Division by 2 on odd-degree hyperelliptic curves and their Jacobians

Yu. G. Zarhin

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

Keywords: hyperelliptic curves, Weierstrass points, Jacobians, torsion points.

In memory of V. A. Iskovskikh

§ 1. Introduction

Let $K$ be an algebraically closed field of characteristic different from 2. Let $g \geq 1$ be an integer. Let $C$ 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 $\alpha_1, \ldots, \alpha_{2g+1}$ are distinct elements of $K$. It is well known that $C$ is a hyperelliptic curve of genus $g$ over $K$ with precisely one infinite point, which we denote by $\infty$. In other words,

$$C(K) = \left\{ (a, b) \in K^2 \left| b^2 = \prod_{i=1}^{2g+1} (a - \alpha_i) \right. \right\} \sqcup \{\infty\}.$$

Partially supported by Simons Foundation Collaboration grant no. 585711. I started to write this paper during my stay at the Max-Planck-Institut für Mathematik (Bonn, Germany) in May–June 2016 and finished it during my next visit to the Institute in May–July 2018. The MPIM hospitality and support are gratefully acknowledged.

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

© 2019 Russian Academy of Sciences (DoM), London Mathematical Society, Turpion Ltd.
It is clear that \( x \) and \( y \) are non-constant rational functions on \( \mathcal{C} \) whose only pole is \( \infty \). More precisely, the polar divisor of \( x \) is \( 2(\infty) \) and the polar divisor of \( y \) is \( (2g + 1)(\infty) \). The zero divisor of \( y \) is \( \sum_{i=1}^{2g+1} (\mathfrak{M}_i) \), where \( \mathfrak{M}_i = (\alpha_i, 0) \in \mathcal{C}(K) \) for \( i = 1, \ldots, 2g, 2g + 1 \).

We write \( \iota \) for the hyperelliptic involution

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

The set of all fixed points of \( \iota \) consists of \( \infty \) and all the \( \mathfrak{M}_i \). It is well known that, for every point \( P \in \mathcal{C}(K) \), 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 \( \mathcal{C} \). Given a divisor \( D \) on \( \mathcal{C} \), we write \( \text{supp}(D) \) for its \textit{support}, which is a finite subset of \( \mathcal{C}(K) \).

We write \( J \) for the Jacobian of \( \mathcal{C} \), a \( g \)-dimensional Abelian variety over \( K \). Given a divisor \( D \) of degree 0 on \( \mathcal{C} \), we write \( \text{cl}(D) \) 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 \textit{Mumford representations} (see [1], Ch. 3a, § 1, [2], § 13.2, pp. 411–415, especially Proposition 13.4, Theorems 13.5 and 13.7, and § 2 below).

We will identify \( \mathcal{C} \) with its image in \( J \) under the canonical regular map \( \mathcal{C} \hookrightarrow J \) that sends \( \infty \) to the identity element of the group \( J(K) \). In other words, a point \( P \in \mathcal{C}(K) \) is identified with \( \text{cl}(P - (\infty)) \in J(K) \). Then the action of \( \iota \) 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 the whole of \( \mathfrak{M}_i \).

Since \( K \) is algebraically closed, the commutative group \( J(K) \) is divisible. It is well known that for each \( b \in J(K) \) there are exactly \( 2^{2g} \) elements \( a = (1/2)b \in J(K) \) such that \( 2a = b \). Stoll ([3], § 5) constructed an \textit{algorithm} for finding the Mumford representations of all such \( a \) in terms of the Mumford representation of \( b \).

The aim of our paper is to give \textit{explicit formulae} (Theorem 3.2) for the Mumford representations of all \((1/2)b\) when \( b \in J(K) \) is given by a point

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

on \( \mathcal{C} \), in terms of the coordinates \( a, b \in K \). (Here \( b^2 = f(a) \).) The case \( b = \infty = 0 \in J(K) \) boils down to the well-known description of points of order 2 on the Jacobian ([1], Ch. 3a, § 2): their Mumford representations can easily be represented explicitly (see Examples 2.1 below).

The paper is organized as follows. In § 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 \( \mathcal{C}(K) \) which is divisible by 2 in the \textit{theta divisor} \( \Theta \) of the Jacobian \( J \) (rather than in \( J(K) \)) is \( \infty \). We also prove (Theorem 2.8) that \( \mathcal{C}(K) \) does \textit{not} contain points of order \( n \) if \( 3 \leq n \leq 2g \). Moreover, we discuss torsion points on certain natural subvarieties of \( \Theta \) in the case when \( J \) has ‘large monodromy’. In § 3, given a point \( P = (a, b) \in \mathcal{C}(K) \), we explicitly describe (in Theorem 3.2) the Mumford representations of the \( 2^{2g} \)
divisor classes $\text{cl}(D - g(\infty))$ such that $D$ is an effective reduced divisor of degree $g\text{ on } C$ and

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

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

This paper is a follow-up of [4], where the (more elementary) case of elliptic curves is discussed. (See also [5], [6].)

I am grateful to Bjorn Poonen, Michael Stoll and Tatiana Bandman for useful comments. My special thanks go to the referee for a thoughtful reading of the manuscript.

§ 2. Divisors on hyperelliptic curves

As usual, a monic polynomial is a polynomial with leading coefficient 1.

Let $D$ be an effective divisor of (non-negative) degree $m$ on a curve $C$ such that the support of $D$ does not contain $\infty$. We recall ([2], §13.2, p.411) that the divisor $D - m(\infty)$ of degree zero is said to be semireduced if it enjoys the following properties.

1) If $W_i$ lies in $\text{supp}(D)$, then it appears in $D$ with multiplicity 1.
2) If a point $Q$ of $C(K)$ lies in $\text{supp}(D)$ and does not coincide with any of the $W_i$, then $\iota(Q)$ does not lie in $\text{supp}(D)$.

If, in addition, $m \leq g$, then $D - m(\infty)$ is said to be reduced.

We note that points of $C(K)$ not coinciding with any of the $W_i$, may appear in a (semi-)reduced divisor with multiplicities greater than 1.

It is known ([1], Ch. 3a, [2], § 13.2, Proposition 3.6, p.413) that for every $a \in J(K)$ one can find exactly one non-negative integer $m$ and an effective divisor $D$ of degree $m$ such that the divisor $D - m(\infty)$ of degree 0 is reduced and $\text{cl}(D - m(\infty)) = a$. For example, the zero divisor and $m = 0$ correspond to $a = 0$. If $m \geq 1$ and $D$ is of the form

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

(here the $Q_j$ need not be distinct), then the corresponding linear equivalence class is

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

The Mumford representation (see [1], Ch. 3a, § 1, [2], § 13.2, pp. 411–415, especially Proposition 13.4, Theorems 13.5 and 13.7) of the element $a \in J(K)$ is a pair $(U(x), V(x))$ of polynomials $U(x), V(x) \in K[x]$ with the following properties.

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

is a monic polynomial of degree $m$. 
2) The degree of $V(x)$ is strictly less than $m = \deg(U)$.
3) The polynomial $V(x)^2 - f(x)$ is divisible by $U(x)$.
4) Each point $Q_j$ is a zero of the rational function $y - V(x)$, that is,
   \[ b_j = V(a_j), \quad Q_j = (a_j, V(a_j)) \in \mathcal{C}(K) \quad \text{for all} \quad j = 1, \ldots, m. \]

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

**Examples 2.1.** (i) The case $a = 0$ corresponds to $m = 0, D = 0$ and the pair $(U(x) = 1, V(x) = 0)$.

(ii) The case 
   \[ a = P = (a, b) \in \mathcal{C}(K) \subset J(K) \]
corresponds to $m = 1, D = (P)$ and the pair $(U(x) = x - a, V(x) = b)$.

(iii) Let $m \leq g$ be a positive integer and $I$ an $m$-element subset of the $(2g + 1)$-element set \{1, $\ldots$, $2g, 2g + 1$\}. We consider an effective divisor
   \[ D_{m,I} = \sum_{i \in I} (\mathcal{M}_i) \]
of degree $m$. Then the divisor $D_{m,I} - m(\infty)$ of degree $0$ is reduced and its linear equivalence class $a_{m,I} := cl(D_{m,I} - m(\infty))$ is a point of order $2$ in $J(K)$ because
   \[ 2cl(D_{m,I} - m(\infty)) = cl(2D_{m,I} - 2m(\infty)) = cl\left(\sum_{i \in I} (2\mathcal{M}_i) - 2m(\infty)\right) = \text{div}\left(\prod_{i \in I} (x - \alpha_i)\right). \]

Consider the polynomials
   \[ U(x) = U_{m,I}(x) := \prod_{i \in I} (x - \alpha_i), \quad V(x) = V_{m,I}(x) := 0. \]

Since $f(x) = \prod_{i=1}^{2g+1} (x - \alpha_i)$ is obviously divisible by $U_{m,I}(x)$, so is the polynomial
   \[ f(x) - V_{m,I}(x)^2 = f(x) - 0^2 = f(x). \]

It follows that $(U_{m,I}(x), 0)$ is the Mumford representation of $a_{m,I}$ since $\mathcal{M}_i = (\alpha_i, 0)$ for all $i$.

Distinct pairs $(m, I)$ clearly correspond to distinct points $a_{m,I}$. Notice that the set of all pairs $(m, I)$ consists of $2^{2g} - 1$ elements (one has to subtract $1$ because we exclude $m = 0$ and empty $I$). At the same time, $2^{2g} - 1$ is the number of elements of order $2$ in $J(K)$. Hence every point of order $2$ in $J(K)$ is of the form $a_{m,I}$ for a unique pair $(m, I)$ (see also [1], Ch. 3a, § 2). Thus, we obtain the Mumford representations of all non-zero halves of zero in $J(K)$.

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

Suppose that \( P = (a, b) \in \mathcal{C}(K) \), that is,
\[
a, b \in K, \quad b^2 = f(a) = \prod_{i=1}^{n}(a - \alpha_i).
\]

Recall that our goal is to divide \( P \) by 2 explicitly in \( J(K) \), that is, to give explicit formulae for the \textit{Mumford representations of all} \( 2^{2g} \) divisor classes \( \text{cl}(D - m(\infty)) \) (with reduced \( D - m(\infty) \)) such that the divisor \( 2D - 2m(\infty) \) is linearly equivalent to \( (P) - (\infty) \), that is, the divisor \( 2D + \iota(P) \) is linearly equivalent to \( (2m + 1)(\infty) \). (We shall see that every such divisor \( D \) has degree \( g \) and its support contains none of the points \( \mathfrak{M}_i \).)

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 \( m \leq 2g + 1 \) and \( \text{supp}(D) \) does not contain \( \infty \). Assume that the divisor \( D - m(\infty) \) is principal.

1. Suppose that \( m \) is odd. Then the following assertions hold.
   (i) \( m = 2g + 1 \) and there is exactly one polynomial \( v(x) \in K[x] \) such that the divisor of the function \( y - v(x) \) coincides with \( D - (2g + 1)(\infty) \). In addition, \( \text{deg}(v) \leq g \).
   (ii) If \( \mathfrak{M}_i \) lies in \( \text{supp}(D) \), then it appears in \( D \) with multiplicity 1.
   (iii) If \( b \) is a non-zero element of \( K \) and a point \( P = (a, b) \in \mathcal{C}(K) \) lies in \( \text{supp}(D) \), then the point \( \iota(P) = (a, -b) \) does not lie in \( \text{supp}(D) \).

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

**Proof.** Let \( h \) be a rational function on \( \mathcal{C} \) whose divisor is equal to \( D - m(\infty) \). Since \( \infty \) is the only pole of \( h \), the function \( h \) is a polynomial in \( x, y \) and, therefore, we can write \( h = s(x)y - v(x) \), where \( s, v \in K[x] \). If \( s = 0 \), then \( h \) has a pole of even order \( 2\text{deg}(v) \) at \( \infty \) and, therefore, \( m = 2\text{deg}(v) \).

Suppose that \( s \neq 0 \). The pole of \( s(x)y \) at \( \infty \) is clearly of odd order \( 2\text{deg}(s) + (2g + 1) \geq (2g + 1) \). Thus the orders of the poles at \( \infty \) for \( s(x)y \) and \( v(x) \) are distinct since they are of different parities. Therefore the order \( m \) of the pole of \( h = s(x)y - v(x) \) coincides with \( \max(2\text{deg}(s) + (2g + 1), 2\text{deg}(v)) \geq 2g + 1 \). It follows that \( m = 2g + 1 \) and, in particular, \( m \) is odd. Hence, \( m \) is even if and only if \( s(x) = 0 \), that is, \( h = -v(x) \). In addition, \( \text{deg}(v) \leq (2g + 1)/2 \), that is, \( \text{deg}(v) \leq g \).

To complete the proof of part (2), it suffices to divide the polynomial \( -v(x) \) by its leading coefficient and denote the result by \( u(x) \). (The uniqueness of the monic polynomial \( u(x) \) is obvious.)

We now prove part (1). Since \( m \) is odd,
\[
m = 2\text{deg}(s) + (2g + 1) > 2\text{deg}(v).
\]
Since \( m \leq 2g + 1 \), we obtain that \( \text{deg}(s) = 0 \), that is, \( s \) is a non-zero element of \( K \) and \( 2\text{deg}(v) < 2g + 1 \). The latter inequality means that \( \text{deg}(v) \leq g \). Dividing \( h \)
by the constant s, we may and will assume that s = 1 and, therefore, h = y − v(x) with
\[ v(x) \in K[x], \quad \deg(v) \leq g. \]
This proves assertion (i). (The uniqueness of v is obvious.) Assertion (ii) is contained in Proposition 13.2(b) on pp. 409, 410 of [2]. To prove assertion (iii), we just follow the arguments on p. 410 of [2] (where it is actually proven). Notice that our \( P = (a, b) \) is a zero of \( y - v(x) \), that is, \( b - v(a) = 0 \). Since \( b \neq 0 \), we have \( v(a) = b \neq 0 \) and the value of the function \( y - v(x) \) at the point \( \iota(P) = (a, -b) \) is \( -b - v(a) = -2b \neq 0 \). Therefore \( \iota(P) \) is not a zero of \( y - v(x) \), that is, \( \iota(P) \) does not lie in \( \operatorname{supp}(D) \). \( \square \)

**Remark 2.3.** Lemma 2.2 (1), (ii), (iii) asserts that if \( m \) is odd, then the divisor \( D - m(\infty) \) is semireduced (see [2], the penultimate paragraph on p. 411).

**Corollary 2.4.** Let \( P = (a, b) \) be a K-point on \( \mathcal{C} \) and let \( D \) be an effective divisor on \( \mathcal{C} \) such that \( m = \deg(D) \leq g \) and \( \operatorname{supp}(D) \) does not contain \( \infty \). Suppose that the divisor \( 2D + \iota(P) - (2m + 1)(\infty) \) of degree 0 is principal. Then the following assertions hold.

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

(ii) If a point \( Q \) lies in \( \operatorname{supp}(D) \), then \( \iota(Q) \) does not lie in \( \operatorname{supp}(D) \). In particular,

1. none of the points \( \mathcal{W}_i \) lies in \( \operatorname{supp}(D) \);
2. the divisor \( D - g(\infty) \) is reduced.

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

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

Let \( d \leq g \) be a positive integer and let \( \Theta_d \subset J \) be the image of the regular map
\[ \mathcal{C}^d \to J, \quad (Q_1, \ldots, Q_d) \mapsto \sum_{i=1}^{d} Q_i \subset J. \]
It is well known that \( \Theta_d \) is an irreducible closed \( d \)-dimensional subvariety of \( J \) that coincides with \( \mathcal{C} \) when \( d = 1 \) and with \( J \) when \( d = g \). In addition, \( \Theta_d \subset \Theta_{d+1} \) for all \( d < g \). Clearly, each \( \Theta_d \) is stable under multiplication by \( -1 \) in \( J \). We write \( \Theta \) for the \((g - 1)\)-dimensional theta divisor \( \Theta_{g-1} \).

**Theorem 2.5.** Suppose that \( g > 1 \) and let
\[ \mathcal{C}_{1/2} := 2^{-1} \mathcal{C} \subset J \]
be the pre-image of \( \mathcal{C} \) under multiplication by 2 in \( J \). Then the intersection of \( \mathcal{C}_{1/2}(K) \) and \( \Theta \) consists of those points of \( J \) whose order divides 2. In particular, the intersection of \( \mathcal{C} \) and \( \mathcal{C}_{1/2} \) consists of \( \infty \) and all the points \( \mathcal{W}_i \). In other words,
\[ \mathcal{C} \cap 2 \cdot \Theta = \{0\}. \]
Remark 2.6. The case $g = 2$ of Theorem 2.5 was done in [8], Proposition 1.5.

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

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

in $J(K)$. We need to prove that $P = \infty$, that is, $P$ is the zero of the 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 the points $Q_j$ are linearly equivalent. Denote the divisors $D$ and $D_m = \sum_{j=1}^{m} (Q_j)$ of degree $m$ on $\mathcal{C}$. Equality in $J$ means that the divisors $2[D - m(\infty)]$ and $(P) - (\infty)$ on $\mathcal{C}$ are linearly equivalent. Hence the divisor $2D + (\iota(P)) - (2m + 1)(\infty)$ is principal. Corollary 2.4 now tells us that $m = g$, which is not the case. The resulting contradiction proves that the intersection of $\mathcal{C}_{1/2}$ and $\Theta$ 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 and 1, that is, it lies in the union of $\infty$ and all the points $\mathfrak{M}_i$. Conversely, since each $\mathfrak{M}_i$ has order 2 in $J(K)$ and $\infty$ has order 1, they all lie in $\mathcal{C}_{1/2}$ (and, of course, in $\mathcal{C}$).

Remark 2.7. It is known ([9], Ch. VI, last paragraph of §11, p.122) that the curve $\mathcal{C}_{1/2}$ is irreducible. (Its projectiveness and smoothness follow readily from the projectiveness of $\mathcal{C} \subset J$, the smoothness of $\mathcal{C}$, and the étaleness of multiplication by 2 in $J$.) See [10] for an explicit description of equations that cut out $\mathcal{C}_{1/2}$ in a projective space.

Theorem 2.8. Suppose that $g > 1$. Let $m$ be a positive integer such that

$$3 \leq m \leq 2g.$$

Then $\mathcal{C}(K)$ contains no points of order $m$ in $J(K)$. In particular, $\mathcal{C}(K)$ contains no points of order 3 or 4.

Remark 2.9. The case $g = 2$ of Theorem 2.8 was done in [8], Proposition 2.1.

Proof of Theorem 2.8. Suppose that there is a point of order $m$ on our curve and denote it by $P$. Consider the effective divisor $D = m(P)$ of degree $m$. Then the divisor $D - m(\infty)$ is principal and its support contains $P$ but does not contain $\iota(P)$.

When $m$ is odd, the desired result follows from Lemma 2.2 (1). Assume that $m$ is even. Clearly, $P$ is neither $\infty$ nor any of the points $\mathfrak{M}_i$, that is, $P \neq \iota(P)$. By Lemma 2.2 (2), the support of $D - m(\infty)$ must contain $\iota(P)$ since it contains $P$. The resulting contradiction shows that there are no points of order $m$ on our curve.

Example 2.10. Assume that $\text{char}(K)$ does not divide $(2g + 1)$. Then, for every non-zero $b \in K$, the reduced polynomial $x^{2g+1} + b^2$ of degree $(2g+1)$ has no multiple roots, and the point $P = (0,b)$ of the hyperelliptic curve

$$\mathcal{C}: y^2 = x^{2g+1} + b^2$$
of genus \( g \) has order \((2g + 1)\) in the Jacobian \( J \) of \( C \). Indeed, the divisor of poles of the rational function \( y - b \) is \((2g + 1)(\infty)\) while \( P \) is the only zero of this function. Since the degree of \( \text{div}(y - b) \) is 0,

\[
\text{div}(y - b) = (2g + 1)(P) - (2g + 1)(\infty) = (2g + 1)((P) - (\infty)).
\]

This means that the \( K \)-point

\[
P \in C(K) \subset J(K)
\]

has a finite order \( m \) that divides \( 2g + 1 \). It is clear that \( m \) is neither 1 nor 2 (since \( P \neq \infty \) and \( y(P) = b \neq 0 \)), that is, \( m \geq 3 \). If \( m < (2g + 1) \), then \( m \leq 2g \) contrary to Theorem 2.8. This proves that the order of \( P \) is \((2g + 1)\).

Notice that hyperelliptic curves of odd degree and genus 2 with points of order \( 5 = 2 \times 2 + 1 \) are classified in [11].

Remark 2.11. If \( \text{char}(K) = 0 \) and \( g > 1 \), then the famous theorem of Raynaud [12] (conjectured by Manin and Mumford) asserts that an arbitrary smooth projective curve of genus \( g \) over \( K \) embedded in its Jacobian contains only finitely many torsion points.

In the rest of this section we obtain some information about torsion points on certain subvarieties \( \Theta_d \) in the case when \( C \) has ‘large monodromy’. In what follows we use the notation \([?]\) for the integer part of a real number ?.

Let us start with the following assertion.

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

\[
k < N, \quad N + k \leq 2g.
\]

We put

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

Let \( K_0 \) be a subfield of \( K \) such that \( f(x) \in K_0[x] \). Suppose that \( a \in J(K) \) lies on \( \Theta_{d_{(N+k)}} \) and there are \( k \) (not necessarily distinct) \( K_0 \)-linear automorphisms

\[
\{\sigma_1, \ldots, \sigma_k\} \subset \text{Aut}(K/K_0)
\]

of the field \( K \) such that \( \sum_{l=1}^{k} \sigma_l(a) = Na \) or \(-Na\). Then \( a \) has order 1 or 2 in \( J(K) \).

**Proof.** It is clear that

\[
d_{(N+k)} \leq \frac{2g}{N+k} \leq \frac{2g}{2+1} \leq g, \quad (N + k) \cdot d_{(N+k)} \leq 2g < 2g + 1.
\]

Assume that \( 2a \neq 0 \) in \( J(K) \). We need to arrive at a contradiction. One can find a positive integer \( r \leq d_{(N+k)} \leq 2g + 1 \) and a sequence of \( r \) points \( P_1, \ldots, P_r \) in \( C(K) \setminus \{\infty\} \) such that the linear equivalence class of \( D := \sum_{j=1}^{r} (P_j) - r(\infty) \) is equal to \( a \). We may assume that \( r \) is the smallest positive integer with this property for the given \( a \). Then the divisor \( D \) is reduced. Indeed, if \( D \) is not reduced, then \( r \geq 2 \) and we may assume without loss of generality that (say) \( P_r = \iota(P_{r-1}) \), that
is, the divisor \((P_{r-1}) + (P_r) - 2(\infty)\) is principal. Since \(a \neq 0\), we have \(r > 2\) and, therefore, \(\tilde{D}\) is linearly equivalent to

\[
\tilde{D} - ((P_{r-1}) + (P_r) - 2(\infty)) = \sum_{j=1}^{r-2} (P_j) - (r-2)(\infty).
\]

This contradicts the minimality of \(r\), thus proving that \(\tilde{D}\) is reduced.

We may assume that (say) \(P_1\) does not coincide with any of the \(2\mathfrak{M}_i\) (here we are using the assumption that \(2a \neq 0\)) and \(P_1\) has the largest multiplicity in \(\tilde{D}\) among \(\{P_1, \ldots, P_r\}\) (we denote this multiplicity by \(M\)). Since \(\tilde{D}\) is reduced, none of the points \(P_j\) coincides with \(\nu P_1\). For any \(l \in \{1, \ldots, k\}\), the divisor \(\sigma_l(\tilde{D}) = \sum_{j=1}^{r} (\sigma_lP_j) - r(\infty)\) is also reduced and its linear equivalence class is equal to \(\sigma_l a\). In particular, the multiplicity of each point \(\sigma_lP_j\) in the divisor \(\sigma_l(\tilde{D})\) does not exceed \(M\). In a similar vein, the multiplicity of each \(\nu\sigma_lP_j\) in \(\sigma_l(\tilde{D})\) does not exceed \(M\) for every \(l\). It follows that if \(P\) is any point of \(\mathfrak{C}(K)\setminus\{\infty\}\) that does not lie in the support of \(\tilde{D}\), then its multiplicity in \(N\tilde{D} + \nu(\sum_{l=1}^{k} \sigma_l(\tilde{D}))\) is a non-negative integer not exceeding \(kM\). In addition, the multiplicity of \(P\) in the divisor \(N\tilde{D} + \sum_{l=1}^{k} \sigma_l(\tilde{D})\) is a non-negative integer not exceeding \(kM\). Notice that \(P_1\) lies in the supports of both of the divisors

\[
N\tilde{D} + \nu\left(\sum_{l=1}^{k} \sigma_l(\tilde{D})\right) \quad \text{and} \quad N\tilde{D} + \left(\sum_{l=1}^{k} \sigma_l(\tilde{D})\right),
\]

and its multiplicities (in both cases) are greater than or equal to \(NM\).

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

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

is a principal divisor on \(\mathfrak{C}\). Since

\[
m := r(N + k) \leq (N + k) \cdot d_{(N+k)} \leq 2g < 2g + 1,
\]

we are in position to apply Lemma 2.2, which tells us at once that \(m\) is even and there is a monic polynomial \(u(x)\) of degree \(m/2\) whose divisor coincides with \(N\tilde{D} + \nu(\sum_{l=1}^{k} \sigma_l(\tilde{D}))\). It follows that every point \(Q \in \mathfrak{C}(K)\setminus\{\infty\}\) appears in \(N\tilde{D} + \nu(\sum_{l=1}^{k} \sigma_l(\tilde{D}))\) with the same (non-negative) multiplicity as \(\nu Q\). Hence the point \(Q = \nu P_1\) appears in \(N\tilde{D} + \nu(\sum_{l=1}^{k} \sigma_l(\tilde{D}))\) with the same multiplicity as \(P_1\). On the other hand, since \(\nu P_1\) does not appear in \(\tilde{D}\), its multiplicity in \(N\tilde{D} + \nu(\sum_{l=1}^{k} \sigma_l(\tilde{D}))\) does not exceed \(kM\). Since the multiplicity of \(P_1\) in \(N\tilde{D} + \nu(\sum_{l=1}^{k} \sigma_l(\tilde{D}))\) is greater than or equal to \(NM\), we conclude that \(NM \leq kM\). But this is not the case since \(k < N\). This gives us the desired contradiction.

If \(\sum_{l=1}^{k} \sigma_l(a) = -Na\), then the same arguments for the principal divisor

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

also lead to a contradiction. \(\square\)
2.13. Let $K_0$ be a subfield of $K$ such that $f(x) \in K_0[x]$ and let $\bar{K}_0$ be the algebraic closure of $K_0$ in $K$. (For example, one may take for $K_0$ the field which is generated over the prime subfield of $K$ by the coefficients of the polynomial $f(x)$.) We write $\text{Gal}(K_0)$ for the absolute Galois group

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

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

Consider the following Galois properties of torsion points in $J(K)$.

(M3) If $a \in J(\bar{K}_0)$ is a torsion point whose order is a power of 2, then there is an automorphism $\sigma \in \text{Gal}(K_0)$ such that $\sigma(a) = 3a$.

(M2) If $b \in J(\bar{K}_0)$ is a point of odd order, then there is an automorphism $\tau \in \text{Gal}(K_0)$ such that $\tau(b) = 2b$.

(M) Let $a, b \in J(\bar{K}_0)$ be torsion points such that the order of $a$ is a power of 2 and the order of $b$ is odd. Then there are $\sigma_1, \sigma_2 \in \text{Gal}(K_0)$ such that $\sigma_1(a) = -a$, $\sigma_1(b) = 2b$, $\sigma_2(a) = 5a$, $\sigma_2(b) = 2b$.

Theorem 2.14. (i) Suppose that $g \geq 2$ and $J$ enjoys the property (M3). Put

$$d_{(4)} = \left\lfloor \frac{2g}{4} \right\rfloor = \left\lfloor \frac{g}{2} \right\rfloor.$$ 

Let $a \in J(K)$ be a torsion point lying in $\Theta_{d_{(4)}}$. If the order of $a$ is a power of 2, then it is either 1 or 2.

(ii) Suppose that $g \geq 2$ and $J$ enjoys the property (M2). Put

$$d_{(3)} = \left\lfloor \frac{2g}{3} \right\rfloor.$$ 

Let $b \in J(K)$ be a torsion point of odd order lying in $\Theta_{d_{(3)}}$. Then $b = 0 \in J(K)$.

(iii) Suppose that $g \geq 3$ and $J$ enjoys the property (M). Put

$$d_{(6)} = \left\lfloor \frac{2g}{6} \right\rfloor = \left\lfloor \frac{g}{3} \right\rfloor.$$ 

Let $c \in J(K)$ be a torsion point lying in $\Theta_{d_{(6)}}$. Then the order of $c$ is either 1 or 2.

Remark 2.15. In the case when $g = 2$, an analogue of Theorem 2.14 (i), (ii) was proven in [8], Corollary 1.6.

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

\[
\sigma_1(a) = -a, \quad \sigma_1(b) = 2b, \quad \sigma_2(a) = 5a, \quad \sigma_2(b) = 2b.
\]

It follows that

\[
\sigma_1(c) + \sigma_2(c) = \sigma_1(a) + \sigma_1(b) + \sigma_2(a) + \sigma_2(b) = -a + 2b + 5a + 2b = 4(a + b) = 4c,
\]

that is, \( \sigma_1(c) + \sigma_2(c) = 4c \). The desired result now 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. Consider a set \( \{\alpha_1, \ldots, \alpha_{2g+1}\} \subset \mathbb{C} \) of \( (2g+1) \) algebraically independent transcendental complex numbers. Put \( K_0 = \mathbb{Q}(\alpha_1, \ldots, \alpha_{2g+1}) \), where \( \mathbb{Q} \) is the field of rational numbers. It follows from results of Poonen and Stoll ([13], Theorem 7.1 and its proof) and Yelton ([6], Theorem 1.1 and Proposition 2.2) that the Jacobian \( J \) of the generic hyperelliptic curve

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

enjoys the following properties.

Choose arbitrary odd integers \( (2n_1 + 1) \) and \( (2n_2 + 1) \) and arbitrary non-negative integers \( m_1 \) and \( m_2 \). Let \( a, b \in J(K_0) \) be torsion points such that the order of \( a \) is a power of 2 and the order of \( b \) is odd. Then there are \( \sigma_1, \sigma_2 \in \text{Gal}(K_0) \) such that

\[
\sigma_1(a) = (2n_1 + 1)a, \quad \sigma_1(b) = 2^{m_1}b, \quad \sigma_2(a) = (2n_2 + 1)a, \quad \sigma_2(b) = 2^{m_2}b.
\]

Choosing \( n_1 = 1 \), we obtain that \( J \) enjoys the property (M3). Choosing \( m_1 = 1 \), we obtain that \( J \) enjoys the property (M2). Choosing

\[
n_1 = 1, \quad n_2 = 2, \quad m_1 = m_2 = 1,
\]

we obtain that \( J \) enjoys the property (M). By Theorem 2.14, the torsion points of \( J(\mathbb{C}) \) possess the following properties.

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

(ii) If \( b \in J(\mathbb{C}) \) is a torsion point of odd order lying on \( \Theta_{2g/3} \), then it is equal to \( 0 \in J(\mathbb{C}) \).

(iii) If \( g \geq 3 \), then any torsion point \( c \in J(\mathbb{C}) \) lying on \( \Theta_{g/3} \) has order 1 or 2.

Notice that Poonen and Stoll ([13], Theorem 7.1) proved that all the torsion points of \( J(\mathbb{C}) \) lying on \( C = \Theta_1 \) are of order 1 or 2. On the other hand, it is well known that \( J \) is a simple complex Abelian variety. A theorem of Raynaud [14] now 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

If \( n \) and \( i \) are positive integers and \( r = \{r_1, \ldots, r_n\} \) is a sequence of \( n \) elements \( r_i \in K \), then we write

\[
s_i(r) = s_i(r_1, \ldots, r_n) \in K
\]

for the value of the \( i \)th basic symmetric function at \( r_1, \ldots, r_n \). If we put \( r_{n+1} = 0 \), then \( s_i(r_1, \ldots, r_n) = s_i(r_1, \ldots, r_n, 0) \).

Suppose that 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 \( a \in J(K) \) such that

\[
P = 2a \in J(K).
\]

We choose such an \( a \). Then there is exactly one effective divisor

\[
D = D(a)
\]

of positive degree \( m \) on \( \mathcal{C} \) such that \( \text{supp}(D) \neq \emptyset \), the divisor \( D - m(\infty) \) is reduced and

\[
m \leq g, \quad \text{cl}(D - m(\infty)) = a.
\]

It follows that the divisor \( 2D + (\iota(P)) - (2m + 1)(\infty) \) is principal and, by Corollary 2.4, \( m = g \) and \( \text{supp}(D) \) contains none of the points \( \mathfrak{W}_i \). (In addition, \( D - g(\infty) \) is reduced.) Write

\[
D = D(a) = \sum_{j=1}^{g} (Q_j)
\]

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

\[
c_j \neq \alpha_i \quad \forall i, j.
\]

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

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

of degree zero is a divisor of the function \( y - v_D(x) \). Since the point \( \iota(P) = (a, -b) \) and all the points \( Q_j \) are zeros of \( y - v_D(x) \), we have

\[
b = -v_D(a), \quad d_j = v_D(c_j) \quad \text{for all} \quad j = 1, \ldots, g.
\]

It follows from Proposition 13.2 on pp. 409, 410 of [2] that

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

In particular, the polynomial \( f(x) - v_D(x)^2 \) is divisible by

\[
u_D(x) := \prod_{j=1}^{g} (x - c_j).
\]
Remark 3.1. To sum up, we have the following expression for the divisor $D$:

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

and the monic polynomial $u_D(x) = \prod_{j=1}^{g} (x - c_j)$ of degree $g$ divides $f(x) - v_D(x)^2$. Thus (see the beginning of §2), the pair $(u_D, v_D)$ is the Mumford representation of $a$ 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, replacing the polynomial $v_D(x)$ by its remainder on division by $u_D(x)$, we get the Mumford representation of $a$ (see below). In particular, when $\deg(v_D) = g$, this remainder is equal to $v_D(x) - cu_D(x)$, where $c \in K$ is the leading coefficient of $v_D(x)$.

Putting $x = \alpha_i$ in (3), we obtain

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

that is,

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

Since none of the differences $c_j - \alpha_i$ vanishes, we can define

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

(5)

where

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

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

(6)

It is clear that all the $r_i$ are distinct elements of $K$ because their squares are obviously distinct. (By the same token, $r_{j_1} \neq \pm r_{j_2}$ if $j_1 \neq j_2$.) Notice that

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

(7)

because

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

(8)

We now obtain that

$$r_i = \frac{v_D(a - r_i^2)}{\prod_{j=1}^{g} (r_i^2 - a + c_j)},$$
that is,
\[ r_i \prod_{j=1}^{g} (r_i^2 - a + c_j) - v_D(a - r_i^2) = 0 \quad \text{for all } i = 1, \ldots, 2g, 2g + 1. \]

This means that the monic polynomial
\[ h_r(t) := t \prod_{j=1}^{g} (t^2 - a + c_j) - v_D(a - t^2) \]
of degree \((2g+1)\) (we recall that \(\deg(v_D) \leq g\)) has \((2g+1)\) distinct roots \(r_1, \ldots, r_{2g+1}\). Hence,
\[ h_r(t) = \prod_{i=1}^{2g+1} (t - r_i). \]

It is clear that \(t \prod_{j=1}^{g} (t^2 - a + c_j)\) coincides with the odd part of \(h_r(t)\) while \(-v_D(a - t^2)\) coincides with the even part. In particular, putting \(t = 0\), we have
\[ (-1)^{2g+1} \prod_{i=1}^{2g+1} r_i = -v_D(a) = b, \]
that is,
\[ \prod_{i=1}^{2g+1} r_i = -b. \] (9)

Here and in what follows,
\[ r = r_D := (r_1, \ldots, r_{2g+1}) \in K^{2g+1}. \]

Since
\[ s_i (r) = s_i (r_1, \ldots, r_{2g+1}) \]
is the value of the \(i\)th basic symmetric function at \(r_1, \ldots, r_{2g+1}\), we have
\[ h_r(t) = t^{2g+1} + \sum_{i=1}^{2g+1} (-1)^i s_i (r) t^{2g+1-i} = \left[ t^{2g+1} + \sum_{i=1}^{2g} (-1)^i s_i (r) t^{2g+1-i} \right] + b. \]

(Since
\[ s_{2g+1} (r) = \prod_{i=1}^{2g+1} r_i = -b, \]
the constant term of \(h_r(t)\) is \(b\).) Then
\[ t \prod_{j=1}^{g} (t^2 - a + c_j) = t^{2g+1} + \sum_{j=1}^{g} s_{2j} (r) t^{2g+1-2j}, \]
\[ -v_D(a - t^2) = \left[ -\sum_{j=1}^{g} s_{2j-1} (r) t^{2g-2j+2} \right] + b. \]
It follows that
\[ \prod_{j=1}^{g}(t-a+c_j) = t^g + \sum_{j=1}^{g}s_{2j}(r)t^{g-j}, \]

\[ v_D(a-t) = \sum_{j=1}^{g}s_{2j-1}(r)t^{g-j+1} - b \]

and, therefore,
\[ v_D(t) = \left[ \sum_{j=1}^{g}s_{2j-1}(r)(a-t)^{g-j+1} \right] - b. \] (10)

It is also clear that if we consider the monic polynomial
\[ U_r(t) := u_D(t) = \prod_{j=1}^{g}(t-c_j) \]

of degree \( g \), then
\[ U_r(t) = (-1)^g (a-t)^g + \sum_{j=1}^{g}s_{2j}(r)(a-t)^{g-j}. \] (11)

Recall that \( \deg(v_D) \leq g \) and notice that the coefficient of \( v_D(x) \) at \( x^g \) is \( (-1)^g s_1(r) \). This implies that the polynomial
\[ V_r(t) := v_D(t) - (-1)^g s_1(r)U_r(t) \]
\[ = \left[ \sum_{j=1}^{g}s_{2j-1}(r)(a-t)^{g-j+1} \right] - b - s_1(r)(a-t)^g + \sum_{j=1}^{g}s_{2j}(r)(a-t)^{g-j} \]
\[ = \sum_{j=1}^{g}(s_{2j+1}(r) - s_1(r)s_{2j}(r))(a-t)^{g-j} \] (12)
has degree \( < g \), that is,
\[ \deg(V_r) < \deg(U_r) = g. \]

It is clear that \( f(x) - V_r(x)^2 \) is still divisible by \( U_r(x) \) because the polynomial \( u_D(x) = U_r(x) \) divides \( f(x) - v_D(x)^2 \) and \( v_D(x) - V_r(x) \). On the other hand,
\[ d_j = v_D(c_j) = V_r(c_j) \quad \text{for all} \quad j = 1, \ldots, g \]
because \( U_r(x) \) divides \( v_D(x) - V_r(x) \) and vanishes at all \( c_j \). Actually, \( \{c_1, \ldots, c_g\} \) is a list of all the roots (with multiplicities) of \( U_r(x) \). Hence,
\[ D = D(a) = \sum_{j=1}^{g}(Q_j), \quad Q_j = (c_j, v_D(c_j)) = (c_j, V_r(c_j)) \quad \forall \ j = 1, \ldots, g. \]

It follows (again see the beginning of § 2) that the pair \( (U_r(x), V_r(x)) \) is the Mumford representation of \( \text{cl}(D - g(\infty)) = a. \)
Thus the formulae (11) and (12) give us an explicit construction of the divisor \( D(\alpha) \) and the point \( \alpha \) in terms of the tuple \( \mathbf{r} = (r_1, \ldots, r_{2g+1}) \) for each of the \( 2^{2g} \) choices of \( \alpha \) with \( 2\alpha = P \in J(K) \). On the other hand, in view of (6)–(8), there are exactly \( 2^{2g} \) possibilities for choosing the square roots \( \sqrt{a-\alpha_i} \) \((1 \leq i \leq 2g)\) with product \(-b\). Combining this observation with (9), we obtain that for every choice of square roots \( \sqrt{a-\alpha_i} \) with \( \prod_{i=1}^{2g+1} \sqrt{a-\alpha_i} = -b \) there is precisely one \( \alpha \in J(K) \) with \( 2\alpha = P \) such that the corresponding element \( r_i \) defined by (5) coincides with the chosen \( \sqrt{a-\alpha_i} \) for all \( i = 1, \ldots, 2g+1 \), and the Mumford representation \((U_\mathbf{r}(x), V_\mathbf{r}(x))\) of this \( \alpha \) is given by (11), (12). This gives us the following assertion.

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

\[
M_{1/2, P} := \{ \alpha \in J(K) \mid 2\alpha = P \in C(K) \subset J(K) \}
\]

can be described as follows. Let \( \mathcal{R}_{1/2, P} \) be the set of all \((2g+1)\)-tuples \( \mathbf{r} = (r_1, \ldots, r_{2g+1}) \) of elements of \( K \) such that

\[
r_i^2 = a - \alpha_i \quad \text{for all} \quad i = 1, \ldots, 2g, 2g+1, \quad \prod_{i=1}^{2g+1} r_i = -b.
\]

Let \( s_i(\mathbf{r}) \) be the value of the \( i \)th basic symmetric function at \( r_1, \ldots, r_{2g+1} \). We put

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

\[
V_\mathbf{r}(x) = \sum_{j=1}^{g} \left( s_{2j+1}(\mathbf{r}) - s_1(\mathbf{r}) s_{2j}(\mathbf{r}) \right) (a-x)^{g-j}.
\]

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

\[
\alpha_\mathbf{r} = \text{cl}(D - g(\infty)) \in J(K), \quad 2\alpha_\mathbf{r} = P,
\]

where the divisor

\[
D = D(\alpha_\mathbf{r}) = \sum_{j=1}^{g} (Q_j), \quad Q_j = (c_j, V_\mathbf{r}(c_j)) \in C(K) \quad \text{for all} \quad j = 1, \ldots, g.
\]

In addition, none of \( \alpha_i \) is a root of \( U_\mathbf{r}(x) \) (that is, the polynomials \( U_\mathbf{r}(x) \) and \( f(x) \) are relatively prime) and

\[
r_i = s_1(\mathbf{r}) + (-1)^g \frac{V_\mathbf{r}(\alpha_i)}{U_\mathbf{r}(\alpha_i)} \quad \text{for all} \quad i = 1, \ldots, 2g, 2g+1.
\]

**Proof.** Actually, we have already proven all the assertions of Theorem 3.2 except for the last formula for \( r_i \). It follows from (4) and (5) that

\[
r_i = (-1)^g \frac{v_{D(\alpha_\mathbf{r})}(\alpha_i)}{u_{D(\alpha_\mathbf{r})}(\alpha_i)} = (-1)^g \frac{v_{D(\alpha_\mathbf{r})}(\alpha_i)}{U_\mathbf{r}(\alpha_i)}.
\]
It follows from (12) that
\[ v_{D(a_i)}(x) = (-1)^g s_1(r) U_\tau(x) + V_\tau(x). \]

This implies that
\[ v_1 = (-1)^g \frac{(-1)^g s_1(r) U_\tau(\alpha_i) + V_\tau(\alpha_i)}{U_\tau(\alpha_i)} = s_1(r) + (-1)^g \frac{V_\tau(\alpha_i)}{U_\tau(\alpha_i)}. \]

**Corollary 3.3.** Under the notation and hypotheses of Theorem 3.2, we have
\[ 2g \cdot s_1(r) = (-1)^{g+1} \sum_{i=1}^{2g+1} \frac{V_\tau(\alpha_i)}{U_\tau(\alpha_i)}. \]

In particular, if \( \text{char}(K) \) does not divide \( g \), then
\[ s_1(r) = \frac{(-1)^{g+1}}{2g} \sum_{i=1}^{2g+1} \frac{V_\tau(\alpha_i)}{U_\tau(\alpha_i)}. \]

On the other hand, if \( \text{char}(K) \) divides \( g \), then
\[ \sum_{i=1}^{2g+1} \frac{V_\tau(\alpha_i)}{U_\tau(\alpha_i)} = 0. \]

**Proof.** It follows from the last assertion of Theorem 3.2 that
\begin{align*}
s_1(r) &= \sum_{i=1}^{2g+1} v_i = \sum_{i=1}^{2g+1} \left( s_1(r) + (-1)^g \frac{V_\tau(\alpha_i)}{U_\tau(\alpha_i)} \right) \\
&= (2g + 1)s_1(r) + (-1)^g \sum_{i=1}^{2g+1} \frac{V_\tau(\alpha_i)}{U_\tau(\alpha_i)}. \end{align*}

This implies that
\[ 0 = 2g \cdot s_1(r) + (-1)^g \sum_{i=1}^{2g+1} \frac{V_\tau(\alpha_i)}{U_\tau(\alpha_i)}, \]
that is,
\[ 2g \cdot s_1(r) = (-1)^{g+1} \sum_{i=1}^{2g+1} \frac{V_\tau(\alpha_i)}{U_\tau(\alpha_i)}. \]

**Corollary 3.4.** Under the notation and hypotheses of Theorem 3.2, suppose that \( i \) and \( l \) are distinct integers such that
\[ 1 \leq i, l \leq 2g + 1. \]

Then
\[ s_1(r) = \frac{(-1)^g}{2} \frac{(\alpha_i + (V_\tau(\alpha_i)/U_\tau(\alpha_i))^2) - (\alpha_i + (V_\tau(\alpha_i)/U_\tau(\alpha_i))^2)}{V_\tau(\alpha_i)/U_\tau(\alpha_i) - V_\tau(\alpha_i)/U_\tau(\alpha_i)}. \]
Proof. We have

\[ r_i = s_1(r) + (-1)^g \frac{V_r(\alpha_i)}{U_r(\alpha_i)}, \quad r_l = s_1(r) + (-1)^g \frac{V_r(\alpha_l)}{U_r(\alpha_l)}. \]

Recall that

\[ r_i^2 = a - \alpha_i \neq a - \alpha_l = r_l^2. \]

In particular, \( r_i \neq r_l \) and, therefore,

\[ \frac{V_r(\alpha_i)}{U_r(\alpha_i)} \neq \frac{V_r(\alpha_l)}{U_r(\alpha_l)}. \]

We have

\[
\begin{align*}
\alpha_l - \alpha_i &= (a - \alpha_i) - (a - \alpha_l) = r_i^2 - r_l^2 \\
&= \left( s_1(r) + (-1)^g \frac{V_r(\alpha_i)}{U_r(\alpha_i)} \right)^2 - \left( s_1(r) + (-1)^g \frac{V_r(\alpha_l)}{U_r(\alpha_l)} \right)^2 \\
&= (-1)^g 2 s_1(r) \left( \frac{V_r(\alpha_i)}{U_r(\alpha_i)} - \frac{V_r(\alpha_l)}{U_r(\alpha_l)} \right) + \left( \frac{V_r(\alpha_i)}{U_r(\alpha_i)} \right)^2 - \left( \frac{V_r(\alpha_l)}{U_r(\alpha_l)} \right)^2.
\end{align*}
\]

It follows that

\[ (-1)^g 2 s_1(r) \left( \frac{V_r(\alpha_i)}{U_r(\alpha_i)} - \frac{V_r(\alpha_l)}{U_r(\alpha_l)} \right) = \left( \alpha_i + \left( \frac{V_r(\alpha_l)}{U_r(\alpha_l)} \right)^2 \right) - \left( \alpha_i + \left( \frac{V_r(\alpha_i)}{U_r(\alpha_i)} \right)^2 \right). \]

This implies that

\[ s_1(r) = \frac{(-1)^g}{2} \frac{\left( \alpha_i + \left( \frac{V_r(\alpha_l)}{U_r(\alpha_l)} \right)^2 \right) - \left( \alpha_i + \left( \frac{V_r(\alpha_i)}{U_r(\alpha_i)} \right)^2 \right)}{V_r(\alpha_i)/U_r(\alpha_i) - V_r(\alpha_l)/U_r(\alpha_l)}. \]

Remark 3.5. Suppose that \( r = (r_1, \ldots, r_{2g+1}) \in \mathcal{R}_{1/2,P} \) with \( P = (a, b) \). Then for all \( i = 1, \ldots, 2g, 2g + 1, \)

\[ (-r_i)^2 = r_i^2 = a - \alpha_i \]

and

\[ \prod_{i=1}^{2g+1} (-r_i) = (-1)^{2g+1} \prod_{i=1}^{2g+1} r_i = (-b) = b. \]

This means that

\[ -r = (-r_1, \ldots, -r_{2g+1}) \in \mathcal{R}_{1/2,\iota(P)} \]

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

\[ U_{-r}(x) = U_r(x), \quad V_{-r}(x) = -V_r(x) \]

and, therefore, \( a_{-r} = -a_r \).

Remark 3.6. The last assertion of Theorem 3.2, combined with Corollary 3.4, enables us to reconstruct \( r = (r_1, \ldots, r_{2g+1}) \) and \( P = (a, b) \) explicitly if we are given the polynomials \( U_r(x), V_r(x) \) (and, of course, \( \{\alpha_1, \ldots, \alpha_{2g+1}\} \)).
Example 3.7. Take the point \( W_{2g+1} = (\alpha_{2g+1}, 0) \) as \( P = (a, b) \). Then \( b = 0 \) and \( r_{2g+1} = 0 \). We have \( 2^{2g} \) arbitrary independent choices of (non-zero) square roots \( r_i = \sqrt{\alpha_{2g+1} - \alpha_i} \) with \( 1 \leq i \leq 2g \) (and every such choice yields an element of \( \mathfrak{R}_{1/2, P} \) ). Theorem 3.2 (with \( a = \alpha_{2g+1}, b = 0 \)) now gives us all the \( 2^{2g} \) points \( \alpha_i \) of order 4 in \( J(K) \) with \( 2\alpha_i = W_{2g+1} \). Namely, let \( s_i \) be the value of the \( i \)th basic symmetric function at \( (r_1, \ldots, r_{2g}) \). Then the Mumford representation \((U_r, V_r)\) of \( \alpha_i \) is given by

\[
U_r(x) = (-1)^g \left[ (\alpha_{2g+1} - x)^g + \sum_{j=1}^{g} s_{2j}(\alpha_{2g+1} - x)^{g-j} \right],
\]

\[
V_r(x) = \sum_{j=1}^{g} (s_{2j+1} - s_1 s_{2j})(\alpha_{2g+1} - x)^{g-j}.
\]

In particular, if \( \alpha_{2g+1} = 0 \) then \( r_i = \sqrt{-\alpha_i} \) for all \( i = 1, \ldots, 2g \),

\[
U_r(x) = x^g + \sum_{j=1}^{g} (-1)^j s_{2j} x^{g-j}, \quad V_r(x) = \sum_{j=1}^{g} (s_{2j+1} - s_1 s_{2j})(-x)^{g-j}.
\]

Bibliography

[1] D. Mumford, Tata lectures on theta, vol. II, Progr. Math., vol. 43, Birkhäuser Boston, Boston, MA 1984; Russian transl., Mir, Moscow 1988.
[2] L. C. Washington, Elliptic curves. Number theory and cryptography, 2nd ed., Discrete Math. Appl. (Boca Raton), Chapman-Hall, Boca Raton, FL 2008.
[3] M. Stoll, “Chabauty without the Mordell–Weil group”, Algorithmic and experimental methods in algebra, geometry, and number theory, Springer, Cham 2017, pp. 623–663; arXiv:1506.04286.
[4] B. M. Bekker and Yu. G. Zarhin, “Division by 2 of rational points on elliptic curves”, Algebra i Analiz 29:4 (2017), 196–239; English transl., St. Petersburg Math. J. 29:4 (2018), 683–713.
[5] E. F. Schaefer, “2-descent on the Jacobians of hyperelliptic curves”, J. Number Theory 51:2 (1995), 219–232.
[6] J. Yelton, “Images of 2-adic representations associated to hyperelliptic Jacobians”, J. Number Theory 151 (2015), 7–17.
[7] M. Stoll, Arithmetic of hyperelliptic curves, Summer semester 2014, Univ. of Bayreuth 2014; http://www.mathe2.uni-bayreuth.de/stoll/teaching/ArithHypKurven-SS2014/Skript-ArithHypCurves-pub-screen.pdf.
[8] J. Boxall and D. Grant, “Examples of torsion points on genus two curves”, Trans. Amer. Math. Soc. 352:10 (2000), 4533–4555.
[9] J.-P. Serre, Groupes algébriques et corps de classes, Publ. Inst. Math. Univ. Nancago, vol. VII, Hermann, Paris 1959; English transl. of 2nd French ed., J.-P. Serre, Algebraic groups and class fields, Grad. Texts in Math., vol. 117, Springer-Verlag, New York 1988; Russian transl., Mir, Moscow 1968.
[10] N. Bruin and E. V. Flynn, “Towers of 2-covers of hyperelliptic curves”, Trans. Amer. Math. Soc. 357:11 (2005), 4329–4347.
[11] J. Boxall, D. Grant, and F. Leprévost, “5-torsion points on curves of genus 2”, *J. London Math. Soc. (2)* 64:1 (2001), 29–43.

[12] M. Raynaud, “Courbes sur une variété abélienne et points de torsion”, *Invent. Math.* 71:1 (1983), 207–233.

[13] B. Poonen and M. Stoll, “Most odd degree hyperelliptic curves have only one rational point”, *Ann. of Math. (2)* 180:3 (2014), 1137–1166.

[14] M. Raynaud, “Sous-variétés d’une variété abélienne et points de torsion”, *Arithmetic and geometry*, vol. I, Papers dedicated to I. R. Shafarevich on the occasion of his sixtieth birthday, Progr. Math., vol. 35, Birkhäuser Boston, Boston, MA 1983, pp. 327–352.

Yuri G. Zarhin
Pennsylvania State University,
Department of Mathematics, PA, USA
E-mail: zarhin@math.psu.edu