Max-Planck-Institut für Mathematik
Bonn

Division by 2 on odd degree hyperelliptic curves and their jacobians

by

Yuri G. Zarhin

Max-Planck-Institut für Mathematik
Preprint Series 2018 (31)

Division by 2 on odd degree hyperelliptic curves and their jacobians

Yuri G. Zarhin

Max-Planck-Institut für Mathematik
Vivatsgasse 7
53111 Bonn
Germany

Pennsylvania State University
Department of Mathematics
University Park, PA 16802
USA

MPIM 18-31

DIVISION BY 2 ON ODD DEGREE HYPERELLIPTIC CURVES AND THEIR JACOBIANS

YURI G. ZARHIN

Abstract. Let K be an algebraically closed field of characteristic different from 2, g a positive integer, $f(x)$ a degree $(2g+1)$ polynomial with coefficients in K and without multiple roots, $\mathcal{C} : y^2 = f(x)$ the corresponding genus g hyperelliptic curve over K and J the jacobian of $\mathcal{C}$. We identify $\mathcal{C}$ with the image of its canonical embedding into J (the infinite point of $\mathcal{C}$ goes to the identity element of J). It is well known that for each $\mathfrak{b} \in J(K)$ there are exactly 2^{2g} elements $\mathfrak{a} \in J(K)$ such that $2\mathfrak{a} = \mathfrak{b}$. M. Stoll constructed an *algorithm* that provides Mumford representations of all such $\mathfrak{a}$ in terms of the Mumford representation of $\mathfrak{b}$. The aim of this paper is to give *explicit formulas* for Mumford representations of all such $\mathfrak{a}$ when $\mathfrak{b} \in J(K)$ is given by $P = (a, b) \in \mathcal{C}(K) \subset J(K)$ in terms of coordinates a, b. We also prove that if $g > 1$ then $\mathcal{C}(K)$ does *not* contain torsion points with order between 3 and $2g$.

1. Introduction

Let K be an algebraically closed field of characteristic different from 2. If n and i are positive integers and $\mathbf{r} = \{r_1, \dots, r_n\}$ is a sequence of n elements $r_i \in K$ then we write

$$\mathbf{s}_i(\mathbf{r}) = \mathbf{s}_i(r_1, \dots, r_n) \in K$$

for the ith basic symmetric function in $r_1, \dots, r_n$. If we put $r_{n+1} = 0$ then $\mathbf{s}_i(r_1, \dots, r_n) = \mathbf{s}_i(r_1, \dots, r_n, r_{n+1})$.

Let $g \ge 1$ be an integer. Let $\mathcal{C}$ be the smooth projective model of the smooth affine plane K-curve

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

where $\alpha_1, \dots, \alpha_{2g+1}$ are *distinct* elements of K. It is well known that $\mathcal{C}$ is a genus g hyperelliptic curve over K with precisely one *infinite* point, which we denote by ∞. In other words,

$$\mathcal{C}(K) = \{(a, b) \in K^2 \mid b^2 = \prod_{i=1}^{2g+1} (a - \alpha_i)\} \bigsqcup \{\infty\}.$$

Clearly, x and y are nonconstant rational functions on $\mathcal{C}$, whose only pole is ∞. More precisely, the polar divisor of x is $2(\infty)$ and the polar divisor of y is $(2g+1)(\infty)$.

2010 *Mathematics Subject Classification.* 14H40, 14G27, 11G10.

Key words and phrases. Hyperelliptic curves, jacobians, Mumford representations.

Partially supported by Simons Foundation Collaboration grant # 585711.

I've started to write this paper during my stay in May-June 2016 at the Max-Planck-Institut für Mathematik (Bonn, Germany) and finished it during my next visit to the Institute in May-July 2018. The MPIM hospitality and support are gratefully acknowledged.

The zero divisor of y is $\sum_{i=1}^{2g+1}(\mathfrak{W}_i)$ where

$$\mathfrak{W}_i=(\alpha_i,0)\in\mathcal{C}(K) \text{ for all } i=1,\dots,2g,2g+1.$$

We write ι for the hyperelliptic involution

$$\iota:\mathcal{C}\to\mathcal{C},(x,y)\mapsto(x,-y),\ \infty\mapsto\infty.$$

The set of fixed points of ι consists of ∞ and all $\mathfrak{W}_i$. It is well known that for each $P\in\mathcal{C}(K)$ the divisor $(P)+\iota(P)-2(\infty)$ is principal. More precisely, if $P=(a,b)\in\mathcal{C}(K)$ then $(P)+\iota(P)-2(\infty)$ is the divisor of the rational function $x-a$ on C. If D is a divisor on $\mathcal{C}$ then we write $\mathrm{supp}(D)$ for its *support*, which is a finite subset of $\mathcal{C}(K)$.

We write J for the jacobian of $\mathcal{C}$, which is a g-dimensional abelian variety over K. If D is a degree zero divisor on $\mathcal{C}$ then we write $\mathrm{cl}(D)$ for its linear equivalence class, which is viewed as an element of $J(K)$. Elements of $J(K)$ may be described in terms of so called **Mumford representations** (see [5, Sect. 3.12], [13, Sect. 13.2, pp. 411–415, especially, Prop. 13.4, Th. 13.5 and Th. 13.7] and Section 2 below.)

We will identify $\mathcal{C}$ with its image in J with respect to the canonical regular map $\mathcal{C}\hookrightarrow J$ under which ∞ goes to the identity element of J. In other words, a point $P\in\mathcal{C}(K)$ is identified with $\mathrm{cl}((P)-(\infty))\in J(K)$. Then the action of ι on $\mathcal{C}(K)\subset J(K)$ coincides with multiplication by -1 on $J(K)$. In particular, the list of points of order 2 on $\mathcal{C}$ consists of all $\mathfrak{W}_i$.

Since K is algebraically closed, the commutative group $J(K)$ is divisible. It is well known that for each $\mathfrak{b}\in J(K)$ there are exactly 2^{2g} elements $\mathfrak{a}=\frac{1}{2}\mathfrak{b}\in J(K)$ such that $2\mathfrak{a}=\mathfrak{b}$. M. Stoll [8, Sect. 5] constructed an *algorithm* that provides Mumford representations of all such $\mathfrak{a}$ in terms of the Mumford representation of $\mathfrak{b}$. The aim of this paper is to give *explicit formulas* (Theorem 3.2) for Mumford representations of all $\frac{1}{2}\mathfrak{b}$ when $\mathfrak{b}\in J(K)$ is given by

$$P=(a,b)\in\mathcal{C}(K)\subset J(K)$$

on $\mathcal{C}$ in terms of its coordinates $a,b\in K$. (Here $b^2=f(a)$.)

The paper is organized as follows. In Section 2 we recall basic facts about Mumford representations and obtain auxiliary results about divisors on hyperelliptic curves. In particular, we prove (Theorem 2.5) that if $g>1$ then the only point of $\mathcal{C}(K)$ that is divisible by two in the *theta divisor* Θ of J (rather than in $J(K)$) is ∞. We also prove that $\mathcal{C}(K)$ does *not* contain points of order n if $3\le n\le 2g$. In addition, we discuss torsion points on certain natural subvarieties of Θ when J has "large monodromy". In Section 3 we describe explicitly for a given $P=(a,b)\in\mathcal{C}(K)$ the Mumford representation of 2^{2g} divisor classes $\mathrm{cl}(D-g(\infty))$ such that D is an effective degree g reduced divisor on $\mathcal{C}$ and

$$2\mathrm{cl}(D-g(\infty))=P\in\mathcal{C}(K)\subset J(K).$$

The description is given in terms of collections of square roots $r_i=\sqrt{a-\alpha_i}$ ($1\le i\le 2g+1$), whose product $\prod_{i=1}^{2g+1}r_i$ is $-b$. (There are exactly 2^{2g} choices of such collections of square roots.)

This paper is a follow up of [1] where the (more elementary) case of elliptic curves is discussed. (See also [11, 14].)

Acknowledgements. I am grateful to Bjorn Poonen and Michael Stoll for useful comments.

2. Divisors on hyperelliptic curves

Recall [13, Sect. 13.2, p. 411] that if D is an effective divisor of (nonnegative) degree m, whose support does *not* contain ∞, then the degree zero divisor $D-m(\infty)$ is called *semi-reduced* if it enjoys the following properties.

- If $\mathfrak{W}_i$ lies in $\mathrm{supp}(D)$ then it appears in D with multiplicity 1.
- If a point Q of $\mathcal{C}(K)$ lies in $\mathrm{supp}(D)$ and does not coincide with any of $\mathfrak{W}_i$ then $\iota(Q)$ does *not* lie in $\mathrm{supp}(D)$.

If, in addition, $m \le g$ then $D - m(\infty)$ is called *reduced*.

It is known ([5, Ch. 3a], [13, Sect. 13.2, Prop. 3.6 on p. 413]) that for each $\mathfrak{a} \in J(K)$ there exist *exactly one* nonnegative m and (effective) degree m divisor D such that the degree zero divisor $D - m(\infty)$ is *reduced* and $\mathrm{cl}(D - m(\infty)) = \mathfrak{a}$. (E.g., the zero divisor with $m = 0$ corresponds to $\mathfrak{a} = 0$.) If

$$m \ge 1,\ D = \sum_{j=1}^{m} (Q_j) \text{ where } Q_j = (a_j, b_j) \in \mathcal{C}(K) \quad \text{for all} \quad j = 1, \dots, m$$

(here Q_j do *not* have to be distinct) then the corresponding

$$\mathfrak{a} = \mathrm{cl}(D - m(\infty)) = \sum_{j=1}^{m} Q_j \in J(K).$$

The *Mumford representation* ([5, Sect. 3.12], [13, Sect. 13.2, pp. 411–415, especially, Prop. 13.4, Th. 13.5 and Th. 13.7] of $\mathfrak{a} \in J(K)$ is the pair $(U(x), V(x))$ of polynomials $U(x), V(x) \in K[x]$ such that

$$U(x) = \prod_{j=1}^{m} (x - a_j)$$

is a degree m monic polynomial while $V(x)$ has degree $< m = \deg(U)$, the polynomial $V(x)^2 - f(x)$ is divisible by $U(x)$, and each Q_j is a zero of $y - V(x)$, i.e.,

$$b_j = V(a_j),\ Q_j = (a_j, V(a_j)) \in \mathcal{C}(K) \quad \text{for all} \quad j = 1, \dots m.$$

Such a pair always exists, is unique, and (as we have just seen) uniquely determines not only $\mathfrak{a}$ but also divisors D and $D - m(\infty)$.

Examples 2.1. The case $\mathfrak{a} = 0$ corresponds to $m = 0, D = 0$ and the pair $(U(x) = 1, V(x) = 0)$.

The case

$$\mathfrak{a} = P = (a, b) \in \mathcal{C}(K) \subset J(K)$$

corresponds to $m = 1, D = (P)$ and the pair $(U(x) = x - a, V(x) = b)$.

Conversely, if $U(x)$ is a monic polynomial of degree $m \le g$ and $V(x)$ a polynomial such that $\deg(V) < \deg(U)$ and $V(x)^2 - f(x)$ is divisible by $U(x)$ then there exists exactly one $\mathfrak{a} = \mathrm{cl}(D - m(\infty))$ where $D - m(\infty)$ is a reduced divisor such that $(U(x), V(x))$ is the Mumford representation of $\mathrm{cl}(D - m(\infty))$.

Let $P = (a, b) \in \mathcal{C}(K)$, i.e.,

$$a, b \in K,\ b^2 = f(a) = \prod_{i=1}^{n} (a - \alpha_i).$$

Recall that our goal is to divide explicitly P by 2 in $J(K)$, i.e., to give explicit formulas for the *Mumford representation* of *all* 2^{2g} divisor classes $\mathrm{cl}(D - g(\infty))$ such that $2D + \iota(P)$ is linearly equivalent to $(2g + 1)\infty$.

The following assertion is a simple but useful exercise in Riemann-Roch spaces (see Example 4.13 in [7]).

Lemma 2.2. *Let D be an effective divisor on $\mathcal{C}$ of degree $m > 0$ such that $m \le 2g+1$ and $\mathrm{supp}(D)$ does not contain ∞. Assume that the divisor $D - m(\infty)$ is principal.*

(1) *Suppose that m is odd. Then:*
   (i) *$m = 2g + 1$ and there exists exactly one polynomial $v(x) \in K[x]$ such that the divisor of $y-v(x)$ coincides with $D-(2g+1)(\infty)$. In addition, $\deg(v) \le g$.*
   (ii) *If $\mathfrak{W}_i$ lies in $\mathrm{supp}(D)$ then it appears in D with multiplicity 1.*
   (iii) *If b is a nonzero element of K and $P = (a, b) \in \mathcal{C}(K)$ lies in $\mathrm{supp}(D)$ then $\iota(P) = (a, -b)$ does not lie in $\mathrm{supp}(D)$.*

(2) *Suppose that $m = 2d$ is even. Then there exists exactly one monic degree d polynomial $u(x) \in K[x]$ such that the divisor of $u(x)$ coincides with $D - m(\infty)$. In particular, every point $Q \in \mathcal{C}(K)$ appears in $D - m(\infty)$ with the same multiplicity as $\iota(Q)$.*

Proof. Let h be a rational function on $\mathcal{C}$, whose divisor coincides with $D - m(\infty)$. Since ∞ is the only pole of h, the function h is a polynomial in x, y and therefore may be presented as $h = s(x)y - v(x)$ with $s, v \in K[x]$. If $s = 0$ then h has at ∞ the pole of even order $2\deg(v)$ and therefore $m = 2\deg(v)$.

Suppose that $s \ne 0$. Clearly, $s(x)y$ has at ∞ the pole of odd order $2\deg(s) + (2g+1) \ge (2g+1)$. So, the orders of the pole for $s(x)y$ and $v(x)$ are distinct, because they have different parity and therefore the order m of the pole of $h = s(x)y - v(x)$ coincides with $\max(2\deg(s) + (2g + 1), 2\deg(v)) \ge 2g + 1$. This implies that $m = 2g + 1$; in particular, m is odd. It follows that m is *even* if and only if $s(x) = 0$, i.e., $h = -v(x)$; in addition, $\deg(v) \le (2g+1)/2$, i.e., $\deg(v) \le g$. In order to finish the proof of (2), it suffices to divide $-v(x)$ by its leading coefficient and denote the ratio by $u(x)$. (The uniqueness of monic $u(x)$ is obvious.)

Let us prove (1). Since m is *odd*,

$$m = 2\deg(s) + (2g + 1) > 2\deg(v).$$

Since $m \le 2g + 1$, we obtain that $\deg(s) = 0$, i.e., s is a nonzero element of K and $2\deg(v) < 2g + 1$. The latter inequality means that $\deg(v) \le g$. Dividing h by the constant s, we may and will assume that $s = 1$ and therefore $h = y - v(x)$ with

$$v(x) \in K[x], \ \deg(v) \le g.$$

This proves (i). (The uniqueness of v is obvious.) The assertion (ii) is contained in Proposition 13.2(b) on pp. 409-10 of [13]. In order to prove (iii), we just follow arguments on p. 410 of [13] (where it is actually proven). Notice that our $P = (a, b)$ is a zero of $y - v(x)$, i.e. $b - v(a) = 0$. Since, $b \ne 0$, $v(a) = b \ne 0$ and $y - v(x)$ takes on at $\iota(P) = (a, -b)$ the value $-b - v(a) = -2b \ne 0$. This implies that $\iota(P)$ is *not* a zero of $y - v(x)$, i.e., $\iota(P)$ does not lie in $\mathrm{supp}(D)$. $\square$

Remark 2.3. Lemma 2.2(1)(ii,iii) asserts that if m is odd the divisor $D - m(\infty)$ is *semi-reduced*. See [13, the penultimate paragraph on p. 411].

Corollary 2.4. *Let $P = (a, b)$ be a K-point on $\mathcal{C}$ and D an effective divisor on $\mathcal{C}$ such that $m = \deg(D) \le g$ and $\mathrm{supp}(D)$ does not contain ∞. Suppose that the degree zero divisor $2D + \iota(P) - (2m+1)(\infty)$ is principal. Then:*

(i) *$m = g$ and there exists a polynomial $v_D(x) \in K[x]$ such that $\deg(v_D) \le g$ and the divisor of $y - v_D(x)$ coincides with $2D + \iota(P) - (2g+1)(\infty)$. In particular, $-b = v_D(a)$.*

(ii) *If a point Q lies in $\mathrm{supp}(D)$ then $\iota(Q)$ does not lie in $\mathrm{supp}(D)$. In particular,*
   (1) *none of $\mathfrak{W}_i$ lies in $\mathrm{supp}(D)$;*
   (2) *$D - g(\infty)$ is reduced.*

(iii) *The point P does not lie in $\mathrm{supp}(D)$.*

Proof. One has only to apply Lemma 2.2 to the divisor $2D + \iota(P)$ of *odd* degree $2m+1 \le 2g+1$ and notice that $\iota(P) = (a, -b)$ is a zero of $y - v(x)$ while $\iota(\mathfrak{W}_i) = \mathfrak{W}_i$ for all $i = 1, \dots, 2g+1$. $\square$

Let $d \le g$ be a positive integer and $\Theta_d \subset J$ be the image of the regular map

$$\mathcal{C}^d \to J, \ (Q_1, \dots, Q_d) \mapsto \sum_{i=1}^{d} Q_i \subset J.$$

It is well known that Θ_d is an irreducible closed d-dimensional subvariety of J that coincides with $\mathcal{C}$ for $d = 1$ and with J if $d = g$; in addition, $\Theta_d \subset \Theta_{d+1}$ for all $d < g$. Clearly, each Θ_d is stable under multiplication by -1 in J. We write Θ for the $(g-1)$-dimensional *theta divisor* Θ_{g-1}.

Theorem 2.5. *Suppose that $g > 1$ and let*

$$\mathcal{C}_{1/2} := 2^{-1}\mathcal{C} \subset J$$

be the preimage of $\mathcal{C}$ with respect to multiplication by 2 in J. Then the intersection of $\mathcal{C}_{1/2}(K)$ and Θ consists of points of order dividing 2 on J. In particular, the intersection of $\mathcal{C}$ and $C_{1/2}$ consists of ∞ and all $\mathfrak{W}_i$'s.

Remark 2.6. The case $g = 2$ of Theorem 2.5 was done in [2, Prop. 1.5]

Proof of Theorem 2.5. Suppose that $m \le g - 1$ is a positive integer and we have m (not necessarily distinct) points $Q_1, \dots Q_m$ of $\mathcal{C}(K)$ and a point $P \in \mathcal{C}(K)$ such that in $J(K)$

$$2\sum_{j=1}^{m} Q_j = P.$$

We need to prove that $P = \infty$, i.e., it is the zero of group law in J and therefore $\sum_{j=1}^{m} Q_j$ is an element of order 2 (or 1) in $J(K)$. Suppose that this is not true. Decreasing m if necessary, we may and will assume that none of Q_j is ∞ (but m is still positive and does not exceed $g - 1$). Let us consider the effective degree m divisor $D = \sum_{j=1}^{m}(Q_j)$ on $\mathcal{C}$. The equality in J means that the divisors $2[D - m(\infty)]$ and $(P) - (\infty)$ on $\mathcal{C}$ are linearly equivalent. This means that the divisor $2D + (\iota(P)) - (2m+1)(\infty)$ is *principal*. Now Corollary 2.4 tells us that $m = g$, which is not the case. The obtained contradiction proves that the intersection of $\mathcal{C}_{1/2}$ and Θ consists of points of order 2 and 1.

Since $g > 1$, $\mathcal{C} \subset \Theta$ and therefore the intersection of $\mathcal{C}$ and $\mathcal{C}_{1/2}$ also consists of points of order 2 or 1, i.e., lies in the union of ∞ and all $\mathfrak{W}_i$'s. Conversely, since each $\mathfrak{W}_i$ has order 2 in $J(K)$ and ∞ has order 1, they all lie in $\mathcal{C}_{1/2}$ (and, of course, in $\mathcal{C}$). $\square$

Remark 2.7. It is known [12, Ch. VI, last paragraph of Sect. 11, p. 122] that the curve $\mathcal{C}_{1/2}$ is irreducible. (Its projectiveness and smoothness follow readily from the projectiveness and smoothness of $\mathcal{C}$ and the étaleness of multiplication by 2 in J.) See [4] for an explicit description of equations that cut out $\mathcal{C}_{1/2}$ in a projective space.

Corollary 2.8. *Suppose that $g > 1$. Let m be an integer such that $3 \le m \le 2g$. Then $\mathcal{C}(K)$ does not contain a point of order m in $J(K)$. In particular, $\mathcal{C}(K)$ does not contain points of order 3 or 4.*

Remark 2.9. The case $g = 2$ of Corollary 2.8 was done in [2, Prop. 2.1]

Proof of Corollay 2.8. Suppose that such a point say, P does exists. Clearly, P is neither ∞ nor one of $\mathfrak{W}_i$, i.e., $P \ne \iota(P)$. Let us consider the effective degree m divisor $D = m(P)$. Then the divisor $D - m(\infty)$ is principal and its support contains P but does *not* contain $\iota(P)$.

If m is odd then the desired result follows from Lemma 2.2(1). Assume that m is even. By Lemma 2.2(2), the support of $D - m(\infty)$ must contain $\iota(P)$, since it contains P. This gives us a contradiction that ends the proof. $\square$

Example 2.10. Let us assume that $\mathrm{char}(K)$ does *not* divide $(2g + 1)$. Then for every nonzero $b \in K$ the monic degree $(2g+1)$ polynomial $x^{2g+1}+b^2$ has no multiple roots and the point $P = (0, b)$ of the genus g hyperelliptic curve

$$\mathcal{C} : y^2 = x^{2g+1} + b^2$$

has order $(2g + 1)$ on the jacobian J of $\mathcal{C}$. Indeed, the polar divisor of rational function $y - b$ is $(2g + 1)(\infty)$ while P is its only *zero*. Since the degree of $\mathrm{div}(y - b)$ is 0,

$$\mathrm{div}(y - b) = (2g + 1)(P) - (2g + 1)(\infty) = (2g + 1)((P) - (\infty)).$$

This means that the K-point

$$P \in \mathcal{C}(K) \subset J(K)$$

has finite order m that divides $2g + 1$. Clearly, m is neither 1 nor 2 (since $P \ne \infty$ and $y(P) = b \ne 0$), i.e., $m \ge 3$. If $m < (2g + 1)$ then $m \le 2g$ and we get a contradiction to Corollary 2.8. This proves that the order of P is $(2g + 1)$.

Notice that odd degree genus 2 hyperelliptic curves with points of order $5 = 2 \times 2 + 1$ are classified in [3].

Remark 2.11. If $\mathrm{char}(K) = 0$ and $g > 1$ then the famous theorem of M. Raynaud (conjectured by Yu.I. Manin and D. Mumford) asserts that an arbitrary genus g smooth projective curve over K embedded into its jacobian contains only finitely many torsion points [9].

The aim of the rest of this section is to obtain an information about torsion points on certain subvarieties Θ_d when $\mathcal{C}$ has "large monodromy". Let us start with the following assertion.

Theorem 2.12. *Suppose that $g > 1$ and let N and k be positive integers such that*

$$1 < N, \ N + k \le 2g.$$

Let us put

$$d_{(N+k)} = \left[\frac{2g}{N+k}\right].$$

Let K_0 be a subfield of K such that $f(x) \in K_0[x]$. Let $\mathfrak{a} \in J(K)$ lies on $\Theta_{d_{(N+k)}}$. Suppose that there exists a collection of k (not necessarily distinct) field automorphisms

$$\{\sigma_1, \dots, \sigma_k\} \subset \mathrm{Aut}(K/K_0)$$

such that $\sum_{l=1}^{k} \sigma_l(\mathfrak{a}) = N\mathfrak{a}$ or $-N\mathfrak{a}$. Then $\mathfrak{a}$ has order 1 or 2 in $J(K)$.

Proof. Clearly,

$$d_{(N+k)} \le \frac{2g}{N+k} \le \frac{2g}{2+1} < g; \ (N+k) \cdot d_{(N+k)} \le 2g < 2g+1.$$

Let us assume that $2\mathfrak{a} \ne 0$ in $J(K)$. We need to arrive to a contradiction. There is a positive integer $r \le d_{(N+k)}$ and a sequence of points $P_1, \dots, P_r$ of $\mathcal{C}(K) \setminus \{\infty\}$ such that $\tilde{D} := \sum_{j=1}^{r}(P_j) - r(\infty)$ is the Mumford representation of $\mathfrak{a}$ while (say) P_1 does not coincides with any of W_i (here we use the assumption that $2\mathfrak{a} \ne 0$); we may also assume that P_1 has the largest *multiplicity* in $\tilde{D}$ say, M among $\{P_1, \dots, P_r\}$. (In particular, none of P_j's coincides with ιP_1.) Then $\sigma_l(\tilde{D}) = \sum_{j=1}^{r}(\sigma_l P_j) - r(\infty)$ is the Mumford representation of $\sigma_l\mathfrak{a}$ for all $l \in \{1, \dots, k\}$. In particular, the multiplicity of each $\sigma_l P_j$ in $\sigma_l(\tilde{D})$ does *not* exceed M; similarly, the multiplicity of each $\iota\sigma_l P_j$ in $\iota\sigma_l(\tilde{D})$ also does *not* exceed M for every l. This implies that if P is any point of $C(K) \setminus \{\infty\}$ that does *not* lie in the support of $\tilde{D}$ then its multiplicity in $N\tilde{D} + \iota\left(\sum_{l=1}^{k} \sigma_l(\tilde{D})\right)$ is a nonnegative integer that does *not* exceed kM; in addition, the multiplicity of P in $N\tilde{D} + \sum_{l=1}^{k} \sigma_l(\tilde{D})$ is also a nonnegative integer that also does *not* exceed kM. Notice also that P_1 lies in the supports of both $N\tilde{D} + \iota\left(\sum_{l=1}^{k} \sigma_l(\tilde{D})\right)$ and $N\tilde{D} + \iota\left(\sum_{l=1}^{k} \sigma_l(\tilde{D})\right)$ and its multiplicities (in both cases) are, at least, NM.

Suppose that $\sum_{l=1}^{k} \sigma_l(\mathfrak{a}) = N\mathfrak{a}$. Then the divisor

$$N\tilde{D} + \iota\left(\sum_{l=1}^{k} \sigma_l(\tilde{D})\right) = N\left(\sum_{j=1}^{r}(P_j)\right) + \sum_{l=1}^{k}\left(\sum_{j=1}^{r}(\iota\sigma_l P_j)\right) - r(N+k)(\infty)$$

is a *principal divisor* on $\mathcal{C}$. Since

$$m := r(N+k) \le (N+k) \cdot d_{(N+k)} \le 2g < 2g+1,$$

we are in position to apply Lemma 2.2, which tells us right away that m is *even* and there is a monic polynomial $u(x)$ of degree $m/2$, whose divisor coincides with $N\tilde{D} + \iota\sum_{l=1}^{k} \sigma_l(\tilde{D})$. This implies that any point $Q \in \mathcal{C}(K) \setminus \{\infty\}$ appears in $N\tilde{D} + \iota\left(\sum_{l=1}^{k} \sigma_l(\tilde{D})\right)$ with the same (nonnegative) multiplicity as ιQ. It follows that $Q = \iota P_1$ appears in $N\tilde{D} + \iota\left(\sum_{l=1}^{k} \sigma_l(\tilde{D})\right)$ with the same multiplicity as P_1. On the other hand, since ιP_1 does not appear in $N\tilde{D}$, its multiplicity in $\tilde{D} + \iota\sum_{l=1}^{k} \sigma_l(\tilde{D})$ does *not* exceed kM. Since the multiplicity of P_1 in $N\tilde{D} + \iota\left(\sum_{l=1}^{k} \sigma_l(\tilde{D})\right)$ is, at least, NM, we conclude that $NM \le kM$, which is not the case, since $k < N$. This gives us the desired contradiction.

If $\sum_{l=1}^{k}\sigma_l(\mathfrak{a}) = -N\mathfrak{a}$ then literally the same arguments applied to the principal divisor

$$N\tilde{D}+\sum_{l=1}^{k}\sigma_l(\tilde{D}) = N\left(\sum_{j=1}^{r}(P_j)\right)+\sum_{l=1}^{k}\left(\sum_{j=1}^{r}(\sigma_l P_j)\right) - r(N+k)(\infty)$$

also lead to the contradiction. □

2.13. Let K_0 be a subfield of K such that $f(x)\in K_0[x]$ and $\bar{K}_0$ the algebraic closure of K_0 in K. We write $\mathrm{Gal}(K_0)$ for the absolute Galois group

$$\mathrm{Gal}(K_0) = \mathrm{Aut}(\bar{K}_0/K)$$

of K_0. It is well known that all torsion points of $J(K)$ actually lie in $J(\bar{K}_0)$.

Let us consider the following Galois properties of torsion points of $J(K)$.

(M3) If $\mathfrak{a}\in J(\bar{K}_0)$ has finite order that is a power of 2 then there exists $\sigma\in\mathrm{Gal}(K_0)$ such that $\sigma(a)=3\mathfrak{a}$.

(M2) If $\mathfrak{b}\in J(\bar{K}_0)$ has finite order that is odd then there exists $\tau\in\mathrm{Gal}(K_0)$ such that $\tau(\mathfrak{b})=2\mathfrak{b}$.

(M) Let $\mathfrak{a},\mathfrak{b}\in J(\bar{K}_0)$ be points of finite order such that the order of $\mathfrak{a}$ is a power of 2 and the order of $\mathfrak{b}$ is odd. Then there exist $\sigma_1,\sigma_2\in\mathrm{Gal}(K_0)$ such that

$$\sigma_1(\mathfrak{a})=-\mathfrak{a},\ \sigma_1(\mathfrak{b})=2\mathfrak{b};\ \sigma_2(\mathfrak{a})=5\mathfrak{a},\ \sigma_2(\mathfrak{b})=2\mathfrak{b}.$$

Theorem 2.14. (i) *Suppose that $g\ge 2$ and J enjoys the property (M3). Let us put*

$$d_{(4)}=[2g/4]=[g/2].$$

Let $\mathfrak{a}\in J(K)$ be a torsion point that lies on $\Theta_{d(4)}$.

If the order of $\mathfrak{a}$ is a power of 2 then it is either 1 or 2.

(ii) *Suppose that $g\ge 2$ and J enjoys the property (M2). Let us put*

$$d_{(3)}=[2g/3].$$

Let $\mathfrak{b}\in J(K)$ be a torsion point of odd order that lies on $\Theta_{d(3)}$.

Then $\mathfrak{b}$ is the identity element of J.

(iii) *Suppose that $g\ge 3$ and J enjoys the property (M). Let us put*

$$d_{(6)}=[2g/6]=[g/3].$$

Let $\mathfrak{c}\in J(K)$ be a torsion point that lies on $\Theta_{d(6)}$.

Then the order of $\mathfrak{c}$ is either 1 or 2.

Remark 2.15. In the case of $g=2$ an analogue of Theorem 2.14(i,ii) was earlier proven in [2, Cor. 1.6].

Proof of Theorem 2.14. Since all torsion points of $J(K)$ lie in $J(\bar{K}_0)$, we may assume that $K=\bar{K}_0$ and therefore $\mathrm{Gal}(K_0)=\mathrm{Aut}(K/K_0)$. In the first two cases the assertion follows readily from Theorem 2.12 with $N=3,k=1$ in the case (i) and with $N=2,k=1$ in the case (ii). Let us do the case (iii). We have $\mathfrak{c}=\mathfrak{a}+\mathfrak{b}$ where the order of $\mathfrak{b}$ is odd and the order of $\mathfrak{b}$ is a power of 2. There exist $\sigma_1,\sigma_2\in\mathrm{Gal}(K_0)=\mathrm{Aut}(K/K_0)$ such that

$$\sigma_1(\mathfrak{a})=-\mathfrak{a},\ \sigma_1(\mathfrak{b})=2\mathfrak{b};\ \sigma_2(\mathfrak{a})=5\mathfrak{a},\ \sigma_2(\mathfrak{b})=2\mathfrak{b}.$$

This implies that

$$\sigma_1(\mathfrak{c})+\sigma_2(\mathfrak{c})=\sigma_1(\mathfrak{a})+\sigma_1(\mathfrak{b})+\sigma_2(\mathfrak{a})+\sigma_2(\mathfrak{b})=-\mathfrak{a}+2\mathfrak{b}+5\mathfrak{a}+2\mathfrak{b}=4(\mathfrak{a}+\mathfrak{b})=4\mathfrak{c},$$

i.e., $\sigma_1(\mathfrak{c}) + \sigma_2(\mathfrak{c}) = 4\mathfrak{c}$. Now the desired result follows from Theorem 2.12 with $N = 4, k = 2$. □

Example 2.16. Suppose that $g > 1$ and K is the field $\mathbb{C}$ of complex numbers, $\{\alpha_1, \dots, \alpha_{2g+1}\}$ is a $(2g+1)$-element set of algebraically independent transendental complex numbers and $K_0 = \mathbb{Q}(\alpha_1, \dots, \alpha_{2g+1})$ where $\mathbb{Q}$ is the field of rational numbers.. It follows from results of B. Poonen and M. Stoll [6, Th. 7.1 and its proof] and J. Yelton [14, Th. 1.1 and Prop. 2.2] that the jacobian J of the *generic* hyperelliptic curve

$$\mathcal{C} : y^2 = \prod_{i=1}^{2g+1} (x - \alpha_i)$$

enjoys the following properties.

Let us choose odd integers $(2n_1 + 1)$ *and* $(2n_2 + 1)$ *and nonnegative integers* m_1 *and* m_2*. Suppose that* $\mathfrak{a}, \mathfrak{b} \in J(\bar{K}_0)$ *be points of finite order such that the order of* $\mathfrak{a}$ *is a power of* 2 *and the order of* $\mathfrak{b}$ *is odd. Then there exist* $\sigma_1, \sigma_2 \in \mathrm{Gal}(K_0)$ *such that*

$$\sigma_1(\mathfrak{a}) = (2n_1 + 1)\mathfrak{a},\ \sigma_1(\mathfrak{b}) = 2^{m_1}\mathfrak{b};\ \sigma_2(\mathfrak{a}) = (2n_2 + 1)\mathfrak{a},\ \sigma_2(\mathfrak{b}) = 2^{m_2}\mathfrak{b}.$$

This implies that J enjoys the properties (M3), (M2) and (M). It follows from Theorem 2.14 that torsion points of $J(\mathbb{C})$ enjoy the following properties.

(i) Any torsion point $\mathfrak{a} \in J(\mathbb{C})$ that lies on $\Theta_{g/2}$ and has order that is a power of 2 actually has order 1 or 2.

(ii) Any torsion point $\mathfrak{b} \in J(\mathbb{C})$ of odd order that lies on $\Theta_{2g/3}$ coincides with the identity of J.

(iii) Let $g \geq 3$. Then any torsion point $\mathfrak{c} \in J(\mathbb{C})$ that lies on $\Theta_{g/3}$ has order 1 or 2.

Notice that B. Poonen and M. Stoll [6, Th. 7.1] proved that the only complex points of finite order in $J(\mathbb{C})$ that lie on $\mathcal{C} = \Theta_1$ are points of order 1 or 2. On the other hand, it is well known that J is a simple complex abelian variety. Now a theorem of Raynaud [10] implies that the set of torsion points on the theta divisor $\Theta = \Theta_{g-1}$ (actually, on every proper closed subvariety) of J is finite.

3. Division by 2

Suppose we are given a point

$$P = (a, b) \in \mathcal{C}(K) \subset J(K).$$

Since $\dim(J) = g$, there are exactly 2^{2g} points $\mathfrak{a} \in J(K)$ such that

$$P = 2\mathfrak{a} \in J(K).$$

Let us choose such an $\mathfrak{a}$. Then there is exactly one effective divisor

$$D = D(\mathfrak{a}) \tag{1}$$

of positive degree m on $\mathcal{C}$ such that $\mathrm{supp}(D)$ does *not* contain ∞, the divisor $D - m(\infty)$ is reduced, and

$$m \leq g,\ \mathrm{cl}(D - m(\infty)) = \mathfrak{a}.$$

It follows that the divisor $2D + (\iota(P)) - (2m+1)(\infty)$ is *principal* and, thanks to Corollary 2.4, $m = g$ and $\mathrm{supp}(D)$ does *not* contains any of $\mathfrak{W}_i$. (In addition, $D - g(\infty)$ is reduced.) Then the degree g effective divisor

$$D = D(\mathfrak{a}) = \sum_{j=1}^{g} (Q_j) \tag{2}$$

with $Q_i = (c_j, d_j) \in \mathcal{C}(K)$. Since none of Q_j coincides with any of $\mathfrak{W}_i$,

$$c_j \neq \alpha_i \ \forall i, j.$$

By Corollary 2.4, there is a polynomial $v_D(x)$ of degree $\leq g$ such that the degree zero divisor

$$2D + (\iota(P)) - (2g+1)(\infty)$$

is the divisor of $y - v_D(x)$. Since the points $\iota(P) = (a, -b)$ and all Q_j's are zeros of $y - v_D(x)$,

$$b = -v_D(a), \ d_j = v_D(c_j) \ \text{ for all } \ j = 1, \dots, g.$$

It follows from Proposition 13.2 on pp. 409–410 of [13] that

$$\prod_{i=1}^{2g+1} (x - \alpha_i) - v_D(x)^2 = f(x) - v_D(x)^2 = (x - a) \prod_{j=1}^{g} (x - c_j)^2. \tag{3}$$

In particular, $f(x) - v_D(x)^2$ is divisible by

$$u_D(x) := \prod_{j=1}^{g} (x - c_j). \tag{4}$$

Remark 3.1. Summing up:

$$D = D(\mathfrak{a}) = \sum_{j=1}^{g} (Q_j), \ Q_j = (c_j, v_D(c_j)) \ \text{ for all } \ j = 1, \dots, g$$

and the degree g monic polynomial $u_D(x) = \prod_{j=1}^{g} (x - c_j)$ divides $f(x) - v_D(x)^2$. Then (see see the beginning of Section 2) the pair (u_D, v_D) is the Mumford representation of $\mathfrak{a}$ if

$$\deg(v_D) < g = \deg(u_D).$$

This is not always the case: it may happen that $\deg(v_D) = g = \deg(u_D)$ (see below). However, if we replace $v_D(x)$ by its remainder with respect to the division by $u_D(x)$ then we get the Mumford representation of $\mathfrak{a}$ (see below).

If in (3) we put $x = \alpha_i$ then we get

$$-v_D(\alpha_i)^2 = (\alpha_i - a) \left(\prod_{j=1}^{g} (\alpha_i - c_j) \right)^2,$$

i.e.,

$$v_D(\alpha_i)^2 = (a - \alpha_i) \left(\prod_{j=1}^{g} (c_j - \alpha_i) \right)^2 \quad \text{for all } \ i = 1, \dots, 2g, 2g+1.$$

Since none of $c_j - \alpha_i$ vanishes, we may define

$$r_i = r_{i,D} := \frac{v_D(\alpha_i)}{\prod_{j=1}^{g} (c_j - \alpha_i)} = (-1)^g \frac{v_D(\alpha_i)}{u_D(\alpha_i)} \tag{5}$$

with

$$r_i^2 = a - \alpha_i \quad \text{for all} \quad i = 1, \dots, 2g+1 \tag{6}$$

and

$$\alpha_i = a - r_i^2, \ c_j - \alpha_i = r_i^2 - a + c_j \quad \text{for all} \quad i = 1, \dots, 2g, 2g+1; j = 1, \dots, g.$$

Clearly, all r_i's are *distinct* elements of K, because their squares are obviously distinct. (By the same token, $r_{j_1} \ne \pm r_{j_2}$ if $j_1 \ne j_2$.) Notice that

$$\prod_{i=1}^{2g+1} r_i = \pm b, \tag{7}$$

because

$$b^2 = \prod_{i=1}^{2g+1} (a - \alpha_i) = \prod_{i=1}^{2g+1} r_i^2.) \tag{8}$$

Now we get

$$r_i = \frac{v_D(a - r_i^2)}{\prod_{j=1}^{g}(r_i^2 - a + c_j)},$$

i.e.,

$$r_i \prod_{j=1}^{g}(r_i^2 - a + c_j) - v_D(a - r_i^2) = 0 \quad \text{for all} \quad i = 1, \dots 2g, 2g+1.$$

This means that the degree $(2g+1)$ *monic* polynomial (recall that $\deg(v_D) \le g$)

$$h_{\mathbf{r}}(t) := t \prod_{j=1}^{g}(t^2 - a + c_j) - v_D(a - t^2)$$

has $(2g+1)$ *distinct* roots $r_1, \dots, r_{2g+1}$. This means that

$$h_{\mathbf{r}}(t) = \prod_{i=1}^{2g+1} (t - r_i).$$

Clearly, $t \prod_{j=1}^{g}(t^2 - a + c_j)$ coincides with the *odd part* of $h_{\mathbf{r}}(t)$ while $-v_D(a - t^2)$ coincides with the *even part* of $h_{\mathbf{r}}(t)$. In particular, if we put $t = 0$ then we get

$$(-1)^{2g+1} \prod_{i=1}^{2g+1} r_i = -v_D(a) = b,$$

i.e.,

$$\prod_{i=1}^{2g+1} r_i = -b. \tag{9}$$

Hereafter

$$\mathbf{r} = \mathbf{r}_D := (r_1, \dots, r_{2g+1}) \in K^{2g+1}.$$

Since

$$\mathbf{s}_i(\mathbf{r}) = \mathbf{s}_i(r_1, \dots, r_{2g+1})$$

is the ith basic symmetric function in $r_1, \dots, r_{2g+1}$,

$$h_{\mathbf{r}}(t) = t^{2g+1} + \sum_{i=1}^{2g+1} (-1)^i \mathbf{s}_i(\mathbf{r}) t^{2g+1-i} = \left[t^{2g+1} + \sum_{i=1}^{2g} (-1)^i \mathbf{s}_i(\mathbf{r}) t^{2g+1-i} \right] + b.$$

(Since

$$\mathbf{s}_{2g+1}(\mathbf{r}) = \prod_{i=1}^{2g+1} r_i = -b,$$

the constant term of $h_{\mathbf{r}}(t)$ equals b.) Then

$$t\prod_{j=1}^{g}(t^2 - a + c_j) = t^{2g+1} + \sum_{j=1}^{g}\mathbf{s}_{2j}(\mathbf{r})t^{2g+1-2j},$$

$$-v_D(a-t^2) = \left[-\sum_{j=1}^{g}\mathbf{s}_{2j-1}(\mathbf{r})t^{2g-2j+2}\right] + b.$$

It follows that

$$\prod_{j=1}^{g}(t - a + c_j) = t^g + \sum_{j=1}^{g}\mathbf{s}_{2j}(\mathbf{r})t^{g-j},$$

$$v_D(a-t) = \sum_{j=1}^{g}\mathbf{s}_{2j-1}(\mathbf{r})t^{g-j+1} - b.$$

This implies that

$$v_D(t) = \left[\sum_{j=1}^{g}\mathbf{s}_{2j-1}(\mathbf{r})(a-t)^{g-j+1}\right] - b. \tag{10}$$

It is also clear that if we consider the degree g monic polynomial

$$U_{\mathbf{r}}(t) := u_D(t) = \prod_{j=1}^{g}(t - c_j)$$

then

$$U_{\mathbf{r}}(t) = (-1)^g\left[(a-t)^g + \sum_{j=1}^{g}\mathbf{s}_{2j}(\mathbf{r})(a-t)^{g-j}\right]. \tag{11}$$

Recall that $\deg(v_D) \le g$ and notice that the coefficient of $v(x)$ at x^g is $(-1)^g\mathbf{s}_1(\mathbf{r})$. This implies that the polynomial

$$V_{\mathbf{r}}(t) := v_D(t) - (-1)^g\mathbf{s}_1(\mathbf{r})U_{\mathbf{r}}(t) =$$

$$\left[\sum_{j=1}^{g}\mathbf{s}_{2j-1}(\mathbf{r})(a-t)^{g-j+1}\right] - b - \mathbf{s}_1(\mathbf{r})\left[(a-t)^g + \sum_{j=1}^{g}\mathbf{s}_{2j}(\mathbf{r})(a-t)^{g-j}\right] =$$

$$\sum_{j=1}^{g}\left(\mathbf{s}_{2j+1}(\mathbf{r}) - \mathbf{s}_1(\mathbf{r})\mathbf{s}_{2j}(\mathbf{r})\right)(a-t)^{g-j} \tag{12}$$

has degree $< g$, i.e.,

$$\deg(V_{\mathbf{r}}) < \deg(U_{\mathbf{r}}) = g.$$

Clearly, $f(x) - V_{\mathbf{r}}(x)^2$ is still divisible by $U_{\mathbf{r}}(x)$, because $u_D(x) = U_{\mathbf{r}}(x)$ divides both $f(x) - v_D(x)^2$ and $v_D(x) - V_{\mathbf{r}}(x)$. On the other hand,

$$d_j = v_D(c_j) = V_{\mathbf{r}}(c_j) \text{ for all } j = 1, \dots g,$$

because $U_{\mathbf{r}}(x)$ divides $v_D(x) - V_{\mathbf{r}}(x)$ and vanishes at all c_j. Actually, $\{c_1, \dots, c_g\}$ is the list of all roots (with multiplicities) of $U_{\mathbf{r}}(x)$. So,

$$D = D(\mathfrak{a}) = \sum_{j=1}^{g} (Q_j), \ Q_j = (c_j, v_D(c_j)) = (c_j, V_{\mathbf{r}}(c_j)) \ \forall j = 1, \dots, g.$$

This implies (again via the beginning of Section 2) that the pair $(U_{\mathbf{r}}(x), V_{\mathbf{r}}(x))$ is the *Mumford representation* of $\mathrm{cl}(D - g(\infty)) = \mathfrak{a}$. So, the formulas (11) and (12) give us an explicit construction of ($D(\mathfrak{a})$ and) $\mathfrak{a}$ in terms of $\mathbf{r} = (r_1, \dots, r_{2g+1})$ for each of 2^{2g} choices of $\mathfrak{a}$ with $2\mathfrak{a} = P \in J(K)$. On the other hand, in light of (6)-(8), there is exactly the same number 2^{2g} of choices of collections of square roots $\sqrt{a - \alpha_i}$ $(1 \le i \le 2g)$ with product $-b$. Combining it with (9), we obtain that for each choice of square roots $\sqrt{a - \alpha_i}$'s with $\prod_{i=1}^{2g+1} \sqrt{a - \alpha_i} = -b$ there is precisely one $\mathfrak{a} \in J(K)$ with $2\mathfrak{a} = P$ such that the corresponding r_i defined by (5) coincides with chosen $\sqrt{a - \alpha_i}$ for all $i = 1, \dots, 2g + 1$, and the Mumford representation $(U_{\mathbf{r}}(x), V_{\mathbf{r}}(x))$ for this $\mathfrak{a}$ is given by formulas (11)-(12). This gives us the following assertion.

Theorem 3.2. *Let $P = (a, b) \in \mathcal{C}(K)$. Then the 2^{2g}-element set*

$$M_{1/2,P} := \{\mathfrak{a} \in J(K) \mid 2\mathfrak{a} = P \in \mathcal{C}(K) \subset J(K)\}$$

can be described as follows. Let $\mathfrak{R}_{1/2,P}$ be the set of all $(2g+1)$-tuples $\mathfrak{r} = (\mathfrak{r}_1, \dots, \mathfrak{r}_{2g+1})$ of elements of K such that

$$\mathfrak{r}_i^2 = a - \alpha_i \ \textit{ for all } \ i = 1, \dots, 2g, 2g+1; \ \prod_{i=1}^{2g+1} \mathfrak{r}_i = -b.$$

Let $\mathbf{s}_i(\mathfrak{r})$ be the ith basic symmetric function in $\mathfrak{r}_1, \dots, \mathfrak{r}_{2g+1}$. Let us put

$$U_{\mathfrak{r}}(x) = (-1)^g \left[(a - x)^g + \sum_{j=1}^{g} \mathbf{s}_{2j}(\mathfrak{r})(a - x)^{g-j} \right],$$

$$V_{\mathfrak{r}}(x) = \sum_{j=1}^{g} \left(\mathbf{s}_{2j+1}(\mathfrak{r}) - \mathbf{s}_1(\mathfrak{r})\mathbf{s}_{2j}(\mathfrak{r}) \right) (a - x)^{g-j}.$$

Then there is a natural bijection between $\mathfrak{R}_{1/2,P}$ and $M_{1/2,P}$ such that $\mathfrak{r} \in \mathfrak{R}_{1/2,P}$ corresponds to $\mathfrak{a}_{\mathfrak{r}} \in M_{1/2,P}$ with Mumford representation $(U_{\mathfrak{r}}, V_{\mathfrak{r}})$. More explicitly, if $\{c_1, \dots, c_g\}$ is the list of all g roots (with multiplicities) of $U_{\mathfrak{r}}(x)$ then $\mathfrak{r}$ corresponds to

$$\mathfrak{a}_{\mathfrak{r}} = \mathrm{cl}(D - g(\infty)) \in J(K), \ 2\mathfrak{a}_{\mathfrak{r}} = P$$

where the divisor

$$D = D(\mathfrak{a}_{\mathfrak{r}}) = \sum_{j=1}^{g} (Q_j), \ Q_j = (c_j, V_{\mathfrak{r}}(c_j)) \in \mathcal{C}(K) \ \textit{ for all } \ j = 1, \dots, g.$$

In addition, none of α_i is a root of $U_{\mathfrak{r}}(x)$ (i.e., the polynomials $U_{\mathfrak{r}}(x)$ and $f(x)$ are relatively prime) and

$$\mathfrak{r}_i = \mathbf{s}_1(\mathfrak{r}) + (-1)^g \frac{V_{\mathfrak{r}}(\alpha_i)}{U_{\mathfrak{r}}(\alpha_i)} \ \textit{ for all } \ i = 1, \dots, 2g, 2g+1.$$

Proof. Actually we have already proven all the assertions of Theorem 3.2 except the last formula for $\mathfrak{r}_i$. It follows from (4) and (5) that

$$\mathfrak{r}_i = (-1)^g \frac{v_{D(\mathfrak{a}_\mathfrak{r})}(\alpha_i)}{u_{D(\mathfrak{a}_\mathfrak{r})}(\alpha_i)} = (-1)^g \frac{v_{D(\mathfrak{a}_\mathfrak{r})}(\alpha_i)}{U_\mathfrak{r}(\alpha_i)}.$$

It follows from (12) that

$$v_{D(\mathfrak{a}_\mathfrak{r})}(x) = (-1)^g \mathbf{s}_1(\mathfrak{r}) U_\mathfrak{r}(x) + V_\mathfrak{r}(x).$$

This implies that

$$\mathfrak{r}_i = (-1)^g \frac{(-1)^g \mathbf{s}_1(\mathfrak{r}) U_\mathfrak{r}(\alpha_i) + V_\mathfrak{r}(\alpha_i)}{U_\mathfrak{r}(\alpha_i)} = \mathbf{s}_1(\mathfrak{r}) + (-1)^g \frac{V_\mathfrak{r}(\alpha_i)}{U_\mathfrak{r}(\alpha_i)}.$$

□

Corollary 3.3. *We keep the notation and assumptions of Theorem 3.2. Then*

$$2g \cdot \mathbf{s}_1(\mathfrak{r}) = (-1)^{g+1} \sum_{i=1}^{2g+1} \frac{V_\mathfrak{r}(\alpha_i)}{U_\mathfrak{r}(\alpha_i)}.$$

In particular, if $\mathrm{char}(K)$ *does not divide* g *then*

$$\mathbf{s}_1(\mathfrak{r}) = \frac{(-1)^{g+1}}{2g} \cdot \sum_{i=1}^{2g+1} \frac{V_\mathfrak{r}(\alpha_i)}{U_\mathfrak{r}(\alpha_i)}.$$

On the other hand, if $\mathrm{char}(K)$ *divides* g *then*

$$\sum_{i=1}^{2g+1} \frac{V_\mathfrak{r}(\alpha_i)}{U_\mathfrak{r}(\alpha_i)} = 0.$$

Proof. It follows from the last assertion of Theorem 3.2 that

$$\mathbf{s}_1(\mathfrak{r}) = \sum_{i=1}^{2g+1} \mathfrak{r}_i = \sum_{i=1}^{2g+1} \left(\mathbf{s}_1(\mathfrak{r}) + (-1)^g \frac{V_\mathfrak{r}(\alpha_i)}{U_\mathfrak{r}(\alpha_i)} \right) =$$

$$(2g+1)\mathbf{s}_1(\mathfrak{r}) + (-1)^g \sum_{i=1}^{2g+1} \frac{V_\mathfrak{r}(\alpha_i)}{U_\mathfrak{r}(\alpha_i)}.$$

This implies that

$$0 = 2g \cdot \mathbf{s}_1(\mathfrak{r}) + (-1)^g \sum_{i=1}^{2g+1} \frac{V_\mathfrak{r}(\alpha_i)}{U_\mathfrak{r}(\alpha_i)},$$

i.e.,

$$2g \cdot \mathbf{s}_1(\mathfrak{r}) = (-1)^{g+1} \sum_{i=1}^{2g+1} \frac{V_\mathfrak{r}(\alpha_i)}{U_\mathfrak{r}(\alpha_i)}.$$

□

Corollary 3.4. *We keep the notation and assumptions of Theorem 3.2. Let* i, l *be two distinct integers such that*

$$1 \le i, l \le 2g+1.$$

Then

$$\mathbf{s}_1(\mathfrak{r}) = \frac{(-1)^g}{2} \times \frac{\left(\alpha_l + \left(\frac{V_\mathfrak{r}(\alpha_l)}{U_\mathfrak{r}(\alpha_l)}\right)^2\right) - \left(\alpha_i + \left(\frac{V_\mathfrak{r}(\alpha_i)}{U_\mathfrak{r}(\alpha_i)}\right)^2\right)}{\left(\frac{V_\mathfrak{r}(\alpha_i)}{U_\mathfrak{r}(\alpha_i)} - \frac{V_\mathfrak{r}(\alpha_l)}{U_\mathfrak{r}(\alpha_l)}\right)}.$$

Proof. We have

$$\mathfrak{r}_i = \mathbf{s}_1(\mathfrak{r}) + (-1)^g \frac{V_\mathfrak{r}(\alpha_i)}{U_\mathfrak{r}(\alpha_i)},\ \mathfrak{r}_l = \mathbf{s}_1(\mathfrak{r}) + (-1)^g \frac{V_\mathfrak{r}(\alpha_l)}{U_\mathfrak{r}(\alpha_l)}.$$

Recall that

$$\mathfrak{r}_i^2 = a - \alpha_i \ne a - \alpha_l = \mathfrak{r}_l^2.$$

In particular,

$$\mathfrak{r}_i \ne \mathfrak{r}_l \text{ and therefore } \frac{V_\mathfrak{r}(\alpha_i)}{U_\mathfrak{r}(\alpha_i)} \ne \frac{V_\mathfrak{r}(\alpha_l)}{U_\mathfrak{r}(\alpha_l)}.$$

We have

$$\alpha_l - \alpha_i = (a - \alpha_i) - (a - \alpha_l) = \mathfrak{r}_i^2 - \mathfrak{r}_l^2 =$$

$$\left(\mathbf{s}_1(\mathfrak{r}) + (-1)^g \frac{V_\mathfrak{r}(\alpha_i)}{U_\mathfrak{r}(\alpha_i)}\right)^2 - \left(\mathbf{s}_1(\mathfrak{r}) + (-1)^g \frac{V_\mathfrak{r}(\alpha_l)}{U_\mathfrak{r}(\alpha_l)}\right)^2 =$$

$$(-1)^g \cdot 2 \cdot \mathbf{s}_1(\mathfrak{r}) \cdot \left(\frac{V_\mathfrak{r}(\alpha_i)}{U_\mathfrak{r}(\alpha_i)} - \frac{V_\mathfrak{r}(\alpha_l)}{U_\mathfrak{r}(\alpha_l)}\right) + \left(\frac{V_\mathfrak{r}(\alpha_i)}{U_\mathfrak{r}(\alpha_i)}\right)^2 - \left(\frac{V_\mathfrak{r}(\alpha_l)}{U_\mathfrak{r}(\alpha_l)}\right)^2.$$

This implies that

$$(-1)^g \cdot 2 \cdot \mathbf{s}_1(\mathfrak{r}) \cdot \left(\frac{V_\mathfrak{r}(\alpha_i)}{U_\mathfrak{r}(\alpha_i)} - \frac{V_\mathfrak{r}(\alpha_l)}{U_\mathfrak{r}(\alpha_l)}\right) = \left(\alpha_l + \left(\frac{V_\mathfrak{r}(\alpha_l)}{U_\mathfrak{r}(\alpha_l)}\right)^2\right) - \left(\alpha_i + \left(\frac{V_\mathfrak{r}(\alpha_i)}{U_\mathfrak{r}(\alpha_i)}\right)^2\right).$$

This means that

$$\mathbf{s}_1(\mathfrak{r}) = \frac{(-1)^g}{2} \times \frac{\left(\alpha_l + \left(\frac{V_\mathfrak{r}(\alpha_l)}{U_\mathfrak{r}(\alpha_l)}\right)^2\right) - \left(\alpha_i + \left(\frac{V_\mathfrak{r}(\alpha_i)}{U_\mathfrak{r}(\alpha_i)}\right)^2\right)}{\left(\frac{V_\mathfrak{r}(\alpha_i)}{U_\mathfrak{r}(\alpha_i)} - \frac{V_\mathfrak{r}(\alpha_l)}{U_\mathfrak{r}(\alpha_l)}\right)}.$$

□

Remark 3.5. Let $\mathfrak{r} = (\mathfrak{r}_1, \dots, \mathfrak{r}_{2g+1}) \in \mathfrak{R}_{1/2,P}$ with $P = (a, b)$. Then for all $i = 1, \dots, 2g, 2g+1$

$$(-\mathfrak{r}_i)^2 = \mathfrak{r}_i^2 = a - \alpha_i$$

and

$$\prod_{i=1}^{2g+1} (-\mathfrak{r}_i) = (-1)^{2g+1} \prod_{i=1}^{2g+1} \mathfrak{r}_i = -(-b) = b.$$

This means that

$$-\mathfrak{r} = (-\mathfrak{r}_1, \dots, -\mathfrak{r}_{2g+1}) \in \mathfrak{R}_{1/2,\iota(P)}$$

(recall that $\iota(P) = (a, -b)$). It follows from Theorem 3.2 that

$$U_{-\mathfrak{r}}(x) = U_\mathfrak{r}(x),\ V_{-\mathfrak{r}}(x) = -V_\mathfrak{r}(x)$$

and therefore $\mathfrak{a}_{-\mathfrak{r}} = -\mathfrak{a}_\mathfrak{r}$.

Remark 3.6. The last assertion of Theorem 3.2 combined with Corollary 3.4 allow us to reconstruct explicitly $\mathfrak{r} = (\mathfrak{r}_1, \dots, \mathfrak{r}_{2g+1})$ and $P = (a, b)$ if we are given the polynomials $U_\mathfrak{r}(x), V_\mathfrak{r}(x)$ (and, of course, $\{\alpha_1, \dots,\ \alpha_{2g+1}\}$).

Example 3.7. Let us take as $P = (a, b)$ the point $\mathfrak{W}_{2g+1} = (\alpha_{2g+1}, 0)$. Then $b = 0$ and $\mathfrak{r}_{2g+1} = 0$. We have $2g$ arbitrary independent choices of (nonzero) square roots $\mathfrak{r}_i = \sqrt{\alpha_{2g+1} - \alpha_i}$ with $1 \le i \le 2g$ (and always get an element of $\mathfrak{R}_{1/2,P}$). Now Theorem 3.2 gives us (if we put $a = \alpha_{2g+1}, b = 0$) all 2^{2g} points $\mathfrak{a}_{\mathfrak{r}}$ of order 4 in $J(K)$ with $2\mathfrak{a}_{\mathfrak{r}} = \mathfrak{W}_{2g+1}$. Namely, let s_i be the ith basic symmetric function in $(\mathfrak{r}_1, \dots, \mathfrak{r}_{2g})$. Then the Mumford representation $(U_{\mathfrak{r}}, V_{\mathfrak{r}})$ of $\mathfrak{a}_{\mathfrak{r}}$ is given by

$$U_{\mathfrak{r}}(x) = (-1)^g \left[(\alpha_{2g+1} - x)^g + \sum_{j=1}^{g} s_{2j} \cdot (\alpha_{2g+1} - x)^{g-j} \right],$$

$$V_{\mathfrak{r}}(x) = \sum_{j=1}^{g} (s_{2j+1} - s_1 s_{2j}) (\alpha_{2g+1} - x)^{g-j}.$$

In particular, if $\alpha_{2g+1} = 0$ then

$$\mathfrak{r}_i = \sqrt{-\alpha_i} \quad \text{for all } i = 1, \dots, 2g,$$

$$U_{\mathfrak{r}}(x) = x^g + \sum_{j=1}^{g} (-1)^j s_{2j} x^{g-j},$$

$$V_{\mathfrak{r}}(x) = \sum_{j=1}^{g} (s_{2j+1} - s_1 s_{2j}) (-x)^{g-j}.$$

References

[1] B.M. Bekker, Yu.G. Zarhin, *The divisibility by 2 of rational points on elliptic curves.* Algebra i Analiz **29:4** (2017), 196–239; St. Petersburg Math. J., to appear; arXiv:1702.02255 [math.NT].

[2] J. Boxall and D. Grant, *Examples of torsion points on genus two curves.* Tran. Amer. Math. Soc. **352** (2000), no. 10, 4533–4555.

[3] J. Boxall, D. Grant and F. Leprévost, *5-torsion points on curves of genus 2.* J. London Math. Soc. (2) **64** (2001), 29–43.

[4] N. Bruin and E.V. Flynn, *Towers of* 2*-covers of hyperelliptic curves.* Trans. Amer. Math. Soc. **357** (2005), no. 11, 4329–4347.

[5] D. Mumford, Tata Lectures on Theta. II. Progress in Math. **43**, Birkhäuser, Boston Basel Stutgart, 1984.

[6] B. Poonen and M. Stoll, *Most odd degree hyperelliptic curves have only one rational point.* Annals of Math. **180** (2014), Issue 3, 1137–1166.

[7] M. Stoll, *Arithmetic of Hyperelliptic Curves.* Available at Summer Semester 2014, University of Bayreuth. http://www.mathe2.uni-bayreuth.de/stoll/teaching/ArithHypKurven-SS2014/Skript-ArithHypCurves-pub-screen.pdf .

[8] M. Stoll, *Chabauty without the Mordell-Weil group.* In: Algorithmic and Experimental Methods in Algebra, Geometry, and Number Theory (G. Böckle, W. Decker, G. Malle, eds.), Springer-Verlag (2018), to appear; arXiv:1506.04286 [math.NT].

[9] M. Raynaud, *Courbes sur une variété abélienne et points de torsion.* Invent. Math. **71** (1983), no. 1, 207–233.

[10] M. Raynaud, *Sous-variétés sur une variété abélienne et points de torsion.* In: Arithmetic and Geometry (Shafarevich Festschrift) I, pp. 327–352. Progress in Math. **35** Birkhäuser, Boston Basel Stutgart, 1983.

[11] E. Schaefer, 2*-descent on the Jacobians of hyperelliptic curves.* J. Number Theory **51** (1995), no. 2, 219–232.

[12] J.-P. Serre, Algebraic groups and class fields. Graduate Texts in Math. **117**, Springer-Verlag, New York, 1988.

[13] L.C. Washington, Elliptic Curves: Number Theory and Cryptography. Second edition. Chapman & Hall/CRC Press, Boca Raton London New York, 2008.

[14] J. Yelton, *Images of 2-adic representations associated to hyperelliptic jacobians.* J. Number Theory **151** (2015), 7–17.

Pennsylvania State University, Department of Mathematics, University Park, PA 16802, USA

E-mail address: `zarhin@math.psu.edu`