphism $(V, T) \to (V', T')$ is an isomorphism $V \to V'$ that intertwines T and T'.)*

Proof. We define maps in each direction which are mutually inverse. Since V_0 is split, there is an obvious map from the set of orbits in W_0 to the set of isomorphism classes of pairs (V, T). Conversely, given (V, T), we can find an isomorphism $f : V \to V_0$ of orthogonal spaces, and then $f \circ T \circ f^{-1} \in W_0$. If $h : V \to V_0$ is another isomorphism, then $h \circ T \circ h^{-1}$ differs from $f \circ T \circ f^{-1}$ by the action of an element of

$$\mathrm{O}(V_0) = \{g \in \mathrm{GL}(V_0) \mid gg^* = 1\}.$$

Since N is odd, we have $\mathrm{O}(V_0) = \mathrm{SO}(V_0) \times \{\pm 1\}$, and $\{\pm 1\}$ acts trivially on W_0. In particular, the $\mathrm{O}(V_0)$-orbits in W_0 are the same as the $\mathrm{SO}(V_0)$-orbits. This completes the proof. □

2.2 An orbit problem over A_f

Let $A = k[x]$. If $f \in A$ is a monic polynoimal of degree $N = 2n + 1$, then we write $A_f = A/(f)$ for the quotient ring, a finite k-algebra.

Definition 2.3. *An orthogonal A-module of dimension N is a pair $(\mathcal{V}, \langle\cdot,\cdot\rangle)$, where:*

1. *$\mathcal{V}$ is a cyclic A-module, of dimension N as a k-vector space.*
2. *$\langle\cdot,\cdot\rangle : \mathcal{V} \times \mathcal{V} \to A_f$ is a non-degenerate symmetric A-bilinear pairing.*

A morphism $(\mathcal{V}, \langle\cdot,\cdot\rangle_{\mathcal{V}}) \to (\mathcal{W}, \langle\cdot,\cdot\rangle_{\mathcal{W}})$ of orthogonal A-modules is an A-linear map $\varphi : \mathcal{V} \to \mathcal{W}$ such that for all $x, y \in \mathcal{V}$, $\langle\varphi(x), \varphi(y)\rangle_{\mathcal{W}} = \langle x, y\rangle_{\mathcal{V}}$.

We call the polynomial $f \in A$ such that $\mathcal{V} \cong A_f$ as A-modules the characteristic polynomial of $\mathcal{V}$. When the pairing is clear from the context we drop it from the notation and simply refer to $\mathcal{V}$ as an orthogonal A-module. If $\mathcal{V}$ is an orthogonal A-module, then we define $\det \mathcal{V} = \langle v_0, v_0\rangle \in A_f^\times/(A_f^\times)^2$, where $v_0 \in \mathcal{A}$ is any choice of generator as A-module. (It is easy to see that this is well-defined.)

Lemma 2.4. *The assignment $\mathcal{V} \mapsto \det \mathcal{V}$ gives a bijection between the set of isomorphism classes of orthogonal A-modules with characteristic polynomial f and the group $A_f^\times/(A_f^\times)^2$.*

Proof. Given $U \in A_f^\times$, define an orthogonal A-module $\mathcal{V}_U$ by the pair $(A_f, \langle\cdot,\cdot\rangle_U)$, where $\langle x, y\rangle_U = Uxy$. Then $\det \mathcal{V}_U = U \bmod (A_f^\times)^2$. This shows that the map $\mathcal{V} \mapsto \det \mathcal{V}$ is surjective.

We now show that it is injective. Suppose that $\mathcal{V}$, $\mathcal{W}$ are orthogonal A-modules with $\det \mathcal{V} = \det \mathcal{W}$. Choose cyclic vectors $v_0 \in \mathcal{V}$, $w_0 \in \mathcal{W}$. After replacing w_0 by an $A_f^\times$-multiple, we can assume that $\langle v_0, v_0\rangle_{\mathcal{V}} = \langle w_0, w_0\rangle_{\mathcal{W}}$. The map $f : \mathcal{V} \to \mathcal{W}$ defined by $v_0 \mapsto w_0$ is then an isomorphism of orthogonal A-modules. □

2.3 Classification of orbits

Let $f \in k[x]$ be a monic polynomial of degree $N = 2n+1$, and suppose that $\Delta(f) \neq 0$.

Proposition 2.5. *The following sets are in canonical bijection.*

1. *The set of isomorphism classes of pairs (V, T), where V is an orthogonal space and $T \in \mathrm{End}_k(V)$ is a self-adjoint linear transformation with characteristic polynomial f.*
2. *The set of isomorphism classes of orthogonal A-modules $\mathcal{V}$ with characteristic polynomial f.*

If V and $\mathcal{V}$ correspond under this bijection, then we have $\mathrm{disc}\, V = \mathbb{N}_{A_f/k} \det \mathcal{V}$ in $k^\times/(k^\times)^2$.

Proposition 2.5 will follow immediately from Lemma 2.6 and Lemma 2.7 below. The k-vector space A_f has a canonical basis, given by the images of the elements $1, x, \ldots, x^{2n}$, and we write $\tau : A_f \to k$ for the element of the dual basis with $\tau(x^{2n}) = 1$.

Lemma 2.6. *Let $\mathcal{V}$ be an orthogonal A-module with characteristic polynomial f, and let V be the orthogonal space with underlying k-vector space $\mathcal{V}$, and $\langle \cdot, \cdot \rangle_V = \tau \circ \langle \cdot, \cdot \rangle_{\mathcal{V}}$.*

1. *We have $\mathrm{disc}\, V = \mathbb{N}_{A_f/k} \det \mathcal{V} \in k^\times/(k^\times)^2$.*
2. *Let $T \in \mathrm{End}_k(V)$ be multiplication by $x \in A$. Then T is a self-adjoint linear operator with characteristic polynomial f.*

Proof. 1. Fix a cyclic vector $v_0 \in \mathcal{V}$. A k-basis of V is then $v_0, xv_0, \ldots, x^{2n}v_0$. We prove the equality $\det\langle x^i v_0, x^j v_0 \rangle_V = (-1)^n \mathbb{N}_{A_f/k} \langle v_0, v_0 \rangle_{\mathcal{V}}$ in $k^\times$, which will imply the first part of the lemma. Suppose first that $\langle v_0, v_0 \rangle_{\mathcal{V}} = 1$. Then the matrix $\langle x^i v_0, x^j v_0 \rangle_V = \tau(x^{i+j})$ has 0's above the anti-diagonal, and 1's on the anti-diagonal, so has determinant $(-1)^n$, giving the desired equality in this case. In general, after making a separable extension of k we can suppose that there exists $\alpha \in A_f^\times$ such that $\alpha^2 = \langle v_0, v_0 \rangle_{\mathcal{V}}$. We then have

$$\det\langle x^i v_0, x^j v_0 \rangle_V = \det\langle x^i \alpha^{-1} v_0, x^j \alpha^{-1} v_0 \rangle_V \cdot \mathbb{N}_{A_f/k}(\alpha)^2 = (-1)^n \mathbb{N}_{A_f/k} \langle v_0, v_0 \rangle_{\mathcal{V}},$$

as required.

2. Immediate.

□

Lemma 2.7. *Let V be an orthogonal space, and let $T \in \mathrm{End}_k(V)$ be a self-adjoint linear operator with characteristic polynomial f. Let $\mathcal{V}$ be the A_f-module with underlying k-vector space V, and the action of $x \in A$ given by T. Then A_f-module $\mathcal{V}$ admits a unique structure of orthogonal A-module such that $\langle x, y \rangle_V = \tau \langle x, y \rangle_{\mathcal{V}}$.*

Proof. Choose a cyclic vector $v_0 \in \mathcal{V}$. There exists a unique element $\alpha \in A_f$ such that $\langle x^i v_0, v_0 \rangle_V = \tau \alpha x^i$ for each $i = 0, \ldots, N-1$. We make $\mathcal{V}$ into an orthogonal A-module by defining $\langle v_0, v_0 \rangle_{\mathcal{V}} = \alpha$. To finish the proof of the lemma, it suffices to show the equality

$$\langle x^i v_0, x^j v_0 \rangle_V = \tau \langle x^i v_0, x^j v_0 \rangle_{\mathcal{V}} = \tau x^{i+j} \alpha$$

for each $0 \leq i, j \leq N-1$. We can write $x^{i+j} = \sum_{m=0}^{N-1} c_m x^m \in A_f$ for unique scalars $c_m \in k$; we then have

$$\langle x^i v_0, x^j v_0 \rangle_V = \langle x^{i+j} v_0, v_0 \rangle_V = \sum_{m=0}^{N-1} c_m \langle x^m v_0, v_0 \rangle_V = \sum_{m=0}^{N-1} c_m \tau \alpha x^m = \tau \alpha x^{i+j}.$$

This completes the proof. □

3 Hyperelliptic curves and 2-descent

Let k be a field of characteristic 0, and let $f \in k[x]$ be a monic polynomial of degree $N = 2n + 1 \geq 5$. Suppose that $\Delta(f) \neq 0$. We write C_f^0 for the smooth affine curve over k which is given by the equation $y^2 = f$, and C_f for its smooth projective completion. We write $J_f = \operatorname{Jac} C_f = \operatorname{Pic}^0 C_f$ for the Jacobian of this hyperelliptic curve of genus n. We write $\pi : C_f \to \mathbb{P}^1$ for the branched double covering given by the x co-ordinate, and $P_\infty \in C_f(k)$ for the unique point above $x = \infty$. Then P_∞ is a Weierstrass point, fixed by the hyperelliptic involution $\iota : C_f \to C_f$ which sends y to $-y$.

Associated to C_f is the Kummer exact sequence (of smooth k-groups):

$$0 \longrightarrow J_f[2] \longrightarrow J_f \xrightarrow{[2]} J_f \longrightarrow 0 \tag{3.1}$$

Taking the long exact sequence in cohomology, we obtain an injective homomorphism $\delta : J_f(k)/2J_f(k) \hookrightarrow H^1(k, J_f[2])$. This Galois cohomology group can be computed explicitly using the following result.

Proposition 3.1. *There is an isomorphism $J_f[2] \cong (\operatorname{Res}_{A_f/k} \mu_2)/\mu_2$ of finite k-groups.*

Proof. See [Sch95, §2]. □

Because $N = \deg f$ is odd, the exact sequence

$$0 \longrightarrow \mu_2 \longrightarrow \operatorname{Res}_{A_f/k} \mu_2 \longrightarrow (\operatorname{Res}_{A_f/k} \mu_2)/\mu_2 \longrightarrow 0 \tag{3.2}$$

is split. Hilbert's Theorem 90 then allows us to compute $H^1(k, J_f[2]) \cong H^1(k, (\operatorname{Res}_{A_f/k} \mu_2)/\mu_2)$, leading us to identify the map δ with a homomorphism

$$\delta : J_f(k)/2J_f(k) \hookrightarrow A_f^\times / k^\times (A_f^\times)^2. \tag{3.3}$$

We now discuss a concrete way to represent elements of the group $J_f(k)$.

Lemma 3.2. *Every line bundle $\mathcal{L}$ on C_f of degree 0 is isomorphic to a unique bundle of the form $\mathcal{O}(D - mP_\infty)$ for some $0 \leq m \leq n$, where D is an effective divisor satisfying the following condition. Extending scalars to an algebraic closure k^s/k, we can write $D = \sum_{i=1}^m P_i$ with $P_i \in C_f(k^s)$. Then:*

1. *If $1 \leq i \leq m$ then $P_i \neq P_\infty$.*
2. *If $1 \leq i < j \leq m$ then $P_i \neq \iota P_j$.*

Proof. Let $m \geq 0$ be the smallest integer such that $H^0(C_f, \mathcal{L}(mP_\infty)) \neq 0$. By Riemann-Roch, we have $m \leq n$, and $H^0(C_f, \mathcal{L}(mP_\infty))$ contains a unique non-zero section s, up to scalar. The divisor of zeroes of s now has the desired properties. □

We now introduce the Mumford representation of divisors on the curve C_f, cf. [Mum07, Ch. IIIa, §2]. Let $0 \leq m \leq n$ be an integer, and suppose given polynomials $U, V, R \in k[x]$ satisfying the following conditions:

1. we have $\deg U = m$, $\deg V = 2n + 1 - m$, and $\deg R \leq m - 1$;
2. the polynomials U and V are monic;
3. and we have the relation $f = UV - R^2$.

(If $m = 0$, then we interpret the first condition as $R = 0$.) Then the effective divisor $D \subset C_f^0$ cut out by the equations $U = 0$, $y = R$ satisfies the conclusions of Lemma 3.2, and we associate to the triple (U, V, R) the degree 0 line bundle $\mathcal{L} = \mathcal{O}(D - mP_\infty)$ on C_f. Conversely, every degree 0 line bundle admits such an expression:

Proposition 3.3. *The assignment $(U, V, R) \mapsto \mathcal{L}$ defines a bijection between the set of tuples of polynomials $U, V, R \in k[x]$ satisfying the conditions 1–3 above and the set of isomorphim classes of degree 0 line bundles on C_f (i.e. the set $J_f(k)$).*

Proof. See [Mum07, Ch. IIIa, §2]. If $\mathcal{L} = \mathcal{O}(D - mP_\infty)$, where $D = \sum_{i=1}^m P_i$ is a divisor satisfying the conclusion of Lemma 3.2, then we define $U = \prod_{i=1}^m (x - x(P_i))$. If the $x(P_i)$ are distinct, then we define R to be the unique polynomial satisfying $R(x(P_i)) = y(P_i)$. In this case, $f - R^2$ is divisible by U, and this in turn determines V. If the $x(P_i)$ are not distinct, then the definition of R is slightly more involved, and we do not describe the details here. □

The inverse assignment $\mathcal{L} \mapsto (U, V, R)$ is what we call the Mumford representation of the line bundle $\mathcal{L}$. We can use it to calculate the image of $\mathcal{L}$ under the 2-descent map (3.3):

Lemma 3.4. *Let $\mathcal{L}$ be a degree 0 line bundle on C_f, representing a point $[\mathcal{L}] \in J_f(k)$, and let (U, V, R) be its Mumford representation. Factor $U = U_0 U_1$ in $k[x]$, where U_0 divides f and U_1 is prime to f. Then $\delta([\mathcal{L}]) = U_1(U_0 - f/U_0)$ mod $k^\times (A_f^\times)^2$.*

Proof. This follows easily from [Sch95, Lemma 2.2]. □

4 Orbits and the arithmetic of hyperelliptic curves

Let k be a field of characteristic 0, let $f \in k[x]$ be a polynomial of odd degree $N = 2n + 1 \geq 5$ and of non-vanishing discriminant $\Delta(f) \neq 0$, and let C_f be the associated hyperelliptic curve. We write $j : \mathcal{W} \hookrightarrow C_f$ for the closed subscheme supported on the $2n + 1$ branch points of the map $\pi : C_f \to \mathbb{P}^1$ not equal to P_∞. Thus $\mathcal{W}$ is in fact contained inside $C_f^0 = \operatorname{Spec} k[x, y]/(y^2 - f)$, where it is defined by the equation $y = 0$. There is a canonical isomorphism $\mathcal{W} \cong \operatorname{Spec} A_f$.

Let $\mathcal{L}$ be a line bundle on C_f of degree 0. We fix a choice of isomorphism $\mathcal{L} \otimes_{\mathcal{O}} \iota^* \mathcal{L} \cong \mathcal{O}$. Since $\iota j = j$, there is a canonical isomorphism $j^* \iota^* \mathcal{L} \cong j^* \mathcal{L}$, and we get an induced bilinear pairing $j^* \mathcal{L} \times j^* \mathcal{L} \to \mathcal{O}_{\mathcal{W}}$. We set $\mathcal{V} = H^0(\mathcal{W}, j^* \mathcal{L})$, and write $\langle \cdot, \cdot \rangle_{\mathcal{V}} : \mathcal{V} \times \mathcal{V} \to A_f$ for the symmetric bilinear pairing we obtain after taking global sections.

Lemma 4.1. *The space $\mathcal{V}$ is an orthogonal A-module with characteristic polynomial f. Moreover, the image of $\det \mathcal{V}$ in $A_f^\times / k^\times (A_f^\times)^2$ is independent of the choice of trivialization of $\mathcal{L} \otimes_{\mathcal{O}} \iota^* \mathcal{L}$.*

Proof. We must show that $\mathcal{V}$ is a free A_f-module of rank 1, and that the pairing $\langle \cdot, \cdot \rangle_{\mathcal{V}}$ is non-degenerate. The first assertion is immediate, since $j^* \mathcal{L}$ is a locally free sheaf of rank 1 and $\mathcal{W}$ is affine. For similar reasons, we see that $\langle \cdot, \cdot \rangle_{\mathcal{V}}$ is non-degenerate. Changing the trivialization changes $\det \mathcal{V}$ by a $k^\times$-multiple, which is therefore trivial in the group $A_f^\times / k^\times (A_f^\times)^2$. □

We now compute $\mathcal{V}$ explicitly. Suppose that $\mathcal{L} = \mathcal{O}(mP_\infty - D)$, where D is an effective divisor satisfying the conditions of Lemma 3.2, and let (U, V, R) be the associated Mumford representation of $\mathcal{L}^{\otimes -1} = \mathcal{O}(D - mP_\infty)$. (If $W \subset C_f$ is a Zariski open, then the non-zero sections of $\mathcal{L}$ over W are the functions $g \in k(C_f)^\times$ satisfying

$$(g) + mP_\infty - D \geq 0$$

in W.) We have $\mathcal{L} \otimes \iota^* \mathcal{L} \cong \mathcal{O}(2mP_\infty - D - \iota^* D)$. The function $U \in k(C_f)^\times$ satisfies $(U) = D + \iota^* D - 2mP_\infty$, and thus defines a choice of trivialization of $\mathcal{O}(2mP_\infty - D - \iota^* D)$. With this choice, the pairing $\mathcal{L} \times \iota^* \mathcal{L} \to \mathcal{O}_{C_f}$ sends a pair (g_1, g_2) to $g_1 g_2 / U$. It follows that the pairing $\mathcal{V} \times \mathcal{V} \to A_f$ can be computed as follows: given $v_1, v_2 \in \mathcal{V}$, choose functions $g_1, g_2 \in k(C_f)$ such that $g_i - D \geq 0$ on $\mathcal{W}$ and $j^* g_i = v_i$. Then the function $g_1 g_2 / U \in k(C_f)$ is regular in a neighborhood of $\mathcal{W}$, and we define $\langle v_1, v_2 \rangle_{\mathcal{V}} = g_1 g_2 / U \bmod y \in A_f$.

Lemma 4.2. *With notation as above, factor $U = U_0 U_1$, where U_0 divides f and U_1 is prime to f. Then $\det \mathcal{V} = U_1(U_0 - f/U_0)$ mod $k^\times (A_f^\times)^2$.*

Proof. The function $y - U_0$ generates $\mathcal{L}$ in a Zariski open neighborhood of $\mathcal{W}$, so its image in $\mathcal{V}$ is a cyclic vector. We calculate

$$\det \mathcal{V} = \langle y - U_0, y - U_0 \rangle_{\mathcal{V}} = \frac{(y - U_0)(-y - U_0)}{U} = \frac{U_0^2 - f}{U} \equiv U_1(U_0 - f/U_0) \bmod k^\times (A_f^\times)^2,$$

as desired. □

Comparing Lemma 4.2 with Lemma 3.4, we immediately obtain:

Corollary 4.3. *The induced map $\delta' : J_f(k) \to A_f^\times / k^\times (A_f^\times)^2$, $\mathcal{L} \mapsto \det \mathcal{V}$ mod $k^\times (A_f^\times)^2$, agrees with the Kummer homomorphism (3.3).*

Lemma 4.4. *Suppose that $\mathcal{L} = \mathcal{O}(mP_\infty - D)$ is a degree 0 line bundle on C_f, where D is an effective divisor satisfying the conditions of Lemma 3.2, and let (U, V, R) be the Mumford representation of $\mathcal{L}^{\otimes -1} = \mathcal{O}(D - mP_\infty)$. Then:*

1. *The functions U, $y - R$ lie in $H^0(C_f^0, \mathcal{L})$, and the set*

$$\mathcal{B} = \left\{U, xU, \ldots, x^{\deg V - 1}U, (y - R), x(y - R), \ldots, x^{\deg U - 1}(y - R)\right\} \subset H^0(C_f^0, \mathcal{L})$$

   projects to a basis of $\mathcal{V}$ as k-vector space.

2. *Let V denote the orthogonal space associated to the orthogonal A-module $\mathcal{V}$ (cf. Lemma 2.6). Then V is split.*

Proof. 1. We first note that $H^0(C_f^0, \mathcal{L})$ is a free A-module of rank 2, a basis being given by the elements $U, y - R$. (We write $A = k[x]$.) Indeed, $H^0(C_f^0, \mathcal{L})$ is generated as an $A[y]$-module by these elements, and we have the relations

$$yU = RU + U(y - R) \text{ and } y(y - R) = VU - R(y - R). \tag{4.1}$$

It follows that $\mathcal{V}$ is isomorphic as A-module to A^2/yA^2, where y acts by the matrix

$$\begin{pmatrix} R & V \\ U & -R \end{pmatrix}.$$

The dimension of $\mathcal{V}$ is equal to the cardinality of $\mathcal{B}$, so it suffices to show that $\mathcal{B}$ spans $\mathcal{V}$ over k. However, this is immediate from the relations (4.1).

2. Let $a = \lfloor \deg U/2 \rfloor$ and $b = \lfloor \deg V/2 \rfloor$. Then $a + b = n$ and we define $\mathcal{U} \subset V$ to be the k-vector subspace spanned by the elements $U, \ldots, x^{b-1}U$ and $(y - R), \ldots, x^{a-1}(y - R)$. We claim that $\mathcal{U}$ is isotropic with respect to the pairing $\langle v, w \rangle_V = \tau \langle v, w \rangle_{\mathcal{V}}$. This follows immediately on recalling that $\tau : A_f \to k$ takes a polynomial to the coefficient of x^{2n}, and noting that $\langle x^i U, x^j U \rangle_{\mathcal{V}} = x^{i+j}U$, $\langle x^i U, x^j (y - R) \rangle_{\mathcal{V}} = -x^{i+j}R$, and $\langle x^i (y - R), x^j (y - R) \rangle_{\mathcal{V}} = -x^{i+j}V$.

□

Example 4.5. *Suppose that $\mathcal{L} = \mathcal{O}_{C_f}$ is the trivial line bundle. Then $\mathcal{V} = A_f$, and $\langle v_1, v_2 \rangle_V = \tau v_1 v_2$. We recover in this way the distinguished orbit of [BG12a, §5].*

Theorem 4.6. *Let k be a field of characteristic 0, and let $f \in k[x]$ be a monic polynomial of odd degree $N = 2n + 1 \geq 5$ of non-zero discriminant $\Delta(f) \neq 0$. Let C_f denote the associated hyperelliptic curve over k, let J_f be its Jacobian, and let V_0 be the orthogonal space (2.1). Then there is a canonical injection from $J_f(k)/2J_f(k)$ to the set of $\mathrm{SO}(V_0)$-orbits on the space W_0 with characteristic polynomial f.*

Proof. Let $\mathcal{L}$ be a degree 0 line bundle representing a point of $J_f(k)$. We recall our constructions so far:

1. In this section, we have associated to $\mathcal{L}$ an orthogonal space $(\mathcal{V}, \langle \cdot, \cdot \rangle_{\mathcal{V}})$ with $\delta'([\mathcal{L}]) = \det \mathcal{V} = \delta([\mathcal{L}])$ in $A_f^\times / k^\times (A_f^\times)^2$. Since N is odd, we can assume after replacing $\langle \cdot, \cdot \rangle_{\mathcal{V}}$ by a $k^\times$-multiple that $\mathbb{N}_{A_f/k} \det \mathcal{V} = 1$.

2. By Lemma 2.6, the orthogonal A-module $\mathcal{V}$ determines an orthogonal space where V with $\operatorname{disc} V = \mathbb{N}_{A_f/k} \det \mathcal{V} = 1$, and equipped with a self-adjoint linear operator $T \in \operatorname{End}_k(V)$ with characteristic polynomial f. Moreover, V is split (by Lemma 4.4).

3. By Lemma 2.2, the pair (V, T) determines a $\mathrm{SO}(V_0)$-orbit in W_0 with characteristic polynomial f.

It follows from Corollary 4.3 and Proposition 2.5 that the composite map induces an injection from the group $J_f(k)/2J_f(k)$ to the set of orbits in W_0 with characteristic polynomial f. This completes the proof. □

References

[BG12a] Manjul Bhargava and Benedict H. Gross. Arithmetic invariant theory. Available at `http://arxiv.org/abs/1206.4774`, 2012.

[BG12b] Manjul Bhargava and Benedict H. Gross. The average size of the 2-Selmer group of Jacobians of hyperelliptic curves having a rational Weierstrass point. Available at `http://www.math.harvard.edu/~gross/preprints/stable23.pdf`, 2012.

[MH73] John Milnor and Dale Husemoller. *Symmetric bilinear forms*. Springer-Verlag, New York, 1973. Ergebnisse der Mathematik und ihrer Grenzgebiete, Band 73.

[Mum07] David Mumford. *Tata lectures on theta. II.* Modern Birkhäuser Classics. Birkhäuser Boston Inc., Boston, MA, 2007. Jacobian theta functions and differential equations, With the collaboration of C. Musili, M. Nori, E. Previato, M. Stillman and H. Umemura, Reprint of the 1984 original.

[Ngô99] Báo Châu Ngô. Faisceaux pervers, homomorphisme de changement de base et lemme fondamental de Jacquet et Ye. *Ann. Sci. École Norm. Sup. (4)*, 32(5):619–679, 1999.

[Sch95] Edward F. Schaefer. 2-descent on the Jacobians of hyperelliptic curves. *J. Number Theory*, 51(2):219–232, 1995.

[Tho13] Jack A. Thorne. Vinberg's representations and arithmetic invariant theory. *Algebra Number Theory*, 7(9):2331–2368, 2013.

[Tho14] Jack A. Thorne. On the 2-selmer groups of plane quartic curves with a marked point. Available at `http://www.dpmms.cam.ac.uk/~jat58/`, 2014.